Dell EMC Data Domain® Operating System

Version 6.2

Guide d'administration

302-005-407
REV. 01

DELL EMC

Publié en Décembre 2018

EMC Computer Systems France
River Ouest 80 quai Voltaire CS 21002 95876 Bezons Cedex
Tél. : +33 1 39 96 90 00 Fax : +33 1 39 96 99 99
www.DellEMC.com/fr-fr/index.htm

SOMMAIRE

Préface

En vue d'améliorer la qualité de sa gamme de produits, Data Domain publie régulièrement des révisions de ses matériels et logiciels. Par conséquent, il se peut que certaines fonctions décrites dans le présent document ne soient pas prises en charge par l'ensemble des versions des logiciels ou matériels actuellement utilisés. Les Notes de mises à jour du produit contiennent les informations les plus récentes au sujet des fonctionnalités des produits, des mises à jour logicielles, des guides de compatibilité logicielle et vous renseignent sur les produits, licences et services Data Domain.

Si un produit ne fonctionne pas correctement ou ne fonctionne pas comme indiqué dans ce document, contactez un professionnel du support technique .

Remarque

Les informations figurant dans ce document sont exactes à la date de publication. Consultez le Support en ligne (https://support.emc.com) afin de vous assurer que vous utilisez la version la plus récente de ce document.

Objectif

Ce guide présente la façon de gérer les systèmes Data Domain® en insistant sur les procédures qui utilisent Data Domain System Manager (DD System Manager), une interface graphique (GUI) de type navigateur. Si une tâche administrative majeure n'est pas prise en charge dans DD System Manager, les commandes d'interface de ligne de commande (CLI) sont décrites.

Remarque

- DD System Manager était anciennement appelé Enterprise Manager.
- Dans certains cas, une commande de CLI peut offrir plus d'options que celles proposées par la fonction correspondante de DD System Manager. Pour obtenir la description complète d'une commande et de ses options, consultez le *Guide de référence des commandes de Data Domain Operating System*.

Audience

Ce guide s'adresse aux administrateurs système qui connaissent les modules logiciels de sauvegarde standard et l'administration générale des sauvegardes.

Documentation connexe

Les documents suivants relatifs au système Data Domain fournissent des informations complémentaires :

- Guide d'installation et de configuration de votre système, par exemple le *Guide d'installation et de configuration du système Data Domain DD9300*
- *Guide des fonctions et caractéristiques techniques du matériel Data Domain*
- *Guide d'installation par USB de Data Domain Operating*
- *Guide d'installation par DVD de Data Domain Operating System*
- *Notes de mise à jour de Data Domain Operating System*
- *Guide de configuration initiale de Data Domain Operating System*
- *Guide de configuration de la sécurité de Data Domain*

- *Livre blanc sur la haute disponibilité de Data Domain Operating System*
- *Guide de référence des commandes de Data Domain Operating System*
- *Référence rapide sur la base de données MIB de Data Domain Operating System*
- *Guide d'utilisation de Data Domain Operating System Offline Diagnostics Suite*
- Guides de remplacement sur site des composants de votre système, par exemple *Field Replacement Guide, Data Domain DD4200, DD4500, and DD7200 Systems, IO Module and Management Module Replacement or Upgrade*
- *Guide de mise à niveau du contrôleur système Data Domain*
- *Guide du matériel Data Domain Expansion Shelf* (pour les modèles de tiroir ES30/ FS15 ou DS60)
- *Guide d'administration de Data Domain Boost pour l'intégration des partenaires*
- *Guide d'administration de Data Domain Boost for OpenStorage*
- *Guide d'administration de Data Domain Boost for Oracle Recovery Manager*
- *Statement of Volatility for the Data Domain DD2500 System*
- *Statement of Volatility for the Data Domain DD4200, DD4500, or DD7200 System*
- *Statement of Volatility for the Data Domain DD6300, DD6800, or DD9300 System*
- *Statement of Volatility for the Data Domain DD9500 or DD9800 System*

Si vous disposez du produit optionnel RSA Data Protection (DPM) Key Manager, consultez la version la plus récente du document intitulé *RSA Data Protection Manager Server Administrator's Guide*, disponible avec le produit RSA Key Manager.

Conventions utilisées dans ce document pour certains points particuliers
Data Domain utilise les conventions suivantes pour attirer l'attention du lecteur sur certains points particuliers :

NOTE

Un avis identifie un contenu mettant en garde contre une perte éventuelle de données ou d'activité.

Remarque

Une remarque identifie des informations accessoires relatives à la rubrique, mais qui ne revêtent pas un caractère essentiel. Les remarques peuvent fournir une explication, un commentaire, un renforcement d'un point dans le texte ou simplement une considération associée.

Conventions typographiques
Les conventions stylistiques suivantes sont utilisées dans ce document :

Tableau 1 Typographie

Gras	Indique les noms d'éléments d'interface, tels que les noms de fenêtres, de boîtes de dialogue, de boutons, de champs, d'onglets, de touches et de chemins de menus (tout ce qui nécessite une sélection ou un clic de l'utilisateur).
Italique	Met en évidence les titres des publications citées dans le texte.
`Monospace`	Fournit des informations sur le système, notamment :

Tableau 1 Typographie (suite)

	• code système ; • sortie du système, telle qu'un message d'erreur ou un script ; • noms de chemins d'accès, noms de fichiers, invites et syntaxe ; • commandes et options.
Monospace italique	Met en évidence un nom de variable qui doit être remplacé par une valeur de variable.
`Monospace gras`	Désigne le texte pour les entrées utilisateur
[ ]	Les crochets entourent les valeurs facultatives
|	Une barre verticale indique les sélections alternatives (la barre signifie « « ou » »).
{ }	Les accolades entourent le contenu que l'utilisateur doit spécifier, c'est-à-dire x, y ou z.
...	Les points de suspension indiquent des informations non essentielles omises dans l'exemple

Obtenir de l'aide

Pour plus d'informations sur le support, les produits et les licences Data Domain, procédez comme suit :

Informations sur les produits

Pour toute information sur la documentation, les notes de mise à jour, les mises à jour logicielles ou les produits Data Domain, consultez le support en ligne à l'adresse : https://support.emc.com.

Support technique

Ouvrez le support en ligne et cliquez sur Centre de service. Vous disposez de plusieurs possibilités pour contacter le support technique. Notez que pour pouvoir ouvrir une demande de service, vous devez disposer d'un contrat de support valide. Pour savoir comment obtenir un contrat de support valide ou si vous avez des questions concernant votre compte, contactez un responsable de compte.

Vos commentaires

Vos suggestions contribuent à améliorer la précision, l'organisation et la qualité d'ensemble des publications destinées à nos utilisateurs. Nous vous invitons à envoyer votre avis sur ce document à l'adresse suivante : DPAD.Doc.Feedback@emc.com.

CHAPITRE 1

Fonctions et intégration d'un système Data Domain

Ce chapitre traite des sujets suivants :

Historique des révisions

L'historique des révisions répertorie les principales modifications apportées au présent document afin de prendre en charge la version 6.2 de DD OS.

Tableau 2 Historique des révisions du document

Révision	Date	Description
01 (6.2.0)	Décembre 2018	Cette révision fournit des informations sur les nouvelles fonctionnalités suivantes : • Configuration des informations d'identification du serveur de messagerie dans le cadre de l'Assistant de configuration DD SM. • Extension de la capacité de DD300 de 8 To à 16 To. • Authentification LDAP sécurisée. • Outil de diagnostic de connexion Active Directory. • Enregistrement des fichiers coredump sur une clé USB. • Notification de modification SMB. • Accès hors ligne au domaine fiable. • Prise en charge de DD Cloud tier pour les fournisseurs Cloud Alibaba et Google Cloud Platform.

Tour d'horizon du système Data Domain

Les systèmes Data Domain sont des appliances de déduplication à la volée sur disque qui permettent la protection des données et la reprise après sinistre dans l'environnement de l'entreprise.

Tous les systèmes exécutent Data Domain Operating System (DD OS), qui fournit une interface de ligne de commande (CLI) permettant d'exécuter toutes les opérations système, ainsi que l'interface utilisateur (GUI) Data Domain System Manager (DD System Manager) pour la configuration, la gestion et la surveillance.

Remarque

DD System Manager était anciennement appelé Enterprise Manager.

Les systèmes se composent d'appliances dont la capacité de stockage et le débit de données varient. Les systèmes sont généralement configurés avec des châssis d'extension qui ajoutent de l'espace de stockage.

Fonctions d'un système Data Domain

Les fonctions d'un système Data Domain ont pour but de garantir l'intégrité des données, la fiabilité des restaurations, l'optimisation des ressources et la simplicité de

gestion. Les fonctions sous licence vous permettent d'adapter votre environnement système à vos besoins et à votre budget.

Intégrité des données

L'architecture DD OS Data Invulnerability Architecture™ protège contre la perte de données dues à des pannes matérielles et logicielles.

- Lors de l'écriture sur disque, DD OS crée et stocke les checksums et les métadonnées dans un format autodescriptif de toutes les données reçues. Après avoir écrit les données sur disque, DD OS recalcule et vérifie les checksums et les métadonnées.
- Une règle d'écriture pour ajout uniquement protège contre l'écrasement de données valides.
- Une fois la sauvegarde terminée, un processus de validation examine ce qui a été écrit sur le disque et vérifie que tous les segments de fichiers sont logiquement corrects dans le système de fichiers et que les données demeurent identiques avant et après l'écriture sur le disque.
- En arrière-plan, l'opération de vérification en ligne vérifie en permanence que les données sur les disques sont correctes et n'ont pas été modifiées depuis le processus de validation précédent.
- Dans la plupart des systèmes Data Domain, le stockage est configuré avec une parité double RAID 6 (deux disques de parité). En outre, la plupart des configurations incluent un élément remplaçable en fonctionnement dans chaque boîtier, à l'exception des systèmes de la gamme DD1xx qui utilisent huit disques. Chaque bande de parité utilise des checksums de bloc pour garantir que les données sont correctes. Les checksums sont utilisés en permanence lors de l'opération de vérification en ligne et lorsque les données sont lues à partir du système Data Domain. Avec la parité double, le système peut corriger les erreurs simultanément sur deux disques au maximum.
- Pour que les données demeurent synchronisées en cas de défaillance matérielle ou d'alimentation, le système Data Domain utilise la NVRAM (mémoire RAM non volatile) pour assurer le suivi des opérations d'E/S restantes. Une carte NVRAM dont les batteries sont entièrement chargées (état classique) peut conserver les données plusieurs heures en fonction du matériel utilisé.
- Lors de la relecture des données dans le cadre d'une opération de restauration, DD OS utilise plusieurs couches de contrôles de cohérence afin de vérifier que les données restaurées sont correctes.
- Lors de l'écriture dans le cache du disque SSD, DD OS exécute les opérations suivantes :
  - Il crée un checksum SL pour tous les enregistrements stockés dans le cache afin de détecter si les données du cache sont corrompues. Ce checksum est validé pour chaque lecture de cache.
  - Il traite la corruption des données du cache comme un échec d'accès au cache et n'entraîne aucune perte de données. Par conséquent, les clients de cache ne peuvent pas stocker la copie la plus récente des données sans un autre mécanisme de sauvegarde tel qu'un disque NVRAM ou un disque dur.
  - Il élimine la nécessité de vérifier à la volée les écritures du cache, car les clients de cache peuvent détecter et gérer les écritures perdues ou mal dirigées. Cela permet également d'économiser la bande passante d'E/S.

- Il élimine la nécessité de nettoyer le disque SSD du système de fichiers, car les données du cache changent fréquemment et sont déjà nettoyées par SAS Background Media Scan (BMS).

Déduplication des données

La déduplication des données DD OS identifie les données redondantes lors de chaque sauvegarde et ne conserve que les données uniques.

Le stockage des données uniques est invisible pour le logiciel de sauvegarde et indépendant du format de données. Les données peuvent être structurées (bases de données, par exemple) ou non structurées (fichiers texte, par exemple). Les données peuvent provenir de systèmes de fichiers ou de volumes bruts.

Les taux de déduplication classiques sont de 20 pour 1, en moyenne, sur plusieurs semaines. Ce taux suppose l'existence de sauvegardes complètes hebdomadaires et de sauvegardes incrémentielles quotidiennes. La déduplication est particulièrement bénéfique pour une sauvegarde qui comporte un grand nombre de fichiers dupliqués ou identiques (fichiers copiés plusieurs fois avec des modifications mineures).

Selon le volume, la taille, la période de rétention et le taux de changement de la sauvegarde, le niveau de déduplication peut varier. La meilleure déduplication a lieu avec des volumes de sauvegarde d'au moins 10 Mio (Mio étant l'équivalent en base 2 du Mo).

Pour tirer pleinement parti de plusieurs systèmes Data Domain, un site comportant plus d'un système Data Domain doit régulièrement sauvegarder le même système client ou ensemble de données sur le même système Data Domain. Par exemple, si une sauvegarde complète de toutes les données commerciales s'effectue vers le système Data Domain A, une déduplication maximale a lieu lorsque les sauvegardes incrémentielles et les sauvegardes complètes futures des données commerciales doivent également se faire vers le système Data Domain A.

Opérations de restauration

Les opérations de restauration de fichiers génèrent très peu, voire aucun conflit d'accès avec les opérations de sauvegarde ou les autres opérations de restauration.

Lors de la sauvegarde sur disque à l'aide du système Data Domain, les sauvegardes incrémentielles sont toujours fiables et facilement accessibles. Avec les sauvegardes sur bande, une opération de restauration peut s'appuyer sur plusieurs bandes détenant des sauvegardes incrémentielles. En outre, plus un site stocke des sauvegardes incrémentielles sur des bandes multiples, plus le processus de restauration prend du temps et présente des risques. Une bande défectueuse peut anéantir la restauration.

Un système Data Domain vous permet d'exécuter plus souvent des sauvegardes complètes sans être pénalisé par l'enregistrement de données redondantes. Contrairement aux sauvegardes de lecteur de bande, plusieurs processus peuvent accéder simultanément à un système Data Domain. Un système Data Domain permet à votre site d'offrir des opérations de restauration sûres et commandées par l'utilisateur d'un fichier unique.

Data Domain Replicator

Data Domain Replicator installe et gère la réplication des données de sauvegarde entre deux systèmes Data Domain.

Une paire de réplication DD implique un système source et un système de destination. Son rôle consiste à répliquer un Dataset ou un répertoire complet entre le système source et le système de destination. Un système Data Domain peut faire partie de

plusieurs paires de réplication et peut servir de source pour une ou plusieurs paires, ainsi que de destination pour une ou plusieurs paires. Une fois que la réplication a démarré, le système source envoie automatiquement les nouvelles données de sauvegarde au système de destination.

Multipathing et équilibrage de charge

Dans une configuration de multipathing Fibre Channel, plusieurs chemins sont établis entre un système Data Domain et un serveur de sauvegarde ou une baie de destination des sauvegardes. En présence de chemins d'accès multiples, le système procède automatiquement à l'équilibrage de charge des sauvegardes entre les différents chemins.

Deux ports HBA au moins sont nécessaires pour créer une configuration multipathing. Lors d'une connexion à un serveur de sauvegarde, chacun des ports HBA en mode multipathing est relié à un port indépendant sur le serveur en question.

Haute disponibilité

La fonction de haute disponibilité (HA) vous permet de configurer deux systèmes Data Domain en tant que paire active/passive, fournissant une redondance en cas de défaillance du système. La haute disponibilité synchronise les systèmes actifs et en veille, de sorte que si le nœud actif rencontre une défaillance en raison de problèmes matériels ou logiciels, le nœud en veille puisse prendre le relais des services et continuer là où le nœud défaillant s'est arrêté.

La fonction HA :

- prend en charge le basculement sur incident des services de sauvegarde, de restauration, de réplication et de gestion dans un système à deux nœuds. Le basculement automatique ne nécessite aucune intervention de l'utilisateur ;
- fournit une conception entièrement redondante sans aucun point unique de défaillance au sein du système lorsqu'elle est configurée comme recommandé ;
- fournit un système actif/passif sans perte de performances lors du basculement sur incident ;
- permet le basculement sur incident en 10 minutes pour la plupart des opérations. CIFS, DD VTL et NDMP doivent être redémarrés manuellement.

  Remarque

  La restauration des applications DD Boost peut durer plus de 10 minutes, car cette opération ne peut pas commencer tant que le basculement sur incident du serveur DD n'est pas terminé. En outre, la restauration des applications Boost ne peut pas démarrer tant que l'application n'aura pas appelé la bibliothèque DD Boost. De même, la restauration NFS peut durer plus longtemps.

- prend en charge la gestion et la configuration via les CLI DD OS ;
- fournit des alertes pour le matériel défaillant ;
- préserve les performances et l'évolutivité du nœud unique au sein d'une configuration HA en mode normal et dégradé ;
- prend en charge les mêmes fonctions que les systèmes DD autonomes ;

  Remarque

  DD Extended Retention et les disques virtuels ne sont pas pris en charge.

- prend en charge les systèmes avec tout type de disque SAS. Cela inclut les systèmes hérités mis à niveau vers des systèmes avec disques SAS.

  Remarque

  Les guides d'installation et de présentation du matériel dédiés aux systèmes Data Domain qui prennent en charge la haute disponibilité expliquent comment installer un nouveau système HA. Le guide *Data Domain Single Node to HA Upgrade* décrit la mise à niveau d'un système existant vers une paire HA.

- n'affecte pas la possibilité de faire évoluer le produit.
- prend en charge les mises à jour logicielles sans interruption.

La haute disponibilité est prise en charge sur les systèmes Data Domain suivants :

- DD6800
- DD9300
- DD9500
- DD9800

Architecture HA

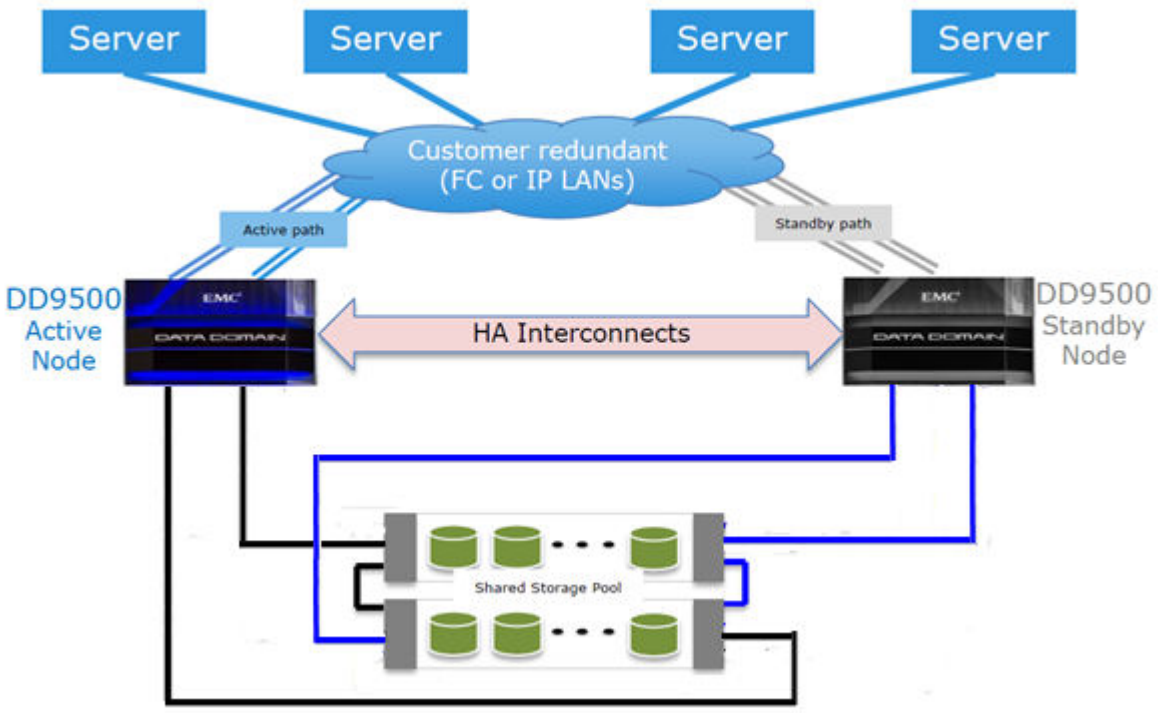
La fonctionnalité HA est disponible pour les connexions IP et Fibre Channel. Les deux nœuds doivent avoir accès aux mêmes réseaux IP, SAN Fibre Channel et hôtes afin de garantir la haute disponibilité pour l'environnement.

Sur les réseaux IP, HA utilise une adresse IP flottante afin de fournir un accès aux données à la paire HA Data Domain, quel que soit le nœud physique actif.

Pour les SAN Fibre Channel, HA utilise la virtualisation NPIV pour déplacer les noms universels Fibre Channel entre les nœuds, ce qui permet aux initiateurs Fibre Channel de rétablir les connexions après un basculement sur incident.

La Figure 1 à la page 27 illustre l'architecture HA.

Figure 1 Architecture HA



Prise en charge des E/S aléatoires

Les optimisations d'E/S aléatoires incluses dans DD OS offrent de meilleures performances pour les applications et les exemples d'utilisation qui génèrent de plus grandes quantités d'opérations de lecture et d'écriture aléatoires que d'opérations séquentielles d'écriture et de lecture.

DD OS est optimisé pour traiter les charges applicatives composées d'opérations de lecture et d'écriture aléatoires, telles que l'accès instantané à la machine virtuelle et sa restauration instantanée, et les sauvegardes incrémentielles systématiques générées par des applications telles qu'Avamar. Ces optimisations :

- améliorent la latence des lectures et des écritures aléatoires ;
- améliorent les E/S par seconde de l'utilisateur avec des tailles de lecture plus petites ;
- prennent en charge les opérations d'E/S simultanées au sein d'un simple flux ;
- fournissent un débit de lecture et d'écriture maximal avec des flux plus petits.

Remarque

Le nombre maximal de flux d'E/S aléatoires est limité au nombre maximal de flux de restauration d'un système Data Domain.

Les améliorations apportées aux E/S aléatoires permettent au système Data Domain de prendre en charge les fonctions d'accès instantané/restauration instantanée des applications de sauvegarde telles que NetWorker et Avamar.

Accès au système par l'administrateur système

Les administrateurs système peuvent accéder au système à des fins de configuration et de gestion au moyen d'une interface de ligne de commande (CLI) ou d'une interface utilisateur (GUI).

- L'interface de ligne de commande DD OS est accessible par l'intermédiaire d'une console série ou de connexions Ethernet utilisant SSH ou Telnet. Les commandes de la CLI servent à effectuer la configuration initiale du système et à apporter des modifications aux paramètres individuels du système. Elles affichent également l'état du système.
- DD System Manager : interface utilisateur graphique basée sur navigateur et disponible par le biais de connexions Ethernet. Utilisez DD System Manager pour procéder à la configuration initiale du système, apporter des modifications à la configuration après la configuration initiale, afficher l'état du système et des composants, ainsi que pour générer des rapports et des graphiques.

Remarque

Certains systèmes prennent en charge l'accès à l'aide d'un clavier et d'un moniteur reliés directement au système.

Fonctions sous licence

L'intérêt des licences est d'acheter uniquement les fonctions que vous avez l'intention d'utiliser. Par exemple, les fonctions DD Extended Retention et DD Boost ou l'augmentation de la capacité de stockage nécessitent des licences.

Consultez votre responsable de compte pour en savoir plus sur l'acquisition des fonctions sous licence.

Tableau 3 Fonctions nécessitant des licences

Nom de fonction	Nom de la licence dans le logiciel	Description
Data Domain ArchiveStore	ARCHIVESTORE	Fournit aux systèmes Data Domain les licences destinées à l'archivage, par exemple à l'archivage de fichiers et d'e-mails, à la hiérarchisation des fichiers et à l'archivage des contenus et bases de données.
Data Domain Boost	DDBOOST	Permet d'utiliser un système Data Domain avec les applications suivantes : Avamar, NetWorker, Oracle RMAN,Quest vRanger Symantec Veritas NetBackup (NBU) et Backup Exec. La fonction de réplication de fichiers gérés (MFR) de DD Boost nécessite également la licence DD Replicator.
Data Domain Capacity on Demand	CONTROLLER-COD	Permet d'accroître la capacité à la demande (et d'atteindre 7,5 To or 13,18 To) sur les systèmes DD2200 à 4 To. Pour porter la capacité à 13,18 To, vous avez besoin, en outre, de la licence EXPANDED-STORAGE.

Tableau 3 Fonctions nécessitant des licences (suite)

Nom de fonction	Nom de la licence dans le logiciel	Description
Data Domain Cloud Tier	CLOUDTIER-CAPACITY	Permet à un système Data Domain de déplacer des données à partir du niveau actif vers un stockage en mode objet haute capacité et économique dans le Cloud public, privé ou hybride à des fins de rétention à long terme.
Data Domain Encryption	ENCRYPTION	Permet de chiffrer les données lors de leur enregistrement et de leur verrouillage sur les disques système ou le stockage externe, lors du déplacement du système à un autre emplacement.
Data Domain Expansion Storage	EXPANDED-STORAGE	Permet d'augmenter la capacité de stockage d'un système Data Domain au-delà du niveau standard.
Data Domain Extended Retention (anciennement DD Archiver)	EXTENDED-RETENTION	Fournit la licence de la fonction de stockage DD Extended Retention.
Data Domain I/OS (pour les environnements d'exploitation IBM i)	I/OS	Une licence I/OS est nécessaire lorsque DD VTL est utilisé pour sauvegarder des systèmes dans l'environnement d'exploitation IBM i. Appliquez cette licence avant d'ajouter des lecteurs de bande virtuels aux bibliothèques.
Data Domain Replicator	REPLICATION	Ajoute DD Replicator en vue de la réplication des données entre deux systèmes Data Domain. Aucune licence n'est requise sur l'un ou l'autre système.
Data Domain Retention Lock Compliance Edition	RETENTION-LOCK-COMPLIANCE	Répond aux exigences les plus strictes en matière de rétention des données imposées par les normes réglementaires telles que SEC17a-4.
Édition Data Domain Retention Lock Governance	RETENTION-LOCK-GOVERNANCE	Protège les fichiers sélectionnés contre toute modification ou suppression avant la fin d'une période de rétention spécifiée.
Data Domain Shelf Capacity-Active Tier	CAPACITY-ACTIVE	Permet de compléter la capacité de stockage du niveau actif d'un système Data Domain par un châssis supplémentaire ou une pile de disques au sein d'un châssis.
Data Domain Shelf Capacity-Archive Tier	CAPACITY-ARCHIVE	Permet de compléter la capacité de stockage du niveau d'archivage d'un système Data Domain par un châssis supplémentaire ou une pile de disques au sein d'un châssis.
Data Domain Storage Migration	STORAGE-MIGRATION-FOR-DATADOMAIN-SYSTEMS	Permet la migration des données entre deux châssis pour prendre en charge le remplacement de châssis plus anciens, moins gourmands en capacité.

Tableau 3 Fonctions nécessitant des licences (suite)

Nom de fonction	Nom de la licence dans le logiciel	Description
Data Domain Virtual Tape Library (DD VTL)	VTL	Permet d'utiliser un système Data Domain en tant que librairie de bandes virtuelle sur un réseau Fibre Channel. Cette licence a pour effet également d'activer la fonction de serveur de bandes NDMP, qui exigeait auparavant une licence à part.
Haute disponibilité	HA-ACTIVE-PASSIVE	Active la fonction de haute disponibilité dans une configuration active/passive. Vous devez uniquement acheter une licence HA. Celle-ci s'exécute sur le nœud actif et est mise en miroir sur le nœud en veille.

Intégration de l'environnement de stockage

Les systèmes Data Domain s'intègrent facilement avec les datacenters existants.

- Tous les systèmes Data Domain peuvent être configurés en tant que destinations de stockage pour les principales applications de sauvegarde et d'archivage utilisant les protocoles NFS, CIFS, DD Boost ou DD VTL.
- Recherchez les *documents sur la compatibilité* sur le site https://support.emc.com pour obtenir des informations sur les applications qui utilisent les différentes configurations.
- Plusieurs serveurs de sauvegarde peuvent partager un système Data Domain.
- Un système Data Domain peut traiter plusieurs opérations de sauvegarde et de restauration simultanées.
- Plusieurs systèmes Data Domain peuvent être connectés à un ou plusieurs serveurs de sauvegarde.

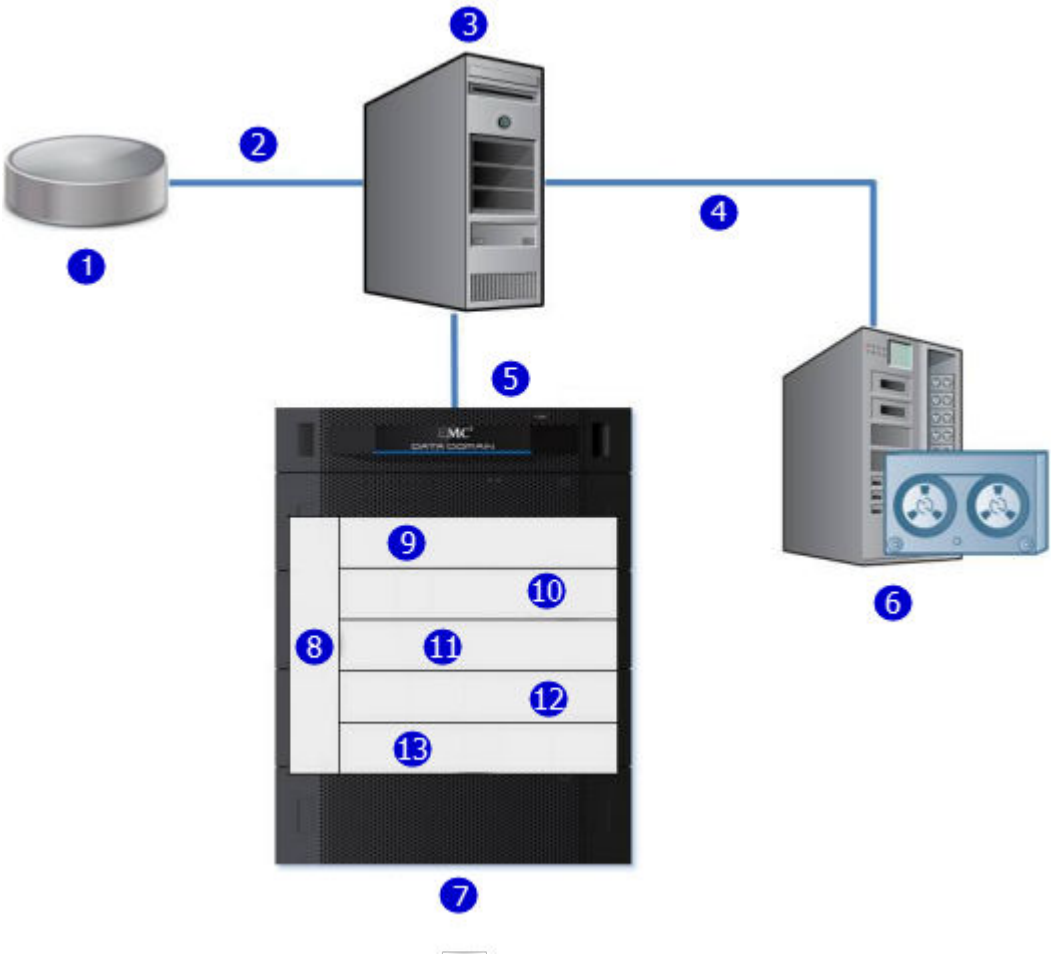
Lorsqu'il doit être utilisé comme destination de sauvegarde, un système Data Domain peut être configuré en tant qu'unité de stockage sur disque avec un système de fichiers accessible au moyen d'une connexion Ethernet ou en tant que librairie de bandes virtuelle accessible via une connexion Fibre Channel. La fonction DD VTL permet aux systèmes Data Domain d'être intégrés dans des environnements dans lesquels le logiciel de sauvegarde est déjà configuré pour les sauvegardes sur bande, ce qui limite les interruptions.

La configuration s'effectue dans DD OS (comme le décrivent les sections appropriées de ce guide) et dans l'application de sauvegarde (comme cela est décrit dans les guides d'administration de l'application de sauvegarde et les guides et notes techniques relatifs à l'application Data Domain).

Toutes les applications de sauvegarde peuvent accéder à un système Data Domain en tant que système de fichiers NFS ou CIFS sur le périphérique du disque Data Domain.

La figure suivante illustre un système Data Domain intégré avec une configuration de sauvegarde de base déjà existante.

Figure 2 Système Data Domain intégré avec un environnement de stockage



1. Stockage primaire
2. Ethernet
3. Serveur de sauvegarde
4. SCSI/Fibre Channel
5. Gigabit Ethernet ou Fibre Channel
6. Système de bandes
7. Système Data Domain
8. Gestion
9. NFS/CIFS/DD VTL/DD Boost
10. Vérification des données
11. Système de fichiers
12. Déduplication et compression globales
13. RAID

Comme l'illustre la Figure 2 à la page 31, les données sont transférées vers un système Data Domain par le biais d'une connexion Ethernet ou Fibre Channel. Les processus de vérification des données commencent immédiatement et se poursuivent pendant que les données résident sur le système Data Domain. Dans le système de fichiers, l'algorithme DD OS Global Compression™ déduplique et compresse les données en vue du stockage. Les données sont ensuite envoyées au sous-système de disques RAID. Lorsqu'une opération de restauration est requise, les données sont récupérées à partir

du système de stockage Data Domain et décompressées. Leur cohérence est vérifiée et elles sont alors transférées via Ethernet vers les serveurs de sauvegarde à l'aide d'Ethernet (pour NFS, CIFS, DD Boost) ou de Fibre Channel (pour DD VTL et DD Boost).

DD OS prend en charge des flux relativement importants de données séquentielles provenant du logiciel de sauvegarde. Il est optimisé pour assurer un débit élevé, une vérification continue des données et un taux de compression élevé. Il prend également en charge un grand nombre de fichiers plus petits dans le stockage nearline (DD ArchiveStore).

Les performances d'un système Data Domain sont optimales lorsque des données provenant d'applications qui ne sont pas spécifiquement des logiciels de sauvegarde sont stockées dans les conditions suivantes.

- Les données sont envoyées au système Data Domain en tant qu'écritures séquentielles (pas de remplacement).
- Les données ne sont ni compressées ni chiffrées avant d'être envoyées au système Data Domain.

CHAPITRE 2

Mise en route

Ce chapitre traite des sujets suivants :

Tour d'horizon de Dell EMC Data Domain System Manager

DD System Manager est une interface utilisateur de type navigateur, disponible par le biais de connexions Ethernet, permettant de gérer un seul système depuis n'importe où. DD System Manager offre une interface de gestion consolidée et unique qui permet de configurer et de surveiller de nombreux paramètres et fonctions du système.

Remarque

Data Domain Management Center vous permet de gérer plusieurs systèmes à partir d'une seule fenêtre de navigateur.

DD System Manager fournit des graphiques et des tableaux en temps réel qui vous permettent de surveiller l'état des composants matériels du système et des fonctions configurées.

En outre, un ensemble de commandes qui exécute toutes les fonctions du système est à la disposition des utilisateurs dans l'interface de ligne de commande (CLI). Les commandes configurent les paramètres système et permettent d'afficher l'état du matériel du système, son fonctionnement et la configuration des fonctions.

L'interface de ligne de commande est accessible par l'intermédiaire d'une console série ou d'une connexion Ethernet utilisant SSH ou Telnet.

Remarque

Certains systèmes prennent en charge l'accès à l'aide d'un clavier et d'un moniteur reliés directement au système.

Versions du logiciel DD OS

Les versions logicielles de DD OS ont trois statuts publics, indiquant le nombre de systèmes installés qui exécutent la version.

- Les versions de **Disponibilité générale** ont été testées par Data Domain Internal QA Testing et sont disponibles pour l'installation dans les environnements de production.
- Les versions de **Disponibilité dirigée - Contrôlée (Disponibilité dirigée)** sont des versions à accès soigneusement contrôlé, destinées à un petit nombre d'installations. Les clients peuvent demander à être qualifiés pour accéder à ces versions.
- **Code cible** : il est recommandé que tous les systèmes effectuent une mise à niveau vers le code cible du système d'exploitation Data Domain OS au sein d'une génération de versions dès que possible.

  Remarque

  Il n'existe qu'une seule version de code cible dans une génération spécifique Les versions de code cible ont respecté les heures d'installation et d'exécution ainsi que les metrics de qualité pour indiquer qu'elles sont stables et qu'elles n'ont aucun problème susceptible d'affecter la plupart des clients. Pour certaines générations, il se peut qu'il n'existe aucun de code cible identifié, en raison de l'adoption limitée par les clients, de problèmes de qualité ou d'autres considérations.

La mise à niveau entre les familles peut entraîner des problèmes de compatibilité de produit, et un examen minutieux de la compatibilité du produit doit précéder toute mise à niveau vers une nouvelle génération de versions.

Connexion à DD System Manager et déconnexion

Servez-vous d'un navigateur pour vous connecter à DD System Manager.

Lorsque vous vous connectez à DD System Manager à partir d'un navigateur Web, toutes les connexions HTTP redirigent automatiquement vers HTTPS.

Procédure

1. Ouvrez un navigateur Web et saisissez l'adresse IP ou le nom d'hôte pour vous connecter à DD System Manager. Il doit s'agir :
   - Un nom de domaine complet (par exemple, `http://dd01.emc.com`)
   - Un nom d'hôte (`http://dd01`)
   - Une adresse IP (`http://10.5.50.5`)

   Remarque

   DD System Manager utilise le port HTTP 80 et le port HTTPS 443. Lorsque votre système Data Domain se trouve derrière un pare-feu, vous devrez peut-être activer le port 80 si vous utilisez le protocole HTTP ou le port 443 si vous utilisez le protocole HTTPS pour atteindre le système. Les numéros de port peuvent être facilement modifiés si la sécurité l'exige.

Remarque

Si Data Domain System Manager ne peut pas être lancé à partir d'un navigateur Web, le message d'erreur affiché est « The GUI Service is temporarily unavailable. Please refresh your browser. If the problem persists, please contact Data Domain support for assistance. » SSH peut être utilisé pour se connecter au système Data Domain et peut exécuter toutes les commandes.
Si vous n'avez pas mis à jour le système d'exploitation DD, mais que vous rencontrez toujours cette erreur d'interface graphique, utilisez la procédure suivante :

a. Fermez la session du navigateur Web sur le système Data Domain avec l'erreur signalée.

b. Exécutez ces commandes dans l'ordre :

- `adminaccess disable http`
- `adminaccess disable https`
- `adminaccess enable http`
- `adminaccess enable https`

c. Attendez 5 minutes pour permettre aux services http et https de démarrer complètement.

d. Ouvrez un navigateur Web et connectez-vous à Data Domain System Manager.

Si vous voyez ce problème d'interface graphique après une mise à niveau de DD OS, suivez la procédure suivante :

a. Fermez la session du navigateur Web sur le système Data Domain avec l'erreur signalée.

b. Exécutez ces commandes dans l'ordre :

- `adminaccess disable http`
- `adminaccess disable https`
- `adminaccess certificate generate self-signed-cert`
- `adminaccess enable http`
- `adminaccess enable https`

a. Attendez 5 minutes pour permettre aux services http et https de démarrer complètement.

b. Ouvrez un navigateur Web et connectez-vous à Data Domain System Manager.

2. Pour une connexion HTTPS sécurisée, cliquez sur **Secure Login**.

   La connexion sécurisée avec HTTPS requiert un certificat numérique pour valider l'identité du système DD OS et prendre en charge le chiffrement bidirectionnel entre DD System Manager et un navigateur Web. DD OS inclut un certificat auto-signé et vous permet d'importer votre propre certificat.

3. Saisissez le nom d'utilisateur et le mot de passe qui vous ont été attribués.

Remarque

Le nom d'utilisateur initial est *sysadmin* et le mot de passe initial est le numéro de série du système. Pour savoir comment configurer un nouveau système, consultez le *Guide de configuration initiale de Data Domain Operating System*.

4. Cliquez sur **Log In**.

   S'il s'agit de votre première connexion, la vue Home s'affiche dans le volet d'information.

Remarque

Si vous saisissez un mot de passe incorrect à 4 reprises, le système verrouillera le nom d'utilisateur spécifié pendant 120 secondes. Le nombre de connexions et la durée du verrouillage sont configurables et peuvent différer sur votre système.

Remarque

S'il s'agit de votre première connexion, vous devrez probablement changer votre mot de passe. Si l'administrateur système a configuré votre nom d'utilisateur pour exiger un changement de mot de passe, vous devrez modifier le mot de passe avant d'accéder à DD System Manager.

5. Pour vous déconnecter, cliquez sur le bouton de déconnexion dans la bannière de DD System Manager.

   Lorsque vous vous déconnectez, le système affiche la page de connexion avec un message indiquant que votre déconnexion est terminée.

Connexion à l'aide d'un certificat

En alternative à la connexion à l'aide d'un nom d'utilisateur et d'un mot de passe, vous pouvez vous connecter à DD System Manager avec un certificat délivré par une autorité de certification.

Pour vous connecter à l'aide d'un certificat, vous devez disposer de privilèges d'autorisation sur le système Data Domain, et ce dernier doit approuver l'autorité de certification. Votre nom d'utilisateur doit être spécifié dans le champ de nom commun du certificat.

Procédure

1. Vous devez avoir un compte utilisateur sur le système Data Domain.

   Vous pouvez être un utilisateur local ou un utilisateur de services de noms (NIS/AD). Pour un utilisateur de services de noms, votre mappage groupe-rôle doit être configuré sur le système Data Domain.

2. Utilisez la commande CLI suivante pour importer la clé publique de l'autorité de certification ayant émis le certificat : `adminaccess certificate import ca application login-auth`.

3. Chargez le certificat au format PKCS12 dans votre navigateur.

   Une fois que l'autorité de certification est approuvée par le système Data Domain, un lien **Log in with certificate** s'affiche sur l'écran de connexion HTTPS.

4. Cliquez sur **Log in with certificate** et choisissez le certificat dans la liste des certificats, lorsque vous y êtes invité par le navigateur.

Résultats

Le système Data Domain valide le certificat utilisateur dans la zone de stockage fiable. Une session System Manager est alors créée pour vous en fonction des privilèges d'autorisation associés à votre compte.

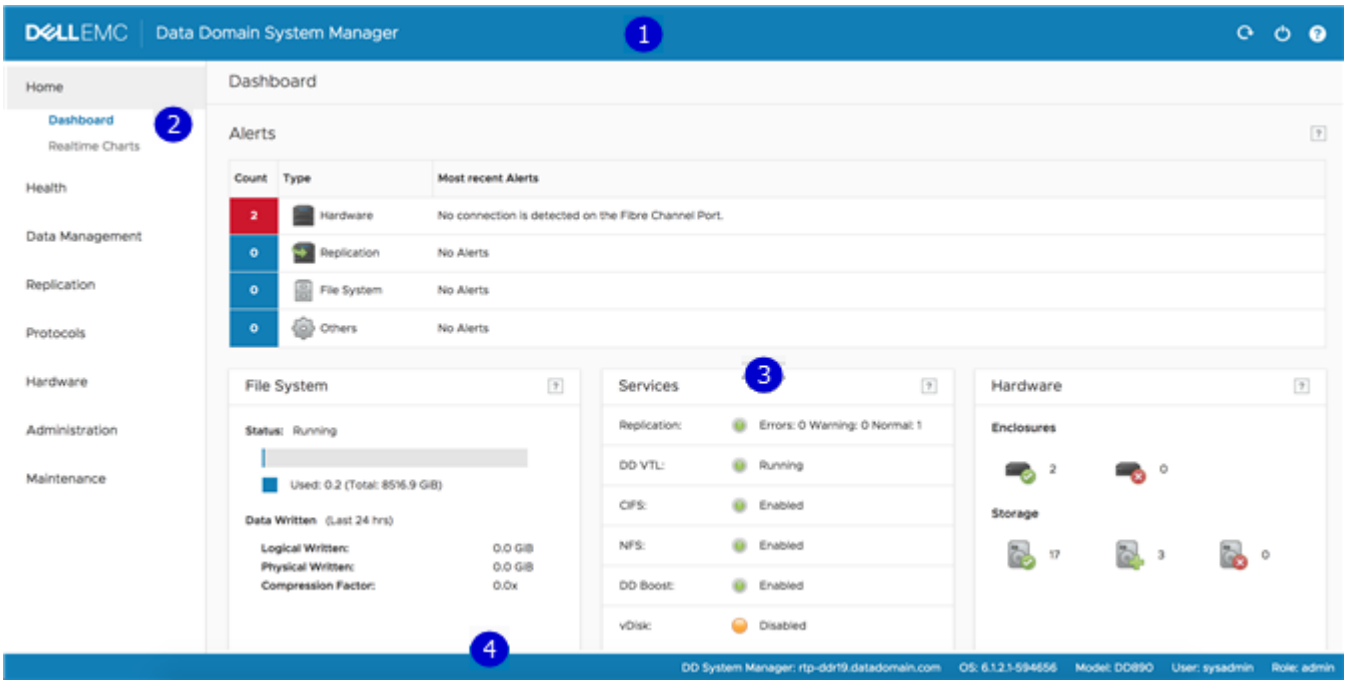
Interface de DD System Manager

L'interface de DD System Manager présente des éléments communs sur la plupart des pages de façon à ce que vous puissiez naviguer rapidement dans la configuration et afficher une aide contextuelle.

Éléments composant la page

La bannière, le volet de navigation, les volets d'information et le pied de page sont les principaux éléments composant la page.

Figure 3 Éléments composant la page de DD System Manager



1. Bannière
2. Volet de navigation
3. Volets d'information
4. Pied de page

Bannière

La bannière de DD System Manager affiche le nom du programme et les boutons **Refresh**, **Log Out** et **Help**.

Volet de navigation

Le volet de navigation affiche les sélections du menu de niveau le plus élevé que vous pouvez utiliser pour identifier le composant système ou la tâche que vous souhaitez gérer.

Le volet de navigation affiche les deux principaux niveaux du système de navigation. Cliquez sur n'importe quel titre de niveau supérieur pour afficher les titres du second niveau. Les onglets et les menus du volet d'information fournissent des contrôles de navigation supplémentaires.

Volet d'information

Le volet d'information contient des renseignements et des contrôles sur l'élément sélectionné dans le volet de navigation. C'est à cet endroit que vous trouvez des données sur l'état du système et que vous configurez un système.

En fonction de la fonction ou de la tâche sélectionnée dans le volet de navigation, le volet d'information peut afficher une barre d'onglets, des rubriques, des contrôles de vue de tableau et le menu More Tasks.

Barre d'onglets
Les onglets permettent d'accéder à différents aspects de la rubrique sélectionnée dans le volet de navigation.

Rubriques
Les rubriques divisent le volet d'information en sections représentant différents aspects de la rubrique sélectionnée dans le volet ou l'onglet parent de navigation.

Pour les systèmes haute disponibilité (HA), l'onglet HA Readiness sur le tableau de bord de System Manager indique si le système haute disponibilité est prêt à basculer du nœud actif vers le nœud en veille. Vous pouvez cliquer sur **HA Readiness** pour accéder à la section **High Availability** sous **HEALTH**.

Utilisation des options d'affichage du tableau
Plusieurs affichages avec des tables d'éléments contiennent des contrôles pour filtrer et trier les informations du tableau et pour y accéder.

Utilisation des contrôles communs du tableau :

- Cliquez sur l'icône en forme de losange dans un en-tête de colonne pour inverser l'ordre de tri des éléments de cette colonne.
- Cliquez sur les flèches **<** et **>** dans le coin inférieur droit de la vue pour avancer ou reculer parmi les pages. Pour accéder directement au début d'une séquence de pages, cliquez sur **|<**. Pour accéder directement à la fin, cliquez sur **>|**.
- Utilisez la barre de défilement pour afficher tous les éléments d'un tableau.
- Saisissez le texte dans la zone **Filter By** pour rechercher ou pour hiérarchiser la liste de ces éléments.
- Cliquez sur **Update** pour rafraîchir la liste.
- Cliquez sur **Reset** pour revenir à la liste par défaut.

Menu More Tasks
Certaines pages comportent un menu More Tasks situé en haut à droite de la vue et qui contient les commandes associées à la vue en cours.

Pied de page

Le pied de page de DD System Manager affiche des informations importantes sur la session de gestion.

La bannière répertorie les informations suivantes.

- Nom d'hôte du système.
- Version du système DD OS
- Numéro de modèle du système sélectionné.
- Nom d'utilisateur et rôle de l'utilisateur actuellement connecté.

Boutons d'aide

Les boutons d'aide, symbolisés par ?, sont visibles dans la bannière, dans le titre de nombreuses zones du volet d'information ainsi que dans diverses boîtes de dialogue. Il suffit de cliquer sur ces boutons pour ouvrir une fenêtre d'aide en rapport avec la fonction utilisée.

La fenêtre d'aide propose un bouton de contenu et un bouton de navigation au-dessus du texte d'aide. Cliquez sur le bouton de contenu pour afficher le contenu du guide et sur un bouton de recherche pour effectuer une recherche dans l'aide. Utilisez les flèches directionnelles pour parcourir les pages de la rubrique d'aide dans un ordre séquentiel.

Contrat de licence utilisateur final

Pour afficher les conditions générales d'utilisation (CGU), sélectionnez **Maintenance** > **System** > **View EULA**.

Configuration d'un système à l'aide de l'assistant de configuration

Il existe deux assistants, à savoir l'assistant de configuration de DD System Manager et un assistant de configuration d'interface de ligne de commande (CLI). Les assistants de configuration vous guident pas à pas pour que votre système soit rapidement opérationnel.

À l'issue de la configuration de base à l'aide d'un assistant, vous pouvez utiliser des contrôles de configuration supplémentaires de DD System Manager et de l'interface de ligne de commande pour configurer votre système plus en détail.

Remarque

La procédure suivante décrit la procédure de démarrage et d'exécution de l'assistant de configuration de DD System Manager après la configuration initiale de votre système. Pour obtenir des instructions sur l'exécution des assistants de configuration au démarrage du système, consultez le *Guide de configuration initiale de Data Domain Operating System*.

Remarque

Si vous souhaitez configurer votre système pour la haute disponibilité (HA), vous devez effectuer cette opération à l'aide de l'Assistant de configuration de la CLI. Pour plus d'informations, reportez-vous au *Guide d'installation et de présentation du matériel des systèmes Data Domain DD9500/DD9800* et au *Guide de configuration initiale de Data Domain Operating System*.

Procédure

1. Sélectionnez **Maintenance** > **System** > **Configure System**.
2. Utilisez les contrôles situés en bas de la boîte de dialogue Configuration Wizard pour sélectionner les fonctions que vous souhaitez configurer et pour naviguer dans l'assistant. Pour afficher l'aide relative à une fonction, cliquez sur l'icône d'aide (point d'interrogation) dans le coin inférieur gauche de la boîte de dialogue.

Page des licences

La page License affiche toutes les licences installées. Cliquez sur **Yes** pour ajouter, modifier ou supprimer une licence ou sur **No** pour ignorer l'installation de la licence.

Configuration des licences

La section **Licenses Configuration** vous permet d'ajouter, de modifier ou de supprimer des licences à partir d'un fichier de licence. Data Domain Operating System 6.0 et ultérieur prend en charge l'octroi de licence ELMS qui vous permet d'inclure plusieurs fonctions via le téléchargement d'un seul fichier.

Lorsque vous utilisez l'Assistant de configuration sur un système sans aucune licence configurée, sélectionnez le type de licence dans le menu déroulant, puis cliquez sur le bouton **...**. Accédez au répertoire où réside le fichier de licence et sélectionnez-le pour le télécharger sur le système.

Tableau 4 Valeurs de page License Configuration

Élément	Description
Add Licenses	Sélectionnez cette option pour ajouter des licences à partir d'un fichier de licence.
Replace Licenses	Si les licences sont déjà configurées, l'option **Add Licenses** devient **Replace Licenses**. Sélectionnez cette option pour remplacer les licences déjà ajoutées.
Delete Licenses	Sélectionnez cette option pour supprimer des licences déjà configurées sur le système.

Réseau

La section **Network** vous permet de configurer les paramètres réseau. Cliquez sur **Yes** pour configurer les paramètres réseau ou cliquez sur **No** pour ignorer la configuration réseau.

Page des paramètres réseau généraux

La page General permet de configurer les paramètres réseau qui définissent la manière dont le système fait partie d'un réseau IP.

Pour configurer ces paramètres réseau en dehors de l'assistant de configuration, sélectionnez **Hardware** > **Ethernet**.

Tableau 5 Paramètres de la page General

Élément	Description
Obtain Settings using DHCP	Sélectionnez cette option pour indiquer que le système se procure les paramètres réseau auprès d'un serveur DHCP (Dynamic Host Control Protocol). Lors de la configuration des interfaces réseau, au moins l'une des interfaces doit être configurée pour utiliser le DHCP.
Manually Configure	Sélectionnez cette option pour utiliser les paramètres réseau définis dans la zone Settings de cette page.
Host Name	Spécifie le nom d'hôte du réseau de ce système. **Remarque** Si vous choisissez d'obtenir les paramètres réseau via le protocole DHCP, vous pouvez configurer manuellement le nom d'hôte via **Hardware** > **Ethernet** > **Settings** ou à l'aide de la commande `net set hostname`. Vous devez configurer manuellement le nom d'hôte lors de l'utilisation de DHCP via IPv6.
Domain Name	Indique le domaine auquel ce système appartient.
Default IPv4 Gateway	Indique l'adresse IPv4 de la passerelle vers laquelle le système transfère les demandes réseau lorsqu'aucune route n'est entrée pour le système cible.
Default IPv6 Gateway	Indique l'adresse IPv6 de la passerelle vers laquelle le système transfère les demandes réseau lorsqu'aucune route n'est entrée pour le système cible.

Page des interfaces réseau

La page Interfaces permet de configurer les paramètres réseau qui définissent la manière dont chaque interface participe à un réseau IP.

Pour configurer ces paramètres réseau en dehors de l'assistant de configuration, sélectionnez **Hardware** > **Ethernet** > **Interfaces**.

Tableau 6 Paramètres de la page Interfaces

Élément	Description
Interface	Répertorie les interfaces disponibles sur votre système.
Enabled	Indique si chaque interface est activée (case cochée) ou désactivée (case décochée). Cochez ou décochez la case pour faire passer l'interface d'un état à l'autre.

Tableau 6 Paramètres de la page Interfaces (suite)

Élément	Description
DHCP	Affiche la configuration DHCP actuelle de chaque interface. Sélectionnez **v4** pour les connexions DHCP IPv4, **ipv6** pour les connexions IPv6 ou **no** pour désactiver le protocole DHCP.
IP Address	Indique une adresse IPv4 ou IPv6 pour ce système. Pour configurer l'adresse IP, vous devez définir le paramètre DHCP sur **No**. **Remarque** Les systèmes DD140, DD160, DD610, DD620 et DD630 ne prennent pas en charge IPv6 sur l'interface eth0a (eth0 sur les systèmes qui utilisent des noms de port hérités) ou sur aucun des réseaux VLAN créés sur cette interface.
Netmask	Spécifie le masque de réseau de ce système. Pour configurer le masque de réseau, vous devez définir le DHCP sur **No**.
Link	Indique si la liaison Ethernet est active (Yes) ou non (No).

Page des paramètres réseau DNS

La page DNS vous permet de configurer la façon dont le système obtient des adresses IP pour les serveurs DNS auprès d'un DNS (Domain Name System).

Pour configurer ces paramètres réseau en dehors de l'assistant de configuration, sélectionnez **Hardware** > **Ethernet** > **Settings**.

Tableau 7 Paramètres de la page DNS

Élément	Description
Obtain DNS using DHCP.	Sélectionnez cette option pour indiquer que le système obtient les adresses IP des serveurs DNS auprès d'un serveur DHCP. Lors de la configuration des interfaces réseau, au moins l'une des interfaces doit être configurée pour utiliser le DHCP.
Manually configure DNS list.	Sélectionnez cette option si vous souhaitez saisir manuellement les adresses IP du serveur DNS.
Bouton d'ajout (+)	Cliquez sur ce bouton pour afficher une boîte de dialogue dans laquelle vous pouvez ajouter une adresse IP de serveur DNS à la liste DNS IP Address. Vous devez sélectionner **Manually configure DNS list** avant d'ajouter ou de supprimer des adresses IP de serveur DNS.
Bouton de suppression (X)	Cliquez sur ce bouton pour supprimer une adresse IP du serveur DNS dans la liste DNS IP Address. Vous devez sélectionner l'adresse IP à supprimer avant d'activer ce bouton. Vous devez également sélectionner **Manually configure DNS list** avant d'ajouter ou de supprimer des adresses IP de serveur DNS.

Tableau 7 Paramètres de la page DNS (suite)

Élément	Description
Cases à cocher en regard des adresses IP	Cochez la case située en regard de l'adresse IP de serveur DNS que vous voulez supprimer. Cochez la case en regard de DNS IP Address si vous voulez supprimer toutes les adresses IP. Vous devez sélectionner **Manually configure DNS list** avant d'ajouter ou de supprimer des adresses IP de serveur DNS.

Système de fichiers

La section **File System** vous permet de configurer le stockage du niveau actif et du niveau cloud. À chaque niveau correspond la page d'un Assistant distinct. Vous pouvez également créer le système de fichiers dans cette section. Les pages de configuration ne sont pas accessibles si le système de fichiers a déjà été créé.

Chaque fois que vous affichez la section **File System** lorsque le système de fichiers n'a pas été créé, le système affiche un message d'erreur. Poursuivez la procédure pour créer le système de fichiers.

Configurer les pages de niveau de stockage

Les pages de configuration du niveau de stockage permettent de configurer le stockage pour chaque niveau sous licence sur le système, Active Tier, Archive Tier et DD Cloud Tier. À chaque niveau correspond une page d'assistant distincte. Les pages de configuration du niveau de stockage ne sont pas accessibles si le système de fichiers a déjà été créé.

Configure Active Tier
La section Configure Active Tier vous permet de configurer les périphériques du niveau de stockage actif. Le niveau actif est l'emplacement de sauvegarde des données. Pour ajouter du stockage au niveau actif, sélectionnez un ou plusieurs périphériques et ajoutez-les au niveau. Vous pouvez ajouter des périphériques de stockage dans la limite de la capacité autorisée par les licences installées.

Le système DD3300 exige des périphériques de 4 To pour le niveau actif.

Tableau 8 Addable Storage

Élément	Description
ID (périphérique dans DD VE)	Identifiant du disque, qui peut être un des éléments suivants. • Le numéro de boîtier et de disque (au format Enclosure Slot ou Enclosure Pack pour les tiroirs DS60) • Le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk • Une LUN
Disks	Disques qui composent la pile de disques ou la LUN. Cela ne s'applique pas aux instances DD VE.
Model	Type de tiroir de disques. Cela ne s'applique pas aux instances DD VE.

Tableau 8 Addable Storage (suite)

Élément	Description
Disk Count	Nombre de disques dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Disk Size (taille dans DD VE)	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
License Needed	Capacité sous licence requise pour ajouter le stockage au niveau.
Failed Disks	Disques défaillants dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Type	SCSI. Cela s'applique uniquement aux instances DD VE.

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Tableau 9 Valeurs Active Tier

Élément	Description
ID (périphérique dans DD VE)	Identifiant du disque, qui peut être un des éléments suivants. • Le numéro de boîtier et de disque (au format Enclosure Slot ou Enclosure Pack pour les tiroirs DS60). Cela ne s'applique pas aux instances DD VE. • Le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk • Une LUN
Disks	Disques qui composent la pile de disques ou la LUN. Cela ne s'applique pas aux instances DD VE.
Model	Type de tiroir de disques. Cela ne s'applique pas aux instances DD VE.
Disk Count	Nombre de disques dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Disk Size (taille dans DD VE)	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
License Used	Capacité sous licence utilisée par le stockage.
Failed Disks	Disques défaillants dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Configured	Stockage nouveau ou existant. Cela ne s'applique pas aux instances DD VE.
Type	SCSI. Cela s'applique uniquement aux instances DD VE.

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Configure Archive Tier

La section Configure Archive Tier vous permet de configurer les périphériques Archive Storage Tier. Le niveau d'archivage est le lieu où résident les données archivées avec la fonction DD Extended Retention. Pour ajouter du stockage au niveau d'archivage, sélectionnez un ou plusieurs périphériques et ajoutez-les au niveau. Vous pouvez ajouter des périphériques de stockage dans la limite de la capacité autorisée par les licences installées.

Le stockage Archive Tier n'est pas disponible sur le système DD3300 ou sur les instances DD VE.

Tableau 10 Addable Storage

Élément	Description
ID	Identifiant du disque, qui peut être un des éléments suivants. • Le numéro de boîtier et de disque (au format Enclosure Slot ou Enclosure Pack pour les tiroirs DS60) • Le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk • Une LUN
Disks	Disques qui composent la pile de disques ou la LUN.
Modèle	Type de tiroir de disques.
Disk Count	Nombre de disques dans la pile de disques ou dans la LUN.
Disk Size (taille dans DD VE)	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
License Needed	Capacité sous licence requise pour ajouter le stockage au niveau.
Failed Disks	Disques défaillants dans la pile de disques ou dans la LUN.

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Tableau 11 Valeurs Archive Tier

Élément	Description
ID	Identifiant du disque, qui peut être un des éléments suivants. • Le numéro de boîtier et de disque (au format Enclosure Slot ou Enclosure Pack pour les tiroirs DS60). Cela ne s'applique pas aux instances DD VE. • Le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk • Une LUN
Disks	Disques qui composent la pile de disques ou la LUN.
Modèle	Type de tiroir de disques.
Disk Count	Nombre de disques dans la pile de disques ou dans la LUN.

Tableau 11 Valeurs Archive Tier (suite)

Élément	Description
Disk Size (taille dans DD VE)	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
License Used	Capacité sous licence utilisée par le stockage.
Failed Disks	Disques défaillants dans la pile de disques ou dans la LUN.
Configured	Stockage nouveau ou existant.

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Configure Cloud Tier

La section Configure Cloud Tier vous permet de configurer les périphériques du niveau de stockage cloud. Pour ajouter du stockage au niveau cloud, sélectionnez un ou plusieurs périphériques et ajoutez-les au niveau. Vous pouvez ajouter des périphériques de stockage dans la limite de la capacité autorisée par les licences installées.

Le système DD3300 exige des périphériques de 1 To pour DD Cloud Tier.

Tableau 12 Addable Storage

Élément	Description
ID (périphérique dans DD VE)	Identifiant du disque, qui peut être un des éléments suivants. • Le numéro de boîtier et de disque (au format Enclosure Slot ou Enclosure Pack pour les tiroirs DS60) • Le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk • Une LUN
Disks	Disques qui composent la pile de disques ou la LUN. Cela ne s'applique pas aux instances DD VE.
Model	Type de tiroir de disques. Cela ne s'applique pas aux instances DD VE.
Disk Count	Nombre de disques dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Disk Size (taille dans DD VE)	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
License Needed	Capacité sous licence requise pour ajouter le stockage au niveau.
Failed Disks	Disques défaillants dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Type	SCSI. Cela s'applique uniquement aux instances DD VE.

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Tableau 13 Valeurs Cloud Tier

Élément	Description
ID (périphérique dans DD VE)	Identifiant du disque, qui peut être un des éléments suivants. • Le numéro de boîtier et de disque (au format Enclosure Slot ou Enclosure Pack pour les tiroirs DS60). Cela ne s'applique pas aux instances DD VE. • Le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk • Une LUN
Disks	Disques qui composent la pile de disques ou la LUN. Cela ne s'applique pas aux instances DD VE.
Model	Type de tiroir de disques. Cela ne s'applique pas aux instances DD VE.
Disk Count	Nombre de disques dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Disk Size (taille dans DD VE)	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
License Used	Capacité sous licence utilisée par le stockage.
Failed Disks	Disques défaillants dans la pile de disques ou dans la LUN. Cela ne s'applique pas aux instances DD VE.
Configured	Stockage nouveau ou existant. Cela ne s'applique pas aux instances DD VE.
Type	SCSI. Cela s'applique uniquement aux instances DD VE.

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Page de création d'un système de fichiers

La page Create File System affiche la taille autorisée de chaque niveau de stockage dans le système de fichiers et vous permet d'activer automatiquement le système de fichiers après sa création.

Paramètres système

La section **System Settings** vous permet de configurer les mots de passe système et les paramètres du courrier électronique. Cliquez sur **Yes** pour configurer les paramètres système ou cliquez sur **No** pour ignorer la configuration des paramètres système.

Page des paramètres système de l'administrateur

La page Administrator vous permet de configurer le mot de passe de l'administrateur et vous indique la façon dont le système communique avec l'administrateur.

Tableau 14 Paramètres de la page Administrator

Élément	Description
User Name	Le nom par défaut de l'administrateur est *sysadmin*. L'utilisateur sysadmin ne peut être ni renommé ni supprimé.
Old Password	Saisissez l'ancien mot de passe du sysadmin.
New Password	Saisissez le nouveau mot de passe du sysadmin.
Verify New Password	Confirmez le nouveau le mot de passe du sysadmin.
Admin Email	Indiquez l'adresse e-mail à laquelle DD System Manager envoie les messages e-mail d'alerte et d'autosupport.
Send Alert Notification Emails to this address	Sélectionnez cette option pour configurer DD System Manager afin qu'il envoie des notifications d'alerte à l'adresse e-mail de l'administrateur lorsque des événements d'alerte se produisent.
Send Daily Alert Summary Emails to this address	Sélectionnez cette option pour configurer DD System Manager afin qu'il envoie des résumés d'alerte à l'adresse e-mail de l'administrateur à la fin de chaque jour.
Send Autosupport Emails to this address	Sélectionnez cette option pour configurer DD System Manager afin qu'il envoie des e-mails d'autosupport de l'utilisateur admin (il s'agit des rapports quotidiens sur l'activité et le statut du système).

Page des paramètres de messagerie et d'emplacement du système

La page Email/Location vous permet de configurer le nom du serveur de messagerie, de contrôler les informations système qui sont envoyées vers Data Domain et de spécifier un nom de site pour identifier votre système.

Tableau 15 Paramètres de la page Email/Location

Élément	Description
Mail Server	Spécifiez le nom du serveur de messagerie qui gère les e-mails envoyés au système et reçus du système.
Informations d'identification	Sélectionnez s'il faut ou non demander des informations d'identification pour le serveur de messagerie.
User Name	Si les informations d'identification sont activées, spécifiez le nom d'utilisateur du serveur de messagerie.
Password	Si les informations d'identification sont activées, spécifiez le mot de passe du serveur de messagerie.
Send Alert Notification Emails to Data Domain	Sélectionnez cette option pour configurer DD System Manager afin qu'il envoie des e-mails de notification d'alerte à Data Domain.
Send Vendor Support Notification Emails to Data Domain	Sélectionnez cette option pour configurer DD System Manager afin qu'il envoie des e-mails de notification de prise en charge des fournisseurs au système Data Domain.
Location	Utilisez cet attribut facultatif en fonction des besoins pour enregistrer l'emplacement de votre système. Si vous spécifiez

Tableau 15 Paramètres de la page Email/Location (suite)

Élément	Description
	un emplacement, ces informations sont stockées comme emplacement du système SNMP.

Protocole DD Boost

La section des paramètres **DD Boost** vous permet de configurer les paramètres du protocole DD Boost. Cliquez sur **Yes** pour configurer les paramètres du protocole DD Boost ou cliquez sur **No** pour ignorer la configuration DD Boost.

Page des unités de stockage DD Boost

La page Storage Unit vous permet de configurer les unités de stockage DD Boost.

Pour configurer ces paramètres en dehors de l'assistant de configuration, sélectionnez **Protocols** > **DD Boost** > **Storage Units** > **+ (signe plus)** pour ajouter une unité de stockage. Sélectionnez le **crayon** pour modifier une unité de stockage ou **X** pour en supprimer une.

Tableau 16 Paramètres de la page Storage Unit

Élément	Description
Storage Unit	Nom de votre unité de stockage DD Boost Storage. Vous pouvez éventuellement modifier ce nom.
User	Pour l'utilisateur DD Boost par défaut, sélectionnez un utilisateur existant, ou sélectionnez Create a new Local User et saisissez le nom d'utilisateur, le mot de passe et le rôle de gestionnaire. Ce rôle peut être l'un des suivants : • *Admin role* : Permet de configurer et de surveiller l'ensemble du système Data Domain. • *User role* : vous permet de surveiller les systèmes Data Domain et de modifier votre propre mot de passe. • *Security role* : en plus d'offrir les privilèges attachés au rôle d'utilisateur, ce mode vous permet de définir des configurations de responsable de la sécurité et de gérer d'autres opérateurs responsables de la sécurité. • *Backup-operator role* : en plus d'offrir les privilèges attachés au rôle d'utilisateur, ce mode vous permet de créer des snapshots, d'importer et d'exporter des bandes vers une DD VTL, ainsi que de déplacer des bandes dans une DD VTL. • *None role* : destiné à l'authentification DD Boost. Lorsque ce rôle est attribué il n'est pas possible de surveiller ni de configurer le système Data Domain. None (aucun) est également le rôle parent pour les rôles d'administrateur de tenant et d'utilisateur de tenant SMT. Il s'agit, en outre, du type d'utilisateur préféré pour les propriétaires

Tableau 16 Paramètres de la page Storage Unit (suite)

Élément	Description
	de stockage DD Boost. La création d'un utilisateur local ne lui permet que de bénéficier du rôle « none ».

Page des paramètres Fibre Channel du protocole DD Boost

La page Fibre Channel vous permet de configurer les groupes d'accès DD Boost sur Fibre Channel.

Pour configurer ces paramètres en dehors de l'assistant de configuration, sélectionnez **Protocols** > **DD Boost** > **Fibre Channel** > **+ (signe plus)** pour ajouter un groupe d'accès. Sélectionnez **le crayon** pour modifier un groupe d'accès ou sélectionnez **X** pour en supprimer un.

Tableau 17 Page des paramètres Fibre Channel

Élément	Description
Configure DD Boost over Fibre Channel	Cochez cette case si vous souhaitez configurer DD Boost sur Fibre Channel.
Group Name (1-128 car.)	Créez un groupe d'accès. Saisissez un nom unique. Les groupes d'accès dupliqués ne sont pas pris en charge.
Initiators	Sélectionnez un ou plusieurs initiateurs. Éventuellement, remplacez le nom de l'initiateur en en saisissant un nouveau. Un initiateur est un client de sauvegarde qui se connecte au système pour lire et écrire des données à l'aide du protocole FC (Fibre Channel). Un initiateur spécifique peut prendre en charge DD Boost over FC ou DD VTL, mais pas les deux.
Devices	Les périphériques à utiliser sont répertoriés. Ils sont disponibles sur tous les points de terminaison. Un point de terminaison est la cible logique, dans le système Data Domain, à laquelle l'initiateur est connecté.

Protocole CIFS

La section des paramètres **CIFS Protocol** vous permet de configurer les paramètres du protocole CIFS. Cliquez sur **Yes** pour configurer les paramètres du protocole CIFS ou cliquez sur **No** pour ignorer la configuration CIFS.

Les systèmes Data Domain utilisent le terme MTree pour décrire les répertoires. Lorsque vous configurez un chemin de répertoire, DD OS crée une structure MTree où les données seront stockées.

Page d'authentification du protocole CIFS

La page Authentication vous permet de configurer les paramètres Active Directory et de groupe de travail pour votre système.

Pour configurer ces paramètres en dehors de l'assistant de configuration, sélectionnez **Administration** > **Access** > **Authentication**.

Tableau 18 Paramètres de la page Authentication

Élément	Description
Active Directory/Kerberos Authentication	Développez ce volet pour activer, désactiver et configurer l'authentification Kerberos d'Active Directory.
Workgroup Authentication	Développez ce volet pour configurer l'authentification de groupe de travail.
authentification LDAP	Développez ce volet pour configurer l'authentification LDAP.
NIS Authentication	Développez ce volet pour configurer l'authentification NIS.

Page de partage de protocole CIFS

La page Share permet de configurer un nom de partage et un chemin de répertoire pour votre système.

Pour configurer ces paramètres en dehors de l'assistant de configuration, sélectionnez **Protocols** > **CIFS** > **Shares** > **Create**.

Tableau 19 Paramètres de la page Share

Élément	Description
Share Name	Saisissez un nom de partage pour le système.
Directory Path	Saisissez un chemin de répertoire pour le système.
Bouton d'ajout (+)	Cliquez sur + pour saisir un client système, un utilisateur ou un groupe.
Icône en forme de crayon	Modifier un client, un utilisateur ou un groupe.
Bouton de suppression (X)	Cliquez sur X pour supprimer un client, un utilisateur ou un groupe sélectionné.

Protocole NFS

La section des paramètres **NFS Protocol** vous permet de configurer les paramètres de protocole NFS. Cliquez sur **Yes** pour configurer les paramètres du protocole NFS ou cliquez sur **No** pour ignorer la configuration NFS.

Les systèmes Data Domain utilisent le terme MTree pour décrire les répertoires. Lorsque vous configurez un chemin de répertoire, DD OS crée une structure MTree où les données seront stockées.

Page d'exportation du protocole NFS

La page Export vous permet de configurer un chemin de répertoire d'exportation pour le protocole NFS, des clients réseau et des références NFSv4.

Pour configurer ces paramètres en dehors de l'assistant de configuration, sélectionnez **Protocols** > **NFS** > **Create**.

Tableau 20 Paramètres de la page Export

Élément	Description
Directory Path	Saisissez un chemin d'accès pour l'exportation.
Bouton d'ajout (+)	Cliquez sur + pour entrer dans un système client ou une référence NFSv4.
Icône en forme de crayon	Modifiez un client ou une référence NFSv4.
Bouton de suppression (X)	Cliquez sur X pour supprimer un client sélectionné ou une référence NFSv4.

Protocole DD VTL

La section des paramètres **DD VTL Protocol** vous permet de configurer les paramètres de Data Domain Virtual Tape Library. Cliquez sur **Yes** pour configurer les paramètres de DD VTL ou cliquez sur **No** pour ignorer la configuration de DD VTL.

Page VTL Protocol Library

La page Library vous permet de configurer les paramètres du protocole DD VTL pour une bibliothèque.

Pour configurer ces paramètres en dehors de l'assistant de configuration, sélectionnez **PROTOCOLS** > **VTL** > **Virtual Tape Libraries** > **VTL Service** > **Libraries** > **More Tasks** > **Library** > **Create**

Tableau 21 Paramètres de la page Library

Élément	Description
Library Name	Saisissez un nom comprenant entre 1 et 32 caractères alphanumériques.
Number of Drives	Nombre de lecteurs de bande pris en charge.
Drive Model	Sélectionnez le modèle désiré dans la liste déroulante : • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (par défaut) • HP-LTO-3 • HP-LTO-4
Number of Slots	Saisissez le nombre de slots par bibliothèque : • Jusqu'à 32 000 slots par bibliothèque • Jusqu'à 64 000 slots par système • Ce nombre doit être supérieur ou égal au nombre de lecteurs.
Number of CAPs	(Facultatif) Saisissez le nombre de ports d'accès aux cartouches (CAP) :

Tableau 21 Paramètres de la page Library (suite)

Élément	Description
	• Jusqu'à 100 ports CAP par bibliothèque • Jusqu'à 1 000 ports CAP par système
Changer Model Name	Sélectionnez le modèle désiré dans la liste déroulante : • L180 (par défaut) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL
Starting Barcode	Saisissez le code-barres souhaité pour la première bande, au format A990000LA.
Tape Capacity	(Facultatif) Saisissez la capacité des bandes. Si elle n'est pas spécifiée, la capacité est obtenue à partir du dernier caractère du code-barres.

Page des paramètres du protocole VTL pour un groupe d'accès

La page Access Group vous permet de configurer les paramètres du protocole DD VTL pour un groupe d'accès.

Pour configurer ces paramètres en dehors de l'assistant de configuration, sélectionnez **PROTOCOLS** > **VTL** > **Access Groups** > **Groups** > **More Tasks** > **Group** > **Create**

Tableau 22 Paramètres de la page Access Group

Élément	Description
Group Name	Saisissez un nom unique comprenant entre 1 et 128 caractères. Les groupes d'accès dupliqués ne sont pas pris en charge.
Initiators	Sélectionnez un ou plusieurs initiateurs. Éventuellement, remplacez le nom de l'initiateur en en saisissant un nouveau. Un initiateur est un client de sauvegarde qui se connecte au système pour lire et écrire des données à l'aide du protocole FC (Fibre Channel). Un initiateur spécifique peut prendre en charge DD Boost over FC ou DD VTL, mais pas les deux.
Devices	Les périphériques (disques et changeur) à utiliser sont répertoriés. Ils sont disponibles sur tous les points d'accès. Un point de terminaison est la cible logique, dans le système Data Domain, à laquelle l'initiateur est connecté.

Interface de ligne de commande de Data Domain

L'interface de ligne de commande (CLI) est une interface de type texte que vous pouvez utiliser à la place ou en complément de DD System Manager. La plupart des

opérations de gestion peuvent être effectuées dans DD System Manager ou à l'aide de la CLI. Dans certains cas, la CLI offre des options de configuration et des rapports non encore pris en charge dans DD System Manager.

Toute commande du système Data Domain qui accepte une liste (par exemple, une liste d'adresses IP) accepte les entrées séparées par des virgules, par des espaces ou par les deux.

La touche de tabulation permet d'effectuer les opérations suivantes.

- Effectuer une entrée de commande lorsque cette entrée est unique. L'utilisation de la touche tabulation est prise en charge pour tous les mots clés. Par exemple, saisir `syst` tabulation `sh` tabulation `st` tabulation affiche la commande `system show stats`.
- Afficher l'option suivante disponible si vous ne saisissez aucun caractère avant d'appuyer sur la touche de tabulation.
- Afficher les jetons partiellement mis en correspondance ou exécuter une entrée unique si vous saisissez des caractères avant d'appuyer sur la touche de tabulation.

Le *Guide de référence des commandes de Data Domain Operating System* fournit des informations sur chacune des commandes de la CLI. L'aide en ligne est disponible et présente la syntaxe complète de chaque commande.

Connexion à la CLI

Vous pouvez accéder à l'interface de ligne de commande (CLI) via une connexion directe au système ou une connexion Ethernet utilisant SSH ou Telnet.

Avant de commencer

Pour tirer parti de la CLI, vous devez établir une connexion locale ou distante au système en utilisant l'une des méthodes suivantes.

- Si vous vous connectez via le port d'une console série du système, reliez un terminal au port et utilisez les paramètres de communication suivants : 9 600 bauds, 8 bits de données, parité nulle et 1 bit d'arrêt.
- Si le système dispose de ports de clavier et de moniteur, reliez un clavier et un moniteur à ces ports.
- Si vous vous connectez via Ethernet, reliez un ordinateur avec un logiciel client SSH ou Telnet à un réseau Ethernet capable de communiquer avec le système.

Procédure

1. Si vous utilisez une connexion SSH ou Telnet pour accéder à la CLI, lancez le client SSH ou Telnet et spécifiez l'adresse IP ou le nom d'hôte du système.

   Pour plus d'informations sur l'établissement de la connexion, consultez la documentation de référence du logiciel client. Le système vous demande d'entrer votre nom d'utilisateur.
2. Saisissez votre nom d'utilisateur système lorsque vous y êtes invité.
3. Saisissez votre mot de passe système lorsque vous y êtes invité.

L'exemple suivant illustre une connexion SSH à un système appelé *mysystem* au moyen du logiciel client SSH.

```
# ssh -l sysadmin mysystem.mydomain.com
Data Domain OS 5.6.0.0-19899
```

```
Password:
```

Recommandations relatives à l'aide en ligne de la CLI

L'interface de ligne de commande (CLI) affiche deux types d'aide, à savoir une aide réservée à la syntaxe et une aide décrivant les commandes qui inclut la syntaxe des commandes. Ces deux types d'aide proposent des fonctions très pratiques permettant de trouver plus rapidement les informations dont vous avez besoin.

Les instructions ci-dessous décrivent la façon d'utiliser l'aide réservée à la syntaxe.

- Pour afficher la liste des commandes de la CLI de niveau supérieur, saisissez un point d'interrogation (`?`) ou entrez la commande `help` lorsque vous y êtes invité.
- Pour répertorier toutes les formes d'une commande de niveau supérieur, entrez la commande sans option à l'invite ou saisissez la *commande* `?`.
- Pour répertorier toutes les commandes qui utilisent un mot clé spécifique, saisissez `help`*keyword* ou `?`*keyword*.
  Par exemple, `? password` affiche toutes les commandes du système Data Domain qui utilisent l'argument de mot de passe.

Les instructions ci-dessous expliquent la façon d'utiliser l'aide de description des commandes.

- Pour afficher la liste des commandes de la CLI de niveau supérieur, saisissez un point d'interrogation (`?`) ou entrez la commande `help` lorsque vous y êtes invité.
- Pour afficher la liste de toutes les formes d'une commande de niveau supérieur avec une introduction, saisissez `help`*command* ou `?`*command*.
- La fin de chaque description d'aide est marquée `END`. Appuyez sur Entrée pour revenir à une invite de la CLI.
- Lorsque la description complète de l'aide ne tient pas sur l'affichage, l'invite deux points (`:`) s'affiche au bas de l'écran. Les instructions ci-dessous expliquent que faire lorsque cette invite apparaît.
  - Pour vous déplacer dans l'affichage de l'aide, utilisez les touches fléchées haut et bas.
  - Pour quitter l'aide actuelle affichée et revenir à l'invite d'interface de ligne de commande, appuyez sur **`q`**.
  - Pour afficher l'aide sur la navigation dans l'affichage de l'aide, appuyez sur **`h`**.
  - Pour rechercher un texte dans l'affichage de l'aide, entrez une barre oblique (`/`) suivie par un modèle à utiliser comme critère de recherche et appuyez sur Entrée. Les correspondances sont mises en surbrillance.

CHAPITRE 3

Gestion des systèmes Data Domain

Ce chapitre traite des sujets suivants :

Présentation de la gestion du système

DD System Manager vous permet de gérer le système sur lequel il est installé.

- Pour prendre en charge la réplication, DD System Manager prend en charge l'ajout de systèmes exécutant les deux versions précédentes, la version actuelle et les deux versions suivantes lorsqu'elles deviennent disponibles. Pour la version 6.0, DD System Manager prend en charge l'ajout de systèmes de réplication pour les versions 5.6 à 5.7 de DD OS, plus les deux versions suivantes.

Remarque

Lors du traitement d'une lourde charge, un système peut être moins réactif que normalement. Dans ce cas, les commandes de gestion émises à partir de DD System Manager ou de l'interface de ligne de commande peuvent prendre plus longtemps pour s'exécuter. Lorsque la durée dépasse les limites autorisées, une erreur d'expiration du délai est renvoyée, même si l'opération s'est terminée.

Le tableau suivant indique le nombre maximal de sessions utilisateur prises en charge par DD System Manager :

Tableau 23 Nombre maximal d'utilisateurs pris en charge par DD System Manager

Modèle de système	Nombre maximal d'utilisateurs actifs	Nombre maximal d'utilisateurs connectés
Modèles à 4 Go[a]	5	10
Modèles à 8 Go[b]	10	15
Modèles à 16 Go et supérieurs[c]	10	20

a. Inclut DD140 et DD2200 (4 To)
b. Inclut DD610 et DD630
c. Inclut DD670, DD860, DD890, DD990, DD2200 (> à 7,5 To), DD4200, DD4500, DD6300, DD6800, DD7200, DD9300, DD9500 et DD9800

Remarque

La configuration initiale du système haute disponibilité ne peut pas être effectuée à partir de DD System Manager, mais l'état d'une haute disponibilité déjà configurée sur le système peut être affiché à partir de DD System Manager.

Tour d'horizon de la gestion d'un système haute disponibilité

La relation HA entre les deux nœuds, l'un actif et l'autre en veille, est configurée via les CLI DDSH.

La configuration initiale peut être exécutée sur l'un des deux nœuds, mais uniquement un à la fois. La haute disponibilité requiert que l'interconnexion du système et un matériel identique soient au préalable configurés sur les deux nœuds.

Remarque

Les deux DDR doivent posséder un matériel identique validé au cours de la configuration et du démarrage du système.

Si la configuration provient d'une nouvelle installation de systèmes, la commande `ha create` doit être exécutée sur le nœud où est installée la licence. Si la configuration provient d'un système existant et d'une nouvelle installation de système (mise à niveau), celle-ci doit être exécutée à partir du système existant.

Maintenance planifiée d'un système haute disponibilité

L'architecture haute disponibilité (HA) assure une mise à niveau consécutive, ce qui réduit les interruptions de service de maintenance pour une mise à niveau DD OS.

Avec une mise à niveau consécutive, les nœuds HA sont mis à niveau un par un, de façon coordonnée et automatiquement. Le nœud en veille est redémarré et mis à niveau en premier. Le nœud récemment mis à niveau prend le rôle actif grâce à un basculement sur incident en mode haute disponibilité. Une fois le basculement sur incident opéré, le deuxième nœud est redémarré et reprend le rôle du nœud en veille après la mise à niveau.

Les opérations de mise à niveau du système nécessitant la conversion des données peuvent ne pas démarrer tant que les deux systèmes n'auront pas été mis à niveau vers la même version et que l'état HA n'aura pas été entièrement restauré.

Redémarrage d'un système

Certaines modifications de la configuration, comme un changement de fuseau horaire, exigent que vous redémarriez le système.

Procédure

1. Sélectionnez **Maintenance** > **System** > **Reboot System**.
2. Cliquez sur le bouton **OK** pour confirmer.

Mise sous tension/hors tension d'un système

Lors de la mise sous tension/hors tension d'un système, il est important de suivre la procédure appropriée pour préserver l'intégrité du système de fichiers et de la configuration.

N'utilisez pas l'interrupteur du châssis pour mettre le système hors tension. Sinon, vous empêchez la commande d'alimentation à distance d'utiliser IPMI. Utilisez la commande `system poweroff` à la place. La commande `system poweroff` arrête le système et coupe l'alimentation.

La fonction IMPI Remote System Power Down n'effectue pas un arrêt normal de DD OS. Utilisez cette fonction uniquement si la commande `system poweroff` échoue.

Pour les systèmes HA, une connexion aux deux nœuds est requise.

Procédez comme suit pour mettre le système Data Domain hors tension :

Procédure

1. Vérifiez que les E/S sont arrêtées sur le système.

   Exécutez les commandes suivantes :

   - `cifs show active`
   - `nfs show active`
   - `system show stats view sysstat interval 2`
   - `system show perf`

2. Pour les systèmes HA, vérifiez l'état de santé de la configuration HA.

   Exécutez la commande suivante :
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

Remarque

Cet exemple de sortie provient d'un système fonctionnel. Si le système est en cours d'arrêt pour remplacer un composant défaillant, l'état du système HA risque de se dégrader, et un ou les deux nœuds ne seront pas affichés hors ligne pour l'état de haute disponibilité.

3. Exécutez la commande `alerts show current`. Pour les paires HA, exécutez la commande sur le nœud actif tout d'abord, puis sur le nœud en veille.
4. Pour les systèmes HA, exécutez la commande `ha offline` si le système est dans un état de haute disponibilité et que les deux nœuds sont en ligne. Ignorez cette étape si l'état de haute disponibilité est dégradé.
5. Exécutez la commande `system poweroff`. Pour les paires HA, exécutez la commande sur le nœud actif tout d'abord, puis sur le nœud en veille.

```
# system poweroff

Continue? (yes|no|?) [no]: yes
```

   Cette commande exécute automatiquement un arrêt normal de tous les processus de DD OS. Elle n'est accessible qu'aux administrateurs.
6. Retirez les cordons d'alimentation des blocs d'alimentation sur le ou les contrôleurs.
7. Vérifiez que le voyant bleu est éteint sur le ou les contrôleurs pour confirmer que le système est hors tension.

   Une fois le contrôleur hors tension, mettez hors tension tous les tiroirs d'extension externes (ES30, DS60, FS15).

Mise sous tension d'un système

Remettez le système Data Domain sous tension lorsque la période d'interruption du système est terminée.

Procédure

1. Mettez sous tension les tiroirs d'extension avant de mettre sous tension le contrôleur Data Domain. Patientez environ trois minutes après que tous les tiroirs d'extension ont été mis sous tension.

Remarque

Un Contrôleur est le châssis et n'importe quel stockage interne. Un *système Data Domain* fait référence au Contrôleur et à tout stockage externe en option.

2. Branchez le cordon d'alimentation de votre contrôleur et, si le contrôleur a un bouton d'alimentation, appuyez sur ce bouton (comme indiqué dans le

document *Installation and Setup Guide* de votre système Data Domain). Pour les systèmes HA, mettez sous tension tout d'abord le nœud actif, puis le nœud en veille

Remarque

Certains périohériques Data Domain n'ont pas de bouton d'alimentation traditionnel, et sont conçus pour être « toujours allumés », et sont mis sous tension dès que l'alimentation CA est appliquée.

3. Pour les systèmes HA, vérifiez l'état de santé de la configuration HA.

   Exécutez la commande suivante :
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   offline
-------------------------- --------- --------- --------
```

4. Pour les systèmes HA, si un des nœuds s'affiche comme étant hors connexion, exécutez la commande `ha online` sur ce nœud pour restaurer la configuration HA.
5. Vérifiez que le système Data Domain est entièrement démarré et que le système d'exploitation fonctionne. Ceci peut être fait avec la console système ou depuis une session SSH vers le système Data Domain. Le système est activé lorsque vous pouvez vous connecter au système.
6. Exécutez la commande `alerts show current`. Pour les paires HA, exécutez la commande sur le nœud actif tout d'abord, puis sur le nœud en veille.

Gestion des mises à niveau du système

Pour mettre à niveau un système DD OS, vous devez vérifier que vous disposez de suffisamment d'espace pour le nouveau logiciel sur le système cible, transférer le logiciel sur le système à mettre à jour, puis démarrer la mise à niveau. Dans le cas d'un système haute disponibilité (HA), transférez le logiciel sur le nœud actif et lancez la mise à niveau à partir du nœud actif.

Pour les systèmes haute disponibilité, utilisez l'adresse IP flottante pour accéder à DD System Manager en vue d'effectuer des mises à niveau logicielles.

⚠ ATTENTION

DD OS 6.0 utilise Secure Remote Support version 3 (ESRSv3). La mise à niveau d'un système exécutant DD OS 5.X vers DD OS 6.0 a pour effet de supprimer la configuration ConnectEMC existante du système. Une fois la mise à niveau terminée, reconfigurez ConnectEMC manuellement.

Si le système utilise des certificats signés MD5, régénérez les certificats avec un algorithme de hachage plus puissant au cours du processus de mise à niveau.

Mise à niveau avec perturbation minimale
La fonction de mise à niveau avec perturbation minimale (MDU) vous permet de mettre à niveau des composants logiciels spécifiques ou d'appliquer des corrections de bogues sans avoir à effectuer le redémarrage du système. Seuls les services qui dépendent du composant mis à niveau sont interrompus. La fonction MDU peut donc

limiter considérablement les temps d'inactivité au cours de certaines mises à niveau logicielles.

Les composants logiciels ne sont pas tous éligibles aux mises à niveau avec perturbation minimale ; ces composants doivent, de ce fait, être mis à niveau dans le cadre d'une mise à niveau du logiciel système DD OS standard. Une mise à niveau du logiciel DD OS exige un RPM particulièrement important (bundle de mise à niveau), lequel exécute des actions de mise à niveau pour tous les composants de DD OS. Or, la fonction de mise à niveau avec perturbation minimale (MDU) fait appel à des bundles de composant plus petits, lesquels effectuent la mise à niveau de composants logiciels spécifiques de façon individuelle.

Vérification de la signature RPM
La procédure de vérification de la signature RPM valide les RPM Data Domain que vous téléchargez pour la mise à niveau. Si le RPM n'est pas falsifié, la signature numérique est valide et vous pouvez utiliser le RPM comme vous le faites d'habitude. Si le RPM est falsifié, la corruption invalide la signature numérique et le RPM est rejeté par DD OS. Un message d'erreur approprié s'affiche.

Remarque

Pour passer de la version 5.6.0.x à la version 6.0, commencez par mettre à niveau le système 5.6.0.x vers 5.6.1.x (ou une version ultérieure) avant de lancer la mise à niveau vers la version 6.0.

Logiciel de support
DD OS 6.1 introduit un type de package logiciel appelé logiciel de support. Le logiciel de support est fourni par les ingénieurs du support Data Domain pour régler certains problèmes. Par défaut, le système Data Domain ne permet pas l'installation du logiciel de support sur le système. Contactez le support technique pour de plus amples informations sur le logiciel de support.

Listes de contrôle et tour d'horizon préalable à la mise à niveau

Avant d'effectuer une mise à niveau de DD OS, vous devez passer en revue les éléments de ces listes de contrôle avant de procéder. Cela peut simplifier le processus de mise à niveau et éviter d'éventuelles difficultés.

Tâches manuelles préalables à la mise à niveau

⚠ ATTENTION

Si vous n'exécutez pas les tâches de cette section, vous risquez d'entraîner l'échec de la mise à niveau.

Il s'agit de tâches que vous devez prévoir d'effectuer avant la mise à niveau. Ces tâches ne sont exécutées automatiquement par aucun processus.

1. Redémarrez le système Data Domain. Pour les systèmes HA, suivez les instructions de redémarrage décrites dans la section Considérations relatives à la mise à niveau pour les systèmes HA à la page 64 après avoir effectué le reste des contrôles de cette section.
2. Vérifiez les alertes en cours ; cela peut révéler de nombreuses défaillances de disque et autres défaillances matérielles qui doivent être corrigées avant la mise à niveau :

   ```
   # alert show current
   ```

3. Vérifiez que les paramètres du registre pour `config.net.*`, `crontab`, et ceux relatifs au réseau sont valides.

   Par exemple, utilisez l'opération `reg show config.net`, et vérifiez si `noauto.enabled`, `noauto.speed` et `noauto.full_duplex` sont correctement définis. Cela permet au réseau de négocier la vitesse. Vérifiez également `.use_dhcp=true`, car cela permettra une configuration rapide non seulement de l'adresse IP et du masque réseau, mais aussi de la passerelle.

   Cette vérification est importante, car si ces éléments sont mal configurés, le redémarrage peut rendre le réseau indisponible.

4. Vérifiez si toutes les interfaces réseau sont opérationnelles et possèdent les adresses IP appropriées, et vérifiez si le système Data Domain est accessible via Data Domain System Manager ou tout autre client utilisé :

   ```
   # net show
   ```

5. Vérifiez l'état des disques et n'effectuez pas la mise à niveau si le système Data Domain est à court de pièces de rechange ou si les disques présentent des états absents, en échec ou en reconstruction :

   ```
   # disk show state
   ```

   ```
   # disk show reliability-data
   ```

6. Vérifiez la fiabilité des disques et remplacez tous les disques qui ont plus de 50 secteurs réaffectés :

   ```
   # disk show reliability-data
   ```

7. Vérifiez l'état du boîtier :

   ```
   # enclosure show all
   ```

   Il doit « OK » pour tous les périphériques.

8. Vérifiez si la topologie du boîtier est correcte :

   ```
   # enclosure show topology
   ```

   Vérifiez également si une erreur s'affiche avec un astérisque (*) à côté du champ **enc.ctrl.port**. Vérifiez également que le champ **Error Message** ne contient pas d'erreurs telles que `"A possible problem was detected for this shelf controller or the cable connected to it."`.

9. Vérifiez que le mappage des ports du périphérique est correct :

   ```
   # system show hardware
   ```

10. Vérifiez la vitesse de liaison pour les ports connectés :

    ```
    # system show ports
    ```

11. Vérifiez l'état du système de fichiers pour vous assurer que le système de fichiers est activé et fonctionne normalement :

    ```
    # filesys status
    ```

12. Vérifiez si le nettoyage du système de fichiers est en cours d'exécution, et si oui, arrêtez-le :

    ```
    # filesys clean status
    ```

    ```
    # filesys clean stop
    ```

13. Si la réplication est activée, vérifiez son état :

```
# replication status
```

14. Si le système est dans une configuration de cluster, vérifiez si le cluster est opérationnel :

    ```
    # cluster show config
    ```

15. Pour un système sur lequel DD Cloud Tier est activé, assurez-vous qu'il n'existe aucun mouvement de données :

    ```
    # data-movement status
    ```

    ```
    # data-movement stop all
    ```

16. Vérifiez si le nettoyage du Cloud est en cours d'exécution, et si oui, arrêtez-le :

    ```
    # cloud clean status
    ```

    ```
    # cloud clean stop
    ```

17. Vérifiez si une activité de sauvegarde et de restauration est en cours et, le cas échéant, arrêtez-la :

    ```
    # system show stats
    ```

18. Vérifiez le log `kern.info`, et si vous remarquez des défaillances fréquentes du matériel, contactez le suppor Data Domain pour que celui-ci inspecte votre système avant d'effectuer la mise à niveau.

    ```
    # log view debug/platform/kern.info
    ```

19. Exécutez un rapport d'autosupport juste avant d'effectuer la mise à niveau de DD OS afin de déterminer si les problèmes restants doivent être résolus :

    ```
    # autosupport send <votre_adresse_e-mail>
    ```

Considérations relatives à la mise à niveau pour les systèmes HA

Les systèmes d'AP nécessitent des étapes uniques avant de démarrer l'opération de mise à niveau et une vérification ultérieure unique une fois la mise à niveau terminée.

⚠ ATTENTION

Effectuez les contrôles manuels décrits dans la section Tâches manuelles préalables à la mise à niveau à la page 62 avant de redémarrer le système HA.

Lors de la mise à niveau d'un système HA, téléchargez le package RPM de mise à niveau vers le nœud actif.

1. Le système HA doit être dans un état de haute disponibilité, avec les deux nœuds en ligne avant d'effectuer la mise à niveau de DD OS. Exécutez la commande `ha status` pour vérifier l'état du système HA.

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com         0      active    online
apollo-ha3a-p1.emc.com         1      standby   online
--------------------------- --------- --------- --------
```

2. Redémarrez le nœud en veille (nœud 1).
3. Exécutez la commande `ha status` pour vérifier l'affichage de l'état du système HA en tant que `highly available` après le redémarrage du nœud en veille.
4. Exécutez la commande `ha failover` pour lancer un basculement du nœud actif vers le nœud en veille.

5. Exécutez la commande `ha status` pour vérifier que le nœud 1 est le nœud actif et que le nœud 0 est le nœud en veille.

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       standby   online
apollo-ha3a-p1.emc.com       1       active    online
-------------------------- --------- --------- --------
```

6. Redémarrez le nœud en veille (nœud 0).
7. Exécutez la commande `ha status` pour vérifier l'affichage de l'état du système HA en tant que `highly available` après le redémarrage du nœud en veille.
8. Exécutez la commande `ha failover` pour lancer un basculement du nœud actif vers le nœud en veille.
9. Exécutez la commande `ha status` pour vérifier que le nœud 0 est le nœud actif et que le nœud 1 est le nœud en veille.

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

Lancez la mise à niveau à partir du nœud actif. DD OS reconnaît automatiquement le système HA et effectue la procédure de mise à niveau sur les deux nœuds. La mise à niveau HA s'exécute dans l'ordre suivant :

1. Le nœud en veille est d'abord mis à niveau, puis redémarre.
2. Une fois le redémarrage terminé, le système HA lance un basculement et le nœud en veille prend le relais en tant que nœud actif.
3. Le nœud actif d'origine est mis à niveau, puis redémarre et reste le nœud en veille.

Une fois les deux nœuds mis à niveau, le système n'effectue plus de basculement pour les ramener à leur configuration initiale.

Une fois la procédure de mise à niveau terminée, exécutez la commande `ha status` afin de vérifier que le système est dans un état de haute disponibilité, et que les deux nœuds sont en ligne.

Exécutez la commande en option `ha failover` pour redonner aux nœuds les rôles dans lesquels ils se trouvaient avant la mise à niveau.

Tâches automatiques effectuées avant la mise à niveau

La compréhension de ces aspects d'une mise à niveau de DD OS assure un processus plus fluide.

La version de DD OS sur votre système Data Domain effectue ces tâches avant la mise à niveau :

1. Détermine si l'initialisation de la réplication est en cours. Si c'est le cas, la mise à niveau n'a pas lieu.
2. Inspecte l'ensemble des résumés et des signatures contenus dans le fichier .rpm pour s'assurer de l'intégrité et de l'origine du package. Si la signature n'est pas valide, la mise à niveau n'a pas lieu.
3. Déterminez si la mise à niveau de l'ancienne version de DD OS vers la nouvelle version est autorisée. Les systèmes Data Domain exécutant DD OS 5.7.x ou 6.0.x

peuvent évoluer directement vers la version 6.1. Cette restriction est due à la signature du RPM. Une mise à niveau n'est généralement pas autorisée dans ces circonstances :

a. La mise à jour se fait entre les mêmes versions, par exemple de 6.0.0.1 à 6.0.0.4. (Ceci peut être ignoré dans certaines circonstances spécifiques ; consultez votre représentant du support Data Domain pour plus de détails.)

b. La mise à niveau est rétrograde, par exemple de 6.0 à 5.7.

c. La mise à niveau dépasse deux générations de fonctionnalités, telles que 5.5 à 6.0.

4. Déterminez si des points de montage NFS sont inconnus. Si un point de montage NFS est inconnu, la mise à niveau n'a pas lieu.
5. Détermine si la mise à niveau précédente, le cas échéant, a été effectuée avec succès. Si la mise à niveau précédente a échoué ou n'a pas été effectuée, la mise à niveau en cours n'a pas lieu.

Tâches automatiques effectuées par le script de mise à niveau (dans le fichier.rpm) avant la mise à niveau

Ces tests précèdent le processus de mise à niveau sur le système Data Domain :

1. Déterminez si deux types différents de cartes NVRAM sont présents.
2. Vérifiez la taille des partitions `/ddr` et `/` (root) pour l'utilisation de l'espace.
3. Recherchez la version OST.
4. Déterminez si le métagroupe RAID est assemblé. S'il n'est pas assemblé, le processus de mise à niveau ne commence pas.
5. Déterminer l'espace disponible pour le système de fichiers.
6. Déterminez si l'espace disponible est suffisant pour la mise à niveau.
7. Vérifiez la version VTL, si VTL est présent.
8. Déterminez si le système de fichiers est activé, et s'il ne l'est pas, activez-le.
9. Déterminez si la VTL est activée.
10. Vérifiez les pools VTL pour vous assurer qu'ils peuvent être convertis en structures MTree.
11. Déterminez si l'espace VTL disponible est suffisant.
12. Assurez-vous que le nombre de structures MTree et de pools VTL ne dépasse pas 100. (Ce contrôle est appliqué à partir de la version 5.0 de DD OS.)
13. Déterminez si tous les disques dg0 sont situés sur l'unité principale. Si ce n'est pas le cas, le processus de mise à niveau ne commence pas et le problème doit être résolu.
14. Vérifiez si ConnectEMC a été configuré. Si tel est le cas, un message d'avertissement s'affiche pour informer le client qu'il doit reconfigurer ConnectEMC après la mise à niveau.

En plus de ces vérifications, le système détermine si le système de fichiers peut être arrêté proprement et sans problème. Si le système de fichiers ne peut pas être arrêté d'une manière appropriée, le processus de mise à niveau s'arrête.

Conditions qui empêchent le processus de mise à niveau

Plusieurs conditions peuvent entraîner l'arrêt du processus de mise à niveau :

- Le système Data Domain n'est pas dans un état fonctionnel. Par exemple :
  - Le stockage est déficient sur le plan fonctionnel, par exemple, il manque un bôitier.
  - Le système de fichiers ne s'est pas arrêté proprement, ce qui a entraîné un vidage mémoire.
  - La mise à niveau précédente ne s'est pas terminée correctement.
- L'utilisation de l'espace est problématique. Par exemple :
  - La partition `/` (root) ou `/ddr` est pleine de fichiers log, de vidages mémoire, etc.
  - L'espace de stockage disponible est insuffisant pour effectuer la mise à niveau des données.
- Le système Data Domain n'est pas configuré correctement. Par exemple, les points de montage NFS ont été créés manuellement sous root.
- Les noms d'unités de stockage ne sont pas convertis en noms MTree. Pour être convertis en noms MTree, les noms d'unités de stockage doivent contenir uniquement des lettres majuscules et minuscules (a-z, A-Z), des chiffres (0-9) et un trait de soulignement (_) et ne pas dépasser 50 caractères.

Le but de la vérification de ces conditions est d'empêcher toute mise à niveau problématique ou toute anomalie du système de fichiers de se produire ou de se propager. Ces conditions s'appliquent également aux mises à niveau impliquant les systèmes partenaires source et destination dans la réplication. Une mise à niveau en échec ou une anomalie de système de fichiers sur un système Data Domain servant de source de réplication ne provoque aucune corruption dans le système de fichiers sur un système Data Domain servant de destination de réplication.

Affichage des packages de mise à niveau sur le système

DD System Manager vous permet de visualiser et de gérer jusqu'à cinq packages de mise à niveau sur un système. Avant de pouvoir mettre à niveau un système, vous devez télécharger un package de mise à niveau à partir du site de support en ligne vers un ordinateur local, puis le télécharger sur le système cible.

Procédure

1. Sélectionnez **Maintenance** > **System**.
2. Si vous le souhaitez, sélectionnez un package de mise à niveau, puis cliquez sur **View Checksum** pour afficher les sommes de contrôle MD5 et SHA256 du package de mise à niveau.

Résultats

Pour chaque package stocké sur le système, DD System Manager affiche le nom du fichier, la taille du fichier et la date de la dernière modification dans la liste intitulée : Upgrade Packages Available on Data Domain System.

Obtention et vérification des modules de mise à niveau

Vous pouvez utiliser DD System Manager pour localiser les fichiers du module de mise à niveau sur le site Web de support de Data Domain et pour télécharger des copies de ces fichiers dans un système.

Remarque

Vous pouvez utiliser le FTP ou le NFS pour copier un module de mise à niveau sur un système. DD System Manager est limité à la gestion de 5 modules de mise à niveau du système, mais il n'existe aucune restriction, en dehors des contraintes d'espace, lorsque vous gérez les fichiers directement dans le répertoire `/ddvar/releases`. Par défaut, la fonction FTP est désactivée. Pour utiliser le NFS, `/ddvar` doit être exporté et monté à partir d'un hôte externe.

Procédure

1. Sélectionnez **Maintenance** > **System**.
2. Pour obtenir un module de mise à niveau, cliquez sur le lien **EMC Online Support**, cliquez sur Downloads et utilisez la fonction de recherche pour localiser le module recommandé pour votre système par le personnel du support. Enregistrez le module de mise à niveau sur l'ordinateur local.
3. Assurez-vous qu'il n'y a pas plus de quatre modules répertoriés dans la liste Upgrade Packages Available on Data Domain System.

   DD System Manager peut gérer jusqu'à cinq modules de mise à niveau. Si cinq modules s'affichent dans la liste, supprimez au moins un module avant de télécharger le nouveau module.
4. Cliquez sur **Upload Upgrade Package** pour initier le transfert du module de mise à niveau vers le système.
5. Dans la boîte de dialogue Upload Upgrade Package, cliquez sur **Browse** pour ouvrir la boîte de dialogue Choose File to Upload. Accédez au dossier contenant le fichier téléchargé, sélectionnez ce dernier et cliquez sur **Open**.
6. Cliquez sur **OK**.

   Une boîte de dialogue de progression de téléchargement s'affiche. Au terme du téléchargement, le fichier téléchargé (portant l'extension .rpm) s'affiche dans la liste intitulée Upgrade Packages Available on Data Domain System.
7. Pour vérifier l'intégrité du module de mise à niveau, cliquez sur **View Checksum** et comparez le checksum calculé affiché dans la boîte de dialogue au checksum faisant autorité présent sur le site de support en ligne.
8. Pour activer manuellement la vérification préalable à une mise à niveau, sélectionnez un module de mise à niveau et cliquez sur **Upgrade Precheck**.

Mise à niveau d'un système Data Domain

Lorsque le fichier d'un module de mise à niveau est présent sur le système, vous pouvez faire appel à DD System Manager pour effectuer une mise à niveau à l'aide de ce module de mise à niveau.

Avant de commencer

Lisez les notes de mise à jour de DD OS pour obtenir des instructions de mise à niveau complètes et des solutions à tous les problèmes qui peuvent avoir un impact sur la mise à niveau.

La procédure qui suit décrit comment démarrer une mise à niveau à l'aide de DD System Manager. Déconnectez-vous des sessions CLI Data Domain sur le système où la mise à niveau doit être effectuée avant d'utiliser DD System Manager pour mettre à niveau le système.

Remarque

Les fichiers du module de mise à niveau portent l'extension de fichier .rpm. Cette section suppose que vous mettez à jour uniquement DD OS. Si vous apportez des modifications matérielles, telles que l'ajout, l'échange ou le déplacement des cartes d'interface, vous devez mettre à jour la configuration de DD OS afin de refléter les modifications du matériel.

Procédure

1. Connectez-vous à DD System Manager sur le système sur lequel la mise à niveau doit être effectuée.

   Remarque

   Pour la plupart des versions, les mises à niveau sont autorisées au maximum pour deux versions précédentes d'une version majeure. Pour la version 6.0, les mises à niveau sont autorisées à partir des versions 5.6 et 5.7.

   Remarque

   Comme recommandé dans les notes de mise à jour, redémarrez le système Data Domain avant la mise à niveau pour vérifier que le matériel est dans un état Clean. Si des problèmes sont détectés lors du redémarrage, résolvez-les avant de démarrer la mise à niveau. Dans le cas d'une mise à niveau MDU, il est possible que le redémarrage ne soit nécessaire.

2. Sélectionnez **Data Management** > **File System** et assurez-vous que le système de fichiers est activé et s'exécute.
3. Sélectionnez **Maintenance** > **System**.
4. Dans la liste Upgrade Packages Available on Data Domain System, sélectionnez le module à utiliser pour la mise à niveau.

   Remarque

   Vous devez sélectionner un module de mise à niveau pour la toute dernière version de DD OS. DD OS ne prend pas en charge une rétrogradation vers des versions antérieures.

5. Cliquez sur **Perform System Upgrade**.

   La boîte de dialogue System Upgrade apparaît. Elle affiche des informations sur la mise à niveau, ainsi qu'une liste des utilisateurs actuellement connectés au système à mettre à niveau.

6. Vérifiez la version du module de mise à niveau, puis cliquez sur **OK** pour poursuivre la mise à niveau.

   La boîte de dialogue System Upgrade indique l'état de la mise à niveau et le temps restant.

   Lors de la mise à niveau du système, vous devez attendre que la mise à niveau soit terminée avant d'utiliser DD System Manager pour gérer le système. Si le système redémarre, la mise à niveau peut se poursuivre après le redémarrage et DD System Manager affiche l'état de la mise à niveau une fois la connexion établie. Si possible, gardez la boîte de dialogue System Upgrade ouverte jusqu'à la fin de la mise à niveau ou jusqu'à la mise hors tension du système. Lorsque

vous mettez à niveau DD OS version 5.5 ou une version supérieure vers une version récente et si la mise à niveau du système ne requiert pas une mise hors tension, un lien de connexion s'affiche lorsque la mise à niveau est terminée.

Remarque

Pour afficher l'état d'une mise à niveau à l'aide de l'interface de ligne de commande, saisissez la commande `system upgrade status`. Les messages de log pour la mise à niveau sont stockés dans `/ddvar/log/debug/platform/upgrade-error.log` et `/ddvar/log/debug/platform/upgrade-info.log`.

7. Si le système se met hors tension, vous devez retirer l'alimentation CA du système pour supprimer la configuration précédente. Débranchez tous les câbles d'alimentation pendant 30 secondes, puis rebranchez-les. Le système se met sous tension et redémarre.
8. Si le système ne se met pas automatiquement sous tension et qu'un bouton d'alimentation est présent sur le panneau avant, appuyez sur ce bouton.

À effectuer

Les conditions suivantes peuvent s'appliquer après avoir terminé une mise à niveau.

- Pour les environnements utilisant des certificats SHA-256 auto-signés, les certificats doivent être régénérés manuellement une fois le processus de mise à niveau terminé. Une relation de confiance doit, par ailleurs, être rétablie avec les systèmes externes qui se connectent au système Data Domain.
  1. Exécutez la commande **`adminaccess certificate generate self-signed-cert regenerate-ca`** pour régénérer les certificats auto-signés AC et les certificats d'hôte. La régénération des certificats rompt les relations de confiance avec les systèmes externes.
  2. Exécutez la commande **`adminaccess trust add host`** ***`hostname`*** **`type mutual`** pour rétablir la relation de confiance mutuelle entre le système Data Domain et le système externe.
- Si le système affiche des ports FC existants ou configurés avec des informations WWPN ou WWNNN manquantes, ou signale qu'aucun pilote d'adaptateur de bus hôte FC (HBA) n'est installé, exécutez la commande `scsitarget endpoint enable all`.

Remarques sur la réplication

Avec la réplication de collection, aucun fichier n'est visible sur le système Data Domain de destination si la réplication n'était pas terminée avant le début de la mise à niveau. Après la mise à niveau, attendez que la réplication soit terminée pour voir les fichiers sur la destination.

Remarques sur ConnectEMC

Dans cette version, ConnectEMC a été modifié pour prendre en charge la passerelle Secure Remote Service Virtual Edition (Secure Remote Services VE). Cette modification nécessite une reconfiguration du système Data Domain pour ConnectEMC après la mise à niveau.

Remarque

ConnectEMC ne fonctionne qu'avec Service Remote Services VE (V3) et ne peut pas envoyer d'e-mails avec d'anciennes versions de Service Remote Services ou par ses propres moyens. Si ConnectEMC a été utilisé avec des versions antérieures de DD OS (par exemple, 5.7 ou 5.6), la configuration du serveur Service Remote Services VE doit être resaisie, car elle a été supprimée pendant le processus de mise à niveau en raison de la mise à niveau technologique.

Remarque

Si une passerelle Service Remote Services plus ancienne est utilisée, la passerelle Service Remote Services VE doit être implémentée pour permettre des communications sécurisées.

Pendant la mise à niveau, si ConnectEMC est détecté tel que configuré, la configuration existante est supprimée. En outre, si la méthode de notification de support est configurée comme étant ConnectEMC pour l'envoi de messages d'événements à l'entreprise, cette méthode passe au courrier électronique. Après la mise à niveau, vous pouvez reconfigurer ConnectEMC avec la nouvelle commande ConnectEMC : `support connectemc device register`.

Une fois ConnectEMC configuré, activez ConnectEMC avec `support notification method set connectemc`.

Suppression d'un module de mise à niveau

Cinq modules de mise à niveau au maximum peuvent être téléchargés sur un système avec DD System Manager. Si le système que vous mettez à niveau contient cinq modules de mise à niveau, vous devez supprimer au moins un module avant de pouvoir mettre à niveau son système.

Procédure

1. Sélectionnez **Maintenance** > **System**.
2. Dans la liste Upgrade Packages Available on Data Domain System, sélectionnez le module à supprimer. Vous ne pouvez supprimer qu'un module à la fois.
3. Cliquez sur **Remove Upgrade Package**.

Gestion des licences électroniques

Ajoutez et supprimez des licences électroniques à partir du système Data Domain. Reportez-vous aux *Notes de mises à jour de Data Domain Operating System* pour obtenir les informations les plus récentes au sujet des fonctionnalités des produits, des mises à jour logicielles, des guides de compatibilité logicielle et vous renseigner sur les produits, licences et services.

Gestion des licences du système haute disponibilité

La haute disponibilité est une fonction sous licence. En outre, la clé de licence du système est enregistrée en suivant la même procédure que celle utilisée pour ajouter n'importe quelle autre licence au système Data Domain.

Un système est configuré comme étant actif/passif, dans le cas où un nœud est désigné comme étant « en veille ». Un seul ensemble de licences est nécessaire, non

des licences individuelles pour chaque nœud. Lors du basculement sur incident, les licences valides pour un nœud basculeront sur l'autre nœud.

Gestion du stockage du système

Les fonctions de gestion du stockage du système vous permettent d'afficher l'état et la configuration de votre espace de stockage, d'utiliser la fonction de signalement par voyant clignotant pour faciliter l'identification des disques, et de changer la configuration du stockage.

Remarque

Tout le stockage qui est connecté ou utilisé par le système haute disponibilité comportant deux nœuds actifs/passifs peut être visualisé comme un seul système.

Utilisation de la CLI pour calculer l'espace de stockage utile

Les valeurs suivantes sont nécessaires pour calculer le stockage utile sur un système Data Domain après prise en compte du temps système RAID :

- *N*= nombre de disques utilisés dans le groupe de disques (dg).
- *C* = capacité de chaque disque après le formatage.
- *R* = 2 (nombre de disques utilisés pour la parité RAID 6)

Ce calcul ne fonctionne pas pour le stockage Cache Tier, car les disques Cache Tier ne sont pas protégés par RAID.

Exécutez la commande `storage show all` pour obtenir les valeurs *N* et *C*.

Figure 4 Exemple de commande `storage show all`

```
sysadmin@ddbeta90# storage show all
Active tier details:
Disk      Disks      Count   Disk       Additional
Group                        Size       Information
-------   --------   -----   --------   -----------
dg2       2.1-2.14   14      2.7 TiB
(spare)   2.15       1       2.7 TiB
-------   --------   -----   --------   -----------

Current active tier size: 32.7 TiB
Active tier maximum capacity: 131.0 TiB
```

Dans cet exemple, 14 disques sont utilisés dans dg2 et chaque disque a une capacité de 2,7 Tio, donc *N* = 14 et *C* = 2,7 Tio

Utilisez la formule (*N*-*R*) x *C* pour obtenir la capacité utile. Dans cet exemple, l'équation est (14-2) x 2,7 Tio.

12 x 2,7 Tio = 32,4 Tio ou 35,6 To.

Remarque

La valeur calculée peut ne pas correspondre exactement au résultat de la commande `storage show all` en raison de la façon dont les valeurs de capacité sont arrondies pour l'affichage. La commande `disk show hardware` affiche la volumétrie avec des décimales supplémentaires.

Affichage des informations sur le stockage du système

La zone d'état du stockage affiche l'état actuel du stockage, par exemple Operational ou Non-Operational, ainsi que l'état de migration du stockage. Sous la zone Status se trouvent les onglets qui organisent la façon dont l'inventaire du stockage est présenté.

Procédure

1. Pour afficher l'état du stockage, sélectionnez **Hardware** > **Storage**.
2. Si un lien Alerts s'affiche après l'état du stockage, cliquez sur le lien pour afficher les alertes du stockage.
3. Si l'état de Storage Migration Status est Not Licensed, vous pouvez cliquer sur **Add License** pour ajouter la licence pour cette fonction.

Onglet Overview

L'onglet Overview affiche des informations sur tous les disques du système Data Domain classés par type. Les catégories qui s'affichent dépendent du type de configuration du stockage utilisé.

Les stockages découverts sont répertoriés dans l'une ou plusieurs des sections suivantes.

- Active Tier
  Les disques du niveau Active sont ceux qui peuvent être utilisés par le système de fichiers Data Domain. Les disques sont répertoriés dans deux tableaux, Disks in Use et Disks Not in Use.
- Retention Tier
  Si la licence Data Domain Extended Retention (anciennement DD Archiver) est installée, cette section affiche les disques qui sont configurés pour le stockage DD Extended Retention. Les disques sont répertoriés dans deux tableaux, Disks in Use et Disks Not in Use.
- Cache Tier
  Les disques SSD du niveau Cache sont utilisés pour la mise en cache des métadonnées. Les disques SSD ne sont pas utilisables par le système de fichiers. Les disques sont répertoriés dans deux tableaux, Disks in Use et Disks Not in Use.
- Cloud Tier
  Les disques du niveau Cloud servent à stocker les métadonnées pour les données qui résident dans le stockage Cloud. Les disques ne sont pas utilisables par le système de fichiers. Les disques sont répertoriés dans deux tableaux, Disks in Use et Disks Not in Use.
- Addable Storage
  Pour les systèmes avec boîtiers en option, cette section affiche les disques et les boîtiers qui peuvent être ajoutés au système.
- Failed/Foreign/Absent Disks (à l'exclusion des disques système)
  Affiche les disques en état d'échec ; ces derniers ne peuvent pas être ajoutés aux niveaux Active ou Retention du système.
- Systems Disks
  Affiche les disques sur lesquels DD OS réside lorsque le contrôleur Data Domain ne contient pas de disques de stockage de données.
- Migration History
  Affiche l'historique des migrations.

Chaque en-tête de section affiche un récapitulatif du stockage configuré pour cette section. Le récapitulatif affiche le total des disques, disques utilisés, disques de

secours, disques de secours pour reconstruction, disques disponibles et disques connus.

Cliquez sur le bouton plus (+) d'une section pour afficher des informations détaillées ou cliquez sur le bouton moins (-) pour les masquer.

Tableau 24 Descriptions des libellés de la colonne Disks In Use

Élément	Description
Disk Group	Nom du groupe de disques qui a été créé par le système de fichiers (par exemple, dg1).
State	État du disque (par exemple Normal, Warning).
Disks Reconstructing	Disques qui subissent actuellement une reconstruction, par ID de disque (par exemple, 1.11).
Total Disks	Nombre total de disques utilisables (par exemple, 14).
Disks	ID des disques utilisables (par exemple, 2.1-2.14).
Size	Taille du groupe de disques (par exemple, 25,47 Tio).

Tableau 25 Descriptions des libellés de la colonne Disks Not In Use

Élément	Description
Disk	Identifiant du disque, qui peut être un des éléments suivants. • Le numéro de boîtier et de disque (au format Enclosure.Slot) • Le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk • Une LUN
Slot	Le boîtier dans lequel se trouve le disque.
Pack	La pile de disques, 1-4, à l'intérieur du châssis dans lequel se trouve le disque. Dans le cas des tiroirs d'extension DS60, cette valeur équivaut à 2-4.
State	État du disque, par exemple In Use, Available, Spare.
Size	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
Type	Connectivité et type de disque (par exemple, SAS).

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Onglet Enclosures

L'onglet Enclosures affiche un tableau récapitulatif des boîters connectés au système.

L'onglet Enclosures contient les détails suivants.

Tableau 26 Description des libellés des colonnes de l'onglet Enclosures

Élément	Description
Enclosure	Numéro du boîtier. Le boîtier 1 est l'unité de commande.
Serial Number	Numéro de série du boîtier.
Disks	Les disques contenus dans un boîtier, au format *<Enclosure-number>*.1-*<Enclosure-number>*.*<N>*.
Model	Modèle du boîtier. Pour le boîtier 1, le modèle est l'unité de commande.
Disk Count	Nombre de disques dans le boîtier.
Disk Size	Capacité de stockage de données du disque lorsqu'il est utilisé dans un système Data Domain.[a]
Failed Disks	Disques défaillants dans le boîtier.
Temperature Status	État de la température du boîtier.

a. La convention de Data Domain en matière de calcul de l'espace disque définit un gibioctet comme 230 octets, ce qui produit une capacité de disque différente de celle évaluée par le fabricant.

Onglet Disks

L'onglet Disks donne des indications sur chacun des disques du système. Vous pouvez filtrer les disques de façon à afficher tous les disques ou uniquement les disques d'un niveau spécifique ou d'un groupe donné.

Le tableau Disk State est un tableau récapitulatif sur l'état de tous les disques du système.

Tableau 27 Descriptions des libellés des colonnes du tableau Disk State

Élément	Description
Total	Nombre total de disques inventoriés dans le système Data Domain.
In Use	Nombre de disques actuellement utilisés par le système de fichiers.
Spare	Nombre de disques de secours (disponibles pour remplacer les disques en échec).
Spare (reconstructing)	Nombre de disques en cours de reconstruction de données (disques de secours remplaçant des disques en échec).
Available	Nombre de disques disponibles pour l'allocation vers un niveau de stockage actif (Active) ou DD Extended Retention.
Known	Nombre de disques non alloués connus.
Unknown	Nombre de disques non alloués inconnus.
Failed	Nombre de disques en échec.
Foreign	Nombre de disques étrangers.
Absent	Nombre de disques absents.

Tableau 27 Descriptions des libellés des colonnes du tableau Disk State (suite)

Élément	Description
Migrating	Nombre de disques sources d'une migration du stockage.
Destination	Nombre de disques cibles d'une migration du stockage.
Powered Off	Nombre de disques non alimentés.
Not Installed	Nombre de slots de disque vides que le système peut détecter.

Le tableau Disks affiche des informations spécifiques sur chaque disque installé dans le système.

Tableau 28 Descriptions des libellés des colonnes du tableau Disks

Élément	Description
Disk	Identifiant du disque, qui peut être : • le numéro du châssis et du disque (au format *Enclosure Slot*) ; • le numéro de périphérique d'un périphérique logique comme ceux utilisés par DD VTL et vDisk ; • une LUN.
Size	Taille du disque .
Slot	Le boîtier dans lequel se trouve le disque.
Pack	La pile de disques, 1-4, à l'intérieur du châssis dans lequel se trouve le disque. Dans le cas des tiroirs d'extension DS60, cette valeur équivaut à 2-4.
State	État du disque, qui peut être : • Absent. Aucun disque n'est installé à l'emplacement indiqué. • Available. Un disque est alloué au niveau actif ou au niveau de rétention, mais n'est pas en cours d'utilisation. • Copy Recovery. Le disque présente un taux élevé d'erreurs, mais n'est pas considéré comme défectueux. Le système RAID copie actuellement son contenu sur un disque de secours et déclarera le disque comme défectueux une fois la reconstruction de la copie terminée. • Destination. Le disque est utilisé comme destination pour la migration du stockage. • Error. Le disque présente un taux élevé d'erreurs, mais n'est pas considéré comme défectueux. Le disque est en attente de reconstruction. Dès que la reconstruction commence, il passe à l'état de restauration de la copie (Copy Recovery). • Foreign. Le disque a été alloué à un niveau, mais selon les données du disque, il semblerait qu'il appartienne à un autre système.

Tableau 28 Descriptions des libellés des colonnes du tableau Disks (suite)

Élément	Description
	• In-Use. Le disque est actuellement utilisé pour stocker des données de sauvegarde. • Known. Le disque est pris en charge et prêt à être alloué. • Migrating. Le disque est utilisé comme source pour la migration du stockage. • Powered Off. Le disque a été mis hors tension par le support. • Reconstruction. Le disque est en cours de reconstruction en réponse à une commande `disk fail` ou aux indications du système RAID/SSM. • Spare. Le disque peut servir de disque de secours. • System. Les disques système servent à stocker les données du système et de DD OS. Vous ne pouvez pas y stocker des données de sauvegarde. • Unknown. L'allocation du disque au niveau actif ou au niveau de rétention a échoué, car il s'agit d'un disque inconnu. L'échec peut être lié à des raisons administratives ou imputable au système RAID.
Manufacturer/Model	Désignation du modèle du fabricant. L'affichage peut inclure un ID de modèle ou un type RAID ou d'autres informations selon la chaîne de fournisseur envoyée par la baie de stockage.
Firmware	Niveau du microprogramme utilisé par le contrôleur de stockage sur disque physique tiers.
Serial Number	Numéro de série du disque déterminé par le fabricant.
Disk Life Used	Pourcentage de la durée de vie nominale écoulée d'un disque SSD.
Type	Connectivité et type de disque (par exemple, SAS).

Onglet Reconstruction

L'onglet Reconstruction affiche un tableau contenant des informations supplémentaires sur la reconstruction des disques.

Le tableau suivant décrit les entrées du tableau Reconstructing.

Tableau 29 Descriptions des libellés des colonnes du tableau sur la reconstruction

Élément	Description
Disk	Identifie les disques en cours de reconstruction. Les libellés de disque sont au format *enclousre disk*. Le châssis 1 correspond au système Data Domain et la numérotation des tiroirs externes commence avec le châssis 2. Par exemple, le libellé 3.4 correspond au quatrième disque dans le deuxième tiroir.
Disk Group	Affiche le groupe RAID (dg#) du disque en cours de reconstruction.

Tableau 29 Descriptions des libellés des colonnes du tableau sur la reconstruction (suite)

Élément	Description
Tier	Nom du niveau auquel le disque en échec est en cours de reconstruction.
Time Remaining	Temps avant l'achèvement de la reconstruction.
Percentage Complete	Pourcentage de reconstruction effectué.

Lorsqu'un disque de secours est disponible, le système de fichiers remplace automatiquement un disque en échec par un disque de secours et démarre le processus de reconstruction pour intégrer le disque de secours au groupe de disques RAID. L'utilisation du disque affiche `Spare` et l'état devient `Reconstructing`. La reconstruction est exécutée sur un seul disque à la fois.

Recherche physique d'un châssis

Si vous avez des difficultés à déterminer quel châssis physique correspond à un châssis affiché dans DD System Manager, vous pouvez utiliser la fonctionnalité beacon de la CLI pour faire clignoter les voyants d'identification (IDENT) du châssis, ainsi que tous les voyants de disque indiquant un fonctionnement normal.

Procédure

1. Ouvrez une session CLI avec le système.
2. Saisissez `enclosure beacon`*enclosure*.
3. Appuyez sur `Ctrl+C` pour arrêter le clignotement.

Recherche physique d'un disque

Si vous avez des difficultés à déterminer les disques physiques qui correspondent à un disque affiché dans DD System Manager, vous pouvez utiliser la fonction de signalement par voyant clignotant sur le disque physique.

Procédure

1. Sélectionnez **Hardware** > **Storage** > **Disks**.
2. Sélectionnez un disque dans le tableau **Disks** et cliquez sur **Beacon**.

   Remarque

   Vous pouvez sélectionner un seul disque à la fois.

   La boîte de dialogue Beaconing Disk s'affiche et le voyant du disque se met à clignoter.

3. Cliquez sur **Stop** pour arrêter le signalement par voyant clignotant.

Configuration du stockage

Les fonctions de configuration du stockage permettent d'ajouter et de retirer des châssis d'extension des niveaux actif, rétention et Cloud. L'espace de stockage dans un châssis d'extension (qui est parfois appelé tiroir d'extension) n'est disponible qu'à condition d'être ajouté à un niveau.

Remarque

Pour avoir accès à un stockage supplémentaire, il convient de détenir la ou les licences appropriées et de disposer d'une quantité suffisante de mémoire pour gérer la nouvelle capacité de stockage. Des messages d'erreur s'affichent si plus de licences ou de mémoire sont nécessaires.

Les systèmes DD6300 permettent d'utiliser des châssis ES30 avec des disques de 4 To (43,6 Tio) à un taux d'utilisation de 50 % (soit 21,8 Tio) sur le niveau actif, si la capacité sous licence disponible correspond exactement à 21,8 Tio. Les directives suivantes s'appliquent à l'utilisation de tiroirs à capacité partielle.

- Les autres types de châssis ou les autres tailles de disque ne sont pas pris en charge dans le cadre d'une utilisation partielle de la capacité.
- Un tiroir partiel ne peut exister que sur le niveau actif.
- Un seul châssis ES30 partiel est permis dans le niveau actif.
- Une fois créé, aucun autre châssis ES30 ne peut être configuré sur ce niveau, tant que le tiroir partiel n'est pas ajouté à pleine capacité.

  Remarque

  La capacité supplémentaire sous licence doit être suffisante pour tirer parti des 21,8 Tio restants du tiroir partiel.

- Si la capacité disponible dépasse 21,8 To, il est impossible d'ajouter un tiroir partiel.
- La suppression d'une licence de 21 Tio ne permet pas de convertir automatiquement un tiroir entièrement utilisé en tiroir partiel. Le tiroir doit être retiré, puis rajouté en tant que tiroir partiel.

Procédure

1. Sélectionnez **Hardware** > **Storage** > **Overview**.
2. Développez la boîte de dialogue pour accéder à l'un des niveaux de stockage disponibles :
   - **Active Tier**
   - **Extended Retention Tier**
   - **Cache Tier**
   - **Cloud Tier**
3. Cliquez sur **Configure**.
4. Dans la boîte de dialogue Configure Storage, choisissez le stockage à ajouter à partir de la liste **Addable Storage**.
5. Dans la liste **Configure**, sélectionnez **Active Tier** ou **Retention Tier**.

   La quantité maximale de stockage pouvant être ajoutée au niveau actif dépend du contrôleur DD utilisé.

   Remarque

   La barre de la capacité sous licence affiche la partie de la capacité sous licence (utilisée et restante) pour les châssis installés.

6. Cochez cette case pour que le tiroir soit ajouté.

7. Cliquez sur le bouton **Add to Tier**.
8. Cliquez sur **OK** pour ajouter le stockage.

Remarque

Pour supprimer un tiroir ajouté, sélectionnez-le dans la liste Tier Configuration, cliquez sur **Remove from Configuration**, puis cliquez sur **OK**.

Extension de la capacité d'un système DD3300

Le système DD3300 est disponible en trois configurations de capacité différentes. Les extensions de la capacité d'une configuration à une autre sont prises en charge.

Le système DD3300 est disponible dans les configurations de capacité suivantes.

- 4 To
- 8 To
- 16 To
- 32 To

Les conditions de mise à niveau suivantes s'appliquent :

- Un système de 4 To peut être mis à niveau jusqu'à 16 To.
- Un système de 8 To peut être mis à niveau à 16 To, et de 16 To à 32 To.
- Un système de 16 To peut être mis à niveau jusqu'à 32 To.
- Il n'existe aucun chemin de mise à niveau à partir de 4 To vers 32 To.

Sélectionnez **Maintenance** > **System** pour accéder aux informations d'accès sur l'extension de la capacité et pour lancer le processus d'extension de la capacité.

L'extension de la capacité est un processus unique. Le volet **Capacity Expansion History** indique si le système a déjà été étendu. Si le système n'a pas été étendu, cliquez sur le bouton **Capacity Expand** pour lancer l'extension de la capacité.

Toutes les extensions de capacité nécessitent l'installation de disques et de mémoire supplémentaires dans le système. N'essayez pas d'augmenter la capacité tant que les mises à niveau matérielles ne sont pas terminées. Le tableau suivant indique la configuration matérielle requise pour la mise à niveau et l'extension de la capacité.

Tableau 30 Exigences de mise à niveau du DD3300 pour l'extension de capacité

Extension de la capacité	Mémoire supplémentaire	Disques durs supplémentaires	Disque SSD supplémentaire
Entre 4 et 16 To	32 Go	6 disques dur de 4 To	1 disque SSD de 480 Go
Entre 8 et 16 To	L'extension de 8 To à 16 To nécessite uniquement des modifications de licence et de configuration. Aucune mise à niveau matérielle n'est nécessaire.		
Entre 16 et 32 To	16 Go	6 disques dur de 4 To	s.o.

Le *Guide de mise à niveau et de remplacement sur site du système Data Domain DD3300* fournit des instructions détaillées pour étendre la capacité du système.

Extension de la capacité

Indiquez la capacité cible dans la liste déroulante **Select Capacity**. Une extension de la capacité peut être empêchée en cas de mémoire insuffisante, de capacité physique

insuffisante (disques durs), si le système a déjà été étendu ou si la cible de l'extension de la capacité n'est pas prise en charge. Si l'extension de la capacité ne peut pas être terminée, la raison s'affiche ici.

Historique de l'extension de la capacité

Le tableau **Capactiy Expansion History** affiche des informations sur la capacité du système. Le tableau fournit la capacité du système lorsque le logiciel a été installé pour la première fois, à la date de l'installation logicielle initiale. Si la capacité a été étendue, le tableau fournit également la capacité étendue et la date à laquelle l'extension a été effectuée.

Mettre en échec et annuler la mise en échec des disques

La fonction de mise en échec de disque vous permet de placer manuellement un disque à l'état d'échec de façon à forcer la reconstruction des données stockées sur le disque. La fonction d'annulation de mise en échec de disque vous permet de rétablir le fonctionnement d'un disque en état d'échec.

Mettre en échec un disque

Cette fonction permet de mettre un disque en échec et de forcer la reconstruction des données. Sélectionnez **Hardware** > **Storage** > **Disks** > **Fail**.

Sélectionnez un disque dans le tableau, puis cliquez sur **Fail**.

Annuler la mise en échec d'un disque

Cette fonction permet de rendre un disque précédemment marqué comme Failed ou Foreign, accessible au système. Sélectionnez **Hardware** > **Storage** > **Disks** > **Unfail**.

Sélectionnez un disque dans le tableau, puis cliquez sur **Unfail**.

Gestion des connexions réseau

Les fonctions de gestion des connexions réseau permettent d'afficher et de configurer les interfaces réseau, les paramètres réseau généraux et les routes du réseau.

Gestion des connexions réseau d'un système haute disponibilité

Le système haute disponibilité s'appuie sur deux types différents d'adresses IP : fixes et flottantes. Chaque type possède des limitations et des comportements spécifiques.

Sur un système haute disponibilité, les adresses IP fixes :

- Sont utilisées pour gérer les nœuds via la CLI ;
- Sont rattachées (« fixées ») au nœud ;
- Peuvent être statiques ou attribuées via DHCP, SLAAC IPv6.
- La configuration est effectuée sur le nœud spécifique avec l'argument facultatif `type fixed`.

Remarque

Tous les accès à un système de fichiers doivent s'effectuer par le biais d'une adresse IP flottante.

Les adresses IP flottantes existent uniquement dans le système haute disponibilité à deux nœuds. Pendant le basculement sur incident, les adresses IP « flottent » vers le nouveau nœud actif et sont :

- Uniquement configurées sur le nœud actif ;
- Utilisées pour l'accès au système de fichiers et à la majeure partie de la configuration.
- Elles peuvent uniquement être statiques.
- La configuration requiert l'argument `type floating`.

Gestion des interfaces du réseau

Les fonctions de gestion des interfaces du réseau permettent de gérer les interfaces physiques qui connectent le système à un réseau et de créer des interfaces logiques pour prendre en charge l'agrégation de liens, l'équilibrage de charge et le basculement de liaison ou de nœud sur incident.

Affichage des informations sur l'interface

L'onglet Interfaces permet de gérer les interfaces physiques et virtuelles, les réseaux VLAN, les serveurs DHCP, le mode DDNS, les adresses IP et les alias.

Tenez compte des consignes suivantes lors de la gestion des interfaces IPv6.

- L'interface de ligne de commande (CLI) prend en charge IPv6 pour les commandes de réseau et de réplication Data Domain de base, mais pas pour les commandes de sauvegarde et DD Extended Retention (`archive`). Les commandes CLI gèrent les adresses IPv6. Vous pouvez utiliser DD System Manager pour afficher les adresses IPv6, mais pas pour gérer IPv6.
- Les réplications de collection, de répertoire et de structure MTree sont prises en charge sur les réseaux IPv6, ce qui vous permet de tirer parti de l'espace d'adressage IPv6. Une réplication simultanée sur les réseaux IPv6 et IPv4 est également prise en charge, de même que la réplication de fichiers gérés à l'aide de DD Boost.
- Il existe quelques restrictions pour les interfaces avec des adresses IPv6. Par exemple, la MTU minimale est de 1 280. Si vous tentez de définir la MTU sur une valeur inférieure à 1 280 sur une interface dotée d'une adresse IPv6, un message d'erreur s'affiche et l'interface est supprimée du service. Une adresse IPv6 peut affecter une interface même si elle se trouve sur un réseau VLAN lié à l'interface et pas directement sur l'interface.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.

   Le tableau suivant décrit les informations relatives à l'onglet Interfaces.

   Tableau 31 Description des libellés de l'onglet Interface

Élément	Description
Interface	Nom de chaque interface associée au système sélectionné.
Enabled	Indique si l'interface est activée. • Sélectionnez **Yes** pour activer l'interface et la connecter au réseau.

Tableau 31 Description des libellés de l'onglet Interface (suite)

Élément	Description
	• Sélectionnez **No** pour désactiver l'interface et la déconnecter du réseau.
DHCP	Indique si l'interface est configurée manuellement (`no`), par un serveur IPv4 DHCP (Dynamic Host Configuration Protocol) (`v4`) ou par un serveur IPv6 DHCP (`v6`).
IP Address	Adresse IP associée à l'interface. Adresse utilisée par le réseau pour identifier l'interface. Si l'interface est configurée via DHCP, un astérisque s'affiche après cette valeur.
Netmask	Masque de réseau associé à l'interface. Utilise le format de masque de réseau IP standard. Si l'interface est configurée via DHCP, un astérisque s'affiche après cette valeur.
Link	Indique si la connexion Ethernet est active (Yes) ou non (No).
Address Type	Sur un système haute disponibilité, le type d'adresse indique s'il s'agit d'une adresse fixe, flottante ou d'une interconnexion.
Additional Info	Paramètres supplémentaires de l'interface. Par exemple, le mode de liaison.
IPMI interfaces configured	Affiche Yes ou No et indique si la surveillance de l'état de santé IPMI et la gestion de l'alimentation sont configurées pour l'interface.

2. Pour filtrer la liste d'interfaces par nom d'interface, saisissez une valeur dans le champ **Interface Name** et cliquez sur **Update**.

   Les filtres prennent en charge les caractères génériques, tels que eth*, veth* ou eth0*.

3. Pour filtrer la liste d'interfaces par type d'interface, sélectionnez une valeur dans le menu **Interface Type** et cliquez sur **Update**.

   Sur un système haute disponibilité, il existe un menu déroulant dont l'objectif est de filtrer en fonction du type d'adresse IP (fixe, flottante ou interconnexion).

4. Pour réinitialiser le tableau des interfaces à la liste par défaut, cliquez sur **Reset**.
5. Sélectionnez une interface dans le tableau pour renseigner la zone Interface Details.

Tableau 32 Description des libellés des détails de l'interface

Élément	Description
Auto-generated Addresses	Affiche les adresses IPv6 automatiquement générées pour l'interface sélectionnée.
Auto Negotiate	Lorsque cette fonction affiche `Enabled`, l'interface négocie automatiquement les paramètres Speed et Duplex. Lorsque cette fonction affiche `Disabled`, les paramètres Speed et Duplex doivent être définis manuellement.
Cable	Indique si l'interface est de type cuivre ou fibre.

Tableau 32 Description des libellés des détails de l'interface (suite)

Élément	Description
	Remarque Certaines interfaces doivent être activées pour que l'état du câble soit valide.
Duplex	Utilisé en conjonction avec la valeur Speed pour définir le protocole de transfert de données. Les options sont Unknown, Full, Half.
Hardware Address	Adresse MAC de l'interface sélectionnée. Par exemple, 00:02:b3:b0:8a:d2.
Interface Name	Nom de l'interface sélectionnée.
Latent Fault Detection (LFD) : systèmes HA uniquement	Le champ LFD possède un lien `View Configuration` affichant une fenêtre contextuelle qui répertorie les adresses et les interfaces LFD.
Maximum Transfer Unit (MTU)	Valeur MTU attribuée à l'interface.
Speed	Utilisé en conjonction avec la valeur Duplex pour définir le débit du transfert de données. Les options sont Unknown, 10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gb/s.
	Remarque Les interfaces automatiquement négociées doivent être installées avant que la vitesse, le mode duplex et la vitesse prise en charge ne soient visibles.
Supported Speeds	Répertorie toutes les vitesses pouvant être utilisées par l'interface.

6. Pour afficher les options de configuration et de gestion des interfaces IPMI, cliquez sur **View IPMI Interfaces**.

   Ce lien affiche les informations **Maintenance** > **IPMI**.

Noms et limites des interfaces physiques

Le format des noms des interfaces physiques varie en fonction des systèmes Data Domain et des cartes en option, et des limites s'appliquent à certaines interfaces.

- Pour la plupart des systèmes, le format du nom de l'interface physique est `eth`*xy*, où *x* correspond au numéro du slot pour un port intégré ou une carte en option et *y* à une chaîne alphanumérique. Par exemple, eth0a.
- Pour la plupart des interfaces verticales avec carte réseau intégrées, l'interface supérieure est nommée eth0a et l'interface inférieure eth0b.
- Pour la plupart des interfaces horizontales avec carte réseau intégrées, l'interface de gauche (vue de l'arrière) est nommée eth0a et celle de droite eth0b.
- Les systèmes DD990 fournissent quatre interfaces intégrées : deux en haut et deux en bas. L'interface située en haut à gauche est nommée eth0a, celle située en haut à droite est nommée eth0b, celle située en bas à gauche est nommée eth0c et celle située en bas à droite est nommée eth0d.

- Les systèmes DD2200 fournissent quatre ports intégrés pour carte réseau 1G Base-T : ethMa (en haut à gauche), ethMb (en haut à droite), ethMc (en bas à gauche) et ethMd (en bas à droite).
- Les systèmes DD2500 fournissent six interfaces intégrées. Les quatre ports de carte réseau 1 G Base-T intégrés sont nommés ethMa (en haut à gauche) ethMb (en haut à droite), ethMc (en bas à gauche) et ethMd (en bas à droite). Les deux ports de carte réseau 10 G Base-T intégrés sont nommés ethMe (en haut) et ethMf (en bas).
- Les systèmes DD4200, DD4500 et DD7200 fournissent un port Ethernet intégré, nommé ethMa.
- Pour les systèmes entre DD140 et DD990, les noms d'interface physique pour les modules d'E/S débutent en haut du module ou à gauche. La première interface est ethxa, la suivante est ethxb, puis ethxc, etc.
- Sur les modules d'E/S DD2500 horizontaux, les ports sont numérotés dans l'ordre à partir de l'extrémité opposée à la poignée du module (à gauche). Le premier port a le numéro 0 et correspond à l'interface physique nommée ethxa ; la suivante est nommée 1/ethxb, puis 2/ethxc, etc.
- Sur les modules d'E/S DD4200, DD4500 et DD7200 verticaux, les ports sont numérotés dans l'ordre à partir de l'extrémité opposée à la poignée du module (en bas). Le premier port a le numéro 0 et correspond à l'interface physique nommée ethxa ; la suivante est nommée 1/ethxb, puis 2/ethxc, etc.

Instructions générales de configuration d'une interface

Lisez les instructions générales de configuration d'une interface avant de configurer les interfaces du système.

- Lorsque des trafics de sauvegarde et de réplication doivent être pris en charge, utilisez, si possible, des interfaces distinctes pour chaque type de trafic afin qu'aucun des deux types de trafic n'ait un impact négatif sur l'autre.
- Lorsque le trafic de réplication attendu est inférieur à 1 Gbit/s, n'utilisez pas, si possible, des interfaces 10 GbE pour le trafic de réplication, car ces interfaces sont optimisées pour un trafic plus rapide.
- Si un service Data Domain utilise un port non standard et que l'utilisateur souhaite effectuer une mise à niveau vers DD OS 6.0 ou modifier un service en vue d'utiliser un port non standard sur un système DD OS 6.0, ajoutez une fonction de filtre de réseau pour tous les clients à l'aide de ce service afin que les adresses IP du client puissent tirer parti du nouveau port.
- Sur les systèmes DD4200, DD4500 et DD7200 qui utilisent IPMI, réservez, si possible, l'interface ethMa pour le trafic IPMI et le trafic de gestion du système (via des protocoles tels que HTTP, Telnet et SSH). Quant au trafic des données de sauvegarde, il doit être dirigé vers d'autres interfaces.

Configuration des interfaces physiques

Vous devez configurer au moins une interface physique pour que le système puisse se connecter à un réseau.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Sélectionnez l'instance à configurer.

Remarque

Les systèmes DD140, DD160, DD610, DD620 et DD630 ne prennent pas en charge IPv6 sur l'interface eth0a (eth0 sur les systèmes qui utilisent des noms de port hérités) ou sur aucun des réseaux VLAN créés sur cette interface.

3. Cliquez sur **Configure**.
4. Dans la boîte de dialogue Configure Interface, déterminez la façon dont l'adresse IP de l'interface doit être spécifiée :

Remarque

Sur un système haute disponibilité, la boîte de dialogue Configure Interface contient un champ pour désigner ou non l'adresse IP flottante (Yes/No). La sélection de **Yes** sélectionne automatiquement le bouton radio `Manually Configure IP Address`. Les interfaces IP flottantes peuvent uniquement être configurées manuellement.

- Use DHCP to assign the IP address : dans la zone IP Settings, sélectionnez **Obtain IP Address using DHCP**, puis choisissez **DHCPv4** pour un accès IPv4 ou **DHCPv6** pour un accès IPv6.
  La définition d'une interface physique pour utiliser DHCP active automatiquement l'interface.

  Remarque

  Si vous choisissez d'obtenir les paramètres réseau via le protocole DHCP, vous pouvez configurer manuellement le nom d'hôte via **Hardware** > **Ethernet** > **Settings** ou à l'aide de la commande `net set hostname`. Vous devez configurer manuellement le nom d'hôte lors de l'utilisation de DHCP via IPv6.

- Specify IP Settings manually : dans la zone IP Settings, sélectionnez **Manually configure IP Address**.
  Les champs **IP Address** et **Netmask** deviennent actifs.

5. Si vous avez choisi de saisir manuellement l'adresse IP, saisissez une adresse IPv4 ou IPv6. Si vous avez saisi une adresse IPv4, saisissez une adresse de masque de réseau.

Remarque

Vous ne pouvez attribuer qu'une seule adresse IP à une interface à l'aide de cette procédure. Même si vous attribuez une autre adresse IP, la nouvelle adresse remplace l'ancienne adresse. Pour associer une adresse IP supplémentaire à une interface, créez un alias IP.

6. Spécifiez les paramètres Speed/Duplex.

   La combinaison des paramètres de vitesse et de duplex définit le débit du transfert de données sur l'interface. Sélectionnez l'une des options suivantes :

   - **Autonegotiate Speed/Duplex** : cette option permet à la carte d'interface réseau de négocier automatiquement la vitesse de transmission et le duplex de l'interface. La négociation automatique *n'est pas* prise en charge sur les modules d'E/S DD2500, DD4200, DD4500 et DD7200 suivants :

- Carte optique SR 10 GbE double port avec connecteurs LC (utilisant des SFP)
- Carte en cuivre Direct Attach 10 GbE double port (câbles SFP+)
- Carte en cuivre à 4 ports dont 2 ports 1 GbE (RJ45)/carte optique SR 1 GbE double port

- **Manually configure Speed/Duplex** : cette option permet de définir manuellement le débit de transfert de données de l'interface. Sélectionnez la vitesse et le duplex dans les menus.
  - Il existe deux options pour le mode duplex : Half-duplex, Full-duplex et Unknown.
  - Les options de vitesse répertoriées sont limitées par les capacités du matériel. Les options disponibles sont 10 Mbit, 100 Mbit, 1 000 Mbit (1 Gbit), 10 Gbit et Unknown. Le matériel 10 G Base-T ne prend en charge que les paramètres 100 Mbit, 1000 Mbit et 10 Gbit.
  - L'option Half-duplex n'est disponible que pour les vitesses de transmission 10 Mbit et 100 Mbit.
  - Les vitesses de transmission de 1000 Mbit et 10 Gbit nécessitent le mode Full-duplex.
  - Sur les modules d'E/S 10 GbE DD2500, DD4200, DD4500 et DD7200, les interfaces en cuivre ne prennent en charge que la vitesse 10 Gbit.
  - Le paramètre par défaut pour les interfaces 10 G Base-T est Autonegotiate Speed/Duplex. Si vous définissez manuellement la vitesse sur 1000 Mbit ou 10 Gbit, vous devez définir le paramètre Duplex sur Full-duplex.

7. Spécifiez la taille de la MTU (Maximum Transfer Unit) pour l'interface physique (Ethernet).

   Effectuez ce qui suit :

   - Cliquez sur le bouton **Default** pour réinitialiser ce paramètre à la valeur par défaut.
   - Assurez-vous que tous vos composants réseau prennent en charge la valeur définie ici.

8. Vous pouvez, si vous le souhaitez, sélectionner **Dynamic DNS Registration**.

   Dynamic DNS (DDNS) est un protocole qui enregistre les adresses IP locales sur un serveur DNS (Domain Name System). Dans cette version, DD System Manager prend en charge le mode DDNS Windows. Pour utiliser le mode DDNS UNIX, utilisez la commande CLI `net ddns`.

   Pour que cette option puisse être utilisée, le DDNS doit être enregistré.

   Remarque

   Cette option désactive DHCP pour cette interface.

9. Cliquez sur **Next**.

   La page Configure Interface Settings Summary s'affiche. Les valeurs répertoriées reflètent l'état actualisé du système et des interfaces, qui est appliqué lorsque vous cliquez sur Finish.

10. Cliquez sur **Finish**, puis sur **OK**.

Valeurs de taille de la MTU

Il est important de définir correctement la taille de la MTU pour optimiser les performances d'une connexion réseau. En effet, une taille de MTU incorrecte peut nuire aux performances de l'interface.

Les valeurs prises en charge pour définir la taille d'une MTU pour l'interface (Ethernet) physique sont comprises entre 350 et 9 000. Dans le cas d'un réseau Gigabit ou 100 Base-T, la valeur par défaut est de 1 500.

Remarque

La MTU minimale pour les interfaces IPv6 est de 1 280. L'interface échoue si vous essayez de définir la valeur MTU sur une valeur inférieure à 1 280.

Déplacement d'une adresse IP statique

Une adresse IP statique spécifique ne doit être attribuée qu'à une seule interface sur un système. Il est nécessaire de supprimer correctement une adresse IP statique d'une interface avant de la configurer sur une autre interface.

Procédure

1. Si l'interface qui héberge l'adresse IP statique fait partie d'un groupe d'interfaces DD Boost, supprimez l'interface de ce groupe.
2. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
3. Supprimez l'adresse IP statique que vous souhaitez déplacer.
   a. Sélectionnez l'interface qui utilise actuellement l'adresse IP que vous souhaitez déplacer.
   b. Dans la colonne Enabled, sélectionnez **No** pour désactiver l'interface.
   c. Cliquez sur **Configure**.
   d. Définissez l'adresse IP sur 0.

      Remarque

      Définissez l'adresse IP sur 0 s'il n'y a pas d'autre adresse IP à attribuer à l'interface. La même adresse IP ne doit pas être attribuée à plusieurs interfaces.

   e. Cliquez sur **Next**, puis sur **Finish**.
4. Ajoutez l'adresse IP statique supprimée à une autre interface.
   a. Sélectionnez l'interface vers laquelle vous souhaitez déplacer l'adresse IP.
   b. Dans la colonne Enabled, sélectionnez **No** pour désactiver l'interface.
   c. Cliquez sur **Configure**.
   d. Définissez l'adresse IP pour qu'elle corresponde à l'adresse IP statique que vous avez supprimée.
   e. Cliquez sur **Next**, puis sur **Finish**.
   f. Dans la colonne Enabled, sélectionnez **Yes** pour activer l'interface mise à jour.

Recommandations sur la configuration de l'interface virtuelle

Les instructions de configuration de l'interface virtuelle s'appliquent aux interfaces virtuelles de basculement sur incident et d'agrégation. Il existe d'autres consignes pour l'une ou l'autre de ces interfaces (mais pas les deux).

- Le nom *virtual-name* doit respecter le format `veth`*x* où *x* représente un nombre. Le nombre maximal recommandé est 99 en raison des limites appliquées à la taille des noms.
- Vous pouvez créer autant d'interfaces virtuelles qu'il y a des interfaces physiques.
- Chaque interface utilisée dans une interface virtuelle doit d'abord être désactivée. Une interface qui fait partie d'une interface virtuelle est considérée comme désactivée pour les autres options de configuration du réseau.
- Lorsqu'une interface virtuelle est détruite, les interfaces physiques qui lui sont associées restent désactivées. Vous devez réactiver manuellement les interfaces physiques.
- Le nombre et le type de cartes installées déterminent le nombre de ports Ethernet disponibles.
- Chaque interface physique ne peut appartenir qu'à une seule interface virtuelle.
- Un système peut prendre en charge plusieurs interfaces virtuelles mixtes d'agrégation et de basculement, sous réserve des précédentes restrictions.
- Les interfaces virtuelles doivent être créées à partir d'interfaces physiques identiques. Par exemple, toutes de type cuivre, optique, 1 Gbit ou 10 Gbit. Toutefois, les interfaces 1 Gbit prennent en charge la liaison d'un mélange d'interfaces de types cuivre et optique. Cela s'applique aux interfaces virtuelles sur différentes cartes ayant des interfaces physiques identiques, à l'exception des cartes Chelsio. Pour les cartes Chelsio, seul le basculement sur incident est pris en charge, et ce uniquement pour les interfaces figurant sur la même carte.
- Les liaisons de basculement et d'agrégation améliorent les performances et la résilience du réseau via l'utilisation de plusieurs interfaces réseau en parallèle, ce qui permet d'accroître la vitesse de liaison des liens agrégés et la fiabilité, par rapport à une interface unique.
- La fonction de suppression est disponible via le bouton **Configure**. Cliquez sur une interface virtuelle dans la liste des interfaces de l'onglet Interfaces, puis cliquez sur **Configure**. Dans la liste des interfaces de la boîte de dialogue, décochez la case correspondant à l'interface pour qu'elle soit supprimée de la liaison (basculement ou agrégation), puis cliquez sur **Next**.
- Dans le cas d'une interface liée, celle-ci est créée avec les esclaves restants en cas de défaillance du matériel prévu pour une interface esclave. En l'absence d'esclave, l'id d'interface liée est créée sans esclave. Cette défaillance matérielle liée aux esclaves génère des alertes gérées, une par esclave défaillant.

  Remarque

  L'alerte concernant un esclave défaillant disparaît une fois l'esclave en question retiré du système. Si un nouveau matériel est installé, les alertes disparaissent et l'interface liée utilise la nouvelle interface esclave après le redémarrage.

- Sur les systèmes DD3300, DD4200, DD4500 et DD7200, l'interface ethMa ne prend pas en charge le basculement sur incident ou l'agrégation de liens.

Recommandations relatives à la configuration d'une interface virtuelle en vue d'une agrégation de liens

L'agrégation de liens améliore les performances réseau et la résilience en utilisant une ou plusieurs interfaces réseau en parallèle, ce qui permet d'accroître la fiabilité et la vitesse de la liaison par rapport à une interface unique. Ces consignes permettent d'utiliser l'agrégation de liens de façon optimale.

- Les modifications apportées aux interfaces Ethernet désactivées vident la table de routage. Nous vous conseillons de ne modifier l'interface que pendant les périodes d'interruption pour maintenance programmée. Ensuite, reconfigurez les règles de routage et les passerelles.
- Activez l'agrégation sur une interface virtuelle existante en spécifiant les interfaces physiques et le mode, et en lui donnant une adresse IP.
- Les cartes Ethernet à port optique unique de 10 Gbit ne prennent pas en charge l'agrégation de liens.
- Les interfaces 1 GbE et 10 GbE ne peuvent pas être agrégées.
- Les interfaces en cuivre et optiques ne peuvent pas être agrégées.
- Sur les systèmes DD4200, DD4500 et DD7200, l'interface ethMA ne prend pas en charge l'agrégation de liens.

Recommandations relatives à la configuration d'une interface virtuelle en vue d'un basculement sur incident

Le basculement de liaison sur incident améliore la stabilité et les performances du réseau en identifiant les interfaces de secours pouvant prendre en charge le trafic sur le réseau lorsque l'interface principale est hors service. Ces consignes permettent d'utiliser le basculement de liaison sur incident de façon optimale.

- Une interface principale doit faire partie du basculement sur incident. Si une tentative de suppression de l'interface principale se produit lors d'un basculement sur incident, un message d'erreur apparaît.
- Lorsqu'une interface principale est utilisée dans une configuration de basculement sur incident, celle-ci doit être explicitement spécifiée et doit également être une interface liée à l'interface virtuelle. Si l'interface principale tombe en panne et que plusieurs interfaces sont toujours disponibles, l'interface suivante est sélectionnée de manière aléatoire.
- Toutes les interfaces d'une interface virtuelle doivent se trouver sur le même réseau physique. Tous les switches réseau utilisés par une interface virtuelle doivent se trouver sur le même réseau physique.
- Le nombre d'interfaces physiques recommandé pour le basculement sur incident est supérieur à un. Vous pouvez cependant configurer une interface principale et une ou plusieurs interfaces de basculement sur incident, sauf si vous utilisez les cartes suivantes :
  - Cartes Ethernet CX4 10 Gbit, qui sont limitées à une interface principale et une interface de basculement sur incident sur la même carte.
  - Cartes Ethernet optiques à un port 10 Gbit, qui ne peuvent pas être utilisées.
- Sur les systèmes DD4200, DD4500 et DD7200, l'interface ethMA ne prend pas en charge le basculement de liens sur incident.

Création d'une interface virtuelle

Créez une interface virtuelle pour prendre en charge l'agrégation de liens ou le basculement sur incident. L'interface virtuelle fait office de conteneur pour les liens à agréger ou à associer au basculement sur incident.

Création d’une interface virtuelle pour l’agrégation de liens

Créez une interface virtuelle (pour l’agrégation de liens) à titre de conteneur afin d’associer les liens impliqués dans l’agrégation.

Ce type d’interface doit spécifier un mode de liaison et peut nécessiter la sélection d’un hachage. Vous pouvez, par exemple, activer une agrégation de liens sur une interface virtuelle *veth1* vers des interfaces physiques *eth1* et *eth2* en utilisant le mode LACP (Link Aggregation Control Protocol) et un hachage XOR-L2L3.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Dans le tableau Interfaces, désactivez l’interface physique sur laquelle l’interface virtuelle doit être ajoutée en cliquant sur **No** dans la colonne **Enabled**.
3. Dans le menu **Create**, sélectionnez **Virtual Interface**.
4. Dans la boîte de dialogue Create Virtual Interface, spécifiez un nom d’interface virtuelle dans la zone **veth**.

   Saisissez un nom d’interface virtuelle au format *vethx*, où *x* représente un ID unique (généralement à 1 ou 2 chiffres). *veth56.3999:199*, par exemple, est un nom d’interface virtuelle complet, avec VLAN et alias IP. Le nom complet ne peut comporter que 15 caractères maximum. Les caractères spéciaux ne sont pas autorisés, et les nombres doivent être compris entre 0 et 4 094, inclus.

5. Dans la liste **Bonding Type**, sélectionnnez **Aggregate**.

   Remarque

   La configuration du registre peut être différente de celle de la liaison. Lorsque vous ajoutez des interfaces à l’interface virtuelle, les informations ne sont pas envoyées au module de liaison tant que l’interface virtuelle n’a pas d’adresse IP et qu’elle n’est pas activée. En attendant, la configuration du registre et celle du pilote de liaison sont différentes.

6. Dans la liste **Mode**, sélectionnez un mode de liaison.

   Spécifiez le mode qui est compatible avec les exigences du système auquel les interfaces sont directement connectées.

   - Round-robin
     Les paquets sont transmis sur les interfaces de l’agrégat suivant le principe du tourniquet, c’est-à-dire tour à tour en commençant par le premier lien disponible jusqu’au dernier.
   - Balanced
     Les données envoyées sur les interfaces dépendent de la méthode de hachage sélectionnée. Les interfaces associées sur le switch doivent alors être regroupées dans une liaison EtherChannel (trunk) et se voir attribuer un hachage via le paramètre Load Balance.

- LACP
  Le mode LACP (Link Aggregation Control Protocol) est similaire au mode Balanced, à cette différence près qu'il utilise un protocole de contrôle qui communique avec l'autre extrémité et coordonne les liens pouvant être utilisés au sein de la liaison. Ce mode fournit une sorte de basculement sur incident pour les heartbeats et doit être configuré aux deux extrémités de la liaison.

7. Si vous avez sélectionné le mode Balanced ou LACP, spécifiez un type de hachage de liaison dans la liste **Hash**.

   Les options sont les suivantes : XOR-L2, XOR-L2L3 ou XOR-L3L4.

   XOR-L2 transmet via une interface liée avec un hachage XOR de couche 2 (adresses MAC entrantes et sortantes).

   XOR-L2L3 transmet via une interface liée avec un hachage XOR de couche 2 (adresses MAC entrantes et sortantes) et de couche 3 (adresses IP entrantes et sortantes).

   XOR-L3L4 transmet via une interface liée avec un hachage XOR de couche 3 (adresses IP entrantes et sortantes) et de couche 4 (ports entrants et sortants).

8. Pour sélectionner l'interface à ajouter à la configuration de l'agrégation, cochez la case correspondant à l'interface, puis cliquez sur **Next**.

   La boîte de dialogue Create virtual interface *veth_name* s'affiche.

9. Entrez une adresse IP, ou saisissez `0` pour ne définir aucune adresse IP.
10. Entrez une adresse de masque de réseau ou un préfixe.
11. Spécifiez les options Speed/Duplex.

    La combinaison des paramètres de vitesse et de duplex définit le débit du transfert de données sur l'interface. Sélectionnez :

    - **Autonegotiate Speed/Duplex**
      Cette option permet à la carte d'interface réseau de négocier automatiquement la vitesse de transmission et le duplex de l'interface.
    - **Manually configure Speed/Duplex**
      Cette option permet de définir manuellement le débit de transfert de données de l'interface.
      - Il existe deux options pour le mode duplex : Half-duplex et Full-duplex.
      - Les options de vitesse répertoriées sont limitées par les capacités du matériel. Les options disponibles sont 10 Mbit, 100 Mbit, 1 000 Mbit et 10 Gbit.
      - L'option Half-duplex n'est disponible que pour les vitesses de transmission 10 Mbit et 100 Mbit.
      - Les vitesses de transmission de 1000 Mbit et 10 Gbit nécessitent le mode Full-duplex.
      - Les interfaces optiques nécessitent l'option Autonegotiate.
      - La carte réseau de cuivre 10 GbE offre, par défaut, une vitesse de transmission de 10 Gbit. Si une interface cuivre est définie sur une vitesse de transmission de 1 000 Mbit ou 10 000 Gbit, le mode duplex doit être défini sur Full-duplex.

12. Spécifiez le paramètre MTU.
    - Cliquez sur **Default** pour afficher les valeurs par défaut (1500).
    - Pour sélectionner un paramètre différent, saisissez le paramètre dans la zone MTU. Assurez-vous que tous vos composants réseau prennent en charge la valeur définie ici.
13. Vous pouvez, si vous le souhaitez, sélectionner l'option Dynamic DNS Registration.

    Dynamic DNS (DDNS) est un protocole qui enregistre les adresses IP locales sur un serveur DNS (Domain Name System). Dans cette version, DD System Manager prend en charge le mode DDNS Windows. Pour utiliser le mode DDNS UNIX, utilisez la commande CLI `net ddns`.

    Pour que cette option puisse être utilisée, le DDNS doit être enregistré.
14. Cliquez sur **Next.**

    La page Configure Interface Settings Summary s'affiche. Les valeurs répertoriées reflètent l'état actualisé du système et des interfaces.
15. Cliquez sur **Finish**, puis sur **OK**.

Création d'une interface virtuelle pour le basculement de liaison sur incident

Créez une interface virtuelle (pour le basculement de liaison sur incident) à titre de conteneur afin d'associer les liens impliqués dans le basculement sur incident.

L'interface virtuelle activée pour les basculements sur incident représente un groupe d'interfaces secondaires, l'une d'entre elles pouvant être définie comme l'interface principale. Le système fait de l'interface principale l'interface active chaque fois qu'elle est opérationnelle. Une option de délai de basculement configurable vous permet de configurer un délai de basculement sur incident par intervalle de 900 millisecondes. Le délai de basculement sur incident permet de protéger un système contre de multiples basculements lorsqu'un réseau est instable.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Dans le tableau Interfaces, désactivez l'interface physique à laquelle l'interface virtuelle sera ajoutée en cliquant sur **No** dans la colonne **Enabled**.
3. Dans le menu **Create**, sélectionnez **Virtual Interface**.
4. Dans la boîte de dialogue Create Virtual Interface, spécifiez un nom d'interface virtuelle dans la zone **veth**.

   Saisissez un nom d'interface virtuelle au format `veth`*x*, où *x* représente un ID unique (généralement à 1 ou 2 chiffres). *veth56.3999:199*, par exemple, est un nom d'interface virtuelle complet, avec VLAN et alias IP. Le nom complet ne peut comporter que 15 caractères maximum. Les caractères spéciaux ne sont pas autorisés, et les nombres doivent être compris entre 0 et 4 094, inclus.
5. Dans la liste **Bonding Type**, sélectionnnez **Failover**.
6. Sélectionnez une interface à ajouter à la configuration de basculement sur incident, puis cliquez sur **Next**. Les interfaces virtuelles d'agrégation peuvent être utilisées pour le basculement sur incident.

   La boîte de dialogue Create virtual interface *veth_name* s'affiche.

7. Entrez une adresse IP, ou saisissez `0` pour ne définir aucune adresse IP.
8. Entrez un masque de réseau ou un préfixe.
9. Spécifiez les options Speed/Duplex.

   La combinaison des paramètres de vitesse et de duplex définit le débit du transfert de données sur l'interface.

   - Sélectionnez **Autonegotiate Speed/Duplex** pour permettre à la carte d'interface réseau de négocier automatiquement la vitesse de transmission et le duplex de l'interface.
   - Sélectionnez **Manually configure Speed/Duplex** pour définir manuellement le débit de transfert de données de l'interface.
     - Il existe deux options pour le mode duplex : Half-duplex et Full-duplex.
     - Les options de vitesse répertoriées sont limitées par les capacités du matériel. Les options disponibles sont 10 Mbit, 100 Mbit, 1 000 Mbit et 10 Gbit.
     - L'option Half-duplex n'est disponible que pour les vitesses de transmission 10 Mbit et 100 Mbit.
     - Les vitesses de transmission de 1000 Mbit et 10 Gbit nécessitent le mode Full-duplex.
     - Les interfaces optiques nécessitent l'option Autonegotiate.
     - L'interface cuivre par défaut offre une vitesse de transmission de 10 Gbit. Si une interface cuivre est définie sur une vitesse de transmission de 1 000 ou 10 000 Gbit, le mode duplex doit être défini sur Full-duplex.
10. Spécifiez le paramètre MTU.
    - Cliquez sur **Default** pour afficher la valeur par défaut (1500).
    - Pour sélectionner un paramètre différent, saisissez le paramètre dans la zone MTU. Assurez-vous que tous vos composants du chemin réseau prennent en charge la valeur définie ici.
11. Vous pouvez, si vous le souhaitez, sélectionner l'option Dynamic DNS Registration.

    Dynamic DNS (DDNS) est un protocole qui enregistre les adresses IP locales sur un serveur DNS (Domain Name System). Dans cette version, DD System Manager prend en charge le mode DDNS Windows. Pour utiliser le mode DDNS UNIX, utilisez la commande CLI `net ddns`.

    Pour que cette option puisse être utilisée, le DDNS doit être enregistré.

    Remarque

    Cette option désactive DHCP pour cette interface.
12. Cliquez sur **Next**.

    La page Configure Interface Settings Summary s'affiche. Les valeurs répertoriées reflètent l'état actualisé du système et des interfaces.
13. Renseignez toutes les valeurs relatives à l'interface, cliquez sur **Finish**, puis sur **OK**.

Modification d'une interface virtuelle

Après avoir créé une interface virtuelle, vous pouvez mettre à jour les paramètres pour répondre aux changements du réseau ou résoudre des problèmes.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Dans la colonne Interfaces, sélectionnez l'interface, puis désactivez l'interface virtuelle en cliquant sur **No** dans la colonne **Enabled**. Cliquez sur **OK** dans la boîte de dialogue d'avertissement.
3. Dans la colonne **Interfaces**, sélectionnez l'interface, puis cliquez sur **Configure**.
4. Dans la boîte de dialogue **Configure Virtual Interface**, modifiez les paramètres.
5. Cliquez sur **Next**, puis sur **Finish**.

Configuration d'un VLAN

Vous pouvez créer une nouvelle interface VLAN à partir d'une interface physique ou d'une interface virtuelle.

Le nombre total d'interfaces VLAN recommandé est de 80. Vous pouvez créer jusqu'à 100 interfaces (moins le nombre d'interfaces d'alias, physiques et virtuelles) avant que le système ne vous empêche d'en créer davantage.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Dans le tableau des interfaces, sélectionnez l'interface à laquelle vous souhaitez ajouter le réseau VLAN.

   L'interface sélectionnée doit être configurée avec une adresse IP pour vous permettre d'ajouter un réseau VLAN.
3. Cliquez sur **Create** et sélectionnez **VLAN**.
4. Dans la boîte de dialogue Create VLAN, spécifiez un ID de VLAN en saisissant un nombre dans la zone **VLAN Id**.

   Les valeurs d'ID de VLAN sont comprises entre 1 et 4 094 inclus.
5. Entrez une adresse IP, ou saisissez `0` pour ne définir aucune adresse IP.

   L'adresse IP (Internet Protocol) correspond à l'étiquette numérique attribuée à l'interface, par exemple : 192.168.10.23.
6. Entrez un masque de réseau ou un préfixe.
7. Spécifiez le paramètre MTU.

   Une MTU de VLAN doit être inférieure ou égale à la MTU définie pour l'interface physique ou virtuelle à laquelle elle est affectée. Si la MTU définie pour l'interface physique ou virtuelle de prise en charge est réduite en dessous de la valeur VLAN configurée, la valeur VLAN est automatiquement réduite pour correspondre à l'interface de prise en charge. Si la valeur de la MTU de l'interface de prise en charge est augmentée au-dessus de la valeur VLAN configurée, la valeur VLAN reste inchangée.

   - Cliquez sur **Default** pour afficher les valeurs par défaut (1500).
   - Pour sélectionner un paramètre différent, saisissez le paramètre dans la zone MTU. DD System Manager n'accepte pas une taille de MTU supérieure

à celle définie pour l'interface physique ou virtuelle à laquelle le réseau VLAN est affecté.

8. Spécifiez l'option Dynamic DNS Registration.

   Dynamic DNS (DDNS) est un protocole qui enregistre les adresses IP locales sur un serveur DNS (Domain Name System). Dans cette version, DD System Manager prend en charge le mode DDNS Windows. Pour utiliser le mode DDNS UNIX, utilisez la commande CLI `net ddns`.

   Pour que cette option puisse être utilisée, le DDNS doit être enregistré.

9. Cliquez sur **Next.**

   La page récapitulative **Create VLAN** s'affiche.

10. Vérifiez les paramètres de la configuration, puis cliquez sur **Finish** et **OK**.

Modification d'une interface VLAN

Après avoir créé une interface VLAN, vous pouvez mettre à jour les paramètres pour répondre aux changements du réseau ou résoudre des problèmes.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Dans la colonne **Interfaces**, cochez la case correspondant à l'interface et désactivez l'interface VLAN en cliquant sur **No** dans la colonne **Enabled**. Cliquez sur **OK** dans la boîte de dialogue Avertissement.
3. Dans la colonne Interfaces, cochez la case correspondant à l'interface, puis cliquez sur **Configure**.
4. Dans la boîte de dialogue **Configure VLAN Interface**, modifiez les paramètres.
5. Cliquez sur **Next**, puis sur **Finish**.

Configuration d'un alias IP

Un alias IP attribue une adresse IP supplémentaire à une interface physique, à une interface virtuelle ou à un VLAN.

Le nombre total recommandé d'interfaces d'alias IP, de réseau VLAN et virtuelles pouvant exister sur le système est de 80. Toutefois, il est possible d'avoir 100 interfaces au maximum. Vous remarquerez peut-être un ralentissement de l'affichage à mesure que vous approcherez de ce nombre maximal.

Remarque

Lorsque vous utilisez un système haute disponibilité Data Domain, si un utilisateur est créé et se connecte au nœud en veille sans se connecter d'abord au nœud actif, l'utilisateur n'aura pas un alias par défaut à utiliser. Par conséquent, pour pouvoir utiliser des alias sur le nœud en veille, l'utilisateur doit tout d'abord se connecter à un nœud actif.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Cliquez sur **Create** et sélectionnez **IP Alias**.

   La boîte de dialogue Create IP Alias s'affiche.

3. Spécifiez un ID d'alias IP en saisissant un nombre dans la zone **IP ALIAS Id**.

   La plage est comprise entre 1 et 4 094 inclus.

4. Saisissez une adresse IPv4 ou IPv6.
5. Si vous avez saisi une adresse IPv4, entrez une adresse de masque de réseau.
6. Spécifiez l'option Dynamic DNS Registration.

   Dynamic DNS (DDNS) est un protocole qui enregistre les adresses IP locales sur un serveur DNS (Domain Name System). Dans cette version, DD System Manager prend en charge le mode DDNS Windows. Pour utiliser le mode DDNS UNIX, utilisez la commande CLI `net ddns`.

   Pour que cette option puisse être utilisée, le DDNS doit être enregistré.

7. Cliquez sur **Next**.

   La page Create IP Alias Summary s'affiche.

8. Vérifiez les paramètres de la configuration, puis cliquez sur **Finish** et **OK**.

Modification d'une interface d'alias IP

Après avoir créé un alias IP, vous pouvez mettre à jour les paramètres pour répondre aux changements du réseau ou résoudre des problèmes.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Dans la colonne **Interfaces**, cochez la case de l'interface et désactivez l'interface d'alias IP en cliquant sur **No** dans la colonne **Enabled**. Cliquez sur **OK** dans la boîte de dialogue Avertissement.
3. Dans la colonne **Interfaces**, cochez la case de l'interface, puis cliquez sur **Configure**.
4. Dans la boîte de dialogue Configure IP alias, modifiez les paramètres comme décrit dans la procédure de création d'un alias IP.
5. Cliquez sur **Next**, puis sur **Finish**.

Enregistrement des interfaces via le protocole DDNS

Dynamic DNS (DDNS) est un protocole qui enregistre les adresses IP locales sur un serveur DNS (Domain Name System).

Dans cette version, DD System Manager prend en charge le mode DDNS Windows. Pour utiliser le mode DDNS UNIX, utilisez la commande CLI `net ddns`. Vous pouvez effectuer les opérations ci-après.

- Enregistrer manuellement (ajouter) des interfaces configurées à la liste des enregistrements DDNS.
- Supprimer des interfaces de la liste des enregistrements DDNS.
- Activer ou désactiver les mises à jour DNS.
- Indiquer si l'enregistrement DDNS est activé ou non.
- Afficher les interfaces dans la liste des enregistrements DDNS.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces** > **DDNS Registration**.

2. Dans la boîte de dialogue DDNS Windows Mode Registration, cliquez sur **Add** pour ajouter une interface à la liste des enregistrements DDNS.

   La boîte de dialogue Add Interface s'affiche.

   a. Entrez un nom dans le champ **Interface**.

   b. Cliquez sur **OK**.

3. Si vous le souhaitez, vous pouvez supprimer une interface de DDNS :

   a. Sélectionnez l'interface à supprimer, puis cliquez sur **Remove**.

   b. Dans la boîte de dialogue Confirm Remove, cliquez sur **OK**.

4. Spécifiez l'état DDNS.

   - Sélectionnez **Enable** afin d'activer les mises à jour pour toutes les interfaces déjà enregistrées.
   - Cliquez sur **Default** afin de sélectionner les paramètres par défaut pour les mises à jour DDNS.
   - Décochez la case **Enable** afin de désactiver les mises à jour DDNS pour les interfaces enregistrées.

5. Pour terminer l'enregistrement DDNS, cliquez sur **OK**.

Destruction d'une interface

Vous pouvez utiliser DD System Manager pour détruire ou supprimer des interfaces virtuelles, VLAN et d'alias IP.

Lorsqu'une interface virtuelle est détruite, le système la supprime, libère l'interface physique qui lui était associée et supprime tous les VLAN ou alias liés à l'interface virtuelle. Lorsque vous supprimez une interface VLAN, le système d'exploitation supprime le réseau VLAN et toutes les interfaces d'alias IP créées sous lui. Lorsque vous détruisez un alias IP, le système d'exploitation supprime uniquement cette interface d'alias.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces**.
2. Cochez la case en regard de chaque interface que vous souhaitez détruire (virtuelle, VLAN ou d'alias IP).
3. Cliquez sur **Destroy**.
4. Cliquez sur le bouton **OK** pour confirmer.

Affichage d'une hiérarchie d'interface dans l'arborescence

La boîte de dialogue Tree View affiche l'association entre les interfaces physiques et virtuelles.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Interfaces** > **Tree View**.
2. Dans la boîte de dialogue Tree View, sélectionnez les cases plus ou moins pour développer ou réduire l'arborescence affichant la hiérarchie.
3. Pour quitter cette vue, cliquez sur **Close**.

Gestion des paramètres réseau généraux

Les paramètres de configuration relatifs au nom d'hôte, au nom de domaine, aux domaines de recherche, au mappage d'hôtes et à la liste DNS sont gérés à partir de l'onglet Settings.

Affichage des informations sur les paramètres réseau

L'onglet Settings indique la configuration actuelle du nom d'hôte, du nom de domaine, des domaines de recherche, du mappage des hôtes et du DNS.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Settings**.

Résultats

L'onglet Settings affiche les informations ci-après.

Host Settings

Host Name
Nom d'hôte du système sélectionné.

Domain Name
Nom de domaine complet associé au système sélectionné.

Search Domain List

Search Domain
Liste des domaines de recherche utilisés par le système sélectionné. Le système applique le domaine de recherche comme un suffixe au nom d'hôte.

Hosts Mapping

IP Address
Adresse IP de l'hôte à résoudre.

Host Name
Noms d'hôte associés à l'adresse IP.

DNS List

DNS IP Address
Adresses IP du serveur DNS en cours associées au système sélectionné. Un astérisque (*) indique que les adresses IP ont été attribuées via DHCP.

Définition du nom d'hôte de DD System Manager

Vous pouvez configurer les noms d'hôte et de domaine DD System Manager manuellement, ou configurer DD OS pour recevoir automatiquement les noms d'hôte et de domaine à partir d'un serveur DHCP (Dynamic Host Configuration Protocol).

La configuration manuelle des noms d'hôte et de domaine présente un avantage : elle vous permet de supprimer la dépendance entre le serveur DHCP et l'interface conduisant au serveur DHCP. Pour minimiser les risques d'interruption de service, si possible, configurez manuellement les noms d'hôte et de domaine.

Lors de la configuration des noms d'hôte et de domaine, tenez compte des consignes suivantes :

- N'insérez pas de trait de soulignement dans le nom d'hôte ; ce caractère n'est pas compatible avec certains navigateurs.
- La réplication et l'authentification CIFS doivent être reconfigurées une fois les noms modifiés.
- Si un système a été précédemment ajouté sans nom complet (aucun nom de domaine), vous devez, pour modifier le nom de domaine, supprimer et ajouter le système concerné ou mettre à jour la liste des domaines de recherche afin d'inclure le nouveau nom de domaine.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Settings**.
2. Cliquez sur **Edit** dans la zone **Host Settings**. La boîte de dialogue Configure Host s'affiche.
3. Pour configurer manuellement les noms d'hôte et de domaine :
   a. Sélectionnez **Manually configure host**.
   b. Saisissez le nom d'hôte dans la zone **Host Name**.
      Par exemple, `id##.yourcompany.com`
   c. Saisissez un nom de domaine dans la zone **Domain Name**.
      Il s'agit du nom de domaine associé à votre système Data Domain et, en général, du nom de domaine de votre entreprise. Par exemple, *yourcompany.com*
   d. Cliquez sur **OK**.
      Le système affiche des messages de progression au fur et à mesure de la mise en œuvre des modifications.
4. Pour obtenir les noms d'hôte et de domaine d'un serveur DHCP, sélectionnez **Obtain Settings using DHCP**, puis cliquez sur **OK**.
   Au moins une interface doit être configurée pour utiliser DHCP.

Gestion de la liste de recherche de domaine

Utilisez la liste de recherche de domaine pour spécifier les domaines dans lesquels le système peut effectuer des recherches.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Settings**.
2. Cliquez sur **Edit** dans la zone Search Domain List.
3. Pour ajouter un domaine de recherche à l'aide de la boîte de dialogue Configure Search Domains :
   a. Cliquez sur Add (**+**).
   b. Dans la boîte de dialogue Add Search Domain, entrez un nom dans la zone **Search Domain**.
      Par exemple, `id##.yourcompany.com`
   c. Cliquez sur **OK**.

Le système ajoute le nouveau domaine à la liste des domaines pouvant faire l'objet d'une recherche.

d. Cliquez sur **OK** pour appliquer les modifications et revenir à la vue Settings.

4. Pour supprimer un domaine de recherche à l'aide de la boîte de dialogue Configure Search Domains :

a. Sélectionnez le domaine de recherche à supprimer.

b. Cliquez sur Delete (**X**).

Le système supprime le domaine sélectionné de la liste des domaines pouvant faire l'objet d'une recherche.

c. Cliquez sur **OK** pour appliquer les modifications et revenir à la vue Settings.

Ajout et suppression de mappages d'hôtes

Un mappage d'hôte associe une adresse IP à un nom d'hôte, de façon à pouvoir utiliser indifféremment l'adresse IP ou le nom d'hôte pour spécifier l'hôte.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Settings**.
2. Procédez comme suit pour ajouter un mappage d'hôte.

a. Dans la zone Hosts Mapping, cliquez sur **Add**.

b. Dans la boîte de dialogue Add Hosts, saisissez l'adresse IP de l'hôte dans la zone **IP Address**.

c. Cliquez sur le bouton d'ajout (**+**).

d. Dans la boîte de dialogue Add Host, saisissez un nom d'hôte dans la zone `Host Name`, tel que **id##.yourcompany.com**.

e. Cliquez sur **OK** pour ajouter le nouveau nom d'hôte à la liste Host Name.

f. Cliquez sur **OK** pour revenir à l'onglet Settings.

3. Pour supprimer un mappage d'hôte, procédez comme suit.

a. Dans la zone Hosts Mapping, sélectionnez le mappage d'hôte à supprimer.

b. Cliquez sur le bouton de suppression (**X**).

Configuration des adresses IP des serveurs DNS

Les adresses IP des serveurs DNS désignent les serveurs DNS sur lesquels le système peut obtenir les adresses IP pour les noms d'hôtes ne figurant pas dans la table de mappage des hôtes.

Vous pouvez configurer manuellement les adresses IP DNS ou configurer DD OS pour recevoir automatiquement les adresses IP d'un serveur DHCP. La configuration manuelle d'adresses IP DNS présente un avantage : elle vous permet de supprimer la dépendance entre le serveur DHCP et l'interface conduisant au serveur DHCP. Pour minimiser les risques d'interruption de service, EMC vous recommande de configurer manuellement les adresses IP DNS.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Settings**.
2. Cliquez sur **Edit** dans la zone DNS List.
3. Pour ajouter manuellement une adresse IP DNS :

a. Sélectionnez **Manually configure DNS list**.

Les cases d'adresse IP du serveur DNS deviennent actives.

b. Cliquez sur Add (**+**).

c. Dans la boîte de dialogue Add DNS, saisissez l'adresse IP DNS à ajouter.

d. Cliquez sur **OK**.

Le système ajoute la nouvelle adresse IP dans la liste des adresses IP du serveur DNS.

e. Cliquez sur **OK** pour appliquer les modifications.

4. Pour supprimer une adresse IP DNS dans la liste :

a. Sélectionnez **Manually configure DNS list**.

Les cases d'adresse IP du serveur DNS deviennent actives.

b. Sélectionnez l'adresse IP DNS à supprimer et cliquez sur Delete (**X**).

Le système supprime l'adresse IP de la liste des adresses IP du serveur DNS.

c. Cliquez sur **OK** pour appliquer les modifications.

5. Pour obtenir les adresses DNS auprès d'un serveur DHCP, sélectionnez **Obtain DNS using DHCP**, puis cliquez sur **OK**.

Au moins une interface doit être configurée pour utiliser DHCP.

Gestion des routes du réseau

Les routes définissent le chemin utilisé pour le transfert des données vers l'hôte local (le système Data Domain), ou depuis ce dernier vers un autre réseau ou hôte.

Les systèmes Data Domain ne génèrent ni ne répondent à aucun des protocoles de gestion du routage réseau (RIP, EGRP/EIGRP et BGP). Le seul routage implémenté sur un système Data Domain est basé sur des règles de routage IPv4, ce qui autorise une seule voie vers une passerelle par défaut par table de routage. Il peut y avoir plusieurs tables de routage et plusieurs passerelles par défaut. Une table de routage est créée pour chaque adresse possédant le même sous-réseau que la passerelle par défaut. Les règles de routage envoient les paquets avec l'adresse IP source qui correspond à l'adresse IP utilisée pour créer le tableau de cette table de routage. Tous les autres paquets dépourvus d'adresses IP source correspondant à une table de routage sont envoyés vers la table de routage principale.

Des routes statiques peuvent être ajoutées au sein de chaque table de routage, mais comme le routage source sert à envoyer des paquets vers la table, les seules routes statiques opérationnelles sont celles qui utilisent l'interface possédant l'adresse source de chaque table. Les autres devront être placées dans la table principale.

En plus du routage source IPv4 appliqué à ces autres tables de routage, les systèmes Data Domain utilisent un routage basé sur la source pour les tables de routage principales IPv4 et IPv6. Cela signifie que les paquets sortants correspondant au sous-réseau de plusieurs interfaces sont acheminés via l'interface physique (dont l'adresse IP correspond à l'adresse IP source des paquets), c'est-à-dire leur point d'origine.

Pour IPv6, configurez des routes statiques si plusieurs interfaces contiennent le même sous-réseau IPv6, et si les connexions sont établies vers les adresses IPv6 avec ce sous-réseau. Normalement, les routes statiques ne sont pas nécessaires avec les adresses IPv4 ayant le même sous-réseau, comme dans le cas de sauvegardes. Dans certains cas, des adresses statiques peuvent être requises pour permettre le fonctionnement des connexions, telles que les connexions du système Data Domain vers des systèmes distants.

Les routes statiques peuvent être ajoutées et supprimées à partir de tables de routage individuelles en ajoutant ou supprimant le table depuis la spécification du routage. Cela fournit les règles pour acheminer des paquets possédant des adresses source spécifiques via des tables de routage spécifiques. Si une route statique est requise pour les paquets avec ces adresses source, les routes doivent être ajoutées à la table spécifique vers laquelle l'adresse IP est acheminée.

Remarque

Le routage pour des connexions déclenchées par le système Data Domain, comme pour la réplication, dépend de l'adresse source utilisée pour les interfaces figurant sur le même sous-réseau. Pour forcer le trafic d'une interface spécifique vers une destination donnée (même si cette interface se trouve sur le même sous-réseau que les autres interfaces), configurez une entrée de routage statique entre les deux systèmes : ce routage statique remplace le routage source. Cela n'est pas nécessaire si l'adresse source est une adresse IPv4 et est associée à une passerelle par défaut. Dans ce cas, le routage source est déjà géré via sa propre table de routage.

Affichage des informations sur les routes

L'onglet Routes affiche les passerelles par défaut, les routes statiques et les routes dynamiques.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Routes**.

Résultats

La zone Static Routes répertorie la spécification de route utilisée pour configurer chaque route statique. Le tableau relatif aux routes dynamiques vous renseigne sur chacune des routes allouées de façon dynamique.

Tableau 33 Description des libellés des colonnes de routes dynamiques

Élément	Description
Destination	Hôte/réseau de destination auquel le trafic réseau (données) est envoyé.
Gateway	Adresse du routeur dans le réseau DD ou 0.0.0.0 si aucune passerelle n'est définie.
Genmask	Masque de réseau pour le réseau de destination. Définissez ce paramètre sur 255.255.255.255 pour une destination d'hôte et sur 0.0.0.0 pour la route par défaut.
Flags	Les valeurs possibles sont les suivantes : U : la route est active, H : la cible est un hôte, G : utiliser la passerelle, R : rétablir la route pour un routage dynamique, D : dynamiquement installé pour un processus ou rediriger, M : modifié par rapport au processus de routage ou rediriger, A : installé par addrconf, C : entrée de cache et ! : rejeter la route.
Metric	Distance à la cible (généralement comptée en hop). Cette option n'est pas utilisée par DD OS, mais peut être requise par les processus de routage.
MTU	Taille de l'unité de transmission maximale (MTU, Maximum Transfer Unit) pour l'interface physique (Ethernet).

Tableau 33 Description des libellés des colonnes de routes dynamiques (suite)

Élément	Description
Window	Taille de la fenêtre par défaut pour les connexions TCP établies via cette route.
IRTT	Temps d'aller-retour d'origine utilisé par le noyau pour estimer les meilleurs paramètres de protocole TCP sans attendre les réponses éventuellement lentes.
Interface	Nom de l'interface associé à l'interface de routage.

Définition de la passerelle par défaut

Vous pouvez configurer la passerelle par défaut manuellement ou configurer DD OS pour recevoir automatiquement les adresses IP de la passerelle par défaut d'un serveur DHCP.

La configuration manuelle de la passerelle par défaut présente un avantage : elle vous permet de supprimer la dépendance entre le serveur DHCP et l'interface conduisant au serveur DHCP. Pour minimiser les risques d'interruption de service, si possible, configurez manuellement l'adresse IP de la passerelle par défaut.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Routes**.
2. Cliquez sur **Edit** en regard du type de passerelle par défaut (IPv4 ou IPv6) à configurer.
3. Pour configurer manuellement l'adresse de la passerelle par défaut :
   a. Sélectionnez **Manually Configure**.
   b. Indiquez l'adresse de la passerelle dans la zone **Gateway**.
   c. Cliquez sur **OK**.
4. Pour obtenir l'adresse de la passerelle par défaut auprès d'un serveur DHCP, sélectionnez **Use DHCP value**, puis cliquez sur **OK**.

   Au moins une interface doit être configurée pour utiliser DHCP.

Création de routes statiques

Les routes statiques définissent les hôtes ou les réseaux de destination avec lesquels le système peut communiquer.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Routes**.
2. Cliquez sur **Create** dans la zone Static Routes.
3. Dans la boîte de dialogue **Create Routes**, sélectionnez l'interface qui hébergera la route statique, puis cliquez sur **Next**.
4. Spécifiez la destination.
   - Pour spécifier un réseau de destination, sélectionnez **Network**, puis entrez l'adresse réseau et le masque de réseau associés au réseau de destination.
   - Pour spécifier un hôte de destination, sélectionnez **Host**, puis entrez le nom d'hôte ou l'adresse IP de l'hôte de destination.

5. Vous pouvez, si vous le souhaitez, spécifier la passerelle à utiliser pour la connexion au réseau ou à l'hôte de destination.
   a. Sélectionnez **Specify a gateway for this route**.
   b. Indiquez l'adresse de la passerelle dans la zone **Gateway**.
6. Vérifiez la configuration, puis cliquez sur **Next**.

   La page Create Routes Summary s'affiche.
7. Cliquez sur **Finish**.
8. Une fois le processus terminé, cliquez sur **OK**.

   La nouvelle route apparaît dans la liste Route Spec.

Suppression de routes statiques

Supprimez une route statique pour empêcher le système de communiquer avec un hôte de destination ou un réseau.

Procédure

1. Sélectionnez **Hardware** > **Ethernet** > **Routes**.
2. Sélectionnez la spécification de route à supprimer dans la liste Route Spec.
3. Cliquez sur **Delete**.
4. Cliquez sur **Delete** pour confirmer, puis sur **Close**.

   La spécification de route sélectionnée est supprimée de la liste Route Spec.

Gestion des phrases de passe du système

La phrase de passe du système est une clé qui permet de transférer un système Data Domain sur le système à l'aide de clés de chiffrement. Les clés de chiffrement protègent les données alors que la phrase de passe du système protège les clés de chiffrement.

La phrase de passe du système est une clé lisible (compréhensible) par l'utilisateur (comme une carte à puce) qui est utilisée pour générer une clé de chiffrement AES 256 lisible par une machine. Si le système est volé durant les échanges, un pirate ne peut pas restaurer facilement les données ; au pire, il peut restaurer les données utilisateur et les clés chiffrées.

Cette phrase de passe est stockée en interne sur une partie masquée du sous-système de stockage Data Domain. Le système Data Domain peut ainsi démarrer et continuer à permettre l'accès aux données sans aucune intervention de l'administrateur.

Définition de la phrase de passe du système

La phrase de passe du système doit être définie pour que le système soit capable de prendre en charge le chiffrement des données ou de demander des certificats numériques.

Avant de commencer

Aucune longueur minimale n'est fixée pour la phrase de passe à l'installation de DD OS, mais la CLI offre une commande à cet effet. Pour déterminer si la phrase de passe doit respecter une longueur minimale, entrez la commande de CLI `system passphrase option show`.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.

   Si aucune phrase de passe n'est définie, le bouton **Set Passphrase** apparaît dans la zone Passphrase. Si une phrase de passe est définie, le bouton **Change Passphrase** apparaît pour que vous puissiez changer de phrase de passe, au besoin.

2. Cliquez sur le bouton **Set Passphrase**.

   La boîte de dialogue Set Passphrase s'affiche.

3. Saisissez la phrase de passe du système dans la zone prévue à cet effet et cliquez sur **Next**.

   Si une longueur minimale a été configurée pour la phrase de passe du système, veillez à respecter le nombre minimal de caractères requis.

Résultats

La phrase de passe du système est définie et le bouton **Change Passphrase** remplace le bouton **Set Passphrase**.

Modification de la phrase de passe du système

L'administrateur peut modifier la phrase de passe sans avoir à gérer les véritables clés de chiffrement. La modification de la phrase de passe change indirectement le chiffrement des clés, mais n'a pas d'incidence sur les données utilisateur ou sur la clé de chiffrement sous-jacente.

La modification de la phrase de passe nécessite l'authentification de deux utilisateurs pour empêcher toute destruction de données.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Pour modifier la phrase de passe du système, cliquez sur **Change Passphrase**.

   La boîte de dialogue Change Passphrase s'affiche.

   Remarque

   Le système de fichiers doit être désactivé pour modifier la phrase de passe. Si le système de fichiers est en cours d'exécution, vous êtes invité à le désactiver.

3. Dans les zones de texte, entrez :
   - Le nom d'utilisateur et le mot de passe d'un compte de responsable de la sécurité (un utilisateur autorisé dans le groupe Security User sur ce système Data Domain).
   - La phrase de passe actuelle lors de la modification de la phrase de passe.
   - La nouvelle phrase de passe qui doit être composée du nombre minimum de caractères configuré avec la commande `system passphrase option set min-length`.
4. Cochez la case **Enable file system now**.
5. Cliquez sur **OK**.

NOTE

Notez soigneusement la phrase de passe. En cas d'oubli, vous ne pourrez plus déverrouiller le système de fichiers ni accéder aux données ; les données seront irrémédiablement perdues.

Gestion de l'accès au système

Les fonctions de gestion de l'accès au système permettent de contrôler l'accès des utilisateurs d'une base de données locale ou d'un autre répertoire réseau. Différents contrôles supplémentaires sont proposés pour définir les niveaux d'accès et les protocoles susceptibles d'accéder au système.

Contrôle d'accès basé sur les rôles

Le contrôle d'accès basé sur les rôles (RBAC) est une stratégie d'authentification qui détermine les contrôles DD System Manager et les commandes de la CLI auxquels un utilisateur peut accéder sur un système.

Par exemple, les utilisateurs dotés du rôle *admin* peuvent configurer et surveiller l'ensemble d'un système, tandis que les utilisateurs dotés du rôle *user* peuvent seulement surveiller un système. Une fois connectés à DD System Manager, les utilisateurs ne voient que les fonctions du programme qu'ils sont autorisés à utiliser selon le rôle qui leur a été attribué. Les rôles suivants sont disponibles pour l'administration et la gestion de DD OS.

admin

Un utilisateur doté du rôle *admin* peut configurer et surveiller l'ensemble du système Data Domain. La plupart des fonctions et commandes de configuration ne sont disponibles que pour les utilisateurs dotés du rôle *admin*. Cependant, certaines fonctions et commandes nécessitent l'approbation d'un utilisateur doté du rôle *security* pour qu'une tâche soit exécutée.

limited-admin

Le rôle *limited-admin* permet de configurer et de surveiller le système Data Domain avec certaines limitations. Les utilisateurs auxquels ce rôle est attribué ne peuvent pas lancer des opérations de suppression de données, modifier le registre ou passer en mode bash ou SE.

user

Le rôle *user* permet aux utilisateurs de surveiller les systèmes et de modifier leur propre mot de passe. Les utilisateurs dotés du rôle de gestion *user* peuvent afficher l'état du système, mais ils ne peuvent pas modifier la configuration du système.

security (responsable de la sécurité)

Un utilisateur doté du rôle *security*, parfois appelé responsable de la sécurité, peut gérer d'autres responsables de la sécurité, autoriser des procédures nécessitant l'approbation d'un responsable de la sécurité et effectuer toutes les tâches prises en charge pour les utilisateurs dotés du rôle user.

Le rôle *security* est fourni conformément à la réglementation WORN (Write Once Read-Many). Cette réglementation nécessite que les données d'entreprise stockées au format électronique soient conservées dans leur état d'origine, non altéré à différentes fins telles que l'e-discovery. Data Domain a ajouté des options

d'audit et de consignation afin d'améliorer cette fonction. En raison des procédures de mise en conformité, la plupart des options de commande permettant de gérer les opérations sensibles, telles que DD Encryption, DD Retention Lock Compliance et l'archivage, nécessitent désormais l'approbation d'un responsable de la sécurité.

Dans un scénario type, un utilisateur doté du rôle *admin* émet une commande et, si l'approbation d'un responsable de sécurité est requise, le système affiche une invite pour approbation. Pour effectuer la tâche d'origine, le responsable de la sécurité doit saisir son nom d'utilisateur et son mot de passe sur la console où la commande a été exécutée. Si le système reconnaît ces informations d'identification, la procédure est autorisée. Dans le cas contraire, une alerte de sécurité est générée.

Voici quelques consignes qui s'appliquent aux utilisateurs dotés du rôle security :

- Seul l'utilisateur doté du rôle *sysadmin* (le rôle par défaut créé lors de l'installation de DD OS) peut créer le premier responsable de la sécurité, après quoi le privilège permettant de créer des responsables de la sécurité est retiré à l'utilisateur *sysadmin*.
- Une fois le premier responsable de la sécurité créé, seuls les responsables de la sécurité peuvent créer d'autres responsables de la sécurité.
- La création d'un responsable de la sécurité n'active pas la règle d'autorisation. Pour activer la règle d'autorisation, un responsable de la sécurité doit se connecter et l'activer.
- La séparation des privilèges et des responsabilités s'applique. Les utilisateurs dotés du rôle *admin* ne peuvent pas effectuer les tâches d'un responsable de la sécurité, et les responsables de la sécurité ne peuvent pas effectuer des tâches de configuration du système.
- Lors d'une mise à niveau, si la configuration du système contient des responsables de la sécurité, une autorisation sec-off-defaults est créée avec la liste de tous les responsables de la sécurité actuels.

backup-operator

Un utilisateur doté du rôle *backup-operator* peut effectuer toutes les tâches incombant au rôle *user*, créer des snapshots pour les structures MTree, importer, exporter et déplacer des bandes entre les éléments d'une librairie de bandes virtuelle, et copier des bandes entre des pools.

Un utilisateur doté du rôle *backup-operator* peut également ajouter et supprimer des clés publiques SSH pour des connexions ne nécessitant pas de mot de passe. (Cette fonction est essentiellement utilisée pour la rédaction de scripts automatisés.) Il peut ajouter, supprimer, réinitialiser et afficher les alias de commande CLI, synchroniser les fichiers modifiés et attendre la fin de la réplication sur le système cible.

none

Le rôle *none* est réservé à l'authentification DD Boost et aux utilisateurs d'une unité locataire. Un utilisateur doté du rôle *none* peut se connecter à un système Data Domain et peut modifier son mot de passe, mais il ne peut pas surveiller, gérer ou configurer le système principal. Lorsque le système principal est partitionné en unités locataires, le rôle *tenant-admin* ou *tenant-user* est utilisé pour définir le rôle d'un utilisateur par rapport à une unité locataire spécifique. L'utilisateur tenant se voit d'abord attribuer le rôle *none* pour limiter son accès au système principal, puis le rôle *tenant-admin* ou *tenant-user* est ajouté à cet utilisateur.

tenant-admin

Un rôle *tenant-admin* peut être ajouté aux autres rôles (non tenant) lorsque la fonction Secure Multi-Tenancy (SMT) est activée. Un utilisateur doté du rôle *tenant-admin* peut configurer et surveiller une unité locataire spécifique.

tenant-user

Un rôle *tenant-user* peut être ajouté aux autres rôles (non tenant) lorsque la fonction SMT est activée. Le rôle *tenant-user* permet à un utilisateur de surveiller une unité locataire spécifique et de modifier son mot de passe. Les utilisateurs dotés du rôle de gestion *tenant-user* peuvent afficher l'état de l'unité locataire, mais ils ne peuvent pas modifier la configuration de cette unité locataire.

Gestion de l'accès au système pour les protocoles IP

Cette fonction gère l'accès au système pour les protocoles FTP, FTPS, HTTP, HTTPS, SSH, SCP et Telnet.

Affichage de la configuration des services IP

L'onglet Administrator Access affiche l'état de la configuration des protocoles IP grâce auxquels vous pouvez accéder au système. Les protocoles FTP et FTPS sont les seuls protocoles réservés exclusivement aux administrateurs.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.

Résultats

La page Access Management regroupe les onglets Administrator Access, Local Users, Authentication et Active Users.

Tableau 34 Informations relatives à l'onglet Administrator Access

Élément	Description
Passphrase	Si aucune phrase de passe n'est définie, le bouton **Set Passphrase** apparaît. Si une phrase de passe est définie, le bouton **Change Passphrase** apparaît.
Services	Nom d'un service/protocole pouvant accéder au système.
Enabled (Yes/No)	État du service. Si le service est désactivé, activez-le en le sélectionnant dans la liste, puis en cliquant sur **Configure**. Renseignez les champs de l'onglet General de la boîte de dialogue. Si le service est activé, modifiez ses paramètres en le sélectionnant dans la liste, puis en cliquant sur **Configure**. Modifiez les paramètres dans l'onglet General de la boîte de dialogue.
Allowed Hosts	Le ou les hôtes autorisés à accéder au service.
Service Options	Valeur d'expiration de port ou de session du service sélectionné dans la liste.
FTP/FTPS	Seule l'expiration de session peut être définie.
HTTP port	Numéro du port ouvert pour le protocole HTTP (port 80, par défaut).

Tableau 34 Informations relatives à l'onglet Administrator Access (suite)

Élément	Description
HTTPS port	Numéro du port ouvert pour le protocole HTTPS (port 443, par défaut).
SSH/SCP port	Numéro du port ouvert pour le protocole SSH/SCP (port 22, par défaut).
Telnet	Aucun numéro de port ne peut être défini.
Session Timeout	Durée d'inactivité autorisée avant la fermeture d'une connexion. La valeur par défaut est Infinite, c'est-à-dire que la connexion ne se ferme pas. Si possible, définissez un délai maximum d'expiration de session de cinq minutes. Utilisez l'onglet **Advanced** de la boîte de dialogue pour définir une expiration du délai en secondes.

Gestion de l'accès FTP

Le protocole FTP (File Transfer Protocol) permet aux administrateurs d'accéder aux fichiers sur le système Data Domain.

Vous pouvez donner l'accès FTP ou FTPS aux utilisateurs dotés du rôle de gestion admin. L'accès FTP transmet les noms d'utilisateur et les mots de passe au réseau en texte clair, ce qui en fait une méthode d'accès non sécurisée. FTPS est recommandé comme méthode d'accès sécurisée. Lorsque vous activez un accès FTP ou FTPS, l'autre méthode d'accès est désactivée.

Remarque

Seuls les utilisateurs associés au rôle de gestion admin sont autorisés à accéder au système via FTP

Remarque

Les clients LFTP qui se connectent à un système Data Domain via FTPS ou FTP sont déconnectés après un délai défini. Le client LFTP utilise toutefois ses nom d'utilisateur et mot de passe en cache pour se reconnecter après l'expiration du délai pendant que vous exécutez une commande.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Sélectionnez **FTP** et cliquez sur **Configure**.
3. Pour gérer l'accès FTP et les hôtes pouvant se connecter, sélectionnez l'onglet General et procédez comme suit :
   a. Pour activer l'accès FTP, sélectionnez **Allow FTP Access**.
   b. Pour permettre à tous les hôtes de se connecter, sélectionnez **Allow all hosts to connect**.
   c. Pour limiter l'accès aux hôtes sélectionnés, choisissez **Limit Access to the following systems**, puis modifiez la liste Allowed Hosts.

Remarque

Vous pouvez identifier un hôte à l'aide du nom d'hôte complet, d'une adresse IPv4 ou d'une adresse IPv6.

- Pour ajouter un hôte, cliquez sur Add (**+**). Saisissez l'identification de l'hôte, puis cliquez sur **OK**.
- Pour modifier un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Edit (crayon). Modifiez l'ID d'hôte, puis cliquez sur **OK**.
- Pour supprimer un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Delete (**X**).

4. Pour définir une expiration de session, sélectionnez l'onglet **Advanced**, puis entrez la valeur du délai en secondes.

   Remarque

   La valeur d'expiration de session par défaut est Infinite, autrement dit la connexion ne se ferme pas.

5. Cliquez sur **OK**.

   Si FTPS est activé, un message d'avertissement apparaît et vous êtes invité à cliquer sur **OK** pour continuer.

Gestion de l'accès FTPS

Le protocole FTPS (FTP sécurisé) permet aux administrateurs d'accéder aux fichiers sur le système Data Domain.

Le protocole FTPS fournit une sécurité supplémentaire par rapport au protocole FTP, notamment la prise en charge des protocoles de chiffrement TSL (Transport Layer Security) et SSL (Secure Sockets Layer). Tenez compte des points suivants lors de l'utilisation de FTPS.

- Seuls les utilisateurs qui ont un rôle de gestion administrateur sont autorisés à accéder au système via FTPS.
- Le fait d'activer l'accès FTPS désactive automatiquement l'accès FTP.
- Le protocole FTPS n'apparaît pas en tant que service pour les systèmes DD exécutant DD OS 5.2, géré à partir d'un système DD exécutant DD OS 5.3 ou version supérieure.
- Lorsque vous exécutez la commande `get`, le message d'erreur fatale `SSL_read: wrong version number lftp` apparaît si les versions correspondantes de SSL ne sont pas installées sur le système Data Domain et compilées sur le client LFTP. Une solution consiste à tenter d'émettre à nouveau la commande `get` sur le même fichier.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Sélectionnez **FTPS**, puis cliquez sur **Configure**.
3. Pour gérer l'accès FTPS et déterminer quels hôtes peuvent se connecter, sélectionnez l'onglet General et procédez comme suit :

   a. Pour activer l'accès FTPS, sélectionnez **Allow FTPS Access**.

b. Pour permettre à tous les hôtes de se connecter, sélectionnez **Allow all hosts to connect**.

c. Pour limiter l'accès aux hôtes sélectionnés, choisissez **Limit Access to the following systems**, puis modifiez la liste des hôtes.

Remarque

Vous pouvez identifier un hôte à l'aide du nom d'hôte complet, d'une adresse IPv4 ou d'une adresse IPv6.

- Pour ajouter un hôte, cliquez sur Add (**+**). Saisissez l'identification de l'hôte, puis cliquez sur **OK**.
- Pour modifier un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Edit (crayon). Modifiez l'ID d'hôte, puis cliquez sur **OK**.
- Pour supprimer un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Delete (**X**).

4. Pour définir une expiration de session, sélectionnez l'onglet **Advanced**, puis entrez la valeur du délai en secondes.

Remarque

La valeur d'expiration de session par défaut est Infinite, autrement dit la connexion ne se ferme pas.

5. Cliquez sur **OK**. Si FTP est activé, un message d'avertissement apparaît et vous êtes invité à cliquer sur **OK** pour continuer.

Gestion de l'accès HTTP et HTTPS

Vous avez besoin d'un accès HTTP ou HTTPS pour que le navigateur soit capable d'accéder à DD System Manager.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Sélectionnez **HTTP** ou **HTTPS**, puis cliquez sur **Configure**.

   La boîte de dialogue Configure HTTP/HTTPS Access s'affiche. Elle contient des onglets pour la configuration générale, la configuration avancée et la gestion des certificats.
3. Pour gérer la méthode d'accès et les hôtes pouvant se connecter, sélectionnez l'onglet General et procédez comme suit :

   a. Cochez les cases correspondant aux méthodes d'accès que vous souhaitez autoriser.

   b. Pour permettre à tous les hôtes de se connecter, sélectionnez **Allow all hosts to connect**.

   c. Pour limiter l'accès aux hôtes sélectionnés, choisissez **Limit Access to the following systems**, puis modifiez la liste des hôtes.

Remarque

Vous pouvez identifier un hôte à l'aide du nom d'hôte complet, d'une adresse IPv4 ou d'une adresse IPv6.

- Pour ajouter un hôte, cliquez sur Add (**+**). Saisissez l'identification de l'hôte, puis cliquez sur **OK**.
- Pour modifier un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Edit (crayon). Modifiez l'ID d'hôte, puis cliquez sur **OK**.
- Pour supprimer un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Delete (**X**).

4. Pour configurer les ports du système et les valeurs d'expiration de session, sélectionnez l'onglet **Advanced** et remplissez le formulaire.
   - Dans la zone **HTTP Port**, saisissez le numéro de port. Le port 80 est attribué par défaut.
   - Dans la zone **HTTPS Port**, saisissez le numéro. Le port 443 est attribué par défaut.
   - Dans la zone **Session Timeout**, saisissez le délai en secondes avant la fermeture d'une connexion. Le délai minimal est de 60 secondes et le délai maximal est de 31 536 000 secondes (un an).

   Remarque

   Le délai d'expiration de la session est de 10 800 secondes par défaut.

5. Cliquez sur **OK**.

Gestion des certificats d'hôte pour HTTP et HTTPS

Un certificat d'hôte permet aux navigateurs de vérifier l'identité du système lors de la mise en œuvre de sessions de gestion.

Demande d'un certificat d'hôte pour HTTP et HTTPS

Vous pouvez utiliser DD System Manager pour générer une demande de certificat d'hôte que vous pouvez transférer ensuite vers une autorité de certification (AC).

Remarque

Vous devez configurer une phrase de passe du système (phrase de passe système définie) avant de pouvoir générer une demande CSR.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Dans la zone Services, sélectionnez **HTTP** ou **HTTPS**, puis cliquez sur **Configure**.
3. Sélectionnez l'onglet **Certificate**.
4. Cliquez sur Ajouter.

   Une boîte de dialogue s'affiche pour le protocole précédemment sélectionné dans cette procédure.

5. Cliquez sur **Generate the CSR for this Data Domain system**.

   La boîte de dialogue se développe pour afficher un formulaire de demande de signature de certificat (CSR).

Remarque

DD OS ne prend en charge qu'une demande CSR active à la fois. Lorsqu'une demande CSR est générée, le lien **Generate the CSR for this Data Domain system** est remplacé par le lien **Download the CSR for this Data Domain system**. Pour supprimer une demande CSR, utilisez la commande CLI `adminaccess certificate cert-signing-request delete`.

6. Renseignez le formulaire de demande de signature de certificat (CSR), puis cliquez sur **Generate and download a CSR**.

   Le fichier CSR est enregistré sur le chemin d'accès suivant : `/ddvar/certificates/CertificateSigningRequest.csr`. Utilisez SCP, FTP ou FTPS pour transférer le fichier CSR du système vers un ordinateur à partir duquel vous pouvez envoyer la demande CSR à une autorité de certification.

Ajout d'un certificat d'hôte pour HTTP et HTTPS

Vous pouvez utiliser DD System Manager pour ajouter un certificat d'hôte au système.

Procédure

1. Si vous n'avez pas demandé de certificat d'hôte, demandez-en un auprès d'une autorité de certification.
2. Lorsque vous acceptez un certificat d'hôte, copiez-le ou déplacez-le sur l'ordinateur à partir duquel vous exécutez DD Service Manager.
3. Sélectionnez **Administration** > **Access** > **Administrator Access**.
4. Dans la zone Services, sélectionnez **HTTP** ou **HTTPS**, puis cliquez sur **Configure**.
5. Sélectionnez l'onglet **Certificate**.
6. Cliquez sur **Add**.

   Une boîte de dialogue s'affiche pour le protocole précédemment sélectionné dans cette procédure.

7. Pour ajouter un certificat d'hôte contenu dans un fichier .p12, procédez comme suit :
   a. Sélectionnez **I want to upload the certificate as a .p12 file**.
   b. Entrez la phrase de passe dans la zone **Password**.
   c. Cliquez sur **Browse**, puis sélectionnez le fichier de certificat d'hôte à télécharger sur le système.
   d. Cliquez sur **Add.**
8. Pour ajouter un certificat d'hôte contenu dans un fichier .pem, procédez comme suit :
   a. Sélectionnez **I want to upload the public key as a .pem file and use a generated private key**.
   b. Cliquez sur **Browse**, puis sélectionnez le fichier de certificat d'hôte à télécharger sur le système.
   c. Cliquez sur **Add.**

Suppression d'un certificat d'hôte pour HTTP et HTTPS

DD OS prend en charge un certificat d'hôte pour HTTP et HTTPS. Si le système utilise actuellement un certificat d'hôte et que vous avez l'intention d'utiliser un autre

certificat d'hôte, vous devez supprimer le certificat actuel avant d'en ajouter un nouveau.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Dans la zone Services, sélectionnez **HTTP** ou **HTTPS**, puis cliquez sur **Configure**.
3. Sélectionnez l'onglet **Certificate**.
4. Sélectionnez le certificat à supprimer.
5. Cliquez sur **Delete**, puis sur **OK**.

Gestion de l'accès SSH et SCP

SSH est un protocole sécurisé offrant un accès réseau à la CLI du système, avec ou sans SCP (copie sécurisée). Vous pouvez utiliser DD System Manager pour autoriser l'accès système via le protocole SSH. SCP nécessite SSH, de sorte que lorsque SSH est désactivé, SCP est automatiquement désactivé.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Sélectionnez **SSH** ou **SCP**, puis cliquez sur **Configure**.
3. Pour gérer la méthode d'accès et les hôtes pouvant se connecter, sélectionnez l'onglet **General**.
   a. Cochez les cases correspondant aux méthodes d'accès que vous souhaitez autoriser.
   b. Pour permettre à tous les hôtes de se connecter, sélectionnez **Allow all hosts to connect**.
   c. Pour limiter l'accès aux hôtes sélectionnés, choisissez **Limit Access to the following systems**, puis modifiez la liste des hôtes.

   Remarque

   Vous pouvez identifier un hôte à l'aide du nom d'hôte complet, d'une adresse IPv4 ou d'une adresse IPv6.

   - Pour ajouter un hôte, cliquez sur Add (**+**). Saisissez l'identification de l'hôte, puis cliquez sur **OK**.
   - Pour modifier un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Edit (crayon). Modifiez l'ID d'hôte, puis cliquez sur **OK**.
   - Pour supprimer un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Delete (**X**).
4. Pour configurer les ports du système et les valeurs d'expiration de session, cliquez sur l'onglet **Advanced**.
   - Dans la zone de saisie de texte **SSH/SCP Port**, indiquez le numéro de port. Le port 22 est attribué par défaut.
   - Dans la zone **Session Timeout**, saisissez le délai en secondes avant la fermeture d'une connexion.

Remarque

La valeur d'expiration de session par défaut est Infinite, autrement dit la connexion ne se ferme pas.

Remarque

Cliquez sur **Default** pour revenir à la valeur par défaut.

5. Cliquez sur **OK**.

Gestion de l'accès Telnet

Telnet est un protocole non sécurisé offrant un accès réseau à la CLI du système.

Remarque

L'accès Telnet transmet les noms d'utilisateur et les mots de passe au réseau en texte clair, ce qui en fait une méthode d'accès non sécurisée.

Procédure

1. Sélectionnez **Administration** > **Access** > **Administrator Access**.
2. Sélectionnez **Telnet**, puis cliquez sur **Configure**.
3. Pour gérer un accès Telnet et les hôtes pouvant s'y connecter, sélectionnez l'onglet **General**.
   a. Pour activer l'accès Telnet, sélectionnez **Allow Telnet Access**.
   b. Pour permettre à tous les hôtes de se connecter, sélectionnez **Allow all hosts to connect**.
   c. Pour limiter l'accès aux hôtes sélectionnés, choisissez **Limit Access to the following systems**, puis modifiez la liste des hôtes.

   Remarque

   Vous pouvez identifier un hôte à l'aide du nom d'hôte complet, d'une adresse IPv4 ou d'une adresse IPv6.

   - Pour ajouter un hôte, cliquez sur Add (**+**). Saisissez l'identification de l'hôte, puis cliquez sur **OK**.
   - Pour modifier un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Edit (crayon). Modifiez l'ID d'hôte, puis cliquez sur **OK**.
   - Pour supprimer un ID d'hôte, sélectionnez l'hôte dans la liste **Hosts**, puis cliquez sur Delete (**X**).
4. Pour définir une expiration de session, sélectionnez l'onglet Advanced, puis entrez la valeur du délai en secondes.

   Remarque

   La valeur d'expiration de session par défaut est Infinite, autrement dit la connexion ne se ferme pas.

5. Cliquez sur **OK**.

Gestion du compte utilisateur local

Un utilisateur local est un compte utilisateur (nom d'utilisateur et mot de passe) configuré sur le système Data Domain au lieu d'être défini dans un annuaire Windows Active Directory, un groupe de travail Windows ou un annuaire NIS.

Une fois qu'un domaine de confiance est configuré, les utilisateurs qui appartiennent à ce domaine peuvent se connecter au système Data Domain, même si ce domaine de confiance est hors ligne.

Conflits d'UID : comptes d'utilisateur local et d'utilisateur NIS

Lorsque vous configurez un système Data Domain dans un environnement NIS, des risques de conflits d'UID entre les comptes d'utilisateur local et d'utilisateur NIS sont possibles.

Les comptes d'utilisateur local d'un système Data Domain commencent par un UID de 500. Pour éviter tout conflit, tenez compte de la taille des comptes locaux potentiels lorsque vous définissez les plages UID autorisées pour les utilisateurs NIS.

Affichage des informations sur l'utilisateur local

Un utilisateur local est un compte utilisateur configuré sur le système, au lieu d'être défini dans Active Directory, un groupe de travail ou UNIX. Vous pouvez afficher le nom de l'utilisateur local, le rôle de gestion, l'état de la connexion et la date de désactivation de la cible. Vous pouvez également afficher les contrôles relatifs au mot de passe de l'utilisateur et les unités locataires auxquelles l'utilisateur a accès.

Remarque

Le module d'authentification des utilisateurs utilise l'heure GMT (heure du méridien de Greenwich). Pour s'assurer que les comptes et les mots de passe des utilisateurs expirent comme prévu, utilisez l'heure GMT correspondant à l'heure locale de la cible.

Procédure

1. Sélectionnez **Administration** > **Access** > **Local Users**.

   La vue Local Users s'affiche et présente le tableau des utilisateurs locaux, ainsi que la zone relative aux informations détaillées.

   Tableau 35 Liste des utilisateurs locaux, description des libellés de colonne

Élément	Description
Name	ID utilisateur, tel qu'il a été ajouté au système.
Management Role	Le rôle affiché est admin, user, security, backup-operator ou none. Dans ce tableau, les rôles tenant-user s'affichent sous le rôle *none*. Pour visualiser un rôle de tenant attribué, sélectionnez l'utilisateur et affichez le rôle dans la zone Detailed Information.
État	• L'accès au compte de type utilisateur actif est autorisé. • Disabled : l'accès au compte de type utilisateur est refusé, car le compte est désactivé par l'administrateur ; la date actuelle dépasse la date d'expiration du compte, ou il est nécessaire de renouveler le mot de passe du compte verrouillé.

Tableau 35 Liste des utilisateurs locaux, description des libellés de colonne (suite)

Élément	Description
	• Locked : l'accès utilisateur est refusé, car le mot de passe a expiré.
Disable Date	Date à laquelle le compte doit être désactivé.
Last Login From	Dernier emplacement à partir duquel l'utilisateur s'est connecté.
Last Login Time	Heure à laquelle l'utilisateur s'est connecté pour la dernière fois.

Remarque

Les comptes utilisateur dotés des rôles d'administrateur ou de responsable de la sécurité peuvent afficher tous les utilisateurs. Les utilisateurs dotés d'autres rôles ne peuvent afficher que leurs propres comptes utilisateur.

2. Sélectionnez l'utilisateur que vous voulez afficher dans la liste des utilisateurs. Les informations sur l'utilisateur sélectionné s'affichent dans la zone Detailed Information.

Tableau 36 Informations détaillées sur l'utilisateur, description des libellés de ligne

Élément	Description
Password Last Changed	Date à laquelle le mot de passe a été modifié pour la dernière fois.
Minimum Days Between Change	Nombre minimal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. La valeur par défaut est 0.
Maximum Days Between Change	Nombre maximal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. Par défaut : 90.
Warn Days Before Expire	Nombre de jours qui doivent s'écouler avant d'avertir l'utilisateur de l'expiration de son mot de passe. La valeur par défaut est 7.
Disable Days After Expire	Nombre de jours qui doivent s'écouler après l'expiration d'un mot de passe pour désactiver le compte utilisateur. La valeur par défaut est Never.

Remarque

Les valeurs par défaut sont les valeurs initiales de la stratégie de mots de passe par défaut. Un administrateur système (rôle d'administrateur) peut les modifier en sélectionnant **More Tasks.** > **Change Login Options**.

Création d'utilisateurs locaux

Créez des utilisateurs locaux si vous avez l'intention de gérer l'accès sur un système local au lieu de le faire via un répertoire externe. Les systèmes Data Domain prennent en charge un maximum de 500 comptes d'utilisateur local.

Procédure

1. Sélectionnez **Administration** > **Access** > **Local Users**.
   La vue Local Users s'affiche.

2. Cliquez sur **Create** pour créer un nouvel utilisateur.

   La boîte de dialogue Create User s'affiche.

3. Entrez les informations utilisateur dans l'onglet General.

Tableau 37 Boîte de dialogue Create User, contrôles généraux

Élément	Description
User	ID ou nom de l'utilisateur.
Password	Mot de passe de l'utilisateur. Définissez un mot de passe par défaut, que l'utilisateur pourra modifier ultérieurement.
Verify Password	Indiquez de nouveau le mot de passe de l'utilisateur.
Management Role	Rôle attribué à l'utilisateur. Il peut être admin, user, security, backup-operator ou none. **Remarque** Seul l'utilisateur sysadmin (l'utilisateur par défaut créé lors de l'installation de DD OS) peut créer le premier utilisateur doté du rôle security. Une fois le premier utilisateur doté du rôle security créé, seuls les utilisateurs dotés du rôle security peuvent créer d'autres utilisateurs dotés du rôle security.
Force Password Change	Sélectionnez cette case pour exiger de l'utilisateur qu'il modifie le mot de passe lors de la première connexion à DD System Manager ou à la CLI avec SSH ou Telnet.

La valeur par défaut pour la longueur minimale d'un mot de passe est de 6 caractères. La valeur par défaut pour le nombre minimal de classes de caractères requises dans un mot de passe utilisateur est 1. Les classes de caractères autorisées sont les suivantes :

- Lettres minuscules (a à z)
- Lettres majuscules (A à Z)
- Chiffres (0 à 9)
- Caractères spéciaux ($, %, #, +, etc.)

Remarque

L'utilisateur sysadmin est l'utilisateur doté du rôle admin par défaut ; il ne peut être ni supprimé, ni modifié.

4. Pour gérer l'expiration des mots de passe et du compte, sélectionnez l'onglet Advanced et utilisez les contrôles décrits dans le tableau suivant.

Tableau 38 Boîte de dialogue Create User, contrôles avancés

Élément	Description
Minimum Days Between Change	Nombre minimal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. La valeur par défaut est 0.

Tableau 38 Boîte de dialogue Create User, contrôles avancés (suite)

Élément	Description
Maximum Days Between Change	Nombre maximal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. Par défaut : 90.
Warn Days Before Expire	Nombre de jours qui doivent s'écouler avant d'avertir l'utilisateur de l'expiration de son mot de passe. La valeur par défaut est 7.
Disable Days After Expire	Nombre de jours qui doivent s'écouler après l'expiration d'un mot de passe pour désactiver le compte utilisateur. La valeur par défaut est Never.
Disable account on the following date	Cochez cette case et saisissez la date (jj/mm/aaaa) à laquelle le compte doit être désactivé. Vous pouvez également cliquer sur le calendrier pour choisir une date.

5. Cliquez sur **OK**.

Remarque

Remarque : La stratégie de mot de passe par défaut peut changer si un utilisateur doté du rôle admin la modifie (**More Tasks** > **Change Login Options**). Les valeurs par défaut sont les valeurs initiales de la stratégie de mots de passe par défaut.

Modification d'un profil d'utilisateur local

Après avoir créé un utilisateur, vous pouvez changer sa configuration à l'aide de DD System Manager.

Procédure

1. Sélectionnez **Administration** > **Access** > **Local Users**.

   La vue Local Users s'affiche.

2. Cliquez sur un nom d'utilisateur dans la liste.
3. Cliquez sur **Modify** pour apporter des modifications à un compte utilisateur.

   La boîte de dialogue Modify User s'affiche.
4. Mettez à jour les informations sous l'onglet General.

Remarque

Si SMT est activée et si un changement de rôle est demandé pour un autre rôle que le rôle none, le changement sera accepté uniquement si l'utilisateur n'est pas affecté à une unité tenant en tant qu'utilisateur de gestion, s'il n'est pas un utilisateur DD Boost ayant une unité tenant définie par défaut et s'il n'est pas le propriétaire d'une unité de stockage attribuée à une unité tenant.

Remarque

Pour modifier le rôle d'un utilisateur DD Boost qui ne détient pas toutes les unités de stockage, annulez son attribution en tant qu'utilisateur DD Boost, modifiez le rôle d'utilisateur et réattribuez-le tant qu'utilisateur DD Boost.

Tableau 39 Boîte de dialogue Modify User, contrôles généraux

Élément	Description
User	ID ou nom de l'utilisateur.
Role	Sélectionnez le rôle dans la liste.

5. Mettez à jour les informations sous l'onglet Advanced.

Tableau 40 Boîte de dialogue Modify User, contrôles avancés

Élément	Description
Minimum Days Between Change	Nombre minimal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. La valeur par défaut est 0.
Maximum Days Between Change	Nombre maximal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. Par défaut : 90.
Warn Days Before Expire	Nombre de jours qui doivent s'écouler avant d'avertir l'utilisateur de l'expiration de son mot de passe. La valeur par défaut est 7.
Disable Days After Expire	Nombre de jours qui doivent s'écouler après l'expiration d'un mot de passe pour désactiver le compte utilisateur. La valeur par défaut est Never.

6. Cliquez sur **OK**.

Suppression d'un utilisateur local

Vous pouvez supprimer certains utilisateurs selon votre rôle d'utilisateur. Si l'un des utilisateurs sélectionnés ne peut pas être supprimé, le bouton Delete est désactivé.

L'utilisateur sysadmin ne peut pas être supprimé. Les utilisateurs dotés du rôle admin ne peuvent pas supprimer les responsables de la sécurité. Les responsables de la sécurité peuvent supprimer, activer et désactiver les autres responsables de la sécurité.

Procédure

1. Sélectionnez **Administration** > **Access** > **Local Users**.

   La vue Local Users s'affiche.

2. Cliquez sur un ou plusieurs noms d'utilisateur dans la liste.
3. Cliquez sur **Delete** pour supprimer les comptes utilisateur.

   La boîte de dialogue Delete User s'affiche.

4. Cliquez sur **OK**, puis sur **Close**.

Activation et désactivation d'utilisateurs locaux

Les administrateurs peuvent activer ou désactiver tous les utilisateurs à l'exception du sysadmin et des responsables de la sécurité. L'utilisateur sysadmin ne peut pas être désactivé. Seuls les responsables de la sécurité ont le droit d'activer ou de désactiver d'autres responsables de la sécurité.

Procédure

1. Sélectionnez **Administration** > **Access** > **Local Users**.

   La vue Local Users s'affiche.

2. Cliquez sur un ou plusieurs noms d'utilisateur dans la liste.
3. Cliquez sur **Enable** ou sur **Disable** pour activer ou désactiver des comptes utilisateur.

   La boîte de dialogue Enable or Disable User s'affiche.

4. Cliquez sur **OK**, puis sur **Close**.

Activation de l'autorisation de sécurité

Vous pouvez utiliser l'interface de ligne de commande (CLI) du système Data Domain pour activer et désactiver la règle d'autorisation de sécurité.

Pour plus d'informations sur les commandes utilisées dans cette procédure, consultez le *Guide de référence des commandes de Data Domain Operating System*.

Remarque

La licence DD Retention Lock Compliance doit être installée. Vous n'êtes pas autorisé à désactiver la règle d'autorisation sur les systèmes DD Retention Lock Compliance.

Procédure

1. Connectez-vous à l'interface de ligne de commande à l'aide du nom d'utilisateur et du mot de passe du responsable de la sécurité.
2. Pour activer la règle d'autorisation du responsable de la sécurité, saisissez : `# authorization policy set security-officer enabled`

Modification des mots de passe des utilisateurs

Après avoir créé un utilisateur, vous pouvez changer son mot de passe à l'aide de DD System Manager. Chaque utilisateur peut également, s'il le souhaite, modifier son mot de passe personnel.

Procédure

1. Cliquez sur **Administration** > **Access** > **Local Users**.

   La vue Local Users s'affiche.

2. Cliquez sur un nom d'utilisateur dans la liste.
3. Cliquez sur **Change Password** pour modifier le mot de passe de l'utilisateur.

   La boîte de dialogue Change Password s'affiche.

4. Saisissez l'ancien mot de passe dans le champ **Old Password**.
5. Saisissez le nouveau mot de passe dans le champ **New Password**.
6. Saisissez une nouvelle fois le nouveau le mot de passe dans le champ **Verify New Password**.
7. Cliquez sur **OK**.

   Seuls les utilisateurs ayant un rôle d'administrateur peuvent modifier le mot de passe des autres utilisateurs. L'administrateur peut changer le mot de passe d'autres utilisateurs depuis la CLI en exécutant la commande `user change password [<user>] .`

Remarque

Pour des raisons de sécurité, les utilisateurs ayant un rôle d'administrateur ne peuvent pas changer les mots de passe des autres utilisateurs administrateurs. Si un mot de passe d'utilisateur administrateur doit être modifié en se connectant en tant qu'un autre utilisateur, contactez le support DELL-EMC en créant une demande d'assistance ou une demande d'assistance par chat.

Modification de la stratégie relative aux mots de passe et des contrôles de connexion

La stratégie relative aux mots de passe et les contrôles de connexion définissent les conditions de connexion pour l'ensemble des utilisateurs. Les administrateurs peuvent définir la fréquence à laquelle il convient de changer un mot de passe, les critères à respecter pour créer un mot de passe valide et la façon dont le système gère les tentatives de connexion non valides.

Procédure

1. Sélectionnez **Administration** > **Access**.
2. Sélectionnez **More Tasks** > **Change Login Options**.

   La boîte de dialogue Change Login Options s'affiche.

3. Spécifiez la nouvelle configuration dans les zones correspondant à chaque option. Pour sélectionner la valeur par défaut, cliquez sur **Default** en regard de l'option appropriée.
4. Cliquez sur **OK** pour enregistrer les paramètres de mot de passe.

Boîte de dialogue Change Login Options

Utilisez cette boîte de dialogue pour définir la stratégie relative aux mots de passe, préciser le nombre maximum de tentatives de connexion à ne pas dépasser et configurer la durée de verrouillage du compte utilisateur.

Tableau 41 Contrôles de la boîte de dialogue Change Login Options

Élément	Description
Minimum Days Between Change	Nombre minimal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. Cette valeur doit être inférieure à la valeur **Maximum Days Between Change** moins la valeur **Warn Days Before Expire**. Paramètre par défaut : 0.
Maximum Days Between Change	Nombre maximal de jours entre chaque modification du mot de passe qu'un utilisateur est autorisé à effectuer. La valeur minimale est 1. La valeur par défaut est 90.
Warn Days Before Expire	Nombre de jours qui doivent s'écouler avant d'avertir l'utilisateur de l'expiration de son mot de passe. Cette valeur doit être inférieure à la valeur **Maximum Days Between Change** moins la valeur **Minimum Days Between Change**. Paramètre par défaut : 7.
Disable Days After Expire	Le système désactive un compte utilisateur après l'expiration du mot de passe et à l'issue du nombre de jours spécifié à l'aide de cette option. Vous pouvez sélectionner *never* (jamais) ou un

Tableau 41 Contrôles de la boîte de dialogue Change Login Options (suite)

Élément	Description
	nombre supérieur ou égal à 0. Le paramètre par défaut est « never ».
Minimum Length of Password	Longueur minimale de mot de passe obligatoire. Par défaut : 6.
Minimum Number of Character Classes	Nombre minimal de caractères requis dans le mot de passe d'un utilisateur. La valeur par défaut est 1. Les classes de caractères incluent, notamment : • Lettres minuscules (a à z) • Lettres majuscules (A à Z) • Chiffres (0 à 9) • Caractères spéciaux ($, %, #, +, etc.)
Lowercase Character Requirement	Indique si le mot de passe doit obligatoirement comporter ou non au moins une minuscule. Par défaut, cet élément est désactivé.
Uppercase Character Requirement	Indique si le mot de passe doit obligatoirement comporter ou non au moins une majuscule. Par défaut, cet élément est désactivé.
One Digit Requirement	Indique si le mot de passe doit obligatoirement comporter ou non au moins un caractère numérique. Par défaut, cet élément est désactivé.
Special Character Requirement	Indique si le mot de passe doit obligatoirement comporter ou non au moins un caractère spécial. Par défaut, cet élément est désactivé.
Max Consecutive Character Requirement	Indique si le mot de passe doit obligatoirement comporter ou non un maximum de trois caractères répétés consécutifs. Par défaut, cet élément est désactivé.
Number of Previous Passwords to Block	Spécifiez le nombre de mots de passe à mémoriser. La valeur doit être comprise entre 0 et 24. La valeur par défaut est 1. **Remarque** Si vous réduisez cette valeur, la liste des mots de passe mémorisés restera la même jusqu'à la prochaine modification du mot de passe. Si vous passez de 4 à 3, par exemple, les quatre derniers mots de passe resteront mémorisés tant que vous ne changerez pas de mot de passe.
Maximum login attempts	Indique le nombre maximum de tentatives de connexion autorisées avant qu'un compte utilisateur soit verrouillé. Cette limite s'applique à tous les comptes utilisateur, y compris le compte sysadmin. Aucune autre tentative de connexion ne pourra avoir lieu tant que le compte sera verrouillé. La valeur doit être comprise entre 4 et 10. La valeur par défaut est 4.
Unlock timeout (secondes)	Indique la durée pendant laquelle le compte utilisateur restera verrouillé en cas de dépassement du nombre maximum de tentatives de connexion autorisées. L'utilisateur pourra à nouveau essayer de se connecter au compte une fois ce délai écoulé. La valeur doit être comprise entre 120 et 600 secondes. La valeur par défaut est de 120 secondes.

Tableau 41 Contrôles de la boîte de dialogue Change Login Options (suite)

Élément	Description
Nombre maximal de connexions actives	Spécifie le nombre maximum de connexions actives à autoriser. La valeur par défaut est 100.

Gestion des utilisateurs et des groupes Active Directory

Vous pouvez utiliser DD System Manager pour gérer l'accès au système des utilisateurs et des groupes dans Windows Active Directory, NIS ou un groupe de travail Windows. L'authentification Kerberos est une option pour les clients CIFS et NFS.

Affichage des informations relatives à l'authentification Active Directory et Kerberos

La configuration Active Directory/Kerberos détermine les méthodes que les clients CIFS et NFS utilisent pour s'authentifier. Le volet Active Directory/Kerberos Authentication affiche cette configuration.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.
2. Développez le volet Active Directory/Kerberos Authentication.

Tableau 42 Description des libellés de l'authentification Active Directory/Kerberos

Élément	Description
Mode	Type de mode d'authentication. Dans le mode Windows/Active Directory, les clients CIFS utilisent une authentification Active Directory et Kerberos. Les clients NFS utilisent, quant à eux, une authentification Kerberos. Dans le mode Unix, les clients CIFS utilisent une authentification par groupe de travail (sans Kerberos), et les clients NFS utilisent une authentification Kerberos. Dans le mode Disabled, l'authentification Kerberos est désactivée et les clients CIFS utilisent l'authentification par groupe de travail.
Realm	Nom du realm du groupe de travail ou d'Active Directory.
DDNS	Indique si le système DNS est activé ou non.
Domain Controllers	Nom du contrôleur de domaine pour le groupe de travail ou Active Directory.
Organizational Unit	Nom de l'unité d'organisation pour le groupe de travail ou Active Directory.
CIFS Server Name	Nom du serveur CIFS en cours d'utilisation (mode Windows uniquement).
WINS Server	Nom du serveur WINS en cours d'utilisation (mode Windows uniquement).
Short Domain Name	Nom abrégé du domaine.
NTP	Activé/désactivé (mode UNIX uniquement)
NIS	Activé/désactivé (mode UNIX uniquement)

Tableau 42 Description des libellés de l'authentification Active Directory/Kerberos (suite)

Élément	Description
Key Distribution Centers	Nom(s) d'hôte ou adresse(s) IP du Centre de distribution de clés en cours d'utilisation (mode UNIX uniquement)
Active Directory Administrative Access	Activé/Désactivé : Cliquez sur Enable ou Disable Administrative Access pour les groupes Active Directory (Windows).

Tableau 43 Rôles et groupes d'administration Active Directory

Élément	Description
Windows Group	Nom du groupe Windows.
Management Role	Rôle du groupe (administrateur, utilisateur, etc.)

Configuration de l'authentification Active Directory et Kerberos

La configuration de l'authentification Windows Active Directory permet d'intégrer le système Data Domain dans un realm Windows Active Directory. les clients CIFS et NFS utilisent l'authentification Kerberos.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet Active Directory/Kerberos Authentication.
3. Cliquez sur **Configure...** en regard du mode pour lancer l'assistant de configuration.

   La boîte de dialogue Active Directory/Kerberos Authentication s'affiche.
4. Sélectionnez **Windows/Active Directory**, puis cliquez sur **Next**.
5. Saisissez le nom de realm complet du système (par exemple : domain1.local), le nom d'utilisateur et le mot de passe du système Data Domain. Cliquez ensuite sur **Next**.

   Remarque

   Utilisez le nom de realm complet. Vérifiez que l'utilisateur dispose des privilèges suffisants pour ajouter le système au domaine. Le nom d'utilisateur et le mot de passe doivent être compatibles avec les exigences Microsoft relatives au domaine Active Directory. Cet utilisateur doit également avoir l'autorisation de créer des comptes dans ce domaine.

6. Sélectionnez le nom de serveur CIFS par défaut ou **Manual**, puis entrez un nom de serveur CIFS.
7. Pour sélectionner des contrôleurs de domaine, sélectionnez **Automatically assign** ou **Manual**, puis saisissez jusqu'à trois noms de contrôleur de domaine.

   Vous pouvez saisir des noms de domaine complets, des noms d'hôte ou des adresses IP (IPv4 ou IPv6).
8. Pour sélectionner une unité d'organisation, sélectionnez **Use default Computers** ou **Manual**, puis saisissez un nom d'unité d'organisation.

Remarque

Le compte est déplacé vers la nouvelle unité d'organisation.

9. Cliquez sur **Next**.

   La page Summary de la configuration s'affiche.

10. Cliquez sur **Terminer**.

    Le système affiche les informations de configuration dans la vue d'authentification.

11. Pour activer l'accès administratif, cliquez sur **Enable** à droite de **Active Directory Administrative Access**.

Sélection du mode d'authentification

La sélection du mode d'authentification détermine comment les clients CIFS et NFS s'authentifient à l'aide des différentes méthodes d'authentification disponibles (Active Directory, groupe de travail et Kerberos).

DD OS prend en charge les options d'authentification suivantes.

- Disabled : L'authentification Kerberos est désactivée pour les clients CIFS and NFS. Les clients CIFS, quant à eux, utilisent l'authentification par groupe de travail.
- Windows/Active Directory : L'authentification Kerberos est activée pour les clients CIFS and NFS. Les clients CIFS, quant à eux, utilisent l'authentification Active Directory.
- Unix : L'authentification Kerberos est activée uniquement pour les clients NFS. Les clients CIFS, quant à eux, utilisent l'authentification par groupe de travail.

Gestion de groupes d'administration pour Active Directory

Vous pouvez utiliser le volet Active Directory/Kerberos Authentication pour créer, modifier et supprimer des groupes Active Directory (Windows) et leur attribuer des rôles de gestion (admin, backup-operator, etc.).

Pour préparer la gestion des groupes, sélectionnez **Administration** > **Access Management** > **Authentication** , développez le volet Active Directory/Kerberos Authentication, puis cliquez sur le bouton **Enable** pour Active Directory Administrative Access.

Création de groupes d'administration pour Active Directory

Créez un groupe d'administration lorsque vous voulez attribuer un rôle de gestion à tous les utilisateurs configurés dans un groupe Active Directory.

Avant de commencer

Activez Active Directory Administrative Access dans le volet Active Directory / Kerberos Authentication dans la page **Administration** > **Access** > **Authentication**.

Procédure

1. Cliquez sur **Create...**.
2. Entrez le domaine et le nom du groupe séparés par une barre oblique inversée. Par exemple : nom de domaine\nom de groupe.
3. Sélectionnez le rôle de gestion pour le groupe dans le menu déroulant.

4. Cliquez sur **OK**.

Modification de groupes d'administration pour Active Directory

Modifiez un groupe d'administration lorsque vous voulez modifier le nom de groupe d'administration ou le rôle de gestion configuré pour un groupe Active Directory.

Avant de commencer

Activez Active Directory Administrative Access dans le volet Active Directory / Kerberos Authentication de la page **Administration** > **Access** > **Authentication**.

Procédure

1. Sélectionnez un groupe à modifier sous l'en-tête **Active Directory Administrative Access**.
2. Cliquez sur **Modify...**.
3. Modifiez le domaine et le nom du groupe. Ces noms sont séparés par une barre oblique inversée. Par exemple : nom de domaine\nom de groupe.
4. Modifiez le rôle de gestion du groupe en sélectionnant un autre rôle dans le menu déroulant.

Suppression des groupes d’administration pour Active Directory

Supprimez un groupe d’administration lorsque vous voulez résilier l’accès au système de tous les utilisateurs configurés dans un groupe Active Directory.

Avant de commencer

Activez Active Directory Administrative Access dans le volet Active Directory / Kerberos Authentication de la page **Administration** > **Access** > **Authentication**.

Procédure

1. Sélectionnez un groupe à supprimer sous l’en-tête **Active Directory Administrative Access**.
2. Cliquez sur **Delete**.

Configuration d’une authentification Kerberos en mode UNIX

La configuration d’une authentification Kerberos en mode UNIX permet aux clients NFS d’utiliser l’authentification Kerberos. Les clients CIFS, quant à eux, utilisent l’authentification par groupe de travail.

Avant de commencer

NIS doit être en cours d’exécution pour que l’authentification Kerberos en mode UNIX fonctionne. Pour obtenir des instructions sur l’activation de Kerberos, reportez-vous à la section relative à l’activation des services NIS.

La configuration de Kerberos pour UNIX permet aux clients NFS d’utiliser l’authentification Kerberos. Les clients CIFS, quant à eux, utilisent l’authentification par groupe de travail.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s’affiche.

2. Développez le volet Active Directory/Kerberos Authentication.
3. Cliquez sur **Configure...** en regard du mode pour lancer l’assistant de configuration.

La boîte de dialogue Active Directory/Kerberos Authentication s'affiche.

4. Sélectionnez **Unix**, puis cliquez sur **Next**.
5. Saisissez le nom de realm (par exemple : domain1.local) et jusqu'à trois noms d'hôte ou adresses IP (IPv4 ou IPv6) pour les Centres de distribution de clés (KDC).
6. Si vous le souhaitez, cliquez sur **Browse** pour télécharger un fichier keytab, puis cliquez sur **Next**.

   La page Summary de la configuration s'affiche.

   Remarque

   Les fichiers keytab sont générés sur les serveurs d'authentification (KDC) et contiennent un secret partagé entre le serveur KDC et le DDR.

   NOTE

   Un fichier keytab doit être téléchargé et importé afin que l'authentification Kerberos fonctionne correctement.
7. Cliquez sur **Terminer**.

   Le système affiche les informations de configuration dans le volet Active Directory/Kerberos Authentication.

Désactivation de l'authentification Kerberos

La désactivation de l'authentification Kerberos empêche les clients CIFS et NFS d'utiliser cette méthode d'authentification. Les clients CIFS, quant à eux, utilisent l'authentification par groupe de travail.

Procédure

1. Sélectionnez **Administration** > **Access Management** > **Authentication**.

   La vue Authentication s'affiche.
2. Développez le volet Active Directory/Kerberos Authentication.
3. Cliquez sur **Configure...** en regard du mode pour lancer l'assistant de configuration.

   La boîte de dialogue Active Directory/Kerberos Authentication s'affiche.
4. Sélectionnez **Disabled**, puis cliquez sur **Next**.

   Le système affiche une page récapitulative avec les modifications indiquées en caractères gras.
5. Cliquez sur **Finish**.

   Le système affiche la mention Disabled en regard du Mode dans le volet Active Directory/Kerberos Authentication.

Affichage des informations d'authentification par groupe de travail

Utilisez le volet Workgroup Authentication pour afficher les informations relatives à la configuration d'un groupe de travail.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.
2. Développez le volet Workgroup Authentication.

Tableau 44 Description des libellés d'authentification par groupe de travail

Élément	Description
Mode	Type de mode d'authentification (groupe de travail ou Active Directory).
Workgroup name	Groupe de travail spécifié.
CIFS Server Name	Nom du serveur CIFS utilisé.
WINS Server	Nom du serveur WINS utilisé.

Configuration des paramètres d'authentification par groupe de travail

Les paramètres d'authentification par groupe de travail permettent de configurer un nom de groupe de travail et un nom de serveur CIFS.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet Workgroup Authentication.
3. Cliquez sur **Configure**.

   La boîte de dialogue Workgroup Authentication s'affiche.

4. Pour le nom du groupe de travail, sélectionnez **Manual**, puis saisissez un nom de groupe de travail à associer, ou utilisez la valeur par défaut.

   Le mode Groupe de travail associe un système Data Domain à un domaine de groupe de travail.

5. Pour le nom du serveur CIFS, sélectionnez **Manual**, puis saisissez un nom de serveur (DDR), ou utilisez la valeur par défaut.
6. Cliquez sur **OK**.

Affichage des informations d'authentification LDAP

Le volet LDAP Authentication affiche les paramètres de configuration LDAP et indique si l'authentification LDAP est activée ou non.

L'activation de LDAP vous permet d'utiliser un serveur ou un déploiement OpenLDAP existant avec le système Data Domain pour l'authentification utilisateur au niveau système, le mappage ID NFSv4, NFSv3 Kerberos avec LDAP ou NFSv4 Kerberos avec LDAP.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification LDAP.

Résultats

Tableau 45 Éléments du volet LDAP Authentication

Élément	Description
LDAP Status	Activé ou Désactivé
Base Suffix	Suffixe de base LDAP.
Bind DN	Nom du compte associé au serveur LDAP.
SSL	Activé ou Désactivé
Server	Serveur(s) d'authentification.
Groupe LDAP	Nom du groupe LDAP.
Management Role	Rôle du groupe (administrateur, utilisateur, etc.).

Activation et désactivation de l'authentification LDAP

Utilisez le panneau d'authentification LDAP pour activer, désactiver ou réinitialiser l'authentification LDAP.

Procédure

1. Sélectionnez **Maintenance** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification LDAP.
3. Cliquez sur **Enable** en regard de l'état LDAP pour activer ou sur **Disable** pour désactiver l'authentification LDAP.

   La boîte de dialogue Enable/Disable LDAP authentication s'affiche.

   Remarque

   Un serveur LDAP doit exister avant d'activer l'authentification LDAP.

4. Cliquez sur **OK**.

Réinitialisation de l'authentification LDAP.

Le bouton **Reset** désactive l'authentification LDAP et efface les informations de configuration LDAP.

Configuration de l'authentification LDAP

Utilisez le panneau d'authentification LDAP pour configurer l'authentification LDAP.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification LDAP.
3. Cliquez sur **Configure**.

   La boîte de dialogue Configure LDAP Authentication s'affiche.

4. Spécifiez le suffixe de base dans le champ **Base Suffix**.
5. Spécifiez le nom du compte à associer au serveur LDAP dans le champ **Bind DN**.
6. Spécifiez le mot de passe pour le compte Bind DN dans le champ **Bind Password**.
7. Vous pouvez aussi sélectionner **Enable SSL**.
8. Si vous le souhaitez, sélectionnez **Demand server certificate** pour demander au système Data Domain d'importer un certificat CA à partir du serveur LDAP.
9. Cliquez sur **OK**.
10. Si nécessaire, cliquez ultérieurement sur **Reset** pour rétablir les valeurs par défaut de la configuration LDAP.

Spécification des serveurs d'authentification LDAP

Utilisez le volet LDAP Authentication pour spécifier des serveurs d'authentification LDAP.

Avant de commencer

L'authentification LDAP doit être désactivée avant de configurer un serveur LDAP.

Remarque

Les performances de DD SM lors de la connexion avec LDAP diminuent à mesure que le nombre de hops entre le système Data Domain et le serveur LDAP augmente.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification LDAP.
3. Cliquez sur le bouton **+** pour ajouter un serveur.
4. Spécifiez le serveur LDAP dans l'un des formats suivants :
   - Adresse IPv4 : `10.26.16.250`
   - Adresse IPv6 : `[ ::ffff:9.53.96.21]`
   - Nom d'hôte : `myldapserver`
5. Cliquez sur **OK**.

Configuration des groupes LDAP

Utilisez le panneau d'authentification LDAP pour configurer les groupes LDAP.

La configuration du groupe LDAP s'applique uniquement lorsque vous utilisez LDAP pour l'authentification utilisateur sur le système Data Domain.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification LDAP.
3. Configurez les groupes LDAP dans le tableau LDAP Group.

- Pour ajouter un groupe LDAP, cliquez sur Add (**+**), saisissez le nom de groupe LDAP et le rôle, puis cliquez sur **OK**.
- Pour modifier un groupe LDAP, cochez la case correspondant au nom du groupe LDAP dans la liste des groupes LDAP, puis cliquez sur Edit (crayon). Modifiez le nom du groupe LDAP, puis cliquez sur **OK**.
- Pour supprimer un nom de groupe LDAP, sélectionnez le groupe dans la liste, puis cliquez sur Delete **X**.

Utilisation de l'interface de ligne de commande (CLI) pour configurer l'authentification LDAP

Vous pouvez utiliser l'interface de ligne de commande Data Domain pour configurer un serveur OpenLDAP existant ou un déploiement avec un système Data Domain pour l'authentification utilisateur au niveau système, le mappage ID NFSv4, NFSv3 Kerberos avec LDAP ou NFSv4 Kerberos avec LDAP.

Configurer des serveurs LDAP

Vous pouvez configurer un ou plusieurs serveurs LDAP en même temps.

Remarque

LDAP doit être désactivé lorsque vous apportez des modifications à la configuration.

Spécifiez le serveur LDAP dans l'un des formats suivants :

- adresse IPv4 : `10.<A>.<B>.<C>`
- Adresse IPv4 avec un numéro de port : `10.<A>.<B>.<C>:400`
- Adresse IPv6 : `[ ::ffff:9.53.96.21]`
- Adresse IPv6 avec un numéro de port : `[::ffff:9.53.96.21]:400`
- Nom d'hôte : `myldapserver`
- Nom d'hôte avec un numéro de port : `myldapserver:400`

Lorsque vous configurez plusieurs serveurs :

- Séparez chaque serveur par un espace.
- Le premier serveur répertorié lors de l'utilisation de la commande `authentication ldap servers add` devient le serveur primaire.
- Si un des serveurs ne peut pas être configuré, la commande échoue pour tous les serveurs répertoriés.

Procédure

1. Ajoutez un ou plusieurs serveurs LDAP en utilisant la commande `authentication ldap servers add`:

```
# authentication ldap servers add 10.A.B.C 10.X.Y.Z:400
LDAP server(s) added
LDAP Server(s):        2
#     IP Address/Hostname
---   --------------------
1.    10.A.B.C (primary)
2.    10.X.Y.Z:400
---   --------------------
```

2. Supprimez un ou plusieurs serveurs LDAP en utilisant la commande `authentication ldap servers del`:

```
# authentication ldap servers del 10.X.Y.Z:400
LDAP server(s) deleted.
```

```
LDAP Servers: 1
#   Server
-   ------------   ---------
1   10.A.B.C       (primary)
-   ------------   ---------
```

3. Supprimez tous les serveurs LDAP en utilisant la commande `authentication ldap servers reset` :

```
# authentication ldap servers reset
LDAP server list reset to empty.
```

Configurer le suffixe de base LDAP

Le suffixe de base est le nom unique de base pour la recherche, dans lequel l'annuaire LDAP commence la recherche.

Procédure

1. Définissez le suffixe de base LDAP à l'aide de la commande `authentication ldap base set` :

```
# authentication ldap base set "dc=anvil,dc=team"
LDAP base-suffix set to "dc=anvil,dc=team".
```

2. Réintialisez le suffixe de base LDAP à l'aide de la commande `authentication ldap base reset` :

```
# authentication ldap base reset
LDAP base-suffix reset to empty.
```

Configurer l'authentification du client LDAP

Configurez le compte (Bind DN) et le mot de passe (Bind PW) utilisés pour s'authentifier auprès du serveur LDAP et effectuer des requêtes.

Vous devez toujours configurer le nom unique et le mot de passe de liaison. En règle générale, lles serveurs LDAP nécessitent une liaison authentifiée par défaut. Si `client-auth` n'est pas défini, l'accès anonyme est demandé, sans fournir de nom ou de mot de passe. Le résultat de `authentication ldap show` est le suivant :

```
# authentication ldap show
LDAP configuration
        Enabled:         yes (*)
        Base-suffix:     dc=u2,dc=team
        Binddn:          (anonymous)
        Server(s):       1
#   Server
-   -------------   ---------
1   10.207.86.160   (primary)
-   -------------   ---------

Secure LDAP configuration
        SSL Enabled:     no
        SSL Method:      off
        tls_reqcert:     demand

(*) Requires a filesystem restart for the configuration to take
effect.
```

Si binddn est défini à l'aide de la CLI `client-auth`, mais bindpw n'est pas fourni, un accès non authentifié est demandé.

```
# authentication ldap client-auth set binddn
"cn=Manager,dc=u2,dc=team"
Enter bindpw:
```

```
** Bindpw is not provided. Unauthenticated access would be requested.
LDAP client authentication binddn set to "cn=Manager,dc=u2,dc=team".
```

Procédure

1. Définissez le nom unique et le mot de passe de liaison à l'aide de la commande `authentication ldap client-auth set binddn` :

```
# authentication ldap client-auth set binddn
"cn=Administrator,cn=Users,dc=anvil,dc=team"
    Enter bindpw:
    LDAP client authentication binddn set to
"cn=Administrator,cn=Users,dc=anvil,dc=team".
```

2. Réinitialisez le nom unique et le mot de passe de liaison à l'aide de la commande `authentication ldap client-auth reset` :

```
# authentication ldap client-auth reset
LDAP client authentication configuration reset to empty.
```

Activer le protocole LDAP

Avant de commencer

Une configuration LDAP doit exister avant d'activer LDAP. En outre, vous devez désactiver NIS, vous assurer que le serveur LDAP est accessible et être en mesure d'interroger le DSE racine du serveur LDAP.

Procédure

1. Activez le protocole LDAP en utilisant la commande `authentication ldap enable` :

```
# authentication ldap enable
```

Les détails de la configuration LDAP sont affichés pour que vous puissiez confirmer avant de continuer. Pour continuer, saisissez **`yes`** et redémarrez le système de fichiers pour que la configuration LDAP prenne effet.

2. Affichez la configuration LDAP en cours à l'aide de la commande `authentication ldap show` :

```
# authentication ldap show
LDAP configuration
        Enabled:         no
        Base-suffix:     dc=anvil,dc=team
        Binddn:
cn=Administrator,cn=Users,dc=anvil,dc=team
        Server(s):       2
#   Server
-   ---------------   ---------
1   10.26.16.250      (primary)
2   10.26.16.251:400
-   ---------------   ---------

Secure LDAP configuration
        SSL Enabled:     no
        SSL Method:      off
        tls_reqcert:     demand
```

Les détails de la configuration LDAP de base et de la configuration LDAP sécurisée sont affichés.

3. Affichez l'état LDAP en cours à l'aide de la commande `authentication ldap status` :

```
# authentication ldap status
```

L'état LDAP s'affiche. Si l'état LDAP n'est pas `good`, le problème est identifié dans la sortie. Par exemple :

```
# authentication ldap status
Status: invalid credentials
```

ou

```
# authentication ldap status
Status: invalid DN syntax
```

4. Désactivez le protocole LDAP en utilisant la commande `authentication ldap disable` :

```
# authentication ldap disable
LDAP is disabled.
```

Activer LDAP sécurisé

Vous pouvez configurer DDR pour utiliser le protocole LDAP sécurisé en activant SSL.

Avant de commencer

S'il n'existe aucun certificat d'autorité de certification LDAP et que `tls_reqcert` est défini sur `demand`, l'opération échoue. Importez un certificat d'autorité de certification LDAP et réessayez.

Si `tls_reqcert` est défini sur `never`, un certificat d'autorité de certification LDAP n'est pas requis. Pour plus d'informations, reportez-vous à la section Configurer la vérification des certificats de serveur LDAP avec des certificats d'autorité de certification importés à la page 136.

Procédure

1. Activez SSL en utilisant la commande `authentication ldap ssl enable` :

```
# authentication ldap ssl enable
Secure LDAP is enabled with 'ldaps' method.
```

La méthode par défaut est LDAP sécurisé, ou *ldaps*. Vous pouvez spécifier d'autres méthodes, telle que TLS :

```
# authentication ldap ssl enable method start_tls
Secure LDAP is enabled with 'start_tls' method.
```

2. Désactivez SSL en utilisant la commande `authentication ldap ssl disable` :

```
# authentication ldap ssl disable
Secure LDAP is disabled.
```

Configurer la vérification des certificats de serveur LDAP avec des certificats d'autorité de certification importés

Vous pouvez modifier le comportement du certificat de demande TLS

Procédure

1. Modifiez le comportement du certificat de demande TLS en utilisant la commande `authentication ldap ssl set tls_reqcert`.

Ne vérifiez pas le certificat :

```
# authentication ldap ssl set tls_reqcert never
"tls_reqcert" set to "never". LDAP server certificate will not
be verified.
```

Vérifiez le certificat :

```
# authentication ldap ssl set tls_reqcert demand
“tls_reqcert” set to "demand". LDAP server certificate will be
verified.
```

2. Réintialisez le comportement du certificat de demande TLS en utilisant la commande `authentication ldap ssl reset tls_reqcert.demand` est le comportement par défaut :

```
# authentication ldap ssl reset tls_reqcert
tls_reqcert has been set to "demand". LDAP Server certificate
will be verified with imported CA certificate.Use "adminaccess"
CLI to import the CA certificate.
```

Gérer les certificats CA pour LDAP

Vous pouvez importer ou supprimer des certificats et afficher des informations sur le certificat en cours.

Procédure

1. Importez un certificat CA pour la vérification du certificat de serveur LDAP à l’aide de la commande `adminaccess certificate import`.

   Spécifiez `ldap` pour `ca application` :

```
# adminaccess certificate import{host application {all | aws-
federal | ddboost | https| keysecure | rkm | <application-
list>}| ca application { ldap }} [file <file-name>] Import host
or ca certificate
```

2. Supprimer un certificat CA pour la vérification du certificat de serveur LDAP à l’aide de la commande `adminaccess certificate delete`.

   Spécifiez `ldap` pour `application` :

```
# adminaccess certificate delete
{ subject <subject-name> | fingerprint <fingerprint>}
[application { ldap }]
```

   Spécifiez `ldap` pour `imported-ca application` :

```
# adminaccess certificate delete
{ imported-host application { all | aws-federal | ddboost |
https
| keysecure | rkm | <application-list>}
| imported-ca application { ldap }}
```

3. Affichez les informations en cours du certificat CA pour la vérification du certificat du serveur LDAP à l’aide de la commande `adminaccess certificate show`.

```
# adminaccess certificate show imported-ca ldap
```

Affichage des informations d’authentification NIS

Le volet NIS Authentication affiche les paramètres de configuration NIS et indique si l’authentification NIS est activée ou non.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s’affiche.

2. Développez le volet d’authentification NIS.

Résultats

Tableau 46 Éléments du volet NIS Authentication

Élément	Description
NIS Status	Activé ou Désactivé
Domain Name	Nom du domaine pour ce service.
Server	Serveur(s) d'authentification.
NIS Group	Nom du groupe NIS.
Management Role	Rôle du groupe (administrateur, utilisateur, etc.).

Activation et désactivation de l'authentification NIS

Utilisez le volet NIS Authentication pour activer et désactiver l'authentification NIS.

Procédure

1. Sélectionnez **Maintenance** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification NIS.
3. Cliquez sur **Enable** en regard de l'état NIS pour activer l'authentification NIS ou sur **Disable** pour la désactiver.

   La boîte de dialogue Enable or Disable NIS s'affiche.

4. Cliquez sur **OK**.

Configuration du nom de domaine NIS

Utilisez le volet NIS Authentication pour configurer le nom de domaine NIS.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification NIS.
3. Cliquez sur **Edit** en regard du nom de domaine NIS pour le modifier.

   La boîte de dialogue Configure NIS Domain Name s'affiche.

4. Entrez le nom de domaine dans la zone **Domain Name**.
5. Cliquez sur **OK**.

Spécification des serveurs d'authentification NIS

Utilisez le volet NIS Authentication pour spécifier des serveurs d'authentification NIS.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.

2. Développez le volet d'authentification NIS.

3. Sous Domain Name, sélectionnez l'une des options suivantes :
   - **Obtain NIS Servers from DHCP** Le système obtient automatiquement des serveurs NIS avec DHCP
   - **Manually Configure** Utilisez les procédures suivantes pour configurer manuellement des serveurs NIS.
   - Pour ajouter un serveur d'authentification, cliquez sur Add (**+**) dans le tableau des serveurs, saisissez le nom du serveur, puis cliquez sur **OK**.
   - Pour modifier un serveur d'authentification, sélectionnez le nom du serveur d'authentification, puis cliquez sur l'icône de modification (crayon). Modifiez le nom du serveur, puis cliquez sur **OK**.
   - Pour supprimer un nom de serveur d'authentification, sélectionnez un serveur, cliquez sur l'icône X, puis cliquez sur **OK**.
4. Cliquez sur **OK**.

Configuration des groupes NIS

Utilisez le volet NIS Authentication pour configurer des groupes NIS.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**.

   La vue Authentication s'affiche.
2. Développez le volet d'authentification NIS.
3. Configurez les groupes NIS dans le tableau NIS Group.
   - Pour ajouter un groupe NIS, cliquez sur Add (**+**), saisissez le nom de groupe NIS et le rôle, puis sélectionnez **Validate**. Cliquez sur **OK** pour fermer la boîte de dialogue d'ajout de groupe NIS. Cliquez à nouveau sur **OK** pour fermer la boîte de dialogue **Configure Allowed NIS Groups**.
   - Pour modifier un groupe NIS, cochez la case correspondant au nom du groupe NIS dans la liste des groupes NIS, puis cliquez sur Edit (crayon). Modifiez le nom du groupe NIS, puis cliquez sur **OK**.
   - Pour supprimer un nom de groupe NIS, sélectionnez le groupe dans la liste, puis cliquez sur Delete **X**.
4. Cliquez sur **OK**.

Diagnostic des problèmes d'authentification

Data Domain Operating System permet de diagnostiquer les problèmes d'authentification d'Active Directory à partir de l'interface Data Domain System Manager.

Procédure

1. Sélectionnez **Administration** > **Access** > **Authentication**
2. Développez le volet Active Directory/Kerberos Authentication.
3. Cliquez sur **Diagnose**.
4. Sélectionnez un problème à examiner, puis cliquez sur **Diagnose**.
5. Saisissez les informations demandées.

   Pour diagnostiquer les problèmes de connexion en tant qu'utilisateur Active Directory, spécifiez les informations suivantes :

- Adresse IP du serveur Active Directory
- Nom de domaine complet du serveur Active Directory
- Nom d'utilisateur du service Active Directory

Remarque

Le compte utilisateur Active Directory spécifié ici nécessite les privilèges suivants :

- Accès en lecture seule au nom unique de base identifié par le nom de domaine.
- Accès en lecture seule aux attributs de requête de tous les utilisateurs compris dans le nom unique de base.
- Accès en lecture seule aux attributs de requête du compte d'ordinateur pour le système Data Domain.

- Mot de passe Active Directory manquant
- Nom d'utilisateur Data Domain rencontrant un échec de la connexion

Pour diagnostiquer les problèmes liés à l'intégration du système Data Domain à un domaine Active Directory, spécifiez les informations suivantes :

- Adresse IP du serveur Active Directory
- Nom de domaine complet du serveur Active Directory
- Nom d'utilisateur du service Active Directory
- Mot de passe Active Directory manquant

6. Cliquez sur **Diagnose**.
7. Affichez le rapport.
   - Cliquez sur **View Report** pour consulter le rapport en ligne. Vous pouvez cliquer sur chaque élément du tableau Action Items pour obtenir plus de détails.
   - Cliquez sur **Download** pour télécharger une copie du rapport.
8. Examinez et implémentez les correctifs suggérés pour le problème et réessayez l'opération.

Modifier la méthode d'authentification du système

Le système Data Domain prend en charge l'authentification par mot de passe ou par certificat. L'authentification par mot de passe est la méthode par défaut.

Avant de commencer

L'authentification par certificat nécessite des clés SSH et des certificats CA sont importés pour permettre aux utilisateurs de s'authentifier auprès du système lorsque l'authentification par mot de passe est désactivée.

Effectuez les étapes suivantes pour passer de l'authentification par mot de passe à l'authentification par certificat.

Procédure

1. Sélectionnez **Administration** > **Access**.

   La vue Access Management s'affiche.

2. Cliquez sur **Manage CA Certificates**.
3. Cliquez sur **Add** pour créer un nouveau certificat.
4. Ajoutez le certificat.
   - Sélectionnez **I want to upload the certificate as a .pem file**, puis cliquez sur **Choose File** pour sélectionner le fichier de certificat et le télécharger dans le système.
   - Sélectionnez **I want to copy and paste the certificate text** pour copier-coller le texte du certificat dans le champ de texte.
5. Cliquez sur **Add**.
6. Sélectionnez **More Tasks** > **Change Login Options**.
7. Dans le menu déroulant **Password Based Login**, sélectionnez **Disable**.

   Remarque

   Le menu déroulant est désactivé si les clés SSH et les certificats CA requis ne sont pas configurés sur le système.

8. Cliquez sur **OK**.

   Si une politique de sécurité est configurée, le système demande les informations d'identification du responsable de la sécurité. Spécifiez les informations d'identification, puis cliquez sur **OK**.

Réinitialiser la méthode d'authentification du système sur l'authentification par mot de passe

Effectuez les étapes suivantes pour passer de l'authentification par certificat à l'authentification par mot de passe.

Procédure

1. Sélectionnez **Administration** > **Access**.

   La vue Access Management s'affiche.

2. Sélectionnez **More Tasks** > **Change Login Options**.
3. Dans le menu déroulant **Password Based Login**, sélectionnez **Enable**.
4. Cliquez sur **OK**.

   Si une politique de sécurité est configurée, le système demande les informations d'identification du responsable de la sécurité. Spécifiez les informations d'identification, puis cliquez sur **OK**.

Configuration des paramètres du serveur de messagerie

L'onglet Mail Server permet de spécifier le serveur de messagerie auquel DD OS transmet des rapports par e-mail.

Procédure

1. Sélectionnez **Administration** > **Settings** > **Mail Server**.
2. Sélectionnez **More Tasks** > **Set Mail Server**.

   La boîte de dialogue Set Mail Server s'affiche.

3. Spécifiez le nom du serveur de messagerie dans le champ **Mail Server**.

4. Utilisez le bouton **Credentials** pour activer ou désactiver l'utilisation des informations d'identification pour le serveur de messagerie.
5. Si les informations d'identification sont activées, spécifiez le nom d'utilisateur du serveur de messagerie dans le champ **User Name**.
6. Si les informations d'identification sont activées, spécifiez le mot de passe du serveur de messagerie dans le champ **Password**.
7. Cliquez sur **Set**.
8. Vous pouvez également utiliser l'interface CLI pour vérifier et dépanner la configuration du serveur de messagerie.
   a. Exécutez la commande `config show mailserver` pour vérifier que le serveur de messagerie est configuré.
   b. Exécutez la commande `net ping <mailserver-hostname> count 4` pour envoyer un ping au serveur de messagerie.
   c. Si le serveur de messagerie n'est pas configuré correctement, exécutez la commande `config set mailserver <mailserver-hostname>` pour configurer le serveur de messagerie, puis tentez à nouveau d'envoyer un ping.
   d. Exécutez la commande `net show dns` pour vérifier que le serveur DNS est configuré.
   e. Exécutez la commande `net ping <DNS-hostname> count 4` pour envoyer un ping au serveur DNS.
   f. Si le serveur DNS n'est pas configuré correctement, exécutez la commande `config set dns <dns-IP>` pour configurer le serveur DNS, puis tentez à nouveau d'envoyer un ping.
   g. Vous pouvez aussi exécuter la commande `net hosts add <IP-address> <hostname>` pour ajouter l'adresse IP et le nom d'hôte du serveur de messagerie au fichier d'hôtes Data Domain pour une résolution locale.
   h. Exécutez la commande `net ping <mailserver-hostname> count 4` pour envoyer un ping au serveur de messagerie.

Gestion des paramètres de date et d'heure

L'onglet Time and Date Settings permet de connaître et de configurer la date et l'heure du système ou de configurer le protocole NTP en vue de définir la date et l'heure.

Procédure

1. Pour afficher la configuration actuelle pour l'heure et la date, sélectionnez **Administration** > **Settings** > **Time and Date Settings**.

   La page Time and Date Settings présente la date et l'heure actuelles du système, indique si NTP est activé ou non, et répertorie les adresses IP ou les noms d'hôte des serveurs NTP configurés.

2. Pour changer la configuration, sélectionnez **More Tasks** > **Configure Time Settings**.

   La boîte de dialogue Configure Time Settings s'affiche.

3. Dans la liste déroulante **Time Zone**, sélectionnez le fuseau horaire auquel le système Data Domain appartient.

4. Pour définir manuellement l'heure et la date, sélectionnez **None**, entrez la date dans la zone **Date**, puis sélectionnez l'heure dans les listes déroulantes **Time**.
5. Pour synchroniser l'heure à l'aide du protocole NTP, sélectionnez NTP et définissez le mode d'accès au serveur NTP.
   - Pour sélectionner automatiquement un serveur à l'aide du protocole DHCP, sélectionnez **Obtain NTP Servers using DHCP**.
   - Pour configurer une adresse IP d'un serveur NTP, sélectionnez **Manually Configure**, ajoutez l'adresse IP du serveur, puis cliquez sur **OK**.

   Remarque

   L'utilisation de la synchronisation horaire d'un contrôleur de domaine Active Directory peut entraîner des modifications horaires excessives sur le système si le protocole NTP et le contrôleur de domaine modifient tous deux l'heure.
6. Cliquez sur le bouton **OK**.
7. Si vous avez modifié le fuseau horaire, vous devez redémarrer le système.
   a. Sélectionnez **Maintenance** > **System**.
   b. Dans le menu More Tasks, sélectionnez Reboot System.
   c. Cliquez sur OK pour confirmer.

Gestion des propriétés système

L'onglet System Properties permet d'afficher et de configurer les propriétés système (emplacement du système géré, adresse e-mail de l'administrateur, nom d'hôte, etc.).

Procédure

1. Pour afficher la configuration en cours, sélectionnez **Administration** > **Settings** > **System Properties**.

   L'onglet System Properties affiche l'emplacement du système, l'adresse e-mail et le nom d'hôte de l'administrateur.
2. Pour changer la configuration, sélectionnez **More Tasks** > **Set System Properties**.

   La boîte de dialogue Set System Properties s'affiche.
3. Dans la zone **Location**, entrez les informations sur l'emplacement du système Data Domain.
4. Dans la zone **Admin Email**, saisissez l'adresse e-mail de l'administrateur système.
5. Dans la zone **Admin Host**, entrez le nom du serveur d'administration.
6. Cliquez sur **OK**.

Gestion de SNMP

SNMP (Simple Network Management Protocol) est un protocole standard d'échange d'informations de gestion réseau qui fait partie de la suite de protocoles TCP/IP (Transmission Control Protocol/Internet Protocol). Pour les administrateurs réseau, le protocole SNMP est un outil qui leur permet de surveiller et de gérer les périphériques

rattachés au réseau, par exemple les systèmes Data Domain, en cas de problème nécessitant leur attention.

Pour surveiller des systèmes Data Domain à l'aide de SNMP, vous devez installer la base de données MIB Data Domain dans votre système de gestion SNMP. DD OS prend également en charge la base de données MIB-II standard. Vous pouvez ainsi interroger les statistiques MIB-II à la recherche de données générales, telles que les statistiques sur le réseau. Pour couvrir toutes les données disponibles, vous devez utiliser les deux bases de données MIB Data Domain et MIB-II standard.

L'agent SNMP du système Data Domain accepte les requêtes pour des informations spécifiques à Data Domain à partir des systèmes de gestion utilisant SNMP v1, v2c et v3. SNMP V3 fournit un niveau de sécurité supérieur à v2c et v1 en remplaçant les chaînes de communauté libellées en texte clair (utilisée pour l'authentification) par une authentification utilisateur via MD5 ou SHA1. Avec SNMP v3, les paquets d'authentification utilisateur peuvent aussi être chiffrés et leur intégrité peut être vérifiée avec DES ou AES.

Les systèmes Data Domain peuvent envoyer des traps SNMP (qui sont des messages d'alerte) à l'aide de SNMP v2c et SNMP v3. Puisque les traps SNMP v1 ne sont pas pris en charge, utilisez, si possible, SNMP v2c et v3.

Le port ouvert par défaut lorsque SNMP est activé est le port 161. Les traps sont envoyées via le port 162

- Le document *Guide de configuration initiale de Data Domain Operating System* décrit comment configurer le système Data Domain pour utiliser la surveillance SNMP.
- Le *Guide de référence de la base de données MIB Data Domain Operating System* décrit l'ensemble des paramètres MIB inclus dans le secteur Data Domain MIB.

Affichage de l'état et de la configuration SNMP

L'onglet SNMP indique l'état et la configuration SNMP en cours.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.

   La vue SNMP affiche l'état SNMP, les propriétés SNMP, la configuration SNMP V3 et la configuration SNMP V2C.

Libellés de l'onglet SNMP

Les libellés de l'onglet SNMP affichent l'état général SNMP, les valeurs des propriétés SNMP et les configurations pour SNMPv3 et SNMPv2.

État

La zone Status indique si l'agent SNMP est activé (Enabled) ou désactivé (Disabled) sur le système.

Propriétés du SNMP

Tableau 47 Description des propriétés SNMP

Élément	Description
SNMP System Location	Emplacement du système Data Domain surveillé.
SNMP System Contact	Personne désignée comme la personne à contacter pour l'administration du système Data Domain.
SNMP System Notes	(Facultatif) Données de configuration SNMP supplémentaires.

Tableau 47 Description des propriétés SNMP (suite)

Élément	Description
SNMP Engine ID	Identifiant hexadécimal unique pour le système Data Domain.

Configuration de SNMP V3

Tableau 48 Description des colonnes SNMP Users

Élément	Description
Name	Nom de l'utilisateur sur le gestionnaire SNMP ayant accès à l'agent pour le système Data Domain.
Access	Autorisations d'accès pour l'utilisateur SNMP, qui peut être accessible en lecture seule ou en lecture/écriture.
Authentication Protocols	Protocole d'authentification utilisé pour valider l'utilisateur SNMP, qui peut être MD5, SHA1 ou None.
Privacy Protocol	Protocole de chiffrement utilisé lors de l'authentification de l'utilisateur SNMP, qui peut être AES, DES ou None.

Tableau 49 Description des colonnes d'hôtes de trap

Élément	Description
Host	Nom de domaine ou adresse IP de l'hôte de gestion SNMP.
Port	Port utilisé pour la communication de trap SNMP avec l'hôte. Par exemple, 162 est le port par défaut.
User	Utilisateur de l'hôte de trap authentifié pour accéder aux informations relatives à SNMP Data Domain.

Configuration de SNMP V2C

Tableau 50 Description des colonnes de communautés

Élément	Description
Community	Nom de la communauté. Par exemple, public, private ou localCommunity.
Access	Autorisation d'accès attribuée ; peut être un accès en lecture seule ou en lecture/écriture.
Hosts	Hôtes de cette communauté.

Tableau 51 Description des colonnes d'hôtes de trap

Élément	Description
Host	Systèmes désignés pour recevoir les traps SNMP générées par le système Data Domain. Si ce paramètre est défini, les systèmes reçoivent des messages d'alerte même si l'agent SNMP est désactivé.

Tableau 51 Description des colonnes d'hôtes de trap (suite)

Élément	Description
Port	Port utilisé pour la communication de trap SNMP avec l'hôte. Par exemple, 162 est le port par défaut.
Community	Nom de la communauté. Par exemple, public, private ou localCommunity.

Activation et désactivation de SNMP

Utilisez l'onglet SNMP pour activer ou désactiver SNMP.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone Status, cliquez sur **Enable** ou **Disable**.

Téléchargement de la base de données MIB SNMP

Utilisez l'onglet SNMP pour télécharger la base de données MIB SNMP.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Cliquez sur **Download MIB file**.
3. Dans la boîte de dialogue Opening DATA_DOMAIN.mib, sélectionnez **Open**.
4. Cliquez sur **Browse** et sélectionnez un navigateur pour afficher la base de données MIB dans une fenêtre de navigateur.

   Remarque

   Si vous utilisez le navigateur Microsoft Internet Explorer, activez l'option Demander confirmation pour les téléchargements des fichiers.

5. Sauvegardez la base de données MIB ou quittez le navigateur.

Configuration des propriétés SNMP

Utilisez l'onglet SNMP pour configurer les entrées de texte pour un emplacement et un contact de système.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone SNMP Properties, cliquez sur **Configure**.

   La boîte de dialogue SNMP Configuration s'affiche.

3. Dans les champs de texte, spécifiez les informations suivantes :
   - SNMP System Location : description de l'emplacement du système Data Domain.
   - SNMP System Contact : adresse e-mail de l'administrateur système du système Data Domain.

- SNMP System Notes : (facultatif) informations de configuration SNMP supplémentaires.
- SNMP Engine ID : Identifiant unique pour l'entité SNMP. L'ID du moteur doit comporter entre 5 et 34 caractères hexadécimaux (SNMPv3 uniquement).

Remarque

Le système affiche un message d'erreur si l'ID du moteur SNMP ne répond pas aux exigences de longueur, ou utilise des caractères non valides.

4. Cliquez sur **OK**.

Gestion des utilisateurs SNMP V3

Utilisez l'onglet SNMP pour créer, modifier et supprimer des utilisateurs et des hôtes de trap SNMPv3.

Création d'utilisateurs SNMP V3

Pour créer un utilisateur SNMPv3, vous définissez un nom d'utilisateur, choisissez le type d'accès (lecture seule ou lecture-écriture) et sélectionnez un protocole d'authentification.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone SNMP Users, cliquez sur **Create**.

   La boîte de dialogue Create SNMP User s'affiche.

3. Dans la zone de texte **Name**, entrez le nom de l'utilisateur auquel vous souhaitez accorder un accès à l'agent du système Data Domain. Le nom doit comporter 8 caractères minimum.
4. Sélectionnez un accès en lecture seule ou en lecture/écriture pour cet utilisateur.
5. Pour authentifier l'utilisateur, sélectionnez **Authentication**.
   a. Sélectionnez le protocole MD5 ou SHA1.
   b. Entrez la clé d'authentification dans la zone de texte **Key**.
   c. Pour activer le chiffrement de la session d'authentification, sélectionnez **Privacy**.
   d. Sélectionnez le protocole AES ou DES.
   e. Entrez la clé d'authentification dans la zone de texte **Key**.
6. Cliquez sur **OK**.

   Le compte utilisateur qui vient d'être ajouté apparaît dans le tableau d'utilisateurs SNMP.

Modification des utilisateurs SNMP V3

Vous pouvez changer le niveau d'accès (lecture seule ou lecture-écriture) et le protocole d'authentification des utilisateurs SNMPv3 existants.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone **SNMP Users**, cochez la case relative à l'utilisateur, puis cliquez sur **Modify**.

   La boîte de dialogue Modify SNMP User s'affiche. Ajoutez ou modifiez l'un des paramètres ci-après.

3. Sélectionnez un accès en lecture seule ou en lecture/écriture pour cet utilisateur.
4. Pour authentifier l'utilisateur, sélectionnez **Authentication**.
   a. Sélectionnez le protocole MD5 ou SHA1.
   b. Entrez la clé d'authentification dans la zone de texte Key.
   c. Pour activer le chiffrement de la session d'authentification, sélectionnez **Privacy**.
   d. Sélectionnez le protocole AES ou DES.
   e. Entrez la clé d'authentification dans la zone de texte **Key**.
5. Cliquez sur **OK**.

   Les nouveaux paramètres pour ce compte utilisateur s'affichent dans le tableau des utilisateurs SNMP.

Suppression d'utilisateurs SNMP V3

Utilisez l'onglet SNMP pour supprimer des utilisateurs SNMPv3.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone SNMP Users, cochez la case associée à un utilisateur et cliquez sur **Delete**.

   La boîte de dialogue Delete SNMP User s'affiche.

   Remarque

   Si le bouton **Delete** est désactivé, cela signifie que l'utilisateur sélectionné est utilisé par un ou plusieurs hôtes de notification. Supprimez les hôtes de notification, puis supprimez l'utilisateur.

3. Vérifiez le nom de l'utilisateur à supprimer et cliquez sur **OK**.
4. Dans la boîte de dialogue Delete SNMP User Status, cliquez sur **Close**.

   Le compte utilisateur est supprimé du tableau des utilisateurs SNMP.

Gestion des communautés SNMP V2C

Définissez des communautés SNMP v2c (faisant office de mots de passe) pour contrôler l'accès du système de gestion au système Data Domain. Pour restreindre l'accès à des hôtes spécifiques tirant parti de la communauté spécifiée, allouez les hôtes à la communauté.

Remarque

La chaîne SNMP V2c Community est envoyée en texte clair et est très facile à intercepter. Si cela se produit, l'intercepteur peut récupérer des informations sur les périphériques de votre réseau, modifier leur configuration, et éventuellement les arrêter. SNMP V3 offre des fonctions d'authentification et de chiffrement pour empêcher l'interception.

Remarque

Les définitions des communautés SNMP ne permettent pas de transmettre des traps SNMP vers une station de gestion. Vous devez définir des hôtes de trap pour assurer l'envoi vers des stations de gestion.

Création de communautés SNMP V2C

Créez des communautés pour limiter l'accès au système DDR ou pour envoyer des traps à un hôte de trap. Vous devez créer une communauté et l'affecter à un hôte avant de pouvoir la sélectionner pour l'utiliser avec l'hôte de trap.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone Communities, cliquez sur **Create**.

   La boîte de dialogue Create SNMP V2C Community s'affiche.
3. Dans la zone **Community**, saisissez le nom d'une communauté à laquelle vous souhaitez octroyer l'accès à l'agent du système Data Domain.
4. Sélectionnez un accès en lecture seule ou en lecture/écriture pour cette communauté.
5. Si vous voulez associer la communauté à un ou plusieurs hôtes, ajoutez les hôtes de la façon suivante :
   a. Cliquez sur **+** pour ajouter un hôte.

      La boîte de dialogue Host s'affiche.
   b. Dans la zone de texte **Host**, saisissez l'adresse IP ou le nom de domaine de l'hôte.
   c. Cliquez sur **OK**.

      L'hôte est ajouté à la liste des hôtes.
6. Cliquez sur **OK**.

   La nouvelle entrée de communauté s'affiche dans le tableau **Communities** et répertorie les hôtes sélectionnés.

Modification des communautés SNMP V2C

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone Communities, cochez la case correspondant à la communauté, puis cliquez sur **Modify**.

   La boîte de dialogue Modify SNMP V2C Community s'affiche.

3. Pour changer le mode d'accès pour cette communauté, sélectionnez l'accès **en lecture seule** ou **en lecture-écriture**.

   Remarque

   Les boutons Access correspondant à la communauté sélectionnée sont désactivés lorsqu'un hôte de trap figurant sur le même système est configuré dans cette communauté. Pour changer le paramètre d'accès, supprimez l'hôte de trap, puis rajoutez-le après modification de la communauté.

4. Pour ajouter un ou plusieurs hôtes à cette communauté, procédez comme suit :
   a. Cliquez sur **+** pour ajouter un hôte.

      La boîte de dialogue Host s'affiche.

   b. Dans la zone de texte **Host**, saisissez l'adresse IP ou le nom de domaine de l'hôte.

   c. Cliquez sur **OK**.

      L'hôte est ajouté à la liste des hôtes.
5. Pour supprimer un ou plusieurs hôtes de la liste des hôtes, procédez comme suit :

   Remarque

   DD System Manager ne permet pas de supprimer un hôte lorsqu'un hôte de trap appartenant au même système est configuré comme membre de cette communauté. Pour supprimer un hôte de trap d'une communauté, supprimez l'hôte de trap, puis rajoutez-le après modification de la communauté.

   Remarque

   Les boutons Access correspondant à la communauté sélectionnée ne sont pas désactivés lorsque l'hôte de trap utilise une adresse IPv6 et que le système est géré par une version antérieure de DD OS qui ne prend pas en charge IPv6. Si possible, sélectionnez toujours un système de gestion qui utilise la même version ou une version de DD OS plus récente que les systèmes qu'il gère.

   a. Cochez la case correspondant à chaque hôte ou cliquez sur la case Host dans l'en-tête du tableau pour sélectionner l'ensemble des hôtes répertoriés.

   b. Cliquez sur le bouton de suppression (X).
6. Pour modifier un nom d'hôte, procédez comme suit :
   a. Cochez la case correspondant à l'hôte.

   b. Cliquez sur le bouton d'édition (icône en forme de crayon).

   c. Modifiez le nom de l'hôte.

   d. Cliquez sur **OK**.
7. Cliquez sur **OK**.

   L'entrée de communauté modifiée s'affiche dans le tableau des communautés.

Suppression de communautés SNMP V2C

Utilisez l'onglet SNMP pour supprimer des communautés SNMPv2.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone **Communities**, cochez la case correspondant à la communauté, puis cliquez sur **Delete**.

   La boîte de dialogue Delete SNMP V2C Communities s'affiche.

   Remarque

   Si le bouton **Delete** est désactivé, cela signifie que la communauté sélectionnée est utilisée par un ou plusieurs hôtes de notification. Supprimez les hôtes de notification, puis supprimez la communauté.

3. Vérifiez le nom de la communauté à supprimer et cliquez sur **OK**.
4. Dans la boîte de dialogue Delete SNMP V2C Communities Status, cliquez sur **Close**. L'entrée de la communauté est supprimée du tableau des communautés.

Gestion des hôtes de trap SNMP

Les définitions d'hôtes de trap permettent aux systèmes Data Domain d'intégrer des messages d'alerte dans des messages de trap SNMP et de les envoyer à une station de gestion SNMP.

Création d'hôtes de trap SNMP V2C et V3

Les définitions d'hôtes de trap identifient les hôtes distants qui reçoivent des messages de trap SNMP du système.

Avant de commencer

Si vous avez l'intention d'associer une communauté SNMP v2c existante à un hôte de trap, commencez pas allouer l'hôte de trap à la communauté à partir de la zone Communities.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone SNMP V3 Trap Hosts ou SNMP V2C Trap Hosts, cliquez sur **Create**.

   La boîte de dialogue Create SNMP [V3 ou V2C] Trap Hosts s'affiche.

3. Dans la zone **Host**, entrez l'adresse IP ou le nom de domaine de l'hôte SNMP auquel sont destinés les traps.
4. Dans la zone **Port**, saisissez le numéro de port pour l'envoi de traps (le port 162 est un port courant).
5. Sélectionnez l'utilisateur (SNMP V3) ou la communauté (SNMP V2C) dans le menu déroulant.

Remarque

La liste des communautés affiche uniquement les communautés auxquelles l'hôte de trap a déjà été attribué.

6. Pour créer une nouvelle communauté, procédez comme suit :
   a. Choisissez **Create New Community** dans le menu déroulant Community.
   b. Saisissez le nom de la nouvelle communauté dans la zone **Community**.
   c. Sélectionnez le type d'accès.
   d. Cliquez sur le bouton d'ajout (+).
   e. Saisissez le nom de l'hôte de trap.
   f. Cliquez sur **OK.**
   g. Cliquez sur **OK.**
7. Cliquez sur **OK**.

Modification des hôtes de trap SNMP V2C et V3

Vous pouvez modifier le numéro de port et la sélection de communautés pour des configurations d'hôte de trap existantes.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone **SNMP V3 Trap Hosts** ou **SNMP V2C Trap Hosts**, sélectionnez une entrée d'hôte de trap, puis cliquez sur **Modify**.

   La boîte de dialogue Modify SNMP [V3 or V2C] Trap Hosts s'affiche.

3. Pour modifier le numéro de port, saisissez un nouveau numéro dans la zone **Port** (le port 162 est un port courant).
4. Sélectionnez l'utilisateur (SNMP V3) ou la communauté (SNMP V2C) dans le menu déroulant.

Remarque

La liste des communautés affiche uniquement les communautés auxquelles l'hôte de trap a déjà été attribué.

5. Pour créer une nouvelle communauté, procédez comme suit :
   a. Choisissez **Create New Community** dans le menu déroulant Community.
   b. Saisissez le nom de la nouvelle communauté dans la zone **Community**.
   c. Sélectionnez le type d'accès.
   d. Cliquez sur le bouton d'ajout (+).
   e. Saisissez le nom de l'hôte de trap.
   f. Cliquez sur **OK.**
   g. Cliquez sur **OK.**
6. Cliquez sur **OK**.

Suppression d'hôtes de trap SNMP V2C et V3

Utilisez l'onglet SNMP pour supprimer des configurations d'hôtes de trap.

Procédure

1. Sélectionnez **Administration** > **Settings** > **SNMP**.
2. Dans la zone **Trap Hosts** (pour V3 ou V2C), cochez la case correspondant à l'hôte de trap, puis cliquez sur **Delete**.

   La boîte de dialogue Delete SNMP [V3 or V2C] Trap Hosts s'affiche.

3. Vérifiez le nom d'hôte à supprimer, puis cliquez sur **OK**.
4. Dans la boîte de dialogue Delete SNMP [V3 or V2C] Trap Hosts Status, cliquez sur **Close**.

   L'entrée d'hôte de trap est supprimée du tableau des **hôtes de trap**.

Gestion des rapports autosupport

La fonction autosupport génère un rapport appelé ASUP. Ce rapport présente les informations d'identification du système ainsi que les résultats consolidés issus des commandes du système Data Domain et les valeurs contenues dans divers fichiers log. Des statistiques internes complètes et détaillées apparaissent en fin de rapport. Ce rapport est conçu pour faciliter la prise en charge par le support de Data Domain des problèmes liés au système de débogage.

Un rapport ASUP est généré à chaque démarrage du système de fichiers, c'est-à-dire une fois par jour en général. Il est possible, cependant, de démarrer le système de fichiers plusieurs fois par jour.

Vous pouvez configurer des adresses e-mail pour la réception des rapports ASUP quotidiens et activer ou désactiver l'envoi de ces rapports à Data Domain. L'heure par défaut d'envoi du rapport ASUP quotidien, fixée à 06:00 du matin, est configurable. Lors de l'envoi des rapports ASUP à Data Domain, vous avez la possibilité de sélectionner la méthode non sécurisée héritée ou la méthode ConnectEMC qui permet de chiffrer les informations avant leur transmission.

Simplicité de gestion de l'autosupport du système haute disponibilité et des bundles de support

La configuration est effectuée sur le nœud actif. Elle est aussi mise en miroir sur le nœud en veille. Par conséquent, les deux nœuds possèdent la même configuration, mais ceux-ci n'ont pas un bundle de support et des rapports ASUP communs.

Outre des informations sur le nœud local, l'autosupport et le bundle de support sur le nœud actif contiennent des informations sur la réplication, le protocole et le système de fichiers ainsi que des données complètes relatives à la haute disponibilité. L'autosupport et le bundle de support sur le nœud en veille incluent uniquement des informations sur le nœud local ainsi que certaines informations relatives à la haute disponibilité (configuration et état). Ils ne vous renseignent ni sur le système de fichiers, ni sur le protocole et ni sur la réplication. L'autosupport et les bundles de support des deux nœuds sont nécessaires pour le débogage des problèmes liés à l'état du système haute disponibilité (système de fichiers, réplication, protocoles et configuration HA).

Activation et désactivation du reporting d'autosupport à Data Domain

Vous pouvez activer ou désactiver le reporting d'autosupport à Data Domain sans incidence sur les alertes envoyées à Data Domain.

Procédure

1. Pour afficher l'état du reporting d'autosupport , sélectionnez **Maintenance** > **Support** > **Autosupport**.

   L'état du reporting d'autosupport est mis en surbrillance en regard du libellé d'autosupport planifié dans la zone du Support. Selon la configuration en cours, un bouton **Enable** ou **Disable** s'affiche dans la ligne de l'autosupport planifié.
2. Pour activer le reporting de l'autosupport à Data Domain, cliquez sur **Enable** dans la ligne de l'autosupport planifié.
3. Pour désactiver le reporting de l'autosupport à Data Domain, cliquez sur **Disable** dans la ligne de l'autosupport planifié.

Vérification des rapports d'autosupport générés

Examinez les rapports autosupport pour prendre connaissance des statistiques du système et des informations de configuration précédemment capturées. Le système stocke un maximum de 14 rapports autosupport.

Procédure

1. Sélectionnez **Maintenance** > **Support** > **Autosupport**.

   La page Autosupport Reports indique la taille et le nom du fichier-rapport d'autosupport, et la date à laquelle le rapport a été généré. Les rapports sont automatiquement nommés. Le rapport le plus récent se nomme autosupport, celui généré la veille se nomme autosupport.1, et le numéro augmente au fur et à mesure que les rapports s'éloignent dans le temps.

   Équivalent CLI

   ```
   # autosupport show history
   ```

2. Cliquez sur le lien du nom de fichier pour afficher le rapport à l'aide d'un éditeur de texte. Si cela est requis par votre navigateur, téléchargez d'abord le fichier.

Configuration de la liste de diffusion d'autosupport

Les abonnés à la liste de diffusion d'autosupport reçoivent des messages relatifs à autosupport par e-mail. Utilisez l'onglet Autosupport pour ajouter, modifier et supprimer des abonnés.

Les e-mails d'autosupport sont envoyés via le serveur de messagerie configuré à tous les abonnés figurant dans la liste de publipostage d'autosupport. Une fois le serveur de messagerie et la liste de publipostage d'autosupport configurés, il est recommandé de tester la configuration pour vérifier que les messages d'autosupport atteignent bien les destinations prévues.

Procédure

1. Sélectionnez **Maintenance** > **Support** > **Autosupport**.
2. Cliquez sur **Configure**.

   La boîte de dialogue Configure Autosupport Subscribers s'affiche.

3. Pour ajouter un abonné, procédez comme suit :
   a. Cliquez sur Add (**+**).
      La boîte de dialogue Email s'affiche.
   b. Saisissez l'adresse e-mail des destinataires dans la zone Email.
   c. Cliquez sur OK.

   Équivalent CLI

   ```
    # autosupport add asup-detailed emails djones@company.com # autosupport add alert-summary emails djones@company.com
   ```

4. Pour supprimer un abonné, procédez comme suit :
   a. Dans la boîte de dialogue Configure Autosupport Subscribers, sélectionnez l'abonné à supprimer.
   b. Cliquez sur **Delete (X)**.

   Équivalent CLI

   ```
    # autosupport del asup-detailed emails djones@company.com # autosupport del alert-summary emails djones@company.com
   ```

5. Pour modifier l'adresse e-mail d'un abonné, procédez comme suit :
   a. Dans la boîte de dialogue Configure Autosupport Subscribers, sélectionnez le nom de l'abonné à modifier.
   b. Cliquez sur Modify (icône représentant un crayon).
      La boîte de dialogue Email s'affiche.
   c. Modifiez l'adresse e-mail comme il convient.
   d. Cliquez sur OK.
6. Cliquez sur **OK** pour fermer la boîte de dialogue Configure Autosupport Subscribers.
   La liste d'e-mails d'autosupport révisée apparaît dans la zone Autosupport Mailing List.

Vérifier que le système Data Domain est capable d'envoyer des e-mails ASUP et d'alerte à des destinataires externes

Confirmez que les destinataires externes du courrier électronique peuvent recevoir les e-mails d'autosupport (ASUP) et d'alerte que vous envoyez depuis votre périphérique Data Domain.

Vérifiez que l'e-mail d'autosupport (ASUP) est relayé par le serveur Exchange.

Procédure

1. Vérifiez si les ASUP peuvent être envoyés à une adresse e-mail locale, une adresse e-mail sur le même serveur de messagerie.

   ```
   # autosupport send [internal-email-addr]
   ```

2. Vérifiez si les ASUP peuvent être envoyés à une adresse e-mail en dehors du serveur de messagerie local.

   ```
   # autosupport send [external email-addr]
   ```

3. Si l'e-mail n'arrive pas à l'adresse e-mail externe sur le serveur de messagerie, vous pouvez recevoir une erreur du type suivant :

   ```
   **** Unable to send message: (errno 51: Unrecoverable errors
   from server--giving up)
   ```

   Dans ce cas, il est probable que la redirection doive être activée pour le système Data Domain sur le serveur de messagerie local en suivant les étapes décrites dans l'article de la KB *Configurer le relais du courrier électronique sur MS Exchange*, disponible à l'adresse https://support.emc.com/kb/181900.

4. Si l'ASUP peut être envoyé à une adresse e-mail externe, mais ne parvient pas au système Data Domain, un problème peut exister avec la configuration du pare-feu ou les filtres anti-spam.
5. Si les alertes ASUP arrivent dans le système Data Domain, mais qu'elles ne provoquent pas la création d'un dossier, cela peut être dû à des caractères invalides dans l'objet ou le corps du message d'alerte. Pour effectuer cette vérification :

   a. Regardez dans l'autosupport en cours et vérifiez la présence de guillemets simples ou d'apostrophes dans HOSTNAME, SYSTEM_ID et LOCATION. Ce caractère n'est pas valide et doit être supprimé dans DD OS versions 4.9.2.0 et antérieures.

   ```
   Example:


   ==========  GENERAL INFO  ==========
   GENERATED_ON=Thu Apr 28 06:54:55 PDT 2011


   VERSION=Data Domain OS 4.9.2.6-226914
   SYSTEM_ID=7FP5105000


   MODEL_NO=DD510
   HOSTNAME=system.datadomain.com


   LOCATION=123 O Malley Lane
   ```

   b. Supprimez tous les caractères non valides des champs HOSTNAME et/ou LOCATION du système. Les commandes sont

   ```
   net set hostname <host>

   config set location "location"
   ```

   c. Testez le nouveau paramètre en simulant une alerte. La manière la plus simple est de mettre manuellement en échec un lecteur de disque de rechange, de vérifier l'alerte envoyée, et de réparer immédiatement le même lecteur pour le remettre dans son état de réserve.

Gestion du bundle de support

Un bundle de support est un fichier qui contient les informations d'exploitation et de configuration du système. Il est recommandé de générer un bundle de support avant une mise à niveau logicielle ou une modification de la topologie du système (telle que la mise à niveau d'un contrôleur).

Le support Data Domain demande fréquemment un bundle de support lors d'un service d'assistance.

L'article de la KB *Comment collecter/télécharger un bundle de support (SUB) à partir d'un Data Domain Restorer (DDR)*, disponible à l'adresse https://support.emc.com/kb/180563, fournit des informations supplémentaires sur l'utilisation des bundles de support.

Génération d'un bundle de support

Pour résoudre les problèmes, le support Data Domain peut demander un bundle de support, c'est-à-dire une sélection de fichiers log compressés au format .tar.gz, accompagnée d'un fichier README incluant les en-têtes d'identification d'autosupport.

Procédure

1. Sélectionnez **Maintenance** > **Support** > **Support Bundles**.
2. Cliquez sur **Generate Support Bundle**.

   Remarque

   Le système prend en charge un maximum de 5 bundles de support. Si vous essayez de générer un sixième bundle de support, le système supprime automatiquement le bundle de support le plus ancien. Vous pouvez également supprimer des bundles de support à l'aide de la commande CLI `support bundle delete`.

   En outre, si vous générez un bundle de support sur un système mis à niveau contenant un bundle de support dont le nom utilise l'ancien format, `support-bundle.tar.gz`, ce fichier est renommé pour utiliser le nouveau format de nom.

3. Envoyez le fichier au Support Clients, à l'adresse support@emc.com.

   Remarque

   Si le bundle est trop volumineux pour être envoyé par e-mail, utilisez le site du support en ligne pour le télécharger. (Accédez à https://support.emc.com.)

Affichage de la liste des bundles de support

Utilisez l'onglet Support Bundles pour afficher les fichiers des bundles de support sur le système.

Procédure

1. Sélectionnez **Maintenance** > **Support** > **Support Bundles**.

   La liste des bundles de support s'affiche.

   Le nom du fichier du bundle de support, sa taille ou la date à laquelle il a été généré sont indiqués. Les bundles de support prennent automatiquement le nom *hostname*`-support-bundle-`*datestamp*`.tar.gz`. Le nom de fichier est par exemple `localhost-support-bundle-1127103633.tar.gz`, ce qui indique que le bundle de support a été créé sur le système d'hôte local le 27 novembre à 10:36:33.

2. Cliquez sur le lien du nom de fichier, puis sélectionnez un outil de décompression gz/tar pour afficher le contenu ASCII du bundle.

Gestion du coredump

Lorsque DD OS plante à cause d'un coredump, un fichier mémoire décrivant le problème est créé dans le répertoire `/ddvar/core`. Ce fichier peut être volumineux et difficile à copier à partir du système Data Domain.

Si le fichier mémoire ne peut pas être copié à partir du système Data Domain parce qu'il est trop volumineux, exécutez la commande **`support coredump split <filename> by <n> {MiB|GiB}`**, où :

- *<filename>* est le nom du fichier mémoire dans le répertoire `/ddvar/core`
- *<n>* est le nombre de fragments plus petits qui décomposent le fichier mémoire en

Remarque

Un seul fichier mémoire peut être décomposé en un maximum de 20 fragments. La commande échoue avec une erreur si la taille spécifiée risque d'entraîner plus de 20 fragments.

Par exemple, diviser un fichier mémoire de 42,1 Mo nommé `cpmdb.core.19297.1517443767` en fragments de 10 Mo donnerait cinq morceaux.

```
# support coredump split cpmdb.core.19297.1517443767 10 MiB
cpmdb.core.19297.1517443767 will be split into 5 chunks.
Splitting...

The md5 and split chunks of cpmdb.core.19297.1517443767:
File                                Size       Time Created
---------------------------------   --------   ------------------------
cpmdb.core.19297.1517443767_5_01    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_02    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_03    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_04    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_05    2.1 MiB    Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767.md5     0 MiB      Mon Feb  5 11:50:58 2018
---------------------------------   --------   ------------------------
Download the files as soon as possible. Otherwise they will be automatically delete in 48
hours.
```

Exécutez la commande **`support coredump save <file-list>`** pour enregistrer les fichiers coredump spécifiés sur une clé USB.

Gestion des notifications d'alerte

La fonctionnalité d'alertes génère un événement et des rapports récapitulatifs pouvant être distribués à des listes d'adresses e-mail configurables et à Data Domain.

Les rapports d'événement sont immédiatement envoyés et contiennent des informations détaillées sur un événement système. Les listes de diffusion des alertes d'événements sont appelées *groupes de notification*. Vous pouvez configurer un groupe de notification pour inclure une ou plusieurs adresses e-mail. Vous pouvez également configurer les types et le niveau de gravité des rapports d'événement envoyés à ces adresses. Par exemple, vous pouvez configurer un groupe de notification pour les personnes qui doivent connaître les événements critiques et un autre groupe pour les personnes chargées de surveiller les événements moins critiques. Il est également possible de configurer des groupes pour différentes technologies. Par exemple, vous pouvez configurer un groupe de notification qui

recevra les e-mails sur tous les événements du réseau et un autre groupe qui recevra les messages relatifs aux problèmes de stockage.

Des rapports récapitulatifs sont envoyés quotidiennement et résument les événements s'étant produits au cours des dernières 24 heures. Ces rapports ne contiennent pas toutes les informations fournies par les rapports d'événement. Par défaut, le rapport quotidien est généré à 8h00, ce qui peut être modifié. Les rapports récapitulatifs sont envoyés à l'aide d'une liste d'adresses e-mail dédiées, distincte des groupes de notification d'événements.

Vous pouvez activer ou désactiver la diffusion d'alertes à Data Domain. Lors de l'envoi de rapports à Data Domain, vous avez la possibilité de sélectionner la méthode non sécurisée héritée ou la méthode Secure Remote Services pour les transmissions sécurisées.

Gestion des notifications d'alerte d'un système haute disponibilité

La fonction d'alerte sur un système haute disponibilité génère un rapport d'événement et récapitulatif tout comme un système non HA, mais la façon dont le système haute disponibilité gère ces alertes est différente en raison de sa configuration à deux nœuds.

La configuration initiale des alertes est effectuée sur le nœud actif, puis mise en miroir sur le nœud en veille (en d'autres termes, la configuration est identique sur les deux nœuds). Les alertes locales et AM sont envoyées par e-mail conformément aux paramètres de notification. Elles incluent également des informations indiquant si elles proviennent d'un système haute disponibilité et si elles ont été générées par un nœud actif ou en veille.

Si des alertes sont actives sur le système de fichiers, la réplication ou les protocoles lorsqu'un basculement sur incident se produit, celles-ci continueront de s'afficher sur le nouveau nœud actif après le basculement si leurs conditions n'ont pas été effacées.

Les alertes historiques sur le système de fichiers, la réplication et les protocoles sont conservées dans leur nœud d'origine au lieu de basculer avec le système de fichiers lors d'un basculement sur incident. Cela signifie que la CLI sur le nœud actif ne présentera pas une vue complète/continue des alertes historiques pour le système de fichiers, la réplication et les protocoles.

Lors d'un basculement sur incident, les alertes historiques locales sont conservées dans leur nœud d'origine. Toutefois, les alertes historiques pour le système de fichiers, la réplication et les protocoles (généralement appelées « alertes logiques ») basculent avec le système de fichiers.

Remarque

Le volet **Health** > **High Availability** affiche uniquement les alertes liées à la haute disponibilité. Ces alertes peuvent être filtrées par composant HA majeur, comme HA Manager, le nœud, l'interconnexion, le stockage et la connexion SAS.

Affichage de la liste de groupes de notification

Un groupe de notification définit un ensemble de types d'alerte (classes) et un groupe d'adresses e-mail (pour les abonnés). Chaque fois que le système génère un type d'alerte sélectionné dans une liste de notification, cette alerte est envoyée aux abonnés de la liste.

Procédure

1. Sélectionnez **Health** > **Alerts** > **Notification**.
   Équivalent CLI

```
# alerts notify-list show
```

2. Pour limiter (filtrer) les entrées dans la liste de noms de groupe, saisissez un nom de groupe dans la zone Group Name ou l'e-mail d'un abonné dans la zone Alert Email, puis cliquez sur **Update**.

   Remarque

   Cliquez sur **Reset** pour afficher tous les groupes configurés.

3. Pour afficher des informations détaillées sur un groupe, sélectionnez le groupe dans la liste Group Name.

Onglet Notification

L'onglet Notification permet de configurer les groupes d'adresses e-mail qui reçoivent des alertes système, selon les types d'alerte et les niveaux de gravité sélectionnés.

Tableau 52 Liste des noms de groupe, description des libellés de colonne

Élément	Description
Group Name	Nom donné au groupe.
Classes	Nombre de classes d'alertes signalées au groupe.
Subscribers	Nombre d'abonnés configurés pour recevoir des notifications par e-mail.

Tableau 53 Informations détaillées, description des libellés

Élément	Description
Class	Service ou sous-système pouvant transmettre des alertes. Les classes répertoriées sont celles pour lesquelles le groupe de notification reçoit des alertes.
Severity	Niveau de gravité déclenchant l'envoi d'un e-mail au groupe de notification. Le groupe de notification reçoit automatiquement un message dès que le seuil d'alerte fixé est atteint ou dépassé.
Subscribers	Liste de toutes les adresses e-mail d'abonnés configurées pour le groupe de notification.

Tableau 54 Contrôles de l'onglet Notification

Contrôle	Description
Bouton Add	Cliquez sur le bouton **Add** pour commencer à créer un groupe de notification.
Bouton Class Attributes Configure	Cliquez sur ce bouton pour changer les classes et les niveaux de gravité ayant pour effet de générer des alertes pour le groupe de notification sélectionné.
Bouton Delete	Cliquez sur le bouton **Delete** pour supprimer le groupe de notification sélectionné.

Tableau 54 Contrôles de l'onglet Notification (suite)

Contrôle	Description
Zone Filter By: Alert Email	Saisissez, dans cette zone de filtrage, le texte devant figurer dans les adresses e-mail de façon à limiter les entrées de la liste de noms de groupe.
Zone Filter By: Group Name	Saisissez, dans cette zone de filtrage, le texte devant figurer dans les noms de groupe de façon à limiter les entrées de la liste de noms de groupe.
Bouton Modify	Cliquez sur le bouton **Modify** pour changer la configuration du groupe de notification sélectionné.
Bouton Reset	Cliquez sur ce bouton pour supprimer les filtres définis dans les zones Filter By et afficher tous les noms de groupe.
Bouton Subscribers Configure	Cliquez sur ce bouton pour changer la liste des adresses e-mail pour le groupe de notification sélectionné.
Bouton Update	Cliquez sur ce bouton pour mettre à jour la liste des noms de groupe après avoir saisi du texte dans une zone de filtrage.

Création d'un groupe de notification

Utilisez l'onglet Notification pour ajouter des groupes de notification et sélectionner le niveau de sévérité pour chaque groupe.

Procédure

1. Sélectionnez **Health** > **Alerts** > **Notification**.
2. Cliquez sur **Add**.

   La boîte de dialogue Add Group s'affiche.

3. Saisissez le nom du groupe dans la zone **Group Name**.
4. Cochez la case d'une ou de plusieurs classes d'alertes dont vous souhaitez être informé.
5. Pour modifier le niveau de gravité par défaut (avertissement) d'une classe, sélectionnez un autre niveau dans la zone déroulante associée.

   Les niveaux de gravité sont répertoriés dans l'ordre croissant. *Emergency* est le niveau de gravité le plus élevé.

6. Cliquez sur **OK**.

   Équivalent CLI

   ```
   # alerts notify-list create eng_grp class hardwareFailure
   ```

Gestion de la liste des abonnés d'un groupe

Utilisez l'onglet Notification pour ajouter, modifier ou supprimer des adresses e-mail d'une liste d'abonnés d'un groupe de notification.

Procédure

1. Sélectionnez **Health** > **Alerts** > **Notification**.
2. Cochez la case correspondant à un groupe dans la liste des groupes de notification, puis exécutez l'une des opérations suivantes :
   - Cliquez sur **Modify**, puis sélectionnez **Subscribers.**
   - Cliquez sur **Configure** dans la liste Subscribers.
3. Pour ajouter un abonné au groupe, procédez comme suit :
   a. Cliquez sur l'icône **+**.

      La boîte de dialogue Email Address s'affiche.

   b. Saisissez l'adresse e-mail d'un abonné.

   c. Cliquez sur **OK**.

      Équivalent CLI

      ```
       # alerts notify-list add eng_lab emails
      mlee@urcompany.com,bob@urcompany.com
      ```

4. Pour modifier une adresse e-mail, procédez comme suit :
   a. Cochez la case correspondant à l'adresse e-mail dans la liste **Subscriber Email**.

   b. Cliquez sur l'icône représentant un crayon.

   c. Modifiez l'adresse e-mail dans la boîte de dialogue Email Address.

   d. Cliquez sur **OK**.
5. Pour supprimer une adresse e-mail, cochez la case correspondant à l'adresse e-mail dans la liste **Subscriber Email**, puis cliquez sur l'icône **X**.

   Équivalent CLI

   ```
   # alerts notify-list del eng_lab emails bob@urcompany.com
   ```

6. Cliquez sur **Finish** ou sur **OK**.

Modification d'un groupe de notification

Utilisez le tableau Notification pour modifier les attributs de classe d'un groupe existant.

Procédure

1. Sélectionnez **Health** > **Alerts** > **Notification**.
2. Cochez la case correspondant au groupe à modifier dans la liste de groupes.
3. Pour modifier les attributs de classe d'un groupe, procédez comme suit :
   a. Cliquez sur **Configure** dans la zone Class Attributes.

      La boîte de dialogue Edit Group s'affiche.

b. Cochez ou décochez la case correspondant à un ou plusieurs attributs de classe.

c. Pour modifier le niveau de gravité associé à un attribut de classe, sélectionnez un niveau dans la zone de liste correspondante.

d. Cliquez sur **OK**.

Équivalent CLI

```
# alerts notify-list add eng_lab class cloud severity warning
# alerts notify-list del eng_lab class cloud severity notice
```

4. Pour modifier la liste des abonnés d'un groupe, procédez comme suit :

a. Cliquez sur **Configure** dans la zone Subscribers.

La boîte de dialogue Edit Subscribers s'affiche.

b. Pour supprimer des abonnés de la liste de groupes, cochez les cases correspondant aux abonnés à supprimer, puis cliquez sur l'icône de suppression (X).

c. Pour ajouter un abonné, cliquez sur l'icône d'ajout (+), saisissez l'adresse e-mail de l'abonné, puis cliquez sur OK.

d. Cliquez sur **OK**.

Équivalent CLI

```
# alerts notify-list add eng_lab emails
mlee@urcompany.com,bob@urcompany.com
# alerts notify-list del eng_lab emails bob@urcompany.com
```

5. Cliquez sur **OK**.

Suppression d'un groupe de notification

Utilisez l'onglet Notification pour supprimer un ou plusieurs groupes de notification existants.

Procédure

1. Sélectionnez **Health** > **Alerts** > **Notification**.
2. Cochez une ou plusieurs cases correspondant à des groupes dans la liste Notifications group, puis cliquez sur **Delete**.

   La boîte de dialogue Delete Group s'affiche.

3. Vérifiez la suppression, puis cliquez sur **OK**.

   Équivalent CLI

   ```
   # alerts notify-list destroy eng_grp
   ```

Réinitialisation de la configuration du groupe de notification

Utilisez l'onglet Notification pour supprimer tous les groupes de notification ajoutés au groupe par défaut, ainsi que toutes les modifications qui y ont été apportées.

Procédure

1. Sélectionnez **Health** > **Alerts** > **Notification**.

2. Sélectionnez **More Tasks** > **Reset Notification Groups**.
3. Dans la boîte de dialogue Reset Notification Groups, cliquez sur **Yes** dans la fenêtre de vérification.

   Équivalent CLI

   ```
   # alerts notify-list reset
   ```

Configuration de l'ordonnanceur récapitulatif quotidien et de la liste de diffusion

Tous les jours, chaque système géré envoie un e-mail récapitulatif des alertes quotidiennes aux abonnés configurés pour le groupe d'e-mails alertssummary.list. L'e-mail de récapitulatif des alertes quotidiennes contient les messages des alertes actuelles et historiques relatives aux situations matérielles non critiques et aux différentes utilisations de l'espace disque à traiter prochainement.

Une panne de ventilateur est un exemple de problème non critique que vous souhaiterez régler dans un délai raisonnable. Lorsque le support reçoit la notification de défaillance, l'équipe vous contacte pour organiser avec vous le remplacement du composant.

Procédure

1. Sélectionnez **Health** > **Alerts** > **Daily Alert Summary**.
2. Si l'heure de livraison par défaut de 8h00 n'est pas acceptable, procédez comme suit :
   a. Cliquez sur **Schedule**.

      La boîte de dialogue Schedule Alert Summary s'affiche.

   b. Utilisez les zones de liste pour sélectionner l'heure, les minutes, le matin (AM) ou l'après-midi (PM) pour le rapport récapitulatif.
   c. Cliquez sur **OK**.

      Équivalent CLI

      ```
      # autosupport set schedule alert-summary daily 1400
      ```

3. Pour configurer la liste des abonnées aux alertes quotidiennes, procédez comme suit :
   a. Cliquez sur **Configure**.

      La boîte de dialogue Daily Alert Summary Mailing List s'affiche.

   b. Modifiez la liste des abonnés aux alertes quotidiennes comme suit.
      - Pour ajouter un client, cliquez sur l'icône **+**, saisissez l'adresse e-mail, puis cliquez sur **OK**.
        Équivalent CLI

        ```
        # autosupport add alert-summary emails djones@company.com
        ```

      - Pour modifier une adresse e-mail, cochez la case correspondant à l'abonné, cliquez sur l'icône représentant un crayon, modifiez l'adresse e-mail, puis cliquez sur **OK**.
      - Pour supprimer une adresse e-mail, cochez la case correspondant à l'abonné, puis cliquez sur **X**.
        Équivalent CLI

```
# autosupport del alert-summary emails djones@company.com
```

c. Cliquez sur **Finish**.

Onglet Daily Alert Summary

L'onglet Daily Alert Summary permet de configurer une liste des adresses e-mail auxquelles vous souhaitez envoyer un récapitulatif quotidien de toutes les alertes système. Les destinataires définis dans cette liste doivent faire partie, en outre, d'un groupe de notification pour pouvoir recevoir des alertes individuelles.

Tableau 55 Daily Alert Summary, description des libellés

Élément	Description
Delivery Time	Affiche l'heure configurée pour l'envoi des e-mails quotidiens.
Email List	Affiche les adresses e-mail de toutes les personnes qui reçoivent des e-mails quotidiens.

Tableau 56 Contrôles de l'onglet Daily Alert Summary

Contrôle	Description
Bouton Configure	Cliquez sur le bouton **Configure** pour modifier la liste des adresses e-mail des abonnés.
Bouton Schedule	Cliquez sur le bouton **Schedule** pour définir l'heure à laquelle le rapport quotidien est envoyé.

Activation et désactivation de la notification des alertes à Data Domain

Vous pouvez activer ou désactiver la notification des alertes à Data Domain sans incidence sur les rapports d'autosupport envoyés à Data Domain.

Procédure

1. Pour afficher l'état du reporting d'autosupport, sélectionnez **Maintenance** > **Support** > **Autosupport**.

   L'état de notification des alertes est mis en surbrillance en vert en regard du libellé d'alerte en temps réel dans la zone de Support. Selon la configuration en cours, un bouton **Enable** ou **Disable** s'affiche dans la ligne de l'alerte en temps réel.
2. Pour activer le reporting des alertes à Data Domain, cliquez sur **Enable** dans la ligne de l'alerte en temps réel.
3. Pour désactiver le reporting des alertes à Data Domain, cliquez sur **Disable** dans la ligne de l'alerte en temps réel.

Test de la fonction d'alerte par e-mail

Utilisez l'onglet Notification pour envoyer un e-mail de test aux groupes de notification ou aux adresses e-mail sélectionnés. Cette fonction vous permet de déterminer si le système est correctement configuré pour envoyer des messages d'alerte.

Procédure

1. Pour vérifier si une alerte de test a été envoyée à Data Domain, procédez comme suit :
   a. Sélectionnez **Maintenance** > **Support** > **Autosupport**.
   b. Dans la zone **Alert Support**, cliquez sur **Enable** ou **Disable** pour vérifier si l'e-mail de test a été envoyé.

      Vous ne pouvez pas modifier l'adresse e-mail.
2. Sélectionnez **Health** > **Alerts** > **Notification**.
3. Sélectionnez **More Tasks** > **Send Test Alert**.

   La boîte de dialogue Send Test Alert apparaît.
4. Dans la liste **Notification Groups**, sélectionnez les groupes qui recevront l'e-mail de test, puis cliquez sur **Next**.
5. Si vous le souhaitez, vous pouvez ajouter d'autres adresses e-mail pour l'envoi de cet e-mail.
6. Cliquez sur **Send Now**, puis sur **OK**.

   Équivalent CLI

   ```
   # alerts notify-list test jsmith@yourcompany.com
   ```
7. Si vous avez désactivé l'envoi d'alertes de test à Data Domain et que vous souhaitez activer cette fonction maintenant, procédez comme suit :
   a. Sélectionnez **Maintenance** > **Support** > **Autosupport**.
   b. Dans la zone **Alert Support**, cliquez sur **Enable**.

Résultats

Pour tester des e-mails d'alerte nouvellement ajoutés pour des problèmes d'envoi de messages, saisissez : `autosupport test email`*email-addr*

Par exemple, après l'ajout de l'adresse e-mail djones@yourcompany.com à la liste, vérifiez l'adresse à l'aide de la commande : `autosupport test email` *djones@yourcompany.com*

Gestion de l'envoi au support

La gestion des envois définit la manière dont les rapports d'autosupport et les alertes sont envoyés à Data Domain. Par défaut, les rapports d'autosupport et les alertes sont envoyés au support client de Data Domain par e-mail standard (non sécurisé). La méthode ConnectEMC envoie des messages dans un format sécurisé via la passerelle Secure Remote Services Virtual Edition (VE).

Lorsque la méthode ConnectEMC est utilisée avec une passerelle Secure Remote Services, l'avantage est qu'une passerelle peut transférer des messages provenant de systèmes différents, ce qui permet de configurer les paramètres de sécurité réseau uniquement au niveau de la passerelle Secure Remote Services, au lieu de le faire pour chacun des systèmes. En outre, un rapport de renseignements sur l'utilisation est généré et envoyé si des licences électroniques sont adoptées.

Lors de la configuration d'une passerelle Secure Remote Services, le système Data Domain prend en charge l'enregistrement de plusieurs passerelles pour assurer la redondance.

Sélection de l'envoi par e-mail standard à Data Domain

Lorsque vous sélectionnez la méthode d'envoi par e-mail standard (non sécurisée), celle-ci s'applique à la fois au reporting d'alertes et d'autosupport.

Procédure

1. Sélectionnez **Maintenance** > **Support** > **Autosupport**.
2. Cliquez sur **Configure** dans la ligne Channel de la zone Support.

   La boîte de dialogue Configure EMC Support Delivery s'affiche. La méthode d'envoi s'affiche après le libellé Channel dans la zone Support.
3. Dans la zone de la liste **Channel**, sélectionnez **Email to datadomain.com**.
4. Cliquez sur **OK**.

   Équivalent CLI

   ```
   # support notification method set email
   ```

Sélection et configuration de la livraison de Secure Remote Services

La passerelle Secure Remote Services Virtual Edition (VE) fournit la fonction d'automatisation Connect Home et des activités de support à distance grâce à une solution IP améliorée par un système de sécurité complet.

Une paserelle Secure Remote Services version 3 sur site permet de surveiller les systèmes Data Domain et les instances DD VE sur site, ainsi que les instances cloud de DD VE.

Procédure

1. Sélectionnez **Maintenance** > **Support** > **Autosupport**.
2. Cliquez sur **Configure** dans la ligne Channel de la zone Support.

   La boîte de dialogue Configure Dell EMC Support Delivery s'affiche. La méthode d'envoi s'affiche après le libellé Channel dans la zone Support.
3. Dans la zone de liste **Channel**, sélectionnez **Secure Remote Services**.
4. Saisissez le nom d'hôte de la passerelle et sélectionnez l'adresse IP locale pour le système Data Domain.
5. Cliquez sur **OK**.
6. Saisissez le nom d'utilisateur et le mot de passe de la liaison de service.
7. Cliquez sur **Register**.

   Les détails relatifs à Secure Remote Services sont affichés dans le panneau Autosupport.

   Équivalent de la CLI

```
# support connectemc device register ipaddr esrs-gateway [host-list] [ha-peer ipaddr]
```

⚠ ATTENTION

Lors de la configuration de la fourniture des services Secure Remove Services sur une paire HA Data Domain :

- **Le paramètre** `ha-peer` **est nécessaire lors de la configuration des Secure Remote Services sur des paires HA Data Domain pour enregistrer les deux nœuds.**
- **Le client doit fournir les informations d'identification Service Link pour exécuter la commande** `support connectemc device register` **sur une paire HA, car tenter d'enregistrer la paire HA en tant qu'utilisateur échoue et entraîne une désynchronisation du jeton de clé RSA.**

Test de fonctionnement de ConnectEMC

Une commande de la CLI vous permet de tester le fonctionnement de ConnectEMC en envoyant un message de test au support via la passerelle Secure Remote Services.

Procédure

1. Pour tester le fonctionnement de ConnectEMC, utilisez la CLI.

```
#support connectemc test
Sending test message through ConnectEMC...
Test message successfully sent through ConnectEMC.
```

Gestion des fichiers log

Le système Data Domain conserve un jeu de fichiers log, qui peuvent être rassemblés et envoyés au support afin de résoudre les problèmes liés au système que vous êtes susceptible de rencontrer. Les fichiers log ne peuvent pas être modifiés ou supprimés par un utilisateur avec DD System Manager, mais ils peuvent être copiés à partir du répertoire de logs et gérés en dehors du système.

Remarque

Les messages de fichiers log sur un système haute disponibilité sont conservés sur le nœud d'origine du fichier log.

Les fichiers log sont soumis à une rotation hebdomadaire. Chaque dimanche à 0h45, le système ouvre automatiquement les nouveaux fichiers log pour les logs existants et renomme les fichiers précédents en leur ajoutant un nombre. Par exemple, après la première semaine de fonctionnement, le fichier de la semaine précédente `messages` est renommé `messages.1`, et de nouveaux messages sont stockés dans un nouveau fichier de messages. Chaque fichier numéroté est incrémenté d'un numéro chaque semaine. Par exemple, après la deuxième semaine, le fichier `messages.1` est renommé `messages.2`. Si le fichier `messages.2` existe déjà, il est renommé `messages.3`. À la fin de la période de rétention (affichée dans le tableau ci-après, le log ayant expiré est supprimé. Par exemple, un fichier `messages.9` existant est supprimé lorsque `messages.8` est renommé `messages.9`.

Le fichier `audit.log` ne fait pas l'objet d'une rotation hebdomadaire. Au lieu de cela, il est en rotation lorsque la taille du fichier atteint 70 Mo.

Sauf mention contraire dans la présente section, les fichiers log sont placés dans `/ddvar/log`.

Remarque

Les fichiers figurant dans le répertoire `/ddvar` peuvent être supprimés à l'aide des commandes Linux si l'utilisateur Linux dispose des autorisations d'*écriture* pour ce répertoire.

L'ensemble de fichiers log sur chaque système est déterminé par les fonctions configurées sur le système et les événements qui surviennent. Le tableau suivant décrit les fichiers log pouvant être générés par le système.

Tableau 57 Fichiers log du système

Log File	Description	Retention Period
audit.log	Messages relatifs aux événements de connexion de l'utilisateur.	15 semaines
cifs.log	Les messages provenant du sous-système CIFS sont consignés uniquement dans `debug/cifs/cifs.log`. La taille est limitée à 50 Mio.	10 semaines
messages	Messages relatifs aux événements généraux du système, notamment les commandes exécutées.	9 semaines
secure.log	Messages relatifs aux événements d'utilisateur, tels que les connexions ayant abouti et échoué, les ajouts et les suppressions d'utilisateur et les changements de mot de passe. Seuls les utilisateurs dotés du rôle admin peuvent afficher ce fichier.	9 semaines
space.log	Messages relatifs à l'utilisation de l'espace disque par les composants du système et messages relatifs au processus de nettoyage. Un message sur l'utilisation de l'espace est généré toutes les heures. Chaque fois qu'un processus de nettoyage est exécuté, environ 100 messages sont créés. Tous les messages sont enregistrés au format csv, avec des balises que vous pouvez utiliser pour séparer les messages relatifs à l'espace disque de ceux concernant le nettoyage. Vous pouvez utiliser des logiciels tiers pour analyser l'un ou l'autre de ces ensembles de messages. Le fichier log utilise les balises ci-après. • CLEAN pour les lignes de données relatives aux opérations de nettoyage. • CLEAN_HEADER pour les lignes contenant des en-têtes pour les lignes de données relatives aux opérations de nettoyage. • SPACE pour les lignes de données relatives à l'espace disque. • SPACE_HEADER pour les lignes contenant des en-têtes pour les lignes de données relatives à l'espace de disque.	Un seul fichier est conservé de manière permanente. Il n'y a pas de rotation des fichiers log pour ce log.

Affichage des fichiers log dans DD System Manager

Utilisez l'onglet Logs pour afficher et ouvrir les fichiers log du système dans DD System Manager.

Procédure

1. Sélectionnez **Maintenance** > **Logs**.

   La liste des fichiers log affiche les noms de fichier log, leurs tailles et la date de création de chaque fichier log.

2. Cliquez sur le nom d'un fichier log pour afficher son contenu. Vous pouvez être invité à sélectionner une application, telle que Notepad.exe, pour ouvrir le fichier.

Affichage d'un fichier log dans la CLI

Utilisez la commande `log view` pour afficher un fichier log dans la CLI.

Procédure

1. Pour consulter un fichier log dans l'interface de ligne de commande, utilisez la commande `log view .`

   Sans argument, la commande affiche le fichier de messages en cours.

2. Lors de l'affichage du log, utilisez les flèches vers le haut et le bas pour parcourir le fichier ; utilisez la touche q pour quitter ; puis saisissez une barre oblique (/) et un schéma à rechercher dans le fichier.

Le fichier de messages est similaire au fichier affiché ci-après. Le dernier message de cet exemple est un message horaire d'état du système que le système Data Domain génère automatiquement. Le message indique la durée de fonctionnement du système, la quantité de données stockées, les opérations NFS et le volume d'espace disque utilisé pour le stockage des données (%). Les messages horaires sont consignés dans le log du système et dans la console série, le cas échéant.

```
# log view
Jun 27 12:11:33 localhost rpc.mountd: authenticated unmount
request from perfsun-g.emc.com:668 for /ddr/col1/segfs (/ddr/
col1/segfs)

Jun 27 12:28:54 localhost sshd(pam_unix)[998]: session opened
for user jsmith10 by (uid=0)

Jun 27 13:00:00 localhost logger: at 1:00pm up 3 days, 3:42,
52324 NFS ops, 84763 GiB data col. (1%)
```

Remarque

Gio = Gibibytes = l'équivalent binaire des gigaoctets.

En savoir plus sur les messages des fichiers log

Consultez les messages d'erreur dans le catalogue des messages d'erreur pour votre version de DD OS.

Le texte du fichier log est similaire au texte ci-dessous.

```
Jan 31 10:28:11 syrah19 bootbin: NOTICE: MSG-SMTOOL-00006: No
replication throttle schedules found: setting throttle to
unlimited.
```

Le message intègre les composants ci-dessous.

```
DateTime Host Process [PID]: Severity: MSG-Module-MessageID: Message
```

Les niveaux de gravité sont, du plus important au moins important : Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.

Procédure

1. Rendez-vous sur le site Web de support en ligne à l'adresse https://support.emc.com, saisissez *Catalogue des messages d'erreur* dans la zone de recherche, puis cliquez sur le bouton de recherche.
2. Dans la liste des résultats, repérez le catalogue de votre système et cliquez sur le lien.
3. Servez-vous de la fonction de recherche de votre navigateur pour rechercher une chaîne de texte unique dans le message.

   La description du message d'erreur est similaire à la description ci-dessous.

   ```
   ID: MSG-SMTOOL-00006 - Severity: NOTICE - Audience:
   customerMessage: No replication throttle schedules found:
   setting throttle to unlimited.

   Description: The restorer cannot find a replication
   throttle schedule. Replication is running with throttle
   set to unlimited.

   Action: To set a replication throttle schedule, run the
   replication throttle add command.
   ```

4. Pour résoudre un problème, effectuez l'action recommandée.

   Dans l'exemple de description de message, vous pouvez exécuter la commande `replication throttle add` pour définir la limitation.

Enregistrement d'une copie de fichiers log

Enregistrez des copies de fichiers log sur un autre périphérique lorsque vous souhaitez archiver ces fichiers.

Utilisez le montage NFS, CIFS ou FTP pour copier les fichiers sur un autre ordinateur. Si vous utilisez CIFS ou NFS, montez /ddvar sur votre ordinateur et copiez les fichiers à partir du point de montage. La procédure suivante décrit comment utiliser FTP pour déplacer des fichiers vers un autre ordinateur.

Procédure

1. Sur le système Data Domain, utilisez la commande `adminaccess show ftp` pour déterminer si le service FTP est activé. Si le service est désactivé, utilisez la commande `adminaccess enable ftp`.
2. Sur le système Data Domain, utilisez la commande `adminaccess show ftp` pour déterminer si la liste d'accès FTP contient l'adresse IP de votre ordinateur distant. Si l'adresse ne figure pas dans la liste, utilisez la commande `adminaccess add ftp` *ipaddr*.

3. Sur l'ordinateur distant, ouvrez un navigateur Web.
4. Dans la zone **Address** située dans la partie supérieure du navigateur Web, utilisez FTP pour accéder au système Data Domain, comme indiqué dans l'exemple suivant.

   `ftp://Data Domain system_name.yourcompany.com/`

   Remarque

   Certains navigateurs Web ne demandent pas automatiquement une connexion si une machine n'accepte pas les connexions anonymes. Dans ce cas, ajoutez un nom d'utilisateur et un mot de passe à la ligne FTP. Exemple : **`ftp://sysadmin:your-pw@Data Domain system_name.yourcompany.com/`**

5. Dans la fenêtre de connexion, connectez-vous au système Data Domain en tant qu'utilisateur **`sysadmin`**.
6. Sur le système Data Domain, vous êtes dans le répertoire situé juste au-dessus du répertoire de logs. Ouvrez le répertoire de logs pour répertorier les fichiers de messages.
7. Copiez le fichier à enregistrer. Cliquez avec le bouton droit sur l'icône du fichier et sélectionnez **Copy To Folder** dans le menu. Choisissez un emplacement pour la copie du fichier.
8. Si vous souhaitez que le service FTP soit désactivé sur le système Data Domain, une fois la copie de fichier effectuée, utilisez SSH pour vous connecter au système Data Domain en tant que sysadmin et exécutez la commande `adminaccess disable ftp`.

Transmission des messages de fichiers log aux systèmes distants

Certains messages de fichier log peuvent être envoyés à d'autres systèmes depuis le système Data Domain. Pour publier des messages de fichier log vers les systèmes distants, DD OS utilise le processus syslog.

Le système Data Domain exporte les sélecteurs d'installation/priorité (facility.priority) suivants pour les fichiers log. Pour plus d'informations sur la gestion des sélecteurs et la réception des messages sur un système tiers, consultez la documentation de votre système de réception.

- *.notice : envoie tous les messages correspondants ou supérieurs à la priorité indiquée (notice).
- *.alert : envoie tous les messages correspondants ou supérieurs à la priorité de l'alerte (les alertes sont incluses dans *.notice).
- kern.* : envoie tous les messages du noyau (fichiers log kern.info).

Les `log host` commandes gèrent le processus d'envoi des messages de fichiers log à un autre système.

Affichage de la configuration de la transmission des fichiers log

Utilisez la commande `log host show` de la CLI pour vérifier si la transmission des fichiers log est activée et identifier les hôtes auxquels ces fichiers log sont destinés.

Procédure

1. Pour afficher la configuration, entrez la commande `log host show`.

```
# log host show
Remote logging is enabled.
Remote logging hosts
     log-server
```

Activation et désactivation de la transmission des messages de log

Vous devez utiliser des commandes de la CLI pour activer ou désactiver la transmission des messages de log.

Procédure

1. Pour activer l'envoi des messages de log vers d'autres systèmes, utilisez la commande `log host enable`.
2. Pour désactiver l'envoi des messages de log vers d'autres systèmes, utilisez la commande `log host disable`.

Ajout ou suppression d'un hôte récepteur

Vous devez utiliser des commandes de la CLI pour ajouter ou supprimer un hôte récepteur.

Procédure

1. Pour ajouter un système à la liste qui reçoit les messages de log du système Data Domain, utilisez la commande `log host add`.
2. Pour supprimer un système de la liste qui reçoit les messages de log du système, utilisez la commande suivante : `log host del`.

La commande suivante ajoute le système *log-server* aux hôtes qui reçoivent les messages de log.

```
log host add log-server
```

La commande suivante supprime le système *log-server* des hôtes qui reçoivent des messages de log.

```
log host del log-server
```

La commande suivante désactive l'envoi des logs et efface la liste des noms d'hôte de destination.

```
log host reset
```

Gestion de l'alimentation sur les systèmes distants à l'aide de l'interface IPMI

Les systèmes DD sélectionnés prennent en charge la gestion de l'alimentation à distance à l'aide de l'interface de gestion de plate-forme intelligente (IPMI), ainsi que la surveillance à distance de la séquence d'amorçage à l'aide du SOL (Serial Over LAN).

La gestion de l'alimentation IPMI s'effectue entre un initiateur IPMI et un hôte distant IPMI. L'initiateur IPMI est l'hôte qui contrôle l'alimentation sur l'hôte distant. Pour prendre en charge la gestion de l'alimentation à distance à partir d'un initiateur, l'hôte distant doit être configuré avec un nom d'utilisateur et un mot de passe IPMI.

L'initiateur doit fournir ce nom d'utilisateur et ce mot de passe lorsque vous tentez de gérer l'alimentation sur un hôte distant.

IPMI fonctionne indépendamment du DD OS et permet à un utilisateur IPMI de gérer l'alimentation du système tant que le système distant est raccordé à une source d'alimentation et à un réseau. Une connexion réseau IP est requise entre un initiateur et un système distant. Correctement configurée et connectée, la gestion IPMI vous dispense d'être physiquement présent pour mettre sous ou hors tension un système distant.

Vous pouvez utiliser DD System Manager et la CLI pour configurer des utilisateurs IPMI sur un système distant. Après avoir configuré IPMI sur un système distant, vous pouvez utiliser les fonctions d'initiateur IPMI sur un autre système pour vous connecter et gérer l'alimentation.

Remarque

Si un système n'est pas capable de prendre en charge IPMI en raison de limitations matérielles ou logicielles, DD System Manager affiche un message de notification lorsque vous essayez d'accéder à une page de configuration.

Le SOL est utilisé pour afficher la séquence d'amorçage après un cycle de marche/arrêt sur un système distant. Le SOL permet aux données de console textuelles qui sont normalement transmises vers un port série ou une console directement connectée, d'être envoyées via un réseau local et affichées par un hôte de gestion.

L'interface de ligne de commande DD OS vous permet de configurer un système distant pour SOL et d'afficher le résultat de la console distante. Cette fonction est uniquement prise en charge dans la CLI.

NOTE

La coupure de l'alimentation IPMI est prévue dans les situations d'urgence au cours desquelles les tentatives d'arrêt de l'alimentation à l'aide des commandes DD OS échouent. La coupure de l'alimentation IPMI arrête simplement l'alimentation dans le système ; elle n'effectue pas un arrêt normal du système de fichiers DD OS. Pour couper et remettre l'alimentation de manière adéquate, utilisez la commande `system reboot` DD OS. Pour couper l'alimentation du système de manière adéquate, utilisez la commande `system poweroff` DD OS et attendez que la commande arrête correctement le système de fichiers.

Limitations des protocoles IPMI et de SOL

La prise en charge des protocoles IPMI et SOL est limitée sur certains systèmes Data Domain.

- IPMI est pris en charge sur tous les systèmes supportés par cette version à l'exception des systèmes suivants : DD140, DD610 et DD630.
- La prise en charge d'utilisateurs IPMI varie comme suit.
  - Modèle DD990 : Nombre maximal d'ID utilisateur = 15. Trois utilisateurs par défaut (NULL, anonymous, root). Nombre maximal d'ID utilisateur disponibles = 12.
  - Modèles DD640, DD4200, DD4500, DD7200 et DD9500 : Nombre maximal d'ID utilisateur = 10. Deux utilisateurs par défaut (NULL, root). Nombre maximal d'ID utilisateur disponibles = 8.

- SOL est pris en charge sur les systèmes suivants : DD160, DD620, DD640, DD670, DD860, DD890, DD990, DD2200, DD2500 (version DD OS 5.4.0.6 ou version supérieure requise), DD4200, DD4500, DD7200 et DD9500.

Remarque

L'utilisateur root n'est pas pris en charge pour les connexions IPMI sur les systèmes DD160.

Ajout et suppression d'utilisateurs IPMI à l'aide de DD System Manager

Chaque système contient sa propre liste d'utilisateurs IPMI configurés, qui est utilisée pour contrôler l'accès aux fonctions de gestion d'alimentation locale. Un autre système fonctionnant en tant qu'initiateur IPMI peut gérer l'alimentation du système à distance uniquement après la spécification d'un nom d'utilisateur et d'un mot de passe valides.

Pour donner à un utilisateur IPMI le droit de gérer l'alimentation sur plusieurs systèmes gérés, vous devez ajouter cet utilisateur à chacun des systèmes distants.

Remarque

La liste des utilisateurs IPMI pour chaque système distant est distincte des listes DD System Manager pour l'accès des administrateurs et des utilisateurs locaux. Les administrateurs et les utilisateurs locaux n'héritent d'aucune autorisation pour la gestion de l'alimentation IPMI.

Procédure

1. Sélectionnez **Maintenance** > **IPMI**.
2. Pour ajouter un utilisateur, procédez comme suit.
   a. Au-dessus du tableau des utilisateurs IPMI, cliquez sur **Add**.
   b. Dans la boîte de dialogue Add User, saisissez le nom d'utilisateur (16 caractères maximum) et le mot de passe dans les zones appropriées (saisissez à nouveau le mot de passe dans la zone **Verify Password**).
   c. Cliquez sur **Create**.
   L'entrée utilisateur apparaît dans le tableau **IPMI Users**.
3. Pour supprimer un utilisateur, procédez comme suit.
   a. Dans la liste des utilisateurs IPMI, sélectionnez un utilisateur, puis cliquez sur **Delete**.
   b. Dans la boîte de dialogue Delete User, cliquez sur **OK** pour confirmer la suppression de l'utilisateur.

Modification du mot de passe d'un utilisateur IPMI

Modifiez le mot de passe de l'utilisateur IPMI pour empêcher l'utilisation de l'ancien mot de passe pour gérer l'alimentation.

Procédure

1. Sélectionnez **Maintenance** > **IPMI**.
2. Dans le tableau des utilisateurs IPMI, sélectionnez un utilisateur, puis cliquez sur **Change Password**.

3. Dans la boîte de dialogue Change Password, saisissez le mot de passe dans la zone de texte appropriée, puis entrez à nouveau le mot de passe dans la zone **Verify Password**.
4. Cliquez sur **Update**.

Configuration d'un port IPMI

Lorsque vous configurez un port IPMI pour un système, vous sélectionnez le port à partir d'une liste de ports réseau et définissez les paramètres de configuration IP pour ce port. La sélection des ports IPMI affichés est déterminée par le modèle du système Data Domain.

Certains systèmes prennent en charge un ou plusieurs ports dédiés, qui peuvent être utilisés uniquement pour le trafic IPMI. D'autres systèmes prennent en charge des ports qui peuvent être utilisés pour le trafic IPMI et l'ensemble du trafic IP pris en charge par les interfaces physiques de la vue **Hardware** > **Ethernet** > **Interfaces**. Les systèmes qui fournissent des ports dédiés IPMI ne disposent pas de ports partagés.

Les noms de port de la liste des ports réseau IPMI utilisent le préfixe bmc, qui représente le contrôleur de gestion BMC (Baseboard Management Controller). Pour déterminer si un port est un port dédié ou un port partagé, comparez la partie restante du nom du port aux ports de la liste des interfaces réseau. Si l'autre partie du nom du port IPMI correspond à une interface de la liste des interfaces réseau, il s'agit d'un port partagé. Si l'autre partie du nom du port IPMI diffère des noms de la liste des interfaces réseau, il s'agit d'un port IPMI dédié.

Remarque

Les systèmes DD4200, DD4500 et DD7200 font exception à la règle de dénomination précédemment décrite. Sur ces systèmes, le port IPMI, bmc0a, correspond au port partagé de l'interface ethMa dans la liste des interfaces réseau. Si possible, réservez le port partagé de l'interface ethMa au trafic IPMI et au trafic de gestion du système (via des protocoles tels que HTTP, Telnet et SSH). Le trafic des données de sauvegarde doit être dirigé vers d'autres ports.

Lorsque le trafic IPMI et le trafic IP non-IPMI partagent un port Ethernet, n'utilisez pas si possible la fonction d'agrégation de liens sur l'interface partagée car des modifications de l'état du lien peuvent interférer avec la connectivité IPMI.

Procédure

1. Sélectionnez **Maintenance** > **IPMI**.

   La zone IPMI Configuration présente la configuration IPMI relative au système géré. Le tableau des ports réseau répertorie les ports sur lesquels IPMI peut être activé et configuré. Le tableau des utilisateurs IPMI répertorie les utilisateurs IPMI pouvant accéder au système géré.

   Tableau 58 Description des colonnes de la liste des ports réseau

Élément	Description
Port	Nom logique d'un port qui prend en charge les communications IPMI.
Enabled	Indique si le port est activé pour IPMI (Yes ou No).
DHCP	Indique si le port utilise le serveur DHCP pour définir son adresse IP (Yes ou No).

Tableau 58 Description des colonnes de la liste des ports réseau (suite)

Élément	Description
MAC Address	Adresse MAC du matériel pour le port.
IP Address	Adresse IP du port.
Netmask	Masque de sous-réseau pour le port.
Gateway	Adresse IP de la passerelle pour le port.

Tableau 59 Description des colonnes de la liste des utilisateurs IPMI

Élément	Description
User Name	Nom d'un utilisateur disposant des droits permettant de gérer le système distant.

2. Dans le tableau **Network Ports**, sélectionnez le port à configurer.

Remarque

Si le port IPMI prend également en charge le trafic IP (pour l'accès administrateur ou le trafic de sauvegarde), le port d'interface doit être activé avant la configuration IPMI.

3. Au-dessus du tableau **Network Ports**, cliquez sur **Configure**.

   La boîte de dialogue Configure Port s'affiche.

4. Choisissez la manière dont les informations relatives aux adresses réseau sont attribuées.
   - Pour collecter l'adresse IP, le masque de réseau et la configuration de la passerelle auprès d'un serveur DHCP, sélectionnez **Dynamic (DHCP)**.
   - Pour définir manuellement la configuration réseau, sélectionnez **Static (Manual)**, puis saisissez l'adresse IP, le masque de réseau et l'adresse de la passerelle.

5. Pour activer un port réseau IPMI désactivé, sélectionnez le port réseau dans le tableau **Network Ports**, puis cliquez sur **Enable**.
6. Pour désactiver un port réseau IPMI activé, sélectionnez le port réseau dans le tableau **Network Ports**, puis cliquez sur **Disable**.
7. Cliquez sur **Apply**.

Préparation à la gestion de l'alimentation à distance et surveillance de la console avec la CLI

La surveillance de la console à distance utilise la fonction SOL (Serial Over Lan) pour activer l'affichage de la sortie de la console basée sur du texte sans serveur série. Vous devez utiliser la CLI pour configurer un système de surveillance à distance de la console et de la gestion de l'alimentation.

La surveillance de la console à distance est généralement utilisée conjointement avec la commande `ipmi remote power cycle` pour afficher la séquence de démarrage du système distant. Cette procédure doit être utilisée sur chacun des systèmes pour

lesquels vous souhaitez pouvoir visualiser la console à distance pendant la séquence de démarrage.

Procédure

1. Connectez la console au système directement ou à distance.
   - Utilisez les connecteurs suivants pour établir une connexion directe.
     - Ports de type DIN pour un clavier PS/2
     - Port USB-A femelle pour un clavier USB
     - Connecteur DB15 femelle pour un écran VGA

     Remarque

     Les systèmes DD4200, DD4500 et DD7200 ne prennent pas en charge la connexion directe, y compris KVM.

   - Pour une connexion série, utilisez un connecteur DB9 mâle standard ou micro-DB9 femelle. Les systèmes DD4200, DD4500 et DD7200 comportent un connecteur Micro-DB9 femelle. Pour une connexion classique à un ordinateur portable, un câble null modem équipé de connecteurs micro-DB9 mâle et DB9 femelle standard est inclus.
   - Pour une connexion IPMI/SOL à distance, utilisez la prise RJ45 appropriée comme suit.
     - Pour les systèmes DD990, utilisez le port par défaut eth0d.
     - Pour d'autres systèmes, utilisez le port de maintenance ou le port de service. Pour les emplacements de port, consultez la documentation relative au système, comme un guide d'installation et de configuration ou de présentation du matériel.
2. Pour prendre en charge la surveillance de la console à distance, utilisez les paramètres du BIOS par défaut.
3. Pour afficher le nom du port IPMI, entrez `ipmi show config`.
4. Pour activer IPMI, saisissez `ipmi enable {`*`port`* `| all}`.
5. Pour configurer le port IPMI, entrez `ipmi config port { dhcp | ipaddress` *`ipaddr`* `netmask` *`mask`* `gateway` *`ipaddr`* `}`.

   Remarque

   Si le port IPMI prend également en charge le trafic IP (pour l'accès des administrateurs ou le trafic de sauvegarde), le port d'interface doit être activé avec la commande `net enable` avant la configuration d'IPMI.

6. S'il s'agit de la première utilisation du protocole IPMI, exécutez la commande `ipmi user reset` pour supprimer les utilisateurs IPMI qui peuvent être désynchronisés entre deux ports, et pour désactiver les utilisateurs par défaut.
7. Pour ajouter un nouvel utilisateur IPMI, saisissez `ipmi user add` *`user`*.
8. Pour configurer SOL, procédez comme suit :
   a. Accédez à `system option set console lan`.
   b. Lorsque vous y êtes invité, entrez `y` pour redémarrer le système.

Gestion de l’alimentation avec DD System Manager

Une fois IPMI correctement configuré sur un système distant, vous pouvez utiliser DD System Manager en tant qu’initiateur IPMI pour vous connecter au système distant, afficher et modifier l’état de l’alimentation.

Procédure

1. Sélectionnez **Maintenance** > **IPMI**.
2. Cliquez sur **Login to Remote System**.

   La boîte de dialogue IPMI Power Management s’affiche.

3. Saisissez l’adresse IP IPMI du système distant ou son nom d’hôte, ainsi que le nom d’utilisateur et le mot de passe IPMI, puis cliquez sur **Connect**.
4. Affichez l’état IPMI.

   La boîte de dialogue IPMI Power Management s’affiche et présente l’identification du système cible et l’état de l’alimentation actuel. La zone Status affiche toujours l’état actuel.

   Remarque

   L’icône d’actualisation (flèches bleues) en regard de l’état souhaité peut être utilisée pour actualiser l’état de configuration (par exemple, si l’adresse IP ou la configuration de l’utilisateur IPMI ont été modifiées au cours des 15 dernières minutes à l’aide des commandes CLI).

5. Pour modifier l’état de l’alimentation IPMI, cliquez sur le bouton approprié.
   - **Power Up** : apparaît lorsque le système distant est mis hors tension. Cliquez sur ce bouton pour mettre le système distant sous tension.
   - **Power Down** : apparaît lorsque le système distant est mis sous tension. Cliquez sur ce bouton pour mettre le système distant hors tension.
   - **Power Cycle** : apparaît lorsque le système distant est mis sous tension. Cliquez sur ce bouton pour effectuer un cycle de marche/arrêt du système distant.
   - **Manage Another System** : cliquez sur ce bouton pour vous connecter à un autre système distant pour la gestion de l’alimentation IPMI.
   - **Done** : cliquez sur ce bouton pour fermer la boîte de dialogue IPMI Power Management.

   NOTE

   L’option IPMI Power Down n’exécute pas un arrêt normal de DD OS. Cette option est utile si DD OS se bloque. Elle ne permet pas un arrêt progressif du système.

Gestion de l'alimentation à l'aide de la CLI

Vous pouvez gérer l'alimentation sur un système distant et démarrer la surveillance de la console à distance à l'aide de la CLI.

Remarque

Le système distant doit être correctement configuré pour que vous puissiez gérer l'alimentation ou surveiller le système.

Procédure

1. Ouvrez une session d'interface de ligne de commande sur le système à partir duquel vous souhaitez surveiller un système distant.
2. Pour gérer l'alimentation sur le système distant, entrez `ipmi remote power {on | off | cycle | status} ipmi-target <`*ipaddr* `|` *hostname*`> user` *user*.
3. Pour démarrer la surveillance de la console à distance, entrez `ipmi remote console ipmi-target <`*ipaddr* `|` *hostname*`> user` *user*.

   Remarque

   Le nom d'utilisateur est un nom d'utilisateur IPMI défini pour IPMI sur le système distant. Les noms d'utilisateur DD OS ne sont pas automatiquement pris en charge par IPMI.

4. Pour vous déconnecter d'une session de surveillance de la console à distance et revenir à la ligne de commande, entrez le signe arobase (@).
5. Pour mettre fin à la surveillance de la console à distance, entrez le signe tilde (~).

CHAPITRE 4

Surveillance des systèmes Data Domain

Ce chapitre traite des sujets suivants :

Affichage de l'état du système individuel et des informations d'identité

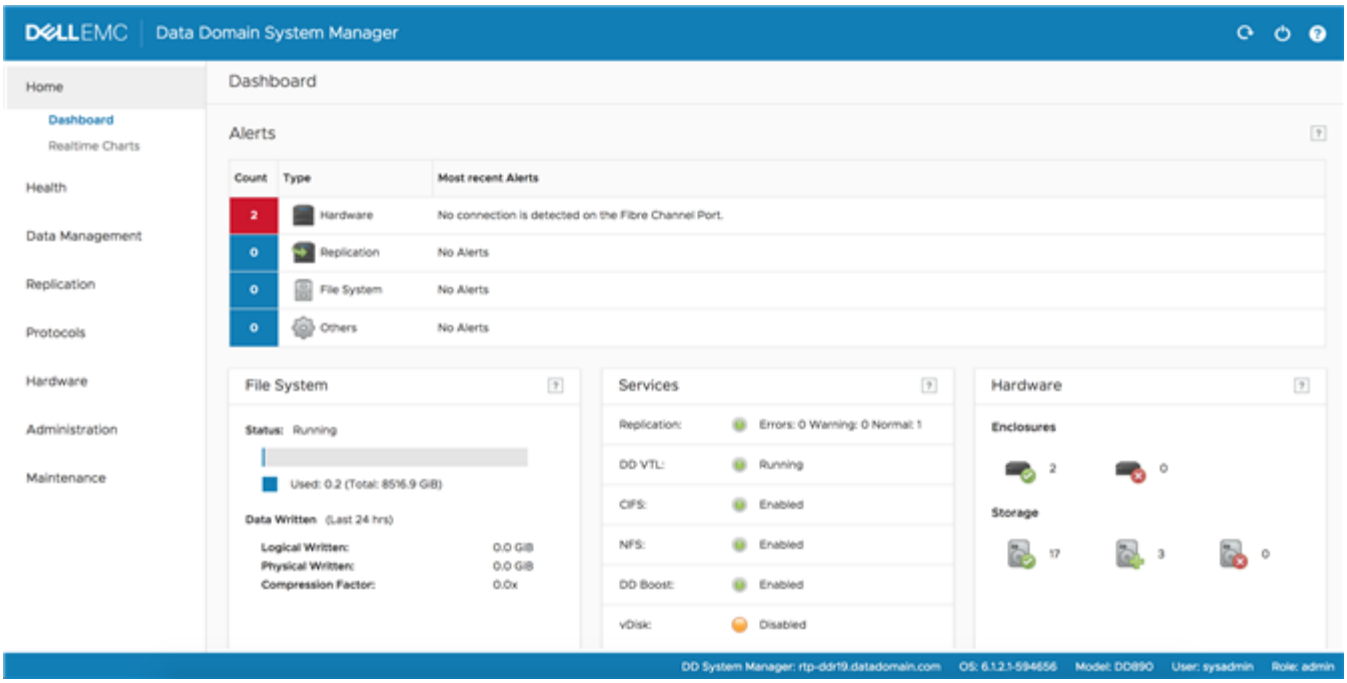
La zone **Dashboard** affiche des informations récapitulatives et l'état des alertes, le système de fichiers, les services sous licences et les châssis. La zone **Maintenance** affiche des informations système supplémentaires, y compris les temps de fonctionnement du système et les numéros de série du système et du châssis.

Le nom du système, la version du logiciel et les informations utilisateur apparaissent dans le pied de page à tout moment.

Procédure

1. Pour afficher le tableau de bord système, sélectionnez **Home** > **Dashboard**.

   Figure 5 Tableau de bord système



2. Pour afficher la durée de fonctionnement du système et les informations d'identité, sélectionnez **Maintenance** > **System**.

   Les informations d'identification et relatives au temps de fonctionnement système s'affiche dans la zone System.

Zone Dashboard Alerts

La zone Dashboard Alerts affiche le nombre, le type et le texte des alertes les plus récentes dans le système, pour chaque sous-système (matériel, réplication, système de fichiers, etc.). Cliquez n'importe où dans la zone des alertes pour afficher des informations supplémentaires sur les alertes en cours.

Tableau 60 Description des colonnes de la zone Dashboard Alerts

Colonne	Description
Count	Nombre d'alertes en cours pour le type de sous-système spécifié dans la colonne adjacente. La couleur d'arrière-plan indique la gravité de l'alerte.
Type	Sous-système ayant généré l'alerte.
Most recent alerts	Texte de l'alerte la plus récente pour le type de sous-système spécifié dans la colonne adjacente.

Zone Dashboard File System

La zone Dashboard File System affiche des statistiques pour la totalité du système de fichiers. Cliquez n'importe où dans la zone File System pour afficher des informations supplémentaires.

Tableau 61 Description des libellés de la zone File System

Colonne	Description
Status	État actuel du système de fichiers.
X.Xx	Facteur moyen de réduction de la compression dans le système de fichiers.
Used	Espace total du système de fichiers en cours d'utilisation.
Data Written: Pre-compression	Quantité de données reçues par le système avant la compression.
Data Written: Post-compression	Quantité de données stockées sur le système après la compression.

Zone Dashboard Services

La zone Dashboard Services affiche l'état des services de réplication, DD VTL, CIFS, NFS, DD Boost et vDisk. Cliquez sur un service pour afficher des informations détaillées sur ce celui-ci.

Tableau 62 Descriptions des colonnes de la zone Services

Colonne	Description
Colonne de gauche	La colonne de gauche répertorie les services pouvant être utilisés sur le système. Parmi ces services, peuvent figurer la réplication, DD VTL, CIFS, NFS, DD Boost et vDisk.
Colonne de droite	La colonne de droite indique l'état opérationnel du service. Ces services peuvent avoir un état activé (Enabled), désactivé (Disabled) ou sans licence (Not licensed). La

Tableau 62 Descriptions des colonnes de la zone Services (suite)

Colonne	Description
	ligne du service de réplication indique le nombre de contextes de réplication ayant un état normal, des avertissements et des erreurs. Une case à code couleur s'affiche en vert pour un fonctionnement normal, en jaune en cas d'avertissement ou en rouge en cas d'erreurs.

Zone Dashboard HA Readiness

Dans les systèmes haute disponibilité (HA), le volet HA indique si le système peut basculer à partir du nœud actif vers le nœud en veille, si nécessaire.

Vous pouvez cliquer sur le volet **HA** pour accéder à la section **High Availability** sous **HEALTH**.

Zone Dashboard Hardware

La zone Dashboard Hardware affiche l'état des châssis et des disques du système. Cliquez n'importe où dans la zone Hardware pour afficher des informations supplémentaires sur ces composants.

Tableau 63 Description des libellés de la zone Hardware

Libellé	Description
Enclosures	Les icônes de châssis indiquent le nombre de châssis ayant un fonctionnement normal (coche verte) et dégradés (X rouge).
Storage	Les icônes de stockage indiquent le nombre de disques durs ayant un fonctionnement normal (coche verte), en mode secours (+ vert) ou en échec (X rouge).

Zone Maintenance System

La zone Maintenance System affiche le numéro de modèle du système, la version DD OS, la durée de fonctionnement du système et les numéros de série du système et du châssis.

Tableau 64 Description des libellés de la zone System

Libellé	Description
Model Number	Le numéro de modèle représente le numéro attribué au système Data Domain.
Version	La version représente la version DD OS et le numéro de build du logiciel exécuté sur le système.

Tableau 64 Description des libellés de la zone System (suite)

Libellé	Description
System Uptime	Ce libellé indique la durée de fonctionnement du système depuis le dernier démarrage. L'heure entre parenthèses indique la date de mise à jour récente de la durée de fonctionnement du système.
System Serial No.	Ce libellé indique le numéro de série attribué au système. Sur les systèmes plus récents, tels que DD4500 et DD7200, le numéro de série du système est indépendant du numéro de série du châssis et reste inchangé lors de nombreux types d'événements de maintenance, dont les remplacements de châssis. Sur les systèmes existants, tels que DD990 et version antérieure, le numéro de série du système est défini sur le numéro de série du châssis.
Chassis Serial No.	Le numéro de série du châssis représente le numéro figurant sur le châssis du système en cours.

Volet Health Alerts

Les alertes sont des messages envoyés par les services et les sous-systèmes du système signalant des événements système. Le volet Health > Alerts affiche des onglets vous permettant de voir les alertes en cours et antérieures, les groupes configurés pour la notification des alertes, ainsi que la configuration des utilisateurs souhaitant recevoir quotidiennement des rapports récapitulatifs sur les alertes.

Les alertes sont également envoyées sous la forme de traps SNMP. Consultez le document *MIB Quick Reference Guide* ou la base de données MIB pour obtenir la liste complète des traps.

Affichage et suppression des alertes actuelles

L'onglet Current Alerts affiche une liste de toutes les alertes en cours et peut afficher des informations détaillées sur une alerte sélectionnée. Une alerte est automatiquement supprimée de la liste des alertes en cours lorsque la situation sous-jacente est résolue ou lorsqu'elle est manuellement supprimée.

Procédure

1. Pour afficher toutes les alertes en cours, sélectionnez **Health** > **Alerts** > **Current Alerts**.
2. Procédez comme suit pour limiter le nombre d'entrées dans la liste d'alerte en cours.
   a. Dans la zone Filter By, sélectionnez un **niveau de gravité** et une **classe** pour afficher uniquement les alertes répondant à ces critères.
   b. Cliquez sur **Update**.

Toutes les alertes qui ne correspondent pas au niveau de gravité et à la classe indiqués sont supprimées de la liste.

3. Pour afficher les informations supplémentaires d'une alerte spécifique dans la zone **Details**, cliquez sur l'alerte en question dans la liste.
4. Pour supprimer une alerte, sélectionnez la case à cocher de l'alerte dans la liste, puis cliquez sur **Clear.**

   L'alerte de suppression n'apparaît plus dans la liste des alertes en cours, mais celle-ci peut être récupérée dans la liste de l'historique des alertes.

5. Pour supprimer le filtre et revenir à la liste complète des alertes en cours, cliquez sur **Reset**.

Onglet Current Alerts

L'onglet Current Alerts affiche une liste d'alertes et des informations détaillées sur une alerte sélectionnée.

Tableau 65 Liste des alertes, description des libellés de colonne

Élément	Description
Message	Texte du message d'alerte.
Severity	Niveau de gravité de l'alerte. Par exemple : warning, critical, info ou emergency.
Date	Date et heure d'émission de l'alerte.
Class	Sous-système dans lequel l'alerte est survenue.
Object	Composant physique dans lequel l'alerte est survenue.

Tableau 66 Zone de détails, description des libellés de ligne

Élément	Description
Name	Identifiant textuel de l'alerte
Message	Texte du message d'alerte.
Severity	Niveau de gravité de l'alerte. Par exemple : warning, critical, info ou emergency.
Class	Sous-système et périphérique dans lesquels l'alerte est survenue.
Date	Date et heure d'émission de l'alerte.
Object ID	Composant physique dans lequel l'alerte est survenue.
Event ID	Identifiant d'événement.
Tenant Units	Répertorie les unités tenant concernées.
Description	Informations plus détaillées sur l'alerte.
Action	Action suggérée pour corriger l'alerte.
Object Info	Informations supplémentaires sur l'objet concerné.
SNMP OID	ID d'objet SNMP.

Affichage de l'historique des alertes

L'onglet Alerts History affiche une liste de toutes les alertes supprimées et peut afficher des informations détaillées sur une alerte sélectionnée.

Procédure

1. Pour afficher l'ensemble de l'historique des alertes, sélectionnez **Health** > **Alerts** > **Alerts History**.
2. Procédez comme suit pour limiter le nombre d'entrées dans la liste d'alerte en cours.
   a. Dans la zone Filter By, sélectionnez un **niveau de gravité** et une **classe** pour afficher uniquement les alertes répondant à ces critères.
   b. Cliquez sur **Update**.

   Toutes les alertes qui ne correspondent pas au niveau de gravité et à la classe indiqués sont supprimées de la liste.
3. Pour afficher les informations supplémentaires d'une alerte spécifique dans la zone **Details**, cliquez sur l'alerte en question dans la liste.
4. Pour supprimer le filtre et revenir à la liste complète des alertes supprimées, cliquez sur **Reset**.

Onglet Alerts History

L'onglet Alerts History affiche une liste des alertes supprimées et des détails sur une alerte sélectionnée.

Tableau 67 Liste des alertes, description des libellés de colonne

Élément	Description
Message	Texte du message d'alerte.
Severity	Niveau de gravité de l'alerte. Par exemple : warning, critical, info ou emergency.
Date	Date et heure d'émission de l'alerte.
Class	Sous-système dans lequel l'alerte est survenue.
Object	Composant physique dans lequel l'alerte est survenue.
Status	Indique si l'état est Posted ou Cleared. Une alerte publiée n'a pas été supprimée.

Tableau 68 Zone de détails, description des libellés de ligne

Élément	Description
Name	Identifiant textuel de l'alerte
Message	Texte du message d'alerte.
Severity	Niveau de gravité de l'alerte. Par exemple : warning, critical, info ou emergency.
Class	Sous-système et périphérique dans lesquels l'alerte est survenue.

Tableau 68 Zone de détails, description des libellés de ligne (suite)

Élément	Description
Date	Date et heure d'émission de l'alerte.
Object ID	Composant physique dans lequel l'alerte est survenue.
Event ID	Identifiant d'événement.
Tenant Units	Répertorie les unités tenant concernées.
Additional Information	Informations plus détaillées sur l'alerte.
Status	Indique si l'état est Posted ou Cleared. Une alerte publiée n'a pas été supprimée.
Description	Informations plus détaillées sur l'alerte.
Action	Action suggérée pour corriger l'alerte.

Affichage de l'état des composants matériels

Le volet Hardware châssis affiche un dessin de bloc pour chaque châssis d'un système, avec le numéro de série et l'état du châssis. Chaque dessin de bloc contient les composants du châssis, tels que les disques, les ventilateurs, les modules d'alimentation, la NVRAM, les CPU et la mémoire. Les composants qui s'affichent dépendent du modèle de système.

Sur les systèmes exécutant DD OS 5.5.1 et version ultérieure, le numéro de série du système est également indiqué. Sur les systèmes plus récents, tels que DD4500 et DD7200, le numéro de série du système est indépendant du numéro de série du châssis et reste inchangé lors de nombreux types d'événements de maintenance, dont les remplacements de châssis. Sur les systèmes existants, tels que DD990 et version antérieure, le numéro de série du système est défini sur le numéro de série du châssis.

Procédure

1. Sélectionnez **Hardware** > **châssis**.

   La vue châssis affiche les châssis du système. Le châssis 1 correspond au contrôleur système, et les autres composants apparaissent en dessous du châssis 1.

   Les composants rencontrant des problèmes s'affichent en jaune (avertissement) ou en rouge (erreur) ; sinon, le composant affiche OK.

2. Passez le pointeur de la souris sur un composant pour afficher des informations détaillées sur son état.

État des ventilateurs

Les ventilateurs sont numérotés, ce qui permet d'identifier leur emplacement dans le châssis. Placez le pointeur de la souris sur un des ventilateurs du système pour afficher une infobulle sur ce ventilateur.

Tableau 69 Infobulle relative au ventilateur, description des libellés de colonne

Élément	Description
Description	Nom du ventilateur.
Level	Plage de vitesse de fonctionnement actuelle (Low, Medium, High). La vitesse de fonctionnement change en fonction de la température à l'intérieur du châssis.
Status	État de santé du ventilateur.

État de la température

Les systèmes Data Domain et certains composants sont configurés pour s'exécuter dans une plage de températures spécifique, qui est définie par un profil de température non configurable. Placez le pointeur de la souris sur la zone Temperature pour afficher l'infobulle relative à la température.

Tableau 70 Infobulle relative à la température, description des libellés de colonne

Élément	Description
Description	Emplacement au sein du châssis dans lequel la mesure est réalisée. Les composants répertoriés dépendent du modèle et sont souvent affichés sous forme abrégée. Voici quelques exemples : • CPU 0 Temp (unité centrale de traitement) • MLB Temp 1 (carte mère) • BP middle temp (backplane) • LP temp (FRU de l'adaptateur de connexion d'E/S, format compact) • FHFL temp (FRU de l'adaptateur de connexion d'E/S, plein format) • FP temp (panneau avant)
C/F	La colonne C/F affiche la température en degrés Celsius et Fahrenheit. Lorsque la description d'un CPU indique *relatif* (CPU *n* relatif), cette colonne indique, pour chaque CPU, le nombre de degrés en dessous de la température maximale autorisée et la température réelle à l'intérieur du châssis (température ambiante du châssis).
État	Affiche l'état de la température : • OK : la température est acceptable. • Critical : la température est plus élevée que la température d'arrêt. • Warning : la température est plus élevée que la température d'avertissement (mais inférieure à la température d'arrêt). • Trait (-) : aucun seuil de température n'a été configuré pour ce composant. Aucun état ne peut donc être affiché.

État du panneau de gestion

Les systèmes DD6300, DD6800 et DD9300 ont un panneau de gestion fixe avec un port Ethernet pour le réseau de gestion à l'arrière du châssis. Placez le pointeur de la souris sur le port Ethernet pour afficher une info-bulle.

Tableau 71 Info-bulle relative au panneau de gestion, description des libellés de colonne

Élément	Description
Description	Type de carte réseau installée dans le panneau de gestion.
Vendor	Fabricant de la carte réseau degestion.
Ports	Nom du réseau de gestion (Ma).

État des disques SSD (DD6300 uniquement)

Le DD6300 permet d'insérer jusqu'à deux disques SSD dans les slots à l'arrière du châssis. Les slots de disque SSD sont numérotés, ce qui permet d'identifier leur emplacement dans le châssis. Placez le pointeur de la souris sur un disque SSD pour afficher une infobulle au sujet de ce périphérique.

Tableau 72 Infobulle relative au disque SSD, description des libellés de colonne

Élément	Description
Description	Nom du disque SSD.
Status	État du disque SSD.
Life Used	Pourcentage de la durée de vie nominale écoulée d'un disque SSD.

État des alimentations

L'infobulle affiche l'état des alimentations (OK ou DEGRADED si une alimentation est manquante ou défaillante). Vous pouvez également rechercher à l'arrière du boîtier le voyant correspondant à chaque alimentation afin d'identifier celles qui doivent être remplacées.

État des slots PCI

Les slots PCI affichés dans la vue du châssis indiquent le nombre de slots PCI et les numéros de chaque slot. Les infobulles indiquent l'état des composants de chaque carte dans un slot PCI. Par exemple, l'infobulle d'un modèle de carte NVRAM affiche la taille de la mémoire, les données de température, ainsi que les niveaux de la batterie.

État NVRAM

Placez le pointeur de la souris sur NVRAM pour afficher des informations sur la mémoire RAM non volatile, les batteries et d'autres composants.

Tableau 73 Infobulle NVRAM, description des libellés de colonne

Élément	Description
Composant	Les éléments figurant dans la liste des composants dépendent de la mémoire NVRAM installée dans le système et peuvent être les suivants. • Version du microprogramme • Taille de la mémoire • Compteurs d'erreurs • Compteurs d'erreurs du contrôleur Flash • Température de la carte • Température du CPU • Nombre de batteries (le nombre de batteries dépend du type de système) • Nombre de slots actuel pour NVRAM
C/F	Affiche la température des composants sélectionnés au format Celsius/Fahrenheit.
Valeur	Les valeurs sont fournies pour les composants sélectionnés et décrivent les éléments ci-après. • Numéro de version du microprogramme • Taille de la mémoire dans les unités affichées • Compteurs d'erreurs pour la mémoire, les slots PCI et le contrôleur • Les compteurs d'erreurs du contrôleur Flash sont triés dans les groupes suivants : erreurs de configuration (Cfg Err), fonctionnement de manière inattendue (Panic), bus bloqué, avertissement de blocs défectueux (Bad Blk Warn), erreur de sauvegarde (Bkup Err) et erreurs de restauration (Rstr Err) • Informations sur la batterie, telles que le pourcentage de charge et l'état (activé ou désactivé)

Affichage des statistiques du système

L'onglet Realtime Charts permet d'afficher jusqu'à sept graphiques présentant des statistiques de performances en temps réel du sous-système, telles que le taux d'utilisation du CPU et le trafic sur le disque.

Procédure

1. Sélectionnez **Home** > **Realtime Charts**.

   La zone Performance Graphs affiche les graphiques actuellement sélectionnés.
2. Pour modifier la sélection des graphiques à afficher, cochez et décochez les cases associées aux graphiques dans la zone de liste.
3. Pour afficher des informations spécifiques d'un point de données, placez le pointeur de la souris sur un point du graphique.

4. Lorsqu'un graphique contient plusieurs données, vous pouvez utiliser les cases à cocher situées dans l'angle supérieur droit du graphique pour sélectionner les éléments à afficher. Par exemple, si la case Read n'est pas cochée dans l'angle supérieur droit du graphique de l'activité du disque, seules les données d'écriture sont représentées sous forme graphique.

Résultats

Chaque graphique affiche le taux d'utilisation au cours des 200 dernières secondes. Cliquez sur **Pause** pour arrêter temporairement l'affichage. Cliquez sur **Resume** pour le redémarrer et afficher les points manqués pendant l'interruption.

Graphiques de statistiques des performances

Les graphiques de statistiques des performances fournissent des statistiques pour les principaux composants et fonctionnalités du système.

DD Boost Active Connections

Le graphique relatif aux connexions actives DD Boost affiche le nombre de connexions DD Boost actives au cours des 200 dernières secondes. Les lignes distinctes sur le graphique affichent le nombre de connexions de lecture (restauration) et d'écriture (sauvegarde).

DD Boost Data Throughput

Le graphique relatif au débit des données DD Boost affiche les octets/seconde transférés au cours des 200 dernières secondes. Les lignes distinctes sur le graphique indiquent les taux de données lues depuis le système et de données écrites sur le système par les clients DD Boost.

Disk

Le graphique relatif au disque affiche le volume de données exprimé dans l'unité de mesure appropriée en fonction des données reçues, en KiB ou Mio par seconde, qui entrent et sortent de tous les disques du système.

File System Operations

Le graphique des opérations du système de fichiers affiche le nombre d'opérations par seconde qui se sont produites au cours des 200 dernières secondes. Les lignes distinctes sur le graphique indiquent les opérations NFS et CIFS par seconde.

Network

Le graphique relatif au réseau affiche le volume de données exprimé dans l'unité de mesure appropriée en fonction des données reçues, en KiB ou Mio par seconde, qui transitent via chaque connexion Ethernet. Une ligne s'affiche pour chaque port Ethernet.

Recent CPU Usage

Le graphique relatif au taux d'utilisation récent du CPU affiche le pourcentage du taux d'utilisation du CPU au cours des 200 dernières secondes.

Replication (une licence DD Replicator est requise)

Le graphique relatif à la réplication affiche le volume de données de réplication qui ont transité sur le réseau au cours des 200 dernières secondes. Les lignes distinctes indiquent les données entrantes et sortantes, comme suit :

- In : Nombre total de données, exprimé dans une unité de mesure telle que les kilo-octets par seconde, reçues par ce côté depuis l'autre côté de la paire de

réplication DD. Pour la destination, la valeur inclut les données de sauvegarde, les charges de réplication et réseau. Pour la source, la valeur inclut les charges de réplication et réseau.

- Out : Nombre total de données, exprimé dans une unité de mesure telle que les kilo-octets par seconde, envoyés par ce côté vers l'autre côté de la paire de réplication DD. Pour la source, la valeur inclut les données de sauvegarde, les charges de réplication et réseau. Pour la destination, la valeur inclut les charges de réplication et réseau.

Affichage des utilisateurs actifs

L'onglet Active Users indique les noms des utilisateurs connectés au système et fournit des statistiques sur les sessions utilisateur en cours.

Procédure

1. Sélectionnez **Administration** > **Access** > **Active Users**.

   La liste des utilisateurs actifs s'affiche et présente des informations sur chaque utilisateur.

Tableau 74 Liste des utilisateurs actifs, description des libellés de colonne

Élément	Description
Name	Nom de l'utilisateur connecté.
Idle	Temps écoulé depuis la dernière activité de l'utilisateur.
Last Login From	Système à partir duquel l'utilisateur s'est connecté.
Last Login Time	Date/heure auxquelles l'utilisateur s'est connecté.
TTY	Notation du terminal pour la connexion. L'interface utilisateur s'affiche pour les utilisateurs DD System Manager.

Remarque

Pour gérer les utilisateurs locaux, cliquez sur **Go to Local Users**.

Gestion des rapports d'historique

DD System Manager vous permet de générer des rapports afin de surveiller l'utilisation de l'espace d'un système Data Domain sur des périodes allant jusqu'à deux ans. Vous pouvez également générer des rapports utiles pour suivre la progression et afficher des rapports quotidiens et cumulatifs sur le système de fichiers.

La vue Reports est divisée en deux sections. La section supérieure vous permet de créer les différents types de rapport. La section inférieure vous permet quant à elle d'afficher et de gérer les rapports enregistrés.

Ces rapports s'affichent sous forme de tableaux et de graphiques, en fonction du type de rapport. Vous pouvez sélectionner un rapport pour un système Data Domain spécifique et indiquer une période spécifique.

Ces rapports affichent des données historiques, et non des données en temps réel. Une fois le rapport généré, les graphiques sont statiques et ne sont pas mis à jour.

Voici quelques exemples des types d'informations que vous pouvez obtenir dans les rapports :

- Quantité de données sauvegardées sur le système et niveau de déduplication atteint
- Estimations du moment où le système Data Domain sera plein, d'après les tendances d'utilisation hebdomadaires de l'espace
- Utilisation de la sauvegarde et de la compression selon des intervalles sélectionnés
- Performances de l'historique du nettoyage, dont la durée de cycle de nettoyage, la quantité d'espace nettoyée et la quantité d'espace récupérée
- Quantité de bande passante WAN utilisée par la réplication, pour la source et la cible, et si la bande passante est suffisante pour répondre aux besoins en matière de réplication
- Performances du système et utilisation des ressources

Types de rapport

La zone New Report répertorie les types de rapports que vous pouvez générer sur votre système.

Remarque

Les rapports de réplication ne peuvent être créés que si le système possède une licence de réplication et qu'un contexte de réplication valide a été configuré.

Rapport cumulatif d'utilisation de l'espace du système de fichiers

Le rapport cumulatif d'utilisation de l'espace du système de fichiers affiche 3 graphiques qui détaillent l'utilisation de l'espace sur le système, au cours de la période indiquée. Il vous permet d'analyser la quantité de données sauvegardées, la quantité de déduplication effectuée et la quantité d'espace utilisée.

Tableau 75 Description des libellés du graphique représentant l'utilisation du système de fichiers

Élément	Description
Data Written (Gio)	Quantité de données écrites avant la compression. Celle-ci est indiquée par une zone grisée violette sur le rapport.
Time	Chronologie des données qui ont été écrites. Le temps affiché sur ce rapport change en fonction de la sélection de la durée lors de la création du graphique.
Total Compression Factor	Le facteur de compression totale indique le taux de compression.

Tableau 76 Description des libellés du graphique représentant la consommation du système de fichiers

Élément	Description
Used (Gio)	Quantité d'espace utilisé après la compression.
Time	Date à laquelle les données ont été écrites. Le temps affiché sur ce rapport change en fonction de la sélection de la durée lors de la création du graphique.

Tableau 76 Description des libellés du graphique représentant la consommation du système de fichiers (suite)

Élément	Description
Used (Post Comp)	Quantité de stockage utilisé après la compression.
Usage Trend	La ligne en pointillé noire représente la tendance de l'utilisation du stockage. Lorsque la ligne atteint la ligne rouge du haut, le stockage est quasiment saturé.
Capacity	Capacité totale d'un système Data Domain.
Cleaning	Cycle de nettoyage (heures de début et de fin de chaque cycle de nettoyage). Les administrateurs peuvent utiliser ces informations pour choisir le meilleur moment pour le nettoyage de l'espace et le meilleur paramètre de régulation.

Tableau 77 Description des libellés du graphique des capacités hebdomadaires cumulées du système de fichiers

Élément	Description
Date (or Time for 24 hour report)	Dernier jour de chaque semaine, en fonction des critères définis pour le rapport. Dans les rapports, une période de 24 heures s'étend de midi à midi.
Data Written (Pre-Comp)	Données écrites cumulées avant la compression pour la période de temps spécifiée.
Used (Post-Comp)	Données écrites cumulées après la compression pour la période de temps spécifiée.
Compression Factor	Facteur de compression totale. Celui-ci est indiqué par une ligne noire sur le rapport.

Rapport quotidien détaillant l'utilisation de l'espace du système de fichiers

Le rapport quotidien de l'utilisation de l'espace du système de fichiers contient cinq graphiques qui présentent en détail l'utilisation de l'espace sur la durée spécifiée. Il vous permet d'analyser les activités quotidiennes.

Tableau 78 Description des libellés de champ représentant l'utilisation quotidienne de l'espace du système de fichiers

Élément	Description
Space Used (Gio)	Quantité d'espace utilisé. Les données post-compression sont représentées par une zone grisée rouge. Les données pré-compression sont représentées par une zone grisée violette.
Time	Date à laquelle les données ont été écrites.
Compression Factor	Facteur de compression totale. Celui-ci est indiqué par un carré noir sur le rapport.

Tableau 79 Description des libellés de champ représentant l'utilisation quotidienne des capacités du système de fichiers

Élément	Description
Date	Date à laquelle les données ont été écrites.
Data Written (Pre-Comp)	Quantité de données écrites avant la compression.
Used (Post-Comp)	Quantité de stockage utilisé après la compression.
Total Compression Factor	Facteur de compression totale.

Tableau 80 Description des libellés de champ représentant l'utilisation hebdomadaire des capacités du système de fichiers

Élément	Description
Start Date	Premier jour de la semaine de ce récapitulatif.
End Date	Dernier jour de la semaine de ce récapitulatif.
Available	Volume total de stockage disponible.
Consumed	Volume total de stockage utilisé.
Data (Post -Comp)	Données écrites cumulées avant la compression pour la période de temps spécifiée.
Replication (Post-Comp)	Données écrites cumulées après la compression pour la période de temps spécifiée.
Overhead	Espace supplémentaire utilisé pour le stockage hors données.
Reclaimed by Cleaning	Espace total récupéré après le nettoyage.

Tableau 81 Description des libellés de champ récapitulatif de la compression du système de fichiers

Élément	Description
Time	Période de collecte des données pour ce rapport.
Data Written (Pre-Comp)	Quantité de données écrites avant la compression.
Used (Post-Comp)	Quantité de stockage utilisé après la compression.
Total Compression Factor	Facteur de compression totale.

Tableau 82 Description des libellés de champ représentant l'opération de nettoyage du système de fichiers

Élément	Description
Start Time	Heure de début de l'opération de nettoyage.
End Time	Heure de fin de l'opération de nettoyage.
Duration (Hours)	Durée totale requise pour le nettoyage en heures.
Space Reclaimed	Espace récupéré en Gibibytes (Gio).

Rapport sur l'état de la réplication

Le rapport sur l'état de la réplication contient trois graphiques qui indiquent l'état de la tâche de réplication en cours sur le système. Il vous donne une vue d'ensemble des opérations en cours pour tous les contextes de réplication, pour mieux appréhender l'état global de la réplication sur le système Data Domain.

Tableau 83 Description des libellés de champ récapitulatif des contextes de réplication

Élément	Description
ID	Identification du contexte de réplication.
Source	Nom du système source.
Destination	Nom du système de destination.
Type	Type de contexte de réplication : MTree, Directory, Collection ou Pool.
Status	Les types d'état de la réplication sont les suivants : Error, Normal.
Sync as of Time	Date et heure de la dernière synchronisation.
Estimated Completion	Heure à laquelle la réplication est censée se terminer.
Pre-Comp Remaining	Quantité de données précompressées à répliquer. Cela s'applique uniquement au type Collection.
Post-Comp Remaining	Quantité de données post-compressées à répliquer. Cela s'applique uniquement aux types Directory et Pool.

Tableau 84 Description des libellés de champ d'état d'erreur des contextes de réplication

Élément	Description
ID	Identification du contexte de réplication.
Source	Nom du système source.
Destination	Nom du système de destination.
Type	Type de contexte de réplication : Directory ou Pool.
Status	Les types d'état de la réplication sont les suivants : Error, Normal et Warning.
Description	Description de l'erreur.

Tableau 85 Description des libellés de champ représentant la disponibilité de l'espace sur le système de destination de la réplication

Élément	Description
Destination	Nom du système de destination.
Space Availability (Gio)	Volume total de stockage disponible.

Rapport récapitulatif de la réplication

Le rapport récapitulatif de la réplication fournit des informations de performance de l'utilisation globale du réseau, en entrée et en sortie, d'un système pour la réplication, ainsi que par niveaux de contexte sur une durée spécifiée. Sélectionnez les contextes à analyser dans la liste.

Tableau 86 Description des libellés du rapport récapitulatif de la réplication

Élément	Description
Network In (Mio)	Quantité de données entrantes dans le système. Le réseau entrant est indiqué par une fine ligne verte.
Network Out (Mio)	Quantité de données sortantes dans le système. Le réseau sortant est indiqué par une épaisse ligne orange.
Time	Date à laquelle les données ont été écrites.
Pre-Comp Remaining (Mio)	Quantité de données précompressées à répliquer. Cette quantité de données précompressées est indiquée par une ligne bleue.

Affichage du log des tâches

Le log de tâches contient la liste des tâches actuellement en cours d'exécution, telles que la réplication ou les mises à niveau du système. DD System Manager peut gérer plusieurs systèmes et démarrer des tâches sur ces systèmes. Si une tâche est démarrée sur un système distant, la progression de cette tâche est indiquée dans le log des tâches de la station de gestion, et non dans celui des tâches du système distant.

Procédure

1. Sélectionnez **Health** > **Jobs**.

   La vue Tasks s'affiche.

2. Sélectionnez un filtre permettant d'afficher le log de tâches dans la zone de liste Filter By. Vous pouvez sélectionner **All**, **In Progress**, **Failed** ou **Completed**.

   La vue Tasks affiche l'état de toutes les tâches en fonction du filtre sélectionné et s'actualise toutes les 60 secondes.

3. Pour actualiser manuellement la liste de tâches, effectuez l'une des opérations suivantes :

   - Cliquez sur **Update** pour mettre à jour le log de tâches.
   - Cliquez sur **Reset** pour afficher toutes les tâches et supprimer tous les filtres qui ont été définis.

4. Pour afficher des informations détaillées sur une tâche, sélectionnez la tâche dans la liste des tâches.

Tableau 87 Informations détaillées, description des libellés

Élément	Description
System	Nom du système.
Task Description	Description de la tâche.
Status	État de la tâche (completed, failed ou in progress).
Start Time	Date et heure de début de la tâche.
End Time	Date et heure de fin de la tâche.
Error Message	Message d'erreur applicable, le cas échéant.

Affichage de l'état HA du système

Vous pouvez utiliser le volet **High Availability** pour afficher des informations détaillées sur l'état HA du système et savoir s'il peut effectuer un basculement sur incident si nécessaire.

Procédure

1. Sélectionnez **Health > High Availability** sur DD System Manager.

   L'écran **Health High Availability** s'affiche.
   Une coche verte indique que le système fonctionne normalement et qu'il est prêt pour le basculement sur incident.

   L'écran affiche le nœud actif, qui est généralement le nœud 0.

2. Passez le curseur sur un nœud pour voir son état.

   Le nœud est encadré en bleu s'il est actif.

3. Cliquez sur le menu déroulant dans la bannière si vous voulez basculer entre l'affichage du nœud actif et celui du nœud en veille, qui est généralement le nœud 1.

État de la haute disponibilité

La vue **Health High Availability**(HA) vous informe de l'état du système à l'aide d'un schéma des nœuds et de leur stockage connecté. En outre, vous pouvez également voir les alertes en cours, ainsi que des informations détaillées sur le système.

Vous pouvez déterminer si le nœud actif et le stockage sont opérationnels en déplaçant le curseur sur ceux-ci. Chacun d'entre eux est encadré en bleu, ce qui indique un fonctionnement normal. Le nœud en veille doit apparaître en gris.

Vous pouvez également filtrer le tableau des alertes en cliquant sur un composant. Seules les alertes concernant les composants sélectionnés s'affichent.

Figure 6 Indicateurs d'intégrité/de haute disponibilité

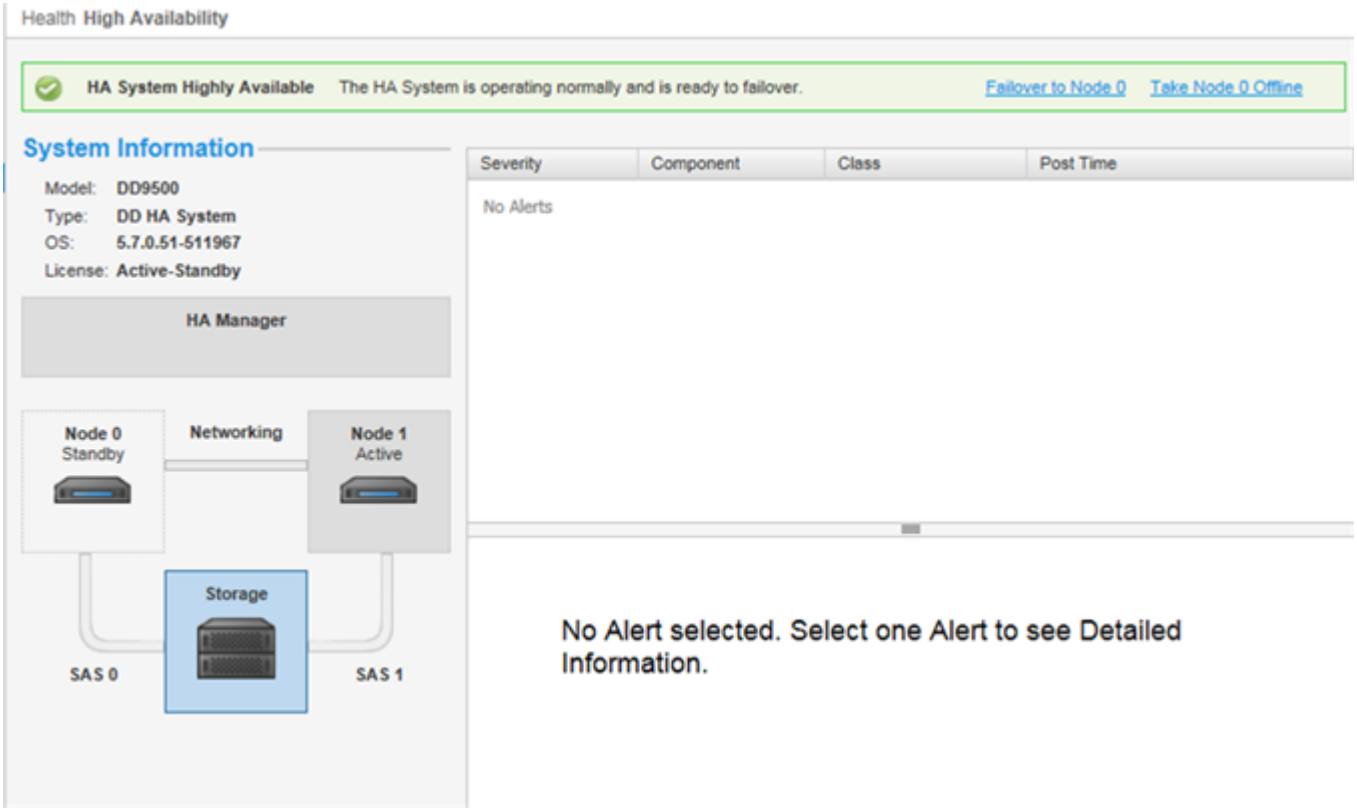


Tableau 88 Indicateurs de la haute disponibilité

Élément	Description
Barre du système haute disponibilité	Affiche une coche verte lorsque le système fonctionne normalement et qu'il est prêt pour le basculement sur incident.
Failover to Node 0	Vous permet de basculer manuellement sur le nœud en veille.
Take Node 1 Offline	Vous permet de mettre le nœud actif hors ligne si nécessaire.
System Information	Répertorie le modèle du système Data Domain, le type de système, la version du système d'exploitation Data Domain en cours d'utilisation et la licence HA appliquée.
HA Manager	Affiche les nœuds, leur stockage rattaché, l'interconnexion HA et le câblage.
Severity	Indique la gravité de toutes les alertes susceptibles d'avoir un impact sur l'état HA du système.
Component	Indique quel composant est affecté.
Class	Indique la classe de l'alerte reçue, telle que le matériel, l'environnement et d'autres.

Tableau 88 Indicateurs de la haute disponibilité (suite)

Élément	Description
Post Time	Indique l'heure et la date auxquelles l'alerte a été publiée.

CHAPITRE 5

Système de fichiers

Ce chapitre inclut les sections suivantes :

Tour d’horizon du système de fichiers

Découvrez comment utiliser le système de fichiers.

Mode de stockage des données utilisé par le système de fichiers

Le meilleur moyen de gérer la capacité de stockage de Data Domain consiste à effectuer plusieurs sauvegardes et à garder 20 % d'espace libre pour accueillir des sauvegardes jusqu'au prochain nettoyage. L'utilisation de l'espace est principalement affectée en fonction de la taille et de la compressibilité des données, et de la période de rétention.

Un système Data Domain est conçu comme un système en ligne très fiable pour les sauvegardes et l'archivage des données. Au fur et à mesure que de nouvelles sauvegardes sont ajoutées au système, les anciennes deviennent obsolètes. Les suppressions de ce type sont normalement effectuées sous le contrôle d'un logiciel de sauvegarde ou d'archivage en fonction de la période de rétention définie.

Lorsque le logiciel de sauvegarde expire ou supprime une ancienne sauvegarde d'un système Data Domain, l'espace correspondant sur le système Data Domain ne devient disponible qu'une fois que le système Data Domain a nettoyé les données des sauvegardes expirées sur le disque. Un bon moyen de contrôler l'espace sur un système Data Domain consiste à conserver autant de sauvegardes en ligne que possible avec de l'espace vide (environ 20% de l'espace total disponible) pour accueillir aisément des sauvegardes jusqu'au nettoyage programmé suivant, qui s'exécute une fois par semaine par défaut.

Une certaine capacité de stockage est utilisée par les systèmes Data Domain pour les index internes et d'autres métadonnées. La quantité de stockage utilisée dans le temps pour les métadonnées dépend du type de données stockées et de la taille des fichiers stockés. Avec deux systèmes identiques, un système peut au fil du temps réserver davantage d'espace que l'autre pour les métadonnées et moins d'espace pour les données de sauvegarde réelles si différents datasets sont envoyés à chaque système.

L'utilisation de l'espace sur un système Data Domain est principalement affectée par :

- La taille et la compressibilité des données de sauvegarde.
- La période de rétention définie dans le logiciel de sauvegarde.

De hauts niveaux de compression sont mis en œuvre lors de la sauvegarde de datasets contenant un grand nombre de doublons et lors de leur conservation pendant de longues périodes.

Mode de création de rapports sur l’utilisation de l’espace par le système de fichiers

Toutes les commandes du système et les fenêtres DD System Manager affichent la capacité de stockage à l’aide de calculs en base 2. Par exemple, une commande qui affiche 1 Gio d’espace disque utilisé indique 2^{30} octets = 1 073 741 824 octets.

- 1 KiB = 2^{10} = 1 024 octets
- 1 Mio = 2^{20} = 1 048 576 octets
- 1 Gio = 2^{30} = 1 073 741 824 octets
- 1 Tio = 2^{40} = 1 099 511 627 776 octets

Mode de compression utilisé par le système de fichiers

Le système de fichiers utilise la compression pour optimiser l'espace disque disponible en stockant les données, ce qui signifie que l'espace disque est calculé de deux manières : physiquement et logiquement. (Reportez-vous à la section concernant les types de compression.) L'espace physique est l'espace disque physique réellement utilisé sur le système Data Domain. L'espace logique est la quantité de données non compressées écrites sur le système.

Les outils de reporting de l'espace du système de fichiers (graphiques DD System Manager et la commande `filesys show space` ou l'alias `df`) affichent les espaces physique et logique. Ces outils indiquent également la taille et les quantités de l'espace utilisé et disponible.

Lorsqu'aucun système Data Domain n'est monté, les outils traditionnels permettant d'afficher l'espace physique utilisé d'un système de fichiers peuvent être utilisés.

Le système Data Domain génère des messages d'avertissement lorsque le système de fichiers atteint 90 %, 95 % et 100 % de sa capacité. Les informations ci-après relatives à la compression des données contiennent des instructions sur l'utilisation de disques au fil du temps.

La quantité d'espace disque utilisée au fil du temps par un système Data Domain dépend des points suivants :

- La taille de la sauvegarde complète initiale.
- Le nombre de sauvegardes supplémentaires (incrémentielles et complètes) conservées au fil du temps.
- Le taux de croissance du dataset de sauvegarde.
- Le taux de modification des données.

Pour les datasets avec des taux habituels de modification et de croissance, la compression des données répond généralement aux lignes directrices suivantes :

- Pour la première sauvegarde complète sur un système Data Domain, le facteur de compression est généralement de 3:1.
- Chaque sauvegarde incrémentielle jusqu'à la sauvegarde complète initiale a un facteur de compression généralement de l'ordre de 6:1.
- La sauvegarde complète suivante a un facteur de compression d'environ 60:1.

Au fil du temps, avec un planning de sauvegardes complètes (hebdomadaires) et incrémentielles (quotidiennes), le facteur de compression global pour toutes les données est d'environ 20:1. Le facteur de compression est plus faible pour les sauvegardes de données uniquement incrémentielles ou pour les sauvegardes avec moins de données en double. Le facteur de compression est plus élevé lorsque toutes les sauvegardes sont des sauvegardes complètes.

Types de compression

Data Domain compresse les données à deux niveaux : global et local. La compression globale compare les données reçues aux données déjà stockées sur les disques. Les données dupliquées n'ont pas besoin d'être à nouveau stockées, tandis que les nouvelles données sont localement compressées avant d'être écrites sur le disque.

Compression locale
Un système Data Domain utilise un algorithme de compression locale développé spécifiquement pour optimiser le débit lors de l'écriture des données sur le disque. L'algorithme par défaut (lz) permet de réduire les fenêtres de sauvegarde pour les procédures de sauvegarde, mais utilise plus d'espace. Deux autres types de

compression locale sont disponibles, gzfast et gz. Les deux offrent une compression accrue sur lz, mais au détriment de la charge de CPU supplémentaire. Les options de compression locale offrent un compromis entre des performances réduites et l'utilisation de l'espace. Il est également possible de désactiver la compression locale. Pour modifier la compression, reportez-vous à la compression Modification de la compression locale à la page 228

Une fois la compression modifiée, toutes les nouvelles écritures utilisent le nouveau type de compression. Les données existantes sont converties vers le nouveau type de compression lors du nettoyage. Il faut plusieurs cycles de nettoyage pour recompresser toutes les données qui existaient avant la modification de la compression.

Le premier nettoyage après la modification de compression peut prendre plus longtemps que d'habitude. Chaque fois que vous modifiez le type de compression, surveillez attentivement le système pendant une ou deux semaines pour vérifier qu'il fonctionne correctement.

Mode de mise en œuvre de l'intégrité des données par le système de fichiers

Plusieurs couches de vérification des données sont réalisées par le système de fichiers DD OS sur les données reçues depuis les applications de sauvegarde, afin de garantir que les données sont correctement écrites sur les disques du système Data Domain. Les données peuvent ainsi être extraites sans erreur.

DD OS est conçu pour la protection des données, ainsi que pour l'invulnérabilité des données, de par son architecture. Quatre points spécifiques, décrits dans les sections suivantes, doivent être considérés avec attention.

Vérification de bout en bout

Les vérifications de bout en bout protègent toutes les données et les métadonnées du système de fichiers. Lorsque les données arrivent dans le système, un checksum fort est calculé. Les données sont dédupliquées et enregistrées dans le système de fichiers. Une fois toutes les données vidées sur le disque, elles sont relues et leur checksum est à nouveau contrôlé. Les checksums sont comparés pour vérifier que les données et les métadonnées du système de fichiers sont correctement enregistrées.

Prévention et maîtrise des pannes

Data Domain utilise un système de fichiers journalisé qui n'écrase ou n'actualise jamais des données existantes. Les nouvelles données sont toujours écrites dans de nouveaux conteneurs et ajoutées à d'anciens conteneurs existants. Les anciens conteneurs et les anciennes références restent en place et sont sécurisés même en cas de bugs logiciels ou de pannes matérielles lors du stockage de nouvelles sauvegardes.

Détection et correction des pannes en continu

La détection et la correction des pannes en continu évitent les pannes du système de stockage. Le système revérifie régulièrement l'intégrité des bandes RAID, et s'appuie sur la redondance du système RAID pour corriger les éventuelles pannes. Lors d'une lecture, l'intégrité des données est revérifiée et toutes les erreurs sont corrigées à la volée.

Capacité de restauration du système de fichiers

Les données sont enregistrées dans un format autodescriptif. Si nécessaire, il est possible de recréer le système de fichiers en analysant le journal et en le reconstruisant à partir des métadonnées stockées avec les données.

Mode de récupération d'espace de stockage utilisé par le système de fichiers avec nettoyage du système de fichiers

Lorsque votre application de sauvegarde (par exemple NetWorker ou NetBackup) définit des données comme ayant expiré, celles-ci sont désignées pour la suppression par le système Data Domain. Cependant, elles ne sont pas immédiatement éliminées du disque ; elles ne le sont qu'au nettoyage suivant.

- Pendant l'opération de nettoyage, le système de fichiers reste disponible pour toutes les opérations habituelles, notamment pour la sauvegarde (écriture) et la restauration (lecture).
- Bien que le nettoyage utilise intensément les ressources système, l'opération s'autorégule et abandonne les ressources système en présence de trafic utilisateur.
- Il est recommandé d'exécuter une opération de nettoyage après la première sauvegarde complète d'un système Data Domain. Lors d'une sauvegarde complète, le facteur de compression locale initial est généralement compris entre 1,5 et 2,5. Une opération de nettoyage immédiate permet une compression supplémentaire d'un facteur compris entre 1,15 et 1,2, avec récupération de l'espace disque correspondant.
- Une fois l'opération de nettoyage terminée, un message est envoyé au log du système, indiquant le pourcentage d'espace de stockage récupéré.

Un planning par défaut exécute l'opération de nettoyage tous les mardis à 6h00 (tue 0600). Vous pouvez modifier le planning ou exécuter l'opération manuellement (reportez-vous à la section relative à la modification d'un planning de nettoyage).

Data Domain recommande d'exécuter une opération de nettoyage une fois par semaine.

Toute opération qui désactive le système de fichiers ou arrête un système Data Domain lors d'une opération de nettoyage (comme une mise hors tension ou le redémarrage du système) arrête l'opération de nettoyage. L'opération de nettoyage ne redémarre pas immédiatement lors du redémarrage du système. Vous pouvez redémarrer manuellement l'opération de nettoyage ou attendre le prochain nettoyage planifié.

Avec la réplication de collection, les données dans un contexte de réplication sur le système source qui n'a pas été répliqué ne peuvent pas être traitées pour le nettoyage du système de fichiers. Si le nettoyage du système de fichiers n'est pas terminé parce que les systèmes sources et cibles ne sont pas synchronisés, le système signale l'état de l'opération de nettoyage comme étant `partiel`, et seules des statistiques limitées sont disponibles pour l'opération de nettoyage. Si la réplication de collection est désactivée, la quantité de données qui ne peuvent pas être traitées pour le nettoyage du système de fichiers augmente car la source de réplication et les systèmes cibles restent désynchronisés. L'article de la base de connaissances : *Data Domain : Un tour d'horizon des phases de nettoyage et de collecte de garbage (GC) de Data Domain File System (DDFS)*, disponible sur le site de support en ligne à l'adresse https://support.emc.com fournit des informations supplémentaires.

Dans le cadre d'une réplication de structures MTree, si un fichier est créé, puis supprimé lors de la réplication d'un snapshot, le snapshot suivant n'aura alors aucune

information sur ce fichier et le système ne répliquera aucun contenu associé à ce fichier. La réplication de répertoire réplique les opérations de création et de suppression, même si elles se produisent à un court laps de temps l'une de l'autre.

Avec le log de réplication utilisé par la réplication de répertoire, les opérations telles que les suppressions, les changements de nom, etc., s'exécutent comme un seul flux. Cela peut réduire le débit de la réplication. L'utilisation d'une réplication de snapshots par MTree résout ce problème.

Interfaces prises en charge

Interfaces prises en charge par le système de fichiers.

- NFS
- CIFS
- DD Boost
- DD VTL

Logiciel de sauvegarde pris en charge

Vous trouverez sur le site support.emc.com des instructions sur la configuration des logiciels et serveurs de sauvegarde à utiliser avec des systèmes Data Domain.

Flux de données envoyés à un système Data Domain

Pour des performances optimales, Data Domain recommande des limites sur les flux simultanés entre les systèmes Data Domain et vos serveurs de sauvegarde.

Un flux de données, dans le cadre du tableau suivant, fait référence à un grand flux d'octets associé à un accès séquentiel aux fichiers, tel qu'un flux d'écriture dans un fichier de sauvegarde ou un flux de lecture d'une image de restauration. Un flux source ou cible de réplication fait référence à une opération de réplication de répertoire ou à un flux de réplication de fichiers DD Boost associé à une opération de réplication de fichiers.

Tableau 89 Flux de données envoyés à un système Data Domain

Modèle	RAM/ NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD140, DD160, DD610	4 Go ou 6 Go/ 0,5 Go	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630 et DD640	8 Go/0,5 Go ou 1 Go	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 Go ou 20 Go/1 Go	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90

Tableau 89 Flux de données envoyés à un système Data Domain (suite)

Modèle	RAM/ NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD670, DD860	36 Go/1 Go	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 Go[b] / 1 Go	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 Go/2 Go	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 ou 256 Go[b] / 4 Go	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 Go	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 Go	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 ou 64 Go/ 2 Go	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 Go[b] / 4 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 Go[b] / 4 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 ou 256 Go[b] / 4 Go	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 Go	1 885	300	540	1 080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD9800	256/768 Go	1 885	300	540	1 080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD6300	48/96 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270

Tableau 89 Flux de données envoyés à un système Data Domain (suite)

Modèle	RAM/ NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD6800	192 Go	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8 To	8 Go / 512 Mo	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE (16 To)	16 Go / 512 Mo ou 24 Go / 1 Go	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE (32 To)	24 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (48 To)	36 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 To	48 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (96 To)	64 Go/2 Go	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 (4 To)	12 Go (mémoire virtuelle) / 512 Mo	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 To	32 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (16 To)	32 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (32 To)	46 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. Flux DirRepl, OptDup, MTreeRepl
b. La fonction Data Domain Extended Retention n'est disponible que pour ces périphériques avec une mémoire (maximale) étendue

Limitations du système de fichiers

Limitations du système de fichiers, y compris les limites du nombre de fichiers, de la batterie et ainsi de suite.

Limites au nombre de fichiers d'un système Data Domain

Conséquences et remarques pour le stockage de plus de 1 milliard de fichiers.

Data Domain recommande de ne pas stocker plus d'un milliard de fichiers sur un système. Enregistrer un plus grand nombre de fichiers peut dégrader les performances, ainsi que la longueur du nettoyage. De même, certains processus, tels que le nettoyage du système de fichiers, peuvent nécessiter beaucoup plus de temps avec un très grand nombre de fichiers. Par exemple, la phase d'énumération du nettoyage peut durer de quelques minutes à plusieurs heures en fonction du nombre de fichiers dans le système.

Remarque

Les performances globales du système Data Domain chuteront à des niveaux inacceptables si le système doit prendre en charge la quantité maximale de fichiers et que la charge applicative des machines clientes n'est pas soigneusement contrôlée.

Lorsque le système de fichiers franchit la limite du milliard de fichiers, plusieurs processus ou opérations peuvent être sévèrement affectés, par exemple :

- Le nettoyage peut prendre beaucoup de temps, à savoir plusieurs jours.
- Les opérations d'autosupport peuvent prendre plus de temps encore.
- Tout processus ou commande nécessitant d'énumérer tous les fichiers.

S'il y a un grand nombre de petits fichiers, d'autres éléments doivent être pris en compte :

- Le nombre de fichiers distincts pouvant être créés par seconde (même si les fichiers sont très petits) peut être plus limitant que le nombre de Mo/s pouvant être déplacés vers un système Data Domain. Lorsque les fichiers sont volumineux, le taux de création de fichiers n'est pas significatif, mais lorsque les fichiers sont petits, ce taux prédomine et peut devenir un facteur à prendre en compte. Le taux de création de fichiers est d'environ 100 à 200 fichiers par seconde selon le nombre de structures MTree et de connexions CIFS. Ce taux doit être pris en compte lors du dimensionnement des systèmes quand un traitement en bloc d'un grand nombre de fichiers est exigé par un environnement client.
- Les temps de latence d'accès aux fichiers sont affectés par le nombre de fichiers figurant dans un répertoire. Dans la mesure du possible, il est recommandé que les répertoires contiennent moins de 250 000 fichiers. Des tailles de répertoire supérieures peuvent entraîner des réponses plus lentes pour les opérations de métadonnées, telles que la génération de la liste des fichiers figurant dans le répertoire et l'ouverture ou la création d'un fichier.

Limites de la batterie

Dans les systèmes qui utilisent NVRAM, le système d'exploitation crée une alerte de batterie faible si le niveau de charge de la batterie tombe en dessous de 80 % de la capacité. Le système de fichiers est ensuite désactivé.

NOTE

Le système Data Domain DD2200 n'utilise pas NVRAM de sorte que les calculs du microprogramme déterminent si la charge de la batterie est suffisante pour enregistrer les données et désactivent le système de fichiers en cas de perte d'alimentation CA.

Nombre maximal d'inodes pris en charge

Suite à une demande client NFS ou CIFS, un système Data Domain indique une capacité d'environ deux milliards d'inodes (fichiers et répertoires). Un système Data Domain peut dépasser cette valeur, mais le reporting sur le client peut être incorrect.

Longueur maximale de nom de chemin d'accès

La longueur maximale d'un nom de chemin complet (caractères `/data/col1/backup` inclus) est de 61 caractères. La longueur maximale d'un lien symbolique est également de 61 caractères.

Accès limité lors d'un basculement sur incident HA

L'accès aux fichiers peut être interrompu pendant 10 minutes au maximum au cours du basculement sur incident sur les systèmes haute disponibilité (DD Boost et NFS nécessitent davantage de temps).

Surveillance de l'utilisation du système de fichiers

Affichez des statistiques sur le stockage de données en temps réel.

La vue File System contient des onglets et des commandes donnant accès à des statistiques sur le stockage de données en temps réel, à des informations sur les unités de Cloud et sur le chiffrement et aux volumes d'espace utilisés sous forme de graphiques, aux facteurs de consommation et aux tendances des données écrites. Elle contient également des commandes de gestion du nettoyage, de l'extension, de la copie et la destruction du système de fichiers.

Accès à la vue File System

Cette section décrit la fonctionnalité File System.

Procédure

- Sélectionnez **Data Management** > **File System**.

À propos du panneau File System Status

Affichez l'état des services de système de fichiers.

Pour accéder au panneau File System Status, cliquez sur **Data Management** > **File System** > **Show Status of File System Services**.

Système de fichiers
Le champ **File System** contient un lien **Enable/Disable** et indique l'état de fonctionnement du système de fichiers :

- Enabled and running : et la dernière durée ininterrompue durant laquelle le système de fichiers a été activé et en cours d'exécution.
- Disabled and shutdown : désactivé et arrêté.

- Enabling and disabling : en cours d'activation et de désactivation.
- Destroyed : si le système de fichiers est supprimé.
- Error : s'il existe une condition d'erreur, telle qu'un problème d'initialisation du système de fichiers.

Cloud File Recall
Le champ **Cloud File Recall** contient un lien **Recal** pour lancer un rappel des fichiers à partir du niveau cloud. Un lien **Details** n'est disponible que si les rappels actifs sont en cours. Pour plus d'informations, consultez la rubrique « Rappel d'un fichier à partir du niveau cloud ».

Mesure de la capacité physique
Le champ **Physical Capacity Measurement** contient un bouton **Enable** lorsque l'état de la mesure de la capacité physique est Disabled (désactivé). Après l'activation, le système affiche les boutons **Disable** et **View**. Cliquez sur **View** pour afficher les mesures de capacité physique en cours d'exécution : MTree, priorité, heure d'envoi, heure de début et durée.

Déplacement de données
Le champ **Data Movement** contient les boutons**Start/Stop** et indique la date de la dernière opération de déplacement des données, le nombre de fichiers copiés et la quantité de données copiées. Le système affiche un bouton **Start** lorsque l'opération de déplacement des données est disponible, ainsi qu'un bouton **Stop** lorsqu'une opération de déplacement des données est en cours d'exécution.

Nettoyage du niveau actif
Le champ **Active Tier Cleaning** contient un bouton **Start/Stop** et indique la date de la dernière opération de nettoyage ou l'état de nettoyage actuel si l'opération est en cours d'exécution. Par exemple :

```
Cleaning finished at 2009/01/13 06:00:43
```

ou, si le système de fichiers est désactivé :

```
Unavailable
```

Nettoyage du niveau Cloud
Le champ **Cloud Tier Cleaning** contient un bouton **Start/Stop** et indique la date de la dernière opération de nettoyage ou l'état de nettoyage actuel si l'opération est en cours d'exécution. Par exemple :

```
Cleaning finished at 2009/01/13 06:00:43
```

ou, si le système de fichiers est désactivé :

```
Non disponible
```

À propos de l'onglet Summary

Cliquez sur l'onglet Summary pour afficher les statistiques d'utilisation de l'espace pour le niveau actif et le niveau Cloud et pour accéder aux commandes permettant d'afficher l'état du système de fichiers, de configurer les paramètres du système de fichiers, d'exécuter une opération Fast Copy, d'étendre la capacité et de détruire le système de fichiers.

Les statistiques d'utilisation de l'espace, présentées pour chaque niveau, sont les suivantes :

- **Size** : quantité totale d'espace sur le disque physique disponible pour les données.
- **Used** : espace physique réel utilisé pour les données compressées. Les messages d'avertissement sont envoyés au fichier journal et une alerte par e-mail est générée lorsque l'utilisation atteint 90 %, 95 % et 100 %. À 100 %, le système Data Domain n'accepte plus de données provenant des serveurs de sauvegarde. Si la quantité utilisée est toujours élevée, vérifiez l'ordonnanceur de nettoyage pour savoir combien de fois les opérations de nettoyage s'exécutent automatiquement. Utilisez ensuite la procédure de modification de l'ordonnanceur de nettoyage pour effectuer l'opération plus souvent. Envisagez également de réduire la période de rétention des données ou de séparer une partie des données de sauvegarde sur un autre système Data Domain.
- **Available** (Gio) : quantité totale d'espace disponible pour le stockage de données. Ce nombre peut changer car un index interne peut se développer à mesure que le système Data Domain se remplit de données. L'extension de l'index s'effectue au détriment de la quantité de Gio d'espace disponible.
- **Pre-Compression** (Gio) : données écrites avant la compression.
- **Total Compression Factor (Reduction %)** : pré-compression / post-compression.
- **Cleanable** (Gio) : quantité d'espace pouvant être récupérée en cas d'exécution d'un nettoyage.

Pour Cloud Tier, le champ **Cloud File Recall** contient un lien **Recal** pour lancer un rappel des fichiers à partir du niveau cloud. Un lien **Details** n'est disponible que si les rappels actifs sont en cours. Pour plus d'informations, consultez la rubrique « Rappel d'un fichier à partir du niveau cloud ».

Des panneaux distincts présentent les statistiques suivantes (relatives aux dernières 24 heures) pour chaque niveau :

- **Pre-Compression** (Gio) : données écrites avant la compression.
- **Post-Compression** (Gio) : stockage utilisé après la compression.
- **Global Compression Factor** : (pré-compression / taille après compression globale).
- **Local Compression Factor** : (taille après compression globale / post-Compression).
- **Total Compression Factor (Reduction %)** : [(pré-compression) - post-compression) / pré-compression] * 100.

À propos de des paramètres du système de fichiers

Affichez et modifiez les options système, ainsi que le planning de nettoyage en cours.

Pour accéder à la boîte de dialogue File System Settings, cliquez sur **Data Management** > **File System** > **Settings**.

Tableau 90 Paramètres généraux

Paramètres généraux	Description
Local Compression Type	Type de compression locale en cours d'utilisation. • Reportez-vous à la section relative aux types de compression pour obtenir un aperçu. • Reportez-vous à la section relative à la modification de la compression locale.

Tableau 90 Paramètres généraux (suite)

Paramètres généraux	Description
Cloud Tier Local Comp	Type de compression en cours d'utilisation pour la hiérarchisation du Cloud. • Reportez-vous à la section relative aux types de compression pour obtenir un aperçu. • Reportez-vous à la section relative à la modification de la compression locale.
Report Replica as Writable	Comment les applications perçoivent un réplica. • Reportez-vous à la section relative à la modification des paramètres en lecture seule.
Staging Reserve	Gestion du stockage temporaire sur disque. • Reportez-vous à la section relative à l'utilisation du stockage temporaire sur disque. • Reportez-vous à la section relative à la configuration du stockage temporaire sur disque.
Marker Type	Marqueurs de logiciel de sauvegarde (marqueurs de bande, en-têtes de balise ou d'autres noms sont utilisés) dans les flux de données. Reportez-vous à la section relative aux paramètres de marqueurs de bande.
Throttle	Reportez-vous à la section relative à la configuration de la régulation de la mesure de la capacité physique.
Cache	L'initialisation du cache de la capacité physique nettoie les caches et améliore la vitesse de mesure.

Vous pouvez régler l'équilibrage de la charge du système de fichiers pour améliorer les performances en fonction de votre utilisation.

Tableau 91 Paramètres d'équilibrage de charge applicative

Paramètres d'équilibrage de charge applicative	Description
Random workloads (%)	L'utilisation de charges applicatives aléatoires donne de meilleurs résultats en termes d'accès instantanés et de restaurations.
Sequential workloads (%)	Les sauvegardes et les restaurations traditionnelles sont plus efficaces avec des charges applicatives séquentielles.

Tableau 92 Paramètres de déplacement des données

Paramètres de règle de déplacement des données	Description
File Age Threshold	Lorsque le déplacement des données débute, tous les fichiers qui n'ont pas été modifiés durant le nombre de jours seuil

Tableau 92 Paramètres de déplacement des données (suite)

Paramètres de règle de déplacement des données	Description
	spécifié seront déplacés du niveau actif vers le niveau de rétention.
Schedule	Jours et heures auxquels les données sont déplacées.
Throttle	Pourcentage de ressources disponibles que le système utilise pour le déplacement des données. Une valeur de régulation de 100 % représente la régulation par défaut et signifie que le déplacement des données ne sera pas régulé.

Tableau 93 Paramètres de nettoyage

Paramètres de planification du nettoyage	Description
Time	Date/heure de l'exécution des opérations de nettoyage. • Reportez-vous à la section relative à la modification d'un planning de nettoyage.
Throttle	Allocation des ressources du système. • Reportez-vous à la section relative à la régulation de l'opération de nettoyage.

À propos de l'onglet Cloud Units

Affichez les données récapitulatives des unités de Cloud, ajoutez et modifiez des unités de Cloud et gérez les certificats.

L'onglet Cloud Units de la page File Systems s'affiche à condition d'avoir activé la licence DD Cloud Tier optionnelle. Cette vue contient des données récapitulatives (état du Cloud, bande passante réseau, accès en lecture, compression locale, déplacement des données et état des données), le nom du fournisseur de Cloud, la capacité utilisée et la capacité sous licence. Plusieurs commandes sont proposées pour modifier l'unité de Cloud, gérer les certificats et ajouter une nouvelle unité de Cloud.

À propos de l'onglet Retention Units

Affichez l'unité de rétention ainsi que son état, son statut et sa taille.

L'onglet Retention Units de la page File Systems s'affiche à condition d'avoir activé la licence DD Extended Retention optionnelle. Cette vue répertorie l'unité de rétention et affiche son état (new, sealed ou target), son statut (disabled ou ready) et sa taille. Si l'unité a été scellée, ce qui signifie qu'aucune autre donnée ne peut être ajoutée, la date à laquelle elle a été scellée est indiquée.

Sélectionnez le symbole en forme de losange situé à droite d'un en-tête de colonne pour trier les valeurs dans l'ordre inverse.

À propos de l'onglet DD Encryption

Affichez entre autres l'état, la progression et les algorithmes de chiffrement.

Tableau 94 Paramètres de chiffrement DD

Paramètre	Description
DD System	Les états disponibles sont les suivants : • Not licensed : aucune autre information n'est fournie. • Not configured : la licence du logiciel Encryption est installée, mais pas configurée. • Enabled : le logiciel Encryption est activé et en cours d'exécution. • Disabled : le logiciel Encryption est désactivé.
Active Tier	Permet d'afficher l'état du chiffrement pour le niveau actif : • Enabled : le logiciel Encryption est activé et en cours d'exécution. • Disabled : le logiciel Encryption est désactivé.
Cloud Unit	Permet d'afficher l'état du chiffrement par unité de cloud : • Enabled : le logiciel Encryption est activé et en cours d'exécution. • Disabled : le logiciel Encryption est désactivé.
Encryption Progress	Permet d'afficher les détails de l'état du chiffrement pour le niveau actif par rapport à l'application des modifications et au rechiffrement des données. Les états disponibles sont les suivants : • None (aucun) • Pending (en attente) • Running (en cours d'exécution) • Done (terminé) Cliquez sur View Details pour afficher la boîte de dialogue Encryption Status Details qui contient les informations suivantes pour le niveau actif : • Type (exemple : appliquez les modifications lorsque le chiffrement a déjà été lancé ou le rechiffrement lorsque le chiffrement est le résultat de données compromises, peut-être une clé précédemment détruite.) • Status (exemple : Pending) • Details : (exemple : demandé en décembre, le xx/xx/xx et prendra effet après le prochain nettoyage du système).
Encryption Algorithm	Algorithme utilisé pour chiffrer les données : • AES 256-bit (CBC) (valeur par défaut) • AES 256-bit (GCM) (plus sécurisé mais plus lent) • AES 128-bit (CBC) (pas aussi sécurisé que la version 256-bit)

Tableau 94 Paramètres de chiffrement DD (suite)

Paramètre	Description
	• AES 128-bit (GCM) (pas aussi sécurisé que la version 256-bit) Pour plus d'informations, reportez-vous à la section Modification de l'algorithme de chiffrement.
Encryption Passphrase	Une fois celle-ci configurée, s'affiche sous la forme « ***** ». Pour modifier la phrase de passe, reportez-vous à la section Gestion de la phrase de passe du système.
File System Lock	
Status	L'état de verrouillage du système de fichiers peut être : • Unlocked : la fonction n'est pas activée. • Locked : la fonction est activée.
Key Management	
Key Manager	Embedded Key Manager (intégré à Data Domain) ou RSA DPM (Data Protection Manager) Key Manager. Cliquez sur **Configure** pour passer d'un gestionnaire de clés à l'autre (si les deux sont configurés) ou pour modifier les options du gestionnaire de clés.
Server	Nom du serveur RSA Key Manager.
Server Status	En ligne ou hors ligne, ou les messages d'erreur renvoyés par le serveur RSA Key Manager.
Key Class	Type de classe de sécurité spécialisé utilisé par le RSA DPM (Data Protection Manager) Key Manager, regroupant les clés de chiffrement qui possèdent des caractéristiques similaires. Le système Data Domain extrait une clé du serveur RSA par classe de clés. Classe de clés à configurer afin de renvoyer la clé actuelle ou générer une nouvelle clé à chaque fois. **Remarque** Le système Data Domain ne prend en charge que les classes de clés configurées pour renvoyer la clé actuelle.
Port	Numéro de port du serveur RSA.
FIPS mode	Détermine si le certificat d'hôte importé est conforme à la norme FIPS. Le mode par défaut est activé.
Encryption Keys	Répertorie les clés par numéros d'ID. Indique la date de création d'une clé, sa durée de validité, son type (RSA DPM Key Manager ou la clé interne de Data Domain), son état (voir Utilisation du RSA DPM Key Manager, États des clés de chiffrement de gestion de la protection des données pris en charge par Data Domain) et la quantité de données chiffrées avec la clé. Le système affiche l'heure de la dernière mise à jour des informations de la clé au-dessus de la colonne de droite. Les clés sélectionnées dans la liste peuvent être :

Tableau 94 Paramètres de chiffrement DD (suite)

Paramètre	Description
	• Synchronisées afin que la liste affiche les nouvelles clés ajoutées au serveur RSA (mais ne peuvent pas être utilisées tant que le système de fichiers n'a pas été redémarré). • Supprimées. • Détruites.

À propos de la vue Space Usage (système de fichiers)

Affichez une représentation visuelle (mais statique) de l'utilisation des données du système de fichiers à certains points dans le temps.

Cliquez sur **Data Management** > **File System** > **Charts**. Sélectionnez **Space Usage** dans la liste déroulante Chart.

Pour afficher les données correspondant à un point, cliquez sur ce point sur le graphique. Les lignes du graphique indiquent les mesures suivantes :

- Pre-comp Written : volume total de données envoyé à la MTree par les serveurs de sauvegarde. Les données précompressées se trouvant sur une MTree sont considérées par le serveur de sauvegarde comme les données non compressées totales conservées par une « MTree comme unité de stockage », représentées sur l'axe vertical du graphique correspondant à l'espace utilisé (à gauche).
- Post-comp Used : volume total de stockage sur disque en cours d'utilisation sur la structure MTree, indiqué sur l'axe vertical Space Used, à gauche du graphique.
- Comp Factor : facteur de compression appliqué par le système Data Domain aux données reçues (taux de compression), indiqué sur l'axe vertical Compression Factor, à droite du graphique.

Vérification de l'utilisation historique de l'espace
Un clic sur une plage de dates (1w, 1m, 3m,1y ou All) au-dessus du graphique Space Usage vous permet de modifier le nombre de jours de données affichés sur le graphique (de 1 semaine à toutes les plages de dates).

À propos de la vue Consumption

Affichez l'espace utilisé dans le temps, par rapport à la capacité totale du système.

Cliquez sur **Data Management** > **File System** > **Charts**. Sélectionnez **Consumption** dans la liste déroulante Chart.

Pour afficher les données correspondant à un point, cliquez sur ce point sur le graphique. Les lignes du graphique indiquent les mesures suivantes :

- Capacity : volume total de stockage sur disque disponible pour les données sur le système Data Domain. Ce volume est indiqué sur l'axe vertical Space Used, à gauche du graphique. Cochez la case Capacity pour activer/désactiver cette ligne.
- Post-comp : volume total de stockage sur disque en utilisation sur le système Data Domain. Il est indiqué sur l'axe vertical Space Used (Espace utilisé), à gauche du graphique.
- Comp Factor : facteur de compression appliqué par le système Data Domain aux données reçues (taux de compression). Le facteur de compression est indiqué sur l'axe vertical Compression Factor, à droite du graphique.

- Cleaning : un losange gris s'affiche sur le graphique chaque fois qu'une opération de nettoyage du système de fichiers est démarrée.
- Data Movement : quantité d'espace disque déplacée vers la zone de stockage d'archivage (si la licence d'archivage est activée).

Contrôle de l'utilisation de la consommation historique
Un clic sur une plage de dates (1w, 1m, 3m,1y ou All) au-dessus du graphique Consumption vous permet de modifier le nombre de jours de données affichés sur le graphique (de 1 semaine à toutes les plages de dates).

À propos de la vue Daily Written (système de fichiers)

Affichez le flux de données au fil du temps. Les volumes de données sont présentés dans le temps avant et après compression.

Cliquez sur **Data Management** > **File System** > **Charts**. Sélectionnez **Daily Written** dans la liste déroulante Chart.

Pour afficher un encadré contenant les données correspondant à un point, cliquez sur ce point sur le graphique. Les lignes du graphique indiquent les mesures suivantes :

- Pre-comp Written : volume total de données écrites sur le système de fichiers par les serveurs de sauvegarde. Les données précompressées sur le système de fichiers sont celles qu'un serveur de sauvegarde considère comme le volume total de données non compressées détenues par le système de fichiers.
- Post-Comp Written : volume total des données écrites sur le système de fichiers une fois la compression effectuée, indiqué en Gio.
- Total Comp Factor : quantité totale de compression appliquée par le système Data Domain aux données reçues (taux de compression), représentée par la valeur Total Compression Factor sur l'axe vertical (droit) du graphique.

Vérification des données écrites historiques
Un clic sur une plage de dates (1w, 1m, 3m,1y ou All) au-dessus du graphique Daily Written vous permet de modifier le nombre de jours de données affichés sur le graphique (de 1 semaine à toutes les plages de dates).

Lorsque le système de fichiers est plein ou presque plein

Les systèmes Data Domain disposent de trois niveaux de saturation progressifs. À chaque nouveau niveau atteint, de moins en moins d'opérations sont autorisées. À chaque niveau, la suppression de données et l'exécution d'une opération de nettoyage du système de fichiers libèrent de l'espace disque.

Remarque

Le processus de suppression de fichiers et de retrait de snapshots ne permet pas de récupérer immédiatement de l'espace disque. La prochaine opération de nettoyage récupérera de l'espace.

- Niveau 1 : au premier niveau de saturation, aucune nouvelle donnée ne peut être écrite sur le système de fichiers. Une alerte d'espace insuffisant est générée à titre d'information.
  Solution : supprimez les Datasets inutiles, réduisez la période de conservation, supprimez des snapshots et exécutez une opération de nettoyage du système de fichiers.
- Niveau 2 : au deuxième niveau de saturation, les fichiers ne peuvent pas être supprimés. En effet, la suppression de fichiers nécessite également de l'espace

disponible, mais le système dispose de si peu d'espace libre qu'il ne peut même pas supprimer des fichiers.
Solution : faites expirer des snapshots et exécutez une opération de nettoyage du système de fichiers.

- Niveau 3 : au troisième et dernier niveau de saturation, les tentatives de faire expirer des snapshots, de supprimer des fichiers ou d'écrire de nouvelles données échouent.
Solution : exécutez une opération de nettoyage du système de fichiers afin de libérer suffisamment d'espace pour supprimer au moins quelques fichiers ou faire expirer certains snapshots, puis réexécutez l'opération de nettoyage.

Surveillance de l'utilisation de l'espace avec des alertes par e-mail

Des alertes sont générées lorsque le système de fichiers atteint 90 %, 95 % ou 100 % de sa capacité. Pour envoyer ces alertes, ajoutez l'utilisateur à la liste de diffusion des alertes.

Remarque

Pour accéder à liste de diffusion des alertes, reportez-vous à la section relative à l'affichage et la suppression des alertes.

Gestion des opérations du système de fichiers

Cette section décrit les opérations de nettoyage du système de fichiers et la réalisation d'opérations de base.

Exécution d'opérations de base

Les opérations de base relatives au système de fichiers incluent l'activation et la désactivation du système de fichiers et, dans de rares cas, la destruction d'un système de fichiers.

Création d’un système de fichiers

Créez un système de fichiers dans la page Data Management > File System à l’aide de l’onglet Summary.

Il existe trois raisons de créer un système de fichiers :

- Pour un nouveau système Data Domain.
- Lorsqu’un système est démarré après une installation correcte.
- Après la destruction d’un système de fichiers.

Pour créer un système de fichiers :

Procédure

1. Vérifiez que le stockage a été installé et configuré (reportez-vous à la section relative à l’affichage des informations de stockage du système pour en savoir plus). Si le système ne répond pas à cette condition préalable, un message d’avertissement s’affiche. Installez et configurez le stockage avant d’essayer de créer un système de fichiers.
2. Sélectionnez **Data Management** > **File System** > **Summary** > **Create**.

Cela a pour effet de lancer l'assistant de création de système de fichiers. Suivez les instructions fournies.

Activation ou désactivation du système de fichiers

L'option permettant d'activer ou de désactiver le système de fichiers dépend de l'état actuel du système de fichiers. Autrement dit, si ce dernier est activé, vous pouvez le désactiver, et inversement.

- L'activation du système de fichiers permet aux opérations du système Data Domain de commencer. Cette capacité n'est accessible qu'aux administrateurs.
- La désactivation du système de fichiers arrête toutes les opérations du système Data Domain, y compris le nettoyage. Cette capacité n'est accessible qu'aux administrateurs.

⚠ ATTENTION

La désactivation du système de fichiers lorsqu'une application de sauvegarde envoie les données au système peut provoquer l'échec du processus de sauvegarde. Certaines applications logicielles de sauvegarde sont en mesure d'effectuer des restaurations en redémarrant là où elles s'étaient arrêtées lorsqu'elles peuvent reprendre correctement la copie des fichiers ; d'autres risquent d'échouer et de fournir une sauvegarde incomplète à l'utilisateur.

Procédure

1. Sélectionnez **Data Managment** > **File System** > **Summary**.
2. Activez ou désactivez le **système de fichiers** en cliquant sur **Enable** ou **Disable**.
3. Cliquez sur **Close** dans la boîte de dialogue de confirmation.

Extension du système de fichiers

Vous devrez peut-être augmenter la taille d'un système de fichiers si les suggestions décrites dans la section « Lorsque le système de fichiers est plein ou presque plein » n'ont pas permis de libérer suffisamment d'espace pour les opérations normales.

Toutefois, un système de fichiers peut ne pas être extensible, pour les raisons suivantes :

- Le système de fichiers n'est pas activé.
- Il n'y a aucun disque ou châssis inutilisé dans les niveaux Active, Retention ou Cloud.
- Aucune licence basée sur le stockage étendu n'est installée.
- Le nombre de licences basées sur la capacité installées n'est pas suffisant.

Les systèmes DD6300 permettent d'utiliser des châssis ES30 avec des disques de 4 To (43,6 Tio) à un taux d'utilisation de 50 % (soit 21,8 Tio) sur le niveau actif, si la capacité sous licence disponible correspond exactement à 21,8 Tio. Les directives suivantes s'appliquent à l'utilisation de tiroirs à capacité partielle.

- Les autres types de châssis ou les autres tailles de disque ne sont pas pris en charge dans le cadre d'une utilisation partielle de la capacité.
- Un tiroir partiel ne peut exister que sur le niveau actif.
- Un seul châssis ES30 partiel est permis dans le niveau actif.

- Une fois créé, aucun autre châssis ES30 ne peut être configuré sur ce niveau, tant que le tiroir partiel n'est pas ajouté à pleine capacité.

  Remarque

  La capacité supplémentaire sous licence doit être suffisante pour tirer parti des 21,8 Tio restants du tiroir partiel.

- Si la capacité disponible dépasse 21,8 To, il est impossible d'ajouter un tiroir partiel.
- La suppression d'une licence de 21 Tio ne permet pas de convertir automatiquement un tiroir entièrement utilisé en tiroir partiel. Le tiroir doit être retiré, puis rajouté en tant que tiroir partiel.

Pour étendre le système de fichiers :

Procédure

1. Sélectionnez **Data Managment** > **File System** > **Summary** > **Expand Capacity**.

   Cela a pour effet de lancer l'assistant d'extension de la capacité de stockage du système de fichiers (Expand File System Capacity). La liste déroulante **Storage Tier** contient toujours le niveau actif (Active), et elle peut éventuellement proposer le niveau de rétention étendue (Extended Retention) ou le niveau Cloud comme choix secondaire. L'assistant affiche la capacité actuelle du système de fichiers pour chaque niveau, ainsi que l'espace de stockage supplémentaire disponible pour l'extension.

   Remarque

   La capacité du système de fichiers peut être étendue uniquement si les disques physiques sont installés sur le système et que le système de fichiers est activé.

2. Sélectionnez un niveau dans la liste déroulante **Storage Tier**.
3. Dans la zone **Addable Storage**, sélectionnez les périphériques de stockage à utiliser, puis cliquez sur **Add to Tier**.
4. Suivez les instructions de l'assistant. Lorsque la page de confirmation s'affiche, cliquez sur **Close**.

Destruction du système de fichiers

La destruction du système de fichiers ne doit être effectuée que sur instruction du Support Clients. Cette action supprime toutes les données du système de fichiers, y compris des bandes virtuelles. Les données supprimées ne peuvent pas être restaurées. Cette opération supprime également les paramètres de configuration de la réplication.

Cette opération est utilisée lorsqu'il est nécessaire de nettoyer les données existantes, de créer une nouvelle destination de réplication de collection, de remplacer une source de collecte ou pour des raisons de sécurité lorsque le système est retiré de l'exploitation.

⚠ ATTENTION

L'opération facultative Write zeros to disk écrit des zéros sur tous les disques du système de fichiers, supprimant efficacement toutes traces de données. Si le système Data Domain contient un grand nombre de données, cette opération peut prendre plusieurs heures, voire une journée.

Remarque

Comme il s'agit d'une procédure destructrice, cette opération n'est accessible qu'aux utilisateurs administrateurs.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Summary** > **Destroy**.
2. Dans la boîte de dialogue Destroy File System, saisissez le mot de passe sysadmin (le seul mot de passe à être accepté).
3. Vous pouvez, si vous le souhaitez, cocher la case **Write zeros to disk** pour supprimer complètement les données.
4. Cliquez sur **OK**.

Exécution d'un nettoyage

Cette section fournit des informations sur le nettoyage et décrit comment démarrer, arrêter et modifier les programmes de nettoyage.

DD OS tente de maintenir un compteur appelé « Cleanable GiB » pour le niveau actif. Ce nombre est une estimation de l'espace physique (après compression) qui peut être récupéré dans le niveau actif par l'exécution du nettoyage et de la collecte de garbage. Ce compteur s'affiche à l'aide des commandes `filesys show space` et `df`.

```
Active Tier:
Resource Size GiB Used GiB Avail GiB Use% Cleanable GiB*
---------------- -------- --------- --------- ----
--------------
/data: pre-comp - 7259347.5 - - -
/data: post-comp 304690.8 251252.4 53438.5 82% 51616.1 <=== NOTE
/ddvar 29.5 12.5 15.6 44% -
---------------- -------- --------- --------- ----
--------------
```

Exécutez le nettoyage du niveau actif propre si :

- La valeur de « Cleanable GiB » est importante
- Le SFDD est plein à 100 % (et est donc en lecture seule).

Le nettoyage peut ne pas récupérer tout l'espace potentiel en une seule exécution. Sur les systèmes Data Domain contenant de très grands ensembles de données, le nettoyage s'applique à la partie du système de fichiers contenant les données les plus superflues et peut devoir être exécuté plusieurs fois avant que tout l'espace potentiel soit récupéré.

Démarrage du nettoyage

Pour démarrer immédiatement une opération de nettoyage.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Summary** > **Settings** > **Cleaning**.

   L'onglet **Cleaning** de la boîte de dialogue **File System Setting** affiche les paramètres configurables pour chaque niveau.

2. Pour le niveau actif :

   a. Dans la zone de texte Throttle %, saisissez le pourcentage de régulation du système. Il s'agit du pourcentage de l'utilisation du CPU dédiée au nettoyage. La valeur par défaut est 50 %.

b. Dans la liste déroulante Frequency, sélectionnez l'une des fréquences suivantes : Never, Daily, Weekly, Biweekly et Monthly. La fréquence hebdomadaire (Weekly) est définie par défaut.

c. Pour At, configurez une heure spécifique.

d. Pour On, sélectionnez un jour de la semaine.

3. Pour le niveau Cloud :

a. Dans la zone de texte Throttle %, saisissez le pourcentage de régulation du système. Il s'agit du pourcentage de l'utilisation du CPU dédiée au nettoyage. La valeur par défaut est 50 %.

b. Dans la liste déroulante Frequency, sélectionnez l'une des fréquences suivantes : Never, After every 'N' Active Tier cleans.

Remarque

Toute unité de Cloud non accessible pendant le nettoyage du niveau Cloud sera ignorée. Le nettoyage sur l'unité de Cloud en question aura lieu lors de l'exécution suivante, à condition que l'unité de Cloud devienne disponible. Le planning de nettoyage détermine l'intervalle entre deux exécutions. Si l'unité de Cloud devient disponible et que vous ne pouvez pas attendre la prochaine exécution planifiée, vous pouvez démarrer le nettoyage de façon manuelle.

4. Cliquez sur **Save**.

Remarque

Pour démarrer l'opération de nettoyage à l'aide de la CLI, utilisez la commande `filesys clean start`.

```
# filesys clean start
Cleaning started. Use 'filesys clean watch' to monitor progress.
```

Pour confirmer que le nettoyage est en cours, utilisez la commande `filesys status`.

```
# filesys status
The filesystem is enabled and running.
Cleaning started at 2017/05/19 18:05:58: phase 1 of 12 (pre-merge)
50.6% complete, 64942 GiB free; time: phase 0:01:05, total 0:01:05
```

Si le nettoyage est déjà en cours, le message suivant s'affiche lorsqu'on tente de le démarrer.

```
**** Cleaning already in progress. Use 'filesys clean watch' to monitor
progress.
```

Remarque

Si le nettoyage n'est pas en mesure de démarrer, contactez le fournisseur de support contractuel pour obtenir de l'aide supplémentaire. Ce problème peut indiquer que le système a rencontré une `erreur de segment manquant`, provoquant la désactivation du nettoyage.

Planification ou arrêt du nettoyage

Pour arrêter immédiatement ou planifier une opération de nettoyage.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Summary** > **Settings** > **Cleaning**.

   L'onglet Cleaning de la boîte de dialogue File System Setting affiche les paramètres configurables pour chaque niveau.

2. Pour le niveau actif :

   a. Dans la liste déroulante Frequency, sélectionnez la fréquence souhaitée.

3. Pour le niveau Cloud :

   a. Dans la liste déroulante Frequency, sélectionnez la fréquence souhaitée.

4. Cliquez sur **Save**.

Remarque

La CLI peut être utilisée pour vérifier qu'un planning de nettoyage a été défini.

```
# filesys clean show schedule
```

Si nécessaire, définissez un planning de nettoyage du niveau actif. L'exemple suivant définit le nettoyage à effectuer tous les mardis à 06h00 :

```
# filesys clean set schedule Tue 0600
Filesystem cleaning is scheduled to run "Tue" at "0600".
```

Sur les systèmes qui sont configurés avec la fonction Extended Retention (ER), le nettoyage peut être configuré pour s'exécuter après que le mouvement des données est terminé et peut ne pas avoir son propre planning séparé.

Réalisation d'un nettoyage

Pour vous conformer aux recommandations de l'administration, vous devez effectuer un nettoyage, aussi appelé destruction des données, lorsque des données sensibles ou classifiées sont écrites sur un système qui n'est pas homologué pour stocker ce type de données.

Lorsqu'un incident se produit, l'administrateur système doit prendre des mesures immédiates pour supprimer totalement les données qui ont été accidentellement écrites. L'objectif est de ramener efficacement le périphérique de stockage à l'état qu'il aurait si l'événement ne s'était jamais produit. Si la fuite d'informations concerne des données sensibles, l'ensemble du stockage doit être nettoyé en appliquant la méthodologie de suppression des données sécurisées des Professional Services pour Data Domain.

La commande de nettoyage de Data Domain a pour vocation de permettre à l'administrateur de supprimer des fichiers au niveau logique, qu'il s'agisse d'un jeu de sauvegardes ou de fichiers individuels. Dans la plupart des systèmes de fichiers, la suppression d'un fichier se résume à baliser le fichier ou à supprimer les références aux données sur le disque afin de libérer de l'espace physique en vue d'une utilisation ultérieure. Toutefois, cette action simple est à l'origine d'un problème, à savoir qu'elle laisse une représentation résiduelle physique des données sous-jacentes sur des disques. Les environnements de stockage dédupliqués ne sont pas immunisés contre ce problème.

La destruction des données dans un système implique d'éliminer la représentation résiduelle de ces données et donc la possibilité que ce fichier soit accessible après sa destruction. L'approche appliquée par Data Domain au nettoyage est conforme aux versions 2007 des spécifications suivantes de la directive 5220.22 du Ministère américain de la défense (DoD) :

- *Directive 5220.22-M du Ministère américain de la défense, Clearing and Sanitization Matrix*
- *Publication spéciale 800-88 du National Institute of Systems and Technology (NIST), Guidelines for Media Sanitization*

Nettoyage de données dédupliquées

Les systèmes Data Domain nettoient les données en place, dans leur état natif dédupliqué.

Les systèmes de stockage avec déduplication extraient les modèles de données courants à partir des fichiers envoyés au système et n'enregistrent que des copies uniques de ces modèles, en référençant toutes les instances redondantes. Étant donné que ces modèles ou segments de données sont susceptibles d'être partagés entre plusieurs fichiers dans le système, le processus de nettoyage doit d'abord déterminer si chaque segment du fichier contaminé est partagé avec un fichier propre, puis effacer uniquement les segments qui ne sont pas partagés, ainsi que toutes les métadonnées contaminées.

Tous les niveaux de stockage, caches, capacités inutilisées et espaces libres sont supprimés afin que chaque copie de chaque segment appartenant exclusivement aux fichiers supprimés soit éliminée. Le système récupère et écrase tout le stockage occupé par ces segments afin de ramener efficacement le périphérique de stockage à l'état qu'il aurait si aucun fichier contaminé n'avait jamais existé dans ce système.

Niveau de nettoyage 1 : effacement ou destruction des données

Si les données que vous devez supprimer ne sont pas classifiées, selon la définition qu'en donne la Directive 5220.22-M du Ministère américain de la Défense, Clearing and Sanitization Matrix, le nettoyage de niveau 1 peut être utilisé pour écraser une seule fois le stockage concerné. Cela constitue la base du traitement de la plupart des cas de destruction des données et de nettoyage du système.

La fonction de nettoyage du système Data Domain garantit que chaque copie de chaque segment appartenant uniquement à des fichiers supprimés est écrasée à l'aide d'un mécanisme d'insertion de zéros à passage unique. Les données propres se trouvant dans le système en cours de nettoyage sont en ligne et disponibles pour les utilisateurs.

Procédure

1. Supprimez les fichiers ou les sauvegardes contaminés par le biais du logiciel de sauvegarde ou du client correspondant. Dans le cas de sauvegardes, assurez-vous que vous gérez le logiciel de sauvegarde correctement pour veiller à ce que les fichiers associés sur cette image soient rapprochés, les enregistrements de catalogue gérés en fonction des besoins, et ainsi de suite.
2. Exécutez la commande `system sanitize start` sur le système Data Domain contaminé pour que tout l'espace utilisé précédemment dans ce système soit écrasé en une fois (voir la figure ci-dessous).
3. Attendez que le système affecté soit nettoyé. Le nettoyage peut être surveillé à l'aide de la commande `system sanitize watch`.

   Si la réplication est activée sur le système Data Domain affecté, tous les systèmes contenant des réplicas doivent être traités de la même manière. En fonction de la quantité de données présentes dans le système et de la façon dont elles sont distribuées, l'exécution de la commande `system sanitize` peut prendre un certain temps. Toutefois, pendant ce temps, toutes les données propres du système sont à la disposition des utilisateurs.

Niveau de nettoyage 2 : nettoyage complet du système

Si les données que vous devez supprimer sont classifiées, selon la définition qu'en donne la Directive 5220.22-M du Ministère américain de la Défense, Clearing and Sanitization Matrix, le nettoyage de niveau 2, ou nettoyage complet du système, est alors nécessaire.

Data Domain recommande Blancco pour les écrasements multipasses avec n'importe quel modèle d'écrasement et un certificat. Cela constitue la base du traitement des exigences universelles du Ministère de la défense qui imposent un nettoyage complet du système. Pour en savoir plus, rendez-vous sur :

https://www.emc.com/auth/rcoll/servicekitdocument/cp_datadomaindataerase_psbasddde.pdf

Modification des paramètres de base

Modifiez le type de compression utilisé, les types de marqueur, l'état d'écriture du réplica et le pourcentage de réserve de stockage temporaire, comme décrit dans cette section.

Modification de la compression locale

Pour configurer le type de compression local, utilisez l'onglet General de la boîte de dialogue File System Settings.

Remarque

Ne modifiez le type de compression locale que si cela est nécessaire.

Procédure

1. Sélectionnez **Data Managment** > **File System** > **Summary** > **Settings** > **General**.
2. Dans la liste déroulante Local Compression Type, sélectionnez un type de compression.

Tableau 95 Type de compression

Option	Description
NONE	Ne pas compresser les données.
LZ	Algorithme par défaut offrant le meilleur débit. Data Domain recommande d'utiliser l'option lz.
GZFAST	Compression de type zip qui utilise moins d'espace pour les données compressées, mais plus de cycles CPU (deux fois plus que l'option lz). L'option gzfast est la solution alternative recommandée pour les sites qui souhaitent obtenir plus de compression au détriment des performances.
GZ	Compression de type zip qui utilise le moins d'espace pour le stockage de données (de 10 à 20 % de moins que la compression lz en moyenne ; toutefois, certains datasets obtiennent une compression beaucoup plus élevée). Cette option utilise également le plus de cycles CPU (jusqu'à cinq fois plus que l'option lz). Le type de compression gz est couramment utilisé pour les applications de stockage nearline dont les exigences de performances sont faibles.

3. Cliquez sur **Save**.

Modification des paramètres de lecture seule

Faites passer le réplica à l'état inscriptible. Certaines applications de sauvegarde doivent voir le réplica comme étant inscriptible pour effectuer une opération de restauration ou de stockage en chambre forte à partir du réplica.

Procédure

1. Sélectionnez **Data Managment** > **File System** > **Summary** > **Settings** > **General**.
2. Dans la zone Report Replica as Writable, basculez entre **Disabled** (désactivé) et **Enabled** (activé) comme il convient.
3. Cliquez sur **Save**.

Utilisation du stockage temporaire sur disque

Le stockage temporaire sur disque permet d'utiliser un système Data Domain comme périphérique de staging, dans lequel le système est considéré comme un disque de base via un partage CIFS ou un point de montage NFS.

Le stockage temporaire sur disque peut être utilisé conjointement avec votre logiciel de sauvegarde, tel que Symantec NetBackup (NBU) et NetWorker. Il ne nécessite pas de licence et est désactivé par défaut.

Remarque

La fonction DD VTL n'est pas requise ou n'est pas prise en charge lorsque le système Data Domain est utilisé en tant que périphérique de stockage temporaire sur disque.

Certaines applications de sauvegarde utilisent des périphériques de stockage temporaire sur disque afin d'activer la diffusion des lecteurs de bande en continu. Une fois les données copiées sur bandes, elles sont conservées sur disque tant qu'il y a suffisamment d'espace disponible. Si une restauration doit être effectuée à partir d'une sauvegarde récente, il est plus probable que les données soient toujours sur le disque et puissent être plus facilement restaurées à partir du disque, plutôt qu'à partir des bandes. Une fois le disque plein, les anciennes sauvegardes peuvent être supprimées pour libérer de l'espace. Cette politique de suppression à la demande optimise l'utilisation du disque.

En fonctionnement normal, le système Data Domain ne récupère pas d'espace des fichiers supprimés tant qu'une opération de nettoyage n'est pas effectuée. Cela n'est pas compatible avec un logiciel de sauvegarde qui fonctionne en mode staging, qui s'attend à ce que l'espace soit récupéré lorsque des fichiers sont supprimés. Lorsque vous configurez le stockage temporaire sur disque, vous réservez un pourcentage de l'espace total, habituellement de 20 à 30 %, afin de permettre au système de simuler la libération immédiate de l'espace.

La quantité d'espace disponible est réduite de la quantité réservée pour le staging. Lorsque la quantité de données stockées utilise tout l'espace disponible, le système est saturé. Toutefois, dès qu'un fichier est supprimé, le système estime la quantité d'espace qui sera récupérée par le nettoyage et emprunte ce même volume dans la réserve de staging afin d'augmenter l'espace disponible. Lors de l'exécution d'une opération de nettoyage, l'espace est réellement récupéré et la réserve restaurée à sa taille d'origine. La quantité d'espace rendue disponible par la suppression des fichiers n'étant qu'une estimation, la quantité d'espace réellement récupérée par l'opération de nettoyage peut être différente. L'objectif du stockage temporaire sur disque est de

configurer suffisamment d'espace de réserve pour qu'il y en ait assez avant l'exécution de l'opération de nettoyage planifiée.

Configuration du stockage temporaire sur disque

Activez le stockage temporaire sur disque et définissez un pourcentage de réserve de stockage temporaire.

Procédure

1. Sélectionnez **Data Managment** > **File System** > **Summary** > **Settings** > **General**.
2. Dans la zone Staging Reserve, basculez entre **Disabled** (désactivé) et **Enabled** (activé) comme il convient.
3. Si l'option Staging Reserve est activée, entrez une valeur dans la case % of Total Space.

   Cette valeur représente le pourcentage de l'espace disque total à réserver pour le stockage temporaire sur disque ; en général 20 à 30 %.
4. Cliquez sur **Save**.

Paramètres de marqueur de bande

Les logiciels de sauvegarde de certains fournisseurs insèrent des marqueurs (marqueurs de bande, en-têtes de balise ou d'autres noms sont utilisés) dans tous les flux de données (système de fichiers et sauvegardes DD VTL) envoyés vers un système Data Domain.

Les marqueurs peuvent entraîner une dégradation significative de la compression des données sur un système Data Domain. Ainsi, le type de marqueur par défaut est automatiquement défini et ne peut pas être modifié par l'utilisateur. Si ce paramètre n'est pas compatible avec votre logiciel de sauvegarde, contactez votre fournisseur de services contractuel.

Remarque

Pour plus d'informations sur le fonctionnement des applications dans un environnement Data Domain, reportez-vous à la section *Intégration des systèmes EMC Data Domain dans l'environnement de stockage.* Vous pouvez utiliser ces matrices et ces guides d'intégration pour résoudre les problèmes liés aux fournisseurs.

Partage de charge applicative aléatoire de disque SSD

La valeur de seuil à laquelle vous souhaitez limiter les E/S aléatoires sur le système Data Domain peut être ajustée à partir de la valeur par défaut pour tenir compte de l'évolution des conditions et des schémas d'E/S.

Par défaut, le système Data Domain définit le partage de charge applicative aléatoire de disque SSD à 40 %. Cette valeur peut être revue à la hausse ou à la baisse, si cela est nécessaire. Sélectionnez **Data Managment** > **File System** > **Summary** > **Settings** > **Workload Balance**, puis faites glisser le curseur.

Cliquez sur **Save**.

Opérations Fast Copy

Une opération Fast Copy clone des fichiers et les arborescences d'un répertoire source vers un répertoire de destination sur un système Data Domain.

L'option `force` permet d'écraser le répertoire de destination, s'il existe. L'exécution d'une opération Fast Copy affiche une boîte de dialogue indiquant l'état de la progression.

Remarque

Une opération Fast Copy rend la destination identique à sa source, mais pas à un point spécifique dans le temps. Il n'y a aucune garantie que les deux soient ou n'aient jamais été identiques si vous modifiez l'un des répertoires pendant cette opération.

Exécution d'une opération Fast Copy

Copie une arborescence de fichiers ou de répertoires d'un répertoire du système Data Domain source vers une autre destination du système Data Domain

Procédure

1. Sélectionnez **Data Managment** > **File System** > **Summary** > **Fast Copy**.

   La boîte de dialogue Fast Copy s'affiche.

2. Dans la zone de texte Source, saisissez le chemin d'accès au répertoire contenant les données à copier. Par exemple, `/data/col1/backup/.snapshot/`*`snapshot-name`*`/dir1`.

   Remarque

   col1 utilise un L minuscule suivi du numéro 1.

3. Dans la zone de texte Destinataire, saisissez le chemin d'accès au répertoire dans lequel les données copiées seront stockées. Par exemple, `/data/col1/backup/dir2`. Ce répertoire de destination doit être vide, au risque d'entraîner l'échec de l'opération.

   - Si le répertoire de destination existe, cochez la case **Overwrite existing destination if it exists**.

4. Cliquez sur **OK**.
5. Dans la boîte de dialogue de progression qui s'affiche, cliquez sur **Close** pour quitter.

CHAPITRE 6

Structures MTree

Ce chapitre inclut les sections suivantes :

Présentation des structures MTrees

Une structure MTree est une partition logique du système de fichiers.

Vous pouvez utiliser des structures MTree de la façon suivante : pour les unités de stockage DD Boost, des pools DD VTL ou un partage NFS/CIFS. Les structures MTree permettent une gestion granulaire des snapshots, des quotas et du logiciel DD Retention Lock. Pour les systèmes dotés de l'option DD Extended Retention et d'une gestion granulaire des règles de migration de données du niveau actif au niveau de rétention, les opérations MTree peuvent être exécutées sur une structure MTree spécifique, plutôt que sur l'ensemble du système de fichiers.

Remarque

Il peut exister jusqu'à un nombre maximum configurable de structures MTree désignées pour les contextes de réplication MTree.

Ne placez pas les fichiers utilisateur dans le répertoire de premier niveau d'une structure MTree.

Restrictions en matière de MTree

Restrictions en matière de MTree pour les systèmes Data Domain

Tableau 96 Structures MTree prises en charge

Système Data Domain	Version du système DD OS	Prise en charge de structures MTree configurables	Prise en charge de structures MTrees simultanément actives
DD9800	6.0 et versions supérieures	256	256
DD9500	5.7 et versions supérieures	256	256
DD6800, DD9300	6.0 et versions supérieures	128	128
DD6300	6.0 et versions supérieures	100	32
DD2500, DD4200, DD4500, DD7200	5.7 et versions supérieures	128	128
Tous les autres systèmes DD	5.7 et versions supérieures	100	Jusqu'à 32 en fonction du modèle
DD9500	5.6	100	64

Tableau 96 Structures MTree prises en charge (suite)

Système Data Domain	Version du système DD OS	Prise en charge de structures MTree configurables	Prise en charge de structures MTrees simultanément actives
DD990, DD890	5.3 et versions supérieures	100	Jusqu'à 32 en fonction du modèle
DD7200, DD4500, DD4200	5.4 et versions supérieures	100	Jusqu'à 32 en fonction du modèle
Tous les autres systèmes DD	5.2 et versions supérieures	100	Jusqu'à 14 en fonction du modèle

Quotas

Les quotas MTree ne s'appliquent qu'aux données logiques écrites sur cette structure MTree.

L'administrateur peut définir une limite d'espace de stockage pour une structure MTree, une unité de stockage ou un pool DD VTL afin de l'empêcher de consommer trop d'espace. Il existe deux types de limites de quota : des limites strictes et des limites souples. Vous pouvez définir une limite souple, une limite stricte ou les deux. Les deux valeurs de limite doivent être des nombres entiers, et la limite souple doit être inférieure à la limite stricte.

Lorsqu'une limite souple est définie, une alerte est envoyée lorsque la taille de la structure MTree dépasse cette limite, mais les données peuvent encore y être écrites. Lorsqu'une limite stricte est définie, les données ne peuvent pas être écrites sur la structure MTree lorsque cette limite est atteinte. Par conséquent, toutes les opérations d'écriture échouent tant que des données ne sont pas supprimées de la structure MTree.

Pour plus d'informations, reportez-vous à la section Configuration des quotas de MTree à la page 248.

Application de quotas

Activez ou désactivez l'application de quotas.

À propos du volet MTree

Répertorie toutes les structures MTree actives sur le système et indique des statistiques de stockage de données en temps réel. Les informations affichées dans la zone de présentation sont utiles pour visualiser les tendances de l'utilisation de l'espace.

Sélectionnez **Data Management** > **MTree**.

- Sélectionnez une case correspondant à une structure MTree dans la liste pour afficher les détails et effectuer la configuration dans la vue Summary.
- Saisissez le texte (les caractères génériques sont pris en charge) dans le champ Filter By MTree Name, puis cliquez sur **Update** pour répertorier des noms de structure MTree spécifiques dans la liste.

- Supprimez le texte de filtre et cliquez sur **Reset** pour revenir à la liste par défaut.

Tableau 97 Informations sur le volet MTree Overview

Élément	Description
MTree Name	Chemin d'accès à la structure MTree.
Quota Hard Limit	Pourcentage de limite de quota stricte utilisée.
Last 24 Hr Pre-Comp (pre-compression)	Quantité de données brutes issues de l'application de sauvegarde qui ont été écrites au cours des dernières 24 heures.
Last 24 Hr Post-Comp (post-compression)	Quantité de stockage utilisée après la compression au cours des dernières 24 heures.
Last 24 hr Comp Ratio	Taux de compression au cours des dernières 24 heures.
Weekly Avg Post-Comp	Quantité moyenne de stockage compressé utilisée au cours des cinq dernières semaines.
Last Week Post-Comp	Quantité moyenne de stockage compressé utilisée au cours des sept derniers jours.
Weekly Avg Comp Ratio	Taux de compression moyen des cinq dernières semaines.
Last Week Comp Ratio	Taux de compression moyen des sept derniers jours.

À propos de la vue Summary

Affichez des statistiques importantes sur le système de fichiers.

Affichage d'informations détaillées

Sélectionnez une structure MTree pour afficher des informations.

Tableau 98 Informations détaillées sur la structure MTree sélectionnée

Élément	Description
Full Path	Chemin d'accès à la structure MTree.
Pre-Comp Used	Quantité actuelle de données brutes issues de l'application de sauvegarde, qui a été enregistrée sur cette structure MTree.
Status	État de la structure MTree (les combinaisons sont prises en charge). Cet état peut être : • D : Supprimée • RO : Lecture seule • RW : Lecture/écriture • RD : Replication destination • RLCE : DD Retention Lock Compliance activé • RLCD : DD Retention Lock Compliance désactivé • RLGE : DD Retention Lock Governance activé • RLGD : DD Retention Lock Governance désactivé

Tableau 98 Informations détaillées sur la structure MTree sélectionnée (suite)

Élément	Description
Quota	
Quota Enforcement	Activé ou Désactivé
Pre-Comp Soft Limit	Valeur actuelle. Cliquez sur Configure pour mettre à jour les limites de quota.
Pre-Comp Hard Limit	Valeur actuelle. Cliquez sur Configure pour mettre à jour les limites de quota.
Quota Summary	Pourcentage de limite stricte utilisé.
Protocols	
CIFS Shared	L'état du partage CIFS. Cet état peut être : • Yes : la structure MTree ou son répertoire parent est partagé(e). • Partial : le sous-répertoire sous cette structure MTree est partagé. • No : cette structure MTree et son répertoire parent ou son sous-répertoire ne sont pas partagés. Cliquez sur le lien CIFS pour afficher la vue CIFS.
NFS Exported	L'état de l'exportation de NFS. Cet état peut être : • Yes : la structure MTree ou son répertoire parent est exporté(e). • Partial : le sous-répertoire sous cette structure MTree est exporté. • No : cette structure MTree et son répertoire parent ou son sous-répertoire ne sont pas exportés. Cliquez sur le lien NFS pour afficher la vue NFS.
DD Boost Storage Unit	L'état de l'exportation de DD Boost. Cet état peut être : • Yes : la structure MTree est exportée. • No : la structure MTree n'est pas exportée. • Unknown : aucune information disponible. Cliquez sur le lien DD Boost pour afficher la vue DD Boost.
DD VTL Pool	État du rapport de pool VTL. Cet état peut être : • Yes : la structure MTree est un pool MTree DD VTL. • Non : la structure MTree n'est pas un pool MTree DD VTL. • Unknown : aucune information disponible.
vDisk Pool	État du rapport vDisk. Cet état peut être : • Unknown : le service vDisk n'est pas activé. • No : le service vDisk est activé, mais la structure MTree n'est pas un pool vDisk.

Tableau 98 Informations détaillées sur la structure MTree sélectionnée (suite)

Élément	Description
	• Yes : le service vDisk est activé et la structure MTree est un pool vDisk.
Physical Capacity Measurements	
Used (Post-Comp)	Espace MTree utilisé après que les données de compression ont été acquises.
Compression	Global-comp factor.
Last Measurement Time	Heure de la dernière mesure de la structure MTree par le système.

Schedules	Nombre de plannings attribués.
	Cliquez sur **Assign** pour afficher et attribuer des plannings à la structure MTree.
	• Name : Nom du planning.
	• Status : Activé ou Désactivé
	• Priority :
	  ▪ Normal : envoie une tâche de mesure à la file d'attente de traitement.
	  ▪ Urgent : envoie une tâche de mesure au début de la file d'attente de traitement.
	• Schedule : heure à laquelle la tâche s'exécute.
	• MTree Assignments : Nombre de structures MTree auxquelles le planning est attribué.

Submitted Measurements	Affiche l'état de post-compression de la structure MTree. Cliquez sur **Measure Now** pour soumettre une tâche de post-compression manuelle pour la structure MTree et sélectionner une priorité pour la tâche. • 0 : aucune tâche de mesure soumise. • 1 : 1 tâche de mesure en cours d'exécution. • 2 : 2 tâches de mesure en cours d'exécution.
Snapshots	Affiche les statistiques suivantes : • Total Snapshots • Expired • Unexpired • Oldest Snapshot • Newest Snapshot • Next Scheduled • Assigned Snapshot Schedules

Tableau 98 Informations détaillées sur la structure MTree sélectionnée (suite)

Élément	Description
	Cliquez sur **Total Snapshots** pour accéder à la vue **Data Management** > **Snapshots**. Cliquez sur **Assign Schedules** pour configurer des plannings de snapshots.

Affichage des informations sur la réplication de structures MTree

Affichez la configuration de la réplication MTree.

Si la structure MTree sélectionnée est configurée pour la réplication, des informations récapitulatives sur la configuration s'affichent dans cette zone. Dans le cas contraire, cette zone affiche `No Record Found`.

- Cliquez sur le lien Replication afin d'accéder à la page de réplication et effectuer ainsi la configuration ou afficher des informations supplémentaires.

Tableau 99 Informations relatives à la réplication de structures MTree

Élément	Description
Source	Chemin d'accès à la structure MTree source.
Destination	Chemin d'accès à la structure MTree cible.
Status	État de la paire de réplication MTree. Cet état peut être Normal, Error ou Warning.
Sync As Of	Date et heure de la dernière synchronisation de la paire de réplication.

Affichage des informations sur les snapshots d'une structure MTree

Si la structure MTree sélectionnée est configurée pour des snapshots, des informations récapitulatives sur la configuration des snapshots s'affichent.

- Cliquez sur le lien **Snapshots** pour accéder à la page Snapshots afin d'effectuer la configuration ou d'afficher des informations supplémentaires.
- Cliquez sur **Assign Schedules** pour affecter un planning de snapshots à la structure MTree sélectionnée. Cochez la case correspondant au planning, puis cliquez sur **OK** et sur **Close**. Pour créer un planning de snapshots, cliquez sur **Create Snapshot Schedule** (reportez-vous à la section relative à la création d'un planning de snapshots pour obtenir des instructions).

Tableau 100 Informations sur les snapshots d'une structure MTree

Élément	Description
Total Snapshots	Nombre total de snapshots créés pour cette structure MTree. Un total de 750 snapshots peut être créé pour chaque structure MTree.
Expired	Nombre de snapshots de cette structure MTree qui ont été marqués pour suppression, mais qui n'ont pas encore été supprimés par l'opération de nettoyage.

Tableau 100 Informations sur les snapshots d'une structure MTree (suite)

Élément	Description
Unexpired	Nombre de snapshots de cette structure MTree qui sont marqués pour être conservés.
Oldest Snapshot	Date du plus ancien snapshot de cette structure MTree.
Newest Snapshot	Date du snapshot le plus récent de cette structure MTree.
Next Scheduled	Date du prochain snapshot planifié.
Assigned Snapshot Schedules	Nom du planning de snapshots affecté à cette structure MTree.

Affichage d'informations sur le verrouillage pour rétention d'une structure MTree

Si la structure MTree sélectionnée est configurée pour l'une des options de DD Retention Lock, des informations récapitulatives sur la configuration de DD Retention Lock s'affichent.

Remarque

Pour plus d'informations sur la gestion de DD Retention Lock pour une structure MTree, reportez-vous à la section relative à l'utilisation de DD Retention Lock.

Tableau 101 Informations sur DD Retention Lock

Élément	Description
Status	Indique si DD Retention Lock est activé ou désactivé.
Mode	Indique si la structure MTree est configurée pour DD Retention Lock Compliance ou DD Retention Lock Governance.
Use	Indique l'utilisation de la structure MTree.
Retention period min	Indique la durée minimale de mise en œuvre DD Retention Lock.
Retention period max	Indique la durée maximale de mise en œuvre de DD Retention Lock.

Paramètres d'activation et de gestion du verrouillage de rétention DD

Utilisez la zone DD Retention Lock de l'interface utilisateur pour modifier les périodes de verrouillage de la rétention.

Procédure

1. Sélectionnez **Data Management** > **MTree** > **Summary**.
2. Dans la section Retention Lock, cliquez sur **Edit**.
3. Dans la boîte de dialogue Modify Retention Lock, sélectionnez **Enable** pour activer le verrouillage de la rétention DD sur le système Data Domain.
4. Modifiez la valeur minimale ou maximale de la période de rétention (la fonction doit d'abord être activée) dans le volet Retention Period.
5. Sélectionnez un intervalle (minutes, heures, jours, années). Cliquez sur **Default** pour afficher les valeurs par défaut.

6. Cliquez sur **OK**.

Résultats

Une fois la boîte de dialogue Modify Retention Lock fermée, les informations actualisées sur la structure MTree s'affichent dans la zone récapitulative du verrouillage de la rétention DD.

À propos de la vue Space Usage (MTrees)

Affichez une représentation visuelle de l'utilisation des données pour une structure MTree à certains points ans le temps.

Sélectionnez **Data Management** > **MTree** > **Space Usage**.

- Pour afficher un encadré contenant les données correspondant à un point, cliquez sur ce point sur le graphique.
- Pour ouvrir la boîte de dialogue d'impression standard, cliquez sur **Print** (au bas du graphique).
- Pour afficher le graphique dans une nouvelle fenêtre de navigateur, cliquez sur **Show**.

Les lignes du graphique donnent des mesures sur :

- Pre-comp Written : volume total de données envoyé à la MTree par les serveurs de sauvegarde. Les données précompressées se trouvant sur une MTree sont considérées par le serveur de sauvegarde comme les données non compressées totales conservées par une « MTree comme unité de stockage », représentées sur l'axe vertical du graphique correspondant à l'espace utilisé (à gauche).
- Post-comp Used : volume total d'espace de stockage consommé sur la structure MTree après compression, indiqué par l'axe vertical Space Used (à gauche) du graphique.
- Comp Factor : taux de compression des données stockées sur la structure MTree, représenté par l'axe vertical Comp Factor (à droite) du graphique.

Remarque

Pour la vue MTrees Space Usage, le système n'affiche que les informations avant compression. Les données peuvent être partagées entre les MTrees, de sorte qu'il n'est pas possible d'indiquer l'utilisation de la compression pour une MTree unique.

Vérification de l'utilisation historique de l'espace

Sur le graphique Space Usage, un clic sur un intervalle (c'est-à-dire 1 semaine, 1 mois, 3 mois ou 1 an) sur la ligne de durée au-dessus du graphique vous permet de modifier le nombre de jours de données affichés sur le graphique, de 7 à 120 jours.

Pour afficher l'utilisation de l'espace pour des intervalles de plus de 120 jours, exécutez la commande suivante :

```
# filesys show compression [summary | daily | daily-detailed] {[last n
{hours | days | weeks | months}] | [start date [end date]]}
```

À propos de la vue Daily Written (MTrees)

Affichez le flux de données des 24 dernières heures. Les volumes de données sont présentés dans le temps avant et après compression.

La vue présente également les totaux pour les volumes de compression globaux et locaux, et les volumes avant et après compression.

- Pour afficher un encadré contenant les données correspondant à un point, cliquez sur ce point sur le graphique.
- Pour ouvrir la boîte de dialogue d'impression standard, cliquez sur **Print** (au bas du graphique).
- Pour afficher le graphique dans une nouvelle fenêtre de navigateur, cliquez sur l'option **Show in new window**.

Les lignes du graphique indiquent les mesures suivantes :

- Pre-Comp Written : volume total de données écrit dans la MTree par les serveurs de sauvegarde. Les données précompressées se trouvant sur une MTree sont considérées par le serveur de sauvegarde comme les données non compressées totales conservées par une « MTree comme unité de stockage ».
- Post-Comp Written : quantité totale de données écrites sur la MTree une fois la compression effectuée, indiquée en Gio/s.
- Total Comp Factor : quantité totale de compression appliquée par le système Data Domain aux données reçues (taux de compression), représentée par la valeur Total Compression Factor sur l'axe vertical (droit) du graphique.

Vérification des données écrites historiques
Dans le graphique Daily Written, un clic sur un intervalle (c'est-à-dire 7 jours, 30 jours, 60 jours ou 120 jours) sur la ligne de durée située au-dessus du graphique vous permet de modifier le nombre de jours de données affichés sur le graphique (de 7 à 120 jours).

Sous le graphique Daily Written, les totaux suivants s'affichent pour la valeur de durée actuelle :

- Pre-Comp Written
- Post-Comp Written
- Global-Comp Factor
- Local-Comp Factor
- Total-Comp Factor

Surveillance de l’utilisation des structures MTree

Affichez l’espace utilisé et les tendances des données écrites pour une structure MTree.

Procédure

- Sélectionnez **Data Management** > **MTree**.

  La vue MTree affiche la liste des structures MTree configurées. Une fois la structure sélectionnée dans la liste, les détails de la structure MTree sont affichés sous l’onglet Summary. Les onglets Space Usage et Daily Written affichent des graphiques indiquant visuellement les volumes d’espace utilisés et les tendances des données écrites pour la structure MTree sélectionnée. La vue contient également les options permettant de configurer la structure MTree pour les protocoles CIFS, NFS et DD Boost, ainsi que les sections dédiées à la gestion des snapshots et au verrouillage de la rétention (avec DD Retention Lock) d’une structure MTree.

  La vue de la structure MTree comporte un volet de présentation de la structure MTree et trois onglets décrits en détail dans les sections suivantes.

  - À propos du volet MTree à la page 235

- À propos de la vue Summary à la page 236
- À propos de la vue Space Usage (MTrees) à la page 241
- À propos de la vue Daily Written (MTrees) à la page 241

Remarque

La mesure de la capacité physique (PCM) fournit des informations sur l'utilisation de l'espace pour les structures MTree. Pour plus d'informations sur PCM, reportez-vous à la section relative au fonctionnement de la mesure de la capacité physique.

Fonctionnement de la mesure de la capacité physique

La fonction de mesure de la capacité physique (PCM) fournit des informations sur l'utilisation de l'espace pour un sous-ensemble de l'espace de stockage Dans DD System Manager, cette fonction fournit des informations sur l'utilisation de l'espace pour les structures Mtree, mais vous pouvez, à partir de l'interface de ligne de commande, afficher des informations sur l'utilisation de l'espace pour les structures Mtree, les tenants, les unités de tenant et les ensembles de chemins.

Une fois qu'un chemin est sélectionné pour PCM, tous les chemins en dessous sont automatiquement inclus. Ne sélectionnez pas un chemin enfant une fois que son chemin parent est déjà sélectionné. Par exemple, si `/data/col1/mtree3` est sélectionné, ne sélectionnez pas tous les sous-répertoires sous mtree3.

Le *Guide de référence des commandes de Data Domain Operating System* fournit plus d'informations sur l'utilisation de PCM à partir de la ligne de commande.

Activation, désactivation et affichage des mesures de la capacité physique

La mesure de la capacité physique fournit des informations sur l'utilisation de l'espace d'une structure MTree.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Summary**.

   Le système affiche l'onglet Summary dans le volet File System.
2. Cliquez sur **^** dans le coin inférieur droit pour afficher le panneau d'état.
3. Cliquez sur **Enable** à droite de **Physical Capacity Measurement Status** pour activer la mesure de la capacité physique.
4. Cliquez sur **Details** à droite de **Physical Capacity Measurement Status** pour afficher les tâches de mesure de la capacité physique en cours d'exécution.
   - **MTree** : structure MTree dont la capacité physique est mesurée.
   - **Priority** : priorité (normale ou urgente) pour la tâche.
   - **Submit Time** : heure à laquelle la tâche a été demandée.
   - **Duration** : durée de l'exécution de la tâche de mesure de la capacité physique.
5. Cliquez sur **Disable** à droite de **Physical Capacity Measurement Status** pour désactiver la mesure de la capacité physique et annuler toutes les tâches de mesure en cours d'exécution.

Initialisation de la mesure de la capacité physique

L'initialisation de la mesure de la capacité physique (PCM) est une action à usage unique qui peut avoir lieu uniquement si la fonction PCM est activée et que le cache

n'a pas été initialisé. Elle nettoie les caches et améliore la vitesse de mesure. Au cours du processus d'initialisation, vous pouvez toujours gérer et exécuter les tâches PCM.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Configuration**.
2. Cliquez sur **Initialize** dans Physical Capacity Measurement à droite du champ Cache.
3. Cliquez sur **Yes**.

Gestion des plannings de mesure de la capacité physique

Créez, modifiez, supprimez et affichez des plannings de mesure de la capacité physique. Cette boîte de dialogue affiche uniquement les plannings créés pour les structures Mtree et ceux n'ayant actuellement pas d'attributions.

Procédure

1. Sélectionnez **Data Management** > **MTree** > **Manage Schedules**.
   - Cliquez sur **Add** (+) pour créer le planning.
   - Sélectionnez un planning, puis cliquez sur **Modify** (crayon) pour modifier le planning.
   - Sélectionnez un planning, puis cliquez sur **Delete** (X) pour supprimer un planning.
2. Si vous le souhaitez, cliquez sur les noms d'en-tête pour trier par planning : **Name**, **Status** (Enabled ou Disabled) **Priority** (Urgent ou Normal), **Schedule** (heure du planning) et **MTree Assignments** (nombre de structures MTree auxquelles le planning s'applique).

Création de plannings de mesure de la capacité physique

Créez des plannings de mesure de la capacité physique et attribuez-les à des structures Mtree.

Procédure

1. Sélectionnez **Data Management** > **MTree** > **Manage Schedules**.
2. Cliquez sur **Add** (+) pour créer un planning.
3. Saisissez le nom du planning.
4. Sélectionnez l'état :
   - **Normal** : envoie une tâche de mesure à la file d'attente de traitement.
   - **Urgent** : envoie une tâche de mesure au début de la file d'attente de traitement.
5. Sélectionnez la fréquence à laquelle le planning déclenche une occurrence de mesure : chaque jour (**Day**), semaine (**Week**) ou mois (**Month**).
   - Pour **Day**, sélectionnez l'heure.
   - Pour **Week**, sélectionnez l'heure et le jour de la semaine.
   - Pour **Month**, sélectionnez l'heure et le jour au cours du mois.
6. Sélectionnez les attributions de structure MTree pour le planning (structures Mtree auxquelles le planning s'applique) :
7. Cliquez sur **Create**.

8. Si vous le souhaitez, cliquez sur les noms d'en-tête pour trier par planning : **Name**, **Status** (Enabled ou Disabled) **Priority** (Urgent ou Normal), **Schedule** (heure du planning) et **MTree Assignments** (nombre de structures MTree auxquelles le planning s'applique).

Modification des plannings de mesure de la capacité physique

Modifiez un planning de mesure de la capacité physique.

Procédure

1. Sélectionnez **Data Management** > **MTree** > **Manage Schedules**.
2. Sélectionnez un planning, puis cliquez sur **Modify** (crayon).
3. Modifiez le planning, puis cliquez sur **Save**.

   Les options de planning sont décrites dans la rubrique Création de plannings de mesure de la capacité physique.
4. Si vous le souhaitez, cliquez sur les noms d'en-tête pour trier par planning : **Name**, **Status** (Enabled ou Disabled) **Priority** (Urgent ou Normal), **Schedule** (heure du planning) et **MTree Assignments** (nombre de structures MTree auxquelles le planning s'applique).

Attribution de plannings de mesure de la capacité physique à une structure MTree

Rattachez des plannings à une structure MTree.

Avant de commencer

Vous devez créer des plannings de mesure de la capacité physique.

Remarque

Les administrateurs peuvent attribuer jusqu'à trois plannings de mesure à une structure MTree.

Procédure

1. Sélectionnez **Data Management** > **MTree** > **Summary**.
2. Sélectionnez les structures Mtree auxquelles des plannings seront attribués.
3. Faites défiler vers le bas jusqu'à la zone Physical Capacity Measurements, puis cliquez sur **Assign**à droite des plannings.
4. Sélectionnez les plannings à attribuer à la structure MTree, puis cliquez sur **Assign**.

Démarrage immédiat de la mesure de la capacité physique

Démarrez le processus de mesure dès que possible.

Procédure

1. Sélectionnez **Data Management** > **MTree** > **Summary**.
2. Faites défiler vers le bas jusqu'à la zone Physical Capacity Measurements, puis cliquez sur **Measure Now** à droite de Submitted Measurements.
3. Sélectionnez **Normal** (envoie une tâche de mesure à la file d'attente de traitement) ou **Urgent** (envoie une tâche de mesure au début de la file d'attente de traitement).
4. Cliquez sur **Submit**.

Définition de la régulation de la mesure de la capacité physique

Définissez le pourcentage de ressources du système dédiées à la mesure de la capacité physique.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Settings**.
2. Dans la zone Physical Capacity Measurement, cliquez sur **Edit** à gauche du champ Throttle.
3.

Option	Description
Click Default	Saisit la valeur par défaut de 20 % du système.
Type throttle percent	Pourcentage de ressources du système dédiées à la mesure de la capacité physique.

4. Cliquez sur **Save**.

Gestion des opérations MTree

Cette section décrit la création d'une structure MTree, sa configuration, l'activation et la désactivation des quotas MTree, etc.

Création d'une structure MTree

Une structure MTree est une partition logique du système de fichiers. Utilisez des structures MTree pour les unités de stockage DD Boost, des pools DD VTL ou un partage NFS/CIFS.

Les structures MTree sont créées dans la zone /data/col1/*mtree_name*.

Procédure

1. Sélectionnez **Data Management** > **MTree**.
2. Dans la zone de présentation de la structure MTree, cliquez sur **Create**.
3. Saisissez le nom de la structure MTree dans la zone de texte MTree Name. Les noms de structure MTree peuvent compter jusqu'à 50 caractères. Les caractères suivants sont acceptés :
   - Lettres majuscules et minuscules : A-Z, a-z
   - Chiffres : 0-9
   - Espace
   - Virgule (,)
   - Point (.), tant qu'il ne précède pas le nom.
   - Point d'exclamation (!)
   - Dièse (#)
   - Dollar ($)
   - Signe de pourcentage (%)
   - Signe plus (+)
   - Arobase (@)

- Signe égal (=)
- Esperluette (&)
- Point-virgule (;)
- Parenthèse [(et)]
- Crochets ([et])
- Accolades ({et})
- Accent circonflexe (^)
- Tilde (~)
- Apostrophe (signe droit et unique)
- Apostrophe courbe (‘)

4. Définissez des restrictions de l’espace de stockage pour la structure MTree afin de l’empêcher de consommer trop d’espace. Saisissez une limite de quota souple ou stricte, ou les deux. En cas de limite souple, une alerte est envoyée lorsque la taille de la structure MTree dépasse la limite fixée, mais que des données peuvent encore être écrites dans la structure MTree. Les données ne peuvent pas être écrites dans la structure MTree lorsque la limite stricte est atteinte.

   Remarque

   Les limites de quota sont des valeurs précompressées.
   Pour définir les limites de quota d’une structure MTree, sélectionnez **Set to Specific value**, puis saisissez une valeur. Sélectionnez une unité de mesure : Mio, Gio, Tio ou Pio.

   Remarque

   Si vous définissez une limite souple et une limite stricte, la limite souple d’un quota ne peut pas dépasser sa limite stricte.

5. Cliquez sur **OK**.

   La nouvelle structure MTree s’affiche dans le tableau MTree.

   Remarque

   Vous devrez peut-être augmenter la largeur de la colonne des noms de structure MTree pour afficher l’intégralité du chemin d’accès.

Configuration et activation/désactivation des quotas de MTree

Définissez la limite d’espace de stockage pour une structure MTree, une unité de stockage ou un pool DD VTL.

La page **Data Management** > **Quota** indique à l'administrateur combien de structures MTree n'ont aucun quota souple ou strict défini. Pour les structures MTree avec des quotas définis, la page indique le pourcentage des limites souple et stricte des données précompressées utilisées.

Tenez compte des informations suivantes lors de la gestion des quotas.

- Les quotas MTree s'appliquent pour traiter des opérations d'acquisition. Ces quotas peuvent être appliqués aux données sur les systèmes qui disposent du logiciel DD Extended Retention, quel que soit le niveau sur lequel il réside, ainsi que DD VTL, DD Boost, CIFS et NFS.
- Les snapshots ne sont pas pris en compte.
- Il n'est pas possible de définir des quotas sur le répertoire `/data/col1/backup`.
- La valeur de quota maximale autorisée est 4 096 Pio.

Configuration des quotas de MTree

Utilisez les onglets MTree ou Quota pour configurer les quotas de MTree.

Procédure

1. Sélectionnez l'un des chemins de menu suivants :
   - Sélectionnez **Data Management** > **MTree**.
   - Sélectionnez **Data Management** > **Quota**.
2. Sélectionnez une seule MTree sous l'onglet MTree, ou une ou plusieurs MTrees sous l'onglet Quota.

   Remarque

   Il n'est pas possible de définir des quotas sur le répertoire `/data/col1/backup`.
3. Sous l'onglet MTree, cliquez sur l'onglet **Summary**, puis sur le bouton **Configure** dans la zone Quota.
4. Sous l'onglet Quota, cliquez sur le bouton **Configure Quota**.

Configuration des quotas de MTree

Entrez les valeurs des quotas souples et stricts, puis sélectionnez l'unité de mesure.

Procédure

1. Dans la boîte de dialogue Configure Quota for MTrees, entrez les valeurs des quotas souples et stricts, puis sélectionnez l'unité de mesure : Mio, Gio, Tio ou Pio.
2. Cliquez sur le bouton **OK**.

Suppression d'une MTree

Supprime la structure MTree du tableau MTree. Les données MTree seront supprimées lors du prochain nettoyage.

Remarque

La structure MTree et les données qui lui sont associées n'étant pas supprimées tant que le nettoyage des fichiers n'est pas effectué, vous ne pouvez pas créer de nouvelle structure MTree avec le même nom qu'une structure supprimée tant que celle-ci n'est pas entièrement supprimée du système de fichiers par l'opération de nettoyage.

Procédure

1. Sélectionnez **Data Management** > **MTree**.
2. Sélectionnez une structure MTree.

3. Dans la zone de présentation de la structure MTree, cliquez sur **Delete**.
4. Cliquez sur **OK** dans la boîte de dialogue Warning.
5. Cliquez sur **Close** dans la boîte de dialogue Delete MTree Status après l'affichage de la progression.

Annulation de la suppression d'une structure MTree

L'annulation de la suppression permet de récupérer une structure MTree supprimée et ses données, et la replace dans le tableau MTree.

L'annulation de la suppression d'une structure MTree permet de récupérer une structure MTree supprimée et ses données, et la replace dans le tableau MTree.

Une annulation n'est possible que si le nettoyage de fichier n'a pas été effectué après que la structure MTree a été marquée pour suppression.

Remarque

Vous pouvez également utiliser cette procédure pour annuler la suppression d'une unité de stockage.

Procédure

1. Sélectionnez **Data Management** > **MTree** > **More Tasks** > **Undelete**.
2. Cochez les cases des structures MTree que vous souhaitez récupérer, puis cliquez sur **OK**.
3. Cliquez sur **Close** dans la boîte de dialogue Undelete MTree Status après l'affichage de la progression.

   La structure MTree récupérée s'affiche dans le tableau MTree.

Attribution d'un nouveau nom à une MTree

Utilisez l'interface utilisateur Data Management MTree pour renommer des structures MTree.

Procédure

1. Sélectionnez **Data Management** > **MTree**.
2. Sélectionnez une structure MTree dans le tableau MTree.
3. Sélectionnez l'onglet Summary.
4. Dans la zone Detailed Information, cliquez sur **Rename**.
5. Entrez le nom de la structure MTree dans la zone de texte New MTree Name.

   Reportez-vous à la section consacrée à la création d'une structure MTree pour obtenir la liste des caractères autorisés.

6. Cliquez sur **OK**.

   La structure MTree renommée s'affiche dans le tableau MTree.

CHAPITRE 7

Snapshots

Ce chapitre traite des sujets suivants :

Tour d'horizon des snapshots

Ce chapitre explique comment utiliser la fonction de snapshot avec des structures MTree.

Un snapshot enregistre une copie en lecture seule (appelée *snapshot*) d'une structure MTree donnée à une heure spécifique. Vous pouvez utiliser un snapshot en tant que point de restauration. Vous pouvez aussi gérer les snapshots et les ordonnanceurs de MTree, et afficher des informations sur l'état des snapshots existants.

Remarque

Les snapshots créés sur le système Data Domain source sont répliqués vers la destination avec une réplication de collection et de structure MTree. Il n'est pas possible de créer des snapshots sur un système Data Domain qui est un réplica pour la réplication de collection. Il n'est donc pas possible de créer un snapshot sur la structure MTree cible de la réplication de structure MTree. La réplication de répertoire ne réplique pas les snapshots ; elle nécessite la création distincte de snapshots sur le système cible.

Les snapshots d'une structure MTree nommés `backup` sont créés dans le répertoire système `/data/col1/backup/.snapshot`. Chaque répertoire sous `/data/col1/backup` contient également un répertoire `.snapshot` avec le nom de chaque snapshot incluant le répertoire. Comme chaque structure MTree présente le même type de structure, une structure MTree nommée SantaClara aura un répertoire système `/data/col1/SantaClara/.snapshot`, et chaque sous-répertoire de `/data/col1/SantaClara` aura également un répertoire `.snapshot`.

Remarque

Le répertoire `.snapshot` n'est pas visible si seul `/data` est monté. Lorsque la structure MTree est elle-même montée, le répertoire .snapshot est visible.

Un snapshot expiré reste disponible jusqu'à la prochaine opération de nettoyage du système de fichiers.

Le nombre maximal de snapshots autorisés par MTree est de 750. Des avertissements sont envoyés lorsque le nombre de snapshots par MTree atteint 90 % du nombre maximal autorisé (de 675 à 749 snapshots), et une alerte est générée lorsque le nombre maximal est atteint. Pour supprimer l'avertissement, faites expirer les snapshots, puis exécutez l'opération de nettoyage du système de fichiers.

Remarque

Pour identifier une structure MTree qui s'approche du nombre maximal de snapshots, vérifiez les informations relatives aux snapshots de MTree qui s'affichent sur le volet Snapshots de la page MTree.

La rétention de snapshots pour une structure MTree ne prend pas d'espace supplémentaire, mais s'il existe un snapshot et que le fichier d'origine n'y est plus, cet espace ne peut pas être récupéré.

Remarque

Snapshots et protocole CIFS : À partir de la version 5.0 de DD OS, le répertoire `.snapshot` n'est plus visible dans la liste des répertoires de l'Explorateur Windows ou du shell CMD DOS. Vous pouvez accéder au répertoire `.snapshot` en entrant son nom dans la barre d'adresse de l'Explorateur Windows ou du shell CMD DOS. Par exemple, `\\dd\backup\.snapshot` ou `Z:\.snapshot` lorsque `Z:` est mappé comme `\\dd\backup`).

Surveillance des snapshots et de leurs ordonnanceurs

Cette section fournit des informations détaillées et résumées sur l'état des snapshots et des ordonnanceurs de snapshots.

À propos de la vue Snapshots

Les rubriques de cette section décrivent la vue Snapshot.

Volet Snapshot Overview

Affichez le nombre total de snapshots, le nombre de snapshots expirés, ceux non expirés et l'heure du prochain nettoyage.

Sélectionnez **Data Management** > **Snapshots**.

Tableau 102 Informations du volet Snapshot Overview

Champ	Description
Total Snapshots (Across all MTrees)	Nombre total de snapshots, actifs et expirés, sur l'ensemble des structures MTree du système.
Expired	Nombre de snapshots marqués pour suppression, mais qui n'ont pas encore été supprimés lors d'une opération de nettoyage.
Unexpired	Nombre de snapshots marqués pour être conservés.
Next file system clean scheduled	Date d'exécution de la prochaine opération de nettoyage du système de fichiers planifiée.

Vue Snapshots

Affichez des informations relatives aux snapshots : nom, MTree, heure de création, état actif ou inactif et date d'expiration.

L'onglet Snapshots affiche la liste des snapshots, ainsi que les informations suivantes.

Tableau 103 Informations sur les snapshots

Champ	Description
Selected MTree	Liste déroulante permettant de sélectionner la structure MTree concernée par le snapshot.
Filter By	Éléments à rechercher dans la liste des snapshots qui s'affiche. Les options sont les suivantes :

Tableau 103 Informations sur les snapshots (suite)

Champ	Description
	• **Name** : nom du snapshot (les caractères génériques sont acceptés). • **Year** : liste déroulante permettant de sélectionner l'année.
Name	Nom de l'image de snapshot.
Creation Time	Date de création du snapshot.
Expires On	Date d'expiration du snapshot.
Status	État du snapshot, qui peut être Expired ou vide si le snapshot est actif.

Vue des plannings

Affichez les jours au cours desquels les snapshots seront pris, les heures, le moment où ils seront conservés et la convention de dénomination.

Tableau 104 Informations relatives au planning de snapshots

Champ	Description
Name	Nom du planning de snapshots.
Days	Jours où les snapshots seront pris.
Times	Heure de la journée à laquelle les snapshots seront pris.
Retention Period	Durée pendant laquelle le snapshot sera conservé.
Snapshot Name Pattern	Chaîne de caractères et de variables qui se transforme en un nom de snapshot (par exemple, `scheduled-%Y-%m-%d-%H-%M`, qui se transforme en « scheduled-2010-04-12-17-33 »).

1. Sélectionnez un planning dans l'onglet Schedules. La section Detailed Information qui s'affiche répertorie les structures MTree qui partagent le même planning que la structure MTree sélectionnée.
2. Cliquez sur le bouton **Add/Remove** pour ajouter ou supprimer des structures MTree dans la liste des plannings.

Gestion des snapshots

Cette rubrique décrit comment gérer les snapshots.

Création d'un snapshot

Créez un snapshot lorsqu'un snapshot non planifié est requis.

Procédure

1. Sélectionnez **Data Management** > **Snapshots** pour ouvrir la vue Snapshots.
2. Dans la vue Snapshots, cliquez sur **Create**.
3. Dans le champ Name, entrez le nom du snapshot

4. Dans la zone Mtrees, cochez la case en regard d'une ou plusieurs MTrees dans le volet Available MTrees et cliquez sur **Add**.
5. Dans la zone Expiration, sélectionnez l'une des options d'expiration suivantes :
   a. **Never Expire**.
   b. Saisissez une valeur dans le champ de texte In et sélectionnez **Days**, **Weeks**, **Month** ou **Years** dans la liste déroulante. Le snapshot est conservé jusqu'à la même heure de la journée que celle à laquelle il a été créé.
   c. Saisissez une date (au format *mm/dd/yyyy*) dans le champ de texte On ou cliquez sur l'option **Calendar**, puis sur une date. Le snapshot est conservé jusqu'à minuit (0h00, la première minute du jour) de la date indiquée.
6. Cliquez sur **OK**, puis sur **Close**.

Modification de la date d'expiration d'un snapshot

Modifiez les dates d'expiration des snapshots afin de les supprimer ou d'étendre leur durée de vie pour l'audit ou la conformité.

Procédure

1. Sélectionnez **Data Management**>**Snapshots** pour ouvrir la vue Snapshots.
2. Cochez la case correspondant à l'entrée de snapshot dans la liste, puis cliquez sur **Modify Expiration Date**.

   Remarque

   Vous pouvez sélectionner plusieurs snapshots. Pour ce faire, cochez toutes les cases correspondantes.

3. Dans la zone Expiration, sélectionnez l'une des options suivantes pour la date d'expiration :
   a. **Never Expire**.
   b. Dans la zone de texte In, entrez un nombre et sélectionnez **Days**, **Weeks**, **Months** ou **Years** dans la liste déroulante. Le snapshot est conservé jusqu'à la même heure de la journée que celle à laquelle il a été créé.
   c. Dans la zone de texte **On**, saisissez une date (au format *mm/dd/yyyy*) ou cliquez sur **Calendar** puis sur une date. Le snapshot est conservé jusqu'à minuit (0h00, la première minute du jour) de la date indiquée.
4. Cliquez sur **OK**.

Attribution d'un nouveau nom de snapshot

Utilisez l'onglet Snapshot pour renommer un snapshot.

Procédure

1. Sélectionnez **Data Management** > **Snapshots** pour ouvrir la vue Snapshots.
2. Cochez la case de l'entrée du snapshot dans la liste et cliquez sur **Rename**.
3. Entrez un nouveau nom dans le champ Name.
4. Cliquez sur **OK**.

Expiration d'un snapshot

Les snapshots ne peuvent pas être supprimés. Pour libérer de l'espace disque, faites expirer des snapshots pour qu'ils soient supprimés lors du prochain cycle de nettoyage après la date d'expiration.

Procédure

1. Sélectionnez **Data Management** > **Snapshots** pour ouvrir la vue Snapshots.
2. Cochez la case en regard de l'entrée de snapshot dans la liste, puis cliquez sur **Expire**.

Remarque

Vous pouvez sélectionner plusieurs snapshots. Pour ce faire, cochez toutes les cases correspondantes.
Le snapshot présente l'état expiré dans la colonne Status et sera supprimé lors du prochain nettoyage.

Gestion des plannings de snapshots

Configurez et gérez une série de snapshots qui sera prise automatiquement à des intervalles réguliers (planning des snapshots).

Plusieurs ordonnanceurs de snapshots peuvent être actifs simultanément.

Remarque

Si plusieurs snapshots ayant le même nom sont planifiés pour s'exécuter en même temps, un seul est conservé. Celui qui est conservé n'est pas défini, de sorte qu'un seul snapshot ayant le nom en question doit être planifié pour un moment donné.

Création d'un planning de snapshots

Créez un planning de snapshots hebdomadaires ou mensuels à l'aide de l'interface utilisateur Data Management.

Procédure

1. Sélectionnez **Data Management** > **Snapshots** > **Schedules** pour ouvrir la vue Schedules.
2. Cliquez sur **Create**.
3. Dans la zone de texte **Name**, entrez le nom du planning.
4. Dans la zone de texte **Snapshot Name Pattern**, entrez un modèle de nom.

   Entrez une chaîne de caractères et de variables qui se transforme en un nom de snapshot (par exemple, `scheduled-%Y-%m-%d-%H-%m` se transforme en « scheduled-2012-04-12-17-33 »). Utilisez des caractères alphabétiques, des chiffres, les caractères _ et -, ainsi que des variables qui se transforment en valeurs actuelles.

5. Cliquez sur **Validate Pattern & Update Sample**.
6. Cliquez sur **Next**.

7. Sélectionnez la date à laquelle le planning sera exécuté :
   a. Weekly : cochez les cases en regard des jours de la semaine ou sélectionnez **Every Day**.
   b. Monthly : cliquez sur l'option **Selected Days**, puis sur les dates dans le calendrier, ou sélectionnez l'option **Last Day of the Month**.
   c. Cliquez sur **Next**.
8. Sélectionnez l'heure de la journée à laquelle le planning sera exécuté :
   a. At Specific Times : cliquez sur **Add**, puis entrez l'heure au format *hh:mm* dans la boîte de dialogue Time, et cliquez sur **OK**.
   b. In Intervals : cliquez sur les flèches déroulantes pour sélectionner les heures de début et de fin au format *hh:mm* et AM (matin) ou PM (après-midi). Cliquez sur les flèches déroulantes **Interval** pour sélectionner un nombre, puis les heures ou les minutes de l'intervalle.
   c. Cliquez sur **Next**.
9. Dans la zone de saisie Retention Period, saisissez un nombre et cliquez sur la flèche déroulante pour sélectionner days, months ou years, puis cliquez sur **Next**.

   Les plannings doivent indiquer explicitement une durée de rétention.
10. Vérifiez les paramètres du récapitulatif du planning, puis cliquez sur **Finish** pour terminer le planning ou sur **Back** pour modifier des entrées.
11. Si une structure MTree n'est pas associée au planning, une boîte de dialogue d'avertissement vous demande si vous souhaitez ajouter une structure MTree au planning. Cliquez sur **OK** pour continuer (ou sur **Cancel** pour quitter).
12. Pour attribuer une structure MTree au planning, dans la zone MTree, cochez la case d'une ou de plusieurs structures MTree dans le volet Available MTrees, puis cliquez sur **Add** et **OK**.

Conventions de dénomination pour les snapshots créés par un ordonnanceur

La convention d'affectation de noms pour les snapshots planifiés consiste à utiliser le mot scheduled suivi de la date à laquelle le snapshot doit se produire, au format `scheduled-`*`yyyy-mm-dd-hh-mm`*. Par exemple, `scheduled-2009-04-27-13-30`.

Le nom « mon_thurs » est le nom d'un ordonnanceur de snapshot. Les snapshots générés par cet ordonnanceur peuvent avoir pour nom `scheduled-2008-03-24-20-00`, `scheduled-2008-03-25-20-00`, etc.

Modification d'un planning de snapshots

Modifiez le nom, la date et la période de rétention du planning de snapshots.

Procédure

1. Sélectionnez un planning dans la liste des plannings, puis cliquez sur **Modify**.
2. Dans la zone de texte Name, entrez le nom du planning, puis cliquez sur **Next**.

   Vous pouvez utiliser des caractères alphanumériques, des traits de soulignement (_) et des tirets (-).
3. Sélectionnez la date à laquelle le planning doit être exécuté :
   a. Weekly : cochez les cases en regard des jours de la semaine ou sélectionnez **Every Day**.

b. Monthly : cliquez sur l'option **Selected Days**, puis sur les dates dans le calendrier, ou sélectionnez l'option **Last Day of the Month**.

c. Cliquez sur **Next**.

4. Sélectionnez l'heure de la journée à laquelle le planning doit être exécuté :

a. At Specific Times : cochez la case correspondant à l'heure planifiée dans la liste Times, puis cliquez sur **Edit**. Dans la boîte de dialogue Times qui s'affiche, saisissez une nouvelle heure au format *hh:mm*, puis cliquez sur **OK**. Ou cliquez sur **Delete** pour supprimer l'heure planifiée.

b. In Intervals : cliquez sur les flèches déroulantes pour sélectionner les heures de début et de fin au format *hh:mm* et AM (matin) ou PM (après-midi). Cliquez sur les flèches déroulantes Interval pour sélectionner un nombre, puis les heures ou les minutes de l'intervalle.

c. Cliquez sur **Next**.

5. Dans la zone de saisie Retention Period, saisissez un nombre et cliquez sur la flèche déroulante pour sélectionner days, months ou years, puis cliquez sur **Next**.

6. Vérifiez les paramètres du récapitulatif du planning, puis cliquez sur **Finish** pour terminer le planning ou sur **Back** pour modifier des entrées.

Suppression d'un planning de snapshots

Supprimez un planning de snapshots de la liste de plannings.

Procédure

1. Dans la liste Schedule, cochez la case en regard d'un ordonnanceur pour sélectionner ce dernier et cliquez sur **Delete**.
2. Dans la boîte de dialogue de vérification, cliquez sur **OK**, puis sur **Close**.

Restauration de données à partir d'un snapshot

Utilisez une opération Fast Copy pour récupérer les données stockées dans un snapshot. Reportez-vous à la section concernant les opérations Fast Copy.

CHAPITRE 8

CIFS

Ce chapitre traite des sujets suivants :

Tour d'horizon du système CIFS

Les clients CIFS (Common Internet File System) peuvent accéder aux répertoires système du système Data Domain.

- Le répertoire `/data/col1/backup` est le répertoire cible des données compressées des serveurs de sauvegarde.
- Le répertoire `/ddvar/core` contient les fichiers mémoire et les fichiers log du système Data Domain (supprimez les anciens fichiers mémoire et fichiers log pour libérer de l'espace dans cette zone).

Remarque

Vous pouvez également supprimer des fichiers mémoire du répertoire `/ddvar` ou `/ddvar/ext` s'il existe.

Les clients, tels que les serveurs de sauvegarde qui effectuent les opérations de sauvegarde et de restauration avec un système Data Domain doivent au moins pouvoir accéder au répertoire `/data/col1/backup`. Les clients qui disposent d'un accès administratif doivent pouvoir accéder au répertoire `/ddvar/core` pour récupérer les fichiers mémoire et les fichiers log.

Dans le cadre de la configuration initiale du système Data Domain, les clients CIFS ont été configurés pour accéder à ces répertoires. Ce chapitre explique comment modifier ces paramètres et contrôler l'accès aux données à l'aide de Data DD Manager et de la commande `cifs`.

Remarque

- La page **Protocols** > **CIFS** de DD System Manager permet d'effectuer des opérations CIFS importantes, comme activer et désactiver le système CIFS, définir l'authentification, gérer les partages et afficher les informations relatives à la configuration et aux partages.
- La commande `cifs` contient toutes les options de gestion de sauvegarde du système CIFS et les restaurations entre les clients Windows et les systèmes Data Domain. Elle affiche également l'état du système CIFS et des statistiques. Pour plus d'informations sur les commandes `cifs`, consultez le *Guide de référence des commandes de Data Domain Operating System*.
- Pour plus d'informations sur la configuration initiale du système, consultez le document intitulé *Guide de configuration initiale de Data Domain Operating System*.
- Pour plus d'informations sur la façon de configurer des clients pour qu'ils utilisent le système Data Domain en tant que serveur, consultez le guide de réglage s'y rapportant (par exemple, *CIFS Tuning Guide*) disponible sur le site Web support.emc.com. Recherchez le nom complet du document à l'aide du champ Search.

Configuration de la signature SMB

Sur une version de DD OS qui prend en charge cette fonction, vous pouvez configurer la signature SMB à l'aide de l'option CIFS appelée signature de serveur.

Cette fonction est désactivée par défaut, car elle altère les performances. Lorsqu'elle est activée, la signature SMB peut entraîner une baisse de 29 % (lectures) à 50 % (écritures) des performances en termes de débit, bien que les performances du seul système puissent varier. La signature SMB peut être définie sur trois valeurs différentes : disabled, auto et mandatory.

- Lorsque la signature SMB est définie sur disabled, elle est désactivée. Il s'agit de la valeur par défaut.
- Lorsque la signature SMB est définie sur required, elle est requise et doit être activée sur les deux ordinateurs figurant sur la connexion SMB.

Commandes CLI de la signature SMB

`cifs option set "server-signing" required`
Définit la signature du serveur comme étant obligatoire.

`cifs option reset "server-signing"`
Réinitialise la signature du serveur sur la valeur par défaut (disabled).

Conformément aux bonnes pratiques, chaque fois que vous modifiez les options de signature SMB, vous devez désactiver, puis activer le service CIFS (redémarrage) à l'aide des commandes CLI suivantes :

```
cifs disable
cifs enable
```

L'interface DD System Manager indique si l'option de signature SMB est désactivée ou définie sur auto ou sur mandatory. Pour afficher ce paramètre dans l'interface, accédez à **Protocols** > **CIFS** > **Configuration tab**. Dans la section Options, la valeur de l'option de signature SMB sera disabled, auto ou mandatory, reflétant ainsi la valeur définie à l'aide des commandes CLI.

Configuration d'un système CIFS

Cette section contient des instructions pour activer des services CIFS, à savoir le serveur CIFS, etc.

Systèmes haute disponibilité et CIFS

Les systèmes haute disponibilité sont compatibles avec les systèmes CIFS. Toutefois, si une tâche CIFS est en cours d'exécution lors d'un basculement sur incident, celle-ci devra être redémarrée.

« /ddvar est un système de fichiers ext3, qui ne peut pas être partagé comme un partage basé sur une MTree normale. Les informations contenues dans /ddvar deviennent obsolètes lorsque le nœud actif bascule sur le nœud en veille, car les descripteurs de fichier sont différents sur les deux nœuds. Si /ddvar est monté pour accéder aux fichiers log ou mettre à niveau le système, démontez et remontez /ddvar si un basculement sur incident s'est produit depuis la dernière fois que /ddvar a été monté. »

Préparation des clients pour l'accès aux systèmes Data Domain

La documentation est disponible en ligne.

Procédure

1. Connectez-vous au site Web de support en ligne (support.emc.com).
2. Dans le champ Search, saisissez le nom du document que vous recherchez.

3. Sélectionnez le document approprié, tel que *CIFS and Data Domain Systems Tech Note*.
4. Suivez les instructions décrites dans le document.

Activation des services CIFS

Autorisez le client à accéder au système via le protocole CIFS.

Après avoir configuré l'accès d'un client aux systèmes Data Domain, vous devez activer les services CIFS afin que ce client puisse accéder au système via le protocole CIFS.

Procédure

1. Pour le système Data Domain sélectionné dans l'arborescence de navigation de DD System Manager, cliquez sur **Protocols** > **CIFS**.
2. Dans la zone CIFS Status, cliquez sur **Enable**.

Attribution de nom au serveur CIFS

Le nom d'hôte du système Data Domain qui joue le rôle de serveur CIFS est défini lors de la configuration initiale du système.

Pour modifier le nom d'un serveur CIFS, reportez-vous aux procédures décrites dans la section concernant la définition des paramètres d'authentification.

Le nom d'hôte du système Data Domain doit correspondre au nom attribué à son ou ses adresses IP dans la table DNS. Si ce n'est pas le cas, l'authentification, ainsi que les tentatives de rejoindre un domaine, peuvent échouer. Si vous devez modifier le nom d'hôte d'un système Data Domain, utilisez la commande `net set hostname` et modifiez également l'entrée du système dans la table DNS.

Lorsque le système Data Domain joue le rôle de serveur CIFS, il prend le nom d'hôte du système. À des fins de compatibilité, il crée également un nom NetBIOS. Ce nom NetBIOS est le premier composant du nom d'hôte entièrement indiqué en lettres majuscules. Par exemple, le nom d'hôte `jp9.oasis.local` est tronqué en nom NetBIOS `JP9`. Le serveur CIFS répond aux deux noms.

Vous pouvez configurer le serveur CIFS pour qu'il réponde à différents noms aux niveaux du NetBIOS en changeant le nom d'hôte NetBIOS.

Modification du nom d'hôte NetBios

Modifiez le nom d'hôte NetBIOS à l'aide de la CLI.

Procédure

1. Affichez le nom NetBios actuel en entrant la commande suivante :

   ```
   # cifs show config
   ```

2. Utilisez la commande `cifs set nb-hostname`*`nb-hostname`*.

Définition des paramètres d'authentification

Définissez les paramètres d'authentification Data Domain pour utiliser CIFS.

Cliquez sur le lien Configure à droite de l'étiquette Authentication dans l'onglet Configuration. Le système accède à l'onglet **Administration** > **Access** > **Authentication**, où vous pouvez configurer l'authentification pour Active Directory, Kerberos, les groupes de travail et NIS.

Définition des options CIFS

Affichez la configuration CIFS et limitez le nombre de connexions anonymes.

Procédure

1. Sélectionnez **Protocols** > **CIFS** > **Configuration**.
2. Dans la zone Options, cliquez sur **Configure Options**.
3. Pour limiter le nombre de connexions anonymes, cochez la case de l'option **Enable** dans la zone Restrict Anonymous Connections.
4. Dans la zone Log Level, cliquez sur la liste déroulante pour sélectionner le nombre de niveaux.

   Le niveau est un nombre entier compris entre 1 (un) et 5 (cinq). La valeur Un correspond au niveau du système par défaut qui envoie le niveau le moins détaillé de messages de log relatifs au système CIFS, alors que la valeur Cinq produit le plus de détails. Les messages de log sont stockés dans `/ddvar/log/debug/cifs/cifs.log`.

   Remarque

   Un niveau de log de 5 nuit aux performances du système. Cliquez **Default** dans la zone Log Level après avoir débogué un problème. Ceci ramène le niveau à 1.

5. Dans la zone Server Signing, sélectionnez :
   - **Enabled** pour activer la signature du serveur
   - **Disabled** pour désactiver la signature du serveur
   - **Required** lorsque la signature du serveur est requise

Désactivation des services CIFS

Évitez que les clients puissent accéder au système Data Domain.

Procédure

1. Sélectionnez **Protocols** > **CIFS**.
2. Dans la zone Status, cliquez sur **Disable**.
3. Cliquez sur **OK**.

   Même après avoir désactivé l'accès CIFS, les services d'authentification CIFS continuent de s'exécuter sur le système Data Domain. Cette continuation est nécessaire pour authentifier les utilisateurs du domaine Active Directory pour l'accès administratif.

Utilisation des partages

Pour partager des données, créez des partages sur le système Data Domain.

Les partages sont gérés sur le système Data Domain et les systèmes CIFS.

Création de partages sur le système Data Domain

Lorsque vous créez des partages, vous devez attribuer séparément un accès client à chaque répertoire et supprimer séparément l'accès à partir de chaque répertoire. Par

exemple, il est possible de supprimer un client du répertoire `/ddvar` et de maintenir son accès à `/data/col1/backup`

Un système Data Domain prend en charge jusqu'à 3 000 partages CIFS,[1] Par ailleurs, 600 connexions simultanées sont autorisées. Toutefois, le nombre maximal de connexions prises en charge est basé sur une mémoire système. Pour plus d'informations, reportez-vous à la section relative à la définition du nombre maximal de fichiers ouverts sur une connexion.

Remarque

Lorsque la réplication doit être implémentée, un système Data Domain peut recevoir des sauvegardes de clients CIFS et NFS, à condition d'utiliser des répertoires distincts pour chaque type de données. Ne mélangez pas les données CIFS et NFS dans le même répertoire.

Procédure

1. Sélectionnez les onglets **Protocols** > **CIFS** pour accéder à la vue CIFS.
2. Assurez-vous que l'authentification a été configurée, comme indiqué dans la section concernant la configuration des paramètres d'authentification.
3. Sur le client CIFS, définissez les options de sécurité ou les autorisations des répertoires partagés.
4. Dans la vue CIFS, cliquez sur l'onglet Shares.
5. Cliquez sur **Create**.
6. Dans cette boîte de dialogue, saisissez les informations suivantes :

Tableau 105 Informations de la boîte de dialogue Shares

Élément	Description
Share Name	Nom descriptif du partage.
Directory Path	Le chemin du répertoire cible (par exemple, `/data/col1/backup/dir1`). **Remarque** col1 utilise un L minuscule suivi du chiffre 1.
Comment	Commentaire décrivant le partage.

Remarque

Le nom du partage peut comporter 80 caractères au maximum et ne doit pas contenir les caractères suivants : \ / : * ? " < > | + [ ] ; , = ou caractères ASCII étendus.

7. Pour ajouter un client, cliquez sur Add (+) dans la zone Clients. La boîte de dialogue Client s'affiche. Saisissez le nom du client dans la zone de texte Client, puis cliquez sur **OK**.

   Tenez compte des informations suivantes lors de la saisie du nom de client.

1. Ce nombre peut dépendre des limitations matérielles.

- Les caractères blancs ou de tabulation (espace blanc) sont autorisés.
- Il est déconseillé d'utiliser un astérisque (*) et un nom de client individuel ou une adresse IP pour un partage donné. Lorsqu'un astérisque (*) est présent, aucune autre entrée de client n'est utilisée pour ce partage.
- Il n'est pas nécessaire d'utiliser le nom du client et l'adresse IP du client pour le même client sur un partage donné. Utilisez des noms de client lorsque les noms de client sont définis dans la table DNS.
- Pour rendre le partage disponible pour tous les clients, spécifiez un astérisque (*) en tant que client. Tous les utilisateurs figurant dans la liste des clients peuvent accéder au partage, sauf si un ou plusieurs noms d'utilisateur sont définis, auquel cas seuls les noms répertoriés peuvent accéder au partage.

Reprenez cette étape pour chacun des clients à configurer.

8. Dans la zone Max Connections, sélectionnez la zone de texte et saisissez le nombre maximal de connexions au partage autorisées simultanément. La valeur par défaut, c'est-à-dire zéro, (également définissable à l'aide du bouton Unlimited) n'impose aucune limite au nombre de connexions.
9. Cliquez sur **OK**.

   Le partage qui vient d'être créé s'affiche à la fin de la liste des partages, sités au centre du volet Shares.

Équivalent de la CLI

Procédure

1. Exécutez la commande`cifs status` pour vérifier que CIFS est activé.
2. Exécutez la commande`filesys status` pour vérifier que le système de fichiers est activé.
3. Exécutez la commande `hostname` pour déterminer le nom d'hôte du système.
4. Créez le partage CIFS.

   `cifs share create <share> path <path> {max-connections <max connections> | clients <clients> | users <users> | comment <comment>}`

   ```
   # cifs share create backup path /backup
   ```

5. Accordez l'accès client au partage.

   `cifs share modify <share> {max-connections <max connections> | clients <clients> | browsing {enabled | disabled} | writeable {enabled | disabled} | users <users> | comment <comment>}`

   ```
   # cifs share modify backup clients
   "srvr24.yourdomain.com,srvr24,10.24.160.116
   ```

6. Si vous le souhaitez, rendez le partage visible.

   `cifs share <share> browsing enabled`

   ```
   # cifs share backup browsing enabled
   ```

7. Vous pouvez aussi rendre le partage disponible en écriture.

   `cifs share <share> writeable enabled`

```
# cifs share backup writeable enabled
```

8. Dans le système Windows, sélectionnez **Start** > **Run**, puis saisissez le nom d'hôte et le répertoire du partage CIFS.

   <DDhostname>.*<DDdomain.com>**<sharename>*

9. En cas de problèmes de connexion au partage CIFS, exécutez la commande `cifs share show` pour vérifier l'état du partage.

   L'avertissement `WARNING: The share path does not exist!` s'affiche si le partage n'existe pas ou a été mal orthographié lors de la création.

```
# cifs share show
--------------- share backup ---------------

enabled: yes
path: /backup
```

10. Si le partage CIFS n'est toujours pas accessible, vérifiez que toutes les informations client figurent dans la liste d'accès et que toutes les connexions réseau sont fonctionnelles.

Modification d'un partage sur un système Data Domain

Modifiez les informations du partage et les connexions.

Procédure

1. Sélectionnez **Protocols** > **CIFS** > **Shares** pour accéder à la vue CIFS et à l'onglet Shares.
2. Cochez la case en regard du partage que vous souhaitez modifier dans la liste Share Name.
3. Cliquez sur **Modifier**.
4. Modifiez les informations relatives au partage :
   a. Pour modifier le commentaire, saisissez le nouveau texte dans le champ Comment.
   b. Pour modifier des noms d'utilisateurs ou de groupes, cochez la case correspondant à l'utilisateur ou au groupe dans la liste User/Group, puis cliquez sur **Edit** (icône représentant un crayon) ou sur **Delete** (X). Pour ajouter un utilisateur ou un groupe, cliquez sur le signe plus (**+**) et, dans la boîte de dialogue User/Group, sélectionnez l'option Type for User or Group, puis saisissez le nom de l'utilisateur ou du groupe.
   c. Pour modifier le nom d'un client, cochez la case en regard de son nom dans la liste Client, puis cliquez sur **Edit** (icône représentant un crayon) ou sur **Delete** (X). Pour ajouter un client, cliquez sur Ajouter (**+**) et ajoutez le nom dans la boîte de dialogue Client.

   Remarque

   Pour rendre le partage disponible pour tous les clients, spécifiez un astérisque (*) en tant que client. Tous les utilisateurs figurant dans la liste des clients peuvent accéder au partage, sauf si un ou plusieurs noms d'utilisateur sont définis, auquel cas seuls les noms répertoriés peuvent accéder au partage.

d. Cliquez sur **OK**.

5. Dans la zone Max Connections de la zone de texte, modifiez le nombre maximal de connexions au partage autorisées simultanément ou sélectionnez Unlimited pour n'appliquer aucune limite au nombre de connexions.
6. Cliquez sur **OK**.

Création d'un partage à partir d'un partage existant

Créez un partage à partir d'un partage existant et modifiez le nouveau partage si nécessaire.

Remarque

Les autorisations utilisateur du partage existant sont transmises au nouveau partage.

Procédure

1. Dans l'onglet CIFS Shares, cochez la case correspondant au partage que vous souhaitez utiliser comme source.
2. Cliquez sur **Create From**.
3. Modifiez les informations relatives au partage, comme décrit dans la section relative à la modification d'un partage sur un système Data Domain.

Désactivation d'un partage sur un système Data Domain

Désactivez un ou plusieurs partages existants.

Procédure

1. Sous l'onglet Shares, cochez la case du partage que vous souhaitez désactiver dans la liste Share Name.
2. Cliquez sur **Disable**.
3. Cliquez sur **Close**.

Activation d'un partage sur un système Data Domain

Activez un ou plusieurs partages existants.

Procédure

1. Sous l'onglet Shares, cochez la case en regard des partages que vous souhaitez activer dans la liste Share Name.
2. Cliquez sur **Enable**.
3. Cliquez sur **Close**.

Suppression d'un partage sur un système Data Domain

Supprimez un ou plusieurs partages existants.

Procédure

1. Sous l'onglet Shares, cochez la case en regard des partages que vous souhaitez supprimer dans la liste Share Name.
2. Cliquez sur **Delete**.

   Une boîte de dialogue d'avertissement s'affiche.

3. Cliquez sur le bouton **OK**.

   Les partages sont supprimés.

Administration via MMC

Utilisez Microsoft Management Console (MMC) pour l'administration.

DD OS prend en charge les fonctions de MMC suivantes :

- Gestion des partages, à l'exception de la navigation lors de l'ajout d'un partage, ou modification des paramètres de mise hors ligne par défaut (qui est une procédure manuelle).
- Gestion des sessions.
- Gestion de fichier ouverte, sauf pour la suppression de fichiers.

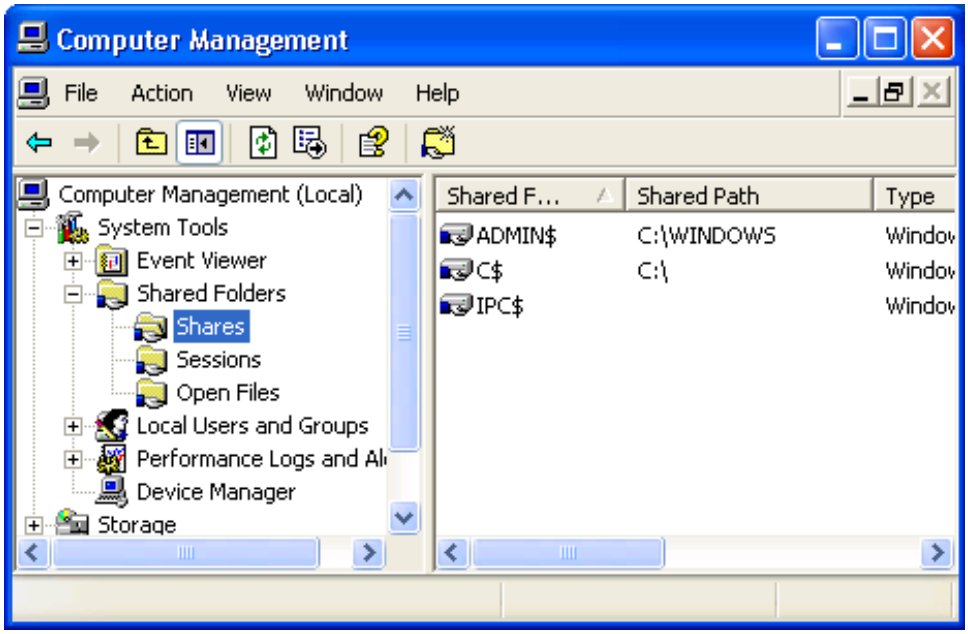
Connexion à un système Data Domain pour un client CIFS

Utilisez le système CIFS pour connecter un système Data Domain et créez un sous-dossier de sauvegarde en lecture seule.

Procédure

1. Sur la page CIFS du système Data Domain, vérifiez que l'état CIFS indique que le système CIFS est activé et en cours d'exécution.
2. Dans le panneau de configuration, ouvrez Administrative Tools, puis sélectionnez **Computer Management**.
3. Dans la boîte de dialogue Computer Management, cliquez avec le bouton droit de la souris sur **Computer Management (local)**, puis sélectionnez **Connect to another computer** dans le menu.
4. Dans la boîte de dialogue Select Computer, sélectionnez **Another computer**, puis saisissez le nom ou l'adresse IP du système Data Domain.
5. Créez un sous-dossier `\backup` en lecture seule. Pour plus d'informations, reportez-vous à la section relative à la création d'un sous-dossier /data/col1/backup en lecture seule.

Figure 7 Boîte de dialogue Computer Management



Création d'un sous-dossier \data\col1\backup en lecture seule

Saisissez un chemin, partagez un nom et sélectionnez des autorisations.

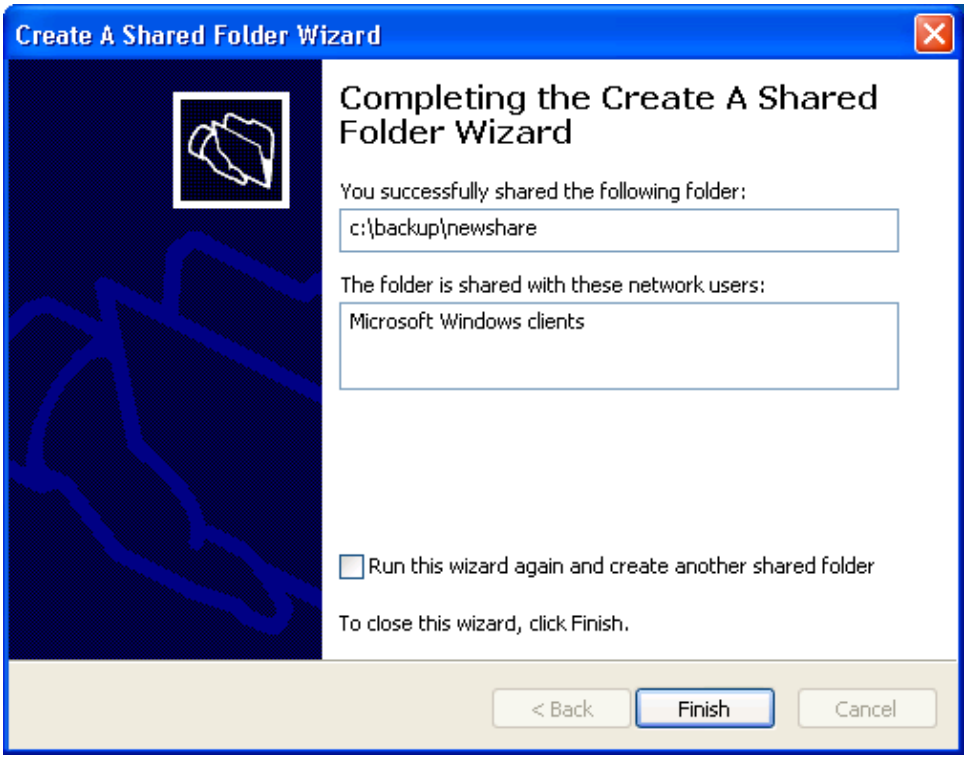
Procédure

1. Dans le panneau de configuration, ouvrez Administrative Tools, puis sélectionnez **Computer Management**.
2. Cliquez avec le bouton droit de la souris sur **Shares** sur le répertoire des dossiers partagés.
3. Sélectionnez **New File Share** dans le menu.

   L'assistant **Create a Shared Folder** s'ouvre. Le nom de l'ordinateur doit être le nom ou l'adresse IP du système Data Domain.

4. Saisissez le chemin d'accès au répertoire à partager. Entrez, par exemple, `C:\data\col1\backup\newshare`.
5. Saisissez le nom du partage. Entrez, par exemple, **`newshare`**. Cliquez sur **Next**.
6. Pour les autorisations d'accès au dossier partagé, les administrateurs sélectionnés bénéficient d'un accès complet. D'autres utilisateurs disposent d'un accès en lecture seule. Cliquez sur **Next**.

Figure 8 Exécution de l'assistant de création d'un dossier partagé



7. La boîte de dialogue d'exécution indique que vous avez correctement partagé le dossier avec tous les clients Microsoft Windows du réseau. Cliquez sur **Finish**.

   Le dossier partagé que vous venez de créer est répertorié dans la boîte de dialogue Computer Management.

Affichage d'informations CIFS

Affichez des informations sur les dossiers partagés, les sessions et les fichiers ouverts.

Procédure

1. Dans le panneau de configuration, ouvrez Administrative Tools, puis sélectionnez **Computer Management**.
2. Dans le répertoire System Tools, sélectionnez l'un des dossiers partagés (**Shares**, **Sessions** ou **Open Files**).

   Des informations sur les dossiers partagés, les sessions et les fichiers ouverts s'affichent dans le volet de droite.

Gestion du contrôle d'accès

Accédez aux partages à partir d'un client Windows, fournissez un accès administratif et autorisez l'accès aux utilisateurs d'un domaine fiable.

Accès aux partages à partir d'un client Windows

Utilisez la ligne de commande pour mapper un partage.

Procédure

- À partir d'un client Windows, utilisez la commande DOS suivante :
  `net use`*drive*`:`*backup-location*

Par exemple, saisissez :

```
# \\dd02\backup /USER:dd02\backup22
```

Cette commande mappe le partage des sauvegardes du système Data Domain dd02 au lecteur H du système Windows, et octroie à l'utilisateur appelé backup22 un accès au répertoire `\\DD_sys\backup`.

DD OS prend en charge la fonctionnalité SMB Change Notify. Celle-ci améliore les performances CIFS sur le client Windows en permettant au CIFS server d'informer automatiquement le client Windows des modifications apportées au partage CIFS et élimine le besoin pour le client d'interroger le système Data Domain pour rechercher les modifications apportées au partage.

Octroi d'un accès administrateur aux utilisateurs d'un domaine

Utilisez la ligne de commande pour ajouter le système CIFS et inclure le nom de domaine dans l'instruction ssh.

Procédure

- Entrez : **`adminaccess authentication add cifs`**

  La commande SSH, Telnet ou FTP permettant d'accéder au système Data Domain doit inclure entre guillemets le nom de domaine, une barre oblique inverse, ainsi que le nom d'utilisateur. Exemple :

  ```
  C:> ssh "domain2\djones" @dd22
  ```

Autorisation d'accès administratif concédée à un système Data Domain pour les utilisateurs du domaine

Utilisez la ligne de commande pour mapper un numéro de groupe de système DD, puis activez l'accès d'administration CIFS.

Procédure

1. Pour mapper un numéro de groupe de système Data Domain par défaut à un nom de groupe Windows qui diffère du nom de groupe par défaut, utilisez la commande
   `cifs option set "dd admin group2" ["windows`*grp-name*`"].`

   Le nom de groupe Windows est un groupe (basé sur l'un des rôles de l'utilisateur, à savoir administrateur, utilisateur ou opérateur de sauvegarde) existant sur un contrôleur de domaine Windows. Et vous pouvez posséder jusqu'à 50 groupes (dd admin group1 à dd admin group50)

   Remarque

   Pour obtenir une description des rôles d'utilisateur et de groupes Windows dans DD OS, reportez-vous à la section relative à la gestion des systèmes Data Domain.

2. Activez l'accès d'administration CIFS en saisissant

   ```
   adminaccess authentication add cifs
   ```

- Le groupe de systèmes Data Domain par défaut, dd admin group1, est mappé au groupe Windows Domain Admins.
- Vous pouvez mapper le groupe de systèmes Data Domain group dd admin group2 à un groupe Windows appelé Data Domain que vous créez sur un contrôleur de domaine Windows.
- L'accès est possible via SSH, Telnet, FTP, HTTP et HTTPS.
- Après avoir configuré l'accès administrateur au système Data Domain à partir du groupe `Data Domain` Windows, vous devez activer l'accès administrateur CIFS à l'aide de la commande `adminaccess`.

Restriction de l'accès administratif à partir de Windows

Utilisez la ligne de commande pour refuser l'accès aux utilisateurs dépourvus d'un compte DD.

Procédure

- Entrez : `adminaccess authentication del cifs`

  Cette commande interdit aux utilisateurs Windows d'accéder au système Data Domain s'ils ne disposent pas d'un compte sur ce système.

Accès aux fichiers

Cette section contient des informations sur les listes de contrôle d'accès (ACL), la définition des autorisations DACL et SACL à l'aide de l'Explorateur Windows, etc.

Listes de contrôle d'accès NT

Des listes de contrôle d'accès (ACL) sont activées par défaut sur le système Data Domain.

⚠ ATTENTION

Data Domain vous recommande de ne pas désactiver les listes ACL NTFS une fois qu'elles ont été activées. Contactez le support Data Domain avant de désactiver les listes de contrôle d'accès NTFS.

Autorisations ACL par défaut

Les autorisations par défaut, qui sont attribuées aux nouveaux objets créés via le protocole CIFS lorsque des listes ACL sont activées dépendent de l'état du répertoire parent. Il existe trois possibilités :

- Le répertoire parent n'a aucune liste ACL, car il a été créé via le protocole NFS.
- Le répertoire parent dispose d'une liste ACL pouvant être héritée, soit parce qu'il a été créé via le protocole CIFS ou parce qu'une liste ACL a été explicitement définie. La liste ACL héritée est définie sur de nouveaux objets.
- Le répertoire parent dispose d'une liste ACL, mais celle-ci ne peut pas être héritée. Les autorisations sont les suivantes :

Tableau 106 Autorisations

Type	Nom	Autorisation	S'applique à
Autoriser	SYSTEM	Contrôle total	Ce dossier uniquement
Autoriser	CREATOR OWNER	Contrôle total	Ce dossier uniquement

Remarque

CREATOR OWNER est remplacé par l'utilisateur qui a créé le fichier/répertoire pour les utilisateurs standard et par les administrateurs pour les administrateurs.

Autorisations pour un nouvel objet lorsque le répertoire parent n'a aucune liste ACL

Les autorisations sont les suivantes :

- BUILTIN\Administrators:(OI)(CI)F
- NT AUTHORITY\SYSTEM:(OI)(CI)F
- CREATOR OWNER:(OI)(CI)(IO)F
- BUILTIN\Users:(OI)(CI)R
- BUILTIN\Users:(CI)(special access:)FILE_APPEND_DATA
- BUILTIN\Users:(CI)(IO)(special access:)FILE_WRITE_DATA
- Everyone:(OI)(CI)R

Ces autorisations sont décrites plus en détail ci-après :

Tableau 107 Détails des autorisations

Type	Nom	Autorisation	S'applique à
Autoriser	Administrators	Contrôle total	Ce dossier, les sous-dossiers et les fichiers
Autoriser	SYSTEM	Contrôle total	Ce dossier, les sous-dossiers et les fichiers
Autoriser	CREATOR OWNER	Contrôle total	Les sous-dossiers et les fichiers uniquement
Autoriser	Users	Lecture/exécution	Ce dossier, les sous-dossiers et les fichiers
Autoriser	Users	Création de sous-dossiers	Ce dossier et les sous-dossiers uniquement
Autoriser	Users	Création de fichiers	Sous-dossiers uniquement
Autoriser	Everyone	Lecture/exécution	Ce dossier, les sous-dossiers et les fichiers

Définition des autorisations ACL et de la sécurité

Des outils de sauvegarde et de restauration basés sur Windows, tels que NetBackup, peuvent être utilisés pour sauvegarder des fichiers protégés DACL et SACL sur le système Data Domain, et les restaurer à partir du système Data Domain.

Autorisations granulaires et complexes (DACL)

Vous pouvez définir des autorisations granulaires et complexes (DACL) sur n'importe quel objet fichier ou dossier dans le système de fichiers, à l'aide des commandes

Windows telles que `cacls`, `xcacls`, `xcopy` et `scopy` ou du protocole CIFS via l'interface utilisateur de l'Explorateur Windows.

ACL d'audit (SACL)
Vous pouvez définir une liste ACL d'audit (SACL) sur n'importe quel objet dans le système de fichiers, à l'aide de commandes ou du protocole CIFS via l'interface utilisateur de l'Explorateur Windows.

Définition des autorisations DACL à l'aide de l'Explorateur Windows

Utilisez les paramètres des propriétés de l'Explorateur pour sélectionner des autorisations DACL.

Procédure

1. Cliquez sur le fichier ou le dossier avec le bouton droit de la souris et sélectionnez **Properties**.
2. Dans la boîte de dialogue Properties, cliquez sur l'onglet Security.
3. Sélectionnez le nom de groupe ou d'utilisateur, par exemple **Administrators**, dans la liste. Les autorisations s'affichent, dans le cas présent pour `Administrators, Full Control`.
4. Cliquez sur le bouton **Advanced** pour définir des autorisations spéciales.
5. Dans la boîte de dialogue Advanced Security Settings for ACL, cliquez sur l'onglet Permissions.
6. Sélectionnez l'entrée d'autorisation dans la liste.
7. Pour afficher plus d'informations sur une entrée d'autorisation, sélectionnez l'entrée et cliquez sur **Edit**.
8. Sélectionnez l'option Inherit from parent pour que les objets enfants héritent des autorisations des entrées parentes, puis cliquez sur **OK**.

Définition des autorisations SACL à l'aide de l'Explorateur Windows

Utilisez les paramètres des propriétés de l'Explorateur pour sélectionner des autorisations SACL.

Procédure

1. Cliquez sur le fichier ou sur le dossier avec le bouton droit de la souris et sélectionnez l'option **Properties** dans le menu.
2. Dans la boîte de dialogue Properties, cliquez sur l'onglet Security.
3. Dans la liste, sélectionnez le nom du groupe ou de l'utilisateur, par exemple **Administrators**. Les autorisations s'affichent alors, en l'occurrence `Full Control`.
4. Cliquez sur le bouton **Advanced** pour définir des autorisations spéciales.
5. Dans la boîte de dialogue Advanced Security Settings for ACL, cliquez sur l'onglet Auditing.
6. Sélectionnez l'entrée d'audit dans la liste.
7. Pour afficher plus d'informations sur des entrées d'audit spéciales, sélectionnez une entrée et cliquez sur **Edit**.
8. Sélectionnez l'option Inherit from parent pour que les objets enfants héritent des autorisations des entrées parentes, puis cliquez sur **OK**.

Affichage ou modification de l'ID de sécurité du propriétaire actuel (SID de propriétaire)

Utilisez la boîte de dialogue Advanced Security Settings for ACL.

Procédure

1. Dans la boîte de dialogue Advanced Security Settings for ACL, cliquez sur l'onglet Owner.
2. Pour modifier le propriétaire, sélectionnez un nom dans la liste Change owner, puis cliquez sur **OK**.

Contrôle du mappage des ID de compte

L'option CIFS idmap-type contrôle le comportement du mappage des ID de compte.

Cette option possède deux valeurs : rid (valeur par défaut) et none. Lorsque l'option est définie sur rid, le mappage ID-à-ID est effectué en interne. Lorsque l'option est définie sur none, tous les utilisateurs CIFS sont mappés à un utilisateur UNIX local nommé « cifsuser » appartenant au groupe des utilisateurs UNIX locaux.

Tenez compte des informations suivantes lors de la gestion de cette option.

- Pour que cette option puisse être configurée, le CIFS doit être désactivé. Si CIFS est en cours d'exécution, désactivez les services CIFS.
- L'option idmap-type peut être définie sur none uniquement lorsque la prise en charge ACL est activée.
- Lorsque le type idmap est modifié, la conversion des métadonnées d'un système de fichiers peut être requise pour permettre un accès correct aux fichiers. Sans conversion, l'utilisateur risque de ne pas être en mesure d'accéder aux données. Pour convertir les métadonnées, consultez votre fournisseur de services contractuel.

Surveillance d’une opération du système CIFS

Rubriques sur la surveillance d'une opération du système CIFS.

Affichage de l’état du système CIFS

Affichez et activez/désactivez l’état du système CIFS.

Procédure

1. Dans DD System Manager, sélectionnez **Protocols** > **CIFS**.
   - L’état est soit activé et en cours, soit désactivé mais avec l’authentification CIFS qui s’exécute.
     Pour activer le système CIFS, reportez-vous à la section concernant l’activation des services CIFS. Pour désactiver le système CIFS, reportez-vous à la section concernant la désactivation des services CIFS.
   - L’option **Connections** répertorie le total des connexions ouvertes et des fichiers ouverts.

Tableau 108 Informations détaillées sur les connexions

Élément	Description
Open Connections	Connexions CIFS ouvertes

Tableau 108 Informations détaillées sur les connexions (suite)

Élément	Description
Connection Limit	Nombre maximal de connexions autorisées
Open Files	Fichiers ouverts actuellement
Max Open Files	Nombre maximal de fichiers ouverts sur un système Data Domain

2. Cliquez sur **Connection Details** afin d'afficher plus d'informations sur les connexions.

Tableau 109 Informations détaillées sur les connexions

Élément	Description
Sessions	Sessions CIFS actives
Computer	Adresse IP ou nom d'ordinateur connecté avec DDR pour la session
User	Utilisateur se servant de l'ordinateur connecté avec DDR
Open Files	Nombre de fichiers ouverts pour chaque session
Connection Time	Durée de la connexion en minutes
User	Nom de domaine de l'ordinateur
Mode	Autorisations sur les fichiers
Locks	Nombre de verrous sur le fichier
Files	Emplacement du fichier

Affichage de la configuration CIFS

Cette section affiche la configuration CIFS.

Configuration de l'authentification

Les informations affichées dans le volet d'authentification changent selon le type d'authentification configuré.

Cliquez sur le lien Configure à droite de l'étiquette Authentication dans l'onglet Configuration. Le système accède à la page **Administration** > **Access** > **Authentication** où vous pouvez configurer l'authentification pour Active Directory, Kerberos, les groupes de travail et NIS.

Configuration Active Directory

Tableau 110 Informations de configuration Active Directory

Élément	Description
Mode	Le mode Active Directory s'affiche.
Realm	Le realm configuré s'affiche.
DDNS	L'état du serveur DDNS s'affiche : activé ou désactivé.

Tableau 110 Informations de configuration Active Directory (suite)

Élément	Description
Domain Controllers	Les noms des contrôleurs de domaine configurés s'affichent ou un astérisque * apparaît si tous les contrôleurs sont autorisés.
Organizational Unit	Les noms des unités d'organisation configurés s'affichent.
CIFS Server Name	Le nom du serveur CIFS configuré s'affiche.
WINS Server Name	Le nom du serveur WINS configuré s'affiche.
Short Domain Name	Le nom abrégé du domaine s'affiche.

Configuration du groupe de travail

Tableau 111 Informations sur l'authentification via la configuration d'un groupe de travail

Élément	Description
Mode	Le mode Groupe de travail s'affiche.
Workgroup Name	Le nom du groupe de travail configuré s'affiche.
DDNS	L'état du serveur DDNS s'affiche : activé ou désactivé.
CIFS Server Name	Le nom du serveur CIFS configuré s'affiche.
WINS Server Name	Le nom du serveur WINS configuré s'affiche.

Affichage d'informations sur les partages

Cette section affiche des informations sur les partages.

Affichage des partages configurés

Affichez la liste des partages configurés.

Tableau 112 Informations relatives aux partages configurés

Élément	Description
Share Name	Nom du partage (par exemple, share1).
Share Status	État du partage : activé ou désactivé.
Directory Path	Chemin de répertoire vers le partage (par exemple, `/data/col1/backup/dir1`). **Remarque** col1 utilise la lettre L en minuscule suivie du numéro 1.
Directory Path Status	État du chemin d'accès au répertoire.

- Pour obtenir des informations sur un partage spécifique, entrez le nom du partage dans la zone de texte Filter by Share Name, puis cliquez sur **Update**.
- Cliquez sur **Update** pour revenir à la liste par défaut.

- Pour faire défiler la liste des partages, cliquez sur les flèches **<** et **>** situées en bas à droite de la vue pour aller vers l'avant ou vers l'arrière. Pour accéder directement au début de la liste, cliquez sur **|<**. Pour accéder directement à la fin de la liste, cliquez sur **>|**.
- Cliquez sur la flèche de la liste déroulante **Items per Page** pour modifier le nombre d'entrées de partage répertoriées sur une page. Les options disponibles sont les suivantes : 15, 30 ou 45 entrées.

Affichage d'informations détaillées sur un partage

Affichez des informations détaillées sur un partage en cliquant sur le nom de ce partage dans la liste des partages.

Tableau 113 Informations sur les partages

Élément	Description
Share Name	Nom du partage (par exemple, share1).
Directory Path	Le chemin du répertoire du partage (par exemple,`/data/col1/backup/dir1`). **Remarque** col1 utilise un L minuscule suivi du numéro 1.
Directory Path Status	Indique si le chemin configuré pour le répertoire existe sur le DDR. Les valeurs possibles sont Path Exists ou Path Does Not Exist, cette dernière indiquant une configuration CIFS incorrecte ou incomplète.
Max Connections	Nombre maximal de connexions au partage autorisées simultanément. La valeur par défaut est Unlimited.
Commentaire	Commentaire configuré lors de la création du partage.
Share Status	État du partage : activé ou désactivé.

- La zone Clients répertorie les clients configurés pour accéder au partage, ainsi que le total des clients sous la liste.
- La zone User/Groups répertorie les noms et types d'utilisateurs ou de groupes configurés pour accéder au partage, ainsi qu'un total d'utilisateurs ou de groupes sous la liste.
- La zone Options répertorie le nom et la valeur des options configurées.

Affichage des statistiques CIFS

Utilisez la ligne de commande pour afficher des statistiques CIFS.

Procédure

- Entrez : `cifs show detailed-stats`

  La sortie indique le nombre de demandes SMB diverses reçues et le temps qu'il a fallu pour les traiter.

Dépannage du système CIFS

Cette section décrit les procédures de dépannage de base.

Remarque

Les commandes `cifs troubleshooting` fournissent des informations détaillées sur les utilisateurs et les groupes CIFS.

Affichage de l'activité en cours des clients

Utilisez la ligne de commande pour afficher les sessions CIFS et des informations sur les fichiers ouverts.

Procédure

- Saisissez :`CIFS show active`

Résultats

Tableau 114 Sessions

Ordinateur	Utilisateur	Fichiers ouverts	Temps de connexion (secondes)	Temps d'inactivité (secondes)
::ffff:10.25.132.84	ddve-25179109\sysadmin	1	92	0

Tableau 115 Fichiers ouverts

Utilisateur	Mode	Verrouillages	Fichier
ddve-25179109\sysadmin	1	0	C:\data\col1\backup

Définition du nombre maximal de fichiers ouverts sur une connexion

Utilisez la ligne de commande pour définir le nombre maximal de fichiers pouvant être ouverts simultanément.

Procédure

- Saisissez : `cifs option set max-global-open-files` *value*.

  La *value* pour le nombre maximal de fichiers ouverts globalement peut être compris entre 1 et la limite maximale de fichiers ouverts. La limite maximale est basée sur la quantité de mémoire système DDR. Pour les systèmes disposant d'une mémoire supérieure à 12 Go, la limite du nombre maximal de fichiers ouverts est de 30 000. Pour les systèmes ayant une mémoire inférieure ou égale à 12 Go, la limite du nombre maximal de fichiers ouverts est de 10 000.

Tableau 116 Limites de connexion et du nombre maximal de fichiers ouverts

Modèles DDR	Mémoire	Limite de connexion	Limite maximale de fichiers ouverts
DD620, DD630 et DD640	8 Go	300	10 000
DD640	16 Go	600	30 000
DD640	20 Go	600	30 000
DD860	36 Go	600	30 000
DD860, DD860ArT	72 Go	600	30 000
	96 Go	600	30 000
	128 Go	600	30 000
	256 Go	600	30 000

Remarque

Le système a une limite maximale de 600 connexions CIFS et de 250 000 fichiers ouverts. Toutefois, si le système ne contient pas suffisamment de fichiers ouverts, le nombre de fichiers peut être étendu.

Remarque

Les temps de latence d'accès aux fichiers sont affectés par le nombre de fichiers figurant dans un répertoire. Dans la mesure du possible, il est recommandé que les répertoires contiennent moins de 250 000 fichiers. Des tailles de répertoire supérieures peuvent entraîner des réponses plus lentes aux opérations de métadonnées, telles que la génération de la liste des fichiers figurant dans le répertoire et l'ouverture ou la création d'un fichier.

Horloge du système Data Domain

Lorsque vous utilisez le mode Active Directory pour l'accès CIFS, l'horloge du système Data Domain ne peut être décalée de plus de cinq minutes par rapport à celle du contrôleur de domaine.

L'onglet **Administration** > **Settings** > **Time and Date Settings** de DD System Manager synchronise l'horloge avec un serveur de synchronisation.

Étant donné que le contrôleur de domaine Windows obtient l'heure d'une source externe, le protocole NTP doit être configuré. Consultez la documentation Microsoft pour savoir comment configurer NTP pour la version ou le service pack du système d'exploitation Windows en cours d'exécution sur votre contrôleur de domaine.

En mode d'authentification Active Directory, le système Data Domain synchronise régulièrement l'horloge avec un contrôleur de domaine Windows Active Directory.

Synchronisation à partir d'un contrôleur de domaine Windows

Utilisez la ligne de commande sur un contrôleur de domaine Windows pour une synchronisation avec un serveur NTP.

Remarque

Cet exemple concerne Windows 2003 SP1 ; remplacez votre serveur de domaine par le nom du serveur NTP (*ntpservername*).

Procédure

1. Sur le système Windows, entrez des commandes similaires aux commandes suivantes :

   ```
   C:\>w32tm /config /syncfromflags:manual /manualpeerlist: ntp-server-name C:\>w32tm /config /update C:\>w32tm /resync
   ```

2. Une fois NTP configuré sur le contrôleur de domaine, configurez la synchronisation du serveur de synchronisation, comme décrit dans la section relative à l'utilisation des paramètres de date et d'heure.

Synchronisation à partir d'un serveur NTP

Configurez la synchronisation du serveur de synchronisation comme cela est décrit dans la section concernant l'utilisation des paramètres d'heure et de date.

CHAPITRE 9

NFS

Ce chapitre traite des sujets suivants :

Tour d'horizon de NFS

Les clients NFS peuvent accéder aux répertoires système ou aux MTrees du système Data Domain.

- Le répertoire `/backup` est la destination par défaut des données compressées des serveurs de sauvegarde hors MTree.
- Le répertoire `/data/col1/backup` est la destination racine lorsque des structures MTrees sont utilisées pour les données compressées des serveurs de sauvegarde.
- Le répertoire `/ddvar/core` contient les fichiers mémoire et les fichiers log du système Data Domain (supprimez les anciens fichiers mémoire et fichiers log pour libérer de l'espace dans cette zone).

Remarque

Sur les systèmes Data Domain, le répertoire `/ddvar/core` se trouve sur une partition distincte. Si vous montez `/ddvar` seulement, vous ne serez pas en mesure de naviguer vers `/ddvar/core` à partir du point de montage `/ddvar`.

Les clients, tels que les serveurs de sauvegarde qui effectuent des opérations de sauvegarde et de restauration avec un système Data Domain doivent pouvoir accéder à la zone `/backup` ou `/data/col1/backup`. Les clients qui disposent d'un accès administratif doivent pouvoir accéder au répertoire `/ddvar/core` pour récupérer les fichiers mémoire et les fichiers log.

Dans le cadre de la configuration initiale du système Data Domain, les clients NFS ont été configurés pour accéder à ces zones. Ce chapitre décrit comment modifier ces paramètres et comment gérer l'accès aux données.

Remarque

- Pour plus d'informations sur la configuration initiale du système, consultez le document intitulé *Guide de configuration initial de Data Domain Operating System*.
- La commande `nfs` gère les sauvegardes et les restaurations entre les clients NFS et les systèmes Data Domain, et affiche l'état et des statistiques NFS. Pour plus d'informations sur la commande `nfs`, consultez le *Guide de référence des commandes de Data Domain Operating System*.
- Pour plus d'informations sur la configuration de clients tiers afin d'utiliser le système Data Domain comme serveur, consultez le guide d'optimisation correspondant, tel que le document *Solaris System Tuning*, disponible sur le site Web du support Data Domain. Sur la page Documentation > Integration Documentation, sélectionnez le fournisseur dans la liste, puis cliquez sur **OK**. Sélectionnez le guide d'optimisation dans la liste.

Systèmes haute disponibilité et NFS

Les systèmes haute disponibilité sont compatibles avec le protocole NFS. Si une tâche NFS est en cours lors d'un basculement sur incident, la tâche n'aura **pas** besoin d'être redémarrée.

Remarque

/ddvar est un système de fichiers ext3, qui ne peut pas être partagé comme un partage basé sur une MTree normale. Les informations contenues dans /ddvar deviennent obsolètes lorsque le nœud actif bascule sur le nœud en veille, car les descripteurs de fichier sont différents sur les deux nœuds. Si /ddvar est monté pour accéder aux fichiers log ou mettre à niveau le système, démontez et remontez /ddvar si un basculement sur incident s'est produit depuis la dernière fois que /ddvar a été monté.

Pour créer des exportations NFS valides autorisant un basculement sur incident en mode haute disponibilité, il convient de créer les exportations à partir du nœud haute disponibilité actif et de les partager, en général, sur les interfaces réseau de basculement sur incident.

Gestion de l'accès client NFS à un système Data Domain

Les rubriques de cette section expliquent comment gérer l'accès du client NFS à un système Data Domain.

L'article KB *Meilleures pratiques NFS pour Data Domain et les OS clients*, disponible à l'adresse https://support.emc.com/kb/180552, fournit des renseignements supplémentaires sur les pratiques exemplaires en matière de SNF.

Activation des services NFS

Activez les services NFS pour que le client puisse accéder au système à l'aide du protocole NFS.

Procédure

1. Sélectionnez **Protocols** > **NFS**.

   La vue NFS s'ouvre en affichant l'onglet Exports.

2. Cliquez sur **Enable**.

Désactivation des services NFS

Désactivez les services NFS pour empêcher le client d'accéder au système à l'aide du protocole NFS.

Procédure

1. Sélectionnez les onglets **Protocols** > **NFS**.

   La vue NFS s'ouvre en affichant l'onglet Exports.

2. Cliquez sur **Désactiver**.

Création d'une exportation

Vous pouvez utiliser le bouton Create de Data Domain System Manager dans la vue NFS ou l'assistant de configuration pour préciser quels clients NFS peuvent accéder aux zones `/backup`, `/data/col1/backup`,`/ddvar`, `/ddvar/core`, ou à la zone `/ddvar/ext` si elle existe.

Un système Data Domain prend en charge un maximum de 2 048 exportations[2], le nombre de connexions étant mis à l'échelle selon la mémoire système.

Remarque

Vous devez attribuer un accès client à chaque exportation séparément et supprimer l'accès à partir de chaque exportation séparément. Par exemple, il est possible de supprimer un client du répertoire `/ddvar` et de maintenir son accès à `/data/col1/backup`.

⚠ ATTENTION

Lorsque la réplication doit être implémentée, un système Data Domain unique peut recevoir des sauvegardes de clients CIFS et de clients NFS, à condition d'utiliser des répertoires ou MTrees distincts pour chacun. Ne mélangez pas les données CIFS et NFS dans la même zone.

Procédure

1. Sélectionnez **Protocols > NFS**.

   La vue NFS s'ouvre, affichant l'onglet Exports.

2. Cliquez sur **Create**.
3. Saisissez le chemin d'accès dans la zone de texte Directory Path (par exemple, `/data/col1/backup/dir1`).

   Remarque

   `col1` utilise la lettre L minuscule suivie du numéro 1.

4. Dans la zone Clients, sélectionnez un client existant ou cliquez sur l'icône **+** pour en créer un.

   La boîte de dialogue Client s'affiche.

   a. Saisissez un nom de serveur dans la zone de texte.

   Saisissez des noms de domaine complets, des noms d'hôte ou des adresses IP. L'utilisation du caractère générique astérisque (*) indique que tous les serveurs de sauvegarde peuvent être utilisés comme clients.

   Remarque

   Les clients autorisés à accéder au répertoire `/data/col1/backup` ont accès à l'ensemble de ce répertoire. Un client ayant accès à un sous-répertoire de `/data/col1/backup` ne peut accéder qu'à ce sous-répertoire.

   - Un client peut être un nom d'hôte complet, une adresse IP de type IPv4 ou IPv6, une adresse IPv4 avec un masque de réseau ou une longueur de préfixe, une adresse IPv6 avec longueur de préfixe, un nom de groupe réseau NIS précédé du préfixe `@` ou le caractère générique astérisque (`*`) avec un nom de domaine, tel que `*.votreentreprise.com`.
   - Un client ajouté à un sous-répertoire de `/data/col1/backup` n'a accès qu'à ce sous-répertoire.

2. Peut être affecté par les limitations matérielles.

- Saisissez un astérisque (*) comme liste de clients pour accorder l'accès à tous les clients du réseau.

b. Cochez les cases des options NFS appropriées pour le client.

Général :

- Read-only permission (ro).
- Allow connections from ports below 1024 (secure) (default).

UID/GID anonyme :

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (root _squash).
- Map all user requests to the anonymous UID/GID (all _squash).
- Use Default Anonymous UID/GID.

Modes d'authentification Kerberos autorisés :

- Unauthenticated connections (sec=sys). Sélectionnez cette option pour ne pas utiliser l'authentification.
- Authenticated Connections (sec=krb5).

Remarque

L'intégrité et la confidentialité sont prises en charge, bien qu'elles puissent considérablement ralentir les performances.

c. Cliquez sur **OK**.

5. Cliquez sur **OK** pour créer l'exportation.

Modification d'une exportation

Modifiez le chemin du répertoire, le nom de domaine et d'autres options à l'aide de l'interface utilisateur.

Procédure

1. Sélectionnez **Protocols** > **NFS**.

   La vue NFS s'ouvre en affichant l'onglet Exports.

2. Cochez la case correspondant à une exportation dans le tableau des exportations NFS.
3. Cliquez sur **Modify**.
4. Modifiez le chemin d'accès dans la zone de texte Directory Path.
5. Dans la zone Clients, sélectionnez un autre client et cliquez sur l'icône du crayon (modifier) ou cliquez sur l'icône **+** pour créer un client.

   a. Saisissez un nom de serveur dans la zone de texte Client.

   Saisissez des noms de domaine complets, des noms d'hôte ou des adresses IP. L'utilisation du caractère générique astérisque (*) indique que tous les serveurs de sauvegarde peuvent être utilisés comme clients.

Remarque

Les clients autorisés à accéder au répertoire `/data/col1/backup` ont accès à l'ensemble de ce répertoire. Un client ayant accès à un sous-répertoire de `/data/col1/backup` ne peut accéder qu'à ce sous-répertoire.

- Un client peut être un nom d'hôte de domaine complet, une adresse IPv4 ou IPv6, une adresse IPv4 avec un masque de réseau ou une longueur de préfixe, une adresse IPv6 avec une longueur du préfixe, un nom de groupe réseau NIS avec le préfixe `@`, ou un astérisque (`*`) avec un nom de domaine, tel que `*.yourcompany.com`.
  Un client ajouté à un sous-répertoire de `/data/col1/backup` n'a accès qu'à ce sous-répertoire.
- Saisissez un astérisque (`*`) comme liste de clients pour accorder l'accès à tous les clients du réseau.

b. Cochez les cases des options NFS appropriées pour le client.

Général :

- Read-only permission (ro).
- Allow connections from ports below 1024 (secure) (default).

UID/GID anonyme :

- Map requests from UID (user identifier) or GID (group identifier) 0 to the anonymous UID/GID (root _squash).
- Map all user requests to the anonymous UID/GID (all _squash).
- Use Default Anonymous UID/GID.

Modes d'authentification Kerberos autorisés :

- Unauthenticated connections (sec=sys). Sélectionnez cette option pour ne pas utiliser l'authentification.
- Authenticated Connections (sec=krb5).

Remarque

Les options Integrity et Privacy ne sont pas prises en charge.

c. Cliquez sur **OK**.

6. Cliquez sur **OK** pour modifier l'exportation.

Création d'une exportation à partir d'une exportation existante

Créez une exportation à partir d'une exportation existante, puis modifiez-la selon les besoins.

Procédure

1. Dans l'onglet NFS Exports, cochez la case en regard de l'exportation à utiliser comme source.
2. Cliquez sur **Create From**.

3. Modifiez les informations d'exportation ainsi que l'explique la section sur la modification d'une exportation.

Suppression d'une exportation

Supprimez une exportation à partir de l'onglet NFS Exports.

Procédure

1. Dans l'onglet NFS Exports, cochez la case de l'exportation que vous souhaitez supprimer.
2. Cliquez sur **Delete**.
3. Cliquez sur **OK**, puis sur **Close** pour supprimer l'exportation.

Affichage d'informations NFS

Les rubriques de cette section indiquent comment utiliser DD System Manager pour surveiller l'état du client NFS et la configuration NFS.

Affichage de l'état NFS

Déterminez si NFS est actif et Kerberos activé.

Procédure

- Cliquez sur **Protocols** > **NFS**.

  Le volet supérieur affiche l'état de fonctionnement du NFS. Il indique, par exemple, si l'option NFS est actuellement active et en fonctionnement, et si le mode Kerberos est activé.

  Remarque

  Cliquez sur Configure pour afficher l'onglet **Administration** > **Access** > **Authentication** dans lequel vous pouvez configurer l'authentification Kerberos.

Affichage des exportations NFS

Affichez la liste des clients autorisés à accéder au système Data Domain.

Procédure

1. Cliquez sur **Protocols** > **NFS**.

   La vue Exports affiche un tableau des exportations NFS qui sont configurées pour le système Data Domain et le chemin de montage, l'état et les options NFS pour chaque exportation.

2. Cliquez sur une exportation dans le tableau pour renseigner la section Detailed Information, en dessous du tableau Exports.

   En plus du chemin d'accès au répertoire d'exportation, des options configurées et de l'état de l'exportation, le système affiche la liste des clients.

   Utilisez la zone de texte Filter By pour trier par chemin de montage.

   Cliquez sur **Update** pour que le système actualise le tableau et utilise les filtres fournis.

Cliquez sur **Reset** pour que le système supprime les filtres Path et Client.

Affichage des clients NFS actifs

Affichez tous les clients connectés au cours des 15 dernières minutes, en indiquant leur chemin de montage.

Procédure

- Sélectionnez l'onglet **Protocols** > **NFS** > **Active Clients**.

  La vue Active Clients s'ouvre et affiche tous les clients qui ont été connectés au cours des 15 dernières minutes, ainsi que le chemin de montage.

  Utilisez les zones de texte Filter By pour trier par chemin de montage et nom de client.

  Cliquez sur **Update** pour que le système actualise le tableau et utilise les filtres fournis.

  Cliquez sur **Reset** pour que le système supprime les filtres Path et Client.

Intégration d'un module DDR dans un domaine Kerberos

Définissez le nom de domaine, le nom d'hôte et le serveur DNS pour le module DDR.

Permettez au module DDR d'utiliser le serveur d'authentification comme un Centre de distribution de clés (pour UNIX) ou comme un Centre de distribution (pour Windows Active Directory).

⚠ ATTENTION

Les exemples fournis dans cette description sont spécifiques du système d'exploitation utilisé tout au long de cet exercice. Vous devez utiliser les commandes spécifiques de votre système d'exploitation.

Remarque

Pour le mode Kerberos UNIX, un fichier keytab doit être transféré du serveur du Centre de distribution de clés (KDC), où elles sont générées, vers le module DDR. Si vous utilisez plusieurs modules DDR, chaque module nécessite un fichier keytab distinct. Le fichier keytab contient le code secret partagé par le serveur KDC et le module DDR.

Remarque

Lorsque vous utilisez un KDC UNIX, le serveur DNS ne doit pas nécessairement être le serveur KDC ; il peut s'agir d'un serveur distinct.

Procédure

1. Définissez le nom d'hôte et le nom de domaine pour le module DDR, à l'aide des commandes DDR.

   ```
   net set hostname <host>
   ```

   ```
   net set {domainname <local-domain-name>}
   ```

Remarque

Le nom d'hôte est le nom du module DDR.

2. Configurez une entité de sécurité NFS (nœud) pour le module DDR du Centre de distribution de clés (KDC).

   Exemple :
   addprinc nfs/hostname@realm

   Remarque

   Le nom d'hôte est le nom du module DDR.

3. Vérifiez qu'il existe des entrées nfs ajoutées en tant qu'entités de sécurité au KDC.

   Exemple :
   listprincs
   ```
   nfs/hostname@realm
   ```

4. Ajoutez l'entité de sécurité DDR à un fichier keytab.

   Exemple :
   ktadd <keytab_file> nfs/hostname@realm

5. Vérifiez qu'il existe un fichier keytab nfs configuré sur le KDC.

   Exemple :
   klist -k <keytab_file>

   Remarque

   Le <keytab_file> correspond au fichier keytab utilisé pour configurer des clés dans une étape précédente.

6. Copiez le fichier keytab depuis l'emplacement dans lequel les clés pour le module DDR NFS sont générées vers le module DDR dans le répertoire /ddvar/.

   Tableau 117 Destination du fichier keytab

Copiez le fichier depuis :	Copiez le fichier vers :
<keytab_file> (le fichier keytab configuré dans une étape précédente.)	/ddvar/

7. Supprimez le realm du module DDR, à l'aide de la commande DDR suivante :

   authentication kerberos set realm <home realm> kdc-type <unix, windows.> kdcs <IP address of server>

8. Lorsque le type de KDC est UNIX, importez le fichier keytab de /ddvar/ vers /ddr/etc/, où l'attend le fichier de configuration Kerberos. Utilisez la commande DDR suivante pour copier le fichier :

   authentification kerberos keytab importation

NOTE

Cette étape est requise uniquement lorsque le type kdc est UNIX.

La configuration de Kerberos est maintenant terminée.

9. Pour ajouter un point de montage NFS afin d'utiliser Kerberos, utilisez la commande nfs add.

   Consultez le *Guide de référence des commandes de Data Domain Operating System* pour plus d'informations.

10. Ajoutez des entités de sécurité pour l'hôte, NFS et les utilisateurs concernés pour chaque client NFS du Centre de distribution de clés (KDC).

    Exemple : **`listprincs`**

    ```
    host/hostname@realm
    nfs/hostname@realm
    root/hostname@realm
    ```

11. Pour chaque client NFS, importez toutes ses entités de sécurité dans un fichier keytab sur le client.

    Exemple :

    `ktadd -k <keytab_file> host/hostname@realm`

    `ktadd -k <keytab_file> nfs/hostname@realm`

Ajout et suppression de serveurs KDC après la configuration initiale

Après avoir intégré un module DDR dans un domaine Kerberos et, par conséquent, avoir permis au module DDR d'utiliser le serveur d'authentification comme un Centre de distribution de clés (pour UNIX) ou un Centre de distribution (pour Windows Active Directory), vous pouvez ajouter ou supprimer des serveurs KDC en procédant comme suit.

Procédure

1. Reliez le module DDR à un serveur Windows Active Directory (AD) ou à un Centre de distribution de clés (KDC) UNIX.

   `authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}`

   Exemple : **`authentication kerberos set realm krb5.test kdc-type unix kdcs nfskrb-kdc.krb5.test`**

   Cette commande permet de relier le système au realm krb5.test et active l'authentification Kerberos pour les clients NFS.

   Remarque

   Un fichier keytab généré sur ce KDC doit exister sur le module DDR pour effectuer une authentification à l'aide de Kerberos.

2. Vérifiez la configuration de l'authentification Kerberos.

   `authentication kerberos show config`

```
Home Realm:           krb5.test
KDC List:             nfskrb-kdc.krb5.test
KDC Type:             unix
```

3. Ajoutez un second serveur KDC.

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   Exemple : **authentication kerberos set realm krb5.test kdc-type unix kdcs ostqa-sparc2.krb5.test nfskrb-kdc.krb5.test**

   Remarque

   Un fichier keytab généré sur ce KDC doit exister sur le module DDR pour effectuer une authentification à l'aide de Kerberos.

4. Vérifiez que deux serveurs KDC ont été ajoutés.

   authentication kerberos show config

```
Home Realm:           krb5.test
KDC List:             ostqa-sparc2.krb5.test, nfskrb-
kdc.krb5.test
KDC Type:             unix
```

5. Affichez la valeur de la clé de configuration Kerberos.

   reg show config.keberos

```
config.kerberos.home_realm = krb5.test
config.kerberos.home_realm.kdc1 = ostqa-sparc2.krb5.test
config.kerberos.home_realm.kdc2 = nfskrb-kdc.krb5.test
config.kerberos.kdc_count = 2
config.kerberos.kdc_type = unix
```

6. Supprimez un serveur KDC.

   Vous pouvez supprimer un serveur KDC à l'aide de la commande **authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}** sans lister le serveur KDC que vous souhaitez supprimer. Par exemple, si les serveurs KDC existants sont nommés kdc1, kdc2 et kdc3 et que vous souhaitez supprimer le serveur kdc2 du realm, vous pouvez utiliser l'exemple suivant :

   authentication kerberos set realm <realm-name> kdc-type <kdc_type> kdcs kdc1,kdc3

CHAPITRE 10

NFSv4

Ce chapitre traite des sujets suivants :

Présentation de la fonction NFSv4

Puisque les clients NFS utilisent de plus NFSv4.x comme niveau de protocole NFS par défaut, les systèmes Data Domain peuvent maintenant utiliser NFSv4 au lieu de demander au client de travailler dans un mode de compatibilité en amont.

Dans les systèmes Data Domain, les clients peuvent travailler dans des environnements mixtes dans lesquels NFSv4 et NFSv3 doivent être en mesure d'accéder aux mêmes exportations NFS.

Le serveur NFS Data Domain peut être configuré pour prendre en charge NFSv4 et NFSv3, selon les exigences du site. Vous pouvez rendre chaque exportation NFS disponible pour les clients NFSv4 uniquement, les clients NFSv3 uniquement ou les deux.

Plusieurs facteurs peuvent affecter le choix entre NFSv4 ou NFSv3 :

- Client NFS pris en charge
  Certains clients NFS peuvent prendre en charge NFSv3 ou NFSv4 seulement, ou peuvent mieux fonctionner avec une version qu'avec l'autre.
- Exigences opérationnelles
  Une entreprise peut être strictement obligée d'utiliser NFSv4 ou NFSv3.
- Sécurité
  Si vous avez besoin d'une plus grande sécurité, NFSv4 offre un niveau de sécurité supérieur à NFSv3, y compris pour les listes de contrôle d'accès et la configuration étendue des propriétaires et des groupes.
- Exigences de fonctions
  Si vous avez besoin de fichiers UTF-8 ou du verrouillage de plage d'octets, vous devez choisir NFSv4.
- Sous-montages NFSv3
  Si votre configuration existante utilise des sous-montages NFSv3, NFSv3 est probablement le choix approprié.

Comparaison de NFSv4 à NFSv3 sur des systèmes Data Domain

NFSv4 fournit des fonctionnalités améliorées par rapport à NFSv3.

Le tableau suivant compare les fonctionnalités NFSv3 à celles de NFSv4.

Tableau 118 NFSv4 comparé à NFSv3

Fonction	NFSv3	NFSv4
Système de fichiers réseau basé sur des standards	Oui	Oui
Prise en charge de Kerberos	Oui	Oui
Kerberos avec LDAP	Oui	Oui
Rapports sur les quotas	Oui	Oui
Plusieurs exportations avec les listes d'accès basées sur le client	Oui	Oui
Mappage des ID	Oui	Oui
Prise en charge des caractères UTF-8	Non	Oui

Tableau 118 NFSv4 comparé à NFSv3 (suite)

Fonction	NFSv3	NFSv4
Listes ACL basées sur des fichiers/répertoires	Non	Oui
Propriétaire/groupe étendu (OWNER@)	Non	Oui
Blocage du partage de fichiers	Non	Oui
Verrouillage de la page d'octets	Non	Oui
Intégration de DD-CIFS (verrouillage, ACL, AD)	Non	Oui
Ouverture et récupération des fichiers à états	Non	Oui
PseudoFS et espace de nommage global	Non	Oui
Espace de nommage multisystème utilisant des références	Non	Oui

Ports NFSv4

Vous pouvez activer ou désactiver NFSv4 et NFSv3 indépendamment. En outre, vous pouvez déplacer les versions de NFS sur différents ports ; les deux versions n'ont pas besoin d'occuper le même port.

Avec NFSv4, vous n'avez pas besoin de redémarrer le système de fichiers Data Domain, si vous modifiez les ports. Seul un redémarrage NFS est nécessaire dans de tels cas.

Comme NFSv3, NFSv4 fonctionne sur le port 2049 par défaut s'il est activé.

NFSv4 n'utilise pas portmapper (port 111) ou mountd (port 2052).

Tour d'horizon du mappage des identifiants

NFSv4 identifie les propriétaires et les groupes avec un format uniformisé externe, tels que `joe@example.com`. Ces formats courants sont appelés identifiants ou ID.

Les identifiants sont stockés dans un serveur NFS et utilisent des représentations internes telles que le code ID 12345 ou ID S-123-33-667-2. La conversion entre les identifiants internes et externes est appelée mappage d'ID.

Les identifiants sont associés à ce qui suit :

- Propriétaires des fichiers et des répertoires
- Groupes propriétaires des fichiers et des répertoires
- Entrées dans les listes de contrôle d'accès (ACL)

Les systèmes Data Domain utilisent un format interne commun pour les protocoles NFS et CIFS/SMB, ce qui permet de partager les fichiers et répertoires entre NFS et CIFS/SMB. Chaque protocole convertit le format interne vers son propre format externe avec son propre mappage d'ID.

Formats externes

Le format externe pour les identifiants NFSv4 suit les normes NFSv4 (par exemple, RFC-7530 pour NFSv4.0). En outre, des formats supplémentaires sont pris en charge pour l'interopérabilité.

Formats standard d'identifiant

Les identifiants externes standards pour NFSv4 ont le format *identifier@domain*. Cet identifiant est utilisé pour les propriétaires, les groupes propriétaires et les entrées de contrôle d'accès (ACE) NFSv4. Le domaine doit correspondre au domaine NFSv4 configuré qui a été défini à l'aide de la commande `nfs option`.

L'exemple suivant de la CLI définit le domaine NFSv4 sur `mycorp.com` pour le serveur NFS Data Domain :

```
nfs option set nfs4-domain mycorp.com
```

Consultez la documentation spécifique au client que vous avez pour définir le domaine NFS client. Selon le système d'exploitation, vous devrez peut-être mettre à jour un fichier de configuration (par exemple, `/etc/idmapd.conf`) ou utiliser un outil d'administration client.

Remarque

Si vous ne définissez pas la valeur par défaut, le système d'exploitation utilisera le nom DNS pour le système Data Domain.

Remarque

Le système de fichiers doit être redémarré après avoir changé le domaine DNS de sorte que le domaine nfs4 soit automatiquement mis à jour.

Identifiants étendus des entrées de contrôle d'accès (ACE)

Pour les entrées ACE des listes de contrôle d'accès, les serveurs NFS Data Domain prennent également en charge les identifiants étendus des entrées de contrôle d'accès (ACE) NFSv4 standard définis par la norme RFC NFSv4 :

- OWNER@, propriétaire du fichier ou du répertoire.
- GROUP@, groupe propriétaire en cours du fichier ou du répertoire.
- Les identifiants spéciaux INTERACTIVE@, NETWORK@, DIALUP@, BATCH@, ANONYMOUS@, AUTHENTICATED@, SERVICE@.

Autres formats

Pour permettre l'interopérabilité, les serveurs NFSv4 sur les systèmes Data Domain prennent en charge certains autres formats d'identifiant pour les entrées et les sorties.

- Identifiants numériques ; par exemple, « 12345 ».
- Identifiants de sécurité (SID) compatibles Windows exprimés avec « S-NNN-NNN-... »

Voir les sections sur le mappage en entrée et en sortie pour plus d'informations sur les restrictions qui concernent ces formats.

Formats d'identifiant internes

Le système de fichiers Data Domain stocke les identificateurs avec chaque objet (fichier ou répertoire) dans le système de fichiers. Tous les objets ont un ID utilisateur numérique (UID) et un ID de groupe (GID). Ces derniers, ainsi qu'un ensemble de bits

de mode, permettent une identification et des contrôles d'accès UNIX/Linux traditionnels.

Les objets créés par le protocole CIFS/SMB, ou par le protocole NFSv4 lorsque les listes de contrôle d'accès NFSv4 sont activées, ont également un descripteur de sécurité (SD) étendu. Chaque SD contient les éléments suivants :

- Un identifiant de sécurité du propriétaire (SID)
- Un identifiant SID du groupe propriétaire
- Une liste de contrôle d'accès discrétionnaire (DACL)
- (Facultatif) Une liste de contrôle d'accès système (SACL)

Chaque identifiant SID contient un ID relatif (RID) et un domaine distinct de manière similaire aux identifiants SID Windows. Consultez la section relative à l'interopérabilité NFSv4 et CIFS pour plus d'informations sur les identifiants SID et le mappage des identifiants SID.

Lorsque le mappage d'identifiant se produit

Le serveur Data Domain NFSv4 effectue le mappage dans les circonstances suivantes :

- Mappage en entrée
  Le serveur Data Domain NFS reçoit l'identifiant d'un client NFSv4. Reportez-vous à la section Mappage en entrée à la page 299.
- Mappage en sortie
  Un identifiant est envoyé au client NFSv4 par le serveur Data Domain NFS. Reportez-vous à la section Mappage en sortie à la page 300.
- Mappage d'informations d'identification
  Les informations d'identification du client RPC sont mappées à une identité interne pour le contrôle d'accès et d'autres opérations. Reportez-vous à la section Mappage d'informations d'identification à la page 300.

Mappage en entrée

Le mappage en entrée se produit lorsqu'un client NFSv4 envoie un identifiant sur le serveur Data Domain NFSv4, lors de la configuration du propriétaire ou groupe propriétaire d'un fichier, par exemple. Le mappage en entrée diffère du mappage des informations d'identification. Pour plus d'informations sur le mappage des informations d'identification, consultez xxxx

Les identifiants de format standard tels que `joe@mycorp.com` sont convertis en un UID/GID interne selon les règles de conversion configurées. Si les listes de contrôle d'accès NFSv4 sont activées, un identifiant SID sera également généré, selon les règles de conversion configurées.

Les identifiants numériques (par exemple, « 12345 ») sont directement convertis en un UID/GID correspondant, si le client n'utilise pas l'authentification Kerberos. Si Kerberos est utilisé, une erreur sera générée tel que recommandé par la norme NFSv4. Si les listes de contrôle d'accès NFSv4 sont activées, un identifiant SID sera également généré, selon les règles de conversion.

Les identifiants SID Windows (par exemple, « S-NNN-NNN-... ») sont validés et directement convertis en identifiants SID correspondants. Un UID/GID sera généré selon les règles de conversion.

Mappage en sortie

Le mappage en sortie se produit lorsqu'un serveur NFSv4 envoie un identifiant au client NFSv4, par exemple, si le serveur renvoie le propriétaire ou le groupe propriétaire d'un fichier.

1. Si cela est configuré, la sortie peut être l'ID numérique.
   Cela peut être utile pour les clients NFSv4 qui ne sont pas configurés pour le mappage d'ID (par exemple, certains clients Linux).
2. Le mappage est tenté en utilisant les services de mappage configurés, (par exemple, NIS ou Active Directory).
3. La sortie est une chaîne d'ID numérique ou d'identifiant SID, si le mappage échoue et que la configuration est autorisée.
4. Sinon, « nobody » est renvoyé.

La commande **nfs option *nfs4-idmap-out-numeric*** configure le mappage sur la sortie :

- Si la commande **nfs option *nfs4-idmap-out-numeric*** est définie sur la valeur **map-first**, le mappage sera tenté. En cas d'erreur, une chaîne numérique est sortie si cela est autorisé. Il s'agit de l'option par défaut.
- Si la commande **nfs option *nfs4-idmap-out-numeric*** est définie sur la valeur **always**, la sortie sera toujours une chaîne numérique si autorisé..
- Si la commande **nfs option *nfs4-idmap-out-numeric*** est définie sur la valeur **never**, le mappage sera tenté. En cas d'erreur, **nobody@nfs4-domain** est la sortie. Si la connexion RPC utilise ESG/Kerberos, une chaîne numérique n'est jamais autorisée et **nobody@nfs4-domain** est la sortie.

L'exemple suivant configure le serveur NFS Data Domain de sorte qu'il attende toujours d'obtenir une chaîne numérique sur la sortie. Pour Kerberos, le nom « nobody » est retourné :

```
nfs option set nfs4-idmap-out-numeric always
```

Mappage d'informations d'identification

Le serveur NFSv4 fournit des informations d'identification pour le client NFSv4.

Ces informations d'identification effectuent les fonctions suivantes :

- Déterminer la politique d'accès pour l'opération, par exemple, la capacité de lire un fichier.
- Déterminer le propriétaire par défaut et le groupe propriétaire pour les nouveaux fichiers et répertoires.

Les informations d'identification envoyées par le client peuvent être `john_doe@mycorp.com`, ou des informations d'identification système telles que `UID=1000, GID=2000`. Les informations d'identification système spécifient un UID/GID avec les ID de groupe auxiliaires.

Si vous avez désactivé les listes de contrôle d'accès NFSv4, l'UID/GID et les ID de groupe auxiliaires sont utilisés pour les informations d'identification.

Si les listes de contrôle d'accès NFSv4 sont activées, les services de mappage configurés sont utilisés pour créer un descripteur de sécurité étendu pour les informations d'identification :

- Les identifiants SID pour le propriétaire, le groupe propriétaire et le groupe auxiliaire mappés et ajoutés au descripteur de sécurité (SD).
- Les privilèges d'informations d'identification sont ajoutés au descripteur de sécurité le cas échéant.

Interopérabilité de NFSv4 et CIFS/SMB

Les descripteurs de sécurité utilisés par NFSv4 et CIFS sont similaires du point de vue du mappage des identifiants, bien qu'il existe des différences.

Vous devez être conscient de ce qui suit afin d'assurer une interopérabilité optimale :

- Active Directory doit être configuré pour CIFS et NFSv4, et le mappeur d'identifiants NFS doit être configuré de sorte qu'il utilise Active Directory pour le mappage des identifiants.
- Si vous utilisez intensivement des listes de contrôle d'accès CIFS, vous pouvez généralement améliorer la compatibilité en activant aussi les listes de contrôle d'accès NFSv4.
  - L'activation des listes de contrôle d'accès NFSv4 permet de mapper les informations d'identification NFSv4 sur l'identifiant de sécurité approprié lors de l'évaluation de l'accès à la liste DACL.
- Le serveur CIFS reçoit des informations d'identification du client CIFS, y compris les privilèges utilisateur et ceux de la liste de contrôle d'accès par défaut.
  - En revanche, le serveur NFSv4 reçoit un ensemble plus limité d'informations d'identification et crée des informations d'identification lors de l'exécution à l'aide de son outil de mappage d'identifiants. Voilà pourquoi, le système de fichiers peut voir différentes informations d'identification.

Intégration à Active Directory avec CIFS/SMB

Le serveur NFSv4 Data Domain peut être configuré pour utiliser la configuration de Windows Active Directory qui est définie avec le serveur CIFS Data Domain.

Le système Data Domain est mappé pour utiliser Active Directory si possible. Cette fonctionnalité est désactivée par défaut, mais vous pouvez l'activer à l'aide de la commande suivante :

```
nfs option set nfs4-idmap-active-directory enabled
```

DACL par défaut pour NFSv4

NFSv4 définit une autre DACL (liste de contrôle d'accès discrétionnaire) par défaut que celle fournie par défaut par CIFS.

Seuls les identifiants OWNER@, GROUP@ and EVERYONE@ sont définis dans la DACL NFSv4 par défaut. Vous pouvez utiliser la liste de contrôle d'accès héritée pour ajouter automatiquement des entrées de contrôle d'accès (ACE) importantes pour CIFS par défaut, le cas échéant.

Identifiants SID par défaut du système

Les fichiers et répertoires créés par NFSv3 et NFSv4 sans listes de contrôle d'accès, utilisent le domaine par défaut du système, qui est parfois appelé domaine UNIX par défaut :

- Les identifiants SID utilisateur du domaine système ont le format `S-1-22-1-N`, où N est l'UID.
- Les identifiants SID de groupe du domaine système ont le format `S-1-22-2-N`, où N est le GID.
  Par exemple, un utilisateur avec `UID 1234` aura l'identifiant SID de propriétaire `S-1-22-1-1234`.

Identifiants communs dans les listes de contrôle d'accès NFSv4 et les identifiants SID

L'identifiant EVERYONE@ et les autres identifiants spéciaux (tels que BATCH@, par exemple) dans des listes de contrôle d'accès NFSv4 utilisent des identifiants de sécurité CIFS équivalents et sont compatibles.

Les identifiants OWNER@ et GROUP@ n'ont aucune correspondance directe dans CIFS ; ils apparaissent comme le propriétaire en cours et le groupe propriétaire en cours du fichier ou du répertoire.

Références NFS

La fonctionnalité de références permet à un client NFSv4 d'accéder à une exportation (ou à un système de fichiers) dans un ou plusieurs emplacements. Les emplacements peuvent se trouver sur le même serveur NFS ou sur des serveurs NFS différents et utiliser un chemin d'accès identique ou différent pour atteindre l'exportation.

Puisque les références sont une fonctionnalité de NFSv4, elles s'appliquent uniquement aux montages NFSv4.

Les références peuvent être envoyées à n'importe quel serveur qui utilise NFSv4 ou une version ultérieure, y compris aux appareils suivants :

- Un système Data Domain exécutant NFS avec NFSv4 activé
- Les autres serveurs prenant en charge NFSv4, y compris les serveurs Linux, les appliances NAS et les systèmes VNX.

Une référence peut utiliser un point d'exportation NFS avec ou sans un chemin d'accès sous-jacent en cours dans le système de fichiers Data Domain.

Les exportations NFS avec références peuvent être montées par le biais de NFSv3, mais les clients NFSv3 ne seront pas redirigés puisque les références sont une fonctionnalité de NFSv4. Cette caractéristique est utile dans les systèmes scale-out pour permettre la redirection des exportations à un niveau de gestion de fichiers.

Emplacements de référence

Les références NFSv4 ont toujours un ou plusieurs emplacements.

Ces emplacements contiennent les éléments suivants :

- Un chemin d'accès sur un serveur NFS distant pour le système de fichiers visé.
- Une ou plusieurs adresses réseau serveur qui permettent au client d'atteindre le serveur NFS distant.

En général, quand plusieurs adresses serveur sont associées au même emplacement, ces adresses se trouvent sur le même serveur NFS.

Noms des emplacements de référence

Vous pouvez nommer chaque emplacement de référence d'une exportation NFS. Vous pouvez utiliser le nom pour accéder à la référence et pour la modifier ou la supprimer.

Un nom de référence peut contenir au maximum 80 caractères compris dans les jeux de caractères suivants :

- a-z
- A-Z
- 0-9
- "."
- ","
- "_"
- "-"

Remarque

Vous pouvez inclure des espaces tant que ces espaces sont incorporés dans le nom. Si vous utilisez des espaces incorporés, vous devez mettre le nom entier entre des guillemets doubles.

Les noms qui commencent par «. » sont réservés pour la création automatique par le système Data Domain. Vous pouvez supprimer ces noms, mais vous ne pouvez pas les créer ou les modifier à l'aide de l'interface de ligne de commande (CLI) ou les services de gestion système (SMS).

Références et systèmes scale-out

Les références et emplacements NFSv4 peuvent permettre un meilleur accès si vous mettez à l'échelle vos systèmes Data Domain

Puisque votre système Data Domain peut ou non déjà contenir un espace de nommage global, les deux scénarios suivants décrivent comment vous pouvez utiliser les références NFSv4 :

- Votre système Data Domain ne contient pas un espace de nommage global.
  - Vous pouvez utiliser des références NFSv4 pour créer cet espace de nommage global. Les administrateurs système peuvent créer ces espaces de nommage globaux ou vous pouvez utiliser un élément de gestionnaire système (SM) intelligent pour créer des références si besoin.
- Votre système Data Domain possède déjà un espace de nommage global.
  - Si votre système possède un espace de nommage global avec des structures MTree placées dans des nœuds spécifiques, les références NFS peuvent être créées pour rediriger l'accès vers ces structures MTree sur les nœuds ajoutés dans le système mis à l'échelle. Vous pouvez créer ces références ou les exécuter automatiquement dans NFS si les informations nécessaires du gestionnaire de fichiers (FM) ou du gestionnaire système sont disponibles. Pour plus d'informations sur les structures MTree, consultez le *Guide d'administration de Data Domain Operating System.*

NFSv4 et haute disponibilité

Avec NFSv4, les exportations de protocole (par exemple, `/data/col1/<mtree>`) se retrouvent dans une configuration haute disponibilité. Toutefois, les exportations de configuration telles que `/ddvar` ne sont pas inversées.

Le système de fichiers `/ddvar` est unique à chaque nœud d'une paire HA. Ainsi, les exportations `/ddvar` et leurs listes d'accès client associées ne sont pas mises en miroir sur le nœud en veille dans un environnement HA.

Les informations contenues dans `/ddvar` deviennent périmées lorsque le nœud actif bascule sur le nœud en veille. Toutes les autorisations client accordées à `/ddvar` sur le nœud actif d'origine doivent être recréées sur le nœud actif récemment créé après un basculement.

Vous devez également ajouter des exportations /ddvar supplémentaires et leurs clients (par exemple, `/ddvar/core`) qui ont été créés sur le nœud actif d'origine sur le nœud actif récemment créé après un basculement.

Enfin, toutes les exportations `/ddvar` souhaitées doivent être démontées à partir du client, puis remontées après un basculement.

Espaces de nommage globaux NFSv4

Le serveur NFSv4 fournit une arborescence de répertoires virtuels, appelée PseudoFS qui vous permet de vous connecter à des exportations NFS dans un ensemble consultable de chemins d'accès.

L'utilisation d'un PseudoFS distingue NFSv4 de NFSv3, qui utilise le protocole auxiliaire MOUNTD.

Dans la plupart des configurations, le passage de MOUNTD NFSv3 à un espace de nommage global NFSv4 est transparent et automatiquement géré par le client et le serveur NFSv4.

Espaces de nommage globaux NFSv4 et sous-montages NFSv3

Si vous utilisez des sous-montages d'exportation NFSv3, les espaces de nommage globaux caractéristiques de NFSv4 risquent d'empêcher les sous-montages d'être vus sur le montage NFSv4.

Exemple 1 Principales exportations et exportations de sous-montage NFSv3

Si NFSv3 a une exportation principale et une exportation de sous-montage, ces exportations risquent d'utiliser les mêmes clients NFSv3 tout en ayant des niveaux d'accès différents :

Tableau 119 Principales exportations et exportations de sous-montage NFSv3

Exportation	Chemin	Client	Options
Mt1	`/data/col1/mt1`	client1.example.com	ro
Sub-Mt1	`/data/col1/mt1/subdir`	client1.example.com	rw

Exemple 1 Principales exportations et exportations de sous-montage NFSv3 (suite)

Dans le tableau précédent, ce qui suit s'applique à NFSv3 :

- Si client1.example.com monte /data/col1/mt1, le client obtient un accès en lecture seule.
- Si client1.example.com monte /data/col1/mt1, le client obtient un accès en lecture/écriture.

NFSv4 opère de la même manière en ce qui concerne les chemins d'exportation du plus haut niveau. Pour NFSv4, client1.example.com parcourt le PseudoFS NFSv4 jusqu'à ce qu'il atteigne le chemin d'exportation du plus haut niveau, `/data/col1/mt1`, où il obtient l'accès en lecture seule.

Cependant, puisque l'exportation a été sélectionnée, l'exportation du sous-montage (Mt1-sub) ne fait pas partie du PseudoFS pour le client et l'accès en lecture-écriture n'est pas autorisé.

Bonne pratique
Si votre système utilise des sous-montages d'exportation NFSv3 pour donner au client un accès en lecture/écriture basé sur le chemin du montage, vous devez considérer ceci avant d'utiliser NFSv4 avec ces exportations de sous-montage.

Avec NFSv4, chaque client dispose d'un PseudoFS individuel.

Tableau 120 Exportations de sous-montage NFSv3

Exportation	Chemin	Client	Options
Mt1	`/data/col1/mt1`	client1.example.com	ro
Sub-Mt1	`/data/col1/mt1/subdir`	client2.example.com	rw

Configuration NFSv4

La configuration par défaut du système Data Domain autorise uniquement NFSv3. Pour pouvoir utiliser NFSv4, vous devez d'abord activer le serveur NFSv4.

Activation du serveur NFSv4

Procédure

1. Saisissez `nfs enable version 4` pour activer NFSv4 :

```
# nfs enable version 4
NFS server version(s) 3:4 enabled.
```

2. (Facultatif) Si vous souhaitez désactiver NFSv3, saisissez `nfs disable version 3`.

```
# nfs disable version 3
NFS server version(s) 3 disabled.
NFS server version(s) 4 enabled.
```

À effectuer

Une fois le serveur NFSv4 activé, vous devrez peut-être effectuer des tâches de configuration NFS supplémentaires spécialement pour votre site. Ces tâches peuvent notamment inclure l'exécution des actions suivantes sur le système Data Domain :

- Définir le domaine NFSv4
- Configurer le mappage ID NFSv4
- Configurer des listes de contrôle d'accès

Configuration du serveur par défaut pour inclure NFSv4

L'option **`default-server-version`** de la commande NFS Data Domain contrôle la version NFS qui est activée lorsque vous saisissez la commande `nfs enable` sans spécifier une version.

Procédure

1. Saisissez la commande `nfs option set default-server-version 3:4` :

```
# nfs option set default-server-version 3:4
NFS option 'default-server-version' set to '3:4'.
```

Mise à jour des exportations existantes

Vous pouvez mettre à jour les exportations existantes pour modifier la version NFS utilisée par votre système Data Domain.

Procédure

1. Saisissez la commande `nfs export modify all` :

```
# nfs export modify all clients all options version=numéro de version
```

Pour vous assurer que tous les clients ont bien la version 3 ou 4 ou les deux, vous pouvez modifier la version NFS dans la chaîne appropriée. L'exemple suivant montre comment modifier NFS pour inclure les versions 3 et 4 :

```
#nfs export modify all clients all options version=3:4
```

Reportez-vous au *Guide de référence des commandes de Data Domain Operating System* pour plus d'informations au sujet de la commande `nfs export`.

Kerberos et NFSv4

NFSv4 et NFSv3 utilisent le mécanisme d'authentification Kerberos pour sécuriser les informations d'identification utilisateur.

Kerberos empêche les informations d'identification utilisateur d'être usurpées dans des paquets NFS et les protège contre toute manipulation non autorisée en cours de route vers le système Data Domain.

Il existe des types distincts d'authentification Kerberos via NFS :

- Kerberos 5 (**`sec=krb5`**)
  Utilisez Kerberos pour les informations d'identification utilisateur.
- Kerberos 5 avec intégrité (**`sec=krb5i`**)

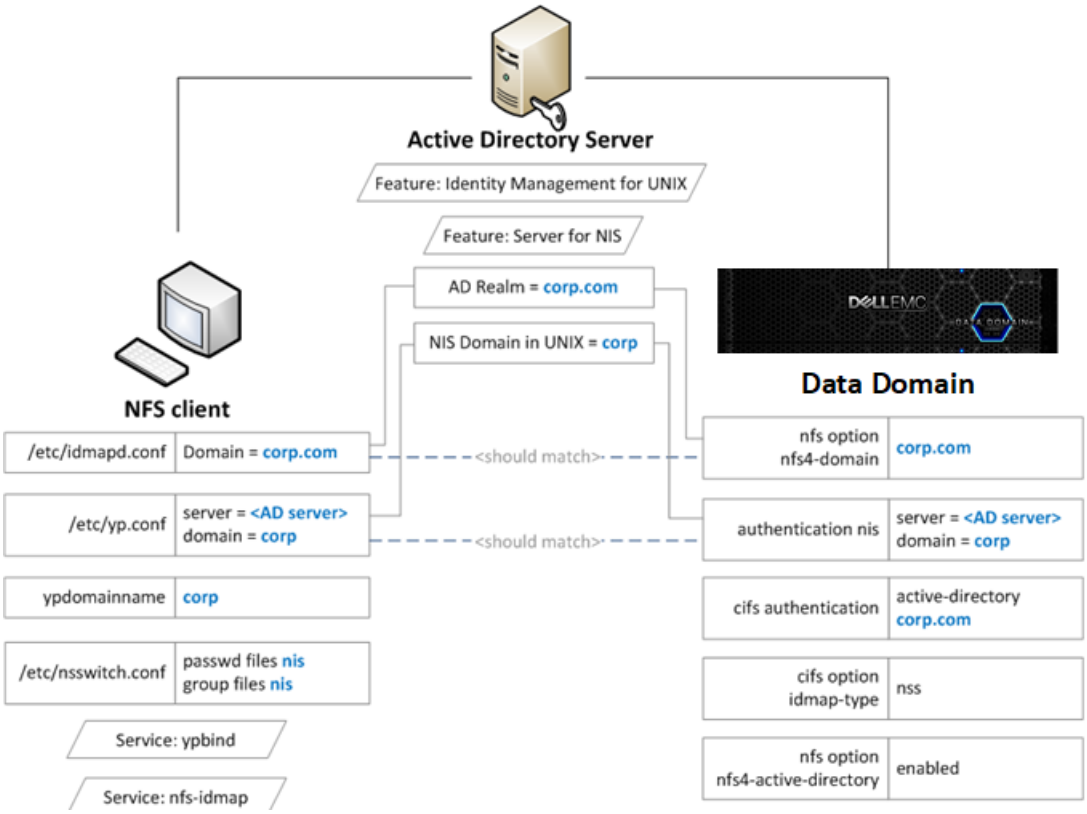
Utilisez le protocole Kerberos et vérifiez l'intégrité de la charge utile NFS à l'aide d'une somme de contrôle chiffrée.

- Kerberos 5 avec sécurité (`sec=krb5p`)
  Utilisez Kerberos 5 avec intégrité et chiffrez la totalité de la charge utile NFS.

Remarque

`krb5i` et `krb5p` peuvent tous deux causer une dégradation des performances en raison de la charge de calcul supplémentaire sur le client NFS et le système Data Domain.

Figure 9 Configuration Active Directory



Vous vous servez des commandes existantes utilisées pour NFSv3 lorsque vous configurez votre système pour Kerberos. Voir le chapitre nfsv3 du *Guide de référence des commandes Data Domain* pour plus d'informations.

Configuration de Kerberos avec un KDC basé sur Linux

Avant de commencer

Vous devez vous assurer que tous vos systèmes peuvent accéder au Centre de distribution des clés (KDC).

Si les systèmes ne peuvent pas atteindre le KDC, vérifiez les paramètres DNS.

Les étapes suivantes vous permettent de créer des fichiers keytab pour le client et le système Data Domain :

- Dans les étapes 1 à 3, vous créez le fichier keytab pour le système Data Domain.
- Dans les étapes 4 et 5, vous créez le fichier keytab pour le client.

Procédure

1. Créez l'entité de sécurité du service **nfs/<ddr_dns_name>@<realm>**.

   ```
   kadmin.local: addprinc -randkey nfs/ddr12345.<domain-
   name>@<domain-name>
   ```

2. Exportez **nfs/<ddr_dns_name>@<realm>** vers un fichier keytab.

   ```
   kadmin.local: ktadd -k /tmp/ddr.keytab nfs/
   ddr12345.corp.com@CORP.COM
   ```

3. Copiez le fichier keytab dans le système Data Domain situé à l'emplacement suivant :

   ```
   /ddr/var/krb5.keytab
   ```

4. Créez l'une des entités de sécurité suivantes pour le client et exportez-le vers le fichier keytab :

   ```
   nfs/<client_dns_name>@<REALM>
   root/<client_dns_name>@<REALM>
   ```

5. Copiez le fichier keytab dans le client à l'emplacement suivant :

   ```
   /etc/krb5.keytab
   ```

Remarque

Nous vous recommandons d'utiliser un serveur NTP pour garder le temps synchronisé sur toutes les entités.

Configuration du système Data Domain pour utiliser l'authentification Kerberos

Procédure

1. Configurez le realm KDC et Kerberos sur le système Data Domain en utilisant la commande `authentication` :

   ```
   # authentication kerberos set realm <realm> kdc-type unix kdcs
   <serveur kdc>
   ```

2. Importez le fichier keytab :

   ```
   # authentication kerberos keytab import
   ```

3. (Facultatif) Configurez le serveur NIS en entrant les commandes suivantes :

   ```
   # authentication nis servers add <serveur>
   # authentication nis domain set <nom de domaine>
   # authentication nis enable
   # filesys restart
   ```

4. (Facultatif) Rendez le **domaine nfs4** identique au realm Kerberos à l'aide de la commande `nfs option` :

   ```
   nfs option set nfs4-domain <realm Kerberos>
   ```

5. Ajoutez un client à une exportation existante en ajoutant **sec=krb5** à la commande `nfs export add` :

```
nfs export add <nom de l'exportation> clients * options
version=4,sec=krb5
```

Configuration des clients

Procédure

1. Configurez le serveur DNS et vérifiez que les recherches directes et inversées fonctionnent.
2. Configurez le realm Kerberos et KDC en modifiant le fichier de configuration `/etc/krb5.conf`.

   Vous devrez peut-être exécuter cette étape en respectant la procédure prévue pour le système d'exploitation client que vous utilisez.
3. Configurez NIS ou un autre service externe de mappage de noms.
4. (Facultatif) Modifiez le fichier `/etc/idmapd.conf` pour vous assurer qu'il est identique à celui du realm Kerberos.

   Vous devrez peut-être exécuter cette étape en respectant la procédure prévue pour le système d'exploitation client que vous utilisez.
5. Vérifiez que le fichier keytab **/etc/krb5.keytab** contient une entrée pour l'entité de sécurité du service **nfs /** ou l'entité de sécurité **root/**.

```
[root@fc22 ~]# klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
--------------------------------------------------------------------
----------
3 nfs/fc22.domain-name@domain-name
```

6. Montez l'exportation à l'aide de l'option **sec=krb5**.

```
[root@fc22 ~]# mount ddr12345.<domain-name>:/data/col1/
mtree1 /mnt/nfs4 -o sec=krb5,vers=4
```

Activation d'Active Directory

La configuration de l'authentification Windows Active Directory permet d'intégrer le système Data Domain dans un realm Windows Active Directory. Les clients CIFS et NFS utilisent l'authentification Kerberos.

Procédure

1. Associez un realm Active Directory à l'aide de la commande `cifs set` :

```
# cifs set authentication active-directory <realm>
```

   Kerberos est automatiquement défini sur le système Data Domain. L'entité de sécurité du service nfs/ est créée automatiquement sur le KDC.
2. Configurez NIS à l'aide de la commande `authentication nis` :

```
# authentication nis servers add <serveur ad windows>
# authentication nis domain set <realm ad>
# authentication nis enable
```

3. Configurez CIFS pour utiliser NSS pour le mappage d'ID à l'aide des commandes `cifs` :

```
# cifs disable
# cifs option set idmap-type nss
# cifs enable
# filesys restart
```

4. Définissez le **`domaine nfs4`** de sorte qu'il soit identique au realm Active Directory :

```
# nfs option set nfs4-domain <realm ad>
```

5. Activez Active Directory pour le mappage d'ID NFSv4 en utilisant la commande `nfs` :

```
# nfs option set nfs4-idmap-active-directory enabled
```

Configuration d'Active Directory

Procédure

1. Installez le rôle Active Directory Domain Services (AD DS) sur le serveur Windows.
2. Installez la gestion des identités pour les composants UNIX.

```
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:adminui /all
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:nis /all
```

3. Vérifiez que le domaine NIS est configuré sur le serveur.

```
C:\Windows\system32>nisadmin
The following are the settings on localhost

Push Interval : 1 days
Logging Mode  : Normal

NIS Domains
NIS Domain in AD  Master server  NIS Domain in UNIX
----------------  -------------  ----------------
corp              win-ad-server  corp
```

4. Attribuez des UID/GID UNIX aux utilisateurs et groupes AD pour le serveur NFSv4.
   a. Accédez à **Server Manager** > **Tools** > **Active Directory**.
   b. Ouvrez les **propriétés** pour un utilisateur ou un groupe AD.
   c. Sous l'onglet UNIX Attributes, renseignez les champs NIS domain, UID et Primary GID.

Configuration des clients sur Active Directory

Procédure

1. Créez un utilisateur AD sur le serveur AD pour représenter l'entité de sécurité du service du client NFS.
2. Créez l'entité de sécurité du service nfs/ pour le client NFS.

```
> ktpass -princ nfs/<client_dns_name>@<REALM> -mapuser nfsuser -
pass **** -out nfsclient.keytab
/crytp rc4-hmac-nt /ptype KRB5_NT_PRINCIPAL
```

3. (Facultatif) Copiez le fichier keytab dans `/etc/krb5.keytab` sur le client.

   La nécessité d'effectuer cette étape dépend du système d'exploitation client que vous utilisez.

CHAPITRE 11

Migration du stockage

Ce chapitre traite des sujets suivants :

Tour d'horizon de la migration du stockage

La migration du stockage prend en charge le remplacement des châssis de stockage existants par de nouveaux châssis pouvant offrir des performances plus élevées, une capacité supérieure et un encombrement réduit.

Après l'installation des nouveaux châssis, vous pouvez migrer les données issues d'anciens châssis vers de nouveaux châssis tandis que le système continue à prendre en charge d'autres processus tels que l'accès aux données, leur extension, leur nettoyage et leur réplication. La migration du stockage nécessite des ressources système, mais vous pouvez contrôler cela à l'aide des paramètres de régulation qui donnent à la migration une priorité relativement supérieure ou inférieure. Vous pouvez également interrompre une migration afin de libérer davantage de ressources pour les autres processus, puis reprendre la migration lorsque la demande de ressources est moindre.

Lors de la migration, le système utilise les données situées sur les châssis sources et cibles. Les nouvelles données sont écrites sur les nouveaux châssis. Les données non migrées sont mises à jour sur les châssis sources, et les données migrées sont mises à jour sur les châssis cibles. Si la migration est interrompue, la migration peut reprendre les blocs de migration qui n'ont pas été marqués comme migrés.

Lors de la migration, chaque bloc de données est copié et vérifié. Le bloc source est libéré et marqué comme migré, et l'index du système est mis à jour pour utiliser le nouvel emplacement. Les nouvelles données qui devaient atterrir dans le bloc source seront désormais redirigées vers le bloc cible. Toutes les nouvelles allocations du bloc de données qui auraient été allouées à partir de la source sont allouées à partir de la destination.

Le processus de copie de la migration s'effectue au niveau du tiroir, non au niveau des données logiques. Ainsi, tous les secteurs du disque du tiroir source sont accessibles et copiés, même s'il existe des données sur ces derniers. Par conséquent, l'utilitaire de migration du stockage ne peut pas être utilisé pour réduire l'encombrement des données logiques.

Remarque

Le jeu de données étant divisé entre les châssis sources et les châssis cibles pendant la migration, vous ne pouvez pas arrêter une migration et reprendre l'utilisation des châssis sources uniquement. Une fois commencée, la migration doit se terminer. Si une défaillance, par exemple un disque défaillant, interrompt la migration, résolvez le problème et reprenez la migration.

Selon la quantité de données à migrer et les paramètres de régulation sélectionnés, une migration du stockage peut prendre plusieurs jours ou semaines. Lorsque toutes les données sont migrées, le processus de finalisation, qui doit être initié manuellement à l'aide de la commande `storage migration finalize`, redémarre le système de fichiers. Pendant le redémarrage, les châssis sources sont supprimés de la configuration du système et les châssis cibles font désormais partie du système de fichiers. Lorsque le processus de finalisation est terminé, les châssis sources peuvent être supprimés du système.

Après une migration du stockage, le nombre de tiroirs de disques signalés par DD OS peut ne pas être séquentiel. Cela peut arriver car la numérotation des tiroirs est liée au numéro de série de chaque tiroir de disque. Reportez-vous à l'article 499019 de la base de connaissances : *Data Domain : Storage enclosure numbering is not sequential*, disponible sur https://support.emc.com pour obtenir des informations

supplémentaires. Dans DD OS version 5.7.3.0 et versions ultérieures, la commande `enclosure show persistent-id` décrite dans l'article nécessite un accès administrateur, non un accès au SE.

Considérations relatives à la planification d'une migration

Tenez compte des consignes suivantes avant de démarrer une migration du stockage.

- La migration du stockage nécessite une licence d'utilisation unique et s'exécute sur des modèles de système pris en charge par DD OS version 5.7 ou une version supérieure.

  Remarque

  Plusieurs opérations de migration du stockage nécessitent plusieurs licences. Il est possible, toutefois, de migrer plusieurs châssis vers plusieurs châssis de destination au cours d'une seule opération.

- La migration du stockage repose sur la capacité, non sur le nombre de châssis. Par conséquent :
  - Un châssis source peut être migré vers un seul châssis de destination.
  - Un châssis source peut être migré vers plusieurs châssis de destination.
  - Plusieurs châssis source peuvent être migrés vers un seul châssis de destination.
  - Plusieurs châssis source peuvent être migrés vers plusieurs châssis de destination.
- Les châssis de destination doivent :
  - Être des tiroirs neufs, non attribués ou sans licence.
  - pris en charge sur le modèle du système DD ;
  - posséder une capacité utile au moins équivalente à celle des châssis qu'ils remplacent.

    Remarque

    Il n'est pas possible de déterminer le taux d'utilisation du tiroir source. Le système Data Domain effectue tous les calculs en fonction de la capacité du tiroir.
- Le modèle du système DD doit avoir une capacité mémoire suffisante pour prendre en charge la capacité de stockage du niveau actif des nouveaux châssis.
- La migration des données n'est pas prise en charge pour les disques situés dans le Contrôleur système.
- **⚠ ATTENTION**

  Ne mettez pas à niveau DD OS tant que la migration du stockage en cours d'exécution n'est pas terminée.
- La migration du stockage ne peut pas démarrer lorsque le système de fichiers est désactivé ou lorsqu'une mise à niveau de DD OS est en cours d'exécution, qu'une autre migration est en cours ou qu'une reconstruction RAID est en cours.

Remarque

Si une opération de migration du stockage est en cours, une nouvelle licence de migration du stockage est nécessaire pour démarrer une nouvelle opération une fois la migration en cours terminée. La présence ou l'absence d'une licence de migration du stockage est signalée lors de la pré-vérification de la mise à niveau.

- Tous les châssis sources spécifiés doivent se trouver dans le même niveau (actif ou archivage).
- Il ne peut y avoir qu'un seul groupe de disques dans chaque châssis source et tous les disques du groupe de disques doivent être installés dans un même châssis.
- Tous les disques de chaque châssis cible doivent être du même type (par exemple, SATA ou SAS).
- Après le début de la migration, les châssis cibles ne peuvent pas être supprimés.
- Les châssis sources ne peuvent pas être retirés tant que la migration n'est ni terminée ni finalisée.
- La durée de la migration du stockage dépend des ressources système (qui diffèrent en fonction des modèles de système), de la disponibilité des ressources système et de la quantité de données à migrer. La migration du stockage peut prendre plusieurs jours ou semaines.

Considérations relatives aux tiroirs DS60

Le tiroir dense DS60 peut contenir 60 disques, ce qui permet au client d'exploiter la totalité de l'espace disponible dans le rack. Les disques sont accessibles à partir du haut du tiroir, en tirant le tiroir de l'armoire. En raison du poids des tiroirs (environ 100 kg à pleine charge), veuillez lire attentivement cette section avant de procéder à une migration du stockage vers les tiroirs DS60.

Tenez compte des considérations suivantes lorsque vous travaillez avec le tiroir DS60 :

⚠ ATTENTION

- **Le chargement des tiroirs par le haut du rack risque de faire basculer le tiroir.**
- **Assurez-vous que le sol est capable de supporter le poids total des tiroirs DS60.**
- **Assurez-vous que les racks peuvent fournir l'alimentation dont les tiroirs DS60 ont besoin.**
- **Lorsque vous ajoutez plus de cinq tiroirs DS60 dans le premier rack ou plus de six tiroirs DS60 dans le deuxième rack, des barres de stabilisation et une échelle sont nécessaires pour maintenir les tiroirs DS60 parfaitement stables.**

Affichage de l'état de migration

DD System Manager propose deux moyens d'afficher l'état de la migration du stockage.

Procédure

1. Sélectionnez **Hardware** > **Storage**.

   Dans la zone Storage, vérifiez la ligne Storage Migration Status. Si l'état est Not Licensed, vous devez ajouter une licence avant d'utiliser les fonctions de

migration du stockage. Si la licence de migration du stockage est installée, l'état peut être l'un des états suivants : None, Starting, Migrating, Paused by User, Paused by System, Copy Completed - Pending Finalization, Finalizing, Failed during Copy ou Failed during Finalize.

2. Si une migration du stockage est en cours, cliquez sur **View Storage Migration** pour afficher les boîtes de dialogue de la progression.

Remarque

L'état de migration affiche le pourcentage de blocs transférés. Dans un système doté de plusieurs blocs disponibles, les blocs disponibles ne sont pas migrés, mais ils sont inclus dans l'indication de progression. Dans ce cas, l'indication de progression augmentera rapidement et ralentira au démarrage de la migration des données.

3. Lorsqu'une migration du stockage est en cours, vous pouvez également afficher l'état en sélectionnant **Health** > **Jobs**.

Évaluation du niveau de préparation de la migration

Vous pouvez utiliser le système pour évaluer le niveau de préparation de la migration du stockage sans valider le démarrage de la migration.

Procédure

1. Installez les châssis cibles en suivant les instructions fournies dans les guides d'installation du produit.
2. Sélectionnez **Administration** > **Licenses** et vérifiez que la licence de migration du stockage est installée.
3. Si la licence de migration du stockage n'est pas installée, cliquez sur **Add Licenses** et ajoutez la licence.
4. Sélectionnez **Hardware** > **Storage**, puis cliquez sur **Migrate Data**.
5. Dans la boîte de dialogue Select a Task, sélectionnez **Estimate**, puis cliquez sur **Next**.
6. Dans la boîte de dialogue Select Existing Enclosures, utilisez les cases à cocher pour sélectionner chacun des châssis sources pour la migration du stockage, puis cliquez sur **Next**.
7. Dans la boîte de dialogue Select New Enclosures, utilisez les cases à cocher pour sélectionner chacun des châssis cibles pour la migration du stockage, puis cliquez sur **Next**.

   Le bouton Add Licenses vous permet d'ajouter des licences de stockage pour les nouveaux châssis en fonction des besoins, sans interrompre la tâche en cours.
8. Dans la boîte de dialogue Review Migration Plan, vérifiez le planning de migration estimé, puis cliquez sur **Next**.
9. Passez en revue les résultats de la vérification préalable dans la boîte de dialogue Verify Migration Preconditions, puis cliquez sur Close.

Résultats

Si un des tests de vérification préalable échoue, résolvez le problème avant de commencer la migration.

Migration du stockage à l'aide de DD System Manager

Le processus de migration du stockage évalue le niveau de préparation du système, vous invite à confirmer que vous souhaitez démarrer la migration, migre les données et vous invite ensuite à finaliser le processus.

Procédure

1. Installez les châssis cibles en suivant les instructions fournies dans les guides d'installation du produit.
2. Sélectionnez **Administration** > **Licenses** et vérifiez que la licence de migration du stockage est installée.
3. Si la licence de migration du stockage n'est pas installée, cliquez sur **Add Licenses** et ajoutez la licence.
4. Sélectionnez **Hardware** > **Storage**, puis cliquez sur**Migrate Data**.
5. Dans la boîte de dialogue Select a Task, sélectionnez **Migrate**, puis cliquez sur **Next**.
6. Dans la boîte de dialogue Select Existing Enclosures, utilisez les cases à cocher pour sélectionner chacun des châssis sources pour la migration du stockage, puis cliquez sur **Next**.
7. Dans la boîte de dialogue Select New Enclosures, utilisez les cases à cocher pour sélectionner chacun des châssis cibles pour la migration du stockage, puis cliquez sur **Next**.

   Le bouton Add Licenses vous permet d'ajouter des licences de stockage pour les nouveaux châssis en fonction des besoins, sans interrompre la tâche en cours.
8. Dans la boîte de dialogue Review Migration Plan, vérifiez le planning de migration estimé, puis cliquez sur **Start**.
9. Dans la boîte de dialogue Start Migration, cliquez sur **Start**.

   La boîte de dialogue Migrate s'affiche et se met à jour pendant les trois phases de la migration : Starting Migration, Migration in Progress et Copy Complete.
10. Lorsque le titre de la boîte de dialogue Migrate affiche Copy Complete et qu'un redémarrage du système de fichiers est acceptable, cliquez sur **Finalize**.

    Remarque

    Cette tâche redémarre le système de fichiers et prend généralement 10 à 15 minutes. Le système n'est pas disponible pendant cette période.

Résultats

Lorsque la tache de finalisation de la migration est terminée, le système utilise les châssis cibles, et les châssis sources peuvent être supprimés.

Descriptions des boîtes de dialogue de migration du stockage

Les descriptions des boîtes de dialogue DD System Manager fournissent des informations supplémentaires sur la migration du stockage. Ces informations sont également disponibles en cliquant sur l'icône d'aide dans les boîtes de dialogue.

Boîte de dialogue Select a Task

La configuration dans cette boîte de dialogue détermine si le système évalue le niveau de préparation de la migration du stockage et s'arrête, ou s'il évalue le niveau de préparation avant de procéder à la migration du stockage.

Sélectionnez **Estimate** pour évaluer le niveau de préparation du système et interrompre.

Sélectionnez **Migrate** pour démarrer la migration après l'évaluation du système. Une boîte de dialogue vous invite à confirmer ou à annuler la migration du stockage entre l'évaluation du système et le début de la migration.

Boîte de dialogue Select Existing Enclosures

La configuration dans cette boîte de dialogue sélectionne le niveau actif ou le niveau de rétention et les châssis source pour la migration.

Si la fonction DD Extended Retention est installée, utilisez la zone de liste pour sélectionner **Active Tier** (niveau actif) ou **Retention Tier** (niveau de rétention). La zone de liste n'apparaît pas lorsque la fonction DD Extended Retention n'est pas installée.

La liste Existing Enclosures affiche les châssis qui sont éligibles pour la migration du stockage. Sélectionnez la case à cocher pour chacun des châssis à migrer. Lorsque vous êtes prêt à continuer, cliquez sur **Next**.

Boîte de dialogue Select New Enclosures

La configuration dans cette boîte de dialogue sélectionne les châssis cibles pour la migration. Cette boîte de dialogue affiche également l'état de la licence de stockage et un bouton **Add Licences**.

La liste Available Enclosures affiche les châssis qui sont des destinations éligibles pour la migration du stockage. Sélectionnez la case à cocher pour chacun des châssis cibles souhaités.

La barre d'état de la licence représente toutes les licences de stockage installées sur le système. La partie verte représente les licences qui sont en cours d'utilisation et la partie claire représente la capacité de stockage sous licence disponible pour les châssis cibles. Si vous avez besoin installer des licences supplémentaires pour prendre en charge les Contrôleurs cibles sélectionnés, cliquez sur **Add Licenses**.

Lorsque vous êtes prêt à continuer, cliquez sur **Next**.

Boîte de dialogue Review Migration Plan

Cette boîte de dialogue présente une estimation de la durée de la migration du stockage, organisée en trois phases.

La phase 1 de la migration du stockage exécute une série de tests afin de vérifier que le système est prêt pour la migration. Les résultats du test s'affichent dans la boîte de dialogue Verify Migration Preconditions.

Pendant la phase 2, les données sont copiées à partir des châssis sources vers les châssis cibles. Lorsqu'une grande quantité de données est présente, la copie peut prendre plusieurs jours ou semaines car celle-ci est effectuée en arrière-plan, tandis que le système continue de servir les clients de sauvegarde. Un paramètre de la boîte de dialogue Migfration in Progress vous permet de modifier la priorité de la migration, ce qui peut accélérer ou ralentir la migration.

La phase 3, qui est initiée manuellement à partir de la boîte de dialogue Copy Complete, met à jour la configuration du système pour utiliser les châssis cibles et supprime la configuration des Contrôleurs sources. Au cours de cette phase, le système de fichiers est redémarré et le système n'est pas disponible pour les clients de sauvegarde.

Boîte de dialogue Verify Migration Preconditions

Cette boîte de dialogue affiche les résultats des tests qui s'exécutent avant le démarrage de la migration.

La liste suivante affiche la séquence de test et fournit des informations supplémentaires sur chacun des tests.

P1. La plate-forme de ce système est prise en charge.

Les anciens modèles du système DD ne prennent pas en charge la migration du stockage.

P2. Une licence de migration du stockage est disponible.

Une licence de migration du stockage est nécessaire.

P3. Aucune migration n'est en cours d'exécution.

Une migration de stockage précédente doit se terminer avant d'en commencer une autre.

P4. La demande actuelle de migration est identique à la demande de migration interrompue.

Reprenez et terminez la migration interrompue.

P5. Vérifiez la disposition du groupe de disques sur les châssis existants.

La migration du stockage nécessite que chaque châssis source ne contienne qu'un seul groupe de disques, et que tous les disques du groupe doivent se trouver dans ce châssis.

P6. Vérifiez la capacité du système final.

La capacité totale du système après la migration et la suppression des châssis sources ne doit pas dépasser la capacité prise en charge par le modèle du système DD.

P7. Vérifiez la capacité des châssis de remplacement.

La capacité utile des châssis cibles doit être supérieure à celle des châssis sources.

P8. Les châssis sources se trouvent dans le même niveau actif ou la même unité de rétention.

Le système prend en charge la migration du stockage à partir du niveau actif ou du niveau de rétention. Il ne prend pas en charge la migration des données à partir des deux niveaux en même temps.

P9. Les châssis sources ne font pas partie de l'unité de commande.

Bien que le Contrôleur système soit répertorié sous la forme d'un châssis dans la CLI, la migration du stockage ne prend pas en charge la migration à partir de disques installés dans le Contrôleur système.

P10. Des châssis de remplacement peuvent être ajoutés au stockage.

Tous les disques de chaque châssis cible doivent être du même type (par exemple, SATA ou SAS).

P11. Aucune reconstruction RAID ne se produit dans les Contrôleurs sources.

La migration du stockage ne peut pas démarrer si une reconstruction RAID est en cours.

P12. Le tiroir source appartient à un niveau pris en charge.

Le boîtier du disque source doit faire partie d'un niveau pris en charge sur la destination de la migration.

Boîtes de dialogue de la progression de la migration

Cette série de boîtes de dialogue présente l'état de la migration du stockage et les contrôles qui s'appliquent à chaque étape.

Migrate - Starting Migration
Lors de la première phase, la progression s'affiche sur la barre de progression et aucun contrôle n'est disponible.

Migrate - Migration in Progress
Lors de la deuxième phase, les données sont copiées entre les châssis sources et les châssis cibles, et la progression s'affiche sur la barre de progression. Étant donné que la copie des données peut prendre plusieurs jours ou semaines, des contrôles sont fournis afin que vous puissiez gérer les ressources utilisées lors de la migration et interrompre la migration lorsque les ressources sont nécessaires pour d'autres processus.

Vous pouvez cliquer sur **Pause** pour interrompre la migration, puis cliquez sur **Resume** ultérieurement pour poursuivre la migration.

Les boutons **Low**, **Medium** et **High** définissent les paramètres de régulation pour les besoins en ressources de migration du stockage. Un paramètre de régulation faible donne à la migration du stockage une priorité de ressources plus faible, ce qui se traduit par une migration plus lente et nécessite moins de ressources système. À l'inverse, un paramètre de régulation élevé donne à la migration du stockage une priorité de ressources plus élevée, ce qui se traduit par une migration plus rapide et nécessite davantage de ressources système. Le paramètre Medium sélectionne une priorité intermédiaire.

Vous n'êtes pas obligé de laisser cette boîte de dialogue ouverte pendant la durée de la migration. Pour vérifier l'état de la migration après la fermeture de cette boîte de dialogue, sélectionnez **Hardware** > **Storage** et affichez l'état de la migration. Pour revenir à cette boîte de dialogue à partir de la page Hardware/Storage, cliquez sur **Manage Migration**. La progression de la migration peut également être affichée en sélectionnant **Health** > **Jobs**.

Migrate - Copy Complete
Lorsque la copie est terminée, le processus de migration attend que vous cliquiez sur **Finalize**. Pendant la phase finale, qui prend 10 à 15 minutes, le système de fichiers est redémarré et le système n'est pas disponible. Il est recommandé de commencer cette phase lors d'une fenêtre de maintenance ou d'une période de faible activité du système.

Migration du stockage à l'aide de la CLI

Une migration requiert simplement le déplacement de tous les blocs alloués à partir des blocksets mis en forme sur des groupes de périphériques sources (par exemple, les blocksets sources) vers les blocksets formatés sur des groupes de périphériques cible (par exemple, les blocksets cibles). Lorsque tous les blocs alloués ont été déplacés à partir des blocksets source, ces blocksets peuvent être supprimés du système de fichiers ; leurs disques peuvent être supprimés de leur niveau de stockage et les châssis et les disques physiques peuvent être supprimés de DDR.

Remarque

La préparation des nouveaux châssis pour la migration du stockage est gérée par le processus de migration du stockage. Ne préparez pas les châssis cible comme vous le feriez pour ajouter un châssis. Par exemple, l'utilisation de la commande `filesys expand` est appropriée pour ajouter un châssis, mais cette commande empêche les châssis d'être utilisés comme des cibles pour la migration du stockage.

Un tiroir de disques DS60 contient quatre piles de disques composées chacune de 15 disques. Lorsque la source ou la destination de la migration est un tiroir DS60, les piles de disques sont référencées de la façon suivante : ***châssis*:*pile***. Dans cet exemple, la source est le châssis 7, pile 2 (7:2), et la destination est le châssis 7, pile 4 (7:4).

Procédure

1. Installez les châssis cible en suivant les instructions fournies dans les guides d'installation du produit.
2. Vérifiez si la licence des fonctions de migration du stockage est installée.

   ```
   # elicense show
   ```
3. Si la licence n'est pas installée, effectuez une mise à jour pour ajouter la licence des fonctions de migration du stockage.

   ```
   # elicense update
   ```
4. Affichez les états de disque pour les disques source et cible.

   ```
   # disk show state
   ```

   Les disques source doivent être à l'état Active, et les disques cibles doivent être à l'état Unknown.
5. Exécutez la commande de vérification préalable à la migration du stockage afin de déterminer si le système est prêt pour la migration.

   ```
   # storage migration precheck source-enclosures 7:2 destination-enclosures 7:4
   ```
6. Affichez la paramètre de régulation de la migration.

   ```
   storage migration option show throttle
   ```
7. Lorsque le système est prêt, commencez la migration du stockage.

```
# storage migration start source-enclosures 7:2 destination-
enclosures 7:4
```

8. Affichez, si besoin est, les états de disque pour les disques source et cible pendant la migration.

   ```
   # disk show state
   ```

   Lors de la migration, les disques source doivent être à l'état de migration, et les disques cible doivent être à l'état de destination.

9. Passez en revue l'état de la migration si nécessaire.

   ```
   # storage migration status
   ```

10. Affichez les états de disque pour les disques source et cible.

    ```
    # disk show state
    ```

    Lors de la migration, les disques source doivent être à l'état de migration, et les disques cible doivent être à l'état de destination.

11. Lorsque la migration est terminée, mettez à jour la configuration pour utiliser les châssis cible.

    Remarque

    Cette tâche redémarre le système de fichiers et prend généralement 10 à 15 minutes. Le système n'est pas disponible pendant cette période.

    ```
    storage migration finalize
    ```

12. Si vous souhaitez supprimer toutes les données de chacun des châssis source, supprimez-les maintenant.

    ```
    storage sanitize start enclosure <enclosure-id>[:<pack-id>]
    ```

    Remarque

    La command storage sanitize ne produit pas un effacement certifié des données. Data Domain propose l'effacement certifié des données en tant que service. Pour plus d'informations, contactez votre responsable de compte Data Domain.

13. Affichez les états de disque pour les disques source et cible.

    ```
    # disk show state
    ```

    Après la migration, les disques source doivent être à l'état Unknown, et les disques cible doivent être à l'état Active.

Résultats

Lorsque la tâche de finalisation de la migration est terminée, le système utilise le stockage cible, et le stockage source peut être supprimé.

Exemple de migration du stockage avec la CLI

elicense show

```
# elicense show
Feature licenses:
## Feature     Count Mode            Expiration Date
-- ----------- ----- --------------- ---------------
```

```
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

elicense update

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature          Count   Mode             Expiration Date
-- -----------       -----  ---------------  ---------------
1  REPLICATION       1      permanent (int)  n/a
2  VTL               1      permanent (int)  n/a
3  Storage Migration 1      permanent (int)
-- -----------       -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above EMC ELMS
licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

disk show state

Figure 10 `disk show state`

```
# disk show state
Enclosure        Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
-------------   ---------------------------------------------
1                .  .  .  .
2                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7               |--------|--------|--------|--------|
                | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)   |U  U  U |.  .  s |U  U  U |U  U  U |
     D(37-48)   |U  U  U |.  .  . |U  U  U |U  U  U |
     C(25-36)   |U  U  U |.  .  . |U  U  U |U  U  U |
     B(13-24)   |U  U  U |.  .  . |U  U  U |U  U  U |
     A( 1-12)   |U  U  U |.  .  . |U  U  U |U  U  U |
                |--------|--------|--------|--------|
-------------   ---------------------------------------------

Legend   State            Count
------   ---------------  -----
.        In Use Disks     18
s        Spare Disks      1
v        Available Disks  15
U        Unknown Disks    105
------   ---------------  -----
```

storage migration precheck

```
#storage migration precheck  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

      1 "Verifying platform support.....................................................PASS"
      2 "Verifying valid storage migration license exists.........................PASS"
```

```
      3 "Verifying no other migration is running.................................PASS"
      4 "Verifying request matches interrupted migration.........................PASS"
      5 "Verifying data layout on the source shelves.............................PASS"
      6 "Verifying final system capacity.........................................PASS"
      7 "Verifying destination capacity..........................................PASS"
      8 "Verifying source shelves belong to same tier............................PASS"
      9 "Verifying enclosure 1 is not used as source.............................PASS"
     10 "Verifying destination shelves are addable to storage.....................PASS"
     11 "Verifying no RAID reconstruction is going on in source shelves...........PASS"
Migration pre-check PASSED

Expected time to migrate data: 8 hrs 33 min
```

storage migration show history

Figure 11 `storage migration show history`

```
# storage migration show history
Id   Source       Source Enclosure   Dest         Dest Enclosure    Status      Start Time                 End Time
     Enclosure*   Serial No.         Enclosure*   Serial No.
--   ----------   ----------------   ----------   ---------------   ---------   ------------------------   ------------------------
2    9:0          SHU952400106A23    7:0          SHU9524084G055B   Finalized   Sat Aug  8 11:59:37 2015   Mon Aug 10 11:10:11 2015
1    9:0          SHU952400106A23    7:0          SHU9524084G055B   Finalized   Thu Aug  6 16:39:55 2015   Fri Aug  7 10:28:07 2015
                                     8:0          SHU9524084G04LR
--   ----------   ----------------   ----------   ---------------   ---------   ------------------------   ------------------------
(*) Enclosure ids at migration start time.
```

storage migration start

```
#storage migration start  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

  Expected time to migrate data: 84 hrs 40 min

**   Storage migration once started cannot be aborted.
     Existing data on the destination shelves will be overwritten.
        Do you want to continue with the migration? (yes|no) [no]: yes

Performing migration pre-check:
      1 Verifying platform support.................................................PASS
      2 Verifying valid storage migration license exists...........................PASS
      3 Verifying no other migration is running...................................PASS
      4 Verifying request matches interrupted migration...........................PASS
      5 Verifying data layout on the source shelves...............................PASS
      6 Verifying final system capacity...........................................PASS
      7 Verifying destination capacity............................................PASS
      8 Verifying source shelves belong to same tier..............................PASS
      9 Verifying enclosure 1 is not used as source...............................PASS
     10 Verifying destination shelves are addable to storage.....................PASS
     11 Verifying no RAID reconstruction is going on in source shelves...........PASS

Migration pre-check PASSED

Storage migration will reserve space in the filesystem to migrate data.
Space reservation may add up to an hour or more based on system resources.
```

```
Storage migration process initiated.
Check storage migration status to monitor progress.
```

storage migration status

Figure 12 `storage migration status`

```
# storage migration status
Id   Source          Destination     State       Percent    Estimated Time to Complete   Current Throttle
     Enclosure(s)    Enclosure(s)                Complete                                Setting
--   ------------    ------------    ---------   --------   --------------------------   ----------------
5    7:2             7:4             migrating   45%        30 hrs 18 mins               high
--   ------------    ------------    ---------   --------   --------------------------   ----------------
```

disk show state, migration en cours

Figure 13 `disk show state, migration in progress`

```
# disk show state
Enclosure         Disk
  Row(disk-id)     1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------   ------------------------------------------------
1                  .  .  .  .
2                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                 |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
      E(49-60)    |U  U  U |m  m  s |U  U  U |s  d  d |
      D(37-48)    |U  U  U |m  m  m |U  U  U |d  d  d |
      C(25-36)    |U  U  U |m  m  m |U  U  U |d  d  d |
      B(13-24)    |U  U  U |m  m  m |U  U  U |d  d  d |
      A( 1-12)    |U  U  U |m  m  m |U  U  U |d  d  d |
                  |--------|--------|--------|--------|
--------------   ------------------------------------------------

Legend   State                Count
------   -----------------    -----
.        In Use Disks         4
s        Spare Disks          2
v        Available Disks      15
U        Unknown Disks        90
m        Migrating Disks      14
d        Destination Disks    14
```

storage migration finalize

Figure 14 `storage migration finalize`

```
# storage migration finalize

Storage migration finalize restarts the filesystem.
This can take several minutes and the filesystem is unavailable until the operation completes.
        Do you want to continue? (yes|no) [no]: yes

Performing migration finalization pre-check:
(P1)    Verifying storage migration is ready for finalization....PASS
(P2)    Verifying there are no foreign disks.....................PASS
(P3)    Verifying data layout on the source shelves..............PASS

Migration finalization pre-check PASSED
Finalizing the storage migration with id 5:

Notifying filesystem to finalize migration...

Done.

Disabling the filesystem
Please wait..........
The filesystem is now disabled.
Removing source enclosures from filesystem...

Done.

Removing source enclosures from storage tier...

Done.

Enabling the filesystem
Please wait.....................
The filesystem is now enabled.
Storage migration with id 5 from enclosure(s) 7.2 to enclosure(s) 7.4 has been finalized.
```

disk show state, migration terminée

Figure 15 `disk show state, migration complete`

```
# disk show state
Enclosure         Disk
  Row(disk-id)     1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------    ------------------------------------------------
1                  .  .  .  .
2                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                 |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)     |U  U  U |U  U  U |U  U  U |s  .  . |
     D(37-48)     |U  U  U |U  U  U |U  U  U |.  .  . |
     C(25-36)     |U  U  U |U  U  U |U  U  U |.  .  . |
     B(13-24)     |U  U  U |U  U  U |U  U  U |.  .  . |
     A( 1-12)     |U  U  U |U  U  U |U  U  U |.  .  . |
                  |--------|--------|--------|--------|
--------------    ------------------------------------------------

Legend   State            Count
------   ---------------  -----
.        In Use Disks     18
s        Spare Disks      1
v        Available Disks  15
U        Unknown Disks    105
------   ---------------  -----
```

Remarque

La migration du stockage est actuellement uniquement prise en charge sur le nœud actif. La migration du stockage n'est pas prise en charge sur le nœud en veille du cluster HA.

CHAPITRE 12

Métadonnées sur disques Flash

Ce chapitre traite des sujets suivants :

Présentation des métadonnées sur disques Flash (MDoF)

MDoF crée des caches pour les métadonnées du système de fichiers à l'aide de technologies Flash. Le cache de disque SSD est un cache à faible latence qui gère un nombre élevé d'opérations d'E/S par seconde (IOPS) en vue d'accélérer l'accès aux données et aux métadonnées.

Remarque

La version logicielle minimale requise est DD OS 6.0.

La mise en cache des métadonnées du système de fichiers sur des disques SSD améliore les performances en matière d'E/S pour les charges applicatives traditionnelles et aléatoires.

Dans le cas des charges applicatives traditionnelles, le fait de décharger l'accès aléatoire aux métadonnées des disques durs vers les disques SSD permet aux disques durs de traiter les requêtes de lecture et d'écriture en continu.

Pour ce qui est des charges de travail aléatoires, le cache SSD garantit des opérations de métadonnées à faible temps de latence, ce qui permet aux disques durs de traiter les requêtes de données au lieu des requêtes de cache.

Le cache de lecture sur le disque SSD améliore les performances des lectures aléatoires en mettant en cache les données fréquemment consultées. L'écriture des données en NVRAM, combinée aux opérations de métadonnées à faible temps de latence pour décharger plus rapidement le module NVRAM, améliore la latence d'écriture aléatoire. L'absence de cache n'empêche pas le fonctionnement du système de fichiers. Elle affecte uniquement ses performances.

Lorsque le niveau cache est créé pour la première fois, un redémarrage du système de fichiers est uniquement nécessaire si le niveau de cache est ajouté après l'exécution du système de fichiers. Pour les nouveaux systèmes livrés avec disques de niveau cache, aucun redémarrage du système de fichiers n'est nécessaire si le niveau de cache est créé avant la première activation du système de fichiers. Il est possible d'ajouter du cache supplémentaire à un système actif, sans avoir à désactiver et à réactiver le système de fichiers.

Remarque

Les systèmes DD9500 mis à niveau de DD OS 5.7 à DD OS 6.0 nécessitent un redémarrage du système de fichiers après la création initiale du niveau cache.

Lorsque le nombre de blocs restants sur un disque SSD est proche de zéro, le disque SSD passe en condition de lecture seule. Lorsque cette condition se produit, DD OS traite le disque en tant que cache en lecture seule et émet une alerte.

La fonction MDoF est prise en charge sur les systèmes Data Domain suivants :

- DD6300
- DD6800
- DD9300
- DD9500
- DD9800

- Les instances DD VE, y compris les systèmes DD3300, dans des configurations de capacité de 16 To et plus (niveau de cache SSD pour DD VE)

Octroi de licence et capacité MDoF

Une licence activée via ELMS est nécessaire pour utiliser la fonction MDoF ; la licence relative au cache de disque SSD n'est pas activée par défaut.

Le tableau suivant décrit les différentes licences de capacité de disque SSD et les capacités de disque SSD pour chaque système indiqué :

Tableau 121 Licences de capacité de disque SSD par système

Modèle	Mémoire	Nombre de disques SSD	Capacité SSD
DD6300	48 Go (Base)	1	800 Go
	96 Go (étendue)	2	1 600 Go
DD6800	192 Go (Base)	2	1 600 Go
	192 Go (étendue)	4	3 200 Go
DD9300	192 Go (Base)	5	4 000 Go
	384 Go (étendue)	8	6 400 Go
DD9500	256 Go (base)	8	6 400 Go
	512 Go (étendue)	15	12 000 Go
DD9800	256 Go (base)	8	6 400 Go
	768 Go (étendue)	15	12 000 Go

Niveau de cache SSD pour DD VE

Les instances DD VE et les systèmes DD3300 n'ont pas besoin d'une licence pour le niveau de cache SSD. La capacité SSD maximale prise en charge est de 1 % de la capacité du niveau actif.

Le tableau suivant décrit les différentes licences de capacité de disque SSD et les capacités de disque SSD pour chaque système indiqué :

Tableau 122 Capacité SSD de DD VE et DD3300

Configuration de la capacité	Capacité maximale SSD
DD VE (16 To)	160 Go
DD VE (32 To)	320 Go
DD VE (48 To)	480 Go
DD VE (64 To)	640 Go
DD VE (96 To)	960 Go
DD3300 8 To	160 Go
DD3300 (16 To)	160 Go
DD3300 (32 To)	320 Go

Niveau de cache SSD

Le niveau de cache SSD fournit le stockage de cache SSD pour le système de fichiers. Le système de fichiers exploite le stockage nécessaire du niveau de cache SSD sans intervention active de l'utilisateur.

Niveau cache SSD MDoF - gestion du système

Tenez compte des considérations suivantes au sujet du cache de disque SSD :

- Lorsque les disques SSD sont déployés au sein d'un contrôleur, ces disques SSD sont traités comme des disques racine internes. Ils apparaissent en tant que châssis 1 dans la sortie de la commande `storage show all`.
- La commande `disk` permet de gérer les disques SSD de la même manière que les disques durs.
- Exécutez la commande `storage add` pour ajouter un disque SSD ou un châssis de disque SSD au niveau cache SSD.
- L'espace du niveau cache SSD n'a pas besoin d'être géré. Le système de fichiers récupère le stockage nécessaire du niveau cache SSD et le partage entre ses clients.
- La commande `filesys create` crée un volume SSD si les disques SSD sont disponibles dans le système.

  Remarque

  Si les disques SSD sont ajoutés par la suite au système, le système doit automatiquement créer le volume SSD et en informer le système de fichiers. Le gestionnaire de cache SSD (SSD Cache Manager) prévient les clients enregistrés pour leur permettre de créer leurs objets en cache.

- Si le volume SSD ne contient qu'un seul disque actif, le dernier disque mis hors ligne est remis automatiquement en ligne si le disque actif est retiré du système.

La section suivante décrit comment gérer le niveau cache SSD à partir de Data Domain System Manager et à l'aide de la CLI de DD OS.

Gestion du niveau cache SSD

Les fonctions de configuration du stockage permettent d'ajouter et de retirer du stockage du niveau cache SSD.

Procédure

1. Sélectionnez **Hardware** > **Storage** > **Overview**.
2. Développez la boîte de dialogue **Cache Tier**.
3. Cliquez sur **Configure**.

   La quantité maximale de stockage pouvant être ajoutée au niveau actif dépend du contrôleur DD utilisé.

   Remarque

   La barre de la capacité sous licence affiche la partie de la capacité sous licence (utilisée et restante) pour les châssis installés.

4. Cochez cette case pour que le tiroir soit ajouté.
5. Cliquez sur le bouton **Add to Tier**.
6. Cliquez sur **OK** pour ajouter le stockage.

Remarque

Pour supprimer un tiroir ajouté, sélectionnez-le dans la liste Tier Configuration, cliquez sur **Remove from Configuration**, puis cliquez sur **OK**.

Équivalent de l'interface de ligne de commande (CLI)
Lorsque les disques SSD du niveau cache sont installés dans l'unité de commande :

a. Ajoutez les disques SSD au niveau cache.

```
#  storage add disks 1.13,1.14 tier cache
Checking storage requirements...done
Adding disk 1.13 to the cache tier...done

Updating system information...done

Disk 1.13 successfully added to the cache tier.


Checking storage requirements...
done
Adding disk 1.14 to the cache tier...done

Updating system information...done

Disk 1.14 successfully added to the cache tier.
```

b. Vérifiez l'état des disques SSD nouvellement ajoutés.

```
# disk show state
Enclosure   Disk
             1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------   ---------------------------------------------
1            .  .  .  .  s  .  .  s  s  s  s  s  v  v
2            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
---------   ---------------------------------------------

Legend   State             Count
------   ---------------   -----
.        In Use Disks      6
s        Spare Disks       6
v        Available Disks   2
U        Unknown Disks     30
------   ---------------   -----
Total 44 disks
```

Lorsque les disques SSD du niveau cache sont installés dans un tiroir externe :

a. Assurez-vous que le système reconnaît le tiroir de disque SSD. Dans l'exemple ci-dessous, le tiroir de disque SSD est le châssis 2.

```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    ---------------------------------------------
1            .  .  .  .
2            U  U  U  U  U  U  U  U  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
```

```
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10          |--------|--------|--------|--------|
            | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60) |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48) |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36) |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24) |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12) |v  v  v |v  v  v |v  v  v |v  v  v |
            |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------   -----------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

b. Identifiez l'ID du tiroir de disque SSD. Les disques SSD sont identifiés comme `SAS-SSD` ou `SATA-SSD` dans la colonne `Type`.

```
#  disk show hardware
```

Figure 16

Disk (enc/disk)	Slot	Manufacturer/Model	Firmware	Serial No.	Capacity	Type
1.1	0	TG32C10400GA3EMC_____118000371	PRO6E344	FG009826	372.61 GiB	SATA-SSD
1.2	1	TG32C10400GA3EMC_____118000371	PRO6E344	FG0097VL	372.61 GiB	SATA-SSD
1.3	2	TG32C10400GA3EMC_____118000371	PRO6E344	FG009881	372.61 GiB	SATA-SSD
1.4	3	TG32C10400GA3EMC_____118000371	PRO6E344	FG00988X	372.61 GiB	SATA-SSD
2.1	0	HITACHI HUSMR148_CLAR800	C29C	07V4P2AA	745.22 GiB	SAS-SSD
2.2	1	HITACHI HUSMR148_CLAR800	C29C	07V4P3LA	745.22 GiB	SAS-SSD
2.3	2	HITACHI HUSMR148_CLAR800	C29C	07V4P2XA	745.22 GiB	SAS-SSD
2.4	3	HITACHI HUSMR148_CLAR800	C29C	07V4TW4A	745.22 GiB	SAS-SSD
2.5	4	HITACHI HUSMR148_CLAR800	C29C	07V4ULYA	745.22 GiB	SAS-SSD
2.6	5	HITACHI HUSMR148_CLAR800	C29C	07V4P0BA	745.22 GiB	SAS-SSD
2.7	6	HITACHI HUSMR148_CLAR800	C29C	07V4UVBA	745.22 GiB	SAS-SSD
2.8	7	HITACHI HUSMR148_CLAR800	C29C	07V4UTNA	745.22 GiB	SAS-SSD

c. Ajouter le tiroir de disque SSD au niveau cache.

```
#  storage add enclosure 2 tier cache

Checking storage requirements...done
Adding enclosure 2 to the cache tier...Enclosure 2
successfully added to the cache tier.

Updating system information...done

Successfully added: 2  done
```

d. Vérifiez l'état des disques SSD nouvellement ajoutés.

```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    -----------------------------------------------
1            .  .  .  .
2            .  .  .  .  .  .  .  .  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10          |--------|--------|--------|--------|
            | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60) |v  v  v |v  v  v |v  v  v |v  v  v |
```

```
   D(37-48) |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36) |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24) |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12) |v  v  v |v  v  v |v  v  v |v  v  v |
            |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------   -----------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------- -----
Total 222 disks
```

Pour retirer un disque SSD monté avec un contrôleur du niveau cache :

```
# storage remove disk 1.13

Removing disk 1.13...done

Updating system information...done

Disk 1.13 successfully removed.
```

Pour retirer un tiroir de disque SSD du système :

```
# storage remove enclosure 2

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done
```

Alertes de disque SSD

Il existe trois alertes spécifiques du niveau cache SSD.

Les alertes du niveau cache SSD sont les suivantes :

- Octroi de licences
  Si le système de fichiers est activé et que la capacité de cache physique configurée est inférieure à la quantité autorisée par la licence, vous obtenez une alerte qui signale la capacité actuelle du cache du disque SSD et la capacité à laquelle vous donne droit la licence. Cette alerte est considérée comme une alerte d'avertissement. L'absence de cache n'empêche pas le fonctionnement du système de fichiers. Elle affecte uniquement ses performances. Il est possible d'ajouter du cache supplémentaire à un système actif, sans avoir à désactiver et à réactiver le système de fichiers.
- Condition de lecture seule
  Lorsque le nombre de blocs restants est proche de zéro, le disque SSD passe en condition de lecture seule. Lorsque cette condition se produit, DD OS traite le disque en tant que cache en lecture seule.

  L'alerte `EVT-STORAGE-00001` s'affiche lorsque le disque SSD est en état de lecture seule et doit être remplacé.
- Fin de vie du disque SSD

Lorsqu'un disque SSD arrive en fin de vie, le système génère une alerte de défaillance matérielle identifiant l'emplacement du disque SSD dans le tiroir de disque SSD. Cette alerte est considérée comme une alerte critique.

L'alerte `EVT-STOCKAGE-00016` apparaît lorsque le compteur de fin de vie atteint la valeur 98. Le disque est mis en échec de façon proactive lorsque le compteur de fin de vie atteint la valeur 99.

CHAPITRE 13

SCSI Target

Ce chapitre traite des sujets suivants :

Présentation de SCSI Target

SCSI (Small Computer System Interface) Target est un processus de gestion pour tous les services et transports SCSI. SCSI Target prend en charge DD VTL (Virtual Tape Library), DD Boost over FC (Fibre Channel), les services vDisk/ProtectPoint Block Services, ainsi que tous les services ayant une LUN (unité logique) cible sur un système DD.

Services et transports SCSI Target

Le processus SCSI Target démarre lorsqu'il existe des ports FC ou une licence DD VTL. Elle assure la gestion unifiée de tous les *services* et *transports* d'une cible SCSI.

- Un *service* type possède une LUN (unité logique) cible sur un système DD qui utilise des commandes SCSI, telle que DD VTL (lecteurs de bande et changeurs) et DD Boost over FC (périphériques de processeur) ou vDisk (Virtual Disk Device).
- Un *transport* type permet aux *périphériques* de devenir visibles pour les *initiateurs*.
- Un *initiateur* est un client de sauvegarde qui se connecte à un système pour lire et écrire des données à l'aide du protocole Fibre Channel. Un initiateur spécifique peut prendre en charge DD Boost over FC, vDisk ou DD VTL, mais pas les trois.
- Les *périphériques* sont visibles sur un réseau SAN (réseau de zone de stockage) via des ports physiques. Les initiateurs hôtes communiquent avec le système DD via le réseau SAN.
- Les *groupes d'accès* gèrent les accès entre les périphériques et les initiateurs.
- Un *point de terminaison* est la cible logique, dans le système DD, à laquelle un initiateur est connecté. Vous pouvez activer, désactiver et renommer les points de terminaison. Pour supprimer des points de terminaison, le matériel de transport associé ne doit plus exister. Les points de terminaison sont automatiquement découverts et créés lorsqu'une nouvelle connexion de transport est établie. Les points de terminaison présentent les caractéristiques suivantes : topologie des ports, état FCP2-RETRY, WWPN et WWNN.
- *NPIV*(N_port ID Virtualization) est une fonction Fibre Channel qui permet à plusieurs points de terminaison de partager un seul port physique. NPIV facilite la configuration matérielle requise et offre des fonctions de basculement sur incident.
- Dans DD OS 6.0, les utilisateurs peuvent spécifier la séquence des adresses système secondaires pour le basculement sur incident. Par exemple, si le système indique 0, 0b, 1a, 1b et que l'utilisateur spécifie 1b, 1a, 0, 0b, la séquence définie par l'utilisateur est appliquée lors du basculement sur incident. La commande `scsitarget endpoint show detailed` affiche la séquence définie par l'utilisateur.

Notez les exceptions suivantes :

- DD Boost peut servir simultanément des clients FC et IP ; cependant, ces deux transports ne peuvent pas partager le même initiateur.
- Un seul initiateur doit être présent par groupe d'accès. Chaque groupe d'accès est affecté à un type (DD VTL, services vDisk/ProtectPoint Block ou DD Boost over FC).

Architectures SCSI Target prises en charge et non prises en charge

SCSI Target prend en charge les architectures suivantes :

- **DD VTL plus DD Boost over FC à partir d'initiateurs différents :** Deux initiateurs différents (sur des clients identiques ou différents) peuvent accéder à un système DD utilisant DD VTL et DD Boost over FC, via les points de terminaison cibles identiques ou différents du système DD.
- **DD VTL plus DD Boost over FC à partir d'un initiateur vers deux systèmes DD différents :** Un seul initiateur peut accéder à deux systèmes DD différents utilisant n'importe quel service.

SCSI Target ne prend pas en charge l'architecture suivante :

- **DD VTL plus DD Boost over FC à partir d'un initiateur vers le même système DD :** Un seul initiateur ne peut pas accéder au même système via des services différents.

Protocole d'allocation dynamique

Le protocole d'allocation dynamique (Thin) est un processus léger pour VDisk et DD VTL qui répond aux commandes SCSI lorsque le protocole principal ne peut pas. Pour les environnements Fibre Channel avec plusieurs protocoles, le protocole d'allocation dynamique :

- Empêche le blocage de l'initiateur
- Empêche les abandons inutiles de l'initiateur
- Empêche la disparition des périphériques de l'initiateur
- Prend en charge un mode veille
- Prend en charge les systèmes découvrables de façon précoce et rapide
- Améliore le comportement de haute disponibilité du protocole
- Ne nécessite pas d'accès au registre rapide

Pour de plus amples informations sur DD Boost et la commande scscitarget (CLI)

Pour plus d'informations sur l'utilisation de DD Boost via DD System Manager, reportez-vous au chapitre correspondant du présent guide. Pour d'autres types d'informations sur DD Boost, consultez le document *Guide d'administration de Data Domain Boost for OpenStorage*.

Ce chapitre aborde l'utilisation de la fonction SCSI Target via DD System Manager. Une fois que vous êtes familiarisé avec les tâches de base, la commande `scscitarget` du *Guide de référence des commandes de Data Domain Operating System* offre des tâches de gestion plus avancées.

En cas de trafic DD VTL intense, évitez d'exécuter la commande `scsitarget group use` qui permute les listes des points de terminaison en cours d'utilisation pour un ou plusieurs périphériques SCSI Target ou vdisk d'un groupe entre les listes de points de terminaison primaires et secondaires.

Vue Fibre Channel

La vue Fibre Channel affiche l'état actuel de l'activation de Fibre Channel et/ou de la virtualisation NPIV. Elle affiche également deux onglets : Resources et Access Groups. Les ressources incluent les ports, les initiateurs et les points d'accès. Un groupe d'accès contient un ensemble de WWPN (noms de ports internationaux) ou d'alias d'initiateurs, ainsi que les disques et changeurs auxquels ils sont autorisés à accéder.

Activation de NPIV

NPIV (N_port ID Virtualization) est une fonction Fibre Channel qui permet à plusieurs points de terminaison de partager un seul port physique. NPIV facilite la configuration

matérielle requise et offre des fonctions de basculement sur incident/retour arrière pour les points de terminaison. NPIV n'est pas configuré par défaut, vous devez donc l'activer.

Remarque

NPIV est activé par défaut dans une configuration HA.

NPIV assure une consolidation simplifiée de plusieurs systèmes :

- NPIV est une norme ANSI T11 qui permet à un seul port physique d'adaptateur HBA de s'enregistrer auprès d'un fabric Fibre Channel à l'aide de plusieurs WWPN
- Les ports virtuels et physiques ont les mêmes propriétés et se comportent exactement de la même façon.
- Il peut exister des relations m:1 entre les points de terminaison et le port. Autrement dit, plusieurs points de terminaison peuvent partager le même port physique.

Plus spécifiquement, l'activation de la virtualisation NPIV active les fonctions suivantes :

- Plusieurs points de terminaison sont autorisés par port physique, chacun utilisant un port (NPIV) virtuel. Le port de base est un espace réservé pour le port physique et n'est pas associé à un point de terminaison.
- La fonction de basculement sur incident/retour arrière des points de terminaison est automatiquement activée lors de l'utilisation de NPIV.

  Remarque

  Une fois la virtualisation NPIV activée, la « seconde adresse système » doit être spécifiée sur chacun des points de terminaison. Dans le cas contraire, le basculement sur incident du point de terminaison n'aura pas lieu.

- Plusieurs systèmes DD peuvent être regroupés dans un seul système DD. En revanche, le nombre d'adaptateurs HBA reste la même sur le système Data Domain unique.
- Le basculement sur incident du point de terminaison est déclenché lorsque FC-SSM détecte qu'un port n'est plus en ligne. Dans le cas où le port physique est hors ligne avant que scsitarget soit activé et où le port est toujours hors ligne après l'activation de scsitarget, un basculement sur incident du point de terminaison n'est pas possible, car FC-SSM ne génère pas un événement de port hors ligne. Si le port est de nouveau en ligne et si le retour arrière automatique est activé, tous les points de terminaison basculés qui utilisent ce port comme port primaire reviendront sur ce port primaire.

Les fonctions HA Data Domain nécessitent que la virtualisation NPIV déplace les noms universels entre les nœuds d'une paire HA au cours du processus de basculement sur incident.

Remarque

Les conditions suivantes doivent être respectées avant d'activer NPIV :

- Le système DD doit exécuter DD OS 5.7.
- Tous les ports doivent être connectés à un adaptateur HBA à 4, 8 et 16 Gbit Fibre Channel et une carte SLIC.
- L'ID du système DD doit être valide. Autrement dit, il ne doit pas être 0.

En outre, les topologies de port et les noms de port seront examinés et peuvent empêcher l'activation de NPIV :

- NPIV est autorisée si la topologie pour *tous* les ports est loop-preferred.
- NPIV est autorisée si la topologie de *certains* ports est loop-preferred. Toutefois, NPIV doit être désactivée pour les ports loop-only, ou vous devez reconfigurer la topologie sur loop-preferred pour une fonctionnalité appropriée.
- NPIV n'est *pas* autorisée si *aucun* port ne dispose d'une topologie loop-preferred.
- Si les noms de port sont présents dans les groupes d'accès, ils seront remplacés par les noms de point de terminaison associés.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel**.
2. En regard de NPIV : Disabled, sélectionnez **Enable**.
3. Dans la boîte de dialogue Enable NPIV, vous êtes averti que tous les ports Fibre Channel doivent être désactivés avant l'activation de NPIV. Si vous voulez vraiment effectuer cette opération, sélectionnez **Yes**.

   Équivalent de l'interface de ligne de commande (CLI)

   a. Assurez-vous que NPIV (global) est activée.

   ```
   # scsitarget transport option show npiv
   SCSI Target Transport Options
   Option   Value
   ------   --------
   npiv     disabled
   ------   --------
   ```

   b. Si la virtualisation NPIV est désactivée, activez-la. Vous devez d'abord désactiver tous les ports.

   ```
   # scsitarget port disable all
   All ports successfully disabled.
   # scsitarget transport option set npiv enabled
   Enabling FiberChannel NPIV mode may require SAN zoning to
   be changed to configure both base port and NPIV WWPNs.
   Any FiberChannel port names used in the access groups will
   be converted to their corresponding endpoint names in order
   to prevent ambiguity.
       Do you want to continue? (yes|no) [no]:
   ```

   c. Réactivez les ports désactivés.

   ```
   # scsitarget port enable all
   All ports successfully enabled.
   ```

   d. Assurez-vous que le paramètre de la virtualisation NPIV des ports physiques est définie sur « auto ».

   ```
   # scsitarget port show detailed 0a
   System Address:     0a
   ```

```
Enabled:             Yes
Status:              Online
Transport:           FibreChannel
Operational Status: Normal
FC NPIV:             Enabled (auto)
.
.
.
```

e. Créez un nouveau point de terminaison via les ports primaires et secondaires que vous avez sélectionnés.

```
# scsitarget endpoint add test0a0b system-address 0aprimary-
system-address 0a secondary-system-address 0b
```

Notez que le point de terminaison est désactivé par défaut, activez-le donc.

```
# scsitarget endpoint enable test0a0b
```

Puis, affichez les informations sur le point de terminaison.

```
# scsitarget endpoint show detailed test0a0b
Endpoint:                  test0a0b
Current System Address:    0b
Primary System Address:    0a
Secondary System Address: 0b
Enabled:                   Yes
Status:                    Online
Transport:                 FibreChannel
FC WWNN:                   50:02:18:80:08:a0:00:91
FC WWPN:                   50:02:18:84:08:b6:00:91
```

f. Segmentez un système hôte pour le WWPN généré automatiquement du point de terminaison nouvellement créé.

g. Créez un périphérique DD VTL, vDisk ou DD Boost over Fibre Channel (DFC) et rendez ce périphérique disponible sur le système hôte.

h. Assurez-vous que le périphérique DD choisi est accessible sur l'hôte (lecture et/ou écriture).

i. Testez le basculement sur incident du point de terminaison à l'aide de l'option « secondary » permettant de déplacer le point de terminaison vers l'adresse système secondaire (SSA).

```
# scsitarget endpoint use test0a0b secondary
```

j. Assurez-vous que le périphérique DD choisi est toujours accessible sur l'hôte (lecture et/ou écriture). Testez le retour arrière à l'aide de l'option « primary » pour faire revenir le point de terminaison sur l'adresse système primaire (PSA).

```
# scsitarget endpoint use test0a0b primary
```

k. Assurez-vous que le périphérique DD choisi est toujours accessible sur l'hôte (lecture et/ou écriture).

Désactivation de la virtualisation NPIV

Avant de pouvoir désactiver la virtualisation NPIV, aucun port ne doit posséder plusieurs points de terminaison.

Remarque

La virtualisation NPIV est requise pour une configuration HA. Elle est activée par défaut et ne peut pas être désactivée.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel**.
2. En regard de NPIV : Enabled, sélectionnez **Disable**.
3. Dans la boîte de dialogue Disable NPIV, lisez les messages à propos de la correction de la configuration, puis sélectionnez **OK** lorsque vous êtes prêt.

Onglet Resources

L'onglet **Hardware** > **Fibre Channel** > **Resources** affiche des informations sur les ports, les points de terminaison et les initiateurs.

Tableau 123 Ports

Élément	Description
System Address	Adresse système du port
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC
Enabled	État opérationnel du port : activé ou désactivé.
NPIV	État de la virtualisation NPIV : activé ou désactivé.
Link Status	État de la liaison : en ligne ou hors ligne ; autrement dit, si le port est actif et capable de traiter le trafic.
Operation Status	État de l'opération : Normal ou Marginal.
# of Endpoints	Nombre de points de terminaison associés à ce port.

Tableau 124 Points de terminaison

Élément	Description
Name	Nom du point de terminaison.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC
System Address	Adresse système du point de terminaison.
Enabled	État opérationnel du port : activé ou désactivé.
Link Status	En ligne ou hors ligne ; autrement dit, si le port est actif et capable de traiter le trafic.

Tableau 125 Initiateurs

Élément	Description
Name	Nom de l'initiateur.
Service	Prise en charge du service par l'initiateur, qui est DD VTL, DD Boost ou vDisk.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
Vendor Name	Modèle de l'initiateur.
Online Endpoints	Points de terminaison vus par cet initiateur. Affiche `none` ou `offline` si l'initiateur n'est pas disponible.

Configuration d'un port

Les ports sont détectés, et un seul point de terminaison est automatiquement créé pour chaque port, au démarrage.

Les propriétés du port de base dépendent de l'activation ou de la désactivation du mode NPIV :

- Hors mode NPIV, les ports utilisent les mêmes propriétés que le point de terminaison. En d'autres termes, le WWPN du port de base et le point de terminaison sont identiques.
- En mode NPIV, les propriétés du port de base sont dérivées des valeurs par défaut. Autrement dit, un nouveau WWPN est généré pour le port de base. Celui-ci est également conservé afin de permettre une permutation cohérente entre les modes NPIV. En outre, le mode NPIV offre la possibilité de prendre en charge plusieurs points de terminaison par port.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sous **Ports**, sélectionnez un port puis cliquez sur **Modify** (crayon).
3. Dans la boîte de dialogue Configure Port, spécifiez si vous souhaitez activer ou désactiver automatiquement NPIV pour ce port.
4. Dans le champ Topology, sélectionnez Loop Preferred, Loop Only, Point to Point ou Default.
5. Dans le champ Speed, sélectionnez 1, 2, 4, 8 ou 16 Gbit/s ou auto.
6. Sélectionnez **OK**.

Activation d'un port

Les ports doivent être activés avant de pouvoir les utiliser.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.

2. Sélectionnez **More Tasks** > **Ports** > **Enable**. Si tous les ports sont déjà activés, une notification s'affiche.
3. Dans la boîte de dialogue Enable Ports, sélectionnez un ou plusieurs ports dans la liste, puis cliquez sur **Next**.
4. Après la confirmation, cliquez sur **Next** pour terminer la tâche.

Désactivation d'un port

Vous pouvez simplement désactiver un port (ou des ports), ou vous pouvez choisir de basculer tous les points de terminaison sur le port (ou les ports) vers un autre port.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sélectionnez **More Tasks** > **Ports** > **Disable**.
3. Dans la boîte de dialogue Disable Ports, sélectionnez un ou plusieurs ports dans la liste, puis cliquez sur **Next**.
4. Dans la boîte de dialogue de confirmation, vous pouvez continuer simplement en désactivant le port, ou vous pouvez choisir de basculer tous les points de terminaison sur les ports vers un autre port.

Ajout d'un point de terminaison

Un point de terminaison est un objet virtuel qui est mappé à un port virtuel sous-jacent. Hors mode NPIV (non disponible sur une configuration HA), un seul point de terminaison est autorisé par port physique, et le port de base est utilisé pour configurer ce point de terminaison sur le fabric. Lorsque la virtualisation NPIV est activée, plusieurs points de terminaison sont autorisés par port physique, chacun utilisant un port (NPIV) virtuel, et le basculement sur incident/retour arrière est activé pour les points de terminaison.

Remarque

Le mode non NPIV n'est pas disponible sur les configurations HA. La virtualisation NPIV est activée par défaut et ne peut pas être désactivée.

Remarque

En mode NPIV, les points de terminaison :

- disposent d'une adresse système primaire ;
- peuvent avoir zéro ou plusieurs adresses système secondaires ;
- sont tous candidats pour le basculement vers une adresse de l'autre système en cas de défaillance d'un port. Toutefois, le basculement vers un port marginal n'est pas pris en charge ;
- peuvent réutiliser leur port primaire lorsque celui-ci est à nouveau en ligne.

Remarque

Lors de l'utilisation de la virtualisation NPIV, il vous est recommandé d'utiliser un seul protocole (autrement dit, DD VTL Fibre Channel, DD Boost-over-Fibre Channel ou vDisk Fibre Channel) par point de terminaison. Pour les configurations de basculement sur incident, les points de terminaison secondaires doivent également être configurés pour avoir le même protocole que le point de terminaison primaire.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sous **Endpoints**, sélectionnez **Add** (signe +).
3. Dans la boîte de dialogue Add Endpoint, saisissez un nom pour le point de terminaison (entre 1 et 28 caractères). Le champ ne peut pas être vide ou contenir le mot « all », et ne doit pas comporter les caractères suivants : astérisque (*), point d'interrogation (?), barres obliques normales ou inverses (/, \) ou parenthèses ouvrantes ou fermantes [(,)].
4. Pour Endpoint Status, sélectionnez Enabled ou Disabled.
5. Si la virtualisation NPIV est activée, sélectionnez l'adresse système primaire dans la liste déroulante. L'adresse système primaire doit être différente de toute adresse système secondaire.
6. Si la virtualisation NPIV est activée, cochez la case appropriée en regard de l'adresse système secondaire pour Fails over to secondary system addresses.
7. Sélectionnez **OK**.

Configuration d'un point de terminaison

Après avoir ajouté un point de terminaison, vous pouvez le modifier à l'aide de la boîte de dialogue Configure Endpoint.

Remarque

Lors de l'utilisation de la virtualisation NPIV, il vous est recommandé d'utiliser un seul protocole (autrement dit, DD VTL Fibre Channel, DD Boost-over-Fibre Channel ou vDisk Fibre Channel) par point de terminaison. Pour les configurations de basculement sur incident, les points de terminaison secondaires doivent également être configurés pour avoir le même protocole que le point de terminaison primaire.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sous **Endpoints**, sélectionnez un point de terminaison, puis cliquez sur **Modify** (crayon).
3. Dans la boîte de dialogue Configure Endpoint, saisissez un nom pour le point de terminaison (entre 1 et 28 caractères). Le champ ne peut pas être vide ou contenir le mot « all », et ne doit pas comporter les caractères suivants : astérisque (*), point d'interrogation (?), barres obliques normales ou inverses (/, \) ou parenthèses ouvrantes ou fermantes [(,)].
4. Pour Endpoint Status, sélectionnez Enabled ou Disabled.
5. Sélectionnez l'adresse système primaire dans la liste déroulante. L'adresse système primaire doit être différente de toute adresse système secondaire.
6. Cochez la case appropriée en regard de l'adresse système secondaire pour Fails over to secondary system addresses.
7. Sélectionnez **OK**.

Modification de l'adresse système d'un point de terminaison

Vous pouvez modifier l'adresse système active d'un point de terminaison SCSI Target à l'aide de la commande `scsitarget endpoint modify`. Cela est utile si le point de terminaison est associé à une adresse système qui n'existe plus, par exemple, après la mise à niveau d'un contrôleur ou le déplacement d'un adaptateur HBA de contrôleur. Lorsque l'adresse système d'un point de terminaison est modifiée, toutes les

propriétés de ce point de terminaison, y compris WWPN et WWNN (nom de port universel et nom de nœud universel, respectivement), le cas échéant, sont conservées et utilisées avec la nouvelle adresse du système.

Dans l'exemple suivant, le point de terminaison ep-1 a été attribué à l'adresse système 5a, mais cette adresse système n'est plus valide. Un nouvel adaptateur HBA du Contrôleur a été ajouté à l'adresse système 10a. Le sous-système SCSI Target a automatiquement créé un nouveau point de terminaison ep-new pour l'adresse système récemment découverte. Puisqu'un seul point de terminaison peut être associé à une adresse système donnée, ep-new doit être supprimé, puis ep-1 doit être attribué à l'adresse système 10a.

Remarque

La mise en ligne d'un point de terminaison modifié prend un certain temps, selon l'environnement SAN, étant donné que les propriétés WWPN et WWNN ont été déplacées vers une autre adresse système. Vous devrez probablement effectuer une mise à jour de la segmentation SAN afin de refléter la nouvelle configuration.

Procédure

1. Affichez tous les points d'accès afin de vérifier les points d'accès à modifier :

   ```
   # scsitarget endpoint show list
   ```

2. Désactivez tous les points d'accès :

   ```
   # scsitarget endpoint disable all
   ```

3. Supprimez le nouveau point de terminaison devenu inutile, ep-new :

   ```
   # scsitarget endpoint del ep-new
   ```

4. Modifiez le point de terminaison que vous souhaitez utiliser, ep-1, en lui attribuant la nouvelle adresse système 10a :

   ```
   # scsitarget endpoint modify ep-1 system-address 10a
   ```

5. Activez tous les points d'accès :

   ```
   # scsitarget endpoint enable all
   ```

Activation d'un point de terminaison

L'activation d'un point de terminaison active le port uniquement s'il est actuellement désactivé. Autrement dit, vous n'êtes pas en mode NPIV.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sélectionnez **More Tasks** > **Endpoints** > **Enable**. Si tous les points de terminaison sont déjà activés, une notification s'affiche.
3. Dans la boîte de dialogue Enable Endpoints, sélectionnez un ou plusieurs points de terminaison dans la liste, puis cliquez sur **Next**.
4. Après la confirmation, cliquez sur **Next** pour terminer la tâche.

Désactivation d'un point de terminaison

La désactivation d'un point de terminaison ne désactive pas le port associé, sauf si tous les points de terminaison utilisant le port sont désactivés, autrement dit, si vous êtes hors mode NPIV.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sélectionnez **More Tasks** > **Endpoints** > **Disable**.
3. Dans la boîte de dialogue Disable Endpoints, sélectionnez un ou plusieurs points de terminaison dans la liste, puis cliquez sur **Next**. Si un point de terminaison est en cours d'utilisation, vous êtes averti que sa désactivation peut perturber le système.
4. Sélectionnez **Next** pour terminer la tâche.

Suppression d'un point de terminaison

Vous devrez probablement supprimer un point de terminaison lorsque le matériel sous-jacent n'est plus disponible. Toutefois, si le matériel sous-jacent est toujours présent ou redevient disponible, un nouveau point de terminaison est découvert automatiquement pour le matériel et configuré d'après les valeurs par défaut.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sélectionnez **More Tasks** > **Endpoints** > **Delete**.
3. Dans la boîte de dialogue Delete Endpoints, sélectionnez un ou plusieurs points de terminaison dans la liste, puis cliquez sur **Next**. Si un point de terminaison est en cours d'utilisation, vous êtes averti que sa suppression peut perturber le système.
4. Sélectionnez **Next** pour terminer la tâche.

Ajout d'un initiateur

Ajoutez des initiateurs pour fournir des clients de sauvegarde qui se connectent au système pour lire et écrire des données à l'aide du protocole FC (Fibre Channel). Un initiateur spécifique peut prendre en charge DD Boost over FC ou DD VTL, mais pas les deux. Il est possible de configurer 1 024 initiateurs au maximum pour un système DD.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sous Initiators, sélectionnez Add (signe +)
3. Dans la boîte de dialogue Add Initiator, saisissez le WWPN unique du port au format spécifié.
4. Saisissez un nom pour l'initiateur.
5. Sélectionnez la méthode d'adressage : **Auto** est utilisée pour l'adressage standard et **VSA** (Volume Set Addressing) est principalement utilisée pour l'adressage des bus, cibles et LUN virtuels.
6. Sélectionnez **OK**.

Équivalent de l'interface de ligne de commande (CLI)

```
# scsitarget group add My_Group initiator My_Initiator
```

Modification ou suppression d'un initiateur

Pour qu'un initiateur puisse être supprimé, il doit d'abord être mis hors ligne et n'être rattaché à aucun groupe. Si ce n'est pas le cas, vous recevez un message d'erreur et l'initiateur n'est pas supprimé. Vous devez supprimer tous les initiateurs d'un groupe

d'accès avant de pouvoir supprimer le groupe d'accès. Si un initiateur reste visible, il peut être redécouvert automatiquement.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sous Initiators, sélectionnez l'un des initiateurs. Si vous voulez le supprimer, sélectionnez Delete (X). Si vous voulez le modifier, sélectionnez Modify (crayon) pour afficher la boîte de dialogue Modify Initiator.
3. Modifiez le nom et la méthode d'adressage de l'initiateur [**Auto** est utilisé pour l'adressage standard et **VSA** (adressage d'ensembles de volumes) est principalement utilisé pour l'adressage des bus, cibles et LUN virtuels.]
4. Sélectionnez **OK**.

Recommandation pour définir les alias d'initiateur - CLI uniquement
Nous vous conseillons vivement de définir les alias d'initiateur d'une façon qui minimise la confusion et l'erreur humaine lors du processus de configuration.

```
# vtl initiator set alias NewAliasName wwpn 21:00:00:e0:8b:9d:0b:e8
# vtl initiator show
Initiator  Group    Status   WWNN                     WWPN                     Port
---------  -------  -------  -----------------------  -----------------------  ---
NewVTL     aussie1  Online   20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6a
                    Offline  20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6b

Initiator  Symbolic Port Name  Address Method
---------  ------------------  --------------
NewVTL                              auto
---------  ------------------  --------------
```

Définition d'une adresse matérielle (ID de boucle)

Certains logiciels de sauvegarde nécessitent que toutes les cibles de boucle privée aient une adresse matérielle (ID de boucle) ne créant pas de conflit avec un autre nœud. La plage de valeurs de l'ID de boucle est comprise entre 0 et 125.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sélectionnez **More Tasks** > **Set Loop ID**.
3. Dans la boîte de dialogue Set Loop ID, entrez l'ID de boucle (compris entre 0 et 125), puis sélectionnez **OK**.

Définition des options de basculement sur incident

Vous pouvez définir des options de basculement automatique sur incident et de retour arrière lorsque la fonction NPIV est activée.

Voici le comportement attendu pour le basculement sur incident du port Fibre Channel, par application :

- Le fonctionnement de DD Boost-over-Fibre Channel est censé continuer sans intervention de l'utilisateur lorsque les points de terminaison Fibre Channel effectuent un basculement sur incident.
- Le fonctionnement de DD VTL Fibre Channel est censé s'interrompre lorsque les points de terminaison DD VTL Fibre Channel effectuent un basculement sur incident. Vous devrez peut-être procéder à la découverte (c'est-à-dire, découverte du système d'exploitation et configuration des périphériques DD VTL) sur les initiateurs à l'aide du point de terminaison Fibre Channel concerné. Vous devrez redémarrer les opérations de sauvegarde et de restauration actives.

- Le fonctionnement de vDisk Fibre Channel est censé continuer sans intervention de l'utilisateur lorsque les points de terminaison Fibre Channel effectuent un basculement sur incident.

Le retour arrière automatique n'est pas garanti si tous les ports sont désactivés et réactivés par la suite (opération pouvant être déclenchée par l'administrateur), car l'ordre dans lequel les ports sont activés n'est pas spécifié.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources**.
2. Sélectionnez **More Tasks** > **Set Failover Options**.
3. Dans la boîte de dialogue Set Failover Options, saisissez des valeurs pour les champs Failover et Failover Delay (en secondes). Puis indiquez si vous souhaitez activer Automatic Failback avant de sélectionner **OK**.

Onglet Access Groups

L'onglet **Hardware** > **Fibre Channel** > **Access Groups** fournit des informations sur les groupes d'accès DD Boost et DD VTL. Sélectionnez le lien *View DD Boost Groups* ou *View VTL Groups* pour accéder aux pages DD Boost ou DD VTL.

Tableau 126 Groupes d'accès

Élément	Description
Group Name	Nom du groupe d'accès.
Service	Service pour ce groupe d'accès : DD Boost ou DD VTL.
Endpoints	Points d'accès associés à ce groupe d'accès.
Initiators	Initiateurs associés à ce groupe d'accès.
Number of Devices	Nombre de périphériques associés à ce groupe d'accès.

Différences de surveillance de la liaison FC entre les différentes versions de DD OS

Les différentes versions de DD OS gèrent la surveillance de la liaison FC (Fibre Channel) de façons différentes.

DD OS versions 5.3 et ultérieures
La surveillance des ports détecte un port FC au démarrage du système, puis émet une alerte si le port est activé et hors ligne. Pour supprimer l'alerte, désactivez un port inutilisé à l'aide des commandes `scsitarget port`.

DD OS versions 5.1 à 5.3
Si un port est hors ligne, une alerte vous informe que la liaison est interrompue. Cette alerte est gérée, ce qui signifie qu'elle reste active jusqu'à sa suppression. Cela se produit lorsque le port FC de DD VTL est en ligne ou désactivé. Si le port n'est pas en cours d'utilisation, désactivez-le à moins qu'il ne doive être surveillé.

DD OS versions 5.0 à 5.1
Si un port est hors ligne, une alerte vous informe que la liaison est interrompue. L'alerte n'est pas gérée, ce qui signifie qu'elle ne reste pas active et qu'elle n'apparaît pas dans la liste des alertes en cours. Si un port est en ligne, une alerte vous informe

que la liaison est établie. Si le port n'est pas en cours d'utilisation, désactivez-le à moins qu'il ne doive être surveillé.

DD OS versions 4.9 à 5.0
Un port FC doit faire partie d'un groupe DD VTL pour être surveillé.

CHAPITRE 14

Utilisation de DD Boost

Ce chapitre traite des sujets suivants :

À propos de Data Domain Boost

Data Domain Boost (DD Boost) garantit des performances optimales et une simplicité d'utilisation sans pareil grâce à son excellente intégration aux applications de sauvegarde et aux applications d'entreprise. DD Boost confie des parties du processus de déduplication au serveur de sauvegarde ou aux clients d'applications pour une déduplication côté client autorisant une sauvegarde et une restauration plus rapides et plus efficaces.

DD Boost est un produit facultatif qui nécessite une licence distincte pour fonctionner sur le système Data Domain. Vous pouvez acheter une clé de licence logicielle DD Boost pour un système Data Domain, directement à partir de Data Domain.

Remarque

Une licence spéciale, BLOCK-SERVICES-PROTECTPOINT, est disponible pour permettre aux clients d'utiliser les services en mode bloc de ProtectPoint et leur offrir les fonctionnalités de DD Boost sans une licence DD Boost. Si DD Boost est activé pour les clients ProtectPoint uniquement : en d'autres termes, si seule la licence BLOCK-SERVICES-PROTECTPOINT est installée, l'état de la licence indique que DD Boost est activé pour ProtectPoint uniquement.

DD Boost est composé de deux éléments : un composant qui s'exécute sur le serveur de sauvegarde et un autre qui s'exécute sur le système Data Domain.

- Dans le contexte de l'application de sauvegarde NetWorker, l'application de sauvegarde Avamar et d'autres applications de sauvegarde partenaires DD Boost, le composant qui s'exécute sur le serveur de sauvegarde (bibliothèques DD Boost) est intégré dans l'application de sauvegarde.
- Dans le contexte des applications de sauvegarde Symantec (NetBackup et Backup Exec) et du plug-in Oracle RMAN, vous devez télécharger une version appropriée du plug-in DD Boost qui est installé sur chaque serveur de média. Le plug-in DD Boost comprend les bibliothèques DD Boost à intégrer avec le serveur DD Boost qui s'exécute sur le système Data Domain.

L'application de sauvegarde (par exemple, Avamar, NetWorker, NetBackup ou Backup Exec) définit les règles qui déterminent le moment où les sauvegardes et les duplications se produisent. Les administrateurs gèrent les sauvegardes, les duplications et les restaurations à partir d'une seule console et peuvent utiliser toutes les fonctions de DD Boost, y compris le logiciel de réplication du WAN. L'application gère tous les fichiers (ensembles de données) du catalogue, y compris ceux créés par le système Data Domain.

Sur le système Data Domain, les unités de stockage que vous créez sont exposées à des applications de sauvegarde qui utilisent le protocole DD Boost. Pour les applications Symantec, les unités de stockage sont considérées comme des pools de disques. Pour NetWorker, les unités de stockage sont considérées comme des unités de stockage logiques (LSU). Une unité de stockage est une structure MTree. Par conséquent, elle prend en charge les paramètres de quota MTree. (Ne créez pas de structure MTree à la place d'une unité de stockage.)

Ce chapitre ne contient pas d'instructions d'installation. Consultez la documentation relative au produit que vous souhaitez installer. Par exemple, pour plus d'informations sur la configuration de DD Boost avec les applications de sauvegarde Symantec (NetBackup et Backup Exec), consultez le document *Data Domain Boost for OpenStorage Administration Guide*. Pour plus d'informations sur la façon de configurer

DD Boost avec une autre application, consultez la documentation spécifique de cette dernière.

Des informations complémentaires sur la configuration et la gestion de DD Boost sur le système Data Domain sont également disponibles dans les documents *Guide d'administration de Data Domain Boost for OpenStorage* (pour NetBackup et Backup Exec) et *Guide d'administration de Data Domain Boost pour l'intégration des partenaires* (pour les autres applications de sauvegarde).

Gestion de DD Boost avec DD System Manager

Accédez à la vue DD Boost dans DD System Manager.

Procédure

1. Sélectionnez **Data Management** > **File System**. Vérifiez que le système de fichiers est activé et qu'il fonctionne en vérifiant son état.
2. Sélectionnez **Protocols** > **DD Boost**.

   Si vous accédez à la page DD Boost sans licence, l'état indique que la licence DD n'est pas installée. Cliquez sur **Add License** et saisissez une licence valide dans la boîte de dialogue Add License Key.

   Remarque

   Une licence spéciale, BLOCK-SERVICES-PROTECTPOINT, est disponible pour permettre aux clients d'utiliser les services en mode bloc de ProtectPoint et leur offrir les fonctionnalités de DD Boost sans une licence DD Boost. Si DD Boost est activé pour les clients ProtectPoint uniquement : en d'autres termes, si seule la licence BLOCK-SERVICES-PROTECTPOINT est installée, l'état de la licence indique que DD Boost est activé pour ProtectPoint uniquement.

   Utilisez les onglets DD Boost (Settings, Active Connections, IP Network, Fibre Channel et Storage Units) pour gérer DD Boost.

Spécification des noms d'utilisateur de DD Boost

Un utilisateur de DD Boost est également un utilisateur de DD OS. Spécifiez un utilisateur de DD Boost en sélectionnant un nom d'utilisateur de DD OS existant ou en créant un nouveau nom d'utilisateur de DD OS et en faisant de ce nom un utilisateur de DD Boost.

Les applications de sauvegarde utilisent le nom d'utilisateur et le mot de passe DD Boost pour se connecter au système Data Domain. Vous devez configurer ces informations d'identification sur chaque serveur de sauvegarde qui se connecte à ce système. Le système Data Domain prend en charge une multitude d'utilisateurs DD Boost. Pour obtenir des informations complètes sur la configuration de DD Boost avec Symantec NetBackup et Backup Exec, reportez-vous au *Guide d'administration de Data Domain Boost for OpenStorage*. Pour plus d'informations sur la configuration de DD Boost avec d'autres applications, reportez-vous au *Guide d'administration de Data Domain Boost for OpenStorage* et à la documentation spécifique de l'application.

Procédure

1. Sélectionnez **Protocols** > **DD Boost**.
2. Sélectionnez **Add** (+) au-dessus de la liste Users with DD Boost Access.

   La boîte de dialogue Add User apparaît.

3. Pour sélectionner un utilisateur existant, sélectionnez son nom dans la liste déroulante.

   Si possible, sélectionnez un nom d'utilisateur dont les privilèges liés au rôle de gestion sont définis sur *none*.

4. Pour créer et choisir un nouvel utilisateur, sélectionnez **Create a new Local User**, puis procédez comme suit :

   a. Saisissez le nom du nouvel utilisateur dans le champ User.

      L'utilisateur doit être configuré dans l'application de sauvegarde pour se connecter au système Data Domain.

   b. Saisissez deux fois le mot de passe, dans les champs prévus à cet effet.

5. Cliquez sur **Add**.

Modification des mots de passe d'utilisateur DD Boost

Changez le mot de passe d'utilisateur DD Boost.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Settings**.
2. Sélectionnez un utilisateur dans la liste Users with DD Boost Access.
3. Cliquez sur le bouton **Edit** (icône de crayon) au-dessus de la liste des utilisateurs DD Boost.

   La boîte de dialogue Change Password s'affiche.

4. Saisissez deux fois le mot de passe, dans les zones prévues à cet effet.
5. Cliquez sur **Change**.

Suppression d'un nom d'utilisateur DD Boost

Supprimez un utilisateur de la liste d'accès DD Boost.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Settings**.
2. Sélectionnez l'utilisateur à supprimer dans la liste Users with DD Boost Access.
3. Cliquez sur **Remove** (X) au-dessus de la liste des utilisateurs DD Boost.

   La boîte de dialogue Remove User s'affiche.

4. Cliquez sur **Remove**.

   Une fois la suppression effectuée, l'utilisateur reste dans la liste d'accès DD OS.

Activation de DD Boost

Utilisez l'onglet DD Boost Settings pour activer DD Boost et pour sélectionner ou ajouter un utilisateur DD Boost.

Procédure

1. Sélectionnez **Protocols** > **DD Boost**.
2. Dans la zone DD Boost Status, cliquez sur **Enable**.

   La boîte de dialogue Enable DD Boost s'affiche.

3. Sélectionnez un nom d'utilisateur existant dans le menu, ou ajoutez un nouvel utilisateur en indiquant ses nom, mot de passe et rôle.

Configuration de Kerberos

Vous pouvez configurer Kerberos à l'aide de l'onglet DD Boost Settings.

Procédure

1. Sélectionnez **Protocols > DD Boost > Settings**.
2. Cliquez sur **Configure** dans la zone Kerberos Mode status.

   Cela a pour effet d'afficher l'onglet Authentication sous **Administration > Access**.

   Remarque

   Vous pouvez également activer Kerberos en accédant directement à l'authentification sous **Administration > Access** dans System Manager.

3. Sous Active Directory/Kerberos Authentication, cliquez sur **Configure**.

   La boîte de dialogue Active Directory/Kerberos Authentication s'affiche. Choisissez le type de KDC (Key Distribution Center) Kerberos à utiliser :

   - **Disabled**

     Remarque

     Si vous sélectionnez **Disabled**, les clients NFS n'auront pas recours à l'authentification Kerberos. Les clients CIFS, quant à eux, utilisent l'authentification par groupe de travail.

   - **Windows/Active Directory**

     Remarque

     Renseignez les champs Realm Name, Under Name et Password pour l'authentification Active Directory.

   - **Unix**

     a. Saisissez le nom de domaine ainsi que les noms d'hôte/l'adresse IP de l'un des trois serveurs KDC.

     b. Téléchargez le fichier keytab depuis un des serveurs KDC.

Désactivation de DD Boost

Désactiver DD Boost entraîne l'abandon de toutes les connexions actives au serveur de sauvegarde. Lorsque vous désactivez ou détruisez DD Boost, le service FC de DD Boost est également désactivé.

Avant de commencer

Vérifiez qu'aucune tâche n'est en cours d'exécution à partir de votre application de sauvegarde avant d'effectuer la désactivation.

Remarque

La réplication de fichiers démarrée par DD Boost entre deux restaurations Data Domain n'est pas annulée.

Procédure

1. Sélectionnez **Protocols** > **DD Boost**.
2. Dans la zone DD Boost Status, cliquez sur **Disable**.
3. Cliquez sur **OK** dans la boîte de dialogue de confirmation Disable DD Boost.

Affichage des unités de stockage DD Boost

Accédez à l'onglet Storage Units pour afficher et gérer les unités de stockage DD Boost.

L'onglet DD Boost Storage Unit :

- Répertorie les unités de stockage et fournit les informations suivantes pour chaque unité de stockage :

Tableau 127 Informations sur les unités de stockage

Élément	Description
Storage Unit	Nom de l'unité de stockage.
User	Utilisateur DD Boost détenant l'unité de stockage.
Quota Hard Limit	Pourcentage de limite de quota stricte utilisée.
Last 24 hr Pre-Comp	Quantité de données brutes de l'application de sauvegarde ayant été écrites au cours des dernières 24 heures.
Last 24 hr Post-Comp	Quantité de stockage utilisée après la compression au cours des dernières 24 heures.
Last 24 hr Comp Ratio	Taux de compression au cours des dernières 24 heures.
Weekly Avg Post-Comp	Quantité moyenne de stockage compressé utilisée dans les cinq dernières semaines.
Last Week Post-Comp	Quantité moyenne de stockage compressé utilisée au cours des sept derniers jours.
Weekly Avg Comp Ratio	Taux de compression moyen des cinq dernières semaines.
Last Week Comp Ratio	Taux de compression moyen des sept derniers jours.

- Vous permet de créer, modifier et supprimer des unités de stockage.
- Affiche quatre onglets associés pour une unité de stockage sélectionnée dans la liste : Storage Unit, Space Usage, Daily Written et Data Movement.

  Remarque

  L'onglet Data Movement n'est disponible que si une licence facultative Data Domain Extended Retention (anciennement DD Archiver) ou Data Domain Cloud Tier (DD Cloud Tier) est installée.

- Vous pouvez accéder à **Replication** > **On-Demand** > **File Replication** lorsque vous cliquez sur le lien **View DD Boost Replications**.

Remarque

Une licence DD Replicator est nécessaire pour que DD Boost affiche des onglets autres que l'onglet File Replication.

Création d'une unité de stockage

Vous devez créer au moins une unité de stockage sur le système Data Domain et un utilisateur de DD Boost doit être attribué à cette unité de stockage. Utilisez l'onglet Storage Units pour créer une unité de stockage.

Chaque unité de stockage est un sous-répertoire de niveau supérieur du répertoire `/data/col1` ; il n'existe aucune hiérarchie entre les unités de stockage.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Storage Units**.
2. Cliquez sur **Create** (+).

   La boîte de dialogue Create Storage Unit s'affiche.

3. Saisissez le nom de l'unité de stockage dans le champ Name.

   Chaque nom de l'unité de stockage doit être unique. Les noms d'unité de stockage peuvent contenir jusqu'à 50 caractères. Les caractères suivants sont acceptés :

   - Lettres majuscules et minuscules : A-Z, a-z
   - Chiffres : 0-9
   - Espace intégré.

     Remarque

     Le nom de l'unité de stockage doit être placé entre guillemets doubles (") si le nom contient un espace intégré.

   - Virgule (,)
   - Point (.), tant qu'il ne précède pas le nom
   - Point d'exclamation (!)
   - Dièse (#)
   - Dollar ($)
   - Signe de pourcentage (%)
   - Signe plus (+)
   - Arobase (@)
   - Signe égal (=)
   - Esperluette (&)
   - Point-virgule (;)
   - Parenthèse [(et)]
   - Crochets ([et])
   - Accolades ({et})
   - Accent circonflexe (^)

- Tilde (~)
- Apostrophe (signe droit et unique)
- Guillemet simple incliné (’)
- Signe moins (-)
- Caractère de soulignement (_)

4. Pour sélectionner un nom d’utilisateur existant qui aura accès à cette unité de stockage, sélectionnez le nom de l’utilisateur dans la liste déroulante.

   Si possible, sélectionnez un nom d’utilisateur dont les privilèges liés au rôle de gestion sont définis sur *none*.

5. Pour créer et sélectionner un nouveau nom d’utilisateur qui aura accès à cette unité de stockage, sélectionnez **Create a new Local User** puis :

   a. Saisissez le nom du nouvel utilisateur dans la zone User.

      L’utilisateur doit être configuré dans l’application de sauvegarde pour se connecter au système Data Domain.

   b. Saisissez deux fois le mot de passe, dans les zones prévues à cet effet.

6. Pour définir les restrictions d’espace de stockage afin d’empêcher une unité de stockage de consommer l’espace excédentaire : saisissez un quota de limite souple ou stricte, ou une limite stricte et une limite souple. Lorsqu’une limite souple est définie, une alerte est envoyée quand la taille de l’unité de stockage dépasse la limite fixée, mais des données peuvent encore y être écrites. Les données ne peuvent pas être écrites sur l’unité de stockage lorsque la limite stricte est atteinte.

   Remarque

   Les limites de quota sont des valeurs précompressées. Pour définir des limites de quota, sélectionnez **Set to Specific Value** et saisissez la valeur. Sélectionnez une unité de mesure : Mio, Gio, Tio ou Pio.

   Remarque

   Si vous définissez une limite souple et une limite stricte, la limite souple d’un quota ne peut pas dépasser sa limite stricte.

7. Cliquez sur **Create**.
8. Répétez ces étapes pour chaque système sur lequel Data Domain Boost est activé.

Affichage des informations sur les unités de Stockage et

Depuis l’onglet DD Boost, vous pouvez sélectionner une unité de stockage et accéder aux onglets Storage Unit, Space Usage, Daily Written et Data Movement correspondants.

Onglet Storage Unit
L’onglet Storage Unit présente des informations détaillées sur l’unité de stockage sélectionnée dans ses volets Summary et Quota. Le volet Snapshot affiche des détails sur un snapshot, vous permettant de créer de nouveaux snapshots et plannings, et contient un lien vers l’onglet **Data Management** > **Snapshots**.

- Le volet Summary contient des informations récapitulatives pour l'unité de stockage sélectionnée.

  Tableau 128 Volet Summary

Élément du volet Summary	Description
Total Files	Nombre total d'images de fichiers sur l'unité de stockage. Pour obtenir des informations de compression, que vous pouvez télécharger dans un fichier log, cliquez sur le lien Download Compression Details. La génération du fichier peut prendre quelques minutes. Une fois le fichier généré, cliquez sur Download.
Full Path	`/data/col1/filename`
Status	R : lecture ; W : écriture ; Q: quota défini
Pre-Comp Used	Quantité de stockage précompressé déjà utilisée.

- Le volet Quota contient des informations de quota pour l'unité de stockage sélectionnée.

  Tableau 129 Volet Quota

Élément du volet Quota	Description
Quota Enforcement	Activé ou désactivé. Lorsque vous cliquez sur Quota, vous accédez à l'onglet **Data Management** > **Quota**, où vous pouvez configurer des quotas.
Pre-Comp Soft Limit	Valeur actuelle du quota souple défini pour l'unité de stockage.
Pre-Comp Hard Limit	Valeur actuelle du quota strict défini pour l'unité de stockage.
Quota Summary	Pourcentage de limite stricte utilisé.

  Pour modifier les limites souple et stricte des données précompressées, affichées sous l'onglet :

  1. Cliquez sur le lien **Quota** dans le panneau Quota.
  2. Dans la boîte de dialogue Configure Quota, saisissez les valeurs des quotas souple et strict, puis sélectionnez l'unité de mesure : Mio, Gio, Tio ou Pio. Cliquez sur **OK**.

- Snapshots
  Le volet Snapshots affiche des informations sur les snapshots de l'unité de stockage.

  Tableau 130 Volet Snapshots

Élément	Description
Total Snapshots	Nombre total de snapshots créés pour cette structure MTree. Un total de 750 snapshots peut être créé pour chaque structure MTree.
Expired	Nombre de snapshots de cette structure MTree qui ont été marqués pour suppression, mais qui n'ont pas encore été supprimés par l'opération de nettoyage.

Tableau 130 Volet Snapshots (suite)

Élément	Description
Unexpired	Nombre de snapshots de cette structure MTree qui sont marqués pour être conservés.
Oldest Snapshot	Date du plus ancien snapshot de cette structure MTree.
Newest Snapshot	Date du snapshot le plus récent de cette structure MTree.
Next Scheduled	Date du prochain snapshot planifié.
Assigned Snapshot Schedules	Nom du planning de snapshots affecté à cette structure MTree.

À l'aide du volet Snapshots, vous pouvez :

- attribuer un planning des snapshots à l'unité de stockage sélectionnée : Cliquez sur **Assign Schedules**. Cochez la case correspondant au planning. Cliquez sur **OK**, puis sur **Close**.
- Créez un planning : Cliquez sur **Assign Snapshot Schedules** > **Create Snapshot Schedule**. Saisissez le nom du nouveau planning.

  Remarque

  Le nom de snapshot peut uniquement contenir des lettres, des chiffres, _, -, `%d`(jour numérique du mois : 01 à 31), `%a` (nom abrégé du jour de la semaine), `%m` (mois numérique de l'année : 01 à 12), `%b` (nom de mois abrégé), `%y` (année, deux chiffres), `%Y` (année, quatre chiffres), `%H` (heure : 00 à 23), et `%M` (minute : 00 à 59), suivant le modèle indiqué dans la boîte de dialogue. Saisissez le nouveau modèle, puis cliquez sur **Validate Pattern & Update Sample**. Cliquez sur **Next**.

  - Sélectionnez quand le planning doit être exécuté : toutes les semaines, tous les jours (ou certains jours sélectionnés), certains jours de chaque mois que vous sélectionnez en cliquant sur cette date dans le calendrier ou le dernier jour du mois. Cliquez sur **Next**.
  - Saisissez les heures de la journée auxquelles le planning doit être exécuté : Sélectionnez At Specific Times ou In Intervals. Si vous sélectionnez une heure spécifique, sélectionnez-la dans la liste. Cliquez sur Add (**+**) pour ajouter une heure (au format 24 heures). Pour les intervalles, sélectionnez In Intervals et définissez les heures de début et de fin, ainsi que la fréquence (Every), comme toutes les huit heures, par exemple. Cliquez sur **Next**.
  - Saisissez la durée de rétention des snapshots en jours, mois ou années. Cliquez sur **Next**.
  - Vérifiez le récapitulatif de votre configuration. Cliquez sur **Back** pour modifier l'une des valeurs. Cliquez sur **Finish** pour créer le planning.

- Cliquez sur le lien Snapshots pour accéder à l'onglet **Data Management** > **Snapshots**.

Onglet Space Usage

Le graphique de l'onglet Space Usage offre une représentation visuelle de l'utilisation des données pour l'unité de stockage au fil du temps.

- Pour afficher un encadré contenant les données correspondant à un point, cliquez sur ce point sur le graphique.
- Pour ouvrir la boîte de dialogue d'impression standard, cliquez sur **Print** (au bas du graphique).
- Pour afficher le graphique dans une nouvelle fenêtre de navigateur, cliquez sur **Show in new window**.

Deux types de données de graphique s'affichent. Logical Space Used (Pre-Compression) et Physical Capacity Used (Post-Compression).

Onglet Daily Written
Le graphique de la vue Daily Written (Données écrites quotidiennement) présente visuellement les données écrites chaque jour dans le système au cours d'une certaine période, comprise entre 7 et 120 jours et que vous pouvez sélectionner. Les volumes de données sont présentés dans le temps avant et après compression.

Onglet Data Movement
Un graphique au même format que le graphique des données écrites quotidiennement (Daily Written) présente le volume d'espace disque déplacé vers la zone de stockage DD Extended Retention (si la licence DD Extended Rentention est activée).

Modification d'une unité de stockage

Utilisez la boîte de dialogue Modify Storage Unit pour renommer une unité de stockage, changer d'utilisateur, créer et sélectionner un nouvel utilisateur, et modifier les paramètres de quota.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Storage Units**.
2. Dans la liste des unités de stockage, sélectionnez l'unité de stockage à modifier.
3. Cliquez sur l'icône représentant un crayon.

   La boîte de dialogue Modify Storage Unit s'affiche.

4. Pour renommer l'unité de stockage, modifiez le contenu du champ **Name**.
5. Pour sélectionner un autre utilisateur existant, sélectionnez le nom de l'utilisateur dans la liste déroulante.

   Si possible, sélectionnez un nom d'utilisateur dont les privilèges liés au rôle de gestion sont définis sur *none*.

6. Pour créer et choisir un nouvel utilisateur, sélectionnez **Create a new Local User**, puis procédez comme suit :
   a. Saisissez le nom du nouvel utilisateur dans la zone User.

      L'utilisateur doit être configuré dans l'application de sauvegarde pour se connecter au système Data Domain.

   b. Saisissez deux fois le mot de passe, dans les zones prévues à cet effet.
7. Modifiez les paramètres de quota comme il convient.

   Pour définir les restrictions d'espace de stockage afin d'empêcher une unité de stockage de consommer l'espace excédentaire : saisissez un quota de limite souple ou stricte, ou une limite stricte et une limite souple. Lorsqu'une limite souple est définie, une alerte est envoyée quand la taille de l'unité de stockage dépasse la limite fixée, mais des données peuvent encore y être écrites. Les

données ne peuvent pas être écrites sur l'unité de stockage lorsque la limite stricte est atteinte.

Remarque

Les limites de quota sont des valeurs précompressées. Pour définir des limites de quota, sélectionnez **Set to Specific Value** et saisissez la valeur. Sélectionnez une unité de mesure : Mio, Gio, Tio ou Pio.

Remarque

Si vous définissez une limite souple et une limite stricte, la limite souple d'un quota ne peut pas dépasser sa limite stricte.

8. Cliquez sur **Modifier**.

Changement de nom d'une unité de stockage

Utilisez la boîte de dialogue Modify Storage Units pour renommer une unité de stockage.

Cette opération a pour effet de changer le nom de l'unité de stockage, mais conserve les éléments suivants :

- Propriété du nom d'utilisateur
- Configuration de la limite de flux de données
- Configuration du quota de capacité et taille physique indiquée
- Association AIR sur le système Data Domain local

Procédure

1. Accédez à **Protocols** > **DD Boost** > **Storage Units**.
2. Dans la liste des unités de stockage, sélectionnez l'unité de stockage à renommer.
3. Cliquez sur l'icône représentant un crayon.

   La boîte de dialogue Modify Storage Unit s'affiche.

4. Modifiez le contenu du champ **Name**.
5. Cliquez sur **Modifier**.

Suppression d'une unité de stockage

Utilisez l'onglet Storage Units pour supprimer une unité de stockage de votre système Data Domain. Cette opération a pour effet de supprimer l'unité de stockage, ainsi que toutes les images qu'elle contient, de votre système Data Domain.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Storage Units**.
2. Sélectionnez l'unité de stockage à supprimer de la liste.
3. Cliquez sur **Delete** (X).
4. Cliquez sur **OK**.

Résultats

L'unité de stockage est supprimée de votre système Data Domain. Vous devez également supprimer manuellement les entrées du catalogue d'applications de sauvegarde qui lui sont associées.

Annulation de la suppression d'une unité de stockage

Utilisez l'onglet Storage Units pour annuler la suppression d'une unité de stockage.

Cette opération a pour effet de restaurer une unité de stockage supprimée, ainsi que les éléments suivants :

- Propriété du nom d'utilisateur
- Configuration de la limite de flux de données
- Configuration du quota de capacité et taille physique indiquée
- Association AIR sur le système Data Domain local

Remarque

Les unités de stockage supprimées sont disponibles jusqu'à la prochaine exécution de la commande `filesys clean`.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Storage Units** > **More Tasks** > **Undelete Storage Unit...**.
2. Dans la boîte de dialogue Undelete Storage Units, sélectionnez la ou les unités de stockage dont vous souhaitez annuler la suppression.
3. Cliquez sur **OK**.

Sélection des options de DD Boost

Utilisez la boîte de dialogue Set DD Boost Options pour définir les paramètres de traitement distribué des segments, de sauvegardes synthétiques virtuelles, d'optimisation de bande passante faible pour la réplication des fichiers, de chiffrement de la réplication de fichiers et de réseau préféré pour la réplication des fichiers (IPv4 ou IPv6).

Procédure

1. Pour afficher les paramètres des options DD Boost, sélectionnez **Protocols** > **DD Boost** > **Settings** > **Advanced Options**.
2. Pour modifier les paramètres, sélectionnez **More Tasks** > **Set Options**.

   La boîte de dialogue Set DD Boost Options s'affiche.

3. Sélectionnez une option à activer.
4. Désélectionnez toute option devant être désactivée.

   Pour désélectionner une option File Replication Network Preference, sélectionnez l'autre option.

5. Définissez les options de sécurité de DD Boost.

   a. Sélectionnez une valeur pour le mode d'authentification (**Authentication Mode**).

- None
- Two-way
- Two-way Password

b. Sélectionnez une valeur pour la puissance de chiffrement (**Encryption Strength**) :

- None
- Medium
- High

Le système Data Domain compare le mode d'authentification et la puissance de chiffrement définis globalement au mode d'authentification et à la puissance de chiffrement définis pour chaque client afin de calculer le mode d'authentification et la puissance de chiffrement efficaces. Le système n'utilise pas le mode d'authentification le plus élevé d'une entrée et les paramètres de chiffrement les plus élevés d'une autre entrée. Le mode d'authentification et la puissance de chiffrement efficaces proviennent de l'entrée unique qui fournit le mode d'authentification le plus élevé.

6. Cliquez sur **OK**.

Remarque

Vous pouvez également gérer le traitement distribué des segments via les commandes `ddboost option`, qui sont décrites en détail dans le *Guide de référence des commandes de Data Domain Operating System*.

Traitement distribué des segments

Le traitement distribué des segments accroît le débit de sauvegarde dans presque tous les cas en supprimant la transmission de données dupliquées entre le serveur de média et le système Data Domain.

Vous pouvez gérer le traitement distribué des segments via les commandes `ddboost option`, qui sont décrites en détail dans le *Guide de référence des commandes de Data Domain Operating System*.

Remarque

Le traitement distribué des segments est activé par défaut avec des configurations Data Domain Extended Retention (anciennement Data Domain Archiver) et ne peut pas être désactivé.

Sauvegardes synthétiques virtuelles

Une sauvegarde complète synthétique virtuelle est la combinaison de la dernière sauvegarde (synthétique ou complète) et de toutes les sauvegardes incrémentielles suivantes. Les sauvegardes synthétiques virtuelles sont activées par défaut.

Optimisation de bande passante faible

Si vous utilisez la réplication des fichiers sur un WAN (réseau à faible bande passante), vous pouvez augmenter la vitesse de réplication à l'aide de l'optimisation de bande passante faible. Cette fonction permet une compression supplémentaire lors du

transfert des données. La compression de bande passante faible est disponible pour les systèmes Data Domain disposant d'une licence de réplication installée.

L'optimisation de la bande passante faible, qui est désactivée par défaut, est conçue pour une utilisation sur des réseaux dont la bande passante agrégée est inférieure à 6 Mbit/s. Ne choisissez pas cette option si vous avez besoin de performances maximales en écriture sur le système de fichiers.

Remarque

Vous pouvez également gérer l'optimisation de bande passante faible à l'aide des commandes `ddboost file-replication` , lesquelles sont décrites en détail dans le *Guide de référence des commandes de Data Domain Operating System*.

Chiffrement de la réplication de fichiers

Vous pouvez chiffrer le flux de réplication des données en activant l'option de chiffrement de la réplication de fichiers DD Boost.

Remarque

Si le chiffrement de la réplication de fichiers DD Boost est utilisé sur des systèmes sans l'option Data at Rest, il doit être activé pour les systèmes source et de destination.

Configuration du port TCP de réplication de fichiers gérés
Pour la réplication de fichiers gérés DD Boost, utilisez le même port d'écoute universel sur les systèmes Data Domain source et cible. Pour configurer le port d'écoute, utilisez la commande `replication option` en procédant comme indiqué dans le *Guide de référence des commandes de Data Domain Operating System*.

Réseau préféré pour la réplication des fichiers

Utilisez l'option File Replication Network Preference pour définir le type de réseau préféré (IPv4 ou IPv6) pour la réplication des fichiers DD Boost.

Gestion des certificats pour DD Boost

Un certificat d'hôte permet aux programmes clients DD Boost de vérifier l'identité du système lors de l'établissement d'une connexion. Les certificats AC identifient les autorités de certification à considérer comme fiables pour le système. Les rubriques de cette section expliquent comment gérer les hôtes et les certificats AC pour DD Boost.

Ajout d'un certificat d'hôte pour DD Boost

Ajoutez un certificat d'hôte à votre système. DD OS prend en charge un certificat d'hôte pour DD Boost.

Procédure

1. Si vous n'avez pas encore demandé de certificat d'hôte, demandez-en un auprès d'une autorité de certification de confiance.
2. Lorsque vous recevez un certificat d'hôte, copiez-le ou déplacez-le sur l'ordinateur à partir duquel vous exécutez DD Service Manager.
3. Démarrez DD System Manager sur le système auquel vous souhaitez ajouter un certificat d'hôte.

Remarque

DD System Manager ne prend en charge la gestion des certificats que sur le système de gestion (qui est le système exécutant DD System Manager).

4. Sélectionnez **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**.

Remarque

Si vous tentez de gérer les certificats à distance sur un système géré, DD System Manager affiche un message d'information en haut de la boîte de dialogue de gestion des certificats. Pour gérer les certificats d'un système, vous devez démarrer DD System Manager sur ce système.

5. Dans la zone Host Certificate, cliquez sur **Add**.
6. Pour ajouter un certificat d'hôte contenu dans un fichier .p12, procédez comme suit :
   a. Sélectionnez **I want to upload the certificate as a .p12 file**.
   b. Entrez la phrase de passe dans la zone **Password**.
   c. Cliquez sur **Browse**, puis sélectionnez le fichier de certificat d'hôte à télécharger sur le système.
   d. Cliquez sur **Add.**
7. Pour ajouter un certificat d'hôte contenu dans un fichier .pem, procédez comme suit :
   a. Sélectionnez **I want to upload the public key as a .pem file and use a generated private key**.
   b. Cliquez sur **Browse**, puis sélectionnez le fichier de certificat d'hôte à télécharger sur le système.
   c. Cliquez sur **Add.**

Ajout de certificats AC pour DD Boost

Ajoutez un certificat d'une autorité de certification (AC) de confiance sur votre système. DD OS prend en charge une multitude de certificats pour des autorités de certification de confiance.

Procédure

1. Procurez-vous un certificat pour l'autorité de certification de confiance.
2. Copiez ou déplacez le certificat AC de confiance sur l'ordinateur à partir duquel vous exécutez DD Service Manager.
3. Démarrez DD System Manager sur le système auquel vous souhaitez ajouter le certificat AC.

Remarque

DD System Manager ne prend en charge la gestion des certificats que sur le système de gestion (qui est le système exécutant DD System Manager).

4. Sélectionnez **Protocols** > **DD Boost** > **More Tasks** > **Manage Certificates...**.

Remarque

Si vous tentez de gérer les certificats à distance sur un système géré, DD System Manager affiche un message d'information en haut de la boîte de dialogue de gestion des certificats. Pour gérer les certificats d'un système, vous devez démarrer DD System Manager sur ce système.

5. Dans la zone CA Certificate, cliquez sur **Add**.

   La boîte de dialogue Add CA Certificate for DD Boost s'affiche.

6. Pour ajouter un certificat AC contenu dans un fichier .pem, procédez comme suit :
   a. Sélectionnez **I want to upload the certificate as a .pem file**.
   b. Cliquez sur **Browse**, sélectionnez le fichier de certificat à télécharger sur le système, puis cliquez sur **Open**.
   c. Cliquez sur **Add.**
7. Pour ajouter un certificat AC par copier-coller, procédez comme suit :
   a. Copiez le texte du certificat dans le presse-papiers à l'aide des commandes de votre système d'exploitation.
   b. Sélectionnez **I want to copy and paste the certificate text**.
   c. Collez le texte du certificat dans la zone en dessous de la sélection copier-coller.
   d. Cliquez sur **Add.**

Gestion de l'accès et du chiffrement des clients DD Boost

Utilisez l'onglet DD Boost Settings pour désigner les clients ou l'ensemble de clients susceptibles d'établir une connexion DD Boost avec le système Data Domain et indiquer si le client utilisera ou non le chiffrement. Par défaut, le système est configuré pour accorder un accès à tous les clients, sans chiffrement.

Remarque

L'activation du chiffrement à la volée aura un impact sur les performances du système.

Remarque

DD Boost offre des options globales pour l'authentification et le chiffrement en vue de défendre votre système contre les attaques de type Man-in-the-middle (MITM). Vous spécifiez les paramètres d'authentification et de chiffrement à l'aide de l'interface utilisateur ou des commandes de la CLI sur le système Data Domain. Consultez le *Guide de référence des commandes de Data Domain 6.1* et la section Ajout d'un client DD Boost à la page 369, ou le *Guide d'administration de Data Domain Boost for OpenStorage 3.4* pour plus de détails.

Ajout d'un client DD Boost

Créez un client DD Boost autorisé et indiquez s'il utilisera ou non le chiffrement.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Settings**.
2. Dans la section Allowed Clients, cliquez sur **Create (+).**

   La boîte de dialogue Add Allowed Client s'affiche.

3. Saisissez le nom d'hôte du client.

   Il peut s'agir d'un nom de domaine complet (ex. : host1.emc.com) ou d'un nom d'hôte avec un caractère générique (ex. : *.emc.com).

4. Sélectionnez la puissance de chiffrement.

   Vous avez le choix entre trois options : None (pas de chiffrement), Medium (AES128-SHA1) ou High (AES256-SHA1).

5. Sélectionnez le mode d'authentification.

   Vous avez le choix entre quatre options : One Way, Two Way, Two Way Password ou Anonymous.

6. Cliquez sur **OK**.

Modification d'un client DD Boost

Changez le nom, la puissance de chiffrement et le mode d'authentification d'un client DD Boost autorisé.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Settings**.
2. Dans la liste Allowed Clients list, sélectionnez le client à modifier.
3. Cliquez sur le bouton **Edit**, qui affiche une icône représentant un crayon.

   La boîte de dialogue Modify Allowed Clients s'affiche.

4. Pour changer le nom d'un client, modifiez le texte correspondant.
5. Pour changer la puissance de chiffrement, sélectionnez l'option correspondante.

   Vous avez le choix entre trois options : None (pas de chiffrement), Medium (AES128-SHA1) ou High (AES256-SHA1).

6. Pour changer le mode d'authentification, sélectionnez l'option correspondante.

   Vous avez le choix entre trois options : One Way (unidirectionnel), Two Way (bidirectionnel) ou Anonymous (anonyme).

7. Cliquez sur **OK**.

Suppression d'un client DD Boost

Supprimez un client DD Boost autorisé.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Settings**.
2. Sélectionnez le client dans la liste.
3. Cliquez sur **Delete (X)**.

   La boîte de dialogue Delete Allowed Clients s'affiche.

4. Confirmez et sélectionnez le nom du client. Cliquez sur **OK**.

À propos des groupes d'interfaces

La fonction IFGROUP vous permet de combiner plusieurs liaisons Ethernet au sein d'un groupe et d'enregistrer uniquement une interface sur le système Data Domain auprès de l'application de sauvegarde. La bibliothèque DD Boost Library négocie avec le système Data Domain pour obtenir l'interface cible des données la plus appropriée. L'équilibrage de charge garantit un débit plus élevé vers le système Data Domain.

La configuration d'un groupe d'interfaces crée, au sein du système Data Domain, un réseau privé comprenant des adresses IP indiquées en tant que groupe. Les clients sont affectés à un groupe unique et l'interface du groupe applique l'équilibrage de charge pour optimiser le transfert de données et accroître la fiabilité.

Par exemple, dans un environnement Symantec NetBackup, les clients du serveur de média utilisent une seule adresse IP de réseau public pour accéder au système Data Domain. Toutes les communications avec le système Data Domain sont initiées via cette connexion IP gérée configurée sur le serveur NetBackup.

Si un groupe d'interfaces est configuré, lorsque le système Data Domain reçoit les données des clients du serveur de média, la charge du transfert de données est équilibrée et le transfert est distribué sur toutes les interfaces du groupe, ce qui permet un débit supérieur en entrée et en sortie, notamment pour les clients qui utilisent plusieurs connexions de 1 GigE.

La charge du transfert de données est équilibrée en fonction du nombre de connexions inachevées sur les interfaces. Seules les connexions destinées aux tâches de sauvegarde et de restauration ont une charge équilibrée. Reportez-vous au chapitre Connexions actives pour obtenir plus d'informations sur le nombre de connexions inachevées sur les interfaces d'un groupe.

En cas de défaillance d'une interface du groupe, toutes les tâches en cours de transfert vers cette interface sont automatiquement reprises sur les liaisons opérationnelles fonctionnelles (à l'insu des applications de sauvegarde). Toutes les tâches qui sont démarrées après cette défaillance sont également acheminées vers une interface fonctionnelle dans le groupe. Si le groupe est désactivé, ou en cas d'échec d'une tentative pour effectuer une restauration sur une autre interface, l'IP gérée est utilisée pour la restauration. En cas de défaillance dans un groupe, les interfaces d'un autre groupe ne sont pas utilisées.

Tenez compte des points suivants lors de la gestion des groupes d'interfaces.

- L'adresse IP doit être configurée sur le système Data Domain, et son interface doit être activée. Pour vérifier la configuration de l'interface, sélectionnez la page **Hardware** > **Ethernet** > **Interfaces** et recherchez les ports libres. Consultez le chapitre `net` du *Guide de référence des commandes de Data Domain Operating System* ou du document *Guide de configuration initiale de Data Domain Operating System* pour obtenir des informations sur la configuration d'une adresse IP pour une interface.
- Vous pouvez exécuter les commandes `ifgroup` pour gérer les groupes d'interfaces ; ces commandes sont décrites, de façon détaillée, dans le *Guide de référence des commandes de Data Domain Operating System*.
- Les groupes d'interfaces offrent une prise en charge complète des adresses IPv6 statiques, offrant les mêmes fonctions aux adresses IPv6 et IPv4. Les connexions client IPv4 et IPv6 simultanées sont autorisées. Un client connecté avec IPv6 voit uniquement les interfaces ifgroup IPv6. Un client connecté avec IPv4 voit uniquement les interfaces ifgroup IPv4. Les ifgroups individuels incluent toutes les adresses IPv4 ou toutes les adresses IPv6. Pour plus d'informations, consultez le

document *Guide d'administration de Data Domain Boost pour l'intégration des partenaires* ou le *Guide d'administration de Data Domain Boost for OpenStorage*.

- Les interfaces configurées sont répertoriées dans Active Connections, au bas de la page Activities.

Remarque

Reportez-vous à la rubrique Utilisation de DD Boost sur des systèmes haute disponibilité à la page 384 pour obtenir des informations importantes sur l'utilisation des groupes d'interfaces avec des systèmes haute disponibilité.

Les rubriques suivantes expliquent comment gérer les groupes d'interfaces.

Interfaces

IFGROUP gère des interfaces physiques et virtuelles.

Une interface IFGROUP fait partie d'un seul IFGROUP *<group-name>* et peut être composée d'un des éléments suivants :

- Interface physique telle que `eth0a`
- Interface virtuelle, créée pour le basculement de lien sur incident ou l'agrégation de liens, telle que `veth1`
- Interface d'alias virtuelle telle que `eth0a:2` ou `veth1:2`
- Interface VLAN virtuelle telle que `eth0a.1` ou `veth1.1`
- Dans un IFGROUP *<group-name>*, toutes les interfaces doivent se trouver sur des interfaces uniques (Ethernet, Virtual Ethernet) pour assurer le basculement sur incident en cas d'erreur réseau.

Un IFGROUP assure la prise en charge complète des adresses IPv6 statiques, offrant les mêmes fonctions aux adresses IPv6 et IPv4. Les connexions client IPv4 et IPv6 simultanées sont autorisées. Un client connecté avec IPv6 voit uniquement les interfaces IFGROUP IPv6. Un client connecté avec IPv4 voit uniquement les interfaces IFGROUP IPv4. Les IFGROUPS individuels incluent toutes les adresses IPv4 ou toutes les adresses IPv6.

Pour plus d'informations, consultez le *Guide d'administration de Data Domain Boost pour l'intégration des partenaires* ou le *Guide d'administration de Data Domain Boost for OpenStorage*.

Application de force de l'interface

IFGROUP permet d'imposer une connectivité réseau privée pour éviter qu'une tâche victime d'erreurs réseau se reconnecte sur le réseau public.

Lorsque la contrainte d'interface est activée, une tâche ayant échoué peut uniquement réessayer sur une autre adresse IP de réseau privé. La contrainte d'interface est uniquement disponible pour les clients utilisant des interfaces IFGROUP.

Par défaut, cette fonction est désactivée (FALSE). Pour activer la contrainte d'interface, vous devez ajouter le paramètre suivant au registre système :

`system.ENFORCE_IFGROUP_RW=TRUE`

Après avoir ajouté cette entrée au registre, vous devez exécuter une commande `filesys restart` pour appliquer le paramètre.

Pour plus d'informations, consultez le *Guide d'administration de Data Domain Boost pour l'intégration des partenaires* ou le *Guide d'administration de Data Domain Boost for OpenStorage*.

Clients

IFGROUP gère différents formats de dénomination pour les clients. La sélection des clients tient compte de l'ordre de priorité spécifié.

Un client IFGROUP fait partie d'un seul ifgroup *<group-name>* et peut être composé d'un des éléments suivants :

- Un nom de domaine complet (FQDN) tel que ddboost.datadomain.com
- Un hôte partiel, qui permet d'effectuer une recherche sur les premiers caractères *n* du nom d'hôte. Par exemple, lorsque n=3, les formats valides sont `rtp_.*emc.com` et `dur_.*emc.com`. Cinq valeurs différentes de *n* (1-5) sont prises en charge.
- Des caractères génériques tels que `*.datadomain.com` ou « * »
- Un nom de client abrégé, tel que ddboost
- Une plage IP publique du client, par exemple 128.5.20.0/24

Avant le traitement en lecture ou écriture, le client fait la demande d'une adresse IP IFGROUP auprès du serveur. Pour sélectionner l'association IFGROUP du client, les informations client sont évaluées en fonction de l'ordre de priorité.

1. Une adresse IP du système Data Domain connecté. Si une connexion a déjà été établie entre le client et le système Data Domain, et si la connexion existe sur l'interface de l'IFGROUP, le client pourra alors accéder aux interfaces IFGROUP.
2. Une plage IP du client connecté. Une vérification du masque IP est réalisée par rapport à l'adresse IP source du client. Si cette dernière correspond au masque de la liste de clients IFGROUP, le client pourra alors accéder aux interfaces IFGROUP.
   - Pour IPv4, vous pouvez sélectionner cinq masques ayant des plages différentes, en fonction du réseau.
   - Pour IPv6, les masques fixes /64 /112 et /128 sont disponibles.

   Cette vérification de la portée de l'hôte est utile pour les réseaux VLAN distincts munis d'un grand nombre de clients et qui ne possèdent pas un nom d'hôte partiel unique (domaine).
3. Nom du client : `abc-11.d1.com`
4. Nom de domaine du client : `*.d1.com`
5. Tous les clients : `*`

Pour plus d'informations, consultez le *Guide d'administration de Data Domain Boost pour l'intégration des partenaires*.

Création de groupes d'interfaces

Utilisez l'onglet IP Network pour créer des groupes d'interfaces et ajouter des interfaces et des clients aux groupes.

L'existence de plusieurs groupes d'interfaces améliore l'efficacité de DD Boost en vous permettant de réaliser les opérations suivantes :

- Configurer DD Boost pour utiliser les interfaces spécifiques configurées dans des groupes.

- Attribuer des clients à l'un de ces groupes d'interfaces.
- Surveiller les interfaces actives avec clients DD Boost.

Commencez par créer des groupes d'interfaces, puis ajoutez des clients à un groupe d'interfaces (à mesure que de nouveaux serveurs de média deviennent disponibles).

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Intergace Groups, cliquez sur Add (**+**).
3. Saisissez le nom du groupe d'interfaces.
4. Sélectionnez une ou plusieurs interfaces. Un maximum de 32 interfaces peut être configuré.

   Remarque

   En fonction des configurations d'alias, il est possible que certaines interfaces ne puissent pas être sélectionnées si elles partagent une interface physique avec une autre interface du même groupe. Cela est dû au fait que chaque interface au sein du groupe doit se trouver sur une interface physique différente pour garantir la restauration après basculement sur incident.

5. Cliquez sur **OK**.
6. Dans la section Configured Clients, cliquez sur Add (**+**).
7. Entrez un nom du client complet ou `*.mydomain.com`.

   Remarque

   Initialement, le client * est disponible pour le groupe par défaut. Le client * peut uniquement être membre d'un ifgroup.

8. Sélectionnez un groupe d'interfaces configuré précédemment, puis cliquez sur **OK**.

Activation et désactivation des groupes d'interfaces

Utilisez l'onglet IP Network pour activer et désactiver des groupes d'interfaces.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Interface Groups, sélectionnez le groupe d'interfaces dans la liste.

   Remarque

   Si les clients et les interfaces du groupe d'interfaces ne sont pas attribués, vous ne pouvez pas activer le groupe.

3. Cliquez sur **Modify** (crayon).
4. Cliquez sur **Enabled** pour activer le groupe d'interfaces. Décochez la case pour désactiver.
5. Cliquez sur **OK**.

Modification d'un nom de groupe d'interfaces et des interfaces

Utilisez l'onglet IP Network pour changer un nom de groupe d'interfaces et les interfaces associées au groupe.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Interface Groups, sélectionnez le groupe d'interfaces dans la liste.
3. Cliquez sur **Modify** (crayon).
4. Saisissez une seconde fois le nouveau nom.

   Le nom du groupe doit comporter entre 1 et 24 caractères, et ne contenir que des lettres, des chiffres, des traits de soulignements et des tirets. Il ne doit pas être identique à un autre nom de groupe et ne peut pas être « default », « yes », « no » ou « all ».

5. Sélectionnez ou désélectionnez des interfaces client dans la liste des interfaces.

   Remarque

   Si vous supprimez toutes les interfaces du groupe, celui-ci est automatiquement désactivé.

6. Cliquez sur **OK**.

Suppression d'un groupe d'interfaces

Utilisez l'onglet IP Network pour supprimer un groupe d'interfaces. Cette opération a pour effet de supprimer l'ensemble des interfaces et des clients associés au groupe.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Interface Groups, sélectionnez le groupe d'interfaces dans la liste. Le groupe par défaut ne peut pas être supprimé.
3. Cliquez sur Delete (**X**).
4. Confirmez la suppression.

Ajout d'un client dans un groupe d'interfaces

Utilisez l'onglet IP Network pour ajouter des clients dans des groupes d'interfaces.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Configured Clients, cliquez sur le bouton d'ajout (**+**).
3. Saisissez un nom pour le client.

   Les noms des clients doivent être uniques et peuvent être constitués des éléments suivants :

   - `FQDN`
   - `*.domain`

- Plage d'adresses IP publiques du client :
  - Pour IPv4, `xx.xx.xx.0/24` applique un masque 24 bits à l'adresse IP de connexion. La mention /24 représente le nombre de bits masqués lorsque l'adresse IP source du client est évaluée pour un accès à l'IFGROUP.
  - Pour IPv6, `xxxx::0/112` offre un masque de 112 bits pour l'adresse IP en cours de connexion. La mention /112 représente le nombre de bits masqués lorsque l'adresse IP source du client est évaluée pour un accès à l'IFGROUP.

Les noms de client se composent de 128 caractères au maximum.

4. Sélectionnez un groupe d'interfaces configuré précédemment, puis cliquez sur **OK**.

Modification du nom d'un client ou d'un groupe d'interfaces

Utilisez l'onglet IP Network pour changer le nom d'un client ou un groupe d'interfaces.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Configured Clients, sélectionnez le client.
3. Cliquez sur **Edit** (crayon).
4. Saisissez un nouveau nom de client.

   Les noms des clients doivent être uniques et peuvent être constitués des éléments suivants :

   - **`FQDN`**
   - **`*.domain`**
   - Plage d'adresses IP publiques du client :
     - Pour IPv4, `xx.xx.xx.0/24` applique un masque 24 bits à l'adresse IP de connexion. La mention /24 représente le nombre de bits masqués lorsque l'adresse IP source du client est évaluée pour un accès à l'IFGROUP.
     - Pour IPv6, `xxxx::0/112` offre un masque de 112 bits pour l'adresse IP en cours de connexion. La mention /112 représente le nombre de bits masqués lorsque l'adresse IP source du client est évaluée pour un accès à l'IFGROUP.

   Les noms de client se composent de 128 caractères au maximum.

5. Sélectionnez un nouveau groupe d'interfaces dans le menu.

   Remarque

   En l'absence de clients, l'ancien groupe d'interface est désactivé.

6. Cliquez sur **OK**.

Suppression d'un client du groupe d'interfaces

Utilisez l'onglet IP Network pour supprimer un client d'un groupe d'interfaces.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.

2. Dans la section Configured Clients, sélectionnez le client.
3. Cliquez sur Delete (**X**).

Remarque

Si le groupe d'interfaces auquel le client appartient n'a aucun autre client, le groupe d'interfaces est désactivé.

4. Confirmez la suppression.

Utilisation des groupes d'interfaces pour la réplication de fichiers gérée

Les groupes d'interfaces peuvent être utilisés pour contrôler les interfaces utilisées pour la réplication de fichiers gérés par DD Boost, et ce, afin de diriger la connexion de réplication sur un réseau spécifique et d'utiliser plusieurs interfaces réseau dotées d'une large bande passante et d'une grande fiabilité en cas de basculement sur incident. Tous les types d'adresses IP Data Domain sont pris en charge : IPv4 ou IPv6, alias IP/adresse IP de réseau VLAN et l'agrégation LACP/basculement sur incident.

Remarque

Les groupes d'interfaces utilisés pour la réplication sont différents des groupes d'interfaces précédemment décrits. Ils sont, de plus, uniquement pris en charge pour la réplication de fichiers gérés par DD Boost. Pour obtenir des informations détaillées sur l'utilisation des groupes d'interfaces pour la réplication de fichiers gérés, consultez le document *Guide d'administration de Data Domain Boost pour l'intégration des partenaires* ou le *guide d'administration de Data Domain Boost for OpenStorage*.

Si vous n'utilisez pas des groupes d'interfaces, la configuration de la réplication nécessite plusieurs étapes :

1. Ajout d'une entrée dans le fichier `/etc/hosts` sur le système Data Domain source pour le système Data Domain cible et codage en dur de l'une des interfaces réseau LAN privées en tant qu'adresse IP de destination.
2. Ajout d'une route sur le système Data Domain source vers le système Data Domain cible en spécifiant un port physique ou virtuel sur le système Data Domain source à l'adresse IP de destination distante.
3. Configuration de LACP via le réseau sur tous les switches situés entre les systèmes Data Domain pour l'équilibrage de charge et le basculement sur incident.
4. Différentes applications sont nécessaires pour utiliser des noms différents pour le système Data Domain cible et éviter les conflits de dénomination dans le fichier `/etc/hosts`.

L'utilisation de groupes d'interfaces pour la réplication simplifie cette configuration grâce à l'utilisation de commandes DD System Manager ou de la CLI de DD OS. L'utilisation de groupes d'interfaces pour configurer le chemin de réplication vous permet de :

- Rediriger une adresse IP résolue en nom d'hôte en dehors du réseau public, à l'aide d'une autre adresse IP du système Data Domain privé.
- Identifier un groupe d'interfaces en fonction des critères de sélection configurés, en fournissant un groupe d'interfaces unique dans lequel toutes les interfaces sont accessibles à partir du système Data Domain cible.
- Sélectionner une interface de réseau privé dans la liste des interfaces appartenant à un groupe, en s'assurant que l'interface est fonctionnelle.

- Fournir un équilibre de charge sur plusieurs interfaces Data Domain au sein du même réseau privé.
- Fournir une interface de basculement sur incident pour la restauration pour les interfaces du groupe d'interfaces.
- Fournir un basculement sur incident de l'hôte si cette option est configurée sur le système Data Domain source.
- Utiliser NAT (Network Address Translation)

L'ordre de sélection pour déterminer une correspondance de groupe d'interfaces pour la réplication de fichiers est :

1. Chemin d'accès à la structure MTree locale (unité de stockage) et nom d'hôte Data Domain distant spécifique
2. Chemin d'accès à la structure MTree locale (unité de stockage) avec un nom d'hôte Data Domain distant
3. Chemin d'accès à la structure MTree (unité de stockage) avec un nom d'hôte Data Domain spécifique

La même structure MTree peut apparaître dans plusieurs groupes d'interfaces uniquement si elle possède un nom d'hôte Data Domain différent. Le même nom d'hôte Data Domain peut apparaître dans plusieurs groupes d'interfaces uniquement s'il possède un autre chemin d'accès à la structure MTree. Le nom d'hôte distant doit être un nom de domaine complet, par exemple dd890-1.emc.com.

La sélection du groupe d'interfaces s'effectue localement sur le système Data Domain source et le système Data Domain cible, indépendamment de l'un et de l'autre. Pour un réseau WAN de réplication, seul le groupe d'interfaces distant doit être configuré étant donné que l'adresse IP source correspond à la passerelle de l'adresse IP distante.

Ajout d'un chemin de réplication dans un groupe d'interfaces

Utilisez l'onglet IP Network pour ajouter des chemins de réplication dans des groupes d'interfaces.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Configured Replication Paths, cliquez sur le bouton d'ajout (**+**).
3. Saisissez des valeurs pour **MTree** et/ou **Remote Host**.
4. Sélectionnez un groupe d'interfaces configuré précédemment, puis cliquez sur **OK**.

Modification d'un chemin de réplication pour un groupe d'interfaces

Utilisez l'onglet IP Network pour modifier les chemins de réplication pour des groupes d'interfaces.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Configured Replication Paths, sélectionnez le chemin de réplication.
3. Cliquez sur **Edit** (Crayon).
4. Modifiez n'importe quelle valeur ou toutes les valeurs dans **MTree**, **Remote Host** ou**Interface Group**.

5. Cliquez sur **OK**.

Suppression d'un chemin de réplication pour un groupe d'interfaces

Utilisez l'onglet IP Network pour supprimer les chemins de réplication pour des groupes d'interfaces.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **IP Network**.
2. Dans la section Configured Replication Paths, sélectionnez le chemin de réplication.
3. Cliquez sur Delete (**X**).
4. Dans la boîte de dialogue Delete Replication Path(s), cliquez sur **OK**.

Destruction de DD Boost

Utilisez cette option pour supprimer définitivement toutes les données (images) contenues dans des unités de stockage. Lorsque vous désactivez ou détruisez DD Boost, le service FC de DD Boost est également désactivé. Seul un administrateur peut détruire DD Boost.

Procédure

1. Supprimez manuellement (faites expirer) les entrées de catalogue correspondantes de l'application de sauvegarde.

   Remarque

   Si plusieurs applications de sauvegarde utilisent le même système Data Domain, supprimez toutes les entrées de chacun des catalogues de ces applications.

2. Sélectionnez **Protocols** > **DD Boost** > **More Tasks** > **Destroy DD Boost...**.
3. Saisissez vos informations d'identification d'administrateur lorsque vous y êtes invité.
4. Cliquez sur **OK**.

Configuration du mode de transport DD Boost-over-Fibre Channel

Dans les versions antérieures de DD OS, toutes les communications entre la librairie DD Boost et un système Data Domain quelconque utilisaient des réseaux IP. DD OS propose désormais un autre mécanisme de transport pour la communication entre la librairie DD Boost et le système Data Domain : Fibre Channel.

Remarque

Les environnements clients Windows, Linux, HP-UX (architecture Itanium 64 bits), AIX et Solaris sont pris en charge.

Activation des utilisateurs de DD Boost

Avant de configurer le service DD Boost-over-FC sur un système Data Domain, vous devez ajouter un ou plusieurs utilisateurs de DD Boost et activer DD Boost.

Avant de commencer

- Connectez-vous à DD System Manager. Pour savoir comment procéder, reportez-vous à la section « Connexion à DD System Manager et déconnexion ».
  Équivalent CLI

```
Connectez-vous en tant que : sysadmin
Data Domain OS 5.7.x.x-12345
Using keyboard-interactive authentication.
Password:
```

- Si vous utilisez la CLI, assurez-vous que le processus cible SCSI est activé :

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

Remarque

Si vous utilisez DD System Manager, le processus cible SCSI est automatiquement activé dès que vous activez le service DD Boost-over-FC (plus loin dans cette procédure).

- Vérifiez que la licence DD Boost est installée. Dans DD System Manager, sélectionnez **Protocols** > **DD Boost** > **Settings**. Si l'état montre que vous ne détenez pas de licence DD Boost, cliquez sur **Add License** et saisissez une clé de licence valide dans la boîte de dialogue Add License Key.
  Équivalents CLI

```
# license show
```

```
# license add license-code
```

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Settings**.
2. Dans la section Users with DD Boost Access, spécifiez un ou plusieurs noms d'utilisateur DD Boost.

   Un utilisateur de DD Boost est également un utilisateur de DD OS. Lorsque vous indiquez un nom d'utilisateur de DD Boost, vous pouvez sélectionner un nom d'utilisateur de DD OS existant ou créer un nouveau nom d'utilisateur de DD OS et faire de ce nom un utilisateur de DD Boost. Cette version prend en charge plusieurs utilisateurs de DD Boost. Pour obtenir des instructions détaillées, reportez-vous à la section « Spécification des noms d'utilisateur de DD Boost ».

   Équivalents CLI

```
# user add username [password password]
```

```
# ddboost set user-name exampleuser
```

3. Cliquez sur **Enable** pour activer DD Boost.

   Équivalent CLI

```
# ddboost enable
Starting DDBOOST, please wait..............
DDBOOST is enabled.
```

Résultats

Vous êtes maintenant prêt à configurer le service DD Boost-over-FC sur le système Data Domain.

Configuration de DD Boost

Après avoir ajouté un/des utilisateur(s) et activé DD Boost, il convient d'activer l'option Fibre Channel et de spécifier le nom du serveur DD Boost Fibre Channel. Selon votre application, vous aurez éventuellement besoin de créer une ou plusieurs unités de stockage et d'installer l'API/plug-in DD Boost sur des serveurs de média ayant accès au système Data Domain.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Fibre Channel**.
2. Cliquez sur le bouton **Enable** pour activer le transport Fibre Channel.

   Équivalent CLI

   ```
   # ddboost option set fc enabled
   Please wait...
   DD Boost option "FC" set to enabled.
   ```

3. Pour changer la valeur par défaut (nom d'hôte) attribuée au nom du serveur DD Boost Fibre Channel, cliquez sur **Edit**, saisissez un nouveau nom de serveur, puis cliquez sur **OK**.

   Équivalent CLI

   ```
   # ddboost fc dfc-server-name set DFC-ddbeta2
   DDBoost dfc-server-name is set to "DFC-ddbeta2" for DDBoost FC.
   Configure clients to use "DFC-DFC-ddbeta2" for DDBoost FC.
   ```

4. Accédez à l'onglet **Protocols** > **DD Boost** > **Storage Units** pour créer une unité de stockage (si elle n'a pas déjà été créée par l'application).

   Vous devez créer au moins une unité de stockage sur le système Data Domain et un utilisateur de DD Boost doit être attribué à cette unité de stockage. Pour obtenir des instructions détaillées, reportez-vous à la section « Création d'une unité de stockage ».

   Équivalent CLI

   ```
   # ddboost storage-unit create storage_unit_name-su
   ```

5. Installez, au besoin, l'API/plug-in DD Boost (cela dépend de l'application).

   Le logiciel du plug-in DD Boost OpenStorage doit être installé sur des serveurs de média NetBackup qui doivent accéder au système Data Domain. Ce plug-in inclut la bibliothèque DD Boost requise qui s'intègre au système Data Domain. Pour obtenir des instructions détaillées sur l'installation et la configuration, consultez le document intitulé *Guide d'administration de Data Domain Boost pour l'intégration des partenaires* ou le *Guide d'administration de Data Domain Boost for OpenStorage*.

Résultats

Vous pouvez, à présent, vérifier la connectivité et créer des groupes d'accès.

Vérification de la connectivité et création de groupes d'accès

Accédez à **Hardware** > **Fibre Channel** > **Resources** pour gérer les initiateurs et les points de terminaison des points d'accès. Accédez à **Protocols** > **DD Boost** > **Fibre Channel** pour créer et gérer des groupes d'accès DD Boost-over-FC.

Remarque

Évitez de modifier vos groupes d'accès lorsque des tâches de sauvegarde ou de restauration sont en cours, pour ne pas prendre le risque de les voir échouer. L'impact des modifications lorsqu'une tâche est en cours dépend de la configuration de l'hôte et de celle du logiciel de sauvegarde.

Procédure

1. Sélectionnez **Hardware** > **Fibre Channel** > **Resources** > **Initiators** pour vérifier que les initiateurs sont présents.

   Il est recommandé d'attribuer des alias aux initiateurs pour limiter les risques de confusion lors de la procédure de configuration.

   Équivalent CLI

   ```
   # scsitarget initiator show list
   Initiator      System Address                Group   Service
   ------------   -----------------------   ----------   -------
   initiator-1    21:00:00:24:ff:31:b7:16         n/a       n/a
   initiator-2    21:00:00:24:ff:31:b8:32         n/a       n/a
   initiator-3    25:00:00:21:88:00:73:ee         n/a       n/a
   initiator-4    50:06:01:6d:3c:e0:68:14         n/a       n/a
   initiator-5    50:06:01:6a:46:e0:55:9a         n/a       n/a
   initiator-6    21:00:00:24:ff:31:b7:17         n/a       n/a
   initiator-7    21:00:00:24:ff:31:b8:33         n/a       n/a
   initiator-8    25:10:00:21:88:00:73:ee         n/a       n/a
   initiator-9    50:06:01:6c:3c:e0:68:14         n/a       n/a
   initiator-10   50:06:01:6b:46:e0:55:9a         n/a       n/a
   tsm6_p23       21:00:00:24:ff:31:ce:f8   SetUp_Test       VTL
   ------------   -----------------------   ----------   -------
   ```

2. Pour attribuer un alias à un initiateur, sélectionnez un des initiateurs et cliquez sur le bouton d'édition (icône en forme de crayon). Saisissez l'alias dans le champ Name de la boîte de dialogue Modify Initiator, puis cliquez sur **OK**.

   Équivalents CLI

   ```
   # scsitarget initiator rename initiator-1 initiator-renamed
   Initiator 'initiator-1' successfully renamed.
   ```

   ```
   # scsitarget initiator show list
   Initiator           System Address                 Group
   Service
   -----------------   -----------------------   ----------
   -------
   initiator-2         21:00:00:24:ff:31:b8:32          n/a
   n/a
   initiator-renamed   21:00:00:24:ff:31:b7:16          n/a
   n/a
   -----------------   -----------------------   ----------
   -------
   ```

3. Dans l'onglet Resources, assurez-vous que des points de terminaison sont présents et activés.

   Équivalent CLI

   ```
   # scsitarget endpoint show list
   -------------   --------------   ------------   -------   ------
   ```

```
endpoint-fc-0   5a              FibreChannel   Yes       Online
endpoint-fc-1   5b              FibreChannel   Yes       Online
-------------   --------------  ------------   -------   ------
```

4. Accédez à **Protocols** > **DD Boost** > **Fibre Channel**.
5. Dans la zone DD Boost Access Groups, cliquez sur l'icône **+** pour ajouter un groupe d'accès.
6. Saisissez un nom unique pour le groupe d'accès. Les doublons ne sont pas acceptés.

   Équivalent CLI

   ```
   # ddboost fc group create test-dfc-group
   DDBoost FC Group "test-dfc-group" successfully created.
   ```

7. Sélectionnez un ou plusieurs initiateurs. Éventuellement, remplacez le nom de l'initiateur en en saisissant un nouveau. Cliquez sur **Next.**

   Équivalent CLI

   ```
   #ddboost fc group add test-dfc-group initiator initiator-5
   Initiator(s) "initiator-5" added to group "test-dfc-group".
   ```

   Un initiateur est un port sur un adaptateur HBA rattaché à un client de sauvegarde qui se connecte au système pour lire et écrire des données à l'aide du protocole Fibre Channel. Le WWPN est le nom de port international unique du port Fibre Channel dans le serveur de média.

8. Spécifiez le nombre de périphériques DD Boost réservés au groupe. Ce nombre détermine les périphériques susceptibles d'être découverts par l'initiateur et, par conséquent, le nombre de chemins d'E/S au système Data Domain. Par défaut, la valeur minimale est un, et la valeur maximale est 64.

   Équivalent CLI

   ```
   # ddboost fc group modify Test device-set count 5
   Added 3 devices.
   ```

   Reportez-vous au document intitulé *EMC Data Domain Boost for OpenStorage Administration Guide* pour connaître la valeur recommandée pour différents clients.

9. Précisez les points de terminaison à inclure au groupe : tous, aucun ou à une sélection dans la liste des points de terminaison. Cliquez sur **Next**.

   Équivalents CLI

   ```
   # scsitarget group add Test device ddboost-dev8 primary-
   endpoint allsecondary-endpoint all
   Device 'ddboost-dev8' successfully added to group.
   ```

   ```
   # scsitarget group add Test device ddboost-dev8 primary-
   endpointendpoint-fc-1 secondary-endpoint fc-port-0
   Device 'ddboost-dev8' is already in group 'Test'.
   ```

   Lors de la présentation des numéros d'unité logique (LUN) via les ports FC rattachés sur les adaptateurs HBA, trois désignations de ports sont possibles : primaire, secondaire ou aucune désignation. Un port primaire pour un ensemble de LUN représente le port exposant actuellement ces LUN à un fabric. Un port secondaire est un port qui diffusera un ensemble de LUN en cas d'échec du chemin principal (cette opération nécessite une intervention manuelle). Utilisez le paramètre None si vous ne souhaitez pas annoncer les LUN sélectionnées. La présentation des LUN dépend de la topologie SAN.

10. vérifiez la synthèse et effectuez les modifications éventuelles. Cliquez sur **Finish** pour créer le groupe d'accès qui s'affiche alors dans la liste DD Boost Access Groups.

    Équivalent de l'interface de ligne de commande (CLI)

    ```
    # scsitarget group show detailed
    ```

    Remarque

    Pour modifier les paramètres d'un groupe d'accès existant, sélectionnez-le dans la liste et cliquez sur le bouton d'édition (icône en forme de crayon).

Suppression des groupes d'accès

Utilisez l'onglet Fibre Channel pour supprimer des groupes d'accès.

Procédure

1. Sélectionnez **Protocols** > **DD Boost** > **Fibre Channel**.
2. Sélectionnez le groupe à supprimer dans la liste des groupes d'accès DD Boost.

   Remarque

   Vous ne pouvez pas supprimer un groupe auquel des initiateurs ont été attribués. Modifiez d'abord le groupe en supprimant les initiateurs.

3. Cliquez sur Delete (**X**).

Utilisation de DD Boost sur des systèmes haute disponibilité

La haute disponibilité permet le basculement sur incident transparent de n'importe quelle application utilisant DD Boost. Autrement dit, toute opération de sauvegarde ou de restauration s'effectue sans intervention manuelle. Tous les autres scénarios d'utilisation de DD Boost sont pris en charge sur les systèmes haute disponibilité, y compris la réplication de fichiers gérés (MFR), le traitement distribué des segments (DSP), la copie de fichiers et les groupes d'interfaces dynamiques (DIG).

Tenez compte de ces informations pour l'utilisation de DD Boost sur des systèmes haute disponibilité :

- Sur les systèmes Data Domain compatibles HA, les basculements sur le serveur DD se produisent en moins de 10 minutes. Toutefois, la restauration des applications DD Boost peut durer plus longtemps, car cette opération ne peut pas commencer tant que le basculement sur incident du serveur DD n'est pas terminé. En outre, la restauration des applications Boost ne peut pas démarrer tant que l'application n'aura pas appelé la bibliothèque DD Boost.
- DD Boost sur des systèmes haute disponibilité exige que les applications Boost utilisent des bibliothèques HA Boost. Les applications n'utilisant pas ce type de bibliothèques ne peuvent pas exécuter un basculement sur incident de façon transparente.
- La réplication des fichiers gérés (MFR) bascule en toute transparence lorsque les systèmes sources et cibles sont configurés pour la haute disponibilité. La réplication des fichiers gérés (MFR) est également prise en charge sur les configurations HA partielles (autrement dit, lorsque le système source ou cible est

activé, mais pas les deux) lorsque la panne se produit sur le système haute disponibilité. Pour obtenir des informations supplémentaires, consultez le *Guide d'administration de DD Boost for OpenStorage* ou le *Guide d'administration de Data Domain Boost pour l'intégration des partenaires*.

- Les groupes d'interfaces dynamiques ne doivent pas inclure les adresses IP associées à l'interconnexion directe entre les systèmes Data Domain actifs et en veille.
- L'utilisation des adresses IP flottantes doit être configurée pour les clients DD Boost.

À propos des onglets DD Boost

Apprenez à utiliser les onglets DD Boost dans DD System Manager.

Paramètres

Utilisez l'onglet Settings pour activer ou désactiver DD Boost, sélectionner les clients et les utilisateurs et spécifier des options avancées.

L'onglet Settings permet de savoir si DD Boost est activé (Enabled) ou désactivé (Disabled). Utilisez le bouton **Status** pour basculer entre l'état **Enabled** et **Disabled**.

Sous **Allowed Clients**, sélectionnez les clients autorisés à accéder au système. Servez-vous des boutons **Add**, **Modify** et **Delete** pour gérer la liste des clients.

Sous **Users with DD Boost Access**, sélectionnez les utilisateurs devant accéder à DD Boost. Servez-vous des boutons **Add**, **Change Password** et **Remove** pour gérer la liste des utilisateurs.

Développez **Advanced Options** pour connaître les options avancées activées. Accédez à **More Tasks** > **Set Options** pour réinitialiser ces options.

Connexions actives

Utilisez l'onglet Active Connections pour afficher des informations au sujet des clients, des interfaces et des fichiers sortants.

Tableau 131 Informations sur le client connecté

Élément	Description
Client	Nom du client connecté.
Idle	Indique si le client est inactif (Yes) ou pas (No).
Plug-In Version	Version du plug-in DD Boost installé (par exemple 2.2.1.1).
OS Version	Version du système d'exploitation installé (par exemple, Linux 2.6.1 7-1.2142_FC4smp x86_64).
Application Version	Version de l'application de sauvegarde installée (par exemple, NetBackup 6.5.6).
Encrypted	Indique si la connexion est chiffrée (Yes) ou pas (No).
DSP	Indique si la connexion utilise ou non le traitement distribué des segments (DSP).
Transport	Type de transport utilisé, comme IPv4, IPv6 ou FC (Fibre Channel).

Tableau 132 Informations sur la connexion d'interface configurée

Élément	Description
Interface	Adresse IP de l'interface.
Interface Group	L'une des valeurs suivantes : • Nom du groupe d'interfaces. • Aucun, si elle n'est pas membre d'un groupe.
Sauvegarder	Nombre de connexions de sauvegarde actives.
Restaurer	Nombre de connexions de restauration actives.
Réplication	Nombre de connexions de réplication actives.
Synthétique	Nombre de sauvegardes synthétiques.
Total	Nombre total de connexions de l'interface.

Tableau 133 Informations sur la réplication de fichiers sortants

Élément des fichiers sortants	Description
File Name	Nom du fichier d'image sortant.
Target Host	Nom de l'hôte recevant le fichier.
Logical Bytes to Transfer	Nombre d'octets logiques à transférer.
Logical Bytes Transferred	Nombre d'octets logiques déjà transférés.
Low Bandwidth Optimization	Nombre d'octets de faible bande passante déjà transférés.

Réseau IP

L'onglet IP Network répertorie les groupes d'interfaces configurés. Les informations détaillées précisent si un groupe est activé ou non et indiquent les interfaces client configurées. Les administrateurs peuvent également utiliser le menu Interface Group pour afficher les clients associés à un groupe d'interfaces.

Fibre Channel

L'onglet Fibre Channel répertorie les groupes d'accès DD Boost configurés. Utilisez l'onglet Fibre Channel pour créer et supprimer des groupes d'accès et configurer des initiateurs, des périphériques et des points de terminaison pour les groupes d'accès DD Boost.

Unités de stockage

Utilisez l'onglet **Storage Units** pour afficher, créer, modifier et supprimer des unités de stockage.

Tableau 134 Onglet Storage Units

Élément	Description
Unités de stockage	
View DD Boost Replications	Affichez les contextes de réplication DD Boost.
Storage Unit	Nom de l'unité de stockage.
User	Nom d'utilisateur associé à l'unité de stockage.
Quota Hard Limit	Quota strict défini pour l'unité de stockage.
Last 24hr Pre-Comp	Quantité de données écrites dans l'unité de stockage au cours des 24 dernières heures, avant compression.
Last 24hr Post-Comp	Quantité de données écrites dans l'unité de stockage au cours des 24 dernières heures, après compression.
Last 24hr Comp Ratio	Taux de compression des données écrites dans l'unité de stockage au cours des dernières 24 heures.
Weekly Avg Post-Comp	Quantité moyenne de données écrites dans l'unité de stockage chaque semaine, après compression.
Last Week Post-Comp	Quantité de données écrites dans l'unité de stockage au cours de la dernière semaine, après compression.
Weekly Avg Comp Ratio	Taux de compression moyen des données écrites dans l'unité de stockage chaque semaine.
Last Week Comp Ratio	Taux de compression des données écrites dans l'unité de stockage au cours de la dernière semaine.

Sélectionnez une unité de stockage pour obtenir des informations détaillées à son sujet. Des informations détaillées sont disponibles sous trois onglets :

- Onglet Storage Unit

  Tableau 135 Détails sur l'unité de stockage : Onglet Storage Unit

Élément	Description
Total Files	Nombre total d'images de fichiers sur l'unité de stockage.
Full Path	Chemin complet de l'unité de stockage.
État	État actuel de l'unité de stockage (les combinaisons sont prises en charge). Cet état peut être : ■ D - Supprimé ■ RO - Lecture seule ■ RW - Lecture/Écriture ■ RD - Destination de réplication ■ RLE - DD Retention Lock activé ■ RLD - DD Retention Lock désactivé
Pre-Comp Used	Quantité de stockage précompressé déjà utilisée.

Tableau 135 Détails sur l'unité de stockage : Onglet Storage Unit (suite)

Élément	Description
Used (Post-Comp)	Taille totale après compression des fichiers dans l'unité de stockage.
Compression	Taux de compression obtenu sur les fichiers.
Schedules	Nombre de plannings de mesure de la capacité physique affectés à l'unité de stockage.
Submitted Measurements	Nombre de fois que la capacité physique de l'unité de stockage a été mesurée.
Quota Enforcement	Cliquez sur Quota pour accéder à la page Data Management Quota qui répertorie les valeurs/pourcentages de quotas souples et stricts utilisés par les MTrees.
Pre-Comp Soft Limit	Valeur actuelle du quota souple défini pour l'unité de stockage.
Pre-Comp Hard Limit	Valeur actuelle du quota strict défini pour l'unité de stockage.
Quota Summary	Pourcentage de limite stricte utilisé.
Total Snapshots	Nombre total de snapshots de l'unité de stockage.
Expired	Nombre de snapshots expirés de l'unité de stockage.
Unexpired	Nombre de snapshots non expirés de l'unité de stockage.
Oldest Snapshot	Le plus ancien snapshot de l'unité de stockage.
Newest Snapshot	Le plus récent snapshot de l'unité de stockage.
Next Scheduled	Le prochain snapshot planifié de l'unité de stockage.
Assigned Snapshot Schedules	Les plannings instantanés affectés à l'unité de stockage.

- Onglet Space Usage : Affiche un graphique montrant les octets de pré-compression utilisés, les octets de post-compression utilisés et le facteur de compression.
- Onglet Daily Written : Affiche un graphique montrant les octets de pré-compression écrits, les octets de post-compression écrits et le facteur de compression total.

CHAPITRE 15

DD Virtual Tape Library

Ce chapitre traite des sujets suivants :

Présentation de DD Virtual Tape Library

Data Domain Virtual Tape Library (DD VTL) est un système de sauvegarde sur disque qui émule l'utilisation de bandes physiques. Il permet aux applications de sauvegarde de se connecter au stockage du système DD et de le gérer à l'aide d'une fonctionnalité quasiment identique à une bibliothèque de bandes physique.

Les lecteurs de bande virtuels sont accessibles au logiciel de sauvegarde de la même manière que les lecteurs de bande physiques. Une fois que vous avez créé ces lecteurs dans une librairie de bandes virtuelle (DD VTL), ils apparaissent dans le logiciel de sauvegarde sous forme de lecteurs de bandes SCSI. DD VTL, en soi, est considéré par le logiciel de sauvegarde comme un périphérique robotique SCSI, accessible via des interfaces de pilote standard. Toutefois, le logiciel de sauvegarde (non le système DD configuré en tant que DD VTL) gère le déplacement du changeur de média et des images de sauvegarde.

Les termes suivants ont une signification particulière lorsqu'ils sont utilisés en référence à DD VTL :

- *Bibliothèque* : une bibliothèque émule une bibliothèque de bandes physique avec des lecteurs, un changeur, des ports CAP (ports d'accès aux cartouches) et des slots (slots de cartouches).
- *Bande* : une bande est représentée comme un fichier. Les bandes peuvent être importées de la chambre forte vers une bibliothèque. Les bandes peuvent être exportées d'une bibliothèque vers la chambre forte. Les bandes peuvent être déplacées au sein d'une bibliothèque sur les lecteurs, slots et ports CAP.
- *Pool* : un pool est un ensemble de bandes qui est mappé à un répertoire du système de fichiers. Les pools servent à répliquer des bandes sur une destination. Par défaut, les pools sont créés en tant que pools MTree sauf si vous les spécifiez comme pools de répertoires lors de leur création. Vous pouvez convertir des pools basés sur répertoire en pools basés sur MTree afin de profiter des fonctionnalités plus importantes des MTree.
- *Chambre forte* : la chambre forte contient les bandes qui ne sont utilisées par aucune bibliothèque. Les bandes résident dans une bibliothèque ou dans la chambre forte.

DD VTL a été testé avec des configurations de sauvegarde logicielles et matérielles spécifiques et est pris en charge par celles-ci. Pour plus d'informations, consultez le document *Backup Compatibility Guide* approprié sur le site de support en ligne.

DD VTL prend simultanément en charge l'utilisation des interfaces de la bibliothèque de bandes et du système de fichiers (NFS/CIFS/DD Boost).

Lorsqu'une reprise après sinistre est nécessaire, les pools et les bandes peuvent être répliqués dans un système DD distant à l'aide de DD Replicator.

Pour protéger les données sur bandes contre toute modification, les bandes peuvent être verrouillées à l'aide du logiciel DD Retention Lock Governance.

Remarque

Pour l'instant, à 16 Gbit/s, Data Domain prend en charge les topologies de type fabric et point à point. Les autres topologies connaissent des problèmes.

L'article de la base de connaissances : *Data Domain : Le Guide des bonnes pratiques VTL*, disponible à l'adresse https://support.EMC.com/kb/180591, fournit des informations supplémentaires sur les meilleures pratiques pour DD VTL.

Planification d'une DD VTL

Une DD VTL (Virtual Tape Library, librairie de bandes virtuelle) nécessite un environnement particulier. Il faut notamment disposer des licences adéquates, de cartes d'interface, d'autorisations utilisateur, etc. Les conditions requises sont détaillées ci-dessous avec les recommandations d'usage.

- Une licence DD VTL appropriée.
  - DD VTL est une fonction concédée sous licence, et vous devez utiliser le protocole NDMP (Network Data Management Protocol) sur IP (Internet Protocol) ou la DD VTL directement sur FC (Fibre Channel).
  - Une licence supplémentaire est nécessaire pour les systèmes IBM i : la licence I/OS.
  - L'ajout d'une licence DD VTL par l'intermédiaire de DD System Manager désactive et réactive automatiquement la fonction DD VTL.
- Une carte d'interface FC installée ou une DD VTL configurée pour utiliser le NDMP.
  - Si la communication de la DD VTL entre un serveur de sauvegarde et un système DD s'effectue via une interface FC, une carte d'interface FC doit être installée sur le système DD. Notez que chaque fois qu'une carte d'interface FC est supprimée d'un système DD (ou modifiée dans ce système), toute configuration de DD VTL associée à cette carte doit être mise à jour.
  - Si la communication de la DD VTL entre un serveur de sauvegarde et un système DD s'effectue via NDMP, aucune carte d'interface FC n'est requise. Cependant, vous devez configurer le groupe d'accès au serveur de bandes. En outre, en cas d'utilisation de NDMP, toutes les fonctionnalités d'initiateur et de port ne s'appliquent pas.
  - Le filtre de réseau doit être configuré pour permettre au client NDMP d'envoyer des informations au système DD. Exécutez la commande `net filter add operation allow clients <adresse IP du client>` pour autoriser l'accès pour le client NDMP.
    - Pour plus de sécurité, exécutez la commande `net filter add operation allow clients <adresse IP du client> interfaces <adresse IP de l'interface DD>`.
    - Associez l'option `seq-id 1` à la commande pour appliquer cette règle avant toute autre règle de filtre de réseau.
- Une taille d'enregistrement minimale (bloc) du logiciel de sauvegarde.
  - Si possible, configurez le logiciel de sauvegarde de façon à utiliser une taille d'enregistrement minimale (bloc) de 64 KiB ou plus. Des tailles importantes assurent généralement plus de rapidité et une meilleure compression des données.
  - Selon votre application de sauvegarde, en cas de modification de la taille après la configuration initiale, les données écrites avec la taille initiale peuvent devenir illisibles.
- Un accès utilisateur approprié au système.
  - Pour le fonctionnement et la surveillance de base de la bande, une seule connexion utilisateur est requise.

- Pour activer et configurer les services DD VTL et effectuer d'autres tâches de configuration, une connexion sysadmin est requise.

Limites de DD VTL

Avant de configurer ou d'utiliser une bibliothèque de bandes virtuelle (DD VTL), prenez en compte les limites en matière de taille, de nombre de slots, etc.

- Taille d'E/S : la taille d'E/S maximale prise en charge par un système DD utilisant une DD VTL est 1 Mo.
- Bibliothèques : une DD VTL prend en charge jusqu'à 64 bibliothèques par système DD (c'est-à-dire 64 instances de DD VTL sur chaque système DD).
- Initiateurs : une DD VTL prend en charge jusqu'à 1 024 initiateurs ou WWPN (noms universels des ports) par système DD.
- Lecteurs de bande : les informations relatives aux lecteurs de bande sont présentées dans la section suivante.
- Flux de données : les informations sur les flux de données sont présentées dans le tableau suivant.

Tableau 136 Flux de données envoyés à un système Data Domain

Modèle	RAM/NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD140, DD160, DD610	4 Go ou 6 Go/ 0,5 Go	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630 et DD640	8 Go/0,5 Go ou 1 Go	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 Go ou 20 Go/ 1 Go	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 Go/1 Go	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 Go[b] / 1 Go	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 Go/2 Go	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 ou 256 Go[b] / 4 Go	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 Go	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20

Tableau 136 Flux de données envoyés à un système Data Domain (suite)

Modèle	RAM/NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD2200	16 Go	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 ou 64 Go/ 2 Go	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 Go[b] / 4 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 Go[b] / 4 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 ou 256 Go[b] / 4 Go	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 Go	1 885	300	540	1 080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 Go	1 885	300	540	1 080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 Go	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8 To	8 Go / 512 Mo	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE (16 To)	16 Go / 512 Mo ou 24 Go / 1 Go	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE (32 To)	24 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90

Tableau 136 Flux de données envoyés à un système Data Domain (suite)

Modèle	RAM/NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD VE (48 To)	36 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 To	48 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (96 To)	64 Go/2 Go	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 (4 To)	12 Go (mémoire virtuelle) / 512 Mo	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 To	32 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (16 To)	32 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (32 To)	46 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. Flux DirRepl, OptDup, MTreeRepl
b. La fonction Data Domain Extended Retention n'est disponible que pour ces périphériques avec une mémoire (maximale) étendue

- Slots : une DD VTL prend en charge un maximum de :
  - 32 000 slots par bibliothèque
  - 64 000 slots par système DD

  Le système DD ajoute automatiquement des slots pour que le nombre de slots demeure supérieur ou égal au nombre de lecteurs.

  Remarque

  Certains pilotes de périphérique (les pilotes de lecteur de bande IBM AIX, par exemple) limitent les configurations de bibliothèque à certains lecteurs/slots ; or, ce nombre peut être inférieur à celui autorisé par le système DD. Cette limite peut avoir une incidence sur les applications de sauvegarde et les lecteurs utilisés par celles-ci.

- CAP : une DD VTL prend en charge un maximum de :
  - 100 ports CAP par bibliothèque

- 1 000 ports CAP par système DD

Nombre de disques pris en charge par une DD VTL

Le nombre maximal de disques pris en charge par une DD VTL dépend du nombre de cœurs de CPU et de la quantité de mémoire installée (RAM et NVRAM, le cas échéant) sur votre système DD.

Remarque

Ce tableau ne fait pas référence à des numéros de modèles, car il existe de nombreuses combinaisons de cœurs de CPU et de mémoire pour chaque modèle. En outre, le nombre de disques pris en charge dépend *uniquement* des cœurs de CPU et des mémoires, et non d'un modèle spécifique.

Tableau 137 Nombre de disques pris en charge par une DD VTL

Nombre de cœurs de CPU	RAM (en Go)	NVRAM (en Go)	Nombre maximal de disques pris en charge
Moins de 32	4 ou moins	NA	64
	Plus de 4, et jusqu'à 38	NA	128
	Plus de 38, et jusqu'à 128	NA	256
	Plus de 128	NA	540
De 32 à 39	Jusqu'à 128	Moins de 4	270
	Jusqu'à 128	4 ou plus	540
	Plus de 128	NA	540
De 40 à 59	NA	NA	540
60 ou plus	NA	NA	1 080

Code-barres de bande

Lorsque vous créez une bande, vous devez préalablement lui attribuer un *code-barres* unique (ne jamais dupliquer des codes-barres, car cela peut entraîner un comportement imprévisible). Chaque code-barres se compose de huit caractères : les six premiers sont des chiffres ou des lettres majuscules (0-9, A-Z), et les deux derniers correspondent au code de bande pour le type de bande pris en charge, comme indiqué dans le tableau suivant.

Remarque

Bien qu'un code-barres DD VTL se compose de huit caractères, six ou huit caractères peuvent être transmis à une application de sauvegarde, en fonction du type de changeur.

Tableau 138 Codes de bande par type de bande

Type de bande	Capacité par défaut (sauf mention contraire)	Code de bande
LTO-1	100 Gio	N1
LTO-1	50 Gio (autre que par défaut)	LA[a]
LTO-1	30 Gio (autre que par défaut)	LB
LTO-1	10 Gio (autre que par défaut)	LC
LTO-2	200 Gio	N2
LTO-3	400 Gio	N3
LTO-4	800 Gio	L4
LTO-5 (par défaut)	1,5 Tio	L5

a. Pour TSM, utilisez le code de bande L2 si le code LA est ignoré.

Lorsqu'il y a plusieurs bibliothèques de bandes, les codes-barres sont automatiquement incrémentés si le sixième caractère (juste avant le « L ») est un chiffre. Si un dépassement (9 à 0) se produit, la numérotation se déplace d'une place vers la gauche. Si le caractère suivant à incrémenter est une lettre, l'incrémentation s'arrête. Voici quelques exemples de codes-barres et de la façon dont chacun sera incrémenté :

- 000000L1 crée des bandes d'une capacité de 100 Gio et peut accepter jusqu'à 100 000 bandes (de 000 000 à 99 999).
- AA0000LA crée des bandes d'une capacité de 50 Gio et peut accepter jusqu'à 10 000 bandes (de 0 000 à 9 999).
- AAAA00LB crée des bandes d'une capacité de 30 Gio et peut accepter jusqu'à 100 bandes (de 00 à 99).
- AAAAAALC crée une bande d'une capacité de 10 Gio. Une seule bande portant ce nom peut être créée.
- AAA350L1 crée des bandes d'une capacité de 100 Gio et peut accepter jusqu'à 650 bandes (de 350 à 999).
- 000AAALA crée une bande d'une capacité de 50 Gio. Une seule bande portant ce nom peut être créée.
- 5M7Q3KLB crée une bande d'une capacité de 30 Gio. Une seule bande portant ce nom peut être créée.

Compatibilité des lecteurs de bandes LTO

Votre environnement peut être constitué de différentes générations de technologies LTO (Linear Tape-Open) ; la compatibilité entre ces différentes générations est présentée sous forme tabulaire.

Dans ce tableau :

- RW = compatible avec la lecture et l'écriture

- R = uniquement compatible avec la lecture
- — = non compatible

Tableau 139 Compatibilité des lecteurs de bandes LTO

Format de bande	Disque LTO-5	Disque LTO-4	Disque LTO-3	Disque LTO-2	Disque LTO-1
Bande LTO-5	RW	—	—	—	—
Bande LTO-4	RW	RW	—	—	—
Bande LTO-3	R	RW	RW	—	—
Bande LTO-2	—	R	RW	RW	—
Bande LTO-1	—	—	R	RW	RW

Configuration d'une DD VTL

Pour configurer une simple DD VTL, exécutez l'assistant de configuration décrit dans le chapitre *Mise en route*.

Vous trouverez également des informations à ce sujet dans le *Guide de configuration initiale de Data Domain Operating System*.

Étudiez ensuite les rubriques suivantes pour activer la librairie de bandes virtuelle DD VTL, créer des bibliothèques, mais aussi créer et importer des bandes.

Remarque

Si l'environnement de déploiement inclut un système AS400 en tant que client DD VTL, reportez-vous à la section Configuration des options par défaut de la DD VTL à la page 401 pour configurer le préfixe de numéro de série des changeurs et lecteurs VTL avant de configurer la relation DD VTL entre le système Data Domain et le système client AS400.

Systèmes haute disponibilité et DD VTL

Les systèmes haute disponibilité sont compatibles avec les bibliothèques de bandes virtuelles DD VTL. Toutefois, si une tâche de bibliothèque de bandes virtuelle est en cours d'exécution lors d'un basculement sur incident, celle-ci devra être redémarrée manuellement une fois le basculement sur incident terminé.

Le *Guide de la compatibilité des sauvegardes Data Domain Operating System* fournit des informations supplémentaires sur les exigences relatives à l'adaptateur HBA, au switch, au microprogramme et au pilote pour utiliser une bibliothèque de bandes virtuelle DD VTL dans un environnement HA.

Copie de bandes DD VTL sur le cloud

DD VTL prend en charge le stockage de la chambre forte VTL sur le stockage DD Cloud Tier. Pour utiliser cette fonctionnalité, le système Data Domain doit avoir une configuration Cloud Tier prise en charge et disposer d'une licence Cloud Tier en plus de la licence VTL.

Attribuez une licence et configurez le stockage DD Cloud Tier avant de configurer DD VTL pour pouvoir utiliser le stockage cloud comme chambre forte. La section Hiérarchisation du Cloud avec DD à la page 515 fournit des informations

supplémentaires sur la configuration requise pour DD Cloud Tier et indique comment configurer DD Cloud Tier.

Les exigences de l'interface FC et réseau pour la VTL sont les mêmes pour le stockage en chambre forte locale et cloud. DD VTL ne nécessite pas de configuration spéciale pour utiliser le stockage cloud pour la chambre forte. Lorsque vous configurez la DD VTL, sélectionnez le stockage cloud comme emplacement de la chambre forte. Toutefois, lorsque vous utilisez une chambre forte sur le cloud, certaines options de gestion des données sont propres à la chambre forte du cloud. Pour plus d'informations, reportez-vous à la section Utilisation de la chambre forte Cloud à la page 421.

Gestion d'une DD VTL

Vous pouvez gérer une DD VTL à l'aide de Data Domain System Manager (DD System Manager) ou de l'interface de ligne de commande (CLI) du système d'exploitation Data Domain (DD OS). Une fois connecté, vous pouvez vérifier l'état de votre processus DD VTL, consulter les informations relatives aux licences et examiner et configurer les options.

Connexion

Connectez-vous à DD System Manager pour utiliser une interface utilisateur en vue de gérer votre bibliothèque de bandes virtuelle DD (DD VTL).

Équivalent de l'interface de ligne de commande (CLI)

Vous pouvez également vous connecter à partir de la CLI.

```
login as: sysadmin
Data Domain OS
Using keyboard-interactive authentication.
Password:
```

Activation du processus cible SCSI (CLI uniquement)

Si vous vous connectez à partir de la CLI, vous devez activer le processus scsitarget (c'est-à-dire le service Fibre Channel). Ce processus est activé lors des sélections DD VTL ou DD Boost-FC dans DD System Manager. Depuis la CLI, il est nécessaire d'activer ces processus séparément.

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

Accès aux DD VTL

Dans le menu à gauche de DD System Manager, sélectionnez **Protocols** > **VTL**.

État

Dans la zone **Virtual Tape Libraries** > **VTL Service**, vous pouvez voir que l'état de votre processus DD VTL s'affiche en haut, par exemple, **Enabled: Running**. La première partie de l'état est **Enabled** (activé) ou **Disabled** (désactivé). La deuxième partie se compose de l'un des états de processus suivants.

Tableau 140 États de processus DD VTL

State	Description
Running	Le processus DD VTL est activé et actif (représenté en vert).
Starting	Le processus DD VTL démarre.
Stopping	Le processus DD VTL est en cours d'arrêt.

Tableau 140 États de processus DD VTL (suite)

State	Description
Stopped	Le processus DD VTL est désactivé (représenté en rouge).
Timing out	Le processus DD VTL s'est bloqué et tente un redémarrage automatique.
Stuck	Après plusieurs essais infructueux de redémarrage automatique, le processus DD VTL ne peut pas s'arrêter normalement et fait l'objet d'une tentative de destruction.

Licence DD VTL

La ligne VTL License vous indique si votre licence de bibliothèque de bandes virtuelle DD (DD VTL) a été appliquée. Si elle indique Unlicensed, sélectionnez **Add License**. Saisissez votre clé de licence dans la boîte de dialogue Add License Key. Cliquez sur **Next**, puis sur **OK**.

Remarque

Toutes les informations propres aux licences doivent avoir été complétées dans le cadre de la procédure de configuration en usine ; cependant, si la DD VTL a été achetée ultérieurement, il est possible que la clé de licence DD VTL n'ait pas été disponible à ce moment-là.

Équivalent de l'interface de ligne de commande (CLI)

Vous pouvez également vérifier si la licence DD VTL a bien été installée à partir de la CLI :

```
# elicense show
## License Key                    Feature
--    -------------------        -----------
1     DEFA-EFCD-FCDE-CDEF        Replication
2     EFCD-FCDE-CDEF-DEFA        VTL
--    -------------------        -----------
```

En cas d'absence de la licence, chaque unité est accompagnée d'une documentation (une carte d'installation rapide) qui indique les licences acquises. Saisissez l'une des commandes suivantes pour remplir la clé de licence.

```
# license add <license-code>
```

```
# elicense update <license-file>
```

Licence I/OS (pour les utilisateurs IBM i)

Pour les clients d'IBM i, la ligne I/OS License vous indique si votre licence I/OS a été appliquée. Si elle indique Unlicensed, sélectionnez **Add License**. Vous devez saisir une licence I/OS valide dans l'un des formats suivants : **xxxx-xxxx-xxxx-xxxx** ou **xxxx-xxxx-xxxx-xxxx-xxxx**. Votre licence I/OS doit être installée avant de créer une bibliothèque, ainsi que les disques à utiliser sur un système IBM i. Cliquez sur **Next**, puis sur **OK**.

Activation d'une DD VTL

L'activation d'une DD VTL a pour effet de diffuser le nom universel (WWN) de l'adaptateur HBA de Data Domain au fabric du client et d'activer l'ensemble des bibliothèques et des disques de bibliothèque. Si un plan de transfert est requis dans le cadre des processus de contrôle des changements, il doit être activé pour faciliter la segmentation.

Procédure

1. Assurez-vous que vous disposez d'une licence DD VTL et que le système de fichiers est activé.
2. Sélectionnez **Virtual Tape Libraries** > **VTL Service**.
3. Sur la droite de la zone Status, sélectionnez **Enable**.
4. Dans la boîte de dialogue Enable Service, sélectionnez **OK**.
5. Une fois la DD VTL activée, notez que l'état est désormais **Enabled: Running**, en vert. Notez également que les options configurées pour la DD VTL sont affichées dans la zone Option Defaults.

   Équivalent de l'interface de ligne de commande (CLI)

   ```
   # vtl enable Starting VTL, please wait ... VTL is enabled.
   ```

Désactivation d'une DD VTL

La désactivation d'une bibliothèque de bandes virtuelle DD VTL permet de fermer toutes les bibliothèques et d'arrêter le processus DD VTL.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service**.
2. Sur la droite de la zone Status, sélectionnez **Disable**.
3. Dans la boîte de dialogue Disable Service, sélectionnez **OK**.
4. Une fois la bibliothèque de bandes virtuelle DD VTL désactivée, notez que l'état est désormais **Disabled: Stopped**, en rouge.

   Équivalent de l'interface de ligne de commande (CLI)

   ```
   # vtl disable
   ```

Valeurs par défaut de l'option DD VTL

La zone Option Default de la page VTL Service affiche les paramètres en cours des options DD VTL par défaut (auto-eject, auto-offline et barcode-length) que vous pouvez configurer.

Dans la zone **Virtual Tape Libraries** > **VTL Service**, les options par défaut en cours pour votre DD VTL s'affichent. Sélectionnez **Configure** pour modifier l'une de ces valeurs.

Tableau 141 Valeurs par défaut de l'option DD VTL

Élément	Description
Property	Répertorie les options configurées : • auto-eject • auto-offline • barcode-length
Value	Indique la valeur de chaque option configurée :

Tableau 141 Valeurs par défaut de l'option DD VTL (suite)

Élément	Description
	• auto-eject : par défaut (désactivé), activé ou désactivé • auto-offline : par défaut (désactivé), activé ou désactivé • barcode-length : par défaut (8), 6 ou 8

Configuration des options par défaut de la DD VTL

Vous pouvez configurer des options DD VTL par défaut lorsque vous ajoutez une licence, créez une bibliothèque ou à un stade ultérieur.

Remarque

Les bibliothèques de bandes virtuelles (DD VTL) se voient attribuer par défaut des options générales. Et, celles-ci sont mises à jour à chaque fois que les options générales sont modifiées, sauf si vous les modifiez manuellement à l'aide de cette méthode.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service**.
2. Dans la zone Option Defaults, sélectionnez **Configure**. Dans la boîte de dialogue Configure Default Options, modifiez la totalité ou une partie des options par défaut.

Tableau 142 Options DD VTL par défaut

Option	Valeurs	Remarques
auto-eject	par défaut (désactivé), activé ou désactivé	Lorsque l'éjection automatique est activée, toute bande introduite dans un CAP (port d'accès à la cartouche) est automatiquement déplacée vers la chambre forte virtuelle, sauf si : • La bande provenait de la chambre forte, auquel cas elle demeure dans le CPA. • Une commande `ALLOW_MEDIUM_REMOVAL` avec une valeur 0 (faux) a été émise vers la bibliothèque pour éviter la suppression du média du CAP vers l'extérieur.
auto-offline	par défaut (désactivé), activé ou désactivé	L'activation de la mise hors ligne automatique met

Tableau 142 Options DD VTL par défaut (suite)

Option	Valeurs	Remarques
		automatiquement un disque hors ligne avant l'exécution d'une opération de déplacement de bande.
barcode-length	par défaut (8), 6 ou 8 [automatiquement défini sur 6 pour les modèles de changeur L180, RESTORER-L180 et DDVTL]	Bien qu'un code-barres DD VTL soit composé de 8 caractères, 6 ou 8 caractères peuvent être transmis à une application de sauvegarde, en fonction du type de changeur.

3. Sélectionnez **OK**.
4. Autrement, pour désactiver toutes ces options de service, sélectionnez **Reset to Factory**, et les valeurs seront rétablies immédiatement sur les valeurs d'usine par défaut.

À effectuer

Si l'environnement DD VTL contient un AS400 comme client DD VTL, configurez manuellement l'option DD VTL pour le préfixe de numéro de série avant d'ajouter l'AS400 à l'environnement DD VTL. Ceci est nécessaire pour éviter les numéros de série en double lorsque plusieurs systèmes Data Domain utilisent DD VTL. La valeur du préfixe du numéro de série doit :

- Être une valeur unique à six chiffres de sorte qu'aucune autre DD VTL sur un système Data Domain dans l'environnement n'ait le même numéro de préfixe.
- Ne pas se terminer par un zéro

Configurez cette valeur une seule fois pendant le déploiement du système Data Domain et la configuration de DD VTL. Cette valeur persiste avec toutes les futures mises à niveau DD OS du système. La définition de cette valeur ne nécessite pas de redémarrage du service DD VTL. Toute bibliothèque DD VTL créée après avoir défini cette valeur utilise le nouveau préfixe pour le numéro de série.

CLI equivalent

```
# vtl option set serial-number-prefix value
# vtl option show serial-number-prefix
```

Utilisation des librairies

Une librairie émule une librairie de bandes physique avec des lecteurs, un changeur, des ports CAP (ports d'accès aux cartouches) et des slots (slots de cartouches). Lorsque vous sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries**, des informations détaillées sur toutes les librairies configurées s'affichent.

Tableau 143 Informations sur la librairie

Élément	Description
Name	Nom d'une librairie configurée.
Drives	Nombre de disques configurés dans la librairie.

Tableau 143 Informations sur la librairie (suite)

Élément	Description
Slots	Nombre de slots configurés dans la librairie.
CAPs	Nombre de ports CAP (ports d'accès aux cartouches) configurés dans la librairie.

Dans le menu More Tasks, vous pouvez créer et supprimer des librairies, ainsi que rechercher des bandes.

Création de bibliothèques

DD VTL prend en charge jusqu'à 64 bibliothèques par système, c'est-à-dire 64 instances de bibliothèques de bandes virtuelles actives simultanément sur chaque système DD.

Avant de commencer

Si l'environnement de déploiement inclut un système AS400 en tant que client DD VTL, reportez-vous à la section Configuration des options par défaut de la DD VTL à la page 401 pour configurer le préfixe du numéro de série des changeurs et lecteurs VTL avant de créer la bibliothèque DD VTL et de configurer la relation DD VTL entre le système Data Domain et le système client AS400.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries**.
2. Sélectionnez **More Tasks** > **Library** > **Create**
3. Dans la boîte de dialogue Create Library, saisissez les informations suivantes :

Tableau 144 Boîte de dialogue Create Library

Champ	Saisie utilisateur
Library Name	Saisissez un nom comprenant entre 1 et 32 caractères alphanumériques.
Number of Drives	Saisissez le nombre de disques (de 1 à 98, voir remarque). Le nombre de disques à créer correspondra au nombre de flux de données écrivant dans une bibliothèque. **Remarque** Le nombre maximal de disques pris en charge par une DD VTL dépend du nombre de cœurs de CPU et de la quantité de mémoire installée (RAM et NVRAM, le cas échéant) sur votre système DD.
Drive Model	Sélectionnez le modèle désiré dans la liste déroulante : • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (par défaut)

Tableau 144 Boîte de dialogue Create Library (suite)

Champ	Saisie utilisateur
	• HP-LTO-3 • HP-LTO-4 Ne mélangez pas les types de disque ou les types de média au sein d'une même bibliothèque. Vous risqueriez d'obtenir des résultats inattendus et/ou des erreurs lors de l'opération de sauvegarde.
Number of Slots	Saisissez le nombre de slots de la bibliothèque. Tenez compte des points suivants : • Le nombre de slots doit être supérieur ou égal au nombre de lecteurs. • Le nombre maximal est de 32 000 slots par bibliothèque. • Vous pouvez compter jusqu'à 64 000 slots par système. • Prévoyez suffisamment de slots pour conserver les bandes dans la DD VTL et empêcher leur exportation vers une chambre forte. Cela simplifie les opérations de gestion et évite d'avoir à reconfigurer la DD VTL. • Prenez en compte les applications concédées sous licence par nombre de slots. Admettons, par exemple, que vous configuriez 5 000 slots pour une cartouche standard de 100 Go sur un DD580. Cela serait suffisant pour stocker jusqu'à 500 To (pour un taux de compression raisonnable).
Number of CAPs	(Facultatif) Saisissez le nombre de ports d'accès aux cartouches (CAP). • Le nombre maximal est de 100 CAP par bibliothèque. • Vous pouvez compter jusqu'à 1000 CAP par système. Pour obtenir de l'aide, consultez la documentation de votre application de sauvegarde sur le site de support en ligne.
Changer Model Name	Sélectionnez le modèle désiré dans la liste déroulante : • L180 (par défaut) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL Pour obtenir de l'aide, consultez la documentation de votre application de sauvegarde sur le site de support en ligne. Reportez-vous également à la matrice de support de la DD VTL pour savoir si les bibliothèques émulées sont compatibles avec le logiciel.
Options	

Tableau 144 Boîte de dialogue Create Library (suite)

Champ	Saisie utilisateur
auto-eject	par défaut (désactivé), activé ou désactivé
auto-offline	par défaut (désactivé), activé ou désactivé
barcode-length	par défaut (8), 6, 8 [automatiquement défini sur 6 pour les modèles de changeur L180, RESTORER-L180 et DDVTL]

4. Sélectionnez **OK**.

   Lorsque la boîte de dialogue d'état Create Library indique **Completed**, sélectionnez **OK**.

   La nouvelle bibliothèque s'affiche sous l'icône des bibliothèques dans l'arborescence du service VTL et les options que vous avez configurées apparaissent sous forme d'icônes sous la bibliothèque. La sélection de la bibliothèque permet d'afficher des informations détaillées sur celle-ci dans le volet d'information.

   Notez que l'accès aux bibliothèques de bandes virtuelles et aux disques est géré par des groupes d'accès.

Équivalent CLI

```
# vtl add NewVTL model L180 slots 50 caps 5
This adds the VTL library, NewVTL. Use 'vtl show config NewVTL'
to view it.

# vtl drive add NewVTL count 4 model IBM-LTO-3
This adds 4 IBM-LTO-3 drives to the VTL library, NewVTL.
```

Suppression de bibliothèques

Si une bande est insérée dans un lecteur d'une bibliothèque et que vous supprimez cette dernière, la bande est déplacée dans la chambre forte. Cependant, le pool de la bande reste inchangé.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries**.
2. Sélectionnez **More Tasks** > **Library** > **Delete**.
3. Dans la boîte de dialogue Delete Libraries, cochez la case des éléments à supprimer :
   - nom de chaque bibliothèque ;
   - noms de bibliothèque, pour supprimer toutes les bibliothèques.
4. Sélectionnez **Next**.
5. Vérifiez les bibliothèques à supprimer, puis sélectionnez **Submit** dans les boîtes de dialogue de confirmation
6. Lorsque la boîte de dialogue Delete Libraries Status affiche `Completed`, sélectionnez **Close**. Les bibliothèques sélectionnées sont supprimées de la bibliothèque de bandes virtuelle DD VTL.

Équivalent de l'interface de ligne de commande (CLI)

```
# vtl del OldVTL
```

Recherche de bandes

Différents critères (emplacement, pool et/ou code-barres) peuvent être utilisés pour rechercher une bande.

Procédure

1. Sélectionnez **Virtual Tape Libraries** ou **Pools**.
2. Choisissez la zone (librairie, chambre forte, pool) à laquelle appliquer la recherche.
3. Sélectionnez **More Tasks** > **Tapes** > **Search**.
4. Dans la boîte de dialogue Search Tapes, saisissez des informations au sujet de la bande ou des bandes à localiser.

Tableau 145 Boîte de dialogue Search Tapes

Champ	Saisie utilisateur
Location	Spécifiez un emplacement ou conservez la valeur par défaut (All).
Pool	Sélectionnez le nom du pool dans lequel rechercher la bande. Si aucun pool n'a été créé, utilisez le pool par défaut.
Barcode	Spécifiez un code-barres unique ou conservez la valeur par défaut (*) pour renvoyer un groupe de bandes. Le code-barres autorise les caractères génériques ? et *, où ? remplace n'importe quel caractère unique et * correspond à 0 ou à plusieurs caractères.
Count	Saisissez le nombre maximal de bandes à vous retourner. Si vous laissez ce champ vide, le code-barres par défaut (*) est utilisé.

5. Sélectionnez **Search**.

Utilisation d'une librairie sélectionnée

Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *bibliothèque* pour afficher des informations détaillées sur une librairie sélectionnée.

Tableau 146 Périphériques

Élément	Description
Device	Éléments de la librairie tels que des lecteurs, slots et CAP (ports d'accès aux cartouches).
Loaded	Nombre de périphériques comportant des médias chargés.
Vide	Nombre de périphériques sans médias chargés.
Total	Nombre total de périphériques chargés et vides.

Tableau 147 Options

Propriété	Valeur
auto-eject	activé ou désactivé
auto-offline	activé ou désactivé
barcode-length	6 ou 8

Tableau 148 Tapes

Élément	Description
Pool	Nom du pool dans lequel les bandes se trouvent.
Tape Count	Nombre de bandes dans ce pool.
Capacity	Capacité totale configurée des données des bandes de ce pool, exprimée en Gio (Gibioctet, l'équivalent base-2 des Go, ou Gigaoctets).
Used	Quantité d'espace utilisée sur les bandes virtuelles dans ce pool.
Average Compression	Quantité moyenne de compression atteinte sur les données se trouvant sur les bandes de ce pool.

Dans le menu More Tasks, vous pouvez supprimer, renommer ou définir les options d'une librairie, à savoir créer, supprimer, importer, exporter ou déplacer des bandes ; et ajouter ou supprimer des slots et des ports CAP.

Création de bandes

Vous pouvez créer des bandes dans une librairie ou un pool. S'il est initié à partir d'un pool, le système crée d'abord des bandes, puis les importe dans la librairie.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque* ou **Vault** ou **Pools** > **Pools >** *pool*.
2. Sélectionnez **More Tasks** > **Tapes** > **Create**.
3. Dans la boîte de dialogue Create Tapes, saisissez les informations suivantes sur la bande :

Tableau 149 Boîte de dialogue Create Tapes

Champ	Saisie utilisateur
Library (si initié à partir d'une librairie)	Si un menu déroulant est activé, sélectionnez la librairie ou conservez la sélection par défaut.
Pool Name	Sélectionnez, dans la liste déroulante, le nom du pool auquel la bande appartient. Si aucun pool n'a été créé, utilisez le pool par défaut.
Number of Tapes	Pour une librairie, sélectionnez une valeur entre 1 et 20. Pour un pool, sélectionnez une valeur entre 1 et 100 000, ou conservez la valeur par

Tableau 149 Boîte de dialogue Create Tapes (suite)

Champ	Saisie utilisateur
	défaut (20). (Bien que le nombre de bandes prises en charge soit illimité, vous ne pouvez pas créer plus de 100 000 bandes à la fois.)
Starting Barcode	Entrez le numéro de code-barres initial (au format A99000LA).
Tape Capacity	(Facultatif) spécifiez le nombre de Gio de 1 à 4 000 pour chaque bande (ce paramètre remplace le paramètre de capacité de code-barres). Pour une utilisation efficace de l'espace disque, utilisez 100 Gio maximum.

4. Sélectionnez **OK**, puis **Close**.

Équivalent de l'interface de ligne de commande (CLI)

```
 # vtl tape add A00000L1 capacity 100 count 5 pool VTL_Pool ...
added 5 tape(s)...
```

Remarque

Vous devez également auto-incrémenter les noms de volume de bande au format base10.

Suppression de bandes

Vous pouvez supprimer des bandes dans une librairie ou un pool. S'il est initié à partir d'une librairie, le système exporte d'abord les bandes, puis les supprime. Les bandes doivent être placées dans la chambre forte, pas dans une librairie. Sur un système DD de destination de la réplication, la suppression d'une bande n'est pas autorisée.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque* ou **Vault** ou **Pools** > **Pools >** *pool*.
2. Sélectionnez **More Tasks** > **Tapes** > **Delete**.
3. Dans la boîte de dialogue Delete Tapes, saisissez les informations de recherche relatives aux bandes à supprimer et sélectionnez **Search** :

Tableau 150 Boîte de dialogue Delete Tapes

Champ	Saisie utilisateur
Location	Si une liste déroulante est disponible, sélectionnez une librairie ou conservez la sélection par défaut (**Vault**).
Pool	Sélectionnez le nom du pool dans lequel rechercher la bande. Si aucun pool n'a été créé, utilisez le pool par défaut.
Barcode	Spécifiez un code-barres unique ou conservez la valeur par défaut (*) pour rechercher un groupe de bandes. Le code-barres autorise les caractères génériques ? et *, où ? remplace n'importe quel caractère unique et * correspond à 0 ou à plusieurs caractères.
Count	Saisissez le nombre maximal de bandes à vous retourner. Si vous laissez ce champ vide, le code-barres par défaut (*) est utilisé.

Tableau 150 Boîte de dialogue Delete Tapes (suite)

Champ	Saisie utilisateur
Tapes Per Page	Sélectionnez le nombre maximal de bandes à afficher par page (les valeurs possibles sont 15, 30 et 45).
Select all pages	Cochez la case **Select All Pages** pour sélectionner toutes les bandes renvoyées par la requête de recherche.
Items Selected	Affiche le nombre de bandes sélectionnées sur plusieurs pages (mis à jour automatiquement pour chaque bande sélectionnée).

4. Cochez la case correspondant à la bande à supprimer ou la case correspondant à la colonne d'en-tête pour supprimer toutes les bandes, puis sélectionnez **Next**.
5. Sélectionnez **Submit** dans la fenêtre de confirmation et sélectionnez **Close**.

Remarque

Une fois la bande supprimée, l'espace disque physique utilisé pour la bande n'est récupéré qu'après une opération de nettoyage du système de fichiers.

Équivalent de l'interface de ligne de commande (CLI)

```
# vtl tape del barcode [count count] [pool pool]
```

Par exemple :

```
# vtl tape del A00000L1
```

Remarque

Vous pouvez agir sur des plages ; toutefois, s'il manque une bande dans la plage, l'action s'interrompra.

Importation de bandes

Importer une bande signifie qu'une bande existante sera déplacée de la chambre forte vers un slot de bibliothèque, un lecteur ou un port d'accès à la cartouche (CAP).

Le nombre de bandes que vous pouvez importer simultanément est limité par le nombre de slots disponibles dans la bibliothèque. En d'autres termes, vous ne pouvez pas importer plus de bandes qu'il n'y a de slots disponibles actuellement.

Pour afficher les slots disponibles pour une bibliothèque, sélectionnez la bibliothèque dans le menu de la pile de disques. Le volet d'information pour la bibliothèque indique leur nombre dans la colonne Empty.

- Si une bande se trouve dans un lecteur et qu'il est établi que l'origine de la bande est un slot, un slot est réservé.
- Si une bande se trouve dans un lecteur et que l'origine de la bande est inconnue (slot ou CAP), un slot est réservé.
- Si une bande se trouve dans un lecteur et qu'il est établi que l'origine de la bande est un CAP, aucun slot n'est réservé. (La bande revient vers le CAP une fois supprimée du disque.)
- Pour déplacer une bande vers un lecteur, reportez-vous à la section sur le déplacement des bandes ci-dessous.

Procédure

1. Vous pouvez importer des bandes en suivant l'étape a ou b.

   a. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque*. Choisissez ensuite **More Tasks** > **Tapes** > **Import**. Dans la boîte de dialogue Import Tapes, saisissez les informations relatives aux bandes à importer et sélectionnez **Search** :

   Tableau 151 Boîte de dialogue Import Tapes

Champ	Saisie utilisateur
Location	Si une liste déroulante est disponible, sélectionnez l'emplacement de la bande ou conservez la sélection par défaut (**Vault**).
Pool	Sélectionnez le nom du pool dans lequel rechercher la bande. Si aucun pool n'a été créé, utilisez le pool par défaut.
Barcode	Spécifiez un code-barres unique ou conservez la valeur par défaut (*) pour renvoyer un groupe de bandes. Le code-barres autorise les caractères génériques ? et *, où ? remplace n'importe quel caractère unique et * correspond à 0 ou à plusieurs caractères.
Count	Saisissez le nombre maximal de bandes à vous retourner. Si vous laissez ce champ vide, le code-barres par défaut (*) est utilisé.
Select Destination > Device	Sélectionnez le périphérique de destination où la bande sera importée. Les valeurs possibles sont Drive, CAP et Slot.
Tapes Per Page	Sélectionnez le nombre maximal de bandes à afficher par page. Les valeurs possibles sont 15, 30 at 45.
Items Selected	Affiche le nombre de bandes sélectionnées sur plusieurs pages (mis à jour automatiquement pour chaque bande sélectionnée).

   En fonction des conditions précédentes, la recherche porte sur un ensemble de bandes par défaut afin de sélectionner les bandes à importer. Si le pool, le code-barres ou le nombre est modifié, sélectionnez Search pour mettre à jour l'ensemble des bandes pouvant être choisies.

   b. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries***> library***> Changer** > **Drives >** *drive* **> Tapes**. Sélectionnez les bandes à importer en cochant la case en regard :

   - d'une bande individuelle, ou
   - de la colonne **Barcode** appropriée pour sélectionner toutes les bandes de la page actuelle, ou
   - de la case **Select all pages** pour sélectionner toutes les bandes renvoyées par la requête de recherche.

   Seules les bandes dont l'emplacement est marqué « Vault » peuvent être importées.

   Sélectionnez **Import from Vault**. Ce bouton est désactivé par défaut et activé uniquement lorsque toutes les bandes sélectionnées proviennent de la chambre forte.

2. Dans la vue Import Tapes : library, vérifiez les informations récapitulatives et la liste des bandes, puis sélectionnez **OK**.

3. Sélectionnez **Close** dans la fenêtre d'état.

Équivalent de la CLI

```
# vtl tape show pool VTL_Pool
Processing tapes....
Barcode  Pool     Location State    Size    Used (%)           Comp ModTime
-------- -------- -------- ----- ------- --------------- ---- -------------------
A00000L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00001L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00002L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00003L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00004L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
-------- -------- -------- ----- ------- --------------- ---- -------------------
VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x

# vtl import NewVTL barcode A00000L3 count 5 pool VTL_Pool
... imported 5 tape(s)...

# vtl tape show pool VTL_Pool
Processing tapes....

VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x
```

Exportation de bandes

Exporter une bande revient à retirer cette bande d'un slot, d'un lecteur ou d'un port d'accès à la cartouche (CAP) et à la transférer dans la chambre forte.

Procédure

1. Vous pouvez exporter des bandes en suivant l'étape a ou b.

   a. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque*. Choisissez ensuite **More Tasks** > **Tapes** > **Export**. Dans la boîte de dialogue Export Tape, saisissez les informations de recherche relatives aux bandes à exporter et sélectionnez **Search** :

   Tableau 152 Boîte de dialogue Export Tapes

Champ	Saisie utilisateur
Location	Si une liste déroulante est disponible, sélectionnez le nom de la bibliothèque contenant la bande ou conservez la bibliothèque sélectionnée.
Pool	Sélectionnez le nom du pool dans lequel rechercher la bande. Si aucun pool n'a été créé, utilisez le pool par défaut.
Barcode	Spécifiez un code-barres unique ou conservez la valeur par défaut (*) pour renvoyer un groupe de bandes. Le code-barres autorise les

Tableau 152 Boîte de dialogue Export Tapes (suite)

Champ	Saisie utilisateur
	caractères génériques ? et *, où ? remplace n'importe quel caractère unique et * correspond à 0 ou à plusieurs caractères.
Count	Saisissez le nombre maximal de bandes à vous retourner. Si vous laissez ce champ vide, le code-barres par défaut (*) est utilisé.
Tapes Per Page	Sélectionnez le nombre maximal de bandes à afficher par page. Les valeurs possibles sont 15, 30 at 45.
Select all pages	Cochez la case **Select All Pages** pour sélectionner toutes les bandes renvoyées par la requête de recherche.
Items Selected	Affiche le nombre de bandes sélectionnées sur plusieurs pages (mis à jour automatiquement pour chaque bande sélectionnée).

b. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries***> library***> Changer** > **Drives >** *drive* **> Tapes**. Sélectionnez les bandes à exporter en cochant la case en regard :

- d'une bande individuelle, ou
- de la colonne **Barcode** appropriée pour sélectionner toutes les bandes de la page actuelle, ou
- de la case **Select all pages** pour sélectionner toutes les bandes renvoyées par la requête de recherche.

Seules les bandes ayant un nom de bibliothèque dans la colonne Location peuvent être exportées.

Sélectionnez **Export from Library**. Ce bouton est désactivé par défaut et activé uniquement si toutes les bandes sélectionnées possèdent un nom dans la colonne Location.

2. Dans la vue Export Tapes : library, vérifiez les informations récapitulatives et la liste des bandes, puis sélectionnez **OK**.
3. Sélectionnez **Close** dans la fenêtre d'état.

Équivalent de la CLI

```
# vtl export NewVTL cap address 1 count 4
... exported 4 tape(s)...
```

Déplacement de bandes entre des périphériques dans une bibliothèque

Les bandes peuvent être déplacées entre les périphériques physiques d'une bibliothèque afin d'imiter les procédures du logiciel de sauvegarde s'appliquant aux bibliothèques de bandes physiques (qui, dans une bibliothèque, déplacent une bande d'un slot vers un lecteur, d'un slot vers un CAP, d'un CAP vers un lecteur, et inversement). Dans une bibliothèque de bandes physique, le logiciel de sauvegarde ne déplace jamais une bande hors de la bibliothèque. Par conséquent, la bibliothèque de destination ne peut pas changer et apparaît uniquement pour plus de clarté.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***bibliothèque***.

Notez qu'une fois ouvert à partir d'une bibliothèque, le volet Tapes permet uniquement aux bandes d'être déplacées entre les périphériques.

2. Sélectionnez **More Tasks** > **Tapes** > **Move**.

   Notez qu'une fois ouvert à partir d'une bibliothèque, le volet Tapes permet uniquement aux bandes d'être déplacées entre les périphériques.

3. Dans la boîte de dialogue Move Tape, saisissez les informations relatives aux bandes à déplacer et sélectionnez **Search** :

   Tableau 153 Boîte de dialogue Move Tape

Champ	Saisie utilisateur
Location	L'emplacement ne peut pas être modifié.
Pool	Sélectionnez un pool.
Barcode	Spécifiez un code-barres unique ou conservez la valeur par défaut (*) pour renvoyer un groupe de bandes. Le code-barres autorise les caractères génériques ? et *, où ? remplace n'importe quel caractère unique et * correspond à 0 ou à plusieurs caractères.
Count	Saisissez le nombre maximal de bandes à vous retourner. Si vous laissez ce champ vide, le code-barres par défaut (*) est utilisé.
Tapes Per Page	Sélectionnez le nombre maximal de bandes à afficher par page. Les valeurs possibles sont 15, 30 at 45.
Items Selected	Affiche le nombre de bandes sélectionnées sur plusieurs pages (mis à jour automatiquement pour chaque bande sélectionnée).

4. Dans la liste des résultats de la recherche, sélectionnez la ou les bandes à déplacer.
5. Exécutez l'une des opérations suivantes :
   a. Sélectionnez le périphérique dans la liste Device (par exemple, un slot, un lecteur ou un CAP) et saisissez une adresse de début en utilisant des numéros qui se suivent pour la deuxième bande et pour les bandes suivantes. Pour chaque bande devant être déplacée, si l'adresse spécifiée est occupée, c'est l'adresse disponible suivante qui est utilisée.
   b. Laissez l'adresse vide si la bande se trouvant dans un lecteur provient initialement d'un slot et doit être renvoyée à ce slot ou si la bande doit être déplacée vers le prochain slot disponible.
6. Sélectionnez **Next**.
7. Dans la boîte de dialogue Move Tape, vérifiez les informations récapitulatives et la liste des bandes, puis sélectionnez **Submit**.
8. Sélectionnez **Close** dans la fenêtre d'état.

Ajout de slots

Vous pouvez ajouter des slots à partir d'une bibliothèque configurée afin de modifier le nombre d'éléments de stockage.

Remarque

Certaines applications de sauvegarde ne reconnaissent pas automatiquement que des slots ont été ajoutés à une bibliothèque de bandes virtuelle DD VTL. Consultez la documentation de votre application pour obtenir plus d'informations sur la configuration de l'application pour qu'elle reconnaisse ce type de modification.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque*.
2. Sélectionnez **More Tasks** > **Slots** > **Add**.
3. Dans la boîte de dialogue Add Slots, saisissez le nombre de slots à ajouter. Le nombre total de slots d'une bibliothèque, ou de l'ensemble des bibliothèques d'un système, ne peut pas dépasser 32 000 pour une bibliothèque et 64 000 pour un système.
4. Sélectionnez **OK** et **Close** lorsque que l'état est `Completed`.

Suppression de slots

Vous pouvez supprimer des slots d'une bibliothèque configurée pour modifier le nombre d'éléments de stockage.

Remarque

Certaines applications de sauvegarde ne reconnaissent pas automatiquement que des slots ont été supprimés d'une bibliothèque de bandes virtuelle DD VTL. Consultez la documentation de votre application pour obtenir plus d'informations sur la configuration de l'application pour qu'elle reconnaisse ce type de modification.

Procédure

1. Si le slot à supprimer contient des cartouches, transférez ces cartouches dans la chambre forte. Le système supprime uniquement les slots vides, non validés.
2. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque*.
3. Sélectionnez **More Tasks** > **Slots** > **Delete**.
4. Dans la boîte de dialogue Delete Slots, saisissez le nombre de slots à supprimer.
5. Sélectionnez **OK** et **Close** lorsque que l'état est `Completed`.

Ajout de CAP

Vous pouvez ajouter des CAP (ports d'accès à la cartouche) à partir d'une librairie configurée pour modifier le nombre d'éléments de stockage.

Remarque

Seul un nombre limité d'applications de sauvegarde utilise les CAP. Consultez la documentation de votre application afin de vous assurer que les CAP sont pris en charge.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque*.
2. Sélectionnez **More Tasks** > **CAPs** > **Add**.

3. Dans la boîte de dialogue Add CAPs, entrez le nombre de CAP à ajouter. Vous pouvez ajouter de 1 à 100 CAP par librairie et de 1 à 1 000 CAP par système.
4. Sélectionnez **OK** et **Close** lorsque que l'état est `Completed`.

Suppression de ports d'accès aux cartouches

Vous pouvez supprimer des ports d'accès aux cartouches (CAP) à partir d'une bibliothèque configurée pour modifier le nombre d'éléments de stockage.

Remarque

Certaines applications de sauvegarde ne détectent pas automatiquement que les ports d'accès aux cartouches (CAP) ont été supprimés d'une bibliothèque de bandes virtuelle DD VTL. Consultez la documentation de votre application pour obtenir plus d'informations sur la configuration de l'application pour qu'elle reconnaisse ce type de modification.

Procédure

1. Si le port d'accès aux cartouches à supprimer contient des cartouches, transférez ces cartouches vers la chambre forte, ou cela sera effectué automatiquement.
2. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque*.
3. Sélectionnez **More Tasks** > **CAPs** > **Delete**.
4. Dans la boîte de dialogue Delete CAPs, saisissez le nombre de ports d'accès aux cartouches à supprimer. Vous pouvez supprimer 100 ports CAP maximum par bibliothèque ou 1 000 ports CAP maximum par système.
5. Sélectionnez **OK** et **Close** lorsque que l'état est `Completed`.

Affichage des informations sur le changeur

Il ne peut y avoir qu'un seul changeur par DD VTL. Le modèle de changeur que vous sélectionnez dépend de votre configuration spécifique.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries**.
2. Sélectionnez une bibliothèque spécifique.
3. Si celle-ci n'est pas développée, sélectionnez le signe plus (**+**) sur la gauche pour ouvrir la bibliothèque, puis sélectionnez un élément Changer pour afficher le volet des informations relatives au changeur. Celui-ci contient les données suivantes.

Tableau 154 Volet des informations relatives aux changeurs

Élément	Description
Vendor	Nom du fournisseur du changeur
Product	Nom de modèle
Révision	Niveau de révision
Serial Number	Numéro de série du changeur

Utilisation des disques

Lorsque vous sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries** *> library >***Drives**, des informations détaillées sur tous les disques s'affichent pour une bibliothèque sélectionnée.

Tableau 155 Volet des informations relatives aux disques

Colonne	Description
Drive	Liste des lecteurs présentés par nom, dans laquelle le nom est « Drive # », # étant un nombre compris entre 1 et n qui représente l'adresse ou l'emplacement du lecteur dans la liste des lecteurs.
Vendor	Fabricant ou fournisseur du lecteur, par exemple, IBM.
Product	Nom de produit du lecteur, par exemple, ULTRIUM-TD5.
Revision	Numéro de révision du lecteur.
Serial Number	Numéro de série du lecteur.
Status	Indique si le lecteur est vide, ouvert, verrouillé ou chargé. Une bande doit être présente pour que le lecteur soit verrouillé ou chargé.
Tape	Code-barres de la bande se trouvant dans le lecteur (le cas échéant).
Pool	Pool de la bande dans le lecteur (le cas échéant).

Pilotes de bibliothèques et de bandes : pour utiliser des disques, vous devez utiliser les pilotes de bibliothèques et de bandes fournis par l'éditeur de votre logiciel de sauvegarde, qui prennent en charge les disques BM LTO-1, IBM LTO-2, IBM LTO-3, IBM LTO-4, IBM LTO-5 (par défaut), HP-LTO-3 ou HP-LTO-4 et les bibliothèques StorageTek L180 (par défaut), RESTORER-L180, IBM TS3500, I2000, I6000 ou DDVTL. Pour plus d'informations, consultez les documents *Application Compatibility Matrices and Integration Guides* correspondant à l'éditeur de votre logiciel. Lors de la configuration des disques, gardez également à l'esprit les limites relatives aux flux de données de sauvegarde, qui sont définies par la plate-forme en cours d'utilisation.

Capacités de disque LTO : étant donné que le système DD considère les disques LTO comme des disques virtuels, vous pouvez définir une capacité de 4 Tio (4 000 Gio) maximum pour chaque type de disque. Les capacités par défaut pour chaque type de disque LTO sont les suivantes :

- Disque LTO-1 : 100 Gio
- Disque LTO-2 : 200 Gio
- Disque LTO-3 : 400 Gio
- Disque LTO-4 : 800 Gio
- Disque LTO-5 : 1,5 Tio

Migration de bandes LTO-1 : vous pouvez migrer des bibliothèques de bandes virtuelles de type LTO-1 existantes vers des bibliothèques de bandes virtuelles contenant d'autres disques et bandes de type LTO pris en charge. Les options de migration sont différentes pour chaque application de sauvegarde. Par conséquent, suivez les instructions décrites dans le guide de migration de bandes LTO spécifique de votre application. Pour trouver le guide approprié, accédez au site de support en ligne, puis saisissez **LTO Tape Migration for VTLs** dans la zone de texte de recherche.

Bande pleine : avertissement précoce : vous recevez un avertissement lorsque l'espace restant sur la bande est quasi plein, c'est-à-dire supérieur à 99,9, mais inférieur à 100 pour cent. L'application peut continuer à écrire jusqu'à ce que la capacité de la bande atteigne 100 %. La dernière écriture ne peut toutefois pas être récupérée.

Dans le menu More Tasks, vous pouvez créer ou supprimer un disque.

Création de disques

Pour déterminer le nombre maximal de disques pris en charge par votre DD VTL, reportez-vous à la section *Nombre de disques pris en charge par une DD VTL*.

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque***> Changer** > **Drives**.
2. Sélectionnez **More Tasks** > **Drives** > **Create**.
3. Dans la boîte de dialogue Create Drive, saisissez les informations suivantes :

   Tableau 156 Boîte de dialogue Create Drive

Champ	Saisie utilisateur
Location	Sélectionnez un nom de bibliothèque ou conservez le nom sélectionné.
Number of Drives	Reportez-vous au tableau de la section *Nombre de disques pris en charge par une DD VTL* dont il est question plus haut dans ce chapitre.
Model Name	Sélectionnez le modèle dans la liste déroulante. Si un autre disque existe déjà, cette option est inactive et le type de disque existant doit être utilisé. Vous ne pouvez pas associer plusieurs types de disque dans la même bibliothèque. • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (par défaut) • HP-LTO-3 • HP-LTO-4

4. Sélectionnez **OK** et, lorsque l'état indique `Completed`, sélectionnez **OK**.

   Le disque ajouté apparaît dans la liste des disques.

Suppression de lecteurs

Videz le lecteur avant de le supprimer.

Procédure

1. Si le lecteur que vous souhaitez supprimer contient une bande, retirez celle-ci.
2. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries >** *bibliothèque***> Changer** > **Drives**.
3. Sélectionnez **More Tasks** > **Drives** > **Delete**.

4. Dans la boîte de dialogue Delete Drives, cochez les cases des lecteurs à supprimer ou cochez la case **Drive** pour supprimer tous les lecteurs.
5. Sélectionnez **Next**. Assurez-vous que le ou les lecteurs corrects ont été sélectionnés en vue de la suppression et sélectionnez **Submit**.
6. Lorsque la boîte de dialogue Delete Drive Status indique `Completed`, sélectionnez **Close**.

   Le lecteur est retiré de la liste des lecteurs.

Utilisation d'un lecteur sélectionné

Les options **Virtual Tape Libraries** > **VTL Service** > **Libraries** > *bibliothèque*> **Drives** >*lecteur* affichent des informations détaillées sur un lecteur sélectionné.

Tableau 157 Onglet Drive

Colonne	Description
Drive	Liste des lecteurs présentés par nom, dans laquelle le nom est « Drive # », # étant un nombre compris entre 1 et n qui représente l'adresse ou l'emplacement du lecteur dans la liste des lecteurs.
Vendor	Fabricant ou fournisseur du lecteur, par exemple, IBM.
Product	Nom de produit du lecteur, par exemple, ULTRIUM-TD5.
Revision	Numéro de révision du lecteur.
Serial Number	Numéro de série du lecteur.
Status	Indique si le lecteur est vide, ouvert, verrouillé ou chargé. Une bande doit être présente pour que le lecteur soit verrouillé ou chargé.
Tape	Code-barres de la bande se trouvant dans le lecteur (le cas échéant).
Pool	Pool de la bande dans le lecteur (le cas échéant).

Tableau 158 Onglet Statistics

Colonne	Description
Endpoint	Nom spécifique du point d'accès.
Ops/s	Opérations par seconde.
Read KiB/s	Vitesse des lectures en KiB/s par seconde.
Write KiB/s	Vitesse des écritures en KiB/s par seconde.

Le menu More Tasks permet de supprimer le disque ou d'effectuer une actualisation.

Utilisation des bandes

Une bande est représentée comme un fichier. Les bandes peuvent être importées de la chambre forte vers une bibliothèque. Les bandes peuvent être exportées d'une bibliothèque vers la chambre forte. Il est possible de déplacer des bandes entre des

disques, des slots (slots de cartouches) et des ports CAP (ports d'accès aux cartouches) d'une bibliothèque.

Une fois créées, les bandes sont placées dans la chambre forte. Une fois ajoutées à la chambre forte, elles peuvent être importées, exportées, déplacées, recherchées ou supprimées.

Lorsque vous sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries***> librairie >***Tapes**, des informations détaillées sur toutes les bandes s'affichent poubibliothèquerairie sélectionnée.

Tableau 159 Description des bandes

Élément	Description
Barcode	Code-barres unique pour la bande.
Pool	Nom du pool qui contient la bande. Le pool par défaut contient toutes les bandes qui n'ont pas été attribuées à un pool créé par l'utilisateur.
Location	Emplacement de la bande, qu'elle se trouve dans une bibliothèque (et disque, port CAP ou numéro de slot) ou dans la chambre forte virtuelle.
State	État de la bande. • RW – Read-Writeable (lecture-écriture) • RL – Retention-Lock (rétention verrouillée) • RO – Read-Only (lecture seule) • WP – Write-Protected (protégé en écriture) • RD – Replication destination (destination de réplication)
Capacity	Capacité totale de la bande.
Used	Quantité d'espace utilisée sur la bande.
Compression	Taux de compression effectué sur les données de la bande.
Last Modified	Date de la dernière modification apportée aux informations relatives à la bande. Les heures de modification utilisées par le système pour les stratégies basées sur l'âge peuvent différer de l'heure de la dernière modification affichée dans les sections d'informations sur les bandes de DD System Manager.
Locked Until	Si un délai de verrouillage de la rétention (DD Retention Lock) a été spécifié, l'heure définie s'affiche. S'il n'y a aucun verrouillage de rétention, cette valeur est `Not specified`.

Dans le volet d'information, vous pouvez importer une bande depuis la chambre forte, exporter une bande vers la bibliothèque, définir l'état d'une bande, créer une bande ou supprimer une bande.

Dans le menu More Tasks, vous pouvez déplacer une bande.

Modification de l'état de verrouillage de la rétention ou de l'écriture d'une bande

Avant de modifier l'état de verrouillage de la rétention ou de l'écriture d'une bande, cette dernière doit avoir été créée et importée. Les bandes DD VTL doivent respecter la stratégie standard relative au verrouillage de la rétention Data Domain. Au terme de la période de rétention d'une bande, celle-ci ne peut pas accueillir de nouvelle écriture ou être modifiée (elle peut toutefois être supprimée).

Procédure

1. Sélectionnez **Virtual Tape Libraries** > **VTL Service** > **Libraries** > ***bibliothèque*** > **Tapes**.
2. Sélectionnez la bande à modifier dans la liste, puis **Set State** (au-dessus de la liste).
3. Dans la boîte de dialogue Set Tape State, sélectionnez **Read-Writeable**, **Write-Protected** ou **Retention-Lock**.
4. Si l'état est Retention-Lock,
   - saisissez la date d'expiration de la bande dans un nombre défini de jours, semaines, mois ou années, ou
   - sélectionnez l'icône de calendrier, puis choisissez une date dans le calendrier. L'état Retention-Lock expire à midi à la date sélectionnée.
5. Sélectionnez **Next**, puis **Submit** pour modifier l'état.

Utilisation de la chambre forte

La chambre forte contient les bandes qui ne sont utilisées par aucune bibliothèque. Les bandes résident dans une bibliothèque ou dans la chambre forte.

La sélection de **Virtual Tape Libraries** > **VTL Service** > **Vault** affiche des informations détaillées sur le pool par défaut et sur tous les autres pools de la chambre forte.

Les systèmes avec DD Cloud Tier et DD VTL permettent de stocker la chambre forte sur le stockage cloud.

Tableau 160 Récapitulatif du pool

Élément	Description
Pool Count	Nombre de pools VTL.
Tape Count	Nombre de bandes dans les pools.
Size	Quantité totale d'espace dans les pools.
Logical Used	Quantité totale d'espace utilisée dans les pools.
Compression	Quantité moyenne de compression dans les pools.

Le volet **Protection Distribution** affiche les informations suivantes.

Remarque

Ce tableau s'affiche uniquement si DD Cloud Tier est activé sur le système Data Domain.

Tableau 161 Distribution de la protection

Élément	Description
Storage type	Stockage en chambre forte ou Cloud.
Fournisseur de Cloud	Pour les systèmes avec bandes dans DD Cloud Tier, il existe une colonne pour chaque fournisseur de Cloud.
Logical Used	Quantité totale d'espace utilisée dans les pools.
Pool Count	Nombre de pools VTL.
Tape Count	Nombre de bandes dans les pools.

Le menu More Tasks vous permet de créer, supprimer et rechercher des bandes dans la chambre forte.

Utilisation de la chambre forte Cloud

DD VTL prend en charge plusieurs paramètres qui sont uniques pour les configurations dans lesquelles la chambre forte est stockée sur un stockage DD Cloud Tier.

Les opérations suivantes sont disponibles pour utiliser le stockage de la chambre forte Cloud.

- Configurez la règle de déplacement des données et les informations de l'unité de Cloud pour le pool VTL spécifié. Exécutez la commande **`vtl pool modify <pool-name> data-movement-policy {user-managed | age-threshold <days> | none} to-tier {cloud} cloud-unit <cloud-unit-name>`**.
  Les politiques de déplacement des données disponibles sont :
  - User-managed : l'administrateur peut définir cette politique sur un pool afin de sélectionner manuellement les bandes du pool pour la migration vers le niveau cloud. Les bandes migrent vers le niveau cloud au cours de la première opération de déplacement des données après la sélection des bandes.
  - Age-threshold : l'administrateur peut définir cette politique sur un pool de sorte que DD VTL puisse sélectionner automatiquement les bandes du pool pour la migration vers le niveau cloud en fonction de l'ancienneté de la bande. Les bandes sont sélectionnées pour la migration dans un délai de six heures après qu'elles aient atteint le seuil d'ancienneté. Puis, elles sont transférées au cours de la première opération de déplacement des données après la sélection des bandes.
- Sélectionnez une bande spécifiée pour la migration vers le niveau cloud. Exécutez la commande **`vtl tape select-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}`**.
- Désélectionnez une bande spécifiée pour la migration vers le niveau cloud. Exécutez la commande **`vtl tape deselect-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}`**.
- Rappelez une bande à partir du niveau cloud. Exécutez la commande **`vtl tape recall start barcode <barcode> [count <count>] pool <pool>`**.
  Après le rappel, la bande réside dans une chambre forte DD VTL et doit être importée dans la bibliothèque pour y accéder.

Remarque

Exécutez la commande `vtl tape show` à tout moment pour vérifier l'emplacement en cours d'une bande. L'emplacement de la bande est mis à jour dans l'heure qui suit le déplacement de la bande vers ou depuis le niveau cloud.

Préparer le pool VTL pour le déplacement de données

Définissez la règle de déplacement des données sur le pool VTL pour gérer la migration des données VTL à partir de la chambre forte locale vers DD Cloud Tier.

Le déplacement des données pour VTL se produit au niveau du volume de bande. Les volumes de bandes individuels ou les collections de volumes de bande peuvent être déplacés vers le niveau Cloud, mais uniquement à partir de l'emplacement de la chambre forte. Les bandes dans d'autres éléments d'une VTL ne peuvent pas être déplacées.

Remarque

Le pool VTL par défaut et la chambre forte, les répertoires `/data/col1/backup` ou les configurations de bibliothèque héritées ne peuvent servir pour déplacer des bandes sur le Cloud.

Procédure

1. Sélectionnez **Protocols** > **DD VTL**.
2. Développez la liste des pools, puis sélectionnez un pool sur lequel vous activez la migration vers DD Cloud Tier.
3. Dans le volet **Cloud Data Movement**, cliquez sur **Create** sous **Cloud Data Movement Policy**.
4. Dans la liste déroulante **Policy**, sélectionnez une règle de déplacement des données :
   - **Age of tapes in days**
   - **Manual selection**
5. Définissez les détails de la règle de déplacement des données.
   - Pour **Age of tapes in days**, sélectionnez un seuil d'ancienneté après lequel les bandes sont migrées vers DD Cloud Tier et spécifiez une unité de Cloud de destination.
   - Pour **Manual selection**, spécifiez une unité de Cloud de destination.
6. Cliquez sur **Create**.

   Remarque

   Après avoir créé la règle de déplacement des données, les boutons **Edit** et **Clear** peuvent être utilisés pour modifier ou supprimer la règle de déplacement des données.

Équivalent CLI

Procédure

1. Définissez la règle de déplacement des données sur user-managed ou age-threshold

   Remarque

   Le pool VTL et l'unité de Cloud sont sensibles à la casse et les commandes échouent si la casse n'est pas correcte.

   - Pour définir la règle de déplacement des données sur user-managed, exécutez la commande suivante :
     `vtl pool modify cloud-vtl-pool data-movement-policy user-managed to-tier cloud cloud-unit ecs-unit1`

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy is set to "user-managed" for VTL pool "cloud-vtl-pool".
```

   - Pour définir la règle de déplacement des données sur age-threshold, exécutez la commande suivante :

     Remarque

     La valeur minimum est de 14 jours et la valeur maximum de 182 250 jours.

     `vtl pool modify cloud-vtl-pool data-movement-policy age-threshold 14 to-tier cloud cloud-unit ecs-unit1`

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy "age-threshold" is set to 14 days for the VTL pool "cloud-
vtl-pool".
```

2. Vérifiez la règle de déplacement des données pour le pool VTL.

   Exécutez la commande suivante :
   `vtl pool show all`

```
VTL Pools
Pool                  Status   Tapes   Size (GiB)   Used (GiB)   Comp   Cloud Unit
Cloud Policy
--------------------  ------   -----   ----------   ----------   ----   ----------
------------
cloud-vtl-pool        RW          50          250           41    45x   ecs-unit1
user-managed
Default               RW           0            0            0     0x   -
none
--------------------  ------   -----   ----------   ----------   ----   ----------
------------
8080 tapes in 5 pools

 RO  : Read Only
 RD  : Replication Destination
 BCM : Backwards-Compatibility
```

3. Vérifiez que la règle pour la structure MTree du pool VTL est `app-managed`.

   Exécutez la commande suivante :
   `data-movement policy show all`

```
Mtree                      Target(Tier/Unit Name)   Policy        Value
-------------------------  ----------------------   -----------   -------
```

```
/data/col1/cloud-vtl-pool   Cloud/ecs-unit1          app-managed   enabled
-------------------------   ----------------------   -----------   -------
```

Retirer les bandes de l'inventaire de l'application de sauvegarde

Utilisez l'application de sauvegarde pour vérifier que les volumes de bande qui seront déplacés vers le cloud sont marqués et inventoriés selon les exigences de l'application de sauvegarde.

Sélectionner des volumes de bande pour le déplacement des données

Sélectionnez manuellement les bandes pour la migration vers DD Cloud Tier (immédiatement ou lors de la prochaine migration de données planifiées) ou supprimez manuellement les bandes dans le planning de migration.

Avant de commencer

Vérifiez que l'application de sauvegarde est au courant des changements de statut pour les volumes déplacés sur le stockage cloud. Réalisez toutes les étapes nécessaires pour que l'application de sauvegarde actualise son inventaire afin de refléter le dernier état des volumes.

Si la bande n'est pas dans la chambre forte, elle ne peut pas être migrée vers DD Cloud Tier.

Procédure

1. Sélectionnez **Protocols** > **DD VTL**.
2. Développez la liste des pools et sélectionnez le pool qui est configuré pour migrer des bandes vers DD Cloud Tier.
3. Dans le volet Pool, cliquez sur l'onglet **Tape**.
4. Sélectionnez les bandes pour la migration vers DD Cloud Tier.
5. Cliquez sur **Select for Cloud Move** pour migrer la bande lors de la migration planifiée suivante, ou sur **Move to Cloud Now** pour migrer immédiatement la bande.

   Remarque

   Si la règle de déplacement des données est basée sur l'ancienneté des bandes, l'option **Select for Cloud Move** n'est pas disponible, car le système Data Domain sélectionne automatiquement les bandes pour la migration.

6. Dans la fenêtre de confirmation, cliquez sur **Yes**.

Désélectionner des volumes de bande pour le déplacement des données

Les bandes sélectionnées pour la migration vers DD Cloud Tier peuvent être supprimées à partir du planning de migration.

Procédure

1. Sélectionnez **Protocols** > **DD VTL**.
2. Développez la liste des pools et sélectionnez le pool qui est configuré pour migrer des bandes vers DD Cloud Tier.
3. Dans le volet Pool, cliquez sur l'onglet **Tape**.
4. Sélectionnez les bandes pour la migration vers DD Cloud Tier.

5. Cliquez sur **Unselect Cloud Move** pour supprimer la bande du planning de migration.
6. Dans la fenêtre de confirmation, cliquez sur **Yes**.

Équivalent CLI

Procédure

1. Identifiez l'emplacement du volume de bande à déplacer.

   Exécutez la commande suivante :
   `vtl tape show cloud-vtl`

```
Processing tapes....
Barcode    Pool             Location            State    Size           Used (%)
Comp   Modification Time
--------   --------------   -----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1    RW      5 GiB   5.0 GiB (99.07%)
205x   2017/05/05 10:43:43
T00002L3   cloud-vtl-pool   cloud-vtl slot 2    RW      5 GiB   5.0 GiB (99.07%)
36x   2017/05/05 10:45:10
T00003L3   cloud-vtl-pool   cloud-vtl slot 3    RW      5 GiB   5.0 GiB (99.07%)
73x   2017/05/05 10:45:26
```

2. Spécifiez la valeur numérique du logement pour exporter la bande à partir de la DD VTL.

   Exécutez la commande suivante :
   `vtl export cloud-vtl-pool slot 1 count 1`

3. Vérifiez que la bande se trouve dans la chambre forte.

   Exécutez la commande suivante :
   `vtl tape show vault`

4. Sélectionnez la bande pour le déplacement des données.

   Exécutez la commande suivante :
   `vtl tape select-for-move barcode T00001L3 count 1 pool cloud-vtl-pool to-tier cloud`

   Remarque

   Si la règle de déplacement des données est définie sur age-threshold, le déplacement des données s'effectue automatiquement au bout de 15-20 minutes.

5. Affichez la liste des bandes devant être déplacées vers le stockage cloud au cours de la prochaine opération de déplacement des données. Les bandes sélectionnées pour le déplacement s'affiche dans un `(S)` dans la colonne Location.

   Exécutez la commande suivante :
   `vtl tape show vault`

```
Processing tapes.....
Barcode    Pool               Location    State      Size          Used (%)   Comp
Modification Time
--------   ----------------   ---------   ------   ------   ----------------   ----
-------------------
T00003L3   cloud-vtl-pool     vault (S)   RW        5 GiB   5.0 GiB (99.07%)    63x
2017/05/05 10:43:43
T00006L3   cloud-vtl-pool     ecs-unit1   n/a       5 GiB   5.0 GiB (99.07%)    62x
2017/05/05 10:45:49
--------   ----------------   ---------   ------   ------   ----------------   ----
```

```
-------------------
* RD : Replication Destination
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4024
Total pools:               3
Total size of tapes:       40175 GiB
Total space used by tapes: 39.6 GiB
Average Compression:       9.7x
```

6. Si la règle de déplacement des données est définie sur user-managed, lancez l'opération de déplacement des données.

   Exécutez la commande suivante :
   `data-movement start`

7. Observez l'état de l'opération de déplacement des données.

   Exécutez la commande suivante :
   `data-movement watch`

8. Vérifiez que les volumes de la bande se déplacent correctement vers le stockage cloud.

   Exécutez la commande suivante :
   `vtl tape show all cloud-unit ecs-unit1`

```
Processing tapes.....
Barcode  Pool           Location  State  Size         Used (%) Comp Modification Time
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
T00001L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  89x 2017/05/05 10:41:41
T00006L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  62x 2017/05/05 10:45:49
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4
Total pools:               2
Total size of tapes:       16 GiB
Total space used by tapes: 14.9 GiB
Average Compression:       59.5x
```

Restaurer les données contenues dans le cloud

Lorsqu'un client demande à ce que des données soient restaurées à partir du serveur de l'application de sauvegarde, cette dernière doit générer une alerte ou un message demandant les volumes nécessaires de l'unité de cloud.

Le volume doit être rappelé sur le cloud et archivé dans la bibliothèque VTL Data Domaine avant que l'application de sauvegarde soit avisée de la présence des volumes.

Remarque

Vérifiez que l'application de sauvegarde est au courant des changements de statut pour les volumes déplacés sur le stockage cloud. Réalisez toutes les étapes nécessaires pour que l'application de sauvegarde actualise son inventaire afin de refléter le dernier état des volumes.

Rappeler manuellement un volume de bande à partir d'un stockage cloud

Rappel d'une bande à partir de DD Cloud Tier vers la chambre forte VTL locale.

Procédure

1. Sélectionnez **Protocols** > **DD VTL**.
2. Développez la liste des pools et sélectionnez le pool qui est configuré pour migrer des bandes vers DD Cloud Tier.
3. Dans le volet Pool, cliquez sur l'onglet **Tape**.
4. Sélectionnez une ou plusieurs bandes situées dans une unité de cloud.
5. Cliquez sur **Recall Cloud Tapes** pour rappeler des bandes à partir de DD Cloud Tier.

Résultats

Après la prochaine migration des données planifiée, les bandes sont rappelées à partir de l'unité de cloud vers la chambre forte. Les bandes peuvent être renvoyées de la chambre forte vers une bibliothèque.

Équivalent CLI

Procédure

1. Identifiez le volume requis pour restaurer les données.
2. Rappelez le volume de bande à partir de la chambre forte.

   Exécutez la commande suivante :
   ```
   vtl tape recall start barcode T00001L3 count 1 pool cloud-vtl-pool
   ```
3. Vérifiez que l'opération de rappel a commencé.

   Exécutez la commande suivante :
   ```
   data-movement status
   ```
4. Vérifiez l'aboutissement de l'opération de rappel.

   Exécutez la commande suivante :
   ```
   vtl tape show all barcode T00001L3
   ```

```
Processing tapes....
Barcode    Pool             Location           State    Size           Used (%)
Comp   Modification Time
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1   RW      5 GiB   5.0 GiB (99.07%)
239x   2017/05/05 10:41:41
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     1
Total pools:               1
Total size of tapes:       5 GiB
Total space used by tapes: 5.0 GiB
Average Compression:       239.1x
```

5. Validez l'emplacement du fichier.

Exécutez la commande suivante :
`filesys report generate file-location path /data/col1/cloud-vtl-pool`

```
filesys report generate file-location path /data/col1/cloud-vtl-pool
------------------------------      --------------------------
File Name                           Location(Unit Name)
------------------------------      --------------------------
/data/col1/cloud-vtl-pool/.vtl_pool     Active
/data/col1/cloud-vtl-pool/.vtc/T00001L3 Active
----------------------------------------------------------------
```

6. Importez la bande rappelée dans la DD VTL.

   Exécutez la commande suivante :
   `vtl import cloud-vtl barcode T00001L3 count 1 pool cloud-vtl-pool element slot`

```
imported 1 tape(s)...sysadmin@ddbeta70# vtl tape show cloud-vtlProcessing tapes.....
```

7. Vérifiez le volume dans l'inventaire de l'application de sauvegarde.
8. Restaurez les données par le biais de l'application de sauvegarde.
9. Lorsque la restauration est terminée, vérifiez le volume de bande de l'inventaire de l'application de sauvegarde.
10. Exportez le volume de bande à partir de la librairie de bandes virtuelle Data Domain vers la chambre forte Data Domain.
11. Replacez la bande dans l'unité de Cloud.

Utilisation des groupes d'accès

Les *groupes d'accès* sont créés afin de contenir un ensemble de WWPN (noms de ports internationaux) ou d'alias d'initiateurs, ainsi que les disques et changeurs auxquels ils sont autorisés à accéder. Un groupe DD VTL par défaut nommé *TapeServer* vous permet d'ajouter des périphériques qui prendront en charge les applications de sauvegarde basées sur NDMP (Network Data Management Protocol).

La configuration du groupe d'accès permet aux initiateurs (généralement des applications de sauvegarde) de lire et d'écrire des données sur des périphériques dans le même groupe d'accès.

Les groupes d'accès n'autorisent les clients à accéder qu'à des LUN (changeurs de médias ou lecteurs de bandes virtuelles) sélectionnées sur un système. Un client configuré pour un groupe d'accès peut uniquement accéder aux périphériques de ce groupe d'accès.

Évitez de modifier vos groupes d'accès lorsque des tâches de sauvegarde ou de restauration sont en cours, pour ne pas prendre le risque de les voir échouer. L'impact des modifications lorsqu'une tâche est en cours dépend de la configuration de l'hôte et de celle du logiciel de sauvegarde.

La sélection de **Access Groups** > **Groups** affiche les informations suivantes pour tous les groupes d'accès.

Tableau 162 Informations sur le groupe d'accès

Élément	Description
Group Name	Nom du groupe.
Initiators	Nombre d'initiateurs dans le groupe.

Tableau 162 Informations sur le groupe d'accès (suite)

Élément	Description
Devices	Nombre de périphériques dans le groupe.

La sélection de **View All Access Groups** vous permet d'accéder à la vue Fibre Channel.

Le menu More Tasks vous permet de créer ou de supprimer un groupe.

Création d'un groupe d'accès

Les groupes d'accès gèrent les accès entre les périphériques et les initiateurs. N'utilisez pas le groupe d'accès TapeServer par défaut sauf si vous utilisez NDMP.

Procédure

1. Sélectionnez **Access Groups** > **Groups**.
2. Sélectionnez **More Tasks** > **Group** > **Create**
3. Dans la boîte de dialogue Create Access Group, saisissez un nom comportant entre 1 et 128 caractères, puis sélectionnez **Next.**
4. Ajoutez les périphériques, puis sélectionnez **Next.**
5. Consultez le récapitulatif, puis sélectionnez **Finish** ou **Back** le cas échéant.

   Équivalent de la CLI

   ```
   # vtl group create My_Group
   ```

Ajout d'un périphérique à un groupe d'accès

La configuration du groupe d'accès permet aux initiateurs (généralement des applications de sauvegarde) de lire et d'écrire des données sur des périphériques dans le même groupe d'accès.

Procédure

1. Sélectionnez **Access Groups** > **Groups**. Vous pouvez également sélectionner un *groupe* spécifique.
2. Sélectionnez **More Tasks** > **Group** > **Create** ou **Group** > **Configure**.
3. Dans la boîte de dialogue Create or Modify Access Group, saisissez ou modifiez le **nom du groupe**, le cas échéant. (Ce champ est obligatoire.)
4. Pour configurer des initiateurs pour le groupe d'accès, cochez la case en regard de l'initiateur. Vous pourrez ajouter des initiateurs au groupe ultérieurement.
5. Sélectionnez **Next**.
6. Dans le volet Devices, sélectionnez Add (**+**) pour afficher la boîte de dialogue Add Devices.
   a. Vérifiez que la bibliothèque appropriée est sélectionnée dans la liste déroulante Library Name, ou sélectionnez une autre bibliothèque.
   b. Dans la zone Device, cochez les cases correspondant aux périphériques (changeur et disques) à inclure dans le groupe.
   c. Vous pouvez également spécifier une LUN de départ dans la zone de texte LUN Start Address.

      Il s'agit de la LUN que le système DD renvoie à l'initiateur. Chaque périphérique est identifié de manière unique par la bibliothèque et son propre

nom. (Par exemple, il est possible qu'il y ait un disque 1 dans la bibliothèque 1 et un disque 1 dans la bibliothèque 2). Par conséquent, une LUN est associée à un périphérique, identifié par sa bibliothèque et son nom.

Lors de la présentation des numéros d'unité logique (LUN) via les ports FC rattachés sur les adaptateurs HBA / cartes SLIC Fibre Channel, trois désignations de ports sont possibles : primaire, secondaire ou aucune désignation. Le port principal d'un ensemble d'unités logiques (LUN) est le port qui annonce actuellement ces LUN sur un fabric. Un port secondaire est un port qui diffusera un ensemble de LUN en cas d'échec du chemin principal (cette opération nécessite une intervention manuelle). Utilisez le paramètre None si vous ne souhaitez pas annoncer les LUN sélectionnées. La présentation des LUN dépend de la topologie SAN en question.

Les initiateurs du groupe d'accès interagissent avec les périphériques de la LUN qui ont été ajoutés au groupe.

Le nombre maximal de LUN acceptées lors de la création d'un groupe d'accès est de 16 383.

Une LUN ne peut être utilisée qu'une seule fois pour chaque groupe individuel. La même LUN peut être utilisée avec plusieurs groupes.

Certains initiateurs (clients) sont dotés de règles spécifiques pour la numérotation des LUN cible, nécessitant, par exemple, la LUN 0 ou des LUN consécutives. Si ces règles ne sont pas respectées, un initiateur ne sera pas en mesure d'accéder à certaines ou à toutes les LUN attribuées à un port cible de DD VTL.

Consultez la documentation relative à votre initiateur pour connaître les règles qui lui sont associées et, si nécessaire, modifiez les LUN du périphérique sur le port cible de DD VTL pour respecter ces règles. Par exemple, si un initiateur requiert que la LUN 0 soit attribuée sur le port cible de DD VTL, examinez les LUN des périphériques attribués aux ports et si aucun périphérique n'est attribué à la LUN 0, modifiez la LUN d'un périphérique de sorte que celui-ci soit attribué à la LUNO 0.

d. Dans la zone Primary and Secondary Endpoints, sélectionnez une option pour déterminer les ports à partir desquels le périphérique sélectionné sera visible. Les conditions suivantes s'appliquent aux ports désignés :

- all : le périphérique sélectionné est visible à partir de tous les ports.
- none : le périphérique sélectionné n'est visible à partir d'aucun port.
- select : le périphérique sélectionné est visible à partir des ports sélectionnés. Cochez les cases correspondant aux ports appropriés. Si seuls les ports principaux sont sélectionnés, le périphérique sélectionné n'est visible que par ces ports.

  Si seuls les ports secondaires sont sélectionnés, le périphérique sélectionné n'est visible que par ces ports. Les ports secondaires peuvent être utilisés si les ports principaux deviennent indisponibles.

Le basculement vers un port secondaire ne se fait pas automatiquement. Vous devez basculer manuellement le périphérique DD VTL vers les ports secondaires si les ports principaux deviennent indisponibles.

La liste des ports contient des numéros des ports physiques. Un numéro de port indique le slot PCI, et une lettre indique le port sur une carte PCI. Par exemple : 1a, 1b ou 2a, 2b.

Un disque s'affiche avec la même LUN sur tous les ports que vous avez configurés.

e. Sélectionnez **OK**.

Vous êtes redirigé vers la boîte de dialogue Devices dans laquelle le nouveau groupe est répertorié. Pour ajouter d'autres périphériques, répétez ces cinq sous-étapes.

7. Sélectionnez **Next**.
8. Sélectionnez **Close** lorsque le message d'état `Completed` s'affiche.

Équivalent CLI

```
# vtl group add VTL_Group vtl NewVTL changer lun 0 primary-port all secondary-port all#
vtl group add VTL_Group vtl NewVTL drive 1 lun 1 primary-port all secondary-port all#
vtl group add SetUp_Test vtl SetUp_Test drive 3 lun 3 primary-port endpoint-fc-0
secondary-port endpoint-fc-1

# vtl group show Setup_Test
Group: SetUp_Test

Initiators:
Initiator Alias   Initiator WWPN
---------------   ----------------------
tsm6_p23          21:00:00:24:ff:31:ce:f8
---------------   ----------------------

Devices:
Device Name          LUN   Primary Ports   Secondary Ports    In-use Ports
------------------   ---   -------------   ---------------   -------------
SetUp_Test changer     0             all               all             all
SetUp_Test drive 1     1             all               all             all
SetUp_Test drive 2     2              5a                5b              5a
SetUp_Test drive 3     3   endpoint-fc-0     endpoint-fc-1   endpoint-fc-0
------------------   ---   -------------   ---------------   -------------
```

Modification ou suppression d'un périphérique d'un groupe d'accès

Il se peut que vous deviez modifier ou supprimer un périphérique d'un groupe d'accès.

Procédure

1. Sélectionnez **Protocols** > **VTL** > **Access Groups** > **Groups** > *groupe*.
2. Sélectionnez **More Tasks** > **Group** > **Configure**.
3. Dans la boîte de dialogue Modify Access Group, saisissez ou modifiez le nom du groupe (**Group Name**). (Ce champ est obligatoire.)
4. Pour configurer des initiateurs pour le groupe d'accès, cochez la case en regard de l'initiateur. Vous pourrez ajouter des initiateurs au groupe ultérieurement.
5. Sélectionnez **Next**.
6. Sélectionnez un périphérique, puis cliquez sur l'icône de modification (crayon) pour afficher la boîte de dialogue Modify Devices. Suivez ensuite les étapes a à e. Si vous souhaitez simplement supprimer le périphérique, sélectionnez l'icône de suppression (x) et passez à l'étape e.
   a. Vérifiez que la bibliothèque appropriée est sélectionnée dans la liste déroulante Library, ou sélectionnez une autre bibliothèque.
   b. Dans la zone Devices to Modify, cochez les cases des périphériques (changeur et disques) à modifier.
   c. Vous pouvez également modifier la LUN (unité logique) de départ dans la zone LUN Start Address.

      Il s'agit de la LUN que le système DD renvoie à l'initiateur. Chaque périphérique est identifié de manière unique par la bibliothèque et son propre

nom. (Par exemple, il est possible qu'il y ait un disque 1 dans la bibliothèque 1 et un disque 1 dans la bibliothèque 2). Par conséquent, une LUN est associée à un périphérique, identifié par sa bibliothèque et son nom.

Les initiateurs du groupe d'accès interagissent avec les périphériques de la LUN qui ont été ajoutés au groupe.

Le nombre maximal de LUN acceptées lors de la création d'un groupe d'accès est de 16 383.

Une LUN ne peut être utilisée qu'une seule fois pour chaque groupe individuel. La même LUN peut être utilisée avec plusieurs groupes.

Certains initiateurs (clients) sont dotés de règles spécifiques pour la numérotation des LUN cible, nécessitant, par exemple, la LUN 0 ou des LUN consécutives. Si ces règles ne sont pas respectées, un initiateur ne sera pas en mesure d'accéder à certaines ou à toutes les LUN attribuées à un port cible de DD VTL.

Consultez la documentation relative à votre initiateur pour connaître les règles qui lui sont associées et, si nécessaire, modifiez les LUN du périphérique sur le port cible de DD VTL pour respecter ces règles. Par exemple, si un initiateur requiert que la LUN 0 soit attribuée sur le port cible de DD VTL, examinez les LUN des périphériques attribués aux ports et si aucun périphérique n'est attribué à la LUN 0, modifiez la LUN d'un périphérique de sorte que celui-ci soit attribué à la LUNO 0.

d. Dans la zone Primary and Secondary Ports, modifiez l'option qui détermine les ports à partir desquels le périphérique sélectionné est visible. Les conditions suivantes s'appliquent aux ports désignés :

   - all : le périphérique sélectionné est visible à partir de tous les ports.
   - none : le périphérique sélectionné n'est visible à partir d'aucun port.
   - select : le périphérique sélectionné est visible à partir des ports sélectionnés. Cochez les cases correspondant aux ports à partir desquels il sera visible.
     Si seuls les ports principaux sont sélectionnés, le périphérique sélectionné n'est visible que par ces ports.

     Si seuls les ports secondaires sont sélectionnés, le périphérique sélectionné n'est visible que par ces ports. Les ports secondaires peuvent être utilisés si les ports principaux deviennent indisponibles.

   Le basculement vers un port secondaire ne se fait pas automatiquement. Vous devez basculer manuellement le périphérique DD VTL vers les ports secondaires si les ports principaux deviennent indisponibles.

   La liste des ports contient des numéros des ports physiques. Un numéro de port indique le slot PCI, et une lettre indique le port sur une carte PCI. Par exemple : 1a, 1b ou 2a, 2b.

   Un disque s'affiche avec la même LUN sur tous les ports que vous avez configurés.

e. Sélectionnez **OK**.

Suppression d'un groupe d'accès

Avant de pouvoir supprimer un groupe d'accès, vous devez supprimer tous ses initiateurs et toutes ses LUN.

Procédure

1. Supprimez tous les initiateurs et toutes les LUN du groupe.
2. Sélectionnez **Access Groups** > **Groups**.
3. Sélectionnez **More Tasks** > **Group** > **Delete**.
4. Dans la boîte de dialogue Delete Group, cochez la case correspondant au groupe à supprimer, puis sélectionnez **Next**.
5. Dans la boîte de dialogue de confirmation des groupes, vérifiez la suppression, puis sélectionnez **Submit**.
6. Sélectionnez **Close** lorsque Delete Groups Status affiche `Completed`.

Équivalent de l'interface de ligne de commande (CLI)

```
# scsitarget group destroy My_Group
```

Utilisation d'un groupe d'accès sélectionné

Lorsque vous sélectionnez **Access Groups** > **Groups** > *groupe*, les informations suivantes s'affichent pour un groupe d'accès sélectionné.

Tableau 163 Onglet LUNs

Élément	Description
LUN	Adresse du périphérique : le nombre maximal est de 16 383. Une LUN ne peut être utilisée qu'une seule fois au sein d'un groupe, mais peut être réutilisée dans un autre groupe. Les périphériques DD VTL ajoutés à un groupe doivent utiliser des LUN consécutives.
Library	Nom de la bibliothèque associée à la LUN.
Device	Changeurs et disques.
In-Use Endpoints	Ensemble de points de terminaison actuellement utilisés : primaire ou secondaire.
Primary Endpoints	Point de terminaison d'origine (ou par défaut) utilisé par l'application de sauvegarde. En cas de panne sur ce point de terminaison, le point de terminaison secondaire peut être utilisé, s'il est disponible.
Secondary Endpoints	Ensemble des points de terminaison de basculement à utiliser si le point de terminaison primaire est défaillant.

Tableau 164 Onglet Initiators

Élément	Description
Name	Nom de l'initiateur. Il s'agit du WWPN ou de l'alias attribué à l'initiateur.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).

Le menu More Tasks d'un groupe sélectionné vous permet de configurer ce groupe ou de définir les points de terminaison en cours d'utilisation.

Sélection de points d'accès pour un périphérique

Puisque les points d'accès connectent un périphérique à un initiateur, utilisez ce processus pour configurer les points d'accès avant de connecter le périphérique.

Procédure

1. Sélectionnez **Access Groups** > **Groups***> group*.
2. Sélectionnez **More Tasks** > **Endpoints** > **Set In-Use**.
3. Dans la boîte de dialogue Set in-Use Endpoints, sélectionnez uniquement des périphériques spécifiques, ou utilisez l'option **Devices** pour sélectionner tous les périphériques de la liste.
4. Précisez si les points d'accès sont principaux et secondaires.
5. Sélectionnez **OK**.

Configuration du groupe de serveurs de bandes du périphérique NDMP

Le groupe de serveurs de bandes DD VTL contient les lecteurs de bande qui interagissent avec des applications de sauvegarde NDMP (Network Data Management Protocol) et qui envoient des informations de contrôle et des flux de données via IP au lieu de Fibre Channel (FC). Un périphérique utilisé par le serveur de bandes NDMP doit se trouver dans le serveur de bandes du groupe DD VTL. Il est *uniquement* disponible sur le serveur de bandes NDMP.

Procédure

1. Ajoutez des lecteurs de bande à une bibliothèque nouvelle ou existante (nommée « dd990-16 » dans cet exemple).
2. Créez des slots et des ports d'accès aux cartouches pour la bibliothèque.
3. Ajoutez les périphériques créés dans une bibliothèque (nommée « dd990-16 » dans cet exemple) au groupe d'accès aux serveurs de bandes.
4. Activez le processus NDMP en saisissant ce qui suit dans la ligne de commande :

```
# ndmpd enable
Starting NDMP daemon, please wait.............
NDMP daemon is enabled.
```

5. Assurez-vous que le processus NDMP voit les périphériques du groupe de serveurs de bandes :

```
# ndmpd show devicenames
NDMP Device          Virtual Name       Vendor   Product       Serial Number
-----------------    ----------------   ------   -----------   -------------
/dev/dd_ch_c0t0l0    dd990-16 changer   STK      L180          6290820000
/dev/dd_st_c0t1l0    dd990-16 drive 1   IBM      ULTRIUM-TD3   6290820001
/dev/dd_st_c0t2l0    dd990-16 drive 2   IBM      ULTRIUM-TD3   6290820002
/dev/dd_st_c0t3l0    dd990-16 drive 3   IBM      ULTRIUM-TD3   6290820003
/dev/dd_st_c0t4l0    dd990-16 drive 4   IBM      ULTRIUM-TD3   6290820004
-----------------    ----------------   ------   -----------   -------------
```

6. Ajoutez un utilisateur NDMP (ndmp dans cet exemple) à l'aide de la commande suivante :

```
# ndmpd user add ndmp
Enter password:
Verify password:
```

7. Vérifiez que l'utilisateur ndmp est correctement ajouté :

```
# ndmpd user show
ndmp
```

8. Affichez la configuration NDMP :

```
# ndmpd option show all
Name             Value
--------------   --------
authentication   text
debug            disabled
port             10000
preferred-ip
--------------   --------
```

9. Modifiez l'authentification par mot de passe par défaut des utilisateurs pour utiliser le chiffrement MD5 afin d'en améliorer la sécurité, puis vérifiez la modification (notez les valeurs d'authentification modifiées entre la version texte et la version md5) :

```
# ndmpd option set authentication md5# ndmpd option show all
Name             Value
--------------   --------
authentication   md5
debug            disabled
port             10000
preferred-ip
--------------   --------
```

Résultats

NDMP est maintenant configuré, et le groupe d'accès aux serveurs de bandes affiche la configuration du périphérique. Consultez le chapitre `ndmpd` du *Guide de référence des commandes de Data Domain Operating System* pour obtenir une présentation des options et de l'ensemble des commandes.

Utilisation des ressources

La sélection de **Resources** > **Resources** affiche des informations sur les initiateurs et les points de terminaison. Un *initiateur* est un client de sauvegarde qui se connecte au système pour lire et écrire des données à l'aide du protocole FC (Fibre Channel). Un initiateur spécifique peut prendre en charge DD Boost over FC ou DD VTL, mais pas les deux. Un *point de terminaison* est la cible logique, dans le système DD, à laquelle l'initiateur est connecté.

Tableau 165 Onglet Initiators

Élément	Description
Name	Nom de l'initiateur. Il s'agit du WWPN ou de l'alias attribué à l'initiateur.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
Online Endpoints	Nom du groupe dans lequel l'initiateur peut voir les ports. Affiche `None` ou `Offline` si l'initiateur est indisponible.

Tableau 166 Onglet Endpoints

Élément	Description
Name	Nom spécifique du point de terminaison.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
System Address	Adresse système du point de terminaison.
Enabled	État opérationnel du port de l'adaptateur HBA, qui est soit `Yes` (activé) soit `No` (désactivé).
État	État de la liaison DD VTL, qui est soit `Online` (capable de traiter le trafic), soit `Offline`.

Configure Resources
La sélection de **Configure Resources** permet d'accéder à la zone Fibre Channel où il est possible de configurer les points de terminaison et les initiateurs.

Utilisation des initiateurs

La sélection de **Physical Resources** > **Physical Resources** > **Initiators** permet d'afficher des informations sur les initiateurs. Un *initiateur* est un WWPN (nom de port international) de HBA FC (adaptateur HBA Fibre Channel) de système client avec lequel le système DD communique. Un *nom d'initiateur* est un alias du WWPN du client permettant une plus grande facilité d'utilisation.

Lorsqu'un client est mappé en tant qu'initiateur (avant, cependant, qu'un groupe d'accès n'ait été ajouté), il ne peut pas accéder aux données d'un système DD.

Une fois qu'un groupe d'accès pour l'initiateur ou le client a été ajouté, le client peut uniquement accéder aux périphériques de ce groupe d'accès. Un client est susceptible d'avoir des groupes d'accès à plusieurs périphériques.

Un groupe d'accès peut contenir plusieurs initiateurs, mais un initiateur ne peut appartenir qu'à un seul groupe d'accès.

Remarque

Il est possible de configurer 1 024 initiateurs au maximum pour un système DD.

Tableau 167 Informations sur l'initiateur

Élément	Description
Name	Nom de l'initiateur.
Group	Groupe associé à l'initiateur.
Online Endpoints	Points de terminaison vus par l'initiateur. Affiche `none` ou `offline` si l'initiateur est indisponible.

Tableau 167 Informations sur l'initiateur (suite)

Élément	Description
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
Vendor Name	Nom du fournisseur de l'initiateur.

La sélection de **Configure Initiators** donne accès à la zone Fibre Channel dans laquelle vous pouvez configurer les points de terminaison et les initiateurs.

Équivalent CLI

```
# vtl initiator show
Initiator  Group      Status  WWNN                    WWPN                    Port
---------  ---------  ------  ----------------------  ----------------------  ----
tsm6_p1    tsm3500_a  Online  20:00:00:24:ff:31:ce:f8  21:00:00:24:ff:31:ce:f8 10b
---------  ---------  ------  ----------------------  ----------------------  ----

Initiator  Symbolic Port Name                          Address Method
---------  ------------------------------------------  --------------
tsm6_p1    QLE2562 FW:v5.06.03 DVR:v8.03.07.15.05.09-k  auto
---------  ------------------------------------------  --------------
```

Utilisation des points d'accès

Sélectionnez **Resources** > **Resources** > **Endpoints** pour obtenir des informations sur le matériel et la connectivité du point de terminaison.

Tableau 168 Onglet Hardware

Élément	Description
System Address	Adresse système du point de terminaison.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
Enabled	État opérationnel du port de l'adaptateur HBA (adaptateur de bus hôte), qui est soit `Yes` (activé), soit `No` (désactivé).
NPIV	État NPIV de ce point de terminaison : Enabled ou Disabled.
Link Status	État de la liaison de ce point de terminaison : Online ou Offline.
Operation Status	État de l'opération de ce point de terminaison : Normal ou Marginal.

Tableau 168 Onglet Hardware (suite)

Élément	Description
# of Endpoints	Nombre de points de terminaison associés à ce point de terminaison.

Tableau 169 Onglet Endpoints

Élément	Description
Name	Nom spécifique du point de terminaison.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
System Address	Adresse système du point de terminaison.
Enabled	État opérationnel du port de l'adaptateur HBA, qui est soit `Yes` (activé) soit `No` (désactivé).
Link Status	État de la liaison de ce point de terminaison : Online ou Offline.

Configure Endpoints
Sélectionnez **Configurer Endpoints** pour accéder à la zone Fibre Channel, où vous pourrez modifier les informations ci-dessus pour le point de terminaison.

Équivalent CLI

```
# scsitarget endpoint show list
Endpoint       System Address  Transport     Enabled  Status
--------       --------------  ---------     -------  ------
endpoint-fc-0  5a              FibreChannel  Yes      Online
endpoint-fc-1  5b              FibreChannel  Yes      Online
```

Utilisation d'un point de terminaison sélectionné

La sélection de **Resources** > **Resources** > **Endpoints** > *endpoint* fournit des informations sur le matériel, la connectivité et les statistiques du point de terminaison.

Tableau 170 Onglet Hardware

Élément	Description
System Address	Adresse système du point de terminaison.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).

Tableau 170 Onglet Hardware (suite)

Élément	Description
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
Enabled	État opérationnel du port de l'adaptateur HBA (adaptateur de bus hôte), qui est soit `Yes` (activé), soit `No` (désactivé).
NPIV	État NPIV de ce point de terminaison : Enabled ou Disabled.
Link Status	État de la liaison de ce point de terminaison : Online ou Offline.
Operation Status	État de l'opération de ce point de terminaison : Normal ou Marginal.
# of Endpoints	Nombre de points de terminaison associés à ce point de terminaison.

Tableau 171 Onglet Summary

Élément	Description
Name	Nom spécifique du point de terminaison.
WWPN	Nom de port international unique. Il s'agit de l'identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du port Fibre Channel (FC).
WWNN	Nom de nœud international unique. Il s'agit d'un identifiant de 64 bits (une valeur de 60 bits précédée d'un identifiant *Network Address Authority* de 4 bits) du nœud FC.
System Address	Adresse système du point de terminaison.
Enabled	État opérationnel du port de l'adaptateur HBA (adaptateur de bus hôte), qui est soit `Yes` (activé), soit `No` (désactivé).
LInk Status	État de la liaison de ce point de terminaison : Online ou Offline.

Tableau 172 Onglet Statistics

Élément	Description
Endpoint	Nom spécifique du point de terminaison.
Library	Nom de la librairie contenant le point de terminaison.
Device	Nombre de périphériques.
Ops/s	Opérations par seconde.
Read KiB/s	Vitesse des lectures en Kio/s par seconde.
Write KiB/s	Vitesse des écritures en Kio/s par seconde.

Tableau 173 Onglet Detailed Statistics

Élément	Description
Endpoint	Nom spécifique du point de terminaison.
# of Control Commands	Nombre de commandes de contrôle.
# of Read Commands	Nombre de commandes de lecture
# of Write Commands	Nombre de commandes d'écriture.
In (Mio)	Nombre de Mio écrits (l'équivalent binaire de Mo).
Out (Mio)	Nombre de Mio lus.
# of Error Protocol	Nombre d'erreurs de protocole.
# of Link Fail	Nombre d'échecs de liaison
# of Invalid Crc	Nombre de CRC (vérifications de redondance cyclique) non valides.
# of Invalid TxWord	Nombre de mots Tx (transmission) non valides.
# of Lip	Nombre de LIP (primitives d'initialisation de la boucle).
# of Loss Signal	Nombre de signaux ou de connexions perdus.
# of Loss Sync	Nombre de signaux ou de connexions qui ont perdu la synchronisation.

Utilisation des pools

La sélection de **Pools** > **Pools** affiche des informations détaillées sur le pool par défaut et sur tout autre pool existant. Un *pool* est un ensemble de bandes qui est mappé à un répertoire du système de fichiers. Les pools servent à répliquer des bandes sur une destination. Vous pouvez convertir des pools basés sur répertoire en pools basés sur MTree afin de profiter des fonctionnalités plus importantes des MTree.

Tenez compte des points suivants concernant les pools :

- Les pools peuvent être de deux types : Mtree (recommandé) ou répertoire, à compatibilité descendante.
- Un pool peut être répliqué quel que soit l'emplacement des bandes individuelles. Les bandes peuvent se trouver dans la chambre forte ou dans une bibliothèque (slot, CAP ou disque).
- Vous pouvez copier et déplacer des bandes d'un pool vers un autre.
- Le logiciel de sauvegarde n'a pas accès aux pools.
- Aucune configuration ni licence de DD VTL n'est nécessaire sur une destination de réplication lors de la réplication des pools.
- Vous devez créer des bandes dont les codes-barres sont uniques. Les codes-barres dupliqués peuvent provoquer un comportement imprévisible des applications de sauvegarde et être source de confusion pour les utilisateurs.
- Il est possible pour deux bandes se trouvant dans deux pools différents sur un système DD de porter le même nom. Dans ce cas, aucune bande ne peut être déplacée vers le pool de l'autre bande. De même, un pool envoyé à une destination de réplication doit posséder un nom qui est unique sur la destination.

Tableau 174 Onglet Pools

Élément	Description
Name	Nom du pool.
Type	Indique s'il s'agit d'un pool de répertoires ou de MTrees.
État	État du pool.
Tape Count	Nombre de bandes dans le pool.
Size	Capacité totale configurée des données des bandes du pool, exprimée en Gio (Gibioctet, l'équivalent base-2 des Go, ou Gigaoctets).
Physical Used	Quantité d'espace utilisée sur les bandes virtuelles du pool.
Compression	Quantité moyenne de compression atteinte pour les données se trouvant sur les bandes du pool.
Cloud Unit	Le nom de l'unité Cloud vers laquelle le pool DD VTL migre les données.
Cloud Data Movement Policy	Règle de mouvement des données qui régit la migration des données DD VTL vers le stockage DD Cloud Tier.

Tableau 175 Onglet Replication

Élément	Description
Name	Nom du pool.
Configured	Indique si la réplication est configurée pour le pool : yes (oui) ou no (non).
Remote Source	Contient une entrée uniquement si le pool est répliqué depuis un autre système DD.
Remote Destination	Contient une entrée uniquement si le pool est répliqué vers un autre système DD.

Le menu More Tasks permet de créer et de supprimer des pools, ainsi que de rechercher des bandes.

Création de pools

Vous pouvez créer des pools rétrocompatibles (si votre configuration l'exige), par exemple, à des fins de réplication avec un système antérieur à DD OS 5.2.

Procédure

1. Sélectionnez **Pools** > **Pools**.
2. Sélectionnez **More Tasks** > **Pool** > **Create**.
3. Dans la boîte de dialogue Create Pool, saisissez un nom de pool, en gardant à l'esprit qu'un nom de pool :
   - ne peut pas être « all, » « vault » ou « summary ».
   - ne doit pas débuter ou se terminer par un espace ou un point ;
   - n'est pas sensible à la casse.

4. Si vous souhaitez créer un pool de répertoires (compatible avec la version précédente de DD System Manager), sélectionnez l'option « Create a directory backwards compatibility mode pool. » Toutefois, rappelez-vous que l'utilisation d'un pool MTree présente de nombreux avantages, notamment la possibilité de réaliser les opérations suivantes :
   - effectuer des snapshots individuels et planifier des snapshots ;
   - appliquer des verrous de rétention ;
   - définir une politique de rétention individuelle ;
   - obtenir des informations de compression ;
   - obtenir des règles de migration de données au niveau de rétention ;
   - créer une règle d'utilisation de l'espace de stockage (prise en charge de quota) en définissant des limites souple et stricte.
5. Sélectionnez **OK** pour afficher la boîte de dialogue Create Pool Status.
6. Lorsque la boîte de dialogue Create Pool Status affiche `Completed`, sélectionnez **Close**. Le pool est ajouté au sous-arbre des pools, et vous pouvez désormais lui ajouter des bandes virtuelles.

Équivalent CLI

```
# vtl pool add VTL_Pool
A VTL pool named VTL_Pool is added.
```

Suppression de pools

Avant de pouvoir supprimer un pool, vous devez avoir supprimé toutes les bandes qu'il contient. Si la réplication est configurée pour le pool, la paire de réplication doit également être supprimée. Supprimer un pool consiste à renommer la Mtree, puis à la supprimer, ce qui se produit lors du processus de nettoyage suivant.

Procédure

1. Sélectionnez **Pools** > **Pools** > ***pool***.
2. Sélectionnez **More Tasks** > **Pool** > **Delete**.
3. Dans la boîte de dialogue Delete Pools, cochez la case des éléments à supprimer :
   - le nom de chaque pool, ou
   - **Pool Names** pour supprimer tous les pools.
4. Sélectionnez **Submit** dans les boîtes de dialogue de confirmation.
5. Lorsque la boîte de dialogue Delete Pool Status indique `Completed`, sélectionnez **Close**.

   Le pool sera supprimé de la sous-arborescence Pools.

Utilisation d'un pool sélectionné

Aussi bien **Virtual Tape Libraries** > **VTL Service** > **Vault** > *pool* que **Pools** > **Pools** > *pool* affichent des informations détaillées sur un pool. Vous pouvez remarquer que le pool « Default » existe toujours.

Onglet Pool

Tableau 176 Récapitulatif

Élément	Description
Convert to MTree Pool	Sélectionnez ce bouton pour convertir un pool de répertoires en pool de MTrees.
Type	Indique s'il s'agit d'un pool de répertoires ou de MTrees.
Tape Count	Nombre de bandes dans le pool.
Capacity	Capacité totale configurée des données des bandes du pool, exprimée en Gio (Gibioctet, l'équivalent base-2 des Go, ou Gigaoctets).
Logical Used	Quantité d'espace utilisée sur les bandes virtuelles du pool.
Compression	Quantité moyenne de compression atteinte pour les données se trouvant sur les bandes du pool.

Tableau 177 Onglet Pool : Cloud Data Movement - Protection Distribution

Élément	Description
Pool type (%)	Pool VTL et cloud (le cas échéant), avec le pourcentage de données en cours entre parenthèses.
Name	Nom du pool VTL local ou fournisseur de cloud.
Logical Used	Quantité d'espace utilisée sur les bandes virtuelles du pool.
Tape Count	Nombre de bandes dans le pool.

Tableau 178 Onglet Pool : Cloud Data Movement - Cloud Data Movement Policy

Élément	Description
Policy	Ancienneté des bandes en jours ou sélection manuelle.
Older Than	Seuil d'ancienneté pour une règle de déplacement des données basées sur l'ancienneté.
Cloud Unit	Unité de cloud de destination.

Onglet Tape

Tableau 179 Commandes pour les bandes

Élément	Description
Create	Créez une bande.
Delete	Supprimez les brandes sélectionnées.
Copy	Effectuez la copie d'une bande.
Move between Pool	Déplacez les bandes sélectionnées vers un autre pool.
Select for Cloud Move[a]	Planifiez la migration des bandes sélectionnées vers DD Cloud Tier.

Tableau 179 Commandes pour les bandes (suite)

Élément	Description
Unselect from Cloud Move[a]	Supprimez les bandes sélectionnées du planning de migration vers DD Cloud Tier.
Recall Cloud Tapes	Rappelez les bandes sélectionnées à partir de DD Cloud Tier.
Move to Cloud Now	Migrez les bandes sélectionnées vers DD Cloud Tier sans attendre la prochaine migration planifiée.

a. Cette option n'est disponible que si la règle de déplacement des données est configurée pour la sélection manuelle.

Tableau 180 Informations sur les bandes

Élément	Description
Barcode	Code-barres des bandes.
Size	Taille maximale de la bande.
Physical Used	Capacité de stockage physique utilisée par la bande.
Compression	Taux de compression sur la bande.
Location	Emplacement de la bande.
Modification Time	Heure de la dernière modification de la bande.
Recall Time	Heure du dernier rappel de la bande.

Onglet Replication

Tableau 181 Réplication

Élément	Description
Name	Nom du pool.
Configured	Indique si la réplication est configurée pour le pool : oui ou non.
Remote Source	Contient une entrée uniquement si le pool est répliqué depuis un autre système DD.
Remote Destination	Contient une entrée uniquement si le pool est répliqué vers un autre système DD.

Vous pouvez également sélectionner le bouton **Replication Detail**, dans le coin supérieur droit, pour accéder directement au volet d'information Replication concernant le pool sélectionné.

Dans le menu More Tasks, la zone Virtual Tape Libraries ou Pools permet de créer, supprimer, déplacer, copier ou rechercher une bande dans le pool.

Dans le menu More Tasks, la zone Pools permet, en outre, de renommer ou de supprimer un pool.

Conversion d'un pool de répertoires en pool de Mtrees

Les pools de MTrees présentent de nombreux avantages par rapport aux pools de répertoires. Pour plus d'informations, reportez-vous à la section *Création de pools*.

Procédure

1. Assurez-vous que les préalables exigés suivants ont été respectés :
   - Les pools source et de destination doivent avoir été synchronisés pour que le nombre de bandes et les données de chaque côté restent inchangés.
   - Le pool de répertoires ne doit pas être une source ou une destination de réplication.
   - Le système de fichiers ne doit pas être plein.
   - Le système de fichiers ne doit pas avoir atteint le nombre maximal de Mtrees autorisé (100).
   - Il ne doit pas y avoir de Mtree portant déjà le même nom.
   - Si le pool de répertoires est en cours de duplication sur plusieurs systèmes, ces systèmes de réplication doivent être connus du système de gestion.
   - Si le pool de répertoires est répliqué sur un DD OS plus ancien (par exemple, de DD OS 5.5 à DD OS 5.4), il ne peut pas être converti. Solution :
     - Répliquez le pool de répertoires sur un deuxième système DD.
     - Répliquez le pool de répertoires du deuxième système DD vers un troisième système DD.
     - Supprimez les deuxième et troisième systèmes DD du réseau Data Domain du système de gestion DD.
     - Sur n'importe quel système exécutant DD OS 5.5, dans le sous-menu Pools, sélectionnez **Pools** ou un pool de répertoires. Sur l'onglet Pools, sélectionnez **Convert to MTree Pool**.
2. Le pool de répertoires que vous souhaitez convertir étant en surbrillance, choisissez **Convert to MTree Pool**.
3. Dans la boîte de dialogue MTree Pool, sélectionnez **OK**.
4. Gardez à l'esprit que la conversion a l'effet suivant sur la réplication :
   - La DD VTL est temporairement désactivée sur les systèmes répliqués lors de la conversion.
   - Les données de destination sont copiées dans un nouveau pool sur le système de destination afin de conserver les données jusqu'à ce que la nouvelle réplication soit initialisée et synchronisée. Vous pouvez ensuite supprimer en toute sécurité ce pool temporairement copié, nommé **CONVERTED-***pool*, dans lequel *pool* est le nom du pool qui a été mis à niveau (ou les 18 premiers caractères des noms de pool longs). [Cela s'applique uniquement à DD OS 5.4.1.0 et versions supérieures.]
   - Le répertoire de réplication cible est converti au format Mtree. [Ceci s'applique uniquement à DD OS 5.2 et versions supérieures].
   - Les paires de réplication sont rompues avant la conversion du pool. Elles sont rétablies ensuite si aucune erreur ne se produit.

- DD Retention Lock ne peut pas être activé sur les systèmes concernés par la conversion de pool de Mtrees.

Déplacement de bandes entre des pools

Lorsqu'elles résident dans la chambre forte, les bandes peuvent être déplacées d'un pool à un autre pour autoriser des opérations de réplication. Par exemple, des pools sont nécessaires si toutes les bandes ont été créées dans le pool par défaut, mais, plus tard, vous aurez besoin de groupes indépendants pour la réplication de groupes de bandes. Vous pouvez créer des pools nommés et réorganiser les groupes de bandes dans de nouveaux pools.

Remarque

Vous ne pouvez pas déplacer des bandes à partir d'un pool de bandes qui est une source de réplication de répertoire. Pour contourner ce problème, vous pouvez procéder comme suit :

- Copiez la bande vers un nouveau pool, puis supprimez la bande de l'ancien pool.
- Utilisez un pool de structure MTree pour déplacer des bandes à partir d'un pool de bandes qui est une source de réplication de répertoire.

Procédure

1. Avec un pool mis en surbrillance, sélectionnez **More Tasks** > **Tapes** > **Move**.

   Notez que lorsque la procédure est initiée à partir d'un pool, le volet de bandes permet le déplacement des bandes entre des pools.

2. Dans la boîte de dialogue Move Tapes, saisissez les informations relatives aux bandes à déplacer et sélectionnez **Search** :

   Tableau 182 Boîte de dialogue Move Tapes

Champ	Saisie utilisateur
Location	L'emplacement ne peut pas être modifié.
Pool	Sélectionnez le nom du pool dans lequel les bandes résident. Si aucun pool n'a été créé, utilisez le pool par défaut.
Barcode	Spécifiez un code-barres unique ou conservez la valeur par défaut (*) pour importer un groupe de bandes. Le code-barres autorise les caractères génériques ? et *, où ? remplace n'importe quel caractère unique et * correspond à 0 ou à plusieurs caractères.
Count	Saisissez le nombre maximal de bandes à vous retourner. Si vous laissez ce champ vide, le code-barres par défaut (*) est utilisé.
Tapes Per Page	Sélectionnez le nombre maximal de bandes à afficher par page. Les valeurs possibles sont 15, 30 at 45.
Items Selected	Affiche le nombre de bandes sélectionnées sur plusieurs pages (mis à jour automatiquement pour chaque bande sélectionnée).

3. Dans la liste des résultats de la recherche, sélectionnez les bandes à déplacer.

4. Dans la liste Select Destination: Location, sélectionnez l'emplacement du pool dans lequel les bandes doivent être déplacées. Cette option n'est disponible que lorsqu'elle est démarrée à partir de la vue (nommée) Pool.
5. Sélectionnez **Next**.
6. Dans la vue Move Tapes, vérifiez les informations récapitulatives et la liste de bandes, puis sélectionnez **Submit**.
7. Sélectionnez **Close** dans la fenêtre d'état.

Copie de bandes entre des pools

Les bandes peuvent être copiées entre les pools, ou de la chambre forte dans un pool, pour faciliter les activités de réplication. Cette option n'est disponible que lorsqu'elle est démarrée à partir de la vue (nommée) Pool.

Procédure

1. Avec un pool mis en surbrillance, sélectionnez **More Tasks** > **Tapes** > **Copy**.
2. Dans la boîte de dialogue Copy Tapes Between Pools, cochez les cases en regard des bandes à copier ou saisissez les informations permettant de rechercher les bandes à copier, puis sélectionnez **Search** :

Tableau 183 Boîte de dialogue Copy Tapes Between Pools

Champ	Saisie utilisateur
Location	Sélectionnez une librairie ou la **chambre forte** pour localiser la bande. Même si les bandes apparaissent toujours dans un pool (sous le menu Pools), techniquement parlant, elles se trouvent dans une librairie ou dans la chambre forte, mais pas dans les deux, et elles ne se trouvent jamais dans deux librairies simultanément. Utilisez les options d'importation/exportation pour déplacer des bandes entre la chambre forte et une librairie.
Pool	Pour copier des bandes entre des pools, sélectionnez le nom du pool dans lequel les bandes résident actuellement. Si aucun pool n'a été créé, utilisez le pool **par défaut**.
Barcode	Spécifiez un code-barres unique ou conservez la valeur par défaut (*) pour importer un groupe de bandes. Le code-barres autorise les caractères génériques ? et *, où ? remplace n'importe quel caractère unique et * correspond à 0 ou à plusieurs caractères.
Count	Saisissez le nombre maximal de bandes à importer. Si vous laissez ce champ vide, le code-barres par défaut (*) est utilisé.
Tapes Per Page	Sélectionnez le nombre maximal de bandes à afficher par page. Les valeurs possibles sont 15, 30 at 45.
Items Selected	Affiche le nombre de bandes sélectionnées sur plusieurs pages (mis à jour automatiquement pour chaque bande sélectionnée).

3. Dans la liste des résultats de la recherche, sélectionnez les bandes à copier.
4. Dans la liste Select Destination: Pool, sélectionnez le pool dans lequel les bandes doivent être copiées. Si une bande portant un code-barres correspondant se trouve déjà dans le pool de destination, une erreur s'affiche et la copie est abandonnée.
5. Sélectionnez **Next**.

6. Dans la boîte de dialogue Copy Tapes Between Pools, vérifiez les informations résumées et la liste de bandes, puis sélectionnez **Submit**.
7. Dans la fenêtre Copy Tapes Between Pools Status, sélectionnez **Close**.

Modification du nom des pools

Un pool peut être renommé uniquement si aucune de ses bandes n'est dans une bibliothèque

Procédure

1. Sélectionnez **Pools** > **Pools** > ***pool***.
2. Sélectionnez **More Tasks** > **Pool** > **Rename**.
3. Dans la boîte de dialogue Rename Pool, saisissez le nouveau nom du pool, en respectant les restrictions suivantes :
   - ne peut pas être « all, » « vault » ou « summary ».
   - ne doit pas débuter ou se terminer par un espace ou un point ;
   - n'est pas sensible à la casse.
4. Sélectionnez **OK** pour afficher la boîte de dialogue Rename Pool Status.
5. Lorsque la boîte de dialogue Rename Pool Status affiche `Completed`, sélectionnez **OK**.

   Le pool sera renommé dans la sous-arborescence Pools à la fois dans les zones Pools et Virtual Tape Libraries.

CHAPITRE 16

DD Replicator

Ce chapitre traite des sujets suivants :

Présentation de DD Replicator

Data Domain Replicator (DD Replicator) garantit une réplication efficace en réseau, automatisée, basée sur des règles et chiffrée, à des fins de reprise après sinistre et de consolidation de sauvegarde et d'archivage multisite. DD Replicator réplique, de manière asynchrone, seulement des données dédupliquées et compressées sur un WAN (réseau étendu).

DD Replicator effectue deux niveaux de déduplication pour réduire considérablement les besoins en bande passante : la déduplication *locale* et celle *entre plusieurs sites*. La déduplication locale détermine les segments uniques à répliquer via un WAN. La déduplication entre sites réduit les besoins en bande passante lorsque plusieurs sites sont répliqués vers le même système. De plus, tout segment redondant précédemment transféré par tout autre site ou dans le cadre d'une sauvegarde ou d'un archivage en local n'est pas répliqué une nouvelle fois. Le réseau entre les sites est plus efficace et les besoins quotidiens en bande passante réseau peuvent être réduits de 99 %, rendant la réplication réseau rapide, fiable et économique.

Pour répondre aux nombreuses exigences en matière de reprise après sinistre, DD Replicator fournit plusieurs topologies de réplication flexibles, y compris la mise en miroir intégrale du système, ainsi que la réplication bidirectionnelle, un vers plusieurs/plusieurs vers un et en cascade. Vous pouvez également répliquer toutes les données ou seulement un sous-ensemble de données sur le système DD. Pour renforcer la sécurité, DD Replicator peut chiffrer les données en cours de réplication entre les systèmes DD à l'aide du protocole SSL.

DD Replicator bénéficie de performances et de taux de réplication consolidée capables de prendre en charge les grands environnements d'entreprise.

Avant de commencer à utiliser DD Replicator, tenez compte des conditions générales suivantes :

- DD Replicator est un produit sous licence. Pour acheter des licences, contactez votre responsable de compte Data Domain.
- Généralement, vous pouvez uniquement effectuer une réplication entre des machines différentes de deux versions au maximum, par exemple, de la version 5.6 vers la version 6.0. Toutefois, il existe des exceptions à cela (notamment suite à une numérotation atypique de la version). Par conséquent, passez en revue les tableaux de la section *Compatibilité entre les versions en matière de réplication* ou contactez votre responsable de compte Data Domain.
- Si vous ne pouvez pas gérer et surveiller DD Replicator à partir de la version actuelle de DD System Manager, utilisez les commandes `replication` décrites dans le *Guide de référence des commandes de Data Domain Operating System*.

Préalables à la configuration de la réplication

Avant de configurer une réplication, tenez compte des conditions préalables suivantes pour minimiser le temps de transfert initial des données, éviter tout remplacement accidentel des données, etc.

- **Contextes** : déterminez le nombre maximum de contextes qu'il convient de créer pour vos systèmes DD en examinant les nombres de flux de réplication indiqués dans le tableau suivant.

  Tableau 184 Flux de données envoyés à un système Data Domain

Modèle	RAM/NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD140, DD160, DD610	4 Go ou 6 Go/ 0,5 Go	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620, DD630 et DD640	8 Go/0,5 Go ou 1 Go	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640, DD670	16 Go ou 20 Go/ 1 Go	90	30	60	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670, DD860	36 Go/1 Go	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 Go[b] / 1 Go	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 Go/2 Go	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 ou 256 Go[b] / 4 Go	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 Go	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 Go	60	16	30	60	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 ou 64 Go/ 2 Go	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180

Tableau 184 Flux de données envoyés à un système Data Domain (suite)

Modèle	RAM/NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD4200	128 Go[b] / 4 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 Go[b] / 4 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 ou 256 Go[b] / 4 Go	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256/512 Go	1 885	300	540	1 080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 Go	1 885	300	540	1 080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96 Go	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 Go	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8 To	8 Go / 512 Mo	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE (16 To)	16 Go / 512 Mo ou 24 Go / 1 Go	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE (32 To)	24 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE (48 To)	36 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 To	48 Go/1 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90

Tableau 184 Flux de données envoyés à un système Data Domain (suite)

Modèle	RAM/NVRAM	Flux d'écriture de sauvegarde	Flux de lecture de sauvegarde	Flux source de répl.[a]	Flux cibles de répl.[a]	Mixte
DD VE (96 To)	64 Go/2 Go	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 (4 To)	12 Go (mémoire virtuelle) / 512 Mo	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 To	32 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (16 To)	32 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 (32 To)	46 Go (mémoire virtuelle) / 1 536 Go	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. Flux DirRepl, OptDup, MTreeRepl
b. La fonction Data Domain Extended Retention n'est disponible que pour ces périphériques avec une mémoire (maximale) étendue

- **Compatibilité** : si vous utilisez des systèmes DD exécutant différentes versions de DD OS, consultez la section suivante au sujet de la compatibilité entre les versions en matière de réplication.
- **Réplication initiale** : si la source comporte un grand nombre de données, l'opération de réplication initiale peut durer très longtemps. Envisagez de transférer les deux systèmes DD au même emplacement avec une liaison à haut débit et faible latence. Après la première réplication, vous pouvez déplacer les systèmes vers les emplacements voulus, car seules les nouvelles données seront envoyées.
- **Temps de réponse de la bande passante** : cette valeur doit être la même pour la source et la destination. Ces réglages permettent d'optimiser les performances de la réplication sur des liaisons à latence élevée en contrôlant la taille du tampon du protocole TCP. Le système source est ainsi en mesure d'envoyer suffisamment de données vers la destination pendant qu'il attend un accusé de réception.
- **Un seul contexte pour les répertoires/sous-répertoires** : un répertoire (et ses sous-répertoires) ne peut se trouver que dans un seul contexte à la fois ; veillez donc à ce qu'aucun autre contexte de réplication de répertoire n'utilise un sous-répertoire d'un répertoire source.
- **Stockage adéquat** : la destination doit, au minimum, disposer de la *même quantité d'espace* que la source.
- **Destination vide pour la réplication de répertoire** : lors d'une réplication de répertoire, le répertoire cible doit être vide, ou son contenu doit être devenu inutile car il sera remplacé.

- **Sécurité** : DD OS nécessite que le port 3009 soit ouvert pour pouvoir configurer une réplication sécurisée via une connexion Ethernet.

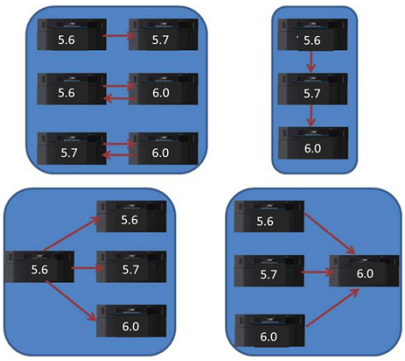
Compatibilité entre les versions en matière de réplication

Pour utiliser des systèmes DD exécutant différentes versions de DD OS pour une source ou une destination, les tableaux suivants indiquent le niveau de compatibilité pour les configurations à nœud unique, DD Extended Retention et DD Retention Lock et les réplications de MTree, de répertoire, de collection, delta (optimisation d'une bande passante faible) et en cascade.

En général :

- Avec DD Boost ou OST, reportez-vous à la section relative à la « compatibilité optimisée entre les versions en matière de réplication » du *Guide d'administration de Data Domain Boost pour l'intégration des partenaires* ou du *Guide d'administration de Data Domain Boost for OpenStorage* pour connaître les configurations prises en charge.
- Il n'est pas possible d'utiliser simultanément la réplication de MTree et de répertoire pour répliquer les mêmes données.
- La procédure de restauration est valide pour toutes les configurations de réplication prises en charge.
- La migration des fichiers est possible chaque fois qu'une réplication de collection est prise en charge.
- La réplication de MTree entre un système DD source exécutant DD OS 5.2.x et un système DD cible exécutant DD OS 5.4.x ou DD OS 5.5.x n'est pas possible si la gouvernance relative au verrouillage de la rétention (DD Retention Lock) est activée sur la structure MTree source.
- Dans le cas d'une réplication de MTree à partir d'un système DD source exécutant DD OS 6.0 vers un système DD cible exécutant une version antérieure de DD OS, le processus de réplication se comporte en fonction de l'ancienne version de DD OS sur le système DD de destination. Si une opération de restauration ou une réplication en cascade est effectuée à partir du système DD de destination, aucune sauvegarde synthétique virtuelle n'est appliquée.
- Dans le cas d'une configuration d'une réplication en cascade, le nombre maximum de tronçons est fixé à deux, soit trois systèmes DD.
  La migration de répertoire vers la structure MTree prend en charge la compatibilité en amont (jusqu'à deux versions précédentes). Reportez-vous à la section Migration de la réplication de répertoire vers la structure MTree à la page 490 pour plus d'informations sur la migration de répertoire vers la structure MTree.
- Les réplications un vers plusieurs, plusieurs vers un et en cascade prennent en charge jusqu'à trois familles de versions DD OS successives, comme le montrent ces figures.

Figure 17 Configurations de réplication valides



Dans ces tableaux :

- Chaque version DD OS contient toutes les versions de cette famille ; DD OS 5.7 inclut, par exemple, 5.7.1, 5.7.x, 6.0, etc.
- c = réplication de collection
- dir = réplication de répertoire
- m = réplication de MTree
- del = réplication delta (optimisation d'une bande passante faible)
- dest = destination
- src = source
- NA = non applicable

Tableau 185 Configuration : nœud unique à nœud unique

src/ dest	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.0 (src)	c, dir, del	dir, del	dir, del	NA	NA	NA	NA	NA	NA	NA	NA
5.1 (src)	dir, del	c, dir, del, m[a]	dir, del, m[a]	dir, del, m[a]	dir, del, m[a]	NA	NA	NA	NA	NA	NA
5.2 (src)	dir, del	dir, del, m[a]	c, dir, del, m[b]	dir, del, m	dir, del, m	dir, del, m	NA	NA	NA	NA	NA
5.3 (src)	NA	dir, del, m[a]	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA	NA	NA	NA
5.4 (src)	NA	dir, del, m[a]	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA	NA	NA
5.5 (src)	NA	NA	dir, del, m	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA	NA
5.6 (src)	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA	NA
5.7 (src)	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m	NA
6.0 (src)	NA	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m	dir, del, m
6.1 (src)	NA	NA	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m	dir, del, m
6.2 (src)	NA	NA	NA	NA	NA	NA	NA	NA	dir, del, m	dir, del, m	c, dir, del, m

a. La réplication de MTree n'est pas compatible avec la DD VTL.
b. La réplication de collection est prise en charge uniquement pour les données de conformité.

Tableau 186 Configuration : DD Extended Retention vers DD Extended Retention

src/ dest	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.0 (src)	c	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.1 (src)	NA	c	m[a]	m[b]	m[b]	NA	NA	NA	NA	NA	NA
5.2 (src)	NA	m[a]	c, m[a]	m[a]	m[a]	m[a]	NA	NA	NA	NA	NA
5.3 (src)	NA	m[c]	m[c]	c, m	m	m	NA	NA	NA		NA
5.4 (src)	NA	m[c]	m[c]	m	c, m	m	m	NA	NA	NA	NA

Tableau 186 Configuration : DD Extended Retention vers DD Extended Retention (suite)

src/ dest	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.5 (src)	NA	NA	m[c]	m	m	c, m	m	m	NA	NA	NA
5.6 (src)	NA	NA	NA	NA	m	m	c, m	m	m		NA
5.7 (src)	NA	NA	NA	NA	NA	m	m	c, m	m	m	NA
6.0 (src)	NA	NA	NA	NA	NA	NA	m	m	c, m	m	m
6.1 (src)	NA	NA	NA	NA	NA	NA	NA	m	m	c, m	m
6.2 (src)	NA	NA	NA	NA	NA	NA	NA	NA	m	m	c, m

a. La migration des fichiers n'est pas prise en charge avec la réplication de MTree sur la source ou la destination dans cette configuration.
b. La migration des fichiers n'est pas prise en charge avec la réplication de MTree sur la source dans cette configuration.
c. La migration des fichiers n'est pas prise en charge avec la réplication de MTree sur la destination dans cette configuration.

Tableau 187 Configuration : nœud unique vers DD Extended Retention

src/ dest	5.0 (dest)	5.1 (dest)	5.2 (dest)	5.3 (dest)	5.4 (dest)	5.5 (dest)	5.6 (dest)	5.7 (dest)	6.0 (dest)	6.1 (dest)	6.2 (dest)
5.0 (src)	dir	dir	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.1 (src)	dir	dir, m[a]	dir, m[a]	dir, m	dir, m	NA	NA	NA	NA	NA	NA
5.2 (src)	dir	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	NA	NA	NA	NA	NA
5.3 (src)	NA	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	NA	NA	NA	NA	NA
5.4 (src)	NA	dir, m[a]	dir, m[a]	dir, m	dir, m	dir, m	dir, m	NA	NA	NA	NA
5.5 (src)	NA	NA	dir, m[a]	dir, m	dir, m	dir, m	dir, m	dir, m	NA	NA	NA
5.6 (src)	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m	dir, m	NA	NA
5.7 (src)	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m	dir, m	NA
6.0 (src)	NA	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m	dir, m
6.1 (src)	NA	NA	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m	dir, m
6.2 (src)	NA	NA	NA	NA	NA	NA	NA	NA	dir, m	dir, m	dir, m

a. La migration des fichiers n’est pas prise en charge dans cette configuration.

Types de réplication

En général, la réplication s'effectue entre un système DD *source*, qui reçoit des données d'un système de sauvegarde, et un ou plusieurs systèmes DD de *destination*. Chaque système DD peut être la source et/ou la destination des contextes de réplication. Les opérations de réplication n'empêchent pas l'exécution de sauvegardes et de restaurations sur chaque système DD.

Chaque type de réplication établit un *contexte* associé à un répertoire ou une structure MTree existant sur la source. Le contexte répliqué est créé sur la destination dès l'instauration d'un contexte. Le contexte génère une paire de réplication toujours active. Toutes les données résidant sur la source sont automatiquement copiées sur la destination dès que la première opportunité se présente. Les chemins définis dans les contextes de réplication sont des références absolues : ils restent les mêmes en fonction du système dans lequel ils sont configurés.

Il est possible de configurer un système Data Domain pour une réplication de répertoire, de collection ou de MTree.

- Dans le cas d'une *réplication de répertoire*, vous répliquez le contenu d’un répertoire donné.

- Dans le cas d'une *réplication de collection*, c'est la totalité du datastore qui est dupliquée sur la source, puis transférée vers la destination. Le volume répliqué est en lecture seule.
- Une *réplication de MTree* permet de répliquer l'intégralité des structures MTree (structures de fichier virtuelles offrant des fonctions de gestion évoluées). Il est possible également de répliquer des pools de médias. Par défaut (à compter de la version DD OS 5.3), la réplication s'applique aux structures MTree créées. (Un pool de médias peut aussi être créé en mode de compatibilité descendante. Après réplication, il deviendra un contexte de réplication de répertoire.)

Quel que soit le type de réplication, les conditions suivantes sont requises :

- Le système Data Domain de destination doit disposer d'un espace de stockage disponible au moins équivalent à la taille maximale attendue du répertoire source. Assurez-vous que la bande passante du réseau et l'espace disque du système Data Domain de destination soient suffisants pour gérer l'ensemble du trafic en provenance des sources de réplication.
- Le système de fichiers doit être activé ou, selon le type de réplication, devra être activé lors de l'initialisation de la réplication.
- La source doit exister.
- La destination ne doit pas exister.
- La destination sera générée après construction et initialisation d'un contexte.
- Après la réinitialisation de la réplication, la propriété et les autorisations de la destination sont identiques à celles de la source.
- Dans les options relatives à la réplication, une paire de réplication spécifique est toujours identifiée par la destination.
- Les deux systèmes doivent disposer d'une route active et visible via le réseau IP, de façon à ce que chaque système soit en mesure de résoudre le nom d'hôte de son partenaire.

Le choix du type de réplication dépend de vos besoins spécifiques. Les sections suivantes traitent de ces trois types de réplication et proposent une brève introduction à la réplication de fichiers gérés utilisée par DD Boost.

Réplication de fichiers gérés

La *réplication de fichiers gérés*, qui est utilisée par DD Boost, est un type de réplication qui est géré et contrôlé par le logiciel de sauvegarde.

La réplication des fichiers gérés transfère des images de sauvegarde directement d’un système DD vers un autre, un par un, à la demande du logiciel de sauvegarde.

Le logiciel de sauvegarde assure le suivi de toutes les copies, ce qui simplifie le contrôle de l’état de la réplication et la restauration depuis plusieurs copies.

Cette réplication propose des topologies de réplication flexibles, notamment la mise en miroir de tout le système, ainsi que des topologies bidirectionnelles, « plusieurs vers un », « un vers plusieurs » et en cascade, ce qui permet une déduplication efficace entre plusieurs sites.

Voici quelques autres points à prendre en compte à propos de la réplication de fichiers gérés :

- Il n’est pas utile de configurer les contextes de réplication.
- Les stratégies de gestion du cycle de vie gèrent la réplication de l’information sans aucune intervention de l’utilisateur.

- DD Boost génère et détruit les contextes nécessaires à la volée.

Pour plus d'informations, reportez-vous au chapitre sur les commandes `ddboost file-replication` dans le *Guide de référence des commandes de Data Domain Operating System*.

Réplication de répertoire

La *réplication de répertoire* permet de transférer des données dédupliquées au sein d'un répertoire du système de fichiers DD configuré comme source de réplication vers un répertoire configuré comme destination de réplication sur un autre système.

Avec la réplication de répertoire, un système DD peut être simultanément la source de certains contextes de réplication et la destination d'autres contextes. Pendant qu'il réplique les données, ce système DD peut également recevoir des données des applications de sauvegarde et d'archivage.

La réplication de répertoire utilise les mêmes topologies de déploiement de réseau flexibles et produit les mêmes effets de déduplication entre sites que la réplication de fichiers gérés (le type utilisé par DD Boost).

Voici quelques points supplémentaires à prendre en compte lors de l'utilisation de la réplication de répertoire :

- Ne mélangez pas les données CIFS et NFS dans le même répertoire. Un même système DD de destination peut recevoir des sauvegardes de clients CIFS et NFS, à condition que des répertoires distincts soient utilisés pour chaque type de client.
- Un répertoire ne peut se trouver que dans un seul contexte à la fois. Il n'est pas possible d'utiliser un répertoire parent dans un contexte de réplication si un répertoire enfant de ce répertoire parent est déjà en cours de réplication.
- Il n'est *pas* permis de renommer (déplacer) des fichiers ou des bandes *dans, ou hors* d'un répertoire source de réplication de répertoire. Il *est* permis de renommer des fichiers ou des bandes *au sein* d'un répertoire source de réplication de répertoire.
- Un système DD de destination doit disposer d'un espace de stockage disponible au moins équivalent à la capacité après compression de la taille maximale attendue du répertoire source après compression.
- Lors de l'initialisation de la réplication, un répertoire de destination est automatiquement créé.
- Ce répertoire se voit associer les mêmes attributs que le répertoire source en ce qui concerne les autorisations et la propriété. Tant que le contexte existe, le répertoire de destination est conservé dans un mode de lecture seule et il peut recevoir des données uniquement à partir du répertoire source.
- À tout moment, en raison de différences au niveau de la compression globale, les répertoires source et de destination peuvent présenter une taille différente.

Recommandations à propos de la création de répertoires

La réplication de répertoire réplique les données au niveau des sous-répertoires individuels sous `/data/col1/backup`.

Pour garantir une séparation granulaire des données, vous devez créer, sur le système hôte, d'autres répertoires (DirA, DirB, etc.) au sein de la structure MTree /backup, en basant chaque répertoire sur votre environnement et en veillant à répliquer ces répertoires vers un autre emplacement. L'objectif ici n'est pas de répliquer la totalité de la structure MTree /backup, mais de configurer des contextes de réplication sur chaque sous-répertoire sous /data/col1/backup/ (ex. /data/col1/backup/DirC). Cette stratégie présente plusieurs intérêts :

- Elle permet de contrôler les emplacements de destination, car DirA peut être situé sur un site et DirB sur un autre.
- Ce niveau de granularité offre des avantages en termes de gestion, de surveillance et de localisation des pannes. Il est possible d'interrompre, d'arrêter ou de détruire chaque contexte de réplication ou d'en assurer le suivi.
- Les performances se limitent à un seul contexte. La création de plusieurs contextes peut améliorer les performances de la réplication d'agrégation.
- En règle générale, il faut prévoir 5 à 10 contextes pour séparer la charge de réplication en plusieurs flux de réplication. Il ne faut pas oublier, cependant, de tenir compte de la conception du site et du volume et de la composition des données à l'emplacement choisi.

Remarque

Le nombre de contextes à créer est tributaire de la conception. Dans certains cas, la façon dont vous séparez les données à des fins d'optimisation de la réplication peut avoir des répercussions importantes. En matière d'optimisation, l'emplacement final compte plus que la méthode suivie pour répliquer les données. Il est important de garder cela à l'esprit si jamais vous décidez de modifier l'environnement de sauvegarde.

Réplication de structures MTree

La *réplication de MTree* permet de répliquer des structures MTree entre des systèmes DD. Des snapshots sont créés périodiquement sur le système source et les différences constatées entre eux sont transmises à la destination en exploitant le même mécanisme de déduplication entre plusieurs sites que celui utilisé pour la réplication de répertoire. Cela garantit que les données sur le système cible sont toujours une copie ponctuelle de la source et cela assure la cohérence des fichiers. Cela réduit également la réplication des pertes dans les données, avec à la clé une utilisation plus efficace du WAN.

Alors que la réplication d'annuaire doit répliquer chaque modification du contenu du répertoire source dans l'ordre, l'utilisation de snapshots avec la réplication de structures MTree permet d'ignorer certaines modifications intermédiaires à la source. Le fait d'ignorer ces modifications réduit davantage la quantité de données envoyées sur le réseau et, par conséquent, le délai de réplication.

Avec la réplication de MTree, un système DD peut être à la fois la source de certains contextes de réplication et la destination d'autres contextes. Pendant qu'il réplique les données, ce système DD peut également recevoir des données des applications de sauvegarde et d'archivage.

Les effets d'une réplication de Mtree sur les topologies de déploiement de réseau flexible et sur la déduplication entre sites sont les mêmes que ceux de la réplication de fichier géré (le type utilisé par DD Boost).

Voici quelques autres points à prendre en compte lors de l'utilisation de la réplication de Mtree :

- Lors de l'initialisation de la réplication, une Mtree cible en lecture seule est automatiquement créée.
- Les données peuvent être réparties de façon logique en plusieurs structures MTree pour optimiser les performances lors de la réplication.
- Il convient de créer des snapshots au niveau des contextes source.
- Vous ne pouvez pas créer de snapshots sur une destination de réplication.

- La période de rétention des snapshots répliqués est fixée à un an ; elle peut cependant être ajustée sur la destination.
- Les contextes de réplication doivent être configurés à la fois sur la source et la destination.
- La réplication des cartouches de bande DD VTL (ou pools) s'applique aux structures MTree ou aux répertoires contenant des cartouches de bande DD VTL. Les pools de médias sont répliqués par défaut lors de la réplication de MTree. Un pool de médias peut être créé en mode de compatibilité descendante, puis dupliqué au moyen d'une réplication de répertoire. Vous ne pouvez pas utiliser la syntaxe pool:// syntax pour créer des contextes de réplication via la ligne de commande. Lorsque vous choisissez une réplication de pool dans DD System Manager, une réplication de répertoire ou de MTree a lieu, selon le type de pool de médias.
- La réplication de répertoires sous une Mtree n'est pas autorisée.
- Un système DD cible doit disposer d'un espace de stockage disponible au moins équivalent à la capacité après compression de la taille maximale attendue de la MTree source après compression.
- Cette MTree se voit attribuer les mêmes attributs que la MTree source en ce qui concerne les autorisations et la propriété. Si un contexte est configuré, la Mtree cible est conservée en mode lecture seule et peut uniquement recevoir des données de la Mtree source.
- À tout moment, en raison de différences au niveau de la compression globale, les MTrees sources et cibles peuvent présenter une taille différente.
- La réplication de Mtree d'un système avec DD Extended Retention vers un système sans DD Extended Retention est prise en charge si tous deux exécutent DD OS 5.5 ou une version ultérieure.
- La conformité DD Retention Lock est prise en charge par défaut avec la réplication de MTree. Si la fonction DD Retention Lock est concédée sous licence sur une source, la destination doit également disposer d'une licence DD Retention Lock. Dans le cas contraire, la réplication échouera. (Pour éviter ce type de situation, vous devez désactiver la fonction DD Retention Lock.) Si la fonction DD Retention Lock est activée sur un contexte de réplication, un contexte de réplication répliqué contiendra systématiquement les données dont la rétention est verrouillée.

Détails de la réplication de structures MTree

La réplication de structures MTree comporte les étapes suivantes :

1. Un snapshot est créé sur le contexte de réplication source.
2. Ce snapshot est comparé au dernier snapshot précédent.
3. Toute différence entre les deux snapshots est envoyée au contexte de réplication de destination.
4. Sur la destination, la structure MTree est mise à jour, mais aucun fichier n'est exposé à l'utilisateur tant que toutes les modifications n'ont pas été reçues par le système de destination.

Ces étapes sont répétées chaque fois qu'un snapshot est créé sur la structure MTree source. Les situations suivantes déclenchent la création d'un snapshot sur le système source :

- Snapshot périodique généré par le système : lorsque le délai de réplication est supérieur à 15 minutes et qu'aucun instantané n'est en cours de réplication.
- snapshot créé par l'utilisateur : à une heure spécifiée par l'utilisateur, par exemple après l'achèvement d'une procédure de sauvegarde.

Pour des exemples montrant l'interaction de différents types de snapshots, reportez-vous l'article de KB *Fonctionnement de la réplication de structures MTree*, disponible à l'adresse https://support.emc.com/kb/180832.

Après la réplication du snapshot, la connexion à la destination est fermée. Une nouvelle connexion entre la source et la destination est établie lors de la réplication du snapshot suivant.

AMS (Automatic Multi-Streaming)
AMS améliore les performances de réplication des structures MTree. Il utilise plusieurs flux pour répliquer un seul gros fichier (32 Go ou plus) afin d'améliorer l'utilisation de la bande passante du réseau pendant la réplication. En augmentant la vitesse de réplication des fichiers individuels, AMS améliore également l'efficacité du pipeline de la file d'attente de réplication et permet d'améliorer le débit de réplication et de réduire le délai de réplication.

Lorsque la charge applicative présente plusieurs choix d'optimisation, AMS sélectionne automatiquement la meilleure option pour la charge applicative. Par exemple, si la charge applicative est un gros fichier avec des attributs fastcopy, l'opération de réplication utilise l'optimisation fastcopy pour éviter le temps système d'analyse du fichier afin d'identifier les segments uniques entre les paires de réplication. Si la charge applicative utilise des données synthétiques, la réplication utilise la réplication synthétique en plus de l'AMS pour tirer parti des opérations locales sur le système de destination pour chaque flux de réplication afin de générer le fichier.

AMS est toujours activé et ne peut pas être désactivé.

Réplication de collection

La *réplication de collection* permet de mettre en miroir la totalité du système dans une topologie de type un vers un. Le transfert des modifications apportées à la collection sous-jacente, y compris tous les répertoires et fichiers logiques du système de fichiers DD, s'effectue en continu.

Si la réplication de collection n'offre pas autant de flexibilité que d'autres types de réplication, elle peut en revanche assurer un débit plus important et prend en charge davantage d'objets avec moins de frais, ce qui peut s'avérer plus intéressant pour les cas métiers de grande envergure.

La réplication de collection réplique l'intégralité de la zone `/data/col1` d'un système DD source vers un système DD de destination.

Remarque

La réplication de collection n'est pas prise en charge sur les systèmes offrant une hiérarchisation Cloud.

Voici quelques autres points à prendre en compte lors de l'utilisation de la réplication de collection :

- Aucun contrôle de réplication granulaire n'est possible. Toutes les données sont copiées de la source à la destination pour produire une copie en lecture seule.
- La réplication de collection exige que la capacité de stockage du système de destination soit supérieure ou égale à la capacité du système source. Si la capacité de la destination est inférieure à celle de la source, la capacité disponible sur la source est réduite à celle de la destination.
- Avant la configuration de la réplication, le système DD devant être utilisé en tant que destination de la réplication de collection doit être vide. Une fois que la

réplication est configurée, ce système est dédié à la réception des données du système source.

- Avec la réplication de collection, tous les comptes et mots de passe utilisateur sont répliqués de la source vers la destination. Toutefois, à compter de DD OS 5.5.1.0, d'autres éléments de configuration et paramètres utilisateur du système DD ne sont pas répliqués sur la destination ; vous devez explicitement les reconfigurer après la restauration.
- La réplication de collection est prise en charge avec DD Secure Multitenancy (SMT). Les informations SMT de base, contenues dans l'espace de nommage du registre, y compris les définitions des tenants et des unités de tenant avec les UUID correspondants, sont automatiquement transférées pendant l'opération de réplication. Toutefois, les informations SMT suivantes ne sont pas automatiquement incluses pour la réplication et doivent être configurées manuellement sur le système de destination :
  - Listes de notifications d'alerte pour chaque unité de tenant
  - Tous les utilisateurs alloués au protocole DD Boost pour être utilisés par des tenants SMT, si DD Boost est configuré sur le système
  - L'unité de tenant par défaut associée à chaque utilisateur DD Boost, le cas échéant, si DD Boost est configuré sur le système

  La section Utilisation de la réplication de la collection pour la reprise après sinistre avec SMT à la page 495 décrit comment configurer manuellement ces éléments sur la destination de réplication.
- DD Retention Lock Compliance prend en charge la réplication de collection.
- La réplication de collection n'est pas prise en charge sur les systèmes offrant une hiérarchisation Cloud.
- Avec la réplication de collection, les données dans un contexte de réplication sur le système source qui n'a pas été répliqué ne peuvent pas être traitées pour le nettoyage du système de fichiers. Si le nettoyage du système de fichiers ne peut pas se terminer car les systèmes sources et cibles ne sont pas synchronisés, le système signale l'état de l'opération de nettoyage comme étant `partiel`, et seules des statistiques limitées sont disponibles pour l'opération de nettoyage. Si la réplication de collection est désactivée, la quantité de données qui ne peuvent pas être traitées pour le nettoyage du système de fichiers augmente car la source de réplication et les systèmes cibles restent désynchronisés. L'article de la base de connaissances : *Data Domain : Un tour d'horizon des phases de nettoyage et de collecte de garbage (GC) de Data Domain File System (DDFS)*, disponible sur le site de support en ligne à l'adresse https://support.emc.com fournit des informations supplémentaires.
- Pour améliorer le débit dans un environnement à bande passante élevée, exécutez la commande suivante **`replication modify <destination> crepl-gc-gw-optim`** pour désactiver l'optimisation de la bande passante de réplication de la collection.

Utilisation de DD Encryption avec DD Replicator

DD Replicator peut être utilisé avec la fonctionnalité facultative *DD Encryption*, ce qui permet aux données chiffrées d'être répliquées à l'aide de la réplication de collection, de répertoire ou de MTree.

Les contextes de réplication sont toujours authentifiés par *code secret partagé*. Ce code secret partagé permet de créer une clé de session à l'aide d'un protocole

d'échange de clés Diffie-Hellman. Cette clé de session est utilisée pour chiffrer et déchiffrer la clé de chiffrement du système Data Domain lorsque cela est nécessaire.

Chaque type de réplication fonctionne uniquement avec le chiffrement et offre le même niveau de sécurité.

- La *réplication de collection* nécessite que la source et la destination aient la même configuration de chiffrement car les données de destination doivent être une réplique exacte des données source. En particulier, la fonctionnalité de chiffrement doit être activée ou désactivée pour la source et la destination et, si cette fonctionnalité est activée, l'algorithme de chiffrement et les phrases de passe du système doivent également correspondre. Les paramètres sont vérifiés lors de la phase d'association de réplication.
  Au cours de la réplication de collection, la source transmet les données sous forme chiffrée et communique également les clés de chiffrement à la destination. Les données peuvent être restaurées à la destination car la destination utilise la même phrase de passe et la même clé de chiffrement du système.

  Remarque

  La réplication de collection n'est pas prise en charge sur les systèmes offrant une hiérarchisation Cloud.

- La *réplication de Mtree ou de répertoire* n'a pas besoin que la configuration du chiffrement soit identique sur la source et sur la destination. À la place, la source et la destination échangent en toute sécurité la clé de chiffrement de la destination lors de la phase d'association de réplication. Les données sont chiffrées à nouveau à la source à l'aide de la clé de chiffrement de la destination avant leur transmission vers la destination.
  Si la destination utilise une configuration de chiffrement différente, les données transmises sont préparées comme il convient. Par exemple, si la fonctionnalité est désactivée sur la destination, la source déchiffre les données et les envoie non chiffrées à la destination.
- Dans une topologie de *réplication en cascade*, un réplica s'effectue en chaîne entre trois systèmes Data Domain. Le dernier système de la chaîne peut être configuré en tant que collection, MTree ou répertoire. Si le dernier système est une destination de réplication de collection, il utilise les mêmes clés de chiffrement et données chiffrées que sa source. Si le dernier système est une destination de réplication de MTree ou de répertoire, il utilise sa propre clé et les données sont chiffrées à sa source. La clé de chiffrement pour la destination à chaque liaison est utilisée pour le chiffrement. Le chiffrement des systèmes dans la chaîne fonctionne comme dans une paire de réplication.

Topologies de réplication

DD Replicator prend en charge cinq topologies de réplication (un vers un, un vers un bidirectionnelle, un vers plusieurs, plusieurs vers un, en cascade). Les tableaux ci-après montrent (1) comment ces topologies fonctionnent avec trois types de réplication (MTree, répertoire et collection) et deux types de système DD [à nœud unique (SN) et DD Extended Retention (ER)] et (2) comment des topologies mixtes sont prises en charge lors d'une réplication en cascade.

En général :

- Les systèmes à nœud unique (SN) prennent en charge toutes les topologies de réplication.
- La topologie nœud unique à nœud unique (SN -> SN) peut être appliquée à tous les types de réplication.

- Les systèmes DD Extended Retention ne peuvent pas faire office de source pour la réplication de répertoire.
- La réplication de collection ne peut pas être configurée d'un système à nœud unique (SN) vers un système DD Extended Retention (ER), et vice versa.
- La réplication de collection ne peut pas être configurée à partir d'un système SN vers un système DD haute disponibilité, ni à partir d'un système DD haute disponibilité vers un système SN.
- Pour la réplication de répertoires et de structures MTree, les systèmes haute disponibilité DD sont traités comme des systèmes SN.
- La réplication de collection ne peut pas être configurée si le niveau de stockage Cloud est activé sur les deux systèmes (ou sur l'un des deux).

Dans ce tableau :

- SN = système DD à nœud unique (sans l'option DD Extended Retention)
- ER = Système DD Extended Retention

Tableau 188 Topologies compatibles par type de réplication et type de système DD

Topologies	Réplication de structure MTree	Réplication de répertoire	Réplication de collection
un vers un	{SN | ER} -> {SN | ER} ER->SN [prise en charge à compter de la version 5.5 ; avant la version 5.5, seule la restauration est possible]	SN -> SN SN -> ER	SN -> SN ER -> ER
un vers un (bidirectionnelle)	{SN | ER} -> {SN | ER}	SN -> SN	non pris en charge
un vers plusieurs	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	non pris en charge
plusieurs vers un	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	non pris en charge
en cascade	{SN | ER } -> {SN | ER} -> {SN | ER}	SN -> SN -> SN SN -> SN -> ER	ER -> ER -> ER SN -> SN -> SN

La réplication en cascade accepte les topologies mixtes à condition que le deuxième tronçon d'une connexion en cascade soit différent du premier (par exemple, A -> B correspond à une réplication de répertoire, et B -> C à une réplication de collection).

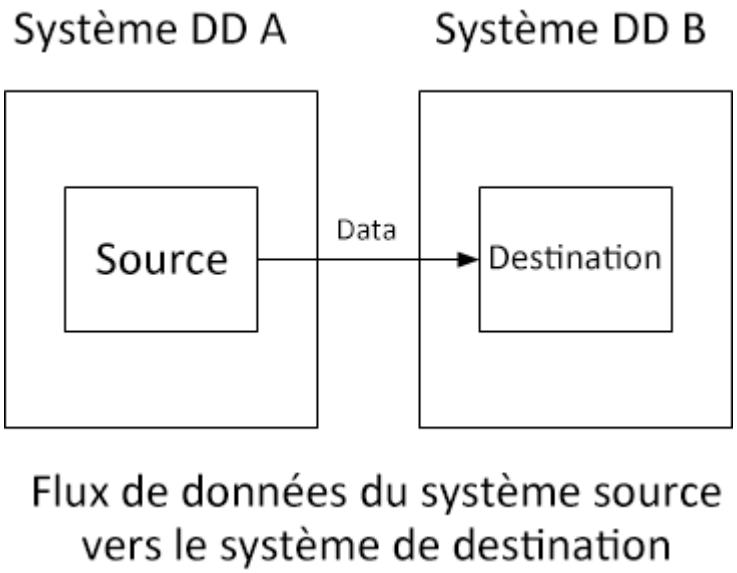
Tableau 189 Topologies mixtes prises en charge lors d'une réplication en cascade

Topologies mixtes	
SN – Répli rép -> ER – Répli MTree -> ER – Répli MTree	SN – Répli rép -> ER – Répli collection -> ER – Répli collection
SN – Répli MTree -> SN – Répli collection -> SN – Répli collection	SN – Répli MTree -> ER – Répli collection -> ER – Répli collection

Réplication un vers un

Le type de réplication le plus simple est celui s'effectuant d'un système DD source vers un système DD de destination, que l'on appelle paire de réplication *un vers un*. Cette topologie de réplication peut être configurée pour les réplications de répertoire, de MTree ou de collection.

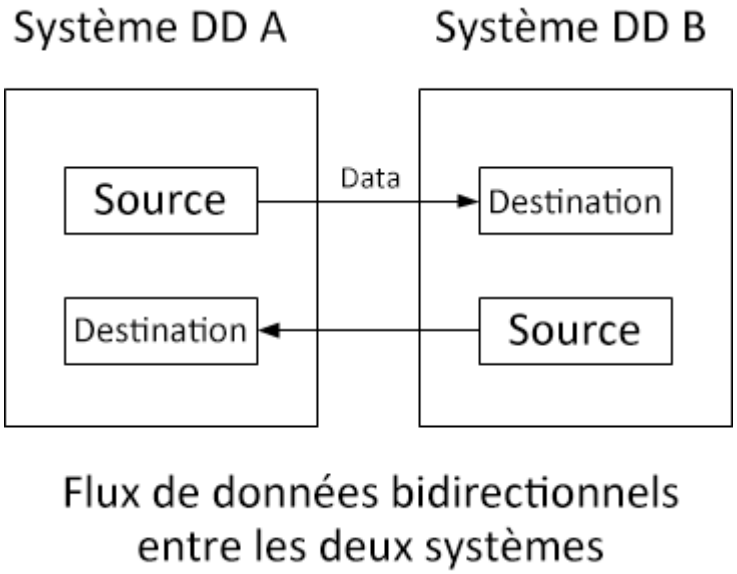
Figure 18 Paire de réplication un vers un



Réplication bidirectionnelle

Dans une paire de réplication bidirectionnelle, les données d'un répertoire ou d'une structure MTree du système DD A sont répliquées vers le système DD B, et d'un autre répertoire ou MTree du système DD B vers le système DD A.

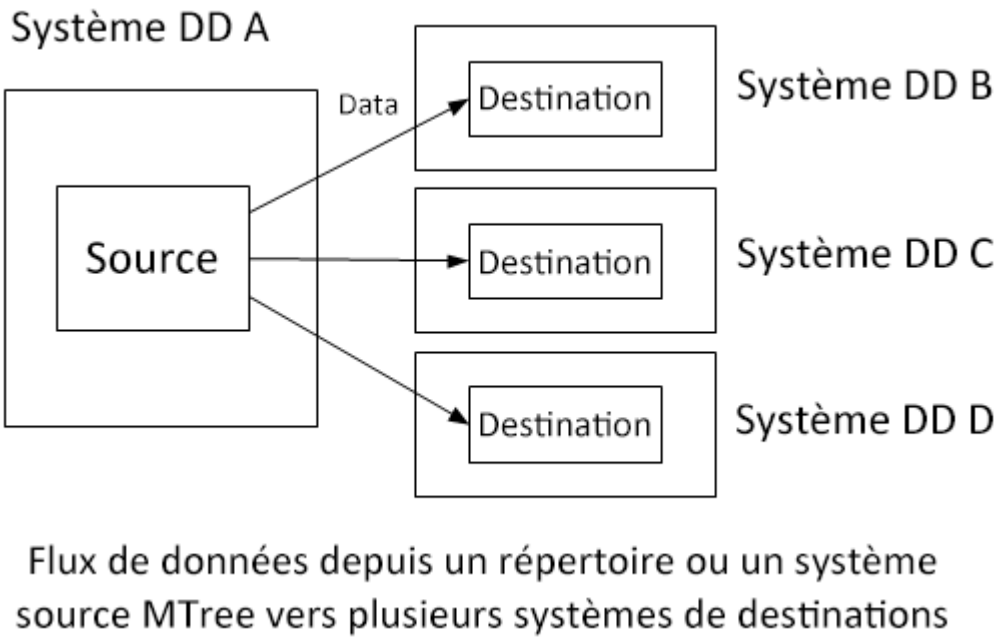
Figure 19 Réplication bidirectionnelle



Réplication un vers plusieurs

Dans une réplication un vers plusieurs, les données transitent d'un répertoire ou d'une MTree source d'un système DD vers plusieurs systèmes DD de destination. Ce type de réplication vous permet de créer plusieurs copies pour améliorer la protection des données ou pour distribuer les données en vue d'une utilisation multisite.

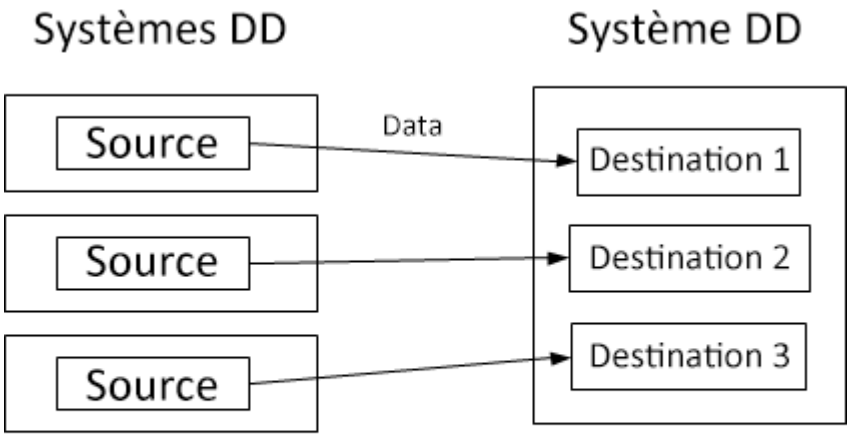
Figure 20 Réplication un vers plusieurs



Réplication plusieurs vers un

Dans une réplication de type plusieurs vers un, que ce soit pour une MTree ou pour un répertoire, les données de réplication de plusieurs systèmes DD source transitent vers un unique système DD de destination. Ce type de réplication permet de protéger la restauration des données de plusieurs filiales sur un seul système informatique au siège social d'une entreprise.

Figure 21 Réplication plusieurs vers un



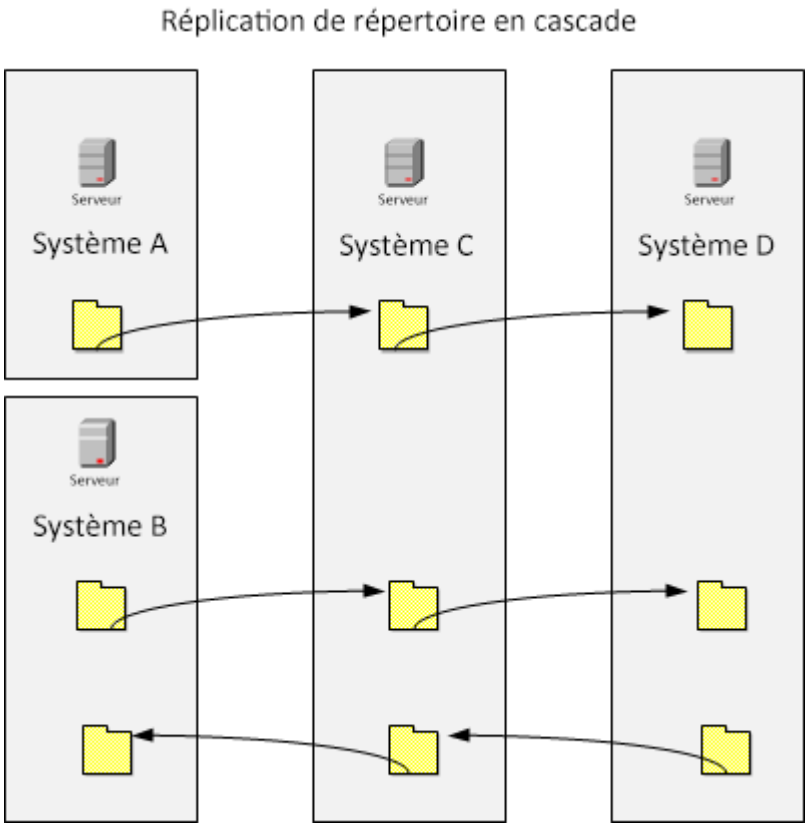
Flux de données de plusieurs systèmes sources vers un système de destination

Réplication en cascade

Dans une topologie de réplication en cascade, la réplication d'un répertoire ou d'une MTree source s'effectue en chaîne sur trois systèmes DD. Le dernier hop dans la chaîne peut être configuré en tant que réplication de collection, de Mtree ou de répertoire, selon que la source est un répertoire ou une Mtree.

Par exemple, le système A DD réplique une ou plusieurs MTrees vers le système B DD, lequel peut ensuite répliquer ces MTrees sur le système C DD. Les MTrees du système B DD sont à la fois une destination (à partir du système A DD) et une source (vers le système C DD).

Figure 22 Réplication de répertoire en cascade



La restauration des données peut être effectuée à partir du contexte de la paire de réplication non dégradée. Exemple :

- Si le système A DD nécessite une restauration, les données peuvent être restaurées à partir du système B DD.
- Si le système B DD nécessite une restauration, la méthode la plus simple consiste à effectuer une resynchronisation de réplication du système A DD (le remplacement) vers le système B DD. Dans ce cas, le contexte de réplication du système B DD vers le système C DD doit être le premier à être arrêté. Une fois la resynchronisation du contexte de réplication du système A DD vers le système B DD terminée, un nouveau contexte du système B DD vers le système C DD doit être configuré et resynchronisé.

Gestion de la réplication

Vous pouvez gérer la réplication à l'aide de Data Domain System Manager (DD System Manager) ou de l'interface de ligne de commande (CLI) du système Data Domain (DD OS).

Connectez-vous à DD System Manager pour utiliser une interface utilisateur en vue de gérer la réplication.

Procédure

1. Dans le menu à gauche de DD System Manager, sélectionnez **Replication**. Si votre licence n'a pas encore été ajoutée, sélectionnez **Add License**.
2. Sélectionnez **Automatic** ou **On-demand** (vous devez disposer d'une licence DD Boost pour la demande).

Équivalent de l'interface de ligne de commande (CLI)

Vous pouvez également vous connecter à partir de la CLI.

```
login as: sysadmin
Data Domain OS 6.0.x.x-12345
Using keyboard-interactive authentication.
Password:
```

État de la réplication

L'*état de la réplication* indique le nombre de contextes de réplication de l'ensemble du système qui présentent un état d'avertissement (texte en jaune) ou d'erreur (texte en rouge), ou si les conditions sont normales.

Vue Summary

La vue Summary recense les contextes de réplication configurés pour un système DD, et présente des informations agrégées au sujet du système DD sélectionné, c'est-à-dire un résumé des paires de réplications entrantes et sortantes. L'accent est mis sur le système DD lui-même, ainsi que sur ses entrées et sorties.

Le tableau Summary peut être filtré en saisissant un nom de source ou de destination, ou en sélectionnant un état (Error, Warning ou Normal).

Tableau 190 Récapitulatif de la réplication

Élément	Description
Source	Nom du système et du chemin du contexte source, au format *système.chemin*. Par exemple, pour le répertoire `dir1` sur`system dd120-22`, vous devriez voir `dd120-22.chaos.local/data/col1/dir1`.
Destination	Nom du système et du chemin du contexte de destination, au format *système.chemin*. Par exemple, pour la structure MTree `MTree1` sur `system dd120-44`, vous devriez voir `dd120-44.chaos.local/data/col1/MTree1`.
Type	Type de contexte : Mtree, répertoire ou pool.
State	États possibles de la paire de réplication : • Normal : si le réplica est en cours d'initialisation, de réplication, de restauration, de resynchronisation ou de migration. • Idle : pour la réplication Mtree, cet état peut indiquer si le processus de réplication n'est pas actuellement actif ou signaler les erreurs réseau (par exemple, si le système cible est inaccessible). • Warning : s'il y a un délai inhabituel pour les cinq premiers états, ou si l'état est de type Uninitialized. • Error : signale toutes les erreurs possibles, par exemple une erreur de type Disconnected.
Synced As Of Time	Horodatage de la dernière opération de synchronisation automatique de réplication exécutée par la source. Pour une réplication de MTree, cette valeur est mise à jour lorsqu'un snapshot est exposé sur la destination. Pour la réplication de

Tableau 190 Récapitulatif de la réplication (suite)

Élément	Description
	répertoire, elle est mise à jour lorsqu'un point de synchronisation inséré par la source est appliqué. Une valeur inconnue s'affiche lors de l'initialisation de la réplication.
Pre-Comp Remaining	Quantité de données précompressées restant à répliquer.
Completion Time (Est.)	Sa valeur est soit `Completed`, soit la quantité de temps jugée nécessaire pour effectuer le transfert des données de réplication en fonction de la vitesse de transfert des dernières 24 heures.

Informations détaillées sur un contexte de réplication

La sélection d'un contexte de réplication dans la vue Summary a pour effet de compléter les informations de ce contexte dans les zones Detailed Information, Performance Graph, Completion Stats et Completion Predictor.

Tableau 191 Informations détaillées

Élément	Description
State Description	Message sur l'état du réplica.
Source	Nom du système et du chemin d'accès du contexte source, au format `system.path`. Voici, par exemple, ce qui est affiché pour le répertoire `dir1` sur le système `dd120-22` : `dd120-22.chaos.local/data/col1/dir1`.
Destination	Nom du système et du chemin d'accès du contexte de destination, au format `system.path`. Voici, par exemple, ce qui est affiché pour la structure MTree `MTree1` sur le système `dd120-44` : `dd120-44.chaos.local/data/col1/MTree1`.
Connection Port	Nom du système et du port d'écoute utilisé pour la connexion de réplication.

Tableau 192 Graphique des performances

Élément	Description
Pre-Comp Remaining	Données précompressées restant à répliquer.
Pre-Comp Written	Données précompressées écrites sur la source.
Post-Comp Replicated	Données après compression qui ont été répliquées.

Tableau 193 Statistiques d'achèvement

Élément	Description
Synced As Of Time	Horodatage de la dernière opération de synchronisation automatique de réplication exécutée par la source. Pour une réplication de MTree, cette valeur est mise à jour lorsqu'un snapshot est exposé sur la destination. Pour la réplication de

Tableau 193 Statistiques d'achèvement (suite)

Élément	Description
	répertoire, elle est mise à jour lorsqu'un point de synchronisation inséré par la source est appliqué. Une valeur inconnue s'affiche lors de l'initialisation de la réplication.
Completion Time (Est.)	Sa valeur est soit `Completed`, soit la quantité de temps jugée nécessaire pour effectuer le transfert des données de réplication en fonction de la vitesse de transfert des dernières 24 heures.
Pre-Comp Remaining	Quantité de données restant à répliquer.
Files Remaining	(Réplication de répertoire uniquement) Nombre de fichiers qui n'ont pas encore été répliqués.
État	Pour les points d'accès source et de destination, affiche l'état (Enabled, Disabled, Not Licensed, etc.) des principaux composants sur le système, notamment : • Réplication • Système de fichiers • DD Retention Lock • DD Encryption at Rest • DD Encryption over Wire • Espace disponible • Low Bandwidth Optimization • Compression Ratio • Low Bandwidth Optimization Ratio

Completion Predictor
Completion Predictor est un widget destiné à effectuer le suivi de l'avancement d'une procédure de sauvegarde et à prévoir quand la réplication s'achèvera pour un contexte sélectionné.

Création d'une paire de réplication

Avant de créer une paire de réplication, assurez-vous que la destination n'*existe* pas, car cela aurait pour effet de générer une erreur.

Procédure

1. Sélectionnez **Replication** > **Automatic** > **Summary** > **Create Pair** .
2. Dans la boîte de dialogue Create Pair, ajoutez des informations pour créer une paire de réplication entrante ou sortante de MTree, de répertoire, de collection ou de pool, comme indiqué dans les sections suivantes.

Ajout d'un système DD pour la réplication

Vous devrez peut-être ajouter un système DD en tant qu'hôte ou destination avant de créer une paire de réplication.

Remarque

Assurez-vous que le système en cours d'ajout exécute une version compatible de DD OS.

Procédure

1. Dans la boîte de dialogue Create Pair, sélectionnez Add System.
2. Pour le système, saisissez le nom d'hôte ou l'adresse IP du système à ajouter.
3. Dans le champ User Name et Password, saisissez le nom d'utilisateur et le mot de passe de l'administrateur du système.
4. Éventuellement, sélectionnez **More Options** pour saisir l'adresse IP proxy (ou le nom du système) d'un système qui n'est pas accessible directement. S'il est configuré, saisissez un port personnalisé à la place du port par défaut 3009.

   Remarque

   Les adresses IPv6 sont uniquement prises en charge lorsque vous ajoutez un système DD OS 5.5 ou version supérieure à un système de gestion utilisant DD OS 5.5 ou version supérieure.

5. Sélectionnez **OK**.

   Remarque

   Si le système est injoignable après son ajout dans DD System Manager, assurez-vous qu'il existe une route) partir du système de gestion vers le système en question. Si un nom d'hôte (nom de domaine complet, c'est-à-dire FQDN, ou non FQDN) est saisi, assurez-vous qu'il peut être résolu sur le système géré. Configurez un nom de domaine pour le système géré et assurez-vous qu'il existe une entrée DNS pour le système ou qu'une adresse IP est définie vers le mappage de nom d'hôte.

6. Si le certificat du système n'a pas été validé, la boîte de dialogue Verify Certificate affiche des détails sur le certificat. Vérifiez les informations d'identification du système. Sélectionnez **OK** si vous faites confiance au certificat ou **Cancel**.

Création d'une paire de réplication de collection

Pour obtenir des informations générales sur ce type de réplication, reportez-vous à la section *Réplication de collection*.

Avant de créer une paire de réplication de collection, assurez-vous que :

- La capacité de stockage du système de destination est supérieure ou égale à celle du système source. (Si la capacité de la destination est inférieure à celle de la source, la capacité disponible sur la source se limite à celle de la destination.)
- La destination a été détruite, puis recréée, mais pas activée.
- Chaque destination et chaque source ne se trouve que dans un seul contexte à la fois.
- Le système de fichiers est désactivé sur le réplica, lors de la configuration et de l'activation du chiffrement sur la source.
- Le système de fichiers est désactivé sur la source, lors de la configuration et de l'activation du chiffrement sur le réplica.

Procédure

1. Dans la boîte de dialogue Create Pair, sélectionnez **Collection** dans le menu **Replication Type**.
2. Sélectionnez le nom d'hôte du système source dans le menu **Source System**.
3. Sélectionnez le nom d'hôte du système de destination dans le menu **Destination System**. La liste inclut uniquement les hôtes de la liste DD-Network.
4. Si vous souhaitez modifier des paramètres de connexion à l'hôte, sélectionnez l'onglet **Advanced**.
5. Sélectionnez **OK**. La réplication de la source vers la destination commence.

Résultats

Les résultats du test provenant de Data Domain ont renvoyé les recommandations suivantes relatives aux performances pour l'initialisation de la réplication. Il s'agit *uniquement* de recommandations et les performances réelles observées dans les environnements de production peuvent varier.

- Sur un LAN Gibioctet : Avec un nombre d'étagères suffisant pour assurer une entrée/sortie maximale et des conditions idéales, la réplication de collection peut saturer une liaison de 1 GigE (temps de protocole de module 10 %), ainsi que 400-900 Mo/s sur 10 GigE, selon la plate-forme.
- Sur un WAN, les performances sont régies par la vitesse de la ligne de liaison, la bande passante, la latence et le taux de perte de paquets du WAN.

Création d’une paire de réplication de MTree, de répertoire ou de pool

Pour obtenir des informations générales sur ces types de réplication, reportez-vous aux sections *Réplication de MTree* et *Réplication de répertoire*.

Lors de la création d’une paire de réplication de MTree, de répertoire ou de pool :

- Assurez-vous que la réplication transite par l’interface appropriée. Lors de la définition d’un contexte de réplication, les recherches directes et inversées doivent permettre de résoudre les noms d’hôte de la source et de la destination. Pour que les données transitent par des interfaces du système autres que l’interface de résolution par défaut, il convient de modifier le contexte de réplication après sa création. Il peut être nécessaire de configurer les fichiers d’hôte pour s’assurer que les contextes sont définis via des interfaces sans fonction de résolution (cross-over).
- Vous pouvez « inverser » le contexte d’une réplication de MTree, c’est-à-dire que vous pouvez intervertir la destination et la source.
- Les sous-répertoires au sein d’une MTree ne peuvent pas être répliqués car la MTree, dans son intégralité, est répliquée.
- La réplication de Mtree d’un système avec DD Extended Retention vers un système sans DD Extended Retention est prise en charge si tous deux exécutent DD OS 5.5 ou une version ultérieure.
- Le système DD de destination doit disposer d’un espace de stockage disponible au moins équivalent à la taille après compression de la taille maximale attendue du répertoire source ou de la structure MTree après compression.
- Lors de l’initialisation de la réplication, un répertoire de destination est automatiquement créé.

- Un système DD peut être à la fois la source d'un contexte et la destination d'un autre contexte.

Procédure

1. Dans la boîte de dialogue Create Pair, sélectionnez **Directory**, **MTree** (valeur par défaut) ou **Pool** dans le menu **Replication Type**.
2. Sélectionnez le nom d'hôte du système source dans le menu **Source System**.
3. Sélectionnez le nom d'hôte du système de destination dans le menu **Destination System**.
4. Indiquez le chemin de la source dans la zone de texte **Source Path** (notez que la première partie du chemin est une constante qui change en fonction du type de réplication sélectionné).
5. Indiquez le chemin de la destination dans la zone de texte **Destination Path** (notez que la première partie du chemin est une constante qui change en fonction du type de réplication sélectionné).
6. Si vous souhaitez modifier des paramètres de connexion à l'hôte, sélectionnez l'onglet **Advanced**.
7. Sélectionnez **OK**.

   La réplication de la source vers la destination commence.

   Les résultats du test du système Data Domain ont renvoyé les recommandations suivantes en ce qui concerne l'estimation du temps nécessaire à l'initialisation de la réplication.

   Il s'agit *uniquement* de recommandations qui peuvent ne pas être exactes dans des environnements de production particuliers.

   - Avec une connexion T3, les performances d'un WAN en 100 ms sont d'environ 40 Mio/s de données précompressées, ce qui permet un transfert de données de :
     40 Mio/s = 25 secondes/Gio = 3,456 Tio/jour
   - Lorsque l'on utilise l'équivalent en base 2 d'un LAN gigabit, les performances sont d'environ 80 Mio/s de données précompressées, ce qui permet un transfert de données environ deux fois supérieur à celui d'un WAN T3.

Exemple 2 Équivalent de la CLI

Voici un exemple de création de paires de réplication MTree dans la CLI. Dans cet exemple, le système Data Domain source est `dd640` et le système Data Domain cible est `dlh5`. Pour plus de détails sur l'utilisation dans d'autres scénarios, reportez-vous au *Guide de référence des commandes Data Domain Operating System*.

1. Créez une structure MTree sur le système Data Domain source :

```
sysadmin@dd640# mtree create /data/col1/Oracle2
MTree "/data/col1/Oracle2" created successfully.
```

2. Créez le contexte de réplication dans le système Data Domain de destination, en utilisant le nom d'hôte complet.

```
sysadmin@dlh5# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

3. Créez le contexte de réplication dans le système Data Domain source, en utilisant le nom d'hôte complet.

```
sysadmin@dd640# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

Exemple 2 Équivalent de la CLI (suite)

4. Pour vérifier que le contexte de réplication MTree a été créé, utilisez la commande `replication show config`.
   La sortie est tronquée horizontalement dans cet exemple.

```
sysadmin@dlh5# replication show config
CTX  Source                                      Destination
---  ------------------------------------------
-----------------------------------------
1    dir://dd640.chaos.local/backup/Oracle2      dir://dlh5.chaos.local/backup/
Oracle2
2    mtree://dd640.chaos.local/data/col1/Oracle2  mtree://dlh5.chaos.local/data/col1/
Oracle2
---  ------------------------------------------
-----------------------------------------
 * Used for recovery only.
```

5. Pour lancer la réplication entre une source et une destination, exécutez la commande `replication initialize` sur la source. Cette commande vérifie si la configuration et les connexions sont correctes et affiche des messages d'erreur en cas de problème.

```
sysadmin@dd640# replication initialize mtree://dlh5.chaos.local/data/col1/Oracle2
 (00:08) Waiting for initialize to start...
 (00:10) Intialize started.
 Use 'replication watch mtree://dlh5.chaos.local/data/col1/Oracle2' to monitor progress.
```

Configuration d'une réplication bidirectionnelle
Pour créer une paire de réplication bidirectionnelle, suivez la procédure de création d'une paire de réplication de répertoire ou de MTree (en utilisant mtree2, par exemple) depuis l'hôte A vers l'hôte B. Procédez de la même manière pour créer une paire de réplication (en utilisant mtree1, par exemple) depuis l'hôte B vers l'hôte A. Dans le cadre de cette configuration, les chemins d'accès de destination ne peuvent pas être identiques.

Configuration d'une réplication un vers plusieurs
Pour créer une paire de réplication de type Un vers plusieurs, suivez la procédure de création d'une paire de réplication de répertoire ou de structure Mtree (par exemple, en utilisant mtree1) sur l'hôte A vers : (1) mtree1 sur l'hôte B, (2) mtree1 sur l'hôte C, et (3) mtree1 sur l'hôte D. Il n'est pas possible d'exécuter une restauration de réplication dans un contexte source dont le chemin mène à d'autres contextes ; les autres contextes doivent être arrêtés et resynchronisés à l'issue de la restauration.

Configuration de la réplication plusieurs vers un
Pour créer une paire de réplication de type Plusieurs vers un, suivez la procédure de création d'une paire de réplication de répertoire ou de Mtree (par exemple, (1) mtree1 depuis l'hôte A vers mtree1 sur l'hôte C et (2) mtree2 sur l'hôte B vers mtree2 sur l'hôte C).

Configuration d'une réplication en cascade
Pour créer une paire de réplication en cascade, suivez la procédure de création d'une paire de réplication de répertoire ou de MTree : (1) mtree1 sur l'hôte A vers mtree1 sur l'hôte B, et (2) sur l'hôte B, créer une paire pour mtree1 vers mtree1 sur l'hôte C. Le contexte de destination final (sur l'hôte C dans cet exemple, mais plus de trois tronçons sont acceptés) peut être un réplica de collection, un répertoire ou un réplica MTree.

Désactivation et activation d'une paire de réplication

La désactivation d'une paire de réplication suspend temporairement la réplication des données entre une source et une destination. La source cesse d'envoyer des données vers la destination et la destination cesse de servir de connexion active à la source.

Procédure

1. Sélectionnez une ou plusieurs paires de réplication dans le tableau Summary et sélectionnez **Disable Pair**.
2. Dans la boîte de dialogue Display Pair, sélectionnez **Next**, puis **OK**.
3. Pour relancer le fonctionnement d'une paire de réplication désactivée, sélectionnez une ou plusieurs paires de réplication dans le tableau Summary et sélectionnez **Enable Pair** pour afficher la boîte de dialogue Enable Pair.
4. Cliquez sur **Next**, puis sur **OK**. La réplication des données reprend.

Équivalent CLI

```
# replication disable {destination | all}

# replication enable {destination | all}
```

Suppression d'une paire de réplication

Lorsqu'une paire de réplication de répertoire ou de Mtree est supprimée, le répertoire ou la Mtree de destination, respectivement, devient inscriptible. En cas de suppression d'une paire de réplication de collection, le système DD de destination devient un système de lecture/écriture autonome et le système de fichiers est désactivé.

Procédure

1. Sélectionnez une ou plusieurs paires de réplication dans le tableau Summary et sélectionnez **Delete Pair**.
2. Dans la boîte de dialogue Delete Pair, sélectionnez **Next**, puis **OK**. Les paires de réplication sont supprimées.

Équivalent de la CLI

Avant d'exécuter cette commande, commencez toujours par exécuter la commande `filesys disable`. Exécutez ensuite la commande `filesys enable`.

```
# replication break {destination | all}
```

Certaines situations peuvent survenir dans lesquelles vous devez resynchroniser la réplication pour résoudre un problème. Pour plus d'informations sur la rupture et la resynchronisation de la réplication, reportez-vous à l'article de la KB *Rupture et resycnhronisation de la réplication des annauaires*, disponible à l'adresse https://support.emc.com/kb/180668.

Modification des paramètres de connexion de l'hôte

Pour diriger le trafic en sortie vers un port spécifique, modifiez un contexte actuel. Veuillez, pour ce faire, changer les paramètres de l'hôte de connexion en utilisant un nom d'hôte précédemment défini dans le fichier des hôtes locaux. Ce nom d'hôte doit correspondre à la destination. L'entrée d'hôte désignera une adresse alternative de destination pour cet hôte. Cette adresse alternative peut être requise sur les systèmes DD source et de destination.

Procédure

1. Sélectionnez la paire de réplication dans le tableau Summary, puis sélectionnez **Modify Settings**. Vous pouvez également modifier ces paramètres lorsque vous effectuez une création de paires, un démarrage de resynchronisation ou un démarrage de restauration en sélectionnant l'onglet **Advanced**.

2. Dans la boîte de dialogue Modify Connection Settings, modifiez l'un de ces paramètres ou tous ces paramètres :

   a. **Use Low Bandwidth Optimization** : pour les entreprises dotées de petits Datasets et de réseaux avec une bande passante inférieure ou égale à 6 Mbit/s, DD Replicator réduit la quantité de données à envoyer à l'aide d'un mode d'*optimisation d'une bande passante faible*. Ainsi, les sites distants dotés d'une bande passante limitée peuvent utiliser moins de bande passante ou répliquer et protéger un volume accru de données sur leurs réseaux existants. Vous devez activer l'optimisation d'une bande passante faible sur les systèmes DD source et de destination. Si, sur ces deux systèmes, les paramètres d'optimisation de la bande passante sont incompatibles, cette fonctionnalité est inactive pour le contexte. Une fois l'optimisation d'une bande passante faible activée sur la source et sur la destination, les deux systèmes doivent subir un cycle de nettoyage complet pour préparer les données existantes. Il faut donc exécuter `filesys clean start` sur les deux systèmes. La durée de ce cycle de nettoyage dépend de la quantité de données sur le système DD, mais prend plus de temps qu'une opération de nettoyage normale. Pour plus d'informations sur les commandes `filesys`, consultez le *Guide de référence des commandes de Data Domain Operating System*.

      Important : l'optimisation d'une bande passante faible n'est pas prise en charge si l'option logicielle DD Extended Retention est activée sur l'un ou l'autre des systèmes DD. Elle n'est pas non plus prise en charge pour la réplication de collection.

   b. **Enable Encryption Over Wire** : DD Replicator prend en charge le chiffrement des données en cours de transfert à l'aide du protocole SSL (Secure Socket Layer) version 1.0.1 standard, lequel utilise la suite de chiffrement ADH-AES256-GCM-SHA384 and DHE-RSA-AES256-GCM-SHA384 pour établir des connexions de réplication sécurisées. Les deux côtés de la connexion doivent activer cette fonction pour que le chiffrement s'effectue.

   c. **Network Preference** : vous pouvez choisir IPv4 ou IPv6. Un service de réplication compatible IPv6 peut toujours accepter des connexions provenant d'un client de réplication IPv4 si le service est accessible via IPv4. Un client de réplication compatible IPv6 peut toujours communiquer avec un service de réplication IPv4 si le service est accessible via IPv4.

   d. **Use Non-default Connection Host** : le système source envoie les données vers le port d'écoute du système cible. Étant donné que, sur un système source, la réplication peut être configurée pour plusieurs systèmes de destination, avec chacun un port d'écoute différent, chaque contexte du système source peut configurer le port de connexion sur le port d'écoute correspondant du système cible.

3. Cliquez sur **Next**, puis sur **Close**.

   Les paramètres de la paire de réplication sont mis à jour et la réplication reprend.

Équivalent CLI

```
#replication modify <destination> connection-host <new-host-
name> [port <port>]
```

Gestion des systèmes de réplication

Vous pouvez ajouter ou supprimer des systèmes Data Domain à utiliser pour la réplication à l'aide de la boîte de dialogue Manage Systems.

Procédure

1. Sélectionnez **Manage Systems**.
2. Dans la boîte de dialogue Manage Systems, ajoutez ou supprimez des systèmes Data Domain, si nécessaire.
3. Sélectionnez **Close**.

Restauration de données à partir d'une paire de réplication

Si les données de réplication source deviennent inaccessibles, elles peuvent être *restaurées* à partir de la destination de la paire de réplication. La source doit être vide pour que la restauration puisse se poursuivre. La restauration peut s'appliquer à toutes les topologies de réplication, à l'exception de la réplication MTree.

La restauration de données à partir d'un pool de répertoires, et de paires de réplication de collection et de répertoire, est décrite dans les sections suivantes.

Restauration de données du pool de répertoires

Vous pouvez restaurer des données d'un pool de répertoires, mais pas d'un pool MTree.

Procédure

1. Sélectionnez **More** > **Start Recover**.
2. Dans la boîte de dialogue Start Recover, sélectionnez **Pool** dans le menu **Replication Type**.
3. Sélectionnez le nom d'hôte du système source dans le menu **System to recover to**.
4. Sélectionnez le nom d'hôte du système de destination dans le menu **System to recover from**.
5. Sélectionnez le contexte sur la destination à partir de laquelle les données sont restaurées.
6. Si vous souhaitez modifier des paramètres de connexion à l'hôte, sélectionnez l'onglet **Advanced**.
7. Cliquez sur **OK** pour démarrer la restauration.

Restauration de données de paires de réplication de collection

Pour restaurer des données de paires de réplication de collection, l'état du système de fichiers source doit être irréprochable et le contexte de destination doit être entièrement initialisé.

Procédure

1. Sélectionnez **More** > **Start Recover** pour afficher la boîte de dialogue Start Recover.
2. Sélectionnez **Collection** dans le menu **Replication Type**.
3. Sélectionnez le nom d'hôte du système source dans le menu **System to recover to**.
4. Sélectionnez le nom d'hôte du système de destination dans le menu **System to recover from**.

5. Sélectionnez le contexte sur la destination à partir de laquelle les données sont restaurées. Une seule collection existera sur la destination.
6. Pour modifier des paramètres de connexion à l'hôte, sélectionnez l'onglet **Advanced**.
7. Cliquez sur **OK** pour démarrer la restauration.

Restauration de données de paires de réplication de répertoire

Pour restaurer des données de paires de réplication de répertoire, vous devez créer le même répertoire que celui utilisé dans le contexte d'origine (mais le laisser vide).

Procédure

1. Sélectionnez **More** > **Start Recover** pour afficher la boîte de dialogue Start Recover.
2. Sélectionnez **Directory** dans le menu **Replication Type**.
3. Sélectionnez le nom d'hôte du *système sur lequel les données doivent être restaurées* dans le menu **System to recover to**.
4. Sélectionnez le nom d'hôte du *système qui sera choisi comme source des données* dans le menu **System to recover from**.
5. Sélectionnez le contexte à restaurer dans la liste de contexte.
6. Pour modifier des paramètres de connexion à l'hôte, sélectionnez l'onglet **Advanced**.
7. Cliquez sur **OK** pour démarrer la restauration.

Abandon de la restauration d'une paire de réplication

Si la restauration d'une paire de réplication échoue ou doit être interrompue, vous pouvez arrêter le processus.

Procédure

1. Dans le menu More, sélectionnez **Abort Recover** pour afficher la boîte de dialogue Abort Recover qui précise les contextes effectuant actuellement une restauration.
2. Dans la liste, cochez la case d'un ou de plusieurs contextes à abandonner.
3. Sélectionnez **OK**.

À effectuer

Il est conseillé de relancer la restauration sur la source dès que cela est possible.

Resynchronisation d'une paire de réplication de MTree, de répertoire ou de pool

La *resynchronisation* est le processus consistant à resynchroniser la source et la destination d'une paire de réplication après une interruption manuelle. La paire de réplication est resynchronisée de sorte que les deux points d'accès contiennent les mêmes données. La resynchronisation est disponible pour la réplication de répertoire, de MTree ou de pool, mais pas pour la réplication de collection.

Une resynchronisation de réplication peut également servir :

- À recréer un contexte qui a été supprimé.
- Lorsqu'une destination commence à manquer d'espace alors que la source doit encore répliquer des données
- À convertir une paire de réplication de répertoire en paire de réplication de MTree.

Procédure

1. Supprimez le contexte sur les systèmes source et destination de réplication.
2. Dans le système source de réplication ou de destination de réplication, sélectionnez **More** > **Start Resync** pour afficher la boîte de dialogue Start Resync.
3. Sélectionnez le type de réplication à resynchroniser : **répertoire**, **MTree** ou **pool**.
4. Sélectionnez le nom d'hôte du système source de réplication dans le menu **Source System**.
5. Sélectionnez le nom d'hôte du système de destination de réplication dans le menu **Destination System**.
6. Saisissez le chemin de la source de réplication dans la zone de texte **Source Path**.
7. Indiquez le chemin de destination de réplication dans la zone de texte **Destination Path**.
8. Pour modifier des paramètres de connexion à l'hôte, sélectionnez l'onglet **Advanced**.
9. Sélectionnez **OK**.

Équivalent de l'interface de ligne de commande (CLI)

```
# replication resync destination
```

Abandon de la resynchronisation d'une paire de réplication

Si la resynchronisation d'une paire de réplication échoue ou doit prendre fin, vous pouvez arrêter le processus de resynchronisation.

Procédure

1. Dans le système source de réplication ou de destination de réplication, sélectionnez **More** > **Abort Resync** pour afficher la boîte de dialogue Abort Resync, qui répertorie tous les contextes exécutant la resynchronisation.
2. Cochez la case d'un ou de plusieurs contextes pour abandonner leur resynchronisation.
3. Sélectionnez **OK**.

Vue DD Boost

La vue DD Boost fournit des informations de configuration et de résolution des problèmes aux administrateurs NetBackup qui ont configuré des systèmes DD pour exécuter DD Boost AIR (réplication automatique d'image) ou n'importe quelle application DD Boost utilisant la réplication de fichiers gérés.

Reportez-vous au document intitulé *Guide d'administration de Data Domain Boost for OpenStorage* pour obtenir les instructions de configuration de DD Boost AIR.

L'onglet **File Replication** affiche les informations suivantes :

- Currently Active File Replication :
  - Direction (entrante et sortante) et nombre de fichiers dans chaque direction.
  - Données restant à répliquer (valeur avant compression en Gio) et quantité de données déjà répliquées (valeur avant compression en Gio).

    - Taille totale : quantité de données à répliquer et de données déjà répliquées (valeur avant compression en Gio).
- Most Recent Status : réplications de fichiers totales avec indication de leur réussite ou de leur échec
    - pendant la dernière heure
    - au cours des dernières 24 heures
- Remote Systems :
    - Sélectionnez une réplication dans la liste.
    - Sélectionnez la période couverte dans le menu.
    - Sélectionnez **Show Details** pour plus d'informations sur ces fichiers de systèmes distants.

L'onglet **Storage Unit Associations** affiche les informations suivantes pouvant servir à des fins d'audit ou pour vérifier l'état d'événements DD Boost AIR utilisés pour les réplications d'images d'unités de stockage :

- Une liste de toutes les **associations** de l'unité de stockage connues du système. La source se trouve sur la gauche et la destination sur la droite. Ces informations indiquent la configuration d'AIR sur le système Data Domain.
- L'option **Event Queue** correspond à la liste des événements en attente. Elle affiche l'unité de stockage locale, l'ID de l'événement et l'état de l'événement.

Le système tente de faire correspondre les deux extrémités d'un chemin DD Boost pour former une paire et la présenter comme paire/enregistrement. Si la correspondance est impossible, pour diverses raisons, le chemin d'accès à distance est signalé comme *Unresolved*.

Fichiers de système distant

Le bouton Show Details fournit des informations sur le système de réplication de fichiers distant sélectionné. L'option File Replication affiche des informations de début et de fin, ainsi que sur la taille et la quantité de données du système de réplication de fichier distant sélectionné. Le graphique des performances affiche les performances au fil du temps pour le système de réplication de fichiers à distance sélectionné.

Tableau 194 Réplication de fichiers

Élément	Description
Start	Début de la période.
End	Fin de la période.
File Name	Nom du fichier de réplication spécifique.
Status	État le plus récent (réussite ou échec).
Pre-Comp Size (Mio)	Volume de données entrantes et sortantes précompressées par rapport au débit du réseau ou aux données après compression (en Mio).
Network Bytes (Mio)	Quantité de données de débit du réseau (en Mio).

Tableau 195 Graphique des performances

Élément	Description
Duration	Durée de la réplication (1 jour, 7 jours ou 30 jours).
Interval	Intervalle de la réplication (chaque jour ou chaque semaine).
Pre-Comp Replicated	Volume de données entrantes et sortantes précompressées (en Gio).
Post-Comp Replicated	Quantité de données après compression (en Gio).
Network Bytes	Quantité de données de débit du réseau (en Gio).
Files Succeeded	Nombre de fichiers ayant été répliqués avec succès.
Files Failed	Nombre de fichiers dont la réplication a échoué.
Show in new window	Ouvre une fenêtre distincte.
Print	Imprime le graphique.

Vue Performance

La vue Performance affiche un graphique qui reflète les fluctuations des données pendant la réplication. Il s'agit des statistiques agrégées de chaque paire de réplication de ce système DD.

- La **durée** (axe des x) est fixée à 30 jours par défaut.
- Les **performances de réplication** (axe des y) sont exprimées en gibioctets ou en mébioctets (les équivalents binaires des gigaoctets et mégaoctets).
- Le **réseau entrant** représente le nombre total d'octets du réseau de réplication entrant dans le système (tous les contextes).
- Le **réseau sortant** représente le nombre total d'octets du réseau de réplication quittant le système (tous les contextes).
- Pour obtenir un relevé à un point dans le temps, placez le curseur à l'endroit voulu sur le graphique.
- Lors des périodes d'inactivité (quand aucune donnée n'est transférée), la forme du graphique peut afficher une ligne progressivement descendante au lieu de la ligne fortement décroissante attendue.

Vue Advanced Settings

L'option Advanced Settings permet de contrôler la régulation et les paramètres réseau.

Paramètres de régulation

- **Throttle Override** : lorsque cette option est configurée, elle présente la vitesse de régulation, ou 0 qui signifie que l'ensemble du trafic de réplication est arrêté.
- **Permanent Schedule** : indique l'heure (et les jours de la semaine) à laquelle la régulation planifiée est effectuée.

Paramètres réseau

- **Bandwidth** : affiche le flux de données défini si la bande passante a été configurée ou Unlimited (valeur par défaut) dans le cas contraire. Le flux de données moyen vers la destination de réplication est d'au moins 98 304 bits par seconde (12 KiB).
- **Delay** : affiche le délai réseau (en millisecondes) si celui-ci a été configuré ou None (valeur par défaut) dans le cas contraire.
- **Listen Port** : affiche le port d'écoute si celui-ci a été configuré ou 2051 (valeur par défaut) dans le cas contraire.

Ajout de paramètres de régulation

Pour modifier la quantité de bande passante utilisée par un réseau pour la réplication, vous pouvez définir une *régulation de la réplication* pour le trafic de réplication.

Il existe trois types de paramètres de régulation de la réplication :

- **Scheduled throttle** : la vitesse de régulation est définie sur une durée ou à une période prédéfinie.
- **Current throttle** : la vitesse de régulation est définie jusqu'à la prochaine modification planifiée ou jusqu'à un redémarrage du système.
- **Override throttle** : les deux types de régulation précédents sont remplacés. Ceci persiste, même en cas de redémarrage, jusqu'à ce que vous sélectionniez **Clear Throttle Override** ou que vous émettiez la commande `replication throttle reset override .`

Vous pouvez également définir une régulation par défaut ou une régulation pour des destinations spécifiques, comme suit :

- **Default throttle** : lorsque cette option est configurée, tous les contextes de réplication sont limités à cette régulation, à l'exception des destinations spécifiées par les régulations de destination (voir l'élément suivant).
- **Destination throttle** : cette régulation est utilisée lorsque seules quelques destinations doivent être régulées, ou lorsqu'une destination nécessite une configuration de régulation différente de la régulation par défaut. Lorsqu'une régulation par défaut existe déjà, elle s'applique en priorité à la destination indiquée. Vous pouvez, par exemple, définir la régulation de la réplication par défaut sur *10 Kbit/s*, mais (en utilisant une régulation de destination) définir un seul contexte de réplication de collection sur *Unlimited*.

Remarque

Actuellement, vous ne pouvez définir et modifier la régulation de destination qu'à l'aide de l'interface de ligne de commande (CLI) ; cette fonctionnalité n'est pas disponible dans DD System Manager. Pour obtenir de la documentation sur cette fonction, reportez-vous au chapitre sur la commande `replication throttle` du *Guide de référence des commandes de Data Domain Operating System*. Si DD System Manager détecte que vous avez défini une ou plusieurs régulations de destination, vous recevez un avertissement et devez utiliser l'interface de ligne de commande pour continuer.

Remarques supplémentaires au sujet de la régulation de la réplication :

- Les régulations ne se définissent qu'à la source. La seule régulation s'appliquant à une destination est l'option **0 Bps (Disabled)** qui désactive tout le trafic de réplication.
- La valeur minimale pour une régulation de la réplication est de 98 304 bits par seconde.

Procédure

1. Pour afficher la boîte de dialogue Add Throttle Setting, sélectionnez **Replication** > **Advanced Settings** > **Add Throttle Setting**.
2. Définissez les jours de la semaine pendant lesquels la régulation doit être active en sélectionnant **Every Day** ou en cochant les cases en regard d'un ou de plusieurs jours.
3. Définissez l'heure à laquelle la régulation doit commencer à l'aide des sélecteurs déroulants **Start Time** pour le format heure:minute et matin/soir.
4. Pour **Throttle Rate** :
   - Sélectionnez **Unlimited** pour ne définir aucune limite.
   - Saisissez un nombre dans la zone de texte (par exemple, 20 000) et sélectionnez la vitesse dans le menu (bps, Kbps, Bps ou KBps).
   - Sélectionnez l'option **0 Bps (disabled)** pour désactiver l'ensemble du trafic de réplication.
5. Cliquez sur **OK** pour définir l'ordonnanceur. Le nouvel ordonnanceur apparaît sous **Permanent Schedule**.

Résultats

Les régulations s'exécutent à la vitesse définie jusqu'à la prochaine modification planifiée ou jusqu'à ce qu'un nouveau paramètre de régulation impose un changement.

Suppression des paramètres de régulation

Vous pouvez supprimer un seul paramètre de régulation ou tous les paramètres de régulation à la fois.

Procédure

1. Pour afficher la boîte de dialogue Delete Throttle Setting, sélectionnez **Replication** > **Advanced Settings** > **Delete Throttle Setting**.
2. Cochez la case du paramètre de régulation à supprimer ou celle de l'en-tête pour supprimer tous les paramètres. Cette liste peut inclure des paramètres pour l'état « Disabled ».
3. Cliquez sur **OK** pour supprimer le paramètre.
4. Dans la boîte de dialogue Delete Throttle Setting Status, sélectionnez **Close**.

Remplacement temporaire d'un paramètre de régulation

Un remplacement de régulation change temporairement un paramètre de régulation. Le paramètre actuel est indiqué en haut de la fenêtre.

Procédure

1. Pour afficher la boîte de dialogue Throttle Override, sélectionnez **Replication** > **Advanced Settings** > **Set Throttle Override**.
2. Définissez un nouveau remplacement de régulation ou effacez un remplacement précédent.
   a. Pour définir un nouveau remplacement de régulation :
      - sélectionnez **Unlimited** pour revenir à la vitesse de régulation définie par le système (aucune régulation effectuée) ; ou
      - définissez la vitesse et les bits de régulation dans la zone de texte (p. ex., 20 000 et bps, Kbps, Bps ou KBps) ; ou

- Sélectionnez **0 Bps (Disabled)** pour définir la vitesse de régulation sur 0, en arrêtant efficacement tout le trafic réseau de la réplication.
- Pour appliquer la modification temporairement, sélectionnez **Clear at next scheduled throttle event**.

b. Pour supprimer un remplacement défini précédemment, sélectionnez **Clear Throttle Override**.

3. Sélectionnez **OK**.

Modification des paramètres réseau

À l'aide des paramètres de bande passante et de délai réseau, la réplication calcule la taille de mémoire tampon TCP adéquate (protocole de contrôle de transmission) pour l'utilisation de la réplication. Ces paramètres réseau sont des paramètres globaux du système DD et n'ont besoin d'être définis qu'une seule fois par système.

Notez les points suivants :

- Vous pouvez déterminer la bande passante réelle et les valeurs réelles de délai réseau pour chaque serveur à l'aide de la commande `ping`.
- Les paramètres réseau par défaut d'un système de restauration sont particulièrement bien adaptés à la réplication dans des configurations à faible latence, par exemple sur un réseau Ethernet local de 100 Mbit/s ou de 1 000 Mbit/s sur lequel le temps de latence aller-retour (tel qu'il est mesuré par la commande `ping`) est généralement inférieur à 1 milliseconde. Ces valeurs par défaut conviennent également à la réplication sur des WAN à bande passante faible à moyenne, sur lesquels la latence peut atteindre 50 à 100 millisecondes. Cependant, pour les réseaux à forte latence et à large bande passante, il est nécessaire d'effectuer quelques réglages des paramètres réseau.
  Le nombre important à prendre en compte lors du réglage est la valeur du délai de bande passante obtenue en multipliant la bande passante par la latence aller-retour du réseau. Cette valeur est une mesure de la quantité de données pouvant être transmises sur le réseau avant qu'un accusé de réception puisse revenir de l'extrémité éloignée. Si la valeur du délai de bande passante d'un réseau de réplication est supérieure à 100 000, il est bénéfique pour les performances de la réplication que les paramètres réseau soient définis dans les deux systèmes de restauration.

Procédure

1. Pour afficher la boîte de dialogue Network Settings, sélectionnez **Replication** > **Advanced Settings** > **Change Network Settings**.
2. Dans la zone Network Settings, sélectionnez **Custom Values**.
3. Saisissez les valeurs des options **Delay** et **Bandwidth** dans les zones de texte. Le paramètre de délai du réseau est exprimé en millisecondes et celui de la bande passante en octets par seconde.
4. Dans la zone Listen Port, saisissez une nouvelle valeur dans la zone de texte. Le port d'écoute IP par défaut d'une destination de réplication destiné à recevoir les flux de données provenant de la source de la réplication est le port 2051. Il s'agit d'un paramètre global du système DD.
5. Sélectionnez **OK**. Les nouveaux paramètres apparaissent dans le tableau des paramètres réseau.

Surveillance de la réplication

DD System Manager offre plusieurs moyens de surveiller l'état d'une réplication : vous pouvez vérifier l'état d'une paire de réplication, assurer un suivi des procédures de sauvegarde, contrôler les performances ou encore suivre le déroulement d'un processus de réplication.

Affichage du temps d'exécution estimé de la réplication d'une procédure de sauvegarde

Utilisez la zone Completion Predictor pour connaître l'heure estimée d'achèvement de la réplication d'une procédure de sauvegarde.

Procédure

1. Sélectionnez **Replication** > **Summary**.
2. Sélectionnez un contexte de réplication pour lequel vous souhaitez afficher des informations détaillées.
3. Dans la zone Completion Predictor, sélectionnez des options de la liste déroulante **Source Time** relatives à l'heure d'achèvement de la réplication et sélectionnez **Track**.

   Une estimation du temps d'exécution nécessaire à la réplication d'une procédure de sauvegarde spécifique sur la destination s'affiche dans la zone Completion Time. Si la réplication est terminée, `Completed` s'affiche dans cette zone.

Vérification des performances d'un contexte de réplication

Pour vérifier les performances d'un contexte de réplication au fil du temps, sélectionnez un contexte de réplication dans la vue Summary, puis sélectionnez **Performance Graph** dans la zone Detailed Information.

Suivi de l'état d'un processus de réplication

Pour afficher la progression de l'initialisation d'une opération de réplication, de resynchronisation ou de restauration, utilisez la vue **Replication** > **Summary** pour connaître l'état actuel.

Équivalent CLI

```
# replication show config all
CTX  Source                                   Destination
Connection Host and Port     Enabled
---  -----------------------        -----------------------        -----------------------
-------
1       dir://host2/backup/dir2     dir://host3/backup/dir3
host3.company.com               Yes
2       dir://host3/backup/dir3     dir://host2/backup/dir2
host3.company.com               Yes
```

En cas de spécification d'une version IP, utilisez la commande suivante pour vérifier sa configuration :

```
# replication show config rctx://2

CTX:                        2
Source:                     mtree://ddbeta1.dallasrdc.com/data/col1/EDM1
Destination:                mtree://ddbeta2.dallasrdc.com/data/col1/EDM_ipv6
Connection Host:            ddbeta2-ipv6.dallasrdc.com
```

```
Connection Port:             (default)
Ipversion:                   ipv6
Low-bw-optim:                disabled
Encryption:                  disabled
Enabled:                     yes
Propagate-retention-lock:    enabled
```

Latence de réplication

Le temps écoulé entre deux copies de données est appelé latence de réplication.

Vous pouvez mesurer la latence de réplication entre deux contextes avec la commande état de réplication. Pour plus d'informations sur la détermination de la cause de la latence de réplication et l'atténuation de son impact, reportez-vous à l'article de la KB *Résolution des problèmes de latence de réplication*, disponible à l'adresse https://support.emc.com/kb/180482.

Réplication avec HA

Les adresses IP flottantes permettent aux systèmes HA de spécifier une seule adresse IP pour la configuration de la réplication qui fonctionnera quel que soit le nœud de la paire HA active.

Sur les réseaux IP, les systèmes HA utilisent une adresse IP flottante afin de fournir un accès aux données à la paire HA Data Domain, quel que soit le nœud physique actif. La commande net config fournit l'option **[type {fixed | floating}]** pour configurer une adresse IP flottante. Consultez le *Guide de référence des commandes de Data Domain Operating System* pour plus d'informations.

Si un nom de domaine est nécessaire pour accéder à l'adresse IP flottante, spécifiez le nom du système HA comme étant le nom de domaine. Exécutez la commande `ha status` pour localiser le nom du système HA.

Remarque

Exécutez la commande `net show hostname type ha-system` pour afficher le nom du système HA et si nécessaire, exécutez la commande `net set hostname ha-system command` pour modifier le nom du système HA.

Tous les accès à un système de fichiers doivent s'effectuer par le biais de l'adresse IP flottante. Lorsque vous configurez des opérations de sauvegarde et de réplication sur une paire HA, spécifiez toujours l'adresse IP flottante comme étant l'adresse IP du système Data Domain. Les fonctions de Data Domain comme DD Boost et la réplication acceptent l'adresse IP flottante pour la paire HA de la même manière qu'ils acceptent l'adresse IP du système pour un système non HA.

Réplication entre des systèmes HA et non HA

Si vous souhaitez configurer une réplication entre un système haute disponibilité (HA) et un système exécutant DD OS 5.7.0.3 ou une version antérieure, vous devez créer et gérer cette réplication sur le système haute disponibilité si vous souhaitez utiliser l'interface utilisateur de DD System Manager.

Toutefois, vous pouvez exécuter des réplications à partir d'un système non HA vers un système HA à l'aide de la CLI, ainsi qu'à partir d'un système HA vers un système non HA.

La réplication de collection entre des systèmes HA et non HA n'est pas prise en charge. La réplication de répertoires ou de structures MTree est nécessaire pour pouvoir répliquer des données entre systèmes HA et non HA.

Réplication d'un système avec quota vers un système sans quota

Répliquez un système Data Domain avec un DD OS prenant en charge les quotas, en un système avec un DD OS n'ayant pas de quotas.

- Une resynchronisation inverse, qui prend les données du système sans quotas et les restaure dans une structure MTree sur le système ayant des quotas activés (et qui continue d'avoir des quotas activés).
- Une initialisation inverse à partir du système sans quotas, qui prend les données et crée une nouvelle structure MTree sur le système qui prend en charge les quotas, mais qui n'a pas de quotas activés, puisqu'il a été créé à partir de données issues d'un système sans quotas.

Remarque

Les quotas ont été introduits dans la version 5.2 de DD OS.

Replication Scaling Context

La fonction Replication Scaling Context vous offre une plus grande flexibilité lors de la configuration des contextes de réplication.

Dans les environnements comportant plus de 299 contextes de réplication de répertoire et de structure MTree, cette fonction vous permet de configurer les contextes dans n'importe quel ordre. Auparavant, il fallait configurer les contextes de réplication de répertoire avant les contextes de réplication de structure MTree.

Le nombre total de contextes de réplication ne peut pas dépasser 540.

Remarque

Cette fonction est disponible uniquement sur les systèmes Data Domain exécutant la version 6.0 de DD OS.

Migration de la réplication de répertoire vers la structure MTree

La fonction d'optimisation de réplication de répertoire vers une structure MTree (D2M) vous permet de migrer des contextes de réplication de répertoire existants vers de nouveaux contextes de réplication basés sur des structures Mtree, c'est-à-dire des partitions logiques du système de fichiers. Cette fonction vous permet également de contrôler le déroulement du processus et de vous assurer qu'il a réussi.

La fonction D2M est compatible avec les versions 5.6, 5.7 et 6.0 du système d'exploitation Data Domain.

Le système Data Domain source doit exécuter DD OS 6.0 pour utiliser cette fonction, mais le système de destination peut exécuter la version 5.6, 5.7 ou 6.0. Toutefois, les bénéfices attendus en matière d'optimisation des performances sont visibles uniquement lorsque les systèmes source et de destination exécutent tous les deux la version 6.0.

Remarque

Bien que vous puissiez utiliser l'interface utilisateur (GUI) pour cette opération, il est recommandé d'utiliser l'interface de ligne de commande (CLI) pour obtenir des performances optimales.

Exécution d'une migration de la réplication de répertoire vers la réplication de MTree

Veillez à ne pas arrêter ou redémarrer votre système lors de la migration (D2M) de répertoire vers une structure MTree.

Procédure

1. Arrêtez toutes les opérations d'acquisition vers le répertoire source de réplication de répertoire.
2. Créez une structure MTree sur le système DD source : **`mtree create /data/col1/`*`mtree-name`***

   Remarque

   Ne créez pas la structure MTree sur le système DD de destination.

3. (Facultatif) Activez DD Retention Lock sur la structure MTree.

   Remarque

   Si le système source contient des fichiers verrouillés pour rétention, vous souhaiterez éventuellement conserver DD Retention Lock sur la nouvelle structure MTree.

   Voir Activation de DD Retention Lock Compliance sur une MTree.
4. Créez le contexte de réplication de MTree sur les systèmes DD source et de destination : **`replication add source mtree://`*`source-system-name/source mtree`*` replication add destination mtree://`*`destination-system-name/destination mtree`***
5. Démarrez la migration D2M : **`replication dir-to-mtree start from`** ***`rctx://1`*** **`to`** ***`rctx://2`***

   Dans l'exemple précédent,
   `rctx://1`
   désigne le contexte de réplication de répertoire, lequel réplique le répertoire `backup backup/dir1` sur le système source ;
   `rctx://2`
   fait référence au contexte de réplication MTree, lequel réplique la structure MTree `/data/col1/mtree1` sur le système source.

   Remarque

   L'exécution de cette commande peut prendre plus de temps que prévu. N'appuyez pas sur Ctrl-C au cours du processus ; cela aurait pour effet d'annuler la migration D2M.

```
Phase 1 of 4 (precheck):
    Marking source directory /backup/dir1 as read-only...Done.
```

```
Phase 2 of 4 (sync):
    Syncing directory replication context...0 files flushed.
current=45 sync_target=47 head=47
current=45 sync_target=47 head=47
Done. (00:09)

Phase 3 of 4 (fastcopy):
    Starting fastcopy from /backup/dir1 to /data/col1/
mtree1...
    Waiting for fastcopy to complete...(00:00)
    Fastcopy status: fastcopy /backup/dir1 to /data/col1/
mtree1: copied 24
files, 1 directory in 0.13 seconds
    Creating snapshot 'REPL-D2M-
mtree1-2015-12-07-14-54-02'...Done

Phase 4 of 4 (initialize):
    Initializing MTree replication context...
(00:08) Waiting for initialize to start...
(00:11) Initialize started.

Use 'replication dir-to-mtree watch rctx://2' to monitor
progress.
```

Affichage de la progression de la migration du répertoire vers la structure MTree

Il est possible de déterminer l'étape de la migration en cours dans le cadre de la réplication de répertoire vers la structure MTree (D2M).

Procédure

1. Saisissez **replication dir-to-mtree watch *rctx://2*** pour afficher la progression.

   `rctx://2`
   spécifie le contexte de réplication.

   Vous devriez voir la sortie suivante :

```
Use Control-C to stop monitoring.
Phase 4 of 4 (initialize).
(00:00) Replication initialize started...
(00:02) initializing:
(00:14)     100% complete, pre-comp: 0 KB/s, network: 0 KB/
s
(00:14) Replication initialize completed.
Migration for ctx 2 successfully completed.
```

Vérification de l'état de la migration de la réplication de répertoire vers la structure MTree

Vous pouvez utiliser la commande `replication dir-to-mtree status` pour vérifier si la migration de la réplication de répertoire vers la structure MTree (D2M) a réussi.

Procédure

1. Pour ce faire, saisissez la commande suivante :
   `rctx://2`
   représente le contexte de réplication de la structure MTree sur le système source :**replication dir-to-mtree status rctx://2**

Le résultat doit ressembler à ceci :

```
Directory Replication CTX:          1
MTree Replication CTX:              2
Directory Replication Source:       dir://127.0.0.2/backup/dir1
MTree Replication Source:           mtree://127.0.0.2/data/
col1/mtree1
MTree Replication Destination:      mtree://127.0.0.3/data/
col1/mtree1
Migration Status:                   completed
```

S'il n'existe aucune migration en cours, voici ce qui s'affiche :

```
# replication dir-to-mtree status rctx://2
No migration status for context 2.
```

2. Commencez l'acquisition des données sur la structure MTree du système DD source une fois le processus de migration terminé.
3. (Facultatif) Arrêtez le contexte de réplication de répertoire sur les systèmes source et cible.

   Reportez-vous au *Guide de référence des commandes de Data Domain Operating System Version 6.0* pour plus d'informations au sujet de la commande `replication break`.

Abandon de la réplication D2M

Si nécessaire, vous pouvez abandonner la procédure de migration du répertoire vers la structure MTree (D2M).

La commande `replication dir-to-mtree abort` permet d'abandonner le processus de migration en cours et de refaire passer le répertoire de l'état lecture seule à l'état lecture-écriture.

Procédure

1. Dans l'interface de ligne de commande (CLI), saisissez la commande suivante : `rctx://2`
   désigne ici le contexte de réplication de la structure MTree : **`replication dir-to-mtree abort rctx://2`**

   Vous devriez voir la sortie suivante :

   ```
   Canceling directory to MTree migration for context dir-name.
   Marking source directory dir-name as read-write...Done.
   The migration is now aborted.
   Remove the MTree replication context and MTree on both source
   and destination
   host by running 'replication break' and 'mtree delete'
   commands.
   ```

2. Brisez le contexte de réplication de la structure MTree : **`replication break rctx://2`**
3. Supprimez la structure MTree sur le système source : **`mtree delete mtree-path`**

Résolution des problèmes liés à la migration D2M

Si vous rencontrez des difficultés pour configurer la réplication de répertoire vers une structure MTree (D2M), une opération peut vous permettre de résoudre différents problèmes.

La procédure `dir-to-mtree abort` peut vous aider à abandonner correctement le processus D2M. Vous devez exécuter cette procédure dans les cas suivants :

- L'état de la migration D2M est signalé comme abandonné.
- Le système Data Domain a redémarré lors de la migration D2M.
- Une erreur s'est produite lors de l'exécution de la commande `replication dir-to-mtree start`.
- L'acquisition n'a pas été arrêtée avant de commencer la migration.
- Le contexte de réplication de la structure MTree a été initialisé avant la saisie de la commande `replication dir-to-mtree start`.

Remarque

N'exécutez pas **`replication break`** sur le contexte de réplication de la structure MTree avant la fin du processus D2M.
Exécutez toujours **`replication dir-to-mtree abort`** avant la commande **`replication break`** sur le contexte de réplication de la structure MTree.

Le fait d'exécuter prématurément la commande **`replication break`** transforme irrémédiablement le répertoire source drepl en lecture seule.

Dans ce cas, contactez le Support.

Procédure

1. Saisissez **`replication dir-to-mtree abort`** pour abandonner le processus.
2. Brisez le contexte de réplication de MTree nouvellement créé sur les systèmes Data Domain source et de destination.

   Dans l'exemple suivant, le contexte de réplication de la structure MTree est `rctx://2`
   .

   ```
   replication break rctx://2
   ```

3. Supprimez les structures MTree correspondantes sur les systèmes source et de destination.

   ```
   mtree delete mtree-path
   ```

   Remarque

   Les structures MTree marquées pour suppression restent dans le système de fichiers jusqu'à l'exécution de la commande `filesys clean`.

   Consultez le *Guide de référence des commandes de Data Domain Operating System Version 6.0* pour plus d'informations.

4. Exécutez la commande `filesys clean start` sur les systèmes source et de destination.

   Pour plus d'informations au sujet des commandes `filesys clean`, reportez-vous au *Guide de référence des commandes d'e Data Domain Operating System Version 6.0*.

5. Redémarrez le processus.

   Reportez-vous à la section Migration de la réplication de répertoire vers la structure MTree.

Résolution d'autres problèmes liés au processus D2M

Plusieurs solutions peuvent être envisagées si vous avez oublié d'activer DD Retention Lock pour la nouvelle structure MTree ou si une erreur se produit après l'initialisation de la migration de répertoire vers une structure MTree.

En cas de non activation de la fonction DD Retention Lock
Si vous avez oublié d'activer DD Retention Lock pour la nouvelle structure MTree et que le répertoire source contient des fichiers ou des répertoires verrouillés pour rétention, plusieurs options sont possibles :

- Laisser la migration D2M se poursuivre. Toutefois,vous ne disposerez pas des informations relatives à DD Retention Lock dans la structure MTree après la migration.
- Abandonner le processus D2M en cours, comme décrit dans la section Abandon de la réplication D2M à la page 493 et redémarrer le processus avec la fonction DD Retention Lock activée sur la structure MTree source.

En cas d'erreur après l'initialisation
Si le processus `replication dir-to-mtree start` se termine sans erreur, mais que vous détectez une erreur lors de l'initialisation de la réplication de la structure MTree (phase 4 du processus de migration D2M), vous pouvez effectuer les étapes suivantes :

1. Assurez-vous qu'il n'existe aucun problème au niveau du réseau.
2. Initialisez le contexte de réplication de la structure MTree.

Utilisation de la réplication de la collection pour la reprise après sinistre avec SMT

Pour utiliser le système de destination d'une paire de réplication de collection configurée avec SMT en tant que système de remplacement pour la reprise après sinistre, des étapes de configuration SMT supplémentaires doivent être effectuées en plus des autres étapes de configuration requises pour remettre un système de remplacement en ligne.

Avant de commencer

Cette utilisation du système de destination de la réplication de collection nécessite la configuration et l'enregistrement de rapports d'autosupport. L'article de la base de connaissances *Collection replica with smt enabled*, disponible sur https://support.emc.com, fournit des informations supplémentaires.

Le système de remplacement n'aura pas les détails SMT suivants :

- Listes de notifications d'alerte pour chaque unité de tenant

- Tous les utilisateurs alloués au protocole DD Boost pour être utilisés par des tenants SMT, si DD Boost est configuré sur le système
- L'unité de tenant par défaut associée à chaque utilisateur DD Boost, le cas échéant, si DD Boost est configuré sur le système

Procédez comme suit pour configurer SMT sur le système de remplacement.

Procédure

1. Dans le rapport d'autosupport, localisez le résultat de la commande `smt tenant-unit show detailed`.

```
Tenant-unit: "tu1"
Summary:
Name   Self-Service   Number of Mtrees   Types           Pre-Comp(GiB)
----   ------------   ----------------   --------        -------------
tu1    Enabled        2                  DD Boost        2.0
----   ------------   ----------------   --------        -------------

Management-User:
User     Role
------   ------------
tu1_ta   tenant-admin
tu1_tu   tenant-user
tum_ta   tenant-admin
------   ------------

Management-Group:
Group    Role
------   ------------
qatest   tenant-admin
------   ------------

DDBoost:
Name   Pre-Comp (GiB)   Status   User    Tenant-Unit
----   --------------   ------   -----   -----------
su1               2.0   RW/Q     ddbu1   tu1
----   --------------   ------   -----   -----------
Q    : Quota Defined
RO   : Read Only
RW   : Read Write

Getting users with default-tenant-unit tu1
DD Boost user   Default tenant-unit
-------------   -------------------
ddbu1           tu1
-------------   -------------------

Mtrees:
Name             Pre-Comp (GiB)   Status   Tenant-Unit
--------------   --------------   ------   -----------
/data/col1/m1               0.0   RW/Q     tu1
/data/col1/su1              2.0   RW/Q     tu1
--------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

Quota:
Tenant-unit: tu1
Mtree            Pre-Comp (MiB)   Soft-Limit (MiB)   Hard-Limit(MiB)
--------------   --------------   ----------------   ----------------
/data/col1/m1                 0              71680             81920
/data/col1/su1             2048              30720             51200
--------------   --------------   ----------------   ----------------
```

```
Alerts:
Tenant-unit: "tu1"
Notification list "tu1_grp"
Members
------------------
tom.tenant@abc.com
------------------

No such active alerts.
```

2. Sur le système de remplacement, activez SMT si cette fonction n'est pas déjà activée.
3. Sur le système de remplacement, activez la licence DD Boost SMT si nécessaire.
4. Si DD Boost est configuré, attribuez chaque utilisateur figurant dans la section `DD Boost` de la sortie « smt tenant-unit show detailed » en tant qu'utilisateur de DD Boost.

   ```
   # ddboost user assign ddbu1
   ```

5. Si DD Boost est configuré, attribuez chaque utilisateur figurant dans la section `DD Boost` de la sortie `smt tenant-unit show detailed` à l'unité de tenant par défaut indiquée, le cas échéant, dans la sortie.

   ```
   # ddboost user option set ddbu1 default-tenant-unit tu1
   ```

6. Créez un nouveau groupe de notification d'alerte portant le même nom que le groupe de notification d'alerte figurant dans la section `Alerts` de la sortie `smt tenant-unit show detailed`.

   ```
   # alert notify-list create tu1_grp tenant-unit tu1
   ```

7. Attribuez chaque adresse e-mail du groupe de notification d'alerte figurant dans la section `Alerts` de la sortie `smt tenant-unit show detailed` au nouveau groupe de notification d'alerte.

   ```
   # alert notify-list add tu1_grp emails tom.tenant@abc.com
   ```

CHAPITRE 17

DD Secure Multitenancy

Ce chapitre traite des sujets suivants :

Tour d'horizon de Data Domain Secure Multitenancy

Data Domain *Secure Multitenancy (SMT)* fait référence à l'hébergement simultané d'une infrastructure IT par un département IT interne ou un fournisseur externe pour plusieurs clients/charges applicatives (entité/service/tenant).

SMT permet d'isoler en toute sécurité plusieurs utilisateurs et charges applicatives dans une infrastructure partagée, afin que les activités d'un tenant ne soient ni apparentes ni visibles pour les autres tenants.

Un *tenant* est un client (entité, service ou client) qui maintient une présence persistante dans un environnement hébergé.

Au sein d'une entreprise, un tenant peut être composé d'une ou de plusieurs entités ou d'un ou de plusieurs services sur un système Data Domain configuré et géré par le personnel IT.

- Dans le cas d'une entité, les services financiers et des ressources humaines d'une entreprise peuvent partager le même système Data Domain, mais chaque service n'aura pas connaissance de la présence de l'autre.
- Dans le cas d'un prestataire de services, celui-ci peut déployer un ou plusieurs systèmes Data Domain pour accueillir différents services de stockage de protection pour plusieurs clients finaux.

Ces deux exemples d'utilisation mettent l'accent sur la ségrégation des différentes données client sur le même système Data Domain physique.

Notions de base de l'architecture SMT

SMT (Secure Multitenancy) propose une approche simple pour configurer des tenants et des unités de tenant à l'aide de structures Mtree. La configuration SMT est effectuée à l'aide de DD Management Center et/ou de l'interface de ligne de commande de DD OS. Ce guide d'administration fournit les principes de SMT, ainsi que des instructions générales pour la ligne de commande.

L'architecture de base de la fonction SMT est la suivante.

- Un tenant est créé sur DD Management Center et/ou le système Data Domain.
- Une unité de tenant est créée sur un système Data Domain pour le tenant.
- Une ou plusieurs MTree sont créées en fonction des besoins de stockage des différents types de sauvegardes du tenant.
- Les structures Mtree qui viennent d'être créées sont ajoutées à l'unité de tenant.
- Les applications de sauvegarde sont configurées pour envoyer chaque sauvegarde configurée de leur structure MTree d'unité de tenant.

Remarque

Pour plus d'informations sur DD Management Center, consultez le *Guide d'utilisation de DD Management Center*. Pour pluq d'informations sur l'interface de ligne de commande de DD OS, consultez la *Référence des commandes DD OS*.

Terminologie utilisée dans un multitenancy sécurisé (SMT)

Comprendre la terminologie utilisée dans un SMT vous permettra de mieux comprendre cet environnement unique.

Structures MTree
Les structures *MTree* sont les partitions logiques du système de fichiers et offrent le plus haut degré de granularité de gestion. Les utilisateurs peuvent en effet exécuter des opérations sur une structure MTree sans affecter l'ensemble du système de fichiers. Des structures MTree sont attribuées à des unités tenant et contiennent des paramètres individualisés permettant de gérer et de surveiller le multitenancy sécurisé.

Multitenancy
Multi-Tenancy fait référence à l'hébergement d'une infrastructure IT par un département IT interne ou un service provider externe pour plusieurs clients/charges applicatives (entité/service/tenant) simultanément. Data Domain SMT active la *protection des données as-a-Service*.

Contrôle d'accès basé sur les rôles (RBAC)
Le *contrôle d'accès basé sur les rôles* offre plusieurs rôles avec différents niveaux de privilèges, qui se combinent pour fournir un isolement administratif sur un système Data Domain multitenant. (Ces rôles seront définis dans la section suivante.)

Unité de stockage
Une *unité de stockage* est une structure MTree configurée pour le protocole DD Boost. L'isolement des données est effectué par la création d'une unité de stockage et son attribution à un utilisateur DD Boost. Le protocole DD Boost ne permet d'accéder qu'aux unités de stockage attribuées aux utilisateurs DD Boost connectés au système Data Domain.

Tenant
Un *tenant* est un client (entité/service/client) qui maintient une présence persistante dans un environnement hébergé.

Tenants en libre service
Tenants en libre service est une méthode qui permet à un tenant de se connecter à un système Data Domain pour exécuter certains services de base (ajouter, modifier ou supprimer des utilisateurs locaux, des groupes NIS et/ou des groupes AD). Cette méthode réduit le goulot d'étranglement causé par le fait de toujours devoir passer par un administrateur pour ces tâches de base. Le tenant peut uniquement accéder aux unités de tenant qui lui ont été attribuées. Les utilisateurs tenants et les administrateurs tenants disposeront bien sûr de privilèges différents.

Unité de tenant
Une *unité de tenant* est la partition d'un système Data Domain qui sert d'unité d'isolement administratif entre les tenants. Les unités de tenant allouées à un tenant peuvent se trouver sur le même système Data Domain ou sur des systèmes différents, et sont sécurisées et logiquement isolées les unes des autres, ce qui assure la sécurité et l'isolement du chemin de contrôle lors de l'exécution simultanée de plusieurs tenants sur l'infrastructure partagée. Les unités de tenant peuvent contenir une ou plusieurs structures *MTree*, qui regroupent tous les éléments de configuration nécessaires à la configuration d'un multitenancy. Les utilisateurs, les groupes de gestion, les groupes de notification et d'autres éléments de configuration font partie d'une unité de tenant.

Isolement du chemin de contrôle et du réseau

L'isolement du chemin de contrôle est obtenu par la création de nouveaux rôles d'utilisateur de type *administrateur tenant* et *utilisateur tenant* pour une unité de tenant. L'*isolement du réseau* pour l'accès aux données et l'accès administratif s'effectue par l'association d'un ensemble fixe d'*adresses IP d'accès aux données* et d'*adresses IP de gestion* à une unité de tenant.

Les rôles *administrateur tenant* et *utilisateur tenant* sont limités en termes de périmètre et de capacité par rapport à des unités tenant spécifiques, et ne peuvent effectuer qu'un ensemble restreint d'opérations sur ces unités tenant. Pour s'assurer que le chemin de données est isolé et sécurisé de manière logique, l'administrateur configure une ou plusieurs structures MTree d'unité tenant pour chaque protocole dans un environnement SMT. Les protocoles pris en charge incluent DD Boost, NFS, CIFS et DD VTL. L'accès est strictement régulé par les mécanismes de contrôle d'accès natifs de chaque protocole.

Les sessions des tenants en libre-service (via ssh) peuvent être limitées à un ensemble fixe d'*adresses IP de gestion* sur un système DD. Les sessions d'accès administrateur (via ssh/http/https) peuvent également être restreintes à un ensemble fixe d'adresses IP de gestion sur des systèmes DD. Par défaut, toutefois, aucune adresse IP de gestion n'est associée à une unité tenant. Par conséquent, la seule restriction standard se fait via l'utilisation des rôles *administrateur tenant*et *utilisateur tenant*. Vous devez utiliser `smt tenant-unit management-ip` pour ajouter et gérer les adresses IP de gestion pour les unités tenant.

De même, l'accès aux données et les flux de données (vers et depuis les unités de tenant) peuvent être limités à un ensemble fixe d'*adresses IP d'accès aux données* locales ou distantes. L'utilisation d'adresses IP (d'accès aux données) allouées renforce la sécurité des protocoles DD Boost et NFS en ajoutant des contrôles de sécurité liés au SMT. Il est possible, par exemple, de restreindre la liste des unités de stockage renvoyée sur le protocole DD Boost RPC en fonction de celles qui appartiennent à l'unité de tenant grâce aux adresses IP d'accès aux données locales allouées. Pour NFS, l'accès et la visibilité des exportations peuvent être filtrés en fonction des adresses IP d'accès aux données locales configurées. Par exemple, le fait d'exécuter `showmount -e` à partir de l'adresse IP d'accès aux données locale d'une unité de tenant affiche uniquement les exportations NFS appartenant à cette unité de tenant.

Le *sysadmin* est tenu d'utiliser `smt tenant-unit data-ip` pour ajouter et gérer les adresses IP d'accès aux données pour les unités de tenant.

Remarque

Si vous essayez de monter une structure MTree dans un SMT à l'aide d'une adresse IP non-SMT, l'opération échouera.

Si plusieurs unités de tenant appartiennent au même tenant, elles peuvent partager une passerelle par défaut. Ce n'est pas le cas si elles appartiennent à différents tenants.

Plusieurs unités de tenant appartenant au même tenant peuvent partager une passerelle par défaut. Les unités de tenant qui appartiennent à différents tenants ne peuvent pas utiliser la même passerelle par défaut.

Présentation de RBAC dans SMT

Dans un multitenancy sécurisé (SMT), la possibilité d'effectuer une tâche dépend du rôle attribué à un utilisateur. DD Management Center utilise le contrôle d'accès basé sur les rôles (RBAC) pour contrôler ces autorisations.

Tous les utilisateurs DD Management Center peuvent :

- Afficher tous les tenants
- Créer, consulter, mettre à jour ou supprimer les unités tenant appartenant à n'importe quel tenant si l'utilisateur est un administrateur du système Data Domain hébergeant l'unité tenant

- Attribuer et retirer des unités tenant à un tenant et à partir de celui-ci, si l'utilisateur est administrateur du système Data Domain hébergeant l'unité tenant
- Afficher les unités tenant appartenant à n'importe quel tenant, si l'utilisateur dispose d'un rôle attribué sur le système Data Domain hébergeant l'unité tenant

L'exécution de tâches plus avancées dépend du rôle de l'utilisateur :

Rôle admin
Un utilisateur doté du rôle *admin* peut effectuer toutes les opérations d'administration sur un système Data Domain. Un *administrateur* peut également effectuer toutes les opérations d'administration SMT sur un système Data Domain, notamment la configuration de SMT, l'attribution des rôles d'utilisateur SMT, l'activation du mode libre-service pour les tenants, la création d'un tenant, etc. Dans un contexte SMT, l'*administrateur* est généralement appelé *owner*. Dans DD OS, ce rôle est appelé *sysadmin*.

Pour pouvoir modifier ou supprimer un tenant, vous devez à la fois être un *administrateur* DD Management Center et avoir le rôle *sysadmin* DD OS sur tous les systèmes Data Domain associés aux unités tenant de ce tenant. Si le tenant ne possède aucune unité tenant, vous pouvez disposer du rôle *administrateur* DD Management Center uniquement pour pouvoir modifier ou supprimer ce tenant.

Rôle limited-admin
Un utilisateur doté du rôle *limited-admin* peut effectuer toutes les opérations d'administration sur un système Data Domain en tant qu'*admin*. Toutefois, les utilisateurs ayant le rôle *limited-admin* ne peuvent pas supprimer ou détruire des structures MTree. Dans DD OS, il existe un équivalent du rôle *limited-admin*.

Rôle tenant-admin
Un utilisateur doté du rôle *tenant-admin* ne peut exécuter certaines tâches que lorsque le mode *libre-service pour les tenants* est activé sur l'unité tenant en question. Celui-ci est notamment chargé de la planification et de l'exécution d'une application de sauvegarde pour le tenant, et de la surveillance des ressources et des statistiques au sein de l'unité de tenant attribuée. L'utilisateur *tenant-admin* est en mesure d'afficher les journaux d'audit, mais le contrôle d'accès basé sur les rôles (RBAC) s'assure que seuls les journaux d'audit de l'unité de tenant (ou des unités de tenant) appartenant à l'utilisateur *tenant-admin* sont accessibles. En outre, les utilisateurs *tenant-admin* garantissent la séparation administrative lorsque le mode libre-service pour les tenants est activé. Dans un contexte SMT, le rôle *tenant-admin* est généralement appelé *backup admin* (administrateur de sauvegarde).

Rôle tenant-user
Un utilisateur doté du rôle *tenant-user* peut surveiller les performances et l'utilisation des composants SMT uniquement sur les unités tenant qui lui ont été allouées et uniquement lorsque le libre-service pour les tenants est activé. Il ne pourra pas, en revanche, afficher les journaux d'audit des unités de tenant qui lui sont allouées. En outre, les utilisateurs *tenant-users* peuvent exécuter les commandes `show` et `list`.

Rôle none
Un utilisateur ayant le rôle *none* ne peut effectuer aucune autre opération sur un système Data Domain que la modification de son mot de passe et l'accès aux données via DD Boost. Cependant, une fois la fonction SMT activée, l'*administrateur* peut choisir un utilisateur doté du rôle *none* dans le système Data Domain et lui attribuer un rôle *tenant-admin* ou *tenant-user* spécifique de SMT. Cet utilisateur pourra alors effectuer des opérations sur les objets de gestion du SMT.

Groupes de gestion
Les BSP (backup service providers) peuvent utiliser des *groupes de gestion* définis dans une instance AD (Active Directory) ou NIS (Network Information Service) unique

pour simplifier la gestion des rôles d'utilisateur sur les unités tenant. Chaque tenant BSP peut être une entreprise externe, distincte et peut utiliser un service de noms tel qu'AD ou NIS.

Grâce aux groupes de gestion SMT, les serveurs Active Directory et NIS sont installés et configurés par l'*administrateur*, de la même manière que les utilisateurs SMT locaux. L'*administrateur* peut demander au responsable AD ou NIS de créer et d'alimenter le groupe. L'*administrateur* attribue ensuite un rôle SMT à l'ensemble du groupe. N'importe quel utilisateur appartenant au groupe qui se connecte au système Data Domain est connecté avec le rôle affecté au groupe.

Lorsque les utilisateurs quittent ou rejoignent une société tenant, ils peuvent être supprimés ou ajoutés au groupe par le responsable AD ou NIS. Il n'est pas nécessaire de modifier la configuration RBAC sur un système Data Domain lorsque les utilisateurs qui appartiennent au groupe sont ajoutés ou supprimés.

Provisionnement d'une unité tenant

La procédure de provisionnement d'un multitenancy sécurisé (SMT) initial commence au démarrage de l'assistant de configuration. Au cours de la procédure, l'assistant crée et provisionne une nouvelle unité tenant d'après les exigences de configuration du tenant. Les informations sont saisies par l'administrateur lorsqu'il y est invité. Une fois la procédure terminée, l'administrateur passe aux tâches suivantes, en commençant par l'activation du mode libre-service pour les tenants. Après la configuration initiale, des étapes manuelles et des modifications de configuration peuvent être effectuées au besoin.

Procédure

1. Démarrez SMT.

   ```
   # smt enable SMT enabled.
   ```

2. Vérifiez que la fonction SMT est activée.

   ```
   # smt status SMT is enabled.
   ```

3. Démarrez l'assistant de configuration SMT.

   ```
   # smt tenant-unit setup No tenant-units.
   ```

4. Suivez les invites de configuration.

```
SMT TENANT-UNIT Configuration

  Configure SMT TENANT-UNIT at this time (yes|no) [no]: yes

  Do you want to create new tenant-unit (yes/no)? : yes

Tenant-unit Name
  Enter tenant-unit name to be created
  : SMT_5.7_tenant_unit
Invalid tenant-unit name.
  Enter tenant-unit name to be created
  : SMT_57_tenant_unit

Pending Tenant-unit Settings
Create Tenant-unit   SMT_57_tenant_unit

Do you want to save these settings (Save|Cancel|Retry): save
SMT Tenant-unit Name Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Configure SMT TENANT-UNIT MANAGEMENT-IP at this time (yes|no) [no]: yes

  Do you want to add a local management ip to this tenant-unit? (yes|no) [no]: yes
```

```
port  enabled  state  DHCP        IP address                netmask     type additional
                                                          /prefix length        setting
----- ------- ------- ---- -------------------------- -------------- ---- ----------
ethMa   yes   running  no  192.168.10.57              255.255.255.0   n/a
                           fe80::260:16ff:fe49:f4b0** /64
eth3a   yes   running ipv4 192.168.10.236*            255.255.255.0*  n/a
                           fe80::260:48ff:fe1c:60fc** /64
eth3b   yes   running  no  192.168.50.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1c:60fd** /64
eth4b   yes   running  no  192.168.60.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1f:5183** /64
----- ------- ------- ---- -------------------------- -------------- ---- ----------
* Value from DHCP
** auto_generated IPv6 address

Choose an ip from above table or enter a new ip address. New ip addresses will need
to be created manually.

Ip Address
  Enter the local management ip address to be added to this tenant-unit
  : 192.168.10.57

  Do you want to add a remote management ip to this tenant-unit? (yes|no) [no]:

Pending Management-ip Settings

Add Local Management-ip    192.168.10.57
  Do you want to save these settings (Save|Cancel|Retry): yes
  unrecognized input, expecting one of Save|Cancel|Retry

  Do you want to save these settings (Save|Cancel|Retry): save
  Local management access ip "192.168.10.57" added to tenant-unit "SMT_57_tenant_unit".

SMT Tenant-unit Management-IP Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Do you want to add another local management ip to this tenant-unit? (yes|no) [no]:

  Do you want to add another remote management ip to this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT DDBOOST Configuration
  Configure SMT TENANT-UNIT DDBOOST at this time (yes|no) [no]:

SMT TENANT-UNIT MTREE Configuration
  Configure SMT TENANT-UNIT MTREE at this time (yes|no) [no]: yes

Name                       Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------  --------------   ------   -----------
/data/col1/laptop_backup          4846.2   RO/RD     -
/data/col1/random                23469.9   RO/RD     -
/data/col1/software2              2003.7   RO/RD     -
/data/col1/tsm6                 763704.9   RO/RD     -
-------------------------  --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create a mtree for this tenant-unit now? (yes|no) [no]: yes

MTree Name
  Enter MTree name
```

```
  :  SMT_57_tenant_unit
Invalid mtree path name.
  Enter MTree name
  :
SMT_57_tenant_unit


Invalid mtree path name.
  Enter MTree name
  : /data/col1/SMT_57_tenant_unit

MTree Soft-Quota
  Enter the quota soft-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

MTree Hard-Quota
  Enter the quota hard-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

Pending MTree Settings
Create MTree        /data/col1/SMT_57_tenant_unit
MTree Soft Limit    none
MTree Hard Limit    none

  Do you want to save these settings (Save|Cancel|Retry): save
  MTree "/data/col1/SMT_57_tenant_unit" created successfully.
  MTree "/data/col1/SMT_57_tenant_unit" assigned to tenant-unit  "SMT_57_tenant_unit".

SMT Tenant-unit MTree Configurations saved.

SMT TENANT-UNIT MTREE Configuration

Name                        Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------   --------------   ------   -----------
/data/col1/laptop_backup           4846.2   RO/RD     -
/data/col1/random                 23469.9   RO/RD     -
/data/col1/software2               2003.7   RO/RD     -
/data/col1/tsm6                  763704.9   RO/RD     -
-------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign another MTree to this tenant-unit? (yes|no) [no]: yes

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create another mtree for this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT SELF-SERVICE Configuration

  Configure SMT TENANT-UNIT SELF-SERVICE at this time (yes|no) [no]: yes
  Self-service of this tenant-unit is disabled

  Do you want to enable self-service of this tenant-unit? (yes|no) [no]: yes

  Do you want to configure a management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure a management group for this tenant-unit (yes|no) [no]: yes

Management-Group Name
  Enter the group name to be assigned to this tenant-unit
  : SMT_57_tenant_unit_group

What role do you want to assign to this group  (tenant-user|tenant-admin) [tenant-user]:
```

```
tenant-admin

Management-Group Type
  What type do you want to assign to this group (nis|active-directory)?
  : nis

Pending Self-Service Settings
Enable Self-Service       SMT_57_tenant_unit
Assign Management-group   SMT_57_tenant_unit_group
Management-group role     tenant-admin
Management-group type     nis

  Do you want to save these settings (Save|Cancel|Retry): save
  Tenant self-service enabled for tenant-unit "SMT_57_tenant_unit"
  Management group "SMT_57_tenant_unit_group" with type "nis" is assigned to tenant-unit
  "SMT_57_tenant_unit" as "tenant-admin".

SMT Tenant-unit Self-Service Configurations saved.

SMT TENANT-UNIT SELF-SERVICE Configuration

  Do you want to configure another management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure another management group for this tenant-unit? (yes|no)
[no]:

SMT TENANT-UNIT ALERT Configuration

  Configure SMT TENANT-UNIT ALERT at this time (yes|no) [no]: yes
  No notification lists.

Alert Configuration

Alert Group Name
  Specify alert notify-list group name to be created
  : SMT_57_tenant_unit_notify

Alert email addresses
  Enter email address to receive alert for this tenant-unit
  : dd_proserv@emc.com

  Do you want to add more emails (yes/no)?
  : no

Pending Alert Settings
Create Notify-list group   SMT_57_tenant_unit_notify
Add emails                 dd_proserv@emc.com

  Do you want to save these settings (Save|Cancel|Retry): save
  Created notification list "SMT_57_tenant_unit_notify" for tenant "SMT_57_tenant_unit".
  Added emails to notification list "SMT_57_tenant_unit_notify".

SMT Tenant-unit Alert Configurations saved.

Configuration complete.
```

Activation du mode libre-service pour les tenants

Pour une séparation administrative des fonctions et une délégation des tâches administratives/de gestion afin d'implémenter le libre-service pour les tenants, lequel est requis pour l'isolement du chemin de contrôle, l'administrateur système peut activer ce mode sur une unité tenant, puis attribuer des utilisateurs pour gérer l'unité dans les rôles tenant-admin ou tenant-user. Ces rôles permettent aux utilisateurs autres que l'administrateur d'effectuer des tâches spécifiques sur l'unité tenant à laquelle ils sont attribués. Outre la séparation administrative, le libre-service pour les

tenants permet également d'alléger la charge de gestion du personnel du fournisseur de services et de l'équipe IT interne.

Procédure

1. Affichez l'état du mode libre-service sur une ou plusieurs unités tenant.

   ```
   # smt tenant-unit option show { tenant-unit | all }
   ```

2. Activez le mode libre-service pour les tenants sur l'unité tenant sélectionnée.

   ```
   # smt tenant-unit option set tenant-unit self-service { enabled
   | disabled }
   ```

Accès aux données par protocole

La sécurisation des chemins de données avec des contrôles d'accès spécifiques au protocole active la sécurité et l'isolement pour les unités tenant. Dans un environnement de multitenancy sécurisé (SMT), les commandes de gestion du protocole d'accès sont également optimisées avec un paramètre d'unité tenant afin de permettre un reporting consolidé.

Les systèmes DD prennent simultanément en charge plusieurs protocoles d'accès aux données, dont DD Boost, NFS, CIFS et DD VTL. Un système DD peut se présenter comme une interface spécifique d'une application telle qu'un serveur de fichiers offrant un accès NFS ou un accès CIFS sur Ethernet, un périphérique DD VTL ou un périphérique DD Boost.

Les mécanismes de contrôle d'accès natifs de chaque protocole pris en charge garantissent que les chemins de données de chaque tenant restent séparés et isolés. Les mécanismes de ce type incluent des listes de contrôle d'accès (ACL) pour CIFS, des exportations pour NFS, et un contrôle d'accès via les informations d'identification DD Boost et Multi-User Boost.

Unités de stockage et Multi-User DD Boost dans le Multitenancy sécurisé

Lors de l'utilisation de Multi-User DD Boost avec un multitenancy sécurisé (SMT), les autorisations utilisateur sont définies par le propriétaire de l'unité de stockage.

Le terme *Multi-User DD Boost* fait référence à l'utilisation de plusieurs informations d'identification d'utilisateur pour le contrôle d'accès DD Boost, où chaque utilisateur possède un nom d'utilisateur et un mot de passe distincts.

Une *unité de stockage* est une structure MTree configurée pour le protocole DD Boost. Un utilisateur peut être associé à, ou « détenir », une ou plusieurs unités de stockage. Les unités de stockage détenues par un utilisateur ne peuvent pas être détenues par un autre utilisateur. Par conséquent, seul l'utilisateur détenant l'unité de stockage peut y accéder pour tout type d'accès aux données, comme une sauvegarde ou une restauration. Le nombre de noms d'utilisateur DD Boost ne peut pas être supérieur au nombre maximal de structures MTree. (Voir le chapitre « Structures MTree » de cet ouvrage pour connaître le nombre maximal de structures MTree pour chaque modèle DD.) Le rôle *none* doit être attribué aux unités de stockage associées à SMT.

Chaque application de sauvegarde doit s'authentifier à l'aide de son nom d'utilisateur et de son mot de passe DD Boost Après l'authentification, DD Boost vérifie les informations d'identification authentifiées pour confirmer la propriété de l'unité de stockage. L'application de sauvegarde est autorisée à accéder à l'unité de stockage uniquement si les informations d'identification d'utilisateur présentées par l'application de sauvegarde correspondent aux noms d'utilisateur associés à l'unité de stockage. Si

les informations d'identification d'utilisateur et les noms d'utilisateur ne correspondent pas, la tâche échoue avec une erreur d'autorisation.

Configuration de l'accès pour CIFS

Le système CIFS (Common Internet File System) est un protocole de partage de fichiers qui permet l'accès aux fichiers à distance. Dans une configuration de multitenancy sécurisé (SMT), les sauvegardes et les restaurations nécessitent l'accès client aux partages CIFS résidant sur la structure MTree de l'unité tenant associée. L'isolement des données s'effectue à l'aide de partages CIFS et de listes de contrôle d'accès (ACL).

Procédure

1. Créez une structure MTree pour CIFS et attribuez-la à l'unité de tenant.

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. Définissez les quotas de capacité souple et strict pour la structure MTree.

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. Créez un partage CIFS pour *pathname* à partir de la structure MTree.

   ```
   # cifs share create share path pathname clients clients
   ```

Configuration de l'accès au système NFS

NFS est un protocole de partage de fichiers, basé sur UNIX qui permet l'accès aux fichiers à distance. Dans un environnement de multitenancy sécurisé (SMT), les sauvegardes et les restaurations nécessitent l'accès client aux exportations NFS résidant sur la structure MTree de l'unité tenant associée. L'isolement des données s'effectue à l'aide des exportations NFS et de l'isolement du réseau. NFS détermine si une structure MTree est associée à une unité tenant isolée du réseau. Si tel est le cas, NFS vérifie les propriétés de connexion associées à l'unité tenant. Les propriétés de connexion incluent l'adresse IP de destination et le nom d'hôte de l'interface ou du client.

Procédure

1. Créez une structure MTree pour NFS et attribuez-la à l'unité de tenant.

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. Définissez les quotas de capacité souple et strict pour la structure MTree.

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. Créez une exportation NFS en ajoutant un ou plusieurs clients à la structure MTree.

   ```
   # nfs add path client-list
   ```

Configuration de l'accès pour DD VTL

L'isolement des données d'un tenant DD VTL s'effectue à l'aide de groupes d'accès DD VTL qui créent un chemin d'accès virtuel entre un système hôte et une bibliothèque DD VTL. (La connexion Fibre Channel physique entre le système hôte et la bibliothèque DD VTL doit déjà exister.)

Placer les bandes dans la bibliothèque DD VTL leur permet d'être écrites dans l'application de sauvegarde du système hôte et d'être lues par celle-ci. Des bandes DD VTL sont créées dans un pool DD VTL, qui est une structure MTree. Étant donné

que les pools DD VTL sont des structures MTree, ils peuvent être attribués à des unités de tenant. Cette association permet la surveillance et le reporting SMT.

Par exemple, si un administrateur tenant se voit attribuer une unité de tenant contenant un pool DD VTL, il peut exécuter des commandes de structure MTree pour afficher des informations en lecture seule. Les commandes ne peuvent s'exécuter que sur le pool DD VTL attribué à l'unité de tenant.

Ces commandes sont les suivantes :

- `mtree list` pour afficher une liste de structures MTree dans l'unité de tenant
- `mtree show compression` pour afficher des statistiques sur la compression MTree
- `mtree show performance` pour afficher des statistiques sur les performances

Le résultat de la plupart des commandes `list` et `show` inclut des statistiques permettant aux fournisseurs de services de mesurer l'utilisation de l'espace et de calculer les frais de refacturation.

Les opérations de bibliothèque DD VTL ne sont pas affectées et continuent à fonctionner normalement.

Utilisation d'un serveur de bandes NDMP DD VTL

L'isolement des données d'un tenant DD VTL est également réalisé à l'aide de NDMP. DD OS met en œuvre un serveur de bandes NDMP (Network Data Management Protocol) qui permet aux systèmes NDMP d'envoyer des données de sauvegarde vers le système DD à l'aide d'une sauvegarde NDMP à trois serveurs.

Les données de sauvegarde sont écrites sur des bandes virtuelles (qui se trouvent dans un pool) par une bibliothèque DD VTL affectée au groupe DD VTL spécifique *TapeServer*.

Étant donné que les données de sauvegarde sont écrites sur les bandes au sein d'un pool, les informations de la section DD VTL relatives aux structures MTree s'appliquent également au serveur de bandes NDMP Data Domain.

Opérations de gestion des données

Les opérations de gestion d'un multitenancy sécurisé (SMT) incluent la surveillance d'unités tenant et d'autres objets, tels que les unités de stockage et les structures MTree. Pour certains objets SMT, une configuration ou une modification supplémentaire peut également être requise.

Collecte des statistiques de performances

Chaque structure MTree peut être évaluée en matière de performances ou d'« utilisation » de statistiques et d'autres informations en temps réel. Les taux historiques de consommation sont disponibles pour les unités de stockage DD Boost. Le résultat de la commande permet à l'administrateur tenant de recueillir des statistiques d'utilisation et les taux de compression d'une structure MTree associée à une unité tenant, ou de l'ensemble des structures MTree et des unités tenant associées. Le résultat peut être filtré pour afficher l'utilisation par intervalles, allant de quelques minutes à quelques mois. Les résultats sont transmis à l'administrateur, qui utilise les statistiques pour la refacturation. Une méthode similaire est utilisée pour recueillir les statistiques d'utilisation et les taux de compression des unités de stockage.

Procédure

1. Collectez les statistiques de performances en temps réel de la structure MTree.

   ```
   # mtree show stats
   ```

2. Collectez les statistiques de performances pour les structures MTree associées à une unité tenant.

   ```
   # mtree show performance
   ```

3. Collectez les statistiques de compression pour les structures MTree associées à une unité tenant.

   ```
   # mtree show compression
   ```

Modification des quotas

Pour répondre aux critères de qualité de service, l'administrateur système utilise des « taquets » DD OS pour ajuster les paramètres requis par la configuration de tenant. Par exemple, l'administrateur peut définir des limites de quota « souples » et « strictes » sur les unités de stockage DD Boost. Des limites de quota « souples » et « strictes » de flux ne peuvent être attribuées que sur des unités de stockage DD Boost attribuées à des unités tenant. Une fois que l'administrateur a défini des quotas, l'administrateur tenant peut surveiller une ou toutes les unités tenant afin de garantir qu'aucun objet ne dépasse les quotas qui lui ont été attribués et prive les autres des ressources du système.

Les quotas sont définis initialement sur invitation de l'assistant de configuration, mais il est possible de les ajuster ou de les modifier ultérieurement. L'exemple ci-dessous indique comment modifier les quotas pour DD Boost. (Vous pouvez également utiliser les commandes `quota capacity` et `quota streams` pour gérer la capacité et les limites, ainsi que les quotas de flux.)

Procédure

1. Pour modifier les limites de quota souples et strictes sur une unité de stockage DD Boost « su33 » :

   ```
   ddboost storage-unit modify su33 quota-soft-limit 10 Gib quota-hard-limit 20 Gib
   ```

2. Pour modifier les limites de quota souples et strictes de flux sur une unité de stockage DD Boost « su33 » :

   ```
   ddboost storage-unit modify su33 write-stream-soft-limit 20 read-stream-soft-limit 6 repl -stream-soft-limit 20 combined-stream-soft-limit 20
   ```

3. Pour signaler la taille physique d'une unité de stockage DD Boost « su33 » :

   ```
   ddboost storage-unit modify su33 report-physical-size 8 GiB
   ```

SMT et réplication

En cas de sinistre, les rôles d’utilisateur expliquent comment un utilisateur peut contribuer aux opérations de restauration des données. Plusieurs types de réplication sont disponibles dans une configuration SMT. (Reportez-vous au chapitre relatif à *DD Replicator* pour plus d’informations sur la manière d’effectuer la réplication.)

Voici quelques points à prendre en compte pour les rôles d’utilisateur :

- L’administrateur peut restaurer des structures MTree à partir d’une copie répliquée.

- L'administrateur tenant peut répliquer des structures MTree d'un système à un autre, à l'aide de la réplication de fichiers gérée par DD Boost.
- L'administrateur tenant peut restaurer des structures MTree à partir d'une copie répliquée, également à l'aide de la réplication de fichiers gérée par DD Boost.

Réplication de collection
Les réplications de collection copient les informations de configuration de l'unité tenant principale.

Réplication sécurisée via une connexion Internet publique
Pour vous protéger contre les attaques Man-in-the-middle (MITM) lors d'une réplication via une connexion Internet publique, l'authentification consiste à valider des informations liées au certificat SSL à la source et à la destination de la réplication.

Réplication d'une structure MTree (NFS/CIFS) à l'aide de la réplication de fichiers gérée par DD Boost
La réplication d'une structure MTree est prise en charge sur les structures MTree attribuées aux unités tenant, à l'aide de la réplication de fichiers gérée par DD Boost. Lors de la réplication d'une structure MTree, une structure MTree attribuée à une unité tenant sur un système peut être répliquée sur une structure MTree attribuée à une unité tenant sur un autre système. La réplication d'une structure MTree n'est pas autorisée entre deux tenants différents sur les deux systèmes DD. Lorsque le mode de sécurité est défini sur *stricte*, la réplication d'une structure MTree est autorisée uniquement lorsque les structures Mtree appartiennent aux mêmes tenants.

Pour garantir la compatibilité en amont, la réplication d'une structure MTree depuis une structure MTree attribuée à une unité tenant vers une structure MTree non attribuée est prise en charge, mais doit être configurée manuellement. La configuration manuelle garantit que la structure MTree cible est dotée des paramètres appropriés pour l'unité tenant. À l'inverse, la réplication d'une structure MTree depuis une structure MTree non attribuée vers une structure MTree attribuée à une unité tenant est également prise en charge.

Lorsque vous configurez la réplication d'une structure MTree compatible avec SMT, le *mode de sécurité* définit la quantité de vérification effectuée sur le tenant. Le mode *par défaut* vérifie que la source et la destination n'appartiennent pas à des tenants différents. Le mode *stricte* garantit que la source et la destination appartiennent au même tenant. Par conséquent, lorsque vous utilisez le mode stricte, vous devez créer un tenant sur la machine cible en utilisant le même UUID que l'UUID du tenant de la machine source qui est associée à la structure MTree en cours de réplication.

Réplication de fichiers gérée par DD Boost (également avec DD Boost AIR)
La réplication de fichiers gérée par DD Boost est prise en charge entre les unités de stockage, qu'une unité de stockage, ou les deux, soient attribuées ou non à des unités tenant.

Lors de la réplication de fichiers gérée par DD Boost, les unités de stockage ne sont pas répliquées dans la totalité. En revanche, certains fichiers d'une unité de stockage sont sélectionnés par l'application de sauvegarde pour la réplication. Les fichiers sélectionnés dans une unité de stockage et attribués à une unité tenant d'un système peuvent être répliqués sur une unité de stockage attribuée à une unité tenant d'un autre système.

Pour garantir la compatibilité en amont, les fichiers sélectionnés dans une unité de stockage attribuée à une unité tenant peuvent être répliqués vers une unité de stockage non attribuée. À l'inverse, les fichiers sélectionnés dans une unité de stockage non attribuée peuvent être répliqués vers une unité de stockage attribuée à une unité tenant.

La réplication de fichiers gérée par DD Boost peut également être utilisée lors de déploiements DD Boost AIR.

Contrôle de la réplication pour garantir la qualité de service
Il est possible de fixer une limite supérieure en matière de débit de réplication (`repl-in`) pour une structure MTree. Étant donné que les structures Mtree de chaque tenant sont attribuées à une unité de Tenant, l'utilisation des ressources de réplication de chaque tenant peut être plafonnée en appliquant cette limite. Le lien entre cette fonction et SMT tient au fait que la réplication de MTree est soumise à cette limite de débit.

Alertes de tenant SMT

Un système DD génère des *événements* lorsqu'il rencontre d'éventuels problèmes avec le matériel ou le logiciel. Lorsqu'un événement est généré, une notification d'*alerte* est immédiatement envoyée par e-mail aux membres figurant dans la liste de notification et à l'administrateur Data Domain.

Les alertes SMT sont spécifiques de chaque unité tenant et diffèrent des alertes système DD. Lorsque le mode libre-service pour les tenants est activé, l'administrateur tenant peut choisir de recevoir les alertes relatives aux divers objets système qui lui sont associés, ainsi que tous les événements critiques, tels qu'un arrêt inattendu du système. Un administrateur tenant peut uniquement afficher ou modifier les listes de notification auxquelles il est associé.

Vous trouverez ci-dessous un exemple d'alerte. Notez que les deux messages d'événement situés au bas de la notification sont propres à chaque environnement multitenant (indiqué par le terme « Tenant »). Pour obtenir la liste complète des alertes DD OS et SMT, consultez le document *Guide de référence rapide de la base de données MIB Data Domain* ou la base de données MIB SNMP.

```
EVT-ENVIRONMENT-00021 – Description: The system has been shutdown by
abnormal method; for example, not by one of the following: 1) Via
IPMI chassis control command 2) Via power button 3) Via OS shutdown.

Action: This alert is expected after loss of AC (main power) event.
If this shutdown is not expected and persists, contact your
contracted support provider or visit us online at https://
my.datadomain.com.

Tenant description: The system has experienced an unexpected power
loss and has restarted.

Tenant action: This alert is generated when the system restarts after
a power loss. If this alert repeats, contact your System
Administrator.
```

Gestion des snapshots

Un *snapshot* est une copie en lecture seule d'une structure MTree capturée à un point donné dans le temps. Un snapshot peut être utilisé pour de nombreuses situations, par exemple, en tant que point de restauration en cas de dysfonctionnement du système. L'utilisation de la commande `snapshot` nécessite le rôle admin ou tenant-admin.

Pour afficher les informations relatives aux snapshots d'une structure MTree ou d'une unité tenant :

```
# snapshot list mtree mtree-path | tenant-unit tenant-unit
```

Pour afficher le planning de snapshots d'une structure MTree ou d'une unité tenant :

```
# snapshot schedule show [name | mtrees mtree-listmtree-list | tenant-
unit tenant-unit]
```

Exécution d'une opération Fast Copy sur un système de fichiers

Une opération Fast Copy clone des fichiers et les arborescences d'un répertoire source vers un répertoire de destination sur un système DD. Une opération Fast Copy peut être effectuée dans des circonstances particulières dans le cas d'un multitenancy sécurisé (SMT).

Voici quelques éléments à prendre en compte lors de l'exécution d'une opération Fast Copy sur un système de fichiers activé avec le mode libre-service pour les tenants :

- Un administrateur tenant peut exécuter une opération Fast Copy sur des fichiers d'une unité tenant vers une autre, lorsque l'administrateur tenant est l'administrateur des deux unités tenant concernées, et que les deux unités tenant appartiennent au même tenant.
- Un administrateur tenant peut exécuter une opération Fast Copy sur des fichiers au sein de la même unité tenant.
- Un administrateur tenant peut exécuter une opération Fast Copy sur des fichiers au sein des unités tenant source et cible.

Pour exécuter une opération Fast Copy sur un système de fichiers :

```
# filesys fastcopy source <src> destination <dest>
```

CHAPITRE 18

Hiérarchisation du Cloud avec DD

Ce chapitre traite des sujets suivants :

Présentation de DD Cloud Tier

DD Cloud Tier est une fonction native de DD OS 6.0 (ou version ultérieure) prévue pour déplacer des données à partir du niveau actif vers un stockage en mode objet haute capacité et économique dans le Cloud public, privé ou hybride à des fins de rétention à long terme. DD Cloud Tier est parfaitement adapté au stockage à long terme des données rarement consultées, conservées à des fins de conformité, de réglementation et de gouvernance. Les données idéales pour DD Cloud Tier sont les données ayant dépassé les limites de la fenêtre de restauration normale.

DD Cloud Tier est géré à l'aide d'un seul espace de nommage Data Domain. Aucune passerelle Cloud séparée ou appliance virtuelle n'est nécessaire. Le déplacement des données est pris en charge par le framework de gestion des règles Data Domain natif. D'un point de vue conceptuel, le stockage sur le Cloud est considéré comme un niveau de stockage supplémentaire (niveau Cloud DD) rattaché au système Data Domain. Les données sont transférées d'un niveau à un autre en fonction des besoins. Les métadonnées du système de fichiers associées aux données stockées dans le Cloud sont conservées dans un stockage local, et également mises en miroir sur le Cloud. Les métadonnées qui résident dans le stockage local facilitent les opérations telles que la déduplication, le nettoyage, les procédures Fast Copy et la réplication. Ce stockage local est divisé en buckets autonomes, appelés unités de cloud, pour faciliter la gestion.

Plates-formes prises en charge

La hiérarchisation du Cloud est permise sur les plates-formes physiques disposant des ressources requises (mémoire, CPU et connectivité de stockage) pour accepter un autre niveau de stockage.

DD Cloud Tierest pris en charge sur ces systèmes :

Tableau 196 Configurations de DD Cloud Tier prises en charge

Modèle	Mémoire	Capacité cloud	Nombre requis de modules d'E/S SAS	Types de tiroirs de disques pris en charge pour le stockage des métadonnées	Nombre requis de tiroirs ES30 ou de piles de disques DS60	Capacité requise pour le stockage des métadonnées
DD990	256 Go	1 140 To	4	ES30	4	60 disques durs de 3 To = 180 To
DD3300 (4 To)	16 Go	8 To	s.o.	s.o.	s.o.	1 disque virtuel de 1 To = 1 To
DD3300 8 To	48 Go	16 To	s.o.	s.o.	s.o.	2 disques virtuels de 1 To = 2 To
DD3300 (16 To)	48 Go	32 To	s.o.	s.o.	s.o.	2 disques virtuels de 1 To = 2 To

Tableau 196 Configurations de DD Cloud Tier prises en charge (suite)

Modèle	Mémoire	Capacité cloud	Nombre requis de modules d'E/S SAS	Types de tiroirs de disques pris en charge pour le stockage des métadonnées	Nombre requis de tiroirs ES30 ou de piles de disques DS60	Capacité requise pour le stockage des métadonnées
DD3300 (32 To)	64 Go	64 To	s.o.	s.o.	s.o.	4 disques virtuels de 1 To = 4 To
DD4200	128 Go	378 To	3	DS60 ou ES30	2	30 disques durs de 3 To = 90 To
DD4500	192 Go	570 To	3	DS60 ou ES30	2	30 disques durs de 4 To = 120 To
DD6800	192 Go	576 To	2	DS60 ou ES30	2	30 disques durs de 4 To = 120 To
DD7200	256 Go	856 To	4	DS60 ou ES30	4	60 disques durs de 4 To = 240 To
DD9300	384 Go	1400 To	2	DS60 ou ES30	4	60 disques durs de 4 To = 240 To
DD9500	512 Go	1728 To	4	DS60 ou ES30	5	75 disques durs de 4 To = 300 To
DD9800	768 Go	2016 To	4	DS60 ou ES30	5	75 disques durs de 4 To = 300 To
DD VE (16 To)	32 Go	32 To	s.o.	s.o.	s.o.	1 disque virtuel de 500 Go = 500 Go[a]
DD VE (64 To)	60 Go	128 To	s.o.	s.o.	s.o.	1 disque virtuel de 500 Go = 500 Go[a]
DD VE (96 To)	80 Go	192 To	s.o.	s.o.	s.o.	1 disque virtuel de 500 Go = 500 Go[a]

a. La taille minimale des métadonnées est une limite stricte. Data Domain recommande aux utilisateurs de commencer avec un disque de 1 To pour le stockage des métadonnées, puis d'utiliser des incréments de 1 To. Le *Guide d'installation et d'administration de Data Domain Virtual Edition* fournit plus de détails sur l'utilisation de DD Cloud Tier avec DD VE.

Remarque

DD Cloud Tier est pris en charge dans un environnement Data Domain haute disponibilité (HA). Les deux nœuds doivent exécuter DD OS 6.0 (ou une version ultérieure) et doivent être à haute disponibilité.

Remarque

DD Cloud Tier n'est pas pris en charge sur les systèmes non répertoriés et n'est pas non plus pris en charge sur les systèmes sur lesquels la fonction Extended Retention est activée ou configurée avec la réplication de collection.

Remarque

La fonction de hiérarchisation du Cloud peut consommer toute la bande passante disponible dans une liaison WAN partagée, en particulier dans une configuration de faible bande passante (1 Gbit/s), et cela peut avoir un impact sur les autres applications partageant la liaison WAN. S'il existe des applications partagées sur le WAN, le recours à la qualité de service ou à toute autre règle de restriction de réseau est recommandé pour éviter la congestion du réseau et garantir des performances prévisibles au fil du temps.
Si la bande passante est limitée, le taux de transfert de données sera lent et vous ne serez pas en mesure de déplacer autant de données vers le cloud. Il est préférable d'utiliser une liaison dédiée pour les données qui migrent vers le niveau de stockage Cloud.

Remarque

N'envoyez pas le trafic via les contrôleurs d'interface du réseau de gestion intégrés (interfaces ethMx).

Performances DD Cloud Tier

Le système Data Domain utilise des optimisations internes pour maximiser les performances de DD Cloud Tier.

Initialisation du cloud

Le moteur de migration en cours vers le Cloud est archivé et un moteur efficace optimisé pour la déduplication est utilisé pour identifier et migrer uniquement les segments uniques vers le Cloud. L'efficacité de ce moteur de migration basé sur les fichiers est élevée lors de la migration de données de génération supérieure vers la hiérarchisation sur le Cloud, qui a déjà quelques données à dédupliquer. Cependant, lorsque la hiérarchisation sur le Cloud est vide ou presque vide, il n'existe aucune donnée à dédupliquer. Il existe une surcharge de cycles de calcul qui sont investis dans la déduplication. Avec la migration basée sur l'ensemencement le filtrage de déduplication est maintenu sur le niveau actif lui-même et seules les données uniques sont migrées en masse vers la hiérarchisation sur le Cloud. Lors de l'ensemencement du Cloud, le moteur migre le contenu du stockage local vers le stockage Cloud sans le traiter pour déduplication. Lorsque l'ensemencement du Cloud est active, les fichiers marqués pour la migration vers le stockage Cloud ne sont pas nettoyés (c'est-à-dire que l'espace n'est pas libéré) dans le cadre du nettoyage du système de fichiers du niveau actif tant que la migration de tous les fichiers identifiés par l'ensemencement n'est pas terminée. Le stockage de niveau actif doit être dimensionné pour tenir compte de cela dans les environnements où de grandes quantités de données sont

migrées vers le stockage cloud. Si le stockage DD Cloud Tier est plein à moins de cinq pour cent, et a une utilisation de données de 30 TiB (ou plus) après compression, comme vu dans la commande show space, le système Data Domain utilise automatiquement l'ensemencement du cloud lors de la migration des données vers le stockage cloud.

Après avoir consommé cinq pour cent de la capacité DD Cloud Tier, l'initialisation du cloud se désactive automatiquement et les données sont traitées pour la déduplication avant la migration vers le stockage cloud.

Voici d'autres points à prendre en compte lors de l'utilisation de la migration par ensemencement :

- La migration n'est prise en charge en mode Seeding que lorsque :
  - La taille utilisée par la post-compression du niveau actif est de 30 TiB ou plus, comme indiqué dans le résultat de la commande filesys show space.
  - Le niveau actif est plein à moins de 70 %, lorsque la migration commence comme indiqué dans le résultat de la commande filesys show space.

  Remarque

  Si l'utilisation du niveau actif pendant le cycle de migration en cours en mode Seeding dépasse 90 %, la migration est interrompue et la migration reprend en mode normal de copie des fichiers.
- La migration en mode ensemencement est automatiquement suspendue par le nettoyage sur le niveau actif, pendant toute la durée du nettoyage sur ce niveau. Une fois le nettoyage terminé, l'ensemencement reprend automatiquement et redémarre la migration vers le Cloud.
- La migration en mode ensemencement est automatiquement suspendue si l'événement UNAVAIL est reçu sur l'unité Cloud (l'unité Cloud est signalée comme « déconnectée ») vers laquelle elle migre et ne reprend que lorsque l'unité Cloud est disponible et signalée comme active.
- Le nettoyage ne peut pas être démarré sur une unité Cloud qui est la destination d'une opération de migration en cours en mode ensemencement.

  Remarque

  Dans un système à deux unités Cloud, pour forcer le nettoyage d'une deuxième unité Cloud qui n'est pas ensemencée, suspendre la migration en mode ensemencement à l'aide de la CLI data-movement suspend, puis exécuter la CLI cloud clean start sur la deuxième unité Cloud.
- La vérification probabiliste des fichiers dans le Cloud, même si elle est programmée selon la règle par défaut, est ignorée et ne se produit pas pour une unité Cloud, sur laquelle la migration est en cours en mode d'ensemencement.
- Si le nettoyage est déjà en cours sur la hiérarchisation sur le Cloud ou le niveau actif et que le mouvement des données planifié commence en mode d'ensemencement, le mouvement des données est automatiquement suspendu pendant la durée de l'activité de nettoyage.
- La migration en mode ensemencement ignore la migration des fichiers, depuis des structures MTree, qui sont des destinations de réplication, même si les fichiers sont éligibles à la migration. Les fichiers de ces structures MTree qui sont des structures MTree de destination de réplication (RO/RD), sont migrés à l'aide d'un moteur de copie de fichiers, une fois que la migration en mode ensemencement de toutes les structures MTree éligibles est terminée.

- Si la fonction de rapport sur la capacité physique est activée et planifiée, la migration en mode ensemencement suspend la fonction de rapport sur la capacité, pendant toute la durée de la migration basée sur l'ensemencement.
- La migration en mode ensemencement est uniquement prise en charge sur tous les systèmes Data Domain du Cloud et les configurations qui ont plus de 80 Go de RAM. La migration basée sur l'ensemencement est désactivée par défaut pour les DD VE.

Objets volumineux
DD Cloud Tier utilise des tailles d'objets de 1 Mo ou 4 Mo (selon le fournisseur de stockage cloud) pour réduire le temps système des métadonnées et diminuer le nombre d'objets à migrer vers le stockage cloud.

Configuration de la hiérarchisation sur le Cloud

Pour configurer la hiérarchisation sur le Cloud, ajoutez la licence et les châssis, définissez une phrase de passe système, et créez un système de fichiers prenant en charge le déplacement des données vers le Cloud.

- Vous avez besoin d'une licence de capacité du Cloud pour définir les niveaux de hiérarchisation sur le Cloud.
- Pour acquérir la licence en question, reportez-vous aux *Notes de mises à jour de Data Domain Operating System* pour obtenir les informations les plus récentes au sujet des fonctionnalités des produits, des mises à jour logicielles, des guides de compatibilité logicielle et vous renseigner sur les produits, licences et services Data Domain.
- Pour définir une phrase de passe système, utilisez l'onglet **Administration** > **Access** > **Administrator Access**.
  Si aucune phrase de passe n'est définie, le bouton **Set Passphrase** apparaît dans la zone Passphrase. Si une phrase de passe est définie, le bouton **Change Passphrase** apparaît pour que vous puissiez changer de phrase de passe, au besoin.
- Pour configurer le stockage, utilisez l'onglet **Hardware** > **Storage**.
- Pour créer un système de fichiers, utilisez l'Assistant de création de système de fichiers.

Configuration du stockage pour DD Cloud Tier

Le stockage Cloud Tier sur le système DD est requis pour les unités de Cloud : il contient les métadonnées des fichiers, tandis que les données résident dans le Cloud.

Procédure

1. Sélectionnez **Hardware** > **Storage**.
2. Dans l'onglet Overview, développez **Cloud Tier**.
3. Cliquez sur **Configure**.

   La boîte de dialogue Configure Cloud Tier s'affiche.
4. Cochez la case à cocher correspondant au tiroir à ajouter à partir de la section Addable Storage.

⚠ ATTENTION

Les systèmes DD3300 nécessitent l'utilisation de périphériques de stockage de 1 To pour le stockage des métadonnées DD Cloud Tier.

5. Cliquez sur le bouton **Add to Tier**.
6. Cliquez sur **Save** pour ajouter le stockage.
7. Sélectionnez **Data Management** > **File System** et activez la fonction de hiérarchisation du Cloud (Cloud Tier).
8. Cliquez sur **Disable** en bas de l'écran pour désactiver le système de fichiers.
9. Cliquez sur **OK**.
10. Une fois le système de fichiers désactivé, sélectionnez **Enable Cloud Tier**.

    Pour activer la hiérarchisation du Cloud, vous devez respecter les conditions de stockage pour la capacité sous licence. Configurer le niveau Cloud du système de fichiers. Cliquez sur **Next**.
    Un système de fichiers Cloud nécessite une zone de stockage locale réservée à la copie locale des métadonnées du Cloud.

11. Sélectionnez **Enable file system**.

    Le niveau Cloud est activé avec le stockage indiqué.

12. Cliquez sur **OK**.

    Vous devez créer les unités de Cloud séparément, une fois le système de fichiers généré.

Estimation de l'espace nettoyable

L'outil d'estimation de l'espace nettoyable (Cleanable Space Estimation) évalue la quantité d'espace qui peut être libérée sur un niveau actif si `data-movement` déplace les fichiers éligibles dans le Cloud et que le GC nettoie le système de fichiers.

Cet outil peut fonctionner avec ou sans licence cloud/archive présente.

Lorsqu'il n'existe aucune licence Cloud/active, indiquer le seuil d'ancienneté qui doit être utilisé pour évaluer l'espace nettoyable total sur le niveau actif. S'il existe à la fois un seuil d'ancienneté et une règle définis sur les structures MTree, la préférence est donnée au seuil d'ancienneté fourni par l'utilisateur.

Il existe trois workflows :

- Un système ayant des règles de migration vers le Cloud définies : les fichiers sont identifiés comme « éligibles » sur la base de la règle définie sur les structures MTree respectives et l'espace nettoyable est calculé.
- Un système ayant des règles de migration vers le Cloud définies, mais avec un seuil d'ancienneté par utilisateur : Les fichiers sont identifiés en fonction du seuil d'ancienneté spécifié par l'utilisateur, ce qui supplante les règles du système.
- Un système sans Cloud : obligation pour l'utilisateur de fournir un seuil d'ancienneté censé être utilisé pour déterminer l'espace nettoyable total.

Quelques points supplémentaires à considérer :

- Le mouvement des données ne peut pas se dérouler en parallèle avec le contrôle de l'éligibilité du mouvement des données et inversement.
- Le nettoyage sur le niveau actif ne peut pas être lancé si le contrôle d'éligibilité est en cours et inversement.

- Le nettoyage sur le niveau Cloud ne peut pas être lancé si le contrôle d'éligibilité est en cours et inversement.
- Si l'événement UNAVAIL est reçu, il ne doit pas avoir d'incidence sur le fonctionnement du contrôle d'éligibilité.
- Si le système de fichiers s'arrête ou subit une panne, la vérification d'éligibilité s'arrête et ne reprend pas automatiquement une fois que le système de fichiers revient à la normale.

Remarque

Il n'existe aucune disposition permettant d'initier une vérification d'éligibilité à partir de la GUI Data Domain System Manager.

Configuration des unités de Cloud

Le niveau Cloud ne peut pas contenir plus de deux unités de Cloud, et comme chaque unité de Cloud est mappée à un fournisseur de Cloud, il est possible d'avoir plusieurs fournisseurs de Cloud par système Data Domain. Le système Data Domain doit être connecté au Cloud et disposer d'un compte auprès d'un fournisseur de Cloud pris en charge.

La configuration des unités de cloud inclut les étapes suivantes :

- Configuration du réseau, y compris des paramètres de proxy et du pare-feu
- Importation de certificats AC
- Ajout d'unités de cloud

Paramètres de pare-feu et de proxy

Ports de pare-feu réseau

- Le port 443 (HTTPS) et/ou le port 80 (HTTP) doivent être ouverts aux réseaux du fournisseur de Cloud à la fois pour l'adresse IP du point de terminaison et pour l'adresse IP d'authentification pour mettre en place un trafic bidirectionnel. Dand le cas d'Amazon S3, par exemple, il faut veiller à ce que le port 80 et/ou le port 443 soit/soient déverrouillé(s) et configuré(s) pour autoriser le trafic IP bidirectionnel pour les adresses s3-ap-southeast-1.amazonaws.com et s3.amazonaws.com.

  Remarque

  Plusieurs fournisseurs de Cloud public utilisent des plages d'adresses IP pour leurs adresses de point de terminaison et d'authentification. Dans ce cas, les plages IP utilisées par le fournisseur doivent être débloquées pour s'adapter aux éventuels changements d'adresses IP.

- Le pare-feu doit être configuré pour accepter les plages d'adresses IP d'authentification d'accès et de destination du fournisseur de Cloud à distance.
- Pour le Cloud privé ECS, les plages d'adresses IP d'authentification ECS locale et de stockage sur le Web (S3), tout comme les ports 9020 (HTTP) et 9021 (HTTPS), doivent être autorisés à transiter par les pare-feu locaux.

Remarque

Il faut également configurer les règles relatives aux ports et aux adresses IP du répartiteur de charge du Cloud privé ECS.

Paramètres proxy

Si des paramètres de proxy ont pour effet de refuser les données au-dessus d'une certaine taille, il convient de redéfinir ces paramètres pour autoriser les objets jusqu'à 4,5 Mo.

Si le trafic du client est acheminé via un proxy, le certificat auto-signé/signé par une autorité de certification (AC) doit être importé. Voir « Importation de certificats AC » pour plus d'informations.

Suites de chiffrement OpenSSL

- Chiffrements : ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384
- Version de TLS : 1.2

Remarque

Une communication par défaut est établie avec tous les fournisseurs de Cloud avec un chiffrement puissant.

Protocoles pris en charge

- HTTP
- HTTPS

Remarque

Une communication par défaut est établie avec tous les fournisseurs de Cloud public via HTTP sécurisé (HTTPS), mais vous pouvez remplacer le paramètre par défaut afin d'utiliser le protocole HTTP.

Importation de certificats AC

Avant de pouvoir ajouter des unités de Cloud pour Elastic Cloud Storage (ECS), Virtustream Storage Cloud, Alibaba Cloud, Amazon Web Services S3 (AWS) et Azure cloud, vous devez importer les certificats AC.

Avant de commencer

Pour les fournisseurs de cloud public AWS, Virtustream et Azure, les certificats d'autorité de certification (AC) racine peuvent être téléchargés depuis https://www.digicert.com/digicert-root-certificates.htm.

- Pour un fournisseur de Cloud AWS, téléchargez le certificat Baltimore CyberTrust Root.
- S'il s'agit d'un fournisseur de Cloud Virtustream, téléchargez le certificat DigiCert High Assurance EV Root CA.
- Pour ECS, l'autorité de certification racine varie en fonction du client. L'implémentation du stockage cloud sur ECS nécessite un équilibreur de charge. Si un point de terminaison HTTPS est utilisé en tant que point d'accès dans la configuration, veillez à importer le certificat racine d'une autorité de certification (CA). Pour plus d'informations, contactez votre fournisseur de répartiteur de charge.

- Pour un fournisseur de Cloud Azure, téléchargez le certificat Baltimore CyberTrust Root.
- Pour un fournisseur S3 Flexible, importez le certificat d'autorité de certification racine. Pour plus d'informations, contactez votre fournisseur de S3 Flexible.

Si votre certificat téléchargé possède une extension .crt, il devra probablement être converti en un certificat codé au format PEM. Dans ce cas, utilisez OpenSSL pour convertir le fichier du format .crt au format .pem (par exemple, `openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out BaltimoreCyberTrustRoot.pem`).

Pour Alibaba :

1. Téléchargez le certificat racine R1 de GlobalSign à l'adresse suivante : https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates.
2. Convertissez le certificat téléchargé au format d'encodage PEM. La commande OpenSSL pour cette conversion est : `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Importez le certificat dans le système Data Domain.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Dans la barre d'outils, cliquez sur **Manage Certificates**.

   La boîte de dialogue Manage Certificates for Cloud s'affiche.
3. Cliquez sur **Add**.
4. Sélectionnez l'une des options suivantes :
   - **I want to upload the certificate as a .pem file.**
     Accédez au fichier de certificat et sélectionnez-le.
   - **I want to copy and paste the certificate text.**
     - Copiez le contenu du fichier .pem dans votre mémoire tampon de copie.
     - Collez le contenu de la mémoire tampon dans la boîte de dialogue.
5. Cliquez sur **Add**.

Ajout d'une unité de Cloud pour Elastic Cloud Storage (ECS)

Un système Data Domain ou une instance DD VE nécessite une synchronisation quasi identique de l'heure avec le système ECS pour pouvoir configurer une unité de cloud Data Domain. La configuration du protocole NTP sur le système Data Domain ou l'instance DD VE permet au système ECS de résoudre ce problème.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur **Ajouter**.

   La boîte de dialogue Add Cloud Unit s'affiche.
3. Saisissez un nom pour cette unité de Cloud. Seuls les caractères alphanumériques sont autorisés.

   Les champs restants dans la boîte de dialogue Add Cloud Unit concernent le compte du fournisseur de Cloud.

4. Pour **Cloud provider**, sélectionnez **EMC Elastic Cloud Storage (ECS)** dans la liste déroulante.
5. Saisissez la **clé d'accès** du fournisseur sous forme de texte du mot de passe.
6. Saisissez la **clé secrète** du fournisseur sous forme de texte du mot de passe.
7. Saisissez le **point de terminaison** du fournisseur au format suivant : `http://<ip/hostname>:<port>`. Si vous utilisez un point d'accès sécurisé, choisissez `https` à la place.

   Remarque

   L'implémentation du stockage cloud sur ECS nécessite un équilibreur de charge.

   Par défaut, ECS exécute le protocole S3 sur le port 9020 pour HTTP et sur le port 9021 pour HTTPS. Avec un répartiteur de charge, ces ports sont parfois remappés respectivement à 80 pour HTTP et 443 pour HTTPS. Consultez votre administrateur réseau pour connaître les ports appropriés.
8. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.

   Saisissez le nom d'hôte du serveur proxy, le port, l'utilisateur et le mot de passe.

   Remarque

   Il existe une étape optionnelle pour exécuter l'outil de vérification du fournisseur Cloud avant d'ajouter l'unité Cloud. Cet outil effectue des tests de pré-vérification pour s'assurer que toutes les exigences sont satisfaites avant d'ajouter l'unité Cloud réelle.
9. Cliquez sur **Add**.

   La fenêtre principale du système de fichiers affiche désormais les informations récapitulatives de la nouvelle unité de Cloud ainsi qu'une commande d'activation et de désactivation de l'unité de Cloud.

Ajout d'une unité de Cloud pour Virtustream

Virtustream propose un éventail de classes de stockage. La *Matrice de compatibilité des fournisseurs Cloud*, disponible sur http://compatibilityguide.emc.com:8080/CompGuideApp/ fournit des informations à jour sur les classes de stockage prises en charge.

Les points de terminaison suivants sont utilisés par le fournisseur de Cloud Virtustream, en fonction de la classe de stockage et de la région. N'oubliez pas que le DNS est en mesure de résoudre ces noms d'hôte avant de configurer les unités de Cloud.

- s-us.objectstorage.io
- s-eu.objectstorage.io
- s-eu-west-1.objectstorage.io
- s-eu-west-2.objectstorage.io
- s-us-central-1.objectstorage.io

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur **Ajouter**.

   La boîte de dialogue Add Cloud Unit s'affiche.
3. Saisissez un nom pour cette unité de Cloud. Seuls les caractères alphanumériques sont autorisés.

   Les champs restants dans la boîte de dialogue Add Cloud Unit concernent le compte du fournisseur de Cloud.
4. Pour **Cloud provider**, sélectionnez **Virtustream Storage Cloud** dans la liste déroulante.
5. Sélectionnez la classe de stockage dans la liste déroulante.
6. Sélectionnez la région appropriée correspondant au type de compte dans la liste déroulante.
7. Saisissez la **clé d'accès** du fournisseur sous forme de texte du mot de passe.
8. Saisissez la **clé secrète** du fournisseur sous forme de texte du mot de passe.
9. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.

   Saisissez le nom d'hôte du serveur proxy, le port, l'utilisateur et le mot de passe.

   Remarque

   Il existe une étape optionnelle pour exécuter l'outil de vérification du fournisseur Cloud avant d'ajouter l'unité Cloud. Cet outil effectue des tests de pré-vérification pour s'assurer que toutes les exigences sont satisfaites avant d'ajouter l'unité Cloud réelle.
10. Cliquez sur **Save**.

    La fenêtre principale du système de fichiers affiche désormais les informations récapitulatives de la nouvelle unité de Cloud ainsi qu'une commande d'activation et de désactivation de l'unité de Cloud.

Ajout d'une unité Cloud pour Azure

Les régions sont configurées au niveau du bucket plutôt qu'au niveau de l'objet. Par conséquent, tous les objets contenus dans un bucket sont stockés dans la même région. Une région est spécifiée lors de la création d'un bucket et ne peut pas être modifiée une fois qu'elle a été créée.

Tableau 197 Régions Alibaba

Régions	Emplacement	Nom de la région
Régions de la Chine continentale	Chine Est 1 (Hangzhou)	oss-cn-hangzhou
	Chine Est 2 (Shanghai)	oss-cn-shanghai
	Chine du Nord 1 (Qingdao)	oss-cn-qingdao
	Chine du Nord 2 (Beijing)	oss-cn-beijing

Tableau 197 Régions Alibaba (suite)

Régions	Emplacement	Nom de la région
	Chine du Nord 3 (zhangjiakou)	oss-cn-zhangjiakou
	Chine du Nord 5 (Huhehaote)	oss-cn-huhehaote
	Chine du Sud 1 (Shenzhen)	oss-cn-shenzhen
Régions internationales	Hong-Kong	oss-cn-hongkong
	Ouest des États-Unis 1 (Silicon Valley)	oss-us-west-1
	Est des États-Unis 1 (Virginie)	oss-us-east-1
	Asie Pacifique SE 1 (Singapour)	oss-ap-southeast-1
	Asie Pacifique SE 2 (Sydney)	oss-ap-southeast-2
	Asie Pacifique SE 3 (Kuala Lumpur)	oss-ap-southeast-3
	Asie Pacifique SE 5 (Jakarta)	oss-ap-southeast-5
	Asie Pacifique NE 1 (Tokyo)	oss-ap-northeast-1
	Asie Pacifique SOU 1 (Mumbaï)	oss-ap-south-1
	Europe centrale 1 (Francfort)	oss-eu-central-1
	Moyen-Orient 1 (Dubaï)	oss-me-east-1

Les informations d'identification de l'utilisateur Alibaba Cloud doivent l'autoriser à créer et supprimer des buckets et à ajouter, modifier et supprimer des fichiers au sein des buckets qu'il crée. AliyunOSSFullAccess est préférable, mais voici les exigences minimales :

- ListBuckets
- GetBucket
- PutBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur **Ajouter**.

   La boîte de dialogue Add Cloud Unit s'affiche.
3. Saisissez un nom pour cette unité de Cloud. Seuls les caractères alphanumériques sont autorisés.

   Les champs restants dans la boîte de dialogue **Add Cloud Unit** concernent le compte du fournisseur de Cloud.

4. Pour **Cloud provider**, sélectionnez **Alibaba Cloud** dans la liste déroulante.
5. Sélectionnez **Standard** ou **IA** à partir de la liste déroulante **Storage class**.
6. Sélectionnez la région dans la liste déroulante **Storage region**.
7. Saisissez la **clé d'accès** du fournisseur sous forme de texte du mot de passe.
8. Saisissez la **clé secrète** du fournisseur sous forme de texte du mot de passe.
9. Assurez-vous que le port 443 (HTTPS) n'est pas bloqué dans les pare-feu. La communication avec le fournisseur Cloud Alibaba se fait sur le port 443.
10. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.

    Saisissez le nom d'hôte du serveur proxy, le port, l'utilisateur et le mot de passe.

    Remarque

    Il existe une étape optionnelle pour exécuter l'outil de vérification du fournisseur Cloud avant d'ajouter l'unité Cloud. Cet outil effectue des tests de pré-vérification pour s'assurer que toutes les exigences sont satisfaites avant d'ajouter l'unité Cloud réelle.

11. Cliquez sur **Add**.

    La fenêtre principale du système de fichiers affiche désormais les informations récapitulatives de la nouvelle unité de Cloud ainsi qu'une commande d'activation et de désactivation de l'unité de Cloud.

Ajout d'une unité de Cloud pour Amazon Web Services S3

AWS propose un éventail de classes de stockage. La *Matrice de compatibilité des fournisseurs Cloud*, disponible sur http://compatibilityguide.emc.com:8080/CompGuideApp/ fournit des informations à jour sur les classes de stockage prises en charge.

Pour une sécurité optimale, la fonction de hiérarchisation sur le Cloud utilise Signature Version 4 pour toutes les demandes AWS. La signature de type Signature Version 4 est activée par défaut.

Les points de terminaison suivants sont utilisés par le fournisseur de Cloud AWS, en fonction de la classe de stockage et de la région. N'oubliez pas que le DNS est en mesure de résoudre ces noms d'hôte avant de configurer les unités de Cloud.

- s3.amazonaws.com
- s3-us-west-1.amazonaws.com
- s3-us-west-2.amazonaws.com
- s3-eu-west-1.amazonaws.com
- s3-ap-northeast-1.amazonaws.com
- s3-ap-southeast-1.amazonaws.com
- s3-ap-southeast-2.amazonaws.com
- s3-sa-east-1.amazonaws.com
- ap-south-1
- ap-northeast-2
- eu-central-1

Remarque

La région de Chine n'est pas prise en charge.

Remarque

Les informations d'identification de l'utilisateur AWS doivent l'autoriser à créer et supprimer des buckets et à ajouter, modifier et supprimer des fichiers au sein des buckets qu'il crée. S3FullAccess est préférable, mais voici les exigences minimales :

- CreateBucket
- ListBucket
- DeleteBucket
- ListAllMyBuckets
- GetObject
- PutObject
- DeleteObject

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur **Ajouter**.

   La boîte de dialogue Add Cloud Unit s'affiche.
3. Saisissez un nom pour cette unité de Cloud. Seuls les caractères alphanumériques sont autorisés.

   Les champs restants dans la boîte de dialogue Add Cloud Unit concernent le compte du fournisseur de Cloud.
4. Pour **Cloud provider**, sélectionnez **Amazon Web Services S3** dans la liste déroulante.
5. Sélectionnez la classe de stockage dans la liste déroulante.
6. Sélectionnez la **région de stockage** appropriée dans la liste déroulante.
7. Saisissez la **clé d'accès** du fournisseur sous forme de texte du mot de passe.
8. Saisissez la **clé secrète** du fournisseur sous forme de texte du mot de passe.
9. Assurez-vous que le port 443 (HTTPS) n'est pas bloqué dans les pare-feu. La communication avec le fournisseur de Cloud AWS s'effectue via le port 443.
10. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.

    Saisissez le nom d'hôte du serveur proxy, le port, l'utilisateur et le mot de passe.

    Remarque

    Il existe une étape optionnelle pour exécuter l'outil de vérification du fournisseur Cloud avant d'ajouter l'unité Cloud. Cet outil effectue des tests de pré-vérification pour s'assurer que toutes les exigences sont satisfaites avant d'ajouter l'unité Cloud réelle.
11. Cliquez sur **Add.**.

La fenêtre principale du système de fichiers affiche désormais les informations récapitulatives de la nouvelle unité de Cloud ainsi qu'une commande d'activation et de désactivation de l'unité de Cloud.

Ajout d'une unité de Cloud pour Azure

Microsoft Azure propose un éventail de types de compte de stockage. La *Matrice de compatibilité des fournisseurs Cloud*, disponible sur http://compatibilityguide.emc.com:8080/CompGuideApp/ fournit des informations à jour sur les classes de stockage prises en charge.

Les points de terminaison suivants sont utilisés par le fournisseur de Cloud Azure, en fonction de la classe de stockage et de la région. N'oubliez pas que le DNS est en mesure de résoudre ces noms d'hôte avant de configurer les unités de Cloud.

- *Nom du compte*. blob.core.windows.net

Le nom du compte est obtenu à partir de la console du fournisseur de cloud Azure.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur **Ajouter**.

   La boîte de dialogue Add Cloud Unit s'affiche.
3. Saisissez un nom pour cette unité de Cloud. Seuls les caractères alphanumériques sont autorisés.

   Les champs restants dans la boîte de dialogue Add Cloud Unit concernent le compte du fournisseur de Cloud.
4. Pour **Cloud provider**, sélectionnez **Microsoft Azure Storage** dans la liste déroulante.
5. Pour **Account Type**, sélectionnez **Government** ou **Public**.
6. Sélectionnez la classe de stockage dans la liste déroulante.
7. Saisissez le nom du compte du fournisseur dans le champ **Account name**.
8. Saisissez la **clé primaire** du fournisseur sous forme de texte du mot de passe.
9. Saisissez la **clé secondaire** du fournisseur sous forme de texte du mot de passe.
10. Assurez-vous que le port 443 (HTTPS) n'est pas bloqué dans les pare-feu. La communication avec le fournisseur de Cloud Azure s'effectue via le port 443.
11. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.

    Saisissez le nom d'hôte du serveur proxy, le port, l'utilisateur et le mot de passe.

    Remarque

    Il existe une étape optionnelle pour exécuter l'outil de vérification du fournisseur Cloud avant d'ajouter l'unité Cloud. Cet outil effectue des tests de pré-vérification pour s'assurer que toutes les exigences sont satisfaites avant d'ajouter l'unité Cloud réelle.
12. Cliquez sur **Add**.

La fenêtre principale du système de fichiers affiche désormais les informations récapitulatives de la nouvelle unité de Cloud ainsi qu'une commande d'activation et de désactivation de l'unité de Cloud.

Ajout d'une unité Cloud pour Google Cloud Provider

Les tableaux suivants répertorient les emplacements du stockage Cloud disponible pour le stockage des données.

Tableau 198 Emplacements multirégionaux

Nom multi-régional	Description multi-régionale
Asie	Datacenters en Asie
US	Datacenters aux États-Unis
UE	Datacenters dans l'Union européenne

Tableau 199 Emplacements régionaux

Emplacements régionaux	Emplacement	Nom de la région
Amérique du Nord	northamerica-northeast1	Montréal
	us-central1	Iowa
	us-east1	Caroline du Sud
	us-east4	Virginie du Nord
	us-west1	Oregon
	us-west2	Los Angeles
Amérique du Sud	southamerica-east1	São Paulo
Europe	europe-north1	Finlande
	europe-west1	Belgique
	europe-west2	Londres
	europe-west3	Francfort
	europe-west4	Pays-Bas
Asie	asia-east1	Taïwan
	asia-northeast1	Tokyo
	asia-south1	Bombay
	asia-southeast1	Singapour
Australie	australia-southeast1	Sydney

Les informations d'identification de l'utilisateur Google Cloud Provider doivent l'autoriser à créer et supprimer des buckets et à ajouter, modifier et supprimer des fichiers au sein des buckets qu'il crée. La configuration minimale requise est la suivante.

- ListBucket
- PutBucket

- GetBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

Remarque

DD Cloud Tier prend uniquement en charge Nearline et est sélectionné automatiquement lors de l'installation.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur **Ajouter**.

   La boîte de dialogue Add Cloud Unit s'affiche.
3. Saisissez un nom pour cette unité de Cloud. Seuls les caractères alphanumériques sont autorisés.

   Les champs restants dans la boîte de dialogue **Add Cloud Unit** concernent le compte du fournisseur de Cloud.
4. Pour **Cloud provider**, sélectionnez **Google Cloud Storage** dans la liste déroulante.
5. Saisissez la **clé d'accès** du fournisseur sous forme de texte du mot de passe.
6. Saisissez la **clé secrète** du fournisseur sous forme de texte du mot de passe.
7. Le champ **Storage class** est défini sur **Nearline** par défaut.

   Si un emplacement multirégional est sélectionné (Asie, UE ou États-Unis), la classe de stockage et la contrainte de localisation sont Nearline Multi-regional. Tous les autres emplacements régionaux ont la classe de stockage définie sur Nearline Regional.
8. Sélectionnez la **région**.
9. Assurez-vous que le port 443 (HTTPS) n'est pas bloqué dans les pare-feu. La communication avec Google Cloud Provider se fait sur le port 443.
10. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.

    Saisissez le nom d'hôte du serveur proxy, le port, l'utilisateur et le mot de passe.

    Remarque

    Il existe une étape optionnelle pour exécuter l'outil de vérification du fournisseur Cloud avant d'ajouter l'unité Cloud. Cet outil effectue des tests de pré-vérification pour s'assurer que toutes les exigences sont satisfaites avant d'ajouter l'unité Cloud réelle.
11. Cliquez sur **Add**.

    La fenêtre principale du système de fichiers affiche désormais les informations récapitulatives de la nouvelle unité de Cloud ainsi qu'une commande d'activation et de désactivation de l'unité de Cloud.

Ajout d'une unité de cloud d'un fournisseur S3 Flexible

La fonction Cloud Tier prend en charge les autres fournisseurs de cloud S3 qualifiés via une option de configuration des fournisseurs S3 Flexible.

L'option du fournisseur S3 Flexible prend en charge les classes de stockage standard et à accès peu fréquent standard. Les points de terminaison varient en fonction du fournisseur cloud, de la classe de stockage et de la région. N'oubliez pas que le DNS est en mesure de résoudre ces noms d'hôte avant de configurer les unités de Cloud.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur **Ajouter**.

   La boîte de dialogue Add Cloud Unit s'affiche.
3. Saisissez un nom pour cette unité de Cloud. Seuls les caractères alphanumériques sont autorisés.

   Les champs restants dans la boîte de dialogue Add Cloud Unit concernent le compte du fournisseur de Cloud.
4. Pour **Cloud provider**, sélectionnez **Flexible Cloud Tier Provider Framework for S3** dans la liste déroulante.
5. Saisissez la **clé d'accès** du fournisseur sous forme de texte du mot de passe.
6. Saisissez la **clé secrète** du fournisseur sous forme de texte du mot de passe.
7. Spécifiez les informations appropriées pour **Storage region**.
8. Saisissez le **point de terminaison** du fournisseur au format suivant : `http://<ip/hostname>:<port>`. Si vous utilisez un point d'accès sécurisé, choisissez `https` à la place.
9. Sélectionnez la classe de stockage appropriée dans la liste déroulante du champ **Storage class**.
10. Assurez-vous que le port 443 (HTTPS) n'est pas bloqué dans les pare-feu. La communication avec le fournisseur de cloud S3 s'effectue via le port 443.
11. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.

    Saisissez le nom d'hôte du serveur proxy, le port, l'utilisateur et le mot de passe.

    Remarque

    Il existe une étape optionnelle pour exécuter l'outil de vérification du fournisseur Cloud avant d'ajouter l'unité Cloud. Cet outil effectue des tests de pré-vérification pour s'assurer que toutes les exigences sont satisfaites avant d'ajouter l'unité Cloud réelle.
12. Cliquez sur **Add**.

    La fenêtre principale du système de fichiers affiche désormais les informations récapitulatives de la nouvelle unité de Cloud ainsi qu'une commande d'activation et de désactivation de l'unité de Cloud.

Modification d'une unité de Cloud ou d'un profil de Cloud

Modifiez les informations d'identification d'unité de Cloud (nom du fournisseur S3 Flexible) ou d'un profil de Cloud.

Modification des informations d'identification des unités de Cloud

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur l'icône en forme de crayon correspondant à l'unité de Cloud dont vous souhaitez modifier les informations d'identification.

   La boîte de dialogue Modify Cloud Unit s'affiche.
3. Pour **Account name**, saisissez le nom du nouveau compte..
4. Pour **Access key**, saisissez la nouvelle clé d'accès du fournisseur sous forme de texte de mot de passe.

   Remarque

   La modification de la clé d'accès n'est pas prise en charge pour les environnements ECS.
5. Pour **Secret key**, saisissez la nouvelle clé secrète du fournisseur sous forme de texte de mot de passe.
6. Pour **Primary key**, saisissez la nouvelle clé principale du fournisseur sous forme de texte de mot de passe.

   Remarque

   La modification de la clé principale n'est prise en charge que pour les environnements Azure.
7. Si un serveur proxy HTTP est nécessaire pour contourner un pare-feu pour ce fournisseur, cliquez sur **Configure** pour **HTTP Proxy Server**.
8. Cliquez sur **OK**.

Modification du nom d'un fournisseur S3 Flexible

Procédure

1. Sélectionnez **Data Management** > **File System** > **Cloud Units**.
2. Cliquez sur l'icône en forme de crayon correspondant à l'unité de Cloud SS3 Flexible dont vous souhaitez modifier le nom.

   La boîte de dialogue Modify Cloud Unit s'affiche.
3. Pour **S3 Provider Name**, saisissez le nom du nouveau fournisseur.
4. Cliquez sur **OK**.

Utilisation de la CLI pour modifier un profil de cloud

Procédure

1. Exécutez la commande `cloud profile modify` pour modifier les détails d'un profil de Cloud. Le système vous demande de modifier les détails du profil de Cloud.

   Pour les profils Virtustream, AWS S3 ou Azure, exécutez cette commande pour ajouter une classe de stockage à un profil de Cloud existant.

   Les détails du profil qui peuvent être modifiés dépendent du fournisseur de cloud :

   - Alibaba Cloud prend en charge la modification de la clé d'accès et de la clé secrète.
   - AWS S3 prend en charge la modification de la clé d'accès et de la clé secrète.
   - Azure prend en charge la modification de la clé d'accès, de la clé secrète et de la clé principale.
   - ECS prend en charge la modification de la clé secrète.
   - Virtustream prend en charge la modification de la clé d'accès et de la clé secrète.
   - S3 Flexible prend en charge la modification de la clé d'accès, de la clé secrète et du nom du fournisseur.

Suppression d'une unité de Cloud

Cette opération entraîne la perte de toutes les données de l'unité de cloud sélectionnée pour la suppression. Veillez à supprimer tous les fichiers avant de supprimer les unités de cloud.

Avant de commencer

- Vérifiez si le déplacement des données vers le cloud est en cours d'exécution (commande CLI : data-movement status). S'il est en cours d'exécution, arrêtez le déplacement des données à l'aide de la commande CLI « data-movement stop ».
- Vérifiez si le nettoyage du cloud est en cours d'exécution pour cette unité de cloud (commande CLI : cloud clean status). S'il est en cours d'exécution, arrêtez le nettoyage du cloud à l'aide de la commande CLI « cloud clean ».
- Vérifiez si une règle de déplacement des données est configurée pour cette unité de cloud (commande CLI : data-movement policy show). Si une règle est configurée, supprimez cette règle à l'aide de la commande CLI « data-movement policy reset ».

Procédure

1. Utilisez la commande CLI suivante pour identifier les fichiers dans l'unité de cloud.

   ```
   # filesys report generate file-location
   ```

2. Supprimez les fichiers qui sont dans l'unité de cloud à supprimer.
3. Utilisez la commande CLI suivante pour exécuter le nettoyage du cloud.

   ```
   # cloud clean start unit-name
   ```

Attendez la fin du nettoyage pour terminer. Le nettoyage peut prendre un certain temps en fonction de la quantité de données présente dans l'unité de cloud.

4. Désactivez le système de fichiers.
5. Utilisez la commande CLI suivante pour supprimer l'unité de cloud.

   ```
   # cloud unit del unit-name
   ```

   En interne, cette opération marque l'unité de cloud comme étant DELETE_PENDING.
6. Utilisez la commande CLI suivante pour vérifier que l'unité de cloud est à l'état DELETE_PENDING.

   ```
   # cloud unit list
   ```

7. Activez le système de fichiers.

   Le système de fichiers lance la procédure en arrière-plan afin de supprimer tous les objets restants dans les compartiments du cloud pour cette unité de cloud et de supprimer les compartiments. Ce processus peut prendre un certain temps, selon le nombre d'objets restants au sein de ces compartiments. Jusqu'à ce que le nettoyage de compartiment soit terminé, cette unité de cloud continue d'utiliser un emplacement sur le système Data Domain, ce qui peut empêcher la création d'une nouvelle unité de cloud si les deux emplacements sont occupés.
8. Vérifiez périodiquement l'état à l'aide de cette commande CLI :

   ```
   # cloud unit list
   ```

   L'état reste DELETE_PENDING tandis que le nettoyage en arrière-plan est en cours d'exécution.
9. Vérifiez à partir du portail S3 du fournisseur de cloud que tous les compartiments correspondants ont été supprimés et que l'espace associé a été libéré.
10. Si nécessaire, reconfigurez les règles de déplacement des données pour les structures MTrees concernées et redémarrez le déplacement des données.

Résultats

Si vous rencontrez des difficultés pour effectuer cette procédure, contactez le support technique.

Déplacement de données

Les données sont déplacées du niveau actif au niveau Cloud, comme spécifié par votre propre règle de déplacement des données. La règle est définie par structure MTree. Le déplacement des données peut être démarré manuellement ou déclenché automatiquement à l'aide d'un planning.

Ajout de règles de déplacement de données à des structures MTree

Un fichier est déplacé du niveau actif au niveau Cloud en fonction de la date de sa dernière modification. Pour préserver l'intégrité des données, l'ensemble du fichier est déplacé à ce stade. La *règle de déplacement des données* définit le seuil d'âge des fichiers, la tranche d'âge et la destination.

Remarque

Une règle de déplacement des données ne peut pas être configurée pour la structure MTree /backup.

Procédure

1. Sélectionnez **Data Management** > **MTree**.
2. Dans le volet supérieur, sélectionnez la structure MTree à laquelle vous souhaitez ajouter une règle de déplacement des données.
3. Cliquez sur l'onglet **Summary**.
4. Sous **Data Movement Policy**, cliquez sur **Add**.
5. Pour **File Age in Days**, définissez la limite d'âge des fichiers (**Older than**) et éventuellement la tranche d'âge (**Younger than**).

   Remarque

   Le nombre minimal de jours pour **Older than** est 14. Pour les applications de sauvegarde non intégrées, il n'est pas possible d'accéder directement aux fichiers déplacés vers le niveau Cloud. Pour y accéder, vous devez les renvoyer vers le niveau actif. Par conséquent, choisissez la valeur de seuil d'âge avec discernement pour éviter, dans la mesure du possible, d'avoir à accéder à un fichier déplacé vers le niveau Cloud.

6. Pour **Destination**, spécifiez l'unité de Cloud de destination.
7. Cliquez sur **Ajouter**.

Déplacement manuel des données

Vous pouvez démarrer et arrêter le déplacement des données de façon manuelle. Cela permet de déplacer les fichiers des structures MTree disposant d'une règle de déplacement des données valide.

Procédure

1. Sélectionnez **Data Management** > **File System**.
2. Au bas de la page, cliquez sur **Show Status of File System Services**.

   Les éléments d'état suivants s'affichent :

   - File System
   - Mesure de la capacité physique
   - Déplacement de données
   - Nettoyage du niveau actif

3. Pour **Data Movement**, cliquez sur **Start**.

Déplacement automatique des données

Vous pouvez déplacer des données de façon automatique, par le biais d'un planning et d'une régulation. Les plannings peuvent être quotidiens, hebdomadaires ou mensuels.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Settings**.

2. Cliquez sur l'onglet **Data Movement** :
3. Définissez la régulation et le planning.

Remarque

La régulation permet d'ajuster les ressources pour les processus internes de Data Domain ; elle n'affecte pas la bande passante réseau.

Remarque

Toute unité de Cloud non accessible pendant le déplacement des données du niveau Cloud sera ignorée. Le déplacement des données sur l'unité de Cloud en question aura lieu lors de l'exécution suivante, à condition que l'unité de Cloud devienne disponible. Le planning de déplacement des données détermine l'intervalle entre deux exécutions. Si l'unité de Cloud devient disponible et que vous ne pouvez pas attendre la prochaine exécution planifiée, vous pouvez démarrer le déplacement des données de façon manuelle.

Rappel d'un fichier à partir du niveau cloud

Pour les applications de sauvegarde non intégrées, vous devez rappeler les données vers le niveau actif avant de pouvoir restaurer les données. Les administrateurs de sauvegarde doivent déclencher un rappel ou les applications de sauvegarde doivent effectuer un rappel avant de procéder à la restauration des sauvegardes basées sur le Cloud. Une fois qu'un fichier est rappelé, son âge est réinitialisé et repart à 0. L'éligibilité du fichier tient compte de la stratégie définie pour l'âge. Un fichier peut être rappelé uniquement sur la même structure MTree. Les applications intégrées peuvent restaurer un fichier directement.

Remarque

Dans un contexte de réplication de MTree, le fichier est en lecture seule sur la structure MTree de destination.

Remarque

Si un fichier réside uniquement dans un snapshot, il ne peut pas être rappelé directement. Pour rappeler un fichier dans un snapshot, utilisez fastcopy pour recopier le fichier à partir du snapshot vers la structure MTree active, puis rappelez le fichier à partir du cloud. Un fichier peut uniquement être rappelé à partir du cloud vers une structure MTree active.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Summary**.
2. Exécutez l'une des opérations suivantes :
   - Dans la section Cloud Tier du panneau Space Usage, cliquez sur **Recall**.
   - Développez le volet File System Status au bas de l'écran et cliquez sur **Recall**.

Remarque

Le lien **Recall** est disponible uniquement si une unité de cloud est créée et si elle possède des données.

3. Dans la boîte de dialogue Recall File from Cloud, saisissez exactement le nom de fichier (sans caractères génériques) et le chemin d'accès complet du fichier à rappeler, par exemple : `/data/col1/mt11/file1.txt`. Cliquez sur **Recall**.
4. Pour vérifier l'état de la procédure de rappel, effectuez l'une des opérations suivantes :
   - Dans la section Cloud Tier du panneau Space Usage, cliquez sur **Details**.
   - Développez le volet File System Status au bas de l'écran et cliquez sur **Details**.

   La boîte de dialogue Cloud File Recall Details s'affiche, indiquant le chemin d'accès, le fournisseur de cloud, la progression du rappel et la quantité de données transférées. Si des erreurs irrécupérables surviennent lors de la procédure de rappel, un message d'erreur s'affiche. Placez le curseur sur le message d'erreur pour afficher une info-bulle contenant plus de détails et décrivant les actions correctives possibles.

Résultats

Une fois que le fichier a été rappelé dans le niveau actif, vous pouvez restaurer les données.

Remarque

Pour les applications de sauvegarde non intégrées, une fois qu'un fichier a été rappelé du niveau cloud au niveau actif, 14 jours au moins doivent s'écouler avant que le fichier devienne éligible pour le déplacement des données. Au terme des 14 jours, un déplacement normal des données sera effectué pour le fichier. Le fichier doit maintenant attendre le seuil ou la tranche d'ancienneté pour revenir dans le Cloud, car cette fois-ci le ptime sera examiné plutôt que le mtime. Cette restriction ne s'applique pas aux applications intégrées.

Remarque

Pour le déplacement des données, les applications non intégrées configurent une règle de déplacement des données basée sur l'âge sur le système Data Domain pour spécifier les fichiers à migrer vers le niveau de cloud, et cette règle s'applique de façon uniforme à tous les fichiers d'une structure MTree. Les applications intégrées utilisent une règle de déplacement de données gérée par l'application, ce qui vous permet d'identifier les fichiers spécifiques à migrer vers le niveau de stockage cloud.

Utilisation de la CLI pour rappeler un fichier à partir du niveau de stockage cloud

Pour les applications de sauvegarde non intégrées, vous devez rappeler les données vers le niveau actif avant de pouvoir restaurer les données. Les administrateurs de sauvegarde doivent déclencher un rappel ou les applications de sauvegarde doivent effectuer un rappel avant de procéder à la restauration des sauvegardes basées sur le Cloud. Une fois qu'un fichier est rappelé, son âge est réinitialisé et repart à 0. L'éligibilité du fichier tiendra compte de la stratégie définie pour l'âge. Un fichier peut

être rappelé uniquement sur la structure MTree source. Les applications intégrées peuvent rappeler un fichier directement.

Remarque

Si un fichier réside uniquement dans un snapshot, il ne peut pas être rappelé directement. Pour rappeler un fichier dans un snapshot, utilisez fastcopy pour recopier le fichier à partir du snapshot vers la structure MTree active, puis rappelez le fichier à partir du cloud. Un fichier peut uniquement être rappelé à partir du cloud vers une structure MTree active.

Procédure

1. Vérifiez l'emplacement du fichier à l'aide de :
   `filesys report generate file-location [path {<path-name> | all}] [output-file <filename>]`

   Le chemin d'accès peut être un fichier ou un répertoire ; s'il s'agit d'un répertoire, tous les fichiers du répertoire sont répertoriés.

   ```
   Filename                    Location
   --------                    --------
   /data/col1/mt11/file1.txt   Cloud Unit 1
   ```

2. Rappelez les fichiers à l'aide de :
   `data-movement recall path <path-name>`

   Cette commande est asynchrone. Elle lance la procédure de rappel.

   ```
   data-movement recall path /data/col1/mt11/file1.txt
   Recall started for "/data/col1/mt11/file1.txt".
   ```

3. Surveillez l'état du rappel à l'aide de
   `data-movement status [path {pathname | all | [queued] [running] [completed] [failed]} | to-tier cloud | all]`

   ```
   data-movement status path /data/col1/mt11/file1.txt
   Data-movement recall:
   ---------------------
   Data-movement for "/data/col1/mt11/file1.txt": phase 2 of 3
   (Verifying)
   80% complete; time: phase  XX:XX:XX total  XX:XX:XX
   Copied (post-comp): XX XX, (pre-comp) XX XX
   ```

   Si l'état indique que la procédure de rappel n'est pas en cours d'exécution pour un chemin donné, cela signifie que le rappel est terminé ou a échoué.

4. Confirmez l'emplacement du fichier à l'aide de :
   `filesys report generate file-location [path {<path-name> | all}] [output-file <filename>]`

   ```
   Filename                    Location
   --------                    --------
   /data/col1/mt11/file1.txt   Active
   ```

Résultats

Une fois que le fichier a été rappelé dans le niveau actif, vous pouvez restaurer les données.

Remarque

Pour les applications de sauvegarde non intégrées, une fois qu'un fichier a été rappelé du niveau cloud au niveau actif, 14 jours au moins doivent s'écouler avant que le fichier devienne éligible pour le déplacement des données. Au terme des 14 jours, un déplacement normal des données sera effectué pour le fichier. Cette restriction ne s'applique pas aux applications intégrées.

Remarque

Pour le déplacement des données, les applications non intégrées configurent une règle de déplacement des données basée sur l'âge sur le système Data Domain pour spécifier les fichiers à migrer vers le niveau de cloud, et cette règle s'applique de façon uniforme à tous les fichiers d'une structure MTree. Les applications intégrées utilisent une règle de déplacement de données gérée par l'application, ce qui vous permet d'identifier les fichiers spécifiques à migrer vers le niveau de stockage cloud.

Restauration directe à partir du niveau cloud

La restauration directe permet aux applications non intégrées de lire les fichiers directement à partir du niveau cloud sans passer par le niveau actif.

Voici les principaux éléments à prendre en compte lorsque vous choisissez d'utiliser la restauration directe :

- La restauration directe ne nécessite pas une application intégrée et est transparente pour les applications non intégrées.
- La lecture à partir du niveau cloud ne nécessite pas d'effectuer en premier une copie dans le niveau actif.
- Des histogrammes et des statistiques sont disponibles pour le suivi des lectures directes à partir du niveau cloud.
- La restauration directe est uniquement prise en charge pour les fournisseurs cloud ECS.
- Les applications connaissent une latence au niveau du cloud.
- La lecture directe à partir du niveau cloud ne bénéficie pas d'une bande passante optimisée.
- La restauration directe prend en charge un petit nombre de tâches.

La restauration directe est utile avec des applications non intégrées qui n'ont pas besoin du niveau cloud et qui n'auront pas à restaurer des fichiers cloud fréquemment.

Utilisation de l'interface de ligne de commande (CLI) pour configurer DD Cloud Tier

Vous pouvez utiliser l'interface de ligne de commande (CLI) pour configurer DD Cloud Tier.

Procédure

1. Configurez le stockage à la fois pour le niveau actif et pour le niveau Cloud. Il faut, au préalable, que les licences de capacité appropriées pour le niveau actif et le niveau Cloud soient installées.
   a. Assurez-vous que les licences pour les fonctions CLOUDTIER-CAPACITY et CAPACITY-ACTIVE sont installées. Pour vérifier la licence ELMS :

```
# elicense show
```

Si la licence n'est pas installée, utilisez la commande `elicense update` pour installer la licence. Saisissez la commande et collez le contenu du fichier de licence après cette invite. Assurez-vous qu'un retour chariot a bien été inséré juste après le contenu collé, puis appuyez sur **Contrôle-D** pour enregistrer. Lorsque vous êtes invité à remplacer les licences, répondez yes (oui) pour appliquer et afficher les licences.

```
# elicense update
Enter the content of license file and then press Control-D,
or press Control-C to cancel.
```

b. Affichez le stockage disponible :

```
# storage show all# disk show state
```

c. Ajoutez le stockage au niveau actif :

```
# storage add enclosures <enclosure no> tier active
```

d. Ajoutez le stockage au niveau Cloud :

```
# storage add enclosures <enclosure no> tier cloud
```

2. Installez les certificats.

   Pour pouvoir créer un profil de Cloud, vous devez installer les certificats associés. Pour plus d'informations, reportez-vous à la section Importation des certificats à la page 633.

   Pour les fournisseurs de Cloud public AWS, Virtustream et Azure, les certificats d'autorité de certification (AC) racine peuvent être téléchargés depuis https://www.digicert.com/digicert-root-certificates.htm.

   - Pour un fournisseur de Cloud AWS ou Azure, téléchargez le certificat Baltimore CyberTrust Root.
   - Pour Alibaba, téléchargez le certificat racine R1 de GlobalSign à partir de https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates.
   - Pour un fournisseur de Cloud Virtustream, téléchargez le certificat DigiCert High Assurance EV Root CA.
   - S'il s'agit d'un fournisseur de Cloud ECS, l'autorité de certification racine varie en fonction du client. Pour plus d'informations, contactez votre fournisseur de répartiteur de charge.

   Les fichiers de certificat téléchargés possèdent l'extension .crt. Utilisez openssl sur tous les systèmes Linux ou Unix où il est installé pour convertir le fichier du format .crt au format .pem.

   ```
   $openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
   -out DigiCertHighAssuranceEVRootCA.pem
   ```

   ```
   $openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
   BaltimoreCyberTrustRoot.pem
   ```

   ```
   # adminaccess certificate import ca application cloud
   Enter the certificate and then press Control-D, or press
   Control-C to cancel.
   ```

3. Pour configurer le système Data Domain en vue du déplacement des données vers le Cloud, vous devez d'abord activer la fonction « Cloud » et définir la phrase secrète du système si elle n'a pas déjà été définie.

```
# cloud enable
Cloud feature requires that passphrase be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
Encryption is recommended on the cloud tier.
    Do you want to enable encryption? (yes|no) [yes]:
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
```

4. Configurez le profil de Cloud à l'aide des informations d'identification du fournisseur de Cloud. Les invites et les variables varient selon le fournisseur.

```
# cloud profile add <profilename>
```

Remarque

Pour des raisons de sécurité, cette commande n'affiche pas les clés d'accès/clés secrètes que vous saisissez.

Sélectionnez le fournisseur :

```
Enter provider name (alibabacloud|aws|azure|ecs|google|
s3_flexible|virtustream)
```

- Alibaba Cloud nécessite la saisie de la clé d'accès, de la clé secrète, de la classe de stockage et de la région.
- AWS S3 nécessite la saisie de la clé d'accès, de la clé secrète, de la classe de stockage et de la région.
- Azure nécessite le nom du compte, que le compte soit ou non un compte Azure Government, une clé primaire et une clé secondaire et une classe de stockage.
- ECS requiert la saisie de la clé d'accès, de la clé secrète et du point de terminaison.
- Google Cloud Platform nécessite une clé d'accès, une clé secrète et une région. (La classe de stockage est Nearline.)
- Les fournisseurs S3 Flexible nécessitent le nom du fournisseur, la clé d'accès, la clé secrète, la région, le point de terminaison et la classe de stockage.
- Virtustream nécessite la saisie de la clé d'accès, de la clé secrète, de la classe de stockage et de la région.

À la fin de chaque ajout de profil, vous devez indiquer si vous souhaitez configurer un proxy. Si vous le faites, les valeurs suivantes sont requises : *nom d'hôte du proxy*, *port du proxy*, *nom d'utilisateur du proxy* et *mot de passe proxy*.

5. Vérifiez la configuration du profil Cloud :

```
# cloud profile show
```

6. Créez le système de fichiers du niveau actif si ce n'est pas déjà fait :

```
# filesys create
```

7. Activez le système de fichiers :

```
# filesys enable
```

8. Configurez l'unité de Cloud :

   ```
   # cloud unit add unitname profile profilename
   ```

   Utilisez la commande `cloud unit list` pour répertorier les unités de Cloud.

9. Vous pouvez également configurer le chiffrement pour l'unité de Cloud.

   a. Vérifiez que la licence ENCRYPTION est installée :

   ```
   # elicense show
   ```

   b. Activez le chiffrement pour l'unité de Cloud :

   ```
   # filesys encryption enable cloud-unit unitname
   ```

   c. Vérifiez l'état du chiffrement :

   ```
   # filesys encryption status
   ```

10. Créez une ou plusieurs structures MTree :

    ```
    # mtree create /data/col1/mt11
    ```

11. Vérifiez la configuration de DD Cloud Tier :

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. Configurez la règle de migration des fichiers pour cette structure MTree. Vous pouvez spécifier plusieurs structures Mtree dans cette commande. La règle peut être basée sur le seuil d'âge ou sur la tranche d'âge.

    a. Pour configurer le seuil d'âge (migration des fichiers plus anciens que l'âge indiqué vers le Cloud) :

    ```
    # data-movement policy set age-threshold age_in_days to-tier
    cloud cloud-unit unitname mtrees mtreename
    ```

    b. Pour configurer la tranche d'âge (migration uniquement des fichiers appartenant à la tranche d'âge spécifiée) :

    ```
    # data-movement policy set age-range min-age age_in_days max-
    age age_in_days to-tier cloud cloud-unit unitname mtrees
    mtreename
    ```

13. Exportez le système de fichiers puis, à partir du client, montez le système de fichiers et procédez à l'acquisition des données dans le niveau actif. Modifiez la date de modification sur les fichiers acquis de façon à ce qu'ils soient désormais éligibles pour la migration des données. (Choisissez une date antérieure à la valeur de seuil d'âge spécifiée lors de la configuration de la règle de déplacement des données).
14. Lancez la migration des fichiers les plus anciens. Une fois encore, vous pouvez spécifier plusieurs structures Mtree avec cette commande.

    ```
    # data-movement start mtrees mtreename
    ```

    Pour vérifier l'état du déplacement des données :

    ```
    # data-movement status
    ```

    Vous pouvez également observer la progression du déplacement des données :

    ```
    # data-movement watch
    ```

15. Assurez-vous que la migration des fichiers a réussi et que les fichiers se trouvent désormais dans le niveau Cloud :

    ```
    # filesys report generate file-location path all
    ```

16. Une fois que vous avez migré un fichier vers le niveau Cloud, il n'est pas possible de lire directement le contenu du fichier (si vous essayez de le faire, un message d'erreur s'affiche). Le fichier peut uniquement être renvoyé vers le niveau actif. Pour rappeler un fichier vers le niveau actif :

    ```
    # data-movement recall path pathname
    ```

Configuration du chiffrement pour les unités de Cloud DD

Le chiffrement peut être activé à trois niveaux : Système Data Domain, niveau actif et unité de Cloud. Le chiffrement au niveau actif n'est applicable que si le chiffrement est activé pour le système Data Domain. Les unités de Cloud ont des commandes distinctes pour l'activation du chiffrement.

Procédure

1. Sélectionnez **Data Management** > **File System** > **DD Encryption**.

Remarque

Si aucune licence de chiffrement n'est présente sur le système, la page Add Licenses s'affiche.

2. Dans le panneau DD Encryption, effectuez l'une des opérations suivantes :
   - Pour activer le chiffrement pour **l'unité de Cloud *x***, cliquez sur **Enable**.
   - Pour désactiver le chiffrement pour **l'unité de Cloud *x***, cliquez sur **Disable**.

Remarque

Vous êtes invité à saisir les informations d'identification du responsable de la sécurité pour activer le chiffrement.

3. Saisissez le **nom d'utilisateur** et le **mot de passe** du responsable de la sécurité. Si besoin est, cochez la case **Restart file system now** pour redémarrer le système de fichiers maintenant.
4. Cliquez sur **Enable** ou **Disable**, comme il convient.
5. Dans le panneau File System Lock, verrouillez ou déverrouillez le système de fichiers.
6. Dans le panneau Key Management, cliquez sur **Configure**.
7. Dans la boîte de dialogue Change Key Manager, configurez les informations d'identification du responsable de la sécurité et le Gestionnaire de clés (Key Manager).

Remarque

Le chiffrement du Cloud est possible uniquement via le Gestionnaire de clés intégré dans Data Domain. Les gestionnaires de clés externes ne sont pas pris en charge.

8. Cliquez sur **OK**.
9. Utilisez le panneau DD Encryption Keys pour configurer les clés de chiffrement.

Informations nécessaires en cas de perte du système

Une fois le niveau cloud configuré sur le système Data Domain, enregistrez les informations suivantes sur le système et stockez-les dans un emplacement en dehors du système Data Domain. Ces informations seront nécessaires pour restaurer les données du niveau cloud en cas de perte du système Data Domain.

Remarque

Ce processus a été conçu pour les situations d'urgence uniquement et demandera beaucoup de temps et d'efforts à l'équipe d'ingénierie Data Domain.

- Numéro de série du système Data Domain d'origine
- Phrase de passe du système Data Domain d'origine
- Numéro de version DD OS du système Data Domain d'origine

- Informations relatives au profil et à la configuration du niveau du cloud

Utilisation de DD Replicator avec DD Cloud Tier

La réplication de collection n'est pas prise en charge sur les systèmes Data Domain offrant une hiérarchisation du Cloud (c'est-à-dire avec DD Cloud Tier activé).

La réplication de répertoire ne fonctionne que sur la structure MTree /backup et cette dernière ne peut être attribuée qu'au niveau Cloud. Par conséquent, la réplication de répertoire n'est pas affectée par DD Cloud Tier.

La réplication de fichiers gérés et la réplication de MTree sont prises en charge sur les systèmes Data Domain sur lesquels DD Cloud Tier est activé. DD Cloud Tier peut être activé sur l'un ou l'autre des systèmes ou sur les deux systèmes à la fois. Si le système source est activé pour la hiérarchisation du Cloud, les données devront éventuellement être lues à partir du Cloud si le fichier a déjà été migré vers le niveau Cloud. Un fichier répliqué est toujours placé en premier dans le niveau actif du système de destination, même lorsque le niveau Cloud est activé. Un fichier peut être rappelé du niveau Cloud au niveau actif sur la structure MTree source uniquement. Le rappel d'un fichier sur la structure MTree de destination n'est pas autorisé.

Remarque

Si le système source exécute DD OS 5.6 ou 5.7 et effectue la réplication vers un système (sur lequel DD Cloud Tier est activé) à l'aide de la réplication de MTree, le système source doit être mis à niveau vers une version capable d'opérer la réplication vers un système à hiérarchisation du Cloud. Pour plus d'informations sur la configuration système requise, consultez les *Notes de mise à jour de DD OS*.

Remarque

Les fichiers appartenant au niveau de Cloud ne peut pas être utilisés comme fichiers de base pour les opérations de sauvegarde synthétique virtuelle. Les sauvegardes synthétiques complètes ou les sauvegardes incrémentielles systématiques doivent s'assurer que les fichiers demeurent sur le niveau actif si vous comptez les utiliser dans la synthèse virtuelle des nouvelles sauvegardes.

Utilisation d'une librairie de bandes virtuelle DD avec Cloud Tier

Sur les systèmes configurés avec Cloud Tier et une DD VTL, le stockage cloud est pris en charge pour une utilisation comme chambre forte de la librairie de bandes virtuelle. Pour utiliser une bande VTL DD sur le cloud, autorisez une licence et configurez le stockage cloud tout d'abord, puis sélectionnez-le comme emplacement de la chambre forte de la VTL.

La section Copie de bandes DD VTL sur le cloud à la page 397 fournit des informations supplémentaires sur l'utilisation de la VTL avec Cloud Tier.

Affichage des graphiques de consommation de capacité pour DD Cloud Tier

Trois graphiques (Space Usage, Consumption et Daily Written.) présentent des statistiques sur l'utilisation de l'espace DD Cloud Tier.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Charts**.
2. Pour **Chart**, sélectionnez l'une des options suivantes :
   - Space Usage (utilisation de l'espace)
   - Consumption (consommation)
   - Daily Written (écrit tous les jours)
3. Pour définir le périmètre (**Scope**), sélectionnez **Cloud Tier** (niveau Cloud).
   - L'onglet Space Usage affiche l'utilisation de l'espace au fil du temps, en Mio. Vous pouvez sélectionner une durée (une semaine, un mois, trois mois, un an, ou toutes les durées (All)). Les données sont présentées (chromocodées) comme suit : données utilisées avant la compression (en bleu), données utilisées après la compression (en rouge) et facteur de compression (en vert).
   - L'onglet Consumption affiche la quantité de stockage utilisée après la compression et le taux de compression au fil du temps, ce qui vous permet d'analyser les tendances de la consommation. Vous pouvez sélectionner une durée (une semaine, un mois, trois mois, un an, ou toutes les durées (All)). Les données sont présentées (chromocodées) comme suit : capacité (en bleu), données utilisées après la compression (en rouge), facteur de compression (vert), nettoyage (orange) et déplacement des données (violet).
   - L'onglet Daily Written affiche la quantité de données écrites par jour. Vous pouvez sélectionner une durée (une semaine, un mois, trois mois, un an, ou toutes les durées (All)). Les données sont présentées (chromocodées) comme suit : données écrites avant la compression (en bleu), données utilisées après la compression (en rouge) et le facteur de compression total (en vert).

Logs DD Cloud Tier

Si DD Cloud Tier subit une défaillance quelconque, dans une configuration ou une opération, le système crée automatiquement un dossier avec un horodatage associé à l'heure de la défaillance.

Montez le répertoire `/ddvar/log/debug` pour accéder aux logs.

Remarque

Le résultat de la commande `log list view` ne répertorie pas tous les fichiers log détaillés qui sont créés pour la défaillance de DD Cloud Tier.

Utilisation de l'interface de ligne de commande (CLI) pour supprimer DD Cloud Tier

Vous pouvez utiliser l'interface de ligne de commande Data Domain pour supprimer la conifguration DD Cloud Tier.

Avant de commencer

Supprimez tous les fichiers dans les unités de cloud avant de supprimer la configuration DD Cloud Tier du système. Exécutez la commande `filesys report generate file-location path all output-file file_loc` pour identifier les fichiers dans les unités de cloud et les supprimer des points de montage NFS des structures MTree.

Remarque

La commande ci-dessus crée le rapport `file_loc` dans le répertoire `/ddr/var/`.

Procédure

1. Désactivez le système de fichiers.

```
# filesys disable

This action will disable the file system.
Applications may experience interruptions
while the file system is disabled.
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Please wait.............
The filesystem is now disabled.
```

2. Répertoriez les unités de cloud sur le système.

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Active
cloud_unit-2   cloudProfile2  Active
------------   ------------   ------
```

3. Supprimez les unités de cloud individuellement.

```
# cloud unit del cloud_unit-1

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-1".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-1"
Cloud unit 'cloud_unit-1' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.

# cloud unit del cloud_unit-2

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-2".
    Are you sure? (yes|no) [no]: yes
```

```
ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-2"
Cloud unit 'cloud_unit-2' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.
```

4. Vérifiez que les opérations de suppression sont en cours.

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Delete-Pending
cloud_unit-2   cloudProfile2  Delete-Pending
------------   ------------   ------
```

5. Redémarrez le système de fichiers.

```
# filesys enable
Please wait.....................................
The filesystem is now enabled.
```

6. Exécutez la commande `cloud unit list` pour vérifier qu'aucune unité de cloud ne s'affiche.

   Contactez le support technique si une unité de cloud ou les deux s'affichent toujours avec l'état `Delete-Pending`.

7. Identifiez les boîtiers de disque qui sont attribués à DD Cloud Tier.

```
# storage show tier cloud

Cloud tier details:
Disk   Disks               Count   Disk     Additional
Group                              Size     Information
------ ------------------- ------  -------- ------------
dgX    2.1-2.15, 3.1-3.15  30      3.6 TiB
------ ------------------- ------  -------- ------------
Current cloud tier size: 0.0 TiB
Cloud tier maximum capacity: 108.0 TiB
```

8. Supprimez les boîtiers de disque de DD Cloud Tier.

```
# storage remove enclosures 2, 3

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done

Removing enclosure 3...Enclosure 3 successfully removed.

Updating system information...done

Successfuly removed: 3 done
```

CHAPITRE 19

DD Extended Retention

Ce chapitre inclut les sections suivantes :

Présentation de l'option DD Extended Retention

L'option Data Domain Extended Retention (DD Extended Retention) repose sur une approche de hiérarchisation interne qui permet une rétention des données de sauvegarde à long terme et économique sur un système DD. DD Extended Retention vous permet d'utiliser les systèmes DD pour la rétention de sauvegardes à long terme et limiter au maximum l'utilisation de bandes.

Remarque

DD Extended Retention s'appelait auparavant *Data Domain Archiver*.

Système de fichiers à deux niveaux

Le système de fichiers à deux niveaux interne d'un système DD activé pour l'option DD Extended Retention est composé d'un *niveau actif* et d'un *niveau de rétention*. Le système de fichiers apparaît toutefois comme une entité unique. Les données entrantes sont d'abord placées dans le niveau actif du système de fichiers. Les données (sous la forme de fichiers entiers) sont ensuite déplacées vers le niveau de rétention du système de fichiers, comme spécifié par votre propre *règle de déplacement des données*. Par exemple, le niveau actif peut conserver les sauvegardes complètes hebdomadaires et les sauvegardes incrémentielles quotidiennes pendant 90 jours, tandis que le niveau de rétention conserve les sauvegardes complètes mensuelles pendant 7 ans.

Le niveau de rétention est composé d'une ou de plusieurs unités de rétention, chacune pouvant récupérer du stockage à partir d'un ou de plusieurs tiroirs.

Remarque

À partir de la version 5.5.1 de DD OS, une seule unité de rétention par niveau de rétention est autorisée. Toutefois, les systèmes configurés avant la version 5.5.1 de DD OS peuvent posséder plusieurs unités de rétention, mais vous ne pourrez pas leur ajouter de nouvelles unités de rétention.

Transparence de l'opération

Les systèmes DD activés pour l'option DD Extended Retention prennent en charge des applications de sauvegarde existantes par le biais de méthodes d'accès aux données, utilisables simultanément via des protocoles de service de fichiers NFS et CIFS sur Ethernet, DD VTL pour les systèmes ouverts et IBMi, ou sous la forme d'une cible sur disque grâce à des interfaces spécifiques des applications, telles que DD Boost (à utiliser avec Avamar®, NetWorker®, Greenplum, Symantec OpenStorage et Oracle RMAN).

DD Extended Retention étend l'architecture DD grâce à un déplacement des données transparent automatique du niveau actif vers le niveau de rétention. Toutes les données figurant dans les deux niveaux sont accessibles, bien qu'un léger retard puisse survenir lors de l'accès initial aux données dans le niveau de rétention. L'espace de nommage du système est de portée globale, et n'est pas affecté par le déplacement des données. Aucun partitionnement du système de fichiers n'est nécessaire pour bénéficier du système de fichiers à deux niveaux.

Règle de déplacement de données

La *règle de déplacement des données*, que vous pouvez personnaliser, est la règle selon laquelle les fichiers sont déplacés du niveau actif vers le niveau de rétention. Elle repose sur le moment où le fichier a été modifié pour la dernière fois. Vous pouvez définir une règle différente pour chaque sous-ensemble de données, car la règle peut

être définie par structure MTree. Les fichiers susceptibles d'être mis à jour nécessitent une règle différente de ceux qui ne sont jamais modifiés.

Déduplication au sein d'une unité de rétention
Pour la localisation des pannes, la déduplication s'effectue entièrement au sein d'une unité de rétention pour les systèmes DD activés pour l'option DD Extended Retention. Aucune déduplication croisée ne s'effectue entre les niveaux actif et de rétention, ou entre différentes unités de rétention (le cas échéant).

Stockage récupéré de chaque niveau
Le concept de hiérarchisation s'étend jusqu'au stockage pour un système DD activé pour l'option DD Extended Retention. Le niveau actif du système de fichiers récupère le stockage du niveau actif du stockage. Le niveau de rétention du système de fichiers récupère le stockage du niveau de rétention du stockage.

Remarque

Pour les niveaux actif et de rétention, la version 5.2 de DD OS et les versions ultérieures prennent en charge les tiroirs ES20 et ES30, et la version 5.7 de DD OS et les versions ultérieures prennent en charge les tiroirs DS60 sur certains modèles. Des types différents de tiroirs Data Domain ne peuvent pas être mélangés dans le même ensemble de tiroirs, et les ensembles de tiroirs doivent être équilibrés conformément aux règles de configuration décrites dans le *Guide du matériel ES30 Expansion Shelf* ou le *Guide du matériel DS60 Expansion Shelf*. Avec DD Extended Retention, vous pouvez attacher significativement plus de stockage au même contrôleur. Par exemple, vous pouvez attacher un maximum de 56 tiroirs ES30 sur un système DD990 avec DD Extended Retention. Le niveau actif doit inclure le stockage composé d'au moins un tiroir. Pour connaître la configuration de tiroir minimale et maximale pour les modèles de Contrôleur Data Domain, consultez les guides de matériel pour les tiroirs d'extension ES30 et DS60.

Protection des données
Sur un système DD activé pour l'option DD Extended Retention, les données sont protégées par des fonctions de localisation des pannes intégrées, une capacité de reprise après sinistre et l'architecture d'invulnérabilité des données (DIA). L'architecture d'invulnérabilité des données vérifie les fichiers lors de leur déplacement du niveau actif vers le niveau de rétention. Une fois les données copiées dans le niveau de rétention, les structures de système de fichiers et de conteneur sont à nouveau lues et vérifiées. L'emplacement du fichier est mis à jour, et de l'espace est récupéré sur le niveau actif après vérification que le fichier été correctement écrit sur le niveau de rétention.

Lorsqu'une unité de rétention est pleine, les informations sur l'espace de nommage et les fichiers système sont copiés dans cet espace, de sorte que les données de l'unité de rétention puissent être restaurées même lorsque d'autres parties du système sont perdues.

Remarque

Le nettoyage et certaines formes de réplication ne sont pas pris en charge sur les systèmes DD activés pour l'option DD Extended Retention.

Récupération d'espace
Pour récupérer de l'espace libéré par le déplacement de données vers le niveau de rétention, vous pouvez utiliser la fonction *Space Reclamation* (introduite dans DD OS 5.3), qui s'exécute en arrière-plan en tant qu'activité de faible priorité. Celle-ci

s'interrompt automatiquement lorsque des activités de plus haute priorité sont exécutées, telles que le déplacement et le nettoyage de données.

Chiffrement des données inactives
À partir de la version 5.5.1 de DD OS, vous pouvez utiliser la fonction *Encryption of Data at Rest* sur les systèmes DD activés pour l'option DD Extended Retention, si vous disposez d'une licence de chiffrement. Par défaut, cette fonction de chiffrement n'est pas activée.

Il s'agit d'une extension de la fonction de chiffrement qui était déjà disponible, avant la version 5.5.1 de DD OS, pour les systèmes qui n'utilisent pas l'option DD Extended Retention.

Reportez-vous au chapitre *Gestion du chiffrement des données inactives* pour obtenir des instructions complètes sur la configuration et l'utilisation de la fonction de chiffrement.

Protocoles prenant en charge DD Extended Retention

Les systèmes DD activés pour l'option DD Extended Retention prennent en charge les protocoles NFS, CIFS et DD Boost. La prise en charge de librairie de bandes virtuelle (DD VTL) a été ajoutée à la version 5.2 de DD OS et la prise en charge de NDMP a été ajoutée à la version 5.3 de DD OS.

Remarque

Pour obtenir la liste des applications prises en charge avec DD Boost, consultez la *DD Boost Compatibility List* sur le site de support en ligne.

Lorsque vous utilisez l'option DD Extended Retention, les données sont d'abord réceptionnées sur le niveau actif. Les fichiers sont déplacés dans leur intégralité vers l'unité de rétention du niveau de rétention, conformément à votre règle de déplacement des données. Tous les fichiers apparaissent dans le même espace de nommage. Il n'est pas nécessaire de partitionner des données et vous pouvez continuer à développer le système de fichiers comme il convient.

Toutes les données sont visibles pour tous les utilisateurs et toutes les métadonnées du système de fichiers sont sur le niveau actif.

En cas de déplacement des données du niveau actif vers le niveau de rétention, le système offre une plus grande capacité mais un temps d'accès légèrement plus lent si l'unité faisant l'objet de l'accès n'est actuellement pas prête pour l'accès.

Haute disponibilité et rétention étendue

Les systèmes Data Domain sur lesquels la haute disponibilité est activée ne prennent pas en charge DD Extended Retention. DD OS ne peut pas actuellement prendre en charge le niveau de rétention étendue avec HA.

Utilisation de DD Replicator avec l'option DD Extended Retention

Certaines formes de réplication sont prises en charge sur les systèmes DD sur lesquels l'option DD Extended Retention est activée.

Les types de réplication pris en charge dépendent des données à protéger :

- Pour protéger les données d'un système en tant que *source*, un système DD activé pour l'option DD Extended Retention prend en charge la réplication de collection, la réplication de structures MTree et la réplication de fichiers gérée par DD Boost.
- Pour protéger les données d'autres systèmes en tant que *destination*, un système DD activé pour l'option DD Extended Retention prend également en charge la réplication de répertoire, la réplication de collection, la réplication de structures MTree et la réplication de fichiers gérée par DD Boost.

Remarque

La réplication en mode delta (optimisation d'une bande passante faible) n'est pas prise en charge par l'option DD Extended Retention. Vous devez désactiver la réplication en mode delta sur tous les contextes avant d'activer l'option DD Extended Retention sur un système DD.

Réplication de collection avec l'option DD Extended Retention

Une réplication de collection survient entre le niveau actif et l'unité de rétention correspondants de deux systèmes DD avec l'option DD Extended Retention activée. Si le niveau actif ou l'unité de rétention à la source tombe en panne, les données peuvent être copiées de l'unité correspondante sur le site distant vers une nouvelle unité, qui est transmise à votre site en tant qu'unité de remplacement.

Les conditions préalables à la configuration de la réplication de collection sont les suivantes :

- Les systèmes source et de destination doivent être configurés en tant que systèmes DD avec l'option DD Extended Retention activée.
- Le système de fichiers ne doit pas être activé sur le système de destination tant que l'unité de rétention ne lui a pas été ajoutée, et que la réplication n'a pas été configurée.

Réplication de répertoire avec l'option DD Extended Retention

Pour la réplication de répertoire, un système DD activé pour l'option DD Extended Retention sert de cible à la réplication et prend en charge des topologies un vers un et plusieurs vers un à partir de n'importe quel système DD pris en charge. Cependant, les systèmes DD activés pour l'option DD Extended Retention ne prennent pas en charge la réplication de répertoire bidirectionnelle et ne peuvent pas être la *source* d'une réplication de répertoire.

Remarque

Pour copier des données à l'aide d'une réplication de répertoire dans un système DD activé pour l'option DD Extended Retention, la source doit exécuter la version 5.0 ou ultérieure de DD OS. Par conséquent, sur les systèmes exécutant DD OS 5.0 ou une version antérieure, vous devez d'abord importer les données dans un système intermédiaire exécutant DD OS 5.0 ou ultérieure. Vous pouvez, par exemple, effectuer une réplication à partir d'un système DD OS 4.9 activé pour l'option DD Extended Retention vers un système DD OS 5.2 qui n'est pas activé pour cette option, puis effectuer une réplication à partir du système DD OS 5.2 vers le système DD OS 4.9.

Réplication de structure MTree avec l'option DD Extended Retention

Vous pouvez configurer la réplication d'une structure MTree entre deux systèmes DD activés pour l'option DD Extended Retention. Les données répliquées sont d'abord

placées dans le niveau actif du système de destination. La règle de déplacement des données définie pour le système de destination détermine le moment où les données répliquées sont déplacées vers le niveau de rétention.

Notez que les règles et les restrictions appliquées à la réplication d'une structure MTree varient selon la version de DD OS, comme suit :

- À partir de la version 5.1 de DD OS, les données peuvent être répliquées d'un système qui n'est pas activé pour l'option DD Extended Retention vers un système activé pour cette option, dans le cadre d'une réplication de structure MTree.
- À partir de la version 5.2 de DD OS, les données peuvent être protégées dans un niveau actif. Pour cela, elles doivent être répliquées au niveau actif d'un système activé pour l'option DD Extended Retention.
- À partir de la version 5.5 de DD OS, la réplication d'une structure MTree est prise en charge d'un système activé pour l'option DD Extended Retention vers un système qui n'est pas activé pour cette option, si les deux systèmes exécutent la version 5.5 de DD OS ou ultérieure.
- Pour les versions 5.3 et 5.4 de DD OS, si vous prévoyez d'activer l'option DD Extended Retention, ne configurez pas la réplication pour la MTree /backup sur la machine source. (Cette restriction ne s'applique pas aux versions 5.5 et ultérieures de DD.)

Réplication de fichiers gérés avec l'option DD Extended Retention

Pour les systèmes DD sur lesquels DD Extended Retention est activé, les topologies prises en charge pour la réplication de fichiers gérés par DD Boost sont de type un vers un, plusieurs vers un, bidirectionnel, un vers plusieurs et en cascade.

Remarque

En ce qui concerne DD Boost 2.3 ou version supérieure, vous pouvez spécifier la façon dont plusieurs copies doivent être créées et gérées dans l'application de sauvegarde.

Matériel et licences pour l'option DD Extended Retention

Certaines configurations matérielles sont requises pour les systèmes sur lesquels l'option DD Extended Retention est activée. L'attribution de licences, en particulier de licences basées sur la capacité des tiroirs, est également spécifique de cette fonction.

Matériel pris en charge pour l’option DD Extended Retention

La configuration matérielle requise pour les systèmes DD prenant en charge l’option DD Extended Retention définit la quantité de mémoire nécessaire, les tiroirs, les cartes réseau/FC et ainsi de suite. Pour plus d’informations sur les configurations matérielles requises pour DD Extended Retention, consultez la guide d’installation et de configuration pour votre système Data Domain, ainsi que les guides du matériel pour vos tiroirs d’extension.

Les systèmes DD suivants prennent en charge l’option DD Extended Retention :

DD860

- 72 Go de RAM
- 1 module d’E/S NVRAM (1 Go)
- 3 modules d’E/S SAS de 4 ports

- 2 ports 1 GbE sur la carte mère
- 0 à 2 cartes réseau d'E/S 1/10 GbE pour la connectivité externe
- 0 à 2 cartes d'E/S HBA FC à 2 ports pour la connectivité externe
- 0 à 2 cartes réseau et FC combinées
- 1 à 24 tiroirs ES20 ou ES30 (disques de 1 ou 2 To), sans dépasser la capacité utile maximale du système qui est de 142 To

Si l'option DD Extended Retention est activée sur un système DD860, la capacité de stockage utile maximale d'un niveau actif est de 142 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 142 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 284 To.

DD990

- 256 Go de RAM
- 1 module d'E/S NVRAM (2 Go)
- 4 modules d'E/S SAS de 4 ports
- 2 ports 1 GbE sur la carte mère
- 0 à 4 cartes réseau d'E/S 1 GbE pour la connectivité externe
- 0 à 3 cartes réseau d'E/S 10 GbE pour la connectivité externe
- 0 à 3 cartes HBA FC à 2 ports pour la connectivité externe
- 0 à 3 cartes réseau et FC combinées, sans dépasser trois cartes réseau et FC combinées pour un module d'E/S spécifique
- 1 à 56 tiroirs ES20 ou ES30 (disques de 1, 2 ou 3 To), sans dépasser la capacité utile maximale du système qui est de 570 To

Si l'option DD Extended Retention est activée sur un système DD990, la capacité de stockage utile maximale du niveau actif est de 570 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 570 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 1140 To.

DD4200

- 128 Go de RAM
- 1 module d'E/S NVRAM (4 Go)
- 4 modules d'E/S SAS de 4 ports
- 1 port 1 GbE sur la carte mère
- 0 à 6 cartes réseau 1/10 GbE pour la connectivité externe
- 0 à 6 cartes HBA FC à 2 ports pour la connectivité externe
- 0 à 5 cartes réseau et FC combinées, sans dépasser quatre d'un modèle de module d'E/S spécifique
- 1 à 16 tiroirs SAS ES30 (disques de 2 ou 3 To), sans dépasser la capacité utile maximale du système qui est de 192 To Les tiroirs SATA ES30 (disques de 1, 2 ou 3 To) sont pris en charge pour les mises à niveau du contrôleur système.

Si l'option DD Extended Retention est activée sur un système DD4200, la capacité de stockage utile maximale du niveau actif est de 192 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 192 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 384 To. La connectivité externe est prise en charge pour les configurations DD Extended Retention jusqu'à 16 tiroirs.

DD4500

- 192 Go de RAM
- 1 module d'E/S NVRAM (4 Go)
- 4 modules d'E/S SAS de 4 ports
- 1 port 1 GbE sur la carte mère
- 0 à 6 cartes réseau d'E/S 1/10 GbE pour la connectivité externe
- 0 à 6 cartes HBA FC à 2 ports pour la connectivité externe
- 0 à 5 cartes réseau et FC combinées, sans dépasser quatre d'un modèle de module d'E/S spécifique
- 1 à 20 tiroirs SAS ES30 (disques de 2 ou 3 To), sans dépasser la capacité utile maximale du système qui est de 285 To Les tiroirs SATA ES30 (disques de 1, 2 ou 3 To) sont pris en charge pour les mises à niveau du contrôleur système.

Si l'option DD Extended Retention est activée sur un système DD4500, la capacité de stockage utile maximale du niveau actif est de 285 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 285 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 570 To. La connectivité externe est prise en charge pour les configurations DD Extended Retention jusqu'à 24 tiroirs.

DD6800

- 192 Go de RAM
- 1 module d'E/S NVRAM (8 Go)
- 3 modules d'E/S SAS de 4 ports
- 1 port 1 GbE sur la carte mère
- 0 à 4 cartes réseau 1/10 GbE pour la connectivité externe
- 0 à 4 cartes HBA FC à 2 ports pour la connectivité externe
- 0 à 4 cartes réseau et FC combinées
- Les combinaisons de tiroir sont documentées dans le guide d'installation et de configuration de votre système Data Domain, et dans les guides du matériel pour vos tiroirs d'extension.

Si l'option DD Extended Retention est activée sur un système DD6800, la capacité de stockage utile maximale du niveau actif est de 288 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 288 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 0,6 Po. La connectivité externe est prise en charge pour les configurations DD Extended Retention jusqu'à 28 tiroirs.

DD7200

- 256 Go de RAM
- 1 module d'E/S NVRAM (4 Go)
- 4 modules d'E/S SAS de 4 ports
- 1 port 1 GbE sur la carte mère
- 0 à 6 cartes réseau 1/10 GbE pour la connectivité externe
- 0 à 6 cartes HBA FC à 2 ports pour la connectivité externe
- 0 à 5 cartes réseau et FC combinées, sans dépasser quatre d'un modèle de module d'E/S spécifique

- 1 à 20 tiroirs SAS ES30 (disques de 2 ou 3 To), sans dépasser la capacité utile maximale du système qui est de 432 To Les tiroirs SATA ES30 (disques de 1, 2 ou 3 To) sont pris en charge pour les mises à niveau du contrôleur système.

Si l'option DD Extended Retention est activée sur un système DD7200, la capacité de stockage utile maximale du niveau actif est de 432 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 432 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 864 To. La connectivité externe est prise en charge pour les configurations DD Extended Retention jusqu'à 32 tiroirs.

DD9300

- 384 Go de RAM
- 1 module d'E/S NVRAM (8 Go)
- 3 modules d'E/S SAS de 4 ports
- 1 port 1 GbE sur la carte mère
- 0 à 4 cartes réseau 1/10 GbE pour la connectivité externe
- 0 à 4 cartes HBA FC à 2 ports pour la connectivité externe
- 0 à 4 cartes réseau et FC combinées
- Les combinaisons de tiroir sont documentées dans le guide d'installation et de configuration de votre système Data Domain, et dans les guides du matériel pour vos tiroirs d'extension.

Si l'option DD Extended Retention est activée sur un système DD9300, la capacité de stockage utile maximale du niveau actif est de 720 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 720 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 1,4 Po. La connectivité externe est prise en charge pour les configurations DD Extended Retention jusqu'à 28 tiroirs.

DD9500

- 512 Go de RAM
- 1 module d'E/S NVRAM (8 Go)
- 4 modules d'E/S SAS de 4 ports
- 1 port 1 GbE sur la carte mère à quatre moteurs
- 0 à 4 cartes réseau d'E/S 10 GbE pour la connectivité externe
- 0 à 4 cartes HBA FC 16 GbE à 2 ports pour la connectivité externe
- Les combinaisons de tiroir sont documentées dans le guide d'installation et de configuration de votre système Data Domain, et dans les guides du matériel pour vos tiroirs d'extension.

Si l'option DD Extended Retention est activée sur un système DD9500, la capacité de stockage utile maximale du niveau actif est de 864 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 864 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 1,7 Po. La connectivité externe est prise en charge pour les configurations DD Extended Retention jusqu'à 56 tiroirs.

DD9800

- 768 Go de RAM
- 1 module d'E/S NVRAM (8 Go)
- 4 modules d'E/S SAS de 4 ports
- 1 port 1 GbE sur la carte mère à quatre moteurs

- 0 à 4 cartes réseau d'E/S 10 GbE pour la connectivité externe
- 0 à 4 cartes HBA FC 16 GbE à 2 ports pour la connectivité externe
- Les combinaisons de tiroir sont documentées dans le guide d'installation et de configuration de votre système Data Domain, et dans les guides du matériel pour vos tiroirs d'extension.

Si l'option DD Extended Retention est activée sur un système DD9800, la capacité de stockage utile maximale du niveau actif est de 1 008 To. Le niveau de rétention peut disposer d'une capacité utile maximale de 1 008 To. Les niveaux actif et de rétention disposent d'une capacité de stockage utile totale de 2,0 Po. La connectivité externe est prise en charge pour les configurations DD Extended Retention jusqu'à 56 tiroirs.

Licences requises pour l'option DD Extended Retention

DD Extended Retention est une option logicielle sous licence installée sur un système DD pris en charge.

Une licence basée sur la capacité des tiroirs distincte est requise pour chaque tiroir de stockage, pour les tiroirs installés à la fois dans le niveau actif et le niveau de rétention. Les licences basées sur la capacité des tiroirs sont spécifiques d'un tiroir du niveau actif ou de rétention.

Une licence de stockage étendu est requise pour étendre la capacité de stockage du niveau actif au-delà de la capacité initiale, qui varie selon le modèle de système Data Domain. Vous ne pouvez pas utiliser le stockage supplémentaire sans appliquer d'abord les licences appropriées.

Ajout de licences basées sur la capacité des tiroirs pour l'option DD Extended Retention

Chaque tiroir d'un système DD activé pour l'option DD Extended Retention doit avoir une licence distincte.

Procédure

1. Sélectionnez **Administration** > **Licenses**.
2. Cliquez sur **Add Licenses**.
3. Entrez une ou plusieurs licences, une par ligne, en appuyant sur la touche Entrée après chaque licence. Cliquez sur **Add** lorsque vous avez terminé. Si des erreurs se produisent, un récapitulatif des licences ajoutées et des licences non ajoutées en raison d'une erreur s'affiche. Sélectionnez la clé de licence incorrecte pour la corriger.

Résultats

Les licences du système DD sont affichées en deux groupes :

- Licences d'option logicielle, qui sont requises pour les options telles que DD Extended Retention et DD Boost.
- Licences basées sur la capacité des tiroirs, qui affichent la capacité des tiroirs en Tio, le modèle de tiroir (ES30, par exemple) et le niveau de stockage du tiroir (actif ou de rétention).

Pour supprimer une licence, sélectionnez-la dans la liste des licences, puis cliquez sur **Delete Selected Licenses**. Si vous êtes invité à confirmer la suppression, lisez l'avertissement, puis cliquez sur **OK** pour continuer.

Configuration du stockage pour l'option DD Extended Retention

Le stockage supplémentaire pour l'option DD Extended Retention nécessite la ou les licences appropriées et suffisamment de mémoire installée sur le système DD pour les prendre en charge. Des messages d'erreur s'affichent si davantage de licences ou de mémoire sont requises.

Procédure

1. Sélectionnez l'onglet **Hardware** > **Storage**.
2. Sous l'onglet Overview, sélectionnez **Configure Storage**.
3. Sous l'onglet Configure Storage, sélectionnez le stockage à ajouter à partir de la liste Addable Storage.
4. Sélectionnez le niveau de configuration approprié (**Active** ou **Retention**) dans le menu. Le niveau actif est identique à un système DD standard et doit être dimensionné de la même manière. La quantité maximale de stockage pouvant être ajoutée au niveau actif dépend du contrôleur DD utilisé.
5. Cochez cette case pour que le tiroir soit ajouté.
6. Cliquez sur le bouton **Add to Tier**.
7. Cliquez sur **OK** pour ajouter le stockage.
8. Pour supprimer un tiroir ajouté, sélectionnez-le dans la liste Tier Configuration, sélectionnez **Remove from Tier**, puis **OK**.

Infrastructure fournie par le client avec l'option DD Extended Retention

Avant d'activer l'option DD Extended Retention, votre environnement et votre configuration doivent respecter certaines conditions.

- **Caractéristiques techniques, exigences du site, espace de rack et câblage d'interconnexion** : consultez le *Guide d'installation et de configuration de Data Domain* correspondant au modèle de votre système DD.
- **Mise en rack et câblage** : nous conseillons d'installer les racks de votre système en tenant compte d'une future extension. Tous les tiroirs sont connectés à un seul système DD.

  Remarque

  - Consultez le *Guide du matériel de Data Domain Expansion Shelf* pour les modèles de tiroir ES20, ES30 ou DS60.

Gestion de l'option DD Extended Retention

Pour configurer et utiliser l'option DD Extended Retention sur votre système DD, vous pouvez utiliser DD System Manager et/ou l'interface de ligne de commande (CLI) DD.

- DD System Manager, anciennement Enterprise Manager, est une interface utilisateur décrite dans le présent guide.
- Les commandes `archive`, saisies dans l'interface de ligne de commande (CLI) Data Domain sont décrites dans le *Guide de référence des commandes de Data Domain Operating System*.

Une seule commande n'est pas disponible lorsque vous utilisez DD System Manager : `archive report`.

Activation des systèmes DD pour l'option DD Extended Retention

Avant d'utiliser un système DD pour l'option DD Extended Retention, vous devez disposer de la licence appropriée et de la configuration de systèmes de fichiers correcte.

Procédure

1. Assurez-vous que la licence appropriée est appliquée. Sélectionnez **Administration** > **Licenses**, et vérifiez la liste Feature Licenses pour Extended Retention.
2. Sélectionnez **Data Management** > **File System** > **More Tasks** > **Enable DD Extended Retention**.

   Cette option n'est disponible que si votre système Data Domain prend en charge DD Extended Retention et si le système de fichiers n'a pas déjà été configuré pour l'option DD Extended Retention. Gardez à l'esprit qu'une fois l'option DD Extended Retention activée, celle-ci ne peut pas être désactivée sans que le système de fichiers ne soit détruit.

   a. Si le système de fichiers est déjà activé (en tant que système non activé pour l'option DD Extended Retention), vous êtes invité à le désactiver. Pour ce faire, cliquez sur **Disable**.

   b. Si vous êtes invité à confirmer que vous souhaitez convertir le système de fichiers en système capable d'utiliser l'option DD Extended Retention, cliquez sur **OK**.

   Une fois le système de fichiers converti en système activé pour l'option DD Extended Retention, la page du système de fichiers est actualisée pour inclure des informations sur les deux niveaux et un nouvel onglet **Retention Units** apparaît.

   Équivalent CLI

   Vous pouvez également vérifier si la licence Extended Retention a bien été installée à partir de la CLI.

   Pour utiliser la méthode héritée d'octroi de licence :

   ```
   # license show
   ## License Key                  Feature
   --    -------------------       -----------
   1     AAAA-BBBB-CCCC-DDDD       Replication
   2     EEEE-FFFF-GGGG-HHHH       VTL
   --    -------------------       -----------
   ```

   En cas d'absence de la licence, chaque unité est accompagnée d'une documentation (une carte d'installation rapide) qui indique les licences acquises. Saisissez la commande suivante pour compléter la clé de licence.

   ```
   # license add license-code
   ```

   Puis, activez Extended Retention :

   ```
   # archive enable
   ```

   Pour utiliser l'octroi de licence électronique :

   ```
   # elicense show
   Feature licenses:
   ## Feature     Count Mode            Expiration Date
   -- ----------- ----- --------------- ---------------
   ```

```
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

Si la licence n'est pas présente, mettez à jour le fichier de licence avec la nouvelle licence de fonctionnalité.

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature            Count   Mode             Expiration Date
-- -----------------  -----  ---------------  ---------------
1  REPLICATION        1      permanent (int)  n/a
2  VTL                1      permanent (int)  n/a
3  EXTENDED RETENTION 1      permanent (int)  n/a
-- ------------------ -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above
EMC ELMS licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

Puis, activez Extended Retention :

```
# archive enable
```

Création d'un système de fichiers à deux niveaux pour l'option DD Extended Retention

L'option DD Extended Retention possède un système de fichiers à deux niveaux pour les niveaux actif et de rétention. L'option DD Extended Retention doit être activée sur le système DD avant de pouvoir activer ce système de fichiers particulier.

Procédure

1. Sélectionnez **Data Management** > **File System**.
2. Si un système de fichiers existe, détruisez le.
3. Sélectionnez **More Tasks** > **Create file system**.
4. Sélectionnez un système de fichiers doté de capacités de rétention, puis cliquez sur **Next**.
5. Cliquez sur **Configure** dans la boîte de dialogue File System Create.

   Vous devez d'abord configurer le stockage pour que le système de fichiers soit créé.
6. Utilisez la boîte de dialogue Configure Storage pour ajouter et supprimer le stockage disponible à partir du niveau actif et du niveau de rétention, puis cliquez sur **OK** lorsque vous avez terminé.

   Le stockage sur le niveau actif est utilisé pour créer le niveau de système de fichiers actif, et le stockage dans le niveau de rétention est utilisé pour créer une unité de rétention.

   Remarque

   À partir de la version 5.5.1 de DD OS, une seule unité de rétention par niveau de rétention est autorisée. Toutefois, les systèmes configurés avant la version 5.5.1 de DD OS peuvent posséder plusieurs unités de rétention, mais vous ne pourrez pas leur ajouter de nouvelles unités de rétention.
7. Utilisez la boîte de dialogue Create File System pour effectuer les opérations suivantes :

a. Sélectionnez la taille de l'unité de rétention dans la liste déroulante.

b. Sélectionnez l'option **Enable the file system after creation**.

c. Cliquez sur **Next**.

Une page récapitulative affiche la taille des niveaux actif et de rétention dans le nouveau système de fichiers.

8. Cliquez sur **Finish** pour créer le système de fichiers.

   La progression de chaque étape de création est affichée, et la barre de progression indique l'état global.

9. Cliquez sur **OK** une fois l'exécution du système de fichiers terminée.

   Équivalent de l'interface de ligne de commande (CLI)
   Pour ajouter des tiroirs, utilisez cette commande une fois pour chaque châssis :

   ```
   # storage add tier archive enclosure 5
   ```

   Créez une unité d'archivage, puis ajoutez-la au système de fichiers. Vous devez spécifier le nombre de châssis dans l'unité d'archivage :

   ```
   # filesys archive unit add
   ```

   Vérifiez que l'unité d'archivage a bien été créée et ajoutée au système de fichiers :

   ```
   # filesys archive unit list all
   ```

   Vérifiez le système de fichiers, tel que vu par le système :

   ```
   # filesys show space
   ```

Volet File System pour DD Extended Retention

Une fois un système DD activé pour l'option DD Extended Retention, le volet **Data Management** > **File System** est légèrement différent (par rapport à un système non activé pour l'option DD Extended Retention).

- L'option **State** indique si le système de fichiers est activé ou désactivé. Vous pouvez modifier l'état à l'aide du bouton Disable/Enable situé sur la droite.
- L'option **Clean Status** indique l'heure de fin de la dernière opération de nettoyage, ou l'état actuel du nettoyage si l'opération de nettoyage est en cours d'exécution. Si le nettoyage peut être exécuté, le bouton **Start Cleaning** s'affiche. Lors de l'exécution de l'opération de nettoyage, le bouton **Start Cleaning** est remplacé par un bouton **Stop Cleaning**.
- L'option **Data Movement Status** indique l'heure de fin du dernier déplacement des données. Si le déplacement de données peut être exécuté, un bouton **Start** s'affiche. Lors de l'exécution du déplacement de données, le bouton **Start** est remplacé par un bouton **Stop**.
- L'option **Space Reclamation Status** indique la quantité d'espace récupérée après la suppression des données dans le niveau de rétention. Si la récupération d'espace peut être exécutée, un bouton **Start** s'affiche. Si elle est déjà en cours d'exécution, les boutons **Stop** et **Suspend** s'affichent. Si elle a été précédemment exécutée et a été interrompue, les boutons **Stop** et **Resume** s'affichent. Le bouton **More Information** s'affiche également. Il permet d'accéder à des informations détaillées telles que les heures de début et de fin, le pourcentage de réalisation, les unités récupérées, l'espace libéré, etc.

- La sélection de **More Tasks** > **Destroy** vous permet de supprimer toutes les données du système de fichiers, bandes virtuelles incluses. Cette opération ne peut être effectuée que par un administrateur système.
- La sélection de **More Tasks** > **Fast Copy** vous permet de cloner les fichiers et les structures MTree d'un répertoire source vers un répertoire de destination. Notez que dans le cas de systèmes activés pour l'option DD Extended Retention, une opération Fast Copy ne déplace pas les données entre les niveaux actif et de rétention.
- La sélection de **More Tasks** > **Expand Capacity** vous permet de développer le niveau actif ou de rétention.

Développement du niveau actif ou de rétention

Lorsque le système de fichiers est activé, vous pouvez développer le niveau actif ou de rétention.

Pour activer le niveau actif (**Active**) :

Procédure

1. Sélectionnez **Data Management > File System > More Tasks > Expand Capacity**.
2. Dans la boîte de dialogue Expand File System Capacity, sélectionnez **Active Tier**, puis cliquez sur **Next**.
3. Cliquez sur **Configure**.
4. Dans la boîte de dialogue Configure Storage, assurez-vous que le niveau actif est sélectionné pour la configuration, puis cliquez sur **OK**.
5. Une fois la configuration terminée, vous êtes redirigé vers la boîte de dialogue Expand File System Capacity. Sélectionnez **Finish** pour terminer le développement du niveau actif.

Pour activer le niveau de rétention (**retention**) :

Procédure

1. Sélectionnez **Data Management > File System > More Tasks > Expand Capacity**.
2. Dans la boîte de dialogue Expand File System Capacity, sélectionnez **Retention Tier**, puis **Next**.
3. Si une unité de rétention est disponible, la boîte de dialogue **Select Retention Unit** s'affichera. Sélectionnez l'unité de rétention à développer, puis **Next**. Si aucune unité de rétention n'est disponible, la boîte de dialogue **Create Retention Unit** s'affichera et vous devrez créer une unité de rétention avant de poursuivre.

   Remarque

   Pour garantir les performances optimales d'un système DD activé pour l'option DD Extended Retention, vous devez toujours développer le niveau de rétention par incréments d'au moins deux tiroirs. De même, vous ne devez pas attendre que l'unité de rétention soit presque pleine pour la développer.

4. Sélectionnez la taille à laquelle développer l'unité de rétention, puis cliquez sur **Configure**.

5. Une fois la configuration terminée, vous êtes redirigé vers la boîte de dialogue Expand File System Capacity. Cliquez sur **Finish** pour terminer l'extension du niveau de rétention.

Récupération d'espace dans le niveau de rétention

Vous pouvez récupérer de l'espace des données supprimées dans le niveau de rétention en exécutant une opération de récupération d'espace (introduite dans la version 5.3 de DD OS). Une récupération d'espace se produit également lors du nettoyage du système de fichiers.

Procédure

1. Sélectionnez **Data Management** > **File System**. Juste au-dessus des onglets, **Space Reclamation Status** indique la quantité d'espace récupérée après la suppression de données dans le niveau de rétention.
2. Si la récupération d'espace peut être exécutée, un bouton **Start** s'affiche. Si elle est déjà en cours d'exécution, les boutons **Stop** et **Suspend** s'affichent. Si elle a été précédemment exécutée et a été interrompue, les boutons **Stop** et **Resume** s'affichent.
3. Cliquez sur **More Information** pour plus d'informations sur le nom de cycle, les heures de début et de fin, la durée d'exécution effective, le pourcentage de réalisation (si l'opération est en cours), les unités récupérées, l'espace libéré sur une unité cible et l'espace total libéré.

Remarque

Lorsque vous utilisez la commande `archive space-reclamation`, le système exécute une récupération d'espace en arrière-plan jusqu'à ce qu'il soit arrêté manuellement, sauf si vous utilisez l'option de cycle unique. Vous pouvez également utiliser la commande `archive space-reclamation schedule set` pour définir l'heure de début de la récupération d'espace.

Équivalent de l'interface de ligne de commande (CLI)
Pour activer la récupération d'espace :

```
# archive space-reclamation start
```

Pour désactiver la récupération d'espace :

```
# archive space-reclamation stop
```

Pour afficher l'état de la récupération d'espace :

```
# archive space-reclamation status-detailed
Space-reclamation will start when 'archive data-movement'
completes.

Previous Cycle:
---------------
Start time                 : Feb 21 2014 14:17
End time                   : Feb 21 2014 14:49
Effective run time         : 0   days, 00:32.
Percent completed          : 00 % (was stopped by user)
Units reclaimed            : None
Space freed on target unit : None
Total space freed          : None
```

Onglets File System pour DD Extended Retention

Une fois un système DD activé pour l'option DD Extended Retention, les onglets **Data Management** > **File System** seront également légèrement différents (par rapport à un

système qui n'est pas activé pour l'option DD Extended Retention) et un onglet supplémentaire s'affiche : **Retention Units**

Onglet Summary
L'onglet Summary affiche des informations sur l'utilisation de l'espace disque et la compression pour les niveaux actif et de rétention.

Space Usage : affiche la taille totale, la quantité d'espace utilisé et la quantité d'espace disponible, ainsi que les totaux combinés des niveaux actif et de rétention. La quantité d'espace pouvant être nettoyé est indiquée pour le niveau actif.

Active Tier and Retention Tier : affiche les valeurs de précompression et de post-compression actuellement utilisées et celles écrites au cours des dernières 24 heures. Affiche également les facteurs de compression globale, locale et totale (pourcentage de réduction).

Onglet Retention Units
L'onglet Retention Units affiche la ou les unités de rétention. À partir de la version 5.5.1.4 de DD OS, une seule unité de rétention par niveau de rétention est autorisée. Toutefois, les systèmes configurés avant la version 5.5.1.4 de DD OS peuvent posséder plusieurs unités de rétention, mais vous ne pourrez pas leur ajouter de nouvelles unités de rétention.

Les informations suivantes s'affichent : l'état de l'unité (New, Empty, Sealed, Target ou Cleaning), son statut (Disabled, Ready ou Stand-by), sa date de début (lorsqu'elle a été déplacée vers le niveau de rétention) et sa taille. L'unité présentera l'état Cleaning si la récupération d'espace est en cours d'exécution. Si l'unité a été scellée, et qu'aucune donnée supplémentaire ne peut donc y être ajoutée, la date du scellement est indiquée. Lorsque vous cochez la case correspondant à l'unité de rétention, des informations supplémentaires s'affichent (Size, Used, Available et Cleanable) dans le volet Detailed Information.

Deux boutons s'affichent : **Delete** (pour supprimer l'unité) et **Expand** (pour l'ajout de stockage à une unité). L'unité doit être dans un état nouveau ou cible pour être développée.

Onglet Configuration
L'onglet Configuration vous permet de configurer votre système.

Lorsque vous sélectionnez le bouton **Options Edit**, la boîte de dialogue Modify Settings s'affiche. Elle vous permet de modifier le type de compression locale (les options sont lz (par défaut), gz et gzfast) et la compression locale du niveau de rétention (les options sont : lz, gz (par défaut) et gzfast), ainsi que d'activer l'option Report Replica as Writable.

Lorsque vous sélectionnez le bouton **Clean Schedule Edit**, la boîte de dialogue Modify Schedule s'affiche. Elle vous permet de modifier le planning de nettoyage, ainsi que le pourcentage de régulation.

Lorsque vous sélectionnez le bouton **Data Movement Policy Edit** affiche la boîte de dialogue Data Movement Policy, qui vous permet de définir plusieurs paramètres. Le seuil d'âge des fichiers est une valeur par défaut définie au niveau du système, qui s'applique à toutes les structures MTree pour lesquelles vous n'avez pas défini de valeur par défaut spécifique. La valeur minimale est de 14 jours. L'option Data Movement Schedule vous permet de définir la fréquence à laquelle les données sont déplacées. La fréquence recommandée est toutes les deux semaines. L'option File System Cleaning vous permet de choisir de ne pas déclencher d'opération de nettoyage du système après le déplacement des données. Toutefois, il est fortement recommandé de conserver cette option sélectionnée.

Lien File Age Threshold per MTree
La sélection du lien **File Age Threshold per MTree** vous permet de passer de la zone File System à la zone MTree (également accessible via **Data Management** > **MTree**), où vous pouvez définir un seuil d'âge des fichiers personnalisé pour chacune de vos structures MTree.

Choisissez une structure MTree, puis sélectionnez **Edit** en regard de la règle de déplacement des données. Dans la boîte de dialogue Modify Age Threshold, entrez une nouvelle valeur de seuil d'âge des fichiers, puis sélectionnez **OK**. À partir de la version 5.5.1 de DD OS, la valeur minimale est de 14 jours.

Onglet Encryption
L'onglet Encryption vous permet d'activer ou de désactiver le chiffrement des données inactives, qui n'est pris en charge que pour les systèmes dotés d'une seule unité de rétention. À partir de la version 5.5.1, l'option DD Extended Retention ne prend en charge qu'une seule unité de rétention, de sorte que les systèmes installés pendant ou après cette version seront parfaitement conformes à cette restriction. Toutefois, les systèmes installés avant la version 5.5.1 peuvent posséder plusieurs unités de rétention. Dès lors, ils ne peuvent utiliser la fonction de chiffrement des données inactives jusqu'à ce que toutes les unités de rétention sauf une ne soient supprimées, ou que les données ne soient déplacées ou migrées vers une seule unité de rétention.

Onglet Space Usage
L'onglet Space Usage vous permet de sélectionner l'un des trois types de graphique ((entire) File System, Active (tier), Archive (tier)) afin de visualiser l'utilisation de l'espace au fil du temps, en Mio. Vous pouvez également sélectionner une durée (7, 30, 60 ou 120 jours) dans l'angle supérieur droit. Les données sont présentées (chromocodées) comme suit : les données écrites avant la compression (en bleu), les données utilisées après la compression (en rouge) et le facteur de compression (en noir).

Onglet Consumption
L'onglet Consumption vous permet de sélectionner l'un des trois types de graphique ((entire) File System; Active (tier); Archive (tier)) afin de visualiser la quantité de stockage utilisée après la compression, ainsi que le taux de compression au fil du temps, ce qui vous permet d'observer les tendances de la consommation. Vous pouvez également sélectionner une durée (7, 30, 60 ou 120 jours) dans l'angle supérieur droit. La case Capacity vous permet de choisir d'afficher ou non le stockage après la compression par rapport à la capacité totale du système.

Onglet Daily Written
L'onglet Daily Written vous permet de choisir une durée (7, 30, 60 ou 120 jours) pour visualiser la quantité de données écrites par jour. Les données sont présentées (chromocodées) sous forme de graphique et de tableau, comme suit : les données écrites avant la compression (en bleu), les données utilisées après la compression (en rouge) et le facteur de compression (en noir).

Développement d'une unité de rétention

Pour garantir des performances optimales, n'attendez pas qu'une unité de rétention soit presque pleine pour la développer, et ne la développez pas par incréments de 1 tiroir. Le stockage ne peut pas être déplacé du niveau actif vers le niveau de rétention une fois le système de fichiers créé. Seuls des châssis inutilisés peuvent être ajoutés au niveau de rétention.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Retention Units**.

2. Sélectionnez l'unité de rétention.

   Notez que si le nettoyage est en cours d'exécution, une unité de rétention ne peut pas être étendue.

3. Cliquez sur **Expand**.

   Le système affiche la taille actuelle du niveau de rétention, une taille estimée d'extension et une capacité étendue totale. Si un stockage supplémentaire est disponible, vous pouvez cliquer sur le lien Configure.

4. Cliquez sur **Next**.

   Le système affiche un message d'avertissement vous indiquant que vous ne pouvez pas rétablir le système de fichiers à sa taille d'origine après cette opération.

5. Cliquez sur **Expand** pour développer le système de fichiers.

Suppression d'une unité de rétention

Si tous les fichiers d'une unité de rétention ne sont plus utiles, leur suppression permet de réutiliser l'unité. Vous pouvez générer un rapport d'emplacement de fichiers pour vous assurer que l'unité de rétention est réellement vide, puis supprimer l'unité de rétention et l'ajouter comme nouvelle unité de rétention.

Procédure

1. Sélectionnez **Data Management** > **File System**, puis cliquez sur **Disable** pour désactiver le système de fichiers s'il est en cours d'exécution.
2. Sélectionnez **Data Management** > **File System** > **Retention Units**.
3. Sélectionnez l'unité de rétention.
4. Cliquez sur **Delete**.

Modification de la compression locale du niveau de rétention

Vous pouvez modifier l'algorithme de compression locale à utiliser pour tout déplacement ultérieur de données vers le niveau de rétention.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Configuration**.
2. Cliquez sur **Edit** à droite d'**Options**.
3. Sélectionnez l'une des options de compression dans le menu Retention Tier Local Comp, puis cliquez sur **OK**.

   La valeur par défaut est gz, ce qui correspond à une compression de type zip qui utilise le moins d'espace pour le stockage de données (de 10 à 20 % de moins que la compression lz en moyenne ; toutefois, certains datasets obtiennent une compression beaucoup plus élevée).

Présentation de la règle de déplacement des données

Un fichier est déplacé du niveau actif vers le niveau de rétention en fonction de la date de sa dernière modification. Pour préserver l'intégrité des données, l'ensemble du fichier est déplacé à ce stade. La *règle de déplacement des données* établit deux éléments : un *seuil d'âge des fichiers* et un *calendrier de déplacement des données*. Si les données n'ont pas été modifiées au cours de la période définie par le seuil d'âge des fichiers, elles sont déplacées du niveau actif vers le niveau de rétention à la date établie par le calendrier de déplacement des données.

Remarque

À partir de la version 5.5.1 de DD OS, le seuil d'âge des fichiers doit être de 14 jours minimum.

Vous pouvez spécifier les divers seuils d'âge des fichiers pour chaque structure MTree définie. Une structure MTree est un sous-arbre de l'espace de nommage, qui correspond à un ensemble de données logique destiné à la gestion. Par exemple, vous pouvez placer des données financières, des e-mails et des données techniques dans des structures MTree distinctes.

Pour tirer pleinement parti de la fonction de *récupération d'espace,* introduite dans la version 5.3 de DD OS, il est recommandé de planifier le déplacement des données et le nettoyage du système de fichiers sur une base bimensuelle (tous les 14 jours). Par défaut, le nettoyage est toujours exécuté une fois le déplacement des données terminé. Il est vivement recommandé de ne pas modifier ce comportement par défaut.

Évitez les fréquentes erreurs de dimensionnement ci-après :

- Définir une règle de déplacement des données trop ambitieuse : les données seront déplacées trop tôt.
- Définir une règle de déplacement de données trop prudente : une fois le niveau actif plein, vous ne pourrez plus écrire de données sur le système.
- Disposer d'un niveau actif sous-dimensionné, puis définir une règle de déplacement de données trop ambitieuse pour compenser.

Tenez compte des restrictions suivantes liées aux snapshots et au nettoyage du système de fichiers :

- Les fichiers contenus dans les snapshots ne sont pas nettoyés, même après avoir été déplacés vers le niveau de rétention. L'espace ne peut pas être récupéré tant que les snapshots n'ont pas été supprimés.
- Il est recommandé de définir le seuil d'âge des fichiers sur 14 jours minimum, pour les snapshots.

Vous trouverez ci-après deux exemples de configuration d'une règle de déplacement de données.

- Vous pouvez séparer les données avec différents degrés de modification en deux structures MTree distinctes et définir le seuil d'âge des fichiers pour déplacer les données peu après la stabilisation des données. Créez une structure MTree A pour les sauvegardes incrémentielles quotidiennes et une structure MTree B pour les sauvegardes complètes hebdomadaires. Définissez le seuil d'âge des fichiers de la structure MTree de sorte que ses données ne soient *jamais* déplacées, mais définissez le seuil d'âge des fichiers de la structure MTree B sur 14 jours (seuil minimal).
- Pour les données qui ne peuvent pas être séparées dans différentes structures MTree, vous pouvez procéder comme suit. Supposons que la période de rétention des sauvegardes incrémentielles quotidiennes est de huit semaines et que la période de rétention des sauvegardes complètes hebdomadaires est de trois ans. Dans ce cas, il est préférable de définir le seuil d'âge des fichiers sur neuf semaines. S'il était défini sur une période plus courte, vous déplaceriez les données incrémentielles quotidiennes qui, en réalité, devraient être bientôt supprimées.

Modification de la règle de déplacement des données

Vous pouvez définir différentes stratégies de déplacement des données pour chaque structure MTree.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Configuration**.
2. Cliquez sur **Edit** à droite de **Data Movement Policy**.
3. Dans la boîte de dialogue Data Movement Policy, indiquez la valeur du seuil d'âge des fichiers par défaut au niveau du système en nombre de jours. À partir de la version 5.5.1 de DD OS, cette valeur doit être supérieure ou égale à 14 jours. Cette valeur s'applique aux structures MTree nouvellement créées et aux structures MTree auxquelles aucune valeur de seuil d'âge par MTree n'a été attribuée via le lien **File Age Threshold per MTree** (reportez-vous à l'étape 7). Lorsque le déplacement des données débute, tous les fichiers qui n'ont pas été modifiés durant le nombre de jours seuil spécifié seront déplacés du niveau actif vers le niveau de rétention.
4. Spécifiez un calendrier de déplacement des données, c'est-à-dire que vous devez indiquer la fréquence à laquelle le déplacement des données doit avoir lieu : tous les jours, toutes les semaines, bimensuelle (tous les 14 jours), tous les mois ou le dernier jour du mois. Vous pouvez également choisir un ou plusieurs jours spécifiques, ainsi qu'une heure (heures et en minutes). Il est vivement recommandé de planifier le déplacement des données et le nettoyage du système de fichiers sur une base bimensuelle (tous les 14 jours) pour bénéficier pleinement de la fonction de récupération d'espace (qui a été introduite dans la version 5.3 DD OS).
5. Spécifiez une régulation de déplacement de données, autrement dit, le pourcentage de ressources disponibles que le système utilise pour déplacer des données. Une valeur de 100 % indique que le déplacement des données ne sera pas régulé.
6. Par défaut, le nettoyage du système de fichiers est toujours exécuté après un déplacement de données. Il est vivement recommandé de conserver l'option **Start file system clean after Data Movement** sélectionnée.
7. Sélectionnez OK.
8. Sous l'onglet Configuration, vous pouvez spécifier des valeurs de seuil d'âge pour chaque structure MTree via le lien **File Age Threshold per MTree** situé dans l'angle inférieur droit.

   Équivalent de l'interface de ligne de commande (CLI)
   Pour définir le seuil d'âge :

   ```
   # archive data-movement policy set age-threshold {days|none}
   mtrees mtree-list
   ```

   Si nécessaire, pour définir le seuil d'âge *par défaut* :

   ```
   # archive data-movement policy set default-age-threshold days
   ```

   Pour vérifier le paramètre de seuil d'âge :

   ```
   # archive data-movement policy show [mtree mtree-list]
   ```

   Pour spécifier le planning de migration :

   ```
   # archive data-movement schedule set days days time time [no-
   clean]
   ```

   Les valeurs de planning acceptables sont les suivantes :

   - days sun time 00:00
   - days mon,tue time 00:00
   - days 2 time 10:00

- days 2,15 time 10:00
- days last time 10:00 - last day of the month

Pour vérifier le planning de migration :

```
# archive data-movement schedule show
```

Pour désactiver le planning de nettoyage des fichiers :

Remarque

La désactivation du planning de nettoyage a pour objectif d'éliminer un conflit de planning entre le nettoyage et le déplacement des données. Le nettoyage démarrera automatiquement une fois le déplacement des données terminé. Si vous désactivez le déplacement des données, vous devez réactiver le nettoyage du système de fichiers.

```
# filesys clean set schedule never
```

Démarrage ou arrêt du déplacement de données à la demande

Vous pouvez démarrer ou arrêter *à la demande* le déplacement de données, même si vous possédez une stratégie régulière de déplacement de données.

Procédure

1. Sélectionnez **Data Management** > **File System**.
2. Cliquez sur le bouton **Start** situé à droite de l'option **Data Movement Status**.
3. La boîte de dialogue Start Data Movement vous avertit que les données doivent être déplacées du niveau actif vers le niveau de rétention, comme défini par votre règle de déplacement des données, déplacement qui devra être suivi d'un nettoyage du système de fichiers. Sélectionnez **Start** pour démarrer le déplacement des données.

   Si un nettoyage du système de fichiers est déjà en cours, le déplacement des données se produira une fois le nettoyage terminé. Cependant, une autre opération de nettoyage est automatiquement démarrée une fois ce déplacement de données demandé terminé.
4. Le bouton **Start** est remplacé par un bouton **Stop**.
5. À tout moment, si vous souhaitez arrêter le déplacement des données, cliquez sur **Stop**, puis sur **OK** dans la boîte de dialogue Stop Data Movement pour confirmer.

Utilisation de la compression des données déplacées

Les données sont compressées dans la partition cible après chaque migration de fichier (à partir de DD OS 5.2). Cette fonction, appelée *compression des données déplacées*, est activée par défaut.

Lorsque cette fonction est activée, la compression globale du niveau de rétention s'améliore, mais le temps de migration augmente légèrement.

Pour déterminer si cette option est activée, sélectionnez **Data Management** > **File System** > **Configuration**.

La valeur actuelle de l'option **Packing data during Retention Tier data movement** peut être Enabled ou Disabled. Contactez un ingénieur système pour modifier cette valeur.

Mises à niveau et restauration avec l'option DD Extended Retention

Les sections suivantes expliquent comment effectuer des mises à niveau logicielles et matérielles, et comment restaurer des données pour les systèmes DD activés pour l'option DD Extended Retention.

Mise à niveau vers DD OS 5.7 avec l'option DD Extended Retention

La règle de mise à niveau d'un système Data Domain sur lequel DD Extended Retention est activé est la même que celle s'appliquant à un système Data Domain standard.

La mise à niveau à partir des deux principales mises à jour antérieures est prise en charge. Pour obtenir des instructions sur la mise à niveau du système d'exploitation de DD, consultez la section d'instructions des *notes de mise à jour* de la version du système d'exploitation DD cible.

Lorsque vous effectuez la mise niveau d'un système DD sur lequel DD Extended Retention est activé vers DD OS 5.7, veillez à mettre à jour les déplacements des données existants selon un planning sur deux semaines (14 jours) afin d'exploiter la fonctionnalité de récupération d'espace.

Les systèmes DD sur lesquels DD Extended Retention est activé exécutent automatiquement un nettoyage à la fin des déplacements de données. Veillez à ne pas planifier de nettoyage séparé à l'aide de DD System Manager ou de la CLI (interface de ligne de commande).

Si le niveau actif est disponible, le processus met à niveau le niveau actif et l'unité de rétention, et il confère au système un état dont la mise à niveau précédente n'a pas vérifié l'achèvement. Cet état est supprimé par le système de fichiers une fois que celui-ci est activé et qu'il a vérifié que le niveau de rétention a été mis à jour. Aucune mise à niveau suivante n'est autorisée tant que cet état n'est pas supprimé.

Si le niveau actif n'est pas disponible, le processus de mise à niveau met le châssis du système à niveau et lui confère un état dans lequel il est prêt à créer ou à accepter un système de fichiers.

Si l'unité de rétention devient accessible à la fin du processus de mise à niveau, l'unité est automatiquement mise à jour lorsqu'elle est raccordée au système ou lors du démarrage suivant du système.

Mise à niveau du matériel avec l'option DD Extended Retention

Vous pouvez effectuer une mise à niveau d'un système DD activé pour l'option DD Extended Retention vers un système identique de version supérieure ou aux performances plus élevées. Vous pouvez, par exemple, remplacer un système DD860 activé pour l'option DD Extended Retention par un système DD990 activé pour l'option DD Extended Retention.

Remarque

Contactez votre fournisseur de services contractuel, puis consultez les instructions fournies dans le document *System Controller Upgrade Guide*.

Ce type de mise à niveau affecte l'option DD Extended Retention comme suit :

- Si le nouveau système dispose d'une version DD OS plus récente que celle des niveaux actif et de rétention, ces derniers sont mis à niveau vers la version du nouveau système. Sinon, le nouveau système est mis à niveau vers la version des niveaux actif et de rétention.
- Les niveaux actif et de rétention qui sont connectés au nouveau système deviennent la propriété du nouveau système.
- S'il existe un niveau actif, le registre de ce niveau actif est installé dans le nouveau système. Sinon, le registre figurant dans le niveau de rétention doté du registre le plus récent est installé dans le nouveau système.

Restauration d'un système activé pour l'option DD Extended Retention

Si le niveau actif et un sous-ensemble des unités de rétention sont perdus, sur un système DD activé pour l'option DD Extended Retention, et qu'il n'y a aucun réplica disponible, le support peut être amené à reconstituer toutes les unités de rétention scellées restantes dans un nouveau système DD.

Un système DD activé pour l'option DD Extended Retention est conçu pour rester disponible afin de traiter les demandes d'écriture et de lecture lorsqu'une ou plusieurs unités de rétention sont perdues. Il est possible que le système de fichiers ne détecte pas la perte d'une unité de rétention tant qu'il n'a pas redémarré ou tenté d'accéder à des données stockées sur l'unité de rétention. Ce dernier cas peut déclencher un redémarrage du système de fichiers. Une fois que le système de fichiers a détecté qu'une unité de rétention est perdue, il renvoie une erreur en réponse aux demandes relatives aux données stockées sur cette unité.

Si les données perdues ne peuvent pas être restaurées à partir d'un réplica, le support peut être amené à nettoyer le système en supprimant l'unité de rétention perdue, ainsi que tous les fichiers qui y résident entièrement ou partiellement.

Utilisation d'une restauration de réplication

La procédure de restauration de la réplication d'un système DD activé pour l'option DD Extended Retention dépend du type de réplication.

- Réplication de collection : la nouvelle source doit être configurée en tant que système DD activé pour l'option DD Extended Retention avec le même nombre d'unités de rétention que la destination (ou un plus grand nombre d'unités). Le système de fichiers ne doit pas être activé sur le nouveau système source tant que des unités de rétention n'ont pas été ajoutées et que la restauration de la réplication n'a pas été configurée

  Remarque

  Si vous devez restaurer uniquement une partie d'un système, comme une unité de rétention, à partir d'un réplica de collection, contactez le Support.

- Réplication de structure MTree : reportez-vous à la section relative à la *réplication d'une structure MTree* du chapitre *Utilisation de DD Replicator*.
- Réplication des fichiers gérée par DD Boost : consultez le *Guide d'administration de Data Domain Boost for OpenStorage*.

Restauration du système après une panne

Un système DD activé pour l'option DD Extended Retention est doté d'outils pour résoudre les pannes pouvant survenir dans les différentes parties du système.

Procédure

1. Restaurez la connexion entre le contrôleur système et le système de stockage. Si le contrôleur système est perdu, remplacez-le par un nouveau contrôleur système.
2. S'il y a une perte des données et qu'un réplica est disponible, essayez de restaurer les données à partir du réplica. Si aucun réplica n'est disponible, limitez la perte de données en utilisant les fonctions de localisation des pannes de l'option DD Extended Retention grâce au Support.

Migration des données à partir du niveau d'archivage vers DD Cloud Tier

Cette procédure utilise la réplication de structures MTree pour migrer les données du niveau d'archivage sur un système Data Domain avec Extended Retention vers un système Data Domain à nœud unique ou une instance DD VE avec DD Cloud Tier.

Avant de commencer

- Des licences pour la réplication et DD Cloud Tier sont nécessaires.
- Le système cible doit exécuter Data Domain Operating System version 6.0 ou ultérieure pour prendre en charge DD Cloud Tier.
- Le système cible doit avoir une capacité de niveau actif suffisante pour pouvoir stocker les données des niveaux actif et d'archivage sur le système source, car les données ne seront pas déplacées vers le stockage DD Cloud Tier sur le système cible pendant au moins 14 jours.
- Data Domain recommande que toute planification de capacité comprenne suffisamment de capacité au niveau actif pour un minimum de 14 jours de données répliquées.
- Toutes les procédures de sauvegarde et autres activités d'écriture sur le système source doivent être redirigées vers le système cible.
- Le système cible doit satisfaire aux mêmes exigences de conformité que le système source.
- Le client doit fournir tous les comptes et justifications d'identité appropriés pour les systèmes Data Domain cibles et sources.

Autres remarques :

- Contactez le support Dell EMC si une migration immédiate des données vers le stockage DD Cloud Tier est nécessaire.
- Les applications de sauvegarde du client peuvent ne pas suivre cette migration de données.
- Cette procédure ne couvre pas la réplication de fichiers gérés (MFR).
- Octroi de licences. Les systèmes Data Domain peuvent utiliser :
  - Des licences héritées : utilisez la commande `license show`
  - Des licences ELMS : utilisez la commande `elicense show`

Les systèmes Data Domain utilisant des licences héritées peuvent ajouter des licences par incréments. Sachez que toutes les nouvelles fonctionnalités ne sont pas prises en charge par les licences héritées.

Les systèmes Data Domain installés avec DD OS 6.0 ou une version ultérieure, convertis ou mis à niveau avec des fonctionnalités nécessitant une licence ELMS utilisent les commandes `elicense` lors de l'application et de l'affichage des licences,

et lorsqu'un nouveau fichier de clé de licence est appliqué, le nouveau jeu de clés remplace entièrement toutes les anciennes clés.

⚠ ATTENTION

Lors de la mise à jour d'une licence ELMS, assurez-vous de ne pas supprimer la capacité ou les fonctionnalités existantes.

Cette procédure couvre les utilisations suivantes :

- Le client souhaite déplacer les données du stockage du niveau d'archivage vers le stockage DD Cloud Tier sur le système cible.
- Le client souhaite déplacer les données du stockage du niveau actif et d'archivage du système source vers le stockage du niveau actif du système cible.
- Le client souhaite déplacer les données du stockage du niveau d'archivage sur plusieurs systèmes sources vers le stockage du niveau actif ou DD Cloud Tier sur le système cible.
- Le client souhaite réutiliser le système source ou ses boîtiers de disque une fois l'opération de migration terminée.

Planification de la capacité

Avant de commencer

Le système cible doit avoir une capacité Active Tier suffisante pour pouvoir stocker les niveaux Active et Archive combinés du système source.

En outre, le niveau actif du système source doit disposer de suffisamment d'espace pour conserver toutes les données des sauvegardes planifiées depuis le moment où le transfert des données vers le niveau d'archivage est arrêté jusqu'à ce que la migration du système source vers le système cible soit terminée.

Cette procédure a été développée et testée avec deux systèmes DD9800 et une connexion LAN 10 GbE.

Procédure

1. En utilisant les informations de connexion du compte sysadmin fournis par le client, connectez-vous au système Data Domain source et identifiez la quantité de données acquises dans le niveau actif du système source au cours des sept derniers jours.

   Remarque

   Ces informations peuvent également être extraites du dernier autosupport généré par le périphérique. Si vous utilisez un autosupport pour ces informations, assurez-vous que ces informations sont les plus récentes.

```
# filesys show compression
From: 2018-08-29 17:00 To: 2018-09-05 17:00

Active Tier:
                Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                   (GiB)       (GiB)        Factor       Factor          Factor
                                                                  (Reduction %)
-------------   --------   ---------   -----------   ----------   -------------
Written:
  Last 7 days    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
  Last 24 hrs    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
```

```
-------------   --------   ---------   -----------   ----------   -------------

Archive Tier:
                Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                   (GiB)       (GiB)        Factor       Factor          Factor
…
…
Currently Used:*
               Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                  (GiB)       (GiB)        Factor       Factor          Factor

…
…
       Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100
```

Dans cet exemple, l'acquisition hebdomadaire est d'environ 37 To par semaine, ce qui équivaut à 5,28 To par jour.

2. Sur le système source, exécutez la commande `filesys show space` pour déterminer l'espace libre dans le niveau actif.

```
# filesys show space
Active Tier:
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB*
----------------   --------   --------   ---------   ----   --------------
/data: pre-comp           -    69480.4           -      -                -
/data: post-comp    30352.2       35.5     30316.7     0%              0.0
/ddvar                 47.2        9.2        35.6    21%                -
/ddvar/core           984.3        2.0       932.3     0%                -
----------------   --------   --------   ---------   ----   --------------

Cloud Tier
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -        0.0           -      -               -
/data: post-comp        0.0        0.0         0.0     0%             0.0
----------------   --------   --------   ---------   ----   -------------

Total:
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -    69480.4           -      -               -
/data: post-comp    30352.2       35.5     30316.7     0%             0.0
/ddvar                 47.2        9.2        35.6    21%               -
/ddvar/core           984.3        2.0       932.3     0%               -
----------------   --------   --------   ---------   ----   -------------
 * Estimated based on last cleaning of 2018/09/04 06:03:57.
```

3. Estimez la quantité d'espace consommée au cours du mois précédent, et combien d'espace supplémentaire sera nécessaire jusqu'à ce que la migration vers le système cible soit terminée.
4. Si l'espace disponible dans le niveau actif du système source est inférieur à ce qui est nécessaire, ajoutez du stockage supplémentaire au niveau actif avant de poursuivre la migration.

   ⚠ ATTENTION

   Pour ce faire, il faut arrêter cette procédure et la reprendre après l'ajout du stockage.

5. Procédez au reste des étapes de migration une fois qu'une capacité suffisante est disponible dans le niveau actif du système source.

Arrêt du mouvement des données vers le niveau d'archivage

Procédure

1. Affichez les plannings d'archivage définis sur le système source.

```
# archive data-movement schedule show
Archive data movement is scheduled to run on day(s) "tue" at
"06:00" hrs
```

2. Définissez le planning d'archivage sur never (jamais) afin d'arrêter le mouvement des données.

```
# archive data-movement schedule set never
The archive data-movement schedule will be deleted.
        Are you sure? (yes|no|?) [no]: yes
Ok, proceeding.
The archive data-movement is not scheduled.
```

3. Vérifiez que le planning de mouvement des données est défini sur never (jamais).

```
# archive data-movement schedule show
There is no archive data movement schedule.
```

4. Déterminez si un planning de récupération de l'espace du niveau d'archivage est configuré sur le système source.

```
# archive space-reclamation schedule show
Archive space-reclamation is scheduled to run on day(s) "mon"
at "10:10" hrs
```

5. Définissez le planning de récupération d'espace sur never (jamais) afin d'arrêter le mouvement des données.

```
# archive space-reclamation schedule set never
The archive space-reclamation schedule will be reset to "never".
        Are you sure? (yes|no|?) [no]: yes
 ok, proceeding.
 The archive space-reclamation schedule is reset to "never".
```

6. Vérifiez que le planning de récupération d'espace est défini sur never (jamais).

```
# archive space-reclamation schedule show
Archive space-reclamation does not have any schedule.
```

7. Vérifiez qu'aucun mouvement de données n'est en cours sur le système source.

```
# archive data-movement status
Data-movement was started on Jun 12 2018 06:00 and completed on
Jun 12 2018 06:01
```

8. Vérifiez qu'aucune récupération de l'espace n'est en cours sur le système source.

```
# archive space-reclamation status
Space-reclamation has never been started.
```

9. Si des opérations de mouvement des données ou de récupération de l'espace sont en cours, laissez-les se terminer avant de continuer.

Vérification de l'emplacement des fichiers

Vous pouvez également afficher les structures MTree du système source pour déterminer si les fichiers de chaque structure MTree se trouvent dans le niveau actif ou dans le niveau d'archivage. Cette tâche a un but informatif et n'est pas nécessaire pour compléter le transfert des données du système source au système cible.

Procédure

1. Affichez les structures MTree du système source qui ont une règle de mouvement des données configurée et enregistrez ces informations pour les utiliser lors de la configuration de la réplication sur le système cible.

```
# archive data-movement policy show
The default age-threshold value is "none".
Mtree-name                    Age-threshold
----------------------------  --------------
/data/col1/backup             none (default)
/data/col1/large_files_100gb  1
----------------------------  --------------
```

2. Affichez les emplacements des fichiers d'une structure MTree spécifique.

```
# archive report generate file-location path /data/col1/large_files_100gb
--------------------------------                --------------------------
File Name                                       Location(Tier/Archive Unit)
--------------------------------                --------------------------
/data/col1/large_files_100gb/File_50g.0002.0000  Active
/data/col1/large_files_100gb/File_50g.0001.0000  Active
/data/col1/large_files_100gb/File_50g.0003.0000  archive-unit-2
/data/col1/large_files_100gb/File_50g.0006.0000  archive-unit-2
```

3. Vous pouvez aussi exécuter la commande `archive report generate file-location path all` pour afficher une liste de tous les fichiers présents sur le système.

Remarque

Selon le nombre de fichiers stockés sur le système source, cette commande peut avoir une durée d'opération longue.

Application de la licence de réplication Data Domain

Procédure

1. Affichez les licences sur un système source ayant des licences héritées.

```
# license show
Feature licenses:
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
--   -------------------   ------------------
```

2. Ajoutez la licence de réplication.

```
# license add <license-key>
```

3. Vérifiez que la licence de réplication est ajoutée sur le système source.

```
# license show
Feature licenses:
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
3    EZXW-SZZF-BGCS-VRZX   REPLICATION
--   -------------------   ------------------
```

4. Affichezz les licences sur le système cible avec la licence ELMS.

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
```

```
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                        Count   Mode              Expiration Date
--   ---------------------------   -----   ---------------   ---------------
1    DDBOOST                           1   permanent         n/a
--   ---------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

5. Ajoutez la licence de réplication en mettant à jour la clé de licence obtenue sur le portail de licences. Ouvrez le fichier de licence dans un éditeur de texte, puis copiez et collez-le dans l'invite de mise à jour suivie de **Ctrl + D**.

```
# elicense update
Enter the content of license file and then press Control-D, or
press Control-C to cancel.
```

6. Vérifiez que la licence de réplication est ajoutée sur le système source.

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                        Count   Mode              Expiration Date
--   ---------------------------   -----   ---------------   ---------------
1    REPLICATION                       1   permanent         n/a
2    DDBOOST                           1   permanent         n/a
--   ---------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

Lancement de la réplication d'un système source à un système cible

Notez le nombre maximum optimal de structures MTree et de contextes de réplication qu'un système Data Domain peut avoir. Si le système source possède un nombre de structures MTree supérieur au nombre maximum de contextes de réplication autorisés à la fois, plusieurs contextes de réplication en série peuvent être nécessaires pour transférer les données vers le système cible. Par exemple, le DD860 prend en charge 90 contextes de réplication de structures MTree et le DD990 prend en charge un maximum de 270 contextes de réplication de structures MTree.

Procédure

1. Déterminez le nom d'hôte du système source.

```
# hostname
The Hostname is: Source.ER.FQDN
```

2. Déterminez le nom d'hôte du système cible.

```
# hostname
The Hostname is: Target.DD.FQDN
```

3. Sur le système source, définissez le contexte de réplication MTree sur le système cible.

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
```

```
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

4. Sur le système cible, définissez le contexte de réplication MTree sur le système source.

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

5. Sur le système source, lancez l'opération de réplication. Cette commande n'a pas besoin d'être exécutée sur le système cible.

Remarque

Le temps nécessaire à l'initialisation du contexte de réplication dépend de la quantité de données présentes dans la structure MTree source qui est répliquée pour la première fois.

```
# replication initialize mtree://Target.ER.FQDN/data/col1/
large_files_100gb
(00:08) Waiting for initialize to start...
(00:10) Initialize started.
Use 'replication watch mtree://Target.DDR.FQDN/data/col1/one'
to monitor progress.
```

6. Sur le système source, vérifiez qu'il n'existe aucune erreur dans la configuration de réplication.

Remarque

Le temps nécessaire à l'initialisation du contexte de réplication dépend de la quantité de données présentes dans la structure MTree source qui est répliquée pour la première fois.

```
#  replication status mtree://target.ER.FQDN/data/col1/
large_files_100gb
CTX:                                    1
Mode:                                   source
Destination:                            mtree://Target.DD.FQDN/
data/col1/one
Enabled:                                yes
Low bandwidth optimization:             disabled
Replication encryption:                 enabled
Replication propagate-retention-lock:   enabled
Local filesystem status:                enabled
Connection:                             connected since Tue Jun
12 17:46:14
State:                                  initializing 3/3 0%
Error:                                  no error
Sync'ed-as-of time:                     -
Current throttle:                       unlimited
```

7. Sur le système source, vérifiez que la réplication est en cours.

```
#  replication watch mtree://Source.ER.FQDN/data/col1/large_files_100gb
Use Control-C to stop monitoring.

(00:00) Replication initialize started...
(00:02) initializing:
(00:18)       0% complete, pre-comp: 213183 KB/s, network: 120855 KB/s
(00:22)       0% complete, pre-comp: 246130 KB/s, network: 120719 KB/s
```

Surveillance de la progression de la réplication

Procédure

1. Affichez les détails de configuration pour tous les contextes de réplication MTree sur le système source.

```
# replication show config
```

2. Affichez l'état de progression global de toutes les opérations de réplication en cours.

```
# replication show detailed-stats
```

3. Visualisez la progression d'une opération de réplication spécifique.

```
# replication show detailed-stats mtree://Target.ER.FQDN/data/col1/large_files_100gb
```

4. Affichez les performances de tous les contextes de réplication.

```
# replication show performance all
06/12 17:58:14
       rctx://1               rctx://2               rctx://3
 Pre-comp    Network     Pre-comp    Network     Pre-comp    Network
  (KB/s)     (KB/s)       (KB/s)     (KB/s)       (KB/s)     (KB/s)
 ---------  ---------    ---------  ---------    ---------  ---------
     29459      37607        36374      38071     13089559      39043
    113832      45061        38138      37327     13012122      38812
     29298      42153        33231      36388     12869385      38387
```

Confirmez que l'initialisation de la réplication est terminée ou synchronisée.

Procédure

1. À partir du système source, affichez les statistiques de réplication.

```
# replication show detailed-stats
```

Lorsqu'une opération de réplication est terminée, la sortie affiche une valeur de zéro dans la colonne `Post-comp Bytes Remaining`. La valeur indiquée dans la colonne `Sync'ed-as-of` affiche l'heure la plus récente à laquelle le système source et le système cible sont synchronisés.

2. Si la réplication est toujours en cours, attendez que les opérations soient terminées.
3. Vérifiez que les tailles de structure MTree des systèmes sources et cibles correspondent. Exécutez la commande suivante sur les deux systèmes.

```
# mtree list
Name                          Pre-Comp (GiB)   Status
----------------------------  --------------   ------
/data/col1/large_files_100gb          2500.0   RW
----------------------------  --------------   ------
```

Rupture du contexte de réplication

Avant de commencer

Vérifiez que la structure MTree du système source ne reçoit plus de données.

Procédure

1. Interrompez le contexte de réplication sur le système source.

```
# replication break mtree://Target.DD.FQDN /data/col1/
large_files_100gb
```

2. Interrompez le contexte de réplication sur le système cible.

```
# replication break mtree://Target.DD.FQDN /data/col1/
large_files_100gb
```

3. Vérifiez que le contexte de réplication est rompu sur le système source.

```
# replication show config
```

4. Vérifiez que le contexte de réplication est rompu sur le système cible.

```
# replication show config
```

5. Vérifiez que la structure MTree du système cible est configurée pour la lecture/écriture.

```
# mtree list
Name                          Pre-Comp (GiB)   Status
----------------------------  --------------   ------
/data/col1/large_files_100gb  2500.0           RW
----------------------------  --------------   ------
```

Réutilisation du système source

Avant de commencer

⚠ ATTENTION

Les éléments suivants doivent être complétés avant de réaffecter le système source. N'exécutez pas cette tâche tant que toutes les exigences n'ont pas été satisfaites :

- **Toutes les données du système source sont répliquées dans le système cible.**
- **Toutes les procédures de sauvegarde pointent maintenant vers le système cible.**
- **Toutes les lectures et restaurations des anciennes sauvegardes sont effectuées par le système cible.**
- **Toutes les exigences de conformité sont satisfaites par le système cible.**

Procédure

1. Détruisez et mettez à zéro le système de fichiers sur le système source.

```
# filesys destroy and-zero
```

Remarque

Le niveau d'archivage ne peut pas être désactivé. La seule façon de le supprimer est de détruire le système de fichiers.

2. Identifiez les boîtiers de disque qui ont été rattachés au niveau d'archivage.

```
# storage show tier archive
Archive tier details:
Disk       Disks      Count   Disk       Additional
Group                         Size       Information
-------    --------   -----   --------   -----------
dg2        4.1-4.15   15      1.8 TiB
dg3        3.1-3.15   15      1.8 TiB
```

3. Retirez les boîtiers de stockage du niveau d'archivage du système.

```
# storage remove enclosures 3
Removing enclosure 3...Enclosure 3 successfully removed.
```

```
Updating system information...done

Successfully removed: 3  done

# storage remove enclosures 4
Removing enclosure 4...Enclosure 4 successfully removed.

Updating system information...done

Successfully removed: 4  done
```

4. Vérifiez que les boîtiers du niveau d'archivage sont retirés du système.

```
# storage show all
Active tier details:
Disk      Disks      Count   Disk       Additional
Group                        Size       Information
-------   --------   -----   --------   -----------
dg1       2.1-2.14   14      1.8 TiB
(spare)   2.15       1       1.8 TiB
-------   --------   -----   --------   -----------
Current active tier size: 21.8 TiB
Active tier maximum capacity: 43.7 TiB
Storage addable disks:
Disk        Disks      Count   Disk       Enclosure   Shelf
Capacity   Additional
Type                           Size       Model       License
Needed   Information
---------   --------   -----   --------   ---------
--------------   ---------
(unknown)   3.1-3.15   15      1.8 TiB    ES30        21.8 TiB
(unknown)   4.1-4.15   15      1.8 TiB    ES30        21.8 TiB
---------   --------   -----   --------   ---------
--------------   ---------
```

5. Retirez les boîtiers du niveau d'archivage du rack.

Configuration de DD Cloud Tier sur le système cible

DD Cloud Tier requiert DD OS 6.0.X ou une version ultérieure, et n'est pris en charge que sur certains modèles de systèmes Data Domain. La section Plates-formes prises en charge à la page 516 fournit la liste des modèles prenant en charge DD Cloud Tier. Le stockage DD Cloud Tier et Archive Tier ne peut pas être configuré simultanément sur le même système Data Domain.

Procédure

1. Configurez le stockage à la fois pour le niveau actif et pour le niveau Cloud. Il faut, au préalable, que les licences de capacité appropriées pour le niveau actif et le niveau Cloud soient installées.

   a. Assurez-vous que les licences pour les fonctions CLOUDTIER-CAPACITY et CAPACITY-ACTIVE sont installées. Pour vérifier la licence ELMS :

   ```
   # elicense show
   ```

   Si la licence n'est pas installée, utilisez la commande `elicense update` pour installer la licence. Saisissez la commande et collez le contenu du fichier de licence après cette invite. Assurez-vous qu'un retour chariot a bien été inséré juste après le contenu collé, puis appuyez sur **Contrôle-D** pour enregistrer. Lorsque vous êtes invité à remplacer les licences, répondez yes (oui) pour appliquer et afficher les licences.

   ```
   # elicense update
   Enter the content of license file and then press Control-D,
   or press Control-C to cancel.
   ```

b. Affichez le stockage disponible :

```
# storage show all# disk show state
```

c. Ajoutez le stockage au niveau actif :

```
# storage add enclosures <enclosure no> tier active
```

d. Ajoutez le stockage au niveau Cloud :

```
# storage add enclosures <enclosure no> tier cloud
```

2. Installez les certificats.

   Pour pouvoir créer un profil de Cloud, vous devez installer les certificats associés. Pour plus d'informations, reportez-vous à la section Importation des certificats à la page 633.

   Pour les fournisseurs de Cloud public AWS, Virtustream et Azure, les certificats d'autorité de certification (AC) racine peuvent être téléchargés depuis https://www.digicert.com/digicert-root-certificates.htm.

   - Pour un fournisseur de Cloud AWS ou Azure, téléchargez le certificat Baltimore CyberTrust Root.
   - Pour Alibaba, téléchargez le certificat racine R1 de GlobalSign à partir de https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates.
   - Pour un fournisseur de Cloud Virtustream, téléchargez le certificat DigiCert High Assurance EV Root CA.
   - S'il s'agit d'un fournisseur de Cloud ECS, l'autorité de certification racine varie en fonction du client. Pour plus d'informations, contactez votre fournisseur de répartiteur de charge.

   Les fichiers de certificat téléchargés possèdent l'extension .crt. Utilisez openssl sur tous les systèmes Linux ou Unix où il est installé pour convertir le fichier du format .crt au format .pem.

   ```
   $openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
   -out DigiCertHighAssuranceEVRootCA.pem
   ```

   ```
   $openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
   BaltimoreCyberTrustRoot.pem
   ```

   ```
   # adminaccess certificate import ca application cloud
   Enter the certificate and then press Control-D, or press
   Control-C to cancel.
   ```

3. Pour configurer le système Data Domain en vue du déplacement des données vers le Cloud, vous devez d'abord activer la fonction « Cloud » et définir la phrase secrète du système si elle n'a pas déjà été définie.

   ```
   # cloud enable
   Cloud feature requires that passphrase be set on the system.
   Enter new passphrase:
   Re-enter new passphrase:
   Passphrases matched.
   The passphrase is set.
   Encryption is recommended on the cloud tier.
       Do you want to enable encryption? (yes|no) [yes]:
   Encryption feature is enabled on the cloud tier.
   Cloud feature is enabled.
   ```

4. Configurez le profil de Cloud à l'aide des informations d'identification du fournisseur de Cloud. Les invites et les variables varient selon le fournisseur.

```
# cloud profile add <profilename>
```

Remarque

Pour des raisons de sécurité, cette commande n'affiche pas les clés d'accès/clés secrètes que vous saisissez.

Sélectionnez le fournisseur :

```
Enter provider name (alibabacloud|aws|azure|ecs|google|
s3_flexible|virtustream)
```

- Alibaba Cloud nécessite la saisie de la clé d'accès, de la clé secrète, de la classe de stockage et de la région.
- AWS S3 nécessite la saisie de la clé d'accès, de la clé secrète, de la classe de stockage et de la région.
- Azure nécessite le nom du compte, que le compte soit ou non un compte Azure Government, une clé primaire et une clé secondaire et une classe de stockage.
- ECS requiert la saisie de la clé d'accès, de la clé secrète et du point de terminaison.
- Google Cloud Platform nécessite une clé d'accès, une clé secrète et une région. (La classe de stockage est Nearline.)
- Les fournisseurs S3 Flexible nécessitent le nom du fournisseur, la clé d'accès, la clé secrète, la région, le point de terminaison et la classe de stockage.
- Virtustream nécessite la saisie de la clé d'accès, de la clé secrète, de la classe de stockage et de la région.

À la fin de chaque ajout de profil, vous devez indiquer si vous souhaitez configurer un proxy. Si vous le faites, les valeurs suivantes sont requises : *nom d'hôte du proxy*, *port du proxy*, *nom d'utilisateur du proxy* et *mot de passe proxy*.

5. Vérifiez la configuration du profil Cloud :

   ```
   # cloud profile show
   ```

6. Créez le système de fichiers du niveau actif si ce n'est pas déjà fait :

   ```
   # filesys create
   ```

7. Activez le système de fichiers :

   ```
   # filesys enable
   ```

8. Configurez l'unité de Cloud :

   ```
   # cloud unit add unitname profile profilename
   ```

   Utilisez la commande `cloud unit list` pour répertorier les unités de Cloud.

9. Vous pouvez également configurer le chiffrement pour l'unité de Cloud.

   a. Vérifiez que la licence ENCRYPTION est installée :

      ```
      # elicense show
      ```

   b. Activez le chiffrement pour l'unité de Cloud :

      ```
      # filesys encryption enable cloud-unit unitname
      ```

c. Vérifiez l'état du chiffrement :

```
# filesys encryption status
```

10. Créez une ou plusieurs structures MTree :

```
# mtree create /data/col1/mt11
```

11. Vérifiez la configuration de DD Cloud Tier :

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. Configurez la règle de migration des fichiers pour cette structure MTree. Vous pouvez spécifier plusieurs structures Mtree dans cette commande. La règle peut être basée sur le seuil d'âge ou sur la tranche d'âge.

a. Pour configurer le seuil d'âge (migration des fichiers plus anciens que l'âge indiqué vers le Cloud) :

```
# data-movement policy set age-threshold age_in_days to-tier
cloud cloud-unit unitname mtrees mtreename
```

b. Pour configurer la tranche d'âge (migration uniquement des fichiers appartenant à la tranche d'âge spécifiée) :

```
# data-movement policy set age-range min-age age_in_days max-
age age_in_days to-tier cloud cloud-unit unitname mtrees
mtreename
```

13. Exportez le système de fichiers puis, à partir du client, montez le système de fichiers et procédez à l'acquisition des données dans le niveau actif. Modifiez la date de modification sur les fichiers acquis de façon à ce qu'ils soient désormais éligibles pour la migration des données. (Choisissez une date antérieure à la valeur de seuil d'âge spécifiée lors de la configuration de la règle de déplacement des données).
14. Lancez la migration des fichiers les plus anciens. Une fois encore, vous pouvez spécifier plusieurs structures Mtree avec cette commande.

    ```
    # data-movement start mtrees mtreename
    ```

    Pour vérifier l'état du déplacement des données :

    ```
    # data-movement status
    ```

    Vous pouvez également observer la progression du déplacement des données :

    ```
    # data-movement watch
    ```

15. Assurez-vous que la migration des fichiers a réussi et que les fichiers se trouvent désormais dans le niveau Cloud :

    ```
    # filesys report generate file-location path all
    ```

16. Une fois que vous avez migré un fichier vers le niveau Cloud, il n'est pas possible de lire directement le contenu du fichier (si vous essayez de le faire, un message d'erreur s'affiche). Le fichier peut uniquement être renvoyé vers le niveau actif. Pour rappeler un fichier vers le niveau actif :

    ```
    # data-movement recall path pathname
    ```

CHAPITRE 20

DD Retention Lock

Ce chapitre traite des sujets suivants :

Tour d'horizon de DD Retention Lock

Lorsque les données sont verrouillées sur une structure MTree sur laquelle DD Retention Lock est activé, DD Retention Lock contribue à assurer le maintien de l'intégrité des données. Aucune donnée verrouillée ne peut être remplacée, modifiée ni supprimée pendant une période de rétention définie par l'utilisateur pouvant aller jusqu'à 70 ans.

Il existe deux éditions de DD Retention Lock :

- *Data Domain Retention Lock Governance Edition* conserve les fonctions de Data Domain Retention Lock avant la version DD OS 5.2. Vous pouvez utiliser Data Domain Retention Lock Governance pour définir des règles de rétention des données qui doivent être conservées pendant une durée déterminée pour respecter les règles de gouvernance IT internes mises en œuvre par l'administrateur système.
- *Data Domain Retention Lock Compliance Edition* vous permet de respecter les exigences les plus strictes en matière de permanence des données imposées par les normes réglementaires, comme la norme 17a-4 (f) de la SEC. Liste complète des normes réglementaires :
  - Règle 1.31b de la CFTC
  - 21 CFR Partie 11 de la FDA
  - Loi Sarbanes-Oxley Act
  - 98025 et 97-22 de l'IRS
  - Norme ISO 15489-1
  - MoREQ2010

  Pour obtenir des informations sur la certification, consultez *Compliance Assessments - Summary and Conclusions – EMC Data Domain Retention Lock Compliance Edition* à l'adresse :

  https://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf

  (La connexion est obligatoire.)

  Le respect de ces normes garantit que les fichiers verrouillés sur un système Data Domain à l'aide du logiciel Data Domain Retention Lock Compliance Edition ne pourront pas être modifiés ou détruits avant l'expiration de la période de rétention. Data Domain Retention Lock Compliance Edition nécessite un responsable de la sécurité pour la mise en œuvre des règles. Un fichier log d'audit est à la disposition de l'administrateur ou du responsable de la sécurité.

Chaque édition nécessite une licence de module complémentaire distincte, et il est possible d'en utiliser une seule ou bien les deux dans un même système Data Domain.

Le protocole de verrouillage pour rétention est le même pour les versions DD Retention Lock Governance et Compliance Edition. Les différences d'utilisation résultent du comportement du système avec DD Retention Lock Compliance Edition car ce dernier impose des restrictions strictes afin de respecter les exigences de conformité. Pour obtenir un aperçu, consultez le document *EMC Data Domain Retention Lock Software – A Detailed Review* (livre blanc) disponible à l'adresse :

https://www.emc.com/collateral/hardware/white-papers/h10666-data-domain-retention-lock-wp.pdf

(La connexion est obligatoire.)

DD Retention Lock Governance Edition ne nécessite pas un responsable de la sécurité. Il fournit un niveau plus élevé de flexibilité pour la rétention des données archivées sur des systèmes Data Domain.

En ce qui concerne les exigences de stockage pour la conformité des archives, les règles de la SEC imposent de stocker une copie séparée des données verrouillées pour rétention avec les mêmes exigences en matière de rétention que l'original. Les fichiers verrouillés pour rétention peuvent être répliqués sur un autre système Data Domain à l'aide de DD Replicator. Si un fichier verrouillé pour rétention est répliqué, il demeure verrouillé pour rétention sur le système cible, avec le même niveau de protection que le fichier source.

DD Retention Lock Governance Edition prend en charge les instances DD VE sur site, dans le cloud et DD3300. DD Retention Lock Compliance Edition n'est pas pris en charge pour les instances DD VE sur site, dans le cloud ou DD3300.

Les rubriques suivantes fournissent des Informations supplémentaires sur DD Retention Lock.

Protocole DD Retention Lock

Seuls les fichiers explicitement validés pour être des fichiers verrouillés pour rétention sont verrouillés pour rétention sur le système Data Domain. Les fichiers destinés à être des fichiers verrouillés pour rétention sont validés à l'aide de commandes de fichiers côté client émises lorsque DD Retention Lock Governance ou Compliance est activé sur la MTree contenant les fichiers.

Remarque

Les environnements clients Linux, Unix et Windows sont pris en charge.

Les fichiers écrits sur des partages ou exportations qui ne sont pas validés pour être conservés (même si DD Retention Lock Governance ou Compliance est activé sur la MTree contenant les fichiers) peuvent être modifiés ou supprimés à tout moment.

Le verrouillage pour rétention empêche toute modification ou suppression des fichiers faisant l'objet de la rétention directement à partir des partages CIFS ou des exportations NFS pendant la période de rétention indiquée par une commande de mise à jour *atime* côté client. Certaines applications d'archivage et de sauvegarde peuvent émettre cette commande lorsqu'elles sont correctement configurées. Les applications ou utilitaires qui n'émettent pas cette commande ne peuvent pas verrouiller des fichiers à l'aide de DD Retention Lock.

Les fichiers verrouillés pour rétention sont toujours protégés contre toute modification ou suppression prématurée, même si le verrouillage pour rétention est ensuite désactivé ou si la licence de verrouillage pour rétention n'est plus valide.

Vous ne pouvez donc ni renommer ni supprimer les dossiers ou répertoires qui ne sont pas vides dans la MTree pour laquelle le verrouillage pour rétention est activé. Toutefois, vous pouvez renommer ou supprimer des dossiers ou répertoires vides et en créer de nouveaux.

La période de rétention d'un fichier verrouillé pour rétention peut être allongée (mais pas écourtée) en mettant à jour le paramètre *atime* du fichier.

Qu'il s'agisse de DD Retention Lock Governance ou de DD Retention Lock Compliance, une fois que la période de rétention d'un fichier expire, le fichier peut être supprimé à l'aide d'une commande, d'un script ou d'une application côté client. Toutefois, le fichier ne peut pas être modifié même après l'expiration de la période de rétention de ce fichier. Le système Data Domain ne supprime jamais automatiquement un fichier lorsque sa période de rétention arrive à expiration.

Flux de DD Retention Lock

Flux général des activités avec DD Retention Lock.

1. Activez le verrouillage pour rétention DD Retention Lock Governance ou Compliance sur les MTrees à l'aide des commandes de DD System Manager ou de DD OS émises par la console du système.
2. Validez les fichiers devant être verrouillés pour rétention sur le système Data Domain à l'aide des commandes côté client émises par une application de sauvegarde ou d'archivage correctement configurée, manuellement ou à l'aide de scripts.

   Remarque

   Il se peut que les clients Windows doivent télécharger des utilitaires logiciels pour la compatibilité avec DD OS.
3. Éventuellement, prolongez la durée de rétention des fichiers à l'aide de commandes côté client.
4. Éventuellement, supprimez les fichiers dont les périodes de rétention sont arrivées à expiration à l'aide de commandes côté client.

Protocoles d'accès aux données pris en charge

DD Retention Lock est compatible avec les protocoles non réinscriptibles WORM (Write-Once-Read-Many), basés sur NAS et conformes aux normes de l'industrie, et l'intégration est qualifiée avec les applications d'archivage telles que Symantec Enterprise Vault, SourceOne, Cloud Tiering Appliance ou DiskXtender. Les clients qui utilisent des applications de sauvegarde telles que CommVault peuvent également développer des scripts personnalisés pour utiliser Data Domain Retention Lock.

La prise en charge des protocoles de DD Retention Lock est la suivante :

- NFS est pris en charge par DD Retention Lock Governance et par DD Retention Lock Compliance.
- CIFS est pris en charge par DD Retention Lock Governance et par DD Retention Lock Compliance.
- La librairie de bandes virtuelle (DD VTL) est prise en charge par DD Retention Lock Governance, mais pas par DD Retention Lock Compliance.
  Les bandes virtuelles, ici appelées *bandes*, sont représentées sous forme de fichiers dans le système de fichiers.
  - Lorsque vous créez un pool de stockage (une collection de bandes mappée à un répertoire dans le système de fichiers), vous créez une MTree, sauf si vous choisissez spécifiquement de créer l'ancien style de pool de répertoires (pour la compatibilité descendante). Vous pouvez également convertir les pools de stockage créés avant DD OS 5.3 en structures MTree. Ces MTrees peuvent être verrouillées pour rétention et répliquées.
  - Vous pouvez verrouiller pour rétention une ou plusieurs bandes à l'aide de la commande `vtl tape modify`, décrite dans le *Guide de référence des commandes de Data Domain Operating System*.
    La commande `mtree retention-lock revert`*path* peut être utilisée pour inverser l'état de verrouillage pour rétention des bandes verrouillées avec la

commande `vtl tape modify`. Une fois la bande déverrouillée, des mises à jour peuvent y être apportées. L'état déverrouillé ne sera pas visible via DD System Manager ou l'interface de ligne de commande tant que le service DD VTL n'aura pas été désactivé, puis activé. Cependant, les mises à jour seront appliquées à la bande déverrouillée. Cette fonction est réservée à DD Retention Lock Governance Edition.

  - La durée de rétention des bandes peut être affichée à l'aide de la commande `vtl tape show` avec l'argument `time-display retention`.
  - Vous pouvez verrouiller une bande individuelle pour rétention à l'aide de DD System Manager.

- DD Boost est pris en charge par DD Retention Lock Governance et par DD Retention Lock Compliance.
  Si les scripts côté client sont utilisés pour verrouiller pour rétention des fichiers de sauvegarde ou des images de sauvegarde, et si une application de sauvegarde (Veritas NetBackup, par exemple) est également utilisée sur le système via DD Boost, n'oubliez pas que l'application de sauvegarde peut ne pas partager le contexte des scripts côté client. Donc, lorsqu'une application de sauvegarde tente de faire expirer ou de supprimer des fichiers qui étaient verrouillés pour rétention par le biais de scripts côté client, l'espace n'est pas libéré sur le système Data Domain.

  Data Domain recommande aux administrateurs de modifier leur règle relative à la période de rétention afin de l'aligner sur la durée de verrouillage pour rétention. Cela concerne de nombreuses applications de sauvegarde qui sont intégrées avec DD Boost, y compris Veritas NetBackup, Veritas Backup Exec et NetWorker.

  La définition du verrouillage pour rétention pendant l'acquisition des données dans un fichier DD BOOST en mode DSP n'est pas autorisée, et le client définissant le verrouillage pour rétention reçoit une erreur. Le verrouillage pour rétention doit être défini après l'acquisition des données.

  La définition du verrouillage pour rétention pendant l'acquisition des données dans un fichier DD BOOST en mode OST ou dans un fichier NSF n'est pas autorisée, et le client qui écrit les données reçoit une erreur dès que le verrouillage de la rétention est défini. Le fichier partiel écrit avant le verrouillage pour rétention est défini, puis enregistré sur le disque en tant que fichier WORM.

Activation de DD Retention Lock sur une structure MTree

Seuls les fichiers se trouvant dans des structures MTree pour lesquelles DD Retention Lock Governance ou Compliance a été activé peuvent être verrouillés pour rétention.

Les structures MTree pour lesquelles DD Retention Lock Compliance a été activé ne peuvent pas être converties en structures MTree DD Retention Lock Governance, et inversement.

Les procédures qui suivent décrivent la procédure d'activation de DD Retention Lock Governance ou de DD Retention Lock Compliance pour des structures MTree.

Activation de DD Retention Lock Governance sur une MTree

Ajoutez une licence DD Retention Lock Governance à un système, puis activez DD Retention Lock Governance sur une ou plusieurs MTree.

Procédure

1. Ajoutez la licence DD Retention Lock Governance, si elle n'est pas répertoriée sous Feature Licenses.

a. Sélectionnez **Administration** > **Licenses**

b. Dans la zone Licenses, cliquez sur **Add Licenses**.

c. Dans la zone de texte License Key, saisissez la clé de licence.

Remarque

Les clés de licence ne sont pas sensibles aux majuscules/minuscules. Incluez les traits d'union lors de la saisie des clés.

d. Cliquez sur **Add**.

2. Sélectionnez une MTree pour le verrouillage pour rétention.

a. Sélectionnez **Data Management** > **MTree**.

b. Sélectionnez la MTree que vous souhaitez utiliser pour le verrouillage de la rétention. Vous pouvez également créer une MTree vide et lui ajouter des fichiers par la suite.

3. Cliquez sur l'onglet MTree Summary pour afficher des informations au sujet de la structure MTree sélectionnée.

4. Faites défiler l'écran jusqu'à la zone Retention Lock, puis cliquez sur **Edit** à droite de Retention Lock.

5. Activez DD Retention Lock Governance sur la MTree et modifiez les périodes de rétention minimale et maximale par défaut pour la MTree, le cas échéant.

Exécutez les actions suivantes dans la boîte de dialogue Modify Retention Lock :

a. Sélectionnez **Enable** pour activer DD Retention Lock Governance sur la MTree.

b. Pour modifier la période de rétention minimale ou maximale d'une MTree, modifiez la période minimale ou maximale :

Saisissez un nombre pour l'intervalle dans la zone de texte (par exemple, `5` ou `14`).

Dans la liste déroulante, sélectionnez un intervalle (en minutes, heures, jours, années).

Remarque

La spécification d'une période de rétention minimale de moins de 12 heures, ou d'une période de rétention maximale de plus de 70 ans, entraîne une erreur.

c. Cliquez sur **OK** pour enregistrer les paramètres.

Une fois la boîte de dialogue Modify Retention Lock fermée, les informations actualisées sur la structure MTree s'affichent dans la zone Retention Lock.

6. Vérifiez les informations sur le verrouillage pour rétention de cette MTree.

Examinez les champs de verrouillage pour rétention suivants :

- En haut :
  - Le champ Status indique l'accès en lecture/écriture d'une MTree et le type de verrouillage pour rétention sur la MTree. Il précise également si le verrouillage pour rétention est activé ou désactivé.

- En bas :
  - Le champ Status indique si le verrouillage pour rétention est activé pour cette MTree.
  - Le champ Retention Period indique les périodes de rétention minimale et maximale d'une MTree. La période de rétention définie pour un fichier dans une MTree doit être supérieure ou égale à la période de rétention minimale, et inférieure ou égale à la période de rétention maximale.
  - Le champ UUID est un numéro d'identification unique généré pour la MTree.

Remarque

Pour vérifier les paramètres de configuration du verrouillage pour rétention d'une MTree, sélectionnez la MTree dans le volet de navigation, puis cliquez sur l'onglet Summary.

À effectuer

Fichiers verrouillés pour rétention dans une MTree pour laquelle le verrouillage pour rétention a été activé.

Activation de DD Retention Lock Compliance sur une MTree

Ajoutez une licence DD Retention Lock Compliance à un système, installez un administrateur système et un ou plusieurs responsables de la sécurité, configurez le système et lui permettre d'utiliser le logiciel DD Retention Lock Compliance, puis activez DD Retention Lock Compliance sur une ou plusieurs structures MTree.

Procédure

1. Ajoutez la licence DD Retention Lock Compliance sur le système, si elle n'est pas présente.
   a. Tout d'abord, vérifiez que la licence est déjà installée.

      ```
      license show
      ```

   b. Si la fonction RETENTION-LOCK-COMPLIANCE ne s'affiche pas, installez la licence.

      ```
      license add license-key
      ```

      Remarque

      Les clés de licence ne sont pas sensibles aux majuscules/minuscules. Incluez les traits d'union lors de la saisie des clés.

2. Configurez un ou plusieurs comptes utilisateur de responsable de la sécurité selon les règles de contrôle d'accès basé sur les rôles (RBAC).
   a. Dans le rôle administrateur système, ajoutez un compte de responsable de la sécurité.

      ```
      user add utilisateur role security
      ```

   b. Activez l'autorisation du responsable de la sécurité.

      ```
      authorization policy set security-officer enabled
      ```

3. Configurez et activez le système pour qu'il puisse utiliser DD Retention Lock Compliance.

   Remarque

   L'activation de DD Retention Lock Compliance applique de nombreuses restrictions à l'accès de bas niveau aux fonctions du système utilisées lors du dépannage. Une fois DD Retention Lock Compliance activé, le seul moyen de le désactiver consiste à initialiser et recharger le système, ce qui a pour effet de détruire toutes les données du système.

   a. Configurez le système pour qu'il utilise DD Retention Lock Compliance.

      ```
      system retention-lock compliance configure
      ```

      Le système redémarre automatiquement.

   b. Une fois le processus de redémarrage terminé, activez DD Retention Lock Compliance sur le système.

      ```
      system retention-lock compliance enable
      ```

4. Activez Compliance sur la MTree qui contiendra les fichiers verrouillés pour rétention.

   ```
   mtree retention-lock enable mode compliance mtree mtree-path
   ```

   Remarque

   Compliance ne peut pas être activé sur une sauvegarde ou des MTrees de pool.

5. Pour modifier les périodes minimale et maximale de verrouillage pour rétention d'une MTree pour laquelle Compliance a été activé, saisissez les commandes suivantes avec l'autorisation du responsable de la sécurité.

   ```
   mtree retention-lock set min-retention-
   period period mtree mtree-path
   mtree retention-lock set max-retention-
   period period mtree mtree-path
   ```

   Remarque

   La *durée* de rétention est spécifiée dans le format [nombre] [unité]. Par exemple : 1 minute, 1 heure, 1 jour, 1 mois ou 1 an. La spécification d'une période de rétention minimale de moins de 12 heures, ou d'une période de rétention maximale de plus de 70 ans, entraîne une erreur.

   Répétez les étapes 4 et 5 pour activer des MTrees supplémentaires.

À effectuer

Les fichiers verrouillés pour rétention se trouvent dans une MTree pour laquelle le verrouillage pour rétention a été activé.

Contrôle des fichiers verrouillés pour rétention côté client

Cette section décrit l'interface de commande cliente de DD Retention Lock servant à verrouiller des fichiers stockés sur les systèmes Data Domain. Les commandes clientes sont les mêmes pour DD Retention Lock Governance et pour DD Retention Lock

Compliance Les environnements clients Linux, Unix et Windows sont pris en charge ; cependant, les clients Windows peuvent nécessiter le téléchargement d'utilitaires comportant des commandes de verrouillage des fichiers.

Remarque

Si votre application prend déjà en charge la norme WORM du secteur, écrire un fichier WORM dans une MTree pour laquelle DD Retention Lock Governance ou Compliance a été activé a pour effet de verrouiller le fichier dans le système Data Domain. La durée de rétention dans l'application doit être conforme aux paramètres de DD Retention Lock. Vous n'avez pas besoin d'utiliser les commandes décrites dans cette section. Pour vérifier si une application est testée et certifiée pour DD Retention Lock, consultez le document *Guide de compatibilité de Data Domain Archive Application*.

Remarque

Certains ordinateurs clients utilisant NFS, mais exécutant un système d'exploitation existant, ne peuvent pas définir de durée de rétention ultérieure à 2038. Le protocole NFS n'impose pas la limite de 2038 et permet de spécifier des périodes jusqu'à 2106. Par ailleurs, DD OS n'impose pas la limite de 2038.

Les commandes côté client servent à gérer le verrouillage pour rétention de fichiers individuels. Ces commandes s'appliquent à tous les systèmes Data Domain compatibles avec le verrouillage pour rétention et doivent être émises en plus de la définition et de la configuration de DD Retention Lock sur le système Data Domain.

Outils requis pour les clients Windows

Vous avez besoin de la commande `touch.exe` pour exécuter un verrouillage pour rétention à partir d'un client basé sur Windows.

Pour obtenir cette commande, téléchargez et installez les utilitaires pour applications basées sur Linux/Unix en fonction de votre version de Windows. Data Domain recommande ces utilitaires et ces derniers doivent être utilisés en fonction de l'environnement du client.

- Pour Windows 8, Windows 7, Windows Server 2008, Windows Vista, Windows Server 2003 et Windows XP : http://sourceforge.net/projects/unxutils/files/latest
- Pour Windows Server 2008, Windows Vista Enterprise, Windows Vista Enterprise édition 64 bits, Windows Vista SP1, Windows Vista Ultimate et Windows Vista Ultimate édition 64 bits : http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23754
- Pour Windows Server 2003 SP1 et Windows Server 2003 R2 : http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20983

Remarque

La commande `touch` pour Windows peut avoir un format différent de celui des exemples Linux présentés dans ce chapitre.

Suivez les instructions d'installation fournies et définissez le chemin de recherche comme il convient sur l'ordinateur client.

Accès client aux fichiers du système Data Domain

Une fois qu'une MTree a été activée pour DD Retention Lock Governance ou Compliance, vous pouvez :

- Créer un partage CIFS basé sur cette MTree. Ce partage CIFS peut être utilisé sur une machine client.
- Créer un montage NFS d'une MTree et accéder à ses fichiers à partir du point de montage NFS sur un ordinateur client.

Remarque

Les commandes répertoriées dans cette section doivent être utilisées uniquement sur le client. Elles ne peuvent pas être émises par le biais de DD System Manager ou de l'interface de ligne de commande. La syntaxe de la commande peut varier légèrement en fonction de l'utilitaire que vous utilisez.

Les rubriques suivantes décrivent la façon de gérer le contrôle de fichier de verrouillage pour rétention côté client.

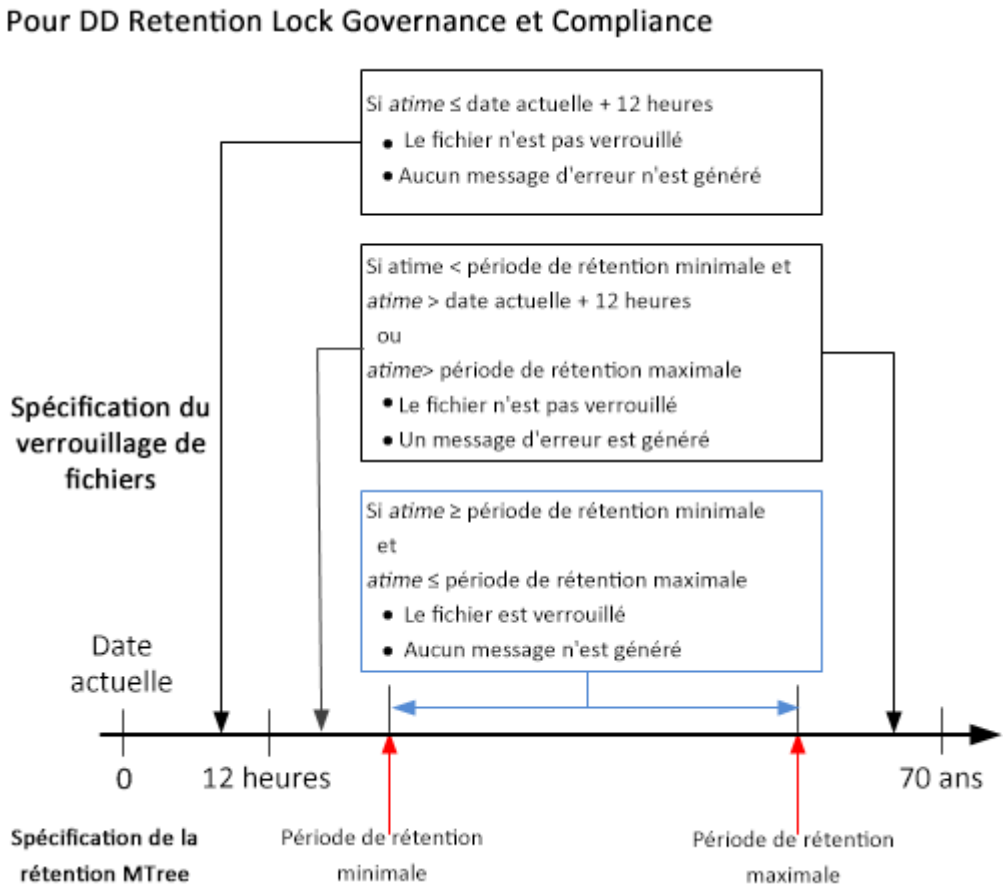
Définition du verrouillage pour rétention sur un fichier

Pour effectuer un verrouillage pour rétention sur un fichier, modifiez la dernière heure d'accès (*atime*) au fichier en choisissant l'heure de rétention voulue du fichier, c'est-à-dire l'heure à laquelle le fichier peut être supprimé.

Cette opération est généralement effectuée par l'application d'archivage. Toutes les applications d'archivage qualifiées aujourd'hui sur des systèmes Data Domain (comme l'indique le *Guide de compatibilité Data Domain Archive Application*) respectent le protocole de verrouillage de base présenté ici.

La future valeur *atime* que vous définissez doit respecter les périodes de rétention minimale et maximale de la MTree du fichier (en tant que décalages par rapport à l'heure actuelle), comme illustré sur la figure suivante.

Figure 23 Valeurs *atimes* valides et non valides pour les fichiers avec verrouillage pour rétention



Remarque

Certains ordinateurs clients utilisant NFS, mais exécutant un système d'exploitation existant, ne peuvent pas définir de durée de rétention ultérieure à 2038. Le protocole NFS n'impose pas la limite de 2038 et permet de spécifier des périodes jusqu'à 2106. Par ailleurs, DD OS n'impose pas la limite de 2038.

Les erreurs sont des erreurs de type refus d'autorisation (appelées EACCESS, erreurs POSIX standard). Elles sont renvoyées au script ou à l'application d'archivage définissant le paramètre *atime*.

Remarque

Un fichier doit être intégralement écrit sur le système Data Domain avant d'être validé pour devenir un fichier Retention-Locked.

La commande suivante peut être utilisée sur les clients pour définir la valeur *atime* :

```
touch -a -t [atime] [filename]
```

Format de la valeur *atime* :

```
[[YY]YY] MMDDhhmm[.ss]
```

Par exemple, supposons que la date et l'heure actuelles soient 13h00 le 18 janvier 2012 (soit 201201181300) et que la période de rétention minimale soit de 12 heures. L'ajout de la période de rétention minimale de 12 heures à cette date et à cette heure entraîne

une valeur de 201201190100. Par conséquent, si la valeur *atime* pour un fichier est définie sur une valeur supérieure à 201201190100, ce fichier sera verrouillé pour rétention.

La commande

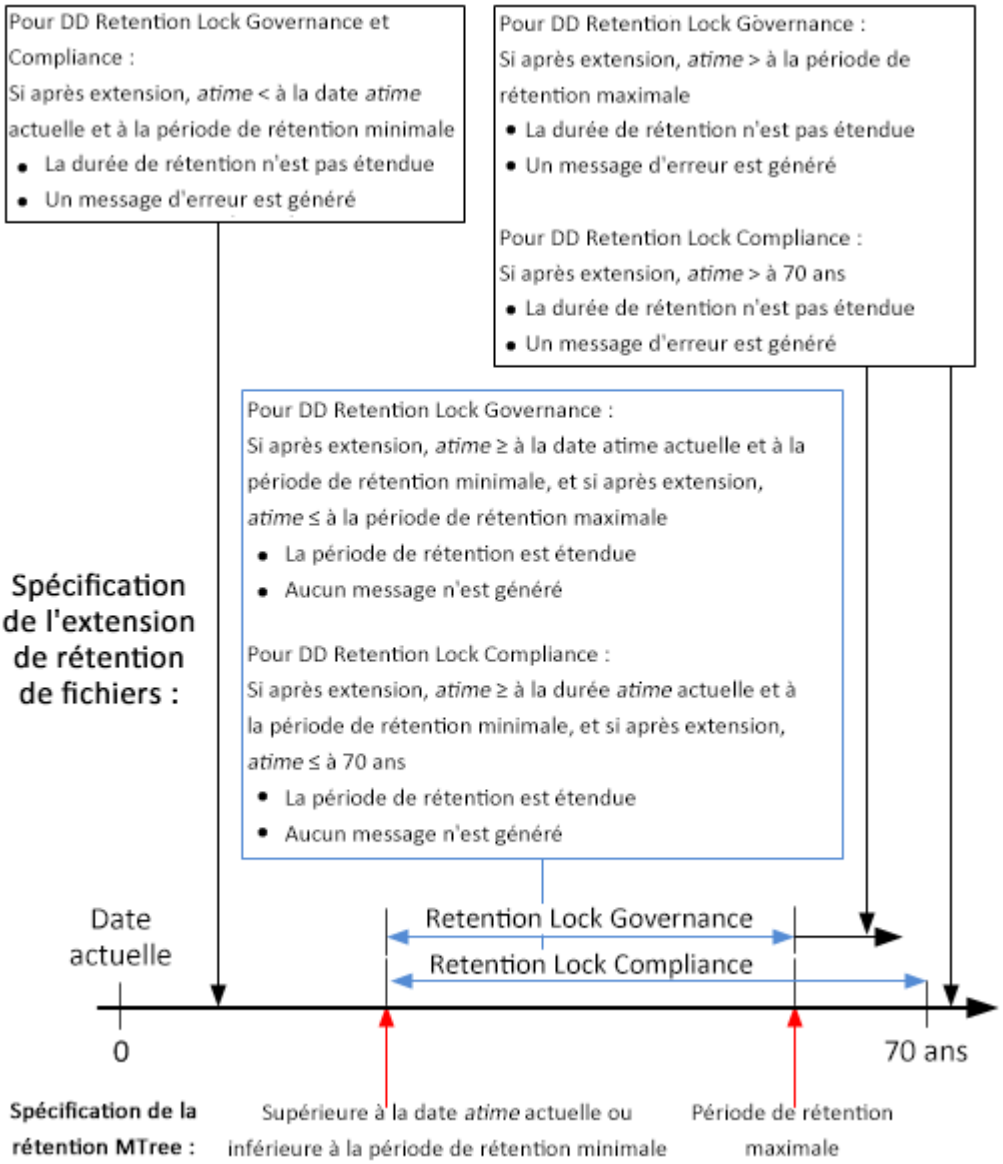
```
ClientOS# touch -a -t 201412312230 SavedData.dat
```

verrouille le fichier `SavedData.dat` jusqu'à 22h30 le 31 décembre 2014.

Extension du verrouillage pour rétention d'un fichier

Pour étendre la durée de rétention d'un fichier Retention-Locked, définissez le paramètre *atime* du fichier sur une valeur supérieure à la valeur *atime* en cours du fichier, mais inférieure à la période de rétention maximale de la MTree du fichier (en décalage par rapport à l'heure actuelle), comme illustré dans la figure suivante.

Figure 24 Valeurs *atimes* valides et non valides pour l'extension du verrouillage pour rétention d'un fichier



Si, par exemple, vous remplacez la valeur *atime* de `201412312230` par `202012121230` à l'aide de la commande :

```
ClientOS# touch -a -t 202012121230 SavedData.dat
```

le fichier sera verrouillé jusqu'à 12:30 le 12 décembre 2020.

Remarque

Certains ordinateurs clients utilisant NFS, mais qui exécutent un système d'exploitation très ancien, ne peuvent pas définir une durée de rétention ultérieure à 2038. Le protocole NFS n'impose pas la limite de 2038 et permet de spécifier des périodes jusqu'à 2106. Par ailleurs, DD OS n'impose pas la limite de 2038.

Les erreurs sont des erreurs de type refus d'autorisation (appelées EACCESS, erreurs POSIX standard). Elles sont renvoyées au script ou à l'application d'archivage définissant le paramètre *atime*.

Identification d'un fichier Retention-Locked

La valeur *atime* d'un fichier Retention-Locked est son heure de rétention. Pour déterminer si un fichier est verrouillé pour rétention, essayez de définir le paramètre *atime* du fichier sur une valeur antérieure à sa valeur *atime* actuelle. Cette action échoue et renvoie une erreur de type autorisation refusée si, et seulement si, le fichier est de type Retention-Locked.

En premier lieu, indiquez la valeur *atime* actuelle. Ensuite, exécutez la commande `touch` avec une valeur *atime* antérieure en utilisant les commandes suivantes :

```
ls -l --time=atime [filename]
touch -a -t [atime] [filename]
```

L'exemple suivant présente la séquence de commandes :

```
ClientOS# ls -l --time=atime SavedData.dat
202012121230
ClientOS# touch -a -t 202012111230 SavedData.dat
```

Si le paramètre *atime* de `SavedData.dat` est 202012121230 (00h30 le 12 décembre 2020) et que la commande `touch` indique une valeur *atime* antérieure, 202012111230 (00h30 le 11 décembre 2020), la commande `touch` échoue, ce qui indique que `SavedData.dat` est verrouillé pour rétention.

Remarque

Les versions d'Unix ne prennent pas toutes en charge l'option `--time=atime`.

Spécification d'un répertoire et intervention sur ces seuls fichiers

Utilisez la ligne de commande pour créer un répertoire racine contenant les fichiers pour lesquels les heures d'accès seront modifiées.

Dans cette procédure de routine, *root directory to start from* contient les fichiers sur lesquels vous souhaitez modifier les heures d'accès à l'aide de cette commande du système client :

```
find [root directory to start from] -exec touch -a -t
[expiration time] {} \;
```

Exemple :

```
ClientOS# find [/backup/data1/] -exec touch -a -t 202012121230 {} \;
```

Lecture d'une liste des fichiers et intervention sur ces seuls fichiers

Dans cette procédure de routine, *name of file list* est le nom d'un fichier texte qui contient les noms des fichiers dont vous souhaitez modifier les heures d'accès. Chaque ligne contient le nom d'un fichier.

Voici la syntaxe d'une commande du système client :

```
touch -a -t [heure d'expiration] 'cat [nom de la liste de fichiers]'
```

Exemple :

```
ClientOS# touch -a -t 202012121230 `cat /backup/data1/filelist.txt`
```

Suppression ou expiration d'un fichier

Supprimez ou faites expirer un fichier dont le verrouillage pour rétention a expiré en utilisant une application client. Vous pouvez également supprimer un fichier à l'aide d'une commande de suppression de fichier classique.

Provoquer l'expiration d'un fichier à l'aide d'une application rend ce fichier inaccessible à l'application. L'opération d'expiration peut ou non supprimer réellement le fichier du système Data Domain. S'il n'est pas supprimé, l'application propose souvent une opération de suppression distincte. Vous devez disposer des droits d'accès appropriés pour supprimer le fichier, indépendamment de DD Retention Lock.

Remarque

Si la période de rétention du fichier verrouillé pour rétention n'est pas arrivée à expiration, l'opération de suppression provoque une erreur d'autorisation refusée.

Suppression avec privilèges

Pour DD Retention Lock Governance (uniquement), vous pouvez supprimer les fichiers verrouillés pour rétention à l'aide de ce processus à deux étapes.

Procédure

1. Utilisez la commande `mtree retention-lock revert` *path* pour rétablir le fichier verrouillé pour rétention.
2. Supprimez le fichier sur le système client à l'aide de la commande `rm` *filename*.

Utilisation de ctime ou mtime sur des fichiers Retention-Locked

ctime correspond à l'heure du dernier changement de métadonnées d'un fichier.

ctime
ctime est défini sur l'heure actuelle lorsque l'un des événements suivants se produit :

- Un fichier non Retention-Locked est verrouillé pour rétention.
- La durée de rétention d'un fichier Retention-Locked est étendue.
- Un fichier Retention-Locked est annulé.

Remarque

Les autorisations d'accès utilisateur pour un fichier Retention-Locked sont mises à jour à l'aide de l'outil de ligne de commande de Linux `chmod`.

mtime
mtime correspond à l'heure de la dernière modification d'un fichier. Il est modifié uniquement lorsque le contenu du fichier change. Donc, la valeur mtime d'un fichier Retention-Locked ne peut pas être modifiée.

Comportement du système avec DD Retention Lock

Les questions relatives au comportement du système sont présentées séparément pour DD Retention Lock Governance et pour DD Retention Lock Compliance dans les sections suivantes.

DD Retention Lock Governance

Certaines commandes de DD OS se comportent différemment avec DD Retention Lock Governance. Les sections suivantes décrivent les différences affectant chacune d'elles.

Réplication

La réplication de collection, la réplication de MTree et la réplication de répertoire répliquent l'état verrouillé ou déverrouillé des fichiers.

Les fichiers verrouillés pour rétention avec Governance sur la source sont verrouillés pour rétention avec Governance sur la destination et ont le même niveau de protection. Pour la réplication, le système source doit disposer d'une licence DD Retention Lock Governance installée. Aucune licence n'est requise pour le système de destination.

La réplication est prise en charge entre des systèmes qui :

- Exécutent de la même version majeure de DD OS (par exemple, les deux systèmes exécutent DD OS 5.5.*x.x*).
- Exécutent des versions de DD OS comprises dans les deux versions supérieures ou inférieures consécutives (par exemple, 5.3.*x.x* vers 5.5.*x.x* ou 5.5.*x.x* vers 5.3.*x.x*). La réplication entre versions est uniquement prise en charge pour la réplication de répertoire et la réplication de MTree.

Remarque

La réplication de MTree n'est pas prise en charge sur DD OS v5.0 et version inférieure.

REMARQUE :

- La réplication de collection et la réplication de MTree répliquent les périodes de rétention minimale et maximale configurées sur les MTrees sur le système de destination.
- La réplication de répertoire ne réplique pas les périodes de rétention minimale et maximale sur le système de destination.

La procédure de configuration et d'utilisation de la réplication de collection, de MTree et de répertoire est la même que pour les systèmes Data Domain qui ne possèdent pas de licence DD Retention Lock Governance.

Resynchronisation de la réplication
La commande `replication resync`*destination* tente de synchroniser la destination avec la source lorsque le contexte de réplication de MTree ou de répertoire est détruit entre les systèmes de destination et source. Cette commande ne peut pas être utilisée avec la réplication de collection. Remarque :

- Si les fichiers sont migrés vers le niveau Cloud avant que le contexte soit rompu, la resynchronisation de réplication MTree remplace toutes les données sur la destination. Il faudra donc recommencer la migration des fichiers vers le niveau Cloud.
- Si DD Retention Lock est activé sur le répertoire de destination, mais pas sur le répertoire source, la resynchronisation d'une réplication de répertoire échoue.
- Avec la réplication de MTree, la resynchronisation échoue si Retention Lock n'est pas activé pour la structure MTree source, contrairement à la structure MTree de destination.
- Avec la réplication MTree, la resynchronisation échoue si Retention Lock est activé sur les structures MTree sources et cibles, alors que l'option propragate retention lock est définie sur FALSE.

Fastcopy

Quand la commande `filesys fastcopy [retention-lock] source` *src*`destination` *dest* est exécutée sur un système comprenant une structure MTree sur laquelle l'option DD Retention Lock Governance est activée, la commande conserve l'attribut de verrouillage de la rétention lors de l'opération de fastcopy.

Remarque

Si la structure MTree cible n'est pas compatible avec le verrouillage de rétention, l'attribut de fichier retention-lock n'est pas conservé.

Filesys destroy

Résultats de la commande `filesys destroy` lorsqu'elle s'exécute sur un système comportant une MTree pour laquelle DD Retention Lock Governance est activé :

- Toutes les données sont détruites, y compris les données verrouillées pour rétention.
- Les valeurs par défaut de toutes les options `filesys` sont rétablies. Cela signifie que le verrouillage pour rétention est désactivé et que les valeurs par défaut des périodes de rétention minimale et maximale sont rétablies sur le système de fichiers nouvellement créé.

Remarque

Cette commande n'est pas autorisée lorsque DD Retention Lock Compliance est activé sur le système.

MTree delete

Lorsque la commande `mtree delete` *mtree-path* tente de supprimer une MTree sur laquelle DD Retention Lock Governance est activé (ou a été précédemment activé) et qui contient actuellement des données, la commande renvoie une erreur.

Remarque

Le comportement de `mtree delete` est identique à celui d'une commande destinée à supprimer un répertoire. Une MTree pour laquelle le verrouillage pour rétention est activé (ou a été précédemment activé) ne peut être supprimée que si elle est vide.

DD Retention Lock Compliance

Certaines commandes de DD OS se comportent différemment lorsque vous utilisez DD Retention Lock Compliance. Les sections suivantes décrivent ces différences entre les deux versions.

Réplication

Une structure MTree pour laquelle DD Retention Lock Compliance est activé peut uniquement être répliquée par l'intermédiaire de la réplication de MTree et de collection. La réplication de répertoire n'est pas prise en charge.

La réplication de MTree et de collection réplique l'état verrouillé ou déverrouillé des fichiers. Les fichiers verrouillés pour rétention avec Compliance sur la source sont verrouillés pour rétention avec Compliance sur la destination et ont le même niveau de protection. Les périodes de rétention minimale et maximale configurées sur les MTrees sont répliquées sur le système de destination.

Pour effectuer la réplication de collection, le même utilisateur responsable de la sécurité doit être présent sur les systèmes source et de destination avant le début de la réplication sur le système de destination, et ensuite pendant la durée de vie de la paire source/réplica.

Resynchronisation de la réplication

La commande `replication resync`*destination* peut être utilisée avec la réplication de MTree, mais pas avec la réplication de collection.

- Si la MTree de destination contient des fichiers verrouillés pour rétention qui n'existent pas sur la source, la resynchronisation échoue.
- Les MTrees source et de destination doivent être activées pour DD Retention Lock Compliance, faute de quoi la resynchronisation échoue.

Procédures de réplication

Les rubriques de cette section décrivent les procédures de réplication de collection et de MTree prises en charge pour DD Retention Lock Compliance.

Remarque

Pour une description complète des commandes auxquelles font référence les rubriques suivantes, consultez le *Guide de référence des commandes de Data Domain Operating System*.

Réplication d'une MTree : Topologie un vers un

Répliquez une structure MTree, sur laquelle DD Retention Lock Compliance a été activé, d'un système source vers un système de destination.

Avant de commencer

Activez DD Retention Lock sur une MTree et configurez le contrôle des fichiers de verrouillage pour rétention côté client avant la réplication.

Procédure

1. Jusqu'à ce que vous receviez une instruction contraire, procédez comme suit sur le système de destination uniquement.
2. Ajoutez la licence DD Retention Lock Compliance sur le système, si elle n'est pas présente.

a. Tout d'abord, vérifiez que la licence est déjà installée.

```
license show
```

b. Si la fonction RETENTION-LOCK-COMPLIANCE ne s'affiche pas, installez la licence.

```
license add license-key
```

Remarque

Les clés de licence ne sont pas sensibles aux majuscules/minuscules. Incluez les traits d'union lors de la saisie des clés.

3. Configurez un ou plusieurs comptes utilisateur de responsable de la sécurité selon les règles de contrôle d'accès basé sur les rôles (RBAC).

a. Dans le rôle administrateur système, ajoutez un compte de responsable de la sécurité.

```
user add utilisateur role security
```

b. Activez l'autorisation du responsable de la sécurité.

```
authorization policy set security-officer enabled
```

4. Configurez et activez le système pour qu'il puisse utiliser DD Retention Lock Compliance.

Remarque

L'activation de DD Retention Lock Compliance applique de nombreuses restrictions à l'accès de bas niveau aux fonctions du système utilisées lors du dépannage. Une fois DD Retention Lock Compliance activé, le seul moyen de le désactiver consiste à initialiser et recharger le système, ce qui a pour effet de détruire toutes les données du système.

a. Configurez le système pour qu'il utilise DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

Le système redémarre automatiquement.

b. Une fois le processus de redémarrage terminé, activez DD Retention Lock Compliance sur le système.

```
system retention-lock compliance enable
```

5. Créez un contexte de réplication.

```
replication add source mtree://source-system-name/data/
col1/mtree-name destination mtree://destination-system-
name/data/col1/mtree-name
```

6. Appliquez la procédure suivante sur le système source uniquement.
7. Créez un contexte de réplication.

```
replication add source mtree://source-system-name/data/
col1/mtree-name destination mtree://destination-system-
name/data/col1/mtree-name
```

8. Initialisez le contexte de réplication.

```
replication initialize mtree://destination-system-name/
data/col1/mtree-name
```

9. Confirmez que la réplication est terminée.

   ```
   replication status mtree://destination-system-name/data/
   col1/mtree-namedetailed
   ```

   Cette commande indique 0 octet précompressé restant une fois la réplication terminée.

Réplication d'une MTree : Topologie un vers plusieurs

Répliquez une structure MTree, sur laquelle DD Retention Lock Compliance a été activé, d'un système source vers plusieurs systèmes de destination.

Avant de commencer

Activez DD Retention Lock Compliance sur une MTree et configurez le contrôle des fichiers de verrouillage pour rétention côté client avant la réplication.

Procédure

1. Jusqu'à ce que vous receviez une instruction contraire, procédez comme suit sur le système de destination uniquement.
2. Ajoutez la licence DD Retention Lock Compliance sur le système, si elle n'est pas présente.
   a. Tout d'abord, vérifiez que la licence est déjà installée.

      ```
      license show
      ```

   b. Si la fonction RETENTION-LOCK-COMPLIANCE ne s'affiche pas, installez la licence.

      ```
      license addlicense-key
      ```

      Remarque

      Les clés de licence ne sont pas sensibles aux majuscules/minuscules. Incluez les traits d'union lors de la saisie des clés.

3. Configurez un ou plusieurs comptes utilisateur de responsable de la sécurité selon les règles de contrôle d'accès basé sur les rôles (RBAC).
   a. Dans le rôle administrateur système, ajoutez un compte de responsable de la sécurité.

      ```
      user addutilisateurrole security
      ```

   b. Activez l'autorisation du responsable de la sécurité.

      ```
      authorization policy set security-officer enabled
      ```

4. Configurez et activez le système pour qu'il puisse utiliser DD Retention Lock Compliance.

   Remarque

   L'activation de DD Retention Lock Compliance applique de nombreuses restrictions à l'accès de bas niveau aux fonctions du système utilisées lors du dépannage. Une fois DD Retention Lock Compliance activé, le seul moyen de le désactiver consiste à initialiser et recharger le système, ce qui a pour effet de détruire toutes les données du système.

a. Configurez le système pour qu'il utilise DD Retention Lock Compliance.

```
system retention-lock compliance configure
```

Le système redémarre automatiquement.

b. Une fois le processus de redémarrage terminé, activez DD Retention Lock Compliance sur le système.

```
system retention-lock compliance enable
```

5. Créez un contexte de réplication.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

6. Appliquez la procédure suivante sur le système source uniquement.
7. Créez un contexte de réplication pour chaque système de destination.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

8. Initialisez le contexte de réplication pour chaque MTree du système de destination.

```
replication initialize mtree://destination-system-name/
data/col1/mtree-name
```

9. Assurez-vous que la réplication est terminée pour chaque système de destination.

```
replication status mtree://destination-system-name/data/
col1/mtree-namedetailed
```

Cette commande indique 0 octet précompressé restant une fois la réplication terminée.

Ajout d'une protection DD Retention Lock Compliance à une paire de réplication de MTree existante

Ajoutez une protection Retention Lock Compliance à une paire de réplication de MTree existante pour laquelle le verrouillage pour rétention n'est pas activé.

Procédure

1. Jusqu'à ce que vous receviez une instruction contraire, appliquez la procédure suivante aux systèmes source et de destination.
2. Connectez-vous à DD System Manager.

   La fenêtre DD System Manager s'affiche et indique **DD Network** dans le volet de navigation.

3. Sélectionnez un système Data Domain.

   Dans le volet de navigation, développez **DD Network** et sélectionnez un système.

4. Ajoutez la licence DD Retention Lock Governance, si elle n'est pas répertoriée sous Feature Licenses.

   a. Sélectionnez **Administration** > **Licenses**

   b. Dans la zone Licenses, cliquez sur **Add Licenses**.

   c. Dans la zone de texte License Key, saisissez la clé de licence.

Remarque

Les clés de licence ne sont pas sensibles aux majuscules/minuscules. Incluez les traits d'union lors de la saisie des clés.

d. Cliquez sur **Add**.

5. Brisez le contexte de MTree actuel sur la paire de réplication.

   `replication break mtree://`*`destination-system-name`*`/data/col1/`*`mtree-name`*

6. Créez le nouveau contexte de réplication.

   `replication add source mtree://`*`source-system-name`*`/data/col1/`*`mtree-name`*`destination mtree://`*`destination-system-name`*`/data/col1/`*`mtree-name`*

7. Appliquez la procédure suivante sur le système source uniquement.
8. Sélectionnez une MTree pour le verrouillage pour rétention.

   Cliquez sur l'onglet **Data Management** > **MTree**, puis cochez la case en regard de la MTree à utiliser pour le verrouillage pour rétention. (Vous pouvez également créer une MTree vide et lui ajouter des fichiers par la suite.)

9. Cliquez sur l'onglet MTree Summary pour afficher des informations au sujet de la structure MTree sélectionnée.
10. Verrouillez les fichiers dans la MTree pour laquelle Compliance a été activé.
11. Assurez-vous que les MTrees source et de destination (réplica) sont identiques.

    `replication resync mtree://`*`destination-system-name`*`/data/col1/`*`mtree-name`*

12. Vérifiez la progression de la resynchronisation.

    `replication watch mtree://`*`destination-system-name`*`/data/col1/`*`mtree-name`*

13. Confirmez que la réplication est terminée.

    `replication status mtree://`*`destination-system-name`*`/data/col1/`*`mtree-name`*`detailed`
    Cette commande indique 0 octet précompressé restant une fois la réplication terminée.

Conversion d'une paire de réplication de collection en paires de réplication de MTree

Procédure destinée aux clients ayant utilisé la réplication de collection sous DD Retention Lock Compliance dans DD OS 5.2 et qui souhaitent convertir, vers des paires de réplication de MTree, les MTrees pour lesquelles Compliance a été activé dans les paires de réplication de collection.

Procédure

1. Sur le système source uniquement :

   a. Créez un snapshot pour chaque MTree pour laquelle DD Retention Lock Compliance a été activé.

      `snapshot create`*`snapshot-name`* `/data/col1/`*`mtree-name`*

   b. Synchronisez la paire de réplication de collection.

```
replication sync col://destination-system-name
```

c. Confirmez que la réplication est terminée.

```
replication status col://destination-system-namedetailed
```

Cette commande indique 0 octet précompressé restant une fois la réplication terminée.

d. Affichez les informations relatives au snapshot pour chaque MTree pour laquelle DD Retention Lock Compliance a été activé.

```
snapshot list mtree /data/col1/mtree-name
```

Notez les noms des snapshots pour une utilisation ultérieure.

2. Sur le système de destination uniquement :

a. Confirmez que la réplication est terminée.

```
replication status mtree://destination-system-name/data/
col1/mtree-namedetailed
```

Cette commande indique 0 octet précompressé restant une fois la réplication terminée.

b. Affichez chaque snapshot de MTree répliqué sur le système de destination.

```
snapshot list mtree /data/col1/mtree-name
```

c. Assurez-vous que tous les snapshots de MTree DD Retention Lock Compliance ont été répliqués en comparant les noms des snapshots générés ici à ceux produits sur le système source.

```
snapshot list mtree /data/col1/mtree-name
```

3. Sur les systèmes source et de destination :

a. Désactivez le système de fichiers.

```
filesys disable
```

b. Brisez le contexte de réplication de collection.

```
replication break col://destination-system-name
```

c. Activez le système de fichiers. (L'autorisation du responsable de la sécurité peut être nécessaire)

```
filesys enable
```

d. Ajoutez un contexte de réplication pour chaque MTree pour laquelle DD Retention Lock Compliance a été activé.

```
replication add source mtree://source-system-name/data/
col1/mtree-namedestination mtree://destination-system-
name/data/col1/mtree-name
```

Remarque

Les noms des MTrees source et de destination doivent être identiques.

4. Sur le système source uniquement :

a. Assurez -vous que les MTrees source et de destination sont identiques.

```
replication resync mtree://destination-system-name
```

b. Vérifiez la progression de la resynchronisation.

```
replication watchdestination
```

c. Confirmez que la réplication est terminée.

```
replication status mtree://destination-system-name/data/
col1/mtree-namedetailed
```

Cette commande indique 0 octet précompressé restant une fois la réplication terminée.

Exécution de la réplication de collection

Répliquez /data/col1 à partir d'un système source vers un système cible sur lesquels Compliance est activé.

Remarque

Pour la réplication de collection, le même compte de responsable de la sécurité doit être utilisé sur les systèmes source et de destination.

Procédure

1. Jusqu'à ce que vous receviez une instruction contraire, procédez comme suit sur le système source uniquement.
2. Connectez-vous à DD System Manager.

   La fenêtre DD System Manager s'affiche et indique **DD Network** dans le volet de navigation.
3. Sélectionnez un système Data Domain.

   Dans le volet de navigation, développez **DD Network** et sélectionnez un système.
4. Ajoutez la licence DD Retention Lock Governance, si elle n'est pas répertoriée sous Feature Licenses.
   a. Sélectionnez **Administration** > **Licenses**
   b. Dans la zone Licenses, cliquez sur **Add Licenses**.
   c. Dans la zone de texte License Key, saisissez la clé de licence.

   Remarque

   Les clés de licence ne sont pas sensibles aux majuscules/minuscules. Incluez les traits d'union lors de la saisie des clés.

   d. Cliquez sur **Add**.
5. Créez le contexte de réplication.

   ```
   replication add source col://source-system-name
   destination col://destination-system-name
   ```
6. Jusqu'à ce que vous receviez une instruction contraire, procédez comme suit sur le système cible uniquement.
7. Détruisez le système de fichiers.

   ```
   filesys destroy
   ```
8. Connectez-vous à DD System Manager.

   La fenêtre DD System Manager s'affiche et indique **DD Network** dans le volet de navigation.

9. Sélectionnez un système Data Domain.

   Dans le volet de navigation, développez **DD Network** et sélectionnez un système.

10. Créez un système de fichiers, mais ne l'activez pas.

    ```
    filesys create
    ```

11. Créez le contexte de réplication.

    ```
    replication add source col://source-system-name
    destination col://destination-system-name
    ```

12. Configurez et activez le système pour qu'il puisse utiliser DD Retention Lock Compliance.

    ```
    system retention-lock compliance configure
    ```

    (Le système redémarre automatiquement et exécute la commande `system retention-lock compliance enable`.)

13. Appliquez la procédure suivante sur le système source uniquement.
14. Initialisez le contexte de réplication.

    ```
    replication initialize source col://source-system-
    namedestination col://destination-system-name
    ```

15. Confirmez que la réplication est terminée.

    ```
    replication status col://destination-system-namedetailed
    ```

    Cette commande indique 0 octet précompressé restant une fois la réplication terminée.

Ajout d'une protection DD Retention Lock Compliance à une paire de réplication de collection existante

Ajoutez une protection DD Retention Lock Compliance à une paire de réplication de collection créée sans que DD Retention Lock Compliance ne soit activé sur les systèmes source et de destination.

Procédure

1. Jusqu'à ce que vous receviez une instruction contraire, appliquez la procédure suivante aux systèmes source et de destination.
2. Désactivez la réplication.

   ```
   replication disable col://destination-system-name
   ```

3. Connectez-vous à DD System Manager.

   La fenêtre DD System Manager s'affiche et indique **DD Network** dans le volet de navigation.

4. Sélectionnez un système Data Domain.

   Dans le volet de navigation, développez **DD Network** et sélectionnez un système.

5. Jusqu'à ce que vous receviez une instruction contraire, appliquez la procédure suivante au système source.
6. Configurez et activez le système pour qu'il puisse utiliser DD Retention Lock Compliance.

   ```
   system retention-lock compliance configure
   ```

(Le système redémarre automatiquement en exécutant la commande `system retention-lock compliance enable`.)

7. Activez le contexte de réplication.

   `replication enable col://`*`destination-system-name`*

8. Jusqu'à ce que vous receviez une instruction contraire, appliquez la procédure suivante au système cible.
9. Configurez et activez le système pour qu'il puisse utiliser DD Retention Lock Compliance.

   `system retention-lock compliance configure`

   (Le système redémarre automatiquement en exécutant la commande `system retention-lock compliance enable`.)

10. Activez le contexte de réplication.

    `replication enable col://`*`destination-system-name`*

Fastcopy

Quand la commande `filesys fastcopy [retention-lock] source` *`src`*`destination` *`dest`* est executée sur un système comprenant une structure MTree sur laquelle l'option DD Retention Lock Governance est activée, la commande conserve l'attribut de verrouillage de la rétention lors de l'opération de fastcopy.

Remarque

Si la structure MTree de destination n'est pas compatible avec le verrouillage de rétention, l'attribut de fichier retention-lock n'est pas conservé.

Utilisation de l'interface de ligne de commande

Remarques pour un système Data Domain avec l'option DD Retention Lock Compliance.

- Les commandes qui ne respectent pas la conformité ne s'exécutent pas. Les commandes suivantes ne sont pas autorisées :
  - `filesys archive unit del`*`archive-unit`*
  - `filesys destroy`
  - `mtree delete`*`mtree-path`*
  - `mtree retention-lock reset {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
  - `mtree retention-lock disable mtree`*`mtree-path`*
  - `mtree retention-lock revert`
  - `user reset`
- La commande suivante nécessite l'autorisation du responsable de la sécurité si la licence en cours de suppression est destinée à DD Retention Lock Compliance :
  - `license del license-feature [`*`license-feature`* `...] | license-code [`*`license-code`* `...]`
- Les commandes suivantes nécessitent l'autorisation du responsable de la sécurité si DD Retention Lock Compliance est activé sur une MTree spécifiée dans la commande :

- `mtree retention-lock set {min-retention-period`*`period`* `| max-retention-period`*`period`*`} mtree`*`mtree-path`*
- `mtree rename`*`mtree-path new-mtree-path`*

- Les commandes suivantes nécessitent l'autorisation du responsable de la sécurité si DD Retention Lock Compliance est activé sur le système :

  Remarque

  Ces commandes doivent être exécutées en mode interactif.

  - `alerts notify-list reset`
  - `config set timezone`*`zonename`*
  - `config reset timezone`
  - `cifs set authentication active-directory realm { [`*`dc1`*` [`*`dc2`*` ...]]`
  - `license reset`
  - `ntp add timeserver`*`time server list`*
  - `ntp del timeserver`*`time server list`*
  - `ntp disable`
  - `ntp enable`
  - `ntp reset`
  - `ntp reset timeservers`
  - `replication break {`*`destination`*` | all}`
  - `replication disable {`*`destination`*` | all}`
  - `system set date`*`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]`

Horloge du système

DD Retention Lock Compliance met en œuvre une horloge de sécurité interne pour éviter les altérations malveillantes de l'horloge du système.

L'horloge de sécurité surveille étroitement et consigne l'horloge du système. S'il existe une désynchronisation accumulée de deux semaines au cours d'une année entre l'horloge de sécurité et l'horloge du système, le système de fichiers est désactivé et ne peut être réactivé que par un responsable de la sécurité.

Identification de la désynchronisation de l'horloge du système
Vous pouvez exécuter la commande DD OS `system retention-lock compliance status` (l'autorisation du responsable de la sécurité est requise) pour obtenir des informations sur le système et sur l'horloge de sécurité, notamment la dernière valeur enregistrée de l'horloge de sécurité et la variation accumulée de l'horloge du système. Cette valeur est mise à jour toutes les 10 minutes.

Suppression de la désynchronisation de l'horloge du système

La désynchronisation de l'horloge est mise à jour chaque fois que l'horloge de sécurité enregistre une nouvelle valeur pour l'horloge du système. Après 1 an, elle est remise à 0.

Vous pouvez à tout moment exécuter la commande de DD OS `system set date`*`MMDDhhmm`*`[[`*`CC`*`]`*`YY`*`]` pour définir l'heure de l'horloge du système (l'autorisation du responsable de la sécurité est requise). Si la désynchronisation de l'horloge est supérieure à la valeur prédéfinie (2 semaines), le système de fichiers est désactivé.

Procédez comme suit pour redémarrer le système de fichiers et supprimer la désynchronisation entre l'horloge de sécurité et l'horloge du système.

Procédure

1. Activez le système de fichiers sur la console du système.

   ```
   filesys enable
   ```

2. À l'invite, confirmez que vous souhaitez quitter la commande `filesys enable` et vérifiez si la date du système est exacte.
3. Affichez la date du système.

   ```
   system show date
   ```

4. Si la date du système est incorrecte, définissez la date correcte (l'autorisation du responsable de la sécurité est requise) et confirmez-la.

   ```
   system set dateMMDDhhmm[[CC]YY]
   system show date
   ```

5. Réactivez le système de fichiers.

   ```
   filesys enable
   ```

6. À l'invite, poursuivez la procédure d'activation.
7. Une invite du responsable de la sécurité s'affiche. Terminez l'autorisation du responsable de la sécurité pour démarrer le système de fichiers. L'horloge de sécurité est automatiquement mise à jour en fonction de la date actuelle du système.

CHAPITRE 21

DD Encryption

Ce chapitre traite des sujets suivants :

Présentation du chiffrement DD

La fonction de chiffrement des données protège les données des utilisateurs en cas de vol du système Data Domain ou de perte de supports de stockage physique lors d'un transport. Elle élimine également le risque d'exposition accidentelle des données d'un disque défaillant que l'on doit remplacer.

Lorsque les données sont introduites dans le système Data Domain à l'aide de l'un des protocoles pris en charge (NFS, CIFS, DD VTL, DD Boost et serveur de bandes NDMP), leur flux est segmenté, marqué d'une empreinte et dédupliqué (compression globale). Elles sont ensuite regroupées dans des zones de compression multisegments, localement compressées et chiffrées avant d'être stockées sur disque.

Lorsqu'elle est activée, la fonction de chiffrement des données inactives chiffre toutes les données qui pénètrent dans le système Data Domain. Vous ne pouvez pas activer le chiffrement des données à un niveau plus granulaire.

⚠ ATTENTION

Les données qui ont été stockées avant que la fonction de chiffrement de DD ne soit activée ne sont pas automatiquement chiffrées. Pour protéger toutes les données du système, veillez à activer la fonction afin de chiffrer les données existantes lorsque vous configurez le chiffrement.

Remarques supplémentaires :
À partir de la version 5.5.1.0 de DD OS, la fonction de chiffrement des données inactives est prise en charge sur les systèmes dotés de l'option DD Extended Retention avec une seule unité de rétention. À partir de la version 5.5.1.0, l'option DD Extended Retention ne prend en charge qu'une seule unité de rétention, de sorte que les systèmes installés pendant ou après cette version seront parfaitement conformes à cette restriction. Toutefois, les systèmes installés avant la version 5.5.1.0 peuvent posséder plusieurs unités de rétention. Dès lors, ils ne peuvent utiliser la fonction de chiffrement des données inactives jusqu'à ce que toutes les unités de rétention sauf une ne soient supprimées, ou que les données ne soient déplacées ou migrées vers une seule unité de rétention.

La commande `filesys encryption apply-changes` applique toutes les modifications apportées à la configuration du chiffrement à l'ensemble des données présentes sur le système de fichiers lors du prochain cycle de nettoyage. Pour plus d'informations sur cette commande, consultez le *Guide de référence des commandes de Data Domain Operating System*.

La fonction de chiffrement des données inactives prend en charge toutes les applications de sauvegarde actuellement prises en charge, décrites dans les guides de compatibilité des sauvegardes, disponibles sur le site Web du support en ligne à l'adresse : http://support.emc.com.

Data Domain Replicator peut être utilisé avec l'option de chiffrement, ce qui permet aux données chiffrées d'être répliquées à l'aide de la réplication de fichiers gérés spécifique de l'application, la structure MTree, le répertoire ou la collection avec les différentes topologies. Chaque forme de réplication fonctionne de manière unique avec le chiffrement et offre le même niveau de sécurité. Pour plus d'informations, reportez-vous à la section relative à l'utilisation du chiffrement des données inactives avec la réplication.

Les fichiers verrouillés à l'aide de Data Domain Retention Lock peuvent être stockés, chiffrés et répliqués.

La fonction d'autosupport contient des informations sur l'état du chiffrement sur le système Data Domain :

- Si le chiffrement est activé ou non
- Le gestionnaire de clés et les clés utilisées
- L'algorithme de chiffrement configuré
- L'état du système de fichiers

Configuration du chiffrement

Cette procédure inclut la configuration d'un gestionnaire de clés.

Si l'état de chiffrement indiqué sur l'onglet **Data Management** > **File System** > **Encryption** est « Not Configured », cliquez sur **Configure** pour définir un chiffrement sur le système Data Domain.

Remarque

La phrase de passe système doit être définie pour pouvoir activer le chiffrement.

Fournissez les informations suivantes :

- Algorithme
  - Sélectionnez un algorithme de chiffrement dans la liste déroulante ou acceptez le mode AES 256-bit (CBC) par défaut.
    Le mode AES 256-bit GCM (Galois Counter Mode) est l'algorithme le plus sécurisé, mais il est plus lent que le mode CBC (Cipher Block Chaining).
  - Déterminez les données à chiffrer : uniquement les nouvelles données ou les données existantes et les nouvelles données. Les données existantes seront chiffrées lors du premier cycle de nettoyage après le redémarrage du système de fichiers. Le chiffrement des données existantes peut prendre plus de temps qu'une opération de nettoyage standard du système de fichiers.
- Key Manager (sélectionnez l'un des trois)
  - Embedded Key Manager
    Le Embedded Key Manager Data Domain est activé par défaut après le redémarrage du système de fichiers, sauf si vous avez configuré RSA DPM Key Manager.

    Vous pouvez activer ou désactiver la rotation des clés. Si cette option est activée, saisissez un intervalle de rotation compris entre 1 à 12 mois.
  - RSA DPM Key Manager
  - SafeNet KeySecure Key Manager

  Remarque

  Consultez la section relative à la gestion des clés pour savoir comment Embedded Key Manager, RSA DPM Key Manager et SafeNet KeySecure Key Manager fonctionnent.

Le récapitulatif affiche les valeurs de configuration sélectionnées. Vérifiez-les. Pour modifier une valeur, cliquez sur **Back** pour accéder à la page de saisie et modifiez-la.

Le système doit être redémarré pour activer le chiffrement. Pour appliquer la nouvelle configuration, sélectionnez l'option permettant de redémarrer le système de fichiers.

Remarque

Les applications peuvent subir une interruption pendant le redémarrage du système de fichiers.

À propos de la gestion des clés

Les clés de chiffrement déterminent le résultat de l'algorithme de chiffrement. Elles sont protégées par une phrase de passe, qui est utilisée pour chiffrer la clé de chiffrement avant son stockage à plusieurs emplacements du disque. Cette phrase de passe est générée par l'utilisateur et ne peut être modifiée que par un administrateur et un responsable de la sécurité.

Un gestionnaire de clés contrôle la génération, la distribution et la gestion du cycle de vie des différentes clés de chiffrement. Un système Data Domain peut utiliser Embedded Key Manager, RSA DPM Key Manager (DPM) ou SafeNet KeySecure Key Manager. La prise en charge de KMIP (Key Management Interoperability Protocol) est introduite avec DD OS 6.1.

Un seul peut être activé à la fois. Lorsque le chiffrement est activé sur un système Data Domain, Embedded Key Manager est activé par défaut. Si vous configurez RSA DPM ou SafeNet KeySecure Key Manager, celui-ci remplace Embedded Key Manager et reste en vigueur jusqu'à ce que vous le désactiviez. Le système de fichiers doit être redémarré pour qu'un nouveau gestionnaire de clés soit opérationnel.

Les deux gestionnaires de clés Embedded et DPM fournissent plusieurs clés, bien que le système n'utilise qu'une clé à la fois pour chiffrer les données entrantes dans un système Data Domain. Lorsque le Key Manager est configuré et activé, les systèmes Data Domain utilisent les clés fournies par le serveur RSA DPM Key Manager. Lorsque le même DPM Key Manager gère plusieurs systèmes Data Domain, tous partagent la même clé active (s'ils utilisent la même classe de clés) lorsque les systèmes sont synchronisés et que le système de fichiers Data Domain a été redémarré. Embedded Key Manager génère ses clés en interne.

Les deux gestionnaires de clés procèdent à une rotation des clés et prennent en charge jusqu'à 254 clés. Embedded Key Manager vous permet d'indiquer la durée de validité (en mois) d'une clé avant qu'elle soit remplacée (après le redémarrage du système de fichiers). RSA DPM Key Manager procède à une rotation normale des clés, en fonction de leur classe. La rotation des clés effectuée par Embedded Key Manager est gérée sur le système Data Domain. La rotation des clés effectuée par Key Manager est gérée sur le serveur Key Manager externe.

KeySecure

KeySecure 8.5 et 8.9 est pris en charge. Il s'agit d'un produit gestionnaire de clés compatible KMIP de Safenet Inc/Gemalto Keysecure. Pour pouvoir utiliser le gestionnaire de clés KMIP, les utilisateurs doivent configurer le gestionnaire de clés et le système Data Domain/DD VE, de sorte que ceux-ci se fassent mutuellement confiance. Les utilisateurs doivent créer au préalable des clés sur le gestionnaire de clés. Un système Data Domain permet d'extraire ces clés et leurs états auprès de KeySecure après avoir établi une connexion TLS sécurisée. Reportez-vous au *Guide d'intégration Gemalto et KeySecure de Data Domain Operating System* pour plus d'informations sur la création des clés et leur utilisation sur un système Data Domain.

Rectification des clés perdues ou corrompues

Créez un fichier contenant toutes les clés de chiffrement actuelles de votre système. Votre fournisseur de services peut utiliser ce fichier pour importer à nouveau les clés

vers votre système si elles sont perdues ou corrompues. Il est recommandé de créer régulièrement un fichier d'exportation.

Vous êtes invité à indiquer les informations d'identification du responsable de la sécurité pour exporter les clés. Pour une protection accrue du fichier de clés, vous pouvez utiliser une phrase de passe différente de celle utilisée au sein d'un système Data Domain. Après l'exportation, il est recommandé de sauvegarder le fichier de clés dans un serveur de fichiers sécurisé accessible uniquement aux utilisateurs autorisés. Vous devez vous souvenir de la phrase de passe utilisée pour le fichier de clés. Si la phrase de passe est perdue ou oubliée, le système Data Domain ne peut pas importer et restaurer les clés. Saisissez :

```
# filesys encryption keys export
```

Prise en charge des gestionnaires de clés

Les deux gestionnaires de clés prennent en charge tous les protocoles de système de fichiers DD OS.

Réplication
Lors de la configuration des systèmes Data Domain pour une réplication MTree de répertoire, configurez chaque système Data Domain séparément. Les deux systèmes peuvent utiliser la même classe de clés ou une autre classe, ainsi que les mêmes gestionnaires de clés ou des gestionnaires différents.

Pour la configuration de la réplication de collection, le système Data Domain doit être configuré sur la source. Suite à une interruption de la réplication, le système Data Domain répliqué d'origine doit être configuré pour le gestionnaire de clés. Sinon, le système Data Domain continue d'utiliser la dernière clé connue.

Utilisation de RSA DPM Key Manager

Lorsque RSA DPM Key Manager est configuré et activé, les systèmes Data Domain utilisent les clés fournies par le serveur RSA DPM Key Manager. Lorsque le même DPM Key Manager gère plusieurs systèmes Data Domain, tous partagent la même clé active (s'ils utilisent la même classe de clés) lorsque les systèmes sont synchronisés et que le système de fichiers Data Domain a été redémarré. La rotation des clés est gérée sur le serveur RSA DPM Key Manager.

Lorsque RSA DPM Key Manager est configuré et activé, les systèmes Data Domain utilisent les clés fournies par le serveur RSA DPM Key Manager. Lorsque le même DPM Key Manager gère plusieurs systèmes Data Domain, tous partagent la même clé active (s'ils utilisent la même classe de clés) lorsque les systèmes sont synchronisés et que le système de fichiers Data Domain a été redémarré. La rotation des clés est gérée sur le serveur RSA DPM Key Manager.

États des clés de chiffrement
Une clé activée en lecture/écriture est toujours en vigueur. Si la clé active est compromise, RSA DPM Key Manager fournit une nouvelle clé. Lorsque le système Data Domain détecte la nouvelle clé, il génère une alerte pour que l'administrateur redémarre le système de fichiers.

Les clés ayant expiré passent en lecture seule pour les données existantes sur le système Data Domain, et une nouvelle clé active est appliquée à toutes les nouvelles données reçues. Lorsqu'une clé est compromise, les données existantes sont à nouveau chiffrées à l'aide de la nouvelle clé de chiffrement après l'exécution d'une opération de nettoyage du système de fichiers. Si le nombre maximal de clés est atteint, les clés inutilisées doivent être supprimées pour faire de la place aux nouvelles clés.

Pour afficher des informations sur les clés de chiffrement qui résident sur le système Data Domain, ouvrez DD System Manager et accédez à l'onglet **Data Management** > **File System** > **Encryption** . Les clés sont répertoriées par ID dans la section **Encryption Keys** de l'onglet Encryption. Les informations suivantes s'affichent pour chaque clé : la date de création d'une clé, sa durée de validité, son type (RSA DPM ou Data Domain), son état (voir États des clés de chiffrement de gestion de la protection des données pris en charge par Data Domain) et sa taille après la compression. Si le système dispose d'une licence Extended Retention, les champs suivants sont également affichés :

Active Size (post comp)

Quantité d'espace physique sur le niveau actif chiffré avec la clé.

Retention Size (post comp)

Quantité d'espace physique sur le niveau de rétention chiffré avec la clé.

Cliquez sur un MUID de clé et le système affiche les informations suivantes sur la clé, dans la boîte de dialogue Key Details : Tier/Unit (exemple : Active, Retention-unit-2), sa date de création, sa date d'expiration, son état (voir États des clés de chiffrement de gestion de la protection des données pris en charge par Data Domain) et la taille après la compression. Cliquez sur Close pour fermer la boîte de dialogue.

Tableau 200 États des clés de chiffrement de gestion de la protection des données pris en charge par Data Domain

État	Définition
Pending-Activated	La clé vient juste d'être créée. Après le redémarrage d'un système de fichiers, la clé est activée en lecture/écriture.
Activated-RW et Activated-RO	Activated-RW et Activated-RO permettent de lire les données chiffrées avec leurs clés respectives. Activated-RW est la dernière clé activée.
De-Activated	Une clé est désactivée lorsque l'heure actuelle est postérieure à la période de validité. La clé est utilisée pour la lecture.
Compromised	La clé ne peut que déchiffrer. Une fois toutes les données chiffrées avec la clé compromise à nouveau chiffrées, l'état passe à l'état Destroyed Compromised. Les clés sont à nouveau chiffrées après l'exécution d'une opération de nettoyage du système de fichiers. Vous pouvez supprimer une clé compromise détruite, si nécessaire.
Marked-For-Destroy	Vous avez marqué la clé comme détruite pour que les données soient à nouveau chiffrées.
Destroyed	Après avoir à nouveau chiffré toutes les données chiffrées avec cette clé, DD OS change son état Marked-For-Destroy en Destroyed. En outre, lorsque la clé détruite est compromise, son état devient Compromised-Destroyed. Vous pouvez

Tableau 200 États des clés de chiffrement de gestion de la protection des données pris en charge par Data Domain (suite)

État	Définition
	supprimer les clés dotées de l'état Destroyed et Compromised-Destroyed. **Remarque** Une clé n'est détruite dans le système Data Domain qu'une fois une opération de nettoyage exécutée et terminée.

Maintien de la synchronisation entre les clés et RSA DPM Key Manager

Une synchronisation automatique des clés a lieu chaque jour à minuit. Une synchronisation manuelle des clés n'est requise que si vous ne pouvez pas attendre la synchronisation planifiée. Chaque fois que de nouvelles clés sont synchronisées sur le système Data Domain, une alerte est générée. Cette alerte s'efface dès que le système de fichiers redémarre.

Une fois que RSA DPM Key Manager Server a généré de nouvelles clés, cliquez sur le bouton **Sync** pour les afficher dans la liste Encryption Key de l'onglet Encryption de Data Domain System Manager.

Remarque

Un redémarrage du système de fichiers est nécessaire si les clés ont été modifiées depuis la dernière synchronisation.

Procédure

1. À l'aide de DD System Manager, sélectionnez le système Data Domain que vous utilisez dans le volet de navigation.

   Remarque

   Utilisez toujours les fonctions de DD System Manager sur le système que vous avez sélectionné dans le volet de navigation.

2. Sélectionnez **Data Management** > **File System** > **Encryption**.
3. Dans la section Encryption Keys, sélectionnez la clé **RSA DPM** et cliquez sur **Sync**.

Destruction d'une clé (RSA DPM Key Manager)

Détruisez une clé si vous ne voulez pas qu'elle serve à chiffrer des données. Cette procédure nécessite des informations d'identification de responsable de la sécurité.

Remarque

Pour plus d'informations sur le responsable de la sécurité, reportez-vous aux sections concernant la création d'utilisateurs locaux et l'activation de l'autorisation de sécurité.

Pour modifier une clé RSA DPM afin que son état permette sa destruction :

Procédure

1. Désactivez la clé sur le serveur RSA DPM.
2. Redémarrez le système de fichiers pour que la clé soit désactivée sur le système Data Domain.
3. À l'aide de DD System Manager, sélectionnez **Data Management** > **File System** > **Encryption**.
4. Dans la section Encryption Keys, sélectionnez la clé à supprimer dans la liste.
5. Cliquez sur **Destroy...**

   Le système affiche la boîte de dialogue Destroy qui inclut le niveau et l'état de la clé.
6. Saisissez le nom d'utilisateur et le mot de passe du responsable de la sécurité.
7. Confirmez la suppression de la clé en cliquant sur **Destroy...**

Remarque

Quand un nettoyage du système de fichiers s'est exécuté, l'état de la clé devient Destroyed.

Suppression d'une clé

Vous pouvez supprimer des clés de Key Manager dont l'état est Destroyed ou Compromised-Destroyed. Toutefois, supprimer une clé devient uniquement nécessaire lorsque le nombre de clés a atteint la limite maximale de 254. Cette procédure nécessite des informations d'identification de responsable de la sécurité.

Remarque

Pour qu'une clé atteigne l'état Destroyed, il faut qu'une procédure de destruction de clé (pour Embedded Key Manager ou pour RSA DPM Key Manager) lui ait été appliquée et qu'un nettoyage du système soit exécuté.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Encryption**.
2. Dans la section Encryption Keys, choisissez la ou les clés à supprimer dans la liste.
3. Cliquez sur **Delete...**

   Le système affiche la clé à supprimer, ainsi que le niveau et l'état de la clé.
4. Saisissez le nom d'utilisateur et le mot de passe de votre responsable de la sécurité.
5. Pour confirmer la suppression d'une ou de plusieurs clés, cliquez sur **Delete**.

Utilisation du Embedded Key Manager

Lorsque Embedded Key Manager est créé, le système Data Domain crée ses propres clés.

Une fois la règle de rotation des clés configurée, une nouvelle clé est automatiquement créée lors de la rotation suivante. Une alerte vous informe de la création d'une nouvelle clé. Vous devez exécuter un redémarrage du système de fichiers pour activer la nouvelle clé et désactiver l'ancienne. Vous pouvez désactiver la règle de rotation des

clés en cliquant sur le bouton Disable associé à l'état de rotation des clés du Embedded Key Manager.

Création d'une clé (Embedded Key Manager)

Créez une clé de chiffrement pour Embedded Key Manager.

Procédure

1. Sélectionnez **Data Management** > **File System** > **DD Encryption**.
2. Dans la section Encryption Keys, cliquez sur **Create...**
3. Saisissez le nom d'utilisateur et le mot de passe de votre responsable de la sécurité.
4. Cliquez sur **Restart the filesystem now** si vous souhaitez redémarrer le système de fichiers.

   Une nouvelle clé Data Domain est créée. Une fois que le système de fichiers a redémarré, la clé précédente est désactivée et la nouvelle clé est activée.
5. Cliquez sur **Create**.

Suppression d'une clé (Embedded Key Manager)

Supprimez une clé de chiffrement pour Embedded Key Manager.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Encryption**.
2. Dans la section Encryption Keys, sélectionnez la clé à supprimer dans la liste.
3. Cliquez sur **Destroy...**

   Le système affiche la boîte de dialogue Destroy qui inclut le niveau et l'état de la clé.
4. Saisissez le nom d'utilisateur et le mot de passe de votre responsable de la sécurité.
5. Confirmez la suppression de la clé en cliquant sur **Destroy...**

Remarque

Quand un nettoyage du système de fichiers s'est exécuté, l'état de la clé devient Destroyed.

Utilisation de KeySecure Key Manager

KeySecure Key Manager prend en charge les gestionnaires de clés externes à l'aide du protocole KMIP (Key Management Interoperability Protocol) et gère de façon centralisée les clés de chiffrement dans une plateforme unique et centralisée.

- Les clés seront préalablement créées dans le gestionnaire de clés.
- KMIP Key Manager ne peut pas être activé sur les systèmes pour lesquels le chiffrement est activé sur une ou plusieurs unités de Cloud.

Utiliser DD System Manager pour configurer et gérer le KeySecure Key Manager

Cette section décrit comment utiliser Data Domain System Manager (DD SM) pour gérer KeySecure Key Manager.

Création d'une clé pour KeySecure Key Manager

Créez une clé de chiffrement pour KeySecure Key Manager (KMIP).

Procédure

1. Faites défiler vers le bas pour afficher le tableau **Key Manager Encryption Keys**.
2. Cliquez sur **Add** pour créer une nouvelle clé de chiffrement Key Manager.
   a. Saisissez le nom d'utilisateur et le mot de passe du responsable de la sécurité.
   b. Cliquez sur **Restart the file system now**.
   c. Cliquez sur **Create**.
3. Cliquez sur **Restart the file system now** pour que les modifications prennent effet.

   Une nouvelle clé KIMP est créée. Une fois que le système de fichiers a redémarré, la clé précédente est désactivée et la nouvelle clé est activée.

Modifier l'état d'une clé existante dans KeySecure Key Manager

Utilisez DD SM pour modifier l'état d'une clé de chiffrement KIMP existante.

Avant de commencer

Passez en revue les conditions de modification d'un état de clé :

- Lorsqu'une clé existe déjà (est active) et qu'une nouvelle clé est créée, la nouvelle clé passe à l'état `Pending-Activated` jusqu'à ce que l'utilisateur redémarre le système de fichiers.
- Les utilisateurs peuvent désactiver une clé dans un état `Activated-RW` seulement s'il existe une clé `Pending-Activated` pour prendre sa place.
- Une clé dans un état `Pending-Activated` n'est désactivée que s'il existe une autre clé `Pending-Activated` pour prendre sa place.
- Une clé dans une clé `Activated-RO` ne nécessite aucune condition. Désactivez-la à tout moment.

Procédure

1. Sélectionnez **Data Management** > **File System** > **DD Encryption**.
2. Faites défiler vers le bas pour afficher le tableau **Key Manager Encryption Keys**.
3. Sélectionnez la clé appropriée dans le tableau **Key Manager Encryption Keys**.
4. Pour désactiver une clé :
   a. Cliquez sur n'importe quelle clé présentant un état `Activated`.
   b. Saisissez le nom d'utilisateur et le mot de passe du responsable de la sécurité.
   c. Cliquez sur **DEACTIVATE**.

Figure 25 Passer la clé KMIP à l'état désactivé

5. Cliquez sur **Restart the filesystem now**.

Résultats

L'état d'une clé existante est modifié.

Configurer KeySecure Key Manager

Utilisez DD SM pour définir la règle de rotation des clés à partir du système Data Domain.

Avant de commencer

Confirmez la période de rotation des clés souhaitée (semaines ou mois), la date de début de la rotation et la date de rotation suivante.

Procédure

1. Sélectionnez **Data Management** > **File System** > **DD Encryption**.
2. Dans la section **Key Management**, cliquez sur **Configure**. La boîte de dialogue **Change Key Manager** s'ouvre.
3. Saisissez le nom d'utilisateur et le mot de passe du responsable de la sécurité.
4. Sélectionnez **KeySecure Key Manager** dans le menu déroulant **Key Manager Type**. Les informations Change Key Manager s'affichent.
5. Définissez la règle principale de rotation :

   Remarque

   La règle de rotation est spécifiée en semaines et en mois. L'incrément minimum de la règle de rotation des clés est d'une semaine, et l'incrément maximum de la règle de rotation des clés est de 52 semaines (ou 12 mois).

   a. Désactivez la règle principale de rotation. Cliquez sur le bouton **Enable Key rotation policy** pour activer.

   b. Saisissez les dates appropriées dans le champ Key rotation schedule.

   c. Sélectionnez le nombre approprié de semaines ou de mois à partir du menu déroulant **Weeks** ou **Months**.

   d. Cliquez sur **OK**.

   e. Cliquez sur **Restart the filesystem now** si vous voulez redémarrer le système de fichiers pour que les modifications prennent effet immédiatement, conformément à la figure 3.

Résultats

La règle de rotation des clés est définie ou modifiée.

Utilisation de la CLI Data Domain pour gérer KeySecure Key Manager

Cette section décrit comment utiliser la CLI pour gérer KeySecure Key Manager.

Créer une nouvelle clé active sur KeySecure Key Manager

Utilisez la CLI Data Domain pour créer une nouvelle clé active.

Avant de commencer

Assurez-vous d'avoir les informations d'identification utilisateur appropriées. Le rôle de sécurité est nécessaire pour pouvoir exécuter ces commandes.

Procédure

1. Connectez-vous au système Data Domain à l'aide du rôle de sécurité :

   Nom d'utilisateur : `<security office user>`

   Mot de passe : `<security officer password>`

2. Créez une nouvelle clé active :

```
# filesys encryption key-manager keys create
```

3. Vous obtenez un résultat du type :

```
New encryption key was successfully created.
The filesystem must be restarted to activate the new key.
```

Résultats

Une nouvelle clé active est créée.

Modifiezr l'état d'une clé existante dans KeySecure Key Manager

Utilisez la CLI Data Domain pour passer l'état d'une clé existante sur l'état désactivé.

Avant de commencer

Assurez-vous d'avoir les informations d'identification utilisateur appropriées. Le rôle de sécurité est nécessaire pour pouvoir exécuter ces commandes.

Procédure

1. Connectez-vous au système Data Domain à l'aide du rôle de sécurité :

   Nom d'utilisateur : `<security officer user>`

   Mot de passe : `<security officer password>`

2. Modifiez l'état d'une clé existante :

   ```
   # filesys encryption key-manager keys modify{<key-id> | muid
   <key-muid>}state deactivated
   ```

   Par exemple :

   ```
   # filesys encryption key-manager keys modify muid
   740D711374A8C964A62817B4AD193C8DC44374A6ED534C85642782014F2E9D
   41 state deactivated
   ```

3. Vous obtenez un résultat du type :

   ```
   Key state modified.
   ```

Résultats

L'état d'une clé existante est modifié.

Définissez ou réinitialisez une règle de rotation des clés dans KeySecure Key Manager.

Utilisez la CLI Data Domain pour définir la règle de rotation des clés sur le système Data Domain pour faire tourner périodiquement les clés. Notez que la règle de rotation est spécifiée en semaines et en mois. L'incrément minimum de la règle de rotation des clés est d'une semaine, et l'incrément maximum de la règle de rotation des clés est de 52 semaines (ou 12 mois).

Avant de commencer

Assurez-vous d'avoir les informations d'identification utilisateur appropriées. Le rôle de sécurité est nécessaire pour pouvoir exécuter ces commandes.

Procédure

1. Connectez-vous au système Data Domain à l'aide du rôle de sécurité :

   Nom d'utilisateur : `sec`

   Mot de passe : `<security officer password>`

2. Définissez une règle de rotation des clés pour la première fois. Dans notre exemple, nous allons définir la règle de rotation sur **trois semaines** :

```
# filesys encryption key-manager set key-rotation-policy
                  {every <n> {weeks | months} | none}
```

Par exemple :

```
# filesys encryption key-manager set key-rotation-policy
every 3 weeks
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 3 weeks.
```

3. Exécutez ensuite cette commande si vous choisissez de modifier la règle de rotation des clés existante. Dans notre exemple, nous allons définir la règle de rotation de **trois semaines** à **quatre mois** :

Remarque

Connectez-vous au système Data Domain en utilisant le rôle de sécurité (où le nom d'utilisateur est `sec`, et le mot de passe est le <`security officer password`>).

```
# filesys encryption key-manager reset [key-rotation-policy]
```

Par exemple :

```
filesys encryption key-manager set key-rotation-policy every
4 months
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 4 months.
```

4. Affichez la règle de rotation des clés en cours ou vérifiez que la règle est correctement définie :

```
# filesys encryption key-manager show
```

Output that is similar to the following appears:

```
The current key-manager configuration is:
Key Manager:                                Enabled
Server Type:                                KeySecure
Server:                                     <IP address of
KMIP server>
Port:                                       5696
Fips-mode:                                  enabled
Status:                                     Online
Key-class:                                  <key-class>
KMIP-user:                                  <KMIP username>
Key rotation period:                        2 months
Last key rotation date:                     03:14:17 03/19
2018
Next key rotation date:                     01:01:00 05/17
2018
```

Résultats

La règle de rotation des clés est définie ou modifiée.

Mode de fonctionnement de l'opération de nettoyage

Le chiffrement affecte les performances des opérations de nettoyage lorsque les données chiffrées avec des clés compromises ou sélectionnées en vue de la destruction sont réintroduites à l'aide de la clé de lecture/écriture activée.

À la fin de l'opération de nettoyage, il n'y a aucune donnée chiffrée avec des clés compromises ou sélectionnées en vue de la destruction. En outre, toutes les données écrites par l'opération de nettoyage sont chiffrées à l'aide de la clé de lecture/écriture activée.

Configuration du gestionnaire de clés

Suivez les instructions s'appliquant au type de gestionnaire de clés que vous utilisez.

Pour plus d'informations sur l'installation de SafeNet KeySecure Key Manager, consultez le *Guide d'intégration Gemalto et KeySecure de Data Domain Operating System*.

Configuration du chiffrement de RSA DPM Key Manager

RSA DPM Key Manager doit être configuré sur RSA DPM Server et sur le système Data Domain.

Exécution de cette configuration sur RSA DPM Server

Les principales étapes de la configuration de RSA DPM Server (à l'aide de son interface utilisateur).

Remarque

Pour plus d'informations sur chaque étape de cette procédure, consultez la dernière version du document *RSA Data Protection Manager Server Administrator's Guide*.

Les paramètres d'algorithme et de mode de chiffrement définis sur RSA DPM Key Manager Server sont ignorés par le système Data Domain. Configurez ces paramètres sur le système Data Domain.

Procédure

1. Créez une identité pour le système Data Domain à l'aide du certificat X509. Un canal sécurisé est créé en fonction de ce certificat.
2. Créez une classe de clés possédant les attributs appropriés :
   - Longueur de la clé : 256 bits.
   - Durée : six mois, par exemple, ou toute durée conforme à votre règle.
   - Génération de clé automatique : sélectionnez la génération automatique des clés.

   Remarque

   Plusieurs systèmes Data Domain peuvent partager la même classe de clés. Pour plus d'informations sur les classes de clés, reportez-vous à la section relative aux classes de clés RSA DPM.
3. Créez une identité en utilisant le certificat d'hôte du système Data Domain en tant que certificat d'identité. L'identité et la classe de clés doivent se trouver dans le même groupe d'identité.
4. Importez les certificats. Pour plus d'informations, reportez-vous à la section relative à l'importation de certificats.

À propos des classes de clés RSA DPM

Le système Data Domain récupère une clé auprès de RSA DPM Key Manager par classe de clés. Une classe de clés est un type spécialisé de classe de sécurité utilisé par RSA DPM Key Manager et regroupant des clés de chiffrement aux caractéristiques semblables.

RSA DPM Key Manager Server permet de configurer une classe de clés pour qu'elle renvoie la clé actuelle ou pour qu'elle génère une nouvelle clé à chaque fois. Le système Data Domain prend uniquement en charge les classes de clés configurées pour renvoyer la clé actuelle. N'utilisez pas de classe de clés configurée pour générer une nouvelle clé à chaque fois.

Remarque

Si la longueur de la clé n'est pas de 256 bits, la configuration DPM échoue.

Importation des certificats

Après avoir obtenu les certificats, importez-les dans le système Data Domain.

Avant de commencer

- Le certificat de l'hôte doit être au format PKCS12.
- Le certificat CA doit être au format PEM.

- Vous devez obtenir des certificats CA et d'hôte compatibles avec RSA DPM Key Manager. Vous pouvez demander ces certificats à des autorités de certificats tierces ou les créer à l'aide d'outils appropriés de l'utilitaire SSL.
- Si la phrase de passe système n'est pas définie, vous ne pouvez pas importer le certificat d'hôte. La phrase de passe est définie lorsque vous activez le chiffrement. Pour la modifier, reportez-vous à la section concernant la modification de la phrase de passe système du chapitre Gestion des systèmes Data Domain.

DD OS prend en charge des certificats sans aucune extension et des certificats avec des extensions de serveur et de client pour une utilisation avec Data DD Manager et avec RSA DPM Key Manager. Les certificats avec extensions de client sont uniquement pris en charge par RSA DPM Key Manager. Les certificats avec extensions de serveurs, quant à eux, sont uniquement pris en charge par DD System Manager.

DD OS ne prend pas en charge la fonction Auto Registration Certificate de RSA DPM Key Manager Server qui télécharge directement un certificat auto-enregistré ou qui importe plusieurs certificats. Par conséquent, vous devez importer les certificats CA et d'hôte pour un système Data Domain.

Les informations suivantes décrivent comment répondre à certaines alertes susceptibles de s'afficher lors de la gestion des certificats.

- Si le protocole HTTPS ne redémarre pas en raison de l'importation de certificats corrompus, des certificats auto-signés sont utilisés. Lorsque cela se produit, une alerte gérée, UnusableHostCertificate, est émise. Pour effacer l'alerte, supprimez les certificats corrompus et réimportez de nouveaux certificats.
- Si les certificats importés sont supprimés, par exemple lors d'une permutation de système, et si la copie des certificats importés échoue, une alerte gérée, MissingHostCertificate, est émise. Importez une nouvelle fois les certificats pour supprimer l'alerte.

Après avoir obtenu les certificats, importez-les dans le système Data Domain de la manière suivante :

Procédure

1. Configurez RSA DPM Key Manager Server pour qu'il utilise des certificats CA et d'hôte. Pour obtenir des instructions, consultez le document *Guide d'administration de RSA DPM Key Manager Server*.
2. Importez les certificats en redirigeant les fichiers de certificats à l'aide de la syntaxe de commande `ssh`. Consultez le *Guide de référence des commandes de Data Domain Operating System* pour plus de détails.

   ssh sysadmin@<*Data-Domain-system*> adminaccess certificate import {host password *password* |ca } < *path_to_the_certificate*
   Par exemple, pour importer le certificat d'hôte host.p12 du bureau de votre ordinateur personnel vers le système Data Domain DD1 utilisant `ssh`, saisissez :

   # ssh sysadmin@DD1 adminaccess certificate import host password abc123 < C:\host.p12

3. Importez le certificat CA (par exemple, ca.pem) de votre ordinateur vers DD1 via SSH en saisissant la commande suivante :

   # ssh sysadmin@DD1**adminaccess certificate import ca < C:\ca.pem**

Exécution de cette configuration sur le système Data Domain

Configurez le chiffrement sur Data Domain System Manager à l'aide de DPM Key Manager.

Procédure

1. Effectuez la configuration de DPM Key Manager sur RSA DPM Server.
2. Le système Data Domain doit être capable de résoudre sa propre adresse IP à l'aide de son nom d'hôte. Si ce mappage n'a donc pas été ajouté au serveur DNS, utilisez la ligne de commande suivante pour ajouter l'entrée dans le fichier `/etc/hosts` :

   # `net hosts add`*ipaddrhost-list*
   où *ipaddr* est l'adresse IP du système Data Domain et où *host-list* est le nom d'hôte du système Data Domain.

   Si vous utilisez un environnement en mode double pile et si le système affiche le message d'erreur suivant : « RKM is not configured correctly », utilisez la commande `net hosts add`*ipaddrhost-list* pour ajouter l'adresse IPv4 du système Data Domain au fichier /etc/hosts.

   Remarque

   Un serveur DPM ne peut pas être activé à l'aide d'un environnement utilisant uniquement des adresses IPv6.

   Remarque

   Par défaut, le mode fips est activé. Si les informations d'identification du client PKCS #12 ne sont pas chiffrées à l'aide de l'algorithme approuvé par FIPS 140-2, par exemple RC2, vous devez désactiver le mode fips. Pour en savoir plus sur la désactivation du mode fips, consultez le *Guide de référence des commandes d'EMC DD OS*.

3. Connectez-vous à DD System Manager et sélectionnez le système Data Domain que vous utilisez dans le volet de navigation.

   Remarque

   Utilisez toujours les fonctions de DD System Manager sur le système que vous avez sélectionné dans le volet de navigation.

4. Cliquez sur l'onglet **Data Management** > **File System** > **Encryption**.
5. Suivez les instructions de la section concernant la configuration du chiffrement et sélectionnez **DPM Key Manager**. Si le chiffrement est déjà défini, suivez les instructions de la section concernant la modification des gestionnaires de clés après la configuration.

Configuration du gestionnaire de clés KMIP

Grâce à la prise en charge de KMIP, une appliance Data Domain peut récupérer les objets de clé symétriques qui sont utilisés pour le chiffrement des données au repos provenant des gestionnaires de clés KMIP.

Procédure

1. Configurez une instance KeySecure avec l'adresse IP <IP1>.
2. Créez et installez un certificat de serveur SSL sur l'instance KeySecure.
3. Activez KMIP en accédant à **Device** > **Key Server**.

   Assurez-vous que <IP1> est l'adresse qui est utilisée, que le port est <Port1> et que le certificat de serveur mentionné à l'étape 2 est utilisé.
4. Créez une demande de signature de certificat pour le système sur le système Data Domain/DD VE ou un ordinateur Linux.

   a. Connectez-vous à Data Domain.

   b. Exécutez la commande `adminaccess certificate cert-signing-request generate`.

   Si la commande réussit, celle-ci génère le fichier `CertificateSigningRequest.csr`, qui se trouve dans `/ddvar/certificates/`.

   Par défaut, les exportations NFS n'ont pas les autorisations nécessaires pour accéder au dossier de certificats, même pour un utilisateur root.

```
# mount 16tbddve:/ddvar /mnt/DDVE
# cd /mnt/DDVE/certificates/
bash: cd: /mnt/DDVE/certificates/: Permission denied
# ls -al /mnt/DDVE/
total 800292
drwxr-xr-x 25 root staff      4096 Apr 10 08:32 .
drwxr-xr-x 26 root root       4096 Oct 24 12:11 ..
-rwxr-xr-x  1 root staff       180 Apr 10 08:36 .bashrc
drwxrwsr-x  2 root staff      4096 Aug 18  2016 benchmark
drwxr-sr-x  3 root staff      4096 Apr  4 15:49 cacerts
drwxrwsr-x  2 root staff      4096 Apr  4 12:50 cdes
drwxrws---  2 root staff      4096 Apr 11  2017 certificates
drwxrwsr-x  3 root staff      4096 Jul  1  2016 core
```

5. Prenez cette demande de signature de certificat et faites en sorte que l'autorité de certification l'émette/la signe sur l'instance KeySecure.

   Si la commande réussit, celle-ci génère le fichier `CertificateSigningRequest.csr`, qui se trouve dans `/ddvar/certificates/`.
6. Téléchargez le certificat signé (fichier pem x.509) sur le système Data Domain et utilisez la clé privée de la demande de signature de certificat pour créer un fichier pkcs #12.

   Renommez `csr` par `pem` dans le nom du fichier.
7. Téléchargez le certificat d'autorité de certification racine émis par l'autorité de certification de l'instance KeySecure (**Security** > **Local CAs**).
8. Sur le système Data Domain/DD VE, utilisez la CLI `adminaccess` pour installer ce certificat client pkcs #12 et le certificat de l'autorité de certification. Utilisez le type d'application **keysecure**.
9. Sur l'instance KeySecure, créez une clé symétrique avec le type d'algorithme et la longueur de clé AES-256.

   a. Définissez le propriétaire pour l'utilisateur qui l'utilisera comme KMIP sur le système Data Domain/DD VE.

   b. Sélectionnez l'option `Exportable`.

c. Sous **Security** > **Keys** > **Attributes** pour la clé, assurez-vous de définir **Application Namespace** sur **DD_DARE_KEYS**. Assurez-vous de définir **Application Data** sur une classe de clé que vous envisagez d'utiliser sur le système Data Domain/DD VE.

10. Utilisez la commande `filesys encryption key-manager set` pour configurer TOUS les paramètres et accéder au gestionnaire de clés KeySecure.
11. Activez le gestionnaire de clés externe en utilisant la commande `filesys encryption key-manager enable`.
12. Activez le chiffrement en utilisant les commandes `filesys encryption enable` et `filesys restart`.

    Cette action redémarre le système de fichiers.
13. Les clés doivent être récupérées automatiquement auprès du gestionnaire de clés keysecure et doivent être visibles dans le tableau de clés locales.

    Exemple de sortie du tableau de clés locales pour `filesys encryption keys show` :

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:02:02 2017.
```

    La clé active en cours est utilisée pour chiffrer toutes les données ingérées.
14. Synchronisez les états des clés.

    a. Sur l'interface Web de keysecure, créez une nouvelle clé active comme décrit précédemment.

    b. Sur l'interface Web de keysecure, désactivez l'ancienne clé en cliquant sur la clé et en accédant à l'onglet **Life Cycle**. Cliquez sur **Edit State**. Définissez **Cryptographic State** sur **Deactivated**. Cliquez sur **Save**.
15. Sur le système Data Domain, synchronisez le tableau de clés locales en exécutant la commande `filesys encryption keys sync`.

    Exemple de sortie du tableau de clés locales pour `filesys encryption keys show` :

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  ------------   ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Deactivated       0
0.3   851631E574D6F02886CAEF2795896D4C401EBC57A0997EFE04A146E584E9A99A  Activated-RW      0
---   ---------------------------------------------------------------  ------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:12:05 2017.
```

Remarque

Les clés peuvent être marquées comme des clés versionnées. Lorsque les 2e et 3e versions d'une clé spécifique sont générées, les requêtes KMIP ne collectent pas réellement ces clés et peuvent poser problème si cette clé est utilisée par un système Data Domain ou DD VE.

Modification des gestionnaires de clés après la configuration

Effectuez une sélection dans Embedded Key Manager ou RSA DPM Key Manager.

Avant de commencer

Pour gérer les certificats d'un système, vous devez démarrer DD System Manager sur ce système.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Encryption**.
2. Sous Key Management, cliquez sur **Configure**.
3. Saisissez le nom d'utilisateur et le mot de passe de votre responsable de la sécurité.
4. Sélectionnez le gestionnaire de clés à utiliser.
   - Embedded Key Manager : sélectionnez cette option pour activer ou désactiver la rotation des clés. Si cette option est activée, entrez un intervalle de rotation de 1 à 12 mois. Sélectionnez **Restart the file system now** et cliquez sur **OK**.
   - RSA DPM Key Manager : saisissez le nom du serveur, la classe de clés, le port (par défaut, il s'agit du port 443) et indiquez si le certificat d'hôte importé est conforme à FIPS. Le mode par défaut est activé. Sélectionnez **Restart the file system now** et cliquez sur **OK**.
5. Cliquez sur **Manage Certificates** pour ajouter des certificats.

Gestion des certificats pour RSA Key Manager

Vous devez utiliser l'hôte et les certificats CA avec RSA Key Manager.

Remarque

Les certificats sont uniquement nécessaires pour RSA Key Manager. Le Embedded Key Manager n'utilise pas les certificats.

Ajout de certificats CA pour RSA Key Manager

Téléchargez ou copiez-collez des certificats CA.

Procédure

1. Sélectionnez l'une des actions suivantes :
   - Sélectionnez l'option de téléchargement d'un certificat CA en tant que fichier .pem et cliquez sur **Browse** pour rechercher le fichier.
   - Sélectionnez l'option permettant de copier et de coller le certificat CA et collez le contenu du certificat dans le champ fourni.
2. Cliquez sur **Add** pour ajouter le certificat.

Ajout d'un certificat d'hôte pour RSA Key Manager

Téléchargez le certificat en tant que fichier .p12 ou téléchargez la clé publique en tant que fichier .pem et utilisez une clé privée générée.

Pour commencer, sélectionnez la première ou la seconde des étapes suivantes :

Procédure

1. Sélectionnez l'option permettant de télécharger le certificat en tant que fichier .p12.
   a. Entrez un mot de passe.
   b. Cliquez sur **Browse** pour rechercher le fichier .p12.
2. Sélectionnez l'option permettant de télécharger la clé publique en tant que fichier .pem et utilisez une clé privée générée.
   a. Cliquez sur **Browse** pour rechercher le fichier .pem.
3. Cliquez sur **Add**.

Suppression de certificats

Sélectionnez un certificat ayant la bonne empreinte.

Procédure

1. Sélectionnez un certificat à supprimer.
2. Cliquez sur **Delete**.

   Le système affiche une boîte de dialogue Delete Certificate avec l'empreinte du certificat à supprimer.
3. Cliquez sur le bouton **OK**.

Vérification des paramètres de chiffrement des données inactives

Vérifiez les paramètres de la fonction DD Encryption.

Cliquez sur les onglets **Data Management** > **File System** > **Encryption**. Le paramètre Key Manager actuellement utilisé s'affiche comme étant activé. Pour obtenir une description des paramètres DD Encryption, reportez-vous à la section relative à la vue Encryption.

Activation et désactivation du chiffrement des données inactives

Une fois DD Encryption configuré, l'état est activé et le bouton Disabled est actif. Lorsque DD Encryption est désactivé, le bouton Enabled est actif.

Activation du chiffrement des données inactives

Utilisez DD System Manager pour activer la fonction de chiffrement.

Procédure

1. À l'aide de DD System Manager, sélectionnez le système Data Domain que vous utilisez dans le volet de navigation.
2. Dans la vue Encryption, cliquez sur le bouton **Enable**.
3. Les deux options suivantes sont accessibles :

- Sélectionnez **Apply to existing data** et cliquez sur **OK**. Le chiffrement des données existantes se produit lors du premier cycle de nettoyage suivant le redémarrage du système de fichiers.
- Sélectionnez **Restart the file system now** et cliquez sur **OK**. Le chiffrement est activé une fois que le système de fichiers a redémarré.

À effectuer

Remarque

Les applications peuvent subir une interruption pendant le redémarrage du système de fichiers.

Désactivation du chiffrement des données inactives

Utilisez DD System Manager pour désactiver la fonction DD Encryption.

Procédure

1. À l'aide de DD System Manager, sélectionnez le système Data Domain que vous utilisez dans le volet de navigation.
2. Dans la vue Encryption, cliquez sur le bouton **Disable**.

   La boîte de dialogue Disable Encryption s'affiche.
3. Dans la zone Security Officer Credentials, saisissez le nom d'utilisateur et le mot de passe d'un responsable de la sécurité.
4. Sélectionnez l'une des actions suivantes :
   - Sélectionnez **Apply to existing data** et cliquez sur **OK**. Le déchiffrement des données existantes se produit lors du premier cycle de nettoyage suivant le redémarrage du système de fichiers.
   - Sélectionnez **Restart the file system now** et cliquez sur **OK**. La fonction DD Encryption est désactivée une fois que le système de fichiers a redémarré.

À effectuer

Remarque

Les applications peuvent subir une interruption pendant le redémarrage du système de fichiers.

Verrouillage et déverrouillage du système de fichiers

Utilisez cette procédure lorsqu'un système Data Domain activé pour l'option DD Encryption (et ses périphériques de stockage externes) est en cours de transport ou si vous souhaitez verrouiller un disque en cours de remplacement. La procédure nécessite deux comptes : rôles de responsable de la sécurité et d'administrateur système.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Encryption**.

   Dans la zone File System Lock, l'option Status indique si le système de fichiers est verrouillé ou déverrouillé.
2. Désactivez le système de fichiers en cliquant sur **Disabled** dans la zone d'état File System.

3. Utilisez cette procédure pour verrouiller ou déverrouiller le système de fichiers.

Verrouillage du système de fichiers

Pour verrouiller le système de fichiers, DD Encryption doit être activé et le système de fichiers désactivé.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Encryption** , puis cliquez sur **Lock File System**.
2. Dans les champs de texte de la boîte de dialogue Lock File System, indiquez :
   - Le nom d'utilisateur et le mot de passe d'un compte de responsable de la sécurité (un utilisateur autorisé dans le groupe Security User sur ce système Data Domain).
   - La phrase de passe actuelle et la nouvelle passe de phrase.
3. Cliquez sur **OK**.

   Cette procédure chiffre à nouveau les clés de chiffrement à l'aide de la nouvelle phrase de passe. Ce processus détruit la copie mise en cache de la phrase de passe actuelle (dans la mémoire et le disque).

   Remarque

   La modification de la phrase de passe nécessite l'authentification de deux utilisateurs pour se prémunir contre le risque qu'un employé indélicat ne détruise les données.

   ⚠ ATTENTION

   Notez soigneusement la phrase de passe. Si vous la perdez, vous ne pourrez plus déverrouiller le système de fichiers ni accéder aux données. Les données seront définitivement perdues.

4. Arrêtez le système :

   ⚠ ATTENTION

   N'utilisez pas l'interrupteur du châssis pour mettre le système hors tension. Saisissez à la place la commande suivante dans la fenêtre d'invite de commandes.

   ```
   # system poweroff The 'system poweroff' command shuts down
   the system and turns off the power. Continue? (yes|no|?)
   [no]:
   ```

5. Transportez le système ou supprimez le disque en cours de remplacement.
6. Rétablissez l'alimentation du système et utilisez la procédure pour déverrouiller le système de fichiers.

Déverrouillage du système de fichiers

Cette procédure prépare un système de fichiers chiffrés en vue de son utilisation à son arrivée à destination.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Encryption**, puis cliquez sur **Unlock File System**.
2. Dans les champs de texte, saisissez la phrase de passe utilisée pour verrouiller le système de fichiers.
3. Cliquez sur **OK**.
4. Cliquez sur **Close** pour quitter la boîte de dialogue.

   Si la phrase de passe n'est pas correcte, le système de fichiers ne parvient pas à démarrer et le système signale l'erreur. Saisissez la phrase de passe correcte, comme indiqué à l'étape précédente.

Modification de l'algorithme de chiffrement

Réinitialisez l'algorithme de chiffrement si nécessaire ou sélectionnez des options pour chiffrer de nouvelles données et des données existantes ou uniquement de nouvelles données.

Procédure

1. Sélectionnez **Data Management** > **File System** > **Encryption**
2. Pour modifier l'algorithme de chiffrement utilisé pour chiffrer le système Data Domain, cliquez sur **Change Algorithm**.

   La boîte de dialogue Change Algorithm s'affiche. Les algorithmes de chiffrement pris en charge sont les suivants :

   - AES-128 CBC
   - AES-256 CBC
   - AES-128 GCM
   - AES-256 GCM

3. Sélectionnez un algorithme de chiffrement dans la liste déroulante ou acceptez le mode AES 256-bit (CBC) par défaut.

   Le mode AES 256-bit GCM (Galois Counter Mode) est l'algorithme le plus sécurisé, mais il est plus lent que le mode CBC (Cipher Block Chaining).

   Remarque

   Pour réinitialiser l'algorithme sur la valeur par défaut, soit AES 256 bits (CBC), cliquez sur Reset to default.

4. Déterminez les données devant être chiffrées :

   - Pour chiffrer des données existantes et de nouvelles données sur le système, sélectionnez **Apply to Existing data, Restart file system now** et cliquez sur **OK**.
     Les données existantes seront chiffrées lors du premier cycle de nettoyage après le redémarrage du système de fichiers.

Remarque

Le chiffrement des données existantes peut prendre plus de temps qu'une opération de nettoyage d'un système de fichiers classique.

- Pour chiffrer uniquement de nouvelles données, sélectionnez **Restart file system now** et cliquez sur **OK**.

5. L'état s'affiche. Au terme du processus, cliquez sur **Close**.

Remarque

Les applications peuvent subir une interruption pendant le redémarrage du système de fichiers.