



Guide d'administration de Sun StorEdge™ 5310 NAS Appliance et Gateway System

Sun Microsystems, Inc.
www.sun.com

Référence : 819-5229-10
Février 2006, révision A

Envoyez vos commentaires concernant ce document à l'adresse : <http://www.sun.com/hwdocs/feedback>

Copyright 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. Tous droits réservés.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit décrit dans ce document. En particulier, et sans limitation aucune, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs des brevets américains répertoriés à l'adresse <http://www.sun.com/patents> et un ou plusieurs brevets supplémentaires ou demandes de brevet en instance aux États-Unis et dans d'autres pays.

Ce document et le produit afférent sont exclusivement distribués avec des licences qui en restreignent l'utilisation, la copie, la distribution et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous quelque forme que ce soit, par quelque moyen que ce soit, sans l'autorisation écrite préalable de Sun et de ses éventuels bailleurs de licence.

Les logiciels détenus par des tiers, y compris la technologie relative aux polices de caractères, sont protégés par copyright et distribués sous licence par des fournisseurs de Sun.

Des parties de ce produit peuvent être dérivées des systèmes Berkeley BSD, distribués sous licence par l'Université de Californie. UNIX est une marque déposée aux États-Unis et dans d'autres pays, distribuée exclusivement sous licence par X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, AnswerBook2, docs.sun.com, Sun StorEdge et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux États-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et désignent des marques de fabrique ou des marques déposées de SPARC International, Inc., aux États-Unis et dans d'autres pays. Les produits portant les marques déposées SPARC reposent sur une architecture développée par Sun Microsystems, Inc.

L'interface graphique utilisateur d'OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. à l'intention des utilisateurs et détenteurs de licences. Sun reconnaît les efforts de pionnier de Xerox en matière de recherche et de développement du concept des interfaces graphique ou visuelle utilisateur pour l'industrie informatique. Sun détient une licence non exclusive de Xerox sur l'interface graphique utilisateur (IG) Xerox, cette licence couvrant également les détenteurs de licences Sun qui mettent en place des IG OPEN LOOK et se conforment par ailleurs aux contrats de licence écrits de Sun.

LA DOCUMENTATION EST FOURNIE « EN L'ÉTAT » ET TOUTE AUTRE CONDITION, DÉCLARATION ET GARANTIE, EXPRESSE OU TACITE, EST FORMELLEMENT EXCLUE, DANS LA MESURE AUTORISÉE PAR LA LOI EN VIGUEUR, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE À LA QUALITÉ MARCHANDE, À L'APTITUDE À UNE UTILISATION PARTICULIÈRE OU À L'ABSENCE DE CONTREFAÇON.



Papier
recyclable



Adobe PostScript

Table des matières

Préface xxi

1. Introduction 1

Navigation dans Web Administrator 1

Utilisation de l'interface graphique utilisateur 2

Exécution de l'assistant de configuration 7

Options de l'assistant de configuration 7

▼ Pour lancer l'assistant 8

Étapes suivantes 9

2. Configuration initiale du réseau 11

Définition du nom du serveur 12

▼ Pour définir le nom du serveur 12

Définition de chemins de LUN 13

Définition de chemins d'unités LUN 17

Activation du basculement 18

Activation du basculement de tête 19

Lancement du rétablissement 20

▼ Pour lancer une récupération 20

Configuration des ports réseau	21
Emplacements des ports de Sun StorEdge 5310 NAS Appliance	21
▼ Pour configurer des adaptateurs réseau	22
Définition de l'adresse de passerelle par défaut	24
▼ Pour spécifier l'adresse de passerelle par défaut	24
Services de noms	24
Configuration de la sécurité Windows	24
Paramétrage WINS	27
Paramétrage DNS	27
Paramétrage NIS	29
Paramétrage de NIS+	30
Configuration des services de noms	32
Paramétrage de la notification par e-mail	33
▼ Pour paramétrer SMTP et envoyer des e-mails aux destinataires	33
Paramétrage de la journalisation	34
▼ Pour paramétrer la journalisation en local ou à distance	35
Sélection de la langue	36
▼ Pour sélectionner la langue	36
Sauvegarde des informations de configuration	36
Étapes suivantes	37
3. Paramétrage et gestion du système de fichiers	39
Concepts relatifs au système de fichiers	39
RAID	39
LUN	42
Partition	42
Volume de fichiers	43
Segment	43

Création d'un système de fichiers	44
Création de jeux RAID et de LUN	44
Conversion d'un disque en disque hot spare	48
Création d'un volume de fichiers ou d'un segment	49
▼ Pour créer un volume de fichiers ou un segment par l'intermédiaire du panneau Create File Volumes (Création de volumes de fichiers)	49
▼ Pour créer un volume de fichiers ou un segment à l'aide du System Manager (Gestionnaire système)	50
Rattachement de segments à un volume de fichiers principal	52
Reconstruction d'un LUN	53
Gestion de volumes de fichiers et de segments	54
Modification des propriétés du volume de fichiers	54
Suppression de volumes de fichiers	57
Affichage des partitions de volume	58
Configuration iSCSI	59
Configuration d'une cible iSCSI	59
Configuration de l'accès de l'initiateur iSCSI	60
▼ Pour créer une liste d'accès iSCSI	60
▼ Pour créer un LUN iSCSI	62
Méthodes de détection de cible iSCSI	64
Configuration d'un serveur iSNS	64
▼ Pour définir le serveur iSNS	64
Étapes suivantes	65
4. Gestion du système	67
Définition du mot de passe de l'administrateur	67
▼ Pour définir le mot de passe administrateur	67

Contrôle de l'heure et de la date	68
Synchronisation temporelle	69
Paramétrage de la synchronisation horaire	69
Réglage manuel de la date et de l'heure	71
Utilisation d'un logiciel antivirus	72
▼ Pour activer la protection antivirus	72
Analyse antivirus	75
5. Gestion des ports système	77
Emplacement des ports	77
À propos des adresses IP alias	79
Liaison de ports	80
Liaisons de type agrégation de ports	80
Liaisons haute disponibilité	81
Liaison de ports sur un système à un serveur	81
Liaison de ports sur un système cluster Sun StorEdge 5310	82
Exemple de liaison de ports sur un système à deux serveurs	84
6. Active Directory Service et l'authentification	87
Services de noms pris en charge	87
Active Directory Service	88
▼ Pour activer ADS	89
▼ Pour vérifier l'ordre de recherche des services de noms	90
▼ Pour vérifier la configuration DNS	91
▼ Pour publier les partages dans ADS	91
▼ Pour mettre à jour des conteneurs de partage ADS	92
▼ Pour supprimer des partages d'ADS	93
Paramétrage LDAP	93
▼ Pour activer le service LDAP	93

Modification de l'ordre de recherche des services de noms	94
▼ Pour définir l'ordre de recherche des utilisateurs, groupes, groupes réseau et hôtes	94
7. Groupes, hôtes et sécurité du répertoire de fichiers	95
Groupes locaux	95
Configuration des privilèges accordés aux groupes locaux	96
Configuration des hôtes	99
Ajout et modification d'hôtes	100
Mappage des références d'utilisateurs et de groupes	101
Utilisateurs et groupes UNIX	102
Utilisateurs et groupes Windows	102
Mappage de références	104
Mappage d'utilisateurs	104
Mappage de groupes	106
Mappage de références intégré	107
▼ Pour définir la stratégie de mappage	108
▼ Pour mapper des utilisateurs et des groupes Windows à des groupes et utilisateurs UNIX	109
Définition de la sécurité du répertoire de fichiers	110
Définition de la sécurité du répertoire de fichiers en mode de groupe de travail	110
Définition de la sécurité du répertoire de fichiers en mode de domaine	110
8. Partages, quotas et exportations	113
Partages	113
Partages statiques	114
Configuration de partages statiques	114
Configuration de clients SMB/CIFS	119
Partages autohome	121

Gestion de quotas	123
Configuration de quotas d'utilisateurs et de groupes	123
Configuration des quotas de la structure de répertoire	127
Paramétrage d'exportations NFS	129
▼ Pour créer des exportations	130
▼ Pour modifier des exportations	131
Suppression d'exportations	131

9. Options système 133

Activation des options système	133
▼ Pour activer une option	134
Sun StorEdge File Replicator	135
Sun StorEdge 5310 NAS Appliance Mise en miroir	135
Préparation de la mise en miroir	135
Conditions requises et limitations de File Replicator dans une configuration en cluster	136
Configuration des systèmes actif et miroir	136
Configuration des volumes de fichiers mis en miroir	138
▼ Pour corriger un miroir fissuré	141
Définition des seuils d'avertissement	141
Interruption de la connexion entre les serveurs miroir	142
Promotion d'un volume de fichiers en miroir	143
Rétablissement d'une connexion miroir	144
Modification des rôles de volumes	147
Compliance Archiving Software	148
Activation de l'archivage en conformité	148
Contrôle de mise en conformité	151
Fonctions d'archivage en conformité supplémentaires	153

10. Contrôle du système	155
Contrôle SNMP (Simple Network Management Protocol)	156
▼ Pour paramétrer le protocole SNMP	156
Visualisation du statut du système	157
▼ Pour visualiser le statut du système	158
Journalisation du système	158
▼ Pour afficher le journal système	160
Événements système	160
Audit du système	161
Configuration de l'audit	161
▼ Pour configurer l'audit du système	161
Fichiers journaux d'audit	162
Événements audités	162
Lecture des journaux d'audit	163
Statut de l'environnement	163
▼ Pour afficher le statut des ventilateurs	163
▼ Pour afficher le statut de la température	164
▼ Pour afficher le statut de l'alimentation	165
▼ Pour afficher le statut de la tension	165
Informations sur l'utilisation	167
▼ Pour afficher les informations sur l'utilisation des volumes de fichiers	167
▼ Pour afficher l'activité réseau	167
▼ Pour afficher l'activité système	168
▼ Pour afficher des statistiques (sur le port) réseau	169
Affichage des routes réseau	170
À propos du routage	170
▼ Pour afficher les routes	171

Contrôle des composants système	172
Contrôle de l'onduleur UPS	172
Affichage des informations sur le contrôleur	173
Affichage du statut de la mise en miroir	173
Affichage du statut de la tâche de sauvegarde	175
▼ Pour afficher le journal de sauvegarde	175
▼ Pour afficher le statut des tâches	176
▼ Pour afficher le statut des bandes	176
11. Maintenance du système	177
Définition des options d'accès à distance	177
▼ Pour définir la sécurité d'accès à distance	178
Configuration de l'accès FTP	178
▼ Pour paramétrer les utilisateurs FTP	179
Arrêt du serveur	180
▼ Pour arrêter, stopper ou redémarrer le serveur	180
Points de contrôle de fichiers	181
Création de points de contrôle de fichiers	181
Planification de points de contrôle de fichiers	182
Partage des points de contrôle de fichiers	185
Accès aux points de contrôle de fichiers	186
Sauvegarde et restauration	187
Paramétrage du protocole NDMP	187
Conversion des caractères CATIA V4/V5	188
▼ Pour activer CATIA à l'aide de la CLI	189
▼ Pour activer automatiquement CATIA au redémarrage	189
Nettoyage des têtes	189
▼ Pour effectuer un nettoyage des têtes	189

Mise à jour du logiciel de Sun StorEdge 5310 NAS Appliance	190
▼ Pour mettre à jour le logiciel	190
Mise à niveau des révisions de microprogramme de baies et d'unités	191
Nécessité de mettre à niveau un microprogramme	191
Mise à niveau des microprogrammes de baies et d'unités (redémarrage nécessaire)	192
Mise à niveau du microprogramme d'une baie (redémarrage inutile)	194
Mise à niveau du microprogramme d'une unité (redémarrage nécessaire)	198
Capture de la sortie de la commande <code>raidctl</code>	200
A. Administration de la console	213
Accès à l'administrateur de la console	214
▼ Pour accéder à l'utilitaire Telnet de Windows	214
▼ Pour accéder à l'interface de ligne de commande	214
Vue d'ensemble des menus de la console	215
Directives élémentaires	215
Description des touches	215
Affichage du menu principal	216
▼ Pour utiliser le menu	216
Sauvegarde de la configuration	216
▼ Pour sauvegarder les informations de configuration	217
Gestion du système	217
▼ Pour configurer le protocole TCP/IP	217
▼ Pour modifier le mot de passe administrateur	218
Contrôle de l'heure et de la date	219
Paramétrage de la protection antivirus	221
Sélection d'une langue	223
Gestion des routes	223
▼ Pour gérer les routes statiques sur le réseau local	223

Services de noms	224
Paramétrage du DNS, de <code>syslogd</code> et de la journalisation locale	224
Paramétrage NIS et NIS+	226
Définition de l'ordre de recherche des services de noms	228
Gestion du système de fichiers serveur	228
Configuration des lettres d'unités	229
▼ Pour créer un nouveau volume de disque	229
▼ Pour renommer une partition	230
▼ Pour ajouter un segment d'extension	231
▼ Pour supprimer un volume de disque	231
Gestion des partages et quotas	232
Paramétrage des partages SMB/CIFS	232
Paramétrage des partages autohome SMB/CIFS	233
▼ Pour définir un partage	234
▼ Pour modifier un partage	235
▼ Pour supprimer un partage	235
Paramétrage du service ADS	236
Activation et désactivation de quotas	237
Sécurité	237
Configuration de groupes d'utilisateurs	237
Privilèges de groupe	239
Mappages d'utilisateurs et de groupes	239
Mappage et objets sécurisables	241
Configuration de la liste d'hôtes	243
Gestion des hôtes de confiance	244
Gestion de l'accès au volume	244
Verrouillage et déverrouillage de la console	245

Mise en miroir de volumes de fichiers	246
Configuration des serveurs actif et miroir	246
Configuration des volumes de fichiers	248
Définition des seuils d'avertissement	250
Promotion d'un volume de fichiers mis en miroir	250
Rétablissement d'un miroir	252
Contrôle	254
Configuration SNMP	254
Configuration de la notification par e-mail	255
Affichage des informations sur le système	256
Maintenance du système	260
Configuration de l'accès FTP	260
Gestion des contrôleurs RAID	262
Montage de systèmes de fichiers	263
Arrêt du système	264
Gestion du basculement	264
Configuration des chemins de LUN	266
Planification de points de contrôle de fichiers	270
Configuration d'une sauvegarde	270
Configuration du logiciel Compliance Archiving Software	271
Configuration de l'audit du système	272
B. Messages d'erreur de Sun StorEdge 5310 NAS Appliance	273
À propos de la notification d'erreur SysMon	273
Messages d'erreur de Sun StorEdge 5310 NAS Appliance	274
Erreurs liées au sous-système de l'UPS	274
Erreurs liées au système de fichiers	277
Erreurs liées au sous-système RAID	278
Événements IPMI	279

C. API Compliance Archiving Software	283
Fonctions de conformité	284
Fichiers WORM	284
Périodes de conservation par fichier	284
Verrouillage administratif	285
Accès à la fonction de conformité	285
Volumes en conformité	285
Fichiers WORM	285
Périodes de conservation des fichiers	288
Définition de l'état d'un fichier	289
Comportement des appels système UNIX	290
access(2)	290
chmod(2), fchmod(2)	290
chown(2), fchown(2)	291
link(2)	291
read(2), readv(2)	291
rename(2)	291
stat(2), fstat(2)	292
unlink(2)	292
utime(2), utimes(2)	292
write(2), writev(2)	292
Comportement des clients Windows	293
Création de fichiers WORM	293
Restrictions relatives aux métadonnées sur les fichiers WORM	293
Paramétrage des périodes de conservation	293
Remarques concernant les clients Windows	294
Autres API	294

D. Composants de l'appareil Sun StorEdge 5310 NAS Appliance	295
Alimentations électriques du serveur	296
Boutons du panneau avant du serveur	297
DEL de statut	297
Panneau arrière du serveur	298
Bibliothèque de bandes à connexion directe	299
Boîtier de contrôleur Sun StorEdge 5300 RAID EU et composants du boîtier d'extension Sun StorEdge 5300 EU	300
Controller Enclosures	300
Expansion Enclosures	301
Unités d'extension FC et SATA mélangées	301
Casiers pour disque dur	302
Alimentations	304
E. Envoi d'un e-mail de diagnostic	305
Index	307

Figures

FIGURE 1-1	Fenêtre principale	2
FIGURE 1-2	Barre d'outils	2
FIGURE 1-3	Volet de navigation	3
FIGURE 2-1	Chemins des unités logiques LUN affichées dans le volet Set LUN Path (Définition du chemin de LUN)	13
FIGURE 2-2	Configuration d'un système à serveur unique	15
FIGURE 2-3	Configuration d'un système à deux serveurs	16
FIGURE 5-1	Liaison de ports sur un système à deux serveurs	84
FIGURE D-1	Alimentation électrique	296
FIGURE D-2	Panneau arrière doté d'une seule carte HBA	298
FIGURE D-3	Casiers pour disque dur Fibre Channel	302
FIGURE D-4	Modules d'alimentation	304

Tableaux

TABLEAU 1-1	Icônes de la barre d'outils	3
TABLEAU 1-2	Symboles de dossiers	4
TABLEAU 1-3	Autres boutons	5
TABLEAU 2-1	Colonnes du panneau de définition des chemins de LUN	14
TABLEAU 2-2	Chemins de LUN dans des systèmes à serveur unique	15
TABLEAU 2-3	Chemins d'unités LUN dans des systèmes à deux serveurs	16
TABLEAU 3-1	Indicateurs d'état des unités de disque de la boîte de dialogue Add LUN (Ajout d'une unité LUN)	47
TABLEAU 3-2	Images représentant l'état des disques hot spare ajoutés	48
TABLEAU 5-1	Exemple de liaison de ports sur un système à deux serveurs	85
TABLEAU 7-1	Privilèges pris en charge	97
TABLEAU 7-2	Privilèges de groupe par défaut	97
TABLEAU 7-3	Champs d'un SID	103
TABLEAU 8-1	Exemples de chemins de partage	114
TABLEAU 8-2	Exemples de permissions Umask	118
TABLEAU 9-1	Format du journal d'audit	152
TABLEAU 10-1	Affichage du statut du système	158
TABLEAU 10-2	Icônes des événements système	160
TABLEAU 10-3	Plages de tension acceptables	166
TABLEAU 10-4	Périphériques système et réseau	168
TABLEAU 11-1	Table de conversion des caractères pour CATIA	188

TABLEAU 11-2	Répertoires et fichiers de microprogramme des composants	193
TABLEAU 11-3	Temps nécessaire à la mise à niveau des microprogrammes	194
TABLEAU 11-4	Répertoires et fichiers de microprogramme des composants	196
TABLEAU A-1	Touches d'écran actives	215
TABLEAU B-1	Messages d'erreur de l'onduleur UPS	274
TABLEAU B-2	Erreurs liées au système de fichiers	277
TABLEAU B-3	Messages d'erreur RAID	278
TABLEAU B-4	Messages d'erreur IPMI	279
TABLEAU C-1	Métadonnées de fichiers WORM modifiables et non modifiables	287
TABLEAU D-1	Indicateurs de statut DEL	297

Préface

Le *Guide d'administration de Sun StorEdge 5310 NAS Appliance et Gateway System* est à la fois un guide de l'administrateur et un guide de l'utilisateur conçu pour Sun StorEdge™ 5310 NAS Appliance, cluster Sun StorEdge™ 5310 et système de passerelle Sun StorEdge™ 5310 NAS Gateway System. Il explique comment utiliser le logiciel Web Administrator à des fins de paramétrage et de contrôle du système. Il comprend également des instructions relatives à l'utilisation de l'interface de ligne de commande (la CLI, command-line interface) et des informations complémentaires sur les composants matériels du système non fournies dans le *Guide de démarrage de Sun StorEdge 5310 NAS Appliance et Gateway System*.

Avant de lire ce document

Avant de lire ce manuel, vous devez avoir déjà installé et configuré le système comme décrit dans le *Guide de démarrage de Sun StorEdge 5310 NAS Appliance et Gateway System*.

Organisation de ce document

Ce document contient des instructions d'administration et d'utilisation de Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System.

Le [Chapitre 1](#) offre une vue d'ensemble des fonctions logicielles de Web Administrator.

Le [Chapitre 2](#) décrit la configuration de base du réseau et du système de fichiers.

Le [Chapitre 3](#) décrit la configuration du système RAID (Redundant Array of Independent Disks).

Le [Chapitre 4](#) décrit les fonctions de gestion.

Le [Chapitre 5](#) décrit les paramètres des ports.

Le [Chapitre 6](#) décrit les conventions de dénomination.

Le [Chapitre 7](#) décrit les paramètres de sécurité.

Le [Chapitre 8](#) décrit les partages, quotas et exportations.

Le [Chapitre 9](#) décrit les options logicielles assorties de licences.

Le [Chapitre 10](#) décrit les fonctions de contrôle.

Le [Chapitre 11](#) décrit les fonctions de maintenance.

L'[Annexe A](#) contient des instructions concernant l'utilisation de la console à des fins d'exécution de tâches système.

L'[Annexe B](#) décrit les messages d'erreur pouvant s'afficher à l'écran.

L'[Annexe C](#) décrit en détail l'API du logiciel Compliance Archiving Software.

L'[Annexe D](#) décrit en détail les composants matériels du système.

L'[Annexe E](#) explique comment envoyer un e-mail de diagnostic.

Conventions typographiques

Police de caractère*	Signification	Exemples
AaBbCc123	Noms de commandes, de fichiers et de répertoires ; affichage sur l'écran de l'ordinateur	Modifiez le fichier <code>.login</code> . Utilisez <code>ls -a</code> pour dresser la liste de tous les fichiers. <code>% Vous avez du courrier.</code>
AaBbCc123	Ce que vous tapez, par opposition à l'affichage sur l'écran de l'ordinateur	<code>% su</code> Mot de passe :
<i>AaBbCc123</i>	Titres d'ouvrages, nouveaux mots ou termes, mots importants. Remplacez les variables de la ligne de commande par des noms ou des valeurs réels.	Lisez le chapitre 6 du <i>Guide de l'utilisateur</i> . Il s'agit d'options de <i>classe</i> . Vous <i>devez</i> être un superutilisateur pour effectuer ces opérations. Pour supprimer un fichier, tapez <code>rm nom-fichier</code> .

* Les paramètres de votre navigateur peuvent différer de ceux-ci.

Documentation connexe

Les documents mis en ligne sont disponibles à l'adresse suivante :

http://www.sun.com/hwdocs/Network_Storage_Solutions/nas

Application	Titre	Référence	Format	Emplacement
Installation	<i>Notes de version de Sun StorEdge 5210 et 5310 NAS Appliance</i>	819-3092- <i>nn</i>	PDF	En ligne
Installation	<i>Sun StorEdge 5310 NAS Appliance Appliance and Gateway System – Guide de démarrage</i>	819-5224- <i>nn</i>	PDF HTML	En ligne En ligne
Installation de l'appareil NAS (sans passerelle)	<i>Setting Up the Sun StorEdge 5310 NAS</i>	819-1168- <i>nn</i>	Imprimé PDF	Kit d'expédition En ligne
Passerelle	<i>Poster de Sun StorEdge 5310 NAS Gateway System</i>	819-5234- <i>nn</i>	Imprimé PDF	Kit d'expédition En ligne

Documentation, support et formation

URL	Description
http://www.sun.com/documentation/	Téléchargez des documents aux formats PDF et HTML, et commandez des guides imprimés.
http://www.sun.com/support/	Demandez le support technique et téléchargez des patches.
http://www.sun.com/training/	Informez-vous sur les formations Sun disponibles.

Sites Web tiers

Sun ne saurait être tenu responsable de la disponibilité des sites Web tiers mentionnés dans ce manuel. Sun décline toute responsabilité quant au contenu, à la publicité, aux produits ou tout autre matériel disponibles dans ou par l'intermédiaire de ces sites ou ressources. Sun ne pourra en aucun cas être tenu responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation des contenus, biens ou services disponibles dans ou par l'intermédiaire de ces sites ou ressources.

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, nous vous invitons à nous faire parvenir vos commentaires et vos suggestions. Vous pouvez nous les envoyer à l'adresse suivante :

<http://www.sun.com/hwdocs/feedback>

N'oubliez pas de mentionner le titre et le numéro de référence du document dans votre commentaire :

Guide d'administration de Sun StorEdge 5310 NAS Appliance et Gateway System, référence 819-5229-10.

Introduction

L'interface graphique utilisateur Web Administrator (IG) de Sun StorEdge 5310 NAS Appliance facilite la configuration des paramètres réseau et de sécurité, ainsi que l'exécution de tâches administratives sur les systèmes Sun StorEdge 5310 NAS Appliance novateurs de Sun Microsystems.

Remarque – La plupart des caractéristiques et fonctions logicielles décrites dans ce manuel s'appliquent à toutes les configurations de Sun StorEdge 5310 NAS Appliance, de cluster Sun StorEdge 5310 et de système de passerelle Sun StorEdge 5310 Gateway System, couramment appelé le « système ». Lorsqu'une caractéristique ou une fonction s'applique à une configuration spécifique uniquement, cette dernière est citée explicitement.

Navigation dans Web Administrator

L'IG de Web Administrator permet de configurer les paramètres système au moyen d'une série de menus et d'écrans à onglets ou encore de panneaux. Ces paramètres et écrans seront abordés dans les chapitres suivants.

Utilisation de l'interface graphique utilisateur

La fenêtre principale de Web Administrator vous permet de parcourir, de configurer et de visualiser les événements système et les services. L'aspect de cette fenêtre varie en fonction de la configuration matérielle.

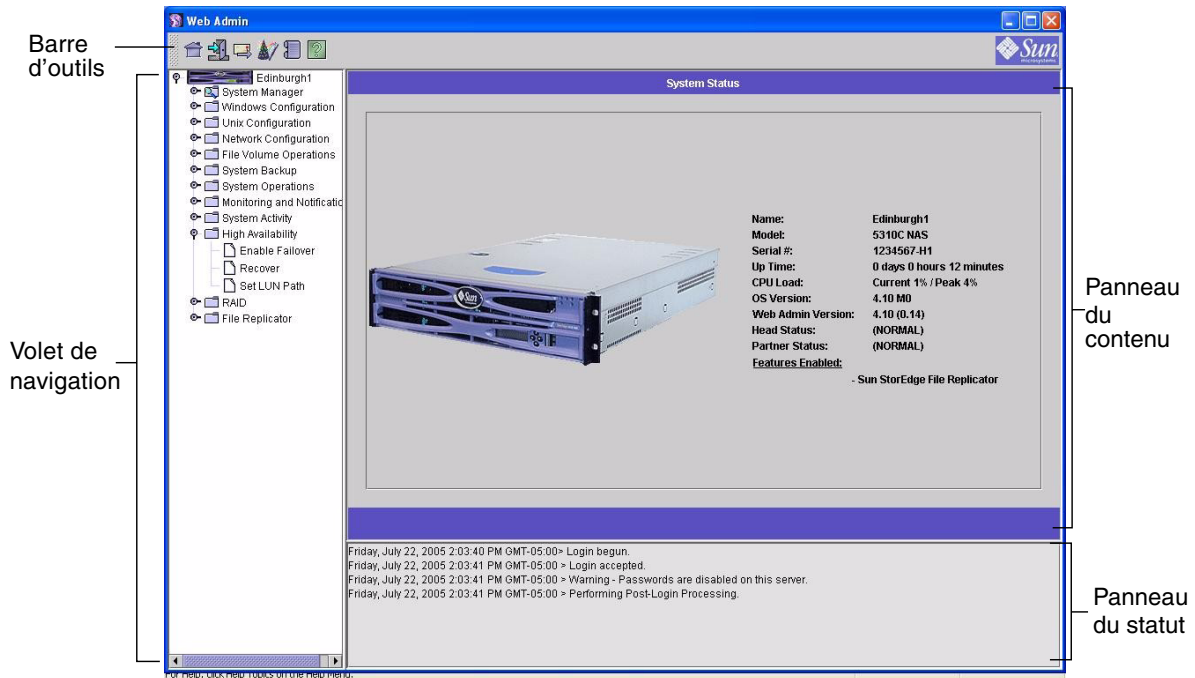


FIGURE 1-1 Fenêtre principale

Barre d'outils







La barre d'outils située en haut de la fenêtre Web Administrator vous permet d'accéder à la fenêtre d'accueil, de vous déconnecter, d'envoyer un e-mail de diagnostic, d'exécuter l'assistant de configuration, d'accéder au journal système et aux pages d'aide.



FIGURE 1-2 Barre d'outils

Le [TABLEAU 1-1](#) présente les différentes icônes de la barre d'outils.

TABLEAU 1-1 Icônes de la barre d'outils

Bouton	Nom	Action
	Accueil	Affichage de l'écran d'accueil du système
	Déconnexion	Déconnexion
	Messagerie	Envoi d'un e-mail de diagnostic
	Assistant	Exécution de l'assistant de configuration
	Journal système	Accès au journal système
	Aide	Accès à l'aide

Volet de navigation

Ce volet vous permet de naviguer dans Web Administrator. Il permet d'accéder à l'ensemble des fonctions d'administration, de paramétrage et de configuration.

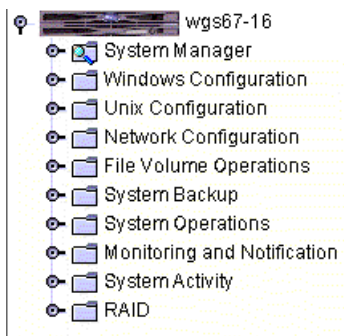















FIGURE 1-3 Volet de navigation

Pour ouvrir un dossier, cliquez sur le symbole  situé en regard du dossier ou double-cliquez sur le dossier. La position du symbole est ainsi modifiée : .

Exemple :   Network Configuration devient :   Network Configuration
 Set Server Name
  Configure TCP/IP
 Bond NIC Ports
 View the Routing Table









Pour fermer le dossier, cliquez à nouveau sur le symbole  pour qu'il revienne à la position .

Symboles de dossiers

Dans Web Administrator, les dossiers sont représentés par des symboles.

Le [TABLEAU 1-2](#) présente les symboles de dossiers.

TABLEAU 1-2 Symboles de dossiers






Symbole	Représentation
	Volume de fichiers
	Volume de fichiers compatible (avec onglet de dossier rouge)
	Volume de fichiers partagés
	Volume de fichiers exportés
	Volume de fichiers partagés et exportés
	Volume de fichiers mis en miroir
	Compatible avec la mise en miroir
	Segment

Autres boutons

Certains écrans de Web Administrator contiennent d'autres boutons.

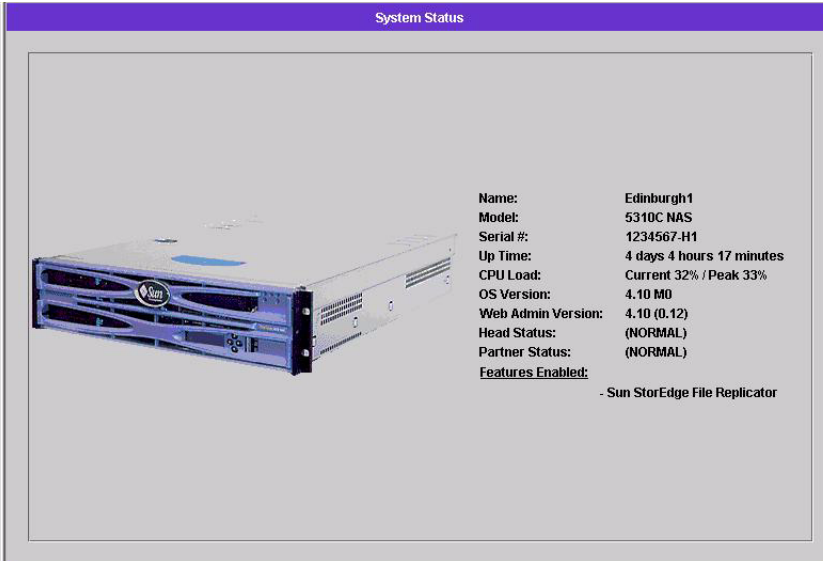
Le [TABLEAU 1-3](#) présente ces boutons supplémentaires.

TABLEAU 1-3 Autres boutons

Bouton	Nom	Action
	Ajouter	Ajoute un élément.
	Monter	Déplace l'élément sélectionné vers le haut.
	Descendre	Déplace l'élément sélectionné vers le bas.
	Corbeille	Supprime l'élément sélectionné.
	Modifier	Modifie l'élément sélectionné.

Panneau de contenu

Ce panneau contient des informations générales sur le système.



System Status

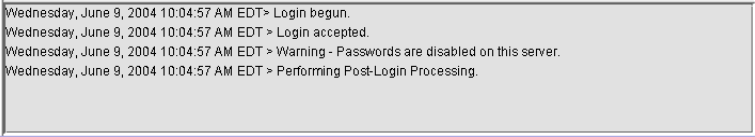
Name: Edinburgh1
Model: 5310C NAS
Serial #: 1234567-H1
Up Time: 4 days 4 hours 17 minutes
CPU Load: Current 32% / Peak 33%
OS Version: 4.10 M0
Web Admin Version: 4.10 (0.12)
Head Status: (NORMAL)
Partner Status: (NORMAL)

Features Enabled:
- Sun StorEdge File Replicator

Pour plus de détails sur le statut du système, reportez-vous à la section « [Visualisation du statut du système](#) », page 157.

Panneau des statuts

Le panneau des statuts, situé au bas de la fenêtre Web Administrator, affiche tous les événements qui se sont produits depuis la dernière connexion. Utilisez ce panneau pour vérifier que vos modifications ont été enregistrées ou que vos commandes système ont été exécutées correctement. Ce panneau affiche également les erreurs et les avertissements.



Wednesday, June 9, 2004 10:04:57 AM EDT > Login begun.
Wednesday, June 9, 2004 10:04:57 AM EDT > Login accepted.
Wednesday, June 9, 2004 10:04:57 AM EDT > Warning - Passwords are disabled on this server.
Wednesday, June 9, 2004 10:04:57 AM EDT > Performing Post-Login Processing.

Remarque – Le panneau des statuts indique la date et l’heure de la machine client exécutant le logiciel Web Administrator et pas celles du système.

Utilisation de l'aide

Le menu d'aide est disponible dans chaque écran de Web Administrator afin de fournir davantage d'informations sur les termes, les champs, les cases à cocher, les boutons radio ou les boutons d'action de l'écran sélectionné.

Pour afficher une rubrique d'aide relative à Web Administrator, cliquez sur le bouton d'aide de la barre d'outils. La fenêtre d'aide correspondant au panneau de contenu actuellement affiché s'ouvre à côté de l'écran de Web Administrator.

Exécution de l'assistant de configuration

L'assistant de configuration s'exécute automatiquement à la première connexion. Cet assistant va vous guider tout au long de la configuration initiale du système. Il vous aide à effectuer toutes les étapes requises pour établir une communication entre le système et le réseau. Une fois l'assistant terminé, vous devrez paramétrer le système de fichiers et configurer l'accès utilisateur.

Options de l'assistant de configuration

L'assistant de configuration propose plusieurs options. Certaines d'entre elles sont définies automatiquement par le système lui-même tandis que d'autres sont spécifiées par l'utilisateur en fonction de l'environnement réseau utilisé. Ce guide ne dispose pas de la place nécessaire pour couvrir la totalité des configurations possibles. Cette section vous propose une présentation de l'assistant de configuration et décrit les options disponibles.

Certaines caractéristiques et fonctions varient également en fonction des paramètres du système. Ces options sont abordées en fonction de l'environnement utilisé.

Cet assistant comporte trois options principales. Ces options dépendent de l'environnement réseau utilisé. Choisissez l'une des trois options suivantes :

- **UNIX only (UNIX uniquement)**. Cette option vous aide à configurer le système pour qu'il fonctionne dans un réseau UNIX[®] pur. Les fonctions associées à Windows ne sont pas prises en compte.
- **Windows only (Windows uniquement)**. Cette option vous aide à configurer le système pour qu'il fonctionne dans un réseau Windows pur. Les fonctions associées à UNIX ne sont pas prises en compte.
- **Both UNIX and Windows (UNIX et Windows à la fois)**. Cette option regroupe l'ensemble des fonctions et caractéristiques afin de vous aider à configurer le système pour un environnement réseau hétérogène Windows/UNIX.

Sélectionnez l'option appropriée à votre environnement réseau.

▼ Pour lancer l'assistant

1. **Pour exécuter l'assistant de configuration, cliquez sur le bouton Wizard de la barre d'outils.**

La page d'accueil de l'assistant est affichée.

2. **Cliquez sur Next (Suivant) afin de continuer.**

L'assistant passe ensuite en revue les étapes suivantes, décrites plus en détail au [Chapitre 2, « Configuration initiale du réseau »](#) :

1. Paramétrage du nom du serveur et des coordonnées de votre société
2. Configuration des adaptateurs réseau
3. Paramétrage de la passerelle par défaut
4. Configuration des domaines et des groupes de travail (sous des environnements Windows et mixtes) et activation et configuration du service Active Directory Service (ADS) (sous des environnements Windows et hétérogènes)
5. Configuration du service WINS (sous des environnements Windows et hétérogènes)
6. Paramétrage du service DNS

Remarque – Si le système a été démarré via DHCP, confirmez que l'adresse du serveur DNS est correcte. Sinon, désactivez la case à cocher Configure DNS (Configurer le DNS) pour éviter tout retard de redémarrage et de basculement.

7. Paramétrage du service Network Information Service (NIS) (sous des environnements UNIX et hétérogènes)
8. Paramétrage du service Network Information Service Plus (NIS+) (sous des environnements UNIX et hétérogènes)
9. Configuration des services de noms (sous des environnements Unix et hétérogènes)
10. Paramétrage de la notification par e-mail
11. Paramétrage de la journalisation en local et à distance
12. Attribution de la langue

3. Confirmation des paramètres

L'assistant enregistre vos paramètres et vous avertit en cas d'échec de certaines modifications apportées à la configuration.

Si vous préférez ne pas exécuter l'assistant, le [Chapitre 2](#), « [Configuration initiale du réseau](#) », vous explique comment accéder à ces mêmes fonctions dans le même ordre via le volet de navigation.

Étapes suivantes

À ce stade, le système doit normalement être en service et opérationnel. Il est par ailleurs supposé que vous disposez de connaissances de base concernant l'utilisation de Web Administrator. Il vous reste à définir le système de fichiers et à configurer les accès utilisateur.

Le paramétrage du système de fichiers implique la configuration de tous les volumes de fichiers, unités logiques LUN, partitions et segments appropriés. Pour plus d'informations sur ces concepts, reportez-vous à la section « [Concepts relatifs au système de fichiers](#) », page 39.

Une fois le système de fichiers configuré, vous devez paramétrer vos droits d'accès utilisateur ainsi que toutes les fonctions de gestion du système appropriées. Le [Chapitre 4](#), « [Gestion du système](#) » traite des principales fonctions de gestion. Consultez l'index pour rechercher une fonction spécifique et obtenir, entre autres, sa description, son mode d'utilisation, ses conditions d'application et toute règle spécifique concernant sa configuration.

Configuration initiale du réseau

Ce chapitre explique comment configurer le système afin qu'il puisse communiquer sur le réseau. Après avoir configuré les services et la communication réseau, vous devrez également configurer le système de fichiers, les droits d'accès utilisateur, les autres fonctions ainsi que les options que vous avez achetées.

Ce chapitre suit l'ordre des étapes de l'assistant de configuration. Toutefois, il n'aborde pas l'ensemble des fonctions que vous pouvez paramétrer. Pour configurer une fonction spécifique non présentée dans ce chapitre, recherchez-la dans l'index afin d'afficher les instructions correspondantes.

Ce chapitre aborde les sujets suivants :

- « Définition du nom du serveur », page 12
- « Définition de chemins de LUN », page 13
- « Activation du basculement », page 18
- « Lancement du rétablissement », page 20
- « Configuration des ports réseau », page 21
- « Définition de l'adresse de passerelle par défaut », page 24
- « Services de noms », page 24
- « Paramétrage de la notification par e-mail », page 33
- « Paramétrage de la journalisation », page 34
- « Sélection de la langue », page 36
- « Sauvegarde des informations de configuration », page 36
- « Étapes suivantes », page 37

Définition du nom du serveur

Vous devez définir un nom de serveur qui servira à identifier le serveur sur le réseau.

▼ Pour définir le nom du serveur

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Set Server Name (Définition du nom du serveur)**.

2. Indiquez le nom du serveur dans la zone **Server Name (Nom du serveur)**.

Ce nom permet d'identifier le système ou cette unité serveur pour des systèmes haute disponibilité à deux serveurs connectés au réseau. Il peut comprendre tout caractère alphanumérique (a-z, A-Z, 0-9), des tirets (-), des traits de soulignement (_) ou des points (.).

Remarque – Le nom du serveur doit commencer par une lettre (a-z ou A-Z), pas par un chiffre ou un symbole. Par exemple, « Astro2 » et « Saturn_05 » sont des noms de serveurs acceptables. En revanche, « 5Saturn » et « _Astro2 » ne le sont pas.

3. Saisissez les coordonnées de votre société, y compris son nom et les coordonnées de l'administrateur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System.

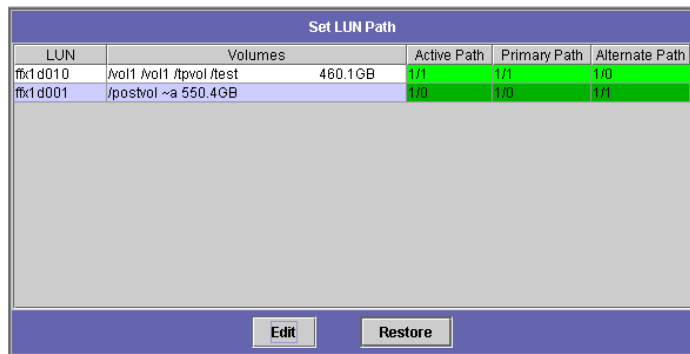
Le système indique ces informations dans tous les e-mails de diagnostic. Pour plus d'informations sur les e-mails de diagnostic, reportez-vous à l'[Annexe E](#).

4. Cliquez sur **Apply (Appliquer)** pour enregistrer les paramètres.

Définition de chemins de LUN

Un chemin de LUN () indique le mode d'accès à un volume de fichiers situé dans une unité logique (LUN) et quels serveur et contrôleur y ont accès. Pour chaque volume, il existe deux chemins d'unités LUN : le chemin principal et le chemin de substitution. En cas d'échec de l'un, le système utilise automatiquement l'autre chemin d'unité LUN disponible pour accéder au volume de fichiers souhaité. Le nombre de chemins d'unités LUN et leurs implémentations dépendent du modèle et de la configuration du système. Dans un système cluster Sun StorEdge 5310, un serveur (une tête) entraîne un basculement de tête (voir « [Activation du basculement de tête](#) », page 19) en cas d'échec des chemins principal et secondaire.

Vous avez la possibilité d'afficher et de modifier les chemins de LUN (voir « [Définition de chemins d'unités LUN](#) », page 17) à partir du panneau Set LUN Path (Définition du chemin de LUN).



LUN	Volumes	Active Path	Primary Path	Alternate Path
ffk1d010	/vol1 /vol1 /tpvol /test 460.1GB	1/1	1/1	1/0
ffk1d001	/postvol ~a 550.4GB	1/0	1/0	1/1

FIGURE 2-1 Chemins des unités logiques LUN affichées dans le volet Set LUN Path (Définition du chemin de LUN)

Le tableau suivant décrit les colonnes disponibles.

TABLEAU 2-1 Colonnes du panneau de définition des chemins de LUN

Colonne	Contenu
LUN	LUN disponibles sur le système.
Volumes	Noms des volumes de fichiers : une unité logique peut contenir plusieurs volumes de fichiers.
Active Path (Chemin actif)	Chemin LUN actif. La mention « 1/1 » désigne le contrôleur 1 et son état actif. D'autres appellations existent : Le premier numéro correspond au numéro HBA (commençant à 1). Le second numéro désigne le SCSI (cible) du contrôleur. Par exemple, la mention « 1/1 » désigne le HBA 1 et la cible SCSI du contrôleur 1.
Primary Path (Chemin principal)	Chemins de LUN principaux, sélectionnés par le système lors de son initialisation. Certains chemins permettent de restaurer les chemins de LUN. Si vous n'indiquez pas de chemin principal, le système utilise le premier chemin disponible.
Alternate Path (Chemin de substitution)	Chemins utilisés en cas d'échec des chemins principaux.

Chemins de LUN dans des systèmes à serveur unique

L'exemple suivant illustre une configuration matérielle standard dans un système à serveur unique.

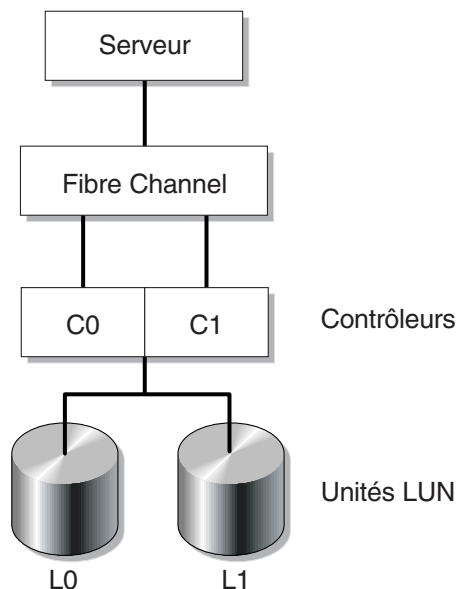


FIGURE 2-2 Configuration d'un système à serveur unique

Le chemin d'unité LUN principal d'un volume de fichier se trouvant dans l'unité LUN0 est C0-L0 tandis que son chemin de substitution est C1-L0. Le chemin d'unité LUN principal d'un volume de fichiers se trouvant dans l'unité LUN1 est C1-L1 tandis que son chemin de substitution est C0-L1. Comme le montre l'illustration, le système dispose des chemins d'unités LUN suivants.

TABLEAU 2-2 Chemins de LUN dans des systèmes à serveur unique

Chemins	LUN0	LUN1
Principal	C0-L0	C1-L1
Substitution	C1-L0	C0-L1

Vous pouvez accéder à chaque unité LUN par le biais du contrôleur 0 (C0) ou 1 (C1).

Chemins d'unités LUN dans des systèmes à deux serveurs

L'exemple suivant illustre une configuration matérielle standard dans un système cluster Sun StorEdge 5310 :

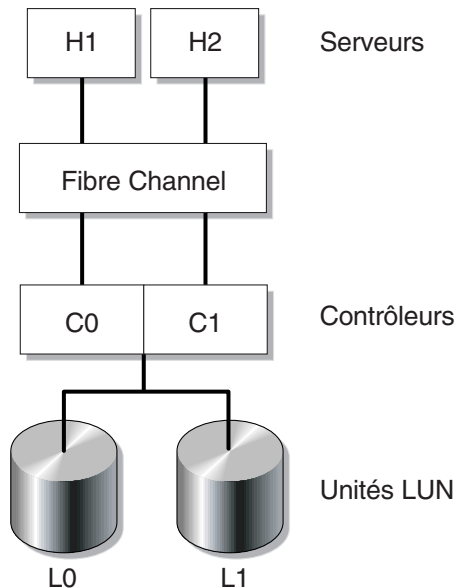


FIGURE 2-3 Configuration d'un système à deux serveurs

Le chemin d'unité LUN principal de la tête 1 est C0-L0 tandis que son chemin de substitution est C0-L1. Le chemin d'unité LUN principal de la tête 2 est C1-L0 tandis que son chemin de substitution est C1-L1. Comme le montre l'illustration, le système dispose des chemins d'unités LUN suivants :

TABLEAU 2-3 Chemins d'unités LUN dans des systèmes à deux serveurs

Tête 1	LUN	LUN0	LUN1
	Chemins	C0-L0	C0-L1
Tête 2	LUN	LUN0	LUN1
	Chemins	C1-L0	C1-L1

Normalement, vous accédez aux volumes de fichiers via le chemin d'unité LUN principal défini pour l'unité LUN à laquelle les volumes appartiennent. Dans une configuration en cluster, une tête entraîne un basculement en cas de panne des chemins principaux ou de substitution (voir « [Activation du basculement de tête](#) », page 19).

Définition de chemins d'unités LUN

En définissant un chemin d'unité LUN, vous déterminez le chemin d'unité LUN actif. celui-ci peut être le chemin principal ou le chemin de substitution. Pour optimiser les performances, il est préférable de choisir le chemin principal. Vous pouvez uniquement réaffecter une unité LUN quand elle ne comporte aucun système de fichiers. Dans un système cluster Sun StorEdge 5310, seul le serveur qui « détient » l'unité LUN est autorisé à la réaffecter à un autre serveur.

Remarque – Dans un système cluster Sun StorEdge 5310, lorsque vous démarrez pour la première fois le système, l'ensemble des unités LUN est affecté au même serveur (H1). Vous devez par conséquent utiliser le serveur H1 pour réaffecter certaines unités LUN au serveur H2 pour une répartition équitable.

Le panneau Set LUN Path vous permet de définir les chemins actifs. Dans un système Sun StorEdge 5310 Cluster, vous pouvez définir un chemin non affecté à partir de n'importe quel serveur.

▼ Pour définir un chemin de LUN

1. Dans le volet de navigation, sélectionnez **High Availability (Haute disponibilité) > Set LUN Path (Définition du chemin de LUN)**.

Remarque – Les unités LUN auxquelles aucun chemin LUN n'est attribué risquent de figurer plusieurs fois dans le panneau Set LUN Path (Paramétrage du chemin de l'unité LUN), étant donné que plusieurs contrôleurs signalent leur présence sur plusieurs chemins. Une fois qu'un chemin est attribué à une unité LUN, celle-ci ne s'affiche plus qu'une fois sur son chemin actuel.

2. Sélectionnez une unité LUN et cliquez sur **Edit (Modifier)**.
3. Dans la liste déroulante **Primary Path (Chemin principal)**, choisissez le contrôleur souhaité.

Exemple : L'option déroulante « 1/0 » affecte l'unité LUN sélectionnée au contrôleur 0 (C0). L'option prend la valeur « X/Y » : La valeur « X » est égale à 0 ou 1. 1 indique que le contrôleur est actif tandis que 0 indique qu'il est inactif.

Répartissez équitablement les attributions d'unités LUN entre les deux chemins disponibles. Par exemple, la première et la troisième à 1/0, et la deuxième et la quatrième à 1/1.

4. Cliquez sur **Apply (Appliquer)**.

▼ Pour restaurer un chemin d'unité LUN

Le chemin actif actuel d'une unité logique LUN n'est pas forcément son chemin principal. L'option de restauration du volet Set LUN Path (Paramétrage du chemin de l'unité LUN) permet de réinitialiser le chemin actif de l'unité logique LUN sur son chemin principal.

Remarque – La restauration d'un chemin d'unité logique LUN ne permet pas de récupérer des données : il ne s'agit pas d'une fonction de récupération en cas de défaillance.

1. Dans le volet de navigation, sélectionnez **High Availability (Haute disponibilité) > Set LUN Path (Définition du chemin de LUN)**.
2. Sélectionnez l'unité logique LUN et cliquez sur **Restore (Restaurer)**.

Activation du basculement

Remarque – Cette option n'est valide que pour les systèmes Sun StorEdge 5310 Cluster.

Un système cluster Sun StorEdge 5310 se compose d'une paire de serveurs actif/actif, appelés « têtes », lesquels partagent un accès aux contrôleurs RAID et à plusieurs autres réseaux. Les contrôleurs RAID sont connectés à chaque serveur par le biais de contrôleurs fibre. Un câble HB dédié connecte la première carte d'interface réseau (NIC) des deux serveurs et permet à chaque serveur de contrôler le statut de l'autre.

Dans le cadre d'un fonctionnement normal, chaque serveur fonctionne de manière autonome en ayant la charge d'un sous-ensemble de LUN. En cas de défaillance matérielle de l'un des serveurs impliquant qu'un chemin de données ne soit plus disponible, le serveur restant devient automatiquement propriétaire des adresses IP et des LUN auparavant gérées par le serveur en panne. Toutes les opérations du serveur défaillant, y compris la propriété du volume RAID et l'adressage de l'interface réseau, reviennent au serveur en service. Ce procédé est connu sous le nom de « basculement de tête ».

Suite à un basculement de cluster, les opérations client utilisant le protocole NFS/UDP sont transférées automatiquement pendant que le protocole NFS/TCP se reconnecte de manière transparente s'il s'agit d'une nouvelle tentative NFS. Le protocole CIFS nécessite également une reconnexion. Même si de nombreuses applications le font de manière transparente, informez l'utilisateur ou demandez-lui une confirmation avant de continuer.

Vous devez exécuter le processus de récupération, appelé « rétablissement », une fois que vous avez réparé et remis en marche le serveur en panne. Le volet Recover (Récupérer), accessible via High Availability (Haute disponibilité) > Recover (Récupérer), permet de déterminer les LUN gérées par chaque tête.

Activation du basculement de tête

En cas de basculement de tête, la tête qui fonctionne prend le contrôle temporaire des adresses et unités logiques LUN qui étaient gérées jusque-là par la tête défaillante.

Remarque – Lorsque vous activez le basculement de tête, le protocole DHCP est automatiquement désactivé.

▼ Pour activer le basculement de tête

1. Dans le volet de navigation, sélectionnez **High Availability (Haute disponibilité) > Enable Failover (Activer le basculement)**.

2. Cliquez sur la case **Automatic Failover (Basculement automatique)**.

3. Cochez la case **Enable Link Failover (Activer le basculement de liaison)**.

Activez le basculement de liaison pour qu'un basculement de tête ait lieu en cas de défaillance des interfaces réseau associées au rôle « principal ». Ce type de défaillance est appelé « défaillance de liaison ». En cas de défaillance de la liaison réseau d'une tête, l'autre tête qui veut activer le basculement doit respecter le délai défini après rétablissement par la tête défaillante de sa liaison réseau.

4. Saisissez les informations suivantes :

- **Down Timeout (Délai d'attente de l'arrêt)** : nombre de secondes pendant lesquelles la tête attend avant d'activer le basculement si la liaison réseau sur l'une des têtes devient instable alors que l'autre est dans un état satisfaisant.
- **Restore Timeout (Délai d'attente de la restauration)** : nombre de secondes pendant lesquelles la liaison principale de la tête de remplacement doit être active pour que le basculement ait lieu. La fonction Restore Timeout (Délai d'attente de la restauration) n'est utilisée que lorsqu'un basculement lié à une liaison défaillante a été lancé mais qu'il a ensuite été abandonné car la liaison principale était inactive.

5. Cliquez sur **Apply (Appliquer)** pour enregistrer vos paramètres.

6. Redémarrez les deux têtes.

Lancement du rétablissement

Le basculement de contrôleur a lieu automatiquement lorsqu'un contrôleur RAID est défaillant. Le contrôleur qui fonctionne gère momentanément les unités logiques LUN qui étaient gérées jusque là par le contrôleur défaillant.

Remarque – Le basculement de contrôleur est activé par défaut et ne peut pas être désactivé.

Lorsque la tête ou le contrôleur RAID en panne est remis(e) en marche, vous devez manuellement lancer la procédure de récupération (le rétablissement) de Sun StorEdge 5310 NAS Appliance ou du système Sun StorEdge 5310 Cluster après une panne de tête ou de contrôleur.

Un serveur en panne ayant entraîné le basculement peut, une fois qu'il est de nouveau entièrement opérationnel, reprendre possession de ses volumes de fichiers d'origine.

Par exemple, le volume A était assigné au serveur H1 qui a connu une défaillance. Le serveur H2 avait par conséquent pris possession du volume A pendant le basculement. Le serveur H1 étant à nouveau en service, il reprend possession du volume A à la place du serveur H2.



Attention – Vérifiez que le serveur défaillant est totalement fonctionnel avant de tenter une récupération.

▼ Pour lancer une récupération

1. **Dans le volet de navigation, sélectionnez High Availability (Haute disponibilité) > Recover (Récupérer) pour accéder au volet de récupération.**
2. **Pour procéder à une récupération de tête, dans la liste RAID, sélectionnez le RAID à récupérer.**
 - La liste Head 1 (Tête 1) identifie les mappages de LUN du serveur H1.
 - La liste Head 2 (Tête 2) (partenaire) identifie les mappages d'unités logiques LUN du serveur partenaire H2.
3. **Pour procéder à une récupération de contrôleur, dans la liste RAID, sélectionnez le RAID à récupérer.**
 - La liste Controller 0 (Contrôleur 0) identifie les mappages de LUN du contrôleur 0.
 - La liste Controller 1 (Contrôleur 1) identifie les mappages de LUN du contrôleur 1.

4. Cliquez sur Recover (Récupérer).

Le serveur réorganise les mappages d'unités logiques LUN de manière à ce qu'ils correspondent à la configuration présentée à l'écran.

Configuration des ports réseau

Vous avez la possibilité d'activer le protocole DHCP ou de spécifier, pour chaque port réseau, l'adresse IP, le masque de réseau, la diffusion et le rôle du port de la carte d'interface réseau (NIC) via le panneau Configure Network Adapters (Configuration des adaptateurs réseau). Vous pouvez également ajouter des adresses IP alias pour chaque port de la carte d'interface réseau.

Remarque – Chaque port de carte d'interface réseau Sun StorEdge 5310 Cluster doit être associé à un rôle.

Vous pouvez relier deux ports ou plus afin de créer une liaison de ports. Une liaison de ports dispose d'une bande passante plus importante que celle affectée aux différents ports qui constituent cette liaison. Pour obtenir plus d'informations et d'instructions sur la liaison des ports réseau, consultez la section « [Liaison de ports](#) », page 80.

Emplacements des ports de Sun StorEdge 5310 NAS Appliance

Sun StorEdge 5310 NAS Appliance identifie les ports dans un ordre prédéfini en fonction de leur type et de leur emplacement physique et logique sur le serveur. Reportez-vous au *Guide de démarrage de Sun StorEdge 5310 NAS Appliance et Gateway System* pour identifier l'emplacement des ports réseau en vue de leur configuration. Notez que les configurations système peuvent varier d'un système à l'autre et que celles indiquées dans le présent manuel ne sont fournies qu'à titre d'exemple.

La relation entre les cartes d'interface réseau (NIC) et les ports est indiquée dans le *Guide de démarrage de Sun StorEdge 5310 NAS Appliance et Gateway System*.

▼ Pour configurer des adaptateurs réseau

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Configure TCP/IP (Configuration TCP/IP) > Configure Network Adapters (Configuration des adaptateurs réseau)**.

2. Si votre réseau a recours à un serveur DHCP pour l'attribution des adresses IP et que vous souhaitez l'activer, cochez la case **Enable DHCP (Activer DHCP)**.

L'activation de ce protocole permet au système d'obtenir une adresse IP de manière dynamique à partir du serveur DHCP. Désélectionnez cette case pour saisir manuellement une adresse IP statique et un masque de réseau. Si vous n'activez pas le protocole DHCP et que le port fait partie d'une agrégation, le masque de réseau reste désactivé. Pour plus d'informations sur la création et la configuration d'agrégations de ports, reportez-vous à la section « [Liaison de ports](#) », page 80.

Remarque – Dans les systèmes cluster Sun StorEdge 5310, vous ne pouvez activer le protocole DHCP que si vous avez désactivé l'option de basculement de tête. Vous pouvez également affecter des adresses IP statiques aux ports afin d'assurer leur stabilité en cas de basculement.

3. **Sélectionnez le port à configurer dans la liste Adapter (Adaptateur).**

Si vous avez déjà créé une liaison de ports et souhaitez y ajouter des adresses IP alias, sélectionnez cette liaison dans la liste. (Pour plus d'informations sur la création de liaisons de ports, reportez-vous à la section « [Liaison de ports](#) », page 80.) Les ports indépendants se présentent sous la forme PORT x et les liaisons de port sous la forme LIAISON x .

Une fois une liaison de ports créée, vous pouvez uniquement ajouter des adresses IP alias à la liaison et non aux ports individuels.

4. **Entrez l'adresse IP de la liaison de ports ou du port sélectionné.**

5. **Entrez le masque de réseau de la liaison de ports ou du port sélectionné.**

Le masque de réseau sépare l'adresse IP en deux parties : une partie identifie l'adresse réseau alors que l'autre identifie l'adresse de l'hôte.

Le champ **Broadcast (Diffusion)** étant en lecture seule, sa valeur est automatiquement définie lorsque vous saisissez l'adresse IP et le masque de réseau. L'adresse de diffusion est une adresse IP utilisée pour la diffusion de messages à tous les ordinateurs du sous-réseau.

6. Pour chaque port, sélectionnez l'un des rôles suivants :

Rôles	Description
Primary	Identifie un port réseau actif.
Independent	Identifie un port réseau actif destiné à des fins autres que le traitement de données, notamment la sauvegarde.
Mirror	Indique que le port connecte ce serveur à un autre afin de créer des volumes de fichier miroir.
Private (Sun StorEdge 5310 Cluster uniquement)	Port réservé aux pulsations, une liaison réseau dédiée au contrôle continu du statut de l'autre tête. Chaque tête ne peut avoir qu'un seul port privé.

Remarque – Au moins un port doit disposer du rôle principal.

Pour plus de détails sur les rôles des ports, reportez-vous à la section « [Emplacement des ports](#) », page 77.

7. Pour ajouter une adresse IP alias au port sélectionné, entrez-la dans le champ **IP-Aliases (Alias IP)**. Cliquez ensuite sur le bouton **Add** pour l'ajouter à la liste correspondante (**IP-Aliases**).

Vous pouvez posséder jusqu'à 9 alias par interface dans un système à tête unique et 4, dans un système à deux têtes. Si vous devez supprimer un alias de la liste, sélectionnez-le et cliquez sur le bouton **Trash** (Corbeille). Cliquez sur **Apply** (**Appliquer**) pour enregistrer les modifications effectuées.

8. Répétez la procédure pour tous les ports de la liste **Adapter** (**Adaptateur**).

9. Cliquez sur **Apply** (**Appliquer**) pour enregistrer les modifications effectuées.

Définition de l'adresse de passerelle par défaut

L'adresse de passerelle par défaut est l'adresse IP de la passerelle ou du routeur du sous-réseau local qui permet la connexion aux autres sous-réseaux. La passerelle et le routeur sont des périphériques qui acheminent des données vers des hôtes distants. Vous devez indiquer l'adresse IP de la passerelle par défaut du système.

▼ Pour spécifier l'adresse de passerelle par défaut

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Configure TCP/IP (Configuration TCP/IP) > Set Gateway Address (Définition de l'adresse de passerelle)**.
2. Indiquez l'adresse de la passerelle dans la zone de texte **Gateway (Passerelle)**.
3. Cliquez sur **Apply (Appliquer)** pour enregistrer les paramètres.

Services de noms

Cette section décrit le paramétrage de la sécurité Windows, des services WINS, DNS, NIS et NIS+ ainsi que la configuration des services de noms.

Pour plus de détails sur les services de noms, reportez-vous au [Chapitre 6](#), section « [Active Directory Service et l'authentification](#) », page 87.

Configuration de la sécurité Windows

La configuration de domaine, de groupe de travail ou d'ADS (Active Directory Service) est une fonction Windows. Sous un environnement réseau UNIX, il n'est pas nécessaire de configurer les domaines ou les groupes de travail Windows.

Activez le groupe de travail Windows, la sécurité du domaine NT ou le service ADS via le panneau **Configure Domains and Workgroups (Configuration de domaines et de groupes de travail)**. Par défaut, le système est configuré en mode de groupe de travail Windows et a pour nom de groupe de travail « groupe de travail ».

▼ Pour configurer la sécurité Windows

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Domains and Workgroups (Configuration de domaines et de groupes de travail)**.

2. Sélectionnez l'option **Domain (Domaine)** pour activer la sécurité du domaine Windows.

Cette option crée un compte dans le domaine du serveur. Vous devez indiquer un compte utilisateur disposant des droits nécessaires pour ajouter des serveurs au domaine spécifié.

- a. Dans le champ **Domain (Domaine)**, entrez le nom du domaine.

Ce nom doit respecter la limitation NetBios qui est de 15 caractères.

- b. Dans les champs **User Name (Nom d'utilisateur)** et **Password (Mot de passe)**, saisissez le nom et le mot de passe de l'utilisateur du domaine d'administration.

Le nom d'utilisateur ne doit pas comporter plus de 16 caractères.

3. Pour activer la sécurité du groupe de travail Windows, sélectionnez l'option **Workgroup (Groupe de travail)**, puis saisissez le nom du groupe de travail dans le champ **Name (Nom)**.

Ce nom doit respecter la limitation de NetBios qui est de 15 caractères.

4. (Facultatif) Dans le champ **Comments (Commentaires)**, donnez une description du système Sun StorEdge 5310 NAS Appliance.

5. Pour activer le service ADS, cochez la case **Enable ADS (Activer ADS)**.

Pour plus de détails sur le service ADS, reportez -vous à la section « [Active Directory Service](#) », page 88.

Remarque – Avant d'activer le service ADS, vérifiez que l'horloge du système et celle des contrôleurs de domaine ADS pour Windows ne diffèrent pas de plus de cinq minutes. Pour vérifier l'heure, sélectionnez **System Operations (Opérations du système) > Set Time and date (Paramétrage de l'heure et de la date)** dans le volet de navigation.

- a. Dans le champ **Domain (Domaine)**, indiquez le domaine Windows dans lequel ADS est exécuté.

Le système doit appartenir à ce domaine.

- b. Dans le champ User Name (Nom d'utilisateur), entrez le nom d'un compte utilisateur Windows disposant des droits d'administrateur.**

Cet utilisateur doit être l'administrateur du domaine ou appartenir au groupe d'administrateurs du domaine. Le client ADS vérifie les mises à jour sécurisées du service ADS avec cet utilisateur.

Remarque – Si vous avez entré le nom de l'administrateur de domaine ici et que la mise à jour d'ADS a échoué, vous devez modifier le mot de passe de l'administrateur (dans le contrôleur de domaine). Cette opération n'est requise que pour l'administrateur et vous pouvez réutiliser le même mot de passe. Pour plus d'informations, consultez le site Web des services de support de Microsoft, article Q248808.

- c. Dans le champ Password (Mot de passe), saisissez le mot de passe de l'administrateur Windows.**

- d. Dans le champ Container (Conteneur), indiquez le chemin d'accès ADS de l'utilisateur administrateur de Windows sous la forme de nom distinctif (DN) LDAP (Lightweight Directory Access Protocol).**

Pour plus d'informations, reportez-vous à la section « [Active Directory Service](#) », page 88.

Remarque – N'incluez pas le nom de domaine dans le chemin.

- e. Si le domaine ADS utilise des sites, saisissez le nom de site approprié dans le champ Site. Sinon, laissez le champ Site vide. Si vous indiquez un site, il sera inclus lors de la sélection d'un contrôleur de domaine.**

- f. Dans la zone Kerberos Realm Info (Infos de domaine Kerberos), entrez le nom de domaine utilisé pour identifier ADS.**

Il s'agit généralement du domaine ADS ou du domaine DNS. Lorsque vous cliquez sur Apply (Appliquer), cette entrée est convertie en lettres majuscules.

- g. Dans le champ Server (Serveur), saisissez le nom d'hôte du serveur Kerberos KDC (Key Distribution Center, centre de distribution de clés).**

Il s'agit généralement du nom d'hôte du contrôleur de domaine principal dans le domaine ADS. Vous pouvez laisser ce champ vide si le système parvient à localiser le serveur KDC via le service DNS.

- 6. Cliquez sur Apply (Appliquer) pour enregistrer les paramètres.**

Si le mode de sécurité passe du mode de groupe de travail à celui du domaine NT, ou inversement, le serveur redémarre automatiquement lorsque vous cliquez sur Apply (Appliquer).

Paramétrage WINS

WINS (Windows Internet Name Service) est une fonction Windows. Sous un environnement réseau UNIX, il n'est pas nécessaire de configurer cette fonction.

▼ Pour paramétrer WINS

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Set Up WINS (Paramétrage WINS)**.

2. **Cochez la case Enable WINS (Activer WINS) pour activer le service correspondant.**

Si vous cochez cette case, le système devient un client WINS.

3. **Saisissez l'adresse IP du serveur WINS principal dans le champ prévu à cet effet.**

Ce serveur est le premier à être consulté lors de la résolution de noms NetBIOS.

4. **Indiquez le serveur WINS secondaire dans le champ prévu à cet effet.**

Si le serveur WINS principal ne répond pas, le système contacte le serveur WINS secondaire.

5. **Entrez l'identificateur d'étendue NetBIOS (facultatif) dans le champ Scope (Étendue).**

La définition d'une étendue empêche l'ordinateur de communiquer avec des systèmes qui ne correspondent pas à cette étendue. Par conséquent, faites attention lorsque vous manipulez ce paramètre. L'étendue s'avère particulièrement utile pour la division d'un groupe de travail Windows de grande taille en plus petits groupes. Si vous utilisez une étendue, l'ID de l'étendue doit respecter les conventions de nom NetBIOS ou de domaine. L'ID ne doit pas dépasser 16 caractères.

6. **Cliquez sur Apply (Appliquer) pour enregistrer les paramètres.**

Paramétrage DNS

Le système DNS (Domain Name System) convertit les noms d'hôtes en adresses IP pour Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System.

Remarque – Si vous utilisez ce service sans activer la fonction de DNS dynamique, ajoutez le nom d'hôte du serveur et son adresse IP à votre base de données DNS. En revanche, si vous utilisez cette fonction, il n'est pas nécessaire de mettre à jour manuellement la base de données DNS. Pour plus d'informations, consultez la documentation relative au service DNS.

▼ Pour configurer le DNS

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Configure TCP/IP (Configuration TCP/IP) > Set Up DNS (Paramétrage DNS)**.
2. **Cochez la case Enable DNS (Activer DNS)**.
3. **Entrez le nom de domaine du serveur DNS**.
4. **Indiquez l'adresse IP d'un serveur DNS que vous souhaitez rendre disponible sur le réseau, puis cliquez sur le bouton Add (Ajouter) pour ajouter ce serveur à la liste Server List.**

Répétez cette étape pour chaque serveur DNS à ajouter. Vous pouvez ajouter jusqu'à deux serveurs DNS à cette liste.

Le système interroge d'abord le serveur DNS qui figure en tête de la liste des serveurs pour la résolution du nom de domaine. Si ce serveur ne parvient pas à résoudre la requête, cette dernière est envoyée au serveur suivant de la liste.

5. **Pour réorganiser les serveurs DNS dans la liste, sélectionnez le serveur à déplacer, puis cliquez sur le bouton Up (Monter) ou Down (Descendre).**

Pour supprimer un serveur de la liste, sélectionnez son adresse IP et cliquez sur le bouton Trash (Corbeille).

6. **Cochez la case Enable Dynamic DNS (Activer le DNS dynamique) pour qu'un client DNS dynamique ajoute Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System à l'espace de noms DNS.**

N'activez pas cette option si votre serveur DNS ne prend pas en charge les mises à jour dynamiques. Vous devez également configurer le domaine (realm) Kerberos et le serveur KDC comme indiqué à la section « [Configuration de la sécurité Windows](#) », page 24. Lorsque vous activez l'option de DNS dynamique, des mises à jour dynamiques non sécurisées se produisent automatiquement sous réserve qu'elles soient autorisées par le serveur DNS.

7. **Si vous souhaitez activer les mises à jour DNS dynamiques sécurisées, vous devez fournir les informations ci-après. Cette obligation ne s'applique pas aux mises à jour non sécurisées.**

- a. **Dans le champ DynDNS User Name (Nom d'utilisateur DNSDyn), saisissez le nom d'un utilisateur Windows autorisé à effectuer les mises à jour DNS dynamiques sécurisées.**

Ce compte utilisateur doit impérativement être hébergé dans le domaine ADS ou Kerberos défini dans le panneau Configure Domains and Workgroups (Configuration de domaines et de groupe de travail) décrit à la section « [Configuration de la sécurité Windows](#) », page 24.

Remarque – Si vous avez entré le nom de l’administrateur de domaine ici et que la mise à jour du service ADS a échoué, l’administrateur de domaine doit modifier son mot de passe dans le contrôleur de domaine. Cette opération n’est requise que pour l’administrateur et vous pouvez réutiliser le même mot de passe. Pour plus d’informations, consultez le site Web des services de support de Microsoft, article Q248808.

b. Dans le champ DynDNS Password (Mot de passe DNSDyn), saisissez le mot de passe de l’utilisateur DNSDyn.

Si vous modifiez le contenu de ce champ, supprimez intégralement le mot de passe présent avant d’en entrer un nouveau.

8. Cliquez sur Apply (Appliquer) pour enregistrer les paramètres.

Paramétrage NIS

NIS (Network Information Service) est une fonction UNIX. Sous un environnement Windows uniquement, il n’est pas nécessaire de configurer cette fonction.

Le panneau **Set Up NIS (Paramétrage NIS)** vous permet d’activer le service NIS et de préciser le nom de domaine et l’adresse IP du serveur.

▼ Pour configurer le NIS

1. Dans le volet de navigation, sélectionnez UNIX Configuration (Configuration UNIX) > Set Up NIS (Paramétrage NIS).

2. Cochez la case Enable NIS (Activer NIS).

Lorsque cette option est activée, le système est activé en vue de l’importation de la base de données NIS contenant les informations relatives aux hôtes, utilisateurs et groupes.

3. Dans le champ Domain Name (Nom du domaine), indiquez le nom du domaine à employer pour les services NIS.

Respectez la convention d’attribution de nom DNS (par exemple, domain.com).

4. Dans le champ Server (Serveur), saisissez l’adresse IP ou le nom du serveur NIS.

La base de données est importée à partir de ce serveur.

Si vous ne connaissez pas l’adresse IP du serveur, laissez le champ **Server** (Serveur) vide. Toutefois, si aucune valeur n’est indiquée dans ce champ, vous devez cocher la case **Use Broadcast (Utiliser la diffusion)**. Lorsque l’option **Use Broadcast** est activée, l’adresse IP appropriée du serveur NIS est automatiquement incluse dans le champ.

5. Saisissez la fréquence (en minutes) à laquelle les informations NIS doivent être rafraîchies. La valeur par défaut est de 5 minutes.
6. Cochez la case **Use Broadcast (Utiliser la diffusion)** pour récupérer automatiquement l'adresse IP du serveur NIS.
7. Cochez la case **Update Hosts (Mettre à jour les hôtes)** afin de télécharger les informations concernant les hôtes du serveur NIS sur le système.
8. Cochez la case **Update Users (Mettre à jour les utilisateurs)** afin de télécharger les informations concernant les utilisateurs du serveur NIS sur le système.
9. Cochez la case **Update Groups (Mettre à jour les groupes)** afin de télécharger les informations concernant les groupes du serveur NIS sur le système.
10. Cochez la case **Update Netgroups (Mettre à jour les groupes réseau)** afin de télécharger les informations concernant les groupes réseau du serveur NIS sur le système.
11. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Paramétrage de NIS+

NIS+ (Network Information Service Plus) est une fonction UNIX. Sous un environnement Windows uniquement, il n'est pas nécessaire de configurer cette fonction.

Remarque – Il n'existe aucun rapport entre NIS+ et NIS. Les commandes ainsi que la structure de NIS+ sont différentes de celles de NIS.

▼ Pour configurer le NIS+

1. Pour assurer le bon fonctionnement de Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310, ou système de passerelle Sun StorEdge 5310 Gateway System dans un environnement NIS+, vous devez ajouter ce système au fichier de références d'hôte sur le serveur NIS+. Effectuez les opérations suivantes sur le serveur NIS+ :
 - a. Connectez-vous en tant que superutilisateur.

b. Entrez la commande suivante :

```
nisaddcred -p unix.SERVER@DOMAIN -P SERVER.DOMAIN. des
```

où *SERVER* désigne Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System system et *DOMAIN* correspond au domaine NIS+ auquel Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System va appartenir.

Remarque – Vous devez ajouter un point à la fin du nom du domaine uniquement pour l'occurrence placée après l'argument **-P**.

Par exemple, si Sun StorEdge 5310 NAS Appliance est dénommé **SS1** et qu'il appartient au domaine NIS+ sun.com, exécutez la commande suivante :

```
nisaddcred -p unix.ss1@sun.com -P ss1.sun.com. des
```

c. À l'invite, saisissez un mot de passe.

Celui-ci sera employé plus avant au cours de cette procédure, lors de la configuration du système en vue de l'utilisation de NIS+. Indiquez le mot de passe.

2. **Sur un client distant, accédez au système à partir de votre navigateur Web et connectez-vous à Web Administrator.**
3. **Dans le volet de navigation, sélectionnez UNIX Configuration (Configuration UNIX) > Set Up NIS+ (Paramétrage NIS+).**
4. **Cochez la case Enable NIS+ (Activer NIS+).**
5. **Dans le champ Home Domain Server (Serveur de domaine d'accueil), entrez l'adresse IP du serveur de domaine d'accueil NIS+.**
Si vous ne connaissez pas cette adresse, laissez le champ vide et cochez la case **Use Broadcast (Utiliser la diffusion)**. Lorsque cette option est sélectionnée, le système récupère automatiquement l'adresse IP appropriée pour le serveur de domaine d'accueil.
6. **Dans le champ NIS+ Domain (Domaine NIS+), indiquez le domaine d'accueil NIS+.**

Remarque – Les noms de domaine NIS+ doivent se terminer par un point (.).

7. **Saisissez le mot de passe d'appel de procédure à distance sécurisé pour le serveur NIS+.**

Il s'agit du mot de passe défini à l'étape 1c., [page 31](#).

8. **Précisez le chemin de recherche sous la forme d'une liste de domaines séparés par deux-points.**

Ce chemin détermine les domaines sur lesquels porteront les recherches NIS+. Si vous souhaitez effectuer des recherches uniquement dans le domaine d'accueil et ses parents, n'indiquez pas de chemin.

Par exemple, si le domaine NIS+ est **eng.sun.com.** et que le chemin de recherche est vide, le système commence par rechercher **eng.sun.com.** puis **sun.com.**, et ainsi de suite, lors de la résolution des noms. En revanche, si vous spécifiez un chemin de recherche tel que **sun.com**, le système n'effectue des recherches que dans le domaine **sun.com** pendant la résolution de noms.

9. **Si vous ne connaissez pas l'adresse IP du serveur de domaine d'accueil, cochez la case Use Broadcast (Utiliser la diffusion) (voir [étape 5](#)).**
10. **Cliquez sur Apply (Appliquer) pour enregistrer les paramètres.**

Configuration des services de noms

L'ordre de recherche des services de noms (NS) détermine l'ordre dans lequel s'effectue la recherche des services de noms pour la résolution d'une requête. Ces services de noms peuvent inclure les services LDAP, NIS, NIS+, DNS et locaux. Pour pouvoir utiliser les services sélectionnés en vue de la résolution de noms, vous devez les activer.

▼ Pour définir l'ordre de recherche des utilisateurs, groupes, groupes réseau et hôtes

1. **Dans le volet de navigation, sélectionnez UNIX Configuration (Configuration UNIX) > Configure Name Services (Configuration des services de noms).**
2. **Sous l'onglet Users Order (Ordre des utilisateurs), sélectionnez l'ordre de recherche des utilisateurs :**
 - a. **Dans la zone des services non sélectionnés, choisissez le service à utiliser pour la recherche d'utilisateurs.**
 - b. **Cliquez sur le bouton > afin de déplacer ce service vers la zone des services sélectionnés.**
 - c. **Répétez la procédure pour chacun des services employés dans la recherche d'utilisateurs.**
 - d. **Si vous souhaitez qu'un service ne soit plus inclus dans la recherche d'utilisateurs, sélectionnez-le et cliquez sur le bouton <.**

- e. Sélectionnez un à un, dans la zone des services sélectionnés, les services utilisés dans la recherche pour modifier leur ordre.
 - f. Cliquez sur les boutons Up (Monter) et Down (Descendre) pour déplacer chaque service vers le haut ou vers le bas. Le premier service utilisé lors de la recherche d'utilisateurs est celui qui figure en tête de la liste.
3. Sous l'onglet Groups Order (Ordre des groupes), sélectionnez les services utilisés dans la recherche de groupes, en suivant la procédure mentionnée à l'étape 2.
 4. De même, sous l'onglet Netgroup Order (Ordre des groupes réseau), sélectionnez les services utilisés dans la recherche de groupes réseau, en suivant toujours la procédure de l'étape 2.
 5. De même, sous l'onglet Hosts Order (Ordre des hôtes), sélectionnez les services utilisés dans la recherche d'hôtes, en suivant toujours la procédure de l'étape 2.
 6. Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.

Paramétrage de la notification par e-mail

Dans cet écran, vous allez définir le nom du serveur SMTP (Simple Mail Transfer Protocol) ainsi que les destinataires de la notification par e-mail. Lorsque le système détecte une erreur, il envoie une notification par e-mail.

Pour garantir la résolution de noms, vous devez avoir configuré le nom d'hôte du serveur SMTP dans le panneau **Configure Hosts (Configuration des hôtes)** (voir la section « [Configuration des hôtes](#) », page 99) ou paramétré le service DNS (voir la section « [Paramétrage DNS](#) », page 27).

▼ Pour paramétrer SMTP et envoyer des e-mails aux destinataires

1. Dans le volet de navigation, sélectionnez **Monitoring and Notification (Contrôle et notification) > Set Up Email Notification (Paramétrage de la notification par e-mail)**.
2. Indiquez le nom du serveur SMTP par lequel vous souhaitez envoyer la notification.
3. Dans le champ **Email Address (Adresse e-mail)**, saisissez l'adresse de messagerie de la personne à avertir automatiquement en cas d'erreurs système.

4. Précisez le type de message à envoyer à ce destinataire. Sélectionnez **Notification (Notification)**, **Diagnostics (Diagnostics)** ou les deux.
5. Cliquez sur le bouton **Add** pour ajouter le nouveau destinataire à la **List (Liste)** des destinataires. Recommencez la procédure de l'[étape 1](#) à l'[étape 4](#) pour chacun des destinataires. Il est possible d'indiquer jusqu'à quatre adresses e-mail.
Si vous devez supprimer un destinataire de la liste, sélectionnez-le et cliquez sur le bouton **Trash (Corbeille)**.
6. Choisissez le niveau de notification.
 - Cochez la case **Errors and Warnings (Erreurs et avertissements)** pour que les destinataires soient avertis de tous les avertissements et erreurs.
 - Cliquez sur **Errors Only (Seulement les erreurs)** pour avertir les destinataires des erreurs, mais pas des avertissements.
 - Cliquez sur **None (Aucune)** pour désactiver la fonction de notification.
7. Cliquez sur **Apply (Appliquer)** pour enregistrer les paramètres.

Paramétrage de la journalisation

L'activation de la journalisation à distance permet au système d'envoyer son journal au serveur désigné et/ou de l'archiver en local. Le serveur approprié doit être un serveur UNIX exécutant `syslogd`. Si vous souhaitez utiliser le nom de domaine comme référence à l'hôte de journalisation, vous devez configurer les paramètres DNS sur le système avant d'activer la journalisation à distance.



Attention – Vous devez activer la journalisation à distance ou créer un fichier journal sur un disque local pour que le journal ne soit pas supprimé lors de l'arrêt du système. À défaut, le système crée un fichier journal temporaire dans sa mémoire volatile au cours du démarrage. Cela suffit pour consigner les erreurs ayant pu se produire au cours du démarrage initial à des fins d'affichage ultérieur. En revanche, les messages ne seront pas conservés en cas de panne de courant ou de redémarrage du système.

▼ Pour paramétrer la journalisation en local ou à distance

1. Dans le volet de navigation, sélectionnez **Monitoring and Notification (Contrôle et notification) > View System Events (Affichage des événements système) > Set Up Logging (Paramétrage de la journalisation)**.
2. Cochez la case **Enable Remote Syslogd (Activer Syslogd à distance)**.
3. Si vous avez configuré les paramètres DNS, indiquez le nom de l'hôte DNS dans le champ **Server (Serveur)**. Sinon, entrez l'adresse IP. Le journal système sera envoyé à cette adresse.
4. Sélectionnez la fonction appropriée.

La fonction indique l'application ou le composant du système qui génère les messages. *Tous les messages envoyés au serveur syslogd seront dotés de cette valeur.* Les valeurs de fonction possibles dans le panneau **Set Up Remote Logging (Paramétrage de la journalisation à distance)** sont les suivantes :

Fonction	Description
Kern	Messages générés par le noyau. Ces messages ne peuvent pas être générés par d'autres processus utilisateur.
User	Messages générés par des processus utilisateur aléatoires. Il s'agit de l'identificateur de fonction par défaut lorsque aucune option n'est spécifiée.
Mail	Système de messagerie.
Daemon	Démons réseau ou système.
Auth	Systèmes d'autorisations, tels que la connexion.
Syslog	Messages générés en interne par syslogd.
Local0–Local7	Réservés à un usage local.

5. Sélectionnez le type d'événements système consignés en cochant le type d'événement approprié (voir la section « **Événements système** », page 160).
6. Cochez la case **Enable Local Log (Activer le journal local)** afin de mettre à jour le fichier journal local.
7. Entrez le chemin du fichier journal (répertoire du système dans lequel vous souhaitez stocker le fichier journal) et son nom de fichier dans le champ **Log File (Fichier journal)**.
8. Indiquez le nombre maximal de fichiers d'archive dans le champ **Archives (Archives)**.

La plage autorisée est comprise entre 1 et 9.

9. Entrez la taille de fichier maximale en kilooctets pour chaque fichier d'archive dans le champ **Size (Taille)**.
La plage autorisée est comprise entre 1 000 et 999,999 kilo-octets.
10. Cliquez sur **Apply (Appliquer)** pour enregistrer les paramètres.

Sélection de la langue

Le système d'exploitation prend en charge le jeu de caractères Unicode, lequel vous permet de définir la langue locale pour NFS et CIFS. Habituellement, vous définissez votre langue lors de l'installation initiale du système. Vous pouvez toutefois la définir ultérieurement, si nécessaire.

▼ Pour sélectionner la langue

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Assign Language (Sélection d'une langue)**.
2. Sélectionnez la langue locale à partir de la liste déroulante qui s'affiche.
3. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Sauvegarde des informations de configuration

Une fois la configuration du système terminée, sauvegardez les informations de configuration afin de vous protéger d'une éventuelle panne système. Reportez-vous à la section « [Sauvegarde de la configuration](#) », page 216 pour plus de détails sur la sauvegarde des informations de configuration.

Étapes suivantes

À ce stade, le système communique parfaitement avec le réseau. Cependant, avant que les utilisateurs ne démarrent le stockage de données, vous devez configurer le système de fichiers et établir les droits d'accès utilisateurs. Le chapitre suivant, « [Paramétrage et gestion du système de fichiers](#) », page 39, décrit la configuration d'un système de fichiers.

Pour obtenir des instructions détaillées sur la configuration des quotas, des partages, des exportations et d'autres contrôles d'accès, reportez-vous à la section « [Partages, quotas et exportations](#) », page 113.

Si vous souhaitez paramétrer une fonction spécifique, recherchez-la dans l'index afin de vous reporter aux instructions appropriées.

Paramétrage et gestion du système de fichiers

Le chapitre traite des concepts, du paramétrage et de la gestion du système de fichiers dans Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310.

Les sujets traités dans ce chapitre sont les suivants :

- « Concepts relatifs au système de fichiers », page 39
- « Création d'un système de fichiers », page 44
- « Création d'un volume de fichiers ou d'un segment », page 49
- « Reconstruction d'un LUN », page 53
- « Gestion de volumes de fichiers et de segments », page 54
- « Configuration iSCSI », page 59
- « Étapes suivantes », page 65

Concepts relatifs au système de fichiers

Quelques-uns des concepts et attributs de base utilisés dans le stockage NAS concernant le système de fichiers auxquels les sections suivantes font référence sont définis ci-après.

RAID

Les systèmes RAID (Redundant Array of Independent Disks) permettent la distribution de données dans plusieurs unités de disque par l'intermédiaire d'un contrôleur de baie et ce, afin d'obtenir des performances optimales, ainsi qu'une sécurité des données et une capacité de récupération accrues. Un système RAID représente la combinaison de plusieurs unités de disque physiques plus petites en

une unité volumineuse considérée comme unique par le réseau. Du point de vue de l'utilisateur, un volume RAID est similaire à une unité de disque. En revanche, pour l'administrateur système, le composant physique du RAID correspond à un groupe d'unités de disque, le RAID lui-même pouvant toutefois être administré en tant qu'unité distincte.

Il existe plusieurs types de configurations RAID. Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310 prennent uniquement en charge la configuration RAID 5. système de passerelle Sun StorEdge 5310 Gateway System prend en charge les configurations RAID 1, RAID 0+1 et RAID 5.

RAID 0 (configuration non prise en charge)

La configuration RAID 0 n'inclut pas la redondance pour laquelle la technologie RAID a été développée. Toutefois, elle offre une hausse significative des performances d'unités. RAID 0 fait appel au concept de *l'entrelacement*. Cela signifie que les données sont divisées en bandes. La première bande est écrite sur la première unité de disque, la bande suivante sur la deuxième unité et ainsi de suite. Le principal avantage de l'entrelacement est la possibilité, pour toutes les unités de disque de la baie, de traiter simultanément les lectures et les écritures. Du fait de cet accès simultané, les deux types d'opération sont beaucoup plus rapides.

Cependant, comme le RAID 0 ne présente aucune redondance, en cas de panne de disque, toutes les données de la baie entière risquent d'être perdues. L'utilisation de RAID 0 est idéale dans les cas où les performances sont prioritaires et les données perdues ont une moindre importance.

RAID 1 (système de passerelle Sun StorEdge 5310 Gateway System uniquement)

La *mise en miroir* d'unités de disque constitue le concept essentiel d'une baie RAID 1, qui multiplie par deux le nombre de disques requis pour fournir le même espace de stockage tout en offrant une sauvegarde actualisée de l'unité. Le disque mis en miroir est toujours connecté et est accessible très rapidement en cas de panne du disque principal. Chaque disque principal est mis en miroir avec un autre disque de la même taille. Toutes les opérations d'écriture sont dupliquées et consignées simultanément sur les deux membres de la baie RAID 1. RAID 1 offre une excellente haute disponibilité. Une configuration RAID 1 s'avère très pratique dans les situations où la sécurité et l'intégrité des données sont capitales alors que les performances importent moins.

RAID 0+1 (système de passerelle Sun StorEdge 5310 Gateway System uniquement)

La configuration RAID 0+1 combine deux concepts RAID en vue d'accroître à la fois les performances et la haute disponibilité : l'entrelacement et la mise en miroir. Les paires de disques mis en miroir sont intégrés à une baie de type RAID 0. Toutes les opérations d'écriture sont dupliquées et consignées simultanément sur les deux disques mis en miroir. L'entrelacement de la configuration RAID 0 accroît les performances globales de la baie tandis que la mise en miroir de disques (configuration RAID 1) offre une excellente haute disponibilité pour chaque disque. La configuration RAID 0+1 s'avère un bon choix pour les environnements dans lesquels la sécurité est prioritaire par rapport aux performances, mais où ces dernières sont néanmoins importantes.

RAID 5

La baie de disques RAID 5 constitue la meilleure solution tant au niveau de l'amélioration des performances liées à l'entrelacement que de la redondance de la mise en miroir, tout en évitant à l'utilisateur de doubler le nombre d'unités de disque de la baie globale.

La configuration RAID 5 utilise des informations relatives à l'entrelacement et à la *parité*. Les données de parité sont créées en associant des bits dans les informations à stocker puis en générant une petite quantité de données de laquelle peuvent être extraites les autres informations. En d'autres termes, les données de parité sont identiques aux données d'origine de sorte que l'ensemble initial complet puisse être reproduit en cas de perte par la simple combinaison des informations restantes et des données de parité. Les informations de parité ne sont pas stockées sur un disque particulier. Au lieu de cela, un disque différent du jeu d'entrelacement est utilisé pour la protection de la parité de différentes zones du jeu RAID 5.

La baie de disques RAID 5 inclut les informations de parité dans une bande spécialement dédiée. Si un problème survient avec l'une des unités de disque de la baie, les données de parité et la partie restante des données d'origine issue des unités non affectées servent à reconstituer les informations manquantes sur l'unité défectueuse. Ainsi, la baie de disques RAID 5 combine la haute disponibilité de la mise en miroir et les performances des bandes, ce qui fait d'elle le type RAID global idéal. En outre, elle présente l'avantage de nécessiter très peu d'espace « supplémentaire » pour le stockage des données de parité et constitue ainsi une solution moins coûteuse.

Le premier boîtier avec des unités dans chaque baie (les unités d'extension 5300 EU RAID pour baies Fibre Channel ou la première unité d'extension EU S connectée à l'unité 5300 RAID vide pour les baies SATA) contient deux groupes de six unités (5+1) RAID 5 plus deux disques hot spare de rechange. Les autres boîtiers d'extension EU F ou EU S contiennent un ou deux groupes de sept unités (6+1) RAID 5 pour un total de 7 ou 14 unités.



Attention – Il est déconseillé de mettre à jour les logiciels système ou les microprogrammes RAID lorsque l'état du sous-système RAID est critique, ou lors de la création d'un volume ou de la reconstitution d'un volume existant.

LUN

Un numéro d'unité logique (LUN, logical unit number) permet d'identifier la représentation logique d'un périphérique physique ou virtuel. Dans Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310, une correspondance bi-univoque est établie entre les jeux RAID et les unités logiques. Néanmoins, le système gère les LUN en tant qu'entités indépendantes et traite chacune d'elle comme un volume de stockage unique.

En traitant les LUN de cette manière, Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310 facilitent nettement le processus de constitution d'un système de fichiers. L'accès à l'espace disponible sur le jeu RAID par le biais du LUN permet de ne pas tenir compte des limites de l'unité physique.

La gestion des ressources de stockage s'effectue par le biais du LUN, rarement directement avec les jeux RAID eux-mêmes. Pour obtenir des instructions et des informations complémentaires sur le paramétrage des jeux RAID et des LUN, reportez-vous à la section « [Création de jeux RAID et de LUN](#) », page 44.

Partition

Les partitions sont des sections de LUN qui permettent de subdiviser la quantité totale d'espace disponible dans un LUN. Les systèmes d'exploitation de Sun StorEdge 5310 NAS Appliance et de cluster Sun StorEdge 5310 prennent en charge jusqu'à 31 partitions par LUN.

Au moment de la création d'un LUN, l'intégralité de l'espace disponible se situe dans la première partition, les autres partitions éventuelles étant vides. Pour pouvoir utiliser l'espace d'une partition, vous devez créer un volume de fichiers.

Chaque partition ne peut contenir qu'un seul volume de fichiers, mais celui-ci peut s'étendre sur plusieurs partitions. Lorsque vous créez un volume de fichiers, la taille de la partition est automatiquement ajustée de manière à correspondre à celle dudit volume. L'espace supplémentaire sur le LUN est systématiquement affecté à la partition suivante. Une fois que vous avez mis au point tous les volumes de fichiers compatibles avec le système d'exploitation, l'espace encore disponible sur le LUN devient inaccessible.

Vous pouvez augmenter la taille d'un volume de fichiers en rattachant un segment (voir la section « [Segment](#) », page 43). Un segment est en fait un autre volume de fichiers doté de caractéristiques spéciales. Lorsque vous ajoutez un segment à un volume, les deux éléments se confondent et la seule différence pour l'utilisateur est un espace plus important sur le volume. Grâce à la flexibilité de ce système, vous pouvez créer un volume de fichiers, puis l'étendre en fonction de vos besoins sans que les utilisateurs n'en soient perturbés ni ne soient forcés de répartir leurs données sur plusieurs volumes.

En effet, si l'administrateur système ajoute des unités de disque ou des unités logiques LUN, cela se traduit uniquement, pour l'utilisateur, par une quantité d'espace supplémentaire sur le volume.

Volume de fichiers

Les volumes de fichiers définissent les espaces disponibles pour le stockage des informations. Ils sont créés à partir des partitions qui disposent d'espace. Si le volume n'exploite pas tout l'espace disponible dans une partition, l'espace restant est automatiquement alloué à la partition suivante. La taille des nouveaux volumes de fichiers ne doit pas dépasser 255 Go. Si vous souhaitez définir un volume de fichiers plus grand, vous pouvez créer et rattacher jusqu'à 63 segments (voir la section « [Segment](#) », page 43) au volume de fichiers initial.

Du point de vue de l'utilisateur, le volume de fichiers et ses structures de répertoires sont la priorité. Si le volume de fichiers vient à saturer, l'administrateur peut rattacher un autre segment et augmenter ainsi la quantité d'espace disponible sur le volume. Cela peut impliquer l'ajout d'unités supplémentaires, voire d'unités d'extension. Toutefois, ces contraintes matérielles ne sont pas connues de l'utilisateur. Ce dernier constate simplement que le volume dispose d'une quantité d'espace de stockage supplémentaire.

Segment

Les segments sont des « volumes » d'espace de stockage créés de manière similaire aux volumes de fichiers. Vous avez la possibilité de rattacher des segments à un volume de fichiers à tout moment. En rattachant un segment, vous augmentez la capacité totale du volume de fichiers initial. Chaque segment doit être créé séparément, puis rattaché à un volume de fichiers. Une fois le rattachement effectué, le volume et le segment sont indissociables.

En règle générale, les segments sont créés au fur et à mesure des besoins et rattachés aux volumes proches de la saturation. Le principal avantage que présente l'ajout d'espace par rattachement de segments est la possibilité de créer le segment sur un nouveau disque, voire une nouvelle baie. Une fois le segment rattaché au volume de fichiers initial, les différents emplacements de stockage physiques ne sont pas visibles pour l'utilisateur. Une quantité d'espace supplémentaire peut donc être ajoutée si nécessaire, sans nécessiter d'interruption du réseau en vue de la restructuration du stockage des données et de la création d'un volume de fichiers plus grand.

Création d'un système de fichiers

Si vous configurez un système système de passerelle Sun StorEdge 5310 Gateway System, servez-vous des outils de configuration de système de stockage en vue de créer des disques hot spare et des LUN. Consultez la documentation fournie avec le système de stockage connecté à la passerelle.

Si vous configurez un appareil Sun StorEdge 5310 NAS Appliance ou un système Cluster, reportez-vous aux sections « [Création de jeux RAID et de LUN](#) », page 44 et « [Conversion d'un disque en disque hot spare](#) », page 48.

Création de jeux RAID et de LUN

Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310 combinent la création et la définition du jeu RAID sous la forme d'une seule opération : la définition du LUN (voir « [Concepts relatifs au système de fichiers](#) », page 39 pour plus d'informations). En effet, vous créez les deux objets simultanément. Les systèmes Sun StorEdge 5310 NAS Appliance et Cluster vous permettent de choisir la structure de base du jeu RAID et définissent le LUN, automatisant ainsi les diverses tâches habituellement associées à la définition de ce type de jeu.



Attention – Utilisateurs de Sun StorEdge 5310 Cluster : chaque serveur gère ses propres LUN. Avant d'ajouter des LUN, assurez-vous que la fonction de basculement est activée et configurée. Pour plus de détails à ce sujet, reportez-vous à la section « [Activation du basculement](#) », page 18.

Les systèmes Sun StorEdge 5310 NAS Appliance et Cluster automatisent également la définition de partitions. Cette opération a lieu lors de la création d'un LUN. Au départ, les systèmes Sun StorEdge 5310 NAS Appliance et Cluster se voient assigner deux disques hot spare et au moins deux LUN par défaut.

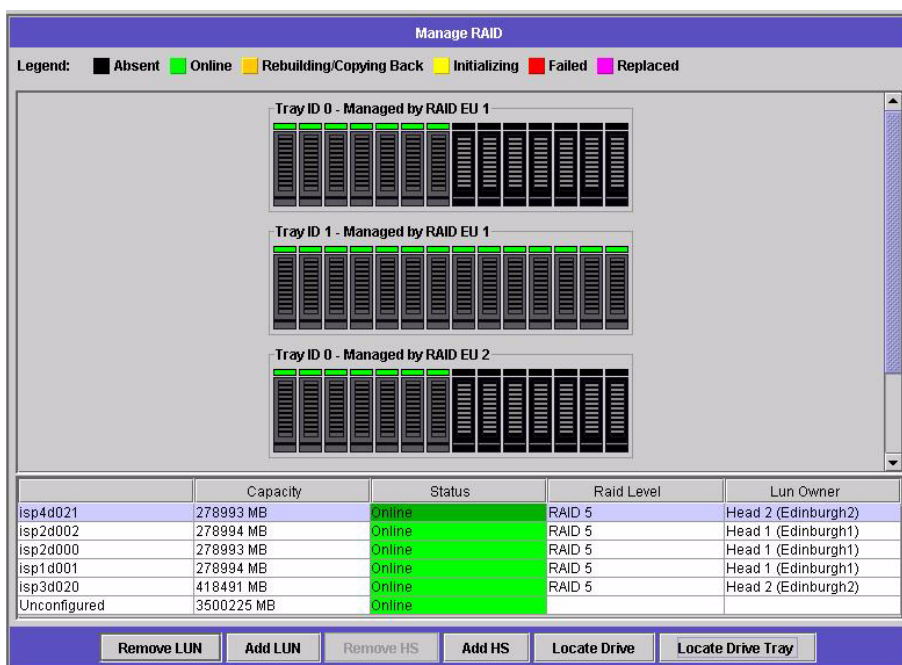
Les jeux RAID et les LUN sont créés en même temps dans les systèmes Sun StorEdge 5310 NAS Appliance et Cluster dans un souci de facilité.

Lorsque vous ajoutez un LUN, assurez-vous de n'avoir affecté aucune autre fonction à ses disques (par exemple, fonction hot spare) avant sa création. Les unités de disque assignées à un autre LUN ou jouant le rôle de disque hot spare ne peuvent pas faire partie d'un nouveau LUN.

▼ Pour ajouter une nouvelle LUN

1. Dans le volet de navigation, sélectionnez RAID > Manage RAID (Gestion des systèmes RAID).

Le panneau correspondant (Manage RAID) s'affiche.



The screenshot shows the 'Manage RAID' interface. At the top, there is a legend with color-coded boxes: Absent (black), Online (green), Rebuilding/Copying Back (yellow), Initializing (orange), Failed (red), and Replaced (magenta). Below the legend, there are three RAID trays, each with 10 drive slots. The first two trays are managed by RAID EU 1, and the third is managed by RAID EU 2. Below the trays is a table with the following data:

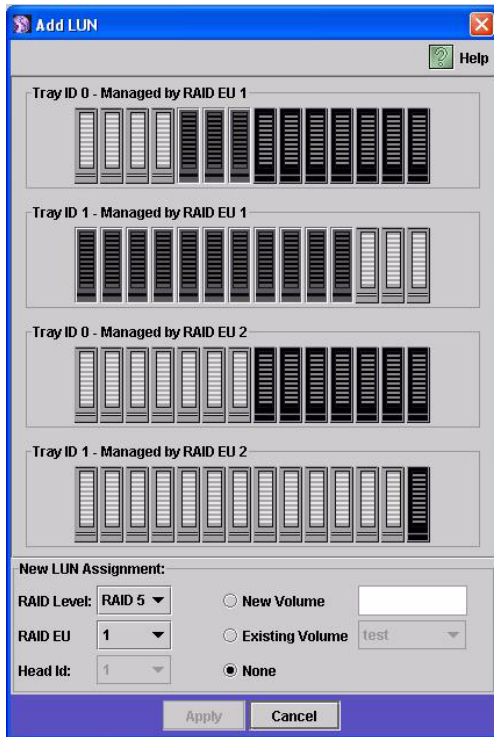
	Capacity	Status	Raid Level	Lun Owner
isp4d021	278993 MB	Online	RAID 5	Head 2 (Edinburgh2)
isp2d002	278994 MB	Online	RAID 5	Head 1 (Edinburgh1)
isp2d000	278993 MB	Online	RAID 5	Head 1 (Edinburgh1)
isp1d001	278994 MB	Online	RAID 5	Head 1 (Edinburgh1)
isp3d020	418491 MB	Online	RAID 5	Head 2 (Edinburgh2)
Unconfigured	3500225 MB	Online		

At the bottom of the interface, there are six buttons: Remove LUN, Add LUN, Remove HS, Add HS, Locate Drive, and Locate Drive Tray.

Remarque – Pour identifier un disque ou une baie, vous pouvez cliquer sur le bouton Locate Drive (Localiser le disque) ou Locate Drive Tray (Localiser le plateau de disques), ce qui déclenchera le clignotement de l'indicateur LCD du disque ou du plateau concerné.

2. Cliquez sur Add LUN (Ajout d'une unité LUN).

La fenêtre correspondante s'affiche.






3. Dans le menu déroulant RAID EU, sélectionnez le numéro du contrôleur auquel vous souhaitez ajouter un LUN.

4. Sélectionnez les unités de disque à inclure dans le LUN en cliquant sur les images correspondantes.

Vous devez choisir au moins trois unités. Les images représentant les unités indiquent l'état de celles-ci.

TABLEAU 3-1 Indicateurs d'état des unités de disque de la boîte de dialogue Add LUN (Ajout d'une unité LUN)

Disque	Signification
	L'unité de disque située à cet emplacement est disponible en vue de son inclusion dans un LUN.
	L'unité de disque située à cet emplacement a été sélectionnée pour être incluse dans un LUN.
	Aucune unité de disque n'est présente à cet emplacement.

5. Choisissez l'une des options de volume suivantes.

Option	Description
New Volume	Cette option permet de créer un volume pour le LUN. Le LUN entier sera utilisé pour la création du volume. Indiquez un nom pour le nouveau volume à l'endroit prévu à cet effet.
Existing Volume	Sélectionnez cette option si l'objectif du LUN est l'ajout d'une quantité d'espace disque supplémentaire à un volume existant (via la création et le rattachement d'un segment). Sélectionnez ensuite le volume en cours d'extension dans le menu déroulant.
None	Cette option permet de créer un LUN sans lui assigner de nom.

6. Cliquez sur Apply (Appliquer) pour ajouter la nouvelle LUN.

Sa création n'est prise en compte par le système qu'au bout de quelques heures.

Conversion d'un disque en disque hot spare

Vous pouvez configurer un disque en tant que disque hot spare pour le système Sun StorEdge 5310 Appliance ou Cluster.




▼ Pour convertir un disque en disque hot spare

1. Dans le volet de navigation, sélectionnez RAID > Manage RAID (Gestion des systèmes RAID).
2. Cliquez sur le bouton Add HS (Ajouter HS) situé au bas de l'écran.
3. Sélectionnez le disque voulu en cliquant sur l'image correspondante.

Veillez à ce que la taille du disque que vous choisissez comme disque hot spare soit au moins égale à celle du disque le plus volumineux parmi toutes les LUN du serveur.

Les images représentant les disques indiquent l'état associé.

TABLEAU 3-2 Images représentant l'état des disques hot spare ajoutés

Disque	Signification
	Le disque situé à cet emplacement peut devenir un disque hot spare.
	Le disque situé à cet emplacement a été sélectionné pour être converti en disque hot spare.
	Aucun disque n'est présent à cet emplacement.

4. Cliquez sur Apply (Appliquer) pour ajouter le nouveau disque hot spare.

Création d'un volume de fichiers ou d'un segment

La taille des nouveaux volumes de fichiers ne doit pas dépasser 255 Go. Si vous souhaitez créer un volume de fichiers plus grand, vous pouvez ajouter au volume principal jusqu'à soixante-trois segments. Dans ce cas, commencez par créer le volume principal, puis le nombre de segments voulu (inférieur ou égal à 63). Rattachez ensuite les segments au volume principal afin d'augmenter sa taille.

Il est possible de créer un volume de fichiers ou un segment par l'intermédiaire du panneau Create File Volumes (Création de volumes de fichier) ou de System Manager (Gestionnaire système).

▼ Pour créer un volume de fichiers ou un segment par l'intermédiaire du panneau Create File Volumes (Création de volumes de fichiers)

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Create File Volumes (Création de volumes de fichiers)**.
2. Si vous venez d'ajouter des disques au système direct (live) sans effectuer de redémarrage, cliquez sur le bouton **Scan For New Disks (Détection de nouveaux disques)**.
3. Dans la zone LUN, sélectionnez le LUN dans lequel créer le volume de fichiers principal.
Le nombre de partitions du volume de fichiers indiqué dans la liste déroulante **Partition** augmente automatiquement au moment de la création du volume de fichiers.
4. Indiquez un nom pour le nouveau volume ou segment dans le champ **Name (Nom)**.
Les caractères valides sont les chiffres et les lettres (a-z, A-Z, 0-9). Le nom ne doit pas comporter plus de 12 caractères et doit commencer par une lettre (a-z, A-Z).
5. Dans le menu déroulant, choisissez l'unité de taille du volume de fichiers : **MB (méga-octets) ou GB (giga-octets)**.
6. Dans le champ **Size (Taille)**, précisez la taille du volume de fichiers sous la forme d'un nombre entier.
La quantité totale d'espace disponible figure juste en dessous de ce champ.

7. Sélectionnez le type du volume de fichiers (Primary (Principal) ou Segment (Segment)).
8. Si l'option Compliance Archiving Software (Logiciel d'archivage en conformité) est installée et que vous souhaitez créer un volume où la conformité est activée, dans la section Compliance (Conformité), cliquez sur Enable (Activer). Indiquez ensuite le type de mise en conformité requis.
 - Si vous sélectionnez Mandatory Enforcement (Application obligatoire), la durée de conservation par défaut sera permanente. La modification à l'aide de droits administratifs n'est pas autorisée.



Attention – Une fois que vous avez activé sur un volume l'archivage en conformité avec application obligatoire, il est impossible de supprimer et de renommer ce volume, de désactiver l'archivage en conformité ou de revenir au niveau de l'application consultative.

- Si vous sélectionnez Advisory Enforcement (Application consultative), la durée de conservation par défaut sera de 0 jour. La modification à l'aide de droits administratifs est autorisée dans ce cas.

Remarque – La diminution de la durée de conservation et la suppression des fichiers conservés avant l'échéance de la période de conservation définie doivent être effectuées par l'utilisateur racine (root) et ce, à partir d'un hôte de confiance. Reportez-vous à la section « [Gestion des hôtes de confiance](#) », page 244.

Pour plus d'informations, reportez-vous à la section « [Compliance Archiving Software](#) », page 148.

9. Cliquez sur Apply (Appliquer) pour créer le volume de fichiers ou le segment.

▼ Pour créer un volume de fichiers ou un segment à l'aide du System Manager (Gestionnaire système)

1. Dans le volet de navigation, cliquez à l'aide du bouton droit de la souris sur System Manager (Gestionnaire système).
2. Dans le menu contextuel, choisissez Create Volume (Créer un volume) ou Create Segment (Créer un segment) afin d'ouvrir la boîte de dialogue correspondante.

3. **Dans la zone LUN, cliquez sur le LUN dans lequel créer le volume de fichiers principal.**
Le nombre de partitions du volume de fichiers indiqué dans la liste déroulante **Partition** augmente automatiquement au moment de la création du volume de fichiers.
4. **Indiquez un nom pour le nouveau volume ou segment dans le champ Name (Nom).**
Les caractères valides sont les chiffres et les lettres (a-z, A-Z, 0-9). Le nom ne doit pas comporter plus de 12 caractères et doit commencer par une lettre (a-z, A-Z).
5. **Dans le menu déroulant, choisissez l'unité de taille du volume de fichiers : MB (méga-octets) ou GB (giga-octets).**
6. **Dans le champ Size (Taille), précisez la taille du volume de fichiers sous la forme d'un nombre entier.**
La quantité totale d'espace disponible figure juste en dessous de ce champ.
7. **Sélectionnez le type du volume de fichiers (Primary (Principal) ou Segment (Segment)).**
8. **Si l'option Compliance Archiving Software (Logiciel d'archivage en conformité) est installée et que vous souhaitez créer un volume où la conformité est activée, dans la section Compliance (Conformité), cliquez sur Enable (Activer). Indiquez ensuite le type de mise en conformité requis.**
 - Si vous sélectionnez Mandatory Enforcement (Application obligatoire), la durée de conservation par défaut sera permanente. La modification à l'aide de droits administratifs n'est pas autorisée.



Attention – Une fois que vous avez activé sur un volume l'archivage en conformité avec application obligatoire, il est impossible de supprimer ou de renommer ce volume, de désactiver l'archivage en conformité ou encore de revenir au niveau de l'application consultative.

- Si vous sélectionnez Advisory Enforcement (Application consultative), la durée de conservation par défaut sera de 0 jour. La modification à l'aide de droits administratifs est autorisée dans ce cas.

Remarque – La diminution de la durée de conservation et la suppression des fichiers conservés avant l'échéance de la période de conservation définie doivent être effectuées par l'utilisateur racine (root) et ce, à partir d'un hôte de confiance. Reportez-vous à la section « [Gestion des hôtes de confiance](#) », page 244.

Pour plus d'informations, reportez-vous à la section « [Compliance Archiving Software](#) », page 148.

9. **Cliquez sur Apply (Appliquer) pour créer le volume de fichiers ou le segment.**

Rattachement de segments à un volume de fichiers principal

Le rattachement de segments à un volume de fichiers principal permet d'augmenter la taille du volume. Le segment est associé de manière permanente au volume et ne peut pas être supprimé. Pour pouvoir attacher un segment à un volume, vous devez d'abord l'avoir créé. Pour les instructions, reportez-vous à la section « [Création d'un volume de fichiers ou d'un segment](#) », page 49.



Attention – Il est impossible d'annuler le rattachement d'un segment à un volume de fichiers principal.

La taille d'un volume de fichiers standard est limitée à 255 Go, mais peut être augmentée grâce au rattachement de 63 segments maximum, issus d'un LUN. La taille de chaque segment doit être comprise entre 8 Mo et 255 Go.

Le rattachement d'un segment peut être effectué par le biais du panneau Attach Segments (Rattachement de segments) ou de System Manager (Gestionnaire système).



Attention – Les volumes sur lesquels la conformité avec application obligatoire est activée ne peuvent pas être supprimés. Si vous ajoutez un segment à un volume sur lequel la conformité avec application obligatoire est activée, vous ne pourrez plus ni supprimer ni récupérer l'espace occupé par le segment.

▼ Pour rattacher un segment via le panneau Attach Segments (Rattachement de segments)

1. Sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Attach Segments (Rattachement de segments)** pour ouvrir le panneau **Attach Segments (Rattachement de segments)**.
2. Dans la zone **Existing Volumes (Volumes existants)**, cliquez sur le volume souhaité.
3. Dans la zone **Available Segments (Segments disponibles)**, sélectionnez le segment voulu.
4. Cliquez sur **Apply (Appliquer)** pour valider le rattachement.

▼ Pour rattacher un segment via System Manager (Gestionnaire système)

1. Dans le volet de navigation, cliquez sur System Manager (Gestionnaire système) afin d'afficher les volumes existants.
2. Cliquez sur le volume de fichiers voulu avec le bouton droit de la souris puis, dans le menu contextuel, sélectionnez Attach Segment (Rattacher un segment).
3. Cliquez sur le segment souhaité.
Vous ne pouvez sélectionner et rattacher qu'un seul segment à la fois.
4. Cliquez sur Apply (Appliquer) pour rattacher le segment sélectionné.
5. Recommencez les opérations 3 et 4 jusqu'à ce que vous ayez ajouté tous les segments voulus.

Reconstruction d'un LUN

Si l'un des LUN tombe en panne, la DEL associée devient orange en continu, indiquant qu'elle est en attente de remplacement.

Remarque – La reconstruction de LUN ne s'applique pas aux configurations système de passerelle Sun StorEdge 5310 NAS Gateway System.

Si un disque hot spare est disponible, le jeu RAID associé au disque en panne sera reconstruit à l'aide de ce disque hot spare. Tous les disques associés à la reconstruction voient les DEL associées clignoter en vert. Ils ne doivent pas être retirés pendant toute la durée de l'opération. Une reconstruction similaire aura lieu lors du remplacement du disque, quand le nouveau disque sera réinséré dans le jeu RAID et que le disque hot spare sera revenu en mode veille. La reconstruction peut prendre plusieurs heures.

Si votre système ne contient pas de disque hot spare, vous devez retirer l'unité de disque en panne et la remplacer par une unité de disque d'une capacité au moins égale à celle déjà installée. Consultez l'[Annexe D](#) pour en savoir plus sur le remplacement d'une unité de disque en panne.

Une fois le remplacement effectué, le contrôleur RAID reconstruit automatiquement le LUN. La reconstruction peut nécessiter plusieurs heures, selon la capacité du disque. Au cours de cette opération, les DEL du LUN clignotent en orange.

Gestion de volumes de fichiers et de segments

Les tâches de gestion du système de fichiers sont les suivantes :

- « [Modification des propriétés du volume de fichiers](#) », page 54
- « [Suppression de volumes de fichiers](#) », page 57
- « [Affichage des partitions de volume](#) », page 58

Modification des propriétés du volume de fichiers

Vous avez la possibilité de modifier les propriétés d'un volume de fichiers via le panneau Edit Properties (Modifier les propriétés).

Remarque – Il est impossible de renommer les volumes sur lesquels la conformité avec application obligatoire est activée ou de désactiver la fonction d'archivage en conformité ou encore de revenir à l'option de conformité avec application consultative.

▼ Pour renommer un volume, activer les points de contrôle et les quotas, ou modifier les propriétés de conformité

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Edit Properties (Modifier les propriétés)**.
2. Dans la liste **Volumes**, sélectionnez le nom du volume à modifier.
3. Dans le champ **New Name (Nouveau nom)**, saisissez le nouveau nom du volume (le cas échéant).

Les caractères valides sont les chiffres et les lettres (a-z, A-Z, 0-9). Le nom ne doit pas comporter plus de 12 caractères et doit commencer par une lettre (a-z, A-Z).

4. Sélectionnez l'une ou les deux options suivantes pour ce volume.

Option	Description
Enable Checkpoints	(Activer les points de contrôle) : cochez cette case si vous souhaitez créer des points de contrôle pour ce volume de fichiers. Par défaut, cette option est activée lors de la création d'un volume de fichiers.
Enable Quotas	(Activer les quotas) : cochez cette case si vous souhaitez activer les quotas du volume choisi. Par défaut, cette option est désactivée lors de la création d'un volume de fichiers.
Enable Attic	(Activer le répertoire Attic) : cochez cette case pour enregistrer temporairement les fichiers supprimés dans le répertoire <code>.attic\$</code> situé à la racine de chaque volume. Par défaut, cette option est activée. Dans des systèmes de fichiers très occupés, il arrive parfois que le répertoire <code>.attic\$</code> soit saturé avant que les opérations de suppression ne soient terminées, ce qui entraîne un manque d'espace disponible et une baisse des performances. Dans ce cas, désactivez le répertoire <code>.attic\$</code> en désélectionnant cette case à cocher.

5. Si la fonction de conformité est activée sur le volume, plusieurs options de la section Compliance Archiving Software sont à votre disposition, selon le niveau de conformité choisi.



Attention – Dans le cas des volumes dont la fonction de conformité avec application obligatoire est activée, la durée de conservation par défaut est « Permanent » (permanente). Dans le cas des volumes dont la fonction de conformité avec application consultative est activée, la durée de conservation par défaut est de zéro jour. Si vous souhaitez définir une durée de conservation par défaut différente, spécifiez la nouvelle période *avant* de commencer à utiliser le volume.



Attention – Une fois que vous avez activé sur un volume l'archivage en conformité avec application obligatoire, il est impossible de supprimer ou de renommer ce volume, de désactiver l'archivage en conformité ou encore de revenir au niveau de l'application consultative.

Pour plus d'informations, reportez-vous à la section « [Compliance Archiving Software](#) », page 148.

Option	Description
Mandatory Enforcement	(Application obligatoire) : si la fonction de conformité avec application consultative est activée sur le volume, vous pouvez sélectionner cette option pour choisir l'application obligatoire.
Advisory Enforcement	(Application consultative) : si la fonction de conformité avec application obligatoire est activée sur le volume, vous ne pouvez pas modifier ce paramètre et cette option est indisponible.
Permanent Retention	(Conservation permanente). Option par défaut. Si vous préférez que les données ne soient pas conservées de manière permanente, vous devez sélectionner l'option Retain for <i>nn</i> Days (Conserver pendant xx jours) avant d'utiliser le volume. Sélectionnez cette option afin de conserver de manière permanente les données sur ce volume.
Retain for <i>nn</i> Days	(Conserver pendant xx jours) : sélectionnez cette option et utilisez le menu déroulant afin de spécifier le nombre de jours pendant lequel les données sont à conserver. Si la fonction de conformité avec application consultative est activée sur le volume, vous pouvez augmenter ou diminuer la durée de conservation. Si la fonction de conformité avec application obligatoire est activée sur le volume, vous pouvez seulement augmenter la durée de conservation.

6. Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.

Suppression de volumes de fichiers

Dans certains cas, il arrive que l'espace disponible reste inchangé après la suppression des fichiers, probablement à cause de la fonction de point de contrôle ou d'activation du répertoire Attic. (Pour plus d'informations sur l'activation du répertoire Attic, reportez-vous à la [page 56](#).)

Par souci de sécurité, les points de contrôle conservent les données ayant été supprimées ou modifiées pendant un certain temps afin de pouvoir les récupérer le cas échéant. Cela signifie que les données ne sont supprimées du disque qu'à l'expiration du point de contrôle (dont la durée maximale est de deux semaines) sauf s'il s'agit de points de contrôle manuels, qui peuvent être conservés indéfiniment.

Si vous supprimez des données en vue de libérer de l'espace disque, vous devez également supprimer ou désactiver les points de contrôle. Reportez-vous à la section « [Pour supprimer un point de contrôle](#) », [page 185](#) pour des instructions sur la suppression des points de contrôle.

Remarque – Il est impossible de supprimer des volumes dont la fonction de conformité avec application obligatoire est activée de même que les volumes déconnectés.

▼ Pour supprimer un volume de fichiers ou un segment

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Delete File Volumes (Suppression de volumes de fichiers)**.
2. Sélectionnez le volume de fichiers ou le segment à supprimer.
3. Cliquez sur **Apply (Appliquer)**.

Affichage des partitions de volume

Le panneau View Volume Partitions (Affichage des partitions de volume) permet d'afficher, en lecture seule, les LUN définies pour Sun StorEdge 5310 NAS Appliance.

▼ Pour afficher les partitions de volume

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > View Volume Partitions (Affichage des partitions de volume)**.
2. Dans la liste **Volumes (Volumes)**, choisissez le volume de fichiers pour lequel afficher les partitions.

Les informations suivantes sont alors générées :

Champ	Description
LUN	Répertorie toutes les LUN associées au volume de fichiers sélectionné.
Partition	Affiche les partitions du volume de fichiers sélectionné.
Use	Indique le pourcentage d'utilisation de la partition.
Type	Affiche le type de partition, sfs2 (principal) ou sfs2ext (segment).
Free	Affiche le volume d'espace disponible sur la partition.
Capacity	Affiche la taille totale de la partition.
Requests	Indique le nombre total des requêtes traitées pour la partition.
Active	Affiche les requêtes actives de la partition qui n'ont pas encore été traitées.

Configuration iSCSI

Vous pouvez configurer le système de sorte qu'il utilise le protocole iSCSI (Internet Small Computer Systems Interface) afin de transporter les données des applications hôte vers Sun StorEdge 5310 Appliance. iSCSI transmet l'état, les données et les commandes SCSI via un réseau TCP/IP. Lorsque le protocole iSCSI est activé, les applications hôte peuvent stocker les données sur l'appareil Sun StorEdge 5310.

Dans un environnement iSCSI, Sun StorEdge 5310 NAS Appliance joue le rôle de la cible iSCSI pour un client initiateur iSCSI. Chaque initiateur et chaque cible iSCSI possèdent un identificateur unique et permanent. Celui de l'initiateur iSCSI est généré par le logiciel iSCSI sur l'hôte. La cible iSCSI prend en charge à la fois les identificateurs EUI (Enterprise Unique Identifier) et IQN (iSCSI Qualified Name).

Configuration d'une cible iSCSI

La configuration d'une cible iSCSI permettant de connecter une cible iSCSI et d'y accéder nécessite les étapes suivantes :

- Configurez le client initiateur iSCSI (voir la documentation fournie avec le logiciel initiateur iSCSI).
- Créez une liste d'accès permettant à l'initiateur iSCSI d'accéder à la cible.
- Créez un LUN et assignez l'accès de l'initiateur iSCSI au LUN.
- Configurez la méthode de détection de la cible et de l'initiateur iSCSI.

La cible iSCSI implémentée sur Sun StorEdge 5310 NAS Appliance repose sur le modèle iSCSI RFC 3720 développé par l'IETF (Internet Engineering Task Force). Le protocole pris en charge compte parmi ses fonctions le hachage d'en-tête, le protocole CHAP (Challenge Handshake Authentication Protocol) initiateur et le niveau de récupération d'erreur 0.

Configuration de l'accès de l'initiateur iSCSI

Vous pouvez définir les initiateurs iSCSI pouvant accéder à un LUN en créant une liste d'accès iSCSI. Cette liste peut comprendre un ou plusieurs initiateurs iSCSI et, éventuellement, un mot de passe et un initiateur CHAP. CHAP permet de garantir que les données sont envoyées par un initiateur iSCSI authentique.



Attention – Vous pouvez configurer plusieurs initiateurs iSCSI en vue d'accéder à la même LUN cible iSCSI. Cependant, une application (de clustering ou base de données) exécutée sur un serveur de clients iSCSI doit fournir un accès synchronisé afin d'éviter d'endommager les données.

▼ Pour créer une liste d'accès iSCSI

1. Dans le volet de navigation, sélectionnez **iSCSI Configuration (Configuration iSCSI) > Configure Access List (Configuration de la liste d'accès)**.
2. **Pour créer une liste d'accès, cliquez sur Add (Ajouter).**

La boîte de dialogue Add iSCSI LUN (Ajouter le LUN iSCSI) s'affiche.

The screenshot shows a dialog box titled "Add iSCSI Access". It features a blue header bar with the title and a close button. Below the header, there is a "Help" icon. The main area contains four input fields: "* Name:", "CHAP Initiator Name:", "CHAP Initiator Password:", and "Initiator IQN Name:". Below these fields is a list box labeled "Initiator IQN List". At the bottom of the dialog, there are "Apply" and "Cancel" buttons. A note "* Required Fields" is located at the bottom left of the dialog area.

3. Saisissez les informations suivantes :

Champ	Description
Name	Donnez un nom à la liste d'accès. Ce nom peut se composer d'un ou de plusieurs caractères et contenir des chiffres et des lettres (a-z, A-Z, 0-9), des points (.), des tirets (-) ou des deux-points (:). <code>iscsiwinxp</code> est un exemple de nom de liste d'accès valable.
CHAP Initiator Name	Indiquez le nom complet de l'initiateur CHAP configuré par le logiciel initiateur iSCSI. Le nom par défaut défini pour un client iSCSI Windows est le suivant : <code>iqn.1991-05.com.microsoft:iscsi-winxp</code> Si vous ne remplissez pas ce champ, l'autorisation CHAP ne sera pas nécessaire. Pour plus d'informations, reportez-vous à la documentation de l'initiateur iSCSI.
CHAP Initiator Password	Si vous avez indiqué un nom d'initiateur CHAP, définissez également le mot de passe de l'initiateur CHAP.
Initiator IQN Name	Indiquez un nom IQN d'initiateur et cliquez sur le bouton Add (Ajouter) afin d'ajouter l'initiateur à la liste. Si vous ne remplissez pas ce champ, n'importe quel initiateur peut accéder à la cible. Ce nom peut se composer d'un ou de plusieurs caractères et contenir des chiffres et des lettres (a-z, A-Z, 0-9), des points (.), des tirets (-) ou des deux-points (:). Pour supprimer un IQN d'initiateur de la liste, sélectionnez son nom et cliquez sur le bouton Trash (Corbeille).

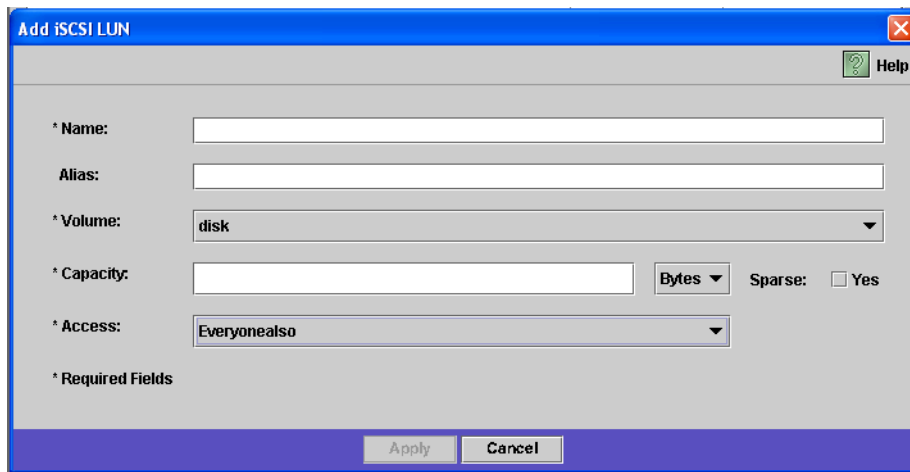
4. Cliquez sur Apply (Appliquer) pour enregistrer ces paramètres.

Vous pouvez modifier une liste d'accès iSCSI en double-cliquant sur l'un des noms de la liste d'accès ou en sélectionnant un nom et en cliquant sur Edit (Modifier). Modifiez les champs de texte voulus et cliquez sur Apply (Appliquer) pour enregistrer les paramètres.

▼ Pour créer un LUN iSCSI

1. Dans le volet de navigation, sélectionnez **iSCSI Configuration (Configuration iSCSI) > Configure iSCSI LUN (Configuration du LUN iSCSI)**.
2. Pour ajouter un LUN iSCSI à la liste, cliquez sur **Add (Ajouter)**.

La boîte de dialogue Add iSCSI LUN (Ajouter un LUN iSCSI) s'affiche.



3. Saisissez les informations suivantes pour le LUN iSCSI :

Champ	Description
Name	<p>Donnez un nom au LUN iSCSI. Ce nom peut se composer d'un ou de plusieurs caractères et contenir des chiffres et des lettres (a-z, A-Z, 0-9), des points (.), des tirets (-) ou des deux-points (:).</p> <p>Le nom cible que vous saisissez sera précédé du nom IQN complet selon la convention de dénomination suivante :</p> <p><i>iqn.1986-03.com.sun:01:adresse-mac.horodatage.nom-spécifique-utilisateur</i></p> <p>Si, par exemple, vous choisissez le nom lun1, le nom complet du LUN de la cible iSCSI sera le suivant :</p> <p><i>iqn.1986-03.com.sun:01:adresse-mac.horodatage.lun1</i></p> <p>Remarque : L'horodatage est une valeur hexadécimale représentant le nombre de secondes après le 01/01/1970.</p>
Alias	Facultatif. Donnez une brève description de la cible.
Volume	Sélectionnez le nom du volume sur lequel sera créé le LUN iSCSI.

Champ	Description
Capacity	Spécifiez la taille maximale du LUN en octets, Ko, Mo ou Go.
Sparse	<p>Cochez la case Yes (Oui) si vous souhaitez créer un LUN fractionné. Un LUN fractionné définit l'attribut de taille de fichier selon la capacité spécifiée, mais les blocs de disque ne sont pas alloués tant que les données ne sont pas consignées sur le disque. Pour plus d'informations, reportez-vous à la section « Utilisation de LUN iSCSI fractionnés », page 63.</p> <p>Si vous créez un LUN non fractionné, les blocs de disque seront alloués en fonction de la capacité du LUN créé. Lors de la création de LUN iSCSI non fractionnés, pensez à réserver environ 10 % d'espace supplémentaire sur le volume pour les métadonnées du système de fichiers. Par exemple, un LUN iSCSI de 100 Go devrait résider sur un volume de 110 Go afin de permettre la création de LUN non fractionnés.</p> <p>Pour plus d'informations sur l'utilisation de LUN fractionnés ou non, reportez-vous à la section « Utilisation de LUN iSCSI fractionnés », page 63.</p>
Access	Sélectionnez la liste d'accès (créée au préalable) associée à cette LUN dans la liste déroulante.

4. Cliquez sur **Apply (Appliquer)** pour enregistrer ces paramètres.

Utilisation de LUN iSCSI fractionnés

En règle générale, il est recommandé d'utiliser des LUN non fractionnés lorsque vous disposez de suffisamment d'espace de stockage.

Les LUN iSCSI fractionnées ne sont pas utiles dans toutes les situations. Si vous créez des LUN fractionnées, l'espace disque n'est pas alloué avant l'utilisation. Les LUN fractionnées sont utiles lorsque vous projetez de créer plusieurs LUN dont la capacité ne sera pas exploitée au maximum. Quand, par exemple, vous projetez que cinq LUN iSCSI de 100 Go chacune n'utiliseront que 55 % de leur capacité, vous pouvez toutes les créer sur un volume pouvant contenir $5 \times 100 \times 0,55 = 275$ Go plus de l'espace à des fins d'extension (50 To) = 325 Go.

À l'aide de ce modèle, vous pouvez contrôler l'utilisation réelle d'un volume et lui allouer de l'espace supplémentaire avant d'être à cours. Si les LUN iSCSI doivent utiliser la majorité de la taille de LUN disponible, il est déconseillé d'activer l'option de LUN fractionné. Certains environnements d'exploitation ne traitent pas correctement les conditions d'espace insuffisant sur les LUN fractionnés. Il est donc déconseillé de manquer d'espace afin de maintenir un comportement optimal du système.

Méthodes de détection de cible iSCSI

Vous pouvez configurer le mode de détection d'une cible iSCSI par un initiateur iSCSI à l'aide de l'une des méthodes suivantes :

- Configuration statique : ajoutez manuellement le nom de la cible iSCSI et l'adresse IP associée à l'hôte de l'initiateur iSCSI. Pour plus de détails, reportez-vous à la documentation fournie avec votre logiciel d'initiateur iSCSI.
- Requête SendTargets : ajoutez l'adresse IP ou le nom DNS du portail cible iSCSI à la configuration de l'initiateur iSCSI. L'initiateur génère une requête SendTargets afin de détecter la liste de cibles iSCSI accessibles au portail cible donné. Pour plus de détails, reportez-vous à la documentation fournie avec votre logiciel d'initiateur iSCSI.
- Serveur Internet Storage Name Service (iSNS) : paramétrez un serveur iSNS en vue d'automatiser la détection des initiateurs et cibles iSCSI. Un serveur iSNS permet aux initiateurs iSCSI de détecter la présence, l'emplacement et la configuration de cibles iSCSI. Le client iSNS est une fonction facultative qui peut être configurée à l'aide de l'interface graphique (IG) de Web Administrator comme décrit à la section suivante.

Configuration d'un serveur iSNS

Pour activer un serveur iSNS, vous spécifiez son adresse IP ou son nom DNS (Domain Name Service). Le client iSNS interagit avec n'importe quelle implémentation de serveur iSNS standard telle que Microsoft iSNS Server 3.0.

Pour plus d'informations, reportez-vous à la documentation de votre serveur et de votre initiateur iSNS.

▼ Pour définir le serveur iSNS

1. **Dans le volet de navigation, sélectionnez iSCSI Configuration (Configuration iScSI) > Configure iSNS Server (Configuration du serveur iSNS).**
2. **Tapez l'adresse IP ou le nom DNS du serveur iSNS et cliquez sur Appliquer.**

Vous pouvez également changer le nom du serveur iSNS en indiquant une adresse IP ou un nom DNS différent(e) dans le champ iSNS Server (Serveur iSNS) et en cliquant sur Apply (Appliquer).

Étapes suivantes

À ce stade, le système de fichiers et les cibles iSCSI sont paramétrés et prêts à fonctionner. Il vous reste à définir les droits d'accès, les quotas et les structures de répertoires dont vous avez besoin. Ces fonctions de gestion sont décrites à partir du [Chapitre 4](#).

Les fonctions de contrôle, essentielles à la gestion des ressources, sont quant à elles évoquées au [Chapitre 10](#). Enfin, les fonctions de maintenance, telles que la sauvegarde et la restauration, sont exposées au [Chapitre 11](#).

Gestion du système

Ce chapitre décrit plusieurs fonctions de base de la gestion du système. Ces fonctions sont principalement utilisées lors du paramétrage initial du système. Elles restent néanmoins disponibles au cas où vous auriez besoin de les réinitialiser.

Les fonctions de gestion système sont les suivantes :

- « Définition du mot de passe de l'administrateur », page 67
- « Contrôle de l'heure et de la date », page 68
- « Utilisation d'un logiciel antivirus », page 72

Définition du mot de passe de l'administrateur

Par défaut, aucun mot de passe n'est défini pour l'administrateur système. Vous pouvez en définir un si vous le souhaitez.

▼ Pour définir le mot de passe administrateur

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Set Administrator Password (Définition du mot de passe de l'administrateur)**.
2. Dans le champ **Old Password (Ancien mot de passe)**, saisissez votre ancien mot de passe.

Si vous n'en possédez pas, laissez ce champ vide.

3. Dans le champ **New Password (Nouveau mot de passe)**, saisissez un nouveau mot de passe.
Le mot de passe doit comprendre entre 1 et 21 caractères. Tous les types de caractères sont autorisés.
4. Dans le champ **Confirm Password (Confirmation du mot de passe)**, saisissez de nouveau le mot de passe.
Si vous préférez désactiver l'utilisation de mots de passe, ne remplissez pas les champs **New Password (Nouveau mot de passe)** et **Confirm Password (Confirmation du mot de passe)**.
5. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Contrôle de l'heure et de la date

La date et l'heure définies sur le serveur sont des paramètres essentiels de la gestion de fichiers. Cette section décrit les fonctions mises à la disposition de l'utilisateur pour conserver des valeurs de date et d'heure correctes.

Vous pouvez utiliser la synchronisation horaire ou définir l'heure manuellement.

Remarque – Lorsque vous réglez la date et l'heure pour la première fois, vous initialisez également *l'horloge sécurisée* du système utilisée par le logiciel de gestion des licences et par le logiciel Compliance Archiving Software pour contrôler les opérations liées à l'heure.



Attention – Une fois l'horloge sécurisée définie, il est impossible de la réinitialiser. Par conséquent, vous devez impérativement définir l'heure et la date avec précision lorsque vous configurez le système.

Synchronisation temporelle

Le système prend en charge deux types de synchronisation horaire : Network Time Protocol (NTP) ou RDATE. Vous pouvez configurer le système de manière à synchroniser son horloge avec celle d'un serveur RDATE ou NTP.

- Le protocole Internet NTP permet de synchroniser toutes vos machines réseau sur une horloge de référence, par exemple, une radio, un récepteur satellite ou un modem. Les configurations NTP classiques utilisent plusieurs serveurs redondants et divers chemins d'accès réseau afin d'allier précision et fiabilité.
- Le protocole RDATE permet d'obtenir la date et l'heure à partir d'un site indépendant. Il peut par exemple récupérer l'heure sur une autre machine du réseau. Les serveurs RDATE sont souvent utilisés avec les systèmes UNIX ; ils vous permettent de synchroniser l'horloge du système avec celle du serveur RDATE.

Une troisième méthode, appelée « synchronisation manuelle » permet de désactiver la synchronisation horaire. L'administrateur système règle alors l'horloge du système, puis il vérifie l'heure indépendamment des autres nœuds sur le réseau.

Paramétrage de la synchronisation horaire

Le panneau **Set Up Time Synchronization (Paramétrage de la synchronisation de l'heure)** permet de configurer la méthode de synchronisation de votre choix.

▼ Pour paramétrer la synchronisation horaire

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Set Up Time Synchronization (Paramétrage de la synchronisation horaire)**.
2. Choisissez l'une des trois options suivantes :
 - **Manual Synchronization (Synchronisation manuelle)** : sélectionnez cette option si vous ne souhaitez pas utiliser la synchronisation horaire RDATE ou NTP.
 - **NTP Synchronization (Synchronisation NTP)** : pour utiliser la synchronisation NTP et disposer d'au moins un serveur NTP sur le réseau, sélectionnez le bouton radio correspondant et remplissez les champs ci-dessous :
 - **Enable Server 1 (Activer le serveur 1)** : pour activer un serveur NTP, cochez la case **Enable Server 1 (Activer le serveur 1)** et entrez les informations requises dans les champs correspondants. Procédez de la même manière si vous souhaitez faire appel à un second serveur NTP. Vous avez la possibilité de configurer jusqu'à deux serveurs NTP.
 - **Enable Server 2 (Activer le serveur 2)** : pour activer un second serveur NTP ou un serveur NTP de substitution, cochez la case **Enable Server 2 (Activer le serveur 2)** et entrez les informations requises dans les champs correspondants. Vous avez la possibilité de configurer jusqu'à deux serveurs NTP.

- **NTP Server (Serveur NTP)** : indiquez le nom ou l'adresse IP du serveur NTP que le système interrogera pour connaître l'heure.
- **Auth Type (Type d'authentification)** : la prise en charge de l'authentification permet au système de vérifier, à l'aide d'une clé et d'un identificateur de clé, que le serveur est connu et digne de confiance. Le serveur NTP et le système doivent décider de la clé et de l'identificateur de clé à utiliser pour l'authentification des messages. Choisissez le type d'authentification **None (Aucun)** (aucune authentification) ou **Symmetric Key (Clé symétrique)**.
- **Key ID (ID de clé)** : si vous avez sélectionné le type d'authentification **Symmetric Key (Clé symétrique)**, vous devez indiquer l'identificateur de clé pour ce serveur NTP. La plage autorisée est comprise entre **1** et **65534**.
- **Min Poll Rate (Fréquence d'interrogation minimale)** : entrez la fréquence d'interrogation minimale pour les messages NTP. Cette valeur, mise à la puissance deux, correspond au nombre minimum de secondes de la fréquence d'interrogation. Par exemple, si vous entrez le chiffre 4, l'intervalle minimal d'interrogation entre les événements est de 16 secondes. La plage autorisée pour ce champ est comprise entre **4** et **17**.
- **Max Poll Rate (Fréquence d'interrogation maximale)** : entrez la fréquence d'interrogation maximale pour les messages NTP. Cette valeur, mise à la puissance deux, correspond au nombre maximum de secondes de la fréquence d'interrogation. Par exemple, si vous entrez le chiffre 4, l'intervalle maximal d'interrogation entre les événements est de 16 secondes. La plage autorisée pour ce champ est comprise entre **4** et **17** et sa valeur doit être supérieure à l'intervalle d'interrogation minimal.
- **Enable Broadcast Client (Activer le client de diffusion)** : cochez cette case afin que le système réponde aux messages de diffusion reçus sur n'importe quelle interface. Cette fonction est destinée aux configurations impliquant un ou plusieurs serveurs NTP dotés d'un grand nombre de clients pour lesquels la synchronisation est nécessaire.
- **Require Broadcast Server Authentication (Demande d'authentification du serveur de diffusion)** : cochez cette case pour que le client NTP s'assure que les serveurs diffusant des messages vers le système sont connus et dignes de confiance.
- **RDATE Synchronization (Synchronisation RDATE)** : pour paramétrer le serveur RDATE et une tolérance, cochez cette case et entrez les informations suivantes :
 - **RDATE Server (Serveur RDATE)** : entrez le nom ou l'adresse IP du serveur RDATE.
 - **Tolerance (Tolérance)** : entrez la valeur de tolérance maximale autorisée pour la réception de l'heure envoyée par le serveur RDATE. Cette valeur est comprise entre **0** et **3 600** secondes. Si l'horloge du système et celle du serveur RDATE ont un écart inférieur au nombre de secondes défini, l'horloge du système est synchronisée avec celle du serveur RDATE. Si l'écart est supérieur, la synchronisation ne se fait pas automatiquement. La vérification a lieu tous les jours à 11:45.

3. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Réglage manuel de la date et de l'heure

Si vous n'utilisez pas la synchronisation horaire, vous pouvez régler la date et l'heure manuellement.

▼ Pour définir manuellement la date et l'heure

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Set Time and Date (Réglage de l'heure et de la date)**.
2. Choisissez l'année appropriée dans le menu déroulant situé au-dessus et à gauche du calendrier.
3. Choisissez le mois approprié dans le menu déroulant situé au-dessus et à droite du calendrier.
4. Cliquez sur la date appropriée dans le calendrier.
5. Choisissez l'heure appropriée dans la liste déroulante située au-dessus de l'horloge et à gauche. Les valeurs autorisées sont comprises entre 0 (minuit) et 23 (11:00).
6. Choisissez ensuite les minutes (de 0 à 59) dans le menu déroulant situé au-dessus de l'horloge et à droite.
7. Dans le menu déroulant situé au bas de l'écran, sélectionnez le fuseau horaire approprié.
Lorsque le fuseau horaire est sélectionné, le serveur passe automatiquement à l'heure d'été.
8. Cliquez sur **Apply (Appliquer)** pour enregistrer les paramètres de l'heure et de la date.

Remarque – Si vous définissez pour la première fois l'heure et la date du système, cette opération règle également l'horloge sécurisée. Assurez-vous que la date et l'heure sont réglées de manière précise, car vous ne pourrez plus changer l'horloge sécurisée.

Utilisation d'un logiciel antivirus

Une protection antivirus est disponible via les connexions ICAP (Internet Content Adaptation Protocol) à des «moteurs d'analyse» installés sur le réseau. Lorsque vous activez la protection antivirus sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System, le système devient client du moteur antivirus utilisé sur le réseau.

Remarque – Si vous configurez la protection antivirus sur le système, vous devez disposer d'au moins un moteur d'analyse en service en permanence, sans quoi les clients Windows risquent de se voir refuser tout accès.

▼ Pour activer la protection antivirus

1. Dans le volet de navigation, sélectionnez **Configure Anti-Virus (Configuration de la protection antivirus)**.
2. Cochez la case **Enable Anti Virus (Activer la protection antivirus)**.

Remarque – Si vous devez désactiver temporairement l'analyse antivirus, activez l'option **Scanning Suspended (Analyse suspendue)**. Ne désactivez pas la case **Enable Anti Virus (Activer la protection antivirus)**.

3. Sélectionnez le mode d'analyse.

Mode d'analyse	Description
Scanning Suspended	(Analyse suspendue) Sélectionnez cette option afin de suspendre temporairement la protection antivirus. Remarque : la protection antivirus est désactivée lorsque cette option est sélectionnée.
Scan after Modify	(Analyse après modification) Sélectionnez cette option pour effectuer une analyse après toute modification apportée aux fichiers. Cette option offre un compromis entre les performances et l'assurance de la protection antivirus, permettant un accès en lecture rapide mais l'activation de la protection antivirus uniquement au moment de la modification des fichiers. Les accès ultérieurs aux fichiers ne tiennent pas compte des éventuelles modifications des définitions de virus.
Scan all Access	(Analyse de tous les accès) Sélectionnez cette option pour effectuer une analyse après tout type d'accès au système. Cette option offre la protection antivirus la plus complète, autorisant uniquement les accès aux données analysées à l'aide des dernières définitions de virus.

4. Spécifiez l'adresse TCP/IP du moteur d'analyse à utiliser.

5. Spécifiez le numéro de port TCP/IP sur lequel le serveur ICAP détecte les connexions ; il s'agit généralement du port 1344.

6. Spécifiez le nombre maximum d'opérations d'analyse de fichiers simultanées que le système enverra au moteur d'analyse (généralement 2).

7. Spécifiez les éléments à inclure et à exclure des analyses en sélectionnant des entrées dans la liste qui s'affiche.

Spécification	Description	Format
File Types Included	(Types de fichiers inclus) À ne pas remplir pour inclure tous les types. Sinon, sélectionnez chaque extension de type de fichier à inclure dans l'analyse.	Au maximum trois caractères. ? peut être utilisé comme caractère générique.
File Types Excluded	(Types de fichiers exclus) Sélectionnez chaque extension de type de fichier à exclure de l'analyse.	Au maximum trois caractères. ? peut être utilisé comme caractère générique.
Exempt Clients	(Clients exclus) Nom ou adresse IP des clients écartés de l'analyse.	
Exempt Groups	(Groupes exclus) Nom des différents groupes Windows NT ou Windows Active Directory (pas UNIX) écartés de l'analyse.	Espaces pris en charge.
Exempt Shares	(Partages exclus) Nom des différents partages CIFS (Common Internet File System) écartés de l'analyse. Remarque : Les partages administratifs (X\$) sont systématiquement exclus de l'analyse.	

Pour ajouter un nouvel élément à une liste, saisissez-le dans la zone prévue à cet effet et cliquez sur **Add** (Ajouter).

Pour supprimer un élément de la liste, sélectionnez-le et cliquez sur le bouton **Remove** (Supprimer).

8. Cliquez sur Apply (Appliquer) pour enregistrer les paramètres.

Remarque – Les fichiers déjà chargés en mémoire ne font pas l'objet d'une analyse. Le meilleur moyen d'activer pleinement l'analyse antivirus consiste à redémarrer le système.

Analyse antivirus

En fonctionnement normal, les utilisateurs travaillant sur des clients CIFS peuvent observer un court délai lors de l'analyse antivirus, en particulier quand l'option Scan all Access (Analyse de tous les accès) est activée.

Lorsqu'un virus est détecté, une entrée est ajoutée au journal système qui enregistre le nom du fichier infecté, le nom du virus et l'action à appliquer au fichier. Dans la plupart des cas, cette action consiste à « mettre en quarantaine » le fichier infecté et à refuser tout accès au client CIFS. Les fichiers placés en quarantaine sont visibles dans le répertoire /quarantine situé à la racine du système de fichiers contenant le fichier infecté. Afin d'éviter les conflits de noms au sein du répertoire /quarantine, les fichiers sont nommés selon une « numérotation interne » : `NNNNNN.vir` est un « lien physique » au fichier infecté et `NNNNNN.log` désigne le fichier texte contenant le nom initial du fichier infecté et les informations détaillées concernant les infections détectées.

Remarque – Par défaut, seul l'administrateur (ou la racine UNIX) peut visualiser le contenu des répertoires /quarantine.

La façon la plus simple de se débarrasser de fichiers infectés (mis en quarantaine) consiste à les supprimer.

▼ Pour supprimer les fichiers placés en quarantaine

1. **Identifiez le nom d'origine à partir du journal système ou du fichier `NNNNNN.log` situé dans le répertoire de mise en quarantaine, puis supprimez ce fichier s'il s'y trouve encore.**
2. **Examinez le répertoire de mise en quarantaine afin d'y détecter les deux fichiers `NNNNNN.vir` et `NNNNNN.log` correspondant au fichier infecté et supprimez-les.**

Gestion des ports système

Ce chapitre décrit les ports réseau et les adresses IP alias. Vous pouvez relier deux ou plusieurs ports afin de créer une liaison de ports. Une liaison de ports dispose d'une bande passante plus importante que celle affectée aux différents ports qui constituent cette liaison.

Les sujets traités dans ce chapitre sont les suivants :

- « [Emplacement des ports](#) », page 77
- « [À propos des adresses IP alias](#) », page 79
- « [Liaison de ports](#) », page 80

Emplacement des ports

Les systèmes Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System identifient les ports dans un ordre prédéfini en fonction de leur type et de leur emplacement physique et logique sur le serveur. Reportez-vous au *Guide de démarrage de Sun StorEdge 5310 NAS Appliance et Gateway System* afin de localiser les ports de votre système.

Chaque port doit être associé à rôle spécifique. Les différents rôles possibles sont les suivants :

- **Primary (Principal)** : rôle identifiant un port réseau actif. Au moins un port doit disposer du rôle principal. Le port principal fait partie intégrante du processus de basculement. Lorsque vous assignez ce rôle à un port, le serveur de substitution (serveur H2) conserve l'adresse IP affectée au port principal en tant qu'adresse IP alias de sauvegarde hors ligne. L'inverse se produit lorsque vous fournissez une adresse IP alias au serveur de substitution. L'adresse IP de substitution est conservée en tant qu'adresse IP alias de réserve par le serveur principal (serveur H1). En cas de basculement, le serveur fonctionnel active les adresses IP alias du serveur de substitution, ce qui permet de conserver l'accès réseau comme si le serveur défaillant était toujours actif.

Remarque – Au moins un port de chaque serveur doit disposer du rôle principal.

- **Independent (Indépendant)** : rôle identifiant un port réseau actif destiné à des fins autres que le traitement de données, notamment la sauvegarde. Dans un système Sun StorEdge 5310 Cluster, le port indépendant ne participe pas au processus de basculement. Les ports indépendants sont généralement utilisés pour la sauvegarde à distance. Vous ne pouvez pas lier de ports indépendants ou leur ajouter d'adresses IP alias. Vous pouvez assigner autant de rôles de ports indépendants que vous le souhaitez, mais vous ne devez en affecter qu'un par tête.
- **Mirror (Miroir)** : rôle indiquant que le port connecte ce serveur à un autre afin de créer des volumes de fichiers miroir. Utilisez le même port sur les serveurs source et cible pour la mise en miroir. Pour plus d'informations sur la mise en miroir, reportez-vous à la section « [Sun StorEdge File Replicator](#) », page 135.
- **Private (Privé)** (Sun StorEdge 5310 Cluster uniquement) : port dédié réservé aux pulsations, qui contrôle en permanence le statut de l'autre tête.

À propos des adresses IP alias

La définition d'alias IP est une fonctionnalité réseau permettant d'assigner plusieurs adresses IP à un seul port. Tous les alias IP du port sélectionné doivent se trouver sur le même réseau physique et disposer du même *masque de réseau* et de la même *adresse de diffusion* que ceux définis pour la première adresse IP (adresse principale associée au port sélectionné).

Pour les utilisateurs d'un seul serveur (d'une seule tête), vous pouvez ajouter jusqu'à neuf adresses IP alias à l'adresse IP principale de chaque port. Dans ce cas, une carte d'interface réseau (NIC) à deux ports peut fournir jusqu'à vingt adresses IP utilisables.

Sur un système Sun StorEdge 5310 Cluster, la définition d'adresses IP alias fait partie intégrante du processus de basculement. Sur un système à deux têtes, vous pouvez ajouter jusqu'à quatre adresses IP alias à l'adresse IP principale de chaque port. Les cinq autres sont réservées à la sauvegarde des adresses principales et IP alias des ports principaux et miroir sur le serveur de substitution. En cas de basculement de tête, le serveur fonctionnel active ces adresses IP de réserve sauvegardées afin que l'accès réseau soit maintenu après une interruption minimale. Pour obtenir plus d'informations sur le basculement de tête, reportez-vous à la section « [Activation du basculement de tête](#) », page 19.

Dans le cas de systèmes à deux serveurs, vous pouvez seulement ajouter des adresses IP alias aux ports associés à un rôle principal. Les options de rôle sont décrites à la section « [Emplacement des ports](#) », page 77.

Remarque – Ne confondez pas le rôle principal avec l'adresse IP principale. Le rôle principal correspond à une assignation représentant la manière dont le port fonctionne dans un système Sun StorEdge 5310 Cluster. L'adresse IP principale est la première adresse attribuée au port sélectionné. Dans Web Administrator, l'adresse IP principale est indiquée dans le panneau Network Configuration (Configuration réseau) > Configure TCP/IP (Configuration TCP/IP) > Configure Network Adapters (Configuration des adaptateurs réseau). Vous pouvez sélectionner le rôle du port au bas de l'écran.

Liaison de ports

Il existe deux types de liaisons de ports : la haute disponibilité et l'agrégation de ports. La liaison de type agrégation de ports associe plusieurs ports adjacents afin d'obtenir un port plus rapide, doté d'une bande passante supérieure. La liaison de type haute disponibilité associe deux ou plusieurs ports afin d'offrir une commutation des ports de la carte d'interface réseau ou des ports pour la sauvegarde.

Remarque – Sun StorEdge 5310 NAS Appliance, le système cluster Sun StorEdge 5310 et le système de passerelle système de passerelle Sun StorEdge 5310 Gateway System prennent en charge la liaison Etherchannel, un sous-ensemble de la spécification 802.3ad. Reportez-vous à la documentation de votre commutateur pour en savoir plus sur les liaisons Etherchannel avant de configurer la liaison des ports.

Un système peut posséder jusqu'à quatre liaisons d'un type quelconque. Chaque liaison peut comporter jusqu'à six ports.

Liaisons de type agrégation de ports

La liaison de type agrégation de ports (également appelée agrégation de canaux, agrégation ou agrégation de liens) vous permet de mettre à l'échelle les E/S du réseau en reliant les ports adjacents. En résulte un canal réseau unique doté d'une large bande passante et composé de plusieurs canaux dotés d'une bande passante moins large.

Une liaison de type agrégation requiert au minimum deux ports disponibles. Ces ports doivent être dotés du même type d'interface (par exemple, Fast Ethernet) et se connecter au même sous-réseau. En outre, ils doivent se connecter aux ports adjacents sur le même commutateur réseau.

Remarque – Le commutateur connecté aux ports configurés pour l'agrégation de canaux doit prendre en charge les agrégations de liaisons de type IEEE 802.3ad. Consultez la documentation relative aux commutateurs de votre réseau local pour obtenir des informations sur la configuration de cette fonction.

Liaisons haute disponibilité

La liaison de ports haute disponibilité (HA) offre des possibilités de basculement des ports sur le système. Plusieurs ports disponibles sont reliés de sorte qu'un port secondaire prenne automatiquement la relève en cas de problème au niveau du port principal afin de permettre aux services de fonctionner sans interruption.

Une liaison de ce type requiert au moins deux ports disponibles. Néanmoins, ces ports ne doivent pas obligatoirement disposer de la même type d'interface, ni être connectés à des ports adjacents.

Remarque – Une liaison haute disponibilité prend en charge tous les types de commutateurs. La seule condition requise est la connexion des commutateurs au même sous-réseau.

Liaison de ports sur un système à un serveur

Cette section explique comment lier des ports pour un système à un serveur.

Vous devez configurer les ports préalablement à leur liaison. Les adresses IP alias ainsi que d'autres éléments de la configuration d'origine risquent alors d'être modifiés. Une fois la liaison de ports définie, reprenez la section « [Configuration des ports réseau](#) », [page 21](#) afin de configurer cette liaison. Lorsque deux ou plusieurs ports sont reliés, vous pouvez uniquement ajouter des alias IP à la liaison et non aux ports individuels.

▼ Pour lier des ports sur un système à un serveur

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Bond NIC Ports (Liaison des ports de la carte NIC)**.
2. Cliquez sur **Create (Créer)**.
3. Cliquez sur **Port Aggregation (Agrégation de ports)** ou sur **High Availability (Haute disponibilité)** pour spécifier le type de liaison à créer.
4. Choisissez au moins deux ports disponibles à relier en cliquant sur le port de votre choix dans la zone **Available NIC Ports (Ports de carte NIC disponibles)**, puis en cliquant sur **>** pour l'ajouter à la liste **NIC Ports in This Bond (Ports de carte NIC de cette liaison)**.

Si, à l'étape 3, vous avez coché l'option **Port Aggregation (Agrégation de ports)**, vous devez obligatoirement choisir des ports du même type d'interface, connectés à des ports adjacents.

Pour supprimer un port de la liste, sélectionnez-le et cliquez sur **<**.

5. Saisissez les informations requises dans les champs **IP Address (Adresse IP)**, **Subnet Mask (Masque de sous-réseau)** et **Broadcast Address (Adresse de diffusion)**.

Par défaut, ces champs contiennent les informations correspondant au port principal, à savoir le premier port répertorié dans la zone **NIC Ports in This Bond** (Ports de la carte NIC de cette liaison).

6. Cliquez sur **Apply (Appliquer)** pour terminer le processus de liaison des ports. **Web Administrator** vous invite alors à redémarrer automatiquement votre système.

Une fois le système redémarré, toutes les adresses IP alias ont été supprimées des ports de la liaison.

Pour ajouter des adresses IP alias à la liaison de ports, reportez-vous à la section « [Pour configurer des adaptateurs réseau](#) », page 22.

Liaison de ports sur un système cluster Sun StorEdge 5310

Pour lier des ports sur des systèmes à deux têtes, effectuez simplement la procédure suivante sur un serveur. Tous les ports doivent être du même type (par exemple, Fast Ethernet) et se connecter au même sous-réseau. En outre, ils doivent se connecter aux ports adjacents sur le même commutateur réseau. Le système redémarre automatiquement après chaque liaison de ports.

Vous devez configurer les ports préalablement à leur liaison. Les adresses IP alias ainsi que d'autres éléments de la configuration d'origine risquent alors d'être modifiés. Une fois la liaison de ports définie, reprenez la section « [Configuration des ports réseau](#) », page 21 afin de configurer cette liaison.

Pour plus d'informations sur la liaison de ports sur des systèmes à deux serveurs, reportez-vous à la section « [Exemple de liaison de ports sur un système à deux serveurs](#) », page 84.

Remarque – Vous ne pouvez lier que des ports dotés du rôle principal. Pour plus d'informations sur les rôles du port, reportez-vous à la section « [Emplacement des ports](#) », page 77.

▼ Pour lier des ports sur un système à deux serveurs

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Bond NIC Ports (Liaison des ports de la carte NIC)**.
2. Cliquez sur **Create (Créer)**.
3. Sélectionnez les ports à lier dans la liste **Available NIC Ports (Ports de carte NIC disponibles)** qui répertorie l'ensemble des ports ne figurant pas dans la liaison. La boîte de dialogue indique l'adresse IP, le masque de sous-réseau et l'adresse de diffusion du premier port de la liste.
4. Sélectionnez un port, puis cliquez sur **>** pour l'ajouter à la liste **NIC Ports in This Bond (Ports de carte NIC de cette liaison)**.

Pour supprimer un port de la liste, sélectionnez-le et cliquez sur **<**.

Vous devez ajouter au moins deux ports à la liste. Tous les ports de la liaison doivent faire partie du même sous-réseau.

Sur le serveur de substitution, les ports correspondants sont automatiquement liés de la même manière dès que vous cliquez sur **Apply (Appliquer)** et que le serveur redémarre. Par exemple, si vous liez les ports 2 et 3 du serveur H1, les ports 2 et 3 du serveur H2 sont également liés.

5. Cliquez sur **Apply (Appliquer)** pour terminer le processus de liaison des ports et redémarrer le système.

Le système assigne automatiquement un ID de liaison à la nouvelle liaison de ports. L'adresse IP de la liaison de ports correspond à celle du premier port ajouté à la liaison.

6. Pour ajouter des adresses IP alias à la liaison de ports, reportez-vous à la section **« Pour configurer des adaptateurs réseau », page 22**.

Lorsque plusieurs ports sont reliés, vous pouvez uniquement ajouter des alias IP à la liaison et non aux ports individuels.

Exemple de liaison de ports sur un système à deux serveurs

La [FIGURE 5-1](#) présente un exemple de système Sun StorEdge 5310 Cluster connecté à deux sous-réseaux distincts. Pour afficher toutes les combinaisons possibles, chaque tête de l'exemple dispose d'un port de pulsation (HB) et de quatre ports supplémentaires. Tous les ports (à l'exception du port de pulsation) de chaque serveur sont dotés du rôle principal.

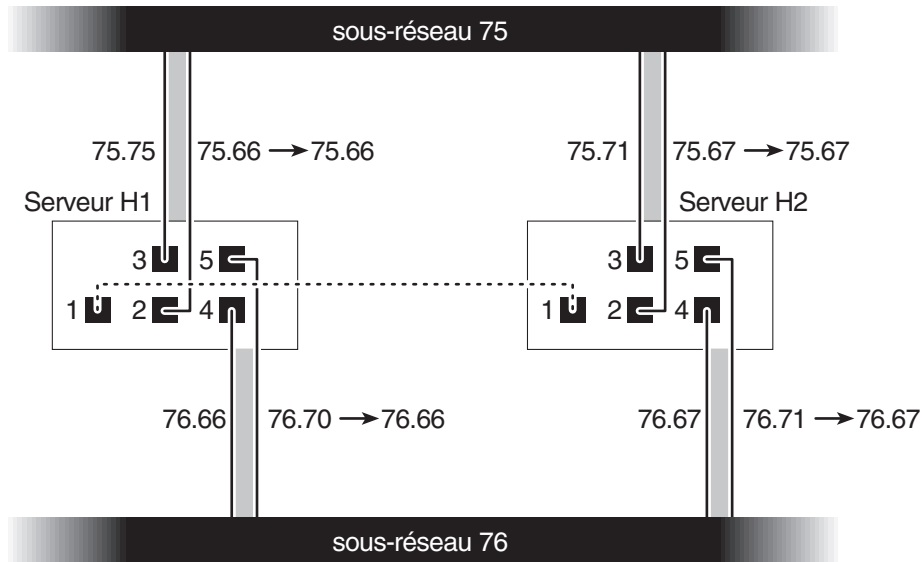


FIGURE 5-1 Liaison de ports sur un système à deux serveurs

Si les ports 2 et 3 sont liés et que les ports 4 et 5 le sont également, la configuration IP est définie comme dans le [TABLEAU 5-1](#).

TABLEAU 5-1 Exemple de liaison de ports sur un système à deux serveurs

Tête	Ports à lier		Liaison de ports		
	Nom	Adresse IP principale	Nom	Adresse IP principale	Adresse IP de sauvegarde
1	Port 2	192.1xx.75.66	Liaison 1	192.1xx.75.66	192.1xx.75.67
	Port 3	192.1xx.75.70			
	Port 4	192.1xx.76.66	Liaison 2	192.1xx.76.66	192.1xx.76.67
	Port 5	192.1xx.76.70			
2	Port 2	192.1xx.75.67	Liaison 1	192.1xx.75.67	192.1xx.75.66
	Port 3	192.1xx.75.71			
	Port 4	192.1xx.76.67	Liaison 2	192.1xx.76.67	192.1xx.76.66
	Port 5	192.1xx.76.71			

L'adresse IP principale de chaque port sur le serveur H1 fait office d'adresse IP de sauvegarde du port correspondant sur le serveur H2, et inversement.

En cas de basculement de tête, le serveur fonctionnel active les adresses IP du serveur en panne. Vous pouvez ajouter des adresses IP alias à l'adresse IP principale d'une liaison de ports. Ces adresses IP prennent part au processus de basculement. Pour plus d'informations sur les alias IP, reportez-vous à la section « [À propos des adresses IP alias](#) », page 79.

Active Directory Service et l'authentification

Ce chapitre décrit en détail Active Directory Service (ADS), le paramétrage du protocole Lightweight Data Access Protocol (LDAP) et la procédure de modification de l'ordre de recherche au sein du service de noms. Vous trouverez les instructions de configuration des autres services de noms à la section « [Services de noms](#) », page 24.

Ce chapitre aborde les sujets suivants :

- « [Services de noms pris en charge](#) », page 87
- « [Active Directory Service](#) », page 88
- « [Paramétrage LDAP](#) », page 93
- « [Modification de l'ordre de recherche des services de noms](#) », page 94

Services de noms pris en charge

Le système prend en charge plusieurs services de noms pour les réseaux Windows et UNIX. Ces services de noms sont les suivants :

- **ADS** : Active Directory Service (ADS) est un service de noms Windows 2000 intégré au système DNS (Domain Name System). Voir la section « [Paramétrage DNS](#) », page 27). Il fonctionne uniquement sur les contrôleurs de domaine. Outre le stockage et la disponibilité des données, ADS protège les objets réseau des accès non autorisés et réplique les objets sur un autre réseau de sorte que les données ne soient pas perdues en cas d'échec du contrôleur de domaine. Lorsque vous activez et paramétrez ADS, le système effectue automatiquement des mises à jour d'ADS. Pour plus d'informations, reportez-vous à la section « [Active Directory Service](#) », page 88.
- **LDAP** : le protocole LDAP (Lightweight Data Access Protocol) est un service UNIX qui active l'authentification.

- **WINS** : un serveur WINS (Windows Internet Naming Service) convertit les noms NetBIOS en adresses IP, permettant aux ordinateurs du réseau de localiser les autres périphériques NetBIOS avec plus d'efficacité et de rapidité. La fonction du serveur WINS pour les environnements Windows est similaire à celle du serveur DNS pour les environnements UNIX. Pour plus d'informations, reportez-vous à la section « [Paramétrage WINS](#) », page 27.
- **DNS** : le système DNS (Domain Name System) convertit les noms de domaine en adresses IP pour le système. Ce service vous permet d'identifier un serveur par son adresse IP ou par son nom. Pour plus d'informations, reportez-vous à la section « [Paramétrage DNS](#) », page 27.
- **NIS** : le service NIS (Network Information Service) configure le système en vue d'importer la base de données NIS. Il gère l'accès aux ressources en fonction des informations sur les groupes d'utilisateurs et les hôtes. Pour plus d'informations, reportez-vous à la section « [Paramétrage NIS](#) », page 29.
- **NIS+** : le service NIS+ (Network Information Service Plus) a été conçu pour remplacer NIS. NIS+ offre une prise en charge limitée aux clients NIS, mais sa fonction principale est de résoudre les problèmes qui ne peuvent pas l'être avec NIS. NIS+ ajoute avant tout des références ainsi qu'un accès sécurisé à la fonctionnalité NIS. Pour plus d'informations, reportez-vous à la section « [Paramétrage de NIS+](#) », page 30.

Active Directory Service

Pour que le système s'intègre parfaitement dans un environnement Active Directory sous Windows 2000, assurez-vous que les éléments suivants sont installés sur le réseau :

- un contrôleur de domaine de serveur Windows 2000 ;
- un serveur DNS dans lequel Active Directory est intégré et qui autorise les mises à jour dynamiques (nécessaires à l'utilisation de la fonction DNS dynamique) est recommandé mais n'est pas requis pour l'utilisation d'ADS.

Une fois le service ADS paramétré, vous pouvez le configurer de manière à publier les partages spécifiques dans le répertoire ADS. Pour ce faire, créez ou mettez à jour les partages SMB et indiquez un conteneur de partage pour chaque partage à publier.

Le paramétrage d'ADS implique les procédures suivantes :

1. Activation d'ADS
2. Vérification de l'ordre de recherche des services de noms
3. Vérification de l'activation et de la configuration du DNS pour la prise en charge d'ADS
4. Publication de partages dans ADS

▼ Pour activer ADS

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Set Time and Date (Réglage de l'heure et de la date)**.
2. Vérifiez que l'horloge du système et celle des contrôleurs de domaine ADS pour Windows 2000 ne diffèrent pas de plus de cinq minutes.
3. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Remarque – Si vous réinitialisez la date et l'heure, vous modifiez l'horloge système utilisée pour la plupart des opérations dépendant de l'heure. En revanche, vous ne modifiez pas l'horloge utilisée par le logiciel de gestion des licences et par le logiciel Compliance Archiving Software (Logiciel d'archivage en conformité).

4. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Domains and Workgroups (Configuration de domaines et de groupes de travail)**.
5. Cochez la case **Enable ADS (Activer ADS)**.
6. Dans le champ **Domain (Domaine)**, indiquez le domaine Windows 2000 dans lequel ADS est exécuté.
Le système doit appartenir à ce domaine.
7. Dans le champ **User Name (Nom d'utilisateur)**, entrez le nom de l'utilisateur Windows 2000 disposant des droits d'administrateur.

Cet utilisateur doit être l'administrateur du domaine ou un utilisateur membre du groupe d'administrateurs du domaine. Le client ADS vérifie les mises à jour sécurisées du service ADS avec cet utilisateur.

Remarque – Si vous entrez le nom de l'administrateur de domaine ici et que la mise à jour d'ADS échoue, le mot de passe de l'administrateur de domaine doit être modifié sur le contrôleur de domaine. Cette opération n'est requise que pour l'utilisateur administrateur et le même mot de passe peut être réutilisé. Pour plus d'informations, consultez le site Web des services de support de Microsoft, article Q248808.

8. Dans le champ **Password (Mot de passe)**, saisissez le mot de passe de l'administrateur Windows 2000.

9. Dans le champ **Container (Conteneur)**, indiquez le chemin d'accès ADS de l'utilisateur administrateur de Windows 2000 sous la forme de nom distinctif (DN) du protocole LDAP.

Les objets, notamment les utilisateurs, sont situés dans les domaines Active Directory en fonction d'un chemin hiérarchique comprenant chaque niveau d'objet « conteneur ». Entrez le chemin en fonction du dossier **nc** (nom courant) ou **uo** (organisation) de l'utilisateur.

Par exemple, si l'utilisateur réside dans le dossier « utilisateurs » au sein d'un dossier parent nommé « comptabilité », entrez les informations suivantes :

uo=utilisateurs,uo=comptabilite

N'incluez pas le nom de domaine dans le chemin.

10. Dans le champ **Site (Site)**, entrez le nom du site ADS local s'il est différent du domaine ADS.
Généralement, ce champ est laissé vide.
11. Dans la zone **Kerberos Realm Info (Infos de domaine Kerberos)**, entrez le nom de domaine utilisé pour identifier ADS.
12. Il s'agit généralement du domaine ADS ou du domaine DNS. Lorsque vous cliquez sur **Apply (Appliquer)**, cette entrée est convertie en lettres majuscules.
13. Dans le champ **Server (Serveur)**, indiquez le nom d'hôte du serveur Kerberos KDC.
Le nom de ce serveur est habituellement le nom de l'hôte du contrôleur de domaine principal dans le domaine ADS. Vous pouvez laisser ce champ vide si le système parvient à localiser le serveur KDC via le service DNS.
14. Cliquez sur **Apply (Appliquer)** pour enregistrer et appliquer les modifications effectuées.

▼ Pour vérifier l'ordre de recherche des services de noms

1. Sélectionnez **UNIX Configuration (Configuration UNIX) > Configure Name Services (Configuration des services de noms)**.
2. Vérifiez que l'ordre de recherche des services de noms pour le DNS est activé et que sa priorité est correctement définie.
 - a. Sélectionnez l'onglet **Hosts Order (Ordre des hôtes)**. Assurez-vous que le service DNS figure dans la liste de droite **Services Selected (Services sélectionnés)**. Si tel n'est pas le cas, sélectionnez-le et cliquez sur le bouton **>**.
 - b. Utilisez les boutons **Up (Monter)** et **Down (Descendre)** pour modifier l'ordre dans lequel les services sélectionnés sont analysés.
3. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

▼ Pour vérifier la configuration DNS

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Configure TCP/IP (Configuration TCP/IP) > Set Up DNS (Paramétrage DNS)**.
2. Si le service DNS n'est pas activé, cochez la case **Enable DNS (Activer DNS)**.
3. Si aucun nom de domaine n'est indiqué, spécifiez un nom dans le champ **DNS Domain Name (Nom de domaine DNS)**.
Ce nom doit être le même que celui du domaine ADS.
4. Dans le champ **Server (Serveur)**, saisissez l'adresse IP du serveur DNS que le système doit utiliser, puis cliquez sur le bouton **Add (Ajouter)** afin de placer l'adresse du serveur dans la liste **DNS Server List**.
Vous pouvez ajouter jusqu'à deux serveurs à cette liste.
5. Cochez la case **Enable Dynamic DNS (Activer le DNS dynamique)**.
Si vous ne l'activez pas, vous devez saisir le nom de l'hôte et l'adresse IP manuellement.
6. Dans le champ **DynDNS User Name (Nom d'utilisateur DynDNS)**, saisissez le nom de l'utilisateur Windows 2000 disposant des droits d'administrateur pour effectuer les mises à jour DNS dynamique sécurisées.
Vous pouvez laisser ce champ vide pour les mises à jour non sécurisées si ces dernières sont autorisées par le serveur DNS.
7. Dans le champ **DynDNS Password (Mot de passe DynDNS)**, entrez le mot de passe de l'utilisateur DNS dynamique.
8. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.
Si la fonction de DNS dynamique est activée, le système met immédiatement à jour le nom de l'hôte et l'adresse IP du DNS.

▼ Pour publier les partages dans ADS

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Shares (Configuration des partages)**.
2. Cliquez sur **Add (Ajouter)**.
3. Entrez un nom de partage dans le champ **Share Name**.

4. (Facultatif) Ajoutez un commentaire pour décrire le partage.
Vous pouvez entrer jusqu'à 60 caractères alphanumériques.
5. Sélectionnez un volume à partager dans le menu déroulant.
6. (Facultatif) Dans le champ Directory (Répertoire), indiquez un répertoire existant situé sur le volume sélectionné à partager.

Remarque – Si aucun répertoire n'est indiqué, le partage est créé au niveau root.

7. Dans le champ Container (Conteneur), entrez l'emplacement du répertoire ADS dans lequel le partage sera publié.
Le champ Container (Conteneur) identifie le conteneur ADS. Entrez l'emplacement ADS du partage sous la forme de nom distinctif (DN) du protocole LDAP. Pour plus d'informations, reportez-vous à la section [étape 9, page 90](#).
8. Cliquez sur Apply (Appliquer) afin d'ajouter le partage au conteneur spécifié.

Remarque – Le conteneur sélectionné doit déjà exister pour que le partage soit publié dans ce conteneur. Le système ne crée pas d'objets conteneur dans l'arborescence ADS.

▼ Pour mettre à jour des conteneurs de partage ADS

1. Dans le volet de navigation, sélectionnez Windows Configuration (Configuration Windows) > Configure Shares (Configuration des partages).
2. Sélectionnez le partage à mettre à jour.
3. Cliquez sur Edit (Modifier) pour afficher la boîte de dialogue Edit Share (Modification d'un partage).
4. Indiquez le nouveau conteneur du partage.
5. Cliquez sur Apply (Appliquer).
Le système met à jour le conteneur de partage.

▼ Pour supprimer des partages d'ADS

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Shares (Configuration des partages)**.
2. Sélectionnez le partage à supprimer du service ADS.
3. Cliquez sur **Edit (Modifier)** pour afficher la boîte de dialogue **Edit Share (Modification d'un partage)**.
4. Supprimez le contenu de partage du champ **Container (Conteneur)**.
5. Cliquez sur **Apply (Appliquer)**.

Paramétrage LDAP

Afin de pouvoir utiliser le service LDAP, assurez-vous que le serveur LDAP est exécuté.

▼ Pour activer le service LDAP

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX) > Set Up NSSLDAP (Paramétrage de NSSLDAP)**.
2. Pour activer le service LDAP, sélectionnez l'option **Enable NSSLDAP (Activer NSSLDAP)**.
3. Dans le champ **Domain (Domaine)**, indiquez le nom de domaine du serveur LDAP (foo.com, par exemple).
4. Dans le champ **Password (Mot de passe)**, saisissez le mot de passe défini pour le serveur LDAP.
5. Dans le champ **Server (Serveur)**, saisissez l'adresse IP du serveur LDAP.
6. Enfin, dans le champ **Proxy (Proxy)**, entrez le domaine du proxy, qui est fonction des paramètres du serveur.
7. Cliquez sur **Apply (Appliquer)** pour enregistrer ces paramètres.

Modification de l'ordre de recherche des services de noms

L'ordre de recherche des services de noms (NS) détermine l'ordre dans lequel le système effectue la recherche des services de noms pour la résolution d'une requête. Ces services de noms peuvent inclure les services LDAP, NIS, NIS+, DNS et locaux. Pour pouvoir utiliser les services en vue de la résolution de noms, vous devez les activer.

▼ Pour définir l'ordre de recherche des utilisateurs, groupes, groupes réseau et hôtes

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX) > Configure Name Services (Configuration des services de noms)**.
2. Sous l'onglet **Users Order (Ordre des utilisateurs)**, sélectionnez l'ordre dans lequel rechercher les utilisateurs.
 - a. Choisissez un service dans la zone **Services Not Selected (Services non sélectionnés)**.
 - b. Cliquez sur le bouton **>** pour le déplacer vers la zone **Services Selected (Services sélectionnés)**.

Pour supprimer un service de la fonction de recherche d'utilisateurs, sélectionnez-le et cliquez sur **<**.
 - c. Sélectionnez un à un, dans la zone **Services Selected (Services sélectionnés)**, les services utilisés dans la recherche afin de modifier leur ordre, puis cliquez sur les boutons **Up** et **Down** pour déplacer chaque service vers le haut ou vers le bas.

Le premier service utilisé lors de la recherche d'utilisateurs est celui qui figure en tête de la liste.
3. Sous l'onglet **Groups Order (Ordre des groupes)**, sélectionnez les services à utiliser dans la recherche de groupes, en suivant la procédure mentionnée à l'étape 2.
4. Sous l'onglet **Netgroup Order (Ordre des groupes réseau)**, sélectionnez les services à utiliser dans la recherche de groupes réseau, en suivant la procédure mentionnée à l'étape 2.
5. Sous l'onglet **Hosts Order (Ordre des hôtes)**, sélectionnez les services à utiliser dans la recherche d'hôtes, en suivant la procédure mentionnée à l'étape 2.
6. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Groupes, hôtes et sécurité du répertoire de fichiers

Ce chapitre fournit des informations sur les groupes locaux, les hôtes, les mappages d'utilisateurs et de groupes ainsi que sur la sécurité du répertoire de fichiers.

Pour plus de détails concernant la configuration de la sécurité Windows, reportez-vous à la section « [Configuration de la sécurité Windows](#) », page 24.

Ce chapitre aborde les sujets suivants :

- « [Groupes locaux](#) », page 95
- « [Configuration des hôtes](#) », page 99
- « [Mappage des références d'utilisateurs et de groupes](#) », page 101
- « [Définition de la sécurité du répertoire de fichiers](#) », page 110

Groupes locaux

Les exigences relatives aux groupes locaux intégrés dans Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System diffèrent de celles d'un système Windows. Avec un appareil NAS, aucun utilisateur n'est connecté localement. Les utilisateurs se connectent par le biais du réseau et sont authentifiés par l'intermédiaire d'un contrôleur de domaine. Par conséquent, les groupes locaux de type Utilisateurs ou Invités ne sont pas nécessaires.

Remarque – Les groupes locaux concernent uniquement la gestion de réseaux CIFS.

Les groupes locaux servent essentiellement à la gestion des ressources et aux opérations de sauvegarde. Il existe trois types de groupes locaux : les administrateurs, les utilisateurs avec pouvoir et les opérateurs de sauvegarde.

- **Administrators (Administrateurs)** : les membres de ce groupe peuvent pleinement administrer les fichiers et les répertoires du système.
- **Power Users (Utilisateurs avec pouvoir)** : les membres de ce groupe deviennent propriétaires des fichiers et répertoires du système, effectuent des sauvegardes et restaurent des fichiers.
- **Backup Operators (Opérateurs de sauvegarde)** : les membres de ce groupe peuvent contourner la sécurité pour sauvegarder et restaurer les fichiers.

Le système prend également en charge les groupes intégrés Authenticated Users (Utilisateurs authentifiés) et Network (Réseau) : tous les utilisateurs connectés deviennent automatiquement membres de ces deux groupes gérés en interne. Vous pouvez ajouter n'importe quel utilisateur de domaine principal ou de confiance valide comme membre d'un groupe local intégré.

Configuration des privilèges accordés aux groupes locaux

Les privilèges constituent une méthode sécurisée de répartition des tâches sur l'ensemble du système. Chaque privilège possède un rôle bien défini et est affecté à un utilisateur ou à un groupe par l'administrateur système. Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310, et système de passerelle Sun StorEdge 5310 Gateway System ne possédant pas d'utilisateur local, les privilèges sont uniquement assignés à des groupes.

Contrairement aux droits d'accès qui sont des autorisations accordées en fonction des objets par le biais de descripteurs de sécurité, les privilèges ne dépendent pas des objets. Les privilèges ne tiennent pas compte des listes de contrôle d'accès basées sur les objets afin d'autoriser les propriétaires de privilèges à exécuter les rôles qui leur sont attribués. Par exemple, les membres appartenant au groupe des opérateurs de sauvegarde doivent passer outre les contrôles de sécurité standard pour pouvoir sauvegarder et restaurer des fichiers auxquels ils n'ont généralement pas accès.

La différence entre un droit d'accès et un privilège est expliquée à l'aide des définitions suivantes :

- Un droit d'accès est accordé ou refusé de manière explicite à un utilisateur ou à un groupe. Les droits d'accès sont attribués en tant qu'autorisation dans une liste de contrôle d'accès discrétionnaire (DACL) au niveau de l'objet.
- Un privilège est un rôle qui accorde implicitement aux membres d'un groupe la possibilité d'exécuter des opérations prédéfinies sur l'ensemble du système. Les privilèges ignorent ou outrepassent les droits d'accès au niveau des objets.

Les privilèges pris en charge sont indiqués dans le [TABLEAU 7-1](#). Vous pouvez assigner ces privilèges à n'importe quel groupe prédéfini. Un utilisateur de domaine pouvant devenir membre d'un groupe prédéfini, vous pouvez attribuer ces privilèges à n'importe quel utilisateur de domaine.

TABLEAU 7-1 Privilèges pris en charge

Privilège	Description
Sauvegarde de fichiers et de répertoires	Permet à l'utilisateur d'effectuer des sauvegardes sans posséder de droits d'accès en lecture sur les fichiers et les dossiers cible.
Restauration de fichiers et de répertoires	Permet à l'utilisateur de restaurer des fichiers sans posséder de droits d'accès en écriture sur les fichiers et les dossiers cible.
Prise de possession de fichiers et de dossiers	Permet à l'utilisateur de devenir propriétaire d'un objet sans posséder de droits d'appartenance. L'appartenance ne peut être définie que pour les valeurs que le propriétaire est en droit d'attribuer à un objet.

Les privilèges par défaut assignés aux groupes locaux intégrés sont indiqués dans le [TABLEAU 7-2](#). Par conséquent, les membres appartenant au groupe local des administrateurs peuvent s'approprier n'importe quel fichier ou dossier et ceux appartenant au groupe des opérateurs de sauvegarde peuvent effectuer des opérations de sauvegarde et de restauration.

TABLEAU 7-2 Privilèges de groupe par défaut

Groupe	Privilège par défaut
Administrateurs	Prise de possession
Opérateurs de sauvegarde	Sauvegarde et restauration
Utilisateurs avec pouvoir	Aucun

Assignment d'une propriété

Par défaut, le groupe des administrateurs du domaine, dont Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System sont membre, est lui-même membre du groupe local des administrateurs. Par conséquent, lorsqu'un membre appartenant au groupe des administrateurs (y compris l'administrateur du domaine), crée ou prend possession d'un fichier ou d'un dossier, ce dernier devient la propriété du groupe local des administrateurs. Cela assure une portabilité maximale lorsque le système est déplacé d'un domaine sur un autre : les objets appartenant au groupe local des administrateurs restent accessibles aux membres du nouveau groupe de domaine des administrateurs.

Les règles d'assignation de propriété décrites ci-dessus s'appliquent également aux utilisateurs réguliers qui sont membres du groupe local des administrateurs. Si un membre de ce groupe crée ou prend possession d'un objet, la propriété est attribuée au groupe local plutôt qu'au membre lui-même.

Sous Windows, l'adhésion de l'administrateur de domaine au groupe local des administrateurs peut être révoquée. Si tel est le cas, les membres du groupe de domaine des administrateurs sont considérés comme des utilisateurs réguliers. Cependant, sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System, l'administrateur du domaine se voit toujours assigner l'appartenance au groupe des administrateurs locaux. Comme son nom ne figure pas en tant que membre du groupe, vous ne pouvez pas le révoquer. Le groupe des administrateurs de domaines doit disposer d'un contrôle administratif sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System puisqu'il n'y a aucun utilisateur local et donc aucun administrateur Windows.

Ajout et suppression des membres d'un groupe et configuration des privilèges

Le panneau **Configure Groups (Configuration de groupes)** vous permet d'ajouter des utilisateurs de domaine aux trois groupes locaux.

▼ Pour ajouter un membre à un groupe ou en supprimer un

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Groups (Configuration de groupes)**.

Les membres existants du groupe sélectionné sont répertoriés dans la zone **Group Members (Membres du groupe)**.

2. Pour ajouter un groupe, procédez comme suit :
 - a. Cliquez sur **Add Group (Ajouter un groupe)**.
 - b. Dans le champ **Group (Groupe)**, saisissez le nom du groupe.
 - c. Dans le champ **Comment (Commentaire)**, entrez une description du groupe ou un commentaire.
 - d. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.
3. Pour supprimer un groupe, procédez comme suit :
 - a. Sélectionnez le groupe à supprimer.
 - b. Cliquez sur **Remove Group (Supprimer un groupe)**.
 - c. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

4. Pour ajouter un membre d'un groupe ou en supprimer un, procédez comme suit :
 - a. Mettez en surbrillance le nom du groupe auquel vous souhaitez ajouter un membre ou duquel vous voulez en supprimer.
Les membres appartenant au groupe sélectionné sont affichés dans la zone Group Members (Membres du groupe).
 - b. Dans la zone Group Members (Membres du groupe), surlignez le membre à ajouter ou à supprimer, puis cliquez sur l'icône d'ajout ou de suppression.
 - c. Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.

Configuration des privilèges

Le panneau Configure Privileges (Configuration de privilèges) permet aux administrateurs d'afficher, d'octroyer ou de révoquer des privilèges.

▼ Pour configurer des privilèges NT

1. Dans le volet de navigation, sélectionnez Windows Configuration (Configuration Windows) > Configure Groups (Configuration de groupes).
2. Dans la zone Groups (Groupes), sélectionnez le groupe auquel vous souhaitez attribuer des privilèges.

Configuration des hôtes

Le panneau Set Up Hosts (Paramétrage des hôtes) permet d'ajouter, de modifier ou de supprimer des entrées dans le fichier d'hôte du système. Le tableau affiche des informations sur les hôtes actuels, notamment leur nom et leur adresse IP et indique s'il s'agit d'hôtes de confiance.



Attention – Accordez le statut d'hôte **de confiance** avec prudence. En effet, les hôtes de confiance bénéficient d'un accès root au système de fichiers ainsi que de droits d'accès en lecture/écriture complets sur tous les fichiers et répertoires de ce système.

Ajout et modification d'hôtes

Le panneau **Set Up Hosts (Paramétrage des hôtes)** permet d'afficher et de modifier des informations sur les hôtes et de différencier les hôtes de confiance des autres hôtes. Un **superutilisateur** défini sur un client NFS dispose de privilèges root sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System et a accès à l'ensemble des fichiers, quels que soient les droits d'accès aux fichiers qui lui ont été octroyés, si le client a été défini en tant qu'**hôte digne de confiance**.

▼ Pour ajouter manuellement un hôte

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX) > Configure NFS (Configuration de NFS) > Set Up Hosts (Paramétrage des hôtes)**.

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

3. Saisissez le nom de l'hôte.

Il s'agit du nom permettant d'identifier l'hôte sur le système. Ce nom peut comporter uniquement des caractères alphanumériques (a-z, A-Z, 0-9), des tirets (-) et des points (.). Le premier caractère doit être une lettre (a-z ou A-Z uniquement).

4. Entrez la nouvelle adresse IP de l'hôte.

5. Si nécessaire, cochez la case **Trusted (De confiance)** pour accorder le statut de confiance à l'hôte.

Un hôte de confiance bénéficie d'un accès root à Sun StorEdge 5310 NAS Appliance, à cluster Sun StorEdge 5310 ou à système de passerelle Sun StorEdge 5310 Gateway System.

6. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

▼ Pour modifier les informations sur l'hôte

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX) > Configure NFS (Configuration de NFS) > Set Up Hosts (Paramétrage des hôtes)**.

2. Sélectionnez l'hôte pour lequel vous souhaitez effectuer des modifications et cliquez sur **Edit (Modifier)**.

3. Le cas échéant, modifiez les informations suivantes.

- **Host Name (Nom de l'hôte)** : il s'agit du nom permettant d'identifier l'hôte sur le système. Utilisez uniquement des lettres majuscules ou minuscules, des chiffres, des points (.) ou des tirets (-). Le premier caractère doit être une lettre.
- **IP Address (Adresse IP)** : il s'agit de l'adresse IP de l'hôte.
- **Trusted (De confiance)** : cochez cette case pour accorder le statut de confiance à l'hôte. Accordez le statut d'hôte de confiance avec vigilance.

4. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

▼ Pour supprimer un mappage d'hôte particulier

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX) > Configure NFS (Configuration de NFS) > Set Up Hosts (Paramétrage des hôtes)**.
2. Sélectionnez l'hôte à supprimer en cliquant sur l'entrée correspondante dans la liste d'hôtes.
3. Cliquez sur **Remove (Supprimer)**.
4. Cliquez sur **Apply (Appliquer)**.

Mappage des références d'utilisateurs et de groupes

Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System sont des serveurs conçus pour résider dans un environnement multiprotocolaire et fournir un modèle intégré pour le partage de données entre systèmes Windows et UNIX. Bien que les utilisateurs puissent accéder aux fichiers en même temps sur les systèmes Windows et UNIX, il n'existe aucun mécanisme normalisé permettant de définir un utilisateur dans les deux environnements (Windows et UNIX). Les objets peuvent être créés à l'aide de l'un ou l'autre environnement, mais les sémantiques de contrôle d'accès sont propres à chaque environnement. Cette section évoque le mappage de références. Pour plus de détails sur l'interaction entre le mappage de références d'utilisateurs ou de groupes et les objets sécurisables au sein du système, reportez-vous à la section « [Mappage et objets sécurisables](#) », page 241.

Le mappage de références permet d'établir une relation d'équivalence entre un utilisateur ou un groupe UNIX défini dans un fichier de configuration local ou une base de données NIS et un utilisateur ou un groupe de domaine Windows spécifié dans une base de données SAM Windows. Le mappage d'utilisateurs et de groupes est un mécanisme conçu pour établir une équivalence de références sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System afin de fournir un accès commun à partir des deux environnements.

Utilisateurs et groupes UNIX

Les utilisateurs et groupes UNIX sont définis dans des fichiers de configuration locaux (`passwd` et `group`) ou dans une base de données NIS. Tous les utilisateurs et groupes sont définis à l'aide d'un identificateur 32 bits connu, respectivement, sous les appellations UID ou GID. La plupart des systèmes UNIX font appel à des identificateurs 16 bits, mais cette fonction a été étendue à 32 bits sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System afin d'éviter les limites imposées par la plage d'un nombre 16 bits. Bien que l'identificateur UID ou GID permette de définir de manière unique un utilisateur ou un groupe au sein d'un domaine UNIX, aucun mécanisme n'est prévu pour assurer ce caractère d'unicité à travers l'ensemble des domaines. En général, la valeur zéro est appliquée au superutilisateur ou au groupe. Le superutilisateur dispose d'un accès quasiment illimité afin de pouvoir s'acquitter de ses tâches administratives.

Utilisateurs et groupes Windows

Les utilisateurs et groupes Windows sont définis dans une base de données SAM (Security Account Manager). Les utilisateurs et les groupes sont tous définis par un identificateur de sécurité SID (Security Identifier). Un SID correspond à une structure de longueur variable qui identifie de manière unique un utilisateur ou un groupe à la fois dans le domaine local et à travers tous les domaines Windows possibles.

Le format d'un SID est défini comme suit :

```
typedef struct _SID_IDENTIFIER_AUTHORITY {
    BYTE Value[6];
} SID_IDENTIFIER_AUTHORITY;

typedef struct _SID {
    BYTE Revision;
    BYTE SubAuthorityCount;
    SID_IDENTIFIER_AUTHORITY IdentifierAuthority;
    DWORD SubAuthority[ANYSIZE_ARRAY];
} SID;
```


Les champs inclus dans la structure du SID peuvent être interprétés comme décrit dans le [TABLEAU 7-3](#).

TABLEAU 7-3 Champs d'un SID

Champ	Valeur
Revision	Version du SID. La valeur de révision active est 1.
SubAuthorityCount	Nombre d'entrées d'autorité secondaire incluses dans le SID. Un SID peut comprendre jusqu'à 15 entrées subalternes.
IdentifierAuthority	Matrice de 6 octets identifiant le sous-système ayant généré le SID.
SubAuthority	Matrice de 32 bits d'autorités secondaires identifiant de manière unique l'objet de sécurité approprié : domaine, utilisateur, groupe ou alias. Un SID de domaine identifie de manière unique un domaine parmi tous les autres domaines d'autorité. Un SID d'utilisateur, de groupe ou d'alias est un SID de domaine auquel vient s'ajouter l'identificateur relatif (RID) approprié. Un RID est un identificateur 32 bits similaire à un UID ou un GID UNIX.

Par souci de lisibilité, les identificateurs de sécurité sont souvent affichés sous forme de chaîne : S-1-5-32-500. Ce SID contient un numéro de version de 1, une autorité de 5 et il contient deux autorités secondaires : 32 et 500. La valeur 500 désigne le RID.

Chaque domaine Windows dispose d'un SID unique ; chaque poste de travail et chaque serveur Windows désignent un domaine local nommé d'après le nom d'hôte associé. Ainsi, tous les postes de travail et tous les serveurs Windows disposent d'un identificateur de sécurité unique. Les domaines Windows répartis sur plusieurs machines sont gérés à partir d'un contrôleur de domaine principal (PDC). Le PDC centralise les tâches administratives relatives aux utilisateurs et aux groupes du domaine, et définit un SID unique pour tout le domaine. Par conséquent, un utilisateur de domaine peut se différencier d'un utilisateur de station de travail locale au moyen de la partie domaine du SID utilisateur.

Pour s'intégrer au modèle de domaine Windows, chaque système Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System génère également un SID en vue de définir son domaine local. Le SID est généré à l'aide d'un algorithme qui produit quatre autorités secondaires. La première autorité secondaire est dotée d'une valeur de 4, représentant une autorité non unique. Les trois autres autorités secondaires sont générées à l'aide d'un algorithme comprenant l'heure actuelle et l'une des adresses MAC3 du système afin de garantir le caractère unique de l'identificateur. Ce SID servira à représenter à la fois les utilisateurs locaux et NIS en ajoutant l'UID ou le GID UNIX au SID du domaine. Ce SID est stocké dans l'équivalent d'une base de données SAM locale.

Mappage de références

Des mappages d'utilisateurs et de groupes peuvent être définis afin de garantir aux utilisateurs l'accès à leurs fichiers à partir de systèmes Windows ou UNIX. Cette section décrit les algorithmes utilisés automatiquement en vue de générer des mappages d'utilisateurs et de groupes, et les stratégies appliquées lors du processus de connexion. Les règles de mappage utilisées pour mapper les utilisateurs et groupes UNIX à des utilisateurs et groupes Windows sont spécifiées par le biais de paramètres de stratégies système tandis que les mappages spécifiques sont définis dans la base de données des stratégies système.

Chaque mappage d'utilisateurs décrit le mode de mappage d'un utilisateur UNIX doté d'un UID spécifique à un utilisateur Windows faisant partie d'un domaine donné et associé à un RID spécifique. De la même manière, chaque mappage de groupes décrit le mode de mappage d'un groupe UNIX doté d'un GID spécifique à un groupe Windows faisant partie d'un domaine donné et associé à un RID spécifique.

Le format de mappage est défini comme suit :

```
<nom-utilisateur-UNIX>:<UID>:<nom-utilisateur-Windows>:<DOMAINE-NT>:<RID>
```

```
<nom-groupe-UNIX>:<GID>:<nom-groupe-Windows>:<DOMAINE-NT>:<RID>
```

Les utilisateurs et les groupes locaux sont définis dans les fichiers de groupe et de mot de passe passwd locaux. Ces fichiers respectent le format UNIX standard suivant :

```
<nom-utilisateur>:<mot-de-passe>:<UID>:<GID>:<commentaire>:<répertoire personnel>:<shell>
```

```
<nom-groupe>:<mot-de-passe>:<GID>:<liste-de-noms-utilisateurs-séparée-par-des-virgules>
```

Mappage d'utilisateurs

Le mappage d'utilisateurs permet de créer une relation d'équivalence entre un utilisateur UNIX et un utilisateur Windows pour lesquels les deux jeux de références doivent disposer de droits équivalents sur le système. Bien que le mécanisme du mappage prenne en charge le mappage bidirectionnel intégral, il est inutile de mapper des utilisateurs UNIX à des utilisateurs Windows en vue d'un accès NFS au système. Cela découle de la décision stratégique d'utiliser le domaine UNIX comme domaine de mappage de base.

Chaque fois qu'un utilisateur Windows se connecte au système, les fichiers de mappage sont vérifiés afin d'identifier les références UNIX de l'utilisateur. Pour déterminer l'UID UNIX de l'utilisateur Windows, une recherche est lancée sur le mappage d'utilisateurs afin de trouver une correspondance avec le nom d'utilisateur

et le nom de domaine Windows. Si une correspondance est détectée, l'UID UNIX est tiré de l'entrée trouvée. En l'absence de correspondance, l'UID UNIX de l'utilisateur est déterminé par le paramètre de stratégie de mappage d'utilisateurs.

Paramètres de stratégie de mappage d'utilisateurs

Il existe quatre paramètres de stratégie de mappage d'utilisateurs.

- `MAP_NONE` indique qu'aucun mappage prédéfini n'existe entre des utilisateurs Windows et des utilisateurs UNIX. Un nouvel UID UNIX unique est alors assigné à l'utilisateur Windows. L'UID est comparé aux occurrences existantes de la base de données `passwd` actuellement configurée et du fichier de mappage d'utilisateurs afin de vérifier qu'il est unique, puis un nouvel UID est défini. En général, le nouvel UID est plus grand d'un incrément que la valeur la plus grande trouvée lors de la recherche. La base de données des mots de passe (`passwd`) peut comprendre le fichier `passwd` NAS local et le fichier `passwd` NIS (si le service NIS est activé). Dans ce cas, vous devez modifier manuellement l'entrée de mappage si l'utilisateur Windows doit être mappé à un utilisateur UNIX existant.
- `MAP_ID` indique que l'UID UNIX correspond au RID de l'utilisateur Windows. Aucune recherche n'est lancée dans la base de données `passwd`.
- `MAP_USERNAME` indique que le nom d'utilisateur de l'utilisateur Windows est recherché dans la base de données `passwd`. Si une correspondance est trouvée entre le nom d'utilisateur Windows et le nom d'utilisateur UNIX, l'UID UNIX est dérivé de l'entrée correspondante. En l'absence de correspondance, un UID UNIX unique est généré à l'aide du mécanisme défini par le mécanisme `MAP_NONE`.
- `MAP_FULLNAME` indique que le nom complet Windows de l'utilisateur Windows est recherché dans la base de données `passwd`. Une correspondance est tentée avec le champ de commentaire UNIX de chaque entrée de mot de passe. Seule l'entrée de nom complet du champ de commentaire de la base de données `passwd` est comparée au nom complet Windows. Si une correspondance est détectée, l'UID UNIX de l'entrée trouvée est utilisé. En l'absence de correspondance, un UID UNIX unique est généré à l'instar du mécanisme `MAP_NONE`.

Les références de groupe appropriées à l'utilisateur Windows sont acquises à l'aide de l'algorithme de mappage de groupes. Pour plus d'informations, reportez-vous à la section « [Mappage de groupes](#) », page 106.

Exemple de stratégie de mappage d'utilisateurs

L'exemple suivant illustre un mappage d'utilisateurs qui associe l'utilisateur Windows `HOME\HOME\jeanm` à l'utilisateur UNIX `jean` et l'utilisateur Windows `HOME\HOME\alainw` à l'utilisateur UNIX `amw`.

```
jean:638:jean:HOME:1031
```

Mappage de groupes

Le mappage de groupes permet de créer une relation d'équivalence entre un groupe UNIX et un groupe Windows. Pour déterminer le GID UNIX approprié d'un utilisateur Windows, une recherche portant sur le mappage de groupes est lancée à l'aide du nom de domaine Windows de l'utilisateur et du nom de groupe principal Windows. Si une correspondance est trouvée, l'entrée de mappage définit le GID UNIX auquel le groupe de l'utilisateur Windows sera mappé. En l'absence de toute correspondance dans le mappage de groupes, le GID UNIX est déterminé par le paramètre de stratégie de mappage de groupes et une nouvelle entrée est créée dans le mappage de groupes, à l'exception de la stratégie `MAP_UNIXGID`.

Paramètres de stratégie de mappage de groupes

Il existe quatre paramètres de stratégie de mappage de groupes.

- `MAP_NONE` indique qu'aucun mappage prédéfini n'existe entre le groupe Windows et un groupe UNIX. Un nouveau GID UNIX unique est alors assigné au groupe. Le GID est comparé aux occurrences existantes de la base de données de groupes actuellement configurée et du fichier de mappage de groupes afin de vérifier qu'il est unique, puis un nouveau GID est défini, avec une valeur supérieure d'un incrément par rapport à la plus grande valeur trouvée lors de la recherche. La base de données des groupes peut comprendre le fichier de groupes NAS local et le fichier de groupes NIS (si le service NIS est activé). Dans ce cas, vous devez modifier manuellement l'entrée de mappage si le groupe Windows doit être mappé à un groupe UNIX existant.
- `MAP_ID` indique que le GID UNIX correspond au RID de groupe de l'utilisateur Windows tel qu'il a été trouvé par le jeton d'accès de l'utilisateur.
- `MAP_GROUPNAME` indique que le nom de groupe de l'utilisateur Windows est recherché dans la base de données des groupes. Si une correspondance est détectée, le GID UNIX est tiré de l'entrée trouvée. En l'absence de toute correspondance, un GID UNIX unique est généré.
- `MAP_UNIXGID` indique que le groupe UNIX de l'utilisateur Windows est déterminé par le champ GID principal dans l'entrée `passwd` obtenue lors du mappage d'utilisateurs.

Dans ce cas, le fichier `group.map` n'est pas consulté. S'il est impossible de déterminer un GID, le GID de groupe vide UNIX (60001) est utilisé.

La dernière étape consiste à déterminer la liste de groupes UNIX à laquelle appartient l'utilisateur. La base de données des groupes est parcourue à la recherche d'occurrences du nom d'utilisateur UNIX, selon les spécifications de la procédure de mappage d'utilisateurs. Le GID de chaque groupe, dans lequel figure le nom d'utilisateur UNIX, est ajouté à la liste de groupes dans les références de l'utilisateur.

Exemple de stratégie de mappage de groupes

L'exemple suivant illustre un mappage de groupes qui associe le groupe `HOME\BASE\Domain Admins` au groupe `wheel` UNIX et le groupe `HOME\BASE\Domain Users` au groupe d'utilisateurs UNIX.

```
wheel:800:Domain Admins:HOME\BASE:1005
```

```
users:100:Domain Users:HOME\BASE:513
```

La règle de mappage par défaut du système sera définie sur `MAP_NONE` pour les utilisateurs comme pour les groupes :

```
map.users=MAP_NONE
```

```
map.groups=MAP_NONE
```

La règle de mappage des utilisateurs ne doit pas nécessairement correspondre à celle des groupes. Un exemple de configuration de mappage possible est fourni ci-après. Dans cet exemple, la règle de mappage d'utilisateurs est définie sur `MAP_USERNAME` et celle des groupes sur `MAP_ID`.

```
map.users=MAP_USERNAME
```

```
map.groups=MAP_ID
```

Mappage de références intégré

L'identificateur root UNIX, 0 (UID ou GID), est toujours mappé au groupe d'administrateurs local. Le SID du groupe d'administrateurs local est un SID Windows prédéfini (intégré) : `S-1-5-32-544`. Ce mappage est conforme à la propriété assignée par Windows aux fichiers créés par l'administrateur du domaine.

La propriété de tels fichiers est toujours assignée au groupe d'administrateurs local intégré afin d'assurer l'autonomie des domaines. Cela permet d'éviter de perdre l'accès à ces fichiers dans le cas où le système est déplacé d'un domaine Windows sur un autre. Dans la zone d'affichage des autorisations Windows, ce SID figure sous l'entrée `HOSTNAME\Administrators`, où `HOSTNAME` désigne le nom d'hôte de Sun StorEdge 5310 NAS Appliance, de cluster Sun StorEdge 5310 ou de système de passerelle Sun StorEdge 5310 Gateway System.

▼ Pour définir la stratégie de mappage

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Manage SMB/CIFS Mapping (Gestion du mappage SMB/CIFS) > Configure Mapping Policy (Configuration de la stratégie de mappage)**.
2. Sélectionnez l'un des paramètres de mappage d'utilisateurs suivants dans la section **Windows <--> UNIX User Mapping Choice (Choix du mappage d'utilisateurs UNIX)**.
 - **Default Mapping (Mappage par défaut)** : sélectionnez cette option si aucune règle de mappage prédéfinie n'existe entre les utilisateurs Windows et UNIX. Les nouveaux utilisateurs recevront un ID unique, récemment créé par le système.
 - **Map by User Name (Mapper par nom d'utilisateur)** : cette option permet au système de mapper des utilisateurs UNIX et Windows portant des noms identiques ; un même utilisateur peut ainsi accéder à Sun StorEdge 5310 NAS Appliance, à cluster Sun StorEdge 5310 ou à système de passerelle Sun StorEdge 5310 Gateway System à partir des deux environnements.
 - **Map by Full Name (Mapper par nom complet)** : sélectionnez cette option pour mapper des utilisateurs UNIX et Windows portant le même nom complet.
3. Sélectionnez l'un des paramètres de mappage de groupes suivants dans la section **Windows <--> UNIX Group Mapping Choice (Choix du mappage de groupes UNIX)**.
 - **Default Mapping (Mappage par défaut)** : sélectionnez cette option si aucune règle de mappage prédéfinie n'existe entre les groupes Windows et UNIX. Les nouveaux groupes recevront un ID unique, récemment créé par le système.
 - **Map by Group Name (Mapper par nom de groupe)** : sélectionnez cette option pour mapper des groupes UNIX et Windows portant le même nom.
 - **Map to Primary Group (Mapper au groupe principal)** : choisissez cette option pour effectuer un mappage au groupe NFS dans le champ de groupe principal du fichier passwd configuré.
4. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Pour plus de détails sur l'interaction entre le mappage de références d'utilisateurs ou de groupes et les objets sécurisables au sein du système, reportez-vous à la section « [Mappage et objets sécurisables](#) », page 241.

▼ Pour mapper des utilisateurs et des groupes Windows à des groupes et utilisateurs UNIX

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Manage SMB/CIFS Mapping (Gestion du mappage SMB/CIFS) > Configure Maps (Configuration des mappages)**.
2. Cliquez sur **Add (Ajouter)**.
3. Dans la zone **NT User (Utilisateur NT)**, entrez les informations suivantes :
 - **Account (Compte)** : indiquez le nom du compte NT de l'utilisateur ou du groupe à mapper.
 - **RID (ID relatif)** : indiquez l'identificateur relatif permettant de définir de manière unique l'utilisateur ou le groupe NT au sein du domaine NT.
4. Dans la zone **UNIX User (Utilisateur UNIX)**, entrez les informations suivantes :
 - **Name (Nom)** : indiquez le nom d'utilisateur ou de groupe UNIX auquel mapper l'utilisateur ou le groupe NT spécifié.
 - **ID** : indiquez l'identificateur permettant de définir de manière unique l'utilisateur ou le groupe UNIX au sein du domaine UNIX.
5. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Pour plus de détails sur l'interaction entre le mappage de références d'utilisateurs ou de groupes et les objets sécurisables au sein du système, reportez-vous à la section « [Mappage et objets sécurisables](#) », page 241.

Définition de la sécurité du répertoire de fichiers

Il existe deux méthodes de définition de la sécurité du répertoire de fichiers :

- « [Définition de la sécurité du répertoire de fichiers en mode de groupe de travail](#) », page 110
- « [Définition de la sécurité du répertoire de fichiers en mode de domaine](#) », page 110

Définition de la sécurité du répertoire de fichiers en mode de groupe de travail

En mode de groupe de travail ou de partage sécurisé, la sécurité est paramétrée sur le partage lui-même (sécurité au niveau des partages) à l'aide de Web Administrator.

En mode de groupe de travail, le système considère qu'aucune authentification n'est effectuée sur le client et demande un mot de passe à chaque requête de connexion au partage.

Reportez-vous à la section « [Pour ajouter un partage SMB](#) », page 115 pour obtenir des instructions sur la définition de la sécurité au niveau des partages lors de l'ajout d'un partage. Reportez-vous à la section « [Pour modifier un partage SMB existant](#) », page 118 pour obtenir des instructions sur la définition de la sécurité au niveau des partages lors de la modification des partages.

Définition de la sécurité du répertoire de fichiers en mode de domaine

Vous pouvez gérer les droits d'accès à partir de Windows 2000 ou de Windows XP uniquement.

Remarque – Lorsque le système est configuré en mode de domaine, la définition des autorisations d'objets est gérée de la même façon que sur un contrôleur de domaine Windows standard. Il existe plusieurs façons de localiser les serveurs et de mapper des unités de disque afin de définir et gérer les autorisations de partage. Un seul exemple de cette procédure est illustré ci-dessous.

Remarque – Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System prennent uniquement en charge la sécurité sur les fichiers et les répertoires. La définition de la sécurité sur un partage transfère l'assignation de sécurité au répertoire sous-jacent.

▼ Pour définir la sécurité

1. Ouvrez l'Explorateur Windows.
2. Cliquez sur Outils > Connecter un lecteur réseau.
3. Dans la boîte de dialogue Connecter un lecteur réseau, sélectionnez une lettre de lecteur dans le menu déroulant Lecteur.
4. Localisez et sélectionnez le système Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System.
5. Cliquez sur OK.
6. Dans la fenêtre de l'Explorateur Windows, cliquez avec le bouton droit de la souris sur le partage de système pour lequel vous souhaitez définir des autorisations au niveau utilisateur.
7. Sélectionnez Propriétés dans le menu contextuel.
8. Sélectionnez l'onglet Sécurité dans la boîte de dialogue des propriétés.
9. Cliquez sur le bouton Autorisations.
10. Définissez les autorisations souhaitées.
Consultez la documentation de Windows pour obtenir plus d'informations sur la définition des autorisations.
11. Cliquez sur OK.

Partages, quotas et exportations

Ce chapitre indique les différentes méthodes permettant de contrôler l'accès des utilisateurs aux fichiers et aux volumes stockés sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System.

Ce chapitre aborde les sujets suivants :

- « Partages », page 113
- « Gestion de quotas », page 123
- « Paramétrage d'exportations NFS », page 129

Partages

Le protocole CIFS (Common Internet File System, protocole classique de système de fichiers Internet) est une version améliorée du protocole SMB (Server Message Block) de Microsoft. Ces deux protocoles permettent aux systèmes client fonctionnant sous environnement Windows d'accéder aux fichiers de Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System.

Une ressource partagée (également appelée **partage**) est une ressource locale située sur un serveur accessible aux clients Windows via le réseau. En général, sur un serveur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System, il s'agit d'un volume de système de fichiers ou d'une structure de répertoires sur un volume. Chaque partage est identifié par un nom sur le réseau. Pour les clients du réseau, le partage apparaît en tant que volume complet sur le serveur ; le chemin d'accès au répertoire local ne figure pas au-dessus de la racine du partage.

Remarque – Les partages et les répertoires sont des entités indépendantes. La suppression d'un partage n'affecte nullement le répertoire sous-jacent.

Les partages servent à fournir un accès réseau aux répertoires personnels d'un serveur de fichiers réseau. Un répertoire personnel est assigné à chaque utilisateur d'un volume de fichiers.

Il existe deux types de partages : les partages SMB/CIFS **statiques** et les partages SMB/CIFS **autohome**. Les partages statiques sont des ressources persistantes ; ils restent définis, que les utilisateurs soient ou non rattachés au serveur. Les partages autohome sont des partages temporaires créés quand un utilisateur se connecte au système. Ils sont ensuite supprimés lorsque l'utilisateur se déconnecte.

Lorsqu'un utilisateur parcourt le système, seuls les partages définis de manière statique et les partages autohome des utilisateurs connectés sont répertoriés.

Partages statiques

Un partage statique est créé afin de permettre à cet utilisateur de mapper son répertoire personnel en tant qu'unité de disque réseau sur une station de travail client. Par exemple, un volume **vol1** peut contenir un répertoire personnel nommé **personnel**, et des sous-répertoires pour les utilisateurs **Pierre** et **Marie**. Les partages sont définis comme suit.

TABLEAU 8-1 Exemples de chemins de partage

Nom du partage	Chemin d'accès au répertoire
Pierre	/vol1/personnel/pierre
Marie	/vol1/personnel/marie

Si la définition et la gestion d'un partage de répertoire personnel statique pour chaque utilisateur Windows ayant accès au système s'avèrent fastidieuses, vous pouvez avoir recours à la fonction autohome. Pour plus d'informations, reportez-vous à la section « [Partages autohome](#) », page 121.

Configuration de partages statiques

Le panneau **Configure Shares (Configuration des partages)** vous permet d'ajouter, de visualiser et de mettre à jour les partages SMB statiques.

Le tableau situé dans la partie supérieure du panneau **Configure Shares (Configuration des partages)** affiche des informations sur tous les partages SMB existants. Sont notamment indiqués le nom du partage et les répertoires partagés, ainsi que les noms de conteneurs et les appels de la base de données du bureau, ainsi que des informations concernant les groupes de travail Windows uniquement (utilisateur, groupe, umask et mots de passe).

Remarque – Pour pouvoir être partagé, le volume ou le répertoire doit d’abord avoir été créé.

Par défaut, un partage est masqué est créé pour la racine de chaque volume et n’est accessible que par les administrateurs du domaine. Les administrateurs se servent généralement de ces partages pour migrer des données et créer des structures de répertoires. Les noms de partage figurent dans l’écran Configure Shares (Configuration des partages). Les partages utilisateur ne sont créés qu’à l’issue de cette étape, étant donné que le partage de répertoires à un niveau inférieur à la racine du volume facilite l’administration de la sécurité.

Création de partages statiques

Pour pouvoir créer un partage, vous devez d’abord avoir créé un volume de fichiers. Pour plus d’informations, reportez-vous à la section « [Création d’un volume de fichiers ou d’un segment](#) », page 49.

▼ Pour ajouter un partage SMB

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Shares (Configuration des partages)**.

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

3. Indiquez le nom du partage à ajouter dans le champ **Share Name (Nom du partage)**.

Il s’agit du nom sous lequel le partage sera connu sur le réseau. Celui-ci ne doit pas dépasser quinze caractères et ne peut contenir aucun des caractères suivants :

= | : ; \ " ? < > * /

4. (Facultatif) Ajoutez un commentaire pour décrire le partage.

Vous pouvez entrer jusqu’à 60 caractères alphanumériques.

5. **Cochez la case Desktop DB Calls (Appels à la base de données du bureau) dans la section Mac Ext. (Extensions Mac) pour permettre au système d'accéder aux informations de la base de données du bureau Macintosh et de les définir.**

La vitesse d'accès au fichier client Macintosh est alors accélérée et les clients non Macintosh sont autorisés à accéder aux fichiers Macintosh sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System.

6. **Sélectionnez le volume à partager dans la liste des volumes disponibles figurant dans le menu déroulant Volume Name (Nom du volume).**

7. **Indiquez un répertoire existant dans le champ Directory (Répertoire).**

Il est impossible de créer un répertoire dans ce champ. Les noms de répertoires doivent respecter la casse.

Remarque – Ne laissez pas le champ Directory (Répertoire) vide.

8. **(Facultatif) Le champ Container (Conteneur) indique le conteneur ADS dans lequel publier le partage.**

Si vous avez activé l'option ADS dans le panneau **Set Up ADS (Paramétrage d'ADS)**, ce champ est disponible. Toutefois, vous n'êtes pas tenu d'indiquer un conteneur ADS.

9. **Si vous souhaitez l'indiquer, tapez le chemin d'accès ADS au partage en utilisant la syntaxe du nom distinctif (DN) LDAP.**

Pour plus d'informations, reportez-vous à la section « [Pour publier les partages dans ADS](#) », page 91.

10. **Remplissez les champs User ID (ID utilisateur), Group ID (ID de groupe) et Password (Mot de passe), si disponible.**

Les champs **User ID (ID utilisateur)**, **Group ID (ID de groupe)** et **Password (Mot de passe)** sont uniquement disponibles si vous avez activé le mode du groupe de travail Windows (et non celui du domaine NT). Pour obtenir des informations sur l'activation des modèles de sécurité Windows, reportez-vous à la section « [Configuration de la sécurité Windows](#) », page 24.

Les groupes de travail Windows appliquent une sécurité au niveau des partages. Dans l'écran ci-dessus, les champs User ID (ID utilisateur), Group ID (Identificateur de groupe) ainsi que ceux réservés aux mots de passe constituent la seule mesure de nature à assurer une protection des fichiers Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System et un contrôle d'accès des utilisateurs appartenant aux groupes de travail Windows. Autrement dit, les droits d'accès à un répertoire sont déterminés en fonction de la

définition du partage et non de l'utilisateur. Le système considère que le client n'effectue aucune authentification et demande un mot de passe à chaque tentative de connexion au partage.

Vous pouvez créer plusieurs partages pour un même répertoire avec des ID utilisateur, ID de groupe ou mots de passe différents et ensuite attribuer, à chaque utilisateur, un mot de passe pour un partage spécifique. À l'aide de quotas, vous pouvez également gérer, de manière individuelle, les restrictions liées à des groupes ou des utilisateurs en fonction de l'espace du volume de fichiers ou du nombre de fichiers utilisés. Pour plus d'informations sur les quotas, reportez-vous à la section « [Gestion de quotas](#) », page 123.



Attention – User ID (ID utilisateur) : vous devez saisir l'ID de l'utilisateur accédant au répertoire bénéficiant de ce partage. La valeur par défaut de ce champ est 0 (zéro), qui correspond à la valeur du superutilisateur UNIX. Cependant, il convient d'utiliser cette valeur avec précaution. En mode de groupe de travail Windows, la valeur zéro désactive la protection de tous les fichiers et répertoires de ce partage.

- **R/W Password (Mot de passe en lecture/écriture) :** saisissez le mot de passe défini pour les utilisateurs du groupe Windows ayant un accès en lecture et en écriture aux répertoires mis en partage.
- **Confirm R/W Password (Confirmation du mot de passe en lecture/écriture) :** ressaisissez le mot de passe en lecture/écriture à titre de confirmation.
- **R/O Password (Mot de passe en lecture seule) :** saisissez le mot de passe défini pour les utilisateurs du groupe de travail Windows ayant un accès au partage en lecture seule.
- **Confirm R/O Password (Confirmation du mot de passe en lecture seule) :** ressaisissez le mot de passe en lecture seule à titre de confirmation.

11. Dans le champ Umask (Umask), entrez le masque de création de fichiers (le cas échéant) que vous souhaitez appliquer au partage.

La commande umask définit les droits qui seront attribués aux fichiers et aux répertoires créés en mode de partage. Elle définit les bits de permission à désactiver lors de la création d'un fichier.

Ce masque est exprimé en mode octal sous la forme d'un nombre de trois bits pouvant être facilement mappé sur la représentation des autorisations de fichiers UNIX. Le masque de protection utilise les règles UNIX standard, à l'exception des

attributs en lecture seule sous DOS. Si l'attribut en lecture seule sous DOS est défini lors de la création du fichier, tous les bits en écriture seront supprimés des droits d'accès au fichier dès que le masque umask est appliqué.

Le tableau suivant affiche des exemples de permissions umask, ainsi que l'impact de l'attribut en lecture seule sous DOS.

TABLEAU 8-2 Exemples de permissions Umask

Umask	Nouvelles permissions de répertoire		Nouvelles permissions de fichier	
	Lecture/écriture sous DOS	Lecture seule sous DOS	Lecture/écriture sous DOS	Lecture seule sous DOS
000	777 (rwxrwxrwx)	555 (r-xr-xr-x)	666 (rw-rw-rw)	444 (r--r--r--)
777	000 (-----)	000 (-----)	000 (-----)	000 (-----)
022	755 (rwxr-xr-x)	555 (r-xr-xr-x)	644 (rw-r--r--)	444 (r--r--r--)
002	775 (rwxrwxr-x)	555 (r-xr-xr-x)	664 (rw-rw-r--)	444 (r--r--r--)

12. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

▼ Pour modifier un partage SMB existant

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Shares (Configuration des partages)**.
2. Sélectionnez le partage à mettre à jour.
3. Cliquez sur **Edit (Modifier)**.
4. Le champ **Old Share Name (Ancien nom du partage)** affiche le nom actuel du partage. Pour le modifier, saisissez un nouveau nom dans le champ **Share Name (Nom du partage)**.

Les caractères suivants ne sont pas valides pour le nom du partage :

= | : ; \ " ? < > * /

5. Vous pouvez modifier la description du partage dans le champ **Comment (Commentaire)**. Vous pouvez entrer jusqu'à 60 caractères alphanumériques.
6. Cochez la case **Desktop DB Calls (Appels à la base de données du bureau)** dans la section **Mac Extensions (Extensions Mac)** pour permettre au système d'accéder aux informations de la base de données du bureau Macintosh et de les définir.

La vitesse d'accès au fichier client Macintosh est alors accélérée et les clients non Macintosh sont autorisés à accéder aux fichiers Macintosh sur Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System.

- 7. Pour modifier le chemin du partage, saisissez un nom d'un répertoire existant dans le champ Path (Chemin).**

Il est impossible de créer un répertoire dans ce champ. Les noms de répertoires doivent respecter la casse.

- 8. Indiquez un nouveau Container (Conteneur), si nécessaire.**

Ce champ permet de spécifier le conteneur ADS dans lequel publier le partage. Il est disponible uniquement si vous avez activé ADS dans le panneau Set Up ADS (Paramétrage d'ADS). Indiquez l'emplacement du chemin d'accès ADS au partage en utilisant la syntaxe du nom distinctif LDAP. Pour plus d'informations, reportez-vous à la section « [Pour activer ADS](#) », page 89.

- 9. Remplissez les champs User ID (ID utilisateur), Group ID (ID de groupe) et Password (Mot de passe), si disponible.**

Pour des informations détaillées sur ces champs, reportez-vous à l'étape 10, page 116.

- 10. Enfin, vous pouvez modifier le paramètre Umask en respectant les règles correspondantes décrites à l'étape 11, page 117.**

- 11. Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.**

▼ Pour supprimer un partage SMB/CIFS

- 1. Dans le volet de navigation, sélectionnez Windows Configuration (Configuration Windows) > Configure Shares (Configuration des partages).**
- 2. Sélectionnez le partage à supprimer du tableau des partages.**
- 3. Cliquez sur Remove (Supprimer).**
- 4. Cliquez sur Yes (Oui) pour supprimer le partage.**

Configuration de clients SMB/CIFS

Une fois la configuration des paramètres réseau et de sécurité terminée, Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System sera accessible par les clients SMB/CIFS en s'enregistrant auprès du navigateur principal de leur réseau local.

Les clients peuvent se connecter de l'une des manières suivantes.

Windows 98, XP et Windows NT 4.0

Les utilisateurs se connectent en mappant l'unité de disque réseau depuis l'Explorateur Windows ou en cliquant sur l'icône Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System dans la fenêtre **Voisinage réseau**.

S'ils décident de mapper l'unité de disque réseau, ils devront indiquer le chemin UNC (Universal Naming Convention) permettant d'accéder à Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System. Un chemin UNC se compose du nom de l'ordinateur suivi du nom du partage, comme suit : \\nom_ordinateur\nom_partage. S'ils se connectent par l'intermédiaire de la fenêtre **Voisinage réseau**, ils devront indiquer le nom du système à utiliser pour identifier Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System sur le réseau.

Windows 2000, XP et 2003

Si le service ADS n'est pas installé, les utilisateurs se connectent en mappant l'unité de disque réseau depuis l'Explorateur Windows ou en cliquant sur l'icône Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System dans la fenêtre **Favoris réseau**.

S'ils mappent l'unité de disque réseau, ils devront indiquer le chemin UNC permettant d'accéder à Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System. Un chemin UNC se compose du nom de l'ordinateur suivi du nom du partage, comme suit : \\nom_ordinateur\nom_partage. S'ils se connectent par l'intermédiaire de la fenêtre **Voisinage réseau**, ils devront indiquer le nom du système à utiliser pour identifier Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System sur le réseau.

Si le service ADS est installé, les utilisateurs peuvent établir une connexion en cliquant sur un partage Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System publié dans ADS.

DOS

Les utilisateurs doivent entrer la commande **net use** dans la ligne de commande pour mapper un partage sur une lettre de lecteur. Ils doivent indiquer le chemin UNC permettant d'accéder à Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 ou système de passerelle Sun StorEdge 5310 Gateway System. Ce chemin se compose du nom de l'ordinateur suivi du nom du partage, comme suit : \\nom_ordinateur\nom_partage.

Partages autohome

La fonction de partage autohome SMB/CIFS dispense les utilisateurs de définir et de gérer les partages de répertoires personnels pour chaque utilisateur Windows accédant au système. Le système crée des partages autohome lorsqu'un utilisateur se connecte et les supprime lorsqu'il se déconnecte. Les tâches administratives nécessaires à la gestion des comptes utilisateur sont ainsi réduites et l'efficacité des ressources du serveur améliorée.

Pour la configurer, activez la fonction autohome et fournissez un chemin autohome correspondant au chemin du répertoire de base pour les partages de répertoires. Par exemple, si le répertoire personnel d'un utilisateur est `/vol1/personnel/marie`, le chemin d'accès à autohome est `/vol1/personnel`. Le partage temporaire est nommé `marie`. Le nom du répertoire personnel de l'utilisateur doit être identique au nom de connexion de l'utilisateur.

Lorsqu'un utilisateur se connecte, le serveur recherche un sous-répertoire correspondant au nom de l'utilisateur. S'il trouve une correspondance et que le partage n'existe pas déjà, il ajoute un partage temporaire. Lorsque l'utilisateur se déconnecte, le serveur supprime le partage.

Les clients Windows peuvent déconnecter automatiquement un utilisateur après 15 minutes d'inactivité entraînant ainsi la suppression du partage autohome de la liste des partages publiés. Il s'agit du comportement normal du protocole CIFS. Si l'utilisateur clique sur le nom du serveur ou s'il tente d'accéder au système (à partir de la fenêtre de l'Explorateur, par exemple), le partage réapparaît automatiquement.

Remarque – Tous les partages autohome sont supprimés à la réinitialisation du système.

Les partages autohome étant créés et supprimés automatiquement, leur configuration dépend essentiellement de l'activation de cette fonction.

▼ Pour activer les partages autohome

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Autohome (Configuration autohome)**.
2. Cochez la case **Enable Autohome (Activer autohome)**.
3. Indiquez un chemin dans le champ **Autohome Path (Chemin d'accès à autohome)**.
Pour plus d'informations sur ce chemin d'accès, reportez-vous à la section « [Partages autohome](#) », page 121.

4. Indiquez un conteneur ADS dans le champ ADS Container.

Pour plus d'informations, reportez-vous à la section « [Active Directory Service](#) », page 88.

5. Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.

Gestion de quotas

Les panneaux de **gestion des quotas** vous permettent d'administrer les quotas d'utilisation des répertoires et des volumes de fichiers de Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System. Les quotas d'utilisateurs et les quotas de groupes déterminent l'espace disque disponible pour un utilisateur ou un groupe et définissent le nombre de fichiers qu'un utilisateur ou qu'un groupe peut écrire dans un volume. Les quotas de la structure de répertoire déterminent l'espace disque disponible pour un répertoire particulier et/ou le nombre de fichiers pouvant y être écrit.

Pour définir les limites de fichier et d'espace pour les utilisateurs et les groupes, reportez-vous à la section « [Configuration de quotas d'utilisateurs et de groupes](#) », page 123. Pour définir les limites de fichiers et d'espace de répertoires spécifiques, reportez-vous à la section « [Configuration des quotas de la structure de répertoire](#) », page 127.

Configuration de quotas d'utilisateurs et de groupes

Le panneau **Configure User and Group Quotas (Configuration des quotas d'utilisateurs et de groupes)** vous permet de gérer les quotas d'utilisation des volumes pour les utilisateurs et les groupes NT et UNIX. Il affiche des quotas individuels, root ou par défaut pour le volume sélectionné. Les paramètres définis pour **l'utilisateur par défaut** et le **groupe par défaut** sont ceux utilisés pour l'ensemble des utilisateurs et des groupes n'ayant pas de quotas individuels.

À propos des limites fixes et dépassables

On appelle **limite fixe** la valeur maximale d'espace disponible pour un utilisateur ou un groupe.

Lorsqu'une **limite dépassable** (valeur inférieure ou égale à la limite fixe) est atteinte, un délai de sept jours est accordé. Une fois cette période écoulée, l'utilisateur ou le groupe ne peut plus écrire dans le volume tant que le volume d'espace utilisé ne passe pas en dessous de la limite dépassable.

La limite fixe doit être égale ou supérieure à la limite dépassable. L'espace disque ne doit pas dépasser environ 2 Téraoctets (To). La limite fixe du nombre de fichiers ne doit pas être supérieure à 4 milliards de fichiers.

Le **superutilisateur** et le **groupe root** sont automatiquement définis de manière à n'avoir aucune limite fixe ou dépassable en matière d'espace ou de nombre de fichiers. Il est également impossible de leur appliquer des quotas.

▼ Pour appliquer des quotas au volume de fichiers

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Edit Properties (Modification des propriétés)**.
2. Sélectionnez le volume de fichiers pour lequel vous activez les quotas dans le menu déroulant **Volume Name (Nom du volume)**.
3. Vérifiez que la case **Enable Quotas (Activer les quotas)** est cochée. Si ce n'est pas le cas, cochez-la.
4. Cliquez sur **Apply (Appliquer)**.

▼ Pour ajouter un quota d'utilisateurs ou de groupes

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Manage Quotas (Gestion de quotas) > Configure User and Group Quotas (Configuration des quotas d'utilisateurs et de groupes)**.
2. Cliquez sur **Users (Utilisateurs)** si vous souhaitez configurer un quota d'utilisateurs ou sur **Groups (Groupes)** si vous souhaitez configurer un quota de groupes.

3. Sélectionnez le nom du volume de fichiers pour lequel vous ajoutez un quota dans la liste déroulante **Volume**.

Le tableau de cet écran indique les quotas d'utilisateurs ou de groupes individuels, root et par défaut du volume de fichiers sélectionné.

4. Pour ajouter des quotas d'utilisateurs ou de groupes, cliquez sur **Add (Ajouter)**.
5. Définissez si l'utilisateur ou le groupe désigné appartient à un environnement **UNIX** ou **NT** en sélectionnant le bouton radio approprié.
6. Indiquez le nom d'utilisateur ou de groupe approprié (ainsi que le nom du domaine pour les utilisateurs ou les groupes NT).
7. Définissez les limites d'espace disque pour l'utilisateur ou le groupe sélectionné. Choisissez l'une des trois options suivantes :
 - **Default (Par défaut)** : choisissez cette option pour définir des limites fixe et dépassable identiques à celles de l'utilisateur ou du groupe par défaut.
 - **No limit (Aucune limite)** : choisissez cette option pour allouer un espace illimité à l'utilisateur ou au groupe.

- **Custom (Personnalisé)** : choisissez cette option pour définir une limite particulière. Indiquez si vous souhaitez afficher les quotas en **Kilo-octets**, **Méga-octets** ou **Giga-octets**. Puis, entrez les limites **Soft (Dépassable)** et **Hard (Fixe)** de l'utilisateur ou du groupe.

Remarque – Lors du paramétrage de quotas d'utilisateurs, vous devez définir les limites fixe et dépassable.

8. **Indiquez le nombre limite de fichiers qu'un utilisateur ou un groupe peut écrire dans le volume de fichiers. Choisissez l'une des trois options suivantes :**
 - **Default (Par défaut)** : choisissez cette option pour définir des limites fixe et dépassable identiques à celles de l'utilisateur ou du groupe par défaut.
 - **No Limit (Aucune limite)** : choisissez cette option pour permettre à l'utilisateur ou au groupe d'écrire un nombre illimité de fichiers dans le volume de fichiers.
 - **Custom (Personnalisé)** : choisissez cette option pour définir une limite de fichier particulière. Puis, entrez les limites **Soft (Dépassable)** et **Hard (Fixe)** correspondant au nombre de fichiers.
9. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

▼ Pour modifier un quota d'utilisateurs ou de groupes

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Manage Quotas (Gestion de quotas) > Configure User and Group Quotas (Configuration des quotas d'utilisateurs et de groupes)**.
2. Cliquez sur **Users (Utilisateurs)** pour modifier un quota d'utilisateurs ou sur **Groups (Groupes)** pour changer un quota de groupes.
3. Sélectionnez le nom du volume de fichiers pour lequel modifier les quotas dans la liste déroulante **Volume**.

Le tableau de cet écran répertorie les quotas d'utilisateurs ou de groupes individuels, root et par défaut pour le volume de fichiers sélectionné.
4. Sélectionnez l'utilisateur ou le groupe pour lequel modifier un quota et cliquez sur **Edit (Modifier)**.
5. Modifiez les limites d'espace disque pour l'utilisateur ou le groupe sélectionné.

Choisissez l'une des trois options suivantes :

- **Default (Par défaut)** : choisissez cette option pour définir des limites fixe et dépassable identiques à celles de l'utilisateur ou du groupe par défaut.
- **No limit (Aucune limite)** : choisissez cette option pour allouer un espace illimité à l'utilisateur ou au groupe.
- **Custom (Personnalisé)** : choisissez cette option pour définir une limite particulière. Indiquez si vous souhaitez afficher les quotas en **Kilo-octets**, **Méga-octets** ou **Giga-octets**. Puis, entrez les limites **Soft (Dépassable)** et **Hard (Fixe)** de l'utilisateur ou du groupe.

6. **Modifiez le nombre limite de fichiers qu'un utilisateur ou un groupe peut écrire dans le volume de fichiers. Choisissez l'une des trois options suivantes :**
 - **Default (Par défaut) :** choisissez cette option pour définir des limites fixe et dépassable identiques à celles de l'utilisateur ou du groupe par défaut.
 - **No Limit (Aucune limite) :** choisissez cette option pour permettre à l'utilisateur ou au groupe d'écrire un nombre illimité de fichiers dans le volume de fichiers.
 - **Custom (Personnalisé) :** choisissez cette option pour définir une limite de fichier particulière. Puis, entrez les limites **Soft (Dépassable)** et **Hard (Fixe)** correspondant au nombre de fichiers.
7. **Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.**

Suppression de quotas d'utilisateurs ou de groupes

Les quotas root et par défaut ne peuvent pas être supprimés. Vous pouvez supprimer un quota individuel en le définissant sur l'espace disque et le nombre de fichiers par défaut.

▼ Pour supprimer un quota

1. **Dans le volet de navigation, sélectionnez File Volume Operations (Opérations sur un volume de fichiers) > Manage Quotas (Gestion de quotas) > Configure User and Group Quotas (Configuration des quotas d'utilisateurs et de groupes).**
2. **Dans le panneau Configure User and Group Quotas (Configuration de quotas d'utilisateurs et de groupes), sélectionnez Users (Utilisateurs) pour supprimer un quota d'utilisateurs ou Groups (Groupes) pour supprimer un quota de groupes.**
3. **Sélectionnez le quota à supprimer du tableau et cliquez sur Edit (Modifier).**
4. **Dans la boîte de dialogue Edit Quota Setting (Modification d'un paramètre de quota), cliquez sur l'option Default (Par défaut) dans les sections Disk Space Limits (Limites d'espace disque) et File Limits (Limites de fichiers).**
5. **Cliquez sur Apply (Appliquer) pour supprimer le paramètre de quota.**

Configuration des quotas de la structure de répertoire

Le panneau **Configure Directory Tree Quotas (Configuration des quotas de la structure de répertoire)** (DTQ) permet d'effectuer la gestion de quotas de certains répertoires du système de fichiers. Les quotas de la structure de répertoire déterminent l'espace disque disponible pour un répertoire et le nombre de fichiers pouvant y être écrit. Vous ne pouvez configurer que les quotas des répertoires créés dans ce panneau et non ceux des répertoires qui existaient précédemment.

▼ Pour créer une structure de répertoire à l'aide d'un DTQ

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Manage Quotas (Gestion de quotas) > Configure Directory Tree Quotas (Configuration des quotas de la structure de répertoire)**.
2. Sélectionnez le volume de fichiers pour lequel vous configurez un quota de structure de répertoire dans le menu déroulant correspondant.
3. Cliquez sur **Add (Ajouter)**.
4. Dans le champ **DTQ Name (Nom DTQ)**, entrez un nom permettant d'identifier le quota de la structure de répertoire.
5. Dans le champ **DirName (Nom_répertoire)**, indiquez le nom du nouveau répertoire.
6. En dessous du champ **Path (Chemin)** figure la structure de répertoire du volume de fichiers sélectionné.
Pour afficher le contenu d'un dossier, cliquez sur le symbole situé en regard du dossier ou double-cliquez sur l'icône du dossier. Sélectionnez ensuite le répertoire dans lequel le nouveau répertoire sera stocké. Développez l'arborescence jusqu'à ce que le chemin complet du répertoire s'affiche dans le champ **Path (Chemin)**.
7. Sélectionnez la limite d'espace disque pour le répertoire dans la section **Disk Space Limits (Limites d'espace disque)**, en sélectionnant **No Limit (Aucune limite)** ou **Custom (Personnalisé)**.
 - Sélectionnez **No Limit (Aucune limite)** afin d'allouer un espace disque illimité au répertoire.
 - Sélectionnez **Custom (Personnalisé)** afin de définir l'espace disque maximal pouvant être occupé par le répertoire.
8. Précisez si vous souhaitez exprimer les quotas en méga-octets ou en giga-octets et indiquez la limite d'espace disque dans le champ **Max Value (Valeur maximale)**.

Si vous paramétrez l'option **Custom (Personnalisé)** sur 0 (zéro), l'effet est le même que si vous sélectionnez l'option **No Limit (Aucune Limite)**.

9. Dans le champ **File Limits (Limites de fichiers)**, sélectionnez le nombre maximal de fichiers pouvant être écrits dans ce répertoire (**No Limit (Aucune limite)** ou **Custom (Personnalisé)**).
 - L'option **No Limit (Aucune limite)** permet d'écrire un nombre illimité de fichiers dans ce répertoire.
 - L'option **Custom (Personnalisé)** permet de définir une limite de fichiers. Saisissez ensuite la limite de fichiers dans le champ **Max Value (Valeur maximale)**.
10. Cliquez sur **Apply (Appliquer)** pour ajouter le quota.

▼ Pour modifier un quota de structure de répertoire existant

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Manage Quotas (Gestion de quotas) > Configure Directory Tree Quotas (Configuration des quotas de la structure de répertoire)**.
2. Sélectionnez le quota à modifier dans le tableau, puis cliquez sur **Edit (Modifier)**.
3. Modifiez le nom qui identifie le quota de la structure de répertoire dans le champ **DTQ Name (Nom DTQ)**.

Le champ **Path (Chemin)** est en lecture seule ; il indique le chemin d'accès au répertoire.
4. Dans la zone **Disk Space Limits (Limites d'espace disque)**, sélectionnez la limite d'espace disque pour le répertoire (**No Limit (Aucune limite)** ou **Custom (Personnalisé)**).
 - Sélectionnez **No Limit (Aucune limite)** afin d'allouer un espace disque illimité au répertoire.
 - Sélectionnez l'option **Custom (Personnalisé)** afin d'attribuer un volume maximal d'espace disque.
5. Précisez si vous souhaitez exprimer les quotas en méga-octets ou en giga-octets et indiquez la limite d'espace disque dans le champ **Max Value (Valeur maximale)**.

Si vous paramétrez l'option **Custom (Personnalisé)** sur 0 (zéro), l'effet est le même que si vous sélectionnez l'option **No Limit (Aucune Limite)**.
6. Dans la zone **File Limits (Limites de fichiers)**, sélectionnez le nombre maximal de fichiers pouvant être consignés dans ce répertoire (**No Limit (Aucune limite)** ou **Custom (Personnalisé)**).
 - L'option **No Limit (Aucune limite)** vous permet d'écrire un nombre illimité de fichiers dans ce répertoire.
 - L'option **Custom (Personnalisé)** permet de définir une limite de fichiers.
7. Saisissez la limite de fichiers dans le champ **Max Value (Valeur maximale)**.
8. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Remarque – Lorsque vous déplacez ou renommez un répertoire contenant un paramètre de quota de structure de répertoire (DTQ), le système met automatiquement à jour la spécification du chemin DTQ.

▼ Pour supprimer un quota de structure de répertoire

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Manage Quotas (Gestion de quotas) > Configure Directory Tree Quotas (Configuration des quotas de la structure de répertoire)**.
2. Sélectionnez le quota à supprimer du tableau.
3. Cliquez sur **Delete (Supprimer)** pour supprimer le paramètre de quota.

La suppression d'un quota de structure de répertoire (DTQ) entraîne celle du paramètre de quota. Cependant, le répertoire ou les fichiers de ce répertoire ne sont pas supprimés.

Remarque – Si vous supprimez un répertoire contenant un paramètre DTQ, le répertoire ainsi que le paramètre DTQ sont supprimés.

Paramétrage d'exportations NFS

Les exportations NFS (Network File System) permettent d'accorder des droits d'accès aux utilisateurs UNIX (et Linux). La table située dans le panneau **Configuring Exports (Configuration des exportations)** contient des informations sur les exportations NFS actuelles, notamment les répertoires accessibles, le nom de l'hôte et le niveau d'accès (lecture/écriture ou lecture seule) pour chacune d'entre elles.

Tout nom d'hôte commençant par le symbole @ correspond à un groupe d'hôtes. Par exemple, le nom d'hôte **@general** comprend tous les hôtes et le nom **@trusted** comprend tous les hôtes de confiance. Pour plus d'informations sur les hôtes de confiance, reportez-vous à la section « [Configuration des hôtes](#) », page 99.

Vous créez des exportations en spécifiant les privilèges d'accès d'un hôte UNIX particulier.

▼ Pour créer des exportations

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX) > Configure NFS (Configuration de NFS) > Configure Exports (Configuration d'exportations)**.

Le tableau situé dans ce panneau contient des informations sur les exportations actuelles. Si vous n'avez pas créé d'exportations, ce panneau est vide.

2. Cliquez sur le bouton **Add (Ajouter)** afin d'ajouter une exportation.
3. Dans le champ **Volume (Volume)**, choisissez le volume pour lequel attribuer des droits d'accès NFS à l'hôte UNIX.
4. Dans le chemin **Path (Chemin)**, indiquez le répertoire pour lequel attribuer des droits d'accès NFS à l'hôte UNIX.
Si vous laissez ce champ vide, le système exporte le répertoire racine du volume.
5. Dans la section **Access (Accès)**, précisez si les hôtes disposent de privilèges de type **Read/Write (Lecture/Écriture)**, **Read/Only (Lecture seule)** ou **No Access (Accès interdit)** sur le volume sélectionné.
6. Dans le champ **Hosts (Hôtes)**, choisissez l'hôte ou les hôtes pour lesquels vous définissez une exportation NFS.

Les options disponibles sont les suivantes :

- **Host Netgroups (Groupes réseau d'hôtes)** : sélectionnez ce bouton radio pour sélectionner un groupe réseau d'hôtes. Dans le menu déroulant correspondant, choisissez le groupe réseau pour lequel vous définissez l'exportation.
- **Host Group (Groupe d'hôtes)** ; sélectionnez ce bouton radio pour sélectionner un groupe d'hôtes. Dans le menu déroulant, choisissez soit **general (général)**, pour tous les hôtes, soit **trusted (de confiance)**, pour les hôtes de confiance, soit un groupe d'hôtes défini par l'utilisateur.
- **Known Host (Hôte connu)** : cette option permet d'assigner l'exportation à un hôte ajouté via le panneau **Set Up Hosts (Paramétrage des hôtes)**. Dans le menu déroulant correspondant, choisissez l'hôte pour lequel vous définissez l'exportation.
- **Other Host (Autre hôte)** : cette option permet d'assigner l'exportation à un hôte n'ayant pas été ajouté via le panneau **Set Up Hosts (Paramétrage des hôtes)**. Entrez ensuite le nom de l'hôte.

7. Dans la section **Map Root User (Mappage de superutilisateur)**, choisissez une méthode pour mapper l'ID utilisateur pour les superutilisateurs.

Les options disponibles sont les suivantes :

- **Anonymous users (Utilisateurs anonymes)** : cette option permet de mapper l'ID utilisateur des superutilisateurs à l'ID des utilisateurs anonymes.
- **Root User (Superutilisateur)** : cette option permet de mapper l'ID utilisateur des superutilisateurs à l'ID de root (UID=0).
- **Map to UID (Mapper à l'ID utilisateur)** : cette option permet d'assigner un ID utilisateur particulier. Entrez ensuite l'ID en question.

8. Cliquez sur **Apply (Appliquer)** pour enregistrer l'exportation.
9. Assurez-vous que le chemin d'accès, l'hôte et les droits d'accès corrects pour l'exportation créée figurent bien dans le panneau **Configure Exports (Configuration d'exportations)**.

▼ Pour modifier des exportations

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX) > Configure NFS (Configuration de NFS) > Configure Exports (Configuration d'exportations)**.
2. Sélectionnez l'exportation à modifier, puis cliquez sur **Edit (Modifier)**.
3. Pour modifier les droits d'accès, cliquez sur **Read/Write (Lecture/Écriture)**, **Read/Only (Lecture seule)** ou **No Access (Aucun accès)**.
La section **Hosts (Hôtes)** est en lecture seule.
4. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.
5. Assurez-vous que le chemin d'accès, l'hôte et les droits d'accès corrects pour l'exportation modifiée figurent bien dans le panneau **Configure Exports (Configuration d'exportations)**.

Suppression d'exportations

Pour supprimer une exportation NFS, cliquez sur l'exportation dans le panneau **Configure Exports (Configuration d'exportations)**, puis cliquez sur le bouton **Trash (Corbeille)**.

Options système

Ce chapitre fournit des instructions concernant l'activation des options que vous pouvez acquérir pour les systèmes Sun StorEdge 5310 NAS Appliance. Il traite en plus des options suivantes :

- Sun StorEdge File Replicator, qui permet de dupliquer les données d'un volume sur un volume mis en miroir se trouvant sur Sun StorEdge 5310 NAS Appliance différent (généralement utilisé dans le cas de systèmes dédiés aux transactions) ;
- Compliance Archiving Software, grâce auquel vous configurez les volumes de sorte qu'ils respectent des directives d'archivage en conformité concernant la conservation et la protection des données.

Les sujets traités dans ce chapitre sont les suivants :

- « [Activation des options système](#) », page 133
- « [Sun StorEdge File Replicator](#) », page 135
- « [Compliance Archiving Software](#) », page 148

Activation des options système

Pour activer les options système, entrez une clé d'activation dans le panneau **Activate Options** (Activation des options). Si vous avez acquis une option, renseignez-vous auprès du représentant du service clientèle de Sun Microsystems au sujet de la clé d'activation.

▼ Pour activer une option

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Activate Options (Activation des options)** et cliquez sur **Add (Ajouter)** pour ajouter la licence.
2. Dans la boîte de dialogue **Add License (Ajout de la licence)**, saisissez le nom du module fourni par Sun (**Sun StorEdge File Replicator**, par exemple).
3. Indiquez la date d'origine fournie par Sun au format **AAAAMMJJ**.
Il s'agit de la date à laquelle la licence devient active, à partir de 00h00. La date 00000000 implique que la licence est active immédiatement.
4. Indiquez la date d'expiration fournie par Sun au format **AAAAMMJJ**.
Il s'agit de la date à laquelle la licence expire, à partir de 23 h 59, 59 s. La date 00000000 implique que la licence n'expire pas.

Remarque – Quand une licence de conformité arrive à échéance ou est supprimée, le système maintient les règles de mise en conformité, mais aucun nouveau volume de conformité ne peut être créé. Pour plus d'informations sur le logiciel Compliance Archiving Software, reportez-vous à la rubrique « [Compliance Archiving Software](#) », page 148.

5. Indiquez le numéro de série fourni par Sun.
6. Cliquez sur **Apply (Appliquer)** pour activer cette option.
En ce qui concerne Sun StorEdge File Replicator, vous devez effectuer des étapes supplémentaires sur le serveur mis en miroir. Pour obtenir des instructions à ce sujet, reportez-vous à la section « [Pour activer Sun StorEdge File Replicator sur le serveur distant](#) », page 139.
7. Si vous n'avez jamais réglé la date et l'heure, saisissez l'heure, la date et le fuseau horaire appropriés.
Vous définissez ainsi l'heure système et l'horloge sécurisée. Le logiciel de gestion des licences et le logiciel Compliance Archiving Software utilisent l'horloge sécurisée pour toutes les opérations d'ordre temporel.

Remarque – L'horloge sécurisée ne peut être définie qu'une seule fois. Soyez précis lorsque vous la réglez.

8. Validez la justesse des nouvelles date et heure.
Si les nouvelles date et heure sont correctes, cliquez sur **Yes (Oui)**. Dans le cas contraire, cliquez sur **No (Non)** et réglez correctement la date et l'heure.

Sun StorEdge File Replicator

Le logiciel Sun StorEdge File Replicator vous permet de conserver des doubles exacts de vos données sur deux serveurs.

Sun StorEdge 5310 NAS Appliance Mise en miroir

La mise en miroir permet de dupliquer certains volumes de fichiers d'un système Sun StorEdge NAS sur un autre système de même type. Le serveur source est appelé « serveur actif » et le serveur cible, « serveur miroir ».

En cas de panne du serveur actif, vous pouvez séparer le miroir sur le serveur miroir, puis promouvoir le volume de fichiers sur le serveur miroir en le rendant disponible aux utilisateurs.

La méthode de mise en miroir utilisée correspond à un miroir transactionnel asynchrone. La mise en miroir fonctionne grâce à un grand tampon miroir permettant de mettre les transactions du système de fichiers dans une file d'attente pour un éventuel transfert vers le système miroir. En vérité, il existe un léger décalage entre les deux serveurs. Le miroir étant transactionnel, l'intégrité du système de fichiers miroir est garantie, même dans les cas d'interruptions de réseau ou de pannes système.

Préparation de la mise en miroir

Avant de commencer, assurez-vous que les conditions suivantes sont remplies :

- Deux serveurs Sun StorEdge NAS sont requis pour la mise en miroir. Vous pouvez utiliser n'importe quel modèle de serveur et même des modèles différents.
- Le serveur miroir doit disposer d'un espace de stockage supérieur ou égal à la taille des volumes de fichiers à mettre en miroir.
- Une connexion réseau disponible en continu et fiable et dotée d'une capacité suffisante doit exister entre les serveurs actif et miroir. Le type d'interface assurant la connexion entre ces deux serveurs peut correspondre à une connexion Ethernet de 100 mégabits ou de 1 000 mégabits. La connexion entre les serveurs peut être établie par le biais d'un commutateur ou d'un routeur. Si vous connectez les serveurs à un routeur, définissez le paramètre de routage statique de sorte que les données mises en miroir soient dirigées vers la route privée. Si vous connectez les serveurs à un commutateur, créez un LAN virtuel (VLAN) pour chaque serveur afin de les isoler du trafic réseau.

- La même version de système d'exploitation doit être installée sur les deux serveurs.
- Les volumes de fichiers actifs à mettre en miroir doivent disposer d'une capacité minimale d'un giga-octet.

Remarque – Une fois que le volume de fichiers est mis en miroir, il est impossible de renommer le volume de fichiers d'origine.

Conditions requises et limitations de File Replicator dans une configuration en cluster

La liste suivante répertorie les conditions requises et les limitations relatives à la mise en miroir avec cluster Sun StorEdge 5310 :

- La licence Sun StorEdge File Replicator doit être activée pour les deux serveurs dans la configuration en cluster.
- Les miroirs doivent être définis vers et depuis le serveur H1 uniquement. (Ne créez pas de miroir du serveur H1 vers le serveur H2 d'un même cluster.)
- Pour effectuer des opérations de gestion de miroirs (création, changement de rôle, promotion et séparation), les deux serveurs du cluster doivent présenter l'état NORMAL.
- Lorsque le cluster est en mode de basculement (autrement dit, l'un des serveurs présente l'état ALONE et l'autre, l'état QUIET) ou tout autre état endommagé, n'effectuez *pas* d'opérations de gestion de miroirs. Vous devez d'abord rétablir l'état NORMAL du cluster avant de procéder à une quelconque opération de gestion.
- Les miroirs existants continuent de fonctionner même en cas de basculement de la configuration en cluster. De même, ils continuent de fonctionner lorsque le cluster est restauré suite un basculement.

Configuration des systèmes actif et miroir

Lors du paramétrage des systèmes, indiquez les rôles des ports reliant les serveurs mis en miroir entre eux (voir la section « [Pour configurer les ports réseau dédiés](#) », page 137). Configurez ensuite la mise en miroir sur les systèmes actif et miroir à partir de l'interface de Web Administrator (voir la section « [Configuration des volumes de fichiers mis en miroir](#) », page 138). Configurez chaque système séparément.

▼ Pour configurer les ports réseau dédiés

1. Dans le volet de navigation du serveur actif, sélectionnez **Network Configuration (Configuration réseau) > Configure TCP/IP (Configuration TCP/IP) > Configure Network Adapters (Configuration des adaptateurs réseau)**.

2. Le cas échéant, assignez les adresses IP et le rôle **Primary (Principal)** aux ports connectés à un réseau local ou à un sous-réseau.

Les ports des systèmes actif et miroir peuvent se trouver sur des sous-réseaux locaux distincts. Pour plus d'informations sur la configuration TCP/IP, reportez-vous à la section « [Configuration des ports réseau](#) », page 21.

3. Assignez l'adresse IP du port utilisé pour la connexion de mise en miroir entre les systèmes actif et miroir.

Remarque – N'utilisez pas le sous-réseau contenant l'interface principale pour la mise en miroir.

Si vous avez créé un réseau isolé pour transporter le trafic du miroir, vous devez utiliser des adresses figurant dans la plage réservée à l'utilisation privée, comme 192.1xx.x.x. Par exemple, associez l'interface de liaison miroir active du système à l'adresse 192.1xx.1.1, et celle du système miroir à l'adresse 192.1xx.1.2.

4. Dans le champ, **Role (Rôle) du port utilisé pour la connexion entre les serveurs actif et miroir**, sélectionnez **Mirror (Miroir)**.
5. Si les interfaces miroir des systèmes actif et miroir ne sont pas connectées au même sous-réseau, configurez une route statique entre eux à l'aide de l'interface de ligne de commande.

Cette opération permet aux serveurs de communiquer entre eux sur des réseaux non directement connectés à leurs interfaces locales. Pour plus d'informations sur cette opération, reportez-vous à la section « [Gestion des routes](#) », page 223.

6. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications.

Configuration des volumes de fichiers mis en miroir

La mise en miroir s'effectue volume par volume. Vous pouvez appliquer la mise en miroir à une partie ou à la totalité des volumes.

Remarque – Seuls les volumes de fichiers dont la taille est supérieure ou égale à 1 giga-octet peuvent être mis en miroir. Une fois le volume de fichiers mis en miroir, il est impossible de renommer le volume d'origine tant que la connexion de mise en miroir est établie.

Lors de la synchronisation initiale de la mise en miroir, aucune opération d'E/S n'est possible sur le volume de fichiers mis en miroir à partir du serveur actif.

Tampon miroir

Le tampon miroir enregistre les transactions d'écriture du système de fichiers lors de leur transfert vers le serveur miroir. L'espace disponible sur le serveur actif pour le volume de fichiers est réduit de l'espace alloué au tampon miroir.

La taille du tampon miroir dépend de nombreux facteurs, mais doit être d'au moins 100 méga-octets. Elle ne doit jamais excéder la moitié de l'espace disponible restant sur un volume de fichiers donné.

Dans une situation normale, il est recommandé de créer un tampon miroir représentant environ 10 % de la taille du volume de fichiers à mettre en miroir. La taille choisie doit dépendre de la quantité d'informations en cours d'écriture sur le volume de fichiers et non de la taille de ce dernier. En règle générale, la taille du tampon miroir est directement proportionnelle à la fréquence d'écriture sur le volume de fichiers et inversement proportionnelle à la vitesse de la connexion réseau établie entre les deux serveurs.

Si une quantité considérable de données est écrite sur le volume de fichiers et que la connexion réseau établie entre les deux serveurs miroirs est lente, il est recommandé de créer un tampon miroir représentant de 25 à 30 % de la taille du volume de fichiers mis en miroir.

La taille du tampon miroir ne peut pas être augmentée dynamiquement. Pour augmenter la taille du tampon miroir, vous devez séparer le miroir existant et recréer un miroir de la bonne taille.

▼ Pour activer Sun StorEdge File Replicator sur le serveur distant

Une fois que vous avez activé l'option Sun StorEdge File Replicator (voir la section « [Activation des options système](#) », page 133), vous devez l'activer sur le serveur distant contenant les volumes de fichiers à mettre en miroir.

1. **Connectez-vous à Web Administrator sur le serveur contenant les volumes de fichiers à mettre en miroir.**
2. **Dans la boîte de dialogue Add License (Ajout de la licence), saisissez le nom du module fourni par Sun (StorEdge File Replicator).**
3. **Indiquez la date d'origine fournie par Sun au format AAAAMMJJ.**
Il s'agit de la date à laquelle la licence devient active, à partir de 00h00. La date 00000000 implique que la licence est active immédiatement.
4. **Indiquez la date d'expiration fournie par Sun au format AAAAMMJJ.**
Il s'agit de la date à laquelle la licence expire, à partir de 23 h 59, 59 s. La date 00000000 implique que la licence n'expire pas.
5. **Indiquez le numéro de série fourni par Sun.**
6. **Cliquez sur Apply (Appliquer) pour activer Sun StorEdge File Replicator.**

▼ Pour ajouter un volume de fichiers

1. **Dans le volet de navigation, sélectionnez File Replicator (Duplicateur de fichier) > Manage Mirrors (Gestion des miroirs).**
2. **Cliquez sur Add (Ajouter).**
3. **Sélectionnez le volume de fichiers à mettre en miroir dans le menu déroulant Volume.**
Le volume de fichiers à mettre en miroir doit disposer d'une capacité supérieure ou égale à 1 giga-octet.
4. **Entrez un nom distinct pour le serveur miroir dans le champ Mirror Host (Hôte miroir).**
5. **Indiquez l'adresse IP du système miroir.**
Il doit s'agir de l'adresse IP choisie pour la carte d'interface réseau (NIC) de mise en miroir du système miroir.
6. **Indiquez l'adresse IP secondaire (facultatif).**
En cas d'indisponibilité de la première adresse IP, le serveur utilise l'adresse IP secondaire pour conserver le miroir.

7. **Entrez le mot de passe de l'administrateur dans le champ Password (Mot de passe), si cela s'avère nécessaire pour accéder au serveur miroir.**

Si vous n'en possédez pas, laissez ce champ vide. Il est vivement recommandé d'utiliser un mot de passe pour protéger vos serveurs.

8. **Indiquez la taille (en méga-octets) du tampon miroir.**

L'espace attribué au tampon miroir est déduit de l'espace disponible alloué au volume de fichiers sur le serveur actif.

9. **Veillez à ce qu'aucune opération d'E/S n'ait lieu sur le volume de fichiers source du serveur actif lors de la création du miroir. Cliquez ensuite sur Apply pour créer le miroir.**

La création du miroir est lancée. Lorsque le miroir atteint l'état **In Sync (Synchronisation)** dans le panneau **Manage Mirrors (Gestion des miroirs)**, le volume de fichiers en miroir est monté en lecture seule. Les opérations d'E/S peuvent reprendre dès que le miroir présente l'état In Sync (Synchronisation).

Vous pouvez modifier l'adresse IP secondaire ou le mot de passe de l'administrateur du serveur miroir d'un miroir existant.

▼ Pour modifier un miroir

1. **Dans le volet de navigation, sélectionnez File Replicator > Manage Mirrors (Gestion des miroirs).**

2. **Sélectionnez le miroir à modifier à partir du tableau.**

3. **Cliquez sur Edit (Modifier).**

Les champs du nom du volume de fichiers et de l'hôte miroir sont en lecture seule.

4. **Modifiez l'adresse IP à utiliser pour la connexion miroir, puis l'adresse IP secondaire dans le champ suivant.**

5. **Si nécessaire, entrez le nouveau mot de passe de l'administrateur pour accéder au serveur hôte miroir.**

Si vous n'en possédez pas, laissez le champ Password (Mot de passe) vide.

6. **Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.**

▼ Pour corriger un miroir fissuré

Si un miroir se fissure, (notamment lorsque la connexion entre deux serveurs est interrompue ou que la taille du tampon miroir est trop limitée pour prendre en charge les nombreuses écritures effectuées sur le volume principal), effectuez les opérations suivantes :

1. **Établissez une connexion réseau plus rapide entre les deux serveurs.**
2. **Arrêtez toutes les opérations d'E/S du système de fichiers principal jusqu'à ce que le miroir présente de nouveau l'état In Sync.**
3. **Après avoir séparé et promu le volume nbd, montez le système de fichiers cible sur le serveur miroir en lecture seule à partir du client CIFS ou NFS.**

Le système de fichiers peut être utilisé pour les opérations de sauvegarde ou toute activité en lecture seule.

Vous pouvez également combiner l'utilisation de points de contrôle avec la fonction de mise en miroir. Lorsqu'un point de contrôle est créé sur le serveur actif, il est également mis en miroir sur le serveur miroir. Il peut être utilisé pour les sauvegardes planifiées ou pour donner aux autres utilisateurs et applications un accès en lecture seule aux points de contrôle.

Définition des seuils d'avertissement

Dans le panneau **File Replicator > Set Threshold Alert (Définition du seuil d'alerte)**, vous pouvez définir le seuil d'alerte de tous les volumes de fichiers mis en miroir. Le seuil d'alerte correspond au pourcentage d'utilisation du tampon miroir à partir duquel un avertissement est envoyé aux destinataires concernés.

Le tampon miroir enregistre les transactions d'écriture du système de fichiers lors de leur transfert vers le serveur miroir. Une augmentation de l'activité d'écriture vers le serveur actif ou vers une liaison réseau endommagée peut entraîner la migration des transactions d'écriture vers le serveur miroir pour une « sauvegarde » dans le tampon miroir. Si, à la suite de cette migration, la capacité du tampon miroir est dépassée, le miroir est désactivé et toute transaction entre le serveur actif et le serveur miroir est interrompue jusqu'à ce que le miroir soit rétabli. Une fois la communication restaurée, le système démarre automatiquement le processus de resynchronisation jusqu'à ce que le volume de fichiers mis en miroir soit de nouveau synchronisé.

Pour empêcher cette situation, le système envoie automatiquement des avertissements à l'aide de notifications par e-mail, du fichier journal système, de dérouterments SNMP et de l'écran LCD lorsque certains seuils de remplissage du tampon (sous forme de pourcentages) sont atteints.

▼ Pour définir le seuil d'alerte

1. **Dans le volet de navigation, sélectionnez File Replicator > Set Threshold Alert (Définition du seuil d'alerte).**
2. **Sélectionnez Mirroring Buffer Threshold 1 (Seuil 3 du tampon de mise en miroir).**
Il s'agit du pourcentage d'utilisation du tampon miroir qui déclenche la première alerte. La valeur par défaut est 70 %. Cela signifie qu'une alerte est automatiquement émise lorsque le tampon miroir a atteint 70 % de sa capacité de remplissage.
3. **Sélectionnez Mirroring Buffer Threshold 2 (Seuil 3 du tampon de mise en miroir).**
Il s'agit du pourcentage d'utilisation du tampon miroir qui déclenche la seconde alerte. La valeur par défaut est 80 %.
4. **Sélectionnez Mirroring Buffer Threshold 3 (Seuil 3 du tampon de mise en miroir).**
Il s'agit du pourcentage d'utilisation du tampon miroir qui déclenche la troisième alerte. La valeur par défaut est 90 %.
5. **Sélectionnez l'option Alert Reset Interval (Hours) (Intervalle de réinitialisation de l'alerte (en heures)).**
Il s'agit du délai d'attente du système avant d'émettre une nouvelle alerte si la condition se reproduit pendant ce laps de temps.

Par exemple, si vous définissez le **seuil 1 du tampon de mise en miroir** sur 10 pour cent et l'**intervalle de réinitialisation de l'alerte** sur deux heures, la première alerte est émise lorsque le tampon miroir est rempli à 10 pour cent. Le système ne va pas émettre à nouveau l'alerte correspondant au seuil 1 dans les deux heures qui suivent. Si, au bout de deux heures, l'utilisation du tampon miroir est toujours au-delà du seuil de 10 pour cent, mais n'atteint pas les seuils 2 ou 3, l'alerte de seuil 1 est à nouveau émise.

La valeur par défaut pour ce champ est 24 heures.
6. **Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.**

Interruption de la connexion entre les serveurs miroir

Si vous souhaitez promouvoir un volume de fichiers sur le serveur miroir (dans le cas où le volume de fichiers sur le serveur actif n'est pas disponible), vous devez d'abord interrompre la connexion miroir. Il est recommandé d'interrompre la connexion sur le serveur actif plutôt que sur le serveur miroir, comme décrit dans la procédure ci-après. Cependant, si le serveur actif est hors service et que vous ne pouvez pas y accéder pour désactiver la connexion, vous pouvez le faire à partir du serveur miroir.

▼ Pour interrompre une connexion miroir

1. Dans le volet de navigation du serveur actif, sélectionnez **File Replicator > Manage Mirrors (Gestion des miroirs)**.

2. Sélectionnez le miroir dans le tableau et cliquez sur **Break (Séparation)**.

Vous êtes invité à confirmer la fin de la connexion miroir. Une fois la connexion miroir désactivée, elle disparaît du tableau de mise en miroir. Pour promouvoir le volume de fichiers, vous devez accéder au panneau **Manage Mirrors (Gestion des miroirs)** sur le serveur miroir. Pour plus d'informations, reportez-vous à la section « [Promotion d'un volume de fichiers en miroir](#) », page 143.

Promotion d'un volume de fichiers en miroir

En cas de panne du serveur actif, le serveur miroir assure une haute disponibilité pour les volumes de fichiers mis en miroir. Vous devez **promouvoir** le volume de fichiers en miroir pour le rendre accessible aux utilisateurs réseau. Pour cela, il vous faut interrompre la connexion miroir, puis promouvoir le volume de fichiers mis en miroir et ensuite configurer ses droits d'accès. Une fois la connexion miroir désactivée et le volume de fichiers en miroir promu, les volumes de fichiers en miroir et d'origine sont entièrement indépendants.



Attention – Le miroir d'un volume doté de la fonction de conformité stricte ne peut pas faire l'objet d'une promotion.

Si vous avez besoin d'un accès temporaire à un volume miroir de ce type, vous pouvez l'exporter en tant que système de fichiers en lecture seule sans le promouvoir.

Vous devez d'abord désactiver la connexion miroir pour promouvoir un volume de fichiers sur le serveur miroir. Pour obtenir des instructions à ce sujet, reportez-vous à la section « [Interruption de la connexion entre les serveurs miroir](#) », page 142.

▼ Pour promouvoir un volume de fichiers sur le serveur miroir

1. Dans le volet de navigation du serveur miroir, sélectionnez **File Replicator > Manage Mirrors (Gestion des miroirs)**.
2. Cliquez sur **Promote (Promouvoir)**.
3. Dans la boîte de dialogue **Promote Volume (Promouvoir le volume)**, sélectionnez le volume à promouvoir et cliquez sur **Apply (Appliquer)**.

Le processus peut prendre plusieurs minutes. Le volume de fichiers en miroir à promouvoir doit avoir atteint l'état **In Sync (Synchronisation)**. Si ce dernier n'est plus synchronisé lors de sa promotion, il va être monté en tant que volume en lecture seule. Avant d'activer l'option d'écriture pour ce volume, exécutez la commande `fsck` pour effectuer les réparations nécessaires.

Suite à la désactivation de la connexion miroir, le système effectue un contrôle du système de fichiers. Si une erreur est détectée lors de ce contrôle, le processus de promotion du volume de fichiers peut durer plus longtemps que prévu. L'intégrité des données n'est pas garantie si le miroir n'est plus synchronisé lors du processus de promotion.

Il se peut que vous deviez configurer les droits d'accès après la promotion du volume de fichiers. Les informations de partage SMB sont automatiquement transférées, mais vous devez tout de même de nouveau configurer l'accès aux volumes de fichiers NFS et les exportations NFS pour ce volume. Pour plus d'informations sur le paramétrage des exportations NFS, reportez-vous à la section « [Paramétrage d'exportations NFS](#) », page 129.

Rétablissement d'une connexion miroir

Cette procédure décrit comment rétablir une connexion miroir suite à la panne du serveur actif et la promotion du volume de fichiers sur le serveur miroir. Le volume de fichiers promu est à présent la version la plus à jour et fonctionne indépendamment du volume de fichiers obsolète situé sur le système actif. Pour rétablir la connexion miroir, vous devez remettre en miroir le volume de fichiers à jour sur le serveur actif, puis le remettre en miroir sur le serveur miroir comme au départ.

Remarque – Si le volume de fichiers mis en miroir n'a pas été promu, ne suivez pas ces instructions. Le système actif ramène automatiquement le miroir à l'état **In Sync (Synchronisation)** lorsqu'il est de nouveau en ligne.

Dans les exemples ci-dessous, *Serveur 1* correspond au serveur actif et *Serveur 2* au serveur miroir.

▼ Pour rétablir une connexion miroir

1. Assurez-vous que le miroir sur le serveur 1 est interrompu.

Reportez-vous à la section « [Pour interrompre la connexion de mise en miroir sur le serveur actif](#) », page 145.

2. Supprimez le volume de fichiers obsolète sur le serveur 1.

Reportez-vous à la section « [Pour supprimer le volume de fichiers obsolète du serveur 1](#) », page 145.

3. Mettez en miroir le volume de fichiers actualisé du serveur 2 sur le serveur 1 (voir la section « [Pour mettre en miroir le volume à jour du serveur 2 sur le serveur 1](#) », page 146).

4. Changez le rôle sur le serveur 2.

Reportez-vous à la section « [Modification des rôles de volumes](#) », page 147.

À la fin de cette procédure, le serveur 1 devrait à nouveau être actif et le serveur 2 devrait être la cible de mise en miroir.

▼ Pour interrompre la connexion de mise en miroir sur le serveur actif

1. Ouvrez une fenêtre de navigateur Web sur le serveur 1.

2. Dans le volet de navigation, sélectionnez File Replicator > Manage Mirrors (Gestion des miroirs).

3. Sélectionnez la connexion miroir à interrompre.

4. Cliquez sur Break (Séparer).

▼ Pour supprimer le volume de fichiers obsolète du serveur 1

1. Dans le volet de navigation du serveur 1, sélectionnez File Volume Operations (Opérations sur un volume de fichiers) > Delete File Volumes (Suppression de volumes de fichiers).

2. Sélectionnez le volume de fichiers qui a été mis en miroir.

Comme le volume de fichiers du serveur miroir a été promu et qu'il correspond à la version la plus récente, le volume de fichiers du serveur actif est obsolète et doit être supprimé.



Attention – Veillez à supprimer le volume de fichiers source obsolète du **serveur actif** avant d'effectuer l'étape suivante. Par ailleurs, assurez-vous que le volume de fichiers à jour sur le serveur miroir est vérifié et promu en premier.

3. Cliquez sur Apply (Appliquer) pour supprimer le volume de fichiers obsolète.

▼ Pour mettre en miroir le volume à jour du serveur 2 sur le serveur 1

1. Ouvrez une fenêtre de navigateur Web sur le serveur 2.
2. Dans le volet de navigation, sélectionnez **File Replicator > Manage Mirrors** (Gestion des miroirs).
3. Cliquez sur **Add (Ajouter)**.
4. Sélectionnez le volume de fichiers à mettre en miroir dans le menu déroulant **Volume**.
5. Indiquez le nom de la mise en miroir sur le serveur 1 dans le champ **Mirror Host** (Hôte miroir).
6. Saisissez l'adresse IP du port du serveur 1 utilisé pour la connexion de mise en miroir.
7. Indiquez l'Adresse IP secondaire.
8. Entrez le mot de passe de l'administrateur dans le champ **Password (Mot de passe)** si cela s'avère nécessaire pour accéder au serveur 1.
Si vous n'en possédez pas, laissez ce champ vide.
9. Indiquez la taille du tampon miroir.
Pour plus d'informations sur le tampon miroir, reportez-vous à la section « [Sun StorEdge 5310 NAS Appliance Mise en miroir](#) », page 135.
Vérifiez qu'aucune opération d'E/S n'a lieu sur le volume de fichiers source du *Serveur 2* lors de la synchronisation du miroir.
10. Cliquez sur **Apply (Appliquer)** pour créer le miroir.
La création du miroir est lancée. Lorsque le miroir atteint l'état **In Sync (Synchronisation)**, une réplique exacte du volume de fichiers existe sur les serveurs 1 et 2.
11. Dans le panneau **Manage Mirrors (Gestion des miroirs)** du serveur 1, sélectionnez le volume de fichiers promu, puis cliquez sur **Change Roles (Modifier les rôles)**.
Pour plus d'informations, reportez-vous à la section « [Modification des rôles de volumes](#) », page 147.
La connexion miroir d'origine est désormais rétablie.

Modification des rôles de volumes

Un administrateur peut échanger le rôle des volumes actif et miroir. La modification des rôles de volumes permet au volume actif de fonctionner en tant que volume miroir et inversement. Cependant, la configuration d'origine de chaque volume reste inchangée. La modification des rôles n'est pas une fonction de reprise sur sinistre.

Remarque – Les volumes doivent être parfaitement synchronisés pour que la modification des rôles soit possible.

Le changement des rôles peut s'effectuer dans le panneau Manage Mirrors (Gestion des miroirs) à partir du serveur actif ou du serveur miroir.

▼ Pour changer les rôles

1. Dans le volet de navigation, cliquez sur **File Replicator > Manage Mirrors (Gestion des miroirs)**.
2. Sélectionnez un volume dans la colonne **Volume**.
3. Cliquez sur **Change Roles (Changer les rôles)**.
4. Cliquez sur **Yes (Oui)** pour confirmer.

Compliance Archiving Software

Le logiciel Compliance Archiving Software permet à une société de s'adapter aux pratiques commerciales et aux règlements de conformité qui s'appliquent au stockage et à la protection des informations. Ces règlements et cadres législatifs s'articulent autour de la réglementation SEC (Security and Exchange) 17 CFR § 240.17a-4 (17a-4), de la loi Sarbanes Oxley, BASEL II et de nombreuses directives à la protection et à la confidentialité des données.

Le logiciel Compliance Archiving Software a été mis au point en collaboration avec des experts de la conformité de la gestion des informations et de la gestion de contenu d'entreprise. Il permet de répondre aux principales exigences relatives au stockage et à la protection de supports de données électroniques. Compliance Archiving Software utilise des fichiers WORM (Écriture unique, lectures multiples) conformément aux règles de mise en conformité.

Activation de l'archivage en conformité

Le logiciel Compliance Archiving Software est décliné en deux versions : une forme assouplie (appelée « application consultative ») et une forme stricte (dite « application obligatoire »).

Lorsque le logiciel Compliance Archiving Software est activé (voir « [Activation des options système](#) », page 133), vous avez la possibilité, quand vous créez un volume, d'activer la fonction de mise en conformité avec application consultative ou obligatoire.

Remarque – Les configurations système de passerelle Sun StorEdge 5310 Gateway System prennent en charge la mise en conformité avec application consultative exclusivement.

Remarque – Pour que le logiciel Compliance Archiving Software fonctionne correctement, vous devez avoir au préalable procédé à une configuration physique adaptée du matériel du système Sun StorEdge 5310 NAS Appliance ou cluster Sun StorEdge 5310. En particulier, les baies de contrôleur des unités d'extension de Sun StorEdge 5300 RAID ne doivent être connectées à aucun périphérique ou réseau en dehors d'une connexion Fibre Channel privée à la tête NAS ou aux éventuels boîtiers d'extension des unités d'extension de Sun StorEdge 5300.

Remarque – Pour garantir un respect optimal de vos règles de conservation des données, vous devez prendre toutes les mesures nécessaires pour assurer la sécurité physique de votre système Sun StorEdge 5310 NAS Appliance ou cluster Sun StorEdge 5310. Le stockage de données géré par logiciel ne remplacera jamais les précautions physiques prises pour contrôler l'accès au matériel du système.



Attention – Vous ne devez pas autoriser un archivage en conformité sur des volumes utilisés par des applications (et des utilisateurs) qui n'appliquent pas les règles de conservation de données dictées par le logiciel Compliance Archiving Software.

Le logiciel Compliance Archiving Software permet aux administrateurs d'activer l'archivage en conformité sur tous les nouveaux volumes qu'ils créent à condition qu'ils le précisent au moment même de cette création. Suivez les instructions de la section « [Pour créer un volume de fichiers ou un segment par l'intermédiaire du panneau Create File Volumes \(Création de volumes de fichiers\)](#) », page 49 pour créer un volume en conformité.

Conformité avec application obligatoire

La mise en conformité avec application obligatoire respecte les directives relatives à la protection, à la conservation et à la confidentialité des données :

- Vous ne pouvez pas détruire les volumes en conformité dont l'option d'application obligatoire est activée.
- Vous ne pouvez pas détruire les fichiers WORM tant que la période de conservation n'a pas expiré.
- Vous pouvez augmenter ou réduire la durée de conservation d'un volume, mais vous pouvez seulement étendre la période de conservation d'un fichier WORM.
- Vous ne pouvez pas restaurer un fichier WORM à partir d'un point de contrôle.



Attention – Une fois que vous avez activé sur un volume l'archivage en conformité avec application obligatoire, il est impossible de supprimer et de renommer ce volume, de désactiver l'archivage en conformité ou de revenir au niveau de l'application consultative.

Conformité avec application consultative

Contrairement à la fonction de conformité avec application obligatoire, l'option de conformité avec application consultative se caractérise par les points suivants :

- Un administrateur autorisé peut détruire des fichiers WORM et des volumes en conformité (à l'aide de la fonction de suppression contrôlée).

Remarque – Avant la suppression d'un volume, vous devez récupérer les journaux d'audit se trouvant sur le volume en question en les copiant sur un autre système de fichiers. À défaut, ces journaux seront définitivement perdus.

- Un administrateur autorisé peut augmenter et diminuer la durée de conservation.
- Un administrateur autorisé peut restaurer des fichiers WORM à partir d'un point de contrôle (à l'aide de la fonction de suppression contrôlée).
- La période de conservation par défaut, définie en usine sur zéro jour, est modifiable.

Remarque – La diminution de la durée de conservation et la suppression des fichiers conservés avant l'échéance de la période de conservation définie doivent être effectuées par l'utilisateur racine (root) et ce, à partir d'un hôte de confiance. Reportez-vous à la section « [Gestion des hôtes de confiance](#) », page 244.

Quand un volume doté de la fonction de conformité avec application consultative est mis à niveau vers l'option d'application obligatoire, la période de conservation par défaut de ce volume devient permanente. Ce paramètre est modifiable via le panneau Edit Properties (Modifier les propriétés).

Remarque – La mise à niveau d'un volume dont la fonction de conformité avec application consultative est activée n'est pas prise en charge par les configurations de passerelle.

Contrôle de mise en conformité

Le contrôle de mise en conformité dispose d'un journal au format texte consignnant les tentatives de modification ou de suppression des données (avec ou sans titre d'autorité approprié). Il est activé par le biais de l'API DRAS (Data Retention Audit Service), qui comprend les fonctions suivantes :

- Suivi des modifications et des tentatives de modifications portant sur les fichiers conservés
- Mécanisme de consignation permettant de stocker les événements contrôlables
- Protection et conservation du journal d'audit pendant toute la durée de vie du système
- Informations du journal d'audit disponibles dans un format immédiatement lisible et accès sécurisé au journal d'audit par le biais de protocoles d'accès système standard

Les événements contrôlables sont les suivants :

- Conservation d'un fichier
- Extension de la période de conservation d'un fichier conservé
- Requêtes de déconnexion (suppression) d'un fichier conservé
- Requêtes d'écriture sur un fichier conservé
- Requêtes de changement de nom d'un fichier conservé
- Requêtes de suppression d'un répertoire
- Requêtes de changement de nom d'un répertoire

Limites de taille pour les fichiers

Les volumes en conformité disposent d'une quantité d'espace disponible réservée à la consignation des opérations contrôlables sur le volume. Quand l'espace disponible restant sur un volume en conformité passe sous la limite, les opérations contrôlables ne sont pas exécutées. Un message est généré, indiquant que le volume ne dispose pas de suffisamment d'espace pour exécuter à la fois l'opération et le contrôle. Un e-mail d'avertissement vous est envoyé, sous réserve que la fonction de messagerie ait été configurée sur le système.

Journal d'audit

Le journal d'audit concernant chaque volume dont la fonction de conformité est activée réside dans le répertoire racine de ce volume.

Les enregistrements du journal d'audit sont au format texte et sont accessibles par le biais de protocoles réseau tels que NFS et CIFS. Le répertoire `.audit$` doit faire partie du chemin de partage du contenu pour être visible par les clients exécutant Windows 2000 ou XP. Pour plus d'informations sur la création de partages, reportez-vous à la section « [Partages](#) », page 113.

Le format du journal d'audit est indiqué dans le [TABLEAU 9-1](#).

TABLEAU 9-1 Format du journal d'audit

Champ	Longueur	Description
Version	7	Numéro de version du service DRAS (Data Retention Audit Service)
Serial Number	11	Numéro de séquence unique
Length	5	Longueur de l'enregistrement dans le journal d'audit
Horodateur	21	Date et heure auxquelles l'événement s'est produit
TID	11	Identificateur du thread à partir duquel l'événement a été exécuté
Volume ID	11	ID du volume contrôlé
Protocol	9	Protocole réseau par lequel l'opération a été demandée
Inode	11	Numéro inode de système de fichiers pour le fichier
Client IP Address	16	Adresse IP du client à partir duquel l'opération a été demandée
Server IP Address	16	Adresse IP par laquelle la requête du client a été reçue
UID	11	Référence de l'utilisateur
GID	11	Référence du groupe principal
Operation	8	Événement soumis au contrôle
Status	Variable	Résultat de l'opération
Domain	Variable	Domaine Windows auquel appartient l'utilisateur (le cas échéant)
File/Directory Name	Variable	Nom du fichier ou du répertoire auquel s'applique l'opération (si disponible)
Path/Extra Data	Variable	Informations supplémentaires générées lors du contrôle (le cas échéant)

Fonctions d'archivage en conformité supplémentaires

Pour obtenir une présentation technique des fonctions et de l'interface de programmation du logiciel Compliance Archiving Software, consultez l'[Annexe C](#).
Pour modifier les paramètres d'archivage en conformité, reportez-vous à la section « [Configuration du logiciel Compliance Archiving Software](#) », page 271.

Contrôle du système

Ce chapitre décrit les fonctions de contrôle du système Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System. Le contrôle du système et les fonctions de maintenance étant étroitement liés, un grand nombre des fonctions de contrôle décrites ci-après font référence à d'autres chapitres de ce document dans lesquels sont présentées les actions nécessaires à la résolution des problèmes. En outre, les fonctions de contrôle indiquent l'état d'achèvement des activités de maintenance ou de gestion.

Ce chapitre aborde les sujets suivants :

- « [Contrôle SNMP \(Simple Network Management Protocol\)](#) », page 156
- « [Visualisation du statut du système](#) », page 157
- « [Journalisation du système](#) », page 158
- « [Audit du système](#) », page 161
- « [Statut de l'environnement](#) », page 163
- « [Informations sur l'utilisation](#) », page 167
- « [Affichage des routes réseau](#) », page 170
- « [Contrôle des composants système](#) », page 172
- « [Affichage du statut de la tâche de sauvegarde](#) », page 175

Contrôle SNMP (Simple Network Management Protocol)

Vous pouvez effectuer des contrôles SNMP en activant les communications SNMP. Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System prennent uniquement en charge le contrôle SNMP (pas la gestion SNMP).

Afin d'interpréter les blocs d'information MIB (Message Information Blocks), vous avez besoin des fichiers MIB. Ces fichiers sont installés avec l'image dans le répertoire *répertoire_initialisation/www/data/mib*. Exemple :
/cvol/nf1/www/data/mib.

Vous pouvez également télécharger les fichiers MIB à partir du site <http://sunsolve.sun.com>. Pour obtenir plus d'informations sur le mode d'utilisation de ces fichiers, reportez-vous à la documentation concernant l'application de gestion réseau.

▼ Pour paramétrer le protocole SNMP

1. Dans le volet de navigation, sélectionnez **Monitoring and Notification (Contrôle et notification) > Configurer SNMP (Configuration SNMP)**.

Configure SNMP

Enable SNMP

Server SNMP Community:

Contact Info:

System Location:

Destination IP Address	Port #	Version	Community	Enable
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>
* * *	162		Unused	<input type="checkbox"/>

Cancel Apply

2. Cochez la case **Enable SNMP (Activer SNMP)** pour activer le protocole correspondant.
3. Dans le champ **Server SNMP Community (Communauté de serveurs SNMP)**, indiquez la communauté SNMP à laquelle Sun StorEdge 5310 NAS Appliance appartient.
4. Dans le champ **Contact Info (Coordonnées)**, saisissez le nom de la personne responsable du système.
5. Dans le champ **System Location (Emplacement du système)**, indiquez l'emplacement sur le réseau.
Cet emplacement peut être physique ou logique.
6. Pour ajouter une nouvelle adresse cible, entrez les informations suivantes sur une ligne vide de la table SNMP :
 - **Destination IP Address (Adresse IP de destination)** : saisissez l'adresse TCP/IP du serveur que vous voulez désigner comme destination du déROUTement SNMP en cas d'erreur système.
 - **Port # (N° de port)** : indiquez le port auquel le système envoie les déROUTements. La valeur par défaut est le port 162.
 - **Version (Version)** : dans le menu déroulant, choisissez la version SNMP (1 ou 2) voulue.
 - **Community (Communauté)** : précisez la chaîne de communauté de la destination du déROUTement.
 - **Enable (Activation)** : cochez l'une des cases de cette colonne pour que l'adresse cible correspondante devienne une destination de déROUTement.
7. Pour supprimer une adresse cible, sélectionnez la ligne concernée et cliquez sur le bouton **Trash (Corbeille)**.
8. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

Visualisation du statut du système

Web Administrator affiche le statut de base du système lorsque vous y accédez pour la première fois. Les écrans de statut peuvent varier d'un modèle à l'autre, selon les fonctions et les caractéristiques physiques du modèle.

Les informations affichées sur cet écran peuvent vous être utiles lorsque vous contactez le support client et peuvent, dans certains cas, fournir les causes probables du dysfonctionnement.

▼ Pour visualiser le statut du système

Cliquez sur le bouton de démarrage de la barre d'outils.

L'écran présente un relevé en lecture seule des données figurant dans le [TABLEAU 10-1](#).

TABLEAU 10-1 Affichage du statut du système

Nom	Description
Name	Nom du serveur
Model	Modèle du système
Serial #	Numéro de série unique du système
Up Time	Temps écoulé depuis la dernière mise sous tension du système
CPU Load	Charge actuelle et maximale du processeur
OS Version	Version du système d'exploitation installé sur le serveur
Web Admin Version	Version de Web Administrator installée sur le système
Head Status	État du serveur H1 (Cluster uniquement) : NORMAL, QUIET, ALONE
Partner Status	État du serveur H2 (Cluster uniquement) : NORMAL, QUIET, ALONE
Features Enabled	Fonctions facultatives activées sur le système

Journalisation du système

Un journal système contient des informations de base sur tous les événements système. Il fournit des informations essentielles sur les erreurs qui se sont produites.



Attention – Vous devez activer la journalisation à distance ou créer un fichier journal sur un disque local pour que le journal ne soit pas supprimé lors de l'arrêt du système. Lors de son premier démarrage, le système crée un fichier journal temporaire dans sa mémoire volatile afin de consigner les erreurs ayant pu se produire au cours du démarrage initial.

Le panneau **Display System Log (Affichage du journal système)** répertorie la totalité des événements système, des avertissements et des erreurs, y compris la date et l'heure à laquelle ceux-ci ont eu lieu. Ce panneau affiche d'abord les événements système les plus récents. Vous pouvez utiliser la barre de défilement pour afficher des événements antérieurs.

Remarque – Les modifications apportées à la configuration de l'unité de disque, notamment la suppression ou l'insertion d'une unité de disque, peuvent nécessiter jusqu'à 30 secondes pour être prises en compte dans le journal d'événements. Si plusieurs modifications sont effectuées pendant ce laps de temps, certains événements risquent de ne pas être consignés.

Display System Log

Log Name:

Date	Time	Description
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11244 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11244 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11242 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11244 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11242 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11240 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11238 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11238 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11236 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11234 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11232 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11230 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11228 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11226 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11224 length 32768
12/20/04	18:48:08	nmir: nmdeseq: Write error on xid 11224 length 32768
12/20/04	18:48:06	nmir: nmdeseq: Write error on xid 11222 length 32768
12/20/04	18:48:06	nmir: nmdeseq: Write error on xid 11224 length 32768
12/20/04	18:48:06	nmir: nmdeseq: Write error on xid 11222 length 32768

Event Types

Emergency Alert Critical Error Warning Notice Information Debug

Refresh Print Log Save As... Silence Alarm

▼ Pour afficher le journal système









1. Dans le volet de navigation, sélectionnez **Monitoring and Notification (Contrôle et notification) > View System Events (Affichage des événements système) > Display System Log (Affichage du journal système)**.
2. **Cochez les cases des types d'événements que vous souhaitez afficher.**
Pour plus d'informations, reportez-vous à la section « [Événements système](#) », page 160.
3. Cliquez sur **Refresh (Rafraîchir)**.

Remarque – Si le journal système contient des messages d'erreur indiquant la présence de volumes de type SFS2 non attribués, contactez le support technique pour obtenir de l'aide.

Événements système

Le journal système consigne huit types d'événements système. Chaque événement est représenté par une icône, comme illustré dans le [TABLEAU 10-2](#).

TABLEAU 10-2 Icônes des événements système

	Emergency (Urgence) : indique les messages d'urgence. Ces messages ne sont pas envoyés à tous les utilisateurs. Les messages d'urgence prioritaires sont enregistrés dans un fichier distinct pour vérification.
	Alert (Alerte) : indique les messages importants qui nécessitent une attention immédiate. Ces messages sont envoyés à tous les utilisateurs.
	Critical (Critique) : indique les messages critiques non répertoriés en tant qu'erreurs (tels que les problèmes matériels). Les messages critiques et les messages possédant une priorité plus haute sont envoyés à la console système.
	Error (Erreur) : indique des messages représentant des conditions d'erreur, telles que l'échec d'écriture sur le disque.
	Warning (Avertissement) : désigne des messages concernant des conditions anormales mais néanmoins récupérables.
	Notice (Avis) : désigne des messages d'information importants. Les messages sans indication de priorité sont regroupés dans ce message de priorité.
	Information (Informations) : désigne des messages d'information. Ces messages sont utiles pour l'analyse du système.
	Debug (Débogage) : indique des messages de débogage.

Audit du système

L'audit du système permet à l'administrateur système de contrôler des événements système particuliers en stockant les enregistrements associés dans des fichiers journaux. L'audit se distingue de `syslog`. En effet, une piste de vérification du système est consignée dans des fichiers binaires situés sur le système local.

L'audit du système doit être activé par l'administrateur système avec un volume de fichiers configuré en tant que volume de stockage de pistes de vérification. Vous pouvez activer et configurer la fonction d'audit par le biais de Web Administrator, des menus de l'opérateur ou encore à l'aide des commandes de la CLI.

Configuration de l'audit

Vous devez définir le volume d'audit, lequel peut correspondre à tout volume non système. Bien que le système ne requiert pas l'utilisation exclusive de ce volume à des fins d'audit, il est déconseillé de se servir de volumes d'audit à des fins de stockage classique.

Une valeur par défaut est définie pour la taille maximale d'un fichier journal d'audit, mais l'utilisateur peut la modifier. Lorsque le journal d'audit actif atteint la taille définie (à 1 kilo-octet près), il se ferme et un nouveau fichier journal est automatiquement créé.

▼ Pour configurer l'audit du système

1. Dans le volet de navigation, sélectionnez **Monitoring and Notification (Contrôle et notification) > Enable System Auditing (Activation de l'audit du système)**.
2. Pour activer l'audit du système, cochez la case **Enable System Auditing (Activer l'audit du système)**.
3. Sélectionnez un volume destiné au stockage des journaux d'audit du système.

Il ne doit pas s'agir de volumes système. Vous devez créer des volumes dédiés à la fonction d'audit. Vous trouverez des instructions à la section « [Pour créer un volume de fichiers ou un segment par l'intermédiaire du panneau Create File Volumes \(Création de volumes de fichiers\)](#) », page 49.

4. Indiquez la taille maximale du fichier journal d'audit, celle-ci devant être comprise entre 1 et 1 024 méga-octets.

Le fichier journal verra sa taille augmenter de 0 méga-octet à la valeur maximale définie avant la création d'un nouveau fichier journal d'audit. Les fichiers journaux d'audit existants ne sont pas supprimés. Quand le volume atteint un seuil de 90 pour cent, les alertes sont envoyées mais ne sont plus consignées dans des fichiers journaux.

5. Cliquez sur **Apply (Appliquer)** pour enregistrer vos paramètres.

Fichiers journaux d'audit

Les fichiers journaux d'audit sont formatés à l'aide de valeurs d'horodatage et du nom d'hôte du système. Le fichier journal actif est formaté comme suit : `AAAAMMJJhhmmss.not_terminated.nom-hôte`.

Les date et heure sont précisées au format GMT. Si, par exemple, le fichier journal actif a démarré le 21 octobre 2005 à 13:15 GMT sur l'hôte Sun StorEdge 5310 NAS Appliance =hôte-test, le fichier s'intitule `20051021131500.not_terminated.hôte-test`.

Une fois qu'un fichier journal est fermé, son nom est converti selon le même format d'horodatage. Si l'on reprend l'exemple ci-dessus, lorsque le même fichier journal atteint sa taille maximale le 30 octobre 2005 à 19:35 GMT, son nom est converti en `20051021131500.20051030193500.hôte-test`.

Les fichiers journaux d'audit disposent d'attributs spéciaux. Outre la particularité de n'avoir aucune autorisation, ces fichiers sont marqués comme non supprimables et non modifiables, ce qui les protège des tentatives de suppression, de changement de nom ou de modification par toute entité autre que le système lui-même. Ces attributs peuvent être retirés par l'administrateur à l'aide de la commande `chattr`.

Remarque – Actuellement, il n'existe aucune prise en charge IG pour la lecture ou la suppression de journaux d'audit.

Événements audités

Seul un nombre réduit d'événements sont audités : le démarrage et l'arrêt du système, la création et la suppression de partitions de disque et de volumes.

Il n'est pas possible de configurer ces événements.

Lecture des journaux d'audit

Comme les journaux d'audit sont stockés au format binaire, ils doivent être lus à l'aide de la commande `praudit`, laquelle convertit les informations binaires contenues dans les journaux d'audit en texte lisible.

Statut de l'environnement

Vous pouvez visualiser des informations sur les ventilateurs, la température, l'alimentation électrique et la tension du système.

▼ Pour afficher le statut des ventilateurs

- Pour afficher le statut opérationnel et le nombre de tours par minute (r/min) de tous les ventilateurs installés dans l'unité principale de Sun StorEdge 5310 NAS Appliance, sélectionnez **Monitoring and Notification (Contrôle et notification) > View Environmental Status (Affichage du statut de l'environnement) > View Fan Status (Affichage du statut du ventilateur)** dans le volet de navigation.

The screenshot shows a window titled "View Fan Status" with a table of fan data and a log of system events below it.

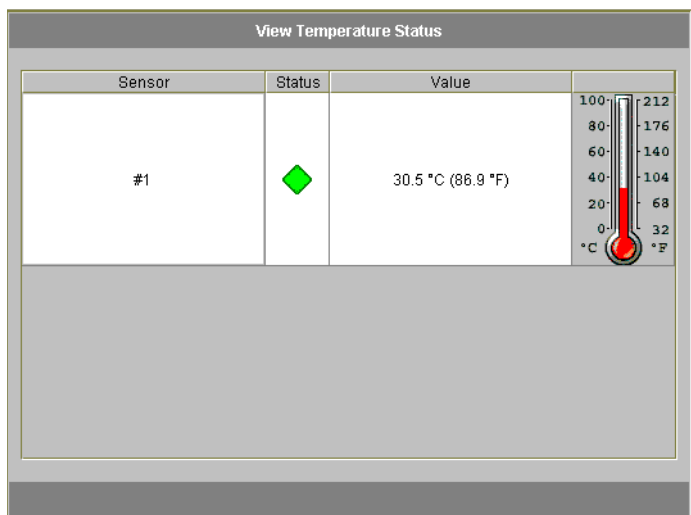
Fan	Status	RPM
CPU Fan		4920
#1		5880
#2		5664
#3		5664
#4		5880

Wednesday, May 15, 2002 11:09:25 AM PDT> Performing Post-Login Processing
Wednesday, May 15, 2002 11:09:27 AM PDT > Login begun.
Wednesday, May 15, 2002 11:09:27 AM PDT > Login accepted.
Wednesday, May 15, 2002 11:09:27 AM PDT > Warning - Passwords are disabled on this server.

La capture d'écran ci-dessus indique le statut de chaque ventilateur. Un losange de couleur verte situé dans la colonne **Status (Statut)** indique que le nombre de tours par minute du ventilateur est normal. Un losange de couleur rouge indique que le ventilateur fonctionne en surrégime. Lorsqu'un ventilateur passe en dessous de 1 800 r/min ou tombe en panne, un e-mail est envoyé aux destinataires appropriés. Pour plus d'informations sur le paramétrage de la notification par e-mail, reportez-vous à la section « [Paramétrage de la notification par e-mail](#) », page 33.

▼ Pour afficher le statut de la température

- Pour afficher le statut de la température, sélectionnez **Monitoring and Notification (Contrôle et notification) > View Environmental Status (Affichage du statut de l'environnement) > View Temperature Status (Affichage du statut de la température)** dans le volet de navigation.

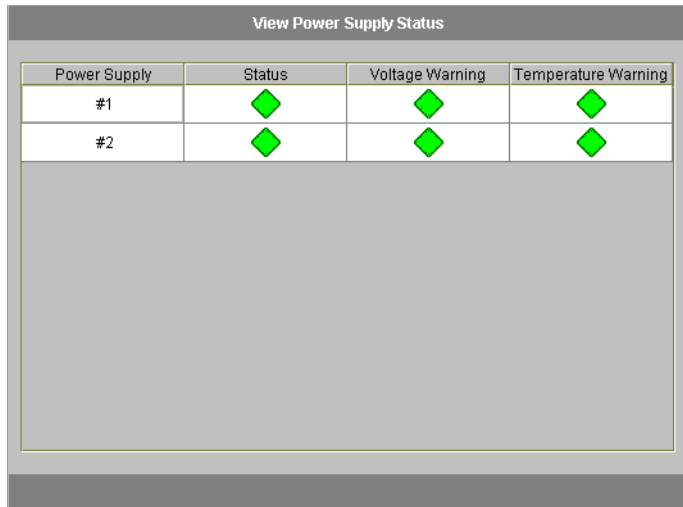


Cet écran affiche la température des sondes placées dans l'unité principale. Un losange de couleur verte situé dans la colonne **Status (Statut)** indique que l'unité fonctionne à une température normale. Un losange de couleur rouge indique que la température a dépassé la plage des valeurs acceptables. Lorsque la température dépasse 55° Celsius (131° Fahrenheit), un e-mail est envoyé aux destinataires appropriés. Pour plus d'informations sur le paramétrage de la notification par e-mail, reportez-vous à la section « [Paramétrage de la notification par e-mail](#) », page 33.

Remarque – Les seuils de température ne sont pas modifiables.

▼ Pour afficher le statut de l'alimentation

- Pour afficher le statut de l'alimentation, sélectionnez **Monitoring and Notification (Contrôle et notification) > View Environmental Status (Affichage du statut de l'environnement) > View Power Supply Status (Affichage du statut de l'alimentation)** dans le volet de navigation.



















Power Supply	Status	Voltage Warning	Temperature Warning
#1	◆	◆	◆
#2	◆	◆	◆

Trois colonnes indiquent le statut de l'alimentation. La colonne **Status (Statut)** indique si l'alimentation est normale. Les colonnes **Voltage Warning (Avertissement tension)** et **Temperature Warning (Avertissement température)** indiquent si la tension et la température sont correctes.

Si dans l'une de ces colonnes le losange affiché est de couleur verte, la tension ou la température sont correctes. S'il est rouge, alors la tension ou la température dépassent la limite acceptable. Dans ce cas, une notification par e-mail est envoyée aux destinataires appropriés. Pour plus d'informations sur la notification par e-mail, reportez-vous à la section « [Paramétrage de la notification par e-mail](#) », page 33.

▼ Pour afficher le statut de la tension

- Pour connaître la tension actuelle, sélectionnez **Monitoring and Notification (Contrôle et notification) > View Environmental Status (Affichage du statut de l'environnement) > View Voltage Regulator Status (Affichage du statut du régulateur de tension)** dans le volet de navigation.

View Voltage Regulator Status		
Voltage Regulator	Status	Current Value
Baseboard 1.2V		1.21
Baseboard 1.25V		1.27
Baseboard 1.8V		1.78
Baseboard 1.8VSB		1.78
Baseboard 2.5V		2.53
Baseboard 3.3V		3.38
Baseboard 3.3AUX		3.29
Baseboard 5.0V		4.97
Baseboard 5VSB		5.1
Baseboard 12V		12.03
Baseboard 12VRM		12.09
Baseboard -12V		-12.04
Baseboard VBAT		3.08
SCSI A Term Pwr		4.04
SCSI B Term Pwr		4.04
Processor Vccp		1.51

Consultez le [TABLEAU 10-3](#) pour obtenir des informations sur les plages de tension acceptables.

TABLEAU 10-3 Plages de tension acceptables

Valeur de la tension	Plage acceptable
Plaque 1,2 V	1,133 à 1,250 V
Plaque 1,25 V	1 074 V à 1 406 V
Plaque 1,8 V	1 700 V à 1 875 V
Plaque 1,8VSB (en veille)	1 700 V à 1 875 V
Plaque 2,5 V	2 285 V à 2 683 V
Plaque 3,3 V	3 096 V à 3 388 V
Plaque 3,3 AUX	3,147 V à 3,451 V
Plinthe 5 V	4,784 V à 5,226 V
Plaque 5 VSB (en veille)	4,781 V à 5,156 V
Plaque 12 V	11,5 V à 12,56 V

TABEAU 10-3 Plages de tension acceptables (*Suite*)

Plaque 12 VRM	11,72 V à 12,80 V
Plaque -12 V	-12,62 V à -10,97 V
Plaque VBAT	2,859 V à 3,421 V
SCSI A - Alim. Term.	4,455 V à 5,01 V
SCSI B - Alim. term.	4,455 V à 5,01 V
Processeur VCCP	1,116 V à 1,884 V

Informations sur l'utilisation

Vous pouvez visualiser des informations sur l'utilisation des volumes de fichiers, l'activité réseau, l'activité système et les ports réseau.

▼ Pour afficher les informations sur l'utilisation des volumes de fichiers

- **Pour afficher la quantité d'espace occupée et disponible pour les volumes de fichiers sur le système, sélectionnez *Monitoring and Notification (Contrôle et notification)* dans le volet de navigation. Sélectionnez ensuite *View File Volume Usage (Affichage du volume de fichiers disponible)* pour afficher l'espace libre et utilisé.**

Si l'utilisation d'un volume de fichiers dépasse 95 pour cent, un e-mail est envoyé aux destinataires concernés.

▼ Pour afficher l'activité réseau

- **Pour afficher le nombre de requêtes d'E/S par seconde de tous les clients Sun StorEdge 5310 NAS Appliance, sélectionnez *System Activity (Activité du système)* > *View Networking Activity (Affichage de l'activité réseau)* à partir du volet de navigation.**

▼ Pour afficher l'activité système

Sun StorEdge 5310 NAS Appliance contrôle la charge et l'activité de plusieurs périphériques présents sur le système de stockage. Notez que les noms et le nombre de périphériques contrôlés varient en fonction de votre configuration matérielle.

- **Pour afficher le nombre de requêtes d'E/S des périphériques système, sélectionnez System Activity (Activité système) > View System Activity (Affichage de l'activité système) à partir du volet de navigation.**

Les périphériques système et réseau sont répertoriés dans le [TABLEAU 10-4](#).

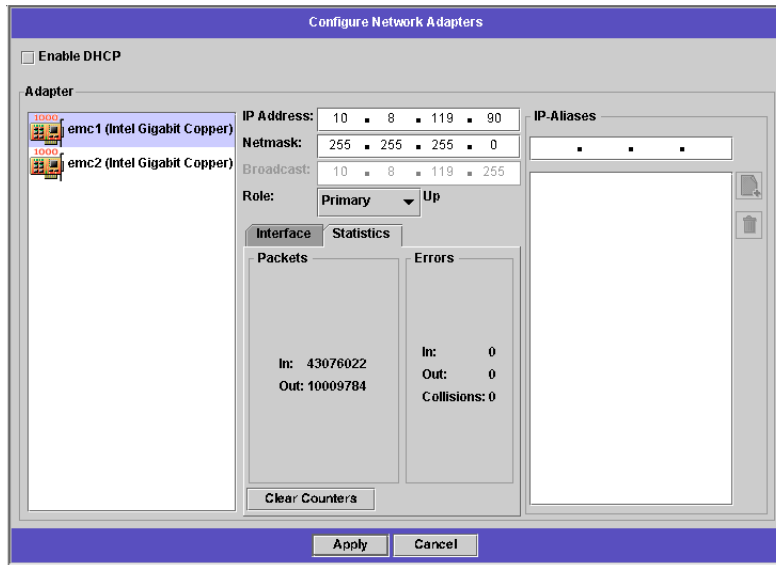
TABLEAU 10-4 Périphériques système et réseau

Code de périphérique	Périphérique
CPU	Unité de calcul central de Sun StorEdge 5310 NAS Appliance
Memory	Mémoire vive (RAM) du système Sun StorEdge 5310 NAS Appliance
Port Aggregation <i>x</i>	Liaison de port <i>x</i>
Controller <i>x</i>	Contrôleur RAID <i>x</i>
dac010 <i>xx</i>	Numéros d'unités logiques (LUN) <i>xx</i>
PORT <i>x</i>	Port <i>x</i>
Host Adapter <i>x</i>	Adaptateur hôte SCSI <i>x</i> (pour périphérique de sauvegarde sur bande)

▼ Pour afficher des statistiques (sur le port) réseau

1. Dans le volet de navigation, sélectionnez **Network Configuration (Configuration réseau) > Configure TCP/IP (Configuration TCP/IP) > Configure Network Adapters (Configuration des adaptateurs réseau)**.

L'écran des statistiques réseau (Viewing Network Statistics) s'affiche.



2. Sélectionnez un port dans la liste Adapter (Adaptateur).

L'onglet **Interface (Interface)** affiche les informations suivantes :

- **Description (Description)** : fournit une description du port sélectionné.
- **H/W Address (Adresse matérielle/logicielle)** : indique, en notation hexadécimale, l'adresse matérielle ou l'adresse MAC (adresse unique) utilisée par le logiciel réseau afin de différencier cette carte des autres cartes réseau. Cette adresse est gravée sur la carte réseau lors de sa fabrication.
- **Speed (Vitesse)** : spécifie la vitesse (en Mbits/s) à laquelle les données sont envoyées sur le réseau.
- **MTU** : indique l'unité de transmission maximale (MTU) de l'adaptateur sélectionné. Cette unité correspond à la taille de trame maximale pouvant être envoyée sur un support physique. La valeur par défaut est 1500. Cette dernière correspond à la valeur maximale, tandis que la valeur minimale est 552.

La taille du plus grand segment TCP correspond à la taille du plus grand datagramme IP moins 40. La taille par défaut du plus grand datagramme IP est de 576 octets. La taille par défaut du plus grand segment TCP est de 536 octets.

3. Cliquez sur l'onglet **Statistics (Statistiques)** pour afficher les informations d'entrée/sortie sur le port sélectionné :
 - **Packets In/Out (Paquets en entrée/sortie)** : nombre de paquets entrants/sortants (reçus/envoyés) par ce port.
 - **Errors In/Out (Erreurs en entrée/sortie)** : nombre d'erreurs d'entrées/sorties de ce port.
 - **Collisions** : nombre de collisions lors des transmissions pour ce port.
-

Affichage des routes réseau

Le panneau **View the Routing Table (Affichage de la table de routage)** permet de visualiser les routes qu'empruntent les paquets pour atteindre un hôte ou un réseau. Ces routes se composent d'un réseau de destination et d'un point d'entrée.

À propos du routage

Il existe deux types de routes : **réseau** et **hôte**. Les routes réseau permettent d'envoyer les paquets à un hôte sur un réseau spécifique. Les routes hôte sont rarement utilisés et servent à envoyer des paquets à un hôte rattaché à un autre hôte ou à une autre passerelle, et non à un réseau connu.

Voici quelques exemples de routes figurant dans la table de routage :

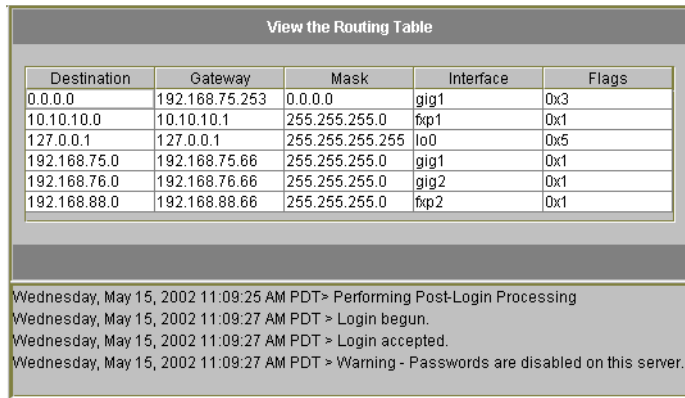
- **0x1** : indique que la route est utilisable.
- **0x2** : indique que la destination est une passerelle.
- **0x4** : indique que la destination est une entrée hôte.
- **0x8** : indique que l'hôte ou le réseau est inaccessible.
- **0x10** : indique que la destination a été créée de manière dynamique.
- **0x20** : indique que la destination a été modifiée de manière dynamique.

Certains indicateurs peuvent être la somme d'indicateurs individuels. Par exemple, **0x3** représente une route utilisable (**0x1**) plus une passerelle (**0x2**).

▼ Pour afficher les routes

Pour afficher le statut des routes du réseau local, accédez au volet de navigation et sélectionnez **Network Configuration (Configuration réseau) > View the Routing Table (Affichage de la table de routage)**.

Le panneau View the Routing Table (Affichage de la table de routage) s'affiche.



Destination	Gateway	Mask	Interface	Flags
0.0.0.0	192.168.75.253	0.0.0.0	gig1	0x3
10.10.10.0	10.10.10.1	255.255.255.0	fxp1	0x1
127.0.0.1	127.0.0.1	255.255.255.255	lo0	0x5
192.168.75.0	192.168.75.66	255.255.255.0	gig1	0x1
192.168.76.0	192.168.76.66	255.255.255.0	gig2	0x1
192.168.88.0	192.168.88.66	255.255.255.0	fxp2	0x1

Wednesday, May 15, 2002 11:09:25 AM PDT> Performing Post-Login Processing
Wednesday, May 15, 2002 11:09:27 AM PDT > Login begun.
Wednesday, May 15, 2002 11:09:27 AM PDT > Login accepted.
Wednesday, May 15, 2002 11:09:27 AM PDT > Warning - Passwords are disabled on this server.

Cet écran affiche les informations suivantes pour chaque route réseau :

- **Destination** : adresse IP de la destination (réseau ou hôte). Une route par défaut (0.0.0.0), une route loopback (127.0.0.1) et au moins une route réseau et une route hôte doivent obligatoirement exister.
- **Gateway (Passerelle)** : adresse de passerelle vers laquelle envoyer les paquets.
- **Mask (Masque)** : masque de réseau du réseau de destination.
- **Interface** : type d'interface utilisée pour envoyer des paquets sur le réseau.
- **Flags (Indicateurs)** : indicateurs signalant le statut de la route. Chaque type d'indication de statut est représenté par un nombre, en notation hexadécimale. Pour plus d'informations, reportez-vous à la section « [À propos du routage](#) », page 170.

Contrôle des composants système

Vous pouvez contrôler l'UPS (Uninterruptible Power Supply, alimentation non interrompible), le contrôleur et le statut de mise en miroir.

Contrôle de l'onduleur UPS

Si vous avez installé l'unité avec un onduleur UPS, vous pouvez contrôler l'UPS.

Remarque – Vous devez connecter l'onduleur UPS au système Sun StorEdge 5310 NAS Appliance avant d'activer son contrôle. Si vous ne le faites pas, le système de contrôle vous renvoie un échec lié à l'onduleur UPS. De plus, Sun StorEdge 5310 NAS Appliance prend uniquement en charge le contrôle et non la gestion de l'onduleur UPS. Reportez-vous au Guide de démarrage de *Sun StorEdge 5310 NAS Appliance et Gateway System* pour des informations détaillées sur l'utilisation de l'UPS.

Capacité de contrôle de l'UPS

Le contrôle de l'UPS fournit une notification dans les cas suivants :

- **Power failure (Coupure de courant)** : indique qu'une coupure de courant s'est produite et que le système fonctionne sur batterie.
- **Power restoration (Restauration du courant)** : indique que le courant a été rétabli.
- **Low battery (Batterie faible)** : indique que la batterie est faible.
- **Recharged battery (Batterie rechargée)** : indique que la batterie de l'onduleur UPS a été correctement chargée.
- **Battery replacement (Remplacement de la batterie)** : indique que l'onduleur UPS a détecté une défaillance au niveau de la batterie et qu'elle doit être remplacée.
- **UPS alarms (Alarmes de l'UPS)** : indique que l'onduleur UPS a détecté une température ambiante ou un taux d'humidité au-delà du seuil acceptable.
- **UPS failure (Erreur de l'UPS)** : indique que le système ne parvient pas à communiquer avec l'onduleur UPS.

Toutes les erreurs, à l'exception de l'erreur batterie rechargée, vous sont envoyées de l'une des manières suivantes : e-mail de notification, notification au serveur SNMP, affichage de l'erreur sur écran LCD ou écriture de l'erreur dans le journal système. La notification de batterie rechargée peut vous être envoyée par e-mail, par notification SNMP ou par consignation dans le journal système, mais non par affichage sur écran LCD.

▼ Pour activer le contrôle de l'onduleur UPS

1. Dans le volet de navigation, sélectionnez **Monitoring and Notification (Contrôle et notification) > Enable UPS Monitoring (Activation du contrôle de l'onduleur UPS)**.
2. Sélectionnez l'option **Enable UPS monitoring (Activer le contrôle de l'onduleur UPS)**.
3. Cliquez sur **Apply (Appliquer)** pour enregistrer la modification.

Affichage des informations sur le contrôleur

Le panneau **View Controller Information (Affichage des informations sur le contrôleur)**, disponible en lecture seule, indique le fournisseur du contrôleur, son modèle et la version du microprogramme.

▼ Pour afficher le fournisseur et le modèle du contrôleur, et la version du microprogramme

Dans le volet de navigation, sélectionnez **RAID > View Controller Information (Affichage des informations sur le contrôleur)**.

Affichage du statut de la mise en miroir

Sun StorEdge 5310 NAS Appliance réalise toute une panoplie de statistiques réseau concernant les volumes de fichiers mis en miroir. Ces statistiques sont uniquement disponibles sur le serveur actif pour chaque volume de fichiers mis en miroir.

▼ Pour afficher les statistiques de mise en miroir

1. À partir du volet de navigation, sélectionnez **File Replicator > View Mirror statistics (Affichage des statistiques de miroir)**.
2. Sélectionnez un volume de fichiers dans la liste **Select Volume (Sélection d'un volume)**.

Le système affiche les informations suivantes concernant le volume de fichiers mis en miroir sélectionné :

- **Status (Statut)** : ce champ indique le statut du miroir. Pour obtenir une définition des indicateurs de statut, reportez-vous à la section « [États du statut du miroir](#) », page 175.
- **Incoming Transactions (Transactions entrantes)** : cette section affiche les statistiques du volume de fichiers sélectionné suivantes :

- **Average (Moyenne)** : nombre moyen de transactions par seconde provenant du serveur actif.
- **Minimum** : nombre minimal de transactions par seconde provenant du serveur actif. La date et l'heure à laquelle ce nombre a été atteint sont affichées à droite.
- **Maximum** : nombre maximal de transactions par seconde provenant du serveur actif. La date et l'heure à laquelle ce nombre a été atteint sont affichées à droite.
- **Outgoing Transactions (Transactions sortantes)** : cette section affiche les statistiques du volume de fichiers sélectionné suivantes :
 - **Average (Moyenne)** : nombre moyen de transactions par seconde provenant du serveur actif et rejoignant le serveur miroir.
 - **Minimum** : nombre minimal de transactions par seconde provenant du serveur actif et rejoignant le serveur miroir. La date et l'heure à laquelle ce nombre a été atteint sont affichées à droite.
 - **Maximum** : nombre maximal de transactions par seconde provenant du serveur actif et rejoignant le serveur miroir. La date et l'heure à laquelle ce nombre a été atteint sont affichées à droite.
- **Mirror Buffer (Tampon miroir)** : cette section affiche le statut du tampon miroir comme suit :
 - **Size (Taille)** : nombre maximum de transactions que le tampon peut traiter.
 - **Free (Libre)** : nombre de transactions restantes dans le tampon miroir.
 - **Utilization (Utilisation)** : pourcentage de transactions dans le tampon miroir.
 - **Fill Rate (Taux de remplissage)** : taux auquel le tampon miroir se remplit, en termes de transactions par seconde. Si ce taux de remplissage est supérieur à zéro, assurez-vous que toutes les liaisons réseaux fonctionnent correctement. Cela implique que les transactions provenant du système actif sont plus rapides que les transactions provenant du système miroir, remplissant ainsi le tampon.
- **Network Statistics (Statistiques sur le réseaux)** : cette section affiche les statistiques réseau du tampon miroir comme suit :
 - **Host (Hôte)** : nom de l'hôte et statut de la connexion du tampon miroir.
 - **Link (Lien)** : statut, qualité et autres statistiques de liens du tampon miroir.
 - **Request Control Blocks (Blocs de requêtes de contrôle)** : nombre de blocs de contrôle envoyés, nombre total d'octets envoyés ainsi que la taille et le taux moyen.
 - **Transfer Rate (Taux de transfert)** : taux moyen auquel les transferts se produisent, nombre maximum et heure à laquelle le maximum de transferts s'est produit.
 - **Response Time (Temps de réponse)** : temps de réponse moyen, temps de réponse maximum et heure à laquelle le temps de réponse maximum s'est produit.

États du statut du miroir

Le statut d'un miroir est affiché dans le panneau **Manage Mirrors (Gestion des miroirs)**. Les différents états possibles sont les suivants :

- **New (Nouveau)** : un miroir est en cours de création.
- **Creating mirror log (Création d'un journal miroir)** : le tampon miroir est en cours d'initialisation.
- **Connecting to host (Connexion à l'hôte)** : le serveur actif se connecte au serveur miroir distant.
- **Creating extent (Création d'une extension)** : le serveur miroir crée des partitions de disque.
- **Ready (Prêt)** : le système est prêt et attend que l'autre système le soit aussi.
- **Down (Hors service)** : la liaison réseau est interrompue.
- **Cracked (Fissuré)** : le miroir est fissuré.
- **Syncing Volume (Volume de synchronisation)** : le serveur miroir synchronise le volume de fichiers.
- **In Sync (Synchronisation)** : le miroir est en cours de synchronisation.
- **Out of Sync (Fin de la synchronisation)** : le miroir n'est plus synchronisé.
- **Error (Erreur)** : une erreur s'est produite.

Affichage du statut de la tâche de sauvegarde

Vous pouvez visualiser des informations sur les tâches de sauvegarde, notamment le journal, le statut des tâches et des bandes.

▼ Pour afficher le journal de sauvegarde

Dans le volet de navigation, sélectionnez **System Backup (Sauvegarde système) > Manage Backup Jobs (Gestion des tâches de sauvegarde) > View Backup Log (Affichage du journal de sauvegarde)**.

Le journal de sauvegarde affiche une liste complète des événements qui se sont produits au cours des processus de sauvegarde système et inclut la date, l'heure et une description de chaque événement. Faites défiler la zone vers le haut pour visualiser les événements de sauvegarde antérieurs.

La taille totale du fichier est affichée en haut de l'écran. Cliquez sur **Refresh (Rafraîchir)** pour actualiser le fichier journal.

▼ Pour afficher le statut des tâches

Dans le volet de navigation, sélectionnez **System Backup (Sauvegarde système) > Manage Backup Jobs (Gestion des tâches de sauvegarde) > View Backup Status (Affichage du statut de la sauvegarde)**.

L'écran présente les processus de sauvegarde, de restauration et de nettoyage les plus récents.

Si un processus de sauvegarde ou de restauration est en cours d'exécution, le bouton **Abort Job (Abandonner la tâche)** est activé. Cliquez sur ce bouton pour suspendre un processus en cours d'exécution et consultez le panneau des événements système pour vérifier que la tâche a été annulée. Veuillez patienter quelques minutes pour que l'annulation soit effective.

▼ Pour afficher le statut des bandes

1. Dans le volet de navigation, sélectionnez **System Backup (Sauvegarde système) > Manage Backup Jobs (Gestion des tâches de sauvegarde) > View Tape Status (Affichage du statut de la bande)**.

2. Sélectionnez les informations de bande à afficher.

- Pour consulter les informations concernant une bande particulière, sélectionnez l'option **Choose Tape Slot (Choix de l'emplacement de la bande)**. Puis, sélectionnez l'emplacement correspondant à la bande que vous souhaitez afficher à partir de la liste.

La numérotation d'emplacement sur cet écran débute avec le chiffre 1. Cependant, la numérotation d'emplacement de périphérique de sauvegarde de la bande individuelle peut varier. Si la numérotation des emplacements de votre périphérique de bande commence par 0 (zéro), sélectionnez l'emplacement 1 sur cet écran pour consulter les informations relatives à l'emplacement 0 de votre périphérique de bande.

- Pour consulter les informations concernant toutes les bandes se trouvant dans le périphérique de bande, sélectionnez l'option **All Slots (Tous les emplacements)**.

Le système prend 1 à 2 minutes par emplacement pour récupérer des informations de bande qui sont affichées dans la zone au bas de l'écran. La sélection de l'option **All Slots (Tous les emplacements)** augmente sensiblement le temps de l'obtention des informations. Le périphérique de bande ne peut récupérer des informations concernant l'emplacement au cours d'un processus de sauvegarde, de restauration ou de nettoyage de la tête.

3. Cliquez sur **Apply (Appliquer)** pour démarrer la découverte de bande.

Remarque – Il est impossible de consulter ces données au cours d'un processus de sauvegarde, de restauration ou de nettoyage de la tête.

Maintenance du système

Ce chapitre décrit les fonctions de maintenance du système.

Ce chapitre aborde les sujets suivants :

- « Définition des options d'accès à distance », page 177
- « Configuration de l'accès FTP », page 178
- « Arrêt du serveur », page 180
- « Points de contrôle de fichiers », page 181
- « Sauvegarde et restauration », page 187
- « Nettoyage des têtes », page 189
- « Conversion des caractères CATIA V4/V5 », page 188
- « Mise à jour du logiciel de Sun StorEdge 5310 NAS Appliance », page 190
- « Mise à niveau des révisions de microprogramme de baies et d'unités », page 191

Définition des options d'accès à distance

Les fonctions de sécurité du système comprennent la définition des options d'accès à distance. Vous avez la possibilité d'activer ou de désactiver les services réseau utilisés pour l'accès à distance au système. Vous pouvez exécuter le système en mode sécurisé afin d'assurer une sécurité maximale ou vous pouvez expressément activer certaines fonctions d'accès à distance telles que Telnet, la connexion à distance et le shell à distance.

Les services sécurisés sont Secure Web Admin (Web Admin sécurisé), qui utilise Secure Socket Layer (SSL) sur http, et Secure Shell (ssh) (Shell sécurisé).

▼ Pour définir la sécurité d'accès à distance

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Set Remote Access (Définition de l'accès à distance)**.
2. **Cochez la case Secure Mode (Mode sécurisée) pour une sécurité maximale.**
En mode sécurisé, seuls **Secure Web Admin (Web Admin sécurisé)** et **Secure Shell (shell sécurisé)** peuvent être activés en cochant la case associée.
3. Si vous n'utilisez pas le mode sécurisé, cochez les cases en regard de chaque service à activer :
 - Web Admin
 - Telnet
 - Remote Login
 - Remote Shell
4. Cliquez sur **Apply (Appliquer)**.
5. Si vous avez choisi **Secure Mode (Mode sécurisé)**, vous devez redémarrer le serveur afin que les paramètres soient pris en compte. Reportez-vous à la section « **Arrêt du serveur** », page 180.

Configuration de l'accès FTP

FTP (File Transfer Protocol, protocole de transfert de fichier) est un protocole Internet permettant de copier des fichiers entre un client et un serveur. Lorsqu'un client se connecte à un serveur, il doit s'identifier à l'aide d'un nom d'utilisateur et d'un mot de passe.

Vous pouvez configurer trois types d'utilisateurs :

- **Administrators (Administrateurs)** : ils disposent du nom d'utilisateur admin et utilisent le même mot de passe que celui utilisé par les clients de l'interface graphique (IG).
L'administrateur dispose d'un accès root à tous les volumes, répertoires et fichiers du système. Le répertoire personnel de l'administrateur est défini comme « / ».
- **Users (Utilisateurs)** : leurs nom d'utilisateur et mot de passe sont définis dans le fichier local de mots de passe ou sur un serveur de noms NIS, NIS+ ou LDAP distant.
L'utilisateur dispose d'un accès à tous les répertoires et fichiers du répertoire personnel de l'utilisateur. Le répertoire personnel est défini en même temps que les informations sur le compte de l'utilisateur et est récupéré par le service de noms.

- **Guests (Invités)** : les invités se connectent avec le nom d'utilisateur « ftp » ou son alias « anonyme ». Bien qu'un mot de passe soit demandé, il n'est pas vérifié. Les invités disposent d'un accès à l'ensemble des répertoires et fichiers du répertoire personnel de l'utilisateur ftp.

Remarque – Les invités ne sont pas autorisés à renommer, écraser ou supprimer des fichiers. Ils ne peuvent ni créer ou supprimer des répertoires, ni modifier les autorisations des fichiers ou répertoires existants.

▼ Pour paramétrer les utilisateurs FTP

1. Dans le volet de navigation, sélectionnez **UNIX Configuration (Configuration UNIX)> Set Up FTP (Paramétrage de FTP)**.
2. Cochez la case **Enable FTP (Activer FTP)**.
3. Sélectionnez le type d'accès FTP en cochant les cases appropriées :
 - L'option **Allow Guest Access (Autoriser l'accès aux invités)** autorise l'accès au serveur FTP par les utilisateurs anonymes.
 - L'option **Allow User Access (Autoriser l'accès aux utilisateurs)** autorise l'accès au serveur FTP par tous les utilisateurs. Cette option ne modifie pas les droits d'accès de l'utilisateur admin ou root.

Remarque – Les noms d'utilisateur et les mots de passe doivent être spécifiés dans le fichier local de mots de passe ou sur un serveur de noms NIS, NIS+ ou LDAP distant.

- L'option **Allow Admin Access (Autoriser l'accès aux administrateurs)** propose un accès root aux personnes en possession du mot de passe administrateur (utilisez cette option avec précaution).

Remarque – Un utilisateur root est un utilisateur possédant un UID égal à 0 et l'admin utilisateur Sun StorEdge 5310 NAS Appliance spécial.

4. Pour activer la journalisation, cochez la case **Enable Logging (Activation de la journalisation)** et indiquez le nom du fichier journal.
5. Cliquez sur **Apply (Appliquer)** pour enregistrer les paramètres.

Arrêt du serveur

Le panneau **Shut Down the Server (Arrêt du serveur)** vous permet d'arrêter, de stopper ou de redémarrer le serveur. (Pour plus d'informations sur l'arrêt du système à l'aide de Telnet, reportez-vous à la section « [Pour arrêter le système](#) », page 264.)

▼ Pour arrêter, stopper ou redémarrer le serveur

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Shut Down the Server (Arrêt du serveur)**.
2. Sélectionnez l'une des options suivantes :
 - **None (Aucune)** : cliquez sur cette option pour ne pas arrêter le serveur.
 - **Halt Both Heads (Arrêter les deux têtes)** : cliquez sur cette option pour arrêter les deux serveurs dans une configuration en cluster. Pour redémarrer, vous devez manuellement mettre sous tension les serveurs.
 - **Reboot Both Heads (Redémarrer les deux têtes)** : cliquez sur cette option pour arrêter puis redémarrer les deux serveurs dans une configuration en cluster.
 - **Reboot Previous Version (Redémarrer la version précédente)** : cliquez sur cette option pour arrêter et redémarrer le serveur à l'aide de la version du logiciel précédemment chargée. Utilisez cette option si vous avez rencontré des problèmes lors de la mise à niveau du logiciel, par exemple. Elle vous permet de redémarrer à l'aide de la dernière version utilisée avant la mise à niveau.



Attention – Renseignez-vous auprès du support technique avant de sélectionner l'option **Reboot Previous Version (Redémarrer la version précédente)**.

- **Halt This Head (Arrêter cette tête)** : cliquez sur cette option pour arrêter ce serveur (celui auquel vous êtes connecté). L'autre serveur reste en ligne. Pour redémarrer, vous devez manuellement mettre sous tension le serveur.
 - **Reboot This Head (Redémarrer cette tête)** : cliquez sur cette option pour arrêter puis redémarrer ce serveur (celui auquel vous êtes connecté). L'autre serveur reste en ligne.
3. Cliquez sur **Apply (Appliquer)**.

Points de contrôle de fichiers

Un point de contrôle, également appelé « point de cohérence » (ou point c), est une copie virtuelle en lecture seule d'un volume de fichiers principal. Si le volume de fichiers reste en lecture/écriture, toutes les données qui existent au moment de la création du point de contrôle demeurent accessibles. Les points de contrôle sont utilisés pour récupérer des fichiers supprimés ou modifiés par erreur et pour stabiliser les sauvegardes.

Remarque – Un point de contrôle est une copie virtuelle du volume de fichiers, stockée dans le même emplacement physique que le volume lui-même. Il ne s'agit pas d'une sauvegarde en ligne. Si le volume de fichiers est perdu, il en est de même pour les points de contrôle.

Pour utiliser les points de contrôle de fichiers, vous activez cette fonction et créez des points de contrôle individuels ou vous en planifiez.

Création de points de contrôle de fichiers

Vous pouvez planifier un point de contrôle ou en créer un tout de suite. Pour plus d'informations sur le paramétrage d'une planification régulière de points de contrôle, reportez-vous à la section « [Planification de points de contrôle de fichiers](#) », page 182.

Dans le panneau **Manage Checkpoints (Gestion des points de contrôle)**, vous avez la possibilité de créer des points de contrôle immédiats, et de renommer et supprimer ceux qui existent déjà. Contrairement aux points de contrôle planifiés, créés à une date et une heure déterminées à l'avance, les points de contrôle immédiats peuvent être créés à tout moment à partir de cet écran.

▼ Pour créer manuellement un point de contrôle

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Edit Properties (Modification des propriétés)**.
2. Sélectionnez le volume pour lequel vous souhaitez créer un point de contrôle dans le menu déroulant **Volume Name (Nom du volume)**.
3. Vérifiez que la case **Enable Checkpoints (Activer les points de contrôle)** est cochée.
Si tel n'est pas le cas, cochez-la et cliquez sur **Apply (Appliquer)**.

4. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Configure Checkpoints (Configuration des points de contrôle) > Manage Checkpoints (Gestion des points de contrôle)**.
5. Pour créer un point de contrôle, cliquez sur **Create (Créer)**.
6. Dans le menu déroulant, sélectionnez le nom du volume pour lequel créer un point de contrôle.
7. Sélectionnez l'une des options de points de contrôle ci-après :
 - **Auto Delete (Suppression automatique)** : sélectionnez **Auto Delete (Suppression automatique)** pour supprimer automatiquement le point de contrôle une fois le nombre de **jours de conservation** et le nombre d'**heures de conservation** écoulés. Pour cette option, le système attribue automatiquement un nom au point de contrôle. Si vous sélectionnez cette option, choisissez le nombre de jours et d'heures de conservation du point de contrôle.
 - **Backup (Sauvegarde)** : pour cette option, le nom par défaut du point de contrôle est **Backup (Sauvegarde)**. Le point de contrôle est utilisé pour des sauvegardes locales du système de fichiers de Sun StorEdge 5310 NAS Appliance. Le point de contrôle n'est pas automatiquement supprimé après une durée spécifiée.
 - **Manual (Manuel)** : sélectionnez cette option si vous souhaitez attribuer un nom autre que **Backup (Sauvegarde)** au point de contrôle. Entrez ensuite le nom dans le champ **Name (Nom)**. Le point de contrôle n'est pas automatiquement supprimé après une durée spécifiée.
8. Cliquez sur **Apply (Appliquer)** pour créer le point de contrôle.

Planification de points de contrôle de fichiers

Le panneau **Schedule Checkpoints (Planification des points de contrôle)** contient la planification actuelle des points de contrôle et vous permet d'ajouter, de modifier et de supprimer les points de contrôle planifiés. Pour chaque point de contrôle planifié, cet écran affiche le nom du volume de fichiers, une description, les heures et les dates programmées, ainsi que la durée de conservation du point de contrôle. La durée de la colonne **Keep (Conservation)** se compose du nombre de jours et du nombre d'heures.

Lorsqu'une ligne est ajoutée à la planification, le système configure automatiquement un point de contrôle pour les heures et les dates requises.

Vous pouvez planifier jusqu'à cinq points de contrôle par volume et plusieurs points de contrôle par planification.

Un exemple de points de contrôle multiples est illustré ci-dessous.

Enabled (Activation)	Description	Days (Jours)	Hours AM (Heures AM)	Hours PM (Heures PM)	Keep (Conservation)	
		SMTWTFS	M1234567890E	M1234567890E	Days + Hours (Jours + heures)	
1. 0	MTWTF5am5pm	-*****-	-----*-----	-----*-----	1	0
2. 0	SunWed1pm	*--*---	-----	-*-----	0	12
3. 0	MWFmidnight	-*-*--	*-----	-----	0	3
4. 0	Week-end	*-----*	*-----*	*-----*	0	6
5. 0	FriEvery2hrs	-----*	*-*-*-*-*	*-*-*-*-*	0	2

▼ Pour ajouter un point de contrôle à la planification

1. **Activez les points de contrôle du volume de fichiers.**
 - a. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Edit Properties (Modification des propriétés)**.
 - b. Sélectionnez le volume pour lequel vous souhaitez ajouter un point de contrôle dans le menu déroulant **Volume Name (Nom du volume)**.
 - c. Vérifiez que la case **Enable Checkpoints (Activer les points de contrôle)** est cochée.
Si tel n'est pas le cas, cochez-la et cliquez sur **Apply (Appliquer)**.
2. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Configure Checkpoints (Configuration des points de contrôle) > Schedule Checkpoints (Planification des points de contrôle)**.
3. Pour ajouter un point de contrôle à la planification, cliquez sur **Add (Ajouter)**.
4. Sélectionnez le volume de fichiers pour lequel vous planifiez des points de contrôle.
5. Entrez une description pour le point de contrôle dans le champ du même nom.
Il s'agit d'un champ obligatoire. Vous pouvez y entrer des informations, telles que le laps de temps entre les points de contrôle, toutes les semaines ou tous les jours, par exemple.
6. Choisissez le nombre de jours et d'heures de conservation du point de contrôle dans les listes déroulantes **Keep Days + Hours (Conserver Jours + Heures)**.

7. **Dans la liste déroulante Days (Jours), sélectionnez les jours où vous souhaitez qu'un point de contrôle soit créé.**
Pour sélectionner plusieurs jours dans cette liste, cliquez sur les jours choisis tout en maintenant la touche Ctrl enfoncée.
8. **Dans la liste AM Hours (Heures AM), sélectionnez l'heure (de minuit à 11 heures du matin) à laquelle le point de contrôle sera créé.**
Pour sélectionner plusieurs éléments dans cette liste, cliquez sur les éléments choisis tout en maintenant la touche Ctrl enfoncée.
9. **Dans la liste PM Hours (Heures PM), sélectionnez l'heure (de midi à 11 heures du soir) à laquelle le point de contrôle sera créé.**
Pour sélectionner plusieurs éléments dans cette liste, cliquez sur les éléments choisis tout en maintenant la touche Ctrl enfoncée.
10. **Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.**

▼ Pour modifier une planification de points de contrôle

1. **Dans le volet de navigation, sélectionnez File Volume Operations (Opérations sur un volume de fichiers) > Configure Checkpoints (Configuration des points de contrôle) > Schedule Checkpoints (Planification des points de contrôle).**
2. **Sélectionnez la ligne à modifier dans la planification et cliquez sur Edit (Modifier).**
3. **Les informations qui sont affichées dans cet écran sont les mêmes que celles de la boîte de dialogue Add Checkpoint Schedule (Ajout de points de contrôle à la planification), mais il ne vous permet pas de modifier le nom du volume.**
4. **Modifiez les informations pertinentes.**
Pour plus d'informations, reportez-vous à la section « [Pour ajouter un point de contrôle à la planification](#) », page 183.
5. **Cliquez sur Apply (Appliquer) pour enregistrer les modifications effectuées.**

▼ Pour supprimer une ligne de la planification

1. **Dans le volet de navigation, sélectionnez File Volume Operations (Opérations sur un volume de fichiers) > Configure Checkpoints (Configuration des points de contrôle) > Schedule Checkpoints (Planification des points de contrôle).**
2. **Sélectionnez la ligne de planification à supprimer en cliquant sur la ligne correspondante, puis cliquez sur Remove (Supprimer).**

▼ Pour renommer un point de contrôle

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Configure Checkpoints (Configuration des points de contrôle) > Manage Checkpoints (Gestion des points de contrôle)**.
2. Sélectionnez le point de contrôle à renommer et cliquez sur **Rename (Renommer)**.
Les champs **Volume Name (Nom du volume)** et **Old Name (Ancien nom)** sont en lecture seule.
3. Dans le champ **New Name (Nouveau nom)**, entrez le nouveau nom du point de contrôle.



Attention – Si vous attribuez un nom standard au point de contrôle auto-delete, le point de contrôle n'est plus supprimé automatiquement.

4. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées.

▼ Pour supprimer un point de contrôle

1. Dans le volet de navigation, sélectionnez **File Volume Operations (Opérations sur un volume de fichiers) > Configure Checkpoints (Configuration des points de contrôle) > Manage Checkpoints (Gestion des points de contrôle)**.
2. Sélectionnez le point de contrôle à supprimer et cliquez sur **Remove (Supprimer)**.

Partage des points de contrôle de fichiers

Les points de contrôle peuvent être partagés, permettant ainsi aux utilisateurs d'avoir accès aux données appropriées lors de la création du point de contrôle.

▼ Pour partager des points de contrôle de fichiers

1. Dans le volet de navigation, sélectionnez **Windows Configuration (Configuration Windows) > Configure Shares (Configuration des partages)**.
2. Cliquez sur **Add (Ajouter)**.
3. Dans la zone **Share Name (Nom de partage)**, saisissez le nouveau nom du partage du point de contrôle.
Le nom de partage est utilisé pour accéder au point de contrôle à partir du réseau.
4. L'option **Mac Extensions (Extensions Mac)** est cochée par défaut.

5. Cliquez sur la case du menu déroulant **Volume Name (Nom du volume)** et sélectionnez le volume de points de contrôle dans la liste.
Les volumes de points de contrôle sont dotés de l'extension `.chkpnt`.
6. Laissez le champ **Directory (Répertoire)** vide.
7. Si **ADS** est activé et configuré, entrez un contexte ADS dans la zone de texte **Container (Conteneur)**.
8. Les champs et options suivants sont grisés si le système est configuré pour le mode de domaine NT. Sinon, remplissez-les comme suit :

- a. Saisissez **0** dans la zone **User (Utilisateur)**.

- b. Saisissez **0** dans la zone **Group (Groupe)**.

- c. Laissez les zones **R/W Password (Mot de passe de lecture/écriture)** et **R/O Password (Mot de passe de lecture seule)** vides.

Les volumes de points de contrôle sont en lecture seule.

9. Cliquez sur **Apply (Appliquer)**.

Remarquez que le nouveau point de contrôle est répertorié en tant que partage dans le panneau **Configure Share (Configuration du partage)**.

Accès aux points de contrôle de fichiers

Les utilisateurs peuvent avoir accès aux points de contrôle et ainsi aux données appropriées lors de la création du point de contrôle.

▼ Pour accéder à un point de contrôle

1. Sur un poste en réseau, cliquez sur le menu **Démarrer de Windows**.
2. Sélectionnez **Exécuter**.
3. Dans la boîte de dialogue **Exécuter**, saisissez le nom de partage d'un point de contrôle et l'adresse IP du serveur **Sun StorEdge 5310 NAS Appliance**.
Par exemple, tapez `\\xxx.xxx.xxx.xxx\nom-de-partage`.
4. Cliquez sur **OK**.

Sauvegarde et restauration

Le système Sun StorEdge 5310 NAS Appliance prend en charge les sauvegardes réseau NDMP.

Paramétrage du protocole NDMP

Le protocole de gestion de données en réseau (NDMP, Network Data Management Protocol) est un protocole ouvert aux sauvegardes en réseau. L'architecture NDMP vous permet d'utiliser des applications d'administration de sauvegarde conformes à NDMP pour sauvegarder le périphérique de stockage associé au réseau.

Remarque – L'application d'administration de sauvegarde doit être configurée de manière à ce que l'utilisateur doive utiliser le nom d'utilisateur administrateur et le mot de passe de l'administrateur de la console (interface de ligne de commande) pour se connecter.

Remarque – Les points de contrôle doivent être activés pour que les volumes puissent être sauvegardés par le protocole NDMP. Reportez-vous à la section « [Création de points de contrôle de fichiers](#) », page 181.

▼ Pour paramétrer le protocole NDMP

1. Dans le volet de navigation, sélectionnez **System Backup (Sauvegarde système) > Set Up NDMP (Paramétrage du protocole NDMP)**.
2. Sélectionnez la carte d'interface réseau (NIC) NDMP à utiliser pour transférer les données vers le lecteur de sauvegarde sur bande.
3. L'adresse de passerelle est affichée pour chaque port.
Si le périphérique de sauvegarde sur bande NDMP est situé sur un autre réseau, veillez à sélectionner le port qui permet la connexion à la passerelle associée.
4. Cliquez sur **Apply (Appliquer)**.

Conversion des caractères CATIA V4/V5

Sun StorEdge 5310 NAS Appliance et Gateway System interagissent avec les produits CATIA V4/V5 (développés par Dassault Systèmes).

CATIA V4 est un produit uniquement compatible avec UNIX tandis que CATIA V5 est disponible pour les plates-formes UNIX et Windows. CATIA V4 peut utiliser certains caractères dans des noms de fichiers qui ne sont pas reconnus par Windows. Lorsque des clients CATIA migrent de la version V4 à la version V5, les fichiers V4 risquent de devenir inaccessibles sous Windows si leur nom comprend des caractères non valides sous ce système d'exploitation. Par conséquent, une option de conversion des caractères est fournie pour l'interopérabilité UNIX/Windows entre les versions V4/V5 de CATIA.

La table de conversion est illustrée dans le [TABLEAU 11-1](#).

TABLEAU 11-1 Table de conversion des caractères pour CATIA

Caractère UNIX dans CATIA V4	Caractère Windows dans CATIA V5	Description du caractère dans CATIA V5
Guillemets double ouverts arrondis (non reproduits)	¨	Tréma
*	¤	Symbole monétaire
/	ø	Lettre latine O minuscule barrée
:	÷	Symbole de la division
<	«	Guillemets angulaires double pointant à gauche
>	»	Guillemets angulaires double pointant à droite
?	¿	Point d'interrogation inversé
\	ÿ	Lettre latine Y minuscule avec tréma
	Barre verticale interrompue (non reproduite)	Barre verticale interrompue

Par défaut, la prise en charge de l'interopérabilité des versions V4/V5 de CATIA est désactivée. Vous pouvez activer cette fonction soit manuellement via la CLI soit automatiquement après une initialisation du système.

▼ Pour activer CATIA à l'aide de la CLI

- Exécutez la commande CLI `load catia`. Avec cette méthode, vous devez réactiver la prise en charge de CATIA après chaque redémarrage du système.

▼ Pour activer automatiquement CATIA au redémarrage

1. Modifiez le fichier `/dvol/etc/inetload.ncf` en insérant le mot `catia` sur une ligne distincte du fichier.

2. Exécutez les deux commandes CLI suivantes afin de redémarrer le service `inetload`:

```
unload inetload  
load inetload
```

Si la prise en charge des versions V4/V5 de CATIA a été activée correctement, une entrée similaire à la suivante figure dans le journal système :

```
07/25/05 01:42:16 I catia: $Revision: 1.1.4.1
```

Nettoyage des têtes

Vous pouvez afficher des informations sur le dernier nettoyage des têtes ou paramétrage du prochain nettoyage des têtes du périphérique de bande local.

▼ Pour effectuer un nettoyage des têtes

1. Dans le volet de navigation, sélectionnez **System Backup (Sauvegarde système) > Assign Cleaning Slot (Attribution d'un emplacement de nettoyage)**.
2. Sélectionnez le numéro d'emplacement qui contient la bande pour le nettoyage des têtes.

La numérotation d'emplacement sur cet écran commence au chiffre 1. Cependant, la numérotation d'emplacement de périphérique de sauvegarde de la bande individuelle peut varier. Si la numérotation des emplacements de votre périphérique de bande commence par 0 (zéro), sélectionnez l'emplacement 1 sur cet écran pour consulter les informations relatives à l'emplacement 0 de votre périphérique de bande.

3. Entrez un chiffre dans la zone **Cleaning Count (Nombre de nettoyages)** afin de garder un suivi du nombre d'utilisations d'une bande pour le nettoyage des têtes. Une bande de nettoyage ne doit pas être utilisée plus de dix fois. Ce chiffre est augmenté de 1 à chaque fois qu'un nettoyage des têtes a lieu.
4. Pour effectuer un nettoyage des têtes tout de suite, cochez **Run Immediately (Exécuter tout de suite)**. Le nettoyage est lancé avec le numéro d'emplacement spécifié et le nombre de nettoyages.
5. Cliquez sur **Apply (Appliquer)** pour enregistrer les modifications effectuées. Si vous avez coché la case **Run Immediately (Exécuter tout de suite)**, le nettoyage commence immédiatement.

Mise à jour du logiciel de Sun StorEdge 5310 NAS Appliance

Contactez le support technique de Sun Microsystems afin d'obtenir les fichiers de mise à jour correspondant à la configuration de votre système. Une fois les fichiers obtenus, utilisez le panneau **Update Software (Mise à jour du logiciel)** pour mettre à jour le logiciel de Sun StorEdge 5310 NAS Appliance.



Attention – Il est déconseillé de mettre à jour les logiciels système ou les microprogrammes RAID lorsque l'état du sous-système RAID est critique, ou lors de la création d'un volume ou de la reconstitution d'un volume existant.

▼ Pour mettre à jour le logiciel

La procédure suivante nécessite le redémarrage du système une fois la mise à jour effectuée. Le redémarrage du système requiert l'arrêt de toutes les activités d'E/S. Par conséquent, planifiez l'exécution de la mise à jour du logiciel lors d'une période de maintenance programmée.

Remarque – Dans une configuration en cluster, effectuez cette procédure sur les deux serveurs du cluster.

1. Dans le volet de navigation, sélectionnez **System Operations (Opérations du système) > Update Software (Mise à jour du logiciel)**.

2. Dans le panneau Update Software (Mise à jour du logiciel), saisissez le chemin d'accès aux fichiers de mise à jour.
S'il faut rechercher le chemin d'accès, cliquez sur **Browse (Parcourir)**.
3. Cliquez sur Update (Mise à jour) pour lancer le processus.
4. A la fin du processus de mise à jour, cliquez sur Yes (Oui) pour redémarrer ou sur No (Non) pour continuer sans redémarrer le système.
La mise à jour n'est effective qu'au redémarrage du système.

Mise à niveau des révisions de microprogramme de baies et d'unités

Cette section explique comment identifier les niveaux de révision des microprogrammes de baies et d'unités et comment mettre à niveau ces microprogrammes. Elle aborde les sujets suivants :

- [« Nécessité de mettre à niveau un microprogramme », page 191](#)
- [« Mise à niveau des microprogrammes de baies et d'unités \(redémarrage nécessaire\) », page 192](#)
- [« Mise à niveau du microprogramme d'une baie \(redémarrage inutile\) », page 194](#)
- [« Mise à niveau du microprogramme d'une unité \(redémarrage nécessaire\) », page 198](#)

Nécessité de mettre à niveau un microprogramme

Avant de procéder à la mise à niveau d'un microprogramme, vérifiez si cela s'avère nécessaire en identifiant le niveau de révision actuel du microprogramme des différents composants de la baie.

Vous pouvez utiliser la commande `raidctl profile` afin de capturer et d'enregistrer le niveau de révision actuel du microprogramme des unités de contrôleur RAID, unités d'extension, NVSRAM de contrôleur et unités de disque. Pour plus d'informations, reportez-vous à la section [« Capture de la sortie de la commande `raidctl` », page 200](#).

Mise à niveau des microprogrammes de baies et d'unités (redémarrage nécessaire)

Cette procédure permet de mettre à niveau les microprogrammes des baies RAID et des unités de disque. Elle requiert le redémarrage du serveur NAS.

Si vous ne parvenez pas à redémarrer le serveur NAS et devez seulement mettre à niveau le microprogramme de la baie, reportez-vous à la section « [Mise à niveau du microprogramme d'une baie \(redémarrage inutile\)](#) », page 194.

Le temps nécessaire à la procédure de mise à niveau du microprogramme est variable et dépend de la configuration. Par exemple, il faut environ 50 minutes pour mettre à niveau et redémarrer un serveur NAS doté de deux contrôleurs RAID, d'une unité d'extension FC (Fibre Channel) et d'une unité d'extension SATA (Serial Advanced Technology Attachment). Consultez le [TABLEAU 11-3](#) pour déterminer le temps requis pour l'opération en fonction de votre configuration.

Remarque – La mise à niveau du microprogramme des unités implique obligatoirement le redémarrage du serveur NAS.

Remarque – Les unités de chaque type seront mises à niveau, y compris celles déjà au même niveau que le fichier du microprogramme sélectionné.



Attention – N'appliquez pas la procédure à une unité en panne qui se trouve en état de reconstruction. Ces informations sont consignées dans le journal système ou disponibles à partir de la page RAID de Web Administrator.

Avant de commencer, assurez-vous que la version 4.10.18 (au minimum) du serveur NAS est installée sur le système. Ne tentez pas de mettre à niveau le microprogramme d'une baie ou d'une unité d'un serveur NAS exécutant une version antérieure du système d'exploitation (SE).

1. **Téléchargez le dernier patch à partir du site www.sunsolve.sun.com et décompressez le fichier.**
2. **Parcourez le fichier `readme` (Lisezmoi) du patch afin de connaître les niveaux de révision du microprogramme associés au patch.**
3. **À partir d'un client NAS, activez le protocole FTP.**

Pour plus d'informations sur l'activation du protocole FTP à partir de l'IG, reportez-vous à la section « [Configuration de l'accès FTP](#) », page 178. Consultez la section « [Configuration de l'accès FTP](#) », page 260 si vous vous servez de la CLI.

4. Accédez au répertoire dans lequel vous avez téléchargé le patch.
5. Utilisez le protocole FTP pour vous connecter au serveur NAS en tant qu'utilisateur admin.
6. Tapez `bin` pour activer le mode binaire.
7. À l'invite `ftp`, créez les répertoires suivants sur `/cvol` en exécutant les commandes ci-dessous :

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctlr
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
mkdir /cvol/firmware/2882/drive
```

8. Accédez au répertoire que vous venez de créer pour le microprogramme et copiez le fichier de ce dernier (voir [TABLEAU 11-2](#)) à l'aide de la commande `put`.

Par exemple, pour charger le microprogramme du contrôleur RAID, exécutez les commandes suivantes :

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

9. Poursuivez le chargement de fichiers de microprogramme dans les répertoires appropriés.

Le [TABLEAU 11-2](#) indique le répertoire et un exemple de fichier de microprogramme pour chaque composant.

TABLEAU 11-2 Répertoires et fichiers de microprogramme des composants

Composant	Répertoire	Exemple de nom de fichier
Contrôleur RAID	<code>/cvol/firmware/2882/ctlr</code>	<code>SNAP_288X_06120910.dlp</code>
NVSRAM de contrôleur RAID	<code>/cvol/firmware/2882/nvsram</code>	<code>N2882-612843-503.dlp</code>
Unité d'extension (EU) FC	<code>/cvol/firmware/2882/jbod</code>	<code>esm9631.s3r</code>
EU SATA	<code>/cvol/firmware/2882/jbod</code>	<code>esm9722.dl</code>
Types d'unités :		
Seagate ST314680	<code>/cvol/firmware/2882/drive</code>	<code>D_ST314680FSUN146G_0407.dlp</code>
Seagate 10K	<code>/cvol/firmware/2882/drive</code>	<code>D_ST314670FSUN146G_055A.dlp</code>

TABLEAU 11-2 Répertoires et fichiers de microprogramme des composants (Suite)

Composant	Répertoire	Exemple de nom de fichier
Hitachi 400GB HDS724040KLSA80	/cvol/firmware/2882/drive	D_HDS7240SBSUN400G_AC7A.dlp
Fujitsu MAT3300F 300GB	/cvol/firmware/2882/drive	D_MAT3300FSUN300G_1203.dlp
Seagate 10K 300GB	/cvol/firmware/2882/drive	D_ST330000FSUN300G_055A.dlp

10. Fermez la session FTP.**11. Utilisez le protocole Telnet pour vous connecter au serveur NAS et accéder à un compte utilisateur avec les privilèges admin.****12. Redémarrez le système. Dans une configuration en cluster, redémarrez les deux serveurs.**

Le [TABLEAU 11-3](#) indique le temps approximatif nécessaire à la mise à niveau du microprogramme des différents composants.

TABLEAU 11-3 Temps nécessaire à la mise à niveau des microprogrammes

Composant	Durée de la mise à niveau
Contrôleur RAID	Redémarrage + 15 minutes
NVSRAM de contrôleur RAID	Redémarrage + 5 minutes
EU FC ou SATA	Redémarrage + 5 minutes
Unités	Redémarrage + une minute trente par unité

13. Vérifiez que le nouveau microprogramme est bien chargé en exécutant la commande suivante :

```
raidctl get type=lsi target=profile ctrl=0
```

Vous pouvez également consulter le journal système pour repérer les éventuels échecs.

Mise à niveau du microprogramme d'une baie (redémarrage inutile)

Cette procédure décrit la mise à niveau des microprogrammes de baies RAID sans nécessiter le redémarrage du serveur NAS.

Avant de commencer, gardez à l'esprit les points suivants :

- La version 4.10.18 (au minimum) du serveur NAS doit être installée. Ne tentez pas de mettre à niveau le microprogramme d'un serveur NAS disposant d'une version antérieure du SE.

- Cette procédure fonctionne mieux en présence de peu d'activités E/S. Le contrôleur met en attente les E/S pendant la mise à niveau.



Attention – N'appliquez pas la procédure à une unité en panne qui se trouve en état de reconstruction. Ces informations sont consignées dans le journal système.

1. Téléchargez le dernier patch à partir du site www.sunsolve.sun.com et décompressez le fichier.
2. Parcourez le fichier `readme (Lisezmoi)` du patch afin de connaître les niveaux de révision du microprogramme associés au patch.
3. Accédez au répertoire dans lequel vous avez téléchargé le patch.
4. À partir d'un client NAS, activez le protocole FTP.
Pour plus d'informations sur l'activation du protocole FTP à partir de l'IG, reportez-vous à la section « [Configuration de l'accès FTP](#) », page 178. Consultez la section « [Configuration de l'accès FTP](#) », page 260 si vous vous servez de la CLI.
5. Utilisez le protocole FTP pour vous connecter au serveur NAS et accéder à un compte utilisateur avec les privilèges admin.
6. Tapez `bin` pour activer le mode binaire.
7. À l'invite `ftp`, créez les répertoires suivants sur `/cvol` en exécutant les commandes suivantes :

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctlr
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
```

8. Accédez au répertoire que vous venez de créer pour le microprogramme et copiez le fichier de ce dernier (voir [TABLEAU 11-4](#)) à l'aide de la commande `put`.

Par exemple, pour charger le microprogramme du contrôleur RAID, exécutez les commandes suivantes :

```
cd /cvol/firmware/2882/ctlr
put SNAP_288X_06120910.dlp
```

9. Poursuivez le chargement de fichiers de microprogramme dans les répertoires appropriés.

Le [TABLEAU 11-4](#) indique le répertoire et un exemple de fichier de microprogramme pour chaque composant.

TABLEAU 11-4 Répertoires et fichiers de microprogramme des composants

Composant	Répertoire	Exemple de nom de fichier
Contrôleur RAID	/cvol/firmware/2882/ctlr	SNAP_288X_06120910.dlp
NVSRAM de contrôleur RAID	/cvol/firmware/2882/nvsram	N2882-612843-503.dlp
EU FC	/cvol/firmware/2882/jbod	esm9631.s3r
EU SATA	/cvol/firmware/2882/jbod	esm9722.dl

10. Fermez la session FTP.

11. Utilisez le protocole Telnet pour vous connecter au serveur NAS et accéder à un compte utilisateur avec les privilèges admin.

12. Exécutez la commande `raidctl download` pour charger chaque fichier dans le répertoire cible.

Par exemple, pour charger le microprogramme du contrôleur à partir du répertoire `ctlr` sur les contrôleurs 0 et 1, exécutez cette commande :

```
raidctl download type=lsi target=ctlr ctlr=0
```

Cette commande permet de télécharger le fichier de microprogramme sur les deux contrôleurs et de supprimer le fichier du répertoire.

Remarque – La commande `raidctl download` permet de supprimer le fichier de microprogramme après chaque lancement de la commande. Par conséquent, vous devez recopier le fichier de microprogramme après la mise à niveau des différents composants (unité de contrôleur, NVSRAM de contrôleur, unité d’extension, unités).

Pour télécharger le microprogramme situé dans le répertoire `jbod` vers le boîtier d’extension 0, exécutez la commande suivante :

```
raidctl download type=lsi target=jbod ctlr=0
```

13. Vérifiez la progression de chaque téléchargement depuis la session Telnet.

Le temps nécessaire à la procédure complète de mise à niveau se définit comme suit :

Composant	Minutes par composant
EU de contrôleur RAID	15 minutes
NVSRAM de contrôleur RAID	5 minutes
EU FC ou SATA	5 minutes

Remarque – Une fois la mise à niveau terminée, le curseur telnet peut prendre jusqu'à 5 minutes pour réapparaître. Patientez jusqu'à ce que le curseur soit à nouveau visible.

14. Avant de passer au composant suivant, vérifiez dans le journal système que le téléchargement est terminé.

L'exemple suivant illustre la sortie du journal système :

```
Ctrl-  
  
Firmware Download 90% complete  
Firmware Download 95% complete  
Firmware Download 100% complete  
Waiting for controllers to become ACTIVE  
Controller 0 - now ACTIVE  
Controller 1 - now ACTIVE  
Controllers are now active  
nvram-  
  
raidctl download type=lsi target=nvsram ctrlr=0  
Flashing C0 NVSRAM: /cvol/nf2/./firmware/2882/nvsram/n2882-  
61.dlp (48068)  
Firmware Download 100% complete  
Waiting for controllers to become ACTIVE  
Controller 0 - now ACTIVE  
Controller 1 - now ACTIVE  
Controllers are now active  
ESM-
```

```

>> raidctl download type=lsi target=jbod ctrlr=0 tray=1

Flashing C0 JBOD 1 with
/cvol/nf1/./firmware/2882/jbod/esm9631.s3r (663604)
Firmware Download 20% complete
Firmware Download 30% complete
Firmware Download 50% complete
Firmware Download 60% complete
Firmware Download 90% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
Drive-
10/26/05 10:57:42 I Firmware Download 20% complete
10/26/05 10:57:46 I Firmware Download 30% complete
10/26/05 10:57:50 I Firmware Download 40% complete
10/26/05 10:57:54 I Firmware Download 50% complete
10/26/05 10:57:58 I Firmware Download 60% complete
10/26/05 10:58:03 I Firmware Download 70% complete
10/26/05 10:58:08 I Firmware Download 80% complete
10/26/05 10:58:13 I Firmware Download 90% complete
10/26/05 10:58:18 I Bytes Downloaded: 628224 (2454 256 chunks),
imageSize=62804
      8
10/26/05 10:59:01 I Flashed OK - drive in tray 2 slot 12
10/26/05 10:59:01 I Downloaded firmware version 0407 to 27 drives

```

Mise à niveau du microprogramme d'une unité (redémarrage nécessaire)

Cette procédure décrit la mise à niveau du seul microprogramme des unités. Elle requiert le redémarrage du serveur NAS.

Remarque – La mise à niveau du microprogramme des unités implique obligatoirement le redémarrage du serveur NAS.

Remarque – Les unités de chaque type seront mises à niveau, y compris celles déjà au même niveau que le fichier du microprogramme sélectionné.

Le temps nécessaire à la procédure de mise à niveau du microprogramme est variable. Il dépend du nombre d'unités installées et du temps nécessaire au redémarrage du serveur NAS. Consultez le [TABLEAU 11-3](#) pour déterminer le temps requis en fonction de votre configuration.



Attention – N'appliquez pas la procédure à une unité en panne qui se trouve en état de reconstruction. Ces informations sont consignées dans le journal système.

Avant de commencer, assurez-vous que la version 4.10.18 (au minimum) du serveur NAS est installée sur le système. Ne tentez pas de mettre à niveau le microprogramme d'un serveur NAS disposant d'une version antérieure du SE.

1. **Téléchargez le dernier patch à partir du site www.sunsolve.sun.com et décompressez le fichier.**
2. **Parcourez le fichier `readme` (Lisezmoi) du patch afin de connaître les niveaux de révision du microprogramme associés au patch.**
3. **Accédez au répertoire dans lequel vous avez téléchargé le patch.**
4. **À partir d'un client NAS, activez le protocole FTP.**
Pour plus d'informations sur l'activation du protocole FTP à partir de l'IG, reportez-vous à la section « [Configuration de l'accès FTP](#) », page 178. Consultez la section « [Configuration de l'accès FTP](#) », page 260 si vous vous servez de la CLI.
5. **Utilisez le protocole FTP pour vous connecter au serveur NAS en tant qu'utilisateur `admin`.**
6. **Tapez `bin` pour activer le mode binaire.**
7. **À l'invite `ftp`, créez le répertoire suivant sur `/cvol` en exécutant la commande suivante :**

```
mkdir /cvol/firmware/2882/drive
```
8. **Accédez au répertoire que vous venez de créer pour le microprogramme des unités et copiez le fichier de ce dernier (voir [TABLEAU 11-2](#)) à l'aide de la commande `put`.**
Par exemple, pour charger le microprogramme de l'unité Seagate ST314680, exécutez les commandes suivantes :

```
cd /cvol/firmware/2882/drive  
put D_ST314680FSUN146G_0407.dlp
```
9. **Fermez la session FTP.**

10. Utilisez le protocole Telnet pour vous connecter au serveur NAS en tant qu'utilisateur `admin`.
11. Redémarrez le système. Dans une configuration en cluster, redémarrez les deux serveurs.
Le temps nécessaire à la procédure complète de mise à niveau se compose du temps de redémarrage + une minute trente par unité.
12. Vérifiez que le nouveau microprogramme est bien chargé en exécutant la commande suivante :

```
raidctl get type=lsi target=profile ctrl=0
```


Vous pouvez également consulter le journal système pour repérer les éventuels échecs.

Capture de la sortie de la commande `raidctl`

Vous pouvez utiliser la commande `raidctl profile` afin de déterminer le niveau de révision actuel du microprogramme des unités de contrôleur RAID, unités d'extension, NVSRAM de contrôleur et unités de disque. Cette section fournit les instructions des procédures suivantes :

- « Pour capturer la sortie de la commande `raidctl` depuis un client Solaris », page 200
- « Pour capturer la sortie de la commande `raidctl` depuis un client Windows », page 211

▼ Pour capturer la sortie de la commande `raidctl` depuis un client Solaris

1. Sur un client Solaris, tapez la commande `script` et un nom de fichier. Exemple :

```
> script raidctl
```
2. Utilisez le protocole Telnet pour vous connecter au serveur NAS.
3. Pour recueillir les données générées, tapez la commande `raidctl` suivante :

```
raidctl get type=lsi target=profile ctrl=0
```
4. Tapez `exit` pour fermer la session Telnet.
5. Tapez à nouveau `exit` pour fermer le fichier intitulé `raidctl`.

L'exemple suivant illustre la sortie générée par la commande, avec la commande et les niveaux de microprogramme résultants en gras :

```
telnet 10.8.1xx.x2
Trying 10.8.1xx.x2...
Connected to 10.8.1xx.x2.
Escape character is '^]'.
connect to (? for list) ? [menu] admin
password for admin access ? *****
5310 > raidctl get type=lsi target=profile ctrl=0

SUMMARY-----
Number of controllers: 2
Number of volume groups: 4
Total number of volumes (includes an access volume): 5 of 1024 used
    Number of standard volumes: 4
    Number of access volumes: 1
Number of drives: 28
Supported drive types: Fibre (28)
Total hot spare drives: 2
    Standby: 2
    In use: 0
Access volume: LUN 31
Default host type: Sun_SE5xxx (Host type index 0)
Current configuration
    Firmware version: PkgInfo 06.12.09.10
    NVSRAM version: N2882-612843-503
Pending configuration
```

```
CONTROLLERS -----
Number of controllers: 2

Controller in Tray 0, Slot B
  Status: Online
  Current Configuration
    Firmware version: 06.12.09.10
    Appware version: 06.12.09.10
    Bootware version: 06.12.09.10
    NVSRAM version: N2882-612843-503
  Pending Configuration
    Firmware version: None
    Appware version: None
    Bootware version: None
    NVSRAM version: None
    Transferred on: None
  Board ID: 2882
  Product ID: CSM100_R_FC
  Product revision: 0612
  Serial number: 1T44155753
  Date of manufacture: Sat Oct 16 00:00:00 2004
  Cache/processor size (MB): 896/128
  Date/Time: Thu Nov  2 19:15:49 2006
  Associated Volumes (* = Perferred Owner):
    lun4* (LUN 3)
Ethernet port: 1
  Mac address: 00.A0.B8.16.C7.A7
  Host name: gei
  Network configuration: Static
  IP address: 192.168.128.106
  Subnet mask: 255.255.255.0
  Gateway: 192.168.128.105
  Remote login: Enabled
Drive interface: Fibre
  Channel: 2
  Current ID: 124/0x7C
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:02:00:A0:B8:16:C7:A7
  World-wide node name: 20:00:00:A0:B8:16:C7:A7
  Part type: HPFC-5400      revision 6
```

```
Drive interface: Fibre
  Channel: 2
  Current ID: 124/0x7C
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:02:00:A0:B8:16:C7:A7
  World-wide node name: 20:00:00:A0:B8:16:C7:A7
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 2
  Current ID: 255/0x3
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
  World-wide port name: 20:07:00:A0:B8:16:C6:FB
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 2
  Current ID: 255/0x3
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
  World-wide port name: 20:07:00:A0:B8:16:C6:FB
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6

Controller in Tray 0, Slot A
  Status: Online
  Current Configuration
    Firmware version: 06.12.09.10
    Appware version: 06.12.09.10
    Bootware version: 06.12.09.10
    NVSRAM version: N2882-612843-503
  Pending Configuration
    Firmware version: None
    Appware version: None
    Bootware version: None
    NVSRAM version: None
    Transferred on: None
```

```
Board ID: 2882
Product ID: CSM100_R_FC
Product revision: 0612
Serial number: 1T44155741
Date of manufacture: Sun Oct 10 00:00:00 2004
Cache/processor size (MB): 896/128
Date/Time: Thu Nov  2 19:15:45 2006
Associated Volumes (* = Perferred Owner):
lun1* (LUN 0), lun2* (LUN 1), lun3* (LUN 2)
Ethernet port: 1
  Mac address: 00.A0.B8.16.C6.F9
  Host name: gei
  Network configuration: Static
  IP address: 192.168.128.105
  Subnet mask: 255.255.255.0
  Gateway: 192.168.128.105
  Remote login: Enabled
Drive interface: Fibre
  Channel: 1
  Current ID: 125/0x7D
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:01:00:A0:B8:16:C6:F9
  World-wide node name: 20:00:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Drive interface: Fibre
  Channel: 1
  Current ID: 125/0x7D
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:01:00:A0:B8:16:C6:F9
  World-wide node name: 20:00:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 1
  Current ID: 255/0x0
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
```

```
Link status: Down
Topology: Unknown
World-wide port name: 20:06:00:A0:B8:16:C6:FA
World-wide node name: 20:06:00:A0:B8:16:C6:F9
Part type: HPFC-5400      revision 6
Host interface: Fibre
Channel: 1
Current ID: 255/0x0
Maximum data rate: 200 MB/s
Current data rate: 200 MB/s
Data rate control: Auto
Link status: Down
Topology: Unknown
World-wide port name: 20:06:00:A0:B8:16:C6:FA
World-wide node name: 20:06:00:A0:B8:16:C6:F9
Part type: HPFC-5400      revision 6
```

VOLUME GROUPS-----

```
Number of volume groups: 4
Volume group 1 (RAID 5)
Status: Online
Tray loss protection: No
Associated volumes and free capacities:
    lun1 (681 GB)
Associated drives (in piece order):
Drive at Tray 0, Slot 7
Drive at Tray 0, Slot 6
Drive at Tray 0, Slot 5
Drive at Tray 0, Slot 4
Drive at Tray 0, Slot 3
Drive at Tray 0, Slot 8
Volume group 2 (RAID 5)
Status: Online
Tray loss protection: No
Associated volumes and free capacities:
    lun2 (681 GB)
Associated drives (in piece order):
Drive at Tray 0, Slot 14
Drive at Tray 0, Slot 13
Drive at Tray 0, Slot 12
Drive at Tray 0, Slot 11
Drive at Tray 0, Slot 10
Drive at Tray 0, Slot 9
```

Volume group 3 (RAID 5)
 Status: Online
 Tray loss protection: No
 Associated volumes and free capacities:
 lun3 (817 GB)
 Associated drives (in piece order):
 Drive at Tray 11, Slot 5
 Drive at Tray 11, Slot 4
 Drive at Tray 11, Slot 3
 Drive at Tray 11, Slot 2
 Drive at Tray 11, Slot 1
 Drive at Tray 11, Slot 7
 Drive at Tray 11, Slot 6

Volume group 4 (RAID 5)
 Status: Online
 Tray loss protection: No
 Associated volumes and free capacities:
 lun4 (817 GB)
 Associated drives (in piece order):
 Drive at Tray 11, Slot 13
 Drive at Tray 11, Slot 12
 Drive at Tray 11, Slot 11
 Drive at Tray 11, Slot 10
 Drive at Tray 11, Slot 9
 Drive at Tray 11, Slot 8
 Drive at Tray 11, Slot 14

STANDARD VOLUMES-----

SUMMARY

Number of standard volumes: 4

NAME	STATUS	CAPACITY	RAID LEVEL	VOLUME GROUP
lun1	Optimal	681 GB	5	1
lun2	Optimal	681 GB	5	2
lun3	Optimal	817 GB	5	3
lun4	Optimal	817 GB	5	4

DETAILS

Volume name: lun1
Volume ID: 60:0A:0B:80:00:16:C6:F9:00:00:23:B4:43:4B:53:3A
Subsystem ID (SSID): 0
Status: Optimal
Action: 1
Tray loss protection: No
Preferred owner: Controller in slot A
Current owner: Controller in slot B
Capacity: 681 GB
RAID level: 5
Segment size: 64 KB
Associated volume group: 1
Read cache: Enabled
Write cache: Enabled
Flush write cache after (in seconds): 8
Cache read ahead multiplier: 1
Enable background media scan: Enabled
Media scan with redundancy check: Disabled

DRIVES-----

SUMMARY

Number of drives: 28
Supported drive types: Fiber (28)

BASIC:

CURRENT	PRODUCT	FIRMWARE			
TRAY, SLOT	STATUS	CAPACITY	DATA RATE	ID	REV
0,1	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,7	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,6	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,5	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,4	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,3	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,2	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,14	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,13	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,12	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,11	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,10	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,9	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
0,8	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307

11,5	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,4	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,3	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,2	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,1	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,13	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,12	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,11	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,10	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,9	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,8	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,7	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,6	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,14	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307

HOT SPARE COVERAGE:

The following volume groups are not protected:

Total hot spare drives: 2

Standby: 2

In use: 0

DETAILS:

Drive at Tray 0, Slot 1 (HotSpare)

Available: 0

Drive path redundancy: OK

Status: Optimal

Raw capacity: 136 GB

Usable capacity: 136 GB

Product ID: ST314680FSUN146G

Firmware version: 0307

Serial number: 3HY90HWJ00007510RKKV

Vendor: SEAGATE

Date of manufacture: Sat Sep 18 00:00:00 2004

World-wide name: 20:00:00:11:C6:0D:BA:3E

Drive type: Fiber

Speed: 10033 RPM

Associated volume group: None

Available: No

Vendor: SEAGATE
Date of manufacture: Sat Sep 18 00:00:00 2004
World-wide name: 20:00:00:11:C6:0D:CA:12
Drive type: Fiber
Speed: 10033 RPM
Associated volume group: 3
Available: No

Drive at Tray 11, Slot 1
Drive path redundancy: OK
Status: Optimal
Raw capacity: 136 GB
Usable capacity: 136 GB
Product ID: ST314680FSUN146G
Firmware version: 0307
Serial number: 3HY90JEW00007511BDPL
Vendor: SEAGATE
Date of manufacture: Sat Sep 18 00:00:00 2004
World-wide name: 20:00:00:11:C6:0D:C8:8B
Drive type: Fiber
Speed: 10033 RPM
Associated volume group: 3
Available: No

Drive Tray 1 Overall Component Information
Tray technology: Fibre Channel
Minihub datarate mismatch: 0
Part number: PN 54062390150
Serial number: SN 0447AWF011
Vendor: VN SUN
Date of manufacture: Mon Nov 1 00:00:00 2004
Tray path redundancy: OK
Tray ID: 11

Tray ID Conflict: 0
Tray ID Mismatch: 0
Tray ESM Version Mismatch: 0
Fan canister: Optimal
Fan canister: Optimal
Power supply canister
Status: Optimal
Part number: PN 30017080150
Serial number: SN A6847502330F
Vendor: VN SUN
Date of manufacture: Sun Aug 1 00:00:00 2004

Power supply canister
Status: Optimal
Part number: PN 30017080150
Serial number: SN A6847502330F
Vendor: VN SUN
Date of manufacture: Sun Aug 1 00:00:00 2004

Power supply canister
Status: Optimal
Part number: PN 30017080150
Serial number: SN A68475023N0F
Vendor: VN SUN
Date of manufacture: Sun Aug 1 00:00:00 2004

Temperature: Optimal

Temperature: Optimal

Esm card

Status: Optimal
Firmware version: 9631
Maximum data rate: 2 Gbps
Current data rate: 2 Gbps
Location: A (left canister)
Working channel: -1
Product ID: CSM100_E_FC_S
Part number: PN 37532180150
Serial number: SN 1T44462572
Vendor: SUN
FRU type: FT SBOD_CEM
Date of manufacture: Fri Oct 1 00:00:00 2004

Esm card

Status: Optimal
Firmware version: 9631
Maximum data rate: 2 Gbps
Current data rate: 2 Gbps
Location: B (right canister)
Working channel: -1

▼ Pour capturer la sortie de la commande `raidctl` depuis un client Windows

1. Cliquez sur Démarrer > Exécuter, puis tapez `cmd`. Cliquez sur OK.
2. Cliquez avec le bouton droit de la souris en haut de la fenêtre et choisissez Propriétés.
La boîte de dialogue des propriétés s'affiche.
3. Modifiez la valeur du paramètre Hauteur de l'option Taille mémoire tampon écran en choisissant 3000.
4. Cliquez sur l'onglet Options et désactivez la case à cocher Mode insertion.
5. Utilisez Telnet pour vous connecter au serveur NAS, puis tapez la commande `raidctl` suivante pour recueillir la sortie générée :

```
raidctl get type=lsi target=profile ctrl=0
```
6. Copiez le texte dans un fichier à partir de tout éditeur de texte. Exemple :
 - a. Sélectionnez la sortie générée et appuyez sur Ctrl+C afin de copier les données.
 - b. Ouvrez Wordpad en cliquant sur Démarrer > Programmes > Accessoires > Wordpad.
 - c. Cliquez dans la fenêtre et appuyez sur Ctrl+V afin d'y coller le texte.
 - d. Enregistrez le fichier.
7. Ouvrez le fichier et recherchez-y le numéro de version du microprogramme de chaque composant.

Administration de la console

La console constitue une alternative au logiciel Web Administrator pour gérer Sun StorEdge 5310 NAS Appliance, cluster Sun StorEdge 5310 et système de passerelle Sun StorEdge 5310 Gateway System. Un certain nombre de protocoles, tels que Telnet, Secure Shell (SSH) et RLogin permettent d'établir une connexion avec la console d'administration dès lors que l'application utilisée dispose d'un émulateur de terminal compatible ANSI (American National Standards Institute). Dans cette annexe, le protocole Telnet est utilisé, car il est déjà disponible sous Windows.

Remarque – Vous devrez peut-être modifier les paramètres de sécurité d'accès à distance afin d'utiliser l'interface de ligne de commande. Pour plus d'informations sur l'accès à distance, reportez-vous à la section « [Pour définir la sécurité d'accès à distance](#) », page 178.

Cette annexe aborde les sujets suivants :

- « [Accès à l'administrateur de la console](#) », page 214
- « [Vue d'ensemble des menus de la console](#) », page 215
- « [Affichage du menu principal](#) », page 216
- « [Sauvegarde de la configuration](#) », page 216
- « [Gestion du système](#) », page 217
- « [Gestion des routes](#) », page 223
- « [Services de noms](#) », page 224
- « [Gestion du système de fichiers serveur](#) », page 228
- « [Gestion des partages et quotas](#) », page 232
- « [Sécurité](#) », page 237
- « [Mise en miroir de volumes de fichiers](#) », page 246
- « [Contrôle](#) », page 254
- « [Maintenance du système](#) », page 260

Accès à l'administrateur de la console

Dans cet exemple, le protocole Telnet de Windows est utilisé. Cependant, vous pouvez recourir à un autre protocole dès lors qu'il dispose d'un émulateur de terminal compatible ANSI.

▼ Pour accéder à l'utilitaire Telnet de Windows

1. Cliquez sur le menu Démarrer à partir de la barre des tâches du bureau.
2. Choisissez Exécuter.
3. Dans la fenêtre Exécuter, tapez `cmd` et cliquez sur OK.
4. À l'invite de la commande, saisissez `telnet adresse-ip`, où *adresse-ip* désigne l'adresse IP du serveur. Appuyez ensuite sur Entrée.
5. Si l'accès administratif est protégé par un mot de passe, saisissez ce dernier.

Une fois la connexion établie, l'écran Telnet affiche l'invite de ligne de commande suivante :

```
connect to (? for list) ? [menu]
```

Vous pouvez maintenant atteindre directement le menu principal ou accéder à l'interface de ligne de commande (la CLI) afin d'exécuter des commandes particulières.

Pour accéder au menu principal, appuyez sur la touche Entrée.

▼ Pour accéder à l'interface de ligne de commande

1. À l'invite de connexion, tapez `admin` et appuyez sur Entrée.
 2. Saisissez ensuite le mot de passe de l'administrateur et appuyez sur Entrée.
- L'invite de ligne de commande s'affiche. Vous pouvez taper une commande ou sélectionner menu pour accéder au menu principal de la console.



Attention – Exécutez les commandes avec précaution afin d'éviter tout résultat inattendu.

Pour revenir à la ligne de commande, appuyez sur Échap à partir du menu principal.

Vue d'ensemble des menus de la console

Cette section offre une description des divers éléments qui composent l'écran Telnet en vue du paramétrage et de la maintenance du système.

Directives élémentaires

Voici quelques directives élémentaires à propos de l'utilisation de la console :

- Pour sélectionner un menu, appuyez sur le chiffre ou la lettre associé(e) à l'élément. Par exemple, appuyez sur **1** pour sélectionner l'écran 1. Activity Monitor (1. Moniteur d'activité).
- La zone située au bas de chaque écran indique les tâches que vous pouvez effectuer ainsi que la lettre à sélectionner pour effectuer l'action désirée.
- Utilisez la barre d'espace pour faire défiler une liste.

Description des touches

Les touches permettant de modifier les champs d'écran sont répertoriées dans le tableau suivant.

TABLEAU A-1 Touches d'écran actives

Touches	Description
Ret.Arr, Suppr, Ctrl+H	Supprime le caractère précédent.
Ctrl+U	Supprime entièrement le champ.
Entrée, Ctrl+M, Ctrl+J, Ctrl+I, Tab	L'entrée est complète et le curseur passe au champ suivant.
Échap	Quitte l'écran sans qu'aucune modification ne soit apportée.

Si vous ne voulez pas modifier la valeur d'un champ, appuyez sur Entrée. Le curseur passe au champ suivant sans modifier les données.

Affichage du menu principal

Le menu principal se compose des sections suivantes :

- **Operations (Opérations)** : appuyez sur un chiffre pour exécuter l'opération serveur correspondante.
- **Configurations** : appuyez sur une lettre pour exécuter la commande de configuration du serveur correspondante.
- **Access Control (Contrôle d'accès)** : appuyez sur une lettre pour paramétrer l'accès aux options de menu correspondantes.
- **Extensions** : appuyez sur une lettre pour sélectionner l'extension correspondante. Utilisez la barre d'espace pour faire défiler la liste d'extensions.

▼ Pour utiliser le menu

1. Choisissez une option de menu en appuyant sur la lettre ou le chiffre correspondant(e).
2. Appuyez sur la barre d'espace pour afficher d'autres options sous les listes Extension.

Sauvegarde de la configuration

Une fois le système configuré, il est conseillé de procéder à la sauvegarde de la configuration.



Attention – Le système stocke des copies redondantes des informations de configuration, mais vous devez en faire une copie de sauvegarde en cas de panne du système.

▼ Pour sauvegarder les informations de configuration

Dans une configuration en cluster, effectuez la procédure suivante sur un seul serveur. La configuration est ensuite automatiquement synchronisée entre les serveurs. Il est donc inutile de créer une copie de sauvegarde de la configuration sur chaque serveur.

1. Suivez les instructions de la section « [Pour accéder à l'interface de ligne de commande](#) », page 214.



Attention – Exécutez les commandes avec précaution afin d'éviter tout résultat inattendu.

2. Sur la ligne de commande, saisissez `load unixtools`.
3. Tapez `cp r v /dvol/etc chemin-de-sauvegarde`, où *chemin-de-sauvegarde* désigne le chemin d'accès complet (nom du volume inclus) à l'emplacement du répertoire de sauvegarde des fichiers de configuration. Ce répertoire doit déjà exister et être vide.

Ce processus copie l'ensemble des informations de configuration qui figurent dans le répertoire `/dvol/etc` vers l'emplacement défini.

Gestion du système

Vous pouvez utiliser l'administrateur de la console en vue d'effectuer des tâches de gestion du système.

▼ Pour configurer le protocole TCP/IP

1. Dans le menu Configuration, sélectionnez Host Name & Network (Nom de l'hôte et réseau).
2. Sélectionnez 1. Edit fields (Modifier les champs).
3. Saisissez le nom d'hôte du serveur, puis appuyez sur Entrée.
4. Indiquez l'unité de transfert maximum MTU (Maximum Transfer Unit) ou appuyez sur Entrée pour conserver la valeur par défaut.

5. Indiquez l'adresse IP du serveur, puis appuyez sur Entrée.
6. Indiquez le masque de sous-réseau IP du réseau, puis appuyez sur Entrée.
7. Indiquez l'IP de diffusion du réseau, puis appuyez sur Entrée.
8. Sélectionnez 1. Setup (Configuration) pour configurer les adresses IP alias, puis appuyez sur Entrée.
9. Recommencez la procédure de l'étape 3 à l'étape 8 pour chacun des ports. Appuyez sur Entrée pour continuer.

Remarque – Utilisez la barre d'espace pour faire défiler la liste des ports.

10. Indiquez l'adresse de passerelle, puis appuyez sur Entrée.
11. Sélectionnez 7. Save changes (Enregistrer les modifications).

▼ Pour modifier le mot de passe administrateur

1. Dans le menu Access Control (Contrôle d'accès), sélectionnez Admin Access (Accès administrateur).
2. Sélectionnez Y. Yes (Oui) pour activer la protection par mot de passe ou N. No (Non) pour la désactiver.

Remarque – Il est recommandé de toujours protéger par mot de passe le système.

3. Si vous avez sélectionné Yes (Oui), suivez les étapes ci-après en réponse aux invites :
 - a. Saisissez deux fois le mot de passe d'accès administrateur, la seconde fois à titre de confirmation.
 - b. Sélectionnez 7. Save changes (Enregistrer les modifications) pour activer le nouveau mot de passe.

Contrôle de l'heure et de la date

Utilisez l'option de menu **Timezone, Time, Date (Fuseau horaire, heure et date)** pour modifier le fuseau horaire, l'heure et la date définis sur le système. L'horloge en temps réel de la carte mère assure le suivi de l'heure locale.

Remarque – Lorsque vous réglez l'heure et la date pour la première fois sur le système, vous initialisez également l'horloge sécurisée du système. Cette horloge est utilisée par le logiciel de gestion des licences et par le logiciel Compliance Archiving Software pour contrôler les opérations liées à l'heure.



Attention – Une fois l'horloge sécurisée définie, elle ne peut pas être réinitialisée. Par conséquent, vous devez impérativement définir l'heure et la date avec précision lorsque vous configurez le système.

▼ Pour régler le fuseau horaire, l'heure et la date

1. Dans le menu **Configuration**, sélectionnez **Timezone, Time, Date (Fuseau horaire, heure et date)**.
2. Sélectionnez le fuseau horaire approprié, puis appuyez sur **Entrée**.
3. Spécifiez **Y (O)** ou **N (N)** pour activer ou non l'heure d'été.
4. Indiquez la nouvelle date, puis appuyez sur **Entrée**.
Le format utilisé est AAAAMMJJ, où AAAA correspond à l'année, MM au mois et JJ au jour. Par exemple, **20051001** correspond au 1er octobre 2005.
5. Indiquez l'heure actuelle, puis appuyez sur **Entrée**.
Le système affiche l'heure au format 24 heures.
6. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

Définition de la synchronisation horaire

Vous pouvez configurer le système de manière à synchroniser son horloge avec celle d'un serveur NTP (Network Time Protocol) ou RDATE.

NTP (Network Time Protocol, protocole NTP) est un protocole Internet qui permet de synchroniser les horloges de vos machines sur une horloge de référence. Les configurations NTP classiques utilisent plusieurs serveurs redondants et divers chemins d'accès réseau afin d'allier précision et fiabilité.

Les serveurs RDATE sont généralement utilisés avec les systèmes UNIX ; ils vous permettent de synchroniser l'horloge du serveur du système avec celle du serveur RDATE.

▼ Pour paramétrer le protocole NTP

1. Dans le menu **Extensions**, sélectionnez **NTP Configuration (Configuration NTP)**.
2. Sélectionnez **1. Edit fields (Modifier les champs)** pour configurer les paramètres NTP.
3. Sélectionnez **Y. Yes (Oui)** pour activer le protocole NTP.

4. Suivez les étapes ci-après pour chacun des serveurs NTP à configurer.

Vous avez la possibilité de configurer jusqu'à deux serveurs NTP.

- a. Sélectionnez **Y. Yes (Oui)** pour activer le premier serveur NTP.
- b. Indiquez le nom ou l'adresse IP du serveur NTP interrogé par Sun StorEdge 5310 NAS Appliance à propos de l'heure, puis appuyez sur **Entrée**.
- c. Choisissez le type d'authentification à utiliser : **0. none (Aucun)** ou **1. symmetric-key (Clé symétrique)**.

La prise en charge de l'authentification par clé symétrique permet à Sun StorEdge 5310 NAS Appliance de vérifier, à l'aide d'une clé et d'un ID de clé, que le serveur NTP est connu et digne de confiance. Les serveurs NTP et Sun StorEdge 5310 NAS Appliance doivent décider de la clé et de l'identificateur de clé à utiliser pour l'authentification des messages.

- d. Si vous avez sélectionné le type d'authentification **Symmetric Key (Clé symétrique)** à l'étape précédente, vous devez indiquer l'identificateur de clé associé à la clé privée dans le fichier de clés à utiliser avec ce serveur NTP.

La plage autorisée est comprise entre 1 et 65534.

5. Dans le champ **Min. Polling Interval (Intervalle d'interrogation minimal)**, entrez la fréquence d'interrogation minimale pour les messages NTP.

Cette valeur, mise à la puissance deux, correspond au nombre minimum de secondes de la fréquence d'interrogation. Par exemple, si vous entrez la valeur 4, l'intervalle d'interrogation est de 16 secondes. La plage autorisée pour ce champ est comprise entre 4 et 17.

6. Dans le champ **Max. Polling Interval (Intervalle d'interrogation maximal)**, entrez la fréquence d'interrogation maximale pour les messages NTP.

Cette valeur, mise à la puissance deux, correspond au nombre maximum de secondes de la fréquence d'interrogation. Par exemple, si vous entrez la valeur 4, l'intervalle d'interrogation est de 16 secondes. La plage autorisée pour ce champ est comprise entre 4 et 17 et sa valeur doit être supérieure à l'intervalle d'interrogation minimal.

7. Dans le champ **Broadcast Client Enabled (Client de diffusion activé)**, sélectionnez **Y. Yes (Oui)** pour que le serveur Sun StorEdge 5310 NAS Appliance réponde aux messages de diffusion reçus sur n'importe quelle interface.
8. Dans le champ **Require Server authentication (Exiger l'authentification du serveur)**, sélectionnez **Y. Yes (Oui)** pour exiger une authentification pour les serveurs utilisant le client de diffusion.
Les serveurs NTP ne faisant pas appel à l'authentification ne sont pas acceptés.
9. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

▼ Pour paramétrer le serveur RDATE et une tolérance

1. Dans le menu **Extensions**, sélectionnez **RDATE time update (Mise à jour de l'heure RDATE)**.
2. Sélectionnez **1. Edit fields (Modifier les champs)**.
3. Entrez le nom ou l'adresse IP du serveur RDATE, puis appuyez sur **Entrée**.
4. Indiquez la tolérance et appuyez sur **Entrée**.
Si l'horloge du système Sun StorEdge 5310 NAS Appliance et celle du serveur RDATE ont un écart inférieur au nombre de secondes défini, l'horloge du système Sun StorEdge 5310 NAS Appliance est synchronisée sur celle du serveur RDATE. La vérification a lieu tous les jours à 23:45.
5. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

Paramétrage de la protection antivirus

Si un moteur d'analyse antivirus est exécuté sur le réseau, vous pouvez configurer une protection antivirus sur le système. Pour plus de détails sur la protection antivirus, reportez-vous à la section « [Utilisation d'un logiciel antivirus](#) », page 72.

▼ Pour activer la protection antivirus

1. Dans le menu **Extensions**, sélectionnez **Anti-Virus Configuration (Configuration de la protection antivirus)**.
2. Sélectionnez **1. Edit fields (Modifier les champs)**.
3. Dans le champ **AVA Enable (Activer AVA)**, activez la protection antivirus en choisissant **Yes (Oui)**.

4. Dans le champ du mode d'analyse (Scan mode), sélectionnez une option d'analyse.
Pour plus d'informations sur les options de mode d'analyse, reportez-vous à la section « [Pour activer la protection antivirus](#) », page 72.
5. Spécifiez l'adresse TCP/IP du moteur d'analyse à utiliser.
6. Spécifiez le numéro de port TCP/IP sur lequel le serveur ICAP détecte les connexions ; il s'agit généralement du port 1344.
7. Spécifiez le nombre maximum d'opérations d'analyse de fichiers simultanées que le système enverra au moteur d'analyse (généralement 2).
8. Spécifiez les types de fichiers à inclure et exclure de même que les clients, groupes ou partages écartés de l'analyse.

Spécification	Description	Format
File Types Included	(Types de fichiers inclus) Chaque extension de type de fichier à inclure. À ne pas remplir pour inclure tous les types.	Au maximum trois caractères, séparés par des virgules. ? peut être utilisé comme caractère générique.
File Types Excluded	(Types de fichiers exclus) Chaque extension de type de fichier à exclure de l'analyse.	Au maximum trois caractères, séparés par des virgules. ? peut être utilisé comme caractère générique.
Exempt Clients	(Clients exclus) Nom ou adresse IP des clients écartés de l'analyse.	Entrées séparées par des virgules.
Exempt Groups	(Groupes exclus) Nom des différents groupes Windows NT ou Windows Active Directory (pas UNIX) écartés de l'analyse.	Espaces autorisés, entrées séparées par des virgules.
Exempt Shares	(Partages exclus) Nom des différents partages CIFS écartés de l'analyse. Remarque : les partages administratifs (X\$) sont systématiquement exclus de l'analyse.	Entrées séparées par des virgules.

9. Sélectionnez 7. Save changes (Enregistrer les modifications).

Sélection d'une langue

Vous pouvez choisir la langue des services NFS et CIFS.

▼ Pour sélectionner une langue

1. Dans le menu **Extensions**, sélectionnez **Language Selection (Sélection de la langue)**.
2. **Entrez la langue de votre choix, puis appuyez sur Entrée.**

Les langues prises en charge sont affichées dans la partie supérieure de l'écran.

Gestion des routes

La table des routes contient une liste de chemins d'accès réseau utilisés par le système pour acheminer des paquets réseau vers des destinations spécifiques. Chaque entrée de route se compose d'une adresse de destination et d'un chemin d'accès.

La destination est soit un réseau soit un hôte. Le chemin d'accès représente le périphérique de passerelle par l'intermédiaire duquel le paquet atteint sa destination.

▼ Pour gérer les routes statiques sur le réseau local

1. Dans le menu **Configuration**, sélectionnez **Host Name & Network (Nom de l'hôte et réseau)**.
2. Sélectionnez **2. Manage Routes (Gérer les routes)**.
3. Sélectionnez **1. Add route (Ajouter une route)**, puis **1. Edit (Modifier)**.
4. Définissez si le type de route est destiné à un hôte, un réseau, un hôte via une passerelle ou un réseau via une passerelle.
5. Saisissez l'adresse IP de destination, puis appuyez sur **Entrée**.
6. **Entrez le chemin ou l'adresse de passerelle permettant d'établir une connexion entre Sun StorEdge 5310 NAS Appliance et sa destination, puis appuyez sur Entrée.**

Le périphérique de passerelle doit établir une connexion avec le même sous-réseau que celui de Sun StorEdge 5310 NAS Appliance.

7. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

Services de noms

Le nom, les services et les fonctions disponibles dans l'interface de la console diffèrent de ceux disponibles dans l'interface graphique.

Paramétrage du DNS, de `syslogd` et de la journalisation locale

DNS est un système de noms hiérarchique permettant de convertir des noms de domaines en adresses IP. Quant à `syslogd`, il s'agit d'un utilitaire prenant en charge la journalisation à distance. Vous avez la possibilité d'activer la journalisation à distance uniquement si vous disposez d'un système UNIX doté de l'utilitaire `syslogd` sur le réseau pouvant recevoir le journal système de Sun StorEdge 5310 NAS Appliance. Toutes ces fonctions sont configurées à partir du même écran.

Une fois l'utilitaire `syslogd` configuré, tous les messages du journal sont envoyés au serveur sélectionné. Vous pouvez ainsi centraliser, sur un seul serveur, les messages reçus de tous les serveurs.

▼ Pour paramétrer le DNS, le DNS dynamique, `syslogd` et la journalisation locale

1. Dans le menu **Configuration**, sélectionnez **DNS & SYSLOGD**.
2. Sélectionnez **1. Edit fields (Modifier les champs)**.
3. Sélectionnez **Y. Yes (Oui)** pour activer le service de noms de domaine (DNS).
4. Indiquez l'adresse IP du serveur DNS à consulter en premier pour la résolution de noms, puis appuyez sur **Entrée**.
5. Indiquez l'adresse IP du serveur à consulter en deuxième pour la résolution de noms, puis appuyez sur **Entrée**.
Si vous ne possédez pas de serveur DNS secondaire, laissez ce champ vide.
6. Indiquez le nom de domaine du serveur DNS, puis appuyez sur **Entrée**.
7. Indiquez le nombre maximal de tentatives de requêtes DNS que le système peut lancer sur chaque serveur DNS, puis appuyez sur **Entrée**.
8. Indiquez le délai d'attente (en secondes) entre deux tentatives de requête DNS, puis appuyez sur **Entrée**.

9. Pour activer la journalisation à distance, sélectionnez **Y. Yes (Oui)**. Si aucun serveur `syslogd` ne se trouve sur le réseau, sélectionnez **N. No (Non)** et passez à l'étape 15.

Cette fonction permet à Sun StorEdge 5310 NAS Appliance d'envoyer des messages du fichier journal à un serveur `SYSLOGD` distant.

10. Entrez le nom ou l'adresse IP du serveur `syslogd`, puis appuyez sur Entrée.
11. Sélectionnez la fonction appropriée, puis appuyez sur Entrée. La fonction identifie l'application ou le composant système qui génère les messages. Les fonctions disponibles sont les suivantes :
- **Kern (Noyau)** : messages générés par le noyau. Ces messages ne peuvent pas être générés par d'autres processus utilisateur.
 - **User (Utilisateur)** : messages générés par des processus utilisateur aléatoires. Il s'agit de l'identificateur de fonction par défaut lorsque aucune option n'est spécifiée.
 - **Mail (Courrier)** : système de messagerie.
 - **Daemon (Démon)** : démons réseau ou système.
 - **Auth (Autorisation)** : systèmes d'autorisations, tels que la connexion.
 - **Syslog** : messages générés en interne par `syslogd`.
 - **Local0 – Local7** : utilisation locale uniquement.
12. Sélectionnez les types d'événements système à inclure dans les journaux de Sun StorEdge 5310 NAS Appliance :
- a. Sélectionnez le type d'événement approprié.
 - b. Sélectionnez **Y. Yes (Oui)** pour activer la journalisation de ce type d'événement. Les types d'événements sont les suivants :
 - **Emerg** : messages d'urgence. Ces messages ne sont pas envoyés à tous les utilisateurs. Les messages d'urgence prioritaires peuvent être enregistrés dans un fichier distinct pour vérification.
 - **Alert (Alerte)** : messages importants qui nécessitent une attention immédiate. Ces messages sont envoyés à tous les utilisateurs.
 - **Crit** : messages critiques non répertoriés en tant qu'erreurs (problèmes matériels, par exemple). Les messages critiques et les messages possédant une priorité plus haute sont envoyés à la console système.
 - **Err** : messages représentant des conditions d'erreur, telles que l'échec d'écriture sur le disque.
 - **Warning (Avertissement)** : messages concernant des conditions anormales mais néanmoins récupérables.
 - **Notice (Information)** : messages d'information importants. Les messages sans indication de priorité sont regroupés dans ce message de priorité.

- **Info** : messages fournis à titre d'information. Ces messages sont utiles pour l'analyse du système.
 - **Debug (Débogage)** : messages de débogage.
- c. Appuyez sur Entrée pour passer au type d'événement suivant.
13. Sélectionnez **Y. Yes (Oui)** pour activer les mises à jour DNS dynamiques.
Ces mises à jour autorisent les mises à jour dynamiques non sécurisées lors de l'initialisation.
 14. Pour activer les mises à jour sécurisées, entrez le nom de l'utilisateur Windows auprès duquel le client DNS dynamique peut vérifier les mises à jour.
Appuyez ensuite sur Entrée.
Cet utilisateur doit disposer des droits d'administrateur.
 15. Saisissez le mot de passe de l'utilisateur DNS dynamique, puis appuyez sur Entrée.
 16. Entrez **Y. Yes (Oui)** pour activer la journalisation locale.
 17. Saisissez le chemin d'accès au fichier journal (répertoire) et le nom du fichier dans le champ Log File (Fichier journal).
 18. Indiquez le nombre maximal de fichiers d'archive dans le champ Archives (Archives).
La plage autorisée est comprise entre 1 et 9.
 19. Entrez la taille de fichier maximale en kilo-octets pour chaque fichier d'archive dans le champ Size (Taille).
La plage autorisée est comprise entre 1 000 et 999 999 kilo-octets.
 20. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

Paramétrage NIS et NIS+

Remarque – Une fois le service NIS (Network Information Service) configuré, contrôlez régulièrement le serveur pour voir si les fichiers principaux ont été modifiés. Lorsqu'un fichier est modifié, il est copié à partir d'un serveur NIS vers le fichier local. Le champ **Enable (Activer)** vous permet de désactiver les mises à jour NIS sans que les données de configuration ne soient perdues. Par conséquent, celles-ci seront disponibles lors de la prochaine activation.

▼ Pour activer le service NIS ou NIS+

1. Dans le menu Configuration, sélectionnez NIS & NIS+ (NIS et NIS+).
2. Sélectionnez 1. Edit fields (Modifier les champs).
3. Sélectionnez Y. Yes (Oui) pour que Sun StorEdge 5310 NAS Appliance mette régulièrement à jour ses fichiers hôte, utilisateur et groupe à l'aide d'un serveur NIS.
4. Entrez le nom de domaine NIS, puis appuyez sur Entrée.
5. Entrez le nom ou l'adresse IP du serveur NIS, puis appuyez sur Entrée.
6. Sélectionnez Y. Yes (Oui) pour mettre à jour le fichier d'hôtes à l'aide du serveur NIS.
7. Sélectionnez Y. Yes (Oui) pour mettre à jour le fichier d'utilisateurs à l'aide du serveur NIS.
8. Sélectionnez Y. Yes (Oui) pour mettre à jour le fichier de groupes à l'aide du serveur NIS.
9. Sélectionnez Y. Yes (Oui) pour mettre à jour le fichier de groupes réseau à l'aide du serveur NIS.
10. Définissez un délai d'attente (en minutes) entre chaque mise à jour NIS. Cette valeur doit être comprise entre 0 et 9. Appuyez ensuite sur la touche Entrée.
11. Sélectionnez Y. Yes (Oui) afin d'activer le service NIS+ pour Sun StorEdge 5310 NAS Appliance.
12. Entrez l'adresse du serveur de domaine d'accueil NIS+, puis appuyez sur Entrée.
13. Entrez le nom de domaine d'accueil NIS+, puis appuyez sur Entrée.
14. Saisissez le mot de passe d'appel de procédure à distance sécurisé pour le serveur NIS+. Appuyez sur la touche Entrée.
15. Précisez le chemin de recherche, sous la forme d'une liste de domaines séparés par des deux-points. Si vous souhaitez effectuer des recherches uniquement dans le domaine d'accueil et ses parents, n'indiquez pas de chemin. Appuyez sur la touche Entrée.
16. Sélectionnez 7. Save changes (Enregistrer les modifications).

Définition de l'ordre de recherche des services de noms

Vous pouvez choisir le service utilisé en premier pour les fonctions de recherche d'utilisateurs, de groupes et d'hôtes.

▼ Pour définir l'ordre de recherche

1. Dans le menu **Configuration**, sélectionnez **Lookup orders (Ordre de recherche)**.
2. Sélectionnez **1. Edit fields (Modifier les champs)**.
3. Sélectionnez l'ordre de résolution des informations sur les utilisateurs (entre **NIS** et **NIS+**), puis appuyez sur **Entrée**.
4. Sélectionnez l'ordre de résolution des informations sur les groupes (entre **NIS** et **NIS+**), puis appuyez sur **Entrée**.
5. Sélectionnez le premier, le deuxième, le troisième et le dernier service pour la résolution des informations sur les hôtes, puis appuyez sur **Entrée**.
6. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

Gestion du système de fichiers serveur

Dans la console, les volumes SFS (Server File System, système de fichiers serveur) peuvent être gérés de plusieurs façons. Les procédures de gestion les plus courantes sont les suivantes :

- Configuration des lettres d'unités de disque
- Configuration d'un nouveau volume de disque
- Attribution d'un nouveau nom à une partition de disque
- Suppression d'un volume de disque
- Activation et désactivation de quotas et de points de contrôle

Configuration des lettres d'unités

Les lettres d'unités sont automatiquement affectées aux volumes de fichiers disponibles pour le partage via SMB (Server Message Block)/CIFS. Vous pouvez utiliser la console pour définir des mappages de lettre d'unité manuellement, sauf pour le disque C : qui peut uniquement être affecté à `\cvol1`.

Il est possible de ne pas disposer de suffisamment de lettres d'unités, auquel cas le message de journal suivant peut s'afficher :

```
No drive letter available
```

Ce message est généré à titre d'information uniquement. Le système de fichiers sera créé mais, pour lui affecter une lettre d'unité, vous devez réaffecter une lettre déjà utilisée par un autre système de fichiers.

▼ Pour réaffecter manuellement une lettre d'unité à un volume de fichiers

1. Dans le menu **Configuration**, sélectionnez **Drive Letters (Lettres d'unités)**.
2. Saisissez la lettre d'unité à changer, puis appuyez sur **Entrée**.
3. Entrez le nom du volume de fichiers à affecter à la nouvelle lettre d'unité, puis appuyez sur **Entrée**.
Une lettre d'unité ne peut être affectée qu'à un volume de fichiers existant.
4. Appuyez sur **Échap** pour quitter cet écran.

▼ Pour créer un nouveau volume de disque

1. Dans le menu **Configuration**, sélectionnez **Disks & Volumes (Disques et volumes)**.
2. Entrez la lettre de l'unité à configurer.
3. Sélectionnez **1. Edit (Modifier)**.
4. Sélectionnez **1. Create partition (Créer une partition)**.
5. Sélectionnez le type de partition de l'unité ou appuyez sur **Entrée** pour valider le type par défaut, comme `sfs2` (volume principal) ou `sfs2ext` (segment).
6. Indiquez l'étiquette du volume de disque, puis appuyez sur **Entrée**.

Le système vous invite à activer la fonction d'archivage en conformité sur le volume.

7. Si vous disposez d'une licence pour le logiciel Compliance Archiving et que vous souhaitez créer un volume en conformité, appuyez sur Y (Oui).

Remarque – Les configurations système de passerelle Sun StorEdge 5310 Gateway System prennent en charge la mise en conformité avec application consultative exclusivement.



Attention – Une fois que vous avez activé sur un volume l'archivage en conformité avec application obligatoire, il est impossible de supprimer ou de renommer ce volume, de désactiver l'archivage en conformité ou encore de revenir au niveau de l'application consultative.

8. Appuyez sur Entrée pour accepter la taille par défaut, ou entrez la taille du volume de disque en Mo et appuyez sur la touche Entrée.
9. Sélectionnez 7. Proceed with create (Poursuivre la création).
Attendez que les messages Initialization OK (Initialisation OK) et Mount OK (Montage OK) s'affichent, puis appuyez sur Esc (Échap) pour revenir au menu Configure Disk (Configuration du disque).
10. Appuyez sur la touche Échap jusqu'à ce que vous reveniez au menu principal.

▼ Pour renommer une partition

1. Dans le menu Configuration, sélectionnez Disks & Volumes (Disques et volumes).
2. Entrez la lettre de l'unité à renommer.
3. Sélectionnez 1. Edit (Modifier).
4. Sélectionnez 3. Rename (Renommer).
5. Saisissez le nouveau nom de la partition, puis appuyez sur Entrée.

Remarque – Les volumes sur lesquels la fonction de mise en conformité stricte est activée ne peuvent pas être renommés.

▼ Pour ajouter un segment d'extension

Pour ajouter une extension, vous devez d'abord créer une partition `sfs2ext` sur ce même volume.

Remarque – Une fois que le volume d'extension est rattaché au volume de fichiers `sfs`, il ne peut plus être détaché. Cette opération est irréversible. La seule façon de les séparer consiste à supprimer le volume de fichiers `sfs`.

1. Dans le menu **Configuration**, sélectionnez **Disks & Volumes (Disques et volumes)**.
2. Entrez la lettre de l'unité à configurer.

Remarque – Si vous disposez de plus de 26 unités de disque (volumes de disque), appuyez sur la barre d'espace pour les faire défiler.

3. Entrez le chiffre situé en regard de la partition à modifier.
4. Sélectionnez **5. Segments**.
5. Sélectionnez **1. Add an extension segment (Ajout d'un segment d'extension)**.
6. Sélectionnez la lettre située en regard de l'extension de l'unité de disque de votre choix.
7. Sélectionnez **7. Proceed (Continuer)**.

▼ Pour supprimer un volume de disque

Remarque – Les volumes sur lesquels la fonction de mise en conformité avec application obligatoire est activée ne peuvent pas être supprimés.



Attention – Toutes les données d'un volume sont perdues lors de la suppression de ce dernier.

▼ Pour supprimer un volume de disque

1. Dans le menu **Configuration**, sélectionnez **Disks & Volumes (Disques et volumes)**.
2. Entrez la lettre de l'unité à configurer.

Remarque – Si vous disposez de plus de 26 unités de disque (volumes de disque), appuyez sur la barre d'espace pour les faire défiler.

3. Sélectionnez **1. Edit (Modifier)**.
4. Sélectionnez **8. Delete (Supprimer)**.
5. Saisissez le nom du volume de disque, puis appuyez sur **Entrée**.
6. Sélectionnez **7. Proceed with delete (Poursuivre la suppression)**. Patientez jusqu'à l'affichage des messages « **Delete OK** » (**Suppression terminée**) et « **Delpart OK** » (**Suppression de part. terminée**).
7. Appuyez sur **Échap** pour revenir au menu **Configure Disk (Configuration du disque)**.
8. Appuyez plusieurs fois sur **Échap** pour revenir au menu principal.

Gestion des partages et quotas

Vous pouvez gérer les partages et les quotas à l'aide de la console.

Paramétrage des partages SMB/CIFS

Le système CIFS est un service de partage de fichiers Windows qui utilise le protocole SMB. Il permet aux systèmes client Windows d'accéder aux fichiers de Sun StorEdge 5310 NAS Appliance.

▼ Pour paramétrer les partages

1. Dans le menu **Extensions**, sélectionnez **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **A. Domain Configuration (A. Configuration de domaine)**.
3. Dans le champ **Domain (Domaine)**, indiquez un nom de domaine ou de groupe de travail.

4. Le cas échéant, définissez l'étendue du domaine.
5. Entrez une description du serveur Sun StorEdge 5310 NAS Appliance.
6. Le cas échéant, entrez les adresses IP principale et secondaire des serveurs WINS (Windows Internet Naming Service).
7. Définissez le paramètre Keep Alive (Garder actif).
Il s'agit du nombre de secondes au bout duquel le système interrompt les connexions inactives.
8. Assignez un mode de sécurité à partir du niveau de partage sécurisé et de l'UID auto de domaine NT.
9. Si vous choisissez le mode NT Domain Auto UID (ID utilisateur du domaine NT), vous devez saisir le nom et le mot de passe de l'utilisateur administrateur.
10. Sélectionnez 7. Save changes (Enregistrer les modifications).

Si vous avez modifié le mode de sécurité entre Secure Share Level et NT Domain Auto UID, Sun StorEdge 5310 NAS Appliance redémarre.

Paramétrage des partages autohome SMB/CIFS

Les partages autohome sont des partages temporaires créés lorsqu'un utilisateur se connecte au système. Ils sont ensuite supprimés lorsque l'utilisateur se déconnecte.

La fonction de partage autohome requiert deux paramètres de configuration (état et chemin d'accès à autohome), définis comme suit :

- Le paramètre state (état) définit si la fonction est ou non activée. La variable d'environnement `smb.autohome.enable` indique l'état actif de la fonction ; la valeur doit être yes (oui) or no (non).
- Le paramètre de chemin autohome indique le chemin d'accès au répertoire de base des partages temporaires. Il est défini par la variable d'environnement `smb.autohome.path`. Par exemple, si le répertoire personnel d'un utilisateur est `/vol1/personnel/marie`, il est conseillé de définir le chemin d'accès à autohome sur `/vol1/personnel`. Le partage temporaire est nommé `marie`. Le nom du répertoire personnel de l'utilisateur doit être identique au nom de connexion de l'utilisateur.

Si la fonction est désactivée, le paramètre de chemin autohome n'est pas pertinent et ne sera pas validé.

Si la fonction est activée et que le chemin est une chaîne nulle, la configuration n'est pas prise en compte. Dans les autres cas, le chemin est validé. Si le paramètre du chemin autohome ne représente pas un chemin d'accès à un répertoire existant, un

message d'information est consigné dans le journal système. Si, par exemple, le chemin de base spécifié était `/vol1/personnel`, le message consigné dans le journal serait le suivant :

```
SMB autohome: /vol1/personnel: no such directory
```

Le message entré dans le journal est destiné à informer l'administrateur système de la situation, bien que la configuration soit toujours considérée comme valable. Le système fonctionnera normalement, mais les partages autohome ne seront pas créés. Si le chemin d'accès au répertoire est créé par la suite, les partages autohome seront ajoutés et supprimés, selon les besoins, à partir de ce moment-là.

▼ Pour activer les partages autohome

1. Dans le menu **Extensions**, sélectionnez **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **F. Autohome Setup (Paramétrage autohome)**.
3. Sélectionnez **1. Edit fields (Modifier les champs)**.
4. Sélectionnez **Y. Yes (Oui)** pour activer les partages autohome.
5. Précisez le chemin d'accès à autohome.

Ce chemin correspond au répertoire de base des partages. Par exemple, si le répertoire personnel d'un utilisateur est `/utilisateur/personnel/jean`, définissez le paramètre du chemin d'accès à autohome sur `/utilisateur/personnel`. Le partage temporaire est appelé `jean`. Le système considère que les noms du répertoire personnel et de connexion de l'utilisateur sont identiques.

6. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

▼ Pour définir un partage

Une fois le paramétrage SMB/CIFS terminé, vous devez définir les partages SMB/CIFS. Les partages permettent aux utilisateurs Windows d'accéder aux répertoires de Sun StorEdge 5310 NAS Appliance.

1. Dans le menu **Extensions**, sélectionnez **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **E. Shares (Partages)**.
3. Sélectionnez **8. Add a share (Ajout d'un partage)**.
4. Entrez un nom de partage.
5. Indiquez un chemin dans le répertoire, sous la forme *volume/répertoire*.

6. Entrez un commentaire sur le répertoire, si nécessaire.
7. Si votre système est configuré pour le mode de groupe de travail, procédez comme suit :
 - a. Dans le menu déroulant Password Protection (Protection par mot de passe), sélectionnez Yes (Oui) ou No (Non).

Si cette option est activée, vous avez le choix entre une protection en lecture/écriture ou en lecture seule.
 - b. Saisissez l'ID utilisateur, l'ID de groupe et le masque Umask.
8. Sélectionnez 7. Save changes (7. Enregistrer les modifications).

▼ Pour modifier un partage

1. Dans le menu Extensions, sélectionnez CIFS/SMB Configuration (Configuration CIFS/SMB).
2. Sélectionnez E. Shares (Partages).
3. Entrez la lettre correspondant au partage à modifier.
4. Sélectionnez 1. Edit fields (Modifier les champs).
5. Indiquez les nouveaux nom de partage, répertoire, commentaire, mot de passe, ID utilisateur et ID de groupe.
6. Indiquez le conteneur ADS, tel qu'il est décrit à l'étape 7 de la section précédente, « [Pour définir un partage](#) », page 234.
7. Sélectionnez 7. Save changes (Enregistrer les modifications).

▼ Pour supprimer un partage

1. Dans le menu Extensions, sélectionnez CIFS/SMB Configuration (Configuration CIFS/SMB).
2. Sélectionnez E. Shares (Partages).
3. Entrez la lettre correspondant au partage à supprimer.
4. Sélectionnez 8. Delete (Supprimer).

Paramétrage du service ADS

Lorsque vous activez et paramétrez le service ADS (Active Directory Service) dans cet écran, Sun StorEdge 5310 NAS Appliance effectue automatiquement les mises à jour de ce service.

▼ Pour activer le service ADS

1. Dans le menu **Extensions**, sélectionnez **ADS Setup (Paramétrage ADS)**.
2. Sélectionnez **1. Edit fields (Modifier les champs)**.
3. Sélectionnez **Y. Yes (Oui)** pour permettre au client ADS de publier des partages de Sun StorEdge 5310 NAS Appliance sur le service ADS.
4. Indiquez le domaine Windows sur lequel le service ADS est exécuté.
Sun StorEdge 5310 NAS Appliance doit également appartenir à ce domaine.
5. Saisissez le nom d'un utilisateur Windows disposant de droits d'administrateur.
Le client ADS vérifie les mises à jour sécurisées du service ADS avec cet utilisateur.
6. Saisissez le mot de passe de l'utilisateur administrateur de Windows.
7. Dans le champ **User Container (Conteneur utilisateur)**, entrez le chemin d'accès au service ADS de l'administrateur Windows en utilisant la syntaxe du nom distinctif LDAP.
Pour plus d'informations, reportez-vous à la section « [Pour activer ADS](#) », page 89.
8. Entrez le nom du site ADS local dans le champ **Site**.
9. En lettres majuscules, entrez le nom de domaine (realm) Kerberos utilisé pour identifier ADS.
Il s'agit généralement du domaine ADS.
10. Saisissez le nom d'hôte du serveur Kerberos KDC (Key Distribution Center, centre de distribution de clés).
Il s'agit généralement du nom d'hôte du contrôleur de domaine principal dans le domaine ADS. Vous pouvez laisser ce champ vide si le client ADS ou le client DNS dynamique parvient à localiser le serveur KDC à l'aide du service DNS.
11. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

Activation et désactivation de quotas

Les quotas permettent de déterminer le volume d'espace disque utilisé par chaque utilisateur ou groupe. Vous pouvez activer ou désactiver la fonction de suivi des quotas. Cette fonction active et désactive les quotas uniquement. Elle ne définit pas leurs limites.

Remarque – Pendant l'opération d'initialisation des quotas, qui nécessite généralement plusieurs minutes, le volume est verrouillé et indisponible.

▼ Pour activer ou désactiver des quotas

1. Dans le menu **Configuration**, sélectionnez **Disks & Volumes (Disques et volumes)**.
2. Sélectionnez l'unité pour laquelle vous souhaitez activer des quotas.
3. Sélectionnez **1. Edit (Modifier)**.
4. Sélectionnez **4. Quotas on/off (Quotas activés/désactivés)**.
5. Sélectionnez **1. Turn quotas on (Activation des quotas)** ou **8. Turn quotas off (Désactivation des quotas)**.

Sécurité

Vous pouvez paramétrer les groupes et le mappage de références afin de garantir la sécurité.

Configuration de groupes d'utilisateurs

Les exigences liées aux groupes locaux intégrés diffèrent de celles d'un système Windows NT. Pour obtenir une description détaillée des groupes d'utilisateurs, reportez-vous à la section « [Groupes locaux](#) », page 95.

▼ Pour ajouter un groupe

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **B. Local Groups (Groupes locaux)**.
3. Sélectionnez **8. Add a Group (Ajout d'un groupe)** pour ajouter un groupe local.

4. Saisissez le nom du groupe et appuyez sur la touche Entrée.
5. Saisissez une description du groupe, si nécessaire, puis appuyez sur Entrée.
6. Sélectionnez 7. Save changes (Enregistrer les modifications) afin d'enregistrer le nouveau groupe.

▼ Pour ajouter un membre à un groupe

1. À partir du menu Extensions, sélectionnez l'option CIFS/SMB Configuration (Configuration CIFS/SMB).
2. Sélectionnez B. Local Groups (Groupes locaux).
3. Saisissez la lettre du groupe à modifier.
4. Sélectionnez 2. Members (Membres) pour modifier l'appartenance au groupe.
5. Sélectionnez 8. Add (Ajout) pour ajouter un membre.
6. Indiquez les noms de domaine et d'utilisateur au format suivant *domaine\nom-utilisateur*.
Le nom de domaine est le domaine dans lequel le système peut vérifier le nom de l'utilisateur. Par exemple, BENCHLAB\jean identifie le domaine BENCHLAB dans lequel il est possible d'authentifier l'utilisateur jean.
7. Appuyez sur Entrée.
8. Appuyez sur 7. Save changes (Enregistrer les modifications) pour enregistrer le nouveau membre.

▼ Pour supprimer un membre d'un groupe

1. À partir du menu Extensions, sélectionnez l'option CIFS/SMB Configuration (Configuration CIFS/SMB).
2. Sélectionnez B. Local Groups (Groupes locaux).
3. Saisissez la lettre du groupe à modifier.
4. Appuyez sur 2. Members (Membres) pour modifier l'appartenance au groupe.
5. Appuyez sur la lettre correspondant au membre de groupe à supprimer.
6. Appuyez sur la touche Y (O).

Privilèges de groupe

La description des privilèges accordés aux groupes d'utilisateurs est fournie dans la section « [Configuration des privilèges accordés aux groupes locaux](#) », page 96.

▼ Pour modifier les privilèges d'un groupe local

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **B. Local Groups (Groupes locaux)**.
3. Saisissez la lettre du groupe à modifier.
4. Appuyez sur **3. Privileges (Privilèges)** pour modifier les privilèges des membres du groupe.
5. Entrez la lettre du privilège à ajouter ou à supprimer.
6. Appuyez sur **7. Save changes (Enregistrer les modifications)** pour enregistrer les modifications apportées.

Mappages d'utilisateurs et de groupes

Pour obtenir une description détaillée des références d'utilisateurs et de groupes, reportez-vous à la section « [Mappage des références d'utilisateurs et de groupes](#) », page 101.

▼ Pour ajouter un mappage d'utilisateur

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **C. User Mapping (Mappage d'utilisateur)**.
3. Sélectionnez **8. Add a map (Ajout d'un mappage)**.
4. Dans le champ **Account (Compte)**, indiquez le nom et le domaine de l'utilisateur NT à mapper à un utilisateur UNIX.
Suivez le format *domaine\nom-utilisateur*.
5. Dans le champ **Name (Nom)**, indiquez le nom de l'utilisateur UNIX à mapper à l'utilisateur NT.
6. Appuyez sur **7. Save changes (Enregistrer les modifications)**.

▼ Pour modifier un mappage d'utilisateur

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **C. User Mapping (Mappage d'utilisateur)**.
3. Appuyez sur la lettre du mappage à modifier.
4. Appuyez sur **1. Edit Fields (Modifier les champs)**.
5. Entrez vos modifications et appuyez sur la touche **Entrée**.
6. Appuyez sur **7. Save changes (Enregistrer les modifications)**.

▼ Pour supprimer un mappage d'utilisateur

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **C. User Mapping (Mappage d'utilisateur)**.
3. Appuyez sur la lettre du mappage d'utilisateur à supprimer.
4. Appuyez sur **8. Delete (Supprimer)**.

▼ Pour ajouter un mappage de groupe

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **D. Group Mapping (Mappage de groupe)**.
3. Appuyez sur **8. Add a map (Ajout d'un mappage)**.
4. Dans le champ **Account (Compte)**, indiquez le nom et le domaine du groupe NT à mapper à un groupe UNIX. Suivez le format *domaine\nom-utilisateur*.
5. Dans le champ **Name (Nom)**, indiquez le nom du groupe UNIX à mapper au groupe NT.
6. Appuyez sur **7. Save changes (7. Enregistrer les modifications)**.

▼ Pour modifier un mappage de groupe

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **D. Group Mapping (Mappage de groupe)**.
3. Appuyez sur la lettre du mappage de groupe à modifier.
4. Appuyez sur **1. Edit Fields (Modifier les champs)**.
5. Entrez vos modifications et appuyez sur la touche **Entrée**.
6. Appuyez sur **7. Save changes (Enregistrer les modifications)**.

▼ Pour supprimer un mappage de groupe

1. À partir du menu **Extensions**, sélectionnez l'option **CIFS/SMB Configuration (Configuration CIFS/SMB)**.
2. Sélectionnez **D. Group Mapping (Mappage de groupe)**.
3. Appuyez sur la lettre du mappage de groupe à supprimer.
4. Appuyez sur **8. Delete (Supprimer)**.

Mappage et objets sécurisables

Cette section décrit en détail l'interaction existant entre le mappage de références d'utilisateurs ou de groupes et les objets sécurisables au sein du système, notamment les fichiers et les répertoires du système de fichiers.

Les objets résidant sur le système sont classés d'après le domaine à partir duquel les attributs de sécurité du système ont été définis. Les objets créés à l'aide du protocole NFS sont uniquement dotés d'attributs de sécurité UNIX et sont donc classés en tant qu'objets UNIX. Les objets créés à l'aide du protocole SMB sont dotés à la fois d'attributs de sécurité UNIX et Windows ; ils sont classés en tant qu'objets Windows. Bien qu'il soit possible de migrer des objets du domaine A vers le domaine B et vice versa, comme les attributs de sécurité ont été modifiés, la stratégie choisie implique que la migration ne peut se faire que dans un sens. Un objet UNIX devient un objet Windows quand ses attributs de sécurité sont modifiés à l'aide du protocole SMB. Par défaut, il est impossible de modifier les attributs de sécurité d'un objet Windows à l'aide du protocole NFS. Cela s'explique par le fait que la sécurité Windows repose sur des descripteurs de sécurité, lesquels ne peuvent pas toujours être bien représentés à l'aide d'attributs de sécurité UNIX. En autorisant la conversion d'un objet Windows en objet UNIX, vous risqueriez d'affaiblir potentiellement le contrôle d'accès protégeant l'objet.

Deux mécanismes sont destinés à permettre la modification des attributs d'un objet Windows via le protocole NFS : la commande `ch smb` et la variable d'environnement `acl.override.allowed`.

Si cette dernière n'est pas fournie ou qu'elle est définie sur `no` (non), le comportement par défaut sera appliqué. Autrement dit, les attributs d'un objet Windows ne sont pas modifiables via le protocole NFS.

Si la variable d'environnement `acl.override.allowed` est définie sur `yes` (oui), les commandes UNIX, telles que `chown`, `chgrp` et `chmod`, seront autorisées conformément aux règles d'accès UNIX standard. Si les attributs d'un objet Windows sont modifiés à l'aide du protocole NFS, le descripteur de sécurité Windows sera supprimé et l'objet sera converti en objet UNIX.

La commande `ch smb` offre la possibilité de supprimer un descripteur de sécurité Windows spécifique ou la totalité de la base de données de descripteurs de sécurité Windows associée à un volume. Pour appliquer la commande `ch smb` à un fichier ou un répertoire unique, vous devez spécifier le chemin d'accès absolu à cet objet. Sachez que la commande `ch smb` n'effectue pas d'opérations récursives. De ce fait, lorsque vous l'appliquez à un répertoire, elle n'affecte pas les sous-répertoires ou les fichiers sous-jacents. Les exemples suivants illustrent l'utilisation de la commande `ch smb`.

Pour supprimer le descripteur de sécurité et rétablir les autorisations UNIX appliquées au fichier `/vol1/shared/bin/fichier.doc`, exécutez la commande suivante :

```
ch smb /vol1/shared/bin/fichier.doc
```

Pour supprimer tous les descripteurs de sécurité appliqués au volume `/vol1` et rétablir les autorisations UNIX aux fichiers qu'il contient, exécutez la commande suivante :

```
ch smb /vol1
```

La commande `ch smb` affectant la sécurité des fichiers, utilisez-la avec précaution. Lorsqu'un volume est spécifié, la commande `ch smb` émet un avertissement et vous invite à confirmer l'opération avant son exécution.

Aucun mappage n'est effectué quand un utilisateur Windows accède à un objet Windows. De la même manière, aucun mappage n'est effectué quand un utilisateur UNIX accède à un objet UNIX. Ces conditions sont considérées comme étant des conditions d'accès en natif. De plus, comme les objets Windows sont dotés d'attributs de sécurité Windows et UNIX, aucun mappage n'est nécessaire quand un utilisateur UNIX accède à un objet Windows, même s'il s'agit d'un cas d'accès non natif. Cet avantage direct résulte de la décision prise au moment de la conception : choisir l'un des domaines comme mappage par défaut plutôt que de créer un mappage neutre indépendant. Par conséquent, la seule situation requérant l'utilisation d'un mappage est celle dans laquelle un utilisateur Windows accède à un objet UNIX. Dans ce cas, les attributs de sécurité UNIX de l'objet sont mappés au domaine Windows et la stratégie de sécurité Windows est appliquée.

Configuration de la liste d'hôtes

La console vous permet de configurer les informations relatives à un hôte.

▼ Pour ajouter un hôte

1. Dans le menu **Configuration**, sélectionnez **Hosts (Hôtes)**.
2. Saisissez le nouveau nom de l'hôte, puis appuyez sur **Entrée**.
Le système vérifie que ce nom d'hôte n'existe pas.
3. Appuyez sur **Entrée** pour ajouter l'hôte.
4. Entrez la nouvelle adresse IP de l'hôte.
5. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

▼ Pour modifier un hôte existant

1. Dans le menu **Configuration**, sélectionnez **Hosts (Hôtes)**.
2. Saisissez le nom d'hôte à modifier, puis appuyez sur **Entrée**.
3. Sélectionnez **1. Edit (Modifier)**.
4. Entrez la nouvelle adresse IP ou le nouveau nom d'hôte.
5. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

▼ Pour supprimer un hôte

1. Dans le menu **Configuration**, sélectionnez **Hosts (Hôtes)**.
2. Saisissez le nom d'hôte à supprimer, puis appuyez sur **Entrée**.
3. Sélectionnez **8. Delete (Supprimer)**.

Gestion des hôtes de confiance

Utilisez l'option **Trusted Hosts (Hôtes de confiance)** afin de gérer les hôtes bénéficiant d'un accès illimité à toutes les ressources.

▼ Pour définir un hôte de confiance

1. Dans le menu **Access Control (Contrôle d'accès)**, sélectionnez **Trusted Hosts (Hôtes de confiance)**.
2. Saisissez un nom de l'hôte, puis appuyez sur **Entrée**.

Remarque – Pour ajouter un hôte de confiance, l'hôte doit figurer dans la liste d'hôtes ou les services NIS.

Le système vérifie que le nom de l'hôte de confiance n'existe pas encore. Si l'hôte de confiance existe déjà, les informations de l'hôte sont affichées. S'il ne s'agit pas d'un hôte de confiance, le système affiche un avertissement.

3. Sélectionnez **7. Add to list (Ajouter à la liste)**.

Le nouvel hôte de confiance est ajouté et le système affiche le nom en haut de l'écran.

▼ Pour supprimer un hôte de confiance

1. Dans le menu **Access Control (Contrôle d'accès)**, sélectionnez **Trusted Hosts (Hôtes de confiance)**.
2. Saisissez le nom d'hôte de confiance à supprimer, puis appuyez sur **Entrée**.
3. Sélectionnez **8. Delete (Supprimer)**.

L'hôte de confiance est supprimé de la liste.

Gestion de l'accès au volume

Une fois les modifications enregistrées, les montages NFS existants provenant des clients sont mis à jour afin de refléter les nouveaux paramètres.

N'accordez aucun accès, que ce soit en lecture ou en écriture, au volume `cvol`.

Remarque – Les hôtes de confiance disposent automatiquement d'un accès en lecture/écriture aux volumes de fichiers, quels que soient les paramètres d'accès aux volumes concernés.

▼ Pour gérer l'accès au volume pour les clients NFS

1. Dans le menu **Access Control (Contrôle d'accès)**, sélectionnez **Volume Access (Accès au volume)**.
2. Saisissez la lettre correspondant au volume dont vous voulez modifier l'accès.
3. Entrez le chiffre correspondant au type d'accès que vous souhaitez affecter : lecture/écriture, lecture seule ou aucun accès.

Remarque – Les hôtes figurant sur la liste de confiance disposent d'un accès en lecture/écriture, quels que soient les paramètres d'accès aux volumes concernés.

4. Sélectionnez **7. Save changes (Enregistrer les modifications)**.

Verrouillage et déverrouillage de la console

Vous pouvez utiliser la console pour activer ou désactiver la plupart des options du menu principal et empêcher ainsi tout accès non autorisé à la console. Vous devez définir le mot de passe administrateur pour sécuriser la console.

▼ Pour verrouiller la console

1. Dans le menu **Operations (Opérations)**, sélectionnez **Lock Console (Verrouillage de la console)**.
2. Saisissez le mot de passe administrateur.
3. Sélectionnez **Y (Yes) O (Oui)**.

▼ Pour déverrouiller la console

1. Dans le menu principal, sélectionnez **Unlock Console (Déverrouillage de la console)**.
2. Saisissez le mot de passe administrateur.
3. Sélectionnez **Y (Yes) O (Oui)**.

Mise en miroir de volumes de fichiers

Cette section décrit la mise en miroir de volumes de fichiers à partir d'un système Sun StorEdge 5310 NAS Appliance actif vers un système Sun StorEdge 5310 NAS Appliance miroir. Pour plus d'informations sur la mise en miroir, reportez-vous au [Chapitre 9](#).

Remarque – Lors de l'utilisation de la réplication de fichiers sur cluster Sun StorEdge 5310, vous ne devez pas effectuer d'opérations de mise en miroir (telles qu'un changement de rôle) quand le cluster se trouve dans un état endommagé.

Configuration des serveurs actif et miroir

Une fois que les adresses IP principales ont été configurées sur les serveurs actif et miroir et que vous avez défini les rôles des ports assurant la connexion entre les serveurs miroir Sun StorEdge 5310 NAS Appliance, vous pouvez configurer la mise en miroir sur les deux serveurs via l'interface de la console.

▼ Pour configurer un nouveau serveur actif avec un nouveau serveur miroir

1. Dans le menu Configuration, sélectionnez Host Name and Network (Nom de l'hôte et réseau).
2. Sélectionnez 1. Edit Fields (Modifier les champs).
3. Si cela n'est pas encore fait, configurez les ports connectés à un sous-réseau ou réseau local.
Pour plus d'informations sur la configuration TCP/IP à l'aide de la console, reportez-vous à la section « [Pour configurer le protocole TCP/IP](#) », page 217. Pour plus d'informations sur la configuration des ports, reportez-vous au [Chapitre 5](#).
4. Assignez le nom du serveur et l'adresse IP au port utilisé pour connecter les systèmes actif et miroir.
5. Dans le champ Role (Rôle) du port assurant la connexion entre les deux serveurs, sélectionnez Mirror (Miroir).
6. Sélectionnez Save (Enregistrer) afin d'enregistrer les modifications et revenir au menu principal.

7. Le cas échéant, paramétrez les services DNS et NIS/NIS+, ainsi que l'ordre de recherche du service de noms.

Pour plus d'informations sur le paramétrage des services de noms, reportez-vous à la section « [Services de noms](#) », page 224.

8. Ouvrez une fenêtre Telnet pour le système miroir, puis recommencez la procédure de l'étape 1 à l'étape 6.

Les connexions réseau des systèmes actif et miroir sont désormais configurées. Consultez la section suivante pour continuer.

▼ Pour configurer un serveur actif existant avec un nouveau serveur miroir

1. Sur le serveur actif, dans le menu Configuration, sélectionnez Host Names and Network (Noms d'hôtes et réseau).
2. Sélectionnez 1. Edit Fields (Modifier les champs).
3. Assignez le nom du serveur et l'adresse IP au port utilisé pour connecter les systèmes actif et miroir.
4. Dans le champ Role (Rôle) du port assurant la connexion entre les deux serveurs, sélectionnez Mirror (Miroir).
5. Ouvrez une fenêtre Telnet pour le système miroir, puis recommencez la procédure de l'étape 1 à l'étape 4.

6. Dans la fenêtre Telnet du serveur actif, appuyez sur Échap jusqu'à ce que la ligne de commande suivante s'affiche :

```
connect to (? for list) ? [menu]
```

7. Connectez-vous en tant qu'administrateur et saisissez ce qui suit :

```
ping xxx.xxx.xx.xx
```

où xxx.xxx.xx.xx correspond à l'adresse IP du serveur miroir.

8. Recommencez l'étape 7 sur le serveur miroir, en saisissant l'adresse IP du serveur actif.

Les connexions réseau des systèmes actif et miroir sont désormais configurées. Poursuivez en configurant les volumes de fichiers pour la mise en miroir.

Configuration des volumes de fichiers

La mise en miroir s'effectue volume par volume. Vous pouvez appliquer la mise en miroir à une partie ou à la totalité des volumes.

Remarque – Une fois qu'un volume de fichiers est mis en miroir, vous ne pouvez pas le renommer tout en maintenant la connexion de mise en miroir. Vous pouvez seulement mettre en miroir des volumes de fichiers dont la capacité est supérieure ou égale à 1 giga-octet.

▼ Pour paramétrer un volume de fichiers à des fins de mise en miroir

Suivez les étapes ci-après sur le système actif puis sur le système miroir.

1. **Créez un volume de fichiers de petite taille (32 Mo, par exemple) intitulé `SYS` avant de créer tout autre volume.**

Si le système actif comporte déjà des volumes de fichiers, cette étape est facultative.

2. **Dans le menu Configuration, sélectionnez Disks & Volumes (Disques et volumes).**
3. **Sélectionnez l'unité de disque sur laquelle vous souhaitez créer le nouveau volume de fichiers.**
4. **Sélectionnez 3. Create & init partition (3. Création et partition init.). Sélectionnez 1. sfs2.**
5. **Saisissez `SYS` comme nom et 64 comme taille en Mo.**

Cette étape oblige le répertoire `/etc` et les fichiers de configuration de Sun StorEdge 5310 NAS Appliance sous-jacents à résider sur le volume `SYS`.

Ne créez aucun autre volume de fichiers sur le système miroir.

▼ Pour mettre en miroir de volumes de fichiers

1. **À l'aide de Telnet, connectez-vous au système actif et entrez dans le menu principal.**
2. **Dans le menu Operations (Opérations), sélectionnez Licenses (Licences), puis appuyez sur la lettre correspondant à la mise en miroir (Mirroring).**
3. **Saisissez la clé d'activation telle qu'elle vous a été fournie par Sun Microsystems.**
4. **Appuyez sur Échap jusqu'à ce que vous reveniez au menu principal.**
5. **Dans le menu Extensions, sélectionnez Mirrors (Miroir).**

6. Sélectionnez **Add mirror (Ajouter un miroir)** pour définir une nouvelle mise en miroir.

7. Sélectionnez un volume de fichiers à mettre en miroir en appuyant sur la lettre correspondante.

Le volume de fichiers doit disposer d'une capacité supérieure ou égale à 1 Go.

8. Saisissez le nom d'hôte du système miroir.

9. Le cas échéant, saisissez l'adresse IP privée.

Il s'agit de l'adresse IP utilisée pour la connexion de mise en miroir avec le serveur miroir.

10. Saisissez les adresses IP de remplacement dans les champs **Alt IP Address (Adresse IP alternative)**.

11. Si l'accès au serveur miroir nécessite un mot de passe administrateur, saisissez-le dans le champ du mot de passe **Remote admin password (Mot de passe admin distant)**.

12. Indiquez la taille de la réserve du tampon de transactions, puis appuyez sur **Entrée**.

13. Sélectionnez **7. Proceed (Continuer)** afin d'ajouter le volume de fichiers mis en miroir.

Lorsque le volume miroir atteint un état de synchronisation avec le volume actif, il est monté en lecture seule.

Remarque – Aucune activité d'E/S en direction du serveur actif n'est alors possible lors de la synchronisation de mise en miroir initiale.

Pendant et après le processus de création du volume miroir, le système affiche l'écran **Mirror Creation (Création d'un miroir)**.

14. Pour afficher le statut du volume miroir, sélectionnez **A**.

15. Pour modifier les adresses IP de remplacement ou le mot de passe administrateur, sélectionnez **1. Edit (Modifier)**.

Définition des seuils d'avertissement

Lorsque la réserve du tampon de transactions se remplit et déborde, le miroir « se fissure ». Cet écran vous permet de définir les seuils (en pourcentage) auxquels les avertissements sont émis. Les valeurs par défaut sont 70, 80 et 90 pour cent.

▼ Pour définir les seuils d'émission d'avertissements (en pourcentage)

1. **Sur le système actif, sélectionnez Mirrors (Volumes miroir) dans le menu Extensions.**
2. **Sélectionnez 3. Threshold Config. (Config. des seuils).**
3. **Sélectionnez 1. Edit (Modifier) afin de modifier les pourcentages affichés à l'écran.**
4. **Saisissez les valeurs souhaitées.**
5. **Dans le champ Alert Silent Period (Période d'alerte silencieuse), saisissez le nombre d'heures pendant lequel le système doit patienter avant d'émettre à nouveau le même avertissement de dépassement de seuil.**
6. **Sélectionnez 7. Proceed (Continuer).**

Promotion d'un volume de fichiers mis en miroir

En cas de panne du système actif, le système miroir offre une haute disponibilité. Vous devez promouvoir le volume de fichiers en miroir pour le rendre accessible aux utilisateurs réseau. Commencez par séparer la mise en miroir en mettant fin à la connexion entre les deux volumes de fichiers. Procédez ensuite à la promotion du volume et configurez les droits d'accès du volume de fichiers mis en miroir. Une fois le miroir séparé et la promotion du volume de fichiers mis en miroir terminée, les deux volumes de fichiers se retrouvent totalement indépendants l'un de l'autre.

▼ Pour promouvoir un volume de fichiers sur le système miroir

1. **Sur le système miroir, affichez le statut du volume de fichiers en sélectionnant Disks & Volumes (Disques et volumes) dans le menu Configuration.**

Un astérisque (*) placé après le nom du volume indique qu'il s'agit d'un volume de fichiers actuellement mis en miroir.

Remarque – Vous devez seulement séparer le volume de fichiers mis en miroir du système miroir quand le système actif n'est pas disponible. Pour promouvoir un volume de fichiers lorsque le système actif est disponible, séparez le miroir depuis le système actif, pas depuis le système miroir.

2. Dans le menu **Extensions**, sélectionnez **Mirrors (Miroir)**.
3. Sélectionnez la lettre correspondant au volume de fichiers mis en miroir à séparer.
4. Sélectionnez **8. Break (Séparer)**.
5. Lorsque vous êtes invité à confirmer la séparation des volumes, sélectionnez **Y. Yes (O. Oui)** pour continuer.
6. Appuyez sur la touche **Échap** pour revenir au menu **Mirrors (Miroir)** principal.
7. Dans le menu **Extensions**, sélectionnez **Mirrors (Miroir)**.
8. Sélectionnez **1. Promote Volume (Promouvoir le volume)**.
9. Sélectionnez la lettre correspondant au volume de fichiers à promouvoir.
10. Sélectionnez **7. Proceed (Continuer)** afin de promouvoir le volume de fichiers.

Le processus peut prendre plusieurs minutes. Un volume de fichiers mis en miroir ne peut être promu qu'à condition d'avoir atteint au moins une fois l'état **In Sync (Synchronisé)**.

11. Lorsque le système a terminé la promotion du volume de fichiers, appuyez sur **Échap** pour revenir au menu principal.
12. (Facultatif) Pour configurer l'accès au volume de fichiers NFS, sélectionnez **Volume Access (Accès aux volumes)** dans le menu **Access Control (Contrôle d'accès)**.
13. Définissez les droits d'accès au volume de fichiers en sélectionnant la lettre correspondante.
14. Choisissez **Read/write (Lecture/écriture)**, **Read only (Lecture seule)** ou **None (Aucun)**.
15. Sélectionnez **7. Save changes (7. Enregistrer les modifications)** pour continuer.

La promotion du volume est terminée. Pour redéfinir un miroir, reportez-vous à la section suivante, « [Rétablissement d'un miroir](#) », page 252.

Rétablissement d'un miroir

Cette procédure décrit comment rétablir un miroir suite à la panne du serveur actif et la promotion du volume de fichiers sur le serveur miroir. Le volume de fichiers promu est à présent la version la plus à jour et fonctionne indépendamment du volume de fichiers obsolète situé sur le système actif. Pour rétablir le miroir, remettez en miroir le volume de fichiers à jour sur le serveur actif, puis remettez-le en miroir sur le serveur miroir comme au départ.

Remarque – Si vous n'avez pas promu le volume de fichiers mis en miroir, ne suivez pas ces instructions. Le système actif rétablit automatiquement l'état In Sync (Synchronisation) du miroir lorsqu'il est à nouveau en ligne.

Dans les exemples ci-dessous, le Serveur 1 correspond au serveur actif et le Serveur 2 au serveur miroir.

Le rétablissement d'un miroir implique les étapes suivantes :

1. Séparation du miroir sur le Serveur 1
2. Suppression du volume de fichiers obsolète sur le Serveur 1
3. Mise en miroir du volume de fichiers actualisé du Serveur 2 sur le Serveur 1
4. Changement de rôles, avec le Serveur 1 comme serveur actif et le Serveur 2 comme serveur miroir

Lorsque le serveur actif est à nouveau en ligne, il peut tenter de rétablir le miroir. C'est pourquoi vous devez séparer le miroir sur le Serveur 1.

▼ Pour séparer le miroir sur le Serveur 1

1. **Sur le Serveur 1, sélectionnez Mirrors (Volumes miroir) dans le menu Extensions.**
2. **Sélectionnez la lettre correspondant au volume de fichiers mis en miroir.**
3. **Sélectionnez 8. Break (Séparer).**
4. **Sélectionnez Y. Yes (Oui) afin de confirmer la séparation du miroir.**

▼ Pour supprimer le volume de fichiers obsolète du serveur 1

1. Appuyez sur Échap pour revenir au menu principal.
2. Dans le menu Configuration, sélectionnez Disks & Volumes (Disques et volumes).
3. Sélectionnez le chiffre correspondant au volume de fichiers mis en miroir.



Attention – Avant de passer à l'étape suivante, assurez-vous de supprimer le volume de fichiers obsolète sur le Serveur 1. De même, vérifiez que le volume de fichiers à jour situé sur le Serveur 2 a été contrôlé et promu.

4. Sélectionnez 8. Delete (Supprimer).
5. Saisissez le nom de fichier du volume obsolète.
6. Sélectionnez 7. Proceed with delete (Continuer la suppression) pour supprimer le volume de fichiers obsolète.

▼ Pour remettre en miroir le volume de fichiers à jour du serveur 2 sur le serveur 1

1. Sur le Serveur 2, sélectionnez Mirrors (Volumes miroir) dans le menu Extensions.
2. Sélectionnez 8. Add mirror (Ajouter un miroir).
3. Sélectionnez la lettre correspondant au volume de fichiers à mettre en miroir.
4. Saisissez le nom d'hôte privé du Serveur 1.
5. Le cas échéant, saisissez l'adresse IP privée et le mot de passe administrateur.
6. Indiquez la réserve du tampon de transactions.

Pour plus d'informations, reportez-vous à la section « [Pour mettre en miroir de volumes de fichiers](#) », page 248.

7. Sélectionnez 7. Proceed (Continuer).
8. Lors du processus de création du miroir, sélectionnez la lettre correspondant au nouveau volume de fichiers mis en miroir.

Lorsque le miroir atteint l'état In Sync (Synchronisation), une réplique exacte du volume de fichiers existe à la fois sur le Serveur 1 et sur le Serveur 2. Consultez les sections qui suivent pour continuer.

▼ Pour changer les rôles

Remarque – Assurez-vous que les volumes sont entièrement synchronisés avant de changer les rôles.

1. Dans le menu principal, sélectionnez l'option **Mirror (Miroir)** sur le **Serveur 1**.
2. Sélectionnez le volume souhaité en appuyant sur la lettre appropriée.
Par exemple, appuyez sur A pour sélectionner le volume de fichiers `cv011`.
3. Dans le menu **Mirror Status (Statut du miroir)**, sélectionnez l'option **Change Role (Changer de rôle)**.
4. Sélectionnez **Yes (Oui)** pour confirmer.

Contrôle

La console vous permet d'effectuer des tâches de contrôle.

Configuration SNMP

Le menu SNMP vous permet d'envoyer des messages à un contrôleur SNMP (Simple Network Management Protocol) distant et de modifier la chaîne de communauté, les coordonnées et l'emplacement du contrôleur SNMP.

▼ Pour configurer le protocole SNMP

1. Dans le menu **Extensions**, sélectionnez **SNMP Configuration (Configuration SNMP)**.
Le nom de la communauté par défaut est **Public (Public)**, mais vous pouvez utiliser tout autre nom.
2. Sélectionnez **1-5. Edit a Trap Destination (Modifier une destination de déroutement)** pour ajouter, modifier ou supprimer une destination de déroutement, **6. Edit Community (Modifier une communauté)** pour modifier la chaîne de communauté, **7. Edit Contact (Modifier les coordonnées)** pour modifier les informations de contact ou **8. Edit Location (Modifier l'emplacement)** pour modifier l'emplacement du contrôleur SNMP distant.
3. Sélectionnez **Y. Yes (O. Oui)** pour enregistrer les modifications effectuées.

Configuration de la notification par e-mail

Lorsqu'une erreur se produit sur le système, Sun StorEdge 5310 NAS Appliance envoie un e-mail aux destinataires concernés.

Remarque – Le DNS doit être configuré pour que la notification par e-mail fonctionne correctement.

▼ Pour configurer la notification par e-mail

1. Dans le menu **Extensions**, sélectionnez **EMAIL Configuration (Configuration E-MAIL)**.
2. Sélectionnez **1. Edit fields (Modifier les champs)**.
3. Saisissez les informations requises pour chaque champ. Appuyez sur la touche **Entrée** pour passer d'un champ à l'autre.
 - **SMTP Server (Serveur SMTP)** : serveur de messagerie vers lequel tous les e-mails sont dirigés. Le fichier d'hôte ou le serveur DOS doivent comporter le nom du serveur.

Remarque – Vous pouvez utiliser l'adresse IP ou le nom. Le nom doit être résolu par votre serveur DNS.

- **Recipient 1-4 (Destinataire 1-4)** : adresses e-mail des quatre personnes automatiquement informées en cas de problème.
 - **Notification Level (Niveau de notification)** : niveau qu'un problème doit atteindre avant qu'une notification ne soit envoyée par e-mail aux destinataires. Sélectionnez l'un des niveaux suivants :
 - **Errors (Erreurs)** : notifications concernant les erreurs uniquement.
 - **Errors and warnings (Erreurs et avertissements)** : notifications concernant les erreurs et les avertissements de basse priorité.
 - **None (Aucune)** : aucune notification n'est envoyée.
4. Sélectionnez **7. Save changes (Enregistrer les modifications)** pour enregistrer la configuration actuelle.
 5. Appuyez sur **Échap** pour revenir au menu principal.

Affichage des informations sur le système

Vous pouvez visualiser les informations sur le système à partir de la console.

▼ Pour afficher le statut du serveur

1. Dans le menu **Operations (Opérations)**, sélectionnez **Activity Monitor (Moniteur d'activité)**.

L'écran Activity Monitor (Moniteur d'activité) répertorie les informations suivantes :

- **Volume** : indique les 22 premiers volumes de fichiers.
- **Use% (% util.)** : indique la quantité d'espace utilisée sur le volume.
- **Reqs (Requêtes)** : indique le nombre de requêtes traitées pour le volume au cours des 10 dernières secondes.
- **Device (Périphérique)** : indique le nom du périphérique.
- **Load (Charge)** : indique le pourcentage de la puissance de calcul de l'unité.
- **Peak (Pointe)** : indique la plus grande utilisation par seconde au cours des 10 dernières minutes.
- **Client (Client)** : indique le nom ou l'adresse de l'utilisateur.
- **Reqs (Requêtes)** : indique le nombre de requêtes traitées pour le volume au cours des 10 dernières secondes.

2. Appuyez sur **Échap** pour revenir au menu principal.

▼ Pour afficher le journal système

- Dans le menu **Operations (Opérations)**, sélectionnez **Show Log (Afficher le journal)**.

Le journal affiche deux types d'entrées :

- **System Startup Log Entries (Entrées de journal au démarrage du système)** : indique les configurations de périphérique, les volumes ainsi que d'autres informations utiles.
- **Normal Operation Log Entries (Entrées de journal des opérations standard)** : indique les erreurs de périphérique, les violations de sécurité ainsi que d'autres informations relatives à l'état du routage. Le numéro de version et le numéro de série du logiciel sont répertoriés en dernier.

▼ Pour afficher une liaison de ports

1. Dans le menu Configuration, sélectionnez Host Name & Network (Nom de l'hôte et réseau).
2. Appuyez sur la barre d'espace pour passer à la page suivante.
La colonne bond1 affiche la première liaison de ports. Les informations d'entrée/sortie de cette colonne correspondent à la somme des informations d'entrée/sortie des deux ports reliés.

▼ Pour afficher l'analyse des points de contrôle

1. Dans le menu Configuration, sélectionnez Disks & Volumes (Disques et volumes).
2. Saisissez la lettre correspondant à l'unité de disque à configurer.
3. Sélectionnez Change/Delete (Modifier/supprimer) *nom-volume*.
4. Sélectionnez 6. Checkpoints (Points de contrôle).
5. Sélectionnez 3. Analysis (Analyse). Faites défiler le contenu de l'analyse à l'aide de la barre d'espace.
6. Sélectionnez 0. End Analysis (Fin de l'analyse) pour quitter cet écran.

▼ Pour afficher le statut d'un volume de fichiers mis en miroir

1. Sur le système actif, sélectionnez Mirrors (Volumes miroir) dans le menu Extensions.
2. Sélectionnez le volume de fichiers mis en miroir.

L'écran du statut se divise en trois sections :

- La première ligne présente les informations sur l'état du miroir : nom du volume de fichiers, état du miroir, indicateur de progression, message sur le statut, etc. Il existe dix états de miroir :
 - ERR : une erreur s'est produite.
 - NEW : un nouveau miroir est en cours de création.
 - INIT : le tampon du miroir est en cours d'initialisation.
 - MKPT : des partitions de disque sont en cours de création sur le système miroir.
 - RDY : le système est prêt et attend que l'autre système le soit aussi.
 - DOWN : la liaison réseau est indisponible.
 - CRK : le miroir est fissuré.
 - RPL : la phase de réplication est en cours.
 - OOS : le miroir n'est plus synchronisé.
 - SYNC : le miroir est synchronisé.

L'indicateur de progression affiche sous forme de pourcentage l'évolution des différentes activités. Un message de statut décrit également sous forme succincte le statut du miroir.

- La seconde ligne affiche la condition de la réserve du tampon de transactions. Les informations affichées ici indiquent le nombre maximum de transactions que le tampon peut contenir, l'ID de la transaction suivante, l'ID de la transaction synchronisée, l'ID de transaction de la tête et un indicateur du pourcentage de synchronisation décrivant l'état de la synchronisation entre les systèmes actif et miroir.

Sur le système actif, les informations disponibles sont les suivantes :

- Le « next xid » (next transaction ID, ID de transaction suivante) identifie la prochaine transaction du système de fichiers.
- Le « sync xid » (sync transaction ID, ID de transaction de synchronisation) identifie la dernière transaction transférée sur le système miroir.
- Le « head xid » (head transaction ID, ID de transaction de tête) identifie la dernière transaction reconnue par le système miroir.
- Lorsque l'indicateur de pourcentage de synchronisation est égal à 100 pour cent, le système miroir dispose d'une copie intégrale du système actif. Si l'indicateur de pourcentage de synchronisation affiche 0 %, cela signifie que le miroir est fissuré et le serveur actif effectue automatiquement une resynchronisation bloc par bloc. Pendant que l'état du miroir est Out Of Sync (Non Synchronisé), le volume miroir est volatile.

Sur le système miroir, les informations disponibles sont les suivantes :

- Le « next xid » (next transaction ID, ID de transaction suivante) identifie la prochaine transaction attendue de la part du système actif.
- Le « sync xid » (sync transaction ID, ID de transaction de synchronisation) identifie la dernière transaction planifiée pour être écrite sur le disque.
- Le « head xid » (head transaction ID, ID de transaction de tête) identifie la dernière transaction reconnue sur le disque.
- Lorsque l'indicateur de pourcentage de synchronisation est égal à 100 pour cent, cela signifie que toutes les transactions miroir ont été écrites sur le disque et que le volume du système miroir est une copie conforme du volume du système actif.

- 3. Pour modifier les adresses IP de remplacement ou le mot de passe administrateur, sélectionnez 1. Edit (Modifier).**
- 4. Modifiez les champs, puis sélectionnez 7. Proceed (Continuer) pour enregistrer vos modifications.**

5. Pour afficher les statistiques réseau sur le volume de fichiers mis en miroir, sélectionnez 2. Statistics (Statistiques).

L'écran affiche les statistiques relatives au système actif, notamment le nombre de transactions vers le volume de fichiers actif (IN, ENTRÉE) et du système actif vers le volume de fichiers mis en miroir (OUT, SORTIE). L'écran présente les transactions individuelles par seconde (t/s) moyennes, minimales et maximales.

Le système affiche la quantité d'espace disponible restant dans la réserve du tampon de transactions (Buffer, Tampon) ainsi que le taux de remplissage. Si ce taux de remplissage est supérieur à zéro, assurez-vous que toutes les liaisons réseau fonctionnent correctement. Cela implique que les transactions provenant du système actif sont plus rapides que les transactions provenant du système miroir, remplissant ainsi le tampon. Lorsque le tampon sature, le miroir « se fissure ».

▼ **Pour afficher les statistiques réseau relatives aux volumes de fichiers mis en miroir**

1. Sur le système actif, sélectionnez Mirrors (Volumes miroir) dans le menu Extensions.

2. Sélectionnez 2. Network Statistics (Statistiques réseau).

L'écran affiche le nombre total de blocs de requêtes de contrôle (RCB, request control block) envoyés, le nombre de RCB envoyés par seconde et la taille moyenne des RCB, de même que leur temps de réponse et leur taux de transfert moyens.

3. Sélectionnez 1. Reset (Réinitialiser) pour réactualiser l'affichage.

Maintenance du système

Plusieurs fonctions de configuration et de maintenance système sont seulement possibles à partir de la console. Ces fonctions sont décrites dans les sections suivantes :

- « Configuration de l'accès FTP », page 260
- « Gestion des contrôleurs RAID », page 262
- « Montage de systèmes de fichiers », page 263

Les sections ci-après décrivent des tâches supplémentaires pouvant être effectuées à partir de l'administrateur de la console comme de Web Administrator :

- « Arrêt du système », page 264
- « Gestion du basculement », page 264
- « Configuration des chemins de LUN », page 266
- « Planification de points de contrôle de fichiers », page 270
- « Configuration d'une sauvegarde », page 270
- « Configuration du logiciel Compliance Archiving Software », page 271
- « Configuration de l'audit du système », page 272

Configuration de l'accès FTP

FTP (File Transfer Protocol, protocole de transfert de fichier) est un protocole Internet permettant de copier des fichiers entre un client et un serveur. Avec le protocole FTP, quand un client demande à se connecter à un serveur, il doit s'identifier au moyen d'un nom d'utilisateur et d'un mot de passe.

Vous pouvez configurer trois types d'utilisateurs :

- **Administrators (Administrateurs)** : ils disposent du nom d'utilisateur `admin` et utilisent le même mot de passe que celui utilisé par les clients de l'interface graphique (IG).

L'administrateur dispose d'un accès root à tous les volumes, répertoires et fichiers du système. Le répertoire personnel de l'administrateur est défini comme `/`.

- **Users (Utilisateurs)** : leurs nom d'utilisateur et mot de passe sont définis dans le fichier local de mots de passe ou sur un serveur de noms NIS ou NIS+ distant.

L'utilisateur dispose d'un accès à tous les répertoires et fichiers du répertoire personnel de l'utilisateur. Le répertoire personnel est défini en même temps que les informations sur le compte de l'utilisateur et est récupéré par le service de noms.

- **Guests (Invités)** : utilisateurs se connectant sous le nom ftp ou son alias anonymous (anonyme). Bien qu'un mot de passe soit demandé, il n'est pas vérifié. Les invités disposent d'un accès à l'ensemble des répertoires et fichiers du répertoire personnel de l'utilisateur ftp.

Remarque – Les invités ne sont pas autorisés à renommer, écraser ou supprimer des fichiers. Ils ne peuvent ni créer ou supprimer des répertoires, ni modifier les autorisations des fichiers ou répertoires existants.

▼ Pour paramétrer les utilisateurs FTP

1. Dans le menu Extensions, sélectionnez FTP Configuration (Configuration FTP).
2. Sélectionnez 1. Edit Fields (Modifier les champs).
3. Sélectionnez Y. Yes (Oui) ou N. No (Non) pour activer ou non le service FTP.
Si le service est activé, le serveur FTP accepte les demandes de connexion entrantes.
4. Dans la zone Allow guest access (Autoriser l'accès aux invités), sélectionnez Yes (Oui) pour permettre aux utilisateurs anonymes d'accéder au serveur FTP ou No (Non) pour en empêcher l'accès.
5. Dans la zone Allow user access (Autoriser l'accès aux utilisateurs), sélectionnez Yes (Oui) pour permettre à tous les utilisateurs d'accéder au serveur FTP ou No (Non) pour en empêcher l'accès.

Cette option ne modifie pas les droits d'accès de l'utilisateur admin ou root.

Remarque – Les noms d'utilisateur et les mots de passe doivent être spécifiés dans le fichier local de mots de passe ou sur un serveur de noms NIS ou NIS+ distant.

6. Dans la zone Allow admin access (Autoriser l'accès aux administrateurs), sélectionnez (Oui) pour permettre un accès root à tous les utilisateurs disposant du mot de passe d'administrateur de Sun StorEdge 5310 NAS Appliance (à utiliser avec parcimonie) ou No (Non) pour désactiver cet accès.

Remarque – Un utilisateur root est un utilisateur possédant un UID (ID utilisateur) égal à 0 et l'admin utilisateur Sun StorEdge 5310 NAS Appliance spécial.

7. Dans la zone Enable logging (Activation de la journalisation); sélectionnez Yes (Oui) pour activer la journalisation ou No (Non) pour la désactiver.
8. Si vous activez la journalisation, indiquez le nom du fichier journal dans la zone prévue à cet effet.
9. Sélectionnez 7. Save changes (Enregistrer les modifications).

Gestion des contrôleurs RAID

La commande `raidctl` vous permet de gérer les contrôleurs RAID depuis la CLI.

Pour toutes les commandes `raidctl`, suivez les instructions de la section « [Pour accéder à l'interface de ligne de commande](#) », page 214.



Attention – Faites très attention lorsque vous utilisez des commandes afin d'éviter tout résultat inattendu.

▼ Pour obtenir de l'aide sur les commandes sous-jacentes

1. Sur la ligne de commande, saisissez `raidctl help`.

▼ Pour contrôler les DEL

- Pour que toutes DEL d'un plateau clignotent, tapez cette commande :
`raidctl locate type=lsi target=tray ctrl=0..n tray=0..n`
- Pour que toutes DEL d'une unité spécifique clignotent, tapez cette commande :
`raidctl locate type=lsi target=drive ctrl=0..n tray=0..n slot=1..n`
- Pour arrêter le clignotement des DEL d'un contrôleur spécifique, tapez cette commande :
`raidctl locate type=lsi action=stop ctrl=0..n`

▼ Pour obtenir les événements et les informations de configuration

- Pour obtenir tous les événements relatifs à un contrôleur donné, tapez cette commande :

```
raidctl get type=lsi target=events ctrl=0..n
```

Le journal contenant tous les événements sera consigné dans le fichier `/cvol1/log/2882ae.log`. Si ce fichier existe, un message vous propose trois options : écraser le fichier existant, indiquer un nouveau nom de fichier ou annuler l'opération.

- Pour obtenir les événements critiques relatifs à un contrôleur donné, tapez cette commande :

```
raidctl get type=lsi target=events ctrl=0..n etype=critical
```

Le journal contenant les événements critiques sera consigné dans le fichier `/cvo1/log/2882ce.log`. Si ce fichier existe, un message vous propose trois options : écraser le fichier existant, indiquer un nouveau nom de fichier ou annuler l'opération.

- Pour obtenir les informations de configuration relatives à un contrôleur donné, tapez cette commande :

```
raidctl get type=lsi target=profile ctrl=0..n
```

▼ Pour régler l'heure du contrôleur et l'âge de la batterie

- Pour réinitialiser l'âge de la batterie d'un contrôleur donné, tapez cette commande :

```
raidctl set type=lsi target=battery-age ctrl=0..n
```

- Pour synchroniser l'heure d'un contrôleur avec celle du serveur, tapez cette commande :

```
raidctl set type=lsi target=ctrl_time-age ctrl=0..n
```

▼ Pour télécharger le microprogramme

Exécutez la commande `raidctl download` afin de télécharger le microprogramme.

Remarque – Vous trouverez les procédures détaillées de mise à niveau du microprogramme dans le [Chapitre 11](#).

Montage de systèmes de fichiers

Après plusieurs redémarrages continus, un ou plusieurs systèmes de fichiers peuvent avoir été démontés. Pour monter les systèmes de fichiers, tapez la commande suivante :

```
mount -f nom_volume
```

Arrêt du système

Le système Sun StorEdge 5310 NAS Appliance est conçu pour fonctionner en continu, mais si vous devez l'arrêter, faites-le à partir de Web Administrator, de la console ou de l'écran LCD.

▼ Pour arrêter le système

1. Dans le menu **Operations (Opérations)**, sélectionnez **Shutdown (Arrêter)**.
2. Sélectionnez l'option souhaitée en appuyant sur la lettre appropriée.
 - **R. Reboot (Redémarrer)** : tapez la lettre R pour redémarrer le système.
 - **H. Halt (Arrêter)** : tapez la lettre H pour arrêter le système.
 - **P. Boot Previous Version 4.x.xx.xxx (Démarrer la version précédente 4.x.xx.xxx)** : tapez P pour redémarrer le système à partir de la version précédente du SE. Cette option est disponible pour les systèmes sur lesquels plusieurs versions du SE sont installées.
 - **ESC (ÉCHAP)** : appuyez sur la touche Échap pour annuler et revenir au menu principal.

Si vous choisissez de redémarrer, d'arrêter ou d'initialiser une version antérieure du SE, le serveur redémarre ou s'arrête uniquement lorsque l'opération d'écriture décalée est terminée.

Gestion du basculement

Un basculement se produit lorsque l'un des deux contrôleurs RAID ou têtes devient instable et que l'ensemble des LUN qu'il ou elle contrôle doit être déplacé vers le contrôleur ou la tête qui fonctionne. Le menu Failover (Basculement) gère les ressources de disque lorsqu'un erreur RAID récupérable se produit.

▼ Pour configurer le basculement

1. Dans le menu Extensions, sélectionnez Failover/Move LUNs (Basculer/Déplacer les LUN).

Le basculement est configuré par défaut et ne peut pas être désactivé.

2. Si l'option est disponible, sélectionnez 3. Edit Failover (Modifier le basculement).

Remarque – Vous ne pouvez ni activer ni désactiver le basculement sur le système à une tête Sun StorEdge 5310 NAS Appliance.

3. Sélectionnez Y. Yes (Oui) pour activer le basculement de tête ou de contrôleur.
4. Procédez comme suit avec un serveur à deux têtes Sun StorEdge 5310 Cluster ou système de passerelle Sun StorEdge 5310 Gateway System dans une configuration en cluster :
 - a. Sélectionnez Y. Yes (Oui) pour activer le basculement de liaison.

Un basculement de liaison garantit l'activation d'une liaison réseau de substitution lorsqu'une liaison principale tombe en panne.
 - b. Entrez le nombre de secondes à patienter avant le basculement de liaison lorsqu'une liaison réseau devient instable.
 - c. Entrez le nombre de secondes à patienter avant la restauration de liaison lorsque la liaison d'origine est réparée ou reconnectée.
5. À l'attention des utilisateurs d'un système Sun StorEdge 5310 Cluster ou système de passerelle Sun StorEdge 5310 Gateway System configuré en cluster : sélectionnez 2. Modify (Modifier) pour réorganiser les possessions de LUN par adaptateur.

Les valeurs indiquées ici déterminent la configuration utilisée lors du processus de restauration.

- a. Indiquez les LUN associés à chaque adaptateur.
 - b. Séparez les numéros par un espace (par exemple, 0 2 8 10).
 - c. Appuyez sur Entrée.
6. Sélectionnez Y. Yes (Oui) pour enregistrer les modifications effectuées.

▼ Pour restaurer le système et lancer le rétablissement

1. Remplacez ou réparez le composant défaillant et vérifiez qu'il est en ligne.
2. Dans le menu Extensions, sélectionnez Failover/Move LUNs (Basculer/Déplacer les LUN).
3. Sélectionnez 1. Restore (Restaurer).
4. Sélectionnez Y. Yes (Oui) pour lancer le processus de restauration.

Configuration des chemins de LUN

Reportez-vous à la section « Définition de chemins de LUN », page 13 pour plus d'informations sur les chemins de numéros d'unités logiques (LUN) et sur l'utilisation de l'IG dans la définition de ces chemins.

▼ Pour définir ou modifier un chemin de LUN

1. Dans le menu Extensions, appuyez sur la barre d'espace jusqu'à ce que l'option LUN Ownership (Propriété de LUN) s'affiche et sélectionnez-la.

L'écran LUN Ownership (Propriété de LUN) affiche l'ensemble des LUN dont les chemins peuvent être modifiés. Vous pouvez uniquement réaffecter un LUN quand il ne comporte aucun système de fichiers. Sur un système Sun StorEdge 5310 Cluster ou système de passerelle Sun StorEdge 5310 Gateway System configuré en cluster, seule la tête « détenant » un LUN peut réaffecter celui-ci à une autre tête.

Remarque – Sur un système Sun StorEdge 5310 Cluster ou système de passerelle Sun StorEdge 5310 Gateway System configuré en cluster, tous les LUN sont affectés à la même tête (Head 1) lors du démarrage initial du système. Vous devez par conséquent utiliser la tête 1 (Head 1) pour réaffecter certains LUN à la tête 2 (Head 2) en vue d'une répartition équitable.

Remarque – Les LUN auxquels aucun chemin LUN n'est affecté risquent de figurer plusieurs fois dans l'écran LUN Ownership (Propriété de LUN), car leur existence est signalée par plusieurs contrôleurs sur plusieurs chemins. Une fois qu'un chemin est affecté à un LUN, celui-ci ne s'affiche qu'une seule fois sur son chemin actuel.

2. Sélectionnez un chemin de LUN en tapant la lettre à gauche du chemin souhaité.

3. Sélectionnez 1. Edit (Modifier) pour modifier le chemin de LUN.

L'écran Configure LUN Path (Configurer le chemin de LUN) indique l'ensemble des chemins disponibles pour le LUN. Le chemin actuel/actif du LUN est signalé par la mention Active (Actif). Si le chemin principal est défini pour le LUN, il est signalé par la mention PRIMARY (PRINCIPAL).

4. Tapez le numéro du chemin de LUN que vous souhaitez activer et appuyez sur la touche Entrée.

Répartissez équitablement les affectations de LUN entre les deux chemins disponibles. Par exemple, les premier et troisième LUN au chemin 1, et les deuxième et quatrième, au chemin 2.

5. Sélectionnez Y. Yes (Oui) pour enregistrer les modifications effectuées.

Procédures d'annulation de mappage et de reconfiguration de LUN pour le système de passerelle

Suivez la procédure ci-dessous pour annuler le mappage d'un LUN mappé au système de passerelle Sun StorEdge 5310 NAS Gateway System. Vous pouvez également reconfigurer le LUN afin d'accéder aux données par la suite.

Les procédures d'annulation de mappage et de reconfiguration se résument comme suit :

1. Annulation du mappage d'un LUN

- a. Démontez les volumes résidant sur le LUN concerné.
- b. Annulez le mappage du LUN à l'aide du logiciel pour hôtes de gestion SAN.
- c. Réanalysez les LUN du système de passerelle.

2. Reconfiguration d'un LUN

- a. Reconfigurez le LUN à l'aide du logiciel pour hôtes de gestion SAN.
- b. Réanalysez les LUN du système de passerelle.
- c. Remontez les volumes auxquels vous souhaitez accéder.

Les procédures suivantes utilisent la baie Sun StorEdge 6130 comme exemple.

▼ Pour annuler le mappage d'un LUN

1. Démontez le volume sur le système de passerelle :
 - a. Utilisez le protocole Telnet pour vous connecter au système NAS Gateway.
 - b. À la première invite, tapez `admin` pour lancer la CLI.
 - c. Tapez `mount` pour dresser la liste des volumes montés sur le LUN dont vous voulez annuler le mappage. La colonne Origin (Origine) affiche le nom des périphériques bruts contenant les volumes. Prenez note des noms des volumes (indiqués dans la colonne la plus à gauche) à démonter.
 - d. Démontez tous les volumes résidant sur le LUN concerné à l'aide de la commande `umount`. Tapez `mount` et vérifiez qu'aucun des volumes faisant partie du LUN ne sont montés.
2. À partir de l'hôte de gestion Sun StorEdge 6130, annulez le mappage du LUN depuis la baie d'arrière-plan.
 - a. Ouvrez un navigateur et tapez l'adresse <https://nom-hôte:6789>, puis connectez-vous au logiciel de gestion.
 - b. Cliquez sur Sun StorEdge 6130 Configuration Service.
 - c. Cliquez sur la baie contenant le LUN dont vous souhaitez annuler le mappage.
 - d. Cliquez sur le nom du LUN dont vous souhaitez annuler le mappage.
 - e. Cliquez sur le bouton Unmap (Annuler le mappage).
 - f. Cliquez sur OK dans la fenêtre contextuelle afin de confirmer la suppression du LUN.
3. Procédez à une nouvelle analyse sur Gateway System.
 - a. Identifiez le LUN dont vous souhaitez annuler le mappage.
 - b. Utilisez le protocole Telnet pour vous connecter au système NAS Gateway.
 - c. À la première invite, tapez `menu` pour lancer l'interface de menu alphanumérique.
 - d. Tapez la lettre `d` pour afficher le menu Disks and Volumes (Disques et volumes).
 - e. Dans le menu Disks and Volumes (Disques et volumes), tapez `9` pour détecter les nouveaux disques (ou LUN). Patientez jusqu'à la disparition du message « Scanning for new disks, please wait... » (Détection des nouveaux disques en cours... Veuillez patienter.).

▼ Pour reconfigurer un LUN

1. À partir de l'hôte de gestion Sun StorEdge 6130, reconfigurez le mappage de LUN depuis la baie d'arrière-plan.
 - a. Ouvrez un navigateur et tapez l'adresse <https://<nom-hôte>:6789>, puis connectez-vous au logiciel de gestion.
 - b. Cliquez sur Sun StorEdge 6130 Configuration Service.
 - c. Cliquez sur la baie contenant le LUN à reconfigurer.
 - d. Cochez la case en regard du nom du LUN à reconfigurer.
 - e. Appuyez sur le bouton Map (Mapper).
La fenêtre Map Volumes (Mappage de volumes) s'affiche.
 - f. Cliquez sur l'hôte auquel vous souhaitez mapper le LUN.
2. Réanalysez les LUN sur le système de passerelle :
 - a. Utilisez le protocole Telnet pour vous connecter au système Gateway.
 - b. À la première invite, tapez `menu` pour lancer l'interface de menu alphanumérique.
 - c. Tapez la lettre `d` pour afficher le menu Disks and Volumes (Disques et volumes).
 - d. Dans le menu Disks and Volumes (Disques et volumes), tapez `9` pour détecter les nouveaux disques (ou LUN). Patientez jusqu'à la disparition du message « Scanning for new disks, please wait... » (Détection des nouveaux disques en cours... Veuillez patienter.).
3. Remontez le volumes sur le système de passerelle.
 - a. Utilisez le protocole Telnet pour vous connecter au système Gateway.
 - b. À la première invite, tapez `admin` pour lancer la CLI.
 - c. Montez tous les volumes résidant sur la LUN reconfigurée.
 - d. Tapez `mount` afin de vérifier que tous les volumes sont reconfigurés.

Planification de points de contrôle de fichiers

Un point de contrôle est une copie virtuelle, en lecture seule, d'un volume de fichiers principal. Pour plus d'informations sur les points de contrôle, reportez-vous à la section « [Points de contrôle de fichiers](#) », page 181.

▼ Pour planifier des points de contrôle

1. Dans le menu Configuration, sélectionnez **Disks & Volumes (Disques et volumes)**.
2. Sélectionnez l'unité pour laquelle vous souhaitez planifier des points de contrôle.

Remarque – Si vous disposez de plus de 26 unités (volumes de disque), appuyez sur la barre d'espacement pour les faire défiler.

3. Sélectionnez **1. Edit (Modifier)**.
4. Sélectionnez **6. Checkpoints (Points de contrôle)**.
5. Suivez les invites affichées au bas de l'écran et appuyez sur la touche Entrée pour passer d'un champ à l'autre.
6. Une fois les informations relatives au point de contrôle saisies, sélectionnez **7. Save changes (Enregistrer les modifications)**.

Configuration d'une sauvegarde

Pour sauvegarder des volumes système, commencez par ajouter une tâche de sauvegarde, puis planifiez son exécution ou exécutez-la directement. Assurez-vous que le périphérique de sauvegarde est en ligne avant de poursuivre.

Remarque – Les points de contrôle doivent être activés pour que les volumes puissent être sauvegardés par le protocole NDMP (Network Data Management Protocol). Reportez-vous à la section « [Création de points de contrôle de fichiers](#) », page 181.

▼ Pour paramétrer le protocole NDMP

1. Dans le menu **Extensions**, sélectionnez **NDMP Setup (Paramétrage NDMP)**.
2. Sélectionnez le port **NIC (Network Interface Card)** à utiliser pour les transferts de données vers le lecteur de bande de sauvegarde, puis appuyez sur **Entrée**.
Tous les ports disponibles sont indiqués sous ce champ.
3. Sélectionnez un chemin d'accès au volume de rechange (`/vol_ndmp`, par exemple) d'une capacité d'au moins 2 Go afin d'enregistrer les fichiers de données et journaux NDMP.
Il est conseillé d'utiliser un volume de fichiers dédié à ces tâches, distinct des volumes planifiés pour les opérations de sauvegarde.
4. **Enregistrez vos modifications.**

Configuration du logiciel Compliance Archiving Software

Si vous avez acheté et activé l'option **Compliance Archiving Software** (voir la section « [Pour activer une option](#) », page 134), d'autres paramètres sont à votre disposition via la CLI.

Remarque – Les configurations système de passerelle Sun StorEdge 5310 Gateway System prennent en charge la mise en conformité avec application consultative exclusivement.



Attention – Exécutez les commandes avec précaution afin d'éviter tout résultat inattendu.

▼ Pour modifier la période de conservation par défaut

1. Suivez les instructions de la section « [Pour accéder à l'interface de ligne de commande](#) », page 214.
2. Sur la ligne de commande, tapez `fsctl compliance volume drt heure`, où *volume* désigne le nom du volume dont vous souhaitez définir le délai de conservation par défaut et où *heure* désigne la durée de conservation par défaut en secondes.

Pour définir une période de conservation permanente par défaut, utilisez la valeur maximale autorisée, à savoir 2147483647.

Activation de la mise en conformité CIFS

Dans sa configuration initiale, le logiciel Compliance Archiving Software ne prend en charge que les requêtes de conservation de données qui proviennent des clients NFS. Vous pouvez activer l'accès CIFS à cette fonction à partir de l'interface de ligne de commande.



Attention – Exécutez les commandes avec précaution afin d'éviter tout résultat inattendu.

▼ Pour autoriser la fonction d'archivage en conformité sur les clients Windows

1. Suivez les instructions de la section « [Pour accéder à l'interface de ligne de commande](#) », page 214.
2. Sur la ligne de commande, tapez :
`fsctl compliance wte on`

Configuration de l'audit du système

L'audit du système est un service vous permettant de contrôler des événements système particuliers en stockant les enregistrements associés dans des fichiers journaux. Pour plus de détails sur l'audit du système, reportez-vous à la section « [Audit du système](#) », page 161.

▼ Pour configurer l'audit de système

1. Dans le menu Extensions, sélectionnez System Audit Configuration (Configuration d'un audit du système).
2. Sélectionnez 1. Edit fields (1. Modifier les champs).
3. Activez l'audit et indiquez le chemin d'accès au journal d'audit ainsi que la taille de fichier maximum du journal.
4. Sélectionnez 7. Save changes (7. Enregistrer les modifications).

Messages d'erreur de Sun StorEdge 5310 NAS Appliance

Cette annexe contient une description détaillée des différents messages d'erreur système dont l'administrateur peut prendre connaissance de l'une des manières suivantes : e-mail, notification SNMP, écran LCD ou journal système. Le thread de contrôle *SysMon* de Sun StorEdge 5310 NAS Appliance permet de contrôler l'état des périphériques RAID, des onduleurs UPS, des systèmes de fichiers, des unités principales, des sous-systèmes et des variables d'environnement. Les messages d'erreur et de contrôle varient en fonction du modèle et de la configuration.

Les colonnes de tableaux ne comportant aucune entrée ont été supprimées.

À propos de la notification d'erreur SysMon

Le thread de contrôle *SysMon* de Sun StorEdge 5310 NAS Appliance capture des événements liés aux erreurs de sous-système, puis détermine l'action ou les actions les plus appropriées : envoi d'un e-mail, notification au serveur SNMP, affichage de l'erreur sur écran LCD ou écriture d'un message d'erreur dans le journal système. Les notifications par e-mail et les journaux système indiquent l'heure de l'événement.

Messages d'erreur de Sun StorEdge 5310 NAS Appliance

Les sections ci-après décrivent les différents messages d'erreur associés à l'utilisation des périphériques RAID, des onduleurs UPS, des systèmes de fichiers et des modules IPMI de Sun StorEdge 5310 NAS Appliance.

Erreurs liées au sous-système de l'UPS

Reportez-vous au [TABLEAU B-1](#) pour obtenir des informations sur les conditions d'erreur de l'onduleur UPS.

TABLEAU B-1 Messages d'erreur de l'onduleur UPS

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
Power Failure (Coupure de courant)	AC Power Failure (Coupure d'alimentation CA) : AC power failure. (Coupure d'alimentation CA.) System is running on UPS battery. (Le système fonctionne sur la batterie de l'UPS.) Action: (Action :) Restore system power. (Restaurez l'alimentation système.) Severity = Error (Gravité = Erreur)	EnvUpsOn Battery	U20 on battery (U20 Sur batterie)	UPS: (UPS :) AC power failure. (Coupure d'alimentation CA.) System is running on UPS battery. (Le système fonctionne sur la batterie de l'UPS.)
Power Restored (Courant rétabli)	AC power restored: (Alimentation CA rétablie :) : AC power restored. (Alimentation CA rétablie.) System is running on AC power. (Le système fonctionne sur l'alimentation CA.) Severity = Notice (Gravité = Avertissement)	EnvUpsOff Battery	U21 power restored (U21 courant rétabli)	UPS: (UPS :) AC power restored. (Alimentation CA rétablie.)

TABLEAU B-1 Messages d'erreur de l'onduleur UPS (*Suite*)

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
Low Battery (Batterie faible)	UPS battery low: (Batterie de l'UPS faible :) UPS battery is low. (La batterie de l'UPS est faible.) The system will shut down if AC power is not restored soon. (Le système va s'arrêter si le courant n'est pas rapidement rétabli.) Action: (Action :) Restore AC power as soon as possible. (Rétablissez l'alimentation CA au plus vite.) Severity = Critical (Gravité = Critique)	EnvUpsLow Battery	U22 low battery (U22 Batterie faible)	UPS: (UPS :) Low battery condition. (Condition de batterie faible.)
Normal Battery (Batterie normale)	UPS battery recharged: (La batterie de l'UPS est rechargée :) The UPS battery has been recharged. (La batterie de l'UPS a été rechargée.) Severity = Notice (Gravité = Avertissement)	EnvUps Normal Battery	U22 battery normal (U22 Batterie normale)	UPS: (UPS :) Battery recharged to normal condition. (La batterie est rechargée à sa condition normale.)
Replace Battery (Remplacement de la batterie)	Replace UPS Battery: (Remplacement de la batterie de l'UPS :) The UPS battery is faulty. (La batterie de l'UPS est défectueuse.) Action: (Action :) Replace the battery. (Remplacez la batterie.) Severity = Notice (Gravité = Avertissement)	EnvUps Replace Battery	U23 battery fault (U23 Batterie défectueuse)	UPS: (UPS :) Battery requires replacement. (La batterie a besoin d'être remplacée.)
UPS Alarms - Ambient temperature or humidity outside acceptable thresholds (Alarmes UPS : la température ambiante ou l'humidité dépasse le seuil acceptable.)	UPS abnormal temperature/humidity: (Température/humidité anormale pour l'UPS :) Abnormal temperature/humidity detected in the system (Une température/humidité anormale a été détectée dans le système.) Action: (Action :) 1. Check UPS unit installation, OR (Vérifiez l'installation de l'onduleur UPS ou) 2. Contact technical support. (Contactez le support technique.) Severity = Error (Gravité = Erreur)	EnvUps Abnormal	U24 abnormal ambient (U24 Températur e ambiante anormale)	UPS: (UPS :) Abnormal temperature and/or humidity detected. (Une température ou une humidité anormale a été détectée.)

TABLEAU B-1 Messages d'erreur de l'onduleur UPS (*Suite*)

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
Write-back cache is disabled. (Le cache à écriture différée est désactivé.)	<p>Controllor Cache Disabled: (Le cache du contrôleur est désactivé :)</p> <p>Either AC power or UPS is not charged completely. (Coupure de courant CA ou charge incomplète de l'onduleur UPS.)</p> <p>Action: (Action :) 1 - If AC power has failed, restore system power. (En cas de coupure de courant, rétablissez l'alimentation système.) 2 - If after a long time UPS is not charged completely, check UPS. (Si la batterie de l'UPS n'est pas entièrement chargée au bout d'un certain temps, vérifiez-la.)</p> <p>Severity = Warning (Gravité = Avertissement)</p>		Cache Disabled (Mise en cache désactivée)	write-back cache for ctrl x disabled (Le cache à écriture différée ctrl x est désactivé.)
Write-back cache is enabled. (Le cache à écriture différée est activé.)	<p>Controllor Cache Enabled: (Le cache du contrôleur est activé :)</p> <p>System AC power and UPS are reliable again. (L'alimentation du système en courant alternatif est rétablie et la batterie de l'UPS est de nouveau opérationnelle.)</p> <p>Write-back cache is enabled. (Le cache à écriture différée est activé.)</p> <p>Severity = Notice (Gravité = Avertissement)</p>		Cache Enabled (Mise en cache activée)	write-back cache for ctrl n enabled (Le cache à écriture différée ctrl n est activé.)
UPS is shutting down. (UPS en cours d'arrêt.)	<p>UPS shutdown: (Arrêt de l'UPS :)</p> <p>The system is being shut down because there is no AC power and the UPS battery is depleted. (Le système va s'arrêter, car le courant est coupé et la batterie déchargée.)</p> <p>Severity = Critical (Gravité = Critique)</p>			!UPS: (UPS :) Arrêt
UPS Failure (Erreur de l'UPS)	<p>UPS failure: (Erreur de l'UPS :)</p> <p>Communication with the UPS unit has failed. (La connexion à l'onduleur UPS a échoué.)</p> <p>Action: (Action :) 1. Check the serial cable connecting the UPS unit to one of the CPU enclosures, OR (Vérifiez le câble série reliant l'onduleur UPS à l'unité centrale OU)</p> <p>2. Check the UPS unit and replace if necessary. (Vérifiez l'onduleur UPS et remplacez-le si nécessaire.)</p> <p>Severity = Critical (Gravité = Critique)</p>	EnvUpsFail	U25 UPS failure (U25 Erreur de l'UPS)	UPS: (UPS :) Communication failure. (Échec de la connexion)

Erreurs liées au système de fichiers

Des messages d'erreur liés au système de fichiers sont générés lorsque la limite d'utilisation du système de fichiers est dépassée. La limite d'utilisation par défaut est de 95 pour cent.

TABLEAU B-2 Erreurs liées au système de fichiers

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
File System Full (Système de fichiers saturé)	File system full: (Système de fichiers saturé :) File system <nom> is xx% full. (Système de fichiers (nom] saturé à xx %.) Action: (Action :) 1. Delete any unused or temporary files, OR (Supprimez les fichiers temporaires ou inutilisés OU) 2. Extend the partition by using an unused partition, OR (Augmentez le volume de la partition à l'aide d'une partition inutilisée OU) 3. Add additional disk drives and extend the partition after creating a new partition. (Ajoutez des unités de disque supplémentaires et étendez la partition après en avoir créé une nouvelle.) (Severity=Error) (Gravité = Erreur)	PartitionFull	F40 FileSystemName full (F40 Nom_système_ fichier complet)	File system <nom> usage capacity is xx%. (La capacité d'utilisation du système de fichiers [nom] est de xx %.)

Erreurs liées au sous-système RAID

Le [TABLEAU B-3](#) présente les messages d'erreurs et d'événements de Sun StorEdge 5310 NAS Appliance.

TABLEAU B-3 Messages d'erreur RAID

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
LUN Failure (Panne de LUN)	RAID LUN failure: (Panne de LUN RAID :) RAID LUN <i>N</i> failed and was taken offline. (Le LUN du système RAID <i>N</i> a rencontré une erreur et a été déconnecté.) Slot <i>n</i> is offline. (L'emplacement <i>n</i> est hors ligne.) Action: (Action :) Replace bad drives and restore data from backup. (Remplacez les unités de disque défectueuses et restaurez les données à partir de la sauvegarde.) Severity = Error (Gravité = Erreur)	RaidLunFail	R10 Lun failure (R10 Panne de LUN)	RAID LUN <i>N</i> failed and was taken offline. (Le LUN du système RAID <i>N</i> a rencontré une erreur et a été déconnecté.) Slot <i>n</i> is offline. (L'emplacement <i>n</i> est hors ligne.) (Severity=Error) (Gravité = Erreur)
Disk Failure (Panne de disque)	Disk drive failure: (Panne de l'unité de disque :) Disk drive failure. (Panne de l'unité de disque.) Failed drives are: (Les unités défectueuses sont les suivantes :) Slot#, Vendor, Product ID, Size (n° d'emplacement, fournisseur, ID de produit, taille). Severity = Error (Gravité = Erreur)	RaidDiskFail	R11 Drive failure (R11 Panne de l'unité de disque)	Disk drive failure. (Panne de l'unité de disque.) Failed drives are: (Les unités défectueuses sont les suivantes :) Slot#, Vendor, Product ID, Size (n° d'emplacement, fournisseur, ID de produit, taille). (Severity=Error) (Gravité = Erreur)
Controller Failure (Panne du contrôleur)	RAID controller failure: (Panne du contrôleur RAID :) RAID controller <i>N</i> has failed. (Panne du contrôleur RAID <i>N</i> .) Action: (Action :) Contact technical support. (Contactez le support technique.) Severity = Error (Gravité = Erreur)	RaidControllerFail	R12 Ctlr failure (R12 Panne du contrôleur)	RAID controller <i>N</i> failed. (Panne du contrôleur RAID <i>N</i> .)

Événements IPMI

Le serveur Sun StorEdge 5310 NAS Appliance utilise la carte IPMI pour contrôler les systèmes d'environnement et envoyer des messages concernant des problèmes de ventilateur, d'alimentation ou de température.

Remarque – L'Annexe D indique l'emplacement des différents périphériques.

Le TABLEAU B-4 offre une description des messages d'erreur liés au système IPMI de Sun StorEdge 5310 NAS Appliance.

TABLEAU B-4 Messages d'erreur IPMI

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
Fan Error (Panne de ventilateur)	Fan Failure: (Panne de ventilateur :) Blower fan xx has failed. (Panne du ventilateur soufflant xx.) Fan speed = xx RPM. (Vitesse du ventilateur = xx r/min.) Action: (Action :) The fan must be replaced as soon as possible. (Le ventilateur doit être remplacé au plus vite.) If the temperature begins to rise, the situation could become critical. (Si la température augmente, la situation risque de devenir critique.) Severity = Error (Gravité = Erreur)	envFanFail trap	P11 Fan xx failed (P11 Panne du ventilateur xx)	Blower fan xx has failed ! (Panne du ventilateur soufflant xx.)
Power Supply Module Failure (Panne du bloc d'alimentation)	Power supply failure: (Panne d'alimentation :) The power supply unit xx has failed. (Panne de l'unité d'alimentation xx.) Action: (Action :) The power supply unit must be replaced as soon as possible. (L'unité d'alimentation doit être remplacée au plus vite.) Severity = Error (Gravité = Erreur)	envPowerFail trap	P12 Power xx failed (P12 Panne de l'unité d'alimentation xx)	Power supply unit xx has failed. (Panne de l'unité d'alimentation xx.)

TABLEAU B-4 Messages d'erreur IPMI (Suite)

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
Power Supply Module Temperature (Température du bloc d'alimentation)	<p>Power supply temperature critical: (La température du bloc d'alimentation est excessive :)</p> <p>The power supply unit xx is overheating. (Surchauffe de l'unité d'alimentation xx.)</p> <p>Action: (Action :) Replace the power supply to avoid any permanent damage. (Remplacez le bloc d'alimentation afin d'éviter des dégâts irréversibles.)</p> <p>Severity = Critical (Gravité = Critique)</p>	envPowerTemp Critical trap	P22 Power xx over-heated (P22 Surchauffe de l'unité d'alimentation xx)	Power supply unit xx is overheating. (Surchauffe de l'unité d'alimentation xx.)
Temperature Error (Problème de température)	<p>Temperature critical: (La température est excessive :)</p> <p>Temperature in the system is critical. (La température du système est trop élevée.) It is xxx Degrees Celsius. (Elle est de xxx degrés Celsius.)</p> <p>Action: (Action :) 1. Check for any fan failures, OR (Vérifiez le fonctionnement du ventilateur OU)</p> <p>2. Check for blockage of the ventilation, OR (Vérifiez que le système de ventilation n'est pas obstrué OU)</p> <p>3. Move the system to a cooler place. (Déplacez le système dans un lieu plus frais.)</p> <p>Severity = Error (Gravité = Erreur)</p>	envTemperature Error trap	P51 Temp error (P51 Problème de température)	The temperature is critical. (La température est incorrecte.)
Primary Power Cord Failure (Mauvaise connexion du cordon d'alimentation principal)	<p>Power cord failure: (Mauvaise connexion du cordon d'alimentation :)</p> <p>The primary power cord has failed or been disconnected. (Mauvaise connexion du cordon d'alimentation principal.)</p> <p>Action: (Action :) 1. Check the power cord connections at both ends, OR (Vérifiez les deux extrémités du cordon d'alimentation OU)</p> <p>2. Replace the power cord. (Remplacez-le.)</p> <p>Severity = Error (Gravité = Erreur)</p>	envPrimary PowerFail trap	P31 Fail PWR cord 1 (P31 Mauvaise connexion cordon d'alimentation 1)	The primary power cord has failed. (Le cordon d'alimentation principal ne fonctionne pas correctement.)

TABLEAU B-4 Messages d'erreur IPMI (Suite)

Événement	Objet de l'e-mail : Texte	Déroutement SNMP	Écran LCD	Journal
Secondary Power Cord Failure (Mauvaise connexion du cordon d'alimentation secondaire)	<p>Power cord failure: (Mauvaise connexion du cordon d'alimentation :)</p> <p>The secondary power cord has failed or been disconnected. (Mauvaise connexion du cordon d'alimentation secondaire.)</p> <p>Action: (Action :) 1. Check the power cord connections at both ends, OR (Vérifiez les deux extrémités du cordon d'alimentation OU)</p> <p>2. Replace the power cord. (Remplacez-le.)</p> <p>Severity = Error (Gravité = Erreur)</p>	envSecondary PowerFail trap	P32 Fail PWR cord 2 (P32 Mauvaise connexion cordon d'alimentation 2)	The secondary power cord has failed. (Le cordon d'alimentation secondaire ne fonctionne pas correctement.)

API Compliance Archiving Software

Le produit Sun StorEdge 5310 NAS Appliance prend en charge le stockage de données en conformité par le biais d'une extension faisant l'objet d'une clé de licence et appelée « Compliance Archiving Software ».

Le logiciel Compliance Archiving Software est décliné en deux versions : une forme assouplie (appelée « application consultative ») et une forme stricte (dite « application obligatoire »). Pour des informations générales sur Compliance Archiving Software, reportez-vous à la section « [Compliance Archiving Software](#) », page 148.

Cette annexe propose une présentation technique des fonctions et de l'interface de programmation du logiciel Compliance Archiving Software avec application obligatoire.

Remarque – Pour que le logiciel Compliance Archiving Software fonctionne correctement, vous devez avoir au préalable procédé à une configuration physique adaptée du matériel du système Sun StorEdge 5310 NAS Appliance. En particulier, les baies de contrôleur des unités d'extension de Sun StorEdge 5300 RAID ne doivent être connectées à aucun périphérique ou réseau en dehors d'une connexion Fibre Channel privée à la tête NAS ou aux éventuels boîtiers d'extension des unités d'extension de Sun StorEdge 5300.

Remarque – Pour garantir un respect optimal de vos règles de conservation données, vous devez prendre toutes les mesures nécessaires pour assurer la sécurité physique de votre système Sun StorEdge 5310 NAS Appliance. Le stockage de données géré par logiciel ne remplacera jamais les précautions physiques prises pour contrôler l'accès au matériel du système.

Fonctions de conformité

Le logiciel Compliance Archiving Software propose des garanties de stockage au niveau de l'exactitude, de l'intégrité et de la conservation des fichiers. Cette fonction se compose de trois fonctionnalités principales :

- Fichiers WORM (Write-Once, Read-Many – Écriture unique, lectures multiples)
- Périodes de conservation par fichier
- Verrouillage administratif

Fichiers WORM

Les fichiers WORM renforcent les contrôles d'accès aux fichiers par rapport à l'accès traditionnel fourni par les protocoles NFS et CIFS. Lorsqu'une application désigne un fichier comme étant un fichier WORM, il ne peut plus être modifié. Les fichiers WORM ne peuvent être ni modifiés, ni complétés, ni renommés, quelle que soit l'identité du client ou utilisateur faisant cette tentative et quels que soient les privilèges dont il dispose. En outre, les fichiers WORM ne peuvent être supprimés que sur la base des règles de conservation des fichiers décrites ci-après.

Remarque – Même si ces fichiers portent le nom de WORM, ce qui désigne un stockage non réinscriptible et non effaçable, il serait plus juste de parler de « statut de lecture seule permanent ». Le système Sun StorEdge 5310 NAS Appliance n'impose aucune restriction quant à la rédaction du fichier ou à sa modification tant qu'il n'est pas transformé en fichier WORM.

Périodes de conservation par fichier

Le logiciel Compliance Archiving Software associe une période de conservation à chaque fichier WORM. Un fichier WORM ne peut être supprimé qu'une fois sa période de conservation échu. Les périodes de conservation peuvent être prolongées, mais non écourtées. Vous pouvez attribuer une nouvelle période de conservation à un fichier dont la période précédente est arrivée à expiration.

Verrouillage administratif

Pour garantir la conservation et la préservation des fichiers WORM, et le respect des périodes de conservation, certaines fonctions d'administration système (comme la suppression ou la modification des volumes de fichiers) sont désactivées ou limitées sur les volumes en conformité. Ces restrictions ont une incidence sur les fonctions d'administration système qui pourraient nuire à la conservation d'un fichier (par exemple, la suppression d'un volume de fichiers).

Accès à la fonction de conformité

Pour garantir une totale compatibilité avec les systèmes d'exploitation et applications client existants, les fonctions du logiciel Compliance Archiving Software sont mises en œuvre sous la forme d'extensions des protocoles d'accès aux fichiers existants pris en charge par le système Sun StorEdge 5310 NAS Appliance (NFS et CIFS). En particulier, le système Sun StorEdge 5310 NAS Appliance complète les attributs de fichier existants en indiquant l'état WORM d'un fichier et la fin de sa période de conservation. Cela simplifie la prise en charge des applications existantes de gestion des documents et des enregistrements étant donné que ces champs de métadonnées peuvent être définis et affichés à l'aide d'API et d'utilitaires client standard.

Volumes en conformité

Vous devez désigner les volumes en conformité dès leur création, car une fois que les volumes existent, ils ne peuvent plus être convertis par la suite. Un même système Sun StorEdge 5310 NAS Appliance peut comporter plusieurs volumes dont certains sont des volumes en conformité.

Vous ne devez pas permettre un archivage en conformité sur des volumes utilisés par des applications (et des utilisateurs) qui n'appliquent pas les règles de conservation de données dictées par le logiciel Compliance Archiving Software.

Fichiers WORM

Les fichiers WORM ne peuvent être ni modifiés ni mis à jour. Une fois qu'un fichier devient WORM, il est en lecture seule jusqu'à sa suppression.

Création de fichiers WORM

Le logiciel Compliance Archiving Software utilise un déclencheur WORM pour convertir un fichier normal en fichier WORM. Lorsqu'une application client ou un utilisateur exécute le déclencheur sur un fichier, le logiciel Compliance Archiving Software considère que le fichier cible doit être converti en fichier WORM.

Le déclencheur WORM pour clients UNIX définit le mode d'autorisation d'un fichier sur 4 000. Les applications client ou les utilisateurs peuvent activer ce déclencheur WORM à l'aide de la commande `chmod` ou de l'appel système. Lorsque le logiciel Compliance Archiving Software reçoit cette requête, il convertit le fichier cible en fichier WORM de la manière suivante :

- Définition du bit `setuid`
- Effacement des éventuels bits d'écriture qui seraient définis sur le fichier
- Conservation des bits d'accès en lecture sur le fichier

Remarque – Les fichiers exécutables ne peuvent pas devenir des fichiers WORM. Dans le cas de fichiers créés à partir de clients Windows, cela signifie qu'un fichier ne peut pas être converti en fichier WORM si sa liste de contrôle d'accès (ACL) comporte des entrées de contrôle d'accès (ACE) octroyant une autorisation d'exécution sur le fichier.

Dans l'exemple suivant, un fichier dont le mode d'accès est de 640 est converti en fichier WORM. Une fois le déclencheur WORM lancé, le mode d'accès du fichier devient 4440.

```
$ ls -l testfile
-rw-r----- 1 smith  staff      12139 Dec  2 13:18 testfile
$ chmod 4000 testfile
$ ls -l testfile
-r-Sr----- 1 smith  staff      12139 Dec  2 13:18 testfile
```

Le logiciel Compliance Archiving Software utilise ce déclencheur WORM car cette opération a très peu de chance d'être utilisée par les applications existantes.

Le déclencheur WORM pour les clients Windows définit à la fois les bits de lecture seule et système sur un fichier. Le déclencheur WORM définit le bit de lecture seule du fichier mais ne modifie pas son bit système.

Une fois que le fichier est devenu un fichier WORM, vous ne pouvez plus inverser le processus. À partir de clients Windows, il est impossible d'effacer le bit de lecture seule et de modifier le bit système. À partir de clients UNIX, il est impossible d'effacer le bit `setuid`. De même, il est impossible d'ajouter des autorisations d'exécution ou d'écriture au mode d'accès du fichier.

Les volumes en conformité convertissent ces paramètres WORM entre les protocoles CIFS et NFS. Par exemple, si un client UNIX affiche un fichier WORM créé par un client Windows, le mode d'accès WORM se présente sous la forme décrite précédemment.

Comportement des fichiers WORM

Il n'est pas possible de modifier, d'écraser ou d'étendre des fichiers WORM. Toute tentative d'écriture dans un fichier WORM échoue et renvoie une erreur, quels que soient les privilèges d'accès et l'identité de l'utilisateur client.

Ni le propriétaire du fichier WORM ni un utilisateur disposant de privilèges d'administration (ou même de privilèges de superutilisateur) ne sont autorisés à modifier un fichier WORM. Les fichiers WORM ne peuvent ni être renommés ni reconvertis en fichiers standard (non WORM).

Métadonnées des fichiers WORM

Le logiciel Compliance Archiving Software n'autorise pas la modification des métadonnées contenant, protégeant, décrivant ou nommant des données client. Seul un sous-ensemble limité de champs de métadonnées peut être éventuellement modifié, en fonction du système d'exploitation, comme l'indique le [TABLEAU C-1](#).

TABLEAU C-1 Métadonnées de fichiers WORM modifiables et non modifiables

Système d'exploitation	Modifiables	Non modifiables
UNIX	<ul style="list-style-type: none">• Définir ou effacer des bits de lecture• Changer le propriétaire du fichier et du groupe	<ul style="list-style-type: none">• Activer les bits d'écriture et d'exécution• Effacer le bit setuid• Modifier la taille ou l'heure (mtime)
Windows	<ul style="list-style-type: none">• Définir ou effacer des bits de lecture• Modifier le bit d'archive• Créer et modifier des listes de contrôle d'accès (même si un fichier WORM est impossible à modifier quels que soient les paramètres de ces listes)	<ul style="list-style-type: none">• Modifier les bits de lecture seule, bits système et bits cachés• Modifier la taille ou l'heure (mtime)

Restrictions relatives à l'espace de noms

Le logiciel Compliance Archiving Software ne permet pas de renommer les fichiers WORM. En outre, seuls les répertoires vides peuvent être renommés. Cette règle permet d'empêcher le chemin complet d'un fichier WORM de changer pendant la durée de vie du fichier.

Remarques

Lorsqu'un client UNIX configure le mode d'un fichier sur 4000 (en appelant le déclencheur WORM), en général, le mode d'accès au fichier qui en résulte n'est pas 4000, ce qui est contraire aux mesures standard prises par la commande `chmod` et l'appel système. Par conséquent, la version GNU de la commande `chmod(1)` (utilisée par la plupart des distributions Linux) génère un message d'avertissement lorsqu'elle est utilisée pour exécuter le déclencheur WORM. Vous pouvez ignorer ce message.

Périodes de conservation des fichiers

Chaque WORM est associé à une période de conservation pendant laquelle il ne peut pas être supprimé. Cette période est définie à l'aide d'un horodatage indiquant la fin de la période. Le délai de conservation peut être défini de manière explicite par les applications ou utilisateurs client. Si le client ne précise aucune période de conservation, le logiciel Compliance Archiving Software utilise la *période de conservation par défaut* définie pour le volume au moment de sa création.

Toute tentative de suppression d'un fichier WORM avant la fin de sa période de conservation échoue. En revanche, une fois cette période arrivée à expiration, vous pouvez supprimer le fichier quand vous le souhaitez.

Remarque – Les périodes de conservation ne déterminent que la possibilité de supprimer les fichiers. Un fichier WORM ne peut en aucun cas être modifié même une fois sa période de conservation arrivée à terme.

Définition des horodatages de conservation

Les horodatages de conservation du logiciel Compliance Archiving System sont stockés au niveau de l'attribut `atime`, définissant les temps d'accès, des fichiers WORM. En règle générale, les clients définissent l'attribut `atime` avant de mettre le fichier en lecture seule. Lorsqu'un fichier devient un fichier WORM, la valeur de son attribut `atime` est arrondie à la valeur inférieure (au nombre de secondes le plus près) afin de déterminer l'horodatage de conservation.

Si l'attribut `atime` correspond à une date dans le passé, la période de conservation par défaut du système de fichiers est utilisée pour calculer l'horodatage de conservation : le système ajoute la période de conservation par défaut à l'heure actuelle.

Conservation permanente

Les applications ou utilisateurs client peuvent demander la conservation permanente d'un fichier. Pour cela, ils doivent paramétrer l'attribut `atime` d'un fichier sur la valeur légale maximale d'un entier 32 bits signé. Cette valeur (0x7fffffff) est 2 147 483 647. Sur les systèmes UNIX, cette valeur est définie sous la forme `INT_MAX` dans le fichier d'en-tête `limits.h`. Elle correspond à l'horodatage suivant : 03:14:07 GMT, Jan 19, 2038.

Modification des périodes de conservation

Les périodes de conservation peuvent être prolongées. Lorsque la période de conservation d'un fichier est arrivée à expiration, vous pouvez en définir une nouvelle. Pour ce faire, redéfinissez l'attribut `atime` d'un fichier `WORM`. Ces modifications sont autorisées à condition que la nouvelle valeur corresponde à une date ultérieure par rapport à l'ancien horodatage de conservation.

Temps d'accès ignoré

Étant donné que l'attribut de temps d'accès (`atime`) est utilisé par le logiciel Compliance Archiving Software pour stocker les horodatages de conservation, cet attribut n'est pas mis à jour en cas de modification au niveau du système de fichiers standard, qu'un fichier soit ou non un fichier `WORM`.

Définition de l'état d'un fichier

Les applications et utilisateurs client peuvent déterminer l'état de conservation d'un fichier en lisant les métadonnées du fichier via les outils et API standard. Sur des clients UNIX, par exemple, vous pouvez lire les attributs d'un fichier via l'appel système de `stat` (2) ou à l'aide de la commande `ls`. (La commande `ls -lu` répertorie les fichiers en indiquant pour chacun leurs droits d'accès et leurs horodatages `atime`.)

Comportement des appels système UNIX

Les applications client UNIX accèdent au logiciel Compliance Archiving Software via leur interface locale d'appel système. Elles appellent ainsi la mise en œuvre NFS client qui convertit les appels système en requêtes standard pour le protocole NFS. Étant donné que le comportement des systèmes de fichier Compliance diffère de celui des systèmes de fichiers NAS standard, ces différences se retrouvent également au niveau des appels système client.

Cette section décrit les appels système UNIX standard dont le comportement diffère lorsqu'un client les exécute sur un partage Sun StorEdge 5310 NAS Appliance ou Compliance est activé. Les appels système qui ne figurent pas dans cette liste se comportent normalement.

N'oubliez pas que les interfaces du système Sun StorEdge 5310 NAS Appliance sont les protocoles d'accès aux fichiers NFS et CIFS. Par conséquent, cette section présente à la fois le comportement Compliance du système Sun StorEdge 5310 NAS Appliance en réponse aux requêtes des protocoles standard, et les correspondances entre les appels système et les requêtes NFS. Le comportement de ces appels a été vérifié sur les clients exécutant le système d'exploitation Solaris et devrait être identique sur les autres clients UNIX.

`access (2)`

Toute tentative d'attribution d'autorisation d'écriture sur un fichier WORM (c'est-à-dire tout appel de la commande `access (2)` où l'argument `amode` comporte le bit `W_OK`) échoue et renvoie une erreur (`EPERM`).

`chmod (2), fchmod (2)`

Si le fichier cible est un fichier non-WORM ordinaire pour lequel aucun bit d'autorisation d'exécution n'est défini et que le nouveau droit d'accès est paramétré sur 4000 (`S_ISUID`), le fichier cible devient un fichier WORM. Dans ce cas, le fichier reçoit un nouveau mode d'accès obtenu en ajoutant le bit `setuid` aux éventuels bits de lecture existants dans le mode d'accès du fichier. Plus précisément, si l'ancien mode d'accès d'un fichier est `ancien_mode` et que le fichier en obtient un nouveau après exécution du déclencheur WORM, vous obtenez :

```
nouveau_mode = S_ISUID | (ancien_mode & 0444)
```

Les fichiers exécutables ne peuvent pas être convertis en fichiers WORM. Vous ne pouvez pas exécuter le déclencheur WORM (mode 4000) sur un fichier disposant d'au moins un bit d'exécution. Si vous essayez, l'erreur (EACCES) s'affiche.

Vous pouvez en revanche définir ou supprimer des bits d'accès en lecture sur les fichiers WORM. Toute tentative d'activation d'un droit d'accès en écriture ou en exécution sur un fichier WORM, de définition du bit setgid (S_ISGID) ou du bit sticky (S_ISVTX), ou encore toute tentative de suppression du bit setuid échoue et renvoie une erreur (EPERM).

chown(2), fchown(2)

Le comportement de ces appels est identique pour les fichiers WORM et non WORM.

link(2)

Les clients peuvent créer des liens physiques vers les fichiers WORM. Les liens physiques vers un fichier WORM ne peuvent être supprimés qu'à l'issue de la période de conservation du fichier. (Voir [unlink\(2\)](#), [page 292](#)).

read(2), readv(2)

Les clients sont autorisés à lire les fichiers WORM. Étant donné que les horodatages de conservation sont stockés au niveau de l'attribut atime, cette valeur n'est pas mise à jour pour refléter l'accès en lecture aux fichiers WORM.

rename(2)

Toute tentative visant à renommer un fichier WORM ou un répertoire non vide dans un système de fichiers Compliance échoue et renvoie une erreur (EPERM).

`stat(2)`, `fstat(2)`

Lorsque ces appels sont utilisés afin d'obtenir des informations sur les fichiers ordinaires, la structure `stat` obtenue contient des valeurs Compliance. Le champ `st_mode` contient (comme à l'accoutumée) le mode et les droits d'accès du fichier. Dans le cas d'un fichier WORM, le bit `setuid` est défini, contrairement aux bits d'écriture et d'exécution. Le champ `st_atime` contient un horodatage indiquant la fin de la période de conservation du fichier. Si cette valeur est égale au paramètre `INT_MAX` défini dans le fichier `limits.h`, le fichier est conservé définitivement.

`unlink(2)`

Les liens des fichiers WORM ne peuvent être supprimés que si l'heure actuelle, indiquée par l'horloge sécurisée de Sun StorEdge 5310 NAS Appliance, est ultérieure à la date stockée dans l'attribut `atime` du fichier (c'est-à-dire à l'horodatage de conservation). Si cette condition n'est pas remplie, la commande `unlink(2)` échoue et renvoie une erreur (`EPERM`).

`utime(2)`, `utimes(2)`

Ces appels permettent de définir les attributs de temps d'accès (`atime`) et d'heure de modification (`mtime`) d'un fichier. S'ils sont utilisés avec un fichier non-WORM, ils se comportent normalement et vous donnent la possibilité d'indiquer l'horodatage de conservation avant la conversion du fichier en WORM.

Lorsqu'ils sont utilisés avec des fichiers WORM, ces appels permettent de prolonger la période de conservation du fichier ou d'attribuer une nouvelle période de conservation à un fichier dont la période précédente était arrivée à expiration. Ces appels réussissent pour un fichier WORM si la nouvelle valeur `atime` est supérieure (c'est-à-dire ultérieure) à la valeur précédente. Si la nouvelle valeur `atime` est inférieure ou égale au paramètre `atime` actuel, ces appels échouent et renvoient une erreur (`EPERM`). Dans le cas d'un fichier WORM, l'argument `mtime` est ignoré.

`write(2)`, `writev(2)`

Toute tentative d'écriture dans un fichier WORM échoue et renvoie une erreur (`EPERM`).

Comportement des clients Windows

Création de fichiers WORM

Un fichier normal (non WORM) peut être converti en fichier WORM à partir de Windows uniquement si ses bits d'archive et cachés ne sont pas définis. Le déclencheur WORM entraîne la définition du bit de lecture seule du fichier, mais ne modifie pas l'état de son bit système.

Une fois que le fichier est devenu un fichier WORM, vous ne pouvez plus inverser le processus. À partir de clients Windows, il est impossible d'effacer le bit de lecture seule et de modifier le bit système.

Restrictions relatives aux métadonnées sur les fichiers WORM

Les clients Windows peuvent modifier le bit d'archive d'un fichier WORM. En revanche, ils ne peuvent pas modifier les bits de lecture seule, les bits cachés ou le bit système. Les clients Windows peuvent modifier les listes de contrôle d'accès des fichiers WORM, mais les droits d'accès qu'elles contiennent seront ignorés dans le cas d'un fichier WORM. Toute tentative de modification des données d'un fichier WORM échoue quels que soient les droits définis dans la liste de contrôle d'accès.

Paramétrage des périodes de conservation

Tout comme les clients UNIX, les clients Windows définissent des périodes de conservation en stockant des horodatages de conservation au niveau de l'attribut atime de temps d'accès d'un fichier.

Remarques concernant les clients Windows

Précautions à observer au niveau du bit de lecture seule

Les volumes de fichiers en conformité doivent impérativement être réservés à une utilisation par les applications et utilisateurs Windows appliquant le comportement spécifiquement adapté aux fichiers WORM. De nombreux utilitaires Windows standard de copie de fichiers ajoutent des bits de lecture seule et système à un fichier. Si vous utilisez ces outils pour procéder à des copies de fichiers WORM sur un volume en conformité, les fichiers qui en résultent risquent de devenir des fichiers WORM étant donné que leurs bits de lecture seule et système sont définis.

Logiciel antivirus

De nombreux programmes de vérification des virus tentent de préserver le temps d'accès dont ils disposent sur les fichiers qu'ils examinent. En règle générale, ces programmes lisent l'attribut atime d'un fichier avant de rechercher les éventuels virus qu'il serait susceptible de contenir, et réinitialisent ensuite l'attribut atime sur la valeur qu'il avait avant l'analyse. Cela peut poser problème dans le cas où un programme de recherche des virus analyse un fichier en même temps qu'une autre application définit un délai de conservation pour le fichier. Le délai de conservation attribué au fichier peut être incorrect.

Pour éviter ce problème, faites en sorte qu'aucun programme de recherche des virus ne soit exécuté sur les systèmes de fichiers Compliance, ou au moins qu'ils ne soient pas exécutés au moment où d'autres applications créent des fichiers WORM.

Des applications personnalisées peuvent également éviter ce problème en utilisant une période de conservation par défaut courte et en redéfinissant la période de conservation du fichier sur sa vraie valeur une fois le déclencheur WORM exécuté.

Autres API

Vous pouvez accéder au logiciel Compliance Archiving Software par le biais de nombreuses autres API client, comme Java, Perl, C++, etc. Tous ces langages utilisent les mêmes appels système de base pour accéder aux partages montés via NFS ou CIFS.

Composants de l'appareil Sun StorEdge 5310 NAS Appliance

Cette annexe décrit certains composants matériels (de l'écran) du serveur Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310, le boîtier du contrôleur d'unité d'extension Sun StorEdge 5300 RAID EU et le boîtier d'extension Sun StorEdge 5300 EU.



Attention – Seul un technicien qualifié est habilité à retirer les capots des unités afin d'accéder aux composants internes.

Remarque – The general Sun StorEdge 5310 NAS Appliance features described in this appendix also apply to the Sun StorEdge 5310 Cluster.

Les informations suivantes sont présentées :

- « Alimentations électriques du serveur », page 296
- « Boutons du panneau avant du serveur », page 297
- « Panneau arrière du serveur », page 298
- « Boîtier de contrôleur Sun StorEdge 5300 RAID EU et composants du boîtier d'extension Sun StorEdge 5300 EU », page 300

Alimentations électriques du serveur

L'alimentation d'un système est également fournie pour l'ensemble de ses composants. Les systèmes d'alimentation de l'ensemble des unités sont des périphériques de détection automatique qui s'adaptent automatiquement aux tensions comprises entre 100 et 240 volts, et 50 et 60 Hz.

L'alimentation système d'un serveur se compose de deux modules redondants remplaçables à chaud qui se présentent sous la forme d'une configuration 1+1. Chacun de ces modules est capable de supporter une charge de 500 watts. Au moins une alimentation est nécessaire au bon fonctionnement du système, mais il est indispensable de disposer de deux alimentations à des fins de redondance.

Un voyant rouge à l'arrière du module d'alimentation indique que le cordon d'alimentation est débranché.

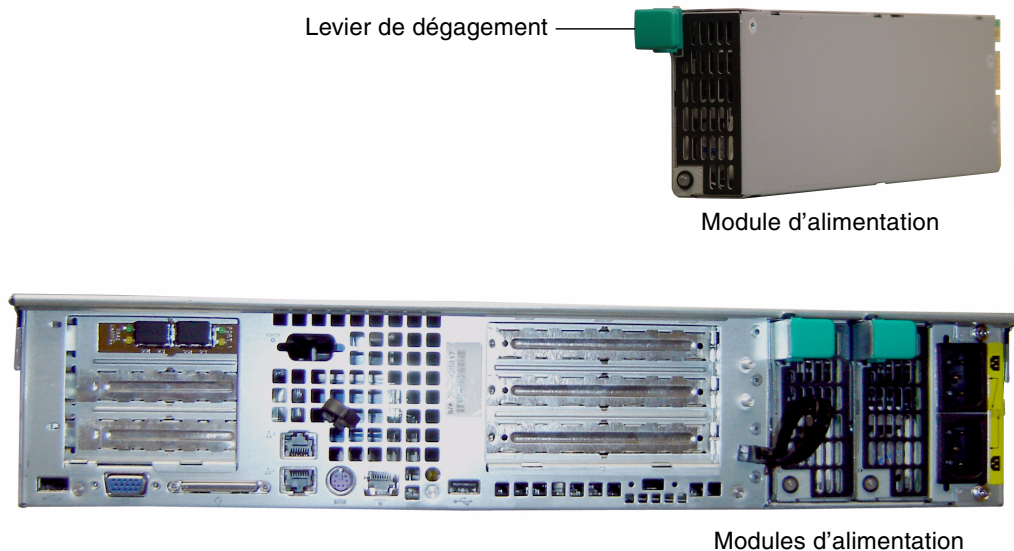


FIGURE D-1 Alimentation électrique

Les fonctions de l'alimentation sont les suivantes :

- une capacité de sortie de 500 watts ;
- des indicateurs de statut DEL ;
- des ventilateurs de refroidissement internes à plusieurs vitesses ;
- une fonctionnalité de partage de charge intégrée ;
- une capacité de protection contre les surcharges intégrée ;
- une poignée intégrale pour les insertions/retraits.

Boutons du panneau avant du serveur

Bouton de mise en marche : interrupteur à rappel (conforme à la spécification APCI) qui permet de mettre le système sous tension et hors tension.



Attention – N'utilisez pas le bouton marche/arrêt pour arrêter le système. Suivez toujours scrupuleusement la procédure d'arrêt décrite à la section « [Arrêt du serveur](#) », page 180. Si l'arrêt ne se déroule pas correctement, vous risquez de perdre des données.

Bouton d'ID de système : bouton permettant d'allumer le voyant bleu à l'avant et à l'arrière du système et de repérer ainsi l'emplacement d'une unité dans un rack.

Bouton Reset : bouton permettant de réinitialiser le système.



Attention – N'utilisez pas ce bouton pour réinitialiser le système. Suivez toujours scrupuleusement la procédure d'arrêt.

DEL de statut

Les DEL de statut du panneau avant signalent les activités en cours du système.

TABLEAU D-1 Indicateurs de statut DEL

DEL d'alimentation	Lorsque cette DEL est verte et allumée en continu, cela signifie que le système est sous tension. Lorsqu'elle est de couleur ambre, l'un des cordons d'alimentation est débranché. Lorsqu'elle est éteinte, le système est hors tension.
DEL de la carte réseau intégrée 1	Lorsque cette DEL est verte, cela signale la présence d'une activité réseau par le biais du port de carte d'interface réseau intégrée 1.
DEL de la carte réseau intégrée 2	Lorsque cette DEL est verte, cela signale la présence d'une activité réseau par le biais du port de carte d'interface réseau intégrée 2.

TABLEAU D-1 Indicateurs de statut DEL (*Suite*)

DEL de statut du disque dur	<ul style="list-style-type: none">• Non applicable.
DEL de statut du système	<ul style="list-style-type: none">• Lorsque cette DEL est verte et allumée en continu, cela signifie que le système fonctionne normalement.• Lorsqu'elle est verte mais clignote, le fonctionnement du système est anormal.• Lorsqu'elle est de couleur ambre et allumée en continu, le système se trouve dans un état critique ou n'est pas réparable.• Lorsqu'elle est de couleur ambre mais clignote, le système est dans un état non critique.• Lorsque cette DEL est rouge, cela signifie que l'un des cordons d'alimentation est débranché.• Enfin, lorsqu'elle est éteinte et sous réserve que la DEL d'alimentation soit verte, cela implique que le système est en pause.
DEL d'ID de système	<ul style="list-style-type: none">• Lorsque cette DEL est bleue et allumée en continu, cela signifie que le bouton d'ID est enfoncé.• Lorsqu'elle est éteinte, le bouton d'ID n'est pas enfoncé.

Panneau arrière du serveur

L'illustration ci-après montre les divers ports et connecteurs qui figurent sur le panneau arrière du serveur.

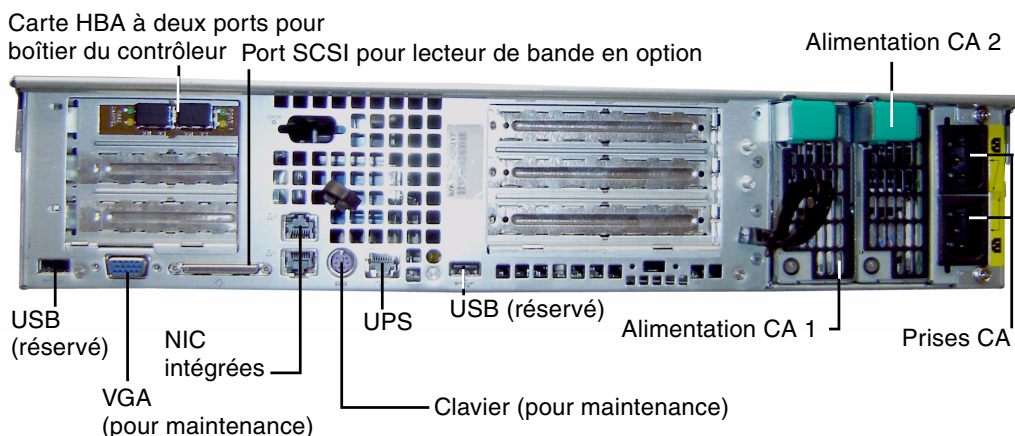


FIGURE D-2 Panneau arrière doté d'une seule carte HBA

Remarque – N'utilisez pas de ports VGA sur les panneaux avant et arrière. Ces connecteurs sont réservés au personnel du service de support technique de Sun Microsystems.

Remarque – Le panneau arrière de Sun StorEdge 5310 NAS Appliance relié à deux boîtiers de contrôleur est pourvu de deux cartes HBA à deux ports.

Bibliothèque de bandes à connexion directe

Vous avez la possibilité de connecter une unité de sauvegarde sur bande locale au port SCSI situé dans le coin inférieur gauche du panneau arrière du serveur.

Remarque – Assurez-vous que le lecteur de bande figure bien dans la liste des unités prises en charge. Pour obtenir les dernières informations relatives aux périphériques de bande pris en charge, contactez votre représentant commercial Sun.

L'ID SCSI de la bibliothèque de bandes doit être inférieur à celui du lecteur de bande. Vous pouvez par exemple définir l'ID de la bibliothèque sur la valeur **0** et l'ID de l'unité sur une valeur non conflictuelle comme **5**.

Pour plus de détails sur le lecteur de bande que vous employez, consultez la documentation fournie avec le système.

Boîtier de contrôleur Sun StorEdge 5300 RAID EU et composants du boîtier d'extension Sun StorEdge 5300 EU

Le boîtier de contrôleur et les boîtiers d'extension offrent de l'espace de stockage pour Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310.

Controller Enclosures

Les boîtiers de contrôleur d'unités d'extension Sun StorEdge 5300 RAID EU sont compatibles avec des boîtiers d'extension Fibre Channel (EU F) ou SATA (EU S).



Attention – Pour ajouter ou supprimer des boîtiers d'extension, vous devez arrêter le système.

Le panneau avant du boîtier de contrôleur Fibre Channel contient 14 disques durs remplaçables à chaud organisés en deux groupes RAID 5 de six unités, plus deux unités hot spare de rechange. Chaque unité a une capacité brute de 146 giga-octets et une capacité disponible de 133 giga-octets pour une capacité totale disponible de 1,3 téraoctets sur l'ensemble du boîtier.

La configuration RAID d'unités FC de 300 Go se compose d'un groupe RAID 5 de 6 unités (5+1), d'un groupe RAID 5 de 7 unités (6+1), plus un disque hot spare de rechange.

Le boîtier de contrôleur utilisé par un système SATA est fourni sans disque dur. À la place, toutes les unités SATA sont contenues dans les boîtiers d'extension EU S.



Attention – N'installez pas à la fois des unités de disque Fibre Channel et SATA dans une même baie ou dans un même boîtier de contrôleur.

Remarque – Dans une configuration à deux baies, une baie peut contenir des unités de disque Fibre Channel (dans le boîtier de contrôleur et les boîtiers d'extension) et l'autre, des unités de disque SATA (dans les boîtiers d'extension uniquement).

Expansion Enclosures

Les boîtiers d'extension vous permettent d'étendre les capacités de stockage du système.

Le panneau avant de chaque boîtier d'extension EU F contient 14 disques durs Fibre Channel remplaçables à chaud organisés en deux groupes RAID 5 de sept unités. Chaque unité a une capacité brute de 146 giga-octets et une capacité disponible de 133 giga-octets pour une capacité totale disponible de 1,6 téraoctets par boîtier d'extension EU F.

Le panneau avant du premier boîtier d'extension EU S contient 14 disques durs SATA remplaçables à chaud organisés en deux groupes RAID 5 de six unités, plus deux unités hot spare de rechange. Chaque unité SATA a une capacité brute de 400 giga-octets et une capacité disponible de 360 giga-octets pour une capacité totale disponible de 3,6 téra-octets pour le premier boîtier d'extension EU S.

Les autres boîtiers d'extension d'unités d'extension contiennent 14 disques durs SATA remplaçables à chaud organisés en deux groupes RAID 5 de 7 unités pour une capacité disponible supplémentaire de 4,4 téra-octets.



Attention – N'installez pas à la fois des unités de disque Fibre Channel et SATA dans un même boîtier d'extension.

Unités d'extension FC et SATA mélangées

Les configurations d'unités d'extension (EU) SATA (Serial Advanced Technology Attachment) et Fibre Channel sont à présent prises en charge avec les stipulations suivantes.

- Les unités d'extension complètes doivent se composer d'unités d'un seul type (Fibre Channel ou SATA). Le mélange des deux types d'unités au sein d'une unité d'extension (EU) n'est pas pris en charge.
- L'EU RAID peut contenir des unités Fibre Channel même si les EU incluent des unités SATA. L'EU RAID ne peut pas contenir d'unités SATA.
- Un disque hot spare unique doit être disponible pour les types SATA et Fibre Channel en observant la même capacité que celle utilisée dans la baie.
- Les LUN ne peuvent pas contenir simultanément des unités SATA et Fibre Channel.

Casiers pour disque dur



Attention – Seules les unités Fibre Channel or SATA fournies par Sun Microsystems fonctionnent avec Sun StorEdge 5310 NAS Appliance et cluster Sun StorEdge 5310. Pour obtenir les dernières informations relatives à la prise en charge, contactez un représentant commercial Sun.

Chaque disque dur est inséré dans un casier qui lui est réservé. Vous pouvez remplacer ces casiers indépendamment, sans arrêter le boîtier d'extension, le boîtier du contrôleur, Sun StorEdge 5310 NAS Appliance ou Cluster.



Attention – N'installez pas à la fois des unités de disque Fibre Channel et SATA dans une même baie, ou un même boîtier d'extension ou de contrôleur.



Attention – Vous ne devez remplacer à chaud qu'un seul casier pour disque dur à la fois. Vérifiez que le sous-système RAID a procédé correctement à la reconstruction avant de retirer un autre casier.



Attention – Il est déconseillé de mettre à jour les logiciels système ou les microprogrammes RAID lorsque l'état du sous-système RAID est critique ou lors de la création ou de la reconstruction d'un jeu RAID.

▼ Pour localiser un disque ou un boîtier

1. Dans le volet de navigation de Web Administrator, sélectionnez RAID > Manage RAID (Gestion des systèmes RAID).
2. Cliquez sur le bouton Locate Drive (Localiser le disque) ou Locate Drive Tray (Localiser le plateau de disques), ce qui déclenchera le clignotement de l'indicateur LCD du disque ou du boîtier concerné.



FIGURE D-3 Casiers pour disque dur Fibre Channel

▼ Pour identifier un disque à remplacer

En cas de panne d'unité de disque, utilisez l'entrée de journal pour faciliter l'identification de ce disque. (Vous pouvez interpréter les emplacements de disques en vous aidant du journal système et des rapports de diagnostic.) Voici un exemple d'entrée de journal :

```
Controller 0 enclosure 0 row 0 column 6
```

Pour interpréter de telles entrées de journal, conservez à l'esprit les points suivants :

- Ignorez les éventuels numéros de canaux et de cibles.
- La numérotation des contrôleurs commence à 0. Par exemple, les contrôleurs de la première baie (RAID EU) portent les numéros 0 (emplacement A) et 1 (emplacement B) tandis que ceux de la deuxième baie portent les numéros 2 et 3.
- La numérotation des boîtiers commence à 0 et dépend de la baie dans laquelle ils se trouvent. Par exemple, si la première baie contient 2 boîtiers, ces derniers sont identifiés par les numéros 0 et 1.
- La numérotation des lignes est toujours égale à 0 pour cluster Sun StorEdge 5310.
- La numérotation des colonnes commence à 0 et indique le numéro d'emplacement dans le boîtier.

Vous pouvez par conséquent interpréter l'exemple comme indiquant l'emplacement 7 du premier boîtier de la première baie.

Remarque – Aucune méthode standard ne permet d'identifier la baie comme étant la première ou la seconde. En règle générale, le premier port HBA est connecté à la première baie, le deuxième étant connecté à la deuxième, etc.

Alimentations

Le boîtier du contrôleur et les boîtiers d'extension utilisent les mêmes modules d'alimentation.



Module d'alimentation

Boîtier de contrôleur



Module d'alimentation

Module d'alimentation

Boîtier d'extension



Module d'alimentation

Module d'alimentation

FIGURE D-4 Modules d'alimentation


Envoi d'un e-mail de diagnostic

La fonction d'envoi d'un e-mail de diagnostic vous permet d'adresser des e-mails à l'équipe du support technique de Sun Microsystems ou à tout autre destinataire de votre choix. Les e-mails de diagnostic contiennent des informations sur la configuration système de Sun StorEdge 5310 NAS Appliance, le sous-système de disque, le système de fichiers, la configuration réseau, les partages SMB, les procédures de sauvegarde et de restauration, des informations sur le répertoire /etc, le journal système, les données d'environnement ainsi que des informations sur l'administrateur.

Chaque e-mail de diagnostic doit contenir toutes ces informations et ce, quel que soit le problème.

Dans une configuration en cluster, vous devez configurer un e-mail de diagnostic pour chaque serveur faisant partie du cluster.

Pour configurer l'envoi d'e-mail de diagnostic :

1. Cliquez sur le bouton  de la barre d'outils située en haut de l'écran.
Les fenêtres Diagnostic Email (E-mail de diagnostic) s'affichent.
2. Entrez une description du problème dans le champ **Problem Description (Description du problème)**.
Ce champ est obligatoire et peut contenir jusqu'à 256 caractères.
3. Veillez à ce que la case **Diagnostics** soit cochée pour un destinataire au minimum.
Pour savoir comment ajouter ou modifier des destinataires, reportez-vous aux instructions de la section « Paramétrage de la notification par e-mail », page 33.
4. Cliquez sur **Send (Envoyer)** pour envoyer le message.

Index

A

Accès, points de contrôle 186

Activation

ADS

IG 89

Telnet 236

Autohome, partage

IG 121

Telnet 233

Basculement

IG 18

Telnet 265

Basculement de contrôleur

IG 20

Telnet 265

Basculement de liaison

IG 19

Telnet 265

Basculement de tête

Telnet 265

Contrôle de l'onduleur UPS 173

DNS

IG 27

Telnet 224

DNS dynamique 28

Telnet 224

Journalisation 34

À distance, Telnet 224

En local, Telnet 224

Langues étrangères

IG 36

Telnet 223

LDAP 93

NIS 29

Telnet 227

NIS+ 30

Telnet 227

Notification par e-mail 33

Telnet 255

Options 133

Partages statiques

IG 115

Telnet 232

Points de contrôle, Telnet 270

Protection antivirus 72

Quotas d'utilisateurs

IG 124

Telnet 237

Quotas de groupes

IG 124

Telnet 237

Quotas, Telnet 237

Sécurité

Domaine 25

Groupe de travail 25

Services de noms 32

Telnet 224

SNMP

IG 156

Telnet 254

WINS 27

Active Directory Service, voir ADS

Adaptateurs réseau, configuration 22

Telnet 217

Administrateur, groupe 96

Adresse IP alias, à propos 79

- ADS
 - À propos 87, 88
 - Activation 89
 - Configuration
 - Clients Windows 2000 120
 - IG 89
 - Telnet 236
 - Définition 8
 - Mise à jour des conteneurs de partage 92
 - Noms de conteneurs 90
 - Paramétrage 25
 - IG 89
 - Telnet 236
 - Publication de partages 91
 - Suppression de partages 93
- Affectation
 - Disque hot spare 48
 - Langue 36
 - Rôles du port 23
- Affichage
 - Activité réseau 167
 - Activité système 168
 - Analyse de points de contrôle, Telnet 257
 - Environnement, statut 163
 - Événements système 160
 - Informations sur le contrôleur 173
 - Journal système 158
 - IG 158
 - Telnet 256
 - Liaison de ports, Telnet 257
 - Moniteur d'activité, Telnet 256
 - Route 171
 - Route réseau 171
 - Sauvegarde
 - Journal, IG 175
 - Statut de la bande 176
 - Statut de la tâche 176
 - Statistiques de miroir
 - IG 173
 - Telnet 259
 - Statut 157
 - Alimentation 165
 - Miroir individuel, Telnet 257
 - Miroir, Telnet 257
 - Température 164
 - Tension 165
 - Ventilateur 163
 - Utilisation du volume de fichiers 167
- Agrégation de canaux, voir Liaison de ports
- Agrégation de liens, voir Liaison de ports
- Agrégation, voir Liaison de ports
- Aide en ligne, utilisation 7
- Aide, utilisation 7
- Ajout
 - Exportations NFS 129
 - Hôtes 100
 - Telnet 243
 - Hôtes de confiance
 - IG 100
 - Telnet 244
 - LUN 45
 - Membres de groupe
 - IG 98
 - Telnet 238
 - Partages statiques
 - IG 115
 - Telnet 234
 - Points de contrôle
 - IG 181
 - Telnet 270
 - Quotas
 - Groupes 124
 - Structures de répertoire 127
 - Utilisateurs 124
 - RAID 45
 - Segment, Telnet 231
 - Volume de fichiers, Telnet 229
- Alerte
 - Événements, journal système 160
 - Seuils du tampon miroir 141
- Alias IP
 - À propos 79
 - Système à deux serveurs 79
- Alimentation électrique 304
 - Statut 165
- Alimentation non interruptible, voir UPS
- Analyse antivirus 75
- Antivirus, protection, paramétrage 72
- Arrêt 180
 - Telnet 264
- Arrêt du serveur 180
 - Telnet 264
- Assignation de propriété, privilège de groupe 97

- Assistant
 - Démarrage 8
 - Exécution 7
 - Options 7
- Attribution d'un nouveau nom
 - Partitions, Telnet 230
 - Point de contrôle 185
- Attribution, nom du serveur 12
- Autohome, partage
 - À propos 121
 - Configuration 121
 - Paramétrage, Telnet 233
- B**
- Barre d'outils
 - Icônes 2
 - Utilisation 2
- Basculement
 - Activation 18
 - Configuration, Telnet 265
 - Contrôleur, activation 20
 - Définition 18
 - Gestion, Telnet 264
 - Liaison 19
 - Activation 19
- Boîtier d'extension, casier pour disque dur 301
- C**
- Casier pour disque dur 301
- Centre de distribution de clés, voir KDC
- Changement
 - Exportations NFS 131
 - Hôtes 100
 - Telnet 243
 - Langue, Telnet 223
 - Miroir 140
 - Noms de partition, Telnet 230
 - Ordre de recherche des services de noms
 - Telnet 228
 - Partages statiques
 - IG 118
 - Telnet 235
 - Point de contrôle planifié 184
 - Quotas
 - Groupes 125
 - Structures de répertoire 128
 - Utilisateurs 125

- CIFS
 - Autohome, partage
 - Configuration 121
 - Paramétrage, Telnet 233
 - Compliance Archiving Software 271
 - Configuration des clients
 - DOS 120
 - Windows 120
 - Définition 113
 - Mappage de lettre d'unité 229
 - Partages statiques
 - À propos 113
 - Ajout 115
 - Configuration 114
 - Création 115
 - Effacement 119
 - Modification 118
 - Paramétrage, Telnet 232
 - Sécurité 116
 - Restrictions liées au nom du partage 115, 118
- Clients
 - Configuration 119
 - DOS 120
 - Windows 120
- Cluster
 - Activation du basculement de tête 18
 - Rôles du port 23
- Compliance Archiving Software 148
 - API 283
 - Configuration 271
- Composants
 - Matériels 298
 - Panneau arrière 298
- Configuration
 - Adaptateurs réseau 22
 - ADS 25
 - IG 89
 - Telnet 236
 - Autohome, partage
 - IG 121
 - Telnet 233
 - Basculement, Telnet 265
 - Clients SMB/CIFS 119
 - Compliance Archiving Software 271
 - Date 71
 - Telnet 219

- DNS
 - IG 27
 - Telnet 224
- DNS dynamique, Telnet 224
- Exécution de l'assistant 7
- Exportations NFS 129
- FTP 178, 260
- Fuseau horaire
 - IG 71
 - Telnet 219
- Groupe
 - Privilèges 96
 - Privilèges, Telnet 239
 - Quotas 123
- Groupes d'utilisateurs, Telnet 237
- Heure 71
 - Telnet 219
- Hôtes, IG 99
- Journalisation 34
 - À distance, Telnet 224
 - Locale, Telnet 224
- Lancement de l'assistant 8
- Langue
 - IG 36
 - Telnet 223
- LDAP 93
- Lettres d'unités dans Telnet 229
- Mise en miroir de volumes de fichiers
 - IG 138
 - Telnet 248
- Mise en miroir, Telnet 246
- NDMP
 - IG 187
 - Telnet 271
- NIC 22
- NIS 29
 - Telnet 227
- NIS+ 30
 - Telnet 227
- Nom du serveur 12
- Notification par e-mail 33
 - Telnet 255
- NTP 69
 - Telnet 219
- Options de l'assistant 7
- Partages statiques
 - IG 114
 - Telnet 232
- Passerelle, adresse 24
- Ports
 - IG 22
 - Mise en miroir 137
 - Telnet 217
- Privilèges
 - IG 99
 - Telnet 239
- Quotas
 - Structures de répertoire 127
 - Utilisateurs 123
- RDATE 70
 - Telnet 220
- Rétablissement, Telnet 266
- Sauvegarde, Telnet 270
- Sécurité Windows 24
- Serveur actif
 - IG 136
 - Telnet 246
- Serveur cible
 - IG 136
 - Telnet 246
- Serveur miroir
 - IG 136
 - Telnet 246
- Serveur source
 - IG 136
 - Telnet 246
- Services de noms 32
 - Telnet 224
- Seuils d'avertissement 141
- SMTP, Telnet 255
- SNMP
 - IG 156
 - Telnet 254
- Synchronisation horaire
 - IG 69
 - Telnet 219
- TCP/IP, elnet 217
- Vérification du DNS pour ADS 91
- WINS 27
- Conservation, Compliance Archiving Software 271
- Console 213
 - Verrouillage 245
- Conteneur, mise à jour des partages ADS 92
- Contrôle
 - Configuration SNMP 156
 - UPS 172
 - Activation 173

- Contrôleur
 - Basculement, activation 20
 - Informations, affichage 173
- Conventions, nom de serveur 12
- Création
 - Exportations NFS 129
 - Hôtes 100
 - Telnet 243
 - Hôtes de confiance
 - IG 100
 - Telnet 244
 - LUN 45
 - Partages statiques
 - IG 115
 - Telnet 234
 - Point de contrôle planifié, Telnet 270
 - Points de contrôle
 - IG 181
 - Telnet 270
 - Quotas
 - Groupes 124
 - Structures de répertoire 127
 - Utilisateurs 124
 - RAID 45
 - Segment 49
 - Telnet 231
 - Système de fichiers 44
 - Volume de fichiers 49
 - Telnet 229
- D**
- Date, définition 71
 - Telnet 219
- Dédié, port
 - Mise en miroir 137
 - Paramétrage du rôle du port 137
- Définition
 - Adresse de passerelle 24
 - Date 71
 - Telnet 219
 - Fuseau horaire 71
 - Telnet 219
 - Heure 71
 - Telnet 219
 - Langue, Telnet 223
 - LUN 45
 - Mot de passe administrateur 67
 - Nom du serveur 12
 - Ordre de recherche des services de noms 32
 - Telnet 228
 - Quotas
 - Groupes 123
 - Utilisateurs 123
 - RAID 45
 - Sécurité 111
 - Segment 49
 - Seuils d'avertissement
 - IG 141
 - Telnet 250
 - Volume de fichiers 49
- DEL de statut 297
- Délai d'attente de l'arrêt, définition 19
- Déverrouillage de la console 245
- DHCP, désactivation du basculement de tête 18
- DN, définition 26
- DNS
 - À propos 88
 - Paramétrage
 - IG 27
 - Telnet 224
 - Vérification de la configuration 91
- DNS dynamique
 - Activation 28
 - Paramétrage, Telnet 224
- Domaine, sécurité 25
- DOS, configuration pour SMB/CIFS 120
- Droits d'accès, définition 96
- DTQ
 - Définition 127
 - Voir Quotas de structures de répertoire
- E**
- Effacement
 - Exportations NFS 131
- Hôtes
 - IG 101
 - Telnet 243
- Hôtes de confiance
 - IG 101
 - Telnet 244
- Membres de groupe
 - IG 98
 - Telnet 238

- Partages statiques
 - IG 119
 - Telnet 235
- Point de contrôle 185
 - Planifié 184
- Quotas de structures de répertoire 129
- Volume de fichiers, Telnet 232
- E-mail de diagnostic, envoi 305
- Ensemble redondant de disques indépendants, voir RAID
- Entrelacement, définition 40
- Environnement, statut
 - Affichage 163
 - Alimentation système 165
 - Température 164
 - Tension 165
 - Ventilateurs système 163
- Envoi d'un e-mail de diagnostic 305
- Erreurs liées au sous-système
 - RAID 278
 - UPS 274
- Erreurs liées au système de fichiers 277
- Événements
 - Avertissement, journal système 160
 - Avis, journal système 160
 - Critiques, journal système 160
 - Débogage, journal système 160
 - Erreur, journal système 160
 - Information, journal système 160
 - IPMI 279
 - Journal système 160
 - Journalisation dans Telnet 225
 - Urgence, journal système 160
- Exécution
 - Assistant de configuration 7
 - Nettoyage des têtes 189
- Exigences
 - Mise en miroir 135
 - Nom du serveur 12
- Exportation
 - Création 129
 - Effacement 131
 - Modification 131
 - Paramétrage 129

F

- File Replicator 135
- FTP
 - Accès 179, 261
 - Configuration 178, 260

G

- Gestion
 - Accès au volume de fichiers, Telnet 245
 - Basculement, Telnet 264
 - Hôtes de confiance, Telnet 244
 - Quotas 123
 - Route, Telnet 223
- Groupe
 - Administrateur 96
 - Ajout de membres
 - IG 98
 - Telnet 238
 - Opérateurs de sauvegarde 96
 - Privilèges
 - IG 96
 - Telnet 239
 - Quotas
 - Ajout 124
 - Configuration 123
 - Modification 125
 - Par défaut 123
 - Références, mappage 101
 - Root, quotas 124
 - Suppression de membres
 - IG 98
 - Telnet 238
 - Utilisateur, à propos 95
 - Utilisateurs avec pouvoir 96
- Groupe de travail, sécurité, activation 25

H

- Haute disponibilité, basculement 18
 - Liaison, activation 19
- Heure
 - Définition 71
 - Telnet 219
 - Synchronisation
 - À propos 69
 - Définition, Telnet 219
 - NTP 69
 - Paramétrage 69
 - RDATE 69

- Zone, définition 71
 - Telnet 219
- Hot spare, affectation 48
- Hôtes
 - Ajout 100
 - Telnet 243
 - Attribution de nom 100
 - Configuration 99
 - De confiance 100
 - Ajout, Telnet 244
 - Configuration 99
 - Effacement 101
 - Suppression, Telnet 244
 - Telnet 244
 - Effacement 101
 - Modification 100
 - Telnet 243
 - Route 170
 - Suppression, Telnet 243
- Hôtes de confiance
 - À propos 100
 - Ajout
 - IG 100
 - Telnet 244
 - Effacement 101
 - Gestion, Telnet 244
 - Suppression, Telnet 244
- I**
- Icônes de barre d'outils 2
- ID de groupe, définition 116
- ID utilisateur, définition 116
- Identification des emplacements de ports 21, 77
- IG
 - Aide en ligne 7
 - Barre d'outils 2
 - Définition 1
 - Panneau de contenu 6
 - Panneau des statuts 6
 - Utilisation 2
 - Volet de navigation 3
- Immédiats, points de contrôle, création 181
- Indépendant, rôle du port 78
- Indicateurs DEL, statut 297
- Interface de ligne de commande 213
- Interface graphique, voir Interface graphique (IG)

- Interrupteurs 297
 - Électriques 297
 - Panneau avant 297
- IP, adresse, définition d'alias 79
- IPMI, événements 279
- iSCSI, configuration 59
- iSNS, serveur 64

J

- Journalisation
 - Affichage du journal 158
 - Affichage du journal système
 - IG 158
 - Telnet 256
 - Distance, paramétrage, Telnet 224
 - Événements
 - Alerte 160
 - Avertissement 160
 - Avis 160
 - Critiques 160
 - Débogage 160
 - Erreur 160
 - Information 160
 - Système 160
 - Urgence 160
 - Fonctions 35
 - Journal de sauvegarde, IG 175
 - Local, paramétrage, Telnet 224
 - Paramétrage 34
 - Types d'événements 225
 - Utilitaires, Telnet 225
- Journalisation à distance
 - Paramétrage
 - Telnet 224
- Journalisation à distance, voir Journalisation
- Journalisation en local, voir Journalisation

K

- KDC, définition 26

L

- Lancement
 - Récupération
 - Contrôleur 20
 - Tête 20
 - Rétablissement, IG 20

- Langue
 - Affectation 36
 - Sélection, Telnet 223
 - LDAP
 - À propos 87
 - Activation 93
 - Configuration 93
 - Paramétrage 93
 - Lettres d'unité, configuration de Telnet 229
 - Liaison de ports 80
 - Affichage, Telnet 257
 - Système à deux serveurs 82
 - Limites
 - Dépassables 123
 - Fixes 123
 - Noms
 - Conteneur 90
 - Conteneur ADS 90
 - Domaine 25
 - Étendue 27
 - Hôte 100
 - NetBIOS 25
 - Partage 115, 118
 - Segment 49
 - Serveur 12
 - Volume de fichiers 49
 - Logiciels
 - File Replicator 135
 - Mise à jour 190
 - Mise en miroir 135
 - LUN
 - À propos 42
 - Ajout 45
 - Création 45
 - Définition 42
 - Reconstruction 53
 - LUN, chemin 15
 - À propos 13
 - Définition 17
 - Système à deux serveurs 16
- M**
- Macintosh
 - Appels à la base de données du bureau 116, 118
 - Prise en charge 116, 118
 - Mappage
 - Lettres d'unités, Telnet 229
 - Références 101
 - Menu principal de Telnet 216
 - Message, langue d'affichage 36
 - Messages d'erreur 273
 - Erreurs liées au sous-système
 - RAID 278
 - UPS 274
 - Erreurs liées au système de fichiers 277
 - IPMI, événements 279
 - SysMon 273
 - MIB, fichiers 156
 - Microprogramme
 - Mise à niveau 191
 - RAID, baie 192
 - Répertoires et fichiers 193
 - Miroir
 - Rôle de port 78
 - Serveur
 - Configuration 136
 - Configuration, Telnet 246
 - Définition 135
 - Paramétrage 136
 - Tampon
 - Définition 135
 - Seuils d'alerte 141
 - Miroirs individuels, statut depuis Telnet 257
 - Mise à jour
 - Conteneurs de partage ADS 92
 - Logiciels 190
 - Mise en miroir
 - À propos 135
 - Affichage, Telnet
 - Statistiques 259
 - Statut individuel 257
 - Avant de commencer 135
 - Changement 140
 - Configuration
 - Port dédié 137
 - Serveur actif, Telnet 246
 - Serveur cible, Telnet 246
 - Serveur miroir, Telnet 246
 - Serveur source, Telnet 246
 - Volume de fichiers, Telnet 248
 - Définition des seuils d'avertissement, Telnet 250
 - Désactivation
 - Miroir 142
 - Telnet 252
 - Exigences 135

- Modification 140
 - Paramétrage
 - Port dédié 137
 - Telnet 248
 - Volume de fichiers 138
 - Promotion du volume de fichiers
 - IG 143
 - Telnet 250
 - RAID, définition 40
 - Rétablissement d'un miroir
 - IG 144
 - Telnet 252
 - Serveur actif, définition 135
 - Serveur cible, définition 135
 - Serveur miroir, définition 135
 - Serveur source, définition 135
 - Statistiques d'utilisation 173
 - Statuts de l'état 175
 - Suppression du volume de fichiers, Telnet 253
 - Tampon miroir, définition 135
 - Telnet 246
- Modification**
- Exportations NFS 131
 - Hôtes 100
 - Telnet 243
 - Miroir 140
 - Ordre de recherche des services de noms 94
 - Partages statiques
 - IG 118
 - Telnet 235
 - Point de contrôle planifié 184
 - Quotas
 - Groupes 125
 - Structures de répertoire 128
 - Utilisateurs 125
 - Telnet, privilèges de groupe 239
 - Touches utilisées avec Telnet 215
- Moniteur d'activité, affichage, Telnet 256
- Mot de passe, administrateur, définition 67
- N**
- Navigation
 - Telnet 215
 - Web Administrator 1
 - NDMP
 - Définition 187
 - Paramétrage 187
 - Paramétrage dans Telnet 271
 - Network Data Management Protocol, voir NDMP
 - Network File System, voir NFS
 - Network Information Service Plus, voir NIS+
 - Network Information Service, voir NIS
 - Network Time Protocol, voir NTP
 - NFS
 - Définition 129
 - Exportation
 - Création 129
 - Effacement 131
 - Modification 131
 - Paramétrage 129
 - NIC
 - Configuration 22
 - Définition 21
 - NIS
 - À propos 88
 - Définition 8
 - Paramétrage 29
 - Telnet 227
 - NIS+
 - À propos 88
 - Définition 8
 - Paramétrage 30
 - Telnet 227
 - Niveaux de notification par e-mail 34
 - Nom
 - Chemin, ADS 90
 - Conteneur, limites 90
 - Domaine 25
 - Étendue 27
 - Hôtes 100
 - Limitation du NetBIOS 25
 - Restrictions liées au nom du partage 115, 118
 - Segment 49
 - Serveur
 - Conventions 12
 - Définition 12
 - Volume de fichiers 49
 - Notification par e-mail
 - Configuration, Telnet 255
 - Diagnostic, envoi 305
 - Niveaux de notification 34
 - Paramétrage 33
 - NSSLDAP, voir LDAP
 - NTP
 - Définition 69

- Paramétrage 69
 - Telnet 219
- Synchronisation horaire 69
 - Telnet 219
- Numéro d'unité logique, voir LUN

O

- Options
 - Activation 133
 - Assistant de configuration 7
 - Compliance Archiving Software 148, 271
 - API 283
 - Mise en miroir 135
- Ordre de recherche
 - Définition dans Telnet 228
 - Modification 94
 - Services de noms, vérification 90

P

- Panneau
 - Arrière, composants 298
 - Avant, interrupteurs 297
 - Contenu, utilisation 6
 - Interrupteurs à l'avant 297
- Paramétrage
 - Adaptateurs réseau 22
 - ADS 25
 - IG 89
 - Telnet 236
 - Autohome, partage
 - IG 121
 - Telnet 233
 - Basculement, telnet 265
 - Clients SMB/CIFS 119
 - Compliance Archiving Software 271
 - DNS
 - Dynamique, Telnet 224
 - IG 27
 - Telnet 224
 - Exportations NFS 129
 - FTP 178, 260
 - Hôtes 99
 - Journalisation
 - Locale, Telnet 224
 - Telnet 224
 - Langue 36
 - LDAP 93
 - Lettres d'unités, Telnet 229

- Mise en miroir
 - Telnet 248
 - Volumes de fichiers 138
- NDMP
 - IG 187
 - Telnet 271
- NIC 22
- NIS 29
 - Telnet 227
- NIS+ 30
 - Telnet 227
- Notification par e-mail 33
 - Telnet 255
- NTP 69
 - Telnet 219
- Partages statiques
 - IG 114
 - Telnet 232
- Ports
 - IG 22
 - Mise en miroir 137
 - Telnet 217
- Privilèges 99
 - De groupe 96
- Quotas de structures de répertoire 127
- RDATE 70
 - Telnet 220
- Récupération
 - Contrôleur 20
 - Tête 20
- Rétablissement 20
- Sauvegarde, Telnet 270
- Sécurité Windows 24
- Serveur actif
 - IG 136
 - Telnet 246
- Serveur cible
 - IG 136
 - Telnet 246
- Serveur miroir
 - IG 136
 - Telnet 246
- Serveur source
 - IG 136
 - Telnet 246
- Services de noms 32
- SNMP
 - IG 156
 - Telnet 254

- Synchronisation horaire 69
 - Telnet 219
 - TCP/IP, Telnet 217
 - WINS 27
- Parité, définition 41
- Partages 113
 - À propos 113
 - Autohome
 - À propos 121
 - Configuration 121
 - Paramétrage, Telnet 233
 - Mappage de lettres d'unités 229
 - Mise à jour des conteneurs ADS 92
 - Points de contrôle 185
 - Publication dans ADS 91
 - Restrictions liées au nom 115, 118
 - Statiques
 - À propos 113
 - Ajout, Telnet 234
 - Configuration 114
 - Création 115
 - Effacement 119
 - Modification 118
 - Modification, Telnet 235
 - Paramétrage, Telnet 232
 - Sécurité 116
 - Suppression, Telnet 235
 - Suppression d'ADS 93
- Partages statiques
 - À propos 113
 - Configuration 114
 - Création 115
 - Effacement 119
 - Modification 118
 - Restrictions liées au nom 115, 118
 - Sécurité 116
- Partition
 - À propos 42
 - Attribution d'un nouveau nom, Telnet 230
- Passerelle, adresse, définition 24
- Planification
 - Points de contrôle 182
 - Effacement 184
 - Modification 184
 - Telnet 270
- Points c, à propos 181
- Points de cohérence, à propos 181
- Points de contrôle
 - À propos 181
 - Accès 186
 - Ajout à la planification, Telnet 270
 - Analyse, affichage dans Telnet 257
 - Attribution d'un nouveau nom 185
 - Création 181
 - Effacement 185
 - Modification de la planification 184
 - Partage 185
 - Planification
 - IG 182
 - Telnet 270
 - Suppression 184
- Points de contrôle Sun StorEdge, voir Points de contrôle
- Ports
 - Affichage de la liaison de ports, Telnet 257
 - Configuration, Telnet 217
 - Emplacement, identification 21, 77
 - Liaison 80
 - Système à deux serveurs 82
 - Mise en miroir
 - Configuration 137
 - Paramétrage 137
 - Rôles 79
 - Affectation 23
 - Indépendant 78
 - Miroir 78
 - Paramétrage du port dédié 137
 - Principal 78
 - Privé 78
- Pouvoir, groupe d'utilisateurs 96
- Principal, rôle du port 78
- Prise en charge des niveaux RAID 39
- Privé, rôle du port 78
- Privilèges
 - Assignation de propriété 97
 - Configuration 99
 - Définition 96
 - Groupes d'utilisateurs 96
 - Superutilisateur 100
- Promotion, volume de fichiers
 - IG 143
 - Telnet 250
- Protection antivirus 72

Protocole classique de système de fichiers Internet,
voir CIFS
Protocole de transfert de fichiers, voir FTP
Protocole LDAP, voir LDAP
Protocole SMTP (Simple Mail Transfer Protocol),
voir SMTP
Protocole SNMP, voir SNMP
Publication de partages dans ADS 91

Q

Quarantaine, fichiers, suppression 75
Quotas
 Activation, Telnet 237
 Gestion 123
 Groupe
 Ajout 124
 Configuration 123
 Modification 125
 Par défaut 123
 Root 124
 Limites
 Dépassables 123
 Fixes 123
 Structure de répertoire
 Ajout 127
 Configuration 127
 Modification 128
 Suppression 129
 Superutilisateur 124
 Utilisateur
 Ajout 124
 Configuration 123
 Modification 125
 Par défaut 123
 Suppression 126
Quotas de structures de répertoire
 Ajout 127
 Configuration 127
 Modification 128
 Suppression 129
Quotas par défaut
 Groupe 123
 Utilisateur 123

R

RAID
 À propos 39
 Ajout 45
 Baie, microprogramme 192
 Création 45
 Définition de la mise en miroir 40
 Entrelacement, définition 40
 Jeux 39
 Messages d'erreur 278
 Niveaux pris en charge 39
 Parité, définition 41
raidctl profile, commande 200
Rattachement de segments, Telnet 231
RDATE
 Paramétrage 70
 Telnet 220
 Synchronisation horaire 69
 Telnet 220
Reconstruction, LUN 53
Récupération, lancement 20
Redémarrage
 Serveur 180
 Telnet 264
Références, mappage 101
Réseau
 Activité, statistiques d'utilisation 167
 Route 170
 Affichage 171
 Statistiques 170
Réseau, carte d'interface, voir NIC
Restauration
 Délai d'attente, définition 19
 Nettoyage des têtes 189
Rétablissement
 Configuration, Telnet 266
 Définition 19
 Lancement, IG 20
Rétablissement d'un miroir
 IG 144
 Mise en miroir du volume à jour
 IG 146
 Telnet 253
 Séparation du miroir
 IG 145
 Telnet 252

- Suppression du volume de fichiers obsolète
 - IG 145
 - Telnet 253
 - Telnet 252
- Route
 - À propos 170
 - Affichage 171
 - Gestion dans Telnet 223
 - Hôte 170
 - Indicateurs 170
- S**
- Sauvegarde
 - Affichage
 - Journal 175
 - Statut de la bande 176
 - Statut de la tâche 176
 - Configuration, Telnet 270
 - Groupe d'opérateurs 96
 - NDMP
 - IG 187
 - Telnet 271
 - Nettoyage des têtes 189
- Sécurité
 - Accès au volume de fichiers, Telnet 245
 - Définition 111
 - Déverrouillage de la console 245
 - Mot de passe administrateur 67
 - Partages statiques 116
 - Répertoire de fichiers 110
 - Verrouillage de la console 245
 - Windows 24
- Segment
 - À propos 43
 - Ajout, Telnet 231
 - Création 49
 - Rattachement, Telnet 231
 - Restrictions liées au nom 49
- Sélection d'une langue, Telnet 223
- Séparation
 - IG 142
 - Serveur 1
 - IG 145
 - Telnet 252
 - Telnet 252
- Server Message Block, voir SMB
- Serveur
 - Arrêt 180
 - Basculement de tête 18
 - Nom
 - Conventions 12
 - Définition 12
 - Redémarrage 180
 - Rétablissement 19
 - Tête, définition 18
- Serveur actif
 - Configuration
 - IG 136
 - Telnet 246
 - Mise en miroir
 - Définition 135
 - Telnet 246
- Serveur cible
 - Configuration
 - IG 136
 - Telnet 246
 - Définition 135
 - Mise en miroir, Telnet 246
- Serveur source
 - Configuration
 - IG 136
 - Telnet 246
 - Mise en miroir
 - Définition 135
 - Telnet 246
- Services de noms
 - Configuration 32
 - Définition de l'ordre de recherche, Telnet 228
 - DNS 32
 - Locaux 32
 - Modification de l'ordre de recherche 94
 - NIS 32
 - NIS+ 32
 - Vérification de l'ordre de recherche 90
- Seuil 141
- Seuils d'avertissement
 - À propos 141
 - Définition
 - IG 141
 - Telnet 250
- Seuils, définition
 - IG 141
 - Telnet 250

- SMB
 - Autohome, partage
 - Activation 121
 - Configuration 121
 - Configuration
 - Clients 119
 - Clients DOS 120
 - Clients Windows 120
 - Définition 113
 - Mappage de lettre d'unité 229
 - Paramétrage
 - Partages autohome, Telnet 233
 - Partages statiques, Telnet 232
 - Partages statiques
 - À propos 113
 - Activation 115
 - Ajout 115
 - Changement 118
 - Configuration 114
 - Création 115
 - Effacement 119
 - Modification 118
 - Suppression 119
 - Restrictions liées au nom du partage 115, 118
 - Sécurité, partages statiques 116
- SMTP, définition 33
- SNMP
 - Configuration
 - IG 156
 - Telnet 254
 - Définition 156
- Statistiques d'utilisation
 - Activité réseau 167
 - Activité système 168
 - Mise en miroir 173
 - Volume de fichiers 167
- Statut 157
 - Activité réseau 167
 - Activité système 168
 - Alimentation 165
 - Bandes de sauvegarde 176
 - Environnement, affichage 163
 - Indicateur DEL 297
 - Informations sur le contrôleur 173
 - Miroir individuel, Telnet 257
 - Mise en miroir
 - IG 173
 - Telnet 257
 - Route réseau 170
 - Statistiques d'un miroir, Telnet 259
 - Statuts de miroir 175
 - Système 297
 - Tâches de sauvegarde 176
 - Température 164
 - Tension 165
 - UPS 172
 - Utilisation du volume de fichiers 167
 - Ventilateurs 163
- Sun StorEdge 5310 NAS Appliance
 - Composants du panneau arrière 298
 - DEL de statut 297
 - Interrupteurs 297
- Superutilisateur
 - Privilèges définis par l'état de l'hôte 100
 - Quotas 124
- Suppression
 - Exportations NFS 131
 - Fichiers en quarantaine 75
 - Hôtes
 - IG 101
 - Telnet 243
 - Hôtes de confiance
 - IG 101
 - Telnet 244
 - Membres de groupe
 - IG 98
 - Telnet 238
 - Partages d'ADS 93
 - Partages statiques
 - IG 119
 - Telnet 235
 - Point de contrôle 185
 - Point de contrôle planifié 184
 - Quotas d'utilisateurs 126
 - Quotas de structures de répertoire 129
 - Volume de fichiers
 - En miroir, Telnet 253
 - Telnet 232
 - Volume de fichiers obsolète
 - IG 145
 - Telnet 253
- Synchronisation 69
 - Synchronisation horaire
 - À propos 69
 - Paramétrage 69
 - Telnet 219

- syslogd, définition 34
- SysMon, à propos 273
- Système
 - Arrêt
 - IG 180
 - Telnet 264
 - Événements, affichage 160
 - Journal
 - Affichage 158
 - Affichage, Telnet 256
 - Statistiques d'utilisation des activités 168
 - Statut, panneau, utilisation 6
- Système à deux serveurs
 - Activation du basculement de tête 18
 - Telnet 265
 - Alias IP 79
 - Liaison de ports 82
 - Rôles du port 23
- Système de fichiers
 - Création 44
 - Gestion dans Telnet 229
 - Messages d'erreur 277

T

- TCP/IP, configuration, Telnet 217
- Telnet
 - Activation de quotas 237
 - Affichage
 - Analyse de points de contrôle 257
 - Journal système 256
 - Liaison de ports 257
 - Moniteur d'activité 256
 - Statistiques de miroir 259
 - Statut d'un miroir individuel 257
 - Statut, miroir 257
 - Ajout
 - Hôtes 243
 - Hôtes de confiance 244
 - Membres de groupe 238
 - Partages 234
 - Points de contrôle 270
 - Segments 231
 - Arrêt 264
 - Attribution d'un nouveau nom à une partition 230
 - Configuration
 - Basculement 265
 - Groupes d'utilisateurs 237

- Lettres d'unités 229
- Mise en miroir de volumes de fichiers 248
- Notification par e-mail 255
- Rétablissement 266
- Sauvegarde 270
- Serveur actif 246
- Serveur cible 246
- Serveur miroir 246
- Serveur source 246
- SNMP 254
- TCP/IP 217
- Création de volumes de fichiers 229
- Définition
 - Date 219
 - Fuseau horaire 219
 - Heure 219
 - Ordre de recherche des services de noms 228
 - Seuils d'avertissement 250
 - Synchronisation horaire 219
- Déverrouillage de la console 245
- Gestion
 - Accès au volume de fichiers 245
 - Basculement 264
 - Hôtes de confiance 244
 - Route 223
 - Système de fichiers 229
- Journalisation
 - Événements 225
 - Utilitaires 225
- Menu principal 216
- Menus 215
- Mise en miroir 246
 - Affichage du statut 257
 - Promotion du volume de fichiers 250
 - Séparation 252
- Modification
 - Hôtes 243
 - Partages 235
 - Privilèges de groupe 239
- Navigation 215
- Paramétrage
 - ADS 236
 - Autohome, partage 233
 - DNS 224
 - DNS dynamique 224
 - Journalisation 224
 - Journalisation locale 224
 - Miroir 248
 - NDMP 271

- NIS 227
- NIS+ 227
- NTP 219
- Partages statiques 232
- RDATE 220
- Planification, points de contrôle 270
- Redémarrage 264
- Rétablissement d'un miroir 252
- Sélection d'une langue 223
- Séparation 252
- Suppression
 - Hôtes 243
 - Hôtes de confiance 244
 - Membres d'un groupe 238
 - Partages 235
 - Volume de fichiers 232
 - Volume de fichiers en miroir 253
- Touches de modification 215
- Verrouillage de la console 245
- Température, statut 164
- Tension, statut 165
- Tête
 - Basculement, définition 18
 - Définition 18
 - Nettoyage 189

U

- umask 117
- Unité, mise à niveau du microprogramme 191
- UNIX, paramètres
 - Mappage 108, 109
 - Ordre de recherche des services de noms 32
- UPS
 - Activation du contrôle 173
 - Contrôle 172
 - Définition 172
 - Messages d'erreur 274
- Utilisateur
 - Groupes
 - À propos 95
 - Ajout de membres, Telnet 238
 - Configuration, Telnet 237
 - Modification des privilèges, Telnet 239
 - Privilèges 96
 - Suppression de membres, Telnet 238

- Quotas
 - Ajout 124
 - Configuration 123
 - Modification 125
 - Par défaut 123
 - Suppression 126
- Références, mappage 101
- Root, quotas 124

Utilisation

- Aide en ligne 7
- Barre d'outils 2
- IG 2
- Panneau de contenu 6
- Panneau des statuts 6
- Volet de navigation 3
- Utilitaire, Telnet 225

V

- Ventilateur, statut 163
- Vérification
 - Configuration DNS 91
 - Ordre de recherche des services de noms 90
- Verrouillage de la console 245
- Virus, analyse 75
- Volet de navigation, uUtilisation 3
- Volume de fichiers
 - À propos 43
 - Autohome, partage
 - À propos 121
 - Telnet 233
 - Création 49
 - Telnet 229
 - Extension, Telnet 231
 - Gestion de l'accès, Telnet 245
 - Mise en miroir
 - IG 138
 - Telnet 248
 - Mise en miroir du volume à jour
 - IG 146
 - Telnet 253
 - Partages statiques
 - À propos 113
 - Telnet 232
 - Promotion
 - IG 143
 - Telnet 250
 - Restrictions liées au nom 49

- Rétablissement d'un miroir
 - IG 144
 - Telnet 252
- Statistiques d'utilisation 167
- Suppression du volume de fichiers obsolète
 - IG 145
 - Telnet 253
- Suppression, Telnet 232

W

Web Administrator

- Aide en ligne 7
- Barre d'outils 2
- IG 2
- Navigation 1
- Panneau de contenu 6
- Panneau des statuts 6
- Volet de navigation 3

Windows

- Autohome, à propos du partage 121
- Configuration SMB/CIFS 120
- Domaine, activation 25
- Groupe de travail
 - Activation 25
 - Sécurité 116
 - Sécurité du répertoire de fichiers 110
- Mappage de références 108
- Partages statiques, à propos 113
- Sécurité, modèles 24

WINS

- À propos 88
- Paramétrage 27

