

**Guide d'administration des systèmes
Oracle® ZFS Storage Appliance,
version OS8.6.0**



Référence: E74754-01
Juillet 2016

Référence: E74754-01

Copyright © 2009, 2016, Oracle et/ou ses affiliés. Tous droits réservés.

Ce logiciel et la documentation qui l'accompagne sont protégés par les lois sur la propriété intellectuelle. Ils sont concédés sous licence et soumis à des restrictions d'utilisation et de divulgation. Sauf stipulation expresse de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, accorder de licence, transmettre, distribuer, exposer, exécuter, publier ou afficher le logiciel, même partiellement, sous quelque forme et par quelque procédé que ce soit. Par ailleurs, il est interdit de procéder à toute ingénierie inverse du logiciel, de le désassembler ou de le décompiler, excepté à des fins d'interopérabilité avec des logiciels tiers ou tel que prescrit par la loi.

Les informations fournies dans ce document sont susceptibles de modification sans préavis. Par ailleurs, Oracle Corporation ne garantit pas qu'elles soient exemptes d'erreurs et vous invite, le cas échéant, à lui en faire part par écrit.

Si ce logiciel, ou la documentation qui l'accompagne, est livré sous licence au Gouvernement des Etats-Unis, ou à quiconque qui aurait souscrit la licence de ce logiciel pour le compte du Gouvernement des Etats-Unis, la notice suivante s'applique :

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

Ce logiciel ou matériel a été développé pour un usage général dans le cadre d'applications de gestion des informations. Ce logiciel ou matériel n'est pas conçu ni n'est destiné à être utilisé dans des applications à risque, notamment dans des applications pouvant causer un risque de dommages corporels. Si vous utilisez ce logiciel ou matériel dans le cadre d'applications dangereuses, il est de votre responsabilité de prendre toutes les mesures de secours, de sauvegarde, de redondance et autres mesures nécessaires à son utilisation dans des conditions optimales de sécurité. Oracle Corporation et ses affiliés déclinent toute responsabilité quant aux dommages causés par l'utilisation de ce logiciel ou matériel pour des applications dangereuses.

Oracle et Java sont des marques déposées d'Oracle Corporation et/ou de ses affiliés. Tout autre nom mentionné peut correspondre à des marques appartenant à d'autres propriétaires qu'Oracle.

Intel et Intel Xeon sont des marques ou des marques déposées d'Intel Corporation. Toutes les marques SPARC sont utilisées sous licence et sont des marques ou des marques déposées de SPARC International, Inc. AMD, Opteron, le logo AMD et le logo AMD Opteron sont des marques ou des marques déposées d'Advanced Micro Devices. UNIX est une marque déposée de The Open Group.

Ce logiciel ou matériel et la documentation qui l'accompagne peuvent fournir des informations ou des liens donnant accès à des contenus, des produits et des services émanant de tiers. Oracle Corporation et ses affiliés déclinent toute responsabilité ou garantie expresse quant aux contenus, produits ou services émanant de tiers, sauf mention contraire stipulée dans un contrat entre vous et Oracle. En aucun cas, Oracle Corporation et ses affiliés ne sauraient être tenus pour responsables des pertes subies, des coûts occasionnés ou des dommages causés par l'accès à des contenus, produits ou services tiers, ou à leur utilisation, sauf mention contraire stipulée dans un contrat entre vous et Oracle.

Accessibilité de la documentation

Pour plus d'informations sur l'engagement d'Oracle pour l'accessibilité à la documentation, visitez le site Web Oracle Accessibility Program, à l'adresse <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Accès aux services de support Oracle

Les clients Oracle qui ont souscrit un contrat de support ont accès au support électronique via My Oracle Support. Pour plus d'informations, visitez le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> ou le site <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> si vous êtes malentendant.

Table des matières

A propos d'Oracle ZFS Storage Appliance	17
Fonctionnalités clés d'Oracle ZFS Storage Appliance	17
Protocoles pris en charge	18
Services de données pour l'appareil	18
Disponibilité des données	19
Interface utilisateur de navigateur (BUI, Browser User Interface)	20
Icônes de réseau	27
Icônes du tableau de bord	27
Icônes de la barre d'outils d'analyse	28
Icônes de mappage des identités	29
Navigateurs pris en charge	29
Interface de ligne de commande (CLI, Command Line Interface)	30
Contextes de la CLI	31
Propriétés de la CLI	37
Utilisation de l'écriture de scripts CLI	40
Utilisation des commandes de traitement par lots	40
Présentation des commandes d'écriture de script CLI	41
▼ Accès à l'environnement de script CLI	42
Présentation des fonctions CLI intégrées	42
▼ Utilisation de la fonction run	43
▼ Utilisation de la fonction get	43
▼ Utilisation de la fonction list	44
▼ Utilisation de la fonction children	47
▼ Utilisation de la fonction Choices	48
Utilisation des fonctions pour la génération des sorties	49
Présentation des erreurs de script CLI	49
 Configuration de l'appareil	51
Configuration initiale de l'appareil	51
Configuration réseau	51
Configuration réseau (BUI)	52

Configuration réseau (CLI)	64
Utilisation de la page de configuration réseau	73
Configuration de l'interface de gestion	74
Configuration des liaisons de données réseau	75
Configuration des interfaces réseau	77
Configuration du multiacheminement IP (IPMP) réseau	79
Configuration des performances et de la disponibilité réseau	80
Configuration du routage réseau	81
Configuration du stockage	84
▼ Création d'un pool de stockage (BUI)	85
▼ Création d'un pool de stockage (CLI)	87
▼ Importation d'un pool de stockage existant (BUI)	89
▼ Importation d'un pool de stockage existant (CLI)	90
▼ Ajout d'une étagère de disques à un pool de stockage existant (BUI)	91
▼ Ajout d'une étagère de disques à un pool de stockage existant (CLI)	93
▼ Ajout d'un périphérique de cache ou de journal à un pool de stockage existant (BUI)	95
▼ Ajout d'un périphérique de cache ou de journal à un pool de stockage existant (CLI)	97
▼ Suppression d'un périphérique de cache ou de journal d'un pool de stockage existant (BUI)	99
▼ Suppression d'un périphérique de cache ou de journal d'un pool de stockage existant (CLI)	99
▼ Annulation de la configuration d'un pool de stockage (BUI)	101
▼ Annulation de la configuration d'un pool de stockage (CLI)	101
▼ Modification du nom d'un pool de stockage (BUI)	102
▼ Modification du nom d'un pool de stockage (CLI)	103
▼ Nettoyage d'un pool de stockage (BUI)	104
▼ Nettoyage d'un pool de stockage (CLI)	105
▼ Consultation du statut des pools et des périphériques (BUI)	106
Concepts liés aux pools de stockage	107
Profils de données pour les pools de stockage	108
Présentation du statut de l'appareil	111
Statut sur le tableau de bord	112
Résumé de l'utilisation de la mémoire	117
Tableau de bord d'activité du disque	118
CLI du tableau de bord	120
▼ Exécution continue de l'écran Tableau de bord	122
Paramètres de statut du tableau de bord	122
▼ Modification des statistiques d'activité affichées	124

▼ Modification des seuils d'activité	125
Statut NDMP	125
Etats NDMP	127
Configuration du réseau de stockage SAN	127
▼ Configuration des modes de port FC (BUI)	128
▼ Détection de ports FC (BUI)	129
▼ Création de groupes d'initiateurs FC (BUI)	131
▼ Association d'un LUN à un groupe d'initiateurs FC (BUI)	132
▼ Changement de mode de port FC (CLI)	134
▼ Détection de ports FC (CLI)	134
▼ Création de groupes d'initiateurs FC (CLI)	135
▼ Association d'un LUN à un groupe d'initiateurs FC (CLI)	136
▼ Scripts de création d'alias pour les initiateurs et groupes d'initiateurs (CLI)	136
▼ Création d'une feuille de travail Analyse (BUI)	138
▼ Configuration des cibles SAN iSER	139
▼ Ajout d'une cible iSCSI possédant un IQN généré de manière automatique (CLI)	141
▼ Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné (CLI)	142
▼ Ajout d'un initiateur iSCSI utilisant l'authentification CHAP (CLI)	143
▼ Ajout d'un groupe de cibles iSCSI (CLI)	144
▼ Ajout d'un groupe d'initiateurs iSCSI (CLI)	144
▼ Configuration des cibles SRP (BUI)	145
▼ Configuration des cibles SRP (CLI)	146
Présentation de SAN	147
Configuration Fibre Channel SAN	149
Configuration SAN iSCSI	153
Configuration de l'initiateur SAN iSCSI	155
Configuration SAN SRP	156
Terminologie SAN	158
Configuration des utilisateurs	160
▼ Ajout d'un administrateur ou d'un utilisateur (BUI)	160
▼ Ajout d'un administrateur ou d'un utilisateur (CLI)	162
▼ Modification d'un mot de passe utilisateur (BUI)	164
▼ Modification d'un mot de passe utilisateur (CLI)	164
▼ Modification des exceptions liées à un utilisateur (BUI)	165
▼ Modification des exceptions liées à un utilisateur (CLI)	166
▼ Suppression des exceptions liées à un utilisateur (BUI)	168
▼ Suppression des exceptions liées à un utilisateur (CLI)	168

▼ Ajout d'un rôle (BUI)	169
▼ Ajout d'un rôle (CLI)	170
▼ Modification des autorisations liées à un rôle (BUI)	171
▼ Modification des autorisations liées à un rôle (CLI)	172
▼ Suppression des autorisations d'un rôle (BUI)	173
▼ Suppression des autorisations d'un rôle (CLI)	174
▼ Ajout d'un utilisateur autorisé à afficher le tableau de bord	175
Présentation des utilisateurs et des rôles	175
Autorisations utilisateur	176
Gestion des propriétés utilisateur	177
Configuration des préférences pour l'appareil	179
▼ Configuration des préférences (BUI)	180
▼ Configuration des préférences (CLI)	180
▼ Configuration des clés publiques SSH (BUI)	182
▼ Configurations des clés publiques SSH (CLI)	182
Propriétés des préférences	183
Configuration des alertes	184
▼ Ajout d'une action d'alerte (BUI)	185
▼ Ajout d'une action d'alerte (CLI)	185
Envoi d'alertes par e-mail (CLI)	186
Envoi d'un déroutement SNMP (CLI)	187
Catégories d'alertes	188
Alertes avec seuil	189
Reprise/suspension de feuilles de travail et d'ensembles de données de l'analyse	190
Configuration d'appareils en cluster	191
Vue de la BUI de configuration du cluster	192
▼ Mise à niveau d'un appareil autonome vers une configuration clustérisée (BUI)	194
▼ Arrêt de la configuration clustérisée (BUI)	195
▼ Arrêt de la configuration clustérisée (CLI)	197
Terminologie du cluster	199
Présentation du clustering	200
Avantages et inconvénients des clusters	201
E/S d'interconnexion de cluster	203
Gestion des ressources du cluster	206
Reprise et rétablissement du cluster	209
Modifications de la configuration dans un environnement clustérisé	212
Considérations relatives au clustering pour le stockage	213
Considérations relatives au clustering pour la gestion réseau	215

Interfaces IP locales privées	217
Considérations relatives au clustering pour Infiniband	218
Prévention des états split-brain	220
Estimation et réduction de l'impact de la reprise	222
Services de l'appareil	225
Gestion des services	226
▼ Affichage d'un service dans la BUI	226
▼ Sélection d'un service dans la CLI	227
▼ Activation d'un service (BUI)	227
▼ Activation d'un service (CLI)	227
▼ Désactivation d'un service (BUI)	228
▼ Désactivation d'un service (CLI)	228
▼ Affichage des états d'un service dans la CLI	229
▼ Affichage de l'aide d'un service dans la CLI	229
▼ Définition des propriétés du service (BUI)	230
▼ Définition des propriétés du service (CLI)	231
▼ Affichage des journaux de service (BUI)	232
▼ Affichage des journaux de service (CLI)	233
Liste des services disponibles	233
Ports de service requis	235
Configuration des services	236
Configuration NFS	237
Configuration iSCSI	242
Configuration SMB	243
Configuration FTP	261
Configuration HTTP	263
Configuration NDMP	266
Configuration de la migration shadow	276
Configuration SFTP	276
Configuration SRP	279
Configuration TFTP	280
Configuration de l'analyse antivirus	280
Configuration NIS	284
Configuration LDAP	285
Configuration d'Active Directory	293
Configuration du mappage des identités	299
Configuration du DNS	310
Configuration IPMP	314

Configuration NTP	314
Configuration de Phone Home	318
Configuration du routage dynamique	321
Configuration des indicateurs de maintenance	321
Configuration SMTP	322
Configuration SNMP	322
Configuration Syslog	326
Configuration de l'identité du système	332
Configuration SSH	340
Configuration de l'API RESTful	341
Partages et projets	343
▼ Création d'un projet (BUI)	344
▼ Création d'un projet (CLI)	344
▼ Modification d'un projet (BUI)	346
▼ Modification d'un projet (CLI)	346
▼ Modification du nom d'un projet (BUI)	348
▼ Modification du nom d'un projet (CLI)	348
▼ Suppression d'un projet (BUI)	349
▼ Suppression d'un projet (CLI)	349
▼ Création d'un système de fichiers ou d'un LUN dans un projet (BUI)	350
▼ Création d'un système de fichiers ou d'un LUN dans un projet (CLI)	350
▼ Modification d'un système de fichiers ou d'un LUN (BUI)	353
▼ Modification d'un système de fichiers ou d'un LUN (CLI)	353
▼ Modification du nom d'un système de fichiers ou d'un LUN (BUI)	355
▼ Modification du nom d'un système de fichiers ou d'un LUN (CLI)	356
▼ Déplacement d'un système de fichiers ou d'un LUN vers un autre projet (BUI)	356
▼ Déplacement d'un système de fichiers ou d'un LUN vers un autre projet (CLI)	357
▼ Suppression d'un système de fichiers ou d'un LUN (BUI)	357
▼ Suppression d'un système de fichiers ou d'un LUN (CLI)	358
▼ Configuration des quotas d'utilisateurs ou de groupes (BUI)	359
▼ Configuration des quotas d'utilisateurs ou de groupes (CLI)	360
A propos des pools de stockage, des projets et des partages	361
Propriétés des projets et partages	363
Propriétés héritées	364
Propriétés locales du LUN	371
Autres propriétés	372
Propriétés statiques	373
Propriétés des projets	377

Propriétés des systèmes de fichiers	384
Propriétés du LUN	394
Gestion de l'espace pour les partages	400
Terminologie relative aux partages	401
Gestion de l'espace du système de fichiers et du projet	402
Configuration des quotas d'utilisateurs ou de groupes	403
Utilisation de la gestion des identités	404
Utilisation de l'espace de noms du système de fichiers	404
Statistiques d'utilisation des partages	406
Protocoles de partage et de projet	407
Protocole NFS	408
Protocole SMB	414
Protocole HTTP	419
Protocole FTP	419
Protocole SFTP	419
Protocole TFTP	420
Listes de contrôle d'accès des systèmes de fichiers	420
Accès au répertoire racine	420
Comportement ACL en cas de changement de mode	421
Comportement d'héritage ACL	422
ACL du répertoire racine	424
Utilisation des schémas	427
▼ Création d'un schéma (BUI)	428
▼ Création d'un schéma (CLI)	428
Propriétés de schéma	429
Migration shadow	431
Présentation de la migration shadow	432
Création d'un système de fichiers shadow	435
Gestion de la migration en arrière-plan	435
Gestion des erreurs de migration	435
Contrôle de la progression de la migration	436
Annulation d'une migration	436
Instantanés de systèmes de fichiers shadow	437
Sauvegarde de systèmes de fichiers shadow	437
Réplication de systèmes de fichiers shadow	437
Migration de systèmes de fichiers locaux	438
Utilisation des analyses de migration shadow	438
▼ Test d'une migration shadow potentielle à l'aide de la CLI	439

▼ Migration des données à partir d'un serveur NFS actif à l'aide de la CLI	439
Instantanés et clones	441
Gestion de l'espace pour les instantanés	443
▼ Réalisation d'un instantané (BUI)	444
▼ Réalisation d'un instantané (CLI)	445
▼ Planification des instantanés (BUI)	446
▼ Planification des instantanés (CLI)	448
▼ Définition d'une étiquette d'instantané planifié (BUI)	450
▼ Définition d'une étiquette d'instantané planifié (CLI)	451
▼ Affichage des instantanés et des calendriers (BUI)	451
▼ Affichage des instantanés et des calendriers (CLI)	452
▼ Modification d'une stratégie de conservation des instantanés (BUI)	454
▼ Modification d'une stratégie de conservation des instantanés (CLI)	454
▼ Suppression d'un calendrier d'instantané (BUI)	455
▼ Suppression d'un calendrier d'instantané (CLI)	456
▼ Affichage du répertoire d'instantanés du système de fichiers (BUI)	457
▼ Affichage du répertoire d'instantanés du système de fichiers (CLI)	458
▼ Accès à un répertoire d'instantanés masqué du système de fichiers (CLI)	459
▼ Accès à un répertoire d'instantanés visible du système de fichiers (CLI)	460
▼ Modification du nom d'un instantané (BUI)	460
▼ Modification du nom d'un instantané (CLI)	461
▼ Restauration d'un instantané (BUI)	462
▼ Restauration d'un instantané (CLI)	463
▼ Destruction d'un instantané (BUI)	464
▼ Destruction d'un instantané (CLI)	465
▼ Clonage d'un instantané (BUI)	466
▼ Clonage d'un instantané (CLI)	468
▼ Clonage d'un clone	470
▼ Affichage des clones d'un instantané (BUI)	470
▼ Affichage des clones d'un instantané (CLI)	471
▼ Affichage de l'origine d'un clone (BUI)	471
▼ Affichage de l'origine d'un clone (CLI)	472
Réplication distante	473
▼ Workflow de réplication distante	474
▼ Vérification de la compatibilité entre les appareils source et cible	474
▼ Configuration d'interfaces réseau et de routage statique (BUI)	475
▼ Configuration d'interfaces réseau et de routage statique (CLI)	477

▼ Création d'une cible de réplication (BUI)	478
▼ Création d'une cible de réplication (CLI)	479
▼ Création d'une action de réplication (BUI)	480
▼ Création d'une action de réplication (CLI)	482
▼ Configuration de la réplication pour un environnement de cluster	484
▼ Envoi manuel d'une mise à jour de réplication (BUI)	485
▼ Envoi manuel d'une mise à jour de réplication (CLI)	485
Création d'une réplication hors ligne (BUI)	486
▼ Configuration d'un serveur NFS pour une réplication hors ligne	486
▼ Configuration d'un chemin d'exportation vers le serveur NFS (BUI)	487
▼ Exportation d'une mise à jour de réplication (BUI)	487
▼ Vérification du flux de réplication sur le serveur NFS	488
▼ Importation du flux de réplication à partir du serveur NFS (BUI)	488
▼ Mise à jour manuelle de réseau (BUI)	489
▼ Inversion de la réplication pour une réplication hors ligne (BUI)	489
Création d'une réplication hors ligne (CLI)	490
▼ Configuration d'un serveur NFS pour une réplication hors ligne	491
▼ Configuration d'un chemin d'exportation vers le serveur NFS (CLI)	491
▼ Exportation d'une mise à jour de réplication (CLI)	492
▼ Vérification d'un flux de réplication sur le serveur NFS	494
▼ Importation d'un flux de réplication à partir du serveur NFS (CLI)	495
▼ Mise à jour manuelle de réseau (CLI)	496
▼ Inversion de la réplication pour une réplication hors ligne (CLI)	498
▼ Surveillance de la progression de la réplication (BUI)	501
▼ Surveillance de la progression de la réplication (CLI)	501
Alertes de réplication et événements d'audit	502
Utilisation des analyses de réplication	503
▼ Modification d'une cible de réplication (BUI)	503
▼ Modification d'une cible de réplication (CLI)	504
▼ Modification d'une mise à jour de réplication (BUI)	504
▼ Modification d'une mise à jour de réplication (CLI)	505
▼ Désactivation de la compression de réplication (BUI)	505
▼ Désactivation de la compression de réplication (CLI)	506
▼ Annulation d'une mise à jour de réplication (BUI)	507
▼ Annulation d'une mise à jour de réplication (CLI)	507
▼ Clonage d'un package de réplication (BUI)	508
▼ Clonage d'un package de réplication (CLI)	512
▼ Modification d'un package de réplication (BUI)	515
▼ Modification d'un package de réplication (CLI)	516
▼ Désactivation d'un package de réplication (BUI)	517

▼ Désactivation d'un package de réplication (CLI)	518
▼ Dissociation d'un package de réplication (BUI)	518
▼ Dissociation d'un package de réplication (CLI)	519
Configuration de réplication distante pour récupération après sinistre (BUI)	519
▼ Configuration d'un appareil cible sur un site de récupération (BUI)	520
▼ Basculement des opérations vers le site de récupération (BUI)	520
▼ Mise à jour du site de production (BUI)	521
▼ Inversion de la réplication vers le site de production (BUI)	522
Configuration de réplication distante pour récupération après sinistre (CLI)	522
▼ Configuration d'un appareil cible sur un site de récupération (CLI)	523
▼ Basculement des opérations vers le site de récupération (CLI)	524
▼ Mise à jour du site de production (CLI)	525
▼ Inversion de la réplication vers le site de production (CLI)	526
Utilisation de la réplication pour la sauvegarde disque à disque	528
Concepts de la réplication distante	529
Cibles de réplication	532
Actions et packages de réplication	533
Pools de stockage de réplication	534
Réplication de projet et réplication de partage	535
Autorisations de réplication	536
Configuration de la réplication pour les appareils en cluster	537
Exemple : Configuration de réplication pour des appareils en cluster	538
Instantanés de réplication et cohérence des données	545
Gestion des instantanés de réplication	546
Réplication et configurations iSCSI	547
Echecs de réplication	548
Propriétés des actions de réplication	551
Réplication compressée	552
Packages de réplication	553
Clonage d'un package de réplication ou d'un partage	554
Exportation de systèmes de fichiers répliqués	556
Dissociation de la réplication	557
Fonctionnement de la réplication inversée	557
Destruction d'un package de réplication	561
Sauvegardes de réplique cible	561
Chiffrement de données	563
▼ Workflow de chiffrement de données	564
▼ Configuration du chiffrement par le keystore LOCAL (BUI)	565

▼ Configuration du chiffrement par le keystore LOCAL (CLI)	567
▼ Configuration du chiffrement par le keystore OKM (BUI)	568
▼ Configuration du chiffrement par le keystore OKM (CLI)	569
▼ Création d'un projet chiffré (BUI)	570
▼ Création d'un projet chiffré (CLI)	571
▼ Modification d'une clé de chiffrement de projet (BUI)	572
▼ Modification de la clé de chiffrement d'un projet (CLI)	573
▼ Création d'un système de fichiers ou d'un LUN chiffré (BUI)	574
▼ Création d'un système de fichiers ou d'un LUN chiffré (CLI)	574
▼ Modification d'une clé de chiffrement de partage (BUI)	576
▼ Modification d'une clé de chiffrement de partage (CLI)	577
▼ Sauvegarde d'une clé locale (BUI)	578
▼ Sauvegarde d'une clé locale (CLI)	578
▼ Suppression d'une clé de chiffrement (BUI)	579
▼ Suppression d'une clé de chiffrement (CLI)	581
▼ Restauration d'une clé LOCAL (BUI)	582
▼ Restauration d'une clé LOCAL (CLI)	583
Propriétés de cryptage	584
Gestion des clés de chiffrement	585
Maintenance des clés	586
Présentation des valeurs de clés de chiffrement	586
Impact du chiffrement sur les performances	587
Cycle de vie d'une clé de chiffrement	588
Sauvegarde et restauration de données chiffrées	588
Réplication d'un partage chiffré	589
Maintenance des workflows	591
Présentation des workflows	591
Présentation des paramètres de workflow	592
Paramètres de workflow restreints	594
Paramètres de workflow facultatifs	595
Gestion des erreurs des workflows	596
Validation des entrées des workflows	597
Audits et rapports sur l'exécution des workflows	598
Présentation de la gestion des versions des workflows	600
Utilisation des workflows pour les actions d'alerte	601
Utilisation de workflows programmés	603
Utilisation d'un workflow programmé	604
Codage des calendriers de workflow	605

Création d'une feuille de travail à partir d'un type de lecteur donné	606
Téléchargement de workflows à l'aide de la BUI	609
▼ Téléchargement de workflows à l'aide de la CLI	610
▼ Création d'une liste de workflows à l'aide de la CLI	610
▼ Exécution de workflows à l'aide de la CLI	611
▼ Audit de workflows à l'aide de la CLI	612
 Intégration	 613
Configuration d'Oracle ZFS Storage Appliance pour les clients de la base de données Oracle	614
Sauvegarde d'Oracle Exadata Database Machine	614
Configuration de l'appareil pour Exadata	615
Configuration d'Exadata pour l'appareil	618
Sauvegarde d'Oracle SuperCluster	623
Configuration de la sauvegarde de l'appareil pour SuperCluster	623
Configuration d'Oracle SPARC SuperCluster pour la sauvegarde d'un appareil	641
Protocole OISP (Oracle Intelligent Storage Protocol)	645
Taille des enregistrements de la base de données	645
Indice de décalage d'écriture synchrone	645
Ventilation des analyses par nom de base de données	645
Clients et protocoles compatibles OISP	646
Plug-in ZFS Storage Appliance Network pour Oracle Solaris Cluster	646
Appliance Plug-in for Oracle Solaris Cluster Geographic Edition	646
Appliance Plug-in for Oracle Enterprise Manager System Monitoring	646
Configuration pour la surveillance d'Oracle Enterprise Manager	647
Annulation de la configuration de la surveillance d'Oracle Enterprise Manager	648
Appliance Plug-in for Oracle Virtual Machine Storage Connect	648
Appliance Plug-in Provider for Volume Shadow Copy Service Software	648
Prise en charge FC avec Symantec Dynamic Multi-Pathing et Storage Foundation	649
Appliance Replication Adapter for VMware Site Recovery Manager	650

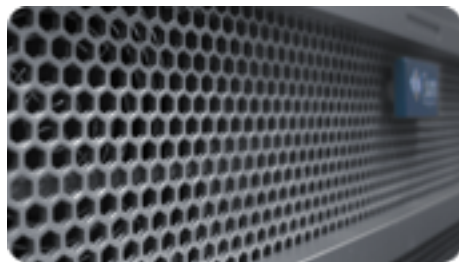
A propos d'Oracle ZFS Storage Appliance

La gamme de produits (appareils) Oracle ZFS Storage Appliance offre des services de données de fichiers et de données par blocs performants à des clients par le biais d'un réseau, ainsi qu'un large éventail de services de données pouvant être appliqués aux données stockées sur le système.

Pour obtenir des informations sur la configuration et l'utilisation d'Oracle ZFS Storage Appliance, reportez-vous aux sections suivantes :

- [Fonctionnalités clés d'Oracle ZFS Storage Appliances](#)
- ["Protocoles pris en charge" à la page 18](#)
- [Services de données Oracle ZFS Storage Appliance](#)
- ["Disponibilité des données" à la page 19](#)
- [Interface utilisateur de navigateur \(BUI\)](#)
- [Network Icons](#)
- [Dashboard Icons](#)
- [Icônes de la fonction d'analyse](#)
- [Icônes de mappage des identités](#)
- [Navigateurs pris en charge](#)
- [Interface de ligne de commande \(CLI\)](#)
- [Utilisation de l'écriture de scripts CLI](#)

Fonctionnalités clés d'Oracle ZFS Storage Appliance



Oracle ZFS Storage Appliance intègre des technologies visant à offrir le meilleur rapport prix/performance en matière de stockage et une qualité d'observation inédite de vos charges de travail en cours de production, avec notamment les outils suivants :

- Analytics, un système d'observation dynamique du comportement des systèmes en temps réel et de visualisation graphique des données
- Le pool de stockage hybride ZFS, formé de périphériques à mémoire Flash optionnels accélérant les lectures et les écritures, de disques haute capacité à faible consommation d'énergie et de mémoire DRAM, tous ces éléments étant gérés de manière transparente dans une hiérarchie de données unique
- Prise en charge de divers matériel

Pour plus d'informations sur l'analyse et le matériel, reportez-vous à la documentation de l'[Oracle Technology Network \(http://www.oracle.com/technetwork/indexes/documentation/index.html\)](http://www.oracle.com/technetwork/indexes/documentation/index.html)

Protocoles pris en charge

L'appareil Oracle ZFS Storage Appliance prend en charge une variété de protocoles clients aux normes industrielles, dont NFS, iSCSI, SMB, FTP, HTTP, NDMP, Fibre Channel, SRP, iSER et SFTP.

Pour plus d'informations sur ces protocoles, reportez-vous aux rubriques suivantes :

- ["Configuration Fibre Channel SAN" à la page 149](#)
- ["Configuration des cibles SAN iSER" à la page 139](#)
- ["Configuration NFS" à la page 237](#)
- ["Configuration iSCSI" à la page 242](#)
- ["Configuration SMB" à la page 243](#)
- ["Configuration FTP" à la page 261](#)
- ["Configuration HTTP" à la page 263](#)
- ["Configuration NDMP" à la page 266](#)
- ["Configuration SFTP" à la page 276](#)
- ["Configuration SRP" à la page 279](#)

Services de données pour l'appareil

Pour gérer les données exportées à l'aide de ces protocoles, vous pouvez configurer l'appareil à l'aide de l'ensemble intégré de services de données avancés, notamment :

NOTICE RELATIVE A LA LICENCE : *La réplication distante et le Clonage peuvent faire l'objet d'une évaluation à titre gratuit, mais chacune de ces fonctions requiert l'achat d'une licence distincte pour un usage en production. Au terme de la période d'évaluation, il convient d'acheter une licence pour ces fonctions ou de les désactiver. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

- Configurations de disques RAID-Z (RAID-5 et RAID-6) en miroir et entrelacés (voir ["Configuration du stockage" à la page 84](#))
- Nombre illimité d'instantanés en lecture seule et en lecture-écriture, avec possibilité de planification (voir ["Instantanés et clones" à la page 441](#))
- Contrôle de suppression des doublons de données (voir ["Suppression des doublons de données" à la page 366](#))
- Compression de données intégrée (voir ["Compression des données" à la page 367](#))
- Réplication distante des données à des fins de récupération après sinistre (voir ["Réplication distante" à la page 473](#))
- Clustering actif-actif pour haute disponibilité (voir ["Configuration d'appareils en cluster" à la page 191](#))
- Provisionnement fin des LUN iSCSI (voir ["Configuration iSCSI" à la page 242](#))
- Analyse antivirus et quarantaine (voir ["Configuration de l'analyse antivirus" à la page 280](#))
- Sauvegarde NDMP et restauration (voir ["Configuration NDMP" à la page 266](#))

Disponibilité des données

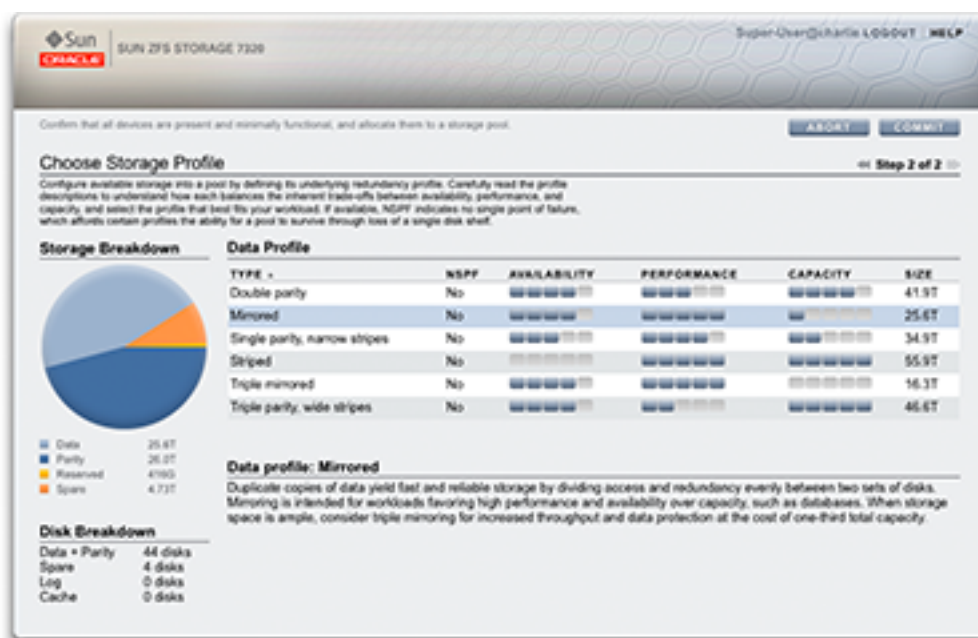
Pour maximiser la disponibilité de vos données en cours de production, l'appareil intègre une architecture de bout en bout complète visant à assurer l'intégrité des données et prévoyant des redondances à chaque niveau de la pile. Les principales fonctionnalités sont les suivantes :

- Autorétablissement prédictif et diagnostic de toutes les pannes matérielles des systèmes : CPU, DRAM, cartes d'E/S, disques, ventilateurs, alimentations
- Sommes de contrôle de données de bout en bout ZFS de toutes les données et métadonnées, protégeant les données dans l'ensemble de la pile
- RAID-6 (double et triple parité) et RAID-6 optionnelle sur plusieurs étagères de disques
- Clustering actif-actif pour haute disponibilité (voir ["Configuration d'appareils en cluster" à la page 191](#))
- Groupements de liaisons et multipathing IP pour la protection du réseau contre les pannes (voir ["Configuration réseau" à la page 51](#))
- Multipathing d'E/S entre le contrôleur et les étagères de disques
- Redémarrage logiciel intégré de tous les services logiciels du système (voir ["Services de l'appareil" à la page 225](#))

- Service Phone Home de transmission de téléméasures pour tous les problèmes logiciels et matériels (voir "[Configuration de Phone Home](#)" à la page 318)
- Gestion à distance de chaque système permettant un contrôle à distance de l'alimentation ainsi qu'un accès distant à la console

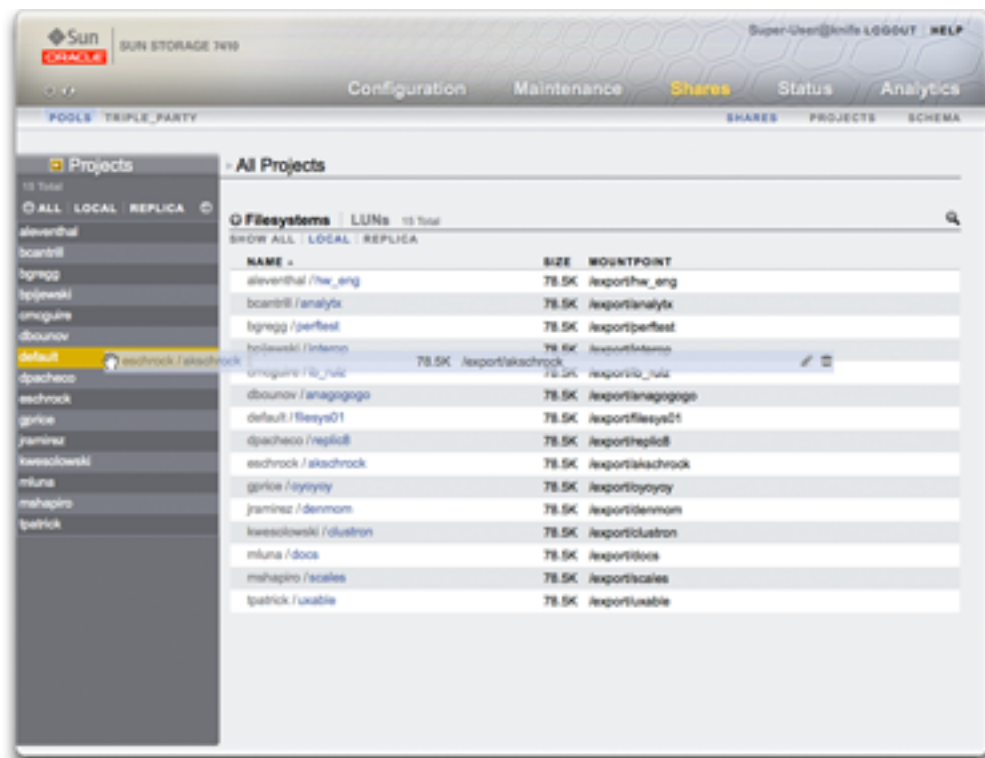
Interface utilisateur de navigateur (BUI, Browser User Interface)

La BUI d'Oracle ZFS Storage Appliance est l'outil graphique d'administration de l'appareil. La BUI offre un environnement intuitif pour les tâches d'administration, la visualisation des concepts et l'analyse des données relatives aux performances. La BUI offre un environnement clair permettant de visualiser le comportement du système et d'identifier les problèmes de performances affectant l'appareil.



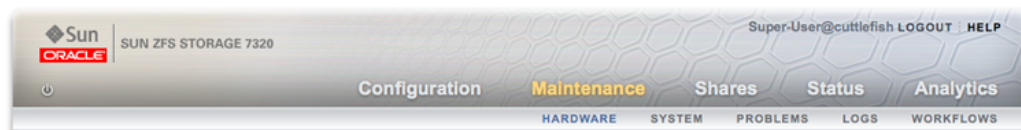
Orientez votre navigateur vers le système à l'aide de l'adresse IP ou du nom d'hôte que vous avez assigné au port NET-0 lors de la configuration initiale de la manière suivante : <https://ipaddress:215> ou <https://hostname:215>. L'écran de connexion s'affiche.

L'aide en ligne accessible dans l'angle supérieur droit de la BUI est contextuelle. Vous pouvez afficher l'aide en ligne associée à chaque écran de premier et de deuxième niveau de la BUI en cliquant sur le bouton Aide.



Modification des propriétés d'un système de fichiers en le déplaçant dans un autre projet à l'aide du panneau latéral Projets

Le cadre masthead contient plusieurs éléments d'interface servant à la navigation et à la notification, ainsi que les fonctionnalités principales. Sur la gauche, de haut en bas, se trouvent le logo Sun/Oracle, un badge indiquant le modèle du matériel et les boutons d'arrêt et de remise en marche du matériel. Sur la droite, à nouveau de haut en bas, se trouvent l'identification de connexion, la déconnexion, l'aide, la navigation principale et la sous-navigation.

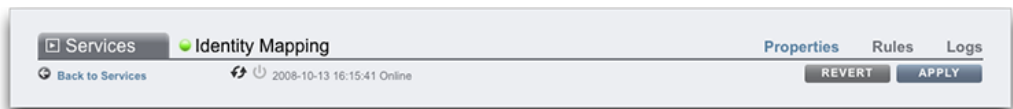


Les alertes système apparaissent dans le cadre Masthead lorsqu'elles sont déclenchées. Si plusieurs alertes sont déclenchées de façon séquentielle, reportez-vous à la liste d'alertes récentes accessible dans l'écran Tableau de bord ou le journal complet disponible dans l'écran Journaux.

Servez-vous des liens de navigation pour basculer entre les zones Configuration, Maintenance, Partages, Statut et Analyse de la BUI. Servez-vous des liens secondaires pour accéder aux fonctionnalités et aux fonctions de chaque zone.

Si vous saisissez une annotation de session, elle s'affiche sous votre ID de connexion et le bouton de déconnexion. Si vous souhaitez modifier votre annotation de session pour des actions d'administration ultérieures, cliquez sur le lien textuel. Reportez-vous à la section "[Configuration des utilisateurs](#)" à la page 160 pour plus de détails sur les annotations de session.

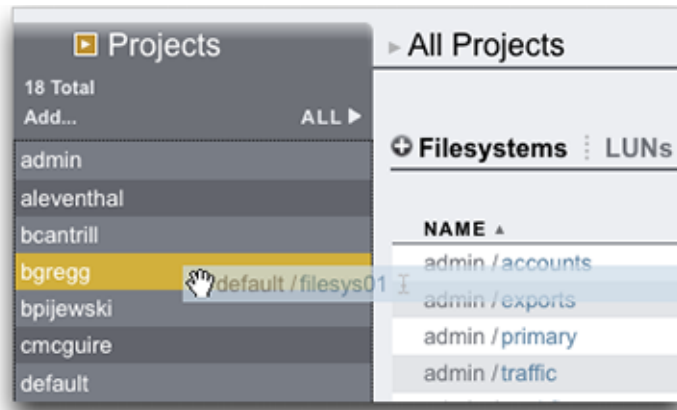
La barre de titre s'affiche sous le cadre Masthead et fournit des liens de navigation locaux ainsi que des fonctions qui varient en fonction de la vue en cours.



Par exemple, la barre de titre du service de mappage d'identités offre les éléments suivants :

- Accès à la liste de services complète par le biais du panneau latéral
- Contrôles permettant d'activer ou de désactiver le service de mappage d'identités.
- Vue du temps de fonctionnement du mappage d'identités
- Accès aux écrans Propriétés, Règles et Journaux du service Mappage de l'identité
- Bouton permettant d'appliquer les modifications de la configuration effectuées dans l'écran actuel
- Bouton permettant d'annuler les modifications de la configuration effectuées dans l'écran actuel

Pour basculer rapidement entre les vues Service et Projet, ouvrez et fermez le panneau latéral en cliquant sur le titre ou le flèche de développement .



Pour ajouter des projets, cliquez sur le lien Ajouter... dans la barre latérale.

Pour déplacer des partages entre des projets, cliquez sur l'icône de déplacement  et faites glisser un partage de système de fichiers vers le projet approprié dans le panneau latéral.

Notez que le déplacement d'un partage dans un autre projet modifie ses propriétés si celles-ci sont configurées pour être reprises du projet parent.

La plupart des contrôles de la BUI utilisent des entrées de formulaire Web standard, mais quelques exceptions clés sont à noter :

TABLEAU 1 Exceptions clés de formulaire Web

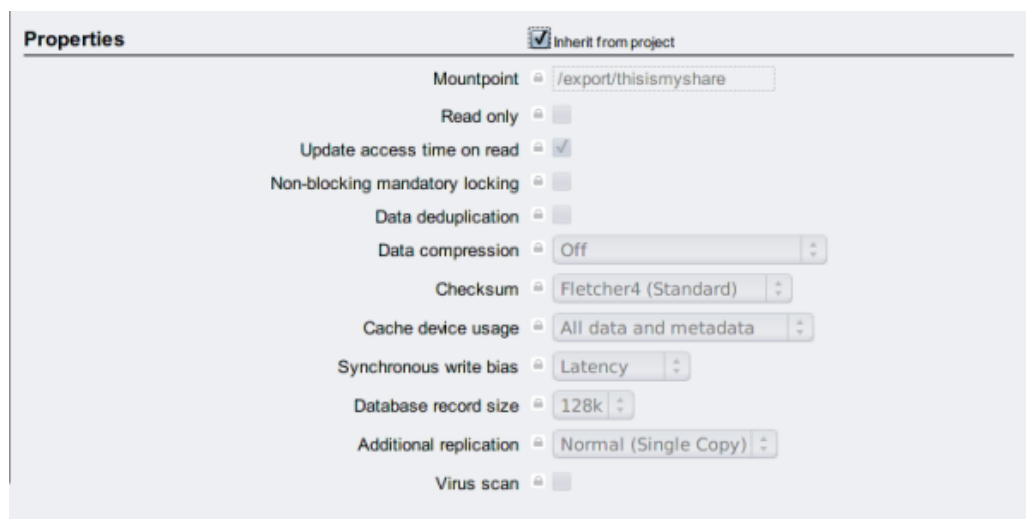
Récapitulatif des contrôles de la BUI	
Modifier une propriété	Cliquez sur l'icône de modification  et renseignez la boîte de dialogue
Ajouter un élément à une liste ou ajouter une entrée de propriété	Cliquez sur l'icône d'ajout 
Retirer un élément d'une liste ou retirer une entrée de propriété	Cliquez sur l'icône de suppression 
Enregistrer les modifications	Cliquez sur le bouton Appliquer
Annuler les modifications enregistrées	Cliquez sur le bouton Rétablir
Supprimer un élément dans une liste	Cliquez sur l'icône de la corbeille  (placez le pointeur de la souris sur la ligne de l'élément pour voir l'icône)
Rechercher un élément dans une liste	Cliquez sur l'icône de recherche  dans le coin supérieur droit de la liste
Trier par titres de liste	Cliquez sur les sous-titres en gras pour tirer à nouveau la liste
Déplacer ou faire glisser un élément	Cliquez sur l'icône de déplacement 

Récapitulatif des contrôles de la BUI	
Renommer un élément	Cliquez sur l'icône de changement de nom 
Afficher des informations détaillées sur le système	Cliquez sur le logo Oracle ou le badge indiquant le modèle pour accéder à la page Web oracle.com correspondant à votre modèle
Ouvrir le panneau latéral de manière automatique	Faites glisser un élément vers le panneau latéral

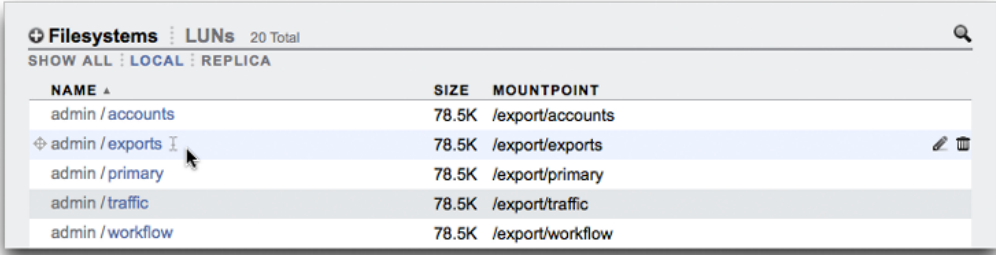
Lors de la définition des autorisations, les cases R, W et X sont des cibles sur lesquelles il est possible de cliquer. Cliquer sur l'étiquette d'un groupe d'accès (Utilisateur, Groupe, Autre) permet d'activer ou de désactiver collectivement toutes les autorisations de l'étiquette concernée.



Pour modifier les propriétés d'un partage, désactivez la case à cocher Hériter du projet.

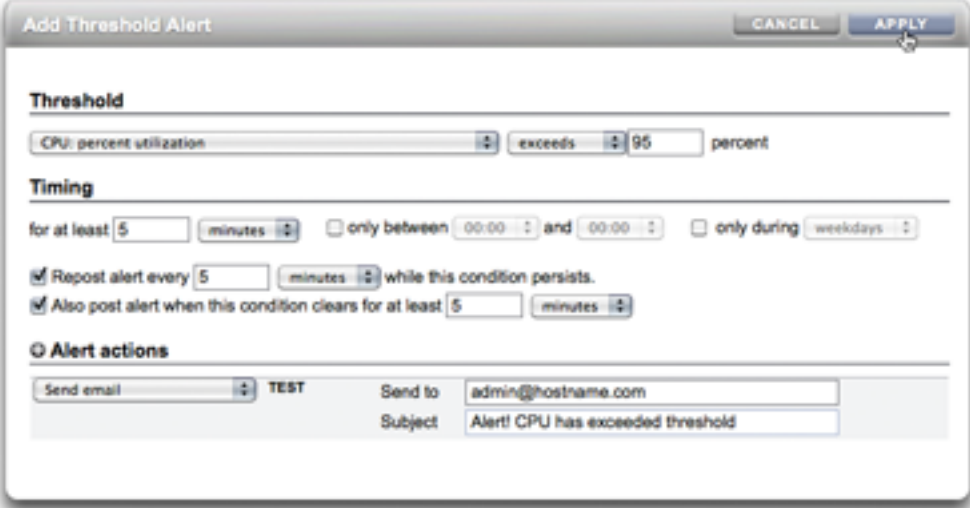


Pour afficher les contrôles d'un élément de liste, placez le pointeur de la souris sur la ligne concernée.



NAME	SIZE	MOUNTPOINT
admin /accounts	78.5K	/export/accounts
admin /exports	78.5K	/export/exports
admin /primary	78.5K	/export/primary
admin /traffic	78.5K	/export/traffic
admin /workflow	78.5K	/export/workflow

Toutes les boîtes de dialogue modales comportent dans leur partie supérieure des titres et des boutons décrivant et validant ou annulant l'action en cours, et du contenu dans la partie inférieure. Les zones de contenu modales suivent les mêmes conventions que la zone de contenu principale, mais elles s'en distinguent par le fait qu'elles doivent être fermées à l'aide des boutons figurant dans la barre de titre avant que d'autres actions ne puissent être effectuées.



Add Threshold Alert [CANCEL] [APPLY]

Threshold

CPU: percent utilization [dropdown] exceeds 95 percent

Timing

for at least 5 minutes [dropdown] ☐ only between 00:00 and 00:00 ☐ only during weekdays

☒ Repost alert every 5 minutes [dropdown] while this condition persists.

☒ Also post alert when this condition clears for at least 5 minutes [dropdown]

Alert actions

Send email [dropdown] TEST Send to admin@hostname.com Subject Alert! CPU has exceeded threshold

Les icônes indiquent l'état du système et fournissent l'accès aux fonctionnalités. Dans la plupart des cas, ils servent également de boutons déclenchant des actions lorsque vous cliquez dessus. Il peut être utile de placer le pointeur de la souris sur des icônes d'interface pour en afficher l'info-bulle. Les tableaux qui suivent constituent un récapitulatif des conventions utilisées dans l'interface.

Les voyants d'état sont des indicateurs de base de l'intégrité du système et de l'état du service :

TABLEAU 2 Indicateurs d'état

Icône	Description	Icône	Description
	en marche		Avertissement
	Désactivé		désactivé

Les icônes suivantes se trouvent dans l'interface utilisateur et couvrent la plupart des fonctionnalités de base :

TABLEAU 3 Icônes de la BUI

Icône*		Description	Icône*		Description
--		renommer (modifier du texte)	--		dissocier
--		déplacer	--		cloner
		modifier	--		restaurer
		détruire	--		alimentation de l'appareil
		ajouter	--		appliquer
		supprimer	--		rétablir
		annuler/fermer	--		Informations
--		Erreur	--		trier la colonne (décroissant)
--		alerte	--		trier la colonne (croissant)
		bouton marche/ arrêt			première page
		redémarrer			page précédente
--		localisation			page suivante
		désactiver/mettre hors ligne			dernière page
		verrouillage	--		rechercher
--		roue d'attente			menu
--		inverser le sens			Panneau

* Les icônes désactivées sont représentées sur la gauche.

Les icônes suivantes permettent de distinguer différents types d'objets et fournissent des informations d'importance secondaire.

TABLEAU 4 Icônes diverses

Icône	Description	Icône	Description
	autoriser		SAS
	refuser		Port SAS
	pool de stockage		

Icônes de réseau

Ces icônes indiquent l'état des périphériques réseau et le type de liaisons de données réseau :

TABLEAU 5 Icônes de réseau

Icône	Description	Icône	Description
	périphérique réseau actif		port Infiniband actif
	périphérique réseau inactif		port Infiniband inactif
	liaison de données réseau		liaison de données réseau (partition IB)
	liaison de données réseau VLAN		
	groupement de liaisons de données réseau		
	groupement de liaisons de données réseau VLAN		

Icônes du tableau de bord

Les icônes suivantes indiquent l'état actuel des statistiques faisant l'objet d'une surveillance par rapport aux seuils paramétrables par l'utilisateur définis dans les Paramètres.

TABLEAU 6 Icônes du tableau de bord

Icône	Description	Icône	Description
	ensoleillé		ouragan

Icône	Description	Icône	Description
	partiellement nuageux		ouragan de catégorie 2
	nuageux		ouragan de catégorie 3
	pluvieux		ouragan de catégorie 4
	orageux		ouragan de catégorie 5

Icônes de la barre d'outils d'analyse

Cet ensemble d'icônes est regroupé dans une barre d'outils et sert à paramétrer l'affichage des informations dans les feuilles de travail de la fonctionnalité d'analyse.

TABLERAU 7 Icônes de la barre d'outils d'analyse

Icône	Description	Icône	Description
	reculer		afficher le minimum
	avancer		afficher le maximum
	avancer jusqu'à maintenant		afficher le graphique à courbes
	mettre en pause		afficher le graphique en aires
	zoom arrière		rognage des valeurs aberrantes
	zoom avant		synchroniser feuille de travail avec cette statistique
	afficher une minute		annuler synchronisation feuille de travail-statistiques
	afficher une heure		analyse descendante
	afficher un jour		exporter les données statistiques (télécharger sur le client)
	afficher une semaine		enregistrer les données statistiques

Icône	Description	Icône	Description
	afficher un mois		archiver l'ensemble de données
			envoyer la feuille de travail avec le lot de support

Pour plus d'informations sur l'analyse, reportez-vous à la documentation de l'[Oracle Technology Network](http://www.oracle.com/technetwork/indexes/documentation/index.html) (<http://www.oracle.com/technetwork/indexes/documentation/index.html>)

Icônes de mappage des identités

Ces icônes indiquent le type de rôle appliqué lors de la mise en correspondance des utilisateurs et groupes Windows avec les utilisateurs et groupes Unix.

TABLEAU 8 Icônes de mappage des identités

Icône*	Description	Icône*	Description
	autoriser Windows vers Unix		autoriser Unix vers Windows
	refuser Windows vers Unix		refuser Unix vers Windows
	autoriser bidirectionnel		

*Les icônes désactivées sont sur la partie gauche.

Rubriques connexes

- ["Présentation du statut de l'appareil" à la page 111](#)
- ["Configuration réseau" à la page 51](#)
- ["Configuration du stockage" à la page 84](#)
- ["Configuration des alertes" à la page 184](#)
- ["Services de l'appareil" à la page 225](#)

Pour plus d'informations sur l'analyse, reportez-vous à la documentation de l'[Oracle Technology Network](http://www.oracle.com/technetwork/indexes/documentation/index.html) (<http://www.oracle.com/technetwork/indexes/documentation/index.html>)

Navigateurs pris en charge

Cette section définit les navigateurs pris en charge par la BUI.

La BUI est conçue pour être entièrement fonctionnelle sur les navigateurs suivants :

- Firefox 10 et versions ultérieures
- Internet Explorer 9 et versions ultérieures
- Safari 5 et versions ultérieures
- Google Chrome 31 et versions ultérieures

Les éléments de la BUI risquent de s'afficher de manière imparfaite dans les navigateurs suivants et certaines fonctionnalités risquent d'être indisponibles, mais toutes les fonctions indispensables sont parfaitement opérationnelles. Un message d'avertissement s'affiche lors de la connexion si vous utilisez l'un des navigateurs suivants :

- Firefox 6 à 9
- Internet Explorer 7 et 8
- Google Chrome 21 à 30
- Opera 23 et versions antérieures

Les navigateurs suivants sont incompatibles et ne sont pas pris en charge en raison de problèmes connus ; la connexion n'aboutira pas.

- Firefox 5 et versions antérieures
- Internet Explorer 6 et versions antérieures
- Google Chrome 20 et versions antérieures
- Safari 4 et versions antérieures
- Opera 22 et versions antérieures

Rubriques connexes

- ["Configuration des utilisateurs" à la page 160](#)
- ["Configuration des préférences pour l'appareil" à la page 179](#)

Interface de ligne de commande (CLI, Command Line Interface)

La CLI offre les mêmes fonctionnalités que la BUI tout en fournissant un environnement de script performant idéal pour effectuer des tâches répétitives. La ligne de commande est un outil efficace et puissant permettant d'exécuter des tâches administratives répétitives. L'appareil présente une interface de ligne de commande disponible via la console ou SSH. L'interaction avec le système par le biais de la CLI peut être préférable dans plusieurs cas de figure :

- **Indisponibilité du réseau** - Si le réseau est indisponible, la gestion par l'intermédiaire du navigateur est impossible et la console est le seul moyen d'assurer la gestion ; la console prend uniquement en charge une interface basée sur du texte

- **Moyen le plus opportun** - Le temps de démarrage d'un navigateur peut être prohibitif, en particulier si vous souhaitez seulement vérifier un aspect particulier du système ou effectuer un changement de configuration rapide
- **Précision** - Dans certaines situations, les informations fournies par le navigateur sont plutôt de nature qualitative que quantitative, et il vous faut une réponse plus précise
- **Automatisation** - L'interaction via navigateur n'est pas facile à automatiser. Si vous avez des tâches répétitives ou strictement définies, il est préférable de scripter les tâches

Lors de la navigation dans la CLI, vous devez avoir connaissance des deux principes suivants :

- **La saisie semi-automatique par tabulation est largement utilisée** : si vous n'êtes pas certain du texte à saisir dans un contexte donné, vous pouvez afficher les options possibles en appuyant sur la touche de tabulation. Dans l'ensemble de la documentation, l'appui sur la touche de tabulation est représenté par le mot "tab" noté en caractères gras et en italique.
- **L'aide est disponible à tout moment** : la commande `help` permet d'afficher l'aide contextuelle. Il est possible d'afficher l'aide portant sur un thème particulier en saisissant le thème concerné en tant qu'argument de la commande `help`, par exemple `help commands`. Pour afficher les thèmes disponibles, saisissez la commande `help` et appuyez sur la touche de tabulation ou saisissez `help topics`.

Vous pouvez combiner ces deux principes comme suit :

```
dory:> help tab
builtins    commands  general    help        properties  script
```

Pour vous connecter à distance par le biais de la CLI, faites appel à un client `ssh`. Si vous n'avez pas suivi les instructions figurant dans la section "[Configuration des utilisateurs](#)" à la page 160 pour administrer l'appareil, vous devrez vous connecter en tant qu'utilisateur `root`. Lorsque vous vous connectez, la CLI affiche une invite qui se compose du nom d'hôte suivi d'un caractère deux-points et d'un caractère supérieur à :

```
% ssh root@dory
Password:
Last login: Mon Oct 13 15:43:05 2009 from kiowa.sf.fishpo
dory:>
```

Rubriques connexes

- "[Interface utilisateur de navigateur \(BUI, Browser User Interface\)](#)" à la page 20
- "[Contextes de la CLI](#)" à la page 31
- "[Propriétés de la CLI](#)" à la page 37

Contextes de la CLI

Le *contexte* dans lequel les commandes sont exécutées constitue l'un des principes fondamentaux de la CLI. Le contexte détermine les éléments du système pouvant être gérés

et les commandes disponibles. Les contextes ont une structure en arborescence dans laquelle les contextes peuvent à leur tour contenir des contextes imbriqués. La structure reflète généralement celle des vues de la BUI.

Le contexte initial au moment de la connexion est le *contexte root*, qui fait office de parent ou d'ancêtre pour tous les contextes. Pour accéder à un contexte, exécutez le nom du contexte en tant que commande. Par exemple, les fonctions disponibles dans la vue Configuration du navigateur sont disponibles dans le contexte configuration de la CLI. Dans le contexte root, vous pouvez y accéder en saisissant directement ce qui suit :

```
dory:> configuration
dory:configuration>
```

Notez que l'invite change pour refléter le contexte, le contexte s'affichant entre le caractère deux-points et le caractère supérieur à dans l'invite.

La commande show affiche les contextes enfant. Par exemple, depuis le contexte configuration :

```
dory:configuration> show
Children:
    net => Configure networking
    services => Configure services
    version => Display system version
    users => Configure administrative users
    roles => Configure administrative roles
    preferences => Configure user preferences
    alerts => Configure alerts
    storage => Configure Storage
```

Ces contextes enfant correspondent aux vues disponibles sous la vue Configuration dans le navigateur, notamment Réseau, Services et utilisateurs, Préférences, etc. Pour sélectionner l'un de ces contextes enfant, saisissez son nom :

```
dory:configuration> preferences
dory:configuration preferences>
```

Accédez directement à un contexte subordonné à partir d'un ancêtre en indiquant les contextes intermédiaires, séparés par des espaces. Par exemple, pour accéder directement à configuration preferences à partir du contexte root, saisissez simplement :

```
dory:> configuration preferences
dory:configuration preferences>
```

Certains contextes enfant sont *dynamiques*, au sens où ils ne correspondent pas à des vues figées dans le navigateur, mais à des entités dynamiques créées par l'utilisateur ou le système. Il existe deux façons d'accéder à ces contextes : vous pouvez utiliser la commande select suivie du nom du contenu dynamique, ou vous pouvez placer le nom du contexte dynamique entre guillemets. La commande list permet d'afficher les noms des contextes dynamiques compris

dans un contexte donné. Par exemple, le contexte `users` est un contexte statique, mais chaque utilisateur constitue un contexte dynamique pour lui-même.

```
dory:> configuration users
dory:configuration users> list
NAME                USERNAME          UID      TYPE
John Doe            bmc               12345    Dir
Super-User          root              0        Loc
```

Pour sélectionner l'utilisateur nommé `bmc`, émettez la commande `select bmc` ou `"bmc"` :

```
dory:configuration users> "bmc"
dory:configuration users bmc>
```

Dans certains contextes, il est également possible d'utiliser les guillemets, ainsi que les commandes `select` et `destroy` pour sélectionner une entité en fonction de ses propriétés. La commande suivante peut par exemple être exécutée pour sélectionner des entrées de journal émises par le module `reboot` dans le contexte `maintenance logs system` :

```
dory:maintenance logs system> select module=reboot
dory:maintenance logs system entry-034> show
Properties:
  timestamp = 2010-8-14 06:24:41
  module = reboot
  priority = crit
  text = initiated by root on /dev/console syslogd: going down on signal 15
```

A l'instar d'autres commandes, la commande `select` ou les guillemets peuvent être associés à des commandes entraînant un changement de contexte. Par exemple, pour sélectionner l'utilisateur nommé `bmc` à partir du contexte `root` :

```
dory:> configuration users select bmc
dory:configuration users bmc>
```

La commande `last` permet d'accéder directement à un contexte sélectionné ou créé précédemment. L'exemple suivant crée une action de réplication, puis exécute les commandes `last` et `get id` pour récupérer l'ID de l'action de réplication. Ensuite, une action différente est sélectionnée et les commandes `last` et `get id` permettent de récupérer l'ID de la dernière action de réplication visitée.

Avec la commande `last`, vous pouvez retourner au dernier noeud visité :

```
dory:configuration net interfaces> "igb4"
dory:configuration net interfaces igb4> done
dory:configuration net interfaces> last
net:configuration net interfaces igb4>
```

La commande `last` est aussi utile pour extraire des valeurs ayant été automatiquement définies par l'appareil pendant la création d'un noeud dynamique. Par exemple, chaque action de réplication se voit attribuer un ID par l'appareil lorsqu'elle est créée. En utilisant la commande

last avec la commande `get id`, vous pouvez extraire l'ID sans utiliser le nom de l'action de réplication :

```
dory:shares pl/share replication> create
dory:shares pl/share action (uncommitted)> set target=dory
                                target = dory (uncommitted)
dory:shares pl/share action (uncommitted)> set pool=p0
                                pool = p0 (uncommitted)
dory:shares pl/share action (uncommitted)> commit
dory:shares pl/share replication> last get id
                                id = 7034367a-d4d8-e26f-fa93-c3b454e3b595
dory:shares pl/share replication>
```

Notez que quand `last` est combinée avec une autre commande (dans ce cas, `get id`), la commande est exécutée dans le contexte du dernier noeud visité, mais le noeud actuel reste inchangé.

Parce que `last` vous permet d'extraire le dernier noeud visité et ses valeurs sans spécifier le nom du noeud, cette commande est particulièrement pratique pour l'écriture de scripts :

```
script
    project = 'myproj';
    target = 'mytarget';
    target_pool = 'notmypool';

    run('cd /');
    run('shares select ' + project);
    run('replication');
    run('create');
    set('target', target);
    set('pool', target_pool);
    run('commit');
    run('last');
    id = get('id');
    printf("Sending update for replication action id %s ...", id);
    run('sendupdate');
    while (get('state') != 'idle') {
        printf(".");
        run('sleep 1');
    }
    printf("done\n");
.
```

Pour revenir au contexte précédent, exécutez la commande `done` :

```
dory:configuration> done
dory:>
```

Cela vous renvoie au contexte précédent, qui n'est pas nécessairement le contexte parent, comme suit :

```
dory:> configuration users select bmc
dory:configuration users bmc> done
```

```
dory:>
```

La commande `done` peut être utilisée à plusieurs reprises pour revenir à des contextes antérieurs :

```
dory:> configuration
dory:configuration> users
dory:configuration users> select bmc
dory:configuration users bmc> done
dory:configuration users> done
dory:configuration> done
dory:>
```

Pour accéder à un contexte parent, utilisez la commande `cd`. Inspirée de la commande UNIX classique, la commande `cd` suivie de l'argument `..` permet de revenir au contexte parent :

```
dory:> configuration users select bmc
dory:configuration users bmc> cd ..
dory:configuration users>
```

Et, comme pour la commande UNIX, `"cd /"` permet d'accéder au contexte `root` :

```
dory:> configuration
dory:configuration> users
dory:configuration users> select bmc
dory:configuration users bmc> cd /
dory:>
```

De même, toujours à l'instar de la commande UNIX, `"cd ../../"` permet d'accéder au contexte grand-parent :

```
dory:> configuration
dory:configuration> users
dory:configuration users> select bmc
dory:configuration users bmc> cd ../../
dory:configuration>
```

Les noms des contextes prennent en charge la saisie semi-automatique par tabulation, qu'il s'agisse des contextes statiques (saisie semi-automatique normale basée sur la commande) ou des contextes dynamiques (saisie semi-automatique basée sur la commande `select`). L'exemple suivant indique comment sélectionner l'utilisateur nommé `bmc` à partir du contexte `root` en quinze frappes seulement, au lieu des trente et une normalement requises sans saisie semi-automatique par tabulation :

```
dory:> configtab
dory:> configuration utab
dory:> configuration users setab
dory:> configuration users select tab
bmc  root
dory:> configuration users select btab
dory:> configuration users select bmcenter
```

```
dory:configuration users bmc>
```

Lorsque vous vous trouvez dans un contexte, exécutez des commandes spécifiques au contexte. Par exemple, pour obtenir les préférences de l'utilisateur actuel, exécutez la commande `get` dans le contexte `configuration preferences` :

```
dory:configuration preferences> get
      locale = C
      login_screen = status/dashboard
      session_timeout = 15
      session_annotation =
      advanced_analytics = false
```

Si une commande est suivie d'une entrée entraînant un changement de contexte, la commande concernée est exécutée dans le contexte cible, mais le contrôle revient au contexte appelant. Par exemple, pour obtenir les préférences à partir du contexte `root` sans modifier le contexte, ajoutez la commande `get` aux commandes de navigation du contexte :

```
dory:> configuration preferences get
      locale = C
      login_screen = status/dashboard
      session_timeout = 15
      session_annotation =
      advanced_analytics = false
```

Lors de la création d'une nouvelle entité dans le système, le contexte associé à la nouvelle entité est fréquemment créé avec l'état *uncommitted* ("non validé"). Vous pouvez par exemple créer une alerte avec seuil en exécutant la commande `create` à partir du contexte `configuration alerts threshold` :

```
dory:> configuration alerts thresholds create
dory:configuration alerts threshold (uncommitted)>
```

La mention `(uncommitted)` dans l'invite indique qu'il s'agit d'un contexte non validé. Une entité non validée est validée via la commande `commit`. Toute tentative de quitter un contexte non validé déclenche l'affichage d'une invite de confirmation :

```
dory:configuration alerts threshold (uncommitted)> cd /
Leaving will abort creation of "threshold". Are you sure? (Y/N)
```

Lors de la validation d'une entité non validée, les propriétés associées à la nouvelle entité sont validées et une erreur est générée si l'entité ne peut pas être créée. Par exemple, la création d'une nouvelle alerte avec seuil nécessite la spécification d'un nom de statistique, sans quoi une erreur se produit :

```
dory:configuration alerts threshold (uncommitted)> commit
error: missing value for property "statname"
```

Pour résoudre ce problème, résolvez l'erreur et retentez la validation :

```
dory:configuration alerts threshold (uncommitted)> set statname=cpu.utilization
```

```

statname = cpu.utilization (uncommitted)
dory:configuration alerts threshold (uncommitted)> commit
error: missing value for property "limit"
dory:configuration alerts threshold (uncommitted)> set limit=90
limit = 90 (uncommitted)
dory:configuration alerts threshold (uncommitted)> commit
dory:configuration alerts thresholds> list
THRESHOLD      LIMIT      TYPE  STATNAME
threshold-000  90       normal cpu.utilization

```

Rubriques connexes

- ["Interface de ligne de commande \(CLI, Command Line Interface\)" à la page 30](#)
- ["Propriétés de la CLI" à la page 37](#)

Propriétés de la CLI

Les *propriétés* sont des couples nom/valeur saisis au clavier et associés à un contexte. Les propriétés associées à un contexte donné peuvent être affichées à l'aide de la commande "help properties". L'exemple suivant indique comment extraire les propriétés associées aux préférences d'un utilisateur :

```

dory:configuration preferences> help properties
Properties that are valid in this context:

locale           => Locality

login_screen     => Initial login screen

session_timeout  => Session timeout

session_annotation => Current session annotation

advanced_analytics => Make available advanced analytics statistics

```

La commande get permet de récupérer les propriétés d'un contexte donné. L'exemple suivant illustre l'utilisation de la commande get pour récupérer les préférences d'un utilisateur :

```

dory:configuration preferences> get
locale = C
login_screen = status/dashboard
session_timeout = 15
session_annotation =
advanced_analytics = false

```

La commande get renvoie toute propriété saisie en tant qu'argument. Par exemple, pour obtenir la valeur de la propriété login_screen :

```

dory:configuration preferences> get login_screen

```

```
login_screen = status/dashboard
```

Appuyer sur la touche de tabulation après avoir saisi la commande `get` permet d'afficher les noms des propriétés disponibles. Par exemple, pour afficher une liste des propriétés disponibles pour le service iSCSI :

```
dory:> configuration services iscsi get tab
<status>          isns_server      radius_secret      target_chap_name
isns_access        radius_access    radius_server      target_chap_secret
```

La commande `select`, ou une commande placée entre guillemets, permet de sélectionner un nœud dynamique par propriété. Par exemple, pour sélectionner la commande `key-000` par utilisateur :

```
hostname:configuration services sftp keys> show
Keys:

NAME      MODIFIED          CIPHER  USER  COMMENT
key-000  2015-6-5 19:48:23  RSA     u1     1

hostname:configuration services sftp keys> "user=u1"
hostname:configuration services sftp key-000>
```

La commande `set` permet de définir une propriété sur une valeur spécifique, le nom de la propriété et sa valeur étant séparés par le caractère égal. Par exemple, pour définir la propriété `login_screen` sur `"shares"` :

```
dory:configuration preferences> set login_screen=shares
login_screen = shares (uncommitted)
```

Notez que dans le cas de propriétés constituant un état de l'appareil, définir la propriété n'a *pas* pour effet de changer la valeur, mais la valeur définie est enregistrée avec l'indication que la valeur de la propriété est non validée.

Pour forcer l'application des valeurs de propriétés définies, elles doivent être explicitement validées, ce qui permet la modification de plusieurs valeurs en une modification unique et cohérente. Exécutez la commande `commit` pour valider toute valeur de propriété non validée :

```
dory:configuration preferences> get login_screen
login_screen = shares (uncommitted)
dory:configuration preferences> commit
dory:configuration preferences> get login_screen
login_screen = shares
```

Si vous tentez de quitter un contexte contenant des propriétés non validées, le système vous avertit que la sortie du contexte vous fera perdre les valeurs de propriétés définies, et vous serez invité à confirmer que vous souhaitez quitter le contexte. Par exemple :

```
dory:configuration preferences> set login_screen=maintenance/hardware
login_screen = maintenance/hardware (uncommitted)
```

```
dory:configuration preferences> done
You have uncommitted changes that will be discarded. Are you sure? (Y/N)
```

Si une propriété associée à un contexte est définie à partir d'un autre contexte, c'est-à-dire si la commande `set` suit une commande ayant pour effet de changer le contexte, la validation est *implicite* et intervient avant que le contrôle ne revienne au contexte d'origine. Par exemple :

```
dory:> configuration preferences set login_screen=analytics/worksheets
      login_screen = analytics/worksheets
dory:>
```

Certaines propriétés acceptent une liste de valeurs. Pour ces propriétés, les éléments de la liste doivent être séparés par des virgules. Par exemple, la propriété `servers` NTP peut être définie sur une liste de serveurs NTP :

```
dory:configuration services ntp> set servers=0.pool.ntp.org,1.pool.ntp.org
      servers = 0.pool.ntp.org,1.pool.ntp.org (uncommitted)
dory:configuration services ntp> commit
```

Si une valeur de propriété contient une virgule, le signe égal, une apostrophe ou un espace, l'ensemble de la valeur doit être placé entre guillemets. Par exemple, la propriété des partages `sharenfs` pour le projet par défaut peut être définie en lecture seule, mais peut accorder un accès en lecture/écriture à l'hôte `kiowa`. Pour plus d'informations, reportez-vous à la section ["Partages et projets" à la page 343](#).

```
dory:> shares select default
dory:shares default> set sharenfs="ro,rw=kiowa"
      sharenfs = ro,rw=kiowa (uncommitted)
dory:shares default> commit
```

Certaines propriétés sont inaltérables. Vous pouvez obtenir leurs valeurs mais pas les définir. Toute tentative de définir une propriété inaltérable se solde par une erreur. L'exemple suivant illustre une tentative de définition de la propriété inaltérable `space_available` du projet par défaut. Pour plus d'informations, reportez-vous à la section ["Partages et projets" à la page 343](#).

```
dory:> shares select default
dory:shares default> get space_available
      space_available = 1.15T
dory:shares default> set space_available=100P
error: cannot set immutable property "space_available"
```

D'autres propriétés ne sont inaltérables que dans certaines conditions. Pour ces propriétés, la commande `set` n'est pas valide. Par exemple, si l'utilisateur nommé `bmc` est un utilisateur réseau, la propriété `fullname` sera inaltérable :

```
dory:> configuration users select bmc set fullname="Rembrandt Q. Einstein"
error: cannot set immutable property "fullname"
```

Rubriques connexes

- ["Interface utilisateur de navigateur \(BUI, Browser User Interface\)" à la page 20](#)
- ["Interface de ligne de commande \(CLI, Command Line Interface\)" à la page 30](#)

Utilisation de l'écriture de scripts CLI

La CLI est conçue pour fournir un environnement de script performant idéal pour effectuer des tâches répétitives.

Vous pouvez utiliser des commandes de traitement par lots ou des commandes de script (ou une combinaison des deux), mais dans tous les cas l'infrastructure automatisée nécessite un accès automatisé à l'appareil. Ceci doit s'effectuer via la configuration utilisateur, les autorisations d'utilisateur et la définition des clés publiques SSH à l'aide de la CLI.

Pour plus d'informations sur la configuration des utilisateurs, consultez les sections suivantes :

- ["Configuration des utilisateurs" à la page 160](#)
- ["Autorisations utilisateur" à la page 176](#)
- ["Configurations des clés publiques SSH \(CLI\)" à la page 182](#)

Pour utiliser l'écriture de scripts CLI, reportez-vous aux sections suivantes :

- [Utilisation des commandes de traitement par lots](#)
- [Présentation des commandes d'écriture de script CLI](#)
- [Accès à l'environnement de script CLI](#)
- [Présentation des fonctions CLI intégrées](#)
- [Utilisation de la fonction run](#)
- [Utilisation de la fonction get](#)
- [Utilisation de la fonction list](#)
- [Utilisation de la fonction children](#)
- [Utilisation de la fonction Choices](#)
- [Utilisation des fonctions pour la génération des sorties](#)
- [Présentation des erreurs de script CLI](#)

Utilisation des commandes de traitement par lots

Le mécanisme de script le plus simple est le traitement par lots de commandes de shell de l'appareil. Par exemple, pour réaliser automatiquement un instantané appelé "newsnap" dans le projet "myproj" et le système de fichiers "myfs", placez les commandes suivantes dans un fichier :


```
shares
select myproj
select myfs
snapshots snapshot newsnap
```

Connectez-vous ensuite par ssh à l'appareil et redirigez l'entrée standard vers le fichier :

```
% ssh root@dory < myfile.txt
```

Dans de nombreux shells, vous pouvez abréger cette opération en utilisant un fichier appelé "here file", dans lequel les entrées jusqu'à un jeton donné sont envoyées à l'entrée standard. Ce qui suit reproduit l'exemple qui précède à l'aide d'un fichier "here file" :

```
% '''ssh root@dory << EOF
shares
select myproj
select myfs
snapshots snapshot newsnap
EOF'''
```

Ce mécanisme est suffisant pour une automatisation des plus élémentaires, et peut éventuellement faire l'affaire s'il est inclus dans une logique de programmation dans un langage de script de shell de niveau supérieur sur un client, mais laisse généralement à désirer.

Présentation des commandes d'écriture de script CLI

Le traitement par lots de commandes peut être suffisant pour les opérations les plus élémentaires, mais son inclusion dans une logique de programmation peut s'avérer fastidieuse. Par exemple, pour obtenir des informations d'utilisation de l'espace pour chaque partage, il vous faut un grand nombre d'invocations différentes de la CLI, incluses dans un langage de niveau supérieur sur le client qui a analysé la sortie de commandes données. Le résultat est une infrastructure d'automatisation lente et fragile. Pour permettre une automatisation plus rapide et plus robuste, l'appareil est doté d'un *environnement de script* basé sur ECMAScript 3. Ce document n'a pas pour objet de fournir un tutoriel sur ECMAScript. Sachez toutefois qu'il s'agit d'un langage à saisie dynamique possédant une syntaxe de type C prenant en charge :

- Le code à exécution conditionnelle (`if/else`)
- Le code à exécution itérative (`while`, `for`, etc.)
- La manipulation de données structurées et de tableaux via des types d'objets et de tableaux de première classe
- Les expressions régulières et la manipulation de chaînes de type Perl (`split()`, `join()`, etc.)
- Exceptions
- Des fonctions de langage fonctionnel sophistiquées telles que les fermetures

▼ Accès à l'environnement de script CLI

1. Dans la CLI, accédez à l'environnement de script à l'aide de la commande **script** :

```
dory:> script
("." to run)>
```

2. Lorsque l'invite d'environnement de script s'affiche, vous pouvez saisir votre script, en saisissant à la fin ".", seul sur une ligne, pour l'exécuter :

```
dory:> script
("." to run)> for (i = 10; i > 0; i--)
("." to run)>   printf("%d... ", i);
("." to run)>   printf("Blastoff!\n");
("." to run)> .
10... 9... 8... 7... 6... 5... 4... 3... 2... 1... Blastoff!
```

3. Si votre script ne comporte qu'une seule ligne, vous pouvez simplement le saisir en tant qu'argument de la commande **script** ; vous pouvez ainsi facilement vous entraîner à l'écriture de scripts :

```
dory:> script print("It is now " + new Date())
It is now Tue Oct 14 2009 05:33:01 GMT+0000 (UTC)
```

Présentation des fonctions CLI intégrées

Il est évident que les scripts présentent uniquement un intérêt s'ils sont en mesure d'interagir avec le système dans son ensemble. Plusieurs fonctions intégrées permettent à vos scripts d'interagir avec le système :

TABEAU 9 Fonctions intégrées pour la prise en charge des interactions avec le système

Fonction	Description
get	Récupère la valeur de la propriété spécifiée. Notez que cette fonction renvoie la valeur au format natif (par exemple, les dates sont renvoyées comme des objets Date).
list	Renvoie un tableau de jetons correspondant aux enfants dynamiques du contexte actuel.
run	Exécute la commande spécifiée dans le shell et renvoie les éventuelles sorties en tant que chaînes. Notez que si la sortie contient plusieurs lignes, la chaîne renvoyée contient des nouvelles lignes incorporées.
props	Renvoie un tableau des noms de propriétés du noeud actuel.
set	Nécessite deux chaînes en tant qu'arguments et définit la propriété spécifiée sur la valeur spécifiée.

Fonction	Description
choicies	Renvoie une série de valeurs de la propriété valide pour toute propriété dont l'ensemble de valeurs est connu et énumérable.

▼ Utilisation de la fonction run

1. La manière la plus simple pour les scripts d'interagir avec le système dans son ensemble est l'utilisation de la fonction "run" : celle-ci nécessite une commande à exécuter et renvoie la sortie de cette commande en tant que chaîne. Par exemple :

```
dory:> configuration version script dump(run('get boot_time'))
'
      boot_time = 2009-10-12 07:02:17\n'
```

2. La fonction `dump` intégrée procède au vidage de l'argument sans accroître les éventuelles nouvelles lignes incorporées. Les fonctionnalités de gestion des chaînes d'ECMAScript peuvent être utilisées pour décomposer la sortie. Voici par exemple le résultat de la scission sur la base des espaces de la sortie ci-dessus :

```
dory:> configuration version script dump(run('get boot_time').split(/\s+/))
[&#39;;', 'boot_time', '=', '2009-10-12', '07:02:17', &#39;']
```

▼ Utilisation de la fonction get

La fonction `run` est suffisamment puissante pour que l'utilisateur soit tenté de s'appuyer exclusivement sur l'analyse des sorties afin d'obtenir des informations sur le système. Son indéniable inconvénient est que les scripts correspondants analysent des sorties lisibles à l'oeil qui sont susceptibles de changer à l'avenir. Pour collecter des informations sur le système de manière plus fiable, servez-vous de la fonction "get" intégrée. Dans le cas de la propriété `boot_time`, cette fonction renvoie l'objet `Date` d'ECMAScript plutôt que la chaîne, et permet ainsi la manipulation par programmation de cette valeur de propriété.

1. Par exemple, vous pouvez souhaiter utiliser la propriété `boot_time` conjointement avec l'heure actuelle pour déterminer la durée écoulée depuis l'initialisation :

```
script
run('configuration version');
now = new Date();
uptime = (now.valueOf() - get('boot_time').valueOf()) / 1000;
printf('up %d day%s, %d hour%s, %d minute%s, %d second%s\n',
      d = uptime / 86400, d < 1 || d >= 2 ? 's' : '',
      h = (uptime / 3600) % 24, h < 1 || h >= 2 ? 's' : '',
```

```
m = (uptime / 60) % 60, m < 1 || m >= 2 ? 's': '',  
s = uptime % 60, s < 1 || s >= 2 ? 's': '';
```

2. **En supposant que le script ci-dessus est enregistré dans un fichier "uptime.aksh", vous pouvez l'exécuter de la manière suivante :**

```
% ssh root@dory < uptime.aksh  
Pseudo-terminal will not be allocated because stdin is not a terminal.  
Password:  
up 2 days, 10 hours, 47 minutes, 48 seconds
```

Le message concernant l'allocation d'un pseudo-terminal est du au client ssh ; le problème correspondant peut être résolu en spécifiant l'option "-T" pour ssh.

▼ Utilisation de la fonction list

Dans un contexte possédant des enfants dynamiques, il peut s'avérer utile d'itérer ces enfants par programmation. Ceci peut être réalisé à l'aide de la fonction list, qui renvoie un tableau d'enfants dynamiques.

1. **L'exemple de script ci-dessous itère chaque partage de chaque projet et imprime la quantité d'espace occupée et la quantité d'espace disponible :**

```
script  
  run('shares');  
  projects = list();  
  
  for (i = 0; i < projects.length; i++) {  
    run('select ' + projects[i]);  
    shares = list();  
  
    for (j = 0; j < shares.length; j++) {  
      run('select ' + shares[j]);  
      printf("%s/%s %1.64g %1.64g\n", projects[i], shares[j],  
        get('space_data'), get('space_available'));  
      run('cd ..');  
    }  
  
    run('cd ..');  
  }  
}
```

2. **La sortie obtenue après l'exécution du script, enregistré dans le fichier "space.aksh", est présentée ci-dessous :**

```
% ssh root@koi < space.aksh  
Password:  
admin/accounts 18432 266617007104  
admin/exports 18432 266617007104  
admin/primary 18432 266617007104
```

```

admin/traffic 18432 266617007104
admin/workflow 18432 266617007104
aleventhal/hw_eng 18432 266617007104
bcantrill/analytx 1073964032 266617007104
bgregg/dashbd 18432 266617007104
bgregg/filesys01 26112 107374156288
bpijewski/access_ctrl 18432 266617007104
...

```

3. **Pour obtenir une version plus "présentable" (bien que plus difficile à gérer du point de vue de la programmation), il est possible d'analyser directement la sortie de la commande get :**

```

script
  run('shares');
  projects = list();

  printf('%-40s %-10s %-10s\n', 'SHARE', 'USED', 'AVAILABLE');

  for (i = 0; i < projects.length; i++) {
    run('select ' + projects[i]);
    shares = list();

    for (j = 0; j < shares.length; j++) {
      run('select ' + shares[j]);

      share = projects[i] + '/' + shares[j];
      used = run('get space_data').split(/\s+/)[3];
      avail = run('get space_available').split(/\s+/)[3];

      printf('%-40s %-10s %-10s\n', share, used, avail);
      run('cd ..');
    }

    run('cd ..');
  }
}

```

4. **La sortie obtenue après l'exécution de ce nouveau script, enregistré dans le fichier "prettyspace.aksh", est présentée ci-dessous :**

```

% ssh root@koi < prettyspace.aksh
Password:
SHARE                                     USED      AVAILABLE
admin/accounts                          18K        248G
admin/exports                           18K        248G
admin/primary                           18K        248G
admin/traffic                           18K        248G
admin/workflow                          18K        248G
aleventhal/hw_eng                       18K        248G
bcantrill/analytx                       1.00G      248G
bgregg/dashbd                           18K        248G
bgregg/filesys01                        25.5K      100G
bpijewski/access_ctrl                   18K        248G
...

```

5. La fonction list prend en charge les arguments facultatifs depth et filter.

Son format est le suivant : `list ([depth, [filter]])`. L'argument `depth` peut être défini par un nombre. Plus le nombre pour `depth` est élevé, plus le nombre de détails affichés sera important. L'argument `filter` se présente sous la forme suivante : `{<prop1>:<val1>, <prop2>:<val2> ...}`. Si `filter` est indiqué, `depth` doit l'être également.

Syntaxe et comportement de l'entrée :

- `list()` - Renvoie uniquement des noms de noeuds.
- `list(0)` - Renvoie les propriétés de noeud et uniquement les noms des enfants.
- `list(0, {kiosk_mode: true})` - Renvoie une liste filtrée lorsque la commande `kiosk_mode` est définie sur `true` avec les noms des enfants.
- `list(1)` - Renvoie les propriétés de noeud, les noms et les propriétés des enfants, et uniquement les noms des petits-enfants.
- `list(1, {kiosk_mode: true})` - Renvoie une liste filtrée lorsque la commande `kiosk_mode` est définie sur `true` avec des détails jusqu'à `depth=1`.
- `list(2)` - Renvoie les propriétés de noeud, les noms et propriétés des enfants, et la sortie `list(0)` des petits-enfants.
- `list(2, {fullname: 'Super*', kiosk_mode: true})` - Renvoie une liste filtrée pour `fullname` contenant `Super`, lorsque la commande `kiosk_mode` est définie sur `true` avec des détails jusqu'à `depth=2`.

6. Voici un exemple de sortie pour une liste avec depth=2 :

Le libellé `name` indique le nom de l'élément de liste (à savoir, un noeud). Le libellé `properties` indique les propriétés de l'élément de liste. Le libellé `children` indique les enfants statiques de l'élément de liste. Le libellé `list` indique les enfants dynamiques de l'élément de liste.

```
script
("." to run)> dump(list(2));
("." to run)> .

[{
  name: 'restuser',
  properties: {
    kiosk_screen: 'status/dashboard',
    kiosk_mode: false,
    roles: ['basic'],
    require_annotation: false,
    initial_password: 'DummyPassword',
    fullname: 'REST User',
    logname: 'restuser'
  },
  children: [{
    name: 'preferences',
    properties: {
      advanced_analytics: false,
      session_timeout: 15,
```

```

        login_screen: 'status/dashboard',
        locale: 'C'
    },
    {
        name: 'exceptions',
        list: [{
            name: 'auth-000',
            properties: {
                allow_configure: false,
                scope: 'alert'
            }
        }, {
            name: 'auth-001',
            properties: {
                allow_workgroup: false,
                allow_domain: false,
                name: '*',
                scope: 'ad'
            }
        }
    ]
}]
}]

```

▼ Utilisation de la fonction children

Même dans un contexte possédant des enfants statiques, il peut s'avérer utile d'itérer ces enfants par programmation. Ceci peut être réalisé à l'aide de la fonction `children`, qui renvoie un tableau d'enfants statiques.

1. **Voici par exemple un script qui itère chaque service et imprime le statut du service :**

```

configuration services
script
    var svcs = children();
    for (var i = 0; i < svcs.length; ++i) {
        run(svcs[i]);
        try {
            printf("%-10s %s\n", svcs[i], get('<status>'));
        } catch (err) { }
        run("done");
    }
}

```

2. **La sortie obtenue après l'exécution du script, enregistré dans le fichier "svcinfo.aksh", est présentée ci-dessous :**

```

% ssh root@koi < space.aksh
Password:
cifs      disabled

```

dns	online
ftp	disabled
http	disabled
identity	online
idmap	online
ipmp	online
iscsi	online
ldap	disabled
ndmp	online
nfs	online
nis	online
ntp	online
scrk	online
sftp	disabled
smtp	online
snmp	disabled
ssh	online
tags	online
vscan	disabled

▼ Utilisation de la fonction Choices

La fonction Choices retourne une série de valeurs de la propriété valide pour toute propriété dont l'ensemble de valeurs est connu et énumérable. Par exemple, le script suivant extrait la liste de tous les pools sur le noeud de partage à l'aide de la fonction Choices, puis itère tous les pools pour répertorier les projets et les partages ainsi que l'espace disponible.

1. **Par exemple, le script suivant extrait la liste de tous les pools sur le noeud de partage à l'aide de la fonction Choices, puis itère tous les pools pour répertorier les projets et les partages ainsi que l'espace disponible.**

```
fmt = '%-40s %-15s %-15s\n';
printf(fmt, 'SHARE', 'USED', 'AVAILABLE');
run('cd /');
run('shares');
pools = choices('pool');
for (p = 0; p < pools.length; p++) {
    set('pool', pools[p]);
    projects = list();
    for (i = 0; i < projects.length; i++) {
        run('select ' + projects[i]);
        shares = list();
        for (j = 0; j < shares.length; j++) {
            run('select ' + shares[j]);
            share = pools[p] + ':' + projects[i] + '/' + shares[j];
            printf(fmt, share, get('space_data'),
                get('space_available'));
            run('cd ..');
        }
    }
    run('cd ..');
```



```
}
}
```

2. La sortie obtenue après l'exécution du script est présentée ci-dessous :

SHARE	USED	AVAILABLE
pond:projectA/fs1	31744	566196178944
pond:projectA/fs2	31744	566196178944
pond:projectB/lun1	21474836480	587670999040
puddle:deptA/share1	238475	467539219283
puddle:deptB/share1	129564	467539219283
puddle:deptB/share2	19283747	467539219283

Utilisation des fonctions pour la génération des sorties

Pour signaler un état du système, il est nécessaire de générer des sorties. Plusieurs fonctions intégrées sont mises à la disposition des scripts pour générer des sorties :

TABLEAU 10 Fonctions intégrées de génération de la sortie

Fonction	Description
dump	Vide l'argument spécifié vers le terminal sans accroître les nouvelles lignes incorporées. Les objets sont affichés dans un format semblable à JSON. Utile pour le débogage.
print	Imprime l'objet spécifié en tant que chaîne, suivi d'une nouvelle ligne. Si l'objet ne possède pas de méthode toString, il est imprimé de façon opaque.
printf	Comme printf(3C) de C, imprime les arguments spécifiés conformément à la chaîne de formatage spécifiée.

Présentation des erreurs de script CLI

Lorsque le système génère une erreur, une exception est levée. L'exception est généralement un objet qui contient les membres suivants :

- code : code numérique associé à l'erreur
- message : message lisible à l'oeil associé à l'erreur

Les exceptions peuvent être interceptées et gérées, ou elles peuvent être levées hors de l'environnement de script. Si un environnement présente une exception non interceptée, la CLI affiche les informations détaillées à ce sujet. Par exemple :

```
dory:> script run('not a cmd')
```

```
error: uncaught error exception (code EAKSH_BADCMD) in script: invalid command
      "not a cmd" (encountered while attempting to run command "not a cmd")
```

Pour voir de plus amples informations sur l'exception, vous pouvez l'intercepter et la vider :

```
dory:> script try { run('not a cmd') } catch (err) { dump(err); }
{
  toString: <function>,
  code: 10004,
  message: 'invalid command "not a cmd" (encountered while attempting to
           run command "not a cmd")'
}
```

Ceci vous permet également de mettre en oeuvre une gestion explicite des erreurs, par exemple :

```
#!/usr/bin/ksh -p

ssh -T root@dory <<EOF
script
  try {
    run('shares select default select $1');
  } catch (err) {
    if (err.code == EAKSH_ENTITY_BADSELECT) {
      printf('error: "$1" is not a share in the ' +
            'default project\n');
      exit(1);
    }

    throw (err);
  }

  printf('"default/$1": compression is %s\n', get('compression'));
  exit(0);
EOF
```

Si ce script est nommé "share.ksh" et exécuté avec un nom de partage incorrect, un message d'erreur explicite est généré :

```
% ksh ./share.ksh bogus
error: "bogus" is not a share in the default project
```

Configuration de l'appareil

Pour configurer l'appareil, reportez-vous aux sections suivantes :

- ["Configuration initiale de l'appareil" à la page 51](#)
- ["Configuration réseau" à la page 51](#)
- ["Configuration du stockage" à la page 84](#)
- ["Présentation du statut de l'appareil" à la page 111](#)
- ["Configuration du réseau de stockage SAN" à la page 127](#)
- ["Configuration des utilisateurs" à la page 160](#)
- ["Configuration des préférences pour l'appareil" à la page 179](#)
- ["Configuration des alertes" à la page 184](#)
- ["Configuration d'appareils en cluster" à la page 191](#)

Configuration initiale de l'appareil

La configuration initiale peut être répétée ultérieurement en cliquant sur le bouton CONFIGURATION INITIALE sur l'écran Maintenance > Système ou en saisissant le contexte `maintenance system setup` dans la CLI.

Les informations détaillées de configuration initiale se trouvent dans la section ["Configuration initiale de l'appareil" du Guide d'installation des systèmes Oracle ZFS Storage Appliance](#).

Configuration réseau

Les fonctions de configuration de la gestion réseau vous permettent de créer diverses configurations de gestion réseau avancées à l'aide de vos ports réseau physiques, notamment des groupements de liaisons, des NIC virtuels (VNIC), des LAN virtuels (VLAN) et des groupes à chemins d'accès multiples. Vous pouvez ensuite définir un nombre quelconque d'adresses IPv4 et IPv6 pour ces abstractions, ces adresses devant servir à la connexion à divers services de données sur le système.

La configuration réseau d'un système comporte quatre composants :

- **Périphériques** : ports réseau physiques. Ils correspondent aux connexions réseau physiques ou partitions IPoIB (IP on InfiniBand).
- **Liaisons de données** : les éléments de base pour l'envoi et la réception de paquets. Les liaisons de données peuvent correspondre exactement à un périphérique (c'est-à-dire à un port réseau physique) ou une partition IB, ou vous pouvez définir des liaisons de données de type Groupement, VLAN et VNIC composées d'autres services et liaisons de données.
- **Interface** : l'élément de base pour la configuration et l'adressage IP. Chaque interface IP est associée à une liaison de données unique, ou est définie comme un groupe IPMP formé d'autres interfaces.
- **Routage** : la configuration du routage IP. Celui-ci détermine la manière dont le système oriente les paquets IP.

Pour procéder à la configuration réseau de l'appareil, reportez-vous aux sections suivantes :

- ["Configuration réseau \(BUI\)" à la page 52](#)
- ["Configuration réseau \(CLI\)" à la page 64](#)
- ["Utilisation de la page de configuration réseau" à la page 73](#)
- ["Configuration de l'interface de gestion" à la page 74](#)
- ["Configuration des liaisons de données réseau" à la page 75](#)
- ["Configuration des interfaces réseau" à la page 77](#)
- ["Configuration du multiacheminement IP \(IPMP\) réseau" à la page 79](#)
- ["Configuration des performances et de la disponibilité réseau" à la page 80](#)
- ["Configuration du routage réseau" à la page 81](#)

Configuration réseau (BUI)

Lorsque la configuration du réseau est modifiée par l'intermédiaire de la BUI, le système s'efforce de préserver la connexion réseau en cours au navigateur. Toutefois, certaines modifications de la configuration du réseau, comme par exemple la suppression de l'adresse exacte à laquelle le navigateur est connecté, entraînent nécessairement une interruption de la connexion du navigateur. C'est pourquoi il est recommandé de réserver une adresse IP et un périphérique réseau particuliers à l'usage des administrateurs, et de ne pas modifier la configuration de cette adresse. Vous pouvez également effectuer les tâches de reconfiguration du réseau particulièrement complexes à partir de la CLI, par le biais de la console série si nécessaire.

Les icônes suivantes sont utilisées dans la section Configuration > Réseau :

TABEAU 11 Icônes de configuration réseau

icône	description
	Ajouter une nouvelle liaison de données/interface/route
	Modifier les paramètres d'une liaison de données/interface/route

icône	description
	Modification désactivée
	Détruire une liaison de données/interface/route
	Destruction désactivée
	Icône glisser-déplacer
	port réseau connecté
	port réseau connecté avec activité d'E/S
	port réseau déconnecté (liaison interrompue, problème de câble ?)
	port Infiniband actif
	port Infiniband actif avec activité d'E/S
	port Infiniband inactif (état down, init ou arm)
	périphérique de partition InfiniBand est en marche
	périphérique de partition InfiniBand est arrêté (problème de gestionnaire sous-réseau)
	liaison de données réseau
	liaison de données réseau VLAN ou VNIC
	groupement de liaisons de données réseau
	groupement de liaisons de données VLAN ou VNIC
	partition IB liaison de données réseau
	interface utilisée pour l'envoi et la réception de paquets (en marche ou détériorée)
	interface désactivée par l'utilisateur
	interface hors ligne (appartenant au pair du cluster)
	interface défaillante ou configurée avec une adresse IP en double

Dans l'angle supérieur droit vous pouvez accéder aux rubriques Configuration, Adresses et Routage, qui affichent d'autres vues de configuration.

La page Configuration est affichée par défaut et répertorie les périphériques, les liaisons de données et les interfaces, avec les boutons destinés à l'administration. Placez le pointeur de la souris sur une entrée pour afficher une icône  supplémentaire et cliquez sur n'importe quelle entrée pour mettre en évidence d'autres composants qui lui sont associés.

La liste Périphériques affiche le statut des liens sur la droite, ainsi qu'une icône reflétant l'état du port réseau. Si des ports sont indiqués comme déconnectés, assurez-vous qu'ils sont correctement rattachés au réseau.

Pour configurer une adresse IP sur un périphérique réseau, créez tout d'abord une liaison de données, puis créez une interface utilisant cette liaison de données. L'icône  permet d'effectuer ces deux opérations : elle affiche des boîtes de dialogue permettant de définir les propriétés des liaisons de données et des interfaces.

Vous pouvez procéder de différentes manières pour configurer une interface réseau. Vous pouvez par exemple cliquer sur l'icône  d'un périphérique, puis faire glisser celui-ci dans la table de liaisons de données. Vous pouvez ensuite faire glisser la liaison de données vers la table d'interfaces. D'autres déplacements sont possibles. Cette manière de procéder peut être utile pour les configurations complexes, dans lesquelles les déplacements autorisés sont mis en surbrillance.

Cette page affiche un tableau récapitulatif de la configuration actuelle du réseau contenant les champs suivants :

TABLEAU 12 Récapitulatif de la configuration réseau actuelle

Champ	Description	Exemple
Liaison de données réseau	Nom de la liaison de données et récapitulatif des détails	datalink1 (via igb0)
Interface réseau	Nom de l'interface et récapitulatif des détails	IPv4 DHCP, via datalink1
Adresses réseau	Adresses hébergées par l'interface concernée	192.168.2.80/22
Noms d'hôtes	Noms d'hôtes résolus pour les adresses réseau	caji.sf.example.com

Cette page affiche la configuration de la table de routage IP et des propriétés correspondantes, telle que décrites plus haut. Par défaut, toutes les entrées de la table de routage sont affichées, mais la table peut être filtrée en fonction du type ou à l'aide de la barre de sous-navigation.

Pour vérifier une route spécifique, exécutez `traceroute` dans la CLI.

```
zfssa-source:> traceroute 10.80.198.102
traceroute: Warning: Multiple interfaces found; using 10.80.198.101 @ igb3
traceroute to 10.80.198.102 (10.80.198.102), 30 hops max, 40 byte packets
1 10.80.198.1 (10.80.198.1) 6.490 ms 0.924 ms 0.834 ms
2 10.80.198.102 (10.80.198.102) 0.152 ms 0.118 ms 0.099 ms
zfssa-target:> traceroute 10.80.198.101
traceroute: Warning: Multiple interfaces found; using 10.80.198.102 @ igb3
traceroute to 10.80.198.101 (10.80.198.101), 30 hops max, 40 byte packets
1 10.80.198.1 (10.80.198.1) 1.031 ms 0.905 ms 0.769 ms
2 10.80.198.101 (10.80.198.101) 0.158 ms 0.111 ms 0.109 ms
```

▼ Configuration de l'interface de gestion (BUI)

Utilisez la procédure suivante pour configurer les interfaces de gestion.

1. **Accédez à Configuration > Réseau.**
2. **Cliquez sur l'icône d'ajout  en regard de Liaisons de données.**
3. **Définissez les propriétés de liaison de données minimales suivantes et cliquez sur APPLIQUER.**
 - **VNIC** - Cochez cette case.
 - **Nom** - Saisissez un nom pour la liaison de données.
4. **Faites glisser la liaison de données créée jusqu'à la colonne Interfaces.**
5. **Dans la boîte de dialogue Interface réseau, définissez les propriétés d'interface minimales suivantes et cliquez sur APPLIQUER :**
 - **Nom** - Saisissez un nom pour l'interface.
 - **Activer l'interface** - Cochez cette case pour activer l'interface.
 - **Autoriser l'administration** - Cochez cette case pour la définir comme interface de gestion, ce qui active les connexions de la BUI sur le port 215 et les connexion de la CLI sur le port ssh 22.

Remarque - L'option Autoriser l'administration transforme l'interface en une interface de gestion, ce qui permet d'établir des connexions BUI sur le port 215 et des connexions CLI sur le port ssh 22.

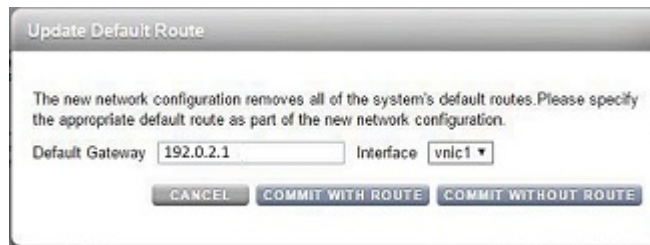
- **Utiliser le protocole IPv4** ou **Utiliser le protocole IPv6** - Sélectionnez un protocole, son type d'adresse et saisissez une ou plusieurs adresses IP au format de notation CIDR.
6. **Dans le cas de contrôleurs clustérisés, répétez les étapes 1 à 5 sur le deuxième contrôleur.**
 7. **Cliquez sur l'icône de corbeille  en regard de l'option Interface sans titre, qui est l'interface par défaut, pour la supprimer.**

Remarque - Lorsqu'une interface est supprimée, toutes les routes qui lui sont associées le sont également.

8. **Dans la boîte de dialogue Route par défaut de la mise à jour, saisissez la passerelle par défaut et sélectionnez une interface dans le menu déroulant. Cliquez sur VALIDER AVEC LA ROUTE.**

La passerelle par défaut est l'adresse IP du routeur par défaut. Pour l'interface, sélectionnez la liaison de données que vous avez affectée à la première interface de gestion.

Remarque - Il est fortement recommandé de définir une route car elle permet de communiquer avec l'appareil via la BUI et la CLI. Sans route, le seul moyen de communiquer avec l'appareil est d'utiliser une connexion Oracle ILOM vers le processeur de service.



Rubriques connexes

- Pour obtenir une présentation de la configuration d'une interface réseau, reportez-vous à la section ["Utilisation de la page de configuration réseau"](#) du manuel *Guide d'administration des systèmes Oracle ZFS Storage Appliance, version OS8.6.0*.
- Pour une configuration plus approfondie, reportez-vous à la section ["Configuration de l'appareil"](#) du manuel *Guide d'administration des systèmes Oracle ZFS Storage Appliance, version OS8.6.0*.
- Pour mettre à niveau le logiciel sur un contrôleur autonome, reportez-vous à la section ["Mise à niveau du logiciel"](#) dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.
- Pour verrouiller les interfaces de gestion de cluster, reportez-vous à la section ["Verrouillage des interfaces de gestion de cluster \(BUI\)"](#) à la page 56.

▼ Verrouillage des interfaces de gestion de cluster (BUI)

Après la configuration initiale, les contrôleurs clustérisés sont à l'état actif-actif. Lorsqu'un basculement se produit, un contrôleur actif reprend toutes les interfaces non privées, et le contrôleur pair devient passif et inaccessible par la BUI et la CLI. Pour conserver l'accès à un contrôleur quel que soit son état, verrouillez son interface de gestion pour la rendre privée. La procédure suivante permet de verrouiller l'interface de gestion sur chaque contrôleur clustérisé.



Attention - Si vous ne configurez pas d'interfaces de gestion verrouillées sur des contrôleurs clustérisés, les temps de diagnostic et de résolution des pannes matérielles risquent d'être inutilement allongés.

1. Dans la BUI du premier contrôleur, accédez à **Configuration > Cluster**.

2. Dans la BUI du second contrôleur, accédez à **Configuration > Cluster**.
3. Dans la BUI du premier contrôleur, choisissez l'interface de gestion du premier contrôleur dans la liste **Ressource**.
4. Cliquez sur l'icône en forme de cadenas  pour verrouiller l'interface de gestion sur ce contrôleur.
L'interface affiche une icône verrouillée  en regard de son nom dans la liste **Ressource**.
5. Dans la BUI du second contrôleur, choisissez l'interface de gestion du second contrôleur dans la liste **Ressource**.
6. Cliquez sur l'icône en forme de cadenas  pour verrouiller l'interface de gestion sur ce contrôleur.
L'interface affiche une icône verrouillée  en regard de son nom dans la liste **Ressource**.

Rubriques connexes

- Pour mettre à niveau le logiciel, reportez-vous à la section ["Mise à niveau du logiciel" dans le Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance](#).

▼ Création d'une interface à port unique (BUI)

1. Cliquez sur l'icône  **Liaisons de données**.
2. (Facultatif) Définissez le nom et sélectionnez le bouton radio correspondant à MTU personnalisé, en saisissant 9000 dans la zone de texte.
3. Sélectionnez un périphérique dans la liste **Périphériques**.
4. Cliquez sur **"APPLIQUER"**. La liaison de données s'affiche dans la liste **Datalinks**.
5. Cliquez sur l'icône  **Interface**.
6. Définissez les propriétés souhaitées et sélectionnez la liaison de données que vous venez de créer.
7. Cliquez sur **"APPLIQUER"**. L'interface s'affiche dans la liste **Interfaces**.
8. La configuration réseau de l'appareil en cours d'exécution n'est pas encore modifiée. Lorsque vous avez terminé la configuration des interfaces, cliquez sur **"APPLIQUER"** en haut de l'écran pour valider la configuration.

▼ Modification d'une interface (BUI)

1. Cliquez sur l'icône de modification de la liaison de données ou de l'interface.
2. Réglez les paramètres sur les valeurs souhaitées.
3. Cliquez sur "APPLIQUER" dans la boîte de dialogue.
4. Cliquez sur "APPLIQUER" en haut de la page pour valider la configuration.

▼ Déverrouillage d'une interface de données (BUI)

1. Accédez à Configuration > Cluster.
2. Vérifiez que les icônes de verrou des interfaces de données sont grises, ce qui indique qu'elles sont déverrouillées .
3. Si les icônes de verrou sont noires , cliquez sur chacune d'elles pour déverrouiller les interfaces.
4. Cliquez sur APPLIQUER pour enregistrer les modifications.

▼ Déverrouillage d'une interface de données (CLI)

1. Accédez à configuration cluster resources.

```
hostname:> configuration cluster resources
```

2. Saisissez show.

Toutes les interfaces de données doivent avoir leur TYPE défini sur singleton.

```
hostname:configuration cluster resources> show
```

Resources:

RESOURCE	OWNER	TYPE	LABEL	CHANGES	DETAILS
net/vnic2	zs34-02	private	mgmt-02	no	10.80.218.170
net/vnic3	zs34-02	private	data-01	no	10.80.216.46
net/vnic4	zs34-02	singleton	data-02	no	10.80.216.47
zfs/pool-01	zs34-01	singleton		no	
zfs/pool-02	zs34-02	singleton		no	53.5T

3. Si le type d'une interface de données est défini sur privé, sélectionnez la ressource et définissez son type sur singleton.

```
hostname:configuration cluster resources> select net/vnic3
```

```
hostname:configuration cluster resources net/vnic3> set type=singleton
type = singleton
```

4. Saisissez commit.

```
hostname:configuration cluster resources> commit
```

▼ Création d'une interface à port unique (BUI)

1. Placez le pointeur de la souris sur un périphérique et cliquez sur l'icône glisser-déplacer (⊕).
2. Faites-le glisser vers la liste de liaisons de données et relâchez le bouton de la souris.
3. (Facultatif) Définissez le nom et réglez jumbo MTU.
4. Cliquez sur "APPLIQUER".
5. Faites ensuite glisser la liaison de données vers la liste d'interfaces.
6. Définissez les propriétés souhaitées et cliquez sur "APPLIQUER".
7. Cliquez sur "APPLIQUER" en haut de l'écran pour valider la configuration.

▼ Création d'une interface de liaison groupée LACP (BUI)

1. Cliquez sur l'icône ⊕ Liaisons de données.
2. (Facultatif) Définissez le nom de la liaison de données.
3. Sélectionnez Groupement LACP.
4. Sélectionnez deux périphériques ou plus dans la liste Périphériques et cliquez sur "APPLIQUER".
5. Cliquez sur l'icône ⊕ Interfaces.
6. Définissez les propriétés souhaitées, sélectionnez la liaison groupée dans la liste Liaisons de données et cliquez sur "APPLIQUER".
7. Cliquez sur "APPLIQUER" en haut de l'écran pour valider la configuration.

▼ **Création d'un groupe IPMP à l'aide de la détection des défaillances basée sur sondes et sur l'état des liaisons**

N'utilisez pas la détection des défaillances basée sur sondes lorsqu'aucun système (autre que le pair du cluster) sur le même sous-réseau que les adresses IPMP de test n'est configuré pour répondre aux demandes d'écho ICMP.

1. **Créez une ou plusieurs interfaces IP "sous-jacentes" qui seront utilisées en tant que composants du groupe IPMP. Chaque interface doit disposer d'une adresse IP utilisée en tant que source des sondes (voir la tâche de création d'interfaces à port unique décrite ci-avant).**
2. Cliquez sur l'icône  Interface.
3. (Facultatif) Modifiez le nom de l'interface.
4. Activez la case à cocher Groupe IP MultiPathing.
5. Cliquez sur Utiliser le protocole IPv4 ou/et Utiliser le protocole IPv6 et indiquez les adresses IP de l'interface IPMP.
6. Sélectionnez les interfaces créées au cours de la première étape dans la liste Interfaces.
7. Définissez librement chaque interface sélectionnée comme "Active" ou "De secours".
8. Cliquez sur "APPLIQUER".

▼ **Création d'un groupe IPMP à l'aide de la détection des défaillances basée uniquement sur l'état des liaisons**

1. **Créez une ou plusieurs interfaces IP "sous-jacentes" ayant l'adresse IP 0.0.0.0 /8 qui seront utilisées en tant que composants du groupe IPMP (voir la tâche de création d'interfaces à port unique décrite ci-avant).**
2. Cliquez sur l'icône  Interface.
3. (Facultatif) Modifiez le nom de l'interface.
4. Activez la case à cocher Groupe IP MultiPathing.
5. Cliquez sur Utiliser le protocole IPv4 ou/et Utiliser le protocole IPv6 et indiquez les adresses IP de l'interface IPMP.

6. Sélectionnez les interfaces créées au cours de la première étape dans la liste Interfaces.
7. Définissez librement chaque interface sélectionnée comme "Active" ou "De secours".
8. Cliquez sur "APPLIQUER".

▼ Extension d'un groupement LACP (BUI)

1. Placez le pointeur de la souris sur un périphérique de la liste Périphériques.
2. Cliquez sur l'icône  et faites glisser le périphérique sur une liaison de données de groupement, puis relâchez le bouton de la souris.
3. Cliquez sur "APPLIQUER" en haut de la page pour valider cette configuration.

▼ Extension d'un groupe IPMP (BUI)

1. Placez le pointeur de la souris sur une interface de la liste Interfaces.
2. Cliquez sur l'icône  et faites glisser le périphérique sur une interface IPMP, puis relâchez le bouton de la souris.
3. Cliquez sur "APPLIQUER" en haut de la page pour valider cette configuration.

▼ Création d'une liaison de données et d'une interface de partition InfiniBand (BUI)

1. Cliquez sur l'icône  Liaisons de données.
2. (Facultatif) Définissez un nom.
3. Activez la case à cocher IB Partition.
4. Sélectionnez un périphérique dans la liste Périphériques de partition.
5. Entrez un nombre hexadécimal à quatre chiffres pour la clé de partition, qui doit correspondre au nombre défini dans le gestionnaire de sous-réseau InfiniBand.

6. Choisissez le mode de liaison dans le menu déroulant.
7. Cliquez sur "APPLIQUER". La nouvelle liaison de données de partition s'affiche dans la liste Liaisons de données.
8. Cliquez sur l'icône  Interface.
9. Définissez les propriétés souhaitées et sélectionnez la liaison de données que vous venez de créer.
10. Cliquez sur "APPLIQUER". L'interface s'affiche dans la liste Interfaces.
11. La configuration réseau de l'appareil en cours d'exécution n'est pas encore modifiée. Lorsque vous avez terminé la configuration des interfaces, cliquez sur "APPLIQUER" en haut de l'écran pour valider la configuration.

▼ Création d'un VNIC sans ID de VLAN pour des contrôleurs en cluster (BUI)

Cet exemple s'applique à une configuration active-active avec la moitié des ports réseau en veille. Cette tâche crée une interface IP via une liaison de données de périphérique et lui affecte une tête. Un VNIC est construit sur la même liaison de données, et une interface IP est configurée au sommet du VNIC puis affectée à l'autre tête. La configuration d'un VNIC au lieu de plusieurs VNIC via une même liaison de données assure les meilleures performances. Le trafic passe par un câble associé au port actif sous-jacent sur une tête, ainsi que sur le port de secours sous-jacent sur l'autre tête. De ce fait, le port de secours qui serait en veille peut être utilisé avec les VNIC.

1. Lorsque l'état du cluster est AKCS_CLUSTERED, cliquez sur l'icône  Liaisons de données.
2. (Facultatif) Définissez le nom et réglez le MTU.
3. Sélectionnez un périphérique dans la liste Périphériques et cliquez sur "APPLIQUER". La liaison de données s'affiche dans la liste Liaisons de données.
4. Cliquez sur l'icône  Interface.
5. Définissez les propriétés souhaitées, sélectionnez la liaison de données que vous venez de créer et cliquez sur "APPLIQUER". L'interface s'affiche dans la liste Interfaces.
6. Cliquez sur l'icône  Liaisons de données.

7. **Activez la case à cocher VNIC, définissez le nom et le MTU si vous le souhaitez (avec une valeur inférieure ou égale à celle de l'étape 2), et cliquez sur "APPLIQUER". La nouvelle liaison de données VNIC s'affiche dans la liste Liaisons de données.**
8. **Cliquez sur l'icône  Interface.**
9. **Définissez les propriétés souhaitées, sélectionnez la liaison de données VNIC que vous venez de créer et cliquez sur "APPLIQUER". L'interface s'affiche dans la liste Interfaces.**
10. **La configuration réseau de l'appareil en cours d'exécution n'est pas encore modifiée. Lorsque vous avez terminé la configuration des interfaces, cliquez sur "APPLIQUER" en haut de l'écran pour valider la configuration.**
11. **Cliquez sur l'onglet Cluster. Les interfaces nouvellement créées apparaissent dans la section Ressource avec les propriétaires par défaut.**
12. **Utilisez la liste déroulante Propriétaire pour affecter une des deux interfaces à l'autre tête et cliquez sur "APPLIQUER".**

▼ **Création de VNIC avec le même ID de VLAN pour des contrôleurs en cluster (BUI)**

Cet exemple s'applique à une configuration active-active avec la moitié des ports réseau en veille. Cette tâche crée deux VNIC avec des ID de VLAN identiques au sommet de la même liaison de données du périphérique. Chaque VNIC est configuré avec une interface, et chaque interface est affectée à une tête différente. Le trafic passe par un câble associé au port actif sous-jacent sur une tête, ainsi que sur le port de secours sous-jacent sur l'autre tête. De ce fait, le port de secours qui serait en veille peut être utilisé avec les VNIC.

1. **Lorsque l'état du cluster est AKCS_CLUSTERED, cliquez sur l'icône  Liaisons de données.**
2. **Activez la case à cocher VNIC, définissez le nom et le MUT (facultatif), définissez l'ID de VLAN, sélectionnez un périphérique dans la liste Périphériques et cliquez sur "APPLIQUER". La nouvelle liaison de données VNIC s'affiche dans la liste Liaisons de données.**
3. **Cliquez sur l'icône  Interface.**
4. **Définissez les propriétés souhaitées, sélectionnez la liaison de données VNIC que vous venez de créer et cliquez sur "APPLIQUER". L'interface s'affiche dans la liste Interfaces.**

5. Créez un autre VNIC comme décrit dans les étapes 1 et 2 avec le même périphérique et le même ID de VLAN, et créez l'interface correspondante comme décrit dans les étapes 3 et 4.
6. La configuration réseau de l'appareil en cours d'exécution n'est pas encore modifiée. Lorsque vous avez terminé la configuration des interfaces, cliquez sur "APPLIQUER" en haut de l'écran pour valider la configuration.
7. Cliquez sur l'onglet Cluster. Les interfaces nouvellement créées apparaissent dans la section Ressource avec les propriétaires par défaut.
8. Utilisez la liste déroulante Propriétaire pour affecter une des deux interfaces à l'autre tête et cliquez sur "APPLIQUER".

▼ Ajout d'une route statique (BUI)

1. Accédez à Configuration>Réseau>Routage.
2. Cliquez sur l'icône d'ajout.
3. Renseignez les propriétés comme indiqué ci-avant.
4. Cliquez sur "AJOUTER". La nouvelle route s'affiche dans la table.

▼ Suppression d'une route statique (BUI)

1. Accédez à Configuration>Réseau>Routage.
2. Placez le pointeur de la souris sur l'entrée de la route, puis cliquez sur l'icône de corbeille sur la droite.

Configuration réseau (CLI)

La configuration du réseau est accessible sous `configuration net`, qui dispose des sous-commandes `devices`, `datalinks`, `interfaces` et `routing`. La commande `show` peut être associée à chacune de ces sous-commandes pour afficher la configuration actuelle :

```
caji:> configuration net
caji:configuration net> devices show
Devices:
```

DEVICE	UP	SPEED	MAC


```

igb0      true  1000 Mbit/s  0:14:4f:9a:b9:0
igb1      true  1000 Mbit/s  0:14:4f:9a:b9:1
igb2      true  1000 Mbit/s  0:14:4f:9a:b8:fe
igb3      true  1000 Mbit/s  0:14:4f:9a:b8:ff

```

```

caji:configuration net> datalinks show
Datalinks:

```

DATALINK	CLASS	LINKS	LABEL
igb0	device	igb0	datalink1

```

caji:configuration net> interfaces show
Interfaces:

```

INTERFACE	STATE	CLASS	LINKS	ADDRS	LABEL
igb0	up	ip	igb0	192.168.2.80/22	caji

```

caji:configuration net> routing show
Properties:
    multihoming = loose

```

Routes:

ROUTE	DESTINATION	GATEWAY	INTERFACE	TYPE
route-000	0.0.0.0/0	192.168.1.1	igb0	dhcp
route-001	192.168.0.0/22	192.168.2.142	igb0	system

Saisissez `help` dans chaque section pour afficher les commandes pertinentes de création et de configuration de liaisons de données, d'interfaces et de routes. Les sous-commandes valides dans ce contexte sont les suivantes :

<code>help [topic]</code>	=> Get context-sensitive help. If [topic] is specified, it must be one of "builtins", "commands", "general", "help", "script" or "properties".
<code>show</code>	=> Show information pertinent to the current context
<code>commit</code>	=> Commit current state, including any changes
<code>abort</code>	=> Abort creation of "vnic"
<code>done</code>	=> Finish operating on "vnic"
<code>get [prop]</code>	=> Get value for property [prop]. ("help properties" for valid properties.) If [prop] is not specified, returns values for all properties.
<code>set [prop]</code>	=> Set property [prop] to [value]. ("help properties" for valid properties.) For properties taking list values, [value] should be a comma-separated list of values.
<code>available</code>	=> Get values that can be assigned to the links parameter when creating a network component.

La commande `available` permet d'afficher les valeurs pouvant être assignées au paramètre `links` lors de la création d'un composant réseau. L'exemple suivant illustre la sortie de la commande `available` de la CLI :

```
caji:configuration net datalinks> device
caji:configuration net datalinks device (uncommitted)> available
igb7,igb6

caji:configuration net datalinks> vnic
caji:configuration net datalinks vnic (uncommitted)> available
igb5,igb4,aggr2,aggr1

caji:configuration net datalinks> vlan
caji:configuration net datalinks vlan (uncommitted)> available
igb5,igb4,aggr2,aggr1

caji:configuration net datalinks> aggregation
caji:configuration net datalinks aggregation (uncommitted)> available
igb7,igb6

caji:configuration net interfaces> ip
caji:configuration net interfaces ip (uncommitted)> available
aggr2,aggr1

caji:configuration net interfaces> ipmp
caji:configuration net interfaces ipmp (uncommitted)> available
vnic4,vnic3,igb5,igb4
```

L'exemple suivant illustre la création d'un lien de données à l'aide de la commande `device` et d'une interface à l'aide de la commande `ip` :

```
caji:configuration net> datalinks
caji:configuration net datalinks> device
caji:configuration net datalinks device (uncommitted)> set links=igb1
links = igb1 (uncommitted)
caji:configuration net datalinks device (uncommitted)> set label=datalink2
label = datalink2 (uncommitted)
caji:configuration net datalinks device (uncommitted)> set mtu=9000
mtu = 9000 (uncommitted)
caji:configuration net datalinks device (uncommitted)> commit
caji:configuration net datalinks> show
Datalinks:

    DATALINK CLASS      LINKS      LABEL
    igb0 device        igb0       datalink1
    igb1 device        igb1       datalink2

caji:configuration net datalinks> cd ..
caji:configuration net> interfaces
caji:configuration net interfaces> ip
caji:configuration net interfaces ip (uncommitted)> set label="caji2"
label = caji2 (uncommitted)
caji:configuration net interfaces ip (uncommitted)> set links=igb1
links = igb1 (uncommitted)
```

```
caji:configuration net interfaces ip (uncommitted)> set v4addrs=10.0.1.1/8
v4addrs = 10.0.1.1/8 (uncommitted)
caji:configuration net interfaces ip (uncommitted)> commit
caji:configuration net interfaces> show
Interfaces:
```

INTERFACE	STATE	CLASS	LINKS	ADDRS	LABEL
igb0	up	ip	igb0	192.168.2.80/22	caji
igb1	up	ip	igb1	10.0.1.1/8	caji2

L'exemple suivant illustre la création d'une route par défaut via 10.0.1.2 passant par la nouvelle interface IP igb1 :

```
caji:configuration net routing> create
caji:configuration net route (uncommitted)> set family=IPv4
family = IPv4 (uncommitted)
caji:configuration net route (uncommitted)> set destination=0.0.0.0
destination = 0.0.0.0 (uncommitted)
caji:configuration net route (uncommitted)> set mask=0
mask = 0 (uncommitted)
caji:configuration net route (uncommitted)> set interface=igb1
interface = igb1 (uncommitted)
caji:configuration net route (uncommitted)> set gateway=10.0.1.2
gateway = 10.0.1.2 (uncommitted)
caji:configuration net route (uncommitted)> commit
```

▼ Configuration de l'interface de gestion (CLI)

Utilisez la procédure suivante pour configurer les interfaces de gestion.

1. Accédez à configuration net, puis entrez datalinks.

```
hostname:> configuration net
hostname:configuration net> datalinks
```

2. Saisissez show pour afficher les liaisons de données.

```
hostname:configuration net datalinks> show
Datalinks:
```

DATALINK	CLASS	LINKS	STATE	ID	LABEL
igb0	device	igb0	up	-	Untitled Datalink

3. Créez une carte VNIC pour la liaison de données de gestion en accédant au contexte vnic et en définissant son libellé pour indiquer que la liaison est destinée à la gestion. Vous pouvez éventuellement lui affecter un ID VLAN. Saisissez commit, puis cd .. pour revenir au contexte adapté à l'étape suivante.

```
hostname:configuration net datalinks> vnic
hostname:configuration net datalinks vnic (uncommitted)> set links=igb0
links = igb0 (uncommitted)
```

```
hostname:configuration net datalinks vnic (uncommitted)> set label=management-datalink-1
label = management-datalink-1 (uncommitted)
hostname:configuration net datalinks vnic (uncommitted)> commit
hostname:configuration net datalinks vnic> cd ..
```

Pour affecter un ID VLAN, procédez comme suit :

```
hostname:configuration net datalinks vnic> set id=100
id = 100 (uncommitted)
hostname:configuration net datalinks vnic (uncommitted)> commit
hostname:configuration net datalinks vnic> cd ..
```

4. **Dans le cas de contrôleurs clustérisés, créez une carte VNIC pour la deuxième liaison de données de gestion en accédant au contexte `vnic` et en définissant un libellé unique. Vous pouvez éventuellement lui affecter un ID VLAN. Saisissez `commit`, puis `cd ..` pour revenir au contexte adapté à l'étape suivante.**

```
hostname:configuration net datalinks> vnic
hostname:configuration net datalinks vnic (uncommitted)> set links=igb0
links = igb0 (uncommitted)
hostname:configuration net datalinks vnic (uncommitted)> set label=management-datalink-2
label = management-datalink-2 (uncommitted)
hostname:configuration net datalinks vnic (uncommitted)> commit
hostname:configuration net datalinks vnic> cd ..
```

Pour affecter un ID VLAN, procédez comme suit :

```
hostname:configuration net datalinks vnic (uncommitted)> set id=100
id = 100 (uncommitted)
hostname:configuration net datalinks vnic> commit
hostname:configuration net datalinks vnic> cd ..
```

5. **Créez une interface IP pour le contrôleur et affectez-la à la carte VNIC.**

```
hostname:configuration net> interfaces
hostname:configuration net interfaces> ip
hostname:configuration net interfaces ip (uncommitted)> set v4addrs=192.168.1.101/24
v4addrs = 192.168.1.101/24 (uncommitted)
hostname:configuration net interfaces ip (uncommitted)> set label=management-controller-1
label = management-controller-1 (uncommitted)
hostname:configuration net interfaces ip (uncommitted)> set links=vnic1
links = vnic1 (uncommitted)
hostname:configuration net interfaces ip (uncommitted)> commit
```

6. **Dans le cas de contrôleurs clustérisés, créez une interface IP et affectez-la à la carte VNIC du deuxième contrôleur. Saisissez `commit`, puis `done`.**

```
hostname:configuration net interfaces> ip
hostname:configuration net interfaces ip (uncommitted)> set v4addrs=192.168.1.102/24
v4addrs = 192.168.1.102/24 (uncommitted)
hostname:configuration net interfaces ip (uncommitted)> set label=management-controller-2
label = management-controller-2 (uncommitted)
```

```

hostname:configuration net interfaces ip (uncommitted)> set links=vnic2
links = vnic2 (uncommitted)
hostname:configuration net datalinks vnic (uncommitted)> commit
hostname:configuration net datalinks> done

```

7. **Configurez le routage pour le premier contrôleur. Dans le cas de contrôleurs clustérisés, configurez le routage pour le deuxième contrôleur. Saisissez `commit`, puis `done`.**

Premier contrôleur :

```

hostname:configuration net> routing
hostname:configuration net routing> create
hostname:configuration net route (uncommitted)> set destination=0.0.0.0
destination = 0.0.0.0 (uncommitted)
hostname:configuration net route (uncommitted)> set mask=0
mask = 0 (uncommitted)
hostname:configuration net route (uncommitted)> set interface=vnic1
interface = vnic1 (uncommitted)
hostname:configuration net route (uncommitted)> set gateway=192.168.1.1
gateway = 192.168.1.1 (uncommitted)
hostname:configuration net route (uncommitted)> set family=IPv4
family = IPv4
hostname:configuration net route (uncommitted)> commit
hostname:configuration net route> done

```

Deuxième contrôleur :

```

hostname:configuration net> routing
hostname:configuration net routing> create
hostname:configuration net route (uncommitted)> set destination=0.0.0.0
destination = 0.0.0.0 (uncommitted)
hostname:configuration net route (uncommitted)> set mask=0
mask = 0 (uncommitted)
hostname:configuration net route (uncommitted)> set interface=vnic2
interface = vnic2 (uncommitted)
hostname:configuration net route (uncommitted)> set gateway=192.168.1.1
gateway = 192.168.1.1 (uncommitted)
hostname:configuration net route (uncommitted)> set family=IPv4
family = IPv4
hostname:configuration net route (uncommitted)> commit
hostname:configuration net route> done

```

8. **Supprimez l'interface par défaut, nommée Interface sans titre, entrez `cd ...`, puis `done`.**

Remarque - Lorsqu'une interface est supprimée, toutes les routes qui lui sont associées le sont également.

```

hostname:configuration net> interfaces
hostname:configuration net interfaces> show

```

Interfaces:

INTERFACE	STATE	CLASS	LINKS	ADDRS	LABEL
igb0	up	ip	igb0	192.168.1.101/24	Untitled Interface
vnic1	duplicate	ip	vnic1	192.168.1.101/24	management-controller-1
vnic2	duplicate	ip	vnic2	192.168.1.102/24	management-controller-2

```
hostname:configuration net interfaces> destroy igb0
This will destroy "igb0" and any networking objects exclusively built over it.
```

```
Are you sure? (Y/N) y
```

```
hostname:configuration net interfaces> cd ..
```

```
hostname:configuration net> done
```

Rubriques connexes

- Pour une configuration plus approfondie, reportez-vous à la section "[Configuration de l'appareil](#)" du manuel *Guide d'administration des systèmes Oracle ZFS Storage Appliance, version OS8.6.0*.
- Pour mettre à niveau le logiciel sur un contrôleur autonome, reportez-vous à la section "[Mise à niveau du logiciel](#)" dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.
- Pour verrouiller les interfaces de gestion, reportez-vous à la section "[Verrouillage des interfaces de gestion de cluster \(CLI\)](#)" à la page 71.

▼ Configuration des interfaces réseau (CLI)

Avant de commencer

Pour assurer l'emploi des interfaces réseau appropriées pour les connexions de réplication entre les appareils source et cible, configurez des routes /32 (spécifiques aux hôtes).

Si vous configurez une réplication pour une configuration de cluster, sélectionnez une interface réseau singleton (déverrouillée) afin qu'à la suite d'une reprise ou d'un rétablissement de cluster, l'interface se déplace sur le noeud sur lequel l'opération de réplication est en cours. Les deux noeuds de cluster source peuvent effectuer une réplication sur le même noeud cible uniquement si le noeud source fournit deux adresses IP, une pour chaque noeud dans le cluster source. La réplication vers la même adresse IP cible depuis les deux noeuds d'un cluster source n'est pas prise en charge.

1. Accédez à configuration services routing sur l'appareil source.

Utilisez une route statique /32 (spécifique à l'hôte) vers l'adresse IP du système cible via l'interface réseau dédiée. Dans l'exemple suivant, mask=32 signifie qu'il s'agit d'une route spécifique à l'hôte.

```
host_source:configuration services routing> create
```

```
host_source:configuration services route (uncommitted)> get
family = (unset)
```

```
destination = (unset)
mask = (unset)
gateway = (unset)
interface = (unset)
host_source:configuration services route (uncommitted)> set family=IPv4
host_source:configuration services route (uncommitted)> set destination=203.34.56.78
host_source:configuration services route (uncommitted)> set mask=32
host_source:configuration services route (uncommitted)> set gateway=203.34.56.254
host_source:configuration services route (uncommitted)> set interface=nge3
host_source:configuration services route (uncommitted)> commit
host_source:configuration services routing> show
route-000  0.0.0.0/0                203.24.30.254  nge0          static
route-001  203.24.30.0/32           203.24.30.28   nge0          dynamic
route-002  203.24.150.0/32                203.24.150.10  ibd0          dynamic
route-003  203.24.101.65/32              203.24.30.254  nge1          inactive
route-005  203.34.56.78/32              203.34.56.254  nge3          static
```

2. **Après avoir défini la route statique de l'appareil source vers l'appareil cible, répétez ces étapes sur l'appareil cible pour définir la route statique de la cible vers la source.**
3. **Pour vérifier que le trafic est routé par le biais des bonnes interfaces source et cible, utilisez la commande `traceroute`.**

Pour plus d'informations sur l'utilisation de la commande `traceroute`, reportez-vous à la section "[Configuration du routage réseau](#)" à la page 81.

Remarque - Lorsqu'une interface est supprimée, toutes les routes qui lui sont associées le sont également.

Rubriques connexes

- "[Workflow de réplication distante](#)" à la page 474
- "[Concepts de la réplication distante](#)" à la page 529

▼ Verrouillage des interfaces de gestion de cluster (CLI)

Après la configuration initiale, les contrôleurs clustérisés sont à l'état actif-actif. Lorsqu'un basculement se produit, un contrôleur actif reprend toutes les interfaces non privées, et le contrôleur pair devient passif et inaccessible par la BUI et la CLI. Pour conserver l'accès à un contrôleur quel que soit son état, verrouillez son interface de gestion pour la rendre privée. La procédure suivante permet de verrouiller l'interface de gestion sur chaque contrôleur clustérisé.



Attention - Si vous ne configurez pas d'interfaces de gestion verrouillées sur des contrôleurs clustérisés, les temps de diagnostic et de résolution des pannes matérielles risquent d'être inutilement allongés.

1. **Sur le premier contrôleur, accédez à configuration cluster resources et sélectionnez l'interface de gestion du premier contrôleur, en la faisant précéder de net/.**

```
controller-a:> configuration cluster resources select net/igb0
```

2. **Verrouillez l'interface en définissant son type sur privé :**

```
configuration cluster resources (uncommitted)> set type=private  
configuration cluster resources (uncommitted)> commit
```

3. **Sur le deuxième contrôleur, accédez à configuration cluster resources et sélectionnez l'interface de gestion du deuxième contrôleur, en la faisant précéder de net/.**

```
controller-b:> configuration cluster resources select net/igb1
```

4. **Verrouillez l'interface en définissant son type sur privé :**

```
configuration cluster resources (uncommitted)> set type=private  
configuration cluster resources (uncommitted)> commit
```

Rubriques connexes

- Pour mettre à niveau le logiciel, reportez-vous à la section "[Mise à niveau du logiciel](#)" dans [le Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance](#).

▼ Ajout d'une route statique (CLI)

1. **Accédez à configuration net routing.**
2. **Saisissez create.**
3. **Saisissez show pour afficher la liste des propriétés requises et définissez chacune d'entre elles à l'aide de set.**
4. **Saisissez commit.**

▼ Suppression d'une route statique (CLI)

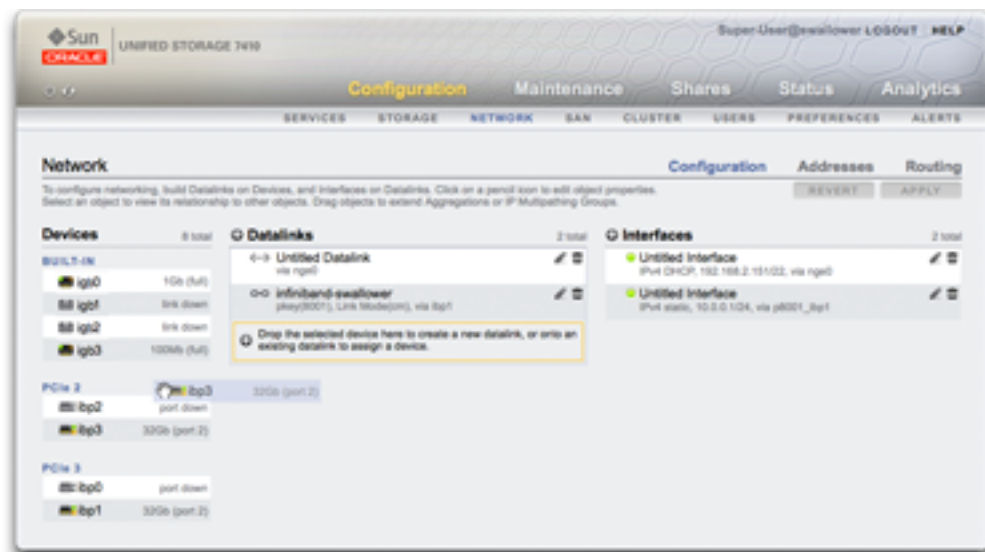
1. **Accédez à configuration net routing.**
2. **Saisissez show pour afficher la liste des routes et des noms de routes (par exemple, route-002).**
3. **Saisissez destroy nom de la route.**

▼ Réglage de la propriété de multihébergement sur strict (CLI)

1. Accédez à configuration net routing.
2. Saisissez `set multihoming=strict`.
3. Saisissez `commit`.

Utilisation de la page de configuration réseau

Dans un modèle d'appareil, les périphériques réseau sont créés par le système pour représenter les ports réseau ou InfiniBand disponibles : ils n'ont aucune propriété configurable. Les liaisons de données sont des entités de couche 2 et doivent être créées pour appliquer des paramètres tels que LACP à ces périphériques réseau. Les interfaces sont des entités de couche 3 contenant les paramètres IP, qu'elles mettent à disposition par le biais d'une liaison de données. Ce modèle a séparé les paramètres d'interface réseau en deux parties : les liaisons de données pour les paramètres de couche 2 et les interfaces pour les paramètres de couche 3.



La colonne Périphériques correspond aux ports de la carte d'interface réseau (NIC) physique sur le contrôleur, qui sont généralement intitulés igb0, igb1, igb2 et igb3. Le port NET-0 correspond au périphérique igb0, le port NET-1 à igb1, et ainsi de suite. Il est fortement recommandé d'utiliser un port NIC par contrôleur en tant qu'*interface de gestion*. Cette colonne contient

également les ports InfiniBand physiques sur le contrôleur, qui sont généralement intitulés ibp0, ibp1, ibp2 et ibp3.

La colonne Liaisons de données correspond à l'élément permettant d'envoyer et de recevoir des paquets pour un périphérique réseau spécifique. Les liaisons de données prennent en charge les VLAN, les cartes VNIC, les partitions IB et le groupement LACP. Les liaisons de données sont indispensables à l'achèvement de la configuration du réseau, même si elles n'appliquent pas des paramètres spécifiques aux périphériques réseau.

L'entité de liaison de données (que nous avons nommée "aggr1") rassemble les périphériques réseau de manière configurable (stratégie de groupement LACP). L'entité d'interface (que nous avons nommée "phobos") fournit des paramètres d'adresse IP configurables, qu'elle rend disponibles sur le réseau par le biais de la liaison de données. Les périphériques réseau (nommés "igb1", "igb2", ..., par le système) n'ont pas de paramètres directs.

La colonne Interfaces correspond aux paramètres d'adresse IP configurables et à d'autres propriétés pour les liaisons de données. Les interfaces sont accessibles via une liaison de données unique ou sont définies comme un groupe IPMP formé d'un pool de liaisons de données, qui permet la migration automatique des adresses IP en provenance de liaisons de données défaillantes vers des liaisons de données fonctionnelles.

L'exemple ci-dessous illustre une adresse IP unique sur un port unique (configuration fréquente) :

- Périphériques - igb0
- Liaison de données - datalink1
- Interface - deimos (192.168.2.80/22)

La configuration suivante correspond à un groupement de liaisons à 3 éléments :

- Périphériques - igb1, igb2, igb3
- Liaison de données - aggr1 (groupement LACP)
- Interface - phobos (192.168.2.81/22)

Configuration de l'interface de gestion

Si vous n'avez pas défini d'interface de gestion lors de la configuration initiale, utilisez les procédures suivantes pour configurer une carte d'interface réseau (NIC) en tant qu'interface de gestion. Une interface de gestion est une interface réseau avec accès d'administration.

Les ports physiques correspondent aux interfaces, à partir desquelles vous pouvez choisir de créer une interface de gestion. Tous les contrôleurs autonomes doivent être dotés d'au moins un port NIC configuré en tant qu'interface de gestion. Dans toutes les installations en cluster, chaque contrôleur doit être doté d'au moins un port NIC configuré en tant qu'interface de gestion. En outre, le numéro d'instance NIC doit être unique sur chaque contrôleur clustérisé.

Pour les contrôleurs clustérisés, il est recommandé de verrouiller les interfaces de gestion.

Pour configurer les interfaces de gestion et verrouiller les interfaces de gestion de cluster, utilisez les procédures suivantes :

- ["Configuration de l'interface de gestion \(BUI\)" à la page 55](#)
- ["Configuration de l'interface de gestion \(CLI\)" à la page 67](#)
- ["Verrouillage des interfaces de gestion de cluster \(BUI\)" à la page 56](#)
- ["Verrouillage des interfaces de gestion de cluster \(CLI\)" à la page 71](#)

Configuration des liaisons de données réseau

Les liaisons de données réseau gèrent les périphériques et sont utilisées par les interfaces. Elles prennent en charge :

- **Protocole LACP (Link Aggregation Control Protocol)** - Le protocole LACP permet de regrouper plusieurs périphériques réseau de manière à ce qu'ils se comportent comme un seul périphérique. Ceci améliore les performances (en augmentant la bande passante) et la fiabilité (en assurant une protection contre les pannes de port réseau). Toutefois, l'appareil doit être connecté à un commutateur prenant en charge LACP et ayant activé ce protocole pour ces ports.
- **Partitions InfiniBand (IB)** - Les partitions InfiniBand permettent la connexion à des domaines Fabric IB isolés de manière logique.
- **LAN virtuels (VLAN)** - Les LAN permettent d'améliorer la sécurité et l'isolement du réseau local. Les VLAN sont recommandés pour l'administration de l'appareil ; sinon, utilisez des VNIC.
- **VNIC (Virtual Network Interface, cartes d'interface de réseau virtuel)** - Les VNICS permettent de séparer les liaisons de données Ethernet simples ou groupées en plusieurs liaisons de données (Ethernet) virtuelles. Les VNIC peuvent être facultativement marqués avec des ID de VLAN et permettre le partage de port réseau physique dans un cluster. Vous trouverez des instructions détaillées dans la section ["Considérations relatives au clustering pour la gestion réseau" à la page 215](#) ci-dessous.

Remarque - Les liaisons de données basées sur des VNIC ou VLAN ne peuvent pas partager le même ID de VLAN.

La norme IEEE802.3ad (groupement de liaisons) ne prend pas explicitement en charge les groupements sur plusieurs commutateurs mais certains fournisseurs proposent la prise en charge de plusieurs commutateurs par le biais d'extensions propriétaire. Si un commutateur configuré avec ces extensions est conforme à la norme IEEE et que les extensions sont transparentes pour les nœuds finaux, son utilisation est prise en charge avec l'appareil. Si un problème est rencontré, le support Oracle peut demander à ce qu'il soit reproduit sur une configuration à un seul commutateur.

Les paramètres de liaisons de données suivants sont disponibles :

TABEAU 13 Paramètres de liaisons de données

Propriété	Description
Nom	Utiliser le nom personnalisé défini. Par exemple : "interne", "externe", "adminnet", etc.
Débit	Utiliser la vitesse définie. Les valeurs valides sont auto, 10, 100, 1000 et 10000, signifiant négociation automatique, 10Mbit/s forcé, 100Mbit/s forcé, 1Gbit/s forcé et 10Gbit/s forcé. Les valeurs de Speed et Duplex doivent être soit toutes deux forcées sur des valeurs données, soit toutes deux réglées sur négociation automatique. Certains périphériques réseau ne prennent pas en charge le réglage forcé sur toutes les combinaisons vitesse/duplex possibles. Il est fortement déconseillé de désactiver la négociation automatique. Toutefois, si la négociation automatique est désactivée sur le commutateur, la définition forcée de la vitesse (et de duplex) sur une valeur donnée peut être indispensable pour garantir l'exécution de la liaison de données à la vitesse et avec la valeur de duplex attendues.
Duplex	Utiliser la direction de transmission définie. Les valeurs de CLI valides sont auto, half et full, signifiant négociation automatique, semi-duplex et duplex intégral. Les valeurs de Speed et Duplex doivent être soit toutes deux forcées sur des valeurs données, soit toutes deux réglées sur négociation automatique.
VLAN	Utiliser des en-têtes VLAN.
ID de VLAN	Utiliser l'identifiant de VLAN défini (facultatif pour les VNIC).
VNIC	Utiliser un VNIC.
MTU	Utiliser la taille d'unité de transmission maximale (MUT) définie. La MTU par défaut est de 1 500 octets. Indiquez une MTU inférieure (1 280 au minimum) pour laisser un plafond de paquet (par exemple, pour les protocoles de mise en tunnel). Indiquez une MTU supérieure (9 000 au maximum) pour améliorer les performances réseau. Tous les systèmes et commutateurs du même réseau local (LAN) doivent être configurés sur la valeur de MTU sélectionnée. Une fois la valeur MTU réglée et la nouvelle configuration réseau validée pour le système, vous pouvez retourner à l'écran Réseau et afficher le statut de la liaison de données pour connaître la valeur de MTU exacte en octets qui a été sélectionnée. Notez qu'un VLAN ou VNIC ne peut pas être configuré à l'aide d'une valeur de MTU supérieure à celle de la liaison de données sous-jacente.
Groupe LACP	Utiliser le groupement LACP de périphériques réseaux multiples.
Stratégie LACP	Utiliser la stratégie LACP définie pour sélectionner un port sortant. L2 hache l'adresse MAC d'origine et de destination ; L3 utilise l'adresse IP d'origine et de

Propriété	Description
	destination ; L4 utilise le port de niveau de transport d'origine et de destination
Mode LACP	Utiliser le mode de communication LACP défini. Le mode Active envoie et reçoit des messages LACP pour négocier les connexions et surveiller le statut des liaisons. Le mode Passive écoute uniquement les messages LACP. Le mode Off utilise la liaison groupée mais ne détecte pas les défaillances de liaisons ou les changements de configuration du commutateur. Certaines configurations de commutateur réseau, notamment Cisco Etherchannel, n'utilisent pas le protocole LACP : le mode LACP doit être réglé sur "off" en cas d'utilisation d'un groupement non LACP sur le réseau.
Minuterie LACP	Utiliser l'intervalle défini entre les messages LACP pour le mode Actif.
Partition IB	Utiliser des partitions IB.
Clé de partition	Utiliser la partition (domaine Fabric) dont est membre le périphérique de port sous-jacent. La clé de la partition (pkey) est accessible et est configurée par le gestionnaire de sous-réseau. La clé pkey peut être définie avant la configuration du gestionnaire de sous-réseau, mais la liaison de données conserve le statut "down" tant que la partition de sous-réseau n'a pas été correctement configurée avec le GUID du port comme membre. Il est important que l'appartenance aux partitions des ports HCA reste conforme aux règles indiquées dans les sections "Configuration IPMP" à la page 314 et "Configuration d'appareils en cluster" à la page 191 pour le gestionnaire de sous-réseau.
Mode liaison IB	Utiliser le mode liaison IB défini. IPoIB fournit deux modes de liaison : Connexion (mode par défaut) et Datagramme non fiable. Le mode Connexion offre un meilleur rendement et est préférable au mode Datagramme non fiable. Utilisez ce dernier uniquement pour des raisons techniques. Le mode Connexion utilise les paires de files d'attente IB et dédie une paire de files d'attente locales à la communication avec une paire de files d'attente distantes. Le mode Connexion utilise un MTU de 65 520 et fournit un meilleur rendement que le mode Datagramme non fiable. Datagramme non fiable permet à une paire de files d'attente locales de communiquer avec plusieurs autres paires de files d'attente sur tous les hôtes et les messages sont communiqués de manière inconnue à la couche IB. Le mode Datagramme non fiable utilise un MTU de 2 044 et possède un rendement plus faible.

Configuration des interfaces réseau

Les interfaces configurent les adresses IP par le biais de liaisons de données. Elles prennent en charge :

- Les protocoles IPv4 et IPv6.
- IPMP - La fonctionnalité de multipathing IP, permettant d'augmenter la fiabilité du réseau en autorisant la migration automatique des adresses IP de liaisons de données défaillantes vers des liaisons de données opérationnelles.

Pour plus d'informations sur la manière de configurer des interfaces réseau, reportez-vous à la section ["Configuration des interfaces réseau \(CLI\)"](#) à la page 70.

Les paramètres d'interface suivants sont disponibles :

TABLEAU 14 Paramètres d'interface

Propriété	Description
Nom	Nom personnalisé de l'interface.
Activer l'interface	Active l'utilisation de l'interface concernée pour le trafic IP. Si une interface est désactivée, l'appareil n'envoie ou ne reçoit plus de trafic IP par son intermédiaire, et il n'utilise plus non plus les adresses IP qui y sont configurées. A l'heure actuelle, la désactivation d'une interface IP active dans un groupe IPMP ne déclenche pas l'activation d'une interface de secours.
Autoriser l'administration	Les connexions à la BUI ou à la CLI d'administration de l'appareil peuvent être autorisées via cette interface. Si votre environnement réseau comporte un réseau d'administration distinct, il est possible de n'activer cette option que pour le réseau d'administration afin d'améliorer la sécurité
IPv4 Configurer avec	Soit "Liste d'adresses statiques" saisies manuellement, soit "DHCP" pour les requêtes dynamiques
Adresse/Masque IPv4	Une ou plusieurs adresses IPv4, en notation CIDR (192.168.1.1/24)
IPv6 Configurer avec	Soit "Liste d'adresses statiques" pour une liste d'adresses saisie manuellement, soit "Configuration automatique IPv6" pour utiliser une adresse liaison locale automatiquement générée (et une adresse site local si une réponse est reçue d'un routeur IPv6)
Adresse/Masque IPv6	Une ou plusieurs adresses IPv6, en notation CIDR (1080::8:800:200C:417A/32)
Réseau(x) accessible(s) directement	Réseau(x) accessible(s) directement, exprimé(s) sous la forme d'une adresse IP et d'un masque en notation CIDR, dont l'adresse IP locale n'est pas membre, mais au(x)quel(s) la liaison de données de son interface est physiquement connectée. Cela améliore l'évolutivité en conservant l'adresse IP et peut réduire la congestion du trafic par le biais de commutateurs et de routeurs coeur.
Groupe IP MultiPathing	Configurer la fonctionnalité de chemins d'accès multiples, où un pool de liaisons de données peut être utilisé pour la redondance

Configuration du multiacheminement IP (IPMP) réseau

Les groupes IP MultiPathing servent à fournir des adresses IP qui restent disponibles en cas de défaillance d'une interface IP (due à la déconnexion d'un câble physique ou à une défaillance de la connexion entre un périphérique réseau et son commutateur par exemple), ou en cas de défaillance du chemin entre le système et ses passerelles système. Le système détecte les défaillances en surveillant les notifications de fonctionnement ou de défaillance de la liaison de données sous-jacente de l'interface IP et, de façon optionnelle, en effectuant des vérifications à l'aide d'adresses de test pouvant être assignées à chaque interface IP du groupe, comme décrit plus bas. Il est possible de placer un nombre quelconque d'interfaces IP dans un groupe IPMP, à condition qu'elles se trouvent toutes sur la même liaison (LAN, partition IB ou VLAN) ; de même, il est possible d'assigner un nombre quelconque d'adresses haute disponibilité à un groupe IPMP.

Au sein d'un groupe IPMP, chaque interface IP est désignée soit comme *active* ou *de secours* :

- **Active** : l'interface IP est utilisée pour envoyer et recevoir des données tant qu'IPMP établit qu'elle fonctionne correctement.
- **De secours** : l'interface IP est uniquement utilisée pour envoyer et recevoir des données si une interface active (ou une interface de secours précédemment activée) cesse de fonctionner.

Il est possible de configurer plusieurs interfaces IP actives et de secours, mais chaque groupe IPMP doit être configuré avec une interface IP active au moins. IPMP s'efforce d'activer autant d'interfaces IP de secours que nécessaire pour préserver le nombre d'interfaces actives configuré. Si un groupe IPMP est configuré avec deux interfaces actives et deux interfaces de secours par exemple et que toutes les interfaces fonctionnent correctement, seules les deux interfaces actives sont utilisées pour envoyer et recevoir des données. Si une interface active subit une panne, l'une des interfaces de secours est activée. Si l'autre interface active est défaillante (ou l'interface de secours activée tombe en panne), la seconde interface de secours est activée. Si, par la suite, les interfaces activées sont réparées, les interfaces de secours sont à nouveau désactivées.

Les interfaces IP peuvent être détectées par la détection via les liens ou via la détection par sonde (c'est-à-dire qu'une adresse de test est configurée).

Si la détection des défaillances basée sur sondes est activée sur une interface IP, le système détermine les systèmes cible à sonder de manière dynamique. La table de routage est tout d'abord analysée pour identifier les passerelles (routeurs) situées sur le même sous-réseau que l'adresse de test de l'interface IP, et jusqu'à cinq d'entre elles sont sélectionnées. Si aucune passerelle n'est trouvée sur le même sous-réseau, le système envoie une sonde ICMP multidiffusion (à 224.0.0.1. pour IPv4 ou ff02::1 pour IPv6) et sélectionne les cinq premiers systèmes situés sur le même sous-réseau qui envoient une réponse. Lors de la détection et de la réparation des défaillances réseau à l'aide d'IPMP, vous avez ainsi la garantie qu'au moins un

voisin sur chaque liaison ou que la passerelle par défaut répond aux demandes d'écho ICMP. IPMP fonctionne aussi bien avec des configurations d'adresse IPv4 qu'avec des configurations d'adresse IPv6. Dans le cas d'IPv6, l'adresse liaison locale est utilisée en tant qu'adresse de test.

Remarque - N'utilisez pas la détection des défaillances basée sur sondes lorsqu'aucun système (autre que le pair du cluster) sur le même sous-réseau que les adresses IPMP de test n'est configuré pour répondre aux demandes d'écho ICMP.

Le système sonde les systèmes cible à tour de rôle. Si cinq sondes successives restent sans réponse, l'interface IP est considérée comme défaillante. Inversement, s'il obtient des réponses à dix sondes successives, le système considère comme réparée une interface IP précédemment défaillante. Vous pouvez définir la valeur de temps de la détection des défaillances par sondes IPMP du système dans l'écran IPMP. Cette valeur détermine de manière indirecte le taux d'envoi des sondes et l'intervalle de réparation : un temps de détection des défaillances de 10 secondes, par exemple, signifie que le système envoie des sondes à intervalles de deux secondes environ et que le système aura besoin de 20 secondes pour détecter une réparation d'interface basée sur sondes. Vous ne pouvez pas contrôler directement les systèmes cible sélectionnés par le système, mais vous pouvez les contrôler de manière indirecte par le biais de la table de routage.

Le système surveille la table de routage et, le cas échéant, ajuste automatiquement les systèmes cible sélectionnés. Par exemple, si le système utilise des cibles détectées par multidiffusion, mais qu'une route comportant une passerelle sur le même sous-réseau que l'adresse de test de l'interface IP est ajoutée par la suite, le système passe automatiquement à l'envoi de sondes à la passerelle. De même, s'il procède à l'envoi de sondes à des cibles détectées par multidiffusion, le système actualise régulièrement l'ensemble de cibles sélectionnées, par exemple parce que des cibles précédemment sélectionnées ne répondent plus.

Pour obtenir des instructions détaillées sur la création de groupes IPMP, reportez-vous à la section "[Configuration IPMP](#)" à la page 314.

Pour plus d'informations sur les interfaces locales privées, reportez-vous à la section "[Configuration d'appareils en cluster](#)" à la page 191.

Configuration des performances et de la disponibilité réseau

IPMP et le groupement de liaisons sont des technologies différentes disponibles dans l'appareil pour améliorer les performances et préserver la disponibilité du réseau. En règle générale, le groupement de liaisons est mis en oeuvre pour accroître les performances du réseau, tandis qu'IPMP sert à assurer la haute disponibilité. Les deux technologies se complètent et, déployées conjointement, elles offrent les avantages cumulés d'un accroissement des performances et d'une augmentation de la disponibilité du réseau.

Dans les groupements de liaisons, le trafic entrant est réparti sur les multiples liaisons qui forment le groupement. Les performances du réseau augmentent alors à mesure que de nouvelles cartes réseau NIC sont installées pour ajouter des liaisons au groupement. Le trafic IPMP utilise les adresses de données de l'interface IPMP car elles sont liées aux interfaces actives disponibles. Si, par exemple, tout le trafic de données circule uniquement entre deux adresses IP mais pas nécessairement sur la même connexion, alors l'ajout de plusieurs cartes réseau n'améliore pas les performances avec IPMP car seules deux adresses IP restent utilisables.

Les performances peuvent souffrir du nombre de VNIC/VLAN configurés sur une liaison de données pour un périphérique donné, ainsi que de l'utilisation d'un ID de VLAN. La configuration de plusieurs VNIC via un périphérique donné peut avoir un impact sur les performances de toutes les liaisons de données pouvant atteindre cinq pourcents, même si les VNIC ne sont pas en cours d'utilisation. Si plus de huit VNIC/VLAN sont configurés via une même liaison de données, les performances peuvent être détériorées de manière significative. De plus, si un lien de données utilise un ID de VLAN, les performances de toutes les liaisons de données de ce périphérique subiront une réduction de cinq pourcents supplémentaires.

Configuration du routage réseau

Le système fournit une table de routage IP unique qui se compose d'un ensemble d'entrées de table de routage. Lorsqu'un paquet IP doit être envoyé à une destination donnée, le système sélectionne l'entrée de routage dont la destination est la plus proche de l'adresse de destination du paquet (en fonction de la stratégie de multihébergement du système, voir plus loin). Il se sert ensuite des informations de l'entrée de routage pour déterminer l'interface IP sur laquelle le paquet doit être envoyé - lorsque la destination n'est pas directement joignable - ainsi que la passerelle du prochain saut à utiliser. Si aucune entrée de routage ne concorde avec la destination, le paquet est rejeté. Si plusieurs entrées de routage rivalisent en tant que correspondance la plus proche (et que la stratégie de multihébergement n'accorde de priorité à aucune d'entre elles), le système effectue une répartition des charges sur ces entrées sur la base des connexions.

Le système ne fait pas office de routeur.

La table de routage se compose d'entrées de routage, chacune disposant des champs suivants :

TABLEAU 15 Champs d'entrée de routage

Champ	Description	Exemples
Destination	Ensemble d'adresses de destination IP (en notation CIDR) pouvant correspondre à la route	192.168.0.0/22
Gateway	Saut suivant (adresse IP) pour envoyer le paquet (excepté les routes "système", voir ci-dessous)	192.168.2.80

Champ	Description	Exemples
Family	Protocole Internet	IPv4, IPv6
Type	Origine de la route	dhcp, direct, statique, système
Status	Statut de la route	Active, inactive (route statique ou directe associée à une interface IP désactivée ou hors ligne).
Interface	Interface IP sur laquelle le paquet sera envoyé	igb0

Une entrée de routage dont le champ "destination" affiche `0.0.0.0/0` offre une correspondance avec n'importe quel paquet (à condition qu'aucune autre route ne présente de correspondance plus proche) et constitue donc une route "par défaut". Dans la BUI, les routes par défaut se distinguent des autres routes par une propriété supplémentaire :

TABEAU 16 Distinction entre les routes par défaut et les autres routes

Catégorie	Type de route	Par défaut, réseau

Comme indiqué plus haut, un paquet donné sera envoyé sur l'interface IP indiquée dans le champ "interface" de l'entrée de routage. Si une interface IPMP est indiquée, alors l'une des interfaces IP actives du groupe IPMP est sélectionnée au hasard sur la base des connexions et est automatiquement actualisée si l'interface IP sélectionnée devient inutilisable par la suite. Inversement, si une interface IP donnée fait partie d'un groupe IPMP, elle ne peut pas être indiquée dans le champs "interface" car une telle route ne serait pas hautement disponible.

Les entrées de routage proviennent d'un certain nombre d'origines différentes, comme indiqué par le champ "type". Bien que l'origine d'une entrée de routage ne détermine en aucune manière la façon dont elle est utilisée par le système, elle détermine si et comment l'entrée peut être modifiée ou supprimée. Le système prend en charge les types de routes suivants :

TABEAU 17 Types de routes pris en charge

Type	Description
Statique	Créée et gérée par l'administrateur de l'appareil.
Dynamique	Automatiquement créée par l'appareil via les protocoles de routage dynamiques RIP et RIPng (lorsqu'ils sont activés).
DHCP	Automatiquement créée par l'appareil dans le cadre de l'activation d'une interface IP configurée pour utiliser DHCP. Une route DHCP est créée pour chaque route par défaut fournie par le serveur DHCP.
Système	Automatiquement créée par l'appareil dans le cadre de l'activation d'une interface IP. Une route système est créée pour chaque sous-réseau IP directement joignable par l'appareil. Etant donné que ces routes sont directement joignables, le champ "passerelle" identifie

Type	Description
	à leur place l'adresse IP de l'appareil sur le sous-réseau concerné.
Direct	Créée et gérée comme une propriété d'interface réseau : Réseau(x) accessible(s) directement. Sous-réseau accessible directement, dont l'adresse IP locale n'est pas membre, mais auquel la liaison de données de son interface est physiquement connectée. Cela améliore l'évolutivité en conservant l'adresse IP et peut réduire la congestion du trafic par le biais de commutateurs et de routeurs cœur.

Remarquez que les routes directes sont configurées en tant qu'interfaces réseau à l'aide de l'écran Configuration > BUI réseau ou du contexte de la CLI configuration `net interfaces`. Les routes directes ne sont pas gérées par le biais de l'écran de routage de la BUI ni par le contexte de la CLI `routing`.

TABLEAU 18 Propriétés de routage

Propriété	Description
Modèle multihébergement	Contrôle la stratégie du système en ce qui concerne l'acceptation et la transmission de paquets IP lorsque plusieurs interfaces IP sont activées simultanément. Les valeurs autorisées sont "souple" (par défaut), "adaptative" et "stricte". Reportez-vous au tableau qui suit.

Si un système est configuré avec plusieurs interfaces IP, plusieurs routes équivalentes vers une destination donnée peuvent coexister, ce qui oblige le système à choisir l'interface IP par l'intermédiaire de laquelle envoyer un paquet. De même, un paquet peut arriver sur une interface IP, mais être destiné à une adresse IP hébergée par une autre interface IP. Dans de tels cas de figure, le comportement du système dépend de la stratégie de multihébergement sélectionnée. Trois stratégies sont prises en charge :

TABLEAU 19 Stratégies de multihébergement

Police	Description
Souple	Ne pas imposer de liaison entre un paquet IP et l'interface IP utilisée pour son envoi ou sa réception : 1) Un paquet IP est accepté sur une interface IP dès lors que son adresse IP de destination est activée sur l'appareil. 2) Un paquet IP est transmis via l'interface IP liée à la route concordant le mieux avec l'adresse de destination du paquet IP, sans que les adresses IP hébergées sur l'interface IP concernée n'entrent en ligne de compte. S'il n'existe aucune route qui corresponde, rejeter le paquet.
Adaptative	Identique à "souple", à la différence près que des routes possédant une adresse de passerelle sur le même sous-réseau que l'adresse IP source du paquet doivent

Police	Description
	être préférées : 1) Un paquet IP est accepté sur une interface IP dès lors que son adresse IP de destination est activée sur l'appareil. 2) Un paquet IP est transmis via l'interface IP liée à la route concordant le mieux avec l'adresse de destination du paquet IP. Si plusieurs routes correspondent aussi bien les unes que les autres, préférer les routes possédant une adresse de passerelle sur le même sous-réseau que l'adresse source du paquet. S'il n'existe aucune route qui corresponde, rejeter le paquet.
Stricte	Imposer une liaison stricte entre un paquet IP et l'interface IP utilisée pour son envoi ou sa réception : 1) Un paquet IP est accepté sur une interface IP dès lors que son adresse IP de destination est activée sur l'appareil. 2) Un paquet IP est uniquement transmis par le biais d'une interface IP si son adresse IP source est activée sur l'interface concernée. Pour appliquer cette règle, l'appareil ignore toutes les routes possédant des adresses de passerelle sur un sous-réseau différent de l'adresse source du paquet. S'il ne subsiste aucune route qui corresponde, rejeter le paquet.

L'un des principaux points à considérer lors de la sélection d'une stratégie de multihébergement est de savoir si l'une des interfaces IP de l'appareil sera dédiée à l'administration (pour un accès dédié à la BUI par exemple) et sera ainsi accessible via un réseau d'administration distinct. En particulier si une route par défaut est créée pour fournir un accès à distance au réseau d'administration et qu'une autre route par défaut est créée pour fournir un accès à distance aux protocoles de stockage, la stratégie système par défaut "souple" peut entraîner l'utilisation pour le trafic de stockage de la route par défaut pour l'administration. Si la stratégie "adaptative" ou "stricte" est sélectionnée, l'appareil tient compte de l'adresse IP associée à la demande au moment de la sélection de la route pour la réponse. Si aucune route n'est trouvée sur la même interface IP, le système utilise n'importe quelle route disponible avec la stratégie "adaptative", alors qu'avec la stratégie "stricte", le paquet est rejeté.

Configuration du stockage

L'appareil utilise des pools de stockage pour gérer des périphériques de stockage physique. Une fois que vous avez configuré ces pools en fonction des caractéristiques physiques et du niveau de redondance de données souhaité, vous pouvez stocker des systèmes de fichiers et des LUN, collectivement appelés partages, dans ces pools. Les partages, qui sont contenus dans des projets, augmentent automatiquement au sein de l'espace disque alloué au pool, et les pools peuvent s'étendre sur plusieurs périphériques de stockage. Il n'est pas nécessaire de dimensionner les partages de façon statique, mais vous pouvez contrôler l'utilisation de l'espace à l'aide de quotas et de réservations. Pour plus d'informations, reportez-vous à la section ["Gestion de l'espace pour les partages" à la page 400](#).

Pour configurer et gérer le stockage, utilisez ces tâches :

- Création d'un pool de stockage - [BUI](#), [CLI](#)
- Importation d'un pool de stockage existant - [BUI](#), [CLI](#)
- Ajout d'une étagère de disques à un pool de stockage existant - [BUI](#), [CLI](#)
- Ajout d'un périphérique de cache ou de journal à un pool de stockage existant - [BUI](#), [CLI](#)
- Suppression d'un périphérique de cache ou de journal d'un pool de stockage existant - [BUI](#), [CLI](#)
- Annulation de la configuration d'un pool de stockage - [BUI](#), [CLI](#)
- Modification du nom d'un pool de stockage - [BUI](#), [CLI](#)
- Nettoyage d'un pool de stockage - [BUI](#), [CLI](#)
- [Viewing Pool and Device Status](#)

Pour comprendre les notions de base du stockage, consultez les rubriques suivantes :

- ["Concepts liés aux pools de stockage" à la page 107](#)
- ["Profils de données pour les pools de stockage" à la page 108](#)
- ["Gestion de l'espace pour les partages" à la page 400](#)

▼ Création d'un pool de stockage (BUI)

Les pools de stockage permettent de stocker des données et peuvent être créés pendant ou après la configuration initiale. Les pools peuvent contenir des disques de données, des périphériques de cache de lecture et des périphériques de journal. Si, pour une raison quelconque, un pool n'est pas configuré, vous pouvez l'importer comme décrit dans la section ["Importation d'un pool de stockage existant \(BUI\)" à la page 89](#).

Avant de commencer

- Vous trouverez des recommandations concernant le nombre de disques à sélectionner par pool, reportez-vous à la section ["Nombre de périphériques par pool" à la page 108](#).
- Pour comprendre les différents profils de données, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).
- N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à Maintenance > Système.

1. **Accédez à Configuration > Stockage.**
2. **En regard de Pools disponibles, cliquez sur l'icône d'ajout .**
3. **Entrez un nom pour le pool de stockage, puis cliquez sur APPLIQUER.**

4. **Sélectionnez le nombre de disques de données affectés au pool de stockage pour chaque étagère de disques. Vous pouvez également sélectionner des périphériques de cache et de journal disponibles.**

Confirm that all devices are present and minimally functional, and allocate them to a storage pool. ABORT COMMIT

Verify and allocate devices Step 1 of 2

Verify that storage is correctly attached and functioning. If devices are missing or malfunctioning, they will not be available for use and cannot be added without reconfiguring the pool. It is recommended that you fix any problems before configuring storage on the appliance. Mixing device types and speeds is strongly discouraged.

NAME	MODEL	TYPE	RPM	DATA	LOG	CACHE
ar7320-230	Sun ZFS Storage 7320	System	--	-	-	0 (1.40T)
1235FMT007	Oracle Storage DE2-24C	HDD	7200	0 (19.1T)	-	-



Attention - Une fois qu'un disque a été ajouté à un pool, il ne peut en être retiré qu'au prix de la destruction intégrale du pool et de la perte de toutes les données.

Si toutes les étagères de disques connectées ne s'affichent pas, cliquez sur ABANDONNER, vérifiez le câblage et l'alimentation de l'étagère de disques, puis relancez cette procédure.

- Si toutes les unités présentent la même taille ou la même vitesse de rotation, ou si une taille est sélectionnée parmi plusieurs possibilités, le nombre maximum d'unités disponibles est alloué par défaut. Si le périphérique de stockage contient des disques de modèles différents ou présentant diverses vitesses de rotation, aucun disque n'est alloué par défaut.
- Il est fortement recommandé qu'un pool contienne uniquement les appareils avec des tailles et des vitesses de rotation identiques, afin de bénéficier de caractéristiques de performances constantes.
- Surveillez ou limitez l'utilisation d'espace car vous risquez de voir les performances chuter lorsque les pools approchent de leur pleine capacité.

5. **Cliquez sur VALIDER.**

Les unités sont allouées au pool de stockage, puis leur présence et leurs fonctionnalités minimales sont vérifiées. En cas d'échec de la vérification, cliquez sur ABANDONNER, corrigez le problème et relancez cette procédure. Si vous allouez un pool dont certains appareils sont manquants ou défectueux, vous ne pourrez pas ajouter les appareils manquants ou défectueux ultérieurement.

6. **Dans l'écran Choix d'un profil de stockage, sélectionnez le profil de données souhaité qui répond à vos objectifs de fiabilité, de disponibilité, de facilité de maintenance et de performances.**

Pour obtenir une description de chaque profil, cliquez sur le nom du profil de données, ou reportez-vous à la section "[Profils de données pour les pools de stockage](#)" à la page 108.

7. **Si vous avez alloué des périphériques de journalisation ou de cache, sélectionnez les profils appropriés.**

- Pour les périphériques de journalisation, cliquez sur Profil de journal et sélectionnez le profil en miroir ou entrelacé. Si vous avez alloué un nombre pair de périphériques de journalisation au pool, sélectionnez le profil en miroir.



Attention - Un double échec peut provoquer la perte des données du journal dans une configuration entrelacée. Il est fortement recommandé de configurer un profil de journalisation en miroir pour augmenter la redondance. Pour plus d'informations, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).

- Pour les périphériques de cache, le profil est toujours entrelacé, comme indiqué sous Profil de cache.

8. Cliquez sur **VALIDER**.

Rubriques connexes

- ["Importation d'un pool de stockage existant \(BUI\)" à la page 89](#)
- ["Ajout d'une étagère de disques à un pool de stockage existant \(BUI\)" à la page 91](#)
- ["Modification du nom d'un pool de stockage \(BUI\)" à la page 102](#)
- ["Concepts liés aux pools de stockage" à la page 107](#)

▼ Création d'un pool de stockage (CLI)

Les pools de stockage permettent de stocker des données et peuvent être créés pendant ou après la configuration initiale. Les pools peuvent contenir des disques de données, des périphériques de cache de lecture et des périphériques de journal. La tâche suivante présuppose que la configuration initiale est terminée. La création et la configuration d'un pool de stockage s'effectue en deux étapes. La présence et les fonctionnalités minimales des périphériques de stockage sont d'abord vérifiées, puis vous affectez des unités ou même des étagères de disques complètes au pool. Vous sélectionnez ensuite un profil pour les unités, en fonction des besoins de votre entreprise. Si, pour une raison quelconque, un pool est non configuré, vous pouvez l'importer comme décrit dans la section ["Importation d'un pool de stockage existant \(CLI\)" à la page 90](#).

Avant de commencer

- Vous trouverez des recommandations concernant le nombre de disques à sélectionner par pool, reportez-vous à la section ["Nombre de périphériques par pool" à la page 108](#).
- Pour comprendre les différents profils de données, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).
- N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à `maintenance system updates`.

1. Accédez à configuration storage.**2. Entrez config et le nom du nouveau pool de stockage.**

```
hostname: configuration storage> config pool0
hostname: configuration storage (pool0) verify>
```

3. Saisissez show pour afficher les informations du périphérique pour le pool :

```
hostname:configuration storage (pool0) verify> show
ID STATUS ALLOCATION DATA LOG CACHE RPM
0 ok custom 0 0 0/4 1.86T
1 ok custom 0 0/2 34G 0 15000
2 ok custom 0 0/2 34G 0 15000
```

4. Saisissez set et l'ID étagère de disques ou l'ID contrôleur, et le nombre de disques de données à utiliser. Vous pouvez également sélectionner des périphériques de cache et de journal disponibles.

Attention - Une fois qu'un disque a été ajouté à un pool, il ne peut en être retiré qu'au prix de la destruction intégrale du pool et de la perte de toutes les données.

L'ID "0" désigne le contrôleur et les ID restants correspondent aux étagères de disques. Dans l'exemple suivant, 1-data=8 alloue huit disques de données de la première étagère de disques.

```
hostname:configuration storage (pool1) verify> set 1-data=8
1-data = 8
```

Cet exemple alloue un périphérique de cache du contrôleur.

```
hostname:configuration storage (pool1) verify> set 0-cache=1
0-cache = 1
```

5. Saisissez done.

```
hostname:configuration storage (pool1) verify> done
```

6. Saisissez show pour afficher le profil.

```
hostname:configuration storage (pool1) config> show
PROFILE CAPACITY NSPF DESCRIPTION
log_profile = log_stripe 17G no Striped log
```

7. Si vous avez alloué des périphériques de journal au pool, saisissez set log_profile= et définissez le profil de journal sur log_mirror ou log_stripe. Utilisez log_mirror si le pool cette fois contient un nombre pair de périphériques de journal.



Attention - Un double échec peut provoquer la perte des données du journal dans une configuration entrelacée. Il est fortement recommandé de configurer un profil de journalisation en miroir pour augmenter la redondance. Pour plus d'informations, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108.](#)

```
hostname:configuration storage (pool1)> set log_profile=log_mirror
```

Remarque - Si vous avez alloué des périphériques de cache au pool, le profil est toujours entrelacé.

8. Saisissez **done** pour terminer la tâche .

```
hostname:configuration storage (pool1)> done
```

Rubriques connexes

- ["Importation d'un pool de stockage existant \(CLI\)" à la page 90](#)
- ["Ajout d'une étagère de disques à un pool de stockage existant \(CLI\)" à la page 93](#)
- ["Modification du nom d'un pool de stockage \(CLI\)" à la page 103](#)
- ["Concepts liés aux pools de stockage" à la page 107.](#)

▼ Importation d'un pool de stockage existant (BUI)

L'importation vous permet d'importer un pool de stockage non configuré. Un pool de stockage peut être non configuré par inadvertance, par une réinitialisation d'usine ou une opération de service pour récupérer des données utilisateur. L'importation d'un pool de stockage requiert le balayage de tous les périphériques de stockage connectés et la détection de tout état existant. Ces opérations peuvent prendre beaucoup de temps et empêchent la réalisation de toute autre opération de configuration du stockage.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à Maintenance > Système.

1. Accédez à Configuration > Stockage.

La liste des pools de stockage s'affiche, notamment certaines caractéristiques d'identification. Si l'espace de stockage a été détruit ou est incomplet, le pool de stockage ne peut pas être importé. Contrairement à ce qui se passe lors de la configuration du stockage, le nom du pool de stockage ne s'affiche pas initialement, mais après la sélection du pool.

2. Cliquez sur IMPORTER.

3. Sélectionnez le pool de stockage à importer.

Par défaut, les noms des pools de stockage précédents sont affichés.

4. **Pour renommer le pool de stockage, cliquez sur le nom du pool et modifiez-le.**
5. **Cliquez sur VALIDER.**

Rubriques connexes

- ["Annulation de la configuration d'un pool de stockage \(BUI\)" à la page 101](#)
- ["Modification du nom d'un pool de stockage \(BUI\)" à la page 102](#)

▼ Importation d'un pool de stockage existant (CLI)

L'importation vous permet d'importer un pool de stockage non configuré. Un pool de stockage peut être non configuré par inadvertance, par une réinitialisation d'usine ou une opération de service pour récupérer des données utilisateur. L'importation d'un pool de stockage requiert l'itération de tous les périphériques de stockage connectés et la détection de tout état existant. Ces opérations peuvent prendre beaucoup de temps et empêchent la réalisation de toute autre opération de configuration du stockage.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à `maintenance system updates`.

1. **Accédez à configuration storage.**
2. **Saisissez import.**

```
hostname:configuration storage (pool0)> import
```

Search for storage. Begin the process of searching for existing storage pools.

Subcommands that are valid in this context:

<code>help [topic]</code>	=> Get context-sensitive help. If [topic] is specified, it must be one of "builtins", "commands", "general", "help" or "script".
<code>show</code>	=> Show information pertinent to the current context
<code>abort</code>	=> Abort this task (potentially resulting in a misconfigured system)
<code>done</code>	=> Finish operating on "discover"

```
hostname:configuration storage (pool0) discover>
```

3. **Saisissez done.**

4. Saisissez show.

```
hostname:configuration storage (pool0)> show
Pools:
```

POOL	OWNER	DATA PROFILE	LOG PROFILE	STATUS	ERRORS
-> pool0	hostname	mirror	log_stripe	online	0
pool1	hostname	-	-	exported	-

```
Properties:
```

```

    pool = pool0
    status = online
    errors = 0
    owner = hostname
    profile = mirror
    log_profile = log_stripe
    cache_profile = cache_stripe
    scrub = none requested
```

5. Saisissez set pool= ainsi que le nom du pool à importer.

Remarque - Si vous possédez un seul pool, son nom n'est pas affiché, mais il est sélectionné.

```
hostname:configuration storage select> set pool=pool1
    pool = pool1
```

Un message vous rappelle de vérifier que le stockage est connecté et fonctionne correctement.

6. Saisissez done.**Rubriques connexes**

- ["Annulation de la configuration d'un pool de stockage \(CLI\)" à la page 101](#)
- ["Modification du nom d'un pool de stockage \(CLI\)" à la page 103](#)

▼ Ajout d'une étagère de disques à un pool de stockage existant (BUI)

Exécutez la tâche suivante pour ajouter une étagère de disques à un pool de stockage existant.

Avant de commencer

- Vous trouverez des recommandations concernant le nombre de disques à sélectionner par pool ainsi que d'autres considérations et conseils dans la section ["Concepts liés aux pools de stockage" à la page 107](#).
- Vous devez sélectionner le même profil de données que celui actuellement utilisé dans le pool existant. Pour comprendre les différents profils de données, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).

- Si le stockage disponible est insuffisant pour configurer le système pour le profil de données et ses options, certains attributs risquent de ne pas être pris en charge. Par exemple, il est impossible de conserver les caractéristiques NSPF lors de l'ajout d'une seule étagère de disques à une configuration RAID double parité avec l'option NSPF. Vous pouvez ajouter l'étagère de disques, mais vous ne pouvez pas utiliser l'option NSPF.
- N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à Maintenance > Système.



Attention - Une fois qu'un disque a été ajouté à un pool, il ne peut en être retiré qu'au prix de la destruction intégrale du pool et de la perte de toutes les données.

1. **Installez la nouvelle étagère de disques en suivant la procédure "Ajout d'une nouvelle étagère de disques" du *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.**
2. **Accédez à Configuration > Stockage.**
3. **Dans la liste de pools disponibles, sélectionnez le pool en ligne auquel vous ajoutez l'étagère de disques.**
4. **Cliquez sur AJOUTER.**
5. **Pour cette étagère de disques, sélectionnez le nombre de disques de données pour le pool de stockage.**

Si la nouvelle étagère de disques ne s'affiche pas, cliquez sur ABANDONNER, vérifiez le câblage et l'alimentation de l'étagère de disques, puis relancez cette procédure.

 - Si toutes les unités présentent la même taille ou la même vitesse de rotation, ou si une taille est sélectionnée parmi plusieurs possibilités, le nombre maximum d'unités disponibles est alloué par défaut. Si le périphérique de stockage contient des disques de modèles différents ou présentant diverses vitesses de rotation, aucun disque n'est alloué par défaut.
 - Il est fortement recommandé qu'un pool contienne uniquement les appareils avec des tailles et des vitesses de rotation identiques, afin de bénéficier de caractéristiques de performances constantes.
 - Surveillez ou limitez l'utilisation d'espace car vous risquez de voir les performances chuter lorsque les pools approchent de leur pleine capacité.
6. **(Facultatif) Ajoutez des périphériques de cache ou de journal de l'étagère de disques au pool.**
7. **Cliquez sur VALIDER.**
8. **Pour les disques de données, sélectionnez le même profil de données que celui utilisé dans le pool existant.**

9. **Si vous avez alloué des périphériques de journalisation ou de cache, sélectionnez les profils appropriés.**

- Pour les périphériques de journalisation, cliquez sur Profil de journal et sélectionnez le profil en miroir ou entrelacé. Si vous avez alloué un nombre pair de périphériques de journalisation au pool, sélectionnez le profil en miroir.



Attention - Un double échec peut provoquer la perte des données du journal dans une configuration entrelacée. Il est fortement recommandé de configurer un profil de journalisation en miroir pour augmenter la redondance. Pour plus d'informations, reportez-vous à la section "[Profils de données pour les pools de stockage](#)" à la page 108.

- Pour les périphériques de cache, le profil est toujours entrelacé, comme indiqué sous Profil de cache.

10. **Cliquez sur VALIDER.**

Rubriques connexes

- "[Annulation de la configuration d'un pool de stockage \(BUI\)](#)" à la page 101
- "[Ajout d'un périphérique de cache ou de journal à un pool de stockage existant \(BUI\)](#)" à la page 95

▼ **Ajout d'une étagère de disques à un pool de stockage existant (CLI)**

Exécutez la tâche suivante pour ajouter une étagère de disques à un pool de stockage existant.

Avant de commencer

- Vous trouverez des recommandations concernant le nombre de disques à sélectionner par pool ainsi que d'autres considérations et conseils dans la section "[Concepts liés aux pools de stockage](#)" à la page 107.
- Vous devez sélectionner le même profil de données que celui actuellement utilisé dans le pool existant. Pour comprendre les différents profils de données, reportez-vous à la section "[Profils de données pour les pools de stockage](#)" à la page 108.
- Si le stockage disponible est insuffisant pour configurer le système pour le profil de données et ses options, certains attributs risquent de ne pas être pris en charge. Par exemple, il est impossible de conserver les caractéristiques NSPF lors de l'ajout d'une seule étagère de disques à une configuration RAID double parité avec l'option NSPF. Vous pouvez ajouter l'étagère de disques, mais vous ne pouvez pas utiliser l'option NSPF.
- N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à `maintenance system updates`.



Attention - Une fois qu'un disque a été ajouté à un pool, il ne peut en être retiré qu'au prix de la destruction intégrale du pool et de la perte de toutes les données.

1. **Installez la nouvelle étagère de disques en suivant la procédure "Ajout d'une nouvelle étagère de disques" du *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.**
2. **Accédez à configuration storage.**
3. **Si vous disposez de plusieurs pools, un pool par défaut est sélectionné et affiché. S'il ne s'agit pas du pool auquel vous voulez ajouter le périphérique, saisissez `set pool=` et spécifiez un autre pool en ligne.**

Remarque - Si vous possédez un seul pool, son nom n'est pas affiché, mais il est sélectionné.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

Un message vous rappelle de vérifier que le périphérique est correctement installé. Notez qu'il est fortement déconseillé de mélanger des types et vitesses de périphériques différents.

4. **Saisissez `add`.**

```
hostname:configuration storage (pool1)> add
```

5. **Saisissez `show` pour afficher les informations du périphérique pour le pool :**

```
hostname:configuration storage (pool1) verify> show
ID STATUS ALLOCATION DATA LOG CACHE RPM
0 ok custom 0 0 0/4 0 1.86T
1 ok custom 0 0/2 34G 0 15000
2 ok custom 0 0/2 34G 0 15000
```

6. **Indiquez une étagère de disques ou le contrôleur et le nombre de disques de données à utiliser.**

L'ID "0" désigne le contrôleur et les ID restants correspondent aux étagères de disques. Dans l'exemple suivant, `1-data=8` alloue huit disques de données de la première étagère de disques.

```
hostname:configuration storage (pool1) verify> set 1-data=8
1-data = 8
```

7. **(Facultatif) Indiquez une étagère de disques ou le contrôleur et le nombre de périphériques de cache ou de journal à utiliser.**

L'ID "0" désigne le contrôleur et les ID restants correspondent aux étagères de disques. Dans l'exemple suivant, `set 0-cache=1` alloue un périphérique de cache du contrôleur :

```
hostname:configuration storage (pool1) verify> set 0-cache=1
```

0-cache = 1

8. Saisissez done.

```
hostname:configuration storage (pool1) verify> done
```

La présence et les fonctionnalités minimales des périphériques de stockage sont vérifiées. En cas d'échec de la vérification, corrigez le problème et relancez cette procédure. Si vous allouez un pool dont certains appareils sont manquants ou défectueux, vous ne pourrez pas ajouter les appareils manquants ou défectueux ultérieurement.

9. Saisissez show pour afficher le profil.

```
hostname:configuration storage (pool1) config> show
PROFILE  CAPACITY  NSPF  DESCRIPTION
log_profile  17G      no    Striped log
```

10. Entrez le même profil de données que le reste du pool en saisissant set profile= et le nom du profil.

11. Saisissez done.

12. Si vous avez alloué des périphériques de journal au pool, saisissez set log_profile= et log_mirror ou log_stripe. Utilisez log_mirror si le pool contient un nombre pair de périphériques de journal.

```
hostname:configuration storage (pool1)> set log_profile=log_mirror
```

Remarque - Si vous avez alloué des périphériques de cache au pool, le profil est toujours entrelacé.

13. Saisissez done.

Rubriques connexes

- ["Annulation de la configuration d'un pool de stockage \(CLI\)" à la page 101](#)
- ["Ajout d'un périphérique de cache ou de journal à un pool de stockage existant \(CLI\)" à la page 97](#)

▼ Ajout d'un périphérique de cache ou de journal à un pool de stockage existant (BUI)

Exécutez la tâche suivante pour ajouter un périphérique de cache de lecture ou un périphérique de journal à un pool de stockage existant.

Avant de commencer

- Vous trouverez des recommandations concernant le nombre de disques à sélectionner par pool ainsi que d'autres considérations et conseils dans la section ["Concepts liés aux pools de stockage" à la page 107](#).
- Vous devez sélectionner le même profil de données que celui actuellement utilisé dans le pool existant. Pour comprendre les différents profils de données, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).
- N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à Maintenance > Système.

1. **Installez le nouveau périphérique de cache de lecture ou de journal dans le premier emplacement disponible et adéquat. Pour déterminer l'emplacement approprié, reportez-vous à la section ["Disk Shelf Configurations" dans Oracle ZFS Storage Appliance Customer Service Manual](#).**
2. **Accédez à Configuration > Stockage.**
3. **Dans la liste de pools disponibles, sélectionnez le pool en ligne auquel vous ajoutez le périphérique.**
4. **Cliquez sur AJOUTER.**
5. **Sélectionnez le périphérique à ajouter au pool et cliquez sur VALIDER.**
6. **Si vous avez alloué des périphériques de journalisation ou de cache, sélectionnez les profils appropriés.**
 - Pour les périphériques de journalisation, cliquez sur Profil de journal et sélectionnez le profil en miroir ou entrelacé. Si vous avez alloué un nombre pair de périphériques de journalisation au pool, sélectionnez le profil en miroir.



Attention - Un double échec peut provoquer la perte des données du journal dans une configuration entrelacée. Il est fortement recommandé de configurer un profil de journalisation en miroir pour augmenter la redondance. Pour plus d'informations, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).

- Pour les périphériques de cache, le profil est toujours entrelacé, comme indiqué sous Profil de cache.

7. **Cliquez sur VALIDER.**

Rubriques connexes

- ["Suppression d'un périphérique de cache ou de journal d'un pool de stockage existant \(BUI\)" à la page 99](#)

- ["Ajout d'une étagère de disques à un pool de stockage existant \(BUI\)" à la page 91](#)

▼ Ajout d'un périphérique de cache ou de journal à un pool de stockage existant (CLI)

Exécutez la tâche suivante pour ajouter un périphérique de cache de lecture ou un périphérique de journal à un pool de stockage existant.

Avant de commencer

- Vous trouverez des recommandations concernant le nombre de disques à sélectionner par pool ainsi que d'autres considérations et conseils dans la section ["Concepts liés aux pools de stockage" à la page 107](#).
- Vous devez sélectionner le même profil de données que celui actuellement utilisé dans le pool existant. Pour comprendre les différents profils de données, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).
- N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à `maintenance system updates`.

1. **Installez le nouveau périphérique de cache de lecture ou de journal dans le premier emplacement disponible et adéquat. Pour déterminer l'emplacement approprié, reportez-vous à la section ["Disk Shelf Configurations" dans Oracle ZFS Storage Appliance Customer Service Manual](#).**
2. **Accédez à configuration storage.**
3. **Si vous disposez de plusieurs pools, un pool par défaut est sélectionné et affiché. S'il ne s'agit pas du pool auquel vous voulez ajouter un périphérique, saisissez `set pool=` et spécifiez un autre pool en ligne.**

Remarque - Si vous possédez un seul pool, son nom n'est pas affiché, mais il est sélectionné.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

Un message vous rappelle de vérifier que le stockage est connecté et fonctionne correctement.

4. **Saisissez `add` :**

```
hostname:configuration storage (pool1)> add
```

5. **Saisissez `show` pour afficher les informations du périphérique pour le pool.**

```
hostname:configuration storage (pool1) verify> show
ID STATUS ALLOCATION DATA LOG CACHE RPM
```

```

0      ok      custom      0      0      0/4      1.86T
1      ok      custom      0      0/2      34G      0      15000
2      ok      custom      0      0/2      34G      0      15000

```

6. Saisissez `set` et l'ID étagère de disques ou l'ID contrôleur, et le nombre de périphériques de cache ou de journal à utiliser.

L'ID "0" désigne le contrôleur et les ID restants correspondent aux étagères de disques. Dans l'exemple suivant, `2-log=1` alloue un périphérique de journal de la seconde étagère de disques.

```

hostname:configuration storage (pool1) verify> set 2-log=1
2-log = 1

```

Remarque - Une valeur de `"1-log=2"` allouerait deux périphériques de journal de la première étagère de disques.

Cet exemple alloue un périphérique de cache de la seconde étagère de disques.

```

hostname:configuration storage (pool1) verify> set 2-cache=1
2-cache = 1

```

7. Saisissez `done`.

```

hostname:configuration storage (pool1) verify> done

```

8. Saisissez `show` pour afficher le profil.

```

hostname:configuration storage (pool1) config> show
PROFILE          CAPCTY  NSPF  DESCRIPTION
log_profile = log_stripe    17G    no  Striped log

```

9. Si vous avez alloué des périphériques de journal au pool, saisissez `set log_profile=` et définissez le profil de journal sur `log_mirror` ou `log_stripe`. Utilisez `log_mirror` si le pool cette fois contient un nombre pair de périphériques de journal.



Attention - Un double échec peut provoquer la perte des données du journal dans une configuration entrelacée. Il est fortement recommandé de configurer un profil de journalisation en miroir pour augmenter la redondance. Pour plus d'informations, reportez-vous à la section ["Profils de données pour les pools de stockage" à la page 108](#).

```

hostname:configuration storage (pool1)> set log_profile=log_mirror

```

Remarque - Si vous avez alloué des périphériques de cache au pool, le profil est toujours entrelacé.

10. Saisissez `done` pour terminer la tâche .

```

hostname:configuration storage (pool1)> done

```

Rubriques connexes

- ["Suppression d'un périphérique de cache ou de journal d'un pool de stockage existant \(CLI\)" à la page 99](#)
- ["Ajout d'une étagère de disques à un pool de stockage existant \(CLI\)" à la page 93](#)

▼ Suppression d'un périphérique de cache ou de journal d'un pool de stockage existant (BUI)

Exécutez la tâche suivante pour supprimer un périphérique de cache de lecture ou de journal dans un pool de stockage existant.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à Maintenance > Système.

1. **Accédez à Configuration > Stockage.**
2. **Dans la liste de pools disponibles, sélectionnez le pool en ligne duquel supprimer le périphérique.**
3. **Cliquez sur SUPPRIMER.**
4. **Sélectionnez le nombre de périphériques de journal et de cache à supprimer du pool de stockage.**

Remarque - Si les périphériques de journal utilisent un profil en miroir, un message vous rappelle de sélectionner un nombre pair de périphériques de journal à supprimer. S'ils utilisent un profil entrelacé, vous pouvez supprimer un nombre pair ou impair de périphériques.

5. **Cliquez sur VALIDER.**

Rubriques connexes

- ["Ajout d'un périphérique de cache ou de journal à un pool de stockage existant \(BUI\)" à la page 95](#)

▼ Suppression d'un périphérique de cache ou de journal d'un pool de stockage existant (CLI)

Exécutez la tâche suivante pour supprimer un périphérique de cache de lecture ou de journal dans un pool de stockage existant.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à maintenance `system updates`.

1. **Accédez à configuration storage.**
2. **Si vous disposez de plusieurs pools, un pool par défaut est affiché et sélectionné. S'il ne s'agit pas du pool auquel vous voulez ajouter le périphérique, saisissez `set pool=` et spécifiez un autre pool en ligne.**

Remarque - Si vous possédez un seul pool, son nom n'est pas affiché, mais il est sélectionné.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. **Saisissez `show` pour afficher les informations du périphérique pour le pool.**

```
hostname:configuration storage (pool1) verify> show
ID STATUS ALLOCATION DATA LOG CACHE RPM
0 ok custom 0 0 0/4 1.86T
1 ok custom 0 0/2 34G 0 15000
2 ok custom 0 0/2 34G 0 15000
```

4. **Saisissez `remove`.**

```
hostname:configuration storage (pool1)> remove
```

5. **Indiquez le contrôleur ou l'étagère de disques ainsi que le nombre de périphériques de journal ou de cache à supprimer.**

L'ID "0" désigne le contrôleur et les ID restants correspondent aux étagères de disques. Dans l'exemple suivant, `1-log=2` supprime deux périphériques de journal de la première étagère de disques :

```
hostname:configuration storage (pool1) remove> set 1-log=2
1-log = 2
```

Cet exemple supprime un périphérique de cache du contrôleur :

```
hostname:configuration storage (pool1) remove> set 0-cache=1
0-cache = 1
```

6. **Saisissez `done`.**

```
hostname:configuration storage (pool1) remove> done
```

Remarque - Si les périphériques de journal utilisent un profil en miroir, un message vous rappelle de sélectionner un nombre pair de périphériques de journal à supprimer. Si les périphériques de journal utilisent un profil entrelacé, vous pouvez supprimer un nombre pair ou impair de périphériques.

Rubriques connexes

- ["Ajout d'un périphérique de cache ou de journal à un pool de stockage existant \(CLI\)" à la page 97](#)

▼ Annulation de la configuration d'un pool de stockage (BUI)

L'annulation de la configuration d'un pool de stockage retire les systèmes de fichiers et LUN actifs et remet à disposition l'espace de stockage brut pour une configuration ultérieure du stockage. Il est possible d'annuler ce processus en important le pool de stockage dont la configuration a été annulée, si l'espace de stockage brut n'a pas été utilisé entre-temps dans un pool de stockage actif.



Attention - L'annulation de la configuration d'un pool rend les données inaccessibles, crée un risque de perte de données et met en échec les répliquions entrantes.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à Maintenance > System.

1. **Accédez à Configuration > Stockage.**
2. **Dans la liste de pools disponibles, sélectionnez le pool en ligne dont vous souhaitez annuler la configuration.**
3. **Cliquez sur ANNULER LA CONFIGURATION.**

Rubriques connexes

- ["Importation d'un pool de stockage existant \(BUI\)" à la page 89](#)
- ["Modification du nom d'un pool de stockage \(BUI\)" à la page 102](#)

▼ Annulation de la configuration d'un pool de stockage (CLI)

L'annulation de la configuration d'un pool de stockage retire les systèmes de fichiers et LUN actifs et remet à disposition l'espace de stockage brut pour une configuration ultérieure du stockage. Il est possible d'annuler ce processus en important le pool de stockage dont la configuration a été annulée, si l'espace de stockage brut n'a pas été utilisé entre-temps dans un pool de stockage actif.



Attention - L'annulation de la configuration d'un pool rend les données inaccessibles, crée un risque de perte de données et met en échec les répliquions entrantes.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, naviguez jusqu'à `maintenance system updates` dans la CLI.

1. **Accédez à configuration storage.**
2. **Si vous disposez de plusieurs pools, un pool par défaut est sélectionné et affiché. S'il ne s'agit pas du pool dont vous voulez annuler la configuration, saisissez `set pool=` et spécifiez un autre pool en ligne.**

Remarque - Si vous possédez un seul pool, son nom n'est pas affiché, mais il est sélectionné.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. **Saisissez `unconfig`.**

```
hostname:configuration storage (pool1)> unconfig
```

4. **Saisissez `done`.**

Rubriques connexes

- ["Importation d'un pool de stockage existant \(CLI\)" à la page 90](#)
- ["Modification du nom d'un pool de stockage \(CLI\)" à la page 103](#)

▼ Modification du nom d'un pool de stockage (BUI)

Pour renommer un pool de stockage, vous devez annuler sa configuration puis importer immédiatement le pool avec un nouveau nom. Pendant l'annulation de la configuration du pool de stockage, les données ne sont pas accessibles et il existe un risque de perte de données. L'importation d'un pool de stockage peut prendre énormément de temps.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à `Maintenance > Système`.

1. **Accédez à Configuration > Stockage.**
2. **Dans la liste de pools disponibles, sélectionnez le pool en ligne à renommer.**

3. Cliquez sur **ANNULER LA CONFIGURATION**, puis sur **VALIDER**.
4. Cliquez sur **IMPORTER**, puis sélectionnez le pool de stockage dont vous venez d'annuler la configuration.
5. Cliquez sur le nom du pool de stockage et modifiez-le.
6. Cliquez sur **VALIDER**.

Rubriques connexes

- ["Annulation de la configuration d'un pool de stockage \(BUI\)" à la page 101](#)
- ["Importation d'un pool de stockage existant \(BUI\)" à la page 89](#)

▼ Modification du nom d'un pool de stockage (CLI)

Pour renommer un pool de stockage, vous devez annuler sa configuration puis importer immédiatement le pool avec un nouveau nom. Pendant l'annulation de la configuration du pool de stockage, les données ne sont pas accessibles et il existe un risque de perte de données. L'importation d'un pool de stockage peut prendre énormément de temps.

Avant de commencer

N'effectuez pas d'opération de configuration du pool lorsqu'une mise à niveau du microprogramme du disque est en cours. Pour vérifier si une mise à niveau est en cours, accédez à `maintenance system updates`.

1. **Accédez à `configuration storage`.**
2. **Si vous disposez de plusieurs pools, un pool par défaut est sélectionné et affiché. S'il ne s'agit pas du pool que vous voulez renommer, saisissez `set pool=` et spécifiez un autre pool en ligne.**

Remarque - Si vous possédez un seul pool, son nom n'est pas affiché, mais il est sélectionné.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. **Saisissez `unconfig`.**

```
hostname:configuration storage (pool1)> unconfig
```

4. **Saisissez `done`.**

5. **Saisissez `import`.**

```
hostname:configuration storage> import
```

Search for storage. Begin the process of searching for existing storage pools.

Subcommands that are valid in this context:

<code>help [topic]</code>	=> Get context-sensitive help. If [topic] is specified, it must be one of "builtins", "commands", "general", "help" or "script".
<code>show</code>	=> Show information pertinent to the current context
<code>abort</code>	=> Abort this task (potentially resulting in a misconfigured system)
<code>done</code>	=> Finish operating on "discover"

```
hostname:configuration storage> discover>
```

6. Saisissez done.

7. Pour sélectionner le pool de stockage dont vous venez d'annuler la configuration, entrez `set pool=` et le nom du pool.

```
hostname:configuration storage select> set pool=pool1
pool = pool1
```

8. Pour renommer le pool de stockage, entrez `set name=` et un nouveau nom.

```
hostname:configuration storage (pool1)> set name=NewPool
pool = NewPool
```

9. Saisissez done.

Rubriques connexes

- ["Annulation de la configuration d'un pool de stockage \(CLI\)" à la page 101](#)
- ["Importation d'un pool de stockage existant \(CLI\)" à la page 90](#)

▼ Nettoyage d'un pool de stockage (BUI)

Le nettoyage d'un pool de stockage permet de vérifier son contenu en recherchant les éventuelles erreurs. Si des erreurs irrécupérables sont identifiées, soit à l'occasion d'un nettoyage, soit dans le cadre du fonctionnement normal, la BUI affiche les fichiers affectés.

En général, un nettoyage doit être effectué au minimum lors de l'expiration de la sauvegarde la plus ancienne. Il est recommandé d'effectuer un nettoyage tous les trois mois environ. Un nettoyage doit également être exécuté avant une mise à niveau de logiciel.

1. **Accédez à Configuration > Stockage.**
2. **Dans la liste de pools disponibles, sélectionnez le pool en ligne à nettoyer.**
3. **Cliquez sur NETTOYAGE.**
Le statut du nettoyage s'affiche, notamment la date et l'heure du nettoyage, le nombre d'erreurs et les noms des fichiers présentant des erreurs.
4. **(Facultatif) Pour arrêter le nettoyage, cliquez sur ARRETER.**
Si vous cliquez à nouveau sur NETTOYAGE, le nettoyage reprend là où il s'est arrêté.

Rubriques connexes

- ["Concepts liés aux pools de stockage" à la page 107](#)

▼ Nettoyage d'un pool de stockage (CLI)

Le nettoyage d'un pool de stockage permet de vérifier son contenu en recherchant les éventuelles erreurs. Si des erreurs irrécupérables sont identifiées, soit à l'occasion d'un nettoyage, soit dans le cadre du fonctionnement normal, la CLI affiche les fichiers affectés. Si vous le souhaitez, vous pouvez interrompre le processus de nettoyage avant la fin.

En général, un nettoyage doit être effectué au minimum lors de l'expiration de la sauvegarde la plus ancienne. Il est recommandé d'effectuer un nettoyage tous les trois mois environ. Un nettoyage doit également être exécuté avant une mise à niveau de logiciel.

1. **Accédez à configuration storage.**
2. **Si vous disposez de plusieurs pools, un pool par défaut est sélectionné et affiché. S'il ne s'agit pas du pool que vous voulez nettoyer, saisissez `set pool=` et spécifiez un autre pool en ligne.**

Remarque - Si vous possédez un seul pool, son nom n'est pas affiché, mais il est sélectionné.

```
hostname:configuration storage (pool0)> set pool=pool1
pool = pool1
```

3. **Entrez `scrub start`.**

hostname:configuration storage (pool1)> **scrub start**
4. **(Facultatif) Pour arrêter le nettoyage avant la fin, saisissez `scrub stop`.**

hostname:configuration storage (pool1)> **scrub stop**

Si vous entrez à nouveau la commande `scrub start`, le nettoyage reprend là où il s'est arrêté.

Rubriques connexes

- ["Concepts liés aux pools de stockage" à la page 107](#)

▼ Consultation du statut des pools et des périphériques (BUI)

Vous pouvez vérifier le statut des pools et des périphériques qui les composent. En cas de problème sur un pool, des informations sur le statut des périphériques sont également fournies.

1. **Accédez à Configuration > Stockage.**
2. **Cliquez sur un pool pour le sélectionner et afficher des détails supplémentaires.**
Le tableau suivant décrit les différents statuts d'un pool.

Statut du pool	Description
En ligne	Pool dont tous les périphériques fonctionnent normalement.
Détérioré	Pool présentant un ou plusieurs périphériques défectueux, mais les données sont toujours disponibles grâce à la configuration redondante.
En panne	Un ou plusieurs périphériques sont hors ligne et il n'existe pas suffisamment de répliques pour assurer la poursuite du fonctionnement.
Hors ligne	Un pool a été mis hors ligne explicitement.
Non disponible	Pool dont les métadonnées sont endommagées ou qui comprend un ou plusieurs périphériques indisponibles et des répliques insuffisantes pour continuer de fonctionner.
Exporté	Un pool est actif sur le pair du cluster et il est prêt pour une opération de rétablissement du cluster.

3. **Consultez le statut des périphériques du pool sélectionné dans la section Statut des périphériques.**

Les statuts de périphérique sont décrits dans le tableau suivant.

Statut du périphérique	Description
En ligne	Le périphérique est en ligne et fonctionnel. Il se peut que ce statut ne s'affiche pas et qu'un message du type "Aucune panne n'a été détectée dans le pool de stockage" apparaisse à la place.
Détérioré	Le périphérique n'est pas dans un état optimal. Soit il est sur le point de tomber en panne, soit la réargerture d'une pièce de rechange n'est pas encore terminée.
En panne	Le périphérique est défectueux ; des informations complémentaires sont fournies dans les journaux de maintenance.

Statut du périphérique	Description
Hors ligne	Le périphérique a été mis hors ligne explicitement ; aucune opération de lecture ou d'écriture n'y sera effectuée tant qu'il n'aura pas été remis en ligne.
Retiré	Le périphérique a été retiré physiquement.
Hot spare	Ce périphérique de rechange est utilisé activement en tant que disque de données dans le pool pour remplacer un périphérique tombé en panne.
Non disponible	Le périphérique n'a pas pu être ouvert ou le pool n'a pas réussi à le détecter.

4. **Pour obtenir des informations plus détaillées sur les erreurs des pool et des périphériques, accédez à Maintenance > Problèmes (pour les erreurs actives) ou à Maintenance > Journaux (pour l'historique de tous les problèmes).**

Concepts liés aux pools de stockage

Le stockage est configuré en pools caractérisés par leur redondance de données sous-jacente, et offre de l'espace partagé entre tous les systèmes de fichiers et LUN. Pour plus d'informations sur la relation entre les pools de stockage et les différents systèmes de fichiers ou LUN, reportez-vous à la section ["A propos des pools de stockage, des projets et des partages" à la page 361](#).

Configuration des pools de stockage

La création de pools peut s'effectuer par configuration d'un nouveau pool ou importation d'un pool existant. L'importation de pools existants ne peut servir qu'à importer des pools précédemment configurés sur un appareil Oracle ZFS Storage Appliance. Elle est utile en cas de reconfiguration involontaire, par exemple un déplacement de pools entre contrôleurs, ou à la suite d'une panne catastrophique de contrôleur.

Pools multiples

Chaque contrôleur peut comporter un nombre de pools quelconque et l'appartenance des pools peut être librement définie au sein d'un cluster. Avec la possibilité de contrôler l'accès aux périphériques de journalisation ou de mise en cache en fonction des partages, le mode de fonctionnement recommandé est la configuration d'un pool unique. Bien qu'un nombre quelconque de pools soit pris en charge, la création d'un grand nombre de pools présentant les mêmes caractéristiques de redondance et appartenant à la même tête de cluster n'est pas recommandée, car elle entraîne une détérioration des performances, une allocation non optimale des ressources, un partitionnement artificiel du stockage et accroît l'effort d'administration. La configuration de plusieurs pools sur le même hôte est uniquement recommandée si des caractéristiques de redondance ou de performances radicalement différentes sont requises, par exemple un pool mis en miroir pour les bases de données et un pool RAID-Z pour les charges de travail de transmission.

Nombre de périphériques par pool

Les unités peuvent être allouées individuellement dans l'ensemble du châssis, mais un soin particulier doit être apporté à l'allocation de disques appartenant à des étagères de disques afin de garantir des configurations de pools optimales. En règle générale, une configuration comportant un petit nombre de pools et un grand nombre de disques par pool est préférable à la configuration inverse, car une telle configuration facilite la gestion et offre un pourcentage plus élevé de capacité totale utilisable.

Bien que le système soit en mesure d'allouer l'espace de stockage par incréments quelconques, il est recommandé que chaque allocation comprenne 8 disques répartis sur toutes les étagères de disques au minimum, et beaucoup plus dans l'idéal.

Caractéristiques et performances des disques

Respectez les restrictions suivantes lorsque vous configurez des pools de stockage :

- Tous les disques de données contenus dans un noeud de tête ou une étagère de disques doivent avoir la même vitesse de rotation (vitesse de rotation des médias). Le logiciel de l'appareil détecte les mauvaises configurations et génère une erreur à leur propos.
- En raison de problèmes de performances non prévisibles, évitez d'associer différentes vitesses de rotation de disque au sein d'un même pool.
- Pour obtenir des performances optimales, n'associez pas des étagères de disques présentant différentes vitesses de rotation de disque dans le même Fabric SAS (connexion HBA). Une telle association fonctionne correctement, mais les performances des périphériques les plus rapides sont susceptibles d'être ralenties.
- Evitez d'associer des disques de capacité différente au sein d'un même pool. Lors de la configuration de pools de stockage contenant des disques de données de capacité différente, ZFS affecte dans certains cas la taille des disques de capacité moindre à certains disques ou à tous les disques du pool de stockage, réduisant ainsi la capacité totale attendue. Les tailles utilisées dépendent du profil de stockage, de la configuration et des périphériques associés.

Capacité de pool de stockage

Lors de l'allocation d'espace de stockage brut aux pools, gardez à l'esprit qu'un remplissage complet des pools entraîne une détérioration importante des performances, en particulier lors de l'écriture vers des partages ou des LUN. Ces effets deviennent de plus en plus perceptibles à mesure que le pool approche de sa capacité maximale.

Profils de données pour les pools de stockage

Une fois que les périphériques de stockage sont vérifiés physiquement et que des ressources sont allouées à un pool de stockage, l'étape suivante consiste à choisir un profil de stockage

qui correspond à vos objectifs en matière de fiabilité, disponibilité et facilité de maintenance (RAS), ainsi qu'en termes de performances. L'ensemble de profils proposés dépend du stockage disponible. Le tableau suivant répertorie tous les profils possibles et leur description.

TABLEAU 20 Profils de données

Profil de données	Description
Options double parité	
Triple mirrored	Les données sont triplement mises en miroir et garantissent un système haute fiabilité à performances élevées (idéal pour le stockage d'une base de données critique par exemple). Cette configuration est prévue pour les situations où des performances et une disponibilité maximales sont nécessaires. Par rapport à la mise en miroir double, la mise en miroir triple permet une augmentation du nombre d'opérations d'E/S par seconde (IOPS) par bloc stocké et une meilleure protection contre les pannes. Remarque : un contrôleur sans stockage d'extension ne doit pas être configuré avec une mise en miroir triple.
Double parity RAID	Système RAID dans lequel chaque bande contient deux disques de parité. Comme pour la mise en miroir triple, ceci garantit une haute disponibilité, étant donné que les données restent disponibles en cas de défaillance de deux disques quelconques. Le RAID double parité est une option offrant une capacité plus grande que les options de mise en miroir et est prévue soit pour les charges de travail haut débit à accès séquentiel (telles que les sauvegardes), soit pour le stockage de grands volumes de données à composante lecture aléatoire faible.
Options simple parité	
Mirrored	Les données sont mises en miroir, ce qui réduit de moitié la capacité, mais le système obtenu présente une haute fiabilité et des performances élevées. Cette option est recommandée lorsque l'espace disponible est abondant et que des performances élevées sont considérées primordiales (pour le stockage de bases de données par exemple).
Single parity RAID, narrow stripes	Système RAID dans lequel chaque bande est limitée à trois disques de données et un disque simple parité. Pour les situations dans lesquelles la protection simple parité est suffisante, le RAID simple parité constitue une solution à capacité bien supérieure à la mise en miroir simple. A cette capacité accrue s'opposent des performances de lecture aléatoire inférieures à celles des options avec mise en miroir. Le RAID simple parité peut entrer en ligne de compte pour les applications non critiques à composante lecture aléatoire modérée. Pour les charges de travail impliquant uniquement la transmission en continu, préférez l'option RAID double parité, qui offre une capacité supérieure et un débit plus élevé.
Autre	

Profil de données	Description
Striped	Les données sont agrégées par bandes sur plusieurs disques, sans redondance. Bien que les performances et les capacités soient maximisées, toute panne de disque se solde par une perte de données. Cette configuration n'est pas recommandée. Pour les charges de travail impliquant uniquement la transmission en continu, envisagez d'utiliser l'option RAID double parité. En raison de l'absence de redondance, les disques configurés avec ce profil entrelacé ne reçoivent pas les mises à jour de microprogramme, sauf si les pools de stockage configurés sont dans l'état Exporté.
Triple parity RAID, wide stripes	Système RAID dans lequel chaque bande contient trois disques de parité. Il s'agit de l'option offrant la plus grande capacité, exception faite de l'option Striped Data. La réécriture de données après la défaillance d'une ou de plusieurs unités peut prendre bien plus de temps en raison de la largeur des bandes et des faibles performances d'E/S aléatoires. Comme pour d'autres configurations RAID, la présence d'un cache peut corriger les effets sur les performances de lecture. Cette configuration n'est pas recommandée en règle générale.

Remarque - Les versions antérieures des logiciels prenaient en charge la double parité avec bandes larges. Cette option a été remplacée par la triple parité avec bandes larges, car cette dernière améliore sensiblement la fiabilité. Les pools configurés avec l'option double parité avec bandes larges dans une version antérieure du logiciel sont toujours pris en charge, mais les nouveaux pools configurés ou les pools reconfigurés ne peuvent pas sélectionner cette option.

Pour les systèmes extensibles, certains profils peuvent être disponibles avec une option "NSPF". Ce sigle signifie "no single point of failure" (aucun point de panne unique) et indique que les données sont organisées en miroirs ou en bandes RAID de telle manière qu'une panne d'étagère de disques pathologique ne provoque aucune perte de données. Notez que les systèmes sont déjà configurés de manière à assurer la redondance de la quasi-totalité des composants. Chaque étagère de disques a des chemins redondants, des contrôleurs redondants ainsi que des alimentations et des ventilateurs redondants. Les seules pannes vis-à-vis desquelles NSPF offre une protection sont une panne de backplane de disque (un composant essentiellement passif) ou une erreur d'administration grave (dissociation des deux chemins vers une étagère de disques). En général, l'activation de NSPF entraîne une réduction de la capacité, car cette option s'accompagne d'exigences supplémentaires par rapport à la largeur de bande.

Les périphériques de journalisation peuvent uniquement être configurés à l'aide de l'un des deux profils suivants : striped ou mirrored. Les périphériques de journal sont uniquement utilisés en cas de défaillance d'un noeud. L'unique cas de figure où des données risquent d'être perdues avec des journaux non mis en miroir est une panne de périphérique immédiatement suivie d'une réinitialisation du noeud. Il s'agit d'un scénario hautement improbable. Cependant, une mise en miroir des périphériques de journalisation permet d'éliminer complètement ce risque, car il nécessiterait alors deux pannes de périphérique simultanées et une défaillance du noeud dans un laps de temps très court.

Remarque - Lorsque des périphériques de journalisation de tailles différentes se trouvent dans différents châssis, seuls les profils de journaux striped peuvent être créés.

Les disques hot spare sont alloués sous forme de pourcentage de la taille totale du pool et sont indépendants du profil sélectionné (à l'exception de 'striped', qui ne prend pas en charge les disques hot spare). Etant donné que les disques hot spare sont alloués pour chaque étape de configuration du stockage, il est bien plus efficace de configurer le stockage comme un tout plutôt que d'ajouter de l'espace de stockage par petits incréments.

Dans une configuration de cluster, les périphériques de cache installés dans les emplacements du contrôleur sont disponibles uniquement pour le nœud pour lequel le pool de stockage est importé. Dans un cluster, il est possible de configurer des périphériques de mise en cache sur les deux nœuds destinés à faire partie du même pool. Pour ce faire, reprenez le pool sur le nœud passif, puis ajoutez du stockage et sélectionnez les périphériques de mise en cache. De cette manière, à tout moment donné, la moitié du nombre total de périphériques de mise en cache est configurée. Tandis que les données des périphériques de mise en cache sont perdues en cas de basculement, les nouveaux périphériques de mise en cache peuvent être utilisés sur le nouveau nœud.

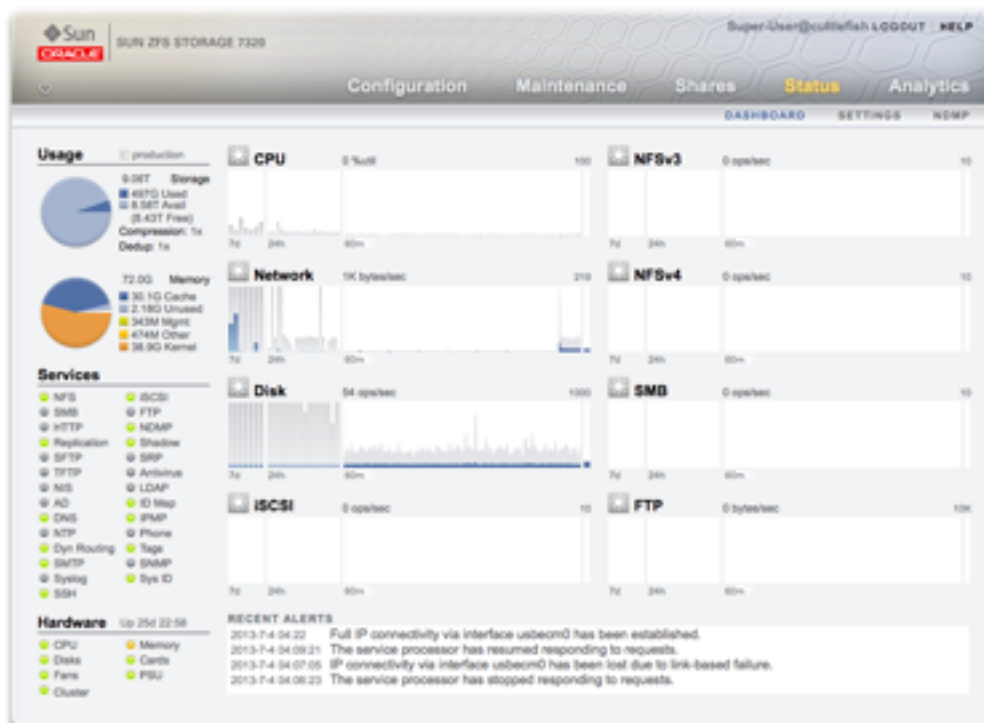
Lorsqu'ils sont ajoutés à un pool, les périphériques de cache installés dans des emplacements d'étagère de disques sont automatiquement importés lors de la reprise ou du rétablissement du cluster. Aucune configuration de pool supplémentaire n'est nécessaire.

Présentation du statut de l'appareil

La section Statut présente un récapitulatif du statut de l'appareil et des options de configuration. Les sections suivantes fournissent plus d'informations sur les concepts et procédures mis en oeuvre dans les vues de statut de l'appareil et la configuration des services correspondants :

- ["A propos d'Oracle ZFS Storage Appliance" à la page 17](#)
- ["Statut sur le tableau de bord" à la page 112](#)
- ["Résumé de l'utilisation de la mémoire" à la page 117](#)
- ["Tableau de bord d'activité du disque" à la page 118](#)
- ["CLI du tableau de bord" à la page 120](#)
- ["Exécution continue de l'écran Tableau de bord" à la page 122](#)
- ["Paramètres de statut du tableau de bord" à la page 122](#)
- ["Modification des statistiques d'activité affichées" à la page 124](#)
- ["Modification des seuils d'activité" à la page 125](#)
- ["Statut NDMP" à la page 125](#)
- ["Etats NDMP" à la page 127](#)

Statut sur le tableau de bord

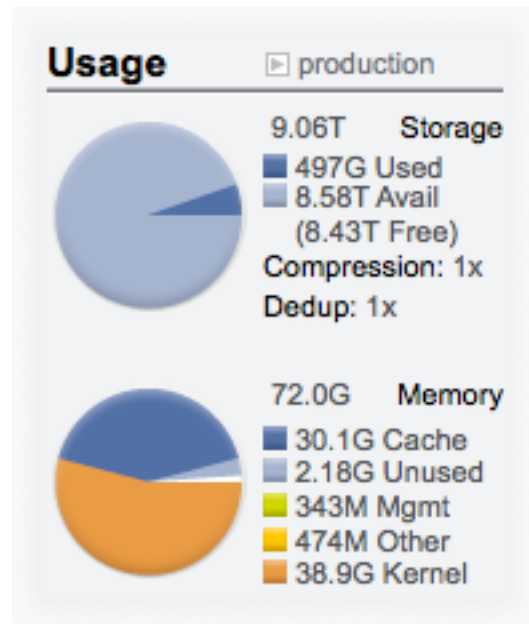


Le Tableau de bord récapitule l'état de l'appareil.

Le Tableau de bord de statut fournit des liens vers tous les écrans principaux de l'interface utilisateur de navigateur (BUI). Plus de 100 éléments visibles sur l'écran Dashboard constituent des liens vers des écrans de la BUI ; ces liens sont mis en évidence par un cadre ou du texte en surbrillance qui s'affiche lors du passage de la souris. La section suivante décrit en détail les différentes zones du Tableau de bord.

Zone Utilisation du tableau de bord

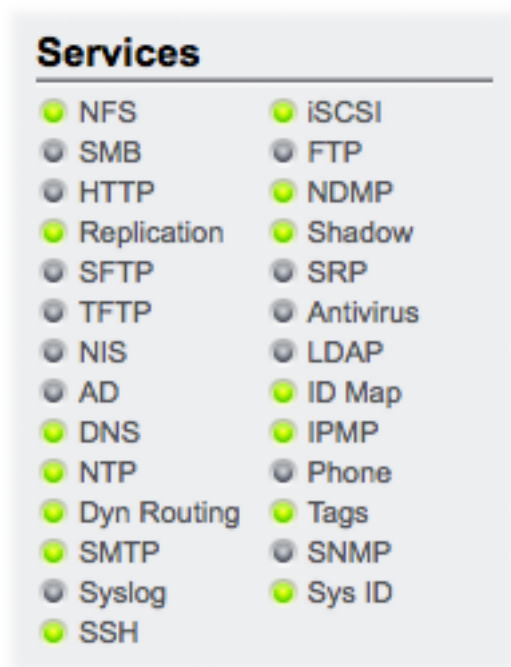
La zone Utilisation du Tableau de bord fournit un résumé de votre utilisation du pool de stockage et de la mémoire principale. Le nom du pool apparaît dans l'angle supérieur droit de la zone Utilisation. Si plusieurs pools sont configurés, utilisez la liste déroulante pour sélectionner le pool que vous souhaitez afficher.

FIGURE 1 Utilisation du tableau de bord de statut

La capacité totale du pool est affichée au sommet de cette zone. Le graphique à secteurs Stockage détaille l'espace utilisé, disponible et libre. Pour accéder à l'écran Partages du pool, cliquez sur le graphique à secteurs Stockage.

Services du tableau de bord

Cette zone du Tableau de bord affiche le statut des services de l'appareil avec une icône lumineuse pour afficher le statut de chaque service.

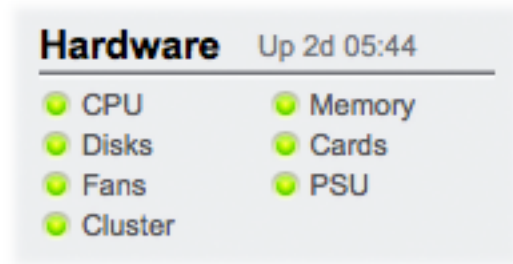
FIGURE 2 Tableau de bord des services

L'icône de la plupart des services s'affiche en vert, ce qui indique que le service correspondant est en ligne, ou en gris, ce qui indique que le service correspondant est désactivé. Reportez-vous à la section "[Interface utilisateur de navigateur \(BUI, Browser User Interface\)](#)" à la page 20 pour voir la liste de tous les états et couleurs d'icônes possibles.

Pour accéder à l'écran de configuration associé, cliquez sur le nom d'un service. L'écran Propriétés s'affiche et contient des champs configurables, des icônes de redémarrage, d'activation et de désactivation et un lien vers l'écran Journaux du service concerné.

Section Matériel du Tableau de bord

Cette zone du Tableau de bord affiche une présentation du matériel sur l'appareil.

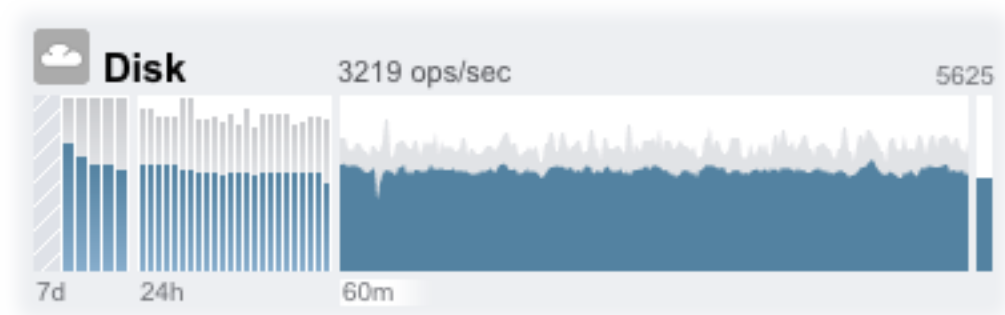
FIGURE 3 Tableau de bord du matériel

En cas de panne connue, l'icône de panne orange 🟡 s'affiche.

Pour accéder à l'écran de matériel et voir une présentation détaillée de l'état du matériel, cliquez sur le nom d'un composant matériel.

Activité du Tableau de bord

La zone d'activité du Tableau de bord affiche des graphiques de huit statistiques de performance par défaut. L'exemple illustré dans cette section montre le nombre d'opérations effectuées par le disque chaque seconde. La moyenne statistique est représentée en bleu et la valeur maximale en gris clair.

FIGURE 4 Tableau de bord d'activité du disque

Pour accéder à la feuille de travail d'analyse d'une activité, cliquez sur l'un des quatre graphiques (jour, heure, minute, seconde) de la statistique que vous souhaitez évaluer.

Pour afficher la moyenne de chaque graphique, placez le pointeur de la souris sur un graphique ; celle-ci s'affiche dans une infobulle. L'icône météorologique dans l'angle supérieur gauche donne une indication de l'activité en fonction de seuils que vous pouvez personnaliser pour chaque statistique dans l'écran "[Paramètres de statut du tableau de bord](#)" à la page 122.

TABLEAU 21 Récapitulatif des graphiques de statistiques

Récapitulatif des graphiques de statistiques	
Graphique sur 7 jours (7j)	Graphique à barres sur lequel chaque barre représente un jour.
Graphique sur 24 heures (24h)	Graphique à barres sur lequel chaque barre représente une heure.
Graphique sur 60 minutes (60m)	Graphique à courbes représentant l'activité sur une heure (également représenté en tant que première barre d'heure dans le graphique sur 24 heures).
Graphique sur 1 seconde	Graphique à courbes correspondant à une représentation de l'activité en temps réel.

La moyenne du tracé sélectionné est représentée sous forme numérique au-dessus du graphique. Pour modifier la moyenne affichée, sélectionnez la moyenne souhaitée, à savoir 7d, 24h ou 60m.

L'échelle verticale de tous les graphiques s'affiche en haut à droite, et tous les graphiques sont dimensionnés à cette hauteur. La hauteur est calculée à partir du graphique sélectionné (avec ajout d'une marge). La hauteur est redimensionnée en fonction de l'activité dans le graphique sélectionné, à l'exception des graphiques d'utilisation qui ont une hauteur fixe de 100 %.

Etant donné que la hauteur peut être redimensionnée, 60 minutes d'inactivité peuvent apparaître comme 60 minutes d'activité. Contrôlez toujours la hauteur des graphiques avant d'essayer de les interpréter.

L'interprétation de certaines statistiques peut s'avérer ardue ; vous pouvez par exemple ne pas savoir si une activité de 1000 opérations NFSv3 par seconde doit être considérée comme forte ou faible pour un appareil donné dans votre environnement. Dans ce cas, les tracés sur 24 heures et sur 7 jours peuvent vous être d'un grand secours, car ils vous permettent de comparer l'activité actuelle et les données historiques.

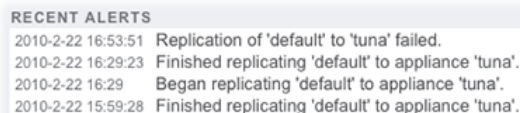
La hauteur d'un tracé est calculée à partir du tracé sélectionné. Le tracé sur 60 minutes est sélectionné par défaut. La hauteur correspond donc à l'activité maximale au cours de cet intervalle de 60 minutes (additionné d'une marge). Pour redimensionner tous les tracés en fonction du pic d'activité au cours des 7 derniers jours, sélectionnez 7d. Vous pouvez ainsi comparer facilement l'activité actuelle et l'activité du jour ou de la semaine qui vient de s'écouler.

Les icônes météorologiques ont pour but d'attirer votre attention sur un niveau d'activité particulièrement élevé ou faible. Cliquez sur l'icône météorologique pour accéder à la page de configuration du seuil météorologique. Il n'y a pas de bon ou de mauvais seuil ; la BUI fournit une gamme de niveaux évolutifs pour chaque statistique d'activité. Les statistiques sur lesquelles les icônes météorologiques sont basées donnent un aperçu *approximatif* des performances de l'appareil, qu'il vous appartient de personnaliser selon les principes suivants :

- Les niveaux de performance acceptables (latence) varient d'un environnement à l'autre et il n'y a donc pas de seuil universel qui conviendrait dans tous les cas de figure.
- Les statistiques du tableau de bord sont basées sur le nombre d'opérations et d'octets par seconde ; pour un suivi détaillé des performances du système, il est recommandé d'avoir recours à des feuilles de travail d'analyse.

Alertes récentes

FIGURE 5 Alertes récentes



```

RECENT ALERTS
2010-2-22 16:53:51 Replication of 'default' to 'tuna' failed.
2010-2-22 16:29:23 Finished replicating 'default' to appliance 'tuna'.
2010-2-22 16:29 Began replicating 'default' to appliance 'tuna'.
2010-2-22 15:59:28 Finished replicating 'default' to appliance 'tuna'.
  
```

Cette section affiche les quatre dernières alertes de l'appareil. Cliquez sur le rectangle pour accéder à l'écran Journaux et examiner en détail les alertes récentes.

Résumé de l'utilisation de la mémoire

La mémoire physique totale du système est affichée au sommet de cette zone. Un graphique à secteurs affichant l'utilisation de la mémoire par composant s'affiche sur la gauche. Pour accéder à la feuille de travail Analytics et visualiser l'utilisation dynamique de la mémoire en fonction du nom d'application, cliquez sur le graphique à secteurs Memory.

TABLEAU 22 Récapitulatif de l'utilisation du pool

Récapitulatif de l'utilisation du pool	
Utilisé	Espace utilisé par ce pool, y compris données et instantanés.
Dispo	Quantité d'espace disque physique disponible. L'espace disponible pour les données de fichiers (tel qu'indiqué

Récapitulatif de l'utilisation du pool	
	dans l'écran Partages) est inférieur à cette valeur, en raison de l'espace occupé par les métadonnées de systèmes de fichiers.
Libre	Quantité d'espace disponible au sein de la capacité LUN, moins l'espace inutilisé réservé aux projets et aux partages au sein d'un pool. Fournit de l'espace disque disponible lorsque l'espace disque est réservé en avance et/ou lors de la création de LUN.
Compression	Taux de compression actuel atteint par ce pool. Le taux affiche 1x si la compression est désactivée.
Suppr doublons	Taux de suppression des doublons actuel atteint par ce pool. Le taux affiche 1x si la suppression des doublons est désactivée.

TABLEAU 23 Récapitulatif de l'utilisation de la mémoire principale

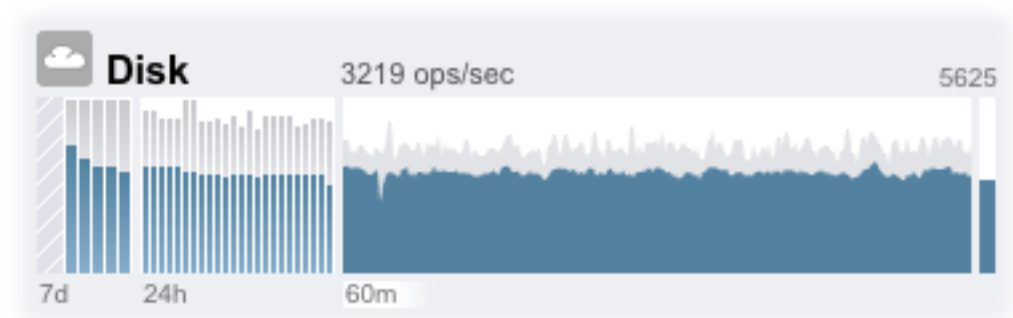
Récapitulatif de l'utilisation de la mémoire principale (RAM)	
Cache	Octets utilisés par le cache du système de fichiers pour améliorer les performances.
Inutilisé	Octets actuellement inutilisés. Après l'initialisation, cette valeur diminue à mesure que l'espace utilisé par le cache du système de fichiers augmente.
Gestion	Octets utilisés par le logiciel de gestion de l'appareil.
Autre	Octets utilisés par divers logiciels du système d'exploitation.
Noyau	Octets utilisés par le noyau du système d'exploitation.

Notez que les utilisateurs doivent disposer de l'autorisation `analytics/component create +read` pour visualiser l'utilisation de la mémoire. Sans cette autorisation, les détails de la mémoire ne s'affichent pas dans l'écran Tableau de bord.

Tableau de bord d'activité du disque

La zone d'activité du Tableau de bord affiche des graphiques de huit statistiques de performance par défaut. L'exemple illustré dans cette section montre le nombre d'opérations effectuées par le disque chaque seconde. La moyenne statistique est représentée en bleu et la valeur maximale en gris clair.

FIGURE 6 Tableau de bord d'activité du disque



Pour accéder à la feuille de travail d'analyse d'une activité, cliquez sur l'un des quatre graphiques (jour, heure, minute, seconde) de la statistique que vous souhaitez évaluer.

Pour afficher la moyenne de chaque graphique, placez le pointeur de la souris sur un graphique ; celle-ci s'affiche dans une infobulle. L'icône météorologique dans l'angle supérieur gauche donne une indication de l'activité en fonction de seuils pouvant être personnalisés pour chaque statistique dans l'écran Paramètres de statut .

TABLEAU 24 Récapitulatif des graphiques de statistiques

Récapitulatif des graphiques de statistiques	
Graphique sur 7 jours (7j)	Graphique à barres sur lequel chaque barre représente un jour.
Graphique sur 24 heures (24h)	Graphique à barres sur lequel chaque barre représente une heure.
Graphique sur 60 minutes (60m)	Graphique à courbes représentant l'activité sur une heure (également représenté en tant que première barre d'heure dans le graphique sur 24 heures).
Graphique sur 1 seconde	Graphique à courbes correspondant à une représentation de l'activité en temps réel.

La moyenne du tracé sélectionné est représentée sous forme numérique au-dessus du graphique. Pour modifier la moyenne affichée, sélectionnez la moyenne souhaitée, à savoir 7d, 24h ou 60m.

L'échelle verticale de tous les graphiques s'affiche en haut à droite, et tous les graphiques sont dimensionnés à cette hauteur. La hauteur est calculée à partir du graphique sélectionné (avec ajout d'une marge). La hauteur est redimensionnée en fonction de l'activité dans le graphique sélectionné, à l'exception des graphiques d'utilisation qui ont une hauteur fixe de 100 %.

Etant donné que la hauteur peut être redimensionnée, 60 minutes d'inactivité peuvent apparaître comme 60 minutes d'activité. Contrôlez toujours la hauteur des graphiques avant d'essayer de les interpréter.

L'interprétation de certaines statistiques peut s'avérer ardue ; vous pouvez par exemple ne pas savoir si une activité de 1000 opérations NFSv3 par seconde doit être considérée comme forte ou faible pour un appareil donné dans votre environnement. Dans ce cas, les tracés sur 24 heures et sur 7 jours peuvent vous être d'un grand secours, car ils vous permettent de comparer l'activité actuelle et les données historiques.

La hauteur d'un tracé est calculée à partir du tracé sélectionné. Le tracé sur 60 minutes est sélectionné par défaut. La hauteur correspond donc à l'activité maximale au cours de cet intervalle de 60 minutes (additionné d'une marge). Pour redimensionner tous les tracés en fonction du pic d'activité au cours des 7 derniers jours, sélectionnez 7d. Vous pouvez ainsi comparer facilement l'activité actuelle et l'activité du jour ou de la semaine qui vient de s'écouler.

Les icônes météorologiques ont pour but d'attirer votre attention sur un niveau d'activité particulièrement élevé ou faible. Cliquez sur l'icône météorologique pour accéder à la page de configuration du seuil météorologique. Il n'y a pas de bon ou de mauvais seuil ; la BUI fournit une gamme de niveaux évolutifs pour chaque statistique d'activité. Les statistiques sur lesquelles les icônes météorologiques sont basées donnent un aperçu *approximatif* des performances de l'appareil, qu'il vous appartient de personnaliser selon les principes suivants :

- Les niveaux de performance acceptables (latence) varient d'un environnement à l'autre et il n'y a donc pas de seuil universel qui conviendrait dans tous les cas de figure.
- Les statistiques du tableau de bord sont basées sur le nombre d'opérations et d'octets par seconde ; pour un suivi détaillé des performances du système, il est recommandé d'avoir recours à des feuilles de travail d'analyse.

CLI du tableau de bord

Vous pouvez accéder à une version textuelle de l'écran Statut > Tableau de bord à partir de la CLI en saisissant la commande `status dashboard` :

```
cuttlefish:> status dashboard
Storage:
  pool_0:
    Used      497G bytes
    Avail     8.58T bytes
    Free      8.43T bytes
    State      online
    Compression 1x

Memory:
  Cache      30.1G bytes
  Unused     2.18G bytes
  Mgmt       343M bytes
```



```

Other      474M bytes
Kernel    38.9G bytes

Services:
ad          disabled      smb          disabled
dns         online         ftp          disabled
http        online         identity     online
idmap       online         ipmp         online
iscsi       online         ldap         disabled
ndmp        online         nfs          online
nis         online         ntp          online
routing     online         scrk         maintenance
snmp        online         ssh          online
tags        online         vscan        online

Hardware:
CPU         online         Cards        online
Disks       faulted      Fans         online
Memory      online         PSU          online

Activity:
CPU         1 %util       Sunny
Disk        32 ops/sec  Sunny
iSCSI       0 ops/sec    Sunny
NDMP        0 bytes/sec Sunny
NFSv3       0 ops/sec    Sunny
NFSv4       0 ops/sec    Sunny
Network     13K bytes/sec Sunny
SMB         0 ops/sec    Sunny

```

Recent Alerts:

```
2013-6-15 07:46: A cluster interconnect link has been restored.
```

Les descriptions figurant dans la section précédente s'appliquent, avec les différences suivantes :

- Bien que nous ayons pensé à utiliser aalib, les tracés représentant l'activité ne sont pas représentés sous forme de texte.
- Dans la CLI, la section sur l'utilisation du stockage affiche des informations sur tous les pools disponibles, alors que l'espace disponible dans la BUI ne permet que d'afficher le récapitulatif d'un seul pool.

Des vues distinctes sont possibles, par exemple `status activity show` :

```

caji:> status activity show
Activity:
CPU         10 %util       Sunny
Disk        478 ops/sec    Partly Cloudy
iSCSI       0 ops/sec    Sunny
NDMP        0 bytes/sec    Sunny
NFSv3       681 ops/sec    Partly Cloudy
NFSv4       0 ops/sec    Sunny
Network     22.8M bytes/sec    Partly Cloudy
SMB         0 ops/sec    Sunny

```

caji:>

▼ Exécution continue de l'écran Tableau de bord

Des problèmes de mémoire du navigateur risquent de survenir lorsque l'écran Tableau de bord est ouvert en permanence dans un navigateur (24h sur 24 et 7 jours sur 7). La taille du navigateur augmente en raison de fuites de mémoire. Les navigateurs gèrent assez efficacement la mémoire lors de la navigation sur plusieurs sites Web (ainsi que l'ouverture et la fermeture d'onglets). Le problème est que l'écran Tableau de bord est laissé ouvert et en pleine exécution, ce qui ouvre et rouvre les images d'activité, et réduit ainsi les performances de rendu d'image.

Si vous constatez ce problème avec Firefox, désactivez la mémoire cache comme suit :

1. **Ouvrez about:config**
2. **Effectuez un filtrage sur ""memory""**
3. **Paramétrez browser.cache.memory.enable sur false.**

Paramètres de statut du tableau de bord

L'écran Statut > Paramètres permet de personnaliser le tableau de bord de statut, notamment les statistiques affichées et les seuils d'activité représentés par les icônes météorologiques.

The screenshot shows the 'Configure Dashboard' window with the 'Layout' tab selected. On the left, there is an 'About' section with explanatory text. The main area contains a 2x4 grid of dropdown menus for selecting activity metrics: CPU, Network, Disk, iSCSI, NFSv3, NFSv4, SMB2, and ARC Ratio. At the top right, there are 'Layout' and 'Thresholds' tabs, and 'REVERT' and 'APPLY' buttons.

Choisissez l'onglet Disposition pour sélectionner les graphiques s'affichant dans la zone Activité dans tableau de bord en suivant les indications du tableau suivant.

TABLEAU 25 Paramètres de présentation du statut

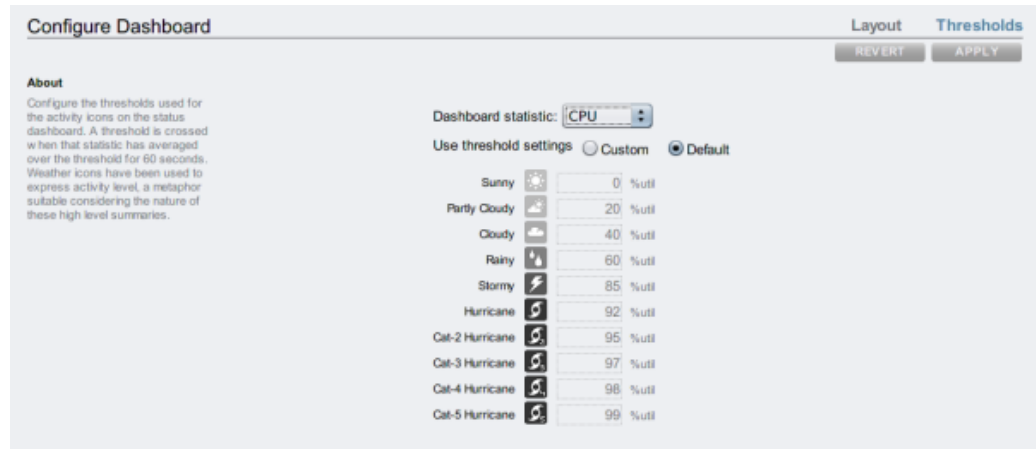
Nom	Unités	Description
<empty>	-	Aucun graphique n'est affiché à cet endroit.

Nom	Unités	Description
CPU	utilisation	Nombre moyen de cycles pendant lesquels les CPU de l'appareil sont occupées. Les cycles de CPU comprennent notamment les cycles d'attente mémoire.
Ratio ARC	utilisation	Pourcentage moyen de succès/d'échecs ARC. Une chute du pourcentage de succès indique un problème potentiel de performances.
HTTP	opérations/sec	Nombre moyen d'opérations HTTP.
Disque	opérations/sec	Nombre moyen d'opérations vers les périphériques de stockage physiques.
iSCSI	opérations/sec	Nombre moyen d'opérations iSCSI.
FC	opérations/sec	Nombre moyen d'opérations Fibre Channel.
NDMP	octets/sec	Nombre moyen d'octets réseau NDMP.
NFSv2	opérations/sec	Nombre moyen d'opérations NFSv2.
NFSv3	opérations/sec	Nombre moyen d'opérations NFSv3.
NFSv4	opérations/sec	Nombre moyen d'opérations NFSv4.
Réseau	octets/sec	Nombre moyen d'octets par seconde dans l'ensemble des interfaces réseau physiques.
SMB	opérations/sec	Nombre moyen d'opérations SMB.
SMB2	opérations/sec	Nombre moyen d'opérations SMB2.
FTP	octets/sec	Nombre moyen d'octets FTP.
SFTP	octets/sec	Nombre moyen d'octets SFTP.

Remarque : pour réaliser la réduction de trafic réseau requise pour actualiser l'écran Tableau de bord, il est recommandé de définir certains graphiques d'activité comme "<empty>".

L'écran Seuils permet de configurer les icônes météorologiques de l'activité dans tableau de bord . Les valeurs par défaut d'origine sont conçues pour des charges de travail élevées et ne sont pas forcément adaptées à votre environnement.

FIGURE 7 Paramètres d'activité dans tableau de bord



L'icône météorologique qui s'affiche dans l'écran Tableau de bord indique la valeur de seuil de laquelle l'activité actuelle est la plus proche, l'activité actuelle correspondant à l'activité moyenne sur les 60 dernières secondes. Par exemple, si l'utilisation de la CPU s'élevait à 41 %, l'icône météorologique Nuageux s'afficherait, car le seuil correspondant est fixé à 40 %, qui est la valeur de seuil la plus proche de l'activité actuelle. Sélectionnez le bouton radio Personnalisés pour configurer les seuils et assurez-vous de les configurer dans l'ordre dans lequel ils apparaissent à l'écran.

Les valeurs de Tableau de bord ne peuvent pas actuellement être configurées depuis la CLI. Ce sont les paramètres configurés pour Tableau de bord dans la BUI qui s'appliquent à la représentation de Tableau de bord dans la CLI.

▼ Modification des statistiques d'activité affichées

1. Accédez à l'écran Statut > Paramètres > Disposition.
2. Sélectionnez les statistiques que vous souhaitez afficher dans l'écran Tableau de bord dans les menus déroulants.

3. Cliquez sur le bouton Appliquer pour enregistrer vos choix.

▼ Modification des seuils d'activité

1. Accédez à l'écran Statut > Paramètres > Seuils.
2. Sélectionnez la statistique que vous souhaitez configurer dans le menu déroulant.
3. Cliquez sur le bouton radio Personnalisées.
4. Personnalisez les valeurs de la liste dans l'ordre dans lequel elles apparaissent. Certaines statistiques comportent un menu déroulant Unités, ce qui permet de sélectionner Kilo/Mega/Giga.
5. Cliquez sur le bouton Appliquer pour enregistrer votre configuration.

Statut NDMP

Lorsque le service NDMP est configuré et actif, la page Statut=>NDMP affiche les périphériques NDMP ainsi que l'activité récente des clients. Un indicateur vert s'affiche lorsque le périphérique est en ligne. Lorsqu'il est hors ligne, un indicateur gris s'affiche.

Cliquez sur les en-têtes des colonnes pour avoir recours à la liste des périphériques NDMP. Double cliquez sur un périphérique pour afficher les informations le concernant.

Le statut NDMP n'est pas disponible depuis la CLI.

FIGURE 8 BUI, statut NDMP

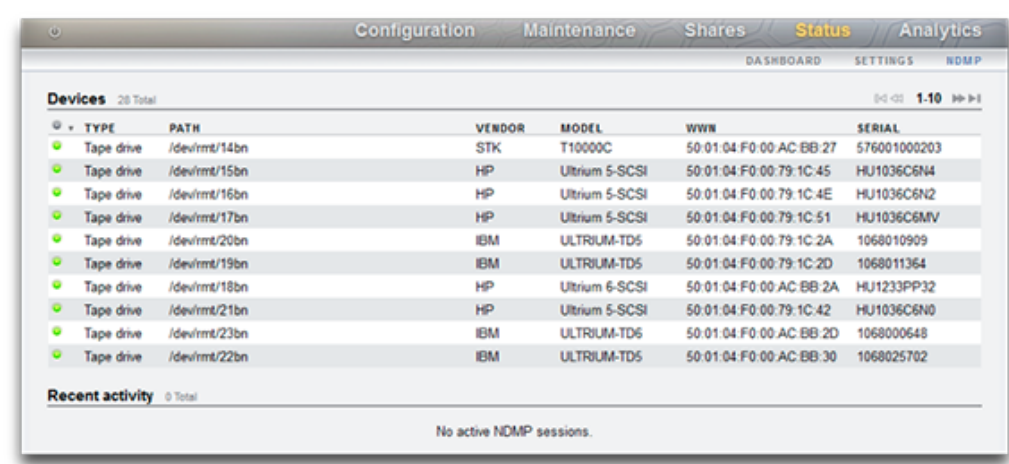


TABLEAU 26 Statut NDMP : périphériques

Champ	Description	Exemples
Type	Type de périphérique NDMP	Robot, Lecteur de bande
Chemin	Chemin d'accès du périphérique NDMP	/dev/rmt/14bn
Fournisseur	Nom du fournisseur du périphérique	STK
Modèle	Nom du modèle du périphérique	T1000C
WWN	Sigle de World Wide Name, nom universel.	50:01:04:F0:00:AC:BB:27
Numéro de série	Numéro de série de périphérique	576001000203

TABLEAU 27 Statut NDMP : activité récente

Champ	Description	Exemples
ID	ID de sauvegarde NDMP	49
Actif	Sauvegarde actuellement active	Non
Client distant	Adresse et port du client NDMP	192.168.1.219:4760
Authentifié	Indique si le client a terminé l'authentification	Oui, Non
Etat de données	Voir l'état de données	Actif, Inactif, ...
Etat du moteur	Voir l'état du moteur	Actif, Inactif, ...
Opération en cours	Opération NDMP actuelle	Sauvegarde, Restauration, Aucune

Champ	Description	Exemples
Progression	Barre de progression pour la sauvegarde concernée	

Etats NDMP

L'état des données NDMP indique l'état de l'opération de sauvegarde ou de restauration. Valeurs possibles :

- **Actif** : les données sont sauvegardées ou restaurées.
- **Inactif** : la sauvegarde ou la restauration n'a pas encore débuté ou est déjà terminée.
- **Connecté** : la connexion a été établie mais la sauvegarde ou la restauration n'a pas encore débuté.
- **Arrêté** : la sauvegarde ou la restauration est terminée, a échoué ou a été annulée.
- **A l'écoute** : l'opération attend de recevoir une connexion distante.

L'état du moteur NDMP indique l'état du sous-système du périphérique NDMP. Exemples concernant les périphériques à bande :

- **Actif** : les données sont en cours de lecture ou d'écriture sur la bande.
- **Inactif** : l'opération de la bande n'a pas encore débuté ou est déjà terminée.
- **Mis en pause** : la bande est terminée ou attend d'être changée.
- **Arrêté** : l'opération d'écriture/lecture est terminée, a échoué ou a été annulée.
- **A l'écoute** : l'opération attend de recevoir une connexion distante.

Configuration du réseau de stockage SAN

La page de configuration SAN vous permet de connecter votre appareil à votre réseau de stockage SAN. Un SAN est constitué de trois composants de base :

- Un client qui accède à l'espace de stockage sur le réseau
- Un appareil de stockage qui fournit l'espace de stockage sur le réseau
- Un réseau reliant le client à l'espace de stockage

Pour configurer le réseau de stockage SAN, reportez-vous aux sections suivantes :

- [Configuration des modes de port FC \(BUI\)](#)
- [Détection de ports FC \(BUI\)](#)
- [Création de groupes d'initiateurs FC \(BUI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(BUI\)](#)
- [Changement de mode de port FC \(CLI\)](#)
- [Détection de ports FC \(CLI\)](#)
- [Création de groupes d'initiateurs FC \(CLI\)](#)

- Association d'un LUN à un groupe d'initiateurs FC (CLI)
- Scripts de création d'alias pour les initiateurs et groupes d'initiateurs (CLI)
- Configuration des initiateurs SAN iSCSI
- Création d'une feuille de travail Analyse (BUI)
- Ajout d'une cible iSCSI possédant un IQN généré de manière automatique (CLI)
- Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné (CLI)
- Ajout d'un initiateur iSCSI utilisant l'authentification CHAP (CLI)
- Ajout d'un groupe de cibles iSCSI (CLI)
- Ajout d'un groupe d'initiateurs iSCSI (CLI)
- Configuration des cibles SRP (BUI)
- Configuration des cibles SRP (CLI)

Pour en savoir plus sur SAN, consultez les sections suivantes :

- Présentation de SAN
- Configuration Fibre Channel SAN
- Configuration SAN iSCSI
- Configuration de la cible SAN iSER
- Configuration SAN SRP
- Terminologie SAN

▼ Configuration des modes de port FC (BUI)

1. Pour utiliser les ports FC, définissez-les sur le mode Cible dans l'écran Configuration > SAN de la BUI, à l'aide du menu déroulant représenté dans l'image suivante. Vous devez disposer des autorisations `root` pour effectuer cette action. Notez que dans une configuration de cluster, vous définissez des ports sur le mode Cible sur chaque serveur séparément.



2. Après avoir défini les ports souhaités sur Cible, cliquez sur le bouton Appliquer. Un message de confirmation annonçant que l'appareil va se réinitialiser immédiatement s'affiche. Confirmez la réinitialisation.
3. Lorsque l'appareil s'initialise, les cibles FC actives sont représentées avec l'icône  et l'icône de déplacement  s'affiche lorsque vous placez le pointeur de la souris au-dessus de ces icônes.

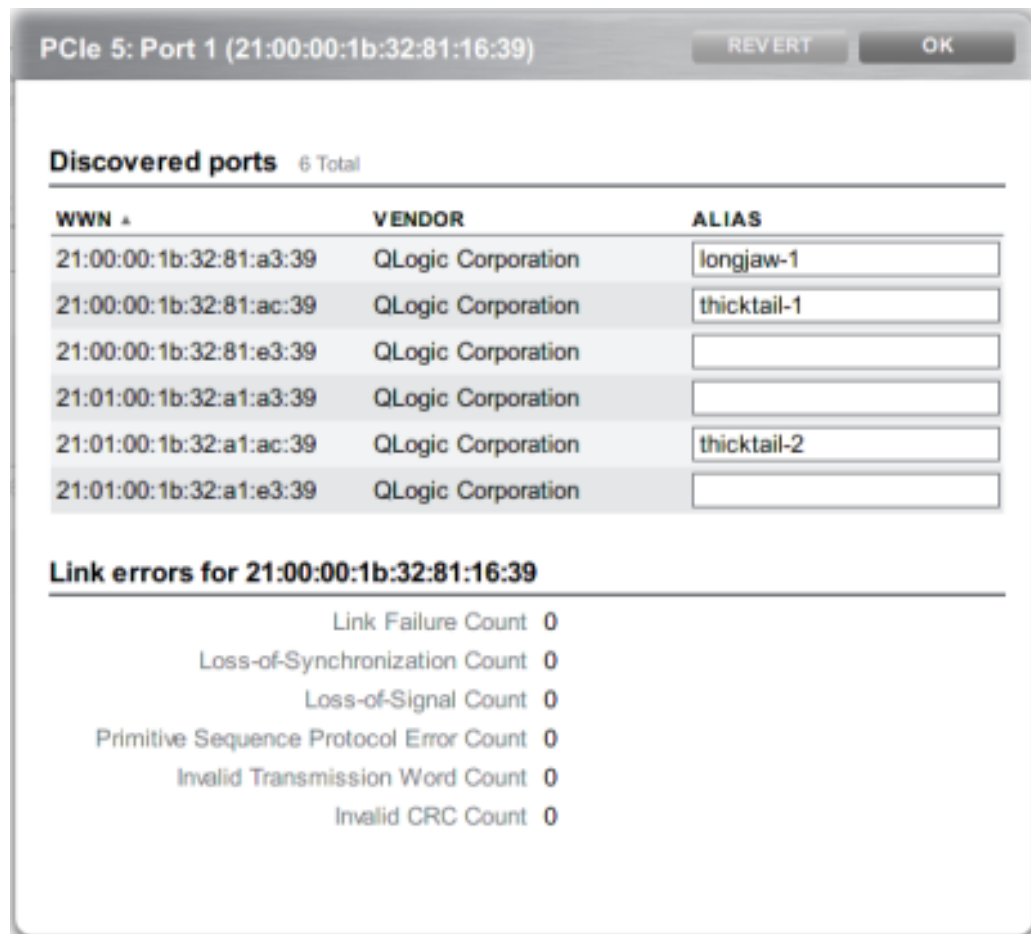
Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Détection de ports FC (BUI)

1. Cliquez sur l'icône d'informations  pour afficher la boîte de dialogue Ports détectés dans laquelle vous pouvez résoudre les erreurs de liaison. Dans la boîte de dialogue Ports détectés, cliquez sur un nom universel de la liste pour afficher les erreurs de liaisons associées.

FIGURE 9 Ports FC détectés



2. Dans la boîte de dialogue Ports détectés, cliquez sur un nom universel de la liste pour afficher les erreurs de liaisons associées.

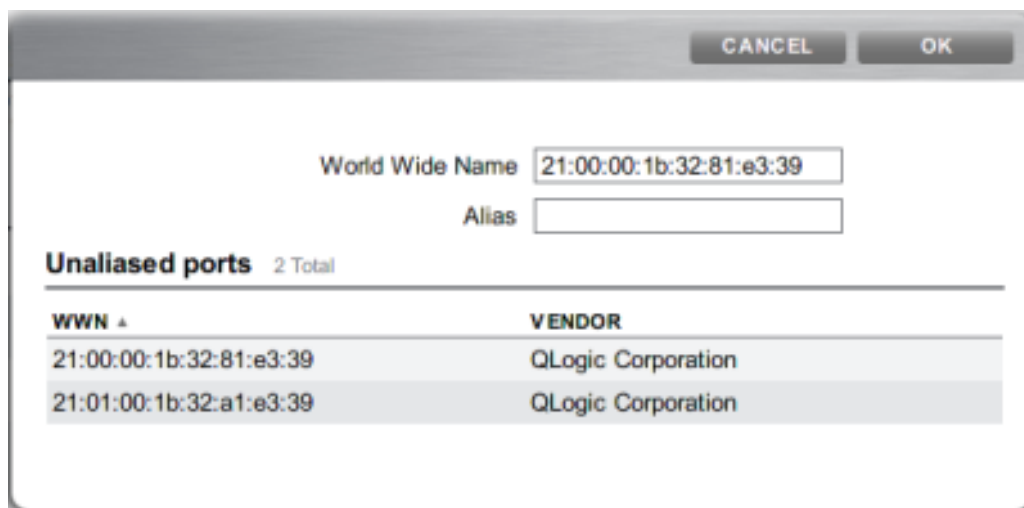
Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)

- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Création de groupes d'initiateurs FC (BUI)

1. Créez et gérez des groupes d'initiateurs dans l'écran Initiateurs. Cliquez sur l'icône d'ajout  pour afficher les ports sans alias. Cliquez sur un nom universel de la liste pour ajouter un alias explicite dans le champ Alias.



The screenshot shows a window titled 'Initiateurs' with 'CANCEL' and 'OK' buttons at the top right. Inside, there are two input fields: 'World Wide Name' containing '21:00:00:1b:32:81:e3:39' and 'Alias' which is empty. Below these fields, a section titled 'Unaliased ports' with a subtitle '2 Total' contains a table with two columns: 'WWN' and 'VENDOR'.

WWN	VENDOR
21:00:00:1b:32:81:e3:39	QLogic Corporation
21:01:00:1b:32:a1:e3:39	QLogic Corporation

2. Sur la page Initiateurs, faites glisser les initiateurs vers la liste Groupes d'initiateurs FC pour les ajouter à des groupes existants ou créer de nouveaux groupes.

FIGURE 10 Liste des groupes d'initiateurs FC



3. Cliquez sur le bouton Appliquer pour valider le nouveau groupe d'initiateurs. Vous pouvez ensuite créer un LUN disposant d'un accès exclusif au groupe d'initiateurs client.

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Association d'un LUN à un groupe d'initiateurs FC (BUI)

1. Pour créer le LUN, reportez le groupe d'initiateurs et cliquez sur l'icône d'ajout de LUN . La boîte de dialogue Créer un LUN s'affiche, et le groupe d'initiateurs associé y est sélectionné.

FIGURE 11 Association d'un LUN à un groupe d'initiateurs FC

The screenshot shows a 'Create LUN' dialog box with the following fields and options:

- Project:** A dropdown menu showing 'default'.
- Name:** An empty text input field.
- Volume size:** A text input field containing '0' and a unit dropdown menu showing 'G'.
- Thin provisioned:** An unchecked checkbox.
- Volume block size:** A dropdown menu showing '8k'.
- Online:** A checked checkbox.
- Target group:** A dropdown menu showing 'All targets'.
- Initiator group(s):** A dropdown menu showing 'All initiators', 'initiators-0', and 'initiators-1'.
- LU number:** Two radio buttons: '0' (unchecked) and 'Auto-assign' (checked).

At the top right of the dialog are 'CANCEL' and 'APPLY' buttons.

2. Définissez le nom et la taille et cliquez sur Appliquer pour ajouter le LUN au pool de stockage.

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Changement de mode de port FC (CLI)

- Pour changer de mode de port FC, utilisez les commandes CLI suivantes :

```
dory:configuration san fc targets> set targets="wwn.2101001B32A11639"
      targets = wwn.2101001B32A11639 (uncommitted)
dory:configuration san fc targets> commit
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Détection de ports FC (CLI)

- Pour procéder à la détection de ports FC, utilisez les commandes CLI suivantes :

```
dory:configuration san fc targets> show
Properties:
      targets = wwn.2100001B32811639,wwn.2101001B32A12239

Targets:
NAME      MODE      WWN              PORT              SPEED
target-000 target    wwn.2100001B32811639  PCIe 5: Port 1    4 Gbit/s
target-001 initiator wwn.2101001B32A11639  PCIe 5: Port 2    0 Gbit/s
target-002 initiator wwn.2100001B32812239  PCIe 2: Port 1    0 Gbit/s
target-003 target    wwn.2101001B32A12239  PCIe 2: Port 2    0 Gbit/s
dory:configuration san fc targets> select target-000
dory:configuration san fc targets target-000> show
Properties:
      wwn = wwn.2100001B32811639
      port = PCIe 5: Port 1
      mode = target
      speed = 4 Gbit/s
      discovered_ports = 6
      link_failure_count = 0
      loss_of_sync_count = 0
      loss_of_signal_count = 0
      protocol_error_count = 0
      invalid_tx_word_count = 0
      invalid_crc_count = 0

Ports:
PORT      WWN              ALIAS              MANUFACTURER
port-000  wwn.2100001B3281A339  longjaw-1          QLogic Corporation
```

port-001	wwn.2101001B32A1A339	longjaw-2	QLogic Corporation
port-002	wwn.2100001B3281AC39	thicktail-1	QLogic Corporation
port-003	wwn.2101001B32A1AC39	thicktail-2	QLogic Corporation
port-004	wwn.2100001B3281E339	<none>	QLogic Corporation
port-005	wwn.2101001B32A1E339	<none>	QLogic Corporation

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Création de groupes d'initiateurs FC (CLI)

- Pour créer des groupes d'initiateurs FC, utilisez les commandes CLI suivantes :

```
dory:configuration san fc initiators> create
dory:configuration san fc initiators (uncommitted)> set name=lefteye
dory:configuration san fc initiators (uncommitted)>
    set initiators=wwn.2101001B32A1AC39,wwn.2100001B3281AC39
dory:configuration san fc initiators (uncommitted)> commit
dory:configuration san fc initiators> list
GROUP      NAME
group-001  lefteye
          |
          +--> INITIATORS
                wwn.2101001B32A1AC39
                wwn.2100001B3281AC39
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Association d'un LUN à un groupe d'initiateurs FC (CLI)

L'exemple suivant illustre la création d'un LUN appelé `lefty` et son association au groupe d'initiateurs `fera`.

- **Pour associer un LUN à un groupe d'initiateurs FC, utilisez les commandes CLI suivantes :**

```
dory:shares default> lun lefty
dory:shares default/lefty (uncommitted)> set volsize=10
                                volsize = 10 (uncommitted)
dory:shares default/lefty (uncommitted)> set initiatorgroup=fera
                                initiatorgroup = default (uncommitted)
dory:shares default/lefty (uncommitted)> commit
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Scripts de création d'alias pour les initiateurs et groupes d'initiateurs (CLI)

Reportez-vous aux sections [Utilisation de la CLI](#) et [Commandes simples d'écriture de scripts et de traitement par lots](#) pour plus d'informations sur la modification et l'utilisation des exemples de scripts suivants.

- **Pour créer des alias par script pour des initiateurs et groupes d'initiateurs, utilisez les commandes CLI suivantes :**

```
script
/*
 * This script creates both aliases for initiators and initiator
 * groups, as specified by the below data structure. In this
 * particular example, there are five initiator groups, each of
 * which is associated with a single host (thicktail, longjaw, etc.),
 * and each initiator group consists of two initiators, each of which
 * is associated with one of the two ports on the FC HBA. (Note that
```



```

* there is nothing in the code that uses this data structure that
* assumes the number of initiators per group.)
*/
groups = {
  thicktail: {
    'thicktail-1': 'wnn.2100001b3281ac39',
    'thicktail-2': 'wnn.2101001b32a1ac39'
  },
  longjaw: {
    'longjaw-1': 'wnn.2100001b3281a339',
    'longjaw-2': 'wnn.2101001b32a1a339'
  },
  tecopa: {
    'tecopa-1': 'wnn.2100001b3281e339',
    'tecopa-2': 'wnn.2101001b32a1e339'
  },
  spinedace: {
    'spinedace-1': 'wnn.2100001b3281df39',
    'spinedace-2': 'wnn.2101001b32a1df39'
  },
  fera: {
    'fera-1': 'wnn.2100001b32817939',
    'fera-2': 'wnn.2101001b32a17939'
  }
};
for (group in groups) {
  initiators = [];
  for (initiator in groups[group]) {
    printf('Adding %s for %s ... ',
      groups[group][initiator], initiator);
    try {
      run('select alias=' + initiator);
      printf('(already exists)\n');
      run('cd ..');
    } catch (err) {
      if (err.code != EAKSH_ENTITY_BADSELECT)
        throw err;
      run('create');
      set('alias', initiator);
      set('initiator', groups[group][initiator]);
      run('commit');
      printf('done\n');
    }
    run('select alias=' + initiator);
    initiators.push(get('initiator'));
    run('cd ..');
  }
  printf('Creating group for %s ... ', group);
  run('groups');
  try {
    run('select name=' + group);
    printf('(already exists)\n');
    run('cd ..');
  } catch (err) {

```

```
        if (err.code != EAKSH_ENTITY_BADSELECT)
            throw err;
        run('create');
        set('name', group);
        run('set initiators=' + initiators);
        run('commit');
        printf('done\n');
    }
    run('cd ..');
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Création d'une feuille de travail Analyse (BUI)

Pour créer une feuille de travail d'analyse afin d'observer les opérations par initiateur, effectuez les opérations suivantes :

1. **Accédez à l'écran Analyse.**
2. **Cliquez sur l'icône d'ajout  pour Ajouter une statistique. Un menu répertoriant toutes les statistiques s'affiche.**
3. **Sélectionnez Opérations iSCSI > Ventilé par initiateur dans la section Protocoles du menu. Un graphique représentant les opérations actuelles par initiateur s'affiche.**
4. **Pour observer des informations d'analyse plus détaillées, sélectionnez l'initiateur dans le champ situé sur la gauche du graphique et cliquez sur l'icône . Un menu se rapportant à des analyses détaillées s'affiche.**

Rubriques connexes

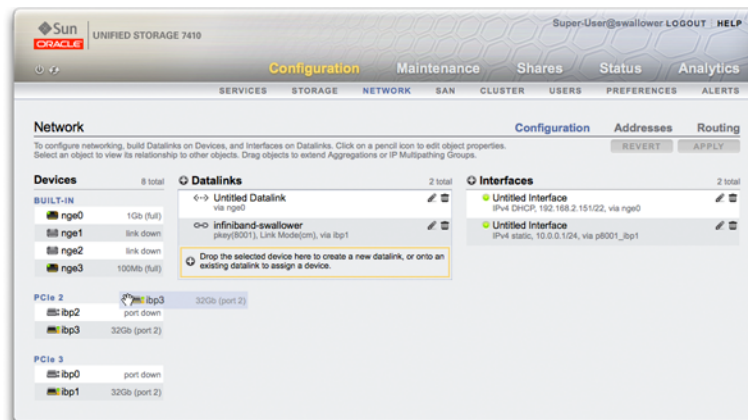
- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)

- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Configuration des cibles SAN iSER

Dans la BUI, les cibles iSER sont gérées en tant que cibles iSCSI dans l'écran Configuration > SAN.

1. Pour configurer des interfaces ibd(x), sélectionnez l'interface ibd(x) (ou ipmp), puis faites-la glisser dans la liste Liaisons de données afin de créer la liaison de données dans l'écran Configuration > Réseau.
2. Faites glisser la liaison de données dans la liste Interfaces pour créer une nouvelle interface.



3. Pour créer une cible iSER, sur la page Configuration > SAN, cliquez sur le lien Cibles iSCSI.
4. Pour ajouter une nouvelle cible iSER avec un alias, cliquez sur l'icône d'ajout .

5. Pour créer un groupe de cibles, faites glisser la cible que vous venez de créer dans la liste Groupes de cibles iSCSI.

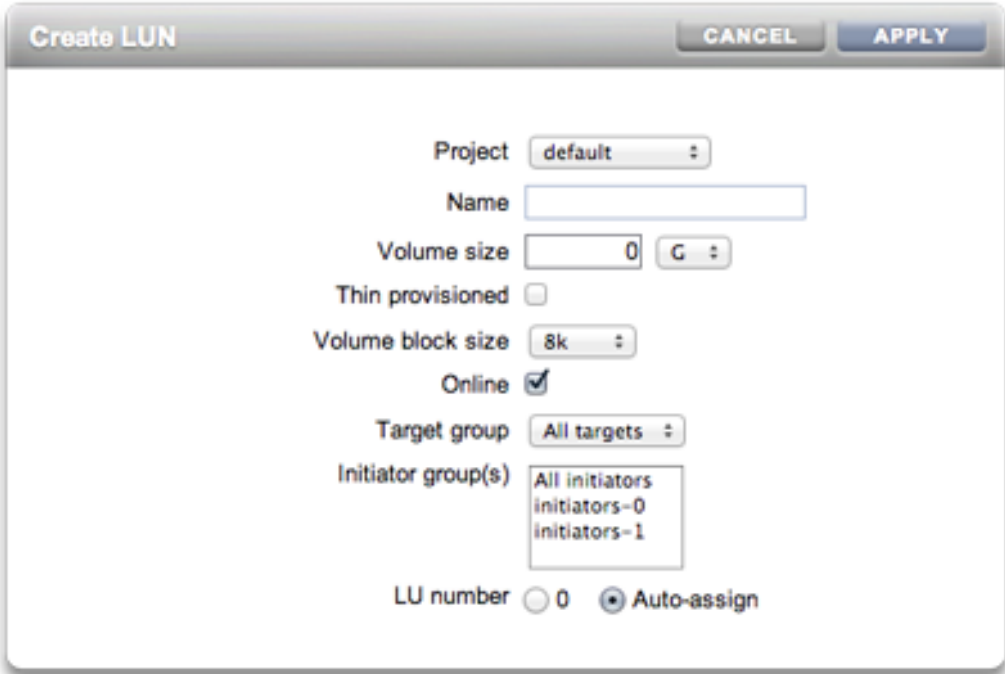


6. Pour créer un initiateur, cliquez sur le lien Initiateur puis sur Initiateurs iSCSI.
7. Pour ajouter un initiateur, cliquez sur l'icône d'ajout .
8. Saisissez l'IQN de l'initiateur, un alias, puis cliquez sur OK. La création d'un groupe d'initiateurs est facultative, mais le LUN associé à la cible sera disponible pour tous les initiateurs si vous ne créez pas de groupes.
9. Pour créer un groupe, faites glisser l'initiateur dans la liste iSCSI Initiator Groups.



10. Pour créer un LUN, sur la page Partages, cliquez sur LUN.

11. Cliquez sur l'icône d'ajout  et associez le nouveau LUN aux groupes de cibles ou d'initiateurs que vous avez créés à l'aide du menu Groupe de cibles ou Groupe d'initiateurs.



The image shows a 'Create LUN' dialog box with the following fields and options:

- Project:** default
- Name:** (empty text field)
- Volume size:** 0 GB
- Thin provisioned:** ☐
- Volume block size:** 8k
- Online:** ☒
- Target group:** All targets
- Initiator group(s):** All initiators, initiators-0, initiators-1
- LU number:** ☐ 0 ☒ Auto-assign

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Ajout d'une cible iSCSI possédant un IQN généré de manière automatique (CLI)

- Pour ajouter une cible iSCSI possédant un IQN généré de manière automatique, utilisez les commandes CLI suivantes :

```
ahi:configuration san iscsi targets> create
ahi:configuration san iscsi targets target (uncommitted)> set alias="Target 0"
ahi:configuration san iscsi targets target (uncommitted)> set auth=none
ahi:configuration san iscsi targets target (uncommitted)> set interfaces=igb1
ahi:configuration san iscsi targets target (uncommitted)> commit
ahi:configuration san iscsi targets> list
TARGET      ALIAS
target-000 Target 0
      |
      +--> IQN
            iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné (CLI)

- Pour ajouter une cible iSCSI avec IQN spécifique et authentification RADIUS, utilisez les commandes CLI suivantes :

```
ahi:configuration san iscsi targets> create
ahi:configuration san iscsi targets target (uncommitted)> set alias="Target 1"
ahi:configuration san iscsi targets target (uncommitted)>
      set iqn=iqn.2001-02.com.acme:12345
ahi:configuration san iscsi targets target (uncommitted)> set auth=radius
ahi:configuration san iscsi targets target (uncommitted)> set interfaces=igb1
ahi:configuration san iscsi targets target (uncommitted)> commit
ahi:configuration san iscsi targets> list
TARGET      ALIAS
target-000 Target 0
      |
      +--> IQN
            iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
target-001 Target 1
      |
      +--> IQN
            iqn.2001-02.com.acme:12345
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Ajout d'un initiateur iSCSI utilisant l'authentification CHAP (CLI)

- Pour ajouter un initiateur iSCSI utilisant l'authentification CHAP, utilisez les commandes CLI suivantes :

```
ahi:configuration san iscsi initiators> create
ahi:configuration san iscsi initiators initiator (uncommitted)>
    set initiator=iqn.2001-02.com.acme:initiator12345
ahi:configuration san iscsi initiators initiator (uncommitted)> set alias="Init 0"
ahi:configuration san iscsi initiators initiator (uncommitted)>
    set chapuser=thisismychapuser
ahi:configuration san iscsi initiators initiator (uncommitted)>
    set chapsecret=123456789012abc
ahi:configuration san iscsi initiators initiator (uncommitted)> commit
ahi:configuration san iscsi initiators> list
NAME          ALIAS
initiator-000 Init 0
|
+--> INITIATOR
      iqn.2001-02.com.acme:initiator12345
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Ajout d'un groupe de cibles iSCSI (CLI)

- Pour ajouter un groupe de cibles iSCSI, utilisez les commandes CLI suivantes :

```
ahi:configuration san iscsi targets groups> create
ahi:configuration san iscsi targets group (uncommitted)> set name=tg0
ahi:configuration san iscsi targets group (uncommitted)>
  set targets=iqn.2001-02.com.acme:12345,
    iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
ahi:configuration san iscsi targets group (uncommitted)> commit
ahi:configuration san iscsi targets groups> list
GROUP      NAME
group-000  tg0
|
+--> TARGETS
      iqn.2001-02.com.acme:12345
      iqn.1986-03.com.sun:02:daf0161f-9f5d-e01a-b5c5-e1efa9578416
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Ajout d'un groupe d'initiateurs iSCSI (CLI)

- Pour ajouter un groupe d'initiateurs iSCSI, utilisez les commandes CLI suivantes :

```
ahi:configuration san iscsi initiators groups> create
ahi:configuration san iscsi initiators group (uncommitted)> set name=ig0
ahi:configuration san iscsi initiators group (uncommitted)>
  set initiators=iqn.2001-02.com.acme:initiator12345
ahi:configuration san iscsi initiators group (uncommitted)> commit
ahi:configuration san iscsi initiators groups> list
GROUP      NAME
group-000  ig0
|
+--> INITIATORS
      iqn.2001-02.com.acme:initiator12345
```


Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Configuration des cibles SRP (BUI)

La procédure qui suit décrit les étapes de configuration des cibles SRP.

1. **Connectez les ports HCA aux interfaces IB.**
2. **Les cibles sont détectées automatiquement par l'appareil.**
3. **Pour créer un groupe de cibles, accédez à l'écran Configuration > SAN.**
4. **Cliquez sur le lien Cible puis sur les cibles SRP.**
5. **La page des cibles SRP s'affiche.**
6. **Pour créer le groupe de cibles, cliquez sur l'icône de déplacement  pour faire glisser une cible dans la liste Groupes de cibles.**
7. **Cliquez sur Appliquer.**
8. **(Facultatif) Pour créer un initiateur et un groupe d'initiateurs dans l'écran Initiateur, cliquez sur l'icône , obtenez le GUID à partir de l'initiateur, affectez-lui un nom, puis faites le glisser dans le groupe d'initiateurs.**
9. **Pour créer un LUN et l'associer à la cible et aux initiateurs SRP que vous avez créés dans les étapes précédentes, accédez à l'écran Partages.**
10. **Cliquez sur le lien LUN, puis sur l'icône LUN . Dans les menus Groupe de cibles et Groupe d'initiateurs de la boîte de dialogue Créer un LUN, sélectionnez les groupes SRP à associer au LUN.**

Rubriques connexes

- [Présentation de SAN](#)

- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

▼ Configuration des cibles SRP (CLI)

L'exemple suivant illustre la création d'un groupe de cibles SRP nommé targetSRPgroup dans le contexte configuration san targets srp groups de la CLI :

- **Pour configurer les cibles SRP, utilisez les commandes CLI suivantes :**

```
swallower:configuration san targets srp groups> create
swallower:configuration san targets srp group (uncommitted)> set name=targetSRPgroup
                        name = targetSRPgroup (uncommitted)
swallower:configuration san targets srp group (uncommitted)>
set targets=eui.0002C903000489A4
                        targets = eui.0002C903000489A4 (uncommitted)
swallower:configuration san targets srp group (uncommitted)> commit
swallower:configuration san targets srp groups> list
GROUP      NAME
group-000 targetSRPgroup
|
+--> TARGETS
      eui.0002C903000489A4
```

Exemple 1 Création d'un LUN associé au groupe SRP cible à l'aide de la CLI

L'exemple ci-dessous indique comment créer un LUN et l'associer au groupe SRP cible dans le contexte shares de la CLI :

```
swallower:shares default> lun mylun
swallower:shares default/mylun (uncommitted)> set targetgroup=targetSRPgroup
                        targetgroup = targetSRPgroup (uncommitted)
swallower:shares default/mylun (uncommitted)> set volsize=10
                        volsize = 10 (uncommitted)
swallower:shares default/mylun (uncommitted)> commit
swallower:shares default> list
Filesystems:
NAME      SIZE      MOUNTPOINT
test      38K        /export/test
LUNs:
NAME      SIZE      GUID
mylun     10G       600144F0E9D19FFB00004B82DF490001
```

Rubriques connexes

- [Présentation de SAN](#)
- [Configuration Fibre Channel SAN](#)
- [Configuration SAN iSCSI](#)
- [Configuration de la cible SAN iSER](#)
- [Configuration SAN SRP](#)
- [Terminologie SAN](#)

Présentation de SAN

Ces trois composants restent inchangés, indépendamment du protocole utilisé sur le réseau. Dans certains cas, le réseau peut consister en un câble reliant l'initiateur et la cible, mais dans la plupart des cas, le réseau implique de la commutation sous une forme ou une autre.

Les cibles et les initiateurs sont configurés par protocole. Pour plus d'informations, reportez-vous à la documentation sur un protocole particulier ("[Configuration Fibre Channel SAN](#)" à la page 149, iSCSI ou "[Configuration SRP](#)" à la page 279).

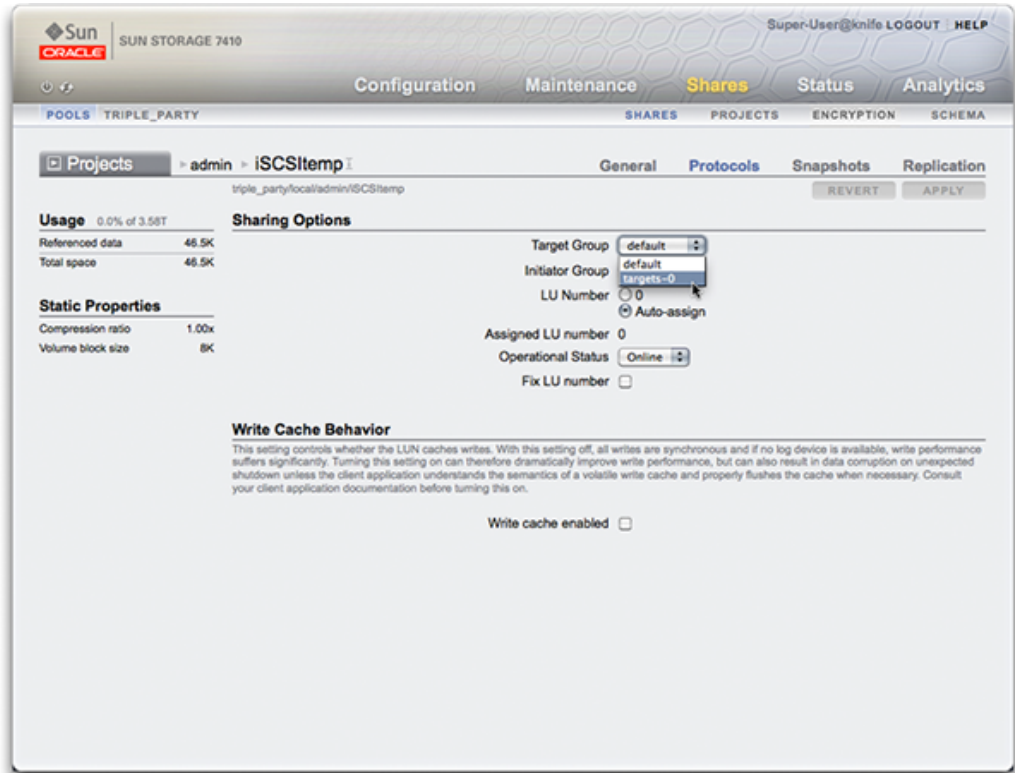
Les groupes de cibles et d'initiateurs définissent des ensembles de cibles et d'initiateurs pouvant être associés à des LUN. Un LUN associé à un groupe de cibles est uniquement visible par le biais des cibles appartenant à ce groupe. Si un LUN n'est pas explicitement associé à un groupe de cibles, il appartient au *groupe de cibles par défaut* et est accessible via toutes les cibles, indépendamment du protocole. De la même manière, un LUN est uniquement visible par les initiateurs dans le ou les groupes auxquels il appartient. Si un LUN n'est pas explicitement associé à un groupe d'initiateurs, il appartient au *groupe d'initiateurs par défaut* et est accessible par tous les initiateurs. Bien qu'elle puisse présenter un intérêt pour des évaluations, l'utilisation du groupe d'initiateurs par défaut n'est pas recommandée car elle peut exposer le LUN à des initiateurs non souhaités ou incompatibles.

Pour éviter les éventuels conflits de LUN lorsqu'un initiateur appartient à plusieurs groupes, configurez les initiateurs au sein de tous les groupes avant d'associer les groupes aux LUN.

Pour configurer les cibles, accédez à la page Configuration > BUI SAN, utilisez Fibre Channel, iSCSI et SRP pour naviguer, puis configurez les contrôles Ports, Initiateur et Groupes de cibles.

Pour associer un LUN, accédez à la page Partages > Partages > Protocoles et configurez les contrôles Groupe de cibles et Groupe d'initiateurs.

FIGURE 12 Associer un LUN



Accédez au contexte configuration `san` de la CLI pour effectuer des opérations sur les cibles et les initiateurs en fonction du type de protocole. Accédez ensuite au contexte `shares` de la CLI pour créer des LUN et les associer à des groupes de cibles et d'initiateurs.

Rubriques connexes

- [Configuration des modes de port FC \(BUI\)](#)
- [Détection de ports FC \(BUI\)](#)
- [Création de groupes d'initiateurs FC \(BUI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(BUI\)](#)
- [Changement de mode de port FC \(CLI\)](#)
- [Détection de ports FC \(CLI\)](#)
- [Création de groupes d'initiateurs FC \(CLI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(CLI\)](#)

- Scripts de création d'alias pour les initiateurs et groupes d'initiateurs (CLI)
- Configuration des initiateurs SAN iSCSI
- Création d'une feuille de travail Analyse (BUI)
- Ajout d'une cible iSCSI possédant un IQN généré de manière automatique (CLI)
- Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné (CLI)
- Ajout d'un initiateur iSCSI utilisant l'authentification CHAP (CLI)
- Ajout d'un groupe de cibles iSCSI (CLI)
- Ajout d'un groupe d'initiateurs iSCSI (CLI)
- Configuration des cibles SRP (BUI)
- Configuration des cibles SRP (CLI)

Configuration Fibre Channel SAN

Fibre Channel (FC) est une technologie de mise en réseau haut débit utilisée presque exclusivement pour transporter le protocole iSCSI. FC est l'un des protocoles de transfert par blocs pris en charge par l'appareil ; pour permettre le partage de LUN via FC, l'appareil doit être équipé d'une ou de plusieurs cartes FC.

Par défaut, tous les ports FC sont configurés pour être en mode cible. Si l'appareil est utilisé pour se connecter à une bande SAN pour des opérations de sauvegarde, un ou plusieurs ports doivent être configurés en mode initiateur. Pour configurer un port en mode initiateur, l'appareil doit être réinitialisé. Plusieurs ports peuvent être configurés en mode initiateur simultanément.

Un nom universel (WWN) est affecté à chaque port FC et, comme pour d'autres protocoles de transfert par blocs, les cibles FC peuvent être rassemblées en groupes de cibles et d'initiateurs SAN. De cette manière, la bande passante d'un port peut être dédiée à des LUN ou groupes de LUN particuliers. Une fois qu'un port FC a été configuré en tant que cible, les ports distants détectés peuvent être examinés et vérifiés.

Reportez-vous au livre blanc *Implementing Fibre Channel SAN Boot with Oracle's Sun ZFS Storage Appliance* à l'adresse <http://www.oracle.com/technetwork/articles/servers-storage-admin/fbsanboot-365291.html> pour plus de détails sur les solutions d'initialisation SAN FC à l'aide de l'appareil Oracle ZFS Storage Appliance.

Dans un cluster, les initiateurs disposent de deux chemins (ou ensembles de chemins) vers chaque LUN : un chemin (ou ensemble de chemins) pointant vers la tête ayant importé l'espace de stockage associé au LUN et un chemin (ou ensemble de chemins) pointant vers le pair en cluster de cette même tête. Le premier chemin (ou ensemble de chemins) est *actif* et le second (ou ensemble de chemins) est un chemin *de secours*. En cas de reprise, les chemins actifs ne sont plus disponibles et les chemins de secours deviennent actifs (après un court moment), après quoi les E/S se poursuivent. Cette approche de la gestion des chemins d'accès multiples est connue sous le nom d'ALUA (Asymmetric Logical Unit Access) et, lorsqu'elle est associée

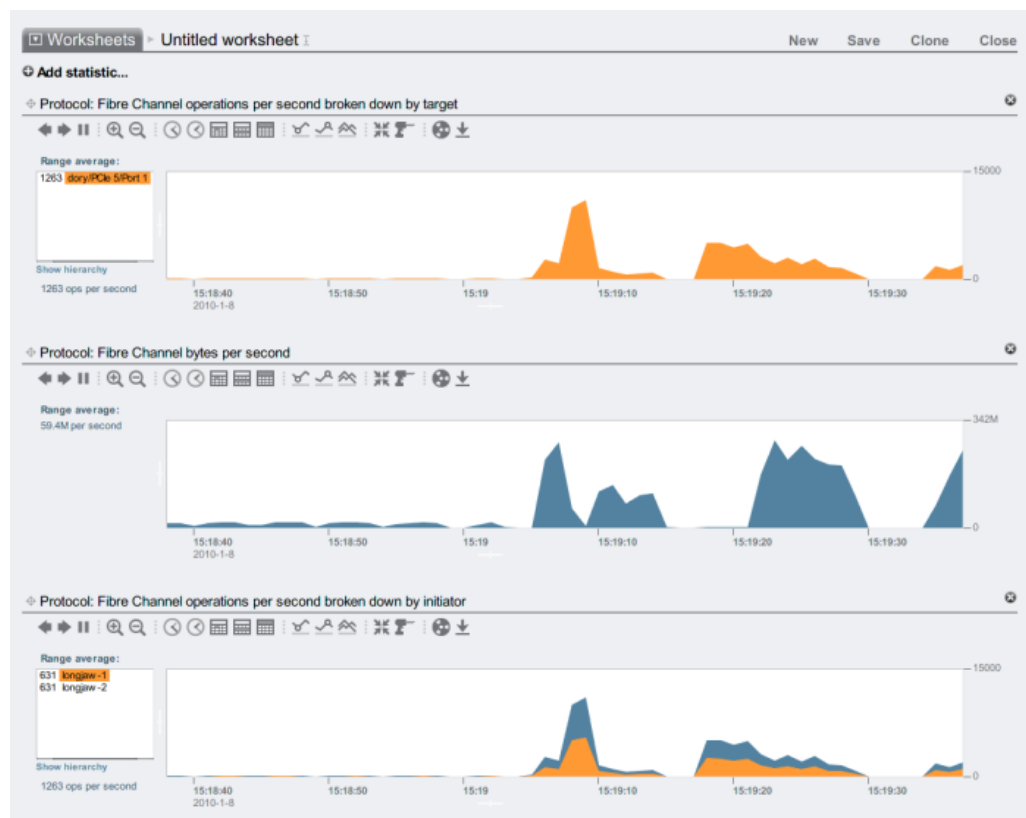
à un initiateur compatible ALUA, permet la reprise de cluster d'être transparente pour les applications de haut niveau.

Les initiateurs sont identifiés par leur WWN. Comme pour les autres protocoles, les alias peuvent être créés pour des initiateurs. Pour faciliter la création d'alias pour les initiateurs FC, un WWN peut être sélectionné parmi les WWN des ports détectés. En outre, comme pour d'autres protocoles de transfert par blocs, les initiateurs peuvent être rassemblés en groupes. Lorsqu'un LUN est associé à un groupe d'initiateurs particulier, ce LUN est uniquement visible pour les initiateurs appartenant au groupe concerné. Dans la plupart des réseaux de stockage FC, les LUN sont toujours associés au groupe d'initiateurs correspondant au(x) système(s) pour le(s)quel(s) ils ont été créés.

L'appareil est une baie compatible ALUA. La configuration correcte d'un initiateur FC dans un environnement ALUA nécessite un pilote compatible ALUA et peut nécessiter un réglage spécifique à l'initiateur. Reportez-vous à la section "Oracle ZFS Storage Appliance : comment paramétrer la gestion des chemins d'accès multiples pour les clients" (ID de doc 1628999.1) pour plus d'informations.

Le module Analyse permet d'observer les performances FC et de détailler les opérations ou le débit par initiateur, cible ou LUN.

FIGURE 13 Performances FC



En outre, les opérations peuvent être détaillées par offset, latence, taille et commande SCSI, ce qui permet non seulement de comprendre *sur quoi* portent les opérations FC, mais également *comment* et *pourquoi* elles sont réalisées.

L'appareil a été conçu pour utiliser un ensemble de ressources global afin de gérer des LUN sur chaque noeud de tête. Il n'est donc pas généralement nécessaire de limiter la profondeur de file d'attente sur les clients étant donné que les ports FC de l'appareil peuvent prendre en charge un grand nombre de demandes simultanées. Toutefois, il existe un risque très faible de voir la capacité de ces files dépassée, ce qui se traduit par des erreurs de transport SCSI. Ces dépassements de capacité de file d'attente sont souvent associés à un ou plusieurs des éléments suivants :

- Ports surchargés dans la partie frontale : nombre excessif d'hôtes associés à un port FC et/ou nombre excessif de LUN connectés via un port FC donné

- Modes de fonctionnement de l'appareil détériorés, tels qu'une reprise de cluster dans ce qui est conçu pour être une configuration de cluster active-active

Bien que le risque de voir des dépassements de capacité des files d'attente se produire soit faible, il peut être éliminé complètement en limitant la profondeur des files d'attente pour chaque client individuel. La profondeur de file d'attente appropriée est déterminée en multipliant le nombre de ports cible par le nombre maximal de commandes simultanées par port (2048), et en divisant le produit par le nombre de LUN alloués. Pour gérer les modes de fonctionnement détériorés, il faut additionner le nombre de LUN sur les paires de cluster pour déterminer le nombre de LUN, mais utiliser comme nombre de ports cible la valeur minimale des deux paires de cluster. Par exemple, dans un cluster actif-actif 7420 à deux têtes dans lequel une tête comporte 2 ports FC et 100 LUN et l'autre tête 4 ports FC et 28 LUN, la profondeur de file d'attente maximale est égale à 2 ports fois 2048 commandes, divisé par 100 LUN plus 28 LUN, soit 32 commandes par LUN.

Le réglage de la profondeur de file d'attente maximale est spécifique à l'initiateur, mais sous Solaris, celui-ci est effectué par ajustement de la variable globale `ssd_max_throttle`.

Pour résoudre les problèmes de liaison (par exemple, des fibres optiques cassées ou un câble mal placé), examinez les statistiques d'erreur de chaque port port FC. Si un nombre n'est pas égal à zéro ou augmente, cela peut indiquer que des problèmes de liaison se sont produits et qu'un diagnostic de niveau liaison est nécessaire.

Rubriques connexes

- [Configuration des modes de port FC \(BUI\)](#)
- [Détection de ports FC \(BUI\)](#)
- [Création de groupes d'initiateurs FC \(BUI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(BUI\)](#)
- [Changement de mode de port FC \(CLI\)](#)
- [Détection de ports FC \(CLI\)](#)
- [Création de groupes d'initiateurs FC \(CLI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(CLI\)](#)
- [Scripts de création d'alias pour les initiateurs et groupes d'initiateurs \(CLI\)](#)
- [Configuration des initiateurs SAN iSCSI](#)
- [Création d'une feuille de travail Analyse \(BUI\)](#)
- [Ajout d'une cible iSCSI possédant un IQN généré de manière automatique \(CLI\)](#)
- [Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné \(CLI\)](#)
- [Ajout d'un initiateur iSCSI utilisant l'authentification CHAP \(CLI\)](#)
- [Ajout d'un groupe de cibles iSCSI \(CLI\)](#)
- [Ajout d'un groupe d'initiateurs iSCSI \(CLI\)](#)
- [Configuration des cibles SRP \(BUI\)](#)
- [Configuration des cibles SRP \(CLI\)](#)

Configuration SAN iSCSI

Internet SCSI est l'un des protocoles de transfert par blocs pris en charge par l'appareil pour le partage du stockage SCSI.

Lors de l'utilisation du protocole iSCSI, le terme "portail cible" fait référence à l'association unique d'une adresse IP et d'un numéro de port TCP par le biais de laquelle un initiateur peut contacter une cible.

Lors de l'utilisation du protocole iSCSI, un groupe de portails cibles est un ensemble de portails cibles. Les groupes de portails cible sont gérés de manière transparente : à chaque interface réseau est associé un groupe de portails cible contenant les adresses actives de l'interface concernée. Lier une cible à une interface a pour effet de publier la cible iSCSI concernée à l'aide du groupe de portails qui lui est associé.

Remarque - Les connexions multiples par session ne sont pas prises en charge.

Un nom qualifié iSCSI (IQN iSCSI) est l'identifiant unique d'un périphérique dans un réseau iSCSI. iSCSI utilise la forme `iqn.date.authority:uniqueid` pour les IQN. Par exemple, l'appareil peut utiliser l'IQN : `iqn.1986-03.com.sun:02:c7824a5b-f3ea-6038-c79d-ca443337d92c` pour identifier l'une de ses cibles iSCSI. Ce nom indique qu'il s'agit d'un périphérique iSCSI fabriqué par une entreprise enregistrée en mars 1986. L'autorité de dénomination est simplement l'inversion du nom DNS de l'entreprise, "com.sun" dans ce cas. Tout ce qui suit est un ID unique utilisé par Oracle pour identifier la cible.

TABLEAU 28 Propriétés de la cible iSCSI

Propriété de la cible	Description
IQN de la cible	L'IQN de la cible concernée. L'IQN peut être spécifié manuellement ou généré de manière automatique.
Pseudonyme	Pseudonyme lisible à l'oeil de la cible concernée.
Mode d'authentification	Une valeur parmi les suivantes : Aucune, CHAP ou RADIUS.
Nom CHAP	En cas d'utilisation de l'authentification CHAP, il s'agit du nom d'utilisateur CHAP.
Secret CHAP	En cas d'utilisation de l'authentification CHAP, il s'agit du secret CHAP.
Interfaces réseau	Interfaces dont les portails cible sont utilisés pour exporter la cible concernée.

En plus de ces propriétés, la BUI indique si une cible est en ligne ou hors ligne :

TABLEAU 29 Icônes de statut de la cible

icône	description
	La cible est en ligne
	La cible est hors ligne

Sur les plates-formes en cluster, les cibles ayant au moins une interface active sur le noeud de cluster concerné sont en ligne. Soyez attentif lorsque vous assignez des interfaces à des cibles : une cible peut être configurée pour l'utilisation de groupes de portails sur des noeuds de tête disjoints. Dans ce cas de figure, la cible est en ligne sur les deux noeuds de tête, mais exporte des LUN différents selon l'espace de stockage appartenant à chaque noeud de tête. Etant donné que les interfaces réseau migrent entre les têtes de cluster à l'occasion de reprises/rétablisements ou de changements de propriétaire, les cibles iSCSI passent en ligne et hors ligne à mesure que leurs interfaces réseau respectives sont importées et exportées.

Les cibles liées à une interface IPMP sont uniquement publiées via les adresses du groupe IPMP concerné. La cible concernée n'est pas joignable via les adresses test du groupe. Les cibles liées à des interfaces construites sur un groupement LACP utilisent l'adresse du groupement concerné. Si un groupement LACP est ajouté à un groupe IPMP, une cible ne peut plus utiliser l'interface du groupement concerné, étant donné que cette adresse devient une adresse test IPMP.

Rubriques connexes

- [Configuration des modes de port FC \(BUI\)](#)
- [Détection de ports FC \(BUI\)](#)
- [Création de groupes d'initiateurs FC \(BUI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(BUI\)](#)
- [Changement de mode de port FC \(CLI\)](#)
- [Détection de ports FC \(CLI\)](#)
- [Création de groupes d'initiateurs FC \(CLI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(CLI\)](#)
- [Scripts de création d'alias pour les initiateurs et groupes d'initiateurs \(CLI\)](#)
- [Configuration des initiateurs SAN iSCSI](#)
- [Création d'une feuille de travail Analyse \(BUI\)](#)
- [Ajout d'une cible iSCSI possédant un IQN généré de manière automatique \(CLI\)](#)
- [Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné \(CLI\)](#)
- [Ajout d'un initiateur iSCSI utilisant l'authentification CHAP \(CLI\)](#)
- [Ajout d'un groupe de cibles iSCSI \(CLI\)](#)
- [Ajout d'un groupe d'initiateurs iSCSI \(CLI\)](#)
- [Configuration des cibles SRP \(BUI\)](#)
- [Configuration des cibles SRP \(CLI\)](#)

Configuration de l'initiateur SAN iSCSI

Les initiateurs iSCSI ont les propriétés configurables suivantes.

TABEAU 30 Propriétés des initiateurs SAN iSCSI

Propriété	Description
IQN de l'initiateur	IQN de l'initiateur concerné.
Pseudonyme	Pseudonyme lisible à l'oeil de l'initiateur concerné.
Utiliser CHAP	Active ou désactive l'authentification CHAP
Nom CHAP	En cas d'utilisation de l'authentification CHAP, il s'agit du nom d'utilisateur CHAP.
Secret CHAP	En cas d'utilisation de l'authentification CHAP, il s'agit du secret CHAP.

Lors de la planification de la configuration de votre client iSCSI, vous aurez besoin des informations suivantes :

- Quels initiateurs (et IQN correspondants) accéderont au réseau de stockage ?
- Si vous prévoyez d'utiliser l'authentification CHAP, quelles informations d'identification CHAP l'initiateur utilise-t-il ?
- Combien de disques iSCSI (LUN) sont nécessaires et quelle doit être leur taille ?
- Les LUN doivent-ils être partagés entre plusieurs initiateurs ?

Pour permettre à l'appareil d'effectuer l'authentification CHAP à l'aide de RADIUS, les conditions suivantes doivent être remplies :

- L'appareil doit spécifier l'adresse du serveur RADIUS et le secret à utiliser lors de la communication avec le serveur RADIUS concerné
- Le serveur RADIUS (par exemple dans son fichier clients) doit comporter une entrée indiquant l'adresse de l'appareil et spécifiant le même secret que ci-dessus
- Le serveur RADIUS (par exemple dans son fichier users) doit comporter une entrée indiquant le nom CHAP et correspondant au secret CHAP de chaque initiateur
- Si l'initiateur utilise son nom IQN en tant que nom CHAP (configuration recommandée), l'appareil n'a pas besoin d'une entrée Initiateur distincte pour chaque case Initiateur, le serveur RADIUS peut effectuer toutes les étapes d'authentification.
- Si l'initiateur utilise un nom CHAP distinct, l'appareil doit comporter une entrée Initiateur distincte pour l'initiateur concerné indiquant le mappage du nom IQN vers le nom CHAP. Cette entrée Initiateur n'a PAS besoin d'indiquer le secret CHAP de l'initiateur.

Pour obtenir des informations sur le dépannage des erreurs fréquentes de configuration iSCSI, reportez-vous à la section [iSCSI](#).

Le module Analyse permet d'observer les performances iSCSI et de détailler les opérations ou le débit par initiateur, cible ou LUN.

Rubriques connexes

- [Configuration des modes de port FC \(BUI\)](#)
- [Détection de ports FC \(BUI\)](#)
- [Création de groupes d'initiateurs FC \(BUI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(BUI\)](#)
- [Changement de mode de port FC \(CLI\)](#)
- [Détection de ports FC \(CLI\)](#)
- [Création de groupes d'initiateurs FC \(CLI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(CLI\)](#)
- [Scripts de création d'alias pour les initiateurs et groupes d'initiateurs \(CLI\)](#)
- [Configuration des initiateurs SAN iSCSI](#)
- [Création d'une feuille de travail Analyse \(BUI\)](#)
- [Ajout d'une cible iSCSI possédant un IQN généré de manière automatique \(CLI\)](#)
- [Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné \(CLI\)](#)
- [Ajout d'un initiateur iSCSI utilisant l'authentification CHAP \(CLI\)](#)
- [Ajout d'un groupe de cibles iSCSI \(CLI\)](#)
- [Ajout d'un groupe d'initiateurs iSCSI \(CLI\)](#)
- [Configuration des cibles SRP \(BUI\)](#)
- [Configuration des cibles SRP \(CLI\)](#)

Configuration SAN SRP

SRP, ou SCSI RDMA Protocol, est un protocole pris en charge par l'appareil et servant au partage de l'espace de stockage SCSI via un réseau fournissant des services RDMA (c.-à-d. InfiniBand).

Les ports SRP sont partagés avec d'autres services de port IP tels que IPoIB et RDMA. Il est possible que le service SRP ne fonctionne qu'en mode cible. Les cibles iSCSI ont les propriétés configurables suivantes.

TABEAU 31 Propriétés des cibles SRP

Propriété	Description
EUI de la cible	L'identificateur unique étendu (EUI, Extended Unique Identifier) de la cible concernée. L'EUI est assigné de manière automatique par le système et est égal au GUID du HCA par l'intermédiaire duquel le service du port SRP s'exécute.
Pseudonyme	Pseudonyme lisible à l'oeil de la cible concernée.

En plus de ces propriétés, la BUI indique si une cible est en ligne ou hors ligne :

TABEAU 32 Icônes de statut de la cible SRP

icône	description
	La cible est en ligne
	La cible est hors ligne

Sur les plates-formes en cluster, les cibles de pairs doivent être configurées dans le même groupe de cibles pour créer des configurations hautement disponibles (à chemins d'accès multiples). SRP multipathed I/O est une option de configuration réglée côté initiateur.

Les initiateurs SRP ont les propriétés configurables suivantes.

TABEAU 33 Propriétés des initiateurs SRP

Propriété	Description
EUI de l'initiateur	L'EUI de l'initiateur concerné.
Pseudonyme	Pseudonyme lisible à l'oeil de l'initiateur concerné.

Le module Analyse permet d'observer les performances SRP et de détailler les opérations ou le débit par initiateur ou cible.

Rubriques connexes

- [Configuration des modes de port FC \(BUI\)](#)
- [Détection de ports FC \(BUI\)](#)
- [Création de groupes d'initiateurs FC \(BUI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(BUI\)](#)
- [Changement de mode de port FC \(CLI\)](#)
- [Détection de ports FC \(CLI\)](#)
- [Création de groupes d'initiateurs FC \(CLI\)](#)
- [Association d'un LUN à un groupe d'initiateurs FC \(CLI\)](#)
- [Scripts de création d'alias pour les initiateurs et groupes d'initiateurs \(CLI\)](#)
- [Configuration des initiateurs SAN iSCSI](#)
- [Création d'une feuille de travail Analyse \(BUI\)](#)
- [Ajout d'une cible iSCSI possédant un IQN généré de manière automatique \(CLI\)](#)
- [Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné \(CLI\)](#)
- [Ajout d'un initiateur iSCSI utilisant l'authentification CHAP \(CLI\)](#)
- [Ajout d'un groupe de cibles iSCSI \(CLI\)](#)
- [Ajout d'un groupe d'initiateurs iSCSI \(CLI\)](#)
- [Configuration des cibles SRP \(BUI\)](#)

- [Configuration des cibles SRP \(CLI\)](#)

Terminologie SAN

Pour configurer l'appareil de manière à ce qu'il fonctionne sur un SAN, une bonne compréhension des termes de base suivants est indispensable :

TABEAU 34 Terminologie SAN

Terme	Description
Cible SCSI	Une cible SCSI est un point d'extrémité de système de stockage fournissant un service de traitement de commandes SCSI et de demandes d'E/S émises par un initiateur. Les cibles SCSI sont créées par l'administrateur du système de stockage et sont identifiées à l'aide de méthodes d'adressage uniques. Une fois configurée, une cible SCSI se compose de zéro ou d'un nombre quelconque d'unités logiques de stockage.
Initiateur SCSI	Un initiateur SCSI est un point d'extrémité d'une application ou d'un système de production, capable de lancer une session SCSI ainsi que d'envoyer des commandes SCSI et des demandes d'E/S. Les initiateurs SCSI sont également identifiés à l'aide de méthodes d'adressage uniques (voir Cible SCSI).
Unité logique de stockage	Le terme "Unité logique de stockage" est un terme utilisé pour décrire un composant d'un système de stockage. Portant un numéro unique, ce composant est également désigné par le sigle LUN, pour Logical Unit Number. Du fait de sa haute configurabilité, un système de stockage peut contenir un grand nombre de LUN. Ces LUN, associés à une ou plusieurs cibles SCSI, forment un périphérique SCSI unique auquel un ou plusieurs initiateurs SCSI peuvent accéder.
iSCSI	Internet SCSI, protocole de partage de l'espace de stockage SCSI via des réseaux IP. L'appareil prend en charge la spécification de réservations persistantes SCSI-3.
iSER	iSCSI Extension for RDMA, protocole mappant le protocole iSCSI via un réseau fournissant des services RDMA (c.-à-d. InfiniBand). Le protocole iSER est sélectionné de façon transparente par le sous-système iSCSI, en fonction de la présence de matériel IB correctement configuré. Dans la CLI et la BUI, tous les composants compatibles iSER (cibles et initiateurs) sont gérés en tant que composants iSCSI.
FC	Fibre Channel, protocole de partage de l'espace de stockage SCSI via un réseau de stockage (SAN) composé de câbles à fibres optiques, de commutateurs FC et de HBA. L'appareil prend en charge les topologies de boucle arbitrée Fibre Channel (FC-AL) de 4 et 8 Go.

Terme	Description
SRP	SCSI RDMA Protocol, protocole de partage de l'espace de stockage SCSI via un réseau fournissant des services RDMA (c.-à-d. InfiniBand).
IQN	Nom qualifié iSCSI, identifiant unique d'un périphérique dans un réseau iSCSI. iSCSI utilise la forme <code>iqn</code> . <code>date.authority:uniqueid</code> pour les IQN. Par exemple, l'appareil peut utiliser l'IQN : <code>iqn.1986-03.com.sun:02:c7824a5b-f3ea-6038-c79d-ca443337d92c</code> pour identifier l'une de ses cibles iSCSI. Ce nom indique qu'il s'agit d'un périphérique iSCSI fabriqué par une entreprise enregistrée en mars 1986. L'autorité de dénomination est simplement l'inversion du nom DNS de l'entreprise, "com.sun" dans ce cas. Tout ce qui suit est un ID unique utilisé par Sun pour identifier la cible.
Portail cible	Lors de l'utilisation du protocole iSCSI, le terme "portail cible" fait référence à l'association unique d'une adresse IP et d'un numéro de port TCP par le biais de laquelle un initiateur peut contacter une cible.
Groupe de portails cibles	Lors de l'utilisation du protocole iSCSI, un groupe de portails cibles est un ensemble de portails cibles. Les groupes de portails cible sont gérés de manière transparente : à chaque interface réseau est associé un groupe de portails cible contenant les adresses actives de l'interface concernée. Lier une cible à une interface a pour effet de publier la cible iSCSI concernée à l'aide du groupe de portails qui lui est associé.
CHAP	Challenge-handshake authentication protocol, protocole de sécurité permettant d'authentifier une cible auprès d'un initiateur, un initiateur auprès d'une cible, ou les deux.
RADIUS	Système permettant d'utiliser un serveur centralisé pour effectuer l'authentification CHAP au nom des noeuds de stockage.
Groupe de cibles	Ensemble de cibles. Les LUN sont exportés par le biais de toutes les cibles vers un groupe de cibles particulier.
Groupe d'initiateurs	Ensemble d'initiateurs. Lorsqu'un groupe d'initiateurs est associé à un LUN, seuls les initiateurs appartenant au groupe concerné peuvent accéder au LUN.
Cible	Point d'extrémité d'un système de stockage fournissant un service de traitement de commandes SCSI et de demandes d'E/S émises par un initiateur. Les cibles sont créées par l'administrateur du système de stockage et sont identifiées à l'aide de méthodes d'adressage uniques. Une fois configurée, une cible se compose de zéro ou d'un nombre quelconque d'unités logiques de stockage.
Initiateur	Point d'extrémité d'une application ou d'un système de production, capable de lancer une session SCSI ainsi que d'envoyer des commandes SCSI et des demandes d'E/S. Les initiateurs sont également identifiés à l'aide de méthodes d'adressage uniques.

Chaque LUN possède plusieurs propriétés qui déterminent la manière dont le volume est exporté. Pour plus d'informations, reportez-vous à la section [Protocoles](#).

Configuration des utilisateurs

Cette section décrit les *utilisateurs* de l'appareil, les *rôles* permettant de gérer les autorisations accordées aux utilisateurs ainsi que la manière de les ajouter au système via la BUI ou la CLI.

Pour configurer les utilisateurs et les rôles, reportez-vous aux sections suivantes :

- Ajout d'un administrateur ou d'un utilisateur [BUI](#), [CLI](#)
- Modification d'un mot de passe d'utilisateur [BUI](#), [CLI](#)
- Modification des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Suppression des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Ajout d'un rôle [BUI](#), [CLI](#)
- Modification des autorisations liées à un rôle [BUI](#), [CLI](#)
- Suppression des autorisations liées à un rôle [BUI](#), [CLI](#)
- Ajout d'un utilisateur uniquement autorisé à afficher le tableau de bord [BUI](#)

Pour obtenir des informations sur les utilisateurs et les rôles, reportez-vous aux sections suivantes :

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Ajout d'un administrateur ou d'un utilisateur (BUI)

Utilisez la procédure suivante pour créer un utilisateur avec ou sans le rôle d'administrateur. Vous trouverez une description des différents types d'utilisateur dans la section "[Présentation des utilisateurs et des rôles](#)" à la page 175.

1. **Accédez à Configuration > Utilisateurs.**
2. **Cliquez sur l'icône d'ajout  en regard des Utilisateurs.**

3. Choisissez le type d'utilisateur approprié dans le menu déroulant.

Properties
This is an appliance administrator managed by a directory service.

Type ☒ Directory
☐ Local
☐ Data
☐ No-login

Username

User ID

Full Name

Password

Confirm

Require session annotation ☐

Kiosk user ☐

Kiosk screen <https://ar7320-230:215/#status/dashboard>

Roles **Exceptions**

1 Total

NAME ▲	DESCRIPTION
☒ basic	Basic administration

4. Entrez les propriétés requises.
5. (Facultatif) Pour affecter des rôles aux utilisateurs locaux et d'annuaire, cochez les cases correspondant à ces rôles.
6. (Facultatif) Pour ajouter des exceptions aux utilisateurs locaux et d'annuaire :
 - a. Cliquez sur Exceptions.
 - b. Cochez les cases correspondant aux exceptions à ajouter.
 - c. Cliquez sur AJOUTER dans la section Exceptions.
7. Cliquez sur AJOUTER en haut de la boîte de dialogue.
Le nouvel utilisateur apparaît dans la liste Utilisateurs.

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)

- [Gestion des propriétés utilisateur](#)

▼ Ajout d'un administrateur ou d'un utilisateur (CLI)

Utilisez la procédure suivante pour créer un utilisateur avec ou sans les rôles d'administrateur. Vous trouverez une description des différents types d'utilisateur dans la section "[Présentation des utilisateurs et des rôles](#)" à la page 175.

1. **Accédez à configuration users.**

```
hostname:> configuration users
```

2. **Saisissez l'un des types d'utilisateur suivants suivi d'un nom.**

directory - pour un utilisateur d'annuaire (NIS, LDAP).

local - pour un utilisateur local.

data - pour un utilisateur des données seulement.

nologin - pour un utilisateur sans connexion.

3. **Saisissez get pour afficher la liste des propriétés qui doivent obligatoirement être définies.**

```
hostname:configuration users john (uncommitted)> get
      logname = john
        uid = (unset)
      fullname = (unset)
  initial_password = (unset)
    require_annotation = false
```

4. **Entrez la commande set suivie du nom de la propriété à définir, puis tapez commit.**

```
hostname:configuration users john (uncommitted)> set initial_password=password
      initial_password = ***** (uncommitted)
hostname:configuration users john (uncommitted)> commit
```

Vous avez alors créé un utilisateur mais n'avez pas personnalisé toutes ses propriétés.

5. **(Facultatif) Pour ajouter des rôles à un utilisateur local ou d'annuaire, tapez la commande select suivie d'un nom d'utilisateur.**
6. **(Facultatif) Tapez show pour afficher la liste complète des préférences.**

Vous pouvez alors ajouter des rôles et des exceptions d'autorisation pour l'utilisateur considéré.

Exemple 2 Création d'un utilisateur local

```
hostname:configuration users > local john
hostname:configuration users john (uncommitted) > get
    logname = john
    uid = (unset)
    fullname = (unset)
    initial_password = (unset)
    require_annotation = false
hostname:configuration users john (uncommitted) > set initial_password=password
    initial_password = ***** (uncommitted)
hostname:configuration users john (uncommitted) > commit
hostname:configuration users > select john
hostname:configuration users john > show
Properties:
    logname = john
    type = local
    uid =
    fullname =
    initial_password = *****
    require_annotation = false
    roles =
    kiosk_mode = false
    kiosk_screen = status/dashboard

Children:
    exceptions => Configure this user's exceptions
    preferences => Configure user preferences

hostname:configuration users john > set roles=
basic      basic2      test_role1 test_role2
hostname:configuration users john > set roles=basic
    roles = basic (uncommitted)
hostname:configuration users john > commit
hostname:configuration users > select john
hostname:configuration users john > show
Properties:
    logname = john
    type = local
    uid =
    fullname =
    initial_password = *****
    require_annotation = false
    roles = basic
    kiosk_mode = false
    kiosk_screen = status/dashboard

Children:
    exceptions => Configure this user's exceptions
    preferences => Configure user preferences
```

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Modification d'un mot de passe utilisateur (BUI)

Utilisez la procédure suivante pour modifier le mot de passe d'un utilisateur. Pour modifier le mot de passe d'un utilisateur autre que vous-même, vous devez détenir les privilèges de superutilisateur (root) ou un rôle doté de l'autorisation/exception utilisateur.

1. **Accédez à Configuration > Utilisateurs.**
2. **Cliquez sur l'icône de modification  en regard de l'utilisateur dont vous souhaitez changer le mot de passe.**
3. **Dans la boîte de dialogue Modifier l'utilisateur local, tapez un nouveau mot de passe, puis saisissez-le à nouveau pour le confirmer.**
4. **Cliquez sur APPLIQUER.**

Rubriques connexes

- Modification des exceptions liées à un utilisateur [BUI](#)
- Modification des autorisations liées à un rôle [BUI](#)

▼ Modification d'un mot de passe utilisateur (CLI)

Utilisez la procédure suivante pour modifier le mot de passe d'un utilisateur. Pour modifier le mot de passe d'un utilisateur autre que vous-même, vous devez détenir les privilèges de superutilisateur (root) ou un rôle doté de l'autorisation/exception utilisateur.

1. **Accédez à configuration users, puis saisissez show pour afficher une liste d'utilisateurs.**

```
hostname:> configuration users
hostname:configuration users > show
Users:
```

NAME	USERNAME	UID	TYPE
Super-User	root	0	Loc

2. Entrez la commande **select** suivie du nom de l'utilisateur dont vous souhaitez changer le mot de passe. Saisissez ensuite **show**.

```
hostname:configuration users > select root
hostname:configuration users root > show
Properties:

    logname = root
    fullname = Super-User
    initial_password = *****
    require_annotation = false

Children:

    preferences => Configure user preferences
```

3. Entrez **set initial_password=** et le nouveau mot de passe.

```
hostname:configuration users root > set initial_password=[new password]
    initial_password = ***** (uncommitted)
```

4. Saisissez **commit**.

```
hostname:configuration users root > commit
```

Rubriques connexes

- Modification des exceptions liées à un utilisateur [CLI](#)
- Modification des autorisations liées à un rôle [CLI](#)

▼ Modification des exceptions liées à un utilisateur (BUI)

Utilisez la procédure suivante pour modifier les exceptions liées à un utilisateur.

1. Accédez à **Configuration > Utilisateurs**.
2. Déplacez le pointeur de la souris sur l'utilisateur concerné dans la liste **Utilisateurs** et cliquez sur l'icône de modification .
3. Cliquez sur **Exceptions**.
4. Sélectionnez **Portée**.
Si des filtres sont disponibles pour cette portée, ils sont répertoriés sous le sélecteur de portée.
5. Cochez les cases correspondant aux exceptions que vous souhaitez ajouter.

6. Cliquez sur **AJOUTER** dans la section **Exceptions**.

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Modification des exceptions liées à un utilisateur (CLI)

Utilisez la procédure suivante pour modifier les exceptions liées à un utilisateur.

1. Accédez à configuration **users**.
2. Saisissez **select** suivi du nom d'utilisateur.
3. Saisissez **exceptions**.
4. Saisissez **create**.
5. Saisissez **set scope=** suivi du nom de la portée. Affichez la liste à l'aide de la saisie semi-automatique via la touche **TAB**.
6. Saisissez **show** pour afficher la liste des propriétés.
7. Saisissez **set** pour activer les propriétés voulues.
8. Saisissez **commit**.

L'exception est alors ajoutée.

Exemple 3 Ajout d'une exception pour exclure les autorisations d'une portée

Cet exemple ajoute une exception afin d'exclure les autorisation de portée **svc** pour l'utilisateur "brendan" :

```
hostname:configuration users brendan > exceptions
hostname:configuration users brendan exceptions > create
hostname:configuration users brendan auth (uncommitted) > show
Properties:
    scope = (unset)
hostname:configuration users brendan auth (uncommitted) > set scope=svc
    scope = svc
hostname:configuration users brendan auth (uncommitted) > show
```

```

Properties:
    scope = svc
    service = *
    allow_administer = false
    allow_configure = false
    allow_restart = false
hostname:configuration users brendan auth (uncommitted) > commit
hostname:configuration users brendan exceptions > show
Auths:

NAME          OBJECT          PERMISSIONS
auth-000      svc.*           none

hostname:configuration users brendan exceptions > select auth-000
hostname:configuration users brendan auth-000 > show
Properties:
    scope = svc
    service = *
    allow_administer = false
    allow_configure = false
    allow_restart = false

hostname:configuration users brendan auth-000 >

```

Exemple 4 Ajout d'une exception pour inclure les autorisations d'une portée

Cet exemple ajoute une exception pour inclure une autorisation de portée ne faisant pas partie du rôle "webadmin" :

```

hostname:configuration users brendan exceptions > create
hostname:configuration users brendan auth (uncommitted) > set scope=appliance
    scope = appliance
hostname:configuration users brendan auth (uncommitted) > show
Properties:
    scope = appliance
    service = *
    allow_audit = false
    allow_factoryReset = false
    allow_powerOff = false
    allow_reboot = false
    allow_setName = false
    allow_shell = false

hostname:configuration users brendan auth (uncommitted) > set allow_audit=true
    allow_audit = true (uncommitted)
hostname:configuration users brendan auth (uncommitted) > commit
hostname:configuration users brendan exceptions > show
Auths:

NAME          OBJECT          PERMISSIONS
auth-000      svc.*           none
auth-001      appliance.*     audit

```

```
hostname:configuration users brendan exceptions >
```

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Suppression des exceptions liées à un utilisateur (BUI)

Utilisez la procédure suivante pour supprimer les exceptions liées à un utilisateur.

1. **Accédez à Configuration > Utilisateurs.**
2. **Déplacez le pointeur de la souris sur l'utilisateur concerné dans la liste Utilisateurs et cliquez sur l'icône de modification .**
3. **Cliquez sur Exceptions.**
4. **Déplacez le pointeur de la souris sur l'exception dans la liste du bas et cliquez sur l'icône de la corbeille .**
5. **Cliquez sur APPLIQUER en haut de la boîte de dialogue.**

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Suppression des exceptions liées à un utilisateur (CLI)

Utilisez la procédure suivante pour supprimer les exceptions liées à un utilisateur.

1. **Accédez à `configuration users`.**
2. **Saisissez `select` suivi du nom d'utilisateur.**

3. Saisissez **exceptions**.
4. Saisissez **show** pour afficher la liste des exceptions.
5. Saisissez la commande **destroy** suivie du nom de l'exception. L'exception est alors détruite.

Exemple 5 Suppression d'une exception pour un utilisateur

```
hostname:configuration users > select john
hostname:configuration users john > ls
Properties:
    logname = john
    type = local
    uid = 2000000001
    fullname = john
    initial_password = *****
    require_annotation = false
    kiosk_mode = false
    kiosk_screen = status/dashboard

Children:
    exceptions => Configure this user's exceptions
    preferences => Configure user preferences

hostname:configuration users john > exceptions
hostname:configuration users john exceptions > show
Auths:

NAME      OBJECT      PERMISSIONS
auth-000  ad.*        domain
                               workgroup

hostname:configuration users john exceptions > destroy auth-000
This will destroy "auth-000". Are you sure? (Y/N)
hostname:configuration users john exceptions > show
hostname:configuration users john exceptions >
```

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Ajout d'un rôle (BUI)

Utilisez la procédure suivante pour ajouter un rôle.

1. **Accédez à Configuration > Utilisateurs.**
2. **Cliquez sur l'icône d'ajout  en regard des Rôles.**
3. **Définissez le nom et la description du rôle.**
4. **(Facultatif) Sous Autorisations, sélectionnez une portée.**
Si des filtres sont disponibles pour cette portée, ils figurent sous le sélecteur Portée.
5. **(Facultatif) Sélectionnez les filtres appropriés pour la portée, le cas échéant.**
6. **(Facultatif) Cochez la case correspondant à chaque autorisation à ajouter.**
7. **Cliquez sur AJOUTER en haut de la boîte de dialogue.**
Le nouveau rôle apparaît dans la liste Rôles.

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Ajout d'un rôle (CLI)

Utilisez la procédure suivante pour ajouter un rôle.

1. **Accédez à configuration roles.**
2. **Saisissez role suivi du nom de rôle que vous souhaitez créer.**
3. **Définissez la description, puis validez le rôle à l'aide de la commande commit.**
4. **(Facultatif) Saisissez authorizations.**
5. **(Facultatif) Saisissez create pour ajouter une autorisation.**
6. **(Facultatif) Saisissez set scope= suivi du nom de la portée. Affichez la liste à l'aide de la saisie semi-automatique via la touche TAB.**
7. **(Facultatif) Saisissez show pour afficher à la fois les filtres et les autorisations disponibles.**

8. **(Facultatif) Définissez les autorisations de votre choix sur true à l'aide de la commande set et définissez les filtres (si disponibles). La saisie semi-automatique via la touche TAB permet d'afficher les paramètres de filtre qui sont valides.**
9. **Saisissez commit.**
Le nouveau rôle a été ajouté.

Exemple 6 Création du rôle "webadmin"

```
hostname:> configuration roles
hostname:configuration roles > role webadmin
hostname:configuration roles webadmin (uncommitted) > set
                        description="web server administrator"
                        description = web server administrator (uncommitted)
hostname:configuration roles webadmin (uncommitted) > commit
hostname:configuration roles > show
Roles:
```

NAME	DESCRIPTION
basic	Basic administration
webadmin	web server administrator

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Modification des autorisations liées à un rôle (BUI)

Un rôle est un ensemble de privilèges qui peut être assigné à un utilisateur. Utilisez la procédure suivante pour modifier les autorisations liées à un rôle.

1. **Accédez à Configuration > Utilisateurs.**
2. **Déplacez le pointeur de la souris sur le rôle concerné dans la liste Rôles et cliquez sur l'icône de modification .**
3. **Sous Autorisations, sélectionnez une portée.**
Si des filtres sont disponibles pour cette portée, ils figurent sous le sélecteur Portée.
4. **Sélectionnez les filtres appropriés pour la portée, le cas échéant.**

5. **Cochez la case correspondant à chaque autorisation à ajouter.**
6. **Cliquez sur AJOUTER dans la section Autorisations.**
Les autorisations sont ajoutées au bas de la boîte de dialogue.
7. **Cliquez sur APPLIQUER en haut de la boîte de dialogue.**

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Modification des autorisations liées à un rôle (CLI)

Un rôle est un ensemble de privilèges qui peut être assigné à un utilisateur. Utilisez la procédure suivante pour modifier les autorisations liées à un rôle.

1. **Accédez à configuration roles.**
2. **Saisissez select suivi du nom de rôle.**
3. **Saisissez authorizations.**
4. **Saisissez create pour ajouter une autorisation.**
5. **Saisissez set scope= suivi du nom de la portée. Affichez la liste à l'aide de la saisie semi-automatique via la touche TAB.**
6. **Saisissez show pour afficher à la fois les filtres et les autorisations disponibles.**
7. **Définissez les autorisations de votre choix sur true à l'aide de la commande set et définissez les filtres (si disponibles). La saisie semi-automatique via la touche TAB permet d'afficher les paramètres de filtre qui sont valides.**
8. **Saisissez commit.**
L'autorisation est alors ajoutée.

Exemple 7 Ajout de l'autorisation de redémarrer le service HTTP

L'exemple présent illustre l'ajout de l'autorisation à redémarrer le service HTTP. Il présente également le résultat de la saisie semi-automatique par tabulation qui répertorie les valeurs d'entrée valides et aide à déterminer les portées et les options de filtre valides.

```

hostname:configuration roles > select webadmin
hostname:configuration roles webadmin > authorizations
hostname:configuration roles webadmin authorizations > create
hostname:configuration roles webadmin auth (uncommitted) > set scope=tab
ad          cluster    net          schema      update
alert       hardware   replication  stat        user
appliance   nas             role        svc         worksheet
hostname:configuration roles webadmin auth (uncommitted) > set scope=svc
scope = svc
hostname:configuration roles webadmin auth (uncommitted) > show
Properties:
scope = svc
service = *
allow_administer = false
allow_configure = false
allow_restart = false

hostname:configuration roles webadmin auth (uncommitted) > set service=tab
*          ftp         ipmp        nis         ssh
ad         http        iscsi      ntp         tags
smb        identity    ldap       routing     vscan
datalink:igb0 idmap    ndmp       scrk
dns        interface:igb0 nfs        snmp
hostname:configuration roles webadmin auth (uncommitted) > set service=http
service = http (uncommitted)
hostname:configuration roles webadmin auth (uncommitted) > set allow_restart=true
allow_restart = true (uncommitted)
hostname:configuration roles webadmin auth (uncommitted) > commit
hostname:configuration roles webadmin authorizations > list
NAME      OBJECT                                PERMISSIONS
auth-000  svc.http                             restart

```

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Suppression des autorisations d'un rôle (BUI)

Utilisez la procédure suivante pour supprimer les autorisations liées à un rôle.

1. **Accédez à Configuration > Utilisateurs.**
2. **Déplacez le pointeur de la souris sur le rôle concerné dans la liste Rôles et cliquez sur l'icône de modification .**

3. Déplacez le pointeur de la souris sur l'autorisation dans la liste du bas et cliquez sur l'icône de la corbeille .
4. Cliquez sur **APPLIQUER** en haut de la boîte de dialogue.

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

▼ Suppression des autorisations d'un rôle (CLI)

Utilisez la procédure suivante pour supprimer les autorisations liées à un rôle.

1. **Accédez à configuration roles.**
2. **Saisissez select suivi du nom de rôle.**
3. **Saisissez authorizations.**
4. **Saisissez show pour afficher la liste des autorisations.**
5. **Saisissez la commande destroy suivie du nom de l'autorisation.**

Exemple 8 Suppression d'une autorisation liée à un rôle

```
hostname:configuration roles > select test_role1
hostname:configuration roles test_role1 > authorizations
hostname:configuration roles test_role1 authorizations > show
Auths:

NAME      OBJECT      PERMISSIONS
auth-000  ad.*        domain
                               workgroup

hostname:configuration roles test_role1 authorizations > destroy auth-000
This will destroy "auth-000". Are you sure? (Y/N)
hostname:configuration roles test_role1 authorizations > show
hostname:configuration roles test_role1 authorizations >
```

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)

- [Gestion des propriétés utilisateur](#)

▼ Ajout d'un utilisateur autorisé à afficher le tableau de bord

Utilisez la procédure suivante pour ajouter un utilisateur qui peut uniquement afficher le tableau de bord.

1. **Ajoutez un utilisateur d'annuaire ou local comme indiqué dans la section "[Ajout d'un administrateur ou d'un utilisateur \(BUI\)](#)" à la page 160.**
2. **Cochez la case Kiosk. Vérifiez que l'écran Kiosk est configuré sur statut/tableau de bord.**
3. **Cliquez sur AJOUTER.**

L'utilisateur doit maintenant pouvoir se connecter et afficher uniquement le tableau de bord.

Rubriques connexes

- [Présentation des utilisateurs et des rôles](#)
- [Autorisations utilisateur](#)
- [Gestion des propriétés utilisateur](#)

Présentation des utilisateurs et des rôles

Un utilisateur peut présenter l'un des types suivants :

Utilisateur avec privilèges d'administrateur	Utilisateur sans privilège d'administrateur
Local - Administrateur d'appareils défini localement. Il peut recevoir des privilèges via l'assignation de rôles personnalisés. Il peut éventuellement être défini avec un ID d'utilisateur (UID) spécifique. Bien que les utilisateurs locaux soient pris en charge pour les services de données, les groupes locaux ne sont pas pris en charge.	Données seules - Utilisateur défini localement pour les données (SMB, NFS, FTP, etc.), sans accès administrateur. Un UID peut éventuellement lui être affecté.
Annuaire - Administrateur d'appareils géré par un service d'annuaire (NIS ou LDAP). Il peut recevoir des privilèges via l'affectation de rôles personnalisés.	Sans connexion - Nom d'utilisateur et UID réservés au mappage d'identités. Ce type d'utilisateur n'est pas autorisé à se connecter à l'appareil et peut éventuellement être défini avec un UID.

Les utilisateurs locaux et d'annuaire sont des types d'administrateur qui peuvent être dotés de privilèges via l'affectation de *rôles* personnalisés.

Un rôle est un ensemble de privilèges qui peut être assigné à un utilisateur. Par exemple, vous pouvez créer les rôles *administrateur* et *opérateur* avec des niveaux d'autorisation différents. Les membres du personnel peuvent recevoir n'importe quel rôle adapté à leurs besoins, sans qu'il soit nécessaire d'assigner des privilèges inutiles.

L'utilisation de rôles est une solution plus sécurisée que l'affectation du mot de passe *root* à tout le monde. Les rôles limitent les utilisateurs aux autorisations nécessaires uniquement. Leurs actions respectives sont attribuées à leur nom d'utilisateur individuel dans le journal.

Rubriques connexes

- Ajout d'un administrateur ou d'un utilisateur [BUI](#), [CLI](#)
- Modification d'un mot de passe d'utilisateur [BUI](#), [CLI](#)
- Modification des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Suppression des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Ajout d'un rôle [BUI](#), [CLI](#)
- Modification des autorisations liées à un rôle [BUI](#), [CLI](#)
- Suppression des autorisations liées à un rôle [BUI](#), [CLI](#)
- Ajout d'un utilisateur uniquement autorisé à afficher le tableau de bord [BUI](#)

Autorisations utilisateur

Les autorisations permettent aux utilisateurs d'effectuer des tâches spécifiques telles que la création de partages, la réinitialisation de l'appareil et la mise à jour du logiciel système. Les autorisations sont regroupées en *portées*, chacune étant susceptible d'être limitée par un ensemble de filtres facultatifs. Par exemple, au lieu de posséder une autorisation de redémarrage de tous les services, vous pouvez définir un filtre afin de permettre à cette autorisation de ne redémarrer que le service HTTP.

Le tableau suivant présente les portées disponibles :

TABLEAU 35 Portées utilisateur disponibles

Portée (BUI)	Portée (CLI)	Exemple d'autorisation	Exemple de filtre
Active Directory	ad	Rejoindre un domaine Active Directory	Nom de domaine
Alertes	alerte	Configuration de filtres et de seuils d'alerte	-
Analyse	stat	Lecture de statistiques en présence de cette analyse descendante	Analyses descendantes
Appareil	appliance	Réinitialiser l'appareil	Nom de l'appareil
Clustering	cluster	Rétablissement des ressources sur un pair de cluster	-

Portée (BUI)	Portée (CLI)	Exemple d'autorisation	Exemple de filtre
Ensembles de données	ensemble de données	Gestion des aspects des ensembles de données d'analyse	Configuration
Matériel	Matériel	Gestion des disques en ligne et hors ligne	-
Keystores	keystore	Configuration de keystores	-
Réseau	net	Configuration de périphériques réseau, de liaisons de données et d'interfaces	-
Projets et partages	nas	Modification des propriétés générales des projets et des partages	Pool, projet, partage
Rôles	rôle	Configuration des autorisations pour un rôle	Nom de rôle
SAN	stmf	Configuration des autorisations pour SAN	-
Services	svc	Redémarrage d'un service	Nom de service
Schéma de propriétés de partages	schema	Modification du schéma de propriétés	-
Mise à jour	update	Mise à jour du logiciel système	-
Utilisateurs	utilisateur	Modification d'un mot de passe	Nom d'utilisateur
Workflow	Workflow	Modification du workflow	Nom du workflow
Feuille de travail	Feuille de calcul	Modification de la feuille de travail	Nom de feuille de travail

Rubriques connexes

- Ajout d'un administrateur ou d'un utilisateur [BUI](#), [CLI](#)
- Modification d'un mot de passe d'utilisateur [BUI](#), [CLI](#)
- Modification des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Suppression des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Ajout d'un rôle [BUI](#), [CLI](#)
- Modification des autorisations liées à un rôle [BUI](#), [CLI](#)
- Suppression des autorisations liées à un rôle [BUI](#), [CLI](#)
- Ajout d'un utilisateur uniquement autorisé à afficher le tableau de bord [BUI](#)

Gestion des propriétés utilisateur

La page Configuration > Utilisateurs répertorie les utilisateurs et les groupes et propose des boutons d'administration. Déplacez le pointeur de la souris sur une entrée pour afficher

les boutons permettant de la cloner, de la modifier et de la détruire. Double-cliquez sur un utilisateur ou un rôle ou cliquez sur son icône de modification  pour afficher l'écran d'édition correspondant. Les icônes sont décrites ci-après :

TABLEAU 36 Icônes de la page Utilisateurs de la BUI

Icône	Description
	Ajouter un utilisateur ou un rôle. Une nouvelle boîte de dialogue s'ouvre pour vous permettre d'entrer les propriétés requises.
	Ouvrir une boîte de dialogue de recherche. Saisissez une chaîne de recherche et appuyez sur Entrée pour rechercher ce texte dans les listes d'utilisateurs ou de rôles et n'afficher que les entrées correspondantes. Cliquez à nouveau sur cette icône pour retourner à la liste complète.
	Cloner un utilisateur ou un rôle. Ajoutez un utilisateur ou un rôle en commençant par les champs correspondant aux valeurs de cette saisie.
	Modifier un utilisateur ou un rôle.
	Supprimer un utilisateur, un rôle ou une autorisation.

En fonction du type d'utilisateur, toutes les propriétés suivantes peuvent être définies lors de l'ajout d'un utilisateur mais seulement un sous-ensemble d'entre elles lors de la modification d'un utilisateur :

TABLEAU 37 Propriétés utilisateur

Propriété	Description
Type	Vous trouverez une description des différents types d'utilisateur dans la section " Présentation des utilisateurs et des rôles " à la page 175.
Nom d'utilisateur	Nom unique de l'utilisateur
ID utilisateur	Activée uniquement pour les utilisateurs des types Local, Données seules et Sans connexion. Vous pouvez opter pour une affectation automatique ou indiquer l'ID utilisateur de votre choix. L'ID affecté automatiquement ne peut pas être inférieur à 100, ni supérieur à 2147483646, ni égal à 60001, 60002 ou 65534.
Nom complet	Description de l'utilisateur
Mot de passe/Confirmer	Pour les utilisateurs des types Local et Données seules, entrez le mot de passe initial dans ces deux champs.
Exiger annotation de session	Si cette propriété est activée, les utilisateurs doivent fournir un texte justifiant leur connexion quand ils se connectent à l'appareil. Cette annotation peut être utilisée pour suivre le travail effectué pour les demandes dans un système de création de tickets et l'ID de ticket peut servir

Propriété	Description
	d'annotation de session. L'annotation de session apparaît dans le journal.
Utilisateur Kiosk	Si cette propriété est activée, l'utilisateur peut uniquement afficher l'écran dans le paramètre "Ecran Kiosk". Cela peut permettre de limiter l'accès d'un utilisateur à la consultation du tableau de bord, par exemple. Un utilisateur Kiosk ne peut pas accéder à l'appareil via la CLI.
Ecran Kiosk	Ecran auquel cet utilisateur Kiosk est restreint lorsque la propriété "Utilisateur Kiosk" est activée.
Rôles	Rôles affectés à un utilisateur local ou d'annuaire.
Exceptions	Ces autorisations sont incluses ou exclues de celles qui sont habituellement disponibles pour les rôles sélectionnés. Par exemple, une exception peut être ajoutée pour exclure l'intégralité ou une partie des autorisations de portée pour un rôle assigné à un utilisateur, ou pour inclure des autorisations de portée pour un utilisateur sans définir cette portée dans un rôle.

Les propriétés suivantes peuvent être définies dans le cadre de la gestion des rôles.

TABLEAU 38 Propriétés des rôles

Propriété	Description
Nom	Nom du rôle tel qu'il figure dans la liste
Description	Description détaillée du rôle, le cas échéant
Exceptions	Exceptions associées à ce rôle

Rubriques connexes

- Ajout d'un administrateur ou d'un utilisateur [BUI](#), [CLI](#)
- Modification d'un mot de passe d'utilisateur [BUI](#), [CLI](#)
- Modification des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Suppression des exceptions pour un utilisateur [BUI](#), [CLI](#)
- Ajout d'un rôle [BUI](#), [CLI](#)
- Modification des autorisations liées à un rôle [BUI](#), [CLI](#)
- Suppression des autorisations liées à un rôle [BUI](#), [CLI](#)
- Ajout d'un utilisateur uniquement autorisé à afficher le tableau de bord [BUI](#)

Configuration des préférences pour l'appareil

Cette section contient des paramètres de préférence relatifs à votre localité, aux propriétés de votre session, à l'analyse avancée et aux clés SSH.

Pour configurer vos préférences, reportez-vous aux sections suivantes :

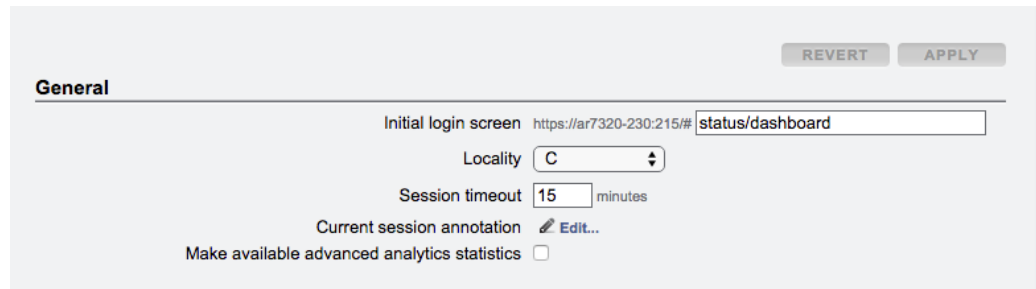
- Configuration des préférences - [BUI](#), [CLI](#)
- Configuration des clés publiques SSH - [BUI](#), [CLI](#)
- [Propriétés des préférences](#)

▼ Configuration des préférences (BUI)

Utilisez la procédure suivante pour définir les préférences pour le compte utilisateur en cours. Si vous vous connectez à la BUI à l'aide d'un autre compte que le vôtre, les préférences sont enregistrées pour cet utilisateur, par exemple l'utilisateur root.

Pour modifier les préférences de comptes utilisateur autres que celui actuellement connecté, reportez-vous à la section "[Configuration des préférences \(CLI\)](#)" à la page 180.

1. **Accédez à Configuration > Préférences.**
2. **Modifiez les propriétés à l'aide des valeurs décrites dans la section [Propriétés des préférences](#).**



3. **Cliquez sur APPLIQUER.**

▼ Configuration des préférences (CLI)

Utilisez les exemples suivants pour définir les préférences des comptes utilisateur. Si vous vous connectez à la CLI à l'aide d'un autre compte que le vôtre, les préférences sont enregistrées pour cet utilisateur, par exemple l'utilisateur root. L'exemple 2 indique comment modifier les préférences de comptes utilisateur autres que celui actuellement connecté.

- **Choisissez l'exemple approprié.**

Exemple 9 Configuration des préférences pour le compte utilisateur en cours

Utilisez les commandes d'interface de ligne de commande suivantes pour définir les préférences du compte utilisateur en cours.

Cet exemple illustre la configuration de la propriété d'annotation de session, qui ne peut être définie que pour l'utilisateur actuellement connecté.

```
hostname:> configuration preferences
hostname:configuration preferences> show
Properties:
    locale = C
    login_screen = status/dashboard
    session_timeout = 15
    session_annotation =
    advanced_analytics = false

Children:
    keys => Manage SSH public keys

hostname:configuration preferences> set session_annotation="Editing my user preferences"
    session_annotation = Editing my user preferences (uncommitted)
hostname:configuration preferences> commit
```

Exemple 10 Configuration des préférences pour un autre compte utilisateur

Utilisez les commandes d'interface de ligne de commande suivantes pour définir les préférences d'un autre compte utilisateur. Il convient toutefois de noter que vous ne pouvez pas définir d'annotation de session pour un autre utilisateur que celui actuellement connecté.

Cet exemple illustre l'activation de l'analyse avancée pour un utilisateur donné.

```
hostname:> configuration users
hostname:configuration users> select brendan
hostname:configuration users brendan> preferences
hostname:configuration users brendan preferences> show
Properties:
    locale = C
    login_screen = status/dashboard
    session_timeout = 15
    advanced_analytics = false

Children:
    keys => Manage SSH public keys

hostname:configuration users brendan preferences> set advanced_analytics=true
    advanced_analytics = true (uncommitted)
hostname:configuration users brendan preferences> commit
```

▼ Configuration des clés publiques SSH (BUI)

Les clés publiques SSH permettent d'autoriser les connexions SSH sans mot de passe. Cette fonctionnalité est utile pour les administrateurs et pour l'exécution automatique de scripts.

Procédez comme suit pour configurer les clés publiques SSH pour l'utilisateur en cours. Pour configurer des clés pour d'autres utilisateurs, reportez-vous à la section "[Configurations des clés publiques SSH \(CLI\)](#)" à la page 182.

1. **Accédez à Configuration > Préférences.**
2. **Cliquez sur l'icône d'ajout  en regard de Clés publiques SSH.**
3. **Sélectionnez un type, puis saisissez la clé publique SSH et un commentaire de clé.**
4. **Cliquez sur AJOUTER.**

▼ Configurations des clés publiques SSH (CLI)

Les clés publiques SSH permettent d'autoriser les connexions SSH sans mot de passe. Cette fonctionnalité est utile pour les administrateurs et pour l'exécution automatique de scripts.

Utilisez les exemples suivants pour configurer les clés publiques SSH pour les comptes utilisateur. Si vous vous connectez à la CLI à l'aide d'un autre compte que le vôtre, les clés sont enregistrées pour cet utilisateur, par exemple l'utilisateur root. L'exemple 2 indique comment modifier les clés de comptes utilisateur autres que celui actuellement connecté.

- **Choisissez l'exemple approprié.**

Exemple 11 Configuration des clés publiques SSH pour le compte utilisateur en cours

Utilisez les commandes d'interface de ligne de commande suivantes pour définir les clés publiques SSH du compte utilisateur en cours.

```
hostname:> configuration preferences
hostname:configuration preferences> show
Properties:
    locale = C
    login_screen = status/dashboard
    session_timeout = 15
    advanced_analytics = false

Children:
    keys => Manage SSH public keys
```

```

hostname: configuration preferences> keys
hostname:configuration preferences keys> create
hostname:configuration preferences key (uncommitted)> set type=DSA
hostname:configuration preferences key (uncommitted)> set key="...DSA key text..."
      key = ...DSA key text...(uncommitted)
hostname:configuration preferences key (uncommitted)> set comment="fw-log1"
      comment = fw-log1 (uncommitted)
hostname:configuration preferences key (uncommitted)> commit
hostname:configuration preferences keys> show
Keys:

NAME      MODIFIED          TYPE  COMMENT
key-000   07/12/2015 10:54:58  DSA   fw-log1

```

Exemple 12 Configuration des clés publiques SSH pour un autre compte utilisateur

Utilisez les commandes d'interface de ligne de commande suivantes pour définir les clés publiques SSH d'un autre compte utilisateur.

```

hostname:> configuration users
hostname:configuration users> select john
hostname:configuration users john> preferences show
Properties:
      locale = C
      login_screen = status/dashboard
      session_timeout = 15
      advanced_analytics = false

Children:
      keys => Manage SSH public keys

hostname: configuration users john> preferences keys
hostname:configuration users john preferences keys> create
hostname:configuration users john preferences key (uncommitted)> set type=DSA
hostname:configuration users john preferences key (uncommitted)> set key="...DSA key text..."
      key = ...DSA key text...(uncommitted)
hostname:configuration users john preferences key (uncommitted)> set comment="fw-log2"
      comment = fw-log2 (uncommitted)
hostname:configuration users john preferences key (uncommitted)> commit
hostname:configuration users john preferences keys> show
Keys:

NAME      MODIFIED          TYPE  COMMENT
key-001   07/13/2015 10:57:58  DSA   fw-log2

```

Propriétés des préférences

Le tableau suivant décrit les propriétés permettant de configurer les préférences utilisateur.

TABLEAU 39 Propriétés des préférences

Propriété	Description
Ecran de connexion initial	Première page chargée par la BUI après la réussite d'une connexion. Par défaut, il s'agit du tableau de bord de statut.
Localité	Par défaut, C. Les localités C et POSIX prennent uniquement en charge les caractères ASCII ou le texte brut. ISO 8859-1 prend en charge les langues suivantes : afrikaans, basque, catalan, danois, néerlandais, anglais, féroïen, finnois, français, galicien, allemand, islandais, irlandais, italien, norvégien, portugais, espagnol et suédois.
Délai d'expiration de la session	Délai au-delà duquel le navigateur sera automatiquement déconnecté de la session après avoir quitté la BUI
Annotation de la session actuelle	Commentaire ajouté aux journaux d'audit
Statistiques d'analyse avancée	Permet d'accéder à des statistiques supplémentaires dans Analyse.
Clés publiques SSH	Clés publiques RSA/DSA. Des commentaires peuvent être associés aux clés afin d'expliquer aux administrateurs la raison pour laquelle elles ont été ajoutées. Dans la BUI, ces clés s'appliquent uniquement à l'utilisateur en cours. Pour ajouter des clés à d'autres utilisateurs, utilisez la CLI.

Configuration des alertes

Cette section décrit les Alertes système, la manière de les personnaliser et l'emplacement des journaux d'alertes. Pour surveiller les statistiques depuis Analyse, créez des alertes avec seuil personnalisées. Pour configurer le système afin qu'il réponde à certains types d'alertes, utilisez les actions d'alerte.

Pour configurer les alertes, reportez-vous aux sections suivantes :

- [Ajout d'une action d'alerte \(BUI\)](#)
- [Ajout d'une action d'alerte \(CLI\)](#)
- [Envoi d'alertes par e-mail \(CLI\)](#)
- [Envoi d'un déroutement SNMP \(CLI\)](#)

Pour plus de détails sur les alertes, reportez-vous aux sections suivantes :

- [Catégories d'alertes](#)
- [Envoi de messages SYSLOG](#)
- [Exécution d'un workflow](#)
- [Alertes avec seuil](#)

- [Reprise/suspension de feuilles de travail et d'ensembles de données](#)

▼ Ajout d'une action d'alerte (BUI)

1. Cliquez sur l'icône d'ajout en regard de "Actions d'alerte".
2. Sélectionnez la catégorie ou sélectionnez "Tous les événements" pour tout.
3. Sélectionnez Tous les événements ou un sous-ensemble d'événements. Si le sous-ensemble est sélectionné, personnalisez la liste de sélection pour qu'elle corresponde aux événements d'alerte de votre choix.
4. Dans "Actions d'alerte", sélectionnez le type d'alerte dans le menu déroulant.
5. Saisissez les détails de l'action d'alerte. Le bouton "TEST" permet de créer une alerte test et d'exécuter cette action d'alerte (permet de vérifier si la messagerie électronique ou le protocole SNMP sont correctement configurés).
6. Vous pouvez cliquer sur l'icône d'ajout en regard de "Actions d'alerte" pour ajouter plusieurs actions d'alerte.
7. Cliquez sur "AJOUTER" dans la partie supérieure droite.

Rubriques connexes

- [Catégories d'alertes](#)
- [Envoi de messages SYSLOG](#)
- [Exécution d'un workflow](#)
- [Alertes avec seuil](#)
- [Reprise/suspension de feuilles de travail et d'ensembles de données](#)

▼ Ajout d'une action d'alerte (CLI)

1. Saisissez le contexte configuration alerts actions, puis la commande create.
2. Accédez à la propriété "category" en saisissant `get category = (unset)`.
3. Saisissez `set category=thresholds`.

4. Saisissez `set thresholdid=[id]`, où `[id]` correspond à l'identifiant créé automatiquement pour l'alerte avec seuil.
5. Saisissez `commit`.
6. Saisissez `list` pour déterminer le nom, y compris le numéro, de la nouvelle action d'alerte. Recherchez un seuil sans action et gestionnaire assignés.
7. Saisissez `select actions-[nombre]`, où `[nombre]` correspond au nombre identifié dans l'étape précédente.
8. Saisissez `action`, puis `get`.
9. Par défaut le type d'alerte est e-mail. S'il s'agit de ce que vous souhaitez, passez à l'étape suivante. Sinon, saisissez `set handler=[type]`, où `[type]` correspond à `snmptrap`, `syslog`, `resumedataset`, `suspenddataset`, `resumeworksheet`, `suspendworksheet` OU `executeworkflow`. Saisissez ensuite `get` pour afficher les arguments nécessaires. Seuls `snmptrap` et `syslog` ne disposent pas d'arguments.
10. Définissez chaque argument nécessaire. Par exemple, pour définir une ligne d'objet pour une alerte e-mail, saisissez `set subject=[objet]` où `[objet]` correspond à la ligne d'objet de l'e-mail souhaitée.
11. Exécutez la commande `show` pour vous assurer que tous les arguments ont été saisis.
12. Saisissez `commit`, puis `list`. Si nécessaire, corrigez tout argument maintenant.
13. Saisissez `done`, puis `done à nouveau`.

Rubriques connexes

- [Catégories d'alertes](#)
- [Envoi de messages SYSLOG](#)
- [Exécution d'un workflow](#)
- [Alertes avec seuil](#)
- [Reprise/suspension de feuilles de travail et d'ensembles de données](#)

Envoi d'alertes par e-mail (CLI)

Il est possible d'envoyer un e-mail contenant les détails de l'alerte. La configuration requiert une adresse électronique et une ligne d'objet de l'e-mail. L'exemple suivant présente une alerte avec

seuil par e-mail. Les détails de l'envoi des e-mails par l'appareil peuvent être configurés dans l'écran du service SMTP .

```
From aknobody@caji.com Mon Oct 13 15:24:47 2009
Date: Mon, 13 Oct 2009 15:24:21 +0000 (GMT)
From: Appliance on caji <noreply@caji.com>
Subject: High CPU on caji
To: admin@hostname.com
```

```
SUNW-MSG-ID: AK-8000-TT, TYPE: Alert, VER: 1, SEVERITY: Minor
EVENT-TIME: Mon Oct 13 15:24:12 2009
PLATFORM: i86pc, CSN: 0809QAU005, HOSTNAME: caji
SOURCE: svc:/appliance/kit/akd:default, REV: 1.0
EVENT-ID: 15a53214-c4e7-eae4-dae6-a652a51ea29b
DESC: cpu.utilization threshold of 90 is violated.
AUTO-RESPONSE: None.
IMPACT: The impact depends on what statistic is being monitored.
REC-ACTION: The suggested action depends on what statistic is being monitored.
```

```
SEE: https://192.168.2.80:215/#maintenance/alert=15a53214-c4e7-eae4-dae6-a652a51ea29b
```

Rubriques connexes

- [Catégories d'alertes](#)
- [Envoi de messages SYSLOG](#)
- [Exécution d'un workflow](#)
- [Alertes avec seuil](#)
- [Reprise/suspension de feuilles de travail et d'ensembles de données](#)

Envoi d'un déroutement SNMP (CLI)

Il est possible d'envoyer un déroutement SNMP contenant des détails d'alerte si une destination de déroutement SNMP est configurée dans le service SNMP et si ce service est en ligne.

L'exemple suivant illustre l'envoi d'un déroutement SNMP, tel qu'il est visible dans l'outil Net-SNMP `snmptrapd -P` :

```
# /usr/sfw/sbin/snmptrapd -P
2009-10-13 15:31:15 NET-SNMP version 5.0.9 Started.
2009-10-13 15:31:34 caji.com [192.168.2.80]:
    iso.3.6.1.2.1.1.3.0 = Timeticks: (2132104431) 246 days, 18:30:44.31
    iso.3.6.1.6.3.1.1.4.1.0 = OID: iso.3.6.1.4.1.42.2.225.1.3.0.1
    iso.3.6.1.4.1.42.2.225.1.2.1.2.36.55.99.102.48.97.99.100.52.45.51.48.
99.49.45.52.99.49.57.45.101.57.99.98.45.97.99.50.55.102.55.49.50.54.
98.55.57 = STRING: "7cf0acd4-30c1-4c19-e9cb-ac27f7126b79"
    iso.3.6.1.4.1.42.2.225.1.2.1.3.36.55.99.102.48.97.99.100.52.45.51.48.
99.49.45.52.99.49.57.45.101.57.99.98.45.97.99.50.55.102.55.49.50.54.
98.55.57 = STRING: "alert.ak.xmlrpc.threshold.violated"
```

```
iso.3.6.1.4.1.42.2.225.1.2.1.4.36.55.99.102.48.97.99.100.52.45.51.
48.99.49.45.52.99.49.57.45.101.57.99.98.45.97.99.50.55.102.55.49.50.
54.98.55.57 = STRING: "cpu.utilization threshold of 90 is violated."
```

Rubriques connexes

- [Catégories d'alertes](#)
- [Envoi de messages SYSLOG](#)
- [Exécution d'un workflow](#)
- [Alertes avec seuil](#)
- [Reprise/suspension de feuilles de travail et d'ensembles de données](#)

Catégories d'alertes

Les événements importants de l'appareil, y compris les pannes matérielles et logicielles, déclenchent des alertes. Ces alertes apparaissent dans le journal et peuvent aussi être configurées pour exécuter une action d'alerte.

Les alertes sont regroupées dans les catégories suivantes :

TABLERAU 40 Catégories d'alertes

Catégorie	Description
Cluster	Événements de cluster, notamment les échecs de liaison et les erreurs de pair
Personnalisé	Événements générés à partir de la configuration d'alertes personnalisées
Événements matériels	Initialisation de l'appareil et modification de la configuration matérielle
Pannes matérielles	Tout type de panne matérielle
Opérations NDMP	Événements de début et de fin liés à la sauvegarde et à la restauration NDMP TAR/DUMP. Ce groupe est disponible en tant que "NDMP : sauvegarde uniquement" et "NDMP : restauration uniquement".
Réseau	Événements et échecs liés au port réseau, à la liaison de données et à l'interface IP
Phone Home	Événements liés au chargement de l'offre groupée de support
Réplication distante	Événements et échecs d'envoi et de réception. Ce groupe est disponible en tant que "Réplication distante : source uniquement" et "Réplication distante : cible uniquement", respectivement réservé à aux événements source ou cible
Echecs du service	Événements de panne de service logiciel
Seuils	Alertes personnalisées basées sur les statistiques d'Analyse

Catégorie	Description
Pool ZFS	Événements du pool de stockage, y compris le nettoyage et l'activation

Envoi de messages SYSLOG

Lorsque le service Syslog est activé, il est possible d'envoyer un message Syslog contenant des détails d'alerte vers un ou plusieurs systèmes distants. Pour plus d'informations sur l'envoi de messages Syslog, reportez-vous à la section [Service de relais Syslog](#).

Exécution d'un workflow

Il est possible d'exécuter les workflows en tant qu'actions d'alerte. Pour permettre à un workflow de faire office d'action d'alerte, son action `alert` doit être définie sur `true`. Pour plus d'informations sur l'exécution d'un workflow, reportez-vous à la section ["Maintenance des workflows" à la page 591](#).

Alertes avec seuil

Ces alertes sont basées sur les statistiques d'Analyse. Les propriétés suivantes sont disponibles lors de la création d'alertes avec seuil.

TABLEAU 41 Propriétés des alertes avec seuil

Propriété	Description
Seuil	La statistique de seuil est issue de l'analyse et est autodescriptive (par exemple, "Protocole : opérations NFSv4 par seconde").
excède/est inférieur	Définit la manière dont la valeur de seuil est comparée aux statistiques actuelles.
Délai : pendant au moins	Durée pendant laquelle la valeur des statistiques actuelles dépasse le seuil ou est inférieure à celui-ci.
uniquement entre/uniquement pendant	Vous pouvez définir ces propriétés pour que le seuil ne soit envoyé qu'à certains moments de la journée, notamment pendant les heures de travail.
Renvoyer l'alerte toutes les... tant que le problème persiste.	Si elle est activée, cette propriété réexécute l'action d'alerte (telle que l'envoi d'un e-mail) à chaque intervalle défini en cas de dépassement du seuil.
Egalement envoyer alerte lorsque le problème est résolu pendant au moins...	Envoie une alerte de suivi en cas de dépassement du seuil durant au moins la durée définie pour l'intervalle.

La boîte de dialogue "Ajouter une alerte avec seuil" a été organisée pour être lue comme un paragraphe de description de l'alerte. Les textes par défaut sont :

CPU seuil : le pourcentage d'utilisation dépasse 95 pour cent.

Délai pendant 5 minutes au moins uniquement entre 0:00 et 0:00 pendant les jours ouvrés.

Renvoyer l'alerte toutes les 5 minutes tant que le problème persiste.

Egalement envoyer alerte lorsque le problème est résolu pendant au moins 5 minutes.

Rubriques connexes

- ["Configuration d'une alerte avec seuil \(BUI\)" du manuel *Guide de la fonction d'analyse des systèmes Oracle ZFS Storage Appliance, version OS8.6.0*](#)
- ["Configuration d'une alerte avec seuil \(CLI\)" du manuel *Guide de la fonction d'analyse des systèmes Oracle ZFS Storage Appliance, version OS8.6.0*](#)
- [Ajout d'une action d'alerte \(BUI\)](#)
- [Ajout d'une action d'alerte \(CLI\)](#)
- [Envoi d'alertes par e-mail \(CLI\)](#)
- [Envoi d'un déroutement SNMP \(CLI\)](#)

Reprise/suspension de feuilles de travail et d'ensembles de données de l'analyse

Les ensembles de données de l'analyse peut être repris ou suspendus. Cette action est particulièrement utile lors du suivi des problèmes de performance survenant sporadiquement et lorsqu'il n'est pas souhaitable d'activer ces ensembles de données 24 heures sur 24 et 7 jours sur 7.

Par exemple, supposons que vous ayez remarqué un pic d'activité de la CPU une à deux fois par semaine tandis qu'une autre analyse affichait une baisse associée des performances NFS. Vous activez des ensembles de données supplémentaires mais vous ne disposez pas de suffisamment d'informations pour identifier le problème. Si vous pouviez activer le NFS par ensembles de données hostname et filename, il serait certainement bien plus simple de déterminer la cause du problème. Toutefois, ces ensembles de données peuvent s'avérer plus lourds et le fait de les laisser activés en continu peut dégrader les performances. Les actions de reprise/d'interruption des ensembles de données peuvent alors s'avérer utiles. Une alerte avec seuil peut alors être configurée pour *repandre* le NFS suspendu par les ensembles de données hostname et filename, uniquement si un pic d'activité de la CPU est détecté. Vous pouvez configurer une deuxième alerte pour *suspendre* ces ensembles de données après un court intervalle de collecte de données. En cas de problème, vous collectez donc uniquement les données nécessaires et minimisez l'impact sur les performances durant la collecte de données.

Pour plus d'informations sur les ensembles de données, reportez-vous à la section ["A propos des ensembles de données d'analyse"](#) du manuel *Guide de la fonction d'analyse des systèmes Oracle ZFS Storage Appliance, version OS8.6.0*.

Ces actions consistent à reprendre ou suspendre une feuille de travail d'analyse, qui est susceptible de contenir de nombreux ensembles de données. Les raisons de cette action sont semblables à celles de la reprise/suspension d'ensembles de données. Pour plus d'informations, reportez-vous à la section ["Graphiques de feuille de travail" du manuel *Guide de la fonction d'analyse des systèmes Oracle ZFS Storage Appliance*, version OS8.6.0.](#)

Rubriques connexes

- ["Configuration d'une alerte avec seuil \(BUI\)" dans le *Guide de la fonction d'analyse des systèmes Oracle ZFS Storage Appliance*](#)
- ["Configuration d'une alerte avec seuil \(CLI\)" dans le *Guide de la fonction d'analyse des systèmes Oracle ZFS Storage Appliance*](#)
- ["Ajout d'une action d'alerte \(BUI\)" à la page 185](#)
- ["Ajout d'une action d'alerte \(CLI\)" à la page 185](#)
- ["Envoi d'alertes par e-mail \(CLI\)" à la page 186](#)
- ["Envoi d'un déroutement SNMP \(CLI\)" à la page 187](#)

Configuration d'appareils en cluster

L'appareil Oracle ZFS Storage Appliance prend en charge le clustering coopératif d'appareils. Cette stratégie s'inscrit dans une approche intégrée d'amélioration de la disponibilité et peut également inclure l'équilibrage de la charge sur le client, la planification sur site adaptée, la maintenance et la réparation proactive et réactive ainsi que la redondance matérielle sur un même dispositif, le tout intégré aux appareils de la série Oracle ZFS Storage Appliance.

Remarque - Si vous configurez le clustering pour deux nouveaux contrôleurs, suivez la procédure ["Configuration initiale de l'appareil" dans le *Guide d'installation des systèmes Oracle ZFS Storage Appliance*.](#)

Pour les tâches relatives au clustering d'appareils, reportez-vous aux sections :

- ["Connexion de câbles de cluster" dans le *Guide de câblage des systèmes Oracle ZFS Storage Appliance*](#)
- ["Vue de la BUI de configuration du cluster" à la page 192](#)
- ["Mise à niveau d'un appareil autonome vers une configuration clustérisée \(BUI\)" à la page 194](#)
- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Pour une meilleure compréhension du clustering d'appareils, reportez-vous aux sections :

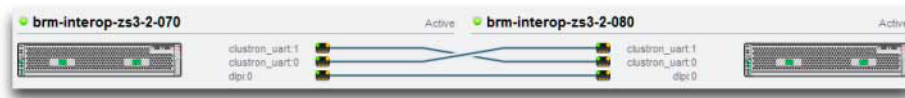
- ["Terminologie du cluster" à la page 199](#)
- ["Présentation du clustering" à la page 200](#)

- "Avantages et inconvénients des clusters" à la page 201
- "E/S d'interconnexion de cluster" à la page 203
- "Gestion des ressources du cluster" à la page 206
- "Reprise et rétablissement du cluster" à la page 209
- "Modifications de la configuration dans un environnement clustérisé" à la page 212
- "Considérations relatives au clustering pour le stockage" à la page 213
- "Considérations relatives au clustering pour la gestion réseau" à la page 215
- "Interfaces IP locales privées" à la page 217
- "Considérations relatives au clustering pour Infiniband" à la page 218
- "Prévention des états split-brain" à la page 220
- "Estimation et réduction de l'impact de la reprise" à la page 222

Vue de la BUI de configuration du cluster

La vue Configuration > Cluster offre une présentation graphique du statut de la carte de cluster, des états du nœud de contrôleur du cluster et de toutes les ressources.

FIGURE 14 Connexions du cluster



Remarque - Des câbles de cluster doivent être connectés entre les deux contrôleurs pour que les trois connexions apparaissent sous forme de lignes pleines dans la BUI. Pour plus de détails sur le câblage de clusters, reportez-vous à la section "[Connexion de câbles de cluster](#)" dans le [Guide de câblage des systèmes Oracle ZFS Storage Appliance](#).

L'interface contient les objets suivants :

- À gauche, une image miniature de chaque système précise le système dont l'interface d'administration est accessible. Chaque miniature est étiquetée avec le nom de l'appareil canonique et son état de cluster en cours (l'icône située au-dessus ainsi qu'une étiquette descriptive).
- Une miniature de chaque connexion de carte de cluster est mise à jour de façon dynamique avec le matériel : une ligne continue représente une liaison lorsque cette liaison est

connectée et active et la ligne disparaît si cette connexion est interrompue ou lors du redémarrage/de la réinitialisation de l'autre système.

- La liste des ressources PRIVATE et SINGLETON actuellement assignées à chaque système apparaît sous l'image miniature de chaque nœud de cluster, avec différents attributs des ressources.
- Pour chaque ressource, il est précisé l'appareil auquel la ressource est attribuée (à savoir, l'appareil qui fournira la ressource lorsque les deux sont dans l'état CLUSTERED). Lorsque l'appareil en cours se trouve dans l'état OWNER, le champ propriétaire s'affiche sous forme de menu contextuel qu'il est possible de modifier et de valider en cliquant sur Appliquer.
- Pour chaque ressource, une icône de verrou  indique si la ressource est privée ou non. Lorsque l'appareil est à l'état OWNER ou CLUSTERED, il est possible de verrouiller une ressource (définie sur PRIVATE) ou de la déverrouiller (définie sur SINGLETON) en cliquant sur l'icône de verrou , puis sur Appliquer. Notez que les ressources PRIVATE appartenant au pair distant ne figurer dans aucune liste de ressources.

La BUI contient les boutons suivants :

TABLEAU 42 Boutons de l'interface cluster

Bouton	Description
Configurer	Si le cluster n'est pas encore configuré, exécutez la tâche de configuration guidée du cluster, puis revenez à l'écran actuel.
Annuler config	Mettre à jour un nœud en vue d'un fonctionnement autonome en annulant la configuration du cluster.
Appliquer	Si des modifications de ressource sont en attente (lignes surlignées en jaune), valider ces modifications dans le cluster.
Rétablir	Si des modifications de ressource sont en attente (lignes surlignées en jaune), rétablir ces modifications et afficher la configuration de cluster en cours.
Rétablissement	Si l'appareil actuel (à gauche) est le propriétaire (OWNER), restaurer les ressources possédées par l'autre appareil sur ce dernier en laissant les deux nœuds dans l'état CLUSTERED (actif/actif).
Reprise	Si l'appareil actuel (à gauche) est CLUSTERED ou STRIPPED, forcer la réinitialisation de l'autre appareil puis à prendre le contrôle de ses ressources, en faisant de l'appareil en cours le propriétaire (OWNER)

Rubriques connexes

- ["Exécution de la configuration initiale \(BUI\)" dans le *Guide d'installation des systèmes Oracle ZFS Storage Appliance*](#)
- ["Mise à niveau d'un appareil autonome vers une configuration clustérisée \(BUI\)" à la page 194](#)

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

▼ Mise à niveau d'un appareil autonome vers une configuration clustérisée (BUI)

La procédure ci-dessous permet de mettre à niveau un appareil autonome vers une configuration clustérisée.

Remarque - Il est fortement recommandé d'utiliser la BUI pour configurer des contrôleurs en cluster.

Avant de commencer

Vérifiez les points suivants :

- Le deuxième contrôleur est un nouveau contrôleur ou un contrôleur dont les paramètres d'usine par défaut ont été restaurés. Reportez-vous à la section ["Réinitialisation des paramètres d'usine"](#) dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.
- Les deux contrôleurs doivent être du même modèle. Notez que la série 7420 (avec CPU 2 GHz ou 2,40 GHz) est basée sur la même plate-forme et peut être mise en cluster avec le modèle 7420 (avec CPU 1,86 GHz ou 2,00 GHz).
- L'appareil autonome est mis sous tension. Il n'est pas nécessaire de mettre l'appareil autonome hors tension lors de cette procédure.

1. Connectez les câbles de cluster entre l'appareil autonome et le deuxième contrôleur.

Pour plus de détails sur le câblage de clusters, reportez-vous à la section ["Connexion de câbles de cluster"](#) dans le *Guide de câblage des systèmes Oracle ZFS Storage Appliance*.

2. Sur le deuxième contrôleur, branchez les câbles d'alimentation aux unités d'alimentation 0 et 1. Connectez ensuite chaque câble à la source d'alimentation externe.

Le deuxième contrôleur se met automatiquement sous tension.

3. Connectez le deuxième contrôleur aux étagères de disques.

Consultez la documentation fournie avec votre appareil ou reportez-vous à la section ["Initiation au câblage"](#) dans le *Guide de câblage des systèmes Oracle ZFS Storage Appliance*.

4. Sur le contrôleur autonome, accédez à Configuration > Cluster.

5. Confirmez que les liaisons de communication entre les deux contrôleurs sont connectées et actives.

Si trois lignes pleines ne s'affichent pas, assurez-vous que les trois câbles de cluster sont bien connectés et correctement branchés dans leurs connecteurs.

6. Cliquez sur **CONFIGURER**.
7. Saisissez le nom d'hôte du deuxième contrôleur et le même mot de passe root que celui défini sur le premier contrôleur.

Remarque - L'exécution d'une configuration de cluster initiale peut prendre plusieurs minutes.

8. Sur le contrôleur autonome, accédez à **Configuration > Cluster** et cliquez sur l'icône de verrou  de l'interface de gestion.
Le verrouillage de l'interface de gestion sur le contrôleur permet d'empêcher un transfert des ressources en cas de rétablissement.
9. Configurez l'interface de gestion pour le deuxième contrôleur à partir du contrôleur autonome.
 - a. Accédez à **Configuration > Réseau** et cliquez sur l'icône d'ajout  en regard de l'option **Interfaces**.
 - b. Saisissez un nom pour l'interface de gestion et cochez les cases **Activer l'interface** et **Autoriser l'administration**.
 - c. Sélectionnez une adresse IP et cliquez sur **APPLIQUER**.
10. Accédez à **Configuration > Cluster** et cliquez sur **RETABLISSEMENT** pour faire passer le cluster en mode **Actif : Actif**.
Les deux contrôleurs sont maintenant configurés en tant que pairs de cluster.
11. Sur le deuxième contrôleur, accédez à **Configuration > Cluster** et cliquez sur l'icône de verrou  de l'interface de gestion.

Rubriques connexes

- ["Considérations relatives au clustering pour le stockage" à la page 213](#)
- ["Vue de la BUI de configuration du cluster" à la page 192](#)

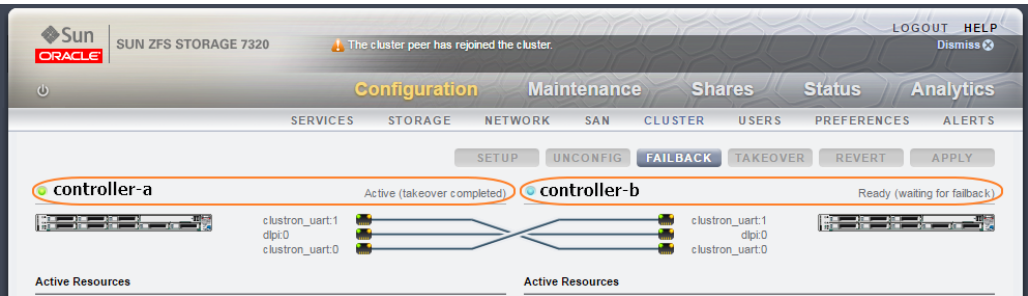
▼ Arrêt de la configuration clustérisée (BUI)

La procédure ci-dessous permet d'arrêter une configuration clustérisée.

1. A partir de l'un des contrôleurs pairs, accédez à Configuration > Cluster.

2. Déterminez l'état des deux contrôleurs.

Dans la figure suivante, le contrôleur actif est controller-a, tandis que le contrôleur de secours est controller-b.



Le tableau suivant permet de déterminer l'état de chaque contrôleur.

controller-a	controller-b	Conditions
 Actif	 Actif	Les deux contrôleurs s'exécutent dans une condition clustérisée normale.
 Actif (reprise terminée)	 Prêt (en attente du rétablissement)	controller-a est le propriétaire de toutes les ressources et est le contrôleur actif. controller-b est en mode veille et ne contient aucune ressource. Pour limiter le nombre de déplacements d'un pool, arrêtez d'abord le contrôleur de secours.
 Actif (reprise terminée)	 Retour au cluster...	controller-b est en cours de réinitialisation et controller-a contient toutes les ressources.
 Actif (reprise terminée)	Inconnu (déconnecté ou en cours de redémarrage)	controller-b est hors tension ou en cours de réinitialisation, toutes ses liaisons d'interconnexion sont interrompues ou le clustering n'a pas encore été configuré.

3. Connectez-vous à la BUI du contrôleur B et cliquez sur l'icône d'alimentation  sur le côté gauche sous le cadre masthead.

Remarque - Pour limiter le nombre de déplacements d'un pool, arrêtez d'abord le contrôleur de secours.

4. A partir de la BUI du contrôleur A, accédez à Configuration > Cluster pour confirmer que le contrôleur B est hors tension et que l'état du cluster est Inconnu (déconnecté ou en cours de redémarrage).
5. A partir de la BUI du contrôleur A, cliquez sur l'icône d'alimentation  sur le côté gauche sous le cadre masthead.
6. (Facultatif) Pour vérifier que les deux contrôleurs sont hors tension, connectez-vous à Oracle ILOM et saisissez :

```
->show /SYS power_state
```

Pour plus d'informations sur l'accès à ILOM, reportez-vous à la section "[Connexion à distance à Oracle ILOM à l'aide d'une interface de ligne de commande \(CLI\)](#)" dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*..

7. Mettez hors tension les étagères de disques.
 - a. Placez les interrupteurs Marche/Arrêt sur la position « O » (Arrêt).
 - b. Déconnectez les cordons d'alimentation de la source d'alimentation externe de l'armoire.

Remarque - Il est nécessaire de débrancher tous les cordons d'alimentation pour retirer toute source d'alimentation de l'étagère de disques.

Pour plus d'informations, reportez-vous à la section "[Powering Off a Disk Shelf](#)" dans *Oracle ZFS Storage Appliance Installation Guide*.

▼ Arrêt de la configuration clustérisée (CLI)

La procédure ci-dessous permet d'arrêter une configuration clustérisée.

Remarque - Dans cette procédure, les contrôleurs clustérisés sont appelés controller-a et controller-b.

1. Vérifiez l'état du cluster de chaque contrôleur à l'aide des commandes suivantes :

Dans l'exemple suivant, controller-a est le propriétaire et se trouve à l'état Actif. Son pair, controller-b, est le contrôleur de secours et se trouve à l'état Stripped.

```
controller-a:>configuration cluster  
controller-a:configuration cluster> show
```

```
state = AKCS_OWNER
description = Active (takeover completed)
peer_asn = 365ed33c-3b9d-c533-9349-8014e9da0408
peer_hostname = controller-b
peer_state = AKCS_STRIPPED
peer_description = Ready (waiting for failback)
```

2. Utilisez le tableau suivant pour vérifier l'état de chaque contrôleur.

controller-a	controller-b	Conditions
AKCS_CLUSTERED	AKCS_CLUSTERED	Les deux contrôleurs s'exécutent dans une condition clustérisée normale.
AKCS_OWNER	AKCS_STRIPPED	controller-a est le propriétaire de toutes les ressources et est le contrôleur actif. controller-b est en mode veille et ne contient aucune ressource. Pour limiter le nombre de déplacements d'un pool, arrêtez d'abord le contrôleur STRIPPED.
AKCS_OWNER	réinitialisation	controller-b est en cours de réinitialisation et controller-a contient toutes les ressources.
AKCS_OWNER	inconnu	controller-b est hors tension ou en cours de réinitialisation, toutes ses liaisons d'interconnexion sont interrompues ou le clustering n'a pas encore été configuré.

Remarque - Si l'état de chaque contrôleur n'est **pas** d'accord, le cluster peut rencontrer un problème. Contactez les services de support Oracle avant de lancer la procédure.

3. Arrêtez le contrôleur controller-b à l'aide des commandes suivantes :

```
controller-b:configuration cluster> cd /
controller-b:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N)Y
```

Remarque - Si les deux contrôleurs sont à l'état AKCS_CLUSTERED, une reprise du contrôleur encore fonctionnel démarre automatiquement.

4. A partir du contrôleur controller-a, utilisez la commande show pour vérifier que controller-b a été mis hors tension et se trouve à l'état OWNER/unknown.

```
controller-a:configuration cluster> show
state = AKCS_OWNER
description = Active (takeover completed)
```

```
peer_asn = 365ed33c-3b9d-c533-9349-8014e9da0408
peer_hostname = controller-b
peer_state = OWNER/unknown
peer_description =
```

5. Arrêtez le contrôleur controller-a à l'aide des commandes suivantes :

```
controller-a:configuration cluster> cd /
controller-a:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N) Y
```

6. (Facultatif) Pour vérifier que les deux contrôleurs sont hors tension, connectez-vous à Oracle ILOM et saisissez :

```
->show /SYS power_state
```

Pour plus d'informations sur l'accès à ILOM, reportez-vous à la section "[Connexion à distance à Oracle ILOM à l'aide d'une interface de ligne de commande \(CLI\)](#)" dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*..

7. Mettez hors tension les étagères de disques.

- a. **Placez les interrupteurs Marche/Arrêt sur la position « O » (Arrêt).**
- b. **Déconnectez les cordons d'alimentation de la source d'alimentation externe de l'armoire.**

Remarque - Il est nécessaire de débrancher tous les cordons d'alimentation pour retirer toute source d'alimentation de l'étagère de disques.

Pour plus d'informations, reportez-vous à la section "[Powering Off a Disk Shelf](#)" dans *Oracle ZFS Storage Appliance Installation Guide*.

Rubriques connexes

- "[Présentation du clustering](#)" à la page 200
- "[Terminologie du cluster](#)" à la page 199
- "[Gestion des ressources du cluster](#)" à la page 206
- "[Reprise et rétablissement du cluster](#)" à la page 209
- "[Modifications de la configuration dans un environnement clustérisé](#)" à la page 212

Terminologie du cluster

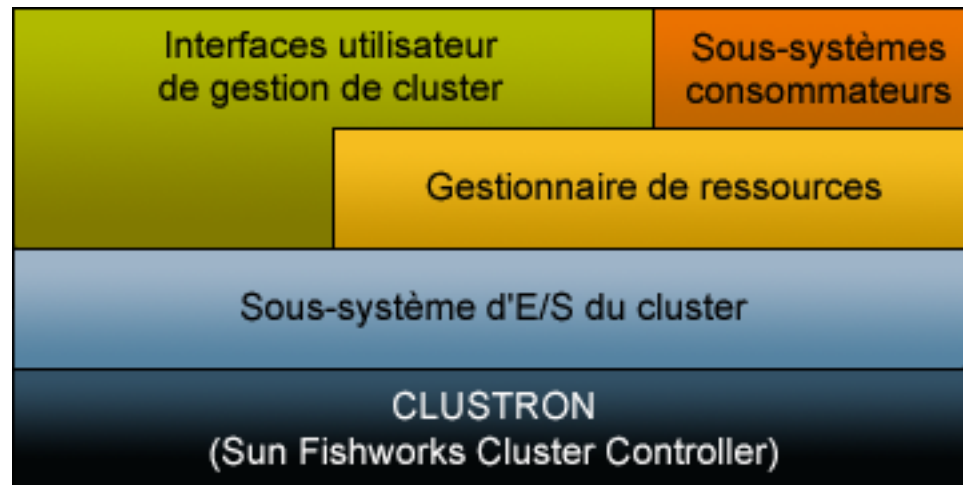
Les termes définis dans cette section sont utilisés dans l'ensemble du document. Dans la plupart des cas, ils sont expliqués plus en détail et avec plus de contexte avec les concepts plus vastes

impliqués. Les états et les types de ressource du cluster sont décrits dans la section suivante. Le cas échéant, reportez-vous à cette section en guise de référence.

- **Exportation** : processus permettant de rendre une ressource inactive sur un contrôleur donné
- **Rétablissement** : passage de l'état AKCS_OWNER à l'état AKCS_CLUSTERED, lors duquel les ressources étrangères (assignées au pair) sont exportées puis importées par le pair
- **Importation** : processus permettant de rendre une ressource active sur un contrôleur donné
- **Pair** : l'autre appareil dans un cluster
- **Rejoindre** : récupérer et resynchroniser la carte des ressources à partir du pair
- **Ressource** : objet physique ou virtuel présent, et probablement actif, sur l'un des contrôleurs ou les deux
- **Reprise** : processus de passage de l'état AKCS_CLUSTERED ou AKCS_STRIPPED à l'état AKCS_OWNER, dans lequel toutes les ressources sont importées

Présentation du clustering

Le sous-système de clustering intégré à la série contient trois blocs fonctionnels (voir la figure suivante). Le sous-système d'E/S du cluster et le périphérique matériel fournissent un transport pour la communication entre les contrôleurs d'un même cluster tout en assurant la surveillance de l'état du pair. Ce transport est utilisé par le gestionnaire de ressources, ce qui permet aux fournisseurs du service de données et aux autres sous-systèmes de gestion d'interagir avec le système de clustering. Enfin, les interfaces utilisateur de gestion du cluster fournissent les tâches de configuration, l'allocation et l'assignation des ressources, la surveillance et les opérations de reprise et de rétablissement. Chacun de ces blocs fonctionnels est décrit en détails dans les sections suivantes.

FIGURE 15 Sous-système de clustering

Annulation de la configuration du clustering

L'annulation de la configuration du clustering est une opération destructive qui permet de restaurer la configuration usine par défaut des contrôleurs du stockage en cluster et de réaffecter la propriété de toutes les ressources vers le pair encore fonctionnel. Il existe deux motifs d'annulation de la configuration du clustering :

- Vous ne souhaitez plus utiliser le clustering, mais configurer deux appareils de stockage indépendants à la place.
- Vous remplacez un contrôleur de stockage défaillant par du matériel neuf ou un contrôleur de stockage équipé du logiciel de l'appareil sorti de l'usine (généralement ce remplacement est effectué par votre fournisseur de service).

Contactez le support Oracle en raison du risque de perte de données lors de l'annulation de la configuration du clustering.

Avantages et inconvénients des clusters

Il est primordial de comprendre la portée de l'implémentation du clustering de la série Oracle ZFS Storage Appliance. Dans le secteur, le terme "cluster" fait référence à de nombreuses technologies et à des buts très divers. Dans la présente documentation, il fait référence à un métasystème composé de deux contrôleurs d'appareil et d'un système de stockage partagé

permettant une meilleure disponibilité au cas où l'un des contrôleurs subirait des pannes matérielles ou logicielles. Un cluster contient exactement deux appareils ou contrôleurs de stockage, ci-après dénommés *contrôleurs* pour des raisons de concision. Il est possible d'attribuer à chaque contrôleur un ensemble de stockage, une mise en réseau et d'autres ressources issues de l'ensemble disponible sur le cluster qui permettent la construction de l'une des deux topologies majeures. De nombreuses personnes utilisent le terme *actif-actif* pour décrire un cluster contenant aux moins deux pools de stockage, dont l'un est attribué à chaque contrôleur avec les ressources réseau utilisées par les clients pour atteindre les données stockées dans ce pool, et *actif-passif* pour désigner le pool de stockage unique auquel le contrôleur désigné comme *actif* ainsi que ses interfaces réseau associées sont attribuées. Les deux topologies sont prises en charge par le système Oracle ZFS Storage Appliance. La distinction entre ces topologies est artificielle. Il n'existe aucune différence logicielle ou matérielle entre les deux et vous pouvez passer de l'une à l'autre quand vous le souhaitez en ajoutant ou en détruisant un pool de stockage. Dans les deux cas, si un contrôleur échoue, l'autre (son *pair*) prend le contrôle de toutes les ressources connues et fournit les services associés à celles-ci.

Pour pallier aux heures ou aux jours d'inactivité requis pendant la réparation du contrôleur, le clustering fournit un pair qui distribue le service durant la réparation ou le remplacement. En outre, les clusters prennent en charge la mise à niveau non simultanée de logiciels qui permet de réduire les interruptions d'activité associées à la migration vers de nouveaux logiciels. Certaines technologies de clustering sont dotées de fonctionnalités supplémentaires allant au-delà l'amélioration de la disponibilité. Mais le sous-système de clustering de la série Oracle ZFS Storage Appliance n'a pas été conçu pour cela. En particulier, il ne permet pas l'équilibrage de charge sur plusieurs contrôleurs, n'améliore pas la disponibilité en cas de panne de stockage, n'offre pas aux clients l'espace de noms du système de fichiers unifié entre plusieurs appareils ni ne divise la responsabilité du service au sein d'une zone géographique étendue en cas de récupération après sinistre. Ces fonctions sont également hors de portée du présent document. Néanmoins, Oracle ZFS Storage Appliance et les protocoles de données qu'il fournit prennent en charge de nombreuses fonctions et stratégies permettant d'améliorer la disponibilité :

- La réplication de données, qui peut être utilisée pour la récupération après sinistre depuis un ou plusieurs sites éloignés géographiquement.
- La mise en miroir des données côté client peut être effectuée à l'aide des LUN iSCSI fournies par plusieurs serveurs de stockage localisés de façon arbitraire.
- L'équilibrage de charge est intégré au protocole NFS et peut être fourni pour certains autres protocoles via un matériel ou un logiciel externe (s'applique aux données en lecture seule).
- Les composants matériels redondants incluent les alimentations, les périphériques réseau et les contrôleurs de stockage.
- Le logiciel de gestion des pannes permet d'identifier les composants défectueux, de les supprimer du service et de guider les techniciens dans la réparation ou le remplacement par du matériel correct.
- La redondance de la topologie Fabric réseau, permise par les fonctionnalités LACP et IPMP.
- Les périphériques de stockage redondants (RAID)

Des informations supplémentaires relatives aux autres fonctions de disponibilité sont disponibles dans les sections appropriées du présent document.

Avant de vous décider entre une configuration en cluster ou autonome de la série Oracle ZFS Storage Appliance, il est important de peser le pour et le contre. Dans le secteur des technologies de l'information, il est courant de considérer le clustering comme un choix d'architecture automatique, bien que cette approche reflète une vision idéalisée des risques et des avantages du clustering promulguée par certains vendeurs du secteur. En plus de l'avancée incontestable, des coûts de matériel et de support induits associés au marché du second contrôleur, le clustering présente également des risques techniques et opérationnels supplémentaires. Certains de ces risques peuvent être atténués en s'assurant que la totalité du personnel est parfaitement formé aux opérations du cluster, les autres étant intrinsèques au fonctionnement en cluster. Les risques sont les suivants :

- Intolérance potentielle de l'application aux comportements dépendant du protocole durant la reprise
- Possibilité que le logiciel de cluster tombe lui-même en panne ou qu'il induise une panne dans un autre sous-système qui n'aurait pas eu lieu dans une opération autonome
- Plus grande complexité de gestion et plus forte probabilité que des erreurs opérateur surviennent lors de l'exécution de tâches de gestion
- Possibilité que plusieurs erreurs ou une erreur opérateur grave induise une perte ou une altération des données qui n'aurait pas lieu dans une configuration autonome
- Plus grande difficulté de récupération à partir des états logiciels et/ou matériels non anticipés.

Ces coûts et ces risques sont fondamentaux et s'appliquent d'une manière ou d'une autre à tous les produits clustérisés ou compatibles avec le clustering du marché (y compris la série Oracle ZFS Storage Appliance) et ne peuvent pas être entièrement éliminés ni limités. Les architectes de stockage doivent peser le pour et le contre par rapport à l'avantage principale du clustering : l'opportunité de transformer les heures ou jours d'indisponibilité en minutes, ou moins, dans le rare cas d'une panne matérielle ou logicielle catastrophique. Le fait que l'analyse coût/bénéfice favorise ou non l'utilisation du clustering dans un déploiement de la série Oracle ZFS Storage Appliance dépend de facteurs locaux tels que les termes du contrat de niveau de service, le personnel de support disponible et ses qualifications ainsi que les contraintes budgétaires, l'anticipation des différentes pannes potentielles et les autres stratégies d'amélioration de la disponibilité. Ces facteurs dépendent étroitement du site, de l'application et des activités et doivent être évalués au cas par cas. La compréhension de la documentation dans le reste de cette section vous aidera à prendre les bonnes décisions lors de la conception et l'implémentation de votre infrastructure de stockage unifié.

Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

E/S d'interconnexion de cluster

Toute la communication entre les contrôleurs consiste en la transmission d'un ou de plusieurs messages via l'une des trois liaisons d'E/S de cluster fournies par le matériel CLUSTRON (voir illustration ci-dessous). Ce périphérique permet deux liaisons série bas débit et une

liaison Ethernet. L'utilisation des liaisons série offre une plus grande fiabilité car les liaisons Ethernet peuvent ne pas être traitées suffisamment vite par un système supportant une charge extrêmement lourde. La détection erronée de pannes et la reprise non souhaitée sont les pires manières pour un système clustérisé de répondre à une charge. Durant la reprise, les requêtes ne sont pas traitées et sont placées dans une file d'attente par les clients, ce qui entraîne une multitude de requêtes différées en plus d'une charge déjà lourde. Les liaisons série utilisées par les appareils de la série Oracle ZFS Storage Appliance ne sont pas sujets à ce type de panne. La liaison Ethernet offre de meilleures performances de transport pour les messages qui n'ont pas trait aux pulsations, notamment la synchronisation de réunion, et fournit un signal d'activité de sauvegarde.

Les trois liaisons sont formées à l'aide de câbles droits ordinaires EIA/TIA-568B (8 fils, Gigabit Ethernet). Pour autoriser l'utilisation de câbles droits entre deux contrôleurs identiques, vous devez utiliser les câbles pour connecter des sockets opposés sur les deux connecteurs, comme indiqué dans la section "Connexion de câbles de cluster" du *Guide de câblage des systèmes Oracle ZFS Storage Appliance*.

FIGURE 16 Ports d'E/S des clusters de contrôleurs ZS4-4, ZS3-4 et 7x20

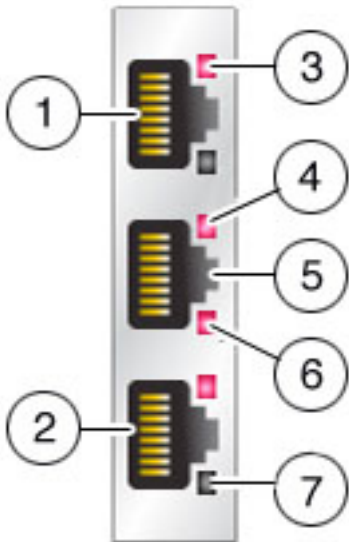


TABLEAU 43 Ports d'E/S des clusters de contrôleurs ZS4-4, ZS3-4 et 7x20

Légende de la figure			
1 Numéro de série 1	2 Numéro de série 0	3 DEL d'activité série	4 DEL d'activité Ethernet
5 Ethernet	6 DEL d'état Ethernet	7 DEL d'état série	

FIGURE 17 Ports d'E/S du cluster de contrôleurs ZS3-2



TABLEAU 44 Ports d'E/S du cluster de contrôleurs ZS3-2

Légende de la figure			
1 Numéro de série 0	2 DEL d'activité série	3 DEL d'état série	4 Ethernet
5 Numéro de série 1	6 DEL d'état Ethernet	7 DEL d'activité Ethernet	

Les contrôleurs clustérisés ne communiquent jamais via un réseau de service ou d'administration. Leurs interconnexions ont lieu sur un réseau privé sécurisé. Les messages sont divisés en deux catégories générales : les pulsations régulières utilisées pour détecter la panne d'un contrôleur distant et le trafic de haut niveau associé au gestionnaire de ressources ainsi qu'au sous-système de gestion du cluster. Les pulsations sont envoyées et attendues sur les trois liaisons. Elles sont transmises en continu à intervalles fixes et ne sont jamais reconnues ni retransmises car elles sont toutes identiques et ne contiennent pas d'informations spécifiques. D'autres trafics peuvent être envoyés par l'intermédiaire d'une autre liaison quelconque, il s'agit généralement de la plus rapide disponible au moment de la transmission. Ce trafic est reconnu, vérifié puis retransmis si nécessaire pour garantir un transport fiable aux logiciels de niveau supérieur.

Quel que soit son type ou son origine, chaque message est envoyé en tant que paquet unique de 128 octets et contient une charge utile de données comprise entre 1 et 68 octets et une valeur de hachage de vérification de 20 octets visant à garantir l'intégrité des données. Les liaisons série s'exécutent à 115 200 bps avec 9 octets de données et un seul bit de démarrage et d'arrêt. La liaison Ethernet s'exécute à 1 Gbps. Par conséquent, la latence de message effective sur les liaisons série est d'environ 12,2 ms. La latence Ethernet varie énormément. Tandis que les

temps d'attente standard s'expriment en microsecondes, les temps d'attente effectifs vers le logiciel de gestion de l'appareil peuvent être plus longs en raison de la charge du système.

Normalement, les pulsations sont envoyées par chaque contrôleur sur les trois liaisons d'E/S du cluster à 50 ms d'intervalle. L'impossibilité de réceptionner un message est considérée comme un échec de liaison après 200 ms (liaisons série) ou 500 ms (liaisons Ethernet). Si les trois liens échouent, le pair est considéré en échec ; l'arbitrage de la reprise est alors effectué. En cas de panique, le contrôleur concerné transmet un seul message de notification à chacune des liaisons série ; son pair effectue automatiquement la reprise indépendamment de l'état de ces autres liaisons. Compte tenu de ces caractéristiques, le sous-système de clustering peut normalement détecter l'échec de son pair dans un délai de :

- 550 ms si le pair a arrêté de répondre ou n'est plus alimenté ;
- 30 ms si le pair a rencontré une erreur logicielle fatale ayant déclenché une panique du système d'exploitation.

Toutes les valeurs décrites dans cette section sont fixes. En tant qu'appareil, le système de stockage Oracle ZFS Storage Appliance ne permet pas (ni ne requiert) de régler ces paramètres. Elles sont considérées comme des détails d'implémentation et sont fournies à titre informatif uniquement. Elles peuvent être changées à tout moment et sans préavis.

Remarque - Pour éviter l'altération des données après le déplacement physique d'un cluster, vérifiez que tout le câblage du cluster est correctement installé dans le nouvel emplacement. Pour plus d'informations, reportez-vous à la section "[Prévention des états split-brain](#)" à la page 220.

Rubriques connexes

- "[Arrêt de la configuration clustérisée \(CLI\)](#)" à la page 197

Gestion des ressources du cluster

Le gestionnaire de ressources veille à la solidité de l'installation des interfaces réseau, vérifie que les pools de stockage adaptés sont actifs et s'assure de la synchronisation des nombreux paramètres de configuration avec les deux contrôleurs clustérisés. La plupart des activités de ce sous-système sont invisibles pour les administrateurs ; néanmoins, un aspect important est exposé. Les ressources sont classées en plusieurs types qui régissent le moment où elles sont importées et décident de leur importation ou non (activation). Notez que la définition d'activation varie d'une classe de ressources à une autre. Par exemple, une interface réseau appartient à la classe net et devient active lorsque l'interface s'affiche.

Les trois plus importants types de ressources sont singleton, privé et réplique.

- **Ressources réplique** - Les répliques sont les plus simples : elles ne sont jamais exposées aux administrateurs et n'apparaissent pas dans l'écran de configuration du cluster. Les répliques existent toujours et sont toujours actives sur les deux contrôleurs. De manière

générale, elles agissent simplement comme des conteneurs de propriétés de service à synchroniser entre les deux contrôleurs.

- **Ressources singleton** - De même que les répliques, les ressources singleton permettent la synchronisation de l'état. Toutefois, les singletons sont toujours actifs sur un contrôleur exactement. Les administrateurs peuvent choisir le contrôleur sur lequel activer le singleton de manière générale. En cas d'échec sur ce contrôleur, son pair importe le singleton. Les singletons sont la clé des caractéristiques de disponibilité du clustering ; ils représentent les ressources que l'on imagine déplacer d'un contrôleur défaillant vers son pair encore fonctionnel et incluent les interfaces réseau et les pools de stockage. Etant donné qu'une interface réseau est un ensemble d'adresses IP utilisées par les clients pour rechercher un ensemble connu de services de stockage, il est essentiel que chaque interface soit assignée au même contrôleur que celui que les clients du pool de stockage s'attendent à voir en accédant aux adresses de l'interface. Dans l'illustration 4, toutes les adresses associées à l'interface PrimaryA sont toujours fournies par le contrôleur ayant importé pool-0, tandis que les adresses associées à PrimaryB sont toujours fournies par le même contrôleur que pool-1.
- **Ressources privées** - Les ressources privées sont uniquement connues par le contrôleur auquel elles sont assignées et ne sont jamais reprises en cas de panne. Ce type est généralement utile pour les interfaces réseau (voir la discussion suivante relative aux cas d'utilisation spécifiques).

FIGURE 18 Exemple de clustering ZS3-2



D'autres types de ressources existent : il s'agit de détails d'implémentation qui ne sont pas exposés aux administrateurs. On trouve par exemple le type symbiote qui permet à une ressource d'en suivre une autre en cas d'importation et d'exportation. Ce type de ressource est le plus souvent utilisé pour représenter les disques et les périphériques flash dans le pool de stockage. Ces ressources se présentent sous la forme d'ensembles de disques et doivent toujours être importées avant le pool ZFS qu'elles contiennent. Chaque ensemble de disques est composé

pour moitié de disques dans un boîtier de stockage externe. Un système de stockage clustérisé peut posséder un nombre illimité d'ensembles de disques joints (en fonction de la prise en charge matérielle) et chaque pool ZFS est formé à partir des périphériques de stockage dans un ou plusieurs ensembles de disques. Etant donné que les ensembles de disques peuvent contenir des périphériques ATA, ils doivent être importés et exportés de manière explicite afin d'éviter certains comportements liés à l'affiliation typiques des périphériques ATA utilisés dans des environnements à chemins d'accès multiples. Représenter ces disques sous forme de ressources est une manière simple d'effectuer ces activités au bon moment. Lorsqu'un administrateur définit ou modifie la propriété d'un pool de stockage, l'assignation de la propriété des ensembles de disques associés est modifiée simultanément de façon transparente. De même que tous les symbiotes, les ressources ensembles de disques n'apparaissent pas dans l'interface utilisateur de configuration du cluster.

TABLEAU 45 Gestion des ressources du cluster

Ressource	Icône	Omniprésent	Reprise en cas de panne
SINGLETON		Non	Oui
REPLIQUE	Aucune	Oui	N/D
PRIVE		Non	Non
SYMBIOTE	Aucune	Identique au type parent	Identique au type parent

Lorsqu'une nouvelle ressource est créée, elle est initialement assignée au contrôleur sur lequel elle est créée. Il est impossible de modifier cette propriété tant que le contrôleur est à l'état AKCS_OWNER. Il est donc nécessaire soit de créer des ressources sur le contrôleur qui devrait les posséder, soit d'assurer le relais avant de modifier la propriété des ressources. Il est généralement possible de détruire des ressources sur tous les contrôleurs, à l'exception des pools de stockage exportés. Les meilleurs résultats sont généralement obtenus en détruisant les ressources sur le contrôleur qui est alors chargé de les contrôler, indépendamment du contrôleur auquel elles appartiennent.

La plupart des paramètres de configuration, notamment les propriétés du service, les utilisateurs, les rôles, les règles de mappage des identités, les règles autohome SMB et les définitions d'initiateur iSCSI sont répliqués automatiquement sur les deux contrôleurs. Il n'est donc jamais nécessaire de configurer ces paramètres sur les deux contrôleurs, quel que soit l'état du cluster. Si un appareil est hors service durant la modification de la configuration, cette dernière est répliquée lorsque l'autre appareil rejoint le cluster à la prochaine initialisation, avant de fournir tout service. Il existe quelques exceptions :

- Les définitions et les options des partages et des LUN peuvent uniquement être définies sur le contrôleur qui contrôle le pool sous-jacent, indépendamment du contrôleur auquel le pool est normalement affecté.
- La configuration du service "Identity" (c'est-à-dire le nom et l'emplacement de l'appareil) n'est pas répliquée.
- Les noms donnés au châssis sont uniquement visibles sur le contrôleur auquel ils ont été assignés.

- Chaque route réseau est liée à une interface spécifique. Si chaque contrôleur est associé à une interface contenant une adresse dans un sous-réseau particulier et que ce dernier contient un routeur vers lequel les appareils sont censés diriger le trafic, vous devez impérativement créer une route pour chaque interface, même lorsque l'adresse de passerelle est utilisée. Ainsi, chaque route peut devenir active individuellement lorsque le contrôle des ressources réseau sous-jacentes bascule d'un contrôleur à un autre. Pour plus d'informations, reportez-vous à la section "[Considérations relatives au clustering pour la gestion réseau](#)" à la page 215.
- Les clés d'hôte SSH ne sont pas répliquées et ne sont jamais partagées. Par conséquent, si aucune interface d'administration privée n'a été configurée, des incohérences de clé sont à prévoir lorsque vous tentez de vous connecter à la CLI à l'aide d'une adresse affectée à un nœud défaillant. Les mêmes limitations s'appliquent aux certificats SSL utilisés pour accéder à la BUI.

D'après le modèle de base, la configuration commune est répliquée de façon transparente et les administrateurs attribuent un ensemble de ressources à chaque contrôleur de l'appareil. Ces affectations de ressources forment à leur tour la liaison des adresses réseau aux ressources de stockage que les clients s'attendent à voir. Quel que soit l'appareil qui contrôle l'ensemble des ressources, les clients peuvent accéder au stockage dont ils ont besoin sur les emplacements réseau auxquels ils s'attendent.

Rubriques connexes

- "[Arrêt de la configuration clustérisée \(CLI\)](#)" à la page 197

Reprise et rétablissement du cluster

Les nœuds de contrôleur clustérisés se trouvent dans l'un des petits ensembles d'états à un moment donné :

TABLEAU 46 Etats du cluster

Etat	Icône	Expression de la CLI/BUI	Description
UNCONFIGURED		Le clustering n'est pas configuré	Un système ne contenant aucun clustering possède cet état. Soit le système est en cours de configuration, soit la tâche de configuration du cluster n'a jamais été terminée.
OWNER		Actif (reprise terminée)	Le clustering est configuré et ce nœud a pris le contrôle de toutes les ressources partagées de ce cluster. Un système saisit immédiatement cet état dans son interface utilisateur une fois la configuration du cluster

Etat	Icône	Expression de la CLI/BUI	Description
			effectuée et lorsqu'il détecte l'échec de son pair (p. ex après la reprise). Il reste dans cet état jusqu'à ce qu'un administrateur exécute manuellement une opération de rétablissement.
STRIPPED		Prêt (en attente du rétablissement)	Le clustering est configuré et ce noeud ne contrôle aucune ressource de données. Un système reçoit immédiatement l'état STRIPPED une fois la configuration du cluster terminée à partir de l'interface utilisateur de l'autre noeud, ou à la suite d'une réinitialisation, d'une coupure de courant ou d'une autre panne. Un noeud reste dans cet état jusqu'à ce qu'un administrateur exécute manuellement une opération de rétablissement.
CLUSTERED		Actif	Le clustering est configuré et les deux noeuds possèdent des ressources partagées en fonction des ressources qui leur sont affectées. Si chaque noeud possède un pool ZFS et qu'il est défini sur l'état CLUSTERED, les deux noeuds forment ce qui est communément appelé un cluster actif-actif.
-		Retour au cluster...	L'appareil a été récemment réinitialisé ou le logiciel de gestion des appareils a été redémarré après une panne interne. L'état de la ressource est en cours de resynchronisation.
-		Inconnu (déconnecté ou en cours de redémarrage)	L'appareil pair est hors tension ou en cours de réinitialisation, toutes ses liaisons d'interconnexion sont interrompues ou le clustering n'a pas encore été configuré.

Les transitions entre ces états ont lieu dans le cadre de deux opérations : la reprise et le rétablissement.

La reprise peut avoir lieu à tout moment et est tentée dès qu'une défaillance du pair est détectée. Vous pouvez également le déclencher manuellement à l'aide de la CLI ou de la BUI de configuration du cluster. Cela peut être utile à des fins de test ou pour effectuer des mises à niveau logicielles non simultanées (lors desquelles un contrôleur est mis à niveau tandis que l'autre fournit le service exécutant l'ancien logiciel ; une fois le nouveau logiciel validé, le deuxième contrôleur est alors mis à niveau). Enfin, la reprise a lieu lorsqu'un contrôleur est initialisé et qu'il détecte que son pair est absent. Cela permet au service de reprendre normalement lorsqu'un contrôleur est en panne de façon permanente ou lorsque les deux contrôleurs ont subi temporairement une panne de courant.

Le rétablissement ne se fait jamais automatiquement. Lorsqu'un contrôleur est réparé puis réinitialisé, il rejoint le cluster (en resynchronisant l'affichage de toutes ses ressources et propriétés) puis attend qu'un administrateur exécute une opération de rétablissement. Jusqu'ici, le contrôleur encore fonctionnel d'origine continue de fournir tous les services. Cela permet d'étudier en détail le problème à l'origine de la reprise, de valider une nouvelle révision du logiciel ou de réaliser d'autres tâches d'administration avant que le contrôleur ne reprenne le service de production. Etant donné que le rétablissement perturbe les clients, il doit être planifié en fonction des besoins et des processus métier spécifiques. Il existe une exception : supposons que le contrôleur A soit en panne et que le contrôleur B ait pris le relais. Lorsque le contrôleur A rejoint le cluster, il peut assurer une reprise s'il détecte que le contrôleur B est absent ou défectueux. Le principe est le suivant : il vaut toujours mieux être en service qu'inactif, même si cela implique de ne pas examiner le problème d'origine. Alors que le rétablissement vers un contrôleur précédemment défaillant ne s'effectue jamais automatiquement, il peut néanmoins effectuer la reprise à tout moment.

Une fois que vous avez configuré un cluster, l'état initial comprend le noeud ayant initialisé la configuration, dont l'état est OWNER, ainsi que l'autre noeud dont l'état est STRIPPED. Après avoir exécuté une opération de rétablissement initiale pour octroyer au noeud STRIPPED sa part de ressources partagées, les deux noeuds sont CLUSTERED. Si les deux noeuds clustérisés sont en panne ou mis hors tension, ils font l'objet d'un arbitrage lors du démarrage, au cours duquel l'un d'eux devient OWNER et l'autre STRIPPED.

Durant le rétablissement, toutes les ressources étrangères (celles qui sont assignées au pair) sont exportées puis importées par le pair. Un pool qui ne peut pas être importé en raison de sa défaillance déclenche la réinitialisation du noeud STRIPPED. Une tentative de rétablissement à l'aide d'un pool défectueux peut réinitialiser le noeud STRIPPED en raison de l'échec d'importation.

Pour réduire le temps d'arrêt pour maintenance, les statistiques et les ensembles de données ne sont pas disponibles lors des opérations de rétablissement et de reprise. Les données ne sont pas collectées et toute tentative de suspension ou de reprise des statistiques est différée jusqu'à la fin des opérations de rétablissement et de reprise et jusqu'à la reprise automatique de la collecte de données.

Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Modifications de la configuration dans un environnement clustérisé

La majorité de la configuration de l'appareil est représentée par des propriétés service ou des propriétés partage/LUN. Alors que les propriétés partage et LUN sont stockées avec les données de l'utilisateur sur le pool de stockage (et sont par conséquent toujours accessibles au propriétaire en cours de cette ressource de stockage), la configuration de service est stockée dans chaque contrôleur. Afin de garantir que les deux contrôleurs fournissent un service cohérent, toutes les propriétés service doivent être synchronisées en cas de modification ou lorsqu'un contrôleur précédemment hors service rejoint son pair. Etant donné que tous les services sont représentés par des ressources réplique, la synchronisation est automatiquement effectuée par le logiciel de l'appareil dès lors qu'une propriété est modifiée sur l'un des contrôleurs.

Par conséquent, il n'est pas nécessaire pour les administrateurs de répliquer les modifications de la configuration, et ce serait redondant. Les procédures de fonctionnement standard doivent refléter cet attribut et appeler à des modifications sur un seul des deux contrôleurs en cas de modification de la configuration du cluster d'origine. Notez également que le processus de configuration du cluster d'origine réplique toute la configuration existante sur le pair bénéficiant d'une nouvelle configuration. Il en découle généralement deux meilleures pratiques en matière de modification de la configuration en cluster :

- Apportez toutes les modifications de la configuration liées au stockage et au réseau sur le contrôleur qui contrôle actuellement (ou contrôlera plus tard, si une nouvelle ressource est en cours de création) les ressources de stockage ou d'interface réseau sous-jacentes.
- Apportez toutes les autres modifications à l'un des contrôleurs, mais pas aux deux. La stratégie du site doit indiquer quel contrôleur doit alors être considéré comme le *maître*, ce qui dépend à son tour de quel contrôleur est en cours de fonctionnement et du nombre de pools de stockage qui ont été configurés. Notez que le logiciel de l'appareil ne fait pas cette distinction.

Le problème d'*amnésie*, selon lequel des modifications disjointes de configuration sont effectuées puis perdues sur chaque contrôleur lorsque son pair ne fonctionne pas, est très surestimé. Cela est particulièrement vrai pour la série Oracle ZFS Storage Appliance, qui n'inclut aucun mécanisme pour effectuer des modifications indépendantes de la configuration système sur chaque contrôleur. Cette simplification réduit considérablement le besoin de référentiels de configuration centralisés et plaide pour une approche simplifiée : le contrôleur en cours de fonctionnement est censé détenir la configuration appropriée et son pair sera synchronisé par rapport à lui lors de l'initialisation. Alors que des améliorations futures du produit pourront permettre de sélectionner une stratégie alternative pour la résolution des divergences de configuration, cette approche basique est simple et facile à comprendre : le deuxième contrôleur adopte un ensemble de paramètres de configuration déjà utilisés par un

système de production existant (dont le degré d'exactitude est par conséquent très élevé). Pour s'assurer que cela reste vrai, les administrateurs doivent vérifier qu'un contrôleur défaillant rejoint le cluster dès sa réparation.

Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Considérations relatives au clustering pour le stockage

Lorsque vous redimensionnez un système de la série Oracle ZFS Storage Appliance pour l'utiliser dans une configuration en cluster, deux considérations sont très importantes :

- Vous devez décider si tous les pools sont la propriété du même contrôleur ou s'ils sont divisés entre les deux contrôleurs.
- Vous devez décider si vous voulez des pools sans point de panne unique (NSPF).

Affectation de la propriété du pool de stockage - La décision la plus importante consiste certainement à décider d'attribuer la propriété à tous les pools de stockage ou à la diviser entre ces derniers. Plusieurs compromis doivent être pris en compte, comme indiqué dans le [Tableau 47, "Considérations relatives au clustering pour les pools de stockage"](#).

Généralement, les pools doivent être configurés sur un seul contrôleur, sauf en cas d'optimisation du débit durant l'opération nominale ou lorsque les performances de basculement ne sont pas prises en compte. En état de basculement, les modifications exactes des caractéristiques des performances dépendent largement de la nature et de la taille de la charge de travail. En général, plus un contrôleur est proche de fournir des performances maximales sur un axe particulier, plus la dégradation des performances est importante le long de l'axe lorsque la charge de travail est reprise par le pair du contrôleur. En cas de pools multiples, cette dégradation s'applique aux deux charges de travail.

Les périphériques de cache de lecture sont situés dans le contrôleur ou l'étagère de disques, en fonction de votre configuration.

Les périphériques de cache de lecture, qui se trouvent dans un emplacement de contrôleur (L2ARC interne), ne suivent pas les pools de données dans les situations de reprise ou de rétablissement. Un périphérique de cache de lecture n'est actif que dans un noeud de cluster particulier lorsque le pool assigné au périphérique de cache de lecture est importé sur le noeud sur lequel se trouve le périphérique. En l'absence d'étapes de configuration supplémentaires, le cache de lecture ne sera pas disponible pour un pool qui a migré en raison d'un événement de basculement. Afin d'activer un périphérique de cache de lecture pour un pool qui n'appartient pas à un pair de cluster, reprenez le pool sur le noeud sans appartenance, puis ajoutez du stockage et sélectionnez les périphériques de mise en cache pour la configuration. Il est donc conseillé de configurer les périphériques de cache de lecture dans un noeud de cluster

comme décrit à la section ["Configuration du stockage" à la page 84](#). Les périphériques de journalisation optimisés pour l'écriture sont situés dans la topologie Fabric de stockage et restent accessibles à tous les contrôleurs ayant importé le pool.

Si les périphériques de cache de lecture sont situés dans une étagère de disques (L2ARC externe), le cache de lecture est toujours disponible. Lors d'une opération de rétablissement ou de reprise, le cache de lecture reste partageable entre les contrôleurs. Dans ce cas, les performances de lecture sont maintenues. Pour plus de détails sur la configuration du cache de lecture externe, reportez-vous à la section ["Configurations d'étagère de disques" dans le Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance](#).

Configuration sans point de panne unique (NSPF) - Une deuxième considération importante relative au stockage a trait à l'utilisation des configurations de pool sans point de panne unique. Etant donné que l'utilisation du clustering implique que l'application donne une importance significative à la disponibilité, il existe rarement une bonne raison de configurer des pools de stockage d'une manière autorisant l'échec d'une étagère de disques unique et par conséquent une perte de disponibilité. L'inconvénient de cette approche est que les configurations NSPF nécessitent un plus grand nombre d'étagères de disques que les configurations ayant un point de panne unique. Lorsque la capacité requise est très faible, l'installation d'un nombre suffisant d'étagères de disques pour autoriser la configuration NSPF au niveau RAID voulu peut ne pas être économique.

Le tableau suivant décrit la propriété du pool de stockage pour les configurations en cluster.

TABEAU 47 Considérations relatives au clustering pour les pools de stockage

Variable	Propriété d'un pool de contrôleur unique	Pools multiples possédés par des contrôleurs différents
Débit total (opération nominale)	Jusqu'à 50 % des ressources de CPU totales, 50 % de la DRAM et 50 % de la connectivité réseau totale peuvent être utilisés pour fournir le service à un moment précis. C'est simple : un seul contrôleur traite les requêtes du client, l'autre est inactif.	Toutes les ressources de CPU et de DRAM peuvent être utilisées pour fournir le service à tout moment. Jusqu'à 50 % de la connectivité réseau peut être utilisée à tout moment (des périphériques réseau invisibles sont requis sur chaque contrôleur pour prendre en charge le basculement).
Débit total (basculement)	Aucune modification du débit par rapport à l'opération nominale.	100 % des ressources de contrôleur encore fonctionnelles sont utilisées pour fournir le service. Le débit total relatif à l'opération nominale est compris entre environ 40 et 100 %, en fonction de l'utilisation durant l'opération nominale.
Latence d'E/S	Le cache de lecture interne n'est pas disponible durant une opération de rétablissement ou de reprise, ce qui peut considérablement augmenter les temps d'attente pour les charges de travail intégrées au cache de lecture disponible. Le temps d'attente	Le cache de lecture interne n'est pas disponible durant une opération de rétablissement ou de reprise, ce qui peut considérablement augmenter les temps d'attente pour les charges de travail intégrées au cache de lecture disponible. Le temps

Variable	Propriété d'un pool de contrôleur unique	Pools multiples possédés par des contrôleurs différents
	des opérations d'écriture n'est pas concerné. Dans les configurations de cache de lecture externe (EL2ARC), les performances de lecture ne sont pas affectées. Le cache de lecture est partagé entre les pairs du cluster lors d'une opération de rétablissement ou de reprise, évitant ainsi tout temps d'attente pour la lecture.	d'attente des opérations de lecture et d'écriture peut être augmenté en raison des conflits importants en matière d'utilisation des ressources de contrôleur résultant de l'exécution de deux charges de travail sur le contrôleur encore fonctionnel à la place du contrôleur habituel. Lorsque les charges de travail nominales de chaque contrôleur atteignent les capacités maximales du contrôleur, les temps d'attente dans l'état de basculement peuvent être extrêmement longs. Dans les configurations de cache de lecture externe (EL2ARC), les performances de lecture ne sont pas affectées. Le cache de lecture est partagé entre les pairs du cluster lors d'une opération de rétablissement ou de reprise, évitant ainsi tout temps d'attente pour la lecture.
Flexibilité du stockage	Les partages et les LUN peuvent tirer parti de toutes les unités de stockage physiques disponibles.	Les partages et les LUN d'un pool peuvent utiliser uniquement le stockage alloué à ce pool. Le stockage n'est pas partagé entre les pools. Si un pool est saturé tandis que l'autre possède de l'espace libre, de l'espace de stockage risque donc d'être gaspillé.
Connectivité réseau	Tous les périphériques réseau de chaque contrôleur peuvent être utilisés tandis que le contrôleur est en service.	Seule la moitié de l'ensemble des périphériques réseau de chaque contrôleur peut être utilisée lorsque le contrôleur est en service. Chaque pool peut donc être connecté à seulement la moitié des réseaux physiquement disjoints.

Rubriques connexes

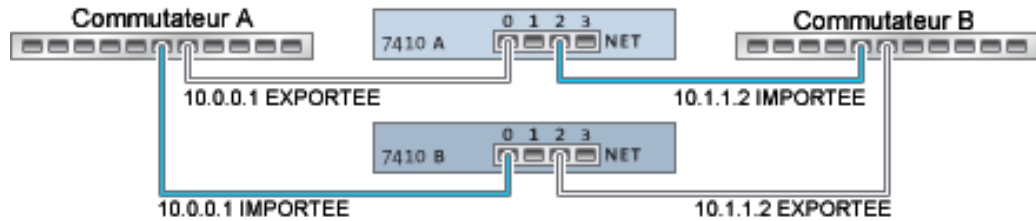
- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Considérations relatives au clustering pour la gestion réseau

La défaillance d'un périphérique réseau, d'une liaison de données et de l'interface ne provoque pas l'échec d'un contrôleur d'un sous-système en cluster. Pour vous protéger des pannes réseau à l'intérieur ou à l'extérieur de l'appareil, utilisez plutôt IPMP et/ou LACP. Une approche globale

de la disponibilité nécessite la configuration appropriée du réseau et un plan de redondance à l'échelle du réseau.

FIGURE 19 Clustering pour la gestion réseau



Les interfaces réseau peuvent être configurées en tant que ressources singleton ou privées, à condition qu'elles possèdent une configuration IP statique. Les interfaces configurées à l'aide de DHCP doivent être privées et l'utilisation de DHCP dans les clusters est déconseillée. Lorsqu'ils sont configurés en tant que ressources singleton, tous les périphériques et les liaisons de données utilisés pour construire une interface peuvent être actifs sur un seul contrôleur à la fois. De la même manière, les périphériques correspondants sur chaque contrôleur doivent être connectés aux mêmes réseaux afin que le service soit fourni dans l'état de basculement. Pour un exemple, voir l'illustration ci-dessus.

Lors de la construction des interfaces réseau à partir de périphériques et de liaisons de données, il est essentiel pour le bon fonctionnement du cluster que chaque interface singleton contienne un périphérique dont l'identifiant et les fonctionnalités sont les mêmes sur les deux contrôleurs. Les identifiants étant dépendants du type de périphérique et de l'ordre dans lequel ils sont détectés par l'appareil, le matériel installé sur les contrôleurs clustérisés doit être identique. Chaque emplacement doit recevoir du matériel identique, installé dans le même ordre sur les deux contrôleurs. Vous pouvez obtenir l'aide de votre revendeur Oracle agréé ou de tout agent technique pour la planification des mises à niveau matérielles compatibles.

Une route est toujours explicitement liée à une seule interface réseau. Les routes sont représentées dans le gestionnaire de ressources en tant que symbiotes et peuvent devenir actives uniquement lorsque les interfaces auxquelles elles sont associées sont opérationnelles. Par conséquent, une route liée à une interface actuellement en mode veille (exportée) est sans conséquence jusqu'à ce que l'interface soit activée lors du processus de reprise. Cela a son importance lorsque deux pools sont configurés et sont rendus disponibles sur un sous-réseau commun. Si un sous-réseau constitue l'emplacement d'origine d'un routeur utilisé par les appareils pour atteindre un ou plusieurs réseaux, une route distincte (par exemple, une deuxième route par défaut) doit être configurée, puis liée à chacune des interfaces actives et en veille associées à ce sous-réseau.

Exemple :

- L'interface e1000g3 est assignée à "alice" et l'interface e1000g4 à "bob".
- Chaque interface possède une adresse dans le réseau 172.16.27.0/24 et peut permettre de fournir le service aux clients dans le réseau 172.16.64.0/22, accessible via 172.16.27.1.
- Deux routes doivent être créées sur 172.16.64.0/22 via 172.16.27.1. L'une doit être associée à e1000g3 et l'autre à e1000g4.

Une bonne idée consiste à affecter à chaque contrôleur clustérisé une adresse IP utilisée uniquement pour l'administration (généralement sur un réseau de gestion dédié) et à désigner l'interface en tant que ressource privée. Cela garantit l'accès à tous les contrôleurs qui fonctionnent à partir du réseau de gestion, même lorsque leur état est AKCS_STRIPPED et qu'ils sont en attente de rétablissement. Ce type d'attribution est important en cas d'utilisation de services tels que LDAP et Active Directory, qui nécessitent d'accéder aux autres ressources réseau lorsque le contrôleur ne fournit pas le service. Si cela n'est pas pratique, ce processeur de service doit être connecté à un réseau fiable et/ou à un concentrateur de terminaux série afin que le contrôleur puisse être géré à partir de la console système.

Si aucune de ces actions n'est effectuée, il est impossible de gérer ou de surveiller un contrôleur qui vient d'être initialisé tant que le rétablissement n'est pas terminé. Vous pouvez souhaiter surveiller ou gérer le contrôleur fournissant actuellement le service pour un pool de stockage particulier. Cette approche est probablement plus utile lorsque vous souhaitez modifier certains aspects du stockage lui-même, comme modifier une propriété de partage ou créer un nouveau LUN. Pour cela, vous pouvez effectuer des tâches administratives dans les interfaces de service ou affecter une interface singleton distincte à utiliser uniquement pour gérer le pool avec lequel elle est mise en correspondance. Dans les deux cas, l'interface doit être affectée au même contrôleur que le pool utilisé pour la gestion.

Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Interfaces IP locales privées

Suivez les instructions suivantes lors de la création d'interfaces IP locales privées :

- La création d'une interface IP avec le même nom qu'une interface IP privée sur un pair de cluster entraîne la création locale d'une interface IP privée.
- Les liaisons de données utilisées par les interfaces privées du pair ne peuvent pas être supprimées et le bouton de suppression est grisé.
- Les interfaces IP qui appartiennent à un groupe IPMP doivent toutes être du même type et appartenir au même contrôleur. Pour créer un groupe IPMP, vous devez utiliser des interfaces IP qui sont entièrement singleton ou entièrement privées et votre noeud de cluster doit être propriétaire de ces interfaces.
- Le type de groupe IPMP est défini uniquement à la création et est déterminé par le type de liaisons sous-jacentes.

- Les interfaces IP qui appartiennent aux groupes IPMP n'apparaissent pas sur la page Cluster:Ressources car la propriété de l'interface IP ne peut pas être modifiée indépendamment de la propriété du groupe IPMP.
- Les groupes IPMP privés n'apparaissent pas sur la page Cluster:Ressources car ce type ou cette propriété ne peut pas être modifié.

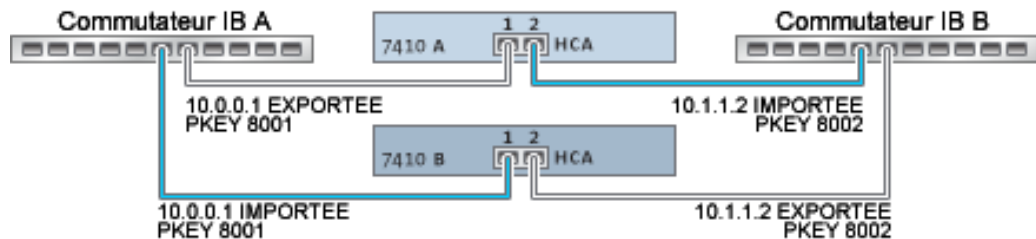
Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Considérations relatives au clustering pour Infiniband

A l'instar d'un réseau construit au-dessus de périphériques Ethernet, un réseau Infiniband doit faire partie d'une topologie Fabric redondante pour se prémunir des pannes réseau à l'intérieur et à l'extérieur de l'appareil. La topologie réseau doit inclure IPMP pour protéger contre les pannes réseau au niveau de la liaison avec un plan de redondance plus large pour les adaptateurs de canal hôte (HCA), les commutateurs et les gestionnaires de sous-réseau.

FIGURE 20 Considérations relatives au clustering pour Infiniband

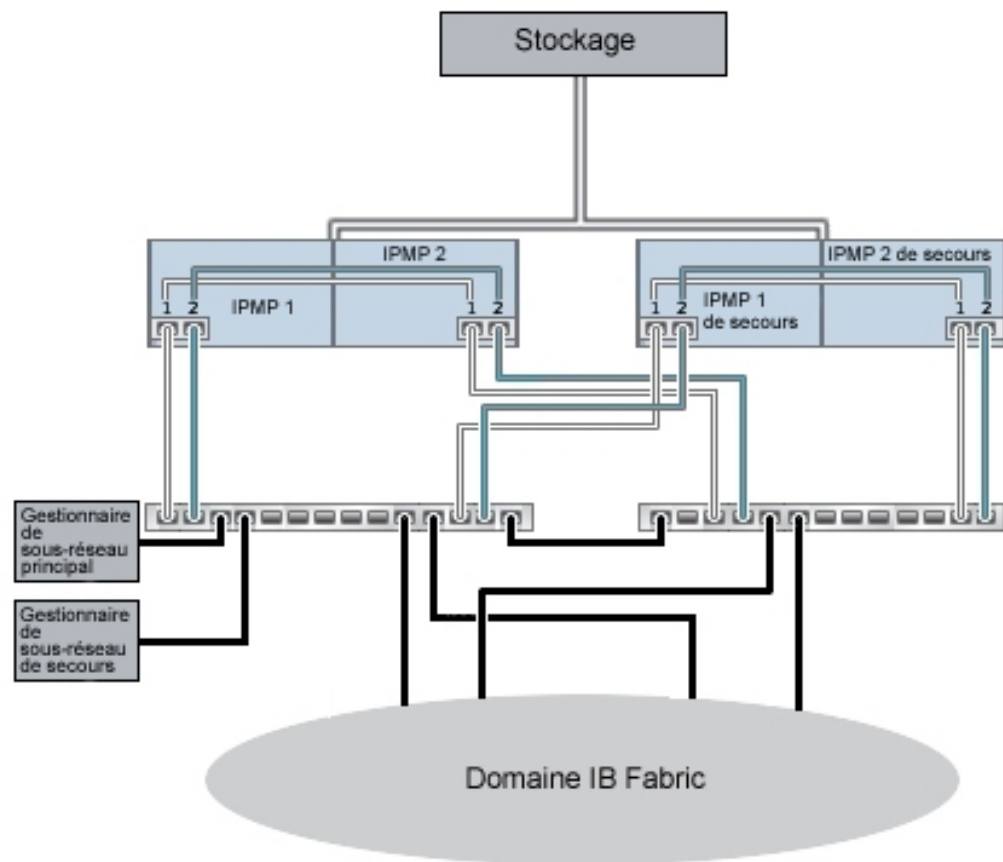


Pour garantir une configuration de cluster appropriée, chaque contrôleur doit recevoir des HCA identiques dans des emplacements identiques. En outre, chaque port HCA correspondant doit être configuré dans la même partition (pkey) sur le gestionnaire de sous-réseau avec des privilèges d'appartenance identiques associés au même réseau. Pour limiter la complexité et garantir une redondance adaptée, il est recommandé d'intégrer chaque port à une seule partition du sous-réseau Infiniband. Il est possible de configurer les interfaces réseau en tant que ressources singleton ou privées, à condition qu'elles possèdent une configuration IP statique. Lorsqu'ils sont configurés en tant que ressources singleton, tous les périphériques et les liaisons de données de la partition Infiniband doivent être actifs sur un seul contrôleur à un moment précis. Pour un exemple concret, voir l'illustration ci-dessus. Les modifications apportées à l'appartenance de la partition pour les ports correspondants doivent avoir lieu en même temps et

conformément aux règles de clustering décrites plus haut. Vous pouvez obtenir l'aide de votre revendeur Oracle agréé ou de tout agent technique dans la planification des mises à niveau matérielles compatibles.

L'illustration suivante présente la configuration du cluster pour la redondance du gestionnaire de sous-réseau. Une plus grande redondance est permise en connectant deux HCA à double accès à une paire redondante de commutateurs de serveur.

FIGURE 21 Configuration du cluster pour la redondance du gestionnaire de sous-réseau



Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Prévention des états split-brain

Un mode d'échec courant dans les systèmes clustérisés est le *split-brain*. Dans cette condition, chacun des contrôleurs clustérisés croit que son pair subit une défaillance et tente une reprise. En dehors de toute logique supplémentaire, cet état peut entraîner une large gamme de comportements inattendus et destructifs qu'il peut être difficile de diagnostiquer ou de corriger. Le déclenchement canonique de cette condition est l'échec du moyen de communication partagé par les contrôleurs. Dans le cas des appareils de la série Oracle ZFS Storage Appliance, cela aurait lieu en cas d'échec des liaisons d'E/S du cluster. En plus de la redondance à liaison triple associée (une seule liaison est requise pour éviter le déclenchement de la reprise), le logiciel de l'appareil exécute également une procédure d'arbitrage afin de déterminer le contrôleur qui poursuivra la reprise.

Un certain nombre de mécanismes d'arbitrage sont utilisés par des produits similaires. En général, ils impliquent l'utilisation de *disques de quorum* (à l'aide de réservations SCSI) ou de *serveurs de quorum*. Pour prendre en charge l'utilisation de disques ATA sans recourir à du matériel supplémentaire, l'appareil Oracle ZFS Storage Appliance utilise une approche différente basée sur la topologie Fabric de stockage elle-même afin de fournir l'exclusivité mutuelle requise. Le processus d'arbitrage consiste à tenter d'exécuter une commande SAS ZONE LOCK sur chacun des expandeurs SAS visibles dans la topologie Fabric de stockage dans un ordre prédéfini. L'appareil sur lequel aboutit la tentative d'obtention des verrouillages poursuit la reprise, l'autre est réinitialisé. Dans la mesure où un appareil clustérisé qui est initialisé et détecte que son pair est inaccessible tente la reprise et effectue le même processus d'arbitrage, il est réinitialisé dans une boucle continue jusqu'à ce qu'au moins une liaison d'E/S du cluster soit restaurée. Cela garantit que la panne qui s'en suit sur l'autre contrôleur n'entraîne pas d'interruption de service étendue. Ces verrous de zone SAS sont libérés lors du rétablissement ou environ 10 secondes après le renouvellement de l'accès à la topologie Fabric de stockage pour le contrôleur dont l'état est AKCS_OWNER.

Le mécanisme d'arbitrage est simple, peu onéreux et ne nécessite pas de matériel supplémentaire. Il repose sur les appareils clustérisés ayant accès à au moins un expandeur SAS commun dans la topologie Fabric de stockage. Dans des conditions normales, chaque appareil a accès à tous les expandeurs et l'arbitrage est réalisé à l'aide d'au moins deux verrous de zone SAS. Il est néanmoins possible de concevoir des scénarios à pannes multiples dans lesquels les appareils n'ont accès à aucun expandeur commun. Par exemple, si deux des câbles SAS sont débranchés ou si une étagère de disques est mise hors tension, chaque appareil a accès à des sous-ensembles disjoints d'expandeurs. Dans ce cas, chaque appareil verrouille tous les expandeurs accessibles, conclut que son pair subit une défaillance et tente de procéder à la reprise. Cela peut entraîner des blocages irrécupérables en raison des conflits d'affiliation de disque et/ou d'une grave altération de données.

Notez que, bien que les conséquences de cet état soient graves, elles ne surviennent qu'en cas de pannes multiples (souvent après quatre pannes ou plus). La solution de clustering intégrée aux appareils de la gamme Oracle ZFS Storage Appliance a été conçue pour garantir l'absence de point de panne unique et protéger les données et la disponibilité contre toute panne éventuelle sans impliquer de coûts ou de complexité supplémentaires. Il reste possible qu'un grand nombre

de pannes multiples entraîne une perte de service et/ou de données, de la même manière qu'aucune configuration RAID n'offre de protection contre un nombre illimité de défaillances de disque.

FIGURE 22 Prévention des conditions split-brain



Heureusement, la plupart de ces scénarios de panne sont dus à une erreur humaine et peuvent être entièrement évités si le matériel est correctement installé et si vous formez du personnel à la configuration du cluster et aux meilleures pratiques de gestion. Les administrateurs doivent toujours veiller à ce que les trois liaisons d'E/S du cluster soient connectées et fonctionnelles (voir illustration) et s'assurer que le câblage du stockage respecte le schéma de configuration fourni avec vos appareils. Il est particulièrement important que les deux chemins soient détectés vers chaque étagère de disques (voir illustration) avant et après la mise en production du cluster, exception faite évidemment des modifications temporaires de câblage pour prendre en charge les améliorations des fonctionnalités ou le remplacement des composants défectueux. Les administrateurs doivent utiliser des alertes pour surveiller l'état des liaisons d'interconnexion du cluster et des chemins d'étagères de disques et corriger rapidement toute panne. En vous assurant du maintien de la connectivité, vous pourrez protéger à la fois la disponibilité et l'intégrité des données en cas de défaillance d'un composant matériel ou logiciel.

FIGURE 23 Cluster à deux chemins

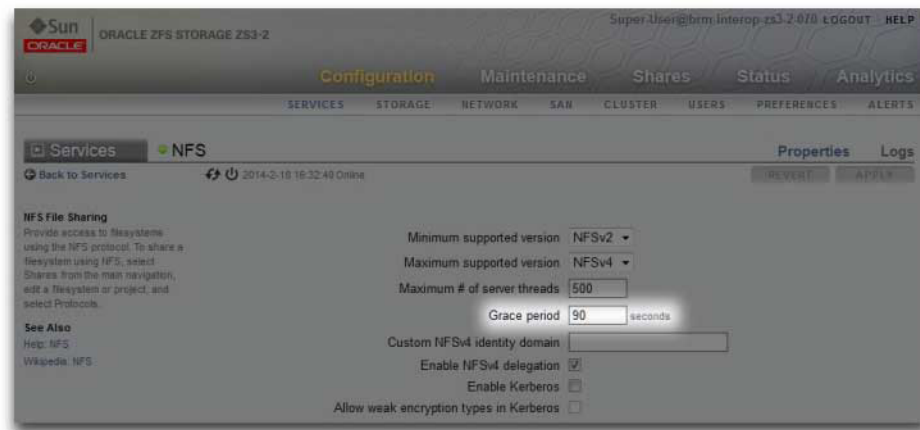
Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Estimation et réduction de l'impact de la reprise

Il existe un intervalle entre la reprise et le rétablissement durant lequel l'accès au stockage ne peut pas être fourni aux clients. La durée de cet intervalle varie en fonction de la configuration. Les effets exacts sur les clients dépendent du/des protocole(s) qu'ils utilisent pour accéder aux données. La compréhension et la limitation de ces effets peut faire la différence entre un déploiement de cluster réussi et une panne dommageable survenant au pire moment possible.

Les clients NFS (toutes versions confondues) cachent généralement les interruptions de service aux applications logicielles, ce qui entraîne le retard des opérations d'E/S durant l'indisponibilité d'un serveur. NFSv2 et NFSv3 sont des protocoles sans état dont la récupération est quasiment instantanée durant la restauration du service. NFSv4 intègre une période de grâce du client au démarrage, durant laquelle aucune opération d'E/S ne peut généralement être réalisée. La durée de cette période de grâce peut être réglée sur les appareils de la gamme Oracle ZFS Storage Appliance. Si vous la réduisez, l'impact apparent de la reprise et/ou du rétablissement est réduit. Pour les interruptions de service planifiées, l'appareil Oracle ZFS Storage Appliance fournit une récupération sans grâce pour les clients NFSv4, qui évite le délai de la période de grâce. Pour plus d'informations sur la récupération sans période de grâce, reportez vous à la propriété de période de grâce dans la section ["Propriétés du service NFS" à la page 237](#).

FIGURE 24 Période de grâce de cluster

Le comportement iSCSI durant les interruptions de service dépend de l'initiateur, mais les initiateurs récupèrent automatiquement si le service est restauré dans un délai d'attente spécifique au client. Pour plus d'informations, consultez la documentation de votre initiateur. La cible iSCSI peut généralement fournir le service dès la fin de la reprise, sans délai supplémentaire.

SMB, FTP et HTTP/WebDAV sont des protocoles orientés connexion. Etant donné que les états de la session associés à ces services ne peuvent pas être transférés avec le stockage sous-jacent et la connectivité réseau, tous les clients utilisant ces protocoles sont déconnectés durant une reprise ou un rétablissement et doivent se reconnecter à l'issue de l'opération.

Même si plusieurs facteurs ont une incidence sur le temps de reprise (et son proche parent, le temps de rétablissement), dans la plupart des configurations, ces délais sont dominés par le temps requis pour importer la/les ressource(s) de l'ensemble de disques. La durée d'importation type de chaque plage d'ensemble de disques est de l'ordre de 15 à 20 secondes (linéaires dans le nombre d'ensembles de disques). N'oubliez pas qu'un ensemble de disques consiste en une demie étagère de disques, à condition que les baies de disque de cette demie-étagère de disques aient été remplies et allouées à un pool de stockage. Les disques non alloués et les baies vides n'ont pas d'incidence sur le temps de reprise. Les paramètres réglables ou éventuellement modifiés par les administrateurs n'ayant pas d'incidence sur le temps requis pour importer les ressources de l'ensemble de disques, les administrateurs planifiant des déploiements clustérisés doivent réaliser l'une des opérations suivantes :

- limiter le stockage installé afin que les clients puissent tolérer les temps de reprise liés ou
- définir des valeurs de délai d'attente côté client supérieures au délai maximal de reprise attendu.

Notez que, même si l'importation de l'ensemble de disques représente la majeure partie du temps de reprise, il ne s'agit pas du seul facteur. Lors de l'importation du pool, tous les enregistrements du journal d'intention doivent être rediffusés et chaque partage et LUN doit être partagé via le(s) service(s) approprié(s). La durée nécessaire à l'exécution de ces activités pour un seul partage ou LUN est très courte (de l'ordre du dixième de seconde). Mais en présence d'un très grand nombre de partages, le délai de reprise peut être bien plus long. En gardant un nombre de partages relativement bas (quelques centaines ou moins), ces temps peuvent être considérablement raccourcis.

La durée de rétablissement est généralement plus longue que le temps de reprise pour n'importe quelle configuration. Cela tient au fait que le rétablissement se fait en deux étapes : d'abord, l'appareil source exporte toutes les ressources dont vous n'êtes pas le propriétaire attitré, puis l'appareil cible effectue la procédure de reprise standard uniquement sur les ressources qui lui ont été attribuées. Il faudra donc plus de temps pour effectuer le rétablissement à partir du contrôleur A vers le contrôleur B qu'il n'en faudra pour que le contrôleur A effectue la reprise à partir du contrôleur B en cas de panne. Ce temps de rétablissement supplémentaire dépend beaucoup moins du nombre d'ensembles de disques en cours d'exportation que du délai de reprise. Par conséquent, le fait de maintenir un petit nombre de partages et de LUN affecte davantage le rétablissement que la reprise. Gardez également à l'esprit que le rétablissement est toujours amorcé par un administrateur. Par conséquent, plus l'interruption du service qu'il entraîne dure et plus celle-ci pourra être planifiée afin de limiter au maximum l'interruption des activités.

Remarque - Les durées estimées citées dans cette section se rapportent à la version logicielle/du microprogramme 2009.04.10,1-0. Les autres versions peuvent se comporter différemment et les performances réelles peuvent varier. Il est important de tester la reprise et ses conséquences exactes sur les applications client avant de déployer un appareil clustérisé dans un environnement de production.

Rubriques connexes

- ["Arrêt de la configuration clustérisée \(CLI\)" à la page 197](#)

Services de l'appareil

Les services de l'appareil sont facilement gérés à partir de l'écran Configuration > Services de la BUI ou du contexte configuration services de la CLI.

Effectuez les tâches suivantes pour consulter et gérer les services des appareils :

- ["Affichage d'un service dans la BUI" à la page 226](#)
- ["Sélection d'un service dans la CLI" à la page 227](#)
- Activation d'un service - [BUI](#), [CLI](#)
- Désactivation d'un service - [BUI](#), [CLI](#)
- ["Affichage des états d'un service dans la CLI" à la page 229](#)
- ["Affichage de l'aide d'un service dans la CLI" à la page 229](#)
- Définition des propriétés du service - [BUI](#), [CLI](#)
- Affichage des journaux de service - [BUI](#), [CLI](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

Pour plus d'informations sur la configuration d'un service particulier, sélectionnez le service approprié dans le tableau suivant :

Services de données	Services d'annuaire	Paramètres système	Accès à distance
NFS	NIS	DNS	SSH
iSCSI	LDAP	IPMP	API RESTful
SMB	Active Directory	NTP	
FTP	Mappage des identités	Phone Home	
HTTP		Routage dynamique	
NDMP		Indicateurs de maintenance	
Réplication distante		SMTP	
Migration shadow		SNMP	
SFTP		Syslog	
SRP		Identité du système	
TFTP			
Analyse antivirus			

Gestion des services

Pour plus d'informations sur la gestion des services de l'appareil, utilisez les tâches suivantes :

- ["Affichage d'un service dans la BUI" à la page 226](#)
- ["Sélection d'un service dans la CLI" à la page 227](#)
- Activation d'un service - [BUI](#), [CLI](#)
- Désactivation d'un service - [BUI](#), [CLI](#)
- ["Affichage des états d'un service dans la CLI" à la page 229](#)
- ["Affichage de l'aide d'un service dans la CLI" à la page 229](#)
- Définition des propriétés du service - [BUI](#), [CLI](#)
- Affichage des journaux de service - [BUI](#), [CLI](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Affichage d'un service dans la BUI

1. **Accédez à Configuration > Services.**
2. **Pour consulter ou modifier les propriétés d'un service spécifique, placez le pointeur de la souris sur l'icône de statut située à gauche du nom de service.**
L'icône de statut se transforme alors en flèche .
3. **Cliquez sur l'icône fléchée  pour afficher l'écran des propriétés du service sélectionné.**
4. **Dans n'importe quel écran de service, il est possible d'afficher un panneau latéral de tous les services en cliquant sur la petite icône en forme de flèche située à gauche du titre Services (près de la partie supérieure gauche de chaque écran). Pour masquer la liste, cliquez à nouveau sur cette icône.**

Rubriques connexes

- ["Activation d'un service \(BUI\)" à la page 227](#)
- ["Définition des propriétés du service \(BUI\)" à la page 230](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Sélection d'un service dans la CLI

Après avoir sélectionné un service, vous pouvez afficher son état, l'activer, le désactiver et définir ses propriétés.

1. **Accédez à configuration services.**
2. **Sélectionnez un service en saisissant son nom. Par exemple, entrez la commande `nis`:**

```
hostname:configuration services> nis
hostname:configuration services nis>
```

Rubriques connexes

- ["Activation d'un service \(CLI\)" à la page 227](#)
- ["Définition des propriétés du service \(CLI\)" à la page 231](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Activation d'un service (BUI)

Suivez la procédure ci-après pour activer un service qui n'est pas en ligne.

1. **Accédez à Configuration > Services.**
2. **Cliquez sur l'icône d'alimentation  pour l'activer .**

Rubriques connexes

- ["Désactivation d'un service \(BUI\)" à la page 228](#)
- ["Définition des propriétés du service \(BUI\)" à la page 230](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Activation d'un service (CLI)

Suivez la procédure ci-après pour activer un service qui n'est pas en ligne.

1. **Accédez à configuration services.**

2. **Sélectionnez un service, puis entrez la commande `enable` pour l'activer.**

```
hostname:configuration services> nis
hostname:configuration services nis> enable
```

Rubriques connexes

- ["Désactivation d'un service \(CLI\)" à la page 228](#)
- ["Définition des propriétés du service \(CLI\)" à la page 231](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Désactivation d'un service (BUI)

Suivez la procédure ci-après pour désactiver un service qui est en ligne.

1. **Accédez à Configuration > Services.**
2. **Cliquez sur l'icône d'alimentation  pour le désactiver .**

Rubriques connexes

- ["Activation d'un service \(BUI\)" à la page 227](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Désactivation d'un service (CLI)

Suivez la procédure ci-après pour désactiver un service qui est en ligne.

1. **Accédez à configuration services.**
2. **Sélectionnez un service, puis entrez la commande `disable` pour le désactiver.**

```
hostname:configuration services> nis
hostname:configuration services nis> disable
```

Rubriques connexes

- ["Activation d'un service \(CLI\)" à la page 227](#)

- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Affichage des états d'un service dans la CLI

Suivez la procédure ci-après pour afficher l'état des services.

1. **Accédez à configuration services.**
2. **Entrez la commande `show` pour afficher l'état actuel de tous les services.**
3. **Pour afficher l'état d'un service particulier, sélectionnez le service et entrez `show`.**

```
hostname:configuration services> nis
hostname:configuration services nis> show
Properties:
    <status> = online
    domain = fishworks
    broadcast = true
    ypservers =
```

Rubriques connexes

- ["Activation d'un service \(CLI\)" à la page 227](#)
- ["Définition des propriétés du service \(CLI\)" à la page 231](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Affichage de l'aide d'un service dans la CLI

Suivez la procédure ci-après pour afficher les commandes disponibles pour un service.

1. **Accédez à configuration services.**
2. **Sélectionnez le service et entrez la commande `help`.**

```
hostname:configuration services> nis
hostname:configuration services nis> help
Subcommands that are valid in this context:

    help [topic]          => Get context-sensitive help. If [topic] is specified,
                           it must be one of "builtins", "commands", "general",
```

	"help", "script" or "properties".
show	=> Show information pertinent to the current context
commit	=> Commit current state, including any changes
done	=> Finish operating on "nis"
enable	=> Enable the nis service
disable	=> Disable the nis service
get [prop]	=> Get value for property [prop]. ("help properties" for valid properties.) If [prop] is not specified, returns values for all properties.
set [prop]	=> Set property [prop] to [value]. ("help properties" for valid properties.) For properties taking list values, [value] should be a comma-separated list of values.

Rubriques connexes

- ["Définition des propriétés du service \(CLI\)" à la page 231](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Définition des propriétés du service (BUI)

Les écrans Configuration > Services vous permettent de consulter les services et de les modifier. Le tableau suivant décrit les icônes et les boutons des écrans de service.

Icône	Description
	Permet d'accéder à l'écran de service pour configurer les propriétés et afficher les journaux. Ce bouton apparaît lorsque vous laissez le pointeur de la souris stationner sur un service.
	Le service est activé et fonctionne normalement.
	Le service est hors ligne ou désactivé.
	Un problème s'est produit sur le service et requiert l'attention d'un opérateur.
	Active ou désactive le service.
	Redémarre le service.
	Impossible d'activer/de désactiver ce service.

Icône	Description
	Impossible de redémarrer le service actuellement (il faut commencer par l'activer).

1. **Accédez à Configuration > Services.**
2. **Double-cliquez sur un service.**
3. **Modifiez les propriétés puis cliquez sur APPLIQUER.**
Pour rétablir les propriétés, cliquez sur RESTAURER.

Rubriques connexes

- ["Activation d'un service \(BUI\)" à la page 227](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Définition des propriétés du service (CLI)

Suivez la procédure ci-après pour définir les propriétés d'un service. Les noms de propriété sont identiques à leur nom dans la BUI tandis que les noms de la CLI sont généralement plus courts et parfois abrégés.

1. **Accédez à configuration services.**
2. **Sélectionnez un service et entrez `show` pour afficher la liste des propriétés que vous pouvez définir pour ce service, ainsi que leurs valeurs actuelles.**

```
hostname:configuration services> nis
hostname:configuration services nis> show
Properties:
    <status> = online
    domain =
    broadcast = true
    ypservers =
```

3. **Exécutez la commande `set` pour définir les propriétés.**

```
hostname:configuration services nis> set domain="mydomain"
domain = mydomain (uncommitted)
```

4. **Après avoir défini les propriétés, entrez `commit` pour enregistrer et activer la nouvelle configuration.**

```
hostname:configuration services nis> commit
hostname:configuration services nis> show
```

Properties:

```
<status> = online
    domain = mydomain
broadcast = true
ypservers =
```

Rubriques connexes

- ["Activation d'un service \(CLI\)" à la page 227](#)
- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Affichage des journaux de service (BUI)

Certains services fournissent des journaux afin de vous aider à diagnostiquer les problèmes du service. Si un bouton Journaux figure dans la partie supérieure droite d'un écran de service, ce dernier propose un journal. Les journaux de service peuvent fournir les heures auxquelles un service a changé d'état, ainsi que les messages d'erreur émis par le service. Le contenu du journal est spécifique à chaque service individuel et est sujet à modification.

1. **Accédez à Configuration > Services et double-cliquez sur un service.**
2. **Cliquez sur le bouton Journaux situé dans la partie supérieure droite de l'écran d'un service.**

Vous trouverez ci-dessous des exemples de messages courants.

Exemple de message du fichier journal	Description
Exécution de la méthode de démarrage	Le service démarre.
La méthode "démarrer" s'est terminée avec l'état 0	Le service a signalé la réussite du démarrage (0 == réussite).
La méthode "actualiser" s'est terminée avec l'état 0	Le service a correctement actualisé sa configuration en fonction de ses paramètres.
Exécution de la méthode d'arrêt	Le service est en cours de fermeture.
Enabled (Activé)	L'état du service a été vérifié pour savoir s'il doit être démarré (lors de l'initialisation du système, par exemple) ; l'état trouvé est activé.
Désactivé	L'état du service a été vérifié pour savoir s'il doit être démarré (lors de l'initialisation du système, par exemple) ; l'état trouvé est désactivé.

L'exemple de journal suivant est extrait du service NTP :


```
[ Oct 15 21:05:31 Enabled. ]
[ Oct 15 21:07:37 Executing start method (...). ]
[ Oct 15 21:13:38 Method "start" exited with status 0. ]
```

Le premier événement de journal montre que le système a été initialisé à 21h05. La deuxième entrée, à 21h07, indique que le démarrage du service a commencé pour se finir à 21h13. En raison de la nature du protocole NTP et de l'ajustement de l'horloge système, il peut falloir plusieurs minutes afin que le démarrage se termine, comme indiqué dans le journal.

Rubriques connexes

- ["Liste des services disponibles" à la page 233](#)
- ["Ports de service requis" à la page 235](#)

▼ Affichage des journaux de service (CLI)

- Il n'est pas possible de consulter les journaux de service dans la CLI. Utilisez la BUI comme décrit dans la section ["Affichage des journaux de service \(BUI\)" à la page 232](#).

Liste des services disponibles

Cette section répertorie les services disponibles pour les appareils et fournit des descriptions succinctes ainsi que des informations sur les ports. Comme indiqué dans le tableau suivant, certains services sont toujours en marche et ne peuvent pas être désactivés.

TABLEAU 48 Services de données

Service	Description	Ports utilisés
NFS	Accès au système de fichiers via les protocoles NFSv3 et NFSv4	111 et 2049
iSCSI	Accès aux LUN via le protocole iSCSI	3260 et 3205
SMB	Accès au système de fichiers via le protocole SMB	SMB via NetBIOS 139
		SMB via TCP 445
		Datagramme NetBIOS 138
		Service de noms NetBIOS 137
FTP	Accès au système de fichiers via le protocole FTP	21
HTTP	Accès au système de fichiers via le protocole HTTP	80

Service	Description	Ports utilisés
NDMP	Service hôte NDMP	10000
Réplication distante	Réplication distante	216 et 217
Migration shadow	Migration des données shadow	
SFTP	Accès au système de fichiers via le protocole SFTP	218
SRP	Blocage de l'accès via le protocole SRP	
TFTP	Accès au système de fichiers via le protocole TFTP	
Analyse antivirus	Analyse antivirus du système de fichiers	

Remarque - Les UID et les GID de 0 à 99 sont réservés par le fournisseur du système d'exploitation en vue de leur utilisation dans de futures applications. Leur utilisation par des utilisateurs système finaux ou des fournisseurs de produits en couches n'est pas prise en charge et peut entraîner des problèmes de sécurité dans de futures applications.

TABLEAU 49 Services d'annuaire

Service	Description	Ports utilisés
NIS	Authentification des utilisateurs et des groupes à partir d'un service NIS	
LDAP	Authentification des utilisateurs et des groupes à partir d'un répertoire LDAP	389
Active Directory	Authentification des utilisateurs à l'aide d'un serveur Active Directory de Microsoft Remarque - Une fois activé, ce service reste toujours en marche et ne peut pas être désactivé	
Mappage des identités	Mappage entre les entités Windows et les ID UNIX Remarque - Service toujours en marche et impossible à désactiver	

TABLEAU 50 Configuration des services

Service	Description	Ports utilisés
DNS	Client du service de noms de domaine Remarque - Service toujours en marche et impossible à désactiver	53
Dynamic Routing	Protocoles de routage dynamiques RIP et RIPng	
IPMP	Multipathing sur réseau IP pour le basculement IP Remarque - Service toujours en marche et impossible à désactiver	
NTP	Client NTP (Network Time Protocol)	
Phone Home	Enregistrement du produit et configuration du support	8 000 (fonction du port ouvert dans le proxy)
Indicateurs de maintenance	Prise en charge de l'inventaire de produits	6481

Service	Description	Ports utilisés
SMTP	Configuration du serveur de courrier sortant Remarque - Service toujours en marche et impossible à désactiver	
SNMP	SNMP pour l'envoi de déroutements en cas d'alertes et d'informations relatives à l'état de l'appareil	
Syslog	Relais Syslog pour l'envoi des messages syslog en cas d'alertes et le transfert des messages syslog du service	
Identité du système	Nom et emplacement du système Remarque - Service toujours en marche et impossible à désactiver	

TABLEAU 51 Services d'accès distant

Service	Description	Ports utilisés
SSH	SSH pour l'accès à la CLI	22
REST	API RESTful Remarque - Service toujours en marche et impossible à désactiver	

TABLEAU 52 Services de sécurité disponibles

Service	Description	Ports utilisés
Kerberos Realms for NFS	Authentification Kerberos V	88
Modification et définition du mot de passe de Kerberos V (SET_CHANGE)	464	
Modification et définition du mot de passe de Kerberos V (RPCSEC_GSS)	749	

Ports de service requis

Pour assurer la sécurité d'un réseau, vous pouvez créer des pare-feux. Les numéros de port sont utilisés pour la création de règles de pare-feu et pour identifier de manière unique une transaction sur un réseau en indiquant l'hôte et le service.

La liste suivante répertorie les ports minimum requis pour la création de règles du pare-feu qui permettent d'utiliser pleinement l'appareil :

Ports entrants

- icmp/0-65535 (PING)
- tcp/1920 (EM)
- tcp/215 (BUI)

- tcp/22 (SSH)
- udp/161 (SNMP)

Ports sortants

- tcp/80 (WEB)
- tcp/443 (SSL WEB)

Remarque - Un port sortant de tcp/443 est utilisé pour l'envoi de messages Phone Home, le téléchargement de lots de support et la mise à jour de notifications. Pour la réplication, utilisez les tunnels Generic Routing Encapsulation (GRE) lorsque cela est possible. Cela permet au trafic de s'exécuter sur les interfaces arrière et permet d'éviter le pare-feu où le trafic pourrait être ralenti. Si les tunnels GRE ne sont pas disponibles sur le noyau NFS, vous devez exécuter la réplication sur l'interface avant. Dans ce cas, les ports 216 et 217 doivent également être ouverts.

Pour plus d'informations sur les ports Kerberos, reportez-vous à la section "[Configuration des domaines Kerberos pour NFS](#)" à la page 239.

Configuration des services

Pour plus d'informations sur la configuration d'un service, sélectionnez l'un des services répertoriés dans le tableau suivant :

Services de données	Services d'annuaire	Paramètres système	Accès à distance
NFS	NIS	DNS	SSH
iSCSI	LDAP	IPMP	API RESTful
SMB	Active Directory	NTP	
FTP	Mappage des identités	Phone Home	
HTTP		Routage dynamique	
NDMP		Indicateurs de maintenance	
Réplication distante		SMTP	
Migration shadow		SNMP	
SFTP		Syslog	
SRP		Identité du système	
TFTP			
Analyse antivirus			

Rubriques connexes

- "[Liste des services disponibles](#)" à la page 233

Configuration NFS

Network File System (NFS) est un protocole standard du marché qui permet de partager des fichiers sur un réseau. L'appareil Oracle ZFS Storage Appliance prend en charge les versions 2, 3 et 4 du protocole NFS. Pour plus d'informations sur la procédure de construction de l'espace de nom du système de fichiers, reportez-vous à la section ["Utilisation de l'espace de noms du système de fichiers" à la page 404](#). Pour plus d'informations sur le fonctionnement du protocole NFS avec des utilisateurs locaux, reportez-vous à la section ["Configuration des utilisateurs" à la page 160](#).

Pour configurer NFS, reportez-vous aux sections suivantes :

- ["Propriétés du service NFS" à la page 237](#)
- ["Configuration des domaines Kerberos pour NFS" à la page 239](#)
- ["Journaux et analyses NFS" à la page 240](#)
- ["Propriétés NFS" à la page 241](#)
- ["Partage d'un système de fichiers via NFS" à la page 241](#)

Propriétés du service NFS

Les propriétés suivantes du service NFS sont disponibles dans Configuration > Services.

- **Version minimale prise en charge** : cette liste déroulante permet de contrôler les versions de NFS prises en charge par l'appareil.
- **Version maximale prise en charge** : cette liste déroulante permet de contrôler les versions de NFS prises en charge par l'appareil.

Remarque - Si vous définissez une valeur identique pour les versions minimale et maximale de NFS, l'appareil communique uniquement avec les clients ayant recours à cette version. Cela peut être utile si vous rencontrez un problème dans l'une des versions de NFS (p. ex les caractéristiques de performance d'une version NFS avec votre charge de travail) et si vous souhaitez forcer les clients à utiliser uniquement la version la plus performante.

- **Nbre maximal de threads serveur** : définit le nombre maximal de demandes NFS simultanées (de 20 à 1000). Il doit couvrir le nombre de clients NFS simultanés que vous avez anticipés. La valeur par défaut est 500.
- **Période de grâce** : définit le nombre de secondes dont disposent tous les clients pour récupérer l'état de verrouillage après un redémarrage de l'appareil (entre 15 et 600 secondes) à la suite d'une interruption de service inattendue. Cette propriété concerne uniquement les clients NFS v4 (NFS v3 est un protocole sans état, il n'y a donc pas d'état à récupérer). Durant cette période, le service NFS traite uniquement les récupérations d'anciens états de verrouillage. Aucune autre demande d'assistance n'est traitée avant la fin de la période de grâce. La période de grâce par défaut est de 90 secondes. Vous pouvez réduire la

période de grâce pour permettre aux clients NFS de reprendre leur fonctionnement plus rapidement après une réinitialisation de serveur, bien que cela augmente également la probabilité qu'un client ne récupère pas tous ses états de verrouillage. L'appareil Oracle ZFS Storage Appliance fournit une récupération sans grâce de l'état de verrouillage pour les clients NFSv4, pendant les interruptions de service planifiées. Les interruptions de service planifiées interviennent pendant des événements tels que les mises à jour et la réinitialisation de l'appareil à l'aide de la commande CLI `maintenance system reboot`

ou de l'icône d'alimentation de la BUI . Pour les interruptions de service planifiées, le service NFS traite toutes les demandes d'assistance sans engager de délai de période de grâce.

- **Domaine d'identité NFSv4 personnalisé** : cette propriété permet de définir le domaine en vue de mapper les identités des utilisateurs et des groupes NFSv4. Si vous ne définissez pas cette propriété, les appareils utilisent le système de noms de domaine pour obtenir le domaine de l'identité, en commençant par rechercher un enregistrement de ressource DNS `_nfsv4idmapdomain` avant de revenir au domaine DNS lui-même.
- **Utiliser des chaînes d'ID numériques NFSv4** : cette propriété permet aux clients NFSv4 d'utiliser des chaînes numériques pour les ID utilisateur et groupe. Si cette propriété n'est pas définie correctement, par défaut les ID utilisateur et groupe sont échangés sous la forme `utilisateur@domaine`. Cette propriété s'applique uniquement si le type d'authentification est `AUTH_SYS`. La propriété de la CLI est `use_numeric_ids`.
- **Activer la délégation NFSv4** : sélectionnez cette propriété pour autoriser les clients à mettre en cache les fichiers localement et à apporter des modifications sans contacter le serveur. Cette option est activée par défaut et entraîne généralement une amélioration des performances. Dans de rares cas, elle peut entraîner des problèmes. Ne désactivez ce paramètre qu'après avoir soigneusement mesuré les performances de votre charge de travail et qu'une fois assuré qu'il représente une amélioration quantifiable des performances. Cette option s'applique uniquement aux montages NFSv4.
- **Visibilité du montage** : cette propriété vous permet de limiter la disponibilité des informations concernant les listes d'accès au partage et les montages à distance à partir des clients NFS. `Full` permet un accès complet. `Restricted` limite l'accès de sorte qu'un client ne peut voir que les partages auquel il peut accéder. Un client ne peut pas voir les listes d'accès des partages définis dans le serveur ou les montages effectués depuis le serveur par d'autres clients. Par défaut, cette propriété est définie sur `Full`.
- **Activer Kerberos** : active/désactive le service Kerberos.
 - **Allow weak encryption types in Kerberos** : active/désactive la prise en charge du DES (`des-cbc-crc`, `des-cbc-md5`) et de l'algorithme de chiffrement ArcFour d'export avec `HMAC/md5` (`arcfour-hmac-exp`). Cette propriété est désactivée par défaut.
 - **Kerberos realm** : un domaine désigne un réseau logique qui définit un groupe de systèmes situé sous un même centre de distribution de clés (KDC) maître. Les noms de domaine peuvent contenir n'importe quelle chaîne ASCII. De manière générale, votre nom de domaine Kerberos est identique à votre nom de domaine DNS, à cette différence près qu'il est en majuscule. Cette convention vous aide à distinguer les problèmes qui surviennent dans le service Kerberos et dans l'espace de noms DNS, tout en continuant d'utiliser un nom familier.

- **Kerberos master KDC** : dans chaque domaine, vous devez inclure un serveur qui conserve une copie maître de la base de données des identités (principal). La différence la plus significative entre un KDC maître et un KDC esclave est que seul le KDC maître gère les demandes d'administration de la base de données. Par exemple, vous devez modifier un mot de passe ou ajouter une nouvelle identité au niveau du KDC maître.
- **Kerberos slave KDC** : l'esclave contient des copies de duplication de la base de données des identités (principal). Le serveur KDC maître et le serveur KDC esclave créent tous deux des tickets permettant d'établir l'authentification.
- **Kerberos admin principal** : cette propriété identifie l'administrateur. Par convention, un nom de principal est divisé en trois composants : le primaire, l'instance et le domaine. Vous pouvez spécifier une identité en tant que joe, joe/admin ou joe/admin@ENG.EXAMPLE.COM. Cette propriété est utilisée dans l'unique but de définir les identités du service Kerberos ; elle n'est pas conservée.
- **Kerberos admin password** : définit un mot de passe pour l'administrateur. Cette propriété est utilisée dans l'unique but de définir les identités du service Kerberos ; elle n'est pas conservée.
- **Oracle Intelligent Storage Protocol** : le service NFSv4 inclut la prise en charge du protocole OISP (Oracle Intelligent Storage Protocol), qui permet aux clients Oracle Database NFSv4 de transmettre des informations d'optimisation au serveur ZFS Storage Appliance NFSv4. Pour plus d'informations, reportez-vous à la section "[Protocole OISP \(Oracle Intelligent Storage Protocol\)](#)" à la page 645.

Rubriques connexes

- "[Propriétés NFS](#)" à la page 241
- Définition des propriétés du service [BUI](#), [CLI](#).

Configuration des domaines Kerberos pour NFS

La configuration d'un domaine Kerberos crée des identités de service et ajoute les clés nécessaires au fichier keytab local du système. Le NTP service doit être configuré avant la configuration d'un système NFS utilisant Kerberos. Les identités de service suivantes sont créées et mises à jour pour prendre en charge le système NFS kerberisé :

```
host/node1.example.com@EXAMPLE.COM
nfs/node1.example.com@EXAMPLE.COM
```

Si vos appareils sont regroupés en cluster, des identités et des clés sont générées pour chaque noeud du cluster :

```
host/node1.example.com@EXAMPLE.COM
nfs/node1.example.com@EXAMPLE.COM
host/node2.example.com@EXAMPLE.COM
nfs/node2.example.com@EXAMPLE.COM
```

Si ces identités ont déjà été créées, la configuration du domaine réinitialise le mot de passe de chacune des identités.

Pour plus d'informations sur la configuration des KDC et des clients Kerberos, reportez-vous à la section [Oracle Solaris 11.1 Administration: Security Services \(http://docs.oracle.com/cd/E26502_01/html/E29015/index.html\)](http://docs.oracle.com/cd/E26502_01/html/E29015/index.html). Après avoir configuré des propriétés NFS pour Kerberos, remplacez le mode Security dans l'écran Partages->Système de fichiers->Protocoles par un mode utilisant Kerberos.

Les ports suivants sont utilisés par l'appareil pour Kerberos.

- Authentification Kerberos V : 88
- Modification et définition du mot de passe SET_CHANGE de Kerberos V : 464
- Modification et définition du mot de passe RPCSEC_GSS de Kerberos V : 749

Remarque - Les clients NFS kerberisés doivent accéder à l'appareil à l'aide d'une adresse IP qui résout ces identités en un nom de domaine complet (FQDN). Par exemple, si un appareil est configuré avec plusieurs adresses IP, seule l'adresse IP qui résout le FQDN de l'appareil peut être utilisée par les clients NFS Kerberized.

Journaux et analyses NFS

Les journaux suivants sont disponibles pour le service NFS :

TABLEAU 53 Journaux disponibles pour NFS

Journal	Description
network-nfs-server:default	Journal du serveur NFS maître
appliance-kit-nfsconf:default	Journal des événements de configuration NFS de l'appareil
network-nfs-cbd:default	Journal du démon callback NFSv4
network-nfs-mapid:default	Journal du démon mapid NFSv4 qui mappe les informations d'identification des utilisateur et des groupes NFSv4
network-nfs-status:default	Journal du démon statd NFS qui assiste les fonctions de panne et de récupération pour les verrous NFS
network-nfs-nlockmgr:default	Journal du démon lockd NFS qui prend en charge les opérations de verrouillage des enregistrements des fichiers

Vous pouvez surveiller l'activité NFS dans la section Analyse. Elle comprend les éléments suivants :

- Opérations NFS par seconde
- ... par type d'opération (lecture/écriture/...)
- ... par nom de partage

- ... par nom d'hôte du client
- ... par nom de fichier consulté
- ... par latence de l'accès

Propriétés NFS

Le tableau suivant décrit le mappage entre les propriétés de la CLI et les descriptions des propriétés de la BUI ci-dessus.

TABLEAU 54 Propriétés NFS

Propriété de la CLI	Propriété de la BUI
version_min	Version minimale prise en charge
version_max	Version maximale prise en charge
nfsd_servers	Nb maximal de threads serveur
grace_period	Période de grâce
mapid_domain	Domaine d'identité NFSv4 personnalisé
use_numeric_ids	Utiliser les ID chaîne numériques NFSv4
enable_delegation	Activer la délégation NFSv4
mount_visibility	Niveau de restriction des informations de partage du client
krb5_allow_weak_crypto	Autorise les types de chiffrement faibles (arcfour-hmac-md5-exp, des-cbc-md5 et des-cbc-crc) dans Kerberos
krb5_realm	Domaine Kerberos
krb5_kdc	KDC maître Kerberos
krb5_kdc2	KDC esclave Kerberos
krb5_admin	Principal admin Kerberos

▼ Partage d'un système de fichiers via NFS

1. **Accédez à Configuration > Services.**
2. **Assurez-vous que le service NFS est activé et en ligne. Si ce n'est pas le cas, activez-le.**
3. **Accédez à l'écran Partages puis modifiez un partage ou créez-en un nouveau.**
4. **Cliquez sur l'onglet Protocoles du partage que vous modifiez et vérifiez que le partage NFS est activé.**

Vous pouvez également configurer le mode du partage NFS (lecture/lecture+écriture) de cet écran.

Configuration iSCSI

Lorsque vous configurez un LUN sur l'appareil, vous pouvez exporter ce volume via une cible iSCSI (Internet Small Computer System Interface). Le service iSCSI permet aux initiateurs iSCSI d'accéder aux cibles par le biais du protocole iSCSI.

Le service prend en charge la détection, la gestion et la configuration à l'aide du protocole iSNS. Le service iSCSI prend en charge l'authentification unidirectionnelle (la cible authentifie l'initiateur) et bidirectionnelle (la cible et l'initiateur s'authentifient mutuellement) par le biais du protocole CHAP. De plus, le service prend en charge la gestion des données d'authentification CHAP dans une base de données RADIUS.

Le système commence par effectuer l'authentification puis l'autorisation au cours de deux étapes indépendantes.

Remarque - Pour consulter des exemples de configuration des cibles et des initiateurs iSCSI, reportez-vous à la section "[Configuration du réseau de stockage SAN](#)" à la page 127.

TABLEAU 55 Propriétés du service iSCSI

Propriété	Description
Utiliser iSNS	La détection iSNS est activée.
Serveur iSNS	Serveur iSNS
Utiliser RADIUS	RADIUS est activé.
Serveur RADIUS	Serveur RADIUS
Secret Serveur RADIUS	Clé secrète du serveur RADIUS

Si l'initiateur local possède un nom et une clé secrète CHAP, le système procède à l'authentification. Si l'initiateur local ne possède pas de propriétés CHAP, le système n'effectue pas d'authentification et tous les initiateurs sont éligibles à l'autorisation.

Le service iSCSI vous permet de spécifier une liste globale d'initiateurs que vous pouvez utiliser au sein de groupes d'initiateurs.

Si l'initiateur ne parvient pas à se connecter à la cible :

- Assurez-vous que l'IQN de l'initiateur correspond à l'IQN identifié dans la liste d'initiateurs.
- Assurez-vous que l'adresse IP du serveur iSNS est correcte et que le serveur iSNS est configuré.
- Vérifiez que l'adresse IP de la cible est correcte côté initiateur.
- Vérifiez que les noms et clés secrètes CHAP sont identiques des deux côtés.
- Vérifiez que le nom et la clé secrète CHAP de la cible ne correspondent pas à ceux d'un des initiateurs.

- Assurez-vous que l'adresse IP et la clé secrète du serveur RADIUS sont correctes et que le serveur RADIUS est configuré.
- Assurez-vous que l'initiateur qui accède au LUN est un membre du groupe d'initiateurs de ce LUN.
- Vérifiez que les cibles chargées d'exporter cette unité logique sont en ligne.
- Vérifiez que le statut de fonctionnement du LUN est en ligne.
- Vérifiez le numéro d'unité logique de chaque LUN.

Si, au cours du basculement/rétablissement, les E/S de la copie réduite iSER du client Red Hat ne sont plus fonctionnelles, modifiez le paramètre `node.session.timeo.replacement_timeout` dans le fichier `/etc/iscsi/iscsid.conf` pour lui donner une valeur de 300sec.

Rubriques connexes

- Définition des propriétés du service [BUI](#), [CLI](#)

Configuration SMB

Le service SMB fournit un accès aux systèmes de fichiers par le biais du protocole SMB. Les version SMB prises en charge sont : SMB 1, SMB 2.0 et SMB 2.1. Pour partager des systèmes de fichiers via SMB, configurez le système de fichiers comme décrit dans la section "[Propriétés des systèmes de fichiers](#)" à la page 384. Le tableau suivant présente les fonctions prises en charge et non prises en charge de SMB 2.1.

TABLEAU 56 Fonctions prises en charge et non prises en charge de SMB 2.1

FONCTIONS PRISES EN CHARGE	FONCTIONS NON PRISES EN CHARGE
Crédits-bails	Mémoire cache de branche
Demande de négociation à plusieurs protocoles	Handles résistants
Opérations d'écriture synchrone individuelles	
Opérations à plusieurs crédits	

Les comptes locaux et les ID utilisateur sont mappés vers les ID utilisateur Windows. Notez que le compte *guest* est un compte spécial, en lecture seule, et qu'il ne peut pas être configuré pour des opérations de lecture/écriture sur l'appareil.

Pour configurer SMB, reportez-vous aux sections suivantes :

- "[Propriétés du service SMB](#)" à la page 244
- "[Définition des propriétés pour exporter des partages via SMB](#)" à la page 245
- "[Interopérabilité NFS/SMB](#)" à la page 246
- "[Espaces de noms DFS SMB](#)" à la page 247

- ["Matrice de support des outils de gestion des espaces de noms DFS autonomes de Microsoft fonctionnant via SMB" à la page 247](#)
- ["Ajout d'espaces de noms à un groupe SMB local" à la page 249](#)
- ["SMB Autohome" à la page 249](#)
- ["Ajout de règles SMB autohome \(CLI\)" à la page 250](#)
- ["Ajout d'un utilisateur à un groupe SMB local" à la page 251](#)
- ["Intégration de MMC via SMB" à la page 252](#)
- ["Gestion des partages SMB" à la page 253](#)
- ["Utilisateurs, groupes et connexions SMB" à la page 254](#)
- ["Etablissement de la liste des Services SMB" à la page 256](#)
- ["Configuration du service \(BUI\)" à la page 258](#)
- ["Configuration d'Active Directory pour SMB \(BUI\)" à la page 260](#)
- ["Configuration d'un projet et d'un partage SMB \(BUI\)" à la page 260](#)
- ["Configuration du service de données SMB \(BUI\)" à la page 261](#)

Propriétés du service SMB

La procédure de modification des propriétés de service est documentée dans les sections ["Définition des propriétés du service \(BUI\)" à la page 230](#) et ["Définition des propriétés du service \(CLI\)" à la page 231](#).

- **Commentaire système** : chaîne de texte compréhensible.
- **Expiration de session inactive** : réglage du délai d'expiration d'une session pour cause d'inactivité.
- **Contrôleur de domaine préféré** : contrôleur de domaine à utiliser de préférence lorsque vous rejoignez un domaine Active Directory. Si ce contrôleur n'est pas disponible, Active Directory se fie aux enregistrements SRV DNS et au site Active Directory pour localiser un contrôleur de domaine approprié. Pour plus d'informations, reportez-vous à la section ["Configuration d'Active Directory" à la page 293](#).
- **Site Active Directory** : site à utiliser lorsque vous joignez un domaine Active Directory. Un site est un ensemble logique de machines toutes connectées par bande passante élevée avec des liaisons réseau à faible latence. Lorsque cette propriété est configurée et que le contrôleur de domaine préféré n'est pas spécifié, le fait de rejoindre un domaine Active Directory privilégie les contrôleurs de domaine situés dans ce site par rapport aux contrôleurs de domaine externes.
- **# Maximal de threads serveur** : nombre maximal de threads (processus) serveur simultanés. La valeur par défaut est 1024.
- **Activation du DNS dynamique** : décide si l'appareil utilise le DNS dynamique pour mettre à jour les enregistrements DNS dans le domaine Active Directory. La valeur par défaut est "désactivé".
- **Activation Oplocks** : décide si l'appareil octroie des verrous opportunistes aux clients SMB. Cela améliore les performances pour la plupart des clients. La valeur par défaut est

on. Le serveur SMB octroie un verrou opportuniste à un processus client afin que celui-ci puisse placer des données dans le cache lorsque le verrou est en place. Lorsque le serveur révoque le verrou opportuniste, le client vide ses données en cache sur le serveur.

- **Restriction d'accès anonyme aux listes de partage** : si cette option est activée, les clients doivent s'authentifier auprès du service SMB avant de recevoir une liste de partages. Si elle est désactivée, les clients anonymes peuvent accéder à la liste de partages.
- **Serveur WINS principal** : adresse WINS principale définie dans la configuration TCP/IP.
- **Serveur WINS secondaire** : adresse WINS secondaire définie dans la configuration TCP/IP.
- **Adresses IP exclues de WINS** : adresses IP exclues de l'inscription avec WINS.
- **Niveau de compatibilité de LAN Manager** : modes d'authentification pris en charge (LM, NTLM, LMv2, NTLMv2). Pour plus d'informations sur les modes d'authentification pris en charge dans chaque niveau de compatibilité, consultez le document Oracle Solaris Information Library pour *smb*. NTLMv2 est le niveau de sécurité minimal recommandé pour éviter les failles de sécurité connues du public.
- **Signature SMB activée** : active l'interopérabilité avec les clients SMB à l'aide de la fonction de signature SMB. Lorsqu'un paquet est signé, la signature est vérifiée. Lorsqu'un paquet n'est pas signé, il est accepté sans vérification de signature (si la signature SMB n'est pas requise : voir ci-dessous).
- **Signature SMB requise** : lorsque la signature SMB est requise, tous les paquets SMB doivent être signés, faute de quoi ils sont rejetés. Les clients qui ne prennent pas en charge la signature ne peuvent donc pas se connecter au serveur.
- **Ignorer zéro VC** : lorsqu'un client SMB établit une nouvelle connexion, il peut demander à l'appareil de nettoyer toutes les connexions précédentes et de classer les verrous de ce client en spécifiant un nombre de circuits virtuels (VC) de zéro. Cependant, cet artefact de protocole ne respecte pas la traduction d'adresses réseau (NAT) pour les clients ou les entrées DNS multiples assignées au même hôte. En parallèle, zéro demandes VC entre des emplacements réseau masqués peuvent engendrer la réinitialisation de connexions actives sans lien. Par défaut, la condition "zéro demandes VC" est respectée afin d'empêcher le verrouillage de fichiers périmés. Cependant, si une erreur engendre la fermeture de sessions SMB, le problème peut être résolu en ignorant la condition "zéro demandes VC".

Définition des propriétés pour exporter des partages via SMB

Plusieurs propriétés de partage doivent être définies lors de l'exportation d'un partage via SMB.

TABEAU 57 Propriétés des partages SMB

Propriété	Description
Sensibilité à la casse	Les clients SMB s'attendent à un comportement sensible à la casse, cette propriété peut donc être "mixed" ou "insensitive". Voir " Propriétés statiques " à la page 373.
Rejeter non UTF-8	Lorsque les noms de fichiers qui ne sont pas au format UTF-8 sont autorisés dans un système de fichiers, les

Propriété	Description
	clients SMB risquent de ne pas fonctionner correctement. Voir "Propriétés statiques" à la page 373.
Verrouillage obligatoire non bloquant	Cette propriété doit être activée pour autoriser le verrouillage par plage d'octets à fonctionner correctement. Voir "Propriétés statiques" à la page 373.
Nom de la ressource	Nom utilisé par les clients pour désigner le partage. Pour plus d'informations sur la façon dont ce nom est hérité d'un projet, reportez-vous à la section "Protocoles de partage et de projet" à la page 407.
ACL au niveau du partage	ACL qui ajoute une couche de contrôle d'accès en plus des ACL stockées dans le système de fichiers. Pour plus d'informations sur cette propriété, reportez-vous à la section "Listes de contrôle d'accès des systèmes de fichiers" à la page 420.

Les propriétés Sensibilité à la casse et Rejeter non UTF-8 peuvent être définies uniquement lors de la création d'un partage.

Deux partages SMB présents sur le même système ne peuvent pas avoir le même nom de ressource. Les noms de ressources hérités de projets ont un comportement spécifique. Pour plus d'informations, reportez-vous à la section ["Partages et projets" à la page 343.](#) Il est limité à 80 caractères et peut contenir tout caractère alphanumérique (A-Z, a-z, 0-9), des espaces et les caractères spéciaux suivants :

" / \ [] : | < > + ; , ? * =

Lorsque la propriété d'énumérations en fonction des accès est activée, les clients peuvent voir des entrées de répertoire des fichiers qu'ils ne peuvent pas ouvrir. Les entrées de répertoire sont filtrées uniquement lorsque le client n'a pas accès au fichier. Par exemple, si un client tente d'ouvrir un fichier avec un accès en lecture-écriture alors que l'ACL n'attribue qu'un accès en lecture, l'ouverture du fichier échoue mais ce fichier est quand même inclus dans la liste des entrées.

Interopérabilité NFS/SMB

L'appareil prend en charge les clients NFS et SMB qui accèdent simultanément aux mêmes partages. Afin de configurer correctement l'appareil pour l'interopérabilité NFS/SMB, configurez les composants suivants :

- Configurez le service Active Directory . Reportez-vous à la section ["Configuration d'Active Directory" à la page 293.](#)
- Etablissez une stratégie de mappage des identités et configurez le service. Reportez-vous à la section ["Configuration du mappage des identités" à la page 299.](#)
- Configurez le protocole SMB. Reportez-vous à la section ["Configuration SMB" à la page 243.](#)

- Configurez le contrôle d'accès, les entrées ACL et l'héritage ACL sur les partages.

SMB et NFSv3 n'utilisent pas le même modèle de contrôle d'accès. Pour des résultats optimaux, configurez l'ACL sur le répertoire root à partir d'un client SMB avec un modèle détaillé de contrôle d'accès SMB. Pour plus d'informations sur les entrées ACL triviales pouvant être héritées, reportez-vous à la section "[Listes de contrôle d'accès des systèmes de fichiers](#)" à la page 420.

Espaces de noms DFS SMB

DFS (Distributed File System, système de fichiers distribué) est une technologie de virtualisation fournie via les protocoles SMB et MSRPC. DFS permet aux administrateurs de regrouper des dossiers partagés situés sur des serveurs différents en les connectant de façon transparente à un ou plusieurs espaces de noms DFS. Un espace de nom DFS est une représentation virtuelle de dossiers partagés au sein d'une organisation. Un administrateur peut sélectionner les dossiers partagés à présenter dans l'espace de noms, concevoir la hiérarchie de présentation de ces dossiers et déterminer les noms affichés par les dossiers partagés dans l'espace de noms. Lorsqu'un utilisateur affiche l'espace de noms, les dossiers semblent résider dans un seul système de fichiers à haute capacité. Les utilisateurs peuvent accéder aux dossiers de l'espace de noms sans avoir l'obligation de connaître le nom du serveur ou du dossier partagé hébergeant les données.

Seul un partage par système peut être alloué en tant qu'espace de noms DFS autonome. Les espaces de noms DFS basés sur un domaine ne sont pas pris en charge. Notez qu'un espace de noms DFS peut être alloué par cluster, même si chaque noeud de cluster comporte un pool de stockage distinct. Pour allouer un partage SMB en tant qu'espace de noms DFS, utilisez le composant logiciel enfichable MMC de gestion DFS pour créer un espace de noms autonome.

Lorsque l'appareil n'est pas joint à un domaine Active Directory, une configuration supplémentaire est nécessaire pour permettre aux utilisateurs du groupe de travail de modifier les espaces de noms DFS. Pour qu'un utilisateur local SMB puisse créer ou supprimer un espace de noms DFS, il doit posséder un compte local distinct créé sur le serveur. Pour plus d'informations sur les étapes à suivre pour permettre à l'utilisateur local SMB `dfsadmin` de manipuler les espaces de noms DFS, reportez-vous à la section "[Ajout d'espaces de noms à un groupe SMB local](#)" à la page 249.

Matrice de support des outils de gestion des espaces de noms DFS autonomes de Microsoft fonctionnant via SMB

La table suivante répertorie les opérations (sous-commandes/options) des outils DFS de Microsoft sur plusieurs versions de systèmes d'exploitation Windows. Elle identifie ceux pris en charge par le service DFS sur l'appareil pour la gestion d'un espace de noms DFS autonome sur cet appareil.

- **y** - pris en charge
- **n** - non pris en charge
- **NA** - non applicable

Microsoft Windows systems	XP	2003	2003	Vista	2008	2008	Win7
			R2			R2	
	SP3	SP2	SP2	SP2	SP2	SP1	SP1
dfscmd CLI:							
/map [comment] [/restore]	y	y	y	y	y	y	y
/unmap	y	y	y	y	y	y	y
/add [/restore]	y	y	y	y	y	y	y
/remove	y	y	y	y	y	y	y
/view [/partial /full]	y	y	y	y	y	y	y
dfsutil CLI (old format):							
/addstdroot [/comment]	y	y	y	n	n	y	y
/remstdroot	y	y	y	n	n	y	y
/root:<DfsName> /view	n	n	n	y	y	y	y
/addlink [/comment]	NA	NA	NA	y	y	y	y
/removelink	NA	NA	NA	y	y	y	y
/state /display	NA	NA	NA	y	y	y	y
/state /enable	NA	NA	NA	y	y	y	y
/state /disable	NA	NA	NA	y	y	y	y
/ttl /display	NA	NA	NA	y	y	y	y
/ttl /set	NA	NA	NA	y	y	y	y
/server:<MachineName> /view	y	y	y	y	y	y	y
dfsutil CLI (new format):							
root addstd [comment]	NA	NA	NA	n	n	y	y
root remove	NA	NA	NA	n	n	y	y
root (view namespace)	NA	NA	NA	y	y	y	y
link add [comment]	NA	NA	NA	y	y	y	y
link remove	NA	NA	NA	y	y	y	y
link (view)	NA	NA	NA	y	y	y	y
target add	NA	NA	NA	y	y	y	y
target remove	NA	NA	NA	y	y	y	y
target (view)	NA	NA	NA	y	y	y	y
property comment (view)	NA	NA	NA	y	y	y	y
property comment set	NA	NA	NA	y	y	y	y
property ttl (view)	NA	NA	NA	y	y	y	y
property ttl set	NA	NA	NA	y	y	y	y
property state (view)	NA	NA	NA	y	y	y	y
property state offline	NA	NA	NA	y	y	y	y
property state online	NA	NA	NA	y	y	y	y
DFS GUI:							

add standalone root	y	y	y	n	n	n	n
remove standalone root	y	y	y	n	n	n	n
change root comment	y	y	y	n	n	n	n
change root timeout	y	y	y	n	n	n	n
add link	y	y	y	n	n	n	n
remove link	y	y	y	n	n	n	n
change link comment	y	y	y	n	n	n	n
change link timeout	y	y	y	n	n	n	n
add link's target	y	y	y	n	n	n	n
remove link's target	y	y	y	n	n	n	n
enable link's referral (target)	y	y	y	n	n	n	n
disable link's referral (target)	y	y	y	n	n	n	n
hide root	y	y	y	y	y	y	y
show root	y	y	y	y	y	y	y
display links	y	y	y	n	n	n	n
display targets	y	y	y	n	n	n	n
	XP	2003	2003	Vista	2008	2008	Win7
			R2			R2	
	SP3	SP2	SP2	SP2	SP2	SP1	SP1

Prenez en compte les éléments suivants :

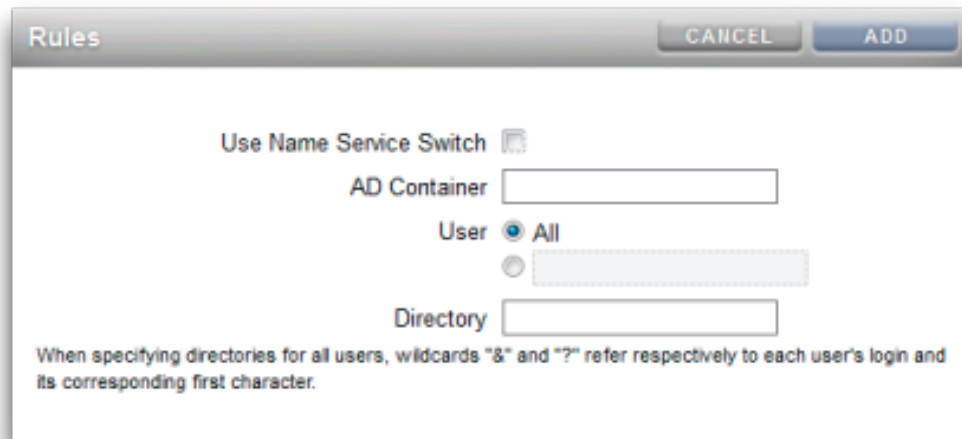
- Solaris ne vérifie pas la cible de lien DFS.
- Les commandes de la CLI permettant la modification et l'affichage de commentaires et du délai d'attente (TTL) s'appliquent à la racine et au lien.
- Les commandes de la CLI permettant l'affichage de l'état s'appliquent à la racine, à sa cible, au lien et à sa cible.
- Les commandes de la CLI permettant la modification de l'état s'appliquent uniquement au lien et à sa cible.

▼ Ajout d'espaces de noms à un groupe SMB local

1. **Créez un compte utilisateur local sur le serveur pour l'utilisateur `dfsadmin`. Veillez à utiliser le même mot de passe qu'au moment de la création de l'utilisateur local sur la machine Windows.**
2. **Ajoutez `dfsadmin` aux administrateurs du groupe SMB local.**
3. **Connectez-vous en tant que `dfsadmin` sur la machine Windows à partir de laquelle vous souhaitez modifier l'espace de noms DFS.**

SMB Autohome

Pour le partage de fichiers Windows, Autohome fournit un accès aux systèmes de fichiers par le biais du protocole SMB. Autohome définit et conserve les partages du répertoire personnel pour les utilisateurs qui accèdent au système via SMB. Les règles autohome mappent les clients SMB aux répertoires personnels.

FIGURE 25 Définition de règles autohome

- **Utiliser le commutateur du service de noms** : permet d'activer ou de désactiver le commutateur de noms (NSS). Il est impossible de créer une règle NSS et une règle autohome simultanément pour chaque utilisateur.
- **Conteneur AD** : définit le conteneur Active Directory, par exemple : dc=com, dc=fishworks, ou=Engineering,CN=myhome.
- **Utilisateur** : définit la règle autohome pour tous les utilisateurs ou pour l'utilisateur spécifié. Lorsque vous spécifiez un utilisateur, les caractères génériques "&" et "?" font référence à l'identification d'un utilisateur et au premier caractère qui lui correspond.
- **Répertoire** : définit le répertoire de la règle, par exemple : /export/wdp.

▼ Ajout de règles SMB autohome (CLI)

1. **Accédez à configuration services smb.**
2. **La commande create permet d'ajouter des règles autohome et la commande list de répertorier des règles existantes.**

Cet exemple ajoute une règle pour l'utilisateur "Bill" avant de répertorier les règles :

```
hostname:> configuration services smb
hostname:configuration services smb> create
hostname:configuration services rule (uncommitted)> set use_nss=false
hostname:configuration services rule (uncommitted)> set user=Bill
hostname:configuration services rule (uncommitted)> set directory=/export/wdp
hostname:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
```

```

ou=Engineering,CN=myhome"
hostname:configuration services rule (uncommitted)> commit
hostname:configuration services smb> list
RULE      NSS      USER      DIRECTORY      CONTAINER
rule-000  false   Bill      /export/wdp     dc=com,dc=fishworks,
ou=Engineering,CN=myhome

```

3. Créez des règles autohome en utilisant des caractères génériques.

L'esperluette & correspond au nom de l'utilisateur et le point d'interrogation ? à la première lettre du nom de l'utilisateur. Les éléments suivants utilisent des caractères génériques pour correspondre à tous les utilisateurs :

```

hostname:configuration services smb> create
hostname:configuration services rule (uncommitted)> set use_nss=false
hostname:configuration services rule (uncommitted)> set user=*
hostname:configuration services rule (uncommitted)> set directory=/export/?/&
hostname:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
ou=Engineering,CN=myhome"
hostname:configuration services rule (uncommitted)> commit
hostname:configuration services smb> list
RULE      NSS      USER      DIRECTORY      CONTAINER
rule-000  false   Bill      /export/wdp     dc=com,dc=fishworks,
ou=Engineering,CN=myhome

```

4. Le commutateur du service de noms (nss) peut également être utilisé pour la création de règles autohome :

```

hostname:configuration services smb> create
hostname:configuration services rule (uncommitted)> set use_nss=true
hostname:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
ou=Engineering,CN=myhome"
hostname:configuration services rule (uncommitted)> commit
hostname:configuration services smb> list
RULE      NSS      USER      DIRECTORY      CONTAINER
rule-000  true     Bill      /export/wdp     dc=com,dc=fishworks,
ou=Engineering,CN=myhome

```

▼ Ajout d'un utilisateur à un groupe SMB local

Les groupes locaux désignent des groupes d'utilisateurs de domaine et/ou locaux qui confèrent des privilèges supplémentaires à ces utilisateurs.

Groupes SMB locaux :

- **Administrateurs** : les administrateurs peuvent contourner les autorisations d'accès aux fichiers pour modifier la propriété des fichiers.
- **Opérateurs de sauvegarde** : les opérateurs de sauvegarde peuvent contourner les contrôles d'accès aux fichiers pour sauvegarder et restaurer des fichiers.

1. Accédez à configuration services smb groups.

```
hostname:configuration services smb> groups
```

2. Saisissez create.

```
hostname:configuration services smb groups> create
```

3. Indiquez l'utilisateur à ajouter au groupe :

```
hostname:configuration services smb member (uncommitted)> set user=Bill
```

4. Saisissez le nom du groupe, puis validez la modification :

```
hostname:configuration services smb member (uncommitted)> set group="Backup Operators"
hostname:configuration services smb member (uncommitted)> commit
```

5. Entrez la commande list pour vérifier que l'utilisateur a été ajouté au groupe spécifié :

```
hostname:configuration services smb groups> list
MEMBER      USER                GROUP
member-000  WINDOMAIN\Bill      Backup Operators
```

Intégration de MMC via SMB

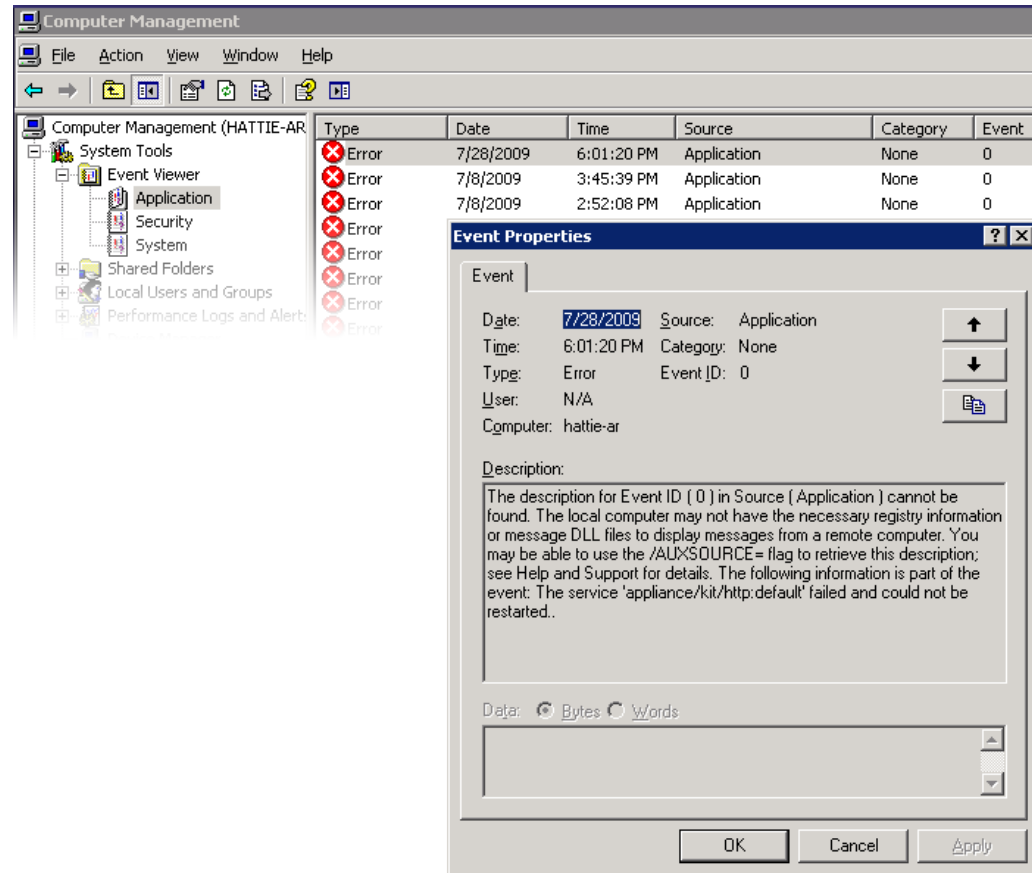
Microsoft Management Console (MMC) est une infrastructure extensible de composants enregistrés, appelés composants logiciels enfichables, qui offre des fonctionnalités de gestion complète pour le système local et des systèmes distants du réseau. Computer Management est un ensemble d'outils de Microsoft Management Console qui permet de configurer, surveiller et gérer les services et les ressources à distance et en local.

Pour utiliser la fonctionnalité MMC sur les appareils Oracle ZFS Storage Appliance en mode groupe de travail, veillez à ajouter l'administrateur Windows qui doit utiliser la console de gestion dans le groupe local des administrateurs de l'appareil. Autrement, l'erreur Access is denied ou une erreur similaire s'affiche dans le client d'administration lors de la tentative de connexion à l'appareil via la console MMC.

Les appareils Oracle ZFS Storage Appliance prennent en charge les fonctions suivantes de gestion de l'ordinateur :

Le composant logiciel enfichable de la MMC de l'Observateur d'événements prend en charge l'affichage du journal de l'application, du journal de sécurité et du journal système. Ces journaux englobent le contenu des journaux d'alertes, d'audit et système de l'appareil Oracle ZFS Storage.

La capture d'écran ci-dessous illustre le journal de l'application et la boîte de dialogue des propriétés en cas d'erreur.

FIGURE 26 Observateur d'événements SMB

Gestion des partages SMB

La prise en charge de la gestion des partages inclut les éléments suivants :

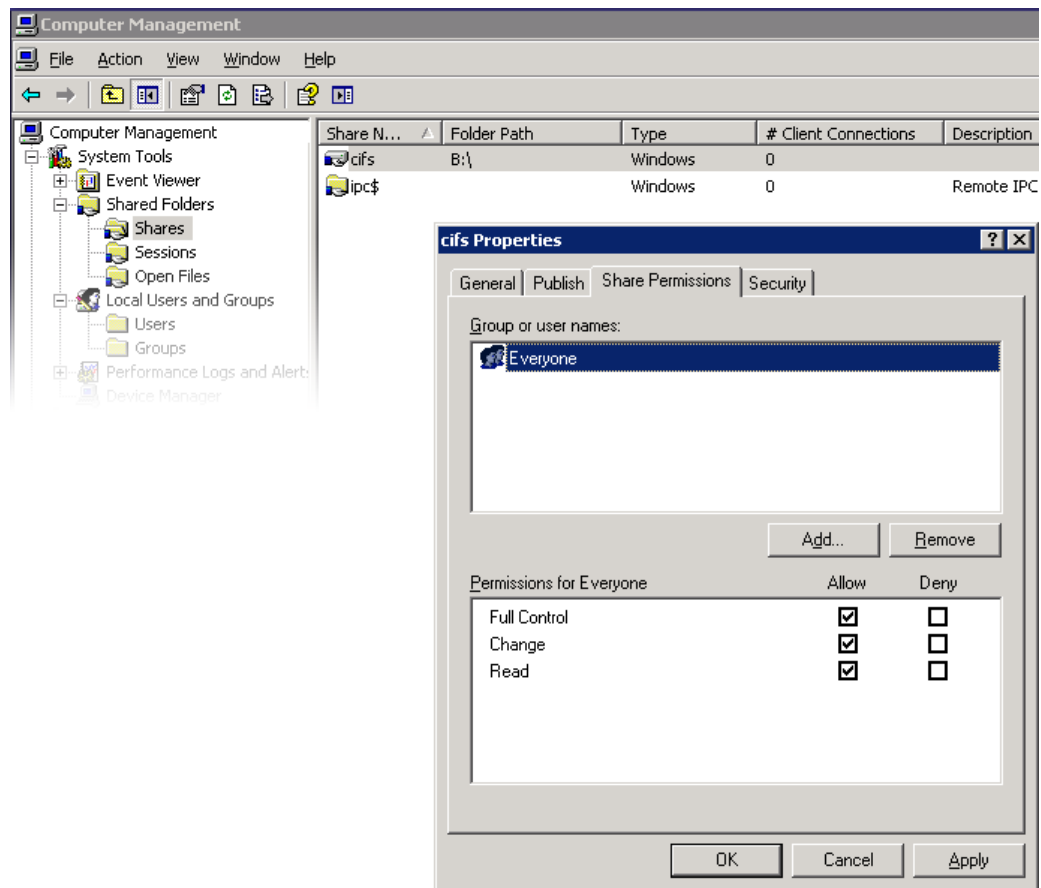
- Etablissement de la liste des partages
- Définition des ACL sur les partages
- Modification des autorisations de partage
- Définition de la description d'un partage

Les fonctionnalités qui ne sont pas prises en charge par la MMC actuellement comprennent les suivantes :

- Ajout ou suppression d'un partage
- Définition de la propriété de mise en cache côté client
- Définition du nombre maximal autorisé de propriétés d'utilisateurs

La capture d'écran suivante illustre les propriétés d'autorisation d'un partage.

FIGURE 27 Propriétés des autorisations de partage SMB



Utilisateurs, groupes et connexions SMB

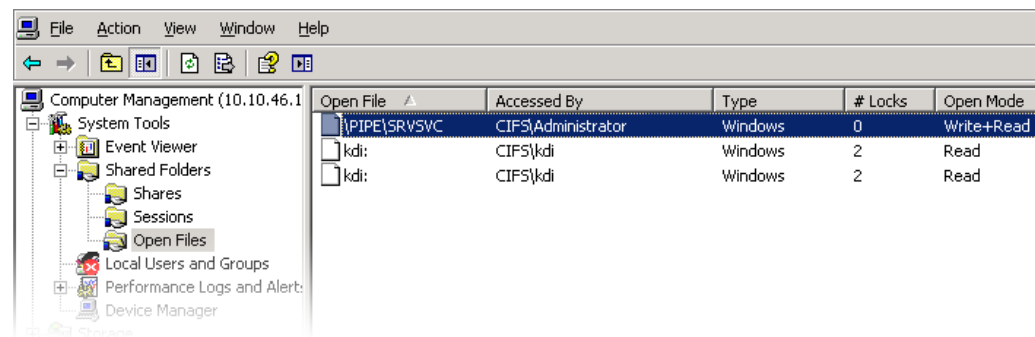
Les fonctionnalités suivantes sont prises en charge :

- Affichage des utilisateurs et des groupes SMB locaux

- Etablissement de la liste des connexions utilisateur, précisant le nombre de fichiers ouverts par connexion
- Fermeture des connexions utilisateur
- Etablissement de la liste des fichiers ouverts, précisant le nombre de verrous sur chaque fichier et le mode (lecture, écriture, etc.)
- Fermeture des fichiers ouverts

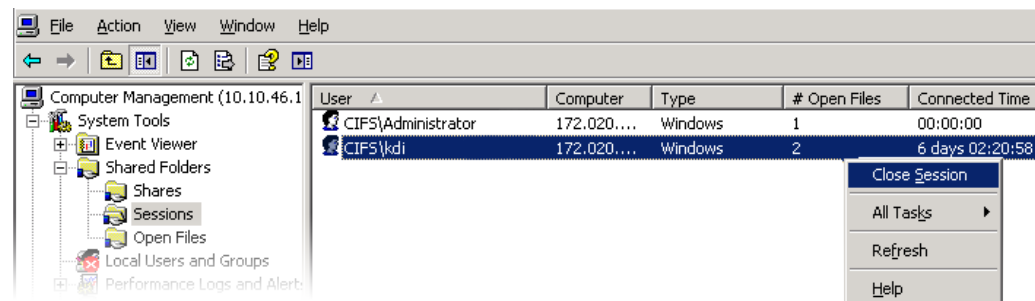
La capture d'écran suivante montre les fichiers ouverts par connexion.

FIGURE 28 Fichiers ouverts par connexion



La capture d'écran suivante illustre les sessions ouvertes.

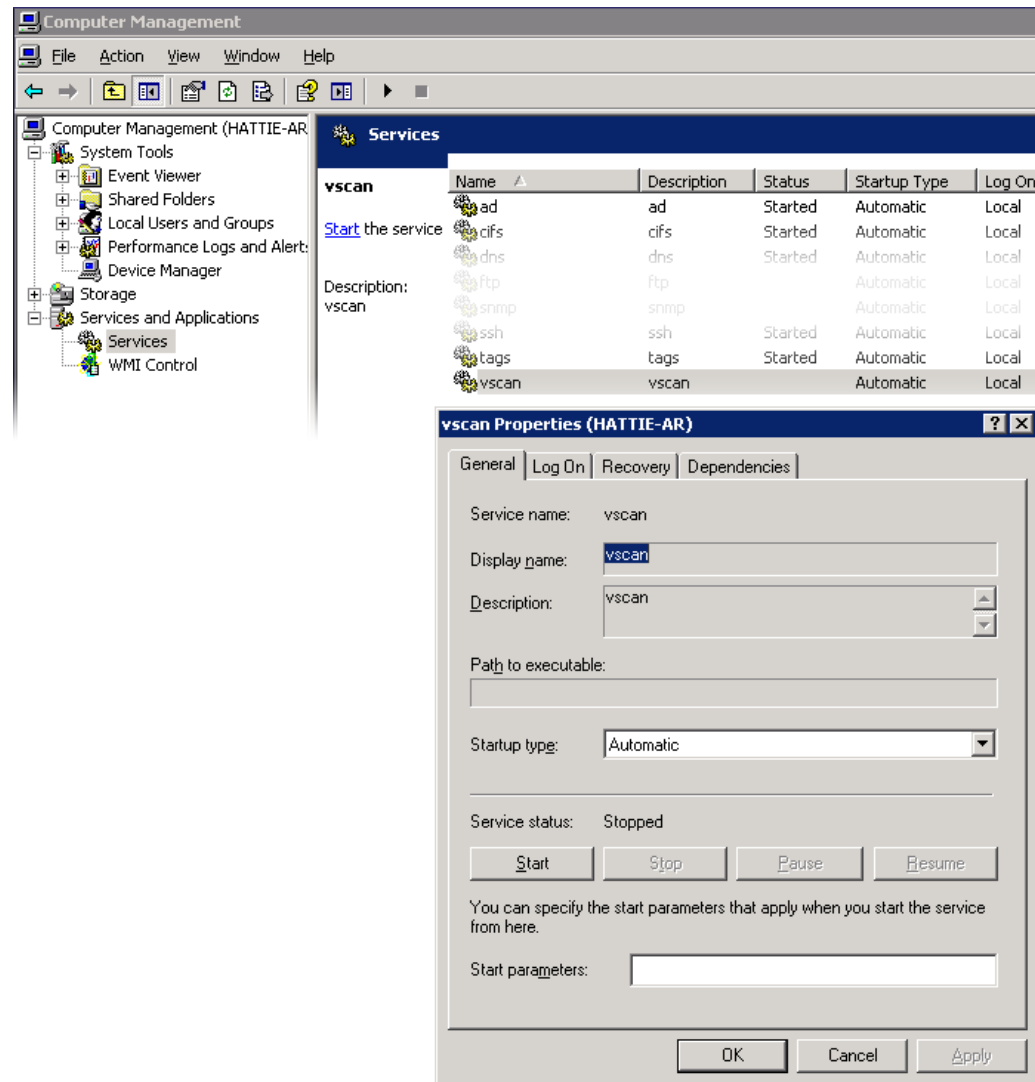
FIGURE 29 Sessions ouvertes



Etablissement de la liste des Services SMB

L'application MMC prend en charge l'affichage de la liste des services dédiés aux appareils. En revanche, elle ne permet pas d'activer ou de désactiver des services. La prise en charge comprend les services de l'appareil. Les services ne peuvent pas être activés ou désactivés à l'aide de l'application Computer Management de la console MMC.

La capture d'écran suivante illustre les propriétés générales associées au service vscan

FIGURE 30 Propriétés vscan

Pour garantir que seuls les utilisateurs appropriés ont accès aux opérations d'administration, les opérations exécutées à distance via la console MMC sont sujettes à un certain nombre de restrictions d'accès.

TABLEAU 58 Utilisateurs et opérations autorisées

Utilisateur	Opérations autorisées
Utilisateurs standard	Etablissement de listes de partages.
Membres des groupes Administrators ou Power Users	Gestion des partages, établissement de listes des connexions utilisateur
Membres du groupe Administrators	Etablissement de la liste des fichiers ouverts et des fichiers fermés, fermeture des connexions utilisateur, consultation du journal des services et du journal des événements

▼ Configuration du service (BUI)

Il est possible de terminer la configuration initiale de l'appareil à l'aide de la BUI ou de la CLI ; l'opération devrait prendre moins de vingt minutes. Elle peut également être réalisée ultérieurement en accédant au contexte Maintenance > Système dans la BUI ou la CLI. La configuration initiale implique les étapes décrites ci-après.

1. **Configurez des périphériques réseau, des liaisons de données et des interfaces.**
 - a. **Créez des interfaces en cliquant sur les icônes  ou en faisant glisser des périphériques dans les listes de liaisons ou d'interfaces.**
 - b. **Définissez les propriétés de votre choix et cliquez sur le bouton Appliquer pour les ajouter à la liste.**
 - c. **Définissez chaque interface sélectionnée comme "active" ou "de secours".**
 - d. **Cliquez sur APPLIQUER en haut de la page pour valider vos modifications.**
2. **Configurez le DNS.**
 - a. **Saisissez le nom de domaine de base.**
 - b. **Fournissez l'adresse IP d'au moins un serveur capable de résoudre les enregistrements serveur et nom d'hôte dans la portion Active Directory de l'espace de noms du domaine.**
3. **Configurez les clés d'authentification NTP afin de garantir la synchronisation temporelle.**
 - a. **Cliquez sur l'icône  pour ajouter une nouvelle clé.**

- b. **Saisissez le mot de passe et le nom d'utilisateur de votre compte en ligne.**
Une déclaration de confidentialité s'affiche ensuite.
- c. **Choisissez parmi vos équipes d'inventaire celle avec laquelle vous inscrire.**
Pour chaque compte, l'équipe par défaut est identique au nom d'utilisateur du compte, précédé du symbole '\$'.
- d. **Validez les modifications apportées à votre configuration initiale.**

▼ Configuration d'Active Directory pour SMB (BUI)

1. **Créez un compte pour l'appareil dans le domaine Active Directory.**
Des instructions détaillées sont fournies dans la section "[Configuration d'Active Directory](#)" à la page 293.
2. **Dans l'écran Configuration > Services > Active Directory, cliquez sur le bouton Rejoindre le domaine.**
3. **Indiquez le domaine Active Directory, l'utilisateur administratif et son mot de passe.**
4. **Cliquez sur APPLIQUER pour valider les modifications.**

▼ Configuration d'un projet et d'un partage SMB (BUI)

1. **Accédez à Partages > Partages.**
2. **Créez un projet.**
 - a. **Dans l'écran Partages, cliquez sur l'icône  pour développer le panneau Projets.**
 - b. **Cliquez sur l'icône d'ajout  pour ajouter un nouveau projet.**
 - c. **Spécifiez le nom du projet et cliquez sur APPLIQUER.**
3. **Sélectionnez le nouveau projet dans le panneau Projets.**
4. **Cliquez sur l'icône d'ajout d'élément  pour ajouter un système de fichiers.**

5. Cliquez sur l'icône de modification  correspondant au système de fichiers.
6. Cliquez sur l'onglet Général et désactivez la case à cocher Hériter du projet.
7. Choisissez un point de montage sous /export, bien que le nom de ressource permette d'accéder aux partages SMB, puis cliquez sur APPLIQUER.
8. Cliquez sur l'onglet Protocoles pour ce projet et activez le nom de ressource SMB.
9. Activez sharesmb et l'ACL au niveau du partage pour le projet.
10. Cliquez sur APPLIQUER pour activer la configuration.

▼ Configuration du service de données SMB (BUI)

1. Accédez à Configuration > Services > SMB et cliquez sur l'icône d'alimentation  pour activer le service.
2. Définissez les propriétés SMB et cliquez sur APPLIQUER pour activer la configuration. Voir la section ["Propriétés du service SMB" à la page 244](#).
3. Dans l'écran Configuration > Services > SMB, cliquez sur l'onglet Autohome pour définir les règles autohome de mappage entre clients SMB et répertoires personnels comme indiqué dans la section ["SMB Autohome" à la page 249](#). Cliquez sur APPLIQUER pour activer la configuration.
4. Dans l'écran Configuration > Services > SMB, cliquez sur l'onglet Groupes locaux et utilisez l'icône d'ajout d'élément  pour ajouter des administrateurs ou des opérateurs de sauvegarde à des groupes locaux, conformément à la section ["Ajout d'un utilisateur à un groupe SMB local" à la page 251](#). Cliquez ensuite sur APPLIQUER pour activer la configuration.

Configuration FTP

Le service FTP (File Transfer Protocol) permet l'accès au système de fichiers à partir des clients FTP. Les connexions anonymes ne sont pas autorisées, les utilisateurs doivent s'authentifier à l'aide du service de noms configuré dans Services.

Pour configurer le service FTP, reportez-vous aux sections suivantes :

- ["Ajout de l'accès FTP à un partage \(BUI\)" à la page 262](#)
- ["Propriétés FTP" à la page 262](#)
- ["Journaux FTP" à la page 263](#)

▼ Ajout de l'accès FTP à un partage (BUI)

1. Accédez à **Configuration > Services**.
2. Assurez-vous que le service FTP est activé et en ligne. Si ce n'est pas le cas, activez-le.
3. Sélectionnez ou ajoutez un partage dans l'écran **Partages**.
4. Cliquez sur l'onglet **Protocoles** et vérifiez que l'accès FTP est activé.
5. (Facultatif) Définissez le mode de partage **Lecture seule** ou **Lecture/écriture**.

Rubriques connexes

- ["Propriétés FTP" à la page 262](#)
- ["Journaux FTP" à la page 263](#)

Propriétés FTP

TABLEAU 59 Propriétés FTP générales

Propriété	Description
Port pour les connexions entrantes	Port sur lequel FTP est à l'écoute. La valeur par défaut est 21.
Nbre maximal de connexions ("0" pour un nombre illimité)	Nombre maximal de connexions FTP simultanées. Définissez cette propriété afin de couvrir le nombre d'utilisateurs simultanés prévus. Par défaut, cette valeur est définie sur 30, étant donné que chaque connexion crée un processus système et qu'en autoriser un trop grand nombre (des milliers) risquerait d'entraîner une attaque par déni de service..
Activer le moteur temporisé pour empêcher les attaques temporelles	Cette propriété insère de courts délais durant l'authentification afin de tromper les tentatives visant à deviner un nom d'utilisateur grâce aux mesures du temps. L'activation de cette propriété permet de renforcer la sécurité..
Identifiant root par défaut	Emplacement de connexion au FTP. La valeur par défaut est "/" et pointe vers le haut de la hiérarchie des partages. Tous les utilisateurs seront connectés à cet emplacement après s'être correctement authentifiés à l'aide du service FTP..
Niveau de journalisation	Niveau de détail du journal proftpd.
Autorisations à masquer sur les nouveaux fichiers et répertoires créés	Autorisations d'accès au fichier à supprimer lorsque des fichiers sont créés. Par défaut, les autorisations en écriture "groupe" et "tout le monde" sont masquées pour empêcher que les téléchargements récents ne soient réécrits par n'importe qui..

TABLEAU 60 Propriétés de sécurité FTP

Propriété	Description
Activer SSL/TLS	Autoriser les connexions FTP chiffrées SSL/TLS. Cette propriété garantit le chiffrement de la transaction FTP. Elle est désactivée par défaut.
Port pour les connexions SSL/TLS entrantes	Port d'écoute du service FTP chiffré SSL/TLS. La valeur par défaut est 21.
Autoriser la connexion de root	Autoriser les connexions FTP pour l'utilisateur root. Cette propriété est désactivée par défaut, car l'authentification FTP en texte clair présente un risque de sécurité par rapport aux attaques survenant durant la détection du réseau.
Nombre maximum de tentatives de connexion autorisées	Nombre de tentatives de connexion ayant échoué avant qu'une connexion FTP soit interrompue et que l'utilisateur doive se reconnecter pour essayer à nouveau. La valeur par défaut est 3.
Autoriser les adresses étrangères de connexion aux données	Permet les connexions étrangères au FTP afin d'activer le transfert direct de fichiers entre les serveurs FTP. Par défaut, cette propriété est désactivée.

Rubriques connexes

- ["Ajout de l'accès FTP à un partage \(BUI\)" à la page 262](#)
- ["Journaux FTP" à la page 263](#)

Journaux FTP**TABLEAU 61** Journaux FTP

Journal	Description
proftpd	Consigne les événements FTP, y compris les connexions réussies et les tentatives de connexions ayant échoué.
proftpd_xfer	Journal de transfert de fichiers.
proftpd_tls	Consigne les événements FTP liés au chiffrement SSL/TLS.

Rubriques connexes

- ["Ajout de l'accès FTP à un partage \(BUI\)" à la page 262](#)
- ["Propriétés FTP" à la page 262](#)

Configuration HTTP

Le service HTTP permet d'accéder aux systèmes de fichiers à l'aide des protocoles HTTP et HTTPS et de l'extension HTTP WebDAV (Web based Distributed Authoring and Versioning).

Les clients peuvent ainsi accéder aux systèmes de fichiers partagés via un navigateur Web ou en tant que système de fichiers local si cette option est prise en charge par le logiciel client. L'URL permettant d'accéder à ces partages HTTP et HTTPS ont les formats respectifs suivants :

- `http://hostname/shares/mountpoint/share_name`
- `https://hostname/shares/mountpoint/share_name`
- Le serveur HTTPS utilise un certificat de sécurité auto-signé.

Pour configurer HTTP, reportez-vous aux sections suivantes :

- ["Ajout de l'accès HTTP à un partage \(BUI\)" à la page 264](#)
- ["Propriétés et journaux HTTP" à la page 264](#)
- ["Authentification et contrôle d'accès HTTP" à la page 265](#)

▼ Ajout de l'accès HTTP à un partage (BUI)

1. **Accédez à Configuration > Services.**
2. **Assurez-vous que le service HTTP est activé et en ligne. Si ce n'est pas le cas, activez-le.**
3. **Sélectionnez ou ajoutez un partage dans l'écran Partages.**
4. **Cliquez sur l'onglet Protocoles et vérifiez que l'accès HTTP est activé.**
5. **(Facultatif) Définissez le mode de partage Lecture seule ou Lecture/écriture.**

Rubriques connexes

- ["Propriétés et journaux HTTP" à la page 264](#)
- ["Authentification et contrôle d'accès HTTP" à la page 265](#)

Propriétés et journaux HTTP

TABLEAU 62 Propriétés HTTP

Propriété	Description
Exiger la connexion des clients	Les clients doivent s'authentifier pour bénéficier de l'accès au partage et pour que les fichiers qu'ils créent leur appartiennent. Si cette propriété n'est pas définie, les fichiers créés appartiendront au service HTTP et l'utilisateur sera "nobody". Voir la section "Authentification et contrôle d'accès HTTP" à la page 265 .

Propriété	Description
Protocoles	Sélectionnez les méthodes d'accès prenant en charge HTTP, HTTPS ou les deux.
Port HTTP (pour les connexions entrantes)	Port HTTP. La valeur par défaut est 80.
Port HTTPS (pour les connexions sécurisées entrantes)	Port HTTP. La valeur par défaut est 443.

TABLEAU 63 Journaux HTTP

Journal	Description
network-http:apache22	Journal du service HTTP

Rubriques connexes

- ["Ajout de l'accès HTTP à un partage \(BUI\)" à la page 264](#)
- ["Authentification et contrôle d'accès HTTP" à la page 265](#)

Authentification et contrôle d'accès HTTP

Si l'option "Exiger la connexion des clients" est activée, l'appareil refuse l'accès aux clients qui ne fournissent pas d'informations d'identification valides pour l'authentification d'un utilisateur local, NIS ou LDAP. L'authentification Active Directory n'est pas prise en charge.

Seule l'authentification HTTP basique est prise en charge. Notez que, si HTTPS n'est pas utilisé, le nom d'utilisateur et le mot de passe non chiffrés sont transmis, ce qui n'est pas nécessairement approprié dans tous les environnements.

En règle générale, les utilisateurs authentifiés ont les mêmes autorisations avec HTTP qu'avec NFS ou FTP. Les fichiers et les répertoires créés par un utilisateur authentifié lui appartiennent, exactement comme c'est le cas avec les autres protocoles. Les utilisateurs privilégiés (qui possèdent un UID inférieur à 100) sont traités en tant que "nobody" aux fins de contrôle d'accès. Les fichiers créés par les utilisateurs privilégiés appartiennent à "nobody".

Si l'option "Exiger la connexion des clients" est désactivée, l'appareil ne tente pas d'authentifier les clients (même s'ils fournissent des informations d'identification). Les fichiers récemment créés appartiennent à "nobody" et tous les utilisateurs sont traités en tant que "nobody" à des fins de contrôle d'accès.

Quel que soit le type d'authentification, aucune autorisation n'est masquée dans les fichiers et les répertoires créés. Les fichiers créés possèdent des autorisations Unix 666 (lisibles et inscriptibles par tous) et les répertoires créés possèdent des autorisations 777 (lisibles, inscriptibles et exécutables par tous).

Rubriques connexes

- ["Ajout de l'accès HTTP à un partage \(BUI\)" à la page 264](#)
- ["Propriétés et journaux HTTP" à la page 264](#)

Configuration NDMP

Le service NDMP (Network Data Management Protocol) permet au système de participer aux opérations de sauvegarde et restauration NDMP contrôlées par un client NDMP distant appelé "application de gestion des données" (DMA, Data Management Application). Avec NDMP, les données stockées dans les partages créés par l'administrateur sur l'appareil peuvent être sauvegardées et restaurées à la fois sur les périphériques à bande connectés en local et sur des systèmes distants. Les périphériques à bande connectés en local peuvent également être exposés sur la DMA pour sauvegarder et restaurer les systèmes distants.

NDMP ne peut pas être utilisé pour sauvegarder et restaurer les données de configuration du système. Utilisez plutôt la fonctionnalité de sauvegarde et restauration de configuration (reportez-vous à la section ["Sauvegarde de la configuration" dans le Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance](#)).

Pour configurer NDMP, reportez-vous aux sections suivantes :

- ["Configurations NDMP locales et configurations NDMP distantes" à la page 266](#)
- ["Formats et types de sauvegarde NDMP" à la page 267](#)
- ["Sauvegarde NDMP à l'aide des types dump et tar" à la page 267](#)
- ["Sauvegarde NDMP à l'aide du type zfs" à la page 269](#)
- ["Sauvegardes incrémentielles NDMP" à la page 270](#)
- ["Sauvegardes de réplique" à la page 272](#)
- ["Propriétés et journaux NDMP" à la page 274](#)

Configurations NDMP locales et configurations NDMP distantes

L'appareil prend en charge la sauvegarde et la restauration tant à l'aide d'une configuration *locale* (où les lecteurs de bande sont physiquement connectés à l'appareil) que via une configuration *distante* (où les données sont transmises vers un autre système du même réseau). Dans les deux cas, il faut gérer la sauvegarde dans une DMA prise en charge.

Dans les configurations locales, les lecteurs de bande pris en charge, y compris les lecteurs et les changeurs (robots), sont physiquement connectés au système à l'aide d'une carte SCSI ou Fibre Channel compatible configurée en mode Initiateur. Ces périphériques sont visibles dans l'écran de Statut NDMP. Le service NDMP présente ces périphériques à une DMA à la recherche de périphériques. Une fois configuré dans la DMA, ces périphériques sont disponibles pour participer à la sauvegarde et à la restauration de l'appareil ou d'autres systèmes du même réseau. Après avoir ajouté des lecteurs de bande ou des changeurs ou supprimé ces périphériques, vous devrez peut-être réinitialiser le système pour que les modifications soient reconnues par le service NDMP. Après cela, il peut être nécessaire de reconfigurer la DMA, en raison de la modification des noms de périphérique à bande.

Dans les configurations distantes, les périphériques à bande ne sont pas physiquement connectés au système en cours de sauvegarde et de restauration (le serveur de données) mais plutôt au système exécutant la DMA ou à un système distinct (le serveur de bandes). On les appelle communément "configurations à trois voies" car la DMA contrôle deux autres systèmes. Dans ce type de configuration, le flux de données est transmis entre le serveur de données et le serveur de bandes via un réseau IP.

Formats et types de sauvegarde NDMP

Le protocole NDMP ne spécifie pas de format pour les données de sauvegarde. L'appareil prend en charge trois types de sauvegarde correspondant aux différentes implémentations et formats sur bande. Les DMA peuvent sélectionner un type de sauvegarde à l'aide des valeurs suivantes pour la variable d'environnement NDMP "TYPE" :

TABLEAU 64 Formats et types de sauvegarde NDMP

Type de sauvegarde	Détails
dump	Basé sur les fichiers pour les systèmes de fichiers uniquement. Prend en charge l'historique des fichiers et la récupération par accès direct (DAR, Direct Access Recovery).
tar	Basé sur les fichiers pour les systèmes de fichiers uniquement. Prend en charge l'historique des fichiers et la récupération par accès direct (DAR, Direct Access Recovery).
zfs	Basé sur les partages pour les systèmes de fichiers et les volumes. Ne prend en charge ni l'historique des fichiers ni la récupération par accès direct (DAR), mais peut être plus rapide pour certains ensembles de données. Uniquement compatible avec NDMPv4.

Il n'existe pas de format de flux de données NDMP standard. Par conséquent, les flux de sauvegarde générés sur l'appareil peuvent être restaurés uniquement sur des appareils de stockage ZFS qui exécutent un logiciel compatible. Les versions logicielles ultérieures de l'appareil permettent généralement de restaurer les flux sauvegardés à partir de versions antérieures du logiciel, mais l'inverse n'est pas toujours vrai. Par exemple, le type de sauvegarde "zfs" a été introduit dans la version 2010.Q3. Les systèmes exécutant 2010.Q1 (ou une version antérieure) ne peuvent donc pas restaurer les flux de sauvegarde créés à l'aide du type "zfs" sous 2010.Q3.

Sauvegarde NDMP à l'aide des types dump et tar

Lorsqu'ils procèdent à une sauvegarde à l'aide des types "dump" et "tar", les administrateurs spécifient les données à sauvegarder par le biais d'un chemin d'accès au système de fichiers

appelé *chemin de sauvegarde*. Par exemple, si l'administrateur configure une sauvegarde de */export/home*, le partage monté à cet emplacement est sauvegardé. De même, si un flux de sauvegarde est restauré sur */export/code*, les fichiers sont restaurés à cet emplacement, même s'ils ont été sauvegardés à partir d'un autre chemin.

Seuls les chemins qui constituent des points de montage de partages existants ou qui se trouvent dans des partages existants peuvent être spécifiés pour la sauvegarde. Si le chemin de sauvegarde correspond à un point de montage de partage, seul ce partage est sauvegardé. Sinon, le chemin doit être contenu dans un partage, auquel cas seule la portion de ce partage située sous ce chemin est sauvegardée. Dans les deux cas, tout autre partage monté dans le partage spécifié sous le chemin de sauvegarde n'est pas sauvegardé. Il faut spécifier ces partages de façon distincte pour la sauvegarde.

Instantanés : Si le chemin de sauvegarde spécifie un système de fichiers live (par exemple, */export/code*) ou un chemin contenu dans un système de fichiers live (par exemple, */export/code/src*), l'appareil prend immédiatement un nouvel instantané à partir duquel il sauvegarde le chemin donné. À l'issue de la sauvegarde, l'instantané est détruit. Si le chemin de sauvegarde spécifie un instantané (par exemple, */export/code/zfs/snapshot/mysnap*), aucun instantané n'est créé et le système sauvegarde à partir de l'instantané spécifié.

Métadonnées de partage : Pour simplifier la sauvegarde et la restauration des configurations de partage complexes, les sauvegardes "dump" et "tar" incluent les métadonnées de partage pour les projets et les partages associés au chemin de sauvegarde. Ces métadonnées décrivent la configuration du partage sur l'appareil, y compris les propriétés de partage de protocole, les propriétés de quota et les autres propriétés configurées dans l'écran Partages. A ne pas confondre avec les métadonnées de système de fichiers telles que la structure de répertoires et les autorisations d'accès au fichier qui sont également sauvegardées et restaurées via NDMP.

Par exemple, si vous sauvegardez */export/proj*, les métadonnées de tous les partages dont les points de montage commencent par */export/proj* sont sauvegardées ainsi que les métadonnées de partage des projets parents. De même, si vous sauvegardez */export/someshare/somedir* et qu'un partage est monté sous */export/someshare*, les métadonnées de ce partage et de son projet sont sauvegardées.

Durant la restauration, si la destination du chemin de restauration n'est pas contenue dans un partage existant, les projets et les partages du flux de sauvegarde sont recréés, si nécessaire avec les propriétés d'origine stockées dans la sauvegarde. Par exemple, si vous sauvegardez */export/foo*, qui contient le projet *proj1* et les partages *share1* et *share2*, puis détruisez le projet et le restaurez à partir de la sauvegarde, ces deux partages et le projet sont recréés avec les propriétés sauvegardées dans le cadre de la restauration.

Lors d'une restauration, si un projet qui autrement aurait été recréé existe, ce projet est utilisé et aucun projet n'est automatiquement créé. En présence d'un partage qui autrement aurait été recréé existe, si son point de montage correspond aux attentes de l'appareil en matière de chemin de sauvegarde d'origine et de destination de la restauration, le partage existant est utilisé et aucun partage n'est créé automatiquement. En son absence, un nouveau partage est automatiquement créé à partir des métadonnées de la sauvegarde. Si un partage du même nom

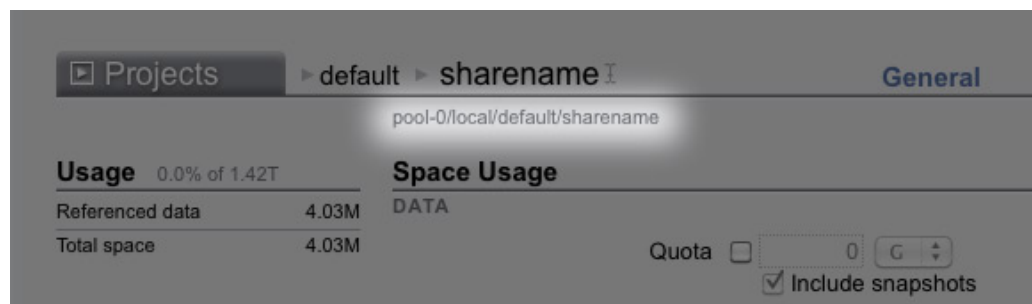
existe déjà (mais avec un point de montage différent), un nom unique commençant par ndmp- est attribué au nouveau partage créé, avec le point de montage correct.

Il est conseillé soit de restaurer un flux dont les ensembles de données n'existent plus sur l'appareil (pour que ce dernier recrée ces ensembles de données comme spécifié dans le flux de sauvegarde), soit de précréer un partage de destination pour les restaurations. Ces deux méthodes évitent d'obtenir des résultats surprenants découlant de la création de partage automatique décrite ci-dessus.

Sauvegarde NDMP à l'aide du type zfs

Lorsqu'ils procèdent à une sauvegarde à l'aide du type "zfs", les administrateurs spécifient les données à sauvegarder par leur nom canonique sur l'appareil. Ce nom se trouve sous celui du partage dans la BUI :

FIGURE 31 Nom de partage NDMP



ou dans la CLI, en tant que valeur de la propriété `canonical_name`. Les noms canoniques ne commencent pas par une barre oblique "/" mais, lorsque vous configurez le chemin de sauvegarde, le nom canonique doit être précédé du symbole "/".

Les projets et les partages peuvent tous deux être spécifiés pour la sauvegarde à l'aide du type "zfs". Si le nom canonique est spécifié tel quel, un nouvel instantané est créé et utilisé pour la sauvegarde. Un instantané spécifique peut être spécifié pour la sauvegarde à l'aide du suffixe `@snapshot` ; dans ce cas, aucun instantané n'est créé et l'instantané spécifié est sauvegardé. Par exemple :

TABLEAU 65 Noms canoniques et partages sauvegardés

Nom canonique	Partages sauvegardés
pool-0/local/default	Nouvel instantané du projet local nommé default et tous ses partages

Nom canonique	Partages sauvegardés
pool-0/local/default@yesterday	Instantané nommé yesterday du projet local default et tous ses partages possédant l'instantané yesterday
pool-0/local/default/code	Nouvel instantané du partage code dans le projet local default, code pouvant être un système de fichiers ou un volume
pool-0/local/default/code@yesterday	Instantané nommé yesterday du partage code dans le projet local default, code pouvant être un système de fichiers ou un volume

Etant donné que les sauvegardes incrémentielles basées sur les niveaux qui utilisent le type "zfs" requièrent un instantané de base issu de la précédente sauvegarde incrémentielle, le comportement par défaut de ces sauvegardes (au cours desquelles un instantané est créé) consiste à conserver le nouvel instantané pour pouvoir l'utiliser lors des sauvegardes incrémentielles suivantes. Si la DMA indique que la sauvegarde ne sera pas utilisée lors de prochaines sauvegardes incrémentielles (UPDATE=n défini), le nouvel instantané est détruit après la sauvegarde. Les instantanés utilisateur existants ne sont jamais détruits après une sauvegarde. Pour plus de détails, reportez-vous à la section "[Sauvegardes incrémentielles NDMP](#)" à la page 270.

Métadonnées de partage : Les métadonnées de partage (configuration du partage) sont toujours incluses dans les sauvegardes "zfs". Lorsque vous restaurez une sauvegarde complète avec le type "zfs", le projet ou le partage de destination ne doivent en aucun cas exister. Ils sont automatiquement recréés à partir des métadonnées dans le flux de sauvegarde. Lorsque vous restaurez une sauvegarde incrémentielle avec le type "zfs", le projet ou le partage de destination doivent exister. Leurs propriétés sont mises à jour à partir des métadonnées dans le flux de sauvegarde. Pour plus de détails, reportez-vous à la section "[Sauvegardes incrémentielles NDMP](#)" à la page 270.

Sauvegardes incrémentielles NDMP

L'appareil prend en charge les sauvegardes incrémentielles basées sur les niveaux pour tous les types de sauvegarde ci-dessus. Pour spécifier un niveau de sauvegarde, les DMA spécifient généralement les trois variables d'environnement suivantes :

Variable	Détails
LEVEL	Entier de 0 à 9 identifiant le niveau de sauvegarde
DMP_NAME	Ensemble de sauvegarde incrémentielle spécifique. Plusieurs ensembles de sauvegardes incrémentielles basées sur les niveaux peuvent être utilisés simultanément en spécifiant des valeurs différentes pour DMP_NAME.
UPDATE	Indique si cette sauvegarde peut servir de base aux sauvegardes incrémentielles suivantes.

Par définition, une sauvegarde de niveau N inclut tous les fichiers modifiés depuis la dernière opération de sauvegarde sur l'ensemble (spécifié par "DMP_NAME") du même partage à l'aide d'une variable inférieure à N pour LEVEL. Les sauvegardes de niveau 0 incluent tous les fichiers. Si la valeur par défaut "y" est définie pour UPDATE, la sauvegarde en cours est enregistrée afin que les futures sauvegardes de niveau supérieur à N utilisent cette sauvegarde comme base. En règle générale, ces variables sont gérées par la DMA et ne doivent pas être configurées directement par les administrateurs.

Vous trouverez ci-dessous un exemple de planification de sauvegarde incrémentielle.

TABLEAU 66 Exemple de planification de sauvegarde incrémentielle

Jour	Détails
Premier du mois	Sauvegarde de niveau 0. La sauvegarde contient tous les fichiers du partage.
Tous les 7, 14 et 21 du mois	Sauvegarde de niveau 1. La sauvegarde contient tous les fichiers modifiés depuis la dernière sauvegarde complète (mensuelle).
Tous les jours	Sauvegarde de niveau 2. La sauvegarde contient tous les fichiers modifiés depuis la sauvegarde de niveau 1.

Pour rétablir un système de fichiers dans l'état où il se trouvait le 24ème jour du mois, un administrateur restaure généralement la sauvegarde de niveau 0 datant du premier jour du mois sur un nouveau partage, puis la sauvegarde de niveau 1 datant du 21ème jour du mois et enfin la sauvegarde de niveau 2 datant du 24ème jour du mois.

Pour implémenter des sauvegardes incrémentielles basées sur les niveaux, l'appareil doit garder une trace de l'historique des sauvegardes basées sur les niveaux pour chaque partage. Pour les sauvegardes "tar" et "dump", cet historique est conservé dans les métadonnées du partage. Les sauvegardes incrémentielles parcourent le système de fichiers et incluent les fichiers modifiés depuis la date de la dernière sauvegarde basée sur les niveaux. Au moment de la restauration, le système restaure simplement tous les fichiers du flux de sauvegarde. Dans l'exemple ci-dessus, il serait donc possible de restaurer la sauvegarde de niveau 2 datant du 24ème jour sur n'importe quel système de fichiers. Les fichiers contenus dans ce flux de sauvegarde seraient restaurés, même si le système de fichiers cible ne correspondait pas au système de fichiers dans lequel les fichiers ont été sauvegardés. Toutefois, la meilleure pratique consiste à suivre une procédure semblable à celle décrite plus haut, qui, à partir d'une arborescence vide, restaure les sauvegardes de niveau précédent afin de rétablir l'état d'origine du système de fichiers.

Pour implémenter efficacement des sauvegardes incrémentielles basées sur les niveaux de type "zfs", le système adopte une autre approche. Les sauvegardes qui font partie d'un ensemble incrémentiel ne détruisent pas l'instantané utilisé pour la sauvegarde mais au contraire, elles le laissent sur le système. Les sauvegardes incrémentielles successives utilisent cet instantané comme base afin d'identifier rapidement les blocs du système de fichiers modifiés et générer le flux de sauvegarde. Par conséquent, il ne faut pas détruire les instantanés conservés par le service NDMP après une sauvegarde si vous souhaitez créer des sauvegardes incrémentielles ultérieures.

Une autre conséquence notable de ce comportement est que, pour pouvoir restaurer un flux incrémentiel, l'état du système de fichiers doit être parfaitement identique à l'état de l'instantané de base du flux incrémentiel. En d'autres termes, pour restaurer une sauvegarde de niveau 2, le système de fichiers doit se trouver exactement dans le même état qu'à la fin de la sauvegarde de niveau 1. Notez que la procédure couramment suivie et décrite plus haut garantit cette similitude. En effet, lors de la restauration du flux de sauvegarde de niveau 2 datant du 24ème jour, le système est exactement tel qu'il était à l'issue de la sauvegarde de niveau 1 datant du 21ème jour, qui vient d'être restaurée.

Le service NDMP signale une erreur si vous tentez de restaurer un flux de sauvegarde incrémentielle "zfs" vers un système de fichiers dont l'instantané le plus récent ne correspond pas à l'instantané de base du flux incrémentiel ou si le système de fichiers a été modifié depuis la prise de cet instantané. Avant de procéder à la restauration, vous pouvez configurer le service NDMP pour restaurer l'instantané de base, en spécifiant la valeur "y" pour la variable d'environnement NDMP "ZFS_FORCE" ou en configurant la propriété "Ensembles de données de restauration" du service NDMP (voir la section "[Propriétés et journaux NDMP](#)" à la page 274).

Sauvegardes de réplique

Les appareils Oracle ZFS Storage Appliance prennent en charge la sauvegarde directe de répliques et les instantanés de répliques avec le type de sauvegarde "zfs". Il n'est pas nécessaire de commencer par cloner un ensemble de données de réplique (projet ou partage) pour le sauvegarder.

Remarque - S'agissant de la sauvegarde d'une réplique, ce sont les propriétés de l'ensemble de données de la source qui sont sauvegardées plutôt que celles de la cible.

Activation des sauvegardes de répliques

- Pour activer les sauvegardes de répliques, appliquez la mise à jour différée correspondante. Pour plus d'informations, reportez-vous à la section "[Mises à jour différées](#)" du manuel *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance pour les contrôleurs ZS5-x, ZS4-4, ZS3-x, 7x20 et les étagères de disques Sun Disk Shelf DE2-24, version OS8.6.0*.
- Les sauvegardes de répliques nécessitent la version logicielle 2011.1.0 (ou ultérieure) sur la source.
- Si la sauvegarde de réplique doit être restaurée sur la source avec l'ensemble de données répliqué d'origine, la source doit exécuter la version logicielle 2013.1.4 (ou ultérieure).

Syntaxe de sauvegarde de réplique

Pour sauvegarder un projet ou un partage répliqué, saisissez le nom de l'ensemble de données ZFS sans extension d'instantané dans la DMA. ndmpd utilise le logiciel de l'appareil pour déterminer l'instantané de réplique complet le plus récent à sauvegarder. Pour indiquer un ensemble de données de réplique pour la sauvegarde, effectuez un copier/coller pour éviter

les erreurs de frappe des longs noms d'ensembles de données de répliques pouvant inclure un UUID.

Si une extension d'instantané générée par l'utilisateur est incluse, ndmpd sauvegarde l'instantané utilisateur indiqué. Si une extension générée par le système est incluse, (commençant par .rr), la sauvegarde échoue et génère un message enregistré dans la console DMA.

Mises en attente persistantes de sauvegardes de répliques

Les mises en attente persistantes sont effectuées sur des instantanés sauvegardés une fois la sauvegarde terminée. Cette opération est nécessaire pour les sauvegardes incrémentielles ultérieures, qui utilisent les instantanés actuels comme base ; à défaut, le sous-système de réplication peut supprimer les instantanés de répliques dont il n'a plus besoin. Les mises en attente sont annulées par ndmpd une fois que les instantanés ne sont plus nécessaires.

Les mises en attente persistantes peuvent être supprimées manuellement. Lors de la suppression d'un instantané de réplique comportant une mise en attente, une confirmation s'affiche pour vous informer de l'impact éventuel sur les sauvegardes NDMP en cours ou ultérieures. Les instantanés requis par le sous-système de réplication ne peuvent pas être supprimés.

Si les sauvegardes incrémentielles ne sont pas nécessaires, empêchez les mises en attente persistantes en définissant le paramètre DMA UPDATE sur no (UPDATE=n). UPDATE=y est la valeur par défaut. Pour plus d'informations sur la variable d'environnement NDMP UPDATE, reportez-vous au livre blanc [NDMP Implementation Guide for the Sun ZFS Storage Appliance](http://www.oracle.com/technetwork/server-storage/sun-unified-storage/appliance/index.html) (<http://www.oracle.com/technetwork/server-storage/sun-unified-storage/appliance/index.html>).

Sauvegardes de répliques incrémentielles

La poursuite (incrémementation) d'une série de sauvegardes sur une inversion ou une dissociation de réplication n'est pas prise en charge ; vous devez démarrer une nouvelle série de sauvegardes à la place. Utilisez une sauvegarde complète (niveau 0) pour la première sauvegarde après la modification d'un état de réplication, comme sur une nouvelle source après une inversion ou une dissociation de réplication.

Les extensions d'instantanés statiques qui ne changent pas en fonction du niveau ne sont PAS prises en charge pour les instantanés de répliques générés par l'utilisateur (instantanés ne commençant pas par .rr). Cela empêche les collisions de noms, qui génèrent une erreur et peuvent entraîner l'échec d'une réplication.

Certaines DMA ne prennent pas en charge les opérations de sauvegarde et de restauration incrémentielle de répliques de type zfs pour les modification de nom d'extension d'instantanés par niveau. Pour préserver l'espace de l'appareil et veiller à ce que de tels instantanés ne soient pas conservés pour des sauvegardes incrémentielles ultérieures, définissez UPDATE=n sur l'heure de la sauvegarde de la réplique. Les instantanés générés par l'utilisateur ne peuvent pas être supprimés manuellement.

Même si aucune donnée utilisateur n'a changé dans un ensemble de données restauré, les métadonnées modifiées peuvent entraîner l'échec des restaurations de répliques incrémentielles.

Pour éviter cela, revenez toujours à l'instantané de base avant les restaurations de répliques incrémentielles en définissant le paramètre ZFS `rollback before restore` sur `Always`.

Pour les sauvegardes de répliques non incrémentielles, par exemple pour les sauvegardes uniques, définissez `UPDATE=n` pour que les instantanés ultérieurs ne soient pas enregistrés et ne prennent ainsi pas d'espace de stockage. Certains anciens instantanés de répliques, conservés pour les sauvegardes incrémentielles ultérieures, telles que celles créées en définissant `UPDATE=y`, peuvent ne plus être nécessaires et ainsi occuper inutilement de l'espace de stockage. Ces instantanés peuvent être supprimés manuellement en toute sécurité. Les instantanés requis par le sous-système de réplication ne peuvent pas être supprimés. Les instantanés non nécessaires peuvent être supprimés après la confirmation du message d'avertissement concernant les conséquences possibles de la suppression de l'instantané sur les sauvegardes NDMP en cours ou ultérieures.

Propriétés et journaux NDMP

La configuration du service NDMP inclut les propriétés et les journaux suivants :

TABLEAU 67 Propriétés NDMP

Propriété	Description
Version	Version NDMP prise en charge par votre DMA.
Port TCP (v4 uniquement)	Le port de connexion NDMP par défaut est 10000. NDMPv3 utilise toujours ce port. NDMPv4 permet d'utiliser un autre port, le cas échéant.
Ignorer les modifications des métadonnées seules	Indique au système de sauvegarder uniquement les fichiers dont le contenu a été modifié et d'ignorer les fichiers dont seules des métadonnées (comme les autorisations ou la propriété) ont été modifiées. Cette option s'applique uniquement aux sauvegardes incrémentielles "tar" et "dump" et est désactivée par défaut.
Pool(s) de restauration cible(s)	Lorsqu'il procède à une restauration complète à l'aide des types "tar" ou "dump", le système recrée les ensembles de données si aucun partage n'est déjà monté au niveau cible. Etant donné que le protocole NDMP spécifie uniquement le point de montage, le système choisit un pool dans lequel recréer des projets et des partages. Sur un système contenant plusieurs pools, cette propriété vous permet de spécifier un ou plusieurs pools. Les pools multiples doivent être spécifiés uniquement dans un cluster avec des pools actifs sur chaque tête. Vous devez vous assurer que cette liste est toujours synchronisée après chaque changement de configuration de stockage. En l'absence totale de pools ou si aucun pool n'est en ligne, le système sélectionne un pool par défaut de façon aléatoire.

Propriété	Description
Autoriser la sauvegarde basée sur jeton	Active ou désactive la méthode à base de jeton pour la sauvegarde ZFS. Par défaut, cette propriété est désactivée.
Restauration ZFS avant restauration (v4 uniquement)	S'applique uniquement aux sauvegardes de type "zfs". Détermine si, au moment de la restauration d'une sauvegarde incrémentielle, le système rétablit le projet et le partage cible de l'instantané utilisé comme base de la restauration incrémentielle. Si le projet et les partages sont rétablis, toutes les modifications apportées depuis la prise de l'instantané sont perdues. Cette propriété est généralement contrôlée par le DMA via la variable d'environnement "ZFS_FORCE", mais elle peut être utilisée pour remplacer le paramètre DMA et décider de restaurer systématiquement ou jamais ces ensembles de données. Pour plus de détails, reportez-vous à la section "Sauvegardes incrémentielles NDMP" à la page 270 . Le fait de ne pas rétablir les ensembles de données peut entraîner l'échec de la restauration, à moins qu'ils n'aient déjà été rétablis manuellement. Cette propriété est conçue pour une utilisation avec les DMA qui n'autorisent pas les administrateurs à configurer de variables d'environnement personnalisées comme ZFS_FORCE.
Autoriser la récupération par accès direct	Permet au système de localiser les fichiers par position plutôt que par recherche séquentielle durant les opérations de restauration. L'activation de cette option permet de réduire le temps requis pour la récupération d'un petit nombre de fichiers sur de nombreuses bandes. Il faut spécifier cette option au moment de la sauvegarde pour pouvoir récupérer des fichiers individuels ultérieurement.
Restaurer les chemins absolus (v3 uniquement)	Spécifie que, lors de la restauration d'un fichier, son chemin d'accès complet absolu est également restauré (et pas uniquement le fichier en question). Cette option est désactivée par défaut.
Création de partage lors de la restauration	Configure l'opération de restauration pour créer un partage en fonction du type de sauvegarde : ■ Tous - Autorise tous les types de sauvegarde à créer un partage lors de la restauration. ■ Tar_Dump - Autorise les types de sauvegarde "tar" et "dump" à créer un partage lors de la restauration. ■ ZFS - Autorise le type de sauvegarde "zfs" à créer un partage lors de la restauration. ■ Aucun - Aucun type de sauvegarde ne peut créer un partage lors de la restauration.
Mode de bande DMA (pour les unités rattachées localement)	Spécifie si la DMA attend à une sémantique System V ou BSD. La valeur par défaut est System V, elle est recommandée pour la plupart des DMA. Cette option s'applique uniquement aux lecteurs de bande connectés en local exportés via NDMP. Consultez votre documentation DMA pour connaître le mode attendu par votre DMA. La modification de cette option

Propriété	Description
	modifie uniquement les périphériques exportés lorsque la DMA recherche des périphériques. Vous devrez donc reconfigurer les périphériques à bande dans votre DMA après avoir modifié ce paramètre.
Nom d'utilisateur et mot de passe DMA	Utilisé pour authentifier la DMA. Le système utilise MD5 pour l'authentification utilisateur

TABLEAU 68 Journaux NDMP

Journal	Description
system-ndmpd:default	Journal du service NDMP

Configuration de la migration shadow

Le service de migration shadow permet de faire migrer automatiquement des données à partir de sources externes ou internes. Cette fonction est décrite en détail dans la section ["Migration shadow" à la page 431](#). Le service, quant à lui, contrôle uniquement la migration automatique en arrière-plan. Les données sont migrées de façon synchrone pour les demandes in-band, que le service soit activé ou non.

Le service peut être désactivé uniquement à des fins de test ou si la charge est trop élevée sur le système en raison de la fonctionnalité de migration shadow. Lorsqu'il est désactivé, aucun système de fichier ne sera en mesure de terminer la migration. Le but principal de ce service est de permettre aux utilisateurs d'ajuster le nombre des threads dédiés à la migration en arrière-plan.

Propriété "Nombre de threads" - Nombre de threads à dédier à la migration des données en arrière-plan. Ces threads sont communs à l'ensemble de la machine et, en augmentant leur nombre, il est possible que cela entraîne l'augmentation de la concurrence et de la vitesse globale de la migration aux dépens d'une consommation accrue des ressources (réseau, E/S et CPU).

Configuration SFTP

Le service SFTP (SSH File Transfer Protocol, protocole de transfert de fichier SSH) permet d'accéder au système de fichiers à partir des clients SFTP. Les connexions anonymes ne sont pas autorisées, les utilisateurs doivent s'authentifier à l'aide du service de noms configuré dans Services.

Pour configurer SFTP, reportez-vous aux sections suivantes :

- ["Ajout de l'accès SFTP à un partage \(BUI\)" à la page 277](#)

- ["Configuration du service SFTP pour un accès à distance \(CLI\)" à la page 277](#)
- ["Propriétés, ports et journaux SFTP" à la page 279](#)

▼ Ajout de l'accès SFTP à un partage (BUI)

1. Accédez à Configuration > Services.
2. Assurez-vous que le service SFTP est activé et en ligne. Si ce n'est pas le cas, activez-le.
3. Accédez à Partages > Partages et sélectionnez ou ajoutez un partage.
4. Accédez à l'onglet Protocoles et vérifiez que l'accès SFTP est activé.
5. (Facultatif) Définissez le mode de partage Lecture seule ou Lecture/écriture.

Rubriques connexes

- ["Configuration du service SFTP pour un accès à distance \(CLI\)" à la page 277](#)
- ["Propriétés, ports et journaux SFTP" à la page 279](#)

▼ Configuration du service SFTP pour un accès à distance (CLI)

1. Créez un utilisateur local ou un utilisateur réseau (LDAP ou NIS) avec un rôle d'administrateur adéquat. (Voir ["Configuration des utilisateurs" à la page 160](#)).
2. Générez une clé d'authentification SSH en saisissant la commande `ssh-keygen -t dsa` sur l'hôte/ le client Solaris.
3. Saisissez un nom pour le fichier où la clé sera stockée.
4. Saisissez une phrase de passe si nécessaire ou laissez ce champ vide afin de vous connectez directement au partage SFTP.

L'emplacement de la clé s'affiche La clé ressemble à ce qui suit :

```
ssh-dss AAAAB3NzaC1kc3MAAACBAPMMs5h8UWk1NPf/
VJDDEo0OAwt+s6iZxkCmmrgAmLfTX9izWk+ bsvNldOlXN/6EgkusLjo/
+UaEt5+704vMHClRaq3AlVHLS5tVjeX3iCs+fDo0qwXZg3Brh8QBAAWk3
ywr2osuII1tHh4v/HwEAHZq5mVWXavOpO3bgmxl0/
+VAAAAFQDIJxnm52DfyEdQQMTY+jRVvzGwMQA AAIaHtP6Ey
+2gGFICKkvUofsc04d8pbqH8duE9P6Y88s0+opuj52GkAdRUt2fRrdM9Cf3h4lIOc8Bw9
```

```
bZIBzrCKBNWBudZG56tsfLdilW6vS6gxKrmL2v7fSp9WYPsxZGhOLfU29zW4n2WVcVHbGyFEoVe
+taq aq+AYJaWoHnjZL1/
LpQAAAIAOLc8+uc3hDOcK3pAkYdg8b2rYIGOAZU4py0rq24DGPeVHd5h5jbe4p
WDM70uYqGCOPYiOKEoMnJpczRX5qjI+BfoUY4sH24WWwsKkT8XX9PUAa0WT
+7axEqg2N6YelaTJ95J vMaj6E7HkAIra2Sj2H/LSDktL42UL+j1Wx5A== username sunray
```

5. **Accédez à Configuration > Services > SFTP. Dans Clés, cliquez sur le signe plus (+).**
6. **Dans la fenêtre Nouvelle Clé, sélectionnez DSA.**
7. **Copiez uniquement la partie de la clé commençant par AAAA et finissant par Wx5A== dans l'exemple ci-dessus et copiez-la dans le champ Clé.**

Remarque - La clé ne doit pas contenir d'espace.

8. **Saisissez un nom d'utilisateur et ajoutez un commentaire qui servira de rappel.**
9. **Accédez à Partages > Partages et cliquez sur l'icône d'ajout d'élément  pour créer un système de fichiers.**
10. **Dans la fenêtre Créer un système de fichiers, saisissez le nom du système de fichiers (sftp, par exemple), modifiez les autorisations du partage en Lecture/Ecriture et cliquez sur APPLIQUER.**
11. **Cliquez sur l'icône de modification  pour configurer les propriétés du partage. (Reportez-vous à la section ["Propriétés des systèmes de fichiers" à la page 384.](#))**
12. **Pour accéder au partage, exécutez la commande sftp comme indiqué dans les exemples ci-dessous :**

```
sftp -o "port=218" <username> 10.x.x.151:/export/sftp
Connecting to 10.x.xx.151...
Changing to: /export/sftp
sftp>
```

Exemple avec l'option -v :

```
sftp -v -o "IdentityFile=/home/<username>/.ssh/id_dsa" -o "port=218"
root 10.x.xx.151:/export/sftp
```

Rubriques connexes

- ["Ajout de l'accès SFTP à un partage \(BUI\)" à la page 277](#)
- ["Propriétés, ports et journaux SFTP" à la page 279](#)

Propriétés, ports et journaux SFTP

Propriétés SFTP

TABLEAU 69 Propriétés SFTP

Propriété	Description
Port (pour les connexions entrantes)	Port d'écoute du service SFTP. La valeur par défaut est 218.
Autoriser la connexion de root	Autorise les connexions SFTP pour l'utilisateur root. Par défaut, cette propriété est désactivée.
Niveau de journalisation	Niveau de détail des messages du journal SFTP.
Clés SFTP	Clés publiques RSA/DSA pour l'authentification SFTP. Des commentaires peuvent être associés aux clés afin d'expliquer aux administrateurs la raison pour laquelle elles ont été ajoutées. À partir de la version logicielle 2011.1, la gestion des clés a été modifiée pour renforcer la sécurité en cas de connexion SFTP. Lorsque vous créez une clé SFTP, il est indispensable d'inclure la propriété user avec une affectation d'utilisateur valide. Les clés SFTP sont regroupées par utilisateur et authentifiées via SFTP à l'aide du nom d'utilisateur. Nous vous recommandons de recréer toutes les clés SFTP existantes qui n'incluent pas la propriété utilisateur, même si l'authentification reste possible.

Ports SFTP

Le service SFTP utilise un numéro de port non standard pour les connexions à l'appareil. Cela permet d'éviter les conflits en cas de connexion SSH administrative au port 22. Par défaut, le port SFTP est le numéro 218 et doit être spécifié sur le client SFTP avant la connexion. Par exemple, un client OpenSolaris utilisant SFTP se connecte à l'aide de la commande suivante :

```
manta# sftp -o "Port 218" root@guppy
```

Journaux SFTP

network-sftp:default : consigne les événements du service SFTP

Rubriques connexes

- ["Ajout de l'accès SFTP à un partage \(BUI\)" à la page 277](#)
- ["Configuration du service SFTP pour un accès à distance \(CLI\)" à la page 277](#)

Configuration SRP

Lorsque vous configurez un LUN sur l'appareil, vous pouvez exporter ce volume via une cible SRP (SCSI Remote Protocol). Le service SRP permet aux initiateurs d'accéder aux cibles par le biais du protocole SRP.

Pour plus d'informations sur les initiateurs et les cibles SRP, reportez-vous à la section ["Configuration du réseau de stockage SAN" à la page 127](#).

Configuration TFTP

TFTP (Trivial File Transfer Protocol) est un protocole simplifié de transfert de fichiers. Le protocole TFTP est conçu pour être petit et facile à implémenter. Il ne possède donc pas la plupart des fonctionnalités d'un FTP classique. Le protocole TFTP lit et écrit des fichiers ou du courrier électronique uniquement en amont ou en aval d'un serveur distant. Il ne peut pas lister les répertoires et ne propose pas de mécanismes d'authentification utilisateur à ce jour.

TABLEAU 70 Propriétés TFTP

Propriété	Description
Répertoire racine par défaut	Emplacement de connexion TFTP. La valeur par défaut /export correspond au sommet de la hiérarchie des partages. Tous les utilisateurs seront connectés à cet emplacement après s'être correctement authentifiés à l'aide du service TFTP.

Pour utiliser le protocole TFTP avec un partage, reportez-vous à la section ["Ajout de l'accès TFTP à un partage \(BUI\)" à la page 280](#).

▼ Ajout de l'accès TFTP à un partage (BUI)

1. **Accédez à Configuration > Services.**
2. **Assurez-vous que le service TFTP est activé et en ligne. Si ce n'est pas le cas, activez-le.**
3. **Accédez à Partages > Partages et sélectionnez ou ajoutez un partage.**
4. **Accédez à l'onglet Protocoles et vérifiez que l'accès TFTP est activé.**
5. **(Facultatif) Définissez le mode de partage Lecture seule ou Lecture/écriture.**

Configuration de l'analyse antivirus

Le service Analyse antivirus vérifie la présence de virus au niveau du système de fichiers. Lorsque vous accédez à un fichier par le biais de n'importe quel protocole, le service Analyse antivirus commence par analyser le fichier. Si un virus est trouvé, l'accès au fichier est bloqué.

et il est mis en quarantaine. Lorsqu'un fichier est analysé à l'aide des dernières définitions de virus, il n'est pas réanalysé jusqu'à sa nouvelle modification. Les fichiers auxquels accèdent les clients NFS qui ont mis des données en mémoire cache ou qui ont reçu du serveur NFSv4 des privilèges délégués de lecture ne peuvent pas être immédiatement placés en quarantaine.

Pour configurer l'analyse antivirus, reportez-vous aux sections suivantes :

- ["Configuration de l'analyse antivirus pour un partage \(BUI\)" à la page 281](#)
- ["Propriétés et journaux de l'analyse antivirus" à la page 281](#)
- ["Extensions de fichiers de l'analyse antivirus" à la page 282](#)
- ["Moteurs d'analyse" à la page 283](#)

▼ Configuration de l'analyse antivirus pour un partage (BUI)

1. **Accédez à Configuration > Services >Analyse antivirus.**
2. **Activez le service.**
3. **Définissez les propriétés requises.**
4. **Cliquez sur APPLIQUER pour valider la configuration.**
5. **Accédez à Partages.**
6. **Modifiez un système de fichiers ou un projet.**
7. **Sélectionnez l'onglet Général.**
8. **Activez l'option d'analyse antivirus.**

Rubriques connexes

- ["Propriétés et journaux de l'analyse antivirus" à la page 281](#)
- ["Extensions de fichiers de l'analyse antivirus" à la page 282](#)
- ["Moteurs d'analyse" à la page 283](#)

Propriétés et journaux de l'analyse antivirus

TABLEAU 71 Propriétés de l'analyse antivirus

Propriété	Description
Taille de fichier maximale pour l'analyse	Les fichiers dépassant cette taille ne sont pas analysés afin d'éviter une dégradation significative des performances. Les fichiers volumineux (comme les

Propriété	Description
	fichiers de base de données) ont peu de chance de s'exécuter eux-mêmes et sont par conséquent moins susceptibles de représenter un risque pour les clients vulnérables. La valeur par défaut est 1 Go.
Autoriser l'accès aux fichiers dépassant la taille maximale	Activée par défaut, cette propriété autorise l'accès aux fichiers dont la taille dépasse la taille d'analyse maximale (qui sont par conséquent exclus de l'analyse avant d'être renvoyés aux clients). Les administrateurs des sites dont les exigences en matière de sécurité sont plus strictes peuvent choisir de désactiver cette option et d'augmenter la taille maximale du fichier afin que tous les fichiers accessibles fassent l'objet d'une analyse antivirus.

TABLEAU 72 Journaux d'analyse antivirus

Journal	Description
vscan	Journal du service Analyse antivirus.

Rubriques connexes

- ["Configuration de l'analyse antivirus pour un partage \(BUI\)" à la page 281](#)
- ["Extensions de fichiers de l'analyse antivirus" à la page 282](#)
- ["Moteurs d'analyse" à la page 283](#)

Extensions de fichiers de l'analyse antivirus

Cette section décrit la procédure de contrôle des fichiers analysés. La valeur par défaut " * " entraîne l'analyse de tous les fichiers. L'analyse de tous les fichiers a des conséquences sur les performances, vous pouvez donc désigner un sous-ensemble de fichiers à analyser.

Par exemple, pour analyser uniquement les fichiers à haut risque, mais pas les fichiers dont les noms correspondent au modèle "data-archive*.zip", il est possible de configurer ce paramètre comme suit :

TABLEAU 73 Extensions de fichiers de l'analyse antivirus

Action	Modèle
Analyser	exe
Analyser	com
Analyser	bat
Analyser	doc
Analyser	zip
Ne pas analyser	data-archive*.zip
Ne pas analyser	*

Remarque - Vous devez utiliser l'option "Ne pas analyser *" pour empêcher l'analyse de tous les autres types de fichiers qui ne figurent pas explicitement dans la liste d'analyse. Un fichier nommé `file.name.exe.bat.jpg123` ne sera *pas* analysé, car seule la partie "jpg123" de son nom (extension) est comparée aux règles.

Les paramètres d'exclusion ne doivent *pas* précéder les paramètres d'inclusion. Par exemple, n'utilisez pas de paramètres "Ne pas analyser *" avant des paramètres d'inclusion puisque cela exclurait tous les types de fichiers qui suivent.

TABLEAU 74 Actions de l'analyse antivirus

Action	Modèle
Ne pas analyser	*
Analyser	exe
Analyser	com
Analyser	bat
Analyser	doc
Analyser	zip
Ne pas analyser	data-archive*.zip

Rubriques connexes

- ["Configuration de l'analyse antivirus pour un partage \(BUI\)" à la page 281](#)
- ["Propriétés et journaux de l'analyse antivirus" à la page 281](#)
- ["Moteurs d'analyse" à la page 283](#)

Moteurs d'analyse

Dans cette section, spécifiez les moteurs d'analyse à utiliser. Un moteur d'analyse est un serveur d'analyse antivirus tiers externe que l'appareil contacte par le biais du protocole ICAP (Internet Content Adaptation Protocol, RFC 3507) pour analyser les fichiers.

TABLEAU 75 Propriétés des moteurs d'analyse

Propriété	Description
Activer	Utiliser ce moteur d'analyse.
Hôte	Nom d'hôte ou adresse IP du serveur du moteur d'analyse.
Connexions maximales	Nombre maximal de connexions simultanées. Certains moteurs d'analyse fonctionnent mieux lorsque les connexions sont limitées à 8.
Port	Port du moteur d'analyse.

Rubriques connexes

- ["Configuration de l'analyse antivirus pour un partage \(BUI\)" à la page 281](#)
- ["Propriétés et journaux de l'analyse antivirus" à la page 281](#)
- ["Extensions de fichiers de l'analyse antivirus" à la page 282](#)

Configuration NIS

NIS (Network Information Service) est un service de noms pour la gestion centralisée. L'appareil peut se comporter comme un client NIS pour les utilisateurs et les groupes de telle manière que :

- Les utilisateurs NIS peuvent se connecter aux services FTP et HTTP.
- Les utilisateurs NIS peuvent recevoir des privilèges pour l'administration de l'appareil. L'appareil complète les informations NIS à l'aide de ses propres privilèges.

Remarque - Les UID et les GID compris entre 0 et 99 inclus sont réservés par le fournisseur du système d'exploitation en vue de leur utilisation dans de futures applications. Leur utilisation par des utilisateurs système finaux ou des fournisseurs de produits en couches n'est pas prise en charge et peut entraîner des problèmes de sécurité dans de futures applications.

Pour configurer NIS, reportez-vous aux sections suivantes :

- ["Ajout d'un administrateur de l'appareil à partir de NIS \(BUI\)" à la page 284](#)
- ["Propriétés et journaux NIS" à la page 285](#)

▼ Ajout d'un administrateur de l'appareil à partir de NIS (BUI)

Si le service NIS comprend un utilisateur qui souhaite se connecter à l'aide de ses informations d'identification NIS et administrer l'appareil :

Remarque - Si NIS et LDAP sont configurés sur l'appareil et que les services renvoient des informations différentes pour un élément spécifique, l'appareil utilise les données fournies par NIS.

1. **Accédez à Configuration > Services > NIS.**
2. **Définissez les propriétés relatives au domaine NIS et au serveur.**
3. **Cliquez sur APPLIQUER pour valider la configuration.**
4. **Accédez à Configuration > Utilisateurs.**
5. **Ajoutez un utilisateur d'annuaire.**

6. Définissez le nom d'utilisateur sur son nom d'utilisateur NIS.
7. Continuez en suivant les instructions de la section "[Configuration des utilisateurs](#)" à la page 160 pour ajouter des autorisations à cet utilisateur.

Rubriques connexes

- "[Propriétés et journaux NIS](#)" à la page 285

Propriétés et journaux NIS

TABLEAU 76 Propriétés NIS

Propriété	Description
Domaine	Domaine NIS à utiliser.
Serveur(s) : Rechercher à l'aide d'une diffusion	L'appareil émet une diffusion NIS afin de localiser les serveurs NIS de ce domaine.
Serveur(s) : Utiliser les serveurs listés	Nom d'hôte ou adresse IP des serveurs NIS.

L'appareil se connecte au premier serveur NIS répertorié, ou à un serveur trouvé à l'aide de la diffusion, et il passe au suivant si ce serveur ne répond plus.

TABLEAU 77 Journaux NIS

Journal	Description
network-nis-client:default	Journal du service client NIS.
appliance-kit-nsswitch:default	Journal du service de noms de l'appareil à travers lequel les requêtes NIS sont effectuées.
system-identity:domain	Journal du configurateur de nom de domaine de l'appareil.

Rubriques connexes

- "[Ajout d'un administrateur de l'appareil à partir de NIS \(BUI\)](#)" à la page 284

Configuration LDAP

LDAP (Lightweight Directory Access Protocol) est un service d'annuaire pour la gestion centralisée d'utilisateurs, de groupes, de noms d'hôte et d'autres ressources (appelées objets). Ce service se comporte comme un client LDAP sur l'appareil de telle manière que :

- Les utilisateurs LDAP peuvent se connecter aux services FTP et HTTP.
- Des noms d'utilisateur LDAP (plutôt que les ID numériques) peuvent être utilisés pour configurer les listes ACL du répertoire root sur un partage.

- Les utilisateurs LDAP peuvent recevoir des privilèges pour l'administration de l'appareil. L'appareil complète les informations LDAP à l'aide de ses propres privilèges.
- Le certificat du serveur LDAP peut être autosigné.
- Il est impossible de fournir une liste de certificats CA ; chaque certificat doit être accepté individuellement par l'administrateur de l'appareil.
- Lorsqu'un certificat de serveur LDAP expire, vous devez supprimer le serveur de la liste puis l'ajouter à nouveau pour qu'il accepte son nouveau certificat.

Remarque - Les UID compris entre 0 et 99 inclus sont réservés par le fournisseur du système d'exploitation en vue de leur utilisation dans de futures applications. Leur utilisation par des utilisateurs système finaux ou des fournisseurs de produits en couches n'est pas prise en charge et peut entraîner des problèmes de sécurité dans de futures applications.

Pour configurer LDAP, reportez-vous aux sections suivantes :

- ["Ajout d'un administrateur de l'appareil \(BUI\)" à la page 286](#)
- ["Définition de propriétés à plusieurs paires valeur attribut \(CLI\)" à la page 287](#)
- Configuration des paramètres de sécurité LDAP - [BUI](#), [CLI](#)
- ["Propriétés LDAP" à la page 290](#)
- ["Mappages LDAP personnalisés" à la page 291](#)

▼ Ajout d'un administrateur de l'appareil (BUI)

Pour permettre à un utilisateur LDAP existant de se connecter à l'aide des informations d'identification LDAP et de gérer l'appareil, procédez comme suit .

Remarque - Si NIS et LDAP sont configurés sur l'appareil et que les services renvoient des informations différentes pour un élément spécifique, l'appareil utilise les données fournies par NIS.

1. **Accédez à Configuration > Services > LDAP et entrez les propriétés que vous souhaitez utiliser.**
Pour plus d'informations sur les propriétés disponibles, reportez-vous à la section ["Propriétés LDAP" à la page 290](#).
2. **Pour appliquer les propriétés sélectionnées, cliquez sur Appliquer. Cliquez sur Rétablir pour recommencer.**
3. **Pour ajouter des serveurs LDAP, cliquez sur l'icône d'ajout d'élément  dans la section Serveurs.**
Pour plus d'informations sur les serveurs, reportez-vous à la section Serveurs, dans ["Propriétés LDAP" à la page 290](#).

4. **Pour configurer le serveur LDAP, saisissez l'adresse du serveur dans la case Nouveau serveur LDAP et sélectionnez la source de certificat LDAP de votre choix.**

En ce qui concerne la source du certificat, sélectionnez Serveur pour lancer une recherche sur le serveur actuel et extraire le certificat (de manière non sécurisée), puis utilisez ce dernier pour valider le certificat présenté ultérieurement.

5. **Accédez à Configuration > Utilisateurs et ajoutez des utilisateurs en utilisant des noms d'utilisateur LDAP.**

Pour plus d'informations sur l'ajout d'utilisateurs, reportez-vous à la section "[Configuration des utilisateurs](#)" à la page 160.

Rubriques connexes

- "[Définition de propriétés à plusieurs paires valeur attribut \(CLI\)](#)" à la page 287
- "[Propriétés LDAP](#)" à la page 290
- "[Mappages LDAP personnalisés](#)" à la page 291

▼ Définition de propriétés à plusieurs paires valeur attribut (CLI)

Pour définir les valeurs de propriétés LDAP comportant plusieurs paires de valeurs d'attributs avec signe égal (=), entourez chaque paire de valeurs de guillemets (doubles).

1. **Accédez à configuration services ldap.**
2. **Pour définir plusieurs paires de valeurs d'attribut, utilisez les commandes suivantes :**

```
hostname:configuration services ldap> set user_mapattr="uid=uid",
"uidnumber=uidNumber","gidnumber=gidNumber",
"gecos=displayName","description=distinguishedName",
"homedirectory=unixHomeDirectory"
```

Rubriques connexes

- "[Ajout d'un administrateur de l'appareil \(BUI\)](#)" à la page 286
- "[Propriétés LDAP](#)" à la page 290
- "[Mappages LDAP personnalisés](#)" à la page 291

▼ Configuration des paramètres de sécurité LDAP (BUI)

Pour configurer les paramètres de sécurité du service LDAP, utilisez la procédure suivante.

1. **Accédez à Configuration > Services.**

2. **Sous Services d'annuaire, sélectionnez LDAP.**

3. **Pour Paramètres de sécurité, vous devez sélectionner l'une des options suivantes :**

- **Anonyme** : permet à l'appareil d'accéder uniquement aux données accessibles à tous. Pour activer si vous le souhaitez les protocoles SSL et TLS, sélectionnez la case à cocher Activer SSL/TLS.
- **Automatique** : authentifie l'appareil à l'aide de l'identité et des informations d'identification de l'utilisateur. L'authentification automatique utilise le chiffrement Kerberos et la méthode d'authentification SASL/GSSAPI.
- **Proxy** : spécifie l'authentification par le biais d'un proxy pour un compte utilisateur spécifique. Définissez les options suivantes :
 - (En option) **Activer SSL/TLS** : sélectionnez cette case à cocher pour activer les protocoles SSL et TLS. Cette option est fortement recommandée lors de l'utilisation de la méthode d'authentification simple pour que le nom distinctif et le mot de passe de l'utilisateur ne soient pas envoyés en texte brut.
 - **Méthode d'authentification** : sélectionnez Simple (RFC 4513) ou SASL/DIGEST-MD5.
 - **DN Proxy** : nom distinctif du compte utilisé pour l'authentification de proxy.
 - **Mot de passe Proxy** : mot de passe du compte utilisé pour l'authentification de proxy.

4. **Cliquez sur APPLIQUER.**

Rubriques connexes

- ["Propriétés LDAP" à la page 290](#)

▼ Configuration des paramètres de sécurité LDAP (CLI)

Pour configurer les paramètres de sécurité du service LDAP, utilisez la procédure suivante. Pour connaître des combinaisons de paramètres de propriété valides, consultez le tableau à la fin de cette tâche.

1. **Accédez à configuration services ldap et saisissez show pour afficher les propriétés.**

```
hostname:configuration services ldap> show
Properties:
    <status> = enabled
    default_servers =
    proxy_dn =
    proxy_password =
    base_dn =
    search_scope = one
    cred_level = anonymous
```



```

auth_method = none
use_tls = false
user_search =
user_mapattr =
user_mapobjclass =
group_search =
group_mapattr =
group_mapobjclass =
netgroup_search =
netgroup_mapattr =
netgroup_mapobjclass =

```

2. Pour définir le niveau d'authentification, saisissez `set cred_level=` et l'une des options suivantes :

- **anonymous** : autorise une authentification anonyme pour accéder aux données accessibles à tous.
- **self** : fournit une authentification automatique aux utilisateurs en fonction de leur identité et de leurs informations d'identification. L'authentification automatique utilise le chiffrement Kerberos et la méthode d'authentification SASL/GSSAPI.
- **proxy** : spécifie l'authentification par le biais d'un proxy pour un compte utilisateur spécifique.

```

hostname:configuration services ldap> set cred_level=proxy
cred_level = proxy (uncommitted)

```

3. Pour définir la méthode d'autorisation, saisissez `set auth_method=` et l'une des options suivantes :

- **none** : aucun (s'utilise avec **anonymous**)
- **sasl/GSSAPI** : SASL/GSSAPI (s'utilise avec **self**)
- **simple** : Simple, RFC 4513 (s'utilise avec **proxy**)
- **sasl/DIGEST-MD5** : SASL/DIGEST-MD5 (s'utilise avec **proxy**)

```

hostname:configuration services ldap> set auth_method=simple
auth_method = simple (uncommitted)

```

4. Pour activer ou désactiver SSL/TLS, saisissez `set use_tls=` et **true ou **false**.**

L'activation de SSL/TLS est fortement recommandée lors de l'utilisation de la méthode d'authentification simple pour que le nom distinctif et le mot de passe de l'utilisateur ne soient pas envoyés en texte brut.

```

hostname:configuration services ldap> set use_tls=true
use_tls = true (uncommitted)

```

5. Si le niveau d'authentification est défini sur **proxy, saisissez `set proxy_dn=`, ainsi que le nom distinctif du compte utilisé pour l'authentification proxy. Saisissez ensuite `set proxy_password=`, ainsi que le mot de passe du compte.**

```
hostname:configuration services ldap> set proxy_dn=ProxyName
proxy_dn = ProxyName (uncommitted)
hostname:configuration services ldap> set proxy_password=MyPassword5
proxy_password = ***** (uncommitted)
```

6. Saisissez commit.

```
hostname:configuration services ldap> commit
```

7. Reportez-vous au tableau suivant pour connaître les combinaisons de paramètres de propriété de sécurité valides.

cred_level	auth_method	use_tls
anonymous	none	true
	none	false
self	sasl/GSSAPI	false
proxy	simple	true
	simple	false
<i>Autorisé, mais non recommandé, car le nom distinctif et le mot de passe de l'utilisateur seront envoyés en texte brut.</i>		
	sasl/DIGEST-MD5	true
	sasl/DIGEST-MD5	false

Rubriques connexes

- ["Propriétés LDAP" à la page 290](#)

Propriétés LDAP

Afin d'obtenir les paramètres adaptés à votre environnement, consultez votre administrateur de serveur LDAP.

Schéma

- **DN de recherche de base** : nom distinctif de l'objet de base (point de départ des recherches de répertoire)
- **Etendue de la recherche** : définit les objets recherchés dans l'annuaire LDAP par rapport à l'objet de base. Les résultats de la recherche peuvent être limités aux objets situés directement en dessous de l'objet de recherche de base (niveau 1) ou bien inclure tous les objets situés en dessous de l'objet de recherche de base (sous-arborescence). La valeur par défaut est one-level.
- **Définition du schéma** : schéma utilisé par l'appareil. Cette propriété permet aux administrateurs de remplacer le descripteur de recherche par défaut, les

mappages d'attributs et de classes d'objet pour les utilisateurs, les groupes et groupes réseau. Pour plus d'informations, reportez-vous à la section "[Mappages LDAP personnalisés](#)" à la page 291.

Paramètres de sécurité

- **S'authentifier en tant que** : informations d'identification permettant d'authentifier l'appareil sur le serveur LDAP.
- **Activer SSL/TLS** : active/désactive TLS (Transport Layer Security, le descendant de SSL) pour établir des connexions sécurisées au serveur LDAP. Si l'authentification est définie sur Automatique, cette option n'est pas disponible, car la méthode automatique utilise le chiffrement Kerberos.
- **Méthode d'authentification** : méthode permettant d'authentifier l'appareil sur le serveur LDAP. Vous pouvez uniquement configurer ce paramètre si l'authentification est définie sur Proxy.

Serveurs LDAP

- **Serveurs** : liste des serveurs LDAP à utiliser. Si un seul serveur est spécifié, l'appareil utilise uniquement ce serveur et les services LDAP deviennent indisponibles en cas d'échec de ce serveur. Si plusieurs serveurs sont spécifiés, tout serveur fonctionnel peut être utilisé à tout moment, sans préférence. Si l'un des serveurs subit une défaillance, un autre serveur de la liste prend le relais. Les services LDAP restent disponibles à moins que tous les serveurs spécifiés ne soient hors service.

Rubriques connexes

- "[Configuration des paramètres de sécurité LDAP \(BUI\)](#)" à la page 287
- "[Configuration des paramètres de sécurité LDAP \(CLI\)](#)" à la page 288

Mappages LDAP personnalisés

Pour rechercher des utilisateurs et des groupes dans l'annuaire LDAP, l'appareil utilise un descripteur de recherche et doit connaître les classes d'objet correspondant aux utilisateurs et aux groupes, ainsi que les attributs correspondant aux propriétés requises. Par défaut, l'appareil utilise les classes d'objet spécifiées par le document RFC 2307 (*posixAccount* et *posixGroup*) ainsi que les descripteurs de recherche par défaut mentionnés ci-dessous qui peuvent néanmoins être personnalisés pour des environnements différents. Le nom distinctif de recherche de base utilisé dans les exemples ci-dessous est `dc=example,dc=com`.

TABLEAU 78 Mappages LDAP personnalisés

Descripteur de recherche	Valeur par défaut	Exemple
utilisateurs	<code>ou=people,nom distinctif de recherche de base</code>	<code>ou=people,dc=example,dc=com</code>
groupes	<code>ou=group,nom distinctif de recherche de base</code>	<code>ou=group,dc=example,dc=com</code>

Descripteur de recherche	Valeur par défaut	Exemple
groupes réseau	<i>ou=netgroup,nom distinctif de recherche de base</i>	<i>ou=netgroup,dc=example,dc=com</i>

Le descripteur de recherche, les classes d'objet et les attributs utilisés peuvent être personnalisés à l'aide de la propriété Définition du schéma. Pour remplacer le descripteur de recherche par défaut, saisissez le nom distinctif entier que vous souhaitez utiliser. L'appareil utilise cette valeur sans la modifier et ignore les valeurs des propriétés DN de recherche de base et Portée de la recherche. Pour remplacer des objets et des attributs d'utilisateur, de groupe et de groupe réseau, sélectionnez l'onglet approprié ("Utilisateurs", "Groupes", ou "Groupes réseau") et spécifiez les mappages en respectant la syntaxe *default = new*, où *default* est la valeur par défaut et *new* la valeur que vous souhaitez utiliser. Par exemple :

- Pour utiliser *unixaccount* à la place de *posixAccount* en tant que classe d'objet utilisateur, saisissez *posixAccount = unixaccount* dans les mappages de classe d'objet de l'onglet Utilisateurs.
- Pour utiliser *employeenumber* à la place de *uid* en tant qu'attribut pour les objets utilisateur, saisissez *uid = employeenumber* dans Mappages d'attributs de l'onglet Utilisateurs.
- Pour utiliser *unixgroup* à la place de *posixGroup* en tant que classe d'objet de groupe, saisissez *posixGroup = unixgroup* dans les mappages de classe d'objet de l'onglet Groupes.
- Pour utiliser *groupaccount* à la place de *cn* en tant qu'attribut pour les objets de groupe, saisissez *cn = groupaccount* dans Mappages d'attributs de l'onglet Groupes.

Voici une liste de classes et d'attributs d'objets que vous pouvez souhaiter mapper :

Classes

- *posixAccount*
- *posixGroup*
- *shadowAccount*

Attributs : Utilisateurs

- *uid*
- *uidNumber*
- *gidNumber*
- *gecos*
- *homeDirectory*
- *loginShell*
- *userPassword*

Attributs : Groupes

- *uid*
- *memberUid*
- *cn*

- userPassword
- gidNumber
- member
- uniqueMember
- memberOf
- isMemberOf

Rubriques connexes

- ["Ajout d'un administrateur de l'appareil \(BUI\)" à la page 286](#)
- ["Définition de propriétés à plusieurs paires valeur attribut \(CLI\)" à la page 287](#)
- ["Propriétés LDAP" à la page 290](#)

Configuration d'Active Directory

Le service Active Directory fournit l'accès à une base de données Microsoft Active Directory qui stocke les informations relatives aux utilisateurs, groupes, partages et à d'autres objets partagés. Ce service inclut deux modes, domaine et groupe de travail, qui régissent la manière dont les utilisateurs SMB sont authentifiés. Lorsque vous travaillez en mode domaine, les clients SMB sont authentifiés via le contrôleur de domaine AD. En mode groupe de travail, les clients SMB sont authentifiés localement en tant qu'utilisateurs locaux. Pour plus d'informations sur les utilisateurs locaux, reportez-vous à la section ["Configuration des utilisateurs" à la page 160](#).

Pour configurer Active Directory, reportez-vous aux sections suivantes :

- ["Ajout à un domaine AD \(BUI\)" à la page 293](#)
- ["Ajout à un groupe de travail AD \(BUI\)" à la page 294](#)
- ["Configuration d'Active Directory \(CLI\)" à la page 294](#)
- ["Rejoindre le domaine Active Directory" à la page 296](#)
- ["Domaines et groupes de travail Active Directory" à la page 297](#)
- ["Prise en charge de Windows Server par Active Directory" à la page 297](#)

▼ Ajout à un domaine AD (BUI)

1. **(Facultatif) Configurez un site Active Directory dans le contexte SMB.**
2. **(Facultatif) Configurez un contrôleur de domaine préféré dans le contexte SMB.**
3. **Activez le service NTP ou assurez-vous que les horloges de l'appareil et du contrôleur de domaine sont synchronisées à cinq minutes près.**
4. **Assurez-vous que votre infrastructure DNS délègue correctement des responsabilités au domaine Active Directory ou ajoutez l'adresse IP de votre**

contrôleur de domaine en tant que serveur de noms supplémentaire dans le contexte DNS.

5. Accédez à **Configuration > Services > Active Directory** et cliquez sur **Rejoindre le domaine**.
6. Configurez le domaine Active Directory, le nom de l'utilisateur administratif et son mot de passe.
7. Cliquez sur **APPLIQUER** pour valider la configuration.

Rubriques connexes

- ["Ajout à un groupe de travail AD \(BUI\)" à la page 294](#)
- ["Configuration d'Active Directory \(CLI\)" à la page 294](#)
- ["Rejoindre le domaine Active Directory" à la page 296](#)
- ["Domaines et groupes de travail Active Directory" à la page 297](#)
- ["Prise en charge de Windows Server par Active Directory" à la page 297](#)

▼ Ajout à un groupe de travail AD (BUI)

1. Accédez à **Configuration > Services > Active Directory** et cliquez sur **Rejoindre le groupe de travail**.
2. Entrez le nom du groupe de travail Windows.
3. Cliquez sur **APPLIQUER** pour valider la configuration.

Rubriques connexes

- ["Ajout à un domaine AD \(BUI\)" à la page 293](#)
- ["Configuration d'Active Directory \(CLI\)" à la page 294](#)
- ["Rejoindre le domaine Active Directory" à la page 296](#)
- ["Domaines et groupes de travail Active Directory" à la page 297](#)
- ["Prise en charge de Windows Server par Active Directory" à la page 297](#)

▼ Configuration d'Active Directory (CLI)

1. Accédez à **configuration services ad**.

```
hostname:> configuration services ad
```
2. Pour consulter une configuration existante, entrez **show**.

```
hostname:configuration services ad> show
```

Properties:

```
<status> = online
mode = domain
domain = eng.fishworks.com
```

Children:

```
domain => Join an Active Directory domain
workgroup => Join a Windows workgroup
```

3. Notez que l'appareil fonctionne actuellement dans le domaine `eng.fishworks.com`.

L'exemple ci-dessous illustre comment quitter ce domaine et rejoindre un groupe de travail.

```
hostname:configuration services ad> workgroup
hostname:configuration services ad workgroup> set workgroup=WORKGROUP
hostname:configuration services ad workgroup> commit
hostname:configuration services ad workgroup> done
hostname:configuration services ad> show
Properties:
    <status> = disabled
    mode = workgroup
workgroup = WORKGROUP
```

4. Pour configurer le site et le contrôleur de domaine préféré en vue de rejoindre un autre domaine, entrez les commandes suivantes :

```
hostname:configuration services ad> done
hostname:> configuration services smb
hostname:configuration services smb> set ads_site=sf
hostname:configuration services smb> set pdc=192.168.3.21
hostname:configuration services smb> commit
hostname:configuration services smb> show
Properties:
    <status> = online
    lmauth_level = 4
    pdc = 192.168.3.21
    ads_site = sf
hostname:configuration services smb> done
```

5. Pour rejoindre le nouveau domaine après avoir configuré les propriétés requises, entrez les commandes suivantes.

Lorsque vous rejoignez un domaine AD, vous devez définir l'utilisateur et le mot de passe à chaque fois que vous validez le noeud.

```
hostname:> configuration services ad
hostname:configuration services ad> domain
hostname:configuration services ad domain> set domain=fishworks.com
hostname:configuration services ad domain> set user=Administrator
hostname:configuration services ad domain> set password=*****
hostname:configuration services ad domain> commit
hostname:configuration services ad domain> done
hostname:configuration services ad> show
```

Properties:

```
<status> = online
mode = domain
domain = fishworks.com
```

Rubriques connexes

- ["Ajout à un domaine AD \(BUI\)" à la page 293](#)
- ["Ajout à un groupe de travail AD \(BUI\)" à la page 294](#)
- ["Rejoindre le domaine Active Directory" à la page 296](#)
- ["Domaines et groupes de travail Active Directory" à la page 297](#)
- ["Prise en charge de Windows Server par Active Directory" à la page 297](#)

Rejoindre le domaine Active Directory

Si aucun compte n'existe dans Active Directory par défaut, un compte de confiance d'ordinateur est automatiquement créé pour le système dans le conteneur défini par défaut pour les comptes d'ordinateurs (cn=Computers). Ce compte fait partie de l'opération permettant de rejoindre le domaine. Les utilisateurs suivants sont autorisés à rejoindre le domaine :

- **Administrateur de domaine** : peut joindre un nombre quelconque de systèmes au domaine avec des comptes de confiance d'ordinateur placés dans tous les conteneurs, sans restrictions.
- **Administrateur délégué ayant autorité sur une ou plusieurs unités d'organisation** : peut joindre un nombre quelconque de systèmes à un domaine à l'aide d'un compte d'ordinateur qui se trouve dans l'une des unités d'organisation qu'ils dirigent.
- **Utilisateur normal avec des comptes d'ordinateur pré-transférés par l'administrateur** : peut joindre un système au domaine comme pré-autorisé par l'administrateur.
- **Utilisateur normal** : généralement autorisé à joindre un nombre limité de systèmes.

Les propriétés suivantes sont disponibles pour rejoindre un domaine Active Directory :

- **Domaine Active Directory** : nom complètement qualifié ou nom NetBIOS d'un domaine Active Directory
- **Utilisateur** : utilisateur AD possédant les informations d'identification permettant de créer un compte d'ordinateur dans Active Directory
- **Mot de passe** : mot de passe de l'utilisateur administratif
- **Unité d'organisation** : spécifie une unité d'organisation alternative dans laquelle le compte de confiance du système est créé. L'unité d'organisation est spécifiée sous forme de liste répertoriant une ou plusieurs paires de noms séparées par des virgules au format de nom distinctif (DN) utilisé par le domaine ; par exemple : ou=innerOU,ou=outerOU.
- **Utiliser un compte précréé** : si le compte du système existe mais qu'il ne fait pas partie de l'unité d'organisation spécifiée, utilisez le compte précréé.

Rubriques connexes

- ["Ajout à un domaine AD \(BUI\)" à la page 293](#)
- ["Ajout à un groupe de travail AD \(BUI\)" à la page 294](#)
- ["Configuration d'Active Directory \(CLI\)" à la page 294](#)
- ["Domaines et groupes de travail Active Directory" à la page 297](#)
- ["Prise en charge de Windows Server par Active Directory" à la page 297](#)

Domaines et groupes de travail Active Directory

La propriété configurable pour rejoindre un groupe de travail est Windows Workgroup.

Au lieu d'activer et de désactiver directement le service, ce dernier est modifié par le fait de rejoindre un domaine ou un groupe de travail. Pour rejoindre un domaine, il faut créer un compte pour l'appareil dans le domaine Active Directory approprié. Le nom de compte peut contenir 15 caractères au maximum et ne doit ressembler à aucun autre nom enregistré dans le domaine Active Directory. Sinon, des conflits peuvent se produire avec des appareils de dénomination proche et entraîner des problèmes de fonctionnalité. Une fois le compte d'ordinateur établi, l'appareil peut interroger la base de données en toute sécurité pour obtenir des informations relatives aux utilisateurs, aux groupes et aux partages.

En rejoignant un groupe de travail, vous quittez implicitement un domaine Active Directory et les clients SMB stockés dans la base de données Active Directory ne peuvent pas se connecter aux partages.

Signature LDAP d'Active Directory

Aucune option de configuration n'existe pour la signature LDAP car cette option est automatiquement négociée en cas de communication avec un contrôleur de domaine. La signature LDAP est mise en oeuvre lors de la communication entre l'appareil de stockage et le contrôleur de domaine, tandis que les opérations de signature SMB s'effectuent lors de la communication entre les clients SMB et l'appareil de stockage.

Rubriques connexes

- ["Ajout à un domaine AD \(BUI\)" à la page 293](#)
- ["Ajout à un groupe de travail AD \(BUI\)" à la page 294](#)
- ["Configuration d'Active Directory \(CLI\)" à la page 294](#)
- ["Rejoindre le domaine Active Directory" à la page 296](#)
- ["Prise en charge de Windows Server par Active Directory" à la page 297](#)

Prise en charge de Windows Server par Active Directory

Les versions 2011.1.5 et ultérieures assurent une prise en charge complète de Windows Server 2012.

TABLEAU 79 Prise en charge de Windows Server 2008 par Active Directory

Version Windows	Versions logicielles prises en charge	Solutions de contournement
Windows Server 2003	Toutes	Aucune
Windows Server 2008 SP1	2009.Q2 3.1 et versions antérieures	Appliquer le correctif indiqué dans l'article KB957441 si nécessaire, voir la section B.
	2009.Q2 4.0 - 2011.1.1	Appliquer le correctif indiqué dans l'article KB951191 et le correctif de KB957441 si nécessaire, voir les sections A et B.
	2011.1.2 et versions ultérieures	Appliquer le correctif indiqué dans l'article KB951191 si nécessaire, voir la section A.
Windows Server 2008 SP2	2009.Q2 4.0 - 2011.1.1	Voir section C
	2011.1.2 et versions ultérieures	Aucune
Windows Server 2008 R2	2009.Q2 4.0 - 2011.1.1	Voir section C
	2011.1.2 et versions ultérieures	Aucune

Prise en charge de Windows Server 2008 par Active Directory Section A : problème lié à Kerberos (KB951191)

- Si vous effectuez une mise à niveau vers la version 2009.Q2.4.0 ou ultérieure et si votre contrôleur de domaine Windows 2008 exécute Windows Server 2008 SP2 ou R2, aucune action n'est requise.
- Si vous effectuez une mise à niveau vers la version 2009.Q2.4.0 ou ultérieure et si votre contrôleur de domaine Windows 2008 exécute Windows Server 2008 SP1, vous devez appliquer le correctif décrit dans l'article KB951191 ou installer Windows 2008 SP2.

Prise en charge de Windows Server 2008 par Active Directory Section B : problème lié à NTLMv2 (KB957441)

- Les instructions suivantes s'appliquent uniquement si votre appareil exécute une version du logiciel antérieure à la version 2011.1.2 :
- Si votre contrôleur de domaine exécute Windows Server 2008 SP1, appliquez le correctif indiqué dans l'article <http://support.microsoft.com/kb/957441/> (<http://support.microsoft.com/kb/957441/>), lequel résout un problème lié à NTLMv2 qui empêche l'appareil de rejoindre le domaine avec son paramètre LMCompatibilityLevel par défaut.
- Si le paramètre LMCompatibilityLevel du contrôleur de domaine Windows 2008 SP1 est réglé sur 5, ce correctif doit être installé. Après avoir appliqué le correctif, vous devez créer et définir une nouvelle clé de registre, comme indiqué dans l'article KB957441.
- Si vous mettez à niveau vers la version 2011.1.2 ou ultérieure, le correctif mentionné ci-dessus n'est pas nécessaire.

Prise en charge de Windows Server 2008 par Active Directory Section C : remarque sur NTLMv2

- Les instructions suivantes s'appliquent uniquement si votre appareil exécute une version du logiciel antérieure à la version 2011.1.2 : si votre contrôleur de domaine exécute Windows Server 2008 SP2 ou R2, inutile d'appliquer le correctif. En revanche, il faut appliquer le paramètre de registre décrit dans l'article KB957441.
- Si vous mettez à niveau vers la version 2011.1.2 ou ultérieure, aucune action n'est nécessaire.

Rubriques connexes

- ["Ajout à un domaine AD \(BUI\)" à la page 293](#)
- ["Ajout à un groupe de travail AD \(BUI\)" à la page 294](#)
- ["Configuration d'Active Directory \(CLI\)" à la page 294](#)
- ["Rejoindre le domaine Active Directory" à la page 296](#)
- ["Domaines et groupes de travail Active Directory" à la page 297](#)

Configuration du mappage des identités

Le mappage des identités vous permet d'associer des identités Windows et UNIX, ce qui permet à un client SMB et un client NFS d'accéder au même ensemble de fichiers. Le service de mappage des identités gère les identités des utilisateurs Windows et UNIX simultanément en créant et en tenant à jour une base de données des mappages entre les identificateurs d'utilisateur (UID) et les identificateurs de groupe (GID) UNIX et les identificateurs de sécurité Windows (SID).

Pour gérer le mappage des identités, exécutez les tâches suivantes :

- Configuration du mappage des identités - [BUI](#), [CLI](#)
- Création d'une règle de mappage - [BUI](#), [CLI](#)
- ["Affichage d'un mappage \(BUI\)" à la page 305](#)
- Vidage des mappages à partir du cache - [BUI](#), [CLI](#)

Pour comprendre le mappage des identités, reportez-vous aux rubriques suivantes :

- ["Pratiques recommandées pour le mappage des identités" à la page 307](#)
- ["Concepts de mappage des identités" à la page 308](#)
- ["Mappages mis en cache et éphémères" à la page 309](#)
- ["Sensibilité à la casse du mappage des identités" à la page 309](#)
- ["Symboles de direction d'une règle de mappage" à la page 310](#)

▼ Configuration du mappage des identités (BUI)

Utilisez la procédure suivante pour configurer un mappage des identités.

Avant de commencer

Assurez-vous de n'avoir rejoint aucun domaine Active Directory. Pour plus d'informations sur Active Directory, reportez-vous à la section "[Configuration d'Active Directory](#)" à la page 293.

1. **Accédez à Configuration > Services > Mappage des identités > Propriétés.**
2. **Sélectionnez l'un des modes de mappage suivants.**
 - **Basé sur les règles**
 - **Basé sur un annuaire** : définit les attributs suivants.
 - **Attribut AD - Nom d'utilisateur UNIX** : nom figurant dans la base de données Active Directory du nom d'utilisateur UNIX équivalent
 - **Attribut AD - Nom de groupe UNIX** : nom figurant dans la base de données Active Directory du nom de groupe UNIX équivalent
 - **Attribut LDAP natif - Nom d'utilisateur Windows** : nom figurant dans la base de données LDAP de l'identité Windows équivalente
 - **IDMU**
3. **Pour enregistrer vos paramètres, cliquez sur APPLIQUER. Pour effacer vos paramètres, cliquez sur RETABLIR.**

Rubriques connexes

- Pour plus d'informations sur les différents modes de mappage, reportez-vous à la section "[Concepts de mappage des identités](#)" à la page 308.
- Pour créer une règle de mappage d'autorisation ou de refus, reportez-vous à la section "[Création d'une règle de mappage \(BUI\)](#)" à la page 301.

▼ Configuration du mappage des identités (CLI)

Utilisez la procédure suivante pour configurer un mappage des identités.

Avant de commencer

Assurez-vous de n'avoir rejoint aucun domaine Active Directory.

1. **Accédez à configuration services idmap.**
2. **Saisissez get pour afficher les propriétés de mappage des identités.**

```
hostname:configuration services idmap> get
```

```
<status> = online
ad_unixuser_attr =
ad_unixgroup_attr =
nldap_winname_attr =
directory_based_mapping = none
```

The three *_attr properties correspond to the three fields on C>S>Identity Mapping>Properties.

3. Définissez `directory_based_mapping` sur l'un des modes de mappage suivants.

- Pour utiliser le mappage basé sur une règle, définissez `directory_based_mapping` sur `none`.

```
hostname:configuration services idmap> set directory_based_mapping=none
hostname:configuration services idmap>
```

- Pour utiliser le mappage basé sur un répertoire, définissez `directory_based_mapping` sur `name` et assignez chacun des attributs suivants.

- `ad_unixuser_attr` : nom figurant dans la base de données Active Directory du nom d'utilisateur UNIX équivalent
- `ad_unixgroup_attr` : nom figurant dans la base de données Active Directory du nom de groupe UNIX équivalent
- `nldap_winname_attr` : nom figurant dans la base de données LDAP de l'identité Windows équivalente

```
hostname:configuration services idmap> set directory_based_mapping=name
hostname:configuration services idmap> set ad_unixuser_attr=demo_unixuser
hostname:configuration services idmap> set ad_unixgroup_attr=demo_group
hostname:configuration services idmap> set nldap_winname_attr=demo_winuser
```

- Pour utiliser IDMU (Identity Management for UNIX), définissez `directory_based_mapping` sur `idmu`.

```
hostname:configuration services idmap> set directory_based_mapping=idmu
hostname:configuration services idmap>
```

Rubriques connexes

- Pour plus d'informations sur les différents modes de mappage, reportez-vous à la section ["Concepts de mappage des identités"](#) à la page 308.
- Pour créer une règle de mappage d'autorisation ou de refus, reportez-vous à la section ["Création d'une règle de mappage \(CLI\)"](#) à la page 303.

▼ Création d'une règle de mappage (BUI)

Utilisez la procédure suivante pour accorder ou refuser des informations d'identification à des utilisateurs spécifiques par le biais du service de mappage des identités. Une règle de mappage d'autorisation accorde à l'identité Windows des informations d'identification à partir d'une identité UNIX ou vice versa. Une règle de mappage de refus empêche une identité Windows de recevoir les informations d'identification d'une identité UNIX ou vice versa.

Remarque - Si vous créez une règle de mappage qui bloque un utilisateur particulier et que le nom de l'utilisateur est ultérieurement modifié, le mappage ne bloque plus cet utilisateur.

Avant de commencer

Configurez un mappage basé sur une règle, comme indiqué dans la section "[Configuration du mappage des identités \(BUI\)](#)" à la page 299.

1. **Accédez à Configuration > Services > Mappage des identités > Règles.**
2. **Cliquez sur l'icône d'ajout d'élément  en regard de Règles.**
3. **Dans la boîte de dialogue Ajouter une règle de mappage, choisissez Allow ou Deny comme type de mappage.**
4. **Remplissez le reste des champs selon le type de mappage sélectionné.**
 - **Mappage d'autorisation :**
 - **Sens du mappage :** choisir un sens dans lequel s'effectue le mappage.
 - **Domaine Windows :** saisir le domaine Active Directory de l'identité Windows, ou sélectionner Tous.
 - **Identité Windows :** saisir le nom de l'identité Windows.
 - **Identité Unix :** saisir le nom de l'identité Unix.
 - **Type d'identité Unix :** sélectionner User ou Group.
 - **Mappage de refus :**
 - a. **Pour définir le sens du mappage, choisissez une des deux options.**
 - **Bloquer le mappage des identités Windows :** empêche une identité Windows d'obtenir les informations d'identification d'une identité UNIX.
 - **Bloquer le mappage des identités Unix :** empêche une identité UNIX d'obtenir les informations d'identification d'une identité Windows.
 - b. **Saisissez les informations relatives à l'identité Windows ou UNIX.**
 - **Si vous avez sélectionné Bloquer le mappage des identités Windows,** saisissez le domaine et l'identité Windows à bloquer.
 - **Si vous avez sélectionné Bloquer le mappage des identités UNIX,** saisissez l'identité UNIX et le type d'identité à bloquer.
5. **Cliquez sur AJOUTER.**

Le nouveau mappage s'affiche dans la liste Règles.

Rubriques connexes

- ["Symboles de direction d'une règle de mappage" à la page 310](#)

▼ Création d'une règle de mappage (CLI)

Utilisez la procédure suivante pour accorder ou refuser des informations d'identification à des utilisateurs spécifiques par le biais du service de mappage des identités. Une règle de mappage d'autorisation accorde à l'identité Windows des informations d'identification à partir d'une identité UNIX ou vice versa. Une règle de mappage de refus empêche une identité Windows de recevoir les informations d'identification d'une identité UNIX ou vice versa.

Remarque - Si vous créez une règle de mappage qui bloque un utilisateur particulier et que le nom de l'utilisateur est modifié, le mappage ne bloque plus cet utilisateur.

Avant de commencer

Configurez un mappage basé sur une règle, comme indiqué dans la section ["Configuration du mappage des identités \(CLI\)" à la page 300](#).

1. **Accédez à configuration services idmap.**
2. **Saisissez create.**

```
hostname:configuration services idmap> create
hostname:configuration services idmap (uncommitted)>
```

3. **Définissez les propriétés de manière appropriée.**

Vous pouvez utiliser la commande `list` pour afficher les propriétés disponibles.

```
hostname:configuration services idmap (uncommitted)> list
Properties:
    windomain = (unset)
    winname = (unset)
    direction = (unset)
    unixname = (unset)
    unixtype = (unset)
```

- a. **windomain : domaine Active Directory de l'identité Windows.**

- b. **winname : définir sur l'une des options. suivantes :**

- **Pour créer un mappage d'autorisation, attribuez à winname le nom de l'identité Windows.**

Saisissez `*` pour indiquer tous les utilisateurs au sein du domaine spécifié.

- Pour créer un mappage de refus qui empêche une identité UNIX de recevoir les informations d'identification d'une identité Windows, définissez la propriété avec le nom de l'identité Windows.
- Pour créer un mappage de refus qui empêche une identité Windows de recevoir les informations d'identification d'une identité UNIX, ne définissez pas `winname`.

c. **direction** : définir sur le sens du mappage :

- `win2unix` : mappage de Windows à UNIX
- `unix2win` : mappage d'UNIX à Windows
- `bi` : mappage bidirectionnel

d. **winname** : définir sur l'une des options suivantes :

- Pour créer un mappage d'autorisation, définissez la propriété avec le nom de l'identité UNIX, ou saisissez `*` pour indiquer tous les utilisateurs du type spécifié.
- Pour créer un mappage de refus qui empêche une identité Windows de recevoir les informations d'identification d'une identité UNIX, définissez la propriété avec le nom de l'identité UNIX.
- Pour créer un mappage de refus qui empêche une identité UNIX de recevoir les informations d'identification d'une identité Windows, ne définissez pas `unixname`.

e. **unixtype** : définir sur `user` ou `group` comme type d'identité UNIX.

```
hostname:configuration services idmap (uncommitted)> set windomain=demo.domain.com
hostname:configuration services idmap (uncommitted)> set winname=*
hostname:configuration services idmap (uncommitted)> set direction=win2unix
hostname:configuration services idmap (uncommitted)> set unixname=
hostname:configuration services idmap (uncommitted)> set unixtype=user
```

4. Saisissez `commit` pour valider les modifications et créer la règle de mappage.

```
hostname:configuration services idmap (uncommitted)> commit
hostname:configuration services idmap>
```

Vous pouvez utiliser la commande `list` pour afficher la nouvelle règle dans la liste Règles.

```
hostname:configuration services idmap> list
```

MAPPING	WINDOWS ENTITY	DIRECTION	UNIX ENTITY


```
idmap-000 Alice@demo.domain.com (U) == wdp (U)
idmap-001 *@demo.domain.com (U) => "" (U)
```

Exemple 13 Création d'un mappage bidirectionnel (CLI)

Cet exemple crée un mappage bidirectionnel basé sur un nom entre un utilisateur Windows et un utilisateur UNIX.

```
hostname:> configuration services idmap
hostname:configuration services idmap> create
hostname:configuration services idmap (uncommitted)> set
windomain=eng.fishworks.com
hostname:configuration services idmap (uncommitted)> set winname=Bill
hostname:configuration services idmap (uncommitted)> set direction=bi
hostname:configuration services idmap (uncommitted)> set unixname=wdp
hostname:configuration services idmap (uncommitted)> set unixtype=user
hostname:configuration services idmap (uncommitted)> commit
hostname:configuration services idmap> list
MAPPING      WINDOWS ENTITY      DIRECTION      UNIX ENTITY
idmap-000    Bill@eng.fishworks.com    (U) ==          wdp (U)
```

Exemple 14 Création d'un mappage de refus (CLI)

L'exemple suivant crée un mappage de refus pour empêcher tous les utilisateurs Windows d'un domaine d'obtenir des informations d'identification.

```
hostname:configuration services idmap> create
hostname:configuration services idmap (uncommitted)> list
Properties:
    windomain = (unset)
    winname = (unset)
    direction = (unset)
    unixname = (unset)
    unixtype = (unset)

hostname:configuration services idmap (uncommitted)> set
windomain=guest.fishworks.com
hostname:configuration services idmap (uncommitted)> set winname=*
hostname:configuration services idmap (uncommitted)> set direction=win2unix
hostname:configuration services idmap (uncommitted)> set unixname=
hostname:configuration services idmap (uncommitted)> set unixtype=user
hostname:configuration services idmap (uncommitted)> commit
hostname:configuration services idmap> list
MAPPING      WINDOWS ENTITY      DIRECTION      UNIX ENTITY
idmap-000    Bill@eng.fishworks.com    (U) ==          wdp (U)
idmap-001    *@guest.fishworks.com    (U) =>          "" (U)
```

▼ **Affichage d'un mappage (BUI)**

Utilisez la procédure suivante pour afficher un mappage existant.

1. **Accédez à Configuration > Services > Mappage des identités > Afficher les mappages.**
2. **Choisissez Windows ou UNIX comme plate-forme à partir de laquelle l'identité est mappée.**
3. **Saisissez les informations relatives à l'identité Windows ou UNIX.**
 - **Si vous avez sélectionné Windows, saisissez le domaine Windows et le nom de l'utilisateur.**
 - **Si vous avez sélectionné UNIX, choisissez User ou Group pour le type, et saisissez le nom de l'entité.**
4. **Cliquez sur AFFICHER LE MAPPAGE.**

Les propriétés de l'identité d'utilisateur ou de groupe sont affichées. La source et l'origine backend du mappage sont également affichées :

Source

- **Nouveau mappage** : le mappage a été créé récemment et n'a pas été récupéré du cache ni prédéfini.
- **Mappage mis en cache** : le mappage a été récupéré du cache, dans lequel les mappages sont stockés pendant 10 minutes après avoir été demandés.
- **Mappage codé en dur** : le mappage est prédéfini sur l'appareil et ne peut pas être modifié. Ces mappages ont été créés pour les identités UNIX et Windows par défaut.
- **Mappage algorithmique** : le mappage par nom d'un UID ou GID UNIX non éphémère étant impossible, le mappage a été réalisé vers un SID généré par algorithme.

Backend

- **Répertoire AD** : il s'agit d'un mappage basé sur un annuaire qui a été créé à l'aide d'annotations d'Active Directory.
- **Répertoire LDAP natif** : il s'agit d'un mappage basé sur un annuaire qui a été créé à l'aide d'annotations du répertoire LDAP.
- **IDMU** : le mappage a été créé à l'aide de la fonctionnalité Windows Identity Management for UNIX.
- **Règle de noms** : le mappage a été créé à l'aide d'une règle de noms.
- **Ephémère** : étant donné qu'il n'existait pas d'identité équivalente au moment où le mappage a été créé, le système en a créé une temporaire à l'aide d'un UID ou d'un GID éphémère.
- **SID local** : le mappage par nom d'un UID ou GID UNIX non éphémère étant impossible, le mappage a été réalisé vers un SID local généré par algorithmes.
- **Mappage bien connu** : le mappage utilise un "SID bien connu". Ces SID Windows identifient des utilisateurs ou des groupes génériques. Leurs valeurs restent constantes sur tous les systèmes d'exploitation.

▼ Vidage des mappages à partir du cache (BUI)

Utilisez la procédure suivante pour vider, ou faire expirer, tous les mappages du cache.

Une fois qu'un mappage demandé a été fourni, il est stocké dans le cache pendant 10 minutes puis expire. Vous pouvez faire expirer immédiatement un mappage, à l'aide de la fonction de vidage, qui fait expirer tous les mappages mis en cache .

1. **Accédez à Configuration > Services > Mappage des identités > Afficher les mappages.**
2. **Cliquez sur VIDER LE CACHE DE CARTE.**
Tous les mappages mis en cache expirent.

▼ Vidage des mappages à partir du cache (CLI)

Utilisez la procédure suivante pour vider, ou faire expirer, tous les mappages du cache.

Une fois qu'un mappage demandé a été fourni, il est stocké dans le cache pendant 10 minutes puis expire. Vous pouvez faire expirer immédiatement un mappage, à l'aide de la fonction de vidage, qui fait expirer tous les mappages mis en cache .

1. **Accédez à configuration services idmap.**
2. **Saisissez flush.**

```
hostname:configuration services idmap> flush  
hostname:configuration services idmap>
```

Tous les mappages mis en cache expirent.

Pratiques recommandées pour le mappage des identités

- Configurez des règles de mappage des identités spécifiques à l'utilisateur lorsque vous souhaitez autoriser un utilisateur à accéder à un ensemble de fichiers commun par le biais des clients NFS et SMB. Si les clients NFS et SMB accèdent à des systèmes de fichiers disjoints, il n'est pas nécessaire de configurer des règles de mappage des identités.
- La reconfiguration du service de mappage des identités n'a pas d'incidence sur les sessions SMB actives. Les utilisateurs qui sont connectés le restent et leur mappage de noms précédent est disponible afin d'autoriser l'accès à des partages supplémentaires pendant dix minutes. Pour empêcher l'accès non autorisé, configurez les mappages avant d'exporter des partages.

- La sécurité offerte par vos mappages d'identités repose sur leur synchronisation avec vos services d'annuaire. Par exemple, si vous créez un mappage basé sur un nom refusant l'accès à un utilisateur donné, et si le nom de l'utilisateur est modifié, le mappage ne bloque plus l'accès à cet utilisateur.
- Un seul mappage bidirectionnel est autorisé sur chaque domaine Windows afin d'établir une correspondance entre tous les utilisateurs du domaine Windows et toutes les identités UNIX. Si vous souhaitez créer plusieurs règles au niveau du domaine, assurez-vous de spécifier que ces règles s'appliquent *uniquement* dans le sens Windows vers UNIX.
- Dans la mesure du possible, privilégiez le mode de mappage IDMU au mappage basé sur un annuaire.

Concepts de mappage des identités

Le service SMB utilise le mappage des identités pour associer des identités Windows et UNIX. Lorsque le service SMB authentifie un utilisateur, il utilise le service de mappage des identités pour mapper l'identité Windows de l'utilisateur avec l'identité UNIX appropriée. Si aucune identité UNIX n'existe pour un utilisateur Windows, le service génère une identité temporaire à l'aide d'un UID et d'un GID éphémère. Grâce à ces mappages, un partage peut être exporté et accessible simultanément par des clients SMB et NFS. En associant les identités Windows et UNIX, les clients NFS et SMB peuvent partager la même identité, ce qui permet notamment d'accéder au même ensemble de fichiers.

Dans le système d'exploitation Windows, un jeton d'accès contient les informations de sécurité d'une session de connexion et identifie l'utilisateur, ses groupes et ses privilèges. Les administrateurs définissent des utilisateurs et des groupes Windows dans un groupe de travail ou une base de données SAM gérés sur un contrôleur de domaine Active Directory. Chaque utilisateur et groupe possède un SID qui l'identifie de manière unique au sein d'un hôte et d'un domaine local, ainsi que dans tous les domaines Windows possibles.

UNIX d'identification utilisateur basées sur l'authentification utilisateur et les autorisations d'accès aux fichiers. Les administrateurs définissent des utilisateurs et des groupes UNIX dans des fichiers de mot de passe et de groupe locaux ou dans un service de noms ou d'annuaire, tel que NIS ou LDAP. Chaque utilisateur et chaque groupe UNIX possède un UID et un GID. En règle générale, l'UID ou le GID identifie de façon unique un utilisateur ou un groupe au sein d'un seul domaine UNIX. Toutefois, ces valeurs ne sont pas uniques dans tous les domaines.

Lorsque vous sélectionnez un mode de mappage, les options suivantes sont disponibles :

- **Mappage basé sur une règle** : permet de créer différentes règles qui mappent les identités par nom, ce qui permet d'établir des équivalences entre les identités Windows et UNIX. Les règles de mappage sont utiles lorsque vous voulez permettre à un utilisateur d'accéder au même ensemble de fichiers par le biais des clients SMB et NFS.
- **Mappage basé sur un annuaire** : permet d'annoter un objet LDAP ou Active Directory à l'aide d'informations relatives à la manière dont l'identité est mise en correspondance avec une identité équivalente sur la plate-forme opposée.

- **Mappage basé sur IDMU** : IDMU (Identity Management for UNIX) est une fonctionnalité offerte par Microsoft pour Windows Server 2003, et intégrée à Windows Server 2003 R2 et aux versions ultérieures. IDMU prend en charge Windows en tant que serveur NIS/NFS en ajoutant un volet réservé aux "Attributs UNIX" à l'interface utilisateur Utilisateurs et ordinateurs d'Active Directory. Ceci permet aux administrateurs de spécifier plusieurs paramètres liés à UNIX, y compris UID, GID, shell de connexion et annuaire personnel. Ces paramètres sont accessibles dans Active Directory via un schéma similaire (mais pas identique) à celui du document RFC 2307 et via le service NIS. Lorsque le mode IDMU est sélectionné, le service de mappage des identités utilise ces attributs UNIX pour établir des correspondances entre les identités Windows et UNIX. Cette approche est très similaire au mappage basé sur un annuaire. La seule différence tient au fait que le service de mappage des identités interroge le schéma de propriété établi par le logiciel IDMU au lieu d'autoriser un schéma personnalisé. Lorsque cette approche est utilisée, aucun autre mappage basé sur un annuaire ne peut avoir lieu.

Mappages mis en cache et éphémères

Lorsque le service de mappage des identités établit une correspondance de noms, il stocke le mappage dans le cache pendant 10 minutes, délai au-delà duquel le mappage expire. Durant ses 10 minutes de validité, un mappage persiste malgré les redémarrages du service de mappage des identités. Les modifications apportées aux mappages ou aux annuaires du service de noms n'ont aucune incidence sur les connexions existantes au cours des 10 minutes de validité d'un mappage. Le service évalue les mappages uniquement lorsque le client tente de se connecter à un partage et qu'aucun mappage non expiré n'existe. Par exemple, si le serveur SMB demande une correspondance pour l'utilisateur après l'expiration du mappage, le service réévalue le mappage.

Si aucune règle de mappage basé sur un nom ne s'applique à un utilisateur spécifique, celui-ci reçoit des informations d'identification temporaires via un mappage éphémère (à moins qu'un mappage de refus ne l'interdise). Lorsqu'un utilisateur Windows portant un nom UNIX éphémère crée un fichier sur le système, les clients Windows qui accèdent au fichier par le biais de SMB voient que le fichier appartient à cette identité Windows. En revanche, pour les clients NFS, le fichier ne présente aucun propriétaire.

Sensibilité à la casse du mappage des identités

Les noms Windows ne sont pas sensibles à la casse, contrairement aux noms UNIX. Les noms d'utilisateur JSMITH, JSmith et jsmith sont équivalents dans Windows, mais différents dans UNIX. La sensibilité à la casse affecte les correspondances de noms différemment en fonction du sens du mappage.

- Pour qu'un mappage Windows vers UNIX produise une correspondance, la casse du nom d'utilisateur Windows doit être identique à celle du nom d'utilisateur UNIX. Par exemple, seul le nom d'utilisateur "jsmith" de Windows correspond au nom d'utilisateur "jsmith" d'UNIX. Le nom d'utilisateur Windows "Jsmith" ne correspond pas.

- Une exception existe dans les exigences du mappage Windows vers UNIX lorsque le caractère générique "*" est utilisé pour établir une correspondance entre plusieurs noms d'utilisateur.
Si le service de mappage des identités rencontre la correspondance d'utilisateur Windows *@some.domain vers l'utilisateur UNIX "*", il commence par rechercher un nom UNIX correspondant exactement au nom Windows. Si aucune correspondance n'est trouvée, le service convertit le nom Windows entier en minuscule et relance la recherche d'un nom UNIX correspondant. Par exemple, le nom d'utilisateur Windows "JSmith@some.domain" correspond au nom d'utilisateur UNIX "jsmith". Si le service ne trouve aucune correspondance après avoir utilisé des lettres minuscules pour le nom d'utilisateur Windows, l'utilisateur n'obtient pas de mappage.
Vous pouvez créer une règle pour mettre en correspondance les chaînes dont seule la casse diffère. Vous pouvez, par exemple, créer un mappage spécifique à l'utilisateur pour établir une correspondance entre l'utilisateur Windows "JSmith@domaine" et l'utilisateur UNIX "jSmith". Autrement, le service affecte un ID éphémère à l'utilisateur Windows.
- Pour qu'un mappage UNIX vers Windows produise une correspondance, il n'est pas nécessaire que la casse soit respectée. Par exemple, le nom d'utilisateur UNIX "jsmith" correspond à n'importe quel nom d'utilisateur Windows comprenant les lettres "JSMITH", indépendamment de la casse.

Symboles de direction d'une règle de mappage

Après avoir créé un mappage basé sur un nom, les symboles suivants indiquent la sémantique de chaque règle.

-  - mappe l'identité Windows vers l'identité UNIX et l'identité Unix vers l'identité Windows
-  : mappe l'identité Windows vers l'identité UNIX
-  : mappe l'identité UNIX vers l'identité Windows
-  : refuse des informations d'identification à l'identité Windows
-  - refuse des informations d'identification à l'identité UNIX

Si une icône est grise et pas noire, la règle correspond à une identité UNIX qui ne peut pas être résolue.

Configuration du DNS

Le client DNS (Domain Name Service), qui permet de résoudre les adresses IP en noms d'hôte (et vice versa), peut être activé ou désactivé. Une résolution facultative de noms d'hôte secondaire via NIS et/ou LDAP, si elle est configurée et activée, peut être requise pour les noms d'hôte et les adresses qui ne peuvent pas être résolus par le biais du service DNS. La résolution

de noms d'hôte est utilisée dans toutes les interfaces de l'appareil, y compris dans les journaux pour indiquer l'emplacement à partir duquel un utilisateur a effectué une action vérifiable et dans l'écran de la fonction Analyse pour fournir des statistiques sur une base par client.

Pour configurer DNS, reportez-vous aux sections suivantes :

- ["Configuration du DNS \(CLI\)" à la page 311](#)
- ["Propriétés et journaux DNS" à la page 311](#)
- ["Active Directory et DNS" à la page 312](#)
- ["Résolution non-DNS" à la page 312](#)
- ["Fonctionnement sans DNS" à la page 313](#)

Configuration du DNS (CLI)

La CLI intègre les commandes `nslookup` et `getent hosts`, grâce auxquelles vous pouvez tester le bon fonctionnement de la résolution de noms d'hôte :

```
hostname:> nslookup deimos
192.168.1.109    deimos.sf.fishworks.com
hostname:> getent hosts deimos
192.168.1.109    deimos.sf.fishworks.com
```

Propriétés et journaux DNS

Les propriétés configurables du client DNS incluent un nom de domaine de base et une liste de serveurs spécifiés par adresse IP. Vous devez fournir un nom de domaine et au moins une adresse de serveur. Le serveur doit en principe renvoyer un enregistrement NS (NameServer) pour le domaine spécifié, même s'il ne doit pas nécessairement faire autorité dans ce domaine.

TABLEAU 80 Propriétés DNS

Propriété	Description
Domaine DNS	Nom du domaine dans lequel commencer la recherche en cas de recherches de nom d'hôte partiels.
Serveur(s) DNS	Un ou plusieurs serveurs DNS. Il faut indiquer des adresses IP.
Domaine(s) de recherche DNS	Vous pouvez répertorier jusqu'à quatre domaines dans lesquels effectuer la recherche après le domaine Active Directory, le domaine de recherche Active Directory obsolète et le domaine DNS spécifié.
Autoriser la résolution IPv4 non-DNS	Les adresse IPv4 doivent être résolues en noms d'hôte, et les noms d'hôte en adresses IPv4, à l'aide de NIS et/ou LDAP si ces protocoles sont configurés et activés.
Autoriser la résolution IPv6 non-DNS	Les adresses IPv4 et IPv6 peuvent être résolues en noms d'hôte, et les noms d'hôte en adresses IPv4 et

Propriété	Description
	IPv6 à l'aide de NIS et/ou LDAP, si ces protocoles sont configurés et activés.

La procédure de modification des propriétés des services est documentée dans les sections ["Définition des propriétés du service \(BUI\)" à la page 230](#) et ["Définition des propriétés du service \(CLI\)" à la page 231](#). Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

TABLEAU 81 Journaux DNS

Journal	Description
network-dns-client:default	Consigne les événements du service DNS

Rubriques connexes

- ["Active Directory et DNS" à la page 312](#)

Active Directory et DNS

Si vous envisagez d'utiliser Active Directory, les serveurs doivent pouvoir résoudre les enregistrements de nom d'hôte et de serveur dans la partie Active Directory de l'espace de noms du domaine. Par exemple, si votre appareil réside dans le domaine example.com et que la portion Active Directory de l'espace de noms est redmond.example.com, vos serveurs de noms doivent pouvoir atteindre un serveur faisant autorité pour example.com et fournir une délégation pour le domaine redmond.example.com à un ou plusieurs serveurs Active Directory de ce domaine. Ces exigences sont imposées par Active Directory, et non par l'appareil lui-même. Si elles ne sont pas satisfaites, il vous sera impossible de rejoindre un domaine Active Directory.

Rubriques connexes

- ["Configuration du DNS" à la page 310](#)
- ["Configuration d'Active Directory" à la page 293](#)

Résolution non-DNS

DNS est un mécanisme de mappage de noms d'hôte et d'adresses IP standard, au niveau de l'entreprise, hautement évolutif et fiable. L'utilisation des serveurs DNS en fonction est vivement conseillée et permet généralement d'optimiser vos résultats. Dans certains environnements, un sous-ensemble d'hôtes peut être résolu uniquement par le biais de mappages NIS ou LDAP. Si c'est le cas dans votre environnement, activez une résolution d'hôtes non-DNS et configurez les services d'annuaire appropriés. Si LDAP est utilisé pour la résolution

d'hôtes, le mappage d'hôtes doit se situer au niveau du DN standard de votre base de données : ou=Hosts,(Base DN). Il doit utiliser le schéma standard. Lorsque des groupes réseau utilisent ce mode avec le partage NFS, il peut être nécessaire pour les systèmes client d'adopter le même mécanisme de résolution de noms d'hôte configuré sur l'appareil, sans quoi les exceptions de partage NFS risquent de ne pas fonctionner correctement.

Lorsque la résolution d'hôtes non-DNS est activée, le service DNS continue d'être utilisé. Les protocoles NIS (s'il est activé) puis LDAP (s'il est activé) sont utilisés pour résoudre un nom d'hôte ou une adresse uniquement s'ils ne peuvent pas être résolus par le biais de DNS. Cela peut entraîner des résultats confus et apparemment incohérents. Vous pouvez valider les résultats de la résolution d'hôtes à l'aide de la commande `getent` de la CLI décrite ci-dessus.

L'utilisation de ces options est vivement recommandée.

Fonctionnement sans DNS

Si l'appareil ne parvient à accéder à aucun des serveurs DNS à partir de son emplacement d'installation sur le réseau, vous pouvez choisir de travailler sans DNS en fournissant l'adresse de serveur 127.0.0.1. Pour travailler sans DNS :

- **BUI** : Accédez à Configuration > Services > DNS. Dans le champ Serveur(s) DNS, saisissez **127.0.0.1**.
- **CLI** : Accédez à `configuration services dns` et saisissez `show`. Saisissez `set servers=127.0.0.1`, puis `commit`.

L'utilisation de ce mode est fortement déconseillée, car plusieurs fonctionnalités ne fonctionneront pas correctement, notamment :

- La fonction d'analyse ne peut pas résoudre les adresses client en noms d'hôte.
- La fonctionnalité Active Directory ne fonctionne pas (vous ne pouvez pas rejoindre un domaine).
- Le service LDAP protégé par SSL ne fonctionne pas correctement avec les certificats contenant des noms d'hôte.
- Les actions d'alerte et de seuil incluant l'envoi d'e-mails peuvent uniquement être envoyées aux serveurs de courrier situés sur un sous-réseau connecté. Toutes les adresses doivent être spécifiées à l'aide de l'adresse IP du serveur de courrier.
- Certaines opérations peuvent prendre plus longtemps que prévu en raison des délais d'attente de résolution de noms d'hôte.

Ces limitations peuvent être partiellement restreintes en utilisant un autre service de résolution d'hôte. Reportez-vous à la section ["Résolution non-DNS" à la page 312](#).

Rubriques connexes

- Activation d'un service [BUI](#), [CLI](#)

- Désactivation d'un service [BUI](#), [CLI](#)

Configuration IPMP

IPMP (Internet Protocol Network Multipathing) permet de regrouper plusieurs interfaces réseau en une seule, pour optimiser la bande passante du réseau et assurer une plus grande fiabilité (redondance de l'interface). Certaines propriétés peuvent être configurées dans cette section. Pour configurer des interfaces réseau dans des groupes IPMP, reportez-vous à la section "[Configuration réseau](#)" à la page 51.

TABLEAU 82 Propriétés IPMP

Propriété	Description
Latence de détection de défaillance	Temps d'attente avant que le service IPMP déclare la défaillance d'une interface réseau et bascule ses adresses IP.
Activer le rétablissement	Permet au service de rétablir les connexions sur une interface réparée.

La procédure de modification des propriétés des services est documentée dans les sections "[Définition des propriétés du service \(BUI\)](#)" à la page 230 et "[Définition des propriétés du service \(CLI\)](#)" à la page 231. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

TABLEAU 83 Journaux IPMP

Journal	Description
network-initial:default	Consigne le processus de configuration réseau

Configuration NTP

Le service NTP (Network Time Protocol) peut permettre de maintenir l'exactitude de l'horloge de l'appareil. Cette pratique est très utile pour l'enregistrement précis des horodatages dans le système de fichiers et pour l'authentification du protocole. L'appareil enregistre les heures d'après le fuseau horaire UTC. Les heures affichées dans la BUI suivent le fuseau horaire de votre navigateur.

Les heures de l'appareil (Server Time) et de votre navigateur (Client Time) sont affichées dans la partie droite de l'écran de la BUI. Si le service NTP n'est pas en ligne, vous pouvez cliquer sur le bouton SYNC pour faire correspondre l'heure de l'appareil avec celle du navigateur client.

Si vous partagez des systèmes de fichiers à l'aide de SMB, les horloges du client doivent être synchronisées à cinq minutes près avec l'horloge de l'appareil afin d'éviter les erreurs.

d'authentification d'utilisateur. Pour garantir la synchronisation de l'horloge, vous pouvez notamment configurer l'appareil et les clients SMB pour qu'ils utilisent le même serveur NTP.

TABLEAU 84 Synchronisation d'horloge NTP

Journal	Description
network-ntp:default	Journal du service NTP

Pour configurer NTP, reportez-vous aux sections suivantes :

- ["Configuration de la synchronisation d'horloge \(BUI\)" à la page 315](#)
- ["Configuration du service NTP \(CLI\)" à la page 315](#)
- ["Propriétés NTP" à la page 317](#)

▼ Configuration de la synchronisation d'horloge (BUI)

Cette opération définit l'heure de l'appareil pour qu'elle corresponde à celle de votre navigateur.

1. **Accédez à Configuration > Services > NTP.**
2. **Désactivez le service NTP.**
3. **Cliquez sur SYNC.**

▼ Configuration du service NTP (CLI)

1. **Sous configuration services ntp, modifiez les autorisations à l'aide de la commande authkey :**

```
hostname:configuration services ntp> authkey
hostname:configuration services ntp authkey>
```

2. **Dans ce contexte, il est possible d'ajouter de nouvelles clés à l'aide de la commande create :**

```
hostname:configuration services ntp authkey> create
hostname:configuration services ntp authkey-000 (uncommitted)> get
keyno = (unset)
type = (unset)
key = (unset)
hostname:configuration services ntp authkey-000 (uncommitted)> set keyno=1
keyno = 1 (uncommitted)
hostname:configuration services ntp authkey-000 (uncommitted)> set type=A
type = A (uncommitted)
hostname:configuration services ntp authkey-000 (uncommitted)> set key=coconuts
```

```
key = ***** (uncommitted)
hostname:configuration services ntp authkey-000 (uncommitted)> commit
hostname:configuration services ntp authkey>
```

3. **Pour associer des clés d'authentification à des serveurs dans la CLI, la propriété `serverkeys` doit être définie sur une liste dont chaque valeur est une clé à associer au serveur correspondant dans la propriété `servers`.**

Si un serveur n'a pas recours à l'authentification, la clé de serveur correspondante doit être définie sur 0. Par exemple, pour utiliser la clé créée ci-dessous afin d'authentifier les serveurs "gefilte" et "carp" :

```
hostname:configuration services ntp> set servers=gefilte,carp
servers = gefilte,carp (uncommitted)
hostname:configuration services ntp> set serverkeys=1,1
serverkeys = 1,1 (uncommitted)
hostname:configuration services ntp> commit
hostname:configuration services ntp>
```

4. **Pour associer des clés d'authentification à des serveurs, définissez la propriété `serverkeys` comme une liste dont chaque valeur est une clé à associer au serveur correspondant dans la propriété `servers`.**

Si un serveur n'a pas recours à l'authentification, la clé de serveur correspondante doit être définie sur 0. Par exemple, pour utiliser la clé créée ci-dessous afin d'authentifier les serveurs "gefilte" et "carp" :

```
hostname:configuration services ntp> set servers=gefilte,carp
servers = gefilte,carp (uncommitted)
hostname:configuration services ntp> set serverkeys=1,1
serverkeys = 1,1 (uncommitted)
hostname:configuration services ntp> commit
hostname:configuration services ntp>
```

5. **Pour authentifier le serveur "gefilte" avec la clé 1, "carp" avec la clé 2 et "dory" avec la clé 3 :**

```
hostname:configuration services ntp> set servers=gefilte,carp,dory
servers = gefilte,carp,dory (uncommitted)
hostname:configuration services ntp> set serverkeys=1,2,3
serverkeys = 1,2,3 (uncommitted)
hostname:configuration services ntp> commit
hostname:configuration services ntp>
```

6. **Pour authentifier les serveurs "gefilte" et "carp" à l'aide de la clé 1 et ne pas authentifier le serveur NTP "dory" :**

```
hostname:configuration services ntp> set servers=gefilte,carp,dory
servers = gefilte,carp,dory (uncommitted)
hostname:configuration services ntp> set serverkeys=1,1,0
serverkeys = 1,1,0 (uncommitted)
hostname:configuration services ntp> commit
```

```
hostname:configuration services ntp>
```

Propriétés NTP

Les propriétés NTP suivantes sont disponibles dans Configuration > Services > NTP :

TABLEAU 85 Propriétés NTP

Propriété	Description	Exemples
Détecter le serveur NTP à l'aide d'une adresse de multidiffusion	Saisissez une adresse de multidiffusion pour localiser automatiquement un serveur NTP.	224.0.1.1
Spécifier le(s) serveur(s) NTP manuellement	Saisissez un ou plusieurs serveurs NTP (et leurs clés d'authentification correspondantes, le cas échéant) pour contacter directement l'appareil.	0.pool.ntp.org
Clés d'authentification NTP	Saisissez une ou plusieurs clés d'authentification NTP pour l'appareil à utiliser lors de l'authentification de la validité des serveurs NTP. Voir la section Tableau 86, "Clés privées et entiers NTP" .	Clé aut : 10, Type : ASCII, Clé privée : SUN7000

Validation - Si une configuration non valide est saisie, un message d'avertissement s'affiche et la configuration n'est pas validée. Cela se produit dans les cas suivants :

- Une adresse de multidiffusion est utilisée mais aucune réponse NTP n'est trouvée.
- Une adresse serveur NTP est utilisée mais ce serveur ne répond pas correctement à NTP.

Authentification - Pour vous prémunir contre les usurpations d'adresse NTP par des serveurs non autorisés, NTP possède un schéma de chiffrement par clé privée via lequel les serveurs NTP sont associés à une clé privée que le client utilise pour vérifier leur identité. Ces clés ne permettent pas de chiffrer le trafic ni d'authentifier le client, mais sont uniquement utilisées par le client NTP (à savoir, l'appareil) pour authentifier le serveur NTP. Pour associer une clé privée à un serveur NTP, il faut commencer par spécifier cette clé. Chaque clé privée est associée à un entier unique ainsi qu'à un type et une clé. Il doit s'agir de l'un des types suivants :

TABLEAU 86 Clés privées et entiers NTP

Type	Description	Exemple
DES	Nombre hexadécimal 64 bits au format DES	0101010101010101
NTP	Nombre hexadécimal 64 bits au format NTP	8080808080808080
ASCII	Chaîne ASCII comprenant 1 à 8 caractères	topsecret

Type	Description	Exemple
MD5	Chaîne ASCII comprenant 1 à 8 caractères utilisant le schéma d'authentification MD5.	md5secret

Une fois les clés spécifiées, un serveur NTP peut être associé à une clé privée particulière. Pour une clé donnée, toutes les valeurs de numéro, type, et clé privée doivent correspondre entre le client et le serveur afin de pouvoir authentifier un serveur NTP.

Configuration de Phone Home

L'écran du service Phone Home permet de gérer l'enregistrement de l'appareil de la même manière que le service de support à distance de Phone Home.

L'enregistrement connecte votre appareil à la fonction [Oracle Auto Service Request \(http://www.oracle.com/us/support/auto-service-request/index.html\)](http://www.oracle.com/us/support/auto-service-request/index.html). Oracle ASR ouvre automatiquement les demandes d'assistance pour des problèmes spécifiques rapportés par votre appareil. L'enregistrement connecte également votre appareil à My Oracle Support (MOS) pour détecter les notifications de mise à jour.

Le service Phone Home communique avec le support Oracle pour fournir les éléments suivants :

- **Compte-rendu des pannes** : le système signale les problèmes actifs à Oracle afin d'assurer une intervention automatisée. En fonction de la nature de la panne, un cas de prise en charge peut être ouvert. Vous trouverez des détails sur ces événements dans l'Affichage des problèmes actifs. Pour plus d'informations, reportez-vous à la section "[Résolution des problèmes](#)" dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.
- **Signal d'activité** : des pulsations quotidiennes sont envoyées à Oracle pour indiquer que le système est actif et en cours d'exécution. Le support Oracle peut informer le contact technique chargé d'un compte lorsque l'un des systèmes activés ne parvient pas à envoyer un signal d'activité pendant une période prolongée.
- **Configuration système** : des messages sont régulièrement envoyés à Oracle pour décrire les versions et la configuration logicielle et matérielle actuelles, ainsi que la configuration du stockage. Aucune donnée ou métadonnée utilisateur n'est transmise dans ce message.
- **Lots d'informations pour le support** : le service Phone Home doit être désactivé avant de pouvoir télécharger les lots d'informations pour le support sur les services de support Oracle. Pour plus d'informations, reportez-vous à la section "[Utilisation des lots de support](#)" dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.
- **Notifications de mise à jour** : crée une alerte quand de nouvelles mises à jour logicielles sont disponibles dans My Oracle Support (MOS). Pour plus d'informations, reportez-vous à la section "[Utilisation de notifications et de mises à jour logicielles](#)" dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.

Vous devez vous connecter pour utiliser le service Phone Home.

Vous devez posséder un nom d'utilisateur et un mot de passe de compte de connexion unique Oracle pour bénéficier des fonctionnalités de compte-rendu des pannes et de signal d'activité du service Phone Home. Accédez à [My Oracle Support \(http://support.oracle.com\)](http://support.oracle.com) et cliquez sur Inscrire pour créer un compte.

Pour configurer le service Phone Home, reportez-vous aux sections suivantes :

- Enregistrement de l'appareil [BUI](#), [CLI](#)
- "[Modification des informations relatives au compte \(BUI\)](#)" à la page 320
- "[Propriétés de Phone Home](#)" à la page 320

▼ Enregistrement de l'appareil (BUI)

1. **Accédez à Configuration > Services > Phone Home.**
2. **Saisissez le mot de passe et le nom d'utilisateur de votre compte de connexion unique Oracle.**
Cliquez sur Clause de confidentialité pour obtenir des informations sur la politique de confidentialité. Vous pouvez la consulter à tout moment dans la BUI et la CLI.
3. **Cliquez sur APPLIQUER pour valider vos modifications.**
4. **Utilisez [My Oracle Support \(http://support.oracle.com/\)](http://support.oracle.com/) pour compléter l'activation d'Auto Service Request (ASR) (<http://www.oracle.com/us/support/auto-service-request/index.html>).**
Reportez-vous à la section "Comment gérer et approuver les actifs ASR en attente dans My Oracle Support" (ID de doc 1329200.1).

▼ Enregistrement de l'appareil (CLI)

1. **Accédez à configuration services scrk.**
2. **Définissez soa_id et soa_password respectivement sur le nom d'utilisateur et le mot de passe de votre compte de connexion unique Oracle.**
3. **Validez vos modifications.**
4. **Utilisez [My Oracle Support \(http://support.oracle.com/\)](http://support.oracle.com/) pour compléter l'activation d'Auto Service Request (ASR) (<http://www.oracle.com/us/support/auto-service-request/index.html>).**
Reportez-vous à la section "Comment gérer et approuver les actifs ASR en attente dans My Oracle Support" (ID de doc 1329200.1).

Exemple 15 Enregistrement de la CLI

```
hostname:> configuration services scrk
hostname:configuration services scrk>set soa_id=myuser
soa_id = myuser(uncommitted)
hostname:configuration services scrk> set soa_password=mypass
soa_password = ***** (uncommitted)
hostname:configuration services scrk> commit
```

▼ Modification des informations relatives au compte (BUI)

1. **Accédez à Configuration > Services > Phone Home.**
2. **Cliquez sur "Changer de compte..." pour modifier le compte de connexion unique Oracle utilisé par l'appareil.**
3. **Validez vos modifications.**
4. **Utilisez My Oracle Support pour compléter l'activation de la fonction ASR.**
Reportez-vous à la section "Comment gérer et approuver les actifs ASR en attente dans My Oracle Support" (ID de doc 1329200.1).

Propriétés de Phone Home

Si l'appareil n'est pas directement connecté à Internet, il peut être nécessaire de configurer un proxy HTTP permettant au service Phone Home de communiquer avec Oracle. Ces paramètres de proxy sont uniquement utilisés pour charger les offres groupées de support. Pour plus d'informations sur les lots de support, reportez-vous à la section "[Utilisation des lots de support](#)" dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.

TABLEAU 87 Paramètres de proxy Web de Phone Home

Propriété	Description
Utiliser un proxy Web	Connexion via un proxy Web
Hôte : port	Nom d'hôte ou adresse IP du proxy Web et port
Nom d'utilisateur	Nom d'utilisateur du proxy Web
Mot de passe	Mot de passe du proxy Web

TABLEAU 88 Statut Phone Home

Propriété	Description
Dernier signal d'activité envoyé à	Heure d'envoi du dernier signal d'activité au support Oracle

Si le service Phone Home est activé avant qu'un compte de connexion unique Oracle ne soit saisi, il apparaît en état de maintenance. Vous devez saisir un compte de connexion unique Oracle pour utiliser le service Phone Home.

Vous trouverez un journal des événements Phone Home sous Maintenance > Journaux > Phone Home.

Configuration du routage dynamique

RIP (Routing Information) est un protocole de routage dynamique à vecteur de distances utilisé par l'appareil pour configurer automatiquement les routes optimales en fonction des messages reçus d'autres hôtes de liaison compatibles avec RIP (généralement des routeurs). L'appareil prend en charge autant RIPv1 et RIPv2 pour IPv4 que RIPng pour IPv6.

Les routes configurées via ces protocoles sont marquées du type "dynamique" dans la table de routage. Les ports d'écoute RIP et RIPng sont respectivement les ports UDP 520 et 521.

TABLEAU 89 Routage dynamique

Journal	Description
network-routing-route:default	Consigne les événements du service RIP
network-routing-ripng:quagga	Consigne les événements du service RIPng

Configuration des indicateurs de maintenance

Les indicateurs de maintenance sont utilisés pour faciliter la prise en charge et l'inventaire des produits, en permettant d'interroger l'appareil sur des données telles que :

- Numéro de série du système
- Type de système
- Numéros de version logicielle

Vous pouvez enregistrer ces indicateurs de maintenance auprès du support Oracle, ce qui vous permet de garder facilement la trace de votre équipement Oracle et de raccourcir la durée des appels liés à la maintenance. Les indicateurs de maintenance sont activés par défaut.

TABLEAU 90 Propriétés des ports UDP/TCP

Propriété	Description
Port de détection	Port UDP utilisé pour la détection d'indicateurs de maintenance. La valeur par défaut est 6481
Port d'écoute	Port TCP utilisé pour demander des données d'indicateurs de maintenance. La valeur par défaut est 6481

Configuration SMTP

Le service SMTP envoie tout le courrier généré par l'appareil, généralement en réponse à des alertes configurées dans l'écran Alerts . Le service SMTP n'accepte pas le courrier externe. Il envoie uniquement les messages générés automatiquement par l'appareil.

Par défaut, le service SMTP utilise DNS (enregistrements MX) pour déterminer la destination du courrier. Si DNS n'est pas configuré pour le domaine de l'appareil ou si les enregistrements MX DNS ne sont pas définis correctement pour le domaine de destination du courrier sortant, l'appareil peut être configuré de façon à faire suivre tous les messages via un serveur de courrier sortant, couramment appelé hôte intelligent.

TABLEAU 91 Propriétés SMTP

Propriété	Description
Envoyer le courrier via l'hôte intelligent	Si cette propriété est activée, l'ensemble du courrier est envoyé via le serveur de courrier sortant spécifié. Autrement, DNS est utilisé pour déterminer où envoyer le courrier pour un domaine spécifique.
Nom d'hôte du serveur intelligent	Nom d'hôte du serveur de courrier sortant.
Autoriser une adresse d'expéditeur personnalisée	Si cette propriété est activée, l'adresse de l'expéditeur du courrier est définie sur Personnalisée dans la propriété adresse. Il peut être utile de personnaliser cette propriété si, par exemple, l'adresse de l'expéditeur par défaut est identifiée en tant que courrier indésirable.
Adresse d'expéditeur personnalisée	Adresse de l'expéditeur à utiliser pour le courrier sortant.

Lorsque vous modifiez les propriétés, vous pouvez utiliser des alertes pour envoyer un e-mail de test afin de vérifier que les propriétés sont correctes. C'est souvent à cause d'une mauvaise configuration de DNS que des messages ne sont pas envoyés. En effet, ce problème empêche l'appareil de déterminer à quel serveur de courrier il doit envoyer le courrier. Comme indiqué précédemment, vous pouvez utiliser un hôte intelligent si vous ne parvenez pas à configurer DNS.

TABLEAU 92 Journaux SMTP

Journal	Description
network-smtp:sendmail	Consigne les événements de service SMTP
mail	Journal des activités SMTP (y compris les messages envoyés)

Configuration SNMP

Le service SNMP (Simple Network Management Protocol) offre deux fonctions différentes sur l'appareil :

- Les informations de statut de l'appareil peuvent être gérées par SNMP.
- Des alertes peuvent être configurées pour envoyer des dérouterments SNMP. Reportez-vous à la section ["Configuration des alertes" à la page 184](#).

Les versions v1, v2c et v3 de SNMP sont disponibles lorsque le service est activé. L'appareil prend en charge un maximum de 128 interfaces réseau physiques et logiques. Plus de 128 interfaces réseau peuvent entraîner des délais d'expiration pour les commandes snmpwalk et snmpget. Si vous avez besoin de plus de 128 interfaces réseau, contactez le support Oracle.

Pour configurer SNMP, reportez-vous aux sections suivantes :

- ["Configuration du service SNMP afin qu'il indique l'état de l'appareil \(BUI\)" à la page 323](#)
- ["Configuration du service SNMP afin d'envoyer des dérouterments \(BUI\)" à la page 323](#)
- ["Propriétés SNMP" à la page 324](#)
- ["Bases de données MIB du service SNMP" à la page 324](#)
- ["MIB Sun FM" à la page 325](#)
- ["MIB Sun AK" à la page 325](#)

▼ Configuration du service SNMP afin qu'il indique l'état de l'appareil (BUI)

1. Accédez à Configuration > Services > SNMP.
2. Définissez le nom de communauté, le réseau autorisé et la chaîne de contact.
3. (Facultatif) Définissez la destination du dérouterment : soit un hôte SNMP distant, soit 127.0.0.1.
4. Cliquez sur APPLIQUER pour valider la configuration.
5. Redémarrez le service.

▼ Configuration du service SNMP afin d'envoyer des dérouterments (BUI)

1. Accédez à Configuration > Services > SNMP.
2. Définissez le nom de communauté, la chaîne de contact et les destinations de dérouterment.
3. (Facultatif) Définissez le réseau autorisé de façon à autoriser les clients SNMP. Sinon, indiquez la valeur 127.0.0.1/8.

4. Cliquez sur **APPLIQUER** pour valider la configuration.
5. Redémarrez le service.
6. Vous devez configurer des alertes afin d'envoyer les dérouterments que vous souhaitez recevoir.
Pour plus d'informations sur les alertes, reportez-vous à la section ["Configuration des alertes"](#) à la page 184.

Rubriques connexes

- ["Propriétés SNMP" à la page 324](#)

Propriétés SNMP

TABLEAU 93 Propriétés SNMP

Propriété	Description
Version	Bascule entre v1/2c et v3.
Nom de communauté	Bascule entre public et user-input. Si vous sélectionnez user-input, vous devez également saisir un nom de communauté. Si vous sélectionnez v3, cette propriété n'est pas disponible.
Réseau/sous-réseau autorisé	Saisissez une adresse IPv4 et un sous-réseau appropriés (entiers entre 0 et 32). Si vous sélectionnez v3, cette propriété n'est pas disponible.
Contact pour l'appareil	Saisissez un contact d'appareil approprié.
Nom d'utilisateur/mot de passe	Saisissez un nom d'utilisateur (501 caractères maximum) et un mot de passe (entre 8 et 501 caractères) valides. Si vous sélectionnez v1/2c, cette propriété n'est pas disponible.
Authentification	Bascule entre les algorithmes d'authentification MD5 et SHA. Si vous sélectionnez v1/2c, cette propriété n'est pas disponible.
Confidentialité	Bascule entre aucun algorithme de chiffrement et l'algorithme DES. Si vous sélectionnez v1/2c, cette propriété n'est pas disponible.
ID de moteur	Valeur EngineID hachée par snmpd. Si le protocole SNMP n'a pas été activé au préalable, l'étiquette affiche "0x000".
Destinations de dérouterment	Permet d'ajouter des adresses IPv4. Utilisez les boutons "+" et "-" pour ajouter ou enlever des adresses.

Le service SNMP fournit également la chaîne de l'emplacement MIB-II. Cette propriété provient de la configuration de [l'identité du système](#).

Bases de données MIB du service SNMP

Si les services SNMP sont en ligne, les réseaux autorisés ont accès aux bases de données MIB (Management Information Bases) suivantes :

TABLEAU 94 Bases de données MIB du service SNMP

MIB	Utilisation
.1.3.6.1.2.1.1	MIB-II system : informations système générales incluant le nom d'hôte, le contact et l'emplacement
.1.3.6.1.2.1.2	MIB-II interfaces - statistiques d'interface réseau
.1.3.6.1.2.1.4	IP MIB-II : informations de protocole Internet (Internet Protocol), incluant les adresses IP et la table route
.1.3.6.1.4.1.42	Sun Enterprise MIB (SUN-MIB.mib.txt)
.1.3.6.1.4.1.42.2.195	Sun FM : statistiques sur la gestion des pannes (voir le lien du fichier MIB ci-dessous)
.1.3.6.1.4.1.42.2.225	Sun AK : informations et statistiques relatives à l'appareil (voir le lien du fichier MIB ci-dessous)

Remarque - Les fichiers Sun MIB sont disponibles à l'adresse https://votre_adresse_IP_ou_nom_d'hôte:215/docs/snmp/.

MIB Sun FM

La MIB Sun FM (SUN-FM-MIB.mib.txt) permet d'accéder à des informations relatives à la gestion des pannes SUN :

- Problèmes actifs sur le système
- Événements de gestion des pannes
- Informations de configuration relatives à la gestion des pannes

Il existe quatre tables principales à lire :

TABLEAU 95 MIB Sun FM

OID	Contenu
.1.3.6.1.4.1.42.2.195.1.1	Problèmes liés à la gestion des pannes
.1.3.6.1.4.1.42.2.195.1.2	Événements de panne de la gestion des pannes
.1.3.6.1.4.1.42.2.195.1.3	Configuration du module de gestion des pannes
.1.3.6.1.4.1.42.2.195.1.5	Ressources défectueuses de la gestion des pannes

Vous trouverez des descriptions complètes dans le fichier MIB.

MIB Sun AK

La MIB Sun AK (SUN-AK-MIB.mib) fournit les informations suivantes :

- Chaîne de description du produit et référence

- Version logicielle de l'appareil
- Numéros de série de l'appareil et du châssis
- Durées d'installation, de mise à jour et d'initialisation
- Etat du cluster
- Etat du partage : nom et taille du partage, octets disponibles et utilisés

Il existe trois tables principales à lire :

TABLEAU 96 MIB Sun AK

OID	Contenu
.1.3.6.1.4.1.42.2.225.1.4	Informations générales relatives à l'appareil
.1.3.6.1.4.1.42.2.225.1.5	Etat du cluster
.1.3.6.1.4.1.42.2.225.1.6	Etat du partage

Vous trouverez des descriptions complètes dans le fichier MIB.

Configuration Syslog

Le service Syslog Relay offre deux fonctions différentes sur l'appareil :

- La fonction Alertes peut être configurée de façon à envoyer des messages Syslog à au moins un système distant. Reportez-vous à la section ["Configuration des alertes" à la page 184](#).
- Les messages syslog des services de l'appareil compatibles sont envoyés aux systèmes distants.

Un *message syslog* désigne un court message d'événement transmis par l'appareil à un ou plusieurs systèmes distants (plus communément appelé "intercontinental printf"). Ce message contient les éléments suivants :

- Facility : indique le type de composant système qui a envoyé le message.
- Severity : indique le niveau de gravité de la condition associée au message.
- Timestamp : indique la date et l'heure associées à l'événement au format UTC (temps universel).
- Hostname : indique le nom canonique de l'appareil
- Tag : indique le nom du composant système qui a envoyé le message. Pour plus de détails sur le format de ces messages, reportez-vous à la section ["Format du message d'alerte SYSLOG" à la page 328](#).
- Message : décrit l'événement. Pour plus de détails sur le format de ces messages, reportez-vous à la section ["Format du message d'alerte SYSLOG" à la page 328](#).

Les récepteurs Syslog sont fournis avec la plupart des systèmes d'exploitation, y compris Solaris et Linux. Certains packages de logiciel de gestion tiers ou disponibles en "open source"

prennent également en charge Syslog. Les récepteurs Syslog permettent aux administrateurs de regrouper les messages provenant d'un grand nombre de systèmes sur un seul système de gestion et de les intégrer dans un ensemble de fichiers journaux.

Le relais Syslog peut être configuré de façon à utiliser le format de sortie "classique" décrit dans le document RFC 3164 ou le format de sortie le plus récent avec version décrit dans le RFC 5424. Les messages Syslog sont transmis en tant que datagrammes UDP. Par conséquent, ils sont susceptibles d'être ignorés par le réseau ou de ne pas être envoyés du tout si le système d'envoi dispose de peu de mémoire ou si le réseau est encombré. Les administrateurs doivent donc partir du principe que, dans certains scénarios de panne complexe de réseau, certains messages peuvent manquer et avoir été ignorés.

Propriétés Syslog

- **Versión du protocole** : version du protocole Syslog à utiliser, à savoir Syslog classique (RFC 3164) ou Syslog mis à jour (RFC 5424).
- **Destinations** : liste des adresses de destination IPv4, IPv6 et FQDN vers lesquelles les messages sont transmis.

Pour configurer Syslog, reportez-vous aux sections suivantes :

- ["Syslog classique : RFC 3164" à la page 327](#)
- ["Syslog mis à jour : RFC 5424" à la page 327](#)
- ["Format de message SYSLOG" à la page 328](#)
- ["Format du message d'alerte SYSLOG" à la page 328](#)
- ["Exemple de configuration d'un récepteur Solaris \(CLI\)" à la page 330](#)
- ["Exemple de configuration d'un récepteur Linux \(CLI\)" à la page 331](#)

Syslog classique : RFC 3164

Le protocole Syslog classique inclut les valeurs facility et level (codées en nombre entier de priorité), timestamp, hostname, tag et le corps du message.

La valeur tag correspond à l'un des indicateurs décrits dans la section ["Format de message SYSLOG" à la page 328](#).

La valeur hostname correspond au nom canonique de l'appareil, comme défini dans la configuration de l'identité du système. Pour plus d'informations, reportez-vous à la section ["Configuration de l'identité du système" à la page 332](#).

Syslog mis à jour : RFC 5424

Le protocole Syslog classique inclut les valeurs facility et level (codées en nombre entier de priorité), un champ version (1), les valeurs timestamp, hostname, app-name et le corps du

message. Les messages Syslog transmis par les systèmes Sun Storage définissent les champs procid, msgid et structured-data de RFC 5424 avec une valeur nulle (-) afin d'indiquer que ces champs ne contiennent aucune donnée.

La valeur app-name correspond à l'un des indicateurs décrits dans la section ["Format de message SYSLOG" à la page 328](#).

La valeur hostname correspond au nom canonique de l'appareil, comme défini dans la configuration de l'identité du système. Pour plus d'informations, reportez-vous à la section ["Configuration de l'identité du système" à la page 332](#).

Format de message SYSLOG

Le protocole Syslog ne définit pas lui-même le format de charge utile du message, laissant ainsi à l'expéditeur le soin d'inclure le nombre approprié de chaînes de données structurées ou non, lisibles par l'utilisateur. Les appareils Sun Storage utilisent l'indicateur de sous-système syslog ak pour indiquer une charge utile de message analysable et structurée, comme décrit ci-après. D'autres indicateurs de sous-système indiquent un texte arbitraire lisible par l'utilisateur, mais les administrateurs doivent considérer ces formats de chaîne comme *instables* et sujets à des changements sans qu'ils en soient informés ou sans qu'ils puissent les supprimer dans les versions futures du logiciel Sun Storage.

TABEAU 97 Formats de message SYSLOG

Utilitaire	Nom de la balise	Description
daemon	ak	Indicateur générique pour les sous-systèmes de l'appareil. Toutes les alertes sont marquées ak, indiquant qu'elles sont suivies de SUNW-MSG-ID.
daemon	idmap	Service de mappage d'identité pour convertir les identités POSIX et Windows. Reportez-vous à la section "Configuration du mappage des identités" à la page 299 .
daemon	smbd	Protocole de données SMB pour l'accès aux partages. Reportez-vous à la section "Configuration SMB" à la page 243 .

Format du message d'alerte SYSLOG

Si une alerte est configurée avec l'action Envoyer un message Syslog, une charge utile de message syslog est produite. Elle contient un texte localisé composé les champs standard suivants. Chaque champ a pour préfixe le nom du champ en lettres MAJUSCULES suivi de deux-points et d'un espace.

TABLEAU 98 Formats du message d'alerte SYSLOG

Nom du champ	Description
SUNW-MSG-ID	Identificateur de message de panne Sun stable associé à l'alerte. Un identificateur unique est attribué dans le catalogue de message de panne Sun à chaque condition système et diagnostic de panne produisant une alerte administrateur. Vous pouvez facilement lire ces identificateurs sur votre téléphone ou les inscrire dans un carnet, puis consulter un article correspondant sur le site d'autorétablissement prédictif (Predictive Self-Healing) de My Oracle Support (https://support.oracle.com/) (Doc ID 1154428.1).
TYPE	Type de condition. Il correspond à l'une des étiquettes suivantes : Panne, indiquant une panne de connecteur ou de composant matériel ; Défaut indiquant une défaillance logicielle ou une mauvaise configuration ; Alerte, indiquant une condition non associée à une panne ou une défaillance, telle que la réussite d'une activité de sauvegarde ou de réplication distante.
VER	Version du format de codage. La description correspond à la version "1" du format SUNW-MSG-ID. Si "1" est présent dans le champ VER, le code d'analyse peut supposer que tous les champs suivants seront présents. Le code d'analyse doit être écrit pour gérer ou ignorer les champs supplémentaires si un nombre décimal supérieur à 1 est spécifié.
SEVERITY	Niveau de gravité d'une condition associé au problème qui a déclenché l'alerte. La liste des niveaux de gravité est affichée ci-dessous.
EVENT-TIME	Heure et date de l'événement. Le format est le suivant : "Jour Mois DD HH:MM:SS AAAA" (UTC). Par exemple : Fri Aug 14 21:34:22 2009 (vendredi 14 août 2009, 21h34 22 secondes).
PLATFORM	Identificateur de plate-forme pour l'appareil. Ce champ est réservé à Oracle Service.
CSN	Numéro de série du châssis de l'appareil.
HOSTNAME	Nom canonique de l'appareil, comme défini dans la configuration de l'identité du système. Voir la section System Identity .
SOURCE	Sous-système du logiciel de l'appareil qui a émis l'événement. Ce champ est réservé à Oracle Service.
REV	Révision interne du sous-système. Ce champ est réservé à Oracle Service.
EVENT-ID	Identificateur unique universel (UUID) associé à cet événement. Le système de gestion des pannes Oracle associe un UUID à chaque alerte et diagnostic de panne de façon à ce que les administrateurs puissent regrouper et mettre en corrélation plusieurs messages associés à une seule condition et détecter les messages dupliqués. Le personnel Oracle Service peut utiliser le type de condition EVENT-ID pour récupérer des informations supplémentaires d'analyse rétrospective associées au

Nom du champ	Description
	problème qui pourraient aider Oracle à résoudre le problème.
DESC	Description de la condition associée à l'événement.
AUTO-RESPONSE	Le cas échéant, réponse automatique au problème par le logiciel de gestion des pannes inclus dans le système. Les réponses automatiques incluent des possibilités telles que la mise hors ligne préventive des disques, puces de mémoire DRAM et coeurs de processeur défectueux.
REC-ACTION	Opération de maintenance recommandée. Il s'agit d'un bref résumé des actions recommandées mais il est conseillé aux administrateurs de consulter l'article de la base de connaissances ainsi que la présente documentation pour obtenir des informations relatives à la procédure de réparation.

Le champ SEVERITY sera défini avec une des valeurs suivantes :

TABLEAU 99 Champs Severity de Syslog

Severity (Gravité)	Niveau syslog	Description
Mineur	LOG_WARNING	Une condition s'est produite mais n'affecte pas encore le fonctionnement et requiert une intervention avant que la situation ne s'aggrave.
Majeur	LOG_ERR	Une condition qui affecte légèrement le fonctionnement s'est produite.
Critique	LOG_CRIT	Une condition qui affecte gravement le fonctionnement s'est produite et requiert une intervention immédiate.

Exemple de configuration d'un récepteur Solaris (CLI)

La plupart des systèmes d'exploitation incluent un récepteur syslog mais il est possible que certaines étapes de configuration soient requises pour l'activer. Consultez la documentation correspondant à votre système d'exploitation ou logiciel de gestion pour obtenir des informations détaillées sur la configuration d'un récepteur syslog.

Solaris comprend un service syslogd (1M) intégré qui peut faire office de récepteur syslog, mais la fonction de réception à distance est désactivée par défaut. Pour que Solaris reçoive le trafic syslog, exécutez les commandes svccfg et svcadm pour modifier les paramètres syslog comme suit :

```
# svccfg -s system/system-log setprop config/log_from_remote = true
# svcadm refresh system/system-log
```

Solaris syslogd comprend uniquement le protocole Syslog classique. Reportez vous à la page de manuel `syslog.conf` (4) pour plus d'informations sur la configuration du filtrage et la journalisation des messages reçus.

Par défaut, Solaris syslogd enregistre les messages dans `/var/adm/messages` et une alerte de test est enregistrée comme suit :

```
Aug 14 21:34:22 poptart.sf.fishpong.com poptart ak: SUNW-MSG-ID: AK-8000-LM, \
TYPE: alert, VER: 1, SEVERITY: Minor\nEVENT-TIME: Fri Aug 14 21:34:22 2009\n\
PLATFORM: i86pc, CSN: 12345678, HOSTNAME: poptart\n\
SOURCE: jsui.359, REV: 1.0\n\
EVENT-ID: 92dfef39-6e15-e2d5-a7d9-dc3e221becea\n\
DESC: A test alert has been posted.\n\
AUTO-RESPONSE: None.\nIMPACT: None.\nREC-ACTION: None.
```

Exemple de configuration d'un récepteur Linux (CLI)

La plupart des systèmes d'exploitation incluent un récepteur syslog mais il est possible que certaines étapes de configuration soient requises pour l'activer. Consultez la documentation correspondant à votre système d'exploitation ou logiciel de gestion pour obtenir des informations détaillées sur la configuration d'un récepteur syslog.

La plupart des distributions Linux incluent un démon `sysklogd` (8) intégré qui peut faire office de récepteur syslog, mais la fonction de réception à distance est désactivée par défaut. Pour activer la réception du trafic syslog dans Linux, modifiez le fichier de configuration `/etc/sysconfig/syslog` de façon à inclure l'option `-r` (fonction qui active la journalisation à distance) :

```
SYSLOGD_OPTIONS="-r -m 0"
```

puis redémarrez le service de journalisation :

```
# /etc/init.d/syslog stop
# /etc/init.d/syslog start
```

Certaines distributions Linux incluent un filtre `ipfilter` qui rejette les paquets UDP syslog par défaut. Il faut donc modifier ce filtre pour qu'il les accepte. Sur ces distributions, exécutez une commande similaire à la suivante pour ajouter une règle INPUT afin d'accepter les paquets UDP syslog :

```
# iptables -I INPUT 1 -p udp --sport 514 --dport 514 -j ACCEPT
```

Par défaut, Linux syslogd enregistre les messages dans `/var/log/messages` et une alerte de test est enregistrée comme suit :

```
Aug 12 22:03:15 192.168.1.105 poptart ak: SUNW-MSG-ID: AK-8000-LM, \
TYPE: alert, VER: 1, SEVERITY: Minor EVENT-TIME: Wed Aug 12 22:03:14 2009 \
PLATFORM: i86pc, CSN: 12345678, HOSTNAME: poptart SOURCE: jsui.3775, REV: 1.0 \
EVENT-ID: 9d40db07-8078-4b21-e64e-86e5cac90912 \
DESC: A test alert has been posted. AUTO-RESPONSE: None. IMPACT: None. \
REC-ACTION: None.
```

Configuration de l'identité du système

Ce service offre une configuration pour le nom et l'emplacement du système. Vous devrez peut-être modifier ces éléments si vous déplacez l'appareil vers un nouveau réseau ou si vous modifiez son utilisation.

L'appareil prend en charge les certificats possédés par les clients. Le cycle de vie d'un certificat début avec la génération d'une demande de signature de certificat (CSR, Certificate Signing Request). La CSR est ensuite envoyée à l'autorité de certification (CA, Certificate Authority) pour signature. Le certificat signé est ensuite retourné par le CA, il peut être installé sur l'appareil. Si un certificat est signé par un CA non-root, vous devez également obtenir des certificats des CA de niveau secondaire et supérieur.

Pour configurer l'identité du système, effectuez les tâches suivantes :

- Création d'un certificat - [BUI](#), [CLI](#)
- Chargement de certificats à partir de CA non-root - [BUI](#), [CLI](#)
- Affichage des détails de CSR et de certificat - [BUI](#), [CLI](#)
- Définition du certificat d'appareil - [BUI](#), [CLI](#)
- Destruction d'une CSR ou d'un certificat - [BUI](#), [CLI](#)

Pour comprendre l'identité du système, reportez-vous aux rubriques suivantes :

- ["Propriétés et journaux de l'identité du système" à la page 339](#)

▼ Création d'un certificat (BUI)

Pour créer un nouveau certificat, procédez comme suit :

1. **Accédez à Configuration > Services > Identité du système.**
2. **Cliquez sur l'onglet Certificats.**
3. **Pour créer une nouvelle CSR, cliquez sur l'icône d'ajout .**
Pour créer une nouvelle CSR sur la base d'une CSR ou d'un certificat existant, déplacez le pointeur de la souris sur l'entrée de votre choix et cliquez sur l'icône de copie .
4. **Complétez le formulaire de la CSR.**
5. **Cliquez sur CREER.**
6. **Lorsque vous êtes invité à ouvrir la CSR ou à l'enregistrer, sélectionnez Enregistrer le fichier et cliquez sur OK pour enregistrer la CSR maintenant, ou cliquez sur Annuler pour l'enregistrer ultérieurement.**

Pour enregistrer la CSR ultérieurement, déplacez le curseur de la souris sur l'entrée et cliquez sur l'icône de téléchargement .

7. **Transférez la CSR vers votre CA de la manière préconisée.**
8. **Après réception du certificat signé par le CA, cliquez sur l'icône de chargement .**
9. **Accédez au certificat signé et sélectionnez-le.**
10. **Cliquez sur CHARGER.**

▼ Création d'un certificat (CLI)

Pour créer un nouveau certificat, procédez comme suit :

1. **Pour créer une nouvelle CSR, saisissez le contexte `configuration services identity certificates` et la commande `create`.**

Sinon, pour créer une nouvelle CSR basée sur une CSR existante ou un certificat, saisissez le contexte ci-dessus puis la commande `clone CSR` or `certificate number`. Par exemple :

```
hostname:configuration services identity certificates> clone cert-000
```

2. **Pour compléter le formulaire de la CSR, utilisez les commandes suivantes de la CLI :**

```
hostname:configuration services identity cert (uncommitted)> get
  subject_commonname = hostname.us.example.com
  subject_organizationname = (unset)
  subject_organizationalunitname = (unset)
  subject_localityname = (unset)
  subject_stateorprovincename = (unset)
  subject_countryname = (unset)
  subject_emailaddress = (unset)
  dns = hostname.us.example.com
  ip = 192.0.2.1
  uri = (unset)
  comment = (unset)
hostname:configuration services identity cert (uncommitted)> set comment="test certificate"
  comment = test certificate (uncommitted)
hostname:configuration services identity cert (uncommitted)> commit
```

3. **Pour afficher la CSR, utilisez les commandes suivantes :**

```
hostname:configuration services identity certificates> show
Properties:
```

```

                                default = auto

Certificates:
CERT      TYPE FOR                                ISSUER                                EXPIRES
cert-000 req  hostname.us.example.com
cert-001 CA   Joe Test CA                        Joe Test CA                        2015-1-2
cert-002 cert hostname.us.example.com           Joe Test CA                        2015-12-3

hostname:configuration services identity certificates> dump cert-000
-----BEGIN CERTIFICATE REQUEST-----
MIICwzCCAasCAQIwIjEgMB4GA1UEAxMXaG9zdG5hbWUudXMuzXhhbXBsZS5jb20w
ggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAAoIBAQU4ErPuRrVfy21K2qyfgY9
P4bSXMLZxP48HKI/jVuS4MNeVHCL3TILvuiXx217qjacCkiIKDG5z1TFIApt2Ee
4rU7PC1YgYw8HAHDq+GJbSV2CWLVC78muNfntSuzsFAljdTr/f/5qQdQwfxvJ+Oi
a4JU03mTn2eUP75EA9ASEmGWH/V3bnWdzuOuc/LFuXRSmb3W0gwYrIeHk6mcJzEE
zZtLIF9KQzSisu4m2JjcScta0YSWIC0TP0war5Gc8vIoIC7gJahw4/WvZAFNZ/8
c/nVBs4/hXhyGMDSII0yULI03U8jJN3Ggssw+4C0KmcgQJMzWJ2Cax4GsSuu8MDh
AgMBAAAGgXDBaBgkqhkiG9w0BCQ4xTTBLMB8GCWCGSAGG+EIBDQCSFhB0ZXN0IGNl
cnRpZmLjYXRlMCgGA1UdEQQhMB+CF2hvc3RuYW1lLnVzLmV4YW1wbGUuY29thwTA
AAIBMA0GCSqGSIb3DQEBQUAA4IBAQBjGSGrS/DoStsAYyYCYu6y4TN5i903ASLW
m9+CXbNj6XYXgWssqDOvJOnW/TGoGHN3f3741Xgbf6snFQ3T1MN9Dm6rcZ95tOM
PLxfVY9ar8WygSE8ttunxPDjNbBRoK0aR7qMq5JMH0rKS9Iuz9WghiaGLw7WBaLN
akCjxFS8yh5sVqF9zAqoa00buXnQ3kfTDVzYvroy2yummBfXrJB5t35bbTqZNT/f
bRoSMtroHL+iWBx1zK+A70S5/+Zuow8PqpHRkf0/j7Y9Jz1tfhTVyu1bbxE6ZyLD
lhwbLMXqR/3xptwym1vy5dYBJsQLKroA8nr/xFb3nhJB8nI+dxSN
-----END CERTIFICATE REQUEST-----

```

4. Copiez la CSR et transférez-la vers votre CA de la manière préconisée.

5. Après réception du certificat signé par le CA, saisissez le contexte configuration services identity certificates puis la commande import.

```

hostname:configuration services identity certificates> import
("." to end)> -----BEGIN CERTIFICATE-----
("." to end)> MIID0DCCArigAwIBAgIBQDANBgkqhkiG9w0BAQUFADCBMDELMAKGA1UEBmCVMx
("." to end)> EzARBgNVBAgMCkNhbgGmb3JuaWExFDASBgNVBAcMC0xvcyBBbmdlbGVzMQ8wDQYD
("." to end)> VQKDAZPcmFjbGUGxEDA0BgNVBAcMB1N5c3RlbXBMxwFDASBgNVBAMMC0pvZSBUZXN0
("." to end)> IENBMSUwIwYJKoZIhvcNAQkBFhZGaXJzdCMYXN0QGV4YW1wbGUuY29tMB4XDTE0
("." to end)> MTIwNDAwMzEzMloXDTE1MTIwNDAwMzEzMlowIjEgMB4GA1UEAxMXaG9zdG5hbWUu
("." to end)> dXMuzXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAAoIBAQU4
("." to end)> 4ErPuRrVfy21K2qyfgY9P4bSXMLZxP48HKI/jVuS4MNeVHCL3TILvuiXx217qja
("." to end)> cCkiIKDG5z1TFIApt2Ee4rU7PC1YgYw8HAHDq+GJbSV2CWLVC78muNfntSuzsFAl
("." to end)> jdTr/f/5qQdQwfxvJ+Oia4JU03mTn2eUP75EA9ASEmGWH/V3bnWdzuOuc/LFuXRS
("." to end)> mb3W0gwYrIeHk6mcJzEEzZtLIF9KQzSisu4m2JjcScta0YSWIC0TP0war5Gc8vI
("." to end)> oIC7gJahw4/WvZAFNZ/8c/nVBs4/hXhyGMDSII0yULI03U8jJN3Ggssw+4C0Kmcg
("." to end)> QJMzWJ2Cax4GsSuu8MDhAgMBAAAGjgZkwgZYwCYDVR0TBAlwADAdBgNVHQ4EFgQU
("." to end)> aB36PqLQLE0+q9Au7PoeFvdSvkwHwYDVR0jBBgwFoAUzD6A5miqxSmbDEtBAI4u
("." to end)> LUPMZU8wHwYJIZIAYb4QgENBBIWEHRlc3QgY2VydGlmawNhdGUwKAYDVR0RBCEw
("." to end)> H4IXaG9zdG5hbWUudXMuzXhhbXBsZS5jb22HBMAAAgEwDQYJKoZIhvcNAQEFBQAD
("." to end)> ggEBAFAmJlCrhnTaulpDCU0H9mFLee7Tft0lvCoh1G1Y33sjwWVgy0F5A3ymrdG
("." to end)> enQgEGdl+CzoxL2qM0bpb7Qk/DdEcYdCypd0hfyg18S6mRwaFDvBidZZ+PRR7zo5
("." to end)> hGFu+eLPddeAq0jq0tLhnlkTESSyseUK5PCv5P5xTtIHRg2bcb5VtUCU0iW2hDT
("." to end)> vyPtjqb0aP6eTuWzDZaM9YWQ5BfIcU6h0+zSWHywhCsDs4S62vh8hYozVf66mgsp
("." to end)> vaGPnv01xBigK+FcPi9PzomHwv+5UKDB0m6QOKkH0d0908jFxxCC1SYw6G/Cj1+g
("." to end)> 2ai9ZwREdTkcjcgQDxeHNZCpcHk=

```

```
("." to end)> -----END CERTIFICATE-----
("." to end)> .
```

6. Pour vérifier les certificats importés, affichez toutes les entrées de certificats à l'aide de la commande `show`.

```
hostname:configuration services identity certificates> show
Properties:
    default = auto
Certificates:
CERT    TYPE FOR                                ISSUER                                EXPIRES
cert-000 req hostname.us.example.com Joe Test CA 2015-12-4
cert-001 CA Joe Test CA Joe Test CA 2015-1-2
cert-002 cert hostname.us.example.com Joe Test CA 2015-12-3
```

▼ Chargement de certificats à partir de CA non-root (BUI)

Si votre certificat est signé par un CA non-root, vous devez également obtenir des certificats pour les CA de niveau secondaire et supérieur. Après l'obtention de ces certificats CA, procédez comme suit pour les charger :

1. **Accédez à Configuration > Services > Identité du système.**
2. **Cliquez sur l'onglet Certificats.**
3. **Cliquez sur l'icône de chargement .**
4. **Accédez au certificat signé et sélectionnez-le.**
5. **Cliquez sur CHARGER.**
6. **Répétez les étapes 3 à 5 pour chaque certificat signé.**

▼ Chargement de certificats à partir de CA non-root (CLI)

Si votre certificat est signé par un CA non-root, vous devez également obtenir des certificats pour les CA de niveau secondaire et supérieur. Après l'obtention de ces certificats CA, procédez comme suit pour les charger :

1. **Pour charger un certificat, saisissez le contexte `configuration services identity certificates` puis la commande `import`.**

```
hostname:configuration services identity certificates> import
("." to end)> -----BEGIN CERTIFICATE-----
("." to end)> MIID0DCCArigAwIBAgIBQDANBgkqhkiG9w0BAQUFADCBmDELMAkGA1UEBhMCVVMx
```

```
(". " to end)> EzARBgNVBAgMCkNhbg1mb3JuaWExFDASBgNVBAcMC0xvcyBBbmdlbGVzMQ8wDQYD
(". " to end)> VQOKDAZPcmFjbGUxEDA0BgNVBA5MB1N5c3RlbXMxZDASBgNVBAMMC0pvZSBUZXN0
(". " to end)> IENBMSUwIwYJKoZIhvcNAQkBFhZGaXJzdC5MYXN0QGV4YW1wbGUuY29tMB4XDTE0
(". " to end)> MTIwNDAwMzEzM1oXDTE1MTIwNDAwMzEzM1owIjEgMB4GA1UEAxMXaG9zdG5hbWUu
(". " to end)> dXMuZXhhbXBsZS5jb20wggEiMA0GCSqGSIb3DQEBQUAA4IBDwAwggEKAoIBAQU
(". " to end)> 4ErPuRrVfy21K2qyfy9P4bSxMLZxP48HKI/jVuS4MNeVHCL3TILvuiXx217qja
(". " to end)> cCkiIKDG5z1TFIApt2Ee4rU7PC1YgYw8HAHDq+GJbSV2CWLVC78muNFntSuzsFAL
(". " to end)> jdTr/f/5qQdQwfxvJ+Oia4JU03mTn2eUP75EA9ASEmGWH/V3bnWdzuOuc/LFuXRS
(". " to end)> mb3W0gwYrIeHk6mcJzEEZztLIF9KQqzSisu4m2JjcScta0YSWIC0TP0war5Gc8vI
(". " to end)> oIC7gJahw4/WvZAFNZ/8c/nVBs4/hXhyGMDsII0yULI03U8jJN3Ggssw+4C0Kmcg
(". " to end)> QJMzWJ2Cax4GsSuu8MDhAgMBAAGjgZkwgZYwCQYDVR0TBAlwADAAdBgNVHQ4EFgQU
(". " to end)> aB36PqLQLE0+q9Au7PoeFvdSvkvHwYDVR0jBBgwFoAUZD6A5miqxSmbDEtBAI4u
(". " to end)> LUPMzU8wHwYJYIZIAyb4QgENBBIWEHRlc3QgY2VydGlmawNhdGUwKAYDVR0RBCEw
(". " to end)> H4IXaG9zdG5hbWUudXMuZXhhbXBsZS5jb22HBMAAAgEwDQYJKoZIhvcNAQEFBQAD
(". " to end)> ggEBAFAmjiCrhnTaulpDCU0H9mFLee7Tft0lvC0h1G1Y33sjwWwVgy0F5A3ymrdG
(". " to end)> enQgEGdl+CzoxL2Qm0bpb7Qk/DdEcYdCyp0hfyg18S6mRwaFDvB1dZZ+PRR7zo5
(". " to end)> hGFu+eLPddeAq0jq0tlnlktESSyseUk5PCv5Px5xTtIHRg2bc5vUUCu0iW2hDT
(". " to end)> vyPtjqb0aP6eTuWzDZaM9YWQ5BfIcU6h0+zSWHywhCsDs4S62vh8hYozVf66mgsp
(". " to end)> vaGPnv01xBigK+FcPi9PzomHwv+SUKDB0m6QOKkH0d0908jFxxCC1SYw6G/Cj1+g
(". " to end)> 2ai9ZwRedTkjcgQDxeHNZCpcHk=
(". " to end)> -----END CERTIFICATE-----
(". " to end)> .
```

2. Répétez l'étape 1 pour chaque certificat signé.

3. Pour vérifier les certificats importés, affichez toutes les entrées de certificats à l'aide de la commande show.

```
hostname:configuration services identity certificates> show
Properties:
    default = auto

Certificates:
CERT    TYPE FOR                                ISSUER                                EXPIRES
cert-000 req hostname.us.example.com Joe Test CA 2015-12-4
cert-001 CA Joe Test CA Joe Test CA 2015-1-2
cert-002 cert hostname.us.example.com Joe Test CA 2015-12-3
```

▼ Affichage des détails de CSR et de certificat (BUI)

Pour afficher les détails de la CSR et du certificat, procédez comme suit :

1. **Accédez à Configuration > Services > Identité du système.**
2. **Cliquez sur l'onglet Certificats.**
3. **Déplacez le pointeur de la souris sur une entrée existante et cliquez sur l'icône d'informations  correspondante.**
4. **Lorsque vous avez terminé, cliquez sur OK pour fermer la fenêtre des détails.**

▼ Affichage des détails de CSR et de certificat (CLI)

Pour afficher les détails de la CSR et du certificat, procédez comme suit :

1. **Pour afficher toutes les entrées de certificat, accédez à configuration services identity certificates et entrez la commande show.**

```
hostname:configuration services identity certificates> show
Properties:
    default = auto
Certificates:
CERT    TYPE FOR                                ISSUER                                EXPIRES
cert-000 req hostname.us.example.com Joe Test CA 2015-12-4
cert-001 CA Joe Test CA Joe Test CA 2015-1-2
cert-002 cert hostname.us.example.com Joe Test CA 2015-12-3
```

2. **Pour afficher les détails d'une CSR ou d'un certificat, utilisez les commandes suivantes :**

```
hostname:configuration services identity certificates> select cert-000
hostname:configuration services identity cert-000> show
Properties:
    uuid = 195071da-66ac-43a6-edfa-bbbd7451f1d5
    subject_commonname = hostname.us.example.com
    issuer_commonname = Joe Test CA
    issuer_organizationname = Oracle
    issuer_organizationalunitname = Systems
    issuer_localityname = Los Angeles
    issuer_stateorprovincename = California
    issuer_countryname = US
    issuer_emailaddress = First.Last@example.com
    dns = hostname.us.example.com
    ip = 192.0.2.1
    comment = test certificate
    notbefore = 2014-12-4 00:31:33
    notafter = 2015-12-4 00:31:33
    shalfingerprint = 81:A2:4B:C4:06:A9:14:1E:3E:0B:8A:70:FB:1A:30:45:2D:93:DD:02
    md5fingerprint = B7:B2:F4:3B:BB:04:8E:11:A2:64:3D:69:BF:8A:79:CC
hostname:configuration services identity cert-000> done
```

▼ Définition du certificat d'appareil (BUI)

Pour définir le certificat d'appareil, procédez comme suit :

1. **Accédez à Configuration > Services > Identité du système.**
2. **Cliquez sur l'onglet Propriétés.**
3. **Dans le menu déroulant des certificats par défaut du système, sélectionnez le certificat que vous souhaitez définir comme certificat par défaut.**

4. Cliquez sur **APPLIQUER**.

▼ Définition du certificat d'appareil (CLI)

Pour définir le certificat d'appareil, procédez comme suit :

1. **Pour afficher toutes les entrées de certificat, accédez à configuration services identity certificates et entrez la commande show.**

```
hostname:configuration services identity certificates> show
Properties:
    default = auto

Certificates:
CERT   TYPE FOR      ISSUER      EXPIRES
cert-000 req hostname.us.example.com Joe Test CA 2015-12-4
cert-001 CA   Joe Test CA   Joe Test CA 2015-1-2
cert-002 cert hostname.us.example.com Joe Test CA 2015-12-3
```

2. **Pour définir un certificat par défaut, utilisez les commandes suivantes :**

```
hostname:configuration services identity certificates> set default=cert-000
    default= cert-000 (uncommitted)
hostname:configuration services identity certificates> commit
```

▼ Destruction d'une CSR ou d'un certificat (BUI)

Pour détruire une CSR ou un certificat, procédez comme suit :

Remarque - La destruction d'une CSR détruit également la clé privée associée. Par conséquent, l'importation d'un certificat dérivé d'une CSR n'est pas possible. La destruction d'un certificat détruit également la clé privée associée. Par conséquent, il ne sera pas possible de réimporter ce certificat.

1. **Accédez à Configuration > Services > Identité du système.**
2. **Cliquez sur l'onglet Certificats.**
3. **Déplacez le curseur de la souris sur une entrée et cliquez sur l'icône de la corbeille .**
4. **Cliquez sur DETRUIRE.**

▼ Destruction d'une CSR ou d'un certificat (CLI)

Pour détruire une CSR ou un certificat, procédez comme suit :

Remarque - La destruction d'une CSR détruit également la clé privée associée. Par conséquent, l'importation d'un certificat dérivé d'une CSR n'est pas possible. La destruction d'un certificat détruit également la clé privée associée. Par conséquent, il ne sera pas possible de réimporter ce certificat.

1. **Pour afficher toutes les entrées de certificat, accédez à configuration services identity certificates et entrez la commande show.**

```
hostname:configuration services identity certificates> show
Properties:
    default = auto
Certificates:
CERT  TYPE FOR                               ISSUER                               EXPIRES
cert-000 req hostname.us.example.com Joe Test CA 2015-12-4
cert-001 CA Joe Test CA Joe Test CA 2015-1-2
cert-002 cert hostname.us.example.com Joe Test CA 2015-12-3
```

2. **Pour détruire une CSR ou un certificat, utilisez les commandes suivantes :**

```
hostname:configuration services identity certificates> destroy cert-002
Caution: Destroying a certificate issued by a certificate authority
also destroys the associated private key.Re-importing the certificate will not be possible.
Destroy appliance certificate? (Y/N) Y
```

Propriétés et journaux de l'identité du système

Les propriétés d'identité du système sont décrites dans le tableau suivant.

TABLEAU 100 Propriétés d'identité du système

Propriété de la BUI	Description
Nom du système	Nom unique au format canonique qui identifie l'appareil dans l'interface utilisateur. Ce nom est différent des noms DNS utilisés pour se connecter au système (qui doit être configuré sur les serveurs DNS distants). Vous pouvez modifier ce nom quand vous le souhaitez.
Emplacement du système	Chaîne de texte décrivant l'emplacement physique de l'appareil. Si le service SNMP est activé, elle sera exportée en tant que chaîne <i>syslocation</i> dans MIB-II.
Certificat par défaut du système	Menu déroulant vous permettant de faire une sélection parmi les certificats existants.

La procédure de modification des propriétés des services est documentée dans les sections "[Définition des propriétés du service \(BUI\)](#)" à la page 230 et "[Définition des propriétés du service \(CLI\)](#)" à la page 231. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

TABLEAU 101 Journaux d'identité du système

Journal	Description
system-identity:node	Consigne les événements de service et les erreurs d'identité du système

Pour afficher les journaux de service, reportez-vous à la section ["Utilisation des journaux"](#) dans le *Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance*.

Configuration SSH

Le service SSH (Secure Shell) permet aux utilisateurs de se connecter à la CLI de l'appareil et d'effectuer la plupart des opérations d'administration pouvant être réalisées dans l'interface utilisateur du navigateur (BUI). SSH peut également servir de moyen d'exécution des scripts automatiques à partir d'un hôte distant, par exemple pour extraire les journaux quotidiens ou les statistiques d'analyse.

Des clés SSH peuvent être configurées pour des comptes individuels à l'aide de la fonction Préférences décrite dans la section ["Configuration des préférences pour l'appareil"](#) à la page 179.

Pour configurer SSH, reportez-vous aux sections suivantes :

- ["Désactivation de l'accès SSH root \(CLI\)"](#) à la page 340
- ["Propriétés et journaux SSH"](#) à la page 340

▼ Désactivation de l'accès SSH root (CLI)

1. **Accédez à configuration services ssh.**
2. **Désactivez l'autorisation de connexion de root.**
3. **Validez la configuration.**

Propriétés et journaux SSH

TABLEAU 102 Propriétés SSH

Propriété	Description	Exemples
Longueur de la clé du serveur	Quantité de bits dans la clé éphémère.	768
Intervalle de régénération de la clé	Intervalle de régénération de la clé éphémère (en secondes).	3600

Propriété	Description	Exemples
Période de grâce pour la connexion	Si le client ne parvient pas à s'authentifier dans le délai imparti, la connexion SSH est interrompue.	120
Autoriser la connexion de root	Permet à l'utilisateur root de se connecter à l'aide de SSH.	oui
Port (pour les connexions entrantes)	Port désigné pour les connexions entrantes.	22

TABLEAU 103 Journaux SSH

Journal	Description
network-ssh:default	Journal des événements et des erreurs du service SSH.

Configuration de l'API RESTful

L'API RESTful d'Oracle ZFS Storage Appliance permet la gestion de l'appareil à l'aide de l'exécution de demandes simples, telles que GET, PUT, POST, et DELETE HTTP dans des chemins d'accès URL de ressources gérées.

L'appareil basé sur une architecture REST est défini en tant que modèle client-serveur en couches. Les avantages de ce modèle sont les suivants : les services peuvent être redirigés de manière transparente à l'aide de hubs, routeurs et autres systèmes réseau standard sans nécessiter la configuration du client. Cette architecture prend en charge la mise en cache d'informations et s'avère utile si de nombreux clients demandent les mêmes ressources statiques.

Pour obtenir toutes les informations concernant l'API RESTful de Oracle ZFS Storage Appliance, reportez-vous au [Guide RESTful API des systèmes Oracle ZFS Storage Appliance](#).

Partages et projets

Oracle ZFS Storage Appliance utilise les pools de stockage, les projets et les partages pour organiser les données. Les partages désignent des systèmes de fichiers et des LUN exportés par des protocoles de données pris en charge vers des clients de l'appareil. Tous les partages au sein d'un projet peuvent avoir des paramètres communs et des quotas peuvent être appliqués au niveau du projet en plus d'être appliqués au niveau du partage. Pour plus d'informations sur la façon dont l'appareil organise les données, reportez-vous à la section "[A propos des pools de stockage, des projets et des partages](#)" à la page 361.

Pour créer et modifier des projets, utilisez ces tâches :

- Création d'un projet - [BUI](#), [CLI](#)
- Modification d'un projet - [BUI](#), [CLI](#)
- Modification du nom d'un projet - [BUI](#), [CLI](#)
- Suppression d'un projet - [BUI](#), [CLI](#)

Pour créer et modifier des systèmes de fichiers ou des LUN, utilisez ces tâches :

- Création d'un système de fichiers ou d'un LUN dans un projet - [BUI](#), [CLI](#)
- Modification d'un système de fichiers ou d'un LUN - [BUI](#), [CLI](#)
- Modification du nom d'un système de fichiers ou d'un LUN - [BUI](#), [CLI](#)
- Déplacement d'un système de fichiers ou d'un LUN dans un projet - [BUI](#), [CLI](#)
- Suppression d'un système de fichiers ou d'un LUN - [BUI](#), [CLI](#)
- Définition de quotas d'utilisateur ou de groupe - [BUI](#), [CLI](#)

Pour mieux comprendre la façon dont l'appareil organise le stockage, consultez les rubriques suivantes :

- "[A propos des pools de stockage, des projets et des partages](#)" à la page 361
- "[Gestion de l'espace pour les partages](#)" à la page 400
- "[Propriétés des projets et partages](#)" à la page 363
- "[Utilisation de l'espace de noms du système de fichiers](#)" à la page 404
- "[Statistiques d'utilisation des partages](#)" à la page 406
- "[Protocoles de partage et de projet](#)" à la page 407
- "[Listes de contrôle d'accès des systèmes de fichiers](#)" à la page 420

- ["Utilisation des schémas" à la page 427](#)

▼ Création d'un projet (BUI)

Utilisez cette tâche pour créer un projet non chiffré. Pour créer un projet chiffré, reportez-vous à la section ["Création d'un projet chiffré \(BUI\)" à la page 570](#).

1. **Accédez à Partages > Projets.**
2. **Cliquez sur l'icône Ajouter  située à côtés de Projets ou dans le panneau étendu Projets. Pour développer le panneau Projets, cliquez sur la flèche.**
3. **Dans la fenêtre Créer un projet, entrez le nom du nouveau projet.**
Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.
4. **Cliquez sur APPLIQUER.**
Le nouveau projet est ajouté à la liste des projets.

Rubriques connexes

- ["Propriétés des projets" à la page 377](#)
- ["Création d'un projet chiffré \(BUI\)" à la page 570](#)

▼ Création d'un projet (CLI)

Utilisez cette tâche pour créer un projet non chiffré. Pour créer un projet chiffré, reportez-vous à la section ["Création d'un projet chiffré \(CLI\)" à la page 571](#).

1. **Accédez à shares.**

```
hostname:> shares
```
2. **Entrez project et le nom d'un projet.**
Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.

```
hostname:shares> project home
```
3. **Pour répertorier les propriétés du projet, utilisez la commande get.**


```

hostname:shares home(uncommitted)> get
      mountpoint = /export (default)
      quota = 0 (default)
      reservation = 0 (default)
      sharesmb = off (default)
      sharenfs = on (default)
      encryption = off (default)
      sharedav = off (default)
      shareftp = off (default)
      sharesftp = off (default)
      sharetftp = off (default)
      default_group = other (default)
      default_permissions = 700 (default)
      default_sparse = true (default)
      default_user = nobody (default)
      default_volblocksize = 8K (default)
      default_volsize = 0 (default)
      aclinherit = (default)
      aclmode = (default)
      atime = (default)
      checksum = (default)
      compression = (default)
      dedup = (default)
      copies = (default)
      logbias = (default)
      readonly = (default)
      recordsize = (default)
      rstchown = (default)
      secondarycache = (default)
      nbmand = (default)
      snapdir = (default)
      vscan = (default)
      defaultuserquota = (default)
      defaultgroupquota = (default)
      snaplabel = (default)
      canonical_name = (default)
      keyname = (default)
      keystore = (default)
      exported = (default)
      nodestroy = (default)
hostname:shares home (uncommitted)>

```

4. **Pour modifier les propriétés du projet, utilisez la commande `set`. Les propriétés d'un projet sont décrites dans la section ["Propriétés des projets" à la page 377](#).**
5. **Saisissez `commit`.**

```
hostname:shares home> commit
```

Rubriques connexes

- ["Propriétés des projets" à la page 377](#)

- ["Création d'un projet chiffré \(CLI\)" à la page 571](#)

▼ Modification d'un projet (BUI)

Pour modifier les propriétés du projet, suivez ces étapes.

1. **Accédez à Partages > Projets.**
2. **Sélectionnez un projet de l'une des manières suivantes :**
 - Déplacez le curseur de la souris sur le projet et cliquez sur l'icône de modification .
 - Cliquez deux fois sur le nom du projet.
 - Cliquez sur l'icône de flèche en regard de Projets pour développer le panneau, puis cliquez sur le nom du projet.

Le projet est sélectionné et les onglets sont affichés pour modifier les propriétés.

3. **Cliquez sur l'un des onglets pour modifier les propriétés du projet.**
4. **Modifiez les propriétés du projet au besoin. Reportez-vous à la section ["Propriétés des projets" à la page 377](#).**

Rubriques connexes

- ["Instantanés et clones" à la page 441](#)
- ["Réplication distante" à la page 473](#)

▼ Modification d'un projet (CLI)

Pour modifier les propriétés du projet, suivez ces étapes.

1. **Accédez à shares.**

```
hostname:> shares
```
2. **Entrez select et le nom d'un projet.**

```
hostname:shares> select home
```
3. **Pour répertorier les propriétés du projet, utilisez la commande get.**

```
hostname:shares home> get
aclinherit = restricted
```

```

        aclmode = discard
        atime = true
        checksum = fletcher4
        compression = off
        compressratio = 100
        copies = 1
        creation = Thu Oct 23 2009 17:30:55 GMT+0000 (UTC)
        mountpoint = /export
        quota = 0
        readonly = false
        recordsize = 128K
        reservation = 0
        rstchown = true
        secondarycache = all
        nbmand = false
        sharesmb = off
        sharenfs = on
        snapdir = hidden
        snaplabel = project1:share1
        vscan = false
    defaultuserquota = 0
    defaultgroupquota = 0
    encryption = off
    snaplabel =
    sharedav = off
    shareftp = off
    sharesftp = off
    sharetftp = off
    pool = Pool1
    canonical_name = Pool1/local/default
    default_group = other
    default_permissions = 700
    default_sparse = false
    default_user = nobody
    default_volblocksize = 8K
    default_volsize = 0
    space_data = 43.9K
    space_unused_res = 0
    space_unused_res_shares = 0
    space_snapshots = 0
    space_available = 12.0T
    space_total = 43.9K
    origin =
hostname:shares home>

```

4. **Pour modifier les propriétés du projet, utilisez la commande `set`. Les propriétés et les valeurs d'un projet sont décrites dans ["Propriétés des projets" à la page 377](#).**

Par exemple, pour activer `vscan` pour ce projet, entrez la commande suivante :

```
hostname:shares home >set vscan=true
```

5. **Saisissez `commit`.**

```
hostname:shares home> commit
```

▼ Modification du nom d'un projet (BUI)



Attention - La modification du nom d'un projet interrompra les opérations d'E/S du client actif.

1. **Déconnectez tout client actif connecté au projet.**
2. **Accédez à Partages > Projets.**
3. **Cliquez sur le nom de projet dans la liste des projets.**

4. **Entrez le nouveau nom du projet.**

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.

5. **Appuyez sur Entrée.**
6. **Cliquez sur OK pour confirmer.**

▼ Modification du nom d'un projet (CLI)



Attention - La modification du nom d'un projet interrompra les opérations d'E/S du client actif.

1. **Déconnectez tout client actif connecté au projet.**
2. **Accédez à shares.**

```
hostname:> shares
```

3. **Pour afficher les propriétés du projet, utilisez la commande `list`.**

```
hostname:shares> list
default
home
```

4. **Entrez `rename`, le nom actuel du projet et le nouveau nom de projet.**

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.

```
hostname:shares> rename home project1
```

5. Pour vérifier que le projet a été renommé, utilisez la commande `list`.

```
hostname:shares> list
default
project1
```

Rubriques connexes

- ["Propriétés des projets" à la page 377](#)

▼ Suppression d'un projet (BUI)



Attention - La suppression d'un projet détruit toutes les données du projet en supprimant ses systèmes de fichiers ou ses LUN.

1. Accédez à **Partages > Projets**.
2. Passez le curseur sur le projet que vous souhaitez supprimer et cliquez sur l'icône **Détruire** .
3. Cliquez sur **OK**.

▼ Suppression d'un projet (CLI)



Attention - La suppression d'un projet détruit toutes les données du projet en supprimant ses systèmes de fichiers ou ses LUN.

1. Accédez à **shares**.
2. Entrez `destroy` et le nom d'un projet.

```
hostname:> shares
```

```
hostname:shares> destroy home
```

3. Entrez `Y`.

```
This will destroy all data in "home"! Are you sure? (Y/N)
```

hostname:shares> Y

▼ Création d'un système de fichiers ou d'un LUN dans un projet (BUI)

Un système de fichiers ou un LUN créé au sein d'un projet hérite les propriétés de ce projet. Consultez la liste des propriétés standard pouvant être héritées dans la section "[Propriétés héritées](#)" à la page 364. Si le projet est chiffré, le système de fichiers ou le LUN créé en son sein est aussi chiffré.

Si vous ajoutez un système de fichiers ou un LUN à un projet personnalisé, le projet doit déjà exister. Pour créer un nouveau projet, reportez-vous à la section "[Création d'un projet \(BUI\)](#)" à la page 344.

1. **Accédez à Partages > Partages.**
2. **Sélectionnez Systèmes de fichiers ou LUN.**
3. **Cliquez sur l'icône d'ajout .**
4. **Renseignez les champs de la boîte de dialogue Créer un système de fichiers ou Créer un LUN.**
 - Pour un système de fichiers, sélectionnez un projet et entrez un nom.
 - Pour un LUN, sélectionnez un projet, entrez un nom et spécifiez la taille du volume.

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.
5. **Cliquez sur Appliquer.**

Rubriques connexes

- "[Propriétés des systèmes de fichiers](#)" à la page 384
- "[Propriétés du LUN](#)" à la page 394
- "[Propriétés héritées](#)" à la page 364
- "[Création d'un système de fichiers ou d'un LUN chiffré \(BUI\)](#)" à la page 574

▼ Création d'un système de fichiers ou d'un LUN dans un projet (CLI)

Un système de fichiers ou un LUN créé au sein d'un projet hérite les propriétés de ce projet. Consultez la liste des propriétés standard pouvant être héritées dans la section "[Propriétés](#)

héritées" à la page 364. Si le projet est chiffré, le système de fichiers ou le LUN créé en son sein est aussi chiffré.

Si vous ajoutez un système de fichiers ou un LUN à un projet personnalisé, le projet doit déjà exister. Pour créer un nouveau projet, reportez-vous à la section "[Création d'un projet \(CLI\)](#)" à la page 344.

1. Accédez à shares.

```
hostname:> shares
```

2. Entrez select et le nom de projet. Dans cet exemple, le projet default est sélectionné.

```
hostname:shares > select default
```

3. Entrez filesystem et le nom d'un système de fichiers, ou lun et le nom d'un LUN.

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux `_ - . :` sont autorisés.

L'exemple suivant crée un système de fichiers nommé `fs-1` dans le projet `default`.

```
hostname:shares default> filesystem fs-1
hostname:shares default/fs-1 (uncommitted)>
```

4. Si vous créez un LUN, entrez set volsize= et la taille du volume.

```
hostname:shares default/lun1 (uncommitted)> set volsize=2G
volsize = 2G (uncommitted)
```

5. Saisissez commit.

```
hostname:shares default/fs-1 (uncommitted)> commit
```

6. Entrez select et le nom d'un système de fichiers ou d'un LUN.

```
hostname:shares default> select fs-1
```

7. Répertoriez les propriétés du partage avec la commande get :

```
hostname:shares default/fs-1> get
      aclinherit = restricted (inherited)
      aclmode = discard (inherited)
      atime = true (inherited)
casesensitivity = mixed
      checksum = fletcher4 (inherited)
      compression = off (inherited)
      dedup = false (inherited)
      compressratio = 100
```

```

        copies = 1 (inherited)
        creation = Wed Apr 29 2015 17:57:18 GMT+0000(UTC)
        logbias = latency (inherited)
        mountpoint = /export/fs-1 (inherited)
        normalization = none
        quota = 0
        quota_snap = true
        readonly = false (inherited)
        recordsize = 128K (inherited)
        reservation = 0
        reservation_snap = true
        rstchown = true(inherited)
        secondarycache = all (inherited)
        shadow = none
        nbmand = false (inherited)
        sharesmb = off (inherited)
        sharenfs = on (inherited)
        snapdir = hidden (inherited)
        utf8only = false
        vscan = false (inherited)
        encryption = off (inherited)
        snaplabel =
        sharedav = off (inherited)
        shareftp = off (inherited)
        sharesftp = off (inherited)
        sharetftp = off (inherited)
        pool = pool_demo
        canonical_name = pool_demo/local/default/fs-1
        exported = true (inherited)
        nodeestroy = false
        maxblocksize = 1M (inherited)
        lz4supported = (inherited)
        space_data = 31K
        space_unused_res = 0
        space_snapshots = 0
        space_available = 29.4T
        space_total = 31K
        root_group = other
        root_permissions = 700
        root_user = nobody
        origin =
    
```

8. **Pour modifier les propriétés du système de fichiers ou du LUN, utilisez la commande `set`. Les propriétés sont décrites dans la section ["Propriétés des projets et partages" à la page 363](#).**

Par exemple, pour désactiver le protocole NFS du système de fichiers nommé fs-1, entrez :

```

hostname:shares default/fs-1> set sharenfs=off
sharenfs = off (uncommitted)
    
```

9. **Saisissez `commit`.**


```
hostname:shares default/fs-1> commit  
hostname:shares default/fs-1>
```

Rubriques connexes

- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés du LUN" à la page 394](#)
- ["Propriétés héritées" à la page 364](#)
- ["Création d'un système de fichiers ou d'un LUN chiffré \(CLI\)" à la page 574](#)

▼ Modification d'un système de fichiers ou d'un LUN (BUI)

Pour modifier les propriétés d'un système de fichiers ou d'un LUN individuel, suivez ces étapes.

1. **Accédez à Partages > Partages.**
2. **Sélectionnez Systèmes de fichiers ou LUN.**
3. **Passez le curseur sur le système de fichiers ou le LUN et cliquez sur l'icône Modifier  ou double-cliquez sur le système de fichiers ou le LUN à modifier.**
Les propriétés générales du système de fichiers ou du LUN sont affichées.
4. **Cliquez sur l'onglet Protocoles, Accès, Instantanés ou Réplication.**
5. **Modifiez les propriétés du système de fichiers ou du LUN avec les valeurs décrites dans les sections ["Propriétés des systèmes de fichiers" à la page 384](#) et ["Propriétés du LUN" à la page 394](#).**

Rubriques connexes

- ["Propriétés des projets et partages" à la page 363](#)

▼ Modification d'un système de fichiers ou d'un LUN (CLI)

Pour modifier les propriétés d'un système de fichiers ou d'un LUN individuel, suivez ces étapes.

1. **Accédez à shares.**


```
hostname:> shares
```
2. **Entrez `select` et le nom du projet qui contient le système de fichiers ou le LUN que vous souhaitez modifier.**

```
hostname:shares> select default
```

3. Entrez select et le nom d'un système de fichiers ou de LUN.

```
hostname:shares default> select fs-1
```

4. Répertoriez les propriétés du partage avec la commande get :

```
hostname:shares default/fs-1> get
aclinherit = restricted (inherited)
aclmode = discard (inherited)
atime = true (inherited)
casesensitivity = mixed
checksum = fletcher4 (inherited)
compression = off (inherited)
dedup = false (inherited)
compressratio = 100
copies = 1 (inherited)
creation = Wed Apr 29 2015 17:57:18 GMT+0000(UTC)
logbias = latency (inherited)
mountpoint = /export/fs-1 (inherited)
normalization = none
quota = 0
quota_snap = true
readonly = false (inherited)
recordsize = 128K (inherited)
reservation = 0
reservation_snap = true
rstchown = true(inherited)
secondarycache = all (inherited)
shadow = none
nbmand = false (inherited)
sharesmb = off (inherited)
sharenfs = on (inherited)
snapdir = hidden (inherited)
utf8only = false
vscan = false (inherited)
encryption = off (inherited)
snaplabel =
sharedav = off (inherited)
shareftp = off (inherited)
sharesftp = off (inherited)
sharetftp = off (inherited)
pool = pool_demo
canonical_name = pool_demo/local/default/fs-1
exported = true (inherited)
nodeestroy = false
maxblocksize = 1M (inherited)
space_data = 31K
space_unused_res = 0
space_snapshots = 0
space_available = 29.4T
space_total = 31K
```

```
root_group = other
root_permissions = 700
root_user = nobody
origin =
```

5. Utilisez la commande **set** pour modifier les propriétés du système de fichiers ou du LUN avec les valeurs décrites dans les sections "[Propriétés des systèmes de fichiers](#)" à la page 384 et "[Propriétés du LUN](#)" à la page 394.

Par exemple, pour désactiver le protocole NFS du système de fichiers nommé fs-1, entrez :

```
hostname:shares default/fs-1> set sharenfs=off
sharenfs = off (uncommitted)
```

6. Saisissez **commit**.

```
hostname:shares default/fs-1> commit
```

Rubriques connexes

- "[Propriétés des projets et partages](#)" à la page 363

▼ Modification du nom d'un système de fichiers ou d'un LUN (BUI)



Attention - La modification du nom d'un partage interrompra les opérations d'E/S du client actif.

1. Déconnectez tous les clients actifs connectés au système de fichiers ou au LUN que vous souhaitez renommer.
2. Accédez à **Partages > Partages**.
3. Sélectionnez **Systèmes de fichiers ou LUN**.
4. Cliquez sur le nom du système de fichiers ou du LUN dans la liste.
5. Entrez le nouveau nom du système de fichiers ou du LUN.
Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux `_` `-` `.` `:` sont autorisés.
6. Appuyez sur **Entrée**.
7. Cliquez sur **OK** pour confirmer.

Rubriques connexes

- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés du LUN" à la page 394](#)

▼ Modification du nom d'un système de fichiers ou d'un LUN (CLI)



Attention - La modification du nom d'un partage interrompra les opérations d'E/S du client actif.

1. **Déconnectez tous les clients actifs connectés au système de fichiers ou au LUN.**

2. **Accédez à shares.**

```
hostname:> shares
```

3. **Pour afficher les propriétés du projet, utilisez la commande `list`.**

```
hostname:shares>list
default
home
```

4. **Entrez `select` et le nom du projet qui contient le système de fichiers ou le LUN que vous souhaitez renommer.**

```
hostname:shares>select default
```

5. **Entrez `rename`, le nom actuel du système de fichiers ou du LUN et le nouveau nom du système de fichiers ou du LUN.**

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux `_` `-` `.` `:` sont autorisés.

```
hostname:shares default> rename fs-1 fs-2
```

Rubriques connexes

- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés du LUN" à la page 394](#)

▼ Déplacement d'un système de fichiers ou d'un LUN vers un autre projet (BUI)

Les systèmes de fichiers ou les LUN d'un projet hérite les propriétés de ce projet.

1. **Accédez à Partages > Partages.**
2. **Sélectionnez Systèmes de fichiers ou LUN.**
3. **Passez le curseur sur le système de fichiers ou le LUN et cliquez sur l'icône Déplacer .**
4. **Faites glisser le système de fichiers ou le LUN vers un autre projet sous Projets.**
Si le panneau Projet est réduit, il se développera automatiquement jusqu'à ce que le partage soit déposé dans un projet.

Rubriques connexes

- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés du LUN" à la page 394](#)

▼ Déplacement d'un système de fichiers ou d'un LUN vers un autre projet (CLI)

Les systèmes de fichiers ou les LUN d'un projet hérite les propriétés de ce projet.

1. **Accédez à shares et sélectionnez le projet qui contient le système de fichiers ou le LUN à déplacer.**

Dans cet exemple, le projet default contient le système de fichiers ou le LUN à déplacer.

```
hostname> shares
hostname:shares> select default
```

2. **Entrez move, le nom du système de fichiers ou du LUN à déplacer, et le nom du projet vers lequel vous souhaitez le déplacer.**

```
hostname:shares default> move foo home
```

Rubriques connexes

- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés du LUN" à la page 394](#)

▼ Suppression d'un système de fichiers ou d'un LUN (BUI)



Attention - La suppression d'un système de fichiers ou d'un LUN détruit toutes les données du partage et est irréversible.

1. **Accédez à Partages > Partages.**
2. **Sélectionnez Systèmes de fichiers ou LUN.**
3. **Passez le curseur sur le système de fichiers ou le LUN que vous souhaitez supprimer et cliquez sur l'icône Détruire .**
4. **Cliquez sur OK.**

Rubriques connexes

- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés du LUN" à la page 394](#)

▼ Suppression d'un système de fichiers ou d'un LUN (CLI)



Attention - La suppression d'un système de fichiers ou d'un LUN détruit toutes les données du partage et est irréversible.

1. **Accédez à shares.**
2. **Entrez `select` et le nom du projet qui contient le système de fichiers ou le LUN.**

```
hostname> shares
```

```
hostname:shares> select default
```

3. **Entrez `select` et le nom du système de fichiers ou du LUN.**

```
hostname:shares default>select fs-1
```

4. **Entrez `destroy`.**

```
hostname:shares default/fs-1> destroy
This will destroy all data in "fs-1"! Are you sure? (Y/N)
```

5. **Entrez `Y`.**

```
hostname:shares default> Y
```

Rubriques connexes

- ["Propriétés des systèmes de fichiers" à la page 384](#)

- ["Propriétés du LUN" à la page 394](#)

▼ Configuration des quotas d'utilisateurs ou de groupes (BUI)

Il est possible de définir des quotas pour un utilisateur ou un groupe au niveau du système de fichiers.

1. **Accédez à Partages > Partages et sélectionnez un projet ou un partage.**
2. **Cliquez sur l'onglet Général.**
3. **Dans la section Utilisation d'espace - Utilisateurs et groupes, sélectionnez Utilisateur, Groupe ou Utilisateur ou groupe dans le menu déroulant.**

Remarque - Un utilisateur qui ne consomme aucun espace sur le système de fichiers et qui n'a pas de quota défini ne figure pas dans la liste des utilisateurs actifs.

4. **Pour définir un quota au niveau du projet, sélectionnez une option parmi trois disponibles :**
 - **Aucun** : aucun quota n'est défini pour ce système de fichiers
 - **Par défaut** : applique le quota par défaut au niveau du projet. Si aucun quota par défaut n'est défini, aucun quota n'est appliqué à ce système de fichiers.
 - Cliquez sur le bouton radio, entrez un quota dans le champ de taille et sélectionnez une mesure.

5. **Cliquez sur APPLIQUER.**

Les propriétés de quotas de groupes et d'utilisateurs sont validées indépendamment des autres propriétés. Toutefois, une erreur de validation s'affiche uniquement si un groupe/utilisateur non valide ainsi qu'une autre propriété incorrecte sont entrés. Si vous corrigez une erreur et que vous appliquez les modifications, les messages d'erreur restants s'affichent.

Si vous voyez un message d'erreur indiquant qu'une propriété incorrecte a été saisie, il peut s'agir d'un utilisateur/groupe non valide et/ou d'une autre propriété incorrecte sur la page. Corrigez une propriété incorrecte et appliquez les modifications pour afficher les messages d'erreur restants.

Rubriques connexes

- ["Configuration des quotas d'utilisateurs ou de groupes" à la page 403](#)

▼ Configuration des quotas d'utilisateurs ou de groupes (CLI)

Il est possible de définir des quotas pour un utilisateur ou un groupe au niveau du système de fichiers.

1. **Accédez à shares, sélectionnez un projet, puis sélectionnez un partage, comme indiqué dans cet exemple.**

```
hostname:> shares select default select eschrock
```

2. **Entrez users, puis list pour afficher les utilisateurs actuels.**

```
hostname:shares default/eschrock> users
hostname:shares default/eschrock users> list
```

USER	NAME	USAGE	QUOTA	SOURCE
user-000	root	321K	-	-
user-001	ahl	9.94K	-	-
user-002	eschrock	20.0G	-	-

Remarque - Un utilisateur qui ne consomme aucun espace sur le système de fichiers et qui n'a pas de quota défini ne figure pas dans la liste des utilisateurs actifs.

3. **Entrez select et name= utilisateur.**

```
hostname:shares default/eschrock users> select name=eschrock
hostname:shares default/eschrock user-002> get
      name = eschrock
    unixname = eschrock
      unixid = 132651
    winname = (unset)
      winid = (unset)
      usage = 20.0G
      quota = (unset)
      source = (unset)
```

4. **Entrez quota= et une valeur. Entrez commit et done.**

Remarque - Pour effacer un quota, définissez la valeur sur '0'.

```
hostname:shares default/eschrock user-002> set quota=100G
      quota = 100G (uncommitted)
hostname:shares default/eschrock user-002> commit
hostname:shares default/eschrock user-002> done
```

5. **Pour définir un quota pour ce genre d'utilisateur ou de groupe, exécutez la commande quota puis définissez le nom et le quota.**

La colonne Source affiche "local" si le quota a été défini au niveau système de fichiers, "default" s'il a été défini au niveau projet ou "-" si aucun quota n'a été défini. Dans l'exemple suivant, le quota d'utilisateurs par défaut défini au niveau projet est de 50 Go.

Si un quota d'utilisateurs ou de groupes a été défini au niveau projet, cette procédure remplace cette valeur.

```
hostname:shares default/eschrock users> quota
hostname:shares default/eschrock users quota (uncommitted)> set name=bmc
name = bmc (uncommitted)
hostname:shares default/eschrock users quota (uncommitted)> set quota=default
quota = default (uncommitted)
hostname:shares default/eschrock users quota (uncommitted)> commit
hostname:shares default/eschrock users> list
```

USER	NAME	USAGE	QUOTA	SOURCE
user-000	root	321K	-	-
user-001	ahl	9.94K	-	-
user-002	eschrock	20.0G	100G	local
user-003	bmc	-	50G	default

Rubriques connexes

- ["Configuration des quotas d'utilisateurs ou de groupes" à la page 403](#)

A propos des pools de stockage, des projets et des partages

Oracle ZFS Storage Appliance gère le stockage physique au moyen d'un modèle de stockage de pools où tous les systèmes de fichiers et les LUN partagent un espace commun. Cette rubrique décrit l'organisation du stockage avec les pools de stockage, les projets et les partages.

Pools de stockage

L'appareil repose sur un système de fichiers ZFS, qui regroupe les périphériques de stockage sous-jacents en pools. Les systèmes de fichiers et les LUN, collectivement appelés partages, effectuent des allocations à partir de ce pool de stockage selon leurs besoins. Avant de créer des systèmes de fichiers ou des LUN, il faut configurer le stockage sur l'appareil. Une fois que le pool de stockage est configuré, il n'est pas nécessaire d'ajuster les systèmes de fichiers de manière statique, car ce comportement peut être appliqué à l'aide de quotas et de réservations.

Bien que plusieurs pools de stockage soient pris en charge, ce type de configuration est déconseillé car il présente de nombreux inconvénients décrits dans la section ["Configuration du stockage" à la page 84](#). L'utilisation de plusieurs pools est conseillée uniquement lorsque les caractéristiques de fiabilité ou de performances de deux profils sont radicalement différentes, par exemple si un pool est mis en miroir pour des bases de données et qu'un pool RAID-Z est mis en miroir pour les charges de travail de transmission.

Lorsque plusieurs pools sont actifs sur un même hôte, la BUI affiche une liste déroulante dans la barre de menu, qui vous permet de passer d'un pool à l'autre. Dans la CLI, le nom du pool en cours s'affiche entre parenthèses et peut être modifié en définissant la propriété 'pool'. Si un seul pool est configuré, ces commandes sont masquées. Quand plusieurs pools sont sélectionnés, le pool par défaut choisi par l'interface utilisateur est arbitraire. Toutes les opérations scriptées doivent donc s'assurer de définir le nom du pool de manière explicite avant de manipuler les partages.

Projets

Tous les systèmes de fichiers et LUN sont regroupés en projets. Un projet peut être considéré comme un groupe de cohérence qui définit un point de contrôle administratif commun pour la gestion des partages. Tous les partages au sein d'un projet peuvent avoir des paramètres en commun, et des quotas peuvent être appliqués au niveau du projet, ainsi qu'au niveau du partage. Les projets peuvent également être utilisés uniquement pour regrouper de manière logique des partages liés, de sorte que leurs attributs communs (par exemple, l'espace accumulé) soient accessibles à partir d'un point unique.

Par défaut, l'appareil crée un seul projet par défaut lorsqu'un pool de stockage est configuré initialement. Il est possible de créer tous les partages dans ce projet par défaut. Cela étant, dans les environnements de taille raisonnable, il est fortement recommandé de créer de projets supplémentaires, ne serait-ce que pour des raisons d'organisation.

Partages

Les partages désignent des systèmes de fichiers et des LUN exportés par des protocoles de données pris en charge vers des clients de l'appareil. Les systèmes de fichiers exportés sont accessibles via SMB, NFS, HTTP/WebDav et FTP. Les LUN exportent des volumes basés sur des blocs et sont accessibles via iSCSI ou Fibre Channel.

Le projet/partage est un identificateur unique d'un partage contenu dans un pool. Les projets dans un pool ne peuvent pas contenir de partages de même nom. Si vous tentez de nommer ou renommer un partage à l'aide d'un nom déjà utilisé, une erreur de point de montage se produit.

En plus des propriétés par défaut, vous pouvez configurer des partages et des projets avec autant de propriétés supplémentaires que souhaitez. Des types de base sont attribués à ces propriétés à des fins de validation et sont héritées, comme la plupart des propriétés standard. Les valeurs ne sont jamais utilisées par le logiciel, de quelque manière que ce soit, et sont réservées à l'utilisateur final. Le schéma de propriété est global au niveau du système, transversal pour tous les pools et synchronisé entre les pairs de cluster.

Rubriques connexes

- ["Gestion de l'espace pour les partages" à la page 400](#)
- ["Propriétés des projets et partages" à la page 363](#)
- ["Instantanés et clones" à la page 441](#)

Propriétés des projets et partages

Tous les projets et partages ont un nombre défini de propriétés associées qui peut être défini avec BUI ou CLI. Cliquez sur l'un des liens suivants pour obtenir la liste des noms et des descriptions de propriété :

- ["Propriétés des projets" à la page 377](#)
- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés du LUN" à la page 394](#)

Les propriétés de projet et de partage peuvent être des types suivants :

TABLEAU 104 Types de propriété de projet et de partage

Type de propriété	Description
Hérité	Les propriétés héritées, le type le plus commun de propriété, représentent la plupart des propriétés configurables de projet et de partage. Les partages qui font partie d'un projet peuvent avoir des propriétés héritées de paramètres locaux ou d'un projet parent. Par défaut, les partages héritent de toutes les propriétés du projet. Si une propriété est modifiée sur un projet, tous les partages qui héritent de cette propriété sont mis à jour en fonction de la nouvelle valeur. Une fois héritées, ces propriétés possèdent la même valeur que celle du projet parent, à l'exception des propriétés du point de montage et de SMB. Une fois héritées, ces propriétés concatènent les paramètres du projet avec leur propre nom de partage.
Lecture seule	Les propriétés en lecture seule représentent des statistiques relatives au projet et au partage et ne peuvent pas être modifiées. Les propriétés les plus courantes de ce type sont les statistiques d'utilisation de l'espace.
Gestion de l'espace	Les propriétés de gestion d'espace (quota et réservation) s'appliquent aux projets et aux partages mais ne sont pas héritées. Un projet avec un quota de 100 Go est appliqué à l'ensemble des partages mais chaque partage n'a pas de quota spécifique à moins qu'il ne soit défini de manière explicite.
Statique (moment de la création)	Les propriétés statiques sont spécifiées au moment de la création d'un système de fichiers ou de LUN mais ne peuvent pas être modifiées après la création du partage. Ces propriétés contrôlent les structures de données sur disque et comprennent des paramètres d'internationalisation, la sensibilité à la casse et la taille des blocs de volume.
Défaut projet	Les propriétés par défaut du projet sont définies pour le projet, mais n'affectent pas le projet en soi. Elles sont utilisées pour renseigner les paramètres initiaux lors de la création d'un système de fichiers ou de LUN et peuvent être très utiles lorsque les partages possèdent un ensemble de propriétés communes qui ne peuvent pas être héritées. La modification de ces propriétés n'affecte

Type de propriété	Description
	pas les partages existants et les propriétés peuvent être modifiées avant ou après la création du partage.
Système de fichiers local	Les propriétés locales du système de fichiers s'appliquent uniquement aux systèmes de fichiers et sont très utiles pour la gestion du répertoire racine du système de fichiers. Elles ne peuvent pas être définies sur les projets. Ces propriétés de contrôle d'accès peuvent également être définies par des opérations de protocole in-band.
LUN local	Les propriétés locales de LUN s'appliquent uniquement aux LUN et ne sont pas héritées. Elles ne peuvent pas être définies sur les projets.
Personnalisés	Les propriétés personnalisées sont des propriétés définies par l'utilisateur.

Propriétés héritées

Les propriétés héritées sont des propriétés standard qui peuvent être héritées du projet ou définies explicitement sur le partage. Dans la BUI, il est uniquement possible d'hériter de toutes les propriétés à la fois mais, dans la CLI, vous pouvez sélectionner les propriétés dont vous souhaitez hériter.

Les partages qui font partie d'un projet peuvent avoir des propriétés héritées de paramètres locaux ou d'un projet parent. Par défaut, les partages héritent de toutes les propriétés du projet. Si une propriété est modifiée sur un projet, tous les partages qui héritent de cette propriété sont mis à jour en fonction de la nouvelle valeur. Une fois héritées, ces propriétés possèdent la même valeur que celle du projet parent, à l'exception des propriétés du point de montage et de SMB. Une fois héritées, ces propriétés concatènent les paramètres du projet avec leur propre nom de partage.

Point de montage

La propriété de point de montage correspond à l'emplacement sur lequel le système de fichiers est monté. Elle est valide uniquement pour les systèmes de fichiers.

Les restrictions suivantes s'appliquent à la propriété mountpoint :

- Doit impérativement être sous /export
- Ne doit pas être en conflit avec un autre partage
- Ne doit pas être en conflit avec un autre partage sur le pair du cluster afin que le basculement s'effectue correctement

Lorsqu'il hérite de la propriété mountpoint, le nom actuel attribué à l'ensemble des données est ajouté au paramètre de point de montage du projet et les deux éléments sont liés par une barre oblique (/). Par exemple, si le projet "home" possède le paramètre mountpoint /export/home</tt>, "home/bob" hérite du point de montage /export/home/bob.

Les partages SMB sont exportés via leur nom de ressource et le point de montage n'est pas visible dans le protocole. Cependant, même les partages qui n'utilisent que le protocole SMB doivent avoir un point de montage unique valide sur l'appareil.

Les points de montage peuvent être imbriqués sous d'autres partages, bien qu'il existe certaines limitations. Pour plus d'informations, reportez-vous à la section "[Utilisation de l'espace de noms du système de fichiers](#)" à la page 404.

Lecture seule

La propriété de lecture seule détermine si le contenu du système de fichiers est en lecture seule. Elle est valide uniquement pour les systèmes de fichiers.

Il est impossible de modifier le contenu d'un système de fichiers en lecture, quels que soient les paramètres du protocole. Cependant, ce paramètre n'empêche pas de renommer, détruire ou modifier les propriétés du système de fichiers. De plus, quand un système de fichiers est en lecture seule, les propriétés du contrôle d'accès ne peuvent pas être modifiées car il faudrait pour cela modifier les attributs du répertoire racine du système de fichiers.

Mise à jour de l'heure d'accès à la lecture

La mise à jour de l'heure d'accès à la lecture détermine si l'heure d'accès aux fichiers a été mise à jour à la lecture de ce dernier. Elle est valide uniquement pour les systèmes de fichiers.

Les normes POSIX exigent que l'heure d'accès à un fichier indiquée corresponde exactement l'heure à laquelle le fichier a été lu pour la dernière fois. Il est donc nécessaire d'effectuer des opérations d'écriture sur le système de fichiers sous-jacent même dans le cas d'une charge de travail effectuée principalement en lecture seule. Pour les charges de travail consistant principalement à effectuer des lectures sur un très grand nombre de fichiers, la désactivation de cette propriété peut entraîner une amélioration des performances aux dépens du respect des normes. Ces mises à jour étant regroupées et se produisant de manière asynchrone, leurs effets ne devraient pas être visibles, sauf dans le cas d'une charge très importante.

Verrouillage obligatoire non bloquant

La propriété de verrouillage obligatoire non bloquant détermine si la sémantique de verrouillage SMB est appliquée sur la sémantique POSIX. Elle est valide uniquement pour les systèmes de fichiers.

Par défaut, les systèmes de fichiers implémentent le comportement d'un fichier en respectant les normes POSIX. Ces normes ne sont absolument pas compatibles avec le comportement requis par le protocole SMB. Pour les partages dans lesquels le protocole principal est SMB, cette option doit toujours être activée. Pour modifier cette propriété, tous les clients doivent être déconnectés puis reconnectés.

Suppression des doublons de données

La propriété de suppression des doublons de données détermine si les doublons de données sont supprimés. La suppression des doublons est une opération qui s'effectue à l'échelle du pool, basée sur le bloc et qui peut être activée par projet ou par partage.

Pour activer la suppression des doublons cochez la case Suppression des doublons de données dans l'écran des propriétés générales des projets ou des partages. Le taux de suppression des doublons apparaît dans la zone Utilisation de l'écran Tableau de bord de statut. Lorsque la propriété de suppression des doublons est activée, les données écrites sont saisies dans la table de suppression des doublons indexée par la somme de contrôle des données. La suppression des doublons force l'utilisation de la somme de contrôle SHA-256 à fortes propriétés cryptographiques. Les écritures consécutives identifient les doublons de données et seule la copie existante est conservée sur le disque. La suppression des doublons est possible uniquement entre les blocs de même taille et données écrites avec la même taille d'enregistrement. Pour obtenir de meilleurs résultats, utilisez la même taille d'enregistrement que celle de l'application qui traite les données. Pour la transmission de charges de travail, utilisez une grande taille d'enregistrement.

Si vos données ne contiennent aucun doublon, l'activation de la propriété Suppression des doublons de données ajoute du temps système (une somme de contrôle plus intensive au niveau de la CPU et des entrées dans la table de suppression de doublons sur disque) sans offrir aucun avantage. Si vos données contiennent des doublons, l'activation de la propriété Suppression des doublons de données permet à la fois d'économiser de l'espace en stockant une seule copie d'un bloc spécifique, quel que soit le nombre d'occurrences. La suppression des doublons a nécessairement un effet sur les performances puisque le coût du calcul de la somme de contrôle est plus élevé et que les métadonnées de la table de suppression de doublons doivent être accessibles et entretenues.

Notez que la suppression des doublons n'a aucune conséquence sur la taille calculée du partage mais influe sur la quantité d'espace de pool utilisée. Par exemple, si deux partages contiennent le même fichier de 1 Go, la taille indiquée de chaque fichier sera de 1 Go mais la taille totale du pool indiquée sera uniquement de 1 Go et le taux de suppression des doublons sera signalé comme 2x.

Par nature, la suppression des doublons nécessite la modification de la table de suppression des doublons lorsqu'un bloc est en cours d'écriture ou libéré. Si la table de suppression des données ne tient pas dans la DRAM, les écritures et l'espace libéré peuvent entraîner une forte activité de lecture aléatoire à des emplacements où il n'y en avait pas auparavant. Par conséquent, l'activation de cette propriété peut avoir de lourdes conséquences sur les performances. Par ailleurs, dans certains cas (en particulier pour la suppression de partages ou d'instantanés), la dégradation des performances due à l'activation de la suppression des doublons peut être ressentie dans la totalité du pool. En général, il n'est pas conseillé d'activer la suppression des doublons, sauf si vous savez qu'un partage compte un grand nombre de doublons et que la DRAM contient suffisamment d'espace pour que ces doublons de données ainsi que la table servant à les référencer y soient exportés.

Pour déterminer si la suppression des doublons a eu une incidence négative sur les performances, activez analyse avancée puis utilisez Analytics pour mesurer les "opérations ZFS DMU ventilées par type d'objet DMU" et recherchez un taux d'opérations DDT (opérations Data Duplication Table) plus élevé que celui des opérations ZFS. Si cela se produit, l'augmentation des E/S est plus utile à la table de suppression des doublons qu'aux E/S de fichier.

Pour utiliser la suppression des doublons avec chiffrement, n'oubliez pas que seul le standard AES accompagné du mode de chiffrement CCM est compatible avec la suppression des doublons. Pour plus d'informations, reportez-vous à la section "[Gestion des clés de chiffrement](#)" à la page 585.

Compression des données

La propriété de compression des données détermine si les données sont compressées avant d'être écrites sur le disque. Les partages peuvent éventuellement compresser les données avant de les écrire sur le pool de stockage. Cette propriété permet une meilleure utilisation de l'espace de stockage mais augmente l'utilisation de la CPU. Par défaut, aucune compression n'est effectuée. Si la compression ne produit pas un minimum d'économie d'espace, le disque n'est pas paramétré pour éviter les opérations de décompression inutiles lors de la lecture des données. Avant de choisir un algorithme de compression, nous vous recommandons d'effectuer tous les tests de performances nécessaires et de mesurer le taux de compression atteint.

Valeur BUI	Valeur CLI	Description
Désactivé	Désactivé	Aucune compression n'est effectuée.
LZJB (vitesse maximale)	lzjb	Codage à exécution simple qui fonctionne uniquement pour les entrées simples mais consomme peu de CPU.
GZIP-2 (rapide)	gzip-2	Version allégée de l'algorithme de compression gzip.
GZIP (défaut)	gzip	Algorithme de compression gzip standard
GZIP-9 (compression maximale)	gzip-9	Compression la plus élevée possible à l'aide de l'algorithme gzip. Elle consomme une grande quantité de CPU et permet parfois d'obtenir seulement des économies minimales.

Somme de contrôle

La propriété de somme de contrôle détermine la somme de contrôle utilisée pour les blocs de données. Sur l'appareil, toutes les données du disque font l'objet d'un contrôle par totalisation d'une façon qui permet d'éviter les problèmes habituels (en particulier les lectures et les

écritures fantômes). Cela permet au système de détecter les données non valides renvoyées par les périphériques. La somme de contrôle par défaut (fletcher4) est suffisante pour une opération classique, toutefois les utilisateurs peuvent augmenter la force de la somme de contrôle bien que cela augmente la charge de la CPU. Les métadonnées font toujours l'objet d'un contrôle par totalisation à l'aide du même algorithme, de sorte que cela n'affecte que les données utilisateur (fichiers ou blocs LUN).

Valeur BUI	Valeur CLI	Description
Fletcher 2 (Hérité)	fletcher2	Somme de contrôle fletcher 16 bits
Fletcher 4 (Standard)	fletcher4	Somme de contrôle fletcher 32 bits
SHA-256 (Sécurité renforcée)	sha256	Somme de contrôle SHA-256
SHA-256-MAC	sha256mac	

Utilisation du périphérique de cache

La propriété d'utilisation du périphérique de cache détermine si les périphériques de cache sont utilisés pour le partage. Par défaut, tous les ensembles de données utilisent les périphériques de cache présents sur le système. Les périphériques de cache sont configurés dans le cadre du pool de stockage et fournissent une couche supplémentaire de mise en cache pour permettre un accès à plusieurs niveaux plus rapide. Pour plus d'informations sur les périphériques de cache, reportez-vous à la section ["Configuration du stockage" à la page 84](#). Cette propriété ne tient pas compte du fait qu'il existe ou non des périphériques de cache configurés dans le pool de stockage. Par exemple, il est possible que cette propriété soit définie sur "all" même si aucun périphérique de cache n'est présent. Si, dans le futur, vous ajoutez ce type de périphérique, le partage tire automatiquement parti de cette amélioration des performances. Cette propriété n'affecte pas l'utilisation du cache principal (DRAM).

Valeur BUI	Valeur CLI	Description
Toutes les données et métadonnées	all	Tous les fichiers classiques ou les données de LUN ainsi que toutes les métadonnées sont mis en cache.
Métadonnées uniquement	metadata	Seules les métadonnées sont conservées sur les périphériques de cache. Cela permet de parcourir rapidement les structures de répertoires. Toutefois, la récupération du contenu des fichiers peut nécessiter la lecture à partir des périphériques de données.
Ne pas utiliser de périphérique de cache	none	Aucune donnée du partage n'est mise en cache sur le périphérique de cache. Les données sont seulement mises en cache dans le cache principal ou stockées sur les périphériques de données.

Décalage d'écriture synchrone

La propriété de décalage d'écriture synchrone détermine le comportement lors du traitement d'écritures synchrones. Par défaut, le système optimise les écritures synchrones pour la latence, ce qui permet au périphérique de journal de fournir des réponses plus rapidement. Dans un environnement comptant plusieurs systèmes de fichiers non joints, cela peut entraîner des conflits d'utilisation sur les périphériques de journal et ainsi, augmenter la latence pour l'ensemble des consommateurs. Même quand plusieurs systèmes de fichiers nécessitent une sémantique synchrone, il peut arriver que certains systèmes de fichiers soient plus sensibles que d'autres à la latence.

Par exemple, il arrive souvent qu'une base de données ait un journal distinct. Le journal est très sensible à la latence. La base de données nécessite elle aussi une sémantique synchrone, mais elle consomme davantage de bande passante et n'est pas sensible à la latence. Dans cet environnement, vous pouvez définir cette propriété sur "débit" dans la base de données principale et laisser le système de fichiers de journal sur "latence" pour améliorer les performances de manière significative. Ce paramètre change de comportement même si aucun périphérique de journal n'est présent (les conséquences étant moins graves dans ce cas).

Le paramètre de décalage d'écriture synchrone peut être contourné par Oracle Intelligent Storage Protocol. Au lieu d'utiliser le décalage d'écriture dans le système de fichier, Oracle Intelligent Storage Protocol peut utiliser la valeur de décalage d'écriture fournie par le client Oracle Database NFSv4. La valeur de décalage d'écriture envoyée par le client Oracle Database NFSv4 est uniquement utilisée pour cette requête d'écriture.

Valeur BUI	Valeur CLI	Description
Latence	latency	Les écritures synchrones sont optimisées pour la latence, ce qui permet d'utiliser les périphériques de journal dédiés, le cas échéant.
Débit	throughput	Les écritures synchrones sont optimisées pour le débit. Les données sont écrites dans les disques de données principaux (et non dans les périphériques de journal) et les écritures sont effectuées de manière à être optimisées pour la totalité de la bande passante du système.

Taille des enregistrements de la base de données

La propriété de taille des enregistrements de la base de données spécifie une taille de bloc suggérée pour les fichiers du système de fichiers. Cette propriété est valide uniquement pour les systèmes de fichiers et s'utilise pour les charges de travail de base de données accédant à des fichiers résidant dans des enregistrements à taille fixe. Le système ajuste automatiquement les tailles en fonction d'algorithmes internes optimisés pour les schémas d'accès classiques. Pour

les bases de données générant des fichiers volumineux mais accédant uniquement à certains fragments de manière aléatoire, ces algorithmes peuvent se révéler inadaptés. La définition d'une taille d'enregistrement supérieure ou égale à la taille d'enregistrement de la base de données peut améliorer les performances du système de manière significative. Il est vivement déconseillé d'utiliser cette propriété pour les systèmes de fichiers à usage générique. En outre, elle peut affecter les performances du système.

La taille d'enregistrement par défaut est de 128 Ko. La taille spécifiée doit être une puissance de 2 supérieure ou égale à 512 octets et inférieure ou égale à 1 Mo. La modification de la taille d'enregistrement du système de fichiers affecte uniquement les fichiers créés ultérieurement : les fichiers existants et les données reçues ne sont pas touchés. Si des tailles de blocs supérieures à 128 Ko sont utilisées pour les projets et les partages, la réplication de ces projets ou partages sur des systèmes qui ne prennent pas en charge les tailles de blocs importantes échouera.

Le paramètre de taille des enregistrements de la base de données peut être contourné par le protocole OISP. Au lieu d'utiliser la taille des enregistrements dans le système de fichier, Oracle Intelligent Storage Protocol peut utiliser la valeur de taille de bloc fourni par le client Oracle Database NFSv4. La taille de bloc fournie par le client Oracle Database NFSv4 peut uniquement être appliquée lors de la création de nouveaux fichiers ou d'un nouveau tableau de base de données. Les tailles de bloc des fichiers et tableaux existants ne seront pas modifiées. Pour plus d'informations, reportez-vous à la section "[Protocole OISP \(Oracle Intelligent Storage Protocol\)](#)" à la page 645.

Réplication supplémentaire

La propriété de réplication supplémentaire contrôle le nombre de copies stockées dans chaque bloc, indépendamment de toute redondance du pool de stockage. Les métadonnées sont toujours stockées en plusieurs exemplaires, mais cette propriété autorise l'application de ce comportement aux blocs de données. Le pool de stockage tente de stocker ces blocs supplémentaires sur d'autres périphériques, mais la réussite de cette opération n'est pas garantie. De plus, un pool de stockage ne peut pas être importé en cas de perte de la totalité d'un périphérique logique (largeur de bande RAID, pair mis en miroir, etc.). Cette propriété ne remplace pas une réplication adaptée dans le pool de stockage mais permet de rassurer les administrateurs inquiets.

Analyse antivirus

La propriété d'analyse antivirus détermine si le système de fichiers est analysé pour détecter d'éventuels virus. Elle est valide uniquement pour les systèmes de fichiers. Le paramétrage de cette propriété est indépendant de l'état du service d'analyse de virus. Même si le service Analyse antivirus est activé, l'analyse du système de fichiers doit être explicitement activée à l'aide de cette propriété. De même, l'analyse antivirus peut être activée pour un partage spécifique même si le service est désactivé. Pour plus d'informations sur la configuration de l'analyse antivirus, reportez-vous à la section [Analyse antivirus](#).

Empêcher la destruction

Lorsque cette propriété est définie, les partages ou les projets ne peuvent pas être détruits. Cela comprend la destruction d'un partage par le biais de clones dépendants, la destruction d'un partage contenu dans un projet ou la destruction d'un package de réplication. Cependant, cela ne concerne pas les partages détruits par le biais des mises à jour de réplication. Si un partage est détruit sur un appareil qui est la source de la réplication, le partage correspondant sur la cible sera détruit, même si cette propriété est activée. Pour détruire un partage, cette propriété doit d'abord être explicitement désactivée au cours d'une étape distincte. Par défaut, cette propriété est désactivée.

Restreindre les modifications de propriété

Par défaut, la propriété des fichiers ne peut pas être modifiée sauf par un utilisateur root (sur un client adapté ayant l'option d'export root activée). Cette propriété peut être désactivée pour un projet ou un système de fichiers spécifique en désactivant cette propriété. Lorsque que cette propriété est désactivée, la propriété de fichier peut être modifiée par le propriétaire du fichier ou du répertoire, ce qui permet aux utilisateurs "d'abandonner" leurs propres fichiers. Lorsque la propriété est modifiée, tous les bits setuid ou setgid sont éliminés, afin d'empêcher les utilisateurs d'augmenter leurs privilèges par cette opération.

Propriétés locales du LUN

Ces propriétés s'appliquent uniquement aux LUN et ne sont pas héritées. Elles ne peuvent pas être définies sur les projets.

Taille de volume

La propriété de taille de volume détermine la taille logique du LUN au moment de l'exportation via iSCSI. Cette propriété contrôle la taille du LUN. Par défaut, les LUN réservent suffisamment d'espace pour remplir la totalité du volume. Si vous modifiez la taille d'un LUN en cours d'exportation vers les clients, cela peut produire des résultats indéfinis. Cela peut imposer la reconnexion des clients et/ou endommager les données sur le système de fichiers situé sur le LUN. Avant d'effectuer cette opération, vérifiez les pratiques recommandées pour votre client iSCSI spécifique.

Provisionnement fin

La propriété de provisionnement fin détermine si l'espace est réservé pour le volume. Par défaut, un LUN réserve exactement la quantité d'espace dont elle a besoin pour remplir la totalité du volume. Cela permet de s'assurer que les clients ne produiront pas d'erreurs en raison

d'un manque d'espace à des moments inopportuns. Cette propriété admet que la taille du volume puisse dépasser la quantité d'espace disponible. Si cette propriété est définie, le LUN consomme uniquement l'espace qui a été écrit dans le LUN. Cette propriété autorise le provisionnement fin des LUN. Cela étant, la plupart des systèmes de fichiers ne s'attendent pas à "manquer d'espace" sur les périphériques sous-jacents et, si le partage est saturé, cela peut entraîner une instabilité et/ou endommager des données sur les clients.

Si cette propriété n'est pas définie, la taille du volume a un comportement similaire à une réservation, sauf en ce qui concerne les instantanés. Toutefois, elle présente les mêmes problèmes que la réservation, comme l'impossibilité de prendre un instantané si ce dernier peut, en théorie, diverger au point de dépasser la quantité d'espace disponible. Pour plus d'informations, consultez les propriétés de réservation à la section "[Gestion de l'espace du système de fichiers et du projet](#)" à la page 402.

Taille de bloc des volumes

La propriété de taille de bloc des volumes définit la taille de bloc natif des LUN. Il peut s'agir de n'importe quelle puissance de 2 allant de 512 octets à 1 Mo et la valeur par défaut est 8 Ko. Cette propriété est statique. Elle est définie lors de la création du LUN et ne peut pas être modifiée.

Autres propriétés

Les propriétés suivantes sont disponibles : Défaut projet, Système de fichiers local, Gestion de l'espace, Lecture seule et Personnalisées.

Défaut projet

Les propriétés par défaut du projet sont définies pour le projet, mais n'affectent pas le projet en soi. Elles sont utilisées pour renseigner les paramètres initiaux lors de la création d'un système de fichiers ou de LUN et peuvent être très utiles lorsque les partages possèdent un ensemble de propriétés communes qui ne peuvent pas être héritées. La modification de ces propriétés n'affecte pas les partages existants et les propriétés peuvent être modifiées avant ou après la création du partage.

Système de fichiers local

Les propriétés locales du système de fichiers s'appliquent uniquement aux systèmes de fichiers et sont très utiles pour la gestion du répertoire racine du système de fichiers. Elles ne sont pas héritées et ne peuvent pas être définies sur les projets. Ces propriétés de contrôle d'accès peuvent également être définies par des opérations de protocole in-band.

Gestion de l'espace

Les propriétés de gestion d'espace (quota et réservation) s'appliquent aux projets et aux partages mais ne sont pas héritées. Un projet avec un quota de 100 Go est appliqué à l'ensemble des partages mais chaque partage n'a pas de quota spécifique à moins qu'il ne soit défini de manière explicite.

Lecture seule

Les propriétés en lecture seule représentent des statistiques relatives au projet et au partage et ne peuvent pas être modifiées. Les propriétés les plus courantes de ce type sont les statistiques d'utilisation de l'espace.

Personnalisé

Les propriétés personnalisées sont définies par l'utilisateur avec un schéma. Pour plus d'informations, voir la section ["Utilisation des schémas" à la page 427](#).

Propriétés statiques

Les propriétés statiques sont spécifiées au moment de la création d'un système de fichiers ou de LUN mais ne peuvent pas être modifiées après la création du partage. Ces propriétés contrôlent les structures de données sur disque et comprennent des paramètres d'internationalisation, la sensibilité à la casse et la taille des blocs de volume.

Dans la BUI, les propriétés statiques peuvent être consultées du côté gauche de l'interface lors de la modification d'un système de fichiers ou d'un LUN.

TABLEAU 105 Propriétés statiques d'un système de fichiers et d'un LUN

Nom dans la BUI	Nom dans la CLI	Description
Date de création	creation	Indique la date de création.
Taux de compression	compressratio	Taux de compression en cours pour le système de fichiers ou le LUN, qui est un produit de l'algorithme de compression. Pour plus d'informations, reportez-vous la section "Taux de compression" à la page 374 .
Sensibilité à la casse	casesensitivity	La propriété de sensibilité à la casse détermine si les recherches de répertoire sont sensibles ou non à la casse. Pour plus d'informations, reportez-vous à la section "Sensibilité à la casse" à la page 374 .
Rejeter non UTF-8	utf8only	Cette propriété applique le codage UTF-8 à tous les fichiers et répertoires. Pour plus

Nom dans la BUI	Nom dans la CLI	Description
		d'informations, reportez-vous à la section "Rejeter non UTF-8" à la page 375 .
Normalisation	normalization	La propriété de normalisation contrôle le type de normalisation Unicode exécuté sur les systèmes de fichiers et les répertoires, le cas échéant. La norme Unicode prend en charge les noms logiques représentés par différents codages. Pour plus d'informations, reportez-vous à la section "Normalisation" à la page 376 .
Taille de bloc des volumes (LUN uniquement)	volblocksize	La propriété de taille de bloc des volumes définit la taille de bloc natif des LUN. Pour plus d'informations, reportez-vous à la section "Taille de bloc des volumes" à la page 376 .
Origine	origin	Affiche le nom de l'instantané à partir duquel le clonage a été effectué. Pour plus d'informations, reportez-vous à la section "Origine" à la page 376 .
Source de migration de données (systèmes de fichiers uniquement)	shadow	Emplacement de la source si le système de fichiers masque activement un système de fichiers existant soit en local, soit sur NFS. Pour plus d'informations, reportez-vous à la section "Source de migration de données" à la page 377 .

Taux de compression

Si la compression est activée, cette propriété permet d'afficher le taux de compression atteint pour le partage. Cette valeur est exprimée sous forme de multiplicateur. Par exemple, une compression de 2x indique que les données consomment deux fois moins d'espace que le contenu non compressé. Pour plus d'informations sur la sélection d'un algorithme de compression, reportez-vous au paragraphe "Compression de données" dans la section ["Propriétés héritées" à la page 364](#).

Sensibilité à la casse

La propriété de sensibilité à la casse détermine si les recherches de répertoire sont sensibles ou non à la casse. Le système prend en charge les options suivantes :

Valeur BUI	Valeur CLI	Description
Mixte	mixed	La sensibilité à la casse dépend du protocole utilisé. Pour les protocoles NFS, FTP et HTTP, les recherches sont sensibles à la casse. Pour SMB, les recherches ne sont pas sensibles à la casse. Il s'agit du paramétrage par défaut. Ce mode permet de classer par ordre de priorité les

Valeur BUI	Valeur CLI	Description
		différents protocoles en fonction de la cohérence entre protocoles. Lorsque vous utilisez ce mode, vous pouvez créer des fichiers qui varient en fonction des protocoles sensibles à la casse, mais cela génère un conflit lors d'une tentative d'accès via le serveur SMB. Dans ce cas, le serveur SMB crée une version "endommagée" de ces conflits qui identifient de manière unique le nom du fichier.
Non sensible	insensitive	Aucune recherche n'est sensible à la casse, même parmi les protocoles tels que NFS qui sont généralement sensibles à la casse. Cela peut entraîner une confusion pour les clients de ces protocoles mais permet d'empêcher les clients de créer des conflits de nom, ce qui provoquerait l'utilisation de noms endommagés sur SMB. Ce paramètre doit être utilisé uniquement lorsque SMB est le protocole principal, que les autres protocoles sont considérés comme secondaires et que la conformité aux normes exigées n'est pas un problème.
Confidentiel	sensitive	Toutes les recherches sont sensibles à la casse, même sur les protocoles SMB qui ne sont généralement pas sensibles à la casse. En général, ce paramètre ne doit pas être utilisé car le serveur SMB peut rencontrer des conflits de nom en raison des noms endommagés. De plus, cela peut entraîner un comportement inhabituel des applications Windows.

Rejeter non UTF-8

Cette propriété applique le codage UTF-8 à tous les fichiers et répertoires. Lorsque ce paramètre est défini, il est impossible de créer un fichier ou un répertoire avec un codage UTF-8 non valide. Cela concerne uniquement NFSv3, dont le codage n'est pas défini par le paramétrage par défaut. Le protocole NFSv4 utilise toujours le codage UTF-8 et SMB négocie le codage approprié. Normalement, ce paramètre doit être "activé", faute de quoi le serveur SMB (qui doit notamment connaître le codage afin d'effectuer des comparaisons sensibles à la casse) ne peut pas décoder les noms de fichiers créés ayant un codage UTF-8 non valide. Ce paramètre doit être "désactivé" uniquement dans les déploiements NFSv3 préexistants dans lesquels les clients sont configurés pour utiliser plusieurs codages. L'activation de SMB ou NFSv4 lorsque cette propriété est "désactivée" produit des résultats inconnus si un client NFSv3

crée un fichier ou un répertoire qui ne représente pas un codage UTF-8 valide. Il faut "activer" cette propriété si la propriété de normalisation est définie sur une autre valeur que "none".

Normalisation

La propriété de normalisation contrôle le type de normalisation Unicode exécuté sur les systèmes de fichiers et les répertoires, le cas échéant. La norme Unicode prend en charge les noms logiques représentés par différents codages. Sans normalisation, le nom stocké sur disque est différent et les recherches utilisant une des formes alternatives peuvent échouer en fonction de la technique utilisée pour créer le fichier et la manière dont on y accède. Si cette propriété est définie sur une valeur différente de "none" (valeur par défaut), il faut "activer" la propriété "Rejeter non UTF-8".

Valeur BUI	Valeur CLI	Description
Aucune	none	Aucune normalisation n'est effectuée.
Form C	formC	<i>NFC (Normalization Form Canonical Composition)</i> : les caractères sont décomposés puis réordonnés par équivalence canonique.
Form D	formD	<i>NFD (Normalization Form Canonical Decomposition)</i> : les caractères sont décomposés par équivalence canonique.
Form KC	formKC	<i>NFKC (Normalization Form Compatibility Composition)</i> : les caractères sont décomposés par équivalence de compatibilité et réordonnés par équivalence canonique.
Form KD	formKD	<i>Normalization Form Compatibility Decomposition (NFKD)</i> : les caractères sont décomposés par équivalence de compatibilité.

Taille de bloc des volumes

La propriété de taille de bloc des volumes définit la taille de bloc natif des LUN. Il peut s'agir de n'importe quelle puissance de 2 allant de 512 octets à 1 Mo et la valeur par défaut est 8 Ko.

Origine

Si c'est un clone, cette propriété correspond au nom de l'instantané à partir duquel le clonage a été effectué.

Source de migration de données

Si cette propriété est définie, ce système de fichiers masque activement un système de fichiers existant soit en local, soit sur NFS. Pour plus d'informations sur la migration de données, reportez-vous à la section ["Migration shadow" à la page 431](#).

Propriétés des projets

Remarque - Dans la CLI, utilisez la commande `get` pour afficher une liste de toutes les propriétés.

Utilisez la commande `list` pour répertorier tous les enfants.

TABLEAU 106 Propriétés des projets

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Créer un projet	Nom	project	Statique	Définit le nom du projet.
	Chiffrement	encryption	Hérité	Définit le type de chiffrement.
	Touche	key	Hérité	Définit une clé locale ou OKM spécifique.
	Nom clé	keyname	Statique	Identifie la clé.
Général - Utilisation de l'espace - Données	Quota	quota	Gestion de l'espace	Définit l'espace maximal pouvant être utilisé par une entité spécifique.
	Réservation	reservation	Gestion de l'espace	Représente un espace garanti pouvant être utilisé par une entité spécifique.
Général - Utilisation de l'espace - Utilisateurs et groupes	Quota de l'utilisateur par défaut	defaultuserquota	Gestion de l'espace	Définit l'espace maximal pouvant être utilisé par l'utilisateur.
	Quota du groupe par défaut	defaultgroupquota	Gestion de l'espace	Définit l'espace maximal pouvant être utilisé par le groupe.
	Utilisateur et groupe	users / groups	--	Spécifie les utilisateurs et/ou les groupes.
	Utilisation	--	Gestion de l'espace	Indique la quantité de données utilisée

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Propriétés héritées				par les utilisateurs et/ou les groupes.
	Point de montage	mountpoint	Hérité	Contrôle le chemin servant à exporter les systèmes de fichiers. Pour plus d'informations, reportez-vous à la section " Point de montage " à la page 364.
	Lecture seule	readonly	Hérité	Cette propriété détermine si le contenu du système de fichiers est en lecture seule. Pour plus d'informations, reportez-vous à la section " Lecture seule " à la page 365.
	Mise à jour de l'heure d'accès à la lecture	atime	Hérité	Cette propriété détermine si l'heure d'accès aux fichiers a été mise à jour à la lecture de ce dernier. Pour plus d'informations, reportez-vous à la section " Mise à jour de l'heure d'accès à la lecture " à la page 365.
	Verrouillage obligatoire non bloquant	nbmand	hérité	Cette propriété détermine si la sémantique de verrouillage SMB est appliquée sur la sémantique POSIX. Pour plus d'informations, reportez-vous à la section " Verrouillage obligatoire non bloquant " à la page 365.
	Suppression des doublons de données (avertissement)	dedup	Hérité	Cette propriété détermine si les doublons de données sont supprimés. Pour plus d'informations, reportez-vous à la section " Suppression des doublons de données " à la page 366.
	Compression des données	compression	Hérité	Cette propriété contrôle que les

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				données soient bien compressées avant d'être écrites sur le disque. Pour plus d'informations, reportez-vous à la section "Compression des données" à la page 367.
	Somme de contrôle	checksum	Hérité	Cette propriété détermine la somme de contrôle utilisée pour les blocs de données. Pour plus d'informations, reportez-vous à la section "Somme de contrôle" à la page 367.
	Utilisation du périphérique de cache	secondarycache	Hérité	Cette propriété vérifie que des périphériques de cache sont utilisés pour le partage. Pour plus d'informations, reportez-vous à la section "Utilisation du périphérique de cache" à la page 368.
	Décalage d'écriture synchrone	logbias	Hérité	Contrôle le comportement lors du traitement d'écritures synchrones. Pour plus d'informations, reportez-vous à la section "Décalage d'écriture synchrone" à la page 369.
	Taille des enregistrements de la base de données	recordsize	Hérité	Spécifie une taille de bloc suggérée pour les fichiers du système de fichiers. Pour plus d'informations, reportez-vous à la section "Taille des enregistrements de la base de données" à la page 369.
	Réplication supplémentaire	copies	Hérité	Cette propriété contrôle le nombre de copies stockées dans chaque bloc,

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				indépendamment de toute redondance du pool de stockage. Pour plus d'informations, reportez-vous à la section " Réplication supplémentaire " à la page 370.
	Analyse antivirus	vscan	Hérité	Cette propriété détermine si un système de fichiers est analysé pour détecter d'éventuels virus. Pour plus d'informations, reportez-vous à la section " Analyse antivirus " à la page 370.
	Empêcher la destruction	nodestroy	Hérité	Lorsque cette option est définie, elle empêche la destruction des partages et des projets. Pour plus d'informations, reportez-vous à la section " Empêcher la destruction " à la page 371.
	Restreindre les modifications de propriété	rstchown	Hérité	Contrôle la propriété et peut être désactivée par système de fichiers ou par projet. Pour plus d'informations, reportez-vous à la section " Restreindre les modifications de propriété " à la page 371.
Général - Propriétés personnalisées	Schéma	custom	--	Peuvent être ajoutées pour lier les balises définies par les utilisateurs aux projets et aux partages. Pour plus d'informations, reportez-vous à la section " Propriétés de schéma " à la page 429.
Général - Paramètres par défaut - Systèmes de fichiers	Utilisateur	default_user	Valeur par défaut	Spécifie un ID ou un nom d'utilisateur.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
	Groupe	default_group	Valeur par défaut	Spécifie un ID ou un nom de groupe.
	Autorisations	default_permissions	Valeur par défaut	Définit les autorisations par défaut du système de fichiers.
Général - Paramètres par défaut - LUN	Taille de volume	default_volsize	LUN uniquement, valeur par défaut	Affiche la taille de volume et l'unité de mesure maximales. Pour plus d'informations, reportez-vous à la section "Taille de volume" à la page 371.
	Provisionnement fin	default_sparse	LUN uniquement, valeur par défaut	Indique uniquement l'espace physique utilisé par les données lorsque l'option est sélectionnée. Pour plus d'informations, reportez-vous à la section "Provisionnement fin" à la page 371.
	Taille de bloc des volumes	default_volblocksize	Valeur par défaut	Affiche la taille de bloc natif des LUN, qui peut être définie de 512 octets à 1 Mo (8 Ko par défaut). Pour plus d'informations, reportez-vous à la section "Taille de bloc des volumes" à la page 372.
Protocoles - NFS	NFS	sharenfs	Hérité	Les paramètres et valeurs de la propriété de protocole NFS sont décrits à la section "Propriétés de protocole NFS" à la page 408.
Protocoles - Exceptions NFS	Des exceptions à l'ensemble des modes de partage peuvent être définies pour les clients ou les collections de clients. Pour plus d'informations, reportez-vous à la section "Exceptions du mode de partage NFS" à la page 409.			
Protocoles - SMB	SMB	sharesmb	Hérité	Les paramètres et valeurs de la propriété de protocole SMB sont décrits à la section

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
"Propriétés de protocole SMB" à la page 414.				
Protocoles - Exceptions SMB	Des exceptions à l'ensemble des modes de partage peuvent être définies pour les clients ou les collections de clients. Reportez-vous à la section "Exceptions du mode de partage du protocole SMB" à la page 416.			
Protocoles - HTTP (hériter du projet)	Mode de partage	sharedav	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".
Protocoles - FTP (hériter du projet)	Mode de partage	shareftp	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".
Protocoles - SFTP (hériter du projet)	Mode de partage	sharesftp	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".
Protocoles - TFTP (hériter du projet)	Mode de partage	sharetftp	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".
Accès	Comportement ACL en cas de changement de mode	aclmode	Hérité	Contrôle la façon dont une demande de modification de mode interagit avec une ACL existante.
	Comportement d'héritage ACL	aclinherit	Hérité	Détermine comment un nouveau fichier ou répertoire hérite des paramètres ACL existants d'un répertoire parent.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Propriétés des instantanés	.zfs/visibilité de l'instantané	snapdir	Hérité	Détermine si les instantanés de système de fichiers sont accessibles par le biais des protocoles de données à l'emplacement <command>. zfs/snapshot</command> à la racine du système de fichiers.
	Etiquette d'instantané planifié	snaplabel	Hérité	Ajoute une étiquette définie par l'utilisateur à chaque instantané planifié et est vide par défaut.
Instantanés - Instantanés	Nom	snapshot name	--	Spécifie le nom de l'instantané.
	Création	creation	--	Spécifie la date et heure de création de l'instantané.
	Unique	space_unique	--	Indique la quantité d'espace unique utilisée par l'instantané.
	Total	space_data	--	Indique la quantité d'espace totale référencée par l'instantané.
Instantanés - Programmmations	Fréquence	frequency	Moment de la création	Indique la fréquence de prise des instantanés.
	Conserver au plus	keep	Moment de la création	Cette propriété contrôle la stratégie de conservation des instantanés.
Réplication (hériter du projet)/Création de nouvelles actions	Cible	cible	Hérité	Identifie le système cible de la réplication.
	Pool	pool	Hérité	Spécifie le pool de stockage sur la cible où le projet sera répliqué.
	Exporter le chemin de données	export_path	Hérité	Indique le chemin d'exportation de données.
	Limite de la bande passante	max_bandwidth	Hérité	Spécifie une vitesse maximale pour

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				cette mise à jour de réplication (en termes de quantités de données transférées chaque seconde sur le réseau).
	Activer le chiffrement SSL	use_ssl	Hérité	Détermine si les données doivent être chiffrées en simultané avec SSL.
	Disable compression	--	Hérité	Détermine si la compression est activée ou désactivée.
	Inclure l'instantané	include_snaps	Hérité	Détermine si les mises à jour de réplication comprennent des instantanés de non-réplication.
	Conserver les instantanés utilisateurs sur la cible	retain_user_snaps_on_target	Hérité	Une fois définie, elle conserve les instantanés générés par l'utilisateur sur l'appareil cible. Continue à retenir les instantanés sur la cible jusqu'à ce que l'option soit désactivée.
	Fréquence de mise à jour	continuous	Hérité	Détermine si cette action fait l'objet d'une réplication en continu, manuelle ou à intervalles programmés.

Propriétés des systèmes de fichiers

Remarque - Dans la CLI, utilisez la commande `get` pour afficher une liste de toutes les propriétés.

TABLEAU 107 Propriétés des systèmes de fichiers

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Créer un système de fichiers	Projet	select nom_projet	--	Définit le projet que le système de fichiers utilise pour hériter des paramètres. Vous pouvez aussi sélectionner le projet par défaut.
	Nom	filesystem	--	Définit le nom du système de fichiers.
	Source de migration de données	shadow	Moment de la création	Affiche l'emplacement de la source lorsque vous migrez des données.
	Utilisateur	root-user	Système de fichiers local	Spécifie le propriétaire du répertoire racine.
	Groupe	root_group	Système de fichiers local	Spécifie le groupe du répertoire racine.
	Autorisations ou utiliser les autorisations par défaut de Windows	root_permission	Système de fichiers local	Spécifie les autorisations standard UNIX du répertoire racine ou les autorisations par défaut de Windows.
	Hériter du point de montage	--	--	Indique que le point de montage est hérité, si l'option est sélectionnée.
	Point de montage	mountpoint	Hérité	Contrôle le chemin servant à exporter les systèmes de fichiers. Pour plus d'informations, reportez-vous à la section "Point de montage" à la page 364.
	Rejeter non UTF-8	utf8only	Moment de la création	Applique le codage UTF-8 à tous les fichiers et répertoires. Pour plus d'informations, reportez-vous à la section "Rejeter non UTF-8" à la page 375.
	Sensibilité à la casse	casesensitivity	Moment de la création	Cette propriété détermine si les recherches de répertoire sont sensibles ou non à

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				la casse, ou si elles sont mixtes. Pour plus d'informations, reportez-vous à la section "Sensibilité à la casse" à la page 374.
	Normalisation	normalization	Moment de la création	Contrôle le type de normalisation Unicode exécuté sur les systèmes de fichiers et les répertoires, le cas échéant. Pour plus d'informations, reportez-vous à la section "Normalisation" à la page 376.
	Chiffrement	encryption	Hérité	Définit le type de chiffrement. Pour plus d'informations, reportez-vous à la section "Gestion des clés de chiffrement" à la page 585.
	Hériter de la clé	--	--	Indique que la clé de chiffrement est héritée du projet parent, si l'option est sélectionnée.
	Touche	key	Hérité	Définit une clé locale ou OKM et est utilisée quand la clé n'est pas héritée du projet parent.
	Nom clé	keyname	Statique	Identifie la clé.
Général - Utilisation de l'espace - Données	Quota	quota	Gestion de l'espace	Définit l'espace maximal pouvant être utilisé par une entité spécifique.
	Quota - Inclure les instantanés	quota_snap	Gestion de l'espace	Définit l'espace maximal pouvant être utilisé par une entité spécifique, y compris les instantanés.
	Réservation	reservation	Gestion de l'espace	Représente un espace garanti pouvant être utilisé par une entité spécifique.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
	Réservation - Inclure les instantanés	reservation_snap	Gestion de l'espace	Représente un espace garanti pouvant être utilisé par une entité spécifique incluant les instantanés.
Général - Utilisation de l'espace - Utilisateurs et groupes	Utilisateurs et groupes	--	--	Spécifie les utilisateurs et/ou les groupes.
	Utilisation	--	--	Indique la quantité de données utilisée par les utilisateurs et/ou les groupes.
	Quota	quota	Gestion de l'espace	Définit l'espace maximal pouvant être utilisé par une entité spécifique.
Général - Propriétés (hériter du projet)	Point de montage	mountpoint	Hérité	Contrôle le chemin servant à exporter les systèmes de fichiers. Pour plus d'informations, reportez-vous à la section " Point de montage " à la page 364.
	Lecture seule	readonly	Hérité	Cette propriété détermine si le contenu du système de fichiers est en lecture seule. Pour plus d'informations, reportez-vous à la section " Lecture seule " à la page 365.
	Mise à jour de l'heure d'accès à la lecture	atime	Hérité	Cette propriété détermine si l'heure d'accès aux fichiers a été mise à jour à la lecture de ce dernier. Pour plus d'informations, reportez-vous à la section " Mise à jour de l'heure d'accès à la lecture " à la page 365.
	Verrouillage obligatoire non bloquant	nbmand	hérité	Cette propriété détermine si la sémantique de verrouillage SMB est appliquée sur la sémantique POSIX. Pour plus d'informations,

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				reportez-vous à la section " Verrouillage obligatoire non bloquant " à la page 365.
	Suppression des doublons de données (avertissement)	dedup	Hérité	Cette propriété détermine si les doublons de données sont supprimés. Pour plus d'informations, reportez-vous à la section " Suppression des doublons de données " à la page 366.
	Compression des données	compression	Hérité	Cette propriété contrôle que les données soient bien compressées avant d'être écrites sur le disque. Pour plus d'informations, reportez-vous à la section " Compression des données " à la page 367.
	Somme de contrôle	checksum	Hérité	Cette propriété détermine la somme de contrôle utilisée pour les blocs de données. Pour plus d'informations, reportez-vous à la section " Somme de contrôle " à la page 367.
	Utilisation du périphérique de cache	secondarycache	Hérité	Cette propriété vérifie que des périphériques de cache sont utilisés pour le partage. Pour plus d'informations, reportez-vous à la section " Utilisation du périphérique de cache " à la page 368.
	Décalage d'écriture synchrone	logbias	Hérité	Contrôle le comportement lors du traitement d'écritures synchrones. Pour plus d'informations, reportez-vous à la section " Décalage d'écriture synchrone " à la page 369.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
	Taille des enregistrements de la base de données	recordsize	Hérité	Spécifie une taille de bloc suggérée pour les fichiers du système de fichiers. Pour plus d'informations, reportez-vous à la section "Taille des enregistrements de la base de données" à la page 369.
	Réplication supplémentaire	copies	Hérité	Cette propriété contrôle le nombre de copies stockées dans chaque bloc, indépendamment de toute redondance du pool de stockage. Pour plus d'informations, reportez-vous à la section "Réplication supplémentaire" à la page 370.
	Analyse antivirus	vscan	Hérité	Cette propriété détermine si un système de fichiers est analysé pour détecter d'éventuels virus. Pour plus d'informations, reportez-vous à la section "Analyse antivirus" à la page 370.
	Empêcher la destruction	nodestroy	Hérité	Lorsque cette option est définie, elle empêche la destruction des partages et des projets. Pour plus d'informations, reportez-vous à la section "Empêcher la destruction" à la page 371.
	Restreindre les modifications de propriété	rstchown	Hérité	Contrôle la propriété et peut être désactivée par système de fichiers ou par projet. Pour plus d'informations, reportez-vous à la section "Restreindre les modifications de propriété" à la page 371.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Général - Propriétés personnalisées (hériter du projet)	--	custom	--	Si nécessaire, des propriétés personnalisées peuvent être ajoutées pour lier les balises définies par les utilisateurs aux projets et aux partages.
Protocoles - NFS	NFS	sharenfs	Hérité	Les paramètres et valeurs de la propriété de protocole NFS sont décrits à la section "Propriétés de protocole NFS" à la page 408.
Protocoles - Exceptions NFS	Des exceptions à l'ensemble des modes de partage peuvent être définies pour les clients ou les collections de clients. Reportez-vous à la section "Exceptions du mode de partage NFS" à la page 409.			
Protocoles - SMB	SMB	sharesmb	Hérité	Les paramètres et valeurs de la propriété de protocole SMB sont décrits à la section "Propriétés de protocole SMB" à la page 414.
Protocoles - Exceptions SMB	Des exceptions à l'ensemble des modes de partage peuvent être définies pour les clients ou les collections de clients. Reportez-vous à la section "Exceptions du mode de partage du protocole SMB" à la page 416.			
Protocoles - ACL au niveau du partage	Type	--	--	Indique le type de l'ACL.
	Cible	--	--	Indique la cible de l'ACL.
	Accès	--	--	Indique si l'accès à l'ACL est autorisé ou refusé.
	Autorisations : héritage	--	--	Spécifie les autorisations standard UNIX de l'ACL.
Protocoles - HTTP (hériter du projet)	Mode de partage	sharedav	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Protocoles - FTP (hériter du projet)	Mode de partage	shareftp	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".
Protocoles - SFTP (hériter du projet)	Mode de partage	sharesftp	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".
Protocoles - TFTP (hériter du projet)	Mode de partage	sharetftp	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Dans la CLI, "on" est un alias de "rw".
Accès : Accès au répertoire racine	Utilisateur	root_user	Système de fichiers local	Spécifie le propriétaire du répertoire racine.
	Groupe	root_group	Système de fichiers local	Spécifie le groupe du répertoire racine.
	Autorisations	root_permissions	Système de fichiers local	Spécifie les autorisations standard UNIX sur le répertoire racine.
Accès : comportement ACL (hériter du projet)	Comportement ACL en cas de changement de mode	aclmode	Hérité	Contrôle la façon dont une demande de modification de mode interagit avec une ACL existante.
	Comportement d'héritage ACL	aclinherit	Hérité	Détermine comment un nouveau fichier ou répertoire hérite des paramètres ACL existants d'un répertoire parent.
Accès : ACL au répertoire racine	Type	--	--	Indique le type de l'ACL.
	Cible	--	--	Indique la cible de l'ACL.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
	Accès	--	--	Indique si l'accès à l'ACL est autorisé ou refusé.
	Autorisations : héritage	--	--	Spécifie les autorisations standard UNIX de l'ACL.
Instantanés - Propriétés (hériter du projet)	.zfs/visibilité de l'instantané	snapdir	Hérité	Détermine si les instantanés de système de fichiers sont accessibles par le biais des protocoles de données à l'emplacement <command>. zfs/snapshot</command> à la racine du système de fichiers.
	Etiquette d'instantané planifié	snaplabel	Hérité	Ajoute une étiquette définie par l'utilisateur à chaque instantané planifié et est vide par défaut.
Instantanés - Instantanés	Nom	--	--	Spécifie le nom de l'instantané.
	Création	--	--	Spécifie la date et heure de création de l'instantané.
	Unique	--	--	Indique la quantité d'espace unique utilisée par l'instantané.
	Total	--	--	Indique la quantité d'espace totale référencée par l'instantané. Cela représente la taille du système de fichiers au moment où l'instantané est pris et tous les instantanés peuvent théoriquement occuper une quantité d'espace égale à celle-ci quand les blocs de données sont réécrits.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
	Clones	--	--	Affiche le nombre de clones de l'instantané.
Instantané - Programmation	Fréquence	frequency	Moment de la création	Indique la fréquence de prise des instantanés.
	Conserver au plus	keep	Moment de la création	Cette propriété contrôle la stratégie de conservation des instantanés.
Réplication (hériter du projet)/Création de nouvelles actions	Cible	cible	Hérité	Identifie le système cible de la réplication.
	Pool	pool	Hérité	Spécifie le pool de stockage sur la cible où le projet sera répliqué.
	Exporter le chemin de données	export_path	Hérité	Indique le chemin d'exportation de données.
	Limite de la bande passante	max_bandwidth	Hérité	Spécifie une vitesse maximale pour cette mise à jour de réplication (en termes de quantités de données transférées chaque seconde sur le réseau).
	Activer le chiffrement SSL	use_ssl	Hérité	Détermine si les données doivent être chiffrées en simultané avec SSL.
	Disable compression	compression	Hérité	Détermine si la compression est activée ou désactivée.
	Inclure l'instantané	include_snaps	Hérité	Détermine si les mises à jour de réplication comprennent des instantanés de non-réplication.
	Conserver les instantanés utilisateurs sur la cible	retain_user_snaps_on_target	Hérité	Une fois définie, elle conserve les instantanés générés par l'utilisateur sur l'appareil cible. Continue à retenir les instantanés sur

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Utilisation				la cible jusqu'à ce que l'option soit désactivée.
	Fréquence de mise à jour	continuous	Hérité	Détermine si cette action fait l'objet d'une réplication en continu, manuelle ou à intervalles programmés.
	Données référencées	space_data	Lecture seule	Affiche l'espace total référencé par le partage actif, indépendamment de tous les instantanés.
	Réservation inutilisée	space_unused_res	Lecture seule	Affiche l'espace restant réservé au système de fichiers.
	Données d'instantanés	space_snapshots	Lecture seule	Affiche la quantité totale de données actuellement détenues par tous les instantanés du partage.
	Données disponibles	space_available	Lecture seule	Affiche tous les quotas d'un partage ou d'un projet ou la capacité totale du pool.
	Espace total	space_total	Lecture seule	Affiche la somme des données référencées, des données d'instantanés et de la réservation inutilisée.

Propriétés du LUN

Remarque - Dans la CLI, utilisez la commande `get` pour afficher une liste de toutes les propriétés.

TABLEAU 108 Propriétés des LUN

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
Créer un LUN	Projet	--	--	Définit le projet que le LUN utilise

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				pour hériter des paramètres.
	Nom	--	--	Définit le nom du LUN.
	Taille de volume	volsize	LUN local	Définit la taille de volume et l'unité de mesure maximales. Pour plus d'informations, reportez-vous à la section " Taille de volume " à la page 371.
	Provisionnement fin	sparse	LUN local	Indique uniquement l'espace physique utilisé par les données lorsque l'option est sélectionnée. Pour plus d'informations, reportez-vous à la section " Provisionnement fin " à la page 371.
	Taille de bloc des volumes	volblocksize	Moment de la création	Taille de bloc natif du LUN ; il peut s'agir de n'importe quelle puissance de 2 allant de 512 octets à 1 Mo et la valeur par défaut est 8 Ko.
	En ligne	status	LUN local	Indique le statut en ligne ou hors ligne.
	Groupe de cibles	targetgroup	LUN local	Affiche les groupes de cibles utilisés lors de l'exportation d'un LUN.
	Groupe(s) d'initiateurs	initiatorgroup	LUN local	Affiche les groupes d'initiateurs en mesure d'accéder au LUN.
	Point de montage	mountpoint	Hérité	Contrôle le chemin servant à exporter les systèmes de fichiers. Pour plus d'informations, reportez-vous à la section " Point de montage " à la page 364.
	Numéro d'unité logique	lunumber	LUN local	Définit l'unité logique de stockage sur zéro ou affecte

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				automatiquement le numéro.
	Chiffrement	encryption	Hérité	Définit le type de chiffrement.
	Hériter de la clé	--	--	Indique que la clé de chiffrement est héritée du projet parent, si l'option est sélectionnée. Pour plus d'informations, reportez-vous à la section "Gestion des clés de chiffrement" à la page 585.
	Touche	key	Hérité	Définit une clé locale ou OKM et est utilisée quand la clé n'est pas héritée du projet parent.
	Nom clé	keyname	Statique	Identifie la clé.
	GUID	lunguid	En lecture seule, LUN local	Un identificateur unique en lecture seule qui identifie le périphérique SCSI.
Général - Utilisation de l'espace - Données	Taille de volume	volsize	LUN local	Définit la taille de volume et l'unité de mesure maximales. Pour plus d'informations, reportez-vous à la section "Taille de volume" à la page 371.
	Provisionnement fin	sparse	LUN local	Indique uniquement l'espace physique utilisé par les données lorsque l'option est sélectionnée. Pour plus d'informations, reportez-vous à la section "Provisionnement fin" à la page 371.
Général - Propriétés (hériter du projet)	Suppression des doublons de données (avertissement)	dedup	Hérité	Cette propriété détermine si les doublons de données sont supprimés. Pour plus d'informations, reportez-vous à la section "Suppression"

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				des doublons de données" à la page 366.
	Compression des données	compression	Hérité	Cette propriété contrôle que les données soient bien compressées avant d'être écrites sur le disque. Pour plus d'informations, reportez-vous à la section "Compression des données" à la page 367.
	Somme de contrôle	checksum	Hérité	Cette propriété détermine la somme de contrôle utilisée pour les blocs de données. Pour plus d'informations, reportez-vous à la section "Somme de contrôle" à la page 367.
	Réplication supplémentaire	copies	Hérité	Cette propriété contrôle le nombre de copies stockées dans chaque bloc, indépendamment de toute redondance du pool de stockage. Pour plus d'informations, reportez-vous à la section "Réplication supplémentaire" à la page 370.
	Utilisation du périphérique de cache	secondarycache	Hérité	Cette propriété vérifie que des périphériques de cache sont utilisés pour le partage. Pour plus d'informations, reportez-vous à la section "Utilisation du périphérique de cache" à la page 368.
	Décalage d'écriture synchrone	logbias	Hérité	Contrôle le comportement lors du traitement d'écritures synchrones. Pour plus d'informations, reportez-vous à la section

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
				"Décalage d'écriture synchrone" à la page 369.
	Empêcher la destruction	nodestroy	Hérité	Lorsque cette option est définie, elle empêche la destruction des partages et des projets. Pour plus d'informations, reportez-vous à la section "Empêcher la destruction" à la page 371.
Propriétés personnalisées (hériter du projet)	Schéma	schema	--	Peuvent être ajoutées pour lier les balises définies par les utilisateurs aux projets et aux partages. Pour plus d'informations, voir la section "Utilisation des schémas" à la page 427.
Protocoles - Options de partage	En ligne	status	LUN local	Indique le statut en ligne ou hors ligne.
	Groupe de cibles	targetgroup	LUN local	Affiche les groupes de cibles utilisés lors de l'exportation d'un LUN.
	Groupe(s) d'initiateurs : numéro LU	initiatorgroup	LUN local	Affiche les groupes d'initiateurs en mesure d'accéder au LUN.
Protocoles - Comportement du cache d'écriture	Cache d'écriture activé	writecache	LUN local	Détermine si le LUN met en cache les données écrites.
Instantanés - Propriétés (hériter du projet)	Etiquette d'instantané planifié	snaplabel	Hérité	Ajoute une étiquette définie par l'utilisateur à chaque instantané planifié et est vide par défaut.
Instantanés - Instantanés	Nom	--	--	Spécifie le nom de l'instantané.
	Création	--	--	Spécifie la date et heure de création de l'instantané.
	Unique	--	--	Indique la quantité d'espace unique utilisée par l'instantané.

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
	Total	--	--	Indique la quantité d'espace totale référencée par l'instantané.
	Clones	--	--	Affiche le nombre de clones de l'instantané.
Instantanés - Programmations	Fréquence	frequency	Moment de la création	Indique la fréquence de prise des instantanés.
	Conserver au plus	keep	Moment de la création	Cette propriété contrôle la stratégie de conservation des instantanés.
Réplication (hériter du projet)/Création de nouvelles actions	Cible	cible	Hérité	Identifie le système cible de la réplication.
	Pool	pool	Hérité	Spécifie le pool de stockage sur la cible où le projet sera répliqué.
	Exporter le chemin de données	export_path	Hérité	Indique le chemin d'exportation de données.
	Limite de la bande passante	max_bandwidth	Hérité	Spécifie une vitesse maximale pour cette mise à jour de réplication (en termes de quantités de données transférées chaque seconde sur le réseau).
	Activer le chiffrement SSL	use_ssl	Hérité	Détermine si les données doivent être chiffrées en simultané avec SSL.
	Disable compression	compression	Hérité	Détermine si la compression est activée ou désactivée.
	Inclure l'instantané	include_snaps	Hérité	Détermine si les mises à jour de réplication comprennent des instantanés de non-réplication.
	Conserver les instantanés	retain_user_snaps_on_target	Hérité	Une fois définie, elle conserve les instantanés générés

Emplacement dans la BUI	Nom dans la BUI	Nom dans la CLI	Type de propriété	Description
	utilisateurs sur la cible			par l'utilisateur sur l'appareil cible.
	Fréquence de mise à jour	continuous	Hérité	Détermine si cette action fait l'objet d'une réplication en continu, manuelle ou à intervalles programmés.
Utilisation	Données référencées	space_data	Lecture seule	Affiche l'espace total référencé par le partage actif, indépendamment de tous les instantanés.
	Données d'instantanés	space_snapshots	Lecture seule	Affiche la quantité totale de données actuellement détenues par tous les instantanés du partage.
	Données disponibles	space_available	Lecture seule	Affiche tous les quotas d'un partage ou d'un projet ou la capacité totale du pool.
	Espace total	space_total	Lecture seule	Affiche la somme des données référencées, des données d'instantanés et de la réservation inutilisée.

Gestion de l'espace pour les partages

Oracle ZFS Storage Appliance gère le stockage physique au moyen d'un modèle de stockage de pools où tous les systèmes de fichiers et les LUN partagent un espace commun. Les systèmes de fichiers n'ont jamais de taille explicite assignée et utilisent simplement l'espace dont ils ont besoin. Les LUN réservent suffisamment d'espace physique pour écrire la totalité du contenu sur le périphérique, à moins qu'une allocation fine ne soit appliquée. Dans ce cas, ils se comportent comme des systèmes de fichiers et utilisent uniquement l'espace consommé par les données.

Ce système offre une flexibilité maximale et une simplicité de gestion dans un environnement qui fait confiance aux utilisateurs pour agir correctement. Un environnement plus strict, dans lequel l'utilisation des données utilisateur est contrôlée et/ou restreinte, nécessite une gestion plus prudente.

Ces rubriques définissent la terminologie et la façon de gérer l'utilisation de l'espace, par partage ou par utilisateur, en utilisant des quotas et des réservations.

- ["Terminologie relative aux partages" à la page 401](#)
- ["Gestion de l'espace du système de fichiers et du projet" à la page 402](#)
- ["Configuration des quotas d'utilisateurs ou de groupes" à la page 403](#)
- ["Utilisation de la gestion des identités" à la page 404](#)
- ["Statistiques d'utilisation des partages" à la page 406](#)

Terminologie relative aux partages

Avant de rentrer dans les détails, il est important de comprendre certains termes basiques utilisés pour parler de l'utilisation de l'espace sur l'appareil.

- **Données physiques** : taille des données stockées physiquement sur le disque. En règle générale, elle correspond à la taille logique des données mais peut être différente au cours de la phase de compression ou du fait d'autres facteurs. Elle inclut l'espace du partage actif ainsi que tous les instantanés. La comptabilisation de l'espace est généralement effectuée et gérée en fonction de l'espace physique.
- **Données logiques** : volume d'espace logique consommé par un système de fichiers. Le calcul des données logiques ne prend pas en compte la compression. Elles peuvent être considérées comme la limite supérieure théorique de l'espace consommée par le système de fichiers. La copie du système de fichiers sur un autre appareil à l'aide d'un algorithme de compression différent n'entraîne pas une consommation plus importante que cette quantité. Cette statistique n'est pas exportée explicitement et peut généralement être calculée en prenant la quantité d'espace physique consommé et en la multipliant par le taux de compression en cours.
- **Données référencées** : espace total référencé par le partage actif, indépendamment de tous les instantanés. Cela représente l'espace qui serait libéré si tous les instantanés étaient détruits. C'est également la quantité de données que l'utilisateur peut gérer directement à l'aide des protocoles de données.
- **Données d'instantané** : quantité totale de données actuellement détenues par tous les instantanés du partage. Cela représente l'espace qui serait libéré si tous les instantanés étaient détruits.
- **Quota** : espace maximal pouvant être utilisé par une entité spécifique. Il peut se baser sur un système de fichiers, un projet, un utilisateur et ne prend pas en compte l'utilisation de l'espace actuel.
- **Réservation** : garantie d'espace pour un projet ou un système de fichiers spécifique. Cela permet de prendre l'espace disponible restant du pool sans augmenter la consommation d'espace actuelle du système de fichiers. Ce paramètre ne peut pas être appliqué aux utilisateurs et aux groupes. Il est possible de créer le concept classique d'un système de fichiers structuré de manière statique en paramétrant un quota et une réservation sur la même valeur.

Gestion de l'espace du système de fichiers et du projet

Le moyen le plus simple d'appliquer des quotas et des réservations est de le faire par projet et par utilisateur. Les quotas et les réservations ne s'appliquent pas aux LUN, bien que leur utilisation soit prise en compte dans les quotas et réservations de la totalité du projet.

Quotas de données - Un quota de données impose une limite sur la quantité d'espace qu'un système de fichiers ou qu'un projet peut utiliser. Par défaut, il inclut les données dans le système de fichiers et dans tous les instantanés. Les clients qui tentent d'écrire de nouvelles données obtiennent un message d'erreur lorsque le système de fichiers est plein, soit à cause du quota, soit parce que le pool de stockage est à court d'espace libre. Comme décrit dans la section ["Gestion de l'espace pour les instantanés" à la page 443](#), il est possible que ce comportement ne soit pas intuitif dans toutes les situations et en particuliers lorsque des instantanés sont présents. La suppression d'un fichier oblige parfois le système de fichiers à écrire de nouvelles données si les blocs de données sont référencés par un instantané. Il est donc possible que la seule façon de réduire l'utilisation de l'espace consiste à détruire les instantanés existants.

Si la propriété "inclure les instantanés" n'est pas définie, le quota s'applique uniquement aux données immédiates référencées par le système de fichiers, et non aux instantanés. L'espace utilisé par les instantanés est appliqué par le quota au niveau du projet (autrement, il n'est pas appliqué). Dans cette situation, la suppression d'un fichier référencé par un instantané entraîne la réduction des données référencées par le système de fichiers, même si l'ensemble du système utilise plus d'espace. Si le pool de stockage est saturé (par opposition au système de fichiers qui atteint la limite d'un quota prédéfini), la seule manière de libérer de l'espace peut consister à détruire des instantanés.

Les quotas de données sont strictement appliqués. Concrètement, lorsque l'utilisation de l'espace est proche de la limite, il convient de modérer la quantité de données pouvant être écrites, car leur quantité précise n'est pas connue tant que les données n'ont pas été reconnues. Cela peut avoir un effet sur les performances lors du fonctionnement à la limite du quota. C'est pourquoi il est en général conseillé de rester en dessous du quota pendant les procédures normales de traitement.

Les quotas sont gérés via la BUI sous Partages -> Général -> Utilisation de l'espace -> Données. Ils sont gérés dans la CLI en tant que propriétés quota et quota_snap.

Réservations de données - La réservation de données permet de s'assurer qu'un système de fichiers ou un projet dispose au moins d'une certaine quantité d'espace disponible, même si d'autres partages du système tentent d'utiliser davantage d'espace. Cette réservation inutilisée étant considérée comme une partie intégrante du système de fichiers, si le reste du pool (ou du projet) atteint la limite, le système de fichiers peut écrire de nouvelles données même si d'autres partages sont saturés.

Par défaut, une réservation inclut tous les instantanés d'un système de fichiers. Si la propriété "inclure les instantanés" n'est pas définie, la réservation s'applique uniquement aux données immédiates du système de fichiers. Le comportement de création d'instantanés peut ne pas être

toujours intuitif. Si une réservation (et non les instantanés) est effective sur des données de système de fichiers, chaque fois qu'un instantané est pris, le système doit réserver assez d'espace pour que l'instantané diverge complètement, même si cela ne se produit jamais. Par exemple, si un système de fichiers de 50 Go a une réservation de 100 Go sans instantané, la prise du premier instantané entraîne une réservation d'espace supplémentaire de 50 Go et le système de fichiers finit par réserver 150 Go d'espace total. S'il n'y a pas suffisamment d'espace pour garantir la divergence complète des données, la prise d'un instantané échoue.

Les réservations sont gérées via la BUI sous Partages -> Général -> Utilisation de l'espace -> Données. Ils sont gérés dans la CLI en tant que propriétés `reservation` et `reservation_snap`.

Gestion de l'espace pour la réplication des LUN - Lorsque vous créez un LUN, l'espace physique total configuré pour le LUN est réservé et ne peut pas être utilisé par d'autres systèmes de fichiers (à moins qu'il ne soit à allocation fine). Pour la réplication, lorsque vous prenez un instantané d'un LUN de n'importe quelle taille, cela entraîne également la réservation d'un espace représentant le double de la taille du LUN selon la quantité d'espace réservé au LUN utilisée.

La liste suivante présente l'espace total maximum nécessaire à la réplication d'un LUN :

- Jusqu'à 100 % sur la source entre les mises à jour
- Jusqu'à 200 % sur la source pendant une mise à jour
- Jusqu'à 200 % sur la cible

Configuration des quotas d'utilisateurs ou de groupes

Il est possible de définir des quotas sur un utilisateur ou un groupe au niveau du système de fichiers ainsi que du projet. Ils imposent une utilisation des données physiques basée sur l'identité POSIX ou Windows du propriétaire ou du groupe du fichier ou du répertoire. Voici quelques-unes des principales différences entre les quotas d'utilisateurs et les quotas de groupes, puis entre les quotas de données de projet et les quotas de systèmes de fichiers :

- Les quotas d'utilisateurs et de groupes peuvent uniquement être appliqués aux systèmes de fichiers et aux projets.
- Les quotas par défaut peuvent être définis au niveau projet et hérités par les systèmes de fichiers du projet.
- Les quotas par défaut peuvent être changés au niveau système de fichiers.
- Les quotas par défaut peuvent être consultés ou modifiés au moyen du protocole SMB.
- Les quotas d'utilisateurs et de groupes sont implémentés à l'aide d'une *mise en oeuvre différée*. Cela signifie que, durant une courte période précédant l'écriture des données sur le disque, les utilisateurs peuvent dépasser le quota. Une fois que les données sont intégrées au disque, l'utilisateur reçoit un message d'erreur sur les nouvelles données écrites, exactement comme dans le cas des quotas au niveau du système de fichiers.

- Les quotas d'utilisateurs et de groupes s'appliquent toujours aux données référencées. Cela signifie que les instantanés n'affectent aucun quota et qu'un clone de l'instantané consomme la même quantité du quota effectif, même si les blocs sous-jacents sont partagés.
- Les réservations d'utilisateur et de groupe ne sont pas prises en charge.
- Les quotas d'utilisateur et de groupe, contrairement aux quotas de données, sont stockés avec les données de système de fichiers standard. Concrètement, si le système de fichiers est saturé, vous ne pouvez pas modifier les quotas d'utilisateur et de groupe. Il faut d'abord libérer de l'espace avant de modifier les quotas d'utilisateur et de groupe.
- Les quotas d'utilisateur et de groupe sont envoyés avec n'importe quelle réplication distante. Il incombe à l'administrateur de s'assurer que les environnements de service de noms sont les mêmes dans la source et dans la destination.
- La sauvegarde et la restauration NDMP de la totalité d'un partage inclut tous les quotas de groupe ou d'utilisateur. La restauration dans un partage existant n'affecte aucun quota actuel.

Utilisation de la gestion des identités

Les quotas d'utilisateur et de groupe optimisent le service de mappage des identités sur l'appareil. Il permet de spécifier l'identité des utilisateurs et des groupes selon l'environnement (UNIX ou Windows). A l'instar de l'appartenance des fichiers, ces identités sont suivies de l'une des manières suivantes :

- En l'absence de mappage UNIX, une référence à l'ID Windows est stockée.
- En présence d'un mappage UNIX, c'est l'ID UNIX qui est stocké.

Cela signifie que la forme canonique de l'identité est l'ID UNIX. Si le mappage est modifié par la suite, le nouveau mappage est appliqué en fonction du nouvel ID UNIX. Si un fichier est créé par un utilisateur Windows quand aucun mappage n'existe et qu'un mappage est créé par la suite, les nouveaux fichiers seront traités avec un propriétaire différent à des fins de contrôle d'accès et de format d'utilisation. Cela implique que l'ID d'utilisateur est réutilisé (c.-à-d. qu'une nouvelle association de nom d'utilisateur est créée) et que tous fichiers ou quotas existants s'affichent comme appartenant au nouveau nom d'utilisateur.

Il est recommandé d'établir toutes les règles de mappage des identités avant d'essayer d'utiliser activement les systèmes de fichiers. Cependant, toute modification du mappage peut avoir des conséquences surprenantes.

Utilisation de l'espace de noms du système de fichiers

Tous les systèmes de fichiers de l'appareil doivent avoir un point de montage unique faisant office de point d'accès pour les données du système de fichiers. Les projets peuvent avoir des points de montage mais ils servent uniquement d'outil pour gérer l'espace de noms à

l'aide des propriétés héritées. Les projets ne sont jamais montés et n'utilisent aucun protocole d'exportation des données.

Tous les partages doivent être montés sous `/export`. Bien qu'il soit possible de créer un système de fichiers monté dans `/export`, ce n'est pas obligatoire. Si ce partage n'existe pas, tous les répertoires seront créés dynamiquement si nécessaire sous cette partie de la hiérarchie. Au sein d'un cluster, chaque point de montage doit être unique.

- **Points de montage d'espaces de noms imbriqués** : il est possible de créer des systèmes de fichiers avec des points de montage en dessous d'autres systèmes de fichiers. Dans ce scénario, les systèmes de fichiers parent sont montés avant les systèmes de fichiers enfant (et inversement). Les cas suivants doivent être considérés lorsque vous utilisez des points de montage imbriqués :
 - Si le point de montage n'existe pas, il est créé et appartient à l'utilisateur root et au mode 0755. Selon les circonstances, il est possible que ce point de montage disparaisse lorsque le système de fichiers est renommé, détruit ou déplacé. Pour assurer la sécurité des points de montage, ils doivent être créés dans le système de fichiers parent avant de créer le système de fichiers enfant.
 - Si le répertoire parent est en lecture seule et que le point de montage n'existe pas, le montage du système de fichiers échoue. Cela peut se produire de façon synchrone lors de la création du système de fichiers, mais également de façon asynchrone lorsque vous effectuez une modification à grande échelle (comme renommer les systèmes de fichiers avec des points de montage hérités).
 - Lorsque vous renommez un système de fichiers ou que vous modifiez son point de montage, tous les enfants situés sous le point de montage actuel et le nouveau point de montage (s'ils sont différents) sont démontés puis remontés après l'application des modifications. Cette action entraîne l'interruption de tous les services de données qui accèdent actuellement au partage.
 - La prise en charge du parcours automatique des points de montage imbriqués dépend du protocole, comme indiqué ci-dessous.
- **Espace de noms NFSv2 / NFSv3 / NFSv4** : sous NFS, chaque système de fichiers est un export unique rendu visible par le protocole MOUNT. NFSv2 et NFSv3 n'ont aucun moyen de parcourir les systèmes de fichiers imbriqués et l'accès à chaque système de fichiers s'effectue grâce à son chemin d'accès complet. Alors que les points de montage imbriqués sont encore fonctionnels, si vous tentez de croiser un point de montage imbriqué, un répertoire vide sera créé sur le client. Même si ce problème peut être atténué par l'utilisation de montages automatiques, la prise en charge transparente des points de montage imbriqués dans un environnement dynamique requiert NFSv4.

En ce qui concerne les points de montage, NFSv4 propose de nombreuses améliorations par rapport à NFSv3. La première de ces améliorations est la possibilité pour les répertoires parent d'être montés, même si aucun partage n'est disponible à ce point de la hiérarchie. Par exemple, si le répertoire `/export/home` a été partagé, il est possible de monter `/export` sur le client et de parcourir les exports effectifs de manière transparente. Une amélioration plus visible est la prise en charge par certains clients NFSv4 (y compris Linux) des montages côté client automatiques, parfois également appelés "montages en miroir". Avec ce type

de client, lorsqu'un utilisateur parcourt un point de montage, le système de fichiers enfant est automatiquement monté au niveau du point de montage local approprié et supprimé lorsque le système de fichiers est démonté. Du point de vue du serveur, il s'agit de requêtes de montage séparées. Toutefois, elles sont liées sur le client pour former un espace de noms de système de fichiers cohérent.

- **Espace de noms SMB** : le protocole SMB n'utilise pas de points de montage car chaque partage est rendu disponible par nom de ressource. Cependant, chaque système de fichiers doit tout de même avoir un point de montage unique. Les points de montage imbriqués (plusieurs systèmes de fichiers dans une seule ressource) ne sont pas pris en charge actuellement et toute tentative de parcourir un point de montage entraîne la création d'un répertoire vide.
- **Espace de noms FTP / FTPS / SFTP** : les systèmes de fichiers sont exportés à l'aide de leur point de montage standard. Les points de montage imbriqués sont totalement pris en charge et sont transparents pour l'utilisateur. Cependant, il est impossible de ne pas partager un système de fichiers imbriqué lorsque son point de montage parent est partagé. Si un point de montage parent est partagé, tous les enfants sont également partagés.
- **Espace de noms HTTP / HTTPS** : les systèmes de fichiers étant exportés sous le répertoire /shares, un système de fichiers situé au niveau /export/home apparaît sous /shares/export/home sur HTTP/HTTPS. Les points de montage imbriqués sont totalement pris en charge et sont transparents pour l'utilisateur. Le même comportement se rapportant aux options de partage en conflit décrites à la section relative au protocole FTP s'applique à HTTP.

Statistiques d'utilisation des partages

Dans la partie gauche de la vue (sous le panneau Projet lorsqu'il est réduit), vous trouverez un tableau explicatif des statistiques d'utilisation de l'espace. Ces statistiques concernent soit un partage en particulier (lorsque vous modifiez un partage), soit l'ensemble du pool (lorsque vous consultez la liste des partages). Si une propriété a la valeur zéro, elle est exclue du tableau.

Certaines statistiques d'utilisation s'affichent également dans le contexte de la CLI `shares show`.

Le tableau suivant décrit les propriétés d'utilisation de la BUI et de la CLI.

Nom dans la BUI	Nom dans la CLI	Description
Espace disponible	--	Cette statistique est implicitement présentée comme la capacité en termes de pourcentage de capacité dans le titre. L'espace disponible reflète tous les quotas d'un partage ou d'un projet ou la capacité totale du pool. Le nombre affiché ici correspond à la somme de l'espace total utilisé et de la quantité d'espace disponible.
Données référencées	usage_data	Il s'agit de la quantité de données référencées par les données. Cela inclut l'intégralité des données de système

Nom dans la BUI	Nom dans la CLI	Description
		de fichiers ou des blocs de LUN en plus des métadonnées requises. Avec la compression, il est possible que cette valeur soit très inférieure à la valeur de la taille logique des données contenues dans le partage. Si le partage est un clone d'un instantané, cette valeur peut être inférieure au stockage physique qu'elle pourrait en théorie inclure et peut être égale à zéro.
Données d'instantanés	usage_snapshots	Il s'agit de la quantité d'espace utilisé par tous les instantanés du partage, y compris les instantanés de projet. La taille n'est pas égale à la somme de l'espace unique consommé par l'ensemble des instantanés. Les blocs référencés par plusieurs instantanés ne sont pas inclus dans les statistiques d'utilisation de l'espace par instantané mais apparaîtront dans le total des données d'instantané du partage.
Réservation inutilisée	--	Si une réservation est définie pour un système de fichiers, cette valeur indique l'espace réservé restant pour ce système de fichiers. Pour les LUN, cette valeur n'est pas définie. L'appareil empêche les autres partages de consommer cet espace afin de garantir que le système de fichiers dispose de suffisamment d'espace. Si la réservation n'inclut pas les instantanés, l'espace doit être suffisant pour que, lors de la prise de l'instantané, la totalité de l'instantané soit écrasé. Pour plus d'informations sur les réservations, reportez-vous à la section "Propriétés des systèmes de fichiers" à la page 384 .
Espace total	usage_total	Il s'agit de la somme des données référencées, des données d'instantanés et de la réservation inutilisée.

Protocoles de partage et de projet

Chaque partage possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour ce partage. Ces propriétés peuvent être définies pour chaque partage ou héritées d'un partage contenu dans un projet.

Pour iSCSI, les initiateurs peuvent détecter la cible par le biais d'un des mécanismes décrits dans la section ["Configuration du réseau de stockage SAN" à la page 127](#).

Pour plus d'informations sur les propriétés de protocole prises en charge, reportez-vous aux sections suivantes :

- ["Protocole NFS" à la page 408](#)
- ["Protocole SMB" à la page 414](#)
- ["Protocole HTTP" à la page 419](#)
- ["Protocole FTP" à la page 419](#)
- ["Protocole SFTP" à la page 419](#)
- ["Protocole TFTP" à la page 420](#)

Rubriques connexes

- "Configuration NFS" à la page 237
- "Configuration SMB" à la page 243

Protocole NFS

Cette section aborde les sujets suivants :

- "Propriétés de protocole NFS" à la page 408
- "Exceptions du mode de partage NFS" à la page 409
- "Encodages de jeux de caractères du protocole NFS" à la page 412
- "Modes de sécurité du protocole NFS" à la page 413

Pour plus d'informations sur le protocole NFS, consultez les rubriques suivantes :

- "Configuration NFS" à la page 237
- "Propriétés des systèmes de fichiers" à la page 384
- "Propriétés des projets" à la page 377
- NFSv2 and NFSv3 Security (RFC 2623) (<http://www.ietf.org/rfc/rfc2623.txt>)
- NFSv4 Protocol (RFC 3530) (<http://www.ietf.org/rfc/rfc3530.txt>)

Pour plus d'informations sur les autres protocoles pris en charge, reportez-vous aux sections suivantes :

- "Protocole SMB" à la page 414
- "Protocole HTTP" à la page 419
- "Protocole FTP" à la page 419
- "Protocole SFTP" à la page 419
- "Protocole TFTP" à la page 420

Propriétés de protocole NFS

Chaque partage possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour ce partage. Ces propriétés peuvent être définies pour chaque partage ou héritées d'un partage contenu dans un projet. Le tableau suivant présente les propriétés de protocole NFS et leurs valeurs possibles.

TABLEAU 109 Propriétés de protocole NFS

Propriété	Valeur(s) CLI	Type de propriété	Description
Mode de partage	off/rw/ro	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture

Propriété	Valeur(s) CLI	Type de propriété	Description
			et l'écriture ou aucun des deux. Reportez-vous à la section " Protocoles de partage et de projet " à la page 407.
Désactiver la création de fichiers setuid/setgid	nosuid	Hérité	Si cette option est sélectionnée, les clients ne pourront pas créer de fichiers avec les bits setuid (S_ISUID) et setgid (S_ISGID) définis, ni activer ces bits sur des fichiers existants via l'appel système chmod(2).
Prevent clients from mounting subdirectories	nosub	Hérité	Si cette option est sélectionnée, les clients ne pourront pas monter directement les sous-répertoires. Ils seront obligés de commencer par monter la racine du partage. Remarque : Cela s'applique uniquement aux protocoles NFSv2 et NFSv3, non aux protocoles NFSv4.
Mappage d'utilisateur anonyme	anon	Hérité	A moins que l'option "root" soit active pour un client spécifique, l'utilisateur root sur ce client est traité comme un utilisateur inconnu. Toutes ses tentatives d'accès aux fichiers des partages sont considérées comme venant d'un utilisateur possédant cet UID. Ces bits d'accès et les ACL du fichier sont alors évalués normalement.
Jeu de caractères	Pour connaître les valeurs admises, reportez-vous à la section Encodages de jeux de caractères .	Hérité	Cette propriété définit le jeu de caractères par défaut de tous les clients.
Mode de sécurité	sec= Pour obtenir une liste des valeurs admises, reportez-vous à la section Modes de sécurité .	Hérité	Cette propriété définit le mode de sécurité de tous les clients.
Imposer des ports réservés pour l'authentification système	resvport	Hérité	Lors de la définition sur un partage ou un projet avec le mode de sécurité d'authentification système, les clients NFS doivent utiliser des ports TCP à faible numérotation (« réservés »). Certains clients NFS, comme Solaris et Linux, utilisent des ports TCP à faible numérotation par défaut. D'autres clients, comme Windows, peuvent nécessiter une configuration.

Exceptions du mode de partage NFS

Des exceptions au mode de partage global peuvent être définies pour des clients ou des groupes de clients via la configuration de modes de partage spécifiques au client ("exceptionnels"). En règle générale, il est recommandé de définir le mode de partage global none, puis d'octroyer progressivement un accès de plus en plus large à des groupes de plus en plus restreints. Par exemple, vous pouvez créer un partage avec le mode de partage global none (qui refuse l'accès

à tous les clients), puis accorder un accès en lecture seule à un sous-ensemble de clients. Ensuite, vous pouvez accorder l'accès en lecture et écriture à un sous-ensemble encore plus réduit de clients, et finalement l'accès en lecture-écriture et root aux seuls hôtes sécurisés.

Les modes de partage spécifiques au client priment sur le mode de partage global. L'accès est accordé à un client en fonction du mode de partage spécifique au client spécifié dans une exception. En l'absence d'exceptions, l'accès est accordé au client sur la base du mode de partage global.

TABLEAU 110 Types de client

Type	Préfixe CLI	Description	Exemple
Hôte (FQDN) ou Netgroup	none	Client unique dont l'adresse IP est résolue en nom complet spécifié ou groupe réseau qui contient les noms complets vers lesquels est résolue l'adresse IP d'un client.	caji.sf.example.com
Domaine DNS	.	Tous les clients dont l'adresse IP est résolue en nom complet qui se termine par ce suffixe.	sf.example.com
Sous-réseau IPv4	@	Tous les clients dont les adresses IP sont comprises dans le sous-réseau IPv4 indiqué, en notation CIDR	192.168.20.0/22
Sous-réseau IPv6	@	Tous les clients dont les adresses IP sont comprises dans le sous-réseau IPv6 indiqué, en notation CIDR	2606:b400:410:d43::/64

Pour chaque client ou collection de clients, spécifiez si le client dispose d'un accès en lecture seule ou en lecture/écriture au partage. Si vous définissez une exception NFS, spécifiez également si le client dispose des privilèges d'un utilisateur root ou s'il doit être traité comme un utilisateur sans accès root.

Gestion de groupes réseau

Il est possible d'utiliser des groupes réseau pour le contrôle d'accès lors des exportations NFS. La gestion de groupes réseau peut toutefois s'avérer complexe. A la place, vous pouvez envisager d'utiliser des règles de sous-réseau IP ou des règles de domaine DNS.

Si des groupes réseau sont utilisés, ils seront résolus à partir de NIS ou LDAP, selon le service activé. Si LDAP est utilisé, chaque groupe réseau doit se trouver à l'emplacement par défaut, ou=Netgroup,(Base DN) et doit utiliser le schéma standard.

En général, le composant nom d'utilisateur d'une entrée de groupe réseau n'a aucune conséquence sur NFS, contrairement au composant nom d'hôte. Les noms d'hôte contenus dans les groupes réseau doivent être canoniques et, s'ils ont été choisis à l'aide de DNS, ils doivent être complets. Concrètement, le sous-système NFS tente de vérifier que l'adresse IP du client qui a fait la demande soit résolue en nom d'hôte canonique qui correspond soit au

nom de domaine complet (FQDN) indiqué, soit à un membre d'un des groupes réseau spécifiés. Cette correspondance doit être exacte, y compris concernant les composants de domaine. Dans le cas contraire, l'exception n'est pas valide et on passe à l'exception suivante. Pour plus d'informations sur la résolution du nom d'hôte, consultez la section [DNS](#).

Depuis la version logicielle 2013.1.0, les utilisateurs de clients UNIX peuvent appartenir à un maximum de 1 024 groupes sans aucune perte de performance. Les versions précédentes prenaient en charge jusqu'à 16 groupes par utilisateur de client UNIX.

Options des modes de partage et d'exception NFS

Dans la CLI, tous les modes de partage NFS et les exceptions sont spécifiés à l'aide d'une chaîne d'options unique pour la propriété `sharenfs`. Cette chaîne est une liste de valeurs séparées par des virgules. Elle doit commencer par `ro`, `rw`, `on` ou `off`, de la même manière que pour les modes de partage globaux décrits dans la BUI.

TABLEAU 111 Valeurs du mode de partage NFS (BUI et CLI)

Valeur BUI	Valeur CLI	Description
Aucune	<code>off</code>	Le mode de partage est désactivé.
Lecture/écriture	<code>on</code>	Le nom de partage correspond au nom d'ensemble de données, et le partage est en mesure de lire et écrire en l'absence d'exceptions SMB. S'il existe des exceptions SMB, le mode de partage est désactivé.
	<code>rw</code>	Le nom de partage correspond au nom d'ensemble de données, et le partage est en mesure de lire et écrire.
Lecture seule	<code>ro</code>	Le nom de partage correspond au nom d'ensemble de données, et le partage est seulement en mesure de lire.

L'exemple suivant définit le mode de partage en lecture seule pour tous les clients. Les utilisateurs `root` sur tous les clients accèdent aux fichiers du partage comme s'ils étaient l'utilisateur générique `"nobody"`.

```
set sharenfs=ro
```

L'une ou les deux options `nosuid` et `anon` peuvent également être ajoutées. Par conséquent, pour définir le mappage de tous les utilisateurs inconnus sur l'UID 153762, vous devez spécifier ceci :

```
set sharenfs="ro,anon=153762"
```

Remarque - Les valeurs de propriété CLI qui contiennent "=" doivent être indiquées entre guillemets.

Il est possible de spécifier des exceptions NFS supplémentaires en ajoutant du texte sous la forme `ro`, `rw` ou `root`, qui définit le type d'accès à octroyer à la collection de clients. La collection est spécifiée par le caractère de préfixe provenant du tableau Types de client et par un nom de domaine/d'hôte DNS ou un numéro de réseau CIDR. Par exemple, pour octroyer l'accès en lecture-écriture à tous les hôtes du domaine `sf.example.com` et l'accès `root` aux hôtes du réseau `192.168.44.0/24`, vous devez utiliser :

```
set sharenfs="ro,anon=153762,rw=.sf.example.com,root=@192.168.44.0/24"
```

Remarque - Cet exemple ne s'applique qu'aux exceptions NFS.

Les noms de groupe réseau peuvent être utilisés partout où un nom d'hôte complet peut être utilisé. Par exemple, vous pouvez autoriser l'accès en lecture-écriture au groupe réseau `"engineering"` comme suit :

```
set sharenfs="ro,rw=engineering"
```

Encodages de jeux de caractères du protocole NFS

Normalement, le codage de jeu de caractères utilisé pour le nom de fichier n'est pas spécifié. Les protocoles NFSv3 et NFSv2 ne spécifient pas le jeu de caractères. NFSv4 est censé utiliser UTF-8 mais ce n'est pas le cas de tous les clients et cette restriction n'est pas appliquée par le serveur. Si l'option UTF-8 uniquement est désactivée pour un partage, ces noms de fichiers sont écrits in extenso dans les systèmes de fichiers sans aucune connaissance de leurs codages. Cela signifie qu'ils peuvent être interprétés uniquement par les clients qui utilisent le même codage. En revanche, SMB nécessite que les noms de fichiers soient stockés en UTF-8 afin qu'ils puissent être interprétés côté serveur. Il est donc impossible de prendre en charge des codages client arbitraires tout en autorisant l'accès sur SMB.

Pour prendre en charge des configurations de ce type, le codage de jeu de caractère peut être défini au niveau de tout le partage ou par client. Les codages de jeu de caractères suivants sont pris en charge :

cp932	euc-tw	iso8859-7	koi8-r
euc-cn	iso8859-1	iso8859-8	shift_jis
euc-jp	iso8859-2	iso8859-9	
euc-jpms	iso8859-5	iso8859-13	
euc-kr	iso8859-6	iso8859-15	

Le comportement par défaut est de ne pas spécifier le codage de jeu de caractères (intercommunication). La BUI permet de choisir le jeu de caractères via le mécanisme de liste d'exception standard. Dans la CLI, chaque jeu de caractère devient une option ayant ou plusieurs hôtes et où le symbole étoile "*" indique le paramétrage du partage. Par exemple :

```
hostname:shares default> set sharenfs="rw,euc-kr=*"
```

partage le système de fichiers avec le codage par défaut "euc-kr". Par exemple,

```
hostname:shares default> set sharenfs="rw,euc-kr=host1.domain.com,euc-jp=host2.domain.com"
```

utilise le codage par défaut pour tous les clients sauf "host1" et "host2" qui utilisent respectivement "euc-kr" et "euc-jp". Le format des listes hôtes est similaire à celui des autres options NFS de la CLI.

Notez que les clients NFS ne prennent pas correctement en charge les autres paramètres locaux. Consultez la documentation client NFS pour obtenir de plus amples détails.

Modes de sécurité du protocole NFS

Les modes de sécurité sont définis par partage. La liste suivante décrit les paramètres de sécurité Kerberos.

- **krb** - Authentification d'utilisateur final via Kerberos V5
- **krb5i** - krb5 plus préservation de l'intégrité (les paquets de données résistent aux dégradations)
- **krb5p** - krb5i plus préservation de la confidentialité (les paquets de données résistent aux dégradations et sont chiffrés)

Les modes de sécurité sont spécifiés en ajoutant du texte sous la forme "*option=mode*", où *option* correspond à *sec* et *mode* est le paramètre de sécurité. Par exemple :

```
hostname: shares default> set sharenfs="sec=krb5"
```

Remarque - Les valeurs de propriété CLI qui contiennent "=" doivent être indiquées entre guillemets.

Les combinaisons de types de Kerberos peuvent être spécifiées dans le paramètre du mode de sécurité. La combinaison de modes de sécurité permet aux clients de monter n'importe quel type de Kerberos répertorié, comme indiqué dans le tableau suivant.

TABLEAU 112 Combinaisons de types de Kerberos

Paramètre	Description
sys	Authentification système
krb5	Kerberos v5 uniquement : les clients doivent monter à l'aide de cette saveur.
krb5:krb5i	Kerberos v5, avec intégrité : les clients peuvent monter avec n'importe quelle saveur répertoriée.
krb5i	Kerberos v5 intégrité uniquement : les clients doivent monter à l'aide de cette saveur.
krb5:krb5i:krb5p	Kerberos v5, avec intégrité ou confidentialité : les clients peuvent monter avec n'importe quelle saveur répertoriée.

Paramètre	Description
krb5p	Kerberos v5 confidentialité uniquement : les clients peuvent monter à l'aide de cette variante.

Ports réservés

Pour définir des ports réservés pour l'authentification système, utilisez `resvport` comme indiqué dans cet exemple :

```
set sharenfs="sec=sys,rw,resvport"
```

Notez que `resvport` ne peut être utilisé qu'avec le mode de sécurité d'authentification système `sec=sys`.

Protocole SMB

Cette section aborde les sujets suivants :

- ["Propriétés de protocole SMB" à la page 414](#)
- ["Propriété de mise en cache côté client" à la page 415](#)
- ["Exceptions du mode de partage du protocole SMB" à la page 416](#)
- ["ACL au niveau du partage" à la page 418](#)

Pour plus d'informations sur le protocole SMB, consultez les rubriques suivantes :

- ["Configuration SMB" à la page 243](#)
- ["Propriétés des systèmes de fichiers" à la page 384](#)
- ["Propriétés des projets" à la page 377](#)

Pour plus d'informations sur les autres protocoles pris en charge, reportez-vous aux sections suivantes :

- ["Protocole NFS" à la page 408](#)
- ["Protocole HTTP" à la page 419](#)
- ["Protocole FTP" à la page 419](#)
- ["Protocole SFTP" à la page 419](#)
- ["Protocole TFTP" à la page 420](#)

Propriétés de protocole SMB

Chaque partage possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour ce partage. Ces propriétés peuvent être définies pour chaque partage ou héritées d'un partage contenu dans un projet. Le tableau suivant présente les propriétés de protocole SMB et leurs valeurs possibles.

TABLEAU 113 Propriétés de protocole SMB

Propriété	Valeur(s) CLI	Type de propriété	Description
Mode de partage	off/rw/ro	Hérité	Détermine si le partage est disponible uniquement pour la lecture, pour la lecture et l'écriture ou aucun des deux. Reportez-vous à la section "Exceptions du mode de partage du protocole SMB" à la page 416.
Nom de la ressource	resource_name/ on	Hérité	Affiche le nom utilisé par les clients SMB pour désigner ce partage. Le nom de ressource off indique qu'aucun client SMB ne peut accéder au partage et le nom de ressource on indique que le partage sera exporté avec le nom du système de fichiers.
Activer l'énumération basée sur les accès	abe	Hérité	Effectue des énumérations en fonction des accès lorsque l'option est activée.
Activer l'accès invité	guestok	Hérité	Autorise l'accès invité lorsque l'option est activée.
Est un espace de noms DFS	dfsroot	Hérité	Indique si ce partage est alloué en tant qu'espace de noms DFS autonome.
Stratégie de mise en mémoire cache côté client	csc	Hérité	Indique les options de configuration par partage fournies pour prendre en charge la mise en cache côté client. Pour plus d'informations, reportez-vous à la section "Propriété de mise en cache côté client" à la page 415.

Propriété de mise en cache côté client

La propriété de mise en cache côté client (csc) détermine si les fichiers et les programmes du partage sont mis en cache sur le client local pour être utilisés hors ligne lorsqu'ils sont déconnectés de l'appareil.

Valeur BUI	Valeur CLI	Description
Sans cache	none	Désactive la mise en cache côté client pour le partage. Aucun des fichiers ou des programmes du partage ne sont disponibles hors ligne.
Mise en cache manuelle	manual	Seuls les fichiers et les programmes spécifiés sont mis en cache sur le client local et sont disponibles hors ligne. En ligne, les programmes spécifiés sont exécutés depuis le client local. Les fichiers hors ligne ne sont pas automatiquement réintégrés lorsque le client local est à nouveau en ligne. Il s'agit de la valeur par défaut.
Mise en cache automatique de documents	documents	Tous les fichiers accédés à partir du partage sont mis en cache sur le

Valeur BUI	Valeur CLI	Description
		client local et disponibles hors ligne. Les fichiers sont automatiquement réintégrés lorsque le client local est à nouveau en ligne. Les programmes accédés à partir du partage ne sont pas disponibles hors ligne à moins qu'ils aient été mis en cache localement.
Mise en cache automatique de programmes	programs	Tous les programmes accédés à partir du partage sont mis en cache sur le client local et disponibles hors ligne. En ligne, les programmes sont exécutés depuis le client local. En outre, tous les fichiers accédés à partir du partage sont mis en cache sur le client local et disponibles hors ligne. Les fichiers sont automatiquement réintégrés lorsque le client local est à nouveau en ligne.

Exceptions du mode de partage du protocole SMB

Des exceptions aux modes de partage global peuvent être définies pour les clients ou les collections de clients en définissant des modes de partage spécifiques au client (ou des exceptions). Cela permet au client d'autoriser de façon générale l'accès en lecture/écriture pour tout un sous-réseau, tout en restreignant l'accès de certains clients. Les modes de partage spécifiques au client priment sur le mode de partage global. L'accès est accordé à un client en fonction du mode de partage spécifique au client spécifié dans une exception. En l'absence d'exceptions, l'accès est accordé au client sur la base du mode de partage global.

TABLEAU 114 Types de client

Type	Préfixe CLI	Description	Exemple
Hôte (FQDN) ou Netgroup	none	Client unique dont l'adresse IP est résolue en nom complet spécifié ou groupe réseau qui contient les noms complets vers lesquels est résolue l'adresse IP d'un client.	caji.sf.example.com
Domaine DNS	.	Tous les clients dont l'adresse IP est résolue en nom complet qui se termine par ce suffixe.	sf.example.com
Sous-réseau IPv4	@	Tous les clients dont les adresses IP sont comprises dans le sous-réseau IPv4 indiqué, en notation CIDR	192.168.20.0/22

Type	Préfixe CLI	Description	Exemple
Sous-réseau IPv6	@	Tous les clients dont les adresses IP sont comprises dans le sous-réseau IPv6 indiqué, en notation CIDR	2606:b400:410:d43::/64

Pour chaque client ou collection de clients, spécifiez si le client dispose d'un accès en lecture seule ou en lecture/écriture au partage.

Gestion des groupes réseau - Les groupes réseau peuvent être utilisés pour contrôler l'accès lors d'exportations NFS. La gestion de groupes réseau peut toutefois s'avérer complexe. A la place, vous pouvez envisager d'utiliser des règles de sous-réseau IP ou des règles de domaine DNS.

Si des groupes réseau sont utilisés, ils seront résolus à partir de NIS ou LDAP, selon le service activé. Si LDAP est utilisé, chaque groupe réseau doit se trouver à l'emplacement par défaut, ou=Netgroup,(Base DN) et doit utiliser le schéma standard.

En général, le composant nom d'utilisateur d'une entrée de groupe réseau n'a aucune incidence sur NFS ou SMB, contrairement au composant nom d'hôte. Les noms d'hôte contenus dans les groupes réseau doivent être canoniques et, s'ils ont été choisis à l'aide de DNS, ils doivent être complets. Concrètement, le sous-système NFS ou SMB tente de vérifier que l'adresse IP du client qui a fait la demande est résolue en nom d'hôte canonique qui correspond soit au nom de domaine complet (FQDN) indiqué, soit à un membre d'un des groupes réseau spécifiés. Cette correspondance doit être exacte, y compris concernant les composants de domaine. Dans le cas contraire, l'exception n'est pas valide et on passe à l'exception suivante. Pour plus d'informations sur la résolution du nom d'hôte, consultez la section [DNS](#).

Depuis la version logicielle 2013.1.0, les utilisateurs de clients UNIX peuvent appartenir à un maximum de 1 024 groupes sans aucune perte de performance. Les versions précédentes prenaient en charge jusqu'à 16 groupes par utilisateur de client UNIX.

Options des modes de partage et d'exception SMB

Dans la CLI, tous les modes de partage SMB et les exceptions sont spécifiés à l'aide d'une chaîne d'options unique pour la propriété `sharesmb`. Cette chaîne est une liste de valeurs séparées par des virgules. Elle doit commencer par `ro`, `rw`, `on` ou `off`, de la même manière que pour les modes de partage globaux décrits dans la BUI.

TABLEAU 115 Valeurs du mode de partage SMB (BUI et CLI)

Valeur BUI	Valeur CLI	Description
Aucune	<code>off</code>	Le mode de partage est désactivé.
Lecture/écriture	<code>on</code>	Le nom de partage correspond au nom d'ensemble de données, et le partage est en mesure de lire et écrire en l'absence d'exceptions SMB. S'il existe des exceptions SMB, le mode de partage est désactivé.

Valeur BUI	Valeur CLI	Description
	rw	Le nom de partage correspond au nom d'ensemble de données, et le partage est en mesure de lire et écrire.
Lecture seule	ro	Le nom de partage correspond au nom d'ensemble de données, et le partage est seulement en mesure de lire.

L'exemple suivant définit le mode de partage en lecture seule pour tous les clients. Les utilisateurs root sur tous les clients accèdent aux fichiers du partage comme s'ils étaient l'utilisateur générique "nobody".

```
set sharesmb=ro
```

Il est possible de spécifier des exceptions SMB supplémentaires en ajoutant du texte sous la forme "option=collection", où "option" correspond à ro ou rw. Vous ne pouvez pas autoriser un accès root avec des exceptions SMB. La collection est spécifiée par le caractère de préfixe provenant du tableau Types de client et par un nom de domaine/d'hôte DNS ou un numéro de réseau CIDR.

Par exemple, pour accorder un accès en lecture-écriture à tous les hôtes du domaine sf.example.com, saisissez :

```
set sharesmb="ro,rw=.sf.example.com"
```

Les noms de groupe réseau peuvent être utilisés partout où un nom d'hôte complet peut être utilisé. Par exemple, vous pouvez autoriser l'accès en lecture-écriture au groupe réseau "engineering" comme suit :

```
set sharesmb="ro,rw=engineering"
```

ACL au niveau du partage

Une liste de contrôle d'accès (ACL) au niveau du partage, lorsqu'elle est combinée avec l'ACL d'un fichier ou d'un répertoire dans le partage, détermine les autorisations en vigueur pour ce fichier. Par défaut, l'ACL octroie un contrôle total à tout le monde. L'ACL offre une couche supplémentaire de contrôle d'accès par rapport aux ACL sur les fichiers et permet de configurer plus précisément le contrôle d'accès. Cette propriété peut être définie uniquement lorsque le système de fichiers a été exporté en configurant le nom de ressource SMB. Si le système de fichiers n'est pas exporté via le protocole SMB, le paramétrage de l'ACL au niveau du partage n'a aucune conséquence.

Lorsque la propriété d'énumérations en fonction des accès est activée, les clients peuvent voir des entrées de répertoire des fichiers qu'ils ne peuvent pas ouvrir. Les entrées de répertoire sont filtrées uniquement lorsque le client n'a pas accès au fichier. Par exemple, si un client tente d'ouvrir un fichier avec un accès en lecture-écriture alors que l'ACL n'attribue qu'un accès en lecture, l'ouverture du fichier échoue mais ce fichier est quand même inclus dans la liste des entrées.

Pour plus d'informations sur les ACL, reportez-vous à la section ["Listes de contrôle d'accès des systèmes de fichiers"](#) à la page 420.

Protocole HTTP

Chaque partage possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour ce partage. Ces propriétés peuvent être définies pour chaque partage ou héritées d'un partage contenu dans un projet. Pour le protocole HTTP (`sharedav`), les utilisateurs peuvent définir le mode de partage pour déterminer si le système de fichiers est accessible en lecture seule (`ro`), en lecture-écriture (`rw` ou `on`), ou ni l'un ni l'autre (`off`).

Rubriques connexes

- ["Propriétés des projets"](#) à la page 377
- ["Propriétés des systèmes de fichiers"](#) à la page 384

Protocole FTP

Chaque partage possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour ce partage. Ces propriétés peuvent être définies pour chaque partage ou héritées d'un partage contenu dans un projet. Pour le protocole FTP (`shareftp`), les utilisateurs peuvent définir le mode de partage pour déterminer si le système de fichiers est accessible en lecture seule (`ro`), en lecture-écriture (`rw` ou `on`), ou ni l'un ni l'autre (`off`).

Rubriques connexes

- ["Propriétés des projets"](#) à la page 377
- ["Propriétés des systèmes de fichiers"](#) à la page 384

Protocole SFTP

Chaque partage possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour ce partage. Ces propriétés peuvent être définies pour chaque partage ou héritées d'un partage contenu dans un projet. Pour le protocole SFTP (`sharesftp`), les utilisateurs peuvent définir le mode de partage pour déterminer si le système de fichiers est accessible en lecture seule (`ro`), en lecture-écriture (`rw` ou `on`), ou ni l'un ni l'autre (`off`).

Rubriques connexes

- ["Propriétés des projets" à la page 377](#)
- ["Propriétés des systèmes de fichiers" à la page 384](#)

Protocole TFTP

Chaque partage possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour ce partage. Ces propriétés peuvent être définies pour chaque partage ou héritées d'un partage contenu dans un projet. Pour le protocole TFTP (`share:tftp`), les utilisateurs peuvent définir le mode de partage pour déterminer si le système de fichiers est accessible en lecture seule (`ro`), en lecture-écriture (`rw` ou `on`), ou ni l'un ni l'autre (`off`).

Rubriques connexes

- ["Propriétés des projets" à la page 377](#)
- ["Propriétés des systèmes de fichiers" à la page 384](#)

Listes de contrôle d'accès des systèmes de fichiers

Vous pouvez définir des options afin de contrôler le comportement ACL et l'accès au répertoire racine du système de fichiers.

Remarque - Les ACL ne sont disponibles que pour les systèmes de fichiers.

Pour plus d'informations sur ACL, reportez-vous aux rubriques suivantes :

- ["Accès au répertoire racine" à la page 420](#)
- ["Comportement ACL en cas de changement de mode" à la page 421](#)
- ["Comportement d'héritage ACL" à la page 422](#)
- ["ACL du répertoire racine" à la page 424](#)

Accès au répertoire racine

Pour définir un contrôle d'accès de base, accédez à **Partages > Partages > Accès au système de fichiers**. Il peut être géré in-band par n'importe quel protocole en cours d'utilisation mais vous pouvez également les spécifier ici si vous le souhaitez. Ces propriétés ne peuvent pas être modifiées sur un système de fichiers en lecture seule, car cela implique de modifier les métadonnées du répertoire root du système de fichiers.

- **Utilisateur** : propriétaire du répertoire root. Il peut être spécifié par son ID utilisateur ou son nom d'utilisateur. Pour plus d'informations sur le mappage des utilisateurs UNIX

et Windows, reportez-vous à la section [Mappage des identités](#). Pour les accès à NFS sur UNIX, l'utilisateur peut être modifié à partir du client à l'aide de la commande `chown`.

- **Groupe** : groupe du répertoire root. Il peut être spécifié par son ID de groupe ou son nom de groupe. Pour plus d'informations sur le mappage des groupes UNIX et Windows, reportez-vous à la section [Mappage des identités](#). Pour les accès à NFS sur UNIX, l'utilisateur peut être modifié à partir du client à l'aide de la commande `chgrp`.
- **Autorisations d'accès** : autorisations d'accès UNIX standard sur le répertoire racine. Pour les accès à NFS sur UNIX, l'utilisateur peut être modifié à partir du client à l'aide de la commande `chmod`. Il existe trois types d'autorisations différentes.

Type d'accès	Description
Utilisateur	Utilisateur actuellement propriétaire du répertoire.
Groupe	Groupe actuellement propriétaire du répertoire.
Autre	Tous les autres accès.

Pour chaque type d'accès, les autorisations suivantes peuvent être octroyées.

Type		Description
Lecture	R	Autorisation de répertorier le contenu du répertoire.
Ecriture	W	Autorisation de créer des fichiers dans le répertoire.*
Exécution	X	Autorisation de rechercher des entrées dans le répertoire. Si des utilisateurs possèdent cette autorisation mais qu'ils n'ont pas d'autorisation de lecture, ils peuvent accéder aux fichiers en spécifiant leur nom, mais ils ne peuvent pas répertorier le contenu du répertoire.

Rubriques connexes

- ["Comportement ACL en cas de changement de mode" à la page 421](#)
- ["Comportement d'héritage ACL" à la page 422](#)
- ["ACL du répertoire racine" à la page 424](#)

Comportement ACL en cas de changement de mode

Lorsqu'une ACL standard est modifiée via la commande `chmod(2)` à l'aide des autorisations standard Unix utilisateur/groupe/autre, la demande de changement de mode simplifié interagit

de différentes façons avec l'ACL existante selon la manière dont la propriété est paramétrée. Pour modifier le comportement de l'ACL en cas de changement de mode, reportez-vous à la section Modification d'un projet - [BUI](#), [CLI](#).

TABLEAU 116 Valeurs du changement de mode

Valeur BUI	Valeur CLI	Description
Ignorer l'ACL	discard	Toutes les entrées ACL qui ne représentent pas le mode du répertoire ou du fichier sont rejetées. Il s'agit du comportement par défaut.
ACL de masque avec mode	mask	Les autorisations sont réduites, de sorte qu'elles ne dépassent pas les autorisations du groupe, à moins qu'il ne s'agisse d'une entrée utilisateur qui possède le même UID que le propriétaire du fichier ou du répertoire. Dans ce cas, les autorisations ACL sont réduites de sorte qu'elles ne dépassent pas les autorisations du propriétaire. La valeur de masque permet également de préserver l'ACL au fur et à mesure des changements de modes successifs, à condition qu'une opération de définition explicite de l'ACL n'ait pas été effectuée.
Ne pas modifier l'ACL	passthrough	Aucune modification n'est apportée à l'ACL, excepté la génération des entrées d'ACL nécessaires pour représenter le nouveau mode du fichier ou du répertoire.

Rubriques connexes

- ["ACL du répertoire racine" à la page 424](#)
- ["Comportement d'héritage ACL" à la page 422](#)
- ["ACL du répertoire racine" à la page 424](#)

Comportement d'héritage ACL

Lorsqu'un fichier ou un répertoire est créé, il est possible qu'il hérite des paramètres ACL existants d'un répertoire parent. Cette propriété contrôle la manière dont cet héritage fonctionne. Ces paramètres de propriété n'affectent en général que les entrées ACL marquées comme pouvant être héritées. Les autres entrées ne sont pas propagées, quelle que soit le paramétrage de cette propriété. Cependant, toutes les entrées ACL triviales peuvent être héritées si elles sont utilisées avec SMB. Une ACL triviale correspond aux entrées owner/group/other

traditionnelles d'Unix. Pour modifier le comportement d'héritage de l'ACL, reportez-vous à la section Modification d'un projet - [BUI](#), [CLI](#).

TABLEAU 117 Valeurs du comportement d'héritage ACL

Valeur BUI	Valeur CLI	Description
Ne pas hériter des entrées	discard	Aucune entrée ACL n'est héritée. Le fichier ou répertoire est créé en fonction des clients et protocoles utilisés.
Hériter uniquement les entrées de refus	noallow	Seules les entrées ACL pouvant être héritées et indiquant les autorisations "deny" sont héritées.
Hériter de tout sauf d'"écrire l'ACL" et de "modifier le propriétaire"	restricted	Les autorisations "write_acl" et "write_owner" sont supprimées si l'entrée ACL est héritée. Sinon, les entrées pouvant être héritées ne sont pas modifiées. Il s'agit de la valeur par défaut.
Hériter de toutes les entrées	passthrough	Toutes les entrées pouvant être héritées le sont. Le mode "passthrough" est généralement utilisé pour permettre la création avec un mode identique de tous les fichiers de "données" au sein d'une structure de répertoires. Un administrateur définit l'héritage ACL de sorte que tous les fichiers sont créés avec un même mode, tel que 0664 ou 0666.
Hériter de tout sauf d'"exécuter" lorsqu'il n'est pas spécifié	passthrough-x	Ce paramètre fonctionne comme le paramètre 'passthrough', à l'exception des entrées ACL owner, group et everyone qui n'héritent de l'autorisation d'exécution que si le mode de création du fichier demande également le bit d'exécution. Le paramètre "passthrough" fonctionne comme prévu pour les fichiers de données, mais vous souhaitez parfois inclure le bit d'exécution à partir du mode de création du fichier dans l'ACL héritée. Prenons par exemple un fichier de sortie généré à partir d'outils tels que "cc" ou "gcc". Si l'ACL héritée n'inclut pas le bit d'exécution, l'exécutable de sortie du compilateur n'est pas exécutable tant que les autorisations du fichier ne sont pas modifiées à l'aide de chmod (1).
Hériter de tout sauf du mode de conservation à partir du client	passthrough-mode-preserve	Les entrées d'ACL pouvant être héritées sont héritées, mais le mode de création spécifié par l'application

Valeur BUI	Valeur CLI	Description
		est préservé. Les bits d'héritage sont donc préservés, de sorte que SMB crée des ACL qui interagissent bien avec les partages accédés simultanément sur NFS et SMB. Cette valeur de propriété n'est disponible qu'après l'application de la mise à jour différée pour l'option passthrough avec préservation du mode. Pour plus d'informations, reportez-vous à la section " Deferred Updates " dans <i>Oracle ZFS Storage Appliance Customer Service Manual</i> .

Lorsque vous utilisez SMB pour créer un fichier dans un répertoire avec une ACL triviale, toutes les entrées d'ACL sont héritées. Le résultat suivant se produit :

- Les bits d'héritage s'affichent différemment dans SMB ou NFS. Lorsque vous consultez le répertoire ACL dans SMB, les bits d'héritage sont affichés. Dans NFS, les bits d'héritage ne sont pas affichés.
- Lorsqu'un fichier est créé dans un répertoire à l'aide de SMB, ses entrées ACL sont affichées comme étant héritées. Mais lorsqu'elles sont affichées dans NFS, le répertoire ne contient pas d'entrées ACL pouvant être héritées.
- Si vous modifiez l'ACL et qu'elle n'est plus triviale en ajoutant par exemple une entrée de contrôle d'accès (ACE), ce comportement ne se produit pas.
- Si l'ACL est modifiée à l'aide de SMB, les bits d'héritage synthétiques précédents sont transformés en bits d'héritage réels dans l'ACL obtenue.

Rubriques connexes

- "[Propriétés des projets](#)" à la page 377

ACL du répertoire racine

Les accès plus fins aux fichiers et aux répertoires sont gérés via les listes de contrôle d'accès (ACL). Une ACL décrit les autorisations octroyées aux utilisateurs et aux groupes, le cas échéant. L'appareil prend en charge les ACL de type NFSv4, également accessibles sur SMB. Les ACL POSIX-draft (utilisés par NFSv3) ne sont pas prises en charge. Certaines ACL triviales peuvent être représentées sur NFSv3, mais des modifications complexes de l'ACL peuvent entraîner un comportement indéfini lors de l'accès sur NFSv3.

De la même manière que la propriété accès au répertoire root, cette propriété affecte le répertoire root du système de fichiers. Les ACL peuvent être contrôlées via la gestion de protocole in-band mais la BUI propose un moyen de définir l'ACL uniquement pour le répertoire root du système de fichiers. Il n'existe aucun moyen de paramétrer l'ACL du répertoire root dans la CLI. Vous pouvez utiliser les outils de gestion in-band si la BUI n'est

pas une option. La modification de l'ACL n'affecte pas les fichiers et les répertoires existants dans le système de fichiers. En fonction du comportement d'héritage des ACL, il est possible que ces paramètres soient ou non hérités lorsque vous créez de nouveaux fichiers et répertoires. Toutefois, toutes les entrées ACL sont héritées si SMB est utilisé pour créer un fichier ou un répertoire avec une ACL triviale.

Une ACL est composée d'un nombre indéfini d'entrées de contrôle d'accès (ACE). Chaque ACE décrit un type/une cible, un mode, un ensemble d'autorisations et des indicateurs d'héritage. Les ACE sont appliquées dans l'ordre, en partant du début de l'ACL, pour déterminer si une action spécifique est autorisée. Pour plus d'informations sur la configuration in-band des ACL via les protocoles de données, consultez la documentation client appropriée. L'interface BUI de gestion des ACL et les effets sur le répertoire racine y sont également décrits.

TABLEAU 118 Partages : Types d'ACL

Type	Description
Propriétaire	Propriétaire actuel du répertoire. Si le propriétaire est modifié, cette ACE s'applique au nouveau propriétaire.
Groupe	Groupe actuel du répertoire. Si le groupe est modifié, cette ACE s'applique au nouveau groupe.
Tout le monde	Tous les utilisateurs
Utilisateurs nommés	Utilisateur désigné dans le champ 'cible'. Vous pouvez spécifier un ID d'utilisateur ou un nom qui peut être résolu par la configuration de service de noms actuelle.
Groupe nommé	Groupe désigné dans le champ 'cible'. Vous pouvez spécifier un ID de groupe ou un nom qui peut être résolu par la configuration de service de noms actuelle.

TABLEAU 119 Partages : Modes d'ACL

Mode	Description
 Autoriser	Les autorisations sont explicitement octroyées à la cible ACE.
 Refuser	Les autorisations sont explicitement refusées à la cible ACE.

TABLEAU 120 Partages : Autorisations ACL

	Autorisations	Description
	Lecture	
(r)	Lire les données/Lister le contenu du répertoire	Autorisation de répertorier le contenu d'un répertoire. Lorsqu'elle est héritée d'un fichier, autorisation de lire les données du fichier.
(x)	Exécuter le fichier/Parcourir le répertoire	Autorisation de parcourir (rechercher) les entrées du répertoire. Lorsqu'elle est héritée d'un fichier, autorisation d'exécuter le fichier.

	Autorisations	Description
(a)	Lire les attributs	Autorisation de lire les attributs basiques (non ACL) d'un fichier. Les attributs basiques sont considérés comme étant les attributs de niveau stat et, après l'octroi de cette autorisation, l'utilisateur peut exécuter les équivalents ls et stat.
(R)	Lire les attributs étendus	Autorisation de lire les attributs étendus d'un fichier ou de réaliser une recherche dans le répertoire des attributs étendus.
	Ecriture	
(w)	Ecrire des données/Ajouter un fichier	Autorisation d'ajouter un fichier au répertoire. Lorsqu'elle est héritée d'un fichier, autorisation de modifier les données du fichier n'importe où dans la plage d'offset. Cette autorisation inclut la capacité d'agrandir le fichier ou d'écrire dans un offset arbitraire.
(p)	Ajouter des données/Ajouter un sous-répertoire	Autorisation de créer un sous-répertoire dans un répertoire. Lorsqu'elle est héritée d'un fichier, autorisation de modifier les données du fichier, mais uniquement en partant de la fin du fichier. Cette autorisation (lorsqu'elle est appliquée aux fichiers) n'est pas pris en charge pour le moment.
(d)	Suppression	Autorisation de supprimer un fichier.
(D)	Supprimer l'enfant	Autorisation de supprimer un fichier dans un répertoire. A partir de la version logicielle 2011.1, si le sticky bit est défini, un fichier enfant peut être supprimé uniquement par le propriétaire du fichier.
(A)	Ecrire des attributs	Autorisation de modifier les horodatages associés à un fichier ou à un répertoire.
(W)	Ecrire des attributs étendus	Autorisation de créer des attributs étendus ou d'écrire dans le répertoire des attributs étendus.
	Admin	
(c)	Lire ACL/Autorisations	Autorisation de lire l'ACL.
(C)	Ecrire ACL/Autorisations	Autorisation d'écrire l'ACL ou de modifier les modes d'accès standard.
(o)	Modifier le propriétaire	Autorisation de modifier le propriétaire.
	Héritage	

	Autorisations	Description
(f)	Appliquer aux fichiers	S'applique à tous les fichiers récemment créés dans un répertoire.
(d)	Appliquer aux répertoires	S'applique à tous les répertoires récemment créés dans un répertoire.
(i)	Ne pas appliquer à soi-même	L'ACE actuelle n'est pas appliquée au répertoire actuel, mais à ses enfants. Cet indicateur impose que le type "Appliquer aux fichiers" ou "Appliquer aux répertoires" soit défini.
(n)	Ne pas appliquer au-delà des enfants	L'ACE actuelle doit s'appliquer à un seul niveau de l'arborescence (seulement aux enfants immédiats). Cet indicateur impose que le type "Appliquer aux fichiers" ou "Appliquer aux répertoires" soit défini.

Si les autorisations Windows par défaut sont utilisées au moment de la création du partage, une ACL est créée pour le répertoire racine du partage avec les trois entrées suivantes :

TABLEAU 121 Partages : Entités du répertoire racine

Type	Action	Accès
Propriétaire	Allow	Contrôle total
Groupe	Allow	Lecture et exécution
Tout le monde	Allow	Lecture et exécution

Utilisation des schémas

En plus des propriétés standard intégrées, vous pouvez configurer autant de propriétés supplémentaires disponibles sur tous les partages et projets que vous souhaitez. Des types de base sont attribués à ces propriétés à des fins de validation et sont héritées, comme la plupart des propriétés standard. Les valeurs ne sont jamais utilisées par le logiciel, de quelque manière que ce soit, et sont réservées à l'utilisateur final. Le schéma de propriété est global au niveau du système, transversal pour tous les pools et synchronisé entre les pairs de cluster.

Pour utiliser des schémas, reportez-vous aux sections suivantes :

- ["Création d'un schéma \(BUI\)" à la page 428](#)
- ["Création d'un schéma \(CLI\)" à la page 428](#)
- ["Propriétés de schéma" à la page 429](#)

▼ Création d'un schéma (BUI)

1. Accédez à Partages > Schéma.
2. Cliquez sur l'icône "+" pour ajouter une nouvelle propriété à la liste de propriétés de schéma.
3. Saisissez le nom de la propriété ("contact")
4. Saisissez une description de la propriété ("Contact propriétaire").
5. Sélectionnez un type pour la nouvelle propriété ("Adresse électronique").
6. Cliquez sur Appliquer.
7. Accédez à un partage ou à un projet existant.
8. Modifiez la propriété "Contact propriétaire" sous la section "Propriétés personnalisées".

▼ Création d'un schéma (CLI)

1. Accédez au contexte de schéma (`shares schema`).
2. Créez une nouvelle propriété nommée "contact" (`create contact`)
3. Définissez la description de la propriété (`set description="Owner Contact"`)
4. Définissez le type de propriété (`set type=EmailAddress`)
5. Validez les modifications (`commit`)
6. Accédez à un partage ou à un projet existant.
7. Définissez la propriété "custom:contact"

Exemple 16 Exemples de schéma

Le contexte de schéma est accessible sous Shares > Schema.

```
carp:> shares schema
carp:shares schema> show
Properties:

NAME          TYPE          DESCRIPTION
owner         EmailAddress  Owner Contact
```

Chaque propriété est un enfant du contexte de schéma, utilisant le nom de la propriété comme jeton. Pour créer une propriété, exécutez la commande `create` :

```
carp:shares schema> create department
carp:shares schema department (uncommitted)> get
      type = String
      description = department
carp:shares schema department (uncommitted)> set description="Department Code"
      description = Department Code (uncommitted)
carp:shares schema department (uncommitted)> commit
carp:shares schema>
```

Dans le contexte d'une propriété particulière, les champs peuvent être définis à l'aide des commandes CLI standard :

```
carp:shares schema> select owner
carp:shares schema owner> get
      type = EmailAddress
      description = Owner Contact
carp:shares schema owner> set description="Owner Contact Email"
      description = Owner Contact Email (uncommitted)
carp:shares schema owner> commit
```

Une fois que les propriétés personnalisées ont été définies, elles sont accessibles de la même façon que toute autre propriété ayant le nom "custom:<property>" :

```
carp:shares default> get
...
      custom:department = 123-45-6789
      custom:owner =
...
carp:shares default> set custom:owner=bob@corp
      custom:owner = bob@corp (uncommitted)
carp:shares default> commit
```

Propriétés de schéma

Pour définir les propriétés personnalisées, accédez à l'élément de navigation Partages > Schéma. Le schéma actuel est affiché sous forme de liste, et les entrées peuvent être saisies ou supprimées selon les besoins. Chaque propriété contient les champs suivants :

TABLEAU 122 Champs des propriétés de schéma

Champ	Description
NOM	Nom de cette propriété dans la CLI. Il doit contenir uniquement des caractères alphanumériques ou les caractères ". : _ \"

Champ	Description
DESCRIPTION	Nom de cette propriété dans la BUI. Il peut contenir des caractères arbitraires et est utilisé dans la section d'aide de la CLI.
TYPE	Type de propriété (à des fins de validation). Ce doit être un des types décrits ci-dessous.

Les types valides pour les propriétés sont les suivants.

TABLEAU 123 Types de propriétés valides

Type BUI	Type CLI	Description
String	String	Données de chaîne arbitraires. Cela équivaut à l'absence de validation.
Integer	Integer	Entier positif ou négatif
Entier positif	PositiveInteger	Entier positif
Boolean	Boolean	Valeur true/false. Dans la BUI, cela se présente sous la forme d'une case à cocher, tandis que dans la CLI, la valeur doit être "true" ou "false".
Adresse électronique	EmailAddress	Adresse électronique. Seule une validation syntaxique minimale est effectuée.
Nom d'hôte ou IP	Hôte	Nom d'hôte DNS ou adresse IP (v4 ou v6) valide.

Une fois définies, les propriétés sont disponibles dans l'onglet des propriétés générales, avec la description fournie dans le tableau des propriétés. Les propriétés étant identifiées par leur nom dans la CLI, le fait de renommer une propriété entraîne la suppression de tous les paramètres existants sur le système. Une propriété supprimée puis renommée avec son nom d'origine renvoie toujours vers les valeurs précédemment définies. La modification des types de propriétés, bien que prise en charge, peut produire des résultats indéfinis sur les propriétés existantes sur le système. Les propriétés existantes conservent leurs paramètres actuels, même si elles n'étaient pas valides du fait du nouveau type de propriété.

Migration shadow

Les administrateurs ont souvent l'occasion de déplacer des données d'un emplacement à un autre. Au sens le plus abstrait, ce problème englobe de nombreux cas d'utilisation qui vont de la réplication des données entre les serveurs à la conservation des données utilisateur sur les ordinateurs portables en synchronisation avec les serveurs. Il existe de nombreux outils externes qui permettent de réaliser ces tâches mais l'appareil est équipé de deux solutions intégrées pour la migration des données, adaptées aux cas d'utilisation les plus courants. La première, appelée réplication, est destinée à la réplication des données entre un ou plusieurs appareils et est détaillée dans la section "[Réplication distante](#)" à la page 473. La seconde solution est la fonction migration shadow décrite ici.

La migration shadow désigne un processus qui permet de migrer les données à partir de sources NAS externes dans le but de remplacer ou d'éliminer les données d'origine au terme de la migration. Cette solution est principalement utilisée lors de l'intégration d'un nouvel appareil dans un environnement existant pour la prise en charge des droits de partage de fichiers d'un autre serveur, mais de nombreuses autres utilisations sont possibles et détaillées ci-dessous.

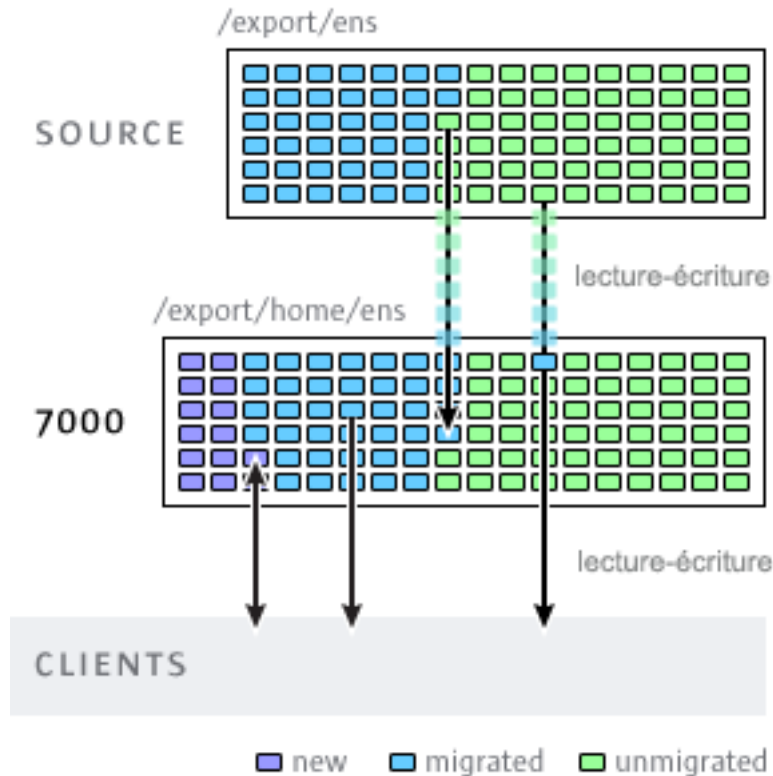
Pour utiliser la migration shadow, reportez-vous aux sections suivantes :

- "[Présentation de la migration shadow](#)" à la page 432
- "[Création d'un système de fichiers shadow](#)" à la page 435
- "[Gestion de la migration en arrière-plan](#)" à la page 435
- "[Gestion des erreurs de migration](#)" à la page 435
- "[Contrôle de la progression de la migration](#)" à la page 436
- "[Annulation d'une migration](#)" à la page 436
- "[Instantanés de systèmes de fichiers shadow](#)" à la page 437
- "[Sauvegarde de systèmes de fichiers shadow](#)" à la page 437
- "[Réplication de systèmes de fichiers shadow](#)" à la page 437
- "[Migration de systèmes de fichiers locaux](#)" à la page 438
- "[Utilisation des analyses de migration shadow](#)" à la page 438
- "[Test d'une migration shadow potentielle à l'aide de la CLI](#)" à la page 439
- "[Migration des données à partir d'un serveur NFS actif à l'aide de la CLI](#)" à la page 439

Présentation de la migration shadow

La migration shadow utilise l'interposition mais est intégrée dans l'appareil et ne requiert pas de machine physique séparée. Lorsque des systèmes de fichiers sont créés, ils peuvent éventuellement "masquer" un répertoire existant, en local ou sur NFS. Dans ce scénario, le temps d'indisponibilité est programmé, l'appareil source X est placé en mode lecture seule puis un partage est créé, dans lequel la propriété shadow est définie. Les clients sont ensuite mis à jour pour pointer vers un nouveau partage sur l'appareil Oracle ZFS Storage Appliance. Les clients peuvent ensuite accéder à l'appareil en mode lecture-écriture.

FIGURE 32 Migration shadow



Une fois que la propriété shadow est définie, les données sont migrées localement en arrière-plan à partir de l'appareil source. Si un client envoie une requête pour un fichier qui n'a pas été encore migré, l'appareil migre automatiquement ce fichier vers un serveur local avant de répondre à la requête. Au début, cela peut causer une latence pour certaines requêtes client.

mais, dès qu'un fichier est migré, tous les accès sont effectués en local sur l'appareil et ont des performances natives. Il arrive souvent que la taille de la mémoire de travail d'un système de fichiers soit inférieure à la taille totale. Ainsi, une fois que cette mémoire de travail a été migrée, il n'y a aucun impact perceptible sur les performances, quelle que soit la taille native totale sur la source.

Toutefois, la migration shadow présente un inconvénient : elle requiert une validation avant la fin de la migration des données. Cela dit, c'est le cas de toutes les méthodes d'interposition. Pendant la migration, certaines parties des données existent à deux endroits, ce qui signifie que les sauvegardes sont difficiles et qu'il est possible que les instantanés soient incomplets et/ou qu'ils n'existent que sur un seul hôte. C'est pourquoi il est très important que toutes les migrations effectuées entre deux hôtes soient d'abord testées minutieusement afin de s'assurer que la gestion des identités et les contrôles d'accès sont définis correctement. Cela n'implique pas de tester la totalité de la migration des données mais il faut vérifier que les fichiers ou les répertoires qui ne sont pas lisibles par tous sont migrés correctement, que les ACL (si elles existent) sont préservées et enfin que les identités sont représentées correctement dans le nouveau système.

La migration shadow étant implémentée à l'aide de données sur disque dans le système de fichiers, il n'y a pas de base de données externe et aucune donnée n'est stockée en local hors du pool de stockage. Si un pool bascule dans un cluster ou que les deux disques système subissent une défaillance et qu'un nouveau noeud de tête est requis, toutes les données nécessaires pour poursuivre la migration shadow sans interruption sont conservées dans le pool de stockage.

Le paragraphe suivant liste les restrictions applicables à la source shadow :

- Afin de migrer les données correctement, le système de fichiers ou le répertoire source *doit être en lecture seule*. Les modifications apportées à la source des fichiers peuvent ou non être propagées selon le moment et les modifications apportées à la structure de répertoires peuvent provoquer des erreurs irréversibles sur l'appareil.
- La migration shadow prend uniquement en charge la migration à partir de sources NFS. Ce sont les systèmes de fichiers NFSv4 qui donnent les meilleurs résultats. Les migrations NFSv2 et NFSv3 sont possibles, mais les ACL seront perdues au cours du processus et les fichiers trop volumineux pour NFSv2 ne peuvent pas être migrés à l'aide de ce protocole. La migration à partir de sources SMB n'est pas prise en charge.
- La migration shadow des LUN n'est pas prise en charge.

Au cours de la migration, si le client accède à un fichier ou à un répertoire qui n'a pas encore été migré, cela a des conséquences visibles. Le paragraphe suivant liste les sémantiques de système de fichiers shadow :

- Pour les répertoires, les demandes de client sont bloquées jusqu'à ce que l'infrastructure de métadonnées soit créée sur la cible de migration pour tous les répertoires intermédiaires pour lesquels l'infrastructure n'est pas encore établie. Pour les fichiers, seule la partie du fichier faisant l'objet de la requête est migré et plusieurs clients peuvent migrer différentes parties d'un fichier au même moment.

- Les fichiers et les répertoires peuvent être arbitrairement renommés, supprimés ou remplacés sur le système de fichiers shadow sans que cela ait un effet sur le processus de migration.
- Pour les fichiers qui sont des liens physiques, il est possible que le nombre de liens physiques ne corresponde pas à la source tant que la migration n'est pas terminée.
- La majorité des attributs de fichier sont migrés à la création du répertoire mais la taille sur disque (st_nblocks dans la structure stat UNIX) n'est pas disponible tant qu'une opération de lecture ou d'écriture n'est pas effectuée sur le fichier. La taille logique est correcte mais une commande du(1) (disk usage) ou toute autre commande signale une valeur de taille nulle jusqu'à ce que le contenu des fichiers soit effectivement migré.
- Si l'appareil est réinitialisé, la migration reprend là où elle s'est arrêtée. Alors qu'il n'est pas nécessaire de migrer les données à nouveau, il peut être nécessaire de parcourir certaines parties du système de fichiers déjà migrées et il est possible que cette interruption ait un impact sur la durée totale de la migration.
- La migration des données fait appel à des attributs étendus privés sur les fichiers. En règle générale, ils ne sont pas visibles sauf sur le répertoire root du système de fichiers ou par le biais des instantanés. L'ajout, la modification ou la suppression d'attributs étendus qui commencent par SUNWshadow peuvent avoir des effets inconnus sur le processus de migration et peuvent entraîner un état endommagé ou incomplet. De plus, l'état filesystem-wide est stocké dans le répertoire .SUNWshadow à la racine du système de fichiers. Toute modification apportée à ce contenu aura le même effet.
- Au terme de la migration d'un système de fichiers, une alerte est envoyée et l'attribut shadow est supprimé, de même que toutes les métadonnées applicables. A ce stade, le système de fichiers est similaire à un système de fichiers normal.
- Les données peuvent être migrées depuis plusieurs systèmes de fichiers dans un seul système de fichiers en utilisant les montages des clients automatiques NFSv4 (parfois appelés "montages en miroir") ou les montages locaux imbriqués.

Afin de migrer des informations d'identité des fichiers, y compris les ACL, il est nécessaire de respecter les règles suivantes :

- Les appareils de migration source et cible doivent avoir la même configuration de service de noms.
- Les appareils de migration source et cible doivent avoir le même domaine mapid NFSv4.
- L'appareil de migration source doit prendre en charge NFSv4. L'utilisation de NFSv3 est possible, mais cela peut entraîner une perte d'informations. Les informations d'identité de base (propriétaire et groupe) et les autorisations POSIX sont conservées, mais toutes les ACL sont perdues.
- La source de la migration peut être exportée avec les autorisations root vers l'appareil.

Si vous voyez des fichiers ou des répertoires "sans propriétaire", cela signifie en général que les services de noms ne sont pas définis correctement sur l'appareil ou que le domaine mapid NFSv4 est différent. Si des messages d'erreurs s'affichent indiquant "autorisation refusée" lorsque vous parcourez les systèmes de fichiers auxquels le client devrait avoir accès, ceci est probablement dû à l'échec de l'exportation de la source de migration avec les autorisations root.

Création d'un système de fichiers shadow

La source de la migration shadow peut uniquement être définie si un système de fichiers a été créé. Dans la BUI, cette option est disponible dans la boîte de dialogue de création d'un système de fichiers. Dans la CLI, cette option est disponible dans la propriété shadow. La propriété prend l'une des formes suivantes :

- **Local** - file:///<path>
- **NFS** - nfs://<host>/<path>

La BUI autorise également la forme alternative <host>:/<path> pour les montages NFS, qui correspond à la syntaxe utilisée dans les systèmes UNIX. La BUI définit également la partie de protocole du paramètre (file:// ou nfs://) via l'utilisation d'un menu déroulant. Lorsque vous créez un système de fichiers, le serveur vérifie que le chemin existe et qu'il peut être monté.

Gestion de la migration en arrière-plan

Lorsqu'un partage est créé, sa migration démarre automatiquement en arrière-plan, parallèlement au traitement des requêtes intégrées. La migration est contrôlée par le service de migration shadow. Le seul paramètre global que vous pouvez modifier est le nombre de threads dédiés à cette tâche. L'augmentation du nombre de threads implique un plus grand parallélisme aux dépens des ressources supplémentaires.

Il est possible de désactiver le service de migration shadow mais cela ne doit être fait qu'à des fins de test ou lorsque la migration shadow active submerge le système au point qu'il doit être temporairement arrêté. Lorsque le service de migration shadow est désactivé, les requêtes synchrones sont tout de même migrées comme nécessaire, mais aucune migration en arrière-plan ne se produit. Aucune migration shadow ne peut arriver à terme si ce service est désactivé, même si l'intégralité du contenu du système de fichiers est lue manuellement. Il est vivement recommandé de toujours conserver ce service actif.

Gestion des erreurs de migration

Il est très important de tester la migration et de rechercher d'éventuelles erreurs car la validation de nouvelles écritures sur le serveur est nécessaire pour que la migration shadow puisse se terminer correctement. Les erreurs détectées pendant la migration en arrière-plan sont conservées et affichées dans la BUI dans le statut de la migration shadow. Les erreurs rencontrées pendant d'autres migrations synchrones ne sont pas suivies, mais seront comptabilisées une fois que le processus en arrière-plan aura accédé au fichier concerné. Pour chaque fichier, le nom du fichier distant ainsi que l'erreur spécifique sont conservés. Pour afficher cette liste détaillée, cliquez sur l'icône d'information située près du compte d'erreur.

La liste des erreurs n'est pas mise à jour lorsque les erreurs sont résolues, mais simplement supprimée au terme d'une migration effective.

La migration shadow n'est pas terminée tant que tous les fichiers ne sont pas migrés sans erreur. Si des erreurs se produisent, la migration en arrière-plan relance la migration jusqu'à ce qu'elle réussisse. Cela permet à l'administrateur de résoudre toutes les erreurs (telles que les problèmes d'autorisation), de laisser la migration s'effectuer et de s'assurer de sa réussite. Si la migration ne peut pas aboutir en raison d'erreurs persistantes, elle peut être annulée tout en conservant dans le système de fichiers les données dont la migration a réussi. Cette solution ne doit être utilisée qu'en dernier recours car, une fois la migration annulée, elle ne peut pas reprendre.

Contrôle de la progression de la migration

Pour surveiller l'avancée de la migration shadow, l'appareil fournit des statistiques telles que :

- Taille des données transférées jusqu'à présent
- Estimation de la taille restante à migrer
- Durée de migration jusqu'à présent
- Erreurs de migration

Au début de la migration, l'appareil obtient les statistiques du système de fichiers source et calcule la taille de ce système. Il utilise ces valeurs pour fournir une représentation visuelle raisonnablement exacte de l'avancée de la migration et une estimation des données restantes à migrer. Le nombre d'octets restants est une estimation basée sur l'hypothèse qu'un système de fichiers entier est en cours de migration. Si une seule partie du système de fichiers source est migrée, l'estimation du nombre d'octets restants n'est pas exacte. Si le système de fichiers source comporte des systèmes de fichiers imbriqués, la taille totale du système de fichiers est recalculée quand le point de montage imbriqué est découvert pendant la migration et le nombre d'octets restants est ré-estimé en fonction du total nouvellement calculé. L'estimation du nombre d'octets restants peut être inexacte si le système de fichiers source utilise la compression. Ces valeurs sont mises à disposition dans la BUI et la CLI via les propriétés du système de fichiers standard et les propriétés du noeud de migration shadow (ou panneau UI).

Remarque - Lors de la migration d'un fichier fragmenté (fichier contenant des blocs vides), la taille du fichier cible sera inférieure à celle du fichier source. La migration shadow n'écrit pas les blocs vides dans le fichier cible, utilisant ainsi moins d'espace.

Annulation d'une migration

La migration peut être annulée, mais cela ne doit être fait que dans certaines circonstances extrêmes lorsque la source n'est plus disponible. Une fois qu'elle a été annulée, la migration ne peut pas reprendre. L'objectif principal est de permettre à la migration de se terminer lorsque

des erreurs irrémédiables sont détectées dans la source. Si la totalité du système de fichiers a été migré (sauf quelques fichiers ou répertoires) et qu'il n'existe aucun moyen de corriger ces erreurs (c.-à-d. que la source est endommagée de manière permanente), l'annulation de la migration permet au système de fichiers de reprendre le statut 'normal'.

Pour annuler la migration dans la BUI, cliquez sur l'icône de fermeture située à côté de la barre de progression dans la colonne de gauche du partage en question. Dans la CLI, migrez le noeud shadow sous le système de fichiers et exécutez la commande `cancel`.

Instantanés de systèmes de fichiers shadow

Il est possible de réaliser des instantanés des systèmes de fichiers, cependant l'état de ce qui est contenu dans l'instantané est arbitraire. Les fichiers qui n'ont pas été migrés seront absents et il est possible que les détails d'implémentation (tels que les attributs étendus SUNWshadow) soient visibles dans l'instantané. Cet instantané peut être utilisé pour restaurer des fichiers individuels déjà migrés ou modifiés depuis le début de la migration. C'est pour cela qu'il est recommandé de conserver tous les instantanés sur la source jusqu'au terme de la migration afin que les fichiers non migrés puissent être restaurés à partir de la source, si nécessaire. Selon la stratégie de conservation, il peut être nécessaire d'étendre la conservation sur la source afin de remplir les exigences de service. Bien qu'il soit possible de prendre des instantanés, ces derniers ne peuvent ni être restaurés ni plus jouer le rôle de source d'un clone.

Sauvegarde de systèmes de fichiers shadow

Il est possible de sauvegarder les systèmes de fichiers qui sont en train de migrer des données shadow à l'aide de NDMP, exactement comme n'importe quel autre système de fichiers. Le paramètre shadow est préservé avec le flux de sauvegarde mais sera restauré uniquement si une restauration complète du système de fichiers est effectuée et que le partage n'existe pas déjà. La restauration de fichiers individuels à partir de ce type de flux de sauvegarde ou la restauration dans des systèmes de fichiers existants peut entraîner un état incohérent ou l'altération des données. Pendant sa restauration intégrale, le système de fichiers est dans un état incohérent (au-delà de l'incohérence normale d'une restauration partielle) et la migration shadow ne sera pas activée. Ce n'est que lorsque la restauration est terminée que le paramètre shadow est restauré. Si la source shadow est absente ou qu'elle a été supprimée, l'administrateur peut consulter les erreurs et les corriger de manière appropriée.

Réplication de systèmes de fichiers shadow

Il est possible de répliquer les systèmes de fichiers qui sont en train de migrer des données shadow à l'aide du mécanisme classique, mais seules les données migrées sont envoyées au

flux de données. Ainsi, la partie distante contient seulement une partie des données, ce qui peut entraîner un état incohérent. Le paramètre shadow étant envoyé avec le flux de réplication, lorsque la cible distante bascule, elle conserve le même paramètre shadow. Comme pour la restauration d'un flux de sauvegarde NDMP, il est possible que ce paramètre soit incorrect dans le contexte d'une cible distante. Après le basculement de la cible, l'administrateur peut observer les erreurs et corriger le paramètre shadow de manière appropriée pour le nouvel environnement.

Migration de systèmes de fichiers locaux

En plus de son objectif principal de migration des données à partir de sources distantes, ce mécanisme peut également permettre de migrer des données à partir du système de fichiers local vers un autre système de fichiers de l'appareil. Il peut être utilisé pour changer des paramètres qui ne peuvent pas être modifiés autrement, notamment pour créer une version compressée d'un système de fichiers ou modifier ultérieurement la propriété recordsize d'un système de fichiers. Dans ce modèle, l'ancien partage (ou sous-répertoire au sein d'un partage) est mis en lecture seule ou mis de côté et un nouveau partage est créé avec la propriété shadow à l'aide du protocole file. Le client accède à ce nouveau partage et les données sont écrites à l'aide des paramètres du nouveau partage.

Utilisation des analyses de migration shadow

En plus du contrôle standard par partage, il est également possible de contrôler la migration shadow à l'échelle du système grâce à l'analyse. Les analyses de migration shadow sont disponibles sous la catégorie "Déplacement de données". Trois types de statistiques classiques sont disponibles :

- **Demandes de migration shadow** : cette statistique effectue le suivi des demandes de fichiers ou de répertoires qui ne sont pas mis en cache et considérés comme locaux par le système de fichiers. Elle ne prend pas en compte la migration ou non des fichiers et des répertoires et peut être utilisée pour suivre le temps de latence engagé dans le cadre de la migration shadow, ainsi que la progression de la migration en arrière-plan. Elle peut être ventilée par fichier, partage, projet ou latence. Elle comprend actuellement la migration synchrone et asynchrone (en arrière-plan). Il n'est donc pas possible d'afficher uniquement la latence visible par les clients.
- **Octets de migration shadow** : cette statistique effectue le suivi des octets transférés dans le cadre de la migration de contenu d'un fichier ou d'un répertoire. Elle ne s'applique pas aux métadonnées (attributs étendus, ACL, etc.). Elle donne une approximation du volume de données transférées, mais les ensembles de données source contenant une grande quantité de métadonnées affichent une bande passante excessivement faible. Vous pouvez observer la bande passante complète en consultant les analyses réseau. Cette statistique peut être ventilée par nom de fichier local, partage ou projet.

- **Opérations de migration shadow** : cette statistique effectue le suivi des opérations qui nécessitent d'accéder au système de fichiers source. Elle peut être utilisée pour suivre la durée de latence des requêtes provenant de la source de la migration shadow. Elle peut être ventilée par fichier, partage, projet ou latence.

▼ Test d'une migration shadow potentielle à l'aide de la CLI

Avant d'essayer d'effectuer une migration totale, il est important de tester la migration pour s'assurer que l'appareil possède les autorisations appropriées et que les attributs de sécurité sont convertis correctement. Une fois que vous êtes certain que la configuration basique est fonctionnelle, les systèmes de fichiers peuvent être configurés pour la migration finale.

Remarque - Lors de la planification de la capacité, n'oubliez pas de prendre en compte les quotas de groupes d'utilisateurs/par défaut car ceux-ci peuvent être dépassés si la source a une taille plus grande que la destination. De plus, la migration shadow échouera si la cible manque d'espace.

1. **Configurez la source de sorte que l'appareil possède les droits d'accès root au partage. En général, cette action implique l'ajout d'une exception NFS basée sur l'hôte ou le paramétrage d'un mappage utilisateur anonyme (ce dernier ayant des conséquences plus importantes en matière de sécurité).**
2. **Créez un partage sur le système de fichiers local avec l'attribut shadow défini sur "nfs://<host>/<snapshotpath>" dans la CLI ou simplement "<host>/<snapshotpath>" dans la BUI (avec le protocole NFS sélectionné). L'instantané doit être une copie en lecture seule de la source. Si aucun instantané n'est disponible, une source en lecture-écriture peut être utilisée mais cela peut causer des erreurs non définies.**
3. **Vérifiez que le contenu de fichiers et le mappage d'identité sont correctement préservés en parcourant la structure de fichiers.**
4. **Si la source des données est en lecture seule (comme pour un instantané), laissez la migration se terminer et vérifiez qu'aucune erreur ne s'est produite pendant le transfert.**

▼ Migration des données à partir d'un serveur NFS actif à l'aide de la CLI

Appliquez la procédure suivante pour migrer les données à partir d'un serveur NFS actif à l'aide de la CLI. Notez que la migration shadow échoue si elle rencontre des fichiers sous procfs ou des fichiers des types suivants : doors, sockets et event ports.

1. **Planifiez la durée d'indisponibilité durant laquelle les clients peuvent être placés en mode quiescence et reconfigurés pour pointer vers un nouveau serveur.**
2. **Configurez la source de sorte que l'appareil possède les droits d'accès root au partage. En général, cette action implique l'ajout d'une exception NFS basée sur l'hôte ou le paramétrage d'un mappage utilisateur anonyme (ce dernier ayant des conséquences plus importantes en matière de sécurité).**
3. **Configurez la source en lecture seule. Techniquement, cette étape est facultative mais il est bien plus facile de garantir la compatibilité si les clients mal configurés ne sont pas en mesure d'écrire dans la source au cours de la migration.**
4. **Créez un partage sur le système de fichiers local avec l'attribut shadow défini sur "nfs://<host>/<path>" dans la CLI ou simplement "<host>/<path>" dans la BUI (avec le protocole NFS sélectionné).**
5. **Configurez à nouveau les clients de sorte qu'ils pointent vers le partage local sur l'appareil.**

A ce stade, la migration shadow doit s'exécuter en arrière-plan et les requêtes client doivent être traitées de manière appropriée. Vous pouvez observer la progression de la migration comme expliqué plus haut. Vous pouvez créer plusieurs systèmes de fichiers au cours d'une même interruption programmée au moyen de l'écriture du script de la CLI (Interface de ligne de commande).

Instantanés et clones

NOTICE RELATIVE A LA LICENCE : *Le clonage peut faire l'objet d'une évaluation à titre gratuit, mais la fonction requiert l'achat d'une licence distincte pour un usage en production. Au terme de la période d'évaluation, il convient d'acheter une licence pour cette fonction ou de la désactiver. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

Les instantanés et les clones permettent d'effectuer des copies ponctuelles d'un partage ou projet. Ces copies peuvent servir de sauvegardes ou de versions de travail alternatives.

Un instantané est une copie en lecture seule d'un système de fichiers, d'un LUN ou d'un projet. Réaliser un instantané d'un projet revient à prendre un instantané de tous les partages au sein du projet. Un instantané n'occupe pas d'espace supplémentaire lors de sa création mais, étant donné que le partage actif est modifié, l'instantané prend de l'espace supplémentaire, avec un maximum correspondant à la taille du partage au moment de la prise de l'instantané.

Un clone désigne une copie accessible en écriture d'un instantané de système de fichiers ou de LUN et peut être considéré comme un partage indépendant. Les clones de projets ne sont pas pris en charge. De la même manière qu'un instantané, un clone ne consomme pas d'espace supplémentaire lors de sa création, mais lorsque de nouvelles données sont écrites dans le clone, l'espace requis pour ces modifications est associé au clone.

Vous pouvez réaliser des instantanés manuellement, ou vous pouvez définir un calendrier pour que des instantanés soient pris de manière automatique toutes les demi-heures, heures, jours, semaines ou mois. Certains instantanés sont pris par l'appareil de manière automatique au cours des mises à jour de réplication ; ceux-ci s'affichent alors sur la page des instantanés et leur nom comprend `.ndmp` et `.rr`.

Pour plus d'informations sur la gestion de l'espace pour les instantanés, reportez-vous à la section suivante :

["Gestion de l'espace pour les instantanés" à la page 443](#)

Pour prendre des instantanés manuels ou planifier des instantanés automatiques de projets ou de partages, effectuez les tâches suivantes :

- ["Réalisation d'un instantané \(BUI\)" à la page 444](#)

-
- ["Réalisation d'un instantané \(CLI\)" à la page 445](#)
 - ["Planification des instantanés \(BUI\)" à la page 446](#)
 - ["Planification des instantanés \(CLI\)" à la page 448](#)
 - ["Définition d'une étiquette d'instantané planifié \(BUI\)" à la page 450](#)
 - ["Définition d'une étiquette d'instantané planifié \(CLI\)" à la page 451](#)

Vous pouvez réaliser des clones d'un instantané, qui peuvent s'avérer utiles pour créer de nombreuses versions de travail d'un même partage. Pour créer des clones, effectuez les tâches suivantes :

- ["Clonage d'un instantané \(BUI\)" à la page 466](#)
- ["Clonage d'un instantané \(CLI\)" à la page 468](#)
- ["Clonage d'un clone" à la page 470](#)
- ["Clonage d'un package de réplication \(BUI\)" à la page 508](#)
- ["Clonage d'un package de réplication \(CLI\)" à la page 512](#)

Pour déterminer les relations entre les instantanés et les clones existants, effectuez les tâches suivantes :

- ["Affichage des clones d'un instantané \(BUI\)" à la page 470](#)
- ["Affichage des clones d'un instantané \(CLI\)" à la page 471](#)
- ["Affichage de l'origine d'un clone \(BUI\)" à la page 471](#)
- ["Affichage de l'origine d'un clone \(CLI\)" à la page 472](#)

Pour afficher et modifier des instantanés, des calendriers d'instantanés et des stratégies de conservation d'instantanés, effectuez les tâches suivantes :

- ["Affichage des instantanés et des calendriers \(BUI\)" à la page 451](#)
- ["Affichage des instantanés et des calendriers \(CLI\)" à la page 452](#)
- ["Modification du nom d'un instantané \(BUI\)" à la page 460](#)
- ["Modification du nom d'un instantané \(CLI\)" à la page 461](#)
- ["Modification d'une stratégie de conservation des instantanés \(BUI\)" à la page 454](#)
- ["Modification d'une stratégie de conservation des instantanés \(CLI\)" à la page 454](#)

Vous pouvez consulter le contenu des instantanés de système de fichier via le répertoire de système de fichiers `.zfs/snapshot`. Les instantanés de LUN ne sont pas directement accessibles. Cependant, ils peuvent être utilisés comme cible de restauration ou comme source d'un clone. Pour gérer et ouvrir le répertoire `.zfs/snapshot`, effectuez les tâches suivantes :

- ["Accès à un répertoire d'instantanés masqué du système de fichiers \(CLI\)" à la page 459](#)
- ["Affichage du répertoire d'instantanés du système de fichiers \(BUI\)" à la page 457](#)
- ["Affichage du répertoire d'instantanés du système de fichiers \(CLI\)" à la page 458](#)

- ["Accès à un répertoire d'instantanés visible du système de fichiers \(CLI\)" à la page 460](#)

Vous pouvez utiliser un instantané existant pour restaurer un système de fichiers ou un LUN à l'état précis qui était le sien au moment de la prise de l'instantané. Pour restaurer un instantané existant à partir d'un système de fichiers, d'un LUN ou d'un projet, effectuez les tâches suivantes :

- ["Restauration d'un instantané \(BUI\)" à la page 462](#)
- ["Restauration d'un instantané \(CLI\)" à la page 463](#)

Pour détruire des instantanés, effectuez les tâches suivantes :

- ["Destruction d'un instantané \(BUI\)" à la page 464](#)
- ["Destruction d'un instantané \(CLI\)" à la page 465](#)

Gestion de l'espace pour les instantanés

Les instantanés constituent un dilemme intéressant pour la gestion des données. Ils représentent l'ensemble de blocs physiques référencés par un partage à un moment donné. Initialement, un instantané ne consomme pas d'espace supplémentaire. Cependant, lorsque les nouvelles données sont remplacées dans le nouveau partage, les blocs du partage actif contiennent uniquement les nouvelles données et les blocs plus anciens seront "détenus" par les instantanés les plus récents (et éventuellement par les anciens également). Il est possible que les instantanés consomment de plus en plus d'espace à mesure que le contenu diverge dans le partage actif. Si vous prenez un instantané d'un système de fichiers de n'importe quelle taille et que vous écrivez à nouveau la totalité des données dans le système de fichiers, vous devez conserver des références au double de données d'origine.

Chaque instantané est associé à deux statistiques : l'espace unique et l'espace référencé. La quantité d'espace référencé correspond à l'espace total consommé par le système de fichiers au moment où l'instantané a été pris. Il représente la taille maximale théorique de l'instantané s'il restait la référence unique pour tous les blocs de données. L'espace unique désigne la quantité d'espace physique référencé uniquement par l'instantané en cours. Lorsqu'un instantané est détruit, l'espace unique est rendu disponible au reste du pool.

Notez que l'espace consommé par la totalité des instantanés n'est pas égal à la somme de l'espace unique dans l'ensemble des instantanés. Avec un partage et un seul instantané, tous les blocs doivent être référencés par l'instantané ou le partage (ou les deux). Cependant, avec plusieurs instantanés, il est possible de référencer un bloc en fonction de certains sous-ensembles d'instantanés. Par exemple, un fichier est créé, deux instantanés X et Y sont réalisés, le fichier est supprimé et un autre instantané Z est pris. Ainsi, les blocs contenus dans le fichier sont détenus par X et Y mais pas par Z. Dans ce cas, la destruction de Z ne libère pas d'espace, contrairement à la destruction de X et Y. C'est pourquoi la destruction de tout instantané peut affecter l'espace unique référencé par les instantanés voisins, même si l'espace total consommé par les instantanés diminue toujours.

Le volume total d'un projet ou d'un partage prend toujours en compte l'espace consommé par tous les instantanés bien que la ventilation de l'utilisation soit également disponible. Des quotas et des réservations peuvent être définis au niveau du projet pour appliquer des contraintes physiques à l'espace total. D'autre part, il est possible de définir des quotas et des réservations au niveau du système de fichiers et ces paramètres peuvent s'appliquer seulement aux données référencées ou à toutes les données.

C'est l'environnement d'administration qui permet de définir si les quotas et les réservations doivent être appliqués uniquement aux données référencées ou à toutes les données physiques. Si les utilisateurs ne contrôlent pas leurs instantanés (c'est-à-dire qu'une programmation de prise d'instantanés automatique a été mise en place pour eux), les quotas n'incluent généralement pas les instantanés dans le calcul. Autrement, l'utilisateur pourrait manquer d'espace et ne pas comprendre pourquoi les fichiers ne peuvent pas être supprimés. Si vous ne possédez pas une bonne compréhension des instantanés ou des moyens de les gérer, vous ne pourrez sans doute pas régler ce type de situation sans l'intervention d'un administrateur. Dans ce scénario, les instantanés représentent un coût de dépassement pris en compte dans les opérations du système afin de fournir une capacité de sauvegarde. D'autre part, dans certains environnements, les utilisateurs se voient facturer leur consommation d'espace physique et les instantanés représentent une option pour fournir un certain niveau de sauvegarde correspondant aux exigences de ces utilisateurs au vu du taux de résiliation de leurs ensembles de données. Dans ces environnements, il est plus judicieux d'appliquer les quotas calculés en fonction de la totalité des données physiques, y compris des instantanés. Les utilisateurs comprennent le coût des instantanés et peuvent obtenir des moyens de les gérer activement (également grâce aux rôles dédiés sur l'appareil).

Gestion des instantanés générés par l'utilisateur

La propriété "Conserver les instantanés utilisateurs sur la cible" vous permet de gérer les instantanés générés par l'utilisateur de manière indépendante sur les appareils source et cible. Lorsque cette option est activée, tous les instantanés générés par l'utilisateur restent sur la cible, même si l'instantané d'origine est supprimé de la source. Tant que cette propriété est activée, les instantanés générés par l'utilisateur ne sont pas détruits sur la cible. Tous les instantanés conservés générés par l'utilisateur, qui ne sont plus nécessaires, doivent être supprimés de manière explicite de l'appareil cible. Pour plus d'informations, reportez-vous à la section Destruction d'un instantané - [BUI](#) ou [CLI](#).

Rubriques connexes

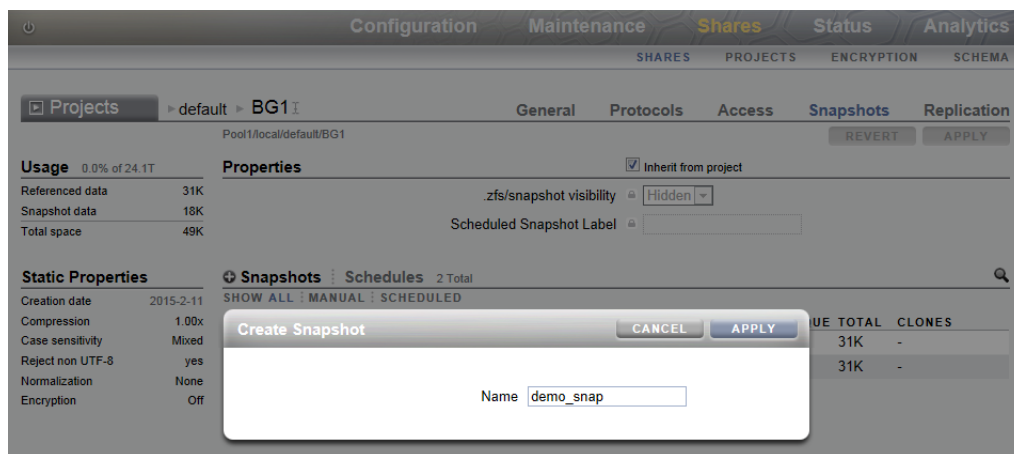
- ["Gestion de l'espace pour les partages" à la page 400](#)
- ["Utilisation de la réplication pour la sauvegarde disque à disque" à la page 528](#)

▼ Réalisation d'un instantané (BUI)

Utilisez la procédure suivante pour prendre un instantané manuel d'un système de fichiers, d'un LUN ou d'un projet.

Pour planifier des instantanés automatiques à intervalles réguliers, reportez-vous à la section ["Planification des instantanés \(BUI\)"](#) à la page 446.

1. **Accédez au partage ou au projet dont vous souhaitez prendre un instantané.**
 - a. **Pour réaliser un instantané d'un système de fichiers, accédez à Partages > Partages.**
 - b. **Pour réaliser un instantané d'un LUN, accédez à Partages > Partages, puis cliquez sur le LUN.**
 - c. **Pour réaliser un instantané d'un projet, accédez à Partages > Projets.**
2. **Déplacez le curseur de la souris sur le partage ou projet et cliquez sur l'icône de modification .**
3. **Cliquez sur l'onglet Snapshot.**
4. **Cliquez sur l'icône d'ajout  en regard de Instantanés.**
5. **Saisissez le nom de l'instantané.**



6. **Cliquez sur APPLIQUER.**

▼ Réalisation d'un instantané (CLI)

Utilisez la procédure suivante pour prendre un instantané manuel d'un système de fichiers, d'un LUN ou d'un projet.

Pour planifier des instantanés automatiques à intervalles réguliers, reportez-vous à la section ["Planification des instantanés \(CLI\)" à la page 448](#).

1. Accédez au partage ou au projet dont vous souhaitez prendre un instantané.

- a. **Pour réaliser un instantané d'un projet, accédez à shares et sélectionnez le projet.**

```
hostname:shares> select myproject
hostname:shares myproject>
```

- b. **Pour réaliser un instantané d'un système de fichiers ou d'un LUN, accédez à shares et sélectionnez le projet contenant le partage, puis sélectionnez ce dernier.**

```
hostname:shares> select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```

2. Saisissez snapshots.

```
hostname:shares myproject/demo_share> snapshots
```

3. Utilisez la commande snapshot suivie du nom que vous souhaitez attribuer au nouvel instantané.

```
hostname:shares myproject/demo_share snapshots> snapshot demo_snap
```

▼ Planification des instantanés (BUI)

Utilisez la procédure suivante pour configurer des instantanés automatiques d'un système de fichiers, d'un LUN ou d'un projet et définissez une stratégie de conservation pour ces instantanés.

Il est possible de prendre des instantanés automatiques toutes les demi-heures, heures, jours, semaines ou mois. Ils sont nommés `.auto[-<snaplabel>]-<timestamp>`. Dans la colonne Création de la liste Instantanés, les heures sont affichées à l'heure locale (navigateur client). Cependant, les horaires sont stockés au format UTC et ne prennent pas en compte les changements d'heure en hiver et en été. Par exemple, un instantané planifié pour 10 heures PST est stocké et exécuté à 18 heures UTC. Il s'agit de l'heure qui figure dans le nom de l'instantané en tant qu'horodatage.

Les instantanés automatiques peuvent être définis sur un projet ou un partage, mais pas sur les deux en même temps. Autrement, il serait impossible de garantir le bon fonctionnement des deux calendriers en raison de la superposition des calendriers et des stratégies de conservation. La suppression d'un intervalle ou la modification de sa stratégie de conservation entraîne

la destruction immédiate de tous les instantanés automatiques non inclus dans le nouveau calendrier. Les instantanés automatiques ayant des clones sont ignorés.

Remarque - Les versions précédentes du logiciel permettaient de définir la fréquence des instantanés automatiques en minutes. C'est pour éviter que les utilisateurs ajoutent une pression supplémentaire sur leur système que cette fonction a été retirée dans la version 2010.Q3. En cas de restauration du logiciel, les minutes existantes sont préservées. Les instances précédentes expirent en fonction du calendrier existant, mais aucun instantané supplémentaire ne sera pris. Une alerte est envoyée si un partage ou un projet possédant ce type de fréquence est détecté.

1. **Accédez au partage ou projet.**
 - a. **Pour planifier des instantanés d'un système de fichiers, accédez à Partages > Partages.**
 - b. **Pour planifier des instantanés d'un LUN, accédez à Partages > Partages, puis cliquez sur le LUN.**
 - c. **Pour planifier des instantanés d'un projet, accédez à Partages > Projets.**
2. **Déplacez le curseur de la souris sur le partage ou projet et cliquez sur l'icône de modification .**
3. **Cliquez sur l'onglet Snapshot.**
4. **Cliquez sur Calendriers.**
5. **Cliquez sur l'icône d'ajout  en regard de Calendriers.**
6. **Définissez chaque champ de manière appropriée.**
 - a. **Définissez la fréquence sur une demi-heure, une heure, un jour, une semaine ou un mois pour indiquer la fréquence des prises d'instantanés automatiques.**
 - b. **Définissez le moment précis des prises d'instantanés automatiques.**

Pour les instantanés pris toutes les demi-heures ou toutes les heures, vous pouvez choisir le temps (en minutes) au bout duquel l'instantané est pris une fois la demi-heure ou l'heure écoulée. Pour les prises d'instantanés quotidiennes, vous pouvez indiquer l'heure et la minute auxquelles l'instantané est réalisé, et pour les prises d'instantanés hebdomadaires ou mensuelles, vous pouvez indiquer le jour, l'heure et la minute.
 - c. **Sélectionnez la propriété "Conserver au plus" pour indiquer le nombre d'instantanés à préserver, ou désactivez la case à cocher pour ne pas définir de stratégie de conservation.**

Les instantanés automatiques peuvent être conservés indéfiniment (sauf pour les instantanés pris toutes les demi-heures et toutes les heures qui sont limités respectivement à 48 et 24), ou ils peuvent être limités à un certain nombre. Lorsque le nombre d'instantanés dépasse la valeur spécifiée ici, les instantanés les plus anciens sont supprimés en premier.

7. Cliquez sur **APPLIQUER**.

▼ Planification des instantanés (CLI)

Utilisez la procédure suivante pour configurer des instantanés automatiques d'un partage et définissez une stratégie de conservation pour ces instantanés.

Il est possible de prendre des instantanés automatiques toutes les demi-heures, heures, jours, semaines ou mois. Ils sont nommés `.auto[-<snaplabel>]-<timestamp>`. Cependant, les horaires de création des instantanés sont stockés au format UTC et ne prennent pas en compte les changements d'heure en hiver et en été. Par exemple, un instantané planifié pour 10 heures PST est stocké et exécuté à 18 heures UTC. Il s'agit de l'heure qui figure dans le nom de l'instantané en tant qu'horodatage.

Les instantanés automatiques peuvent être définis sur un projet ou un partage, mais pas sur les deux en même temps. Autrement, il serait impossible de garantir le bon fonctionnement des deux calendriers en raison de la superposition des calendriers et des stratégies de conservation. La suppression d'un intervalle ou la modification de sa stratégie de conservation entraîne la destruction immédiate de tous les instantanés automatiques non inclus dans le nouveau calendrier. Les instantanés automatiques ayant des clones sont ignorés.

Remarque - Les versions précédentes du logiciel permettaient de définir la fréquence des instantanés automatiques en minutes. C'est pour éviter que les utilisateurs ajoutent une pression supplémentaire sur leur système que cette fonction a été retirée dans la version 2010.Q3. En cas de restauration du logiciel, les minutes existantes sont préservées. Les instances précédentes expirent en fonction du calendrier existant, mais aucun instantané supplémentaire ne sera pris. Une alerte est envoyée si un partage ou un projet possédant ce type de fréquence est détecté.

1. **Accédez à shares et sélectionnez le projet ou partage dont vous souhaitez prendre un instantané.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```

2. **Saisissez snapshots automatic.**

```
hostname:shares myproject/demo_share> snapshots automatic
hostname:shares myproject/demo_share snapshots automatic>
```


3. Exécutez la commande **create** pour saisir un contexte de calendrier non validé.

```
hostname:shares myproject/demo_share snapshots automatic> create
hostname:shares myproject/demo_share snapshots automatic (uncommitted)>
```

4. Exécutez la commande **set** pour définir chaque champ de manière appropriée.

a. Définissez la fréquence sur **halfhour**, **hour**, **day**, **week** ou **month** pour indiquer la fréquence des prises d'instantanés automatiques.

b. Réglez le jour, l'heure et la minute pour définir le moment précis des prises d'instantanés automatiques.

Pour les instantanés pris toutes les demi-heures ou toutes les heures, vous pouvez choisir le temps (en minutes) au bout duquel l'instantané est pris une fois la demi-heure ou l'heure écoulée. Pour les prises d'instantanés quotidiennes, vous pouvez indiquer l'heure et la minute auxquelles l'instantané est réalisé, et pour les prises d'instantanés hebdomadaires ou mensuelles, vous pouvez indiquer le jour, l'heure et la minute.

c. Définissez la propriété **keep** sur le nombre d'instantanés à conserver pour ce calendrier.

Les instantanés automatiques peuvent être conservés indéfiniment (sauf pour les instantanés pris toutes les demi-heures et toutes les heures qui sont limités respectivement à 48 et 24), ou ils peuvent être limités à un certain nombre. Lorsque le nombre d'instantanés dépasse la valeur spécifiée ici, les instantanés les plus anciens sont supprimés en premier.

```
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set frequency=day
frequency = day (uncommitted)
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set hour=14
hour = 14 (uncommitted)
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set minute=30
minute = 30 (uncommitted)
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> set keep=7
keep = 7 (uncommitted)
```

Vous pouvez exécuter la commande **get** pour afficher les paramètres non validés actuels.

```
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> get
frequency = day (uncommitted)
day = (unset)
hour = 14 (uncommitted)
minute = 30 (uncommitted)
keep = 7 (uncommitted)
```

5. Saisissez la commande **commit** pour valider les modifications et créer le calendrier de prise d'instantanés automatique.

```
hostname:shares myproject/demo_share snapshots automatic (uncommitted)> commit
```

Vous pouvez utiliser la commande `list` pour afficher votre nouveau calendrier.

```
hostname:shares myproject/demo_share snapshots automatic> list
NAME                FREQUENCY    DAY          HH:MM KEEP
automatic-000       day          -            14:30    7
```

6. Saisissez `done` pour terminer.

```
hostname:shares myproject/demo_share snapshots automatic> done
hostname:shares myproject/demo_share snapshots>
```

▼ Définition d'une étiquette d'instantané planifié (BUI)

Utilisez la procédure suivante pour définir une étiquette pour les instantanés planifiés d'un système de fichiers, d'un LUN ou d'un projet.

Cette propriété facultative ajoute une étiquette définie par l'utilisateur à chaque instantané planifié et est vide par défaut. Cette étiquette peut être définie soit pour un partage individuel, soit pour un projet et héritée par ses partages, mais pas les deux.

Les étiquettes d'instantané peuvent aider à identifier le projet ou le partage pour lequel un instantané a été pris. Par exemple, "project1:share1" peut indiquer un instantané planifié pris sur le partage share1 au sein du projet project1. Les étiquettes peuvent comporter jusqu'à 35 caractères alphanumériques et inclure les caractères spéciaux `_ - . : .`

- 1. Accédez au partage ou au projet pour lequel vous souhaitez définir une étiquette d'instantané planifié.**
 - a. Pour définir une étiquette pour un système de fichiers, accédez à **Partages > Partages**.
 - b. Pour définir une étiquette pour un LUN, accédez à **Partages > Partages**, puis cliquez sur le LUN.
 - c. Pour définir une étiquette pour un projet, accédez à **Partages > Projets**.
- 2. Déplacez le curseur de la souris sur le partage ou projet approprié et cliquez sur l'icône de modification .**
- 3. Cliquez sur l'onglet Snapshot.**
- 4. Sous Propriétés, saisissez l'étiquette que vous souhaitez définir dans le champ Etiquette d'instantané planifié.**
- 5. Cliquez sur APPLIQUER pour enregistrer la modification.**

Cette étiquette sera incluse dans le nom de tous les instantanés planifiés pris désormais. L'étiquette est placée avant l'horodatage, de sorte que le nom de l'instantané présente la forme suivante : `.auto-<snaplabel>-<timestamp>`.

▼ Définition d'une étiquette d'instantané planifié (CLI)

Utilisez la procédure suivante pour définir une étiquette pour les instantanés planifiés d'un système de fichiers, d'un LUN ou d'un projet.

Cette propriété facultative ajoute une étiquette définie par l'utilisateur à chaque instantané planifié et est vide par défaut. Cette étiquette peut être définie soit pour un partage individuel, soit pour un projet et héritée par ses partages, mais pas les deux.

Les étiquettes d'instantané peuvent aider à identifier le projet ou le partage pour lequel un instantané a été pris. Par exemple, "project1:share1" peut indiquer un instantané planifié pris sur le partage share1 au sein du projet project1. Les étiquettes peuvent comporter jusqu'à 35 caractères alphanumériques et inclure les caractères spéciaux `_ - . : .`

1. **Accédez à shares et sélectionnez le système de fichiers, le LUN ou le projet pour lequel vous souhaitez définir l'étiquette.**

```
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```

2. **Exécutez la commande `set snaplabel` pour créer une étiquette d'instantané planifié.**

```
hostname:shares myproject/demo_share> set snaplabel=myproject:demo_share
```

▼ Affichage des instantanés et des calendriers (BUI)

Utilisez la procédure suivante pour afficher les instantanés et les calendriers d'instantanés automatiques pour un système de fichiers, un LUN ou un projet particulier.

1. **Accédez au partage ou projet.**
 - a. **Pour afficher des instantanés et des calendriers d'instantanés d'un système de fichiers, accédez à Partages > Partages.**
 - b. **Pour afficher des instantanés et des calendriers d'instantanés d'un LUN, accédez à Partages > Partages, puis cliquez sur le LUN.**
 - c. **Pour afficher des instantanés et des calendriers d'instantanés d'un projet, accédez à Partages > Projets.**

2. **Déplacez le curseur de la souris sur le partage ou projet et cliquez sur l'icône de modification .**
3. **Cliquez sur l'onglet Snapshot.**
4. **Affichez les instantanés et les calendriers d'instantanés.**
 - a. **Affichez les instantanés de ce partage sous Instantanés et, si vous le souhaitez, sélectionnez MANUEL ou PROGRAMME pour afficher uniquement les instantanés manuels ou uniquement les instantanés planifiés.**
 Pour chaque instantané, vous pouvez afficher le nom (NAME), la date et l'heure de création (CREATION), la quantité d'espace unique utilisée par l'instantané (UNIQUE), la quantité d'espace totale référencée par l'instantané (TOTAL) et le nombre de clones de l'instantané (CLONES).
 - b. **Cliquez sur Calendriers pour afficher les calendriers d'instantanés automatiques de ce partage.**
 Pour chaque calendrier, vous pouvez afficher la fréquence de prise d'un instantané, le jour et l'heure précis de la prise de l'instantané et le nombre d'instantanés conservés.

▼ Affichage des instantanés et des calendriers (CLI)

Utilisez la procédure suivante pour afficher les instantanés et les calendriers d'instantanés automatiques pour un système de fichiers, un LUN ou un projet particulier.

1. **Accédez à shares et sélectionnez le projet ou le partage.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```
2. **Saisissez snapshots.**

```
hostname:shares myproject/demo_share> snapshots
hostname:shares myproject/demo_share snapshots>
```
3. **Affichez les instantanés et les calendriers d'instantanés à l'aide des commandes appropriées.**
 - a. **Saisissez list pour afficher une liste des instantanés de ce partage ou projet.**

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
```

```
hostname:shares myproject/demo_share snapshots>
```

Vous pouvez sélectionner un instantané et utiliser la commande `list` pour afficher les propriétés suivantes :

- `creation` : date et heure de création de l'instantané au format UTC
- `numclones` : nombre de clones de l'instantané
- `isauto` : indique si l'instantané a été créé manuellement (`false`) ou avec un calendrier d'instantané automatique (`true`)
- `pool` : pool de stockage dans lequel se trouve l'instantané
- `canonical_name` : emplacement de l'instantané
- `shadowsnap` : indique si l'instantané a été pris au cours d'une migration shadow (`true`) ou pas (`false`)
- `space_unique` : quantité d'espace unique utilisée par l'instantané
- `space_data` : quantité d'espace totale référencée par l'instantané

```
hostname:shares myproject/demo_share snapshots> select demo_snap1
```

```
hostname:shares myproject/demo_share snapshots demo_snap1> list
```

Properties:

```
    creation = Thu Jan 22 2015 20:19:49 GMT+0000(UTC)
    numclones = 1
    isauto = false
    pool = pool1
    canonical_name = pool1/local/myproject/demo_share@demo_snap1
    shadowsnap = false
    space_unique = 0
    space_data = 31K
```

b. Saisissez `automatic` et utilisez la commande `list` pour afficher une liste des calendriers d'instantanés automatiques de ce partage ou projet.

```
hostname:shares myproject/demo_share snapshots> automatic
```

```
hostname:shares myproject/demo_share snapshots automatic> list
```

Properties:

```
    convert = false
```

Automatics:

NAME	FREQUENCY	DAY	HH:MM	KEEP
automatic-000	day	-	00:00	4
automatic-001	month	01	00:00	12

▼ Modification d'une stratégie de conservation des instantanés (BUI)

Utilisez la procédure suivante pour modifier une stratégie de conservation des instantanés pour un système de fichiers, un LUN ou un projet. Les calendriers d'instantanés automatiques contiennent des stratégies de conservation des instantanés.

1. **Accédez au projet ou partage approprié.**
 - a. Si le calendrier s'applique à un projet, accédez à **Partages > Projets**.
 - b. Si le calendrier s'applique à un système de fichiers, accédez à **Partages > Partages**.
 - c. Si le calendrier s'applique à un LUN, accédez à **Partages > Partages et cliquez sur le LUN**.
2. **Déplacez le curseur de la souris sur le projet ou partage approprié et cliquez sur l'icône de modification .**
3. **Cliquez sur l'onglet Snapshot.**
4. **Cliquez sur Calendriers.**
5. **Réglez la propriété "Conserver au plus" pour un calendrier pour indiquer le nombre d'instantanés automatiques à préserver à partir de ce calendrier, ou désactivez la case à cocher pour ne pas définir de stratégie de conservation.**

Les instantanés automatiques peuvent être conservés indéfiniment (sauf pour les instantanés pris toutes les demi-heures et toutes les heures qui sont limités respectivement à 48 et 24), ou ils peuvent être limités à un certain nombre. Lorsque le nombre d'instantanés dépasse la valeur spécifiée ici, les instantanés les plus anciens sont supprimés en premier.

▼ Modification d'une stratégie de conservation des instantanés (CLI)

Utilisez la procédure suivante pour modifier une stratégie de conservation des instantanés pour un système de fichiers, un LUN ou un projet. Les calendriers d'instantanés automatiques contiennent des stratégies de conservation des instantanés.

1. **Accédez à shares et sélectionnez le projet ou le partage.**

```
hostname:> shares select myproject
```

```
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```

2. Saisissez `snapshots automatic`.

Vous pouvez utiliser la commande `list` pour afficher une liste des calendriers d'instantanés automatiques de ce partage ou projet.

```
hostname:shares myproject/demo_share> snapshots automatic
hostname:shares myproject/demo_share snapshots automatic> list
Properties:
    convert = false
```

Automatics:

NAME	FREQUENCY	DAY	HH:MM	KEEP
automatic-000	hour	-	-:02	4

3. Sélectionnez le calendrier à modifier.

```
hostname:shares myproject/demo_share snapshots automatic> select automatic-000
```

4. Définissez la propriété `keep` sur le nombre d'instantanés à conserver pour ce calendrier.

Définissez la propriété `keep` sur le nombre d'instantanés à conserver pour ce calendrier (pour les instantanés pris toutes les demi-heures ou toutes les heures, cette valeur est respectivement limitée à 48 et 24). Lorsque le nombre d'instantanés dépasse la valeur spécifiée, les instantanés les plus anciens sont supprimés en premier.

Vous pouvez configurer `keep=0` pour ne pas définir de stratégie de conservation. Dans ce cas, les instantanés automatiques de ce calendrier sont conservés indéfiniment (sauf pour les instantanés pris toutes les demi-heures et toutes les heures qui sont limités respectivement à 48 et 24).

```
hostname:shares myproject/demo_share snapshots automatic-000> set keep=4
keep=4 (uncommitted)
```

5. Saisissez `commit` pour enregistrer la modification.

```
hostname:shares myproject/demo_share snapshots automatic-000> commit
```

▼ Suppression d'un calendrier d'instantané (BUI)

Utilisez la procédure suivante pour supprimer un calendrier d'instantané automatique pour un système de fichiers, un LUN ou un projet.

1. Accédez au projet ou partage approprié.

- a. Si le calendrier s'applique à un projet, accédez à **Partages > Projets**.

- b. Si le calendrier s'applique à un système de fichiers, accédez à **Partages > Partages**.
 - c. Si le calendrier s'applique à un LUN, accédez à **Partages > Partages** et cliquez sur le LUN.
2. Déplacez le curseur de la souris sur le projet ou partage approprié et cliquez sur l'icône de modification .
3. Cliquez sur l'onglet **Snapshot**.
4. Cliquez sur **Calendriers**.
5. Déplacez le pointeur de la souris sur le calendrier à supprimer et cliquez sur l'icône de suppression .
- Une fenêtre s'affiche pour vous avertir que des instantanés automatiques existants risquent d'être détruits.
6. Si vous souhaitez conserver les instantanés automatiques existants, cliquez sur **CONVERTIR** pour les convertir en instantanés manuels. Sinon, cliquez sur **IGNORER** pour les détruire.

▼ Suppression d'un calendrier d'instantané (CLI)

Utilisez la procédure suivante pour supprimer un calendrier d'instantané automatique pour un système de fichiers, un LUN ou un projet.

1. **Accédez au projet ou partage et sélectionnez-le.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. **Saisissez `snapshots automatic`.**

```
hostname:shares myproject/demo_share> snapshots automatic
hostname:shares myproject/demo_share snapshots automatic>
```

Vous pouvez utiliser la commande `list` pour afficher une liste des calendriers d'instantanés automatiques de ce partage ou projet.

```
hostname:shares myproject/demo_share snapshots automatic> list
Properties:
    convert = false
```


Automatics:

NAME	FREQUENCY	DAY	HH:MM	KEEP
automatic-000	day	-	00:00	4

3. Si vous souhaitez conserver les instantanés automatiques existants pris avec ce calendrier, définissez la propriété `convert` sur `true`.

Si vous conservez la propriété `convert = false`, les instantanés automatiques de ce calendrier seront ignorés lorsqu'il sera détruit.

```
hostname:shares myproject/demo_share snapshots automatic> set convert=true
                                convert = true
hostname:shares myproject/demo_share snapshots automatic> commit
```

Vous pouvez utiliser la commande `list` pour afficher la modification.

```
hostname:shares myproject/demo_share snapshots automatic> list
Properties:
    convert = true
```

Automatics:

NAME	FREQUENCY	DAY	HH:MM	KEEP
automatic-000	day	-	00:00	4

4. Utilisez la commande `destroy` suivie du nom du calendrier d'instantané automatique à détruire.

Vous êtes invité à confirmer.

```
hostname:shares myproject/demo_share snapshots automatic> destroy automatic-000
This will destroy "automatic-000". Are you sure? (Y/N)
```

5. Saisissez `y` pour confirmer.

```
This will destroy "automatic-000". Are you sure? (Y/N) Y
```

▼ Affichage du répertoire d'instantanés du système de fichiers (BUI)

Utilisez la procédure suivante pour configurer le répertoire `.zfs/snapshot`, masqué par défaut, de manière à ce qu'il s'affiche comme tout autre répertoire dans un système de fichiers.

Le répertoire `.zfs/snapshot` contient une liste de tous les instantanés du système de fichiers. Les instantanés sont accessibles de la même manière que des données classiques de système de fichiers, mais ils sont en lecture seule. Par défaut, le répertoire `.zfs` n'est pas visible lorsque le contenu des répertoires est listé. Ce paramètre empêche le logiciel de sauvegarde de sauvegarder par inadvertance les instantanés en plus des nouvelles données.

Remarque - Définir le répertoire `.zfs/snapshot` sur "visible" peut entraîner la sauvegarde des instantanés par le logiciel de sauvegarde en plus de données live.

1. **Accédez à Partages > Partages.**
2. **Déplacez le curseur de la souris sur le système de fichiers et cliquez sur l'icône de modification .**
3. **Cliquez sur l'onglet Snapshot.**
4. **Désactivez la case à cocher "Hériter du projet" en regard de Propriétés, ou cliquez sur l'icône de verrou en regard de ".zfs/visibilité de l'instantané."**
5. **Sélectionnez "Visible" dans le menu déroulant en regard de ".zfs/visibilité de l'instantané."**
6. **Cliquez sur APPLIQUER pour enregistrer les modifications.**
Pour masquer à nouveau le répertoire, revenez à cette page et sélectionnez "Masqué" dans le menu déroulant, puis cliquez sur APPLIQUER.

▼ Affichage du répertoire d'instantanés du système de fichiers (CLI)

Utilisez la procédure suivante pour configurer le répertoire `.zfs/snapshot`, masqué par défaut, de manière à ce qu'il s'affiche comme tout autre répertoire dans un système de fichiers.

Le répertoire `.zfs/snapshot` contient une liste de tous les instantanés du système de fichiers. Les instantanés sont accessibles de la même manière que des données classiques de système de fichiers, mais ils sont en lecture seule. Par défaut, le répertoire `.zfs` n'est pas visible lorsque le contenu des répertoires est listé. Ce paramètre empêche le logiciel de sauvegarde de sauvegarder par inadvertance les instantanés en plus des nouvelles données.

Remarque - Définir le répertoire `.zfs/snapshot` sur "visible" peut entraîner la sauvegarde des instantanés par le logiciel de sauvegarde en plus de données live.

1. **Accédez au partage de système de fichiers et sélectionnez-le.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
hostname:shares myproject/demo_share>
```
2. **Exécutez la commande `set snapdir` pour définir le répertoire d'instantanés du système de fichiers sur `visible`.**

```
hostname:shares myproject/demo_share> set snapdir=visible
snapdir=visible(uncommitted)
```

3. Saisissez `commit` pour enregistrer la modification.

```
hostname:shares myproject/demo_share> commit
```

4. Pour masquer à nouveau le répertoire, revenez à ce contexte et exécutez la commande `set snapdir` pour définir le répertoire sur Masqué, puis saisissez `commit` pour enregistrer la modification.

```
hostname:shares myproject/demo_share> set snapdir=hidden
snapdir=hidden(uncommitted)
hostname:shares myproject/demo_share> commit
```

Rubriques connexes

- ["Accès à un répertoire d'instantanés masqué du système de fichiers \(CLI\)" à la page 459](#)
- ["Affichage du répertoire d'instantanés du système de fichiers \(BUI\)" à la page 457](#)
- ["Accès à un répertoire d'instantanés visible du système de fichiers \(CLI\)" à la page 460](#)

▼ Accès à un répertoire d'instantanés masqué du système de fichiers (CLI)

Utilisez la procédure suivante pour accéder à des instantanés de système de fichiers par le biais des protocoles de données à l'emplacement `.zfs/snapshot` à la racine du système de fichiers.

Le répertoire `.zfs/snapshot` contient une liste de tous les instantanés du système de fichiers. Les instantanés sont accessibles de la même manière que des données classiques de système de fichiers, mais ils sont en lecture seule. Par défaut, le répertoire `.zfs` n'est pas visible lorsque le contenu des répertoires est listé, mais il est possible d'y accéder en lançant une recherche explicite. Cela empêche le logiciel de sauvegarde de sauvegarder par inadvertance les instantanés en plus des nouvelles données.

- 1. Dans une fenêtre de terminal, accédez au répertoire dans lequel vous avez monté le partage.**
- 2. Recherchez `.zfs/snapshot`.**
De là, vous pouvez répertorier les instantanés de ce système de fichiers et consulter leur contenu.

Exemple 17 Accès à `.zfs/snapshot`

Cet exemple montre deux instantanés d'un système de fichiers. Le premier instantané contient trois fichiers.

```
$ ls -l /mnt/demo
$ ls -l /mnt/demo/.zfs/snapshot
demo_snap1
demo_snap2
$ ls -l /mnt/demo/.zfs/snapshot/demo_snap1
file1
file2
file3
```

Rubriques connexes

- ["Affichage du répertoire d'instantanés du système de fichiers \(BUI\)" à la page 457](#)
- ["Affichage du répertoire d'instantanés du système de fichiers \(CLI\)" à la page 458](#)
- ["Accès à un répertoire d'instantanés visible du système de fichiers \(CLI\)" à la page 460](#)

▼ Accès à un répertoire d'instantanés visible du système de fichiers (CLI)

Utilisez la procédure suivante pour accéder à des instantanés de système de fichiers dans le répertoire `.zfs/snapshot` après l'avoir rendu visible.

Avant de commencer

Définissez le répertoire `.zfs/snapshot` sur Visible comme indiqué dans la section ["Affichage du répertoire d'instantanés du système de fichiers \(CLI\)" à la page 458](#).

1. **Accédez au répertoire dans lequel vous avez monté le partage.**
2. **Accédez à `.zfs/snapshot` dans ce répertoire.**

De là, vous pouvez répertorier les instantanés de ce système de fichiers et consulter leur contenu.

▼ Modification du nom d'un instantané (BUI)

Utilisez la procédure suivante pour renommer un instantané manuel existant. Il est impossible de renommer un instantané automatique, dont le nom inclut `.auto`, `.rr` ou `.ndmp`.

Si un instantané de partage faisant partie d'un instantané de projet plus grand est renommé, il ne sera plus considéré comme faisant partie du même instantané et si un instantané est renommé de façon à porter le même nom qu'un instantané du projet parent, il sera considéré comme faisant partie de l'instantané du projet.

Avant de commencer

- Pour exécuter cette procédure, vous devez disposer de privilèges superutilisateur ou de l'une des autorisations de rôle suivantes dans les projets et les partages :
 - `renameSnap` - Permet de renommer des instantanés.

- rename - Permet de renommer des projets et des partages, y compris des noms d'instantanés.
 - Pour ajouter des autorisations à un rôle, reportez-vous à la section "[Modification des autorisations liées à un rôle \(BUI\)](#)" à la page 171.
1. **Accédez au partage ou projet contenant l'instantané à renommer.**
 - Pour renommer un instantané de système de fichiers, accédez à **Partages > Partages**.
 - Pour renommer un instantané de LUN, accédez à **Partages > Partages** et cliquez sur le LUN.
 - Pour renommer un instantané de projet, accédez à **Partages > Projets**.
 2. **Déplacez le curseur de la souris sur le partage ou projet contenant l'instantané à renommer, puis cliquez sur l'icône de modification .**
 3. **Cliquez sur l'onglet Snapshot.**
 4. **Sous Instantanés, cliquez sur le nom de l'instantané à renommer.**
Une boîte de saisie de texte s'ouvre à la place du nom de l'instantané.
 5. **Saisissez le nouveau nom de l'instantané.**
Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.
 6. **Appuyez sur Entrée pour valider la modification.**

Rubriques connexes

- "[Présentation des utilisateurs et des rôles](#)" à la page 175
- "[Autorisations utilisateur](#)" à la page 176

▼ Modification du nom d'un instantané (CLI)

Utilisez la procédure suivante pour renommer un instantané manuel existant. Il est impossible de renommer des instantanés automatiques.

Si un instantané de partage faisant partie d'un instantané de projet plus grand est renommé, il ne sera plus considéré comme faisant partie du même instantané et si un instantané est renommé de façon à porter le même nom qu'un instantané du projet parent, il sera considéré comme faisant partie de l'instantané du projet.

Avant de commencer

- Pour exécuter cette procédure, vous devez disposer de privilèges superutilisateur ou de l'une des autorisations de rôle suivantes dans les projets et les partages :
 - `renameSnap` - Permet de renommer des instantanés.
 - `rename` - Permet de renommer des projets et des partages, y compris des noms d'instantanés.
- Pour ajouter des autorisations à un rôle, reportez-vous à la section "[Modification des autorisations liées à un rôle \(CLI\)](#)" à la page 172.

1. Accédez à shares et sélectionnez le projet, ou sélectionnez le projet, puis un partage.

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. Saisissez snapshots.

```
hostname:shares myproject/demo_share> snapshots
```

3. Saisissez list pour afficher la liste des instantanés du projet ou partage.

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
```

4. Pour renommer l'instantané, saisissez la commande rename suivie du nom de l'instantané actuel, d'un espace, puis du nom du nouvel instantané.

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux `_` `-` `.` `:` sont autorisés.

```
hostname:shares myproject/demo_share snapshots> rename demo_snap1 new_name
```

Rubriques connexes

- "[Présentation des utilisateurs et des rôles](#)" à la page 175
- "[Autorisations utilisateur](#)" à la page 176

▼ Restauration d'un instantané (BUI)

Utilisez la procédure suivante pour restaurer un instantané existant d'un système de fichiers ou d'un LUN.

Lorsqu'une restauration se produit, tous les instantanés les plus récents (ainsi que les clones de ces instantanés) sont détruits et les données actives sont réinitialisées à l'état en cours au moment de la prise de l'instantané. Les instantanés incluent uniquement des données, et non des propriétés. Ainsi, les paramètres des propriétés modifiés depuis la prise de l'instantané sont

conservés. Les modifications apportées à l'accès au répertoire racine du système de fichiers sont perdues au cours de la restauration.



Attention - Cette procédure est irréversible.

1. **Accédez au partage ou projet contenant l'instantané à renommer.**
 - **Pour restaurer un instantané de système de fichiers, accédez à Partages > Partages.**
 - **Pour restaurer un instantané de LUN, accédez à Partages > Partages et cliquez sur le LUN.**
2. **Déplacez le curseur de la souris sur le partage contenant l'instantané à restaurer, puis cliquez sur l'icône de modification .**
3. **Cliquez sur l'onglet Snapshot.**
4. **Déplacez le curseur de la souris sur l'instantané à restaurer, cliquez sur son icône de restauration , puis confirmez l'action.**

▼ Restauration d'un instantané (CLI)

Utilisez la procédure suivante pour restaurer un instantané existant d'un système de fichiers ou d'un LUN.

La restauration d'un instantané nécessite de détruire les instantanés les plus récents, ainsi que leurs clones et de rétablir le contenu du partage dans l'état où il était au moment où l'instantané a été pris. Les paramètres de propriété du partage ne sont pas affectés, mais les modifications apportées à l'accès au répertoire racine du système de fichiers sont perdues au cours de la restauration.



Attention - Cette procédure est irréversible.

1. **Accédez au partage contenant l'instantané à restaurer et sélectionnez-le.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. **Saisissez snapshots.**

```
hostname:shares myproject/demo_share> snapshots
```

3. Saisissez **list** pour afficher la liste des instantanés du projet ou partage.

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
```

4. Sélectionnez l'instantané à restaurer, puis saisissez la commande **rollback**.

```
hostname:shares myproject/demo_share snapshots> select demo_snap1
hostname:shares myproject/demo_share@demo_snap1> rollback
```

5. Saisissez **y** pour confirmer.

```
hostname:shares myproject/demo_share@demo_snap1> rollback
Rolling back will revert data to snapshot, destroying newer data. Active initiators will be
disconnected.
```

```
Continue? (Y/N)
hostname: shares myproject/demo_share@demo_snap1> Y
```

▼ Destruction d'un instantané (BUI)

Utilisez la procédure suivante pour détruire un instantané.

Avant de commencer

- Pour exécuter cette procédure, vous devez disposer de privilèges superutilisateur ou de l'une des autorisations de rôle suivantes dans les projets et les partages :
 - **destroySnap** - Permet de détruire des instantanés.
 - **destroy** - Permet de détruire des projets et des partages, y compris des noms d'instantanés.
- Pour ajouter des autorisations à un rôle, reportez-vous à la section "[Modification des autorisations liées à un rôle \(BUI\)](#)" à la page 171.

1. Accédez à l'instantané.

- Pour un instantané d'un système de fichiers ou d'un LUN, accédez à **Partages > Partages** et cliquez sur un système de fichiers ou un LUN selon que l'instantané que vous souhaitez détruire provient d'un système de fichiers ou d'un LUN.
- Pour un instantané d'un projet, accédez à **Partages > Projets**.

2. Déplacez le curseur de la souris sur le partage approprié et cliquez sur l'icône de modification .

3. Cliquez sur l'onglet **Snapshot**.

4. **Déplacez le curseur de la souris sur l'instantané à détruire et cliquez sur l'icône de destruction .**

Une boîte de dialogue de confirmation apparaît.

Si des clones de cet instantané ont été réalisés, une liste s'affiche indiquant ceux qui seront affectés. La destruction d'un instantané détruit également ses clones et leurs descendants.

5. **Cliquez sur OK pour confirmer.**

Rubriques connexes

- ["Présentation des utilisateurs et des rôles" à la page 175](#)
- ["Autorisations utilisateur" à la page 176](#)

▼ Destruction d'un instantané (CLI)

Utilisez la procédure suivante pour détruire un instantané.

Avant de commencer

- Pour exécuter cette procédure, vous devez disposer de privilèges superutilisateur ou de l'une des autorisations de rôle suivantes dans les projets et les partages :
 - `destroySnap` - Permet aux utilisateurs de détruire uniquement des instantanés.
 - `destroy` - Accorde des privilèges permettant de supprimer des projets et des partages, y compris des instantanés.
- Pour ajouter des autorisations à un rôle, reportez-vous à la section ["Modification des autorisations liées à un rôle \(CLI\)" à la page 172](#).

1. **Accédez à shares et sélectionnez le projet, ou sélectionnez le projet, puis un partage.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_share
```

2. **Saisissez `snapshots`.**

```
hostname:shares myproject/demo_share> snapshots
```

3. **Saisissez `list` pour afficher la liste des instantanés du projet ou partage.**

```
hostname:shares myproject/demo_share snapshots> list
demo_snap1
demo_snap2
```

4. **Utilisez la commande `destroy` pour détruire un instantané à l'aide de l'une des deux méthodes suivantes :**

- Sélectionnez l'instantané à supprimer, puis saisissez `destroy`.

```
hostname:shares myproject/demo_share snapshots> select demo_snap1
```

```
hostname:shares myproject/demo_share@demo_snap1> destroy
```

- Saisissez **destroy** suivi du nom de l'instantané.

```
hostname:shares myproject/demo_share snapshots> destroy demo_snap1
```

5. Entrez y pour confirmer l'action.

```
This will destroy all data in "demo_snap1"! Are you sure? (Y/N) Y
```

Rubriques connexes

- ["Présentation des utilisateurs et des rôles" à la page 175](#)
- ["Autorisations utilisateur" à la page 176](#)

▼ Clonage d'un instantané (BUI)

NOTICE RELATIVE A LA LICENCE : *Le clonage peut faire l'objet d'une évaluation à titre gratuit, mais la fonction requiert l'achat d'une licence distincte pour un usage en production. Au terme de la période d'évaluation, il convient d'acheter une licence pour cette fonction ou de la désactiver. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

Utilisez la procédure suivante pour créer un clone d'un instantané existant d'un système de fichiers ou d'un LUN.

Remarque - Les clones de projets ne sont pas pris en charge.

1. **Accédez au partage à cloner.**
 - a. Pour cloner un système de fichiers, accédez à **Partages > Partages**.
 - b. Pour cloner un LUN, accédez à **Partages > Partages** et cliquez sur le LUN.
2. **Déplacez le curseur de la souris sur le partage et cliquez sur l'icône de modification .**
3. **Cliquez sur l'onglet Snapshot.**
4. **Déplacez le curseur de la souris sur l'instantané à cloner et cliquez sur l'icône de clonage .**

Une boîte de dialogue s'affiche indiquant les paramètres et les options du nouveau clone.

5. Définissez chaque champ de manière appropriée.

a. Dans le menu déroulant *Projet*, sélectionnez le projet de destination.

Par défaut, le clone est créé au sein du projet actuel, mais vous pouvez également le créer dans un autre projet.

b. Saisissez un nom pour le clone.

c. (Facultatif) Cliquez sur l'icône de verrou située en regard de *Point de montage* et définissez un point de montage pour le clone.

Si vous laissez ce champ verrouillé, le point de montage du clone reste `/export/<sharename>` (valeur par défaut).

d. (Facultatif) Cliquez sur l'icône de verrou située en regard du nom de la ressource et saisissez l'une des valeurs suivantes :

- **désactivé** - SMB est désactivé
- **activé** - SMB est activé pour que vous puissiez partager le clone via SMB. Le nom du clone dans SMB correspond au nom du clone sur l'appareil.
- **<pick_a_name>** - SMB est activé pour que vous puissiez partager le clone via SMB. Le nom du clone dans SMB correspond au nom spécifié ici plutôt qu'au nom du clone sur l'appareil.

Si vous laissez ce champ verrouillé, la propriété Nom de la ressource hérite de l'instantané cloné.

e. (Facultatif) Cochez la case *Clé d'héritage* ou désélectionnez-la et sélectionnez le keystore (*LOCAL* ou *OKM*) et le nom de la clé de chiffrement à appliquer au clone.

Si la case est cochée, le keystore et le nom de clé du clone seront ceux du projet de destination.

Si la case n'est pas cochée, le keystore et le nom de clé du clone seront ceux du partage parent. Vous pouvez également sélectionner un keystore et un nom de clé différents dans le menu déroulant.

f. (Facultatif) Cochez la case *Conserver les autres paramètres locaux* pour que les propriétés héritées soient conservées comme paramètres locaux dans le nouveau clone.

Ce champ détermine si les propriétés héritées doivent provenir de l'ensemble de données parent ou du projet de destination. Par défaut, la case à cocher est désactivée, ce qui signifie que toutes les propriétés héritées proviennent du projet de destination du nouveau

clone. Si vous activez cette case à cocher, toutes les propriétés actuellement héritées sont conservées comme paramètres locaux dans le nouveau clone.

6. Cliquez sur **APPLIQUER pour confirmer les paramètres et créer le clone.**

Le clone s'affiche dans la liste de partages pour le projet de destination défini. Les clones s'utilisent comme n'importe quel autre partage.

Rubriques connexes

- Pour effectuer des opérations de partage sur un clone, reportez-vous à la section "[Partages et projets](#)" à la page 343.
- Pour réaliser le clone d'un clone, reportez-vous à la section "[Clonage d'un clone](#)" à la page 470.
- Pour afficher tous les clones d'un instantané particulier, reportez-vous à la section "[Affichage des clones d'un instantané \(BUI\)](#)" à la page 470.
- Pour déterminer l'instantané à partir duquel un clone a été créé, reportez-vous à la section "[Affichage de l'origine d'un clone \(BUI\)](#)" à la page 471.

▼ Clonage d'un instantané (CLI)

NOTICE RELATIVE A LA LICENCE : *Le clonage peut faire l'objet d'une évaluation à titre gratuit, mais la fonction requiert l'achat d'une licence distincte pour un usage en production. Au terme de la période d'évaluation, il convient d'acheter une licence pour cette fonction ou de la désactiver. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

Utilisez la procédure suivante pour créer un clone d'un instantané existant d'un système de fichiers ou d'un LUN.

Remarque - Les clones de projets ne sont pas pris en charge.

1. Accédez au système de fichiers, LUN ou projet approprié et saisissez `snapshots`.

```
hostname:shares myproject/demo_share> snapshots
hostname:shares myproject/demo_share snapshots>
```

2. Sélectionnez l'instantané à cloner.

```
hostname:shares myproject/demo_share snapshots> select snap1
```

3. Exécutez la commande `clone`, éventuellement suivie du nom du projet dans lequel vous souhaitez créer le clone.

Par défaut, le clone est créé dans le même projet que celui utilisé pour l'instantané cloné.

```
hostname:shares myproject/demo_share@snap1> clone project1
```

Vous êtes placé dans un contexte de partage non validé. A partir d'ici, vous pouvez ajuster les propriétés si nécessaire avant de valider les modifications pour créer un clone.

4. Exécutez la commande **get** pour afficher les propriétés.

```
hostname:shares myproject/demo_clone (uncommitted clone)> get
aclinherit = restricted (inherited)
aclmode = discard (inherited)
atime = true (inherited)
checksum = fletcher4 (inherited)
compression = off (inherited)
copies = 1 (inherited)
mountpoint = /export/testbed (inherited)
quota = 0 (default)
readonly = false (inherited)
recordsize = 128K (inherited)
reservation = 0 (default)
secondarycache = all (inherited)
nbmand = false (inherited)
sharesmb = off (inherited)
sharenfs = on (inherited)
snapdir = hidden (inherited)
vscan = false (inherited)
sharedav = off (inherited)
shareftp = off (inherited)
root_group = other (default)
root_permissions = 777 (default)
root_user = nobody (default)
quota_snap = true (default)
reservation_snap = true (default)
```

5. Exécutez la commande **set** pour régler les propriétés.

```
hostname:shares myproject/demo_clone (uncommitted clone)> set quota=10G
quota = 10G (uncommitted)
```

6. Exécutez la commande **commit** pour valider les modifications et créer le clone.

```
hostname:shares myproject/demo_clone (uncommitted clone)> commit
hostname:shares myproject/demo_share@demo_clone>
```

Rubriques connexes

- Pour effectuer des opérations de partage sur un clone, reportez-vous à la section "[Partages et projets](#)" à la page 343.
- Pour réaliser le clone d'un clone, reportez-vous à la section "[Clonage d'un clone](#)" à la page 470.

- Pour afficher tous les clones d'un instantané particulier, reportez-vous à la section ["Affichage des clones d'un instantané \(CLI\)" à la page 471.](#)
- Pour déterminer l'instantané à partir duquel un clone a été créé, reportez-vous à la section ["Affichage de l'origine d'un clone \(CLI\)" à la page 472.](#)

▼ Clonage d'un clone

NOTICE RELATIVE A LA LICENCE : *Le clonage peut faire l'objet d'une évaluation à titre gratuit, mais la fonction requiert l'achat d'une licence distincte pour un usage en production. Au terme de la période d'évaluation, il convient d'acheter une licence pour cette fonction ou de la désactiver. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

Utilisez la procédure suivante pour créer un clone d'un clone existant.

Après avoir créé un clone à partir d'un instantané d'un système de fichiers ou d'un LUN, vous pouvez l'utiliser comme n'importe quel autre partage. Vous pouvez prendre un instantané du clone, puis créer un clone de cet instantané. Vous pouvez poursuivre cette procédure de création de clones indéfiniment.

1. **Prenez un instantané du clone en effectuant l'une des procédures suivantes :**
 - ["Réalisation d'un instantané \(BUI\)" à la page 444](#)
 - ["Réalisation d'un instantané \(CLI\)" à la page 445](#)
2. **Clonez l'instantané en effectuant l'une des procédures suivantes :**
 - ["Clonage d'un instantané \(BUI\)" à la page 466](#)
 - ["Clonage d'un instantané \(CLI\)" à la page 468](#)

▼ Affichage des clones d'un instantané (BUI)

Utilisez la procédure suivante pour afficher une liste de tous les clones créés à partir d'un instantané particulier. Ceux-ci sont également appelés les "clones dépendants" de l'instantané.

1. **Accédez à Partages > Partages et cliquez sur un système de fichiers ou un LUN si vous souhaitez afficher les clones d'un système de fichiers ou d'un LUN.**
2. **Déplacez le curseur de la souris sur le partage approprié et cliquez sur l'icône de modification .**

3. Cliquez sur l'onglet Snapshot.
4. Déplacez le curseur de la souris sur l'instantané approprié et cliquez sur "Afficher..." sous Clones.
 Une fenêtre s'affiche avec une liste répertoriant les clones dépendants de l'instantané et les projets dans lesquels ils se trouvent.
 Si le lien "Afficher..." ne s'affiche pas, l'instantané n'a pas de clone.
5. Cliquez sur OK pour fermer la fenêtre.

▼ Affichage des clones d'un instantané (CLI)

Utilisez la procédure suivante pour afficher une liste de tous les clones créés à partir d'un instantané particulier.

1. Accédez à l'instantané et sélectionnez-le.

```
hostname:shares myproject/demo_share> snapshots
hostname:shares myproject/demo_share snapshots> select snap1
hostname:shares myproject/demo_share@snap1>
```

2. Exécutez la commande `list clones`.

```
hostname:shares myproject/demo_share@snap1> list clones
```

Clones: 2 total

```
PROJECT      SHARE
myproject    demo_clone1
myproject    demo_clone2
hostname:shares myproject/demo_share@snap1
```

Le résultat indique le nombre de clones, le projet dans lequel ils résident et le nom de chaque clone.

▼ Affichage de l'origine d'un clone (BUI)

Utilisez la procédure suivante pour déterminer l'instantané à partir duquel le clone a été créé.

1. Accédez au clone.
 - a. Accédez à Partages > Partages.
 - b. Déplacez le curseur de la souris sur le clone et cliquez sur l'icône de modification .

2. **Sous Propriétés statiques à gauche, cliquez sur "Afficher" en regard de "Origine de clone".**

Une fenêtre s'affiche indiquant le nom de l'instantané à partir duquel le clone a été créé.

▼ Affichage de l'origine d'un clone (CLI)

Utilisez la procédure suivante pour déterminer l'instantané à partir duquel le clone a été créé.

1. **Accédez à shares et sélectionnez le projet contenant le clone, puis sélectionnez ce dernier.**

```
hostname:> shares select myproject
hostname:shares myproject> select demo_clone
hostname:shares myproject/demo_clone>
```

2. **Exécutez la commande `get origin`.**

La commande renvoie l'emplacement et le nom de l'instantané à partir duquel le clone a été créé.

```
hostname:shares myproject/demo_clone> get origin
origin = myproject/demo_share@demo_snapshot
```


Réplication distante

NOTICE RELATIVE A LA LICENCE : *La réplication distante et le Clonage peuvent faire l'objet d'une évaluation à titre gratuit, mais chacune de ces fonctions requiert l'achat d'une licence distincte pour un usage en production. Au terme de la période d'évaluation, il convient d'acheter une licence pour ces fonctions ou de les désactiver. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

Les appareils Oracle ZFS Storage Appliance prennent en charge la réplication de projets et de partages basée sur les instantanés d'un appareil source sur un appareil cible, sur un autre pool du même appareil ou sur un serveur NFS pour la réplication hors ligne. Vous pouvez configurer l'exécution manuelle, programmée, ou continue de la réplication. Parmi les cas d'utilisation de la réplication distante, on trouve la récupération après sinistre, la répartition de données, la sauvegarde disque à disque et la migration de données entre les appareils lors de la mise à niveau matérielle ou du rééquilibrage du stockage.

Pour configurer, surveiller et gérer la réplication distante, reportez-vous aux sections suivantes :

- [Workflow de réplication distante](#)
- [Vérification de la compatibilité entre les appareils source et cible](#)
- Configuration d'interfaces réseau et de routage statique - [BUI](#), [CLI](#)
- Création d'une cible de réplication - [BUI](#), [CLI](#)
- Création d'une action de réplication - [BUI](#), [CLI](#)
- [Configuring Replication for a Clustered Configuration](#)
- Création d'une réplication hors ligne - [BUI](#), [CLI](#)
- [Reversing Replication for Offline Replication \(CLI\)](#)
- Désactivation de la compression de réplication - [BUI](#), [CLI](#)
- Surveillance de la progression de la réplication - [BUI](#), [CLI](#)
- Modification d'un package de réplication - [BUI](#), [CLI](#)
- Annulation d'une mise à jour de réplication - [BUI](#), [CLI](#)
- Clonage d'un package de réplication - [BUI](#), [CLI](#)
- Dissociation d'un package de réplication - [BUI](#), [CLI](#)
- Configuration de réplication distante pour récupération après sinistre - [BUI](#), [CLI](#)
- [Réplication distante pour sauvegarde disque à disque](#)

- Désactivation d'un package de réplication - [BUI](#), [CLI](#)

Pour plus d'informations sur les concepts de réplication distante, reportez-vous aux sections suivantes :

- ["Concepts de la réplication distante" à la page 529](#)

▼ Workflow de réplication distante

Les étapes suivantes indiquent la procédure générale de configuration et d'utilisation de la réplication distante. Pour plus d'informations sur les concepts de réplication distante, reportez-vous à la section ["Concepts de la réplication distante" à la page 529](#).

- 1. Vérifiez la compatibilité logicielle sur les appareils source et cible.**

Pour plus d'informations sur la compatibilité logicielle, reportez-vous à la section ["Vérification de la compatibilité entre les appareils source et cible" à la page 474](#).

- 2. Définissez les interfaces réseau et le routage.**

Pour plus d'informations sur la configuration du routage réseau, reportez-vous à la section Configuration d'interfaces réseau et de routage statique - [BUI](#), [CLI](#).

- 3. Définissez une cible de réplication.**

Pour plus d'informations sur la création d'une cible de réplication, reportez-vous à la section Création d'une cible de réplication - [BUI](#), [CLI](#).

- 4. Créez une action de réplication.**

Pour plus d'informations sur la création d'une action de réplication, reportez-vous à la section Création d'une action de réplication - [BUI](#), [CLI](#).

- 5. Envoyez une mise à jour de réplication.**

Pour plus d'informations sur l'envoi d'une mise à jour de réplication, reportez-vous à la section Envoi manuel d'une mise à jour de réplication - [BUI](#), [CLI](#).

- 6. (Facultatif) Créez une réplication hors ligne.**

Pour plus d'informations sur la création d'une action de réplication hors ligne, reportez-vous à la section Création d'une réplication hors ligne - [BUI](#), [CLI](#).

▼ Vérification de la compatibilité entre les appareils source et cible

La réplication distante est compatible avec la plupart des versions des logiciels Oracle ZFS Storage Appliance. Les échecs de compatibilité se produisent si une mise à jour de réplication

utilise une fonctionnalité qui n'est pas prise en charge sur l'appareil cible. Des fonctions sont incluses dans les mises à jour logicielles ou sous forme de mises à jour différées.

Pour plus de détails sur la compatibilité et les fonctions de mise à jour différée, reportez-vous au document de compatibilité de réplication distante des systèmes Oracle ZFS Storage Appliance (ID de doc 1958039.1) sur [My Oracle Support \(http://support.oracle.com/\)](http://support.oracle.com/).

1. **Vérifiez la version logicielle actuelle sur les appareils source et cible.**

Si vous utilisez la BUI, accédez à Maintenance > Système. Si vous utilisez la CLI, accédez à `maintenance system updates` et saisissez `show`.

2. **Assurez-vous que l'appareil cible fournit une prise en charge de toute fonctionnalité de mise à jour différée utilisée par le projet ou le partage source.**

Par exemple, si le partage source utilise des blocs de données de grande taille, assurez-vous que l'appareil cible fournit une prise en charge pour cette fonctionnalité.

3. **Mettez à jour le logiciel et appliquez les mises à jour différées sur l'appareil cible, le cas échéant.**

Pour plus d'informations, reportez-vous à la section "[Application d'une mise à jour différée](#)" dans le [Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance](#).

▼ Configuration d'interfaces réseau et de routage statique (BUI)

Pour assurer l'emploi des interfaces réseau appropriées pour les connexions de réplication entre les appareils source et cible, configurez des routes /32 (spécifiques aux hôtes).

Si vous configurez une réplication pour une configuration de cluster, sélectionnez une interface réseau singleton (déverrouillée) afin qu'à la suite d'une reprise ou d'un rétablissement de cluster, l'interface se déplace sur le noeud sur lequel l'opération de réplication est en cours. Les deux noeuds de cluster source peuvent effectuer une réplication sur le même noeud cible uniquement si le noeud source fournit deux adresses IP, une pour chaque noeud dans le cluster source. La réplication vers la même adresse IP cible depuis les deux noeuds d'un cluster source n'est pas prise en charge.

1. **Accédez à la page Configuration > Réseau > Routage.**

2. Cliquez sur l'icône d'ajout .



The image shows a dialog box titled "Insert Static Route". It has two buttons at the top right: "CANCEL" and "ADD". Below the title bar, there are several configuration options:

- Family:** Two radio buttons, "IPv4" (selected) and "IPv6".
- Kind:** Two radio buttons, "Default" and "Network" (selected).
- Destination:** A text input field containing "203.0.113.254/32".
- Gateway:** A text input field containing "203.0.113.255".
- Interface:** A dropdown menu showing "Untitled Interface (e1000q0)" with a downward arrow.

3. Dans l'écran Insérer une route statique, indiquez les informations suivantes :
 - **Family** : sélectionnez IPv4 ou IPv6.
 - **Kind** : sélectionnez Network.
 - **Destination** : saisissez l'adresse IP et le masque de réseau /32 de l'appareil cible.
 - **Gateway** : saisissez l'adresse de passerelle de l'appareil cible.
 - **Interface** : saisissez le nom de l'interface.
4. Cliquez sur Ajouter.
5. Après avoir défini la route statique de l'appareil source vers l'appareil cible, répétez ces étapes sur l'appareil cible pour définir la route statique de la cible vers la source.
6. Pour vérifier que le trafic est routé par le biais des bonnes interfaces source et cible, utilisez la commande `tracert`.

Pour plus d'informations sur l'utilisation de la commande `tracert`, reportez-vous à la section "[Configuration du routage réseau](#)" à la page 81.

Remarque - Lorsqu'une interface est supprimée, toutes les routes qui lui sont associées le sont également.

Rubriques connexes

- "[Exemple : Configuration de répllication pour des appareils en cluster](#)" à la page 538

- ["Workflow de réplication distante" à la page 474](#)
- ["Concepts de la réplication distante" à la page 529](#)

▼ Configuration d'interfaces réseau et de routage statique (CLI)

Avant de commencer

Pour assurer l'emploi des interfaces réseau appropriées pour les connexions de réplication entre les appareils source et cible, configurez des routes /32 (spécifiques aux hôtes).

Si vous configurez une réplication pour une configuration de cluster, sélectionnez une interface réseau singleton (déverrouillée) afin qu'à la suite d'une reprise ou d'un rétablissement de cluster, l'interface se déplace sur le noeud sur lequel l'opération de réplication est en cours. Les deux noeuds de cluster source peuvent effectuer une réplication sur le même noeud cible uniquement si le noeud source fournit deux adresses IP, une pour chaque noeud dans le cluster source. La réplication vers la même adresse IP cible depuis les deux noeuds d'un cluster source n'est pas prise en charge.

1. Accédez à configuration services routing sur l'appareil source.

Utilisez une route statique /32 (spécifique à l'hôte) vers l'adresse IP du système cible via l'interface réseau dédiée. Dans l'exemple suivant, mask=32 signifie qu'il s'agit d'une route spécifique à l'hôte.

```
host_source:configuration services routing> create

host_source:configuration services route (uncommitted)> get
    family = (unset)
    destination = (unset)
    mask = (unset)
    gateway = (unset)
    interface = (unset)
host_source:configuration services route (uncommitted)> set family=IPv4
host_source:configuration services route (uncommitted)> set destination=203.34.56.78
host_source:configuration services route (uncommitted)> set mask=32
host_source:configuration services route (uncommitted)> set gateway=203.34.56.254
host_source:configuration services route (uncommitted)> set interface=nge3
host_source:configuration services route (uncommitted)> commit
host_source:configuration services routing> show
route-000  0.0.0.0/0                203.24.30.254    nge0            static
route-001  203.24.30.0/32                203.24.30.28     nge0            dynamic
route-002  203.24.150.0/32                203.24.150.10    ibd0            dynamic
route-003  203.24.101.65/32              203.24.30.254    nge1            inactive
route-005  203.34.56.78/32                203.34.56.254    nge3            static
```

2. Après avoir défini la route statique de l'appareil source vers l'appareil cible, répétez ces étapes sur l'appareil cible pour définir la route statique de la cible vers la source.

3. **Pour vérifier que le trafic est routé par le biais des bonnes interfaces source et cible, utilisez la commande `traceroute`.**

Pour plus d'informations sur l'utilisation de la commande `traceroute`, reportez-vous à la section "[Configuration du routage réseau](#)" à la page 81.

Remarque - Lorsqu'une interface est supprimée, toutes les routes qui lui sont associées le sont également.

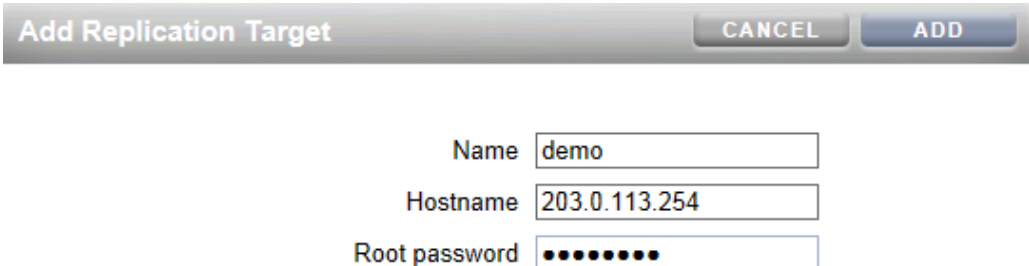
Rubriques connexes

- "[Exemple : Configuration de réplication pour des appareils en cluster](#)" à la page 538
- "[Workflow de réplication distante](#)" à la page 474
- "[Concepts de la réplication distante](#)" à la page 529

▼ Création d'une cible de réplication (BUI)

Une cible de réplication établit une connexion de communication sécurisée entre les appareils source et cible. Pour créer une cible de réplication, procédez comme suit :

1. **A partir de la BUI de l'appareil source, accédez à `Configuration > Services > Réplication distante`.**
2. **Cliquez sur l'icône d'ajout  en regard des Cibles.**



Add Replication Target

CANCEL ADD

Name demo

Hostname 203.0.113.254

Root password

3. **Entrez ce qui suit :**
 - **Name** : nom de la cible à afficher dans la BUI ou la CLI de l'appareil source.
 - **Hostname** : adresse IP, ou nom d'hôte, de l'appareil cible.

Remarque - Utilisez une adresse IP configurée avec une route statique pour forcer le trafic sur une interface réseau spécifique.

- **Root password** : mot de passe root de l'appareil cible, pour autoriser la connexion.

4. Cliquez sur **Ajouter**.

Rubriques connexes

- ["Cibles de réplication" à la page 532](#)
- ["Workflow de réplication distante" à la page 474](#)
- ["Réplication d'un partage chiffré" à la page 589](#)

▼ Création d'une cible de réplication (CLI)

Une cible de réplication établit une connexion de communication sécurisée entre les appareils source et cible. Pour créer une cible de réplication, procédez comme suit :

1. **A partir de l'appareil source, accédez au noeud `targets`, puis saisissez `target` pour configurer un appareil distant en tant que cible de réplication.**

```
host_source:> configuration services replication targets> target
host_source:configuration services replication target (uncommitted)>
```

2. **Définissez les `hostname`, `root_password` et `label` cibles.**

Remarque - Utilisez une adresse IP configurée avec une route statique pour forcer le trafic sur une interface réseau spécifique.

```
host_source:configuration services replication target (uncommitted)> set hostname=203.
123.225.201
host_source:configuration services replication target (uncommitted)> set
  root_password=password
host_source:configuration services replication target (uncommitted)> set label=repl_1
```

3. **Validez les modifications apportées.**

```
host_source:configuration services replication target (uncommitted)> commit
```

Rubriques connexes

- ["Cibles de réplication" à la page 532](#)
- ["Workflow de réplication distante" à la page 474](#)

- ["Réplication d'un partage chiffré" à la page 589](#)

▼ Création d'une action de réplication (BUI)

Une action de réplication décrit le projet ou le partage à répliquer, l'emplacement où envoyer la réplication, le calendrier de réplication et les propriétés de transfert de données telles que l'activation ou la désactivation du chiffrement de la liaison réseau.

- Si vous configurez une réplication distante pour la première fois, il peut-être utile de ne répliquer qu'un minimum de données, en répliquant un projet vide ou en choisissant de ne pas répliquer les instantanés qui se trouvent dans le projet/les partages.
- Si vous répliquez un ensemble de données de grande taille et que la bande passante est limitée en raison de la distance entre les appareils source et cible, vous pouvez exporter la réplication vers un média hors ligne, comme décrit dans la section ["Création d'une réplication hors ligne \(BUI\)" à la page 486](#).

1. **Dans la BUI de l'appareil source, accédez à Partages > Projets.**
2. **Sélectionnez le projet ou le partage et cliquez sur l'onglet Réplication.**
3. **Cliquez sur l'icône d'ajout  en regard des Actions.**

4. Sélectionnez une cible et un pool.

Add Replication Action CANCEL ADD

Properties

Target

Pool

Export data path ☐

Limit bandwidth ☐

Enable SSL-encryption ☒

Disable compression ☐

Include snapshots ☒

Retain user snapshots on target ☐

Include clone origin as data ☐

Update frequency ☒ Scheduled ☐ Continuous

+ Schedule

5. Sélectionnez les propriétés pour cette action.

Pour obtenir une description de toutes les propriétés, reportez-vous à la section ["Propriétés des actions de réplication"](#) à la page 551.

6. Sélectionnez **Scheduled (programmé)**, et définissez une fréquence pour la mise à jour de réplication, ou sélectionnez **Continuous (continu)** pour envoyer les mises à jour de réplication en continu.

Vous pouvez également envoyer des mises à jour de réplication à la demande (voir la section ["Envoi manuel d'une mise à jour de réplication \(BUI\)"](#) à la page 485).

7. Cliquez sur **Ajouter**.

L'action de réplication est ajoutée à la BUI.

Actions		
TARGET ▲	UPDATES	STATUS
 sashimi Manual	Never Synced Never Attempted	 Sync now
 sushi Scheduled	2015-7-1 19:52:03 Synced 2015-7-1 19:52:03 Attempted	 2015-7-1 20:05:00 Next

Rubriques connexes

- ["Propriétés des actions de réplication" à la page 551](#)
- ["Actions et packages de réplication" à la page 533](#)

▼ Création d'une action de réplication (CLI)

Une action de réplication décrit le projet ou le partage à répliquer, l'emplacement où envoyer la réplication, le calendrier de réplication et les propriétés de transfert de données telles que l'activation ou la désactivation du chiffrement de la liaison réseau.

- Si vous configurez une réplication distante pour la première fois, il peut être utile de ne répliquer qu'un minimum de données pour garantir une synchronisation correcte. Vous pouvez répliquer un projet vide ou choisir de ne pas répliquer les instantanés dans le projet/les partages.
- Si vous répliquez un ensemble de données de grande taille et que la bande passante est limitée en raison de la distance entre les appareils source et cible, vous pouvez exporter la réplication, comme décrit dans la section ["Création d'une réplication hors ligne \(BUI\)" à la page 486](#).

1. Accédez au projet ou au partage et saisissez action :

```
host_source:shares PROJECT1/SHARE1 replication> action
```

2. Affichez les propriétés.

```
host_source:shares PROJECT1/SHARE1 action (uncommitted)> get
Properties:
    target = (unset)
    pool = (unset)
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    use_ssl = true
```

3. Définissez les propriétés pour cette action.

Pour obtenir une description des propriétés de la CLI, reportez-vous à la section ["Propriétés des actions de réplication"](#) à la page 551.

```
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set target=repl_sys
                        target = repl_sys (uncommitted)
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set pool=pool-0
                        pool = pool-0 (uncommitted)
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set include_snaps=false
                        include_snaps = false (uncommitted)
host_source:shares PROJECT1/SHARE1 action (uncommitted)> set use_ssl=false
                        use_ssl = false (uncommitted)
host_source:shares PROJECT1/SHARE1 action-000> schedule
host_source:shares PROJECT1/SHARE1 action-000 schedule (uncommitted)> set frequency=day
                        frequency = day (uncommitted)
host_source:shares PROJECT1/SHARE1 action-000 schedule (uncommitted)> set hour=23
                        hour = 23 (uncommitted)
host_source:shares PROJECT1/SHARE1 action-000 schedule (uncommitted)> set minute=05
                        minute = 05 (uncommitted)
```

4. Validez la nouvelle action de réplication.

```
host_source:shares PROJECT1/SHARE1 action (uncommitted)> commit
```

5. Pour afficher les propriétés de la nouvelle action créée, saisissez ls :

```
host_source:shares PROJECT1/SHARE1 replication> ls
Properties:
    inherited = false
Actions:
    TARGET          STATUS      NEXT
    action-000 repl_sys      idle       manual

host_source:shares PROJECT1/SHARE1 action-000> ls
Properties:
    id = a751dc0f-abcd-1234-6789-f5e8315eaffa
    target = repl_sys
    enabled = true
    continuous = false
    include_snaps = false
    max_bandwidth = unlimited
    use_ssl = false
    state = idle
state_description = Idle (no update pending)
next_update = Wed Sep 01 2013 23:05:00 GMT+0000 (UTC)
last_sync = Wed Sep 01 2013 10:24:05 GMT+0000 (UTC)
last_try = Wed Sep 01 2013 10:24:05 GMT+0000 (UTC)
last_result = success
```

6. Pour afficher l'ID de la nouvelle action créée, utilisez la commande last, qui accède au noeud avec la nouvelle action, avec la commande get id, qui récupère l'ID de l'action.

L'ID est utilisé ultérieurement pour sélectionner le noeud d'action de réplication approprié.

```
host_source:shares PROJECT1/SHARE1 replication>last get id
                        id =
fb1bb3fd-3361-42e1-e4a1-b06c426172fb
```

Rubriques connexes

- ["Propriétés des actions de réplication" à la page 551](#)
- ["Actions et packages de réplication" à la page 533](#)

▼ Configuration de la réplication pour un environnement de cluster

Cette section explique comment configurer la réplication dans un environnement de cluster. Suivez les étapes décrites ci-après pour configurer correctement la réplication afin de garantir que la réplication des projets se poursuit après une reprise du cluster, un rétablissement du cluster ou une réplication inverse sur un appareil cible.

Avant de commencer

S'il s'agit de la première fois que vous configurez la réplication pour des appareils en cluster, reportez-vous à la section ["Exemple : Configuration de réplication pour des appareils en cluster" à la page 538](#).

1. **Sur les appareils source et cible de la réplication, sélectionnez les interfaces réseau et les adresses IP à utiliser pour le trafic de réplication, en vous conformant aux recommandations suivantes :**
 - a. **Sélectionnez toujours une interface réseau singleton pour garantir qu'elle sera reprise par le noeud pair après une opération de reprise ou de rétablissement du cluster.**
 - b. **Sur le système source, assurez-vous que l'interface réseau sélectionnée et le pool de stockage à partir duquel les données seront répliquées sont tous les deux affectés au même noeud. C'est toujours le cas lorsque le cluster source est dans l'état CLUSTERED.**
 - c. **Sur le système cible, affectez au même noeud l'interface réseau sélectionnée sur l'appareil cible et le pool de stockage dans lequel les données répliquées seront placées. Cela permet de conserver l'association lorsque la configuration de réplication est effectuée pendant que le cluster cible est dans l'état CLUSTERED.**
 - d. **Assurez-vous que les systèmes source et cible peuvent communiquer à l'aide des interfaces réseau et des adresses IP sélectionnées.**

2. **Sur les appareils source et cible, créez des routes réseau statiques /32 (spécifiques aux hôtes) en utilisant les interfaces réseau et les adresses IP sélectionnées.**
3. **Sur l'appareil source, configurez l'objet cible de la réplication en utilisant l'adresse IP sélectionnée de la cible.**

▼ Envoi manuel d'une mise à jour de réplication (BUI)

Si une réplication continue ou programmée est déjà configurée, les mises à jour de réplication se feront automatiquement. Vous pouvez également mettre à jour manuellement à l'aide de la BUI.

1. **Depuis l'appareil source, accédez à Partages > Projets.**
2. **Ouvrez un projet et cliquez sur l'onglet Réplication.**
3. **Cliquez sur l'icône Synchroniser maintenant .**

Remarque - Cette action n'est en revanche pas possible si une mise à jour est en cours d'envoi. Assurez-vous que l'espace disque est suffisant pour répliquer l'intégralité du projet avant d'envoyer une mise à jour.

La BUI affiche une barre de progression et indique lorsque la mise à jour est terminée.

4. **Si la mise à jour de réplication échoue, supprimez toutes les anciennes actions ou tous les anciens instantanés et réessayez.**

Rubriques connexes

- ["Création d'une action de réplication \(BUI\)" à la page 480](#)
- ["Annulation d'une mise à jour de réplication \(BUI\)" à la page 507](#)

▼ Envoi manuel d'une mise à jour de réplication (CLI)

Si une réplication continue ou programmée est déjà configurée, les mises à jour de réplication se feront automatiquement. Vous pouvez également mettre à jour manuellement à l'aide de la CLI.

1. **Accédez au partage et saisissez la commande `sendupdate` :**

```
host_source:shares PROJECT1/SHARE1 action-000> sendupdate
```

Lorsque la mise à jour est actuellement active, la CLI affiche le statut `sending`.

2. **Si la réplication échoue, supprimez toutes les anciennes actions ou tous les anciens instantanés et réessayez.**

Rubriques connexes

- ["Création d'une action de réplication \(CLI\)" à la page 482](#)
- ["Annulation d'une mise à jour de réplication \(CLI\)" à la page 507](#)

Création d'une réplication hors ligne (BUI)

Utilisez les procédures suivantes pour créer une mise à jour de réplication hors ligne :

- ["Configuration d'un serveur NFS pour une réplication hors ligne" à la page 486](#)
- ["Configuration d'un chemin d'exportation vers le serveur NFS \(BUI\)" à la page 487](#)
- ["Exportation d'une mise à jour de réplication \(BUI\)" à la page 487](#)
- ["Vérification du flux de réplication sur le serveur NFS" à la page 488](#)
- ["Importation du flux de réplication à partir du serveur NFS \(BUI\)" à la page 488](#)
- ["Mise à jour manuelle de réseau \(BUI\)" à la page 489](#)
- ["Inversion de la réplication pour une réplication hors ligne \(BUI\)" à la page 489](#)

▼ Configuration d'un serveur NFS pour une réplication hors ligne

Les étapes de configuration d'un serveur NFS varient selon le type de serveur NFS que vous utilisez. Pour obtenir des instructions spécifiques, reportez-vous à la documentation de votre serveur NFS.

1. **Identifiez un serveur qui est prêt à être relié à un réseau et dont les services NFS sont activés.**
2. **En tant que root du serveur NFS, créez un système de fichiers ou un partage.**
3. **Définissez les droits d'accès au fichier pour exposer le partage NFS uniquement à l'adresse IP des appareils source et cible.**
4. **Pour chiffrer le flux de réplication, activez le chiffrement sur disque pour le partage NFS sur le serveur NFS.**

Remarque - Un flux de réplication exporté n'est jamais chiffré par l'appareil.

5. **Exportez le partage pour qu'il soit accessible pour le client NFS.**

6. Vérifiez que le système de fichiers soit partagé.

Étapes suivantes

- ["Configuration d'un chemin d'exportation vers le serveur NFS \(BUI\)" à la page 487](#)

▼ Configuration d'un chemin d'exportation vers le serveur NFS (BUI)

Avant de commencer

Identifiez ou créez une cible. Reportez-vous à la section ["Création d'une cible de réplication \(BUI\)" à la page 478](#).

1. Dans la BUI de l'appareil source, accédez à **Partages > Projets**.
2. Cliquez sur le projet, puis sur l'onglet **Réplication**.
3. Cliquez sur l'icône d'ajout  en regard des **Actions**.
4. Dans l'écran **Ajout d'actions de réplication**, sélectionnez **Exporter le chemin de données** et saisissez le chemin du partage NFS sous la forme : `nfs://server/path`.
5. Sélectionnez les propriétés supplémentaires pour cette action, puis cliquez sur **Ajouter**.

Remarque - Si vous configurez un calendrier ou sélectionnez le mode de réplication continu, la mise à jour se produit automatiquement après que les opérations d'export et d'import se sont terminées.

Étapes suivantes

- ["Exportation d'une mise à jour de réplication \(BUI\)" à la page 487](#)

▼ Exportation d'une mise à jour de réplication (BUI)

1. Depuis l'appareil source, accédez à **Partages > Projets**.
2. Cliquez sur le projet, puis sur l'onglet **Réplication**.
3. Cliquez sur l'icône d'exportation des données de réplication .
4. Vérifiez l'état de la réplication et attendez que cette dernière soit terminée.

Etapes suivantes

- ["Vérification du flux de réplication sur le serveur NFS" à la page 488](#)

▼ Vérification du flux de réplication sur le serveur NFS

1. **Accédez au répertoire NFS, vérifiez MD5 et affichez les métadonnées.**

```
bigfish25# pwd
/export/init_repl/rr_updates/96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
bigfish25# ls -l
total 67
-rw-r--r--  1 nobody  nobody      633 Nov 17 21:46 metadata.xml
-rw-----  1 nobody  nobody    31016 Nov 17 21:46 stream
-rw-----  1 nobody  nobody      33 Nov 17 21:46 stream.md5
bigfish25# md5sum stream
25b4671c9aaf34455a63e203bcecff49  stream
bigfish25# cat stream.md5
25b4671c9aaf34455a63e203bcecff49
bigfish25# cat metadata.xml
<?xml version="1.0"?>
<!DOCTYPE nvlist SYSTEM "/usr/share/lib/xml/dtd/nvlist.dtd.1">
<nvlist>
  <nvpair name='offline_rr_version'><string value='1.1' /></nvpair>
  <nvpair name='source_asn'><string value='2ea4670f-bc17-cf8f-a420-9211d6edda04' /></nvpair>
  <nvpair name='project'><string value='default' /></nvpair>
  <nvpair name='pkgid'><string value='96366bf2-0b3c-4eec-e85b-e36e1b5bc18c' /></nvpair>
  <nvpair name='basesnap'><string value='/' /></nvpair>
  <nvpair name='newsnap'><string value='.rr-96366bf2-0b3c-4eec-e85b-e36e1b5bc18c-1' /></nvpair>
</nvlist>
bigfish25#
```

2. **Déplacez physiquement le serveur NFS vers le site de l'appareil cible, ou copiez le dossier rr_updates sur un média externe et préparez son expédition.**

Etapes suivantes

- ["Importation du flux de réplication à partir du serveur NFS \(BUI\)" à la page 488](#)

▼ Importation du flux de réplication à partir du serveur NFS (BUI)

1. **Accédez à Partages > Projets > Répliques.**

2. Sélectionnez la réplique qui affiche la source : **importation en attente**.
3. Cliquez sur l'onglet **Réplication**.
4. Dans le champ **Importer le chemin de données**, saisissez le chemin de la réplique.
5. Cliquez sur l'icône d'importation de mise à jour à partir d'un média externe () pour démarrer l'importation.

Etapas suivantes

Une fois le flux de réplication importé sur l'appareil cible, exécutez l'une des procédures suivantes :

- ["Mise à jour manuelle de réseau \(BUI\)" à la page 489](#)
- ["Inversion de la réplication pour une réplication hors ligne \(BUI\)" à la page 489](#)

▼ Mise à jour manuelle de réseau (BUI)

Après l'importation du flux de réplication hors ligne sur l'appareil cible, confirmez que les mises à jour réseau à venir fonctionneront correctement. Si une réplication continue ou programmée est déjà configurée, la mise à jour se fera automatiquement. Sinon, mettez à jour manuellement.

1. Accédez à l'appareil source.
2. Reportez-vous à la section ["Envoi manuel d'une mise à jour de réplication \(BUI\)" à la page 485](#).

▼ Inversion de la réplication pour une réplication hors ligne (BUI)

Appliquez cette procédure pour déplacer un package de réplication hors ligne vers un nouveau projet local configuré pour la réplication sur l'appareil source.

1. Importez le package de réplication hors ligne à partir d'un serveur NFS vers l'appareil cible comme indiqué dans la section ["Importation du flux de réplication à partir du serveur NFS \(BUI\)" à la page 488](#).
2. A partir de l'appareil cible, accédez à **Partages > Projets > Réplique**, puis localisez le package répliqué.

Le projet est nommé *target_appliance:new_project/share*.

3. **Sélectionnez le projet et cliquez sur son icône d'inversion du sens de réplication** .

4. **Dans la fenêtre Réplication inversée, entrez le nom du nouveau projet local.**

Cette action déplace le contenu de ce package dans un nouveau projet local configuré pour effectuer une réplication vers la source. Toutes les modifications des données ou des métadonnées apportées à la source depuis la dernière mise à jour réussie sont perdues lorsque le nouveau projet est répliqué vers la source. Si les actions de réplication sur la source ne sont pas désactivées, les mises à jour ultérieures de ce package échoueront.

5. **Accédez à Partages > Projets.**

6. **Ouvrez le projet et cliquez sur l'onglet Réplication.**

7. **Cliquez sur l'icône d'exportation des données de réplication** .

8. **Vérifiez l'état de la réplication et attendez que cette dernière soit terminée.**

9. **Une fois la mise à jour de la réplication terminée, accédez au nouveau package inversé sur la nouvelle cible.**

La description de l'état devrait être Inactif (en attente d'importation).

10. **Importez la mise à jour à partir du serveur NFS.**

Rubriques connexes

- ["Création d'une réplication hors ligne \(BUI\)" à la page 486](#)

Création d'une réplication hors ligne (CLI)

Utilisez les procédures suivantes pour créer une mise à jour de réplication hors ligne :

- ["Configuration d'un serveur NFS pour une réplication hors ligne" à la page 491](#)
- ["Configuration d'un chemin d'exportation vers le serveur NFS \(CLI\)" à la page 491](#)
- ["Exportation d'une mise à jour de réplication \(CLI\)" à la page 492](#)
- ["Vérification d'un flux de réplication sur le serveur NFS" à la page 494](#)
- ["Importation d'un flux de réplication à partir du serveur NFS \(CLI\)" à la page 495](#)
- ["Mise à jour manuelle de réseau \(CLI\)" à la page 496](#)
- ["Inversion de la réplication pour une réplication hors ligne \(CLI\)" à la page 498](#)

▼ Configuration d'un serveur NFS pour une réplication hors ligne

Les étapes de configuration d'un serveur NFS varient selon le type de serveur NFS que vous utilisez. Pour obtenir des instructions spécifiques, reportez-vous à la documentation de votre serveur NFS.

1. **Identifiez un serveur qui est prêt à être relié à un réseau et dont les services NFS sont activés.**
2. **En tant que root du serveur NFS, créez un système de fichiers ou un partage.**
3. **Définissez les droits d'accès au fichier pour exposer le partage NFS uniquement à l'adresse IP des appareils source et cible.**
4. **Pour chiffrer le flux de réplication, activez le chiffrement sur disque pour le partage NFS sur le serveur NFS.**

Remarque - Un flux de réplication exporté n'est jamais chiffré par l'appareil.

5. **Exportez le partage pour qu'il soit accessible pour le client NFS.**
6. **Vérifiez que le système de fichiers soit partagé.**

Etapes suivantes

- ["Configuration d'un chemin d'exportation vers le serveur NFS \(CLI\)" à la page 491](#)

▼ Configuration d'un chemin d'exportation vers le serveur NFS (CLI)

1. **Identifiez ou créez une cible de réplication.**
2. **Créez une action de réplication, définissez le chemin `export_path` et validez (`commit`) la nouvelle action.**

```
source:shares default replication> action
source:shares default action (uncommitted)> set target=target_a
                                     target = target_a (uncommitted)
source:shares default action (uncommitted)> set pool=pool2
                                     pool = pool2 (uncommitted)
source:shares default action (uncommitted)> set export_path=nfs://nfs_server/export/
init_repl
                                     export_path = nfs://nfs_server/export/init_repl (uncommitted)
```

```
source:shares default action (uncommitted)>commit
```

Remarque - Vous pouvez configurer un mode de réplication continu ou programmé, qui lance la mise à jour après que les opérations d'export et d'import se sont terminées.

3. Accédez de nouveau à l'action de réplication que vous venez de créer et affichez le statut actuel.

```
source:shares default replication> ls
```

Actions:

	TARGET	STATUS	NEXT
action-000	target_a	idle	Export replication data

```
source:shares default replication> last
```

```
source:shares default action-000> ls
```

Properties:

```

        id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
        target = target_a
        enabled = true
        continuous = false
        include_snaps = true
        max_bandwidth = unlimited
        bytes_sent = 0
        estimated_size = 0
        estimated_time_left = 00:00:00
        average_throughput = 0B/s
        use_ssl = true
        compression = on
        export_path = nfs://nfs_server/export/init_repl
        state = idle
        state_description = Idle (export pending)
        export_pending = true
        offline = false
        next_update = Export replication data
        last_sync = <unknown>
        last_try = <unknown>
        last_result = <unknown>

```

Etapes suivantes

- ["Exportation d'une mise à jour de réplication \(CLI\)" à la page 492](#)

▼ Exportation d'une mise à jour de réplication (CLI)

1. Pour exporter la mise à jour de réplication vers le serveur NFS, utilisez la commande **sendupdate**.

```
source:shares default action-000>sendupdate
```

2. Saisissez `ls` pour afficher le statut, comme indiqué dans l'exemple suivant :

```
source:shares default action-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    target = target_a
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0
    estimated_time_left = 00:00:00
    average_throughput = 0B/s
    use_ssl = true
    compression = on
    export_path = nfs://nfs_server/export/init_repl
    state = sending
    state_description = Exporting update
    export_pending = true
    offline = false
    next_update = Export replication data
    last_sync = <unknown>
    last_try = <unknown>
    last_result = <unknown>
```

3. Pour déterminer quand l'exportation se termine, saisissez `ls` pour afficher le statut.

Recherchez `last_result=success`, comme indiqué dans l'exemple suivant :

```
source:shares default action-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    target = target_a
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0
    estimated_time_left = 00:00:00
    average_throughput = 0B/s
    use_ssl = true
    compression = on
    export_path =
    state = idle
    state_description = Idle (no update in progress)
    export_pending = false
    offline = true
    next_update = Sync now
    last_sync = <unknown>
    last_try = Tue Nov 18 2014 04:40:40 GMT+0000 (UTC)
    last_result = success
```

```
source:shares default action-000>
```

Etapes suivantes

- ["Vérification d'un flux de réplication sur le serveur NFS" à la page 494](#)

▼ Vérification d'un flux de réplication sur le serveur NFS

1. **Accédez au répertoire NFS, vérifiez MD5 et affichez les métadonnées.**

```
nfs_server# pwd
/export/init_repl/rr_updates/96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
nfs_server# ls -l
total 67
-rw-r--r--  1 nobody  nobody      633 Nov 17 21:46 metadata.xml
-rw-----  1 nobody  nobody    31016 Nov 17 21:46 stream
-rw-----  1 nobody  nobody      33 Nov 17 21:46 stream.md5
nfs_server# md5sum stream
25b4671c9aaf34455a63e203bcecff49  stream
nfs_server# cat stream.md5
25b4671c9aaf34455a63e203bcecff49
nfs_server# cat metadata.xml
<?xml version="1.0"?>
<!DOCTYPE nvlist SYSTEM "/usr/share/lib/xml/dtd/nvlist.dtd.1">
<nvlist>
  <nvpair name='offline_rr_version'><string value='1.1'/></nvpair>
  <nvpair name='source_asn'><string value='2ea4670f-bc17-cf8f-a420-9211d6edda04'/></nvpair>
  <nvpair name='project'><string value='default'/></nvpair>
  <nvpair name='pkgid'><string value='96366bf2-0b3c-4eec-e85b-e36e1b5bc18c'/></nvpair>
  <nvpair name='basesnap'><string value=''/></nvpair>
  <nvpair name='newsnap'><string value='.rr-96366bf2-0b3c-4eec-e85b-e36e1b5bc18c-1'/></nvpair>
  <nvpair name='compression'><string value='on'/></nvpair>
</nvlist>
nfs_server#
```

2. **Déplacez physiquement le serveur NFS vers le site de l'appareil cible, ou copiez le dossier rr_updates sur un média externe et préparez son expédition.**

Etapes suivantes

- ["Importation d'un flux de réplication à partir du serveur NFS \(CLI\)" à la page 495](#)

▼ Importation d'un flux de réplication à partir du serveur NFS (CLI)

1. Pour importer le flux de réplication à partir du serveur NFS, accédez au package vide sur la cible.

```
target_a:configuration services replication sources> ls
Sources:
source-000 203.80.49.153
          PROJECT          STATE          LAST UPDATE
package-000 <awaiting import>   idle           unknown
```

2. Sélectionnez le noeud source correspondant à l'adresse de votre système source.

```
target_a:configuration services replication sources> select source-000
target_a:configuration services replication source-000> ls
Properties:
          name = 203.80.49.153
          ip_address = 203.80.49.153:216
          asn = 2ea4670f-bc17-cf8f-a420-9211d6edda04
```

```
Packages:
          PROJECT          STATE          LAST UPDATE
package-000 <awaiting import>   idle           unknown
```

3. Sélectionnez le package qui est en attente d'importation.

```
target_a:configuration services replication source-000> select package-000
target_a:configuration services replication source-000 package-000> ls
Properties:
          id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
          enabled = true
          state = idle
          state_description = Idle (awaiting import)
          offline = true
          import_path =
          last_sync = unknown
          last_try = unknown
          last_result = unknown
```

4. Définissez le chemin d'importation des données répliquées, puis entrez commit.

```
target_a:configuration services replication source-000 package-000> set import_path=
nfs://nfs_server/export/init_repl
          import_path = nfs://nfs_server/export/init_repl (uncommitted)
target_a:configuration services replication source-000 package-000> commit
target_a:configuration services replication source-000 package-000> ls
Properties:
          id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
          enabled = true
          state = receiving
```

```

state_description = Importing update
  offline = true
  import_path = nfs://nfs_server/export/init_repl
  last_sync = unknown
  last_try = unknown
  last_result = unknown

target_a:configuration services replication source-000 package-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    enabled = true
    state = idle
state_description = Idle (no update in progress)
  offline = false
  import_path =
  last_sync = Tue Nov 18 2014 05:03:42 GMT+0000 (UTC)
  last_try = Tue Nov 18 2014 05:03:42 GMT+0000 (UTC)
  last_result = success
Projects:
    default
target_a:configuration services replication source-000 package-000>

```

Etapes suivantes

Une fois le flux de réplication importé sur l'appareil cible, exécutez l'une des procédures suivantes :

- ["Mise à jour manuelle de réseau \(CLI\)" à la page 496](#)
- ["Inversion de la réplication pour une réplication hors ligne \(CLI\)" à la page 498](#)

▼ Mise à jour manuelle de réseau (CLI)

Après l'importation du flux de réplication hors ligne sur l'appareil cible, confirmez que les mises à jour réseau à venir fonctionneront correctement. Si une réplication continue ou programmée est déjà configurée, la mise à jour se fera automatiquement. Sinon, mettez à jour manuellement comme indiqué dans l'exemple suivant.

1. Accédez à l'appareil source, puis au partage.

```

source:shares default action-000> ls
Properties:
    id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
    target = target_a
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0

```



```

estimated_time_left = 00:00:00
average_throughput = 0B/s
  use_ssl = true
  compression = on
  export_path =
  state = idle
state_description = Idle (no update in progress)
export_pending = false
  offline = true
  next_update = Sync now
  last_sync = <unknown>
  last_try = Tue Nov 18 2014 04:40:40 GMT+0000 (UTC)
  last_result = success

```

2. Démarrez la mise à jour à l'aide de la commande `sendupdate`, puis affichez le statut à l'aide de la commande `ls`.

source:shares default action-000> **sendupdate**

source:shares default action-000> **ls**

Properties:

```

      id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
      target = target1
      enabled = true
      continuous = false
      include_snaps = true
      max_bandwidth = unlimited
      bytes_sent = 0
      estimated_size = 0
estimated_time_left = 00:00:00
average_throughput = 0B/s
  use_ssl = true
  compression = on
  export_path =
  state = sending
state_description = Ready (awaiting available resources to send update)
export_pending = false
  offline = true
  next_update = Sync now
  last_sync = <unknown>
  last_try = Tue Nov 18 2014 04:40:40 GMT+0000 (UTC)
  last_result = success

```

source:shares default action-000> **ls**

Properties:

```

      id = 96366bf2-0b3c-4eec-e85b-e36e1b5bc18c
      target = target1
      enabled = true
      continuous = false
      include_snaps = true
      max_bandwidth = unlimited
      bytes_sent = 0
      estimated_size = 0
estimated_time_left = 00:00:00
average_throughput = 0B/s

```

```

        use_ssl = true
        compression = on
        export_path =
            state = idle
        state_description = Idle (no update in progress)
        export_pending = false
        offline = false
        next_update = Sync now
        last_sync = Tue Nov 18 2014 04:40:40 GMT+0000 (UTC)
        last_try = Tue Nov 18 2014 04:40:40 GMT+0000 (UTC)
        last_result = success
    
```

▼ Inversion de la réplication pour une réplication hors ligne (CLI)

Appliquez cette procédure pour déplacer un package de réplication hors ligne vers un nouveau projet local configuré pour la réplication sur l'appareil source.

Avant de commencer

Importez le flux de réplication hors ligne d'un serveur NFS vers l'appareil cible, comme décrit dans la section ["Importation d'un flux de réplication à partir du serveur NFS \(CLI\)" à la page 495](#).

1. Depuis l'appareil cible, accédez au package répliqué et localisez le projet.

```

target:configuration services replication source-000 package-000> ls
Properties:
    id = 1c0457eb-45bd-4f91-8e08-bc0dbacd40b7
    enabled = true
    state = idle
    state_description = Idle (no update in progress)
    offline = false
    import_path =
        last_sync = Fri Jul 31 2015 21:59:19 GMT+0000 (UTC)
        last_try = Fri Jul 31 2015 21:59:19 GMT+0000 (UTC)
        last_result = success

Projects:
    proj1
    
```

2. Entrez reverse et le nom de projet.

```

target:configuration services replication source-000 package-000> reverse proj1
This action will move the contents of this package to a new local project configured to
replicate back to the source.
Any data or metadata changes made on the source since the last successful update will be lost
when the new project is
replicated back to the source. If replication actions on the source are not disabled, future
updates to this package
will fail.
    
```

Are you sure? (Y/N) Y

3. Accédez à la nouvelle action de réplication.

```
target:configuration services replication sources> cd /
target:> shares select proj1 replication
target:shares proj1 replication> select action-000
target:shares proj1 action-000> ls
Properties:
        id = 6a10ce61-cc87-4850-89dd-8673f7734d03
        target = new_target
        enabled = true
        continuous = false
        include_snaps = false
        retain_user_snaps_on_target = false
        max_bandwidth = unlimited
        bytes_sent = 0
        estimated_size = 0
        estimated_time_left = 00:00:00
        average_throughput = 0B/s
        use_ssl = false
        compression = on
        export_path =
        state = idle
        state_description = Idle (no update in progress)
        export_pending = false
        offline = false
        next_update = Sync now
        last_sync = <unknown>
        last_try = <unknown>
        last_result = <unknown>
```

4. Pour exporter la première mise à jour de réplication après l'inversion vers un serveur NFS, entrez export_path et le nom du chemin vers le serveur NFS. Entrez commit et exécutez sendupdate.

```
target:shares proj1 action-000> set export_path=nfs://nfs_server/export/init_repl
        export_path = nfs://nfs_server/export/init_repl (uncommitted)
target:shares proj1 action-000> commit
target:shares proj1 action-000> sendupdate
target:shares proj1 action-000> ls
Properties:
        id = 6a10ce61-cc87-4850-89dd-8673f7734d03
        target = new_target
        enabled = true
        continuous = false
        include_snaps = false
        retain_user_snaps_on_target = false
        max_bandwidth = unlimited
        bytes_sent = 0
        estimated_size = 0
        estimated_time_left = 00:00:00
```

```

average_throughput = 0B/s
  use_ssl = false
  compression = on
  export_path =
    state = idle
state_description = Idle (no update in progress)
export_pending = false
  offline = true
  next_update = Sync now
  last_sync = <unknown>
  last_try = Fri Jul 31 2015 22:17:33 GMT+0000 (UTC)
  last_result = success

```

5. **Une fois la mise à jour de la réplication terminée, accédez au nouveau package inversé sur la nouvelle cible. La description de l'état devrait être Inactif (en attente d'importation), comme l'indique l'exemple suivant :**

```

new_target:configuration services replication sources> ls
Sources:

source-000 <unknown>
      PROJECT                STATE                LAST UPDATE
package-000 proj1          idle                unknown

new_target:configuration services replication sources> select source-000 select package-000
new_target:configuration services replication source-000 package-000> ls
Properties:

      id = 6a10ce61-cc87-4850-89dd-8673f7734d03
      enabled = true
      state = idle
state_description = Idle (awaiting import)
  offline = true
  import_path =
    last_sync = unknown
    last_try = unknown
    last_result = unknown

Projects:

      proj1
new_target:configuration services replication source-000 package-000> set import_path=nfs://
nfs_server/export/init_repl
      import_path = nfs://nfs_server/export/init_repl (uncommitted)

```

6. **Importez la mise à jour à partir du serveur NFS.**

```

new_target:configuration services replication source-000 package-000> set import_path=nfs://
nfs_server/export/init_repl
      import_path = nfs://nfs_server/export/init_repl (uncommitted)

```

7. **Entrez commit et répertoriez les propriétés du package pour confirmer l'exécution de la mise à jour.**

```

new_target:configuration services replication source-000 package-000> commit

```

```
new_target:configuration services replication source-000 package-000> ls
Properties:
```

```

    id = 6a10ce61-cc87-4850-89dd-8673f7734d03
    enabled = true
    state = idle
    state_description = Idle (no update in progress)
    offline = false
    import_path =
    last_sync = Fri Jul 31 2015 22:11:32 GMT+0000 (UTC)
    last_try = Fri Jul 31 2015 22:11:32 GMT+0000 (UTC)
    last_result = success
```

Projects:

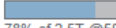
proj1

Rubriques connexes

- ["Importation d'un flux de réplication à partir du serveur NFS \(CLI\)" à la page 495](#)

▼ Surveillance de la progression de la réplication (BUI)

1. Pour surveiller la progression d'une mise à jour de réplication, accédez à Partages > Projets.
2. Cliquez sur l'onglet Réplication. Sous la barre de progression, vérifiez le pourcentage d'octets envoyés, la taille estimée, le débit moyen et le temps restant estimé.

TARGET ▲	UPDATES	STATUS
 brmzs3-2-250 Scheduled	2014-12-24 02:49:52 Synced 2014-12-24 02:49:52 Attempted	  78% of 2.5T @50MB/s (-03:13:10)

Rubriques connexes

- ["Alertes de réplication et événements d'audit" à la page 502](#)
- ["Utilisation des analyses de réplication" à la page 503](#)

▼ Surveillance de la progression de la réplication (CLI)

1. Pour surveiller la progression d'une mise à jour de réplication, accédez au projet ou au partage.
2. Déterminez la progression en vérifiant les propriétés `bytes_sent`, `estimate_size`, `estimated_time_left` et `average_throughput`.

```
brmzs3-2-460:shares 460-non-encrypt action-000> ls
Properties:
    id = 96329c98-6a97-4fd4-810e-be9529ce4dcf
    target = brmzs3-2-250
    enabled = true
    continuous = false
    include_snaps = true
    max_bandwidth = unlimited
    bytes_sent = 1.93T
    estimated_size = 2.5T
    estimated_time_left = 03:11:11
    average_throughput = 50MB/s
    use_ssl = true
    compression = on
    export_path =
    state = sending
    state_description = Sending update
    export_pending = false
    offline = false
    next_update = Wed Dec 24 2014 21:00:00 GMT+0000 (UTC)
    last_sync = Wed Dec 24 2014 08:49:52 GMT+0000 (UTC)
    last_try = Wed Dec 24 2014 08:49:52 GMT+0000 (UTC)
    last_result = success
```

Rubriques connexes

- ["Alertes de réplication et événements d'audit" à la page 502](#)
- ["Utilisation des analyses de réplication" à la page 503](#)

Alertes de réplication et événements d'audit

Le système affiche des alertes lorsque l'un des événements suivants se produit :

- Une mise à jour de réplication manuelle ou programmée démarre ou se termine avec succès (source et cible).
- Une mise à jour de réplication échoue, y compris consécutivement à une annulation expresse de l'administrateur (source et cible).
- Une mise à jour de réplication programmée est ignorée car une autre mise à jour pour la même action est déjà en cours.
- Lorsqu'une réplication continue démarre pour la première fois.
- Lorsqu'une réplication continue échoue.
- Lorsqu'une réplication continue démarre pour la première fois, échoue ou reprend après un échec.

Le système contrôle les événements de réplication suivants et les enregistre dans le journal d'audit.

- Création, modification ou destruction d'actions de réplication
- Ajout ou suppression de partages d'un groupe de réplication
- Création, modification, clonage, inversion, dissociation ou destruction de packages de réplication sur la cible
- Création, modification ou destruction de cibles de réplication

Utilisation des analyses de réplication

Les analyses suivantes sont disponibles pour la réplication :

- Déplacement de données : opérations de réplication
- Déplacement de données : octets de réplication
- Analyse avancée
- Déplacement de données : octets envoyés/reçus lors de la réplication

Pour plus d'informations sur la fonction d'analyse, reportez-vous à la section "[Utilisation de la fonction d'analyse](#)" dans le *Guide de la fonction d'analyse des systèmes Oracle ZFS Storage Appliance*.

▼ Modification d'une cible de réplication (BUI)

1. **Accédez à Configuration > Services > Réplication distante > Cibles.**
2. **Pour la cible que vous souhaitez modifier, déplacez le curseur sur le nom de la cible et cliquez sur l'icône Modifier .**
3. **Modifiez le nom et/ou le nom d'hôte.**

Le nom d'hôte ou l'adresse IP doit correspondre au même appareil qu'avant (vérifié par le numéro de série sur la cible).

Remarque - Si vous souhaitez pointer vers un autre appareil que celui configuré précédemment, vous devez créer une nouvelle cible pour authentifier vis-à-vis du nouvel appareil.

4. **Cliquez sur Appliquer pour enregistrer les modifications apportées.**

Rubriques connexes

- "[Concepts de la réplication distante](#)" à la page 529
- "[Workflow de réplication distante](#)" à la page 474

▼ Modification d'une cible de réplication (CLI)

1. **Accédez au noeud `targets` pour définir ou annuler le paramétrage de la cible `hostname`, `root_password` et `label`.**

```
knife:> configuration services replication targets
```

2. **Depuis ce contexte, vous pouvez :**

- Ajouter de nouvelles cibles.
- Consulter les actions configurées avec la cible existante.
- Modifier l'identifiant unique (étiquette) et/ou le nom d'hôte de la cible.
- Supprimer une cible si aucune action ne l'utilise.

Remarque - La cible ne doit pas être supprimée tant que des actions l'utilisent. Ces actions seraient interrompues de manière permanente. Le système s'efforce d'appliquer cela mais ne peut garantir l'absence d'action dans les pools de stockage exportés qui utilisent une cible donnée.

3. **Si le partage que vous répliquez est chiffré, assurez-vous que la cible prend également en charge le chiffrement de données.**

Rubriques connexes

- ["Réplication d'un partage chiffré" à la page 589](#)
- ["Cibles de réplication" à la page 532](#)

▼ Modification d'une mise à jour de réplication (BUI)

1. **Accédez au projet ou au partage et cliquez sur l'onglet `Réplication`.**
2. **Sélectionnez le projet ou le partage à modifier.**
3. **Cliquez sur l'icône `Modifier` .**
4. **A partir de l'écran `Modifier l'action de réplication`, modifiez les propriétés, puis cliquez sur `Appliquer`.**

Pour obtenir une description des actions de réplication, reportez-vous à la section ["Propriétés des actions de réplication" à la page 551](#).

Rubriques connexes

- ["Actions et packages de réplication" à la page 533](#)

- ["Workflow de réplication distante" à la page 474](#)

▼ Modification d'une mise à jour de réplication (CLI)

1. **Accédez à la cible associée à l'action à modifier, puis sélectionnez-la.**

```
otero:configuration services replication targets> show
Targets:
  TARGET      LABEL      ACTIONS
  target-000  oakmeal    1
otero:configuration services replication targets> select target-000
otero:configuration services replication target-000> show
Properties:
  address = 10.153.34.167:216
  label = oakmeal
  hostname = oakmeal-7320-167
  asn = 4913649f-7549-6d2a-866b-987ddbc4e163
  actions = 1
```

2. **Affichez les actions associées à la cible sélectionnée à l'aide de la commande `actions` :**

```
oakmeal-7320-167:shares project1 replication target-000> actions
POOL      PROJECT      SHARE
pool1     project1     (multiple)
```

3. **Accédez à l'action et modifiez les propriétés, le cas échéant.**
Pour obtenir une liste des commandes d'action de réplication pour la CLI, reportez-vous à la section ["Propriétés des actions de réplication" à la page 551](#).

Rubriques connexes

- ["Création d'une action de réplication \(CLI\)" à la page 482](#)
- ["Workflow de réplication distante" à la page 474](#)

▼ Désactivation de la compression de réplication (BUI)

Vous pouvez désactiver la compression lorsque vous créez ou modifiez une action de réplication. Par défaut, tous les flux de réplication sont compressés avant d'être envoyés sur le réseau.

1. **Depuis l'appareil source, accédez à `Partages > Projets >`, puis double-cliquez sur le projet que vous souhaitez modifier.**
2. **Cliquez sur l'onglet `Réplication`.**
3. **Cliquez sur l'icône `Modifier` .**

4. Cliquez sur **Désactiver la compression**, puis sur **Appliquer**.

Rubriques connexes

- ["Réplication compressée" à la page 552](#)
- ["Workflow de réplication distante" à la page 474](#)

▼ Désactivation de la compression de réplication (CLI)

Vous pouvez désactiver la compression lorsque vous créez ou modifiez une action de réplication. Par défaut, tous les flux de réplication sont compressés avant d'être envoyés sur le réseau. Pour plus d'informations, reportez-vous la section ["Réplication compressée" à la page 552](#).

1. **Pour désactiver la compression, accédez au projet ou au partage et définissez la propriété `compression`, comme indiqué dans l'exemple suivant :**

```
eel:shares proj1 action-000> set compression=off
```

2. **Saisissez `commit` puis `show` pour confirmer la désactivation de la propriété `compression`.**

```
eel:shares proj1 action-000> commit
eel:shares proj1 action-000> show
Properties:
    id = 67f0d3d6-10af-6f30-9d4c-a60d19eb1200
    target = goby-10g
    enabled = true
    continuous = false
    include_snaps = false
    max_bandwidth = unlimited
    bytes_sent = 0
    estimated_size = 0
    estimated_time_left = 00:14:35
    average_throughput = 0B/s
    use_ssl = false
    compression = off
    export_path =
    state = idle
    state_description = idle (no update in progress)
    export_pending = false
    offline = false
    next_update = Sync now
    last_sync = <unknown>
    last_try =
    last_result =
```

Rubriques connexes

- ["Réplication compressée" à la page 552](#)

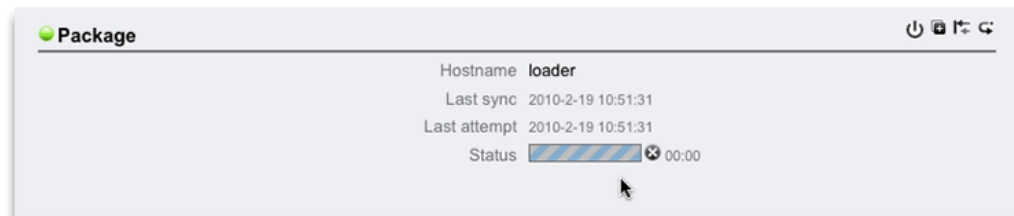
- ["Workflow de réplication distante" à la page 474](#)

▼ Annulation d'une mise à jour de réplication (BUI)

Les packages de réplication sont affichés en tant que projet sous le filtre "Réplique".

1. Depuis l'appareil source, accédez à **Partages > Projets** et cliquez sur **Réplique**.
2. Cliquez sur l'onglet **Réplication**.

Si une mise à jour est en cours, vous verrez une barre de progression hachurée avec une icône d'annulation (ⓧ) situé en regard, comme dans l'illustration suivante :



3. Cliquez sur l'icône d'annulation ⓧ.

L'annulation peut nécessiter plusieurs secondes.

Remarque - Une mise à jour manuelle ne peut pas être lancée depuis l'appareil cible. Vous devez vous connecter à l'appareil source pour lancer une mise à jour manuelle.

Rubriques connexes

- ["Packages de réplication" à la page 553](#)
- ["Envoi manuel d'une mise à jour de réplication \(BUI\)" à la page 485](#)

▼ Annulation d'une mise à jour de réplication (CLI)

Vous pouvez annuler une mise à jour de réplication en cours sur une cible. Les packages de réplication sont organisés par source dans la CLI sous `shares replication sources`.

1. Depuis l'appareil cible, accédez au package de réplication.

```
loader:> shares replication sources
```

```
loader:shares replication sources> show
Sources:

source-000 ayu
      PROJECT   STATE   LAST UPDATE
package-000 oldproj   idle   unknown
package-001 aproj1    receiving Sun Feb 21 2010 22:04:35 GMT+0000 (UTC)
```

2. Sélectionnez d'abord la source, puis un package.

```
loader:shares replication sources> select source-000
loader:shares replication source-000> select package-001
```

3. Saisissez `cancelupdate`.

```
loader:shares replication source-000 package-001> cancelupdate
```

L'annulation peut nécessiter plusieurs secondes.

Remarque - Une mise à jour manuelle ne peut pas être lancée depuis l'appareil cible. Vous devez vous connecter à l'appareil source pour lancer une mise à jour manuelle.

Rubriques connexes

- ["Packages de réplication" à la page 553](#)
- ["Envoi manuel d'une mise à jour de réplication \(CLI\)" à la page 485](#)

▼ Clonage d'un package de réplication (BUI)

Le clone d'un package de réplication repose sur l'instantané de réplication le plus récent reçu.

Lorsque vous créez un projet cloné, évitez les conflits de noms en respectant les règles suivantes :

- Le projet cloné doit avoir un nom unique au sein du pool de projets considéré.
- Le point de montage et le nom de ressource SMB de tous les partages du projet cloné ne doivent créer de conflit avec aucun point de montage ou nom de ressource SMB existant.
- En ce qui concerne les partages qui héritent des propriétés de projet, réglez les conflits en remplaçant le point de montage et/ou le nom de ressource SMB au niveau du projet.
- Dans le cas des partages qui n'héritent pas des propriétés du projet, définissez un suffixe qui sera ajouté au point de montage et/ou aux noms de ressource SMB pour résoudre les conflits, ou bien remplacez individuellement le point de montage ou le nom de ressource SMB pour chaque partage.

Procédez comme suit pour cloner un package de réplication.

1. **Depuis l'appareil cible, accédez au package de réplication que vous souhaitez cloner.**
2. **Cliquez sur l'onglet Réplication.**
3. **Cliquez sur l'icône de clonage .**
4. **Dans la boîte de dialogue Cloner le projet de réplication, renseignez les champs suivants :**
 - a. **Nouveau projet - Entrez un nom unique pour le nouveau projet (clone).**

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.
 - b. **(Facultatif) Point de montage - Entrez un point de montage unique au niveau du projet pour le clone.**

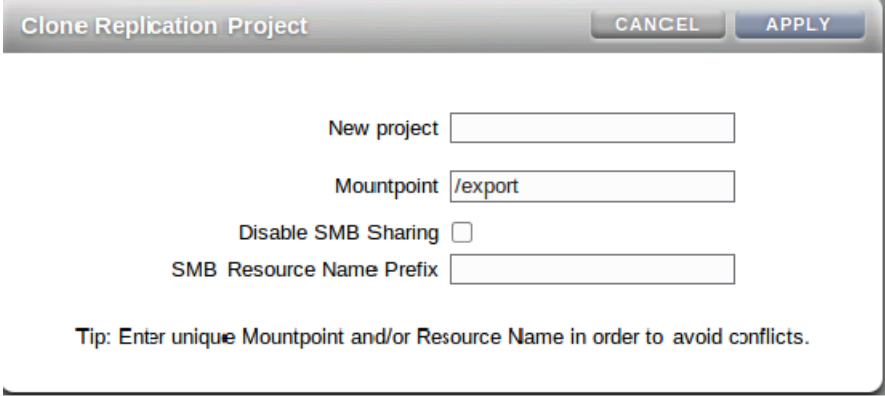
Ce paramètre s'applique aux partages qui héritent du point de montage du projet. La saisie d'un point de montage unique permet d'éviter les conflits.
 - c. **(Facultatif) Désactiver le partage SMB - Cochez pour désactiver SMB.**

Ce paramètre s'applique aux partages qui héritent du partage SMB du projet. Les partages qui n'héritent pas du partage SMB du projet ne sont pas concernés. La désactivation du partage SMB au niveau projet n'a aucun effet sur les partages qui n'héritent pas du partage SMB du projet.

Notez qu'une fois les options de partage SMB modifiées pour un package de réplication, le package cesse de refléter les modifications apportées à la source de réplication. Il devra être réinitialisé au niveau approprié après dissociation ou inversion.
 - d. **(Facultatif) Préfixe du nom de ressource SMB - Entrez un nom de ressource SMB.**

Ce paramètre s'applique aux partages qui héritent du nom de ressources SMB du projet. La saisie d'un nom de ressource unique permet d'éviter les conflits.

Lorsque SMB est activé, le clone peut être partagé via SMB. Le nom de ressource SMB utilisé pour partager les partages hérités du nouveau projet cloné sera constitué à l'aide du préfixe que vous ajoutez et du nom du partage correspondant.



The dialog box titled "Clone Replication Project" has a "CANCEL" button and an "APPLY" button in the top right corner. It contains four input fields: "New project" (empty), "Mountpoint" (containing "/export"), "Disable SMB Sharing" (checkbox, unchecked), and "SMB Resource Name Prefix" (empty). Below the fields is a tip: "Tip: Enter unique Mountpoint and/or Resource Name in order to avoid conflicts."

5. Cliquez sur **APPLIQUER**.

Une alerte s'affiche si le nom de projet est déjà en cours d'utilisation.

En l'absence de conflit de point de montage ou de nom de ressource, l'opération de clonage démarre.

6. (Facultatif) Si des conflits sont détectés, utilisez les boîtes de dialogue supplémentaires pour les résoudre.

a. Réglez les conflits qui héritent du projet un point de montage et/ou des noms de ressource SMB.



The dialog box titled "Clone Replication Project (Resolve Conflicts)" has a "CANCEL" button and an "APPLY" button in the top right corner. It shows "New project: clone-project". Below this, a message states: "Conflicts detected for mountpoints and/or SMB resource names that inherit from the project. Use project level setting to resolve the conflicts." There are three input fields: "Mountpoint" (containing "/export"), "Disable SMB Sharing" (checkbox, unchecked), and "SMB Resource Name Prefix" (empty). At the bottom, there is a section titled "List of Conflicting Shares" with a "Total: 1" indicator, followed by a table with columns for "Share Name", "Mountpoint", and "SMB Resource Name".

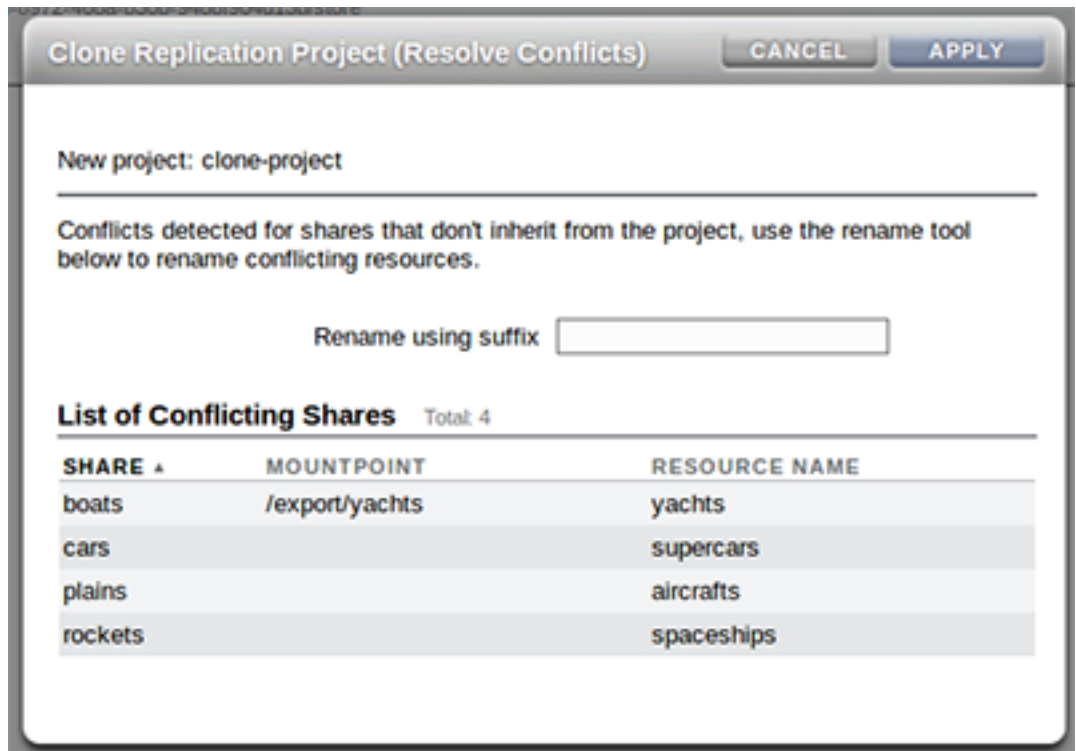
i. Entrez un point de montage unique.

ii. Désactivez le partage SMB ou entrez un préfixe de nom de ressource SMB unique.

iii. Cliquez sur **APPLIQUER**.

- b. **Réglez les conflits liés aux partages qui n'héritent du projet ni point de montage, ni noms de ressource SMB.**

Cette boîte de dialogue s'affiche uniquement après avoir résolu tous les conflits affectant les partages héritiers.



- i. Entrez un suffixe unique qui s'ajoutera au point de montage et/ou aux noms de ressource SMB de ces partages.
 - ii. Cliquez sur **APPLIQUER**.
7. S'il existe encore des conflits, répétez l'étape 6.

Rubriques connexes

- ["Clonage d'un package de réplication ou d'un partage" à la page 554](#)
- ["Packages de réplication" à la page 553](#)

▼ Clonage d'un package de réplication (CLI)

Le clone d'un package de réplication repose sur l'instantané de réplication le plus récent reçu.

Lorsque vous créez un projet cloné, évitez les conflits de noms en respectant les règles suivantes :

- Le projet cloné doit avoir un nom unique au sein du pool de projets considéré.
- Le point de montage et le nom de ressource SMB de tous les partages du projet cloné ne doivent créer de conflit avec aucun point de montage ou nom de ressource SMB existant.
- En ce qui concerne les partages qui héritent des propriétés de projet, réglez les conflits en remplaçant le point de montage et/ou le nom de ressource SMB au niveau du projet.
- Dans le cas des partages qui n'héritent pas des propriétés du projet, définissez un suffixe qui sera ajouté au point de montage et/ou aux noms de ressource SMB pour résoudre les conflits, ou bien remplacez individuellement le point de montage ou le nom de ressource SMB pour chaque partage.

Procédez comme suit pour cloner un package de réplication.

Dans la CLI, vous pouvez également résoudre des conflits en remplaçant les propriétés pour chaque partage séparément.

1. **A partir de l'appareil cible, accédez à `shares replication sources` et sélectionnez la source du package de réplication que vous souhaitez cloner.**

```
hostname:shares replication sources> select source-000
hostname:share replication sources source-000>
```

2. **Sélectionnez le package de réplication que vous souhaitez cloner.**

```
hostname:shares replication source-000> select package-004
hostname:shares replication source-000 package-004>
```

Impossible d'utiliser la commande `list` pour afficher tous les packages de réplication disponibles à partir de cette source.

```
hostname:shares replication source-000> list
PROJECT                STATE                LAST UPDATE
package-000 p3         idle                Tue Apr 21 2015 19:50:43 GMT+0000 (UTC)
package-001 p2         idle                Mon Apr 27 2015 17:05:16 GMT+0000 (UTC)
package-002 p1         idle                Mon Apr 27 2015 17:00:25 GMT+0000 (UTC)
package-003 p4         idle                Tue Apr 21 2015 21:37:16 GMT+0000 (UTC)
package-004 store      idle                Mon Apr 27 2015 16:40:26 GMT+0000 (UTC)
hostname:shares replication source-000>
```

3. **Entrez `clone` pour créer un nouveau projet cloné.**

```
hostname:shares replication source-000 package-004> clone
hostname:shares replication source-000 package-004 clone>
```


4. Définissez target_project sur le nom de projet.

Le nom du projet doit être unique, sinon l'opération de clonage échouera.

Un nom de projet doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces, ni commencer par un point. Les caractères alphanumériques et spéciaux `_` `-` `.` `:` sont autorisés.

```
hostname:shares replication source-000 package-004 clone> set target_project=clone
target_project = clone
```

5. Entrez conflicts pour identifier les conflits.

En cas de conflit, un message similaire au suivant s'affichera :

```
hostname:shares replication source-000 package-004 clone> conflicts
```

Cloning cannot proceed because the following shares have mountpoints or SMB resource names that are invalid or conflict with those of other shares (either on the system or also being failed over). Please specify valid mountpoints or SMB resource names for these shares:

SHARE	MOUNTPOINT	SHARESMB
appliances	/export/appliances	appliances
clothes	/export/clothes (inherited)	clothes (inherited)
electronics	/export/electronics	electronics
furniture	/export/furniture (inherited)	furniture (inherited)
groceries	/export/groceries (inherited)	groceries (inherited)
health	/export/health (inherited)	health (inherited)
toys	/export/toys	toys

```
hostname:shares replication source-000 package-004 clone>
```

Cette commande permet à tout instant au cours de la procédure d'identifier les conflits.

6. (Facultatif) Configurez les propriétés de niveau du projet pour résoudre les conflits concernant les partages qui héritent des propriétés d'un projet.

Utilisez la commande `get` pour afficher les propriétés du clone.

```
hostname:shares replication source-000 package-004 clone> get
```

```
target_project = (unset)
rename_suffix =
original_mountpoint = /export
mountpoint = /export
original_smb_resource_name = share
smb_resource_name = share
```

La propriété `original_mountpoint` indique le point de montage actuel. La propriété `original_smb_resource_name` indique le nom de ressource actuel.

a. Entrez un point de montage unique au niveau du projet pour le clone.

Ce paramètre s'applique aux partages qui héritent d'un point de montage fourni par un projet. Affectez à `original_mountpoint` la valeur `true`. Utilisez la commande `set mountpoint` pour définir le point de montage unique associé au clone.

```
hostname:shares replication source-000 package-004 clone> set original_mountpoint=true
hostname:shares replication source-000 package-004 clone> set mountpoint=/export/clone
hostname:shares replication source-000 package-004 clone>
```

b. Entrez un nom de ressource SMB unique au niveau du projet.

Ce paramètre s'applique aux partages qui héritent du nom de ressources SMB d'un projet. Affectez à `original_smb_resource_name` la valeur `true`. Affectez à `smb_resource_name` un nom de ressource SMB unique.

```
hostname:shares replication source-000 package-004 clone> set
original_smb_resource_name=true
hostname:shares replication source-000 package-004 clone> set smb_resource_name=clone-
share
smb_resource_name = clone-sharesmb
```

c. Définissez `rename_suffix` pour résoudre les conflits de partage restants.

Cette propriété crée un suffixe qui s'ajoute au point de montage et/ou aux noms de ressource SMB en cas de conflit.

```
hostname:shares replication source-000 package-004 clone> set rename_suffix=-clone
```

Remarque - Cette opération supprime le mécanisme d'héritage. Par exemple, si un partage hérite au départ du point de montage du projet, mais que le point de montage est ensuite renommé à l'aide d'un suffixe au cours du clonage, ce partage ne va pas hériter du point de montage du projet cloné mais utiliser celui qui a été renommé de manière unique.

7. Pour définir des propriétés spécifiques à un partage :

a. Sélectionnez le partage.

```
hostname:shares replication source-000 package-004 clone> select appliances
```

b. Remplacez son point de montage et/ou nom de ressource SMB, ou bien définissez `rename_suffix`.

Les exemples suivants montrent comment remplacer le point de montage associé à un partage.

```
hostname:shares replication source-000 package-004 clone appliances> set
original_mountpoint=/export
hostname:shares replication source-000 package-004 clone appliances> set mountpoint=/
export/clone
```

8. Entrez `confirm commit` pour lancer l'opération de clonage.

```
hostname:shares replication source-000 package-004 clone> confirm commit
```

Si des conflits de nom sont détectés, un message du type suivant va s'afficher :

Cloning cannot proceed because the following shares have mountpoints or SMB resource names that are invalid or conflict with those of other shares (either on the system or also being failed over). Please specify valid mountpoints or SMB resource names for these shares:

SHARE	MOUNTPOINT	SHARESMB
appliances	/export/appliances	appliances
clothes	/export/clothes (inherited)	clothes (inherited)
electronics	/export/electronics	electronics
furniture	/export/furniture (inherited)	furniture (inherited)

```
hostname:shares replication source-000 package-004 clone>
```

9. (Facultatif) Résolvez les conflits de noms restants, le cas échéant.

Répétez les étapes 6 et 7 jusqu'à ce qu'il ne subsiste aucun conflit.

Rubriques connexes

- ["Clonage d'un package de réplication ou d'un partage" à la page 554](#)
- ["Workflow de réplication distante" à la page 474](#)

▼ Modification d'un package de réplication (BUI)

1. Depuis l'appareil source, accédez à **Partages > Projets** et cliquez sur **Réplique**.

Le nom, la taille et la date de création de chaque package de réplication s'affiche.

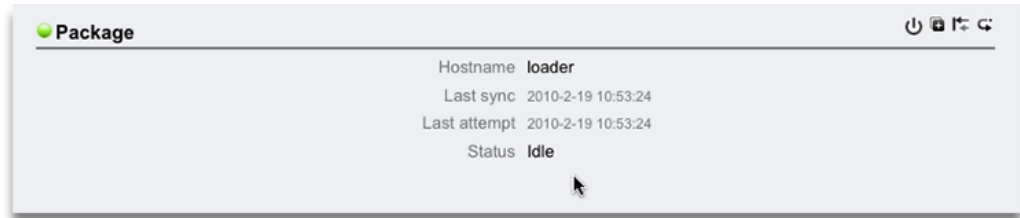


Projects 6 Total			
SHOW ALL LOCAL REPLICA			
NAME	SIZE	CREATION	
loader: default	50.1M	2010-2-18 09:45:49	
loader: default	100M	2010-2-18 13:42:25	

Remarque - Les packages sont affichés dans la BUI seulement après le début de la première mise à jour de réplication. Il est possible qu'ils n'apparaissent dans la liste que quelques instants après la fin de la première mise à jour.

2. Sélectionnez un package de réplication pour le modifier.

Vue des partages pour le projet du package s'affiche.



3. Cliquez sur l'onglet **Réplication** pour modifier les propriétés de package.

Pour obtenir une liste des propriétés que vous pouvez modifier, reportez-vous à la section ["Packages de réplication" à la page 553](#).

Rubriques connexes

- ["Actions et packages de réplication" à la page 533](#)
- ["Réplication distante" à la page 473](#)

▼ Modification d'un package de réplication (CLI)

Les packages de réplication sont organisés par source dans la CLI sous `shares replication sources`.

1. Depuis l'appareil cible, accédez à `shares replication sources` et répertoriez les packages.

```
loader:> shares replication sources
loader:shares replication sources> show
Sources:

source-000 ayu
      PROJECT   STATE      LAST UPDATE
package-000 oldproj   idle       unknown
package-001 aproj1   receiving  Sun Feb 21 2010 22:04:35 GMT+0000 (UTC)
```

2. Sélectionnez une source, puis un package.

Vous pouvez effectuer les opérations au niveau du package sur ce noeud.

```
loader:shares replication sources> select source-000
loader:shares replication source-000> select package-001
loader:shares replication source-000 package-001> show
Properties:
```

```

        enabled = true
        state = receiving
state_description = Receiving update
last_sync = Sun Feb 21 2010 22:04:40 GMT+0000 (UTC)
last_try = Sun Feb 21 2010 22:04:40 GMT+0000 (UTC)

```

Projects:

```
aproj1
```

```

loader:shares replication source-000 package-001> select aproj1
loader:shares replication source-000 package-001 aproj1> get mountpoint
        mountpoint = /export
loader:shares replication source-000 package-001 aproj1> get sharenfs
        sharenfs = on

```

3. Pour modifier les propriétés du projet et les partages, sélectionnez un projet.

Pour obtenir une liste des propriétés que vous pouvez modifier, reportez-vous à la section ["Packages de réplication" à la page 553](#).

4. Pour afficher les sources de réplication depuis configuration services replication, utilisez la propriété show :

```

loader:configuration services replication> show
Properties:
        <status> = online
Children:
        targets => Configure replication targets
        sources => View and manage replication packages

```

Rubriques connexes

- ["Packages de réplication" à la page 553](#)
- ["Réplication distante" à la page 473](#)

▼ Désactivation d'un package de réplication (BUI)

Les mises à jour de réplication pour un package peuvent être complètement désactivées, entraînant l'annulation de toute mise à jour en cours et l'échec des nouvelles mises à jour à partir de l'appareil source.

1. Depuis l'appareil cible, accédez au package.
2. Cliquez sur l'onglet Réplication.
3. Cliquez sur l'icône Alimentation .

L'icône de statut située à gauche indique le statut du package (activé, désactivé ou en échec). Le package reste désactivé tant que vous ne l'activez pas à nouveau à l'aide de la même icône

Alimentation .

Rubriques connexes

- ["Packages de réplication" à la page 553](#)
- ["Réplication distante" à la page 473](#)

▼ Désactivation d'un package de réplication (CLI)

Les mises à jour de réplication pour un package peuvent être complètement désactivées, entraînant l'annulation de toute mise à jour en cours et l'échec des nouvelles mises à jour à partir de l'appareil source.

1. **Depuis l'appareil cible, accédez au package.**
2. **Modifiez la propriété `enabled`.**
3. **Validez vos modifications.**

Le package reste désactivé jusqu'à ce que vous activiez la propriété `enabled`.

Rubriques connexes

- ["Packages de réplication" à la page 553](#)
- ["Réplication distante" à la page 473](#)

▼ Dissociation d'un package de réplication (BUI)

Avant de commencer

Identifiez les conflits de nom de point de montage ou de partage SMB entre les systèmes de fichiers répliqués et les autres systèmes de fichiers du système. Pour résoudre les conflits de point de montage (et/ou de noms de ressource SMB), modifiez les points de montage du projet ou du partage (ou les noms de ressource SMB) dans le package de réplication avant de dissocier un package de réplication. Pour plus d'informations, reportez-vous à la section ["Dissociation de la réplication" à la page 557](#).

1. **Accédez au package de réplication.**
2. **Cliquez sur l'onglet Réplication.**
3. **Cliquez sur l'icône d'interruption .**

4. **Saisissez le nom du nouveau projet local.**

Rubriques connexes

- ["Dissociation de la réplication" à la page 557](#)
- ["Réplication distante" à la page 473](#)

▼ Dissociation d'un package de réplication (CLI)

Avant de commencer

Identifiez les conflits de nom de point de montage ou de partage SMB entre les systèmes de fichiers répliqués et les autres systèmes de fichiers du système. Pour résoudre les conflits de point de montage (et/ou de noms de ressource SMB), modifiez les points de montage du projet ou du partage (ou les noms de ressource SMB) dans le package de réplication avant de dissocier un package de réplication. Pour plus d'informations, reportez-vous à la section ["Dissociation de la réplication" à la page 557](#).

1. **Accédez au package de réplication puis utilisez la commande `sever`.**
2. **Saisissez le nom du nouveau projet local comme argument de la commande `sever`.**

Si aucun argument n'est indiqué, le nom d'origine est utilisé.

Rubriques connexes

- ["Dissociation de la réplication" à la page 557](#)
- ["Réplication distante" à la page 473](#)

Configuration de réplication distante pour récupération après sinistre (BUI)

Un site de récupération après sinistre à deux systèmes comprend un appareil source sur un site de production et un appareil cible situé sur un site de récupération géographiquement éloigné. Si une défaillance catastrophique se produit sur le site de production, les administrateurs redirigent les opérations du client vers le site de récupération en inversant la réplication vers l'appareil cible et en garantissant ainsi la continuité des opérations. Une fois le site de production en mesure de reprendre son activité normale, l'administrateur met à jour le site de production en inversant la réplication au niveau du site de récupération. Pour restaurer la relation source-cible originale, la réplication est à nouveau inversée.

Pour configurer la réplication distante pour récupération après sinistre, procédez comme suit :

- ["Configuration d'un appareil cible sur un site de récupération \(BUI\)" à la page 520](#)

- ["Basculement des opérations vers le site de récupération \(BUI\)" à la page 520](#)
- ["Mise à jour du site de production \(BUI\)" à la page 521](#)
- ["Inversion de la réplication vers le site de production \(BUI\)" à la page 522](#)

Rubriques connexes

- ["Fonctionnement de la réplication inversée" à la page 557](#)
- ["Réplication distante" à la page 473](#)

▼ Configuration d'un appareil cible sur un site de récupération (BUI)

Création d'une cible de réplication à des fins de récupération après sinistre :

1. **Identifiez un appareil cible sur un site de récupération.**
L'appareil cible requiert une version du logiciel compatible avec l'appareil source. Consultez l'article MOS 1958039 pour plus d'informations.
2. **A partir de l'appareil source, créez une cible comme décrit à la section ["Création d'une cible de réplication \(BUI\)" à la page 478](#).**
3. **Créez une action de réplication et programmez une réplication continue.**
Reportez-vous à la section ["Création d'une action de réplication \(BUI\)" à la page 480](#).

Remarque - La réplication continue minimise la perte de données en cas de sinistre sur le site de production.

Etape suivante

- ["Basculement des opérations vers le site de récupération \(BUI\)" à la page 520](#)

▼ Basculement des opérations vers le site de récupération (BUI)

A la suite d'une défaillance sur le site de production, effectuez une réplication inversée sur le site de récupération et redirigez les opérations du client vers le site de récupération.

1. **A partir de l'appareil cible, accédez à [Partages > Projets > Réplique](#), puis recherchez le package de réplication de l'appareil source.**

La réplique est nommée *source_appliance:project/share*.

2. **Double-cliquez sur le package de réplication ou cliquez sur l'icône Modifier** 

3. **Cliquez sur l'onglet Réplication.**

4. **Cliquez sur l'icône Inverser le sens de réplication** .

5. **Dans la fenêtre Réplication inversée, entrez le nom du nouveau projet local.**

Chaque fois que la réplication est inversée, vous indiquez un nouveau nom de projet, et le package est converti en projet local et accessible en écriture.

6. **Cliquez sur OK.**

7. **Transférez l'activité du client vers une adresse IP de l'appareil sur le site de récupération.**

En fonction du protocole utilisé, mappez (clients SMB) ou remontez (clients NFS) les partages utilisés avec l'adresse IP ou le nom de l'appareil sur le site de récupération.

Etape suivante

- ["Mise à jour du site de production \(BUI\)" à la page 521](#)

▼ Mise à jour du site de production (BUI)

Une fois le site de production restauré et en ligne, répliquez les modifications écrites sur le site de récupération au cours de la panne vers le site de production.

1. **A partir de l'appareil du site de récupération, accédez à Partages > Partages > Local, puis sélectionnez le nouveau projet local.**

Le nouveau projet est répertorié avec le statut Never synced.

2. **Cliquez sur Synchroniser maintenant pour démarrer la réplication.**

3. **Attendez que la réplication se termine.**

Dans la partie supérieure de la fenêtre, Finished replicating to the new *project* on the *source appliance* est affiché.

Etape suivante

- ["Inversion de la réplication vers le site de production \(BUI\)" à la page 522](#)

▼ Inversion de la réplication vers le site de production (BUI)

Une fois toutes les modifications répliquées du site de récupération vers le site de production, inversez à nouveau la réplication pour rétablir la relation initiale de réplication entre les appareils source et cible.

1. **A partir de l'appareil de production, accédez à Partages > Projets > Réplique, puis recherchez le nom du nouveau projet.**

Le projet est nommé *target_appliance:new_project/share*.

2. **Sélectionnez le nouveau projet et cliquez sur son icône Modifier .**

3. **Cliquez sur l'onglet Réplication.**

4. **Cliquez sur l'icône Inverser le sens de réplication .**

5. **Dans la fenêtre Réplication inversée, entrez le nom du nouveau projet local.**

Cette action convertit le package en un nouveau projet local configuré pour répliquer à nouveau vers le site de récupération initial.

6. **En fonction du protocole utilisé, remappez (clients SMB) ou remontez (clients NFS) les partages sur l'appareil du site de récupération.**

7. **Supprimez le projet original de l'appareil source.**

- a. **Accédez à Partages > Projets > Local, puis recherchez le projet original, qui devrait être vide.**

- b. **Sélectionnez le projet vide et cliquez sur l'icône Détruire correspondante .**

- c. **Cliquez sur OK.**

Configuration de réplication distante pour récupération après sinistre (CLI)

Un site de récupération après sinistre à deux systèmes comprend un appareil source sur un site de production et un appareil cible situé sur un site de récupération géographiquement éloigné. Si une défaillance catastrophique se produit sur le site de production, les administrateurs

redirigent les opérations du client vers le site de récupération en inversant la réplication vers l'appareil cible et en garantissant ainsi la continuité des opérations. Une fois le site de production en mesure de reprendre son activité normale, l'administrateur met à jour le site de production en inversant la réplication au niveau du site de récupération. Pour restaurer la relation source-cible originale, la réplication est à nouveau inversée.

Pour configurer la réplication distante pour récupération après sinistre, procédez comme suit :

- ["Configuration d'un appareil cible sur un site de récupération \(CLI\)" à la page 523](#)
- ["Basculement des opérations vers le site de récupération \(CLI\)" à la page 524](#)
- ["Mise à jour du site de production \(CLI\)" à la page 525](#)
- ["Inversion de la réplication vers le site de production \(CLI\)" à la page 526](#)

Rubriques connexes

- ["Fonctionnement de la réplication inversée" à la page 557](#)
- ["Réplication distante" à la page 473](#)

▼ Configuration d'un appareil cible sur un site de récupération (CLI)

Création d'une cible de réplication à des fins de récupération après sinistre :

1. **Identifiez un appareil cible sur le site de récupération.**
L'appareil cible requiert une version du logiciel compatible avec l'appareil source. Consultez l'article MOS 1958039 pour plus d'informations.
2. **A partir de l'appareil source, créez une cible comme décrit à la section ["Création d'une cible de réplication \(CLI\)" à la page 479](#).**
3. **Créez une action de réplication et programmez une réplication continue.**
Reportez-vous à la section ["Création d'une action de réplication \(CLI\)" à la page 482](#).

Remarque - La réplication continue minimise la perte de données en cas de sinistre sur le site de production.

Etape suivante

- ["Basculement des opérations vers le site de récupération \(CLI\)" à la page 524](#)

▼ Basculement des opérations vers le site de récupération (CLI)

A la suite d'une défaillance sur le site de production, effectuez une réplication inversée sur le site de récupération et redirigez les opérations du client vers le site de récupération.

1. **A partir de l'appareil cible, entrez `shares replication`.**

```
host-offsite:> shares replication
```

2. **Entrez `sources` pour répertorier les appareils sources associés à cette cible.**

```
host-offsite:shares default replication> sources
```

3. **Recherchez le package répliqué par l'appareil source.**

Dans cet exemple, `source-001` est le numéro de l'appareil source et `host-prod` est le nom de l'appareil source. `kmm2` est le nom de projet local du package de réplication numéro package-001.

```
source-001 host-prod
      PROJECT                STATE      LAST UPDATE
package-000 <unknown>      idle      unknown
package-001 kmm2           idle      Wed May 01 2015 20:06:27 GMT
+0000
      (UTC)
```

4. **Entrez `select` et le numéro de l'appareil source.**

```
host-offsite:shares default replication sources> select source-001
```

5. **Entrez `select` et le numéro de package de réplication.**

```
host-offsite:shares default replication source-001> select package-001
```

6. **Entrez `reverse` et le nom du nouveau projet local, puis entrez `Y` pour confirmer.**

```
host-offsite:shares default replication source-001 package-001> reverse new-kmm2
Are you sure? (Y/N) Y
```

La réplication est désormais inversée, et le package de réplication a été converti en projet local et accessible en écriture, nommé `new-kmm2`.

7. **Transférez l'activité du client vers une adresse IP de l'appareil sur le site de récupération.**

En fonction du protocole utilisé, mappez (clients SMB) ou remontez (clients NFS) les partages utilisés avec l'adresse IP ou le nom de l'appareil sur le site de récupération.

Etape suivante

- ["Mise à jour du site de production \(CLI\)" à la page 525](#)

▼ Mise à jour du site de production (CLI)

Une fois le site de production restauré et en ligne, répliquez les modifications écrites sur le site de récupération au cours de la panne vers le site de production.

1. **A partir de l'appareil du site de récupération, accédez à shares, puis sélectionnez le nouveau projet local.**

```
host-offsite:> shares
host-offsite:shares pool> select new-kmm2
```

2. **Entrez list pour rechercher le nom du partage.**

```
host-offsite:shares pool new-kmm2> list
Filesystems:

NAME          SIZE
  ENCRYPTED    MOUNTPPOINT
karen2        31K   off           /export/karen2
host:shares pool new-kmm2> replication
host:shares pool new-kmm2 replication> show
Actions:

          TARGET
STATUS    NEXT
action-000
host2      idle      Sync now
```

3. **Sélectionnez le numéro de l'action, puis entrez sendupdate pour démarrer la réplication vers l'appareil de production.**

```
host-offsite:shares pool new-kmm2 replication> select action-000
host-offsite:shares pool new-kmm2 action-000> sendupdate
```

4. **Attendez que la réplication se termine.**

L'état passe à idle lorsque la réplication est terminée.

Etape suivante

- ["Inversion de la réplication vers le site de production \(CLI\)" à la page 526](#)

▼ Inversion de la réplication vers le site de production (CLI)

Une fois toutes les modifications répliquées du site de récupération vers le site de production, inversez à nouveau la réplication pour rétablir la relation initiale de réplication entre les appareils source et cible. Avant d'inverser la réplication, supprimez le projet original.

1. Supprimez le projet original de l'appareil source.

a. Accédez à shares, puis sélectionnez le projet original.

```
host-prod:> shares select kmm2
```

b. Assurez-vous que le projet est vide en entrant list. Puis, entrez done.

```
host-prod:shares kmm2> list
host-prod:shares kmm2> done
```

c. Accédez à shares, puis entrez destroy et le nom du projet original. Puis, entrez Y pour confirmer l'action.

```
host-prod:> shares
host-prod:shares> destroy kmm2
This will destroy all data in "kmm2"! Are you sure? (Y/N)Y
```

2. Accédez à shares et entrez les commandes suivantes pour répertorier les appareils sources qui utilisent l'appareil de production originale comme cible de réplication.

```
host-prod:shares> replication
host-prod:shares replication> sources
host-prod:shares replication sources> list
```

Toutes les appareils qui utilisent l'appareil de production originale comme réplication cible sont répertoriées comme l'indique l'exemple suivant. Recherchez l'appareil source qui correspond à votre système de récupération hors site.

```
source-000 ar7420-xxx
      PROJECT                STATE      LAST UPDATE
package-000 test            receiving Wed May 01 2015 20:45:21 GMT
+0000(UTC)
source-001 brmzs3-4-xxx
      PROJECT                STATE      LAST UPDATE
package-000 proj3           idle       Tue Mar 24 2015 17:06:55 GMT
+0000(UTC)
package-004 Proj-X          idle       Thu Mar 26 2015 20:01:42 GMT
+0000(UTC)
source-002 ar7110-xxx
```

```

                PROJECT                STATE                LAST UPDATE
package-000 <unknown>                idle                unknown
package-001 <unknown>                idle                unknown
package-002 <unknown>                idle                unknown
package-003 proj2                    receiving           Wed Apr 02 2015 20:45:23 GMT
+0000 (UTC)

source-003 ar7420-xxx
                PROJECT                STATE                LAST UPDATE
package-000 <unknown>                idle                unknown
package-001 project1                 idle                Wed Oct 08 2014 14:31:11 GMT
+0000(UTC)
package-002 project1                 idle                Mon Mar 09 2015 21:18:51 GMT
+0000(UTC)
package-003 proj1                    idle                Mon Mar 23 2015 15:52:18 GMT
+0000(UTC)

source-004 aus7320-xxx
                PROJECT                STATE                LAST UPDATE
package-000 <unknown>                idle                unknown
package-003 default                  idle                Wed Mar 25 2015 19:12:02 GMT
+0000(UTC)

source-005 host-offsite << This is the name of the offsite disaster recovery system
                PROJECT                STATE                LAST UPDATE
package-000 new-kmm2                 idle                Wed May 01 2015 20:44:34 GMT
+0000 (UTC)

```

3. Sélectionnez le numéro de source et le numéro de package, comme l'indique l'exemple suivant.

```

host-prod:shares replication sources> select source-005
host-prod:shares replication source-005> select package-000

```

4. Entrez reverse et le nom de projet. Puis, entrez Y pour confirmer l'action.

```

host-prod:shares replication source-005 package-000> reverse kmm2
Are you sure? (Y/N) Y

```

Cette action convertit le package en un nouveau projet local configuré pour répliquer à nouveau vers le site de récupération initial.

5. En fonction du protocole utilisé, remappez (clients SMB) ou remontez (clients NFS) les partages sur l'appareil du site de récupération.

Rubriques connexes

- ["Fonctionnement de la réplication inversée" à la page 557](#)
- ["Réplication distante" à la page 473](#)

Utilisation de la réplication pour la sauvegarde disque à disque

La réplique sur un appareil cible contient toutes les données répliquées à partir d'un appareil source à compter de la mise à jour de réplication la plus récemment effectuée. La réplique peut servir de sauvegarde de la source d'origine en cas de destruction ou de corruption des données.

Il est possible d'accéder aux données du package de réplication à l'aide de l'une des méthodes suivantes :

- **Exportation d'un package de réplication** - Lorsque vous exportez un package de réplication sélectionné, les partages exportés contiennent les données de la mise à jour de réplication la plus récemment effectuée. Après avoir exporté les partages, vous pouvez accéder aux données de n'importe quel instantané spécifique pour n'importe quel partage en accédant au répertoire `.zfs/snapshot` dans le répertoire racine du partage. Le répertoire `.zfs` est normalement invisible, mais est accessible en spécifiant de façon explicite un sous-répertoire ou un nom de fichier, comme décrit dans la section [Accès au répertoire caché des instantanés du système de fichiers](#). Pour plus d'informations sur la modification de la propriété de visibilité de l'instantané, reportez-vous à la section Affichage du répertoire d'instantanés du système de fichiers - [BUI](#), [CLI](#).
- **Clonage d'un package de réplication** - La création d'un clone d'un package de réplication exploite les dernières données reçues à partir de l'appareil source. Le clonage convertit un package de réplication en nouveau projet autorisant l'accès en lecture-écriture à toutes les données du projet. Le projet cloné doit disposer d'un nom unique, d'un point de montage et d'un nom de ressource SMB qui n'est pas en conflit avec un projet existant. Pour plus d'informations, reportez-vous à la section Clonage d'un package de réplication - [BUI](#), [CLI](#).
- **Clonage de partage depuis un package de réplication** - Les instantanés de partages individuels, créés avant la réplication la plus récente, peuvent être clonés depuis un package de réplication. Le clonage d'un instantané individuel depuis un package de réplication fournit un accès en lecture-écriture aux données telles qu'elles existaient sur l'appareil source au moment de la création d'un instantané. Pour plus d'informations, reportez-vous aux sections relatives au clonage d'un instantané avec la [BUI](#), [CLI](#).
- **Interruption d'un package de réplication** - L'opération d'interruption convertit un package de réplication en un nouveau projet autorisant l'accès en lecture-écriture aux données du projet. La connexion de réplication entre les appareils source et cible est interrompue après cette opération. Notez que le nouveau projet doit disposer d'un nom unique, d'un point de montage et d'un nom de ressource SMB qui n'est pas en conflit avec les projets existants. Pour plus d'informations, reportez-vous aux sections relatives à l'interruption d'un package de réplication avec la [BUI](#), [CLI](#).
- **Inversion d'un package de réplication** - L'opération d'inversion convertit un package de réplication en un nouveau projet autorisant l'accès en lecture-écriture aux données du projet. La connexion de réplication est préservée et une nouvelle action de réplication est créée. Cette dernière permet d'effectuer une réplication vers l'appareil source d'origine. Pour plus d'informations, reportez-vous à la section "[Fonctionnement de la réplication inversée](#)" à la page 557.

Conservation des instantanés générés par l'utilisateur

La propriété « Conserver les instantanés générés par l'utilisateur sur la cible » fournit une solution de sauvegarde disque à disque perpétuellement incrémentielle utilisant la réplication distante. Les instantanés générés par l'utilisateur créés sur un appareil source sont répliqués sur un appareil cible faisant office de référentiel de sauvegarde.

La définition de cette propriété permet de gérer les instantanés générés par l'utilisateur de façon indépendante sur les appareils source et cible. Normalement, lorsque vous supprimez des instantanés générés par l'utilisateur sur l'appareil source, les instantanés sont immédiatement supprimés sur l'appareil cible après la mise à jour d'une réplication. Pour conserver les instantanés générés par l'utilisateur sur la cible, définissez cette propriété lors de la création ou de la modification d'une action de réplication.

Quand vous n'avez plus besoin des instantanés générés par l'utilisateur, supprimez-les manuellement sur l'appareil cible. Pour supprimer les instantanés, reportez-vous à la section Destruction d'un instantané - [BUI](#), [CLI](#). Pour plus d'informations sur la gestion de l'espace des instantanés sur l'appareil, reportez-vous à la section "[Gestion de l'espace pour les instantanés](#)" à la page 443.

Rubriques connexes

- "[Propriétés des actions de réplication](#)" à la page 551
- Création d'une action de réplication [BUI](#), [CLI](#)
- Modification d'une action de réplication [BUI](#), [CLI](#)

Concepts de la réplication distante

La réplication distante des appareils Oracle ZFS Storage Appliance est une fonctionnalité sous licence qui fournit la réplication de projet et de partage basée sur les instantanés d'un appareil source sur un ou plusieurs appareils cible. La réplication distante effectue une mise à jour complète de l'intégralité du contenu d'un projet et/ou d'un partage, suivie de mises à jour incrémentielles contenant uniquement les modifications depuis la mise à jour précédente.

Cette rubrique décrit les concepts de la réplication distante clé (ou simplement "réplication") ainsi que la terminologie relative à la réplication.

La réplication distante présente les caractéristiques suivantes :

- **Réplication asynchrone basée sur les instantanés** : le sous-système de réplication prend un instantané dans le cadre de chaque opération de mise à jour. Dans le cas d'une mise à jour initiale, le contenu d'un projet et/ou d'un partage est envoyé dans son intégralité. Lors d'une mise à jour incrémentielle, seules les modifications apportées depuis le dernier instantané de réplication pour la même action sont envoyées. La réplication prenant et envoyant des instantanés, les données sont déjà dans un état de stockage stable avant que la réplication

ne commence leur envoi. La réplication en continu envoie des flux de modifications du système de fichiers, mais elle est tout de même asynchrone par rapport aux clients NAS et SAN.

- **Au niveau des blocs** : chaque opération de mise à jour parcourt le système de fichier au niveau du bloc et envoie les données et métadonnées du système de fichier concerné à la cible.
- **Inclusion de toutes les métadonnées** : le flux de réplication sous-jacent sérialise à la fois les données utilisateur et les métadonnées, y compris la plupart des propriétés configurées dans l'écran Partages. Ces propriétés peuvent être modifiées sur la cible une fois la première mise à jour de réplication effectuée, mais elles ne sont pas toutes appliquées avant que la connexion de réplication ne soit dissociée. Par exemple, cela autorise le partage via NFS à un autre ensemble d'hôtes que la source. Pour plus d'informations, reportez-vous à la section ["Packages de réplication" à la page 553](#).
- **Sécurisé** : le protocole de contrôle de réplication utilisé parmi les produits Oracle ZFS Storage Appliance est sécurisé avec SSL (Secure Socket Layer). Les données peuvent éventuellement être protégées par cette dernière. L'appareil Oracle ZFS Storage Appliance peut uniquement répliquer vers/depuis un autre appareil Oracle ZFS Storage Appliance après un processus initial d'authentification manuelle. Pour plus d'informations, reportez-vous à la section ["Cibles de réplication" à la page 532](#).
- **Projets et partages chiffrés** : lorsqu'il est activé, le chiffrement transparent des données protège les partages individuels (systèmes de fichiers et LUN) et les projets. Pour plus d'informations, reportez-vous à la section ["Chiffrement de données" à la page 563](#).
- **Indépendant des protocoles** : le système Oracle ZFS Storage Appliance prend en charge les volumes de stockage basés sur des fichiers et des blocs. Le mécanisme de réplication est indépendant des protocoles.
- **Réplication compressée** : la prise en charge des flux de réplication compressée augmente les performances de réplication et améliore l'utilisation du débit entre plusieurs sites disposant de connexions de bande passante limitées. Pour plus d'informations, reportez-vous à la section ["Réplication compressée" à la page 552](#).

Les limitations connues suivantes s'appliquent à la réplication :

- Les actions ne peuvent pas être déplacées entre les pools.
- Le débit du réseau est limitée à un maximum de 200 Mo/s par réplication au niveau du projet Avec la réplication compressée, le taux effectif de données peut dépasser le taux réel des données du réseau physique.

La liste suivante répertorie les termes couramment associés à la réplication.

- **source de réplication** : appareil qui envoie les mises à jour de réplication à un ou plusieurs appareils cible de manière périodique, continue ou à la demande. Les appareils individuels peuvent faire office à la fois de source et de *cible*, mais ils doivent être l'un ou l'autre dans le cadre d'une *action* de réplication spécifique.
- **cible de réplication** : appareil qui reçoit et stocke des données répliquées depuis un ou plusieurs appareils *source*. Ce terme désigne également un objet de configuration de l'appareil qui permet à ce dernier d'effectuer une réplication vers un autre appareil.

- **pair de réplication** : appareil configuré en tant que source ou cible de réplication.
- **action de réplication** : décrit les données à répliquer, le calendrier de réplication et les propriétés de transfert de données telles que l'activation ou la désactivation du chiffrement de la liaison réseau.
- **groupe de réplication** : intégralité des ensembles de données (pour être précis, un projet et certains partages) répliqués en tant qu'unité. Voir la section "[Réplication de projet et réplication de partage](#)" à la page 535.
- **réplique** : données répliquées contenues dans le package de réplication, sur l'appareil cible.
- **package de réplication** : existe sur la cible et est associé à une action de réplication. Il s'agit d'un objet spécial contenant la réplique. La perte d'un objet nécessite la création d'une nouvelle paire action/package et une mise à jour de réplication complète. La liaison entre une action et son package peut être interrompue, empêchant les mises à jour à venir mais activant l'accès en écriture à la réplique.
- **clone** : un package répliqué peut être cloné en projet mutable. Ce dernier peut être géré comme n'importe quel autre projet du système.
- **synchronisation complète** (ou **mise à jour complète**) : opération de réplication qui envoie l'intégralité du contenu d'un projet et certains de ses partages. La synchronisation initiale d'un projet et/ou d'un partage est une synchronisation complète.
- **mise à jour incrémentielle** : opération de réplication qui envoie uniquement les différences relevées dans un projet et ses partages depuis la mise à jour précédente (que cette dernière ait été complète ou incrémentielle).
- **réplication inverse** : relation de réplication qui échange les rôles source et cible. A la suite d'une récupération après sinistre, les rôles peuvent être à nouveau inversés.

Pour plus d'informations sur les concepts de réplication distante, reportez-vous aux sections suivantes :

- "[Cibles de réplication](#)" à la page 532
- "[Actions et packages de réplication](#)" à la page 533
- "[Pools de stockage de réplication](#)" à la page 534
- "[Réplication de projet et réplication de partage](#)" à la page 535
- "[Autorisations de réplication](#)" à la page 536
- "[Configuration de la réplication pour les appareils en cluster](#)" à la page 537
- "[Exemple : Configuration de réplication pour des appareils en cluster](#)" à la page 538
- "[Instantanés de réplication et cohérence des données](#)" à la page 545
- "[Gestion des instantanés de réplication](#)" à la page 546
- "[Réplication et configurations iSCSI](#)" à la page 547
- "[Echecs de réplication](#)" à la page 548
- "[Propriétés des actions de réplication](#)" à la page 551
- "[Réplication compressée](#)" à la page 552
- "[Packages de réplication](#)" à la page 553
- "[Clonage d'un package de réplication ou d'un partage](#)" à la page 554

- ["Exportation de systèmes de fichiers répliqués" à la page 556](#)
- ["Dissociation de la réplication" à la page 557](#)
- ["Fonctionnement de la réplication inversée" à la page 557](#)
- ["Destruction d'un package de réplication" à la page 561](#)
- ["Sauvegardes de réplique cible" à la page 561](#)

Cibles de réplication

Lors de la création d'une cible de réplication sur un appareil source, une connexion est établie pour permettre une communication sécurisée entre un appareil source et un appareil cible. Cette opération requiert les détails suivants ::

- Nom de l'appareil cible : uniquement utilisé pour identifier la cible dans la BUI et dans la CLI de l'appareil source.
- Adresse IP réseau : l'interface de données de l'appareil cible.
- Mot de passe root de l'appareil cible : pour autoriser l'administrateur à établir la connexion à l'appareil cible.

Les appareils échangent des clés utilisées pour s'identifier mutuellement de manière sécurisée lors des communications ultérieures. Ces clés sont stockées de manière permanente dans la configuration de l'appareil et subsistent après les réinitialisations et mises à niveau. Elles sont perdues si l'appareil est réinstallé ou réinitialisé à sa configuration d'usine. Le mot de passe root n'est jamais stocké de manière permanente, le changer sur l'un ou l'autre appareil ne nécessite donc pas de modifier la configuration de réplication. Le mot de passe n'est jamais transmis en clair car cet échange initial d'identité (comme toutes les opérations de contrôle de réplication) est protégé par la technologie SSL.

Remarque - Si une source de réplication utilise le protocole NIS ou LDAP et mappe directement ces utilisateurs ou groupes de service à la configuration du partage, la configuration de l'appareil cible doit être équivalente. Sinon, les opérations de dissociation et d'inversion de réplication pourraient échouer.

Par défaut, la connexion de la cible de réplication n'est pas bidirectionnelle. Par exemple, si un administrateur configure la réplication à partir d'une *source A* vers une *cible B*, *B* ne peut pas automatiquement utiliser *A* comme cible. Cependant, le système prend en charge l'inversion du sens de réplication, qui crée automatiquement une cible pour la *source A* sur la *cible B* (si elle n'existe pas déjà) pour que la *cible B* puisse répliquer vers la *source A*. Pour plus d'informations, reportez-vous à la section ["Fonctionnement de la réplication inversée" à la page 557](#).

Pour configurer des cibles de réplication, reportez-vous à la section ["Création d'une cible de réplication \(BUI\)" à la page 478](#) ou à la section ["Création d'une cible de réplication \(CLI\)" à la page 479](#).

Rubriques connexes

- ["Workflow de réplication distante" à la page 474](#)
- ["Réplication distante" à la page 473](#)

Actions et packages de réplication

Une action de réplication spécifie le projet ou le partage qui sera répliqué, la fréquence de la mise à jour et les options sélectionnées. Les actions de réplication sont créées sur l'appareil source en spécifiant :

- un groupe de réplication incluant soit un projet soit des partages individuels
- le nom d'un appareil cible
- le nom d'un pool de stockage sur l'appareil cible (utilisé uniquement lors de la configuration initiale)
- une fréquence (programmée ou continue) de la mise à jour
- des options supplémentaires telles que le chiffrement du flux de données ou la désactivation de la compression

Un groupe de réplication est implicitement spécifié par le projet ou le partage sur lequel l'action est configurée (reportez-vous à la section ["Pools de stockage de réplication" à la page 534](#)). L'appareil cible et le pool de stockage ne peuvent pas être modifiés une fois cette action créée, mais il est possible de modifier les autres options à tout moment. Si une mise à jour de réplication est en cours lors de la modification d'une option, la nouvelle valeur sera prise en charge uniquement lors de la prochaine mise à jour.

Lorsqu'une action de réplication est exécutée sur l'appareil source, un package est créé sur l'appareil cible du pool de stockage spécifié. Le package sur l'appareil cible contient une copie exacte du projet et des partages de la source sur lesquels l'action est configurée, à l'heure de démarrage de la dernière mise à jour de réplication. Les actions constituent l'unité principale de la configuration de réplication sur l'appareil.

Modes de réplication : programmé ou continu

Les actions de réplication peuvent être configurées pour envoyer les mises à jour de manière planifiée ou en continu. Le processus de mise à jour de réplication en lui-même reste identique dans les deux cas. Cette propriété contrôle uniquement l'intervalle.

Les actions de réplication envoyant des mises à jour aussi souvent que possible, elles consistent en l'envoi d'un flux constant de modifications du système de fichiers vers le système cible. Pour les systèmes de fichiers dans lesquels de nombreux fichiers ont été créés et supprimés à courts intervalles, il peut en résulter la réplication de bien plus de données que nécessaire. Toutefois, tant que la réplication suit le rythme des modifications de données, une quantité minimale de données sera perdue en cas de sinistre sur le système source.

La réplication en continu est toujours asynchrone. Oracle ZFS Storage Appliance ne prend actuellement pas en charge la réplication synchrone, qui ne considère pas les données affectées

au stockage stable tant qu'elles ne sont pas validées sur les systèmes de stockage à la fois principal et secondaire.

Instantanés de réplication intermédiaires

Lorsque la propriété "Inclure les instantanés" est définie sur true, les mises à jour de réplication incluent les instantanés de non-réplication créés après la précédente mise à jour de réplication (ou depuis la création du partage, dans le cas d'une première mise à jour complète). Cela comprend les instantanés automatiques et les instantanés créés par un administrateur. Cette propriété peut être désactivée pour ignorer ces instantanés et envoyer uniquement les modifications entre les instantanés de réplication avec chaque mise à jour.

Relation entre une action et un package de réplication

Une action et un package de réplication sont liés l'un à l'autre. Si le package est endommagé d'une manière quelconque ou qu'il est supprimé, l'action ne sera pas en mesure d'envoyer les mises à jour de réplication, même si la cible possède les données et les instantanés associés à l'action. De même, si une action est supprimée, le package ne sera pas en mesure de recevoir de nouvelles mises à jour de réplication (même si la source possède les données et les instantanés). Si vous essayez d'effectuer une opération risquant de détruire la connexion entre l'action et le package, un avertissement vous met en garde à la fois dans la BUI et la CLI. Si une erreur ou une opération administrative interrompt la connexion si bien que des mises à jour incrémentielles ne sont plus possibles, vous devez dissocier ou détruire le package et l'action, puis créer une nouvelle action sur la source.

Remarque - L'appareil évite de supprimer des données sur la cible à moins d'une demande explicite de la part de l'administrateur. Par conséquent, si la mise à jour de réplication initiale pour une action échoue après la réplication d'une partie des données (laissant ainsi des données incomplètes à l'intérieur du package), les mises à jour de réplication ultérieures utilisant la même action échoueront également car l'appareil ne peut pas écraser les données reçues précédemment. Pour remédier à ce problème, les administrateurs doivent supprimer l'action et le package existants et créer une nouvelle action, puis redémarrer la réplication.

Rubriques connexes

- ["Packages de réplication" à la page 553](#)
- ["Propriétés des actions de réplication" à la page 551](#)

Pools de stockage de réplication

Lors de la configuration initiale d'une action de réplication, l'administrateur peut choisir le pool de stockage de la cible qui accueillera les données répliquées. Le pool de stockage contenant une action ne peut pas être modifié une fois que l'action a été créée. La création de l'action crée un package vide sur la cible dans le pool de stockage spécifié. Après cette opération, la source n'a pas connaissance de la configuration de stockage de la cible. Elle n'effectue pas de suivi du

pool affecté à la réplication de l'action et elle n'est pas mise à jour lors des modifications de la configuration de stockage sur la cible.

Lorsque la cible est un système clustérisé, le pool de stockage sélectionné doit appartenir au même contrôleur que celui de l'adresse IP utilisée pour la source de réplication. En effet, seuls ces pools garantissent leur accès en permanence lorsque la source contacte la cible via cette adresse IP. Cela est en tous points semblable à la configuration des clients NAS, par exemple des clients NFS et SMB, où le chemin et l'adresse IP requis dans une opération de montage doivent se soumettre à la même contrainte. Lorsque des opérations modifiant la propriété des pools de stockage et des adresses IP dans un cluster sont effectuées, les administrateurs doivent mesurer l'impact sur les sources effectuant des réplications sur le cluster. Il est actuellement impossible de déplacer les packages entre les pools de stockage.

Rubriques connexes

- ["Workflow de réplication distante" à la page 474](#)
- ["Réplication distante" à la page 473](#)

Réplication de projet et réplication de partage

Bien qu'il soit possible de configurer la réplication distante au niveau du projet et au niveau du partage, la réplication au niveau du projet est recommandée pour ces raisons. L'appareil permet aux administrateurs de configurer la réplication distante de niveau projet ou de niveau du partage.

- Les instantanés de réplication sont toujours pris au niveau projet. Plusieurs réplications de niveau partage dans un unique projet peuvent créer une quantité importante de temps système et prendre de la place sur le pool.
- Lors de l'inversion de la réplication de niveau partage, le partage est placé dans son propre projet. Cela signifie que les inversions de réplication se terminent par la séparation du partage des autres partages du projet, à moins qu'ils soient tous répliqués ensemble.

A l'instar des autres propriétés configurable dans l'écran Partages, chaque partage peut soit hériter ou remplacer la configuration de son projet parent. Hériter de la configuration ne signifie pas seulement que le partage est répliqué sur la base du même calendrier, vers la même cible avec les mêmes options que son projet parent, mais également que le partage sera répliqué dans le même flux en utilisant les mêmes instantanés de niveau projet que les autres partages héritant de la configuration du projet. Ce peut être important pour les applications exigeant de la cohérence entre les données stockées sur différents partages. Remplacer la configuration signifie que le partage ne sera pas répliqué avec les actions de niveau projet, bien qu'il puisse être répliqué avec ses propres actions de niveau partage qui comprendront le projet. Il n'est pas possible de remplacer une partie de la configuration de réplication du projet et d'hériter du reste.

Pour être plus précis, la configuration de réplication d'un projet et de ses partages définit un certain nombre de *groupes* de réplication, chacun étant répliqué avec un seul flux à l'aide d'instantanés pris simultanément. Tous les groupes contiennent le projet lui-même

(qui comprend principalement ses propriétés). Un groupe de niveau projet inclut tous les partages héritant de la configuration de réplication du projet parent. Tout partage remplaçant la configuration du projet constitue un nouveau groupe composé uniquement du projet et du partage eux-mêmes.

Par exemple, supposez que vous avez :

- un projet home et des partages bill, cindi et dave.
- la réplication du projet home est configurée avec un certain nombre d'actions.
- les partages home/bill et home/cindi héritent de la configuration de réplication du projet.
- le partage home/dave remplace la configuration de réplication du projet et utilise sa propre configuration, qui comprend un certain nombre d'actions.

Cette configuration définit les groupes de réplication suivant, chacun étant répliqué comme un flux unique par action à l'aide d'instantanés pris simultanément sur le projet et les partages :

- un groupe de niveau projet incluant home, home/bill et home/cindi.
- un groupe de niveau partage home et home/dave.

Remarque - En raison des restrictions actuelles, ne mélangez pas de répliqués de niveau projet et de niveau partage au sein du même projet. Cela permet d'éviter les résultats imprévisibles lors de l'inversion du sens de la réplication ou lors de la réplication de clones. Pour plus de détails, reportez-vous aux sections "[Packages de réplication](#)" à la page 553 et "[Clonage d'un package de réplication ou d'un partage](#)" à la page 554.

Rubriques connexes

- "[Workflow de réplication distante](#)" à la page 474
- "[Réplication distante](#)" à la page 473

Autorisations de réplication

Le sous-système de réplication fournit deux autorisations d'utilisateur sous la portée "Projets et partages" :

Autorisation	Détails
rrsource	Autorise les administrateurs à créer, modifier et détruire les cibles et actions de réplication. De plus, cela permet aux administrateurs d'envoyer ou d'annuler les mises à jour d'actions de réplication.
rrtarget	Autorise les administrateurs à gérer les packages répliqués, y compris la désactivation de la réplication au niveau du package, le clonage d'un package ou de ses membres, la modification des propriétés des ensembles de données reçus, ainsi que la dissociation ou l'inversion

Autorisation	Détails
	de la réplication. D'autres autorisations peuvent être nécessaires pour certaines de ces opérations (comme la définition de propriétés ou le clonage de partages individuels). Consultez les autorisations disponibles dans la portée Projets et partages pour plus d'informations.

L'autorisation `rrsource` est requise pour configurer les cibles de réplication sur un appareil, même s'il est configuré dans l'écran du service Réplication distante. Pour obtenir de l'aide sur les autorisations, voir ["Configuration des utilisateurs" à la page 160](#).

Rubriques connexes

- ["Workflow de réplication distante" à la page 474](#)
- ["Réplication distante" à la page 473](#)

Configuration de la réplication pour les appareils en cluster

La réplication peut être configurée à partir de n'importe quel appareil source sur n'importe quel appareil cible indépendamment du fait que chacun fasse partie d'un cluster ou du fait que la réplication du pair du cluster de l'appareil soit configurée dans les deux sens.

Pour les appareils en cluster, le comportement de réplication est contrôlé par les règles suivantes :

- Les mises à jour de réplication pour les projets et les partages sont envoyées par le pair de cluster qui a importé le pool de stockage conteneur.
- Les pools de stockage qui sont la propriété de chaque contrôleur peuvent effectuer une réplication vers la même cible, uniquement si OS8.6.0 (au minimum) est installé sur les deux contrôleurs.
- Les mises à jour de réplication sont reçues par le pair qui a importé l'adresse IP configurée dans l'action de réplication sur la source. Les administrateurs doivent garantir que le contrôleur de cluster utilisant cette adresse IP importera toujours le pool de stockage contenant la réplique. Pour ce faire, il faut assigner les ressources de pool et d'adresse IP au même contrôleur lors de la configuration de cluster.
- Les mises à jour de réplication (depuis et vers un appareil) en cours lorsqu'un appareil exporte le pool de stockage et l'adresse IP correspondants (dans le cadre d'une reprise ou d'une récupération) échoueront. Les mises à jour de réplication utilisant des pools de stockage et des adresses IP non concernés par une opération de reprise ou de rétablissement ne seront pas affectées par l'opération.

Rubriques connexes

- ["Exemple : Configuration de réplication pour des appareils en cluster" à la page 538](#)

Exemple : Configuration de réplication pour des appareils en cluster

Cet exemple montre comment configurer correctement la réplication pour garantir que la réplication des projets continue après une reprise du cluster, un rétablissement du cluster ou l'exécution d'une réplication inverse sur un appareil cible.

- [Configuration Guidelines](#)
- [Example: Configuring Replication for Clustered Appliances](#)
- [Replication Data Path Illustrated Examples](#)

Instructions de configuration

Lorsque vous configurez la réplication pour des appareils en cluster, respectez les règles suivantes :

- Assurez-vous que les deux appareils source et cible sont dans l'état CLUSTERED. Pour plus de détails, reportez-vous à la section [Tableau 46, "Etats du cluster"](#).
- Sélectionnez les interfaces réseau et les adresses IP à utiliser pour le trafic de réplication sur les appareils source et cible.
 - Sélectionnez une interface réseau singleton. Contrairement à une interface réseau privée, une interface réseau singleton sera reprise par le contrôleur resté fonctionnel après la perte d'un des contrôleurs du cluster. L'utilisation d'une interface singleton garantit la réussite de la réplication à la suite d'une reprise ou d'un rétablissement du cluster. Pour plus d'informations sur les interfaces singleton, reportez-vous à la section [Tableau 45, "Gestion des ressources du cluster"](#).
 - Assurez-vous que l'interface réseau sélectionnée sur l'appareil source et le pool à partir duquel les données seront répliquées sont tous les deux affectés au même contrôleur. C'est toujours le cas lorsque le cluster source est dans l'état CLUSTERED.
 - Pour le cluster cible également, l'interface réseau sélectionnée sur l'appareil cible et le pool dans lequel les données seront répliquées doivent tous les deux être affectés au même contrôleur. Cette association est garantie lorsque la configuration de réplication est effectuée pendant que le cluster cible est dans l'état CLUSTERED.
 - Les appareils source et cible doivent être capables de communiquer à l'aide des interfaces réseau et des adresses IP sélectionnées.
- Créez un routage statique /32 basé sur les hôtes entre les appareils source et cible pour garantir qu'à la suite d'une inversion de réplication, l'interface sélectionnée sera utilisée pour le trafic de réplication sortant une fois que l'inversion aura transformé la cible actuelle en source de réplication.
- Après avoir créé la route statique, configurez l'objet cible de la réplication sur l'appareil source en utilisant l'adresse IP sélectionnée de la cible.
- Lorsque l'appareil cible est dans l'état OWNER, toutes les ressources partagées (y compris les interfaces réseau et les pools de stockage) font l'objet d'une reprise et d'une appropriation

par le seul contrôleur resté fonctionnel et présentant désormais l'état OWNER. Sur le contrôleur en état OWNER, il est possible de sélectionner une interface réseau affectée à un contrôleur et de l'utiliser pour livrer le trafic de réplication à un pool qui est affecté à un contrôleur différent. Lorsque les contrôleurs reprennent l'état CLUSTERED, les interfaces réseau et les pools de stockage retournent à leurs affectations (contrôleurs) d'origine. Il s'ensuit que les mises à jour de réplication risquent d'être impossibles parce que l'appareil source utilise l'interface réseau d'un contrôleur cible qui n'est plus propriétaire du pool. Cette erreur ne peut pas se produire si la configuration de réplication est effectuée alors que l'appareil cible est dans l'état CLUSTERED.

Exemple : Configuration de la réplication pour des appareils en cluster

La procédure décrite dans cet exemple utilise les interfaces réseau source et cible et les adresses IP suivantes :

Le cluster d'appareils source se compose des contrôleurs source S1 et S2. Le pool de stockage sp1 est assigné à S1 et le pool sp2 est assigné à S2. Les interfaces réseau du cluster sont les suivantes :

- Interface privée ixgbe0 sur S1, présentant l'adresse IP 198.51.100.81/24
- Interface privée ixgbe0 sur S2, présentant l'adresse IP 198.51.100.82/24
- Interface singleton ixgbe1 d'adresse IP 192.0.2.101/25 assignée à S1
- Interface singleton ixgbe2 d'adresse IP 192.0.2.102/25 assignée à S2
- Interface singleton ixgbe3 d'adresse IP 192.0.2.201/25 assignée à S1
- Interface singleton ixgbe4 d'adresse IP 192.0.2.202/25 assignée à S2

L'appareil est initialement dans l'état CLUSTERED, où :

- S1 est propriétaire de sp1, ixgbe1 et ixgbe3
- S2 est propriétaire de sp2, ixgbe2 et ixgbe4

Le cluster d'appareils cible se compose des contrôleurs T1 et T2. Le pool de stockage tp1 est assigné à T1 et le pool tp2 est assigné à T2. Les interfaces réseau du cluster sont les suivantes :

- Interface privée ixgbe0 sur T1, présentant l'adresse IP 198.51.100.83/24
- Interface privée ixgbe0 sur T2, présentant l'adresse IP 198.51.100.84/24
- Interface singleton ixgbe1 d'adresse IP 192.0.2.103/25 assignée à T1
- Interface singleton ixgbe2 d'adresse IP 192.0.2.104/25 assignée à T2
- Interface singleton ixgbe3 d'adresse IP 192.0.2.203/25 assignée à T1
- Interface singleton ixgbe4 d'adresse IP 192.0.2.204/25 assignée à T2

L'appareil est initialement dans l'état CLUSTERED, où :

- T1 est propriétaire de tp1, ixgbe1 et ixgbe3
- T2 est propriétaire de tp2, ixgbe2 et ixgbe4

Les étapes décrites ci-après permettent de configurer la réplication pour les projets Red, Blue et Green à l'aide de l'interface de ligne de commande (CLI).

1. Sélectionnez les interfaces réseau et les adresses IP.

- Commencez par sélectionner les interfaces réseau et les adresses IP à utiliser pour la réplication du projet Red.

Comme la source S est dans l'état CLUSTERED, il suffit de s'assurer que les interfaces réseau et adresses IP sélectionnées ne sont pas privées. Sur S1, utilisez par conséquent ixgbe1 ou ixgbe3.

- Il en va de même pour la cible T. Utilisez donc ixgbe1 ou ixgbe3 sur l'appareil T1. Comme ixgbe1 et ixgbe3 (que ce soit sur S1 ou sur T1) appartiennent au même sous-réseau, vous pouvez sélectionner indifféremment l'une ou l'autre interface pour la réplication du projet Red. Cet exemple choisit l'interface ixgbe1 sur S1 et sur T1.

2. Définissez une route statique sur S1.

L'exemple suivant configure la route statique pour la réplication du projet Red du contrôleur source S1 :

```
S1:configuration net routing> create
S1:configuration net route (uncommitted)> set family=IPv4
                                     family = IPv4 (uncommitted)
S1:configuration net route (uncommitted)> set destination=192.0.2.103
                                     destination = 192.0.2.103 (uncommitted)
S1:configuration net route (uncommitted)> set mask=32
                                     mask = 32 (uncommitted)
S1:configuration net route (uncommitted)> set interface=ixgbe1
                                     interface = ixgbe1 (uncommitted)
S1:configuration net route (uncommitted)> set gateway=192.0.2.1
                                     gateway = 192.0.2.1 (uncommitted)
S1:configuration net route (uncommitted)> commit
S1:configuration net routing> list
ROUTE      DESTINATION      GATEWAY      INTERFACE  TYPE      STATUS
...
route-003  192.0.2.103/32    192.0.2.1    ixgbe1     static    active
```

3. Définissez une route statique sur T1.

L'exemple suivant configure la route statique pour la réplication du projet Red du contrôleur cible T1 :

```
T1:configuration net routing> create
T1:configuration net route (uncommitted)> set family=IPv4
                                     family = IPv4 (uncommitted)
T1:configuration net route (uncommitted)> set destination=192.0.2.101
```

```

destination = 192.0.2.101 (uncommitted)
T1:configuration net route (uncommitted)> set mask=32
mask = 32 (uncommitted)
T1:configuration net route (uncommitted)> set interface=ixgbe1
interface = ixgbe1 (uncommitted)
T1:configuration net route (uncommitted)> set gateway=192.0.2.1
gateway = 192.0.2.1 (uncommitted)
T1:configuration net route (uncommitted)> commit
T1:configuration net routing> list
ROUTE      DESTINATION      GATEWAY      INTERFACE      TYPE      STATUS
...
route-003  192.0.2.101/32  192.0.2.1  ixgbe1      static  active

```

4. Créez une cible de réplication sur S1.

L'exemple suivant crée l'objet cible de réplication sur S1 à utiliser pour répliquer le projet Red de sp1 vers tp1 :

```

S1:shares replication
targets>target
S1:shares replication target (uncommitted)> set hostname=192.
0.2.103
hostname = 192.0.2.103 (uncommitted)
S1:shares replication target (uncommitted)> set label=t1-1
label = t1-1 (uncommitted)
S1:shares replication target (uncommitted)> set root_password=*****
root_password = (set) (uncommitted)
S1:shares replication target (uncommitted)> commit

```

5. Créez une action de réplication pour chaque projet.

- Répliquez le projet Red depuis le pool sp1 vers le pool tp1
- Répliquez le projet Blue depuis le pool sp1 vers le pool tp2
- Répliquez le projet Green depuis le pool sp2 vers le pool tp2

L'exemple suivant crée l'action de réplication pour le projet Red :

```

S1:> shares select Red replication action
S1:shares Red action (uncommitted)> set
target=t1-1
target=t1-1 (uncommitted)
S1:shares Red action (uncommitted)> set pool=tp1
pool=tp1 (uncommitted)
S1:shares Red action (uncommitted)> commit

```

6. Configurez la réplication du projet Blue du pool sp1 vers le pool tp2.

Commencez par la sélection d'interfaces et d'adresses : sélectionnez les interfaces S1/ixgbe3 et T2/ixgbe4, en sachant que S comme T sont dans l'état CLUSTERED et que les adresses IP de ces interfaces appartiennent au même sous-réseau (à savoir 192.0.2.128

/25). Ensuite, définissez des routes statiques sur les deux appareils comme illustré dans de précédents exemples. Créez l'objet cible de la réplication t2-2 sur S1, puis créez l'action de réplication sur S1 pour le projet Blue.

7. Configurez la réplication du projet Green du pool sp2 vers le pool tp2.

Commencez par la sélection des interfaces : sélectionnez S2/ixgbe2 et T2/ixgbe2. Créez les routes statiques sur S2 et T2 en utilisant les interfaces sélectionnées et leurs adresses, définissez l'objet cible de la réplication t2-1 avec l'adresse T2/ixgbe2, puis créez l'action de réplication du projet Green avec comme objet cible t2-1.

8. Lancez les trois actions de réplication.

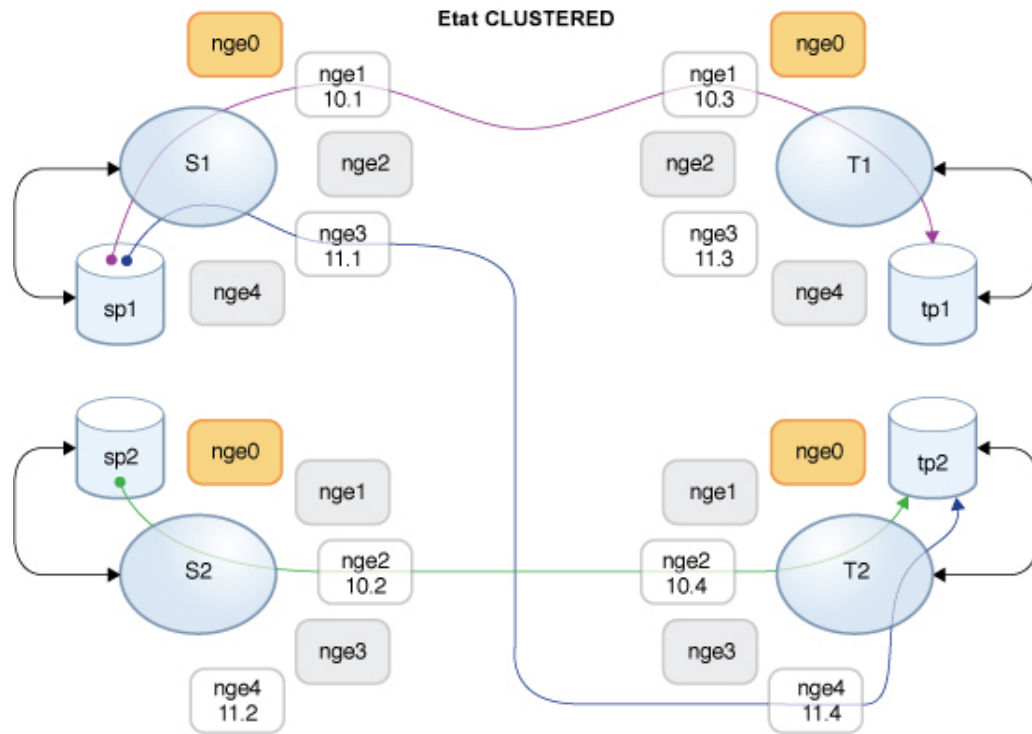
- a. Commencez par le projet Red :

```
S1:> shares select Red replication select action-000  
S1:shares Red action-000> sendupdate
```

- b. En suivant l'exemple précédent, lancez les actions de réplication définies pour les projets Blue et Green.

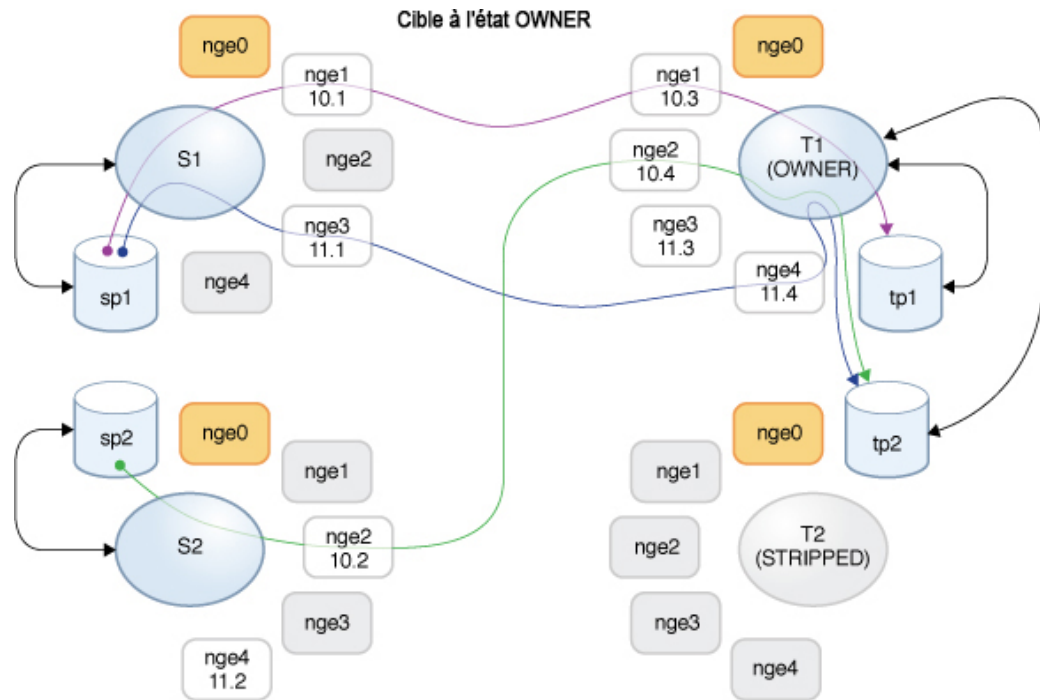
Chemin des données de réplication - Exemples

Les figures suivantes illustrent les chemins de réplication des données empruntés par les actions de réplication des projets Red, Blue et Green :

FIGURE 33 Chemin normal de réplication des données

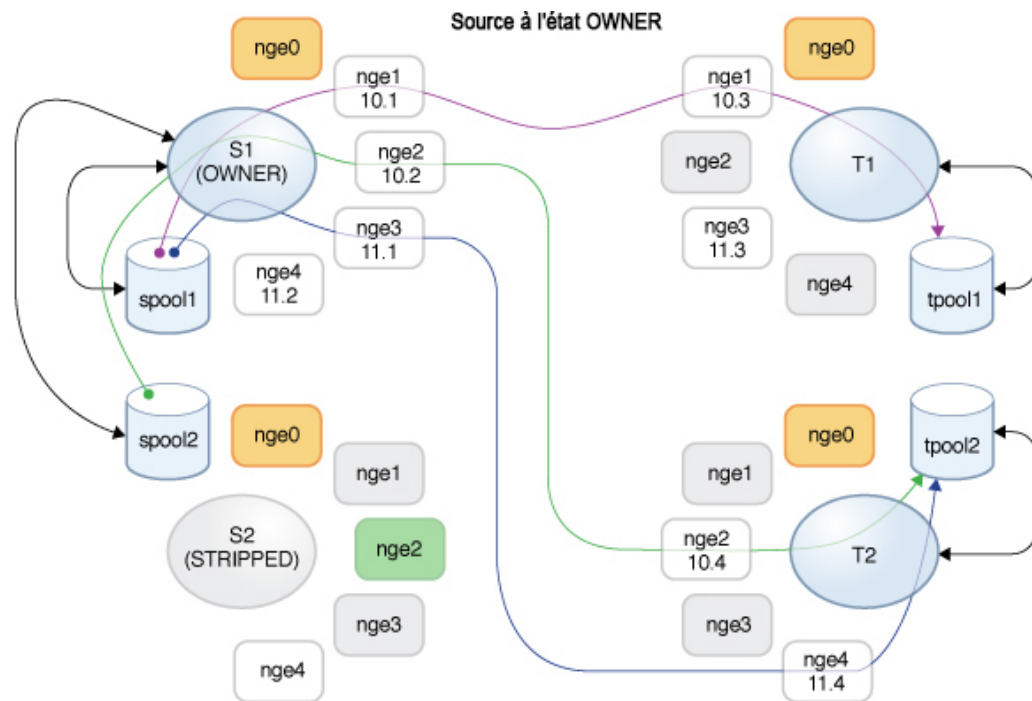
Supposons que le contrôleur T2 a dû être arrêté pour subir une opération de maintenance. T1 a effectué une reprise et détient désormais toutes les ressources. Si des mises à jour de réplication sont en cours pour les projets Blue et Green pendant la reprise, elles seront annulées. Une fois la reprise effectuée par T1, ces mises à jour de réplication peuvent faire l'objet d'une reprise manuelle ou bien attendre une reprise automatique si des calendriers ont été configurés pour les actions de réplication correspondantes.

Lorsque le contrôleur T1 a terminé la reprise, il possède les interfaces `ixgbe2` et `ixgbe4` qui sont nécessaires à la poursuite des mises à jour de réplication pour les projets Blue et Green. La figure suivante illustre le chemin des données de réplication après que T1 a terminé la reprise.

FIGURE 34 Chemin des données de réplication après la reprise par T1

Lorsque T2 est remis en ligne, un rétablissement est effectué sur le contrôleur T1 et il reprend ses ressources. Si des mises à jour de réplication des projets Blue et Green sont en cours, elles sont annulées et pourront être reprises à l'issue de l'opération de rétablissement.

Le contrôleur S2 est alors arrêté pour maintenance et la reprise effectuée sur le contrôleur S1 fait que ce dernier s'approprie toutes les ressources, y compris l'interface requise pour poursuivre la réplication du projet Green. Si une mise à jour de réplication de ce projet est en cours, elle est annulée en attendant de pouvoir être relancée à l'issue de l'opération de reprise.

FIGURE 35 Chemin des données après rétablissement sur T1 et reprise sur S1**Rubriques connexes**

- ["Configuration de la réplication pour un environnement de cluster" à la page 484](#)
- ["Workflow de réplication distante" à la page 474](#)
- ["Réplication distante" à la page 473](#)

Instantanés de réplication et cohérence des données

L'appareil source réplique les instantanés atomiquement vers la cible. En d'autres termes, les contenus de la réplique correspondent toujours exactement au partage de la source au moment de la capture de l'instantané. Les instantanés pour tous les partages envoyés dans un groupe spécifique étant effectués au même moment, après une mise à jour de réplication réussie, l'intégralité du contenu du package correspond exactement au contenu du groupe au moment où l'instantané a été créé sur la source.

Toutefois, les instantanés de chaque partage étant répliqués séparément, il est possible qu'au sein d'un même package, certains partages aient été mis à jour avec un instantané plus récent que d'autres. Cela est vrai durant la mise à jour de réplication et après l'échec d'une mise à jour de réplication.

En résumé :

- Chaque partage est toujours cohérent au moment précis de la création de l'instantané.
- Lorsqu'aucune mise à jour de réplication n'est en cours et que la précédente a réussi, chaque partage de package est également cohérent l'un avec l'autre.
- Lorsqu'une mise à jour de réplication est en cours ou que la précédente a échoué, il est possible que les partages de package soient incohérents les uns par rapport aux autres, mais chacun d'entre eux est cohérent en soi. Si la cohérence du package est importante pour une application, il faut cloner le package de réplication, qui clone toujours l'instantané réussi le plus récent de chaque partage.

Rubriques connexes

- ["Gestion des instantanés de réplication" à la page 546](#)

Gestion des instantanés de réplication

Les instantanés constituent la base de la réplication. La source et la cible doivent toujours avoir un instantané en commun pour poursuivre la réplication incrémentielle, et la source doit pouvoir déterminer l'instantané le plus récent sur la cible. Pour faciliter l'opération, le sous-système de réplication crée et gère ses propres instantanés. En général, les administrateurs n'ont pas besoin de s'en soucier, mais leurs détails sont décrits ici étant donné que les instantanés peuvent avoir des effets significatifs sur l'utilisation du stockage.

Chaque mise à jour de réplication pour une action particulière se compose des étapes suivantes :

- Déterminer s'il s'agit d'une mise à jour incrémentielle ou complète, en fonction des éléments suivants :
 - Une tentative de réplication de cette action a été effectuée antérieurement et
 - la cible dispose déjà de l'instantané nécessaire pour une mise à jour incrémentielle
- Prendre un nouvel instantané de niveau projet.
- Envoyer la mise à jour. Dans le cas d'une mise à jour complète, envoyer l'intégralité du contenu du groupe vers le nouvel instantané. Dans le cas d'une mise à jour incrémentielle, envoyer la différence entre l'instantané précédent (base) et le nouvel instantané.
- Enregistrer le nouvel instantané comme instantané de base pour la prochaine mise à jour et détruire le précédent (pour les mises à jour incrémentielles). L'instantané de base reste sur la cible jusqu'à ce que la mise à jour suivante soit reçue et est alors le premier élément détruit.

Cela présente plusieurs conséquences pour la gestion des instantanés :

- Au cours de la première mise à jour de réplication et après la mise à jour initiale, lorsque la réplication n'est pas active, il y a exactement un seul instantané de niveau projet pour

chaque action configurée sur le projet ou sur tout partage dans le groupe. Une action de réplication peut créer des instantanés sur des partages situés dans le même projet que le(s) partage(s) dans le groupe en cours de réplication par l'action mais qui ne sont pas envoyés dans le cadre de la mise à jour pour le groupe.

- Au cours des mises à jour de réplication ultérieures d'une action particulière, il se peut que deux instantanés de niveau projet soient associés à l'action. Il est possible que les deux instantanés subsistent après la fin de la mise à jour, au cas où une panne survienne rendant la source incapable de déterminer si la cible a bien reçu le nouvel instantané ou non (par exemple, dans le cas d'une coupure réseau au cours de la mise à jour entraînant une défaillance).
- L'administrateur ne peut pas supprimer les instantanés associés à une action de réplication sans interrompre la réplication incrémentielle. Le système n'autorise pas les administrateurs à détruire les instantanés (sur la source ou la cible) nécessaires à l'exécution de la réplication incrémentielle. Pour détruire ces instantanés sur la source, il faut supprimer l'action (ce qui détruit les instantanés associés à l'action). Pour détruire ces instantanés sur la cible, il faut d'abord dissocier le package (ce qui supprime la capacité de réception de mises à jour incrémentielles pour ce package).
- Les administrateurs ne doivent pas rétablir les instantanés créés avant les instantanés de réplication. Cette opération supprimerait tous les instantanés de réplication ultérieurs et interromprait la réplication incrémentielle pour toutes les actions utilisant ces instantanés.
- Pour utiliser des instantanés dans le cadre de la réplication, les administrateurs doivent comprendre la gestion de l'espace sur l'appareil, notamment son application aux instantanés.

Rubriques connexes

- ["Gestion de l'espace pour les partages" à la page 400](#)
- [Réplication distante pour sauvegarde disque à disque](#)

Réplication et configurations iSCSI

Les mises à jour de réplication comprennent la quasi-intégralité de la configuration indiquée sur l'écran Partages pour un projet et ses partages. Cela comprend les groupes de cibles et d'initiateurs associés aux LUN répliqués.

Lors de l'utilisation des groupes de cibles et d'initiateurs personnalisés, les administrateurs doivent garantir que les groupes utilisés par les LUN au sein de projet existent également sur la cible de réplication. Si le groupe cible ou le groupe d'initiateurs n'existe pas sur le système cible, une opération de clonage, de dissociation ou d'inversion de la réplication échouera. Un message d'erreur signale que le nom du groupe cible ou d'initiateurs a été supprimé ou modifié sur le système cible.

Le GUID SCSI associé à un LUN est répliqué avec le LUN. Par conséquent, la LUN sur l'appareil cible possède le même SCSI GUID que la LUN sur l'appareil source. Cela dit, les

clones des LUN répliqués auront différents GUID (tout comme les clones des LUN locaux possèdent des GUID différents de celles d'origine).

Rubriques connexes

- ["Workflow de réplication distante" à la page 474](#)
- ["Réplication distante" à la page 473](#)

Echecs de réplication

Les mises à jour de réplication individuelles peuvent échouer pour différentes raisons. Lorsque c'est possible, l'appareil signale la raison de l'échec de l'action dans les alertes publiées sur l'appareil source ou cible, ou dans l'écran Réplication. Vous pouvez obtenir des détails sur l'échec en cliquant sur l'icône d'alerte orange représentant le statut de l'action.

Les types d'échecs de réplication suivants sont les plus courants :

Echec	Détails
Annulée	La mise à jour de réplication a été annulée par un administrateur. La réplication peut être annulée sur la source ou la cible.
Panne de connectivité réseau	L'appareil n'a pas pu se connecter à l'appareil cible en raison d'un problème réseau. Il existe peut-être une erreur de configuration sur la source, la cible ou le réseau.
Echec de la vérification du pair	L'appareil n'est pas parvenu à vérifier l'identité de la source. Cela se produit généralement lorsque la cible a été réinstallée ou que ses paramètres d'usine ont été rétablis. Il faut configurer une nouvelle cible de réplication sur l'appareil source pour une cible qui a été réinstallée ou dont les paramètres d'usine ont été rétablis afin de générer un nouveau jeu de clés d'authentification. Reportez-vous à la section " Cibles de réplication " à la page 532.
Echec du RPC du pair	Un appel de procédure distante sur le système cible a échoué. Cela se produit généralement lorsque l'appareil cible exécute un logiciel incompatible.
Collision de noms	La réplication de <code><project/share></code> depuis <code><source></code> échoue en raison d'une collision de noms avec <code>@<snapname></code> qui est conservé sur la cible pour NDMP. Pour effectuer une récupération, renommez (ou supprimez) l'instantané sur la source de réplication dont le nom est identique à celui de l'instantané conservé par NDMP sur la cible (celui nommé dans l'alerte), à moins qu'il ne commence par <code>.rr</code> . Puis effectuez une synchronisation manuelle ou autorisez la source de réplication à retenter automatiquement la mise à jour de réplication.
Aucun package	La réplication a échoué car aucun package n'existe sur la cible pour accueillir les données répliquées. Etant

Echec	Détails
	donné que le package est créé après avoir configuré l'action, l'erreur se produit généralement après qu'un administrateur a supprimé le package sur la cible. Cette erreur peut également se produire si le pool de stockage n'est pas importé sur le système cible, ce qui peut arriver si le pool est défectueux ou si le stockage ou la mise en réseau a été reconfiguré(e) sur l'appareil cible.
Un package non vide est présent	La réplication a échoué car le package cible contient des données d'une précédente mise à jour de réplication qui a échoué. Cette erreur se produit lors d'une tentative d'envoi d'une mise à jour de réplication pour une action dont la première mise à jour de réplication a échoué après la réplication d'une partie des données. L'appareil cible ne supprimant pas les données sans ordre explicite de l'administrateur, les données partiellement reçues ne sont pas écrasées. L'administrateur doit supprimer l'action et le package existants et créer une nouvelle action sur la source, puis relancer la réplication.
Désactivé	La réplication a échoué car elle est désactivée sur la cible. Soit le service de réplication est désactivé sur la cible, soit la réplication a été désactivée pour le package spécifique étant répliqué.
Cible occupée	La réplication a échoué car le système cible a atteint le nombre maximal de mises à jour de réplication simultanées. Le système limite le nombre maximal d'opérations de réplication en cours afin d'éviter la saturation des ressources. Lorsque cette limite est atteinte, les tentatives ultérieures de réception de mises à jour échouent et indiquent cette erreur, tandis que les tentatives d'envoi de mises à jour sont mis en attente jusqu'à ce que les ressources soient disponibles.
Espace saturé	La réplication a échoué car le système source ne disposait pas d'espace suffisant pour créer un nouvel instantané. Cela peut être causé par l'absence d'espace physique disponible sur le pool de stockage, ou car le projet ou un de ses partages dépasse des quotas en raison de réservations qui ne comprennent pas les instantanés.
Indisponibilité de clés	La réplication a échoué car la clé de chiffrement utilisée par le partage n'est pas disponible, soit sur le système source soit sur le système cible. Passez les alertes en revue sur les deux systèmes, source et cible, afin de vous assurer que la clé est disponible sur les deux systèmes. Reportez-vous à la section " Réplication d'un partage chiffré " à la page 589 pour plus d'informations sur la réplication de projets et de partages chiffrés.
Cible incompatible	La réplication a échoué car le système cible ne peut pas recevoir le format de flux du système source. Cela peut se produire consécutivement à la mise à niveau d'un système source et à l'application de mises à jour différées sans avoir mis à niveau et appliqué les mêmes mises à jour sur la cible. Consultez les notes de version du logiciel du système à propos des mises à jour différées

Echec	Détails
	et de leurs éventuelles implications pour la réplication distante.
Initiateur/cible iSCSI manquant(e)	L'opération de clone, de dissociation ou d'inversion de réplication a échoué car les LUN de groupe d'initiateurs ou de groupe cible n'existent pas pour les LUN inclus dans le package de réplication. Le nom du groupe cible ou d'initiateurs a été supprimé ou modifié sur le système cible.
Divers	La réplication a échoué, mais aucune information supplémentaire n'est disponible sur la source. Consultez le journal d'alertes sur le système cible et si nécessaire, contactez le support pour obtenir une assistance. Certains modes d'erreur qui entrent dans cette catégorie comprennent l'espace disque insuffisant pour recevoir la mise à jour et la tentative de réplication d'un clone dont l'instantané d'origine n'existe pas sur le système cible.

Une mise à jour de réplication échoue si une partie de la mise à jour échoue. L'implémentation actuelle réplique en série les partages au sein d'un projet et n'annule pas les modifications des mises à jour ayant échoué. Par conséquent, lorsqu'une mise à jour échoue, il est possible que certains partages sur la cible soient à jour, et que d'autres non. Pour plus d'informations, reportez-vous à la section "[Instantanés de réplication et cohérence des données](#)" à la page 545.

Bien que certaines données aient été répliquées avec succès dans le cadre d'une mise à jour ayant échoué, l'implémentation actuelle renvoie toutes les données envoyées dans la précédente mise à jour (en échec). Concrètement, les mises à jour ayant échoué ne reprennent pas là où elles se sont arrêtées, mais démarrent là où la mise à jour qui a échoué a commencé.

Lorsque la réplication en continu ou planifiée échoue, le système attend plusieurs minutes puis effectue une nouvelle tentative. Le système continue à réessayer indéfiniment les réplications en continu ou planifiées. A tout moment pendant la procédure de nouvel essai, lancer une mise à jour manuelle commence immédiatement un nouvel essai, le délai habituel entre les nouveaux essais n'étant pas observé. Si la mise à jour manuelle réussit, elle met fin à la séquence des nouveaux essais et l'action de réplication retrouve ses mises à jour planifiées ou en continu. Les réplications manuelles ayant échoué sans action de réplication planifiée préalable ne font pas l'objet d'un nouvel essai.

Lorsqu'une mise à jour de réplication est en cours et qu'une autre est programmée, cette dernière est retardée jusqu'à la fin de la mise à jour précédente et une alerte est émise.

Rubriques connexes

- *How to Troubleshoot Replication Issues* (ID de doc 1397959.1) sur [My Oracle Support](#) (<http://support.oracle.com/>)

Propriétés des actions de réplication

Les actions de réplication possèdent les propriétés suivantes,

qui sont présentées légèrement différemment dans la BUI et la CLI, conformément au tableau qui suit.

TABLEAU 124 Propriétés de la CLI des actions de réplication (BUI et CLI)

Propriété de la BUI	Propriété de la CLI	Description
Cible	cible	Identifiant unique du système cible de la réplication. Cette propriété est spécifiée si une action est initialement configurée et ne peut pas être modifiée.
Pool	pool	Pool de stockage sur la cible où ce projet sera répliqué. Cette propriété est spécifiée lorsqu'une action est initialement configurée et non affichée par la suite.
Exporter le chemin de données	export_path	Saisissez un chemin vers un partage NFS pour cette action sous la forme <code>NFS://server/path</code> . Vous exportez ainsi le flux de réplication vers un fichier sur un serveur NFS, que vous pouvez déplacer physiquement sur le site cible distant, puis vous pouvez importer la réplique initiale sur l'appareil cible. Pour obtenir les procédures, reportez-vous à la section "Création d'une réplication hors ligne (BUI)" à la page 486 .
Limite de la bande passante	max_bandwidth	Spécifie une vitesse maximale pour cette mise à jour de réplication (en termes de quantités de données transférées chaque seconde sur le réseau). Les modifications apportées à cette propriété lors de la mise à jour de réplication ne sont appliquées qu'à la mise à jour suivante.
Enable SSL-encryption	use_ssl	Chiffre ou non les données simultanément à l'aide de la technologie SSL. L'utilisation de cette fonction peut avoir un impact significatif sur les performances de réplication par action.
Disable compression	compression	Le flux de réplication est compressé par défaut. Désactivez cette propriété si la compression se fait d'une autre manière, par exemple à l'aide d'un accélérateur WAN. Pour plus d'informations, reportez-vous la section "Réplication compressée" à la page 552 .
Include Snapshots	include_snaps	Détermine si les mises à jour de réplication contiennent ou non des instantanés de non-réplication. Pour plus d'informations, reportez-vous à la section "Gestion des instantanés de réplication" à la page 546 .
Conserver les instantanés utilisateurs sur la cible	retain_user_snaps_on_target	Conserve les instantanés générés par l'utilisateur sur l'appareil cible de réplication pour l'action associée, même une fois que les instantanés sont détruits sur l'appareil source. Les instantanés conservés sur la cible peuvent ensuite être utilisés dans le cadre d'une solution de sauvegarde de données ou disque à disque. Pour plus de détails, reportez-vous à la section "Utilisation de la réplication distante pour la sauvegarde disque à disque" .
Inclure l'origine du clone sous forme de données	include_clone_origin_as_data	Contrôle la réplication de chaque partage qui a été cloné à partir d'un partage externe au package de réplication sur la cible. Sélectionnez cette option pour insérer une copie complète des données de l'instantané d'origine du clone dans la réplique du clone. Si vous désélectionnez cette option, un clone créé à partir d'un instantané d'origine externe partagera le stockage avec la réplique de l'instantané d'origine du clone qui se trouve dans le pool de la cible de réplication. Le partage du stockage permet d'économiser de l'espace, mais si la cible de réplication ne contient pas

Propriété de la BUI	Propriété de la CLI	Description
		l'instantané d'origine du clone externe, la réplication du clone échoue. Pour plus de détails, reportez-vous à la section "Clonage d'un package de réplication ou d'un partage" à la page 554.
Fréquence de mise à jour	continuous	Sélectionnez Scheduled (programmé) ou Continuous (continu). Pour plus de détails, reportez-vous à la section "Actions et packages de réplication" à la page 533.
Schedule	schedule frequency	Sélectionnez la fréquence : toutes les demi-heures, toutes les heures, tous les jours, toutes les semaines ou tous les mois.

Le tableau suivant décrit les propriétés des actions de réplication en lecture seule de la CLI :

TABLEAU 125 Propriétés des actions de réplication (CLI, lecture seule)

Propriété de la CLI	Description
Bytes sent	Propriété en lecture seule qui décrit le nombre d'octets envoyé à la cible.
Estimated size	Propriété en lecture seule qui décrit la taille estimée des données à répliquer.
Estimated time left	Propriété en lecture seule qui décrit le temps restant estimé avant la fin.
Average throughput	Propriété en lecture seule qui décrit le débit de réplication moyen.
Etat	Propriété en lecture seule décrivant si l'action est inactive, en cours d'envoi d'une mise à jour ou en cours d'annulation d'une mise à jour.
Last sync	Propriété en lecture seule indiquant l'heure du dernier envoi réussi d'une mise à jour. Cette valeur peut être inconnue si le système n'a pas envoyé une mise à jour réussie depuis l'initialisation.
Last attempt	Propriété en lecture seule indiquant l'heure de la dernière tentative de mise à jour. Cette valeur peut être inconnue si le système n'a pas tenté de procéder à une mise à jour depuis l'initialisation.
Next update	Propriété en lecture seule indiquant quand aura lieu la prochaine tentative. Cette valeur peut être une date (pour une mise à jour programmée), manual ou continuous.

Rubriques connexes

- ["Création d'une action de réplication \(BUI\)" à la page 480](#)
- ["Création d'une action de réplication \(CLI\)" à la page 482](#)

Réplication compressée

La fonctionnalité de réplication compressée améliore les performances lors de la réplication de données compressées entre les sites source et cible dont la bande passante est limitée. Avant l'envoi d'un flux de réplication à la cible, il est automatiquement compressé à un taux basé sur l'utilisation actuelle de la CPU et du débit d'E/S du réseau. Le flux de réplication est ensuite décompressé lorsqu'il est reçu par l'appareil cible. Si une partie des données n'est pas compressible, elle est envoyée comme si la compression était désactivée.

Tous les flux de réplication sont compressés, sauf si vous désactivez explicitement la compression. Si votre équipement WAN fournit la compression, par exemple via un accélérateur WAN, désactivez la fonction de compression en suivant la procédure Désactivation de la compression de réplication - [BUI](#), [CLI](#).

Les appareils source et cible nécessitent la version logicielle 2013.1.4.0 (ou ultérieure) pour prendre en charge la compression de réplication. Si la cible dispose d'une version antérieure, une icône d'avertissement  s'affiche en regard du nom de la cible. Vous devrez mettre à jour l'appareil cible vers la version minimale.

Vous pouvez afficher les statistiques des performances de réplication sur l'appareil source, sous la barre de progression de la réplication.

Actions		
TARGET ▲	UPDATES	STATUS
 hog-10g Manual	Never Synced Never Attempted	43% of 10.0G @548MB/s (-00:00:11)

Packages de réplication

Les packages sont des conteneurs pour les projets et partages répliqués. Chaque action de réplication sur un appareil source correspond à un package sur l'appareil cible.

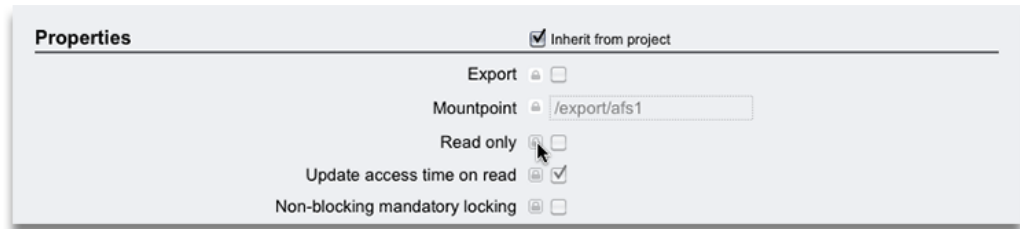
La BUI et la CLI vous permettent de parcourir les projets, partages, instantanés et propriétés répliqués, de la même manière que pour les projets et partages locaux. Cependant, les partages répliqués devant correspondre exactement à leurs homologues sur l'appareil source, une grand quantité d'opérations de gestion ne sont pas autorisées dans les packages de réplication.

Vous pouvez modifier les propriétés suivantes des projets et partages répliqués :

- **Réservation, compression, copies, suppression des doublons et mise en cache** : ces propriétés peuvent être modifiées sur la cible de réplication pour refléter différentes stratégies de coût, de flexibilité, de performances ou de fiabilité sur l'appareil cible, en provenance de la source.
- **Propriétés de partage et point de montage** (p. ex. sharenfs, nom de la ressource SMB, etc.) : ces propriétés contrôlent la façon dont les partages sont exportés vers les clients NAS et peuvent être modifiées pour refléter différentes stratégies de sécurité ou de protection sur l'appareil cible, en provenance de la source.
- **Stratégies en matière d'instantanés automatiques** : les stratégies d'instantané automatique peuvent être modifiées sur l'appareil cible mais n'ont aucun effet tant que le package n'est pas dissocié. Des instantanés automatiques ne sont pas pris ni supprimés sur les projets et partages répliqués.

Les modifications de propriété de ce type persistent après les mises à jour de réplication.

FIGURE 36 Propriétés de gestion des packages de réplication



Rubriques connexes

- ["Propriétés des projets et partages" à la page 363](#)
- ["Dissociation de la réplication" à la page 557](#)

Clonage d'un package de réplication ou d'un partage

Un *clone* d'un package répliqué désigne un projet local et mutable qui peut être géré comme n'importe quel autre projet du système. Lors de la création du projet cloné, le dernier instantané reçu des partages répliqués est utilisé pour créer les partages au sein du projet cloné. Ces clones partagent le stockage avec leurs instantanés d'origine de la même manière que le font les clones des instantanés de partages (reportez-vous à la section Clonage d'un instantané [BUI](#), [CLI](#)). Ce mécanisme peut être utilisé pour un basculement dans le cas d'un problème majeur sur la source de réplication, ou simplement pour fournir une version locale modifiable des données.

Tant qu'un clone existe, son instantané d'origine ne peut pas être supprimé. Lors de la suppression de l'instantané (conséquence possible de la destruction du partage, du projet ou du package de réplication dont l'instantané est membre), le système avertit les administrateurs de la présence de clones dépendants qui seront supprimés par l'opération. Notez que les instantanés peuvent également être détruits sur la source à tout moment, et qu'ils sont supprimés de la cible dans le cadre d'une mise à jour de réplication ultérieure. Si un tel instantané possède des clones, il ne sera pas supprimé tant que le dernier clone n'a pas été supprimé.

Réplication de clones

Lors de la réplication de clones, il est important de comprendre la relation entre une réplique de clone et son instantané d'origine. Par défaut, la réplique d'un clone conserve sa relation avec

son instantané d'origine, mais une réplique de l'instantané d'origine doit également exister sur la cible. Une réplique d'un instantané du clone d'origine doit se trouver dans le même pool que le clone, mais pas forcément dans le même projet.

Pour conserver la relation entre un clone répliqué et son instantané d'origine, ce dernier doit être :

- répliqué sur la cible avant la réplication initiale du clone ou
- répliqué dans le cadre de la même mise à jour.

Cette restriction n'est pas appliquée par le logiciel de l'appareil, mais doit être respectée pour garantir la réussite de la mise à jour de la réplication.

Il existe plusieurs moyens d'assurer la réussite de la réplication d'un clone afin qu'il conserve sa relation avec son instantané d'origine :

- Si l'instantané d'origine du clone se trouve dans le même projet, utilisez la réplication de niveau projet.
- Si le partage contenant l'instantané d'origine du clone ne se trouve pas dans le même projet, ou si le clone ou son partage d'origine ont été omis de la réplication de niveau projet, répliquez le partage d'origine dans un premier temps, puis répliquez le clone à l'aide de la réplication de niveau projet ou partage.
- Sur le système cible, ne détruisez pas l'original du clone à moins de vouloir également supprimer le clone lui-même.

Pour que l'instantané d'origine soit envoyé vers la cible, définissez toujours la propriété "Inclure les instantanés" pour la réplication d'origine.

De même qu'un clone et son instantané d'origine conservent de l'espace sur l'appareil source, un clone répliqué et son instantané d'origine répliqué conservent de l'espace sur l'appareil cible. Si la conservation d'espace sur la cible de la réplication a moins d'importance, l'administrateur peut définir la propriété Inclure l'origine du clone sous forme de données. Lorsque cette propriété est définie et que l'instantané d'origine d'un clone *n'est pas* répliqué dans la même mise à jour que le clone, l'appareil source insère une copie du contenu de données de l'original du clone dans le clone de la réplique. Il n'est donc pas nécessaire de répliquer en premier lieu le partage d'origine du clone, mais la copie des données d'origine du clone consomme un espace de stockage supplémentaire sur la cible.

Lorsque Inclure les instantanés et Inclure l'origine du clone sous forme de données sont tous les deux définis, le clone de la réplique contient uniquement les instantanés qui sont présents dans le clone sur la source. L'appareil source insère le contenu de données d'origine du clone, et non les instantanés d'origine du clone, dans le clone de la réplique. Ainsi, les instantanés présents dans le clone de la réplique correspondent à ceux qui se trouvent dans le clone sur la source.

La propriété Inclure l'origine du clone sous forme de données n'affecte pas la réplication d'un clone et son instantané d'origine lorsqu'ils sont tous deux répliqués dans la

même mise à jour. Lorsqu'ils sont répliqués ensemble par la même action de réplication, la relation entre le clone et son instantané d'origine est préservée et l'avantage du partage d'espace est conservé sur la cible.

Rubriques connexes

- ["Réplication de projet et réplication de partage" à la page 535](#)
- Clonage d'un package de réplication [BUI](#), [CLI](#)
- ["Propriétés des projets et partages" à la page 363](#)

Exportation de systèmes de fichiers répliqués

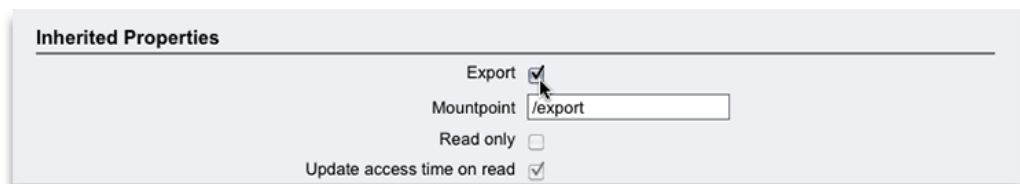
Les systèmes de fichiers peuvent être exportés en lecture seule vers les clients NAS. Cela peut permettre de vérifier les données répliquées ou d'effectuer des sauvegardes ou d'autres opérations utilisant beaucoup de ressources sur les données répliquées (libérant l'appareil source de cette charge de travail).

Le contenu du système de fichiers correspond toujours à l'instantané de réplication le plus récent reçu pour le système de fichier en question. Il se peut qu'il soit plus récent que le dernier instantané reçu pour l'intégralité du package, et il est possible qu'il ne corresponde pas au dernier instantané pour les autres partages dans le même package. Pour plus de détails, reportez-vous à la section ["Instantanés de réplication et cohérence des données" à la page 545](#).

Les mises à jour de réplication sont appliquées atomiquement au niveau du système de fichiers. Les clients consultant les fichiers répliqués verront les mises à jour de réplication comme une modification instantanée dans le système de fichiers sous-jacent. Les clients travaillant avec des fichiers supprimés dans la mise à jour la plus récente rencontreront des erreurs. Les clients travaillant avec des fichiers modifiés dans la mise à jour la plus récente verront immédiatement le contenu mis à jour.

Par défaut, les systèmes de fichiers répliqués ne sont pas exportés. Il sont exportés en modifiant la propriété "exporté" du projet ou du partage dans la BUI ou la CLI :

FIGURE 37 Propriétés héritées



A l'instar des autres propriétés de partage, cette propriété est héritée. Cette propriété ne s'affiche pas pour les projets et partages locaux car ils sont toujours exportés. De plus, dissocier la réplication (ce qui convertit le package en projet local) entraîne l'exportation des partages du package.

Les LUN répliqués ne peuvent actuellement pas être exportés. Ils doivent d'abord être clonés ou le package de réplication doit être dissocié pour en exporter le contenu.

Rubriques connexes

- ["Workflow de réplication distante" à la page 474](#)
- ["Propriétés héritées" à la page 364](#)

Dissociation de la réplication

Un package de réplication peut être converti en projet inscriptible local exploitable comme n'importe quel autre projet local (c'est-à-dire sans les restrictions de gestion appliquées aux packages de réplication) en dissociant la connexion de réplication. Une fois cette opération effectuée, ce package ne peut plus recevoir de mises à jour de réplication. Les mises à jour ultérieures du même projet à partir de la source doivent donc envoyer une mises à jour complète accompagnée d'une nouvelle action (et dans un nouveau package). Les mises à jour de réplication ultérieures échouent car le package correspondant n'existe plus sur la cible.

Cette option est utile essentiellement lors de l'emploi de la réplication pour migrer des données entre les appareils ou dans d'autres scénarios qui n'impliquent pas de réplication des données reçues vers la source dans le cadre d'un plan de récupération après sinistre.

L'opération de dissociation de la réplication convertit un package de réplication en projet local standard. Comme tous les partages locaux sont toujours exportés et qu'ils peuvent être partagés via SMB, l'opération de dissociation échoue s'il existe des conflits de point de montage ou de nom de ressource SMB entre les systèmes de fichiers répliqués et les autres systèmes de fichiers. Il faut résoudre ces conflits avant de dissocier le package de réplication en reconfigurant les points de montage ou les noms de ressource SMB des projets ou des partages.

Rubriques connexes

- Dissociation d'un package de réplication - [BUI](#), [CLI](#)
- Configuration de la réplication distante pour la récupération après sinistre - [BUI](#), [CLI](#)
- [Utilisation de la réplication pour les sauvegardes disque à disque](#)

Fonctionnement de la réplication inversée

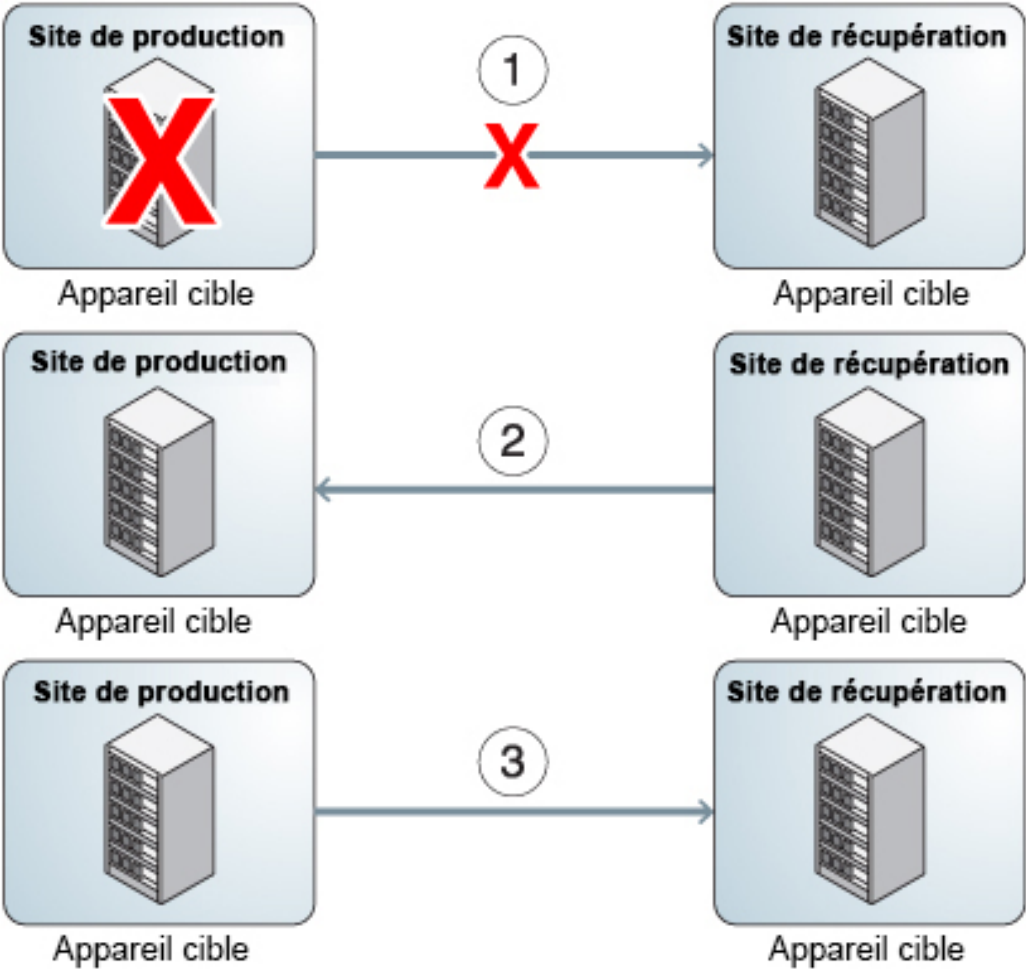
Il est possible d'inverser le sens de réplication pour prendre en charge les plans de récupération après sinistre à deux systèmes et les sauvegardes disque à disque.

Inversion de la réplication pour une récupération après sinistre

L'opération de réplication inversée convertit le package de réplication en un projet local. Cette opération configure également une action de réplication sur le nouveau projet local permettant la réplication incrémentielle vers l'appareil source. La première tentative de mise à jour convertit le projet d'origine sur le système source en package de réplication et annule toute modification effectuée depuis la dernière mise à jour de réplication réussie sur ce système.

La figure suivante décrit une séquence standard de réplication inversée.

FIGURE 38 Réplication distante pour la récupération après sinistre



Légende	Description
1	Le système de production correspond à l'appareil source qui sert la charge de travail du client et réplique vers l'appareil cible situé sur le site de récupération. Une défaillance complète de l'appareil source se produit sur le site de production. Depuis le site de récupération, l'administrateur inverse le sens de la réplication. Cette opération convertit le package de réplication en projet local et accessible en écriture. L'administrateur redirige les charges de travail du client et bascule les adresses IP vers le site de récupération.

Légende	Description
2	Une fois le site de production en mesure de reprendre son activité normale, l'administrateur lance une mise à jour de réplication du site de récupération au site de production. Cette opération convertit la copie de production en package de réplication et restaure l'ensemble des modifications écrites dans le site de récupération pendant que le site de production était en panne.
3	Une fois le site de production mis à jour, le sens de la réplication est à nouveau inversé par l'administrateur, rendant la copie accessible en écriture sur le site de production. L'administrateur redirige ensuite les charges de travail du client et bascule les adresses IP vers le site de production. La relation initiale entre l'appareil source sur le site de production et l'appareil cible sur le site de récupération est rétablie.

Dans le cadre de la conversion du projet source d'origine en package de réplication sur le système source d'origine (faisant désormais office de cible), les partages répliqués en tant que paire action/package en cours d'inversion sont déplacées dans un nouveau package de réplication et leur exportation est annulée. Le projet d'origine reste dans la collection, locale mais peut se retrouver vide si la paire action/package contenait tous ses partages. Lorsque la réplication de niveau partage est inversée, aucun autre partage du projet d'origine n'est modifié.

Après avoir établi la réplication de niveau partage d'un appareil à un autre, l'inversion de cette réplication sur l'appareil cible supprime le calendrier de réplication. Une action de réplication est ensuite créée au niveau projet, qui comprend l'appareil cible correct sans calendrier.

Lors de l'inversion du sens de réplication pour un package, il est vivement recommandé aux administrateurs de commencer par arrêter la réplication de ce projet à partir de la source. Si une mise à jour de réplication est en cours lorsqu'un administrateur inverse le sens de réplication d'un projet, les administrateurs ne peuvent pas savoir quel instantané de réplication cohérent a été utilisé pour créer le projet qui en résulte sur le précédent appareil cible (qui est maintenant l'appareil source).

Tous les partages locaux étant exportés, tous les partages d'un package sont exportés lorsque celui-ci est inversé, qu'ils l'aient déjà été ou non. S'il existe des conflits de point de montage entre les systèmes de fichiers répliqués et les autres systèmes de fichiers, l'opération d'inversion échoue. Il faut résoudre ces conflits avant l'inversion en reconfigurant les points de montage des partages concernés. Cette opération faisant généralement partie du chemin critique de restauration du service de production, il est vivement recommandé de résoudre ces conflits de point de montage lors de la configuration initiale du système plutôt que lors du basculement de récupération après sinistre.

Rubriques connexes

- ["Configuration de réplication distante pour récupération après sinistre \(BUI\)" à la page 519](#)
- ["Configuration de réplication distante pour récupération après sinistre \(CLI\)" à la page 522](#)
- [Réplication distante pour sauvegarde disque à disque](#)

Destruction d'un package de réplication

Le projet et les partages au sein d'un package ne peuvent pas être détruits sans supprimer l'intégralité du package. Il est possible de détruire l'intégralité du package dans la BUI en supprimant le projet correspondant. Un package peut être supprimé dans la CLI en exécutant la commande `destroy` au niveau du noeud `shares replication sources`.

Lorsqu'un package est supprimé, les mises à jour de réplication ultérieures de l'action correspondante échouent. Pour reprendre la réplication, il faut recréer l'action sur la source pour créer un nouveau package sur la cible, qui doit recevoir une nouvelle copie des données.

Sauvegardes de réplique cible

Vous pouvez sauvegarder des ensembles de données de réplique cible (projets ou partages) à l'aide de la sauvegarde NDMP de type `zfs`. La sauvegarde de réplique est activée sur l'appareil en appliquant la prise en charge de mise à jour différée pour la sauvegarde de réplique NDMP de type `zfs`. La fonctionnalité de sauvegarde de réplique choisit l'instantané généré par le système le plus récent pour qu'il soit sauvegardé, sauf si vous indiquez un instantané généré par un utilisateur (extension différente de `.rr`). Pour plus d'informations, reportez-vous à la section ["Sauvegardes de réplique" à la page 272](#).

Certains instantanés de réplication plus anciens, ceux conservés à l'origine pour des sauvegardes incrémentielles à venir, peuvent ne pas être nécessaires et peuvent être supprimés. Si un instantané est conservé par NDMP, une confirmation affiche un avertissement de l'impact potentiel sur les sauvegardes NDMP en cours ou à venir.

La séquence d'événements suivants provoque l'échec d'une réplication et génère une alerte. Pour plus d'informations sur la récupération de cette erreur, reportez-vous à la rubrique "Collision de noms" dans la section ["Echecs de réplication" à la page 548](#).

1. Un instantané de réplique est conservé par NDMP sur l'appareil cible (pour une sauvegarde en cours ou une sauvegarde incrémentielle à venir).
2. L'instantané correspondant sur l'appareil source est supprimé ou renommé.
3. Un nouvel instantané est créé sur l'appareil source avec un nom identique à celui de l'instantané de réplique conservé sur l'appareil cible.
4. Une mise à jour de réplication est tentée.

Chiffrement de données

NOTICE RELATIVE A LA LICENCE : *le chiffrement peut faire l'objet d'une évaluation à titre gratuit, mais cette fonction requiert l'achat d'une licence distincte pour un usage en production. Des licences de fonction de chiffrement sont uniquement disponibles pour les modèles Oracle ZFS Storage ZS4-4 et Oracle ZFS Storage ZS3-4. Au terme de la période d'évaluation, il convient d'acheter une licence pour cette fonction ou de la désactiver. Oracle se réserve le droit de vérifier la conformité de la licence à tout moment. Pour plus d'informations, reportez-vous au document "Oracle Software License Agreement ("SLA") and Entitlement for Hardware Systems with Integrated Software Options (contrat de licence du logiciel Oracle et droits concédés pour les systèmes matériels comprenant des options logicielles intégrées)."*

Oracle ZFS Storage Appliance offre un chiffrement transparent des données pour les partages individuels (systèmes de fichiers et LUN) et les partages créés au sein des projets..

Pour configurer et gérer le chiffrement, utilisez ces tâches :

- ["Workflow de chiffrement de données" à la page 564](#)
- Configuration du chiffrement du keystore LOCAL - [BUI](#), [CLI](#)
- Configuration du chiffrement du keystore OKM - [BUI](#), [CLI](#)
- Création d'un projet chiffré - [BUI](#), [CLI](#)
- Modification de la clé de chiffrement d'un projet - [BUI](#), [CLI](#)
- Création d'un système de fichiers ou d'un LUN chiffré - [BUI](#), [CLI](#)
- Modification d'une clé de chiffrement de partage - [BUI](#), [CLI](#)
- Sauvegarde d'une clé locale - [BUI](#), [CLI](#)
- Suppression d'une clé de chiffrement - [BUI](#), [CLI](#)
- Restauration d'une clé locale - [BUI](#), [CLI](#)
- Clonage d'un instantané - [BUI](#), [CLI](#)

Pour comprendre le chiffrement des données, reportez-vous aux rubriques suivantes :

- ["Propriétés de cryptage" à la page 584](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Impact du chiffrement sur les performances" à la page 587](#)
- ["Cycle de vie d'une clé de chiffrement" à la page 588](#)
- ["Sauvegarde et restauration de données chiffrées" à la page 588](#)
- ["Réplication d'un partage chiffré" à la page 589](#)

▼ Workflow de chiffrement de données

Les étapes suivantes indiquent la procédure générale de configuration et d'utilisation du chiffrement de données. Pour plus d'informations sur les propriétés de chiffrement, reportez-vous à ["Propriétés de cryptage" à la page 584](#).

1. Configurez le chiffrement par le keystore LOCAL ou OKM (Oracle Key Manager).

Pour plus d'informations sur la création des keystores LOCAL ou OKM, reportez-vous aux sections suivantes :

- ["Configuration du chiffrement par le keystore LOCAL \(BUI\)" à la page 565](#) ou ["Configuration du chiffrement par le keystore LOCAL \(CLI\)" à la page 567](#)
- ["Configuration du chiffrement par le keystore OKM \(BUI\)" à la page 568](#) ou ["Configuration du chiffrement par le keystore OKM \(CLI\)" à la page 569](#)

2. Créez des clés de chiffrement LOCAL ou OKM.

Pour plus d'informations sur la création de clés LOCAL ou OKM, reportez-vous aux sections suivantes :

- ["Configuration du chiffrement par le keystore LOCAL \(BUI\)" à la page 565](#) ou ["Configuration du chiffrement par le keystore LOCAL \(CLI\)" à la page 567](#)
- ["Configuration du chiffrement par le keystore OKM \(BUI\)" à la page 568](#) ou ["Configuration du chiffrement par le keystore OKM \(CLI\)" à la page 569](#)

3. (Facultatif) Créez un projet à l'aide de l'une des clés de chiffrement LOCAL ou OKM.

Pour plus d'informations sur la création d'un projet, reportez-vous à la section ["Création d'un projet \(BUI\)" à la page 344](#).

4. Créez un partage dans un projet utilisant une clé de chiffrement ou créez un partage à l'aide de l'une des clés de chiffrement LOCAL ou OKM.

Pour plus d'informations sur la création d'un partage, reportez-vous à la section ["Partages et projets" à la page 343](#) ou ["Création d'un projet chiffré \(CLI\)" à la page 571](#).

Rubriques connexes

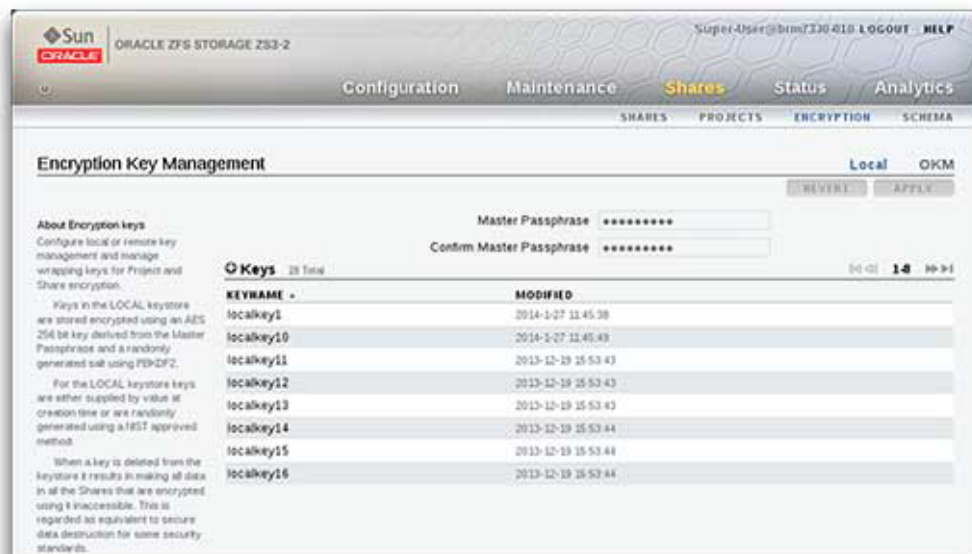
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Impact du chiffrement sur les performances" à la page 587](#)
- ["Cycle de vie d'une clé de chiffrement" à la page 588](#)
- ["Sauvegarde et restauration de données chiffrées" à la page 588](#)

▼ Configuration du chiffrement par le keystore LOCAL (BUI)

Pour configurer le chiffrement à l'aide du keystore LOCAL, configurez premièrement la phrase secrète principale, puis créez des clés à affecter à des partages chiffrés. Pour plus d'informations sur les propriétés de chiffrement, reportez-vous à ["Propriétés de cryptage" à la page 584](#).

Pour créer une clé, indiquez le nom à utiliser pour l'affectation des clés à des projets ou partages. Vous pouvez choisir de laisser le système générer la valeur de la clé ou fournir vous-même la clé raw 256 bits encodée en hexadécimal. Les clés sont stockées sous une forme chiffrée.

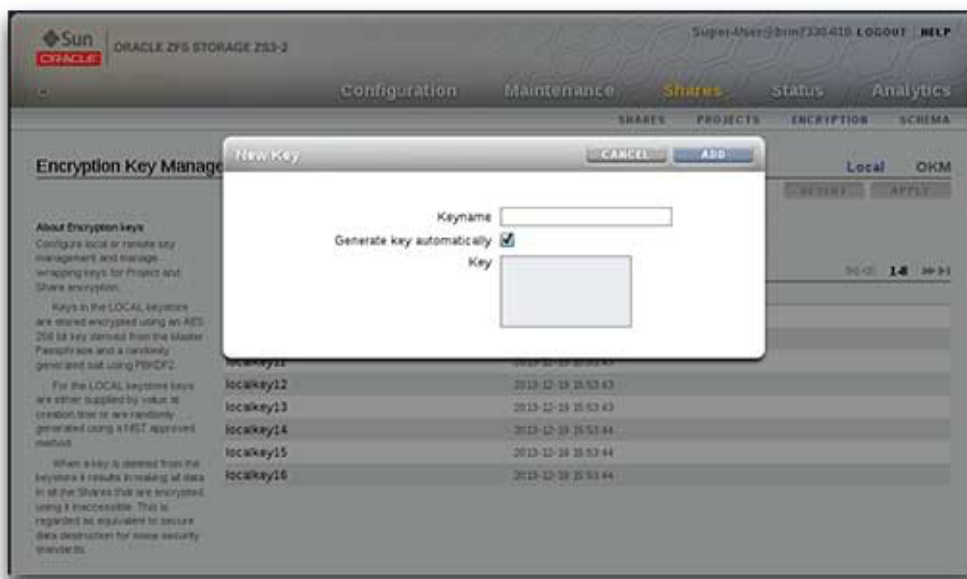
1. **Pour configurer le keystore LOCAL, accédez à la page de la BUI Partages > Chiffrement.**
2. **Cliquez sur Local.**
Les informations du keystore LOCAL s'affichent.



3. **Pour configurer la phrase secrète principale, saisissez la phrase secrète fournie par votre administrateur, puis confirmez-la dans la zone suivante.**
4. **Cliquez sur Appliquer pour enregistrer la phrase secrète principale, ou sur Précédent pour les annuler.**

5. **Pour créer une clé, cliquez sur l'icône Ajouter un élément .**

La boîte de dialogue Nouvel utilisateur s'ouvre.



6. **Saisissez un nom pour la clé.**
7. **Pour utiliser une clé raw 256 bits encodée en hexadécimal, désélectionnez la case "Générer la clé automatiquement", puis saisissez la clé.**
8. **Cliquez sur Ajouter pour enregistrer la clé, ou sur Annuler pour annuler les modifications.**

Si vous cliquez sur Ajouter, la nouvelle clé apparaît dans la liste des clés, ainsi que sa date de création.

Rubriques connexes

- ["Configuration du chiffrement par le keystore LOCAL \(CLI\)" à la page 567](#)
- ["Configuration du chiffrement par le keystore OKM \(BUI\)" à la page 568](#)
- ["Création d'un système de fichiers ou d'un LUN dans un projet \(BUI\)" à la page 350](#)

▼ Configuration du chiffrement par le keystore LOCAL (CLI)

Cette procédure présuppose que le chiffrement n'a pas déjà été configuré sur l'appareil. Pour plus d'informations sur les propriétés de chiffrement, reportez-vous à ["Propriétés de cryptage" à la page 584](#).

1. **Pour configurer la phrase secrète principale, utilisez les commandes CLI suivantes :**

```
hostname:> shares encryption
hostname:shares encryption> show
Children:
    okm => Manage encryption keys
    local => Manage encryption keys

hostname:shares encryption> local
hostname:shares encryption local> show
Properties:
    master_passphrase =

Children:
    keys => Manage this Keystore's Keys

hostname:shares encryption local> set master_passphrase
Enter new master_passphrase:
Re-enter new master_passphrase:
    master_passphrase = *****
```

2. **Pour créer la première clé, utilisez les commandes CLI suivantes et tapez un nom de clé.**

Il s'agit du nom utilisé dans la CLI et la BUI lors de l'affectation d'une clé à un projet ou un partage. Vous pouvez soit laisser la propriété de clé vide et le système générera une valeur de clé aléatoire, soit entrer une valeur de clé raw 256 bits encodée en hexadécimal.

Remarque - Les clés sont stockées sous une forme chiffrée utilisant la phrase secrète principale fournie. Dans l'exemple présent, le système génère la valeur de la clé.

```
hostname:shares encryption local> keys create
hostname:shares encryption local key (uncommitted)> show
Properties:
    cipher = AES
    key =
    keyname = (unset)
hostname:shares encryption local key (uncommitted)> set keyname=MyFirstKey
    keyname = MyFirstKey (uncommitted)
hostname:shares encryption local key (uncommitted)> commit
```

Rubriques connexes

- "Configuration du chiffrement par le keystore LOCAL (BUI)" à la page 565
- "Configuration du chiffrement par le keystore OKM (CLI)" à la page 569
- "Création d'un projet chiffré (CLI)" à la page 571

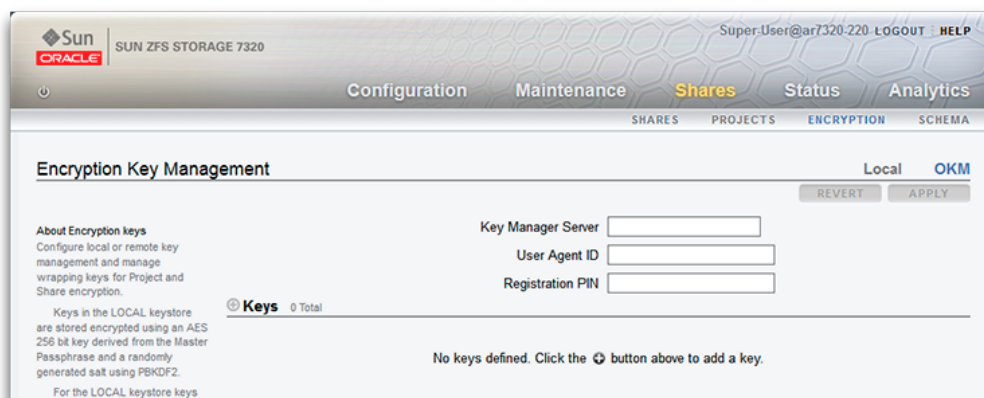
▼ Configuration du chiffrement par le keystore OKM (BUI)

Pour configurer le chiffrement à l'aide d'Oracle Key Manager (OKM), configurez premièrement les informations du serveur de gestion des clés, puis créez des clés à affecter à des partages chiffrés. Pour plus d'informations sur les propriétés de chiffrement, reportez-vous à "[Propriétés de cryptage](#)" à la page 584.

Remarque - Si l'appareil est clustérisé, n'utilisez pas le paramètre "phrase de passe unique" lorsque vous créez l'agent du serveur OKM. Sinon, l'enregistrement sur l'autre noeud de cluster échouera et les clés ne seront pas disponibles lors du basculement.

Pour créer une clé, indiquez le nom à utiliser pour l'affectation des clés à des projets ou partages.

1. **Pour configurer le keystore OKM, accédez à la page de la BUI Partages > Chiffrement.**
2. **Cliquez sur OKM.**
Les informations relatives au keystore OKM s'affichent.



3. **Pour configurer les informations du serveur, saisissez les informations suivantes :**

- Serveur de gestion des clés
 - ID d'agent utilisateur
 - PIN d'enregistrement
4. Cliquez sur **Appliquer pour enregistrer les informations du serveur, ou sur Annuler pour annuler les modifications.**
 5. Pour créer une clé, cliquez sur l'icône **Ajouter un élément** .
La boîte de dialogue Nouvel utilisateur s'ouvre.
 6. Saisissez un nom pour la clé.
 7. Cliquez sur **Ajouter pour enregistrer la clé, ou sur Annuler pour annuler les modifications.**
Si vous cliquez sur Ajouter, la nouvelle clé apparaît dans la liste des clés, ainsi que sa date de création.

Rubriques connexes

- ["Configuration du chiffrement par le keystore LOCAL \(BUI\)" à la page 565](#)
- ["Configuration du chiffrement par le keystore OKM \(CLI\)" à la page 569](#)
- ["Création d'un système de fichiers ou d'un LUN dans un projet \(BUI\)" à la page 350](#)

▼ Configuration du chiffrement par le keystore OKM (CLI)

Pour utiliser le keystore OKM (Oracle Key Manager), configurez les paramètres suivants :

- agent_id
- registration_pin (fourni par votre responsable de sécurité OKM)
- server_addr

Pour plus d'informations sur les propriétés de chiffrement, reportez-vous à ["Propriétés de cryptage" à la page 584](#).

Remarque - Si l'appareil est clustérisé, n'utilisez pas le paramètre "phrase de passe unique" lorsque vous créez l'agent du serveur OKM. Sinon, l'enregistrement sur l'autre noeud de cluster échouera et les clés ne seront pas disponibles lors du basculement.

1. Pour configurer le chiffrement par le keystore OKM, utilisez les commandes CLI suivantes :

```
hostname:> shares encryption
hostname:shares encryption> show
```

```

Children:
    okm => Manage encryption keys
    local => Manage encryption keys

hostname:shares encryption> okm
hostname:shares encryption okm> show
Properties:
    agent_id = ExternalClient041
    registration_pin = *****
    server_addr = 10.80.180.109

Children:
    keys => Manage this Keystore's Keys

```

2. Pour créer une clé OKM, utilisez les commandes CLI suivantes :

```

hostname:shares (pool-290-A) encryption okm keys>
hostname:shares (pool-290-A) encryption okm keys> create
hostname:shares (pool-290-A) encryption okm key-372 (uncommitted)> ls
Properties:
    cipher = AES
    keyname = (unset)
hostname:shares (pool-290-A) encryption okm key-372 (uncommitted)> set
keyname=anykey
    keyname = anykey (uncommitted)
hostname:shares (pool-290-A) encryption okm key-372 (uncommitted)> commit

```

▼ Création d'un projet chiffré (BUI)

Les partages (systèmes de fichiers et LUN) peuvent être chiffrés individuellement ou au niveau projet car ils héritent des propriétés de projet. L'exemple suivant indique comment chiffrer tous les partages au sein d'un projet en chiffrant le projet lui-même.

Avant de commencer

Pour utiliser le chiffrement, vous devez d'abord le configurer. Reportez-vous à la section ["Chiffrement de données" à la page 563](#).

1. **Accédez à Partages > Projets.**
2. **Cliquez sur l'icône d'ajout .**
3. **Affectez un nom au projet.**
4. **Définissez une longueur de clé de chiffrement.**
5. **Sélectionnez LOCAL ou OKM pour le keystore.**
6. **Sélectionnez un nom de clé.**
7. **Enregistrez le projet.**

Rubriques connexes

- ["Propriétés de cryptage" à la page 584](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Modification d'une clé de chiffrement de projet \(BUI\)" à la page 572](#)

▼ Création d'un projet chiffré (CLI)

Les partages (systèmes de fichiers et LUN) peuvent être chiffrés individuellement ou au niveau projet car ils héritent des propriétés de projet. L'exemple suivant indique comment chiffrer tous les partages au sein d'un projet en chiffrant le projet lui-même.

Avant de commencer

Pour utiliser le chiffrement, vous devez d'abord le configurer. Reportez-vous à la section ["Chiffrement de données" à la page 563](#).

1. Pour créer un projet chiffré, utilisez les commandes CLI suivantes :

```
hostname:shares> project myproject
hostname:shares myproject (uncommitted)> set encryption=aes-128-ccm
      encryption = aes-128-ccm (uncommitted)
hostname:shares myproject (uncommitted)> set keystore=LOCAL
      keystore = LOCAL (uncommitted)
hostname:shares myproject (uncommitted)> set keyname=MyFirstKey
      keyname = MyFirstKey (uncommitted)
hostname:shares myproject (uncommitted)> commit
hostname:shares>
```

Tous les partages créés sous ce projet sont automatiquement chiffrés en AES-128 CCM à l'aide de la clé appelée "MaPremièreClé" du keystore LOCAL.

2. Pour créer un système de fichiers dans le nouveau projet et voir les propriétés de chiffrement héritées, utilisez les commandes CLI suivantes :

```
hostname:shares> select myproject
hostname:shares myproject> filesystem f1
hostname:shares myproject/f1 (uncommitted)> commit
hostname:shares myproject> select f1
hostname:shares myproject/f1> get encryption keystore keyname keystatus
      encryption = aes-128-ccm (inherited)
      keystore = LOCAL (inherited)
      keyname = MyFirstKey (inherited)
      keystatus = available
hostname:shares myproject/f1> done
```

Rubriques connexes

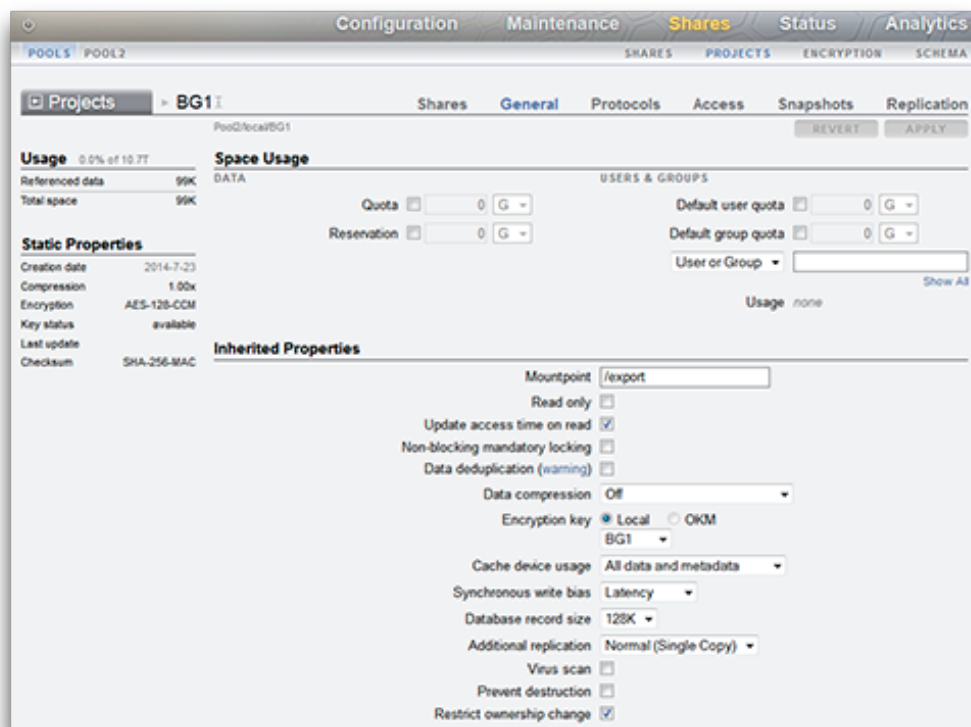
- ["Propriétés de cryptage" à la page 584](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Modification d'une clé de chiffrement de partage \(CLI\)" à la page 577](#)

▼ Modification d'une clé de chiffrement de projet (BUI)

La modification de la clé de chiffrement d'un projet entraîne la modification de la clé pour les partages qui héritent de la clé du projet. Vous pouvez modifier la clé de chiffrement associée à un partage à tout moment, même en cours d'utilisation par des systèmes client. Pour modifier la clé d'un projet, procédez comme suit :

1. Pour afficher le projet que vous souhaitez modifier, accédez à **Partages > Projets**.
2. Pour trouver le partage souhaité, cliquez sur **Tout afficher**, **Local** ou **Réplique**.
3. Déplacez le curseur sur le projet que vous souhaitez modifier et cliquez sur l'icône de modification .
4. Cliquez sur **Général**.

Les paramètres du projet s'affichent.



5. **Pour modifier la clé de chiffrement du projet, sélectionnez Local ou OKM, puis sélectionnez la clé à utiliser.**
6. **Cliquez sur Appliquer pour enregistrer les modifications, ou sur Précédent pour les annuler. Si vous cliquez sur Appliquer, les modifications sont enregistrées et la nouvelle clé apparaît dans la zone Clé de chiffrement.**

Rubriques connexes

- ["Modification de la clé de chiffrement d'un projet \(CLI\)" à la page 573](#)
- ["Suppression d'une clé de chiffrement \(BUI\)" à la page 579](#)
- ["Propriétés de cryptage" à la page 584](#)

▼ Modification de la clé de chiffrement d'un projet (CLI)

La modification de la clé de chiffrement d'un projet entraîne la modification de la clé pour les partages qui héritent de la clé du projet. Vous pouvez modifier la clé de chiffrement associée à un partage à tout moment, même en cours d'utilisation par des systèmes client. Pour modifier la clé d'un projet, procédez comme suit :

1. **Pour voir la clé en cours d'un projet, naviguez jusqu'à ce projet et saisissez `get keyname`.**

```
hostname:shares> select default
hostname:shares default> get keyname
                        keyname = MyFirstKey
```

2. **Pour modifier la clé utilisée pour le projet et tous les partages associés, saisissez `set keyname=` suivi du nouveau nom de clé, puis entrez `commit`.**

```
hostname:shares default> set keyname=MySecondKey
                        keyname = MySecondKey (uncommitted)
hostname: shares default> commit.
```

3. **Pour vérifier la nouvelle clé de projet, saisissez `get keyname`.**

```
shares default> get keyname
                        keyname = MySecondKey
```

Rubriques connexes

- ["Modification d'une clé de chiffrement de projet \(BUI\)" à la page 572](#)
- ["Modification d'une clé de chiffrement de partage \(CLI\)" à la page 577](#)
- ["Suppression d'une clé de chiffrement \(CLI\)" à la page 581](#)
- ["Propriétés de cryptage" à la page 584](#)

▼ Création d'un système de fichiers ou d'un LUN chiffré (BUI)

Les partages (systèmes de fichiers et LUN) peuvent être chiffrés individuellement ou au niveau projet car ils héritent des propriétés de projet. Si le projet est chiffré, le système de fichiers ou le LUN créé en son sein est aussi chiffré. Pour créer un système de fichiers ou un LUN chiffré individuel au sein d'un projet chiffré, appliquez la procédure suivante.

Avant de commencer

Pour utiliser le chiffrement, vous devez d'abord configurer un keystore et des clés. Reportez-vous à la section ["Chiffrement de données"](#) à la page 563.

1. **Accédez à Partages > Partages.**
2. **Sélectionnez Systèmes de fichiers ou LUN.**
3. **Cliquez sur l'icône d'ajout .**
4. **Renseignez les champs de la boîte de dialogue Créer un système de fichiers ou Créer un LUN.**
 - Pour un système de fichiers, sélectionnez un projet et entrez un nom.
 - Pour un LUN, sélectionnez un projet, entrez un nom et spécifiez la taille du volume.
 - Pour activer le chiffrement, sélectionnez Activé.

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux _ - . : sont autorisés.
5. **Cliquez sur APPLIQUER.**

Rubriques connexes

- ["Propriétés de cryptage" à la page 584](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Modification d'une clé de chiffrement de partage \(BUI\)" à la page 576](#)

▼ Création d'un système de fichiers ou d'un LUN chiffré (CLI)

Les partages (systèmes de fichiers et LUN) peuvent être chiffrés individuellement ou au niveau projet car ils héritent des propriétés de projet. Si le projet est chiffré, le système de fichiers ou le LUN créé en son sein est aussi chiffré. Pour créer un système de fichiers ou un LUN chiffré individuel se trouvant dans un projet chiffré, appliquez la procédure suivante.

Avant de commencer Pour utiliser le chiffrement, vous devez d'abord le configurer. Reportez-vous à la section ["Chiffrement de données" à la page 563](#).

1. Accédez à shares.

```
hostname:> shares
```

2. Entrez select et le nom de projet.

Dans cet exemple, le projet default est sélectionné.

```
hostname:shares > select default
```

3. Entrez filesystem et le nom d'un système de fichiers, ou lun et le nom d'un LUN.

Un nom doit comprendre de 1 à 64 caractères, mais ne doit pas inclure d'espaces ni commencer par un point. Les caractères alphanumériques et spéciaux `_ - . :` sont autorisés.

L'exemple suivant crée un système de fichiers nommé `fs-1` dans le projet default.

```
hostname:shares default> filesystem fs-1
hostname:shares default/fs-1 (uncommitted)>
```

4. Si vous créez un LUN, entrez set volsize= et la taille du volume.

```
hostname:shares default/lun1 (uncommitted)> set volsize=2G
volsize = 2G (uncommitted)
```

5. Pour activer le chiffrement, entrez set encryption= et le type de chiffrement.

```
hostname:shares default/fs-1 (uncommitted)> set encryption=aes-128-ccm
encryption = aes-128-ccm (uncommitted)
```

6. Configurez le chiffrement à l'aide du keystore LOCAL ou du keystore OKM (Oracle Key Manager). Entrez set keystore= et soit LOCAL, soit OKM.

```
hostname:shares default/fs-1 (uncommitted)> set keystore=LOCAL
keystore = LOCAL (uncommitted)
```

7. Pour définir la clé de chiffrement, entrez set keyname= et le nom de la clé.

```
hostname:shares default/fs-1 (uncommitted)> set keyname=MyFirstKey
keyname = MyFirstKey (uncommitted)
```

8. Saisissez commit.

```
hostname:shares default/fs-1 (uncommitted)> commit
```

Rubriques connexes

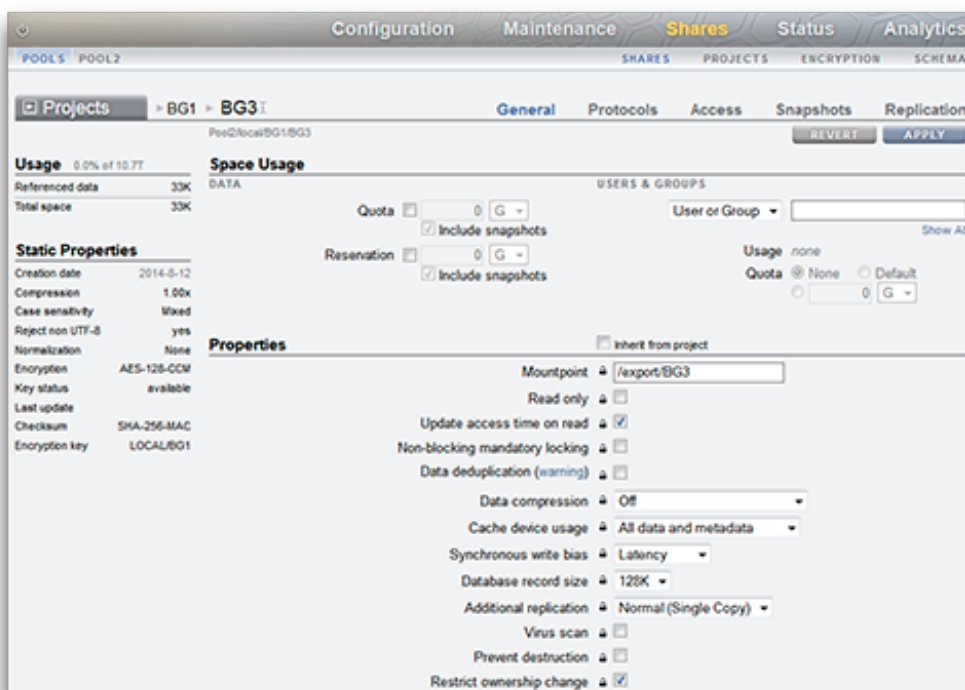
- ["Propriétés de cryptage" à la page 584](#)

- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Modification d'une clé de chiffrement de partage \(CLI\)" à la page 577](#)

▼ Modification d'une clé de chiffrement de partage (BUI)

Vous pouvez modifier la clé de chiffrement associée à un partage à tout moment, même en cours d'utilisation par des systèmes client. Pour modifier la clé d'un partage sans modifier le projet parent, procédez comme suit :

1. Pour afficher les propriétés du partage que vous souhaitez modifier, accédez à **Partages > Partages**.
2. Sélectionnez **Systèmes de fichiers ou LUN**.
3. Pour trouver le partage souhaité, cliquez sur **Tout afficher**, **Local** ou **Réplique**.
4. Déplacez le curseur sur le partage que vous souhaitez modifier et cliquez sur l'icône de modification . Les propriétés de partage s'affichent.



5. Si nécessaire, désactivez l'option Hériter du projet.
6. Pour modifier la clé de chiffrement, sélectionnez Local ou OKM, puis sélectionnez la clé à utiliser.
7. Cliquez sur Appliquer pour enregistrer les modifications, ou sur Précédent pour les annuler. Si vous cliquez sur Appliquer, les modifications sont enregistrées et la nouvelle clé apparaît dans la zone Clé de chiffrement.

Rubriques connexes

- ["Modification d'une clé de chiffrement de projet \(BUI\)" à la page 572](#)
- ["Suppression d'une clé de chiffrement \(BUI\)" à la page 579](#)
- ["Propriétés de cryptage" à la page 584](#)

▼ Modification d'une clé de chiffrement de partage (CLI)

Vous pouvez modifier la clé de chiffrement associée à un partage à tout moment, même en cours d'utilisation par des systèmes client. Pour modifier la clé d'un partage sans modifier le projet parent, procédez comme suit :

1. Pour voir la clé en cours d'un partage, naviguez jusqu'à ce système de fichiers ou ce LUN et saisissez `get keyname`.

```
hostname:shares default> select fs-1
hostname:shares default/fs-1> get keyname
keyname = MyFirstKey
```

2. Pour modifier la clé utilisée pour le partage, saisissez `set keyname=` suivi du nouveau nom de clé, puis entrez `commit`.

```
hostname:shares default/fs-1> set keyname=MySecondKey
keyname = MySecondKey (uncommitted)
hostname: shares default/fs-1> commit.
```

3. Pour vérifier la nouvelle clé de partage, saisissez `get keyname`.

```
shares default/fs-1> get keyname
keyname = MySecondKey
```

Rubriques connexes

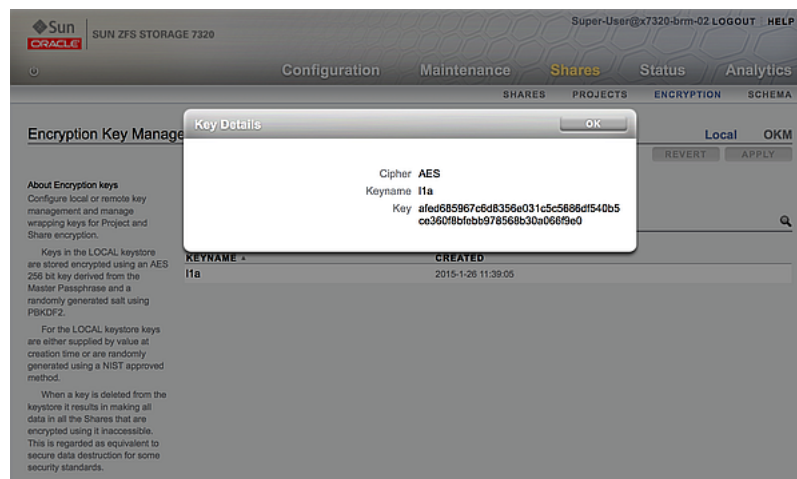
- ["Modification de la clé de chiffrement d'un projet \(CLI\)" à la page 573](#)
- ["Suppression d'une clé de chiffrement \(CLI\)" à la page 581](#)
- ["Propriétés de cryptage" à la page 584](#)

▼ Sauvegarde d'une clé locale (BUI)

Procédez comme suit pour récupérer les informations relatives à une clé LOCAL afin de sauvegarder la clé.

1. **Accédez à Partages > Chiffrement > Local.**
2. **Cliquez sur la clé à sauvegarder.**

Une boîte de dialogue comportant le nom et la valeur de la clé s'affiche.



3. **A l'aide d'une méthode quelconque, enregistrez ces informations dans un emplacement de sauvegarde de votre choix puis cliquez sur OK.**

▼ Sauvegarde d'une clé locale (CLI)

Procédez comme suit pour récupérer les informations relatives à une clé LOCAL afin de sauvegarder la clé.

1. **Sélectionnez la clé :**

```
hostname:shares encryption local keys> select keyname=Mykey
```

2. **Obtenez la valeur de la clé :**

```
hostname:shares encryption local key-005> get key
key = d6a5b801ffb93fcb19ef70a11d662d8092f243c5d4ccd0cd34264b15dd0b7739
```

3. **A l'aide d'une méthode quelconque, enregistrez ces informations dans un emplacement de sauvegarde de votre choix.**

▼ Suppression d'une clé de chiffrement (BUI)

La suppression d'une clé de chiffrement est un moyen rapide et efficace de rendre une grande quantité de données inaccessibles. Les clés peuvent être supprimées même lorsqu'elles sont en cours d'utilisation. Si la clé à supprimer est en cours d'utilisation, un avertissement s'affiche et la confirmation est requise. Tous les partages ou projets utilisant la clé sont annulés et les clients en perdent l'accès.

Si vous devez utiliser à nouveau une clé LOCAL pour accéder aux partages qui lui sont associés, sauvegardez le nom et la valeur de la clé avant de la supprimer. Vous pourrez ultérieurement effectuer une procédure de restauration comme décrit dans la section ["Restauration d'une clé LOCAL \(BUI\)" à la page 582](#).

Utilisez la procédure suivante pour supprimer une clé de chiffrement LOCAL ou OKM.

1. **Accédez à Partages > Chiffrement.**
2. **Sélectionnez Local ou OKM.**
3. **Placez le curseur sur la clé à supprimer et cliquez sur l'icône de suppression .**

L'alerte suivante s'affiche :



4. Cliquez sur OK pour supprimer la clé, ou sur Annuler pour la conserver.

Lorsqu'une clé est supprimée, toutes les données de tous les partages qui l'utilisent deviennent inaccessibles. Cette opération équivaut à une destruction sécurisée des données. Elle est définitive et irréversible, sauf si vous avez préparé la restauration de la clé en la sauvegardant. Pour plus d'informations sur la sauvegarde et la restauration de la clé, reportez-vous aux sections "[Sauvegarde d'une clé locale \(BUI\)](#)" à la page 578 et "[Restauration d'une clé LOCAL \(BUI\)](#)" à la page 582.

Rubriques connexes

- "[Modification d'une clé de chiffrement de partage \(BUI\)](#)" à la page 576
- "[Suppression d'une clé de chiffrement \(CLI\)](#)" à la page 581

- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Cycle de vie d'une clé de chiffrement" à la page 588](#)

▼ Suppression d'une clé de chiffrement (CLI)

La suppression d'une clé de chiffrement est un moyen rapide et efficace de rendre une grande quantité de données inaccessibles. Les clés peuvent être supprimées même lorsqu'elles sont en cours d'utilisation. Si la clé à supprimer est en cours d'utilisation, un avertissement s'affiche et la confirmation est requise. Tous les partages ou projets utilisant la clé sont annulés et les clients en perdent l'accès.

Si vous devez utiliser à nouveau une clé LOCAL pour accéder aux partages qui lui sont associés, sauvegardez le nom et la valeur de la clé avant de la supprimer. Vous pourrez ultérieurement effectuer une procédure de restauration comme décrit dans la section ["Restauration d'une clé LOCAL \(CLI\)" à la page 583](#).

Utilisez la procédure suivante pour supprimer une clé de chiffrement LOCAL ou OKM.

1. Pour supprimer une clé, utilisez la commande CLI suivante :

```
hostname:shares encryption local local_keys> destroy keyname=AKTEST_K1
```

This key has the following dependent shares:

```
Pool2/local/BG1
Pool2/local/BG1/BG3
Pool2/local/BG1/fast1
Pool2/local/default/BG2
```

Destroying this key will render the data inaccessible. Are you sure? (Y/N)

2. Pour vérifier qu'un partage n'est plus accessible par cette clé, accédez au partage et utilisez les commandes CLI suivantes :

```
hostname:> shares select test_project select test_share1
hostname:shares test_project/test_share1> get encryption keystore keyname keystatus
```

```
encryption = aes-128-ccm (inherited)
keystore = LOCAL (inherited)
keyname = AKTEST_K1 (inherited)
keystatus = unavailable
```

Errors:

```
key_unavailable
```

3. Pour répertorier les dépendants, utilisez les commandes CLI suivantes :

```
hostname:shares (pool-010) encryption local keys> select keyname=1 hostname:shares
(pool-010) encryption local key-002> list
```

Properties:

```

cipher = AES
keyname = 1

```

```

hostname:shares (pool-010) encryption local key-002> list dependents DEPENDENTS
pool-010/local/default/a hostname:shares (pool-010) encryption local key-002>

```

Rubriques connexes

- ["Modification d'une clé de chiffrement de partage \(CLI\)" à la page 577](#)
- ["Sauvegarde d'une clé locale \(CLI\)" à la page 578](#)
- ["Restauration d'une clé LOCAL \(CLI\)" à la page 583](#)

▼ Restauration d'une clé LOCAL (BUI)

Pour restaurer une clé LOCAL supprimée, créez une clé LOCAL portant le même nom et possédant la même valeur que la clé précédemment supprimée. Avant la suppression de la clé, vous deviez avoir tout d'abord enregistré ou sauvegardé ces informations. La procédure de sauvegarde est décrite à la section ["Sauvegarde d'une clé locale \(BUI\)" à la page 578](#). Bien que la suppression d'une clé LOCAL rende les partages inaccessibles, vous pouvez à nouveau accéder à ces derniers en recréant la clé LOCAL.

Pour plus d'informations sur la restauration de clés stockées dans le keystore OKM, reportez-vous à la documentation d'Oracle Key Manager sur [Oracle Technology Network \(http://www.oracle.com/technetwork/indexes/documentation/index.html\)](http://www.oracle.com/technetwork/indexes/documentation/index.html).

Procédez comme suit pour restaurer une clé LOCAL sauvegardée.

Remarque - Si le nom de la clé est déjà utilisé avec une autre valeur de clé pour des partages existants, modifiez la clé des partages concernés avant de restaurer la clé LOCAL d'origine. Pour plus d'informations, reportez-vous à la section ["Modification d'une clé de chiffrement de partage \(BUI\)" à la page 576](#).

1. **Récupérez le nom et la valeur de la clé LOCAL à partir de votre emplacement de sauvegarde.**
2. **Accédez à Partages > Chiffrement > Local et cliquez sur l'icône Ajouter.**
3. **Saisissez le même nom de clé que celui de la sauvegarde.**
4. **Décochez l'option "Générer la clé automatiquement" et définissez la valeur de la clé en fonction de la sauvegarde.**
5. **Enregistrez la clé restaurée en cliquant sur AJOUTER.**
Si le nom de la clé est utilisé avec des partages existants, une boîte de dialogue s'affiche. Pour écraser la valeur de la clé dans les partages existants, cliquez sur OK. Cliquez sur Annuler pour

ne pas ajouter la nouvelle clé. Vous pouvez ensuite modifier la clé utilisée pour ces partages avant de répéter la procédure et de restaurer la clé d'origine. Pour plus d'informations, reportez-vous à la section "[Modification d'une clé de chiffrement de partage \(BUI\)](#)" à la page 576.

Rubriques connexes

- "[Modification d'une clé de chiffrement de partage \(BUI\)](#)" à la page 576
- "[Sauvegarde d'une clé locale \(BUI\)](#)" à la page 578
- "[Suppression d'une clé de chiffrement \(BUI\)](#)" à la page 579

▼ Restauration d'une clé LOCAL (CLI)

Pour restaurer une clé LOCAL supprimée, créez une clé LOCAL portant le même nom et possédant la même valeur que la clé précédemment supprimée. Avant la suppression de la clé, vous deviez avoir tout d'abord enregistré ou sauvegardé ces informations. La procédure de sauvegarde est décrite à la section "[Sauvegarde d'une clé locale \(CLI\)](#)" à la page 578. Bien que la suppression d'une clé LOCAL rende les partages inaccessibles, vous pouvez à nouveau accéder à ces derniers en recréant la clé LOCAL.

Pour plus d'informations sur la restauration de clés stockées dans le keystore OKM, reportez-vous à la documentation d'Oracle Key Manager sur [Oracle Technology Network \(http://www.oracle.com/technetwork/indexes/documentation/index.html\)](http://www.oracle.com/technetwork/indexes/documentation/index.html).

Procédez comme suit pour restaurer une clé LOCAL sauvegardée.

Remarque - Si le nom de la clé est déjà utilisé avec une autre valeur de clé pour des partages existants, modifiez la clé des partages concernés avant de restaurer la clé LOCAL d'origine. Pour plus d'informations, reportez-vous à la section "[Modification d'une clé de chiffrement de partage \(CLI\)](#)" à la page 577.

1. **Récupérez le nom et la valeur de la clé LOCAL à partir de votre emplacement de sauvegarde.**

2. **Créez une clé dans le keystore LOCAL :**

```
hostname:shares encryption local keys> create
```

3. **Nommez la clé en fonction de la sauvegarde :**

```
hostname:shares encryption local key-005 (uncommitted)> set keyname=Mykey
keyname = Mykey (uncommitted)
```

4. **Définissez la clé en fonction de la sauvegarde :**

```
hostname:shares encryption local key-005 (uncommitted)> set
key=d6a5b801ffb93fcb19ef70a11d662d8092f243c5d4ccd0cd34264b15dd0b7739
```

```
key = d6a5b801ffb93fcb19ef70a11d662d8092f243c5d4ccd0cd34264b15dd0b7739 (uncommitted)
```

5. Enregistrez la clé :

```
hostname:shares encryption local key-005 (uncommitted)> commit
```

Si le nom de la clé est utilisé avec des partages existants, vous serez alerté :

Existing shares reference the key Mykey from the LOCAL keystore. Are you sure? (Y/N)

Pour écraser la valeur de la clé dans les partages existants, saisissez Y. Saisissez N pour ne pas ajouter la nouvelle clé. Vous pouvez ensuite modifier la clé utilisée pour ces partages avant de répéter la procédure et de restaurer la clé d'origine. Pour plus d'informations, reportez-vous à la section ["Modification d'une clé de chiffrement de partage \(CLI\)" à la page 577](#).

Rubriques connexes

- ["Modification d'une clé de chiffrement de partage \(CLI\)" à la page 577](#)
- ["Sauvegarde d'une clé locale \(CLI\)" à la page 578](#)
- ["Suppression d'une clé de chiffrement \(CLI\)" à la page 581](#)

Propriétés de cryptage

La liste suivante affiche les propriétés de chiffrement disponibles pour gérer les clés, créer les clés et créer des projets et des partages chiffrés.

- **Propriétés de gestion des clés LOCAL**
 - **Phrase secrète principale** : La phrase secrète principale est utilisée pour générer une clé AES afin de chiffrer les clés stockées dans le keystore LOCAL. L'algorithme PKCS#5 PBKDF est utilisé pour générer la clé et la clé est générée de manière aléatoire et gérée par le système.
- **Propriétés de création de clé LOCAL**
 - **Nom de clé** : Nom servant à identifier la clé.
 - **Générer la clé automatiquement** : Générer la clé automatiquement.
 - **Clé** : Clé raw 256 bits encodée en hexadécimal, stockée dans un format chiffré, si la génération de clé automatique n'est pas sélectionnée.
- **Propriétés de gestion des clés OKM** (fournies par votre administrateur OKM)
 - **Serveur OKM** : Adresse IP de votre serveur OKM (Oracle Key Manager).
 - **ID d'agent utilisateur** : ID d'agent utilisateur.
 - **PIN d'enregistrement** : PIN d'enregistrement.
- **Propriétés de création de clé OKM**
 - **Nom de clé** : Nom servant à identifier la clé.
- **Propriétés de chiffrement de partages**

- **Chiffrement** : Type de chiffrement et longueur de clé AES (pour plus d'informations, reportez-vous à la section ["Présentation des valeurs de clés de chiffrement" à la page 586](#)).
- **Clé d'héritage** : Pour hériter de la clé de chiffrement du projet parent.
- **Clé** : Définit une clé LOCAL ou OKM et est utilisée quand la clé n'est pas héritée du projet parent.
- **Propriétés de chiffrement de projet**
 - **Nom** : Nom servant à identifier le projet.
 - **Chiffrement** : Type de chiffrement et longueur de clé AES (pour plus d'informations, reportez-vous à la section ["Présentation des valeurs de clés de chiffrement" à la page 586](#)).
 - **Clé** : Clé LOCAL ou OKM particulière.

Rubriques connexes

- ["Workflow de chiffrement de données" à la page 564](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Impact du chiffrement sur les performances" à la page 587](#)
- ["Cycle de vie d'une clé de chiffrement" à la page 588](#)

Gestion des clés de chiffrement

L'appareil inclut un keystore LOCAL intégré et présente la possibilité de se connecter au système OKM (Oracle Key Manager). Chaque projet ou partage chiffré nécessite une clé d'encapsulation provenant soit du keystore LOCAL, soit du keystore OKM. Les clés de chiffrement des données sont gérées par l'appareil de stockage, stockées de manière permanente et chiffrées par la clé d'encapsulation provenant du keystore LOCAL ou du keystore OKM.

Oracle Key Manager (OKM) est un système de gestion de clés (KMS) complet, conçu pour répondre aux besoins sans cesse croissants des entreprises en matière de chiffrement des données basé sur le stockage. Développé en conformité avec les normes de sécurité ouvertes, OKM fournit la capacité, l'évolutivité et l'interopérabilité nécessaires pour gérer de manière centrale les clés de chiffrement à travers des infrastructures de stockage largement distribuées et hétérogènes.

OKM répond aux défis uniques de la gestion des clés de stockage, notamment :

- **Conservation de clés à long terme** - OKM assure la disponibilité ininterrompue des données et conserve de manière sécurisée les clés de chiffrement pendant la totalité du cycle de vie des données.
- **Interopérabilité** : OKM fournit l'interopérabilité nécessaire à la prise en charge d'une gamme étendue de périphériques de stockage, qui peuvent être connectés à des mainframes ou des plates-formes de systèmes ouverts sous un service unique de gestion des clés de stockage.

- **Haute disponibilité** : fournit une haute disponibilité grâce au clustering actif à N noeuds, l'équilibrage dynamique de la charge et le basculement automatisé, que les appareils soient dans la même pièce ou répartis dans le monde entier.
- **Haute capacité** : OKM peut gérer un grand nombre de périphériques de stockage et plus encore de clés de stockage. Un appareil en cluster unique peut fournir des services de gestion des clés pour des milliers de périphériques de stockage et des millions de clés de stockage.
- **Configuration de clé flexible** : pour un cluster OKM, les clés peuvent être générées automatiquement ou individuellement pour un keystore LOCAL ou OKM. Les administrateurs de la sécurité sont chargés de fournir les noms de clés qui, combinés avec le keystore, associent une clé d'encapsulation données à un projet ou un partage.

Remarque - Si l'appareil est clustérisé, n'utilisez pas le paramètre "phrase de passe unique" lorsque vous créez l'agent du serveur OKM. Sinon, l'enregistrement sur l'autre noeud de cluster échouera et les clés ne seront pas disponibles lors du basculement.

Maintien des clés

Les partages et les projets qui utilisent des clés OKM à l'état désactivé demeurent accessibles. Pour empêcher l'utilisation d'une clé OKM, l'administrateur OKM doit explicitement supprimer la clé.

Pour vous assurer que les partages et les projets chiffrés sont accessibles, sauvegardez vos configurations d'appareil et vos valeurs de clés de keystore LOCAL. Si une ou plusieurs clés ne sont plus disponibles, les partages ou les projets utilisant ces clés ne sont plus accessibles. Si la clé d'un projet n'est pas disponible, de nouveaux partages ne peuvent pas être créés dans ce projet.

Les clés peuvent devenir indisponibles comme suit :

- Les clés sont supprimées
- Restauration d'une version ne prenant pas en charge le chiffrement
- Restauration d'une version où les clés ne sont pas configurées
- Réinitialisation des paramètres d'usine
- Le serveur OKM n'est pas disponible

Présentation des valeurs de clés de chiffrement

Le tableau suivant présente les valeurs et les descriptions des clés de chiffrement de la BUI et de la CLI. Il indique également si le type de chiffrement fonctionne avec la suppression des doublons.

TABLEAU 126 Valeurs de clés de chiffrement

Valeur BUI	Valeur CLI	Description
Désactivé	Désactivé	Le partage/le projet n'est pas chiffré
AES-128-CCM	aes-128-ccm	Chiffrement à impact très faible sur la CPU Suppr. des doublons poss.
AES-192-CCM	aes-192-ccm	Suppr. des doublons poss.
AES-256-CCM	aes-256-ccm	Suppr. des doublons poss.
AES-128-GCM	aes-128-gcm	NIST SP800-38D recommandé, suppr. des doublons impossible
AES-192-GCM	aes-192-gcm	NIST SP800-38D recommandé, suppr. des doublons impossible
AES-256-GCM	aes-256-gcm	Chiffrement à impact très élevé sur la CPU, NIST SP800-38D recommandé, suppr. des doublons impossible

Impact du chiffrement sur les performances

L'utilisation du chiffrement avec les partages peut avoir les impacts suivants sur les performances de la CPU :

- Le mode AES-128-CCM a l'impact le plus faible sur les performances de la CPU et il est recommandé pour toutes les charges de travail pour lesquelles il n'existe aucune exigence LOCAL en matière de sécurité.
- Lorsque les données chiffrées sont lues, elles sont stockées sous forme déchiffrée et décompressée dans le cache DRAM. Pour les charges de travail dominées par la lecture qui peuvent être conservées en tant que charges à lecture dominante depuis le cache DRAM, l'impact du déchiffrement des données est minimal.
- Lorsque des appareils de cache SSD sont utilisés, les blocs de données exclus de DRAM et placés dans le cache sont compressés et chiffrés et doivent être déchiffrés et décompressés lorsqu'ils sont récupérés par le DRAM.
- Pour les charges de travail qui sont à écriture dominante et qui utilisent des blocs de grande taille, particulièrement 128 kilo-octets et 1 méga-octet, l'impact sur la CPU peut être important et entraîner une capacité de traitement inférieure. C'est particulièrement probable si la taille d'enregistrement du système de fichiers ou la taille de bloc de volume LUN est supérieure à la taille de bloc de l'application.

Rubriques connexes

- ["Workflow de chiffrement de données" à la page 564](#)

- ["Propriétés de cryptage" à la page 584](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Cycle de vie d'une clé de chiffrement" à la page 588](#)

Cycle de vie d'une clé de chiffrement

Le cycle de vie d'une clé de chiffrement est flexible car vous pouvez changer de clé à tout moment sans déconnecter les services de données.

Lorsqu'une clé est supprimée du keystore, tous les partages qui l'utilisent sont démontés et les données qu'ils contiennent deviennent inaccessibles. La sauvegarde des clés dans le keystore OKM doit être effectuée à l'aide des services de sauvegarde d'OKM. La sauvegarde des clés dans le keystore LOCAL est incluse dans la sauvegarde de la configuration système. Pour le keystore LOCAL, il est également possible de fournir la valeur de la clé au moment de la création afin de permettre son stockage dans un système externe, offrant ainsi une solution de sauvegarde/restauration de clé alternative.

Rubriques connexes

- ["Workflow de chiffrement de données" à la page 564](#)
- ["Propriétés de cryptage" à la page 584](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Impact du chiffrement sur les performances" à la page 587](#)

Sauvegarde et restauration de données chiffrées

Lorsqu'une clé est restaurée à l'aide de la fonction de restauration ZFS, le partage restauré hérite des propriétés de chiffrement du projet cible si le partage d'origine a hérité de ses propriétés de chiffrement du projet source.

Pour vous assurer que les propriétés de chiffrement d'un partage d'origine sont conservées dans un partage restauré, configurez le chiffrement sur le partage d'origine au lieu de l'hériter de son projet.

Si vous voulez définir le chiffrement différemment pour un partage spécifique au sein d'un projet, configurez manuellement le chiffrement pour le partage source spécifique au lieu de laisser le partage hériter de ses propriétés du projet. Ceci garantit que tous les partages sont sauvegardés et restaurés avec les paramètres de chiffrements voulus.

Pour plus d'informations sur la sauvegarde NDMP, reportez-vous à la section ["Configuration NDMP" à la page 266](#). Pour plus d'informations sur la réplication, reportez-vous à la section ["Réplication distante" à la page 473](#).

Rubriques connexes

- ["Workflow de chiffrement de données" à la page 564](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Cycle de vie d'une clé de chiffrement" à la page 588](#)
- ["Réplication d'un partage chiffré" à la page 589](#)

Réplication d'un partage chiffré

Pour répliquer un partage chiffré, la cible comme la source doivent prendre en charge le chiffrement et se conformer à ces conditions :

- de la version logicielle 2013.1.3.0 ou ultérieure
- des clés d'encapsulation de chiffrement utilisé par le partage
- Le nom de clé OKM doit être identique dans le keystore à la fois sur la source de réplication et sur les appareils cibles.
- L'ID de l'agent OKM doit être unique sur la source de réplication et sur les appareils de réplication cibles. Les appareils pairs de réplication ne peuvent pas utiliser le même agent.
- Les agents OKM dédiés aux pairs de réplication doivent être configurés sur le serveur OKM pour afficher les mêmes groupes de clés. Dans ce cas, il n'est pas nécessaire de créer manuellement la clé OKM sur le système cible de réplication.

Si la cible ne prend pas en charge le chiffrement et que vous tentez de répliquer un partage chiffré, la réplication échouera. Si la clé d'encapsulation n'est pas disponible sur le système source ou cible, ou que le logiciel cible est antérieur à la version 2013.1.3.0, une alerte sera déclarée. Passez les alertes en revue sur les deux systèmes, source et cible, pour déterminer la cause de l'échec de la réplication.

Pour plus d'informations sur la réplication de configuration, reportez-vous à la section ["Réplication distante" à la page 473](#).

Rubriques connexes

- ["Workflow de chiffrement de données" à la page 564](#)
- ["Gestion des clés de chiffrement" à la page 585](#)
- ["Cycle de vie d'une clé de chiffrement" à la page 588](#)
- ["Sauvegarde et restauration de données chiffrées" à la page 588](#)
- Oracle ZFS Storage Appliance : note MOS sur la compatibilité de réplication distante [1958039.1]

Maintenance des workflows

Un workflow est un script CLI téléchargé et géré par l'appareil lui-même. L'utilisateur peut paramétrer et exécuter les workflows avec une grande efficacité depuis l'interface du navigateur ou l'interface de ligne de commande. Il est également possible d'exécuter les workflows sous forme d'actions d'alerte ou à des instants définis. Les workflows permettent une *extension* de l'appareil de manière à prendre en compte des stratégies ou procédures particulières, et peuvent servir, par exemple, à intégrer sous forme de code des pratiques d'excellence prescrites par des organisations ou applications particulières.

Pour utiliser les workflows, reportez-vous aux sections suivantes :

- [Présentation des workflows](#)
- [Présentation des paramètres de workflow](#)
- [Paramètres de workflow restreints](#)
- [Paramètres de workflow facultatifs](#)
- [Gestion des erreurs des workflows](#)
- [Validation des entrées des workflows](#)
- [Audits et rapports sur l'exécution des workflows](#)
- [Présentation de la gestion des versions des workflows](#)
- [Utilisation des workflows pour les actions d'alerte](#)
- [Utilisation de workflows programmés](#)
- [Utilisation d'un workflow programmé](#)
- [Codage des calendriers de workflow](#)
- [Création d'une feuille de travail à partir d'un type de lecteur donné](#)
- [Téléchargement de workflows à l'aide de la BUI](#)
- [Téléchargement de workflows à l'aide de la CLI](#)
- [Création d'une liste de workflows à l'aide de la CLI](#)
- [Exécution de workflows à l'aide de la CLI](#)

Présentation des workflows

Un workflow est matérialisé par un fichier ECMAScript valide contenant une seule variable globale : `workflow`. Ce fichier constitue un objet qui doit contenir trois membres au minimum :

TABLEAU 127 Membres objets obligatoires

Membre obligatoire	Type	Description
name	String	Nom du workflow
description	String	Description du workflow
execute	Fonction	Fonction exécutant le workflow

EXEMPLE 18 Workflow Hello World

Voici un exemple de workflow basique :

```
var workflow = {
  name: 'Hello world',
  description: 'Bids a greeting to the world',
  execute: function () { return ('hello world!') }
};
```

Après téléchargement de ce workflow vers l'appareil, un nouveau workflow nommé "Hello world" est disponible. L'exécution de ce workflow génère la sortie "hello world!"

EXEMPLE 19 Utilisation de la fonction d'exécution de workflow pour obtenir la valeur d'utilisation CPU

Les workflows s'exécutent de manière asynchrone dans le shell de l'appareil ; par défaut, ils s'exécutent comme s'ils étaient eux-mêmes des utilisateurs exécutant des workflows. Les workflows disposent librement de l'utilitaire de script de l'appareil (voir la section ["Utilisation de l'écriture de scripts CLI" à la page 40](#)) et peuvent interagir avec l'appareil comme n'importe quelle autre instance de shell de l'appareil. En d'autres termes, les workflows peuvent exécuter des commandes, analyser des sorties, modifier des états, etc. L'exemple suivant, plus complexe, utilise la fonction run pour renvoyer l'utilisation actuelle de la CPU :

```
var workflow = {
  name: 'CPU utilization',
  description: 'Displays the current CPU utilization',
  execute: function () {
    run('analytics datasets select name=cpu.utilization');
    cpu = run('csv 1').split('\n')[1].split(',');
    return ('At ' + cpu[0] + ', utilization is ' + cpu[1] + '%');
  }
};
```

Présentation des paramètres de workflow

Les workflows qui n'agissent pas sur l'entrée ont une portée limitée ; un grand nombre de workflows doivent être paramétrés pour présenter une utilité. Pour ce faire, il faut ajouter un

membre `parameters` à l'objet `workflow` global. Le membre `parameters` est lui-même un objet comportant normalement un membre pour chaque paramètre. Chaque membre `parameters` doit avoir les membres suivants :

TABLEAU 128 Membres obligatoires des paramètres des workflows

Membre obligatoire	Type	Description
<code>label</code>	String	Etiquette associée à l'entrée du paramètre de workflow
<code>type</code>	String	Type du paramètre de workflow

Le membre `type` doit être défini sur l'un des types suivants :

TABLEAU 129 Noms des types de membres du workflow

Nom du type	Description
<code>Boolean</code>	Valeur booléenne
<code>ChooseOne</code>	Une valeur parmi plusieurs spécifiées
<code>EmailAddress</code>	Adresse électronique
<code>File</code>	Fichier destiné à être transféré à l'appareil
<code>Host</code>	Hôte valide, sous forme de nom ou de décimal avec points
<code>HostName</code>	Nom d'hôte valide
<code>HostPort</code>	Port valide disponible
<code>Integer</code>	Entier
<code>NetAddress</code>	Adresse réseau
<code>NodeName</code>	Nom de noeud réseau
<code>NonNegativeInteger</code>	Entier supérieur ou égal à zéro
<code>Number</code>	Nombre quelconque, notamment nombre à virgule flottante
<code>Password</code>	Mot de passe
<code>Permissions</code>	Autorisations POSIX
<code>Port</code>	Numéro de port
<code>Size</code>	Taille
<code>String</code>	Chaîne
<code>StringList</code>	Liste de chaînes

EXEMPLE 20 Workflow utilisant deux paramètres

Sur la base des types spécifiés, une forme d'entrée appropriée sera générée à l'exécution du workflow. L'exemple ci-dessous présente un workflow à deux paramètres, le nom d'une

division commerciale (à utiliser comme projet) et le nom d'un partage (à utiliser comme nom de partage) :

```
var workflow = {
  name: 'New share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
    unit: {
      label: 'Business unit',
      type: 'String'
    }
  },
  execute: function (params) {
    run('shares select ' + params.unit);
    run('filesystem ' + params.name);
    run('commit');
    return ('Created new share "' + params.name + '"');
  }
};
```

Si vous téléchargez ce workflow et que vous l'exécutez, une boîte de dialogue vous invitera à renseigner le nom du partage et celui de la division commerciale. Une fois que le partage aura été créé, vous en serez informé dans un message.

Paramètres de workflow restreints

Pour certains paramètres, il peut être opportun de limiter les entrées à un petit nombre de valeurs possibles plutôt que d'autoriser la saisie de valeurs quelconques. Ces paramètres doivent être définis comme des paramètres de type ChooseOne et un objet contenant des paramètres de ce type doit avoir deux membres supplémentaires :

TABLEAU 130 Membres obligatoires des paramètres restreints

Membre obligatoire	Type	Description
options	Tableau	Tableau de chaînes indiquant les options valides
optionlabels	Tableau	Tableau de chaînes indiquant les étiquettes associées aux options spécifiées dans options

EXEMPLE 21 Utilisation du paramètre de workflow ChooseOne

Le type de paramètre ChooseOne permet d'améliorer l'exemple précédent et de limiter la division commerciale à un petit nombre de valeurs possibles prédéfinies :

```

var workflow = {
  name: 'Create share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
    unit: {
      label: 'Business unit',
      type: 'ChooseOne',
      options: [ 'development', 'finance', 'qa', 'sales' ],
      optionlabels: [ 'Development', 'Finance',
        'Quality Assurance', 'Sales/Administrative' ],
    }
  },
  execute: function (params) {
    run('shares select ' + params.unit);
    run('filesystem ' + params.name);
    run('commit');
    return ('Created new share "' + params.name + '"');
  }
};

```

Lorsque ce workflow est exécuté, le paramètre `unit` n'est pas saisi à la main, mais il est sélectionné dans la liste d'options possibles indiquée.

Paramètres de workflow facultatifs

Certains paramètres peuvent être considérés comme *facultatifs*, c'est-à-dire que l'interface utilisateur ne subordonne pas l'exécution des workflows concernés à la saisie de valeurs pour ces paramètres. Un tel paramètre est identifié par le champ `optional` du membre `parameters` :

TABLEAU 131 Membres obligatoires des paramètres facultatifs

Membre facultatif	Type	Description
<code>optional</code>	Boolean	Lorsqu'il est réglé sur <code>true</code> , ce champ indique que la définition du paramètre n'est pas indispensable ; l'interface utilisateur peut autoriser l'exécution du script sans qu'une valeur ne soit spécifiée pour le paramètre.

Lorsqu'un paramètre est facultatif et n'est pas défini, son membre dans l'objet de paramètre, passé à la fonction `execute`, est réglé sur `undefined`.

Gestion des erreurs des workflows

Si une erreur se produit lors de l'exécution d'un workflow, une exception est levée. Si l'exception n'est pas interceptée par le workflow lui-même (ou si le workflow lève une exception non interceptée par ailleurs), le workflow échoue et les informations relatives à l'exception sont affichées à la vue de l'utilisateur. Pour permettre une gestion correcte des erreurs, les exceptions doivent être interceptées et traitées. Dans l'exemple qui précède par exemple, une tentative de créer un partage dans un projet inexistant se solde par une exception non interceptée.

EXEMPLE 22 Gestion des erreurs des workflows

Cet exemple peut être modifié de manière à intercepter l'erreur et à créer le projet, dans l'hypothèse où il n'existe pas :

```
var workflow = {
  name: 'Create share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
  },
  unit: {
    label: 'Business unit',
    type: 'ChooseOne',
    options: [ 'development', 'finance', 'qa', 'sales' ],
    optionlabels: [ 'Development', 'Finance',
      'Quality Assurance', 'Sales/Administrative' ],
  }
},
execute: function (params) {
  try {
    run('shares select ' + params.unit);
  } catch (err) {
    if (err.code != EAKSH_ENTITY_BADSELECT)
      throw (err);

    /*
     * We haven't yet created a project that corresponds to
     * this business unit; create it now.
     */
    run('shares project ' + params.unit);
    run('commit');
    run('shares select ' + params.unit);
  }

  run('filesystem ' + params.name);
  run('commit');
  return ('Created new share "' + params.name + '"');
}
```

```
};
```

Validation des entrées des workflows

De manière optionnelle, les workflows peuvent valider leurs entrées ; ceci s'effectue par l'ajout d'un membre `validate` qui accepte comme paramètre un objet contenant les paramètres du workflow en tant que membres. La fonction `validate` doit renvoyer un objet dans lequel chaque membre possède le nom du paramètre dont la validation a échoué, et chaque membre a pour valeur le message d'échec de validation affiché à la vue de l'utilisateur.

EXEMPLE 23 Validation des entrées des workflows

L'exemple ci-dessous développe l'exemple précédent et génère une erreur lorsque l'utilisateur tente de créer un partage existant :

```
var workflow = {
  name: 'Create share',
  description: 'Creates a new share in a business unit',
  parameters: {
    name: {
      label: 'Name of new share',
      type: 'String'
    },
    unit: {
      label: 'Business unit',
      type: 'ChooseOne',
      options: [ 'development', 'finance', 'qa', 'sales' ],
      optionlabels: [ 'Development', 'Finance',
        'Quality Assurance', 'Sales/Administrative' ],
    }
  },
  validate: function (params) {
    try {
      run('shares select ' + params.unit);
      run('select ' + params.name);
    } catch (err) {
      if (err.code == EAKSH_ENTITY_BADSELECT)
        return;
    }

    return ({ name: 'share already exists' });
  },
  execute: function (params) {
    try {
      run('shares select ' + params.unit);
    } catch (err) {
      if (err.code != EAKSH_ENTITY_BADSELECT)
        throw (err);
    }
  }
}
```

```

/*
 * We haven't yet created a project that corresponds to
 * this business unit; create it now.
 */
run('shares project ' + params.unit);
set('mountpoint', '/export/' + params.unit);
run('commit');
run('shares select ' + params.unit);
}

run('filesystem ' + params.name);
run('commit');
return ('Created new share "' + params.name + '"');
}
};

```

Audits et rapports sur l'exécution des workflows

Les workflows peuvent émettre des enregistrements d'audit en appelant la fonction `audit`. Le seul argument de la fonction `audit` est une chaîne qui doit être placée dans le journal d'audit.

Pour les workflows complexes à durée d'exécution prolongée, il peut être utile de fournir à l'utilisateur qui exécute le workflow des informations claires sur l'avancement. Pour permettre un tel signalement de l'avancement de l'exécution d'un workflow, il faut que le membre `execute` retourne une série *d'étapes*. Chaque élément de la série doit contenir les membres suivants :

TABLEAU 132 Membres obligatoires des rapports sur l'exécution

Membre obligatoire	Type	Description
<code>step</code>	String	Chaîne indiquant le nom de l'étape d'exécution
<code>execute</code>	Fonction	Fonction exécutant l'étape du workflow

Comme pour la fonction `execute` appliquée au workflow dans son ensemble, le membre `execute` de chaque étape accepte comme argument un objet contenant les paramètres du workflow.

EXEMPLE 24 Rapports sur l'exécution de workflows

L'exemple suivant illustre un workflow qui crée un nouveau projet, un nouveau partage et un nouvel enregistrement d'audit en trois étapes :

```

var steps = [ {
  step: 'Checking for associated project',
  execute: function (params) {
    try {

```

```

        run('shares select ' + params.unit);
    } catch (err) {
        if (err.code !== EAKSH_ENTITY_BADSELECT)
            throw (err);

        /*
         * We haven't yet created a project that corresponds to
         * this business unit; create it now.
         */
        run('shares project ' + params.unit);
        set('mountpoint', '/export/' + params.unit);
        run('commit');
        run('shares select ' + params.unit);
    }
}, {
    step: 'Creating share',
    execute: function (params) {
        run('filesystem ' + params.name);
        run('commit');
    }
}, {
    step: 'Creating audit record',
    execute: function (params) {
        audit('created "' + params.name + '" in "' + params.unit);
    }
}
];

var workflow = {
    name: 'Create share',
    description: 'Creates a new share in a business unit',
    parameters: {
        name: {
            label: 'Name of new share',
            type: 'String'
        },
    },
    unit: {
        label: 'Business unit',
        type: 'ChooseOne',
        options: [ 'development', 'finance', 'qa', 'sales' ],
        optionlabels: [ 'Development', 'Finance',
            'Quality Assurance', 'Sales/Administrative' ],
    },
},
validate: function (params) {
    try {
        run('shares select ' + params.unit);
        run('select ' + params.name);
    } catch (err) {
        if (err.code === EAKSH_ENTITY_BADSELECT)
            return;
    }
}

return ({ name: 'share already exists' });

```

```
},  
execute: function (params) { return (steps); }  
};
```

La fonction de messagerie permet aux workflows de livrer certains résultats par courrier électronique. Cette fonction doit inclure les arguments suivants : un objet sous la forme de commandes `to` et `subject` et une chaîne `messageBody` représentant le corps du message.

EXEMPLE 25 Exécution de workflows à l'aide d'une fonction de messagerie

```
var workflow = {  
  name: 'email controller state',  
  description: 'email controller state',  
  execute: function () {  
  
    // verify state of the controller  
    var faulted = run('maintenance hardware "chassis-000" get faulted');  
  
    var messageBody = faulted;  
  
    emailAddress = 'first.last@xyz.com';  
    subjectLine = 'Controller State';  
    mail({To: emailAddress, Subject: subjectLine}, messageBody);  
  
  }  
};
```

Présentation de la gestion des versions des workflows

La gestion de versions joue à deux niveaux en ce qui concerne les workflows : le premier niveau est l'expression de la version du logiciel de l'appareil duquel dépend le workflow, le second est l'expression de la version du workflow lui-même. La gestion des versions est exprimée via deux membres facultatifs du workflow :

TABLEAU 133 Membres facultatifs de la gestion des versions

Membre facultatif	Type	Description
required	String	Version minimale du logiciel de l'appareil requise pour exécuter le workflow concerné, y compris l'année, le mois, le jour, le build et la branche minimaux.
version	String	Version du workflow concerné, sous forme décimale (majeure.mineure.micro).

Versions de l'appareil : pour exprimer une version minimale requise du logiciel de l'appareil, ajoutez le champ facultatif `required` au workflow. La version de l'appareil est définie sur la base de l'année, du mois et du jour où le logiciel a été créé, suivi du numéro de build puis du numéro de branche, exprimé sous la forme "year.month.day.build-branch". Par exemple, "2009.04.10,12-0" correspond au douzième build du logiciel initialement créé le 10 avril 2009. Pour obtenir la version du logiciel du kit Oracle ZFS Storage Appliance, exécutez la commande CLI `configuration version get version` ou consultez le champ Version dans l'écran Système de la BUI. L'exemple ci-dessous illustre l'utilisation du champ `required` :

EXEMPLE 26 Utilisation du champ de workflow `required`

L'exemple ci-dessous illustre l'utilisation du champ `required` :

```
var workflow = {
  name: 'Configure FC',
  description: 'Configure fibre channel target groups',
  required: '2009.12.25,1-0',
  ...
}
```

Si un workflow requiert une version logicielle plus récente que la version chargée sur l'appareil, la tentative de télécharger le workflow échoue et un message expliquant la discordance s'affiche.

Versions des workflows : en plus de spécifier la version requise du logiciel de l'appareil, il est également possible de définir le numéro de version des workflows eux-mêmes à l'aide du champ `version`. Cette chaîne représente les numéros de version majeur, mineur et micro du workflow, ce qui permet à plusieurs versions d'un même workflow de coexister sur une machine. Lorsque vous téléchargez un workflow, les versions *compatibles*, *antérieures* du même workflow éventuellement présentes sur la machine sont supprimées. Un workflow est considéré comme *compatible* avec un autre workflow s'il a le même numéro de version majeur, et un workflow est considéré comme *antérieur* à un autre workflow s'il a un numéro de version inférieur. Par conséquent, le téléchargement d'un workflow de version "2.1" supprime le même workflow de version "2.0" (ou la version "2.0.1"), mais ne supprime pas un workflow identique de "1.2" ou "0.1".

Utilisation des workflows pour les actions d'alerte

Il est possible d'exécuter des workflows en tant qu'alertes. Pour permettre à un workflow de faire office d'action d'alerte, son action `alert` doit être définie sur `true`.

Lorsqu'ils sont exécutés en tant qu'actions d'alerte, les workflows prennent l'identité de l'utilisateur qui les a créés. C'est pourquoi le paramètre `reset id` de tout workflow devant pouvoir être utilisé comme action d'alerte doit être défini sur `true`. Les actions d'alerte ont un paramètre d'objet unique possédant les membres suivants :

TABLEAU 134 Membres obligatoires du contexte d'exécution des alertes

Membre obligatoire	Type	Description
class	String	Classe de l'alerte.
code	String	Code de l'alerte.
items	Objet	Objet décrivant l'alerte.
timestamp	Date	Heure de l'alerte.

Le membre `items` de l'objet de paramètre possède les membres suivants :

TABLEAU 135 Membres obligatoires du membre `items`

Membre obligatoire	Type	Description
url	String	URL de la page Web décrivant l'alerte
action	String	Action devant être entreprise par l'utilisateur en réponse à l'alerte.
impact	String	Impact de l'événement qui a déclenché l'alerte.
description	String	Chaîne lisible à l'oeil décrivant l'alerte.
severity	String	Gravité de l'événement qui a déclenché l'alerte.

Les workflows exécutant les actions d'alerte peuvent utiliser la fonction `audit` pour générer des entrées de journal. Il est recommandé d'utiliser la fonction `audit` pour ajouter toute information de débogage pertinente au journal d'audit. Le workflow suivant par exemple exécute un basculement lorsqu'il est en état clustérisé, mais audite tout échec de réinitialisation :

EXEMPLE 27 Audit d'un échec de réinitialisation par un workflow

Le workflow suivant par exemple exécute un basculement lorsqu'il est en état clustérisé, mais audite tout échec de réinitialisation :

```
var workflow = {
  name: 'Failover',
  description: 'Fail the node over to its clustered peer',
  alert: true,
  setid: true,
  execute: function (params) {
    /*
     * To failover, we first confirm that clustering is configured
     * and that we are in the clustered state. We then reboot,
     * which will force our peer to takeover. Note that we're
     * being very conservative by only rebooting if in the
     * AKCS_CLUSTERED state: there are other states in which it
     * may well be valid to failback (e.g., we are in AKCS_OWNER,
```

```

    * and our peer is AKCS_STRIPPED), but those states may also
    * indicate aberrant operation, and we therefore refuse to
    * fallback. (Even in an active/passive clustered config, a
    * FAILBACK should always be performed to transition the
    * cluster peers from OWNER/STRIPPED to CLUSTERED/CLUSTERED.)
    */
    var uuid = params.uuid;
    var clustered = 'AKCS_CLUSTERED';

    audit('attempting failover in response to alert ' + uuid);

    try {
        run('configuration cluster');
    } catch (err) {
        audit('could not get clustered state; aborting');
        return;
    }

    if ((state = get('state')) != clustered) {
        audit('state is ' + state + '; aborting');
        return;
    }

    if ((state = get('peer_state')) != clustered) {
        audit('peer state is ' + state + '; aborting');
        return;
    }

    run('cd /');
    run('confirm maintenance system reboot');
}
};

```

Utilisation de workflows programmés

En définissant un calendrier pour les workflows, il est possible de les démarrer au moyen d'un événement d'horloge. La propriété `schedule` doit être ajoutée à l'objet de workflow et doit être définie sur `true`. Les calendriers peuvent être créés soit par le biais de la CLI après le chargement d'un workflow dans l'appareil, soit par l'ajout d'une propriété de type tableau appelée `calendar` à l'objet workflow.

Chaque entrée de calendrier se compose des propriétés suivantes :

TABLEAU 136 Propriétés des calendriers de workflow

Propriété	Type	Description
NAME	String	Nom du calendrier, généré par le système.
frequency	String	Minute, demi-heure, heure, jour, semaine, mois.

Propriété	Type	Description
day	String	Indique un jour précis et peut être défini sur : lundi, mardi, mercredi, jeudi, vendredi, samedi ou dimanche. Peut être défini si la fréquence est définie sur semaine ou mois.
hour	String	00-23, spécifie la partie heure du calendrier et peut être spécifié lorsque la fréquence est définie sur jour, semaine ou mois.
minute	String	00-59, spécifie la partie minute du calendrier.

Utilisation d'un workflow programmé

Une fois qu'un workflow a été chargé dans l'appareil, il est possible de définir un calendrier qui lui est associé par le biais de l'interface de commande, comme suit :

EXEMPLE 28 Workflow programmé dans la CLI

```
dory:> maintenance workflows
dory:maintenance workflows> "select workflow-002'"
dory:maintenance workflow-002> schedules
dory:maintenance workflow-002 schedules>create
dory:maintenance workflow-002 schedule (uncommitted)> set frequency=day
frequency = day (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set hour=10
hour = 10 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set minute=05
minute = 05 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> commit
dory:maintenance workflow-002 schedules> list
NAME          FREQUENCY    DAY          HH:MM
schedule-001   day          -            10:05
dory:maintenance workflow-002 schedules> create
dory:maintenance workflow-002 schedule (uncommitted)> set frequency=week
frequency = week (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set day=Monday
day = Monday (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set hour=13
hour = 13 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> set minute=15
minute = 15 (uncommitted)
dory:maintenance workflow-002 schedule (uncommitted)> commit
dory:maintenance workflow-002 schedules> list
NAME          FREQUENCY    DAY          HH:MM
schedule-001   day          -            10:05
schedule-002   week        Monday       13:15
dory:maintenance workflow-002 schedules>
```

Codage des calendriers de workflow

Les calendriers peuvent également être spécifiés dans le code du workflow en tant que propriété de l'objet workflow. La syntaxe de la propriété utilisée dans ce cas est différente de celle utilisée pour la création du calendrier via la CLI. Trois propriétés sont utilisées ici :

TABLERAU 137 Propriétés des calendriers de workflow

Propriété	Type	Description
offset	Number	Détermine le point de départ au cours de la période définie.
period	Number	Définit la fréquence du calendrier.
unit	String	Indique si l'unité utilisée dans la définition d'offset et de period est secondes ou mois

EXEMPLE 29 Illustration de l'utilisation des propriétés de workflow

L'exemple de code suivant illustre l'utilisation des propriétés. Notez que l'arithmétique en ligne contribue à rendre plus lisibles les déclarations offset et period.

```
// Example of using Schedule definitions within a workflow
var MyTextObject = {
  MyVersion: '1.0',
  MyName: 'Example 9',
  MyDescription: 'Example of use of Timer',
  Origin: 'Oracle'
};
var MySchedules = [
  // half hr interval
  { offset: 0, period: 1800, units: "seconds" },
  // offset 2 days, 4hr, 30min , week interval
  {offset: 2*24*60*60+4*60*60+30*60, period: 604800,units: "seconds" }
];
var workflow = {
  name: MyTextObject.MyName,
  description: MyTextObject.MyDescription,
  version: MyTextObject.MyVersion,
  alert: false,
  setid: true,
  schedules: MySchedules,
  scheduled: true,
  origin: MyTextObject.Origin,
  execute: function () {
    audit('workflow started for timer; ');
  }
};
```

La propriété `units` dans l'objet `MySchedules` spécifie le type d'unité utilisé pour les propriétés `offset` et `period`. Il peut être défini sur `'seconds'` (secondes) ou sur `'month'` (mois). La propriété `period` indique la fréquence de l'événement et la propriété `offset` indique les unités au cours de la période. Dans l'exemple qui précède, la période du deuxième calendrier est définie sur une semaine et commence le second jour, à 4 h 30. Plusieurs calendriers peuvent être définis dans la propriété `calendars`.

L'objet `MySchedules` utilise dans cet exemple les trois propriétés suivantes :

- `offset` : point de départ du calendrier, le premier janvier 1970. Le point de départ est donné dans l'unité définie dans la propriété `"units"`.
- `periode` : Période du calendrier située entre deux répétitions, également donnée dans l'unité définie dans la propriété `"units"`.
- `units` : peut être définie en secondes ou en mois.

Les calendriers hebdomadaires débutent le jeudi. Cela est dû au fait que l'époque est définie comme débutant le premier janvier 1970, un jeudi.

EXEMPLE 30 Calendrier de workflow tel qu'affiché dans la CLI

Dans l'exemple ci-dessus, la période du deuxième calendrier a pour point de départ 2 jours, 4 heures et 30 minutes. Ainsi, il aura pour point de départ le 3 janvier 1970 à 4 h 30. Ce calendrier se reproduit indéfiniment tous les samedis à 4 h 30. La disposition du calendrier de la CLI est représentée ci-dessous.

```
<small>dory:> maintenance workflows
dory:maintenance workflows> list
WORKFLOW      NAME                                     OWNER SETID ORIGIN                VERSION
workflow-000  Configure for Oracle Solaris Cluster NFS root  false Oracle Corporation    1.0.0
workflow-001  Unconfigure Oracle Solaris Cluster NFS root  false Oracle Corporation    1.0.0
workflow-002  Configure for Oracle Enterprise Manager Monitoring root  false Sun Microsystems,
Inc. 1.1
workflow-003  Unconfigure Oracle Enterprise Manager Monitoring root  false Sun Microsystems,
Inc. 1.0</small>
```

```
dory:maintenance workflow-002 schedules>
```

NAME	FREQUENCY	DAY	HH:MM
schedule-000	halfhour	-	--:00
schedule-001	week	Saturday	04:30

Création d'une feuille de travail à partir d'un type de lecteur donné

L'exemple suivant illustre un workflow créant une feuille de travail à partir d'un type de lecteur donné :

EXEMPLE 31 Sélection du type de périphérique de workflow

```

var steps = [ {
  step: 'Checking for existing worksheet',
  execute: function (params) {
    /*
     * In this step, we're going to see if the worksheet that
     * we're going to create already exists. If the worksheet
     * already exists, we blow it away if the user has indicated
     * that they desire this behavior. Note that we store our
     * derived worksheet name with the parameters, even though
     * it is not a parameter per se; this is explicitly allowed,
     * and it allows us to build state in one step that is
     * processed in another without requiring additional global
     * variables.
     */
    params.worksheet = 'Drilling down on ' + params.type + ' disks';

    try {
      run('analytics worksheets select name="' +
        params.worksheet + '"');

      if (params.overwrite) {
        run('confirm destroy');
        return;
      }

      throw ('Worksheet called "' + params.worksheet +
        '" already exists!');
    } catch (err) {
      if (err.code !== EAKSH_ENTITY_BADSELECT)
        throw (err);
    }
  }, {
    step: 'Finding disks of specified type',
    execute: function (params) {
      /*
       * In this step, we will iterate over all chassis, and for
       * each chassis iterates over all disks in the chassis,
       * looking for disks that match the specified type.
       */
      var chassis, name, disks;
      var i, j;

      run('cd /');
      run('maintenance hardware');

      chassis = list();
      params.disks = [];

      for (i = 0; i < chassis.length; i++) {
        run('select ' + chassis[i]);
      }
    }
  }
];

```

```
name = get('name');
run('select disk');
disks = list();

for (j = 0; j < disks.length; j++) {
  run('select ' + disks[j]);

  if (get('use') == params.type) {
    params.disks.push(name + '/' +
      get('label'));
  }

  run('cd ..');
}

run('cd ../../');
}

if (params.disks.length === 0)
  throw ('No ' + params.type + ' disks found');
run('cd /');
}, {
step: 'Creating worksheet',
execute: function (params) {
  /*
   * In this step, we're ready to actually create the worksheet
   * itself: we have the disks of the specified type and
   * we know that we can create the worksheet. Note that we
   * create several datasets: first, I/O bytes broken down
   * by disk, with each disk of the specified type highlighted
   * as a drilldown. Then, we create a separate dataset for
   * each disk of the specified type. Finally, note that we
   * aren't saving the datasets -- we'll let the user do that
   * from the created worksheet if they so desire. (It would
   * be straightforward to add a boolean parameter to this
   * workflow that allows that last behavior to be optionally
   * changed.)
   */
  var disks = [], i;

  run('analytics worksheets');
  run('create ' + params.worksheet + '');
  run('select name=' + params.worksheet + '');
  run('dataset');
  run('set name=io.bytes[disk]');

  for (i = 0; i < params.disks.length; i++)
    disks.push('' + params.disks[i] + '');

  run('set drilldowns=' + disks.join(',')');
  run('commit');

  for (i = 0; i < params.disks.length; i++) {
```



```

    run('dataset');
    run('set name="io.bytes[disk=' +
        params.disks[i] + ']'");
    run('commit');
  }
}
} ];

var workflow = {
  name: 'Disk drilldown',
  description: 'Creates a worksheet that drills down on system, ' +
    'cache, or log devices',
  parameters: {
    type: {
      label: 'Create a new worksheet drilling down on',
      type: 'ChooseOne',
      options: [ 'cache', 'log', 'system' ],
      optionlabels: [ 'Cache', 'Log', 'System' ]
    },
    overwrite: {
      label: 'Overwrite the worksheet if it exists',
      type: 'Boolean'
    }
  },
  execute: function (params) { return (steps); }
};

```

Téléchargement de workflows à l'aide de la BUI

Pour télécharger les workflows vers l'appareil, il faut cliquer sur l'icône plus, et pour les exécuter, il faut cliquer sur la ligne indiquant le workflow.

FIGURE 39 Workflows affichés dans la BUI

Workflows 5 Total		
NAME ▲	DESCRIPTION	VERSION
Clear locks	Clear locks held on behalf of an NFS client	1.0.0
Configure for Oracle Enterprise Manager Monitoring	Sets up environment to be monitored by Oracle Enterprise Manager	1.1
Configure for Oracle Solaris Cluster NFS	Sets up environment for Oracle Solaris Cluster NFS	1.0.0
Unconfigure Oracle Enterprise Manager Monitoring	Removes the artifacts from the appliance used by Oracle Enterprise Manager	1.0
Unconfigure Oracle Solaris Cluster NFS	Removes the artifacts from the appliance used by Oracle Solaris Cluster NFS	1.0.0

▼ Téléchargement de workflows à l'aide de la CLI

1. La commande `download` permet de télécharger les workflows vers l'appareil, ce qui est identique au mécanisme utilisé pour les mises à jour logicielles :

```
dory:maintenance workflows> download
dory:maintenance workflows download (uncommitted)> get
      url = (unset)
      user = (unset)
      password = (unset)
```

2. Il faut définir la propriété `"url"` sur une URL valide pour le workflow. Il peut s'agir d'une URL locale sur le réseau ou d'une URL accessible sur Internet. L'URL peut être une HTTP (qui commence par `"http://"`) ou FTP (qui commence par `"ftp://"`). Si une authentification est requise, elle peut être incluse dans l'URL (par exemple : `"ftp://myusername:mypasswd@myserver/export/foo"`). Dans le cas contraire, les propriétés utilisateur et mot de passe doivent être définies.

```
dory:maintenance workflows download (uncommitted)> set url=
      ftp://foo/example1.akwf
      url = ftp://foo/example1.akwf
dory:maintenance workflows download (uncommitted)> set user=bmc
      user = bmc
dory:maintenance workflows download (uncommitted)> set password
Enter password:
      password = *****
dory:maintenance workflows download (uncommitted)> commit
Transferred 138 of 138 (100%) ... done
```

▼ Création d'une liste de workflows à l'aide de la CLI

1. La commande `list` exécutée à partir du contexte `maintenance workflows` permet d'afficher la liste des workflow :

```
<small>dory:maintenance workflows> list
WORKFLOW      NAME                                OWNER SETID ORIGIN                VERSION
workflow-000  Configure for Oracle Solaris Cluster NFS root  false Oracle Corporation  1.0.0
workflow-001  Unconfigure Oracle Solaris Cluster NFS root  false Oracle Corporation  1.0.0
workflow-002  Configure for Oracle Enterprise Manager Monitoring root  false Sun Microsystems,
Inc. 1.1
workflow-003  Unconfigure Oracle Enterprise Manager Monitoring root  false Sun Microsystems,
Inc. 1.0</small>
```

2. La commande `show` exécutée à partir du contexte `maintenance workflows` permet d'afficher les workflows :

```
dory:maintenance workflows> select workflow-001
dory:maintenance workflow-001> show
Properties:
      name = Configure for Oracle Solaris Cluster NFS
```

```

description = Sets up environment for Oracle Solaris Cluster NFS
owner = root
origin = Oracle Corporation
setid = false
alert = false
version = 1.0.0
scheduled = false

```

3. La commande `select` permet de sélectionner un workflow :

```

dory:maintenance workflows> select workflow-000
dory:maintenance workflow-000>

```

4. La commande `get` exécutée à partir du contexte d'un workflow sélectionné permet d'obtenir les propriétés du workflow :

```

dory:maintenance workflow-000> get
name = Hello world
description = Bids a greeting to the world
owner = root
origin = <local>
setid = false
alert = false
scheduled = false

```

▼ Exécution de workflows à l'aide de la CLI

1. La commande `execute` exécutée à partir du contexte d'un workflow sélectionné permet d'exécuter ce workflow. Si le workflow ne nécessite pas de paramètre, il va simplement s'exécuter :

```

dory:maintenance workflow-000> execute
hello world!

```

2. Si le workflow nécessite des paramètres, le contexte devient un contexte captif dans lequel les paramètres doivent être spécifiés :

```

dory:maintenance workflow-000> execute
dory:maintenance workflow-000 execute (uncommitted)> get
type = (unset)
overwrite = (unset)

```

3. Toute tentative de valider l'exécution du workflow sans avoir défini au préalable les paramètres requis se solde par un échec explicite :

```

dory:maintenance workflow-000 execute (uncommitted)> commit
error: cannot execute workflow without setting property "type"

```

4. Pour exécuter le workflow, définissez les paramètres spécifiés, puis utilisez la commande `commit` :

```
dory:maintenance workflow-000 execute (uncommitted)> set type=system
                        type = system
dory:maintenance workflow-000 execute (uncommitted)> set overwrite=true
                        overwrite = true
dory:maintenance workflow-000 execute (uncommitted)> commit
```

5. **Si le workflow comporte des étapes spécifiées, ces étapes s'affichent par l'intermédiaire de la CLI, par exemple :**

```
dory:maintenance workflow-000 execute (uncommitted)> commit
Checking for existing worksheet ... done
Finding disks of specified type ... done
Creating worksheet ... done
```

▼ Audit de workflows à l'aide de la CLI

Tous les workflows possèdent une propriété de somme de contrôle calculée par le système. Cette somme de contrôle est le hachage SHA-256 du contenu du workflow. Pour déterminer si un workflow a été modifié, comparez sa somme de contrôle avec sa somme de contrôle précédente.

- **Pour obtenir la propriété de somme de contrôle d'un workflow, utilisez la commande `get checksum` à partir du contexte `maintenance workflows` :**

```
hostname:maintenance workflows> select workflow-001
hostname:maintenance workflow-001> get checksum
checksum = 15f4188643d7add37b5ad8bda6d9b4e7210f1cd890a73df176382e800aec
```

Intégration

L'appareil Oracle ZFS Storage offre un éventail complet de protocoles de données permettant la communication avec une vaste gamme d'hôtes d'applications. Pour améliorer les performances des applications ou parvenir à une meilleure intégration dans votre environnement applicatif, reportez-vous aux sections suivantes :

- Livres blancs et descriptifs de procédures (<http://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/index.html>)
- Plug-ins Oracle ZFS Storage Appliance (<http://www.oracle.com/technetwork/server-storage/sun-unified-storage/downloads/zfssa-plugins-1489830.html>)
- Documentation relative au stockage NAS (<http://www.oracle.com/technetwork/server-storage/sun-unified-storage/documentation/index.html>)

Pour obtenir un exemple indiquant comment obtenir des résultats optimaux à l'aide des protocoles standard, reportez-vous à "Prise en charge FC avec Symantec Dynamic Multi-Pathing et Storage Foundation" à la page 649.

Dans le cas de certaines applications, l'installation de logiciels sur l'hôte d'applications améliore l'interopérabilité. Les articles suivants expliquent dans les grandes lignes la manière dont l'intégration logicielle peut améliorer l'expérience des administrateurs de stockage. Une documentation complète est fournie avec chaque téléchargement.

- "Appliance Plug-in for Oracle Solaris Cluster Geographic Edition" à la page 646
- "Plug-in ZFS Storage Appliance Network pour Oracle Solaris Cluster" à la page 646
- "Appliance Plug-in Provider for Volume Shadow Copy Service Software" à la page 648
- "Appliance Plug-in for Oracle Enterprise Manager System Monitoring" à la page 646
- "Appliance Plug-in for Oracle Virtual Machine Storage Connect" à la page 648
- "Appliance Replication Adapter for VMware Site Recovery Manager" à la page 650
- "Protocole OISP (Oracle Intelligent Storage Protocol)" à la page 645

Avec Oracle Snap Management Utility pour Oracle Database, les administrateurs de base de données peuvent assurer la protection, la disponibilité et le test rapide des données en alimentant, en clonant, en sauvegardant et en restaurant efficacement une base de données Oracle pour l'appareil Oracle ZFS Storage Appliance. Pour plus d'informations, reportez-vous [Oracle Snap Management Utility for Oracle Database \(https://www.oracle.com/storage/nas/snap/index.html\)](https://www.oracle.com/storage/nas/snap/index.html).

L'appareil Oracle ZFS Storage Appliance est conçu pour s'intégrer parfaitement avec les autres produits Oracle. La section suivante décrit la procédure de configuration de l'appareil Oracle ZFS Storage Appliance en tant que cible pour les fichiers de base de données Oracle et en tant que cible de sauvegarde pour Oracle Exadata Database Machine et Oracle SuperCluster.

- ["Sauvegarde d'Oracle Exadata Database Machine" à la page 614](#)
- ["Sauvegarde d'Oracle Exadata Database Machine" à la page 614](#)
- ["Sauvegarde d'Oracle SuperCluster" à la page 623](#)

Configuration d'Oracle ZFS Storage Appliance pour les clients de la base de données Oracle

L'appareil Oracle ZFS Storage Appliance fournit plusieurs fonctions conçues pour s'intégrer aux clients de base de données Oracle, y compris HCC (Hybrid Columnar Compression) et OISP (Oracle Intelligent Storage Protocol).

Pour activer ces fonctions, le service SNMP sur l'appareil Oracle ZFS Storage Appliance doit être configuré afin d'autoriser les demandes SNMP faites par des clients de base de données. Le client utilise ce mécanisme pour identifier un périphérique de stockage en que ZFS Storage Appliance. Pour spécifier le nom d'hôte ou l'adresse IP du client de base de données en tant que destination de déroutement, reportez-vous à la section ["Configuration du service SNMP afin qu'il indique l'état de l'appareil \(BUI\)" à la page 323](#).

Pour vérifier que le service SNMP de l'appareil est correctement configuré, exécutez la commande `snmpget (1)` à partir du système client, en remplaçant `<host>` par la nom ou l'adresse IP de l'appareil.

```
-bash-4.1$ snmpget -v1 -c public <host> .1.3.6.1.4.1.42.2.225.1.4.2.0
SNMPv2-SMI::enterprises.42.2.225.1.4.2.0 = STRING: "Oracle ZFS Storage Appliance"
```

Sauvegarde d'Oracle Exadata Database Machine

Lorsqu'il est équipé des options de connectivité natives QDR InfiniBand et Ethernet 10 Gb, l'appareil Oracle ZFS Storage est idéal pour assurer une sauvegarde fiable d'Oracle Exadata. L'utilitaire de configuration de sauvegarde Oracle Exadata est conçu pour le déploiement à l'aide d'un outil de ligne de commande. Vous avez également la possibilité de configurer manuellement votre appareil à l'aide des instructions fournies dans les sections suivantes :

- [Configuration de l'appareil pour Exadata](#)
- [Configuration d'Exadata pour l'appareil](#)

La documentation complète est fournie avec l'utilitaire, notamment les instructions d'exécution d'une sauvegarde depuis Oracle Exadata. Mais quelle que soit l'approche pour laquelle vous

optez, vous devez également procéder à la configuration, manuelle ou à l'aide de l'utilitaire, du réseau et des pools de stockage.

Pour des informations détaillées sur l'utilisation de votre appareil ZFS Storage comme cible de sauvegarde pour Oracle Exadata, reportez-vous au livre blanc "Protecting Oracle Exadata with the Oracle ZFS Storage Appliance: Configuration Best Practices" sur la page de documentation de NAS Storage. Un cluster Oracle ZFS Storage ZS3-4 est également disponible, fourni pré-monté avec des étagères de disques comme l'appareil Oracle ZFS Storage ZS3-BA pour minimiser la complexité de l'installation. La procédure d'intégration de cet appareil avec Oracle Exadata est identique au processus décrit ci-dessus.

Pour des informations détaillées, reportez-vous au livre blanc "Protecting Oracle Exadata with the Oracle ZFS Storage Appliance: Configuration Best Practices" sur la page de documentation NAS Storage.

Configuration de l'appareil pour Exadata

Pour configurer l'appareil pour Exadata, reportez-vous aux sections suivantes :

- [Configuration réseau de l'appareil](#)
- [Configuration des pools de l'appareil](#)
- [Configuration des partages de l'appareil](#)
- [Configuration d'Oracle RMAN et de l'instance de base de données Oracle](#)
- [Configuration d'Exadata pour l'appareil](#)

▼ Configuration réseau de l'appareil

Cette section décrit la configuration des groupes de multipathing sur réseau IP (IPMP) et celle du routage dans l'appareil ZFS Storage.

Remarque - Si vous avez utilisé l'utilitaire de configuration de sauvegarde Oracle Exadata, configurez le réseau comme indiqué dans cette section. Pour plus d'informations, reportez-vous au livre blanc "Best Practices".

Les clients recherchant davantage de connectivité IB peuvent installer et configurer des HCA IB supplémentaires. Pour plus de détails, consultez la présentation matérielle de votre contrôleur dans le [Manuel d'entretien client des systèmes Oracle ZFS Storage Appliance](#).

Les principes de cette section peuvent être appliqués à une implémentation Ethernet 10 Gb en appliquant la configuration réseau aux interfaces ixgbe au lieu des interfaces ibp. L'implémentation Ethernet 10 Gb peut être configurée en tant qu'IPMP actif/actif. Si l'appareil ZFS Storage se trouve sur un sous-réseau différent d'Oracle Exadata, il peut être nécessaire de

créer des routes statiques entre l'appareil ZFS Storage Appliance et Oracle Exadata. Consultez votre administrateur réseau pour plus d'informations.

1. **Assurez-vous que l'appareil ZFS Storage est connecté à Oracle Exadata.**
2. **Configurez `ibp0`, `ibp1`, `ibp2` et `ibp3` avec l'adresse `0.0.0.0/8` (nécessaire pour IPMP), le mode connecté et la clé de partition `ffff`. Pour identifier la clé de partition utilisée par le système Oracle Exadata, exécutez la commande suivante en tant qu'utilisateur root :># `cat /sys/class/net/ib0/pkey`**
3. **Configurez le groupe IPMP actif/en veille sur `ibd0` et `ibd3`, avec `ibd0` actif et `ibd3` en veille.**
4. **Configurez le groupe IPMP actif/en veille sur `ibd1` et `ibd2`, avec `ibd2` actif et `ibd1` en veille.**
5. **Activation du routage adaptatif pour garantir que la charge du trafic est correctement équilibrée lorsque plusieurs adresses IP sur le même sous-réseau sont détenues par la même tête. Cette situation se produit suite au basculement d'un cluster.**

Configuration des pools de l'appareil

Cette section décrit les éléments à prendre en compte pour déterminer la configuration de pool la plus appropriée pour les opérations de sauvegarde et de restauration de ZFS Storage Appliance for Oracle Recovery Manager (RMAN) en fonction des exigences de protection des données et de performances.

Remarque - Si vous avez utilisé l'utilitaire de configuration de sauvegarde Oracle Exadata, configurez le pool comme indiqué dans cette section. Pour plus d'informations, reportez-vous au livre blanc "Best Practices".

Le planificateur système doit envisager la protection du pool en tenant compte des recommandations suivantes :

- Utiliser la protection basée sur la parité pour les systèmes à usage généraliste et ceux optimisés pour la capacité :
 - RAID-Z pour la protection contre les pannes d'unité de disque unique sur les systèmes soumis à des charges de travail aléatoires.
 - RAID-Z2 pour la protection contre les pannes de deux unités de disque sur les systèmes avec des charges de travail impliquant la transmission en continu.
- Utiliser la mise en miroir pour de hautes performances avec sauvegarde appliquée de façon incrémentielle.
- Configurer les pools en fonction des exigences de performance :

- Configurer un pool unique pour les systèmes optimisés pour la gestion.
- Configurer deux pools pour les systèmes optimisés pour les performances. Les systèmes à deux pools doivent être configurés à l'aide de la moitié des unités de disque de chaque plateau.
- Configurer la protection du périphérique de journalisation :
 - Entrelacer les périphériques de journalisation pour les configurations de pool RAID-Z et en miroir.
 - Mettre en miroir les périphériques de journalisation pour les configurations de pool RAID-Z2.

Remarque - Remarque : si vous avez utilisé l'utilitaire de configuration de sauvegarde Oracle Exadata, passez à la rubrique suivante : [Configuration d'Exadata pour l'appareil](#).

Configuration des partages de l'appareil

Les options par défaut des partages de l'appareil ZFS Storage fournissent une bonne base de départ pour les charges de travail généralistes. Les partages de l'appareil peuvent être optimisés pour les opérations de sauvegarde et de restauration d'Oracle RMAN en procédant comme suit :

- Créez un projet destiné au stockage de tous les partages liés à la sauvegarde et à la restauration d'une base de données unique. Pour une implémentation à deux pools, créez deux projets, un pour chaque pool.
- Configurez les partages qui prennent en charge les charges de travail de sauvegarde et de restauration d'Oracle RMAN avec les valeurs suivantes :
 - Taille des enregistrements de la base de données (`recordsize`) : 128 ko
 - Décalage d'écriture synchrone (`logbias`) : Débit (pour le traitement des jeux de sauvegardes et des copies d'images) ou Latence (pour les sauvegardes appliquées de manière incrémentielle)
 - Utilisation du périphérique de cache (`secondary cache`) : Aucun (pour les jeux de sauvegardes) ou Tous (lors de la prise en charge des sauvegardes appliquées de manière incrémentielle ou des opérations de clonage de base de données)
 - Compression des données (`compression`) : Désactivée pour les systèmes optimisés pour les performances, LZJB ou gzip-2 pour les systèmes optimisés pour la capacité.
 - Nombre de partages par pool : 1 pour les systèmes optimisés pour la gestion, 2 ou 4 pour les systèmes optimisés pour les performances

Des options de configuration supplémentaires des partages, telles qu'une compression gzip ou une réplication de plus haut niveau, peuvent être appliquées aux partages utilisés pour la prise en charge de la sauvegarde et de la restauration Oracle Exadata, comme l'exige le client.

Les clients qui implémentent des services de données supplémentaires de l'appareil ZFS Storage doivent prendre en considération le test spécifique à l'implémentation pour vérifier les implications des déviations des pratiques décrites précédemment.

Configuration d'Oracle RMAN et de l'instance de base de données Oracle

Oracle RMAN est une composante essentielle de la protection du contenu d'Oracle Exadata. Oracle RMAN permet de créer des jeux de sauvegardes, des copies d'images et des sauvegardes mises à jour de manière incrémentielle du contenu d'Oracle Exadata sur les appareils ZFS Storage. Pour optimiser les performances des sauvegardes d'Oracle RMAN depuis Oracle Exadata vers un appareil ZFS Storage, l'administrateur de base de données doit appliquer les règles de meilleure pratique suivantes :

- Equilibrer la charge des canaux Oracle RMAN de manière équitable entre les noeuds de la machine de base de données.
- Equilibrer la charge des canaux Oracle RMAN de manière équitable entre les partages et les contrôleurs de l'appareil ZFS Storage.

Pour optimiser la mise en tampon du canal Oracle RMAN sur l'appareil ZFS Storage, vous pouvez régler les valeurs de plusieurs paramètres cachés de l'instance. Pour Oracle Database 11g version 2, les paramètres suivants peuvent être réglés :

- Pour le jeu de sauvegardes et de restaurations :
 - `_backup_disk_bufcnt=64`
 - `_backup_disk_bufsz=1048576`
- Pour la sauvegarde et la restauration de copies d'images :
 - `_backup_file_bufcnt=64`
 - `_backup_file_bufsz=1048576`

Pour plus d'informations sur le réglage de ces paramètres et le réglage de paramètres équivalents pour les versions antérieures du logiciel de base de données Oracle, reportez-vous à l'article ID 1072545.1 : *Réglage des performances de RMAN à l'aide des paramètres de mémoire tampon* à l'adresse [My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com).

Oracle Direct NFS (dNFS) est un client NFS performant qui offre des performances exceptionnelles pour les opérations de sauvegarde et de restauration d'Oracle RMAN. dNFS doit être configuré pour les clients qui recherchent un débit maximal pour les opérations de sauvegarde et de restauration.

Configuration d'Exadata pour l'appareil

Si vous avez utilisé l'utilitaire de configuration de sauvegarde Oracle Exadata, toutes les étapes à l'exception des étapes 4 à 7 ont déjà été effectuées pour vous.

- [Configuration de l'appareil pour Exadata](#)
- [Configuration de la structure de répertoires pour les partages](#)

- Mise à jour du fichier `/etc/fstab`
- Création d'un service `init.d`
- Mise à jour de `orandstab` pour accéder aux exports de l'appareil
- Montage des partages sur l'hôte
- Configuration de la propriété des partages montés

▼ Configuration de la structure de répertoires pour les partages

- Configurez les points de montage pour les partages sur l'hôte, comme indiqué :

```
mkdir -p /zfssa/dbname/backup1
mkdir -p /zfssa/dbname/backup2
mkdir -p /zfssa/dbname/backup3
mkdir -p /zfssa/dbname/backup4
```

▼ Mise à jour du fichier `/etc/fstab`

Le caractère d'échappement sur une nouvelle ligne (`\`) d'UNIX indique qu'une ligne de code a été répartie sur deux lignes dans la liste ci-dessous. Lorsque vous saisissez une ligne de code répartie sur deux lignes dans `fstab`, supprimez le caractère `\` et rassemblez les segments des deux lignes, séparés par un espace, en une seule ligne.

1. Pour mettre à jour le fichier `/etc/fstab`, utilisez l'une des options suivantes.

Pour une configuration à un pool :

```
192.168.36.200:/export/dbname/backup1 /zfssa/dbname/backup1 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
192.168.36.200:/export/dbname/backup2 /zfssa/dbname/backup2 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
192.168.36.200:/export/dbname/backup3 /zfssa/dbname/backup3 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
192.168.36.200:/export/dbname/backup4 /zfssa/dbname/backup4 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
```

2. *Pour une configuration à deux pools :*

```
192.168.36.200:/export/dbname/backup1 /zfssa/dbname/backup1 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
192.168.36.201:/export/dbname/backup2 /zfssa/dbname/backup2 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
192.168.36.200:/export/dbname/backup3 /zfssa/dbname/backup3 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
192.168.36.201:/export/dbname/backup4 /zfssa/dbname/backup4 nfs \<br/>
rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,tcp,nfsvers= \<br/> 3,timeo=600 0 0
```

▼ Création d'un service init.d

1. Créez un service init.d à l'aide de l'option appropriée suivante.

```
# !/bin/sh
#
# zfssa_dbname: Mount ZFSSA project dbname for database dbname
#
# chkconfig: 345 61 19
# description: mounts ZFS Storage Appliance shares
#

start()
{
    mount /zfssa/dbname/backup1
    mount /zfssa/dbname/backup2
    mount /zfssa/dbname/backup3
    mount /zfssa/dbname/backup4
    echo "Starting $prog: "
}

stop()
{
    umount /zfssa/dbname/backup1
    umount /zfssa/dbname/backup2
    umount /zfssa/dbname/backup3
    umount /zfssa/dbname/backup4
    echo "Stopping $prog: "
}

case "$1" in
    start)
        start
        ;;
    stop)
        stop
        ;;
    restart)
        stop
        start
        ;;
    status)
        mount
        ;;
    *)
        echo "Usage: $0 {start|stop|restart|status}"
        exit 1
esac
```

2. (Facultatif) Activez le service `init.d` pour le démarrage à l'initialisation en entrant :

```
# chkconfig zfssa_dbname on
```

3. **(Facultatif) Démarrez et arrêtez le service manuellement à l'aide des commandes de service :**

```
# service zfssa_dbname start<br/># service zfssa_dbname stop
```

▼ Mise à jour de oranfstab pour accéder aux exports de l'appareil

Si vous avez utilisé l'utilitaire de configuration de sauvegarde Oracle Exadata, vous pouvez également suivre cette procédure.

1. **Pour mettre à jour le fichier oranfstab pour accéder aux exportations de l'appareil ZFS Storage, utilisez l'option appropriée suivante. *Pour une configuration à un pool :***

```
server: 192.168.36.200
path: 192.168.36.200
export: /export/dbname/backup1 mount: /zfssa/dbname/backup1
export: /export/dbname/backup2 mount: /zfssa/dbname/backup2
export: /export/dbname/backup3 mount: /zfssa/dbname/backup3
export: /export/dbname/backup4 mount: /zfssa/dbname/backup4
```

2. *Pour une configuration à deux pools :*

```
server: 192.168.36.200
path: 192.168.36.200
export: /export/dbname/backup1 mount: /zfssa/dbname-2pool/backup1
export: /export/dbname/backup3 mount: /zfssa/dbname-2pool/backup3
server: 192.168.36.201
path: 192.168.36.201
export: /export/dbname/backup2 mount: /zfssa/dbname-2pool/backup2
export: /export/dbname/backup4 mount: /zfssa/dbname-2pool/backup4
```

▼ Montage des partages sur l'hôte

1. **Pour monter les partages sur l'hôte, saisissez l'une des deux options suivantes :**

```
# service mount_dbname start
```

2. **ou**

```
# dcli -l root -g /home/oracle/dbs_group service mount_dbname start
```

▼ Configuration de la propriété des partages montés

Modifiez les paramètres d'autorisation des partages montés pour correspondre aux paramètres d'autorisation de ORACLE_HOME. Dans cet exemple, les propriétés d'utilisateur et de groupe sont définies sur oracle:dba.

Si vous avez utilisé l'utilitaire de configuration de sauvegarde Oracle Exadata, vous pouvez également effectuer l'étape 2, l'étape 1 ayant déjà été effectuée pour vous.

1. **Saisissez l'une des deux options suivantes :** `<br /># chown oracle:dba /zfssa/dbname/*<br />ou<br /># dcli -l root -g /home/oracle/dbs_group chown oracle:dba /zfssa/dbname/*`
2. **Redémarrez l'instance de base de données Oracle pour reprendre les modifications apportées au fichier oranfstab à l'aide de l'une des options suivantes :**
3. **Redémarrez une instance à la fois (mise à niveau non simultanée).**

Exemple 32 Redémarrage d'une instance à la fois

```
$ srvctl stop instance -d dbname -i dbname1
$ srvctl stop instance -d dbname -i dbname1
$ srvctl start instance -d dbname -i dbname1
$ srvctl stop instance -d dbname -i dbname2
$ srvctl start instance -d dbname -i dbname2
$ srvctl stop instance -d dbname -i dbname3
$ srvctl start instance -d dbname -i dbname3
$ srvctl stop instance -d dbname -i dbname4
$ srvctl start instance -d dbname -i dbname4
$ srvctl stop instance -d dbname -i dbname5
$ srvctl start instance -d dbname -i dbname5
$ srvctl stop instance -d dbname -i dbname6
$ srvctl start instance -d dbname -i dbname6
$ srvctl stop instance -d dbname -i dbname7
$ srvctl start instance -d dbname -i dbname7
$ srvctl stop instance -d dbname -i dbname8
$ srvctl start instance -d dbname -i dbname8
```

Redémarrez l'ensemble de la base de données, par exemple :

```
$ srvctl stop database -d dbname
$ srvctl start database -d dbname
```

Sauvegarde d'Oracle SuperCluster

Lorsqu'il est équipé des options de connectivité natives QDR InfiniBand et Ethernet 10 Gb, l'appareil ZFS Storage est idéal pour assurer une sauvegarde fiable d'Oracle SPARC SuperCluster. Suivez les instructions des sections suivantes pour configurer votre système :

- [Configuration de la sauvegarde de l'appareil pour SuperCluster](#)
- [Configuration d'Oracle SPARC SuperCluster pour la sauvegarde d'un appareil](#)

Pour des informations détaillées sur l'utilisation de votre appareil ZFS Storage comme cible de sauvegarde pour Oracle SPARC SuperCluster, reportez-vous au livre blanc "Configuring a Sun ZFS Backup Appliance with Oracle SPARC SuperCluster" sur la page de documentation NAS Storage. Un cluster Oracle ZFS Storage ZS3-4 est également disponible, fourni pré-monté avec des étagères de disques comme l'appareil Oracle ZFS Storage ZS3-BA pour minimiser la complexité de l'installation. La procédure d'intégration de cet appareil avec Oracle SPARC SuperCluster est identique au processus décrit ci-dessus.

Configuration de la sauvegarde de l'appareil pour SuperCluster

Cette section fournit les étapes à suivre pour la configuration d'un appareil ZFS Storage destiné à la sauvegarde avec Oracle SPARC SuperCluster. Pour des informations détaillées, reportez-vous au livre blanc "Configuring a Sun ZFS Backup Appliance with Oracle SPARC SuperCluster" sur la page de documentation NAS Storage.

- ["Configuration des liaisons de données InfiniBand de l'appareil ZFS Storage" à la page 624](#)
- ["Configuration des commutateurs InfiniBand d'Oracle SPARC SuperCluster pour ajouter l'appareil ZFS Storage" à la page 624](#)
- ["Configuration de la gestion réseau de l'appareil ZFS Storage pour une connexion IP unique" à la page 628](#)
- ["Configuration de la gestion réseau de l'appareil ZFS Storage pour une configuration active-active" à la page 628](#)
- ["Configuration du pool de stockage de l'appareil ZFS Storage" à la page 630](#)
- ["Configuration des partages de l'appareil ZFS Storage" à la page 630](#)
- ["Configuration des analyses DTrace Analytics de l'appareil ZFS Storage" à la page 631](#)
- ["Configuration du montage NFS du client" à la page 632](#)
- ["Réglage du réseau et du noyau Solaris 11" à la page 632](#)
- ["Configuration d'Oracle Direct NFS \(dNFS\)" à la page 633](#)
- ["Réglage de l'instance de base de données Oracle pour la sauvegarde et la restauration Oracle RMAN" à la page 634](#)
- ["Création de services dédiés pour les opérations Oracle RMAN" à la page 636](#)

- ["Configuration d'Oracle RMAN" à la page 637](#)
- ["Configuration d'Oracle SPARC SuperCluster pour la sauvegarde d'un appareil" à la page 641](#)

▼ Configuration des liaisons de données InfiniBand de l'appareil ZFS Storage

Suivez les étapes de cette section pour configurer chaque connexion InfiniBand de l'appareil ZFS Storage. Les huit GUID pour les ports HBA InfiniBand qui sont enregistrés lors de cette procédure permettent de configurer les commutateurs InfiniBand d'Oracle SPARC SuperCluster dans la procédure suivante.

1. **Connectez l'appareil ZFS Storage à Oracle SPARC SuperCluster, comme décrit dans le livre blanc "Configuring a Sun ZFS Backup Appliance with Oracle SPARC SuperCluster" sur la page de documentation NAS Storage.**
2. **Connectez-vous à l'interface utilisateur de navigateur (BUI) de la tête 1 et accédez à Configuration > Réseau.**
3. **Cliquez sur icône représentant le signe plus (+) située à côté des liaisons de données. La boîte de dialogue Liaison de données réseau s'affiche.**
4. **Renseignez la boîte de dialogue comme suit :**
 - Activez la case à cocher IB Partition.
 - Saisissez un nom explicite pour la liaison de données.
 - Définissez Partition Key sur 8503.
 - Sélectionnez le mode connecté pour le mode de liaison.
 - N'activez pas la case à cocher LACP Aggregation.
 - Sélectionnez Partition Device ibp0.
 - Enregistrez le numéro du GUID (par exemple, 21280001ef43bb) et cliquez sur Appliquer.
5. **Répétez les étapes 3 et 4 pour chaque interface InfiniBand restante (ibp1, ibp2 et ibp3).**
6. **Répétez les étapes 2 à 5 pour la tête 2.**

▼ Configuration des commutateurs InfiniBand d'Oracle SPARC SuperCluster pour ajouter l'appareil ZFS Storage

Dans cette procédure, les GUID des ports HBA Infiniband de l'appareil ZFS Storage Appliance sont ajoutés à la configuration InfiniBand Oracle SPARC SuperCluster existante. En ajoutant

ces ports et en utilisant une clé de partition de 8503, la communication entre les deux périphériques peut se produire.

1. **Connectez-vous au commutateur Spine InfiniBand d'Oracle SPARC SuperCluster en tant qu'utilisateur root. Par défaut, le commutateur Spine reçoit le nom d'hôte <sscid>sw- ib1, où <sscid> correspond au nom de préfixe donné à l'ensemble du système Oracle SPARC SuperCluster. Dans l'exemple suivant, le <sscid> est aiessc.**

```
login as: root
root@aiesscsw-ib1's password:
Last login: Tue Sep 25 08:19:01 2013 from dhcp-brm-bl5-204-3e
east-10-135-75-254.usdhcp.oraclecorp.com
```

2. **Saisissez la commande `enablesm` pour vérifier que le commutateur exécute le gestionnaire de sous-réseau (ou cette commande lance le gestionnaire de sous-réseau).**

```
[root@aiesscsw-ib1 ~]# enablesm
opensm (pid 15906) is already running...
Starting partitiond daemon
/usr/local/util/partitiond is already running
(You may also perform a 'restart' if wanted)
```

3. **Saisissez la commande `getmaster` pour vérifier qu'il s'agit du commutateur principal de la configuration. Si le commutateur principal n'est pas exécuté sur le commutateur Spine, déconnectez-vous et connectez-vous au commutateur principal désigné pour le reste de la procédure.**

```
[root@aiesscsw-ib1 ~]# getmaster
Local SM enabled and running
20130913 10:16:51 Master SubnetManager on sm lid 13 sm guid
0x2128e8ac27a0a0 : SUN DCS 36P QDR aiesscsw-ib1.us.oracle.com
[root@aiesscsw-ib1 ~]#
```

4. **Sauvegardez la configuration du commutateur d'après les procédures de sauvegarde documentées (http://docs.oracle.com/cd/E26698_01/index.html (http://docs.oracle.com/cd/E26698_01/index.html)).**
5. **Saisissez la commande `smpartition list active` pour vérifier que la clé de partition 0x0503 est assignée au nom de partition "sto" (sto = 0x0503).
> La clé de partition a été définie sur 8503 sur les liaisons de données de l'appareil ZFS Storage, mais le commutateur InfiniBand rapporte 0503. Cela est intentionnel car le protocole InfiniBand réserve le bit le plus significatif (0x8000) de la clé de partition hexadécimale (pkey) pour sa propre utilisation. Par conséquent, les pkeys 0x8503 et 0x0503 sont identiques.**

```
[root@ailesscsw-ib1 ~]# smpartition list active
# Sun DCS IB partition config file
# This file is generated, do not edit
#! version_number : 11
Default=0x7fff, ipoib : ALL_CAS=full, ALL_SWITCHES=full, SELF=
full;
SUN_DCS=0x0001, ipoib : ALL_SWITCHES=full;
ic1s10 = 0x0501, ipoib, defmember=full:
0x0021280001ef30f7,
0x0021280001ef33bf,
0x0021280001ef30b7,
0x0021280001ef314b;
ic2s10 = 0x0502, ipoib, defmember=full:
0x0021280001ef30f8,
0x0021280001ef33c0,
0x0021280001ef30b8,
0x0021280001ef314c;
sto = 0x0503, ipoib, defmember=full:
0x0021280001ef43f8,
0x0021280001ef43b7,
0x0021280001cf90c0,
0x0021280001ef43bb,
...more...
```

6. Ajoutez l'appareil ZFS Storage à la configuration InfiniBand :
7. Saisissez la commande `smpartition start` pour démarrer une session de reconfiguration.

```
# smpartition start<br/>
[root@ailesscsw-ib1 ~]# smpartition start
```

8. Saisissez la commande `smpartition add` pour ajouter les huit nouveaux GUID à la configuration.

```
# smpartition add -n sto -port <GUID1> <GUID2> <GUID3> ... <GUID8><br/>
[root@ailesscsw-ib1 ~]# smpartition add -n sto -port
21280001ef43bb 21280001ef43bc 21280001cf90bf 21280001cf90c0
21280001ef43f7 21280001ef43f8 21280001ef43b7 21280001ef43b8
```

9. Saisissez la commande `smpartition list modified` pour vérifier que les nouveaux GUID ont été ajoutés correctement.

```
# smpartition list modified<br/>
[root@ailesscsw-ib1 ~]# smpartition list modified
# Sun DCS IB partition config file
<nowki># This file is generated, do not edit
#! version_number : 11
```

```
Default=0x7fff, ipoib : ALL_CAS=full, ALL_SWITCHES=full, SELF=
full;
SUN_DCS=0x0001, ipoib : ALL_SWITCHES=full;
ic1s10 = 0x0501, ipoib, defmember=full:
0x0021280001ef30f7,
0x0021280001ef33bf,
0x0021280001ef30b7,
0x0021280001ef314b;
ic2s10 = 0x0502, ipoib, defmember=full:
0x0021280001ef30f8,
0x0021280001ef33c0,
0x0021280001ef30b8,
0x0021280001ef314c;
sto = 0x0503, ipoib, defmember=full:
0x0021280001ef43f8,
0x0021280001ef43b7,
0x0021280001cf90c0,
0x0021280001ef43bb,
0x0021280001ef43bc,
0x0021280001cf90bf,
0x0021280001ef43b8,
0x0021280001ef43f7,
0x0021280001ef3048,
0x0021280001ef30af,
0x0021280001ef30f8,
0x0021280001ef30f7,
0x0021280001ef33c0,
0x0021280001ef33bf,
0x0021280001ef30cc,
0x0021280001ef342b,
0x0021280001ef30b8,
0x0021280001ef30b7,
0x0021280001ef314c,
0x0021280001ef314b,
0x0021280001efec65,
0x0021280001efec66,
0x0021280001efecb1,
0x0021280001efecb2;
```

10. Saisissez la commande `smpartition commit` pour appliquer la nouvelle configuration et propager les modifications de configuration à tous les commutateurs InfiniBand de la configuration.

```
# smpartition commit<br/>
[root@aiesscsw-ib1 ~]# smpartition commit
[root@aiesscsw-ib1 ~]#
```

11. Déconnectez-vous du commutateur InfiniBand.
12. Sauvegardez la configuration InfiniBand d'après les procédures de sauvegarde documentées (documentation du commutateur [Sun Datacenter InfiniBand \(http://docs.oracle.com/cd/E26698_01/index.html\)](http://docs.oracle.com/cd/E26698_01/index.html)).

▼ Configuration de la gestion réseau de l'appareil ZFS Storage pour une connexion IP unique

Cette configuration est uniquement destinée à Oracle SPARC SuperCluster T5 sans commutateur Leaf externe. Pour un meilleur basculement et de meilleures performances, utilisez la configuration active-active (section suivante) pour toutes les autres configurations.

Configurez les ports InfiniBand de l'appareil ZFS Storage pour la connectivité réseau et le basculement de cluster simple à l'aide de la procédure suivante pour configurer le port 1 avec l'adresse IP souhaitée.

1. **Connectez-vous à la BUI de la tête 1 et accédez à Configuration > Réseau.**
2. **Cliquez sur l'icône représentant le signe plus (+) située à côté des interfaces. La boîte de dialogue Interface réseau s'affiche.**
3. **Renseignez la boîte de dialogue comme suit :**
 - Saisissez un nom explicite pour l'interface réseau.
 - Vérifiez que la case `Enable Interface` est sélectionnée.
 - Vérifiez que la case `Allow Administration` est sélectionnée.
 - Vérifiez que la case `Use IPv4 Protocol` est sélectionnée.
 - Vérifiez que la sélection de menu `Configure with` est `Static Address List`.
 - Dans la case ci-dessous, saisissez l'adresse IP souhaitée avec le masque de réseau approprié.
 - Vérifiez que la case `Use IPv6 Protocol` n'est pas sélectionnée.
 - Sélectionnez la liaison de données `ibp0` et cliquez sur `Appliquer`.
4. **Répétez les étapes 1 à 3 sur la tête 2 avec `ibp2` comme liaison de données.**

▼ Configuration de la gestion réseau de l'appareil ZFS Storage pour une configuration active-active

Configurez les ports InfiniBand sur l'appareil ZFS Storage pour le multipathing IP. Quatre adresses IP, sur le sous-réseau de stockage privé, sont requises pour chaque tête de l'appareil ZFS Storage (donc huit adresses au total) car les interfaces sont exécutées dans une configuration active-active.

1. **Configurez l'interface IPMP sur la tête 1.**
 - Connectez-vous à la BUI de la tête 1 et accédez à Configuration > Réseau.
 - Cliquez sur l'icône représentant le signe plus (+) située à côté des interfaces. La boîte de dialogue Interface réseau s'affiche.
 - Renseignez la boîte de dialogue comme suit :

- Saisissez un nom explicite pour l'interface réseau IPMP.
- Vérifiez que la case `Enable Interface` est sélectionnée.
- Vérifiez que la case `Allow Administration` est sélectionnée.
- Vérifiez que la case `Use IPv4 Protocol` est sélectionnée.
- Vérifiez que la sélection de menu `Configure with` est `Static Address List`.
- Cliquez trois fois sur le signe plus (+) en regard de la case vide de sorte à afficher quatre cases vides.
- Dans chaque case vide, saisissez l'une des adresses IP réservées pour les connexions InfiniBand avec sa désignation de masque de réseau /24 respective. Une pratique recommandée consiste à ne pas utiliser des adresses IP consécutives du bloc, mais plutôt une sur deux (par exemple, des adresses paires ou impaires uniquement).
- Vérifiez que la case `Use IPv6 Protocol` n'est pas sélectionnée.
- Activez la case à cocher `IP MultiPathing Group`.
- Activez les cases à cocher en regard des interfaces qui correspondent aux liaisons de données `ibp0` et `ibp3`.
- Assurez-vous que les deux interfaces sont définies sur `Active` et cliquez sur `Appliquer`.
- Dans `Configuration > Réseau`, cliquez sur `Routage`.
- Cliquez sur le modèle de multihébergement correspondant à `Adaptive`.

2. Configurez l'interface IPMP sur la tête 2.

- Connectez-vous à la BUI de la tête 2 et accédez à `Configuration > Réseau`.
- Cliquez sur l'icône représentant le signe plus (+) située à côté des interfaces. La boîte de dialogue `Interface réseau` s'affiche.
- Renseignez la boîte de dialogue comme suit :
 - Saisissez un nom explicite pour l'interface réseau IPMP.
 - Vérifiez que la case `Enable Interface` est sélectionnée.
 - Vérifiez que la case `Allow Administration` est sélectionnée.
 - Vérifiez que la case `Use IPv4 Protocol` est sélectionnée.
 - Vérifiez que la sélection de menu `Configure with` est `Static Address List`.
 - Cliquez trois fois sur le signe plus (+) en regard de la case vide de sorte à afficher quatre cases vides.
 - Dans chaque case vide, saisissez l'une des quatre adresses IP restantes réservées pour les connexions InfiniBand avec sa désignation de masque de réseau /24 respective. Il s'agit de celles qui ne sont pas utilisées sur la tête 1.
 - Vérifiez que la case `Use IPv6 Protocol` n'est pas sélectionnée.
 - Activez la case à cocher `IP MultiPathing Group`.
 - Activez les cases à cocher en regard des interfaces qui correspondent aux liaisons de données `ibp1` et `ibp2`.

- Assurez-vous que les deux interfaces sont définies sur Active et cliquez sur Appliquer.
 - Dans Configuration > Réseau, cliquez sur Routage.
 - Cliquez sur le modèle de multihébergement correspondant à Adaptive.
3. **Vérifiez la connectivité avec les noeuds Oracle SPARC SuperCluster. Vérifiez que chaque noeud peut envoyer une commande ping à chacune des adresses utilisées dans les groupes IPMP sur l'appareil ZFS Storage. Ajoutez les adresses IP à la table `/etc/inet/hosts` de chaque noeud.**

Configuration du pool de stockage de l'appareil ZFS Storage

La configuration de pool affecte des ressources d'unités de disques physiques aux pools de stockage logique pour le stockage des données de sauvegarde. Pour maximiser le débit du système, configurez deux pools de stockage de même taille en affectant la moitié des unités physiques de chaque plateau de disques à chaque pool de stockage.

Le logiciel de gestion de l'appareil ZFS Storage présente un message d'avertissement relatif à l'efficacité lorsque deux pools avec le même profil de protection RAID sont configurés. Ce message peut être ignoré lors de la configuration pour une solution de sauvegarde Oracle RMAN de hautes performances.

▼ Configuration des partages de l'appareil ZFS Storage

La configuration des partages correspond au processus de configuration et d'exécution des points de montage NFS pour l'accès client. Deux projets doivent être créés pour la configuration d'Oracle SPARC SuperCluster : un projet par pool. Un projet est une entité qui fournit un point d'interface de gestion de niveau supérieur pour un ensemble de partages. Pour optimiser la gestion des partages, mettez à jour le point de montage par défaut des partages contenus dans le projet afin de faire référence au nom de la base de données, tel que `/export/dbname`. Pour un système optimisé pour les performances, créez quatre partages pour chaque projet dans chaque pool, pour un total de huit partages (quatre pour chaque tête). Pour configurer un projet, procédez comme suit :

1. **Connectez-vous à la BUI de la tête 1 et accédez à Partages > Projets.**
2. **Cliquez sur l'icône représentant le signe plus (+) située en regard de Projets, saisissez un nom significatif pour le projet et cliquez sur Appliquer. Dans la mesure où un projet similaire sera créé sur l'autre tête, donnez un nom unique au projet de la tête 1, par exemple `H1-mysdb`.**
3. **Cliquez sur l'icône représentant un crayon située à côté du nom du nouveau projet pour modifier le projet.**
4. **Cliquez sur Général et renseignez les propriétés comme suit :**

- Modifiez Mountpoint pour inclure le nom de la base de données (par exemple, /export/H1-mysql).
 - Passez Synchronous write bias de Latency à Throughput et cliquez sur Appliquer.
5. **Cliquez sur Protocoles et ajoutez une exception NFS, comme suit :**
- Cliquez sur l'icône représentant le signe plus (+) située à côté d'Exceptions NFS.
 - Modifiez Type en Network.
 - Saisissez le sous-réseau et le masque de réseau (par exemple, /24) du réseau InfiniBand.
 - Modifiez Access Mode en Read/Write.
 - Vérifiez que Charset est défini sur default.
 - Activez la case à cocher Root Access et cliquez sur Appliquer.
6. **En regard de Général, cliquez sur Partages.**
7. **Créez quatre systèmes de fichiers pour la tête 1 et nommez-les de manière unique de sorte qu'ils soient différents des noms de la tête 2. Pour insérer les flux de sauvegarde afin de distribuer les données sur les deux têtes et, ainsi, fournir de meilleures performances, utilisez des noms impairs pour la tête 1, tels que backup1, backup3, backup5 et backup7 et des noms pairs pour la tête 2, tels que backup2, backup4, backup6 et backup8. Pour créer les systèmes de fichiers, cliquez sur l'icône représentant le signe plus (+) située en regard de Systèmes de fichiers, saisissez le nom du système de fichiers (backup1) et cliquez sur Appliquer. Répétez cette étape pour créer les trois systèmes de fichiers restants (backup3, backup5 et backup7).**
8. **Répétez les étapes 1 à 7 pour la tête 2. N'oubliez pas d'utiliser un nom de projet unique (par exemple, H2-mysql) et d'indiquer des ID de sauvegarde pairs (backup2, backup4, backup6 et backup8) pour les noms des systèmes de fichiers.**

Configuration des analyses DTrace Analytics de l'appareil ZFS Storage

L'appareil ZFS Storage inclut un outil complet d'analyse des performances appelé DTrace Analytics. DTrace Analytics est une structure qui surveille les statistiques importantes de comptabilisation des performances des sous-systèmes. Un sous-ensemble des statistiques de comptabilisation disponibles doit être surveillé pour fournir des données complètes sur l'efficacité et les performances des charges de travail de sauvegarde et de restauration d'Oracle RMAN.

Les analyses suivantes sont disponibles lorsque des analyses avancées sont configurées sur l'appareil ZFS Storage (Configuration > Préférences > Activer les analyses avancées) :

- CPU : pourcentage d'utilisation ventilé par mode CPU
- Disque : nombre moyen d'opérations d'E/S ventilé par état d'opération
- Disque : octets d'E/S par seconde ventilés par type d'opération
- Disque : opérations d'E/S par seconde ventilées par latence
- Disque : disques utilisés à 95 pour cent au moins ventilés par disque
- Réseau : octets d'interface par seconde ventilés par direction
- Réseau : octets d'interface par seconde ventilés par interface
- Protocole : opérations NFSv3 par seconde ventilées par taille
- Protocole : opérations NFSv3 par seconde ventilées par type d'opération
- Protocole : opérations NFSv3 par seconde de type lecture ventilées par latence
- Protocole : opérations NFSv3 par seconde de type écriture ventilées par latence
- Protocole : opérations NFSv3 par seconde de type lecture ventilées par taille
- Protocole : opérations NFSv3 par seconde de type écriture ventilées par taille

L'implémentation de ces statistiques de comptabilisation permet aux utilisateurs finaux d'obtenir un aperçu quantitatif de la consommation instantanée et historique des ressources et de la qualité du service (QoS) pour leur implémentation spécifique.

Configuration du montage NFS du client

Lors de la configuration de l'appareil ZFS Storage, tout serveur qui accède à l'appareil, y compris les noeuds Oracle SPARC SuperCluster, est considéré comme un client. La configuration du montage NFS du client inclut la création de la structure du répertoire cible pour accéder à l'appareil ZFS Storage ainsi que les options de montage NFS spécifiques pour des performances système optimales. Les options de montage pour les clients Solaris sont les suivantes :

```
rw,bg,hard,nointr,rsz=1048576,wsz=1048576,proto=tcp,vers=3,forcedirectio
```

Les points de montage des répertoires créés sur l'appareil ZFS Storage doivent être créés sur chacun des noeuds Oracle SPARC SuperCluster et ajoutés à leur table `/etc/inet/hosts`.

▼ Réglage du réseau et du noyau Solaris 11

1. **Les entrées suivantes doivent être ajoutées au fichier `/etc/system` de chacun des noeuds Oracle SPARC SuperCluster :**

```
set rpcmod:clnt_max_conns = 8
set nfs:nfs3_bsize = 131072
```

2. **De plus, les commandes suivantes doivent être exécutées sur chaque noeud Oracle SPARC SuperCluster chaque fois qu'il est réinitialisé :**


```
/usr/sbin/ndd -set /dev/tcp tcp_max_buf 2097152
/usr/sbin/ndd -set /dev/tcp tcp_xmit_hiwat 1048576
/usr/sbin/ndd -set /dev/tcp tcp_recv_hiwat 1048576
```

3. **Un réglage supplémentaire peut être nécessaire pour atteindre des performances optimales. Pour obtenir les dernières informations, reportez-vous au document 1474401.1 "Oracle SPARC SuperCluster Tunables", disponible via [My Oracle Support \(http://support.oracle.com\)](http://support.oracle.com). De plus, la version QFSDP de janvier 2013 a ajouté un outil qui définit automatiquement les paramètres réglables. Reportez-vous aux notes de version d'Oracle SPARC SuperCluster pour plus d'informations.**

▼ Configuration d'Oracle Direct NFS (dNFS)

Sur chaque nœud d'Oracle SPARC SuperCluster, configurez dNFS comme suit :

1. **Arrêtez l'instance en cours d'exécution du logiciel de base de données Oracle.**
2. **Remplacez le répertoire par \$ORACLE_HOME/rdbms/lib.**
3. **Activez dNFS :
**

```
make -f $ORACLE_HOME/rdbms/lib/ins_rdbms.mk dnfs_on
```

4. **Mettez à jour le fichier oranfstab (situé sous /\$ORACLE_HOME/dbs) avec les noms du serveur, du chemin et de l'exportation spécifiques à la configuration, où :
**
 - Le paramètre du serveur fait référence au nom local de la tête de l'appareil ZFS Storage sur le réseau InfiniBand.

 - Les paramètres de chemin doivent refléter l'adresse ou les adresses de cette tête spécifiée(s) lors de la configuration.

 - Les paramètres d'exportation doivent refléter les points de montage similaires aux entrées créées dans /etc/vfstab. Les entrées doivent ressembler à ce qui suit.

5. **Pour la configuration IP unique (uniquement Oracle SPARC SuperCluster T5 sans commutateur Leaf externe) :**

```
server: aie-zba-h1-stor
path: 192.168.30.100
export: /export/test1/backup1 mount: /zba/test1/backup1
export: /export/test1/backup3 mount: /zba/test1/backup3
export: /export/test1/backup5 mount: /zba/test1/backup5
export: /export/test1/backup7 mount: /zba/test1/backup7
server: aie-zba-h2-stor
path: 192.168.30.101
```

```
export: /export/test1/backup2 mount: /zba/test1/backup2
export: /export/test1/backup4 mount: /zba/test1/backup4
export: /export/test1/backup6 mount: /zba/test1/backup6
export: /export/test1/backup8 mount: /zba/test1/backup8<br/>
```

6. Pour la configuration de groupe IPMP (tous les autres) :

```
server: aie-zba-h1-stor
path: 192.168.30.100
path: 192.168.30.102
path: 192.168.30.104
path: 192.168.30.106
export: /export/test1/backup1 mount: /zba/test1/backup1
export: /export/test1/backup3 mount: /zba/test1/backup3
export: /export/test1/backup5 mount: /zba/test1/backup5
export: /export/test1/backup7 mount: /zba/test1/backup7
server: aie-zba-h2-stor
path: 192.168.30.101
path: 192.168.30.103
path: 192.168.30.105
path: 192.168.30.107
export: /export/test1/backup2 mount: /zba/test1/backup2
export: /export/test1/backup4 mount: /zba/test1/backup4
export: /export/test1/backup6 mount: /zba/test1/backup6
export: /export/test1/backup8 mount: /zba/test1/backup8
```

7. Redémarrez l'instance du logiciel de base de données Oracle.

Réglage de l'instance de base de données Oracle pour la sauvegarde et la restauration Oracle RMAN

L'optimisation des opérations de sauvegarde et de restauration à bande passante élevée à l'aide d'Oracle RMAN et de l'appareil ZFS Storage nécessite de régler les paramètres d'instance qui contrôlent la mise en tampon E/S. Pour plus d'informations sur le réglage de ces paramètres, reportez-vous à l'article ID 1072545.1 : "Réglage des performances de RMAN à l'aide des paramètres de mémoire tampon" via [My Oracle Support \(http://support.oracle.com\)](http://support.oracle.com).

Pour Oracle SPARC SuperCluster, le réglage des quatre paramètres suivants doit être envisagé :

- `_backup_disk_bufcnt` - Nombre de tampons utilisés pour traiter les jeux de sauvegardes
- `_backup_disk_bufsz` - Taille des tampons utilisés pour traiter les jeux de sauvegardes
- `_backup_file_bufcnt` - Nombre de tampons utilisés pour traiter les copies d'images
- `_backup_file_bufsz` - Taille des tampons utilisés pour traiter les copies d'images

Pour les opérations de sauvegarde et de restauration sur les jeux de sauvegarde et les copies d'image, définissez le nombre de tampons sur 64 et la taille des tampons sur 1 Mo :

```
SQL> alter system set "_backup_disk_bufcnt"=64;
SQL> alter system set "_backup_file_bufcnt"=64;
SQL> alter system set "_backup_disk_bufsz"=1048576;
SQL> alter system set "_backup_file_bufsz"=1048576;
```

Ces commandes peuvent être configurées de manière permanente en les ajoutant à SPFILE ou définies dynamiquement dans le bloc d'exécution Oracle RMAN utilisé pour exécuter les opérations de sauvegarde et de restauration.

Les fragments de code suivants montrent comment régler dynamiquement le nombre et la taille des tampons pour les opérations de sauvegarde et de restauration.

- Sauvegarde de jeux de sauvegardes :

```
run
{<br/>
  sql 'alter system set "_backup_disk_bufcnt"=64';<br/>
  sql 'alter system set "_backup_disk_bufsz"=1048576';<br/>
  allocate channel...
...<br/>
  backup as backupset database;
}
```

- Restauration de jeux de sauvegardes :

```
run
{<br/>
  sql 'alter system set "_backup_disk_bufcnt"=64';<br/>
  sql 'alter system set "_backup_disk_bufsz"=1048576';<br/>
  allocate channel...
...<br/>
  restore database;
}
```

- Sauvegarde de copies d'images :

```
run
{<br/>
  sql 'alter system set "_backup_file_bufcnt"=64';<br/>
  sql 'alter system set "_backup_file_bufsz"=1048576';<br/>
  allocate channel...
...<br/>
  backup as copy database;
}
```

- Restauration de copies d'images :

```
run
{<br/>
  sql 'alter system set "_backup_file_bufcnt"=64';<br/>
  sql 'alter system set "_backup_file_bufsz"=1048576';<br/>
  allocate channel...
...<br/>
  restore database;
}
```

L'exécution d'une sauvegarde appliquée de manière incrémentielle nécessite la lecture d'un jeu de sauvegardes incrémentielles et l'écriture d'une copie d'image. Pour régler les tampons pour les sauvegardes appliquées de manière incrémentielle, exécutez ce qui suit :

```
run
{<br/>
  sql 'alter system set "_backup_disk_bufcnt"=64';<br/>
  sql 'alter system set "_backup_disk_bufsz"=1048576';<br/>
  sql 'alter system set "_backup_file_bufcnt"=64';<br/>
  sql 'alter system set "_backup_file_bufsz"=1048576';<br/>
  allocate channel...
...<br/>
  recover copy of database;
}
```

Création de services dédiés pour les opérations Oracle RMAN

Deux services dédiés au traitement d'Oracle RMAN peuvent être configurés pour optimiser la gestion de l'équilibrage de charge, de la haute disponibilité et des mises à jour. La charge de ces services peut être équilibrée de manière équitable sur tous les noeuds d'un système Oracle SPARC SuperCluster. La disponibilité et les performances peuvent être optimisées en configurant l'exécution des services sur une instance préférée tout en les préparant au basculement vers toute autre instance du cluster. Si ces services sont configurés, la mise à niveau d'un quart ou d'un demi-rack du système Oracle SPARC SuperCluster ne nécessite pas de changer la chaîne de connexion du bloc d'exécution d'Oracle RMAN.

L'utilitaire `srvctl` permet d'installer des services pour le traitement Oracle RMAN. Le fragment de code suivant montre comment créer deux services répartis de manière égale sur un cluster à quatre noeuds qui sont configurés pour le basculement vers tout autre noeud du cluster. Dans cet exemple, les services sont installés pour une base de données nommée `dbname` et sont nommés `dbname_bkup`.

```
srvctl add service -d dbname -r dbname1 -a dbname2 -s dbname_bkup1
srvctl start service -d dbname -s dbname_bkup1
srvctl add service -d dbname -r dbname2 -a dbname1 -s dbname_bkup2
srvctl start service -d dbname -s dbname_bkup2
```

Configuration d'Oracle RMAN

La configuration du canal Oracle RMAN et du parallélisme inclut la spécification des cibles du système de fichiers pour les canaux de sauvegarde Oracle RMAN et le nombre total de canaux utilisés pour les opérations de sauvegarde et de restauration. Vous pouvez augmenter les performances en configurant 16 canaux Oracle RMAN qui couvrent les partages disponibles de l'appareil ZFS Storage. Configurez les canaux Oracle RMAN de sorte qu'ils soient distribués de manière égale sur les instances et les noeuds de la base de données Oracle dans le cluster RAC et distribués de manière égale sur les partages exportés à partir de l'appareil ZFS Storage.

Les fragments de code suivants présentent des exemples de blocs d'exécution Oracle RMAN pour l'exécution des opérations de sauvegarde et de restauration des jeux de sauvegardes et des copies d'images ainsi que l'application des fusions incrémentielles sur les copies d'images. L'exemple de code est basé sur la configuration de base de données suivante :

- Nom de la base de données : dbname
- Connexion SYSDBA : sys/welcome
- Adresse SCAN : ad01-scan
- Noms de service de la sauvegarde : dbname_bkup

L'appareil ZFS Storage peut être configuré dans une configuration à un pool dans laquelle l'appareil exporte huit partages utilisés comme huit points de montage.

Les blocs d'exécution Oracle RMAN pour la sauvegarde et la restauration des jeux de sauvegardes et des copies d'images sont présentés dans les exemples des sections ci-dessous. Dans ces exemples, les points de montage de la configuration à quatre partages sont accessibles de /zfssa/dbname/backup1 à /zfssa/dbname/backup4. De plus, les exemples correspondent à une configuration dans laquelle l'appareil ZFS Storage exporte quatre partages utilisés comme quatre points de montage pour 16 canaux Oracle RMAN.

Sauvegarde de jeux de sauvegarde de niveau 0 :

```
run
{<br/>
  sql 'alter system set "_backup_disk_bufcnt"=64 scope=memory';<br/>
  sql 'alter system set "_backup_disk_bufsz"=1048576 scope=memory';<br/>
  allocate channel ch01 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch02 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch03 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup3/%U';<br/>
  allocate channel ch04 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch05 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch06 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch07 device type disk connect 'sys/welcome@ad01-<br/>
```

```

scan/dbname_bkup1' format '/zfssa/dbname/backup3/%U';<br/>
allocate channel ch08 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup4/%U';<br/>
allocate channel ch09 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup2/%U';<br/>
allocate channel ch10 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup1/%U';<br/>
allocate channel ch11 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup4/%U';<br/>
allocate channel ch12 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup3/%U';<br/>
allocate channel ch13 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup2/%U';<br/>
allocate channel ch14 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup1/%U';<br/>
allocate channel ch15 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup4/%U';<br/>
allocate channel ch16 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup3/%U';<br/>
configure snapshot controlfile name to<br/>
'/zfssa/dbname/backup1/snapcf_dbname.f';<br/>
backup as backupset incremental level 0 section size 32g database<br/>
tag 'FULLBACKUPSET_L0' plus archivelog tag 'FULLBACKUPSET_L0';
}

```

Sauvegarde de jeux de sauvegarde de niveau 1 :

```

run
{<br/>
  sql 'alter system set "_backup_disk_bufcnt"=64 scope=memory';<br/>
  sql 'alter system set "_backup_disk_bufsz"=1048576 scope=memory';<br/>
  allocate channel ch01 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch02 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch03 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup3/%U';<br/>
  allocate channel ch04 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch05 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch06 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch07 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup3/%U';<br/>
  allocate channel ch08 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch09 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch10 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch11 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch12 device type disk connect 'sys/welcome@ad01-<br/>

```

```

scan/dbname_bkup2' format '/zfssa/dbname/backup3/%U';<br/>
allocate channel ch13 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup2/%U';<br/>
allocate channel ch14 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup1/%U';<br/>
allocate channel ch15 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup1' format '/zfssa/dbname/backup4/%U';<br/>
allocate channel ch16 device type disk connect 'sys/welcome@ad01-<br/>
scan/dbname_bkup2' format '/zfssa/dbname/backup3/%U';<br/>
configure snapshot controlfile name to<br/>
'/zfssa/dbname/backup1/snapcf_dbname.f';<br/>
backup as backupset incremental level 1 database tag<br/>
'FULLBACKUPSET_L1' plus archivelog tag 'FULLBACKUPSET_L1';
}

```

Sauvegarde de copies d'images :

```

run
{<br/>
  sql 'alter system set "_backup_file_bufcnt"=64 scope=memory';<br/>
  sql 'alter system set "_backup_file_bufsz"=1048576 scope=memory';<br/>
  allocate channel ch01 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch02 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch03 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup3/%U';<br/>
  allocate channel ch04 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch05 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch06 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch07 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup3/%U';<br/>
  allocate channel ch08 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch09 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch10 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch11 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch12 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup3/%U';<br/>
  allocate channel ch13 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup2/%U';<br/>
  allocate channel ch14 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup1/%U';<br/>
  allocate channel ch15 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1' format '/zfssa/dbname/backup4/%U';<br/>
  allocate channel ch16 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2' format '/zfssa/dbname/backup3/%U';<br/>
  configure snapshot controlfile name to<br/>
}

```

```

'/zfssa/dbname/backup1/snapcf_dbname.f';<br/>
backup incremental level 1 for recover of copy with tag 'IMAGECOPY'<br/>
database;
}

```

Fusion incrémentielle de copies d'images :

```

run
{<br/>
  sql 'alter system set "_backup_disk_bufcnt"=64 scope=memory';<br/>
  sql 'alter system set "_backup_disk_bufsz"=1048576 scope=memory';<br/>
  sql 'alter system set "_backup_file_bufcnt"=64 scope=memory';<br/>
  sql 'alter system set "_backup_file_bufsz"=1048576 scope=memory';<br/>
  allocate channel ch01 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch02 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch03 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch04 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch05 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch06 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch07 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch08 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch09 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch10 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch11 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch12 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch13 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch14 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch15 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch16 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  configure snapshot controlfile name to<br/>
  '/zfssa/dbname/backup1/snapcf_dbname.f';<br/>
  recover copy of database with tag 'IMAGECOPY';
}

```

Validation de restauration :

```
run
```



```

{<br/>
  sql 'alter system set "_backup_disk_bufcnt"=64 scope=memory';<br/>
  sql 'alter system set "_backup_disk_bufsz"=1048576 scope=memory';<br/>
  sql 'alter system set "_backup_file_bufcnt"=64 scope=memory';<br/>
  sql 'alter system set "_backup_file_bufsz"=1048576 scope=memory';<br/>
  allocate channel ch01 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch02 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch03 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch04 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch05 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch06 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch07 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch08 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch09 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch10 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch11 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch12 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch13 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch14 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  allocate channel ch15 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup1';<br/>
  allocate channel ch16 device type disk connect 'sys/welcome@ad01-<br/>
  scan/dbname_bkup2';<br/>
  configure snapshot controlfile name to<br/>
  '/zfsa/dbname/backup1/snapcf_dbname.f';<br/>
  restore validate database;
}

```

Configuration d'Oracle SPARC SuperCluster pour la sauvegarde d'un appareil

Pour configurer Oracle SPARC SuperCluster pour la sauvegarde d'un appareil, reportez-vous aux sections suivantes :

- [Configuration de la sauvegarde de l'appareil pour SuperCluster](#)
- [Configuration de la structure de répertoires pour monter les partages sur l'hôte](#)

- Mise à jour du fichier `/etc/vfstab`
- Activation du service client NFS
- Mise à jour d'`orantstab` pour accéder aux exportations de l'appareil ZFS Storage
- Montage des partages sur l'hôte
- Configuration de la propriété des partages montés

▼ Configuration de la structure de répertoires pour monter les partages sur l'hôte

- Configurez les points de montage pour les partages sur l'hôte, comme indiqué :

```
mkdir -p /zfssa/dbname/backup1
mkdir -p /zfssa/dbname/backup2
mkdir -p /zfssa/dbname/backup3
mkdir -p /zfssa/dbname/backup4
```

▼ Mise à jour du fichier `/etc/vfstab`

Le caractère d'échappement sur une nouvelle ligne (`\`) d'UNIX indique qu'une ligne de code a été répartie sur deux lignes dans la liste ci-dessous. Lorsque vous saisissez une ligne de code répartie sur deux lignes dans `fstab`, supprimez le caractère `\` et rassemblez les segments des deux lignes, séparés par un espace, en une seule ligne.

1. Utilisez l'une des options suivantes pour mettre à jour le fichier `/etc/vfstab`.

Pour une configuration à un pool :

```
192.168.36.200:/export/dbname/backup1 - /zfssa/dbname/backup1 \<br/>
nfs - yes rw,bg,hard,nointr,rsz=1048576,wsz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup2 - /zfssa/dbname/backup2 \<br/>
nfs - yes rw,bg,hard,nointr,rsz=1048576,wsz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup3 - /zfssa/dbname/backup3 \<br/>
nfs - yes rw,bg,hard,nointr,rsz=1048576,wsz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup4 - /zfssa/dbname/backup4 \<br/>
nfs - yes rw,bg,hard,nointr,rsz=1048576,wsz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio
```

2. *Pour une configuration à deux pools :*

```
192.168.36.200:/export/dbname/backup1 - /zfssa/dbname/backup1 \<br/>
nfs - yes rw,bg,hard,nointr,rsz=1048576,wsz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio
```

```

192.168.36.201:/export/dbname/backup2 - /zfssa/dbname/backup2 \<br/>
nfs - yes rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio
192.168.36.200:/export/dbname/backup3 - /zfssa/dbname/backup3 \<br/>
nfs - yes rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio
192.168.36.201:/export/dbname/backup4 - /zfssa/dbname/backup4 \<br/>
nfs - yes rw,bg,hard,nointr,rsiz=1048576,wsiz=1048576,proto= \<br/>
tcp,vers=3,forcedirectio

```

▼ Activation du service client NFS

- **Activez le service client NFS sur l'hôte Solaris 11 à l'aide de la commande suivante :**

```
svcadm enable -r nfs/client
```

▼ Mise à jour d'oranstab pour accéder aux exportations de l'appareil ZFS Storage

Pour mettre à jour le fichier oranstab pour accéder aux exportations de l'appareil ZFS Storage, utilisez l'option appropriée suivante.

1. *Pour une configuration à un pool :*

```

server: 192.168.36.200
path: 192.168.36.200
path: 192.168.36.201
path: 192.168.36.202
path: 192.168.36.203
export: /export/dbname/backup1 mount: /zfssa/dbname/backup1
export: /export/dbname/backup2 mount: /zfssa/dbname/backup2
export: /export/dbname/backup3 mount: /zfssa/dbname/backup3
export: /export/dbname/backup4 mount: /zfssa/dbname/backup4

```

2. *Pour une configuration à deux pools :*

```

server: 192.168.36.200
path: 192.168.36.200
path: 192.168.36.202
export: /export/dbname/backup1 mount: /zfssa/dbname-2pool/backup1
export: /export/dbname/backup3 mount: /zfssa/dbname-2pool/backup3
server: 192.168.36.201
path: 192.168.36.201
path: 192.168.36.203
export: /export/dbname/backup2 mount: /zfssa/dbname-2pool/backup2
export: /export/dbname/backup4 mount: /zfssa/dbname-2pool/backup4

```

▼ Montage des partages sur l'hôte

- **Montez les partages manuellement à l'aide de la commande Solaris `mount` standard :**

```
# mount /zfssa/dbname/backup1
# mount /zfssa/dbname/backup2
# mount /zfssa/dbname/backup3
# mount /zfssa/dbname/backup4
```

▼ Configuration de la propriété des partages montés

Modifiez les paramètres d'autorisation des partages montés pour correspondre aux paramètres d'autorisation de `ORACLE_HOME`. Dans cet exemple, les propriétés d'utilisateur et de groupe sont définies sur `oracle:dba`.

1. **Saisissez :**
`<br /># chown oracle:dba /zfssa/dbname/*`
2. **Redémarrez l'instance de base de données Oracle pour reprendre les modifications apportées au fichier `oranfstab` à l'aide de l'une des options suivantes :**
 - Redémarrez une instance à la fois (mise à niveau non simultanée), par exemple :
 - `:$ srvctl stop instance -d dbname -i dbname1`
 - `:$ srvctl start instance -d dbname -i dbname1`
 - `:$ srvctl stop instance -d dbname -i dbname2`
 - `:$ srvctl start instance -d dbname -i dbname2`
 - `:$ srvctl stop instance -d dbname -i dbname3`
 - `:$ srvctl start instance -d dbname -i dbname3`
 - `:$ srvctl stop instance -d dbname -i dbname4`
 - `:$ srvctl start instance -d dbname -i dbname4`
 - `:$ srvctl stop instance -d dbname -i dbname5`
 - `:$ srvctl start instance -d dbname -i dbname5`
 - `:$ srvctl stop instance -d dbname -i dbname6`
 - `:$ srvctl start instance -d dbname -i dbname6`
 - `:$ srvctl stop instance -d dbname -i dbname7`
 - `:$ srvctl start instance -d dbname -i dbname7`
 - `:$ srvctl stop instance -d dbname -i dbname8`
 - `:$ srvctl start instance -d dbname -i dbname8`
 - Redémarrez l'ensemble de la base de données, par exemple :

- `:$ srvctl stop database -d dbname`
- `:$ srvctl start database -d dbname`

Protocole OISP (Oracle Intelligent Storage Protocol)

Le protocole OISP Oracle Intelligent Storage Protocol permet au client Oracle direct NFS (dNFS) de coder et de transmettre les attributs associés aux demandes d'E/S à l'appareil Oracle ZFS Storage. Ces attributs comportent des informations comme le type de fichier de base de données que la demande d'E/S cible, la taille d'enregistrement du fichier, et l'identité de la base de données émettant la demande d'E/S.

L'appareil Oracle ZFS Storage décode ces attributs et les utilise pour simplifier la configuration de la base de données, augmente les performances de cette base de données et fournit une large visibilité de la source des charges de travail des E/S générées par les clients de la base de données.

Taille des enregistrements de la base de données

Le client Oracle dNFS peut transmettre la taille optimale d'enregistrement en fonction du type de fichier pour chaque demande d'E/S. Si la taille d'un enregistrement est transmise, elle remplace la définition de propriété "taille d'enregistrement de base de données" sur le partage ou le projet. Vous pouvez définir la taille d'un enregistrement uniquement pour les nouveaux fichiers créés. Si un fichier existe déjà, la taille d'enregistrement n'est pas modifiée.

Indice de décalage d'écriture synchrone

Le client dNFS Oracle peut transmettre un indice de décalage associé avec les demandes d'écriture d'E/S qui invite l'appareil Oracle ZFS Storage à traiter les demandes d'E/S soit comme sensibles à la latence, soit orientées débit. Si l'indice est transmis, elle remplace le réglage de propriété "décalage d'écriture synchrone" sur le partage ou le projet.

Ventilation des analyses par nom de base de données

Le client Oracle 12c dNFS peut transmettre l'identification de la base de données (SID) ou de la base de données de conteneur et de la base de données pluggable (SID:SID) ayant émis les demandes d'E/S. Les analyses de l'appareil Oracle ZFS Storage permettent de ventiler les statistiques par nom(s) SID de la base de données, en sélectionnant la ventilation ou l'exploration par "ID d'application".

Clients et protocoles compatibles OISP

Protocoles : NFSv4

Clients: Client Oracle Database NFS (dNFS)

Plug-in ZFS Storage Appliance Network pour Oracle Solaris Cluster

Oracle Solaris Cluster (OCS) est un logiciel de cluster haute disponibilité pour le système d'exploitation Oracle Solaris.

Le plug-in Sun ZFS Storage Appliance Network File System Plug In for Oracle Solaris Cluster permet l'utilisation d'OSC avec l'appareil par le biais du protocole NFS. Le plug-in et le fichier readme sont disponibles dans le cadre du plug-in Oracle ZFS Storage Appliance Network File System pour Oracle Solaris Cluster sur Oracle Technology Network.

Appliance Plug-in for Oracle Solaris Cluster Geographic Edition

Oracle Solaris Cluster Geographic Edition est une extension en couches du logiciel Oracle Solaris Cluster. Le logiciel Geographic Edition protège les applications des perturbations inattendues grâce à plusieurs clusters séparés par de longues distances mais également à une infrastructure redondante qui réplique les données entre les sites du cluster. Ce plug-in coordonne la réplication des données entre les sites Oracle Solaris Cluster distants à l'aide du service de réplication distante de l'appareil.

Le package de plug-in est disponible sur la page d'informations Oracle Technology Network Sun NAS Storage.

Appliance Plug-in for Oracle Enterprise Manager System Monitoring

Oracle ZFS Storage Plug-in for Oracle Enterprise Manager System Monitoring offre à l'environnement de Grid Controller un contrôle de premier plan de la famille d'appareils Oracle ZFS Storage Appliance. Le plug-in peut :

- Surveiller Oracle ZFS Storage Appliance

- Collecter des informations sur le système de stockage, sur la configuration et sur les performances des composants de stockage accessibles
- Déclencher des alertes et des violations en fonction de seuils et d'informations de surveillance collectés par l'outil
- Fournir des rapports prêts à l'emploi qui complètent la fonction Analyse
- Prendre en charge la surveillance par des agents distants

Lorsqu'un appareil est configuré pour être surveillé par Grid Control, des feuilles de travail et des ensembles de données Analyse sont créés pour permettre à l'administrateur Grid Control d'accéder au niveau de détail supérieur offert par les analyses en temps réel disponibles au sein de l'appareil.

Le plug-in de gestion est disponible sur le lien suivant : <http://www.oracle.com/technetwork/documentation/index.html>.

Il est fourni avec un guide d'installation qui doit être lu par les administrateurs Grid Control et les administrateur de stockage des appareils surveillés.

Deux workflows sont inclus avec chaque appareil et servent respectivement à préparer un système pour la surveillance et à supprimer les artefacts créés pour l'environnement de surveillance :

- Configuration pour la surveillance d'Oracle Enterprise Manager
- Annuler la configuration de la surveillance d'Oracle Enterprise Manager

Ces workflows sont accessibles depuis la page Maintenance > Workflows de l'interface utilisateur du navigateur.

Configuration pour la surveillance d'Oracle Enterprise Manager

Ce workflow permet de préparer un environnement pour la surveillance ou de restaurer l'état d'origine des artefacts créés par le workflow, dans l'hypothèse où ils auraient été modifiés par l'administrateur de stockage pendant le fonctionnement de l'appareil. L'exécution de ce workflow apporte les modifications suivantes au système :

- Une propriété de rôle *oracle_agent* disposant d'un accès limité au système est créé, pour permettre à l'agent Oracle Enterprise Manager Grid Controller d'obtenir les informations requises pour la surveillance sans altérer le système. Un utilisateur *oracle_agent* sera créé et le rôle correspondant lui sera affecté. L'utilisation de ce rôle et de cet utilisateur est cruciale pour conserver des enregistrements d'audit propres consignait le moment et la manière dont l'agent accède au dispositif.
- Analyse avancée est activé et fournit un ensemble étendu de statistiques à tous les utilisateurs de l'appareil Oracle ZFS Storage.

- La feuille de travail *Oracle Enterprise Manager* est créée et facilite la communication entre l'administrateur Grid Controller et l'administrateur de stockage. Toutes les mesures surveillées par Grid Controller sont disponibles depuis cette feuille de travail.

Annulation de la configuration de la surveillance d'Oracle Enterprise Manager

Ce workflow supprime les artefacts créés par le workflow *Configuration pour la surveillance d'Oracle Enterprise Manager*. En particulier, il :

- Supprime le rôle et l'utilisateur *oracle_agent* ;
- Supprime la feuille de travail *Oracle Enterprise Manager*

Ce workflow ne désactive pas Analyse avancée ou les éventuels ensembles de données activés à des fins de collecte.

Appliance Plug-in for Oracle Virtual Machine Storage Connect

Une des nombreuses nouvelles fonctions d'Oracle VM 3.0 est la structure Storage Connect. Cette structure permet à Oracle VM 3.0 Manager d'accéder directement à des serveurs de stockage et d'allouer des ressources. Elle vous permet d'enregistrer des serveurs de stockage, de détecter les ressources de stockage existantes, de créer et présenter des disques physiques aux pools de serveurs et de partager des référentiels de stockage et des machines virtuelles.

Oracle Virtual Machine Storage Connect Plug-in for the Oracle ZFS Storage Appliance est un composant de la suite logicielle Oracle VM qui permet à Oracle VM de provisionner et de gérer l'appareil Sun ZFS Storage pour la virtualisation. Le plug-in est installé sur le ou les serveurs Oracle VM et communique avec le ou les serveurs de stockage par le biais de workflows installés sur l'appareil.

Le plug-in et le fichier README sont disponibles sur [Oracle Technology Network](#).

Appliance Plug-in Provider for Volume Shadow Copy Service Software

Volume Shadow Copy Services (VSS) pour les systèmes d'exploitation Microsoft fournit une structure permettant d'effectuer des sauvegardes de volumes alors que les applications

d'un système continuant d'écrire dans ces volumes. VSS fournit une interface cohérente qui permet la coordination entre les applications utilisateur qui mettent à jour les données sur disque (enregistreurs VSS) et celles qui sauvegardent les applications (demandeurs VSS). En particulier, VSS fournit :

- Une infrastructure de sauvegarde qui coordonne les applications et les activités du système de fichiers
- Un emplacement où créer des copies ponctuelles et amalgamées appelées *copies Shadow*.

Oracle ZFS Storage Appliance Provider For Volume Shadow Copy Service Software est un fournisseur matériel VSS qui permet à l'appareil Oracle ZFS Storage de prendre des instantanés cohérents pour des hôtes Windows utilisant des cibles de blocs. VSS coordonne les instantanés pour garantir la cohérence des données par blocs. Le fournisseur communique avec un ensemble de workflows sur l'appareil pour coordonner la prise d'instantanés tels qu'observés depuis l'application. Il fonctionne via iSCSI et Fibre Channel.

Oracle ZFS Storage Appliance Provider For Volume Shadow Copy Service Software est installé sur les hôtes qui ont besoin de cette fonctionnalité, ainsi que d'une coordination entre les applications. La documentation complète de cette intégration d'application est fournie avec les composants téléchargés sous la forme d'un fichier readme. Le logiciel et le fichier readme du fournisseur sont compris dans le patch Oracle ZFS Storage Software Providers and Plug-Ins disponible sur [Oracle Technology Network](http://www.oracle.com/technetwork/) Plus d'informations sur VSS sont disponibles sur le site Web de Microsoft : <http://msdn.microsoft.com/en-us/library/aa384649>

Prise en charge FC avec Symantec Dynamic Multi-Pathing et Storage Foundation

- **SF** - Symantec Storage Foundation 5.1
- **SF HA** - Storage Foundation High Availability 5.1
- **SFCFS/SF Oracle RAC** - Storage Foundation Cluster File System/Storage Foundation for Oracle RAC 5.1
- **SFCFS/SFCFS Oracle RAC** - Storage Foundation Cluster File System/Storage Foundation Cluster File System for Oracle RAC 5.1
- Solaris 10 SPARC
- Solaris 10 x86
- Linux RedHat5
- Oracle Enterprise Linux (OEL)

Reportez-vous à la liste de compatibilité matérielle de Symantec : [Note technique matérielle des solutions Symantec Storage Foundation et High Availability \(http://www.symantec.com/business/support/index?page=content&id=TECH47728\)](http://www.symantec.com/business/support/index?page=content&id=TECH47728).

Notez les restrictions suivantes :

- Les bibliothèques ASL d'appareil "requisites" par Symantec doivent être installées et peuvent être téléchargées à l'adresse : <https://vos.symantec.com/asl>
- Symantec requiert également le niveau de patch SF 5.1 VM de 5.1RP2 ou supérieur, qui peut être téléchargé à l'adresse : <https://vos.symantec.com/patch/matrix>
- Symantec nécessite également la configuration des paramètres DMP suivants (uniquement pour les appareils en cluster) :
 - :dmp_health_time=0
 - :dmp_path_age=0
 - :dmp_lun_retry_timeout=200

Reportez-vous à la note technique matérielle de Symantec qui référence les paramètres d'appareil mis en cluster : [Symantec Technical Support \(http://www.symantec.com/business/support/index?page=content&id=TECH74012\)](http://www.symantec.com/business/support/index?page=content&id=TECH74012).

Symantec's Storage Foundation 5.1SP2 for Windows prend en charge les connexions FC à Oracle ZFS Storage Appliance pour les versions suivantes de Windows :

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Reportez-vous à la liste de compatibilité matérielle SF 5.1SP2 : [Hardware Compatibility List \(HCL\) for Symantec Storage Foundation \(http://www.symantec.com/business/support/index?page=content&id=TECH138719\)](http://www.symantec.com/business/support/index?page=content&id=TECH138719)

Appliance Replication Adapter for VMware Site Recovery Manager

SRA (Storage Replication Adapter) Oracle ZFS Storage Appliance pour SRM (Site Recovery Manager) VMware vCenter s'intègre à l'appareil Oracle ZFS Storage Appliance dans les déploiements VMware s'étendant sur plusieurs sites et nécessitant une restauration rapide en cas d'interruption de service de site protégé. SRA se connecte aux environnements VMware vCenter SRM existants et permet aux appareils Oracle ZFS Storage Appliance d'être gérés par le biais des séquences de détection, de test et de basculement de VMware vCenter SRM lors du test et de l'exécution du plan de récupération. L'utilisation de SRA se déroule entièrement dans l'application VMware vCenter SRM.

L'administrateur VMware doit travailler en étroite collaboration avec l'administrateur de l'appareil Oracle ZFS Storage Appliance responsable de l'appareil qui héberge les magasins de données VMware. Pour plus d'informations, reportez-vous au manuel Oracle ZFS Storage Appliance SRA for VMware SRM Administration Guide fourni avec SRA.

Remarque - Vous pouvez télécharger SRA depuis Oracle Technology Network. Un contrat de support Oracle valide pour l'appareil Oracle ZFS Storage Appliance est requis pour obtenir SRA.
