Guide d'administration des systèmes Oracle ZFS Storage Appliance

Référence : E50421
Octobre 2013 E50421–01

Copyright © 2009-2013 , 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 disposition de votre contrat de licence ou de la loi, vous ne pouvez pas copier, reproduire, traduire, diffuser, modifier, breveter, 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 concédé sous licence au Gouvernement des Etats-Unis, ou à toute entité qui délivre la licence de ce logiciel ou l'utilise 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 des 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 ce type d'applications.

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. 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.

140218@25097

Table des matières

Préface 17

1 **Introduction** 19
Overview 19
Présentation 19
User Interface 23
Interface utilisateur de navigateur (BUI, Browser User Interface) 23
Interface de ligne de commande (CLI, Command Line Interface) 24
Browsers 24
Navigateurs pris en charge 24
Main Window 25
Présentation 25
Cadre masthead 25
Barre de titre 26
Panneaux latéraux et titres de menus 27
Liste des contrôles non standard de la BUI 28
Icons 30
Utilisation générale 30
CLI 34
Introduction à la CLI 34
Voir aussi 35
Contexts 35
Contextes de la CLI 35
Retour à un contexte antérieur 37
Accès à un contexte parent 38
Contextes et saisie semi-automatique par tabulation 38
Exécution de commandes spécifiques au contexte 39
Contextes non validés 39

Properties 40
Propriétés de la CLI 40
Obtention de propriétés 40
Définition des propriétés 41
Propriétés inaltérables 42
Scripting 43
Commandes de traitement par lots 43
Ecriture de scripts 44
Automatisation de l'accès 50

2 Statut 51
Status 51
Statut 51
Dashboard 52
Liens 52
CLI 57
Tâches 59
Voir aussi 59
Settings 59
Paramètres 59
BUI 59
CLI 61
Tâches 61
Voir aussi 62
NDMP 62
BUI 62
CLI 64
Voir aussi 64

3 Configuration 65
Configuration 65
Introduction 65
Initial 66
Configuration initiale 66
Conditions préalables 66

Résumé 66
BUI 67
CLI 67
Network 72
Configuration réseau 73
BUI 83
CLI 85
Tâches 87
Storage 92
Stockage 93
Tâches 99
SAN 100
SAN 100
BUI 101
CLI 102
Terms 102
Terminologie SAN 102
FC 103
Fibre Channel 103
BUI 107
CLI 109
FCMPxIO 112
Configuration de la gestion des chemins d'accès multiples pour client FC 112
Tâches 112
iSCSI 119
Introduction 119
Tâches 122
CLI 123
SRP 124
Introduction 124
Tâches 128
CLI 131
Users 132
Utilisateurs 132
Rôles 132
Autorisations 132

Propriétés 133
BUI 134
CLI 135
Tâches 137
Preferences 139
Préférences 139
BUI 140
CLI 140
Clés publiques SSH 141
Alerts 141
Alertes 141
Actions 142
Alertes avec seuil 144
BUI 145
CLI 145
Tâches 146
Voir aussi 146
Cluster 147
Clustering 147
Fonctions et avantages 147
Inconvénients 148
Terminologie 149
Conception du sous-système 150
Modifications de la configuration dans un environnement clusterisé 157
Considérations relatives au clustering pour le stockage 158
Considérations relatives au clustering pour la gestion réseau 160
Considérations relatives au clustering pour Infiniband 162
Prévention des conditions 'split-brain' 163
Estimation et réduction de l'impact de la reprise 165
Tâches 167
Arrêter de la configuration clusterisée 169
Câblage de noeuds 170
Câblage des JBOD 171
BUI 171
Tâches 173

4 Services 175
Services 175
Introduction 175
BUI 178
CLI 180
NFS 183
Introduction 183
Propriétés 184
Domaines Kerberos 185
Journaux 186
Analyse 187
CLI 187
Tâches 188
Voir aussi 188
iSCSI 188
Introduction 188
Propriétés 189
Authentification 189
Autorisation 189
Cibles et initiateurs 189
CLI 189
Conseils 190
Voir aussi 190
SMB 191
Introduction 191
Propriétés 191
Propriétés des partages 192
Interopérabilité NFS/SMB 193
Espaces de noms DFS 193
Tâches 194
Règles autohome 194
Groupes locaux 195
Comptes locaux 195
Intégration de MMC 195
CLI 200
Tâches 201

Voir aussi 203
FTP 204
Introduction 204
Propriétés 204
Journaux 205
Tâches 205
Voir aussi 206
HTTP 206
Introduction 206
Propriétés 206
Authentification et contrôle d'accès 207
Journaux 207
Tâches 208
Voir aussi 208
NDMP 208
Introduction 208
Propriétés 214
Journaux 216
Voir aussi 216
Remote Replication 216
Réplication distante 216
Shadow Migration 217
Migration shadow 217
Propriétés 217
Gestion de la migration shadow 217
SFTP 218
Introduction 218
Propriétés 218
Journaux 219
Tâches 219
Voir aussi 219
SRP 219
Introduction 219
Cibles et initiateurs 220
CLI 220
Voir aussi 220

TFTP 220
Introduction 220
Propriétés 220
Tâches 221
Voir aussi 221
Virus Scan 221
Analyse antivirus 221
Propriétés 221
Journaux 223
Tâches 223
Voir aussi 224
NIS 224
Introduction 224
Propriétés 224
Journaux 225
Tâches 225
Voir aussi 226
LDAP 226
Introduction 226
Propriétés 226
Journaux 228
Tâches 228
Voir aussi 229
Active Directory 229
Introduction 229
Propriétés 229
Domaines et groupes de travail 230
Signature LDAP 230
Prise en charge de Windows Server 2012 231
Prise en charge de Windows Server 2008 231
BUI 232
CLI 232
Tâches 233
Voir aussi 234
Identity Mapping 234
Concepts 234

IDMU 236
Mappage basé sur un annuaire 236
Mappage basé sur un nom 237
Mappage éphémère 239
Pratiques recommandées 239
Test des mappages 240
Exemples 240
Tâches 241
DNS 242
Introduction 242
Propriétés 242
CLI 242
Journaux 243
Active Directory et DNS 243
Résolution non-DNS 243
Fonctionnement sans DNS 244
Voir aussi 244
Dynamic Routing 244
Protocoles de routage dynamiques RIP et RIPng 244
Journaux 245
Voir aussi 245
IPMP 245
Introduction 245
Propriétés 245
Journaux 246
Tâches 246
Voir aussi 246
NTP 246
Introduction 246
Propriétés 246
Horloge de la BUI 249
Conseils 249
Tâches 249
Voir aussi 250
Phone Home 250
Introduction 250

Propriétés 250
Tâches 251
Etat du service 252
Journaux 252
Voir aussi 252
Service Tags 253
Indicateurs de maintenance 253
Propriétés 253
SMTP 253
Introduction 253
Propriétés 254
Journaux 254
Voir aussi 254
SNMP 255
Introduction 255
Propriétés 255
MIB 255
MIB Sun FM 256
MIB Sun AK 257
Tâches 257
Voir aussi 258
Syslog 258
Introduction 258
Propriétés 259
Syslog classique : RFC 3164 259
Syslog mis à jour : RFC 5424 259
Format du message 260
Exemples de configuration du récepteur 262
Voir aussi 263
System Identity 263
Identité du système 263
SSH 264
Introduction 264
Propriétés 264
Journaux 265
Tâches 265

Voir aussi 265

5 Partages 267
Shares 267
Partages 267
Concepts 268
Pools de stockage 268
Projets 269
Partages 269
Propriétés 269
Instantanés 270
Clones 271
Shadow Migration 272
Migration des données shadow 272
Comportement de la migration shadow 274
Gestion de la migration shadow 276
Migration des systèmes de fichiers locaux 280
Tâches 281
Space Management 282
Gestion de l'espace 282
Termes 282
Présentation des instantanés 283
Paramètres du système de fichiers et du projet 285
Paramètres d'utilisateur et de groupe 286
Filesystem Namespace 290
Espace de noms du système de fichiers 290
Shares 292
BUI 292
CLI 298
General 303
Propriétés générales des partages 303
Utilisation de l'espace 304
Propriétés 305
Propriétés personnalisées 311
Protocols 312

Protocoles des partages 312
NFS 312
SMB 317
iSCSI 318
HTTP 319
FTP 319
SFTP 319
Voir aussi 319
Access 320
Contrôle d'accès 320
Accès au répertoire racine 320
Comportement des ACL 321
ACL du répertoire racine 323
Snapshots 326
Instantanés 326
Propriétés des instantanés 326
BUI 327
Tâches 328
CLI 331
Projects 334
BUI 334
CLI 336
General 341
Propriétés générales des projets 341
Utilisation de l'espace 341
Propriétés héritées 342
Propriétés personnalisées 342
Paramètres par défaut de création d'un système de fichiers 342
Paramètres par défaut de création d'une LUN 342
Protocols 343
Protocoles de projet 343
NFS 343
SMB 343
iSCSI 344
HTTP 344
FTP 344

Voir aussi 344
Access 344
Contrôle d'accès 344
Comportement des ACL héritées 344
Snapshots 345
Instantanés 345
Propriétés des instantanés 345
BUI 346
CLI 346
Replication 347
Introduction à la réplication distante 347
Concepts 348
Configuration de la réplication 353
Gestion des packages de réplication 357
Tâches 366
Détails de la réplication distante 370
Schema 378
Propriétés personnalisées des partages 378
BUI 378
CLI 379
Tâches 380

6 Intégration 383
Integration 383
Intégration 383
Symantec 384
Prise en charge FC avec 'DMP' / Storage Foundation de Symantec 384
Oracle Solaris Cluster 385
Plug-in ZFS Storage Appliance Network File System Plug In for Oracle Solaris Cluster .. 385
Oracle Solaris CGeo 385
Sun ZFS Storage Appliance Plug-in for Oracle Solaris Cluster Geographic Edition 385
Microsoft 386
Sun ZFS Storage Appliance Provider For Volume Shadow Copy Service Software 386
Oracle Grid Controller 387
Sun ZFS Storage Management Plug-In for Oracle Enterprise Manager Grid Control 387

Oracle Storage Connect 388
Oracle Virtual Machine Storage Connect Plug-in for the Sun ZFS Storage Appliance 388
VMware Site Recovery Manager 389
Sun ZFS Storage 7000 Storage Replication Adapter for VMware Site Recovery Manager 389
Exadata 389
Oracle Exadata Database Machine 389
Oracle Intelligent Storage Protocol 390
Protocole OISP (Oracle Intelligent Storage Protocol) 390

Glossaire 393

Préface

Le *Guide d'administration des systèmes Oracle ZFS Storage Appliance* contient des informations sur l'administration et la configuration des appareils de la gamme Oracle ZFS Storage Appliance.

Cette documentation est également accessible depuis l'interface utilisateur de navigateur de l'appareil, par un clic sur le bouton Help. La documentation de l'appareil peut être mise à jour à l'aide de la procédure de mise à niveau du système, documentée dans le manuel d'entretien du système.

Utilisateurs de ce manuel

Ces notes sont destinées aux utilisateurs et aux administrateurs qui installent et utilisent les appareils de la gamme Oracle ZFS Storage Appliance.

Documentation connexe

Reportez-vous à la documentation suivante pour obtenir des instructions d'installation, des présentations matérielles, des procédures de maintenance et des remarques sur les mises à jour logicielles.

- Guide d'installation, Guide de la fonction d'analyse et Manuel d'entretien (`http://www.oracle.com/technetwork/documentation/`)

Références à des sites Web tiers connexes

Des URL tierces offrant l'accès à des informations complémentaires sont citées dans ce document.

Remarque – 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. 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.

Accès aux services de support Oracle

Les clients Oracle 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.

◆ ◆ ◆ CHAPITRE 1

1 Introduction

Overview

Présentation

La gamme de produits 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.

Contrôleurs

- ZS3-2
- ZS3-4
- 7120
- 7320
- 7420

Stockage d'extension

- Etagères de disques

Protocoles

Les appareils Oracle ZFS Storage Appliance prennent en charge divers protocoles client usuels dans l'industrie, notamment :

- SMB
- NFS
- HTTP et HTTPS
- WebDAV
- iSCSI
- FC
- SRP
- iSER
- FTP
- SFTP

Fonctions clés

Les systèmes Oracle ZFS Storage intègrent également de nouvelles 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 :

- Analyse, 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

Services de données

Pour gérer les données exportées à l'aide de ces protocoles, vous pouvez configurer le système Oracle ZFS Storage à l'aide de l'ensemble intégré de services de données avancés, comprenant 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) mises en miroir et entrelacées

- Nombre illimité d'instantanés en lecture seule et en lecture-écriture, avec possibilité de planification
- Suppression des doublons de données
- Compression des données intégrée
- Réplication distante des données à des fins de récupération après sinistre
- Clustering actif-actif pour ménager de la haute disponibilité
- Allocation fine des LUN iSCSI
- Analyse antivirus et quarantaine
- Sauvegarde et restauration NDMP

Disponibilité

Pour maximiser la disponibilité de vos données en cours de production, les appareils Oracle ZFS Storage Appliance intègrent 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 fonctions clés incluent :

- Autorétablissement prédictif et diagnostic de toutes les pannes matérielles des systèmes : CPU, DRAM, cartes d'E/S, disques, ventilateurs, sommes de contrôle, 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 ménager de la haute disponibilité
- Groupements de liaisons et multipathing IP pour la protection du réseau contre les pannes
- Multipathing d'E/S entre le contrôleur et les étagères de disques
- Redémarrage logiciel intégré de tous les services logiciels du système
- Service Phone-Home de transmission de télémesures pour tous les problèmes logiciels et matériels
- 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)

L'interface utilisateur de navigateur

La BUI 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.

Le logiciel de gestion est conçu pour être entièrement fonctionnel sur divers navigateurs Web.

Orientez le navigateur vers le système à l'aide de l'adresse IP ou du nom d'hôte que vous avez assigné au port NET0 de la manière suivante : https://adresseip:215 or https://nomhôte: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.

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

La CLI offre les même fonctionnalités que la BUI tout en fournissant un environnement de script performant idéal pour effectuer des tâches répétitives. Les sections suivantes donnent des informations détaillées sur la CLI. Lors de l'utilisation de la CLI, gardez à l'esprit les 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 conjuguer ces deux principes de la manière suivante :

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

User Interface

L'interface utilisateur de navigateur

Interface utilisateur de navigateur (BUI, Browser User Interface)

La BUI 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. Les sections suivantes offrent une présentation de la BUI.

- Fenêtre principale - présentation des éléments et de l'apparence de la BUI
- Icônes - référence d'icône
- Navigateurs - navigateurs pris en charge

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

La CLI offre les même fonctionnalités que la BUI tout en fournissant un environnement de script performant idéal pour effectuer des tâches répétitives. Les sections suivantes donnent des informations détaillées sur la CLI.

- CLI - utilisation
- Contextes - contextes
- Propriétés - propriétés
- Ecriture de scripts - écriture de scripts
- Maintenance:Workflows - workflows

Browsers

Navigateurs pris en charge

Cette section définit les navigateurs pris en charge par la BUI. Pour des résultats optimaux, utilisez un navigateur de niveau 1.

Niveau 1

Le logiciel de la BUI est conçu pour être entièrement fonctionnel sur les navigateurs de niveau 1 suivants :

- Firefox 3.x ou ultérieur
- Internet Explorer 7 ou ultérieur
- Safari 3.1 ou ultérieur
- Google Chrome (stable)
- WebKit 525.13 ou ultérieur

Niveau 2

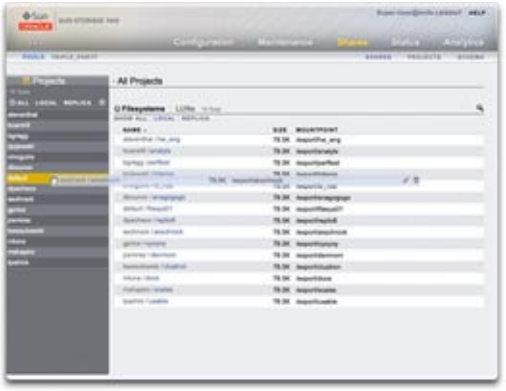
Les éléments de la BUI risquent de s'afficher de manière imparfaite dans les navigateurs de niveau 2 et certaines fonctionnalités risquent d'être indisponibles, mais toutes les fonctions indispensables sont parfaitement opérationnelles. Un message d'avertissement s'affiche pendant la connexion si vous utilisez l'un des navigateurs de niveau 2 suivants :

- Firefox 2.x
- Mozilla 1.7 sous Solaris 10
- Opera 9

Navigateurs non pris en charge

Internet Explorer 6 et les versions antérieures ne sont pas prises en charge et présentent des problèmes connus ; la connexion échoue.

Main Window



Modification des propriétés d'un système de fichiers par déplacement de celui-ci dans un autre projet à l'aide du panneau latéral Projets.

Présentation

La BUI offre un environnement clair permettant de visualiser le comportement du système et d'identifier les problèmes de performances affectant l'appareil.

Cadre masthead

Le cadre masthead contient plusieurs éléments d'interface servant à la navigation et à la notification, ainsi que les fonctionnalités principales. Sur la gauche, du 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 du haut en bas, s'affichent : l'identifiant de connexion, la mention LOGOUT pour la déconnexion, l'aide, les liens de navigation principaux et les liens secondaires.

Navigation

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.

Alertes

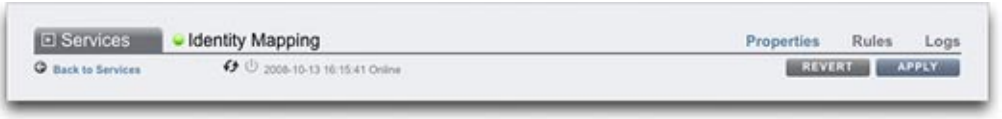
Les alertes système apparaissent dans le Masthead lorsqu'elles sont déclenchées. Si plusieurs alertes sont déclenchées de façon séquentielle, reportez-vous à la liste d'alertes récentes accessible dans l'écran Tableau de bord ou le journal complet disponible dans l'écran Maintenance : journaux.

Annotation de session

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 : utilisateurs pour plus d'informations sur les annotations de session.

Barre de titre

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



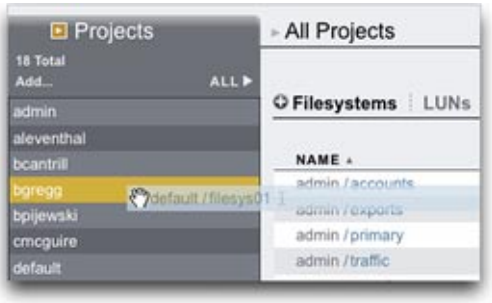
Par exemple, la barre de titre du service Identity Mapping offre les éléments suivants :

- Accès à la liste de services complète par le biais du panneau latéral
- Contrôles permettant d'activer ou de désactiver le service Identity Mapping.
- Vue du temps de fonctionnement d'Identity Mapping

- 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

Panneaux latéraux et titres de menus

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



Main Window Panneaux latéraux et titres de menus

Ajout de projets

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

Déplacement de partages

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 déplacer un partage dans un autre projet aura pour effet de modifier les propriétés du partage si celles-ci sont configurées pour être reprises du projet parent.

Nom d'objet

Pour modifier le nom d'un partage, cliquez sur l'icône de changement de nom dans la ligne de tableau mise en surbrillance correspondant au partage.

Liste des contrôles non standard de la BUI

La plupart des contrôles de la BUI utilisent des entrées de format Web standard. Il y a toutefois quelques exceptions notables :

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 retrait
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
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
Envoyer des commentaires à propos de la BUI	Cliquez sur le lien Commentaires dans l'angle inférieur droit de n'importe quel écran pour nous envoyer vos suggestions à propos de l'interface ou de n'importe quel autre caractéristique de l'appareil

Autorisations

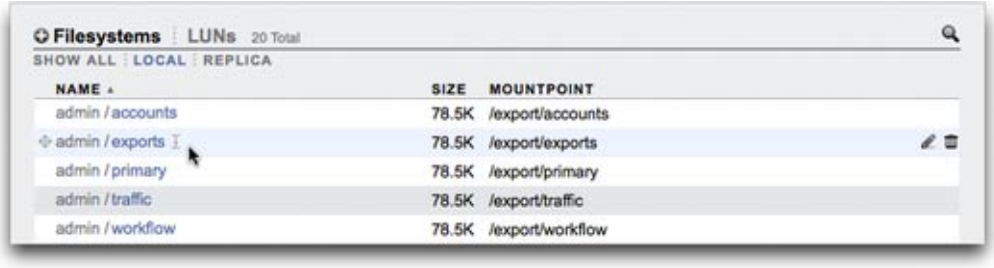
Lors de la définition des autorisations, les rectangles R, W et X sont des cibles sur lesquelles il est possible de cliquer. Cliquer sur l'étiquette d'un groupe d'accès (Utilisateur, Groupe, Autre) permet d'activer ou de désactiver collectivement toutes les autorisations de l'étiquette concernée.

Modification des propriétés des partages

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

Affichage des contrôles d'un élément de liste

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



Boîtes de dialogue modales

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.

Icons

Utilisation générale

Les icônes indiquent le statut du système et donnent accès à des fonctionnalités ; dans la plupart des cas, elles font également office de bouton et permettent d'effectuer des actions par un clic de la souris. 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.

Statut

Les témoins de statut sont des indicateurs de base de l'intégrité du système et de son fonctionnement :

Icône	Description	Icône	Description
	en marche		avertissement
	arrêté		désactivé

Utilisation de base

Les icônes suivantes sont présentes dans l'ensemble de l'interface utilisateur et correspondent aux fonctionnalités les plus élémentaires :

Icône*		Description	Icône*		Description
--		renommer (modifier du texte)	--		dissocier
--		déplacer	--		cloner
		modifier	--		restauration
		détruire	--		alimentation de l'appareil
		ajouter	--		appliquer
		retirer	--		précédent
		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
		verrouiller	--		rechercher
--		roue d'attente			menu
--		inverser le sens			panneau

** Les icônes désactivées sont représentées sur la gauche.*

Réseau

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

Icône	Description	Icône	Description
	périphérique réseau actif		port Infiniband actif

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

Seuils 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 Statut: : Paramètres.

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

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.

Icône	Description	Icône	Description
	reculer		afficher le minimum
	avancer		afficher le maximum
	avancer jusqu'à maintenant		afficher le graphique à courbes

Icône	Description	Icône	Description
	mettre en pause		afficher le graphique en aires
	zoom arrière		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
	afficher un mois		archiver l'ensemble de données
			envoyer la feuille de travail avec le lot de support

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.

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

** Icônes désactivées représentées sur la gauche.*

Icônes diverses

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

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

CLI

Introduction à la CLI

La ligne de commande est un outil particulièrement efficace et puissant d'écriture de scripts permettant d'exécuter des tâches administratives répétitives. L'appareil présente une interface de ligne de commande disponible via the serial console ou SSH.. L'interaction avec la machine par le biais de la ligne de commande 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 série 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 un navigateur ne se laisse pas facilement automatiser ; il est préférable d'écrire des scripts d'exécution pour les tâches répétitives ou définies de manière rigide

Connexion à la CLI

Pour vous connecter à distance par le biais de la CLI, faites appel à un client `ssh`. Si aucun autre utilisateur n'a été configuré pour administrer l'appareil, vous devez vous connecter en tant que `root`. Lorsque vous vous connectez, la CLI affiche une invite composée d'un nom d'hôte suivi du caractère deux-points, suivis du caractère supérieur à :

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

Lors de l'utilisation de la CLI, gardez à l'esprit les 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 conjuguer ces deux principes de la manière suivante :

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

Voir aussi

Utilisez l'aide CLI et la saisie semi-automatique par tabulation pour vous familiariser au CLI. Pour l'explorer plus en profondeur, vous devez vous familiariser avec quelques concepts CLI essentiels comme décrits dans les sections suivantes.

- Contexts - Contexts répertorie les commandes et propriétés disponibles
- Properties - Properties représente les points de contrôle administratif du système
- Scripting - Les tâches peuvent être automatisées grâce un riche environnement d'écriture de scripts.

Contexts

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 et la structure reflète généralement celle des vues de la BUI.

Contexte root

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. A partir du contexte root, ce contexte est accessible en saisissant directement :

```
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.

Contextes enfant

La commande `show` affiche les contextes enfant. Pour le contexte `configuration` par exemple :

```
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. Pour accéder directement au contexte `configuration preferences` à partir du contexte root par exemple, saisissez simplement :

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

Contextes enfant dynamiques

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. Pour accéder à ces contextes, servez-vous de la commande `select` suivie du nom du contexte dynamique. 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` :

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

Dans certains contextes, il est également possible d'utiliser les commandes `select` et `destroy` pour sélectionner une entité sur la base de ses propriétés. La commande suivante peut par exemple être saisie 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` peut être associée à des commandes entraînant un changement de contexte. Par exemple, pour sélectionner l'utilisateur nommé Par exemple, pour sélectionner l'utilisateur nommé `bmc` à partir du contexte root, saisissez à partir du contexte root, saisissez :

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

Retour à un contexte antérieur

La commande `done` permet de retourner au contexte précédent :

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

Notez que cette commande déclenche un retour au contexte précédent, qui n'est pas nécessairement le contexte parent :

```
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:>
```

Accès à un contexte parent

La commande cd permet d'accéder à un contexte parent. 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>
```

Contextes et saisie semi-automatique par tabulation

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>
```

Exécution de commandes spécifiques au contexte

Lorsque vous vous trouvez dans un contexte, exécutez des commandes spécifiques au contexte. Pour obtenir les préférences de l'utilisateur actuel par exemple, 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 changer de contexte, ajoutez la commande `get` après les commandes de navigation du contexte :

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

Contextes non validés

Lorsque vous créez une nouvelle entité dans le système, le contexte associé à la nouvelle entité est fréquemment créé avec l'état *uncommitted* (*non validé* en français). Vous pouvez par exemple créer une alerte de 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 à l'aide de 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. La création d'une nouvelle alerte de seuil par exemple nécessite la saisie d'un nom statistique ; si aucun nom n'est indiqué, une erreur est signalée :

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

Pour régler le problème, résolvez l'erreur et essayez à nouveau de valider :

```
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.
```

Properties

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
```

Obtention de propriétés

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

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

Obtention d'une valeur de propriété unique

La commande `get` renvoie la valeur correspondant à toute propriété saisie en tant qu'argument. Pour obtenir la valeur de la propriété `login_screen` par exemple, saisissez :

```
dory:configuration preferences> get login_screen
                login_screen = status/dashboard
```

Saisie semi-automatique par tabulation

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

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

Définition des propriétés

La commande `set` permet de définir une propriété sur une valeur donnée, le nom de la propriété et la valeur doivent alors être séparées par le caractère égal. Pour définir la propriété `login_screen` sur "`shares`" par exemple, saisissez :

```
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.

Validation d'une valeur de propriété définie

Pour forcer l'implémentation de valeurs de propriétés définies, il faut les valider de manière explicite ; plusieurs valeurs peuvent alors être modifiées en une opération de modification cohérente. Servez-vous de la commande `commit` pour valider les éventuelles valeurs de propriétés non validées :

```
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)
```

Définition d'une valeur de propriété validée de manière implicite

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:>
```

Définition d'une propriété sur une liste de valeurs

Certaines propriétés acceptent des listes de valeurs. Pour ces propriétés, les éléments de la liste doivent être séparés par des virgules. Par exemple, la propriété `servers` du service 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
```

Définition d'une propriété sur une valeur contenant des caractères spéciaux

Si une valeur de propriété contient une virgule, le signe égal, une apostrophe ou un espace, l'ensemble de la valeur doit être placée entre guillemets. Par exemple, pour définir la propriété `sharenfs` du contexte partages sur lecture seule pour le projet par défaut, mais accorder un accès en lecture/écriture à l'hôte "kiowa", saisissez :

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

Propriétés inaltérables

Certaines propriétés sont inaltérables : vous pouvez obtenir leurs valeurs, mais vous ne pouvez pas les définir. Toute tentative de définir une propriété inaltérable se solde par une erreur. L'exemple suivant illustre une tentative de définir la propriété inaltérable `space_available` du projet par défaut :

```
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. La commande `set` n'est pas valide pour ces propriétés. Par exemple, si l'utilisateur nommé `bmc` est un utilisateur réseau, la propriété `fullname` est inaltérable :

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

Scripting

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.

Ecriture de scripts

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* puissant basé sur ECMAScript 3. Ce document n'a pas pour objet de fournir un tutoriel ECMAScript ; sachez toutefois qu'il s'agit d'un langage à typage 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 structurelles 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

L'environnement de script

Dans la CLI, accédez à l'environnement de script à l'aide de la commande `script` :

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

En tant qu'invite de l'environnement de script, vous pouvez entrer votre script, en saisissant "." 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!
```

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)
```

Interaction avec le système

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 aux scripts d'interagir avec le système :

Fonction	Description
`get`	Récupère la valeur de la propriété spécifiée. Notez que cette fonction renvoie les valeurs dans leur format natif ; les dates par exemple sont renvoyées en tant qu'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.

La fonction Run

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'
```

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;']
```

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. Vous pouvez par exemple 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': '');
```

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 due au client ssh ; le problème correspondant peut être résolu en spécifiant l'option "-T" pour ssh.

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. Le script ci-dessous itère par exemple 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 ..');
       }
```

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
...
```

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 ..');
       }
```

Un extrait de la sortie obtenue après l'exécution de ce nouveau script, enregistré dans le fichier "prettyspace.aksh", est présenté 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
...
```

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. Le script suivant par exemple itère chaque service et imprime leur statut :

```
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");
       }
```

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
```

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.

```
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 ..');
        }
}
```

Voici le déroulement de l'exécution du script :

```
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
```

Génération de 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 :

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.

Gestion des erreurs

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

- `code` - un code numérique associé à l'erreur
- `message` - un 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 incorrect, un message d'erreur explicite est généré :

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

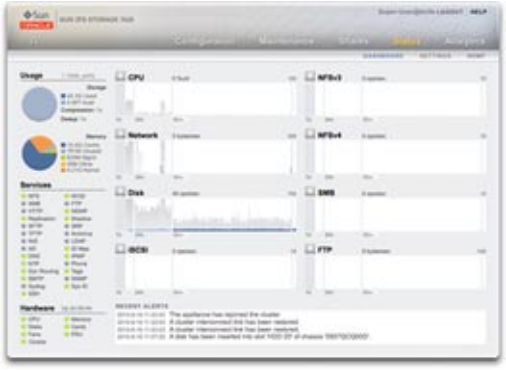
Automatisation de l'accès

Que vous ayez recours au traitement par lot de commandes ou à des scripts (ou à une combinaison des deux), une infrastructure automatisée nécessite un accès automatisé à l'appareil. Pour cela, vous devez créer des utilisateurs, leur octroyer les autorisations requises et télécharger les clés SSH.

◆ ◆ ◆ CHAPITRE 2

Statut

Status



Affichage de l'écran Statut > Tableau de bord

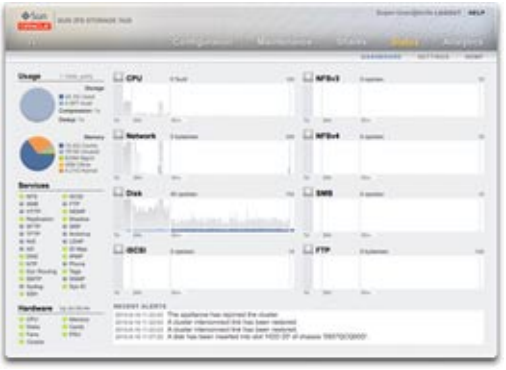
Statut

La section Statut présente un récapitulatif du statut de l'appareil et des options de configuration. Reportez-vous aux sections suivantes pour 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 :

- L'écran Statut > Tableau de bord présente une vue du stockage, de la mémoire, des services, du matériel, de l'activité et des alertes récentes.

- L'écran Statut > Paramètres permet de modifier les graphiques qui s'affichent sur le tableau de bord et de personnaliser les paramètres de seuil liés aux icônes météorologiques associées à chaque graphique dans le tableau de bord.
- L'écran Statut > NDMP présente une vue des périphériques NDMP éventuellement connectés et de l'activité récente de chaque session NDMP.

Dashboard



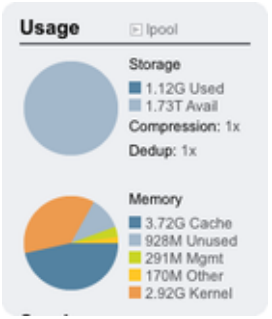
Le Tableau de bord résume le statut de l'appareil

Liens

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 Tableau de bord 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.

Utilisation

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.



Stockage

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.

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 Analyse et visualiser l'utilisation dynamique de la mémoire en fonction du nom d'application, cliquez sur le graphique à secteurs Mémoire.

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 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.

Récapitulatif de l'utilisation de la mémoire principale (RAM)	
Cache	Octets utilisés par le cache du système de fichiers pour améliorer les performances.

Récapitulatif de l'utilisation de la mémoire principale (RAM)	
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.
Kernel	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.

Services

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.

Icônes

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 statut des icônes pour voir la liste de tous les états et couleurs d'icônes possibles.

Liens

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.

Matériel

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

Pannes

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

Liens

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

Activité

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.

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

Vous pouvez visualiser la moyenne de chaque graphique en faisant glisser le pointeur de la souris sur le graphique ; la moyenne s'affiche alors dans une info-bulle. 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.

Graphiques

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.

Moyenne

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.

Echelle verticale

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.

Icônes météorologiques

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 Analyse.

Alertes récentes

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

CLI

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 BUI qui précède s'appliquent, avec les différences suivantes :

- Les tracés représentant l'activité ne sont pas représentés sous forme de texte - bien que nous ayons pensé à utiliser aalib.
- 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:>
```

Tâches

Dashboard Tâches

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 faites face à ce problème lorsque vous utilisez Firefox, désactivez le cache de mémoire en procédant comme suit :

1. Ouvrez about:config
2. Effectuez un filtrage sur "mémoire"
3. Définissez : browser.cache.memory.enable = false

Voir aussi

- Statut : Paramètres

Settings

Paramètres

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

BUI

Disposition

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

Nom	Unités	Description
<empty>	-	Aucun graphique n'est affiché à cet endroit.
SMB	opérations/sec	Nombre moyen d'opérations SMB.
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.
Disque	opérations/sec	Nombre moyen d'opérations vers les périphériques de stockage physiques.
HTTP	opérations/sec	Nombre moyen d'opérations HTTP.
iSCSI	opérations/sec	Nombre moyen d'opérations iSCSI.
FC	opérations/sec	Nombre moyen d'opérations Fibre Channel.
Réseau	octets/sec	Nombre moyen d'octets par seconde dans l'ensemble des interfaces réseau physiques.
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.
FTP	octets/sec	Nombre moyen d'octets FTP.
SFTP	octets/sec	Nombre moyen d'octets SFTP.

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>".

Seuils

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

L'icône météorologique apparaissant 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.

CLI

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.

Tâches

Cette section présente des exemples de tâches pour cette rubrique ; les tâches sont présentées sous forme d'étapes numérotées.

BUI

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.

Voir aussi

Statut:NDMP

NDMP

BUI

Cette page affiche un récapitulatif du statut de NDMP, si le Service NDMP a été configuré et est actif. Les périphériques de sauvegarde et l'activité récente des clients sont affichés.

Périphériques

Les périphériques NDMP sont énumérés ici.

Champ	Description	Exemples
Type	Type de périphérique NDMP	Robot, Lecteur de bande
Chemin	Chemin d'accès du périphérique NDMP	`/dev/rmt/0n`
Fournisseur	Nom du fournisseur du périphérique	STK
Produit	Nom de produit du périphérique	SL500

Activité récente

Cette section affiche un récapitulatif de l'activité NDMP 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 Etat de données	Actif, Inactif, ...
Etat du moteur	Voir Etat du moteur	Actif, Inactif, ...
Opération en cours	Opération NDMP actuelle	Sauvegarde, Restauration, Aucune
Progression	Barre de progression pour la sauvegarde concernée	

Etat des données NDMP

Ce champ indique l'état de l'opération de sauvegarde ou de restauration. Les valeurs possibles sont :

- Actif : les données sont en cours de sauvegarde ou de restauration.
- Inactif : la sauvegarde ou la restauration n'a pas encore débuté ou est déjà terminée.
- Connexion : la connexion a été établie, mais la sauvegarde ou la restauration n'a pas encore commencé.
- Arrêté : la sauvegarde ou la restauration est terminée, a échoué ou a été annulée.
- A l'écoute : l'opération attend l'établissement d'une connexion à distance.

Etat du moteur NDMP

Ce champ indique l'état du sous-système du périphérique NDMP. Exemples pour des 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 fin de la bande a été atteinte ou un changement de bande est attendu.
- Arrêté : l'opération d'écriture/lecture est terminée, a échoué ou a été annulée.
- A l'écoute : l'opération attend l'établissement d'une connexion à distance.

CLI

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

Voir aussi

- http://fr.wikipedia.org/wiki/Network_Data_Management_Protocol (`http://fr.wikipedia.org/wiki/Network_Data_Management_Protocol`)

◆ ◆ ◆ CHAPITRE 3

Configuration

Configuration

L'écran Configuration du réseau

Introduction

Cette section décrit la procédure de configuration de différentes propriétés de l'appareil, notamment les interfaces réseau, les services et les utilisateurs réseau.

- Initial - configuration initiale
- Réseau - réseau
- Services - services de données
- SAN - configuration du réseau de stockage
- Cluster - clustering
- Utilisateurs - comptes utilisateur et contrôle d'accès
- Préférences - préférences utilisateur
- Alertes - alertes personnalisées
- Stockage - reconfigurer les périphériques de stockage

Pour plus de détails sur la configuration ou la gestion de partages, voir la section Partages. To sauvegarder la configuration actuelle avant d'apporter des modifications, servez-vous du bouton Sauvegarder accessible sur l'écran Maintenance Système.

Initial

Configuration initiale

La configuration initiale comporte six étapes de configuration.

1. Réseau
2. DNS
3. Heure
4. Services de noms (NIS, LDAP, Active Directory)
5. Stockage
6. Enregistrement & support

Conditions préalables

La configuration initiale du système s'effectue après la première mise sous tension du système et l'établissement d'une connexion, comme indiqué dans la section Installation.

Notez que la possibilité d'effectuer la configuration initiale d'un cluster est uniquement offerte dans la BUI. Si vous choisissez d'effectuer cette opération, lisez la documentation relative au clustering avant d'effectuer la configuration initiale, afin de connaître les étapes supplémentaires requises pour une configuration réussie d'un cluster. Soyez attentif aux indications données à la section Considérations relatives au clustering pour la gestion réseau. Il est également possible d'effectuer la configuration initiale d'appareils compatibles cluster comme s'ils étaient destinés à un usage en autonome selon la procédure suivante, puis de les reconfigurer ultérieurement pour un fonctionnement en cluster.

Résumé

Cette procédure sert à configurer la connectivité réseau, plusieurs services réseau client et la configuration du pool de stockage pour un fonctionnement en autonome. Une fois qu'elle a été réalisée, l'appareil est prêt à l'usage. Toutefois, il ne comporte aucun partage configuré auquel des clients distants puissent accéder. Pour créer des partages ou réviser les paramètres, reportez-vous aux sections Partages et Configuration.

Vous pouvez répéter cette procédure ultérieurement en cliquant sur le bouton "CONFIGURATION INITIALE" sur l'écran Maintenance > Système ou en accédant au contexte `maintenance system setup` dans la CLI.

BUI

La configuration initiale par le biais de la BUI est la méthode la plus aisée pour chacune des étapes de la configuration initiale.

Cliquez sur Démarrer pour débuter la configuration de base du réseau, du répertoire de la date et de l'heure et des services de support. Cliquez sur Valider pour enregistrer la configuration et accéder à l'écran suivant. Les flèches figurant sous le bouton Valider permettent de revenir aux étapes précédentes et, si nécessaire, de modifier la configuration.

Configuration du port de gestion

Tous les contrôleurs autonomes doivent être dotés d'au moins un port NIC configuré en tant qu'interface de gestion. Sélectionnez l'option Autoriser admin dans la BUI pour activer les connexions de la BUI sur le port 215 et les connexions de la CLI sur le port `ssh` 22.

Dans toutes les installations en cluster, chaque contrôleur doit être doté d'au moins un port NIC configuré en tant qu'interface de gestion, comme décrit plus haut. En outre, le numéro d'instance NIC doit être unique sur chaque contrôleur.

CLI

Vous pouvez également effectuer les étapes de la configuration initiale par le biais de la CLI. Chaque étape débute par l'affichage de l'aide correspondante, qui peut être réaffichée en saisissant `help`. Entrez `done` après chacune des étapes pour indiquer qu'elle est terminée.

Réalisation de la configuration initiale à l'aide de la CLI

Connectez-vous à l'aide du mot de passe que vous avez indiqué lors de l'installation :

```
caji console login: root
Password:
Last login: Sun Oct 19 02:55:31 on console

To setup your system, you will be taken through a series of steps; as the setup
process advances to each step, the help message for that step will be
displayed.

Press any key to begin initial configuration ...
```

Dans cet exemple, les paramètres existants (obtenus du serveur DHCP) sont contrôlés et acceptés par saisie de `done`. Si vous souhaitez les personnaliser à ce stade, accédez à chaque contexte (liaisons de données, périphériques et interfaces) et saisissez `help` pour afficher les actions disponibles dans le contexte concerné. Reportez-vous à la section réseau pour plus d'informations. Soyez attentif aux indications données à la section Considérations relatives au clustering pour la gestion réseau si vous avez l'intention de configurer une mise en cluster.

```
aksh: starting configuration with "net" ...

Configure Networking. Configure the appliance network interfaces. The first
network interface has been configured for you, using the settings you provided
at the serial console.

Subcommands that are valid in this context:

   datalinks            => Manage datalinks

   devices              => Manage devices

   interfaces           => Manage interfaces

   help [topic]         => Get context-sensitive help. If [topic] is specified,
                           it must be one of "builtins", "commands", "general",
                           "help" or "script".

   show                 => Show information pertinent to the current context

   abort                => Abort this task (potentially resulting in a
                           misconfigured system)

   done                 => Finish operating on "net"

caji:maintenance system setup net> devices show
Devices:

     DEVICE UP       MAC                   SPEED
       igb0 true     0:14:4f:8d:59:aa      1000 Mbit/s
       igb1 false    0:14:4f:8d:59:ab      0 Mbit/s
       igb2 false    0:14:4f:8d:59:ac      0 Mbit/s
       igb3 false    0:14:4f:8d:59:ad      0 Mbit/s

caji:maintenance system setup net> datalinks show
```

```
Datalinks:

   DATALINK CLASS          LINKS       LABEL
       igb0 device         igb0        Untitled Datalink

caji:maintenance system setup net> interfaces show
Interfaces:

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

caji:maintenance system setup net> done
```

Reportez-vous à la section DNS pour plus d'informations sur DNS.

```
Configure DNS. Configure the Domain Name Service.

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

   abort                => Abort this task (potentially resulting in a
                           misconfigured system)

   done                 => Finish operating on "dns"

   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.

caji:maintenance system setup dns> show
Properties:
                      <status> = online
                        domain = sun.com
                       servers = 192.168.1.4

caji:maintenance system setup dns> set domain=sf.fishworks.com
                        domain = sf.fishworks.com (uncommitted)
caji:maintenance system setup dns> set servers=192.168.1.5
                       servers = 192.168.1.5 (uncommitted)
caji:maintenance system setup dns> commit
caji:maintenance system setup dns> done
aksh: done with "dns", advancing configuration to "ntp" ...
```

Configurez le protocole NTP (Network Time Protocol) pour synchroniser l'horloge de l'appareil. Reportez-vous à la section NTP pour plus d'informations.

```
Configure Time. Configure the Network Time Protocol.

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

   abort                 => Abort this task (potentially resulting in a
                            misconfigured system)

   done                  => Finish operating on "ntp"

   enable                => Enable the ntp service

   disable               => Disable the ntp 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.

caji:maintenance system setup ntp> set servers=0.pool.ntp.org
                      servers = 0.pool.ntp.org (uncommitted)
caji:maintenance system setup ntp> commit
caji:maintenance system setup ntp> done
aksh: done with "ntp", advancing configuration to "directory" ...
```

Reportez-vous aux sections NIS, LDAP et Active Directory pour plus d'informations.

```
Configure Name Services. Configure directory services for users and groups. You
can configure and enable each directory service independently, and you can
configure more than one directory service.

Subcommands that are valid in this context:

   nis                   => Configure NIS

   ldap                  => Configure LDAP

   ad                    => Configure Active Directory

   help [topic]          => Get context-sensitive help. If [topic] is specified,
                            it must be one of "builtins", "commands", "general",
                            "help" or "script".

   show                  => Show information pertinent to the current context

   abort                 => Abort this task (potentially resulting in a
                            misconfigured system)
```

```
   done                 => Finish operating on "directory"

caji:maintenance system setup directory> nis
caji:maintenance system setup directory nis> show
Properties:
                      <status> = online
                        domain = sun.com
                     broadcast = true
                     ypservers =

caji:maintenance system setup directory nis> set domain=fishworks
                        domain = fishworks (uncommitted)
caji:maintenance system setup directory nis> commit
caji:maintenance system setup directory nis> done
caji:maintenance system setup directory> done
aksh: done with "directory", advancing configuration to "support" ...
```

Configurez des pools de stockage caractérisés par leur redondance de données sous-jacente et prévoyez de l'espace partagé par tous les systèmes de fichiers et LUN. Reportez-vous à la section stockage pour plus d'informations.

```
Configure Storage.

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 "storage"

    config <pool>        => Configure the storage pool

    unconfig             => Unconfigure the storage pool

    add                  => Add additional storage to the storage pool

    import               => Search for existing or destroyed pools to import

    scrub <start|stop>   => Start or stop a scrub

    get [prop]           => Get value for property [prop]. ("help properties"
                            for valid properties.) If [prop] is not specified,
                            returns values for all properties.

    set pool=[pool]      => Change current pool

caji:maintenance system setup storage> show
Properties:
                           pool = pool-0
                         status = online
                        profile = mirror
```

```
                  log_profile = -
                cache_profile = -
caji:maintenance system setup storage> done
aksh: done with "storage", advancing configuration to "support" ...
```

Reportez-vous à la section (Phone Home) pour plus d'informations sur la configuration du support à distance.

```
Remote Support. Register your appliance and configure remote monitoring.

Subcommands that are valid in this context:

   tags                 => Configure service tags

   scrk                 => Configure phone home

   help [topic]         => Get context-sensitive help. If [topic] is specified,
                           it must be one of "builtins", "commands", "general",
                           "help" or "script".

   show                 => Show information pertinent to the current context

   abort                => Abort this task (potentially resulting in a
                           misconfigured system)

   done                 => Finish operating on "support"

 caji:maintenance system setup support> done
 aksh: initial configuration complete
```

Network

Configuration de la gestion réseau

Configuration réseau

Les fonctions de configuration de la gestion réseau vous permettent créer diverses configurations de gestion réseau avancées à partir 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 se compose de quatre éléments :

- Périphériques - Les 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.

Dans ce modèle, les périphériques réseau représentent le matériel disponible : 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.

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

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

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

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

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.

Les liaisons de données sont indispensables à l'achèvement de la configuration du réseau, qu'elles appliquent des paramètres spécifiques aux périphériques réseau ou non.

Périphériques

Les périphériques sont créés par le système pour représenter les ports réseau ou InfiniBand disponibles. Ils ne possèdent aucun paramètre de configuration propre.

Liaisons de données

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

- Le protocole LACP (Link Aggregation Control Protocol) - Un protocole permettant de regrouper plusieurs périphériques réseau de manière à ce qu'ils se comportent comme un seul périphérique. Cette opération améliore les performances (en augmentant la bande passante) et la fiabilité (en résistant à la défaillance de ports réseau) ; cependant, l'appareil doit être connecté à un commutateur prenant en charge le protocole LACP et celui-ci doit être activé sur les ports concernés.
- Partitions IB - Des partitions InfiniBand permettant la connexion à des domaines Fabric IB isolés de manière logique.
- Les VLAN - Des LAN virtuels permettant 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 Cards, cartes d'interface de réseau virtuel, qui 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 permette le partage de port réseau physique dans un cluster. Vous trouverez des instructions détaillées dans la section Tâches, plus loin dans ce document.

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

Les paramètres de liaisons de données suivants sont disponibles :

Propriété	Description
Nom	Utiliser le nom personnalisé défini. Par exemple : "interne", "externe", "adminnet", etc.

Propriété	Description
Speed	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 du VLAN	Utiliser l'identifiant 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 1 500 octets. Indiquez une MTU inférieure (1 280 minimum) pour laisser un plafond de paquet (par exemple, pour les protocoles de mise en tunnel). Indiquez une MTU supérieure (9 000 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.
Groupement 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 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 Actif 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 Désactivé utilise la liaison groupée mais ne détecte pas les défaillances de liaisons ou les changements de configuration du commutateur. Certaines configurations de commutateur réseau telles que Cisco Etherchannel par exemple n'utilisent pas le protocole LACP : le mode LACP doit être réglé sur "désactivé" en cas d'utilisation d'un groupement non LACP sur le réseau.

Propriété	Description
Minuteri 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 IPMP et de clustering sur le gestionnaire de sous-réseau.
Mode liaison IB	Utiliser le mode liaison IB défini. Deux modes sont disponibles : Datagramme non fiable et Connexion. Datagramme non fiable permet à une paire de files locales de communiquer avec plusieurs autres paires de files 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 2044. Le mode Connexion utilise les paires de files IB et dédie une paire de files locales à la communication avec une paire de files distantes. Le mode Connexion utilise un MTU de 65520 et peut fournir un meilleur rendement que le mode Datagramme non fiable.

Interfaces

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

- Les protocoles IPv4 et IPv6.
- L'IPMP - La fonctionnalité de chemins d'accès multiples 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.

Les paramètres d'interface suivants sont disponibles :

Propriété	Description
Nom	Nom personnalisé de l'interface.

Propriété	Description
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
Enable 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.
IPv4 Configurer avec	Soit "Liste d'adresses statiques" pour une liste d'adresses saisie manuellement, soit "DHCP" pour des demandes 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)
Groupe IP MultiPathing	Configurer la fonctionnalité de chemins d'accès multiples, où un pool de liaisons de données peut être utilisé pour la redondance

IPMP (IP MultiPathing)

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, soit comme 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 224.0.01. 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.

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.

Vous trouverez des instructions détaillées sur la création de groupes IPMP dans la section Tâches, plus loin dans ce document.

Performances et disponibilité

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 sont installées pour ajouter des liaisons au groupement. Le trafic IPMP utilise les adresses de données de l'interface IPMP, étant donné qu'elles sont liées aux interfaces actives disponibles. Si, par exemple, le trafic de données transite via deux adresses IP seulement, mais pas nécessairement par le biais de la même connexion, l'ajout de cartes réseau supplémentaires n'a pas pour effet d'augmenter les performances d'IPMP, car les adresses IP utilisables restent au nombre de deux.

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.

Routage

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.

Entrées de routage

La table de routage se compose d'entrées de routage, chaque entrée de routage étant formée des champs suivants :

Champ	Description	Exemples
Destination	Ensemble d'adresses de destination IP (en notation CIDR) pouvant correspondre à la route	192.168.0.0/22
Passerelle	Saut suivant (adresse IP) auquel envoyer le paquet (excepté les routes "système", voir ci-dessous)	192.168.2.80
Family	Protocole Internet	IPv4, IPv6
Type	Origine de la route	dhcp, statique, système
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 :

Nature	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 :

Type	Description
Statique	Créée et gérée par l'administrateur de l'appareil.
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 à leur place l'adresse IP de l'appareil sur le sous-réseau concerné.
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.
Dynamique	Automatiquement créée par l'appareil via les protocoles de routage dynamiques RIP et RIPng (lorsqu'ils sont activés).

Un type supplémentaire identifie une route statique ne pouvant pas actuellement être utilisée :

Inactive	Route statique précédemment créée et associée à une interface IP désactivée ou hors ligne.

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" (valeur 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 :

Stratégie	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 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 "adaptive" ou "strict" 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 "adaptive", alors qu'avec la stratégie "strict", le paquet est rejeté.

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 :

Icône	Description
	Ajouter une nouvelle liaison de données/interface/route
	Modifier les paramètres d'une liaison de données/interface/route
	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 interompue, problème de câble ?)
	port Infiniband actif
	port Infiniband actif avec activité d'E/S

Icône	Description
	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 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.

Configuration

La page Configuration s'affiche par défaut et répertorie les périphériques, les liaisons de données et les interfaces ; elle contient en outre des boutons d'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.

Adresses

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

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

Routage

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.

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.

L'exemple suivant illustre la création d'une liaison de données à l'aide de la commande `device` et celle 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
```

Tâches

BUI

Création d'une interface à port unique

1. Cliquez sur l'icône en regard de 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 Liaisons de données.
5. Cliquez sur l'icône en regard de 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. Une fois que vous avez terminé la configuration des interfaces, cliquez sur "APPLIQUER" en haut de l'écran pour valider la configuration.

Modification d'une interface

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.

Création d'une interface à port unique, glisser-déplacer

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

1. Cliquez sur l'icône en regard de 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 en regard de 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

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 en regard de Interface.
3. (Facultatif) Modifiez le nom de l'interface.
4. Cliquez sur 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 en regard de Interface.
3. (Facultatif) Modifiez le nom de l'interface.
4. Cliquez sur 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

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 la configuration.

Extension d'un groupe IPMP

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 la configuration.

Création d'une liaison de données et d'une interface de partition InfiniBand

1. Cliquez sur l'icône en regard de Liaison de données.
2. (Facultatif) Définissez un nom.
3. Cliquez sur la case à cocher IB Partition
4. Sélectionnez un périphérique dans la liste Périphériques de partition.
5. Cliquez sur "APPLIQUER". La nouvelle liaison de données de partition s'affiche dans la liste Liaisons de données.
6. Cliquez sur l'icône en regard de Interface.

7. Définissez les propriétés souhaitées et sélectionnez la liaison de données que vous venez de créer.
8. Cliquez sur "APPLIQUER". L'interface s'affiche dans la liste Interfaces.
9. La configuration réseau de l'appareil en cours d'exécution n'est pas encore modifiée. Une fois que 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

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 ⊕ des 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 ⊕ en regard de 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 ⊕ en regard de Liaisons de données.
7. Cochez la case 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 ⊕ en regard de 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. Une fois que 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

Cet exemple s'applique à une configuration active-active avec la moitié des ports réseau en veille. Les deux tâches créent 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 des liaisons de données.
2. Cochez la case 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 en regard de 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. Une fois que 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

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

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.

CLI

Ajout d'une route statique

1. Accédez à `configuration net routing`.
2. Saisissez `create`.
3. Exécutez `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

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

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

Storage

Sélection d'un profil de stockage pour un pool.

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 Partages.

Chaque noeud peut comporter un nombre de pools quelconque et l'appartenance des pools peut être librement définie au sein d'un cluster. 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 d'un grand nombre de 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 et un pool RAID-Z. 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.

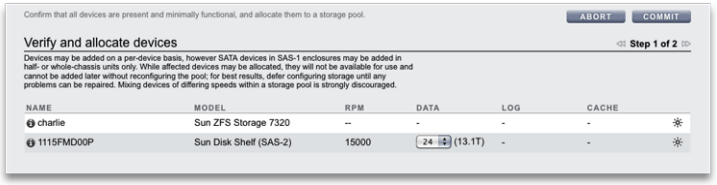
La création de pools peut s'effectuer par configuration d'un nouveau pool ou importation d'un pool existant. L'importation de pools existants ne peut servir qu'à importer des pools précédemment configurés sur un appareil Sun Storage 7000 Appliance et est utile en cas de reconfiguration involontaire, de déplacement de pools entre des noeuds de tête ou de panne catastrophique d'un noeud de tête.

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. Cette détérioration commence généralement à se faire sentir lorsque le taux de remplissage d'un pool dépasse 80%, et peut être très notable lorsque le taux de remplissage du pool dépasse 90%. Pour des résultats optimaux, il est donc indiqué d'augmenter l'allocation d'espace de 20% environ. L'interface utilisateur Partages permet de déterminer la quantité d'espace actuellement utilisée.

Configuration

Cette action configure le pool de stockage. Dans la BUI, cette action peut être effectuée par un clic sur le bouton accessible à côté de la liste de pools ; le système vous invite alors à saisir le nom du nouveau pool. Dans la CLI, cette action peut être effectuée à l'aide de la commande `config` et du nom du pool en tant qu'argument.

Après le démarrage de la tâche, la configuration du stockage comporte deux phases : la vérification et la configuration.



Règles et recommandations pour la configuration

Pour des performances optimales, gardez à l'esprit les points suivants :

`Règle n°1 -` Tous les disques de "données" compris dans un noeud de tête ou un JBOD doivent avoir la même vitesse de rotation (vitesse de rotation des médias). Le logiciel ZFSSA détecte les mauvaises configurations et génère une erreur à leur propos.

`Recommandation n°1 -` En raison de problèmes de performances non prévisibles, évitez d'associer différentes vitesses de rotation de disque au sein d'un même pool.

Recommandation n°2 - Pour des performances optimales, n'associez pas des JBOD présentant des vitesses de rotation de disque différentes dans le même Fabric SAS (connexion HBA). Une telle association fonctionne correctement, mais les performances des périphériques les plus rapides sont susceptible d'être ralenties.

Recommandation n°3 - 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. Evitez d'associer des disques de capacité différente au sein d'un même pool.

Vérification

La vérification permet de s'assurer que l'ensemble des composants de stockage sont connectés et fonctionnent. Tous les appareils de stockage doivent être connectés et fonctionnels avant de pouvoir les allouer. Si vous allouez un pool dont certains appareils sont manquants ou défectueux, vous ne pourrez pas ajouter les appareils manquants ou défectueux ultérieurement.

Dans un système sans appareil de stockage connecté, tous les disques disponibles sont alloués par défaut. Dans un système extensible, le noeud de cluster et la liste des étagères de disques s'affichent, et l'allocation peut être modifiée au sein de chaque étagère de disques. La manière de procéder pour cela peut légèrement varier en fonction du modèle du noeud de cluster ou de l'étagère de disque.

Vous pouvez sélectionner les éléments suivants :

- Taille de l'appareil, filtre les périphériques de données par taille logique. Par défaut, **Any** affiche tous les périphériques de données disponibles.
- Périphériques de données, affiche tous les périphériques de données disponibles, ou le nombre disponible de la taille de périphérique sélectionnée.

Le nombre de disques alloués par défaut dépend des éléments suivants :

- Le nombre maximal disponible, lorsque le stockage connecté contient des appareils de la même taille et avec la même vitesse de rotation, ou lorsqu'une taille est sélectionnée parmi plusieurs tailles
- Aucun, lorsque le stockage connecté contient plusieurs vitesses de rotation différentes.

Remarque : 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 cohérentes.

Allocation sur des systèmes SAS-2

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 JBOD 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 tous les JBOD au minimum, et beaucoup plus dans l'idéal.

Configuration d'un profil

Une fois la vérification terminée, l'étape suivante consiste à sélectionner un profil de stockage conforme aux objectifs de fiabilité, de disponibilité, de facilité de gestion et de performances de votre installation. L'ensemble de profils proposés dépend du stockage disponible. Le tableau suivant répertorie tous les profils possibles et leur description.

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.
RAID double parité	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).

Profil de données	Description
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`	
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.
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 réargenture 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.

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 JBOD 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 JBOD 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 un JBOD). 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 journalisation sont uniquement utilisés en cas de panne d'un noeud : par conséquent, 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. Ce scénario hautement improbable équivaudrait à une double panne. 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.

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 un cluster, seul le noeud sur lequel le pool de stockage a été importé a accès à des périphériques de mise en cache. Dans un cluster, il est possible de configurer des périphériques de mise en cache sur les deux noeuds destinés à faire partie du même pool. Pour ce faire, reprenez le pool sur le noeud 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 noeud.

Remarque : les versions antérieures des logiciels prenaient en charge la double parité avec bandes larges. Cette option a été remplacée par la tripe 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.

Importation

Cette fonction permet d'importer un pool de stockage existant ainsi que d'éventuels pools dont la configuration a été annulée par inadvertance. Elle peut être utilisée après la réinitialisation des paramètres d'usine ou après une opération de maintenance pour récupérer des données utilisateur. L'importation d'un pool 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. Pour importer un pool dans la BUI, cliquez sur le bouton 'IMPORTER' dans l'écran de configuration du stockage. Pour importer un pool dans la CLI, exécutez la commande 'import'.

A l'issue de la phase de détection, une liste des pools disponibles s'affiche ; cette liste mentionne quelques caractéristiques distinctives des pools. Si l'espace de stockage a été détruit ou est incomplet, le pool concerné ne peut pas être importé. Contrairement à ce qui se passe lors de la configuration du stockage, le nom du pool n'est pas indiqué en début de procédure, mais au moment de la sélection du pool. Le nom antérieur du pool est utilisé par défaut, mais vous pouvez le modifier en cliquant sur son nom dans la BUI ou en définissant la propriété 'name' dans la CLI.

Ajouter

Cette action permet d'ajouter de l'espace de stockage supplémentaire au pool existant. L'étape de vérification est identiqueà l'étape de vérification au cours de la configuration initiale. Le stockage doit être ajouté en recourant au même profil que celui utilisé lors de la configuration initiale du pool. Si le stockage disponible est insuffisant pour configurer le système à l'aide du

profil actuel, certains attributs peuvent être sacrifiés. Par exemple, l'ajout d'un seul JBOD à une configuration NSPF RAID-Z double parité ne permet pas la conservation des caractéristiques NSPF. Vous pouvez toutefois ajouter le JBOD et créer des bandes RAID au sein du JBOD, et sacrifier par la même occasion NSPF.

Annuler config

Cette action retire Les systèmes de fichiers et LUN actifs et annule la configuration du pool de stockage ; l'espace de stockage brut est ainsi remis à disposition 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, à condition que l'espace de stockage brut n'ait pas été utilisé entre-temps dans un pool de stockage actif.

Scrub

Cette action lance le processus de nettoyage du pool de stockage, lequel vérifie l'ensemble du contenu pour repérer les erreurs. Si des erreurs non récupérables sont identifiées, soit à l'occasion d'un nettoyage, soit dans le cadre du fonctionnement normal, la BUI affiche les fichiers affectés. Si nécessaire, il est possible d'arrêter le nettoyage.

Tâches

BUI

Configuration d'un pool de stockage

Il est possible d'accéder à cette tâche de deux manières : soit au moment de la configuration initiale de l'appareil, soit dans l'écran Configuration->Stockage.

1. Cliquez sur le bouton au-dessus de la liste de pools de stockage.
2. Entrez le nom du pool de stockage
3. Dans l'écran "Allouer et vérifier le stockage", configurez l'allocation JBOD pour le pool de stockage. L'allocation JBOD peut être réglée sur 'aucune', 'la moitié' ou 'tous'. Si aucun JBOD n'est détecté, contrôlez le câblage et l'alimentation du JBOD.
4. Cliquez sur "VALIDER".
5. Dans l'écran "Configuration du stockage ajouté", sélectionnez le profil de données souhaité. Une évaluation de chaque profil de données en termes de disponibilité, de performances et de capacité est fournie afin de vous aider à trouver la configuration la plus adaptée à vos besoins.
6. Cliquez sur "VALIDER".

SAN

SAN

L'écran de configuration SAN vous permet de connecter votre appareil à votre SAN (Storage Area Network, réseau de stockage). Un SAN est formé 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

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.

Terminologie

Pour configurer l'appareil de manière à ce qu'il fonctionne sur un SAN, une bonne compréhension des termes de base suivants est indispensable :

Terme	Description
Logical Unit, unité logique de stockage	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, associées à une ou plusieurs cibles SCSI, forment un périphérique SCSI unique auquel un ou plusieurs initiateurs SCSI peuvent accéder.
Target	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.
Groupe de cibles	Ensemble de cibles. Les LUN sont exportées par le biais de toutes les cibles vers un groupe de cibles particulier.
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.
Groupe d'initiateurs	Ensemble d'initiateurs. Lorsqu'un groupe d'initiateurs est associé à une LUN, seuls les initiateurs appartenant au groupe concerné peuvent accéder à la LUN. Depuis la version logicielle 2013.1.0, une LUN peut être associée à plusieurs groupes d'initiateurs.

En outre, il est important de connaître les protocoles de transport SCSI :

Terme	Description
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.
iSCSI	internet SCSI, protocole de partage de l'espace de stockage SCSI via des réseaux IP.
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.
SRP	SCSI RDMA Protocol, protocole de partage de l'espace de stockage SCSI via un réseau fournissant des services RDMA (c.-à-d. InfiniBand).

Cibles et initiateurs

Les cibles et les initiateurs sont configurés par protocole. Reportez-vous à la documentation du protocole concerné (FC, iSCSI ou SRP) pour plus d'informations.

Groupes de cibles et d'initiateurs

Les groupes de cibles et d'initiateurs définissent des ensembles de cibles et d'initiateurs pouvant être associés à des LUN. Une LUN associée à un groupe de cibles est uniquement visible par le biais des cibles appartenant à ce groupe. Si une LUN n'est pas explicitement associé à un groupe de cibles, elle appartient au *groupe de cibles par défaut* et est accessible via toutes les cibles, indépendamment du protocole. De la même manière, une LUN est uniquement visible par les initiateurs dans le ou les groupes auxquels elle appartient. Si une LUN n'est pas explicitement associée à un groupe d'initiateurs, elle 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 la LUN à des initiateurs non souhaités ou incompatibles.

Pour éviter les éventuels conflits LUN lorsqu'un initiateur appartient à plusieurs groupes, configurez les initiateurs au sein de tous les groupes avant d'associer les groupes aux LUN.

BUI

Pour configurer les cibles, accédez à la page **Configuration** > **SAN**, utilisez **Fibre Channel**, **iSCSI** et **SRP** pour naviguer, puis configurez les contrôles **Ports**, **Initiateur** et **Groupes de cibles**.

Pour associer une LUN, accédez à la page **Partages** > **Partages** > **Protocoles**, puis configurez les contrôles **Groupe de cibles** et **Groupe d'initiateurs**.

CLI

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.

Terms

Terminologie SAN

Cette section a pour objet de familiariser le lecteur avec les différents concepts liés à la configuration d'un SAN (réseau de stockage). Avant de passer à la configuration et à la gestion du stockage par blocs, il est important qu'il comprenne certains termes essentiels.

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).
Logical Unit, 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, associées 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.
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.

Terme	Description
SRP	SCSI RDMA Protocol, protocole de partage de l'espace de stockage SCSI via un r fournissant des services RDMA (c.-à-d. InfiniBand).
IQN	Nom qualifié iSCSI, identifiant unique d'un périphérique dans un réseau iSCSI. i utilise la forme iqn.date.authority:uniqueid pour les IQN. L'appareil peut par exe utiliser l'IQN : iqn.1986-03.com.sun:02:c7824a5b-f3ea-6038-c79d-ca443337d92 pour identifier l'une de ses cibles iSCSI. Ce nom indique qu'il s'agit d'un périphér 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 cib
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 ensem de portails cibles. Les groupes de portails cible sont gérés de manière transparent chaque interface réseau est associé un groupe de portails cible contenant les adres actives de l'interface concernée. Lier une cible à une interface a pour effet de publ 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 deux.
RADIUS	Système permettant d'utiliser un serveur centralisé pour effectuer l'authentificati CHAP au nom des noeuds de stockage.
Groupe de cibles	Ensemble de cibles. Les LUN sont exportées par le biais de toutes les cibles vers u groupe de cibles particulier.
Groupe d'initiateurs	Ensemble d'initiateurs. Lorsqu'un groupe d'initiateurs est associé à une LUN, seu initiateurs appartenant au groupe concerné peuvent accéder à la LUN.

Chaque LUN possède plusieurs propriétés qui déterminent la manière dont le volume est exporté. Reportez-vous à la section Protocoles pour plus d'informations.

FC

Fibre Channel

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.

Configuration de la cible

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 ; 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 (`http://www.oracle.com/technetwork/articles/servers-storage-admin/fbsanboot-365291.html`) pour plus d'informations sur les possibilités d'initialisation à partir d'un réseau de stockage FC à l'aide d'un appareil Sun ZFS Storage Appliance.

Considérations relatives au clustering

Dans un cluster, les initiateurs disposent de deux chemins (ou ensembles de chemins) vers chaque LUN : un chemin (ou ensemble de chemins) pointant vers le noeud de tête ayant importé l'espace de stockage associé à la LUN et un chemin (ou ensemble de chemins) pointant vers le pair en cluster de ce même noeud de tête. Le premier chemin (ou ensemble de chemins) est le chemin *actif* ; le second chemin (ou ensemble de chemins) est le chemin *de secours* ; en cas de reprise, le chemin actif devient indisponible et le chemin de secours devient, après un court délai, le chemin actif, 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.

Configuration des initiateurs

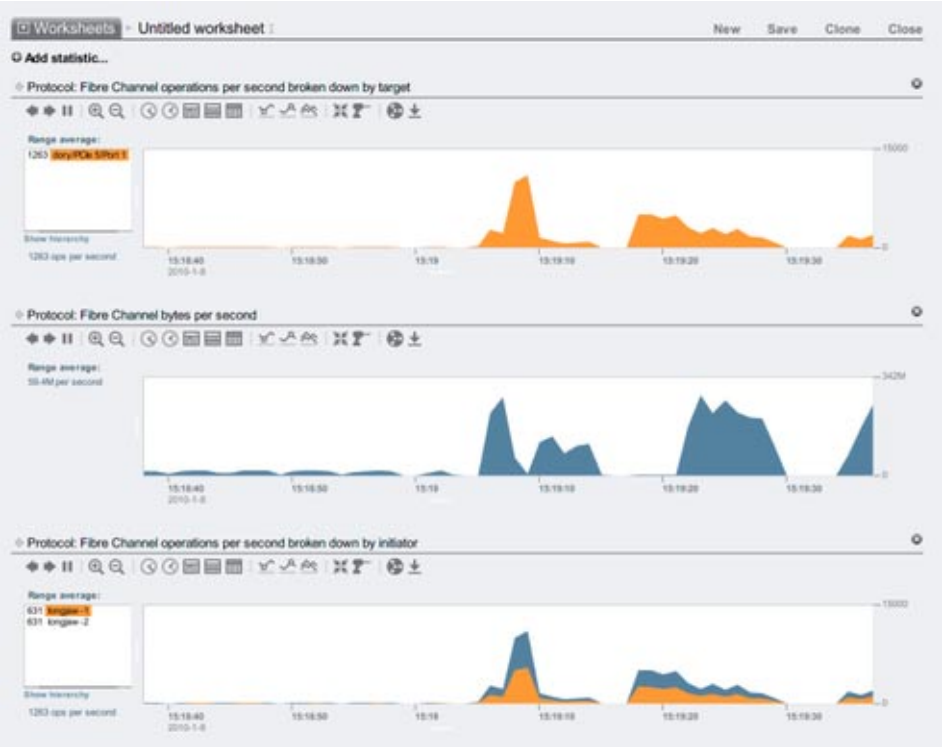
Les initiateurs sont identifiés par leur nom universel (WWN) et, comme pour d'autres protocoles de transfert par blocs, il est possible de créer des alias pour les initiateurs. Pour faciliter la création d'alias pour les initiateurs FC, vous pouvez sélectionner un WWN parmi les WWN des ports détectés. En outre, comme pour d''autres protocoles de transfert par blocs, les initiateurs peuvent être rassemblés en groupes. Lorsqu'une LUN est associée à un groupe d'initiateurs particulier, cette LUN est uniquement visible pour les initiateurs appartenant au groupe concerné. Dans la plupart des réseaux de stockage FC, les LUN sont toujours associées au groupe d'initiateurs correspondant au(x) système(s) pour le(s)quel(s) elles ont été créées.

Considérations relatives au clustering

Comme indiqué à la section Considérations relatives au clustering des cibles, 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.

Considérations relatives aux performances

Le module Analyse permet d'observer les performances FC et de détailler les opérations ou le débit par initiateur, cible ou LUN.



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.

Dépannage

Dépassement de capacité de file d'attente

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 un 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 l'un ou l'autre des phénomènes suivants :

- Ports surchargés dans la partie frontale : nombre excessif d'hôtes associés à un port FC et/ou nombre excessif de LUN connectées 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 allouées. Pour gérer les modes de fonctionnement détériorés, il faut additionner le nombre de LUN sur les pairs de cluster pour déterminer le nombre de LUN, mais utiliser comme nombre de ports cible la valeur minimale des deux pairs de cluster. Par exemple, dans un cluster actif-actif 7420 à deux noeuds de tête 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`.

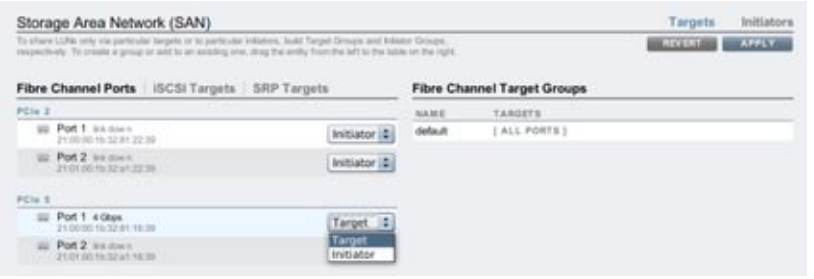
Problèmes au niveau des liaisons

Pour résoudre les problèmes au niveau des liaisons, tels que des dispositifs optiques cassés ou peu fiables ou un câble mal branché, jetez un coup d'oeil aux statistiques d'erreur pour chaque port FC : tout nombre très différent de zéro ou en augmentation peut être une indication que des erreurs ont été rencontrées au niveau des liaisons et qu'il faut effectuer des diagnostics à ce niveau.

BUI

Modification des modes des ports FC

Pour pouvoir 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 la capture d'écran ci-dessous. Vous devez disposez des autorisations `root` pour effectuer cette opération. Notez que dans une configuration en cluster, vous devez définir les ports sur le mode Cible sur chaque noeud de tête séparément ; reportez-vous à la section Considérations relatives au clustering pour plus d'informations.

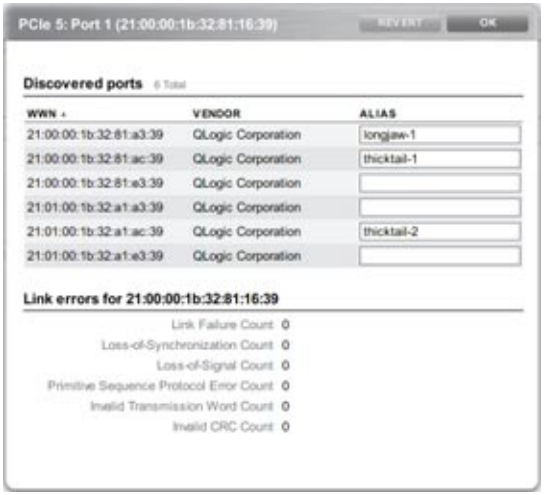


Après avoir défini les ports souhaités sur Cible, cliquez sur le bouton Appliquer. Un message de confirmation annonçant que l'appareil va se réinitialiser immédiatement s'affiche. Confirmez la réinitialisation.

Lorsque l'appareil se réinitialise, les cibles FC sont représentées avec l'icône , et l'icône de déplacement s'affiche lorsque vous placez la pointeur de la souris au-dessus de ces icônes.

Affichage des ports FC détectés

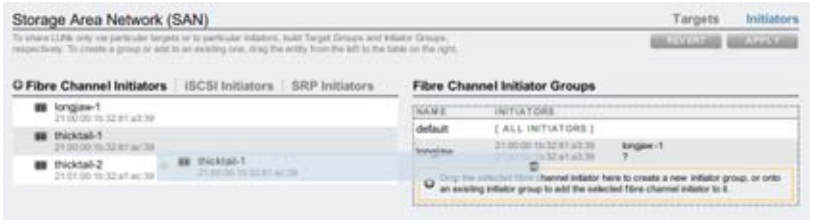
Cliquez sur l'icône d'informations pour afficher la boîte de dialogue Ports détectés dans laquelle vous pouvez résoudre les erreurs de liaison. Dans la boîte de dialogue Ports détectés, cliquez sur un nom universel de la liste pour afficher les erreurs de liaisons associées.



Création de groupes d'initiateurs FC

Créez et gérez des groupes d'initiateurs dans l'écran Initiateurs. Cliquez sur l'icône d'ajout pour visualiser les ports sans alias. Cliquez sur un nom universel de la liste pour ajouter un alias explicite dans le champ Alias.

Dans l'écran Initiateurs, faites glisser des initiateurs vers la liste Groupes d'initiateurs FC pour les ajouter à des groupes existants ou créer de nouveaux groupes.



Cliquez sur le bouton Appliquer pour valider le nouveau groupe d'initiateurs. Vous pouvez ensuite créer une LUN disposant d'un accès exclusif au groupe d'initiateurs client.

Association d'une LUN et d'un groupe d'initiateurs FC

Pour créer la 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. Définissez le nom et la taille et cliquez sur Appliquer pour ajouter la LUN au pool de stockage.

CLI

Modification des modes des ports FC

```
dory:configuration san fc targets> set targets="wwn.2101001B32A11639"
                     targets = wwn.2101001B32A11639 (uncommitted)
dory:configuration san fc targets> commit
```

Affichage des ports FC détectés

```
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
```

Création de groupes d'initiateurs FC

```
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
```

Association d'une LUN et d'un groupe d'initiateurs FC

L'exemple suivant illustre la création d'une LUN appelée `lefty` et son association au groupe d'initiateurs `fera`.

```
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
```

Scripts de création d'alias pour les initiateurs et groupes d'initiateurs

Reportez-vous aux sections Utilisation de la CLI et Commandes CLI simples de génération de scripts et de traitement par lots pour plus d'informations sur la modification et l'utilisation des exemples de scripts suivants.

```
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': 'wwn.2100001b3281ac39',
                      'thicktail-2': 'wwn.2101001b32a1ac39'
               },
               longjaw: {
                       'longjaw-1': 'wwn.2100001b3281a339',
                       'longjaw-2': 'wwn.2101001b32a1a339'
               },
               tecopa: {
                       'tecopa-1': 'wwn.2100001b3281e339',
                       'tecopa-2': 'wwn.2101001b32a1e339'
               },
               spinedace: {
                       'spinedace-1': 'wwn.2100001b3281df39',
                       'spinedace-2': 'wwn.2101001b32a1df39'
               },
               fera: {
                       'fera-1': 'wwn.2100001b32817939',
                       'fera-2': 'wwn.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 ..');
```

FCMPxIO

Configuration de la gestion des chemins d'accès multiples pour client FC

L'appareil Oracle ZFS Storage a recours à l'ALUA (Asymmetric Logical Unit Access) pour permettre aux cibles FC de prendre en charge les chemins d'accès multiples. Reportez-vous à la définition des commandes principales SCSI (SPC) sur t10 à l'adresse http://www.t10.org (`http://www.t10.org`) pour plus d'informations.

Les instructions suivantes indiquent la marche à suivre pour configurer les clients hôte FC connectés à un appareil en cluster compatible avec les cibles FC.

Tâches

FCMPxIO Tâches

Configuration d'initiateurs Solaris

MPxIO est activé sur les plates-formes Solaris x86, mais désactivé par défaut sur les plates-formes SPARC. La commande `mpathadm show LU` montre les modifications de l'état d'un chemin de 'actif' à 'de secours' et de 'de secours' à 'actif'. Vous pouvez également vous servir de la commande `luxadm display` pour afficher l'état d'un chemin.

L'utilitaire `stmsboot` active et désactive MPxIO, par exemple :

- Pour activer MPxIO, exécutez la commande `stmsboot -D fp -e`
- Pour désactiver MPxIO, exécutez la commande `stmsboot -D fp -d`
- Pour vérifier l'état, exécutez la commande `mpathadm show LU`

Configuration d'initiateurs Windows

La gestion des chemins d'accès multiples ALUA est prise en charge par MPIO Windows 2008/R2 natif uniquement. R2 est *indispensable* pour éviter les problèmes pendant le basculement et la reprise de cluster. SP2 n'est **pas** pris en charge.

1. Vérifiez que le pilote Windows HBA FC est installé et que le HBA est opérationnel.
2. Installez ou vérifiez l'installation du composant Windows Server 2008 MPIO Optional Component. Configurez la prise en charge des chemins d'accès multiples pour le SS7000 en émettant la commande `mpclaim.exe -r -i -a ""` à une invite de commandes Windows. Cette commande déclenche une réinitialisation système forcée et est nécessaire pour terminer l'installation et garantir la détection correcte du chemin/LUN.
3. Après la réinitialisation du client, assurez-vous que Windows Client est en mesure de détecter et d'accéder aux LUN du SS7000 et que le nombre de chemins et d'états de chemins affiché est correct. Vous pouvez vous servir pour cela de l'utilitaire Windows Disk Management. Il ne doit y avoir qu'un disque correspondant à chaque LUN du SS7000 dans l'interface utilisateur de Disk Management.
4. En cas de défaillance d'un noeud du SS7000, les compteurs d'horloge DSM Microsoft par défaut risquent d'être insuffisants pour assurer la poursuite des E/S sans interruptions. Pour résoudre ce problème, nous recommandons la définition des valeurs de compteur d'horloge suivantes dans la section relative aux informations DSM des propriétés de périphérique de disque à chemins d'accès multiples d'un disque.

Paramètres réglables Windows - Détails DSM Microsoft

Paramètre réglable Windows	Description	Valeur par défaut	Valeur recommandée
PathVerifyEnabled	Active la vérification des chemins par MPIO sur tous les chemins d'accès toutes les ?N? secondes. N dépend de la valeur définie dans PathVerificationPeriod.	Désactivé	Activé

Paramètre réglable Windows	Description	Valeur par défaut	Valeur recommandée
PathVerificationPeriod	Utilisé pour indiquer la périodicité (en secondes) paramétrée pour la vérification des chemins effectuée par MPIO. Ce champ est uniquement utilisé si PathVerifyEnabled = TRUE.	30 secondes	5 secondes
RetryInterval	Indique l'intervalle de temps après lequel une demande non aboutie est retentée (après décision du DSM et à condition que l'E/S ait été retentée à moins de reprises que RetryCount).	1 seconde	5 secondes
RetryCount	Indique le nombre d'occurrences d'une E/S non aboutie avant que le DSM détermine qu'une demande non aboutie doit être retentée.	3	300
PDORemovePeriod	Contrôle la durée (en secondes) pendant laquelle la pseudo-LUN à chemin d'accès multiples reste en mémoire, même après avoir perdu tous les chemins vers le périphérique.	20 secondes	1500 secondes

Errata : HBA Emulex et Windows Server 2008 : si vous utilisez un client Windows Server 2008 équipé de HBA Emulex, une modification doit être apportée au paramètre du pilote HBA. En vue d'assurer des E/S ininterrompues pendant une opération de basculement/rétablissement de cluster, il faut modifier la valeur NodeTimeout du HBA Emulex et la définir sur 0. Servez-vous de l'utilitaire *OCManager Utility* d'Emulex disponible sur http://www.emulex.com (`http://www.emulex.com`) pour ajuster ce paramètre.

Configuration d'initiateurs Linux

Les instructions suivantes sont valables pour :

- Oracle Enterprise Linux 5.4 (OEL 5.4)
- Oracle Enterprise Linux 5.5 (OEL 5.5)
- SUSE Linux 11 SP 1

1. Assurez-vous que les mappeurs de périphériques corrects sont installés. 2. Arrêtez le service `multipathd`.

```
# service multipathd stop
Stopping multipathd daemon:                                [  OK  ]
```

3. Ajoutez l'extrait de code `/etc/multipath.conf` approprié représenté ci-dessous, en remplaçant **PRODUCT** par la sortie du script CLI suivant :

```
run('cd /');
run('configuration version');
printf(get('product').replace(/^Sun /,"") + '\n');
```

Par exemple :

```
spadefish:> script
("." to run)> run('cd /');
("." to run)> run('configuration version');
("." to run)> printf(get('product').replace(/^Sun /,"") + '\n');
("." to run)> .
ZFS Storage 7420
```

- Pour OEL 5.4 :

```
device
{
   vendor                  "SUN"
   product                 "<i>PRODUCT</i>"
   getuid_callout          "/sbin/scsi_id -g -u -s /block/%n"
   prio_callout            "/sbin/mpath_prio_alua /dev/%n"
   hardware_handler        "0"
   path_grouping_policy    group_by_prio
   failback                immediate
   no_path_retry           queue
   rr_min_io               100
   path_checker            tur
   rr_weight               uniform
}
```

- Pour OEL 5.5 :

```
defaults {
  find_multipaths          yes
  user_friendly_names      yes
}

devices {
  device {
    vendor                 "SUN"
    product                "<i>PRODUCT</i>"
    getuid_callout         "/sbin/scsi_id -g -u -s /block/%n"
    prio                   alua
```

```
    hardware_handler          "1 alua"
    path_grouping_policy      group_by_prio
    failback                  immediate
    no_path_retry             600
    rr_min_io                 100
    path_checker              tur
    rr_weight                 uniform features "0"
  }
}
```

- Pour SUSE Linux 11 SP 1 :

```
defaults {
  multipath_tool              "/sbin/multipath -v0"
  udev_dir                    /dev
  polling_interval            100
  default_selector            "round-robin 0"
  default_path_grouping_policy  group_by_prio
  default_getuid_callout      "/lib/udev/scsi_id -g -u -d /dev/%n"
  default_prio_callout        "/bin/true"
  prio                        "alua"
  default_features            "0"
  rr_min_io                   100
  failback                    immediate
  user_friendly_names         yes
  path_checker                tur
  no_path_retry               1000
}

device {
  vendor                      "SUN"
  product                    "<i>PRODUCT</i>"
}
```

4. Activez les chemins d'accès multiples en démarrant le service `multipathd`.

```
#service multipathd start
Starting multipathd daemon:                                [  OK  ]
```

5. Exécutez la commande `multipath` après la fin de la réanalyse de bus SCSI pour vous assurer que la gestion des E/S sur chemins d'accès multiples est activée. Notez que les chemins de secours seront indiqués comme en raison d'un bogue Linux connu. Il est donc recommandé de vérifier que les chemins d'accès sont opérationnels avant de mettre le système en production. Pour plus d'informations, reportez-vous à la section Dépannage ci-dessous.

```
#multipath ?ll
sdd: checker msg is "tur checker reports path is down"
mpath1 (3600144f094f0bd0300004b31c88f0001) dm-2 SUN,Sun Storage 7420
[size=20G][features=1 queue_if_no_path][hwhandler=0][rw]
\_ round-robin 0 [prio=50][active]
\_ 2:0:0:0 sdb 8:16  [active][ready]
\_ round-robin 0 [prio=0][enabled]
\_ 2:0:1:0 sdd 8:48  [failed][faulty]
```

Configuration d'initiateurs VMware ESX

VMware ESX HCL

http://www.vmware.com/resources/compatibility/search.php (`http://www.vmware.com/resources/compatibility/search.php`)?action=search&deviceCategory=san&key=Oracle

Pour les serveurs ESX 4.1 :

Aucune règle supplémentaire ne doit être ajoutée si le pilote par défaut prend en charge ALUA.

Pour les serveurs ESX 4.0 :

1. Vérifiez le plug-in SATP actuellement utilisé en exécutant la commande `esx nmp device list`

```
# esxcli nmp device list
naa.600144f0ed81720500004bb3c1f60002
   Device Display Name: SUN Fibre Channel Disk (naa.600144f0ed81720500004bb3c1f60002)
   Storage Array Type: VMW_SATP_DEFAULT_AA
   Storage Array Type Device Config:
   Path Selection Policy: VMW_PSP_FIXED
   Path Selection Policy Device Config: {preferred=vmhba0:C0:T1:L0;current=vmhba0:C0:T1:L0}
   Working Paths: vmhba0:C0:T1:L0
```

VMW_SATP_DEFAULT_AA est le plug-in par défaut. Ce plug-in ne prend pas en charge ALUA.

2. Ajoutez des règles pour activer le plug-in ALUA pour les baies ZFS Storage 7000 en exécutant la commande esxcli nmp satp addrule.

```
# esxcli nmp satp addrule -s VMW_SATP_ALUA -e "ZFS Storage 7000" -V "SUN" -M "ZFS Storage 7120" -c "tpgs_on"
# esxcli nmp satp addrule -s VMW_SATP_ALUA -e "ZFS Storage 7000" -V "SUN" -M "ZFS Storage 7320" -c "tpgs_on"
# esxcli nmp satp addrule -s VMW_SATP_ALUA -e "ZFS Storage 7000" -V "SUN" -M "ZFS Storage 7420" -c "tpgs_on"
```

3. Assurez-vous que la règle a été correctement ajoutée.

```
# esxcli nmp satp listrules | grep SUN
```

VMW_SATP_ALUA SUN ZFS Storage 7120 tpgs_on ZFS Storage 7000 VMW_SATP_ALUA SUN ZFS Storage 7320 tpgs_on ZFS Storage 7000 VMW_SATP_ALUA SUN ZFS Storage 7420 tpgs_on ZFS Storage 7000

4. Réinitialisez le serveur VMware ESX Server. Lorsque le serveur a été réinitialisé, vérifiez à l'aide de la commande `esxcli nmp device list` que le plug-in correct est maintenant actif.

```
# esxcli nmp device list
naa.600144f0ed81720500004bb3c1f60002
   Device Display Name: SUN Fibre Channel Disk (naa.600144f0ed81720500004bb3c1f60002)
   Storage Array Type: VMW_SATP_ALUA
   Storage Array Type Device Config: {implicit_support=on;explicit_support=off;
```

```
explicit_allow=on;alua_followover=on;{TPG_id=0,TPG_state=STBY}{TPG_id=1,TPG_state=AO}}
Path Selection Policy: VMW_PSP_MRU
Path Selection Policy Device Config: Current Path=vmhba1:C0:T1:L0
Working Paths: vmhba1:C0:T1:L0
```

Dépannage

Cette section décrit le dépannage des problèmes connus.

Multipath-tools version 0.4.7 fourni avec OEL 5.4 n'est pas en mesure de reconnaître les chemins ayant l'état d'accès de secours ALUA

Dans les spécifications SCSI, un port cible présentant l'état 'de secours' ne répond pas à la commande 'Test Unit Ready', c'est pourquoi les chemins de secours sont indiqués comme (défaillants) comme dans la sortie de la commande multipath.

La solution de ce problème a été enregistrée dans l'arborescence source de multipath-tools le 2009-04-21 (c'est-à-dire après la version officielle 0.4.8). Les utilisateurs doivent télécharger la dernière version du code source de multipath-tools sur le site : http://christophe.varoqui.free.fr/ (http://christophe.varoqui.free.fr/)

La dernière version du code source est accessible à la rubrique 'git repository'. Le correctif n'est pas contenu dans le fichier tar multipath-tools-0.4.8.tar.bz2.

Enfin, le statut affiché dans la sortie de la commande multipath n'a aucun impact sur les fonctionnalités telles que les E/S et le basculement/rétablissement, de sorte que la mise à jour du package n'est pas obligatoire.

Voir aussi

- page fcinfo principale

http://www.oracle.com/technetwork/documentation/oracle-unified-ss-193371.html (http://www.oracle.com/technetwork/documentation/oracle-unified-ss-193371.html)

- Guide d'administration Solaris Fibre Channel et Storage Multipathing

http://www.oracle.com/technetwork/indexes/documentation/index.html (http://www.oracle.com/technetwork/indexes/documentation/index.html)

- Windows Server High Availability with Microsoft MPIO

http://www.microsoft.com/downloads/details.aspx (http://www.microsoft.com/downloads/details.aspx)?FamilyID=CBD27A84-23A1-4E88-B198-6233623582F3&displaylang=en

- Using Device-Mapper Multipath - Red Hat

http://www.redhat.com/docs/manuals/csgfs/browse/4.6/DM_Multipath/index.html (http://www.redhat.com/docs/manuals/csgfs/browse/4.6/DM_Multipath/index.html)

iSCSI

Introduction

Internet SCSI est l'un des protocoles de transfert par blocs pris en charge par l'appareil pour le partage du stockage SCSI.

Configuration de la 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.

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. L'appareil peut par exemple 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 Sun pour identifier la cible.

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.
Alias	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 :

Icône	Description
	La cible est en ligne
	La cible est hors ligne

Considérations relatives au clustering

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 différentes 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/rétablissements 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.

Configuration des initiateurs

Les initiateurs iSCSI ont les propriétés configurables suivantes.

Propriété	Description
IQN de l'initiateur	IQN de l'initiateur concerné.
Alias	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.

Planification de la configuration du client

Au moment de planifier 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 partagées 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 (ce qui correspond à la 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.

Considérations relatives à Solaris iSCSI/iSER et MPxIO

MPxIO prend en charge le groupement et la disponibilité de ports cible dans les configurations iSCSI Solaris configurant plusieurs sessions par cible (MS/T) sur l'initiateur iSCSI.

- Servez-vous d'IPMP pour le groupement et le basculement de deux cartes réseau ou plus.
- Une configuration de base pour un hôte iSCSI est un serveur comportant deux cartes réseau dédiées au trafic iSCSI. Les cartes réseau sont configurées à l'aide d'IPMP. Des cartes réseau supplémentaires sont fournies pour le trafic non iSCSI en vue d'optimiser les performances.
- Le multipathing actif peut uniquement être implémenté au moyen de la fonction iSCSI MS/T de Solaris, ainsi qu'à l'aide du basculement et de la redondance d'une configuration IPMP.
- *Si une carte réseau est défaillante dans une configuration IPMP, IPMP gère le basculement. Le pilote MPxIO ne remarque pas la défaillance. Dans une configuration non IPMP, le pilote MPxIO est défaillant et place le chemin hors ligne.
- *Si un port cible est défaillant dans une configuration IPMP, le pilote MPxIO remarque la défaillance et assure le basculement. Dans une configuration non IPMP, le pilote MPxIO remarque la défaillance et assure le basculement.
- Pour plus d'informations sur l'utilisation de la fonction iSCSI MS/T de Solaris avec l'IPMP et le multipathing, reportez-vous au document SunSolve Infodoc 207607, Understanding an iSCSI MS/T multi-path configuration.

- Pour plus d'informations sur la configuration de plusieurs sessions par cible, reportez-vous à la section Activation de plusieurs sessions iSCSI pour une cible dans le document suivant : http://download.oracle.com/docs/cd/E19253-01/817-5093/gcawf (`http://download.oracle.com/docs/cd/E19253-01/817-5093/gcawf`)
- Pour plus d'informations sur la configuration d'IPMP, reportez-vous à la Partie VI, IPMP, du Guide d'administration système : Services IP dans le document suivant : http://download.oracle.com/docs/cd/E19253-01/816-4554/ipmptm-1 (`http://download.oracle.com/docs/cd/E19253-01/816-4554/ipmptm-1`)

Dépannage

Pour des informations sur le dépannage de d'erreurs de configuration iSCSI fréquentes, reportez-vous à la section.

Observation des performances

Le module Analyse permet d'observer les performances iSCSI et de détailler les opérations ou le débit par initiateur, cible ou LUN.

Tâches

iSCSI Tâches

Création d'une feuille de travail Analyse

Pour créer une feuille de travail 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 afficher le menu déroulant 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.

CLI

Ajout d'une cible iSCSI possédant un IQN généré de manière automatique

```
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
```

Ajout d'une cible iSCSI avec authentification RADIUS et possédant un IQN donné

```
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
```

Ajout d'un initiateur iSCSI utilisant l'authentification CHAP

```
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
```

Ajout d'un groupe de cibles iSCSI

```
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
```

Ajout d'un groupe d'initiateurs iSCSI

```
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:initiator1234
```

SRP

Introduction

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).

Configuration de la cible

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.

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.
Alias	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 :

Icône	Description
	La cible est en ligne
	La cible est hors ligne

Considérations relatives au clustering

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.

Configuration des initiateurs

Les initiateurs SRP ont les propriétés configurables suivantes.

Propriété	Description
EUI de l'initiateur	L'EUI de l'initiateur concerné.
Alias	Pseudonyme lisible à l'oeil de l'initiateur concerné.

Observation des performances

Le module Analyse permet d'observer les performances SRP et de détailler les opérations ou le débit par initiateur ou cible. {{Server}}/wiki/images/cfg_san_srp.png

Considérations relatives aux chemins d'accès multiples

Les instructions suivantes indiquent la marche à suivre pour configurer les clients hôte.

VMWare 4.0

Le plug-in VMware Native MultiPath Plugin (nmp) comporte deux composants pouvant être modifiés en fonction du périphérique, en fonction du chemin ou en fonction de la baie.

Path Selection Plugin (psp)

Contrôle le chemin physique utilisé pour les E/S

```
# esxcli nmp psp list
Name           Description
VMW_PSP_MRU    Most Recently Used Path Selection
VMW_PSP_RR     Round Robin Path Selection
VMW_PSP_FIXED  Fixed Path Selection
```

Storage Array Type Plugin (satp)

Contrôle le fonctionnement du basculement

Pour pouvoir modifier le mode de basculement de base et passer du mode de baie active-active par défaut à ALUA, il faut configurer SATP de manière à ce qu'il reconnaisse le fabricant de la baie ou la chaîne de modèle.

Par défaut, le cluster Sun Storage 7000 a été introduit en tant que baie active/active uniquement.

Pour modifier manuellement cette configuration, ajoutez des règles à l'aide de la CLI ESX pour permettre au plug-in ALUA de récupérer les LUN 7000.

```
# esxcli nmp satp addrule -s VMW_SATP_ALUA -e "ZFS Storage 7000" -V "SUN" -M "ZFS Storage 7120" -c "tpgs_on"
# esxcli nmp satp addrule -s VMW_SATP_ALUA -e "ZFS Storage 7000" -V "SUN" -M "ZFS Storage 7320" -c "tpgs_on"
# esxcli nmp satp addrule -s VMW_SATP_ALUA -e "ZFS Storage 7000" -V "SUN" -M "ZFS Storage 7420" -c "tpgs_on"
```

```
 options are:

 -s VMW_SATP_ALUA - for the ALUA SATP
 -e description of the rule
 -V Vendor
 -M Model
 -c claim option for Target Portal Group (7000 seems to support implicit)
```

Si aucune LUN n'est recherchée/détectée, relancez la recherche de nouvelles LUN dans l'adaptateur afin que ces dernières puissent être récupérées par le plug-in ALUA. Si des LUN sont déjà présentes, réinitialisez l'hôte ESX.

Après la réinitialisation, les LUN en cours d'ajout à la liste doivent s'afficher sous le type de baie VMW_SATP_ALUE.

```
# esxcli nmp device list

naa.600144f096bb823800004b707f2d0001
Device Display Name: Local SUN Disk (naa.600144f096bb823800004b707f2d0001)
Storage Array Type: VMW_SATP_ALUA
```

```
   Storage Array Type Device Config:
      {implicit_support=on;explicit_support=off;explicit_allow=on;
       alua_followover=on; {TPG_id=0,TPG_state=AO}{TPG_id=1,TPG_state=STBY}}
   Path Selection Policy: VMW_PSP_MRU
   Path Selection Policy Device Config: Current Path=vmhba_mlx4_1.1.1:C0:T1:L0
   Working Paths: vmhba_mlx4_1.1.1:C0:T1:L0
```

Les listes de chemin de LUN approprié doivent afficher un chemin actif et un chemin de réserve.

```
   # esxcli nmp path list

   gsan.80fe53553e0100282100-gsan.80fe8f583e0100282100
   -naa.600144f096bb823800004b707f2d0001
   Runtime Name: vmhba_mlx4_1.1.1:C0:T2:L0
   Device: naa.600144f096bb823800004b707f2d0001
   Device Display Name: Local SUN Disk (naa.600144f096bb823800004b707f2d0001)
   Group State: standby
   Storage Array Type Path Config:
   {TPG_id=1,TPG_state=STBY,RTP_id=256,RTP_health=UP}
   Path Selection Policy Path Config: {non-current path}

   gsan.80fe53553e0100282100-gsan.80fe73583e0100282100
   -naa.600144f096bb823800004b707f2d0001
   Runtime Name: vmhba_mlx4_1.1.1:C0:T1:L0
   Device: naa.600144f096bb823800004b707f2d0001
   Device Display Name: Local SUN Disk (naa.600144f096bb823800004b707f2d0001)
   Group State: active
   Storage Array Type Path Config:
   {TPG_id=0,TPG_state=AO,RTP_id=2,RTP_health=UP}
   Path Selection Policy Path Config: {current path}
```

Problèmes liés à VMWare ESX 4.0

- Les chemins actifs et de réserve peuvent être introuvables.

La commande `esxcl nmp path list` doit signaler un chemin actif et un chemin de réserve, chacun étant destiné aux cibles SRP d'une configuration de cluster.

```
[root@ib-client-5 vmware]# esxcli nmp path list
gsan.80fe53553e0100282100-gsan.80fe8f583e0100282100-
naa.600144f096bb823800004b707f2d0001
   Runtime Name: vmhba_mlx4_1.1.1:C0:T2:L0
   Device: naa.600144f096bb823800004b707f2d0001
   Device Display Name: Local SUN Disk
(naa.600144f096bb823800004b707f2d0001)
   Group State: standby
   Storage Array Type Path Config:
{TPG_id=1,TPG_state=STBY,RTP_id=256,RTP_health=UP}
   Path Selection Policy Path Config: {non-current path}

gsan.80fe53553e0100282100-gsan.80fe73583e0100282100-
   naa.600144f096bb823800004b707f2d0001
   Runtime Name: vmhba_mlx4_1.1.1:C0:T1:L0
   Device: naa.600144f096bb823800004b707f2d0001
   Device Display Name: Local SUN Disk
```

```
(naa.600144f096bb823800004b707f2d0001)
   Group State: active
   Storage Array Type Path Config:
{TPG_id=0,TPG_state=AO,RTP_id=2,RTP_health=UP}
   Path Selection Policy Path Config: {current path}
```

Lorsque ce problème survient, le chemin actif ou de réserve risque de ne pas s'afficher dans la sortie de `esxcli nmp path list`.

Solution de contournement : aucune

- Lorsque ce problème survient, le journal du système invité

Linux le signale dans son journal `/var/log/messages` :

```
Feb 10 16:10:00 ib-client-5 vmkernel: 1:21:41:36.385 cpu3:4421)<3>ib_srp:
Send tsk_mgmt target[vmhba_mlx4_1.1.1:2] out of TX_IU head 769313 tail 769313 lim 0
```

Solution de contournement : réinitialiser la VM invitée

Tâches

Cette section décrit les instructions d'utilisation de la BUI pour configurer les cibles et les initiateurs iSER et SRP.

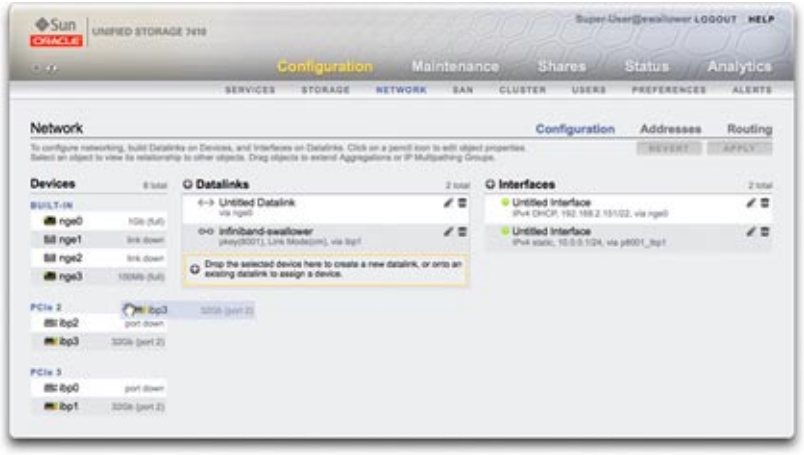
SRP Tâches

Configuration de la cible 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, sélectionnez l'interface ibd (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, accédez à l'écran Configuration > SAN.
4. Cliquez sur le lien Cibles iSCSI puis sur l'icône ⊕ pour ajouter une cible iSER avec un alias.
5. Pour créer un groupe de cibles, faites glisser la cible que vous venez de créer dans la liste Groupe de cibles iSCSIs.

6. Pour créer un initiateur, cliquez sur le lien Initiateur puis sur Initiateurs iSCSI.
7. Cliquez sur l'icône ⊕ pour ajouter un initiateur.
8. Saisissez l'IQN de l'initiateur, un alias, puis cliquez sur OK. La création d'un groupe d'initiateurs est facultative, mais la LUN associée 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 Groupes d'initiateurs iSCSI.

10. Pour créer une unité logique, accédez à l'écran Partages et cliquez sur le lien LUN.
11. Cliquez sur l'icône ⊕ et associez la nouvelle LUN au groupe de cibles ou d'initiateurs que vous avez créé à l'aide du menu Groupe cible et groupe d'initiateurs.

Configuration de la cible SRP

La procédure qui suit décrit les étapes de configuration des cibles SRP.

1. Connectez le port 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 ✥ pour faire glisser une cible dans la liste Groupes de cibles.
7. (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.

8. Pour créer une LUN et l'associer à la cible et aux initiateurs SRP que vous avez créés dans les étapes précédentes, accédez à l'écran Partages.
9. 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 à la LUN.

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 :

```
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
```

L'exemple ci-dessous indique comment créer une LUN et l'associer à targetSRPgroup 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     600144F0E9D19FFB00004B82DF49000
```

Users

Utilisateurs

Cette section décrit les *utilisateurs* susceptibles d'administrer 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.

Les utilisateurs possibles sont :

- Les utilisateurs locaux - toutes leurs informations de compte sont enregistrées dans l'appareil.
- Les utilisateurs d'annuaire - ce type d'utilisateur exploite les comptes NIS ou LDAP existants et enregistre les paramètres d'autorisation supplémentaires sur l'appareil. Cela permet aux utilisateurs NIS ou LDAP existants de bénéficier de privilèges de connexion et d'administration à l'appareil.

Pour accorder ces privilèges aux utilisateurs, il faut leur attribuer des *rôles* personnalisés.

Rôles

Un rôle constitue un ensemble de privilèges pouvant être attribué aux utilisateurs. Il peut être souhaitable de créer des 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 supplémentaires.

L'utilisation de ces rôles est considérée comme beaucoup plus sécurisée que celle des mots de passe administrateur partagés (par exemple, 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 Audit.

Le rôle "Administration de base" existe par défaut. Il contient des autorisations très basiques.

Autorisations

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 facultatif. 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.

Les portées disponibles sont répertoriées ci-dessous avec un exemple d'autorisation et un exemple de filtre (si disponible) :

Portée	Exemple d'autorisation	Exemple de filtre
Active Directory	Rejoindre un domaine Active Directory	Nom de domaine
Alertes	Configuration de filtres et de seuils d'alerte	.
Analyse	Lecture de statistiques en présence de cette analyse descendante	Analyses descendantes
Clustering	Rétablissement des ressources sur un pair de cluster	.
Ensembles de données	Gestion des aspects des ensembles de données d'analyse	Configuration
Matériel	Disques en ligne et hors ligne	.
Réseau	Configuration de périphériques réseau, de liaisons de données et d'interfaces	.
Projets et partages	Modification des propriétés générales des projets et des partages	Pool, projet, partage
Rôles	Configuration des autorisations pour un rôle	Nom de rôle
Services	Redémarrage d'un service	Nom de service
Schéma de propriétés de partages	Modification du schéma de propriétés	.
Système	Réinitialiser l'appareil	Nom de l'appareil
Mise à jour	Mise à jour du logiciel système	.
Utilisateurs	Modification d'un mot de passe	Nom d'utilisateur
Feuille de travail	Modification de la feuille de travail	Nom de feuille de travail

Parcourez les portées de la BUI pour découvrir les autres autorisations existantes. Actuellement, plus de cinquante autorisations différentes sont disponibles et il est à prévoir que des autorisations supplémentaires seront ajoutées aux mises à jour logicielles ultérieures de l'appareil.

Propriétés

Les propriétés suivantes peuvent être définies dans le cadre de la gestion des utilisateurs et des rôles.

Utilisateurs

Toutes les propriétés suivantes peuvent être définies lors de l'ajout d'un utilisateur, et certaines d'entre elles lors de la modification d'un utilisateur :

Propriété	Description
Type	Répertoire (informations d'identification d'accès à partir de NIS ou LDAP) ou Local (enregistrer l'utilisateur sur cet appareil)
Nom d'utilisateur	Nom unique de l'utilisateur
Nom complet	Description de l'utilisateur
Mot de passe/Confirmer	Les utilisateurs locaux doivent saisir leur mot de passe initial dans ces deux champs.
Exiger annotation de session	Si cette propriété est activée, les utilisateurs doivent justifier 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 d'annotation de session. L'annotation de session s'affiche dans le journal Audit.
Utilisateur Kiosk	Si cette propriété est activée, l'utilisateur peut uniquement afficher l'écran dans le paramètre "Ecran Kiosk". Elle peut restreindre l'accès de l'utilisateur au 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 "Utilisateur Kiosk" est activé.
Rôles	Rôles attribués à cet utilisateur
Exceptions	Ces autorisations sont exclues de celles qui sont habituellement disponibles en raison des rôles sélectionnés.

Rôles

Les propriétés suivantes peuvent être définies dans le cadre de la gestion des rôles.

Propriété	Description
Nom	Nom du rôle tel qu'il figure dans la liste
Description	Description détaillée du rôle, le cas échéant
Autorisations	Autorisations accordées à ce rôle

BUI

La page Utilisateurs de la BUI répertorie les utilisateurs et les groupes ainsi que les boutons d'administration. Placez le pointeur sur une entrée à l'aide de la souris pour afficher les boutons permettant de la cloner, modifier et détruire. Double-cliquez sur une entrée pour afficher son écran de modification. Les boutons sont les suivants :

Icône	Description
	Ajouter un rôle/utilisateur. Cette icône affiche une nouvelle boîte de dialogue pour la saisie des nouvelles propriétés requises.
	Afficher une zone de recherche. Entrez une chaîne de recherche et appuyez sur Entrée pour rechercher ce texte dans les listes d'utilisateurs/de rôles et n'afficher que les entrées correspondantes. Cliquez à nouveau sur cette icône ou sur "Tout afficher" pour revenir aux listes complètes.
	Cloner un utilisateur/rôle. Ajoutez un utilisateur/rôle en commençant par les champs correspondant aux valeurs de cette saisie.
	Modifier un utilisateur/rôle.
	Supprimer un utilisateur/rôle/une autorisation.

Reportez-vous à la description des tâches pour connaître les étapes nécessaires à l'ajout d'utilisateurs, de rôles et d'autorisations.

CLI

Les actions possibles dans la BUI le sont également dans la CLI. Lorsque vous naviguez dans l'administration d'utilisateurs, de rôles et d'autorisations, saisissez `help` pour répertorier les commandes disponibles.

En guise d'illustration de l'interface utilisateur et rôles de la CLI, l'exemple suivant ajoute l'utilisateur NIS "brendan" au système et lui accorde l'autorisation de redémarrer le serveur HTTP. Cette étape inclut la création d'un rôle pour cette autorisation.

Commençons par créer le rôle, que nous appellerons "webadmin" :

```
caji:> configuration roles
caji:configuration roles> role webadmin
caji:configuration roles webadmin (uncommitted)> set
   description="web server administrator"
                  description = web server administrator (uncommitted)
caji:configuration roles webadmin (uncommitted)> commit
caji:configuration roles> show
Roles:

NAME             DESCRIPTION
basic            Basic administration
webadmin         web server administrator
```

Maintenant que le rôle webadmin est créé, ajoutons l'autorisation de redémarrer le service HTTP. Cet exemple illustre également la sortie de la saisie automatique via la touche TAB qui permet de répertorier l'entrée valide et de déterminer quelles sont les portées et les options de filtre valides :

```
caji:configuration roles> select webadmin
caji:configuration roles webadmin> authorizations
caji:configuration roles webadmin authorizations> create
caji:configuration roles webadmin auth (uncommitted)> set scope=tab
ad           cluster      net          schema       update
alert        hardware     replication  stat         user
appliance    nas          role         svc          worksheet
caji:configuration roles webadmin auth (uncommitted)> set scope=svc
                        scope = svc
caji:configuration roles webadmin auth (uncommitted)> show
Properties:
                        scope = svc
                      service = *
              allow_administer = false
               allow_configure = false
                 allow_restart = false

caji: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
caji:configuration roles webadmin auth (uncommitted)> set service=http
                      service = http (uncommitted)
caji:configuration roles webadmin auth (uncommitted)> set allow_restart=true
                 allow_restart = true (uncommitted)
caji:configuration roles webadmin auth (uncommitted)> commit
caji:configuration roles webadmin authorizations> list
NAME       OBJECT                                PERMISSIONS
auth-000   svc.http                              restart
```

Une fois le rôle créé, renseignons la section des utilisateurs avec notre utilisateur "brendan" et affectons-lui le rôle "webadmin" :

```
caji:configuration roles webadmin authorizations> cd ../../..
caji:configuration> users
caji:configuration users> netuser brendan
caji:configuration users> show
Users:

NAME                    USERNAME                UID         TYPE
Brendan Gregg           brendan                 130948      Dir
Super-User              root                    0           Loc

caji:configuration users> select brendan
caji:configuration users brendan> show
Properties:
                      logname = brendan
                     fullname = Brendan Gregg
              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
caji:configuration users brendan> set roles=basic,webadmin
                         roles = basic,webadmin (uncommitted)
caji:configuration users brendan> commit
```

L'utilisateur brendan doit maintenant pouvoir se connecter à l'aide du mot de passe NIS et redémarrer le service HTTP sur l'appareil.

Tâches

Cette section présente des exemples de tâches d'administration des utilisateurs et des rôles. Si vous souhaitez utiliser la CLI, il peut être judicieux de vous familiariser avec ces tâches dans la BUI dans un premier temps, dont l'utilisation est plus conviviale et le rendu plus parlant.

BUI

Ajout d'un administrateur

1. Assurez-vous qu'un rôle administrator approprié figure dans la liste Rôles. Si ce n'est pas le cas, ajoutez un rôle (voir la tâche distincte).
2. Cliquez sur l'icône en regard des utilisateurs.
3. Définissez les propriétés de l'utilisateur.
4. Cochez la case correspondant au rôle administrator.
5. Cliquez sur le bouton Ajouter en haut de la boîte de dialogue. Le nouvel utilisateur apparaît dans la liste Utilisateurs.

Ajout d'un rôle

1. Cliquez sur l'icône en regard des rôles.
2. Définissez le nom du rôle et saisissez une description.
3. Ajoutez des autorisations au rôle (voir la tâche distincte).
4. Cliquez sur le bouton Ajouter en haut de la boîte de dialogue. Le nouveau rôle apparaît dans la liste Rôles.

Ajout d'autorisations à un rôle

1. Sélectionnez "Portée". Si des filtres sont disponibles pour cette portée, ils figurent en dessous du sélecteur Portée.
2. Sélectionnez des filtres, le cas échéant.
3. Cochez la case correspondante pour toutes les autorisations que vous souhaitez ajouter.
4. Cliquez sur le bouton Ajouter dans la section Autorisation. L'autorisation sera ajoutée à la liste située au bas de la boîte de dialogue.

Suppression des autorisations d'un rôle

1. Dans la liste Rôles, placez le pointeur sur le rôle concerné et cliquez sur l'icône .
2. Placez le pointeur sur l'autorisation au bas de la liste et cliquez sur l'icône située à droite.
3. Cliquez sur le bouton Appliquer en haut de la boîte de dialogue.

CLI

Ajout d'un administrateur

1. Accédez à `configuration roles`.
2. Saisissez `show`. Trouvez un rôle possédant les autorisations d'administration appropriées en exécutant `select` puis `authorizations show` sur chaque rôle. Si aucun rôle approprié n'existe, commencez par créer le rôle (voir la tâche distincte).
3. Accédez à `configuration users`.
4. Pour les utilisateurs d'annuaire (NIS, LDAP), saisissez `netuser` suivi du nom d'utilisateur existant que vous souhaitez ajouter. Pour les utilisateurs locaux, saisissez `user` suivi du nom d'utilisateur que vous souhaitez ajouter. Saisissez ensuite `show` pour afficher les propriétés à définir. Saisissez alors `set`, puis saisissez `commit`.
5. Vous avez alors créé un utilisateur mais n'avez pas personnalisé toutes ses propriétés. Saisissez `select` suivi du nom d'utilisateur.
6. Saisissez maintenant `show` pour afficher la liste complète des préférences. Il est désormais possible d'ajouter des exceptions en matière de rôles et d'autorisation ainsi que des préférences utilisateur.

Ajout d'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. Ajoutez des autorisations au rôle (voir la tâche distincte).

Ajout d'autorisations à un rôle

1. Accédez à `configuration roles`.
2. Saisissez `select` suivi du nom de rôle.
3. Saisissez `authorizations`.
4. Exécutez `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. Exécutez `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.

Suppression des autorisations d'un rôle

1. Accédez à `configuration roles`.
2. Saisissez `select` suivi du nom de rôle.
3. Saisissez `authorizations`.
4. Exécutez `show` pour répertorier les autorisations.
5. Saisissez `destroy` suivi du nom de l'autorisation (p. ex : "auth-001"). L'autorisation est alors détruite.

Générique

Ajout d'un utilisateur uniquement autorisé à afficher le tableau de bord

1. Ajoutez un utilisateur d'annuaire ou local (voir la tâche distincte).
2. Définissez le mode Kiosk sur true et vérifiez que l'écran Kiosk est défini sur "status/dashboard".
3. L'utilisateur doit maintenant pouvoir se connecter et afficher uniquement le tableau de bord.

Preferences

Préférences

Cette section contient des paramètres de préférence relatifs à votre localité, aux propriétés de votre session et aux clés SSH.

Propriété	Description
Initial login screen	Première page chargée par la BUI après la réussite d'une connexion. Par défaut, il s'agit de Tableau de bord de statut.

Propriété	Description
Locality	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.
Session Timeout	Délai au-delà duquel le navigateur sera automatiquement déconnecté de la session après avoir quitté la BUI
Current session annotation	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.

BUI

Une fois connecté à la BUI, vous pouvez définir les préférences ci-dessous pour votre compte, mais pas pour les comptes d'autres utilisateurs.

CLI

La CLI permet de définir des préférences sous `configuration users`. L'exemple suivant illustre l'activation de l'analyse avancée pour le compte utilisateur "brendan" :

```
caji:> configuration users
caji:configuration users> select brendan
caji:configuration users brendan> preferences
caji:configuration users brendan preferences> show
Properties:
                        locale = C
                  login_screen = status/dashboard
               session_timeout = 15
            advanced_analytics = false

Children:
                             keys => Manage SSH public keys

caji:configuration users brendan preferences> set advanced_analytics=true
            advanced_analytics = true (uncommitted)
caji:configuration users brendan preferences> commit
```

Définissez vos préférences dans la CLI sous `configuration preferences`. L'exemple suivant illustre la définition de l'annotation d'une session pour votre compte.

```
twofish:> configuration preferences
twofish:configuration preferences> show
Properties:
                        locale = C
                  login_screen = status/dashboard
               session_timeout = 15
            session_annotation =
            advanced_analytics = false

Children:
                             keys => Manage SSH public keys

twofish:configuration preferences> set session_annotation="Editing my user preferences"
            session_annotation = Editing my user preferences (uncommitted)
twofish:configuration preferences> commit
```

Clés publiques SSH

Elles peuvent être requises en cas d'automatisation de l'exécution de scripts de la CLI pour un autre hôte. L'exemple suivant illustre l'ajout d'une clé SSH à partir de la CLI.

```
caji:> configuration preferences keys
caji:configuration preferences keys> create
caji:configuration preferences key (uncommitted)> set type=DSA
caji:configuration preferences key (uncommitted)> set key="...DSA key text..."
                           key = ...DSA key text...== (uncommitted)
caji:configuration preferences key (uncommitted)> set comment="fw-log1"
                       comment = fw-log1 (uncommitted)
caji:configuration preferences key (uncommitted)> commit
caji:configuration preferences keys> show
Keys:

NAME     MODIFIED              TYPE   COMMENT
key-000  10/12/2009 10:54:58   DSA    fw-log1
```

'key text' contient le texte de la clé uniquement (généralement constitué d'une centaine de caractères), sans espace.

Alerts

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 de *seuil* personnalisée. Pour configurer le système afin qu'il réponde à certains types d'alertes, utilisez les actions d'alerte.

Les événements importants de l'appareil, y compris les pannes matérielles et logicielles, déclenchent des alertes. Elles figurent dans les journaux de maintenance et peuvent également être configurées pour exécuter n'importe quelle action d'alerte.

Les alertes sont regroupées dans les catégories suivantes :

Catégorie	Description
Cluster	Evénements de cluster, notamment les échecs de liaison et les erreurs de pair
Personnalisés	Evénements générés à partir de la configuration d'alertes personnalisées
Evénements relatifs au matériel	Initialisation de l'appareil et modification de la configuration matérielle
Pannes matérielles	Tout type de panne matérielle
NDMP operations	Evénements de début et de fin liés à la sauvegarde et à la restauration. Ce groupe est disponible en tant que "NDMP : sauvegarde uniquement" et "NDMP : restauration uniquement", respectivement réservé aux événements de sauvegarde ou de restauration
Réseau	Evénements et échecs liés au port réseau, à la liaison de données et à l'interface IP
Phone home	Evénements liés au chargement de l'offre groupée de support
Réplication distante	Evénements et échecs d'envoi et de réception. Ce groupe est disponible en tant que "Réplication distance : source uniquement" et "Réplication distante : cible uniquement", respectivement réservé à aux événements source ou cible
Service failures	Evénements d'échec du Service logiciel
Seuils	Alertes personnalisées basées sur les statistiques de l'Analyse
ZFS pool	Evénements du pool de stockage, y compris le nettoyage et l'activation

Actions

Les actions suivantes sont prises en charge :

Envoyer un e-mail

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 ci-dessous illustre l'envoi d'un e-mail basé sur une alerte avec seuil.

```
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
```

Les détails de l'envoi des e-mails par l'appareil peuvent être configurés dans l'écran du service SMTP.

Envoyer un déroutement SNMP

Il est possible d'envoyer un déroutement SNMP contenant des détails d'alerte si une destination de déroutement SNMP est configurée dans le service SMTP et si ce service est en ligne. L'exemple illustre 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."
```

Envoyer un message Syslog

Il est possible d'envoyer un message Syslog contenant des détails d'alerte vers un ou plusieurs systèmes distants si le service Syslog est activé. Reportez-vous à la documentation décrivant le

service Syslog Relay pour consulter des exemples de transport de données et une description de la procédure de configuration des récepteurs de Syslog sur d'autres systèmes d'exploitation.

Reprendre/suspendre un ensemble de données

L'ensemble de données de l'analyse peut être repris ou suspendu. Cette action est particulièrement utile lors du suivi des problèmes de performance survenant sporadiquement et lorsqu'il n'est pas souhaitable d'activer les 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 *reprendre* 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.

Reprendre/suspendre une feuille de travail

Ces actions consistent à reprendre ou suspendre une feuille de travail d'analyse 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.

Exécuter 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, reportez-vous à la section Workflows en tant qu'actions d'alerte.

Alertes avec seuil

Ces alertes sont basées sur les statistiques de l'analyse. Les propriétés suivantes sont disponibles lors de la création d'alertes avec seuil.

Propriété	Description
Threshold	La statistique de seuil est issue de l'analyse et autodescriptif (p. ex : "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

BUI

Les onglets "Actions d'alerte" et "Alertes avec seuil" sont situés en haut de la page Configuration->Alertes. Vous trouverez des instructions détaillées sur la configuration de ces onglets à la section Tâches, plus loin dans ce document.

CLI

Les alertes peuvent également être configurées depuis la CLI. Entrez `configuration alerts`puis `help`.

Tâches

BUI

Ajout d'une action d'alerte

1. Cliquez sur l'icône d'ajout en regard de "Actions d'alerte".
2. Sélectionnez la catégorie ou "Tous les événements" pour tout sélectionner.
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. Entrez les détails de l'action d'alerte. Vous pouvez cliquer sur le bouton "TEST" pour créer une alerte test et l'exécuter (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.

Ajout d'une alerte avec seuil

1. Cliquez sur l'icône d'ajout en regard de "Actions de seuil".
2. Choisissez la statistique à surveiller. Vous pouvez utiliser Analyse pour afficher la statistique et vérifier si elle convient.
3. Le pic excède/est inférieur au seuil et à la valeur souhaitée.
4. Saisissez les détails du délai. Les valeurs par défaut affichent l'alerte uniquement si le seuil est dépassé pendant au moins 5 minutes. L'alerte sera affichée à nouveau toutes les 5 minutes après disparition du seuil pendant au moins 5 minutes.
5. Sélectionnez l'action d'alerte dans le menu déroulant et remplissez les champs obligatoires sur la droite.
6. Vous pouvez, si vous le souhaitez, cliquer sur l'icône d'ajout en regard de "Actions d'alerte" pour ajouter des actions d'alerte.
7. Cliquez sur "APPLIQUER" en haut de la boîte de dialogue.

Voir aussi

- Configuration:Services:SNMP
- Configuration:Services:Syslog

Cluster

Clustering

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.

La fonction de clustering est basée sur l'accès partagé aux ressources de stockage. Pour configurer le clustering, les deux têtes 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 clusterisée avec le modèle 7420 (avec CPU 1,86 GHz ou 2,00 GHz).

Cette section est présentée dans plusieurs segments, à commencer par la documentation de base qui est très utile dans le processus de planification. Il est essentiel de comprendre cette documentation afin d'effectuer les tâches de maintenance et de configuration décrites dans les segments plus bas et plus généralement pour acquérir une expérience du déploiement du stockage unifié réussi.

Fonctions et avantages

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 têtes d'appareil et d'un système de stockage partagé permettant une meilleure disponibilité au cas où l'une des têtes succombe à des pannes matérielles ou logicielles. Un cluster contient exactement deux appareils ou deux contrôleurs de stockage, ci-après dénommés *têtes* pour des raisons de concision. Il est possible d'attribuer à chaque tête 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 tête 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 la tête désignée comme *active* ainsi que ses interfaces réseau associées sont attribués. 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 ente 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 une tête échoue, l'autre (*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 de la tête, 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 têtes, 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, la famille de produits Oracle ZFS Storage Appliance et les protocoles de données qu'elle fournit prennent en charge de nombreuses fonctions et stratégies permettant d'améliorer la disponibilité :

- La réplication distante de données 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 LUNiSCSI 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 degestion 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 est 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.

Inconvénients

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 encourus associés au marché de la seconde tête, le clustering présente également des risques techniques et opérationnels supplémentaires. Certains de ces

risques peuvent être réduits via la formation consciencieuse du personnel aux opérations de cluster ; les autres sont intrinsèques au concept de fonctionnement en cluster. Ces risques incluent :

- 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 du stockage doivent les confronter à l'avantage principal du clustering : l'opportunité de réduire les périodes d'indisponibilité (en passant de plusieurs heures/jours à quelques minutes voire moins) dans la rare éventualité d'une panne logicielle ou d'une panne 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.

Terminologie

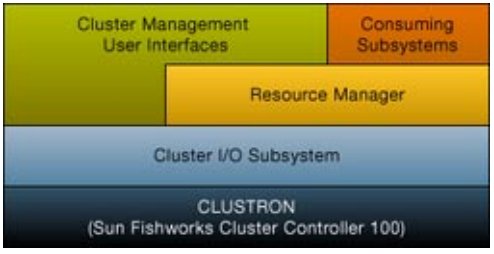
Les termes définis dans cette section sont utilisés dans l'ensemble du document. Dans la plupart des cas, ils sont expliqués plus en détail et avec plus de contexte avec les concepts plus vastes impliqués. Les états et les types de ressource du cluster sont décrits dans la section suivante. Le cas échéant, reportez-vous à cette section en guise de référence.

- export : processus permettant de rendre une ressource inactive sur une tête donnée
- 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
- import : processus permettant de rendre une ressource active sur une tête donnée
- pair : l'autre appareil d'un cluster

- réunir : récupérer et resynchroniser le mappage des ressources à partir du pair
- ressource : objet physique ou virtuel présent et éventuellement actif sur l'une des têtes ou les deux
- reprise : passage de l'état AKCS_CLUSTERED ou AKCS_STRIPPED à l'état AKCS_OWNER dans lequel toutes les ressources sont importées.

Conception du sous-système

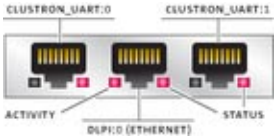
Le sous-système de clustering intégré à la série contient trois blocs fonctionnels (voir l'illustration 1). Le sous-système d'E/S du cluster et le périphérique matériel fournissent un transport pour la communication entre les têtes d'un même cluster tout en assurant la surveillance de l'état du pair. 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 gestion du cluster. 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 de construction sont décrits en détail dans les sections suivantes :



E/S d'interconnexion de cluster

Toute la communication entre les têtes 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 clusterisé 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 EIA/TIA-568B (8 fils, Gigabit Ethernet). Pour permettre l'utilisation de câbles droits entre deux contrôleurs identiques, les câbles doivent servir à connecter les sockets opposés sur les deux connecteurs, comme indiqué ci-dessous dans la section relative au câblage.



Les têtes clusterisées 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'une tête distante 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.

Indépendamment de son type ou de son origine, le message est envoyé en tant que groupe de 128 octets contenant des données traitées égales à 68 octets ainsi qu'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 bits de données et un seul bit de démarrage et d'arrêt. La liaison Ethernet s'exécute à 1 Gbit/s. Par conséquent, le temps d'attente effectif d'un message 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.

Généralement, les pulsations sont envoyées par chaque tête sur les trois liaisons d'E/S du cluster à intervalles de 50 ms. L'impossibilité de réceptionner un message est considérée comme un échec de liaison après 200 ms (liaisons série) ou 500 ms (liaison Ethernet). Lorsque les trois liaisons échouent, le pair est considéré en échec ; l'arbitrage de la reprise est alors effectué. En cas de panique, la tête concernée 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 l'homologue 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, se reporter à la section Prévention des conditions split-brain.

Concepts de gestion des ressources

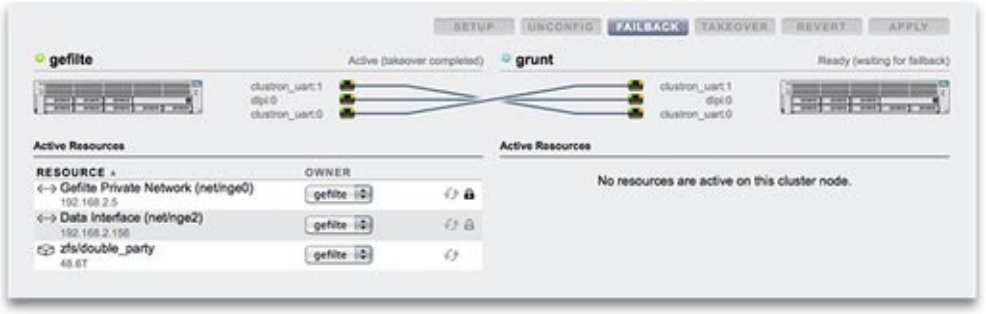
Le gestionnaire de ressources veille à la solidité de l'installation des interfaces réseau, vérifie que les pools de stockage adaptés sont actifs et s'assure de la synchronisation des nombreux paramètres de configuration avec les deux têtes clusterisées. La plupart des activités de ce sous-système sont 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.

Les répliques sont les plus simples : elles ne sont jamais exposées aux administrateurs et n'apparaissent pas dans l'écran de configuration du cluster (voir l'illustration 4). Les répliques existent toujours et sont toujours actives sur les deux têtes. De manière générale, elles agissent simplement comme des conteneurs de propriétés de service à synchroniser entre les deux têtes.

De même que les répliques, les ressources singleton permettent la synchronisation de l'état. Toutefois, les singletons sont toujours actifs sur une tête exactement. Les administrateurs peuvent choisir la tête sur laquelle activer le singleton de manière générale. En cas d'échec sur cette tête, 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'une tête défaillante 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 à la même tête que celle 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 la tête ayant importé pool-0, tandis que les adresses associées à PrimaryB sont toujours fournies par la même tête que pool-1.

Les ressources privées sont uniquement connues par la tête à laquelle elles sont assignées et ne sont jamais reprises en cas de panne. Ce type est généralement utile pour les interfaces réseau

(voir la discussion relative aux cas d'utilisation spécifiques ci-dessous).



Il existe d'autres types de ressources : 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 clusterisé 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.

Ressource	Icône	Omniprésent	Reprise en cas de panne
SINGLETON		Non	Oui
REPLIQUE	Aucune	Oui	S/O
PRIVE		Non	Non
SYMBIOTE	Aucune	Identique au type parent	Identique au type parent

Lorsqu'une nouvelle ressource est créée, elle est initialement assignée à la tête sur laquelle elle est créée. Il est impossible de modifier cette propriété tant que la tête possède l'état AKCS_OWNER. Il est donc nécessaire soit de créer des ressources sur la tête 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 toutes les têtes, à l'exception des pools de stockage exportés. Les meilleurs résultats sont généralement obtenus en détruisant les ressources sur la tête qui est alors chargée de les contrôler, indépendamment de la tête à laquelle la propriété est assignée.

La plupart des paramètres de configuration, notamment les propriétés du service, les utilisateurs, les rôles, les règles autohome SMB et les définitions d'initiateur iSCSI sont répliqués automatiquement sur les deux têtes. Il n'est donc jamais nécessaire de configurer ces paramètres sur les deux têtes, 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 un petit nombre d'exceptions :

- Les définitions et les options des partages et des LUN peuvent uniquement être définies sur la tête qui contrôle le pool sous-jacent, indépendamment de la tête à laquelle le pool est normalement affecté.
- La configuration du service "Identity" (p. ex, le nom et l'emplacement de l'appareil) n'est pas répliquée.
- Les noms donnés au châssis sont uniquement visibles sur la tête à laquelle ils ont été assignés.
- Chaque route réseau est liée à une interface spécifique. Si chaque tête est associée 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'une tête à une autre. Pour plus d'informations, reportez-vous aux considérations relatives à la gestion de réseaux.
- 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 noeud 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 tête 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.

Reprise et rétablissement

Les noeuds de tête clusterisés se trouvent dans l'un des petits ensembles d'états à un moment précis :

Etat	Icône	Expression de la CLI/BUI	Description
UNCONFIGURED		Clustering is not configured	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 noeud 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 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, comme indiqué ci-dessus, tandis que le rétablissement est tenté dès qu'une défaillance 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 une tête est mise à niveau tandis que l'autre fournit le service exécutant l'ancien logiciel, une fois le nouveau logiciel validé, la deuxième tête est alors mise à niveau). Enfin, la reprise a lieu lorsqu'une tête est initialisée et qu'elle détecte que son pair est absent. Cela permet au service de fonctionner à nouveau normalement lorsqu'une tête est défaillante de façon permanente ou lorsque les deux têtes sont temporairement hors tension.

Le rétablissement ne se fait jamais automatiquement. Lorsqu'une tête défaillante est réparée puis réinitialisée, elle 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, la tête encore fonctionnelle 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 la tête 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 la tête A soit en panne et que la tête B ait pris le relais. Lorsque la tête A rejoint le cluster, elle peut assurer une reprise si elle détecte que la tête B est absente ou défectueuse. 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 une tête précédemment défaillante ne s'effectue jamais automatiquement, il peut néanmoins effectuer la reprise à tout moment.

Lorsque vous configurez 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 clusterisés 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.

Modifications de la configuration dans un environnement clusterisé

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 tête. Afin de garantir que les deux têtes fournissent un service cohérent, toutes les propriétés service doivent être synchronisées en cas de modification ou lorsqu'une tête 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'une des têtes.

Par conséquent, il n'est pas nécessaire pour les administrateurs de répliquer les modifications de la configuration (ce qui serait redondant). Les procédures de fonctionnement standard doivent refléter cet attribut et appeler à des modifications sur une seule des deux têtes 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 :

- Apporter toutes les modifications de la configuration liées au stockage et au réseau sur la tête 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.
- Apporter toutes les autres modifications sur une des têtes, mais pas les deux. La stratégie de site doit permettre de spécifier la tête *principale* à utiliser, qui doit à son tour dépendre de la tête qui fonctionne et du nombre de pools de stockage 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 tête 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 tête. Cette simplification réduit considérablement le besoin de référentiels de configuration centralisés et plaide pour une approche simplifiée : la tête en cours de fonctionnement est censée détenir la configuration appropriée et les données de son homologue seront synchronisées par rapport à elle 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 : la deuxième tête adopte un ensemble de paramètres de configuration déjà utilisé 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'une tête défaillante rejoint le cluster dès sa réparation.

Considérations relatives au clustering pour le stockage

Lorsque vous redimensionnez un système de la série Oracle ZFS Storage Appliance pour l'utiliser dans un cluster, deux considérations supplémentaires ont leur importance. 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 répartitions sont possibles, comme indiqué dans le tableau ci-dessous. Généralement, les pools doivent être configurés sur une seule tête, 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 une tête est proche de fournir des performances maximales sur un axe particulier et plus la dégradation des performances est importante le long de l'axe lorsque la charge de travail est reprise par le pair de la tête. En cas de pools multiples, cette dégradation s'applique aux deux charges de travail.

Notez que, dans les deux configurations, un périphérique ReadZilla peut être utilisé uniquement lorsque le pool auquel il est assigné est importé sur la tête à laquelle la propriété de ce pool a été attribuée. Ainsi, lorsqu'un pool fait l'objet d'un relais en cas de défaillance d'une tête, la mise en cache des opérations de lecture est impossible pour ce pool, même si la tête qui l'a importé possède également des périphériques ReadZilla non utilisés. Il est donc conseillé de configurer les périphériques ReadZilla dans un cluster actif-passif, conformément à la documentation relative à la configuration de stockage. Cette recommandation ne s'applique pas aux périphériques LogZilla, situés dans la topologie Fabric de stockage, qui restent accessibles à toutes les têtes ayant importé le pool.

Variable	Propriété mononoeud	Pools multiples possédés par des têtes différentes
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 : une seule tête traite les requêtes du client, l'autre est inactive.	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 un moment donné (des périphériques réseau invisible sont requis sur chaque tête pour prendre en charge le basculement).

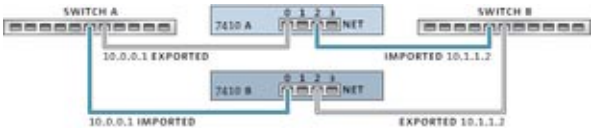
Variable	Propriété mononoeud	Pools multiples possédés par des têtes différentes
Débit total (basculement)	Aucune modification du débit par rapport à l'opération nominale.	100 % des ressources de tête encore fonctionnelles sont utilisées pour fournir le service. Le débit total relatif à l'opération nominale est compris entre environ 40 et 100 % en fonction de l'utilisation durant l'opération nominale.
Temps d'attente d'E/S (basculement)	ReadZilla n'est pas disponible durant une opération de basculement, ce qui peut considérablement augmenter les temps d'attente pour les charges de travail intégrées au cache de lecture disponible. Le temps d'attente des opérations d'écriture n'est pas concerné.	ReadZilla n'est pas disponible durant une opération de basculement, ce qui peut considérablement augmenter les temps d'attente pour les charges de travail intégrées au cache de lecture disponible. Le temps d'attente des opérations de lecture et d'écriture peut être augmenté en raison des conflits importants en matière d'utilisation des ressources de tête résultant de l'exécution de deux charges de travail sur la tête encore fonctionnelle à la place de la tête habituelle. Lorsque les charges de travail nominales de chaque tête atteignent les capacités maximales de la tête, les temps d'attente dans l'état de basculement peuvent être extrêmement longs.
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.

Variable	Propriété mononoeud	Pools multiples possédés par des têtes différentes
Connectivité réseau	Tous les périphériques réseau de chaque tête peuvent être utilisés tandis que la tête est en service.	Seule la moitié de l'ensemble des périphériques réseau de chaque tête peut être utilisée lorsque la tête est en service. Chaque pool peut donc être connecté à seulement la moitié des réseaux physiquement disjoints.

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'un JBOD unique et par conséquent une perte de disponibilité. L'inconvénient de cette approche tient à ce que les configurations sans point de panne unique requièrent un plus grand nombre de JBOD que de configurations avec point de panne unique. Lorsque la capacité requise est très faible, l'installation d'un nombre suffisant de JBOD pour les configurations sans point de panne unique sur le niveau RAID de votre choix n'est pas forcément très économique.

Considérations relatives au clustering pour la gestion réseau

La défaillance d'un périphérique réseau, d'une liaison de données et de l'interface n'amène pas le sous-système de clustering à envisager l'échec d'une tête. Pour vous protéger des pannes réseau (à l'intérieur ou à l'extérieur de l'appareil), utilisez plutôt IPMP et/ou LACP. Ces options de configuration réseau, ainsi qu'un plan de redondance plus large, sont indépendants du clustering et constituent des composants supplémentaires de l'approche globale de l'amélioration de la disponibilité.



Il est possible de configurer les interfaces réseau en tant que ressources singleton ou privées, à condition qu'elles possèdent une configuration IP statique (les interfaces configurées pour utiliser DHCP pouvant uniquement être privées, l'utilisation de DHCP est déconseillée dans les clusters). 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 une seule

tête à un moment précis. De la même manière, les périphériques correspondants sur chaque tête doivent être connectés aux mêmes réseaux afin que le service soit fourni correctement dans l'état de basculement. Pour un exemple concret, voir l'illustration 5. 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 têtes. Etant donné que les identifiants dépendent du type de périphérique et de l'ordre dans lequel il est détecté par l'appareil, le matériel installé sur les têtes clusterisées doit être identique. En outre, chaque emplacement doit recevoir du matériel identique, installé dans le même ordre sur les deux têtes. Vous pouvez obtenir l'aide de votre revendeur Oracle agréé ou de tout agent technique dans 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 répliques. Toutefois, elles peuvent devenir actives uniquement lorsque les interfaces auxquelles elles sont associées sont opérationnelles. Une route liée à une interface actuellement en mode veille (exportée) est sans conséquence tant que l'interface n'est pas activée lors du processus de reprise. Cela a son importance lorsque deux pools sont configurés et qu'ils doivent être rendus disponibles sur un sous-réseau commun. Dans ce cas, si ce sous-réseau constitue l'emplacement d'origine d'un routeur que les appareils doivent utiliser pour atteindre un ou plusieurs réseaux, il faut configurer une route distincte (par exemple, une deuxième route par défaut) puis la lier à chacune des interfaces actives et en veille associées à ce sous-réseau.

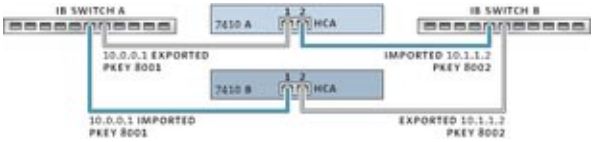
- Exemple : l'interface e1000g3 est affectée à 'alice' et e1000g4 à 'bob'. Chaque interface possède une adresse dans le réseau 172.16.27.0/24 et permettra de fournir le service aux clients dans le réseau 172.16.64.0/22, accessible via 172.16.27.1. Deux routes doivent être créées sur 172.16.64.0/22 via 172.16.27.1. L'une doit être associée à e1000g3 et l'autre à e1000g4.

Il est souvent avantageux d'affecter à chaque tête clustérisée une adresse IP (généralement, sur un réseau de gestion dédié) à utiliser uniquement pour l'administration et pour désigner l'interface sur laquelle est configurée l'adresse en tant que ressource privée. Cela garantit l'accès à toutes les têtes qui fonctionnent à partir du réseau de gestion, même lorsque leur état actuel est AKCS_STRIPPED et qu'elles sont en attente de rétablissement. Ce type d'attribution est encore plus important en cas d'utilisation de services tels que LDAP et Active Directory, qui nécessitent d'accéder aux autres ressources réseau même lorsque la tête ne fournit pas elle-même le service. Si cela n'est pas pratique, il est indispensable que le processeur de service soit affecté à un réseau fiable et/ou à un concentrateur de terminaux série afin que la tête puisse être gérée à partir de la console système. Si aucune de ces actions n'est effectuée, il sera impossible de gérer ou de surveiller une tête qui vient d'être initialisée tant que le rétablissement n'est pas terminé. En revanche, il peut aussi être nécessaire de surveiller ou de gérer la tête fournissant actuellement le service (ou le service pour un pool de stockage particulier). Cette approche est probablement plus utile lorsqu'il est nécessaire de modifier certains aspects du stockage lui-même (p. ex, pour modifier une propriété de partage ou une nouvelle LUN). Pour cela, vous pouvez soit effectuer des tâches administratives dans les interfaces de service, soit affecter une interface singleton

distincte à utiliser uniquement dans le but de gérer le pool avec lequel elle est mise en correspondance. Dans les deux cas, l'interface doit être affectée à la même tête que le pool utilisé pour la gestion.

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.

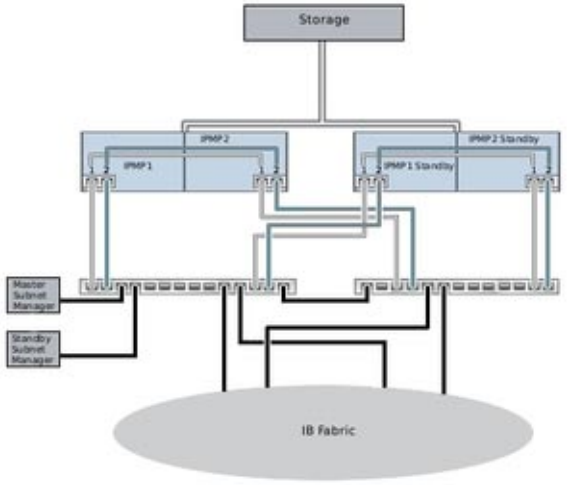


Pour garantir une configuration de cluster appropriée, chaque tête doit recevoir des HCA identiques dans des emplacements identiques. En outre, chaque port HCA correspondant doit être configuré dans la même partition (pkey) sur le gestionnaire de sous-réseau avec des privilèges d'appartenance identiques 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 une seule tête 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 ci-dessus. Vous pouvez obtenir l'aide de votre revendeur Oracle agréé ou de tout agent technique dans la planification des mises à niveau matérielles compatibles.

Scénarios de chemin redondant

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.



Prévention des conditions 'split-brain'

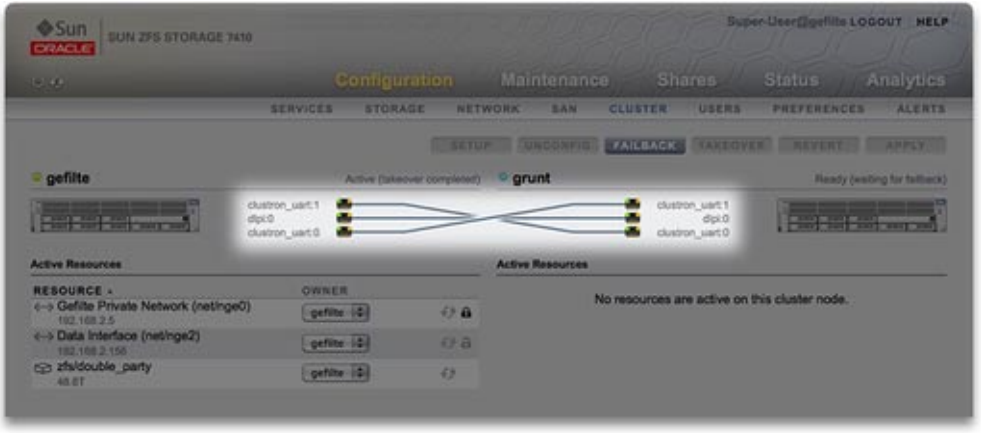
Un mode d'échec courant dans les systèmes clusterisés est le *split-brain*. Dans cette condition, chacune des têtes clusterisées croit que son pair subit une défaillance et tente une reprise. En dehors de toute logique supplémentaire, cette condition peut entraîner une large gamme de comportements inattendus 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 têtes. 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 la tête qui continuera avec la reprise.

Un certain nombre de mécanismes d'arbitrage est utilisé 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 clusterisé 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 tête 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 la tête 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 clusterisés 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 un JBOD est mis 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 cette condition 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.



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

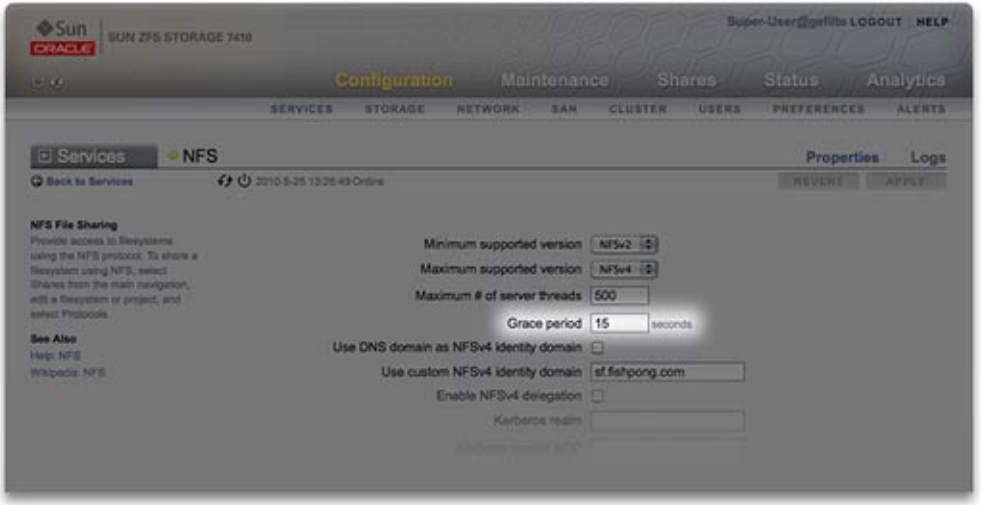
vers chaque JBOD (voir illustration) avant et après la mise en production du cluster, exception faite évidemment des modifications temporaires de câblage pour prendre en charge les améliorations des fonctionnalités ou le remplacement des composants défectueux. Les administrateurs doivent utiliser des alertes pour surveiller l'état des liaisons d'interconnexion du cluster et des chemins JBPD 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.

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 (voir l'illustration). 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 section Propriété de période de grâce

dans NFS Propriétés.



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). Rappelez-vous qu'un ensemble de disques contient une moitié de JBOD à condition que les baies de disque de cette moitié 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 chargés des déploiements clusterisés 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 de la tête A vers la tête B qu'il n'en faudra pour que la tête A effectue la reprise à partir de la tête 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 clusterisé dans un environnement de production.

Tâches

Lorsque vous configurez un cluster à partir de deux nouveaux appareils, suivez la procédure suivante.

Cluster Tâches

Procédure de configuration

1. Branchez les câbles d'alimentation et au moins un câble Ethernet sur chaque appareil.
2. Reliez les contrôleurs d'interconnexion du cluster entre eux, comme indiqué à la section Câblage des noeuds ci-après. Vous pouvez également procéder à la configuration du cluster et ajouter ces câbles de façon dynamique durant le processus de configuration.
3. Reliez les HBA et les JBOD partagés comme indiqué dans les diagrammes de câblage des JBOD du schéma de configuration fourni avec votre appareil.

4. Mettez les deux appareils sous tension mais ne commencez pas la configuration. Sélectionnez un seul des appareils pour procéder à sa configuration (ce choix est arbitraire). Il sera dénommé appareil principal à des fins de configuration. Connectez-vous et accédez à la console série de cet appareil et effectuez la configuration TTY initiale en procédant comme vous le feriez sur un appareil autonome. Remarque : ne procédez pas à la configuration TTY initiale sur l'appareil secondaire. En effet, il sera automatiquement configuré lors de la configuration du cluster.
5. Sur l'appareil principal, accédez à la BUI ou à la CLI pour commencer la configuration du cluster. La configuration du cluster peut être sélectionnée dans le cadre de la configuration initiale lorsque le contrôleur d'interconnexion de cluster a été installé. Vous pouvez également effectuer une configuration autonome à ce stade et remettre à plus tard la configuration du cluster. Dans ce cas, exécutez la tâche de configuration du cluster en cliquant sur le bouton Configuration dans Configuration->Cluster.
6. Lors de la première étape de configuration du cluster, un diagramme des liaisons actives du cluster s'affiche. Vous devez voir trois câbles bleus continus, un pour chaque connexion. Si ce n'est pas le cas, ajoutez les câbles manquants maintenant. Lorsque vous voyez les trois câbles, vous pouvez continuer en cliquant sur le bouton Valider.
7. Entrez le nom de l'appareil et le mot de passe root initial pour le deuxième appareil (cela équivaut à effectuer la configuration de la console série initiale pour le nouvel appareil). Lorsque vous cliquez sur le bouton Valider, des barres de progression s'affichent durant la configuration du deuxième appareil.
8. Si vous configurez le clustering dans le cadre de la configuration initiale de l'appareil principal, vous êtes invité à effectuer la configuration initiale de la même manière que pour un appareil unique. Toutes les modifications apportées à la configuration sont automatiquement propagées sur l'autre appareil. Effectuez la configuration initiale, en prenant en considération les restrictions et remarques : les interfaces réseau configurées via DHCP ne peuvent basculer entre les têtes, et ne peuvent donc pas être utilisées par les clients pour accéder au stockage. Assurez-vous donc d'affecter des adresses IP statiques à toute interface réseau qui sera utilisée par les clients pour accéder au stockage. Si vous avez sélectionné une interface réseau configurée via DHCP durant la configuration initiale TTY et que vous souhaitez utiliser cette interface pour l'accès au client, vous devrez définir son type d'adresse sur Statique avant de continuer. Les meilleures pratiques conseillées incluent la configuration et l'attribution à chaque tête d'une interface réseau privée pour l'administration, ce qui active l'administration via l'une ou l'autre des têtes sur le réseau (BUI ou CLI), indépendamment de l'état du cluster. Si des routes sont requises, assurez-vous de créer une route sur une interface qui sera assignée à chaque tête. Pour des exemples précis, reportez-vous à la section précédente.
9. Poursuivez la configuration initiale jusqu'à l'étape du pool de stockage. Chaque pool de stockage ainsi que les interfaces réseau utilisées par les clients pour atteindre ce dernier peuvent être contrôlés par le pair du cluster lors de la reprise. Si vous créez deux pools de stockage, chaque tête offre normalement aux clients l'accès au pool auquel ils sont affectés. En cas d'échec de l'une des têtes, l'autre fournit aux clients l'accès aux deux pools. Si vous créez un seul pool, la tête à laquelle aucun pool n'est affecté fournit le service aux clients

uniquement en cas d'échec de son pair. Les pools de stockage sont attribués aux têtes au moment de leur création. La boîte de dialogue de configuration du stockage offre la possibilité de créer un pool attribué à chaque tête indépendamment. La plus petite unité de stockage pouvant être attribuée à un pool est un demi-JBOD. Ainsi, si vous souhaitez créer deux pools mais que vous ne possédez qu'un JBOD, accédez au menu contextuel et sélectionnez la moitié de votre JBOD pour chaque pool. D'autre part, il est impossible de créer deux pools si vous ne possédez qu'un JBOD à moitié rempli. Si vous souhaitez créer deux pools, ils ne doivent pas nécessairement être de la même taille et il est possible de créer des sous-divisions de stockage disponible.

10. Après avoir terminé la configuration de base, vous pouvez affecter des ressources à chaque tête. En règle générale, il est nécessaire d'attribuer uniquement des interfaces réseau. Les pools de stockage sont automatiquement attribués au cours de l'étape de configuration du stockage.
11. Validez les attributions de ressources et effectuez le rétablissement initial décrit ci-dessous depuis l'interface utilisateur du cluster. Si vous continuez d'exécuter la configuration d'origine de l'appareil principal, cet écran apparaîtra à la fin de la séquence de configuration. Si vous exécutez manuellement la configuration du cluster après une configuration initiale, accédez à l'écran Configuration/Cluster pour exécuter ces tâches. Pour plus d'informations, reportez-vous à la section Interface utilisateur du cluster ci-après.

Arrêter de la configuration clusterisée

- Vérifiez l'état du cluster à l'aide de la CLI pour exécuter les commandes suivantes :

```
nas-7420-1a:> configuration cluster
nas-7420-1a:configuration cluster> show
```

- Vous trouverez ci-dessous un exemple de propriétés de cluster : **`state`** indique le statut du noeud dans lequel vous avez exécuté la commande ; **`peer_state`** indique l'état de l'autre noeud.

```
state = AKCS_OWNER
description = Active (takeover completed)
peer_asn = 365ed33c-3b9d-c533-9349-8014e9da0408
peer_hostname = nas-7420-1b
peer_state = AKCS_STRIPPED
peer_description = Ready (waiting for failback)
```

- Utilisez le tableau suivant pour vérifier l'état du noeud.

Ce noeud	Autre noeud	Condition
AKCS_CLUSTERED	AKCS_CLUSTERED	Les deux noeuds fonctionnent normalement.

Ce noeud	Autre noeud	Condition
AKCS_OWNER	AKCS_STRIPPED	Ce noeud a toutes les ressources et est en mode actif. L'autre noeud est un noeud de secours et n'a pas de ressources.
AKCS_OWNER	Redémarrage	Un autre noeud est en cours de redémarrage et ce noeud a toutes les ressources.
AKCS_OWNER	inconnu	Ce noeud ne connaît pas de partenaire.

REMARQUE : si l'état des têtes n'est PAS d'accord, le cluster peut rencontrer un problème. Contactez les services de support Oracle avant de lancer la procédure.

- Arrêtez la tête de secours à l'aide de la CLI pour exécuter les commandes suivantes :

```
nas-7420-1b:configuration cluster> cd /
nas-7420-1b:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N)
```

- Pour vérifier que vous souhaitez arrêter l'autre tête, saisissez **Y**.

REMARQUE : si les deux têtes ont un état de AKCS_CLUSTERED, effectuez une reprise sur la tête survivante puis arrêtez la tête de secours.

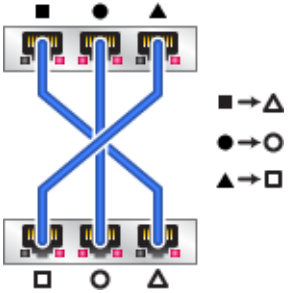
- Confirmez que la tête de secours est éteinte.
- Arrêtez la tête active à l'aide de la CLI pour exécuter les commandes suivantes :

```
nas-7420-1a:configuration cluster> cd /
nas-7420-1a:> maintenance system poweroff
This will turn off power to the appliance. Are you sure? (Y/N)
```

- Pour vérifier que vous souhaitez arrêter l'autre tête, saisissez **Y**.
- Confirmez que les deux têtes sont hors tension.
- Mettez le JBOD hors tension.

Câblage de noeuds

Les noeuds de tête clusterisés doivent être reliés ensemble à l'aide du contrôleur d'interconnexion de cluster.



Le contrôleur fournit trois liaisons redondantes permettant aux têtes de communiquer : deux liaisons série (les deux connecteurs extérieurs) et une liaison Ethernet (connecteur du milieu).

A l'aide de câbles droits Ethernet de catégorie 5 ou supérieure (trois câbles de 1 m sont fournis avec votre configuration de cluster), connectez le noeud de tête conformément au diagramme de gauche.

Le câblage du cluster peut être effectué soit avant la mise sous tension d'une des têtes, soit en direct, durant l'exécution de la tâche de configuration guidée du cluster. L'interface utilisateur affiche le statut de chaque liaison, comme indiqué plus bas sur cette page. Pour pouvoir continuer la configuration du cluster, vous devez établir les trois liaisons.

Câblage des JBOD

Vous devez relier vos JBOD aux deux appareils afin de pouvoir commencer la configuration du cluster. Reportez-vous à la section Installation : diagrammes de câblage ou conformez-vous au schéma de configuration rapide fourni avec votre système.

BUI

La vue Configuration->Cluster offre une présentation graphique du statut de la carte de cluster, du noeud de tête du cluster et de toutes les ressources.

L'interface contient les objets suivants :

- A 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 dernière est connectée et active (la ligne disparaît si cette connexion est interrompue ou lors du redémarrage/de la réinitialisation du système).
- La liste des ressources PRIVATE et SINGLETON (voir la section Introduction ci-dessus) actuellement assignées à chaque système apparaît sous l'image miniature de chaque noeud 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 dans 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.

L'interface contient les boutons suivants :

Bouton	Description
Configuration	Si le cluster n'est pas encore configuré, exécutez la tâche de configuration guidée du cluster, puis revenez à l'écran actuel. Reportez-vous à la section ci-dessus pour une description détaillée de cette tâche.
Annuler config	Mettre à jour un noeud en vue d'un fonctionnement autonome en annulant la configuration du cluster. Reportez-vous à la section ci-dessous pour une description détaillée de cette tâche.
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 noeuds 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)

Tâches

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. Deux raisons justifie d'annuler la configuration du cluster :

- 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).

Cluster Tâches

Annulation de la configuration du clustering

1. Sélectionnez le contrôleur du stockage dont rétablir la configuration d'usine. Notez que, en cas de remplacement d'un contrôleur de stockage défectueux, vous pouvez passer directement à l'étape 3 si ce contrôleur ne sera pas remis en service sur votre site.
2. Dans la console système du contrôleur de stockage dont il faut rétablir la configuration d'origine, réinitialisez les paramètres d'usine.
3. Le contrôleur de stockage est réinitialisé et son pair commence la reprise normalement. Avant de permettre au contrôleur de stockage de réinitialiser les paramètres d'usine (c.-à-d., avant de continuer au-delà du menu d'initialisation), mettez-le hors tension et patientez jusqu'à ce que son pair termine la reprise.
4. Débranchez les câbles d'interconnexion de cluster (voir ci-dessus) et débranchez le contrôleur de stockage mis hors tension des boîtiers de stockage externes du cluster.
5. Sur le contrôleur de stockage restant, cliquez sur le bouton Annuler config de l'écran Configuration -> Clustering. Toutes les ressources sont affectées au contrôleur de stockage restant, l'autre n'étant plus membre d'aucun cluster.

Le cas échéant, le contrôleur de stockage débranché peut désormais être connecté à son propre volume de stockage, mis sous tension, puis configuré normalement. Si vous remplacez un contrôleur de stockage défaillant, branchez le nouvel équipement au contrôleur de stockage restant et au volume de stockage, puis démarrez la tâche de configuration du cluster décrite ci-dessus.

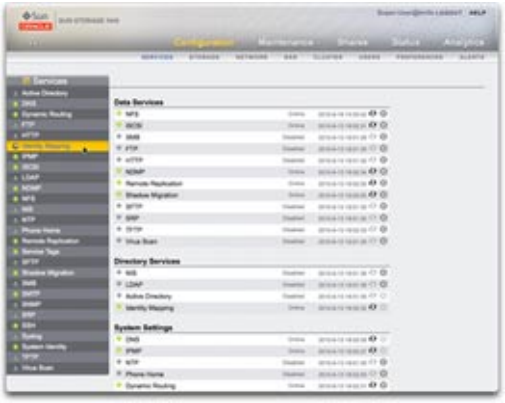
Remarque : si votre cluster compte au moins deux pools, la propriété de tous les pools est attribuée au contrôleur de stockage restant après la configuration. Dans les versions logicielles antérieures à 2010.Q1.0.0, cette configuration n'était pas prise en charge. Si vous exécutez une version antérieure, vous devez soit détruire l'un des deux pools, joindre un nouveau contrôleur de stockage, effectuer la tâche de configuration du cluster décrite ci-dessus, puis réattribuer la

propriété de l'un des pools au contrôleur du stockage de remplacement, soit procéder à une mise à niveau vers la version logicielle 2010.Q1.0.0 ou ultérieure incluant la prise en charge de plusieurs pools par contrôleur de stockage.

◆ ◆ ◆ CHAPITRE 4

Services

Services



L'écran Services présente un panneau latéral pour la navigation rapide entre les services.

Introduction

Vous pouvez configurer les services suivants sur un l'appareil.

Services de données

Service	Description	Ports utilisés
NFS	Accès au système de fichiers via les protocoles NFSv3 et NFSv4	111 et 2049

Service	Description	Ports utilisés
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
NDMP	Service hôte NDMP	10000
Réplication distante	Réplication distante	216
Shadow Migration	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	

Services d'annuaire

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.

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	
Identity Mapping	Mappage entre les entités Windows et les ID Unix	

Paramètres système

Service	Description	Ports utilisés
DNS	Client du service de noms de domaine	53
Routage dynamique	Protocoles de routage dynamiques RIP et RIPng	
IPMP	Multipathing sur réseau IP pour le basculement IP	
NTP	Client NTP (Network Time Protocol)	
Phone Home	Enregistrement du produit et configuration du support	443
Service Tags	Prise en charge de l'inventaire de produits	443
SMTP	Configuration du serveur de courrier sortant	
SNMP	SNMP pour l'envoi de déroutements en cas d'alertes et d'informations relatives à l'état de l'appareil	

Service	Description	Ports utilisés
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	

Accès à distance

Service	Description	Ports utilisés
SSH	SSH pour l'accès à la CLI	22
BUI	Browser User Interface, interface utilisateur de navigateur	215

Sécurité

Service	Description	Ports utilisés
Kerberos	Authentification Kerberos V	88
Modification & définition du mot de passe de Kerberos V (SET_CHANGE)	464	
Modification & définition du mot de passe de Kerberos V (RPCSEC_GSS)	749	

BUI

Les écrans BUI Services permettent d'afficher et de modifier les services et les paramètres décrits dans les tableaux ci-dessus. Double cliquez sur une ligne de service pour afficher l'écran de définition de ce service. Les tableaux suivants décrivent 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 placez le pointeur 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.
	Activer ou désactiver le service
	Redémarrer le service
	Impossible d'activer/de désactiver ce service
	Impossible de redémarrer le service actuellement (il faut commencer par l'activer)

Reportez-vous à la section Utilisation basique de la documentation pour consulter une liste complète des icônes.

Affichage de l'écran d'un service spécifique

Pour consulter ou modifier les propriétés d'un service spécifique, placez le pointeur sur l'icône de statut située à gauche du nom de service. L'icône de statut se transforme en flèche lorsque vous cliquez pour afficher l'écran des propriétés du service sélectionné.

Remarque : 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.

Activation d'un service

Lorsqu'un service n'est pas en ligne, cliquez sur l'icône pour l'activer .

Désactivation d'un service

Si un service est en ligne et que vous souhaitez le désactiver, cliquez sur l'icône pour le mettre hors ligne .

Définition des propriétés

Pour définir les propriétés d'un service, affichez l'écran correspondant (en double-cliquant sur le service souhaité). Modifiez les propriétés puis cliquez sur le bouton APPLIQUER. Le bouton RETABLIR permet de rétablir les propriétés avant que vous ne les modifiiez.

Affichage des journaux de service

Certains écrans de service offrent également 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, il propose des journaux. Les journaux peuvent fournir les informations suivantes :

- Heure de modification de l'état du service
- Messages d'erreur du service

Le contenu du journal est spécifique à chaque service et est susceptible d'être modifié lors des futures mises à jour du logiciel de l'appareil. Les exemples de messages suivants sont fréquemment utilisés dans cette version de l'appareil :

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 param
Execution de la méthode d'arrêt	Le service est en cours de fermeture.
Activé	L'état du service a été vérifié pour savoir s'il doit être démarré (p. ex lors de l'initialisation du système) ; l'état trouvé est activé.
Désactivé	L'état du service a été vérifié pour savoir s'il doit être démarré (p. ex lors de l'initialisation du système) ; l'état trouvé est désactivé.

L'exemple suivant est extrait du service NTP :

```
[ Oct 11 21:05:31 Enabled. ]
[ Oct 11 21:07:37 Executing start method (...). ]
[ Oct 11 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.

CLI

La section des services de la CLI se trouve sous `configuration services`. A l'aide de la commande `show`, répertoriez l'état actuel de tous les services :

```
caji:> configuration services
caji:configuration services> show
Services:
```

```
                ad => disabled
               smb => disabled
               dns => online
        dynrouting => online
               ftp => disabled
              http => disabled
          identity => online
             idmap => online
              ipmp => online
             iscsi => online
              ldap => disabled
              ndmp => online
               nfs => online
               nis => disabled
               ntp => disabled
       replication => online
              scrk => disabled
              sftp => disabled
            shadow => online
              smtp => online
              snmp => disabled
               ssh => online
            syslog => disabled
              tags => online
              tftp => disabled
             vscan => disabled


Children:
                ad => Configure Active Directory
               smb => Configure SMB
               dns => Configure DNS
        dynrouting => Configure Dynamic Routing
               ftp => Configure FTP
              http => Configure HTTP
          identity => Configure System Identity
             idmap => Configure Identity Mapping
              ipmp => Configure IPMP
             iscsi => Configure iSCSI
              ldap => Configure LDAP
              ndmp => Configure NDMP
               nfs => Configure NFS
               nis => Configure NIS
               ntp => Configure NTP
       replication => Configure Remote Replication
              scrk => Configure Phone Home
              sftp => Configure SFTP
            shadow => Configure Shadow Migration
              smtp => Configure SMTP
              snmp => Configure SNMP
               srp => Configure SRP
               ssh => Configure SSH
            syslog => Configure Syslog
              tags => Configure Service Tags
              tftp => Configure TFTP
             vscan => Configure Virus Scan
           routing => Configure Routing Table
```

Sélection d'un service

Sélectionnez un service en saisissant son nom. Par exemple, pour sélectionner `nis` :

```
caji:configuration services> nis
caji:configuration services nis>
```

Après avoir sélectionné un service, vous pouvez afficher son état, l'activer ou le désactiver et définir ses propriétés.

Affichage de l'état d'un service

La commande `show` permet d'afficher l'état d'un service :

```
caji:configuration services nis> show
Properties:
                     <status> = online
                       domain = fishworks
                    broadcast = true
                    ypservers =
```

Activation d'un service

La commande `enable` permet d'activer un service :

```
caji:configuration services nis> enable
```

Désactivation d'un service

La commande `disable` permet de désactiver un service :

```
caji:configuration services nis> disable
```

Définition des propriétés

La commande `set` permet de définir les propriétés du service sélectionné. Après avoir définir les propriétés, exécutez la commande `commit` pour enregistrer et activer la nouvelle configuration :

```
caji:configuration services nis> set domain="mydomain"
                         domain = mydomain (uncommitted)
caji:configuration services nis> commit
caji:configuration services nis> show
Properties:
                     <status> = online
                       domain = mydomain
                    broadcast = true
                    ypservers =
```

Remarque : 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.

Affichage des journaux de service

Il n'est pas possible de consulter les journaux de service dans la CLI. Utilisez la BUI comme indiqué ci-dessus.

Aide sur un service

Entrez `help` pour afficher toutes les commandes d'un service :

```
caji: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
```

NFS

Introduction

Network File System (NFS) est un protocole standard du marché qui permet de partager des fichiers sur un réseau. L'appareil Sun ZFS Storage 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 Espace de noms du système de fichiers.

Propriétés

Propriété	Description
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.
Nb 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.
Période de grâce	Définissez 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) suite à 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 de service 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 pour 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 peuvent survenir pendant des événements comme une mise à niveau non simultanée, et le redémarrage de l'appareil à l'aide de la commande de CLI `maintenance system reboot` ou le redémarrage à l'aide de l'icône de BUI. Pour les interruptions de service planifiées, le service NFS traite toutes les demandes de service 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.
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.

Propriété	Description
Domaine Kerberos	Un domaine désigne un réseau logique qui définit un groupe de systèmes situé s un même centre de distribution de clés (KDC) maître. Les noms de domaine pe contenir n'importe quelle chaîne ASCII. De manière générale, votre nom de do Kerberos est identique à votre nom de domaine DNS, à cette différence près qu'i en majuscule. Cette convention vous aide à distinguer les problèmes qui survie dans le service Kerberos et dans l'espace de noms DNS, tout en continuant d'util un nom familier.
KDC maître Kerberos	Dans chaque domaine, vous devez inclure un serveur qui conserve une copie m de la base de données des identités (principal). La différence la plus significative un KDC maître et un KDC esclave est que seul le KDC maître gère les demande d'administration de la base de données. Par exemple, vous devez modifier un m passe ou ajouter une nouvelle identité au niveau du KDC maître.
KDC esclave Kerberos	L'esclave contient des copies de duplication de la base de données des identités. serveur KDC maître et le serveur KDC esclave créent tous deux des tickets permettant d'établir l'authentification.
Principal admin Kerberos	Cette propriété identifie le client. Par défaut, un nom d'identité inclut trois composants : le client primaire, l'instance et le domaine. Vous pouvez spécifier u identité en tant que `joe`, `joe/admin`, ou `joe/admin@ENG.EXAMPLE.COM`.
Mot de passe admin Kerberos	Définissez le mot de passe de l'identité admin.
Protocole OISP (Oracle Intelligent Storage Protocol)	Le service NFSv4 inclut la prise en charge d'Oracle Intelligent Storage Protocol, permet aux clients Oracle Database NFSv4 de transmettre des informations d'optimisation au serveur ZFS Storage Appliance NFSv4. Pour plus d'informati reporter à la section Oracle Intelligent Storage Protocol.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

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.

Domaines Kerberos

La configuration d'un domaine Kerberos crée des identités de service et ajoute les clés nécessaires au fichier keytab local du système. Le service NTP 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 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. Si vous avez configuré votre appareil pour rejoindre un domaine Active Directory, vous ne pouvez pas le configurer en tant que membre d'un domaine Kerberos.

Pour plus d'informations sur la configuration de KDC et de clients kerberisés, consultez la page Web suivante : 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 Securité 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 Kerberized **`doivent`** accéder à l'appareil à l'aide d'une adresse IP qui résout un nom de domaine complet (FQDN) pour ces identités. 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

Ces journaux sont disponibles pour le service 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

Journal	Description
network-nfs-nlockmgr:default	Journal du démon lockd NFS qui prend en charge les opérations de verrouillage des enregistrements des fichiers

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Analyse

Vous pouvez surveiller l'activité NFS dans la section Analyse. La surveillance inclut :

- 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

Remarque : lorsque le serveur NFS est réinitialisé ou fait l'objet d'un basculement, le nom de fichier est *inconnu* sur le serveur jusqu'à ce qu'il soit à nouveau ouvert à partir du client. Le fichier apparaît comme *inconnu* dans les feuilles de travail Analyse.

CLI

Le tableau suivant décrit le mappage entre les propriétés de la CLI et les descriptions des propriétés de la BUI ci-dessus.

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
enable_delegation	Activer la délégation NFSv4
krb5_realm	Domaine Kerberos
krb5_kdc	KDC maître Kerberos
krb5_kdc2	KDC esclave Kerberos

Propriété de la CLI	Propriété de la BUI
krb5_admin	Principal admin Kerberos

Tâches

NFS Tâches

Partage d'un système de fichiers via NFS

1. Accédez à l'écran 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 existant 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.

Voir aussi

- http://fr.wikipedia.org/wiki/Network_File_System (`http://fr.wikipedia.org/wiki/Network_File_System`)

iSCSI

Introduction

Lorsque vous configurez une 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.

Propriétés

Propriété	Description
Use iSNS	La détection iSNS est activée.
iSNS Server	Serveur iSNS
Use RADIUS	RADIUS est activé.
RADIUS Server	Serveur RADIUS
RADIUS Server Secret	Clé secrète du serveur RADIUS

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Authentification

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.

Autorisation

Le service iSCSI vous permet de spécifier une liste globale d'initiateurs que vous pouvez utiliser au sein de groupes d'initiateurs.

Cibles et initiateurs

Pour plus d'informations sur les initiateurs et les cibles iSCSI, reportez-vous à la section Réseau de stockage (SAN).

CLI

Pour consulter des exemples d'administration des initiateurs et des cibles iSCSI, reportez-vous à la section Réseau de stockage (SAN).

Conseils

Dépannage

Si votre initiateur ne parvient pas à se connecter à votre 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 à la LUN est un membre du groupe d'initiateurs de cette LUN.
- Vérifiez que les cibles chargées d'exporter cette unité logique sont en ligne.
- Vérifiez que le statut de fonctionnement de la LUN est en ligne.
- Vérifiez le numéro d'unité logique de chaque LUN.

Au cours du basculement/rétablissement, si les E/S de la copie réduite iSER du client Red Hat ne sont plus fonctionnelles :

- Attribuez la valeur 300 (secondes) au paramètre `node.session.timeo.replacement_timeout` du fichier `/etc/iscsi/iscsid.conf`.

Voir aussi

- http://fr.wikipedia.org/wiki/ISCSI (`http://fr.wikipedia.org/wiki/ISCSI`)
- http://en.wikipedia.org/wiki/Internet_Storage_Name_Service (`http://en.wikipedia.org/wiki/Internet_Storage_Name_Service`)
- http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service (`http://fr.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service`)
- http://fr.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol (`http://fr.wikipedia.org/wiki/Challenge-Handshake_Authentication_Protocol`)

SMB

Introduction

Le service SMB fournit un accès aux systèmes de fichiers par le biais du protocole SMB. Les systèmes de fichiers doivent être configurés pour le partage via SMB à partir de la configuration Partages.

Propriétés

Propriété	Description
Niveau de compatibilité 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 Oracle Solaris Information Library pour *smb*. NTLMv2 est le niveau de sécurité minimal recommandé pour éviter les failles de sécurité connues du public.
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.
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.
Nb maximal de threads serveur	Nombre maximal de threads (processus) serveur simultanés. La valeur par défaut est 1024.
Activer DNS dynamique	Décide si l'appareil utilise Dynamic DNS pour mettre à jour les enregistrements DNS dans le domaine Active Directory. La valeur par défaut est "désactivé".
Activer 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.
Restreindre l'accès anonyme à la liste de partages	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.
Commentaire système	Chaîne de texte significative.

Propriété	Description
Délai d'expiration de la session inactive	Paramétrage du délai d'attente avant l'inactivité d'une session.
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.
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).
SMB Signing Required	Lorsque la signature SMB est requise, tous les paquets SMB doivent être signés, sans quoi ils seront rejetés. Les clients qui ne prennent pas en charge la signature ne peuvent pas se connecter au serveur.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Propriétés des partages

Il faut suivre une certaine méthode pour définir plusieurs propriétés de partages lors de l'exportation d'un partage via 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 "'non sensible".
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 clients SMB risquent de ne pas fonctionner correctement.
Verrouillage obligatoire non bloquant	Cette propriété doit être activée pour autoriser le verrouillage par plage d'octets à fonctionner correctement.
Nom de la ressource	Nom utilisé par les clients pour désigner le partage. Pour plus d'informations sur la manière dont ce nom est hérité à partir d'un projet, reportez-vous à la documentation relative aux protocoles.

Propriété	Description
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 documentation relative aux protocoles.

Les propriétés Sensibilité à la casse et Rejeter non UTF-8 peuvent être définies uniquement au moment de la création d'un partage.

Interopérabilité NFS/SMB

L'appareil prend en charge les clients NFS et SMB qui accèdent simultanément aux mêmes partages. Pour configurer correctement l'appareil pour l'interopérabilité NFS/SMB, configurez les composants suivants :

- Configurez le service Active Directory.
- Etablissez une stratégie de mappage des identités et configurez le service.
- Configurez le protocole SMB.
- 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 racine 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 documentation relative à l'option Comportement d'héritage ACL.

Espaces de noms DFS

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. Dans l'exemple ci-dessous, les étapes permettent à l'utilisateur local SMB `dfsadmin` de manipuler les espaces de noms DFS.

Tâches

SMB Tâches

Exemple : manipulation d'espaces de nom DFS

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 où vous souhaitez modifier l'espace de noms DFS.

Règles autohome

La fonction de partage autohome élimine la tâche d'administration de définition et de gestion des partages de répertoire personnel pour chaque utilisateur accédant au système par le biais du protocole SMB. Les règles autohome mappent les clients SMB aux répertoires personnels. Il existe trois types de règles autohome :

Type	Description
Commutateur du service de noms	Cette règle autohome permet de rechercher un répertoire personnel via NIS ou LDAP puis de l'exporter vers le client SMB en tant que répertoire personnel lui appartenant.
Tous les utilisateurs	Règle autohome permettant de trouver des répertoires personnels en fonction de caractères génériques. Lorsqu'il remplace le nom de l'utilisateur, "&" correspond à l'utilisateur.
Utilisateur spécifique	Règle autohome qui fournit un répertoire personnel à un utilisateur spécifique.

Une règle autohome définie à l'aide du commutateur du service de noms et une autre définie pour tous les utilisateurs ne peuvent en aucun cas coexister.

Groupes locaux

Les groupes locaux désignent des groupes d'utilisateurs de domaine qui confèrent des privilèges supplémentaires à ces utilisateurs.

Groupe	Description
Administrators	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.

Comptes locaux

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 la lecture/l'écriture depuis l'appareil.

Intégration de MMC

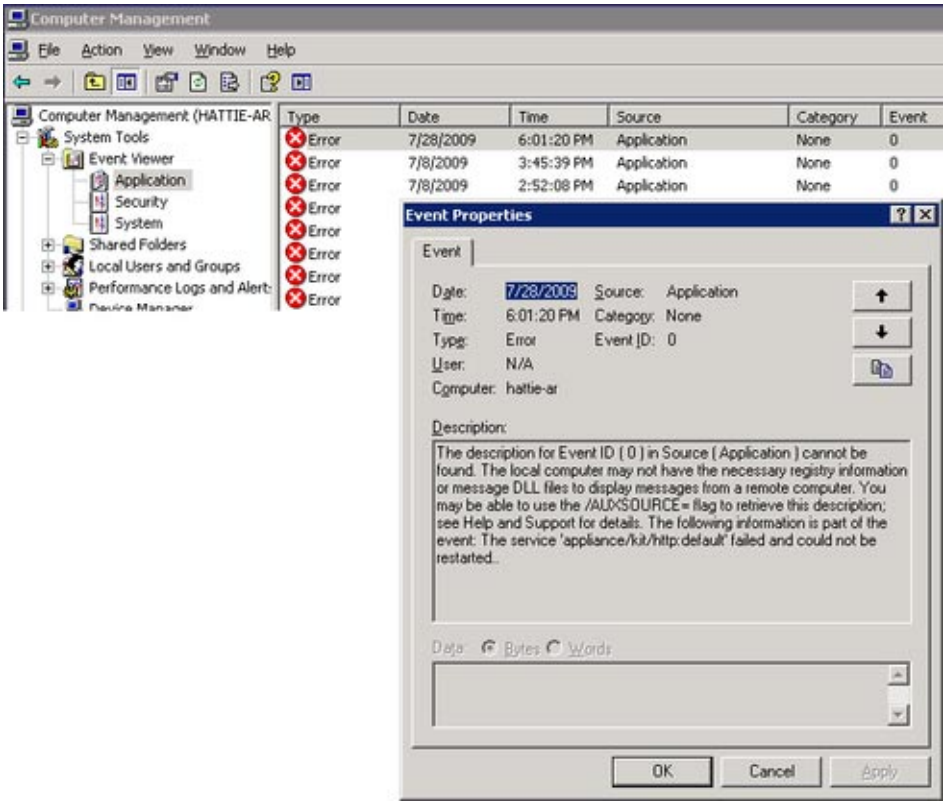
Microsoft Management Console (MMC) (MMC) est une infrastructure extensible de composants enregistrés, appelés composants logiciels enfichables, qui offre des fonctionnalités de gestion complète pour le système local et des systèmes distants du réseau. Computer Management est un ensemble d'outils de Microsoft 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 Sun ZFS Storage 7000 en mode groupe de travail, veillez à ajouter l'administrateur Windows qui doit utiliser la console de gestion dans le groupe local Administrators de l'appareil. Autrement, l'erreur `Access is denied` ou une erreur similaire s'affichera dans le client d'administration lors de la tentative de connexion à l'appareil via la console MMC.

Les appareils Sun ZFS Storage 7000 prennent en charge les fonctions de gestion d'ordinateur suivantes :

Observateur d'événements

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 Sun ZFS Storage 7000. La capture d'écran ci-dessous illustre le journal de d'application et la boîte de dialogue des propriétés en cas d'erreur.



Gestion des partages

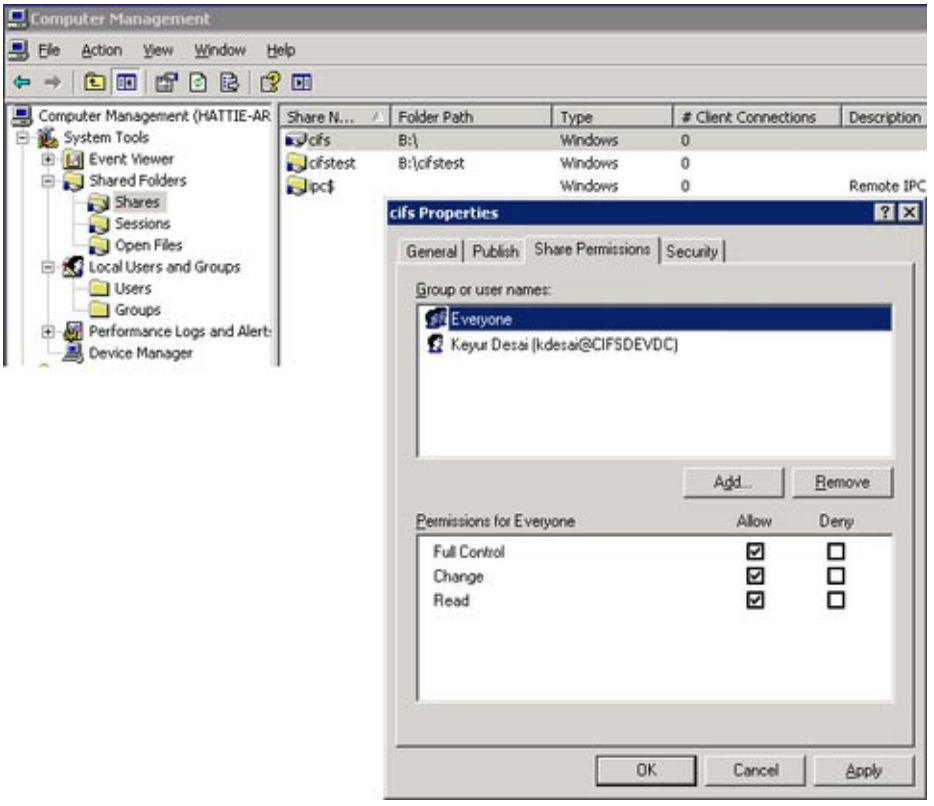
La prise en charge de la gestion des partages inclut les opérations suivantes :

- Etablissement de la liste des partages
- Définition des ACL sur les partages
- Modification des autorisations de partage
- Définition de la description d'un partage

A ce jour, les fonctionnalités suivantes ne sont pas prises en charge par la MMC :

- 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 ci-dessous illustre les propriétés d'autorisation d'un partage.



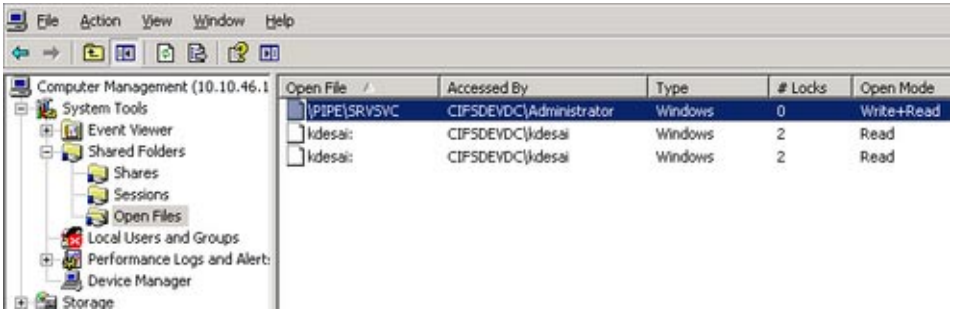
Utilisateurs, groupes et connexions

Les fonctionnalités prises en charge sont les suivantes :

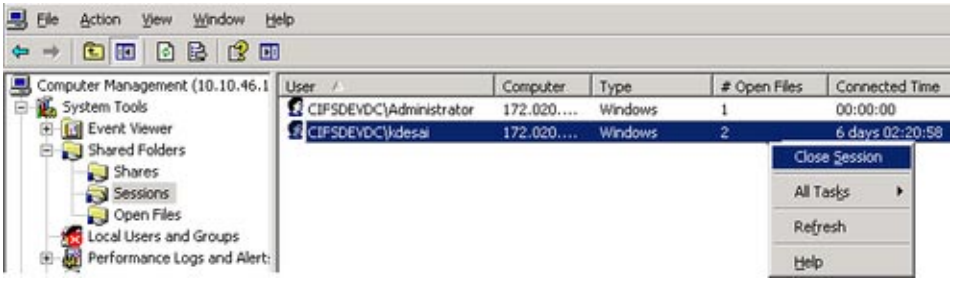
- Affichage des utilisateurs et des groupes SMB locaux
- Etablissement de la liste des connexions utilisateur, précisant le nombre de fichiers ouverts par connexion
- Fermeture des connexions utilisateur
- Etablissement de la liste des fichiers ouverts, précisant le nombre de verrous sur chaque fichier et le mode (lecture, écriture, etc.)

- Fermeture des fichiers ouverts

La capture d'écran ci-dessous illustre les fichiers ouverts par connexion.

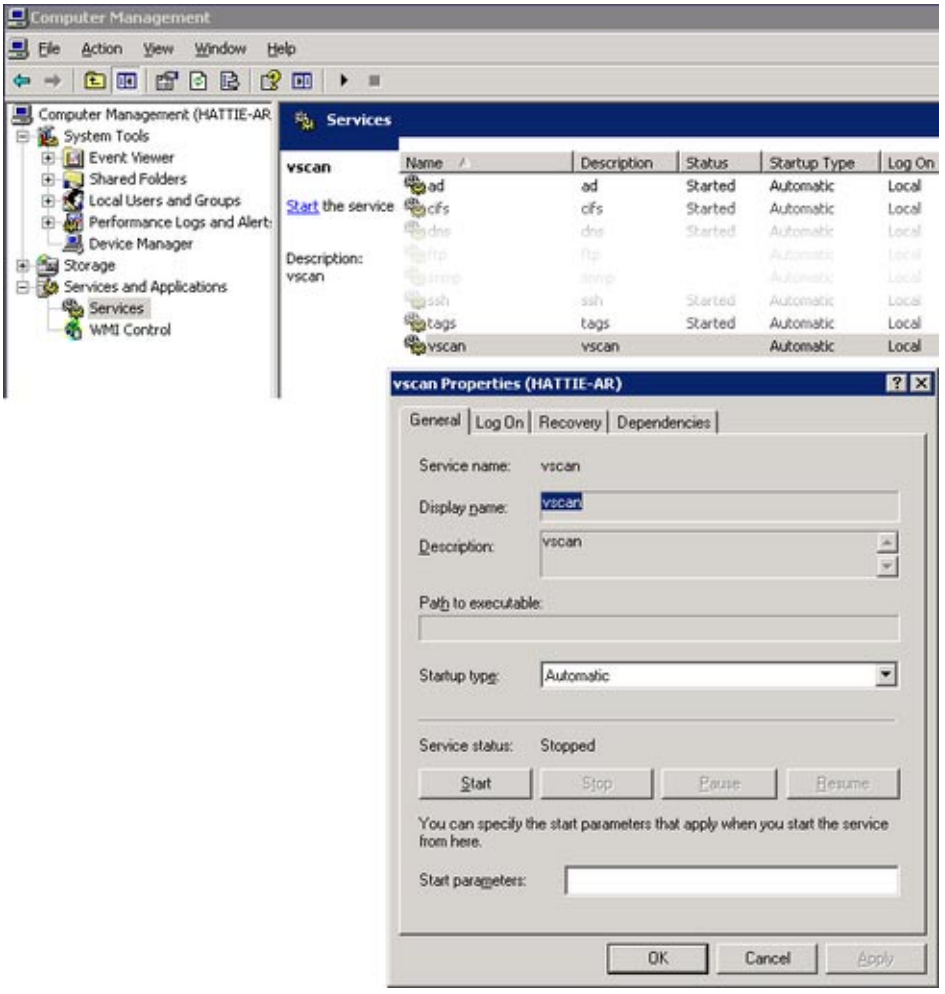


La capture d'écran ci-dessous illustre les sessions ouvertes.



Services

Il est possible d'établir la liste des services du système Sun ZFS Storage 7000. 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 ci-dessous illustre les propriétés générales du service 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.

UTILISATEURS	OPERATIONS AUTORISEES
Utilisateurs standard	Etablissement de listes de partages
Membres des groupes Administrators ou Power Users	Gestion des partages, établissement de listes des connexions utilisateur

UTILISATEURS	OPERATIONS AUTORISEES
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 d'événements

CLI

Vous trouverez ci-après des exemples d'administration SMB dans la CLI.

Ajout de règles autohome

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 :

```
twofish:> configuration services smb
twofish:configuration services smb> create
twofish:configuration services rule (uncommitted)> set use_nss=false
twofish:configuration services rule (uncommitted)> set user=Bill
twofish:configuration services rule (uncommitted)> set directory=/export/wdp
twofish:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
   ou=Engineering,CN=myhome"
twofish:configuration services rule (uncommitted)> commit
twofish:configuration services smb> list
RULE       NSS      USER         DIRECTORY            CONTAINER
rule-000   false    Bill         /export/wdp          dc=com,dc=fishworks,
   ou=Engineering,CN=myhome
```

Les règles autohome peuvent être créées à l'aide de caractères génériques. L'esperluette *&* correspond au nom de l'utilisateur et le point d'interrogation *?* à la première lettre du nom de l'utilisateur. Dans l'exemple suivant, des caractères génériques sont utilisés pour correspondre à tous les utilisateurs :

```
twofish:configuration services smb> create
twofish:configuration services rule (uncommitted)> set use_nss=false
twofish:configuration services rule (uncommitted)> set user=*
twofish:configuration services rule (uncommitted)> set directory=/export/?/&
twofish:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
   ou=Engineering,CN=myhome"
twofish:configuration services rule (uncommitted)> commit
twofish:configuration services smb> list
RULE       NSS      USER         DIRECTORY            CONTAINER
rule-000   false    Bill         /export/wdp          dc=com,dc=fishworks,
   ou=Engineering,CN=myhome
```

Le commutateur du service de noms peut également permettre de créer des règles autohome :

```
twofish:configuration services smb> create
twofish:configuration services rule (uncommitted)> set use_nss=true
twofish:configuration services rule (uncommitted)> set container="dc=com,dc=fishworks,
   ou=Engineering,CN=myhome"
twofish:configuration services rule (uncommitted)> commit
twofish:configuration services smb> list
RULE       NSS      USER         DIRECTORY            CONTAINER
rule-000   true                                       dc=com,dc=fishworks,
   ou=Engineering,CN=myhome
```

Ajout d'un utilisateur à un groupe local

```
twofish:configuration services smb> groups
twofish:configuration services smb groups> create
twofish:configuration services smb member (uncommitted)> set user=Bill
twofish:configuration services smb member (uncommitted)> set group="Backup Operators"
twofish:configuration services smb member (uncommitted)> commit
twofish:configuration services smb groups> list
MEMBER       USER                          GROUP
member-000   WINDOMAIN\Bill                Backup Operators
```

Tâches

Cette section fournit les instructions relatives à la configuration et à l'activation des appareils Sun ZFS Storage 7000 en vue du partage des fichiers via SMB à partir d'une configuration initiale à l'aide de la BUI.

SMB Tâches

Configuration initiale

La configuration initiale de l'appareil peut s'effectuer dans la BUI ou la CLI et prend généralement moins de 20 minutes. Elle peut également être réalisée ultérieurement en accédant au contexte Maintenance > Système dans la BUI ou la CLI. La configuration initiale vous guide généralement tout au long des étapes suivantes de la BUI.

1. Configurez des périphériques réseau, des liaisons de données et des interfaces.
2. Créez des interfaces en cliquant sur l'icône ⊕ ou en faisant glisser des périphériques dans les listes de liaisons ou d'interfaces.
3. Définissez les propriétés de votre choix et cliquez sur le bouton Appliquer pour les ajouter à la liste.
4. Définissez chaque interface sélectionnée comme 'active' ou 'de secours'.
5. Cliquez sur le bouton Appliquer en haut de la page pour valider vos modifications.
6. Configurez le DNS.
7. Saisissez le nom de domaine de base.
8. 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.

9. Configurez les clés d'authentification NTP afin de garantir la synchronisation temporelle.
10. Cliquez sur l'icône pour ajouter une nouvelle clé.
11. Spécifiez le numéro, le type et la valeur privée de la nouvelle clé et appliquez les modifications. La clé s'affiche sous forme d'option en regard de chaque serveur NTP spécifié.
12. Associez la clé au serveur NTP approprié et appliquez les modifications. Pour garantir la synchronisation temporelle, configurez l'appareil et les clients SMB pour qu'ils utilisent le même serveur NTP.
13. Désignez Active Directory comme le service d'annuaire des utilisateurs et des groupes.
14. Définissez le domaine de l'annuaire.
15. Cliquez sur le bouton Appliquer pour valider vos modifications.
16. Configurez un pool de stockage
17. Cliquez sur l'icône pour ajouter un nouveau pool.
18. Définissez le nom du pool.
19. Dans l'écran "Allouer et vérifier le stockage", configurez l'allocation JBOD pour le pool de stockage. L'allocation JBOD peut être réglée sur 'aucune', 'la moitié' ou 'tous'. Si aucun JBOD n'est détecté, contrôlez le câblage et l'alimentation du JBOD.
20. Cliquez sur le bouton Valider pour passer à l'écran suivant.
21. Dans l'écran "Configuration du stockage ajouté", sélectionnez le profil de données souhaité. Une évaluation de chaque profil de données en termes de disponibilité, de performances et de capacité est fournie. Utilisez ces évaluations pour déterminer la configuration la plus adaptée à vos besoins métier.
22. Cliquez sur le bouton Valider pour activer la configuration.
23. Configurez le support à distance.
24. Si l'appareil n'est pas directement connecté à Internet, configurez un proxy HTTP permettant au service de support à distance de communiquer avec Oracle.
25. Entrez le mot de passe et le nom d'utilisateur de votre compte en ligne. Une déclaration de confidentialité s'affiche ensuite.
26. 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 '$'.
27. Validez les modifications apportées à votre configuration initiale.

Configuration d'Active Directory

1. Créez un compte pour l'appareil dans le domaine Active Directory. Reportez-vous à la documentation Active Directory pour obtenir des instructions détaillées.
2. Dans l'écran Configuration > Services > Active Directory, cliquez sur le bouton Rejoindre le domaine.

3. Spécifiez le domaine Active Directory, l'utilisateur administratif et le mot de passe d'administration puis cliquez sur le bouton Appliquer pour valider les modifications.

Configuration d'un projet et d'un partage

1. Créez un projet.
2. Dans l'écran Partages, cliquez sur l'icône pour développer le panneau Projets.
3. Cliquez sur le lien Ajouter... pour ajouter un nouveau projet.
4. Spécifiez le nom du projet et appliquez la modification.
5. Sélectionnez le nouveau projet dans le panneau Projets.
6. Cliquez sur l'icône pour ajouter un système de fichiers.
7. Cliquez sur l'icône pour le système de fichiers.
8. Cliquez sur le lien Général et désactivez la case à cocher Hériter du projet.
9. Choisissez un point de montage sous /export, même si le nom de la ressource permet d'accéder aux partages SMB.
10. Dans l'écran Protocoles, définissez le nom de la ressource sur 'on' pour le projet.
11. Activez sharesmb et l'ACL au niveau du partage pour le projet.
12. Cliquez sur le bouton Appliquer pour activer la configuration.

Configuration du service de données SMB

1. Dans l'écran Configuration > Services > SMB, cliquez sur l'icône pour activer le service.
2. Définissez les propriétés SMB (conformément aux recommandations décrites dans la section des propriétés de cette page) et cliquez sur le bouton Appliquer pour activer la configuration.
3. Cliquez sur le lien Autohome de l'écran Configuration > Services > SMB pour définir des règles autohome afin de mapper les clients SMB vers les répertoires personnels (conformément aux descriptions de la section relative aux règles Autohome ci-dessus) puis cliquez sur le bouton Appliquer pour activer la configuration.
4. Cliquez sur le lien Groupes locaux de l'écran Configuration > Services > SMB, puis sur l'icône pour ajouter des administrateurs ou des opérateurs de sauvegarde à des groupes locaux (conformément aux descriptions de la section Groupes locaux ci-dessus) puis cliquez sur le bouton Appliquer pour activer la configuration.

Voir aussi

- http://en.wikipedia.org/wiki/Server_Message_Block (`http://en.wikipedia.org/wiki/Server_Message_Block`)
- Guides d'installation du système de stockage

- Configuration initiale
- Rejoindre un domaine Active Directory
- Création de projets
- Protocole SMB
- Création de partages
- Propriétés de partages
- DFS Management MMC Snap-in

FTP

Introduction

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.

Propriétés

Paramètres généraux

Propriété	Description
Port (pour les connexions entrantes)	Port d'écoute du service FTP. La valeur par défaut est 21.
Nb maximal de connexions ("0" = illimité)	Nombre maximal de connexions FTP simultanées. Définissez cette propriété afin couvrir le nombre d'utilisateurs simultanés prévus. Par défaut, cette valeur est déf 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 p déni de service.
Activer le moteur temporisé pour empêcher les attaques temporelles	Cette propriété insère de courts délais durant l'authentification afin de tromper le tentatives visant à devenir un nom d'utilisateur grâce aux mesures du temps. L'activation de cette propriété permet de renforcer la sécurité.
Default login root	Emplacement de connexion au FTP. La valeur par défaut est "/" et pointe vers le h de la hiérarchie des partages. Tous les utilisateurs seront connectés à cet emplacer 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 dé les autorisations en écriture *groupe* et *tout le monde* sont masquées pour empêche que les téléchargements récents ne soient réécrits par n'importe qui.

Paramètres de sécurité

Propriété	Description
Activer SSL/TLS	Autoriser les connexions FTP chiffrées SSL/TLS. Cette propriété garantit le chiffrement de la transaction FTP. Elle est activée 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. Elle est désactivée par défaut, car l'authentification FTP en texte brute présente un risque de sécurité lors des attaques survenant durant la détection du réseau
Nb maximal admissible de tentatives de connexion	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 fixée à 3.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Journaux

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

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

FTP Tâches

Autorisation de l'accès FTP à un partage

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. Accédez à la section "Protocoles" et vérifiez que l'accès FTP est activé. Vous pouvez également y définir le mode d'accès (lecture/lecture+écriture).

Voir aussi

- http://www.proftpd.org (`http://www.proftpd.org`)
- http://fr.wikipedia.org/wiki/File_Transfer_Protocol (`http://fr.wikipedia.org/wiki/File_Transfer_Protocol`)
- http://fr.wikipedia.org/wiki/Transport_Layer_Security (`http://fr.wikipedia.org/wiki/Transport_Layer_Security`)

HTTP

Introduction

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 leur logiciel client. Les URL permettant d'accéder à ces partages HTTP et HTTPS sont respectivement au format :

http://*hostname*/shares/*mountpoint*/*share_name*

https://*hostname*/shares/*mountpoint*/*share_name*

Le serveur HTTPS utilise un certificat de sécurité auto-signé.

Propriétés

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". Pour plus d'informations, reportez-vous à la section relative à l'authentification ci-dessous.
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 entrantes sécurisées)	Port HTTPS. La valeur par défaut est 443.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

Authentification et contrôle d'accès

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 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" à des 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).

Journaux

Journal	Description
network-http:apache22	Journal du service HTTP

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

HTTP Tâches

Autorisation de l'accès HTTP à un partage

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. Accédez à la section "Protocoles" et vérifiez que l'accès HTTP est activé. Vous pouvez également y définir le mode d'accès (lecture/lecture+écriture).

Voir aussi

- http://httpd.apache.org (`http://httpd.apache.org`)
- http://fr.wikipedia.org/wiki/WebDAV (`http://fr.wikipedia.org/wiki/WebDAV`)
- http://fr.wikipedia.org/wiki/Transport_Layer_Security (`http://fr.wikipedia.org/wiki/Transport_Layer_Security`)

NDMP

Introduction

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). A l'aide de NDMP, les données utilisateur de l'appareil (p. ex, 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 les 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. Au lieu de cela, utilisez la fonctionnalité [[Maintenance:System:ConfigurationBackup|Sauvegarde et restauration de configuration]].

Configurations locales et configurations 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 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

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" :

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 la série 7000 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 à l'aide de "dump" et de "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 (p. ex., */export/code*) ou un chemin contenu dans un système de fichiers live (p. ex., */export/code/src*), l'appareil prend immédiatement un nouvel instantané à partir duquel il sauvegarde le chemin donné. A l'issue de la sauvegarde, l'instantané est détruit. Si le chemin de sauvegarde spécifie un instantané (p. ex., */export/code/.zfs/snapshot/mysnap*), aucun instantané n'est créé et le système sauvegarde à partir de l'instantané spécifié.

`Share metadata` - Pour simplifier la sauvegarde et la restauration des configurations de partage complexes, les types "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, de même que les métadonnées de partage des projets parents. D'autre part, 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.

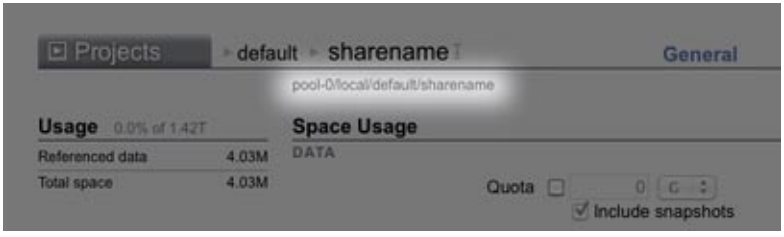
Durant la restauration, si la destination du chemin de restauration n'est pas contenue dans un partage existant, les projets et les partages du flux de sauvegarde sont recréés, si nécessaire avec les propriétés d'origine stockées dans la sauvegarde. Par exemple, si vous sauvegardez **`/export/foo`**, qui contient le projet **`proj1`** et les partages **`share1`** et **`share2`**, et que vous détruisez le projet avant de le restaurer à partir de la sauvegarde, ces deux partages et le projet sont recréés avec les propriétés sauvegardées au cours 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 à l'aide de "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 :



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 défini pour la sauvegarde à l'aide du suffixe '@snapshot', auquel cas aucun instantané n'est créé et l'instantané spécifié est sauvegardé. Par exemple :

Nom canonique	Partages sauvegardés
pool-0/local/default	Nouvel instantané du projet local nommé "default" et tous ses partages
pool-0/local/default@yesterday	Instantané "yesterday" du projet local nommé "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" peut être un système de fichiers ou un volume)
pool-0/local/default/code@yesterday	Instantané nommé "yesterday" dans le partage "code" du projet local "default" ("code" peut 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 d'informations, reportez-vous à la section "Sauvegardes incrémentielles" ci-après.

`Share metadata` - Les métadonnées du partage (p. ex. la 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 e
```

Sauvegardes incrémentielles

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

Variable	Détails
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.

Jour	Détails
First of month	Sauvegarde de niveau 0. La sauvegarde contient tous les fichiers du partage.
Every 7th, 14th, 21st of month	Sauvegarde de niveau 1. La sauvegarde contient tous les fichiers modifiés depuis la dernière sauvegarde complète (mensuelle).
Every day	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 "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 ci-dessous).

Propriétés

La configuration du service NDMP inclut les propriétés suivantes :

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.

Propriété	Description
Pool(s) de restauration par défaut	Lorsqu'il procède à une restauration complète à l'aide des types "tar" ou "dum système recrée les ensembles de données si aucun partage n'est déjà monté au cible. Etant donné que le protocole NDMP spécifie uniquement le point de m le système choisit un pool dans lequel recréer des projets et des partages. Sur u système contenant plusieurs pools, cette propriété vous permet de spécifier u plusieurs pools. Les pools multiples doivent être spécifiés uniquement dans u avec des pools actifs sur chaque tête. Vous devez vous assurer que cette liste es toujours synchronisée après chaque changement de configuration de stockag l'absence totale de pools ou si aucun pool n'est en ligne, le système sélectionne par défaut de façon aléatoire.
Ignorer modifications métadonnées seules	Indique au système de sauvegarder uniquement les fichiers dont le contenu a modifié et d'ignorer les fichiers dont seules des métadonnées (comme les autorisations ou la propriété) ont été modifiées. Cette option s'applique uniqu aux sauvegardes incrémentielles "tar" et "dump" et est désactivée par défaut.
Autoriser la sauvegarde basée sur jeton	Active ou désactive la méthode à base de jeton pour la sauvegarde ZFS. Par dé cette propriété est désactivée.
Restauration ZFS avant restauration (v4 uniquement)	S'applique uniquement aux sauvegardes de type "zfs". Détermine si, au mome restauration d'une sauvegarde incrémentielle, le système rétablit le projet et le cible de l'instantané utilisé comme base de la restauration incrémentielle. Si le et les partages sont rétablis, toutes les modifications apportées depuis la prise l'instantané sont perdues. Cette propriété est généralement contrôlée par la D la variable d'environnement "ZFS_FORCE" (voir "Sauvegardes incrémentiell ci-dessus) mais elle peut être utilisée pour remplacer le paramètre DMA et dé restaurer systématiquement ou jamais ces ensembles de données. Le fait de ne rétablir les ensembles de données peut entraîner l'échec de la restauration, à m qu'ils n'aient déjà été rétablis manuellement. Cette propriété est conçue pour utilisation avec les DMA qui n'autorisent pas les administrateurs à configurer 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 recherc séquentielle durant les opérations de restauration. L'activation de cette option de réduire le temps requis pour la récupération d'un petit nombre de fichiers nombreuses bandes. Il faut spécifier cette option au moment de la sauvegarde 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 a est également restauré (et pas uniquement le fichier en question). Cette optio désactivée par défaut.
Mode de bande DMA (pour les lecteurs connectés en local)	Spécifie si la DMA attend à une sémantique System V ou BSD. La valeur par d System V, elle est recommandée pour la plupart des DMA. Cette option s'app uniquement aux lecteurs de bande connectés en local exportés via NDMP. Co votre documentation DMA pour connaître le mode attendu par votre DMA. modification de cette option modifie uniquement les périphériques exportés la DMA recherche des périphériques. Vous devrez donc reconfigurer les périphériques à bande dans votre DMA après avoir modifié ce paramètre.

Propriété	Description
Mode de bande DMA (pour les lecteurs connectés en local)	Utilisé pour authentifier le DMA. Le système utilise MD5 pour l'authentification utilisateur

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

Journaux

Journal	Description
system-ndmpd:default	Journal du service NDMP

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Voir aussi

- http://fr.wikipedia.org/wiki/Network_Data_Management_Protocol (`http://fr.wikipedia.org/wiki/Network_Data_Management_Protocol`)

Remote Replication

Réplication distante

Le service de réplication distante facilite la réplication des projets et des partages vers et à partir d'autres appareils Oracle ZFS Storage Appliance. Cette fonctionnalité est décrite en détail dans la documentation relative à la réplication.

Lorsque ce service est activé, l'appareil reçoit des mises à jour de réplication à partir des autres appareils et envoie des mises à jour de réplication pour les projets et les partages locaux en fonction des actions configurées. Lorsque le service est désactivé, les mises à jour de réplication entrantes échouent et aucun projet ni partage local n'est répliqué.

Ce service ne possède pas de propriétés, mais permet aux administrateurs d'afficher les appareils qui ont répliqué des données sur cet appareil (sous Sources) et de configurer les appareils vers lesquels cet appareil peut effectuer une réplication (sous Cibles). Les détails relatifs à la gestion d'une réplication distante sont disponibles dans la documentation relative à la réplication.

Shadow Migration

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 documentation partagée relative à la migration shadow. 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.

Propriétés

Propriété	Description
Nombre de threads	Nombre de threads à dédier à la migration en arrière-plan des données. 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).

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

Gestion de la migration shadow

Des informations détaillées sur la gestion de la migration shadow sont disponibles dans la documentation relative aux partages Shadow Migration.

SFTP

Introduction

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.

Propriétés

Propriété	Description
Port (pour les connexions entrantes)	Port d'écoute du service SFTP. La valeur par défaut est 218.
Autoriser la connexion de root	Autoriser les connexions SFTP pour l'utilisateur root. Cette propriété est activée par défaut, étant donné que l'authentification SFTP est chiffrée et sécurisée.
Niveau de journalisation	Niveau de détails 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.

- A 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 "utilisateur" à 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.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Port 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 connecterait à l'aide de la commande suivante :

```
manta# sftp -o "Port 218" root@guppy
```

Journaux

Journal	Description
network-sftp:default	Consigne les événements du service SFTP

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

SFTP Tâches

Autorisation de l'accès SFTP à un partage

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. Sélectionnez ou ajoutez un partage dans l'écran Partages.
4. Accédez à la section "Protocoles" et vérifiez que l'accès SFTP est activée. Vous pouvez également y définir le mode d'accès (lecture/lecture+écriture).

Voir aussi

- http://www.openssh.com (`http://www.openssh.com`)
- http://fr.wikipedia.org/wiki/SSH_File_Transfer_Protocol (`http://fr.wikipedia.org/wiki/SSH_File_Transfer_Protocol`)

SRP

Introduction

Lorsque vous configurez une 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.

Cibles et initiateurs

Pour plus d'informations sur les initiateurs et les cibles SRP, reportez-vous à la section Réseau de stockage (SAN).

CLI

Pour consulter des exemples d'administration des cibles SRP, reportez-vous à la section Réseau de stockage (SAN).

Voir aussi

- http://en.wikipedia.org/wiki/SCSI_RDMA_Protocol (`http://en.wikipedia.org/wiki/SCSI_RDMA_Protocol`)

TFTP

Introduction

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.

Propriétés

Propriété	Description
Répertoire racine par défaut	Emplacement de connexion TFTP. La valeur par défaut est "/export" 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 TFTP.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Tâches

TFTP Tâches

Autorisation de l'accès TFTP à un partage

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. Sélectionnez ou ajoutez un partage dans l'écran Partages.
4. Accédez à la section "Protocoles" et vérifiez que l'accès TFTP est activé. Vous pouvez également y définir le mode d'accès (lecture/lecture+écriture).

Voir aussi

- http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol (`http://en.wikipedia.org/wiki/Trivial_File_Transfer_Protocol`)

Virus Scan

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 possèdent des données de fichiers mises en cache ou auxquels le serveur NFSv4 a accordé des privilèges de lecture ne peuvent pas être immédiatement placés en quarantaine.

Propriétés

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 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 fixée à 1 Go.

Propriété	Description
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.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Extensions de fichier

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 designer 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 :

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 **"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 serait PAS analysé, car seule la partie "jpg123" du nom, l'extension, serait comparée aux règles.

N'utilisez **PAS** de paramètres d'exclusions avant 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. L'exemple suivant n'analyserait aucun fichier :

Action	Modèle
Ne pas analyser	*
Analyser	exe
Analyser	com
Analyser	bat
Analyser	doc
Analyser	zip
Ne pas analyser	data-archive*.zip

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.

Propriété	Description
Activer	Utiliser ce moteur d'analyse
Hôte	Nom d'hôte ou adresse IP du serveur du moteur d'analyse
Maximum Connections	Nombre maximal de connexions simultanées. Certains moteurs d'analyse fonctionnent mieux lorsque les connexions sont limitées à 8.
Port	Port du moteur d'analyse

Journaux

Journal	Description
vscan	Journal du service Analyse antivirus

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

Vous trouverez ci-après des exemples de tâche. Reportez-vous aux sections BUI et CLI pour savoir comment ces tâches s'appliquent à chaque méthode d'interface.

Virus Scan Tâches

Configuration de l'analyse antivirus pour un partage

1. Accédez à Configuration->Services->Analyse antivirus.
2. Définissez les propriétés souhaitées.
3. Appliquez/validez la configuration.
4. Accédez à Partages.
5. Modifiez un système de fichiers ou un projet.
6. Sélectionnez l'onglet "Général".
7. Activez l'option "Analyse antivirus".

Voir aussi

- http://fr.wikipedia.org/wiki/Logiciel_antivirus (`http://fr.wikipedia.org/wiki/Logiciel_antivirus`)

NIS

Introduction

NIS (Network Information Service) est un service de noms pour la gestion centralisée. L'appareil peut se comporter tel un client NIS pour les utilisateurs et les groupes, de sorte que :

- Les utilisateurs NIS peuvent se connecter via un protocole FTP et HTTP/WebDAV.
- 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.

Notez que 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.

Propriétés

Propriété	Description
Domain	Domaine NIS à utiliser

Propriété	Description
Serveur(s) : Rechercher à l'aide de la diffusion	L'appareil émet une diffusion NIS afin de localiser les serveurs NIS de ce do
Serveur(s) : Utiliser les serveurs listés	Nom d'hôte ou adresse IP des serveurs NIS

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

L'appareil connecte le premier serveur NIS répertorié ou trouvé à l'aide de la diffusion, et passe à l'étape suivante si le serveur ne répond plus.

Journaux

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

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

Vous trouverez ci-après des exemples de tâche. Reportez-vous aux sections BUI et CLI pour savoir comment ces tâches s'appliquent à chaque méthode d'interface.

NIS Tâches

Ajout d'un administrateur de l'appareil à partir de NIS

Si le service NIS inclut un utilisateur souhaitant se connecter à l'aide de ses informations d'identification NIS et administrer l'appareil, procédez comme suit :

1. Accédez à Configuration->Services->NIS
2. Définissez les propriétés relatives au domaine NIS et au serveur.
3. Appliquez/validez la configuration.
4. Accédez à Configuration->Utilisateurs
5. Ajoutez l'utilisateur avec le type "directory".

6. Définissez le nom d'utilisateur sur son nom d'utilisateur NIS.
7. Continuez en suivant les instructions de la section Utilisateurs pour ajouter des autorisations à cet utilisateur.

Voir aussi

- http://fr.wikipedia.org/wiki/Network_Information_Service (`http://fr.wikipedia.org/wiki/Network_Information_Service`)

LDAP

Introduction

LDAP (Lightweight Directory Access Protocol) est un service d'annuaire de gestion centralisée des utilisateurs, des groupes, des noms d'hôte et d'autres ressources (appelées objets). Sur l'appareil, ce service fait office de client LDAP de sorte que :

- Les utilisateurs LDAP peuvent se connecter via un protocole FTP et HTTP/WebDAV.
- Des noms d'utilisateur LDAP (plutôt que les ID numériques) peuvent être utilisés pour configurer les listes ACL du répertoire racine 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.

Notez que 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.

Propriétés

Consultez votre administrateur de serveur LDAP pour connaître les paramètres adaptés à votre environnement.

Propriété	Description
Protect LDAP traffic with SSL/TLS	Utiliser TLS (Transport Layer Security, descendant du protocole SSL) pour établir des connexions sécurisées au serveur LDAP
DN de base de recherche	Nom distinctif de l'objet de base (point de départ des recherches de répertoire)

Propriété	Description
Portée 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.
Authentication method	Méthode permettant d'authentifier l'appareil sur le serveur LDAP. L'appareil prend en charge l'authentification simple (RFC 4513), SASL/DIGEST-MD5 et SASL/GSSAPI. Si la méthode d'authentification simple est utilisée, il faut activer SSL/TLS pour que le nom distinctif et le mot de passe de l'utilisateur ne soient pas envoyés en texte simple. Lorsque vous utilisez la méthode d'authentification SASL/GSSAPI, seul le niveau d'authentification de liaison automatique est disponible.
Bind credential level	Informations d'identification permettant d'authentifier l'appareil auprès du serveur LDAP. "Anonyme" permet à l'appareil d'accéder uniquement aux données disponibles pour tout le monde. "Proxy" indique au service d'établir une liaison via un compte spécifié. "Automatique" authentifie l'appareil à l'aide de l'authentification locale. L'authentification automatique peut uniquement être utilisée avec la méthode SASL/GSSAPI.
Proxy DN	Nom distinctif du compte utilisé pour l'authentification de proxy
Proxy Password	Mot de passe du compte utilisé pour l'authentification de proxy
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 et les groupes. Voir la section "Mappages personnalisés" ci-après.
Servers	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.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

Mappages 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*.

Descripteur de recherche	Valeur par défaut	Exemple
users	ou=people,*base search DN*	ou=people,dc=example,dc=com
groups	ou=group,*base search DN*	ou=group,dc=example,dc=com

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, entrez le nom distinctif **entier** que vous souhaitez utiliser. L'appareil utilise cette valeur sans la modifier et ignore les valeurs des propriétés **DN de base de recherche** et **Portée de la recherche**. Pour remplacer des objets et des attributs d'utilisateur et de groupe, choisissez l'onglet approprié ("Utilisateurs" ou "Groupes") 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.

Journaux

Journal	Description
appliance-kit-nsswitch:default	Journal du service de noms de l'appareil à travers lequel les requêtes LDAP sont effectuées

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

Vous trouverez ci-après des exemples de tâche. Reportez-vous aux sections BUI et CLI pour savoir comment ces tâches s'appliquent à chaque méthode d'interface.

LDAP Tâches

Ajout d'un administrateur de l'appareil à partir de LDAP

Si le service LDAP inclut un utilisateur souhaitant se connecter à l'aide de ses informations d'identification LDAP et administrer l'appareil, procédez comme suit :

1. Accédez à Configuration->Services->LDAP
2. Définissez les propriétés du service LDAP.
3. Appliquez/validez la configuration.
4. Accédez à Configuration->Utilisateurs
5. Ajoutez l'utilisateur avec le type "directory".
6. Définissez le nom d'utilisateur sur son nom d'utilisateur LDAP.
7. Continuez en suivant les instructions de la section Utilisateurs pour ajouter des autorisations à cet utilisateur.

Voir aussi

- http://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol (`http://fr.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol`)

Active Directory

Introduction

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 Utilisateurs.

Propriétés

Domaine

Le tableau suivant décrit les propriétés permettant de rejoindre un domaine Active Directory.

Propriété	Description
Active Directory Domain	Le nom complètement qualifié ou le nom NetBIOS d'un domaine Active Directory
Utilisateur administratif	Utilisateur AD possédant les informations d'identification permettant de créer un compte d'ordinateur dans Active Directory
Mot de passe d'administration	Mot de passe de l'utilisateur administratif
Chemin de recherche DNS supplémentaire	Lorsque cette propriété facultative est spécifiée, les requêtes DNS sont résolues dans ce domaine, en plus du domaine DNS principal et du domaine Active Directory

Groupe de travail

Le tableau suivant décrit la propriété configurable pour rejoindre un groupe de travail.

Propriété	Description
Windows Workgroup	Groupe de travail

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Domaines et groupes de travail

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. 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.

Si un domaine utilisant le protocole Kerberos est configuré pour prendre en charge un NFS kerberisé, le système ne peut pas être configuré pour rejoindre un domaine Active Directory.

Signature LDAP

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.

Prise en charge de Windows Server 2012

Windows Server 2012 est entièrement pris en charge dans les version de logiciel 2011.1.5 et ultérieures.

Prise en charge de Windows Server 2008

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

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.

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 LMCompatibilityLevel est défini sur 5 dans Windows 2008 SP1, 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.

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.

BUI

Cliquez sur le bouton "REJOINDRE LE DOMAINE" pour rejoindre un domaine ou sur le bouton "REJOINDRE LE GROUPE DE TRAVAIL" pour rejoindre un groupe de travail.

CLI

Pour illustrer l'interface de la CLI, l'exemple suivant affiche la configuration existante, et rejoint un groupe de travail puis un domaine.

```
twofish:> configuration services ad
twofish: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
```

Notez que l'appareil exploite actuellement le domaine "eng.fishworks.com". L'exemple ci-dessous illustre comment quitter ce domaine et rejoindre un groupe de travail.

```
twofish:configuration services ad> workgroup
twofish:configuration services ad workgroup> set workgroup=WORKGROUP
twofish:configuration services ad workgroup> commit
twofish:configuration services ad workgroup> done
twofish:configuration services ad> show
Properties:
                    <status> = disabled
                        mode = workgroup
                   workgroup = WORKGROUP
```

L'exemple suivant illustre la configuration du site et du contrôleur de domaine préféré en vue de rejoindre un autre domaine.

```
twofish:configuration services ad> done
twofish:> configuration services smb
twofish:configuration services smb> set ads_site=sf
twofish:configuration services smb> set pdc=192.168.3.21
twofish:configuration services smb> commit
twofish:configuration services smb> show
Properties:
                    <status> = online
                lmauth_level = 4
                         pdc = 192.168.3.21
                    ads_site = sf
twofish:configuration services smb> done
```

L'exemple suivant illustre comment rejoindre le nouveau domaine après la configuration des propriétés.

```
twofish:> configuration services ad
twofish:configuration services ad> domain
twofish:configuration services ad domain> set domain=fishworks.com
twofish:configuration services ad domain> set user=Administrator
twofish:configuration services ad domain> set password=*******
twofish:configuration services ad domain> set searchdomain=it.fishworks.com
twofish:configuration services ad domain> commit
twofish:configuration services ad domain> done
twofish:configuration services ad> show
Properties:
                    <status> = online
                        mode = domain
                      domain = fishworks.com
```

Tâches

Reportez-vous aux sections BUI et CLI pour savoir comment ces tâches s'appliquent à chaque méthode d'interface.

Active Directory Tâches

Rejoindre un domaine

1. Configurez un site Active Directory dans le contexte SMB. (facultatif)
2. Configurez un contrôleur de domaine préféré dans le contexte SMB. (facultatif)
3. Activez 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 du contrôleur de domaine en tant que serveur de noms supplémentaire dans le contexte DNS.
5. Configurez le domaine Active Directory, l'utilisateur administratif et son mot de passe.
6. Appliquez/validez la configuration.

Rejoindre un groupe de travail

1. Configurez le nom du groupe de travail.
2. Appliquez/validez la configuration.

Voir aussi

- http://fr.wikipedia.org/wiki/Active_Directory (`http://fr.wikipedia.org/wiki/Active_Directory`)
- http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx (`http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx`)

Identity Mapping

Concepts

Les services de mappage des identités gère les identités des utilisateurs Windows et Unix simultanément à l'aide d'UID (et de GID) Unix traditionnels et de SID Windows. Le service SMB utilise le service de mappage des identités pour associer les 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 vers 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 à des clients SMB et NFS. En associant les identités Windows et Unix, un client 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 chaque groupe possède un SID. Un SID identifie de manière unique un utilisateur ou un groupe au sein d'un hôte et d'un domaine local, ainsi que dans tous les domaines Windows possibles.

Unix crée des informations 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 et 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.

Le service de mappage des identités crée et gère une base de données des mappages entre SID, UID et GID. Vous pouvez adopter une des approches de mappage décrites dans le tableau suivant.

Identity Mapping Concepts

Modes de mappage

Méthode	Description
IDMU	Extrait les informations de mappage d'une base de données Active Directory à l'aide des propriétés IDMU.
Mappage basé sur un annuaire	Extrait les informations de mappage d'une base de données Active Directory ou LDAP.
Mappage basé sur une règle	Configure les mappages à l'aide de mappages basés sur le nom.
Mappage éphémère	Laisse le système créer des mappages temporaires, à la demande.

Lorsque le mappage IDMU est activé, cette méthode prime sur toutes les autres méthodes de mappage. Si le mappage basé sur un annuaire est activé, cette approche prévaut sur les autres. Si le mappage basé sur un annuaire n'est pas disponible, le service tente de mapper une identité à l'aide de l'approche basée sur le nom. Si aucune règle basée sur le nom n'est disponible pour une identité donnée, le service crée un mappage éphémère.

IDMU

Microsoft offre une fonctionnalité appelée "Identity Management for Unix" ou IDMU. Ce logiciel est disponible pour Windows Server 2003 et intégré à Windows Server 2003 R2 et aux versions ultérieures. Cette fonction fait partie du logiciel "Services pour Unix" non fourni en standard.

L'utilisation principale d'IDMU est la prise en charge de Windows en tant que serveur NIS/NFS. IDMU ajoute un volet réservé aux "Attributs UNIX" à l'interface utilisateur Utilisateurs et ordinateurs Active Directory qui permet à l'administrateur de spécifier un nombre de paramètre liés à UNIX : UID, GID, shell de connexion, répertoire personnel et de même type pour les groupes. Ces paramètres sont accessibles dans AD via un schéma similaire (mais pas identique) à celui du document RFC2307 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.

Mappage basé sur un annuaire

Ce type de mappage comprend l'annotation d'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. Ces attributs supplémentaires associés à l'objet doivent être configurés dans les propriétés suivantes.

Identity Mapping Mappage basé sur un annuaire

Propriétés

Propriété	Description
Mappage basé sur un annuaire	Activer le mappage basé sur un annuaire
Attribut AD - Nom d'utilisateur Unix	Nom figurant dans la base de données AD du nom d'utilisateur Unix équival
Attribut AD - Nom de groupe Unix	Nom figurant dans la base de données AD du nom de groupe Unix équivalen
Attribut LDAP natif - Nom d'utilisateur Windows	Nom figurant dans la base de données LDAP de l'identité Windows équivale

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus.

Pour plus d'informations sur l'accroissement des schémas Active Directory ou LDAP, reportez-vous à la section consacrée à la gestion du mappage des identités basé sur un annuaire pour les utilisateurs et les groupes (liste des tâches) du guide d'administration CIFS Solaris.

Mappage basé sur un nom

L'approche du mappage basé sur un nom consiste en la création de différentes règles de mise en correspondance des identités par nom. Ces règles établissent des équivalences entre les identités Windows et Unix.

Identity Mapping Mappage basé sur un nom

Règles de mappage basé sur un nom

Les propriétés suivantes reposent sur une règle basée sur un nom.

Propriété	Description
Type de mappage	Précise si ce mappage octroie ou non des informations d'identification.
Sens du mappage	Sens du mappage. Les informations d'identification peuvent être mappées dans les deux sens, de Windows à Unix uniquement ou d'Unix à Windows uniquement.
Domaine Windows	Domaine Active Directory de l'identité Windows
Windows entity	Nom de l'identité Windows
Entité Unix	Nom de l'identité Unix
Type Unix	Type de l'identité Unix (utilisateur ou groupe)

Sensibilité à la casse

Les noms Windows sont 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 Windows "jsmith" correspond au nom d'utilisateur Unix "jsmith". 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, après avoir converti le nom d'utilisateur Windows en minuscule, le service ne trouve aucune correspondance, l'utilisateur n'obtient aucun mappage. Vous pouvez créer une règle pour mettre en correspondance les chaînes dont seule la casse diffère. Par exemple, créez un mappage spécifique à l'utilisateur pour établir une correspondance entre l'utilisateur Windows "JSmith@sun.com" 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.

Persistance du mappage

Lorsque le service de mappage des identités établit une correspondance de noms, il stocke le mappage 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. Si le serveur SMB demande une correspondance pour l'utilisateur après l'expiration du mappage, le service réévalue les mappages.

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.

Règles au niveau du domaine

Une règle de mappage au niveau du domaine établit une correspondance entre tout ou partie des noms d'un domaine Windows et des noms Unix. Les noms d'utilisateur des deux côtés doivent être exactement identiques (sauf en matière de casse, ce qui dépend des règles mentionnées plus haut). Vous pouvez par exemple créer une règle bidirectionnelle pour établir une correspondance entre tous les utilisateurs Windows de "myDomain.com" et les utilisateurs Unix portant le même nom (et vice versa). Vous pouvez aussi créer une règle pour établir une correspondance entre tous les utilisateurs Windows de "myDomain.com" du groupe "Engineering" et les utilisateurs Unix portant le même nom. Il est impossible de créer des mappages au niveau d'un domaine si ceux-ci sont en conflit avec d'autres mappages.

Mappages de refus

Les règles de mappage de refus empêchent les utilisateurs d'obtenir une correspondance, y compris un ID éphémère, à partir du service de mappage des identités. Vous pouvez créer des mappages au niveau d'un domaine ou des mappages de refus propres aux utilisateurs Windows

et Unix. Vous pouvez par exemple créer un mappage pour refuser l'accès aux partages SMB à tous les utilisateurs Unix du groupe "guest". Il est impossible de créer des mappages de refus si ceux-ci sont en conflit avec d'autres mappages.

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.

Icône	Description
	Mapper l'identité Windows vers l'identité Unix et l'identité Unix vers l'identité Windows
	Mapper l'identité Windows vers l'identité Unix
	Mapper l'identité Unix vers l'identité Windows
	Refuser des informations d'identification à l'identité Windows
	Refuser des informations d'identification à l'identité Unix

Si une icône est grise et pas noire (, , , ,), cette règle correspond à une identité Unix qui ne peut pas être résolue.

Mappage éphémère

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 créé 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 appartient à "nobody".

Pratiques recommandées

- La configuration de règles précises de mappage des identités s'applique uniquement lorsque vous souhaitez qu'un même utilisateur accède à un ensemble de fichiers communs à la fois en tant que client 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 connectés restent connectés et leur mappage de nom précédent est disponible pour autoriser l'accès aux partages supplémentaires pendant un délai allant jusqu'à 10 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.

Test des mappages

L'onglet Mappages de la BUI montre comment les différentes identités sont mappées en fonction de l'ensemble de règles actuel. En spécifiant une entité Windows ou Unix, l'entité est mappée vers son identité correspondante sur la plate-forme opposée. Les informations qui en résultent dans les sections des propriétés de l'utilisateur et des propriétés de groupe affichent les détails relatifs au mappage de l'identité, y compris la source du mappage.

Exemples

L'exemple ci-dessous illustre l'ajout de deux règles basées sur un nom dans la CLI. Le premier exemple créé un mappage bidirectionnel basé sur un nom entre un utilisateur Windows et un utilisateur Unix.

```
twofish:> configuration services idmap
twofish:configuration services idmap> create
twofish:configuration services idmap (uncommitted)> set
   windomain=eng.fishworks.com
twofish:configuration services idmap (uncommitted)> set winname=Bill
twofish:configuration services idmap (uncommitted)> set direction=bi
twofish:configuration services idmap (uncommitted)> set unixname=wdp
twofish:configuration services idmap (uncommitted)> set unixtype=user
twofish:configuration services idmap (uncommitted)> commit
twofish:configuration services idmap> list
MAPPING      WINDOWS ENTITY                    DIRECTION    UNIX ENTITY
idmap-000    Bill@eng.fishworks.com        (U) ==           wdp (U)
```

L'exemple suivant créé un mappage de refus pour empêcher tous les utilisateurs Windows d'un domaine d'obtenir des informations d'identification.

```
twofish:configuration services idmap> create
twofish:configuration services idmap (uncommitted)> list
Properties:
                    windomain = (unset)
                      winname = (unset)
                    direction = (unset)
                     unixname = (unset)
                     unixtype = (unset)

twofish:configuration services idmap (uncommitted)> set
   windomain=guest.fishworks.com
twofish:configuration services idmap (uncommitted)> set winname=*
twofish:configuration services idmap (uncommitted)> set direction=win2unix
twofish:configuration services idmap (uncommitted)> set unixname=
twofish:configuration services idmap (uncommitted)> set unixtype=user
twofish:configuration services idmap (uncommitted)> commit
twofish: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)
```

Tâches

Vous trouverez ci-après des exemples de tâche. Reportez-vous aux sections BUI et CLI pour savoir comment ces tâches s'appliquent à chaque méthode d'interface.

Identity Mapping Tâches

Configuration du mappage des identités

1. Rejoindre un domaine Active Directory
2. Configurez le mappage basé sur un annuaire (facultatif).
3. Configurez des mappages de refus.
4. Configurez des mappages basés sur un nom.

Ajout d'un mappage basé sur un nom

1. Indiquez si le mappage octroie ou non des informations d'identification.
2. Configurez le domaine et le nom de l'identité Windows.
3. Configurez le sens du mappage.
4. Configurez le nom et le type de l'identité Unix.
5. Appliquez/validez la configuration.

DNS

Introduction

Le client DNS (Domain Name Service), qui permet de résoudre les adresses IP en noms d'hôte (et vice versa), est toujours activé sur l'appareil. 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 d'audit pour indiquer l'emplacement à partir duquel un utilisateur a effectué une action vérifiable et dans l'écran Analytics pour offrir des statistiques pour chaque client.

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. Vous recevez un message d'erreur si les serveurs DNS ne répondent pas à ces exigences.

Propriétés

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.
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 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 présentée dans les sections BUI et CLI du chapitre Services.

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 :

```
caji:> nslookup deimos
192.168.1.109   deimos.sf.fishworks.com
caji:> getent hosts deimos
192.168.1.109   deimos.sf.fishworks.com
```

Journaux

Journal	Description
network-dns-client:default	Consigne les événements du service DNS

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Active Directory et DNS

Si vous envisagez d'utiliser Active Directory, au moins un des serveurs doit pouvoir résoudre les enregistrements de nom d'hôte et de serveur dans la portion 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.

Résolution non-DNS

DNS est un mécanisme de mappage standard, au niveau de l'entreprise, hautement évolutif et fiable des noms d'hôte et des adresses IP. 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. Par conséquent, si vous devez opter pour une autre résolution que DNS, vous obtiendrez sans doute de meilleurs résultats en désactivant le service DNS (voir section suivante) et en utilisant exclusivement NIS ou LDAP pour la résolution d'hôtes. 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 le serveur 127.0.0.1. L'utilisation de ce mode est fortement déconseillée. Plusieurs fonctionnalités ne fonctionneront pas correctement, notamment :

- 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" ci-dessus.

Voir aussi

- http://fr.wikipedia.org/wiki/Domain_Name_System (`http://fr.wikipedia.org/wiki/Domain_Name_System`)

Dynamic Routing

Protocoles de routage dynamiques RIP et RIPng

RIP (Routing Information Protocol) 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 à partir des hôtes de liaison activés et compatibles avec RIP

(généralement les 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. En conséquence, la désactivation de ce service entraîne la suppression de toutes les routes dynamiques dans la table de routage. Les ports d'écoute RIP et RIPng sont respectivement les ports UDP 520 et 521.

Journaux

Journal	Description
network-routing-route:default	Consigne les événements du service RIP
network-routing-ripng:quagga	Consigne les événements du service RIPng

Voir aussi

- http://en.wikipedia.org/wiki/Routing (`http://en.wikipedia.org/wiki/Routing`)
- http://en.wikipedia.org/wiki/Routing_Information_Protocol (`http://en.wikipedia.org/wiki/Routing_Information_Protocol`)

IPMP

Introduction

IPMP (Internet Protocol Network Multipathing) permet de regrouper plusieurs interfaces réseau en une seule, à la fois 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 Réseau.

Propriétés

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 présentée dans les sections BUI et CLI du chapitre Services.

Journaux

Journal	Description
network-initial:default	Consigne le processus de configuration réseau

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

Pour configurer IPMP, activez ce service et suivez les instructions de la section Réseau.

Voir aussi

- http://en.wikipedia.org/wiki/IPMP (`http://en.wikipedia.org/wiki/IPMP`)

NTP

Introduction

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 décalage du fuseau horaire de votre navigateur.

Propriétés

Propriété	Description	Exemples
multicast address	Entrez une adresse de multidiffusion pour localiser automatiquement un serveur NTP.	224.0.1.1

Propriété	Description	Exemples
Serveur(s) NTP	Entrez un ou plusieurs serveurs NTP (et leurs clés d'authentification correspondantes, le cas échéant) pour contacter directement l'appareil.	0.pool.ntp.org
NTP Authentication Keys	Entrez 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 Authentification ci-dessous.	Clé aut : 10, Type : ASCII, Clé privée : SUN7000

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

Validation

Si une configuration invalide 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 des serveurs non autorisés, NTP possède un schéma de chiffrement de 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. Ce type doit être l'un des éléments suivants :

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
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.

BUI

Pour ajouter des clés d'authentification NTP dans la BUI, cliquez sur l'icône + et spécifiez le numéro, le type et la valeur de clé privée de la nouvelle clé créée. Après son ajout, la clé s'affiche sous forme d'option en regard du serveur NTP spécifié.

CLI

Sous `configuration services ntp`, modifiez les autorisations à l'aide de la commande `authkey` :

```
clownfish:configuration services ntp> authkey
clownfish:configuration services ntp authkey>
```

Dans ce contexte, il est possible d'ajouter de nouvelles clés à l'aide de la commande `create` :

```
clownfish:configuration services ntp authkey> create
clownfish:configuration services ntp authkey-000 (uncommitted)> get
                        keyno = (unset)
                         type = (unset)
                          key = (unset)
clownfish:configuration services ntp authkey-000 (uncommitted)> set keyno=1
                        keyno = 1 (uncommitted)
clownfish:configuration services ntp authkey-000 (uncommitted)> set type=A
                         type = A (uncommitted)
clownfish:configuration services ntp authkey-000 (uncommitted)> set key=coconuts
                          key = ******** (uncommitted)
clownfish:configuration services ntp authkey-000 (uncommitted)> commit
clownfish:configuration services ntp authkey>
```

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" :

```
clownfish:configuration services ntp> set servers=gefilte,carp
                      servers = gefilte,carp (uncommitted)
clownfish:configuration services ntp> set serverkeys=1,1
                   serverkeys = 1,1 (uncommitted)
clownfish:configuration services ntp> commit
clownfish:configuration services ntp>
```

Pour authentifier le serveur "gefilte" avec la clé 1, "carp" avec la clé 2 et "dory" avec la clé 3 :

```
clownfish:configuration services ntp> set servers=gefilte,carp,dory
                      servers = gefilte,carp,dory (uncommitted)
clownfish:configuration services ntp> set serverkeys=1,2,3
```

```
                  serverkeys = 1,2,3 (uncommitted)
clownfish:configuration services ntp> commit
clownfish:configuration services ntp>
```

Pour authentifier les serveurs "gefilte" et "carp" à l'aide de la clé 1 et ne pas authentifier le serveur NTP "dory" :

```
clownfish:configuration services ntp> set servers=gefilte,carp,dory
                     servers = gefilte,carp,dory (uncommitted)
clownfish:configuration services ntp> set serverkeys=1,1,0
                  serverkeys = 1,1,0 (uncommitted)
clownfish:configuration services ntp> commit
clownfish:configuration services ntp>
```

Horloge de la BUI

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 "SYNCHRO" pour faire correspondre l'heure de l'appareil avec celle du navigateur de votre client.

Conseils

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.

Journal	Description
network-ntp:default	Journal du service NTP

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

NTP Tâches

Synchronisation de l'horloge de la BUI

Cette opération définit l'heure de l'appareil pour qu'elle corresponde à celle de votre navigateur.

1. Désactivez le service NTP.
2. Cliquez sur le bouton "SYNCHRO".

Voir aussi

- http://www.ntp.org (`http://www.ntp.org`)
- http://fr.wikipedia.org/wiki/Network_Time_Protocol (`http://fr.wikipedia.org/wiki/Network_Time_Protocol`)

Phone Home

Introduction

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 au portail d'inventaire Oracle qui vous permet de gérer le matériel Oracle. L'enregistrement est également un prérequis à l'utilisation du service Phone Home.
- 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 la section Problèmes.
- * 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.

Compte de connexion unique Oracle

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 http://support.oracle.com (`http://support.oracle.com`) et cliquez sur Inscrire pour créer un compte.

Propriétés

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Le service Phone Home se nomme `scrk` dans la CLI.

Proxy Web

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 offres groupées de support, reportez-vous à la section Maintenance du système.

Propriété	Description
Utiliser un proxy	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

Tâches

Enregistrement

BUI

Lorsque vous enregistrez l'appareil pour la première fois, fournissez un compte de connexion unique. Accédez à http://support.oracle.com (`http://support.oracle.com`) et cliquez sur Inscrire pour créer votre compte et spécifier l'une des équipes d'inventaire du compte. Dans de la BUI :

1. Entrez le mot de passe et le nom d'utilisateur de votre compte de connexion unique Oracle. Une déclaration de confidentialité s'affiche ensuite. Vous pouvez la consulter ultérieurement dans la BUI et la CLI.
2. L'appareil valide les informations d'identification et vous permet de choisir l'équipe d'inventaire auprès de laquelle vous inscrire. Pour chaque compte, l'équipe par défaut est identique au nom d'utilisateur du compte, précédé du symbole '$'.
3. Validez vos modifications.

CLI

Dans la CLI, le processus implique la configuration de plusieurs propriétés du service :

1. Définissez `soa_id` et `soa_password` respectivement sur le nom d'utilisateur et le mot de passe de votre compte de connexion unique Oracle.
2. Validez vos modifications.

3. Définissez `domain_name` sur le nom de l'équipe d'inventaire auprès de laquelle vous souhaitez enregistrer l'appareil.
4. Validez vos modifications.

Une fois l'appareil enregistré, il n'est pas possible d'annuler l'enregistrement mais vous pouvez le modifier.

- Cliquez sur 'Changer de compte...' pour modifier le compte de connexion unique Oracle utilisé par l'appareil. Vous pouvez ensuite sélectionner l'une des équipes d'inventaire du compte. Validez vos modifications.
- Pour s'inscrire auprès d'une autre équipe d'inventaire avec le même compte, sélectionnez une autre équipe dans la zone déroulante. Validez vos modifications.

Statut

Propriété	Description
Last heartbeat sent at	Heure d'envoi du dernier signal d'activité au support Oracle

Etat du service

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 entrer un compte de connexion unique Oracle pour utiliser le service Phone Home.

Journaux

Un journal des événements Phone Home est disponible sous Maintenance->Journaux->Phone Home.

Voir aussi

- http://support.oracle.com (`http://support.oracle.com`)

Service Tags

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.

Propriétés

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

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

SMTP

Introduction

Le service SMTP envoie tout le courrier généré par l'appareil, généralement en réponse à des alertes configurées dans l'écran Alertes. 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.

Propriétés

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.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

Lorsque vous modifiez les propriétés, vous pouvez utiliser les 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.

Journaux

Journal	Description
network-smtp:sendmail	Consigne les événements de service SMTP
mail	Journal des activités SMTP (y compris les messages envoyés)

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Voir aussi

- http://fr.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol (`http://fr.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol`)

SNMP

Introduction

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. Reportez-vous à la section MIB.
- Des alertes peuvent être configurées pour envoyer des déroutements SNMP.

Les versions 1 et 2c de SNMP sont disponibles lorsque le service est activé.

Propriétés

Propriété	Description
Nom de communauté SNMP	Chaîne de communauté que les clients SNMP doivent fournir lorsqu'ils se connectent.
Réseau autorisé	Réseau autorisé à interroger le serveur SNMP dans la notation CIDR. Pour bloquer tous les clients, utilisez 127.0.0.1/8 (hôte local uniquement) ; pour autoriser tous les clients, utilisez 0.0.0.0/0.
Contact pour l'appareil	Chaîne servie par MIB-II OID .1.3.6.1.2.1.1.4.0. En définissant ce paramètre sur une personne ou un nom de département, vous aiderez les clients à déterminer qui est responsable de cet appareil.
Destinations de déroutements	Noms d'hôte ou adresses IP pour l'envoi des déroutements SNMP. Des déroutements SNMP personnalisés peuvent être configurés dans la section Alertes. Définissez cette propriété sur 127.0.0.1.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus. Après avoir modifié les propriétés, redémarrez le service SNMP.

Le service SNMP fournit également la chaîne de l'emplacement MIB-II. Cette propriété provient de la configuration Identité du système.

MIB

Si les services SNMP sont en ligne, les réseaux autorisés ont accès aux MIB suivantes (Management Information Bases) :

MIB	Objectif
.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) permet d'accéder à des informations relatives à la gestion des pannes SUN :

- Problèmes actifs sur le système
- Evénements de gestion des pannes
- Informations de configuration relatives à la gestion des pannes

Il existe quatre tables principales à lire :

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	Evénements 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

Pour des descriptions complètes, consultez le lien du fichier MIB ci-dessous.

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
- état du cluster
- état du partage - nom et taille du partage, octets disponibles et utilisés

Il existe trois tables principales à lire :

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

Pour des descriptions complètes, consultez le lien du fichier MIB ci-dessous.

Tâches

Vous trouverez ci-après des exemples de tâche pour SNMP. Reportez-vous aux sections BUI et CLI pour savoir comment ces tâches s'appliquent à chaque méthode d'interface.

SNMP Tâches

Configuration de SNMP afin qu'il indique l'état de l'appareil

1. Définissez le nom de communauté, le réseau autorisé et la chaîne de contact.
2. Si vous le souhaitez, définissez la destination du déroutement vers un hôte SNMP distant. Autrement, définissez-la sur 127.0.0.1.
3. Appliquez/validez la configuration.
4. Redémarrez le service.

Configuration de SNMP afin d'envoyer des déroutements

1. Définissez le nom de communauté, la chaîne de contact et les destinations de déroutement.
2. Si vous le souhaitez, définissez le réseau autorisé de façon à autoriser les clients SNMP. Autrement, définissez-le sur 127.0.0.1/8.

3. Appliquez/validez la configuration.
4. Redémarrez le service.

Voir aussi

- http://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol (`http://fr.wikipedia.org/wiki/Simple_Network_Management_Protocol`)

Syslog

Introduction

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 un ou plusieurs systèmes distants.
- 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
- **`gravité`** : 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. Consultez les informations suivantes pour plus de détails sur le format du message.
- **`message`** : décrit l'événement. Consultez les informations suivantes pour plus de détails sur le format du message.

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 service Syslog Relay 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

Propriété	Description
Version du protocole	Version du protocole Syslog à utiliser (classique ou moderne)
Destinations	Liste des adresses IPv4 et IPv6 de destination vers lesquelles les messages sont transmis.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés de la CLI sont des versions abrégées des noms répertoriés ci-dessus. Après avoir modifié les propriétés, redémarrez le service Syslog.

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 ci-dessous.

La valeur **`hostname`** correspond au nom canonique de l'appareil, comme défini dans la configuration de Identité du système.

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), **`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 ci-dessous.

La valeur **`hostname`** correspond au nom canonique de l'appareil, comme défini dans la configuration de Identité du système.

Format du message

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 sujettes à des changements sans qu'ils en soient informés ou sans qu'ils puissent les supprimer dans les versions futures du logiciel Sun Storage.

Utilitaire	Nom de l'indicateur	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 Identity Mapping pour la conversion d'identité POSIX et Windows.
daemon	smbd	Protocole de données SMB pour l'accès aux données partagées.

Format du message d'alerte

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.

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. Un lien vers un article traitant du sujet est disponible à l'adresse sun.com/msg/.
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.

Nom du champ	Description
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	Le **`numéro de série du châssis`** de l'appareil.
HOSTNAME	Nom canonique de l'appareil comme défini dans la configuration de Identité du système.
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 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 :

Gravité	Niveau syslog	Description
Mineure	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.
Majeure	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.

Exemples de configuration du récepteur

La plupart des systèmes d'exploitation incluent un récepteur syslog mais il est possible que certaines étapes de configuration soient requises pour l'activer. Vous trouverez ci-après des exemples de configuration pour les systèmes d'exploitation courants. 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.

Configuration d'un récepteur Solaris

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: 92dfeb39-6e15-e2d5-a7d9-dc3e221becea\n\
DESC: A test alert has been posted.\n\
AUTO-RESPONSE: None.\nIMPACT: None.\nREC-ACTION: None.
```

Configuration d'un récepteur Linux

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"
```

Redémarrez ensuite 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.
```

Voir aussi

- Configuration:Alertes
- Configuration:Services:SNMP

System Identity

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.

Propriétés

Propriété	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 SNMP est activé, elle sera exportée en tant que chaîne *syslocation* dans MIB-II.

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services.

Journaux

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 Journaux du chapitre Services.

SSH

Introduction

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. Le service SSH peut également servir de moyen d'exécution des scripts automatiques à partir d'un hôte distant, comme pour extraire les journaux quotidiens ou les statistiques Analyse.

Propriétés

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
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 s'identifier à l'aide de SSH.	yes

La procédure de modification des propriétés des services est présentée dans les sections BUI et CLI du chapitre Services. Les noms des propriétés CLI sont identiques à ceux répertoriés ci-dessus.

Journaux

Journal	Description
network-ssh:default	Journal des événements et des erreurs du service SSH.

Pour afficher les journaux de service, reportez-vous à la section Journaux du chapitre Services.

Tâches

Vous trouverez ci-après des exemples de tâche. Reportez-vous aux sections BUI et CLI pour savoir comment ces tâches s'appliquent à chaque méthode d'interface.

SSH Tâches

Désactivation de l'accès SSH root

1. Définissez l'identification root sur false.
2. Appliquez/validez la configuration.

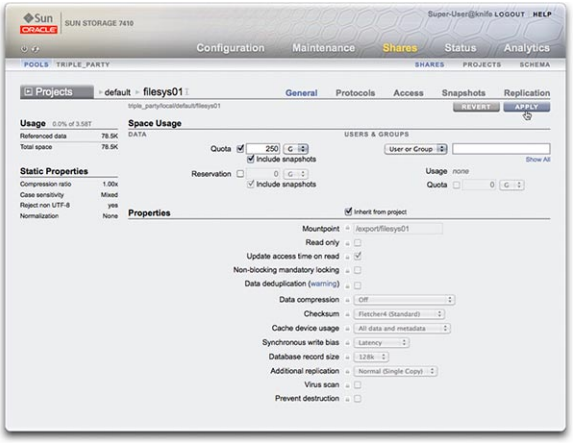
Voir aussi

- http://fr.wikipedia.org/wiki/Secure_Shell (`http://fr.wikipedia.org/wiki/Secure_Shell`)

◆ ◆ ◆ CHAPITRE 5

Partages

Shares



Modification des propriétés générales d'un système de fichiers. Les partages ayant des caractéristiques similaires peuvent être regroupés dans un projet.

Partages

L'appareil de stockage exporte les systèmes de fichiers en tant que partages gérés dans cette section de l'appareil. Les partages peuvent être regroupés en projets à des fins d'administration commune, incluant les paramètre courants et de gestion de l'espace.

- Concepts - informations générales relatives à l'organisation du stockage et la gestion des propriétés de partage

- Migration shadow - migrer automatiquement les données en local ou à partir de serveurs distants
- Gestion de l'espace - gérer l'utilisation de l'espace par utilisateur ou par partage à l'aide des quotas et des réservations
- Espace de noms du système de fichiers - informations sur la manière dont l'espace de nom du système de fichiers est géré et exporté
- Partages - gérer les systèmes de fichiers et les LUN
- Général - gérer les propriétés générales des partages
- Protocoles - gérer les paramètres de protocoles (NFS, SMB, iSCSI, etc.)
- Accès - gérer le contrôle d'accès aux systèmes de fichiers en fonction des utilisateurs.
- Instantanés - gérer les instantanés automatiques et manuels sur les partages
- Réplication - gérer les sources de réplication ciblant cet appareil
- Projets - gérer les projets
- Général - gérer les propriétés générales sur les projets
- Protocoles - gérer les paramètres de protocole sur les projets
- Accès - gérer le contrôle d'accès aux projets en fonction des utilisateurs
- Instantanés - gérer les instantanés automatiques et manuels sur les projets
- Réplication - configurer la réplication de données vers d'autres appareils
- Schéma - définir des propriétés personnalisées à utiliser avec les partages et les projets

Concepts

Pools de stockage

L'appareil est basé sur le système de fichiers ZFS. ZFS regroupe les périphériques de stockage sous-jacents en pools, et les systèmes de fichiers et les LUN sont allouées en conséquence à partir de ce stockage. 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 des quotas et réservations.

Bien que plusieurs pools de stockage sont pris en charge, ce type de configuration est déconseillé car il présente de nombreux inconvénients décrits dans la section de configuration du stockage. 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 menus, 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 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 en plus d'être appliqués 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 exportent une hiérarchie basée sur des fichiers et 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 tuple *projet/partage* est un identificateur unique pour un partage contenu dans un pool. Plusieurs projets peuvent contenir des partages portant le même nom mais un projet unique ne peut pas contenir des partages ayant le même nom. Un projet unique peut contenir des systèmes de fichiers et des LUN, lesquels partagent le même espace de noms.

Propriétés

Tous les projets et partages ont un nombre défini de propriétés associées. Ces propriétés appartiennent aux groupes suivants :

Type de propriété	Description
Hérité	Il s'agit du type de propriété le plus courant et représente la plupart des propriétés de projets et de partages personnalisables. 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	Ces propriétés représentent des statistiques relatives au projet et au partage et ne peuvent être modifiées. Les propriétés les plus courantes de ce type sont les statistiques d'utilisation de l'espace.
Gestion de l'espace	Ces propriétés (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.
Moment de la création	Ces propriétés peuvent être 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	Ces propriétés sont définies sur un projet mais n'affectent pas le projet lui-même. 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	Ces propriétés 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 locale	Ces propriétés s'appliquent uniquement aux LUN et ne sont pas héritées. Elles ne peuvent pas être définies sur les projets.
Personnalisés	Ces propriétés sont définies par l'utilisateur. Pour plus d'informations, reportez-vous à la section Schéma.

Instantanés

Un instantané est une copie ponctuelle d'un système de fichiers ou d'une LUN. Les instantanés peuvent être créés manuellement ou en définissant un calendrier automatique. Initialement, les instantanés ne consomment pas d'espace supplémentaire mais, étant donné que le partage actif

est modifié, les blocs non référencés au préalable sont conservés comme partie du dernier instantané. Au fil du temps, le dernier instantané prend de l'espace supplémentaire avec un maximum correspondant à la taille du système de fichiers au moment de la prise de l'instantané.

Les instantanés de système de fichiers sont accessibles par le biais des protocoles standard présents dans l'instantané `.zfs/snapshot` à la racine du système de fichiers. Le répertoire est masqué par défaut et accessible uniquement en modifiant explicitement le répertoire `.zfs`. Ce comportement peut être modifié dans l'aperçu de l'instantané, mais cela peut entraîner la sauvegarde des instantanés par le logiciel de sauvegarde en plus de données live. Les instantanés de LUN ne sont pas directement accessibles. Cependant, ils peuvent être utilisés comme cible de restauration ou comme source d'un clone. Les instantanés de projet reviennent à prendre un instantané de tous les partages au sein du projet. Ces instantanés sont identifiés par nom. 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.

Les partages prennent en charge la possibilité de restaurer les instantanés précédents. 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.

Clones

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)."*

Un clone désigne une copie accessible en écriture d'un instantané de partage, considéré comme un partage indépendant à des fins d'administration. De la même manière que les instantanés, les clones consomment initialement peu d'espace mais lorsque de nouvelles données sont écrites dans le clone, l'espace requis pour ces modifications est associé au clone. Les clones de projets ne sont pas pris en charge. Dans la mesure où l'espace est partagé entre les instantanés et les clones et qu'un instantané peut avoir plusieurs clones, la suppression d'un instantané entraîne la destruction de tous les clones actifs.

Shadow Migration

Migration des données 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 la série d'appareils Sun Storage 7000 est équipée de deux solutions intégrées pour la migration des données, adaptées aux cas d'utilisation les plus courants. La première, appelée réplication distante , est destinée à la réplication des données entre un ou plusieurs appareils et détaillée dans une autre section. 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 appareil Sun Storage 7000 dans un environnement existant pour la prise en charge des droits de partage de fichiers d'un autre serveur, mais de nombreuses autres utilisations possibles sont détaillées ci-dessous.

Migration traditionnelle des données

Généralement, la migration traditionnelle des fichiers fonctionne d'une des deux manières suivantes : synchronisation répétée ou interposition externe.

Migration par synchronisation

Cette méthode consiste à prendre un hôte actif X et à migrer les données sur le nouvel hôte Y pendant que X reste actif. Les clients continuent à lire et écrire sur l'hôte d'origine alors que cette migration est en cours. Une fois que les données sont migrées, des changements progressifs sont envoyés de manière répétée, jusqu'à ce que le delta soit assez réduit pour être envoyé dans une seule fenêtre d'indisponibilité. A ce stade, le partage initial est en lecture seule, le delta final est envoyé au nouvel hôte et tous les clients sont mis à jour pour pointer vers le nouvel emplacement. La façon la plus courante de procéder est d'utiliser l'outil rsync, bien que d'autres outils intégrés existent. Ce mécanisme présente plusieurs inconvénients :

- Il est difficile d'évaluer précisément la durée de l'indisponibilité mais elle est courte. Si un utilisateur effectue de nombreux changements juste avant l'indisponibilité planifiée, cela peut en allonger la durée.
- Lors de la migration, le nouveau serveur est inactif. Etant donné qu'un nouveau serveur apporte généralement de nouvelles fonctions ou des améliorations en matière de performances, de longues périodes de migration représentent un gaspillage des ressources.

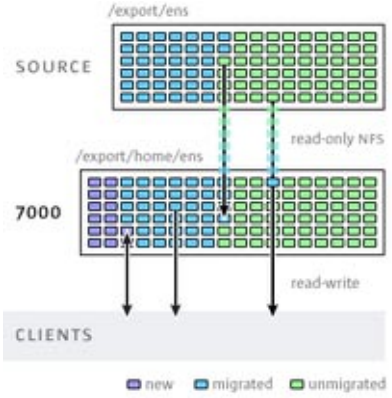
- La coordination de plusieurs systèmes de fichiers est une opération fastidieuse. Lors de la migration de dizaines ou centaines de systèmes de fichiers, chaque migration a une durée différente et il convient de planifier le temps d'indisponibilité en fonction de tous les systèmes de fichiers.

Migration par interposition externe

Cette méthode consiste à prendre un hôte actif X et insérer un nouvel appareil M qui migre les données vers un nouvel hôte Y. Tous les clients sont mis à jour en même temps de façon à pointer vers M et les données sont migrées automatiquement en arrière-plan. Cela permet de donner une plus grande flexibilité en termes d'options de migration (par exemple, pouvoir migrer un nouveau serveur dans le futur sans entraîner d'indisponibilité) et d'utiliser le nouveau serveur contenant les données déjà migrées. Cependant, cette méthode présente des inconvénients importants :

- L'appareil de migration est considéré comme une nouvelle machine physique, ce qui implique des coûts associés (investissement de départ, coûts de maintenance, alimentation et refroidissement) et autres frais de gestion.
- Il représente également un nouveau point de panne au sein du système.
- L'appareil de migration s'interpose entre des données déjà migrées, provoquant la mise en place d'une période de latence plus longue, souvent de manière permanente. En général, ces appareils ne sont pas retirés, bien qu'il soit possible de prévoir une autre fenêtre d'indisponibilité et d'éliminer l'appareil de migration.

Migration shadow



La migration shadow utilise l'interposition mais est intégrée dans l'appareil et ne requiert pas de machine physique séparée. Lorsque des partages 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 Sun Storage 7000. Les clients peuvent ensuite accéder à l'appareil en mode lecture-écriture.

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 été 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.

Comportement de la migration shadow

Restrictions applicables aux sources 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 partages 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.

Sémantique de système de fichiers shadow au cours de la migration

Si le client accède à un fichier ou un répertoire qui n'a pas encore été migré, un effet observable se produit au niveau du comportement :

- Pour les répertoires, les requêtes des clients sont bloquées jusqu'à ce que la totalité du répertoire soit migré. 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 racine 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.

Migration des informations d'identité et des ACL (Access Control List, liste de contrôle d'accès)

Pour migrer correctement les informations d'identité des fichiers, y compris les ACL, vous devez 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.

Gestion de la migration shadow

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`** - `fichier:///<chemin d'accès>`
- **`NFS`** - `nfs://<hôte>/<chemin d'accès>`

La BUI autorise également la forme alternative `<hôte>:/<chemin d'accès>` pour les montages NFS, qui correspond à la syntaxe utilisée dans les systèmes UNIX. La BUI définit également la partie de protocole du paramètre (`fichier://` 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

shadow migration. 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

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 (tels 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

Le contrôle de la progression d'une migration shadow est difficile étant donné le contexte dans lequel est exécutée l'opération. Un seul système de fichiers peut masquer tout ou partie d'un système de fichiers ou plusieurs systèmes de fichiers ayant des points de montage imbriqués. Ainsi, il n'existe aucun moyen d'être sûr que les statistiques concernant la source soient correctes. De plus, même dans le cas de la migration d'un seul système de fichiers, les méthodes utilisées pour calculer la taille disponible ne sont pas les mêmes pour tous les systèmes. Par exemple, il est possible que le système de fichiers distant utilise la compression ou qu'il ne prenne pas en compte la surcharge des métadonnées. C'est pour toutes ces raisons qu'il est impossible d'afficher une barre de progression précise de la migration.

L'exactitude des informations suivantes fournies par l'appareil est garantie :

- Taille totale du système de fichiers local
- Taille logique des données déjà copiées
- Temps déjà consacré à la migration des données

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). Si vous connaissez la taille du système de fichiers distant, vous pouvez utiliser cette information pour évaluer la progression de la migration. La taille des données copiées comprend uniquement le contenu des fichiers standard à migrer à partir de la source. Les répertoires, métadonnées et attributs étendus ne sont pas compris dans ce calcul. La taille des données déjà migrées comprend uniquement les données migrées à distance, mais il est possible que certaines parties du système de fichiers déjà migrées soient parcourues à la reprise de la migration en arrière-plan. Cela peut entraîner une accélération de la migration lors du traitement des premiers répertoires et un ralentissement lorsqu'elle atteint des parties du système de fichiers qui n'ont pas encore été migrées.

Bien qu'il n'existe aucun moyen fiable de calculer la progression, l'appareil donne tout de même une estimation des données restantes en se basant sur l'hypothèse selon laquelle la structure des répertoires serait uniforme. Cette estimation (qui peut être assez précise ou bien complètement inutile en fonction des données) est fournie à titre d'information uniquement. Par exemple, une structure de système de fichiers peut être peu développée mais comprendre une grande quantité de données dans le répertoire qui sera parcouru en dernier. Dans ce scénario, la migration est signalée comme presque terminée puis retombe d'un coup à un pourcentage très bas lorsque ce répertoire est détecté. En revanche, si le premier répertoire traité est très volumineux, l'estimation est faite en considérant que tous les autres répertoires renferment un volume de données similaire puis, lorsqu'ils sont parcourus, l'estimation passe d'un très faible pourcentage de progression à un pourcentage proche de 100 % en découvrant qu'ils sont presque vides. La meilleure façon de mesurer la progression d'une migration est de paramétrer une migration test, de la laisser s'exécuter jusqu'à la fin puis d'utiliser cette valeur pour estimer la progression de la migration d'un système de fichiers de taille et de structure similaires.

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 des 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. Cela reflète l'état incohérent des données sur disque pendant la migration.

Sauvegarde des 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 des 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.

Analyse 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 Analyse. Les analyses de migration shadow sont disponibles sous la catégorie "Déplacement de données". Deux types de statistiques classiques différents 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.

Migration des 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.

Tâches

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 partages peuvent être configurés pour la migration finale.

Shadow Migration Tâches

Test d'une migration shadow potentielle

1. Configurez la source de sorte que l'appareil Sun Storage 7000 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

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 Sun Storage 7000 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 une option, 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 '<hôte>/<chemin>' 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 SS7000.

A ce stade, la migration shadow doit s'exécuter en arrière-plan et les requêtes client traitées de manière appropriée. Vous pouvez observer la progression de la migration comme expliqué plus haut. Vous pouvez créer plusieurs partages au cours d'une même interruption programmée en scriptant la CLI (Interface de ligne de commande).

Space Management

Gestion de l'espace

Le comportement des systèmes de fichiers et des LUN par rapport à la gestion du stockage physique n'est pas le même sur la série 7000 (par rapport à beaucoup d'autres systèmes). Comme indiqué à la page Concepts, l'appareil utilise un modèle de pool de stockage sur lequel tous les systèmes de fichiers et les LUN partagent le même espace. Les systèmes de fichiers n'ont jamais de taille explicite assignée et utilise 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, elles 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 retreinte, nécessite une gestion plus prudente. Cette section décrit certains des outils mis à la disposition de l'administrateur pour contrôler et gérer l'utilisation de l'espace.

Termes

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.

Space Management Termes

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

Il s'agit de l'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'instantanés

Il s'agit de la 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

Un quota représente l'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.

Reservation

Une réservation représente une 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.

Présentation des 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.

Certains autres systèmes tentent de masquer les coûts des instantanés en prétendant qu'ils sont gratuits ou en "réservant" un espace dédié à la conservation des données d'instantané. Ces systèmes tentent de minimiser les inconvénients inhérents aux instantanés. 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 par définition conserver des références au double de données d'origine. Les instantanés ne sont pas gratuits et la seule manière qu'ont les autres systèmes de présenter cette abstraction est de détruire les instantanés en mode silencieux quand il n'y a plus d'espace disponible. C'est parfois la pire chose à faire étant donné qu'un processus de réécriture des données peut entraîner la destruction de tous les instantanés précédents, ce qui empêche toute restauration au cours du processus.

Dans la série Sun Storage 7000, le coût des instantanés est toujours explicite et des outils sont fournis pour gérer cet espace afin de correspondre au mieux au modèle d'administration d'un environnement donné. 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.-à-d. 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 vue 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).

Paramètres 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 à la section relative aux instantanés, 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. Comme indiqué à la section relative aux instantanés, le comportement de prise d'instantanés n'est pas 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`.

Paramètres d'utilisateur et de groupe

Affichage de l'utilisation actuelle

L'utilisation actuelle d'un utilisateur ou d'un groupe peut être demandée pour les systèmes de fichiers et les projets, que des quotas d'utilisateurs et de groupes soient appliqués ou non. Les pools de stockage créés sur des versions antérieures du logiciel doivent parfois appliquer des mises à jour différées avant d'utiliser cette fonction. Après l'application de mises à jour différées, il faut attendre que tous les systèmes de fichiers soient mis à niveau vers une version qui prend en charge les quotas et l'utilisation par utilisateur et par groupe.

BUI

Pour afficher l'utilisation actuelle dans la BUI, accédez à la page "Partages -> Général" sous la section "Utilisation de l'espace -> Utilisateurs et groupes". Vous trouverez ici une zone de saisie de texte ainsi qu'une liste déroulante. Cela vous permet de consulter l'utilisation actuelle de n'importe quel utilisateur ou groupe au sein d'un partage ou dans un projet. Les types pris en charge sont les suivants :

- **Utilisateur ou Groupe** - Rechercher des utilisateurs ou des groupes, avec une préférence pour les utilisateurs en cas de conflit. Etant donné qu'il n'y a, en général, pas de superposition entre les noms d'utilisateurs et les noms de groupes, cela devrait être suffisant pour la majorité des demandes.
- **Utilisateur** - Rechercher des utilisateurs.
- **Groupe** - Rechercher des groupes.

Des recherches sont effectuées en même temps que vous saisissez du texte dans la zone de saisie. Lorsque la recherche est terminée, l'utilisation actuelle s'affiche. De plus, si vous cliquez sur le lien "Tout afficher", une boîte de dialogue s'ouvre, qui contient une liste de l'utilisation actuelle de tous les utilisateurs et groupes. Cette boîte de dialogue permet uniquement de rechercher les utilisateurs et les groupes et ne prend pas en charge la recherche des deux simultanément. Cette liste affiche les noms canoniques UNIX et Windows (si les mappages sont activés), ainsi que l'utilisation et le quota (pour les systèmes de fichiers).

CLI

Dans la CLI, les commandes `users` et `groups` peuvent être exécutées à partir du contexte d'un projet ou d'un partage spécifique. A partir d'ici, la commande `show` permet d'afficher l'utilisation actuelle sous forme de tableau. De plus, l'utilisation d'un utilisateur ou d'un groupe spécifique peut être extraite en sélectionnant l'utilisateur ou le groupe en question et en émettant la commande`get`.

```
clownfish:> shares select default
clownfish:shares default> users
clownfish:shares default users> list
USER       NAME                            USAGE
user-000   root                             325K
user-001   ahl                             9.94K
user-002   eschrock                        20.0G
clownfish:shares default users> select name=eschrock
clownfish:shares default user-002> get
                          name = eschrock
                      unixname = eschrock
                        unixid = 132651
                       winname = (unset)
                         winid = (unset)
                         usage = 20.0G
```

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. 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 différences principales 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.
- 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 pour 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.

BUI

Dans le navigateur, les quotas d'utilisateur sont gérés sous l'onglet Général, sous Utilisation de l'espace -> Utilisateurs et groupes. Comme c'est le cas pour la vue de l'utilisation, l'utilisation actuelle s'affiche lorsque vous saisissez un utilisateur ou un groupe. Une fois que vous avez terminé de saisir le nom de l'utilisateur ou du groupe et que l'utilisation actuelle s'affiche, vous pouvez définir le quota en cochant la case située en regard de "quota" puis en saisissant une valeur dans le champ de taille. Pour désactiver un quota, désélectionnez cette case. Une fois les modifications appliquées, cliquez sur le bouton 'Appliquer' pour les enregistrer.

Alors que toutes les propriétés de la page sont validées en une seule fois, les quotas d'utilisateur et de groupe sont validés séparément des autres propriétés. Si un utilisateur ou un groupe non valide est saisi en même temps qu'une propriété non valide, il est possible qu'un seul message

d'erreur de validation s'affiche. Une fois que vous avez corrigé cette erreur, si vous essayez d'appliquer les changements à nouveau, un message s'affiche pour signaler la deuxième erreur.

CLI

Dans la CLI, les quotas d'utilisateur sont gérés à l'aide des commandes 'users' et 'groups' à partir du contexte du partage. Il est possible de définir des quotas en sélectionnant un utilisateur ou un groupe particulier et à l'aide de la commande 'set quota'. 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. Pour définir un quota pour ce genre d'utilisateur ou de groupe, exécutez la commande 'quota' puis définissez le nom et le quota. Pour effacer un quota, définissez-le sur '0'.

```
clownfish:> shares select default select eschrock
clownfish:shares default/eschrock> users
clownfish:shares default/eschrock users> list
USER       NAME                            USAGE  QUOTA
user-000   root                             321K      -
user-001   ahl                             9.94K      -
user-002   eschrock                        20.0G      -
clownfish:shares default/eschrock users> select name=eschrock
clownfish:shares default/eschrock user-002> get
                         name = eschrock
                     unixname = eschrock
                       unixid = 132651
                      winname = (unset)
                        winid = (unset)
                        usage = 20.0G
                        quota = (unset)
clownfish:shares default/eschrock user-002> set quota=100G
                        quota = 100G (uncommitted)
clownfish:shares default/eschrock user-002> commit
clownfish:shares default/eschrock user-002> done
clownfish:shares default/eschrock users> quota
clownfish:shares default/eschrock users quota (uncomitted)> set name=bmc
                         name = bmc (uncommitted)
clownfish:shares default/eschrock users quota (uncomitted)> set quota=200G
                        quota = 200G (uncommitted)
clownfish:shares default/eschrock users quota (uncomitted)> commit
clownfish:shares default/eschrock users> list
USER       NAME                            USAGE  QUOTA
user-000   root                             321K      -
user-001   ahl                             9.94K      -
user-002   eschrock                        20.0G   100G
user-003   bmc                                 -   200G
```

Gestion des identités

Les quotas d'utilisateur et de groupe optimisent le service de mappage d'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 d'identité avant d'essayer d'utiliser activement les systèmes de fichiers. Cependant, toute modification du mappage peut avoir des conséquences surprenantes.

Filesystem Namespace

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 `/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 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.

Accès par protocole aux points de montage

Tous les systèmes de fichiers doivent avoir un point de montage, quels que soient les paramètres du protocole. Cependant, l'utilisation de ces points de montage dépend du protocole.

NFSv2 / NFSv3

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.

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.

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.

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 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.

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 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.

Shares

BUI

L'interface utilisateur Partages est accessible à partir de "Partages -> Partages". La vue par défaut répertorie les partages disponibles sur l'ensemble des projets du système.

Liste des partages

La vue par défaut est une liste de tous les partages du système. Cette liste vous permet de renommer des partages, de déplacer des partages entre les projets et d'en modifier. Les partages sont divisés en deux listes "Systèmes de fichiers" et "LUN" que vous pouvez sélectionner en passant d'un onglet à l'autre dans cette vue. Les champs suivants sont affichés pour chaque partage :

Champ	Description
Nom	Nom du partage. Si vous regardez tous les projets, ce champ inclut également le nom du projet. Il s'agit d'un champ de texte modifiable. Si vous cliquez sur le nom, vous pouvez saisir un nouveau nom. Appuyez sur la touche Entrée ou déplacez le curseur pour valider la modification. Vous êtes invité à confirmer cette action car elle impose la déconnexion des clients actifs.
Taille	Pour les systèmes de fichiers, il s'agit de la taille totale du système de fichiers. Pour les LUN, il s'agit de la taille du volume, qui peut ou non faire l'objet d'une allocation fine. Pour plus d'informations sur les statistiques d'utilisation, reportez-vous aux documents suivants.
Point de montage	Point de montage du système de fichiers. Il s'agit du chemin d'accès à NFS et du chemin d'accès relatif au FTP et HTTP. Les systèmes de fichiers exportés sur SMB utilisent uniquement leur nom de ressource, même si chacun d'eux nécessite un point de montage unique dans le système.
GUID	GUID SCSI de la LUN. Pour plus d'informations, reportez-vous à la section iSCSI.

Les outils suivants sont disponibles pour chaque partage :

Icône	Description
	Déplacer un partage dans un projet différent. Si le panneau Projet est réduit, cette action le développe automatiquement jusqu'à ce que le partage soit déposé dans un projet.
	Modifier un partage (également accessible en cliquant deux fois sur la ligne).
	Détruire le partage. Vous êtes invité à confirmer cette action car elle entraîne la destruction de toutes les données du partage et ne peut pas être annulée.

Modification d'un partage

Pour modifier un partage, cliquez sur l'icône représentant un crayon ou cliquez deux fois sur la ligne dans la liste des partages. Cette action permet de sélectionner un partage et affiche de nombreux onglets différents qui vous permettent de modifier les propriétés du partage. Vous pouvez consulter l'intégralité des fonctionnalités dans la section correspondant à chaque onglet :

- Général
- Protocoles
- Accès
- Instantanés
- Réplication

Le nom du partage est affiché dans l'angle supérieur gauche, à droite du panneau Projet. Le premier composant du nom est le projet, et si vous cliquez sur le nom du projet, vous accédez aux [[Shares:Projects|détails du projet]]. Vous pouvez également modifier le nom du partage en cliquant dessus et en saisissant le nouveau nom dans la zone de saisie. Vous êtes invité à confirmer cette action car elle impose la déconnexion des clients actifs du partage.

Statistiques d'utilisation

Dans la partie gauche de la vue (sous le panneau Projet lorsqu'il est développé), 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.

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

Il s'agit de la quantité de données référencées par les données. Cela inclut l'intégralité des données de système 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

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 relative aux propriétés générales.

Espace total

Il s'agit de la somme des données référencées, des données d'instantanés et de la réservation inutilisée.

Propriétés statiques

Dans la partie gauche de la vue des partages, vous trouverez les propriétés statiques disponibles lors de la modification d'un partage spécifique. Ces propriétés sont définies au moment de la création et ne peuvent pas être modifiées par la suite.

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 compression et les algorithmes disponibles, consultez la section relative aux propriétés générales.

Sensibilité à la casse

Cette propriété détermine si les recherches de répertoire sont sensibles ou non à la casse. Les options suivantes sont prises en charge :

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 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 créer 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.

Valeur BUI	Valeur CLI	Description
Sensible	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 crées 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 respecte pas le codage UTF-8 valide. Il faut "activer" cette propriété si la propriété de normalisation est définie sur une autre valeur que "none".

Normalisation

Cette propriété 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". Pour plus d'informations sur le fonctionnement de la normalisation et des différentes formes de normalisation, consultez l'article Wikipedia entry consacré à la normalisation Unicode.

Valeur BUI	Valeur CLI	Description
Aucune	none	Aucune normalisation n'est effectuée.
Form C	formC	*NFC (Normalization Form Canonical Composition)* - Les caractères sont décomposés et réordonnés par équivalence canonique.
Form D	formD	*NFD (Normalization Form Canonical Decomposition)* - Les caractères sont décomposés par équivalence canonique.

Valeur BUI	Valeur CLI	Description
Form KC	formKC	*NFKC (Normalization Form Compatibility Composition)* - Les caractères sont décomposés par équivalence de compatibilité et réordonnés par équivalence canonique.
Form KD	formKD	*Normalization Form Compatibility Decomposition (NFKD)* - Les caractères sont décomposés par équivalence de compatibilité.

Taille de bloc des volumes

Cette propriété représente la taille de bloc natif pour les LUN. Il peut s'agir de n'importe quelle puissance de 2 allant de 512 octets à 128 Ko et la valeur par défaut est 8 Ko.

Origin

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 des données, consultez la section relative à la migration shadow.

Panneau Projet

Dans la BUI, les projets disponibles sont toujours accessibles dans le panneau Projet situé dans la partie gauche de la vue. Pour développer ou réduire le panneau Projet, cliquez sur le triangle situé près de la barre de titre "Projets".

Icône	Description
	Développer le panneau Projet
	Réduire le panneau Projet

Si vous sélectionnez un projet dans le panneau, vous accédez à la vue du projet correspondant. De même, ce panneau est développé automatiquement lorsque vous cliquez sur l'outil de déplacement d'une ligne de la liste de partages. Pour déplacer un partage entre des projets, vous pouvez utiliser la fonction glisser-déposer. Le panneau Projet fournit également un raccourci pour la création de nouveaux projets et permet de revenir à la liste des partages présents dans l'ensemble des projets. Si vous cliquez sur "Toutes" , cela produit le même effet que lorsque vous sélectionnez l'élément "Partages" dans la barre de navigation.

Le panneau Projet est très utile pour les systèmes comptant un nombre relativement restreint de projets. Il n'a pas vocation à être l'interface principale de gestion d'un grand nombre de projets. Pour cette tâche, consultez la vue Projecs.

Création de partages

Pour créer un partage, affichez les partages d'un projet ou de tous les projets en sélectionnant l'entrée de sous-navigation "partages". Lorsque vous sélectionnez "Systèmes de fichiers" ou "LUN", une icône représentant le signe plus (+) s'affiche à côté du nom, qui permet d'ouvrir une boîte de dialogue pour créer le partage. Lorsque vous créez un partage, vous pouvez choisir le projet cible dans un menu déroulant puis nommer le partage. Les propriétés correspondant à chaque type de partage sont définies dans d'autres sections :

Pour les systèmes de fichiers :

- Utilisateur
- Groupe
- Autorisations d'accès
- Point de montage
- Rejeter non UTF-8 (disponible uniquement au moment de la création)
- Sensibilité à la casse (disponible uniquement au moment de la création)
- Normalisation (disponible uniquement au moment de la création)

Pour les LUN :

- Taille de volume
- Allocation fine
- Taille de bloc des volumes (disponible uniquement au moment de la création)

CLI

La CLI des partages est disponible sous `shares`

Navigation

Avant de sélectionner un partage, vous devez d'abord sélectionner un projet (y compris le projet par défaut) :

```
clownfish:> shares
clownfish:shares> select default
clownfish:shares default> select foo
clownfish:shares default/foo> get
Properties:
                    aclinherit = restricted (inherited)
                       aclmode = discard (inherited)
                         atime = true (inherited)
                casesensitivity = mixed
```

```
                checksum = fletcher4 (inherited)
             compression = off (inherited)
           compressratio = 100
                  copies = 1 (inherited)
                creation = Mon Oct 13 2009 05:21:33 GMT+0000 (UTC)
              mountpoint = /export/foo (inherited)
           normalization = none
                   quota = 0
              quota_snap = true
                readonly = false (inherited)
              recordsize = 128K (inherited)
             reservation = 0
        reservation_snap = true
          secondarycache = all (inherited)
                  nbmand = false (inherited)
                sharesmb = off (inherited)
                sharenfs = on (inherited)
                 snapdir = hidden (inherited)
               snaplabel = project1:share1
                utf8only = true
                   vscan = false (inherited)
                sharedav = off (inherited)
                shareftp = off (inherited)
             space_data = 43.9K
      space_unused_res = 0
       space_snapshots = 0
       space_available = 12.0T
           space_total = 43.9K
            root_group = other
      root_permissions = 700
             root_user = nobody
```

Opérations relatives aux partages

Pour créer un partage, sélectionnez le projet et émettez la commande `filesystem` ou `lun`. Si nécessaire, vous pouvez modifier les propriétés avant de valider les modifications :

```
clownfish:shares default> filesystem foo
clownfish:shares default/foo (uncommitted)> get
                    aclinherit = restricted (inherited)
                       aclmode = discard (inherited)
                         atime = true (inherited)
                      checksum = fletcher4 (inherited)
                   compression = off (inherited)
                        copies = 1 (inherited)
                    mountpoint = /export/foo (inherited)
                         quota = 0 (inherited)
                      readonly = false (inherited)
                    recordsize = 128K (inherited)
                   reservation = 0 (inherited)
                secondarycache = all (inherited)
                        nbmand = false (inherited)
                      sharesmb = off (inherited)
                      sharenfs = on (inherited)
                       snapdir = hidden (inherited)
                     snaplabel = project1:share1
                         vscan = false (inherited)
```

```
                    sharedav = off (inherited)
                    shareftp = off (inherited)
                  root_group = other (default)
             root_permissions = 700 (default)
                   root_user = nobody (default)
            casesensitivity = (default)
              normalization = (default)
                    utf8only = (default)
                  quota_snap = (default)
             reservation_snap = (default)
                  custom:int = (default)
               custom:string = (default)
                custom:email = (default)
clownfish:shares default/foo (uncommitted)> set sharenfs=off
                    sharenfs = off (uncommitted)
clownfish:shares default/foo (uncommitted)> commit
clownfish:shares default>
```

Vous pouvez détruire un partage à l'aide de la commande `destroy` du contexte share

```
clownfish:shares default/foo> destroy
This will destroy all data in "foo"! Are you sure? (Y/N)
clownfish:shares default>
```

Vous pouvez renommer un partage à partir du contexte project à l'aide la commande `rename` :

```
clownfish:shares default> rename foo bar
clownfish:shares default>
```

Un partage peut être déplacé entre différents projets à partir du contexte project à l'aide de la commande `move` :

```
clownfish:shares default> move foo home
clownfish:shares default>
```

Une fois que vous avez sélectionné le projet ou le partage spécifique, il est possible de gérer l'utilisation et les quotas d'utilisateur et de groupe par le biais des commandes `users` ou `groups`. plus d'informations sur la gestion des quotas d'utilisateur et de groupe, reportez-vous à la section Gestion de l'espace.

Propriétés

Les propriétés suivantes sont disponibles dans la CLI et des propriétés équivalentes existent dans la BUI. Ces propriétés peuvent être définies à l'aide des commandes standard `get` et `set` de la BUI. De plus, ces propriétés peuvent être héritées d'un projet parent en utilisant la commande `unset`.

Nom dans la CLI	Type	Nom dans la BUI	Emplacement dans la BUI
aclinherit	hérité	Comportement d'héritage ACL	Accès

Nom dans la CLI	Type	Nom dans la BUI	Emplacement dans la BUI
aclmode	hérité	Comportement ACL en cas de changement de mode	Accès
atime	hérité	Mise à jour de l'heure d'accès à la lecture	Général
casesensitivity	au moment de la création	Sensibilité à la casse	Statique
checksum	hérité	Somme de contrôle	Général
compression	hérité	Compression des données	Général
compresratio	en lecture seule	Taux de compression	Statique
copies	hérité	Réplication supplémentaire	Général
creation	en lecture seule	-	-
dedup	hérité	Suppression des doublons de données	Général
exporté	hérité, packages de réplication uniquement	Exportation	Général
initiatorgroup	LUN locale	Groupe d'initiateurs	Protocoles
logbias	hérité	Décalage d'écriture synchrone	Général
lunumber	LUN locale	LUN	Protocoles
lunguid	en lecture seule, LUN locale	GUID	Protocoles
mountpoint	hérité	Point de montage	Général
nbmand	hérité	Verrouillage obligatoire non bloquant	Général

Nom dans la CLI	Type	Nom dans la BUI	Emplacement dans la BUI
nodestroy	hérité	Empêcher la destruction	Général
normalization	au moment de la création	Normalisation	Statique
origin	en lecture seule	Origin	Statique
quota	gestion de l'espace	Quota	Général
quota_snap	gestion de l'espace	Quota / Inclure les instantanés	Général
readonly	hérité	Lecture seule	Général
recordsize	hérité	Taille des enregistrements de la base de données	Général
reservation	gestion de l'espace	Reservation	Général
reservation_snap	gestion de l'espace	Réservation / Inclure les instantanés	Général
root_group	système de fichiers local	Groupe	Accès
root_permissions	système de fichiers local	Autorisations d'accès	Accès
root_user	système de fichiers local	Utilisateur	Accès
rstchown	hérité	Restreindre les modifications de propriété	Général
secondary cache	hérité	Utilisation du périphérique de cache	Général
shadow	au moment de la création	Source de migration de données	Statique
sharedav	hérité	Protocoles / HTTP / Mode Partage	Protocoles
shareftp	hérité	Protocoles / FTP / Mode Partage	Protocoles

Nom dans la CLI	Type	Nom dans la BUI	Emplacement dans la BUI
sharenfs	hérité	Protocoles / NFS / Mode Partage	Protocoles
sharesmb	hérité	Protocoles / SMB / Nom de la ressource	Protocoles
snapdir	hérité	Visibilité de .zfs/snapshot	Instantanés
snaplabel	hérité	Etiquette d'instantanés planifiés	Instantanés
space_available	en lecture seule	Espace disponible	Utilisation
space_data	en lecture seule	Données référencées	Utilisation
space_snapshots	en lecture seule	Données d'instantanés	Utilisation
space_total	en lecture seule	Espace total	Utilisation
space_unused_res	en lecture seule	Réservation inutilisée	Utilisation
sparse	LUN locale	Allocation fine	Général
targetgroup	LUN locale	Groupe de cibles	Protocoles
utf8only	au moment de la création	Rejeter non UTF-8	Statique
volblocksize	au moment de la création	Taille de bloc des volumes	Statique
vscan	hérité	Analyse antivirus	Général

General

Propriétés générales des partages

Cette section de la BUI contrôle les paramètres généraux du partage qui sont indépendants de tout protocole spécifique et qui ne sont pas liés au contrôle d'accès ou aux instantanés. Etant donné que la CLI regroupe toutes les propriétés dans une seule liste, cette section décrit le comportement des propriétés dans les deux contextes.

Pour plus d'informations sur la manière dont ces propriétés sont mappées vers la CLI, reportez-vous à la section CLI des projets.

Utilisation de l'espace

L'espace d'un pool de stockage est partagé entre tous les partages. Les systèmes de fichiers peuvent augmenter ou diminuer dynamiquement si nécessaire, même s'il est également possible d'appliquer des restrictions d'espace par partage. Des quotas et des réservations peuvent être appliqués par système de fichiers. Des quotas peuvent également être appliqués par utilisateur et par groupe. Pour plus d'informations sur la gestion de l'utilisation de l'espace des systèmes de fichiers, y compris les quotas et les réservations, consultez la section Gestion de l'espace.

Taille de volume

Cette propriété détermine la taille logique de la LUN au moment de l'exportation via iSCSI. Elle est valide uniquement pour les LUN. Cette propriété contrôle la taille de la LUN. Par défaut, les LUN réservent suffisamment d'espace pour remplir la totalité du volume. Pour plus d'informations, reportez-vous à la propriété Allocation fine. Si vous modifiez la taille d'une 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 la LUN. Avant d'effectuer cette opération, vérifiez les pratiques recommandées pour votre client iSCSI spécifique.

Allocation fine

Cette propriété détermine si de l'espace est réservé pour le volume. Elle est valide uniquement pour les LUN. Par défaut, une 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, la LUN consomme uniquement l'espace qui a été écrit dans la LUN. Cette propriété autorise l'allocation fine 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, reportez-vous à la propriété Réservation.

Propriétés

Ces propriétés standard 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.

Point de montage

Cette propriété détermine l'emplacement de montage du système de fichiers. Elle est valide uniquement pour les systèmes de fichiers.

Les restrictions suivantes s'appliquent uniquement 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`, "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 Espace de noms du système de fichiers.

Lecture seule

Cette propriété 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

Cette propriété 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 à 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

Cette propriété 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

Cette propriété 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. Activez cette propriété en cochant 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. Comme toujours, pour obtenir de meilleurs résultats, utilisez la même taille d'enregistrement que celle de l'application qui traite les données et 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 forcément des conséquences sur les performances ; d'une part, car la somme de contrôle est plus coûteuse à calculer et d'autre part, car il faut accéder aux métadonnées de la table de suppression des doublons et les gérer.

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.

Avertissement relatif aux performances : par nature, la suppression des doublons nécessite la modification de la table de suppression des doublons lorsqu'un bloc écrit 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 l'analyse avancée puis utilisez l'analyse pour mesurer les "opérations ZFS DMU ventilées par type d'objet DMU" et rechercher un taux plus élevé d'opérations DDT (opérations Data Duplication Table) soutenues que les 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.

Compression des données

Cette propriété contrôle que les données soient bien 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	arrêté	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.

Valeur BUI	Valeur CLI	Description
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 minimes.

Somme de contrôle

Cette propriété 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 les plus inquiets 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	16-bit fletcher checksum
Fletcher 4 (Standard)	fletcher4	32-bit fletcher checksum
SHA-256 (Sécurité renforcée)	sha256	SHA-256 checksum

Utilisation du périphérique de cache

Cette propriété vérifie que des 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 de stockage. 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 "tous" 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	Toutes	Tous les fichiers classiques ou les données de LUN ainsi que toutes les métadonnées sont mis en cache.

Valeur BUI	Valeur CLI	Description
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

Ce paramètre contrôle 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 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. Pour plus d'informations, se reporter à la section Oracle Intelligent Storage Protocol.

Valeur BUI	Valeur CLI	Description
Latence	latence	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

Cette propriété contrôle la taille de bloc utilisé par le système de fichiers. Elle est valide uniquement pour les systèmes de fichiers.

Par défaut les systèmes de fichiers utilisent une taille de bloc suffisante pour contenir le fichier ou une taille de bloc de 128 Ko pour les fichiers volumineux. Concrètement, les fichiers dépassant la taille de 128 Ko utilisent des blocs de 128 Ko. Si une application écrit ensuite sur le fichier en plusieurs fois, elle doit lire et écrire la totalité des données du bloc de 128 Ko même si, en comparaison, la quantité de données écrites est relativement faible.

Les partages qui hébergent de faibles charges de travail d'accès aléatoires (ex : les bases de données) doivent ajuster cette propriété de sorte qu'elle ait une valeur approximativement égale à celle de la taille d'enregistrement utilisée par la base de données. Si aucun chiffre précis n'est défini, vous pouvez définir 8 Ko, ce qui est en général un bon choix de valeur pour la majorité des charges de travail de base de données. Vous pouvez définir cette propriété sur n'importe quelle puissance de 2 allant de 512 octets à 128 Ko.

Le paramètre Taille des enregistrements de la base de données peut être contourné par Oracle Intelligent Storage Protocol. 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, se reporter à la section Oracle Intelligent Storage Protocol.

Réplication supplémentaire

Cette propriété 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.

Valeur BUI	Valeur CLI	Description
Normal (copie unique)	1	Comportement par défaut. Conserve une seule copie des blocs de données.
Two Copies	2	Conserve deux copies de chaque bloc de données.
Trois copies	3	Conserve trois copies de chaque bloc de données.

Analyse antivirus

Cette propriété 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 personnalisées

Si nécessaire, des propriétés personnalisées 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 Schéma.

Protocols

Protocoles des partages

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. Les propriétés NFS, SMB, HTTP et FTP s'appliquent uniquement aux systèmes de fichiers tandis que les propriétésiSCSI s'appliquent uniquement aux LUN.

Dans la BUI, chaque protocole affiche le chemin par lequel les clients qui utilisent ce protocole accèdent au partage. Par exemple, le système de fichiers "fs0" sur le serveur "twofish" sera disponible aux emplacements suivants :

Protocole	Emplacement
NFS	twofish:/export/fs0
SMB	\\twofish\fs0
HTTP	//twofish/shares/export/fs0/
FTP	ftp://twofish/export/fs0/
SFTP	/export/fs0/

Pour iSCSI, les initiateurs peuvent détecter la cible par le biais d'un des mécanismes décrits dans la documentation SAN.

NFS

Propriété de la BUI	Propriété de la CLI	Description
Mode de partage	off/ro/rw	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".
Désactiver la création de fichiers setuid/setgid	nosuid	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).

Propriété de la BUI	Propriété de la CLI	Description
Prevent clients from mounting subdirectories	nosub	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 (et non à NFSv4).
Mappage d'utilisateur anonyme	anon	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 du partage sont considérées comme venant d'un utilisateur possédant cet UID. Les bits d'accès et les ACL du fichier sont alors évalués normalement.
Character encoding	Voir ci-dessous	Cette propriété définit le jeu de caractères par défaut de tous les clients. Pour plus d'informations, reportez-vous à la section relative aux codages de jeu de caractères.
Security mode	Voir ci-dessous	Cette propriété définit le mode de sécurité de tous les clients.

Des exceptions à l'ensemble des modes de partage peuvent être définies pour les clients ou les collections de clients. En cas de tentative d'accès de la part d'un client, cet accès sera accepté ou non en fonction de la première exception de la liste qui correspond au client ou, si aucune exception de ce type n'existe, en fonction des modes de partage globaux définis ci-dessus. Ces collections de client doivent être définies à l'aide d'un des trois types suivants :

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
Réseau	@	Tous les clients dont l'adresse IP est comprise dans le sous-réseau IP spécifié, en notation CIDR.	192.168.20.0/22

Pour chaque client ou collection de client, vous définissez ensuite deux paramètres : vous déterminez si le client possède un accès en lecture seule ou en lecture-écriture au partage, puis si l'utilisateur root sur le client doit être traité en tant qu'utilisateur root (si défini) ou inconnu.

Si les groupes réseau sont utilisés, ils seront résolus à partir du service NIS (s'il est activé) puis à partir du serviceLDAP (s'il est activé). Si le service LDAP est utilisé, les groupes de réseau doivent être présents à l'emplacement par défaut, ou=Netgroup,(Base DN) et 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), 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 décision du nom d'hôte, reportez-vous à la section DNS. Il peut être difficile de gérer les groupes réseau. Suivez plutôt les règles de sous-réseau IP ou les règles de domaines DNS quand c'est possible.

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.

Considérations relatives à la CLI

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 séparée par des virgules contenant les valeurs présentées dans le tableau ci-dessus. Elle doit commencer par "ro", "rw" ou "off", de la même manière que pour les modes de partage globaux décrits dans la BUI. Par exemple,

```
set sharenfs=ro
```

définit le mode de partage de tous les clients sur lecture seule. Les utilisateurs root sur tous les clients accèdent aux fichiers du partage comme s'ils étaient des utilisateurs "inconnus".

Il est possible d'ajouter une des deux options "nosuid" et "anon" ou les deux. Rappelez-vous que, dans la CLI, il faut indiquer entre guillemets les valeurs de propriété qui contiennent le symbole égal "=". Par conséquent, pour définir le mappage de tous les utilisateurs inconnus sur l'UID 153762, vous devez spécifier :

```
set sharenfs="ro,anon=153762"
```

Il est possible de spécifier des exceptions supplémentaires en ajoutant du texte sous la forme "option=collection" où "option" est soit "ro", "rw" et "root" et définit le type d'accès à octroyer à la collection de clients. La collection est spécifiée par le caractère de préfixe à partir de la table ci-dessus et par un nom de domaine/domaine DNS ou un numéro de réseau CIDR. Par exemple, pour attribuer un accès en lecture-écriture à tous les hôtes du domaine sf.example.com et l'accès root à ceux du réseau 192.168.44.0/24, vous pouvez utiliser :

```
set sharenfs="ro,anon=153762,rw=.sf.example.com,root=@192.168.44.0/24"
```

Les noms de groupe réseau peuvent être utilisés à tous les endroits 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"
```

Les modes de sécurité sont spécifiés en ajoutant du texte sous la forme "option=mode" où l'option est "sec" et le mode est "sys", "krb5", "krb5:krb5i" ou "krb5:krb5i:krb5p".

```
set sharenfs="sec=krb5"
```

Modes de sécurité

Les modes de sécurité sont définis par partage et peuvent avoir des conséquences sur les performances. Le tableau suivant décrit les paramètres de sécurité Kerberos.

Paramètre	Description
krb5	Authentification d'utilisateur final via Kerberos V5
krb5i	krb5 plus préservation de l'intégrité (les paquets de données résistent aux dégradations)
krb5p	krb5 plus préservation de la confidentialité (les paquets de données résistent aux dégradations et sont chiffrés)

Les combinaisons de saveur Kerberos peuvent être spécifiés dans le paramètre du mode de sécurité. La combination de modes de sécurité permet aux clients de monter n'importe quelle saveur Kerberos répertorié.

Paramètre	Menu
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.

Paramètre	Menu
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.
krb5p	Kerberos v5 confidentialité uniquement - Les clients doivent monter à l'aide de cette saveur.

Pour plus d'informations sur NFS et Kerberos, voir :

- http://www.ietf.org/rfc/rfc2623.txt (`http://www.ietf.org/rfc/rfc2623.txt`) (NFSv2 et NFSv3 Security)
- http://www.ietf.org/rfc/rfc3530.txt (`http://www.ietf.org/rfc/rfc3530.txt`) (Protocole NFSv4)

Codages de jeu de caractères

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 pris en charge sont les suivants :

- euc-cn
- euc-jp
- euc-jpms
- euc-kr
- euc-tw
- iso8859-1

- iso8859-2
- iso8859-5
- iso8859-6
- iso8859-7
- iso8859-8
- iso8859-9
- iso8859-13
- iso8859-15
- koi8-r

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 :

```
set sharenfs="rw,euc-kr=*"
```

partage le système de fichiers avec le codage par défaut 'euc-kr'. Par exemple,

```
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.

SMB

Propriété	Description
Nom de la ressource	Nom utilisé par les clients SMB pour désigner le partage. Le nom de ressource " indique qu'aucun client SMB ne peut accéder au partage et le nom de ressource indique que le partage sera exporté avec le nom du système de fichiers.
Activer l'énumération basée sur les accès	Une fois activée, cette option effectue des énumérations en fonction des accès. C option filtre les entrées de répertoire en fonctions des informations d'identificat client. Lorsqu'un client n'a pas accès à un fichier ou à un répertoire, ce fichier ne pas dans la liste d'entrées envoyée au client. Cette option est désactivée par défa
Is a DFS Namespace	Propriété qui détermine si le partage est alloué comme un espace de noms DFS autonome.

Propriété	Description
ACL au niveau du partage	ACL combinée avec l'ACL d'un fichier ou d'un répertoire dans le partage afin de déterminer 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.

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 de détails, reportez-vous à la section relative aux projets. Un nom de ressource peut comprendre jusqu'à 80 caractères alphanumériques, sauf les caractères 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.

iSCSI

Propriété	Description
Groupe de cibles	Cibles sur lesquelles cette LUN est exportée.
Groupe(s) d'initiateurs	Initiateurs qui peuvent accéder à la LUN. Depuis la version logicielle 2013.1.0, plusieurs groupes d'initiateurs peuvent être affectés à une LUN.
Numéro d'unité logique	Quand les LUN sont associées à des groupes de cibles et d'initiateurs, on leur attribue des numéros d'unité logique uniques par groupe cible et paire d'initiateurs. Deux LUN accessibles par un initiateur via un groupe cible ne peuvent pas porter le même numéro d'unité logique. Cette propriété détermine si le numéro d'une unité logique doit être 0 ou un numéro attribué automatiquement.
Statut opérationnel	Statut opérationnel de cette LUN. Une LUN hors ligne n'est pas accessible aux initiateurs, quelle que soit la configuration de la cible ou de l'initiateur.

Propriété	Description
Comportement du cache d'écriture	Ce paramètre détermine si la LUN met en cache les données écrites. Si ce paramètre est désactivé, toutes les données écrites sont synchrones et si aucun périphérique de journal n'est disponible, les performances d'écriture en souffrent très fortement. Par conséquent, l'activation de ce paramètre améliore de façon significative les performances d'écriture mais peut également entraîner une altération des données à la suite d'arrêts inattendus, à moins que l'application client comprenne la sémantique d'un cache d'écriture volatile et qu'elle vide le cache lorsque cela est nécessaire. Consultez la documentation d'application client avant d'activer ce paramètre.
GUID	Un GUID de LUN est un identificateur unique en lecture seule qui identifie le périphérique SCSI. Ce GUID reste constant dans différents noeuds de cluster et environnements répliqués.

HTTP

Propriété	Description
Mode de partage	Mode de partage HTTP de ce système de fichiers. Le mode de partage est aucun, lecture seule ou lecture/écriture.

FTP

Propriété	Description
Mode de partage	Mode de partage FTP de ce système de fichiers. Le mode de partage est aucun, lecture seule ou lecture/écriture.

SFTP

Propriété	Description
Mode de partage	Mode de partage SFTP de ce système de fichiers. Le mode de partage est aucun, lecture seule ou lecture/écriture.

Voir aussi

- Partages
- Partages:Partages

Access

Contrôle d'accès

Cette vue vous permet de définir des options afin de contrôler le comportement ACL et l'accès au répertoire racine du système de fichiers. Cette vue est disponible uniquement pour les systèmes de fichiers.

Accès au répertoire racine

Ce paramètre permet de contrôler l'accès à la racine du 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 racine du système de fichiers.

Utilisateur

Propriétaire du répertoire racine. 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 au service 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 racine. 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 au service 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

Autorisations standard Unix 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.*
Execute	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.

- A partir de la version logicielle 2011.1, les comportements supplémentaires suivants sont associés à l'autorisation "write" pour tous les répertoires :
- Les fichiers enfant situés dans le répertoire peuvent être supprimés (comme pour l'autorisation D de l'ACL), à moins que le sticky bit soit positionné sur le répertoire, auquel cas les fichiers enfant ne peuvent être supprimés qu'à la demande du propriétaire du fichier.
- L'horodatage associé à un fichier ou à un répertoire peut être modifié (comme pour l'autorisation A de l'ACL)
- Il est possible de créer des attributs étendus et d'écrire dans le répertoire d'attributs étendus (comme pour l'autorisation W de l'ACL)

Dans la BUI, vous sélectionnez les autorisations en cliquant sur les cases correspondantes. Vous pouvez également cliquer sur l'étiquette ("utilisateur", "groupe" ou "autre") pour sélectionner (ou désélectionner) toutes les autorisations de l'étiquette en question. Dans la CLI, les autorisations sont spécifiées à l'aide d'une valeur octale Unix standard dans laquelle le premier chiffre correspond au type d'accès 'utilisateur', le deuxième au 'groupe' et le troisième à 'autre'. Chaque chiffre correspond à la somme des autorisations lecture (4), écriture (2) et exécution (1). La valeur d'autorisation `743` correspond donc au type d'accès utilisateur RWX, groupe R et autre WX.

Plutôt que de définir les bits d'autorisation POSIX à la création du partage, les administrateurs peuvent sélectionner l'option "Utiliser les autorisations Windows par défaut" qui permet d'appliquer une ACL par défaut décrite à la section ACL du répertoire racine ci-dessous. Ce raccourci permet de simplifier l'administration des environnements exclusivement ou majoritairement gérés par les utilisateurs de Windows. Il offre un comportement similaire à celui de la création de partage sur un serveur Windows.

Comportement des ACL

Pour plus d'informations sur les ACL et leur fonctionnement, consultez la documentation relative aux ACL du répertoire racine.

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.

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.

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 `propriétaire/groupe/autre` traditionnelles d'Unix.

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 ACL" et "changer de 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 du paramétrage par défaut.

Valeur BUI	Valeur CLI	Description
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 souhaiterez 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).

Lorsque vous utilisez SMB pour créer un fichier dans un répertoire avec une ACL triviale, toutes les entrées d'ACL sont héritées. Par conséquent, le comportement 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.

Le comportement décrit ci-dessous est susceptible d'être modifié dans les prochaines versions.

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 racine, cette propriété affecte le répertoire racine 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 racine du système de fichiers. Il n'existe aucun moyen de paramétrer l'ACL du répertoire racine 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 root y sont également décrits.

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 nommé	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.

Mode	Description
Allow	Les autorisations sont explicitement octroyées à la cible ACE.
Deny	Les autorisations sont explicitement refusées à la cible ACE.

	Autorisation	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.

	Autorisation	Description
(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.
(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.
(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.
	`Write`	
(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.
(d)	Supprimer	Autorisation de supprimer un fichier.
(D)	Supprimer 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`[1]	
(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`	
(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.

	Autorisation	Description
(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 l'option permettant d'appliquer les autorisations Windows par défaut est utilisée à la création du partage, une ACL est créée pour le répertoire racine du partage et est composée des trois entrées suivantes :

Type	Action	Accès
Propriétaire	Allow	Contrôle total
Groupe	Allow	Lecture et exécution
Tout le monde	Allow	Lecture et exécution

Snapshots

Instantanés

Les instantanés sont des copies en lecture seule d'un système de fichiers à un moment précis. Pour plus d'informations sur les instantanés et leur fonctionnement, reportez-vous à la page Concepts.

Propriétés des instantanés

Visibilité de .zfs/snapshot

Les instantanés de système de fichiers sont accessibles par le biais des protocoles de données à l'emplacement `.zfs/snapshot` à la racine du système de fichiers. Ce répertoire contient une liste de tous les instantanés du système de fichiers, qui sont accessibles de la même manière que des données classiques de système de fichier (en mode de 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.

Valeur BUI	Valeur CLI	Description
Masqué	hidden	Le répertoire .zfs n'est pas visible lorsque le contenu des répertoires est listé dans la racine du système de fichiers. Il s'agit du paramètre par défaut.
Visible	visible	Ce répertoire .zfs s'affiche comme n'importe quel autre répertoire du système de fichiers.

Etiquette d'instantanés planifiés

Cette propriété facultative ajoute une étiquette définie par l'utilisateur à chaque instantané planifié et est vide par défaut. Cette étiquette peut être définie pour un partage individuel ou 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 l'instantané a été pris, par exemple "projet1:partage1" peut indiquer un instantané planifié pris sur le partage1 au sein du projet1. Les étiquettes peuvent comporter jusqu'à 35 caractères alphanumériques et inclure les caractères spéciaux **`_ - . :`**

BUI

Liste des instantanés (BUI)

Sous l'onglet "Instantanés", vous trouverez la liste des instantanés actifs du partage. Cette liste est divisée en deux onglets : l'onglet "Instantanés" permet d'accéder aux instantanés et les gérer. L'onglet "Calendriers" permet la gestion automatique des calendriers d'instantanés. Dans l'onglet "Instantanés", vous pouvez choisir d'afficher tous les instantanés, uniquement les instantanés manuels ou uniquement les instantanés planifiés. Pour chaque instantané, les champs suivants sont affichés :

Champ	Description
Nom	Nom de l'instantané. Il y a deux types d'instantané : manuel et automatique.
	`Instantanés manuels :`, "Nom" est le nom attribué à la création de l'instantané. Vous pouvez renommer les instantanés en cliquant dessus et en saisissant un nouveau nom.
	`Instantanés automatiques :` il en existe trois types différents, et ceux-ci ne peuvent pas être renommés :
	- **`.auto :`** instantanés programmés configurés par l'utilisateur avec des stratégies de conservation personnalisées (reportez-vous à la section Instantanés planifiés).

Champ	Description
	- **.ndmp :** utilisé pour la sauvegarde NDMP et élagué automatiquement.
	- **.rr:** utilisé pour la réplication distante et élagué automatiquement.
Création	Date et heure de création de l'instantané.
Unique	Quantité d'espace unique utilisée par l'instantané. Les instantanés commencent en général par référencer tous les blocs identiques comme le système de fichiers ou la LUN elle-même. Quant le système de fichiers actif diverge, les blocs qui ont été modifiés dans le partage actif peuvent être conservés par un ou plusieurs instantanés. Lorsqu'un bloc fait partie intégrante de plusieurs instantanés, il est comptabilisé dans l'utilisation de l'instantané du partage mais n'apparaît pas dans l'espace unique d'un instantané. L'espace unique correspond à des blocs détenus uniquement par un instantané et représente la quantité d'espace qui serait libéré si l'instantané était détruit.
Total	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.
Clones	Affiche le nombre de clones de l'instantané. Lorsque vous placez le pointeur sur la ligne d'un instantané dont le nombre de clones est différent de 0, un lien "Afficher..." s'affiche. Si vous cliquez sur ce lien, une boîte de dialogue contenant la liste complète des clones s'ouvre.

Tâches

Prise d'instantanés manuels (BUI)

Il y a deux types d'instantané : au niveau projet et au niveau partage/LUN.

Créer un instantané au niveau projet

1. Ouvrez le projet dont vous souhaitez prendre un instantané.
2. Cliquez sur l'onglet Snapshot.
3. Cliquez sur l'icône . La liste des instantanés apparaît.
4. Dans la boîte de dialogue, saisissez un nom pour l'instantané.
5. Cliquez sur "apply" pour créer l'instantané.

Créer un instantané au niveau partage/LUN

1. Ouvrez le partage/LUN dont vous souhaitez prendre un instantané.
2. Cliquez sur l'onglet Snapshot.
3. Cliquez sur l'icône . La liste des instantanés apparaît.

4. Dans la boîte de dialogue, saisissez un nom pour l'instantané.
5. Cliquez sur "apply" pour créer l'instantané.

Le nombre d'instantanés n'est pas limité, mais chaque instantané consomme de la mémoire. Si vous créez un grand nombre d'instantanés, cela peut donc entraîner un ralentissement du système. La limite pratique du nombre d'instantanés sur le système dépend de la configuration système mais elle dépasse les cent mille.

Attribution d'un autre nom à un instantané (BUI)

Pour renommer un instantané, cliquez sur son nom dans la liste des instantanés actifs. Une boîte de saisie de texte s'ouvre. Après avoir modifié le nom de l'instantané dans le champ de saisie, cliquez sur Entrée ou déplacez le curseur pour valider les modifications.

Destruction d'un instantané (BUI)

Pour détruire un instantané, cliquez sur l'icône après avoir placé le pointeur sur la ligne de l'instantané concerné. La destruction d'un instantané impose la destruction de ses clones et descendants. Une liste des clones qui seront affectés s'affiche.

Restauration d'un instantané (BUI)

En plus de permettre l'accès aux données d'un répertoire d'instantané de système de fichiers, les instantanés peuvent également être utilisés pour rétablir une instance précédente d'un système de fichiers ou d'une LUN. Cette action nécessite de détruire les instantanés les plus récents, ainsi que leurs clones et de rétablir le contenu du partage à leur état d'origine au moment où l'instantané a été pris. Cela n'affecte aucun paramètre de propriété sur le partage, même si les modifications apportées à l'accès au répertoire root du système de fichiers seront perdues étant donné qu'elles font partie des données du système de fichiers.

Pour rétablir un système de fichiers, cliquez sur l'icône de l'instantané de destination. Une boîte de dialogue de confirmation s'ouvre avec la liste des clones restants ainsi que leurs descendants. Vous êtes informé que ces éléments seront supprimés au cours du processus.

Clonage d'un instantané (BUI)

Un clone est une copie accessible en écriture d'un instantané. Il est traité comme n'importe quel autre partage. De la même manière que les instantanés du système de fichiers, il ne consomme pas d'espace supplémentaire au départ. Au fur et à mesure que les données contenues dans le clone changent, l'espace occupé par le clone augmente. Vous ne pouvez supprimer l'instantané original qu'en supprimant également son clone. Les instantanés planifiés peuvent être clonés en toute sécurité. Ces instantanés sont ignorés quand des suppressions sont effectuées.

Pour créer un clone, cliquez sur l'icône de l'instantané source. Une boîte de dialogue vous invite à saisir les valeurs suivantes.

Propriété	Description
Projet	Projet de destination. Par défaut, les clones sont créés au sein du projet en cours, mais vous pouvez également les créer dans d'autres projets (ou les déplacer par la suite).
Nom	Nom que vous souhaitez attribuer au clone.
Conserver les propriétés locales	Par défaut, la totalité des propriétés héritées du système de fichiers s'appliquent au projet de destination dans le clone. Les paramètres locaux sont toujours conservés. Si vous définissez cette propriété, les propriétés héritées sont conservées comme paramètre local dans le nouveau clone.
Point de montage	Lorsque vous conservez les propriétés locales, vous devez attribuer un point de montage différent au clone car les partages ne peuvent pas avoir le même point de montage. Cette option est disponible uniquement lorsque la propriété "Conserver les propriétés locales" est activée.

Instantanés planifiés (BUI)

Outre les instantanés manuels, vous pouvez configurer des instantanés automatiques en fonction du tableau ci-dessous. Ces instantanés sont nommés ".auto-<timestamp>" et peuvent être pris toutes les demi-heures, toutes les heures, tous les jours, toutes les semaines Un calendrier est une liste d'intervalles et de stratégies de conservation. Pour ajouter un nouvel intervalle, cliquez sur l'icône lorsque l'onglet "Calendriers" est affiché. Chaque intervalle possède les propriétés suivantes.

Propriété	Description
Fréquence	L'une des valeurs suivantes : "demi-heure", "heure", "jour", "semaine" ou "mois". Cette propriété permet d'indiquer la fréquence de prise des instantanés.
Offset	Cette propriété permet de spécifier un décalage au sein de la fréquence. Par exemple, lorsque vous choisissez la fréquence 'hour', les instantanés peuvent être pris avec un décalage explicite (en minutes). Pour les prises d'instantanés quotidiennes, vous pouvez indiquer un décalage en heures et minutes et pour les prises d'instantanés hebdomadaires ou mensuelles, vous pouvez indiquer un décalage en jours, heures et minutes.
Conserver au plus	Cette propriété contrôle la stratégie de conservation des instantanés. 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). Cette limite permet de supprimer les instantanés automatiques d'un intervalle spécifique s'ils sont antérieures à la limite fixée par la stratégie de conservation. Cette limite est appliquée en fonction du moment où les instantanés ont été pris. Si vous avez défini des prises d'instantanés toutes les heures et que l'appareil est arrêté durant une journée, lorsque vous le redémarrez, tous vos instantanés sont donc supprimés. Les instantanés qui font partie de plusieurs intervalles sont supprimés uniquement si aucun intervalle n'indique qu'ils doivent être conservés.

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.

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.

Les versions précédentes du logiciel permettaient de définir la fréquence des instantanés automatiques en minutes. Il s'est avéré que cela ajoutait une pression supplémentaire sur le système et que c'était rarement utile. C'est pour éviter que les utilisateurs ajoutent une pression supplémentaire sur leur système que cette fonction a été retiré dans la version 2010.Q3. La fréquence des instantanés peut désormais être définie toutes les demi-heures ou plus. Si cette version du logiciel est rétablie, les fréquences en minute sont préservées et les instances précédentes expirent en fonction de ce qui est indiqué dans le 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.

CLI

Pour accéder aux instantanés d'un partage, accédez au partage et au contexte d'instantané.

```
clownfish:> shares select default select builds
clownfish:shares default/builds> snapshots
clownfish:shares default/builds snapshots>
```

Liste des instantanés (CLI)

Ces instantanés peuvent être répertoriés à l'aide des commandes standard de la CLI.

```
clownfish:shares default/builds snapshots> list
today
yesterday
clownfish:shares default/builds snapshots>
```

Prise d'instantanés manuels (CLI)

Pour prendre un instantané manuel au niveau projet, accédez au projet et au noeud de partage, puis utilisez la commande `snapshot` :

```
clownfish:cd /
clownfish:shares select myproject snapshots
clownfish:shares myproject snapshots> snapshot cob_monday
```

Pour prendre un instantané manuel au niveau partage d'un partage individuel, accédez à ce partage et utilisez la commande d'instantané :

```
clownfish:cd /
clownfish:shares select myproject select share1 snapshots
clownfish:snapshot lunchtime
```

Attribution d'un autre nom à un instantané (CLI)

Pour renommer un instantané, exécutez la commande `rename` :

```
clownfish:shares default/builds snapshots> rename test test2
clownfish:shares default/builds snapshots>
```

Destruction d'un instantané (CLI)

Pour détruire un instantané, exécutez la commande `destroy` :

```
clownfish:shares default/builds snapshots> select test2
clownfish:shares default/builds@test2> destroy
This will destroy this snapshot. Are you sure? (Y/N)
clownfish:shares default/builds snapshots>
```

Vous pouvez également exécuter la commande `destroy` à partir du contexte de partage sans sélectionner d'instantané :

```
clownfish:shares default/builds snapshots> destroy test2
This will destroy this snapshot. Are you sure? (Y/N)
clownfish:shares default/builds snapshots>
```

Restauration d'un instantané (CLI)

Pour rétablir un instantané, sélectionnez l'instantané cible et exécutez la commande `rollback` :

```
clownfish:shares default/builds snapshots> select today
clownfish:shares default/builds@today> rollback
Rolling back will revert data to snapshot, destroying newer data. Active
initiators will be disconnected.

Continue? (Y/N)
clownfish:shares default/builds@today>
```

Clonage d'un instantané (CLI)

Pour cloner un instantané, exécutez la commande `clone`. Cette commande vous place dans un contexte de partage non validé identique à celui utilisé pour créer les partages. A partir d'ici, vous pouvez ajuster les propriétés si nécessaire avant de valider les modifications pour créer un clone.

```
clownfish:shares default/builds snapshots> select today
clownfish:shares default/builds@today> clone testbed
clownfish:shares default/testbed (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)
clownfish:shares default/testbed (uncommitted clone)> set quota=10G
                          quota = 10G (uncommitted)
clownfish:shares default/testbed (uncommitted clone)> commit
clownfish:shares default/builds@today>
```

La commande prend également en charge un premier argument facultatif, à savoir le projet dans lequel le clone va être créé. Par défaut, le clone est créé dans le même projet que celui utilisé pour le partage cloné.

Instantanés planifiés (CLI)

Des instantanés planifiés automatiques peuvent être configurés à l'aide de la commande `automatic` à partir du contexte d'instantané, au niveau projet d'un partage individuel. Une fois que vous êtes dans ce contexte, vous pouvez ajouter ou supprimer des intervalles à l'aide des commandes `create` et `destroy`. Chaque intervalle possède un jeu de propriétés mappé vers la vue BUI de la fréquence, de décalage et du nombre d'instantanés à conserver. Les calendriers sont maintenus au format UTC.

```
clownfish:shares default/builds snapshots> automatic
clownfish:shares default/builds snapshots automatic> create
clownfish:shares default/builds snapshots automatic (uncommitted)> set frequency=day
                     frequency = day (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> set hour=14
                          hour = 14 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> set minute=30
                        minute = 30 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> set keep=7
                          keep = 7 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> get
                     frequency = day (uncommitted)
                           day = (unset)
```

```
                        hour = 14 (uncommitted)
                      minute = 30 (uncommitted)
                        keep = 7 (uncommitted)
clownfish:shares default/builds snapshots automatic (uncommitted)> commit
clownfish:shares default/builds snapshots automatic> list
NAME                 FREQUENCY            DAY                  HH:MM KEEP
automatic-000        day                  -                    14:30    7
clownfish:shares default/builds snapshots automatic> done
clownfish:shares default/builds snapshots>
```

Définit de l'étiquette d'instantané planifié (CLI)

Dans la BUI, la propriété "Etiquette d'instantanés planifiés" peut être définie sur un niveau de projet ou de partage. De la même manière dans la CLI, l'étiquette peut être définie en navigant d'abord dans le contexte de projet ou de partage. Pour créer une étiquette d'instantané planifié, exécutez la commande `set snaplabel` :

```
clownfish:shares project1/share1> ’’’set snaplabel=project1:share1
```

Projects

BUI

L'interface utilisateur est accessible à partir de "Partages -> Projets". Cette interface utilisateur présente une liste de tous les projets du système. Vous pouvez sélectionner les projets dans le panneau Projet ou en cliquant sur le nom du projet lorsque vous éditez un partage au sein d'un projet.

Liste des projets

Une fois que vous avez navigué jusqu'à la vue du projet, une liste des projets du système s'affiche. Vous pouvez également naviguer jusqu'à l'écran des partages et ouvrir le panneau Projet pour accéder à un raccourci vers les projets. Ce panneau ne peut pas afficher la liste complète des projets quand ces derniers sont trop nombreux et ne remplace pas la liste complète des projets. Les champs suivants sont affichés pour chaque projet :

Champ	Description
Nom	Nom du partage. Il s'agit d'un champ de texte modifiable. Si vous cliquez sur le nom, vous pouvez saisir un nouveau nom de projet. Appuyez sur la touche Entrée ou déplacez le curseur pour valider la modification. Vous êtes invité à confirmer cette action car elle impose la déconnexion des clients actifs.
Taille	Taille totale de tous les partages d'un projet et de la réservation inutilisée.

Les outils suivants sont disponibles pour chaque projet :

Icône	Description
	Modifier un projet (également accessible en cliquant deux fois sur la ligne).
	Détruire le projet. Vous êtes invité à confirmer cette action car elle entraîne la destruction de toutes les données du partage et ne peut pas être annulée.

Edition d'un projet

Pour modifier un projet, cliquez sur l'icône représentant un crayon, cliquez deux fois sur la ligne dans la liste des projets ou cliquez sur le nom du projet en question dans le panneau Projet. Cette action permet de sélectionner un projet et affiche de nombreux onglets différents qui vous permettent de modifier les propriétés du projet. Vous pouvez consulter l'intégralité des fonctionnalités dans la section correspondant à chaque onglet :

- Général
- Protocoles
- Accès
- Instantanés
- Réplication

Le nom du projet est affiché dans l'angle supérieur gauche, à droite du panneau Projet. Vous pouvez également modifier le nom du projet en cliquant dessus et en saisissant le nouveau nom dans la zone de saisie. Vous êtes invité à confirmer cette action car elle impose la déconnexion des clients actifs du projet.

Statistiques d'utilisation

Dans la partie gauche de la vue (sous le panneau Projet lorsqu'il est développé), vous trouverez un tableau explicatif des statistiques d'utilisation de l'espace. Si une propriété a la valeur zéro, elle est exclue du tableau. La plupart de ces propriétés sont identiques entre les projets et les partages, bien que certaines statistiques ne soient utiles que pour les projets.

Espace disponible

Voir la section Partages.

Données référencées

Il s'agit de la somme des données référencées de tous les partages du projet, en plus d'un faible temps système. Reportez-vous à la section Partages pour plus d'informations sur le calcul des données référencées de partages.

Données d'instantanés

Il s'agit de la somme de toutes les données d'instantané pour tous les partages et les temps système de l'instantané du projet. Reportez-vous à la section Partages pour plus d'informations sur le calcul des données d'instantané de partages.

Réservation inutilisée

Réservation inutilisée du projet. Ce calcul inclut les données qui ne sont pas en cours d'utilisation pour la réservation au niveau du projet. Il n'inclut pas les réservations inutilisées des partages contenus dans le projet.

Réservation inutilisée des partages

Somme des réservations inutilisées de tous les partages. Reportez-vous à la section Partages pour plus d'informations sur le calcul de la réservation inutilisée pour les partages.

Espace total

Somme des données référencées, des données d'instantanés, de la réservation inutilisée et des réservations inutilisées des partages.

Propriétés statiques

Dans la partie gauche de la vue des partages, vous trouverez les propriétés statiques disponibles lors de la modification d'un projet spécifique. Ces propriétés sont en lecture seule et ne peuvent pas être modifiées.

Taux de compression

Reportez-vous à la section Partages pour une description complète.

Création de projets

Pour créer un projet, affichez la liste des projets et cliquez sur le bouton . Vous pouvez également cliquer sur le bouton "Ajouter..." dans le panneau Projet présent sur la même boîte de dialogue. Saisissez le nom du projet et cliquez sur apply pour créer le projet.

CLI

La CLI des projets est disponible sous `shares`

Navigation

Pour sélectionner un projet, exécutez la commande `select` :

```
clownfish:> shares
clownfish:shares> select default
clownfish:shares default> 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
                  secondarycache = all
                           nbmand = false
                       sharesmb = off
                       sharenfs = on
                        snapdir = hidden
                     snaplabel = project1:share1
                          vscan = false
                       sharedav = off
                       shareftp = off
                  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
clownfish:shares default>
```

Opérations relatives aux projets

Un projet est créé à l'aide de la commande `project`. Si nécessaire, vous pouvez modifier les propriétés avant de valider les modifications :

```
clownfish:shares> project home
clownfish:shares home (uncommitted)> get
                     mountpoint = /export (default)
                          quota = 0 (default)
                    reservation = 0 (default)
                       sharesmb = off (default)
                       sharenfs = on (default)
                       sharedav = off (default)
                       shareftp = 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)
                        copies = (default)
                      readonly = (default)
                    recordsize = (default)
                 secondarycache = (default)
                         nbmand = (default)
                        snapdir = (default)
                     snaplabel = project1:share1
                          vscan = (default)
                custom:contact = (default)
             custom:department = (default)
clownfish:shares home (uncommitted)> set sharenfs=off
                     sharenfs = off (uncommitted)
clownfish:shares home (uncommitted)> commit
clownfish:shares>
```

Vous pouvez supprimer un projet à l'aide de la commande `destroy` :

```
clownfish:shares> destroy home
This will destroy all data in "home"! Are you sure? (Y/N)
clownfish:shares>
```

Il est également possible d'exécuter cette commande à partir du contexte de projet après avoir sélectionné un projet.

Vous pouvez renommer un projet à l'aide la commande `rename` :

```
clownfish:shares> rename default home
clownfish:shares>
```

Sélection d'un pool dans un cluster

Dans une configuration de cluster actif/actif, un noeud peut contrôler deux pools pendant le basculement. Dans ce cas, le contexte de la CLI affiche le pool en cours entre parenthèses. Vous pouvez modifier des pools à l'aide de la commande `set` à partir du plus haut niveau du contexte des partages :

```
clownfish:shares (pool-0)> set pool=pool-1
clownfish:shares (pool-1)>
```

Une fois que le contexte de pool est sélectionné, les projets et les partages sont gérés dans ce pool à l'aide des interfaces de la CLI standard.

Propriétés

Les propriétés suivantes sont disponibles dans la CLI et des propriétés équivalentes existent dans la BUI. Ces propriétés peuvent être définies à l'aide des commandes standard `get` et `set` de la BUI. De plus, ces propriétés peuvent être héritées d'un projet parent en utilisant la commande `unset`.

Nom dans la CLI	Type	Nom dans la BUI	Emplacement dans la BUI
aclinherit	hérité	Comportement d'héritage ACL	Accès
aclmode	hérité	Comportement ACL en cas de changement de mode	Accès
atime	hérité	Mise à jour de l'heure d'accès à la lecture	Général
checksum	hérité	Somme de contrôle	Général
compression	hérité	Compression des données	Général
compressratio	en lecture seule	Taux de compression	Statique
copies	hérité	Réplication supplémentaire	Général
creation	en lecture seule	-	-
dedup	hérité	Suppression des doublons de données	Général
default_group	valeur par défaut	Groupe	Général
default_permissions	valeur par défaut	Autorisations d'accès	Général
default_sparse	valeur par défaut	Allocation fine	Général
default_user	valeur par défaut	Utilisateur	Général
default_volblocksize	valeur par défaut	Taille de bloc des volumes	Général
default_volsize	valeur par défaut	Taille de volume	Général

Nom dans la CLI	Type	Nom dans la BUI	Emplacement dans la BUI
mountpoint	hérité	Point de montage	Général
nbmand	hérité	Verrouillage obligatoire non bloquant	Général
quota	gestion de l'espace	Quota	Général
readonly	hérité	Lecture seule	Général
recordsize	hérité	Taille des enregistrements de la base de données	Général
reservation	gestion de l'espace	Reservation	Général
secondary cache	hérité	Utilisation du périphérique de cache	Général
sharedav	hérité	Protocoles / HTTP / Mode Partage	Protocoles
shareftp	hérité	Protocoles / FTP / Mode Partage	Protocoles
sharenfs	hérité	Protocoles / NFS / Mode Partage	Protocoles
sharesmb	hérité	Protocoles / SMB / Nom de la ressource	Protocoles
snapdir	hérité	Visibilité de .zfs/snapshot	Instantanés
snaplabel	hérité	Etiquette d'instantanés planifiés	Instantanés
space_available	en lecture seule	Espace disponible	Utilisation
space_data	en lecture seule	Données référencées	Utilisation
space_snapshots	en lecture seule	Données d'instantanés	Utilisation
space_total	en lecture seule	Espace total	Utilisation
space_unused_res	en lecture seule	Réservation inutilisée	Utilisation

Nom dans la CLI	Type	Nom dans la BUI	Emplacement dans la BUI
space_unused_res_shares	en lecture seule	Réservation inutilisée des partages	Utilisation
vscan	hérité	Analyse antivirus	Général

General

Propriétés générales des projets

Cette section de la BUI contrôle les paramètres généraux du projet qui sont indépendants de tout protocole spécifique et qui ne sont pas liés au contrôle d'accès ou aux instantanés. Etant donné que la CLI regroupe toutes les propriétés dans une seule liste, cette section décrit le comportement des propriétés dans les deux contextes.

Pour plus d'informations sur la manière dont ces propriétés sont mappées vers la CLI, reportez-vous à la section CLI des projets.

Utilisation de l'espace

L'espace d'un pool de stockage est partagé entre tous les partages. Les systèmes de fichiers peuvent augmenter ou diminuer dynamiquement si nécessaire, même s'il est également possible d'appliquer des restrictions d'espace par partage. Pour plus d'informations sur le stockage de pool, reportez-vous à la page Concepts.

Quota

Définit une limite d'espace total consommé par tous les systèmes de fichiers et les LUN au sein d'un projet. Pour plus d'informations, reportez-vous à la section Partages. Contrairement aux systèmes de fichiers, les quotas de projet ne peuvent pas exclure les instantanés et peuvent uniquement être appliqués à l'ensemble des partages et à leurs instantanés.

Reservation

Cette propriété permet de garantir une quantité d'espace minimum à utiliser dans l'ensemble des systèmes de fichiers et des LUN du projet. Pour plus d'informations, reportez-vous à la section Partages. Contrairement aux systèmes de fichiers, les réservations de projet ne peuvent pas exclure les instantanés et peuvent uniquement être appliqués à l'ensemble des partages et à leurs instantanés.

Propriétés héritées

Il s'agit de propriétés standard qui peuvent être héritées par les partages au sein du projet. Le comportement de ces propriétés est identique au comportement au niveau des partages. Des informations plus détaillées sont disponibles dans la section Partages.

- Point de montage
- Lecture seule
- Mise à jour de l'heure d'accès à la lecture
- Verrouillage obligatoire non bloquant
- Compression des données
- Suppression des doublons de données
- Somme de contrôle
- Utilisation du périphérique de cache
- Taille des enregistrements de la base de données
- Réplication supplémentaire
- Analyse antivirus

Propriétés personnalisées

Si nécessaire, des propriétés personnalisées 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 Schéma.

Paramètres par défaut de création d'un système de fichiers

Ces paramètres sont utilisés pour appliquer les valeurs par défaut lors de la création d'un système de fichiers. La modification de ces paramètres n'affecte pas les systèmes de fichiers existants. Vous trouverez plus d'informations à la section Partages appropriée.

- Utilisateur
- Groupe
- Autorisations d'accès

Paramètres par défaut de création d'une LUN

Ces paramètres sont utilisés pour appliquer les valeurs par défaut lors de la création d'une LUN. La modification de ces paramètres n'affecte pas les LUN existantes. Vous trouverez plus d'informations à la section Shares appropriée.

- Taille de volume

- Allocation fine
- Taille de bloc des volumes

Protocols

Protocoles de projet

Chaque projet possède des propriétés de protocole spécifiques qui définissent le comportement de différents protocoles pour les partages de ce projet. En général, lespartages héritent de propriétés de protocoles spécifiques de manière très simple. Les exceptions et cas particuliers sont répertoriés ici. Pour les problèmes relatifs aux protocoles, reportez-vous à la section Dépannage.

NFS

Les propriétés de partage NFS sont héritées normalement et décrites dans la documentation relative aux partages.

SMB

Propriété	Description
Nom de la ressource	Nom utilisé par les clients SMB pour désigner le partage.
Activer l'énumération basée sur les accès	Une fois activée, cette option effectue des énumérations en fonction des accès. C option filtre les entrées de répertoire en fonctions des informations d'identificat client. Lorsqu'un client n'a pas accès à un fichier ou à un répertoire, ce fichier ne pas dans la liste d'entrées envoyée au client. Cette option est désactivée par défa

Deux partages SMB présents sur le même système ne peuvent pas avoir le même nom de ressource. Lorsqu'un système de fichiers hérite des noms de ressources d'un projet, le nom de ressource du partage est construit en fonction des règles suivantes :

Nom de ressource du projet	Nom de ressource du partage
"arrêté"	Les systèmes de fichiers ne sont pas exportés via SMB.
"en marche"	Les systèmes de fichiers sont exportés via SMB avec leur nom comme nom de ressource.

Nom de ressource du projet	Nom de ressource du partage
Tout sauf "off" ou "on"	Un nom de ressource au format <*nom de la ressource du prpjet*>_<*nom du système de fichiers*> est créé pour chaque système de fichiers.

iSCSI

Les propriétés iSCSI ne sont pas héritées.

HTTP

Les propriétés de partage HTTP sont héritées normalement et décrites dans la documentation relative aux partages.

FTP

Les propriétés de partage FTP sont héritées normalement et décrites dans la documentation relative aux partages.

Voir aussi

- Partages:Projets

Access

Contrôle d'accès

Cette vue offre un contrôle sur les propriétés pouvant être héritées et affectant le comportement des ACL.

Comportement des ACL héritées

Ces propriétés se comportent de la même façon qu'elles le font au niveau du partage. La modification de ces propriétés entraîne la modification du comportement correspondant pour tous les systèmes de fichiers qui héritent de ces propriétés.

- Comportement ACL en cas de changement de mode

- Comportement d'héritage ACL

Snapshots

Instantanés

Les instantanés sont des copies en lecture seule d'un système de fichiers à un moment précis. Pour plus d'informations sur les instantanés et leur fonctionnement, reportez-vous à la page Concepts. Les instantanés de projet sont des instantanés de chaque système de fichiers et de chaque LUN du projet, tous ayant des noms identiques. Les partages peuvent supprimer les instantanés individuellement. Même si elle est prise en charge, la création d'un instantané portant un nom identique à celui de l'instantané du projet peut entraîner un comportement indéfini étant donné que l'instantané sera considéré comme faisant partie de l'instantané du projet du même nom.

Propriétés des instantanés

Visibilité de .zfs/snapshot

Les instantanés de système de fichiers sont accessibles par le biais des protocoles de données à l'emplacement `.zfs/snapshot` à la racine du système de fichiers. Ce répertoire contient une liste de tous les instantanés du système de fichiers, qui sont accessibles de la même manière que des données classiques de système de fichier (en mode de 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.

Valeur BUI	Valeur CLI	Description
Masqué	hidden	Le répertoire .zfs n'est pas visible lorsque le contenu des répertoires est listé dans la racine du système de fichiers. Il s'agit du paramètre par défaut.
Visible	visible	Ce répertoire .zfs s'affiche comme n'importe quel autre répertoire du système de fichiers.

Etiquette d'instantanés planifiés

Cette propriété facultative ajoute une étiquette définie par l'utilisateur à chaque instantané planifié et est vide par défaut. Cette étiquette peut être définie pour un partage individuel ou 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 l'instantané a été pris, par exemple

"projet1:partage1" peut indiquer un instantané planifié pris sur le partage1 au sein du projet1. Les étiquettes peuvent comporter jusqu'à 35 caractères alphanumériques et inclure les caractères spéciaux `_ - . :`

BUI

Les instantanés au niveau du projet sont administrés de la même manière que les instantanés au niveau du partage. Les actions suivantes sont décrites sous la section relative aux partages.

- Création d'une liste des instantanés
- Prise d'instantanés
- Attribution d'un autre nom à un instantané
- Destruction d'un instantané
- Instantanés planifiés

Les instantanés de projet ne prennent pas en charge les opérations de restauration ou de clonage.

CLI

Pour accéder à l'instantané d'un projet, accédez au projet en question et exécutez la commande `snapshots`.

```
clownfish:> shares select default
clownfish:shares default> snapshots
clownfish:shares default snapshots>
```

A ce stade, les instantanés sont administrés de la même manière que les instantanés au niveau du partage. Les actions suivantes sont décrites sous la section relative aux partages.

- Création d'une liste des instantanés
- Prise d'instantanés
- Attribution d'un autre nom à un instantané
- Destruction d'un instantané
- Instantanés planifiés

Les instantanés de projet ne prennent pas en charge les opérations de restauration ou de clonage.

Replication

Introduction à la 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 manuelle de projet et de partage basée sur les instantanés sur un nombre illimité d'appareils cible, en fonction d'un calendrier ou de manière continue. La réplication inclut les données et les métadonnées. La réplication distante (ou simplement "réplication") est une fonction générique optimisée pour les cas d'utilisation suivants :

- **Récupération après sinistre** La réplication peut être utilisée pour mettre en miroir un appareil afin d'effectuer une récupération après un sinistre. Dans le cas d'un sinistre qui affecte le service de l'appareil principal (ou même la totalité d'un centre de données), les administrateurs activent ce service sur le site du sinistre pour effectuer une récupération à l'aide des données répliquées les plus récentes. Une fois que le site principal a été restauré, vous pouvez renvoyer vers le site principal les données modifiées lorsque le site de récupération était en service et restaurer le service normal. Il est possible de tester ce type de scénario avant que ces sinistres ne se produisent.
- **Répartition de données** La réplication peut servir à répartir les données (telles que les images ou les médias de la machine virtuelle) dans des systèmes distants du monde entier dans les cas où les clients de l'appareil cible ne seraient pas en mesure d'atteindre l'appareil source directement ou lorsque ce type de configuration présente une latence trop élevée. Un exemple utilise ce schéma pour la mise en mémoire cache locale afin d'améliorer la latence des données en lecture seule (comme les documents).
- **Sauvegarde disque à disque**. La réplication peut être utilisée comme solution de sauvegarde dans les environnements où les sauvegardes sur bande ne sont pas réalisables. Ce peut être notamment le cas car la bande passante disponible est insuffisante ou parce que le temps de récupération est trop élevé.
- **Migration de données**. La réplication peut servir à migrer des données et des configurations entre les appareils lors de mises à niveau matérielles ou en cas de rééquilibrage du stockage. La migration shadow peut également être utilisée à cette fin.

La fonction de réplication distante possède plusieurs propriétés importantes :

- **Snapshot-based**. 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 complète, l'intégralité du contenu du groupe est envoyée vers le nouvel instantané. Lors d'une mise à jour incrémentielle, seules les modifications apportées depuis le dernier instantané de réplication pour la même action sont envoyées.
- **Block-level**. 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.
- **Asynchronous**. La réplication prenant et envoyant des instantanés, les données doivent être 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.
- **Includes metadata**. Le flux de réplication sous-jacent sérialise à la fois les données utilisateur et les métadonnées ZFS, y compris la plupart des propriétés configurées dans à 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 interrompue. Par exemple, cela autorise le partage via NFS à un autre ensemble d'hôtes que la source. Reportez-vous à la section Gestion des cibles de réplication pour des informations détaillées.
- **Secure**. Le protocole de contrôle de réplication utilisé dans les appareils ZFS Storage Appliance est sécurisé grâce à la technologie SSL. Les données peuvent éventuellement être protégées par cette dernière. Les appareils peuvent uniquement répliquer vers/à partir d'autres appareils après un processus d'authentification manuelle initial (voir Création et modification de cibles).

Concepts

Terminologie

- **pair de réplication** (ou simplement **pair** dans ce contexte) : appareil ZFS Storage Appliance configuré en tant que source ou cible de réplication.
- **source de réplication** (ou simplement **source**) : appareil pair contenant des données à répliquer sur un autre appareil pair (la *cible*). 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** (ou simplement **cible**) : appareil pair qui doit recevoir et stocker les données répliquées à partir d'un autre appareil pair (la *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.

- **groupe de réplication** (ou simplement **groupe**) : intégralité des ensembles de données (pour être précis, un projet et certains partages) répliqués en tant qu'unité. Reportez-vous à la section Niveau projet contre niveau partage.
- **action de réplication** (ou simplement **action**) : objet de configuration sur un appareil source indiquant un projet ou un partage, un appareil cible et des options de stratégie (y compris la fréquence d'envoi des mises à jour, le chiffrement simultané ou non, etc.).
- **package** : pendant d'une action côté cible, objet de configuration sur l'appareil cible qui gère les données répliquées dans le cadre d'une action donnée à partir d'une source spécifique. Chaque action effectuée sur un appareil source est associée à exactement un package sur un appareil cible et vice-versa. La perte d'un objet nécessite la création d'une nouvelle paire action/package (et une mise à jour de réplication complète).
- **synchronisation complète** (ou **mise à jour complète**) : opération de réplication qui envoie l'intégralité du contenu d'un projet et certains de ses partages.
- **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).

Cibles

Avant qu'un appareil source puisse effectuer une opération de réplication sur une cible, les deux systèmes doivent établir une connexion de pair de réplication qui permet aux appareils de s'identifier mutuellement de manière sécurisée lors des communications futures. Les administrateurs établissent cette connexion en créant une nouvelle cible de réplication sur l'écran Configuration > Services > Réplication distante de l'appareil source. Pour créer une nouvelle cible, les administrateurs doivent renseigner trois champs :

- Nom (uniquement pour identifier la cible dans la BUI et CLI de l'appareil source)
- Adresse réseau ou nom d'hôte (pour contacter l'appareil cible)
- Mot de passe root de l'appareil cible (pour autoriser l'administrateur à établir la connexion à l'appareil cible)

Ensuite, 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.

Par défaut, la connexion de la cible de réplication n'est pas bidirectionnelle. 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. Toutefois, le système prend charge l'inversion du

sens de la réplication, qui crée automatiquement une cible pour A sur B (si elle n'existe pas déjà) afin que B puisse à son tour effectuer une réplication vers A.

Pour configurer les cibles de réplication, reportez-vous à la section Configuration de la réplication.

Actions et packages

Les cibles représentent une connexion entre les appareils leur permettant de communiquer de manière sécurisée pour la réplication, mais les cibles n'indiquent pas le contenu répliqué, la fréquence et les options de réplication. Pour ce faire, les administrateurs doivent définir des *actions* de réplication sur l'appareil source. Les actions constituent le point de contrôle administratif principal pour la réplication, chacune d'entre elles indiquant les informations suivantes :

- Groupe de réplication (un projet et un certain nombre de partages)
- Appareil cible
- Pool de stockage sur l'appareil cible (utilisé uniquement pendant la configuration initiale)
- Fréquence (manuelle, programmée ou en continu)
- Options supplémentaires, comme le chiffrement du flux de données en simultané

Le groupe est implicitement spécifié par le projet ou le partage sur lequel l'action est configurée (voir la section Réplication de niveau projet et de niveau partage). 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. En général, 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.

Les actions constituent l'unité principale de la configuration de réplication sur l'appareil. Chaque action correspond à un *package* sur l'appareil cible qui 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 administrateurs configurent la fréquence et d'autres options pour les mises à jour de réplication en modifiant les propriétés de l'action correspondante. La création d'une action sur l'appareil source génère le package sur l'appareil cible dans le pool de stockage spécifié. La source doit donc être en mesure de contacter la cible lorsque l'action est créée.

La première mise à jour pour chaque action de réplication envoie une *synchronisation complète* (ou *mise à jour complète*) et l'intégralité du contenu du projet et partages de l'action sont envoyés à l'appareil cible. Au terme de cette synchronisation initiale, les mises à jour de réplication ultérieures sont *incrémentielles* et seules les modifications apportées depuis la mise à jour précédente sont envoyées. L'action (sur la source) et le package (sur la cible) effectuent un suivi des modifications répliquées sur la cible via les instantanés de réplication nommés. En général, tant qu'au moins une synchronisation complète a été envoyée pour une action et que la

connexion action/package n'a pas été endommagée en raison d'une panne logicielle ou d'une action administrative, les mises à jour de réplication sont incrémentielles.

L'action et le package 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). La BUI et la CLI avertissent les administrateurs qui tentent d'effectuer des opérations qui entraîneraient la suppression de la connexion action-package. Si une erreur ou une opération administrative interrompt la connexion si bien que des mises à jour incrémentielles ne sont plus possibles, les administrateurs doivent dissocier ou détruire le package et l'action, puis en créer une nouvelle sur la source.

REMARQUE : L'appareil ne supprime pas de 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, en créer de nouveaux puis redémarrer la réplication.

Dans les versions de logiciel antérieures à 2010.Q1, la configuration d'action et de réplication (comme la configuration cible) était stockée sur le contrôleur, et non en tant que composante de la configuration du projet et du partage sur le pool de stockage. Par conséquent, la réinitialisation des paramètres d'usine supprimait la configuration. Dans les versions 2010.Q1 et ultérieures, la configuration d'action et de package est stockée sur le pool de stockage avec les projets et partages correspondants. Elle est donc disponible même après la réinitialisation des paramètres d'usine. Toutefois, les informations de la cible seront perdues, et les actions aux cibles manquantes ne peuvent actuellement pas être configurées pour renvoyer vers une nouvelle cible.

Pools de stockage

Lors de la configuration initiale de l'action, 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 d'une action entraîne la création du package vide sur la cible dans le pool de stockage indiqué, et une fois cette opération effectuée, la source n'a pas connaissance de la configuration de stockage sur 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 clusterisé, le pool de stockage sélectionné **doit** appartenir au même propriétaire 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 (NFS et SMB), où le chemin et l'adresse IP requis dans une opération de montage doivent obéir 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.

Réplication de niveau projet et de niveau partage

L'appareil permet aux administrateurs de configurer la réplication distante de niveau projet ou de niveau du partage. 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 des 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, admettons que nous ayons les éléments suivants :

- Projet `home` et 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 suivants, chacun étant répliqué en tant que flux unique par action à l'aide d'instantanés pris simultanément sur le projet et les partages :

- Groupe de niveau projet incluant `home`, `home/bill` et `home/cindi`.
- Groupe de niveau partage comprenant `home` et `home/dave`.

Il est vivement recommandé d'éviter la réplication de niveau projet et de niveau partage au sein du même projet car elle pourrait produire des résultats étonnants (notamment en cas d'inversion du sens de la réplication). Consultez la documentation Gestion des packages de réplication pour des informations détaillées.

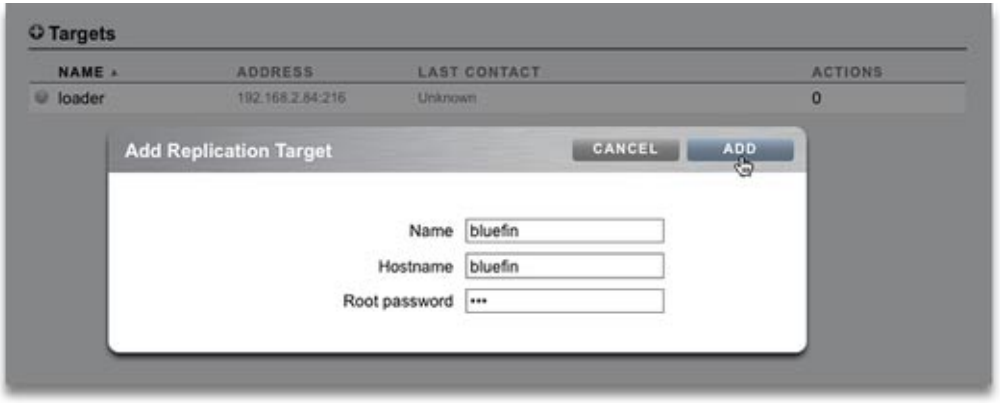
Configuration de la réplication

Avant de procéder à la configuration de la réplication, lisez attentivement les sections ci-dessus à propos des cibles de réplication, des actions et des packages et assurez-vous de comprendre.

Création et modification de cibles

Pour créer des cibles de réplication distante dans la BUI, accédez à Configuration > Services > Réplication distante > Cibles. Cliquez sur Cibles et configurez les paramètres **Nom**, **Nom d'hôte** et **Mot de passe**.

Pour modifier les cibles de réplication distante dans la BUI, accédez à Configuration > Services > Réplication distante > Cibles. Pour la cible que vous souhaitez modifier, déplacer le curseur sur le nom de la cible, cliquez sur l'icône de crayon, et configurez les paramètres **Nom** et/ou **Nom d'hôte**. Le nom d'hôte doit correspondre au même appareil qu'avant (vérifié par le numéro de série sur la cible). 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.



Dans la CLI, accédez au noeud `targets` pour définir ou annuler le paramétrage de la cible `hostname`, `root_password` et `label`.

```
knife:> configuration services replication targets
```

Dans ce contexte, les administrateurs peuvent :

- 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

La cible ne doit pas être supprimée tant que des actions les 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.

Création et modification d'actions

Après la configuration d'au moins une cible de réplication, les administrateurs peuvent configurer des actions, soit dans la BUI en accédant au projet ou au partage local et en cliquant sur l'onglet Réplication, soit dans la CLI en accédant au projet ou au partage local et en sélectionnant le noeud "replication". Ces interfaces affichent l'état des actions existantes configurées sur le projet ou le partage, ainsi que les informations sur l'avancement de la réplication, et permet aux administrateurs de créer de nouvelles actions :

Lors de la réplication d'une cible, deux rangées contenant des informations d'état sont affichées. La première rangée affiche le nom de la cible, la date et l'heure de la dernière synchronisation réussie, et une barre de progression, ou une barre de progression hachurée si la réplication est continue. La deuxième rangée affiche le type de réplication (programmé, manuel ou continu), la date et l'heure de la dernière tentative de synchronisation ou de la dernière synchronisation qui a échoué, et les détails de l'état. Pour les réplications en cours, les détails sur l'état contiennent le pourcentage effectué, la taille estimée des données à répliquer, le débit moyen de réplication, et l'heure de fin estimée. Lorsque la réplication n'est pas en cours, la colonne Statut affiche la prochaine réplication prévue, ou le message "Synchro maintenant", selon le type de réplication.

Les mêmes informations de progression peuvent être affichées dans la CLI, avec l'état `sending` affiché pour une réplication en cours :

```
otoro:shares otoro-proj-01 action-000> show
Properties:
                    id = 80a96f4f-93fe-4abd-eb54-fb82e7f8c69f
                target = chutoro
```

```
            continuous = false
         include_snaps = true
         max_bandwidth = unlimited
            bytes_sent = 505M
        estimated_size = 3.0G
  estimated_time_left = 00:00:41
   average_throughput = 63MB/s
               use_ssl = false
                 state = sending
    state_description = Sending update
          next_update = Sync now
            last_sync = Sun Jul 14 2013 06:04:38 GMT+0000 (UTC)
             last_try = Sun Jul 14 2013 06:04:38 GMT+0000 (UTC)
          last_result = success
```

Remarque : une réplication peut durer assez longtemps, selon la taille des données à répliquer. Utilisez les informations de progression pour déterminer l'état de la mise à jour. Pour une réplication initiale, il est important de ne pas l'interrompre, y compris (mais pas seulement) de redémarrer l'appareil ou d'annuler la mise à jour ; dans le cas contraire, l'ensemble de la réplication initiale devra être repris du début.

Les actions de réplication possèdent les propriétés suivantes, qui sont présentées légèrement différemment dans la BUI et la CLI.

Propriété (nom dans la CLI)	Description
Target	Identifiant unique du système cible de la réplication. Cette propriété est spécifiée si une action est initialement configurée et immuable par la suite.
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.
Mode (CLI: continuous) and schedule	Réplication de l'action en continu, manuelle ou à intervalles programmés. Reportez-vous à la section Modes : programmé ou continu pour plus de détails.
Include Snapshots	Indique si les mises à jour de réplication contiennent ou non des instantanés de non-réplication. Reportez-vous à la section Inclusion d'instantanés intermédiaires pour plus de détails.
Limit bandwidth	Spécifie une vitesse maximale pour cette mise à jour de réplication (en termes de quantités de données transférées chaque seconde sur le réseau).
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.
Utiliser 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.
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 seul 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), "manuel" ou "continu".

Modes : 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, un minimum de données sera perdu en cas de sinistre sur le système source.

La réplication en continu est toujours asynchrone. Les appareils ZFS Storage Appliance ne prennent actuellement pas en charge la réplication synchrone, qui ne considère pas les données affectées au stockage stable tant qu'elles ne le sont pas à la fois validées sur les systèmes de stockage principal et secondaire.

Inclure les instantanés 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.

Envoi et annulation de mises à jour

Pour les cibles configurées pour une réplication programmée ou manuelle, les administrateurs peuvent choisir d'envoyer immédiatement la mise à jour de réplication en cliquant sur le bouton dans la BUI ou en exécutant la commande `sendupdate` dans la CLI. Ce 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.

Si une mise à jour est active, la BUI affiche une barre de progression et la CLI affiche le statut `sendupdate`. Pour annuler la mise à jour, cliquez sur le bouton ou exécutez la commande `cancelupdate`. L'annulation peut nécessiter plusieurs secondes.

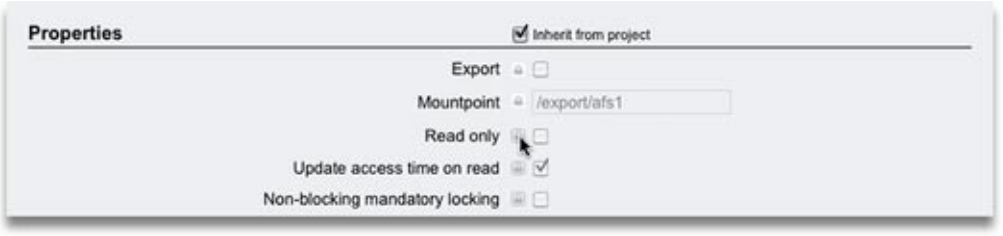
Gestion des packages de réplication

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, comme décrit ci-dessus. La BUI et la CLI permettent aux administrateurs de parcourir les projets, partages, instantanés et propriétés répliqués, de la même manière que pour les projets et partages locaux. Toutefois, étant donné que les partages répliqués doivent être identiques à leurs homologues sur l'appareil source, de nombreuses opérations de gestion ne sont pas autorisées au sein des packages de réplication. Il est notamment impossible de créer, renommer et supprimer des projets et des partages, de créer et renommer des instantanés et de modifier la plupart des propriétés des projets et des partages. Les instantanés autres que ceux utilisés comme base pour la réplication incrémentielle peuvent être supprimés des packages de réplication. Cette pratique n'est pas recommandée mais peut être utilisée lorsque de l'espace disque supplémentaire est nécessaire.

Dans les versions logicielles 2009.Q3 ou antérieures, les propriétés ne pouvaient pas être modifiées sur les partages répliqués. La version 2010.Q1 (avec les mises à niveau différées associées) ajoute une prise en charge limitée des modifications de propriétés des partages répliqués pour implémenter les différentes stratégies sur les appareils source et cible. Les modifications de propriété de ce type persistent après les mises à jour de réplication. Seules les propriétés suivantes des projets et partages répliqués peuvent être modifiés :

- **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 modifiés 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 le système 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.

La BUI et la CLI n'autorisent pas les administrateurs à modifier les propriétés immuables. Pour les partages, une icône différente indique que l'héritage de la propriété ne peut pas être modifié :

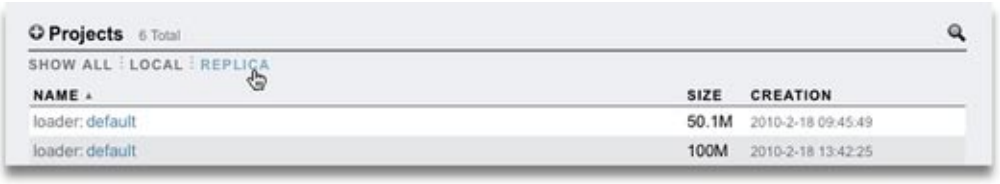


Les mises à jour différées fournies avec la version 2010.Q1 doivent être appliquées sur les cibles de réplication afin de modifier les propriétés sur ces cibles. Le système n'autorise pas les administrateurs à modifier les propriétés au sein des packages de réplication sur les systèmes qui n'ont pas appliqué les mises à jour différées de la version 2010.Q1.

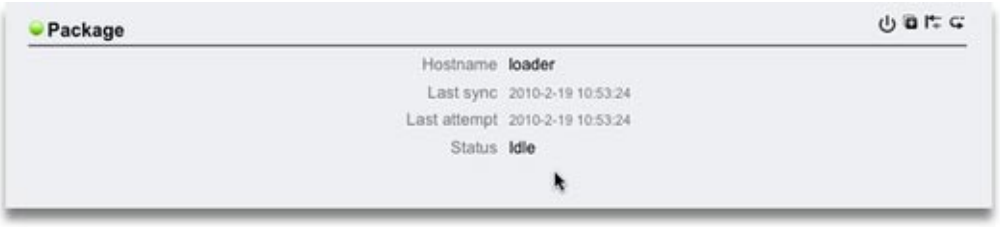
La version actuelle ne prend pas en charge la configuration de la réplication "en chaîne" (à savoir, répliquer des partages répliqués sur un autre appareil).

BUI

Les packages de réplication sont affichés dans la BUI en tant que projet sous le filtre "Réplique" :



Lorsque l'administrateur sélectionne un package de réplication pour le modifier, la vue Partages s'affiche pour le projet du package. A partir de là, les administrateurs peuvent gérer les partages répliqués de la même manière que les partages locaux, hormis les exceptions décrites ci-dessus. Les propriétés de package (y compris le statut) peuvent être modifiées dans l'onglet Réplication :



L'icône de statut située à gauche change lorsque la réplication échoue :

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 quelque instants après la fin de la première mise à jour.

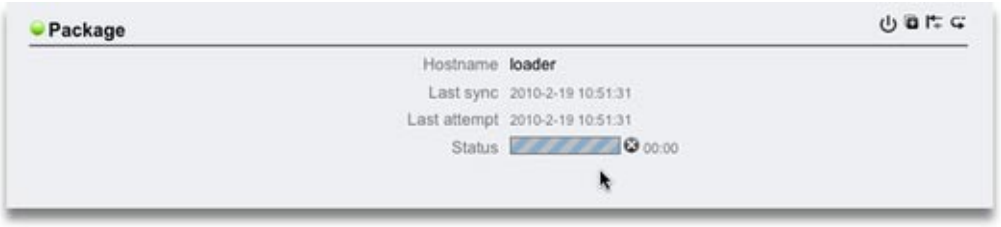
CLI

Les packages de réplication sont organisés par source dans la CLI sous `shares replication sources`. Les administrateurs sélectionnent la source, puis un package. Les opérations au niveau du package peuvent être effectuées sur ce noeud ou le projet peut être sélectionné pour gérer les partages et les propriétés de projet tout comme les projets et partages locaux, hormis les exceptions décrites ci-dessus. Par exemple :

```
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)

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
```

Annulation de mises à jour de réplication

Pour annuler une mise à jour de réplication sur une cible dans la BUI, accédez au package de réplication (voir ci-dessus), puis cliquez sur l'onglet Réplication. Si une mise à jour est en cours, vous verrez une barre de progression hachurée avec un bouton d'annulation (⊗) situé en regard, comme dans l'illustration suivante :



Cliquez sur ce bouton pour annuler la mise à jour.

Pour annuler des mises à jour en cours sur la cible dans la CLI, accédez au package de réplication (voir ci-dessus) et exécutez la commande `cancelupdate`.

Il n'est pas possible de lancer des mises à jour depuis la cible. Les administrateurs doivent se connecter au système source pour lancer une mise à jour manuelle.

Désactivation d'un package

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 la source.

Pour activer ou désactiver si un package dans la BUI, accédez à ce package (voir ci-dessus), puis cliquez sur l'onglet Réplication et enfin sur l'icône . L'icône de statut située à gauche change pour indiquer le statut du package (activé, désactivé ou en échec). Le package reste désactivé tant qu'il n'est pas activé par un administrateur à l'aide du même bouton ou dans la CLI.

Pour activer ou désactiver un package dans la CLI, accédez à ce package (voir ci-dessus), modifiez la propriété `enabled` et validez vos modifications.

Clonage d'un package ou de partages individuels

Un *clone* d'un package répliqué désigne un projet local et mutable qui peut être géré comme n'importe quel autre projet du système. Les partages du clone sont des clones des partages répliqués en fonction du dernier instantané reçu. Ces clones partagent le stockage avec leurs instantanés d'origine de la même manière que le font les clones des instantanés de partages (voir Clonage d'un instantané). 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.

Cliquez sur le bouton dans la BUI ou exécutez la commande `clone` dans la CLI (dans le contexte du package) pour créer un clone de package basé sur l'instantané de réplication le plus récent. Dans les interfaces CLI et BUI, l'administrateur doit indiquer un nom pour le nouveau projet clone et autoriser les administrateurs à remplacer le point de montage du projet ou de ses partages pour garantir qu'ils n'entrent pas en conflit avec ceux des autres partages présents sur le système.

Dans les versions 2009.Q3 et antérieures, le clonage d'un projet répliqué était la seule façon d'accéder à ses données et donc le seul moyen d'implémenter le basculement en cas de récupération après sinistre. Dans les versions 2010.Q1 et ultérieures, les systèmes de fichiers individuels peuvent être exportés en lecture seule sans créer de clone. En outre, les packages de réplication peuvent être convertis directement en projets locaux inscriptibles dans le cadre d'une opération de basculement. Par conséquent, cloner un package n'est plus nécessaire ou recommandé, car ces alternatives offrent les mêmes fonctionnalités avec des opérations plus simples et sans avoir à gérer des clones et leurs dépendances.

Lorsqu'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 instantané de ce type possède des clones, il est renommé avec un nom unique (généralement `recv-XXX`).

Les administrateurs peuvent également cloner des instantanés de partage répliqué dans les interfaces BUI et CLI classiques.

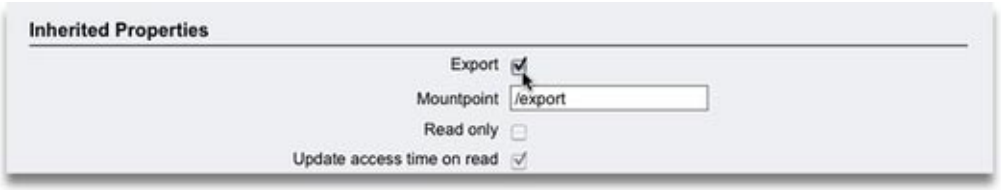
Exportation de systèmes de fichiers répliqués

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. Reportez-vous à la section Cohérence des instantanés et des données pour plus d'informations.

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 :



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, interrompre la réplication (ce qui convertit le package en projet local) entraîne l'exportation des partages du package.

Les LUN répliquées ne peuvent actuellement pas être exportées. Ils doivent d'abord être clonés ou le package de réplication doit être dissocié pour en exporter le contenu.

Interruption 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 interrompant 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 classique.

Pour interrompre la réplication dans la BUI, accédez au package de réplication (voir ci-dessus) et cliquez sur l'onglet Réplication puis sur le bouton . La boîte de dialogue qui s'affiche alors permet à l'administrateur d'indiquer le nom du nouveau projet local.

Pour inverser la réplication dans la CLI, accédez au package de réplication (voir ci-dessus) et exécutez la commande `sever`. Cette commande sélectionne un argument facultatif indiquant le nom du nouveau projet local. Si aucun argument n'est indiqué, le nom d'origine est utilisé.

Tous les partages locaux étant exportés, tous les partages d'un package sont exportés lorsque celui-ci est dissocié, qu'ils l'aient déjà été ou non (voir ci-dessus). S'il existe des conflits de point de montage entre les systèmes de fichiers répliqués et les autres systèmes de fichiers, l'opération de dissociation échoue. Il faut résoudre ces conflits avant l'inversion en reconfigurant les points de montage des partages concernés.

Inversion du sens de réplication

Il est possible d'inverser le sens de réplication pour prendre en charge les plans de récupération après sinistre classiques à deux systèmes. Cette opération est semblable à l'opération de dissociation décrite ci-dessus, mais configure en outre une action de réplication sur le nouveau projet local pour la réplication incrémentielle sur le système source. Aucune modification n'est apportée sur le système source au terme de cette opération. Toutefois, la première tentative de mise à jour utilisant cette action 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.

Cette fonction ne redirige pas automatiquement les charges de travail de production, ne basculent pas les adresses IP ou n'exécute pas d'autres activités liées au basculement en cas de récupération après sinistre en plus de modifier le statut lecture/écriture des copies de données principales et secondaires.

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. Une action de réplication subsiste au niveau du partage contenant le calendrier correct, avec la valeur "None" pour l'appareil cible.

Comme indiqué ci-dessus, cette fonction permet généralement d'implémenter une configuration de récupération après sinistre à deux systèmes dans laquelle un système *principal* se charge des données de production et les réplique vers un système *secondaire* ou *DR* (le plus souvent dans un autre centre de données) prêt à se charger du trafic de production dans le cas d'un sinistre sur le site principal. Dans le cas d'un sinistre sur le site principal, la copie du site secondaire doit être configurée comme "primary" en lui conférant la propriété inscriptible et en redirigeant le trafic de production vers le site secondaire. Lorsque le site principal sera réparé, les modifications qui se seront succédé sur le site secondaire pourront être répliquées vers le site principal et ce dernier pourra reprendre la charge de travail de production.

Une séquence d'événements classique dans un plan de ce type se déroule comme suit :

- Le système principal assume la charge de travail de production et assure la réplication vers le système secondaire.

- Un sinistre se produit, avec pour conséquence possible une panne totale du système sur le site principal. Les administrateurs inversent le sens de la réplication sur le site secondaire, en exportant les partages répliqués dans un nouveau projet configuré pour la réplication vers le site principal lorsque ce dernier est restauré. Entre-temps, la charge de travail de production est redirigée vers le site secondaire.
- Lorsque le site principal est à nouveau en ligne, un administrateur lance une mise à jour de réplication depuis le site secondaire vers le site principal. Cette opération convertit la copie de site principal dans un package de réplication, annulant toute modification effectuée depuis la dernière mise à jour réussie sur la cible (avant la panne). Une fois la copie du site principal à jour, le sens de la réplication est à nouveau inversé par l'administrateur, rendant la copie inscriptible sur le site principal. Le trafic de production est redirigé vers le site principal. La réplication reprend à partir du site principal vers le site secondaire, restaurant ainsi la relation initiale entre les copies principale et secondaire.

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).

Pour inverser la réplication dans la BUI, accédez au package de réplication (voir ci-dessus) et cliquez sur l'onglet Réplication puis sur le bouton . La boîte de dialogue qui s'affiche alors permet à l'administrateur d'indiquer le nom du nouveau projet local.

Pour inverser la réplication dans la CLI, accédez au package de réplication (voir ci-dessus) et exécutez la commande `reverse`. Cette commande sélectionne un argument facultatif indiquant le nom du nouveau projet local. Si aucun argument n'est indiqué, le nom d'origine est utilisé.

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 (voir ci-dessus). 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 DR.`**

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.

Tâches

Les tâches suivantes sont des exemples de procédures de réplication.

Replication Tâches

Inversion de la réplication - Etablir une réplication

Ci-dessous figure un exemple d'inversion de la réplication pour prendre en charge une récupération après sinistre classique à deux systèmes. Dans cet exemple, M11 est le système de production et M5 le système de récupération.

1. Sur le système de production M11, accédez à Configuration > SERVICES.
2. Sur la ligne SMB sous Services de données, si l'état est sur Désactivé, cliquez sur **Activer le service**.
3. Accédez à Configuration > SERVICES > Réplication distante.
4. Cliquez sur Cibles et configurez les paramètres de nom, de nom d'hôte et de mot de passe. Nom=M5, Nom d'hôte=192.168.1.17, Mot de passe root=pppp$1234
5. Sélectionnez **Pool=Pool1**.
6. Accédez à Partages > PROJETS.
7. Cliquez sur **Projets**. Nom=P1
8. Accédez à Partages > PROJETS > P1 > Protocoles.
9. Dans la section SMB, définissez Nom de la ressource=on.
10. Accédez à Partages > PROJETS > P1 > Partages.
11. Cliquez sur **Systèmes de fichiers**. Nom=S1, Utilisateur=root, Groupe=autre, Autorisations=RWX RWX RWX
12. Accédez à Partages > PROJETS > P1 > Partages > S1 > Protocoles. La section SMB indique que S1 est accessible via SMB à l'adresse \\192.168.1.7\S1.
13. Accédez à Partages > PROJETS > P1 > Réplication.
14. Cliquez sur **Actions** et définissez la cible et le pool. Cible=M5, Pool=Pool1
15. Cliquez sur **Calendrier** et définissez la fréquence. Fréquence=Demi-heure à 00 minutes après l'heure.
16. Sur le système client SMB, **Map network drive** \\192.168.1.7\S1 (user=root, password=pppp$1234).

17. Créez le fichier F1.txt.
18. Sur le système de production M11, accédez à Partages > PROJETS > P1 > Réplication.
19. Sur la ligne Action TARGET=M5, cliquez sur **Mettre à jour maintenant**.
20. Une fois que la réplication est terminée, cliquez sur **Désactiver**. STATUT passe alors sur désactivé.

Inversion de la réplication - Simuler la récupération suite à un sinistre

Pour simuler une récupération suite à un sinistre qui empêche l'accès au système de production, utilisez le système de récupération pour inverser la réplication. Lorsque la réplication est inversée, le package de réplication présent sur la cible est converti en projet local. De plus, une action de réplication est configurée pour ce projet local en vue d'une réplication incrémentielle sur le système source d'origine. Cette action de réplication n'est pas activée par défaut. L'administrateur doit envoyer manuellement la mise à jour.

1. Pour simuler une perte de contact avec le système principal M11 sur le système client SMB, sélectionnez **Déconnecter le lecteur réseau**.
2. Sur le système de récupération après sinistre M5, sélectionnez **Pool=Pool1**.
3. Accédez à Partages > PROJETS > REPLIQUE. Le projet M11:P1 est répertorié.
4. Accédez à Partages > PROJETS > REPLIQUE> M11:P1 > Réplication. Le statut du package est Statut=Inactif
5. Cliquez sur **Inverser le sens de réplication** et définissez le nouveau nom de projet. Nom du nouveau projet=P1
6. Accédez à Partages > PROJETS > REPLIQUE. Le projet M11:P1 n'est plus répertorié car le package de réplication présent sur la cible est converti en projet local.
7. Accédez à Configuration > SERVICES.
8. Sur la ligne SMB sous Services de données, si l'état est sur Désactivé, cliquez sur **Activer le service**.
9. Accédez à Partages > PROJETS > LOCAL. Le projet P1 est répertorié.
10. Accédez à Partages > PROJETS > P1 > Protocoles.
11. Dans la section SMB, définissez Nom de la ressource=on.
12. Accédez à Partages > PROJETS > P1 > Partages > S1 > Protocoles. La section SMB indique que S1 est accessible via SMB à l'adresse \\192.168.1.17\S1.
13. Sur le système client SMB, **Map network drive** \\192.168.1.17\S1 (user=root, password=pppp$1234).
14. Modifiez le fichier F1.txt et enregistrez-le sous F2.txt. **REMARQUE :** Lors d'une vraie séquence de récupération suite à un sinistre, une fois que les communications avec le système de production M11 sont rétablies, vous pouvez déclencher des mises à jour de réplication manuelle, planifiée ou continue pendant que les applications continuent d'accéder aux données sur le système de récupération après sinistre M5.

15. Pour préparer la transition vers le système de production, utilisez la fonction **Déconnecter le lecteur réseau**.
16. Sur le système de récupération après sinistre M5, accédez à Partages > PROJETS > P1 > Réplication.
17. Sur la ligne Action TARGET=M11, cliquez sur **Mettre à jour maintenant**.
18. Une fois la réplication terminée, cliquez sur **Désactiver**.

Inversion de la réplication - Reprendre une réplication depuis un système de production

Chaque fois que la réplication est inversée, vous indiquez un nouveau nom de projet qui est utilisé lorsque le package de réplication est converti dans un nouveau projet local. Si vous souhaitez utiliser le même nom et qu'une inversion de réplication antérieure a laissé un projet vide avec ce nom, vous devez supprimer le projet vide existant pour permettre à la prochaine inversion de créer un projet avec le même nom.

1. Sur le système de production M11, accédez à Partages > PROJETS > LOCAL > P1. P1 est vide car la première mise à jour à l'aide du nouveau système source (la cible originale) convertit le projet d'origine sur le système source d'origine en package de réplication. Cet exemple utilise une action de réplication de niveau projet qui réplique tous les partages dans le projet. De ce fait, tous les partages présents dans ce projet local sont désormais présents dans le package de réplication, ce qui laisse le projet local vide.
2. Accédez à Partages > PROJETS > REPLIQUE > M5:P1 > Réplication. Le statut du package est Statut=Inactif.
3. Accédez à Partages > PROJETS > LOCAL.
4. Supprimez P1. Il n'y a aucun risque à supprimer un projet vide car son contenu est déplacé dans le package de réplication dans le cadre de la réplication inversée depuis la cible d'origine.
5. Accédez à Partages > PROJETS > REPLIQUE > M5:P1 > Réplication.
6. Cliquez sur **Inverser le sens de réplication** et définissez le nom du projet. Nom du nouveau projet=P1
7. Sur le système client SMB, **Map network drive** \\192.168.1.7\S1 (user=root, password=pppp$1234). Les fichiers F1.txt et F2.txt sont répertoriés.
8. Sur le système de production M11, accédez à Partages > PROJETS > P1 > Réplication.
9. Sur la ligne Action TARGET=M5, cliquez sur **Modifier l'entrée**.
10. Cliquez sur **Calendrier** et définissez la fréquence. Fréquence=Demi-heure à 00 minutes après l'heure.
11. Sur la ligne Action TARGET=M5, cliquez sur **Mettre à jour maintenant**. Cela permet au système de récupération après sinistre M5 de reconvertir son projet local P1 en package de réplication M11:P1.

12. Surveillez la colonne MISES A JOUR sur la ligne d'action TARGET=M5 et attendez la fin de la mise à jour de réplication.
13. Sur le système de récupération après sinistre M5, accédez à Partages > PROJETS > LOCAL > P1. P1 est vide car le projet a été reconverti en package de réplication.
14. Accédez à Partages > PROJETS > LOCAL.
15. Pour permettre à la prochaine inversion de convertir le package de réplication en projet nommé P1, supprimez P1.

Clonage d'un projet de réplication reçu

Ci-dessous figure un exemple CLI de clonage d'un projet de réplication, qui remplace à la fois le point de montage du projet et celui d'un partage :

```
perch:> shares
perch:shares> replication
perch:shares replication> sources
perch:shares replication sources> select source-000
perch:shares replication source-000> select package-000
perch:shares replication source-000 package-000> clone
perch:shares replication source-000 package-000 clone> set target_project=my_clone
                target_project = my_clone
perch:shares replication source-000 package-000 clone> list
CLONE PARAMETERS
                target_project = my_clone
           original_mountpoint = /export
           override_mountpoint = false
                    mountpoint =

    SHARE                          MOUNTPOINT
    bob                            (inherited)
    myfs1                          (inherited)
perch:shares replication source-000 package-000 clone> set override_mountpoint=true
           override_mountpoint = true
perch:shares replication source-000 package-000 clone> set mountpoint=/export/my_clone
                    mountpoint = /export/my_clone
perch:shares replication source-000 package-000 clone> select bob
perch:shares replication source-000 package-000 clone bob> set override_mountpoint=true
           override_mountpoint = true
perch:shares replication source-000 package-000 clone bob> set mountpoint=/export/bob
                    mountpoint = /export/bob
perch:shares replication source-000 package-000 clone bob> done
perch:shares replication source-000 package-000 clone> commit
CLONE PARAMETERS
                target_project = my_clone
           original_mountpoint = /export
           override_mountpoint = true
                    mountpoint = /export/my_clone

    SHARE                          MOUNTPOINT
    bob                            /export/bob (overridden)
    myfs1                          (inherited)
Are you sure you want to clone this project?
There are no conflicts.
perch:shares replication source-000 package-000 clone>
```

Détails de la réplication distante

Autorisations

Outre le filtre Réplication distante sous la portée Services qui permet aux administrateurs d'arrêter, de démarrer et de redémarrer le service de réplication, le sous-système de réplication fournit deux autorisations sous la portée "Projets et partages" :

Autorisation	Détails
rrsource	Autorise les administrateurs à créer, modifier et supprimer des cibles et actions de réplication, et à envoyer et annuler des mises à jour pour des 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 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. Consultez la documentation sur les autorisations pour de l'aide sur ce sujet.

Alertes

Le système publie 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 (voir ci-dessus).
- 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.

Evénements d'audit de réplication

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, interruption ou destruction de packages de réplication sur la cible
- Création, modification ou destruction de cibles de réplication

Réplication et clustering

La réplication peut être configurée à partir de n'importe quel appareil ZFS Storage Appliance sur n'importe quel autre appareil ZFS Storage Appliance, 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, à l'exception des contraintes suivantes :

- La configuration de la réplication à partir des deux pairs d'un cluster vers la même cible de réplication n'est pas prise en charge, mais une configuration similaire peut être obtenue en utilisant deux adresses IP différentes pour le même appareil cible. Les administrateurs peuvent utiliser les adresses IP multiples de l'appareil cible pour créer une seule cible de réplication sur chaque tête de cluster en vue de son utilisation par cette tête.
- Lors de la configuration de la réplication entre les pairs de cluster, configurez la réplication en définissant les deux contrôleurs sur CLUSTERED. N'utilisez pas d'adresses de réseau privé et distinguez les cibles de réplication pour chaque pool de contrôleur.

Les règles suivantes régissent le comportement de la réplication dans les configurations clusterisées :

- 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 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 la tête 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 à la même tête 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.

Pour des détails sur le clustering et la terminologie relative aux clusters, consultez la documentation sur le clustering.

Cohérence des instantanés et des données

L'appareil réplique les instantanés et la cible reçoit atomiquement chaque instantané. Ainsi, le contenu de la réplique d'un partage sur la cible correspond toujours au contenu du partage sur la source au moment où l'instantané a été pris. Les instantanés pour tous les partages envoyés dans un groupe spécifique étant effectués au même moment (voir ci-dessus), 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 (lorsque la mise à jour de réplication a commencé).

Toutefois, les instantanés de chaque partage étant répliqués séparément (et en série), il est possible que certains partages au sein d'un package aient été mis à jour avec un instantané plus récent que ceux reçus d'autres partages dans le même package. Cela est vrai au cours d'une mise à jour de réplication (après que certains partages ont été mis à jour, mais avant certains autres) et après l'échec d'une mise à jour de réplication (après laquelle certains partages peuvent ne pas avoir été mis à jour, contrairement à certains autres).

En résumé :

- Chaque partage est toujours cohérent au moment précis de la création de l'instantané (cohérence).
- 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 (cohérence de package).
- 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.

Gestion des instantanés

Les instantanés constituent la base de la réplication incrémentielle. 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 instantané 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 de deux facteurs : si nous avons déjà tenté de répliquer cette action et si la cible possède 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).

Cela a plusieurs conséquences sur 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 court 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 comprennent la gestion de l'espace sur l'appareil, notamment son application aux instantanés.

Réplication d'une configuration iSCSI

Comme décrit ci-dessus, 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 répliquées. 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. Les groupes doivent porter un nom identique, mais leur configuration peut être différente. Dans le cas contraire, la conséquence peut être une impossibilité de cloner et d'exporter les LUN répliquées.

Le GUID SCSI associé à une LUN est répliqué avec la 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 répliquées auront différents GUID (tout comme les clones des LUN locales possèdent des GUID différents de celles d'origine).

Réplication de clones

Dans la version 2009.Q3 et antérieures, la réplication était effectuée au niveau du projet uniquement et interdisait expressément la réplication de projets contenant des clones dont les instantanés d'origine étaient hébergés en dehors du projet. Avec la réplication de niveau partage des versions 2010.Q1 et ultérieures, cette restriction a été assouplie, mais les administrateurs doivent tout de même prendre en compte les instantanés originaux des clones étant répliqués. **La réplication initiale d'un clone requiert notamment que l'instantané d'origine ait déjà été répliqué sur la cible ou qu'il soit répliqué dans le cadre de la même mise à jour.** Cette restriction n'est pas appliquée par le logiciel de gestion de l'appareil, mais la tentative de réplication d'un clone échoue si l'instantané d'origine n'existe pas sur la cible.

Concrètement, il existe plusieurs moyens d'assurer la réussite d'une réplication de clone :

- Si l'instantané d'origine du clone se trouve dans le même projet, utilisez simplement la réplication de niveau projet.
- Si l'instantané d'origine du clone n'est pas dans le même projet ou si la réplication de niveau projet comprenant l'origine n'est pas souhaitable pour une raison quelconque, mettez en oeuvre la réplication de niveau partage pour répliquer le partage d'origine dans un premier temps, puis utilisez la réplication de niveau projet ou partage pour répliquer le clone.
- Ne détruisez pas l'original du clone sur le système cible à moins de vouloir également supprimer le clone lui-même.

Dans tous les cas, la propriété "inclure les instantanés" doit être définie sur true sur l'action de l'origine afin d'assurer que l'instantané d'origine est effectivement envoyé à la cible.

Observation de la réplication

Les analyses suivantes sont disponibles pour la réplication :

- Déplacement de données :opérations de réplication
- Déplacement de données : octets de réplication
- Les analyses avancées sont également disponibles.

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'échec suivants sont les plus courants :

Echec	Détails
Annnulée	La mise à jour de réplication a été annulée par un administrateur. La réplication peut être annulée sur la source ou la cible et il est possible qu'un pair ne se rende pas compte que l'autre pair a annulé l'opération.
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.
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. Pour plus détails, reportez-vous à la section Mise à jour à partir de 2009.Q3 et version antérieure.
Aucun package	La réplication a échoué car aucun package n'existe sur la cible pour accueillir les données répliquées. Etant 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.

Echec	Détails
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 et de leurs éventuelles implications pour la réplication distante.
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. Reportez-vous à la section "Cohérence des instantanés et des données" ci-dessus pour plus d'informations.

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 ou la mise à jour qui a échoué a commencé.

Lorsque des mises à jour programmées ou manuelles échouent, le système ne procède pas automatiquement à une nouvelle tentative avant l'exécution de la mise à jour programmée suivante (s'il y en a une). Lorsque la réplication en continu échoue, le système attend plusieurs minutes puis effectue une nouvelle tentative. Le système continue a réessayer indéfiniment les réplications en continu.

Lorsqu'une mise à jour de réplication est en cours et qu'une autre est programmée, cette dernière est complètement ignorée, et non lancée immédiatement après la mise à jour précédente. La mise à jour suivante est envoyée uniquement lorsque la suivante est programmée. Le système publie une alerte lorsqu'une mise à jour est ignorée pour cette raison.

Compatibilité de réplication

Afin d'effectuer une mise à jour de réplication, le service de réplication vérifie que le système cible est compatible avec les nouvelles données de la source.

- Si des fonctionnalités utilisées sur la source ne sont pas compatible avec la cible et que ces fonctionnalités peuvent être désactivées en toute sécurité, le service de réplication désactive les fonctionnalités, effectue la mise à jour et publie un avertissement.

- Si des fonctionnalités utilisées sur la source ne sont pas compatible avec la cible et que ces fonctionnalités ne peuvent pas être désactivées, le service de réplication n'effectue pas la mise à jour et publie une erreur.

REMARQUE : il est toujours recommandé de mettre à jour la cible dès que possible.

Les mises à jour qui rompent la compatibilité de réplication sont fournies en tant que Mises à jour différées. Pour la liste et la description actuelle, reportez-vous à la section Mises à jour différées et aux notes de version de l'appareil Oracle ZFS Storage Appliance de votre version actuelle.

Mise à niveau à partir des versions 2009.Q3 et antérieures

L'implémentation de réplication a beaucoup changé entre les versions 2009.Q3 et 2010.Q1. **Il reste vivement recommandé de suspendre la réplication vers et depuis un appareil avant de lancer une mise à niveau depuis une version 2009.Q3 ou antérieure. Cela est obligatoire dans tous les clusters utilisant la mise à niveau non simultanée.**

Trois modifications importantes sont visibles par l'utilisateur et liées à la mise à niveau vers une version 2010.Q1 ou ultérieure :

- Le protocole réseau utilisé pour la réplication a été amélioré. Les systèmes 2009.Q3 peuvent effectuer des opérations de réplication sur des systèmes exécutant n'importe quelle version (y compris 2010.Q1 et ultérieures). En revanche, les systèmes exécutant une version 2010.Q1 ou ultérieure peuvent uniquement effectuer des opérations de réplication sur cette même version. En pratique, cela signifie que les cibles doivent être mises à niveau avant ou en même temps que leurs sources de réplication pour éviter toute erreur résultant de versions de protocole incompatibles.
- La configuration de l'action de réplication est maintenant enregistrée dans le pool de stockage lui-même, et non dans le système principal. Par conséquent, après une mise à niveau depuis une version 2009.Q3 ou antérieure vers une version 2010.Q1, les administrateurs doivent appliquer les mises à jour différées pour migrer leur configuration de réplication.
- * Jusqu'à ce que les mises à jour soient appliquées, les mises à jour de réplication entrantes pour les répliques existantes échoueront, et les mises à jour de réplication ne seront pas envoyées pour les actions configurées dans les versions 2009.Q3 ou antérieures. De plus, les répliques non migrées qui ne peuvent pas être gérées dans la BUI ou la CLI utiliseront de l'espace sur le pool de stockage.
- * Une fois que ces mises à jour sont appliquées, comme avec toutes les mises à jour différées, l'annulation du logiciel du système produit des résultats indéfinis. Dans l'ancienne version, il faut s'attendre à ce que les données répliquées soient inaccessibles, à ce que la configuration de toutes les actions de réplication soit annulée et que toutes les mises à jour de réplication entrantes soient des mises à jour complètes.

- Les autorisations ont été déplacées de leur champ d'application vers la portée Projets et partages. Toutes les autorisations de réplication configurées dans les versions 2009.Q3 ou antérieures n'existeront plus dans les versions 2010.Q1. Les administrateurs utilisant un contrôle d'accès plus fin pour la réplication doivent déléguer les nouvelles autorisations de réplication aux administrateurs appropriés une fois la mise à niveau effectuée.

Schema

Propriétés personnalisées des partages

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.

BUI

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 possède les champs suivants :

Champ	Description
NOM	Nom de cette propriété dans la CLI. Il doit contenir uniquement des caractères alphanumériques ou les caractères ".:_\".
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.

Type BUI	Type CLI	Description
Chaîne	Chaîne	Données de chaîne arbitraires. Cela équivaut à l'absence de validation.
Integer	Integer	Entier positif ou négatif

Type BUI	Type CLI	Description
Positive Integer	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 Général, 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.

CLI

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
```

Tâches

Création d'une propriété pour effectuer le suivi des coordonnées

Schema Tâches

Dans la BUI

1. Accédez à l'affichage "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 le bouton "Appliquer"
7. Accédez à un partage ou à un projet existant.
8. Modifiez la propriété "Contact propriétaire" sous la section "Propriétés personnalisées".

Dans la 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="Contact propriétaire"`)
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"

◆ ◆ ◆ CHAPITRE 6

Intégration

Integration

Intégration

Les appareils Sun ZFS Storage Appliance mettent à disposition 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, suivez les règles de bonne pratique détaillées dans les **livres blancs et descriptifs de procédures** accessibles sur la page de documentation Sun Unified Storage Documentation. L'article suivant présente par exemple la procédure à suivre pour obtenir des résultats optimaux à partir de protocoles standard pour une application particulière.

- DMP/Storage Foundation de Symantec

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.

- Sun ZFS Storage Appliance Plug-in for Oracle Solaris Cluster Geographic Edition
- Plug-in ZFS Storage Appliance Network File System Plug In for Oracle Solaris Cluster
- Sun ZFS Storage Appliance Provider For Volume Shadow Copy Service Software
- Sun Storage 7000 Management Plug-In for Oracle Enterprise Manager Grid Controller
- Oracle Virtual Machine Storage Connect Plug-in pour l'appareil Sun ZFS Storage
- Sun ZFS Storage 7000 Storage Replication Adapter for VMware Site Recovery Manager
- Oracle Intelligent Storage Protocol

Votre appareil est conçu pour s'intégrer parfaitement avec les autres produits Oracle. La section suivante décrit par exemple la procédure de configuration de l'appareil Sun ZFS Storage Appliance en tant que cible de sauvegarde pour Oracle Exadata Database Machine.

- Sauvegarde Oracle Exadata Database Machine avec l'appareil Sun ZFS Storage Appliance

Pour plus d'informations, consultez la page Sun Unified Storage Documentation.

Symantec

Prise en charge FC avec 'DMP' / Storage Foundation de Symantec

- 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

Prise en charge FC pour Symantec Storage Foundation 5.1RP2 et ultérieur pour les versions de systèmes d'exploitation suivantes

- Solaris 10 SPARC
- Solaris 10 x86
- Linux RedHat5
- Oracle Enterprise Linux (OEL)

Reportez-vous à la liste de compatibilité matérielle (HCL) de Symantec disponible à l'adresse http://www.symantec.com/business/support/index (`http://www.symantec.com/business/support/index`)?page=content&id=TECH74012

Notez les restrictions suivantes :

- Les bibliothèques ASL pour 7000 "imposées" par Symantec doivent être installées ; elles 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
- De plus, Symantec requiert la configuration des paramètres DMP suivante (uniquement pour les 7000 'en cluster') :
- `:dmp_health_time=0`

- `:dmp_path_age=0`
- `:dmp_lun_retry_timeout=200`

Reportez-vous à la note technique HW de Symantec qui fait référence aux paramètres de 7000 'en cluster' à l'adresse : http://www.symantec.com/business/support/index (`http://www.symantec.com/business/support/index`)?page=content&id=TECH47728

Symantec Storage Foundation 5.1SP2 for Windows prend en charge les connexions FC aux séries 7000 pour les versions suivantes de Windows :

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2

Reportez-vous à la liste de compatibilité matérielle (HCL) SF 5.1SP2 HCL à l'adresse http://www.symantec.com/business/support/index (`http://www.symantec.com/business/support/index`)?page=content&id=TECH138719

Oracle Solaris Cluster

Plug-in ZFS Storage Appliance Network File System Plug In for 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 Sun ZFS Storage par le biais du protocole NFS. Le plug-in et le fichier README sont inclus dans le package du plug-in Sun ZFS Storage Appliance Network File System Plugin for Oracle Solaris Cluster, disponible à l'adresse Oracle Technology Network.

Oracle Solaris CGeo

Sun ZFS Storage 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 éloignés à l'aide du service de réplication distante de l'appareil Sun ZFS Storage.

Le package de plug-in est disponible à la page d'information Sun NAS Storage Oracle Technology Network.

Microsoft

Sun ZFS Storage Appliance 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 continuent 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). VSS fournit plus précisément :

- 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*

Sun ZFS Storage Appliance Provider For Volume Shadow Copy Service Software est un fournisseur matériel VSS qui permet à l'appareil Sun 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.

Sun 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 Sun ZFS Storage 7000 Software Providers and Plug-Ins disponible sur Oracle Technology Network]. Plus d'informations sur VSS disponibles sur le site Web de Microsoft, y compris cette [http://msdn.microsoft.com/en-us/library/aa384649 (http://msdn.microsoft.com/en-us/library/aa384649)%28VS.85%29.aspx présentation.

Oracle Grid Controller

Sun ZFS Storage Management Plug-In for Oracle Enterprise Manager Grid Control

Sun ZFS Storage plug-in for Oracle Enterprise Manager Grid Control offre à l'environnement de Grid Control un contrôle de premier plan de la famille d'appareils Sun ZFS Storage Appliance, avec notamment la possibilité de :

- Surveiller les appareils Sun 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 en suivant ce lien : Oracle Technology Network

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 de navigateur.

Oracle Grid Controller Sun ZFS Storage Management Plug-In for Oracle Enterprise Manager Grid Control

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 :

- Un rôle *oracle_agent* disposant d'un accès limité au système est créé, pour permettre à l'agent Oracle Enterprise Manager Grid Control d'obtenir les informations requises pour la surveillance sans altérer le système. Un utilisateur *oracle_agent* est créé et le rôle correspondant lui est affecté. L'utilisation de ce rôle et de cet utilisateur est cruciale pour conserver des enregistrements d'audit propres consignant 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 Sun ZFS Storage.
- La feuille de travail *Oracle Enterprise Manager* est créée et facilite la communication entre l'administrateur Grid Control et l'administrateur de stockage. Toutes les mesures surveillées par Grid Control sont disponibles depuis cette feuille de travail.

Annuler 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.

Oracle Storage Connect

Oracle Virtual Machine Storage Connect Plug-in for the Sun ZFS Storage Appliance

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 Sun 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(s) serveur(s) Oracle VM et communique avec le(s) serveur(s) de stockage par le biais de workflows installés sur le ZFSSA.

Le plug-in et le fichier README sont disponibles à l'adresse Oracle Technology Network.

VMware Site Recovery Manager

Sun ZFS Storage 7000 Storage Replication Adapter for VMware Site Recovery Manager

Sun ZFS Storage 7000 Storage Replication Adapter (SRA) for VMware vCenter Site Recovery Manager (SRM) intègre les appareils Sun ZFS Storage 7000 dans les déploiements VMware qui s'étendent sur plusieurs sites et nécessitent une récupération rapide en cas d'interruption de service de site protégé. SRA se connecte aux environnements VMware vCenter SRM existants et permet aux appareils Sun ZFS Storage 7000 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 Sun ZFS Storage 7000 responsable de l'appareil qui héberge les magasins de données VMware. Pour plus d'informations, reportez-vous au manuel Sun ZFS Storage 7000 SRA for VMware SRM Administration Guide fourni avec SRA.

Remarque : vous pouvez télécharger SRA depuis Oracle Technology Network. Un contrat de support valide pour l'appareil Sun ZFS Storage 7000 est requis pour obtenir SRA.

Exadata

Oracle Exadata Database Machine

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 Exadata. L'utilitaire de configuration de sauvegarde Oracle Exadata est conçu pour être déployé 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 manuelle de la sauvegarde Exadata
- Configuration d'Oracle Exadata pour la restauration Sun ZFS Storage

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 l'appareil Sun ZFS Storage comme cible de sauvegarde pour Oracle Exadata, reportez-vous au livre blanc **`Protecting Oracle Exadata with the Sun ZFS Storage Appliance: Configuration Best Practices`** sur la page de documentation de Sun Unified Storage. Un cluster Sun ZFS Storage 7420 est également disponible, fourni pré-monté en rack en tant qu'appareil de sauvegarde Sun ZFS pour minimiser la complexité de l'installation. La procédure d'intégration de cet appareil avec Oracle Exadata est identique au processus décrit ci-dessus.

Oracle Intelligent Storage Protocol

Protocole OISP (Oracle Intelligent Storage Protocol)

Oracle Database possède une architecture en couches qui inclut Oracle Disk Manager (ODM). ODM fournit un module de gestion des fichiers qui permet à Oracle Database d'utiliser un système de fichiers local, une partition de disque brute ou le serveur NFS pour stocker les informations de base de données.

Pour améliorer les performances de la base de données, l'interface ODM permet à Oracle Database de transmettre les informations avec chaque demande d'E/S. Ces informations définissent plusieurs attributs associés aux E/S, comme le type de fichiers associé à la demande d'E/S. Cela permet de gérer différemment les écritures de fichiers journaux de base de données et de fichiers de données.

Le nouveau protocole OISP permet au client Oracle Database NFSv4 de transmettre les informations d'optimisation ODM au serveur NFSv4 de l'appareil ZFS Storage. L'appareil ZFS Storage profite des informations d'optimisation ODM pour simplifier la configuration et améliorer davantage les performances de la base de données.

Il existe deux fonctions OISP (Oracle Intelligent Storage Protocol) :

- Paramétrage automatique de la taille optimale d'enregistrement des nouveaux fichiers de base de données.
- Utilisation automatique du décalage d'écriture optimal (Latence ZFS ou Débit) pour chaque demande d'écriture.

Paramétrage de la taille optimale d'enregistrement de fichier

Le client NFS transmet la taille optimale d'enregistrement à l'appareil ZFS Storage pour chaque demande d'écriture NFSv4. Le serveur NFSv4 de l'appareil ZFS Storage transmet la taille d'enregistrement au système de fichiers ZFS avec la demande d'E/S. Le système de fichiers ZFS contourne la taille d'enregistrement du système de fichiers par défaut et utilise la valeur de taille d'enregistrement transmise avec la demande d'E/S. 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.

Utilisez le mode d'écriture Latence ZFS ou Débit pour chaque demande

Le client NFS transmet le décalage d'écriture optimal à l'appareil ZFS Storage pour chaque demande d'écriture NFSv4. Le serveur NFSv4 de l'appareil ZFS Storage transmet le décalage d'écriture au système de fichiers ZFS avec la demande d'E/S. Le système de fichiers ZFS contourne le décalage d'écriture du système de fichiers par défaut et utilise la valeur de décalage d'écriture transmise avec la demande d'E/S. Selon l'état du système de fichiers ZFS, il est possible que le décalage d'écriture envoyé avec la demande d'E/S soit ignoré.

Glossaire

7120	Sun ZFS Storage 7120
7320	Sun ZFS Storage 7320
7420	Sun ZFS Storage 7420
Active Directory	serveur Active Directory de Microsoft
Alertes	événements de journal, de messagerie électronique ou de déroutement SNMP configurables
Analyse	fonctionnalité de l'appareil permettant la représentation graphique des statistiques de performances historiques et en temps réel
ARC	Adaptive Replacement Cache, cache de remplacement adaptatif
Barre de titre	section de navigation locale et de fonctions de l'écran de la BUI
Boîte de dialogue modale	nouvel élément de l'écran pour une fonction spécifique
BUI	Browser User Interface, interface utilisateur de navigateur
Cadre masthead	partie supérieure de l'écran de la BUI
CLI	Command Line Interface, interface de ligne de commande
Cluster	têtes multiples connectées à un espace de stockage partagé
Contrôleur de stockage	noeud de tête de l'appareil
Contrôleur	voir "Contrôleur de stockage"
CPU	Central Processing Unit, unité centrale
CRU	Customer Replaceable Component, composant remplaçable par le client
DEL	diode électroluminescente
DIMM	module de mémoire à double rangée de connexions (module DIMM)
DNS	Domaine Name Service, service de noms de domaine

DTrace	structure de suivi dynamique et complète permettant le dépannage en temps réel des problèmes du noyau ou des applications sur des systèmes de production
Ecriture de scripts	automatisation des tâches de la CLI
Ensemble de données	données d'une statistique Analyse enregistrées dans la mémoire et sur disque
Etagère de disques	étagère de stockage d'extension connectée au noeud de tête ou au contrôleur de stockage
FC	Fibre Channel
FRU	Field Replaceable Component, unité remplaçable sur site
FTP	File Transfer Protocol, protocole de transfert de fichier
GigE	Gigabit Ethernet
HBA	Host Bus Adapter, adaptateur de bus hôte
HCA	Host Channel Adapter, adaptateur de canal hôte
HDD	Hard Disk Drive, unité de disque dur
HTTP	HyperText Transfer Protocol, protocole de transfert hypertexte
Icônes	icônes visibles dans la BUI
Instantané	image d'un partage
IOM	Module d'E/S, semblable à un module SIM
iSCSI	Internet Small Computer System Interface
Kiosk	mode limité de la BUI dans lequel un utilisateur ne peut afficher qu'un écran donné
L2ARC	Level 2 Adaptive Replacement Cache, cache de remplacement adaptatif de niveau 2
LDAP	Lightweight Directory Access Protocol, protocole LDAP
Logzilla	accélérateur d'opérations d'E/S par seconde en écriture
Lot d'informations pour le support	fichiers générés automatiquement contenant des informations relatives à la configuration du système et des dumps noyau ; destinés au support distant pour lui permettre d'assurer le débogage des pannes sur le système
LUN	numéro d'unité logique (LUN)
Mises à jour	mises à jour logicielles ou de microprogrammes
NFS	Network File System, système de fichiers réseau
NIC	Network Interface Card, carte d'interface réseau
NIS	Network Information Service, service d'informations réseau

Partage	système de fichiers ZFS partagé à l'aide de protocoles de données
PCIe	Peripheral Component Interconnect Express, interconnexion de composants périphériques express
PCM	Power Cooling Module, module de refroidissement d'alimentation, composé d'une unité d'alimentation et d'un ventilateur au moins
Pool de stockage hybride	associe des disques, des mémoires flash et des mémoires DRAM dans un magasin de données unique, cohérent et intégré.
Pool	fournit de l'espace de stockage partagé par tous les systèmes de fichiers et les LUN
Projet	ensemble de partages
PSU	Power Supply Unit, unité d'alimentation, incluse avec les ventilateurs dans un module de refroidissement d'alimentation
QDR	quad data rate, quadruple vitesse de transfert de données
Readzilla	SSD flash optimisé pour la lecture pour le L2ARC
Restauration	rétablit l'état de l'ensemble des logiciels système et des paramètres de métadonnées antérieur à l'application d'une mise à jour
Réplication distante	réplication de partages sur un autre appareil
SAS-2	Serial Attached SCSI 2.0, SCSI série 2.0
SAS	Serial Attached SCSI, SCSI série
SATA	Serial ATA, ATA série
Schéma	propriétés configurables pour les partages
Service	logiciel de maintenance de l'appareil
SIM	SAS Interface Module, module d'interface SAS
SSD	Solid State Drive, disque dur électronique
SSH	Secure Shell, Shell sécurisé
Statistique	mesure visible dans Analyse
Tableau de bord	tableau de bord, affichage récapitulatif de l'intégrité et de l'activité du système
WebDAV	protocole Web based Distributed Authoring and Versioning
ZFS	sous-système de stockage de données sur disque