

# Dell FluidFS NAS Solutions

## Guide de l'administrateur



# Remarques, précautions et avertissements



**REMARQUE** : Une REMARQUE indique des informations importantes qui peuvent vous aider à mieux utiliser l'ordinateur.



**PRÉCAUTION** : Une PRÉCAUTION indique un risque de dommage matériel ou de perte de données et vous indique comment éviter le problème.



**AVERTISSEMENT** : Un AVERTISSEMENT indique un risque d'endommagement du matériel, de blessure corporelle ou de mort.

© 2013 Dell Inc.

Marques utilisées dans ce document : Dell™, le logo Dell, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ et Vostro™ sont des marques de Dell Inc. Intel®, Pentium®, Xeon®, Core® et Celeron® sont des marques déposées d'Intel Corporation aux États-Unis et dans d'autres pays. AMD® est une marque déposée et AMD Opteron™, AMD Phenom™ et AMD Sempron™ sont des marques d'Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® et Active Directory® sont des marques ou des marques déposées de Microsoft Corporation aux États-Unis et/ou dans d'autres pays. Red Hat® et Red Hat® Enterprise Linux® sont des marques déposées de Red Hat, Inc. aux États-Unis et/ou dans d'autres pays. Novell® et SUSE® sont des marques déposées de Novell Inc. aux États-Unis et dans d'autres pays. Oracle® est une marque déposée d'Oracle Corporation et/ou de ses filiales. Citrix®, Xen®, XenServer® et XenMotion® sont des marques ou des marques déposées de Citrix Systems, Inc. aux États-Unis et/ou dans d'autres pays. VMware®, Virtual SMP®, vMotion®, vCenter® et vSphere® sont des marques ou des marques déposées de VMware, Inc. aux États-Unis ou dans d'autres pays. IBM® est une marque déposée d'International Business Machines Corporation.

2013 - 03

Rev. A01

# Table des matières

<b>Remarques, précautions et avertissements.....</b>	<b>2</b>
<b>Chapitre 1: Introduction.....</b>	<b>11</b>
Termes utilisés dans le document.....	11
Architecture de solutions NAS Dell FluidFS.....	12
Étiquettes de port dans FluidFS .....	13
Principales fonctions .....	14
Vues de la solution en cluster NAS.....	14
Composants du système.....	15
Appliance NAS.....	15
Matrices de stockage.....	16
Réseau SAN.....	16
Réseau d'interconnexion.....	16
Réseau LAN ou Client.....	16
Autres informations utiles.....	17
<b>Chapitre 2: Surveillance de la solution NAS FluidFS.....</b>	<b>19</b>
Tableau de bord.....	19
État.....	19
Capacité .....	19
Performances actuelles.....	19
Performances récentes.....	20
Équilibrage de charge.....	20
Visionneuse d'événements.....	20
Visualisation des événements dans la visionneuse d'événements.....	20
Performances réseau.....	20
Équilibrage de charge.....	21
Visualisation de l'équilibrage de charge dans le temps.....	21
Connexions client .....	21
Gestion des connexions CIFS.....	23
Matériel.....	23
Affichage des états de validation système.....	23
Affichage de l'état détaillé des composants.....	24
Capacité.....	24
Visualisation de l'espace utilisé.....	24
Visualisation de l'utilisation des quotas.....	25
Réplication.....	25

NDMP.....	25
<b>Chapitre 3: Utilisation des partages de volumes et quotas.....</b>	<b>27</b>
Volumes NAS.....	27
Considérations d'utilisation.....	27
Solution 1.....	28
Solution 2.....	29
Solution 3.....	29
Gestion des volumes NAS.....	29
Ajout d'un volume NAS.....	29
Modification d'un volume NAS .....	30
Suppression d'un volume NAS.....	30
Partages et exportations.....	30
Gestion des exportations NFS.....	30
Ajout d'une exportation NFS à la solution en cluster NAS.....	31
Modification d'une exportation NFS.....	31
Suppression d'une exportation NFS.....	32
Accès à l'aide de NFS.....	32
Gestion des partages CIFS.....	33
Affichage des propriétés et de l'état des partages CIFS.....	33
Ajout d'un partage CIFS.....	33
Modification d'un partage CIFS.....	34
Suppression d'un partage CIFS.....	35
Créations de partages de base.....	35
Définition de listes de contrôle des accès et d'autorisations des niveaux de partage sur FluidFS.....	36
Compte Administrateur local FluidFS.....	36
Configuration d'Active Directory.....	37
Configuration des ACL ou des SLP sur un partage CIFS.....	37
Accès à l'aide de CIFS.....	39
Configuration des autorisations de niveau de partages CIFS.....	40
Réinitialisation du mot de passe administrateur local CIFS.....	41
Quotas.....	41
Considérations de quota .....	42
Gestion des quotas par défaut.....	42
Gestion de quotas spécifiques à l'utilisateur ou au groupe.....	42
<b>Chapitre 4: Protection des données sur la solution en cluster NAS FluidFS.....</b>	<b>45</b>
Instantanés.....	45
Ajout ou modification d'une stratégie d'instantané.....	45
Création d'un instantané (sans stratégie).....	46
Accès aux instantanés.....	46
Modification d'un instantané.....	46

Restauration des données.....	47
Suppression d'un instantané.....	47
Restauration d'un volume NAS depuis un instantané.....	47
Réplication.....	48
Partenaires de réplication.....	48
Stratégies de réplication NAS.....	50
Pause, reprise et exécution de la réplication NAS.....	52
Suppression d'une stratégie de réplication.....	52
Restauration après sinistre à l'aide de la réplication.....	52
Sauvegarde et restauration de données.....	57
Sauvegarde des volumes NAS cible de réplication.....	57
Éléments à considérer pour la conception NDMP.....	58
Applications prises en charge.....	58
Activation de la prise en charge NDMP .....	58
Modification du mot de passe et du nom d'utilisateur de secours NDMP.....	59
Modification de la Liste des serveurs DMA .....	59
Spécification du volume NAS pour la sauvegarde.....	60
Affichage des tâches NDMP actives.....	60
Utilisation des applications antivirus.....	60
Affichage des hôtes antivirus existants.....	60
Ajout d'hôtes antivirus.....	60
Retrait d'un hôte antivirus.....	61
Activation de la prise en charge antivirus par partage CIFS.....	61

## **Chapitre 5: Gestion de la solution NAS FluidFS.....63**

Gestion du système.....	63
Gestion de l'accès des clients.....	63
Affichage des sous-réseaux définis.....	63
Ajout d'un sous-réseau.....	63
Modification d'un sous-réseau.....	64
Suppression d'un sous-réseau.....	64
Gestion des utilisateurs administrateurs.....	65
Affichage des utilisateurs administrateurs.....	65
Ajout d'un administrateur.....	65
Modification d'un administrateur.....	66
Modification du mot de passe administrateur.....	66
Suppression d'un administrateur.....	66
Gestion des utilisateurs locaux dans le cadre de l'accès aux partages CIFS et NFS.....	67
Affichage des utilisateurs locaux.....	67
Ajout d'utilisateurs locaux.....	67
Modification des utilisateurs locaux.....	68
Suppression d'utilisateurs locaux.....	68

Modification du mot de passe.....	68
Gestion des groupes locaux.....	69
Affichage des groupes locaux.....	69
Ajout d'un groupe local.....	69
Suppression d'un groupe local.....	70
Authentification.....	70
Configuration d'une base de données de gestion des identités.....	70
Activation de l'authentification des utilisateurs via une base de données NIS.....	70
Activation de l'authentification des utilisateurs via une base de données LDAP.....	71
Désactivation de l'utilisation d'une base de données de gestion des identités UNIX externe.....	71
Active Directory.....	71
Synchronisation de la solution en cluster NAS avec le serveur Active Directory.....	72
Configuration du service Active Directory.....	72
Présentation de la configuration du réseau.....	72
Performances et voies statiques.....	73
Configuration du DNS.....	74
Affichage des serveurs DNS.....	75
Ajout de serveurs et suffixes DNS.....	75
Retrait de serveurs et suffixes DNS.....	75
Gestion des voies statiques.....	75
Affichage des voies statiques .....	75
Ajout de voies statiques.....	75
Modification d'une voie statique.....	76
Suppression d'une voie statique.....	76
Définition des protocoles de système de fichiers.....	76
Configuration des paramètres CIFS.....	77
Configuration des paramètres CIFS généraux.....	77
Interdire aux utilisateurs d'accéder aux fichiers à l'aide du protocole CIFS .....	77
Configuration des paramètres CIFS avancés.....	77
Configuration des paramètres horaires du système.....	78
Changer de fuseau horaire.....	78
Configuration manuelle de la date et de l'heure actuelles.....	78
Suppression d'un serveur NTP.....	79
Synchronisation de la solution en cluster NAS avec un serveur NTP local.....	79
Gestion des licences.....	79
Affichage des licences.....	79
Ajout d'une licence.....	80
Suppression d'une licence.....	80
Configuration des paramètres d'e-mail sur des solutions NAS PowerVault NX3500/NX3600/NX3610 .....	80
Affichage des serveurs SMTP.....	81
Configuration d'un serveur SMTP.....	81
Modification d'une configuration de serveur SMTP.....	81

Pour supprimer un expéditeur d'email.....	81
Configuration d'un expéditeur d'e-mail.....	82
Configuration des options avancées.....	82
Configuration du SNMP.....	82

## **Chapitre 6: Dépannage.....85**

Dépannage suite à des problèmes CIFS .....	85
La mauvaise configuration des paramètres de l'hôte AV entraîne un refus d'accès aux fichiers CIFS.....	85
Refus d'accès au CIFS.....	85
Corruption de l'ACL du CIFS.....	85
Décalage de l'horloge du client CIFS.....	86
Déconnexion du client CIFS à la lecture du fichier.....	86
Déconnexion générale du client CIFS.....	87
Échec de la connexion au client CIFS.....	87
Échec de connexion CIFS.....	87
Refus de la suppression à la fermeture du CIFS.....	87
Accès au fichier CIFS refusé.....	88
Conflit de partage du fichier CIFS.....	88
Compte d'invité CIFS non valide.....	88
Incohérence de verrouillage du CIFS.....	88
Nombre maximum de connexions au CIFS atteint.....	89
Le partage CIFS n'existe pas.....	89
Partage du chemin d'accès CIFS introuvable.....	89
Écriture du CIFS sur un volume en lecture seule.....	90
Dépannage suite à des problèmes NFS .....	90
Impossible de monter l'exportation NFS.....	90
L'exportation NFS n'existe pas.....	92
Accès au fichier NFS refusé.....	92
Accès NFS non sécurisé pour une exportation sécurisée.....	93
Le montage NFS échoue en raison des options d'exportation.....	93
Le montage NFS échoue en raison de l'échec du groupe réseau.....	94
Le chemin d'accès au montage NFS n'existe pas.....	94
Opération limitée par le propriétaire NFS.....	95
Écriture du NFS sur une exportation en lecture seule.....	95
Écriture du NFS sur un volume en lecture seule.....	96
Écriture du NFS sur un instantané.....	96
Accès au NFS refusé à un fichier ou un répertoire.....	96
Dépannage de problèmes de réplication.....	97
Erreur de configuration de la réplication.....	97
Le cluster cible de la réplication est occupé.....	97
Le FS cible de la réplication est occupé.....	97
La destination de la réplication est en panne.....	97

La cible de la réplication n'est pas à l'état optimal.....	98
Le volume cible de la réplication est occupé à récupérer de l'espace.....	98
Le volume cible de la réplication est déconnecté.....	98
Déconnexion de la réplication.....	99
Versions incompatibles avec la réplication.....	99
Erreur interne de réplication.....	99
Les trames Jumbo de réplication sont bloquées.....	99
Le volume cible de réplication ne contient pas suffisamment d'espace libre.....	100
La source de réplication est occupée.....	100
La source de la réplication est en panne.....	100
La source de la réplication n'est pas à l'état optimal.....	100
Le volume source de la réplication est occupé à récupérer de l'espace.....	101
Dépannage de problèmes Active Directory.....	101
Le quota de groupe pour un utilisateur Active Directory ne fonctionne pas.....	101
Authentification Active Directory .....	102
Dépannage de la configuration d'Active Directory.....	102
Dépannage de l'accès au fichier NAS et de problèmes d'autorisation.....	103
Impossible de modifier la propriété d'un fichier ou d'un dossier.....	103
Impossible de modifier les fichiers NAS.....	103
Propriété mixte du fichier refusée.....	104
Accès au SMB problématique à partir d'un client Linux.....	104
Numéros d'UID et de GID étranges sur les fichiers du système NAS Dell.....	104
Dépannage de problèmes de mise en réseau.....	105
Serveur de nom non réactif.....	105
Des clients de sous-réseaux spécifiques ne peuvent pas accéder à la solution en cluster NAS .....	105
Dépannage des configurations DNS.....	105
Détermination de l'IQN des contrôleurs de la solution en cluster NAS à l'aide de la CLI.....	106
Dépannage des messages d'avertissement pour pause du RX et du TX.....	106
Dépannage des problèmes du NAS Manager.....	106
Le tableau de bord du NAS est retardé.....	106
L'heure du système NAS n'est pas correcte.....	107
Impossible de se connecter au NAS Manager.....	108
Écran de connexion vide.....	108
Dépannage des problèmes de sauvegarde.....	109
Dépannage des instantanés.....	109
Dépannage d'une erreur interne du NDMP.....	109
Dépannage des problèmes du système.....	111
Dépannage d'un arrêt du système.....	111
Violation de sécurité du conteneur NAS.....	111
Plusieurs erreurs reçues lors du formatage du système de fichiers.....	112
Association des noms de LUN à des disques virtuels .....	113
L'utilitaire NAS IDU n'est pas parvenu à détecter d'autres contrôleurs .....	114

Échec de l'opération de connexion.....	114
Le contrôleur prend beaucoup de temps à s'amorcer suite à la mise à niveau du Service Pack.....	115
Dépannage des problèmes de l'utilitaire IDU (utilitaire de déploiement initial) NAS.....	115
Erreur reçue pendant l'exécution de l'utilitaire Dell NAS Initial Deployment Utility.....	115
Impossible de lancer l'utilitaire IDU NAS Dell .....	116
<b>Chapitre 7: Maintenance de la solution en cluster NAS.....</b>	<b>117</b>
Arrêt de la solution en cluster NAS.....	117
Mise sous tension de la solution en cluster NAS.....	117
Restauration de la configuration du volume NAS.....	118
Restauration de la configuration du cluster.....	119
Formatage du système de fichiers.....	119
Installation du service-pack.....	120
Mise à niveau du Service Pack à l'aide du NAS Manager.....	120
Extension de la capacité de stockage du cluster NAS.....	120
Extension du pool NAS sur la solution NAS Dell PowerVault NX3500/NX3600/NX3610 .....	120
Extension du pool NAS sur la solution NAS FS8600.....	121
Ajout de LUN à la solution en cluster NAS PowerVault NX3500/NX3600/NX3610.....	121
Exécution des diagnostics.....	122
Diagnostics en ligne.....	122
Diagnostics hors ligne.....	122
Réinstallation de la solution en cluster NAS.....	123
Extension du cluster NAS .....	124
Ajout d'une appliance NAS supplémentaire au cluster NAS.....	124
Création d'un hôte dans les systèmes PowerVault NX3500/NX3600/NX3610.....	125
Remplacement d'un contrôleur de solution en cluster NAS.....	126
Prérequis.....	126
Déconnexion du contrôleur de la solution en cluster NAS .....	126
Retrait et remplacement d'un contrôleur de solution en cluster NAS.....	127
Connexion d'un contrôleur à l'aide du NAS Manager.....	127
Fonctionnalités du NAS Manager en mode dégradé.....	128
<b>Chapitre 8: Internationalisation.....</b>	<b>129</b>
Présentation.....	129
Présentation générale de la prise en charge du client Unicode.....	129
Clients NFS .....	129
Clients CIFS .....	129
Paramètres de Configuration d'Unicode .....	129
Limitations de la configuration d'Unicode.....	130
Taille de fichier et Nom de répertoire.....	130
Problèmes de compatibilité des clients .....	130
Question de compatibilité avec le japonais.....	130


<b>Chapitre 9: Questions fréquemment posées.....</b>	<b>133</b>
NDMP.....	133
Réplication.....	133
<b>Chapitre 10: Gestion sécurisée.....</b>	<b>135</b>
Ports NAS FluidFS utilisés.....	136
<b>Chapitre 11: Obtenir de l'aide.....</b>	<b>139</b>
Contacter Dell.....	139
Localisation du numéro de service de votre système.....	139
Commentaires sur la documentation.....	139

# Introduction

La solution NAS Dell FluidFS est une solution de stockage à disponibilité optimale qui agrège plusieurs contrôleurs NAS dans un cluster et les présente aux clients UNIX, Linux, et Microsoft Windows comme un seul serveur de fichiers virtuels.

## Termes utilisés dans le document

Terme	Description
<b>Bloc d'alimentation de secours (BPS)</b>	Fournit une alimentation de batterie de secours en cas de perte d'alimentation.
<b>Adresse IP virtuelle d'accès client</b>	Les adresses IP virtuelles que les clients utilisent pour accéder aux partages CIFS et aux exportations NFS hébergés par la solution NAS FluidFS. La solution NAS FluidFS prend en charge plusieurs adresses IP virtuelles d'accès client.
<b>Serveur NAS</b>	Deux contrôleurs NAS configurés en paire dans un système en cluster NAS FluidFS. Les données du cache sont mises en miroir entre les contrôleurs NAS en paire dans l'appliance.
<b>Contrôleur (contrôleur ou nœuds NAS)</b>	Les deux composants principaux d'une appliance NAS. Chacun fonctionne en tant que membre distinct dans un cluster NAS FluidFS.
<b>Application de gestion des données (DMA)</b>	Aussi appelée serveur d'application de secours.
<b>Dell PowerVault Modular Disque Storage Manager (MDSM)</b>	Le logiciel de gestion livré avec la matrice MD Series.
<b>Enterprise Manager</b>	Logiciel de gestion de systèmes multiples requis pour la gestion de FluidFS avec le centre de cluster.
<b>Fluid File System (FluidFS)</b>	Logiciel de système de fichiers haute performance et évolutif installé sur les contrôleurs NAS.
<b>Identifiant de port d'hôte</b>	ID unique utilisé pour identifier des hôtes sur un réseau.
<b>Réseau LAN ou client (réseau principal)</b>	Réseau via lequel les clients accèdent aux partages et exportations NAS. La solution NAS FluidFS se sert de ce réseau pour se connecter à l'environnement informatique du client ainsi qu'à ses clients NAS. Il s'agit également du réseau qu'utilise l'administrateur de stockage pour gérer la solution NAS.
<b>Pool de stockage NAS</b>	Le pool de stockage NAS est une couche de stockage virtualisée située sur les disques virtuels et qui correspond à la somme totale des disques virtuels auxquels le cluster NAS FluidFS a accès.
<b>Volume NAS (conteneur ou volume virtuel NAS)</b>	Un volume virtualisé qui consomme de l'espace de stockage dans le pool de stockage NAS. Les administrateurs peuvent créer des partages CIFS et des exportations NFS sur un volume NAS et les partager avec les utilisateurs autorisés. Une solution NAS FluidFS prend en charge plusieurs volumes NAS.
<b>Réplication NAS</b>	Réplication entre deux systèmes NAS FluidFS ou entre deux volumes NAS.

Terme	Description
<b>Partenaires de réplication NAS</b>	Les solutions NAS FluidFS participant à l'activité de réplication.
<b>Protocole de Gestion des Données en Réseau (NDMP)</b>	Le Protocole de Gestion des Données en Réseau utilisé pour la sauvegarde et la restauration.
<b>Contrôleur homologue</b>	Le contrôleur NAS homologue auquel un contrôleur NAS spécifique est associé dans une solution NAS FluidFS.
<b>PowerVault MD3xx0i</b>	Désigne les solutions de stockage iSCSI Dell PowerVault MD3200i, MD3220i, MD3600i et MD3620i.
<b>Storage Center</b>	Les solutions Compellent Storage center series 40 ou SC8000 comprenant au moins un adaptateur HBA pour la connectivité FluidFS.
<b>Dell NAS IDU (Initial Deployment Utility - Utilitaire de déploiement initial)</b>	L'Assistant Configuration utilisé pour la découverte et la configuration initiales d'une solution NAS FluidFS. Cet utilitaire est utilisé uniquement pour la configuration initiale.
<b>NAS Manager</b>	L'interface utilisateur Web faisant partie du logiciel de la solution en cluster NAS et utilisé pour gérer la solution NAS FluidFS.
<b>Solution NAS FluidFS</b>	Une appliance NAS entièrement configurée, à disponibilité optimale et évolutive, fournissant des services NAS (CIFS et/ou NFS), et composée d'une paire de contrôleurs NAS, d'un sous-système de stockage et du NAS Manager.
<b>Contrôleur de secours</b>	Un contrôleur NAS installé avec le logiciel FluidFS mais qui ne fait pas partie d'un cluster. Par exemple, un nouveau contrôleur ou un contrôleur de rechange fourni par Dell est considéré comme étant un contrôleur de secours.
<b>Réseau SAN</b>	Le réseau qui effectue le trafic au niveau du bloc et auquel le sous-système de stockage est connecté.
	 <b>REMARQUE :</b> Il est recommandé que ce réseau soit isolé du réseau LAN ou client.

## Architecture de solutions NAS Dell FluidFS

Les solutions NAS FluidFS combinées aux matrices de stockage vous offrent une solution de stockage unifiée. Cette solution vous permet d'accéder au stockage au niveau des blocs et des fichiers.

La solution NAS en cluster FluidFS consiste en une appliance NAS dotée d'une paire de contrôleurs et de matrices de stockage. En outre, chaque contrôleur NAS est protégé par un bloc d'alimentation de secours (BPS), pour aider à en protéger les données en cas de panne de courant.

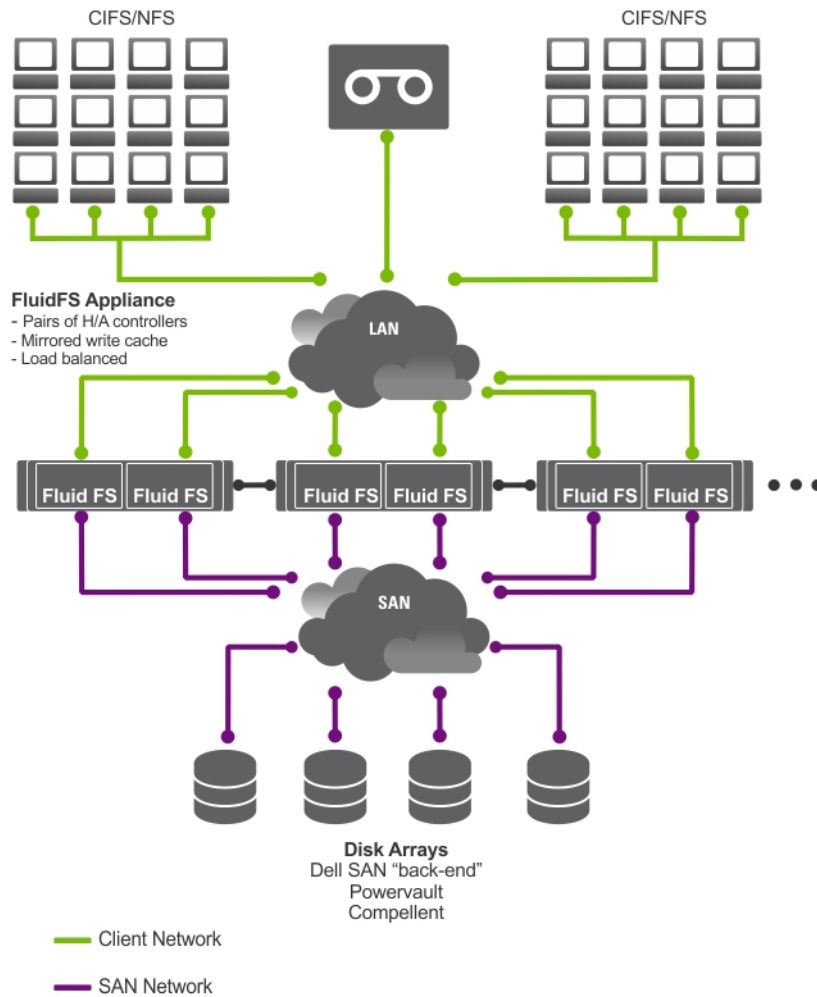


Figure 1. Architecture de la solution en cluster NAS FluidFS

**REMARQUE :** La solution NAS Dell Compellent FS8600 utilise un réseau d'interconnexion supplémentaire, ce qui n'est pas illustré dans cette représentation.

## Étiquettes de port dans FluidFS

Lorsqu'un port Ethernet perd sa connectivité, FluidFS publie un événement indiquant qu'un câble a été débranché et indique le port débranché. Les étiquettes de port sont toujours présentées sous la forme **eth** suivi par un numéro, par exemple **eth0**. Les images suivantes présentent la façon dont les ports physiques sont en corrélation avec les étiquettes **eth**, tel que signalé par le journal d'événements FluidFS.

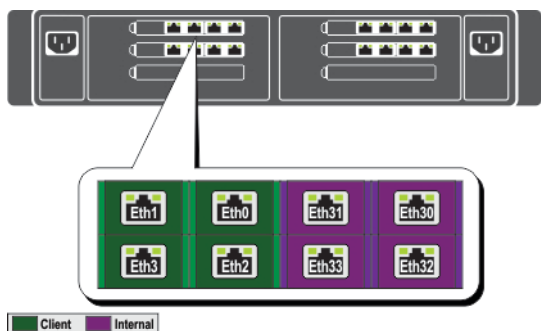


Figure 2. Étiquettes de port des systèmes 1 GbE

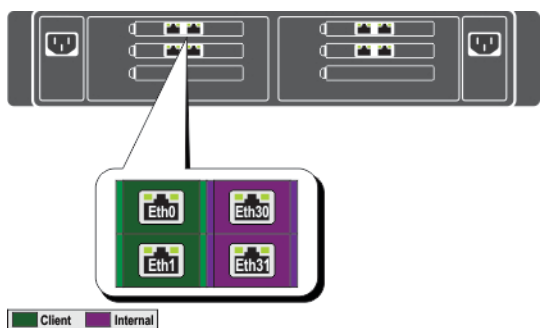


Figure 3. Étiquettes de port des systèmes 10 GbE

## Principales fonctions

La solution en cluster NAS :

- Aide les administrateurs à développer la capacité existante et à améliorer les performances si nécessaire, sans affecter les applications ou les utilisateurs.
- Propose des fonctions administratives aux administrateurs du stockage qui effectuent des opérations quotidiennes sur le système et s'occupent de la gestion du stockage.
- Dispose d'un système de fichiers distribué, ce qui crée une interface unique sur les données.
- Peut stocker des téraoctets de données dans un seul système de fichiers.
- Permet une augmentation dynamique de la capacité.
- Dispose d'une console de gestion NAS basée sur le web, centralisée et facile à utiliser.
- Dispose d'un provisionnement de stockage virtuel à la demande.
- Est capable de fournir des instantanés à un Moment dans le temps accessibles à l'utilisateur.
- Est capable de partager des fichiers avec des utilisateurs Microsoft Windows, Linux, UNIX et Mac.
- Propose une réplication automatisée en ligne et une reprise après sinistre.
- Propose une surveillance des performances intégrée et la planification de la capacité.

## Vues de la solution en cluster NAS

Vous pouvez accéder à la solution en cluster NAS en tant que client ou administrateur, selon les privilèges d'accès dont vous disposez.



**REMARQUE :** Nous vous recommandons vivement de ne pas tenter de vous connecter simultanément à l'interface CLI et au NAS Manager.

### Vue du Client

Pour le client, la solution en cluster NAS se présente en tant que serveur de fichiers unique doté d'un système de fichiers unique, d'une adresse IP et d'un nom. Le système de fichiers global de la solution en cluster NAS sert tous les utilisateurs de manière simultanée sans fluctuations des performances. Elle offre aux utilisateurs finals la possibilité de se connecter à la solution en cluster NAS avec les protocoles NAS de leur propre système d'exploitation.

- Protocole NFS pour les utilisateurs Linux et UNIX.
- Protocole CIFS pour les utilisateurs Windows.

### Vue de l'Administrateur

En tant qu'administrateur, vous pouvez utiliser la CLI ou le NAS Manager pour configurer ou modifier les paramètres du système, comme la configuration de protocoles, l'ajout d'utilisateurs et les autorisations de paramétrage.

Le NAS Manager donne accès à la fonctionnalité du système à l'aide des navigateurs Internet standard.

## Composants du système

La solution en cluster NAS comprend les éléments suivants :

- Matériel
  - Au moins une appliance NAS
  - Matrices de stockage
- Réseau
  - Réseau SAN
  - Réseau interne
  - Réseau LAN ou client

### Appliance NAS

La solution NAS FluidFS comprend une ou plusieurs appliances NAS configurées en tant que cluster. Chaque appliance comprend une paire de contrôleurs NAS dans une configuration active-active qui assure la redondance. Les contrôleurs gèrent l'équilibrage de charge des connexions client ainsi que les opérations de lecture-écriture, effectuent la mise en cache et communiquent avec les serveurs et les stations de travail. Le cluster est un pool de stockage unique doté d'un nom d'espace global et accessible par une adresse IP virtuelle.

Les opérations de lecture-écriture sont traitées via la mémoire RAM mise en miroir. La mise en miroir des données du cache entre les contrôleurs NAS mis en paire assure une réponse rapide aux requêtes des clients tout en maintenant l'intégrité totale des données. Le transfert des données du cache au stockage permanent s'effectue de manière asynchrone via des schémas de placement de données optimisés.

Le système de fichier utilise le cache de manière efficace, fournissant ainsi des lectures-écritures rapides et fiables. L'écriture ou la modification des fichiers se réalise d'abord dans le cache. Les données sont ensuite mises en miroir sur le cache du contrôleur homologue. Cette fonctionnalité assure que toutes les transactions sont effectuées en double et sécurisées.

Chaque contrôleur est doté d'un bloc d'alimentation de secours qui fournit une alimentation continue aux contrôleurs pendant un minimum de cinq minutes en cas de panne de courant. Les contrôleurs surveillent régulièrement l'état de la batterie du bloc d'alimentation de secours, ce qui exige que la batterie maintienne un niveau d'alimentation minimum en

fonctionnement normal. La batterie du bloc d'alimentation de secours dispose d'une alimentation suffisante pour permettre aux contrôleurs de s'arrêter en toute sécurité.

Le bloc d'alimentation de secours permet aux contrôleurs d'utiliser la NVRAM en tant que cache. Il donne également à la solution mise en cluster assez de temps pour qu'elle puisse écrire toutes les données du cache sur le disque en cas de perte d'alimentation du contrôleur.

## Matrices de stockage

Les contrôleurs se connectent à une matrice de stockage, ce qui s'appelle un sous-système RAID. Les sous-systèmes de stockage RAID sont conçus pour éliminer des points de panne uniques. Chaque composant actif du sous-système de stockage est redondant et remplaçable à chaud. La solution prend en charge les configurations RAID typiques, notamment RAID 1/10, RAID 5 et RAID 6.

## Réseau SAN

Le réseau SAN est critique à la solution en cluster NAS. La paire de contrôleurs réside sur le réseau SAN et communique avec le sous-système de stockage à l'aide du protocole iSCSI pour les systèmes Dell PowerVault NX3500/NX3600/NX3610, ou le protocole Fibre Channel pour le système Dell Compellent FS8600.

## Réseau d'interconnexion

Le réseau d'interconnexion est composé de deux réseaux indépendants. Il agit en tant que mécanisme de pulsation et permet le transfert de données internes entre les contrôleurs. Dans un système à deux contrôleurs, aucun commutateur n'est utilisé. Cependant, dans les configurations à plus de deux contrôleurs, le réseau d'interconnexion comprend deux commutateurs. Tous les contrôleurs Dell Fluid File System (FluidFS) sont connectés aux deux commutateurs d'interconnexion. Ces derniers se servent de liaisons doubles afin d'assurer la redondance et l'équilibrage de charge. Afin de réaliser une distribution complète des données et de maintenir une haute disponibilité, chaque contrôleur du système en clusters Dell FluidFS doit avoir accès aux autres contrôleurs du système. Le réseau d'interconnexion assure cet accès. Il fournit la connectivité à la mise en cluster Dell FluidFS, notamment la surveillance de la pulsation, le transfert des données, la mise en miroir des informations entre les caches des contrôleurs et la distribution égale des données sur tous les LUN du système.

## Réseau LAN ou Client

Une fois la configuration initiale effectuée, une adresse IP virtuelle (VIP) connecte la solution en cluster NAS au réseau client ou LAN.

L'adresse IP virtuelle permet aux clients d'accéder à la solution en cluster NAS en tant qu'entité unique, fournissant ainsi un accès au système de fichiers. Elle permet à la solution en cluster NAS d'effectuer des équilibrages de charge entre les contrôleurs et assure un fonctionnement sans interruption, même si un contrôleur venait à échouer.

Chaque contrôleur est doté de ports de réseau LAN ou client destinés à la connexion aux commutateurs de réseau LAN ou client. La solution en cluster NAS est administrée à l'aide du réseau LAN ou client sur les adresses IP virtuelles de gestion NAS. Dans le cas de réseaux routés, le nombre d'adresses IP virtuelles qui répondent au système dépend du nombre de ports client auxquels vous avez accès, par exemple, un système Dell Compellent FS8600 (1 GbE) à quatre appliances dispose de 32 adresses IP virtuelles de client. Dans le cas de réseaux plats, une adresse IP virtuelle de client suffit.

## Autres informations utiles



**AVERTISSEMENT** : Reportez-vous aux informations concernant la sécurité et les réglementations qui accompagnent le système. Des informations sur la garantie peuvent être incluses à ce document ou à un document séparé.


- Le *Getting Started Guide* (Guide de mise en route) présente les procédures de configuration et les spécifications techniques du système.
- Le *Manuel du propriétaire* contient des informations sur les fonctions de la solution, ainsi que des instructions relatives au dépannage et à l'installation ou au remplacement de composants du système.
- La documentation fournie avec le rack indique comment installer le système dans un rack, le cas échéant.
- Le *Guide de déploiement* présente le déploiement du matériel et le déploiement initial du serveur NAS.
- Le *System Placemat (Présentation des informations système)* fournit des informations sur la configuration du matériel et l'installation du logiciel sur votre solution NAS.
- L'*Aide en ligne* fournit des informations sur la configuration et la gestion du logiciel. L'aide en ligne est intégrée au système et accessible depuis l'interface Web du NAS Manager.
- Tous les supports fournis avec le système contiennent de la documentation et des outils permettant de configurer et de gérer le système, notamment les supports du système d'exploitation, du logiciel de gestion du système, des mises à jour système et des composants système que vous avez achetés avec le système.
- Pour obtenir le nom complet d'une abréviation ou connaître la signification d'un sigle utilisé dans ce tableau, voir le Glossaire sur [dell.com/support/manuals](http://dell.com/support/manuals).



**REMARQUE** : Vérifiez toujours si des mises à jour sont disponibles sur le site [support.dell.com/manuals](http://support.dell.com/manuals) et lisez-les en premier, car elles remplacent souvent les informations contenues dans les autres documents.



## Surveillance de la solution NAS FluidFS

 **REMARQUE** : Les informations que contient ce chapitre font référence à la gestion de fichier à l'aide du NAS Manager. La gestion et la surveillance des blocages s'effectuent à l'aide de :

- **Dell PowerVault Modular Disk Storage Management (Gestion du stockage sur disques modulaires Dell PowerVault) (MDSM)** pour la solution NAS Dell PowerVault NX3500/NX3600/NX3610
- **Enterprise Manager** pour la solution NAS Dell Compellent FS8600


Vous pouvez surveiller l'état de la solution NAS dans l'onglet **Monitor (Surveiller)** du NAS Manager. Cet onglet vous permet d'afficher l'état général du système dans la page **Dashboard (Tableau de bord)**, consulter le rapport d'utilisation des quotas et recevoir des rapports sur l'état des tâches de réplication à distance.


Pour accéder aux pages de surveillance, cliquez sur l'onglet **Monitor**. La page **Dashboard** s'affiche par défaut.

### Tableau de bord

La page **Dashboard (Tableau de bord)** affiche l'état de l'intégralité du système en une seule vue et comprend cinq sections en temps réel et à court terme :

- État
- Capacité
- Performances actuelles
- Performances récentes
- Équilibrage de charge

 **REMARQUE** : Les informations de l'écran sont actualisées automatiquement au bout de quelques secondes.

 **REMARQUE** : Pour afficher les paramètres d'état détaillés de chaque section, cliquez sur Section dans le **Dashboard**.

#### État

La section **Status (État)** affiche l'état du système ainsi qu'une liste de composants matériels. Chaque type de composant matériel affiche le nombre total de composants et le nombre de composants à problème. La liste comprend les contrôleurs et les appliances qui y sont associées.

#### Capacité

La section **Capacity (Capacité)** affiche un tableau et diagramme circulaire indiquant la capacité nette totale du système de fichiers Dell Fluid (Dell FluidFS).

#### Performances actuelles

La section **Current Performance (Performances actuelles)** affiche le débit réseau actuel, lequel comprend le débit de données en lecture-écriture (Mo/s) et le nombre d'opérations de lecture-écriture par seconde par protocole.

## Performances récentes

La section **Recent Performance (Performances récentes)** affiche un graphique du débit de lecture/écriture au cours des 30 dernières minutes.

## Équilibrage de charge

La section **Load Balancing (Équilibrage de charge)** affiche un tableau avec des informations en temps réel sur l'état du contrôleur, l'utilisation du processeur et le nombre de connexions pour chaque contrôleur.

## Visionneuse d'événements

La **Events Viewer (Visionneuse de événements)** vous permet de surveiller votre Fluid File System en affichant les événements principaux et informatifs ayant lieu au sein de votre système.

Pour accéder à la page **Events Viewer**, cliquez sur **Events (Événements)** dans l'onglet **Monitoring (Surveillance)**.

Dans la page **Events Viewer**, vous pouvez effectuer les éléments suivants :

- Filtrer les événements
- Trier les événements
- Exporter les événements dans un fichier CSV

## Visualisation des événements dans la visionneuse d'événements

1. Sélectionnez **Monitor (Surveiller)** → **Overview (Aperçu)** → **Events (Événements)**.  
La page **Event Viewer (Visionneuse des événements)** s'affiche.
2. Sélectionnez les filtres appropriés dans les listes **Show (Afficher)**, **events of (les événements de)**, et **from (de)**, puis cliquez sur **Show (Afficher)**.  
Un tableau de la visionneuse des événements s'affiche, selon les paramètres sélectionnés.
3. Pour trier les événements, cliquez sur les en-têtes de colonne du tableau de la visionneuse des événements.
4. Pour afficher les détails concernant l'événement, sélectionnez l'événement pertinent dans le tableau de la visionneuse des événements.  
Les détails de l'événement sélectionné s'affichent dans le volet **View (Vue)**.
5. Pour exporter les événements affichés dans un fichier CVS, cliquez sur **Export to CSV file (Exporter dans un fichier CVS)**.  
Une nouvelle page Web au format CSV contenant les événements s'affiche.
6. Copiez-collez les événements dans un fichier CSV ou enregistrez la page Web sous un fichier CSV.

## Performances réseau

La page **Network Performance Over Time (Performances réseau au fil du temps)** affiche les performances du Dell Fluid File System au fil du temps. Vous pouvez afficher les performances réseau du FluidFS pour les périodes de temps suivantes :

- **dernier jour**
- **semaine dernière**
- **mois dernier**

- **année dernière**

Cliquez sur chaque onglet pour afficher les performances réseau tout au long de la période de temps appropriée. Vous pouvez afficher les détails de performances réseau suivants :

- **Débit du réseau client : lectures**
- **Débit du réseau client : écritures**
- **Opérations par seconde**
- **Débit cumulé du réseau**



**REMARQUE** : Pour en savoir plus sur les **Network Performance Over Time (performances réseau au fil du temps)**, consultez l'*Aide en ligne*.

## Équilibrage de charge

Vous pouvez afficher des informations détaillées relatives aux équilibrages de charge suivants :

- **Dans le temps**
- **Connexions client**
- **Connexions CIFS**

### Visualisation de l'équilibrage de charge dans le temps

1. Sélectionnez **Monitor (Surveiller)** → **Load Balancing (Équilibrage de charge)** → **Over Time (Dans le temps)**. La page **Load Balancing Over Time (Équilibrage de charge dans le temps)** s'affiche. Elle contient la **CPU Load (Charge de l'UC)**, les **CIFS Connections (Connexions CIFS)**, le **Read Throughput (Débit de lecture)** et le **Write Throughput (Débit d'écriture)**.
2. Cliquez sur l'onglet pertinent pour afficher les informations relatives à l'équilibrage de charge concernant la durée requise.

Vous pouvez afficher les informations relatives à l'équilibrage de charge :

- **du dernier jour**
- **de la semaine dernière**
- **du mois dernier**
- **de l'année dernière**

3. Sélectionnez le contrôleur dont vous souhaitez afficher les informations d'équilibrage des charges, puis cliquez sur **Display (Afficher)**.



**REMARQUE** : Par défaut, tous les contrôleurs sont sélectionnés.


4. Pour exporter les événements qui s'affichent dans un fichier CSV, cliquez sur **Export to CSV file (Exporter dans un fichier CSV)**. Une nouvelle page Web au format CSV contenant les événements s'affiche.
5. Copiez-collez les événements dans un fichier CSV ou enregistrez la page Web sous un fichier CSV.

### Connexions client


La page **Client Connections (Connexions client)** vous permet d'effectuer les opérations suivantes :

- Afficher la répartition des clients entre les contrôleurs.
- Migrer manuellement des clients spécifiques d'un contrôleur à l'autre.

- Définir la stratégie pour la migration automatique des clients.

 **REMARQUE** : Par défaut, l'onglet **Clients** affiche la liste de toutes les connexions client.

### Affichage des connexions client

 **REMARQUE** : La page client connexions (connexions client) affiche uniquement les clients qui appartiennent au même sous-réseau en tant que système (clients locaux). Les clients qui accèdent au système via un routeur (ou une couche en 3 commutateurs) ne s'affichent pas sur cette page. Le routeur s'affiche à la place.

1. Sélectionnez **Monitor (Surveiller)** → **Load Balancing (Équilibrage de charge)** → **Client Connections (Connexions client)**.  
La page **Client Connections** s'affiche. L'onglet **Clients** affiche par défaut une liste de toutes les connexions client.
2. Sélectionnez les filtres appropriés dans les listes **Protocols (Protocoles)** et **Controller (Contrôleurs)**.  
Le tableau de connexions client affiche les événements, selon les paramètres sélectionnés.
3. Pour trier les connexions client, cliquez sur les en-têtes de colonne du tableau de connexions client.

### Migration des clients sur un autre contrôleur

Si la charge réseau n'est pas équilibrée, le système peut y remédier en migrant les clients d'un contrôleur à un autre, de manière automatique ou manuelle. Dans la liste, sélectionnez les clients ou routeurs pouvant être migrés vers d'autres contrôleurs.

1. Sélectionnez **Monitor (Surveiller)** → **Load (Charge) Balancing (Équilibrage)** → **Client Connections (Connexions client)**.  
La page **Client Connections** s'affiche. L'onglet **Clients** affiche par défaut une liste de toutes les connexions client.
2. Dans la table des connexions client, sélectionnez une ou plusieurs connexions client à migrer, puis cliquez sur **Assign Interface (Interface d'affectation)**.  
La page **Assign Interface** s'affiche.
3. Sous **Move to (Déplacer vers)**, sélectionnez un contrôleur spécifique comme cible, ou bien sélectionnez **Assigned Controller (Contrôleur affecté)**.
  - Pour migrer tous les clients sélectionnés sur un contrôleur spécifique, choisissez un contrôleur spécifique dans la liste.
  - Pour migrer tous les clients sélectionnés vers leurs contrôleurs d'origine suite à la correction d'un contrôleur précédemment en échec, sélectionnez **Assigned Controller**. Chaque client peut disposer d'un différent contrôleur affecté.
4. Sous **Interface**, sélectionnez l'interface cible appropriée ou autorisez le système à attribuer automatiquement l'interface cible sur le contrôleur.

 **PRÉCAUTION** : Cette opération déconnecte les connexions CIFS si ces dernières sont migrées sur un autre contrôleur.

5. Pour activer **Automatic Rebalance (Rééquilibrage automatique)**, cochez la case à cocher en regard de **Allow these clients to migrate to other controllers when rebalancing the network load (Autoriser ces clients à migrer sur d'autres contrôleurs lors du rééquilibrage de la charge du réseau)**.
6. Cliquez sur **Assign (Attribuer)**.

### Définition de la stratégie de migration

En cas d'échec de contrôleur, le système migre automatiquement les connexions du contrôleur en échec sur un autre contrôleur. Cela entraîne la déconnexion des clients CIFS, à moins que la stratégie **Migrate Manually (Migrer manuellement)** n'ait été précédemment sélectionnée pour CIFS. Cependant, si vous sélectionnez cette option, vous devez migrer les clients manuellement. Quoi qu'il en soit, la migration des clients CIFS entraîne l'interruption des E/S. Cliquez sur le bouton **Windows Annuler**, puis réessayez le transfert. Au redémarrage du contrôleur en échec, le système

rééquilibre la charge en migrant automatiquement les clients sur leur contrôleur d'origine. Cette opération s'appelle « restauration automatique ».

Les clients qui utilisent NFS sont sans état et ne sont pas affectés pendant la restauration automatique. Pour optimiser l'opération de restauration automatique, le système vous fournit les stratégies de migration sur restauration suivantes :

- **Migrate Immediately (Migration immédiate)** : toujours conserver un bon équilibre du système, au risque de déconnecter potentiellement les clients CIFS pendant le temps de travail.
- **Migrate Automatically (Migration automatique)** : toujours conserver un bon équilibre du système si l'échec du contrôleur est de courte durée, au risque de déconnecter les clients CIFS. Si l'échec dure longtemps, cette option amène le système à rester déséquilibré pendant plusieurs jours.  
Ce mode permet de maîtriser les échecs de contrôleur de courte durée car les clients n'ont pas créé de nouveau matériel pendant la courte durée de la panne. Il est donc recommandé de les rééquilibrer le plus vite possible. Si l'échec dure plus de 10 minutes, vous devrez rééquilibrer le système manuellement.
- **Migrate Manually (Migration manuelle)** : ne jamais migrer les clients automatiquement. Cela nécessite une intervention manuelle de la part de l'utilisateur pour rééquilibrer le système. Si le système nécessite une intervention manuelle de la part de l'utilisateur pour le rééquilibrer suite à une restauration automatique, un message indiquant cela est envoyé à l'administrateur.

Pour définir les stratégies de migration :

1. Sélectionnez **Monitor (Surveiller)** → **Load Balancing (Équilibrage de charge)** → **Client Connections (Connexions client)**.  
La page **Client Connections** s'affiche. L'onglet **Clients** affiche par défaut une liste de toutes les connexions client.
2. Cliquez sur **Migration Policy (Stratégie de migration)**.  
La page **Migration Policy** s'affiche.
3. Pour chaque **Protocol (protocole)**, sélectionnez la stratégie de migration appropriée dans **Client Network (Réseau client)**.
4. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Gestion des connexions CIFS

Vous pouvez voir les **connexions CIFS** actuelles sur la page **CIFS Connections (Connexions CIFS)**.

Pour gérer les connexions CIFS :

1. Sélectionnez **Monitor (Surveiller)** → **Load Balancing (Équilibrage de charge)** → **CIFS Connections (Connexions CIFS)**.  
La page **CIFS Connection** s'affiche.
2. Pour déconnecter un client d'un protocole CIFS, sélectionnez le client approprié, puis cliquez sur **Disconnect (Déconnecter)** dans la barre d'**actions**.
3. Pour déconnecter toutes les connexions d'un contrôleur spécifique, sélectionnez le contrôleur approprié, puis cliquez sur **Disconnect** dans la barre d'**actions**.
4. Cliquez sur **Refresh (Actualiser)** pour mettre à jour les informations affichées.

## Matériel

### Affichage des états de validation système

Vous pouvez effectuer une validation système pour valider la configuration système, notamment le matériel et la connectivité réseau.



**REMARQUE** : La validation système peut également être exécutée à l'aide de l'interface CLI.

Elle fournit des informations sur les processeurs, les surveillances de la disponibilité, les cartes réseau, IPMI, la bande passante Ethernet, la surveillance des blocs d'alimentation de secours, et ainsi de suite.

Pour actualiser l'état des composants système :

1. Sélectionnez **Monitor (Surveiller)** → **Hardware (Matériel)** → **System Validation (Validation système)**.  
La page **System Validation** s'affiche.
2. Cliquez sur **Rerun (Exécuter à nouveau)** pour réexécuter la validation système sur chaque composant système, puis actualisez l'état de chacun de ces composants.

## Affichage de l'état détaillé des composants

La page **Component Status (État des composants)** affiche l'état actuel de la solution en cluster NAS. Elle contient des informations sur l'état des composants, leur connectivité et l'alimentation qu'ils fournissent à chaque appliance et leurs contrôleurs.

Pour afficher des informations détaillées supplémentaires sur l'état d'un contrôleur ou d'une appliance spécifique :

1. Sélectionnez **Monitor (Surveiller)** → **Hardware (Matériel)** → **Component Status (État des composants)**.  
La page **Hardware Component Status (État des composants matériel)** s'affiche.
2. Sous **Component (Composant)**, cliquez sur l'appliance ou le contrôleur de votre choix.  
Une page Internet s'ouvre et affiche l'état de chaque composant dans l'appliance ou le contrôleur sélectionné(e).
3. Cliquez sur **Sample Hardware Components (Échantillonner les composants matériels)** pour actualiser l'écran jusqu'à ce que les nouvelles valeurs échantillonnées s'affichent.

Les numéros des appliances et contrôleurs démarre à 0. Appliance0 contient le Contrôleur0 et le Contrôleur1, Appliance1 contient le Contrôleur2 et le Contrôleur3, et ainsi de suite. Pour identifier le matériel physique, vous devez cliquer sur **ApplianceX** et faire correspondre le numéro de service qui s'affiche dans la fenêtre contextuelle avec le numéro de service imprimé sur l'étiquette située sur l'oreillette avant de l'appliance.

## Capacité

### Visualisation de l'espace utilisé

La page **Space Utilization (Utilisation de l'espace)** affiche l'espace utilisé par le Dell Fluid File System ainsi que l'espace utilisé par Dell Fluid File System au fil du temps.

Pour afficher l'espace utilisé :

1. Sélectionnez **Monitor (Surveiller)** → **Capacity (Capacité)** → **Space Utilization (Utilisation de l'espace)**.  
La page **Space Utilization** affiche le tableau « utilisation de l'espace » correspondant à la période sélectionnée. L'utilisation de l'espace **actuelle** s'affiche par défaut.
2. Cliquez sur l'onglet pertinent pour afficher les informations relatives à l'équilibrage de charge pendant le temps requis. Vous pouvez visualiser les informations relatives à l'équilibrage de charge :
  - du dernier jour
  - de la semaine dernière
  - du mois dernier
  - de l'année dernière
3. Pour trier l'utilisation, cliquez sur les en-têtes de colonne du tableau « utilisation de l'espace ».

## Visualisation de l'utilisation des quotas

La page **Quota Usage (Utilisation des quotas)** affiche les quotas et l'utilisation de tous les utilisateurs, y compris les utilisateurs pour lesquels aucun quota n'a été défini. Elle inclut les utilisateurs qui ont été supprimés du système mais en conserve l'utilisation.

Pour afficher l'utilisation des quotas :

1. Sélectionnez **Monitor (Surveiller)** → **Capacity (Capacité)** → **Quota Usage (Utilisation des quotas)**.  
La page **Quota Usage (Utilisation des quotas)** affiche la table d'utilisation des quotas de **tous les volumes NAS**.
2. Dans la liste **Show quotas for NAS Volume (Afficher les quotas du volume NAS)**, sélectionnez le volume NAS approprié ou **All NAS Volumes (Tous les volumes)**.  
La table d'utilisation des quotas affiche les détails d'utilisation des quotas correspondant au volume NAS sélectionné.
3. Pour actualiser l'utilisation des quotas, cliquez sur **Refresh (Actualiser)**.

## Réplication

Vous pouvez afficher l'état et l'avancement du processus de réplication NAS dans la page **NAS Replication (Réplication NAS)**.

Pour afficher l'état et l'avancement des stratégies de réplication NAS :

1. Sélectionnez **Monitor (Surveiller)** → **Replication (Réplication)** → **NAS Replication (Réplication NAS)**.  
La page NAS Replication affiche le tableau de réplifications NAS correspondant aux stratégies de réplication du volume source et/ou volume de destination se trouvant sur ce Dell Fluid File System.
2. Pour trier la réplication NAS, cliquez sur les en-têtes de colonne du tableau « réplifications NAS ».
3. Pour afficher un historique détaillé de l'avancement de la stratégie de réplication, cliquez sur l'état de la stratégie de réplication pertinente.

## NDMP

Pour voir l'état et la progression des tâches NDMP actives, consultez la page **NDMP Active Jobs (Tâches NDMP actives)**.



# Utilisation des partages de volumes et quotas

L'onglet **User Access (Accès utilisateur)** vous permet de définir et gérer le Dell Fluid File System d'une perspective client.

## Volumes NAS

Les volumes du NAS sont des sous-ensembles du pool de stockage dotés de règles spécifiques permettant de contrôler l'allocation d'espace, la protection des données et le type de sécurité.

Ils peuvent être créés et configurés. Les administrateurs peuvent soit créer un grand volume NAS consommant l'intégralité du pool NAS, soit plusieurs volumes NAS. Quoi que vous décidiez, vous pouvez toujours créer, redimensionner, ou supprimer ces volumes NAS.

Cette section décrit comment un administrateur attribue et déploie le stockage de solution en cluster NAS à l'aide de volumes NAS. Pour que les utilisateurs puissent accéder aux volumes NAS, ces derniers doivent être partagés (exportés) séparément. Plus particulièrement, les utilisateurs doivent monter chaque partage.

## Considérations d'utilisation

La définition de plusieurs volumes NAS permet aux administrateurs d'appliquer différentes stratégies de gestion à leurs données, telles que Sauvegarde, Instantanés, Quotas et Style de sécurité. Quelle que soit la stratégie utilisée, le stockage est géré en tant que pool de stockage unique et l'espace libre peut être migré facilement entre les volumes NAS en modifiant simplement l'espace alloué d'un volume NAS.

Avant de choisir une stratégie, prenez en considération les facteurs suivants :

- Exigences générales
  - Les volumes NAS sont logiques ; ils peuvent être aisément créés, supprimés ou modifiés (augmentés ou réduits) selon la capacité du système.
  - Le nom du volume NAS ne doit pas contenir plus de 230 caractères, lesquels ne peuvent être que des lettres, chiffres et tirets de soulignement (\_), et doit commencer par une lettre ou un tiret de soulignement.
  - Vous pouvez créer autant de volumes NAS que vous le souhaitez, cependant la capacité totale ne doit pas dépasser la capacité de stockage totale.
  - Un seul volume peut occuper des données de divers types, si vous définissez plusieurs partages sur les volumes.
  - Il est possible de redimensionner un volume virtuel après l'avoir créé.
  - La taille minimum d'un volume NAS est de 20 Mo (ou si le volume a déjà été utilisé, la taille minimale correspond aux données stockées).
  - La taille maximale d'un volume NAS correspond à l'espace non alloué restant.
- Exigences d'entreprise : une exigence d'entreprise ou d'application pour la séparation ou l'utilisation d'un volume unique doit être considérée. Les volumes NAS peuvent être utilisés pour allouer du stockage aux services à la demande, en utilisant un mécanisme de seuil pour informer les services lorsque l'espace libre qui leur est alloué vient à manquer.
- Instantanés : chaque volume du NAS peut avoir une stratégie de planification d'instantanés dédiée afin de protéger au mieux le type de données qu'il contient.

- Style de sécurité : dans des environnements à plusieurs protocoles, il peut s'avérer utile de séparer les données et définir des volumes NAS avec un style de sécurité UNIX pour les clients UNIX, et NTFS pour les clients Windows. Ceci permet à l'administrateur de faire correspondre le style de sécurité aux exigences d'entreprise ainsi qu'aux divers schémas d'accès aux données. Le style de sécurité peut également être mixte de manière à prendre en charge la sécurité POSIX et les listes de contrôle d'accès Windows sur le même volume.
- Quotas : les quotas sont également définis par volume NAS. Les différentes stratégies de quotas peuvent être appliquées à différents volumes NAS, permettant ainsi à l'administrateur de se concentrer sur la gestion des quotas, le cas échéant.

Voici certains exemples d'utilisation : opérations de copie, opérations de liste et opérations de déplacement. Le tableau suivant représente une entreprise dotée de divers services, et présente comment créer des volumes NAS. La solution à utiliser dépend des exigences du client, car les volumes NAS sont flexibles et peuvent être augmentés ou réduits à la demande.

**Tableau 1. Exemple de volume NAS**

Service	Contrôle de gestion d'accès préféré	Instantanés	Réplication	Sauvegarde	Clients CIFS ou NFS et combinaison lecture/écriture (80/20 est standard)	% de changement de données existantes par heure (1% et supérieur est Élevé)
Post production	NFS	Par heure	Non	Toutes les semaines	20–20/80	1 %
Administration et finances	CIFS	Non	Non	Toutes les semaines	10–50/50	Aucun
Diffusion	Combinaison	Non	Non	Toutes les semaines	10–90/10	Aucun
Appuyer	CIFS	Tous les jours	Non	Non	5–10/90	5 % (approximativement)
Marketing	CIFS	Tous les jours	Oui	Non	5–50/50	Aucun

## Solution 1

Créez cinq volumes NAS basés sur les services. L'administrateur divise logiquement le stockage et la gestion en groupes fonctionnels. Dans ce scénario, les exigences de service sont assez différentes et prennent en charge la création logique de volumes NAS conformément aux services.

Cette solution offre les avantages suivants :

- La gestion logique des volumes NAS est aisée.
- Les volumes NAS sont créés de manière à correspondre aux besoins exacts de chaque service.

Désavantage de cette option : les volumes NAS deviennent difficiles à gérer si le nombre de services au sein de l'organisation augmente.

## Solution 2

Services de groupe ayant des exigences de sécurité similaires dans les volumes NAS. L'administrateur crée trois volumes NAS, un pour NFS, un pour CIFS et un autre mixte. Avantage de cette solution : les volumes NAS fonctionnent séparément entre Windows et Linux. Désavantages de cette solution :

- Tous les fichiers d'un volume NAS sont sauvegardés.
- Des services non souhaités peuvent être fournis à certains services. Si un volume CIFS est créé pour sauvegarder les données des services administratif et financier, les données des services d'édition et juridique sont également sauvegardées, même si cela n'est pas nécessaire.

## Solution 3



Les volumes NAS peuvent également être créés d'après la fonctionnalité. Cependant, avec cette solution, l'adressage utilisateur est requis. Un utilisateur doit choisir un style de sécurité, NTFS ou UNIX, et selon ce dernier, l'adressage approprié pour les autres utilisateurs est défini.

## Gestion des volumes NAS

Vous pouvez afficher l'état actuel des volumes NAS et supprimer ou modifier des volumes NAS existants.

## Ajout d'un volume NAS

Pour ajouter un volume NAS :


1. Sélectionnez **User Access (Accès utilisateur) → NAS Volumes (Volumes NAS) → Configuration**.  
La page **NAS Volumes Configuration (Configuration des volumes NAS)** affiche la liste des volumes NAS.
2. Cliquez sur **Add (Ajouter)**.  
La page **Add NAS volume (Ajouter le volume NAS)** s'affiche.
3. Sous **NAS Volume (Volume NAS)**, saisissez le nom du volume NAS.
4. Sous **NAS volume allocated space (Espace attribué au volume NAS)**, saisissez l'espace attribué à ce volume NAS en Mo, Go ou To.  
 **REMARQUE** : Un volume NAS doit être de 20 Mo au minimum, et sa taille maximale peut correspondre à l'intégralité de l'espace disponible.
5. Sous **Alert when used space reaches (Avertir lorsque l'espace utilisé atteint)**, entrez un pourcentage de l'espace attribué.
6. Dans la liste **Send email alerts to administrator (Envoyer des alertes par e-mail à l'administrateur)**, sélectionnez un administrateur Dell Fluid File System auquel le système enverra les alertes par e-mail.  
 **REMARQUE** : Cette fonctionnalité n'est pas disponible sur les solutions NAS Dell Compellent FS8600. Pour en savoir plus, consultez le document **Enterprise Manager** sur la gestion des alertes avec ces solutions.
7. Dans la liste **Access time granularity (Accéder à la granularité de l'heure)**, sélectionnez la résolution de l'exactitude de l'horodatage d'accès au fichier selon les exigences système en matière de performances.
8. Dans la liste **File Access Security Style (Style de sécurité d'accès aux fichiers)**, sélectionnez le style de sécurité du volume NAS.  
Vous pouvez sélectionner **NTFS, MIXED (Mixte)**, ou **UNIX**.
9. Sous **Default UNIX permissions of Windows files (Autorisations UNIX par défaut des fichiers Windows)**, définissez les autorisations UNIX par défaut des nouveaux fichiers créés depuis les clients Windows.

10. Sous **Default UNIX permissions of Windows directories (Autorisations UNIX par défaut des répertoires Windows)**, définissez les autorisations UNIX par défaut des nouveaux répertoires créés depuis les clients Windows.
11. Cliquez sur **Save Changes (Enregistrer les modifications)** pour créer le volume NAS.

## Modification d'un volume NAS



Pour modifier les paramètres d'un volume CIFS particulier :

1. Sélectionnez **User Access (Accès utilisateur) → NAS Volumes (Volumes NAS) → Configuration**.  
La page **NAS Volumes Configuration (Configuration des volumes NAS)** affiche la liste des volumes NAS.
2. Dans la liste des volumes NAS disponibles, sous **NAS Volume (Volume NAS)**, cliquez sur le volume NAS pertinent.  
La page **Edit NAS Volume (Modifier le volume NAS)** du volume NAS sélectionné s'affiche.
3. Modifiez les paramètres au besoin, puis cliquez sur **Save Changes (Enregistrer les modifications)**.

 **REMARQUE** : Si vous modifiez l'espace alloué au volume NAS, la nouvelle affectation sera limitée par l'espace qu'elle utilise (minimum) et l'espace disponible dans la solution en cluster NAS (maximum).

## Suppression d'un volume NAS

Le volume NAS sélectionné est supprimé. L'espace utilisé par le volume NAS supprimé est récupéré en arrière-plan.

-  **REMARQUE** : Notez également que les exportations NFS, partages CIFS, répliqués du NAS ou références au volume NAS à supprimer doivent être supprimé(e)s avant la suppression d'un volume NAS.
-  **REMARQUE** : La suppression d'un volume NAS entraîne la suppression de tous les fichiers et répertoires et de toutes ses propriétés, c'est-à-dire, les partages, définitions d'instantanés, etc. Une fois le volume NAS supprimé, il ne peut être restauré que s'il est redéfini et restauré depuis une sauvegarde externe.

Pour supprimer un volume NAS :

1. Assurez-vous que le volume NAS n'est pas monté et avertissez les utilisateurs concernés qu'ils seront déconnectés.
2. Sélectionnez **User Access (Accès utilisateur) → NAS Volumes (Volumes NAS) → Configuration**.  
La page **NAS Volumes Configuration (Configuration des volumes NAS)** affiche la liste des volumes NAS.
3. Dans la liste des volumes NAS disponibles, sélectionnez le volume NAS pertinent et cliquez sur **Delete (Supprimer)**.

## Partages et exportations

Vous pouvez définir les autorisations d'accès aux fichiers dans le système de fichiers, selon les autorisations octroyées aux hôtes et utilisateurs. Pour ce faire, partagez les répertoires à l'aide des exportations NFS et des partages CIFS.





## Gestion des exportations NFS

Les exportations NFS sont un moyen efficace de partager les fichiers et les données sur des réseaux UNIX/Linux. Les clients NFS peuvent uniquement monter des répertoires ayant été exportés.

Pour gérer la liste des exportations NFS, depuis l'onglet **User Access (Accès utilisateur)**, sous **Shares (Partages)**, sélectionnez **NFS Exports (Exportations NFS)**. La page **NFS Exports** apparaît et affiche la liste des exportations NFS actuellement définies.

## Ajout d'une exportation NFS à la solution en cluster NAS

Pour ajouter une exportation NFS :

1. Sélectionnez **User Access (Accès utilisateur)** → **Shares (Partages)** → **NFS Exports (Exportations NFS)**.  
La page **NFS Exports** s'affiche.
2. Cliquez sur **Ajouter**.  
La page **Add NFS Export (Ajouter une exportation NFS)** s'affiche. Elle comprend deux onglets : **General (Général)** et **Advanced (Avancé)**. L'onglet **General** s'affiche par défaut.
3. Dans la liste **NAS Volume (Volume NAS)**, sélectionnez le volume NAS sur lequel l'exportation NFS se trouve.
4. Sous **Exported Directory (Répertoire exporté)**, saisissez le chemin du répertoire que vous souhaitez exporter ou cliquez sur l'icône **Browse (Parcourir)** et naviguez vers le répertoire approprié.
5. Sélectionnez **Create the exported directory if it does not exist (Créer le répertoire exporté s'il n'existe pas)**, si le répertoire n'existe pas.
6. Dans la liste **Trust these users (Faire confiance à ces utilisateurs)**, sélectionnez les utilisateurs de confiance.  
 **REMARQUE** : Les autres utilisateurs sont identifiés comme étant invités.
7. Définissez les machines client autorisées à accéder à cette exportation NFS. Sélectionnez une des options suivantes :
  - **All Client Machines (Toutes les machines client)**.
  - **A Single Client Machine (Une seule machine client)** : vous devez saisir l'**adresse IP ou le nom de domaine** du client.
  - **All Client Machines in a Specific Network (Toutes les machines client sur un réseau spécifique)** : vous devez saisir l'**adresse IP ou le masque de réseau** des clients.  
 **REMARQUE** : Par exemple, si vous souhaitez octroyer l'accès à tous les membres du sous-réseau 192.10.x.x/16 avec masque de réseau 255.255.0.0, saisissez 192.10.0.0 dans le champ **IP address (Adresse IP)** et 255.255.0.0 dans le champ **Subnet (Sous-réseau)**.
  - **All Client Machines in a Specific Netgroup (Toutes les machines client sur un groupe de réseaux spécifique)** : vous devez fournir le **nom du groupe de réseaux** des clients.
8. Sous **Allow access for (Autoriser l'accès pour)**, sélectionnez les droits d'accès appropriés pour le partage. Vous devez sélectionner soit **Read/Write (Lecture-Écriture)** soit **Read only (Lecture seule)**.  
 **REMARQUE** : Si les droits d'accès du partage sont plus stricts que les droits d'accès d'un fichier spécifique, les droits d'accès de ce fichier sont écrasés par ceux du partage.
9. Cliquez sur l'onglet **Advanced (Avancé)**.
10. Sous **Limit reported size (Limite de la taille rapportée)**, définissez la limite de la taille rapportée de l'exportation NFS pour donner l'accès aux machines client qui ne peuvent pas prendre en charge des systèmes de fichiers importants.  
 **REMARQUE** : Si vous laissez le champ **Limited reported size (Limite de la taille rapportée)** vide, la taille rapportée est la taille actuelle.
11. Sous **Require secure port? (Port sécurisé requis ?)**, sélectionnez **No (Non)** pour autoriser l'accès via des ports non sécurisés (ports au-delà de 1024).
12. Sous **Comment (Commentaire)**, ajoutez un commentaire ou une description de l'exportation NFS.
13. Cliquez sur **Enregistrer les changements**.

## Modification d'une exportation NFS

Pour modifier les paramètres d'une exportation NFS donnée dans la liste des Exportations NFS :

1. Sélectionnez **User Access (Accès utilisateur)** → **Shares (Partages)** → **NFS Exports (Exportations NFS)**.  
La page NFS Exports s'affiche.
2. Dans la liste des exportations NFS disponibles, sous **Exported Directory (Répertoire exporté)**, cliquez sur l'exportation NFS pertinente.  
La page **Edit NFS Export (Modifier l'exportation NFS)** correspondant à l'exportation NFS sélectionnée s'affiche.
3. Modifiez les paramètres (au besoin) dans les onglets **General (Général)** et **Advanced (Avancé)** et cliquez sur **Save Changes (Enregistrer les modifications)**.

## Suppression d'une exportation NFS

Pour ajouter une exportation NFS :

1. Sélectionnez **User Access (Accès utilisateur)** → **Shares (Partages)** → **NFS Exports (Exportations NFS)**.  
La page NFS Exports s'affiche.
2. Dans la liste des exportations NFS disponibles, sélectionnez l'exportation NFS pertinente et cliquez sur **Delete (Supprimer)**.

## Accès à l'aide de NFS

Pour monter un dossier d'exportation NFS sur un volume NAS, depuis un environnement ou un système client, utilisez la commande `su` pour ouvrir une session en tant que `root` (racine) et exécutez la commande suivante :

```
mount <adresse IP virtuelle du client FluidFS>:<nom du volume>/<dossier exporté> <dossier_local>
```

Cependant, les versions précédentes de UNIX/Linux n'utilisent pas TCP par défaut. La commande de montage fournit les arguments appropriés.

Pour monter un dossier d'exportation NFS sur un volume NAS, depuis un environnement ou un système client, utilisez la commande `su` pour ouvrir une session en tant que `root` (racine) et exécutez la commande suivante :


```
mount -o hard,tcp,nfsvers=3,timeo=3,retrans=10,rsize=32768,wsiz=32768 <adresse IP virtuelle du client FluidFS>:<nom du volume>/<dossier exporté> <dossier_local>
```

Pour la compatibilité descendante avec FluidFS version 1, il est également possible de monter un dossier d'exportation NFS sur le volume NAS par défaut en exécutant la commande :

```
mount -o hard,tcp,nfsvers=3,timeo=3,retrans=10,rsize=32768,wsiz=32768 <adresse IP virtuelle du client FluidFS>:<nom du volume>/<dossier exporté> <dossier_local>
```

Pour monter un dossier d'exportation NFS sur un volume NAS depuis MAC :

```
mount_nfs -T -3 -r 32768 -w 32768 -P <adresse IP virtuelle du client FluidFS>:<nom du volume>/<dossier exporté> <dossier_local>
```

 **REMARQUE** : Les paramètres susmentionnés sont recommandés. Pour en savoir plus et pour connaître d'autres options, consultez la page du manuel de commandes `mount`.

Pour autoriser une connexion UDP ou TCP, configurez les paramètres de pare-feu d'une des deux manières principales suivantes :

- Réglez les paramètres de pare-feu de manière à ce que l'adresse IP source provienne de l'un des deux contrôleurs et non de l'adresse IP virtuelle (VIP) du client.
- Ouvrez la plage de ports UDP pour autoriser les ports en procédant comme suit :

Nom de service	Port FluidFS
portmap	111
Statd	4000 à 4008
NFS	2049 à 2057
NLM (gestionnaire de verrouillage)	4050 à 4058
montage	5001 à 5009
quota	5051 à 5059

## Gestion des partages CIFS

Les partages CIFS offrent un moyen efficace de partager des fichiers et des données sur un réseau Windows.

### Affichage des propriétés et de l'état des partages CIFS


Pour afficher des informations relatives aux partages CIFS existants :

1. Sélectionnez **User Access (Accès utilisateur)** → **Shares (Partages)** → **CIFS Shares (Partages CIFS)**.  
La page **CIFS Shares** s'affiche.
2. Dans la liste **Show CIFS Shares for NAS Volumes (Afficher les partages CIFS des volumes NAS)**, sélectionnez le volume NAS spécifique ou **All NAS Volumes (Tous les volumes NAS)**.  
La table d'exportation CIFS du volume NAS sélectionné s'affiche.


### Ajout d'un partage CIFS

Pour ajouter un partage CIFS :


1. Cliquez sur **User Access (Accès utilisateur)** → **Shares (Partages)** → **CIFS Shares (Partages CIFS)**.  
La page **CIFS Share (Partage CIFS)** s'affiche.
2. Dans la page **CIFS Share**, cliquez sur **Add (Ajouter)**.  
La page **Add CIFS Share (Ajouter un partage CIFS)** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
3. Dans la liste **des volumes NAS**, sélectionnez le volume NAS approprié.
4. Pour définir un répertoire auquel tous les utilisateurs peuvent accéder, sélectionnez **General-access Share (Partage d'accès général)**.
  - a) Sous **Share name (Nom du partage)**, saisissez le nom du partage CIFS.
  - b) Sous **Directory (Répertoire)**, saisissez le chemin du répertoire que vous souhaitez exporter ou cliquez sur l'icône **Browse (Parcourir)** et naviguez vers le répertoire approprié.
  - c) Sélectionnez **Create the exported directory if it does not exist (Créer le répertoire exporté s'il n'existe pas)**, si le répertoire n'existe pas.
5. Pour définir un répertoire utilisateur dans lequel un répertoire est dédié à chaque utilisateur, sélectionnez **CIFS Share containing a user-based directory tree (Partage CIFS contenant une arborescence de répertoire utilisateur)**.  
Pour en savoir plus, voir [Creating Home Shares](#) (Création de partages de base).
  - a) Sous **Path template (Modèle de chemin)**, saisissez le modèle de chemin (la base des répertoires de base) du volume de partage CIFS.
  - b) Sélectionnez **User (Utilisateur)** pour ajouter le nom d'utilisateur au répertoire de base, ou sélectionnez **Group/ User (Groupe/Utilisateur)** pour ajouter le groupe principal et l'utilisateur au chemin du répertoire de base.
6. Sous **Comment (Commentaire)**, entrez une description ou un commentaire concernant le partage CIFS.

 **PRÉCAUTION** : Ne sélectionnez pas **Files should be checked for viruses (Vérifier si les fichiers contiennent des virus)**, sauf si vous disposez d'un serveur Antivirus externe configuré.


7. Sélectionnez **Files should be checked for viruses** pour indiquer si vous souhaitez que le système vérifie ou non si les fichiers contiennent des virus avant d'autoriser l'accès.
8. Cliquez sur l'onglet **Advanced (Avancé)**, puis sous **Hide these files (Masquer ces fichiers)**, saisissez les types de fichier que vous souhaitez masquer lorsque le partage est parcouru.

 **REMARQUE** : Par exemple, entrez \*.tmp pour masquer tous les fichiers dotés d'une extension .tmp.

9. Sous **Allow guests (Autoriser les invités)**, sélectionnez **Yes (Oui)** pour autoriser des utilisateurs inconnus à accéder aux partages en tant qu'invités.


 **REMARQUE** : Si vous sélectionnez **Files should be checked for viruses (vérifier si les fichiers contiennent des virus)** dans l'onglet **General**, l'onglet **Antivirus** est activé.

10. Cliquez sur l'onglet **Antivirus**, puis sous **Select the policy for handling of virus-infected files: (Sélectionner la stratégie de gestion des fichiers infectés par un virus :)**, sélectionnez l'une des options suivantes :
  - **Do nothing (Ne rien faire)** : refuser l'accès au client, mais garder le fichier dans son emplacement d'origine (l'accès est uniquement autorisé via un autre partage CIFS qui n'effectue pas la vérification des virus).
  - **Quarantine the file (Mettre le fichier en quarantaine)** : refuser l'accès au client et déplacer le fichier dans le dossier **.Quarantine** du dossier racine du volume NAS.
  - **Remove the file (Supprimer le fichier)** : refuser l'accès au client et supprimer le fichier.


 **REMARQUE** : Le système applique l'option sélectionnée si un fichier infecté par un virus est identifié que l'hôte antivirus n'a pas été en mesure d'éliminer le virus.

11. Sous **Specify which files should be checked for viruses (Indiquer les fichiers sur lesquels une vérification de virus devrait être effectuée)**, sélectionnez l'une des options suivantes :

- **Effectuer un balayage de tous les fichiers sauf des fichiers dotés d'extensions particulières**
- **Effectuer un balayage des fichiers dotés d'extensions particulières uniquement**

 **REMARQUE** : Utiliser une liste des extension séparée par des virgules. Par exemple : tmp, jpg, jpeg.

12. Sous **Exclude files in the following folders (Exclure les fichiers du dossier suivant)**, saisissez les noms de dossier pour lesquels aucune vérification de virus n'est nécessaire.

 **REMARQUE** : Utilisez une liste de dossiers séparée par des virgules et entourez les fichiers de guillemets s'ils contiennent des espaces ou des virgules. Vous pouvez inclure des caractères spéciaux dans la spécification de dossier. Par exemple, /Marketing/temp\*/Secrets,/All Finance".

13. Cliquez sur **Enregistrer les changements**.


 **REMARQUE** : Ne tentez pas de créer un partage CIFS à l'aide de la console de gestion Microsoft MMC. Utilisez uniquement MMC pour définir les autorisations de niveau de partages (SLP).

## Modification d'un partage CIFS

Une fois que vous avez déterminé si un partage CIFS est un répertoire d'accès général ou un répertoire utilisateur, vous ne pouvez pas modifier ce paramètre. Pour modifier les paramètres d'un partage CIFS particulier :

1. Cliquez sur **User Access (Accès utilisateur)** → **Shares (Partages)** → **CIFS Shares (Partages CIFS)**.  
La page **CIFS Share (Partage CIFS)** s'affiche.
2. Dans la liste des partages CIFS disponibles, dans la colonne **Share (Partages)**, cliquez sur le partage CIFS pertinent.  
La page **Edit CIFS Share (Modifier le partage CIFS)** du partage CIFS sélectionné s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
3. Dans l'onglet **General (Généralités)**, modifiez les paramètres généraux du partage CIFS.

4. Cliquez sur **Advanced (Avancé)** pour modifier les paramètres avancés du partage CIFS.

 **REMARQUE** : Si vous sélectionnez **Files should be checked for viruses (vérifier si les fichiers contiennent des virus)** dans l'onglet **General**, l'onglet **Antivirus** est activé.

5. S'il est activé, cliquez sur **Antivirus** et modifiez la stratégie d'antivirus.
6. Cliquez sur **Enregistrer les changements**.


## Suppression d'un partage CIFS

Pour supprimer un partage CIFS, procédez comme suit :

1. Cliquez sur **User Access (Accès utilisateur)** → **Shares (Partages)** → **CIFS Shares (Partages CIFS)**.  
La page **CIFS Share (Partage CIFS)** s'affiche.
2. Dans la liste des partages CIFS, sélectionnez le partage CIFS approprié, puis cliquez sur **Delete (Supprimer)**.

## Créations de partages de base

Si vous créez un partage CIFS avec une structure de répertoire utilisateur (partage de base), le partage ne sera pas initialement accessible car tous les répertoires utilisateur doivent être créés par l'administrateur. Ceci peut être effectué à l'aide d'un script (script créé par l'utilisateur), d'un fichier de commandes, ou de la commande PowerShell cmdlet écrite par l'administrateur de stockage. En variante, l'administrateur peut créer ces dossiers manuellement. Ceci sert à offrir de meilleurs contrôles d'accès à l'administrateur. L'administrateur peut déterminer manuellement les comptes à donner au partage de base, ou il peut écrire un script afin de générer automatiquement les dossiers, pour certains ou tous les utilisateurs d'un Active Directory spécifique ou d'une base de données d'utilisateurs locaux.

 **REMARQUE** : La procédure suivante doit être effectuée uniquement par un administrateur de domaine qui joue également le rôle d'administrateur de stockage NAS.

Pour créer manuellement les dossiers de partage de base CIFS :

1. Vérifiez que votre système est joint à Active Directory dans le **NAS Manager (Gestionnaire NAS)**.
2. Si vous utilisez Active Directory, sélectionnez **Cluster Management (Gestion des clusters)** → **CIFS Configuration (Configuration CIFS)** dans **NAS Manager** et assurez-vous que l'option **Authenticate users' identity via Active Directory and local users database (Authentifier l'identité des utilisateurs via Active Directory et la base de données des utilisateurs locaux)** est sélectionnée.
3. Dans le **NAS Manager**, créez un partage d'accès général qui sera la racine de tous les dossiers des utilisateurs. Par exemple, dans le répertoire `/utilisateurs`, créez un partage d'accès général avec les mêmes `utilisateurs` de nom de partage et sélectionnez l'option de création du dossier si celui-ci n'existe pas déjà.
4. À l'aide de **Windows Explorer**, montez le partage `utilisateurs` en tant qu'administrateur CIFS local.
5. Dans le paramétrage de sécurité du partage monté, cliquez sur **Advanced (Avancé)** et modifiez le propriétaire en `Domain Admins (Administrateur de domaine)`, ou indiquez le compte d'administrateur de domaine ou administrateur de stockage que vous souhaitez rendre propriétaire.  
Il s'agit du compte qui crée les dossiers (à l'aide d'un script créé par l'utilisateur ou manuellement) pour chacun des partages de base des utilisateurs.
6. Déconnectez ou démontez le partage `utilisateur` et remontez-le en tant que compte propriétaire de ce dernier, tel que précédemment défini (en tant qu'Administrateur de domaine, Administrateur de stockage, ou la propriété de compte particulière sur laquelle il était défini).
7. Dans le **NAS Manager**, créez un nouveau partage CIFS et sélectionnez le type de partage **CIFS share containing a user-based directory tree (Partage CIFS contenant une arborescence de répertoire utilisateur)**.

8. Le partage d'accès général intitulé **utilisateurs** était précédemment créé depuis le chemin **/utilisateurs**. Sous **Path template (Modèle de chemin)**, saisissez **/utilisateurs**, puis choisissez si vous souhaitez que les dossiers des utilisateurs soient au format **/utilisateurs/nom d'utilisateur** ou **/utilisateurs/domaine/nom d'utilisateur**.
9. Cliquez sur **Save Changes (Enregistrer les changements)**.
10. À l'aide de **Windows Explorer**, créez un dossier conforme au modèle de chemin sélectionné à l'étape précédente pour chaque utilisateur auquel vous souhaitez octroyer un partage de base.  
Ceci est réalisable manuellement ou à l'aide d'un script créé par l'utilisateur.

## Définition de listes de contrôle des accès et d'autorisations des niveaux de partage sur FluidFS

Les partages CIFS FluidFS prennent en charge les listes de contrôle d'accès (ACL, Access Control Lists) et les autorisations des niveaux de partage (SLP, Share Level Permissions). Il est recommandé aux administrateurs de suivre les pratiques d'excellence définies par Microsoft. Les SLP traitent entièrement les droits de lecture, de modification et de contrôle de tout utilisateur ou groupe donné au niveau de partage, alors que les ACL fournissent plus de détails aux niveaux de dossier ou de fichiers. Il est recommandé de laisser la configuration par défaut de SLP (chaque utilisateur a un contrôle total) et d'utiliser les ACL pour contrôler l'accès au partage, à moins qu'il existe une exigence spécifique pour les SLP, qui ne peut pas être satisfaite à l'aide des ACL.

### Compte Administrateur local FluidFS

Un compte Administrateur local FluidFS intégré fournit des droits de configuration initiaux et de propriété aux nouveaux partages CIFS. Le compte sert à définir les ACL lorsque le service NAS n'est pas lié à un domaine Active Directory. Ce compte intégré est doté d'un mot de passe généré automatiquement à des fins de sécurité. Modifiez ce mot de passe si vous souhaitez utiliser ce compte pour définir des ACL ou SLP.

### Compte utilisateur à accès total CIFS (Utilisateur de secours)

La fonction de compte à accès total sert à octroyer un accès total d'utilisateur AD (**Active Directory**) à toutes les données sous-jacentes. Normalement, cette fonction s'utilise lorsqu'une appliance de virtualisation de stockage est utilisée avec le périphérique NAS FluidFS. Les appliances de ce type utilisent un compte AD pour accéder à tous les systèmes NAS sous-jacents.

Le système doit être membre d'un AD pour associer ce privilège à un compte AD. Le privilège Full Access User (Utilisateur à accès total) fournit au compte AD un accès total à toutes les données de tous les partages et volumes, quelles que soient les définitions ACL de fichier. Cependant, les paramètres SLP s'appliquent au compte AD détenant le privilège **Full Access User**. Il est de la responsabilité de l'administrateur système NAS de vérifier que le compte AD défini pour un utilisateur à accès total détient tous les SLP pertinents.

Pour gérer le compte Full Access User :

1. Connectez-vous à la CLI à l'aide d'une connexion KMV directe ou via SSH avec l'adresse IP virtuelle de gestion.
2. Pour définir le compte **Full Access User**, ou pour écraser l'entrée actuelle, exécutez la commande suivante dans la CLI :  

```
system authentication full-access-account set DOMAIN+username
```
3. Pour vérifier si le compte **Full Access User** est correctement défini, exécutez la commande suivante :  


```
system authentication full-access-account view
```
4. Pour supprimer le compte **Full Access User**, exécutez la commande suivante :  

```
system authentication full-access-account delete
```


## Configuration d'Active Directory


FluidFS peut se joindre à un domaine Active Directory. Pour ce faire, utilisez le NAS Manager, la **Cluster Management** → **Authentication** → **System Identity** (Gestion de clusters > Authentification > Identité système) ou la CLI. Pour en savoir plus sur la façon de rejoindre Active Directory à l'aide de la CLI, voir le *FluidFS Command Line Interface Guide* (Guide d'interface de ligne de commande FluidFS) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).

Pour joindre l'appliance NAS FluidFS au domaine Active Directory, vous devez fournir des références pour opération d'attachement.

 **REMARQUE** : Ces références sont requises uniquement pour opération d'attachement et ne sont ni stockées ni mises en cache par l'appliance NAS FluidFS.

L'administrateur peut choisir parmi trois options lorsqu'il détermine les références à utiliser pour joindre l'appliance NAS FluidFS à Active Directory :

- Joindre le cluster NAS à l'aide d'un compte Administrateur de domaine.
  -  **REMARQUE** : Il s'agit de la méthode recommandée.
- Joindre le cluster NAS au domaine Active Directory à l'aide d'un compte détenant le privilège **join a computer to the domain** (joindre un ordinateur au domaine) ainsi qu'un contrôle total sur tous les objets d'ordinateur du domaine.
- S'il s'agit d'un compte Administrateur de domaine ou d'un compte à contrôle total sur tous les objets d'ordinateur du domaine, vous ne pouvez pas l'utiliser. Voici les exigences minimales pour attacher l'appliance NAS au domaine Active Directory :
  - Un administrateur OU (Organizational Unit, Unité organisationnelle) détenant le privilège **join a computer to the domain**.
  - L'administrateur OU doit aussi détenir un contrôle total sur les objets dans cette OU, y compris les objets d'ordinateur.
  - Avant d'attacher le système au domaine, l'administrateur OU doit créer un objet d'ordinateur pour le système. Les privilèges de gestion sont fournis dans l'OU.
  - Le nom de l'objet d'ordinateur de l'appliance NAS et le nom NetBIOS utilisé lors de l'attachement doivent correspondre.
  - Lors de la création de l'objet d'ordinateur de l'appliance NAS, sélectionnez le compte admin OU sous dans le champ **User** (Utilisateur) ou **Group** (Groupe) sous « Permissions » (Droits) pour attacher l'objet au domaine. Ensuite, utilisez les références admin OU pour attacher l'appliance NAS.

 **REMARQUE** : Les clusters NAS FluidFS exigent un accès lecture pour l'attribut `tokenGroups` de tous les utilisateurs. La configuration par défaut d'Active Directory pour tous les ordinateurs de domaine autorise un accès en lecture pour l'attribut `tokenGroups`. Si l'autorisation est refusée, les utilisateurs de domaine Active Directory se trouvant dans des groupes ou OU emboîtés rencontrent des erreurs d'**Access Denied** (Accès refusé). Cependant, l'accès est autorisé aux utilisateurs qui ne sont pas en groupes ou OU imbriqués.

## Configuration des ACL ou des SLP sur un partage CIFS

La solution NAS FluidFS prend en charge deux niveaux de contrôle d'accès aux partages, fichiers et dossiers :

- Access Control Lists (ACL) (Listes de contrôle d'accès) : gère l'accès aux fichiers et dossiers spécifiques. L'administrateur peut contrôler un large éventail d'opérations que peuvent effectuer les utilisateurs et les groupes.
- Share Level Permissions (SLP) (Droits de niveaux de partage) : gère l'accès aux partages entiers. L'administrateur contrôle uniquement l'accès lecture, modification ou total à un partage entier.

Les ACL offrent un niveau de contrôle plus élevé et peuvent contrôler bien plus d'opérations que l'accès lecture/modification/total uniquement. Il est recommandé de laisser la configuration par défaut de SLP (chaque utilisateur a un contrôle total) et d'utiliser les ACL pour contrôler l'accès au partage, à moins qu'il n'existe des exigences spécifiques pour les SLP qui ne peuvent pas être satisfaites à l'aide des ACL.

À la création initiale d'un partage CIFS, le propriétaire du partage doit être modifié avant de définir une ACL ou de tenter d'accéder à ce partage. Si la solution en cluster NAS est jointe à un domaine Active Directory, les méthodes suivantes peuvent être utilisées pour définir les ACL :


- En utilisant un compte de domaine Active Directory dont le groupe principal est défini en tant que groupe Administrateurs du domaine.
- En utilisant le compte Administrateur local FluidFS (celui-ci est utilisé s'il n'est pas joint à Active Directory ou si les références d'Administrateur de domaine ne sont pas disponibles).

### Utilisation d'un compte Active Directory défini en tant que Groupe d'administrateurs du domaine

Pour utiliser un compte de domaine Active Directory dont le groupe principal est défini en tant que groupe Administrateurs du domaine :

1. Ouvrez **Windows Explorer** et entrez \\<AccessVip>\C\$ dans la barre d'adresse.  
La liste de tous les volumes NAS disponibles depuis le système FluidFS spécifié s'affiche sous forme de dossiers.
2. Double-cliquez sur le volume demandé.  
La liste de tous les partages CIFS de ce volume NAS s'affiche.
3. Effectuez un clic droit sur le partage (dossier) CIFS voulu et sélectionnez **Properties** (Propriétés).
4. Sélectionnez l'onglet **Security** (Sécurité) puis cliquez sur **Advanced** (Avancé).
5. Cliquez sur l'onglet **Owner** (Propriétaire), puis sur l'onglet **Modifier**.
6. Cliquez sur le bouton **Other users or groups...** (Autres utilisateurs ou groupes), puis choisissez le compte utilisateur d'administrateur du domaine qui définira les ACL pour ce partage ou choisissez le groupe Administrateurs du domaine.
7. Assurez-vous que la case **Replace owner on subcontainers and objects** (Remplacer le propriétaire sur les sous-conteneurs et les objets) est cochée, puis cliquez sur **Apply** (Appliquer).
8. Cliquez sur **Ok** et revenez à la fenêtre **Advanced Security Settings** (Paramètres de sécurité avancés).

Sélectionnez l'onglet **Permissions** (Droits) et suivez les pratiques d'excellence Microsoft pour attribuer des droits ACL au dossier de partage CIFS.

 **REMARQUE** : Si les partages CIFS et NFS sont tous les deux définis sur le même volume NAS, vous pouvez afficher les partages NFS et CIFS que contient/contiennent le(s) volume(s). Assurez-vous de sélectionner uniquement le partage CIFS demandé.

### Utilisation du compte Administrateur local FluidFS


1. Démarrez l'Assistant **Map network drive** (Adresser le lecteur réseau). Dans **Folder** (Dossier), entrez : \\<VIPAccès>\<nom-de-partage>.

 **REMARQUE** : Vous pouvez vous connecter au partage CIFS à l'aide du VIP d'accès client ou du nom DNS.

2. Sélectionnez l'option **Connect using different credentials** (Connexion à l'aide de références différentes).


Utilisez les références suivantes : NetBIOS Name\Administrator

Le nom NetBIOS par défaut est **CIFSStorage**.

 **REMARQUE** : Vous pouvez modifier le nom NetBios dans le NAS Manager (Gestionnaire NAS) en naviguant jusqu'à **System Management** → **Authentication** → **System Identity** (Gestion du système > Authentification > Identité du système).

3. Effectuez un clic droit sur le partage récemment adressé et sélectionnez **Propriétés** (Propriétés).
4. Sélectionnez l'onglet **Security** (Sécurité) puis cliquez sur **Advanced** (Avancé).
5. Cliquez sur l'onglet **Owner** (Propriétaire), puis sur l'onglet **Edit** (Modifier).
6. Cliquez sur le bouton **Other users or groups...** (Autres utilisateurs ou groupes) et sélectionnez le compte utilisateur admin de domaine qui définira les ACL de ce partage, ou choisissez le groupe Domain Admins (Administrateurs de domaine). Vous pouvez également utiliser le compte administrateur local CIFS.
7. Assurez-vous que la case **Replace owner on subcontainers and objects** (Remplacer le propriétaire sur les sous-conteneurs et les objets) est cochée, puis cliquez sur **Apply** (Appliquer).
8. Cliquez sur **Ok** et revenez à la fenêtre **Advanced Security Settings** (Paramètres de sécurité avancés).
9. Une fois le propriétaire défini, annulez l'adressage du lecteur réseau.
10. Adressez de nouveau le lecteur réseau en tant que compte admin de domaine défini comme propriétaire ou comme tout admin de domaine. Si le propriétaire est défini sur le groupe Domain Admins, suivez les pratiques d'excellence Microsoft et attribuez des droits ACL aux utilisateurs et groupes, au besoin.

Si le service NAS n'est pas joint à un domaine Active Directory, l'administrateur du compte administrateur CIFS intégré doit être utilisé pour définir toutes les ACL. Pour définir les SLP, utilisez la console MMC (Microsoft Management Console).

 **REMARQUE** : Ne tentez pas de créer un partage CIFS à l'aide de la console MMC.

### Adressage d'un lecteur du réseau au partage CIFS


Pour adresser un lecteur du réseau au partage CIFS sur lequel les ACL devront être définies :

1. Sélectionnez **Connect using a different user name (Se connecter sous un autre nom d'utilisateur)**.


Lorsque vous y êtes invité, utilisez les coordonnées suivantes :

<Nom NetBios>\Administrateur

Par défaut, le nom NetBios est **CIFSStorage**. S'il n'a pas été modifié, saisissez **CIFSStorage** \Administrator.

 **REMARQUE** : Vous pouvez modifier le nom NetBios dans le NAS Manager en naviguant jusqu'à **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **System Identity (Identité du système)**.

2. Suivez l'ensemble des instructions précédent pour définir le propriétaire du partage CIFS sur un compte d'utilisateur administrateur du domaine ou sur le groupe Administrateurs du domaine.
3. Une fois le propriétaire défini, annulez l'adressage du lecteur réseau.
4. Adressez à nouveau le lecteur du réseau à l'aide d'un compte faisant partie du groupe d'utilisateurs administrateurs de domaine sur lequel la propriété était précédemment définie. Suivez les meilleures pratiques de Microsoft et octroyez des permissions ACL aux utilisateurs et aux groupes, en conséquence.  
Si le service NAS n'est pas joint à un domaine Active Directory, le compte d'administrateur CIFS intégré *Administrateur* doit être utilisé pour définir toutes les ACL. Pour définir les SLP, utilisez la console MMC.

 **REMARQUE** : Ne tentez pas de créer un partage CIFS à l'aide de la console Microsoft Management Console (MMC).

### Accès à l'aide de CIFS

Microsoft Windows propose plusieurs méthodes de connexion aux partages CIFS.

Pour procéder à un adressage depuis Windows, sélectionnez l'une des options suivantes :

### Option 1 :

Exécutez la commande **net use** de l'invite de commande.

```
net use <lettre de lecteur>: \\< nom netbios> \< nom de partage >
```

### Option 2 :

1. Dans le menu **Start (Démarrer)**, sélectionnez **Run (Exécuter)**.  
La fenêtre **Run** s'affiche.
2. Saisissez le chemin d'accès au partage auquel vous souhaitez vous connecter :  
`\\<VIP d'accès client >\<nom partage>`.
3. Cliquez sur **OK**.  
La fenêtre de l'**Explorer (Explorateur)** s'affiche.

### Option 3

1. Ouvrez **Windows Explorer** et sélectionnez **Outils** → **Map Network Drive (Adresser un lecteur réseau)**.  
La boîte de dialogue **Map Network Drive** s'affiche.
2. Dans la liste déroulante **Drive (Lecteurs)**, sélectionnez n'importe quel lecteur disponible.
3. Saisissez le chemin d'accès dans le champ **Folder (Dossier)** ou naviguez jusqu'au dossier partagé.
4. Cliquez sur **Terminer**.

### Option 4



**REMARQUE** : Cette option vous permet de vous connecter au partage mais pas d'effectuer des adressages envers celui-ci.

1. Sur le **bureau** Windows, cliquez sur **Network neighborhood (Voisinage réseau)** et localisez l'appliance NAS.
2. Sélectionnez l'appliance NAS et double-cliquez dessus.
3. Dans la liste **CIFS shares (Partages CIFS)**, sélectionnez le partage auquel vous souhaitez vous connecter.

## Configuration des autorisations de niveau de partages CIFS

La configuration des autorisations de niveau partages (SLP) CIFS ne peut s'effectuer qu'à l'aide de la console Microsoft Management Console (MMC).

Les administrateurs peuvent utiliser un fichier MMC prédéfini (.msc) depuis le menu Démarrer de Windows Server 2000/2003/2008 et ajouter un snap-in de **Shared Folder (dossier partagé)** pour se connecter au cluster NAS.

La console MMC ne vous laisse pas choisir l'utilisateur avec lequel se connecter à un ordinateur à distance. Par défaut, la MMC utilise l'utilisateur connecté à la machine pour établir la connexion.

Pour utiliser le bon utilisateur dans la connexion MMC :

- Si l'appliance NAS que vous tentez de gérer est jointe à un répertoire Active Directory, connectez-vous à la station de gestion avec **<domaine>\Administrator**.
- Avant d'utiliser la MMC, connectez-vous à la solution en cluster NAS à l'aide de l'adresse IP virtuelle d'accès client située dans la barre d'adresses de Windows Explorer. Ouvrez une session avec le compte administrateur, puis connectez-vous à la MMC.

Si vous utilisez cette dernière méthode, vous devez d'abord redéfinir le mot de passe administrateur local.


Si aucun fichier MMC prédéfini n'existe :

1. Cliquez sur **Démarrer** → **Exécuter**.
2. Tapez `mmc` et cliquez sur **OK**.  
La fenêtre **Console 1 - [Console Root]** s'affiche.
3. Cliquez sur **File (Fichier)** → **Add/Remove Snap-in (Ajouter/Supprimer un snap-in)**.
4. Sélectionnez **Shared Folders (Dossiers partagés)**, puis cliquez sur **Add (Ajouter)**.
5. Dans la fenêtre **Shared Folders**, sélectionnez **Another computer (Un autre ordinateur)** et saisissez le nom de votre solution en cluster NAS (tel que configuré dans DNS). En variante, vous pouvez utiliser l'adresse IP virtuelle d'accès client.
6. Cliquez sur **Terminer**.  
La nouvelle arborescence des partages apparaît dans la fenêtre **Console Root (Racine de la console)**.
7. Cliquez avec le bouton droit sur le partage de votre choix et choisissez **Properties (Propriétés)** pour définir les autorisations de niveau partage.
8. Dans la fenêtre **Share Properties (Propriétés du partage)**, choisissez l'onglet **Share Permission (Autorisation du partage)**.

### Énumération de partage d'accès

Dans la 2e version du Dell Fluid File System, l'énumération de partages d'accès SLP est activée par défaut, ce qui signifie que lorsque les autorisations de niveau de partage (SLP) ne sont pas fournies, les utilisateurs et les groupes ne voient pas le partage. Si un utilisateur ou groupe ne possède pas d'autorisations de niveau de partage pour un partage spécifique, lorsque vous accédez au cluster NAS directement depuis `\\<adresse IP virtuelle d'accès client>`, le partage ne s'affiche pas du tout dans la liste des partages disponibles. Dans la version précédente, Dell Fluid File System v1, l'énumération de partages d'accès n'était pas activée, ce qui signifie que le partage s'affichait même si les utilisateurs ne pouvaient pas y accéder.

## Réinitialisation du mot de passe administrateur local CIFS

 **REMARQUE** : Pendant l'installation, un mot de passe est généré de manière aléatoire. Réinitialisez ce dernier.


Vous pouvez maintenant utiliser l'utilisateur administrateur pour parcourir la console MMC. Cet utilisateur est également appelé administrateur CIFS local.

Pour réinitialiser le mot de passe administrateur local CIFS :

1. Connectez-vous au NAS Manager.
2. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **Local Users (Utilisateurs locaux)**.  
L'écran **Local Users** s'affiche.
3. Choisissez l'utilisateur **Administrator (Administrateur)**.
4. Choisissez **Change password (Modifier le mot de passe)**.

## Quotas

Un quota de disque correspond à un ensemble de stratégies visant à restreindre l'espace disque et le nombre de fichiers utilisés par un utilisateur ou un groupe. Un quota peut également restreindre l'espace total utilisé dans un volume NAS ou l'utilisation des utilisateurs ou groupes au sein d'un volume NAS. Les valeurs de quota sont toujours relatives à un volume spécifique et sont indiquées en Mo.


 **REMARQUE** : Les utilisateurs et les groupes pour lesquels un quota individuel n'est pas défini utilisent le quota d'utilisateur/de groupe par défaut.

## Considérations de quota

- Considérations de quota lors de l'utilisation de volumes de types mélangés : pour les volumes NAS aux styles de sécurité mélangés, un quota unique doit être défini pour les utilisateurs Windows (Active Directory) et les utilisateurs UNIX (LDAP ou NIS). Les quotas de l'utilisateur Windows et UNIX sont indépendants l'un de l'autre, même si les utilisateurs sont adressés (automatiquement ou manuellement).
- Considérations de quota lors de l'accès à CIFS et NFS : pour les volumes NAS aux droits de styles NTFS ou UNIX, seul un quota unique doit être défini. La fonctionnalité d'adressage d'utilisateur prend en charge l'interopérabilité entre les protocoles. Les utilisateurs UNIX et Windows partagent le même quota que les comptes Windows et UNIX adressés.

## Gestion des quotas par défaut


Pour gérer les quotas par défaut d'un volume :

 **REMARQUE** : Le quota par défaut peut être remplacé par des quotas spécifiques à l'utilisateur ou au groupe.


1. Sélectionnez **User Access (Accès utilisateur)** → **Quota** → **Default (Par défaut)**.

L'écran **Default Quota (Quota par défaut)** s'affiche :


2. Dans la liste de **NAS Volume (Volumes NAS)**, sélectionnez le volume NAS approprié, auquel le quota peut être ajouté ou modifié.
3. Dans **Default quota per user (Quota par défaut par utilisateur)**, saisissez le quota utilisateur souhaité en Mo ou sélectionnez **Unlimited (Illimité)**.

 **REMARQUE** : Une fois cette limite dépassée, les opérations d'écriture sur le volume NAS sont interdites.


4. Dans **Alert administrator when quota reaches (Avertir l'administrateur lorsque le quota atteint)**, saisissez le quota utilisateur souhaité en Mo ou sélectionnez **Disabled (Désactivé)**.

 **REMARQUE** : Lorsque cette limite est dépassée, un message d'avertissement est envoyé à l'adresse e-mail du destinataire. Cet envoi par défaut s'effectue pour les utilisateurs pour lesquels aucun quota individuel n'est défini.

5. Dans **Default quota per group (Quota par défaut par groupe)**, saisissez le quota utilisateur souhaité en Mo ou sélectionnez **Unlimited (Illimité)**.

 **REMARQUE** : Une fois cette limite dépassée, les opérations d'écriture sur le volume NAS sont interdites.

6. Dans **Alert administrator when quota reaches (Avertir l'administrateur lorsque le quota atteint)**, saisissez le quota de groupe souhaité en Mo ou sélectionnez **Disabled (Désactivé)**.

 **REMARQUE** : Lorsque cette limite est dépassée, un message d'avertissement est envoyé à l'adresse e-mail de l'administrateur. Cet envoi par défaut s'effectue pour les utilisateurs pour lesquels aucun quota individuel n'est défini.

7. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Gestion de quotas spécifiques à l'utilisateur ou au groupe

### Affichage des quotas spécifiques à l'utilisateur ou au groupe existant

Pour afficher les détails d'un quota spécifique à un utilisateur ou un groupe :

1. Sélectionnez **User Access (Accès utilisateur)** → **Quota** → **User/Group (Utilisateur/Groupe)**.

La page **User/Group Quota (Quota de l'utilisateur/du groupe)** s'affiche.

2. Dans la liste **Show quotas for NAS Volume (Afficher les quotas du volume NAS)**, sélectionnez le volume NAS approprié ou **All NAS Volumes (Tous les volumes)**.

La liste **User/Group Quota for the selected NAS volume (Quota d'utilisateur/du groupe disponible pour le volume NAS sélectionné)** s'affiche. Par défaut, les informations relatives au quota de l'utilisateur/du groupe de **tous les volumes NAS** s'affiche.

### Types de quota

Les types de quota suivants sont disponibles :

- User (Utilisateur) : quota par utilisateur.
- All of group (Tout le groupe) : quota total pour l'ensemble du groupe.
- Any user in group (Tout utilisateur dans le groupe) : quota par utilisateur pour tout utilisateur appartenant au groupe.

### Ajout de quotas spécifiques à l'utilisateur/au groupe

Pour ajouter un quota :

1. Sélectionnez **User Access (Accès utilisateur) → Quota → User/Group (Utilisateur/Groupe)**.


La page **User/Group Quota (Quota d'utilisateur/de groupe)** s'affiche.

2. Cliquez sur **Add (Ajouter)**.


La page **Create Quota (Créer un quota)** apparaît.

3. Dans la liste de **NAS Volume (Volumes NAS)**, sélectionnez le volume NAS approprié que vous souhaitez ajouter au quota.


4. Dans la liste **Quota for (Quota pour)**, sélectionnez le type de restriction de quota souhaité, puis saisissez le nom d'utilisateur ou de groupe ou cliquez sur le bouton **Browse (Parcourir)** pour sélectionner l'utilisateur ou le groupe approprié.


 **REMARQUE** : Afficher la liste des utilisateurs peut prendre un certain temps, selon le nombre d'utilisateurs présents dans votre domaine Active Directory. Pendant ce temps, des échecs d'authentifications sporadiques peuvent survenir. Si vous connaissez le nom d'utilisateur, saisissez-le au lieu d'afficher la liste des utilisateurs.

5. Dans **Quota**, saisissez le quota en Mo ou cliquez sur **Unlimited (Illimité)**.

 **REMARQUE** : Si l'utilisateur ou le groupe utilise déjà ces données, aucune nouvelle écriture n'est permise.

6. Dans **Alert administrator when quota reaches (Avertir l'administrateur lorsque le quota atteint)**, saisissez le quota de groupe souhaité en Mo ou sélectionnez **Disabled (Désactivé)**.

 **REMARQUE** : Lorsque cette limite est dépassée, un message d'avertissement est envoyé à l'adresse e-mail de l'administrateur.

 **REMARQUE** : Cet envoi par défaut est utilisé pour les utilisateurs pour lesquels aucun quota individuel n'est défini.

7. Cliquez sur **Save Changes (Enregistrer les changements)**.

### Quotas spécifiques à l'utilisateur/au groupe

Pour modifier un quota existant :

1. Sélectionnez **User Access (Accès utilisateur) → Quota → User/Group (Utilisateur/Groupe)**.

La page **User/Group Quota (Quota de l'utilisateur/du groupe)** s'affiche.

2. Dans la liste **des volumes NAS**, sélectionnez le volume NAS approprié.

La table **User/Group Quota** affiche la liste des **User/Group Quotas (Quotas de l'utilisateur/du groupe)** du volume NAS sélectionné.

3. Dans la liste des quotas de l'utilisateur/du groupe disponibles, sous **Name/ID (Nom/ID)**, cliquez sur le quota de l'utilisateur/du groupe pertinent.

La page **Edit Quota (Modifier un quota)** apparaît.

4. Modifiez les stratégies de quota au besoin, puis cliquez sur **Save Changes (Enregistrer les modifications)**.

### Suppression d'un quota

Pour supprimer une stratégie de quota :

1. Sélectionnez **User Access (Accès utilisateur) → Quota → User/Group (Utilisateur/Groupe)**.

La page **User/Group Quota (Quota de l'utilisateur/du groupe)** s'affiche.

2. Dans la liste **des volumes NAS**, sélectionnez le volume NAS approprié.

La table **User/Group Quota** affiche la liste des **User/Group Quotas (Quotas de l'utilisateur/du groupe)** du volume NAS sélectionné.

3. Dans la liste User/Group Quotas, sélectionnez le quota approprié, puis cliquez sur **Delete (Supprimer)**.

# Protection des données sur la solution en cluster NAS FluidFS

La protection des données fait partie intégrale de toute infrastructure de stockage. Vous pouvez configurer différentes méthodes de protection des données dans votre système de fichiers Dell Fluid, notamment :



- Instantanés
- Réplication
- Restauration du système depuis la sauvegarde
- Configuration de l'agent de sauvegarde

## Instantanés

La technologie d'instantanés crée une sauvegarde point dans le temps des données d'un volume. Il existe diverses stratégies pouvant être définies pour la création d'un instantané. Ces stratégies incluent quand un instantané peut être pris, combien peuvent être conservés et l'espace pouvant être utilisé sur le volume NAS avant que les instantanés ne soient supprimés. Les instantanés sont basés sur un ensemble de modifications. À la création du premier instantané d'un volume NAS, tous les instantanés créés après l'instantané de ligne de base sont un delta (différentiel) de l'instantané précédant.

Pour en savoir plus sur les instantanés, reportez-vous à l'*aide en ligne*.

## Ajout ou modification d'une stratégie d'instantané

1. Sélectionnez **Data Protection (Protection des données)** → **Snapshots (Instantanés)** → **Policies (Stratégies)**.  
La page **Snapshot policies (Stratégies d'instantané)** apparaît.
2. Dans la liste des **NAS Volume (volumes NAS)**, sélectionnez le volume NAS approprié.
3. Sous **Alert the administrator when snapshot space is % of total volume (Avertir l'administrateur lorsque l'espace de l'instantané est à % du volume total)**, saisissez le pourcentage de l'espace total du volume NAS.  
Lorsque cette limite est dépassée, les instantanés sont automatiquement supprimés.  
 **REMARQUE** : Laissez ce champ vide pour désactiver les événements d'espace d'instantané.  
 **REMARQUE** : Les instantanés planifiés et créés par l'utilisateur sont supprimés. Les instantanés de réplication sont conservés.
4. Sélectionnez **Periodic (Périodique)** pour prendre des instantanés au cours de périodes de moins d'une heure :
  - a) Sélectionnez la fréquence en minute dans la liste **Every Minutes (Toutes les minutes)**.
  - b) Saisissez le **nombre d'instantanés à conserver**.
5. Sélectionnez **Hourly (Toutes les heures)** pour prendre des instantanés toutes les heures.
  - a) Vous pouvez soit sélectionner **Every hour (Toutes les heures)**, soit sélectionner **At (À)** et saisir l'heure et les **minutes** spécifiques auxquelles les instantanés sont à prendre.
  - b) Saisissez le **Number of snapshots to keep (nombre d'instantanés à conserver)**.
6. Sélectionnez **Daily (Tous les jours)** pour prendre des instantanés tous les jours.

- a) Vous pouvez soit sélectionner **Every day (Tous les jours)**, soit sélectionner **On (Le)** et saisir des jours spécifiques.
  - b) Sous **At**, sélectionnez l'heure à laquelle l'instantané doit être généré.
  - c) Saisissez le **Number of snapshots to keep (nombre d'instantanés à conserver)**.
7. Sélectionnez **Weekly (Toutes les semaines)** pour prendre des instantanés toutes les semaines.
    - a) Dans la liste **On (Le)**, sélectionnez le jour et l'heure de génération de l'instantané.
    - b) Saisissez le **Number of snapshots to keep (nombre d'instantanés à conserver)**.
  8. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Création d'un instantané (sans stratégie)

1. Sélectionnez **Data Protection (Protection des données)** → **Snapshots (Instantanés)** → **List (Liste)**.  
La page **Snapshots List (Liste des instantanés)** affiche la liste des instantanés existants. Par défaut, les instantanés de tous les volumes NAS sont affichés.
2. Cliquez sur **Create (Créer)**.  
La page **Create Snapshot (Créer un instantané)** apparaît.
3. Dans la liste des **NAS Volume (Volumes NAS)**, sélectionnez le volume NAS approprié.
4. Dans **Snapshot name (Nom d'instantané)**, saisissez le nom du nouvel instantané.
5. Cliquez sur **Create (Créer)**.  
Le nouvel instantané est créé et ajouté à la liste des instantanés de la page **Snapshots List (Liste des instantanés)**.

## Accès aux instantanés


Après la création d'un instantané, vous pouvez accéder à un dossier spécial de l'exportation ou du partage.

Accédez au dossier spécial depuis UNIX sous le répertoire appelé **.snapshots** (instantanés) sous chaque exportation NFS.

Accédez au dossier spécial Microsoft Windows du répertoire **.snapshots (instantanés)** sous chaque Partage. (Cela permet l'intégration à Shadow Copies (duplication en miroir) et active les versions précédentes.)

Les instantanés conservent le même style de sécurité que le système de fichiers actif. Ainsi, même lorsqu'ils utilisent les instantanés, les utilisateurs ne peuvent qu'accéder à leurs propres fichiers, conformément aux autorisations existantes. Les données qui sont disponibles lorsque vous accédez à un instantané spécifique sont au même niveau que le partage spécifique et ses sous-répertoires, assurant ainsi que les utilisateurs ne puissent pas accéder à d'autres parties du système de fichiers.

## Modification d'un instantané

 **REMARQUE** : Vous pouvez modifier le **Snapshot name (nom de l'instantané)**.

1. Sélectionnez **Data Protection (Protection des données)** → **Snapshots (Instantanés)** → **List (Liste)**.  
La page **Snapshots List (Liste des instantanés)** affiche la liste des instantanés existants. Par défaut, les instantanés de tous les volumes NAS sont affichés.
2. Dans la liste **Show Snapshots for NAS Volume (Afficher les instantanés de volumes NAS)**, sélectionnez le volume NAS approprié ou sélectionnez **All NAS volumes (Tous les volumes NAS)**.  
Les instantanés existants des volumes NAS sélectionnés s'affichent.
3. Dans la liste des instantanés disponibles, dans la colonne **Name (Nom)**, cliquez sur l'instantané pertinent.  
L'écran **Edit Snapshot (Modifier l'instantané)** apparaît.

4. Dans **Snapshot name (Nom de l'instantané)**, modifiez le nom existant.
5. Cliquez sur **Calculate Snapshot Delta (Calcul différentiel d'instantané)** pour calculer l'espace réel libéré par le retrait d'un instantané.
6. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Restauration des données

La restauration des données peut s'effectuer de deux façons :

- Copier-coller : restaurations de fichiers individuels  
Si vous avez supprimé ou modifié un fichier par inadvertance et souhaitez le restaurer, accédez au répertoire d'instantanés situé dans le dossier d'exportation ou partage actuel, localisez l'instantané souhaité (selon son heure de création) et copiez le fichier dans son emplacement d'origine. Cette méthode est utile pour les activités quotidiennes de restauration de fichier individuel.
- Restauration d'un volume NAS depuis un instantané.  
Si vous devez restaurer un volume dans son intégralité (en cas d'erreur d'application ou d'attaques de virus) où l'action copier-coller de quantités importantes de données prend beaucoup de temps, le volume NAS peut être restauré dans son intégralité.

## Suppression d'un instantané

1. Sélectionnez **Data Protection (Protection des données) → Snapshots (Instantanés) → List (Liste)**.  
La page **Snapshots List (Liste des instantanés)** affiche la liste des instantanés existants. Par défaut, les instantanés de tous les volumes NAS sont affichés.
2. Dans la liste **Show Snapshots for NAS Volume (Afficher les instantanés de volumes NAS)**, sélectionnez le volume NAS approprié ou sélectionnez **All NAS volumes (Tous les volumes NAS)**.  
Les instantanés existants des volumes NAS sélectionnés s'affichent.
3. Dans la liste des instantanés disponibles, sélectionnez l'instantané pertinent, puis cliquez sur **Delete (Supprimer)**.

## Restauration d'un volume NAS depuis un instantané

1. Sélectionnez **Data Protection (Protection des données) → Snapshots (Instantanés) → Restore (Restaurer)**.  
La page **Snapshot Restore (Restauration d'un instantané)** apparaît.
2. Dans **Choose the volume to be reverted (Choisir le volume à restaurer)**, sélectionnez le volume NAS approprié.  
La liste **Choose a snapshot for revision (Choisir un instantané à réviser)** affiche les instantanés du volume NAS sélectionné.
3. Dans **Choose a snapshot for revision (Choisir un instantané à réviser)**, sélectionnez l'instantané que vous souhaitez utiliser pour la restauration du volume.
4. Cliquez sur **Next (Suivant)**.  
Un message apparaît vous fournissant des instructions que vous devez suivre avant de lancer le processus de restauration.
5. Pour restaurer le volume NAS vers l'instantané sélectionné, cliquez sur **Yes (Oui)**.  
Le volume NAS est restauré à l'instantané.

 **PRÉCAUTION : L'opération de restauration ne peut pas être annulée. Toutes les données créées ou modifiées après la prise de l'instantané seront complètement effacées suite à la restauration.**

# Réplication

La réplication des solutions NAS Dell FluidFS est basée sur les blocs et asynchrone.

- Basée sur les blocs : seuls les blocs auxquels des modifications ont été apportées sont répliqués, et non l'intégralité du fichier
- Asynchrone : la communication avec le client continue même lorsque les données sont en cours de réplication

La réplication est utilisée dans divers scénarios pour atteindre différents niveaux de protection des données. Voici certains des scénarios :

<b>Sauvegarde et restauration rapides</b>	Maintenir des copies intégrales des données pour la protection contre la perte ou la correction des données, ou contre les erreurs d'utilisateurs.
<b>Restauration après sinistre</b>	Mettre les données en miroir sur des emplacements distants pour le basculement.
<b>Accès des données à distance</b>	Les applications permettent l'accès aux données écrites en symétrie en mode lecture-seule ou lecture-écriture.
<b>Migration des données en ligne</b>	Réduire le temps d'arrêt associé à la migration des données.


La réplication tire profit de la technologie d'instantané dans le système de fichiers de la solution en cluster NAS. Après la première réplication, seuls les deltas sont répliqués. Ceci permet une réplication plus rapide et une utilisation efficace des cycles du processeur. Cela économise également de l'espace de stockage tout en conservant la cohérence des données.

La réplication est basée sur les volumes et peut être utilisée pour répliquer les volumes sur la même appliance NAS ou pour répliquer un volume sur une autre appliance NAS. Lorsque vous répliquez un volume sur une autre appliance NAS, celle-ci doit être configurée en tant que partenaire de réplication.

## Partenaires de réplication

Une fois la relation de partenariat établie, la réplication est bidirectionnelle. Un système peut contenir des volumes cible et source de l'autre système et ainsi effectuer des réplifications sur cet autre système. Les données de réplication passent par un tunnel SSH sécurisé d'un système à l'autre sur un réseau client.

Vous pouvez configurer une stratégie de réplication pour qu'elle s'exécute selon différentes planifications ou à la demande. Toutes les configurations système (quotas utilisateur, stratégie d'instantanés, etc.) sont stockées sur chaque volume. Lorsqu'un volume est répliqué, le volume cible contient les mêmes informations. Lors de la suppression d'une stratégie de réplication, l'option de transférer la configuration du volume vous est offerte.

 **REMARQUE** : Les partenaires de réplication doivent disposer du même nombre de contrôleurs. Par exemple, ne tentez pas de répliquer une appliance à quatre contrôleurs vers une appliance à deux contrôleurs.

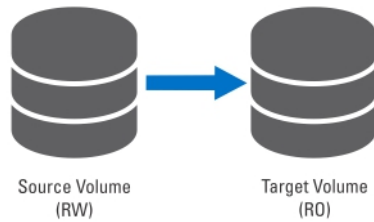


Figure 4. Réplication locale

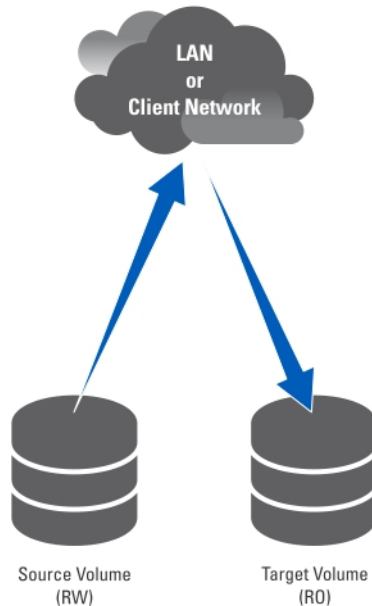


Figure 5. Réplication du partenaire

### Affichage des partenaires de réplication existants

Vous pouvez afficher la liste des partenaires de réplication. Pour afficher les partenaires de réplication auxquels le système sélectionné fait confiance, sélectionnez **Data Protection** → **Replication** → **Replication Partners** (Protection des données > Réplication > Partenaires de réplication). L'écran **Replication Partners** (Partenaires de réplication) affiche la liste des noms de partenaires de réplication existants.


### Configuration d'un partenaire de réplication

Sur un système distant, le système source devient également un partenaire. Il s'agit d'une réplication bidirectionnelle de confiance. Les volumes source et cible peuvent se trouver sur l'un ou l'autre système.

Pour ajouter des partenaires de réplication :

1. Sélectionnez **Data Protection (Protection des données)** → **Replication (Réplication)** → **Replication Partners (Partenaires de réplication)**.  
L'écran **Replication Partners (Partenaires de réplication)** s'affiche.
2. Cliquez sur **Add (Ajouter)**.  
L'écran **Add Replication Partner (Ajouter un partenaire de réplication)** s'affiche.
3. Sous **Remote NAS management VIP (Adresse IP virtuelle de gestion NAS distante)**, saisissez l'adresse IP virtuelle du NAS Manager du système distant.

4. Sous **User name (Nom d'utilisateur)** et **Password (Mot de passe)**, saisissez le nom d'utilisateur et le mot de passe d'un compte administrateur du système distant.

 **REMARQUE** : Ces valeurs ne sont pas stockées dans le Dell Fluid File System.

5. Cliquez sur **Save Changes (Enregistrer les changements)**.

### Modification de la configuration d'un partenaire de réplication

Vous pouvez modifier la configuration d'un partenaire de réplication en modifiant ses paramètres.

Pour modifier les paramètres d'un partenaire de réplication :

1. Sélectionnez **Data Protection (Protection des données)** → **Replication (Réplication)** → **Replication Partners (Partenaires de réplication)**.  
L'écran **Replication Partners** affiche la liste des noms des partenaires de réplication existants..
2. Sous **Replication Partner Name (Nom de partenaires de réplication)**, sélectionnez le nom du partenaire de réplication approprié.  
La page **Edit Replication Partner (Modifier le partenaire de réplication)** s'affiche.
3. Sous **Remote NAS management VIP (Adresse IP virtuelle de gestion NAS distante)**, modifiez l'adresse IP virtuelle, au besoin.
4. Sous **User name (Nom d'utilisateur)** et **Password (Mot de passe)**, modifiez les coordonnées admin, au besoin.
5. Cliquez sur **Save Changes (Enregistrer les changements)**.

### Suppression d'un partenaire de réplication

Vous pouvez supprimer le partenaire de réplication du système en le supprimant de la liste des partenaires de réplication. Lorsque vous supprimez un partenaire de réplication, assurez-vous que les deux systèmes fonctionnent correctement. Si l'un des systèmes est en panne ou non accessible, un message d'avertissement s'affiche.

Pour supprimer la configuration d'un partenaire de réplication :


1. Sélectionnez **Data Protection (Protection des données)** → **Replication (Réplication)** → **Replication Partners (Partenaires de réplication)**.  
L'écran **Replication Partners** affiche la liste des noms des partenaires de réplication existants..
2. Dans la liste des partenaires de réplication existants, sélectionnez le partenaire de réplications, puis cliquez sur **Delete (Supprimer)**.

### Stratégies de réplication NAS

La réplication entre les volumes est gérée par des stratégies. Vous pouvez créer une stratégie de réplication NAS, également appelée connexion de volumes, via le NAS Manager, en procédant comme suit :

1. Créez un niveau de confiance entre les système source et cible.  
Pour ce faire, saisissez l'adresse IP du système distant ainsi qu'un nom d'utilisateur de type administrateur et un mot de passe associé.
2. Ajoutez la stratégie de réplication.  
Pour ce faire, sélectionnez le volume source, le volume cible, et indiquez la planification périodique de la réplication.  
Si des données du système cible ne sont pas accessibles depuis le système source, un avertissement est émis et vous êtes invité à autoriser la perte de ces données.
3. Surveillez l'avancement de la réplication.  
Vérifiez que la réplication s'exécute sans problème.

Vous pouvez supprimer la stratégie de réplication, rendant ainsi le système cible accessible en écriture. Pour en savoir plus sur les stratégies de réplication NAS, voir la rubrique *Online Help (Aide en ligne)*.

 **REMARQUE** : Les volumes cibles de réplication sont en **lecture seule** lorsqu'ils sont associés à une stratégie de réplication.

### Ajout d'une stratégie de réplication

1. Sélectionnez **Data Protection (Protection des données) → Replication (Réplication) → NAS Replication (Réplication NAS)**.  
La page **NAS Replication** affiche une liste des stratégies de réplication NAS existantes.
2. Cliquez sur **Add (Ajouter)**.  
La page **Add NAS Replication Policy (Ajouter une stratégie de réplication NAS)** s'affiche.
3. Sous **Source NAS Volume (Volume NAS source)**, saisissez le nom du volume NAS source ou cliquez sur le bouton **Browse (Parcourir)** et sélectionnez le volume NAS approprié.
4. Dans la liste **Destination cluster (clusters cibles)**, sélectionnez l'un des éléments suivants :
  - **localhost** pour répliquer le volume source dans ce système.
  - un autre partenaire de réplication Dell Fluid File System.
5. Sous **Destination NAS Volume (Volume NAS cible)**, saisissez le nom du volume NAS cible ou cliquez sur le bouton **Browse (Parcourir)** et sélectionnez le volume NAS approprié.
6. Sélectionnez l'une des options de planification de point de restauration suivantes :
  - **Répliquer toutes les heures après**
  - **Répliquer tous les jours à**
  - **Répliquer toutes les semaines le**
  - **Répliquer à la demande (non planifié)**
7. Cliquez sur **Save Changes (Enregistrer les changements)**.

### Modification des stratégies de réplications

1. Sélectionnez **Data Protection (Protection des données) → Replication (Réplication) → NAS Replication (Réplication NAS)**.  
La page **NAS Replication** affiche une liste des stratégies de réplication NAS existantes.
2. Sélectionnez le volume NAS approprié dans la colonne **Source NAS Volume (Volume NAS source)**.  
La page **Edit NAS Replication Policy (Modifier la stratégie de réplication NAS)** s'affiche.
3. Sous **Source NAS Volume**, saisissez le nom du volume NAS source ou cliquez sur le bouton **Browse (Parcourir)** et sélectionnez le volume NAS approprié.
4. Dans la liste **Destination cluster (clusters cibles)**, sélectionnez l'un des éléments suivants :
  - **localhost** pour répliquer le volume source dans ce système.
  - un autre partenaire de réplication Dell Fluid File System.
5. Sous **Destination NAS Volume (Volume NAS cible)**, saisissez le nom du volume NAS cible ou cliquez sur le bouton **Browse (Parcourir)** et sélectionnez le volume NAS approprié.
6. Sélectionnez l'une des options de planification de point de restauration suivantes :
  - **Répliquer toutes les heures après**
  - **Répliquer tous les jours à**
  - **Répliquer toutes les semaines le**
  - **Répliquer à la demande (non planifié)**

7. Cliquez sur **Save Changes (Enregistrer les changements)**.


## Pause, reprise et exécution de la réplication NAS

Vous pouvez mettre en pause, reprendre ou exécuter la réplication NAS à la demande, selon l'état du volume NAS sélectionné.

1. Sélectionnez **Data Protection (Protection des données) → Replication (Réplication) → NAS Replication (Réplication NAS)**.  
La page **NAS Replication** affiche la liste des stratégies de réplication NAS existantes.
2. Dans la liste des volumes NAS existants, sélectionnez le volume NAS approprié.
3. Cliquez sur **Pause** pour mettre la réplication NAS sélectionnée en attente.
4. Cliquez sur **Resume (Reprendre)** pour poursuivre la réplication NAS sélectionnée.
5. Cliquez sur **Replicate Now (Répliquer maintenant)** pour lancer immédiatement la réplication des volumes NAS sélectionnés.

## Suppression d'une stratégie de réplication

Lors de la suppression d'une stratégie de réplication, les deux volumes contiennent la configuration système du système source. Le transfert de la configuration système du système source vers le volume du système cible est facultatif. Cette configuration comprend les utilisateurs, les quotas, les stratégies d'instantanés, le style de sécurité et d'autres propriétés. Cette option s'avère utile pour la restauration après sinistre.

 **REMARQUE** : Si la stratégie de réplication est supprimée du système du volume cible, un avertissement est émis et la stratégie doit également être supprimée du système source.

Pour supprimer la stratégie de réplication :

1. Sélectionnez **Data Protection (Protection des données) → Replication (Réplication) → NAS Replication (Réplication NAS)**.  
La page **NAS Replication** affiche une liste des stratégies de réplication NAS existantes.
2. Dans la liste de volumes NAS existants, sélectionnez le volume NAS approprié et cliquez sur **Delete (Supprimer)**.

## Restauration après sinistre à l'aide de la réplication


Vous pouvez utiliser les fonctions de réplication pour reconstruire un cluster source (cluster A) depuis son cluster de sauvegarde (cluster B).

 **REMARQUE** :

- **Cluster A** : le cluster source contenant les données à sauvegarder.
- **Cluster B** : le cluster de sauvegarde qui est pleinement configuré mais ne possède aucun volume et sauvegarde les données du cluster source A.

Avant de définir la restauration après sinistre sur la réplication, assurez-vous que les conditions suivantes sont remplies :

- Les clusters A et B sont de mêmes type et configuration.

 **REMARQUE** : Par exemple, si le cluster A est un système NX3600 avec quatre processeurs à quatre cœurs, le cluster B doit également être un système NX3600 avec quatre processeurs à quatre cœurs.

- La version de réplication du cluster B est identique à celle du cluster A.
- Le cluster B dispose d'un espace suffisant pour répliquer les données du cluster A.

- Les paramètres réseau (client, SAN, IC etc.) du cluster B sont différents de ceux du cluster source A ; cependant, les deux clusters doivent pouvoir communiquer l'un avec l'autre pour que la réplication puisse se produire.

La restauration après sinistre à l'aide de la réplication comprend trois phases :

- Phase 1 : construction d'une structure de réplication entre le cluster A et cluster B
- Phase 2 : basculement vers le cluster B à la demande du client suite à l'échec du cluster A
- Phase 3 : restauration du cluster A par restauration automatique depuis le cluster B

### Configuration DNS d'un basculement de volume unique

Pour un basculement de volume unique, il est essentiel que l'environnement soit configuré pour bien migrer les utilisateurs des volumes NAS que vous basculez, sans déranger les autres utilisateurs d'autres volumes NAS que vous ne basculez pas.


Si un volume NAS est basculé d'un cluster NAS à l'autre, les adresses IP utilisées pour y accéder passent des adresses IP du cluster A à l'adresse IP du cluster B. Il vous est recommandé de faciliter ce changement à l'aide de DNS.

Lorsqu'un basculement de volume unique est nécessaire, il vous est recommandé de configurer une entrée DNS pour qu'elle soit en corrélation avec chaque volume DNS et de modifier l'entrée DNS des volumes uniques lorsque ceux-ci sont basculés.

Par exemple, les services de Marketing et de Ventes ont leurs propres volumes NAS dotés d'un partage CIFS nommé *marketing\_share* et *sales\_share*. Une entrée DNS nommée *FluidFSmarketing* est créée pour le Marketing et une entrée DNS nommée *FluidFSsales* est créée pour les Ventes. Les deux volumes désignent le même ensemble de VIP d'accès client sur le cluster A source. Le Marketing peut accéder au volume ou partage de Marketing à l'aide de `\FluidFSmarketing\marketing` et les Ventes peuvent accéder au volume ou partage de Ventes à l'aide de `\FluidFSsales\sales`.


Au début, les deux entrées DNS *FluidFSmarketing* et *FluidFSsales* désignent le même ensemble de VIP d'accès client. À ce moment-là, vous pouvez accéder aux partages *marketing* et *sales* depuis l'un des noms DNS, *FluidFSmarketing* ou *FluidFSsales*. Lorsque vous souhaitez basculer un volume unique (par exemple *Marketing*), modifiez les entrées DNS de *FluidFSmarketing* pour résoudre les VIP d'accès client du cluster B.

Il vous est recommandé de maintenir un tableau pour effectuer un suivi des entrées DNS utilisées pour accéder à chaque volume NAS. Ceci est utile lors des basculements et de la configuration des stratégies de groupes.

 **REMARQUE :** Un cluster NAS FluidFS unique peut contenir deux ensembles de partages d'accueil. Disons, par exemple, que le cluster A et le cluster B possèdent tous les deux des partages d'accueil pour différents sites ou bases d'utilisateur. Les clusters A et B servent tous les deux de destinations de réplication du volume NAS de chaque cluster, qui contiennent les partages d'accueil. Au cas où l'administrateur souhaiterait basculer le volume NAS (qui contient les partages d'accueil) du cluster A au cluster B, le cluster B rejette cette opération car il possède déjà des partages d'accueil définis.

### Phase 1: construire le partenariat de réplication entre le cluster source A et le cluster de sauvegarde B

1. Connectez-vous au cluster A.
2. Configurez le partenariat de réplication entre le cluster source A et le cluster de secours B.  
Pour en savoir plus sur la configuration des partenaires de réplication, voir [Configuration d'un partenaire de réplication](#).
3. Créez une stratégie de réplication pour tous les volumes sources dans le cluster A aux volumes cibles du cluster B.  
Pour en savoir plus sur la création de stratégies de réplication, voir [Ajout d'une stratégie de réplication](#).


 **REMARQUE** : La stratégie de réplication a une correspondance un à un sur une base de volumes, par exemple :

Volume source A1 (cluster A) au volume cible B1 (cluster B)

Volume source A2 (cluster A) au volume cible B2 (cluster B)

.....


Volume source  $n$  (cluster A) au volume cible B  $n$  (cluster B)

 **REMARQUE** : FluidFS v2 prend en charge la génération automatique de volumes cible pendant l'ajout de la stratégie de réplication. Pour FluidFS 1.0, vous devez créer les volumes cible dans le cluster B et vous assurer que le volume est assez grand pour supporter les données correspondantes du volume source du cluster A.

4. Lancez le planificateur de réplications pour assurer qu'au moins une réplication a réussi pour tous les volumes sources du cluster A.

Si la réplication échoue, corrigez les problèmes rencontrés et redémarrez le processus de réplication. Cela assure que tous les volumes sources du cluster A ont au moins une copie de réplication réussie dans le cluster B.

Configurez une planification de réplications régulière pour qu'une copie de réplication à jour du cluster A se trouve toujours dans le cluster B.

 **PRÉCAUTION** : La restauration de la réplication n'est pas une restauration BMR complète car la méthode de réplication ne permet pas la sauvegarde et la restauration de certains paramètres, tels que la configuration réseau (client, SAN et IC). Prenez note de tous les paramètres du cluster A (que vous utiliserez pour la restauration du cluster A), notamment la configuration réseau et les paramètres de cluster (tels que le nom du volume, les paramètres d'alerte et ainsi de suite). Si la restauration du système ne restaure pas ces paramètres, vous pouvez les restaurer vous-même manuellement à leurs valeurs d'origine.

## Phase 2 : basculement vers le cluster B à la demande du client suite à l'échec du cluster A

Si le cluster source A ne répond plus en raison d'une panne imprévue, (matériel, disque etc.), procédez comme suit :

1. Connectez-vous au cluster de sauvegarde B.
2. Supprimez la stratégie de réplication existante de tous les volumes cible de réplication.
  - Lors de la suppression de la stratégie de réplication du cluster B de destination : le gestionnaire de réplication FluidFS tente de contacter le cluster A source, qui échoue. La configuration du cluster B de destination doit être restaurée à l'aide de **Cluster Management** → **Restore NAS Volume Configuration**. (**Gestion de cluster > Restaurer la configuration de volumes NAS**)
  - Lors de la suppression de la stratégie de réplication du cluster A source : vous avez l'option d'appliquer la configuration du volume source au volume de destination. Si vous ne sélectionnez pas cette option ou si l'option échoue, vous pouvez restaurer la configuration du volume source du cluster A sur le volume de destination du cluster B à l'aide de **Cluster Management** → **Restore NAS Volume Configuration**. (**Gestion de cluster > Restaurer la configuration de volumes NAS**)
3. Confirmez la suppression de la stratégie de réplication sur le cluster de sauvegarde B et appliquez la configuration du volume source depuis le cluster A.

Les configurations de volume suivantes peuvent actuellement être restaurées :

- Exportations NFS
- Partages CIFS
- Stratégies de quota
- Planification d'instantanés
- Paramètres d'alerte, de style de sécurité et paramètres connexes du volume NAS
- Nom du volume NAS
- Taille du volume NAS

Ceci transforme les volumes cible (B1, B2, .. B*n*) en volumes autonomes. Répétez cette procédure pour transformer tous les volumes cible du cluster B en volumes autonomes en appliquant la configuration de volume du cluster A.

4. Dans l'interface Web du NAS Manager, restaurez la configuration système du NAS depuis le cluster A.

Pour en savoir plus sur la restauration de la configuration système du NAS, voir [Restoring Cluster Configuration](#) (Restauration de la configuration du cluster).

Ceci restaure la configuration du cluster B avec les paramètres du cluster A. Les configurations système de cluster suivantes peuvent actuellement être restaurées :


- Configuration des protocoles
- Utilisateurs et groupes
- Adressages utilisateurs
- Configuration de la surveillance
- Configuration horaire
- Hôtes antivirus

5. Assurez-vous que le cluster B est utilisé pour répondre aux requêtes des clients pendant le basculement.

Les administrateurs doivent effectuer les étapes suivantes pour définir le nom DNS et l'authentification :


- a) Dirigez les noms DNS du serveur DNS au cluster B au lieu du cluster A.

Assurez-vous que le serveur DNS du cluster B est identique au serveur DNS du cluster A (ou se trouve dans la même batterie DNS que le serveur DNS du cluster A). Les connexions client existantes peuvent céder et il est possible que vous deviez les rétablir. Vous devez démonter et remonter les exportations NFS sur le client.

 **REMARQUE** : Effectuez les étapes b, c et d uniquement pour les basculements de volume unique.

- b) Sur DNS, mettez à jour manuellement l'entrée DNS du volume NAS basculée.


Cette étape sert à repointer les utilisateurs finaux qui accèdent à ce volume du cluster A au cluster B, alors que les utilisateurs finaux continuent à y accéder à l'aide du même nom DNS.

 **REMARQUE** : Les systèmes client devront peut-être actualiser le cache DNS.

- c) Pour forcer les clients CIFS et NFS au cluster B, supprimez les partages CIFS et exportations NFS du cluster A.

Ceci force la reconnexion des clients CIFS et NFS et les connecte au cluster B. Suite à la restauration de la configuration du volume source sur le cluster B, tous les partages et exportations sont présents sur le volume de destination (du cluster B) : ainsi, aucune information de configuration de partage/d'exportation n'est perdue.

- d) Vous pouvez désormais accéder au volume basculé à l'aide des mêmes nom DNS et nom de partage que lorsque le volume était hébergé par le cluster A, sauf qu'il est maintenant hébergé par le cluster B.

 **REMARQUE** : Les montages NFS doivent être démontés puis montés à nouveau. Les transferts CIFS actifs échouent au cours de ce processus, mais si les partages CIFS sont adressés en tant que lecteurs locaux, ils sont reconnectés automatiquement une fois la réplication supprimée, le DNS mis à jour et les partages NFS/CIFS supprimés du cluster A.

- e) Joignez le serveur AD ou LDAP/NIS.


Assurez-vous que AD et LDAP se trouvent dans la même batterie AD/LDAP ou dans le même serveur.

### Phase 3 : restauration du cluster A par restauration automatique depuis le cluster B

1. Corrigez les problèmes ayant entraîné l'échec du cluster A (remplacez le matériel, disque, etc.), et réinstallez FluidFS (le cas échéant).
2. Reconstituez le cluster (utilisez les paramètres du cluster A précédemment enregistrés), formatez la réserve NAS et configurez le réseau (client, SAN et IC) comme auparavant.
3. Connectez-vous au cluster B et configurez le partenariat de réplication entre le cluster A et le cluster B.  
Pour en savoir plus sur la configuration des partenaires de réplication, voir [Configuration d'un partenaire de réplication](#).

4. Créez une stratégie de réplication pour tous les volumes sources dans le cluster B sur les volumes cibles du cluster A.

Pour en savoir plus sur la création de stratégies de réplication, voir [Ajout d'une stratégie de réplication](#).


 **REMARQUE** : La stratégie de réplication est basée sur les volumes avec une correspondance un à un, par exemple :

Volume source B1 (cluster B) au volume cible A1 (cluster A)

Volume source B2 (cluster B) au volume cible A2 (cluster A)

.....

Volume source B*n* (cluster B) au volume cible A*n* (cluster A)

 **REMARQUE** : FluidFS v2 prend en charge la génération automatique de volumes cible pendant l'ajout de la stratégie de réplication. Pour FluidFS 1.0, vous devez créer les volumes cible dans le cluster B et vous assurer que le volume est assez grand pour supporter les données correspondantes du volume source du cluster A.

5. Dans l'interface Web du NAS Manager, sélectionnez **Data Protection (Protection des données) → Replication (Réplication) → NAS Replication (Réplication NAS)** et cliquez sur **Replicate Now (Répliquer maintenant)** pour tous les volumes du cluster B (B1, B2, .., B*n*).

Si la réplication échoue, corrigez les problèmes rencontrés et relancez le processus de réplication. Assurez-vous que la réplication de tous les volumes sur le cluster A est réussie.

6. Supprimez la stratégie de réplication de tous les volumes (B1, B2, .. B*n*) et appliquez la configuration du volume source du cluster B au cluster A.

Répétez cette procédure pour supprimer toutes les stratégies de réplication et transformer les volumes cibles du cluster A en volumes autonomes.


- Lors de la suppression de la stratégie de réplication du cluster B de destination : le gestionnaire de réplication FluidFS tente de contacter le cluster A source, qui échoue. La configuration du cluster B de destination doit être restaurée à l'aide de **Cluster Management → Restore NAS Volume Configuration. (Gestion de cluster > Restaurer la configuration de volumes NAS)**
- Lors de la suppression de la stratégie de réplication du cluster A source : vous avez l'option d'appliquer la configuration du volume source au volume de destination. Si vous ne sélectionnez pas cette option ou si l'option échoue, vous pouvez restaurer la configuration du volume source du cluster A sur le volume de destination du cluster B à l'aide de **Cluster Management → Restore NAS Volume Configuration. (Gestion de cluster > Restaurer la configuration de volumes NAS)**

7. Connectez-vous au cluster A.

8. Dans l'interface Web du NAS Manager, restaurez la configuration système du NAS depuis le cluster B.

Pour en savoir plus sur la restauration de la configuration système du NAS, voir [Restauration de la configuration du cluster](#).

Ceci modifie les paramètres de configuration globale du cluster A, tels que le paramétrage des protocoles, horaire, de l'authentification etc, et les fait correspondre aux paramètres du cluster B.

 **REMARQUE** : Si la restauration de la configuration système échoue, redéfinissez-la avec les paramètres d'origine (utilisez les paramètres du cluster A que vous avez précédemment enregistrés).


Le cluster A est restauré avec ses paramètres d'origine.



9. Commencer à utiliser le cluster A pour répondre aux demandes des clients.

Les administrateurs doivent effectuer les étapes suivantes pour définir le nom DNS et l'authentification :


- a) Dirigez les noms DNS du serveur DNS du client vers le cluster A au lieu du cluster B.

Assurez-vous que le cluster A se trouve dans le même serveur DNS que le cluster B (ou dans la même batterie DNS que le serveur DNS du cluster B). Les connexions client existantes peuvent céder et il est possible que vous deviez les rétablir au cours de ce processus.

 **REMARQUE** : Effectuez les étapes b, c et d uniquement pour les basculements de volume unique.

- b) Sur DNS, mettez à jour manuellement l'entrée DNS du volume NAS basculée.  
Cette étape repointe les utilisateurs finaux qui accèdent à ce volume du cluster B au cluster A, alors que les utilisateurs finaux continuent à y accéder à l'aide du même nom DNS.
-  **REMARQUE :** Les systèmes client devront peut-être actualiser le cache DNS.
- c) Pour forcer les clients CIFS et NFS au cluster A, supprimez les partages CIFS et exportations NFS du cluster B.  
Ceci force la reconnexion des clients CIFS et NFS et les connecte au cluster A. Suite à la restauration de la configuration du volume source sur le cluster A, tous les partages et exportations sont présents sur le volume de destination (du cluster A) : ainsi, aucune information de configuration de partage/d'exportation n'est perdue.
- d) Vous pouvez désormais accéder au volume basculé à l'aide du même nom DNS et nom de partage que lorsque le volume était hébergé par le cluster B, sauf qu'il est maintenant hébergé par le cluster A.
-  **REMARQUE :** Les montages NFS doivent être démontés puis montés à nouveau. Les transferts CIFS actifs échouent au cours de ce processus, mais si les partages CIFS sont adressés en tant que lecteurs locaux, ils sont reconnectés automatiquement une fois la réplication supprimée, le DNS mis à jour et les partages NFS/CIFS supprimés du cluster B.
- e) Joignez le serveur AD ou LDAP/NIS.  
Assurez-vous que AD et LDAP se trouvent dans la même batterie AD/LDAP ou dans le même serveur.
10. Construisez la structure de réplication entre le cluster source A et le cluster de sauvegarde B pour configurer la stratégie de réplication entre le cluster A et le cluster B, utiliser les volumes du cluster B en tant que volumes cibles de réplication et vous préparer à la prochaine restauration après sinistre.

## Sauvegarde et restauration de données

 **REMARQUE :** Nous vous recommandons d'effectuer une sauvegarde de vos données à intervalles réguliers.

La solution en cluster NAS prend en charge la sauvegarde et la restauration des données à l'aide du protocole NDMP - Network Data Management Protocol - Protocole de gestion des données réseau). Un agent NDMP installé sur la solution en cluster NAS assure que les données stockées peuvent être sauvegardées et restaurées à l'aide d'une application standard de gestion des données (DMA) qui prend en charge le protocole NDMP, sans besoin d'installer des agents spécifiques de fournisseurs sur l'appliance NAS.

Pour effectuer des opérations de sauvegarde et de restauration, une DMA doit être configurée pour pouvoir accéder à l'appliance NAS à l'aide du réseau LAN ou client. La solution en cluster NAS n'utilise pas d'adresse dédiée pour les opérations de sauvegarde. Toute adresse de réseau LAN ou client peut être utilisée pour des opérations de sauvegarde ou de restauration.

Les sauvegardes NDMP sur la solution en cluster NAS sont effectuées à l'aide du réseau LAN ou client. La DMA doit être configurée de manière à pouvoir accéder aux adresses IP virtuelles de client (ou un nom DNS) de la solution en cluster NAS.


La solution en cluster NAS ne prend pas en charge d'adresse IP de sauvegarde dédiée sur le réseau LAN ou client. Toutes les adresses IP virtuelles configurées sur le réseau LAN ou client peuvent être utilisées par le logiciel de sauvegarde pour effectuer des sauvegardes et des restaurations.

La solution en cluster NAS fournit une interface utilisateur générique afin d'activer l'agent NDMP et est programmée pour travailler indépendamment de l'agent NDMP installé.

## Sauvegarde des volumes NAS cible de réplication

Lors de la réalisation d'une sauvegarde de volumes cible de réplication, FluidFS ne crée aucun instantané NDMP dédié. FluidFS utilise à la place l'instantané de la réplique de base de la dernière réplication réussie.

Si les planifications de réplication et de sauvegarde NDMP se chevauchent, une nouvelle opération de réplication peut s'effectuer et se terminer avant la fin du processus de sauvegarde NDMP des volumes cible. Dans ce cas, l'opération de réplication supprime l'instantané de la réplique de base précédent et crée une nouvelle réplique de base.

 **PRÉCAUTION** : Ceci met fin à la sauvegarde NDMP. Pour éviter ce scénario, planifiez vos opérations de réplication et de sauvegarde de manière à ce que la réplication se termine avant que la sauvegarde ne démarre.

## Éléments à considérer pour la conception NDMP

- Utilisez le nom DNS pour le serveur NDMP lors de la définition de sauvegarde dans le DMA afin que l'équilibrage de charge soit utilisé.
- Limitez le nombre de tâches de sauvegarde simultanées à une par contrôleur pour effectuer plus rapidement le transfert de données.
- Votre solution prend uniquement en charge une sauvegarde à trois voies, dans laquelle le serveur DMA négocie le transfert de données entre l'appliance NAS et le périphérique de stockage. Assurez-vous que le serveur DMA dispose d'une bande passante suffisante.


## Applications prises en charge

La solution en cluster NAS est certifiée pour fonctionner avec les applications DMA suivantes :

- Symantec BackupExec 2010 R3 et Symantec BackupExec 2012
- Symantec NetBackup 7.0 ou version ultérieure
- CommVault Simpana 9.0 ou version ultérieure
- IBM Tivoli 6.3

## Activation de la prise en charge NDMP


Les sauvegardes NDMP sont effectuées à l'aide du réseau client. L'application DMA doit être configurée de manière à accéder à une des adresses IP virtuelles (VIP) client (ou à un nom DNS) du cluster NAS.


 **REMARQUE** : Avant d'activer la prise en charge NDMP, vous devez configurer une VIP client sur le système. Vérifiez que la VIP client est bien configurée en sélectionnant **System Management** → **Network** → **Subnets** (Gestion système > Réseau > Sous-réseaux) et en vérifiant si le sous-réseau **Primary** (Principal) est défini.

Pour activer la prise en charge NDMP :

1. Sélectionnez **Data Protection (Protection des données)** → **NDMP** → **NDMP Configuration (Configuration NDMP)**. La page **NDMP Configuration (Configuration NDMP)** s'affiche.

2. Sélectionnez **Enable NDMP (Activer NDMP)**.

 **REMARQUE** : Le mot de passe **backup\_user** n'est pas défini au départ. Définissez le mot de passe une fois le nom d'utilisateur modifié, ou si vous utilisez le nom d'utilisateur par défaut.

 **REMARQUE** : Par défaut, le port NDMP client est 10000.

3. Sous **DMA server (Serveur DMA)**, saisissez l'adresse IP d'un serveur DMA autorisé.

 **REMARQUE** : Les noms DNS ne sont pas pris en charge.

4. Cliquez sur **Enregistrer les changements**.

## Modification du mot de passe et du nom d'utilisateur de secours NDMP

Un nom d'utilisateur et mot de passe sont requis lors de la configuration d'un serveur NDMP dans la DMA. Le nom d'utilisateur par défaut est **backup\_user**. Le mot de passe par défaut est généré de manière aléatoire et doit être changé avant d'utiliser NDMP.

Pour modifier le mot de passe NDMP :


1. Sélectionnez **Data Protection (Protection des données)** → **NDMP** → **NDMP Configuration (Configuration NDMP)**. La page **NDMP Configuration (Configuration NDMP)** s'affiche.
2. Au besoin, sous **Backup username (Nom d'utilisateur de secours)**, modifiez le nom d'utilisateur de secours actuel et cliquez sur **Save Changes (Enregistrer les modifications)**.  
Le nom d'utilisateur de secours est modifié.
3. Cliquez sur **Change Backup User Password (Modifier le mot de passe utilisateur de secours)**.  
La fenêtre **Change Password (Modifier le mot de passe)** affiche le nom d'utilisateur de secours actuel.
4. Sous **admin password (mot de passe admin)**, saisissez le mot de passe administrateur existant.
5. Sous le nom d'utilisateur de sauvegarde, dans **New password (Nouveau mot de passe)**, saisissez le nouveau mot de passe.
6. Sous **Retype password (Saisir le mot de passe à nouveau)**, saisissez le même mot de passe que vous venez de saisir dans **New password**.
7. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Modification de la Liste des serveurs DMA

Afin de prendre une sauvegarde NDMP de la solution en cluster NAS, le serveur de l'Application de sauvegarde doit être inclus dans la liste blanche des serveurs DMA.

### Ajout de serveurs DMA


Pour ajouter un serveur DMA à la liste :

1. Sélectionnez **Data Protection (Protection des données)** → **NDMP** → **NDMP Configuration (Configuration NDMP)**. La page **NDMP Configuration (Configuration NDMP)** s'affiche.
2. Si aucun champ vide **DMA server (serveur DMA)** n'est disponible, cliquez sur **Add DMA server (Ajouter un serveur DMA)**.  
Un champ **DMA server** supplémentaire est alors ajouté.
3. Dans le champ vide **DMA server**, saisissez l'adresse IP du serveur DMA.  
 **REMARQUE** : Les noms DNS ne sont pas pris en charge.
4. Cliquez sur **Save Changes (Enregistrer les changements)**.

### Suppression de serveurs DMA

Pour supprimer un serveur DMA de la liste :

1. Sélectionnez **Data Protection (Protection des données)** → **NDMP** → **NDMP Configuration (Configuration NDMP)**. La page **NDMP Configuration (Configuration NDMP)** s'affiche.
2. Sélectionnez le serveur DMA approprié, puis cliquez sur **Remove DMA Server (Supprimer le serveur DMA)**.

 **REMARQUE** : La suppression du serveur DMA de la liste blanche n'interrompt pas l'opération de sauvegarde/restauration déjà en cours vers/depuis ce serveur DMA.

## Spécification du volume NAS pour la sauvegarde

La plupart des applications de sauvegarde répertorient automatiquement les volumes disponibles pour la sauvegarde. Dans Symantec NetBackup 7.0, vous pouvez saisir le chemin de volume manuellement.

La solution en cluster NAS présente les volumes de sauvegarde au chemin suivant :

`/<NomduvolumeNAS>`

où `<NomduvolumeNAS>` est le nom exact du volume tel qu'il apparaît dans l'interface utilisateur.

## Affichage des tâches NDMP actives

Toutes les opérations de sauvegarde ou de restauration en cours de traitement par la solution en cluster NAS peuvent être affichées sur la page **NDMP Active Jobs** (Tâches actives NDMP). Pour afficher les tâches NDMP actives, sélectionnez **Data Protection** → **NDMP** → **NDMP Active Jobs** (Protection de données > NDMP > Tâches actives NDMP) ou **Monitor** → **NDMP Active Jobs. (Surveillance > Tâches actives NDMP)**

### Annulation d'une tâche NDMP active

Vous pouvez annuler une tâche NDMP active. Pour ce faire, procédez comme suit :

1. Sélectionnez **Data Protection (Protection des données)** → **NDMP** → **NDMP Active Jobs (Tâches NDMP actives)**.  
La page **NDMP Active Jobs** affiche toutes les tâches NDMP actives.
2. Sélectionnez la session à annuler.
3. Cliquez sur **Kill Active NDMP Job (Arrêter la tâche NDMP active)**.

 **REMARQUE** : Plusieurs sessions peuvent être sélectionnées en même temps.

## Utilisation des applications antivirus

La solution en cluster NAS contient une intégration avec logiciel antivirus ICAP standard pour assurer que les fichiers écrits depuis les clients CIFS ne contiennent pas de virus. L'hôte antivirus doit exécuter Symantec ScanEngine 5.2 ou Symantic Protection Engine for Cloud Services 7.0, lesquels sont des logiciels ICAP.

## Affichage des hôtes antivirus existants

Pour afficher les hôtes antivirus définis pour le système, sélectionnez **Data Protection** → **Antivirus** → **Antivirus Hosts** (Protection des données > Antivirus > Hôtes antivirus). La page **Antivirus Hosts** affiche les détails des hôtes antivirus déjà définis, leur adresse IP (ou nom) et le port ICAP associé.

## Ajout d'hôtes antivirus

Il est recommandé de définir plusieurs hôtes antivirus pour un balayage antivirus hautement disponible et pour réduire les latences lors d'accès aux fichiers. Si aucun hôte antivirus n'est disponible, l'accès aux fichiers peut être refusé, résultant en une perte de service.

Pour activer l'option Antivirus :

1. Sélectionnez **Data Protection (Protection des données)** → **Antivirus** → **Antivirus Hosts (Hôtes antivirus)**.

La page **Antivirus Hosts (Hôtes antivirus)** affiche une liste des hôtes antivirus existants.

2. Si aucun champ vide **Antivirus host** n'est disponible, cliquez sur **Add (Ajouter)**.  
Un champ **Antivirus host** est ajouté.
3. Dans le champ vide **Antivirus host**, saisissez l'adresse IP (ou le nom) de l'hôte antivirus.
4. Dans le champ **Port**, entrez le port sur lequel le protocole ICAP hôte est à l'écoute.  
Par défaut, le port ICAP est 1344.
5. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Retrait d'un hôte antivirus

Pour supprimer un hôte de la liste des hôtes antivirus :

1. Sélectionnez **Data Protection (Protection des données)** → **Antivirus** → **Antivirus Hosts (Hôtes antivirus)**.  
La page **Antivirus Hosts (Hôtes antivirus)** affiche une liste des hôtes antivirus existants.
2. Dans la liste des hôtes antivirus disponibles, sélectionnez l'hôte antivirus approprié et cliquez sur **Delete (Supprimer)**.

## Activation de la prise en charge antivirus par partage CIFS

La prise en charge antivirus est disponible sur une base par partage CIFS.

Pour activer la prise en charge antivirus des partages CIFS :

1. Cliquez sur **User Access (Accès utilisateur)** → **Shares (Partages)** → **CIFS Shares (Partages CIFS)**.
2. Cliquez sur le partage CIFS pour lequel vous souhaitez activer la prise en charge antivirus.
3. Cochez la case **Files should be checked for viruses (Les fichiers doivent être vérifiés pour les virus)** au bas de la page.
4. Cliquez sur le lien **Antivirus** qui apparaît en haut de la page à côté de **General (Généralités)** et **Advanced (Avancé)**.
5. Configurez le comportement de gestion des fichiers infectés par un virus (facultatif).
6. Configurez les fichiers à vérifier pour les virus (facultatif).
7. Configurez la liste d'exclusion (facultatif).
8. Cliquez sur **Enregistrer les changements**.



# Gestion de la solution NAS FluidFS

L'onglet **Cluster Management (Gestion des clusters)** vous permet d'afficher et définir les informations système générales, configurer le système de fichiers et les paramètres réseau, définir les protocoles requis, et configurer les paramètres d'authentification.

Pour accéder aux options de l'onglet **Cluster Management**, lancez le NAS Manager et cliquez sur l'onglet **Cluster Management**. La page **General Information (Informations générales)** s'affiche.

## Gestion du système

Vous pouvez réaliser les opérations de gestion sur le cluster à l'aide du NAS Manager.

Une adresse IP virtuelle de gestion NAS est requise pour accéder au NAS Manager. Cette adresse vous permet de gérer le cluster en tant qu'entité unique.

Des adresses IP supplémentaires sont requises pour les contrôleurs individuels dans le système et pour le système. Les clients ne doivent pas accéder à ces adresses directement.

## Gestion de l'accès des clients

La page **Subnets (Sous-réseaux)** vous permet de définir une ou plusieurs adresses IP virtuelles par lesquelles les clients accèdent aux partages et exportations du système. Si votre réseau est routé, il est recommandé de définir plus d'une adresse IP virtuelle.

Vous pouvez définir plusieurs sous-réseaux pour permettre aux clients d'accéder directement à la solution en cluster NAS sans avoir à passer par un routeur. Configurez un nom unique sur les serveurs DNS de chaque sous-réseau pour permettre l'équilibrage de charge entre ces adresses IP.



**REMARQUE** : Toutes les adresses IP virtuelles doivent être valides sur les réseaux alloués par l'administrateur système du site.

La page **Subnets** vous permet également de mettre à jour les plages d'adresses IP utilisées en interne par le système, à des fins de gestion et d'interconnexion.

Vous pouvez afficher la configuration actuelle des sous-réseaux du système, ajouter de nouvelles informations de sous-réseau et supprimer ou modifier les sous-réseaux existants. Configurez un nom unique sur les serveurs DNS de chaque sous-réseau pour permettre l'équilibrage de charge entre ces adresses IP.

## Affichage des sous-réseaux définis

Pour afficher les sous-réseaux définis, sélectionnez **Cluster Management (Gestion des clusters)** → **Network (Réseau)** → **Subnets (Sous-réseaux)**. La page **Subnets** affiche la liste des sous-réseaux existants.

## Ajout d'un sous-réseau


1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Network (Réseau)** → **Subnets (Sous-réseaux)**.

La page **Subnets (Sous-réseaux)** affiche la liste des sous-réseaux existants.


2. Cliquez sur **Ajouter**.

La fenêtre **Add/Edit Subnet (Ajouter/Modifier un sous-réseau)** s'affiche.


3. Sous **Subnet name (Nom du sous-réseau)**, saisissez un nom pertinent pour le réseau.
4. Dans la liste **Physical network (Réseau physique)**, sélectionnez le réseau pertinent.
5. Sous **Subnet mask (Masque de sous-réseau)**, saisissez l'adresse du masque de sous-réseau.
6. Indiquez l'ID VLAN du sous-réseau, le cas échéant.


 **REMARQUE** : Lorsqu'un VLAN s'étend sur plusieurs commutateurs, l'**ID VLAN** est utilisé pour déterminer les ports et interfaces auxquels envoyer les packets.

7. Sous **Management console VIP (Adresse IP virtuelle de la console de gestion)**, saisissez l'adresse IP de la console de gestion du système.
8. Sous **Private IP (Adresse IP privée)**, saisissez les adresses IP des contrôleurs système individuels pour chaque contrôleur.

 **REMARQUE** : Le support technique utilise ces adresses IP pour la gestion des contrôleurs.


9. Sous **VIP address (Adresse IP virtuelle)**, saisissez les adresses IP virtuelles d'un ou plusieurs clients.


 **REMARQUE** : Ces adresses servent à accéder aux fichiers sur le système.

 **REMARQUE** : Le nombre optimal d'adresses IP virtuelles (VIP) dépend de votre configuration réseau. Des informations supplémentaires sont disponibles dans l'aide en ligne.

10. Cliquez sur **Enregistrer les changements**.

## Modification d'un sous-réseau

 **REMARQUE** : Vous ne pouvez pas renommer le sous-réseau principal, ou tout sous-réseau interne (Interconnect et de gestion). Si vous avez besoin de mettre à jour les adresses IP d'un sous-réseau interne, vous devez arrêter le système de fichiers avant de modifier les adresses IP souhaitées.

 **REMARQUE** : Suite au déploiement initial, ne modifiez pas les sous-réseaux Interconnect (interconnexion) et Management (Gestion). La façon dont ces sous-réseaux sont configurés au cours du déploiement initial est essentielle à une fonctionnalité optimale.

1. Select **Cluster Management** → **Network** → **Subnets**.


La page **Subnets (Sous-réseaux)** affiche la liste des sous-réseaux existants.

2. Cliquez sur le sous-réseau approprié dans la colonne **Subnet Name** (Nom de sous-réseau) de la liste des sous-réseaux.

La page **Add/Edit Subnet (Ajouter/Éditer le sous-réseau)** du sous-réseau sélectionné s'affiche.

3. Modifiez les paramètres au besoin.
4. Cliquez sur **Enregistrer les changements**.

## Suppression d'un sous-réseau

 **REMARQUE** : Vous ne pouvez pas supprimer le sous-réseau principal ni tout sous-réseau interne (Interconnexion et Gestion).

1. Select **Cluster Management** → **Network** → **Subnets**.

La page **Subnets (Sous-réseaux)** affiche la liste des sous-réseaux existants.

2. Dans la liste des sous-réseaux affichés, sélectionnez le sous-réseau approprié, puis cliquez sur **Delete** (Supprimer).

# Gestion des utilisateurs administrateurs

Les administrateurs peuvent gérer le Dell Fluid File System à l'aide de la CLI ou de l'interface Web de ce dernier.

## Affichage des utilisateurs administrateurs

Pour afficher des utilisateurs administrateurs, sélectionnez **Cluster Management** → **General** → **Administrators** (Gestion des clusters > Généralités > Administrateurs). La page **Administrators** affiche la liste des administrateurs actuellement définis.

## Ajout d'un administrateur

Lors de la définition d'un administrateur, vous indiquez également son niveau d'autorisation. Les niveaux d'autorisation sont prédéfinis dans le système.

Les niveaux d'autorisation définis sont les suivants :

- Administrateur
- Afficher uniquement

Le niveau d'autorisation définit l'ensemble d'actions que l'utilisateur peut réaliser à ce niveau.

Pour ajouter un administrateur :


1. Dans le NAS Manager, sélectionnez **Cluster Management (Gestion des clusters)** → **General (Général)** → **Administrators (Administrateurs)**.

La page **Administrators (Administrateurs)** s'affiche.

2. Cliquez sur **Ajouter**.


La page **Add Administrator (Ajouter un administrateur)** s'affiche. L'onglet **Properties (Propriétés)** s'affiche.

3. Sous **User name (Nom d'utilisateur)**, saisissez un nom pour l'administrateur.
4. Sous **Password (Mot de passe)**, saisissez un mot de passe composé d'au moins six caractères.
5. Sous **Retype password (Saisir le mot de passe à nouveau)**, saisissez le même mot de passe que vous venez de saisir dans le champ Password.

 **REMARQUE** : Si le mot de passe est trop simple, vous serez invité à en saisir un autre plus complexe.

6. Sous **User ID (ID utilisateur)**, saisissez un identifiant utilisateur ou utilisez l'ID utilisateur par défaut fourni par le système.


7. Dans la liste **Level (Niveau)**, sélectionnez le niveau d'autorisation de l'administrateur. Vous pouvez sélectionner **3-Administrator** (3 : administrateur) ou **4-View only** (4 : affichage uniquement).

 **REMARQUE** : Vous ne pouvez définir que des administrateurs dont le niveau d'autorisation est hiérarchiquement inférieur au vôtre.

8. Sous **E-mail address (Adresse e-mail)**, saisissez l'adresse e-mail de l'administrateur dans tous les champs d'**adresse e-mail** disponibles.

Le système utilise cette adresse pour envoyer des alertes à l'administrateur. Vous pouvez ajouter des adresses e-mail supplémentaires en cliquant sur **Add Email address** (Ajouter une adresse e-mail). Vous pouvez définir le type d'alerte à envoyer par e-mail à l'administrateur dans l'onglet **Filters (Filtres)**.

9. Cliquez sur l'onglet **Filters (Filtres)** pour définir des stratégies de filtre pour les interruptions SNMP.
10. Définissez la gravité minimale des interruptions qui seront envoyées pour différentes catégories d'interruption.

 **REMARQUE** : L'option par défaut est d'envoyer des interruptions **Major (majeures)** pour toutes les catégories.

11. Cliquez sur **Enregistrer les changements**.

## Modification d'un administrateur

1. Sélectionnez **Cluster Management (Gestion des clusters) → General (Général) → Administrators (Administrateurs)**.  
La page **Administrators** apparaît, affichant la liste des administrateurs actuellement définis.
2. Dans la liste des administrateurs disponibles, dans la colonne **User Name (Nom d'utilisateur)**, cliquez sur l'administrateur pertinent.  
La page **Edit Administrator (Modifier l'administrateur)** s'affiche. Par défaut, l'onglet **Properties (Propriétés)** est sélectionné.
3. Vous pouvez modifier le **niveau** et l'**adresse e-mail** de l'administrateur sélectionné.
4. Vous pouvez changer les stratégies de filtre pour les interruptions SNMP dans l'onglet **Filters (Filtres)**.
5. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Modification du mot de passe administrateur


 **PRÉCAUTION** : Si vous modifiez le mot de passe administrateur dans le système Dell Compellent FS8600, la connexion entre le Enterprise Manager et le cluster échoue. Pour la rétablir, cliquez sur **Reconnect to FluidFS Cluster (Reconnecter au cluster FluidFS)** dans Enterprise Manager après avoir modifié le mot de passe admin.

1. Sélectionnez **Cluster Management (Gestion des clusters) → General (Général) → Administrators (Administrateurs)**.  
La page **Administrators** apparaît, affichant la liste des administrateurs actuellement définis.
2. Dans la liste des administrateurs disponibles, dans la colonne **User Name (Nom d'utilisateur)**, cliquez sur l'administrateur pertinent.  
La page **Edit Administrator (Modifier l'administrateur)** s'affiche. Par défaut, l'onglet **Propriétés** est sélectionné.
3. Cliquez sur **Change Password (Modifier le mot de passe)**.  
La fenêtre **Change Password** s'affiche.
4. Sous **admin password (mot de passe administrateur)**, saisissez le mot de passe actuel de l'administrateur sélectionné.
5. Sous **admin**, dans **New password (Nouveau mot de passe)**, saisissez le nouveau mot de passe.
6. Sous **Retype password (Saisir le mot de passe à nouveau)**, saisissez le même mot de passe que vous venez de saisir dans le champ **New Password (Nouveau mot de passe)**.
7. Dans la fenêtre **Change Password (Modifier le mot de passe)**, cliquez sur **Save Changes (Enregistrer les modifications)**.  
La page **Edit Administrator (Modifier un administrateur)** apparaît.
8. Cliquez sur **Enregistrer les changements**.

## Suppression d'un administrateur

1. Sélectionnez **Cluster Management (Gestion des clusters) → General (Général) → Administrators (Administrateurs)**.  
La page **Administrators** apparaît, affichant la liste des administrateurs actuellement définis.
2. Dans la liste des administrateurs disponibles, sélectionnez l'administrateur pertinent, puis cliquez sur **Delete (Supprimer)**.

# Gestion des utilisateurs locaux dans le cadre de l'accès aux partages CIFS et NFS

 **REMARQUE** : Ignorez cette section si votre site est configuré avec une base de données NIS externe/LDAP.

Une fois configurés, les utilisateurs locaux peuvent accéder au cluster, même lorsqu'un NIS externe, LDAP ou Active Directory est introduit.

Pour les utilisateurs locaux, l'accès au système est déterminé par volumes, partages et exportations.

Pour autoriser la solution en cluster NAS à utiliser les définitions d'utilisateur local :

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **Identity Management Database (Base de données de gestion des identités)**.  
La page **Identity Management Database (Base de données de gestion des identités)** s'affiche.
2. Sélectionnez **Users are not defined in an external user database (Les utilisateurs ne sont pas définis dans une base de données d'utilisateurs externes)**.
3. Dans le cas des utilisateurs CIFS, sélectionnez **Cluster Management (Gestion des clusters)** → **Protocols (Protocoles)** → **CIFS Configuration (Configuration CIFS)**.  
La page **CIFS Protocol Configuration (Configuration de protocole CIFS)** s'affiche.
4. Sélectionnez le mode à utiliser pour authentifier l'identité de l'utilisateur. Vous pouvez sélectionner l'une des options suivantes :
  - **Authenticate users' identity via Active Directory and local users database (Authentifier l'identité des utilisateurs via Active Directory et une base de données d'utilisateurs locaux)**.
  - **Authenticate users' identity via local users database (Authentifier l'identité des utilisateurs via une base de données d'utilisateurs locaux)**.
5. Pour gérer la liste **Local Users (Utilisateurs locaux)**, sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication** → **Local Users (Utilisateurs locaux)**.


## Affichage des utilisateurs locaux

Pour consulter la liste des utilisateurs existants, sélectionnez **Cluster Management** → **Authentication** → **Local Users** (Gestion des clusters > Authentification > Utilisateurs locaux) . La page **Local User** (Utilisateur local) affiche la liste des utilisateurs existants.

## Ajout d'utilisateurs locaux


1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication** → **Local Users (Utilisateurs locaux)**.  
La page **Local Users (Utilisateurs locaux)** s'affiche.
2. Cliquez sur **Add (Ajouter)**.  
La page **Add User (Ajouter un utilisateur)** s'affiche. Par défaut, l'onglet **General (Général)** de la page **Add User** s'affiche.
3. Sous **User name (Nom d'utilisateur)**, saisissez le nom de l'utilisateur local.
4. Sous **Password (Mot de passe)**, saisissez le mot de passe (composé d'au moins 6 caractères) à attribuer à l'utilisateur local.
5. Sous **Retype password (Saisir à nouveau de mot de passe)**, saisissez le même mot de passe que vous avez précédemment saisi dans le champ **Password**.
6. Sous **User ID (ID utilisateur)**, saisissez un ID utilisateur UNIX unique ou utilisez l'ID par défaut fourni par le système.

7. Sous **Primary group (Groupe principal)**, effectuez l'une des actions suivantes :
  - Saisissez le nom du groupe principal de l'utilisateur local.
  - Cliquez sur le bouton **Browse (Parcourir)** pour parcourir la liste des groupes principaux.
  - Utilisez le groupe par défaut fourni par le système.
8. Sous **Additional groups (Groupes supplémentaires)**, saisissez le nom d'un autre groupe auquel l'utilisateur local appartient, ou cliquez sur le bouton **Browse (Parcourir)** pour parcourir la liste des groupes (facultatif).
 

 **REMARQUE** : Vous pouvez ajouter plus d'un groupe.
9. Sélectionnez l'onglet **Advanced (Avancé)** pour afficher des champs supplémentaires et en option.
10. Sous **Real name (Nom réel)**, saisissez le nom réel de l'utilisateur.
11. Sous **Remarks (Remarque)**, entrez des commentaires concernant l'utilisateur (facultatif).
12. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Modification des utilisateurs locaux

1. Sélectionnez **Cluster Management (Gestion des clusters) → Authentication (Authentification) → Local Users (Utilisateurs locaux)**.  
La page **Local User (Utilisateur local)** affiche une liste des utilisateurs locaux existants.
2. Dans la liste des utilisateurs existants, sous **User Name (Nom d'utilisateur)**, cliquez sur le **User Name** approprié.  
La page **Edit User (Modifier l'utilisateur)** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
 

 **REMARQUE** : Vous ne pouvez que modifier les informations de groupe correspondant à l'utilisateur sélectionné dans l'onglet **General (Général)**.
3. Sous **Primary group (Groupe principal)**, effectuez l'une des actions suivantes :
  - Saisissez le nom du groupe principal de l'utilisateur local
  - Cliquez sur le bouton **Browse (Parcourir)** pour parcourir la liste des groupes principaux.
  - Utilisez le groupe par défaut fourni par le système.
4. Sous **Additional groups (Groupes supplémentaires)**, saisissez le nom d'un autre groupe auquel l'utilisateur appartient ou cliquez sur le bouton **Browse (Parcourir)** pour parcourir la liste des groupes et en sélectionner un (facultatif).
5. Sélectionnez l'onglet **Advanced (Avancé)** pour afficher des champs supplémentaires et en option.
6. Sous **Real name (Nom réel)**, saisissez le nom réel de l'utilisateur.
7. Sous **Remarks (Remarque)**, entrez des commentaires concernant l'utilisateur (facultatif).
8. Cliquez sur **Save Changes (Enregistrer les modifications)**.

## Suppression d'utilisateurs locaux

1. Sélectionnez **Cluster Management (Gestion des clusters) → Authentication (Authentification) → Local Users (Utilisateurs locaux)**.  
La page **Local User (Utilisateur local)** affiche une liste des utilisateurs locaux existants.
2. Dans la liste des utilisateurs existants, sélectionnez le nom de l'utilisateur et cliquez sur **Delete (Supprimer)**.

## Modification du mot de passe

Vous pouvez modifier le mot de passe d'un utilisateur local dans la page **Edit User (Modifier un utilisateur)**.  
Pour modifier le mot de passe d'un utilisateur de stockage local :

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication** → **Local Users (Utilisateurs locaux)**.  
La page **Local User (Utilisateur local)** affiche une liste des utilisateurs locaux existants.
2. Dans la liste des utilisateurs existants, sous **User Name (Nom d'utilisateur)**, cliquez sur le nom d'utilisateur approprié.  
La page **Edit User (Modifier l'utilisateur)** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
3. Sous **admin password (mot de passe administrateur)**, saisissez le mot de passe actuel de l'administrateur sélectionné.
4. Sous **admin**, dans **New password (Nouveau mot de passe)**, saisissez le nouveau mot de passe.
5. Sous **Retype password (Saisir le mot de passe à nouveau)**, saisissez le même mot de passe que vous venez de saisir dans le champ **New Password (Nouveau mot de passe)**.
6. Dans la fenêtre **Change Password (Modifier le mot de passe)**, cliquez sur **Save Changes (Enregistrer les modifications)**.  
La page **Edit Administrator (Modifier un administrateur)** apparaît.
7. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Gestion des groupes locaux

Si votre site est configuré avec une base de données NIS externe, vous pouvez ignorer cette section.



Vous devez définir des groupes locaux uniquement, au cas où vous n'auriez que peu d'utilisateurs finals Linux/UNIX ayant besoin d'accéder à la solution en cluster NAS à l'aide du partage NFS, et uniquement si aucune base de données NIS n'existe.

Les groupes de la solution en cluster NAS aident à organiser et gérer les utilisateurs. Lors de la définition des utilisateurs, vous pouvez attribuer des utilisateurs de stockage locaux à un ou plusieurs groupes. La solution en cluster NAS peut également inclure des groupes ou des utilisateurs définis en externe, tels que des groupes définis dans un système UNIX.

### Affichage des groupes locaux

Pour afficher les **Local Groups** (Groupes locaux) existants, sélectionnez **Cluster Management** → **Authentication** → **Local Groups** (Gestion des clusters > Authentification > Groupes locaux). La page **Local Groups** affiche la liste des groupes locaux existants.

### Ajout d'un groupe local

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **Local Groups (Groupes locaux)**.  
La page **Local Groups** s'affiche.
2. Cliquez sur **Add (Ajouter)**.  
La page **Add Group (Ajouter un groupe)** s'affiche.
3. Sous **Group Name (Nom du groupe)**, saisissez le nom du groupe.
4. Sous **Group ID (ID du groupe)**, saisissez l'identifiant du groupe.  
 **REMARQUE** : Les groupes Dell Fluid File System possèdent des ID supérieurs à 200.  
 **REMARQUE** : Le prochain identifiant disponible est automatiquement attribué au groupe. Vous pouvez le modifier, si nécessaire.
5. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Suppression d'un groupe local

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **Local Groups (Groupes locaux)**.

La page **Local Groups (Groupes locaux)** affiche une liste des utilisateurs locaux existants.

2. Dans cette liste, sélectionnez le groupe local approprié, puis cliquez sur **Delete (Supprimer)**.

## Authentification

L'entrée Authentication (Authentification) permet l'authentification des autorités, telles que NIS (Network Information Services - Services d'informations réseau), Active Directory (AD) et du protocole LDAP (Light-weight Directory Access Protocol - Protocole d'accès au répertoire léger). En outre, vous pouvez gérer les utilisateurs et groupes locaux, et adresser les noms d'utilisateur depuis les SID Windows aux UID UNIX.

La solution en cluster NAS prend en charge les modes de configuration suivants :

- Mode mixte et mode natif d'authentification Active Directory
- Authentification NIS uniquement
- Authentification LDAP uniquement
- Utilisateurs internes locaux uniquement
- NIS ou LDAP et Active Directory

## Configuration d'une base de données de gestion des identités

Une **Identity Management Database (Base de données de gestion des identités)** permet au système d'authentifier et de gérer le contrôle d'accès utilisateur. Cette base de données est responsable de la gestion des utilisateurs, de leurs mots de passes, groupes, et des relations entre les utilisateurs et les groupes.

Si le système appartient à un domaine Active Directory, il joue également le rôle de base de données de gestion des identités. Vous pouvez définir des bases de données UNIX supplémentaires, au besoin.

Les bases de données de gestion des identités UNIX comprennent NIS et LDAP, et ne sont pertinentes que lorsque les clients accèdent au système à l'aide du protocole NFS (clients UNIX/Linux).

Vous pouvez choisir l'une des options suivantes, en fonction de votre environnement réseau :

- Activer l'authentification des utilisateurs via une base de données NIS
- Activer l'authentification des utilisateurs via une base de données LDAP
- Désactiver l'utilisation d'une base de données de gestion des identités UNIX externe

## Activation de l'authentification des utilisateurs via une base de données NIS

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication** → **Identity Management Database (Base de données de gestion des identités)**.

La page **Identity Management Database (Base de données de gestion des identités)** s'affiche.

2. Sélectionnez **Users and groups are defined in a NIS database (Les utilisateurs et les groupes sont définis dans une base de données NIS)**.
3. Sous **Domain name (Nom de domaine)**, saisissez le nom de domaine de la base de données NIS.
4. Dans n'importe lequel des champs **NIS server (Serveur NIS)** vides disponibles, saisissez le nom ou l'adresse IP du serveur NIS.
5. Pour ajouter un serveur NIS à des fins de redondance, cliquez sur **Add NIS server** (Ajouter un serveur NIS).

Un **NIS server (Serveur NIS)** supplémentaire s'affiche dans la liste des serveurs NIS.

6. Pour supprimer un serveur NIS de la liste, sélectionnez la case en regard du serveur NIS à supprimer, puis cliquez sur **Delete NIS server(s) (Supprimer le (les) serveur(s) NIS)**.
7. Cliquez sur **OK** lorsque vous êtes invité à accepter les modifications.
8. Cliquez sur **Enregistrer les changements**.

## Activation de l'authentification des utilisateurs via une base de données LDAP

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **Identity Management Database (Base de données de gestion des identités)**.  
La page **Identity Management Database (Base de données de gestion des identités)** s'affiche.
2. Sélectionnez **Users and groups are defined in an LDAP database (Les utilisateurs et les groupes sont définis dans une base de données LDAP)**.
3. Dans le champ **LDAP server (Serveur LDAP)**, saisissez le nom ou l'adresse IP du serveur LDAP.
4. Dans **Base DN (DN de base)**, saisissez le DN de base (nom distinct) que vous souhaitez utiliser à titre d'authentification.  
Le DN de base (nom distinct) est une chaîne LDAP unique représentant le domaine à utiliser pour l'authentification. Il est généralement au format suivant :  
dc=domain  
dc=com
5. Cliquez sur **Enregistrer les changements**.

## Désactivation de l'utilisation d'une base de données de gestion des identités UNIX externe

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **Identity Management Database (Base de données de gestion des identités)**.  
La page **Identity Management Database (Base de données de gestion des identités)** s'affiche.
2. Sélectionnez **Users are not defined in an external user database (Les utilisateurs ne sont pas définis dans une base de données d'utilisateurs externes)**.
3. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Active Directory




Le service Active Directory stocke des informations sur tous les objets du réseau de l'ordinateur et rend ces informations disponibles pour les administrateurs et utilisateurs afin que ces derniers puissent les trouver et les appliquer. Active Directory permet aux utilisateurs d'accéder aux ressources n'importe où sur le réseau à l'aide d'une ouverture de session unique.

De même, les administrateurs disposent ainsi d'un point d'administration unique pour tous les objets du réseau, qu'ils peuvent consulter hiérarchiquement. L'entrée Active Directory vous permet de configurer les paramètres Active Directory et de définir les options d'authentification utilisateur. En outre, vous pouvez joindre le domaine Active Directory.

# Synchronisation de la solution en cluster NAS avec le serveur Active Directory


Si votre site utilise Active Directory et que la solution en cluster NAS fait partie du réseau Windows, synchronisez l'horloge d'après l'horloge du serveur AD. Pour ce faire, sélectionnez **Cluster Management (Gestion des clusters)** → **General (Général)** → **Time Configuration (Configuration horaire)**.


## Configuration du service Active Directory

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Authentication (Authentification)** → **System Identity (Identité du système)**.  
La page **System Identity** s'affiche. Elle affiche la configuration actuelle et indique si oui ou non la solution en cluster NAS est jointe à un domaine Active Directory.
2. Sous **System name (Nom du système)**, saisissez le nom du système.  
Ce nom identifie le Dell Fluid File System dans les alertes envoyées par le système et correspond également au nom par défaut du Dell Fluid File System lorsque vous configurez Active Directory.
3. Sélectionnez **The system is a member of a Microsoft Windows Network (Le système est un membre du réseau Microsoft Windows)** si vous souhaitez joindre Dell Fluid File System à un domaine Active Directory, puis passez à l'étape suivante. Sinon, ne cochez pas la case à cocher en regard de ce champ, et cliquez sur **Save Changes (Enregistrer les modifications)**.
4. Sous **System NetBIOS name (Nom du NetBIOS du système)**, saisissez le nom du NetBIOS Dell Fluid File System affiché dans le voisinage réseau.  
Ce nom est limité à 15 caractères. Sauf indication contraire, utilisez le nom du système.
5. Sous **Domain (Domaine)**, indiquez le domaine auquel appartient Dell Fluid File System.  
Utilisez le FQDN (nom de domaine entièrement qualifié), et non le nom de domaine NetBIOS. Par exemple :  
mydomain.company.com
6. Sous **User name (Nom d'utilisateur)**, saisissez le nom d'utilisateur administrateur à utiliser pour joindre le domaine Active Directory.  
 **REMARQUE** : Ce nom d'utilisateur n'est pas enregistré dans le Dell Fluid File System.
7. Sous **Password (Mot de passe)**, saisissez le mot de passe administrateur.  
 **REMARQUE** : Ce mot de passe n'est pas enregistré dans le Dell Fluid File System.  
 **PRÉCAUTION** : Le champ **Advanced Configuration (Configuration avancée)** doit être désélectionné, sauf indication contraire par l'équipe de support Dell. Ce champ permet de configurer davantage de paramètres relatifs à Active Directory.  
À l'aide de l'option **Advanced Configuration (Configuration avancée)**, vous pouvez spécifier un contrôleur de domaine pour remplacer le contrôleur par défaut sélectionné par le système.
8. Cliquez sur **Enregistrer les changements**.

## Présentation de la configuration du réseau

Pour accéder au système, définissez une adresse IP à laquelle vos clients peuvent accéder. Il vous est recommandé d'ajouter cette adresse IP à votre serveur DNS pour que les clients puissent accéder au système à l'aide du même nom et d'une adresse IP.

 **REMARQUE** : Vous devez configurer CIFS pour authentifier les utilisateurs après avoir rejoint le domaine. Pour authentifier les utilisateurs, allez dans **Cluster Management** → **Protocols** → **CIFS Configuration**. (Gestion des clusters > Protocoles > Configuration CIFS). Sélectionnez **Authenticate users' identity using Active Directory and local user database** (Authentifier l'identité des utilisateurs à l'aide d'Active Directory et de la base de données des utilisateurs locaux).


 **REMARQUE** : L'adresse IP virtuelle d'accès aux clients est configurée lors de la configuration initiale à l'aide de l'utilitaire **Dell NAS Initial Deployment Utility** (Utilitaire de déploiement initial NAS Dell). Vous pouvez afficher l'adresse que vous avez configurée en allant sous NAS Manager (Gestionnaire NAS), **Cluster Management** → **Network** → **Subnets** (Gestion des clusters > Réseau > Sous-réseaux). Cliquez sur **Primary** (Principal) en bas de la page pour afficher l'adresse IP virtuelle d'accès aux clients étiquetée **VIP address** (adresse IP virtuelle).

Étant donné que l'architecture du système correspond à un cluster à deux contrôleurs ou plus, cette adresse IP est une adresse IP virtuelle (VIP) qui sert tous les contrôleurs du cluster. Cela permet aux clients d'accéder au système en tant qu'unité unique et permet au système d'effectuer un équilibrage de charge entre les contrôleurs. Cela permet également la continuité des services en cas d'échec d'un contrôleur. Les clients bénéficient donc de la haute disponibilité et des hautes performances du système.

Les utilisateurs client accèdent au système via différentes topologies réseau. Selon les capacités physiques de l'infrastructure réseau, la solution en cluster NAS :

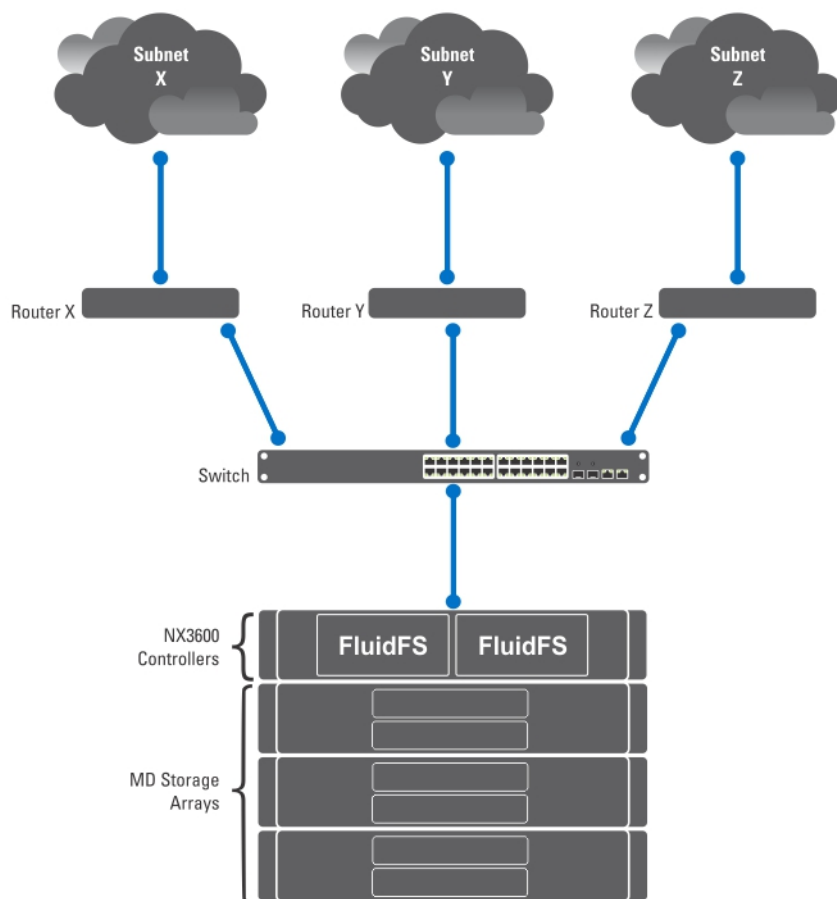
- Appartient à tous les sous-réseaux LAN ou client. Du point de vue des performances, il s'agit de la configuration la plus optimale. Dans de telles configurations réseau, il suffit de définir une adresse VIP pour chaque sous-réseau.
- N'appartient à aucun sous-réseau LAN ou client, auquel cas tous les clients sont considérés comme étant routés. Dans de telles situations, les clients accèdent aux données via un routeur ou des commutateurs en trois couches. Dans de telles configurations réseau, il est recommandé de définir plusieurs adresses IP virtuelles dans un sous-réseau unique et de fournir un mécanisme de sélection aux clients pour qu'ils puissent sélectionner une adresse IP de cette liste.
- Appartient à certains sous-réseaux LAN ou client, auquel cas certains clients sont plats tandis que d'autres sont routés. Dans de telles configurations réseau, il est recommandé d'utiliser les deux méthodes susmentionnées et d'indiquer aux utilisateurs les adresses IP virtuelles à utiliser, selon leur type : plat ou routé.

Il vous est recommandé de fournir une entrée dans le DNS pour tous les sous-réseaux auxquels le système appartient afin que les clients puissent accéder aux données sans avoir à garder en mémoire les adresses IP virtuelles. Si plusieurs adresses IP virtuelles existent dans le sous-réseau, définissez un nom unique dans le serveur DNS qui émet les adresses IP de cette liste. Effectuez cette définition en « tourniquet » afin que tous les clients puissent accéder au système.

 **REMARQUE** : Ne combinez jamais les adresses VIP de différents sous-réseaux dans un même nom DNS.

## Performances et voies statiques

Les réseaux routés vous permettent d'optimiser les performances via une fonction appelée « static routes » (voies statiques). Cette fonction vous permet de configurer les chemins exacts que votre système utilise pour communiquer avec différents clients sur un réseau routé.



**Figure 6. Configuration réseau**

Comme le réseau précédent l'illustre, le système ne peut disposer que d'une passerelle par défaut. Prétendons que vous sélectionniez *router X* (routeur X).

Les paquets qui sont envoyés aux clients en sous-réseau Y sont routés vers le routeur X, puis renvoyés (via le commutateur) au routeur Y. Ces paquets passent inutilement par le routeur X et réduisent le débit vers tous les sous-réseaux de votre réseau.

Pour remédier à ce problème, vous devez définir, en plus de la passerelle par défaut, une passerelle spécifique pour certaines voies statiques configurant des sous-réseaux. Pour ce faire, décrivez chaque sous-réseau dans votre réseau et identifiez la passerelle la mieux appropriée pour accéder à ce sous-réseau.

Il n'est pas nécessaire de le faire pour tout le réseau : une passerelle par défaut suffit largement lorsqu'aucun problème de performances n'existe. Vous pouvez sélectionner quand et où utiliser les voies statiques pour satisfaire au mieux aux besoins de votre système en termes de performances.

## Configuration du DNS

Le DNS (Domain Name System) est le service de résolution de noms qui permet aux utilisateurs de localiser des ordinateurs sur un réseau ou sur Internet (réseau TCP/IP) à l'aide du nom de domaine. Le serveur DNS maintient une base de données de noms de domaine (noms d'hôte) et de leurs adresses IP correspondantes, fournissant ainsi un service de résolution nom à adresse et adresse à nom sur le réseau IP. Vous pouvez configurer un ou plusieurs serveurs

DNS externes (externes à la solution en cluster NAS mais se trouvant dans le site) à utiliser pour les résolutions de noms.

## Affichage des serveurs DNS

Pour afficher la liste des serveurs DNS et de leurs paramètres, sélectionnez **Cluster Management** → **Network** → **DNS Configuration** (Gestion des clusters > Réseau > Configuration DNS). La page **DNS Configuration** affiche la liste des serveurs DNS et de leurs paramètres.

## Ajout de serveurs et suffixes DNS

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Network (Réseau)** → **DNS Configuration (Configuration DNS)**.  
La page **DNS Configuration (Configuration NDMP)** s'affiche.
2. Pour ajouter un serveur DNS, cliquez sur **Add DNS Server (Ajouter le serveur DNS)**.  
Une nouvelle ligne vide est ajoutée à la liste des serveurs DNS.
3. Configurez l'adresse IP du DNS principal de l'environnement client
4. Pour ajouter un suffixe DNS, cliquez sur **Add DNS Suffix (Ajouter le suffixe DNS)**.  
Une nouvelle ligne vide est ajoutée à la liste des suffixes DNS.
5. Saisissez les suffixes DNS dans l'ordre de précedence.
6. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Retrait de serveurs et suffixes DNS

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Network (Réseau)** → **DNS Configuration (Configuration DNS)**.  
La page **DNS Configuration** affiche la liste des serveurs DNS existants et de leurs paramètres.
2. Sélectionnez le serveur DNS approprié et/ou le suffixe DNS approprié, puis cliquez sur **Delete (Supprimer)**.  
Un message vous indique que le serveur DNS supprimé enregistre toutes les autres modifications effectuées.
3. Cliquez sur **OK**.

## Gestion des voies statiques

Pour minimiser les sauts d'un routeur à l'autre, des voies statiques sont suggérées dans les réseaux routés lorsque plusieurs chemins d'accès directs sont disponibles entre la solution en cluster NAS et différents routeurs.

## Affichage des voies statiques

Sélectionnez **Cluster Management** → **Network Management** → **Static Routes** (Gestion des clusters > Gestion du réseau > Voies statiques). La page **Static Routes** affiche la liste des voies statiques actuellement définies.

## Ajout de voies statiques

Lors de la définition d'une voie statique, vous devez indiquer les propriétés de sous-réseau et la passerelle par laquelle accéder à ce sous-réseau.

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Network Management (Gestion du réseau)** → **Static Routes (Voies statiques)**.  
La page **Static Routes** s'affiche.
2. Cliquez sur **Add (Ajouter)**.  
La page **Add Static Routes (Ajouter des voies statiques)** s'affiche.
3. Dans la liste **Network (Réseau)**, sélectionnez le réseau par lequel accéder au sous-réseau.
4. Sous **Gateway IP (Adresse IP de la passerelle)**, fournissez l'adresse IP de la passerelle permettant d'accéder au sous-réseau qui offre le meilleur accès au sous-réseau cible.
5. Sous **Destination Subnet (Sous-réseau cible)**, indiquez le sous-réseau cible auquel la voie statique permet d'accéder.
6. Sous **Netmask (Masque de réseau)**, fournissez le masque de réseau afin de différencier ce sous-réseau des autres sous-réseaux.
7. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Modification d'une voie statique

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Network Management (Gestion du réseau)** → **Static Routes (Voies statiques)**.  
La page **Static Routes** affiche la liste des voies statiques actuellement définies.
2. Dans la liste des voies statiques existantes, sélectionnez la voie statique appropriée, puis cliquez sur **Edit (Modifier)**.  
Les propriétés de la voie statique sélectionnée s'affichent.
3. Modifiez les propriétés au besoin.

## Suppression d'une voie statique

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Network Management (Gestion du réseau)** → **Static Routes (Voies statiques)**.  
La page **Static Routes** affiche la liste des voies statiques actuellement définies.
2. Dans la liste des voies statiques existantes, sélectionnez la voie statique appropriée, puis cliquez sur **Delete (Supprimer)**.

## Définition des protocoles de système de fichiers

Les protocoles de système de fichiers sont des protocoles de mise en réseau qui fournissent des services de partage système. La solution en cluster NAS agit en tant que serveur de système de fichiers en satisfaisant aux protocoles suivants :

- CIFS : le protocole Common Internet File System (Système de fichiers Internet commun) est destiné aux utilisateurs Microsoft Windows ou à d'autres clients CIFS. Le partage des répertoires s'effectue à l'aide des partages CIFS.
- NFS : le protocole Network File System (Système de fichiers réseau) est destiné aux clients ou services UNIX. Il fonctionne en tant que couche NFS. Le partage des répertoires s'effectue à l'aide des exportations NFS.

Les entrées de **Protocole** permettent de gérer les protocoles CIFS et NFS au niveau du système.

# Configuration des paramètres CIFS

La **CIFS Protocol Configuration (Configuration de protocole CIFS)** permet aux utilisateurs Windows de se connecter au système de la solution en clusters NAS. Vous pouvez également autoriser les utilisateurs Linux à accéder au système à l'aide du protocole CIFS et les authentifier via NIS, LDAP ou les utilisateurs locaux de la solution en cluster NAS.

Dans l'onglet **General** (Généralités), sélectionnez si vous souhaitez authentifier les utilisateurs à l'aide du domaine Active Directory ou la base de données d'utilisateurs internes. Vous pouvez également l'utiliser pour activer ou désactiver le protocole CIFS.

## Configuration des paramètres CIFS généraux

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Protocoles** → **CIFS Configuration (Configuration CIFS)**.  
La page **CIFS Protocol Configuration (Configuration du protocole CIFS)** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
2. Cochez la case **Allow clients to access files via the CIFS protocol (Autoriser les clients à accéder aux fichiers via le protocole CIFS)** pour activer le protocole de partage de fichiers CIFS.
3. Sous **System description (Description système)**, saisissez une brève description du serveur.  
Cette description s'affiche dans la barre de titre de Windows Explorer.
4. Sélectionnez une méthode d'authentification de l'identité des utilisateurs parmi les suivantes :
  - Pour authentifier les utilisateurs à l'aide du domaine Active Directory auquel le système est joint, sélectionnez **Authenticate users' identity via Active Directory and local user database (Authentifier l'identité des utilisateurs à l'aide d'Active Directory et de la base de données des utilisateurs locaux)**.
  - Pour authentifier les utilisateurs à l'aide d'une base de données d'utilisateurs internes, sélectionnez **Authenticate users' identity via local users database (Authentifier l'identité des utilisateurs à l'aide de la base de données des utilisateurs locaux)**.
5. Cliquez sur **Enregistrer les changements**.  
Cela redémarre toutes les connexions d'utilisateurs.

## Interdire aux utilisateurs d'accéder aux fichiers à l'aide du protocole CIFS

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Protocoles** → **CIFS Configuration (Configuration CIFS)**.  
La page **CIFS Protocol Configuration (Configuration du protocole CIFS)** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
2. Désélectionnez **Allow clients to access files via the CIFS protocol (Autoriser les clients à accéder aux fichiers via le protocole CIFS)**.
3. Cliquez sur **Save Changes (Enregistrer les changements)**.  
Cela redémarre toutes les connexions d'utilisateurs.


## Configuration des paramètres CIFS avancés

Dans l'onglet **Advanced** (Avancé), vous pouvez définir les paramètres suivants :

- Quels ensembles de caractères seront utilisés par les pages de codes DOS .
- Quel ensemble de caractères UTF-8 sera utilisé par la solution en cluster NAS.

Pour configurer les paramètres CIFS avancés :

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Protocoles** → **CIFS Configuration (Configuration CIFS)**.  
La page **CIFS Protocol Configuration (Configuration du protocole CIFS)** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
2. Cliquez sur l'onglet **Advanced (Avancé)**.
3. Dans la liste **DOS Code Page (Page de codes DOS)**, sélectionnez l'ensemble de caractères utilisé par les clients qui ne prennent pas en charge UNICODE.
4. Dans la liste **Unix Charset**, sélectionnez la version de l'ensemble de caractères UTF8 utilisé par le système. Ceci permet la conversion correcte des ensembles de caractères du client connecté.
5. Cliquez sur **Enregistrer les changements**.

 **REMARQUE** : Cela redémarre toutes les connexions d'utilisateurs.

## Configuration des paramètres horaires du système

Cette page vous permet de configurer l'horloge du système, déterminer comment mettre l'heure à jour automatiquement à l'aide d'un serveur NTP et configurer le fuseau horaire de votre système. La synchronisation de l'horloge est critique au bon fonctionnement du système.

Cela permet :

- Aux clients Windows de monter le système.
- Aux activités planifiées, telles que les instantanés et les tâches de réplication, de se dérouler à l'heure appropriée.
- D'enregistrer l'heure correcte dans le journal système.

### Changer de fuseau horaire


1. Sélectionnez **Cluster Management (Gestion des clusters)** → **General (Général)** → **Time Configuration (Configuration horaire)**.  
La page **Time Configuration (Configuration horaire)** s'affiche.
2. Dans la liste **Time zone (Fuseaux horaires)**, sélectionnez le fuseau horaire de la région dans laquelle se trouve le cluster.
3. Cliquez sur **Save Changes (Enregistrer les changements)**.

### Configuration manuelle de la date et de l'heure actuelles


Si votre environnement ne comprend pas de serveur de synchronisation de l'heure, configurez la date et l'heure manuellement.

Pour configurer manuellement la date et l'heure :

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **General (Général)** → **Time Configuration (Configuration des heures)**.  
La page **Time Configuration** s'affiche.
2. Sélectionnez **There is no NTP server to synchronize time with (Il n'y a pas de serveur NTP avec lequel synchroniser l'heure)**.
3. Sous **Date**, saisissez la date actuelle.

 **REMARQUE** : Utilisez le format suivant : JJ/MM/AAAA, où JJ indique le jour, MM indique le mois et AAAA indique l'année. Par exemple, *30/05/2012*.

4. Sous **Heure**, saisissez l'heure actuelle.

 **REMARQUE** : Utilisez le format suivant : HH:MM:SS, où HH indique un format 24 heures. Par exemple, *17:38:23*.

5. Cliquez sur **Enregistrer les changements**.

## Suppression d'un serveur NTP

Si un serveur NTP n'est plus présent sur le réseau LAN/client, supprimez le serveur NTP.

Pour supprimer un serveur NTP :

1. Cliquez sur **Cluster Management (Gestion des clusters) → General (Général) → Time Configuration (Configuration horaire)**.  
La page **Time Configuration** affiche une liste des serveurs NTP disponibles.
2. Sélectionnez le serveur NTP approprié, puis cliquez sur **Delete NTP server(s) (Supprimer le ou les serveur(s) NTP)**.
3. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Synchronisation de la solution en cluster NAS avec un serveur NTP local

Le protocole NTP (Network Time Protocol) aide à la synchronisation et la coordination de la répartition des heures. Le serveur NTP aide à la synchronisation des horloges sur le réseau.

Si le système ne fait pas partie d'un réseau Windows, configurez-le pour qu'il se synchronise avec un serveur NTP local (le cas échéant), ou avec un serveur NTP sur Internet. Cependant, si le système fait partie d'un réseau Windows, AD peut répondre en tant que serveur NTP.

Pour configurer la solution en cluster NAS pour qu'elle se synchronise avec un serveur NTP local ou un serveur NTP sur Internet :

1. Sélectionnez **Cluster Management (Gestion des clusters) → General (Général) → Time Configuration (Configuration des heures)**.  
La page **Time Configuration** s'affiche.
2. Sélectionnez **Time should be synchronized with an NTP server (L'heure doit être synchronisée avec un serveur NTP)**.
3. Sélectionnez **Serveur NTP (NTP serveur)**.
4. Sous **NTP server**, saisissez le nom du serveur NTP local ou du serveur NTP Internet.
5. Pour ajouter un serveur NTP redondant, cliquez sur **Add NTP server (Ajouter un serveur NTP)** et saisissez le nom du serveur NTP redondant dans le champ **NTP server (Serveur NTP)**.
6. Cliquez sur **Enregistrer les changements**.

## Gestion des licences

Les licences installées peuvent être visualisées et gérées depuis le logiciel NAS Management (Gestion NAS).

### Affichage des licences

Pour afficher les licences installées, sélectionnez **Cluster Management → General → Licensing** (Gestion des clusters > Généralités > Licences). La page **Licensed Features** (Fonctionnalités mises sous licence) affiche la liste des licences installées.

## Ajout d'une licence

Les fonctionnalités du fichier de licence s'affichent à l'écran suite à la réactualisation de l'écran et la validation par le système dudit fichier.

Pour ajouter une licence :

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **General (Général)** → **Licensing (Licences)**.  
La page **Licensed Features (Fonctionnalités mises sous licence)** s'affiche.
2. Sous **Upload the license XML file** (Téléverser le fichier XML de licence), saisissez le chemin de fichier XML de licence ou cliquez sur le bouton **Browse** (Parcourir) pour naviguer vers l'emplacement du fichier XML de licence.
3. Cliquez sur **Upload (Téléverser)** pour téléverser le fichier de licence.  
Les fonctionnalités du fichier de licence s'affichent à l'écran suite à la réactualisation de l'écran et la validation par le système dudit fichier.


## Suppression d'une licence

 **PRÉCAUTION** : La suppression de licence ne doit s'effectuer qu'avec l'aide du support technique Dell.

Les fonctionnalités du fichier de licence s'affichent à l'écran suite à la réactualisation de l'écran et la validation par le système dudit fichier.

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **General (Général)** → **Licensing (Licences)**.  
La page **Licensed Features (Fonctionnalités mises sous licence)** affiche une liste des licences installées.
2. Dans cette liste, sélectionnez la fonctionnalité appropriée, puis cliquez sur **Delete License for feature (Supprimer la licence de cette fonctionnalité)**.

## Configuration des paramètres d'e-mail sur des solutions NAS PowerVault NX3500/NX3600/NX3610

 **REMARQUE** : Cette fonctionnalité n'est pas prise en charge par les solutions NAS Dell Compellent FS8600. Dell Compellent FS8600 utilise Enterprise Manager pour les envois d'alertes par e-mail. Pour en savoir plus, voir le *Enterprise Manager Users Guide (Guide d'utilisation de Enterprise Manager)*.

Dell Fluid File System utilise les messages électroniques pour ses envois d'alertes et son assistance à distance. Vous pouvez déterminer qui a reçu un ou tous les types de messages suivants provenant de Dell Fluid File System :

- **Heartbeats (Pulsations)** : des messages de type « Heartbeats » sont envoyés toutes les 5 minutes à un destinataire e-mail. Cela permet à l'équipe de support de réagir rapidement en cas de défaillances du système.
- **System logs (Journaux système)** : les journaux système sont envoyés périodiquement au destinataire e-mail. Cela permet à l'équipe de support d'identifier les erreurs système bénignes et de les corriger, au besoin.
- **Alerts (Alertes)** : les messages d'alerte envoyés par e-mail qui fournissent des rapports sur le service système.

Vous pouvez ajouter des destinataires supplémentaires si vous le souhaitez. Si vous ajoutez l'administrateur en tant que destinataire, il est recommandé de configurer le système pour qu'il n'envoie que des alertes système.

Vous pouvez effectuer une demande manuelle pour que le système envoie un rapport d'informations, au besoin.

## Affichage des serveurs SMTP

Pour afficher la liste des serveurs SMTP configurés, sélectionnez **Cluster Management** → **Monitoring Configuration** → **Email Configuration** (Gestion des clusters > Configuration de la surveillance > Configuration des e-mails). La page **Email Configuration** affiche la liste des serveurs SMTP configurés.

## Configuration d'un serveur SMTP

Les serveurs SMTP vous permettent d'envoyer un e-mail aux utilisateurs qui ne se trouvent pas dans le même domaine. Un serveur SMTP vous permet de transmettre les messages d'interruption provenant du domaine du client à une boîte aux lettres de support distante.

Pour ajouter des serveurs SMTP :

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Monitoring Configuration (Configuration de la surveillance)** → **Email Configuration (Configuration des e-mails)**.  
La page **Email Configuration** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
2. Cliquez sur **Add SMTP server (Ajouter un serveur SMTP)**.  
La page **Add SMTP server** s'affiche.
3. Sous **SMTP server (Serveur SMTP)**, saisissez l'adresse IP ou le nom du serveur d'e-mail.
4. Sous **Description**, entrez une description du serveur.
5. Sélectionnez **The SMTP server requires authentication (Le serveur SMTP doit être authentifié)** pour authentifier tous les e-mails présents sur le serveur SMTP à l'aide du nom d'utilisateur et du mot de passe associés saisis dans **User name (Nom d'utilisateur)** et **Password (Mot de passe)**.
6. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Modification d'une configuration de serveur SMTP

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Monitoring Configuration (Configuration de la surveillance)** → **Email Configuration (Configuration des e-mails)**.  
La page **Email Configuration** affiche une liste des serveurs SMTP existants.
2. Dans la liste des serveurs SMTP existants, sous **SMTP server (Serveur SMTP)**, cliquez sur le serveur SMTP approprié.  
La page **Edit SMTP server (Modifier le serveur SMTP)** s'affiche.
3. Sous **SMTP server (Serveur SMTP)**, saisissez l'adresse IP mise à jour ou le nom mis à jour du serveur d'e-mail.
4. Sous **Description**, saisissez la description mise à jour du serveur.
5. Sélectionnez **The SMTP server requires authentication (Le serveur SMTP doit être authentifié)** pour authentifier tous les e-mails présents sur le serveur SMTP à l'aide du nom d'utilisateur et du mot de passe associés saisis dans **User name (Nom d'utilisateur)** et **Password (Mot de passe)**.
6. Cliquez sur **Save Changes (Enregistrer les changements)**.

## Pour supprimer un expéditeur d'email

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Monitoring Configuration (Configuration de la surveillance)** → **Email Configuration (Configuration des e-mails)**.

La page **Email Configuration** affiche une liste des serveurs SMTP existants.

2. Dans la liste des serveurs SMTP existants, sélectionnez un ou plusieurs serveurs SMTP et cliquez sur **Delete SMTP Server(s) (Supprimer le ou les serveur(s) SMTP)**.

## Configuration d'un expéditeur d'e-mail

Certains systèmes de messagerie électronique empêchent l'envoi d'e-mails si l'expéditeur n'appartient pas à un domaine spécifique. Vous pouvez configurer le système pour qu'il envoie tous les e-mails d'un utilisateur spécifique du domaine requis.

Pour déterminer quelles adresses e-mail doivent s'afficher dans le champ **From (De)** lors de l'envoi de message par e-mail, entrez l'adresse e-mail appartenant au domaine requis sous **Send E-mails From (Envoyer les e-mails de)**.

## Configuration des options avancées

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Monitoring Configuration (Configuration de la surveillance)** → **Email Configuration (Configuration des e-mails)**.  
La page **Email Configuration** s'affiche. L'onglet **General (Général)** est sélectionné par défaut.
2. Cliquez sur l'onglet **Advanced (Avancé)**.  
La page **Add SMTP server (Ajouter le serveur SMTP)** s'affiche.
3. Sous **Maximum mail size (kB) (Taille maximale en Ko)**, saisissez la taille maximale de chaque message envoyé par e-mail.
4. Sous **Messages sent in intervals of (seconds) (Messages envoyés en intervalles de (secondes))**, saisissez la durée d'attente maximale avant l'envoi d'une alerte.
5. Cliquez sur **Save Changes (Enregistrer les changements)**.


## Configuration du SNMP

Dell Fluid File System prend en charge le protocole simplifié de transfert de courrier (Simple Network Management Protocol ou SNMP), un protocole de gestion réseau couramment utilisé qui autorise les fonctions de gestion compatibles avec ce dernier, telles que la détection de périphériques, la surveillance et la génération d'événements.

La page SNMP vous permet de configurer des fonctions de gestion compatibles avec le protocole SMTP.

Pour configurer les propriétés SNMP :

1. Sélectionnez **Cluster Management (Gestion de clusters)** → **Monitoring Configuration (Configuration de la surveillance)** → **SNMP Configuration (Configuration SNMP)**.  
La page **SNMP Configuration (Configuration SNMP)** s'affiche. Par défaut, l'onglet **Propriétés** est sélectionné.
2. Sous **System contact (Contact système)**, saisissez le nom du contact requis.
3. Sous **System location (Emplacement du système)**, saisissez une description de l'emplacement du système.
4. Sous **Read community (Communauté de lecture)**, saisissez la communauté SNMP des périphériques lisant des variables SNMP du Dell Fluid File System ou utilisez la valeur par défaut.
5. Sous **Trap recipient (Destinataire d'interruptions)**, saisissez l'adresse IP ou le nom d'hôte du Network Management Server (serveur de gestion réseau) ou d'un autre hôte qui reçoit les interruptions SNMP générées par le Dell Fluid File System.
6. Pour ajouter des destinataires d'interruptions supplémentaires, cliquez sur **Add (Ajouter)**.  
Les destinataires d'interruptions sont ajoutés à la liste.
7. Saisissez l'adresse IP ou le nom d'hôte du serveur de gestion réseau.

8. Pour supprimer un destinataire d'interruptions de la liste, sélectionnez le destinataire d'interruptions approprié et cliquez sur **Delete (Supprimer)**.  
Le destinataire d'interruptions est alors supprimé de la liste.
9. Sélectionnez l'onglet **Filter** (Filtre), puis la gravité minimale d'interruptions à envoyer pour les différentes catégories d'interruptions.  
 **REMARQUE** : Par défaut, toutes les interruptions de toutes les catégories sont envoyées.
10. Cliquez sur **Enregistrer les changements**.



# Dépannage

## Dépannage suite à des problèmes CIFS

### La mauvaise configuration des paramètres de l'hôte AV entraîne un refus d'accès aux fichiers CIFS

Description	La solution en cluster NAS Dell prend en charge les balayages antivirus par partage CIFS. Lorsqu'un fichier d'un partage est ouvert par une application client, la solution en cluster NAS envoie le fichier à un hôte antivirus pour y effectuer un balayage. Si aucun hôte antivirus n'est disponible, l'accès au fichier et à l'ensemble du partage est interrompu.
Cause	Dans la mesure où les hôtes antivirus ne sont pas disponibles sur la solution en cluster NAS, les fichiers ne peuvent pas être ouverts sur un partage CIFS activé par un antivirus.
Solution	Assurez-vous que le problème se produit uniquement sur les partages activés par antivirus, alors que les clients qui accèdent à d'autres partages ne rencontrent pas ce type de problème. Vérifiez l'état des hôtes antivirus et le chemin d'accès au réseau entre la solution en cluster NAS et les hôtes antivirus.

### Refus d'accès au CIFS

Description	L'accès du CIFS à un fichier ou un dossier est refusé.
Cause	Un client ne disposant pas des autorisations suffisantes effectue une opération sur un fichier/dossier.
Solution	Vérifiez les autorisations sur le fichier/dossier et définissez les autorisations requises.

### Corruption de l'ACL du CIFS

Description	Corruption de l'ACL du CIFS
Cause	<ul style="list-style-type: none"> <li>Les ACL ont été accidentellement modifiées par un utilisateur ou un script.</li> <li>L'ACL est corrompue après qu'une application d'antivirus a accidentellement mis en quarantaine les fichiers correspondants.</li> </ul>

- L'ACL s'est corrompue après la récupération des données par l'application d'une sauvegarde en raison de problèmes de compatibilité.
- L'ACL s'est corrompue après la migration de données à partir d'un emplacement différent en utilisant une application tierce, par exemple *RoboCopy*.

Solution

Vérifiez la configuration actuelle des ACL dans le client Windows. Redéfinissez les ACL des fichiers à l'aide du client Windows tel que vous les aviez initialement définies. Vérifiez que vous avez défini les ACL en tant que propriétaire des fichiers, répertoires et partages. Si vous ne pouvez pas redéfinir vos ACL car vous ne possédez pas actuellement les autorisations nécessaires, procédez comme suit :

1. Restaurez les fichiers à partir d'instantanés ou d'une sauvegarde.
2. Au cas où vous auriez fait migrer des données depuis un emplacement différent en utilisant l'application **Robocopy**, vous avez de bonnes chances de pouvoir restaurer les ACL en copiant uniquement les métadonnées des ACL, au lieu de recopier toutes les données.
3. Si toutes les ACL d'un système de fichiers sont corrompues, vous pouvez restaurer toutes les données à partir du partenaire de réplication du NAS.

## Décalage de l'horloge du client CIFS

Description

Décalage de l'horloge du client CIFS.

Cause

L'horloge du client doit être réglée sur une plage de 5 minutes par rapport à l'horloge du serveur Kerberos (c'est-à-dire Active Directory).

Solution

Configurez le client pour la synchronisation d'horloge avec le répertoire Active Directory (comme un serveur NTP) afin d'éviter les erreurs dues au décalage d'horloge.

## Déconnexion du client CIFS à la lecture du fichier

Description

Déconnexion du client CIFS à la lecture du fichier.

Cause

Charge de traitement extrême du CIFS au cours du basculement du contrôleur.

Solution

Le client doit se reconnecter et rouvrir le fichier.

## Déconnexion générale du client CIFS

Description	Déconnexion du client CIFS.
Cause	Au cas où le système aurait identifié un problème général au niveau du service CIFS, il serait automatiquement restauré, mais cette défaillance entraînerait une déconnexion de tous les utilisateurs et l'événement ci-dessus serait déclenché.
Solution	Si ce problème se répète fréquemment, contactez Dell.

## Échec de la connexion au client CIFS

Description	Échec de la connexion au client CIFS.
Cause	L'utilisateur a fourni un mot de passe erroné à la connexion.
Solution	Les utilisateurs interactifs peuvent réessayer en saisissant le mot de passe correct. Les applications et les serveurs peuvent exiger une attention particulière car le nom d'utilisateur/mot de passe (généralement défini dans un script ou un fichier de configuration) a probablement expiré.

## Échec de connexion CIFS

Description	Accès au client CIFS refusé.
Cause	L'utilisateur est inconnu dans le serveur Active Directory, et le système NAS a adressé cet utilisateur à un serveur invité. Si le partage n'autorise pas l'accès invité, l'utilisateur reçoit un message d'alerte indiquant que l'accès est refusé.
Solution	Assurez-vous que l'utilisateur est répertorié dans le serveur Active Directory que le NAS utilise. Sinon, supprimez la restriction d'invité du partage. Si l'utilisateur peut maintenant accéder au partage en tant qu'invité, les fichiers nouvellement créés appartiennent à l'utilisateur invité (personne).

## Refus de la suppression à la fermeture du CIFS

Description	Les fichiers sont supprimés pendant leur utilisation.
Cause	Si un fichier est supprimé alors qu'il est ouvert, il est marqué comme fichier à supprimer et est supprimé à sa fermeture. Il apparaît dans son emplacement d'origine jusqu'à sa fermeture, cependant le système refuse son ouverture.
Solution	Informez l'utilisateur qui a tenté d'ouvrir le fichier du fait que le fichier a été supprimé.

## Accès au fichier CIFS refusé

Description	Accès au fichier CIFS refusé.
Cause	Le client possède des autorisations insuffisantes pour réaliser l'opération demandée sur le fichier.
Solution	Il s'agit ici d'un événement informatif. L'utilisateur peut demander à modifier l'ACL du fichier pour autoriser l'accès.

## Conflit de partage du fichier CIFS

Description	Conflit de partage du fichier CIFS.
Cause	Lorsqu'un fichier a été ouvert à l'aide du protocole CIFS, l'application utilisée pour l'ouvrir communique le mode de partage qui doit être utilisé pendant que ce fichier est ouvert. Ce mode de partage décrit les autres activités autorisées sur ce fichier pendant qu'il est ouvert. Cette définition est envoyée par l'application et l'utilisateur ne peut pas la contrôler/la configurer. En cas de violation de partage, l'utilisateur reçoit une erreur de type refus d'accès et cet événement est émis.
Solution	Il s'agit d'un événement informatif, l'administrateur peut contacter l'utilisateur qui procède au verrouillage et demander à fermer l'application faisant référence à fichier. L'application qui a ouvert le fichier peut ne pas s'être arrêtée correctement. Il est recommandé de redémarrer le client, si possible.

## Compte d'invité CIFS non valide

Description	Le service CIFS ne peut pas démarrer.
Cause	Un compte d'invité CIFS valide est requis pour le bon fonctionnement du CIFS.
Solution	Configurez le compte d'invité du système avec un compte valide.

## Incohérence de verrouillage du CIFS

Description	Le service CIFS est interrompu en raison de problèmes de verrouillage du CIFS.
Cause	Scénarios de verrouillage du client CIFS.
Solution	Le système récupère automatiquement en émettant l'événement ci-dessus lorsqu'il est rétabli.

## Nombre maximum de connexions au CIFS atteint

Description	Le nombre maximum de connexions au CIFS par contrôleur NAS a été atteint.
Cause	<p>Chaque appliance NX3600 est limitée à 200 connexions CIFS simultanées, et chaque appliance NX3610 et FS8600 est limitée à 1500 connexions.</p> <ul style="list-style-type: none"><li>• Le système est à l'état optimal et le nombre maximal de clients CIFS accédant à un des contrôleurs est atteint. Dans un tel scénario, pensez à ajouter une autre appliance NAS.</li><li>• Le système se trouve dans un état optimal, mais les clients sont très déséquilibrés entre les contrôleurs NAS. Dans ce cas, rééquilibrez les clients à l'aide du NAS Manager.</li><li>• Le système est en état Dégradé (un ou plusieurs contrôleurs NAS sont en panne) et les clients CIFS se trouvent sur le contrôleur restant. Dans ce cas, patientez jusqu'à ce que le système revienne à l'état optimal ou réduisez le nombre de clients CIFS qui utilisent le système.</li></ul>
Solution	Si tous les contrôleurs NAS sont en mode optimal, les connexions sont divisées entre les deux.

## Le partage CIFS n'existe pas

Description	Le client tente de se connecter à un partage inexistant.
Cause	<ul style="list-style-type: none"><li>• Faute d'orthographe côté client</li><li>• Accès au mauvais serveur</li></ul>
Solution	<p>Répertoriez les partages de NAS disponibles et vérifiez que tous les partages sont affichés et que rien n'a été modifié accidentellement.</p> <p>Vérifiez que vous pouvez accéder au partage problématique en utilisant un client Windows :</p> <ol style="list-style-type: none"><li>1. Cliquez sur <b>Exécuter</b>.</li><li>2. Saisissez l'adresse IP virtuelle d'accès au client et le nom de partage : <code>\\&lt;Adresse_IP_virtuelle_du_client&gt;\&lt;nom_de_partage_CIFS&gt;</code></li></ol>

## Partage du chemin d'accès CIFS introuvable

Description	Le client a accédé à un partage qui fait référence à un répertoire inexistant dans le conteneur NAS.
Cause	<ul style="list-style-type: none"><li>• Le système NAS est restauré depuis une sauvegarde ou une réplication à distance. Lorsque la restauration est en cours, la structure</li></ul>

Solution	<p>du répertoire n'est pas complète et certains répertoires peuvent ne pas exister. Communiquez l'état et attendez que le processus de restauration soit terminé.</p> <ul style="list-style-type: none"> <li>• Un client autorisé supprime ou modifie un répertoire monté par un autre client. Si plusieurs utilisateurs accèdent au même ensemble de données, il vous est recommandé d'appliquer un programme d'autorisation strict afin d'éviter ce genre de conflit.</li> </ul> <p>Répertoriez tous les partages disponibles sur le NAS et identifiez le partage posant problème. Ce dernier indique qu'il n'est pas accessible.</p> <ol style="list-style-type: none"> <li>1. Restaurez le chemin d'accès qui pose problème à partir d'une sauvegarde.</li> <li>2. Créez manuellement les répertoires manquants. Définissez les autorisations pour contrôler l'accès, au besoin.</li> <li>3. Supprimez le partage et communiquez-le au client.</li> </ol>
----------	---

## Écriture du CIFS sur un volume en lecture seule

Description	Un client tente de modifier un fichier qui se trouve sur un volume en lecture seule.
Cause	<p>Un volume NAS est défini comme étant en lecture seule lorsqu'il est la cible d'une réplication.</p> <p>Cet événement est le plus souvent provoqué par :</p> <ul style="list-style-type: none"> <li>• Un utilisateur qui avait l'intention d'accéder au système cible pour lecture, mais qui tente également de modifier un fichier par erreur.</li> <li>• Un utilisateur qui accède au mauvais système en raison d'une ressemblance de nom/adresse IP.</li> <li>• Un utilisateur qui accède à un conteneur NAS, lequel est devenu la cible d'une réplication à son insu.</li> </ul>
Solution	Vous ne pouvez écrire sur ce volume qu'une fois la réplication déconnectée. Indiquez à l'utilisateur l'emplacement correct.

## Dépannage suite à des problèmes NFS

### Impossible de monter l'exportation NFS

Description	<p>Lors d'une tentative de montage d'une exportation NFS, la commande de montage échoue en raison de plusieurs raisons, parmi lesquelles :</p> <ul style="list-style-type: none"> <li>• Autorisation refusée.</li> </ul>
-------------	--

## Cause

- L'appliance ne répond pas en raison d'un échec de l'adressage des ports - délai RPC expiré ou erreur d'entrée/sortie.
- L'appliance ne répond pas car le programme n'est pas enregistré.
- Accès refusé.
- N'est pas un répertoire

- Le client se connecte à l'aide de NFS/UDP et un pare-feu est installé entre les deux.
- Le client ne figure pas dans la liste d'exportation, l'appliance n'a pas pu reconnaître le système client via NIS ou l'appliance n'accepte pas l'identité que vous avez fournie.
- La solution en cluster NAS est en panne ou subit des problèmes de système de fichiers internes.
- La commande de montage est passée à travers l'adresseur de ports, mais le démon de montage NFS **rpc.mountd** n'a pas été enregistré.
- L'adresse IP du système client, la plage IP, le nom de domaine ou le groupe réseau ne figure pas dans la liste d'exportation du volume qu'il tente de monter à partir de la solution en cluster NAS.
- Le chemin d'accès distant ou le chemin d'accès local n'est pas un répertoire.
- Le client ne dispose pas de l'autorité racine ou n'est pas membre du groupe système. Les montages et démontages NFS sont autorisés uniquement pour les utilisateurs racine et membres du groupe système.

## Solution

Si le problème découle de NFS/UDP et du pare-feu, vérifiez si le client est monté à l'aide d'UDP (généralement le protocole par défaut) et si un pare-feu se trouve dans le chemin. Si un pare-feu existe, ajoutez une exception appropriée au pare-feu.

Si le problème est dû aux autorisations :

- Vérifiez que le chemin d'accès que vous avez fourni est correct.
- Vérifiez que vous tentez d'effectuer le montage en tant que racine.
- Vérifiez que l'adresse IP du système, la plage IP, le nom de domaine ou le groupe réseau se trouve dans la liste des exportations.

Si le serveur ne répond pas en raison d'une défaillance de l'adresseur de ports :

- Vérifiez l'état de la solution en cluster NAS.
- Vérifiez la connexion au réseau en essayant le montage NFS à partir d'une autre machine.
- Vérifiez si d'autres utilisateurs rencontrent le même problème.

Si le serveur ne répond pas car le programme n'est pas enregistré, vérifiez si l'adresseur de ports de votre client est en fonctionnement.

Si le problème est dû à un refus d'accès :

- Obtenez la liste des systèmes de fichiers exportés par l'appliance à l'aide de la commande :  
`showmount -e <FluidFS hostname>`
- Vérifiez que le nom du système ou le nom du groupe réseau ne figure pas dans la liste des utilisateurs du système de fichiers.
- Vérifiez les systèmes de fichiers liés au NFS via l'interface utilisateur de la solution en cluster NAS.

Si le problème est lié au répertoire, vérifiez l'orthographe de votre commande et essayez d'exécuter la commande de montage sur les deux répertoires.

## L'exportation NFS n'existe pas

Description

A tenté de monter une exportation qui n'existe pas.

Cause

Cet échec est souvent causé par des erreurs d'orthographe sur le système client ou survient lors de l'accès à un serveur erroné.

Solution

1. Vérifiez les exportations disponibles sur le NAS, assurez-vous que toutes les exportations requises existent.
2. Sur le client posant problème, vérifiez que l'exportation pertinente est disponible pour ce client :
3. `% showmount -e <Nom serveur/IP>`
4. Liste d'exportation pour <Nom serveur/IP>:
5. `/abc 10.10.10.0`
6. `/xyz 10.10.10.0`
7. Si l'exportation est disponible, vérifiez l'orthographe de cette dernière dans la commande de montage pertinente sur le client. Il est recommandé de copier-coller le nom d'exportation depuis la sortie `showmount` sur la commande de montage.

## Accès au fichier NFS refusé

Description

Cet événement est émis lorsqu'un utilisateur NFS ne dispose pas de suffisamment d'autorisations d'accès au fichier sur un conteneur NAS.

Cause

Le propriétaire du fichier est UID/UNIX et l'utilisateur ne dispose pas de droits d'accès au fichier ou le propriétaire du fichier est SID/ACL et après traduction dans UID/UNIX, les autorisations ne permettent pas l'accès au fichier.

Solution	<p>Pour un accès natif (lorsque l'utilisateur CIFS accède au fichier SID/ACL ou lorsque l'utilisateur NFS accède au fichier UID/UNIX), l'autorisation manquante est généralement sous-entendue.</p> <p>Si l'accès n'est pas natif, les règles de traduction entrent en vigueur et il vous est recommandé de contacter le Support technique Dell.</p>
----------	--

## Accès NFS non sécurisé pour une exportation sécurisée

Description	L'utilisateur tente d'accéder à une exportation sécurisée à partir d'un port non sécurisé.
Cause	L'exigence d'exportation sécurisée signifie que les clients qui accèdent au système doivent utiliser un port bien connu (inférieur à 1024), ce qui signifie généralement qu'ils doivent être racine (root) (uid=0) sur le client.
Solution	<ul style="list-style-type: none"> <li>• Identifiez l'exportation pertinente et assurez-vous qu'elle est définie comme sécurisée (requiert un port client sécurisé).</li> <li>• Si l'exportation doit rester sécurisée, consultez la documentation du client NFS pour émettre la demande de montage à partir d'un port bien connu (inférieur à 1024).</li> <li>• Si une exportation sécurisée n'est pas requise (par exemple, si le réseau n'est pas public), assurez-vous que l'exportation n'est pas sécurisée et essayez à nouveau d'y accéder.</li> </ul>

## Le montage NFS échoue en raison des options d'exportation

Description	Cet événement est émis lorsque le montage NFS échoue en raison des options d'exportation.
Cause	La liste d'exportation filtre l'accès des clients par adresse IP, réseau ou groupe réseau et sélectionne les clients qui y accèdent.
Solution	<ol style="list-style-type: none"> <li>1. Vérifiez les détails d'exportation pertinents. Notez toutes les options sur un bout de papier afin de pouvoir y revenir aisément.</li> <li>2. Supprimez les restrictions IP/client à l'exportation et réessayez le montage.</li> <li>3. Si l'opération de montage réussit, vérifiez que l'IP ou le domaine est explicitement spécifié(e) ou fait partie d'un réseau ou des groupes de réseaux définis. Faites attention aux scénarios piège où le masque réseau du réseau n'est pas intuitif, par exemple lorsque 192.175.255.254 fait partie de 192.168.0.0/12 et non de 192.168.0.0/16.</li> <li>4. Une fois le montage réussi, réglez les options d'origine en conséquence.</li> </ol>

## Le montage NFS échoue en raison de l'échec du groupe réseau

Description	Cet événement est émis lorsque le client ne monte pas une exportation NFS car les informations du groupe réseau requises ne sont pas accessibles.
Cause	Cette erreur survient généralement suite à une erreur entre le système NAS et le serveur NIS/LDAP. Celle-ci peut découler d'un problème réseau, d'une surcharge du serveur de répertoire, ou d'un mauvais fonctionnement du logiciel.
Solution	<p>Répétez le processus ci-dessous pour chaque serveur NIS configuré, en laissant chaque fois un seul NIS utilisé, en commençant par le serveur NIS posant problème.</p> <ol style="list-style-type: none"><li>1. Inspectez les journaux du serveur NIS/LDAP et voyez si la raison de l'erreur est signalée dans les journaux.</li><li>2. Effectuez un test réseau en envoyant un ping au NAS depuis un client se trouvant dans le même sous-réseau que le serveur NIS/LDAP.</li><li>3. Envoyez un ping au serveur NIS/LDAP à partir d'un client situé sur le même sous-réseau que le serveur NAS.</li><li>4. Si la perte d'un paquet est évidente sur l'un des serveurs ci-dessus, résolvez les problèmes réseau dans l'environnement.</li><li>5. Depuis un client Linux situé sur le même sous-réseau que le NAS et configuré pour utiliser le même serveur de répertoire, demandez des détails concernant le groupe de réseau au serveur NIS/LDAP à l'aide des commandes pertinentes. Assurez-vous que la réponse est reçue en temps opportun (jusqu'à 3 secondes).</li></ol> <p>Vous pouvez contourner temporairement le problème en supprimant la restriction du groupe réseau sur l'exportation et/ou en définissant un serveur de répertoire alternatif.</p> <p>Identifiez l'exportation pertinente et les options définies pour cette dernière, tout en réglant la définition du groupe de réseau. Documentez le groupe de réseau utilisé afin de le restaurer une fois le problème résolu et pour supprimer la limitation de ce groupe de réseau.</p>

## Le chemin d'accès au montage NFS n'existe pas

Description	Le client tente de monter un chemin qui n'existe pas sur un conteneur NAS.
Cause	Cette erreur se produit généralement dans l'un des scénarios suivants : <ul style="list-style-type: none"><li>• Lorsque vous accédez à un système en cours de restauration depuis une sauvegarde ou une réplique à distance. La structure complète du</li></ul>

Solution	<p>répertoire est uniquement disponible lorsque la restauration est terminée.</p> <ul style="list-style-type: none"> <li>• Un client disposant d'une autorisation d'accès à un répertoire supérieur dans le même chemin d'accès supprime ou modifie un répertoire, lequel est en cours de montage par un autre client.</li> <li>• Si plusieurs utilisateurs accèdent au même jeu de données, il est recommandé d'appliquer un programme d'autorisation strict afin d'éviter ce scénario.</li> </ul> <ol style="list-style-type: none"> <li>1. Si le système NAS est en cours de restauration, communiquez l'état actuel au client et indiquez au client de patienter tant que le processus de restauration n'est pas terminé.</li> <li>2. Dans l'autre cas, trois options sont possibles : <ul style="list-style-type: none"> <li>– Restaurez le chemin d'accès qui pose problème à partir d'une sauvegarde.</li> <li>– Créez manuellement les répertoires manquants pour permettre le montage. Les clients reçoivent des erreurs lorsqu'ils tentent d'accéder aux données existantes d'un chemin supprimé.</li> <li>– Supprimez l'exportation et communiquez cette information au client.</li> </ul> </li> <li>3. Répertoirez toutes les exportations disponibles sur le NAS et identifiez l'exportation posant problème. Cette dernière indique qu'elle n'est pas accessible.</li> <li>4. Supprimez l'exportation ou créez le répertoire sur lequel l'exportation pointe.</li> </ol>
----------	--

## Opération limitée par le propriétaire NFS

Description	Le client NFS n'est pas autorisé à effectuer l'action demandée sur le fichier particulier.
Cause	Un utilisateur NFS a tenté une opération <code>chmod</code> ou <code>chgrp</code> alors qu'il n'est pas le propriétaire du fichier.
Solution	Il s'agit d'un problème utilisateur de bas niveau. Si plusieurs événements de ce type se produisent, cela pourrait indiquer une tentative malveillante d'accéder à des données à accès limité.

## Écriture du NFS sur une exportation en lecture seule

Description	Un client NFS tente de procéder à des modifications sur une exportation en lecture seule.
Cause	Une exportation NFS peut être définie en tant qu'exportation en lecture seule. Un client accédant à une exportation en lecture seule ne peut effectuer aucune opération d'écriture ni modifier les fichiers inclus.

Solution Cet événement, en lui-même, ne requiert aucune intervention administrative.

## Écriture du NFS sur un volume en lecture seule

Description Un utilisateur NFS tente de modifier un fichier qui se trouve sur un volume en lecture seule.

Cause Un volume NAS devient un volume en lecture seule lorsqu'il est défini comme cible d'une relation de réplication. Vous ne pouvez modifier un tel volume qu'une fois la relation de réplication supprimée, après quoi le volume revient à un état normal.

Solution Informez l'utilisateur (les utilisateurs) de l'état du volume NAS.

## Écriture du NFS sur un instantané

Description Un utilisateur NFS tente de modifier un fichier qui se trouve dans un instantané.

Cause Les instantanés de volume NAS ne sont pas modifiables.

Solution Les données d'un instantané ne peuvent pas être modifiées. Un instantané est une représentation exacte des données d'un volume NAS au moment de sa création.

## Accès au NFS refusé à un fichier ou un répertoire

Description Un utilisateur ne peut pas accéder au fichier ou au répertoire du NFS, bien que l'utilisateur appartienne au groupe propriétaire de l'objet NFS et que les membres du groupe soient autorisés à réaliser cette opération.

Cause Les serveurs NFS (versions 2 et 3) utilisent le protocole d'appel de procédure à distance RPC pour authentifier les clients NFS. La plupart des clients RPC sont conçus pour communiquer un maximum de 16 groupes au serveur NFS. Si un utilisateur appartient à plus de 16 groupes UNIX, tel que pris en charge par certaines versions UNIX, certains groupes ne sont pas communiqués et ne sont pas vérifiés par le serveur NFS, ce qui explique pourquoi l'accès de l'utilisateur peut être refusé.


Solution L'un des moyens de vérifier ce problème consiste à utiliser `newgrp` pour modifier temporairement le groupe principal de l'utilisateur et ainsi, s'assurer qu'il est communiqué au serveur.

La solution de contournement simple, même si elle n'est pas toujours réalisable, consiste à supprimer l'utilisateur des groupes inutiles, en ne conservant que 16 groupes ou moins.

# Dépannage de problèmes de réplication

## Erreur de configuration de la réplication

Description	La réplication entre les volumes NAS source et cible échoue car les topologies des systèmes source et cible ne sont pas compatibles.
Cause	Les systèmes source et cible sont incompatibles à des fins de réplication.
Solution	Mettez à niveau la solution en cluster NAS en panne. Vérifiez que la source et la destination possèdent toutes les deux le même nombre de contrôleurs NAS.

 **REMARQUE :** Vous ne pouvez pas effectuer de réplication entre un cluster NAS à 4 nœuds et un cluster NAS à 2 nœuds.

## Le cluster cible de la réplication est occupé

Description	La réplication entre le volume NAS source et le volume NAS cible échoue car le cluster cible n'est pas disponible pour produire la réplication requise.
Cause	La tâche de réplication échoue car le cluster cible n'est pas disponible pour fournir la réplication demandée.
Solution	Les administrateurs doivent vérifier l'état de réplication sur le système cible.

## Le FS cible de la réplication est occupé

Description	La réplication entre le volume NAS source et le volume NAS de destination échoue.
Cause	La tâche de réplication échoue car le cluster cible est temporairement indisponible pour fournir la réplication demandée.
Solution	La réplication continue automatiquement dès que le système de fichiers libère une partie des ressources. Les administrateurs doivent vérifier que la réplication continue bien automatiquement lorsqu'une heure s'est écoulée.

## La destination de la réplication est en panne

Description	La réplication entre le volume NAS source et le volume NAS de destination échoue.
Cause	La tâche de réplication échoue car le système de fichiers du volume NAS cible est en panne.
Solution	Les administrateurs doivent vérifier si le système de fichiers du système cible est en panne à l'aide de la

section de surveillance du NAS Manager. Si le système de fichiers de la solution en cluster NAS ne répond pas, les administrateurs doivent démarrer le système sur le cluster cible. La réplication se poursuit automatiquement après le démarrage du système de fichiers.

## La cible de la réplication n'est pas à l'état optimal

Description	La réplication entre le volume source et le volume cible du NAS échoue car le volume NAS cible n'est pas à l'état optimal.
Cause	La réplication échoue car le système de fichiers du volume NAS cible n'est pas à l'état optimal.
Solution	Les administrateurs doivent vérifier l'état du système cible à l'aide de la section de surveillance du NAS Manager afin de comprendre pourquoi le système de fichiers n'est pas à l'état optimal. La réplication se poursuit automatiquement une fois que le système de fichier revient à l'état optimal.

## Le volume cible de la réplication est occupé à récupérer de l'espace

Description	La réplication entre le volume source et le volume cible du NAS échoue car le volume NAS cible est occupé à libérer de l'espace.
Cause	La tâche de réplication échoue car le volume NAS cible est occupé à libérer de l'espace.
Solution	La réplication continue automatiquement dès que de l'espace est disponible. Les administrateurs doivent vérifier que la réplication continue bien automatiquement lorsqu'une heure s'est écoulée.

## Le volume cible de la réplication est déconnecté

Description	La réplication entre le volume source et le volume cible du NAS échoue car le volume cible du NAS est déconnecté du volume source.
Cause	La tâche de réplication échoue car le volume NAS cible a été préalablement déconnecté du volume NAS source.
Solution	Les administrateurs doivent effectuer une opération de déconnexion du volume NAS source. Au besoin, connectez à nouveau les deux volumes NAS dans une relation de réplication.

## Déconnexion de la réplication

Description	La réplication entre le volume source et le volume cible du NAS échoue car la connexion entre les systèmes source et cible est perdue.
Cause	Déconnexion de l'infrastructure réseau entre la source et la cible.
Solution	L'administrateur doit vérifier si la réplication est restaurée automatiquement. Si elle n'est pas restaurée automatiquement, vérifiez la communication réseau entre les clusters source et cible. Pour ce faire, utilisez un système tiers dans le même sous-réseau pour envoyer un ping aux clusters source et cible.

## Versions incompatibles avec la réplication

Description	La réplication entre le volume source et le volume cible du NAS échoue car la version du système du cluster source du NAS est plus élevée que la version du système du cluster cible.
Cause	La tâche de réplication échoue car la version système du volume source du NAS est plus élevée que la version système du cluster cible.
Solution	Les administrateurs doivent mettre à niveau la version du système du cluster cible pour qu'elle corresponde à la version du système du cluster source.

## Erreur interne de réplication

Description	La réplication entre les volumes source et cible du NAS échoue en raison d'une erreur interne.
Solution	Contactez Dell pour résoudre ce problème.

## Les trames Jumbo de réplication sont bloquées

Description	La réplication entre les volumes source et cible du NAS échoue car les trames Jumbo sont bloquées sur le réseau.
Cause	La tâche de réplication échoue car les trames étendues (Jumbo) sont bloquées sur le réseau.
Solution	L'administrateur doit vérifier que la configuration réseau entre le cluster source et le cluster cible a activé le transfert de trames Jumbo sur les commutateurs ou les routeurs.

## Le volume cible de réplication ne contient pas suffisamment d'espace libre

Description	La réplication entre le volume source et le volume cible du NAS échoue car l'espace disponible sur le volume NAS cible est insuffisant.
Cause	La tâche de réplication échoue car l'espace disponible sur le volume NAS cible est insuffisant.
Solution	Augmentez l'espace disponible sur le volume NAS cible.

## La source de réplication est occupée

Description	La réplication entre le volume source et le volume cible du NAS échoue car le système de fichiers du volume NAS source est occupé à répliquer d'autres volumes du NAS.
Cause	La tâche de réplication échoue car le système de fichiers du volume NAS source est occupé à répliquer d'autres volumes NAS.
Solution	La réplication continue automatiquement dès que le système de fichiers libère une partie des ressources. Les administrateurs doivent vérifier que la réplication continue bien automatiquement lorsqu'une heure s'est écoulée.

## La source de la réplication est en panne

Description	La réplication entre le volume source et le volume cible du NAS échoue car le volume NAS source est à l'arrêt.
Cause	Le système de fichiers du volume NAS source est en panne.
Solution	Les administrateurs doivent vérifier si la solution en cluster NAS est en panne dans le système source en vérifiant la section « surveillance » du NAS Manager. Si la solution du cluster NAS est en panne, les administrateurs doivent démarrer le système de fichiers sur le cluster source. La réplication continue automatiquement au démarrage du système.

## La source de la réplication n'est pas à l'état optimal

Description	La réplication entre les volumes source et cible du NAS échoue car le système de fichiers du volume source du NAS n'est pas à l'état optimal.
Cause	La réplication échoue car le système de fichiers de la source n'est pas à l'état optimal.
Solution	Les administrateurs doivent vérifier l'état du système source en utilisant la section « surveillance » du NAS Manager pour comprendre pourquoi le système de fichiers n'est pas à l'état optimal.

## Le volume source de la réplication est occupé à récupérer de l'espace

Description	La réplication entre le volume source et le volume cible du NAS échoue car le volume NAS source est occupé à récupérer de l'espace.
Cause	La tâche de réplication a échoué car le volume NAS source est occupé à récupérer de l'espace.
Solution	La réplication se poursuit automatiquement lorsque de l'espace est disponible. Les administrateurs doivent vérifier que la réplication se poursuit bien automatiquement après un certain temps (une heure).

## Dépannage de problèmes Active Directory

### Le quota de groupe pour un utilisateur Active Directory ne fonctionne pas

Description	Le quota de groupe est défini pour un groupe Active Directory ; toutefois, lorsqu'un membre du groupe consomme de l'espace, l'utilisation réelle du groupe n'augmente pas et la limite du groupe n'est pas appliquée.
Cause	<p>L'application de quota de la solution en cluster NAS est réalisée en fonction de l'ID utilisateur et du GID du fichier (UNIX) ou du SID et du GSID du groupe principal de l'utilisateur (NTFS) s'il est défini.</p> <p>Dans le cas d'utilisateurs Active Directory, le paramétrage du groupe principal n'est pas obligatoire, et s'il n'est pas défini, l'espace utilisé ne sera comptabilisé pour aucun groupe. Le groupe principal doit être attribué pour que le quota de groupe prenne effet dans le cas d'utilisateurs Active Directory.</p>
Solution	<p>Pour configurer le groupe principal pour un utilisateur d'Active Directory :</p> <ol style="list-style-type: none"><li>1. Ouvrez le Gestionnaire Active Directory.</li><li>2. Cliquez avec le bouton droit sur l'utilisateur de votre choix.</li><li>3. Cliquez sur l'onglet <b>Member of (Membre de)</b>. Le groupe que vous recherchez doit être répertorié.</li><li>4. Cliquez sur le groupe, puis sur le bouton <b>Set Primary Group</b> (Définir le groupe principal).</li></ol> <p>Les quotas prennent maintenant effet pour le groupe de l'utilisateur.</p>

## Authentification Active Directory

Description	Un utilisateur valide d'Active Directory n'est pas authentifié.
Cause	Causes probables : <ul style="list-style-type: none"><li>• L'utilisateur tente de s'authentifier en utilisant un mot de passe incorrect.</li><li>• L'utilisateur est verrouillé ou désactivé dans Active Directory.</li><li>• Les contrôleurs de domaine Active Directory sont hors ligne ou inaccessibles.</li><li>• L'horloge système et l'horloge Active Directory ne sont pas synchronisées.</li></ul>
Solution	<ol style="list-style-type: none"><li>1. Vérifiez si des erreurs se sont produites en consultant le journal des événements système de la solution en cluster NAS du NAS Manager.</li><li>2. Vérifiez que l'utilisateur n'est pas désactivé ni verrouillé dans Active Directory.</li><li>3. Vérifiez que les contrôleurs de domaine sont en ligne et accessibles via le réseau.</li><li>4. Kerberos exige que les horloges du client et du serveur soient synchronisées. Vérifiez que l'horloge système est synchronisée avec l'horloge du contrôleur de domaine et, le cas échéant, configurez le paramétrage NTP du système.</li></ol>

## Dépannage de la configuration d'Active Directory

Description	Impossible d'ajouter des utilisateurs et des groupes Active Directory aux partages CIFS.
Cause	Causes probables : <ul style="list-style-type: none"><li>• Impossible d'envoyer un ping au domaine à l'aide de FQDN.</li><li>• Il est possible que le DNS ne soit pas configuré.</li><li>• Il est possible que le NTP ne soit pas configuré.</li></ul>
Solution	Lors de la configuration du système pour la connexion à un domaine Active Directory : <ol style="list-style-type: none"><li>1. Assurez-vous que vous utilisez FQDN et non le nom NETBIOS du domaine ou l'adresse IP du contrôleur de domaine.</li><li>2. Assurez-vous que l'utilisateur dispose des autorisations d'ajouter des systèmes au domaine.</li><li>3. Utilisez le mot de passe correct.</li><li>4. Accédez à l'onglet <b>DNS Configuration (Configuration du DNS)</b> et entrez les informations correctes.</li></ol>

5. Configurez les informations NTP et assurez-vous que l'heure du système correspond à l'heure du domaine.
6. Si vous utilisez plusieurs systèmes NAS, assurez-vous que vous avez défini différents noms NETBIOS. Le système utilise CIFS Storage (Stockage CIFS) comme nom par défaut.
7. Assurez-vous que vous sélectionnez **Authenticate users' identity via Active Directory and local users database (Authentifier l'identité des utilisateurs via Active Directory et la base de données des utilisateurs locaux)**.

## Dépannage de l'accès au fichier NAS et de problèmes d'autorisation

### Impossible de modifier la propriété d'un fichier ou d'un dossier

Description	Tous les fichiers du système NAS appartiennent à un utilisateur UNIX ou NFS. L'impossibilité de modifier la propriété est traitée différemment, selon le type d'accès : natif ou non.
Cause	L'utilisateur n'est pas autorisé à procéder au changement de propriété.
Solution	Cette action doit être effectuée par un utilisateur autorisé.

### Impossible de modifier les fichiers NAS

Description	Un utilisateur ou une application ne peut pas modifier un fichier.
Cause	<ul style="list-style-type: none"> <li>• Le client ne peut pas modifier un fichier en raison d'un manque d'autorisations d'accès au fichier.</li> <li>• Le volume du NAS est saturé et le système de fichiers refuse toute demande d'écriture, y compris par écrasement.</li> <li>• Le volume NAS est une cible dans une relation de réplication et est en lecture seule.</li> </ul>
Solution	<ul style="list-style-type: none"> <li>• Si le problème ne survient que pour certains fichiers, il s'agit d'un problème d'autorisation d'accès. Modifiez les autorisations du compte utilisateur ou utilisez un compte utilisateur différent.</li> <li>• Si le problème est lié à un volume NAS spécifique :             <ol style="list-style-type: none"> <li>a. Vérifiez que l'espace disponible sur le volume NAS est suffisant ou développez-le.</li> <li>b. Vérifiez que le volume NAS auquel vous avez accédé n'est pas la cible d'une réplication.</li> </ol> </li> </ul>

## Propriété mixte du fichier refusée

Description	Les propriétaires du fichier et du groupe doivent tous les deux disposer du même type d'identité (UNIX ou NTFS). Une tentative de configuration de types d'identité différents a été détectée.
Cause	Il est impossible de modifier seulement l'ID du propriétaire du fichier en le remplaçant par l'UID si la propriété du fichier d'origine est SID/GSID.
Solution	Pour modifier le propriétaire du fichier en le remplaçant par un propriétaire de style UNIX, définissez l'UID et le GID simultanément.

## Accès au SMB problématique à partir d'un client Linux

Description	<p>Un client Linux/UNIX tente de monter un partage de solution en cluster NAS en utilisant SMB (avec /etc/fstab ou directement via smbmount).</p> <p>Un client Linux/UNIX tente d'accéder au système de fichiers en utilisant la commande smbclient, par exemple :</p> <pre>smbclient //&lt;nas&gt;/&lt;share&gt; -U user %password -c ls</pre>
Solution	<p>Nous vous recommandons d'utiliser les interfaces du protocole NFS pour accéder les systèmes Fluid FS de la solution en cluster NAS depuis les clients Linux/UNIX. Pour contourner ce problème :</p> <ol style="list-style-type: none"><li>1. Assurez-vous que votre administrateur crée des exportations NFS vers les emplacements que vous utilisez pour accéder à l'aide de CIFS et connectez-vous à ces emplacements à l'aide de la commande de montage à partir des clients Linux/UNIX.</li><li>2. Utilisez les interfaces NFS pour accéder à la solution en cluster NAS. Par exemple, depuis le système de gestion Linux NAGIOS, utilisez la commande / <code>check_disk</code> au lieu de la commande / <code>check_disk_smb</code>.</li></ol>

## Numéros d'UID et de GID étranges sur les fichiers du système NAS Dell

Description	Les nouveaux fichiers créés à partir de clients Ubuntu 7.x reçoivent un UID ou un GID de 4294967294 (nfsnone).
Cause	Par défaut, les clients NFS Ubuntu 7.x ne fournissent aucune coordonnée rpc sur leurs appels NFS. Par conséquent, les fichiers créés par tout utilisateur à partir de ces clients sont la propriété des UID et GID 4294967294 (nfsnone).
Solution	Pour forcer les coordonnées UNIX sur les appels NFS, ajoutez l'option <b>sec=sys</b> aux montages de la solution en cluster NAS dans le fichier Ubuntu <b>fstab</b> .

# Dépannage de problèmes de mise en réseau

## Serveur de nom non réactif

Description	Tous les serveurs NIS, LDAP ou DNS sont inaccessibles ou ne répondent pas.
Solution	Pour chaque serveur : <ol style="list-style-type: none"><li>1. Envoyez un ping au serveur à partir d'un client situé sur le sous-réseau de la solution en cluster NAS et vérifiez qu'il répond.</li><li>2. Émettez une demande au serveur à partir d'un client situé sur le sous-réseau de la solution en cluster NAS et vérifiez qu'il répond.</li><li>3. Vérifiez les journaux de serveur pour comprendre la raison pour laquelle le serveur ne peut pas répondre aux demandes.</li></ol>

## Des clients de sous-réseaux spécifiques ne peuvent pas accéder à la solution en cluster NAS

Description	Les utilisateurs (nouveaux ou anciens) situés sur des réseaux spécifiques ne peuvent pas accéder à la solution en cluster NAS.
Cause	Le problème découle d'un conflit entre les adresses de sous-réseau de l'utilisateur et l'adresse du réseau interne du système NAS. Le système NAS adresse les paquets de réponse au mauvais réseau.
Solution	<ol style="list-style-type: none"><li>1. Vérifiez les adresses du réseau interne du NAS et vérifiez s'il existe un conflit avec les adresses réseau du client qui posent problème.</li><li>2. Si un conflit existe, modifiez manuellement l'adresse réseau interne du NAS en conflit en utilisant le NAS Manager ou la CLI.</li></ol>

## Dépannage des configurations DNS

Description	Impossible de se connecter à la solution en cluster NAS en utilisant le nom système et/ou impossible de résoudre les noms d'hôte.
Cause	Causes probables : <ul style="list-style-type: none"><li>• Impossible d'envoyer un ping au système en utilisant le nom de domaine pleinement qualifié (FQDN).</li><li>• Impossible de se connecter au Gestionnaire NAS en utilisant le nom système.</li></ul>

Solution

1. Vérifiez que les informations IP du client sont correctement définies.
2. Vérifiez que le contrôleur de la solution en cluster NAS est configuré sur le bon serveur DNS.
3. Contactez l'administrateur de serveur DNS pour vérifier la création de l'enregistrement DNS.

## Détermination de l'IQN des contrôleurs de la solution en cluster NAS à l'aide de la CLI

Description

Détermination de l'IQN des contrôleurs de la solution en cluster NAS à l'aide de la CLI.

Solution

À l'aide d'un client ssh et de la VIP de gestion du NAS, connectez-vous à la CLI de solution en cluster NAS en tant qu'administrateur.

Entrez la commande suivante dans la ligne de commande suivante :

```
system maintenance luns iscsi-  
configuration view
```

## Dépannage des messages d'avertissement pour pause du RX et du TX

Description

Les messages d'avertissement suivants peuvent s'afficher lorsque le NAS Manager signale que la connectivité n'est pas à l'état optimal :

```
Rx_pause for eth(x) sur le nœud 1 est  
désactivé.
```

```
Tx_pause for eth(x) sur le nœud 1 est  
désactivé.
```

Cause

Le contrôle de flux n'est pas activé sur le(s) commutateur(s) connecté(s) au contrôleur de la solution en cluster NAS.

Solution

Consultez la documentation du fournisseur du commutateur pour activer le contrôle de flux sur le(s) commutateur(s).

## Dépannage des problèmes du NAS Manager

### Le tableau de bord du NAS est retardé

Description

Les métriques du tableau de bord du NAS sont retardées et n'indiquent pas immédiatement les valeurs mises à jour.

Cause

La vue du NAS Manager est actualisée toutes les 40 secondes, mais les informations relatives aux métriques spécifiques sont collectées à des intervalles différents, de sorte qu'il n'existe pas de corrélation entre l'actualisation de l'écran et celle des métriques.

Solution

Utilisez le processus de DSFS qui collecte les informations relatives à différentes matrices du système.

- Champs d'état (état général, état de service, état des serveurs) : les informations sont collectées toutes les 40 secondes.
- Capacité : les informations sont collectées toutes les 1 800 secondes.
- Performances actuelles (NFS, CIFS, Réplication, NDMP, Réseau) : les informations sont collectées toutes les 40 secondes.
- Performances récentes (graphique) : les informations sont collectées toutes les 60 secondes.
- Équilibrage de charge (UC, nombre de connexions) : les informations sont collectées toutes les 40 secondes.

## L'heure du système NAS n'est pas correcte

Description

Les tâches planifiées s'exécutent au mauvais moment. La date/heure des messages du journal des événements est erronée.

Cause

- L'heure du système NAS n'est pas correctement réglée.
- Aucun serveur NTP n'est défini pour le système NAS.
- Le serveur NTP utilisé par la solution en cluster NAS est à l'arrêt ou ne fournit plus les services NTP.
- Des problèmes surviennent sur le réseau lors de la communication avec le serveur NTP.

Solution

1. Identifiez le serveur NTP NAS dans la page **System Configuration/ Time Configuration (Configuration système/Configuration horaire)**. Enregistrez le ou les noms d'hôtes ou la ou les adresses IP pour disposer de plus d'informations.
2. Si aucun serveur NTP n'est défini, définissez-en un. Il est recommandé de synchroniser l'horloge du système NAS avec le serveur NTP utilisé par le ADDC (Contrôleur de domaine Active Directory). Ceci empêche la survenue d'une différence d'heures et de problèmes d'authentification éventuels. Dans la plupart des cas, l'ADDC est également le serveur NTP.
3. Vérifiez que le serveur NTP est en fonctionnement et fournit le service NTP.
4. Vérifiez le chemin de réseau entre le système NAS et le serveur NTP en envoyant un ping, par exemple. Vérifiez que le temps de réponse se trouve dans la plage des millisecondes.

## Impossible de se connecter au NAS Manager.

Description	Connexion impossible au NAS Manager.
Cause	Causes probables : <ul style="list-style-type: none"><li>• L'utilisateur tente de se connecter en utilisant une adresse IP incorrecte ou un nom de système erroné.</li><li>• Les informations IP de l'ordinateur du client ne sont pas configurées correctement.</li><li>• L'utilisateur a fourni un nom d'utilisateur ou un mot de passe incorrect.</li><li>• Les propriétés du navigateur de l'utilisateur empêchent la connexion.</li></ul>
Solution	<ol style="list-style-type: none"><li>1. Vérifiez que les informations IP du client sont correctement définies.</li><li>2. Vérifiez que les informations DNS sont correctement configurées.</li><li>3. Vérifiez le nom d'utilisateur et le mot de passe.</li><li>4. Vérifiez les paramètres du proxy dans les paramètres du navigateur.</li><li>5. Si vous utilisez Microsoft Windows Server 2008, désactivez IE ESC.</li></ol>

## Écran de connexion vide

Description	Impossible de se connecter au NAS Manager et l'écran de connexion est vide.
Cause	Causes probables : <ul style="list-style-type: none"><li>• Java script est désactivé.</li><li>• IE SEC est activé.</li></ul>
Solution	<ul style="list-style-type: none"><li>• Si Java script est désactivé, activez-le. Pour en savoir plus sur l'activation de Java script, consultez la rubrique d'aide du navigateur.</li><li>• Si IE SEC est activé, désactivez-le.</li></ul>

# Dépannage des problèmes de sauvegarde

## Dépannage des instantanés

Description	La création et la suppression d'instantanés échouent.
Cause	<p>Causes probables :</p> <ul style="list-style-type: none"><li>• De nombreuses demandes d'E/S de clients sont en attente, y compris une demande de suppression d'un répertoire volumineux.</li><li>• De nombreuses demandes de création/suppression d'instantanés sont en cours de traitement.</li><li>• Une autre demande d'instantané pour le volume est en cours d'exécution.</li><li>• Le nombre total d'instantanés a atteint la limite du système.</li><li>• Une adresse IP erronée a été fournie pour la tâche de sauvegarde.</li></ul>
Solution	<ul style="list-style-type: none"><li>• En cas d'échec d'une demande manuelle, réessayez de créer ou de supprimer l'instantané au bout d'une ou deux minutes.</li><li>• Si la demande provenait du planificateur d'instantanés, patientez un ou deux cycles de plus. Si l'échec persiste, tentez de prendre ou supprimer un instantané manuellement sur le même volume.</li><li>• Consultez le tableau de bord pour vérifier si la charge de travail est importante. Si c'est le cas, attendez jusqu'à ce qu'elle diminue, puis émettez de nouveau la demande d'instantané.</li><li>• Vérifiez la planification d'instantanés. Une planification d'instantanés très dense impacte négativement l'ensemble des performances du système. Le taux cumulé d'instantanés ne doit pas dépasser 20 instantanés par heure par système.</li><li>• Vérifiez le nombre total d'instantanés du système. Si celui-ci se trouve au-dessus de mille, supprimez-en quelques uns, puis réessayez.</li><li>• Assurez-vous que l'adresse IP virtuelle du client est fournie dans la tâche de sauvegarde.</li></ul>

## Dépannage d'une erreur interne du NDMP

Description	Sauvegardez ou restaurez les échecs liés à une erreur interne.
Cause	Les erreurs internes du NDMP indiquent qu'un système de fichiers n'est pas accessible ou qu'un volume du NAS n'est pas disponible.

Si l'application de sauvegarde ne peut pas se connecter à une appliance NAS :

1. Connectez-vous au NAS Manager ou ouvrez un terminal distant sur l'appliance.
2. Dans le NAS Manager, rendez-vous à la page **Data Protection (Protection des données)** → **NDMP** → **NDMP Configuration (Configuration NDMP)** . Dans la CLI NAS, allez dans le menu **Data Protection NDMP Configuration**.
3. Vérifiez que NDMP est activé. Si NDMP est activé, passez à l'étape 5.
4. Dans le NAS Manager, la case **Enabled (Activé)** doit être cochée.
5. Dans la CLI du NAS, saisissez `view` et assurez-vous que **State (État)** est défini sur **Enabled (Activé)**.
6. Si NDMP n'est pas activé, activez-le.
7. Vérifiez que l'adresse IP de l'application de sauvegarde est configurée dans NDMP.
8. Sur le Gestionnaire du NAS, la liste des serveurs DMA devrait inclure l'adresse IP de l'application de sauvegarde.
9. Dans la CLI du NAS, saisissez `view` et assurez-vous que la liste des **DMA Servers (Serveurs DMA)** contient l'adresse IP de l'application DMA qui tente d'accéder au serveur NAS.

Si l'appliance de sauvegarde peut se connecter à une appliance NAS, mais ne parvient pas à s'identifier, utilisez `backup_user` comme nom d'utilisateur pour le client NDMP, tout en configurant la sauvegarde/restauration NDMP dans votre application de sauvegarde. Le mot de passe par défaut du client NDMP est **Stor@ge!**

Pour modifier le mot de passe :

1. Connectez-vous au NAS Manager ou ouvrez un terminal distant sur l'appliance.
2. Dans le NAS Manager, rendez-vous à la page **Data Protection (Protection des données)** → **NDMP** → **NDMP Configuration (Configuration NDMP)** . Dans la CLI NAS, allez dans le menu **Data Protection** → **NDMP** → **Configuration**.
3. Dans le NAS Manager, cliquez sur **Change Password (Modifier le mot de passe)**. Dans la CLI du NAS, exécutez la commande.

```
data-protection ndmp configuration
set-Password <nouveau_mot_de_passe>
```

Si l'application de sauvegarde parvient à se connecter au serveur NAS, mais qu'aucun volume n'est disponible pour la sauvegarde, vérifiez que le serveur NAS dispose de volumes NAS créés sur ce dernier.

# Dépannage des problèmes du système

## Dépannage d'un arrêt du système

Description	Au cours d'un arrêt du système à l'aide du Gestionnaire du NAS, ni le système ni les contrôleurs ne s'arrêtent au bout de 20 minutes.
Cause	<p>La procédure d'arrêt du système se compose de deux processus distincts :</p> <ul style="list-style-type: none"><li>• Arrêt du système de fichiers</li><li>• Mise hors tension des contrôleurs de la solution en cluster NAS.</li></ul> <p>Le système de fichiers peut mettre un certain temps à nettoyer la mémoire cache vers le stockage, soit sous l'effet d'une quantité importante de données, soit en raison d'une connexion intermittente au stockage.</p> <p>Au cours de la phase de mise hors tension, le problème peut être lié à une attente du système d'exploitation/ noyau sur le contrôleur ou à une absence de synchronisation de son état avec le disque local.</p>
Solution	<p>Si le système de fichiers s'est arrêté et si l'un des contrôleurs est toujours actif, vous pouvez mettre manuellement le contrôleur hors tension à l'aide du bouton d'alimentation.</p> <p>Si le système de fichiers n'est pas arrêté, ne l'arrêtez pas. Il subit un délai d'attente de 10 minutes, vide son cache sur les contrôleurs locaux, puis poursuit le processus d'arrêt.</p>

## Violation de sécurité du conteneur NAS

Description	Violation de sécurité du conteneur NAS.
Cause	<p>Le style de sécurité que vous choisissez pour un conteneur NAS détermine le protocole dominant à utiliser pour la définition des autorisations sur les fichiers de ce volume. Le style de sécurité UNIX signifie le protocole NFS, et le style de sécurité NTFS signifie le protocole CIFS.</p> <p>Par conséquent, certaines situations ne sont plus valides :</p> <ul style="list-style-type: none"><li>• Définition des autorisations UNIX pour un fichier situé dans un conteneur de style de sécurité NTFS.</li><li>• Définition de la propriété des UID/GID pour un fichier situé dans un conteneur de style de sécurité NTFS.</li><li>• Définition de la ACL pour un fichier situé dans un conteneur de style de sécurité UNIX.</li><li>• Modification de l'indicateur en lecture seule pour un fichier situé dans un conteneur de style de sécurité UNIX.</li></ul>

- Définition de la propriété des SID/GSID pour un fichier situé dans un conteneur de style de sécurité UNIX.

Le style de sécurité du conteneur NAS doit refléter le protocole principal utilisé pour accéder à ses fichiers.

Solution

Si un utilisateur est souvent amené à procéder à une activité liée à la sécurité inter-protocoles, divisez les données en deux conteneurs NAS distincts en fonction du protocole d'accès principal.

## Plusieurs erreurs reçues lors du formatage du système de fichiers

Description

Vous recevez plusieurs messages d'erreur au cours du formatage d'un système de fichiers.

Cause

Causes probables :

- Des adresses IP SAN erronées sont utilisées dans l'utilitaire Dell NAS Initial Deployment Utility (IDU).
- Des numéros IQN erronés ont été utilisés lors de la définition des hôtes dans le MSDM.
- Un nombre impair de LUN est adressé sur le groupe hôte.
- La taille des LUN est inférieure à la taille minimum requise.
- Nombre inférieur au minimum de LUN requis.

Solution

Si des adresses IP de SAN erronées sont utilisées lors de l'exécution de l'utilitaire IDU NAS :

1. Vérifiez que l'adresse IP de détection MD utilisée lors de l'exécution de l'IDU NAS se trouve sur le même sous-réseau que l'une des deux adresses IP de SAN configurées sur vos contrôleurs.
2. Pour vérifier l'adresse IP de détection MD, connectez-vous à votre IP NAS Manager à l'aide de la CLI et exécutez la commande suivante :  

```
system
maintenance luns configuration
iscsi-view
```

Cette commande affiche l'adresse IP de détection MD.

Si cette adresse IP ne se trouve pas sur le même sous-réseau que les adresses IP configurées pour votre SAN, remplacez l'adresse IP de détection MD par l'un des sous-réseaux définis sur le SAN A et B de votre contrôleur.

Si des numéros IQN erronés sont utilisés lors de la définition des hôtes dans MDSM, vérifiez que les IQN affichés dans MDSM correspondent aux IQN du contrôleur.

Pour modifier l'adresse IP de détection dans la CLI, exécutez la commande suivante :

```
system maintenance luns configuration
iscsi-set -iSCSIDiscoveryIPs <Adresse
IP> none none
```

Une fois la commande terminée, actualisez les identificateurs de port hôte. Vous pouvez maintenant

exécuter l'Assistant Configuration depuis le NAS Manager.

1. Vérifiez si les IQN affichés dans MDSM sont les mêmes que ceux qui figurent sous l'onglet **Mappings** (Adressages) de la section hôtes du NAS Manager.
2. Si une non correspondance existe, corrigez les numéros IQN utilisés pour les hôtes dans MDSM, puis tentez de formater le système. Les LUN doivent être détectés et formatés.

Si le problème est lié à un nombre impair de LUN :

1. Si une erreur survient, vérifiez qu'un nombre pair de LUN sont adressés au groupe d'hôtes. Les nombres impairs ne sont pas pris en charge. Les LUN doivent évoluer en paires, de 2 à 16.
2. Si un nombre impair de LUN est utilisé, corrigez ce nombre en ajoutant ou en supprimant un LUN.
3. Essayez de formater le système.

Si la taille des LUN est inférieure aux exigences minimales :

1. Vérifiez que les LUN dépassent la taille minimale requise de 125 Go.
2. Si les LUN font moins de 125 Go, modifiez la taille des LUN de sorte qu'elle atteigne ou dépasse la taille minimale requise.
3. Essayez de formater le système.

Si le nombre de LUN est inférieur aux exigences minimales :

1. Vérifiez que plus d'un LUN est adressé au groupe d'hôtes. Le nombre de LUN minimal requis est 2.
2. Si le nombre de LUN est inférieur à 2, ajoutez des LUN pour atteindre le nombre minimum de 2.
3. Essayez de formater le système.

## Association des noms de LUN à des disques virtuels


Description	Identification des LUN du NAS Manager qui sont des disques virtuels dans MDSM (Modular Disk Storage Manager).
Solution	Ouvrez l'interface Web du NAS Manager et allez à <b>Cluster Management (Gestion des clusters)</b> → <b>Maintenance</b> → <b>Add Luns (Ajouter des LUN)</b> . Cette page affiche tous les LUN auxquels la solution en cluster NAS a accès (attribués au groupe d'hôtes de la solution en cluster NAS). Chaque LUN peut être identifié à l'aide de son nom universel. Dans l'interface Web du NAS Manager, le nom universel du LUN est doté d'un préfixe.  Ouvrez MDSM et allez dans l'onglet <b>Logical (Logique)</b> , puis cliquez sur <b>Virtual Disk (Disque virtuel)</b> . L'identificateur de nom universel du disque virtuel s'affiche dans le volet <b>Properties (Propriétés)</b> . Cette

solution de contournement vous permet de déterminer quels disques virtuels sont attribués au système de fichiers NAS.

## L'utilitaire NAS IDU n'est pas parvenu à détecter d'autres contrôleurs

Description	L'utilitaire NAS IDU n'est pas parvenu à détecter d'autres contrôleurs.
Cause	Il est possible qu'IPv6 soit désactivé sur votre station de travail.
Solution	Activez la prise en charge IPv6 sur votre station de travail de gestion.

## Échec de l'opération de connexion


Description	L'opération de connexion du contrôleur au cluster NAS a échoué.
Solution	<ul style="list-style-type: none"><li>• Connectez un clavier et moniteur au contrôleur ayant échoué la connexion et affichez le message d'erreur connexe pour déterminer la cause de l'échec.</li><li>• Vérifiez les points suivants :<ul style="list-style-type: none"><li>– Lorsque le contrôleur était déconnecté, l'adresse IP qui lui était attribuée sur le réseau client n'était attribuée à aucun autre hôte. Lorsque le contrôleur est déconnecté, il perd son identité, notamment des adresses IP. Lorsqu'il est connecté, son identité est à nouveau appliquée, y compris ses adresses IP.</li><li>– Vérifiez que la passerelle par défaut de trouve dans le sous-réseau <b>Primary</b> (Principal) à l'aide du NAS Manager. Affichez la passerelle par défaut en allant sous <b>Cluster Management</b> → <b>Network Configuration</b> (Gestion de clusters &gt; Configuration réseau). Allez dans <b>Cluster Management</b> → <b>Subnets</b> (Gestion de clusters &gt; Sous-réseaux) pour afficher le sous-réseau <b>Primary</b> sur le réseau client. Si la passerelle par défaut ne se trouve pas dans le sous-réseau <b>Primary</b>, modifiez-la. Pour que l'opération de connexion réussisse, la passerelle par défaut doit être <b>pingable</b> (pouvant être interrogée par une commande ping).</li></ul></li><li>• Suite à l'échec de l'opération de connexion, le contrôleur doit être réinitialisé manuellement sur le mode Veille. Pour ce faire, connectez un clavier et un moniteur au contrôleur avec lequel la connexion a échoué, puis appuyez sur la touche d'identification système. , tel qu'indiqué dans les instructions à l'écran.</li></ul>

## Le contrôleur prend beaucoup de temps à s'amorcer suite à la mise à niveau du Service Pack

Description	Le contrôleur prend beaucoup de temps à s'amorcer suite à la mise à niveau du service pack du micrologiciel du contrôleur.
Solution	<ul style="list-style-type: none"><li>• Connectez un clavier et un moniteur au contrôleur qui prend beaucoup de temps à s'amorcer.</li><li>• Si le système est en cours d'amorçage, lors de la phase d'amorçage, laissez les mises à niveau se terminer. Ceci peut prendre jusqu'à 60 minutes.</li><li>• Ne réamorcez pas le contrôleur manuellement si celui-ci se trouve en phase d'amorçage <b>Executing System Upgrades (Mises à niveau système en cours d'exécution)</b>.</li></ul>

## Dépannage des problèmes de l'utilitaire IDU (utilitaire de déploiement initial) NAS

### Erreur reçue pendant l'exécution de l'utilitaire Dell NAS Initial Deployment Utility

Description	Une erreur est survenue pendant l'exécution de l'utilitaire Dell NAS Initial Deployment Utility (utilitaire de déploiement initial NAS Dell ou IDU)
Cause	Cette erreur peut être provoquée par la configuration matérielle, la configuration des commutateurs du réseau ou les configurations des systèmes de cluster.
Solution	<p>Si la page de découverte affiche un échec de connexion :</p> <ol style="list-style-type: none"><li>1. Vérifiez que la station de gestion exécutant l'utilitaire <b>NAS IDU (IDU NAS)</b> est dotée d'une connexion réseau au commutateur client du cluster NAS.  <b>REMARQUE</b> : Aucun routeur ne doit être connecté aux contrôleurs NAS, ni aux systèmes exécutant NAS IDU.</li><li>2. Vérifiez si IPv6 est activé sur la station de gestion sur laquelle l'utilitaire de configuration du NAS s'exécute.</li><li>3. Connectez un clavier USB, surveillez les contrôleurs du cluster NAS et vérifiez qu'aucun message répété sur lequel apparaît l'adresse MAC des contrôleurs n'apparaisse, indiquant <b>Press "i" -re-install standby node (Appuyer sur « i » - re-installer le nœud de secours)</b>.</li></ol> <p>Si l'échec se situe dans la page de configuration du cluster NAS :</p> <ol style="list-style-type: none"><li>1. Effectuez une capture d'écran du message d'erreur apparaissant dans la fenêtre de l'utilitaire NAS IDU au cours de la mise en cluster.</li><li>2. Récupérez le fichier de configuration des clusters, le fichier journal de l'utilitaire NAS IDU et le fichier</li></ol>

résultant provenant du répertoire d'installation, puis compressez le dossier de configuration à partir du répertoire d'installation.


3. L'utilitaire NAS IDU doit inviter les utilisateurs à restaurer la fenêtre, dans laquelle les nœuds sont restaurés en mode Veille.
4. Recherchez les messages d'erreur dans les captures d'écran et déterminez la cause probable de l'erreur. Corrigez ces erreurs et reconfigurez le système à l'aide de l'utilitaire NAS IDU.
5. Si l'échec persiste, rassemblez tous les fichiers dans un paquet groupé et contactez le Support Dell.

## Impossible de lancer l'utilitaire IDU NAS Dell

Description	Impossible de lancer l'utilitaire IDU (Utilitaire de déploiement initial) NAS Dell
Cause	Causes probables : <ul style="list-style-type: none"><li>• Le programme d'installation de l'IDU n'est pas parvenu à réaliser l'installation.</li><li>• L'environnement d'exécution JAVA n'est pas correctement installé.</li></ul>
Solution	Procédez comme suit : <ul style="list-style-type: none"><li>• Vérifiez si le programme d'installation de l'utilitaire IDU NAS s'est exécuté correctement.</li><li>• Vérifiez si la version minimale JRE1.6x est installée correctement.</li><li>• Sous Microsoft Windows, exécutez <code>java -version</code> à partir de la console de commande pour afficher une version valide du JRE.</li></ul>


## Maintenance de la solution en cluster NAS

Ce chapitre fournit des informations sur l'arrêt et la mise sous tension du système en cas d'arrêt planifié ou de déplacement du système sur un autre emplacement. Ce chapitre présente également la procédure de mise à niveau du logiciel et l'exécution des diagnostics.

 **REMARQUE** : Voir le *Dell FluidFS NAS Solutions Owner's Manual* (Manuel du propriétaire du matériel Dell FluidFS NAS) à l'adresse [dell.com/support](http://dell.com/support) pour plus d'informations sur la réparation et la maintenance du matériel.


### Arrêt de la solution en cluster NAS

 **PRÉCAUTION** : Suivez strictement la procédure pour éviter toute incohérence des données.

 **REMARQUE** : Cette procédure arrête les deux contrôleurs.

Pour arrêter le système :

1. Ouvrez un navigateur Web et connectez-vous à l'adresse IP virtuelle (VIP) de gestion NAS qui a été configurée pendant la procédure d'installation.
2. Dans le NAS Manager, sélectionnez **Cluster Management (Gestion des clusters)** → **Maintenance** → **System Stop/Start (Arrêt/Démarrage du système)**.  
La page **System Stop/Start** affiche l'état du système.
3. Dans la liste **System action to perform** (Action système à effectuer), sélectionnez **Stop** (Arrêter).
4. Cliquez sur **Suivant**.
5. Lorsque vous êtes invité à confirmer la procédure d'arrêt, cliquez sur **OK**.  
Cette opération copie le cache du système de fichiers sur les disques et arrête le système de fichiers.
6. Appuyez et relâchez le bouton d'alimentation creux situé à l'arrière de chaque contrôleur pour arrêter le contrôleur.

 **REMARQUE** : Le fait de maintenir enfoncé le bouton d'alimentation pendant quelques secondes ne mettra pas le système hors tension.

### Mise sous tension de la solution en cluster NAS

Avant de démarrer le système, assurez-vous que tous les câbles sont connectés entre les contrôleurs du rack et que les composants sont connectés à l'alimentation électrique de l'installation.

Mettez les composants sous tension dans l'ordre suivant :

1. Matrices de stockage
  - Démarrez toutes les matrices de stockage en appuyant sur les interrupteurs MARCHE/ARRÊT sur les deux blocs d'alimentation situés à l'arrière des unités.
  - Patientez pendant la mise sous tension des bloc d'alimentation, contrôleurs et disques LED.
2. Solution de cluster NAS :  
Pour démarrer les contrôleurs, connectez chaque contrôleur ou appliance NAS à une source d'alimentation.

3. Dans le NAS Manager, sélectionnez **Cluster Management (Gestion des clusters)** → **Maintenance** → **System Stop/Start (Arrêt/Démarrage du système)**.  
La page **System Stop/Start** affiche l'état du système.
4. Dans la liste **System action to perform (Action système à effectuer)**, sélectionnez **Start (Démarrer)**.
5. Cliquez sur **Suivant**.


## Restauration de la configuration du volume NAS

Restaurer la configuration des volumes NAS est une méthode effective que l'administrateur système peut utiliser pour restaurer tous les paramètres de volume NAS (exportations, partages, planification d'instantanés, stratégies de quota, et ainsi de suite) sans devoir les reconfigurer manuellement. Cette méthode est particulièrement utile après la création d'un nouveau volume NAS, la nouvelle installation du système ou la restauration d'un système.

Un volume NAS peut être restauré en configurant un volume NAS (même s'il s'agit uniquement d'une configuration enregistrée) sur un autre volume NAS dans le même système ou un système différent. L'administrateur doit copier la configuration sur le volume NAS depuis sa sauvegarde ou un autre volume NAS.

Lorsqu'une modification est apportée à la configuration du volume, la configuration est automatiquement enregistrée dans un format qui vous permet de la restaurer ultérieurement. La configuration est stockée dans le dossier **.clusterConfig**, lequel se trouve dans le dossier racine du volume NAS.


Ce dossier peut être sauvegardé, individuellement ou avec les données utilisateur du volume, puis restauré ultérieurement. Pour que la configuration stockée dans le dossier prenne effet, l'administrateur doit d'abord copier le dossier **.clusterConfig** à restaurer sur le volume NAS puis se rendre dans l'écran **Restore NAS Volume Configuration** (Restaurer la configuration du volume NAS) pour appliquer la configuration au volume NAS.

 **REMARQUE** : Lorsque vous restaurez la configuration d'un volume NAS, celle-ci écrase et remplace la configuration existante. Les utilisateurs actuellement connectés au système sont également déconnectés.

Vous pouvez restaurer les paramètres suivants :

- Exportations NFS
- Partages CIFS
- Stratégies de quota
- Planification d'instantanés
- Paramètres d'alerte, de style de sécurité et paramètres connexes du volume NAS
- Nom du volume NAS
- Taille du volume NAS

Pour restaurer une configuration de volume NAS :

 **REMARQUE** : Lorsque vous utilisez la sauvegarde d'un autre système, l'opération de restauration fonctionne uniquement si la configuration enregistrée provient d'un système utilisant la même version logicielle.

1. Sélectionnez **Cluster Management (Gestion des cluster)** → **Maintenance** → **Restore NAS Volume Configuration (Restaurer la configuration du volume NAS)**.  
La page **Restore NAS Volume Configuration** s'affiche.
2. Dans la liste **Update the configuration of (Mettre à jour la configuration de)**, sélectionnez le système dont vous souhaitez mettre la configuration à jour.
3. Dans la liste **Configuration taken from system (Configuration provient du système)**, sélectionnez le cluster source pour obtenir des informations sur la configuration.
4. Sélectionnez une option ou plus dans la liste des paramètres système pouvant être restaurés.
5. Cliquez sur **Appliquer**.


## Restauration de la configuration du cluster

Restaurer la configuration système est une méthode efficace pour restaurer la plupart des paramètres du système automatiquement (comme la configuration de protocoles et les utilisateurs et groupes locaux). Ceci peut s'avérer utile après une mise à niveau d'un système doté d'une nouvelle version du logiciel, après une installation récente du système ou après une restauration d'un système.

La configuration système peut être restaurée en restaurant sur le système actuel la configuration stockée sur le volume NAS le plus récemment mis à jour dans le cluster. Vous devez copier la configuration depuis sa sauvegarde ou tout autre système sur le volume NAS.

Dès qu'une modification est apportée à la configuration du système, la configuration est automatiquement enregistrée dans un format qui vous permet de la restaurer ultérieurement. La configuration est stockée dans le dossier **.clusterConfig**, situé dans tous les dossiers racines du volume NAS.

Vous pouvez effectuer une sauvegarde de ce dossier, individuellement ou avec les données utilisateur présentes sur le volume, afin de pouvoir le restaurer ultérieurement. Pour que la configuration stockée dans le dossier prenne effet, l'administrateur doit d'abord copier le dossier **.clusterConfig** sur un des volumes NAS du système, puis appliquer la configuration au système.

 **REMARQUE** : Lorsque vous restaurez une configuration système, celle-ci écrase et remplace la configuration existante. Les utilisateurs actuellement connectés au système sont également déconnectés.

Vous pouvez restaurer les paramètres suivants :


- Configuration des protocoles
- Utilisateurs et groupes
- Adressages utilisateurs
- Configuration de la surveillance
- Configuration horaire
- Hôtes antivirus

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Maintenance** → **Restore Cluster Configuration (Restaurer la configuration du cluster)**.

La page **Restore Cluster Configuration** s'affiche.

2. Dans la liste **Configuration taken from system (Configuration prise du système)**, sélectionnez le système dont vous souhaitez mettre la configuration à jour.
3. Sélectionnez une option ou plus dans la liste des paramètres système pouvant être restaurés.
4. Cliquez sur **Apply (Appliquer)**.

## Formatage du système de fichiers


 **REMARQUE** : Seuls les systèmes NX3600 et NX3610 prennent en charge de formatage de systèmes de fichiers à l'aide du **NAS Manager**. Pour FS8600, **File System Format (Formatage du système de fichiers)** est réalisé par **Enterprise Manager** lors du déploiement initial du système FS8600 à l'aide de **Enterprise Manager**.

Un formatage de système de fichiers installe le système de fichiers sur les LUN adressés au NAS. Le formatage efface toutes les données existantes des LUN. Un formatage de système de fichiers doit se produire avant qu'un volume NAS puisse être créé. Ce formatage de système de fichiers est généralement un événement unique, à moins que le NAS ne soit à nouveau déployé et que les données existantes ne soient plus nécessaires.

Pour formater le système de fichiers, sélectionnez **Cluster Management (Gestion des clusters)** → **Maintenance** → **File System Format** et cliquez sur **Format (Formater)**.

# Installation du service-pack

La solution en cluster NAS utilise une méthodologie de servicepack pour la mise à niveau à une version ultérieure du logiciel.


 **REMARQUE** : Pour mettre à jour votre système à l'aide du service pack le plus récent, voir [dell.com/support](http://dell.com/support).

## Mise à niveau du Service Pack à l'aide du NAS Manager

Les Service Packs gardent votre solution NAS Dell FluidFS à jour en termes de micrologiciel et de logiciel. Consultez le site [dell.com/support](http://dell.com/support) et téléchargez les derniers Service Packs pour assurer le bon fonctionnement de votre système.

 **PRÉCAUTION** : Si vous effectuez une mise à niveau du logiciel de la solution NAS de la version 1.x à la version 2.x, utilisez le service pack avec le format de nom de fichier DellIFS-2.0.xxxx-SP.sh. Si vous effectuez une mise à niveau du logiciel de la solution NAS de la version 2.0 et versions ultérieures, utilisez le service pack avec le format de nom de fichier DellFluidFS-2.0.xxxx-SP.sh.

 **PRÉCAUTION** : Ne modifiez pas le nom de fichier du service pack.

 **PRÉCAUTION** : L'installation d'un service pack entraîne le redémarrage des contrôleurs NAS pendant le processus d'installation, ce qui peut engendrer des interruptions avec les connexions clients. Il est donc recommandé d'effectuer les installations de service packs au cours des périodes de maintenance planifiées.

 **PRÉCAUTION** : Le processus d'installation des service packs est irréversible. Une fois mis à jour, votre système ne peut pas revenir à une version précédente.

Pour installer un service pack :

1. Téléchargez le service-pack depuis le site [dell.com/support/downloads](http://dell.com/support/downloads).
2. Dans le NAS Manager, sélectionnez **Cluster Management (Gestion des clusters)** → **Maintenance** → **Service Pack** . La page **Service Pack** s'affiche.
3. Cliquez sur **Parcourir**.
4. Naviguez jusqu'au service pack le plus récent, puis cliquez sur **Open (Ouvrir)**.
5. Cliquez sur **Upload (Téléverser)**.
6. Une fois le fichier service pack téléversé sur le système, cliquez sur **Install** (Installer).


## Extension de la capacité de stockage du cluster NAS

### Extension du pool NAS sur la solution NAS Dell PowerVault NX3500/NX3600/NX3610

Vous pouvez étendre la capacité de stockage de votre système sans affecter les services vers les clients. Cependant, le processus prend un certain temps selon le nombre total de LUN existants et ajoutés, la capacité de stockage totale et la charge de traitement du système. Vous pouvez ajouter des LUN supplémentaires à la solution en cluster NAS depuis la capacité de stockage déjà disponible de votre matrice de stockage.


La matrice de stockage MD doit disposer d'une capacité supplémentaire à attribuer à la solution de stockage NAS. Pour en savoir plus sur l'extension du groupe de disques et du disque virtuel, consultez le Modular Disk Storage Manager Administrator's Guide (Guide de l'administrateur du Gestionnaire de stockage de disques modulaires) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).


Pour étendre la capacité de stockage de la solution en cluster NAS :

1. Lancez le **NAS Manager** sur votre station de gestion et connectez-vous en tant qu'**admin**.  
 **REMARQUE** : Par défaut, le mot de passe admin est **Stor@ge!**.
2. Sélectionnez **Cluster Management (Gestion des clusters)** → **Maintenance** → **Expand Luns (Étendre les LUN)**.  
La page **Expand Luns** s'affiche.
3. Cliquez sur **Expand Luns** dans le coin inférieur droit de la page.  
La page **Status (État)** s'affiche et indique l'avancement de l'opération d'extension des LUN.
4. Cliquez sur **Terminer**.

## Extension du pool NAS sur la solution NAS FS8600


1. Connectez-vous au client **Enterprise Manager**.
2. Cliquez sur **Storage (Stockage)** situé dans le volet gauche.
3. Cliquez sur **Expand NAS Pool (Étendre le pool NAS)** dans le menu supérieur.
4. Saisissez la taille du pool NAS.


 **REMARQUE** : Chaque Storage Center (centre de stockage) est limité à 512 To. Les pools NAS peuvent uniquement être étendus, leur réduction étant interdite.

 **REMARQUE** : Le pool NAS peut également être étendu en ajoutant un deuxième Storage Center. Pour en savoir plus sur l'ajout d'une matrice Storage Center au cluster FluidFS, consultez le *Enterprise Manager Administrator's Guide (Guide de l'administrateur d'Enterprise Manager)*.


## Ajout de LUN à la solution en cluster NAS PowerVault NX3500/NX3600/NX3610

Pour cette procédure, la matrice de stockage MD doit disposer d'une capacité supplémentaire à allouer à la solution en cluster NAS. Pour en savoir plus sur l'extension du groupe de disques et du disque virtuel sur la matrice MD, consultez le MD Series Storage Array Administrator's Guide (Guide de l'administrateur de la matrice de stockage MD Series) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).


 **AVERTISSEMENT** : FluidFS prend en charge un maximum de 32 LUN d'une taille maximale de 32 To chacun, cependant cette limite peut être dépassée avec MDSM. Si vous dépassez cette limite, il est possible que vous subissiez des problèmes de performances et/ou d'accès.

 **REMARQUE** : Il est recommandé d'utiliser moins de LUN de taille supérieure au lieu d'utiliser un nombre plus important de LUN plus petits. Si possible, étendez la taille du pool NAS en étendant la taille des LUN existants.

1. Sous MDSM, créez des disques virtuels supplémentaires en paires.

 **REMARQUE** : Pour en savoir plus, consultez le MD Series Storage Array Administrator's Guide (Guide de l'administrateur de la matrice de stockage MD Series) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).

2. Ajoutez les disques virtuels que vous venez de créer au **Host Group (Groupe d'hôtes)** du cluster.
3. Lancez le **NAS Manager** sur votre station de gestion et connectez-vous en tant qu'**admin**.

 **REMARQUE** : Par défaut, le mot de passe admin est **Stor@ge!**.

4. Sélectionnez **Cluster Management (Gestion des clusters)** → **Maintenance** → **Add Luns (Ajouter des LUN)**.

La page peut prendre quelques minutes à s'afficher. Elle exécute la découverte iSCSI pour tous les disques virtuels/LUN attribués à la solution de cluster NAS.

Chaque LUN peut être identifié à l'aide de son nom universel. Dans le NAS Manager, le nom universel d'un LUN est précédé par Dell FluidFS. La combinaison unique de chiffres et de caractères suivant ce préfixe constitue le nom universel.

La page **Add Luns (Ajouter des LUN)** s'affiche.

5. Cliquez sur **Add LUNs** pour ajouter de nouveaux LUN à la solution en cluster NAS. Le système formate le système de fichiers de manière incrémentielle sur les nouveaux LUN.

Le processus prend un certain temps en fonction de la taille et du nombre de LUN.

À la fin de ce processus, le nouvel espace peut être utilisé.

6. Cliquez sur **Terminer**.

## Exécution des diagnostics

Exécuter des diagnostics vous aide à dépanner les problèmes avant de demander de l'aide à Dell.

Les options de diagnostic disponibles sur votre solution sont :

- Diagnostics en ligne
- Diagnostics hors ligne

### Diagnostics en ligne

Les diagnostics en ligne peuvent être exécutés pendant que le système est en ligne et en cours de remise de données.

Les options de diagnostic suivantes sont disponibles :

- **Général**
- **Système de fichiers**
- **Mise en réseau**
- **Performance**
- **Protocoles : recueillir des journaux**
- **Protocoles : client unique**
- **Protocoles : fichier unique**

Pour exécuter l'un de ces diagnostics :

1. Sélectionnez **Cluster Management (Gestion des clusters) → Maintenance → Diagnostics**.  
La page **Diagnostics** s'affiche.
2. Dans la liste **Diagnostics type (Type de diagnostics)**, sélectionnez l'option appropriée, puis cliquez sur **Start (Démarrer)**.  
Une fois les diagnostics terminés, les liens vers les archives compressées de fichiers de diagnostic s'affichent.
3. Cliquez sur le lien approprié sous les **Download diagnostics archive files (Télécharger les fichiers d'archive de diagnostic)**.  
Un message vous invite à ouvrir ou enregistrer le fichier de diagnostics sélectionné.
4. Cliquez sur **Done (Terminé)**.

### Diagnostics hors ligne



**REMARQUE** : Branchez un clavier et un moniteur avant d'effectuer la procédure suivante.

Votre solution doit être hors ligne avant d'effectuer les diagnostics hors ligne, ce qui signifie que la production et la remise des données sont arrêtées. Ceci est généralement utile lors de dépannage de problèmes de bas niveau.

Cette procédure utilise les outils natifs Dell :

- Mémoire MP


- Dell Diagnostics

## Mémoire MP

MP Memory (Mémoire MP) est un outil de test de la mémoire MS DOS développé par Dell. Cet outil est efficace pour les configurations de mémoire importantes (supérieures à 4 Go). Il prend en charge les configurations à un ou plusieurs processeurs ainsi que les processeurs possédant la technologie Hyper-Threading (HT) d'Intel.

MP Memory fonctionne uniquement sur les contrôleurs dotés d'un processeur Intel. Cet outil complète les tests de diagnostics Dell 32 bits et aide à fournir des diagnostics exhaustifs sur le contrôleur au sein d'un environnement de système de pré-exploitation.


## Exécution des diagnostics intégrés du système


 **PRÉCAUTION** : Utilisez les diagnostics intégrés du système pour tester uniquement votre système. L'utilisation de ce programme avec d'autres systèmes peut entraîner des résultats invalides ou des messages d'erreur.


1. Connectez un clavier, un moniteur, une souris au port VGA et aux ports USB du contrôleur.
2. Pour redémarrer le contrôleur, appuyez sur le bouton d'alimentation (situé à l'arrière du contrôleur) et relâchez-le pour le mettre hors tension et effectuez la même manœuvre pour le remettre sous tension.
3. Au cours du démarrage du système, appuyez sur <F10>.
4. Utilisez les touches fléchées vers le haut et vers le bas pour sélectionner **System Utilities (Utilitaires système)** → **Launch Dell Diagnostics (Lancer les diagnostics Dell)**.  
La fenêtre **ePSA Pre-boot System Assessment (Évaluation du système au pré-amorçage ePSA)** s'affiche, répertoriant tous les périphériques détectés dans le système. Le diagnostic démarre l'exécution des tests sur tous les périphériques détectés.
5. Lorsque vous avez terminé, retirez le clavier, le moniteur et la souris du contrôleur et redémarrez le contrôleur.

## Réinstallation de la solution en cluster NAS

 **PRÉCAUTION** : Réinstaller le logiciel du cluster NAS fait revenir votre système aux valeurs par défaut définies en usine. Si vous procédez à cette réinstallation, toutes les données de la solution NAS seront supprimées.

 **REMARQUE** : Une fois la réinstallation du logiciel de la solution NAS effectuée, installez les dernières mises à jour du pack de service.

 **REMARQUE** : Branchez un clavier et un moniteur avant d'effectuer la procédure suivante.

 **REMARQUE** : Le logiciel de la solution du cluster NAS ne peut pas être installé sur un matériel non pris en charge.

Pour réinstaller le logiciel de la solution en cluster NAS :

1. Mettez le contrôleur hors tension à l'aide du bouton encastré situé à l'arrière du système.
2. Mettez le contrôleur sous tension à l'aide du bouton encastré situé à l'arrière du système.
3. Au démarrage du BIOS, appuyez sur la touche <F11> pour accéder au menu contextuel.
4. Sélectionnez **Generic Storage Device (Périphérique de stockage générique)**.
5. Dans le menu contextuel, sélectionnez **FluidFS Reinstall (Réinstallation FluidFS)**.
6. À l'invite, saisissez `resetmysystem`.  
Le logiciel lance automatiquement l'installation.
7. Une fois l'installation du logiciel terminée, le contrôleur redémarre en mode de secours.

## Extension du cluster NAS

Vous pouvez augmenter le nombre d'appliances dans un cluster NAS. L'extension du nombre d'appliances dans un cluster augmente l'ensemble des performances du cluster NAS en autorisant des connexions supplémentaires de client et en distribuant uniformément les flux de données entre les contrôleurs et le stockage principal. La paire d'appliances d'origine ne consacre plus toutes ses ressources système aux opérations du cluster NAS et réduit son utilisation des ressources système car d'autres paires d'appliances y contribuent leurs ressources.

Une appliance NAS est composée de deux contrôleurs NAS au sein d'un seul châssis. Vous pouvez ajouter un maximum d'une appliance à la fois. Selon la version de la solution en cluster NAS Dell dont vous disposez, le nombre maximal d'appliances dans une solution en cluster NAS est de quatre (total de huit contrôleurs).

- Pour le système Dell PowerVault NX3600, le nombre maximal d'appliances prises en charge est 1 (2 contrôleurs).
- Pour le système Dell PowerVault NX3610, le nombre maximal d'appliances prises en charge est 2 (4 contrôleurs).
- Pour le système Dell Compellent FS8600, le nombre maximal d'appliances prises en charge est 4 (8 contrôleurs).

L'opération d'ajout d'appliances NAS est transparente et n'interrompt aucune des opérations NAS en cours sur le cluster. Une fois les appliances ajoutées avec succès, de nouvelles connexions de client sont automatiquement distribuées sur tous les contrôleurs, assurant ainsi un équilibrage de charge efficace entre tous les contrôleurs.

## Ajout d'une appliance NAS supplémentaire au cluster NAS

Avant d'ajouter une appliance NAS supplémentaire, vérifiez les éléments suivants :

- L'appliance NAS supplémentaire est mise en rack, câblée et sous tension.
- Les numéros de service de l'appliance sont enregistrés.
- De nouvelles adresses IP sont disponibles (pour être ajoutées à l'appliance).

Pour ajouter une appliance NAS supplémentaire :

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Hardware (Matériel)** → **Add NAS Appliance Wizard (Assistant d'ajout d'appliance NAS)**.

L'Assistant **Add NAS Appliance Wizard** apparaît.


2. Cliquez sur **Suivant**.

La page **Add NAS Appliance Wizard (Scan Network for NAS Appliances) (Assistant Ajouter une appliance NAS (Balayer le réseau pour détecter des appliances NAS))** s'affiche.

3. Dans la liste **Chassis number (Numéro de châssis)**, sélectionnez l'appliance NAS que vous souhaitez ajouter au cluster NAS, puis cliquez sur **Next**.

L'Assistant **Add NAS Appliance Wizard (Subnets) (Assistant d'ajout d'appliance NAS) (Sous-réseaux)** apparaît.




4. Utilisez les adresses IP suggérées ou saisissez-en de nouvelles pour la paire de contrôleurs supplémentaire de tous les sous-réseaux requis, puis cliquez sur **Next**.

 **REMARQUE** : Lorsque vous cliquez sur **Next**, le prochain sous-réseau s'affiche jusqu'à ce que les adresses IP de tous les sous-réseaux soient saisies.

Une fois les adresses IP de tous les sous-réseaux saisies, un message s'affiche indiquant que le système est en train d'enregistrer ces adresses IP.

5. Cliquez sur **Suivant**.

La page **Add NAS Appliance Wizard (Prepare Controllers To Add Appliance) (Assistant d'ajout d'appliance NAS (Préparer les contrôleurs pour ajouter l'appliance))** s'affiche.

6. Pour valider les conditions matérielles nécessaires au processus d'extension, cliquez sur **Next**.  
La page **Add NAS Appliance Wizard (System Validation) (Assistant d'ajout d'appliance NAS (Validation du système))** s'affiche. Divers composants et paramètres sont vérifiés et l'état de chaque composant et paramètre de la nouvelle appliance NAS s'affiche.
7. Pour ignorer la validation, cliquez sur **Skip (Ignorer)**.
8. Une fois la validation terminée, cliquez sur **Rerun** (Exécuter à nouveau) pour redémarrer la validation, ou cliquez sur **Next** (Suivant).  
Si vous cliquez sur **Rerun**, le processus de validation démarre. Si vous cliquez sur **Next**, la page **Add NAS Appliance Wizard (Attach New Member) (Assistant d'ajout d'appliance NAS (Connecter un nouveau membre))** s'affiche.
9. Cliquez sur **Suivant**.  
La page **Add NAS Appliance Wizard (Controller Management) (Assistant d'ajout d'appliance NAS (Gestion des contrôleurs))** s'affiche. Les contrôleurs de l'appliance NAS nouvellement ajoutée sont connectés au cluster NAS. Une fois la connexion réussie de l'appliance NAS au cluster, la page **Add NAS Appliance Wizard (LUNs Configuration) (Assistant d'ajout d'appliance NAS (Configuration des LUN))**.
  - Les nouveaux IQN s'affichent pour les solutions PowerVault NX3500/NX3600/NX3610. Dans **Modular Data Storage Manager (MDSM)**, créez les deux nouveaux hôtes virtuels dans le groupe d'hôtes existant et associez les nouveaux IQN aux hôtes virtuels. Pour en savoir plus, voir [Creating A Host In PowerVault NX3500/NX3600/NX3610 \(Création d'un hôte dans les systèmes PowerVault NX3500/NX3600/NX3610\)](#).
    -  **REMARQUE** : Pour en savoir plus sur la création d'hôtes virtuels et les associations IQN, voir le *Modular Disk Storage Manager Administrator's Guide* (Guide de l'administrateur du Gestionnaire de stockage de disques modulaires) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).
    - Pour la solution NAS Dell Compellent FS8600, à l'exception de la **configuration des LUN**, vous pouvez également afficher la **Fibre Channel WWNs Configuration (Configuration des noms universels Fibre Channel)**.
10. Pour la solution NAS FS8600 Dell Compellent, les informations WWN des contrôleurs récemment ajoutés sont affichées dans le tableau supérieur sous FC WWNs.
  -  **REMARQUE** : Les nouvelles WWN définissent les conditions requises de zonage FC du commutateur Fibre Channel avant de poursuivre.
  -  **REMARQUE** : Ignorez l'étape suivante si vous ajoutez une appliance supplémentaire à la solution NAS Dell PowerVault NX3610.
11. Pour les solutions NAS Dell Compellent FS8600, cliquez sur **Rescan (Effectuer un nouveau balayage)**.  
Assurez-vous que les contrôleurs supplémentaires sont maintenant répertoriés dans le tableau inférieur sous **Accessible Controllers** (Contrôleurs accessibles). Si certains contrôleurs ne sont pas répertoriés, vérifiez vos connexions de stockage en cliquant sur le bouton **Verify Storage Connection** (Vérifier la connexion au stockage) dans l'**Enterprise Manager**.
12. Cliquez sur **Suivant**.  
La page **Add NAS Appliance Wizard (Add NAS Appliance) (Assistant d'ajout d'appliance NAS (Ajouter une appliance NAS))** s'affiche.
13. Cliquez sur **Suivant**.  
Un message s'affiche vous indiquant que l'extension du système est terminée et affiche le nombre d'appliances dans le cluster NAS.

## Création d'un hôte dans les systèmes PowerVault NX3500/NX3600/NX3610

Dans le cas des solutions NAS PowerVault NX3500/NX3600/NX3610, vous pouvez créer des hôtes manuellement à l'aide de MDSM (Modular Disk Storage Manager - Gestionnaire de stockage sur disques modulaires).

Pour créer un hôte dans le groupe d'hôtes que vous avez créé :

1. Effectuez un clic droit sur le groupe d'hôtes que vous avez créé.
2. Cliquez sur **Define (Définir) → Host (Hôte)**.  
L'écran **Specify Host Name (Define Host) (Spécifier le nom d'hôte (Définir l'hôte))** s'affiche.
3. Saisissez le nom du nouvel hôte dans le champ **Host name (Nom de l'hôte)**.
4. Cliquez sur **Suivant**.  
L'écran **Specify Host Port Identifiers (Define Host) (Spécifier l'identifiant de port hôte (Définir l'hôte))** s'affiche.
5. Sélectionnez l'identifiant de port hôte dans la liste **Add by selecting a known unassociated host port identifier (Effectuer l'ajout en sélectionnant un identifiant de port hôte non associé connu)**.
6. Saisissez le nom d'hôte dans **User label (Étiquette de l'utilisateur)** et ajoutez IQN à la fin de celui-ci.
7. Cliquez sur **Ajouter**.
8. Cliquez sur **Suivant**.  
L'écran **Specify Host Type (Define Host) (Spécifier le type d'hôte (Définir l'hôte))** s'affiche.
9. Sélectionnez **Linux** dans la liste **Host type (operating system) (Type d'hôte (système d'exploitation))**.
10. Cliquez sur **Suivant**.  
L'écran **Preview (Define Host) (Aperçu (Définir l'hôte))** s'affiche.
11. Cliquez sur **Terminer**.  
L'écran **Creation Successful (Define Host) (Création réussie (Définir l'hôte))** s'affiche.
12. Cliquez sur **Yes (Oui)** pour définir un autre hôte.  
Répétez les étapes 2 à 10 pour créer un autre hôte.

## Remplacement d'un contrôleur de solution en cluster NAS

Vous devez remplacer le contrôleur en cas d'échec catastrophique où le contrôleur existant ne peut pas être remis en ligne.

### Prérequis

Avant de remplacer le contrôleur, assurez-vous que :

- Vous avez un accès physique aux contrôleurs.
- Le contrôleur s'est avéré défectueux (s'il a été remplacé par un nouveau).

La procédure de remplacement d'un contrôleur comprend les actions suivantes :

- Déconnexion du contrôleur
- Retrait et remplacement du contrôleur
- Connexion d'un nouveau contrôleur

### Déconnexion du contrôleur de la solution en cluster NAS

Pour mettre le cluster en mode de journalisation, vous devez déconnecter un contrôleur pendant le remplacement de tout matériel. Cela assure la remise en service du système sans que celui-ci n'ait à subir de temps d'arrêt.

Il se peut que vous deviez débrancher le contrôleur dans les circonstances suivantes :

- Un contrôleur doit être remplacé par un nouveau contrôleur de rechange.
- L'administrateur souhaite joindre un contrôleur en cours de fonctionnement à un autre cluster (plus critique).

## Déconnexion d'un contrôleur à l'aide du NAS Manager

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Hardware (Matériel)** → **Controllers Management (Gestion des contrôleurs)**.

La page **Controllers Management** s'affiche.


2. Dans la liste des contrôleurs disponibles, sélectionnez le contrôleur approprié, puis cliquez sur **Detach (Déconnecter)**.

Le contrôleur sélectionné est déconnecté du cluster, puis mis hors tension. Cette opération prend environ 10 à 15 minutes.

## Retrait et remplacement d'un contrôleur de solution en cluster NAS

Pour retirer et remplacer un contrôleur de solution de cluster NAS :

1. Étiquetez les câbles correctement avant de les déconnecter.
2. Débranchez tous les câbles de l'arrière du contrôleur.
3. Retirez le contrôleur en échec du châssis de l'appliance.
4. Installez le nouveau contrôleur dans le châssis de l'appliance.
5. Connectez tous les câbles au nouveau contrôleur.

 **REMARQUE** : Pour en savoir plus sur le retrait et l'installation du contrôleur, consultez le *Dell FluidFS NAS Solution Owner's Manual* (Manuel du propriétaire de la solution NAS Dell FluidFS) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).

6. Assurez-vous que les câbles sont reconnectés aux mêmes ports lors de l'installation du contrôleur.
7. Mettez le nouveau système sous tension en branchant le câble d'alimentation.

## Connexion d'un contrôleur à l'aide du NAS Manager


Avant de terminer cette procédure, vérifiez que le contrôleur que vous connectez se trouve en mode Veille et est sous tension. Pour ce faire, vérifiez que le voyant d'alimentation du nouveau contrôleur clignote bien vert, avec environ deux clignotements par seconde.


### Connexion d'un contrôleur à l'aide du NAS Manager

1. Sélectionnez **Cluster Management (Gestion des clusters)** → **Hardware (Matériel)** → **Controllers Management (Gestion des contrôleurs)**.


La page **Controllers Management** s'affiche.

2. Dans la liste des contrôleurs disponibles, sélectionnez le contrôleur approprié, puis cliquez sur **Attach (Connecter)**.

 **REMARQUE** : Les étapes suivantes sont requises pour les solutions NAS Dell Compellent FS8600.

 **REMARQUE** : Le zonage de structure doit être mis à jour manuellement sur le commutateur de fibre optique.

3. Une fois l'opération de connexion terminée, le NAS Manager affiche le nom universel du contrôleur nouvellement connecté, pour le zonage du commutateur Fibre Channel.

 **REMARQUE** : Pour afficher les noms universels à tout moment à l'aide de la CLI, exécutez la commande suivante :

```
system maintenance Luns configuration Fc-view
```

## Fonctionnalités du NAS Manager en mode dégradé

Lorsque l'apppliance NAS est en mode dégradé, l'état des fonctionnalités suivantes du NAS Manager sont soit **View only (Afficher uniquement)** ou **Fail (En échec)**.

Tab	Caractéristique	État en mode dégradé
Accès	Supprimer le volume NAS	En échec
	Exportations NFS	Afficher uniquement
	Partages CIFS	Afficher uniquement
Protection des données	Restauration d'instantané	En échec
	Partenaires de réplication	Afficher uniquement
System Management (Gestion du système)	Configuration horaire	Afficher uniquement
	Configuration réseau	Afficher uniquement
	Sous-réseaux	Afficher uniquement
	Hôtes locaux	Afficher uniquement
	Voies statiques	Afficher uniquement
	Configuration CIFS	Afficher uniquement
	NIS/LDAP	Afficher uniquement
	Utilisateurs/groupes locaux	Afficher uniquement
	Adressage	Adressage
	SNMP	Afficher uniquement
	Restauration de la configuration du cluster	En échec
	Formater	En échec
	Étendre les LUN	En échec
	Ajouter des LUN	En échec
	Ajouter des nœuds	En échec

# Internationalisation

## Présentation

La solution en cluster NAS fournit une prise en charge Unicode permettant la prise en charge de différentes langues simultanément. Les répertoires et les noms de fichiers sont maintenus et gérés en interne au format Unicode (UTF-8).

Quel que soit le type de cryptage utilisé par le client qui crée un fichier, la solution en cluster NAS stocke son nom de fichier ou nom de répertoire au format Unicode. Lorsqu'un client non Unicode crée un fichier sur un partage, montage ou volume, ce fichier est immédiatement converti au format Unicode approprié par la solution en cluster NAS.

## Présentation générale de la prise en charge du client Unicode

Les clients Unicode peuvent accéder nativement aux répertoires et fichiers Unicode, alors que les autres clients non Unicode (tels que les clients Windows 98, Windows ME, Mac OS 9.x) peuvent accéder au système de fichiers grâce à la capacité de la solution en cluster NAS de fournir des conversions de pages de code des noms de fichiers, répertoires, partages et volumes, en fonction de la page de code utilisée par le client.

Les clients Unicode natifs comprennent les éléments suivants :

- Microsoft Windows 7/Server 2008 R2
- Microsoft Windows Vista/Server 2008
- Microsoft Windows XP
- Microsoft Windows 2000/2003
- Microsoft Windows NT
- Clients basés sur UNIX

## Clients NFS

Les clients NFS peuvent configurer une page de codes différente pour des partages différents, tout en prenant simultanément en charge les clients non Unicode qui utilisent des langues différentes.

## Clients CIFS

Les utilisateurs CIFS peuvent configurer une page de code pour une utilisation pour tous les clients Windows et DOS non Unicode.



**REMARQUE :** L'interface Web offre une prise en charge Unicode complète. Pour afficher et utiliser des données Unicode à l'aide de la CLI, vous devez utiliser un UTF-8 XTERM.

## Paramètres de Configuration d'Unicode

Les paramètres de configuration suivants peuvent contenir des caractères Unicode.

Paramètre	Caractère Unicode
CIFS	Description du serveur
Partages d'accueil	Nom de répertoire
SNMP	Contact Emplacement
Exportations NFS	Nom de répertoire
Partages CIFS	Nom Répertoire Description Groupes d'utilisateurs

## Limitations de la configuration d'Unicode

Vous trouverez ci-après les limitations de la configuration d'Unicode :

- Taille de fichier et Nom de répertoire
- Problèmes de compatibilité des clients
- Question de compatibilité avec le japonais

## Taille de fichier et Nom de répertoire

La taille du fichier et les noms de répertoire sont limités à 255 octets, ce qui peut être inférieur à 255 caractères si l'on utilise Unicode, car chaque caractère UTF-8 occupe entre 1 et 6 octets.

## Problèmes de compatibilité des clients

Il arrive que différents fournisseurs utilisent un code UTF-8 différent pour les mêmes entrées de page codées, ce qui peut empêcher les caractères de s'afficher ou entraîner leur substitution par d'autres caractères de forme similaire.

## Question de compatibilité avec le japonais

Les administrateurs utilisant la CLI ne seront en mesure de saisir des caractères japonais dans les paramètres de configuration que par l'intermédiaire de l'interface Web, car les applications XTERM telles que KTERM ne vous permettent pas d'utiliser les caractères UTF-8.

Le tableau suivant détaille les caractères japonais incompatibles.

Caractère	UNIX	Windows	Macintosh
TILDE (~)	U+301C (TILDE)	U+FF5E (TILDE PLEINE CHASSE)	U+301C (TILDE)
DOUBLE LIGNE VERTICALE (  )	U+216 (DOUBLE LIGNE VERTICALE)	U+2225 (PARALLÈLE À)	U+216 (DOUBLE LIGNE VERTICALE)
SIGNE MOINS (-)	U+2212 (SIGNE MOINS)	U+FF0D (TIRET PLEINE CHASSE)	U+2212 (SIGNE MOINS)
TIRET EN CHEF (¯)	U+FFE3 (MICRON PLEINE CHASSE)	U+FFE3 (MICRON PLEINE CHASSE)	U+203E (SURLIGNÉ)

Caractère	UNIX	Windows	Macintosh
SYMBOLE CENTIME (¢)	U+00A2 (SYMBOLE CENTIME)	U+FFE0 (SYMBOLE CENTIME PLEINE CHASSE)	U+00A2 (SYMBOLE CENTIME)
SYMBOLE LIVRE (#)	U+00A3 (SYMBOLE LIVRE)	U+FFE1 (SYMBOLE LIVRE PLEINE CHASSE)	U+00A3 (SYMBOLE LIVRE)
SIGNE NÉGATION (¬)	U+00AC (SIGNE NÉGATION)	U+FFE2 (SIGNE NÉGATION PLEINE CHASSE)	U+00AC (SIGNE NÉGATION)

La solution en cluster NAS fournit une page de codes spéciale au service CIFS pour la prise en charge de la portabilité entre les protocoles. Si vous travaillez dans un environnement à plusieurs protocoles et souhaitez partager des fichiers et répertoires entre protocoles, il est recommandé d'utiliser cette option.

Lorsque le service CIFS est configuré pour utiliser UTF-8-JP pour le cryptage interne (page de codes UNIX), le cryptage incompatible Windows est adressé au codage UNIX/ Mac O/S approprié sur la solution en cluster NAS. Cela assure l'adressage correct des caractères corrects et incorrects.



# Questions fréquemment posées

## NDMP

1. NDMP est-il un protocole de haute disponibilité ? Que se passe-t-il si une session de sauvegarde est interrompue en raison d'une perte de connexion ?  
NDMP n'est pas un protocole de haute disponibilité. Une session qui est interrompue est terminée.
2. Comment NDMP fonctionne-t-il ?  
Au début de la session NDMP, un instantané du Fluid File System (FluidFS) est pris sur le système de fichiers NAS. Cet instantané est ensuite transféré sur l'application de gestion des données (DMA, Data Management Application). Une fois la session terminée, il est supprimé.
3. Les instantanés NDMP sont-ils spéciaux ?  
Non, il s'agit simplement d'instantanés à usage unique FluidFS.
4. D'où provient l'équilibrage de charge ?  
NDMP n'a pas d'équilibrage de charge intégré. Les sauvegardes DMA uniques de jusqu'à 10 volumes depuis une VIP client forcent toutes les 10 sessions à se dérouler sur le même nœud. Utilisez le DNS round-robin (tourniquet DNS) pour fournir un équilibrage de charge en indiquant le nom DNS de votre appliance dans l'application DMA.
5. Pourquoi l'instantané `ndmp_backup_xxxx_nodeX` est-il présent sur mon volume ?  
Il s'agit de l'instantané pris par le protocole NDMP. Suite à une session de sauvegarde réussie, cet instantané est supprimé. Si la session de sauvegarde se termine avec une erreur, l'instantané peut ne pas être supprimé automatiquement. Dans ce cas, vous pouvez le supprimer manuellement en toute sécurité.
6. Combien d'applications DMA peuvent exécuter une sauvegarde à tout moment ?  
Jusqu'à 16 applications DMA peuvent être définies sur une solution en cluster NAS. Il n'existe aucune limite quant au nombre d'applications DMA pouvant effectuer des sauvegardes à tout moment donné.
7. Puis-je restaurer un fichier unique ?  
Oui
8. Puis-je restaurer une sauvegarde précédente sur une autre appliance NAS ?  
Oui
9. Puis-je restaurer une sauvegarde sur une autre appliance NDMP ?  
Les données NDMP sont envoyées sous format brut, permettant ainsi à la cible de les prendre en charge.
10. Puis-je voir quelles sauvegardes actives sont en cours ?  
Oui. Vous pouvez utiliser la CLI du NAS pour afficher les sauvegardes actives actuellement en cours. Pour afficher les sauvegardes actives actuellement en cours, exécutez la liste `data-protection ndmp active-jobs`.
11. Puis-je utiliser NDMP pour sauvegarder le lecteur réseau que j'ai adressé à mon client ?  
Non, vous ne pouvez pas utiliser NDMP pour sauvegarder un lecteur réseau.

## Réplication

1. Comment la réplication fonctionne-t-elle ?

La réplication se sert de la technologie d'instantanés FluidFS et d'autres calculs pour assurer que les données du volume virtuel répliqué correspondent aux données du volume virtuel source au moment du lancement de la tâche de réplication. Seuls les blocs ayant été modifiés depuis la dernière tâche de réplication sont transférés sur le réseau client.

2. Combien de temps une réplication prend-elle ?  
Cela dépend du montant de données présentes sur le volume virtuel et du montant de données ayant été modifiées depuis le dernier cycle de réplication. Cependant, la réplication est une tâche de bas niveau qui a la priorité sur les données de service. L'administrateur peut surveiller l'avancement de la réplication en cliquant sur **Refresh (Actualiser)**. L'écran affiche un pourcentage approximatif de la progression.
3. Puis-je répliquer un volume virtuel sur plusieurs volumes virtuels cibles ?  
Non, une fois qu'un volume source est doté d'une stratégie de réplication avec un volume virtuel cible, aucun des volumes virtuels ne peut être utilisé pour la réplication (source ou de destination).
4. Pourquoi ne puis-je pas écrire sur le volume virtuel cible avec NFS ou CIFS ?  
Une fois la stratégie de réplication définie, le volume virtuel cible passe en lecture seule. Lorsque la stratégie de réplication est déconnectée, le volume virtuel cible n'est plus en lecture seule.
5. Je suis sur le système cible et je ne parviens pas à déclencher une réplication pour mon volume virtuel cible.  
Les opérations de réplication doivent être réalisées sur le volume virtuel source.
6. Puis-je effectuer une réplication sur le même système ?  
Oui, vous pouvez effectuer une réplication depuis un volume virtuel source sur un volume virtuel de destination du même système.
7. La réplication bidirectionnelle est-elle prise en charge entre les deux systèmes ?  
Oui, vous disposez d'une combinaison de volumes cible et volumes source sur des partenaires de réplication.
8. Puis-je disposer de plusieurs systèmes de partenaires de réplication ?  
Oui, plusieurs partenaires de réplication sont permis ; cependant, vous ne pouvez pas répliquer un volume virtuel source sur plusieurs volumes cible.
9. Lorsque je supprime la stratégie de réplication, une invite me demande si je souhaite appliquer la configuration du volume source à la configuration du volume cible. Qu'est-ce que cela signifie ?  
Cela signifie que vous avez la possibilité si vous le souhaitez de transférer toutes les propriétés de niveau du volume virtuel (style de sécurité, quotas, exportation NFS, partages CIFS, et ainsi de suite) sur le volume cible. Il serait bon d'effectuer un tel transfert si ce volume virtuel remplace le volume virtuel source, ainsi que dans d'autres scénarios informatiques.
10. Mon réseau client ralentit pendant la réplication. Puis-je modifier la priorité de la réplication comparé aux clients de service ?  
Il s'agit d'un comportement normal. La réplication est un processus de bas niveau et a la priorité sur les clients de service. L'administrateur peut surveiller l'avancement de la réplication en cliquant sur **Refresh (Actualiser)**. L'écran affiche un pourcentage approximatif de la progression.
11. Pourquoi ne puis-je pas supprimer la stratégie de réplication depuis le volume virtuel source ?  
Il s'agit d'un comportement normal. Toutes les modifications de configuration doivent être effectuées sur le volume virtuel source. Si le système dans lequel le volume source se trouve est inaccessible (s'il est en panne, manquant, etc), vous pouvez supprimer la stratégie de réplication depuis le volume cible.

## Gestion sécurisée

Lorsqu'elle est activée, la gestion sécurisée déplace tout le trafic de gestion sur un sous-réseau, rendant tous les autres sous-réseaux disponibles uniquement pour l'accès client (CIFS/NFS), la réplication et le trafic NDMP. Ceci empêche les utilisateurs des sous-réseaux d'accès client (données) d'accéder aux fonctions de gestion. Dans FluidFS, les ports mentionnés ci-dessous ne participent pas à la communication NFS/CIFS, mais sont exposés dans le réseau client. Par défaut, tous les ports de gestion sont ouverts sur tous les sous-réseaux, ainsi que les autres ports nécessaires pour l'accès client, la réplication et NDMP.


Pour certains utilisateurs, le trafic de gestion doit être traité comme un privilège et doit être exposé uniquement dans un sous-réseau unique. Les ports nécessaires pour l'accès clients (CIFS/NFS), la réplication et le trafic NDMP sont ouverts sur le sous-réseau dont la gestion sécurisée est activée.

Service	Port
Services Web	80
Services Web	443
FTP	44421
FTP	44422
SSH	22
SOAP	35451

Le fonction de gestion sécurisée autorise l'activation de la **gestion sécurisée** sur un sous-réseau spécifique. Ainsi, tout le trafic de réseau est limité exclusivement à ce sous-réseau spécifique. Aucun des ports de ces groupes n'écouterà les autres sous-réseaux. Lorsque la gestion sécurisée est activée, vous devez accéder au FluidFS NAS Manager (GUI Web) à l'aide du HTTP sécurisé **https://<VIPdegestion>/** au lieu d'utiliser tout simplement **http**. Lorsque la gestion sécurisée est activée, le port 80 est désactivé sur tous les sous-réseaux. La gestion sécurisée peut être activée uniquement suite au déploiement complet du système.

- La fonction **gestion sécurisée** est gérée au moyen de l'interface de ligne de commande FluidFS.
- Pour sécuriser un sous-réseau :
  - Il doit exister préalablement à l'opération de sécurité
  - Il doit résider dans le réseau physique du client
  - Vous devez vous connecter à la CLI depuis ce sous-réseau

Pour en savoir plus sur la commande CLI de gestion sécurisée, voir le *Dell FluidFS NAS Solutions CLI Reference Guide* (Guide de référence CLI de solutions NAS Dell FluidFS) à l'adresse [dell.com/support/manuals](http://dell.com/support/manuals).

 **REMARQUE** : Le fait d'activer la gestion sécurisée sur un sous-réseau ne déconnecte pas les sessions de gestion existantes résidant sur d'autres sous-réseaux. Si de telles sessions existent, vous en serez averti. Pour vous assurer qu'il n'existe aucune session existante, déconnectez les sessions signalées, désactivez la gestion sécurisée puis réactivez-la. Vérifiez qu'aucune autre session de gestion n'a été signalée.

## Ports NAS FluidFS utilisés

Tableau 2. Ports requis

Numéro de port FluidFS	Protocole	Nom de service
445	TCP et UDP	CIFS/SMB
427	TCP et UDP	SLP
2049 - 2049+(numéro de domaine - 1)	TCP et UDP	NFS
5001 - 5001+(numéro de domaine - 1)	TCP et UDP	montage
5051 - 5051+(numéro de domaine - 1)	TCP et UDP	quota
4050 - 4050+(numéro de domaine - 1)	TCP et UDP	NLM (gestionnaire de verrouillage)
4000 - 4000+(numéro de domaine - 1)	TCP et UDP	statd
111	TCP et UDP	portmap
44421	TCP	FTP
22	TCP	SSH
80	TCP	HTTP
443	TCP	HTTPS de gestion Web
53	UDP	DNS

Tableau 3. Nombre de ports utilisés en fonction des exigences


Numéro de port FluidFS	Protocole	Nom de service
138	UDP	NetBIOS
139	TCP	NetBIOS
88	TCP et UDP	Kerberos
464	TCP et UDP	Kerberos v5
543	TCP	Connexion Kerberos
544	TCP	Shell distant Kerberos
749	TCP et UDP	Administration Kerberos
135	TCP	AD - RPC
711	UDP	NIS
714	TCP	NIS
389	TCP et UDP	LDAP
3268	TCP	Catalogue global LDAP
3 269	TCP	Catalogue global LDAP sur TLS/SSL
636	TCP	LDAP sur TLS/SSL

<b>Numéro de port FluidFS</b>	<b>Protocole</b>	<b>Nom de service</b>
123	UDP	NTP
161	UDP	Agent SNMP
162	TCP	Interruption SNMP
10000	TCP	NDMP
10560-10568	TCP	Réplication
1344	TCP	Antivirus - ICAP
8004	TCP	WebUI du serveur ScanEngine (hôte AV)



# Obtenir de l'aide

## Contacteur Dell

 **REMARQUE** : Dell fournit plusieurs options de service et de support en ligne et par téléphone. Si vous ne possédez pas une connexion Internet active, vous pourrez trouver les coordonnées sur votre facture d'achat, bordereau d'expédition, acte de vente ou catalogue de produits Dell. La disponibilité des produits varie selon le pays et le produit. Il se peut que certains services ne soient pas disponibles dans votre région.

Pour prendre contact avec Dell pour des questions commerciales, de support technique ou de service clientèle :

1. Rendez-vous sur [dell.com/contactdell](http://dell.com/contactdell).
2. Sélectionnez votre pays ou région depuis la carte du monde interactive.  
Les pays correspondant à la région sélectionnée s'affichent lorsque vous sélectionnez une région.
3. Sélectionnez la langue appropriée sous le pays de votre choix.
4. Sélectionnez votre secteur d'activités.  
La page de support principale pour le secteur d'activités sélectionné s'affichera.
5. Sélectionnez l'option appropriée en fonction de vos besoins.

## Localisation du numéro de service de votre système

Votre système est identifié par un code de service express et un numéro de service uniques. Ceux-ci se trouvent à l'avant du système sur l'étiquette d'informations. Dell utilise ces informations pour acheminer les appels de support au personnel approprié.

## Commentaires sur la documentation

Si vous avez des commentaires à faire sur ce document, écrivez à l'adresse [documentation\\_feedback@dell.com](mailto:documentation_feedback@dell.com). Sinon, cliquez sur le lien **Commentaires** sur n'importe laquelle des pages de documentation Dell, remplissez le formulaire et cliquez sur **Soumettre** pour envoyer vos commentaires.