



Sun StorageTek™ 5320 NAS Appliance および Gateway システム管理マニュアル

NAS ソフトウェア Version 4.12

Sun Microsystems, Inc.
www.sun.com

Part No. 819-6919-10
2006 年 7 月, Revision A

コメントの送付: <http://www.sun.com/hwdocs/feedback>

Copyright 2006 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

米国 Sun Microsystems, Inc. (以下、米国 Sun Microsystems 社とします)は、本書に記述されている技術に関する知的所有権を有しています。これら知的所有権には、<http://www.sun.com/patents>に掲載されているひとつまたは複数の米国特許、および米国ならびにその他の国におけるひとつまたは複数の特許または出願中の特許が含まれています。

本書およびそれに付属する製品は著作権法により保護されており、その使用、複製、頒布および逆コンパイルを制限するライセンスのもとにおいて頒布されます。サン・マイクロシステムズ株式会社による事前の許可なく、本製品および本書のいかなる部分も、いかなる方法によっても複製することが禁じられます。

本製品のフォント技術を含む第三者のソフトウェアは、著作権法により保護されており、提供者からライセンスを受けているものです。

本製品の一部は、カリフォルニア大学からライセンスされている Berkeley BSD システムに基づいていることがあります。UNIX は、X/Open Company Limited が独占的にライセンスしている米国ならびに他の国における登録商標です。

本製品は、株式会社モリサワからライセンス供与されたリュウミン L-KL (Ryumin-Light) および中ゴシック BBB (GothicBBB-Medium) のフォント・データを含んでいます。

本製品に含まれる HG 明朝 L と HG ゴシック B は、株式会社リコーがリョービマジクス株式会社からライセンス供与されたタイプフェイスマスタをもとに作成されたものです。平成明朝体 W3 は、株式会社リコーが財団法人日本規格協会 文字フォント開発・普及センターからライセンス供与されたタイプフェイスマスタをもとに作成されたものです。また、HG 明朝 L と HG ゴシック B の補助漢字部分は、平成明朝体 W3 の補助漢字を使用しています。なお、フォントとして無断複製することは禁止されています。

Sun、Sun Microsystems、Java、AnswerBook2、docs.sun.com、Sun StorEdge、Sun StorageTek は、米国およびその他の国における米国 Sun Microsystems 社の商標もしくは登録商標です。サンのロゴマークおよび Solaris は、米国 Sun Microsystems 社の登録商標です。

すべての SPARC 商標は、米国 SPARC International, Inc. のライセンスを受けて使用している同社の米国およびその他の国における商標または登録商標です。SPARC 商標が付いた製品は、米国 Sun Microsystems 社が開発したアーキテクチャーに基づくものです。

OPENLOOK、OpenBoot、JLE は、サン・マイクロシステムズ株式会社の登録商標です。

ATOK は、株式会社ジャストシステムの登録商標です。ATOK8 は、株式会社ジャストシステムの著作物であり、ATOK8 にかかる著作権その他の権利は、すべて株式会社ジャストシステムに帰属します。ATOK Server/ATOK12 は、株式会社ジャストシステムの著作物であり、ATOK Server/ATOK12 にかかる著作権その他の権利は、株式会社ジャストシステムおよび各権利者に帰属します。

本書で参照されている製品やサービスに関しては、該当する会社または組織に直接お問い合わせください。

OPEN LOOK および Sun™ Graphical User Interface は、米国 Sun Microsystems 社が自社のユーザーおよびライセンス実施権者向けに開発しました。米国 Sun Microsystems 社は、コンピュータ産業用のビジュアルまたはグラフィカル・ユーザーインターフェースの概念の研究開発における米国 Xerox 社の先駆者としての成果を認めるものです。米国 Sun Microsystems 社は米国 Xerox 社から Xerox Graphical User Interface の非独占的ライセンスを取得しており、このライセンスは米国 Sun Microsystems 社のライセンス実施権者にも適用されます。

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

本書は、「現状のまま」をベースとして提供され、商品性、特定目的への適合性または第三者の権利の非侵害の黙示の保証を含みそれに限定されない、明示的であるか黙示的であるかを問わない、なんらの保証も行われぬものとします。

本書には、技術的な誤りまたは誤植のある可能性があります。また、本書に記載された情報には、定期的に変更が行われ、かかる変更は本書の最新版に反映されます。さらに、米国サンまたは日本サンは、本書に記載された製品またはプログラムを、予告なく改良または変更することがあります。

本製品が、外国為替および外国貿易管理法 (外為法) に定められる戦略物資等 (貨物または役務) に該当する場合、本製品を輸出または日本国外へ持ち出す際には、サン・マイクロシステムズ株式会社の事前の書面による承諾を得ることのほか、外為法および関連法規に基づく輸出手続き、また場合によっては、米国商務省または米国所轄官庁の許可を得ることが必要です。

原典:	Sun StorageTek 5320 NAS Appliance and Gateway System Administration Guide Part No: 819-6388-10 Revision A
-----	---



目次

はじめに xxix

1. 製品の概要 1

概要 1

Web Administrator の使用法 1

ログイン 2

インタフェースのレイアウトについて 3

ツールバーについて 3

ナビゲーションパネルについて 5

フォルダの記号について 6

その他のボタンについて 7

コンテンツパネルについて 8

状態パネルについて 8

ヘルプの使用法 9

構成ウィザードの使用法 9

構成ウィザードで可能な構成タイプについて 9

構成ウィザードの実行 10

次に実行する作業 11

2. ネットワークの初期構成 13

ネットワークの初期構成について	13
サーバー名の設定	14
LUN パスの管理	14
LUN パスの設定について	15
サーバー 1 台構成のシステムの LUN パスについて	15
サーバー 2 台構成のシステムの LUN パスについて	16
LUN パスの設定	17
LUN パスの復元	18
フェイルオーバーの使用可能への切り替え	18
フェイルオーバーの使用可能への切り替えについて	19
本体のフェイルオーバーの使用可能への切り替え	20
フェイルバック (回復) の開始	20
フェイルバックの開始について	21
回復の開始	21
ネットワークポートおよびアダプタの構成	22
ネットワークポートの構成について	22
Sun StorageTek 5320 NAS Appliance のポートの位置について	22
ネットワークアダプタの構成	23
デフォルトゲートウェイアドレスの設定	24
ネームサービスの管理	25
Windows のセキュリティーの構成	25
WINS の設定	27
DNS の設定	27
NIS の設定	29
NIS+ の設定	30
ネームサービスの構成	31
電子メール通知の設定	32
ロギングの設定	33

言語の割り当て	34
構成情報のバックアップ	35
次に実行する作業	35
3. ファイルシステムの設定と管理	37
ファイルシステムのコセプツ	37
RAID 構成について	38
LUN について	40
パーティションについて	40
ファイルボリュームについて	41
セグメントについて	41
ファイルシステムの作成	42
ファイルシステムの作成について	42
RAID セツトおよび LUN の作成について	42
新しい LUN の追加	43
ホットスペアとしてのドライブの指定	44
ファイルボリュームまたはセグメントの作成	45
ファイルボリュームまたはセグメントの作成について	46
「Create File Volumes」パネルを使用したファイルボリュームまたはセグメントの作成	46
System Manager を使用したファイルボリュームまたはセグメントの作成	47
一次ファイルボリュームへのセグメントの配置	48
LUN の再構築について	50
ファイルボリュームおよびセグメントの管理	50
ファイルボリュームのプロパティの編集	51
ファイルボリュームまたはセグメントの削除	52
ボリュームパーティションの表示	53
iSCSI プロトコルの構成	54
iSCSI の構成について	54

iSCSI ターゲットの構成について	54
iSCSI イニシエータのアクセスの構成について	55
iSCSI アクセスリストの作成	55
iSCSI のスパース LUN について	56
iSCSI LUN の作成	57
iSCSI ターゲットの検出方法について	58
iSNS サーバーの指定	58
次に実行する作業	59

4. システムの管理 61

管理者パスワードの設定 61

日付および時刻の制御 62

日付および時刻の制御について 62

時刻同期について 62

時刻同期の設定 63

日付および時刻の手動設定 63

ウイルス対策ソフトウェアの使用 64

ウイルス対策ソフトウェアについて 64

ウイルスのスキャンについて 65

ウイルス対策保護機能の使用可能への切り替え 65

隔離ファイルの削除 66

5. システムポートの管理 67

ポートの位置について 67

エイリアス IP アドレスの概要 68

ポートの結合 69

ポート結合について 69

ポート集約結合について 70

高可用性結合について 70

サーバー 1 台構成のシステムでのポート結合	70
Sun StorageTek 5320 NAS Cluster Appliance でのポートの結合	71
サーバー 2 台構成でのポート結合の例	73
6. Active Directory サービスおよび認証	75
サポートされているネームサービスについて	75
Active Directory サービスの使用法	76
Active Directory サービスについて	77
ADS の使用可能への切り替え	77
ネームサービスの検索順序の確認	79
DNS 構成の確認	79
ADS での共有の公開	80
ADS 共有コンテナの更新	81
ADS からの共有の削除	81
LDAP の設定	82
ネームサービスの検索順序の変更	82
7. グループ、ホスト、およびファイルディレクトリのセキュリティー	85
ローカルグループの権限の管理	85
ローカルグループについて	86
ローカルグループの権限の構成について	86
所有権の割り当てとグループについて	88
グループメンバーの追加および削除と権限の構成	88
グループの NT 権限の構成	89
ホストの構成	90
ホストの構成について	90
ホストの追加および編集	90
ホストグループの追加および編集	92
ユーザーおよびグループの資格のマッピング	93

ユーザーおよびグループの資格のマッピングについて	94
UNIX のユーザーおよびグループについて	94
Windows のユーザーおよびグループについて	95
資格のマッピングについて	96
ユーザーマッピングポリシーについて	97
グループマッピングポリシーについて	98
組み込みの資格のマッピングポリシーについて	100
Windows のグループおよびユーザーの、UNIX のグループおよびユーザーへのマッピング	101
Windows のグループまたはユーザーと UNIX のグループまたはユーザーとのマッピングの編集	102
ファイルディレクトリのセキュリティーの設定	103
ワークグループモードでのファイルディレクトリのセキュリティーの設定について	103
ドメインモードでのファイルディレクトリのセキュリティーの設定	103
8. 共有、割り当て、およびエクスポート	105
共有の管理	105
共有について	106
静的共有について	106
共有へのアクセス権について	107
静的共有の構成	108
SMB/CIFS クライアントの構成について	112
自動ホーム共有について	113
自動ホーム共有の使用可能への切り替え	113
割り当ての管理	114
割り当ての管理について	114
ユーザーおよびグループの割り当ての構成	115
ディレクトリツリー割り当ての構成	118
NFS エクスポートの設定	120

	NFS エクスポートの設定について	121
	エクスポートの作成	121
	エクスポートの編集	122
	エクスポートの削除	123
9.	システムのオプション	125
	システムのオプションの起動	125
	Sun StorageTek File Replicator Software オプションについて	126
	Sun StorageTek 5320 NAS Appliance のミラー化について	127
	ミラー化の準備について	127
	クラスタ構成での要件および制限事項について	128
	アクティブシステムおよびミラーシステムの構成	128
	ミラー化されたファイルボリュームの構成	129
	破損したミラーの修正	132
	ミラー化ファイルボリュームの警告しきい値の設定	133
	ミラーサーバー間の接続の切断	135
	ミラー化されたファイルボリュームのプロモート	135
	ミラー接続の再確立	136
	ボリュームの役割の変更	139
	規制適合アーカイブオプションについて	139
	Compliance Archiving Software について	140
	Compliance Archiving の使用可能への切り替えについて	140
	必須実施の規制適合について	141
	推奨実施の規制適合について	141
	規制適合の監査	142
	その他の規制適合アーカイブ機能	144
10.	システムの監視	145
	SNMP の監視	145

SNMP 監視について	146
SNMP の設定	146
システム状態の表示	147
システムログ	148
システムログについて	148
システムイベントについて	150
システムログの表示	150
システム監査	151
システム監査について	151
監査の構成について	151
監査ログファイルについて	152
システム監査の設定	152
環境状態の表示	153
ファン状態の表示	153
温度状態の表示	153
電源装置の状態の表示	154
電圧状態の表示	154
使用状況の表示	155
ファイルボリュームの使用量の表示	155
ネットワークの動作状態の表示	156
システムの動作状態の表示	156
ネットワーク (ポート) 統計情報の表示	156
ネットワークルートの表示	156
ネットワークルートについて	157
ルートの表示	157
システム状態の監視	157
UPS 監視について	158
UPS 監視の使用可能への切り替え	158

コントローラ情報の表示	159
ミラーの状態の監視について	159
ミラー化の状態の表示	159
11. システムの保守	161
遠隔アクセスオプションの設定	161
FTP アクセスの構成	162
FTP アクセスの構成について	162
FTP ユーザーの設定	163
サーバーの停止	164
ファイルのチェックポイントの管理	164
ファイルのチェックポイントについて	165
ファイルのチェックポイントの作成	165
ファイルのチェックポイントのスケジュール設定	166
チェックポイントの名前の変更	168
チェックポイントの削除	169
ファイルのチェックポイントの共有	169
ファイルのチェックポイントへのアクセス	170
NDMP バックアップの設定	170
タイムゾーンデータベースの更新	171
CATIA V4/V5 文字変換の使用可能への切り替え	173
CATIA V4/V5 文字変換について	173
CLI による CATIA の使用可能への切り替え	174
再起動時の CATIA の使用可能への自動切り替え	174
Sun StorageTek 5320 NAS Appliance ソフトウェアの更新	175
アレイおよびドライブのファームウェアバージョンのアップグレード	176
ファームウェアのアップグレードの必要性の確認	176
アレイファームウェアおよびドライブファームウェアのアップグレード (再起動が必要)	176

	アレイファームウェアのアップグレード (再起動は不要)	179
	ドライブファームウェアのアップグレード (再起動が必要)	184
	raidctl コマンドの出力の取得	185
12.	サーバーコンポーネントの交換	197
	必要な工具類および供給品	197
	電源切断とカバーの取り外し	197
	サーバーの電源切断	198
	メインカバーの取り外し	199
	正面ベゼルの取り外し	199
	正面側カバーの取り外し	201
	顧客交換可能ユニットの位置	202
	コンポーネントの交換	202
	ファンコネクタボードの交換	203
	フロントパネルインジケータボードの交換	205
	電源装置の交換	207
	メモリーモジュールの交換	208
	ファンモジュールアセンブリの交換	211
	背面側ファントレーの交換	213
	PCI カードの交換	214
A.	コンソール管理	219
	管理者コンソールへのアクセス	220
	Windows Telnet プロトコルへのアクセス	220
	管理者コンソールのコマンド行インタフェースへのアクセス	220
	コンソールメニューの概要	221
	メインメニューの表示	221
	構成情報のバックアップ	222
	システムの管理	222

TCP/IP の構成	223
管理者パスワードの変更	223
日付および時刻の制御	224
時刻同期の設定	224
コマンド行を介した、ウイルス対策保護機能の使用可能への切り替え	226
コマンド行を介した言語の選択	227
ルートの管理	228
ネームサービス	228
DNS、syslogd、およびローカルログインの設定	229
NIS および NIS+ の設定	231
ネームサービスの検索順序の設定	232
サーバーファイルシステムの管理	233
ドライブ文字の構成	233
新しいディスクボリュームの作成	234
パーティションの名前の変更	234
拡張セグメントの追加	235
ディスクボリュームの削除	235
共有および割り当て	236
SMB/CIFS 共有	236
Active Directory サービスの設定	240
割り当てを使用可能および使用不可にする方法	241
セキュリティ	241
ユーザーグループの構成	241
グループ権限の変更	243
ユーザーマップとグループマップ	243
マッピングおよびセキュリティ保護が可能なオブジェクト	245
ホストリストの構成	247
信頼できるホストの管理	248

ボリュームアクセスの管理	248
コンソールのロックおよびロック解除	249
ファイルボリュームのミラー化	250
アクティブサーバーおよびミラーサーバーの構成	250
ファイルボリュームの構成	252
警告しきい値の設定	253
ミラー化されたファイルボリュームのプロモート	254
ミラーの再確立	255
監視	257
SNMP の構成	258
電子メール通知の構成	258
システム情報の表示	259
システムの保守	262
ファイル転送プロトコル (FTP) アクセスの構成	263
RAID コントローラの管理	264
ファイルシステムのマウント	266
システムの停止	266
LUN フェイルオーバーの管理	267
LUN パスの構成	268
ファイルのチェックポイントのスケジュール設定	269
NDMP バックアップの構成	269
Compliance Archiving Software の構成	270
システム監査の構成	271
B. Sun StorageTek 5320 NAS Appliance エラーメッセージ	273
Sun StorageTek 5320 NAS Appliance のエラーメッセージについて	273
SysMon エラー通知について	274
リファレンス: UPS サブシステムエラー	274
リファレンス: ファイルシステムエラー	276

リファレンス: RAID エラー 277

リファレンス: IPMI イベント 277

C. Compliance Archiving Software API 281

規制適合機能 282

WORM ファイル 282

ファイル別保持期間 282

管理ロックダウン 282

規制適合機能の使用 283

規制適合対応のボリューム 283

WORM ファイル 283

ファイル保持期間 286

ファイル状態の確認 287

UNIX システムコールの動作 287

access(2) 287

chmod(2)、fchmod(2) 288

chown(2)、fchown(2) 288

link(2) 288

read(2)、readv(2) 288

rename(2) 289

stat(2)、fstat(2) 289

unlink(2) 289

utime(2)、utimes(2) 289

write(2)、writev(2) 290

Windows クライアントの動作 290

WORM ファイルの作成 290

WORM ファイルのメタデータの制限 290

保持期間の設定 290

Windows クライアントに対する警告 290

- その他の API 291

- D. Sun StorageTek 5320 NAS Appliance コンポーネント 293
 - NAS サーバー 293
 - フロントパネルのボタンおよび LED 294
 - 状態インジケータ LED 295
 - 背面パネルのポートおよび LED 297
 - サーバーの電源装置 299
 - 直接接続のテープライブラリ 300
 - RAID コントローラ格納装置および拡張格納装置コンポーネント 301

- E. 診断電子メールメッセージの送信 307

- F. Web Administrator のパネル 309
 - 「Anti Virus Configuration」のパネル 309
 - 「Configure Anti Virus」パネル 310
 - 「Configuration Wizard」のパネル 311
 - 「Configuration Wizard」パネル 312
 - 「Confirmation」パネル 312
 - 「Select Environment」パネル 312
 - 「File Replicator」のパネル 313
 - 「Add/Edit Mirror」ウィンドウ 313
 - 「Manage Mirrors」パネル 314
 - 「Promote Volume」ウィンドウ 316
 - 「Set Threshold Alert」パネル 316
 - 「View Mirror Statistics」パネル 317
 - ファイルボリューム操作のパネル 320
 - 「Add/Edit Checkpoint Schedule」ウィンドウ 321
 - 「Add/Edit DTQ Setting」ウィンドウ 322
 - 「Add/Edit Quota Setting」ウィンドウ 323

「Attach Segments」 パネル	324
「Configure Directory Tree Quotas」 パネル	325
「Configure User and Group Quotas」 パネル	326
「Create Checkpoint」 ウィンドウ	327
「Create File Volumes/Segments」 パネル	328
「Delete File Volumes」 パネル	330
「Edit Volume Properties」 パネル	330
「Manage Checkpoints」 パネル	332
「Rename Checkpoint」 ウィンドウ	333
「Schedule Checkpoints」 パネル	333
「View Volume Partitions」 パネル	334
「High Availability」 のパネル	335
「Enable Failover」 パネル	335
「Recover」 パネル	337
「Set LUN Path」 パネル	338
「Set Primary Path」 ウィンドウ	338
「iSCSI Configuration」 のパネル	339
「Add/Edit iSCSI Access」 ウィンドウ	339
「Add/Edit iSCSI LUN」 ウィンドウ	340
「Configure Access List」 パネル	342
「Configure iSCSI LUN for MS-Exchange」 パネル	342
「Configure iSNS Server」 パネル	343
「Monitoring and Notification」 のパネル	343
「Configure SNMP」 パネル	344
「Configure System Auditing」 パネル	345
「Display System Log」 パネル	345
「Set Up Email Notification」 パネル	346
「Set Up Logging」 パネル	347

- 「Set Up UPS Monitoring」 パネル 348
- 「View Fan Status」 パネル 349
- 「View File Volume Usage」 パネル 349
- 「View Power Supply Status」 パネル 350
- 「View Temperature Status」 パネル 350
- 「View Voltage Regulator Status」 パネル 351
- 「Network Configuration」 のパネル 351
 - 「Bond NIC Ports」 パネル 352
 - 「Configure Network Adapters」 パネル 353
 - 「Create/Edit Port Bond」 ウィンドウ 357
 - 「Set Gateway Address」 パネル 359
 - 「Set Server Name」 パネル 359
 - 「Set Up DNS」 パネル 360
 - 「View the Routing Table」 パネル 361
- 「RAID」 のパネル 362
 - 「Add Hot Spare」 ウィンドウ 362
 - 「Add LUN」 ウィンドウ 363
 - 「Locate Drive Tray」 ウィンドウ 365
 - 「Locate Drive」 ウィンドウ 365
 - 「Manage RAID」 パネル 366
 - 「View Controller/Enclosure Information」 パネル 367
 - 「View LUN Information」 パネル 368
- 「System Activity」 のパネル 368
 - 「View Networking Activity」 パネル 369
 - 「View System Activity」 パネル 369
- 「System Backup」 のパネル 370
 - 「Set Up NDMP」 パネル 370
- 「System Manager」 のパネル 371

「Edit NFS Export」 ウィンドウ	371
「Server Properties」 ウィンドウ	372
「Volume Properties」 ウィンドウ	372
「System Operations」 のパネル	374
「Activate Options」 パネル	374
「Add License」 ウィンドウ	375
「Assign Language」 パネル	376
「Enable Temporary Licenses」 ウィンドウ	377
「Import Licenses」 ウィンドウ	377
「Set Administrator Password」 パネル	378
「Set Remote Access」 パネル	378
「Set Time and Date」 パネル	379
「Set Up Time Synchronization」 パネル	380
「Shut Down the Server」 パネル	382
「Update Software」 パネル	383
「UNIX Configuration」 のパネル	384
「Add/Edit Comment」 ウィンドウ	385
「Add/Edit Host」 ウィンドウ	385
「Add/Edit NFS Export」 ウィンドウ	386
「Add Hostgroup」 ウィンドウ	387
「Add Hostgroup Member」 ウィンドウ	388
「Configure Exports」 パネル	388
「Configure Name Services」 パネル	390
「Remove NFS Export」 ウィンドウ	391
「Set Up FTP」 パネル	391
「Set Up Hostgroups」 パネル	392
「Set Up Hosts」 パネル	393
「Set Up NIS」 パネル	393

「Set Up NIS+」 パネル	394
「Set Up NSSLDAP」 パネル	395
「Windows Configuration」 のパネル	396
「Add/Edit Group」 ウィンドウ	396
「Add/Edit Share」 ウィンドウ	397
「Add/Edit SMB/CIFS User or Group Map」 ウィンドウ	399
「Configure Autohome」 パネル	400
「Configure Domains and Workgroups」 パネル	401
「Configure Groups」 パネル	403
「Configure Mapping Policy」 パネル	404
「Configure Maps」 パネル	405
「Configure Shares」 パネル	406
「Remove Share」 ウィンドウ	408
「Set Up WINS」 パネル	408
「System Status」 パネル	409

目次

図 1-1	メインウィンドウ	3
図 1-2	ツールバー	3
図 1-3	ナビゲーションパネル	5
図 1-4	ナビゲーションパネルでのフォルダの展開	5
図 1-5	コンテンツパネル	8
図 1-6	状態パネル	8
図 2-1	サーバー 1 台によるシステム構成	15
図 2-2	サーバー 2 台によるシステム構成	16
図 5-1	サーバー 2 台構成のポート結合	73
図 10-1	「Display System Log」パネル	149
図 12-1	電源ボタンと電源/OK LED の位置	198
図 12-2	メインカバーの取り外し	199
図 12-3	正面ベゼルの取り外し	200
図 12-4	正面側カバーの取り外し	201
図 12-5	交換可能コンポーネントの位置	202
図 12-6	ファンベイのドアを開き、ファンモジュールを交換する方法	203
図 12-7	ファンコネクタボードを固定しているねじの取り外し	204
図 12-8	ファンコネクタボードの取り外し	205
図 12-9	フロントパネルインジケータボードのねじの取り外し	206
図 12-10	フロントパネルインジケータボードの取り外し	206

図 12-11	電源装置の指定	207
図 12-12	電源装置の取り外し	208
図 12-13	DIMM スロットの指定	210
図 12-14	DIMM の取り外し	211
図 12-15	ファンコネクタボードおよびファンモジュールの指定	212
図 12-16	ファンベイのドアを開き、ファンモジュールを交換する方法	213
図 12-17	背面側ファントレーの取り外し	214
図 12-18	PCI スロットの指定および速度	216
図 12-19	PCI カードの固定ラッチを開く方法	217
図 12-20	PCI カードのフィルターパネルの取り外し	217
図 12-21	PCI カードの取り付け	218
図 D-1	Sun StorageTek 5320 NAS Appliance の正面図	293
図 12-22	NAS サーバーのフロントパネルのボタンおよび LED	294
図 D-2	1 枚の HBA カードを装備した Sun StorageTek 5320 NAS Appliance の背面パネル	297
図 D-3	サーバーの背面パネルの LED	298
図 D-4	電源装置モジュール	300
図 D-5	ファイバチャネルドライブシャトル	304
図 D-6	電源装置モジュール	306

表目次

表 1-1	ツールバー上のアイコン	4
表 1-2	フォルダの記号	6
表 1-3	その他のボタン	7
表 2-1	サーバー 1 台構成のシステムの一次 LUN パスおよび代替 LUN パス	16
表 5-1	サーバー 2 台構成のポート結合の例	73
表 7-1	サポートされる権限	87
表 7-2	デフォルトのグループ権限	87
表 7-3	SID 内のフィールド	95
表 8-1	共有のパスの例	106
表 8-2	DOS の読み取り専用属性が設定されている場合の umask アクセス権	107
表 9-1	監査ログの形式	143
表 10-1	システム状態の表示	147
表 10-2	システムイベントのアイコン	150
表 10-3	電圧の許容範囲	154
表 11-1	タイムゾーンデータベースファイル	172
表 11-2	CATIA 文字変換表	173
表 11-3	コンポーネントのファームウェアディレクトリおよびファイル	178
表 11-4	ファームウェアのアップグレード時間	179
表 11-5	コンポーネントのファームウェアディレクトリおよびファイル	181
表 12-1	サポートされる PCI カードのパーツ番号	214

表 A-1	画面で利用できるキー	221
表 B-1	UPS エラーメッセージ	274
表 B-2	ファイルシステムエラー	276
表 B-3	RAID エラーメッセージ	277
表 B-4	IPMI のエラーメッセージ	278
表 C-1	変更可能または変更不可能な WORM ファイルのメタデータ	285
表 D-1	NAS サーバーのフロントパネルのボタン	295
表 D-2	正面の LED 状態インジケータ	296
表 D-3	背面パネルの LED 状態インジケータ	299
表 D-4	ドライブ障害メッセージ	305
表 F-1	「Configure Anti Virus」パネルのフィールドおよび要素	310
表 F-2	「Select Environment」パネルのフィールドおよび要素	312
表 F-3	「Add/Edit Mirror」ウィンドウのフィールドおよび要素	313
表 F-4	「Manage Mirrors」パネルのフィールドおよび要素	315
表 F-5	「Promote Volume」ウィンドウのフィールドおよび要素	316
表 F-6	「Set Threshold Alert」パネルのフィールドおよび要素	317
表 F-7	「View Mirror Statistics」パネルのフィールドおよび要素	318
表 F-8	「Add/Edit Checkpoint Schedule」ウィンドウのフィールドおよび要素	321
表 F-9	「Add/Edit DTQ Setting」ウィンドウのフィールドおよび要素	322
表 F-10	「Add/Edit Quota Setting」ウィンドウのフィールドおよび要素	323
表 F-11	「Attach Segments」パネルのフィールドおよび要素	324
表 F-12	「Configure Directory Tree Quotas」パネルのフィールドおよび要素	325
表 F-13	「Configure User and Group Quotas」パネル	326
表 F-14	「Create Checkpoint」ウィンドウのフィールドおよび要素	327
表 F-15	「Create File Volumes/Segments」パネルのフィールドおよび要素	329
表 F-16	「Delete File Volumes」パネルのフィールドおよび要素	330
表 F-17	「Edit Volume Properties」パネルのフィールドおよび要素	330
表 F-18	「Manage Checkpoints」パネルのフィールドおよび要素	332
表 F-19	「Rename Checkpoint」ウィンドウのフィールドおよび要素	333
表 F-20	「Schedule Checkpoints」パネルのフィールドおよび要素	334

表 F-21	「View Volume Partitions」 パネルのフィールドおよび要素	334
表 F-22	「Enable Failover」 パネルのフィールドおよび要素	336
表 F-23	「Recover」 パネルのフィールドおよび要素	337
表 F-24	「Set LUN Path」 パネルのフィールドおよび要素	338
表 F-25	「Set Primary Path」 ウィンドウのフィールドおよび要素	339
表 F-26	「Add/Edit iSCSI Access」 ウィンドウのフィールドおよび要素	340
表 F-27	「Add/Edit iSCSI LUN」 ウィンドウのフィールドおよび要素	341
表 F-28	「Configure Access List」 パネルのフィールドおよび要素	342
表 F-29	「Configure iSCSI LUN for MS-Exchange」 パネルのフィールドおよび要素	342
表 F-30	「Configure iSNS Server」 パネルのフィールドおよび要素	343
表 F-31	「Configure SNMP」 パネルのフィールドおよび要素	344
表 F-32	「Configure System Auditing」 パネルのフィールドおよび要素	345
表 F-33	「Display System Log」 パネルのフィールドおよび要素	346
表 F-34	「Set Up Email Notification」 パネルのフィールドおよび要素	347
表 F-35	「Set Up Logging」 パネルのフィールドおよび要素	348
表 F-36	「Set Up UPS Monitoring」 パネルのフィールドおよび要素	349
表 F-37	「View Fan Status」 パネルのフィールドおよび要素	349
表 F-38	「View File Volume Usage」 パネルのフィールドおよび要素	350
表 F-39	「View Power Supply Status」 パネルのフィールドおよび要素	350
表 F-40	「View Temperature Status」 パネルのフィールドおよび要素	351
表 F-41	「View Voltage Regulator Status」 パネルのフィールドおよび要素	351
表 F-42	「Bond NIC Ports」 パネルのフィールドおよび要素	352
表 F-43	「Configure Network Adapters」 パネルのフィールドおよび要素	354
表 F-44	「Create/Edit Port Bond」 ウィンドウのフィールドおよび要素	357
表 F-45	「Set Gateway Address」 パネルのフィールドおよび要素	359
表 F-46	「Set Server Name」 パネルのフィールドおよび要素	359
表 F-47	「Set Up DNS」 パネルのフィールドおよび要素	360
表 F-48	「View the Routing Table」 パネルのフィールドおよび要素	361
表 F-49	「Add Hot Spare」 ウィンドウのドライブイメージおよびボタン	363
表 F-50	「Add LUN」 ウィンドウのドライブ状態のインジケータ	364

表 F-51	「Add LUN」 ウィンドウのフィールドおよび要素	364
表 F-52	「Locate Drive Tray」 ウィンドウのイメージおよびボタン	365
表 F-53	「Locate Drive」 ウィンドウのドライブ状態インジケータ	366
表 F-54	「Manage RAID」 パネルのフィールドおよび要素	366
表 F-55	「View Controller/Enclosure Information」 パネルのフィールドおよび要素	367
表 F-56	「View LUN Information」 パネルのフィールドおよび要素	368
表 F-57	「View Networking Activity」 パネルのフィールドおよび要素	369
表 F-58	「View System Activity」 パネルのフィールドおよび要素	369
表 F-59	「Set Up NDMP」 パネルのフィールドおよび要素	370
表 F-60	「Edit NFS Export」 ウィンドウのフィールドおよび要素	371
表 F-61	「Server Properties」 ウィンドウのフィールドおよび要素	372
表 F-62	「Edit Volume Properties」 ウィンドウのフィールドおよび要素	373
表 F-63	「Activate Options」 パネルのフィールドおよび要素	374
表 F-64	「Add License」 ウィンドウのフィールドおよび要素	375
表 F-65	「Assign Language」 パネルのフィールドおよび要素	376
表 F-66	「Enable Temporary Licenses」 ウィンドウのフィールドおよび要素	377
表 F-67	「Import Licenses」 ウィンドウのフィールドおよび要素	377
表 F-68	「Set Administrator Password」 パネルのフィールドおよび要素	378
表 F-69	「Set Remote Access」 パネルのフィールドおよび要素	379
表 F-70	「Set Time and Date」 パネルのフィールドおよび要素	379
表 F-71	「Set Up Time Synchronization」 パネルのフィールドおよび要素	380
表 F-72	「Shut Down the Server」 パネルのフィールドおよび要素	382
表 F-73	「Update Software」 パネルのフィールドおよび要素	384
表 F-74	「Add/Edit Comment」 ウィンドウのフィールドおよび要素	385
表 F-75	「Add/Edit Host」 ウィンドウのフィールドおよび要素	385
表 F-76	「Add/Edit NFS Export」 ウィンドウのフィールドおよび要素	386
表 F-77	「Add Hostgroup」 ウィンドウのフィールドおよび要素	387
表 F-78	「Add Hostgroup Member」 ウィンドウのフィールドおよび要素	388
表 F-79	「Configure Exports」 パネルのフィールドおよび要素	389
表 F-80	「Configure Name Services」 パネルのフィールドおよび要素	390

表 F-81	「Remove NFS Export」 ウィンドウのフィールドおよび要素	391
表 F-82	「Set Up FTP」 パネルのフィールドおよび要素	391
表 F-83	「Set Up Hostgroups」 パネルのフィールドおよび要素	392
表 F-84	「Set Up Hosts」 パネルのフィールドおよび要素	393
表 F-85	「Set Up NIS」 パネルのフィールドおよび要素	394
表 F-86	「Set Up NIS+」 パネルのフィールドおよび要素	395
表 F-87	「Set Up NSSLDAP」 パネルのフィールドおよび要素	395
表 F-88	「Add/Edit Group」 ウィンドウのフィールドおよびボタン	397
表 F-89	「Add/Edit Share」 ウィンドウのフィールドおよびボタン	397
表 F-90	「Add/Edit SMB/CIFS User or Group Map」 ウィンドウのフィールドおよびボタン	400
表 F-91	「Configure Autohome」 パネルのフィールドおよびボタン	400
表 F-92	「Configure Domains and Workgroups」 パネル	401
表 F-93	「Configure Groups」 パネルのフィールドおよび要素	403
表 F-94	「Configure Mapping Policy」 パネルのフィールドおよび要素	404
表 F-95	「Configure Maps」 パネルのフィールドおよび要素	405
表 F-96	「Configure Shares」 パネルのフィールドおよびボタン	407
表 F-97	「Remove Share」 ウィンドウのフィールドおよび要素	408
表 F-98	「Set Up WINS」 パネルのフィールドおよびボタン	408
表 F-99	「System Status」 パネルのフィールド	409

はじめに

『Sun StorageTek 5320 NAS Appliance および Gateway システム管理マニュアル』は、Sun StorageTek™ 5320 NAS Appliance、Sun StorageTek™ 5320 Cluster Appliance、および Sun StorageTek™ 5320 NAS Gateway システムの管理者およびユーザーを対象としたマニュアルをまとめたものです。このマニュアルでは、Web Administrator ソフトウェアを使用してシステムを設定および監視する方法について説明します。また、コマンド行インタフェース (CLI) の使用手順と、『Sun StorageTek 5320 NAS Appliance および Gateway システムご使用の手引き』に記載されていないシステムハードウェアに関する詳細についても説明します。

お読みになる前に

このマニュアルを読む前に、『Sun StorageTek 5320 NAS Appliance および Gateway システムご使用の手引き』の説明に従って、システムを設置および構成しておく必要があります。

マニュアルの構成

このマニュアルでは、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムの管理方法および使用方法について説明します。

第 1 章では、Web Administrator ソフトウェアの機能の概要を説明します。

第 2 章では、基本的なネットワークおよびファイルシステムの構成について説明します。

第 3 章では、ファイルシステムの設定と管理について説明します。

第 4 章では、システム管理機能について説明します。

第 5 章では、ポートの設定について説明します。

第 6 章では、命名規則について説明します。

第 7 章では、グループ、ホスト、およびファイルディレクトリのセキュリティー設定について説明します。

第 8 章では、共有、割り当て、およびエクスポートについて説明します。

第 9 章では、ライセンス追加可能なソフトウェアオプションについて説明します。

第 10 章では、監視機能について説明します。

第 11 章では、保守機能について説明します。

第 12 章では、顧客交換可能ユニット (CRU) の取り外し手順および交換手順について説明します。

付録 A では、コンソールを使用してシステムタスクを実行する手順について説明します。

付録 B では、生成される可能性のあるエラーメッセージについて説明します。

付録 C では、Compliance Archiving Software API について詳細に説明します。

付録 D では、システムハードウェアについて詳細に説明します。

付録 E では、診断電子メールの送信方法について説明します。

付録 F では、Web Administrator グラフィカルユーザーインターフェースのパネルについて説明します。

書体と記号について

書体または記号*	意味	例
AaBbCc123	コマンド名、ファイル名、ディレクトリ名、画面上のコンピュータ出力、コード例。	.login ファイルを編集します。 ls -a を実行します。 % You have mail.
AaBbCc123	ユーザーが入力する文字を、画面上のコンピュータ出力と区別して表します。	% su Password:
<i>AaBbCc123</i>	コマンド行の可変部分。実際の名前や値と置き換えてください。	rm <i>filename</i> と入力します。
『 』	参照する書名を示します。	『Solaris ユーザーマニュアル』
「 」	参照する章、節、または、強調する語を示します。	第 6 章「データの管理」を参照。 この操作ができるのは「スーパーユーザー」だけです。
\	枠で囲まれたコード例で、テキストがページ行幅を超える場合に、継続を示します。	% grep `^#define \ XV_VERSION_STRING '

* 使用しているブラウザにより、これらの設定と異なって表示される場合があります。

関連マニュアル

オンラインのマニュアルは、次の URL で参照できます。

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

用途	タイトル	Part No.	形式	場所
安全性	『Sun StorageTek 5320 NAS Server Regulatory and Safety Compliance Manual』	819-6929- <i>nn</i>	PDF HTML	オンライン
安全性	『Sun StorEdge 5300 RAID Expansion Unit and Sun StorEdge 5300 Expansion Unit Safety and Compliance Guide』	819-3091- <i>nn</i>	PDF	オンライン
設置および既知の問題	『Sun StorageTek 5000 NAS OS ソフトウェア ご使用にあたって』	819-6932- <i>nn</i>	PDF HTML	オンライン

用途	タイトル	Part No.	形式	場所
設置	『Sun StorageTek 5320 NAS Appliance および Gateway システムご使用の手引き』	819-6913- <i>nn</i>	PDF HTML	オンライン
NAS Appliance の設置	『Sun StorageTek 5320 NAS Appliance』(ポスター)	819-6938- <i>nn</i>	印刷物 PDF	出荷用キット オンライン
Gateway	『Sun StorageTek 5320 NAS Gateway システム』(ポスター)	819-6944- <i>nn</i>	印刷物 PDF	出荷用キット オンライン

マニュアル、サポート、およびトレーニング

Sun のサービス	URL
マニュアル	http://jp.sun.com/documentation/
サポート	http://jp.sun.com/support/
トレーニング	http://jp.sun.com/training/

Sun 以外の Web サイト

このマニュアルで紹介する Sun 以外の Web サイトが使用可能かどうかについては、Sun は責任を負いません。このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、広告、製品、またはその他の資料についても、Sun は保証しておらず、法的責任を負いません。また、このようなサイトやリソース上、またはこれらを経由して利用できるコンテンツ、商品、サービスの使用や、それらへの依存に関連して発生した実際の損害や損失、またはその申し立てについても、Sun は一切の責任を負いません。

コメントをお寄せください

マニュアルの品質改善のため、お客様からのご意見およびご要望をお待ちしております。コメントは下記よりお送りください。

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

ご意見をお寄せいただく際には、下記のタイトルと Part No. を記載してください。

『Sun StorageTek 5320 NAS Appliance および Gateway システム管理マニュアル』、Part No. 819-6919-10

第1章

製品の概要

この章では、Sun StorageTek™ 5320 NAS Web Administrator グラフィカルユーザーインターフェースの概要について説明します。この章は、次の節で構成されています。

- 1 ページの「概要」
- 1 ページの「Web Administrator の使用法」
- 9 ページの「構成ウィザードの使用法」
- 11 ページの「次に実行する作業」

概要

Sun StorageTek™ 5320 NAS Appliance システムの Web Administrator グラフィカルユーザーインターフェース (GUI) を使用すると、Sun の革新的な Sun StorageTek 5320 NAS Appliance システムに対して、セキュリティーの設定およびネットワークの構成と、管理作業の実行を容易に行うことができます。

注: このマニュアルで説明するソフトウェアのほとんどの機能は、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムソフトウェアのすべての構成に適用されます。その場合は「システム」という一般的な用語を使用します。機能がいずれかの構成に限定される場合は、その構成の名前を具体的に示します。

Web Administrator の使用法

Web Administrator グラフィカルユーザーインターフェース (GUI) では、一連のメニューおよびタブ画面、またはパネルを使用してシステムパラメータを構成できます。これらのタブ画面および設定については後の章で説明します。

この節では、インタフェースのレイアウトと、Web Administrator オンラインヘルプの使用方法について説明します。この節の内容は、次のとおりです。

- 2 ページの「ログイン」
- 3 ページの「インタフェースのレイアウトについて」
- 3 ページの「ツールバーについて」
- 5 ページの「ナビゲーションパネルについて」
- 6 ページの「フォルダの記号について」
- 7 ページの「その他のボタンについて」
- 8 ページの「コンテンツパネルについて」
- 8 ページの「状態パネルについて」

ログイン

「Login」パネルでは、承認ユーザーが Web Administrator グラフィカルユーザーインタフェース (GUI) を介してシステムにアクセスできます。デフォルトでは、システム管理者のパスワードは設定されていません。

システム管理者のパスワードを設定する場合は、61 ページの「管理者パスワードの設定」の手順に従ってください。

Web Administrator GUI にログインするには、次の手順を実行します。

1. 「Password」フィールドにシステム管理者のパスワードを入力します。
パスワードでは大文字と小文字が区別されます。システム管理者のパスワードを設定しない場合、このフィールドは空白のままにします。
2. 「Apply」をクリックします。

インタフェースのレイアウトについて

Web Administrator グラフィカルユーザーインタフェース (GUI) は、次の図に示すように、複数のセクションに分割されています。

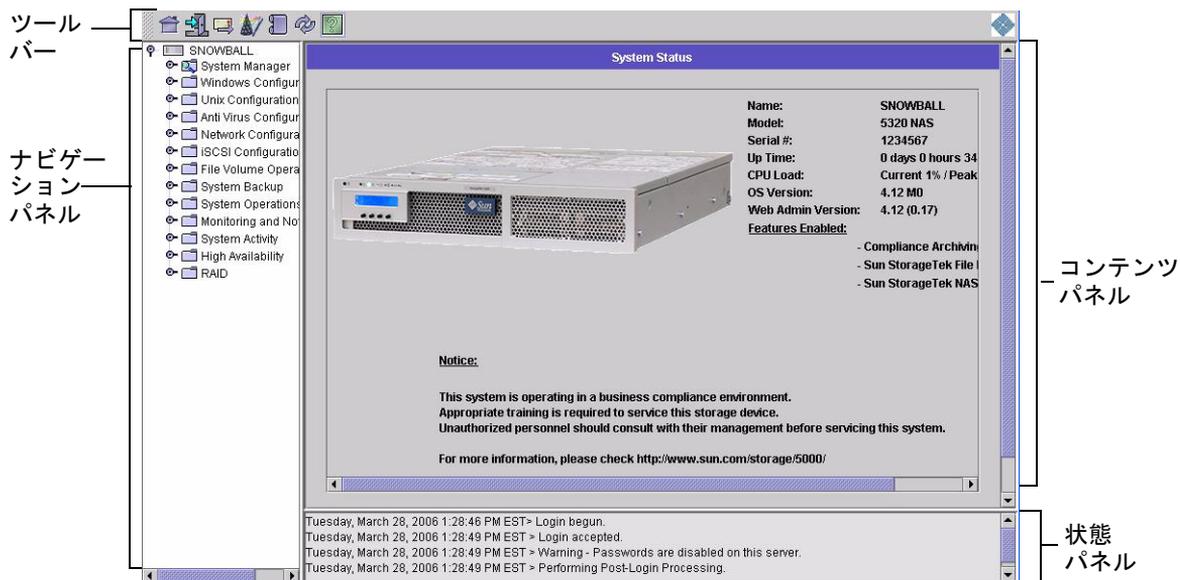


図 1-1 メインウィンドウ

Web Administrator GUI に表示される内容は、ハードウェアの構成によって異なります。

ツールバーについて

次の図に示すツールバーは、Web Administrator グラフィカルユーザーインタフェース (GUI) の一番上に表示されます。



図 1-2 ツールバー

表 1-1 に、ツールバーのアイコンを示します。

表 1-1 ツールバー上のアイコン

ボタン	名前	動作
	Home	ホーム状態画面の表示。
	Log out	ソフトウェアからのログアウト。
	Email	診断電子メールの送信。
	Wizard	構成ウィザードの実行。
	System log	システムログの表示。
	Refresh	現在のパネルおよびナビゲーションパネルの再表示。
	Help	別ウィンドウでのヘルプの起動。

ナビゲーションパネルについて

次の図に示すナビゲーションパネルを使用すると、Web Administrator グラフィカルユーザーインターフェース (GUI) 内をナビゲートできます。このパネルから、構成、設定、および管理に関するすべての機能にアクセスできます。

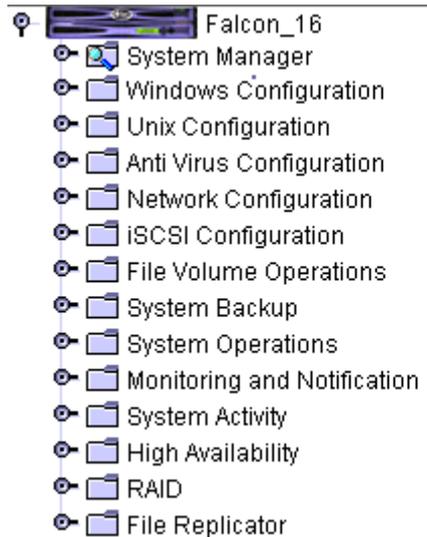


図 1-3 ナビゲーションパネル

フォルダを開くには、フォルダの横の  記号をクリックするか、フォルダをダブルクリックします。次の図に示すように、記号の向きが  に変わります。



図 1-4 ナビゲーションパネルでのフォルダの展開

フォルダを閉じるには、 記号をクリックして  の向きに戻します。

フォルダの記号について

Web Administrator グラフィカルユーザーインターフェース (GUI) では、フォルダがすべて記号で表されます。表 1-2 にフォルダの記号を示します。

表 1-2 フォルダの記号

記号	説明
	ファイルボリューム
	規制適合対応のファイルボリューム (赤いタブ付きのフォルダ)
	共有ファイルボリューム
	エクスポートされたファイルボリューム
	共有およびエクスポートされたファイルボリューム
	ミラー化されたファイルボリューム
	規制適合対応のミラー
	セグメント

その他のボタンについて

Web Administrator グラフィカルユーザーインターフェース (GUI) の一部のパネルには、その他のボタンも表示されます。表 1-3 にその他のボタンを示します。

表 1-3 その他のボタン

ボタン	名前	動作
	Add	項目の追加。
	Up	選択された項目を、リスト内の一つ上のレベルに移動。
	Down	選択された項目を、リスト内の一つ下のレベルに移動。
	Trash	選択された項目の削除。
	Edit	選択された項目の編集。

コンテンツパネルについて

次の図に示すコンテンツパネルには、システムの一般的な情報が表示されます。



図 1-5 コンテンツパネル

システムの状態の詳細は、147 ページの「システム状態の表示」を参照してください。

状態パネルについて

Web Administrator グラフィカルユーザーインターフェース (GUI) の下部にある状態パネルには、最後のログインセッション以降に発生したすべてのイベントが表示されます。このパネルでは、変更が保存されたかどうか、またはシステムコマンドが正常に実行されたかどうかを確認できます。エラーおよび警告も、このパネルに表示されます。

次の図に状態パネルを示します。

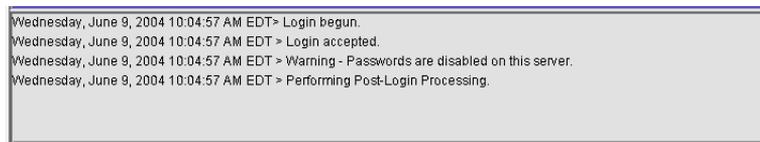


図 1-6 状態パネル

注: 状態パネルには、システムの日付と時刻ではなく、Web Administrator ソフトウェアが動作しているクライアントマシンの日付と時刻が表示されます。

ヘルプの使用方法

Web Administrator ソフトウェアに関する情報を表示するには、Web Administrator グラフィカルユーザーインターフェース (GUI) のツールバーの「Help」ボタンをクリックします。

注: Microsoft Windows システムでポップアップブロックを有効にしている場合は、ヘルプウィンドウが表示されるように、ポップアップブロックを無効にする必要があります。

現在のパネルに関する情報がヘルプウィンドウに表示されます。ヘルプウィンドウは、左のナビゲーション区画と右のトピック区画で構成されています。

利用可能なすべてのトピックを表示するには、「Help Contents」をクリックします。左のパネルには「Contents and Index」タブがあります。選択したトピックに関する情報を参照するには、「Contents」または「Index」のトピックをクリックします。

構成ウィザードの使用方法

構成ウィザードは、Web Administrator ソフトウェアにはじめてログインしたときに自動的に実行されます。このウィザードは、表示された指示に従ってユーザーが処理を進めると、システムの初期設定を行えるように設計されています。このウィザードを使用すると、システムとネットワーク間の通信を確立するために必要なすべての手順を完了できます。このウィザードを完了したあとで、ファイルシステムの設定およびユーザーアクセスの構成を行う必要があります。

構成ウィザードで可能な構成タイプについて

構成ウィザードでは、いくつかのオプションが提供されます。これらのオプションの一部は、システム自体によって自動的に決定されます。その他のオプションは、実行するネットワーク環境に基づいてユーザーが決定します。このマニュアルでは、一部の構成について説明します。この節では、構成ウィザード自体の概要と、このウィザードで選択できる構成タイプについて説明します。

また、システムの機能に応じて異なる機能もあります。これらの構成タイプについては、このマニュアル内の対応する箇所ですべて説明します。

ウィザードで選択できる主要な構成には、3つのタイプがあります。これら3つの構成タイプは、実行するネットワーク環境に基づいて選択してください。3つの構成タイプを次に示します。

- **UNIX only** — このタイプの構成では、純粋な UNIX[®] ネットワークでの操作用にシステムを構成できます。このタイプの構成では、Windows に関連するすべての機能がスキップされます。
- **Windows only** — このタイプの構成では、純粋な Windows ネットワークでの操作用にシステムを構成できます。このタイプの構成では、UNIX に関連するすべての機能がスキップされます。
- **Both UNIX and Windows** — このタイプの構成では、すべての機能を組み合わせて、Windows と UNIX の機能を兼ね備えた混在ネットワーク環境用にシステムを構成できます。

ウィザードの最初の画面で、使用するネットワーク環境に適した構成タイプを選択してください。

構成ウィザードの実行

構成ウィザードを実行するには、次の手順を実行します。

1. ツールバーの「Wizard」ボタン () をクリックします。
ウィザードが別のウィンドウで起動されます。

2. 使用する構成タイプを選択して、「Next」をクリックします。

ウィザードの指示に従って、いくつかの手順を実行します。詳細は、13 ページの「ネットワークの初期構成」を参照してください。実行する手順は次のとおりです。

- サーバー名および連絡先情報を設定します
- ネットワークアダプタを構成します
- デフォルトのゲートウェイを設定します
- ドメインおよびワークグループを構成し (Windows 環境および混在環境の場合)、ADS を使用可能にして構成します (Windows 環境および混在環境の場合)
- Windows Internet Naming Service (WINS) を構成します (Windows 環境および混在環境の場合)
- ドメインネームサービス (DNS) を設定します

注: 動的ホスト構成プロトコル (DHCP) を使用してシステムを起動した場合は、DNS サーバーのアドレスが正しいことを確認してください。アドレスが正しくない場合は、再起動およびフェイルオーバーでの遅延が発生しないように、「Configure DNS」チェックボックスの選択を解除してください。

- ネットワーク情報サービス (NIS) を設定します (UNIX 環境および混在環境の場合)

- ネットワーク情報サービスプラス (NIS+) を設定します (UNIX 環境および混在環境の場合)
 - ネームサービスを構成します (UNIX 環境および混在環境の場合)
 - 電子メール通知を設定します
 - 遠隔ログインおよびローカルログインを設定します
 - 言語を割り当てます
3. 設定を確認し、ウィザードの最終画面で「Finish」をクリックします。
- ウィザードによって設定が保存されます。変更できなかった設定がある場合は、ユーザーに通知されます。

構成ウィザードを実行しない場合は、13 ページの「ネットワークの初期構成」に記載された、ナビゲーションパネルを使用して同じ順序で同じ機能を設定する方法を参照してください。

次に実行する作業

構成ウィザードの実行によりシステムの初期構成が完了していること、システムが起動して動作していること、および **Web Administrator** グラフィカルユーザーインターフェース (GUI) でのナビゲーション方法に関する基本的な知識があることが前提となります。次に、ファイルシステムを設定し、ユーザーアクセスを構成する必要があります。

ファイルシステムの確立には、設定する必要がある任意の LUN、パーティション、ファイルボリューム、およびセグメントの定義が含まれます。これらの概念の詳細は、37 ページの「ファイルシステムのコセプツ」を参照してください。

ファイルシステムの構成が完了したら、ユーザーアクセス権限およびその他のシステム管理機能を設定してください。基本的な管理機能については、61 ページの「システムの管理」で説明します。機能の説明、動作方法、適用する状況とその理由、設定に関する特別なルールなどの特定の項目を検索するには、索引を参照してください。

第2章

ネットワークの初期構成

この章では、使用しているシステムでネットワーク通信を構成する方法について説明します。この章は、次の節で構成されています。

- 13 ページの「ネットワークの初期構成について」
- 14 ページの「サーバー名の設定」
- 14 ページの「LUN パスの管理」
- 18 ページの「フェイルオーバーの使用可能への切り替え」
- 20 ページの「フェイルバック (回復) の開始」
- 22 ページの「ネットワークポートおよびアダプタの構成」
- 24 ページの「デフォルトゲートウェイアドレスの設定」
- 25 ページの「ネームサービスの管理」
- 32 ページの「電子メール通知の設定」
- 33 ページの「ロギングの設定」
- 34 ページの「言語の割り当て」
- 35 ページの「構成情報のバックアップ」
- 35 ページの「次に実行する作業」

ネットワークの初期構成について

ネットワーク通信およびサービスの構成後、ファイルシステム、ユーザーアクセス権限、その他の機能、および購入したすべてのオプションを構成する必要があります。

この章では、構成ウィザードと同じ順序で説明します。ただし、このマニュアルで説明されていない機能の設定が必要になる場合もあります。この章で説明されていない特定の機能を設定する場合は、索引を参照して詳細を確認してください。

サーバー名の設定

使用しているシステムでネットワーク通信を構成するには、ネットワーク上でサーバーを識別するためのサーバー名を設定する必要があります。

サーバー名を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「Network Configuration」 > 「Set Server Name」を選択します。
2. 「Server Name」フィールドにサーバー名を入力します。

このサーバー名によって、システム、またはサーバー 2 台構成の高可用性 (HA) システムではそのサーバー装置が、ネットワーク上で識別されます。サーバー名には、英数字 (a ~ z、A ~ Z、0 ~ 9)、「-」(ダッシュ)、「_」(下線)、および「.」(ピリオド)を使用できます。

注: サーバー名には、数字または記号ではなく、英字 (a ~ z または A ~ Z) から始まる文字列を指定してください。たとえば、「Astro2」や「Saturn_05」は適切なサーバー名ですが、「5Saturn」や「_Astro2」は使用できません。
3. 企業の連絡先情報を入力します。

システムは、すべての診断電子メールメッセージにこの情報を含めて送信します。診断電子メールメッセージの詳細は、307 ページの「診断電子メールメッセージの送信」を参照してください。
4. 「Apply」をクリックして設定を保存します。

LUN パスの管理

この節では、論理ユニット番号 (LUN) と、LUN パスの設定方法および復元方法について説明します。この節の内容は、次のとおりです。

- 15 ページの「LUN パスの設定について」
- 15 ページの「サーバー 1 台構成のシステムの LUN パスについて」
- 16 ページの「サーバー 2 台構成のシステムの LUN パスについて」
- 17 ページの「LUN パスの設定」
- 18 ページの「LUN パスの復元」

LUN パスの設定について

論理ユニット番号 (LUN) パスは、LUN のファイルボリュームにアクセスする NAS サーバーとコントローラ、およびそのアクセス方法を指定します。それぞれのファイルボリュームには、NAS 本体コントローラからディスクアレイコントローラへの、一次パスと代替パスの 2 つの LUN パスがあります。一方のパスに障害が発生すると、システムは自動的にもう一方の使用可能な LUN パスを使用して目的のファイルボリュームにアクセスします。LUN パスの数とそれらの実装は、システムのモデルおよび構成によって異なります。Sun StorageTek 5320 NAS Cluster Appliance では、一次パスおよび代替パスの両方に障害が発生すると、サーバー (本体) が本体のフェイルオーバー (20 ページの「本体のフェイルオーバーの使用可能への切り替え」を参照) を実行します。

詳細は、17 ページの「LUN パスの設定」を参照してください。

サーバー 1 台構成のシステムの LUN パスについて

次の図に、サーバー 1 台構成のシステムの標準的なハードウェア構成を示します。

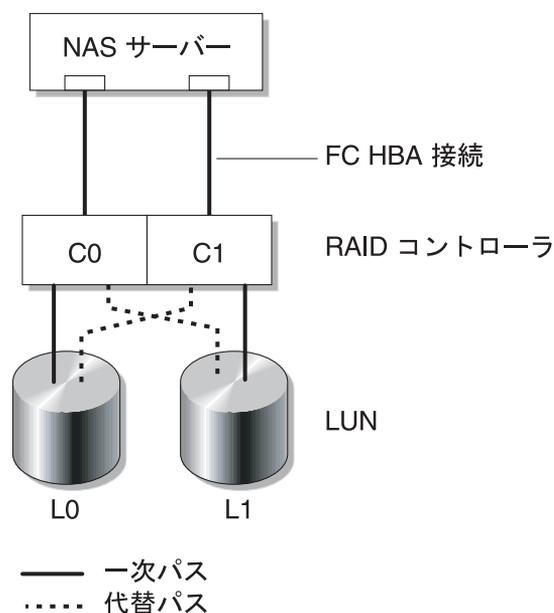


図 2-1 サーバー 1 台によるシステム構成

LUN0 のファイルボリュームへの一次 LUN パスは C0-L0 で、代替パスは C1-L0 です。LUN1 のボリュームへの一次 LUN パスは C1-L1 で、代替パスは C0-L1 です。この図に示すように、システムには次の LUN パスがあります。

表 2-1 サーバー 1 台構成のシステムの一次 LUN パスおよび代替 LUN パス

パス	LUN0	LUN1
一次	C0-L0	C1-L1
代替	C1-L0	C0-L1

各 LUN には、コントローラ 0 (C0) またはコントローラ 1 (C1) のいずれかを介してアクセスできます。

サーバー 2 台構成のシステムの LUN パスについて

次の図に、Sun StorageTek 5320 NAS Cluster Appliance システムの標準的なハードウェア構成を示します。

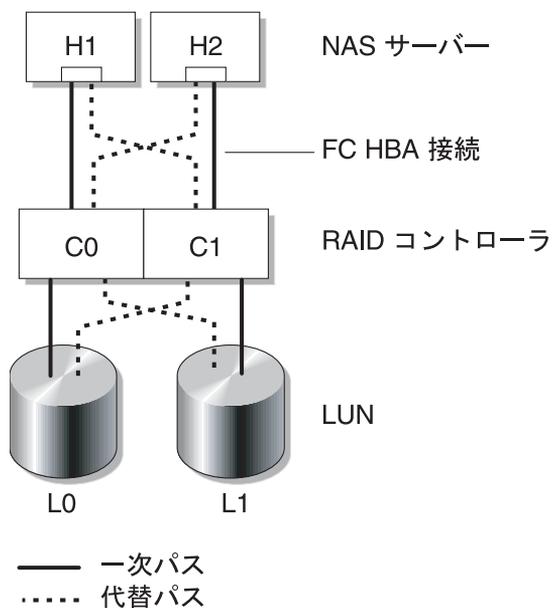


図 2-2 サーバー 2 台によるシステム構成

本体 1 の一次 LUN0 パスは C0-L0 で、代替パスは C0-L1 です。本体 2 の一次 LUN0 パスは C1-L0 で、代替パスは C1-L0 です。

通常、ファイルボリュームへのアクセスは、そのファイルボリュームが属する LUN に指定された一次 LUN パスを介して行われます。クラスタ構成では、一次パスおよび代替パスに障害が発生すると、本体がフェイルオーバーを実行します (20 ページの「本体のフェイルオーバーの使用可能への切り替え」を参照)。

LUN パスの設定

論理ユニット番号 (LUN) パスを設定して、現在アクティブな LUN パスを指定します。現在アクティブな LUN パスは、一次パスまたは代替パスのどちらでもかまいません。最適なパフォーマンスを実現するには、一次パスをアクティブなパスに設定します。LUN にファイルシステムが存在しない場合のみ、LUN を割り当て直すことができます。Sun StorageTek 5320 NAS Cluster Appliance システムでは、LUN を「所有する」サーバーのみが、その LUN を別のサーバーにふたたび割り当てることができます。

注: Sun StorageTek 5320 NAS Cluster Appliance システムでは、はじめてシステムを起動するときに、すべての LUN が 1 台のサーバー (H1) に割り当てられます。LUN を均等に振り分けるために、サーバー H1 を使用して、一部の LUN をサーバー H2 に割り当て直す必要があります。

アクティブなパスを設定するには、「Set LUN Path」パネルを使用します。Sun StorageTek 5320 NAS Cluster Appliance システムでは、どのサーバーからも、割り当てられていないパスを設定することができます。

各 LUN に対して一次パスおよび代替パスを指定するか、すべての LUN パスの自動割り当てを選択することができます。LUN パスの自動割り当てを行う場合は、「Set LUN Paths」ウィンドウの「Auto-assign LUN paths」ボタンをクリックします。

LUN パスを設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「High Availability」>「Set LUN Path」を選択します。

注: 「Set LUN Path」パネルには、最初に、LUN パスが割り当てられていない LUN が何度も表示されることがあります。これは、複数のコントローラが複数のパスを介してそれらの存在を通知するためです。いったん LUN パスが割り当てられると、現在のパスの LUN が一度だけ表示されます。

2. LUN を選択し、「Edit」をクリックします。
3. 「Primary Path」ドロップダウンメニューから、LUN パスを設定するコントローラを選択します。

例: ドロップダウンリストのオプション「1/0」を選択すると、選択した LUN にコントローラ 0 (C0) が割り当てられます。このオプションの値は「X/Y」という形式で、X は HBA、Y は NAS サーバーで LUN の認識に使用されるコントローラ ID (SID) です。「X」の値は、0 または 1 のいずれかです。1 はコントローラが動作中であることを表し、0 は動作していないことを表します。

4. LUN の割り当てを、2 つの使用可能なパスに均等に振り分けます。たとえば、1 つめと 3 つめの LUN を 1/0 に、2 つめと 4 つめの LUN を 1/1 に振り分けます。
5. 「Apply」をクリックします。

LUN パスの復元

論理ユニット番号 (LUN) の現在のアクティブなパスが、一次パスではない場合があります。「Set LUN」パネルの「Restore」オプションを使用すると、現在アクティブな LUN パスを一次 LUN パスに復元できます。

注: LUN パスを復元しても、データは回復されません。これは障害回復のための機能ではありません。代わりに、最適なパフォーマンスを実現するために、LUN の一次パスをアクティブなパスにしてください。

LUN パスを復元するには、次の手順を実行します。

1. ナビゲーションパネルで、「High Availability」> 「Set LUN Path」を選択します。
2. 復元する LUN を選択します。
3. 「Restore」をクリックします。

フェイルオーバーの使用可能への切り替え

この節では、フェイルオーバーの使用可能への切り替えについて説明します。この節の内容は、次のとおりです。

- 19 ページの「フェイルオーバーの使用可能への切り替えについて」
- 20 ページの「本体のフェイルオーバーの使用可能への切り替え」

フェイルオーバーの使用可能への切り替えについて

注: フェイルオーバーの使用可能への切り替えは、Sun StorageTek 5320 NAS Cluster Appliance システムでのみ有効です。

Sun StorageTek 5320 NAS Cluster Appliance システムは、「本体」とも呼ばれる一対のアクティブ/アクティブ・サーバーで構成されます。これらのサーバーは、RAID (Redundant Array of Independent Disk) コントローラおよび複数の異なるネットワークへのアクセスを共有します。RAID コントローラは、ファイバコントローラを介して各サーバーに接続されます。専用のハードビートケーブルで 2 台のサーバーの最初のネットワークインタフェースカード (NIC) が接続されるため、サーバーは互いの健全性状態を監視できます。

正常に動作している間は、各サーバーが独立して動作し、論理ユニット番号 (LUN) のサブセットを管理します。1 台のサーバーにハードウェア障害が発生してデータパスが使用不可になると、障害が発生したサーバーによってそれまで管理されていたインターネットプロトコル (IP) アドレスおよび LUN の所有権が、動作中のサーバーに自動的に引き継がれます。RAID ボリュームの所有権とネットワークインタフェースのアドレス指定を含む、障害が発生したサーバーのすべての動作は、動作中のサーバーに引き継がれます。これは、「本体のフェイルオーバー」と呼ばれます。

注: クラスタ構成では、一意のボリューム名を指定してください。クラスタ内の 2 つのボリュームが同じ名前である場合にフェイルオーバーが発生すると、動作中のサーバーとの衝突を回避するために、障害が発生した本体のファイルシステム名に「x」が追加されます。

クラスタのフェイルオーバー後、ネットワークファイルシステム/ユーザーデータグラムプロトコル (NFS/UDP) を使用するクライアントの動作はただちに引き継がれますが、ネットワークファイルシステム/伝送制御プロトコル (NFS/TCP) では再接続が必要になります。この再接続は、NFS 再試行が行われる中で透過的に実行されます。また、共通インターネットファイルシステム (CIFS) も再接続を必要としますが、別のアプリケーションによって、透過的な再接続、ユーザーへの通知、または続行前のユーザー確認の要求が行われる場合があります。

障害が発生した本体が修復されてオンラインになると、「フェイルバック」と呼ばれる回復処理を開始できます。「High Availability」>「Recover」を選択して「Recover」パネルを表示し、どの LUN をどの本体によって管理するかを決めます。

注: クラスタ構成で 1 台のコントローラ装置の電源の再投入または電源の障害が発生すると、両方の本体がリセットされます。各本体は部分的なボリュームの損失から保護されるように設計されているため、これは予期される動作です。

本体のフェイルオーバーの使用可能への切り替え

1 台の本体に障害が発生すると、フェイルオーバーにより、障害が発生した本体によってそれまで管理されていたインターネットプロトコル (IP) アドレスおよび論理ユニット番号 (LUN) の所有権が一時的に動作中の本体に引き継がれます。

注: 本体のフェイルオーバーを使用可能にすると、動的ホスト構成プロトコル (DHCP) が自動的に使用不可になります。

本体のフェイルオーバーを使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「High Availability」>「Enable Failover」を選択します。
2. 「Automatic Failover」チェックボックスをクリックします。
3. 「Enable Link Failover」チェックボックスを選択します。

リンクのフェイルオーバーを使用可能にすると、「Primary」の役割が割り当てられているいずれかのネットワークインタフェースに障害が発生したときに、本体のフェイルオーバーが必ず実行されます。このタイプの障害は「リンク停止」状態と呼ばれます。パートナーのネットワークリンクが停止した場合、フェイルオーバーを実行する本体を、パートナー本体がネットワークリンクを再確立したあとで、指定された時間が経過するまで待機させてください。

4. 次の項目を入力します。
 - **Down Timeout** – 1 台の本体のネットワークリンクの信頼性が失われ、そのパートナー本体のネットワークリンクが健全である場合に、本体がフェイルオーバーを実行するまで待機する時間を秒単位で指定します。
 - **Restore Timeout** – フェイルオーバーが行われるように、パートナー本体の一次リンクが確立されるまで待機する時間を秒単位で指定します。「Restore Timeout」は、リンク停止によって開始されたフェイルオーバーが、パートナー本体の一次リンクが切断されているために中止された場合にのみ使用されます。
5. 「Apply」をクリックして設定を保存します。
6. 本体を両方とも再起動します。

フェイルバック (回復) の開始

この節では、障害が発生した本体または RAID (Redundant Array of Independent Disk) コントローラがオンラインに戻った場合の、手動でのフェイルバック (回復) の開始について説明します。この節の内容は、次のとおりです。

- 21 ページの「フェイルバックの開始について」

- 21 ページの「回復の開始」

フェイルバックの開始について

障害の発生した本体がオンラインに戻った場合は、システムのフェイルオーバーが実行されたあとで、Sun StorageTek 5320 NAS Appliance または Sun StorageTek 5320 NAS Cluster Appliance システムの回復 (フェイルバック) を手動で開始してください。

障害の発生によりフェイルオーバーを実行したサーバーは、完全に機能する状態になると、元のファイルボリュームの所有権を「取り戻す」ことができます。

たとえば、障害が発生した H1 にボリューム A が割り当てられており、フェイルオーバー中に H2 がボリューム A の所有権を引き継いだとします。サーバー H1 が完全に機能する状態に戻ると、ボリューム A の所有権をサーバー H2 から取り戻すことができます。



注意: 回復を試行する前に、障害の発生したサーバーが完全に動作可能であることを確認してください。

回復の開始

障害の発生した本体がオンラインに戻った場合は、システムのフェイルオーバーが実行されたあとで、Sun StorageTek 5320 NAS Appliance または Sun StorageTek 5320 NAS Cluster Appliance システムの回復 (フェイルバック) を手動で開始してください。

回復を開始するには、次の手順を実行します。

1. ナビゲーションパネルで、「High Availability」>「Recover」を選択します。
「Recover」パネルが表示されます。
2. 本体を回復する場合は、RAID のリストから回復する RAID セットを選択します。
 - 「Head 1」リストには、サーバー H1 の LUN マッピングが表示されます。
 - 「Head 2」(パートナー) リストには、パートナーサーバー H2 の LUN マッピングが表示されます。
3. 「Recover」をクリックします。
サーバーは、LUN マッピングを再調整して、画面に表示された構成を反映します。

ネットワークポートおよびアダプタの構成

この節は、ネットワークポートおよびアダプタの構成について説明します。この節の内容は、次のとおりです。

- 22 ページの「ネットワークポートの構成について」
- 22 ページの「Sun StorageTek 5320 NAS Appliance のポートの位置について」
- 23 ページの「ネットワークアダプタの構成」

ネットワークポートの構成について

「Configure Network Adapters」パネルで、動的ホスト構成プロトコル (DHCP) を使用可能にするか、各ネットワークポートに対してインターネットプロトコル (IP) アドレス、ネットマスク、ブロードキャスト、およびネットワークインタフェースカード (NIC) ポートの役割を指定できます。また、各 NIC ポートのエイリアス IP アドレスも追加できます。

注: Sun StorageTek 5320 NAS Cluster Appliance の各 NIC ポートに役割を割り当ててください。

2 つ以上のポートを結合してポート結合を作成できます。ポート結合では、個々の構成ポートより広い帯域幅を利用できます。ネットワークポートの結合の詳細は、69 ページの「ポート結合について」を参照してください。

Sun StorageTek 5320 NAS Appliance のポートの位置について

Sun StorageTek 5320 NAS Appliance では、ポートのタイプおよびサーバー上の物理的な位置と論理的な位置に基づいて、事前定義された順序でポートが識別されます。構成するネットワークポートの位置を確認するには、297 ページの「背面パネルのポートおよび LED」および『Sun StorageTek 5320 NAS Appliance および Gateway システムご使用の手引き』を参照してください。さまざまなシステム構成が存在しますが、マニュアルで示されているものは一例です。

ネットワークインタフェースカード (NIC) とポートの関係については、『Sun StorageTek 5320 NAS Appliance および Gateway システムご使用の手引き』にも記載されています。

ネットワークアダプタの構成

ネットワークアダプタを構成するには、次の手順を実行します。

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」を選択します。
2. ネットワークでインターネットプロトコル (IP) アドレスの割り当てに動的ホスト構成プロトコル (DHCP) サーバーを使用している場合に、これを使用可能にするには、「Enable DHCP」チェックボックスを選択します。

DHCP を使用可能にすると、システムは DHCP サーバーから IP アドレスを動的に取得できます。静的 IP アドレスおよびネットマスクを手動で入力する場合、このチェックボックスの選択を解除します。DHCP を使用可能にしない場合、集約されたポートの構成ポートのネットマスクは使用不可のままです。集約されたポートの作成および設定については、69 ページの「ポート結合について」を参照してください。

注: Sun StorageTek 5320 NAS Cluster Appliance システムでは、本体のフェイルオーバーが使用不可に設定されていないかぎり、DHCP は使用できません。代わりに、ポートに静的 IP アドレスを割り当て、フェイルオーバーの際に一貫性が保たれるようにする必要があります。

3. 「Adapter」リストから、構成するポートを選択します。

作成済みポート結合にエイリアス IP アドレスを追加する場合、このリストから該当するポート結合を選択します。ポート結合の作成については、69 ページの「ポート結合について」を参照してください。個々のポートは PORTx、ポート結合は BONDx というラベルで示されます。

ポート結合の作成後、個々のポートにはエイリアス IP アドレスを追加できません。ポート結合にのみエイリアス IP アドレスを追加できます。

4. 選択したポートまたはポート結合の IP アドレスを入力します。
5. 選択したポートまたはポート結合のネットマスクを入力します。

ネットマスクによって、IP アドレス内のネットワークアドレスを特定する部分と、ホストアドレスを特定する部分が識別されます。

読み取り専用の「Broadcast」フィールドは、IP アドレスおよびネットマスクを入力すると自動的に設定されます。ブロードキャストアドレスは、ブロードキャストメッセージをサブネットに送信する際に使用される IP アドレスです。

6. 各ポートに対して、次のいずれかの役割を選択します。

役割	説明
Primary	このポートの役割は、アクティブなネットワークポートであることを示します。
Independent	このポートの役割は、バックアップなど、データの提供以外の目的に使用されるアクティブなネットワークポートであることを示します。
Mirror	このポートの役割は、ファイルボリュームをミラー化するために、このサーバーをほかのサーバーに接続するポートであることを示します。
Private - Sun StorageTek 5320 NAS Cluster Appliance のみ	Private ポートは、もう 1 台の本体の状態を定期的に監視するハートビートの専用ネットワークリンクに予約されています。Private ポートは各本体に 1 つのみです。

注: 1 つ以上のポートに、一次ポートの役割を割り当ててください。

ポートの役割の詳細は、69 ページの「ポート結合について」を参照してください。

7. 選択したポートにエイリアス IP アドレスを追加するには、「IP-Aliases」フィールドにそのアドレスを入力します。その後、「Add」ボタンをクリックして「IP-Aliases」リストに追加します。

本体 1 台構成のシステムではインタフェースごとに最大 9 つ、本体 2 台構成のシステムでは最大 4 つのエイリアスを設定できます。リストからエイリアスを削除するには、対象のエイリアスを選択して「Trash」ボタンをクリックします。変更は、「Apply」をクリックまで保存されません。

8. 「Adapter」リスト内のすべてのポートに対して、手順 3 ~ 7 を繰り返します。
9. 「Apply」をクリックして、変更内容を保存します。

デフォルトゲートウェイアドレスの設定

デフォルトゲートウェイアドレスは、ほかのサブネットへの接続にデフォルトで使用される、ローカルサブネット上のゲートウェイまたはルーターのインターネットプロトコル (IP) アドレスです。ゲートウェイまたはルーターは、遠隔の宛先にデータを送信するデバイスです。システムには、デフォルトゲートウェイのアドレスを指定する必要があります。

デフォルトゲートウェイのアドレスを設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Set Gateway Address」を選択します。
2. 「Gateway」テキストボックスにゲートウェイアドレスを入力します。
3. 「Apply」をクリックして設定を保存します。

ネームサービスの管理

この節では、ネームサービスを使用可能にするための Windows でのセキュリティーの設定と、各種ネームサービスの設定について説明します。ネームサービスの詳細は、75 ページの「Active Directory サービスおよび認証」を参照してください。この節の内容は、次のとおりです。

- 25 ページの「Windows のセキュリティーの構成」
- 27 ページの「WINS の設定」
- 27 ページの「DNS の設定」
- 29 ページの「NIS の設定」
- 30 ページの「NIS+ の設定」
- 31 ページの「ネームサービスの構成」

Windows のセキュリティーの構成

Windows 環境でネームサービスを使用するには、Windows のセキュリティーを構成する必要があります。ドメイン、ワークグループ、または Active Directory サービス (ADS) の構成は、Windows の機能です。実行中のネットワークが UNIX のみで構成されている場合、Windows ドメインや Windows ワークグループを構成する必要はありません。

セキュリティーモードを変更すると、サーバーの再起動が必要になります。このため、この手順は定期保守期間中に実行することをお勧めします。

Windows ワークグループ、NT ドメインのセキュリティー、または ADS を使用可能にするには、「Configure Domains and Workgroups」パネルを使用します。デフォルトでは、システムは Windows ワークグループモードで「workgroup」というワークグループ名で構成されます。

注 – ドメインのセキュリティ設定とワークグループのセキュリティ設定は互いに排他的です。ドメインのセキュリティを変更するとワークグループのセキュリティが無効になり、ワークグループのセキュリティを変更するとドメインのセキュリティが無効になります。

Windows のセキュリティを構成するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」 > 「Configure Domains and Workgroups」を選択します。
2. Windows ドメインのセキュリティを使用可能にするには、「Domain」オプションを選択し、「Domain」、「User Name」、および「Password」フィールドに値を入力します。これらのフィールドの詳細は、パネルの「Help」をクリックするか、401 ページの「「Configure Domains and Workgroups」パネル」を参照してください。

このオプションを選択すると、指定したドメイン上にこのサーバー用のアカウントが作成されます。指定したドメインにサーバーを追加する権限を持つユーザーアカウントを指定する必要があります。
3. Windows ワークグループのセキュリティを使用可能にするには、「Workgroup」オプションを選択し、「Name」フィールドにワークグループの名前を入力します。

ワークグループの名前は、NetBIOS の 15 文字の制限に準拠している必要があります。
4. (省略可能) Sun StorageTek 5320 NAS Appliance システムの説明を「Comments」フィールドに入力します。
5. ADS を使用可能にするには、「Enable ADS」チェックボックスを選択し、ADS 関連のフィールドに値を入力します。これらのフィールドの詳細は、パネルの「Help」をクリックするか、401 ページの「「Configure Domains and Workgroups」パネル」を参照してください。

ADS の詳細は、77 ページの「Active Directory サービスについて」を参照してください。

注: ADS を使用可能にする前に、システムの時刻と ADS Windows ドメインコントローラの時刻の誤差が 5 分以内であることを確認してください。時刻を確認するには、ナビゲーションパネルから「System Operations」 > 「Set Time and Date」を選択します。
6. 「Apply」をクリックして設定を保存します。

セキュリティモードをワークグループから NT ドメインに、またはその逆に変更すると、「Apply」をクリックしたときにサーバーが自動的に再起動します。

WINS の設定

Windows インターネットネームサービス (WINS) は Windows の機能です。実行中のネットワークが UNIX のみで構成されている場合、WINS を設定する必要はありません。

WINS を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Set Up WINS」を選択します。
2. WINS を使用可能にするには、「Enable WINS」チェックボックスを選択します。
このボックスを選択すると、システムが WINS クライアントに設定されます。
3. プライマリ WINS サーバーのインターネットプロトコル (IP) アドレスを所定のフィールドに入力します。
プライマリ WINS サーバーは、NetBIOS の名前解決で最初に照会されるサーバーです。
4. セカンダリ WINS サーバーの IP アドレスを所定のフィールドに入力します。
プライマリ WINS サーバーが応答しない場合、システムによってセカンダリ WINS サーバーが照会されます。
5. (省略可能) 「Scope」フィールドに NetBIOS の適用範囲識別子を入力します。
適用範囲を定義すると、このコンピュータと同じ適用範囲が設定されていないすべてのシステムとの通信ができなくなります。このため、この設定には注意が必要です。適用範囲は、大規模な Windows ワークグループを小規模なグループに分割する場合に役立ちます。適用範囲を使用する場合、NetBIOS またはドメインの命名規則に従って、適用範囲 ID を 16 文字以内で設定する必要があります。
6. 「Apply」をクリックして設定を保存します。

DNS の設定

ドメインネームサービス (DNS) ソフトウェアは、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムのホスト名をインターネットプロトコル (IP) アドレスに解決します。

注: 動的 DNS を使用しないで DNS を使用する場合は、使用している DNS データベースにサーバーのホスト名および IP アドレスを追加してください。動的 DNS を使用する場合は、DNS データベースを手動で更新する必要はありません。詳細は、DNS のマニュアルを参照してください。

DNS を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「Network Configuration」 > 「Configure TCP/IP」 > 「Set Up DNS」を選択します。
2. 「Enable DNS」チェックボックスを選択します。
3. DNS サーバーのドメイン名を入力します。
4. ネットワークで使用可能にする DNS サーバーの IP アドレスを入力し、「Add」ボタンをクリックして、このサーバーを「Server List」に追加します。
追加する各 DNS サーバーに対して、この手順を繰り返します。このリストには、DNS サーバーを 2 台まで追加できます。
システムでは、ドメインの名前解決の際に、サーバーリストの一番上にある DNS サーバーが最初に照会されます。そのサーバーで要求が解決されない場合、リスト内の次のサーバーが照会されます。
5. リスト内の DNS サーバーの検索順序を変更するには、移動するサーバーをクリックし、「Up」ボタンまたは「Down」ボタンをクリックします。
リストからサーバーを削除するには、サーバーの IP アドレスを選択し、「Trash」ボタンをクリックします。
6. 「Enable Dynamic DNS」チェックボックスを選択し、動的 DNS クライアントによって Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムが DNS のネームスペースに追加されるようにします。
使用する DNS サーバーで動的更新が許可されていない場合は、このオプションを使用可能にしないでください。また、25 ページの「Windows のセキュリティーの構成」で説明した Kerberos レルムおよび KDC サーバーを構成する必要もあります。DNS サーバーでセキュリティー保護されていない動的更新が許可されている場合に、このチェックボックスを選択して動的 DNS を使用可能にすると、セキュリティー保護されていない動的更新が自動的に実行されます。
7. セキュリティー保護された動的 DNS の更新を可能にするには、「Enable Dynamic DNS」チェックボックスを選択し、「DynDNS User Name」および「DynDNS Password」フィールドに値を入力します。これらのフィールドの詳細は、パネルの「Help」をクリックするか、360 ページの「Set Up DNS」パネルを参照してください。
8. 「Apply」をクリックして設定を保存します。

NIS の設定

ネットワーク情報サービス (NIS) は UNIX の機能です。実行中のネットワークが Windows のみで構成されている場合、NIS を設定する必要はありません。

「Set Up NIS」パネルを使用して、NIS を使用可能にし、ドメイン名およびサーバーのインターネットプロトコル (IP) アドレスを指定します。

NIS を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Set Up NIS」を選択します。
2. 「Enable NIS」チェックボックスを選択します。
NIS を使用可能にすると、NIS データベースからホスト、ユーザー、およびグループの情報をインポートするようにシステムが構成されます。
3. 「Domain Name」フィールドに、NIS サービスに使用するドメインの名前を入力します。
domain.com などの、DNS の命名規則を使用してください。
4. 「Server」フィールドに NIS サーバーの IP アドレスまたは名前を入力します。
これは、データベースのインポート元のサーバーです。
サーバーの IP アドレスが不明な場合、「Server」フィールドは空白のままにしておいてください。ただし、「Server」フィールドを空白にしておく場合は、「Use Broadcast」チェックボックスを選択してください。「Use Broadcast」を選択すると、NIS サーバーの適切な IP アドレスが自動的に取得されます。
5. NIS 情報の更新間隔を分単位で入力します。デフォルトの設定は 5 分です。
6. NIS サーバーの IP アドレスを自動的に取得するには、「Use Broadcast」チェックボックスを選択します。
7. NIS サーバーからシステムにホスト情報をダウンロードするには、「Update Hosts」チェックボックスを選択します。
8. NIS サーバーからシステムにユーザー情報をダウンロードするには、「Update Users」チェックボックスを選択します。
9. NIS サーバーからシステムにグループ情報をダウンロードするには、「Update Groups」チェックボックスを選択します。
10. NIS サーバーからシステムにネットグループ情報をダウンロードするには、「Update Netgroups」チェックボックスを選択します。
11. 「Apply」をクリックして、変更内容を保存します。

NIS+ の設定

ネットワーク情報サービスプラス (NIS+) は UNIX の機能です。実行中のネットワークが Windows のみで構成されている場合、NIS+ を設定する必要はありません。

注: NIS+ と NIS には関連はありません。NIS+ のコマンドおよび構造は、NIS とは異なります。

NIS+ の設定では、次の 2 つの手順を実行します。

1. Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムを NIS+ サーバー上のホスト資格ファイルに追加します。
2. NIS+ を構成します。

Sun StorageTek システムを NIS+ サーバー上のホスト資格ファイルに追加するには、次の手順を実行します。

1. スーパーユーザーとしてログインします。
2. 次のコマンドを入力します。

```
nisaddcred -p unix.server@domain -P server.domain. des
```

server には Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムの名前を、*domain* には Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムが所属する NIS+ ドメインの名前を指定します。

注: **-P** 引数のあとに指定する場合にかぎり、ドメイン名の末尾にピリオドを追加してください。

たとえば、Sun StorageTek 5320 NAS Appliance の名前が **SS1** で、NIS+ ドメインが **sun.com** である場合は、次のように入力してください。

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

3. プロンプトで、パスワードを入力します。
このパスワードは、この手順の後半で NIS+ を使用するようにシステムを構成するときにも使用します。パスワードを入力します。

NIS+ を構成するには、次の手順を実行します。

1. 遠隔クライアントから Web ブラウザウィンドウを開いてシステムに接続し、Web Administrator にログインします。
2. ナビゲーションパネルで、「UNIX Configuration」 > 「Set Up NIS+」を選択します。
3. 「Enable NIS+」チェックボックスを選択します。

4. 「Home Domain Server」フィールドに、NIS+ のホームドメインサーバーの IP アドレスを入力します。

ホームドメインサーバーの IP アドレスが不明な場合は、このフィールドを空白のままにして、「Use Broadcast」チェックボックスを選択してください。このオプションを選択すると、システムによってホームドメインサーバーの適切な IP アドレスが自動的に取得されます。

5. 「NIS+ Domain」フィールドに NIS+ のホームドメインを入力します。

注: NIS+ ドメイン名の末尾には「.」(ピリオド)を付けてください。

6. NIS+ サーバーの、セキュリティー保護された RPC パスワードを入力します。

これは、30 ページの手順 3 で設定したパスワードです。

7. 検索パスとして、コロンで区切ったドメインのリストを入力します。

検索パスには、NIS+ での情報検索時に検索されるドメインを指定します。ホームドメインとその親のみを検索する場合、このフィールドは空白のままにします。

たとえば、NIS+ ドメインが `eng.sun.com.` で検索パスが空白の場合、システムの名前解決では、最初に `eng.sun.com.`、次に `sun.com.` が検索されます。これに対して、検索パスに `sun.com.` を指定した場合は、システムの名前解決では `sun.com` のドメインのみが検索されます。

8. ホームドメインサーバーの IP アドレスが不明な場合は、「Use Broadcast」チェックボックスを選択します(手順 5 を参照)。

9. 「Apply」をクリックして設定を保存します。

ネームサービスの構成

ネームサービス (NS) の検索順序によって、照会を解決するためにネームサービスを検索する順序が制御されます。これらのネームサービスには、LDAP、NIS、NIS+、DNS、ローカルネームサービスなどがあります。名前解決にこれらのサービスを使用するには、選択したサービスを使用可能にする必要があります。

ユーザー、グループ、ネットグループ、およびホストの検索順序を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure Name Services」を選択します。
2. 「Services Not Selected」ボックスからサービスを選択し、「>」ボタンと「<」ボタンを使用してサービスを移動してから、「Services Selected」ボックスで「Up」ボタンと「Down」ボタンを使用して、「Users Order」タブでのユーザー検索の順序を選択します。

- 手順 2 の説明に従って、「Groups Order」タブでグループの検索に使用するサービスを選択します。
- 手順 2 の説明に従って、「Netgroup Order」タブでネットグループの検索に使用するサービスを選択します。
- 手順 2 の説明に従って、「Hosts Order」タブでホストの検索に使用するサービスを選択します。
- 「Apply」をクリックして、変更内容を保存します。

電子メール通知の設定

この画面では、メール転送プロトコル (SMTP) サーバー名および電子メール通知の受信者を設定します。システムでエラーが検出されると、システムによって電子メールメッセージが送信されます。

名前解決を確実に実行するには、「Configure Hosts」パネルで SMTP サーバーホスト名を設定するか (90 ページの「ホストの構成について」を参照)、DNS を設定しておく必要があります (27 ページの「DNS の設定」を参照)。

SMTP を設定して電子メールメッセージを受信者に送信するには、次の手順を実行します。

- ナビゲーションパネルで、「Monitoring and Notification」>「Set Up Email Notification」を選択します。
- 通知の送信に使用する SMTP サーバーの名前を入力します。
- 「Email Address」ボックスに、システムエラーを自動的に通知する宛先となる担当者の電子メールアドレスを入力します。
- この受信者に送信する電子メールのタイプを指定します。「Notification」または「Diagnostics」、あるいはその両方を選択します。
- 「Add」ボタンをクリックして、新しい受信者を受信者のリストに追加します。
- すべての受信者に対して手順 3～手順 5 を繰り返します。電子メールアドレスは 4 つまで入力できます。
リストから受信者を削除するには、該当するアドレスを選択し、「Trash」ボタンをクリックしてください。
- 通知レベルを選択します。
- 「Apply」をクリックして設定を保存します。

ロギングの設定

遠隔ロギングを使用可能にすると、システムによって、システムログの指定サーバーへの送信またはローカルアーカイブへの保存、あるいはその両方が実行されます。指定サーバーは、syslogd が動作している UNIX サーバーである必要があります。ロギングホストをドメイン名で指定する場合は、遠隔ロギングを使用可能にする前に、システム上でドメインネームサービス (DNS) 設定を構成してください。



注意: システムの停止時にログが消去されないようにするには、遠隔ロギングを使用可能にするか、ローカルディスク上にログファイルを作成する必要があります。そうしない場合は、システムによって、起動中に揮発性メモリー内に一時ログファイルが作成されます。この一次ログファイルは、初期起動中に発生するエラーを保持して、あとで表示するには役立ちますが、電源障害発生時またはシステムの再起動時には保持されません。

遠隔ロギングおよびローカルロギングを設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「Monitoring and Notification」>「View System Events」>「Set Up Logging」を選択します。
2. 「Enable Remote Syslogd」ボックスを選択します。
3. DNS 設定が構成されている場合は、「Server」フィールドに DNS ホスト名を入力します。DNS 設定が構成されていない場合は、インターネットプロトコル (IP) アドレスを入力します。これは、システムログの送信先になります。
4. 適切な機能を選択します。

機能は、メッセージを生成するアプリケーションまたはシステムコンポーネントを示します。

注: syslogd サーバーに送信されるすべてのメッセージには、この機能の値が指定されます。

「Set Up Remote Logging」パネルで選択できる機能の値を、次の表に示します。

機能	説明
Kern	カーネルによって生成されるメッセージ。ユーザープロセスでは生成されないメッセージです。
User	ランダムユーザープロセスによって生成されるメッセージ。機能を指定しない場合は、この機能識別子がデフォルトで指定されます。
Mail	メールシステム。
Daemon	システムデーモンまたはネットワークデーモン。

機能	説明
Auth	ログインなどの認証システム。
Syslog	syslogd によって内部的に生成されるメッセージ。
Local0 ~ Local7	ローカルでの使用のために予約済み。

5. ログに記録するシステムイベントの各タイプにチェックマークを付けて、それらのタイプを選択します (150 ページの「システムイベントについて」を参照)。
6. ローカルログを設定するには、「Enable Local Log」を選択します。
7. 「Local File」フィールドに、ログファイルのパス (ログファイルを格納するシステム上のディレクトリ) およびファイル名を入力します。
注: /cvol ディレクトリへのローカルロギングは設定できません。
/dvol/error.txt などの別のディレクトリを指定してください。
8. 「Archives」フィールドに、アーカイブファイルの最大数を入力します。
指定可能な範囲は 1 ~ 9 です。
9. 「Size」フィールドに、各アーカイブファイルの最大ファイルサイズを K バイト単位で入力します。
指定可能な範囲は 100K ~ 999,999K バイトです。
10. 「Apply」をクリックして設定を保存します。

言語の割り当て

このシステムのオペレーティングシステムでは Unicode がサポートされているため、ネットワークファイルシステム (NFS) および共通インターネットファイルシステム (CIFS) に対してローカル言語を設定できます。通常、言語の割り当ては、システムの初期設定時のウィザードで行います。ただし、あとで言語を再設定する必要がある場合は、手動で設定できます。

言語を割り当てるには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Assign Language」を選択します。
2. プルダウンメニューに表示される言語から、ローカル言語を選択します。
3. 「Apply」をクリックして、変更内容を保存します。

構成情報のバックアップ

システムの構成が完了したら、システム障害に備えて構成情報をバックアップしてください。構成情報のバックアップの詳細は、222 ページの「構成情報のバックアップ」を参照してください。

次に実行する作業

この時点で、システムがネットワークと完全に通信可能な状態になっています。ただし、ユーザーがデータの格納を開始する前に、ファイルシステムおよびユーザーアクセス権限を設定する必要があります。詳細は、37 ページの「ファイルシステムの設定と管理」を参照してください。

割り当て、共有、エクスポート、またはその他のアクセス制御の設定については、105 ページの「共有、割り当て、およびエクスポート」を参照してください。

特定の機能を設定する必要がある場合は、索引を参照して詳細を確認してください。

第3章

ファイルシステムの設定と管理

この章では、Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance のファイルシステムの概念、設定、および管理方法について説明します。

この章は、次の節で構成されています。

- 37 ページの「ファイルシステムの概念」
- 42 ページの「ファイルシステムの作成」
- 45 ページの「ファイルボリュームまたはセグメントの作成」
- 50 ページの「LUN の再構築について」
- 50 ページの「ファイルボリュームおよびセグメントの管理」
- 54 ページの「iSCSI プロトコルの構成」
- 59 ページの「次に実行する作業」

ファイルシステムの概念

以降の節では、NAS ストレージで使用されるいくつかの基本的なファイルシステムの概念および属性の定義について説明します。

- 38 ページの「RAID 構成について」
- 40 ページの「LUN について」
- 40 ページの「パーティションについて」
- 41 ページの「ファイルボリュームについて」
- 41 ページの「セグメントについて」

RAID 構成について

このシステムでは、さまざまな RAID システム構成がサポートされています。これらの構成については、次の各節で説明します。

- 38 ページの「RAID システムについて」
- 38 ページの「RAID 0 構成について (未サポート)」
- 39 ページの「RAID 1 構成について (Sun StorageTek 5320 NAS Gateway システムのみ)」
- 39 ページの「RAID 0+1 構成について (Sun StorageTek 5320 NAS Gateway システムのみ)」
- 39 ページの「RAID 5 構成について」

RAID システムについて

RAID (Redundant Array of Independent Disk) システムでは、アレイコントローラを介してデータを複数のドライブに分散できます。これによって、パフォーマンスおよびデータの安全性が向上し、回復の可能性も高くなります。RAID システムの基本概念は、小さい物理ドライブをグループ化し、非常に大きい単一のドライブとしてネットワーク上に表示することです。コンピュータユーザーからは、RAID システムは 1 台のドライブのように見えます。システム管理者には、RAID システムの物理コンポーネントはドライブのグループとして表示されますが、RAID システム自体を単一の装置として管理できます。

RAID 構成には、さまざまな種類があります。Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance ソフトウェアでは、RAID 5 のみをサポートしています。Sun StorageTek 5320 NAS Gateway システムソフトウェアでは、RAID 1、RAID 0+1、および RAID 5 をサポートしています。

RAID 0 構成について (未サポート)

RAID 0 構成は、RAID (Redundant Array of Independent Disk) システムが開発された目的である冗長性を備えていません。ただし、ドライブのパフォーマンスを大幅に向上することができます。RAID 0 構成では、「ストライプ化」という概念を採用しています。ストライプ化とは、データをストライプに分割することです。1 つのストライプが 1 台めのドライブに書き込まれ、次のストライプは 2 台めのドライブに書き込まれ、これ以降も同様に書き込まれます。ストライプ化の主な利点は、アレイ内のすべてのドライブが読み取りおよび書き込みを同時に処理できることです。同時アクセスによって読み取りと書き込みの両方が非常に速くなります。

ただし、RAID 0 構成には冗長性がないため、1 台のドライブに障害が発生するとアレイ全体のすべてのデータが失われる可能性があります。RAID 0 構成は、パフォーマンスを最優先事項とし、データ損失の重要性が低い場合にもっとも適しています。

RAID 1 構成について (Sun StorageTek 5320 NAS Gateway システムのみ)

RAID (Redundant Array of Independent Disk) 1 アレイの主要概念は、ドライブの「ミラー化」です。ミラー化によって、同じ容量のストレージを提供するために必要なドライブ数は 2 倍になりますが、ドライブの最新のバックアップを提供します。ミラー化されたドライブは常にオンラインになっているため、一次ドライブに障害が発生した場合には、非常に迅速にミラー化ドライブにアクセスできます。各一次ドライブは、同じサイズの 2 台めのドライブによってミラー化されます。すべての書き込みは複製され、RAID 1 アレイの両方のメンバーに同時に書き込まれます。RAID 1 アレイは、優れた高可用性を提供します。RAID 1 アレイは、データのセキュリティー保護と完全性が不可欠であり、パフォーマンスはそれほど重要でない場合にもっとも役立ちます。

RAID 0+1 構成について (Sun StorageTek 5320 NAS Gateway システムのみ)

RAID (Redundant Array of Independent Disk) 0+1 は、ストライプ化とミラー化の 2 つの RAID 概念を組み合わせることによって、パフォーマンスと高可用性の両方を向上させます。ミラー化ドライブのペアが、RAID 0 アレイに組み込まれます。すべての書き込みは複製され、両方のミラー化ドライブに同時に書き込まれます。RAID 0 のストライプ化によってアレイ全体のパフォーマンスが向上する一方で、RAID 1 のドライブのミラー化によって個々のドライブの優れた高可用性が提供されます。RAID 0+1 は、パフォーマンスよりセキュリティーが重視される一方で、パフォーマンスも重要である環境に適しています。

RAID 5 構成について

RAID (Redundant Array of Independent Disk) 5 アレイは、アレイ全体のドライブの数を倍増させることなく、ストライプ化によるパフォーマンスの向上と、ミラー化による冗長性の両方を実現します。

RAID 5 では、ストライプ化および「パリティ」情報を使用します。パリティ情報とは、格納される情報のビットを組み合わせる少量のデータで、このデータから残りの情報を抽出できます。つまり、パリティ情報とは、元のデータの一部が失われた場合でも、残りのデータとパリティデータを組み合わせることで完全な元のデータを再生成できるように、元のデータを繰り返したものです。パリティ情報は、特定のドライブに格納されるものではありません。ストライプセット内の異なるドライブを使用して、RAID 5 セットのさまざまな領域がパリティ保護されます。

RAID 5 アレイでは、パリティ情報がストライプの 1 つとしてストライプ配列に含まれます。アレイ内の 1 台のドライブで障害が発生すると、それ以外の使用可能なドライブ内のパリティ情報と元のデータの残りの部分によって、障害が発生したドラ

イブから失われた情報が再構築されます。このように、RAID 5 アレイは、ミラーによる高可用性とストライプによるパフォーマンスの向上を兼ね備えた非常に高度な RAID タイプです。パリティ情報用の余分な領域は少量で済むため、ソリューションにコストがかからないことも利点の 1 つです。

各アレイのドライブが構成されている最初の格納装置 (ファイバチャネルアレイの場合は 5300 RAID EU、SATA アレイの場合は空の 5300 RAID EU に接続された最初の EU S) には、6 台のドライブ (5+1) で構成される RAID 5 グループが 2 つと、グローバルホットスペアが 2 つ含まれます。それ以降のすべての EU F または EU S 格納装置には、7 台のドライブ (6+1) で構成される RAID 5 グループが 1 つまたは 2 つ含まれ、合計で 7 台または 14 台のドライブが構成されます。



注意: RAID サブシステムで重大な障害が発生しているときに、システムソフトウェアまたは RAID ファームウェアを更新して、新しいボリュームを作成したり既存のボリュームを再構築したりしないでください。

LUN について

論理ユニット番号 (LUN) は、物理デバイスまたは仮想デバイスの論理表記を識別するための番号です。Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance の RAID セットと LUN の間には、1 対 1 の対応関係があります。ただし、システムは LUN を独立エンティティとして管理し、単一のストレージボリュームとして処理します。

LUN をこのように取り扱うことで、Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance でのファイルシステムの構築プロセスは大幅に簡略化されます。RAID セットの領域へのアクセスは、ドライブの物理的な境界とは無関係に LUN を介して行われます。

ストレージリソースの管理は LUN を介して実施し、RAID セット自体を直接管理することはほとんどありません。RAID セットおよび LUN の設定の手順およびその詳細は、42 ページの「RAID セットおよび LUN の作成について」を参照してください。

パーティションについて

パーティションは論理ユニット番号 (LUN) 上のセクションで、LUN 内で使用可能な総領域を分割する方法を提供します。Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance のオペレーティングシステムは、1 つの LUN につき最大 31 個のパーティションをサポートします。

LUN の作成時、使用可能なすべての領域は最初のパーティションに配置され、それ以外のパーティションは空になります。パーティション内の領域を使用するには、ファイルボリュームを作成する必要があります。各パーティションに作成できるファ

イルボリュームは 1 つのみですが、1 つのファイルボリュームを複数のパーティションにスパン化することができます。ファイルボリュームを作成すると、パーティションのサイズは自動的にファイルボリュームのサイズに合わせて調整されます。LUN 上のそれ以外の領域は、自動的に次のパーティションに割り当てられます。オペレーティングシステムがサポートするすべてのファイルボリュームを作成したあとは、LUN 上の残りの領域にはアクセスできなくなります。

セグメント (41 ページの「セグメントについて」を参照) を配置することで、ファイルボリュームのサイズを増やすことができます。セグメントは、実際には、特殊な性質を持つ別のファイルボリュームです。既存のボリュームにセグメントを追加すると、そのセグメントはボリュームから分離できなくなります。ユーザーからはボリュームに領域が追加されただけのように見えます。このシステムの柔軟性によって、ユーザーの作業を妨げることなくファイルボリュームを作成し、必要に応じて拡張できます。複数のボリュームにユーザーのデータを分散させる必要もありません。

システム管理者がドライブおよび LUN を追加しても、ユーザーからはボリューム内に領域が追加されたようにしか見えません。

ファイルボリュームについて

情報の格納に使用できる領域を定義するものです。使用可能な領域を持つパーティションから作成されます。パーティション内の使用可能なすべての領域がボリュームに割り当てられていない場合、残りの領域は自動的に次のパーティションに割り当てられます。新しいファイルボリュームのサイズは 255G バイトに制限されます。これを超えるサイズのファイルボリュームを作成するには、最大 63 個のセグメント (41 ページの「セグメントについて」を参照) を作成して元のファイルボリュームに配置します。

ユーザー側では、ファイルボリュームとその内部のディレクトリ構造が重要です。ファイルボリュームの空き領域が少なくなった場合、管理者はセグメントを追加して、ファイルボリューム内の使用可能な領域を増やすことができます。物理的には、ドライブのみでなく拡張格納装置も追加できます。ただし、物理的にはユーザー側に表示されません。ユーザーには、ボリューム内にストレージ領域が追加されたようにしか見えません。

セグメントについて

セグメントは、ファイルボリュームと同じように作成されたストレージ領域の「ボリューム」です。既存のファイルボリュームにいつでも配置できます。セグメントを配置すると、元のファイルボリュームの総容量が増加します。各セグメントは個別に作成してファイルボリュームに配置する必要があります。ファイルボリュームに配置したあとで、セグメントをボリュームから分離することはできません。

通常、セグメントは必要に応じて作成され、ボリュームの空き容量が少なくなるとボリュームに配置されます。セグメントの配置による領域の追加の主な利点は、新しいドライブや、新しいアレイにもセグメントを作成できることです。セグメントを元のファイルボリュームに配置すると、物理的なストレージが異なる場所にあることはユーザーからは見えません。このため、ネットワークを停止することなく、必要なときに領域を追加して、データストレージの再構成や、より大きなファイルボリュームの作成を行うことができます。

ファイルシステムの作成

この節では、Sun StorageTek ファイルシステムの作成について説明します。この節の内容は、次のとおりです。

- 42 ページの「ファイルシステムの作成について」
- 42 ページの「RAID セットおよび LUN の作成について」
- 43 ページの「新しい LUN の追加」
- 44 ページの「ホットスペアとしてのドライブの指定」

ファイルシステムの作成について

Sun StorageTek 5320 NAS Gateway システムを構成する場合は、ストレージシステム構成ツールを使用して、ホットスペアドライブおよび論理ユニット番号 (LUN) を作成します。詳細は、使用しているゲートウェイに接続したストレージシステムに付属のマニュアルを参照してください。

Sun StorageTek 5320 NAS Appliance または Cluster システムを構成する場合は、42 ページの「RAID セットおよび LUN の作成について」および 44 ページの「ホットスペアとしてのドライブの指定」の節を参照してください。

RAID セットおよび LUN の作成について

Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance では、RAID (Redundant Array of Independent Disk) セットの作成および定義が論理ユニット番号 (LUN) の定義に統合されています (詳細は、37 ページの「ファイルシステムのコア」を参照)。つまり、この 2 つのオブジェクトを同時に作成することになります。Sun StorageTek 5320 NAS Appliance および Cluster システムでは、RAID セットの基本構造を選択して LUN を定義することができ、通常は RAID セットの定義に関して必要である多くの作業が自動化されています。



注意: Sun StorageTek 5320 NAS Cluster Appliance ユーザーの場合: サーバーは、それぞれが所有している LUN を管理しています。LUN を追加する前に、フェイルオーバーが使用可能に設定され、構成されていることを確認してください。詳細は、19 ページの「フェイルオーバーの使用可能への切り替えについて」を参照してください。

Sun StorageTek 5320 NAS Appliance および Cluster システムでは、パーティションの定義も自動化されています。パーティションは、LUN の作成時に自動的に定義されます。初期状態では、Sun StorageTek 5320 NAS Appliance および Cluster システムには、割り当て済みの 2 台のホットスペアドライブと、2 つ以上のデフォルトの LUN が存在します。

Sun StorageTek 5320 NAS Appliance および Cluster システムでは、RAID セットと LUN が同時に作成されるようになっており、どちらの構築プロセスも簡略化されています。

LUN を追加する際は、LUN を作成する前に LUN 内のディスクにホットスペアなどの別の機能を割り当てていないことを確認してください。別の LUN に割り当てられているドライブ、またはホットスペアとして割り当てられているドライブを、新しい LUN に含めることはできません。

新しい LUN の追加

新しい論理ユニット番号 (LUN) を追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「RAID」>「Manage RAID」を選択します。
「Manage RAID」パネルが表示されます。
注: 「Locate Drive」または「Locate Drive Tray」ボタンをクリックして、ドライブまたはドライブトレイの位置を確認できます。この操作によって、ドライブまたはドライブトレイの LCD インジケータが点滅します。
2. 「Add LUN」をクリックします。
「Add LUN」ウィンドウが表示されます。
3. 「RAID EU」プルダウンメニューから、LUN を追加するコントローラの番号を選択します。
4. 各ドライブのイメージをクリックして、この LUN に含めるドライブを選択します。
3 つ以上のドライブを選択する必要があります。ドライブのイメージには、各ドライブの状態が示されます。ドライブのイメージとその状態の詳細は、363 ページの「「Add LUN」ウィンドウ」を参照してください。

5. 次の表に示すボリュームオプションのいずれかを選択します。

オプション	説明
New Volume	このオプションは、この LUN に新しいボリュームを作成する場合に選択します。ボリュームの作成には LUN 全体が使用されます。所定のフィールドに新しいボリュームの名前を入力してください。 注: クラスタ構成では、クラスタメンバー間で一意のボリューム名を指定してください。
Existing Volume	このオプションは、この LUN を使用して既存のボリュームにディスク領域を追加 (セグメントを作成および配置) する場合に選択します。次に、プルダウンメニューから拡張するボリュームを選択します。
None	このオプションは、名前を割り当てずに新しい LUN を作成する場合に選択します。

6. 「Apply」をクリックして、新しい LUN を追加します。

システムでの LUN の追加には数時間かかります。

ホットスペアとしてのドライブの指定

Sun StorageTek 5320 NAS Appliance または Cluster システムでは、ドライブをホットスペアとして構成できます。

ドライブをホットスペアとして指定するには、次の手順を実行します。

1. ナビゲーションパネルで、「RAID」>「Manage RAID」を選択します。
2. 画面下部の「Add HS」ボタンをクリックします。
3. ドライブのイメージをクリックして、必要なドライブを選択します。

ホットスペアとして使用するディスクの容量が、このサーバーのすべての論理ユニット番号 (LUN) でもっとも容量の大きいディスクと同じか、それよりも大きいことを確認してください。

次の表に示すように、ドライブのイメージには各ドライブの状態が表示されます。

ドライブ	意味
	このスロットのドライブは、ホットスペアとして使用できます。
	このスロットのドライブは、ホットスペアとしてすでに選択されています。
	このスロットにドライブは存在しません。

4. 「Apply」をクリックして新しいホットスペアを追加します。

ファイルボリュームまたはセグメントの作成

この節では、ファイルボリュームまたはセグメントの作成について説明します。この節の内容は、次のとおりです。

- 46 ページの「ファイルボリュームまたはセグメントの作成について」
- 46 ページの「「Create File Volumes」パネルを使用したファイルボリュームまたはセグメントの作成」
- 47 ページの「System Manager を使用したファイルボリュームまたはセグメントの作成」
- 48 ページの「一次ファイルボリュームへのセグメントの配置」

ファイルボリュームまたはセグメントの作成について

新しいファイルボリュームのサイズは 255G バイトに制限されます。これを超えるサイズのファイルボリュームを作成するには、最大 63 個のセグメントを一次ボリュームに追加します。255G バイトを超えるファイルボリュームを作成する場合は、1 つの一次ボリュームと、最大 63 個のセグメントを作成します。作成したセグメントを一次ボリュームに配置して、サイズを増やします。

ファイルボリュームまたはセグメントは、「Create File Volumes」パネルまたは System Manager を使用して作成できます。

「Create File Volumes」パネルを使用したファイルボリュームまたはセグメントの作成

「Create File Volumes」パネルを使用してファイルボリュームまたはセグメントを作成するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」>「Create File Volumes」を選択します。
2. 動作中のシステムに最近新しいディスクを追加して、まだ再起動を行っていない場合は、「Scan For New Disks」ボタンをクリックします。
「Partition」プルダウンメニュー内のファイルボリュームのパーティション番号は、ファイルボリュームを作成すると自動的に増分されます。
3. 「Name」フィールドに、新しいボリューム名またはセグメント名を入力します。
有効な文字は、英数字 (a ~ z、A ~ Z、0 ~ 9) です。英字 (a ~ z、A ~ Z) から始まる 12 文字以内の名前を指定する必要があります。
注: クラスタ構成では、クラスタメンバー間で一意のボリューム名を指定してください。同一のボリューム名を指定すると、フェイルオーバーが実行された場合に問題が発生します。詳細は、19 ページの「フェイルオーバーの使用可能への切り替えについて」を参照してください。
4. プルダウンメニューをクリックして、ファイルボリュームのサイズの単位を選択します。単位は「MB」(M バイト) または「GB」(G バイト) のいずれかです。
5. ファイルボリュームのサイズを整数で入力します。
使用可能な総容量が、このフィールドの直下に表示されています。
6. ファイルボリュームの種類 (「Primary」または「Segment」) を選択します。



7. Compliance Archiving Software がインストールされている場合に、規制適合対応のボリュームを作成するには、「Compliance」セクションで「Enable」をクリックします。次に、必要な規制適合の実施の種類を指定します。

- 「Mandatory Enforcement」(必須実施) を選択した場合、デフォルトの保持期間は永続的になります。この設定は、管理操作によって変更することができません。

注意: いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

- 「Advisory Enforcement」(推奨実施) を選択した場合、デフォルトの保持期間は 0 日です。この設定は、管理操作によって変更できます。

注: 保持期間の期限が切れる前に、保持期間の短縮および保持ファイルの削除を実行する場合は、信頼できるホストからスーパーユーザーがこの操作を行う必要があります。詳細は、248 ページの「信頼できるホストの管理」を参照してください。

詳細は、140 ページの「Compliance Archiving Software について」を参照してください。

8. 「Apply」をクリックして新しいファイルボリュームまたはセグメントを作成します。

System Manager を使用したファイルボリュームまたはセグメントの作成

System Manager を使用してファイルボリュームまたはセグメントを作成するには、次の手順を実行します。

1. ナビゲーションパネルで「System Manager」を右クリックします。
2. ポップアップメニューから「Create Volume」または「Create Segment」を選択して、目的のウィンドウを開きます。
3. 「LUN」ボックスで、一次ファイルボリュームを作成する論理ユニット番号 (LUN) をクリックします。

「Partition」プルダウンメニュー内のファイルボリュームのパーティション番号は、ファイルボリュームを作成すると自動的に増分されます。

4. 「Name」フィールドに、新しいボリューム名またはセグメント名を入力します。
有効な文字は、英数字 (a ~ z、A ~ Z、0 ~ 9) です。英字 (a ~ z、A ~ Z) から始まる 12 文字以内の名前を指定する必要があります。

5. プルダウンメニューをクリックして、ファイルボリュームのサイズの単位の単位を選択します。単位は「MB」(M バイト)または「GB」(G バイト)のいずれかです。
6. ファイルボリュームのサイズを整数で入力します。
使用可能な総容量が、このフィールドの直下に表示されています。
7. ファイルボリュームの種類 (「Primary」または「Segment」) を選択します。
8. Compliance Archiving Software がインストールされている場合に、規制適合対応のボリュームを作成するには、「Compliance」セクションで「Enable」をクリックします。次に、必要な規制適合の実施の種類を指定します。
 - 「Mandatory Enforcement」(必須実施) を選択した場合、デフォルトの保持期間は永続的になります。この設定は、管理操作によって変更することができません。
注意: いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。
 - 「Advisory Enforcement」(推奨実施) を選択した場合、デフォルトの保持期間は 0 日です。この設定は、管理操作によって変更できます。
注: 保持期間の期限が切れる前に、保持期間の短縮および保持ファイルの削除を実行する場合は、信頼できるホストからスーパーユーザーがこの操作を行う必要があります。詳細は、248 ページの「信頼できるホストの管理」を参照してください。
詳細は、140 ページの「Compliance Archiving Software について」を参照してください。
9. 「Apply」をクリックして新しいファイルボリュームまたはセグメントを作成します。



一次ファイルボリュームへのセグメントの配置

この節では、一次ファイルボリュームへのセグメントの配置について説明します。この節の内容は、次のとおりです。

- 49 ページの「一次ファイルボリュームへのセグメントの配置について」
- 49 ページの「「Attach Segments」パネルを使用したセグメントの配置」
- 49 ページの「System Manager を使用したセグメントの配置」

一次ファイルボリュームへのセグメントの配置について

一次ファイルボリュームにセグメントを配置すると、ボリュームのサイズが大きくなります。セグメントはボリュームに永続的に関連付けられ、削除はできません。セグメントをボリュームに配置するには、事前にセグメントを作成しておく必要があります。詳細は、46 ページの「ファイルボリュームまたはセグメントの作成について」を参照してください。



注意: 一次ファイルボリュームに配置したセグメントは、元に戻せません。

ファイルボリューム自体のサイズは 255G バイトに制限されていますが、どの LUN からも最大 63 個のセグメントをファイルボリュームに配置することができます。各セグメントは 8M ~ 255G バイトに指定できます。

セグメントは、「Attach Segments」パネルまたは System Manager を使用して配置できます。



注意: 必須実施の規制適合対応のボリュームは、削除できません。必須実施の規制適合対応のボリュームにセグメントを追加すると、そのセグメントが使用する領域は削除または再利用できなくなります。

「Attach Segments」パネルを使用したセグメントの配置

「Attach Segments」パネルを使用してセグメントを配置するには、次の手順を実行します。

1. 「File Volume Operations」 > 「Attach Segments」をクリックして、「Attach Segments」パネルを表示します。
2. 「Existing Volumes」ボックスから、対象のボリュームをクリックして選択します。
3. 「Available Segments」ボックスから、対象のセグメントをクリックして選択します。
4. 「Apply」をクリックして配置します。

System Manager を使用したセグメントの配置

System Manager を使用してセグメントを配置するには、次の手順を実行します。

1. ナビゲーションパネルで「System Manager」をクリックし、既存のボリュームを表示します。
2. 対象のファイルボリュームを右クリックしてポップアップメニューを表示し、「Attach Segments」を選択します。

3. 配置するセグメントごとに、対象のセグメントを選択し、「Apply」をクリックして配置します。

一度に配置できるセグメントは、1 つのみです。

LUN の再構築について

論理ユニット番号 (LUN) 内のいずれかのドライブに障害が発生すると、そのドライブの発光ダイオード (LED) がオレンジ色に点灯して、新しいドライブとの交換が必要であることを示します。

注: LUN の再構築は、Sun StorageTek 5320 NAS Gateway システムの構成には適用されません。

ホットスペアドライブを使用できる場合、障害の発生したドライブに関連付けられている RAID (Redundant Array of Independent Disk) セットは、そのホットスペアを使用して再構築されます。再構築処理中は、再構築に関連するすべてのドライブの LED が緑色で点滅し、これらのドライブを取り外すことはできません。同様の再構築は、障害の発生したドライブの交換時に新しいドライブを RAID セット内に挿入し、ホットスペアがスタンバイモードに戻ったときにも実行されます。再構築が完了するには数時間かかる場合があります。

システムにホットスペアが指定されていない場合は、障害が発生したドライブを取り外し、同一またはそれより大きい容量の別のドライブと交換する必要があります。障害の発生したドライブの交換方法については、付録 D を参照してください。

障害が発生したドライブの交換後、RAID コントローラが自動的に LUN を再構築します。ディスク容量によって異なりますが、LUN の再構築には数時間かかる場合があります。LUN の再構築中、LUN ドライブの LED はオレンジ色に点滅します。

ファイルボリュームおよびセグメントの管理

ファイルシステムの管理には、次のような作業があります。

- 51 ページの「ファイルボリュームのプロパティの編集」
- 52 ページの「ファイルボリュームまたはセグメントの削除」
- 53 ページの「ボリュームパーティションの表示」

ファイルボリュームのプロパティの編集

「Edit Volume Properties」パネルを使用すると、ファイルボリュームのプロパティを変更できます。

注: 規制適合対応のボリュームが必須実施に設定されている場合は、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードを実行できません。

ボリュームの名前変更、チェックポイントの使用可能への切り替え、割り当ての使用可能への切り替え、または規制適合プロパティの編集を実行するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」>「Edit Properties」を選択します。
2. 「Volumes」リストから、変更するボリュームの名前を選択します。
3. 「New Name」フィールドに、必要に応じてボリュームの新しい名前を入力します。
有効な文字は、英数字 (a ~ z、A ~ Z、0 ~ 9) です。英字 (a ~ z、A ~ Z) から始まる 12 文字以内の名前を指定する必要があります。
4. 次の表に示すオプションのいずれかを選択します。

オプション	説明
Enable Checkpoints	このチェックボックスを選択すると、ファイルボリュームのチェックポイントが作成されます。チェックポイントは、ファイルボリュームの作成時にデフォルトで使用可能に設定されています。
Enable Quotas	このチェックボックスを選択すると、選択したボリュームの割り当てが使用可能になります。割り当ては、ファイルボリュームの作成時にデフォルトで使用不可に設定されています。
Enable Attic	このチェックボックスを選択すると、各ボリュームのルートにある <code>.attic\$</code> ディレクトリに、削除したファイルが一時的に保存されます。このオプションはデフォルトで使用可能に設定されています。ビジー状態のファイルシステム上でまれに、削除処理が終了する前に <code>.attic\$</code> ディレクトリがいっぱいになり、結果として空き領域が不足してパフォーマンスが低下することがあります。このような場合は、このチェックボックスの選択を解除して、 <code>.attic\$</code> ディレクトリを使用不可にすることをお勧めします。

5. ボリュームが規制適合対応である場合、次の表に示すように、規制適合対応のレベルに応じて「Compliance Archiving Software」セクションにいくつかのオプションが表示されます。



注意: 規制適合対応のボリュームが必須実施に設定されている場合、デフォルトの保持期間は「永続的」です。規制適合対応のボリュームが推奨実施に設定されている場合、デフォルトの保持期間は 0 日です。デフォルトの保持期間に別の値を設定する場合は、ボリュームの使用を開始する前に新しい保持期間を指定する必要があります。



注意: いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能になると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

詳細は、140 ページの「Compliance Archiving Software について」を参照してください。

オプション	説明
Mandatory Enforcement	必須実施が設定された規制適合対応ボリュームである場合は、推奨実施に変更することはできません。
Advisory Enforcement	推奨実施が設定された規制適合対応ボリュームを必須実施が設定された規制適合対応ボリュームに変更する場合は、「Mandatory Enforcement」を選択して設定を変更できます。
Permanent Retention	デフォルト。データを永続的に保持しない場合は、ボリュームを使用する前に「Retain for <i>nn</i> Days」オプションを選択してください。このオプションを選択すると、このボリュームのデータは永続的に保持されます。
Retain for <i>nn</i> Days	データの保持日数を指定するには、このオプションを選択してドロップダウンメニューを使用します。 ボリュームが推奨実施の規制適合対応である場合は、保持期間を短縮または延長することができます。 ボリュームが必須実施の規制適合対応である場合は、保持期間の延長のみが可能です。

6. 「Apply」をクリックして、変更内容を保存します。

ファイルボリュームまたはセグメントの削除

ファイルの削除後でもボリュームの空き領域が変わらない場合、その原因はチェックポイント機能または `attic` の有効化機能である可能性があります。`attic` の使用可能への切り替えについては、51 ページの「ファイルボリュームのプロパティの編集」を参照してください。

チェックポイントは、定義された特定の時間内、削除および変更されたデータを格納することで、データの安全性を維持することを目的としたデータの回復を可能にします。これは、チェックポイントが期限切れにならないかぎり、データがディスクから削除されないことを意味します。有効期限は最大 2 週間ですが、手動チェックポイントによって時間が無期限に設定されている場合は例外です。

データを削除してディスク領域を解放する場合は、チェックポイントを削除するか、使用不可に切り替える必要があります。チェックポイントの削除方法については、169 ページの「チェックポイントの削除」を参照してください。

注: 必須実施が設定された規制適合対応のボリュームは削除できません。また、オフラインのボリュームも削除できません。

ファイルボリュームまたはセグメントを削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Delete File Volumes」を選択します。
2. 削除するファイルボリュームまたはセグメントを選択します。
3. 「Apply」をクリックします。

ボリュームパーティションの表示

「View Volume Partitions」パネルには、Sun StorageTek 5320 NAS Appliance または Cluster システム用に定義された論理ユニット番号 (LUN) が読み取り専用で表示されます。

ボリュームパーティションを表示するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「View Volume Partitions」を選択します。
2. 「Volumes」リストで、パーティションを表示するファイルボリュームを選択します。

iSCSI プロトコルの構成

この節では、iSCSI (Internet Small Computer Systems Interface) プロトコルについて説明します。この節の内容は、次のとおりです。

- 54 ページの「iSCSI の構成について」
- 54 ページの「iSCSI ターゲットの構成について」
- 55 ページの「iSCSI イニシエータのアクセスの構成について」
- 55 ページの「iSCSI アクセスリストの作成」
- 56 ページの「iSCSI のスパース LUN について」
- 57 ページの「iSCSI LUN の作成」
- 58 ページの「iSCSI ターゲットの検出方法について」
- 58 ページの「iSNS サーバーの指定」

iSCSI の構成について

ホストアプリケーションから Sun StorageTek 5320 NAS Appliance ストレージへのデータ移送に iSCSI (Internet Small Computer Systems Interface) プロトコルを使用するよう、システムを構成できます。iSCSI は、SCSI コマンド、データ、および状態をネットワークファイルシステムの TCP/IP (Transmission Control Protocol/Internet Protocol) ネットワークを介して移送します。iSCSI を使用可能にすると、ホストアプリケーションはデータを Sun StorageTek 5320 NAS Appliance に保存できるようになります。

iSCSI 環境では、Sun StorageTek 5320 NAS Appliance は iSCSI イニシエータクライアントの iSCSI ターゲットとして動作します。iSCSI イニシエータおよびターゲットは、それぞれ一意で永続的な識別子を持ちます。この iSCSI イニシエータ識別子は、ホストの iSCSI ソフトウェアによって生成されます。iSCSI ターゲットは、EUI (Enterprise Unique Identifier) および IQN (iSCSI Qualified Name) の両方の識別子をサポートします。

iSCSI ターゲットの構成について

iSCSI (Internet Small Computer Systems Interface) ターゲットの論理ユニット番号 (LUN) に接続してアクセスするように iSCSI ターゲットを構成するには、次の手順を実行する必要があります。

- iSCSI イニシエータクライアントの構成 (iSCSI イニシエータソフトウェアに付属のマニュアルを参照)

- ターゲットへのアクセスを iSCSI イニシエータに許可するためのアクセスリストの作成
- LUN の作成と、iSCSI イニシエータへの LUN アクセスの割り当て
- iSCSI ターゲットおよびイニシエータの検出方法の構成

Sun StorageTek 5320 NAS Appliance に実装されている iSCSI ターゲットは、IETF (Internet Engineering Task Force) が策定した iSCSI RFC 3720 に基づいています。サポートするプロトコルの機能には、ヘッダーのダイジェスト、イニシエータのチャレンジハンドシェイク認証プロトコル (CHAP)、エラー回復レベル 0 などがあります。

iSCSI イニシエータのアクセスの構成について

iSCSI (Internet Small Computer Systems Interface) アクセスリストを作成することで、論理ユニット番号 (LUN) にアクセスできる iSCSI イニシエータを定義できます。アクセスリストには、1 つ以上の iSCSI イニシエータ、および必要に応じて 1 つの CHAP イニシエータとパスワードを登録できます。CHAP を使用すると、承認された iSCSI イニシエータから送信されたデータであることが保証されます。



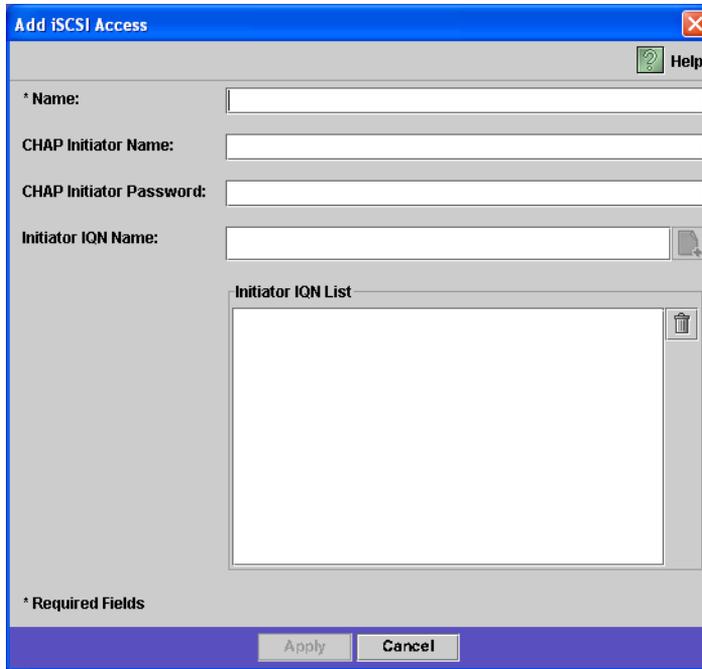
注意: 複数の iSCSI イニシエータから同じ iSCSI ターゲット LUN にアクセスするように構成できます。ただし、iSCSI クライアントサーバー上で動作しているアプリケーション (クラスタまたはデータベース) で同期アクセスを実現して、データ破壊を回避する必要があります。

iSCSI アクセスリストの作成

iSCSI (Internet Small Computer Systems Interface) アクセスリストを作成するには、次の手順を実行します。

1. ナビゲーションパネルで、「iSCSI Configuration」 > 「Configure Access List」を選択します。
2. アクセスリストを作成するには、「Add」をクリックします。

「Add iSCSI Access」ウィンドウが表示されます。



3. 各フィールドに値を入力します。各フィールドの詳細は、ウィンドウの「ヘルプ」ボタンをクリックするか、339 ページの「「Add/Edit iSCSI Access」ウィンドウ」を参照してください。
4. 「Apply」をクリックして設定を保存します。

iSCSI アクセスリストを編集するには、iSCSI アクセスリスト名のいずれかをダブルクリックするか、またはアクセスリスト名を選択して「Edit」をクリックします。テキストフィールドを変更し、「Apply」をクリックして設定を保存します。

iSCSI のスパース LUN について

iSCSI (Internet Small Computer Systems Interface) 論理ユニット番号 (LUN) の作成時に、十分なストレージを使用できるかぎり、原則的にスパースでない LUN を使用してください。

iSCSI のスパース LUN は、必ずしもすべての状況で便利であるとはかぎりません。スパース LUN を作成する場合、ディスク容量は使用するまで割り当てられません。スパース LUN は、容量を使い果たすことのない LUN をいくつか作成する予定である場合に便利です。たとえば、100G バイトの iSCSI LUN が 5 つあり、それぞれが容

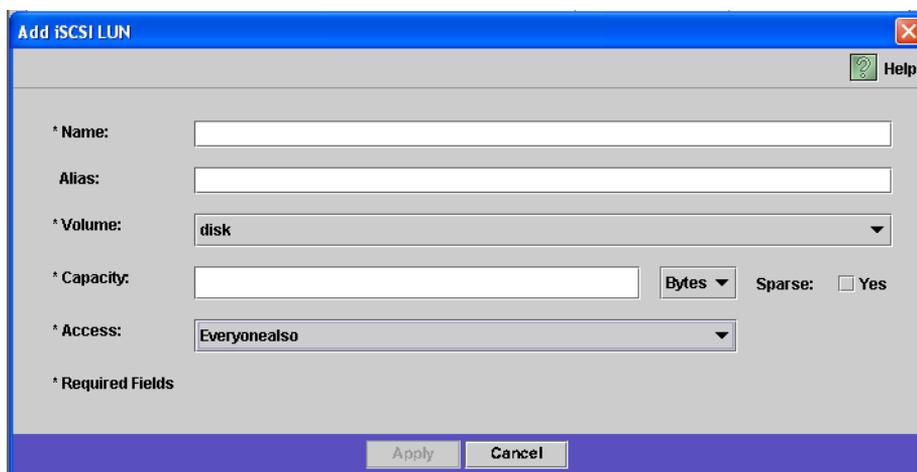
量の 55% のみを使用する予定である場合は、 $5 \times 100 \times 0.55 = 275\text{G}$ バイトに予備として 50G バイトを追加した、325G バイトの容量を維持できるボリュームに、これらの LUN をすべて作成できます。

このモデルでは、実際のボリュームの使用量を監視し、容量が不足する前にボリュームに追加領域を割り当てることができます。iSCSI LUN が、利用可能な LUN サイズの大部分を使用する予定である場合は、スパース LUN オプションを使用しないでください。オペレーティング環境によってはスパース LUN の容量不足の状況が正常に処理されないため、システムの最適な動作を維持するには、容量不足を回避する必要があります。

iSCSI LUN の作成

iSCSI (Internet Small Computer Systems Interface) 論理ユニット番号 (LUN) を作成するには、次の手順を実行します。

1. ナビゲーションパネルで、「iSCSI Configuration」 > 「Configure iSCSI LUN」を選択します。
2. iSCSI LUN をリストに追加するには、「Add」をクリックします。
「Add iSCSI LUN」ウィンドウが表示されます。



3. 各フィールドに値を入力します。各フィールドの詳細は、ウィンドウの「ヘルプ」ボタンをクリックするか、340 ページの「「Add/Edit iSCSI LUN」ウィンドウ」を参照してください。
4. 「Apply」をクリックして設定を保存します。

iSCSI ターゲットの検出方法について

次のいずれかの方法を使用して、iSCSI (Internet Small Computer Systems Interface) イニシエータが iSCSI ターゲットを検出する方法を構成できます。

- 静的構成 – iSCSI ターゲットの名前およびインターネットプロトコル (IP) アドレスを iSCSI イニシエータホストに手動で追加します。詳細は、iSCSI イニシエータソフトウェアに付属のマニュアルを参照してください。
- SendTargets 要求 – iSCSI ターゲットのポータル IP アドレスまたはドメインネームサービス (DNS) 名を iSCSI イニシエータ構成に追加します。イニシエータは SendTargets 要求を発行して、指定されたターゲットポータルでアクセス可能な iSCSI ターゲットのリストを検出します。詳細は、iSCSI イニシエータソフトウェアに付属のマニュアルを参照してください。
- iSNS (Internet Storage Name Service) サーバー – iSNS サーバーを設定して、iSCSI イニシエータと iSCSI ターゲットの検出を自動化します。iSNS サーバーは、iSCSI イニシエータによる iSCSI ターゲットの存在、位置、および構成の検出を可能にします。iSNS クライアントはオプションの機能で、次の節で説明するよう、Web Administrator の GUI を使用して構成できます。

iSNS サーバーの指定

iSNS (Internet Storage Name Service) サーバーを使用可能にするには、その iSNS サーバーのインターネットプロトコル (IP) アドレスまたはドメインネームサービス (DNS) 名を指定します。iSNS クライアントは、Microsoft iSNS Server 3.0 などの、任意の標準 iSNS サーバー実装とともに使用します。

iSNS サーバーを指定するには、次の手順を実行します。

1. ナビゲーションパネルで、「iSCSI Configuration」>「Configure iSNS Server」を選択します。
2. iSNS サーバーの IP アドレスまたは DNS 名を入力し、「Apply」をクリックします。
「iSNS Server」フィールドに別の IP アドレスまたは DNS 名を入力し、「Apply」をクリックして、iSNS サーバーの名前を変更することもできます。

詳細は、使用している iSNS サーバーのマニュアル、および iSCSI イニシエータのマニュアルを参照してください。

次に実行する作業

この時点で、ファイルシステムと iSCSI ターゲットが設定され、使用する準備が整いました。次に、アクセス権限、割り当て、および必要なディレクトリ構造を設定する必要があります。これらの管理機能については、第 4 章以降を参照してください。

リソース管理に必要な監視機能については、第 10 章を参照してください。バックアップ、復元などの保守機能については、第 11 章を参照してください。

第4章

システムの管理

この章では、システム管理のいくつかの基本機能について説明します。これらの機能は、主にシステムの初期設定中にのみ使用されますが、必要に応じて、システムを再設定する場合にも使用できます。

この章は、次の節で構成されています。

- 61 ページの「管理者パスワードの設定」
 - 62 ページの「日付および時刻の制御」
 - 64 ページの「ウイルス対策ソフトウェアの使用」
-

管理者パスワードの設定

デフォルトでは、システム管理者のパスワードは設定されていません。必要に応じてパスワードを設定できます。

システム管理者のパスワードを設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Set Administrator Password」を選択します。
2. 古いパスワードがある場合は、そのパスワードを「Old Password」フィールドに入力します。
古いパスワードがない場合は、このフィールドを空白のままにします。
3. 新しいパスワードを「New Password」フィールドに入力します。
パスワードは 1 ～ 20 文字で指定してください。文字の種類には制限はありません。

4. 新しいパスワードをもう一度「Confirm Password」フィールドに入力します。
パスワードを使用不可にするには、「New Password」フィールドおよび「Confirm Password」フィールドを空白のままにします。
5. 「Apply」をクリックして、変更内容を保存します。

日付および時刻の制御

この節では、システムの日付および時刻の制御について説明します。この節の内容は、次のとおりです。

- 62 ページの「日付および時刻の制御について」
- 62 ページの「時刻同期について」
- 63 ページの「時刻同期の設定」
- 63 ページの「日付および時刻の手動設定」

日付および時刻の制御について

ファイル管理を制御するには、システムの日付および時刻の制御が不可欠です。この節では、正確な日付および時刻の維持に使用できる機能について説明します。

時刻同期を使用するか、または時刻を手動で設定することができます。

注: 日付および時刻をはじめて設定する際、システムの「固定クロック」も初期化されます。このクロックは、ライセンス管理ソフトウェアおよび Compliance Archiving Software で使用され、時間に依存する動作を制御します。

注意: 固定クロックは一度初期化されると再設定できません。したがって、システムを構成する際は、日付および時刻を正確に設定することが重要です。



時刻同期について

このシステムは、時間情報プロトコル (NTP) および RDATE 時間プロトコルの 2 種類の時刻同期をサポートします。NTP サーバーまたは RDATE サーバーのいずれかの時刻と同期をとるように、システムを構成できます。

- NTP は、無線、衛星受信機、モデムなどの基準時刻にコンピュータの時計を同期化するインターネットプロトコルです。一般的な NTP 構成には、複数台の冗長サーバーおよび各種ネットワークパスが使用できるため、高い精度と信頼性を実現できます。

- RDATE 時間プロトコルは、サイトに影響を受けない日付および時刻を提供します。RDATE を使用すると、ネットワーク上の別のマシンから時刻を取得できません。通常、RDATE サーバーは UNIX システム上に存在し、システムの時刻を RDATE サーバーの時刻に同期化できます。

「手動同期」と呼ばれる 3 つめの方法では、時刻同期が使用不可になります。この方法では、システム管理者がシステムの時刻を設定するため、ネットワーク上のほかのノードとの同期化は行われません。

時刻同期の設定

「Set Up Time Synchronization」パネルで、いずれかの方法の時刻同期を設定できます。

時刻同期を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Set Up Time Synchronization」を選択します。
2. 次の 3 つのオプションのいずれかを選択します。
 - **Manual Synchronization** — NTP または RDATE 時刻同期のどちらも使用しない場合は、このオプションを選択します。
 - **NTP Synchronization** — NTP 同期を使用し、ネットワーク上に 1 台以上の NTP サーバーが構成されている場合は、このオプションを選択します。
NTP 同期オプションの詳細は、380 ページの「「Set Up Time Synchronization」パネル」を参照してください。
 - **RDATE Synchronization** — RDATE サーバーおよび許容範囲を設定する場合は、このオプションを選択します。
RDATE 同期オプションの詳細は、380 ページの「「Set Up Time Synchronization」パネル」を参照してください。
3. 「Apply」をクリックして、変更内容を保存します。

日付および時刻の手動設定

時刻同期を使用しない場合は、日付と時刻を手動で設定できます。

日付と時刻を手動で設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Set Time and Date」を選択します。
2. カレンダの左上にあるプルダウンメニューから適切な年を選択します。

3. カレンダの右上にあるプルダウンメニューから適切な月を選択します。
4. カレンダ内の適切な日をクリックします。
5. 時計の左上にあるドロップダウンリストボックスから適切な時間を選択します。
値の範囲は、0 (午前 0 時) ~ 23 (午後 11 時) です。
6. 時計の右上にあるプルダウンメニューから適切な分 (0 ~ 59) を選択します。
7. 画面下部のプルダウンメニューから適切なタイムゾーンを選択します。
適切なタイムゾーンを選択すると、システムで夏時間の設定が自動的に調整できるようになります。
8. 「Apply」をクリックして、日付および時刻の設定を保存します。
注: システムに日付および時刻をはじめて設定する場合は、この手順によって、規制適合ファイルを管理するための固定クロックも同じ日付および時刻に設定されます。固定クロックは一度しか設定できないため、必ず日付および時刻を正確に設定してください。

ウイルス対策ソフトウェアの使用

この節では、ウイルス対策ソフトウェアの使用方法について説明します。この節の内容は、次のとおりです。

- 64 ページの「ウイルス対策ソフトウェアについて」
- 65 ページの「ウイルスのスキャンについて」
- 65 ページの「ウイルス対策保護機能の使用可能への切り替え」
- 66 ページの「隔離ファイルの削除」

ウイルス対策ソフトウェアについて

ウイルス対策保護機能は、ネットワーク上にインストールした「スキャンエンジン」への ICAP (Internet Content Adaptation Protocol) 接続を介して利用できます。Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムでウイルス対策保護機能を使用可能にすると、システムはネットワーク上で使用しているウイルス対策エンジンのクライアントになります。

注: システムでウイルスからの保護を構成する場合は、1 つ以上のスキャンエンジンを常に動作させておく必要があります。スキャンエンジンが動作していないと Windows クライアントからのアクセスが拒否される場合があります。

ウイルスのスキャンについて

正常な動作中でも、ウイルスのスキャン時、特に「Scan all Access」オプションが選択されている場合に、共通インターネットファイルシステム (CIFS) クライアントで短い遅延が生じることがあります。

ウイルスが検出されると、システムログに感染ファイルの名前、ウイルスの名前、および感染ファイルに対する処置を記録するエントリが追加されます。ほとんどの場合、処置は感染ファイルの「隔離」となり、その CIFS クライアントへのアクセスが拒否されるようになります。隔離ファイルは、感染ファイルが格納されているファイルシステムのルートの /quarantine ディレクトリで確認できます。/quarantine ディレクトリ内での名前の衝突を避けるために、ファイルには「内部番号」に基づく名前が付けられます。NNNNNN.vir は感染ファイルへの「ハードリンク」で、NNNNNN.log は感染ファイルの元の名前と検出された感染の詳細が記載されたテキストファイルです。

注: デフォルトでは、管理者 (または UNIX のスーパーユーザー) のみが /quarantine ディレクトリの内容を参照できます。

感染 (隔離) ファイルから回復するもっとも簡単な方法は、そのファイルを削除することです。

ウイルス対策保護機能の使用可能への切り替え

ウイルス対策保護機能を使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「Anti Virus Configuration」>「Configure Anti Virus」を選択します。
2. 「Enable Anti Virus」チェックボックスを選択します。
注: ウイルス対策のスキャンを一時的に使用不可にする必要がある場合は、「Scanning Suspended」オプションを使用します。「Enable Anti Virus」チェックボックスの選択は解除しないでください。
3. スキャンモードを選択します。
4. 使用するスキャンエンジンの TCP/IP (Transmission Control Protocol/Internet Protocol) アドレスを指定します。
5. ICAP サーバーが接続を待機する TCP/IP (Transmission Control Protocol/Internet Protocol) ポート番号を指定します。通常はポート 1344 を使用します。
6. システムがスキャンエンジンに振り分ける、並行ファイルスキャン操作の最大数を指定します。通常は 2 を設定します。
7. 各スキャンの対象に含めるものと除外するものを、表示されたリストからそれぞれ選択して指定します。

8. リストに新しい項目を追加するには、ボックスにその項目を入力して「Add」をクリックします。
リストから項目を削除するには、その項目を選択して「Remove」をクリックします。
9. 「Apply」をクリックして設定を保存します。
注:すでにメモリー内に読み込まれているファイルは、スキャンの対象になりません。ウイルスのスキャンを完全に有効にするには、システムを再起動することをお勧めします。

隔離ファイルの削除

隔離ファイルを削除するには、次の手順を実行します。

1. システムログまたは隔離ディレクトリの NNNNNN.log ファイルのいずれかでファイルの元の名前を確認し、まだ存在する場合はそのファイルを削除します。
2. 隔離ディレクトリで感染ファイルに対応する NNNNNN.vir および NNNNNN.log の 2 つのファイルを探し、これらを削除します。

第5章

システムポートの管理

この章では、ネットワークポートおよびエイリアス IP アドレスについて説明します。2 つ以上のポートを結合してポート結合を作成できます。ポート結合では、個々の構成ポートより広い帯域幅を利用できます。

この章は、次の節で構成されています。

- 67 ページの「ポートの位置について」
- 68 ページの「エイリアス IP アドレスの概要」
- 69 ページの「ポートの結合」

ポートの位置について

Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムでは、ポートのタイプおよびサーバー上の物理的な位置と論理的な位置に基づいて、事前定義された順序でポートが識別されます。システムのポートの位置を確認するには、『Sun StorageTek 5320 NAS Appliance および Gateway システムご使用の手引き』を参照してください。

各ポートには役割を割り当てる必要があります。割り当て可能な役割は、次のとおりです。

- **Primary** — このポートの役割は、アクティブなネットワークポートであることを示します。1 つ以上のポートに、一次ポートの役割を割り当てる必要があります。一次ポートは、フェイルオーバー処理が統合される部分です。ポートにこの役割を割り当てると、パートナーサーバー (サーバー H2) は、一次ポートに割り当てられたインターネットプロトコル (IP) アドレスを、オフラインのバックアップ用エイリアス IP アドレスとして保持します。パートナーサーバーにエイリアス IP アドレスを指定すると、その逆の状態になります。パートナーサーバーの IP アドレスがバックアップ用エイリアス IP アドレスとして主サーバー (サーバー H1) に保持されます。フェイルオーバーが発生すると、健全なサーバーはパートナーサー

バーのエイリアス IP アドレスを使用可能にします。これによって、障害が発生したサーバーが依然として動作中であるかのように、ネットワークアクセスを継続できます。

注: 各サーバーで、1 つ以上のポートに一次ポートの役割を割り当ててください。

- **Independent** – このポートの役割は、バックアップなど、データの提供以外の目的に使用されるアクティブなネットワークポートであることを示します。Sun StorageTek 5320 NAS Cluster Appliance では、このポートはフェイルオーバー処理の対象になりません。Independent ポートは、通常、遠隔バックアップに使用されます。Independent ポートを結合 (集約) したり、エイリアス IP アドレスをこのポートに追加したりすることはできません。この役割を割り当てるポートの数に制限はありませんが、1 台の本体に 1 つだけ割り当てることをお勧めします。
- **Mirror** – このポートの役割は、ファイルボリュームをミラー化するために、このサーバーをほかのサーバーに接続するポートであることを示します。ミラー化するソースサーバーおよびターゲットサーバーの両方で、同じポートを使用してください。ミラー化の詳細は、127 ページの「Sun StorageTek 5320 NAS Appliance のミラー化について」を参照してください。
- **Private** – (Sun StorageTek 5320 NAS Cluster Appliance のみ) このポートは、もう 1 台の本体の状態を定期的に監視するのハートビートの専用ポートとして予約されています。

エイリアス IP アドレスの概要

インターネットプロトコル (IP) エイリアス設定は、単一ポートに複数の IP アドレスを割り当てることができるネットワーク機能です。選択したポートに割り当てられたすべての IP エイリアスは、同一の物理ネットワーク上に存在し、選択したポートに最初に指定されたプライマリ IP アドレスと同一の「ネットマスク」および「ブロードキャストアドレス」を共有する必要があります。

サーバー 1 台 (本体 1 台) 構成のユーザーは、各ポートのプライマリ IP アドレスに最大 9 つのエイリアス IP アドレスを追加できます。そのため、2 つのポートを持つ単一のネットワークインタフェースカード (NIC) では、最大 20 個の IP アドレスを使用できます。

Sun StorageTek 5320 NAS Cluster Appliance では、IP エイリアス設定はフェイルオーバー処理に不可欠な要素です。本体 2 台構成のシステムでは、各ポートのプライマリ IP アドレスに、最大 4 つのエイリアス IP アドレスを追加できます。残り 5 つの IP エイリアスは、パートナーサーバーの一次ポートおよびミラーポートのプライマリ IP アドレスおよびエイリアス IP アドレスをバックアップするために予約されています。本体のフェイルオーバーが発生すると、健全なサーバーはこれらの予約済みのバックアップ IP アドレスを使用可能にします。これによって、最小限の中断でネットワークアクセスを継続できます。本体のフェイルオーバーの詳細は、20 ページの「本体のフェイルオーバーの使用可能への切り替え」を参照してください。

サーバー 2 台構成のシステムでは、Primary の役割を割り当てられたポートにのみエイリアス IP アドレスを追加できます。ポートの役割のオプションについては、67 ページの「ポートの位置について」を参照してください。

注: Primary の役割と、プライマリ IP アドレスを混同しないでください。Primary の役割は、Sun StorageTek 5320 NAS Cluster Appliance でポートがどのように機能するかを示す割り当てのことです。プライマリ IP アドレスは、選択したポートに割り当てられる最初のアドレスのことです。Web Administrator では、プライマリ IP アドレスは、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」パネルに表示されます。画面下部でポートの役割を選択できます。

ポートの結合

この節では、ポートの結合について説明します。この節の内容は、次のとおりです。

- 69 ページの「ポート結合について」
- 70 ページの「ポート集約結合について」
- 70 ページの「高可用性結合について」
- 70 ページの「サーバー 1 台構成のシステムでのポート結合」
- 71 ページの「Sun StorageTek 5320 NAS Cluster Appliance でのポートの結合」
- 73 ページの「サーバー 2 台構成でのポート結合の例」

ポート結合について

ポート結合には、ポート集約結合および高可用性結合の 2 種類があります。ポート集約結合では、2 つ以上の隣接するポートを結合することで、以前よりも高速のポートや帯域幅の広いポートが作成されます。高可用性結合では、2 つ以上のポートを結合することで、ネットワークインタフェースカード (NIC) ポートのフェイルオーバーサービスまたはバックアップポートが提供されます。

注: Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムは、802.3ad 仕様のサブセットである EtherChannel 結合をサポートしています。ポート結合を設定する前に、使用しているスイッチのマニュアルで EtherChannel 結合の詳細を確認してください。

システムでは、結合の種類にかかわらず、最大 4 つのポート結合を設定できます。各結合に設定できる最大ポート数は 6 つです。

ポート集約結合について

ポート集約結合（「チャンネル結合」、「集約」、または「トランキンク」とも呼ばれる）では、隣接するポートを結合してネットワーク入出力を拡大します。これによって、帯域幅の狭い 2 つ以上のチャンネルから、帯域幅の広い単一ネットワークチャンネルを形成できます。

集約結合には、2 つ以上の使用可能なポートが必要です。これらのポートのインタフェースタイプは、Fast Ethernet と Fast Ethernet のように、同じである必要があります。また、同一のサブネットに接続され、同一ネットワークスイッチの隣接するポートに接続されている必要もあります。

注: チャンネル結合用に構成されているポートには、IEEE 802.3ad のリンク集約をサポートしているスイッチを接続してください。この機能の構成に関する詳細は、使用する LAN スwitch のマニュアルを参照してください。

高可用性結合について

高可用性 (HA) ポート結合は、ポートのフェイルオーバー機能をシステムに提供します。2 つ以上の使用可能なポートが結合されているため、一次ポートに障害が発生した場合には、高可用性結合に含まれる二次ポートが自動的に作業を引き継ぎます。これによってサービスを中断せずに継続できます。このタイプの結合では、ポート集約結合の場合のように帯域幅は増加しません。

高可用性ポート結合には、2 つ以上の使用可能なポートが必要です。ただし、これらのポートのインタフェースカードタイプが同じである必要はありません。また、隣接するポートに接続されている必要はありません。

注: 高可用性結合にはすべての種類のスイッチを使用できます。ただし、スイッチは同一のサブネットに接続されている必要があります。

サーバー 1 台構成のシステムでのポート結合

この節では、サーバー 1 台構成のシステムでポートを結合する方法について説明します。

ポートは構成後に結合できます。ただし、エイリアスインターネットプロトコル (IP) アドレスおよび元の構成の一部が変更される場合があります。ポート結合を作成したら、22 ページの「ネットワークポートの構成について」を参照してポート結合を構成します。2 つ以上のポートの結合後、個々のポートには IP エイリアスを追加できません。ポート結合にのみ IP エイリアスを追加できます。

サーバー 1 台構成のシステムでポートを結合するには、次の手順を実行します。

1. ナビゲーションパネルで、「Network Configuration」 > 「Bond NIC Ports」を選択します。
2. 「Create」をクリックします。
3. 「Port Aggregation」または「High Availability」をクリックして、作成する結合の種類を指定します。
4. 「Available NIC Ports」フィールドで、結合する使用可能なポートを2つ以上クリックして選択し、「>」をクリックして「NIC Ports in This Bond」リストに追加します。

手順3で「Port Aggregation」を選択した場合、選択するポートのインタフェースタイプは同じである必要があります。また、隣接するポートに接続されているポートを選択する必要があります。

このリストからポートを削除するには、目的のポートを選択して「<」をクリックします。

5. 「IP Address」、「Subnet Mask」、および「Broadcast Address」の各フィールドに必要な情報を入力します。

デフォルトでは、これらのフィールドには「NIC Ports in This Bond」ボックスの最上位に表示される一次ポートの情報が設定されます。

6. 「Apply」をクリックして、ポート結合の処理を完了します。Web Administratorによって、自動再起動の確認を求めるプロンプトが表示されます。

再起動後には、結合されたポートからすべてのエイリアス IP アドレスが削除されています。

エイリアス IP アドレスをポート結合に追加する方法については、23 ページの「ネットワークアダプタの構成」を参照してください。

Sun StorageTek 5320 NAS Cluster Appliance でのポートの結合

サーバー2台構成のシステムでポートを結合する場合は、1台のサーバーに対してのみ次の手順を実行する必要があります。1つのポート結合に含まれるすべてのポートの種類は、Fast Ethernet と Fast Ethernet のように、同じである必要があります。また、同一のサブネットに接続され、同一のネットワークスイッチの隣接するポートに接続されている必要もあります。各ポートの結合後、システムはただちに自動的に再起動します。

ポートは構成後に結合できます。ただし、エイリアスインターネットプロトコル (IP) アドレスおよび元の構成の一部が変更される場合があります。ポート結合を作成したら、22 ページの「ネットワークポートの構成について」を参照してポート結合を構成します。

サーバー 2 台構成でのポート結合の詳細は、73 ページの「サーバー 2 台構成でのポート結合の例」を参照してください。

注: ポート結合には、**Primary** の役割が割り当てられたポートのみを使用できます。ポートの役割の詳細は、67 ページの「ポートの位置について」を参照してください。

サーバー 2 台構成のシステムでポートを結合するには、次の手順を実行します。

1. ナビゲーションパネルで、「**Network Configuration**」 > 「**Bond NIC Ports**」を選択します。

2. 「**Create**」をクリックします。

3. 「**Available NIC Ports**」リストから結合するポートを選択します。リストには、ポート結合に含まれていないすべてのポートが表示されます。

このウィンドウには、リストの最初のポートの「**IP Address**」、「**Subnet Mask**」、および「**Broadcast Address**」フィールドが表示されます。

4. ポートを選択し、「>」をクリックして「**NIC Ports in This Bond**」リストにポートを追加します。

このリストからポートを削除するには、目的のポートを選択して「<」をクリックします。

2 つ以上のポートをリストに追加する必要があります。結合したすべてのポートは、同一のサブネット上にある必要があります。

「**Apply**」をクリックしてサーバーを再起動すると、パートナーサーバーの対応するポートも自動的に結合されます。たとえば、サーバー **H1** のポート 2 と 3 を結合すると、サーバー **H2** のポート 2 と 3 も結合されます。

5. 「**Apply**」をクリックしてポート結合の処理を完了し、システムを再起動します。

システムは自動的に **Bond ID** を新しいポート結合に割り当てます。ポート結合の **IP** アドレスは、結合に最初に追加されたポートのアドレスと同じです。

6. エイリアス **IP** アドレスをポート結合に追加する方法については、23 ページの「**ネットワークアダプタの構成**」を参照してください。

2 つ以上のポートの結合後、個々のポートには **IP** エイリアスを追加できません。ポート結合にのみ **IP** エイリアスを追加できます。

サーバー 2 台構成でのポート結合の例

図 5-1 に、2 つの異なるサブネットに接続された Sun StorageTek 5320 NAS Cluster Appliance の例を示します。可能な組み合わせをすべて示すために、この例では、それぞれの本体が 1 つのハートビートポートと 4 つの追加ポートを備えていることを表しています。各サーバーのハートビートポートを除くすべてのポートには、Primary の役割が設定されています。

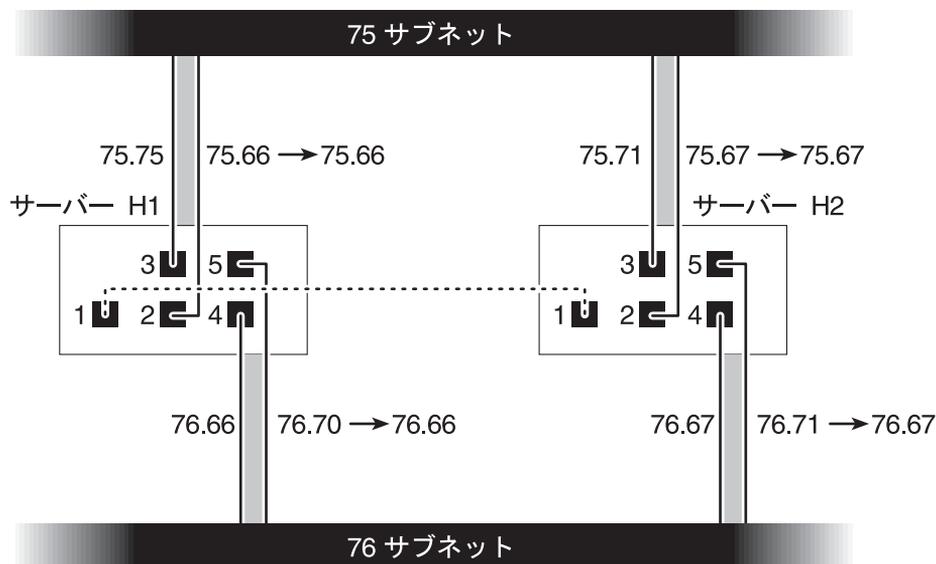


図 5-1 サーバー 2 台構成のポート結合

ポート 2 とポート 3 を結合し、ポート 4 とポート 5 を結合した場合の IP 構成を、表 5-1 に示します。

表 5-1 サーバー 2 台構成のポート結合の例

本体	結合するポート		ポート結合		
	名前	プライマリ IP アドレス	名前	プライマリ IP アドレス	バックアップ IP アドレス
	ポート 2	192.1xx.75.66	結合 1	192.1xx.75.66	192.1xx.75.67
	ポート 3	192.1xx.75.70			
1	ポート 4	192.1xx.76.66	結合 2	192.1xx.76.66	192.1xx.76.67
	ポート 5	192.1xx.76.70			

表 5-1 サーバー 2 台構成のポート結合の例 (続き)

本体	結合するポート		ポート結合		
	名前	プライマリ IP アドレス	名前	プライマリ IP アドレス	バックアップ IP アドレス
2	ポート 2	192.1xx.75.67	結合 1	192.1xx.75.67	192.1xx.75.66
	ポート 3	192.1xx.75.71			
	ポート 4	192.1xx.76.67	結合 2	192.1xx.76.67	192.1xx.76.66
	ポート 5	192.1xx.76.71			

サーバー H1 の各ポートのプライマリインターネットプロトコル (IP) アドレスは、サーバー H2 の対応するポートのバックアップ IP アドレスです。また、その逆も同様です。

本体のフェイルオーバーが発生すると、正常なサーバーが障害の発生したサーバーの IP アドレスを使用可能にします。ポート結合のプライマリ IP アドレスには、エイリアス IP アドレスを追加できます。追加された IP アドレスはフェイルオーバー処理に組み込まれます。IP エイリアスの詳細は、68 ページの「エイリアス IP アドレスの概要」を参照してください。

第6章

Active Directory サービスおよび認証

この章では、Active Directory サービス (ADS) の詳細、LDAP (Lightweight Data Access Protocol) の設定、およびネームサービスの検索順序の変更方法について説明します。その他のネームサービスの設定手順については、25 ページの「ネームサービスの管理」を参照してください。

この章は、次の節で構成されています。

- 75 ページの「サポートされているネームサービスについて」
- 76 ページの「Active Directory サービスの使用法」
- 82 ページの「LDAP の設定」
- 82 ページの「ネームサービスの検索順序の変更」

サポートされているネームサービスについて

Sun StorageTek システムでは、Windows ネットワークおよび UNIX ネットワーク向けの各種ネームサービスをサポートしています。これらのネームサービスを次に示します。

- **ADS** — Active Directory サービス (ADS) は、ドメインネームサービス (DNS) と統合された Windows 2000 のネームサービスです。DNS の詳細は、27 ページの「DNS の設定」を参照してください。ADS はドメインコントローラ上でのみ動作します。ADS は、データを格納および提供するほかに、許可されていないアクセスからネットワークオブジェクトを保護し、1 つのドメインコントローラに障害が発生した場合でもデータが失われないように、ネットワーク全体のオブジェクト

を複製します。ADS を使用可能にして設定を行うと、システムは ADS の更新を自動的に実行するようになります。詳細は、77 ページの「Active Directory サービスについて」を参照してください。

- **LDAP** – LDAP (Lightweight Data Access Protocol) は、認証を使用可能にする UNIX のサービスです。
- **WINS** – Windows インターネットネームサービス (WINS) サーバーは、ネットワーク上のコンピュータがほかの NetBIOS デバイスをよりすばやく効率的に検索できるように、NetBIOS 名をインターネットプロトコル (IP) アドレスに解決します。WINS サーバーは、UNIX 環境の DNS サーバーと同様の機能を Windows 環境で実行します。詳細は、27 ページの「WINS の設定」を参照してください。
- **DNS** – ドメインネームサービス (DNS) は、ドメイン名をシステムの IP アドレスに解決します。このサービスを使用すると、サーバーの IP アドレスまたはサーバー名のいずれかでサーバーを識別できます。詳細は、27 ページの「DNS の設定」を参照してください。
- **NIS** – ネットワーク情報サービス (NIS) は、NIS データベースをインポートするようにシステムを構成します。NIS は、ユーザーグループやホスト情報に基づいてリソースへのアクセスを管理します。詳細は、29 ページの「NIS の設定」を参照してください。
- **NIS+** – ネットワーク情報サービスプラス (NIS+) は、NIS に代わるサービスとして設計されました。NIS+ は NIS クライアントを部分的にサポートしていますが、NIS で解決できなかった問題に対処することを中心に設計されています。主に、NIS+ では資格情報の設定および NIS 機能への安全なアクセスが可能になりました。詳細は、30 ページの「NIS+ の設定」を参照してください。

Active Directory サービスの使用方法

この節では、Active Directory サービス (ADS) のネームスペースと、Web Administrator グラフィカルユーザーインターフェースを介してこのネームスペースを使用する方法について説明します。この節の内容は、次のとおりです。

- 77 ページの「Active Directory サービスについて」
- 77 ページの「ADS の使用可能への切り替え」
- 79 ページの「ネームサービスの検索順序の確認」
- 79 ページの「DNS 構成の確認」
- 80 ページの「ADS での共有の公開」
- 81 ページの「ADS 共有コンテナの更新」
- 81 ページの「ADS からの共有の削除」

Active Directory サービスについて

Active Directory サービス (ADS) は、ドメインネームサービス (DNS) と統合された Windows 2000 のネームサービスです。ADS はドメインコントローラ上でのみ動作します。ADS は、データを格納および提供するほかに、許可されていないアクセスからネットワークオブジェクトを保護し、1つのドメインコントローラに障害が発生した場合でもデータが失われないように、ネットワーク全体のオブジェクトを複製します。

Sun StorageTek システムを Windows 2000 Active Directory サービス環境にシームレスに統合するために、ネットワーク上に必要なものを次に示します。

- Windows 2000 サーバーのドメインコントローラ
- Active Directory が統合された、動的更新が可能な DNS サーバー (動的 DNS 機能を使用するために必要)

注: Active Directory が統合された、動的更新が可能な DNS サーバーを使用することをお勧めしますが、ADS の使用には必要ありません。

401 ページの「「Configure Domains and Workgroups」パネル」を参照して、グラフィカルユーザーインタフェースを介して ADS を使用可能にして構成します。これによって StorEdge ソフトウェアが ADS の更新を自動的に実行できるようになります。

「Configure Domains and Workgroups」パネルで ADS を使用可能にして構成したあと、ADS が ADS ディレクトリで StorEdge の共有を公開できるように設定できます。これを実行するには、406 ページの「「Configure Shares」パネル」を参照して SMB 共有を作成または更新し、公開する各共有に対して共有コンテナを指定します。

ADS の設定では、次の作業を実行します。

1. 77 ページの「ADS の使用可能への切り替え」の説明に従って、ADS を使用可能にします。
2. 79 ページの「ネームサービスの検索順序の確認」の説明に従って、ネームサービスの検索順序を確認します。
3. 79 ページの「DNS 構成の確認」の説明に従って、DNS が使用可能になっており、ADS をサポートするように構成されていることを確認します。
4. 80 ページの「ADS での共有の公開」の説明に従って、ADS で共有を公開します。

ADS の使用可能への切り替え

Active Directory サービス (ADS) を使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Set Time and Date」を選択します。
2. システムの時刻と ADS Windows 2000 ドメインコントローラの時刻の誤差が 5 分以内であることを確認します。
3. 「Apply」をクリックして、変更内容を保存します。

注: 日付および時刻を再設定すると、時間に関連するほとんどの処理で使用されるシステムクロックが変更されます。ライセンス管理ソフトウェアおよび Compliance Archiving Software に使用される固定クロックは変更されません。
4. ナビゲーションパネルで、「Windows Configuration」>「Configure Domains and Workgroups」を選択します。
5. 「Enable ADS」チェックボックスを選択します。
6. 「Domain」に、ADS が動作している Windows 2000 ドメインを入力します。

システムがこのドメインに属している必要があります。
7. 「User Name」フィールドに、管理権限を持つ Windows 2000 ユーザーの名前を入力します。

このユーザーは、ドメイン管理者か、ドメイン管理者グループのメンバーである必要があります。ADS クライアントでは、このユーザーによるセキュリティー保護された ADS の更新が検証されます。

注: このフィールドにドメイン管理者名を入力しても ADS の更新が行われない場合は、ドメインコントローラでドメイン管理者パスワードを変更してください。パスワードの変更は、管理者ユーザーのみが行う必要があります。また、同じパスワードを再使用することもできます。詳細は、Microsoft のサポートサービスの Web サイトで「文書番号 Q248808」を参照してください。
8. 「Password」フィールドに、Windows 2000 管理者ユーザーのパスワードを入力します。
9. 「Container」フィールドに、LDAP (Lightweight Directory Access Protocol) の識別名 (DN) 記法で Windows 2000 管理者ユーザーの ADS のパスを入力します。

ユーザーなどのオブジェクトは、「コンテナ」オブジェクトの各レベルを示す階層的なパスの形式で、Active Directory ドメイン内に格納されます。ユーザーの cn (共通名) フォルダまたは ou (組織単位) フォルダの名前をパスとして入力します。

たとえば、ユーザーが「accounting」という親フォルダ内の「users」フォルダに存在する場合は、次のように入力します。

ou=users,ou=accounting

パスには、ドメイン名を含めないでください。

10. ADS ドメインがサイトを使用する場合は、「Site」フィールドに適切なサイト名を入力します。サイトを使用しない場合は、「Site」フィールドは空白のままにしてください。サイト名を指定すると、ドメインコントローラを選択したときにこのサイトが含まれるようになります。
11. 「Kerberos Realm Info」セクションに、ADS の識別に使用されるレルム名を入力します。
12. これは通常、ADS ドメインまたはドメインネームサービス (DNS) ドメインです。「Apply」をクリックすると、入力した値がすべて大文字に変換されます。
13. 「Server」フィールドに、Kerberos KDC サーバーのホスト名を入力します。
通常、KDC サーバー名は ADS ドメインのメインドメインコントローラのホスト名です。システムが DNS を介して KDC サーバーを検索できる場合は、このフィールドは空白のままでもかまいません。
14. 「Apply」をクリックして、変更内容を保存および適用します。

ネームサービスの検索順序の確認

ネームサービスの検索順序を確認するには、次の手順を実行します。

1. 「UNIX Configuration」 > 「Configure Name Services」を選択します。
2. 「Hosts Order」タブをクリックし、「Services Selected」ボックスのリストに DNS サービスが表示されていることを確認して、ドメインネームサービス (DNS) のネームサービスの検索順序が使用可能になっていることを確認します。
表示されていない場合は、DNS サービスを選択して「>」ボタンをクリックします。
3. (省略可能) 「Services Selected」ボックスの「Up」ボタンと「Down」ボタンを使用して、ネームサービスの検索順序を適切な優先順位に設定します。
この設定により、選択したサービスの走査順序が変更されます。
4. 「Apply」をクリックして、変更内容を保存します。

DNS 構成の確認

ドメインネームサービス (DNS) 構成を確認するには、次の手順を実行します。

1. ナビゲーションパネルで、「Network Configuration」 > 「Configure TCP/IP」 > 「Set Up DNS」を選択します。
2. DNS が使用可能になっていない場合は、「Enable DNS」チェックボックスを選択します。

3. ドメイン名が入力されていない場合は、DNS のドメイン名を入力します。
この名前は、Active Directory サービス (ADS) ドメインと一致させてください。
4. 「Server」フィールドに、システムで使用する DNS サーバーのインターネットプロトコル (IP) アドレスを入力し、「Add」ボタンをクリックしてサーバーのアドレスを「DNS Server List」に追加します。
このリストには、サーバーを 2 台まで追加できます。
5. 「Enable Dynamic DNS」チェックボックスを選択します。
動的 DNS を使用可能にしない場合は、ホスト名および IP アドレスを手動で追加する必要があります。
6. 「DynDNS User Name」フィールドに、セキュリティー保護された動的 DNS の更新の実行に必要な管理権限を持つ Windows 2000 ユーザーの名前を入力します。
DNS サーバーでセキュリティー保護されていない更新が許可されている場合は、このフィールドを空白のままにして保護されていない更新を実行できます。
7. 「DynDNS Password」フィールドに、動的 DNS ユーザーのパスワードを入力します。
8. 「Apply」をクリックして、変更内容を保存します。
動的 DNS が使用可能になっている場合、システムはすぐに自身のホスト名および IP アドレスを使用して DNS を更新します。

ADS での共有の公開

Active Directory サービス (ADS) で共有を公開するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 「Add」をクリックします。
3. 共有名を入力します。
4. (省略可能) 共有についてのコメントを追加します。
60 文字以内の英数字で入力できます。
5. プルダウンボックスから共有するボリュームを選択します。
6. (省略可能) 選択したボリューム上の、共有する既存ディレクトリを「Directory」フィールドに入力します。
注: ディレクトリを指定しない場合は、ルートレベルの共有が作成されます。

7. 「Container」フィールドに、共有が公開される ADS ディレクトリ内の場所を入力します。
「Container」フィールドによって、ADS コンテナが識別されます。共有を公開する ADS の場所を、LDAP の DN 記法で入力します。詳細は、78 ページの手順 9. を参照してください。
8. 「Apply」をクリックして、指定したコンテナに共有を追加します。
注: コンテナ内で共有を公開する場合は、すでに存在しているコンテナを指定してください。システムによって ADS ツリーにコンテナオブジェクトが作成されることはありません。

ADS 共有コンテナの更新

Active Directory サービス (ADS) 共有コンテナを更新するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 更新する共有を選択します。
3. 「Edit」をクリックして、「Edit Share」ウィンドウを表示します。
4. 新しい共有コンテナを入力します。
5. 「Apply」をクリックします。
システムによって共有コンテナが更新されます。

ADS からの共有の削除

Active Directory サービス (ADS) から共有を削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. ADS から削除する共有を選択します。
3. 「Edit」をクリックして、「Edit Share」ウィンドウを表示します。
4. 「Container」フィールドから共有コンテナを削除します。
5. 「Apply」をクリックします。

LDAP の設定

LDAP (Lightweight Data Access Protocol) を使用する前に、LDAP サーバーが動作している必要があります。

LDAP サービスを使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」 > 「Set Up NSSLDAP」を選択します。
2. LDAP を使用可能にするには、「Enable NSSLDAP」チェックボックスを選択します。
3. 「Domain」フィールドに、foo.com などの LDAP サーバーのドメイン名を入力します。
4. 「Password」フィールドに、LDAP サーバーで設定されたパスワードを入力します。
5. 「Server」フィールドに、LDAP サーバーのインターネットプロトコル (IP) アドレスを入力します。
6. 「Proxy」フィールドに、サーバーの設定に応じて、プロキシドメインを入力します。
7. 「Apply」をクリックして設定を保存します。

ネームサービスの検索順序の変更

ネームサービス (NS) の検索順序によって、システムが照会を解決するためにネームサービスを検索する順序が制御されます。これらのネームサービスには、LDAP、NIS、NIS+、DNS、ローカルネームサービスなどがあります。名前解決にこれらのサービスを使用するには、選択したサービスを使用可能にする必要があります。

ユーザー、グループ、ネットグループ、およびホストの検索順序を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」 > 「Configure Name Services」を選択します。
2. 「Users Order」タブをクリックして、ユーザーの検索順序を選択します。
3. 「Services Not Selected」ボックスからサービスを選択します。

4. 「>」をクリックして、選択したサービスを「Services Selected」ボックスに移動します。
ユーザーの検索からサービスを削除するには、サービスを選択して「<」をクリックします。
5. 「Services Selected」ボックス内の各サービスを選択し、「Up」または「Down」ボタンをクリックして上下に移動して、検索サービスの順序を調整します。
リストの最上位にあるサービスが、ユーザーの検索で最初に使用されます。
6. 「Groups Order」タブをクリックして、グループの検索に使用するサービスを選択し、手順 3 ～ 5 を実行します。
7. 「Netgroup Order」タブをクリックして、ネットグループの検索に使用するサービスを選択し、手順 3 ～ 5 を実行します。
8. 「Hosts Order」タブをクリックして、ホストの検索に使用するサービスを選択し、手順 3 ～ 5 を実行します。
9. 「Apply」をクリックして、変更内容を保存します。

第7章

グループ、ホスト、およびファイルディレクトリのセキュリティー

この章では、ローカルグループ、ホスト、ユーザー、およびグループのマッピングと、ファイルディレクトリのセキュリティーに関するさまざまな設定について説明します。この章は、次の節で構成されています。

- 85 ページの「ローカルグループの権限の管理」
- 90 ページの「ホストの構成」
- 93 ページの「ユーザーおよびグループの資格のマッピング」
- 103 ページの「ファイルディレクトリのセキュリティーの設定」

注: Windows のセキュリティーを構成するには、25 ページの「Windows のセキュリティーの構成」を参照してください。

ローカルグループの権限の管理

この節では、ローカルグループの権限の管理について説明します。この節の内容は、次のとおりです。

- 86 ページの「ローカルグループについて」
- 86 ページの「ローカルグループの権限の構成について」
- 88 ページの「所有権の割り当てとグループについて」
- 88 ページの「グループメンバーの追加および削除と権限の構成」
- 89 ページの「グループの NT 権限の構成」

ローカルグループについて

Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムの組み込みローカルグループの要件は、Windows システムのローカルグループの要件とは異なります。ユーザーがネットワーク接続ストレージ (NAS) 機器にローカルでログインすることはありません。すべてのユーザーはネットワークを介して接続し、ドメインコントローラを使用して認証されるため、ユーザーやゲストなどのローカルグループは必要ありません。

注: ローカルグループは、共通インターネットファイルシステム (CIFS) ネットワークにのみ適用されます。

ローカルグループは、主に、リソースの管理およびバックアップ関連の操作の実行に使用します。ローカルグループは、管理者 (Administrators)、パワーユーザー (Power Users)、およびバックアップオペレータ (Backup Operators) の 3 つです。

- **管理者 (Administrators)** — このグループのメンバーは、システム上のファイルおよびディレクトリを完全に管理できます。
- **パワーユーザー (Power Users)** — このグループのメンバーには、システム上のファイルおよびディレクトリの所有権が割り当てられ、ファイルをバックアップおよび復元できます。
- **バックアップオペレータ (Backup Operators)** — このグループのメンバーは、ファイルのセキュリティーを省略して、ファイルをバックアップおよび復元できます。

このシステムでは、認証済みユーザー (Authenticated Users) およびネットワーク (Network) という組み込みグループもサポートされています。すべてのログインユーザーは、自動的に、内部的に管理されるこれらの組み込みグループの両方のメンバーになります。有効な一次ユーザーまたは信頼できるドメインユーザーを、任意の組み込みローカルグループのメンバーとして追加できます。

ローカルグループの権限の構成について

権限は、システム全体に作業の分担を割り当てるための安全なメカニズムを提供します。各権限には、システム管理者によってユーザーまたはグループに割り当てられる明確な役割が設定されています。Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムでは、ローカルのユーザーが存在しないため、権限はグループにのみ割り当てられます。

セキュリティー記述子を使用したオブジェクト単位の許可として割り当てられるアクセス権とは異なり、権限はオブジェクトには依存しません。権限は、オブジェクト単位のアクセス制御リストを無視して、権限の所有者に対して割り当てられた役割の実

行を許可します。たとえば、バックアップオペレータグループのメンバーは、通常のセキュリティーチェックを無視して、通常はアクセス権のないファイルをバックアップおよび復元します。

アクセス権と権限との違いについて、次の定義を使用して説明します。

- アクセス権は、ユーザーまたはグループに対して明示的に付与または禁止されません。アクセス権は、オブジェクト単位で随意アクセス制御リスト (DACL) に許可として割り当てられます。
- 権限は、事前に定義された操作を実行する能力をグループのメンバーに暗黙的に付与する、システム全体での役割です。権限は、オブジェクトレベルのアクセス権より優先され、これを無視します。

表 7-1 に、サポートされる権限を示します。これらの権限のいずれかを任意の組み込みグループに割り当てることができます。任意のドメインユーザーを組み込みグループのメンバーにすることができるため、これらの権限を任意のドメインユーザーに割り当てることができます。

表 7-1 サポートされる権限

権限	説明
ファイルおよびディレクトリのバックアップ	ユーザーに対して、ターゲットのファイルおよびフォルダの読み取りアクセス権を必要とせずに、バックアップの実行を許可します。
ファイルおよびディレクトリの復元	ユーザーに対して、ターゲットのファイルおよびフォルダの書き込みアクセス権を必要とせずに、ファイルの復元を許可します。
ファイルおよびフォルダの所有	ユーザーに対して、所有アクセス権を必要とせずに、オブジェクトの所有を許可します。所有権は、所有者がオブジェクトに割り当てることができる値にのみ設定できます。

表 7-2 に、ローカルの組み込みグループに割り当てられたデフォルトの権限を示します。ローカルの管理者グループのメンバーは任意のファイルまたはフォルダの所有権を取得でき、バックアップオペレータグループのメンバーはバックアップおよび復元操作を実行できます。

表 7-2 デフォルトのグループ権限

グループ	デフォルトの権限
管理者 (Administrators)	所有
バックアップオペレータ (Backup Operators)	バックアップおよび復元
パワーユーザー (Power Users)	なし

所有権の割り当てとグループについて

デフォルトでは、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムがメンバーとして属するドメインの管理者グループは、ローカルの管理者グループのメンバーになっています。そのため、ドメイン管理者で構成されるドメインの管理者グループのメンバーがファイルやフォルダを作成または所有すると、所有権はローカルの管理者グループに割り当てられます。システムをドメイン間で移動させる場合、新しいドメインの管理者グループのメンバーはローカルの管理者グループが所有するオブジェクトにアクセスできるため、最大の移植性が保証されます。

前述の所有権の割り当て規則は、ローカルの管理者グループのメンバーである一般ユーザーにも適用されます。ローカルの管理者グループのメンバーがオブジェクトを作成または所有すると、そのメンバーではなくローカルの管理者グループに所有権が割り当てられます。

Windows システムでは、ドメイン管理者に割り当てられたローカルの管理者グループのメンバーシップが取り消されている場合があります。このような場合、ドメインの管理者グループのメンバーは、一般ユーザーとして扱われます。Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムでは、常にドメイン管理者にローカルの管理者グループのメンバーシップが割り当てられます。ただし、ドメイン管理者がこのグループのメンバーとして一覧に表示されることはないため、このメンバーシップを取り消すことはできません。ローカルユーザーが存在せず、ローカルの Windows 管理者が存在しないために、ドメインの管理者グループが Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムを管理する必要があります。

グループメンバーの追加および削除と権限の構成

「Configure Groups」パネルでは、3つのローカルグループのいずれかに任意のドメインユーザーを追加できます。

グループを追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Groups」を選択します。
2. 「Add Group」をクリックします。
3. 「Group」フィールドにグループの名前を入力します。
4. 「Comment」フィールドに、グループに関する説明またはコメントを入力します。
5. 「Apply」をクリックして、変更内容を保存します。

グループを削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」 > 「Configure Groups」を選択します。
2. 削除するグループを選択します。
3. 「Remove Group」をクリックします。
4. 「Apply」をクリックして、変更内容を保存します。

グループメンバーを追加または削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」 > 「Configure Groups」を選択します。
2. メンバーを追加または削除するグループを強調表示します。
3. 選択したグループの既存のメンバーが「Group Members」ボックスに表示されません。
4. 「Group Members」ボックスで、追加または削除するメンバーを強調表示して、「Add」または「Delete」アイコンをクリックします。
5. 「Apply」をクリックして、変更内容を保存します。

グループの権限を構成するには、「Configure Privileges」パネルを使用します。詳細は、89 ページの「グループの NT 権限の構成」を参照してください。

グループの NT 権限の構成

NT 権限を構成するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」 > 「Configure Groups」を選択します。
2. 「Groups」ボックスで、権限を割り当てるグループを選択します。
3. 「Group Privileges」ボックスで、そのグループに適用する権限の種類を選択します。
4. 「Apply」をクリックして、変更内容を保存します。

ホストの構成

この節では、ホストの構成について説明します。この節の内容は、次のとおりです。

- 90 ページの「ホストの構成について」
- 90 ページの「ホストの追加および編集」
- 92 ページの「ホストグループの追加および編集」

ホストの構成について

「Set Up Hosts」パネルでは、システムホストファイルのエントリを追加、編集、または削除できます。ホスト名、ホストのインターネットプロトコル (IP) アドレス、ホストが信頼できるかどうかなど、ホストの最新情報が表形式で表示されます。



注意: ホストに「信頼できる」(Trusted) の状態を割り当てる場合には注意が必要です。信頼できるホストはファイルシステムにスーパーユーザーの権限でアクセスできるため、そのファイルシステム内のすべてのファイルおよびディレクトリに対して読み取りおよび書き込みアクセスが可能です。

ホストの追加および編集

この節では、ホストの追加および編集について説明します。この節の内容は、次のとおりです。

- 90 ページの「信頼できるホストについて」
- 91 ページの「手動でのホストの追加」
- 91 ページの「ホスト情報の編集」
- 91 ページの「特定のホストのホストマッピングの削除」

信頼できるホストについて

「Set Up Hosts」パネルでは、ホスト情報を表示および編集して、信頼できるホストかどうかを指定できます。ネットワークファイルシステム (NFS) クライアントが信頼できるホストとして定義されており、ファイルへのアクセス権に関係なくすべてのファイルにアクセスできる場合、そのクライアントのスーパーユーザーには、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムに対するスーパーユーザー権限が付与されます。

手動でのホストの追加

ホストを手動でシステム構成に追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Set Up Hosts」を選択します。
2. 「Add」をクリックします。
3. ホスト名を入力します。

これは、システム上でホストが認識される名前です。ホスト名には、英数字 (a ~ z、A ~ Z、0 ~ 9)、「-」(ダッシュ)、および「.」(ピリオド)のみを指定できます。先頭の文字は、英字 (a ~ z または A ~ Z のみ) にする必要があります。

4. 新しいホストのインターネットプロトコル (IP) アドレスを入力します。
5. 必要に応じて、「Trusted」チェックボックスを選択して、ホストに「信頼できる」(Trusted) の状態を割り当てます。

信頼できるホストは、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムにスーパーユーザーでアクセスできます。

6. 「Apply」をクリックして、変更内容を保存します。

ホスト情報の編集

ホスト情報を編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Set Up Hosts」を選択します。
2. 情報を編集するホストを選択して、「Edit」をクリックします。
3. 必要に応じて、ホスト名、インターネットプロトコル (IP) アドレス、および「信頼できる」の状態の情報を変更します。これらのフィールドの詳細は、393 ページの「「Set Up Hosts」パネル」を参照してください。
4. 「Apply」をクリックして、変更内容を保存します。

特定のホストのホストマッピングの削除

特定のホストのホストマッピングを削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Set Up Hosts」を選択します。
2. ホストのリストでエントリをクリックして、削除するホストを選択します。

3. 「Remove」をクリックします。
4. 「Apply」をクリックします。

ホストグループの追加および編集

この節では、ホストグループの追加および編集について説明します。この節の内容は、次のとおりです。

- 92 ページの「ホストグループの追加および編集について」
- 92 ページの「ホストグループの追加」
- 93 ページの「ホストグループへのメンバーの追加」

ホストグループの追加および編集について

「Set Up Hostgroups」パネルでは、ホストグループデータベースを監視および管理できます。このデータベースで、グループおよびグループメンバーの追加または削除を実行できます。ホストグループは、ネットワークファイルシステム (NFS) エクスポートの定義に使用できるホストのコレクションを定義するために使用されます。グループは、定義済みシステムグループとユーザー定義グループで構成されます。「信頼できる」グループと「iso8859」グループの 2 つの定義済みグループがあります。

ホストグループの追加

ホストグループを追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Set Up Hosts」を選択します。
2. 「Groups」メニューの横にある「Add」アイコン () をクリックします。
「Add Hostgroup」ウィンドウが表示されます。
3. ホストグループ名を入力します。
ホストグループ名には、英数字 (a ~ z、A ~ Z、0 ~ 9)、「-」(ダッシュ)、および「。」(ピリオド)のみを指定できます。先頭の文字は、英字 (a ~ z または A ~ Z のみ) にする必要があります。
4. 「Apply」をクリックして、変更内容を保存します。

ホストグループへのメンバーの追加

ホストグループにメンバーを追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」 > 「Configure NFS」 > 「Set Up Hosts」を選択します。
2. 「Group Members」メニューの横にある「Add」アイコン () をクリックします。
「Add Hostgroup Member」ウィンドウが表示されます。
3. 次のいずれかを実行します。
 - ホストネットグループをメンバーとして追加するには、「Host Netgroup」ラジオボタンを選択し、追加するネットグループをドロップダウンメニューから選択します。
 - ホストグループをメンバーとして追加するには、「Host Group」ラジオボタンを選択し、追加するホストネットグループをドロップダウンメニューから選択します。
 - 「Set Up Hosts」パネルから手動で追加したホスト、または NIS サーバー上にメンバーとして存在するホストを追加するには、「Known Host」ラジオボタンを選択し、追加するホストをドロップダウンメニューから選択します。
 - 「Set Up Hosts」パネルから追加していないホストをメンバーとして追加するには、「Other Host」ラジオボタンを選択し、フィールドにホストの名前を入力します。
4. 「Apply」をクリックして、変更内容を保存します。

ユーザーおよびグループの資格のマッピング

この節では、ユーザーまたはグループの資格のマッピングについて説明します。この節の内容は、次のとおりです。

- 94 ページの「ユーザーおよびグループの資格のマッピングについて」
- 94 ページの「UNIX のユーザーおよびグループについて」
- 95 ページの「Windows のユーザーおよびグループについて」
- 96 ページの「資格のマッピングについて」
- 97 ページの「ユーザーマッピングポリシーについて」
- 98 ページの「グループマッピングポリシーについて」
- 100 ページの「組み込みの資格のマッピングポリシーについて」

- 101 ページの「Windows のグループおよびユーザーの、UNIX のグループおよびユーザーへのマッピング」
- 102 ページの「Windows のグループまたはユーザーと UNIX のグループまたはユーザーとのマッピングの編集」

ユーザーおよびグループの資格のマッピングについて

Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムサーバーは、マルチプロトコル環境に存在し、Windows システムと UNIX システムとの間でデータを共有するための統合モデルを提供するように設計されています。Windows システムと UNIX システムの両方からのファイルへの同時アクセスは可能ですが、Windows 環境と UNIX 環境の両方に存在するユーザーを定義するための業界標準のメカニズムは存在しません。いずれかの環境を使用してオブジェクトを作成できますが、それぞれの環境ではアクセス制御の意味に大きな違いがあります。この節では、資格のマッピングについて説明します。ユーザーまたはグループの資格のマッピングと、システム内のセキュリティー保護可能なオブジェクトとの間の相互作用の詳細は、245 ページの「マッピングおよびセキュリティー保護が可能なオブジェクト」を参照してください。

資格のマッピングは、ローカルの構成ファイルまたはネットワーク情報サービス (NIS) データベースで定義された UNIX のユーザーまたはグループと、Windows セキュリティーアカウントマネージャー (SAM) データベースで定義された Windows ドメインのユーザーまたはグループとの間に、対応関係を確立するために使用されます。ユーザーおよびグループのマッピングは、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システム上に資格の対応関係を確立し、いずれかの環境を使用した共通のアクセスを提供するためのメカニズムです。

UNIX のユーザーおよびグループについて

UNIX のユーザーおよびグループは、ローカルの構成ファイル (passwd および group) または ネットワーク情報サービス (NIS) データベースで定義されています。各ユーザーおよびグループは、それぞれ UID または GID と呼ばれる 32 ビットの識別子を使用して識別されます。ほとんどの UNIX システムでは 16 ビットの識別子を使用しますが、16 ビットの数値範囲による制限をなくすため、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムでは 32 ビットに拡張されています。UID または GID は、1 つの UNIX ドメイン内のユーザーまたはグループを一意に識別しますが、複数のドメインにわたって一意性を提供するメカニズムはありません。通常、

値 0 はスーパーユーザーまたはスーパーユーザーグループに適用されます。スーパーユーザーには、管理作業を実行するために、ほぼ無制限のアクセス権が付与されません。

Windows のユーザーおよびグループについて

Windows ユーザーおよびグループは、セキュリティアカウントマネージャー (SAM) データベースで定義されています。各ユーザーおよびグループは、セキュリティ識別子 (SID) で識別されます。SID は可変長の構造を持ち、ローカルドメイン内でも、存在する可能性のあるすべての Windows ドメイン全体でも、ユーザーまたはグループを一意に識別します。

SID の形式は、次のとおりです。

```
typedef struct _SID_IDENTIFIER_AUTHORITY {
    BYTE Value[6];
} SID_IDENTIFIER_AUTHORITY;
typedef struct _SID {
    BYTE Revision;
    BYTE SubAuthorityCount;
    SID_IDENTIFIER_AUTHORITY IdentifierAuthority;
    DWORD SubAuthority[ANYSIZE_ARRAY];
} SID;
```

SID 構造内のフィールドは、表 7-3 に示すように解釈できます。

表 7-3 SID 内のフィールド

フィールド	値
Revision	SID のバージョン。現在のバージョン値は 1 です。
SubAuthorityCount	SID 内の副権限のエントリの数。1 つの SID には、副権限のエントリを最大 15 個含めることができます。
IdentifierAuthority	SID の発行元サブシステムを識別する 6 バイトの配列。
SubAuthority	適切なセキュリティオブジェクト (ドメイン、ユーザー、グループ、またはエイリアス) を一意に識別する、副権限の 32 ビットの配列。ドメイン SID は、すべての権限ドメインの中でドメインを一意に識別します。ユーザー、グループ、またはエイリアスの SID は、適切な相対識別子 (RID) が追加されたドメイン SID です。RID は、32 ビットの識別子で、UNIX のユーザー識別子 (UID) またはグループ識別子 (GID) に類似しています。

わかりやすくするために、SID は、通常、S-1-5-32-500 という形式の文字列として表されます。この SID には、バージョン番号として 1、識別子発行元として 5、副権限として 32 および 500 の 2 つの値が含まれています。値 500 は RID です。

すべての Windows ドメインは一意の SID を持ち、すべての Windows ワークステーションおよび Windows サーバーは、ホスト名と同じ名前前のローカルドメインです。したがって、すべての Windows ワークステーションおよび Windows サーバーは一意の SID を持ちます。複数のマシンにまたがる Windows ドメインは、プライマリドメインコントローラ (PDC) から管理します。PDC は、ドメインのユーザーおよびグループを一元管理する機能を提供し、ドメイン全体に対して一意の SID を定義します。したがって、ユーザー SID のドメインの部分によって、ドメインのユーザーとローカルのワークステーションユーザーとを区別することができます。

Windows ドメインモデルと統合するために、各 Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムでも、そのローカルドメインを定義する SID が生成されます。この SID は 4 つの副権限を作成するアルゴリズムを使用して生成されます。最初の副権限の値は 4 で、一意ではない権限を表します。ほかの 3 つの副権限は、一意性を確実に実現するために、現在の時刻とシステムのいずれかの MAC3 アドレスを含めるアルゴリズムによって生成されます。このドメイン SID に UNIX の UID または GID を追加することによって、この SID は、ローカルユーザーおよびネットワーク情報サービス (NIS) ユーザーの両方を表すために使用されるようになります。この SID は、ローカル SAM データベースと同等のデータベースに保存されます。

資格のマッピングについて

ユーザーおよびグループのマッピングを定義すると、ユーザーは、UNIX システムと Windows システムのどちらからも自身のファイルに確実にアクセスできるようになります。この節では、ユーザーおよびグループのマッピングの自動生成に使用されるアルゴリズム、およびログイン処理中に適用されるポリシーについて説明します。UNIX のユーザーおよびグループを Windows のユーザーおよびグループにマッピングする際のマッピング規則は、システムポリシー設定を介して指定され、具体的なマッピングは、システムポリシーデータベースに格納されます。

各ユーザーマッピングは、特定のユーザー識別子 (UID) を持つ UNIX ユーザーを、特定の相対識別子 (RID) を持つ特定のドメイン内の Windows ユーザーに割り当てる方法を示します。同様に、各グループマッピングは、特定の GID を持つ UNIX グループを、特定の RID を持つ特定のドメイン内の Windows グループに割り当てる方法を示します。

マッピングの形式は、次のとおりです。

```
<UNIX-username>:<UID>:<Windows-username>:<NTDOMAIN>:<RID>
```

```
<UNIX-groupname>:<GID>:<Windows-groupname>:<NTDOMAIN>:<RID>
```

ローカルユーザーおよびローカルグループは、ローカルの `passwd` および `group` ファイルで定義されています。これらのファイルは、次に示すように、標準の UNIX 形式で定義されます。

```
<username>:<password>:<UID>:<GID>:<comment>:<home directory>:<shell>  
<groupname>:<password>:<GID>:<comma-separated-list-of-usernames>
```

ユーザーマッピングポリシーについて

この節では、ユーザーマッピングについて説明します。この節の内容は、次のとおりです。

- 97 ページの「ユーザーマッピングについて」
- 97 ページの「ユーザーマッピングポリシーの設定について」
- 98 ページの「ユーザーマッピングポリシーの例」

ユーザーマッピングについて

ユーザーマッピングは、UNIX ユーザーと Windows ユーザーとの間に対応関係を作成するために使用され、この関係では両方の資格セットがシステムで同等の権限を持つとみなされます。このマッピングメカニズムでは完全に双方向のマッピングがサポートされていますが、システムへの NFS アクセスに関して UNIX ユーザーを Windows ユーザーにマッピングする必要はありません。これは、UNIX ドメインを基本のマッピングドメインとして使用するというポリシー決定があるためです。

Windows ユーザーがシステムにログインするたびに、マッピングファイルが確認されて、そのユーザーの UNIX での資格が決定されます。Windows ユーザーの UNIX ユーザー識別子 (UID) を判定するために、そのユーザーの Windows ドメイン名および Windows ユーザー名に一致する名前がユーザーマップ内で検索されます。一致するものが見つかると、一致したエントリから UNIX UID が取得されます。一致するものがない場合、そのユーザーの UNIX UID は、ユーザーマッピングポリシーの設定に従って決定されます。

ユーザーマッピングポリシーの設定について

ユーザーマッピングポリシーには、次に示す 4 つの設定があります。

- `MAP_NONE` は、Windows ユーザーと UNIX ユーザーの間に事前定義されたマッピングがないことを示します。新しい一意の UNIX ユーザー識別子 (UID) が Windows ユーザーに割り当てられます。現在構成されている `passwd` データベースおよびユーザーマップファイル内を検索され、そこに含まれていない新しい UID が選択されるため、この UID の一意性は検証済みです。通常、新しい UID には、検索で見つかった最大値よりも 1 つ大きい値が使用されます。`passwd` データベースには、ローカルのネットワーク接続ストレージ (NAS) `passwd` ファイル

とネットワーク情報サービス (NIS) passwd ファイル (NIS が使用可能になっている場合) が含まれる場合があります。この場合、Windows ユーザーを既存の UNIX ユーザーにマッピングするには、マッピングエントリを手動で変更する必要があります。

- MAP_ID は、Windows ユーザーの相対識別子 (RID) が UNIX UID になることを示します。passwd データベースは検索されません。
- MAP_USERNAME は、Windows ユーザーのユーザー名を passwd データベースで検索することを示します。Windows ユーザー名と UNIX ユーザー名が一致する場合、一致したエントリから UNIX UID が取得されます。一致しない場合は、MAP_NONE で説明したメカニズムに従って、一意の UNIX UID が生成されます。
- MAP_FULLNAME は、Windows ユーザーの Windows フルネームを passwd データベースで検索することを示します。各パスワードエントリの UNIX コメントのフィールドを使用して一致するものを検索します。passwd データベースのコメントフィールドのフルネームのエントリだけが、Windows フルネームと比較されます。一致するものが見つかり、一致したエントリの UNIX UID が使用されます。一致しない場合は、MAP_NONE メカニズムと同様に、一意の UNIX UID が生成されます。

Windows ユーザーの適切なグループの資格は、グループマッピングのアルゴリズムを使用して取得されます。詳細は、99 ページの「グループマッピングについて」を参照してください。

ユーザーマッピングポリシーの例

次の例は、Windows ユーザー HOMEBASE¥johnm を UNIX ユーザー john に対応付け、Windows ユーザー HOMEBASE¥alanw を UNIX ユーザー amw に対応付けるユーザーマップです。

```
john:638:johnm:HOMEBASE:1031
```

```
amw:735:alanw:HOMEBASE:1001
```

グループマッピングポリシーについて

この節では、グループマッピングについて説明します。この節の内容は、次のとおりです。

- 99 ページの「グループマッピングについて」
- 99 ページの「グループマッピングポリシーの設定について」
- 100 ページの「グループマッピングポリシーの例」

グループマッピングについて

グループマッピングは、UNIX グループと Windows グループとの間に対応関係を作成するために使用されます。Windows ユーザーに対する適切な UNIX グループ識別子 (GID) を決定するには、グループマップでユーザーの Windows ドメイン名と Windows プライマリグループ名を検索します。一致するものが見つかったら、そのマップエントリによって Windows ユーザーのグループが割り当てられる UNIX GID が定義されます。グループマップ内に一致するものがない場合、グループマップポリシーの設定に従って UNIX GID が決定され、グループマップに新しいエントリが作成されます。ただし、MAP_UNIXGID ポリシーは例外です。

グループマッピングポリシーの設定について

グループマッピングポリシーには、次に示す 4 つの設定があります。

- MAP_NONE は、Windows グループと UNIX グループの間に事前設定されたマッピングがないことを示します。新しい一意の UNIX グループ識別子 (GID) がグループに割り当てられます。現在構成されている group データベースおよび group マップファイル内を検索され、検出された最大値よりも 1 つ大きい値である GID が選択されるため、この GID の一意性は検証済みです。group データベースには、ローカルのネットワーク接続ストレージ (NAS) group ファイルとネットワーク情報サービス (NIS) group ファイル (NIS が使用可能になっている場合) が含まれる場合があります。この場合、Windows グループを既存の UNIX グループにマッピングするには、マッピングエントリを手動で変更する必要があります。
- MAP_ID は、ユーザーのアクセストークンで検出された Windows ユーザーのグループ相対識別子 (RID) が UNIX GID になることを示します。
- MAP_GROUPNAME は、Windows ユーザーのグループ名を group データベースで検索することを示します。一致するものが見つかったら、一致したエントリから UNIX GID が取得されます。一致しない場合は、一意の UNIX GID が生成されません。
- MAP_UNIXGID は、Windows ユーザーの UNIX グループが、ユーザーマッピング操作中に取得された passwd エントリの一次 GID フィールドで決定されることを示します。

この場合、group.map ファイルは照会されません。GID を決定できない場合は、UNIX の nobody グループ GID (60001) が使用されます。

最後の手順は、ユーザーが所属する UNIX グループのリストを決定することです。ユーザーマッピング処理の場合と同様に、group データベースで UNIX ユーザー名が検索されます。その UNIX ユーザー名が含まれている各グループの GID が、グループリストのそのユーザーの資格内に追加されます。

グループマッピングポリシーの例

次の例は、`HOMEBAASE\Domain Admins` グループを UNIX の `wheel` グループに対応付け、`HOMEBAASE\Domain Users` グループを UNIX の `users` グループに対応付けるグループマップです。

```
wheel:800:Domain Admins:HOMEBAASE:1005
```

```
users:100:Domain Users:HOMEBAASE:513
```

システムのデフォルトのマッピング規則は、ユーザーとグループのどちらに対しても `MAP_NONE` です。

```
map.users=MAP_NONE
```

```
map.groups=MAP_NONE
```

ユーザーマッピング規則とグループマッピング規則を同一にする必要はありません。実際に使用される可能性のあるマッピング構成の例を、次に示します。この例のユーザーマッピング規則は `MAP_USERNAME` で、グループマッピング規則は `MAP_ID` です。

```
map.users=MAP_USERNAME
```

```
map.groups=MAP_ID
```

組み込みの資格のマッピングポリシーについて

この節では、組み込みの資格のマッピングについて説明します。この節の内容は、次のとおりです。

- 100 ページの「組み込みの資格のマッピングについて」
- 101 ページの「マッピングポリシーの定義」

組み込みの資格のマッピングについて

UNIX のスーパーユーザー識別子の 0 (ユーザー識別子 (UID) またはグループ識別子 (GID)) は、常にローカルの管理者グループにマップされます。ローカルの管理者グループのセキュリティ識別子 (SID) は、`S-1-5-32-544` という組み込み (定義済み) の Windows SID です。このマッピングは、ドメイン管理者が作成したファイルに対して Windows が割り当てる所有権に一致しています。このようなファイルの所有権は、常に組み込みのローカルの管理者グループに割り当てられるため、ドメインの独立性が保たれます。つまり、システムが Windows ドメイン間で移動された場合でも、これらのファイルにアクセスできなくなることを防ぎます。この SID は、Windows の権限表示ボックスには `HOSTNAME¥Administrators` と表示されます。HOSTNAME は、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムのホスト名になります。

マッピングポリシーの定義

マッピングポリシーを定義するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」 > 「Manage SMB/CIFS Mapping」 > 「Configure Mapping Policy」を選択します。
2. 「Windows <--> UNIX User Mapping Choice」セクションで、ユーザーマッピングの設定を選択します。この設定の詳細は、パネルの「ヘルプ」ボタンをクリックするか、404 ページの「「Configure Mapping Policy」パネル」を参照してください。
3. 「Windows <--> UNIX Group Mapping Choice」セクションで、グループマッピングの設定を選択します。この設定の詳細は、パネルの「ヘルプ」ボタンをクリックするか、404 ページの「「Configure Mapping Policy」パネル」を参照してください。
4. 「Apply」をクリックして、変更内容を保存します。

ユーザーまたはグループの資格のマッピングと、システム内のセキュリティー保護可能なオブジェクトとの相互作用の詳細は、245 ページの「マッピングおよびセキュリティー保護が可能なオブジェクト」を参照してください。

Windows のグループおよびユーザーの、UNIX のグループおよびユーザーへのマッピング

Windows のグループおよびユーザーを UNIX のグループおよびユーザーにマッピングするには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」 > 「Manage SMB/CIFS Mapping」 > 「Configure Maps」を選択します。
2. 「Add」をクリックします。
3. 「NT User」ボックスで、次の情報を入力します。
 - **Account** – マッピングするユーザーまたはグループの NT アカウント名を入力します。
 - **RID** – NT ドメイン内で NT ユーザーまたはグループを一意に識別する相対識別子を入力します。
4. 「UNIX User」ボックスで、次の情報を入力します。
 - **Name** – 指定した NT ユーザーまたはグループをマッピングする UNIX ユーザーまたはグループの名前を入力します。
 - **ID** – UNIX ドメイン内で UNIX ユーザーまたはグループを一意に識別する識別子を入力します。

5. 「Apply」をクリックして、変更内容を保存します。

ユーザーまたはグループの資格のマッピングと、システム内のセキュリティー保護可能なオブジェクトとの相互作用の詳細は、245 ページの「マッピングおよびセキュリティー保護が可能なオブジェクト」を参照してください。

Windows のグループまたはユーザーと UNIX のグループまたはユーザーとのマッピングの編集

Windows のグループまたはユーザーと UNIX のグループまたはユーザーとのマッピングを編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」 > 「Manage SMB/CIFS Mapping」 > 「Configure Maps」を選択します。
2. 編集するマッピングの種類に応じて、「Users」または「Groups」を選択します。
3. 表の中で、編集するマッピングをクリックし、「Edit」をクリックします。
「Edit SMB/CIFS Group Map」ウィンドウが表示されます。
4. 「NT User」ボックスまたは「NT Group」ボックスで、任意で次の情報を編集します。
 - **Account** – 現在マッピングされているユーザーまたはグループの NT アカウント名を編集します。
 - **RID** – NT ドメイン内で NT ユーザーまたはグループを一意に識別する相対識別子を編集します。
5. 「Unix User」ボックスまたは「Unix Group」ボックスで、任意で次の情報を編集します。
 - **Name** – 指定した NT ユーザーまたはグループに現在マッピングされている UNIX ユーザーまたはグループの名前を編集します。
 - **ID** – UNIX ドメイン内で UNIX ユーザーまたはグループを一意に識別する識別子を編集します。
6. 「Apply」をクリックして、変更内容を保存します。
ユーザーまたはグループの資格のマッピングと、システム内のセキュリティー保護可能なオブジェクトとの相互作用の詳細は、245 ページの「マッピングおよびセキュリティー保護が可能なオブジェクト」を参照してください。

ファイルディレクトリのセキュリティの設定

ファイルディレクトリのセキュリティを設定するには、次の2つの方法があります。

- 103 ページの「ワークグループモードでのファイルディレクトリのセキュリティの設定について」
- 103 ページの「ドメインモードでのファイルディレクトリのセキュリティの設定」

ワークグループモードでのファイルディレクトリのセキュリティの設定について

ワークグループ/セキュリティ保護された共有モードでは、**Web Administrator** を使用してすべてのセキュリティが共有自体に設定されます。これは、共有レベルセキュリティと呼ばれます。

ワークグループモードでは、システムはクライアント上で認証が実行されないことを前提として、共有接続が要求されるたびに、パスワードを使用したアクセス権の確認を明示的に求めます。

共有を追加する際の共有レベルセキュリティの設定については、108 ページの「静的共有の構成」を参照してください。共有を編集する際の共有レベルセキュリティの設定については、110 ページの「既存の SMB 共有の編集」を参照してください。

ドメインモードでのファイルディレクトリのセキュリティの設定

Windows 2000 または Windows XP からのアクセス権のみを管理できます。

注: システムがドメインモードで構成されている場合、オブジェクトアクセス権の設定は、標準の Windows ドメインコントローラでのオブジェクトアクセス権と同様に処理されます。サーバーを検索してドライブを割り当てて、共有のアクセス権を設定および管理するには、適切な方法がいくつかあります。ここでは、この処理の一例を示します。

注: Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムは、ファイルおよびディレクトリのセキュリティーのみをサポートしており、共有にセキュリティーを設定すると、配下のディレクトリにそのセキュリティーの割り当てが渡されます。

ドメインモードでファイルディレクトリのセキュリティーを設定するには、次の手順を実行します。

1. Windows エクスプローラを起動します。
2. 「Tools」 > 「Map Network Drive」 をクリックします。
3. 「Map Network Drive」 ウィンドウで、「Drive」 プルダウンメニューボックスからドライブ文字を選択します。
4. Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムを検索して選択します。
5. 「OK」 をクリックします。
6. Windows エクスプローラウィンドウで、ユーザーレベルのアクセス権を定義するシステム共有を右クリックします。
7. プルダウンメニューから「Properties」 を選択します。
8. 「Properties」 ウィンドウで「Security」 タブを選択します。
9. 「Permissions」 ボタンをクリックします。
10. 必要なアクセス権を設定します。
アクセス権の設定については、Windows のマニュアルを参照してください。
11. 「OK」 をクリックします。

第8章

共有、割り当て、およびエクスポート

この章では、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システム上のファイルおよびボリュームへのユーザーアクセスを制御するさまざまな方法について説明します。

この章の内容は、次のとおりです。

- 105 ページの「共有の管理」
- 114 ページの「割り当ての管理」
- 120 ページの「NFS エクスポートの設定」

共有の管理

この節では、共有の管理について説明します。この節の内容は、次のとおりです。

- 106 ページの「共有について」
- 106 ページの「静的共有について」
- 107 ページの「共有へのアクセス権について」
- 108 ページの「静的共有の構成」
- 112 ページの「SMB/CIFS クライアントの構成について」
- 113 ページの「自動ホーム共有について」
- 113 ページの「自動ホーム共有の使用可能への切り替え」

共有について

共通インターネットファイルシステム (CIFS) は、Microsoft のサーバーメッセージブロック (SMB) プロトコルの拡張バージョンです。SMB/CIFS を使用すると、Windows 環境のクライアントシステムから Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システム上のファイルにアクセスできます。

共有リソース、つまり共有は、ネットワーク上の Windows クライアントがアクセスできるサーバー上のローカルリソースです。共有は通常、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システム上では、ファイルシステムボリューム、またはボリューム内のディレクトリツリーとして存在します。各共有は、ネットワーク上で名前によって識別されます。ネットワーク上のクライアントに対しては、共有はサーバー上の完全なボリュームとして表示され、共有のルートのすぐ上のローカルディレクトリのパスは表示されません。

注: 共有およびその他のディレクトリは、独立したエンティティです。共有を削除しても、配下のディレクトリには影響しません。

共有は、通常、ネットワークファイルサーバー上のホームディレクトリにネットワークアクセス権を付与するために使用します。各ユーザーは、ファイルボリューム内のホームディレクトリに割り当てられます。

共有には、静的 SMB/CIFS 共有と自動ホーム SMB/CIFS 共有の 2 種類があります。静的共有は、ユーザーがサーバーに接続しているかどうかに関係なく定義されている永続的な共有です。自動ホーム共有は、ユーザーがシステムにログインすると作成され、ログアウトすると削除される、一時的な共有です。

ユーザーがシステムを参照すると、静的に定義された共有と、接続中のユーザーに対する自動ホーム共有だけが表示されます。

静的共有について

静的共有が作成されると、ユーザーのホームディレクトリをクライアントワークステーション上のネットワークドライブとして割り当てることができます。たとえば、vol1 というボリュームに、home という名前のホームディレクトリ、および bob と sally というユーザーのサブディレクトリを含めることができます。この共有は、次の表に示すように定義します。

表 8-1 共有のパスの例

共有の名前	ディレクトリのパス
bob	/vol1/home/bob
sally	/vol1/home/sally

システムへのアクセス権を持つ各 Windows ユーザーに対して静的ホームディレクトリの共有を定義および保持することが難しい場合は、自動ホーム機能を使用できません。詳細は、113 ページの「自動ホーム共有について」を参照してください。

共有へのアクセス権について

「Configure Shares」パネルで「Add」をクリックして共有を追加する場合は、その共有に対する umask アクセス権を指定するオプションを使用できます。umask 機能は、その共有内の新しいディレクトリおよびファイルに対するアクセス権の設定に使用される、3桁の数字です。

umask の 3桁の数字のうち、1桁めは所有者、2桁めはグループ、3桁めは全ユーザーのアクセス権を指定します。各桁は、読み取り権、書き込み権、および実行権を指定する 3つのビットで構成されます。ビット 1 は有効、ビット 0 は無効を指定します。

たとえば、3つのビットをすべて有効 (111) にすると、読み取り権、書き込み権、および実行権が付与されます。8進数で「111」に相当する値は「7」であるため、「Configure Shares」パネルからアクセスできる「Umask」オプションボックスに「7」と入力します。したがって、「Umask」ボックスに「777」と入力すると、所有者、グループ、および全ユーザーに読み取り権、書き込み権、および実行権がすべて付与されます。「700」と入力すると、所有者のみに読み取り権、書き込み権、および実行権が付与されます。

注: ファイル作成要求で DOS の読み取り専用属性が設定されていると、「Umask」オプションの適用時にすべての書き込みビットが無効 (0) に切り替えられます。次の表にこの点を示します。

表 8-2 DOS の読み取り専用属性が設定されている場合の umask アクセス権

umask	新規ディレクトリのアクセス権		新規ファイルのアクセス権	
	DOS RW	DOS RO	DOS RW	DOS RO
000	777 (rwxrwxrwx)	777 (rwxrwxrwx)	666 (rw-rw-rw)	444 (r--r--r--)
777	000 (-----)	000 (-----)	000 (-----)	000 (-----)
022	755 (rwxr-xr-x)	755 (rwxr-xr-x)	644 (rw-r--r--)	444 (r--r--r--)
002	775 (rwxrwxr-x)	775 (rwxrwxr-x)	664 (rw-rw-r--)	444 (r--r--r--)

静的共有の構成

この節では、静的共有の構成について説明します。この節の内容は、次のとおりです。

- 108 ページの「静的共有の構成について」
- 108 ページの「静的共有の作成」
- 110 ページの「既存の SMB 共有の編集」
- 111 ページの「SMB/CIFS 共有の削除」

静的共有の構成について

「Configure Shares」パネルを使用して、静的 Microsoft サーバーメッセージブロック (SMB) 共有を追加、表示、および更新します。

「Configure Shares」パネルの上部の表には、すべての既存の SMB 共有に関する情報が表示されます。この情報には、共有の名前、共有化されたディレクトリ、コンテンツ名、およびデスクトップデータベースの呼び出しのほかに、Windows ワークグループのみにに関する情報 (ユーザー、グループ、umask、およびパスワードの情報) が含まれます。

注: ボリュームまたはディレクトリを共有するには、そのボリュームまたはディレクトリがすでに存在する必要があります。

デフォルトでは、各ボリュームのルートに隠し共有が作成され、ドメイン管理者のみがアクセスできます。通常、これらの共有は、データの移行およびディレクトリ構造の作成を行うために管理者が使用します。共有名は「Configure Shares」画面で確認できます。ユーザーの共有はこの手順のあと作成されます。これはボリュームのルートの下でディレクトリを共有するとセキュリティ管理が容易になるためです。

静的共有の作成

共有を作成する前に、ファイルボリュームを作成する必要があります。詳細は、46 ページの「ファイルボリュームまたはセグメントの作成について」を参照してください。

新しい Microsoft サーバーメッセージブロック (SMB) 共有を追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 「Add」をクリックします。
3. 「Share Name」フィールドに、追加する共有の名前を入力します。

4. (任意) 共有についての説明を「Comment」に入力します。
5. 「Mac Ext.」セクションで「Desktop DB Calls」チェックボックスを選択して、システムが Macintosh デスクトップデータベースにアクセスして情報を設定できるようにします。
6. 「Volume Name」プルダウンメニューに表示された選択可能なボリュームのリストから、共有するボリュームを選択します。
7. 「Directory」フィールドに既存のディレクトリを入力します。

このフィールドではディレクトリを作成できません。ディレクトリの名前は大文字と小文字が区別されます。

注: 「Directory」フィールドは、空白のままにしないでください。
8. (省略可能) 「Set Up ADS」パネルで ADS を使用可能にした場合、「Container」フィールドに共有の ADS パス位置を入力して、共有を公開する ADS コンテナを指定します。詳細は、80 ページの「ADS での共有の公開」を参照してください。
9. ユーザー ID、グループ ID、およびパスワードがある場合は、これらを入力します。

「User ID」、「Group ID」、および「Password」フィールドは、NT ドメインモードではなく Windows ワークグループモードを使用可能にしている場合にのみ使用できます。Windows のセキュリティーモデルを使用可能にする方法については、25 ページの「Windows のセキュリティーの構成」を参照してください。

Windows ワークグループは、共有レベルセキュリティーを使用します。この画面に表示されるユーザー ID (UID)、グループ ID (GID)、およびパスワードの各フィールドは、Windows ワークグループのユーザーが Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムファイルの所有およびアクセスを行うための唯一のセキュリティー手段となります。つまり、ディレクトリに対する権限は、ユーザーではなく、共有の定義によって判断されます。システムは、クライアントが認証を実行しないことを前提として、共有接続が要求されるたびに、パスワードを使用したアクセス権の確認を明示的に求めます。

同一のディレクトリに対して、UID、GID、およびパスワードが異なる複数の共有を作成できます。その後、各ユーザーに対して特定の共有のパスワードを発行できます。割り当てを使用して、ファイルボリュームの容量またはファイルの数について個々のユーザーおよびグループに対する制限値を管理することもできます。割り当ての詳細は、114 ページの「割り当ての管理について」を参照してください。



注意: 「User ID」フィールドに、指定されたディレクトリへのアクセスにこの共有を使用するユーザーの UID を入力してください。このフィールドのデフォルト値は 0 (ゼロ) です。これは、UNIX のスーパーユーザーの値です。ただし、この値を割り当てる場合には注意が必要です。Windows ワークグループモードでは、このフィールドに 0 を入力すると、共有内のすべてのファイルおよびディレクトリに対するセキュリティーがすべて使用不可になります。

- **R/W Password** — この共有に指定したディレクトリに対する読み取り/書き込みアクセス権のある Windows ワークグループのユーザーのパスワードを入力します。
 - **Confirm R/W Password** — 確認のために、読み取り/書き込みパスワードを再入力します。
 - **R/O Password** — 共有に対する読み取り専用アクセス権のある Windows ワークグループのユーザーのパスワードを入力します。
 - **Confirm R/O Password** — 確認のために、読み取り専用パスワードを再入力します。
10. この共有にファイル生成マスクを適用する場合、「Umask」フィールドにマスクを入力します。
- umask は、共有モードで作成されるファイルおよびディレクトリのセキュリティポリシーを定義します。これによって、ファイルの作成時に使用不可になるアクセス権ビットが指定されます。
- umask は 8 進数で定義されます。8 進数は 3 バイトで構成されるため、UNIX ファイルのアクセス権の表記に簡単にマッピングできます。umask は、DOS 読み取り専用属性を除いて、標準の UNIX 規則を使用して適用されます。ファイルの作成時に DOS 読み取り専用属性を設定している場合、umask の適用後にすべての書き込みビットがファイルのアクセス権から削除されます。
- 次の表に、DOS 読み取り専用属性の影響を含む、アクセス権への umask の適用例を示します。詳細は、107 ページの「共有へのアクセス権について」を参照してください。
11. 「Apply」をクリックして、変更内容を保存します。

既存の SMB 共有の編集

既存の Microsoft サーバーメッセージブロック (SMB) 共有を編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 更新する共有を選択します。
3. 「Edit」をクリックします。
4. (省略可能) 旧共有名を変更する場合は、新しい名前を「Share Name」フィールドに入力します。
5. (省略可能) 「Comment」フィールドで共有についての説明を変更します。60 文字以内の英数字で入力できます。

6. 「Mac Extensions」セクションで「Desktop DB Calls」チェックボックスを選択して、システムが Macintosh デスクトップデータベースにアクセスして情報を設定できるようにします。
これによって、Macintosh クライアントのファイルへのアクセスが高速化し、Macintosh 以外のクライアントによる Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システム上の Macintosh ファイルへのアクセスが可能になります。
7. 共有のパスを変更するには、「Path」フィールドに既存のディレクトリの名前を入力します。
このフィールドではディレクトリを作成できません。ディレクトリの名前は大文字と小文字が区別されます。
8. 必要に応じて、新しいコンテナを入力します。
「Container」フィールドでは、共有を公開する Active Directory サービス (ADS) コンテナを指定します。「Set Up ADS」パネルで ADS が使用可能になっている場合にのみ、このフィールドを使用できます。LDAP の DN 記法で共有の ADS パスを入力します。詳細は、77 ページの「ADS の使用可能への切り替え」を参照してください。
9. ユーザー ID、グループ ID、およびパスワードがある場合は、これらを入力します。
これらのフィールドの詳細は、パネルの「ヘルプ」ボタンをクリックするか、397 ページの「Add/Edit Share」ウィンドウを参照してください。
10. (省略可能) 「Umask」フィールドに指定した規則を使用して、umask の設定を変更します。詳細は、107 ページの「共有へのアクセス権について」を参照してください。
11. 「Apply」をクリックして、変更内容を保存します。

SMB/CIFS 共有の削除

Microsoft サーバーメッセージブロック (SMB) または共通インターネットファイルシステム (CIFS) 共有を削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Shares」を選択します。
2. 共有の表から削除する共有を選択します。
3. 「Remove」をクリックします。
4. 「Apply」をクリックして、共有を削除します。

SMB/CIFS クライアントの構成について

セキュリティおよびネットワークの設定の構成が完了すると、ローカルネットワーク上のマスターブラウザで自動的に登録され、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムが Microsoft サーバーメッセージブロック (SMB) クライアントまたは共通インターネットファイルシステム (CIFS) クライアントに対して表示されるようになります。

クライアントは、次のいずれかの方法で接続します。

■ Windows 98、XP、および Windows NT 4.0

ユーザーは、Windows エクスプローラを使用してネットワークドライブを割り当てるか、「Network Neighborhood」ウィンドウで Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムのアイコンをクリックすることによって接続します。

ユーザーがネットワークドライブを割り当てる場合は、`\\computer_name\share_name` のようにコンピュータの名前と共有の名前で構成された Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムの汎用命名規則 (UNC) パスが必要です。「Network Neighborhood」を使用して接続する場合は、ネットワーク上で Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムを識別するために使用されるシステム名が必要です。

■ Windows 2000、XP、および 2003

Active Directory サービス (ADS) がインストールされていない場合、ユーザーは Windows エクスプローラを使用してネットワークドライブを割り当てるか、「My Network Places」ウィンドウで Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムのアイコンをクリックすることによって接続します。

ユーザーがネットワークドライブを割り当てる場合は、`\\computer_name\share_name` のようにコンピュータの名前と共有の名前で構成された Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムの UNC パスが必要です。「Network Neighborhood」を使用して接続する場合は、ネットワーク上で Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムを識別するために使用されるシステム名が必要です。

ADS がインストールされている場合は、ADS に公開されている Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムの共有をクリックすることによって接続できます。

■ DOS

ユーザーは `net use` コマンドを入力して、コマンド行でドライブ文字に共有を割り当ててください。¥¥computer_name¥¥share_name のようにコンピュータの名前と共有の名前で構成された Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムの UNC パスが必要です。

自動ホーム共有について

Microsoft サーバーメッセージブロック (SMB) または共通インターネットファイルシステム (CIFS) の自動ホーム共有機能を使用すると、システムにアクセスする各 Windows ユーザーに対してホームディレクトリの共有を定義し、保持するための管理作業が不要になります。ユーザーがログインするとシステムによって自動ホーム共有が作成され、ログアウトすると削除されます。これによって、ユーザーアカウントを保持するために必要な管理作業が減少し、サーバーリソースの効率が向上します。

自動ホーム機能を構成するには、この機能を使用可能にして、自動ホームパスを指定します。自動ホームパスとは、ディレクトリ共有のベースディレクトリのパスです。たとえば、ユーザーのホームディレクトリが `/vol1/home/sally` の場合、自動ホームパスは `/vol1/home` です。一時的な共有の名前は `sally` になります。ユーザーのホームディレクトリの名前は、ユーザーのログイン名と同じである必要があります。

ユーザーがログインすると、サーバーはユーザーの名前と一致するサブディレクトリを確認します。一致するサブディレクトリが検出され、その共有が存在しない場合、一時的な共有が追加されます。ユーザーがログアウトすると、サーバーはその共有を削除します。

動作していない状態が 15 分間続くと、Windows クライアントによってユーザーが自動的にログアウトされる場合があります。その結果、公開済みの共有のリストに自動ホーム共有が表示されなくなります。これは、CIFS プロトコルの通常の動作です。ユーザーがサーバー名をクリックするか、エクスプローラウィンドウなどでシステムへのアクセスを試みると、共有が自動的に再表示されます。

注: システムが再起動すると、すべての自動ホーム共有が削除されます。

自動ホーム共有は自動的に作成および削除されるため、この機能を使用可能にすることによってほとんどの構成が行われます。

自動ホーム共有の使用可能への切り替え

注: Active Directory 管理ツールを使用してユーザーのホームディレクトリを構成すると、自動ホームパスを検出できないことを示す警告が表示されます。この自動ホーム共有はユーザーがログオンすると作成されるため、このメッセージは無視してかまいません。

自動ホーム共有を使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」>「Configure Autohome」を選択します。
2. 「Enable Autohome」チェックボックスを選択します。
3. 自動ホームパスを入力します。
パスの詳細は、113 ページの「自動ホーム共有について」を参照してください。
4. ADS コンテナを入力します。
詳細は、77 ページの「Active Directory サービスについて」を参照してください。
5. 「Apply」をクリックして、変更内容を保存します。

割り当ての管理

この節では、割り当ての管理について説明します。この節の内容は、次のとおりです。

- 114 ページの「割り当ての管理について」
- 115 ページの「ユーザーおよびグループの割り当ての構成」
- 118 ページの「ディレクトリツリー割り当ての構成」

割り当ての管理について

「Manage Quotas」パネルでは、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムのファイルボリュームおよびディレクトリに対する割り当てを管理できます。ユーザーおよびグループの割り当ては、ユーザーまたはグループが使用可能なディスク容量、およびユーザーまたはグループがボリュームに書き込み可能なファイルの数を決定します。ディレクトリツリー割り当ては、特定のディレクトリで使用可能な容量か、そのディレクトリに書き込み可能なファイルの数、あるいはその両方を決定します。

ユーザーおよびグループに対する容量およびファイル数の制限値の設定については、115 ページの「ユーザーおよびグループの割り当ての構成について」を参照してください。特定のディレクトリに対する容量およびファイル数の制限値の設定については、118 ページの「ディレクトリツリー割り当ての構成について」を参照してください。

ユーザーおよびグループの割り当ての構成

この節では、ユーザーおよびグループの割り当ての構成について説明します。この節の内容は、次のとおりです。

- 115 ページの「ユーザーおよびグループの割り当ての構成について」
- 115 ページの「ファイルボリュームに対する割り当ての使用可能への切り替え」
- 116 ページの「ユーザーまたはグループの割り当ての追加」
- 116 ページの「ユーザーまたはグループの割り当ての編集」
- 117 ページの「ユーザーまたはグループの割り当ての削除」

ユーザーおよびグループの割り当ての構成について

「Configure User and Group Quotas」パネルでは、NT および UNIX のユーザーやグループに対するボリュームの割り当てを管理できます。このパネルには、選択したボリュームに対するスーパーユーザー、デフォルトのユーザー、および個別のユーザー、またはこれらのユーザーのグループへの割り当てが表示されます。デフォルトのユーザーおよびデフォルトのグループの設定は、個別の割り当てが設定されていないすべてのユーザーおよびグループに使用される設定です。

「強い制限値」とは、ユーザーまたはグループが使用できる絶対最大容量です。

「弱い制限値」は、強い制限値以下の値に設定されており、この制限値に達すると7日間の猶予期間に入ります。この猶予期間が過ぎると、ユーザーまたはグループは、使用済みの領域が弱い制限値より小さくなるまでボリュームへの書き込みを行うことができなくなります。

強い制限値は、弱い制限値以上の値に設定する必要があります。ディスク容量で設定する場合、最大値は約 2T バイトです。ファイル数で設定する場合、強い制限値の最大値は 40 億個です。

スーパーユーザーおよびスーパーユーザーグループは、容量またはファイル数の強い制限値や弱い制限値が適用されないように自動的に設定されます。また、これらに割り当てを定義することはできません。

ファイルボリュームに対する割り当ての使用可能への切り替え

ファイルボリュームに対して割り当てを使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Edit Volume Properties」を選択します。

2. 「Volume Name」プルダウンメニューから、割り当てを使用可能にするファイルボリュームを選択します。
3. 「Enable Quotas」ボックスにチェックマークが付いていることを確認します。付いていない場合、このボックスを選択します。
4. 「Apply」をクリックします。

ユーザーまたはグループの割り当ての追加

ユーザーまたはグループの割り当てを追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Manage Quotas」 > 「Configure User and Group Quotas」を選択します。
2. ユーザーの割り当てを構成する場合は、「Users」をクリックします。グループの割り当てを構成する場合は、「Groups」をクリックします。
3. 「Volume」ドロップダウンリストから、割り当てを追加するファイルボリュームの名前を選択します。
この画面の表には、選択したファイルボリュームに対するスーパーユーザー、デフォルトのユーザー、および個別のユーザー、またはこれらのユーザーのグループへの割り当てが表示されます。
4. ユーザーまたはグループの割り当てを追加するには、「Add」をクリックします。
5. 適切なオプションボタンをクリックして、指定したユーザーまたはグループが UNIX 環境と NT 環境のどちらに属しているかを選択します。
6. 適切なユーザー名またはグループ名を選択します。NT ユーザーまたは NT グループの場合には、ドメイン名もあわせて選択します。
7. 選択したユーザーまたはグループのディスク容量の制限値を設定します。ディスク容量の制限値の詳細は、ウィンドウの「ヘルプ」ボタンをクリックするか、323 ページの「「Add/Edit Quota Setting」ウィンドウ」を参照してください。
8. ユーザーまたはグループがファイルボリュームに書き込むことができるファイル数の制限値を設定します。ファイル数の制限値の詳細は、ウィンドウの「ヘルプ」ボタンをクリックするか、323 ページの「「Add/Edit Quota Setting」ウィンドウ」を参照してください。
9. 「Apply」をクリックして、変更内容を保存します。

ユーザーまたはグループの割り当ての編集

ユーザーまたはグループの割り当てを編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Manage Quotas」 > 「Configure User and Group Quotas」を選択します。
2. ユーザーの割り当てを編集するには、「Users」をクリックします。グループの割り当てを編集するには、「Groups」をクリックします。
3. 「Volume」ドロップダウンリストから、割り当てを編集するファイルボリュームの名前を選択します。
この画面の表には、ファイルボリュームに対するスーパーユーザー、デフォルトのユーザー、および個別のユーザー、またはこれらのユーザーのグループへの割り当てが表示されます。
4. 割り当てを編集するユーザーまたはグループを選択して、「Edit」をクリックします。
5. 選択したユーザーまたはグループのディスク容量の制限値を編集します。ディスク容量の制限値の詳細は、ウィンドウの「ヘルプ」ボタンをクリックするか、323 ページの「Add/Edit Quota Setting」ウィンドウを参照してください。
6. ユーザーまたはグループがファイルボリュームに書き込むことができるファイル数の制限値を編集します。ファイル数の制限値の詳細は、ウィンドウの「ヘルプ」ボタンをクリックするか、323 ページの「Add/Edit Quota Setting」ウィンドウを参照してください。
7. 「Apply」をクリックして、変更内容を保存します。

ユーザーまたはグループの割り当ての削除

スーパーユーザーおよびデフォルトのユーザー、またはこれらのユーザーのグループへの割り当ては、削除できません。個別のユーザーまたはグループへの割り当ては、ディスク容量およびファイル数のデフォルト値に設定することによって削除できません。

ユーザーまたはグループの割り当てを削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Manage Quotas」 > 「Configure User and Group Quotas」を選択します。
2. 「Configure User and Group Quotas」パネルで、ユーザーの割り当てを削除するには「Users」を、グループの割り当てを削除するには「Groups」を選択します。
3. 削除する割り当てを表から選択して、「Edit」をクリックします。
4. 「Edit Quota Setting」ウィンドウで、「Disk Space Limits」と「File Limits」の両方のセクションで「Default」オプションをクリックします。
5. 「Apply」をクリックして、割り当ての設定を削除します。

ディレクトリツリー割り当ての構成

この節では、ディレクトリツリー割り当ての構成について説明します。この節の内容は、次のとおりです。

- 118 ページの「ディレクトリツリー割り当ての構成について」
- 118 ページの「ディレクトリツリー割り当てを使用したディレクトリツリーの作成」
- 119 ページの「既存のディレクトリツリー割り当ての編集」
- 120 ページの「ディレクトリツリー割り当ての削除」

ディレクトリツリー割り当ての構成について

「Configure Directory Tree Quotas」(DTQ) パネルでは、ファイルシステムの特定のディレクトリに対する割り当てを管理できます。ディレクトリツリー割り当ては、ディレクトリで使用可能なディスク容量およびこのディレクトリに書き込み可能なファイル数を決定します。このパネルで作成したディレクトリにのみ割り当てを構成できます。以前に作成した既存のディレクトリに割り当てを構成することはできません。

ディレクトリツリー割り当てを使用したディレクトリツリーの作成

ディレクトリツリー割り当てを使用してディレクトリツリーを作成するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Manage Quotas」 > 「Configure Directory Tree Quotas」を選択します。
2. プルダウンメニューから、ディレクトリツリー割り当てを構成するファイルボリュームを選択します。
3. 「Add」をクリックします。
4. 「DTQ Name」フィールドに、このディレクトリツリー割り当てを識別する名前を入力します。
5. 「DirName」フィールドに、新しいディレクトリの名前を入力します。
6. 「Path」フィールドの下に、選択したファイルボリュームのディレクトリツリー構造を示すボックスが表示されます。

フォルダの内容を表示するには、フォルダの横の記号をクリックするか、フォルダのアイコンをダブルクリックします。次に、作成する新しいディレクトリを含めるディレクトリを選択します。「Path」フィールドにディレクトリのフルパスが表示されるまで続けます。

7. 「Disk Space Limits」セクションで、「No Limit」または「Custom」のいずれかを選択して、ディレクトリのディスク容量の制限値を指定します。
 - 「No Limit」を選択すると、ディレクトリのディスク容量を無制限にすることができます。
 - 「Custom」を選択すると、ディレクトリで使用可能なディスク容量の最大値を定義できます。
8. 割り当てを M バイトまたは G バイトのどちらの単位で報告するかを選択して、「Max Value」フィールドにディスク容量の制限値を入力します。

「Custom」の値に 0 (ゼロ) を入力すると、「No Limit」を選択した場合と同様に処理されます。
9. 「File Limits」フィールドで、「No Limit」または「Custom」のいずれかを選択して、このディレクトリに書き込み可能なファイルの最大数を指定します。
 - 「No Limit」を選択すると、このディレクトリに書き込み可能なファイル数を無制限にすることができます。
 - 「Custom」を選択すると、ファイルの最大数を割り当てることができます。そのあと、「Max Value」フィールドにファイル数の制限値を入力します。
10. 「Apply」をクリックして、割り当てを追加します。

既存のディレクトリツリー割り当ての編集

既存のディレクトリツリー割り当てを編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」>「Manage Quotas」>「Configure Directory Tree Quotas」を選択します。
2. 編集する割り当てを表から選択して、「Edit」をクリックします。
3. 「DTQ Name」フィールドで、このディレクトリツリー割り当てを識別する名前を編集します。

「Path」は読み取り専用のフィールドで、ディレクトリのパスを示します。
4. 「Disk Space Limits」セクションで、「No Limit」または「Custom」のいずれかを選択して、ディレクトリのディスク容量の制限を指定します。
 - 「No Limit」を選択すると、ディレクトリで使用できるディスク容量の使用量を無制限にすることができます。
 - 「Custom」を選択すると、ディスク容量の最大値を割り当てることができます。
5. 割り当てを M バイトまたは G バイトのどちらの単位で報告するかを選択して、「Max Value」フィールドにディスク容量の制限値を入力します。

「Custom」の値に 0 (ゼロ) を入力すると、「No Limit」を選択した場合と同様に処理されます。

6. 「File Limits」 セクションで、「No Limit」または「Custom」のいずれかを選択して、このディレクトリに書き込まれるファイルの最大数を指定します。
 - 「No Limit」を選択すると、このディレクトリに書き込み可能なファイル数を無制限にできます。
 - 「Custom」を選択すると、ファイルの最大数を割り当てることができます。
7. 「Max Value」 フィールドにファイル数の制限値を入力します。
8. 「Apply」 をクリックして、変更内容を保存します。

注: ディレクトリツリー割り当て (DTQ) が設定されたディレクトリを移動したり、名前を変更したりすると、DTQ のパスの指定はシステムによって自動的に更新されます。

ディレクトリツリー割り当ての削除

ディレクトリツリー割り当てを削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Manage Quotas」 > 「Configure Directory Tree Quotas」 を選択します。
2. 削除する割り当てを表から選択します。
3. 「Delete」 をクリックして、割り当ての設定を削除します。

ディレクトリツリー割り当て (DTQ) を削除すると、割り当ての設定が削除されます。ただし、ディレクトリ自体やディレクトリ内のファイルは削除されません。

注: DTQ が設定されたディレクトリを削除すると、ディレクトリと DTQ 設定の両方が削除されます。

NFS エクスポートの設定

この節では、NFS エクスポートの設定について説明します。この節の内容は、次のとおりです。

- 121 ページの「NFS エクスポートの設定について」
- 121 ページの「エクスポートの作成」
- 122 ページの「エクスポートの編集」
- 123 ページの「エクスポートの削除」

NFS エクスポートの設定について

ネットワークファイルシステム (NFS) エクスポートを使用すると、UNIX (および Linux) ユーザーのアクセス権限を指定できます。「Configuring Exports」パネルの表には、各エクスポートのアクセス可能なディレクトリ、ホスト名、およびアクセスレベル (読み取り/書き込みまたは読み取り専用) など、現在の NFS エクスポートの情報が表示されます。

「@」で始まるホスト名は、ホストのグループを示します。たとえば、ホスト名が「@general」の場合にはすべてのホストが含まれ、ホスト名が「@trusted」の場合にはすべての信頼できるホストが含まれます。信頼できるホストについては、90 ページの「ホストの構成について」を参照してください。

エクスポートは、特定の UNIX ホストにアクセス権限を指定すると作成されます。

エクスポートの作成

エクスポートを作成するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Configure NFS」>「Configure Exports」を選択します。

このパネルの表には、現在のエクスポートの情報が表示されます。エクスポートを作成していない場合、この部分は空白になります。
2. 「Add」ボタンをクリックして、エクスポートを追加します。
3. 「Volume」ボックスで、UNIX NFS ホストにアクセス権を付与するボリュームを選択します。
4. 「Path」ボックスで、UNIX NFS ホストにアクセス権を付与するディレクトリを指定します。

このフィールドを空白のままにすると、ボリューム全体が選択されます。
5. 「Access」セクションで、選択したボリュームに対する、読み取り/書き込み、読み取り専用、またはアクセス不可のどの権限をホストに付与するかを指定します。
6. 「Hosts」セクションで、ネットワークファイルシステム (NFS) エクスポートを定義する 1 つ以上のホストを選択します。

次のいずれかを選択します。

 - **Host Netgroups** — ネットグループを選択するには、このオプションボタンを選択します。ドロップダウンメニューから、このエクスポートを定義するネットグループを選択します。

- **Host Group** — ホストグループを選択するには、このオプションボタンを選択します。プルダウンメニューから、すべてのホストを示す「general」、すべての信頼できるホストを示す「trusted」、またはユーザー定義のホストグループを選択します。
 - **Known Host** — 「Set Up Hosts」パネルを使用して追加したホストにエクスポートを割り当てるには、このオプションを選択します。プルダウンメニューから、このエクスポートを定義するホストを選択します。
 - **Other Host** — 「Set Up Hosts」パネルを使用して追加していない個々のホストにエクスポートを割り当てるには、このオプションを選択して、ホストの名前を入力します。
7. 「Map Root User」セクションで、スーパーユーザーのユーザー ID をマッピングする方法を選択します。
- 次のいずれかを選択します。
- **Anonymous user** — スーパーユーザーのユーザー ID を匿名ユーザーのユーザー ID に対応付けるには、このオプションボタンを選択します。
 - **Root User** — スーパーユーザーのユーザー ID をスーパーユーザーのユーザー ID (UID=0) に対応付けるには、このオプションボタンを選択します。
 - **Map to UID** — 特定のユーザー ID を割り当てるには、このオプションを選択してユーザー ID を入力します。
8. 「Apply」をクリックして、エクスポートを保存します。
9. 「Configure Exports」パネルで、作成したエクスポートについて、正しいパス、ホスト、およびアクセス権が表示されていることを確認します。

エクスポートの編集

エクスポートを編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」 > 「Configure NFS」 > 「Configure Exports」を選択します。
2. 変更するエクスポートを選択して、「Edit」ボタンをクリックします。
3. アクセス権を変更するには、「Read/Write」、「Read/Only」、または「No Access」をクリックします。
「Hosts」セクションは読み取り専用です。
4. 「Apply」をクリックして、変更内容を保存します。
5. 「Configure Exports」パネルで、編集したエクスポートについて、正しいパス、ホスト、およびアクセス権が表示されていることを確認します。

エクスポートの削除

ネットワークファイルシステム (NFS) エクスポートを削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」 > 「Configure NFS」 > 「Configure Exports」を選択します。
2. 「Trash」 ボタンをクリックします。
3. 削除を確認します。

第9章

システムのオプション

この章では、Sun StorageTek 5320 NAS Appliance システム用に購入できるオプションを起動する方法について説明します。また、次に示すオプションの詳細も、この章で説明します。

- Sun StorageTek File Replicator Software。データを1つのボリュームから異なる Sun StorageTek 5320 NAS Appliance 上のミラー化ボリュームへ複製できます。通常、トランザクション指向のシステムで使用されます。
- Sun StorageTek Compliance Archiving Software。データの保持および保護を目的とする規制適合アーカイブ機能のガイドラインにボリュームを準拠させることができます。

この章は、次の節で構成されています。

- 125 ページの「システムのオプションの起動」
- 126 ページの「Sun StorageTek File Replicator Software オプションについて」
- 139 ページの「規制適合アーカイブオプションについて」

システムのオプションの起動

システムのオプションを起動するには、「Activate Options」パネルで起動キーを入力します。オプションを購入した場合は、ご購入先に起動キーをお問い合わせください。

システムオプションを起動するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Activate Options」を選択し、「Add」をクリックしてライセンスを追加します。
2. 「Add License」ウィンドウで、ご購入先から提供されたモジュールの名前（たとえば Sun StorageTek File Replicator）を「Module」に入力します。
3. ご購入先から提供された開始日を YYYYMMDD の形式で入力します。

これは、時刻が 0000:00 になるとライセンスが有効になる日付を示します。この日付を 00000000 に指定すると、ライセンスはすぐに有効になります。

4. ご購入先から提供された有効期限を YYYYMMDD の形式で入力します。

これは、時刻が 2359:59 になるとライセンスが期限切れになる日付を示します。この日付を 00000000 に設定すると、ライセンスは期限切れになりません。

注: 規制適合のライセンスが期限切れになるか、削除された場合、規制適合規則はシステムに保持されますが、新しい規制適合対応のボリュームは作成できなくなります。Compliance Archiving Software の詳細は、140 ページの「Compliance Archiving Software について」を参照してください。

5. ご購入先から提供されたライセンスキーを入力します。

6. 「Apply」をクリックして、オプションを起動します。

Sun StorageTek File Replicator Software ソフトウェアの場合は、ミラー化サーバー上で追加の手順を実行してください。詳細は、130 ページの「遠隔サーバーでの Sun StorageTek File Replicator Software ソフトウェアの起動」を参照してください。

7. 日付と時刻をまだ設定していない場合は、正確な日付、時刻、およびタイムゾーン情報を入力します。

これによって、システム時間および固定クロックが設定されます。固定クロックは、ライセンス管理ソフトウェアおよび Compliance Archiving Software で、高い精度を必要とする、時間に基づく処理に使用されます。

注: 固定クロックは一度しか設定できません。必ず正確に設定してください。

8. 新しい日付と時刻が正しいことを確認します。

新しい日付と時刻が正しい場合は、「Yes」をクリックします。正しくない場合は、「No」をクリックして正しい日付と時刻を設定します。

Sun StorageTek File Replicator Software オプションについて

この節では、Sun StorageTek File Replicator Software オプションについて説明します。この節の内容は、次のとおりです。

- 127 ページの「Sun StorageTek 5320 NAS Appliance のミラー化について」
- 127 ページの「ミラー化の準備について」
- 128 ページの「クラスタ構成での要件および制限事項について」
- 128 ページの「アクティブシステムおよびミラーシステムの構成」

- 129 ページの「ミラー化されたファイルボリュームの構成」
- 132 ページの「破損したミラーの修正」
- 133 ページの「ミラー化ファイルボリュームの警告しきい値の設定」
- 135 ページの「ミラーサーバー間の接続の切断」
- 135 ページの「ミラー化されたファイルボリュームのプロモート」
- 136 ページの「ミラー接続の再確立」
- 139 ページの「ボリュームの役割の変更」

Sun StorageTek 5320 NAS Appliance のミラー化について

ミラー化を使用すると、1 台の Sun StorageTek NAS システムの一部またはすべてのファイルボリュームを、別の Sun StorageTek NAS システム上に複製できます。ソースサーバーは「アクティブサーバー」と呼ばれ、ターゲットサーバーは「ミラーサーバー」と呼ばれます。

アクティブサーバーに障害が発生した場合、ミラーサーバー上でミラー化を切断し、ミラーサーバー上でミラー化されたファイルボリュームをプロモートして (ユーザーが使用できるように) します。

使用されるミラー化の方法は、非同期トランザクション指向のミラー化です。ミラー化は、大容量の「ミラーバッファー」を使用して実行され、ファイルシステムのトランザクションはミラーシステムへの転送の待ち行列に入れられます。つまり、ミラーサーバーでの処理はアクティブサーバーでの処理よりわずかに遅れて実行されます。ミラー化はトランザクション指向であるため、ネットワークの中断やシステム障害の発生時にも、ミラーファイルシステムの完全性が保証されます。

ミラー化の準備について

ミラー化を開始する前に、次の点を確認してください。

- ミラー化には 2 台の Sun StorageTek NAS サーバーが必要です。サーバーのモデルは任意で、異なるモデルを使用できます。
- ミラーサーバーには、ミラー化するファイルボリュームと同じか、それより大きいストレージ領域が必要です。
- アクティブサーバーとミラーサーバーとの間には、十分な処理能力を持つ、継続的に使用可能な信頼性の高いネットワーク接続が存在している必要があります。これらの 2 つのサーバーを接続するインタフェースには、100M ビット Ethernet または 1000M ビット Ethernet を使用できます。スイッチまたはルーターを介してサーバーを接続することもできます。サーバーをルーターに接続する場合、静的

ルートを設定して、ミラー化データが専用ルートを使用して送信されるようにしてください。サーバーをスイッチに接続する場合は、各サーバーに仮想 LAN (VLAN) を作成して、ネットワークトラフィックを分離します。

- 両方のサーバーにインストールされているオペレーティングシステムのバージョンが同じである必要があります。
- ミラー化するアクティブファイルボリュームは、1G バイト以上である必要があります。

注: いったんファイルボリュームをミラー化すると、元のファイルボリュームの名前を変更できなくなります。

クラスタ構成での要件および制限事項について

次に、Sun StorageTek 5320 NAS Cluster Appliance 構成の Sun StorageTek File Replicator Software ソフトウェアでのミラー化の要件および制限事項の一覧を示します。

- クラスタ構成の両方のサーバーで、Sun StorageTek File Replicator Software ライセンスを使用可能にしてください。
- ミラー化は、サーバー H1 からまたはサーバー H1 に対してのみ確立してください。同一クラスタのサーバー H1 からサーバー H2 に対してミラーを作成しないでください。
- ミラー管理操作を実行するには、クラスタ内のサーバーが両方とも NORMAL 状態である必要があります。ミラー管理操作には、新しいミラーの作成、役割の変更、プロモート、切断などがあります。
- クラスタがフェイルオーバーモードの場合 (つまり、1 台のサーバーが ALONE 状態、もう 1 台のサーバーが QUIET 状態の場合) であるか、または縮退状態である場合は、ミラー管理操作を実行しないでください。ミラー管理操作を実行する前に、クラスタを NORMAL 状態にすることをお勧めします。
- クラスタ構成でフェイルオーバーが行われた場合でも、既存のミラーによるミラー化は続行されます。また、フェイルオーバー後にクラスタが復元されるときにも、既存のミラーによるミラー化は続行されます。
- ミラーバッファリングの制限事項があります。130 ページの「ミラーバッファのミラー化について」を参照してください。

アクティブシステムおよびミラーシステムの構成

システムの設定時に、ミラー化サーバーを相互に接続するポートの役割を指定します。次に、Web Administrator インタフェースを使用して、アクティブシステムおよびミラーシステム上でミラー化を構成します (130 ページの「ミラーバッファのミラー化について」を参照)。それぞれのシステムは個別に構成します。

専用ネットワークポートを構成するには、次の手順を実行します。

1. アクティブサーバーのナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」を選択します。
2. ローカルのネットワークまたはサブネットに接続されたポートにインターネットプロトコル (IP) アドレスおよび「Primary」という役割を割り当てていない場合、これらを割り当てます。

アクティブシステムおよびミラーシステムのポートは、異なるローカルサブネット上に存在することができます。TCP/IP (Transmission Control Protocol/Internet Protocol) の構成の詳細は、22 ページの「ネットワークポートの構成について」を参照してください。

3. アクティブシステムとミラーシステムとのミラー接続に使用するポートに IP アドレスを割り当てます。

注: 主インタフェースを含むサブネットをミラー化に使用しないでください。

ミラー化のトラフィックを配信するための分離ネットワークを作成した場合は、192.1xx.x.x など、プライベート用に予約された範囲のアドレスを使用するようにしてください。たとえば、アクティブシステムのミラーリンクインタフェースを 192.1xx.1.1 に割り当て、ミラーシステムのミラーリンクインタフェースを 192.1xx.1.2 に割り当てます。

4. アクティブサーバーとミラーサーバーとの接続に使用するポートの「Role」フィールドで、「Mirror」を選択します。
5. アクティブシステムおよびミラーシステムのミラーインタフェースが同じサブネット上で接続されていない場合は、コマンド行インタフェースを使用して、これらのシステム間に静的ルートを設定する必要があります。
これによって、サーバーは、ローカルのインタフェースに直接接続されていないネットワーク上で相互に通信できます。この処理の完了については、228 ページの「ルートの管理」を参照してください。
6. 「Apply」をクリックして、変更内容を保存します。

ミラー化されたファイルボリュームの構成

この節では、ミラー化ファイルボリュームの構成について説明します。この節の内容は、次のとおりです。

- 130 ページの「ミラーバッファのミラー化について」
- 130 ページの「遠隔サーバーでの Sun StorageTek File Replicator Software ソフトウェアの起動」
- 131 ページの「ファイルボリュームの追加」
- 132 ページの「ミラーの編集」

ミラーバッファのミラー化について

ミラー化は、ボリューム単位で実行されます。一部またはすべてのボリュームをミラー化するように選択できます。

注: ミラー化できるのは 1G バイト以上のファイルボリュームのみです。いったんファイルボリュームをミラー化すると、ミラー接続が保持されている間は、元のファイルボリュームの名前を変更できません。

ミラーの初期同期中に、アクティブサーバーからミラー化されているファイルボリュームに対して入出力動作を行うことはできません。

ミラーバッファには、ミラーサーバーへのファイルシステムの書き込みトランザクションの転送中に、これらのトランザクションが格納されます。アクティブサーバー上のファイルボリュームの空き領域は、ミラーバッファの割り当てサイズを設定することによって減少します。

ミラーバッファのサイズはさまざまな要因によって異なりますが、100M バイト以上である必要があります。また、ミラーバッファは、特定のファイルボリュームの残りの空き容量の半分以下である必要があります。

通常は、ミラー化するファイルボリュームの約 10% のサイズのミラーバッファを作成することをお勧めします。このサイズは、ファイルボリュームのサイズではなく、ファイルボリュームに書き込まれる情報のサイズによって判断する必要があります。概して、ミラーバッファのサイズは、ファイルボリュームへの書き込みの頻度に正比例し、2 台のサーバー間のネットワーク速度に反比例します。

ファイルボリュームへの書き込み操作の頻度が高く、2 台のミラーサーバー間のネットワーク接続の速度が遅い場合は、ミラー化するファイルボリュームの約 25 ~ 30% のサイズのミラーバッファを作成することをお勧めします。

ミラーバッファのサイズは、動的に増やすことはできません。ミラーバッファのサイズを増やすには、既存のミラーを切断し、新しいミラーバッファサイズでミラーを再度作成する必要があります。

遠隔サーバーでの Sun StorageTek File Replicator Software ソフトウェアの起動

Sun StorageTek File Replicator Software オプションを起動したあと (125 ページの「システムのオプションの起動」を参照)、ミラー化するファイルボリュームが含まれる遠隔サーバー上でもこのオプションを起動してください。

遠隔サーバーで Sun StorageTek File Replicator Software オプションを起動するには、次の手順を実行します。

1. ミラー化するファイルボリュームが含まれるサーバーの Web Administrator にログインします。

2. 「Add License」ウィンドウで、ご購入先から提供されたモジュールの名前 (たとえば Sun StorageTek File Replicator) を入力します。
3. ご購入先から提供された開始日を YYYYMMDD の形式で入力します。
これは、時刻が 0000:00 になるとライセンスが有効になる日付を示します。この日付を 00000000 に指定すると、ライセンスはすぐに有効になります。
4. ご購入先から提供された有効期限を YYYYMMDD の形式で入力します。
これは、時刻が 2359:59 になるとライセンスが期限切れになる日付を示します。この日付を 00000000 に設定すると、ライセンスは期限切れになりません。
5. ご購入先から提供されたライセンスキーを入力します。
6. 「Apply」をクリックして、Sun StorageTek File Replicator Software ソフトウェアを起動します。

ファイルボリュームの追加

構成にファイルボリュームを追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Replicator」>「Manage Mirrors」を選択します。
2. 「Add」をクリックします。
3. 「Volume」プルダウンメニューから、ミラー化するファイルボリュームを選択します。
ミラー化するファイルボリュームは、1G バイト以上である必要があります。
4. 「Mirror Host」フィールドにミラーサーバーを識別できる名前を入力します。
5. ミラーシステムのインターネットプロトコル (IP) アドレスを入力します。
ここには、ミラーシステム上のミラー化ネットワークインタフェースカード (NIC) に対して選択した IP アドレスを入力します。
6. (省略可能) 代替 IP アドレスを入力します。
最初の IP アドレスが使用不可になると、サーバーはこの代替 IP アドレスを使用してミラーを保持します。
7. ミラーサーバーへのアクセスに管理パスワードが必要な場合は、「Password」フィールドに管理パスワードを入力します。
管理パスワードを設定しない場合、このフィールドは空白のままにします。必ずパスワードを使用してサーバーを保護してください。
8. ミラーバッファのサイズを M バイト単位で入力します。

アクティブサーバー上のファイルボリュームの空き領域は、ミラーバッファの割り当てサイズを設定することによって減少します。

9. ミラーの作成中にアクティブサーバー上のソースファイルボリュームに対する入出力動作が発生しないことを確認してから、「Apply」をクリックしてミラーを作成します。

ミラー作成処理が開始されます。「Manage Mirrors」パネルでミラーが「In Sync」の状態になると、ミラー化ファイルボリュームが読み取り専用でマウントされます。いったんミラーの状態が「In Sync」になると、入出力動作を再開できます。

既存のミラーの代替 IP アドレスまたはミラーサーバーの管理者パスワードは、編集が可能です。

ミラーの編集

ミラーを編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Replicator」 > 「Manage Mirrors」を選択します。

2. 編集するミラーを表から選択します。

3. 「Edit」をクリックします。

ファイルボリューム名およびミラーホストは、読み取り専用のフィールドです。

4. ミラー接続に使用するインターネットプロトコル (IP) アドレスを編集して、次のフィールドで代替 IP アドレスを編集します。

5. 必要に応じて、ミラーホストサーバーへのアクセスに必要な新しい管理パスワードを入力します。

管理パスワードを設定しない場合は、「Password」フィールドを空白のままにします。

6. 「Apply」をクリックして、変更内容を保存します。

破損したミラーの修正

ミラーが破損した場合は、破損したミラーを修正できます。ミラーの破損は、2 台のサーバー間の接続がしばらくの間停止していた場合や、ミラーバッファが非常に小さく、マスターボリュームへの書き込みが多い場合に発生します。

破損したミラーを修正するには、次の手順を実行します。

1. 2 台のサーバー間に、より高速のネットワーク接続を確立します。

2. ミラーが In Sync 状態になるまで、マスターファイルシステムへのすべての入出力動作を休止します。
3. nbd ボリュームを切断してプロモートしたあと、共通インターネットファイルシステム (CIFS) クライアントまたはネットワークファイルシステム (NFS) クライアントのどちらかから、ターゲットファイルシステムを読み取り専用でミラーサーバーにマウントします。

このファイルシステムは、バックアップ処理または任意の読み取り専用処理で使用されます。

ミラー化機能にチェックポイントを組み合わせることもできます。アクティブサーバーにチェックポイントが作成されていると、そのチェックポイントもミラーサーバーにミラー化されます。これを使用して、スケジュール設定されたバックアップを実行したり、ほかのユーザーおよびアプリケーションが読み取り専用でチェックポイントにアクセスしたりすることができます。

ミラー化ファイルボリュームの警告しきい値の設定

この節では、警告しきい値の設定について説明します。この節の内容は、次のとおりです。

- 133 ページの「警告しきい値の設定について」
- 134 ページの「しきい値警告の設定」

警告しきい値の設定について

「File Replicator」から「Set Threshold Alert」パネルを表示して、すべてのミラー化ファイルボリュームにしきい値警告を設定できます。しきい値警告とは、ミラーバッファの使用率に応じて指定した受信者に送信される警告です。

ミラーバッファには、ミラーサーバーへのファイルシステムの書き込みトランザクションの転送中に、これらのトランザクションが格納されます。アクティブサーバーへの書き込み操作が増加したり、ネットワークリンクが切断されたりすると、ミラーサーバーへの書き込みトランザクションの代わりに、ミラーバッファへのバックアップが行われる場合があります。この処理によってミラーバッファが制限を超えた場合、ミラーが破損し、ミラーが再確立されるまでアクティブサーバーとミラーサーバー間でトランザクションが発生しなくなります。通信が完全に復元されると、システムは自動的にミラーの再同期処理を開始して、ミラー化されたファイルボリュームの同期をとります。

この状況を回避するため、ミラーバッファの使用率が一定のしきい値パーセンテージに達すると、システムは電子メール通知、システムログファイル、SNMP (ネットワーク管理プロトコル) トラップ、および LCD パネルを使用して、自動的に警告を送信します。

しきい値警告の設定

しきい値警告を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Replicator」 > 「Set Threshold Alert」を選択します。
2. 「Mirroring Buffer Threshold 1」を選択します。

これは、最初の警告が送信されるミラーバッファの使用率です。デフォルト値は 70% です。これは、ミラーバッファの使用率が 70% に達すると、自動的に警告が送信されることを意味します。
3. 「Mirroring Buffer Threshold 2」を選択します。

これは、2 番目の警告が送信されるミラーバッファの使用率です。デフォルト値は 80% です。
4. 「Mirroring Buffer Threshold 3」を選択します。

これは、3 番目の警告が送信されるミラーバッファの使用率です。デフォルト値は 90% です。
5. 「Alert Reset Interval (Hours)」を選択します。

これは、その時間内に状態が再発生してもシステムが警告を再送信せずに待機する時間を示します。

たとえば、「Mirroring Buffer Threshold 1」を 10% に設定し、「Alert Reset Interval」を 2 時間に設定すると、ミラーバッファの使用率が 10% に達したときに最初の警告が送信されます。システムは、その後 2 時間はしきい値 1 警告を再送信しません。2 時間が経過してもミラーバッファの使用率が 10% を超えていて、しきい値 2 または 3 は超えていない場合、しきい値 1 警告が再送信されません。

このフィールドのデフォルト値は 24 時間です。
6. 「Apply」をクリックして、変更内容を保存します。

ミラーサーバー間の接続の切断

たとえば、アクティブサーバー上のファイルボリュームが使用できない場合に、ミラーサーバー上のファイルボリュームをプロモートするには、まず、ミラー接続を切断する必要があります。ミラー接続の切断は、次の手順で説明するとおり、ミラーサーバー上ではなくアクティブサーバー上で行います。ただし、アクティブサーバーが停止し、このサーバーにアクセスして接続を切断できない場合、代わりにミラーサーバーからミラー接続を切断できます。

ミラーサーバー間のミラー接続を切断するには、次の手順を実行します。

1. アクティブサーバーのナビゲーションパネルで、「File Replicator」 > 「Manage Mirrors」を選択します。
2. 表からミラーを選択して、「Break」をクリックします。

ミラー接続の切断を確認するプロンプトが表示されます。ミラー接続を切断すると、そのミラー接続はこのパネルのミラーの表に表示されなくなります。ファイルボリュームをプロモートするには、ミラーサーバー上で「Manage Mirrors」パネルにアクセスします。詳細は、135 ページの「ミラー化されたファイルボリュームのプロモート」を参照してください。

ミラー化されたファイルボリュームのプロモート

ミラーサーバーは、アクティブサーバーに障害が発生した場合に、ミラー化されたファイルボリュームの高可用性を実現します。ミラー化ファイルボリュームをネットワークユーザーが使用できるようにするには、ファイルボリュームをプロモートしてください。まず、ミラー接続を切断し、次に、ミラー化されたファイルボリュームをプロモートして、アクセス権を設定する必要があります。ミラー接続を切断して、ミラー化されたファイルボリュームをプロモートすると、元のファイルボリュームとミラー化されたファイルボリュームは完全に独立した状態になります。



注意: 厳格な規制適合対応のボリュームのミラーはプロモートできません。厳格な規制適合対応のミラーボリュームに一時的にアクセスする必要がある場合は、そのボリュームをプロモートせずに読み取り専用のファイルシステムとしてエクスポートできます。

ミラーサーバー上のファイルボリュームをプロモートするには、まずミラー接続を切断する必要があります。詳細は、135 ページの「ミラーサーバー間の接続の切断」を参照してください。

ミラーサーバー上のファイルボリュームをプロモートするには、次の手順を実行します。

1. ミラーサーバーのナビゲーションパネルで、「File Replicator」 > 「Manage Mirrors」を選択します。

2. 「Promote」をクリックします。
3. 「Promote Volume」ウィンドウで、プロモートするボリュームを選択し、「Apply」をクリックします。

この処理が完了するまでには数分かかる場合があります。ミラー化ファイルボリュームをプロモートするには、ある時点でそのボリュームが「In Sync」の状態になっている必要があります。プロモートが正常に終了したときにミラー化されたファイルボリュームの同期がとれていない場合、そのボリュームは読み取り専用ボリュームとしてマウントされます。ボリュームへの書き込みを許可する前に、fsck コマンドを実行して必要な修復を行います。

ミラー接続を切断すると、システムによってファイルシステムチェックが実行されます。このチェック時にエラーが検出されると、ファイルボリュームのプロモート処理に要する時間が長くなる場合があります。プロモート処理中にミラーの同期がとれていない場合、データの完全性は保証されません。

ファイルボリュームをプロモートしたあとで、アクセス権を再構成する必要があります。Microsoft サーバーメッセージブロック (SMB) 共有の情報は自動的に継承されますが、ネットワークファイルシステム (NFS) ファイルボリュームへのアクセスおよび NFS エクスポートはこのファイルボリューム用に再構成してください。NFS エクスポートの設定の詳細は、121 ページの「NFS エクスポートの設定について」を参照してください。

ミラー接続の再確立

この節では、ミラー接続の再確立について説明します。この節の内容は、次のとおりです。

- 136 ページの「ミラー接続の再確立」
- 137 ページの「アクティブサーバーでのミラー接続の切断」
- 137 ページの「サーバー 1 上の古いファイルボリュームの削除」
- 138 ページの「サーバー 2 からサーバー 1 への最新のファイルボリュームのミラー化」

ミラー接続の再確立

ここでは、アクティブサーバーに障害が発生してミラーサーバー上のファイルボリュームをプロモートしたあとに、ミラー接続を再確立する方法について説明します。プロモートしたファイルボリュームが最新のバージョンになり、アクティブシステム上の古いファイルボリュームから完全に独立して機能します。ミラー接続を再確立するには、最新のファイルボリュームをアクティブサーバーにミラー化し、そのファイルボリュームをミラーサーバーにミラー化して元の状態に戻す必要があります。

注: ミラー化ファイルボリュームをプロモートしていない場合、次の手順を実行しないでください。アクティブシステムがオンラインに戻ると、ミラーが自動的に「In Sync」の状態に戻されます。

次の例では、「サーバー 1」がアクティブサーバー、「サーバー 2」がミラーサーバーです。

ミラー接続を再確立するには、次の手順を実行します。

1. サーバー 1 上でミラーが切断されていることを確認します。
詳細は、137 ページの「アクティブサーバーでのミラー接続の切断」を参照してください。
2. サーバー 1 上の古いファイルボリュームを削除します。
詳細は、137 ページの「サーバー 1 上の古いファイルボリュームの削除」を参照してください。
3. サーバー 2 の最新のファイルボリュームをサーバー 1 にミラー化します。詳細は、138 ページの「サーバー 2 からサーバー 1 への最新のファイルボリュームのミラー化」を参照してください。
4. サーバー 2 の役割を変更します。
詳細は、139 ページの「ボリュームの役割の変更」を参照してください。
この時点で、サーバー 1 が再度アクティブになり、サーバー 2 はミラー化のターゲットになります。

アクティブサーバーでのミラー接続の切断

アクティブサーバーでミラー接続を切断するには、次の手順を実行します。

1. Web ブラウザのウィンドウを開き、サーバー 1 にアクセスします。
2. ナビゲーションパネルで、「File Replicator」 > 「Manage Mirrors」を選択します。
3. 切断するミラー接続を選択します。
4. 「Break」をクリックします。

サーバー 1 上の古いファイルボリュームの削除

サーバー 1 から古いファイルボリュームを削除するには、次の手順を実行します。

1. サーバー 1 のナビゲーションパネルで、「File Volume Operations」 > 「Delete File Volumes」を選択します。



2. ミラー化されていたファイルボリュームを選択します。

ミラーサーバー上のファイルボリュームがプロモートされて最新バージョンになっているため、アクティブサーバー上の古いファイルボリュームを削除する必要があります。

注意: 次の手順を実行する前に、アクティブサーバー上の古いソースファイルボリュームを削除してください。また、事前にミラーサーバー上の最新のファイルボリュームを確認し、このファイルボリュームをプロモートする必要があります。

3. 「Apply」をクリックして、古いファイルボリュームを削除します。

サーバー 2 からサーバー 1 への最新のファイルボリュームのミラー化

サーバー 2 の最新のファイルボリュームをサーバー 1 にミラー化するには、次の手順を実行します。

1. Web ブラウザのウィンドウを開き、サーバー 2 にアクセスします。
2. ナビゲーションパネルで、「File Replicator」 > 「Manage Mirrors」を選択します。
3. 「Add」をクリックします。
4. 「Volume」プルダウンメニューから、ミラー化するファイルボリュームを選択します。
5. 「Mirror Host」フィールドにサーバー 1 のミラー化の名前を入力します。
6. ミラー接続に使用するサーバー 1 のポートのインターネットプロトコル (IP) アドレスを入力します。
7. 代替 IP アドレスを入力します。
8. サーバー 1 へのアクセスに管理パスワードが必要な場合、「Password」フィールドに管理パスワードを入力します。
管理パスワードを設定しない場合、このフィールドは空白のままにします。
9. ミラーバッファのサイズを入力します。
ミラーバッファの詳細は、127 ページの「Sun StorageTek 5320 NAS Appliance のミラー化について」を参照してください。
ミラー同期中は、サーバー 2 上のソースファイルボリュームに対する入出力動作が決して行われないようにしてください。
10. 「Apply」をクリックして、ミラーを作成します。

ミラー作成処理が開始されます。ミラーが「In Sync」の状態になると、サーバー 1 とサーバー 2 の両方にファイルボリュームの同一のコピーが存在するようになります。

11. サーバー 1 の「Manage Mirrors」パネルで、プロモートしたファイルボリュームを選択して、「Change Roles」をクリックします。

詳細は、139 ページの「ボリュームの役割の変更」を参照してください。

元のミラー接続が再確立されました。

ボリュームの役割の変更

管理者は、アクティブボリュームとミラーボリュームとの間で役割を切り替えることができます。ボリュームの役割を変更すると、アクティブボリュームをミラーボリュームとして機能させるか、ミラーボリュームをアクティブボリュームとして機能させることができます。ただし、各ボリュームの元の構成は変更されません。役割の変更は、障害回復のための機能ではありません。

注: 役割を変更するボリュームは、100% 同期している状態である必要があります。

役割の変更は、アクティブサーバーまたはミラーサーバーの「Manage Mirror」パネルで実行できます。

ボリュームの役割を変更するには、次の手順を実行します。

1. ナビゲーションパネルで「File Replicator」>「Manage Mirrors」をクリックします。
2. 「Volume」列でボリュームを選択します。
3. 「Change Roles」をクリックします。
4. メッセージを確認して、「Yes」をクリックします。

規制適合アーカイブオプションについて

この節では、規制適合アーカイブオプションについて説明します。この節の内容は、次のとおりです。

- 140 ページの「Compliance Archiving Software について」
- 140 ページの「Compliance Archiving の使用可能への切り替えについて」
- 141 ページの「必須実施の規制適合について」
- 141 ページの「推奨実施の規制適合について」

- 142 ページの「規制適合の監査」
- 144 ページの「その他の規制適合アーカイブ機能」

Compliance Archiving Software について

Compliance Archiving Software は、情報の保持および保護に関するビジネス上の運用および規制適合規則への企業の対応を支援します。このような記録の保持および保護に関する規則およびフレームワークには、米国証券取引委員会 (SEC) 規制 17 CFR (240.17a-4 (17a-4))、米国企業改革法 (Sarbanes-Oxley Act)、新 BIS 規制 (BASEL II)、およびデータ保護とプライバシーに関する多くの指示があります。

Compliance Archiving Software は、情報管理の規制適合および企業のコンテンツ管理に精通している専門家と協議し基礎から設計されているため、電子ストレージ媒体の保持および保護に関するもっとも厳しい要件への対応に役立ちます。Compliance Archiving Software では、規制適合規則に従って WORM (Write Once, Read Many) ファイルが使用されます。

Compliance Archiving Software を使用可能にする場合は、NAS サーバーとクライアントのクロックが同期している必要があります。NTP を使用して、NAS サーバーを外部の時刻ソースに同期させることができます (62 ページの「時刻同期について」を参照)。クライアントと NAS サーバーの時刻に誤差が生じると、クライアントがクロックスキューよりも短い保持期間を要求した場合に、サーバーはデフォルトの保持期間を適用します。

Compliance Archiving Software の技術的な概要については、付録 A を参照してください。

Compliance Archiving の使用可能への切り替えについて

Compliance Archiving Software は、「推奨実施」と呼ばれる比較的厳しくない形式と、「必須実施」と呼ばれる厳しい形式の両方で使用できます。

Compliance Archiving Software を起動すると (125 ページの「システムのオプションの起動」を参照)、ボリュームの作成時に、規制適合を推奨実施または必須実施のどちらかで使用可能にするかを選択できます。

注: Sun StorageTek 5320 NAS Gateway システムの構成では、推奨実施の規制適合はサポートされていますが、必須実施はサポートされていません。

注: Compliance Archiving Software を適切に動作させるには、Sun StorageTek 5320 NAS Appliance または Sun StorageTek 5320 NAS Cluster Appliance のハードウェアが物理的に正しく構成されている必要があります。特に、Sun StorEdge 5300 RAID

Expansion Unit アレイを、NAS 本体および任意の Sun StorEdge 5300 RAID 拡張ユニット格納装置へのプライベートファイバチャネル接続以外には、どの装置またはネットワークにも決して接続しないでください。

注: できるかぎり強力なデータ保持方針を確実に実現するには、使用している Sun StorageTek 5320 NAS Appliance または Sun StorageTek 5320 NAS Cluster Appliance に物理的なセキュリティーも追加することをお勧めします。ソフトウェア制御によるデータ保持よりも、物理的な保護手段を使用してシステムのハードウェアへのアクセスを制御する方が強力です。



注意: Compliance Archiving Software によって実施されるさまざまなデータ保持規則を認識しないアプリケーションおよびユーザーが使用するボリュームでは、規制適合アーカイブ機能を使用可能にしないでください。

Compliance Archiving Software を使用すると、管理者は、作成するすべての新しいボリュームに対して規制適合アーカイブ機能を使用可能にできます。ただし、これはボリュームをはじめて作成する場合だけです。46 ページの「「Create File Volumes」パネルを使用したファイルボリュームまたはセグメントの作成」に示す手順に従って、規制適合対応のボリュームを作成してください。

必須実施の規制適合について

必須実施の規制適合では、次に示すように、データの保護、保持、およびプライバシーに関する指示が遵守されます。

- 必須実施の規制適合対応ボリュームを破棄することはできません。
- 保持期間が期限切れになるまで、WORM ファイルを破棄することはできません。
- ボリュームの保持期間は短縮または延長できますが、WORM ファイルの保持期間は延長することしかできません。
- チェックポイントから WORM ファイルを復元することはできません。



注意: いったんボリュームで必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。

推奨実施の規制適合について

必須実施の規制適合とは対照的に、推奨実施の規制適合では次の操作が可能です。

- 承認された管理者は、規制適合対応の WORM ファイルおよび規制適合対応のボリュームを、監査対象の削除機能を使用して破棄できます。

注: ボリュームを削除する前に、そのボリューム内の監査ログを別のファイルシステムにコピーして保管しておいてください。保管しない場合、監査ログは失われます。

- 承認された管理者は、保持期間を短縮および延長できます。
- 承認された管理者は、監査対象の削除機能を使用してチェックポイントから WORM ファイルを復元できます。
- 出荷時のデフォルトの保持期間は 0 日ですが、変更できます。

注: 保持期間の期限が切れる前に、保持期間の短縮および保持ファイルの削除を実行する場合は、信頼できるホストからスーパーユーザーがこの操作を行う必要があります。248 ページの「信頼できるホストの管理」を参照してください。

推奨実施の規制適合対応ボリュームを必須実施にアップグレードすると、そのボリュームのデフォルトの保持期間は永続的になります。この変更は、「Edit Properties」パネルで実行できます。

注: 推奨実施の規制適合対応ボリュームのアップグレードは、ゲートウェイ構成ではサポートされません。

規制適合の監査

この節では、規制適合の監査について説明します。この節の内容は、次のとおりです。

- 142 ページの「規制適合の監査について」
- 143 ページの「監査対象のファイルサイズの制限について」

規制適合の監査について

規制適合の監査では、適切な権限の有無にかかわらず、データの編集または削除が試行されると、これをテキストベースのログに記録します。この監査を使用可能にするには、Data Retention Audit Service (DRAS) API を使用します。この API には、次の機能があります。

- 保持ファイルに対する変更および試行された変更の報告
- 監査可能なイベントを記録するロギングメカニズム
- システムの存続期間にわたる、監査ログの保護および保持
- 見やすい形式にまとめられた監査ログ情報と、標準のシステムアクセスプロトコルを介した監査ログへのセキュリティー保護されたアクセス

監査可能なイベントのセットは、次のとおりです。

- ファイルの保持
- 保持ファイルの保持期間の延長
- 保持ファイルへのリンクの解除 (削除) 要求
- 保持ファイルへの書き込み要求
- 保持ファイルの名前の変更要求

- ディレクトリの削除要求
- ディレクトリの名前の変更要求

注 – 保持ファイルへの書き込み要求が監査ログに書き込まれないことがあります。これは、使用しているアプリケーションが、ファイルへの書き込みの前にアクセス権を判定しようとする場合に発生する可能性があります。保持ファイルに対する書き込み権が得られない場合、このアプリケーションは最終的に書き込み要求を実行しません。

監査対象のファイルサイズの制限について

規制適合対応ボリュームでは、ボリュームでの監査可能な操作をログに確実に記録できる容量の空き領域が予約されます。規制適合対応ボリュームの空き領域がこの制限を下回ると、監査可能な操作を実行できなくなります。操作と監査の両方を実行するために必要な領域が不足していることを示すメッセージがログに記録され、システムで電子メールが構成されている場合は警告メールが送信されます。

各規制適合対応ボリュームの監査ログは、ボリュームのルートディレクトリに保存されます。監査ログには、スーパーユーザーが信頼できるホストからアクセスするか、CIFS をドメインモードで実行している場合は Windows ドメイン管理者がアクセスしてください。詳細は、248 ページの「信頼できるホストの管理」を参照してください。

監査ログのレコードはテキストベースで、ネットワークファイルシステム (NFS) や共通インターネットファイルシステム (CIFS) などのネットワークプロトコルを介してアクセスできます。Windows 2000 または Windows XP が動作しているクライアントでログの内容を表示するには、共有のパスに .audit\$ ディレクトリが含まれている必要があります。共有の作成の詳細は、106 ページの「共有について」を参照してください。

表 9-1 に、監査ログの形式を示します。

表 9-1 監査ログの形式

フィールド	長さ	説明
Version	7	Data Retention Audit Service のバージョン番号
Serial Number	11	一意のシーケンス番号
Length	5	監査レコードの長さ
Timestamp	21	イベントが発生した日付と時刻
TID	11	イベントが実行されたスレッドのスレッド ID
Volume ID	11	監査が実行されたボリュームのボリューム ID

表 9-1 監査ログの形式 (続き)

フィールド	長さ	説明
Protocol	9	操作の要求に使用されたネットワークプロトコル
Inode	11	ファイルのファイルシステムの i ノード番号
Client IP Address	16	操作を要求したクライアントのインターネットプロトコル (IP) アドレス
Server IP Address	16	クライアントの要求を受信した IP アドレス
UID	11	ユーザーの資格
GID	11	一次グループの資格
Operation	8	監査イベント
Status	可変	操作の結果
Domain	可変	ユーザーが属する Windows ドメイン (取得可能な場合)
File/Directory Name	可変	操作の実行対象のファイルまたはディレクトリの名前 (取得可能な場合)
Path/Extra Data	可変	監査からの追加情報 (取得可能な場合)

その他の規制適合アーカイブ機能

Compliance Archiving Software の機能およびプログラミングインタフェースの技術的な概要については、付録 C を参照してください。

規制適合アーカイブ機能の設定の変更については、270 ページの「Compliance Archiving Software の構成」を参照してください。

第10章

システムの監視

この章では、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムの監視機能について説明します。システム監視は保守機能と密接に関連しています。ここで説明する多くの監視機能で表示される問題への対処については、ほかの章を参照してください。監視機能では、管理アクティビティーまたは保守アクティビティーの完了や状態も表示されます。

この章は、次の節で構成されています。

- 145 ページの「SNMP の監視」
- 147 ページの「システム状態の表示」
- 148 ページの「システムログ」
- 151 ページの「システム監査」
- 153 ページの「環境状態の表示」
- 155 ページの「使用状況の表示」
- 156 ページの「ネットワークルートの表示」
- 157 ページの「システム状態の監視」

SNMP の監視

この節では、SNMP (ネットワーク管理プロトコル) の監視について説明します。この節の内容は、次のとおりです。

- 146 ページの「SNMP 監視について」
- 146 ページの「SNMP の設定」

SNMP 監視について

SNMP (ネットワーク管理プロトコル) 通信を使用可能にすることによって、SNMP 監視を実行できます。Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムでは、SNMP 監視のみをサポートしています。SNMP 管理はサポートしていません。

メッセージ情報ブロック (MIB) を解釈するには、MIB ファイルが必要です。MIB ファイルは、イメージとともに `boot_directory/www/data/mib` ディレクトリにインストールされています。たとえば、`/cvol/nf1/www/data/mib` ディレクトリを使用します。

MIB ファイルは、<http://sunsolve.sun.com> からダウンロードすることもできます。これらのファイルの使用方法については、ネットワーク管理アプリケーションのマニュアルを参照してください。

SNMP の設定

SNMP (ネットワーク管理プロトコル) を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「Monitoring and Notification」>「Configure SNMP」を選択します。
2. 「Enable SNMP」チェックボックスを選択して、SNMP を使用可能にします。
3. 「Server SNMP Community」フィールドに、Sun StorageTek 5320 NAS Appliance が属する SNMP コミュニティーを入力します。
4. 「Contact Info」フィールドに、このシステムの管理者名を入力します。
5. 「System Location」フィールドに、ネットワーク上の場所を入力します。
物理的な場所または論理的な場所のいずれでもかまいません。
6. 新しいターゲットアドレスを追加する場合は、SNMP 表の空白の行に次の情報を入力します。
 - **Destination IP Address** — システムエラーの発生時に、SNMP トラップの宛先として指定するサーバーの TCP/IP アドレスを入力します。
 - **Port #** — システムによってトラップが送信されるポートを入力します。デフォルト値はポート 162 です。
 - **Version** — プルダウンメニューから SNMP のバージョン (1 または 2) を選択します。
 - **Community** — トラップの宛先のコミュニティ文字列を入力します。
 - **Enable** — このターゲットアドレスをトラップの宛先として使用可能にする場合は、この列のチェックボックスを選択します。

7. ターゲットアドレスを削除する場合は、削除する行を選択して「Trash」ボタンをクリックします。
8. 「Apply」をクリックして、変更内容を保存します。

システム状態の表示

Web Administrator グラフィカルユーザーインターフェースにはじめてアクセスすると、基本的なシステム状態が表示されます。状態画面はモデルの機能および物理的特徴に基づいて表示されるため、モデルによって異なります。

この画面に表示される情報は、ご購入先に連絡する際に役立ちます。この情報によって障害が発生した場所を特定できる場合もあります。

システム状態を表示するには、ツールバーの「Home」ボタンをクリックします。

この画面には、表 10-1 に示すデータが読み取り専用で表示されます。

表 10-1 システム状態の表示

項目	表示
Name	サーバー名
Model	システムモデル
Serial #	システムの一意的シリアル番号
Up Time	システムの電源が最後に投入された時点からの経過時間
CPU Load	プロセッサの現在の負荷および最大負荷
OS Version	サーバーのオペレーティングシステムのバージョン
Web Admin Version	システムの Web Administrator のバージョン
Head Status	サーバー H1 の状態 (Cluster のみ): NORMAL、QUIET、ALONE
Partner Status	サーバー H2 の状態 (Cluster のみ): NORMAL、QUIET、ALONE
Features Enabled	システムで使用可能なすべてのオプション機能

システムログ

この節では、システムログについて説明します。この節の内容は、次のとおりです。

- 148 ページの「システムログについて」
- 150 ページの「システムイベントについて」
- 150 ページの「システムログの表示」

システムログについて

システムログには、すべてのシステムイベントの基本情報が表示されます。このログに表示される情報は、発生したエラーおよびその日時を判断する際に重要です。



注意: システムの停止時にログが消去されないようにするには、遠隔ロギングを使用可能にするか、ローカルディスク上にログファイルを作成してください (33 ページの「ロギングの設定」を参照)。システムをはじめて起動するときに、揮発性メモリー内に一時ログファイルが作成され、初期起動中に発生するすべてのエラーが記録されます。

「Display System Log」パネルには、すべてのシステムイベント、警告、およびエラーが、それらの発生日時を含めて表示されます。このパネルには、最新のシステムイベントが自動的に表示され、スクロールバーを使用することで以前のイベントを表示できます。

注: ドライブ構成の変更 (ドライブの削除、挿入など) は、イベントログに反映されるまでに最大 30 秒かかることがあります。そのため、この時間内に複数の変更を行うと、一部のイベントが報告されない場合があります。

次の図に、「Display System Log」パネルを示します。

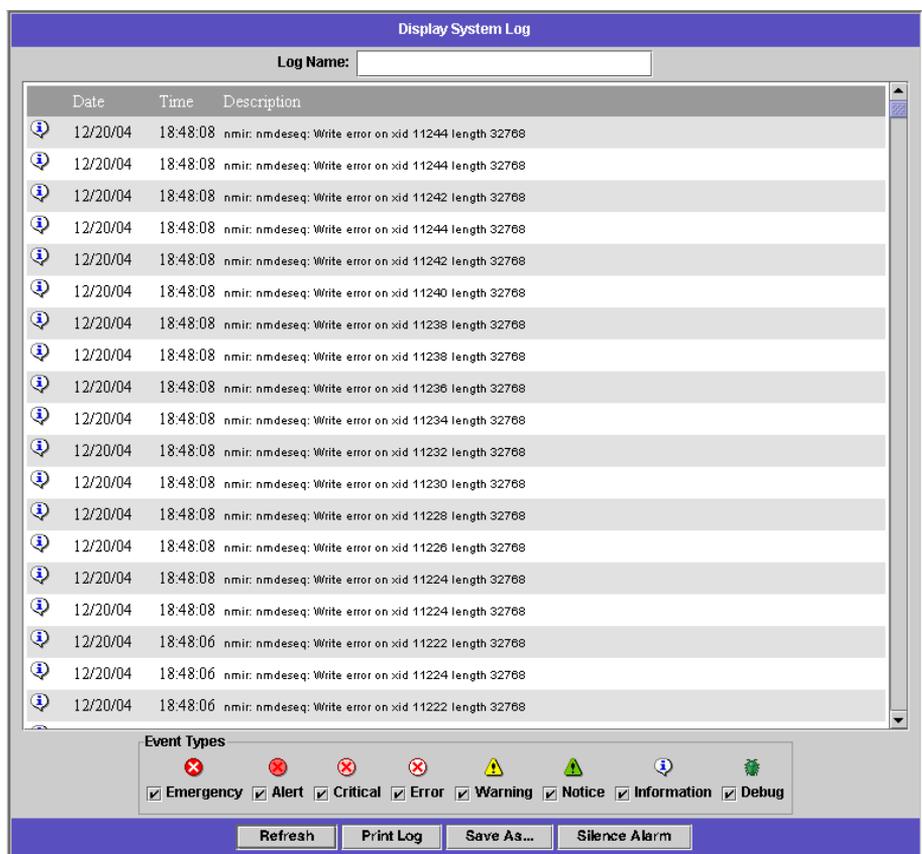


図 10-1 「Display System Log」パネル

システムイベントについて

システムログには、8つのタイプのシステムイベントが記録されます。各イベントは、表 10-2 に示すアイコンで表されます。

表 10-2 システムイベントのアイコン

	Emergency – 緊急メッセージであることを示します。このメッセージは一部のユーザーに送信されます。優先順位が緊急のメッセージは、確認用に別のファイルに記録されます。
	Alert – ただちに対処する必要がある重要メッセージであることを示します。このメッセージはすべてのユーザーに送信されます。
	Critical – ハードウェアの問題など、エラーには分類されない重大メッセージであることを示します。優先順位が重大以上のメッセージはシステムコンソールに送信されません。
	Error – ディスク書き込みの失敗など、エラー状況を表すメッセージであることを示します。
	Warning – 回復可能な異常に関するメッセージであることを示します。
	Notice – 重要な情報メッセージであることを示します。優先順位指定のないメッセージは、この優先順位のメッセージに割り当てられます。
	Information – 情報メッセージであることを示します。このメッセージはシステムの分析に役立ちます。
	Debug – デバッグに関するメッセージであることを示します。

システムログの表示

システムログを表示するには、次の手順を実行します。

- ナビゲーションパネルで、「Monitoring and Notification」>「View System Events」>「Display System Log」を選択します。
- 「Event Types」で、表示するすべてのイベントタイプを選択します。
詳細は、150 ページの「システムイベントについて」を参照してください。
- 「Refresh」をクリックします。

注: システムログに「Unowned SFS2」ボリュームに関するエラーメッセージが含まれている場合は、技術サポートにお問い合わせください。

システム監査

この節では、システム監査について説明します。この節の内容は、次のとおりです。

- 151 ページの「システム監査について」
- 151 ページの「監査の構成について」
- 152 ページの「監査ログファイルについて」
- 152 ページの「システム監査の設定」

システム監査について

システム監査機能は、特定のシステムイベントのレコードをログファイルに格納することによって、システム管理者による監査を可能にします。監査は `syslog` とは異なるもので、システム監査トレールは、ローカルシステム上のバイナリファイルへ書き込まれます。

システム監査は、システム管理者が使用可能に設定し、監査トレール用ストレージボリュームとして構成されたファイルボリュームを使用する必要があります。監査は、**Web Administrator** グラフィカルユーザーインターフェース、オペレータメニュー、または **CLI** コマンドによって、使用可能に設定し構成できます。

監査されるのは少数のイベントに限られます。システムの起動、停止、ディスクパーティションの作成と削除、およびボリュームの作成と削除です。

これらのイベントは設定できません。

監査の構成について

監査に使用するボリュームを指定する必要があります。監査ボリュームには、システムボリューム以外のボリュームを割り当てることができます。システムには、指定したボリュームを監査目的のみに使用するよう強制する機能はありませんが、監査に使用するボリュームを汎用ストレージとして使用しないでください。

監査ログファイルの最大サイズにはデフォルト値が設定されていますが、この値はユーザーが変更できます。現在の監査ログのサイズがこの値に近くなると (差が約 1K バイト以内になると)、そのログファイルは閉じられて新しいログファイルが作成されます。

監査ログファイルについて

監査ログファイルは、日付およびタイムスタンプと、システムのホスト名を使用した形式になります。現在のログファイルは、`YYYYMMDDhhmmss.not_terminated.hostname` の形式になります。

タイムスタンプはグリニッジ標準時 (GMT) 形式です。たとえば、現在のログファイルが Sun StorageTek 5320 NAS Appliance ホスト (testhost) で 2005 年 10 月 21 日午後 1 時 15 分 (GMT) に開始されたとすると、そのファイルは `20051021131500.not_terminated.testhost` になります。

いったんログファイルが閉じられると、そのファイル名は、同じタイムスタンプ形式で変換されます。たとえば、前述の例のログファイルが 2005 年 10 月 30 日午後 7 時 35 分 (GMT) に最大サイズに達した場合、ファイル名は `20051021131500.20051030193500.testhost` に変換されます。

監査ログファイルには、特殊な属性があります。アクセス権がゼロであることに加え、削除できない不変のファイルとしてマークが付けられているため、削除、名前の変更、またはシステム以外からの書き込みが防止されます。これらの属性は、管理者が `chattr` コマンドを使用して削除できます。

注: 現在、監査ログの読み取りまたは削除に対応しているグラフィカルユーザーインタフェースはありません。監査ログはバイナリ形式で格納されるため、`praudit` コマンドを使用して読み取る必要があります。`praudit` コマンドによって、監査ログのバイナリ情報が読みやすいテキストに変換されます。

システム監査の設定

システム監査を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「Monitoring and Notification」 > 「Configure System Auditing」を選択します。
2. システム監査を使用可能にするには、「Enable System Auditing」チェックボックスを選択します。
3. システム監査ログを格納するボリュームを選択します。
システムボリューム以外のボリュームを指定できます。専用の監査ボリュームを作成してください。手順については、46 ページの「「Create File Volumes」パネルを使用したファイルボリュームまたはセグメントの作成」を参照してください。
4. 1M ~ 1024M バイトの範囲で、監査ログファイルの最大サイズを入力します。

ログファイルは、0M バイトから指定した最大サイズまで大きくなります。ファイルが最大サイズに達すると、新しい監査ログファイルが作成されます。既存の監査ログファイルは削除されません。ボリュームがしきい値である 90 % に達すると、警告が送信されてログファイルへの書き込みができなくなります。

5. 「Apply」をクリックして設定を保存します。

環境状態の表示

システムファン、温度、電源装置、および使用電圧に関する情報を表示できます。

この節の内容は、次のとおりです。

- 153 ページの「ファン状態の表示」
- 153 ページの「温度状態の表示」
- 154 ページの「電源装置の状態の表示」
- 154 ページの「電圧状態の表示」

ファン状態の表示

Sun StorageTek 5320 NAS Appliance の本体装置のすべてのファンの動作状態および 1 分あたりの回転数 (RPM) を表示するには、「Monitoring and Notification」 > 「View Environmental Status」 > 「View Fan Status」を選択します。

「View Fan Status」パネルには、各ファンの現在の状態が表示されます。「Status」列の緑色のひし形は、ファンの RPM が正常であることを示します。赤いひし形は RPM が許容範囲を超えていることを示します。いずれかのファンの RPM が 1800 を下回るか、ファンに障害が発生した場合、指定した受信者に電子メールが送信されます。電子メールによる通知の設定については、32 ページの「電子メール通知の設定」を参照してください。

温度状態の表示

温度状態を表示するには、ナビゲーションパネルで「Monitoring and Notification」 > 「View Environmental Status」 > 「View Temperature Status」を選択します。

「View Temperature Status」パネルには、本体装置のセンサーの温度が表示されます。「Status」列の緑色のひし形は、装置が正常な温度範囲で動作していることを示します。赤いひし形は温度が許容範囲を超えていることを示します。温度が摂氏 55

℃ (華氏 131 °F) を超えると、指定した受信者に電子メールメッセージが送信されま
す。電子メールによる通知の設定については、32 ページの「電子メール通知の設
定」を参照してください。

注: 温度のしきい値は変更できません。

電源装置の状態の表示

電源装置の状態を表示するには、ナビゲーションパネルで「Monitoring and
Notification」>「View Environmental Status」>「View Power Supply Status」を選
択してください。

「View Power Supply Status」パネルには、電源装置の状態を示す 3 つの列がありま
す。「Status」列には、電源装置が正常に機能しているかどうかが表示されます。
「Voltage Warning」列および「Temperature Warning」列には、電圧および温度が
許容レベルであるかどうかが表示されます。

これらの列の緑色のひし形は、電圧または温度レベルが正常であることを示します。
赤いひし形は、電圧または温度が許容範囲を超えていることを示します。この場合、
指定した受信者に電子メールによる通知が行われます。電子メールによる通知の詳細
は、32 ページの「電子メール通知の設定」を参照してください。

電圧状態の表示

現在の電圧値を表示するには、ナビゲーションパネルで「Monitoring and
Notification」>「View Environmental Status」>「View Voltage Regulator Status」
を選択します。

各電圧の許容範囲については、表 10-3 を参照してください。

表 10-3 電圧の許容範囲

電圧値	許容範囲
ベースボード 1.2V	1.133V ~ 1.250V
ベースボード 1.25V	1.074V ~ 1.406V
ベースボード 1.8V	1.700V ~ 1.875V
ベースボード 1.8VSB (スタンバイ)	1.700V ~ 1.875V
ベースボード 2.5V	2.285V ~ 2.683V
ベースボード 3.3V	3.096V ~ 3.388V
ベースボード 3.3AUX	3.147V ~ 3.451V

表 10-3 電圧の許容範囲 (続き)

電圧値	許容範囲
ベースボード 5.0V	4.784V ~ 5.226V
ベースボード 5VSB (スタンバイ)	4.781V ~ 5.156V
ベースボード 12V	11.50V ~ 12.56V
ベースボード 12VRM	11.72V ~ 12.80V
ベースボード -12V	-12.62V ~ -10.97V
ベースボード VBAT	2.859V ~ 3.421V
SCSI A 終端電源	4.455V ~ 5.01V
SCSI B 終端電源	4.455V ~ 5.01V
プロセッサ Vccp	1.116V ~ 1.884V

使用状況の表示

ファイルボリュームの使用状況、ネットワークの動作状態、システムの動作状態、およびネットワークポートを表示できます。この節の内容は、次のとおりです。

- 155 ページの「ファイルボリュームの使用量の表示」
- 156 ページの「ネットワークの動作状態の表示」
- 156 ページの「システムの動作状態の表示」
- 156 ページの「ネットワーク (ポート) 統計情報の表示」

ファイルボリュームの使用量の表示

システムのファイルボリュームの使用中の領域および空き領域を表示するには、ナビゲーションパネルで「Monitoring and Notification」>「View File Volume Usage」を選択します。

ファイルボリュームの使用量が 95% を超えると、指定した受信者に電子メールが送信されます。

ネットワークの動作状態の表示

すべての Sun StorageTek 5320 NAS Appliance クライアントの 1 秒あたりの入出力要求数を表示するには、ナビゲーションパネルから「System Activity」>「View Networking Activity」を選択します。

システムの動作状態の表示

Sun StorageTek 5320 NAS Appliance ソフトウェアは、ストレージシステム全体の複数のデバイスの動作状態および負荷を監視します。監視されているデバイスの名前および数は、ハードウェア構成によって異なります。

システムデバイスの入出力要求を表示するには、ナビゲーションパネルで「System Activity」>「View System Activity」を選択します。

「View System Activity」パネルには、システムデバイスおよびネットワークデバイスの動作状態が一覧表示されます。このパネルの各フィールドの詳細は、パネルの「ヘルプ」ボタンをクリックするか、369 ページの「「View System Activity」パネル」を参照してください。

ネットワーク (ポート) 統計情報の表示

ネットワーク (ポート) 統計情報を表示するには、次の手順を実行します。

1. ナビゲーションパネルで、「Network Configuration」>「Configure TCP/IP」>「Configure Network Adapters」を選択します。
「Configure Network Adapters」パネルが表示されます。
2. 「Adapter」リストからポートを選択します。
「Interface」タブと「Statistics」タブに、選択したポートに関する詳細な情報が表示されます。詳細は、353 ページの「「Configure Network Adapters」パネル」を参照してください。

ネットワークルートの表示

ネットワークルートとその表示方法について説明します。この節の内容は、次のとおりです。

- 157 ページの「ネットワークルートについて」
- 157 ページの「ルートの表示」

ネットワークルートについて

ルートには、「ネットワークルート」と「ホストルート」の2種類があります。ネットワークルートは、特定のネットワーク上のホストへのパケット送信に使用されます。ホストルートは頻繁には使用されません。このルートは、既知のネットワークではなく、ほかのホストまたはゲートウェイにのみ接続されているホストへのパケット送信に使用されます。

ルーティングテーブルに表示されるルートフラグの例を次に示します。

- **0x1** – ルートが使用可能であることを示します。
- **0x2** – 宛先がゲートウェイであることを示します。
- **0x4** – 宛先がホストエントリであることを示します。
- **0x8** – ホストまたはネットワークが到達不可能であることを示します。
- **0x10** – 宛先が動的に作成されたことを示します。
- **0x20** – 宛先が動的に変更されたことを示します。

フラグには、個々のフラグの合計を示すものもあります。たとえば、「0x3」は「0x1」と「0x2」の合計で、ルートが使用可能であること (0x1) と、ゲートウェイであること (0x2) を表しています。

ルートの表示

ローカルネットワーク内のすべてのルートの状態を表示するには、ナビゲーションパネルで「Network Configuration」>「View the Routing Table」を選択します。

「View the Routing Table」パネルが表示されます。

システム状態の監視

無停電電源装置 (UPS)、コントローラ、およびミラーの状態を監視できます。詳細は、次の節を参照してください。

- 158 ページの「UPS 監視について」
- 158 ページの「UPS 監視の使用可能への切り替え」
- 159 ページの「コントローラ情報の表示」
- 159 ページの「ミラーの状態の監視について」
- 159 ページの「ミラー化の状態の表示」

UPS 監視について

無停電電源装置 (UPS) を持つ装置を設置した場合は、UPS を監視することができます。

注: UPS 監視を使用可能にする場合は、事前に Sun StorageTek 5320 NAS Appliance システムに UPS を接続してください。UPS が接続されていないと、監視システムは UPS 障害を通知します。Sun StorageTek 5320 NAS Appliance では UPS 監視のみをサポートしており、UPS 管理はサポートしていません。UPS の使用法の詳細は、297 ページの「補助ローカル UPS への接続」を参照してください。

UPS 監視では、次の場合に通知が行われます。

- **電源障害** — 電源障害が発生し、システムがバッテリーの電力で動作していることを示します。
- **電源の復旧** — 電源が復旧したことを示します。
- **バッテリー低下** — バッテリーの電力が低下していることを示します。
- **バッテリー充電完了** — UPS のバッテリーが正常レベルまで充電されたことを示します。
- **バッテリー交換** — UPS のバッテリーに異常が検出されたため、バッテリーの交換が必要であることを示します。
- **UPS アラーム** — UPS の周辺温度または湿度が安全なしきい値の範囲外であることが検出されたことを示します。
- **UPS 障害** — システムが UPS と通信できないことを示します。

バッテリー充電完了以外のすべてのエラーは、エラー通知電子メール、SNMP (ネットワーク管理プロトコル) サーバーへの通知、LCD パネルでの表示、およびシステムログでの表示によってユーザーに通知されます。バッテリー充電完了は、電子メール、SNMP サーバー、およびシステムログでのみ通知されます。LCD パネルには表示されません。

UPS 監視の使用可能への切り替え

無停電電源装置 (UPS) 監視を使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「Monitoring and Notification」>「Enable UPS Monitoring」を選択します。
2. 「Enable UPS Monitoring」を選択します。
3. 「Apply」をクリックして、変更内容を保存します。

コントローラ情報の表示

「View Controller Information」パネルには、RAID コントローラのベンダー、モデル、およびファームウェアリリースが読み取り専用で表示されます。

コントローラのベンダー、モデル、およびファームウェアリリース情報を表示するには、ナビゲーションパネルで「RAID」>「View Controller Enclosure Information」を選択します。

ミラーの状態の監視について

ミラーの状態は「Manage Mirrors」パネルに表示されます。ミラーの状態には、次のようなものがあります。

- **New** — 新しいミラーが作成されています。
- **Creating mirror log** — ミラーバッファが初期化されています。
- **Connecting to host** — アクティブサーバーが遠隔ミラーサーバーに接続していません。
- **Creating extent** — ミラーサーバーがディスクパーティションを作成しています。
- **Ready** — システムの準備が完了して、他方のシステムの準備が完了するまで待機しています。
- **Down** — ネットワークリンクが停止しています。
- **Cracked** — ミラーが破損しています。
- **Syncing Volume** — ミラーサーバーがファイルボリュームと同期をとっています。
- **In Sync** — ミラーは同期がとれています。
- **Out of Sync** — ミラーは同期がとれていません。
- **Error** — エラーが発生しました。

ミラー化の状態の表示

Sun StorageTek 5320 NAS Appliance ソフトウェアは、ミラー化ファイルボリュームのさまざまなネットワーク統計情報を維持します。ミラー化された各ファイルボリュームに関するこれらの統計情報は、アクティブサーバーおよびミラーサーバー上で確認できます。

ミラーの統計情報を表示するには、次の手順を実行します。

1. ナビゲーションパネルから、「File Replicator」>「View Mirror Statistics」を選択します。
2. 「Select Volume」リストから、目的のファイルボリュームを選択します。

システムによって、そのミラー化ファイルボリュームのその後の状態、受信トランザクション、送信トランザクション、ミラーバッファー、およびネットワーク統計情報が表示されます。詳細は、パネルの「**Help**」ボタンをクリックするか、317 ページの「**View Mirror Statistics**」パネルを参照してください。

第11章

システムの保守

この章では、システムの保守機能について説明します。この章は、次の節で構成されています。

- 161 ページの「遠隔アクセスオプションの設定」
- 162 ページの「FTP アクセスの構成」
- 164 ページの「サーバーの停止」
- 164 ページの「ファイルのチェックポイントの管理」
- 170 ページの「NDMP バックアップの設定」
- 171 ページの「タイムゾーンデータベースの更新」
- 173 ページの「CATIA V4/V5 文字変換の使用可能への切り替え」
- 175 ページの「Sun StorageTek 5320 NAS Appliance ソフトウェアの更新」
- 176 ページの「アレイおよびドライブのファームウェアバージョンのアップグレード」

遠隔アクセスオプションの設定

システムのセキュリティー機能を使用して、遠隔アクセスオプションを設定できます。システムへの遠隔アクセスに使用するネットワークサービスを使用可能または使用不可に設定できます。セキュリティー保護されたモードでシステムを実行して安全性を最大限に高めたり、Telnet、遠隔ログイン、リモートシェルなどの特定の遠隔アクセス機能を使用可能にしたりすることができます。

セキュリティー保護されたサービスは、ハイパーテキスト転送プロトコル (HTTP) 上で SSL (Secure Socket Layer) を使用する Secure Web Admin、および Secure Shell (ssh) です。

遠隔アクセスセキュリティーを設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Set Remote Access」を選択します。
2. 安全性を最大限に高めるには、「Secure Mode」チェックボックスを選択します。「Secure Mode」では、該当するチェックボックスを選択して Secure Web Admin および Secure Shell のみを使用可能にできます。
3. 「Secure Mode」を選択しない場合は、次のうちから使用可能にするサービスのチェックボックスをそれぞれ選択します。
 - Web Admin
 - Telnet
 - Remote Login
 - Remote Shell
4. 「Apply」をクリックします。
5. 「Secure Mode」を選択した場合は、サーバーを再起動して設定を有効にします。詳細は、164 ページの「サーバーの停止」を参照してください。

FTP アクセスの構成

この節では、ファイル転送プロトコル (FTP) アクセスの構成について説明します。この節の内容は、次のとおりです。

- 162 ページの「FTP アクセスの構成について」
- 163 ページの「FTP ユーザーの設定」

FTP アクセスの構成について

ファイル転送プロトコル (FTP) は、クライアントとサーバー間でファイルをコピーするために使用されるインターネットプロトコルです。FTP では、サーバーへのアクセスを要求する各クライアントを、ユーザー名およびパスワードで識別します。

次の 3 つのタイプのユーザーを設定できます。

- **管理者** – admin というユーザー名を持ち、グラフィカルユーザーインタフェース (GUI) クライアントと同じパスワードを使用します。

管理者は、システム上のすべてのボリューム、ディレクトリ、およびファイルにスーパーユーザーでアクセスできます。管理者のホームディレクトリは、「/」記号と定義されます。

- **ユーザー** – ローカルのパスワードファイル、あるいは遠隔ネットワーク情報サービス (NIS)、NIS+、または LDAP (Lightweight Directory Access Protocol) ネームサーバーに指定されているユーザー名およびパスワードを持ちます。

ユーザーは、自身のホームディレクトリに含まれる既存のすべてのディレクトリおよびファイルへのアクセス権を持ちます。ホームディレクトリは、ユーザーのアカウント情報の一部として定義され、ネームサービスによって取得されます。

- **ゲスト** – ユーザー名 `ftp` またはそのエイリアス `anonymous` でログインします。パスワードが要求されますが、認証されません。すべてのゲストユーザーは、`ftp` ユーザーのホームディレクトリに含まれるすべてのディレクトリおよびファイルへのアクセス権を持ちます。

注: ゲストユーザーは、ファイルの名前の変更、上書き、または削除を行うことができません。また、ディレクトリの作成または削除、および既存のファイルまたはディレクトリのアクセス権の変更を行うこともできません。

FTP ユーザーの設定

ファイル転送プロトコル (FTP) ユーザーを設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「UNIX Configuration」>「Set Up FTP」を選択します。
2. 「Enable FTP」チェックボックスを選択します。
3. 該当するチェックボックスをクリックして、FTP アクセスのタイプを選択します。
 - 「Allow Guest Access」を選択すると、匿名ユーザーによる FTP サーバーへのアクセスが可能になります。
 - 「Allow User Access」を選択すると、すべてのユーザーによる FTP サーバーへのアクセスが可能になります。これには、`admin` ユーザーまたはスーパーユーザーは含まれません。

注: ユーザー名およびパスワードは、ローカルのパスワードファイル、あるいは遠隔ネットワーク情報サービス (NIS)、NIS+、または LDAP (Lightweight Directory Access Protocol) ネームサーバーで指定してください。
 - 「Allow Admin Access」を選択すると、管理パスワードでの、FTP サーバーへのスーパーユーザーとしてのアクセスが可能になります。管理パスワードの使用には注意が必要です。

注: スーパーユーザーとは、UID が 0 に設定されているユーザー、および Sun StorageTek 5320 NAS Appliance の特別なユーザーである `admin` を示します。
4. ロギングを使用可能にするには、「Enable Logging」チェックボックスを選択して、ログファイルのパス名を指定します。

ログファイルは、NAS サーバーで指定したエクスポート済みのボリュームに保存されます。たとえば、/vol1/ftpllog と指定すると、ftpllog というログファイルが /vol1 ディレクトリに保存されます。

5. 「Apply」をクリックして設定を保存します。

サーバーの停止

「Shut Down the Server」パネルを使用して、サーバーを停止または再起動できます。Telnet を使用したシステムの停止方法については、266 ページの「システムの停止」を参照してください。

サーバーを停止または再起動するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」>「Shut Down the Server」を選択します。
2. 実行する停止の種類を選択します。選択可能な停止オプションの詳細は、パネルの「ヘルプ」ボタンをクリックするか、382 ページの「「Shut Down the Server」パネル」を参照してください。

注意: 「Reboot Previous Version」オプションを選択する前に、技術サポートに確認してください。

3. 「Apply」をクリックします。



ファイルのチェックポイントの管理

この節では、ファイルのチェックポイントの管理について説明します。この節の内容は、次のとおりです。

- 165 ページの「ファイルのチェックポイントについて」
- 165 ページの「ファイルのチェックポイントの作成」
- 166 ページの「ファイルのチェックポイントのスケジュール設定」
- 168 ページの「チェックポイントの名前の変更」
- 169 ページの「チェックポイントの削除」
- 169 ページの「ファイルのチェックポイントの共有」
- 170 ページの「ファイルのチェックポイントへのアクセス」

ファイルのチェックポイントについて

チェックポイント（「整合点」または「c点」とも呼ばれる）は、一次ファイルボリュームの読み取り専用の仮想コピーです。ファイルボリュームに対する読み取り/書き込み操作は引き続き行われますが、チェックポイントの作成時に存在したデータをすべて使用することができます。チェックポイントを使用して、誤って変更または削除したファイルを取得したり、バックアップの一貫性を確保したりします。

注: チェックポイントはファイルボリュームの仮想コピーで、そのボリュームと物理的に同一の場所に格納されます。オンラインバックアップではありません。ファイルボリュームが失われると、チェックポイントもすべて失われます。

ファイルのチェックポイントを使用するには、チェックポイントを使用可能にして、個々のチェックポイントまたはチェックポイントスケジュールを作成してください。

ファイルのチェックポイントの作成

チェックポイントのスケジュールを設定するか、即時にチェックポイントを作成するかを選択できます。定期的なチェックポイントスケジュールの設定方法については、166 ページの「ファイルのチェックポイントのスケジュール設定について」を参照してください。

「**Manage Checkpoints**」パネルでは、既存のチェックポイントの名前の変更および削除だけでなく、即時にチェックポイントを作成できます。事前に設定した日時に作成されるようにスケジュール設定されたチェックポイントとは異なり、この画面でいつでもチェックポイントを即時に作成できます。

新しいチェックポイントを手動で作成するには、次の手順を実行します。

1. ナビゲーションパネルで、「**File Volume Operations**」 > 「**Edit Volume Properties**」を選択します。
2. 「**Volume Name**」プルダウンメニューから、チェックポイントを作成するボリュームを選択します。
3. 「**Enable Checkpoints**」ボックスにチェックマークが表示されていることを確認します。
表示されていない場合は、ボックスを選択して「**Apply**」をクリックします。
4. ナビゲーションパネルで、「**File Volume Operations**」 > 「**Configure Checkpoints**」 > 「**Manage Checkpoints**」を選択します。
5. 新しいチェックポイントを作成するには、「**Create**」をクリックします。
6. 「**Volume Name**」プルダウンメニューから、チェックポイントを作成するボリュームを選択します。

7. いずれかのチェックポイントオプションを選択します。これらのオプションの詳細は、パネルの「ヘルプ」ボタンをクリックするか、327 ページの「「Create Checkpoint」 ウィンドウ」を参照してください。
8. 「Apply」をクリックして、チェックポイントを作成します。

ファイルのチェックポイントのスケジュール設定

この節では、ファイルのチェックポイントのスケジュール設定について説明します。この節の内容は、次のとおりです。

- 166 ページの「ファイルのチェックポイントのスケジュール設定について」
- 167 ページの「チェックポイントのスケジュールへの追加」
- 168 ページの「既存のチェックポイントスケジュールの編集」
- 168 ページの「スケジュールの行の削除」

ファイルのチェックポイントのスケジュール設定について

「Schedule Checkpoints」パネルには現在のチェックポイントスケジュールが表示され、スケジュール設定されたチェックポイントを追加、編集、および削除できます。この画面には、スケジュール設定された各チェックポイントのファイルボリューム名、説明、設定日時、およびチェックポイントが保持される期間が表示されます。「Keep」の期間は、日数と時間で表示されます。

スケジュールの行を追加すると、要求した日時のチェックポイントがシステムで自動的に設定されます。

ボリュームごとに、最大 5 つのチェックポイントのスケジュールを設定できます。1 つのスケジュールに複数のチェックポイントを指定できます。

複数のチェックポイントの例を次に示します。

		Days	Hours AM	Hours PM	Keep	
Enabled	Description	SMTWTFS	M1234567890E	M1234567890E	Days + Hours	
1. Y	MTWTF5am5pm	-*****-	-----*-----	-----*-----	1	0
2. Y	SunWed1pm	*--*---	-----	-*-----	0	12
3. Y	MWFmidnight	-**-*-*	*-----	-----	0	3
4. Y	Weekend	*-----*	*-----*	*-----*	0	6
5. Y	FriEvery2hrs	-----*-	*-**-*-*-*-*	*-**-*-*-*-*	0	2

チェックポイントのスケジュールへの追加

チェックポイントをスケジュールに追加するには、次の手順を実行します。

1. ファイルボリュームのチェックポイントを使用可能にします。
2. チェックポイントをスケジュールに追加します。

ファイルボリュームのチェックポイントを使用可能にするには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Edit Volume Properties」を選択します。
2. 「Volume Name」プルダウンメニューから、チェックポイントを追加するボリュームを選択します。
3. 「Enable Checkpoints」ボックスにチェックマークが表示されていることを確認します。

表示されていない場合は、ボックスを選択して「Apply」をクリックします。

チェックポイントをスケジュールに追加するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Configure Checkpoints」 > 「Schedule Checkpoints」を選択します。
2. スケジュールにチェックポイントを追加するには、「Add」をクリックします。
3. チェックポイントをスケジュール設定するファイルボリュームを選択します。
4. チェックポイントの説明を入力します。
これは必須フィールドです。たとえば、「毎週」、「毎日」など、チェックポイントの間隔を入力します。
5. 「Keep Days + Hours」ドロップダウンボックスから、チェックポイントを保持する日数および時間を選択します。
6. チェックポイントを作成する曜日を選択します。
このリストから複数の曜日を選択するには、Ctrl キーを押しながら追加の曜日をマウスでクリックします。
7. 「AM Hours」リストから、チェックポイントを作成する午前の時刻を選択します。
このリストから複数の項目を選択するには、Ctrl キーを押しながら追加の項目をマウスでクリックします。
8. 「PM Hours」リストから、チェックポイントを作成する午後または夜の時刻を選択します。

このリストから複数の項目を選択するには、Ctrl キーを押しながら追加の項目をマウスでクリックします。

9. 「Apply」をクリックして、変更内容を保存します。

既存のチェックポイントスケジュールの編集

既存のチェックポイントスケジュールを編集するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Configure Checkpoints」 > 「Schedule Checkpoints」を選択します。
2. 編集するスケジュールの行を選択し、「Edit」をクリックします。
この画面に表示される情報は、ボリューム名を変更できない点を除いて「Add Checkpoint Schedule」ウィンドウの情報とまったく同じです。
3. 関連する情報を編集します。
詳細は、167 ページの「チェックポイントのスケジュールへの追加」を参照してください。
4. 「Apply」をクリックして、変更内容を保存します。

スケジュールの行の削除

スケジュールの行を削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Configure Checkpoints」 > 「Schedule Checkpoints」を選択します。
2. 削除するスケジュールの行をクリックして選択し、「Remove」をクリックします。

チェックポイントの名前の変更

チェックポイントの名前を変更するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」 > 「Configure Checkpoints」 > 「Manage Checkpoints」を選択します。
2. 名前を変更するチェックポイントを選択し、「Rename」をクリックします。
「Volume Name」および「Old Name」フィールドは読み取り専用です。
3. 「New Name」にチェックポイントの新しい名前を入力します。



注意: 「Auto Delete」を指定したチェックポイントの名前を通常の名前に変更すると、そのチェックポイントには自動削除が実行されなくなります。

4. 「Apply」をクリックして、変更内容を保存します。

チェックポイントの削除

チェックポイントを削除するには、次の手順を実行します。

1. ナビゲーションパネルで、「File Volume Operations」> 「Configure Checkpoints」> 「Manage Checkpoints」を選択します。
2. 削除するチェックポイントを選択し、「Remove」をクリックします。

ファイルのチェックポイントの共有

ユーザーはチェックポイントを共有して、チェックポイント作成時のデータにアクセスできます。

ファイルのチェックポイントを共有するには、次の手順を実行します。

1. ナビゲーションパネルで、「Windows Configuration」> 「Configure Shares」を選択します。
2. 「Add」をクリックします。
3. 「Share Name」ボックスに、チェックポイントの新しい共有名を入力します。
共有名は、ネットワークからチェックポイントにアクセスするために使用されません。
4. (省略可能) 「Mac Extensions」チェックボックスを選択します。
「Mac Extensions」オプションは、デフォルトで選択されています。
5. 「Volume Name」プルダウンメニューボックスをクリックし、リストからチェックポイントボリュームを選択します。
チェックポイントボリュームには、.chkpnt 拡張子が付いています。
6. 「Directory」フィールドは、空白のままにします。
7. Active Directory サービス (ADS) が使用可能で構成済みの場合は、「Container」テキストボックスに ADS コンテキストを入力します。
8. 次のフィールドおよびオプションが使用可能な場合は、次のように指定します。
 - 「User」ボックスに 0 と入力します。
 - 「Group」ボックスに 0 と入力します。

- 「R/W Password」ボックスおよび「R/O Password」ボックスは、空白のままにしておきます

チェックポイントボリュームは読み取り専用です。

これらのフィールドおよびオプションは、システムが NT ドメインモード用に構成されている場合は使用不可になります。

9. 「Apply」をクリックします。

「Configure Shares」パネルに、新しいチェックポイントが共有として表示されていることを確認してください。

ファイルのチェックポイントへのアクセス

ユーザーはチェックポイントにアクセスして、チェックポイント作成時のデータにアクセスできます。

ファイルのチェックポイントにアクセスするには、次の手順を実行します。

1. ネットワークステーションを使用して、Windows の「スタート」メニューをクリックします。
2. 「ファイル名を指定して実行」を選択します。
3. 「ファイル名を指定して実行」ウィンドウに、Sun StorageTek 5320 NAS Appliance サーバーのインターネットプロトコル (IP) アドレスとチェックポイントの共有名を入力します。
たとえば、「\\xxx.xxx.xxx.xxx\sharename」と入力します。
4. 「OK」をクリックします。

NDMP バックアップの設定

Network Data Management Protocol (NDMP) は、ネットワークベースのバックアップ用のオープンなプロトコルです。NDMP アーキテクチャーによって、NDMP 準拠のバックアップ管理アプリケーションを使用して、ネットワーク接続ストレージデバイスをバックアップできます。

注: バックアップ管理アプリケーションは、コンソール管理者がコマンド行インタフェースで使用するユーザー名「administrator」とそのパスワードでログオンするように構成することをお勧めします。

注: NDMP を使用してバックアップを実行するボリュームでは、チェックポイントを使用可能にしてください。詳細は、165 ページの「ファイルのチェックポイントの作成」を参照してください。

ローカルバックアップを実行する場合は、NDMP は必要ありません。

NDMP を設定するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Backup」 > 「Set Up NDMP」を選択します。
2. バックアップテープドライブへのデータ転送に使用する NDMP ネットワークインタフェースカード (NIC) を選択します。
3. 各ポートについて表示されるゲートウェイアドレスを確認します。
NDMP バックアップテープデバイスが別のネットワークに存在する場合は、適切なゲートウェイに接続するポートを選択する必要があります。
4. 「Apply」をクリックします。

タイムゾーンデータベースの更新

Sun StorageTek NAS 5320 Appliance サーバーは、世界の主要なタイムゾーンをサポートしており、夏時間 (DST) に合わせて現地時間を調整するように設計されています。夏時間の必要性は国や地域によって異なり、DST の期間も異なります。

ソフトウェアリリース 4.10 以降では、<ftp://elsie.nci.nih.gov/pub> で入手可能なタイムゾーンの標準データベース形式を使用しています。

次の節では、NAS サーバー上のタイムゾーンおよび DST の情報を更新する方法について説明します。

1. 現在のタイムゾーンデータベースファイルを <ftp://elsie.nci.nih.gov/pub/> からダウンロードします。
タイムゾーンデータベースファイルは、`tzdataYYYYn.tar.gz` という tar ファイルとして配布されています。YYYY は年を表します。たとえば、`tzdata2005n.tar.gz` という名前になります。
2. `gunzip` および `tar` を使用してデータベースファイルを展開します。
展開されるファイルは、表 11-1 に示すように、さまざまな大陸および地域に対応します。
ファイル名が 8 文字を超えている場合は、展開時に 8 文字のファイル名に変換されます。8 文字のファイル名は /`cv01` ディレクトリの制限事項です。名前が 8 文字を超えるファイルを個別にダウンロードする場合は、ファイルの名前を手動で変更してください。

3. /cvol/defstart での現在の起動ディレクトリ設定に応じて、/cvol/nf1/tz または /cvol/nf2/tz に適切なファイルをコピーします。

defstart ファイルには、1 または 2 が含まれています。これらはそれぞれ、nf1 または nf2 を表します。

次の例では、northamerica データベースファイルが nf1 起動ディレクトリにコピーされます。

```
cp northamerica /cvol/nf1/tz/northame
```

表 11-1 に、各データベースファイルのファイル名と、対応する大陸を示します。タイムゾーンの略語については、

<http://www.timeanddate.com/library/abbreviations/timezones> を参照してください。

表 11-1 タイムゾーンデータベースファイル

ファイル名	大陸/地域
africa	アフリカ
antarctica	南極
asia	アジア
australiasia	オーストラリアおよび太平洋諸島
etcetera	DST なし。GMT オフセットのみ
europe	欧州諸国
northamerica	北米
pacificnew	大統領選挙期間用の代替ルール
solar87	サウジアラビアで 1987 年に行われた特殊な時刻修正
southamerica	南米

4. CLI で zic を使用して、該当する地域のタイムゾーンデータベースファイルをインストールします。

たとえば、次のコマンドを実行すると、northamerica タイムゾーンが nf1 起動ディレクトリにインストールされます。

```
zic /cvol/nf1/tz/northame
```

新しいタイムゾーンを有効にするために、サーバーを再起動する必要はありません。

CATIA V4/V5 文字変換の使用可能への切り替え

Sun StorageTek 5320 NAS Appliance および Gateway システムは、Dessault Systemes 社が開発した CATIA V4/V5 製品と相互運用できます。次に続く節では、CATIA ソフトウェアについて説明します。

- 173 ページの「CATIA V4/V5 文字変換について」
- 174 ページの「CLI による CATIA の使用可能への切り替え」
- 174 ページの「再起動時の CATIA の使用可能への自動切り替え」

CATIA V4/V5 文字変換について

Sun StorageTek 5320 NAS Appliance および Gateway システムは、Dessault Systemes 社が開発した CATIA V4/V5 製品と相互運用できます。

CATIA V4 は UNIX のみに対応する製品ですが、CATIA V5 は UNIX および Windows の両方のプラットフォームで使用できます。CATIA V4 では、ファイル名に Windows では使用できない文字を使用する可能性があります。CATIA ユーザーが V4 から V5 に移行する際、V4 のファイル名に Windows では使用できない文字が含まれていると、Windows から V4 のファイルにアクセスできなくなる場合があります。そのため、CATIA V4/V5 では文字変換オプションを提供することにより、UNIX/Windows の相互運用性を維持しています。

表 11-2 に、変換表を示します。

表 11-2 CATIA 文字変換表

CATIA V4 の UNIX 文字	CATIA V5 の Windows 文字	CATIA V5 の文字の説明
曲線的な 開き二重引用符 (表示不可)	”	ウムラウト
*	⊠	通貨記号
/	ø	ローマ字の小文字 O とスラッシュ
:	÷	除算記号
<	«	左角引用符
>	»	右角引用符

表 11-2 CATIA 文字変換表 (続き)

CATIA V4 の UNIX 文字	CATIA V5 の Windows 文字	CATIA V5 の文字の説明
?	¿	逆疑問符
\	ÿ	ローマ字の小文字 Y とウムラウト
	破線垂直バー (表示不可)	破線垂直バー

CATIA V4/V5 の相互運用性サポートは、デフォルトで使用不可になっています。この機能は、コマンド行インタフェース (CLI) を介して手動で使用可能にするか、システム起動後自動的に使用可能にすることができます。

CLI による CATIA の使用可能への切り替え

コマンド行インタフェース (CLI) を使用して CATIA を使用可能にするには、コマンド `load catia` を実行します。

この方法を使用する場合は、システムを再起動するたびに CATIA サポートを使用可能にする必要があります。

再起動時の CATIA の使用可能への自動切り替え

再起動時に自動的に CATIA を使用可能にするには、次の手順を実行します。

1. `/dvol/etc/inetload.ncf` を編集して、ファイル内の新しい行に `catia` という語を追加します。
2. 次の 2 つの CLI コマンドを実行して `inetload` サービスを再開します。

```
unload inetload
```

```
load inetload
```

CATIA V4/V5 サポートが正常に使用可能になると、次のようなエントリがシステムログに表示されます。

```
07/25/05 01:42:16 I catia: $Revision: 1.1.4.1
```

Sun StorageTek 5320 NAS Appliance ソフトウェアの更新

最新のソフトウェアバージョンを入手するには、www.sunsolve.sun.com にアクセスしてください。ダウンロードするバージョンが不明な場合は、使用しているシステム構成に適したファイルの入手方法を Sun の技術サポートに問い合わせてください。ファイルを手に入れたら、「Update Software」パネルを使用して Sun StorageTek 5320 NAS Appliance ソフトウェアを更新します。



注意: RAID (Redundant Array of Independent Disks) サブシステムで重大な障害が発生しているときに、システムソフトウェアまたは RAID ファームウェアを更新して、新しいボリュームを作成したり既存のボリュームを再構築したりしないでください。

次の手順では、更新処理の完了後にシステムを再起動する必要があります。システムを再起動するにはすべての入出力を停止する必要があるため、ソフトウェアの更新は計画した保守期間内に実施してください。

注: クラスタ構成では、クラスタ内の両方のサーバーでこの手順を実行してから、サーバーを再起動してください。クラスタは更新する前に最適モードにすることをお勧めします。

ソフトウェアを更新するには、次の手順を実行します。

1. ナビゲーションパネルで、「System Operations」 > 「Update Software」を選択します。
2. 「Update Software」パネルで、更新ファイルが格納されている場所へのパスを入力します。
パスを検索する必要がある場合は、「Browse」をクリックします。
3. 「Update」をクリックして処理を開始します。
4. 更新処理が完了したら、「Yes」をクリックしてシステムを再起動するか、「No」をクリックして再起動せずに操作を続行します。
更新内容は、システムを再起動すると有効になります。

アレイおよびドライブのファームウェアバージョンのアップグレード

この節では、アレイおよびドライブの現在のファームウェアバージョンの確認方法と、ファームウェアのアップグレード方法について説明します。この節では、次の事項について説明します。

- 176 ページの「ファームウェアのアップグレードの必要性の確認」
- 176 ページの「アレイファームウェアおよびドライブファームウェアのアップグレード (再起動が必要)」
- 179 ページの「アレイファームウェアのアップグレード (再起動は不要)」
- 184 ページの「ドライブファームウェアのアップグレード (再起動が必要)」
- 185 ページの「raidctl コマンドの出力の取得」

ファームウェアのアップグレードの必要性の確認

ファームウェアのアップグレードを開始する前に、各アレイコンポーネントの現在のファームウェアバージョンを確認して、アップグレードが必要かどうかを判断します。

raidctl profile コマンドを使用すると、RAID コントローラ装置、拡張ユニット、コントローラ NVSRAM、およびドライブの現在のファームウェアバージョンをそれぞれ取得し記録できます。詳細は、185 ページの「raidctl コマンドの出力の取得」を参照してください。

アレイファームウェアおよびドライブファームウェアのアップグレード (再起動が必要)

この手順を実行して、RAID アレイファームウェアおよびドライブファームウェアをアップグレードします。この手順では、NAS サーバーを再起動する必要があります。

NAS サーバーの再起動ができず、アレイファームウェアのみをアップグレードする必要がある場合は、179 ページの「アレイファームウェアのアップグレード (再起動は不要)」を参照してください。

ファームウェアのアップグレードを完了するために必要な時間は、使用する構成によって異なります。たとえば、単一の NAS サーバーに 2 台の RAID コントローラ、1 台のファイバチャネル (FC) 拡張ユニット、および 1 台のシリアル ATA (Serial

Advanced Technology Attachment、SATA) 拡張ユニットが取り付けられている場合、アップグレードおよび再起動に必要な時間は約 50 分です。表 11-4 を参照して、使用する構成をアップグレードするために必要な時間を確認してください。

注: ドライブファームウェアのアップグレードでは、常に NAS サーバーを再起動する必要があります。

注: すでに現在のファームウェアファイルと同じファームウェアバージョンになっているドライブも含めて、ドライブ種別ごとにすべてのドライブがアップグレードされます。



注意: ドライブに障害が発生し、再構築状態にある場合は、この手順を実行しないでください。この情報は、システムログまたは Web Administrator の「RAID」ページで参照できます。

この手順を開始する前に、NAS サーバーのソフトウェア version 4.10 Build 18 以降がインストールされていることを確認してください。それより前のバージョンのオペレーティングシステム (OS) がインストールされている NAS サーバーでは、アレイおよびドライブファームウェアのアップグレードを行わないでください。NAS サーバーソフトが古いバージョンの場合は、www.sunsolve.sun.com にアクセスして最新のソフトウェアバージョンを入手してください。

アレイおよびドライブのファームウェアをアップグレードするには、次の手順を実行します。

1. www.sunsolve.sun.com から最新のパッチをダウンロードし、ファイルを解凍します。
2. パッチの readme ファイルを参照して、パッチに関連付けられているファームウェアバージョンを確認します。
3. NAS クライアントから、FTP を使用可能にします。
GUI を使用して FTP を使用可能にする方法については、162 ページの「FTP アクセスの構成について」を参照してください。CLI を使用する場合は、263 ページの「ファイル転送プロトコル (FTP) アクセスの構成」を参照してください。
4. パッチのダウンロード先のディレクトリに移動します。
5. FTP を使用して NAS サーバーに接続し、admin ユーザーでログインします。
6. bin と入力してバイナリモードへ移行します。
7. ftp プロンプトで次のコマンドを実行して、/cvol 上に各ディレクトリを作成します。

```
mkdir /cvol/firmware
```

```
mkdir /cvol/firmware/2882
```

```
mkdir /cvol/firmware/2882/ctlr
```

```
mkdir /cvol/firmware/2882/nvsram
```

```
mkdir /cvol/firmware/2882/jbod
mkdir /cvol/firmware/2882/drive
```

8. ファームウェアを格納するために作成したディレクトリに移動し、put コマンドを使用してファームウェアファイル (表 11-3 を参照) をコピーします。
- たとえば、RAID コントローラのファームウェアを読み込むには、次のコマンドを実行します。

```
cd /cvol/firmware/2882/ctrlr
put SNAP_288X_06120910.dlp
```

注: ファームウェアファイル名は、関連付けられたディレクトリにファームウェアがコピーされたあと、切り詰められます。

9. 同じ手順を続けて、各ファームウェアファイルを適切なディレクトリに読み込みます。

表 11-3 に、各コンポーネントのディレクトリおよびファームウェアファイルの例を示します。

表 11-3 コンポーネントのファームウェアディレクトリおよびファイル

コンポーネント	ディレクトリ	ファイル名の例
RAID コントローラ	/cvol/firmware/2882/ctrlr	SNAP_288X_06120910.dlp
RAID コントローラ NVSRAM	/cvol/firmware/2882/nvsram	N2882-612843-503.dlp
FC 拡張ユニット (EU)	/cvol/firmware/2882/jbod	esm9631.s3r
SATA EU	/cvol/firmware/2882/jbod	esm9722.dl
ドライブの種類:		
Seagate ST314680	/cvol/firmware/2882/drive	D_ST314680FSUN146G_0407.dlp
Seagate 10K	/cvol/firmware/2882/drive	D_ST314670FSUN146G_055A.dlp
Hitachi 400GB HDS724040KLSA80	/cvol/firmware/2882/drive	D_HDS7240SBSUN400G_AC7A.dlp
Fujitsu MAT3300F 300GB	/cvol/firmware/2882/drive	D_MAT3300FSUN300G_1203.dlp
Seagate 10K 300GB	/cvol/firmware/2882/drive	D_ST330000FSUN300G_055A.dlp

10. FTP セッションからログアウトします。
11. Telnet を使用して NAS サーバーに接続し、admin 権限を持つユーザーアカウントでログインします。
12. システムを再起動します。クラスタ構成では、両方のサーバーを再起動します。

次の表に、各コンポーネントのファームウェアをアップグレードするために必要なおおよその時間を示します。

表 11-4 ファームウェアのアップグレード時間

コンポーネント	アップグレードを完了するために要する時間
RAID コントローラ	再起動時間 + 15 分
RAID コントローラ NVSRAM	再起動時間 + 5 分
FC EU または SATA EU	再起動時間 + 5 分
ドライブ	再起動時間 + ドライブごとに 1.5 分

13. 次のコマンドを実行して、新しいファームウェアが読み込まれていることを確認します。

```
raidctl get type=lsi target=profile ctrl=0
```

システムログで障害を確認することもできます。

アレイファームウェアのアップグレード (再起動は不要)

この手順では、NAS サーバーを再起動することなく、RAID アレイファームウェアをアップグレードします。

この手順を開始する前に、次の事項に注意してください。

- NAS サーバーソフトウェア version 4.10 Build 18 以降がインストールされている必要があります。それより前のバージョンの OS がインストールされている NAS サーバーでは、ファームウェアのアップグレードを行わないでください。
- この手順は、入出力動作が制限されている状態で実行することをお勧めします。この手順の実行中、RAID コントローラは入出力を休止します。



注意: ドライブに障害が発生し、再構築状態にある場合は、この手順を実行しないでください。この情報はシステムログで参照できます。

アレイのファームウェアをアップグレードするには、次の手順を実行します。再起動は不要です。

1. www.sunsolve.sun.com から最新のパッチをダウンロードし、ファイルを解凍します。
2. パッチの readme ファイルを参照して、パッチに関連付けられているファームウェアバージョンを確認します。

3. ファームウェアのアップグレードが必要な各拡張ユニット (JBOD) のトレイ ID を収集します。
 - a. Web Admin で、「RAID」 > 「View Controller/Enclosure Information」を選択します。
 - b. 「Controller Information」ボックスから、適切な RAID コントローラを選択します。
 - c. 「Enclosures Information」ボックスからトレイ ID を選択します。

「Firmware Release」フィールドに、<N/A>、または 9848 などのファームウェアバージョンが表示されます。このフィールドにファームウェアバージョン番号が表示される場合は、選択したトレイ ID が拡張ユニット (JBOD) に対応しています。これは、JBOD のファームウェアをアップグレードするために必要なトレイ ID です。
4. パッチをダウンロードしたディレクトリに移動します。
5. NAS クライアントから、FTP を使用可能にします。

GUI を使用して FTP を使用可能にする方法については、162 ページの「FTP アクセスの構成について」を参照してください。CLI を使用する場合は、263 ページの「ファイル転送プロトコル (FTP) アクセスの構成」を参照してください。
6. FTP を使用して NAS サーバーに接続し、admin 権限を持つユーザーアカウントでログインします。
7. bin と入力してバイナリモードへ移行します。
8. ftp プロンプトで次のコマンドを実行して、/cvol 上に各ディレクトリを作成します。

```
mkdir /cvol/firmware
mkdir /cvol/firmware/2882
mkdir /cvol/firmware/2882/ctrl
mkdir /cvol/firmware/2882/nvsram
mkdir /cvol/firmware/2882/jbod
```
9. ファームウェアを格納するために作成したディレクトリに移動し、put コマンドを使用してファームウェアファイル (表 11-5 を参照) をコピーします。

たとえば、RAID コントローラのファームウェアを読み込むには、次のコマンドを実行します。

```
cd /cvol/firmware/2882/ctrl
put SNAP_288X_06120910.dlp
```
10. 同じ手順を続けて、各ファームウェアファイルを適切なディレクトリに読み込みます。

次の表に、各コンポーネントのディレクトリおよびファームウェアファイルの例を示します。

表 11-5 コンポーネントのファームウェアディレクトリおよびファイル

コンポーネント	ディレクトリ	ファイル名の例
RAID コントローラ	/cvol/firmware/2882/ctlr	SNAP_288X_06120910.dlp
RAID コントローラ NVS RAM	/cvol/firmware/2882/nvsram	N2882-612843-503.dlp
FC EU	/cvol/firmware/2882/jbod	esm9631.s3r
SATA EU	/cvol/firmware/2882/jbod	esm9722.dl

- FTP セッションからログアウトします。
- Telnet を使用して NAS サーバーに接続し、admin 権限を持つユーザーアカウントでログインします。
- raidctl download コマンドを使用して、各ファイルを目的のディレクトリに読み込みます。

注: raidctl コマンドの使用法については、コマンド行に raidctl を引数なしで入力してください。

RAID コントローラのファームウェアを ctlr ディレクトリからコントローラ 0 および 1 に読み込むには、次のコマンドを実行します。

```
raidctl download type=lsi target=ctlr ctlr=0
```

この例では、ファームウェアファイルが両方の RAID コントローラへダウンロードされ、ディレクトリからそのファイルが削除されます。

注: raidctl download コマンドは、このコマンドが正常に呼び出されるたびに、そのあとでコンポーネント固有のファームウェアファイルが /cvol/firmware/2882 から削除されます。たとえば、raidctl download type=lsi target=ctlr ctlr=0 コマンドが正常に呼び出されるたびに、そのあとで /cvol/firmware/2882/ctlr ファイルが毎回削除されます。そのため、RAID コントローラまたは拡張ユニットが複数ある場合は、各コンポーネント (RAID コントローラ装置、コントローラ NVSRAM、拡張ユニット、およびドライブ) をアップグレードしたあと、ファームウェアファイルを再度コピーしてください。RAID コントローラ装置 2 台のクラスタ構成の場合、2 台めの装置は、コマンド raidctl download type=lsi target=ctlr ctlr=2 で ctlr=2 として指定します。

NVS RAM をダウンロードするには、次のコマンドを実行します。

```
raidctl download type=lsi target=nvsram ctlr=0
```

jbod ディレクトリにあるファームウェアをトレイ 1 の拡張格納装置 0 にダウンロードするには、次のコマンドを実行します。

```
raidctl download type=lsi target=jbod ctrlr=0 tray=1
```

14. Telnet セッションで、各ダウンロードの進行状況を監視します。

各アップグレードを完了するために必要なおおよその時間は、次のとおりです。

コンポーネント	コンポーネントあたりの時間 (分)
RAID コントローラ	15 分
RAID コントローラ NVSRAM	5 分
FC EU または SATA EU	5 分

注: アップグレードが完了したあと、telnet のカーソルに戻るまでに最大 5 分かかることがあります。カーソルが表示されるまで、待機してください。

15. 次のコンポーネントの作業に進む前に、システムログでダウンロードが完了していることを確認します。

システムログの出力例を次に示します。

```
Ctrl-  
  
Firmware Download 90% complete  
Firmware Download 95% complete  
Firmware Download 100% complete  
Waiting for controllers to become ACTIVE  
Controller 0 - now ACTIVE  
Controller 1 - now ACTIVE  
Controllers are now active  
nvram-
```

```

raidctl download type=lsi target=nvsram ctrl=0
Flashing C0 NVSRAM: /cvol/nf2/./firmware/2882/nvsram/n2882-
61.dlp (48068)
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
ESM-
>> raidctl download type=lsi target=jbod ctrl=0 tray=1

Flashing C0 JBOD 1 with
/cvol/nf1/./firmware/2882/jbod/esm9631.s3r (663604)
Firmware Download 20% complete
Firmware Download 30% complete
Firmware Download 50% complete
Firmware Download 60% complete
Firmware Download 90% complete
Firmware Download 100% complete
Waiting for controllers to become ACTIVE
Controller 0 - now ACTIVE
Controller 1 - now ACTIVE
Controllers are now active
Drive-
10/26/05 10:57:42 I Firmware Download 20% complete
10/26/05 10:57:46 I Firmware Download 30% complete
10/26/05 10:57:50 I Firmware Download 40% complete
10/26/05 10:57:54 I Firmware Download 50% complete
10/26/05 10:57:58 I Firmware Download 60% complete
10/26/05 10:58:03 I Firmware Download 70% complete
10/26/05 10:58:08 I Firmware Download 80% complete
10/26/05 10:58:13 I Firmware Download 90% complete
10/26/05 10:58:18 I Bytes Downloaded: 628224 (2454 256 chunks),
imageSize=62804
      8
10/26/05 10:59:01 I Flashed OK - drive in tray 2 slot 12
10/26/05 10:59:01 I Downloaded firmware version 0407 to 27 drives

```

16. 各コンポーネントにファームウェアがダウンロードされたあと、

ドライブファームウェアのアップグレード (再起動が必要)

ドライブファームウェアのみをアップグレードするには、この手順を実行してください。この手順では、NAS サーバーを再起動する必要があります。

注: ドライブファームウェアのアップグレードでは、常に NAS サーバーを再起動する必要があります。

注: すでに現在のファームウェアファイルと同じファームウェアバージョンになっているドライブも含めて、ドライブ種別ごとにすべてのドライブがアップグレードされます。

ファームウェアのアップグレードを完了するために必要な時間は、設置されているドライブの数と、NAS サーバーの再起動に必要な時間によって異なります。表 11-4 を参照して、使用する構成をアップグレードするために必要な時間を確認してください。

注意: ドライブに障害が発生し、再構築状態にある場合は、この手順を実行しないでください。この情報はシステムログで参照できます。

ドライブファームウェアをアップグレードする前に、NAS サーバーソフトウェア 4.10 Build 18 以降がインストールされていることを確認してください。それより前のバージョンの OS がインストールされている NAS サーバーでは、ファームウェアのアップグレードを行わないでください。

アレイのファームウェアをアップグレードするには、次の手順を実行します。再起動が必要です。

1. www.sunsolve.sun.com から最新のパッチをダウンロードし、ファイルを解凍します。
2. パッチの `readme` ファイルを参照して、パッチに関連付けられているファームウェアバージョンを確認します。
3. パッチのダウンロード先のディレクトリに移動します。

4. NAS クライアントから、FTP を使用可能にします。

GUI を使用して FTP を使用可能にする方法については、162 ページの「FTP アクセスの構成について」を参照してください。CLI を使用する場合は、263 ページの「ファイル転送プロトコル (FTP) アクセスの構成」を参照してください。

5. FTP を使用して NAS サーバーに接続し、`admin` ユーザーでログインします。

6. `bin` と入力してバイナリモードへ移行します。

7. `ftp` プロンプトで次のコマンドを発行して、`/cvol` 上に次のディレクトリを作成します。

```
mkdir /cvol/firmware/2882/drive
```



8. ドライブファームウェアを格納するために作成したディレクトリに移動し、put コマンドを使用してドライブファームウェアファイル (表 11-3 を参照) をコピーします。

たとえば、Seagate ST314680 ドライブのファームウェアを読み込むには、次のコマンドを実行します。

```
cd /cvol/firmware/2882/drive
put D_ST314680FSUN146G_0407.dlp
```

9. FTP セッションからログアウトします。
10. Telnet を使用して NAS サーバーに接続し、admin ユーザーでログインします。
11. システムを再起動します。クラスタ構成では、両方のサーバーを再起動します。
アップグレードを完了するために必要なおおよその時間は、再起動に要する時間にドライブあたり 1.5 分を加えた時間です。
12. 次のコマンドを実行して、新しいファームウェアが読み込まれていることを確認します。

```
raidctl get type=lsi target=profile ctrlr=0
```

システムログで障害を確認することもできます。

raidctl コマンドの出力の取得

raidctl profile コマンドを使用すると、RAID コントローラ装置、拡張ユニット、コントローラ NVSRAM、およびドライブの、それぞれの現在のファームウェアバージョンを確認できます。この節では、次の手順について説明します。

- 185 ページの「Solaris クライアントからの raidctl コマンドの出力の取得」
- 195 ページの「Windows クライアントからの raidctl の出力の取得」

Solaris クライアントからの raidctl コマンドの出力の取得

Solaris クライアントから raidctl コマンドの出力を取得するには、次の手順を実行します。

1. Solaris クライアントから、script コマンドとファイル名を入力します。次に例を示します。

```
> script raidctl
```

2. Telnet を使用して NAS サーバーに接続します。
3. 次の raidctl コマンドを入力して出力を収集します。

```
raidctl get type=lsi target=profile ctrlr=0
```

次の例に示すように、RAID コントローラ 2 台のクラスタ構成の場合、2 台めの装置は `ctrlr=2` として指定します。

```
raidctl get type=lsi target=profile ctrlr=2
```

4. `exit` と入力して Telnet セッションを終了します。
5. ふたたび `exit` と入力して、`raidctl` という名前のファイルを閉じます。
次にコマンドの出力例を示します。コマンドと、その結果として出力されたファームウェアバージョンは、太字で示します。

```
telnet 10.8.1xx.x2
Trying 10.8.1xx.x2...
Connected to 10.8.1xx.x2.
Escape character is '^]'.
connect to (? for list) ? [menu] admin
password for admin access ? *****
5310 > raidctl get type=lsi target=profile ctrlr=0

SUMMARY-----
Number of controllers: 2
Number of volume groups: 4
Total number of volumes (includes an access volume): 5 of 1024 used
    Number of standard volumes: 4
    Number of access volumes: 1
Number of drives: 28
Supported drive types: Fibre (28)
Total hot spare drives: 2
    Standby: 2
    In use: 0
Access volume: LUN 31
Default host type: Sun_SE5xxx (Host type index 0)
Current configuration
    Firmware version: PkgInfo 06.12.09.10
    NVSRAM version: N2882-612843-503
Pending configuration
```

```
CONTROLLERS -----
Number of controllers: 2

Controller in Tray 0, Slot B
  Status: Online
  Current Configuration
    Firmware version: 06.12.09.10
    Appware version: 06.12.09.10
    Bootware version: 06.12.09.10
    NVSRAM version: N2882-612843-503
  Pending Configuration
    Firmware version: None
    Appware version: None
    Bootware version: None
    NVSRAM version: None
    Transferred on: None
  Board ID: 2882
  Product ID: CSM100_R_FC
  Product revision: 0612
  Serial number: 1T44155753
  Date of manufacture: Sat Oct 16 00:00:00 2004
  Cache/processor size (MB): 896/128
  Date/Time: Thu Nov  2 19:15:49 2006
  Associated Volumes (* = Perferred Owner):
    lun4* (LUN 3)
Ethernet port: 1
  Mac address: 00.A0.B8.16.C7.A7
  Host name: gei
  Network configuration: Static
  IP address: 192.168.128.106
  Subnet mask: 255.255.255.0
  Gateway: 192.168.128.105
  Remote login: Enabled
Drive interface: Fibre
  Channel: 2
  Current ID: 124/0x7C
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:02:00:A0:B8:16:C7:A7
  World-wide node name: 20:00:00:A0:B8:16:C7:A7
  Part type: HPFC-5400      revision 6
```

```
Drive interface: Fibre
  Channel: 2
  Current ID: 124/0x7C
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:02:00:A0:B8:16:C7:A7
  World-wide node name: 20:00:00:A0:B8:16:C7:A7
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 2
  Current ID: 255/0x3
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
  World-wide port name: 20:07:00:A0:B8:16:C6:FB
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 2
  Current ID: 255/0x3
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
  World-wide port name: 20:07:00:A0:B8:16:C6:FB
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6

Controller in Tray 0, Slot A
  Status: Online
  Current Configuration
    Firmware version: 06.12.09.10
    Appware version: 06.12.09.10
    Bootware version: 06.12.09.10
    NVSRAM version: N2882-612843-503
  Pending Configuration
    Firmware version: None
    Appware version: None
    Bootware version: None
    NVSRAM version: None
    Transferred on: None
```

```
Board ID: 2882
Product ID: CSM100_R_FC
Product revision: 0612
Serial number: 1T44155741
Date of manufacture: Sun Oct 10 00:00:00 2004
Cache/processor size (MB): 896/128
Date/Time: Thu Nov  2 19:15:45 2006
Associated Volumes (* = Perferred Owner):
lun1* (LUN 0), lun2* (LUN 1), lun3* (LUN 2)
Ethernet port: 1
  Mac address: 00.A0.B8.16.C6.F9
  Host name: gei
  Network configuration: Static
  IP address: 192.168.128.105
  Subnet mask: 255.255.255.0
  Gateway: 192.168.128.105
  Remote login: Enabled
Drive interface: Fibre
  Channel: 1
  Current ID: 125/0x7D
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:01:00:A0:B8:16:C6:F9
  World-wide node name: 20:00:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Drive interface: Fibre
  Channel: 1
  Current ID: 125/0x7D
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Fixed
  Link status: Up
  Topology: Arbitrated Loop - Private
  World-wide port name: 20:01:00:A0:B8:16:C6:F9
  World-wide node name: 20:00:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 1
  Current ID: 255/0x0
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
```

```
Link status: Down
  Topology: Unknown
  World-wide port name: 20:06:00:A0:B8:16:C6:FA
  World-wide node name: 20:06:00:A0:B8:16:C6:F9
  Part type: HPFC-5400      revision 6
Host interface: Fibre
  Channel: 1
  Current ID: 255/0x0
  Maximum data rate: 200 MB/s
  Current data rate: 200 MB/s
  Data rate control: Auto
  Link status: Down
  Topology: Unknown
World-wide port name: 20:06:00:A0:B8:16:C6:FA
World-wide node name: 20:06:00:A0:B8:16:C6:F9
Part type: HPFC-5400      revision 6
```

VOLUME GROUPS-----

```
Number of volume groups: 4
Volume group 1 (RAID 5)
  Status: Online
  Tray loss protection: No
  Associated volumes and free capacities:
    lun1 (681 GB)
  Associated drives (in piece order):
    Drive at Tray 0, Slot 7
    Drive at Tray 0, Slot 6
    Drive at Tray 0, Slot 5
    Drive at Tray 0, Slot 4
    Drive at Tray 0, Slot 3
    Drive at Tray 0, Slot 8
Volume group 2 (RAID 5)
  Status: Online
  Tray loss protection: No
  Associated volumes and free capacities:
    lun2 (681 GB)
  Associated drives (in piece order):
    Drive at Tray 0, Slot 14
    Drive at Tray 0, Slot 13
    Drive at Tray 0, Slot 12
    Drive at Tray 0, Slot 11
    Drive at Tray 0, Slot 10
    Drive at Tray 0, Slot 9
```

```
Volume group 3 (RAID 5)
  Status: Online
  Tray loss protection: No
  Associated volumes and free capacities:
    lun3 (817 GB)
  Associated drives (in piece order):
    Drive at Tray 11, Slot 5
    Drive at Tray 11, Slot 4
    Drive at Tray 11, Slot 3
    Drive at Tray 11, Slot 2
    Drive at Tray 11, Slot 1
    Drive at Tray 11, Slot 7
    Drive at Tray 11, Slot 6
```

```
Volume group 4 (RAID 5)
  Status: Online
  Tray loss protection: No
  Associated volumes and free capacities:
    lun4 (817 GB)
  Associated drives (in piece order):
    Drive at Tray 11, Slot 13
    Drive at Tray 11, Slot 12
    Drive at Tray 11, Slot 11
    Drive at Tray 11, Slot 10
    Drive at Tray 11, Slot 9
    Drive at Tray 11, Slot 8
    Drive at Tray 11, Slot 14
```

STANDARD VOLUMES-----

SUMMARY

Number of standard volumes: 4

NAME	STATUS	CAPACITY	RAID LEVEL	VOLUME GROUP
lun1	Optimal	681 GB	5	1
lun2	Optimal	681 GB	5	2
lun3	Optimal	817 GB	5	3
lun4	Optimal	817 GB	5	4

DETAILS

Volume name: lun1

Volume ID: 60:0A:0B:80:00:16:C6:F9:00:00:23:B4:43:4B:53:3A

Subsystem ID (SSID): 0

Status: Optimal

Action: 1

Tray loss protection: No

Preferred owner: Controller in slot A

Current owner: Controller in slot B

Capacity: 681 GB

RAID level: 5

Segment size: 64 KB

Associated volume group: 1

Read cache: Enabled

Write cache: Enabled

Flush write cache after (in seconds): 8

Cache read ahead multiplier: 1

Enable background media scan: Enabled

Media scan with redundancy check: Disabled

DRIVES-----

SUMMARY

Number of drives: 28

Supported drive types: Fiber (28)

BASIC:

CURRENT	PRODUCT	FIRMWARE				
TRAY, SLOT	STATUS	CAPACITY	DATA RATE	ID	REV	
0,1	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,7	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,6	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,5	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,4	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,3	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,2	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,14	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,13	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,12	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,11	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,10	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,9	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	
0,8	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307	

11,5	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,4	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,3	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,2	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,1	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,13	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,12	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,11	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,10	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,9	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,8	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,7	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,6	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307
11,14	Optimal	136 GB	2 Gbps	ST314680FSUN146G	0307

HOT SPARE COVERAGE:

The following volume groups are not protected:

Total hot spare drives: 2

Standby: 2

In use: 0

DETAILS:

Drive at Tray 0, Slot 1 (HotSpare)

Available: 0

Drive path redundancy: OK

Status: Optimal

Raw capacity: 136 GB

Usable capacity: 136 GB

Product ID: ST314680FSUN146G

Firmware version: 0307

Serial number: 3HY90HWJ00007510RKKV

Vendor: SEAGATE

Date of manufacture: Sat Sep 18 00:00:00 2004

World-wide name: 20:00:00:11:C6:0D:BA:3E

Drive type: Fiber

Speed: 10033 RPM

Associated volume group: None

Available: No

Vendor: SEAGATE
Date of manufacture: Sat Sep 18 00:00:00 2004
World-wide name: 20:00:00:11:C6:0D:CA:12
Drive type: Fiber
Speed: 10033 RPM
Associated volume group: 3
Available: No

Drive at Tray 11, Slot 1
Drive path redundancy: OK
Status: Optimal
Raw capacity: 136 GB
Usable capacity: 136 GB
Product ID: ST314680FSUN146G
Firmware version: 0307
Serial number: 3HY90JEW00007511BDPL
Vendor: SEAGATE
Date of manufacture: Sat Sep 18 00:00:00 2004
World-wide name: 20:00:00:11:C6:0D:C8:8B
Drive type: Fiber
Speed: 10033 RPM
Associated volume group: 3
Available: No

Drive Tray 1 Overall Component Information
Tray technology: Fibre Channel
Minihub datarate mismatch: 0
Part number: PN 54062390150
Serial number: SN 0447AWF011
Vendor: VN SUN
Date of manufacture: Mon Nov 1 00:00:00 2004
Tray path redundancy: OK
Tray ID: 11

Tray ID Conflict: 0
Tray ID Mismatch: 0
Tray ESM Version Mismatch: 0
Fan canister: Optimal
Fan canister: Optimal
Power supply canister
Status: Optimal
Part number: PN 30017080150
Serial number: SN A6847502330F
Vendor: VN SUN
Date of manufacture: Sun Aug 1 00:00:00 2004

```
Power supply canister
  Status: Optimal
  Part number: PN 30017080150
  Serial number: SN A6847502330F
  Vendor: VN SUN
  Date of manufacture: Sun Aug 1 00:00:00 2004
Power supply canister
  Status: Optimal
  Part number: PN 30017080150
  Serial number: SN A68475023N0F
  Vendor: VN SUN
  Date of manufacture: Sun Aug 1 00:00:00 2004
Temperature: Optimal
Temperature: Optimal
Esm card
  Status: Optimal
  Firmware version: 9631
  Maximum data rate: 2 Gbps
  Current data rate: 2 Gbps
  Location: A (left canister)
  Working channel: -1
  Product ID: CSM100_E_FC_S
  Part number: PN 37532180150
  Serial number: SN 1T44462572
  Vendor: SUN
  FRU type: FT SBOD_CEM
  Date of manufacture: Fri Oct 1 00:00:00 2004
Esm card
  Status: Optimal
  Firmware version: 9631
  Maximum data rate: 2 Gbps
  Current data rate: 2 Gbps
  Location: B (right canister)
  Working channel: -1
```

Windows クライアントからの raidctl の出力の取得

Windows クライアントから raidctl の出力を取得するには、次の手順を実行します。

1. 「スタート」>「ファイル名を指定して実行」をクリックして、cmd と入力します。「OK」をクリックします。

2. ウィンドウの上部を右クリックして、「プロパティ」を選択します。
「Properties」ウィンドウが表示されます。
3. 「画面バッファのサイズ」の「高さ」を 3000 に変更します。
4. 「オプション」タブをクリックして、「挿入モード」の選択を解除します。
5. Telnet を使用して NAS サーバーに接続し、次の `raidctl` コマンドを入力して出力を収集します。
raidctl get type=lsi target=profile ctrl=0
6. 任意のテキストエディタを使用して、ファイルにテキストをコピーします。次に例を示します。
 - a. 出力されたテキストを選択し、**Ctrl-C** を押してデータをコピーします。
 - b. 「スタート」>「プログラム」>「アクセサリ」>「ワードパッド」をクリックして、ワードパッドを開きます。
 - c. ウィンドウの内部をクリックし、**Ctrl-V** を押してテキストを貼り付けます。
 - d. ファイルを保存します。
7. 保存したファイルを開いて、各コンポーネントの現在のファームウェアバージョンを検索します。

第12章

サーバーコンポーネントの交換

この章では、顧客交換可能ユニット (CRU) の取り外しおよび交換の手順について説明します。この章は、次の節で構成されています。

- 197 ページの「必要な工具類および供給品」
- 197 ページの「電源切断とカバーの取り外し」
- 202 ページの「顧客交換可能ユニットの位置」
- 202 ページの「コンポーネントの交換」

必要な工具類および供給品

Sun StorageTek 5320 NAS サーバーは次のものを使用して保守できます。

- プラスのねじ回し (Phillips の 2 番)
- 静電気防止用リストストラップ
- ボールペンまたはその他の針状の器具 (埋め込み式の電源ボタンを押すため)
- 8 mm のナットドライバ (マザーボード交換用)

電源切断とカバーの取り外し

取り外しおよび交換の手順で準備手順を参照するように指示があった場合は、この節を参照してください。

サーバーの電源切断

1. サーバーを停止して主電源モードからスタンバイ電源モードに切り替える方法を選択します。詳細は、図 12-1 を参照してください。
 - Local shutdown – LCD の電源ボタンを使用して、オペレーティングシステムの制御下でサーバーを正常に停止します。
 - Remote shutdown – Web Admin インタフェースで「System Operations」 > 「Shut Down the Server」を選択して、サーバーを正常に停止します。



注意: システムを停止するときに、電源ボタンを使用しないでください。常に、LCD の電源ボタンを使用するか、164 ページの「サーバーの停止」で説明している遠隔停止手順を実行してください。不適切な停止手順を実行すると、データが失われる可能性があります。

主電源が切断されると、フロントパネルの電源/OK LED が点滅し始めます。これはサーバーがスタンバイ電源モードであることを示します。



注意: LCD の電源ボタンを使用してスタンバイ電源モードに切り替えた場合、サービスプロセッサおよび電源装置ファンにはまだ電力が送られています。サーバーの電源を完全に切断するには、サーバーの背面パネルから AC 電源コードを抜いてください。

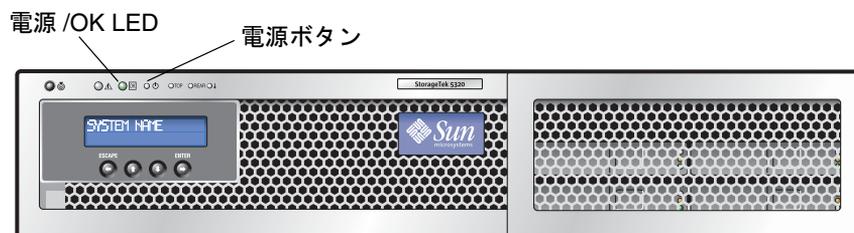


図 12-1 電源ボタンと電源/OK LED の位置

2. 両方の電源コードをサーバーの電源装置から取り外します。
3. システムに接続されている周辺デバイスをすべて停止します。
4. 特定のコンポーネントを取り外して交換するために抜く必要のある周辺装置のケーブルまたは電気通信用ケーブル、あるいはその両方にラベルを付けます。



注意: コンポーネントを取り扱う前に、シャーシの背面に組み込まれているアース端子に静電放電 (ESD) リストストラップを取り付けます。システムのプリント回路基板およびハードディスクドライブには、静電気に非常に弱いコンポーネントが含まれています。

メインカバーの取り外し

1. カバーのリリースボタンを押し下げ、くぼみに手をかけて、メインカバーをシャーシの背面方向に約 12 mm (0.5 インチ) スライドさせます。詳細は、図 12-2 を参照してください。
2. カバーの背面側の端をしっかりと持ち、シャーシから真上に持ち上げます。

注: いずれかのカバーを取り外すと、正面側の I/O ボード上にある侵入スイッチによって、システムの電源が自動的にスタンバイモードに切り替わります。

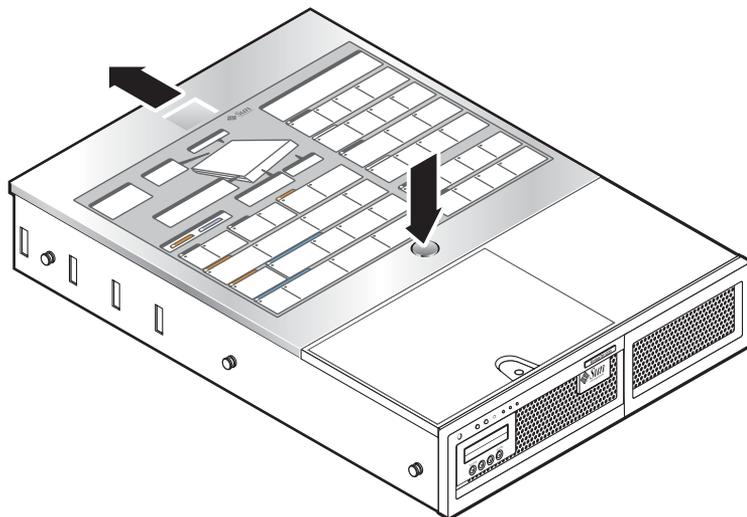


図 12-2 メインカバーの取り外し

正面ベゼルの取り外し

次の手順に従って、シャーシの正面からベゼルを取り外します。

1. ファンベイのドアを開き、プラスのねじ回し (Phillips の 2 番) を使用して、ベゼルを所定の位置に固定している脱落防止機構付きねじを緩めます。詳細は、図 12-3 を参照してください。
2. ベゼルの外側の両端をしっかりと持ち、ベゼルのゆっくりとシャーシから 2.4 cm (1 インチ) 離します。

注意: ベゼルの内側にある LCD に、3 インチの USB ケーブルが接続されています。ベゼルのシャーシから無理に外さないように注意してください。



3. シャーシの USB コネクタからケーブルを取り外します。

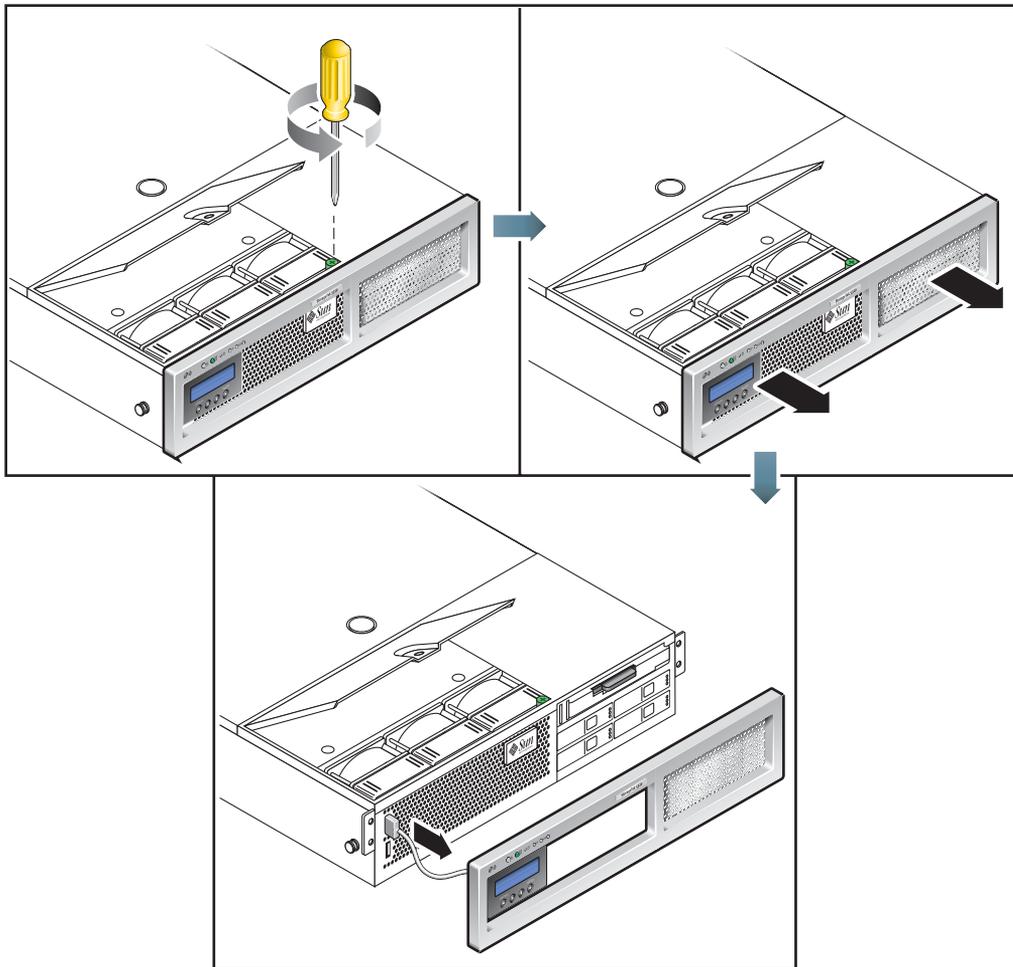


図 12-3 正面ベゼルの取り外し



注意 – 正面ベゼルを取り外すと、フラッシュディスクに手が届くようになります。サーバーの電源が入っている間は、フラッシュディスクを取り外さないでください。フラッシュディスクは顧客交換可能ユニットではないため、Sun の保守担当者が交換します。

正面側カバーの取り外し

1. ファンベイのドアを開きます。詳細は、図 12-4 を参照してください。
2. ファンベイのドアを開いたまま、正面側カバーをシャーシの正面方向に約 6 mm (0.25 インチ) スライドさせます。
3. カバーの背面側の端を持ち上げて、シャーシから引き上げます。

注: 正面側カバーを元に戻す場合は、最初に正面側の端をシャーシに置き、シャーシ側面のはめ込み式のスロットに入れてから、背面側にスライドさせてください。

注: いずれかのカバーを取り外すと、正面の I/O ボード上にある侵入スイッチによって、システムの電源が自動的にスタンバイ電源モードに切り替わります。

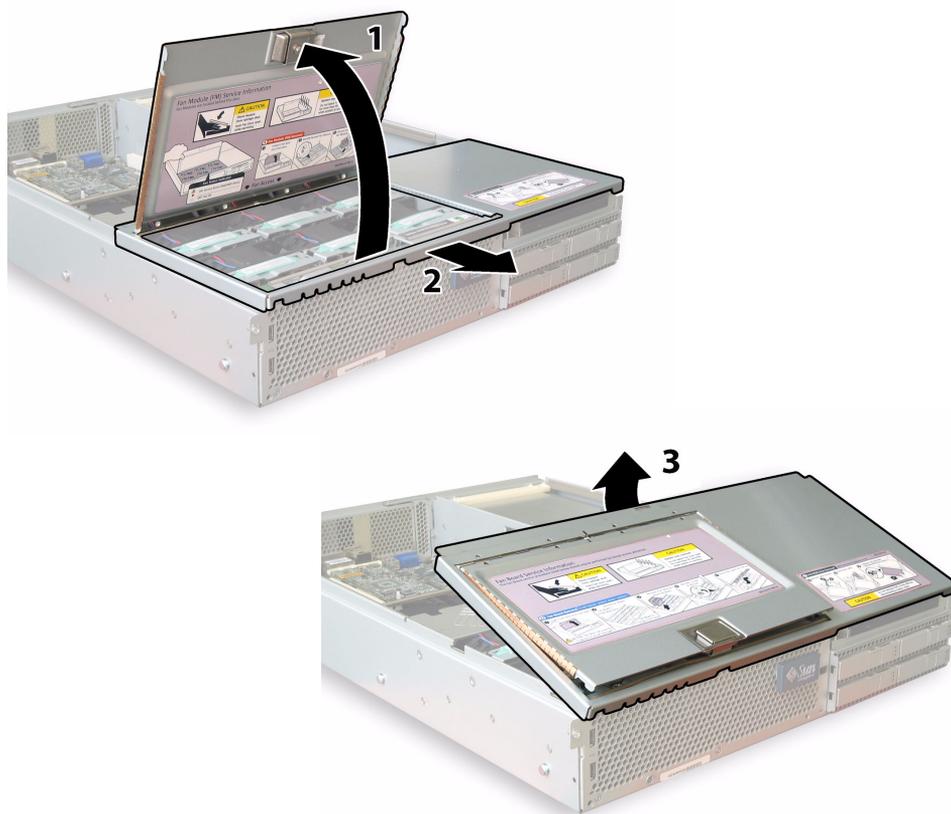


図 12-4 正面側カバーの取り外し

顧客交換可能ユニットの位置

図 12-5 に、この節で説明する顧客交換可能ユニット (CRU) の位置を示します。

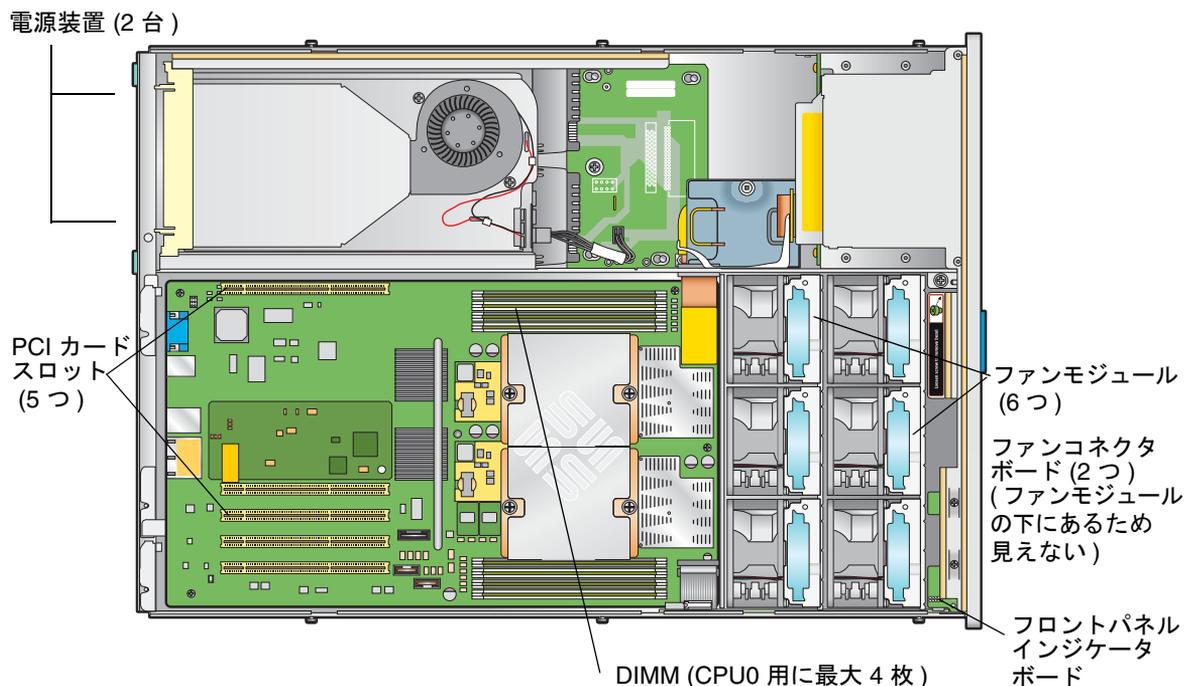


図 12-5 交換可能コンポーネントの位置

コンポーネントの交換

この節では、CRU の取り外しおよび交換の手順について説明します。現場交換可能ユニット (FRU) の交換は、トレーニングを受けた保守技術者だけが行います。FRU の交換については、ご購入先に問い合わせてください。

この節では、次の CRU の交換手順について説明します。

- 203 ページの「ファンコネクタボードの交換」
- 205 ページの「フロントパネルインジケータボードの交換」
- 207 ページの「電源装置の交換」
- 208 ページの「メモリーモジュールの交換」
- 211 ページの「ファンモジュールアセンブリの交換」

- 213 ページの「背面側ファントレーの交換」
- 214 ページの「PCI カードの交換」

ファンコネクタボードの交換

ファンコネクタボードを取り外して交換するには、次の手順を実行します。パーツ番号 501-6917 のファンコネクタボードが、サポートされています。

注: サポートされるパーツの番号は変更される場合があります。

1. 198 ページの「サーバーの電源切断」の説明に従ってサーバーの電源を切ります。
2. サーバーがラックに設置されている場合は、ファンベイのドアが開くように、サーバーをラックから十分に引き出します。
この方法ではコンポーネントを安全に見ることができず、取り扱いできない場合は、サーバーをラックから完全に取り外してください。
3. ファンベイのドアを開き、そのまま保持します。図 12-6 を参照してください。

注意: ファンベイのドアを開くときは、片手で慎重に開いて保持し、ドアが勢いよく閉じて指を痛めることがないようにしてください。サーバーの動作中は、サーバーの過熱を防止するために、ファンベイのドアを 60 秒以上開いたままにしないでください。

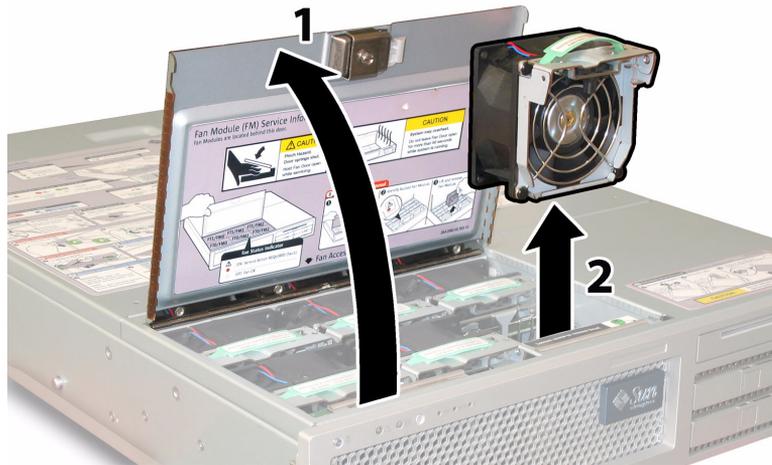


図 12-6 ファンベイのドアを開き、ファンモジュールを交換する方法

4. 交換するファンコネクタボードに接続されている 3 つのファンモジュールを取り外します。

ファンモジュールのプラスチック製のストラップをしっかりと持ち、各ファンモジュールをファンベイから真上に持ち上げます。

5. ファンコネクタボードをシャーシに固定している 1 本のねじを取り外します。詳細は、図 12-7 を参照してください。

注: 次の 2 つの図では、見やすくするために、正面側カバーとすべてのファンが取り外されたサーバーを背面から見た状態を示しています。この手順ではカバーを取り外さないでください。

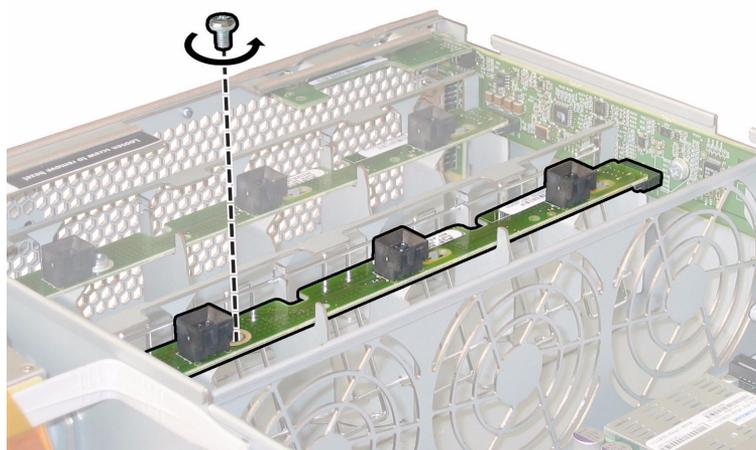


図 12-7 ファンコネクタボードを固定しているねじの取り外し

6. ファンコネクタボードをシャーシの中央方向にスライドさせて、正面側の I/O ボードから取り外し、シャーシの 2 つの位置決め爪から外します。詳細は、図 12-8 を参照してください。

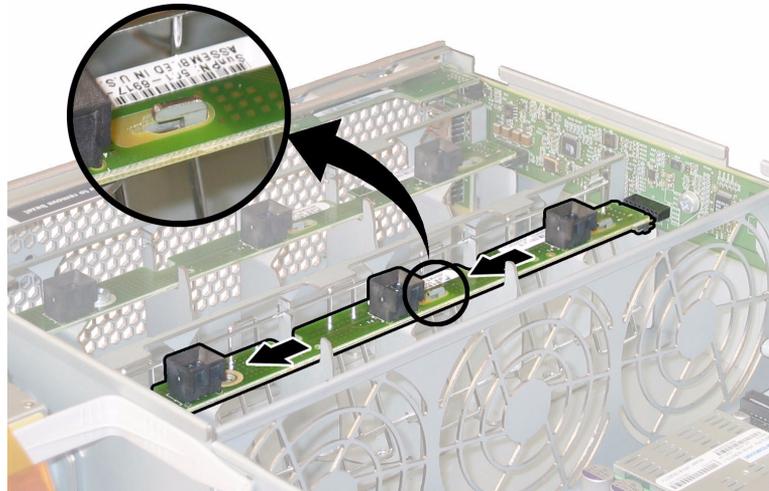


図 12-8 ファンコネクタボードの取り外し

7. ボードを真上に持ち上げて、システムから取り外します。
取り付けはこの逆の手順で行います。

フロントパネルインジケータボードの交換

フロントパネルインジケータボードを取り外して交換するには、次の手順を実行してください。パーツ番号 501-6916 のフロントパネルインジケータボードが、サポートされています。

注: サポートされるパーツの番号は変更される場合があります。

1. 198 ページの「サーバーの電源切断」の説明に従ってサーバーの電源を切ります。
2. サーバーがラックに設置されている場合は、メインカバーと正面側カバーを取り外せるように、サーバーをラックから十分に引き出します。
この方法ではコンポーネントを安全に見ることができず、取り扱いできない場合は、サーバーをラックから完全に取り外してください。
3. 199 ページの「メインカバーの取り外し」の説明に従ってメインカバーを取り外します。
4. 199 ページの「正面ベゼルの取り外し」の説明に従って正面ベゼルを取り外します。

注: ベゼルを取り外す前に、必ずベゼルの固定ねじを緩めてください。

- 201 ページの「正面側カバーの取り外し」の説明に従って正面側カバーを取り外します。
- フロントパネルインジケータボードをシャーシに固定している 2 本のねじを取り外します。

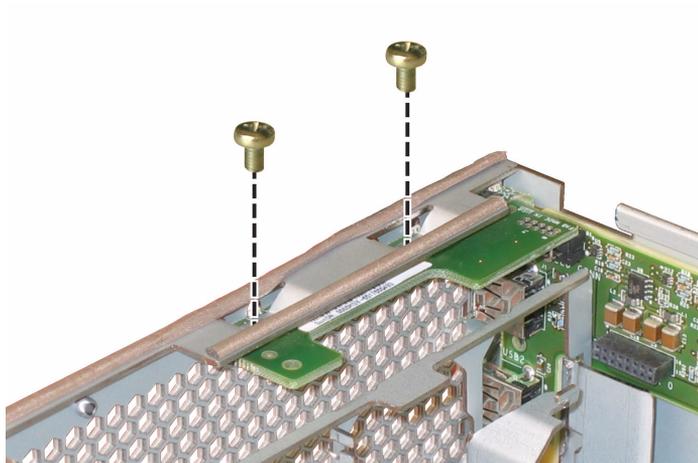


図 12-9 フロントパネルインジケータボードのねじの取り外し

- 右手でインジケータボードを支えながら、左手でインジケータボードをシャーシの中央方向にそっと押して、正面側の I/O ボードから抜き取ります。詳細は、図 12-10 を参照してください。



図 12-10 フロントパネルインジケータボードの取り外し

- フロントパネルインジケータボードをシャーシから取り外します。取り付けはこの逆の手順で行います。

電源装置の交換

電源装置を取り外して交換するには、次の手順を実行します。パーツ番号 300-1757 の電源装置がサポートされています。

注: サポートされるパーツの番号は変更される場合があります。

サーバー内の 2 台の電源装置は、内部システムソフトウェアでは図 12-11 に示すように指定されます。

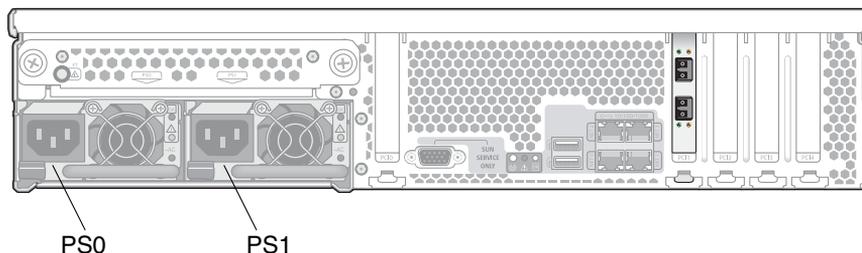


図 12-11 電源装置の指定

1. 交換する電源装置を特定します。

各電源装置には 3 つの LED があり、サーバーの背面から確認することができます。

- 上の LED: 緑色は、電源装置が正常に動作していることを示します。
- 中央の LED: オレンジ色は、電源装置に障害が発生しており、交換が推奨されていることを示します。
- 下の LED: 緑色は、電源装置に接続されている AC 電源が正常に動作していることを示します。

2. 交換する電源装置から AC 電源コードを抜き取ります。

電源装置はホットスワップ対応であるため、サーバーの停止または 2 台めの電源装置の取り外しは必要ありません。

注: 電源装置を取り外すと、フロントパネルと背面パネルの保守要求 LED が点滅します。LED の詳細は、295 ページの「状態インジケータ LED」を参照してください。

3. 電源装置を取り外します。

- a. 電源装置のハンドルをしっかりと持ち、サムラッチを電源装置の中央方向に押しします。詳細は、図 12-12 を参照してください。

- b. ラッチを押したまま、ハンドルを使用して電源装置をシャーシから取り外します。



図 12-12 電源装置の取り外し

取り付けはこの逆の手順で行います。

新しい電源装置を取り付けるときは、電源装置をベイに押し込みます。サムラッチがカチッと音を立てると電源装置が固定されたことを示します。

メモリーモジュールの交換

DIMM (Dual Inline Memory Module) を取り外して交換するには、次の手順を実行します。パーツ番号 540-6453 の DIMM がサポートされています。

注: サポートされるパーツの番号は変更される場合があります。

いずれかの DIMM の取り外しまたは取り付けを行う前に、次のメモリー構成ガイドラインのリストを確認してください。

- CPU は最大 4 枚の DIMM をサポートできます。
- DIMM スロットはペアになっており、DIMM は 2 枚 1 組で取り付けます (0 と 1、2 と 3)。詳細は、図 12-13 を参照してください。メモリーソケットは、どのスロットがペアになっているかを示すため、白と黒に色分けされています。
- DIMM のペアが 1 つのみの CPU では、それらの DIMM を CPU の白の DIMM スロット (0 および 1) に取り付けます。
- PC3200 ECC および PC2700 ECC の登録済み DIMM のみがサポートされます。
- DIMM の各ペアには、同一の DIMM (同じメーカー、容量、および速度) を使用します。

1. 198 ページの「サーバーの電源切断」の説明に従ってサーバーの電源を切ります。
2. サーバーがラックに設置されている場合は、メインカバーを取り外せるように、サーバーをラックから十分に引き出します。
この方法ではコンポーネントを安全に見ることができず、取り扱いできない場合は、サーバーをラックから完全に取り外してください。
3. 199 ページの「メインカバーの取り外し」の説明に従ってメインカバーを取り外します。
4. DIMM の取り付けまたは交換を行うマザーボード上の DIMM スロットを特定します。

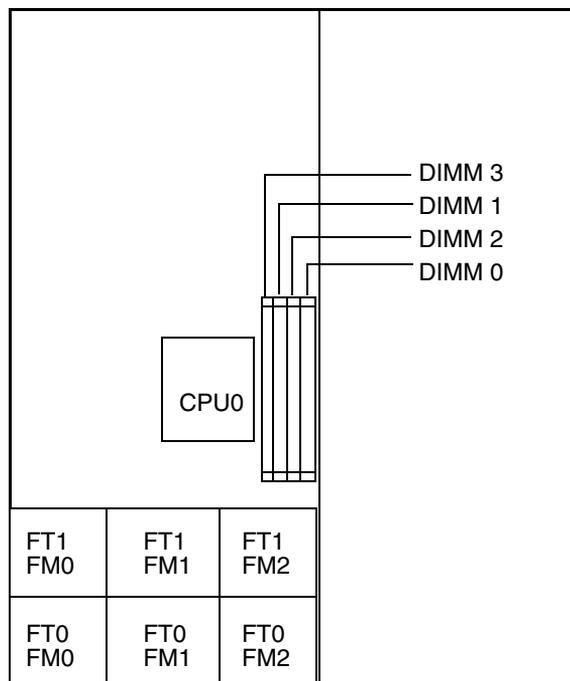
注: DIMM スロットの取り外しレバーの障害 LED を調べるには、サーバーに AC 電源コードを接続して、サーバーをスタンバイ電源モードに切り替えてください。詳細は、198 ページの「サーバーの電源切断」を参照してください。

DIMM の取り外し LED が、DIMM に障害が発生したことを示すことがあります。

- オフ: DIMM が正常に動作しています。
- オン (オレンジ色): DIMM に障害が発生しており、交換が推奨されています。

DIMM スロットは、内部システムソフトウェアでは図 12-13 に示すように指定されません。

サーバーの背面パネル



サーバーのフロントパネル

図 12-13 DIMM スロットの指定

5. DIMM を取り外すには、次の手順を実行します。

- a. 両方の DIMM スロットの取り外しレバーを、外側に完全に倒します。DIMM が部分的にソケットから外れます。詳細は、図 12-14 を参照してください。
- b. DIMM を慎重に真上に持ち上げてソケットから取り外します。

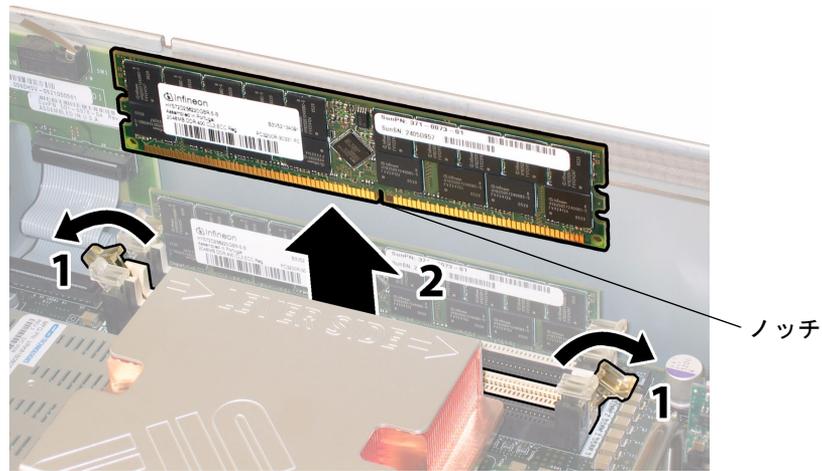


図 12-14 DIMM の取り外し

6. DIMM を取り付けるには、次の手順を実行します。

- a. メモリーソケットの両端にある DIMM スロットの取り外しレバーが完全に開いて (外側に倒れて) いて、新しい DIMM を取り付けられる状態であることを確認します。
- b. DIMM の下端にあるノッチを DIMM ソケットの切り欠けに合わせます。詳細は、図 12-14 を参照してください。
- c. 取り外しレバーが DIMM の左端と右端の切り込みにはまるまで、DIMM 上端の両方の角を均等に押し下げます。

ファンモジュールアセンブリの交換

個別のファンモジュールを取り外して交換するには、次の手順を実行します。パーツ番号 541-0269 のファンモジュールが、サポートされています。

注: サポートされるパーツの番号は変更される場合があります。



注意: ファンはホットスワップ対応であるため、システムの動作中に取り外して交換できます。サーバーの過熱を防止するために、ファンベイのドアを 60 秒以上開いたままにしないでください。取り外して交換するファンは、一度に 1 つのみにしてください。

コネクタボード、つまりファントレー (FT) と、ファンモジュール (FM) は、内部システムソフトウェアでは図 12-15 に示すように指定されています。

FT1 FM0	FT1 FM1	FT1 FM2
FT0 FM0	FT0 FM1	FT0 FM2

サーバーの正面

図 12-15 ファンコネクタボードおよびファンモジュールの指定

1. サーバーがラックに設置されている場合は、ファンベイのドアが開くように、サーバーをラックから十分に引き出します。
この方法ではコンポーネントを安全に見ることができず、取り扱いできない場合は、サーバーをラックから完全に取り外してください。
2. ファンベイのドアを開き、LED を調べて、障害の発生したファンモジュールを特定します。
 - オン: ファンモジュールに障害が発生しており、交換が推奨されています。
 - オフ: ファンモジュールが正常に動作しています。



注意: ファンベイのドアを開くときは、片手で慎重に開いて保持し、ドアが勢いよく閉じて指を痛めることがないようにしてください。サーバーの動作中は、サーバーの過熱を防止するために、ファンベイのドアを 60 秒以上開いたままにしないでください。

3. ファンベイのドアを開いたまま、障害の発生したファンモジュールのプラスチック製のストラップをしっかりと持ち、ファンベイから真上に持ち上げます。詳細は、図 12-16 を参照してください。

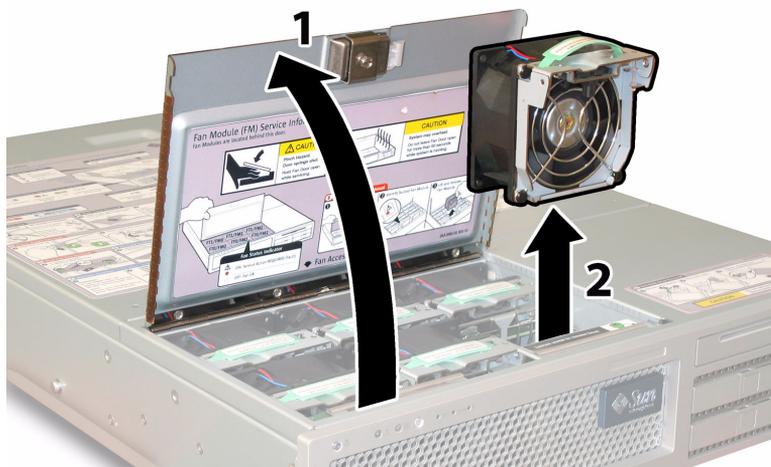


図 12-16 ファンベイのドアを開き、ファンモジュールを交換する方法

取り付けはこの逆の手順で行います。

背面側ファントレーの交換

背面側ファントレー (送風機トレイ) を取り外して交換するには、次の手順を実行します。パーツ番号 541-0645 の送風機トレイが、サポートされています。

注: サポートされるパーツの番号は変更される場合があります。

1. サーバーの背面側から作業をして、背面側ファントレーの表面の 2 本の脱落防止機構付きねじを緩めます。詳細は、図 12-17 を参照してください。

背面側ファントレーは、内部システムソフトウェアでは I/O FAN と指定されます。背面側ファントレーの表面には 1 つの障害 LED があり、次の状態を示します。

- オフ: ファントレーが正常に動作しています。
- オン (オレンジ色): ファントレーに障害が発生しており、交換が推奨されています。

2. 背面側ファントレーをシャーシから取り外します。

ファントレーのケーブルコネクタがシャーシの内部コネクタから外れます。

注: 図 12-17 は、コンポーネントが見えるようにサーバーのカバーを取り外した状態を示しています。この手順ではサーバーを取り外さないでください。

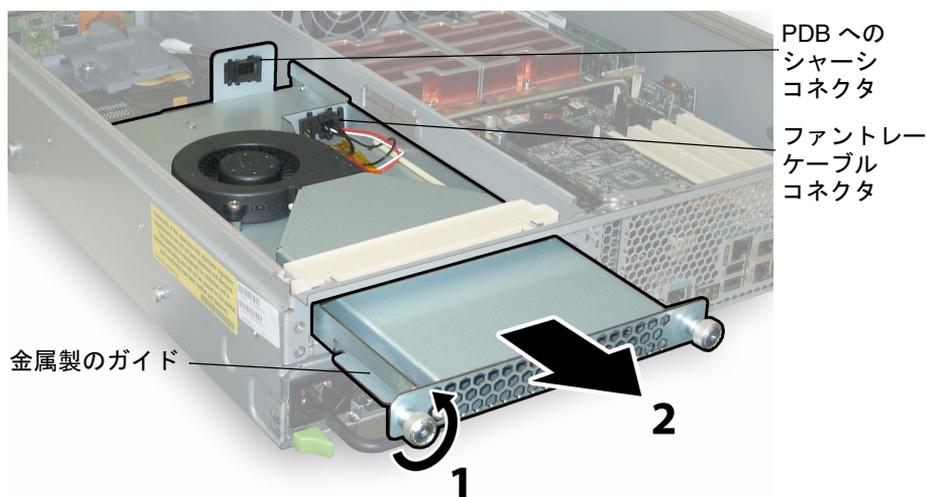


図 12-17 背面側ファントレイの取り外し

取り付けはこの逆の手順で行います。

注: 新しい背面側ファントレイを再度取り付ける際には、必ずファントレイ側面の金属製のガイド (図 12-17 を参照) をシャーシベイの内側のプラスチックレールに均等にはめ込んでください。

PCI カードの交換

PCI カードを取り外して交換するには、次の手順を実行します。

表 12-1 に、このコンポーネントでサポートされるパーツの番号を示します。

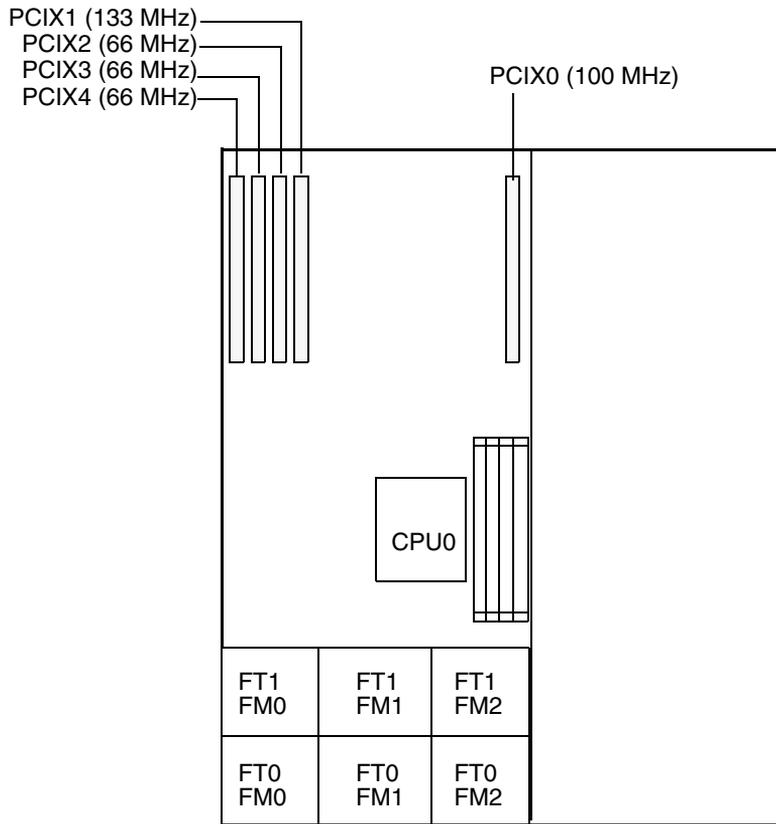
注: サポートされるパーツの番号は変更される場合があります。

表 12-1 サポートされる PCI カードのパーツ番号

コンポーネント	Part No.
デュアルポートファイバチャネル	375-3421
シングルポート U320 SCSI HBA	375-3366
NIC デュアルポート (ファイバ)	375-3250
NIC デュアルポート (銅)	370-6687

1. 198 ページの「サーバーの電源切断」の説明に従ってサーバーの電源を切ります。
2. サーバーがラックに設置されている場合は、メインカバーを取り外せるように、サーバーをラックから十分に引き出します。
この方法ではコンポーネントを安全に見ることができず、取り扱いできない場合は、サーバーをラックから完全に取り外してください。
3. 199 ページの「メインカバーの取り外し」の説明に従ってメインカバーを取り外します。
4. PCI カードの取り付けまたは交換を行う PCI カードスロットを特定します。
図 12-18 に、内部システムソフトウェアでの 5 つの PCI スロットの指定および速度を示します。
PCI-X カード用のスロットは、起動時にシステム BIOS によって 0、2、3、4、1 の順序で検出されます。

注: カードを取り付ける前に、使用する特定の PCI カードのシステム要件および構成情報をメーカーのマニュアルで参照してください。



サーバーのフロントパネル

図 12-18 PCI スロットの指定および速度

5. 既存の PCI カードをスロットから取り外します。
 - a. PCI カードに接続されている外部ケーブルを取り外します。
 - b. シャーシの背面側から作業して、PCI カードの背面コネクタパネルを固定している PCI カードラッチを回転させて開きます。詳細は、図 12-19 を参照してください。

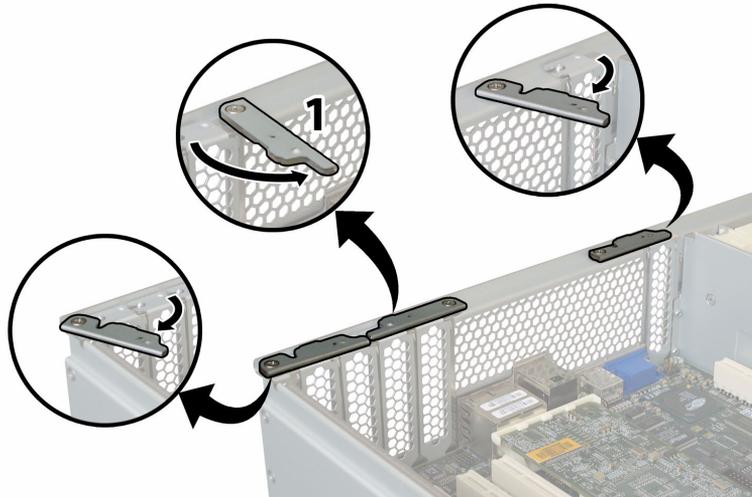


図 12-19 PCI カードの固定ラッチを開く方法

- c. PCI カードを PCI スロットから引き出します。PCI カードの背面コネクタパネルがシャーシの背面パネルの爪から外れます。
- 6. スロットに PCI カードがない場合は、シャーシの背面パネルから PCI カードのフィラーパネルを取り外します。詳細は、図 12-20 を参照してください。

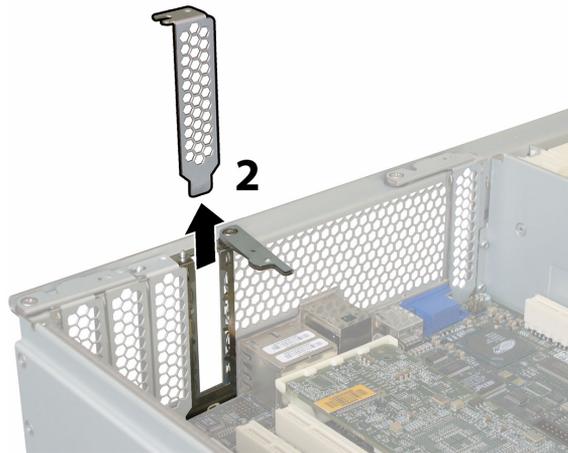


図 12-20 PCI カードのフィラーパネルの取り外し

- 7. PCI カードを取り付けるには、次の手順を実行します。

- a. シャーシの背面側から作業をして、スロットの PCI カードラッチを回転させて開き、新しい PCI カードを取り付けられるようにします。詳細は、図 12-19 を参照してください。
- b. PCI カードを PCI カードスロットに差し込みます。PCI カードの背面コネクタパネルがシャーシの背面パネルの爪にはまっていることを確認してください。詳細は、図 12-21 を参照してください。

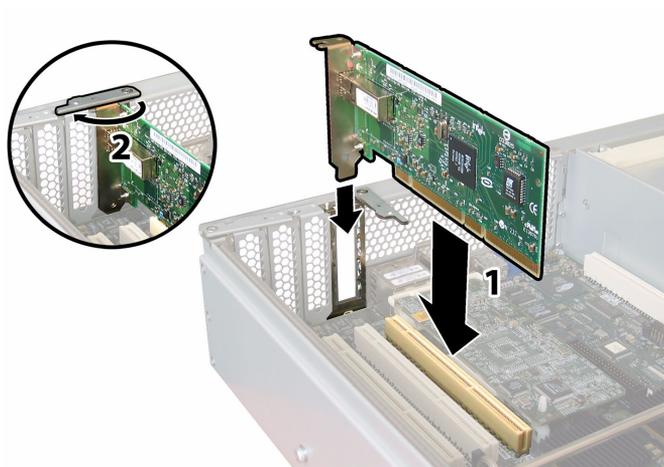


図 12-21 PCI カードの取り付け

- c. PCI カードの背面コネクタパネルが固定されるまで、PCI カードラッチを回転させて閉じます。詳細は、図 12-21 を参照してください。

コンソール管理

Web Administrator アプリケーションの代わりにコンソールを使用して、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、および Sun StorageTek 5320 NAS Gateway システムを管理できます。使用しているアプリケーションに ANSI 互換の端末エミュレータがあれば、Telnet、SSH、RLogin などのさまざまなプロトコルを使用して管理者コンソールに接続できます。この付録では、Windows ですぐに使用可能な Telnet プロトコルを使用します。

注: コマンド行インタフェースにアクセスするために、遠隔アクセスセキュリティーの設定変更が必要な場合があります。遠隔アクセスの詳細は、161 ページの「遠隔アクセスオプションの設定」を参照してください。

この付録は、次の節で構成されています。

- 220 ページの「管理者コンソールへのアクセス」
- 221 ページの「コンソールメニューの概要」
- 221 ページの「メインメニューの表示」
- 222 ページの「構成情報のバックアップ」
- 222 ページの「システムの管理」
- 228 ページの「ルートの管理」
- 228 ページの「ネームサービス」
- 233 ページの「サーバーファイルシステムの管理」
- 236 ページの「共有および割り当て」
- 241 ページの「セキュリティー」
- 250 ページの「ファイルボリュームのミラー化」
- 257 ページの「監視」
- 262 ページの「システムの保守」

管理者コンソールへのアクセス

この例では、Windows Telnet プロトコルを使用して管理者コンソールのコマンド行インタフェースにアクセスします。ただし、ANSI 互換の端末エミュレータがあれば、別のプロトコルを使用することもできます。

Windows Telnet プロトコルへのアクセス

Windows Telnet にアクセスするには、次の手順を実行します。

1. デスクトップのタスクバーから「スタート」をクリックします。
2. 「ファイル名を指定して実行」を選択します。
3. 「ファイル名を指定して実行」ウィンドウで `cmd` と入力して、「OK」をクリックします。
4. コマンドプロンプトで `telnet ipaddress` と入力して、Enter キーを押します。
`ipaddress` はサーバーの IP アドレスです。
5. 管理アクセスがパスワードで保護されている場合は、パスワードを入力します。
接続すると、Telnet の画面に次のコマンド行プロンプトが表示されます。

```
connect to (? for list) ? [menu]
```

この時点で、直接メインメニューに移動するか、コマンド行インタフェース (CLI) にアクセスして特定のコマンドを実行することができます。

メインメニューにアクセスするには、Enter キーを押します。

管理者コンソールのコマンド行インタフェースへのアクセス

Windows Telnet プロトコルを使用して管理者コンソールのコマンド行インタフェースにアクセスするには、次の手順を実行します。

1. 接続プロンプトで `admin` と入力して、Enter キーを押します。
2. 管理パスワードを入力して、Enter キーを押します。
コマンド行プロンプトが表示されます。コマンドを入力するか、`menu` を選択してコンソールのメインメニューにアクセスできます。

注意: 予期しない結果を回避するため、コマンドは注意して使用してください。



コマンド行に戻るには、メインメニューで Esc キーを押します。

コンソールメニューの概要

コンソールの使用に関するいくつかの基本的なガイドラインを次に示します。

- メニューを選択するには、項目に関連付けられた数字または文字を押します。たとえば、「1. Activity Monitor」を選択する場合は、1 キーを押します。
- 各画面の下部のボックスには、実行可能な作業、および処理を実行するために選択する必要がある文字が表示されます。
- リストをスクロールして表示するには、スペースバーを使用します。

画面のフィールドの編集に使用するキーを、次の表に示します

表 A-1 画面で使用できるキー

キー	動作
Backspace、Delete、Ctrl+H	前の文字を削除します。
Ctrl+U	フィールド全体を削除します。
Enter、Ctrl+M、Ctrl+J、Ctrl+I、Tab	現在の入力を完了し、カーソルを次のフィールドに移動します。
Esc	変更せずに画面を終了します。

フィールドの値を変更しない場合は、情報を変更せずに Enter キーを押してカーソルを次のフィールドに移動します。

メインメニューの表示

メインメニューは、次のセクションで構成されます。

- **Operations** — 任意の数字を押して、対応するサーバー操作を実行します。
- **Configurations** — 任意の文字を押して、対応するサーバー構成コマンドを実行します。
- **Access Control** — 任意の文字を押して、対応するメニュー項目へのアクセス方法を設定します。
- **Extensions** — 任意の文字を押して、対応する拡張機能を選択します。拡張機能のリストをスクロールして表示するには、スペースキーを使用します。

メニューを使用するには、次の手順を実行します。

1. 対応する文字または数字を押して、メニュー項目を選択します。
2. 「Extension」リストのほかのオプションを表示するには、スペースバーを押します。

構成情報のバックアップ

システムを構成したら、構成のバックアップを作成することをお勧めします。



注意: システムは構成情報の冗長コピーを格納しますが、システム障害に備えてバックアップコピーを作成してください。

クラスタ構成では、次の手順を 1 台のサーバー上でのみ実行してください。構成はサーバー間で自動的に同期化されるため、サーバーごとに構成のバックアップを作成する必要はありません。

構成情報をバックアップするには、次の手順を実行します。

1. 220 ページの「管理者コンソールへのアクセス」の手順を実行します。

注意: 予期しない結果を回避するため、コマンドは注意して使用してください。



2. コマンド行で `load unixtools` と入力します。
3. `cp rv /dvol/etc backup path` と入力します。*backup path* は、構成ファイルのバックアップ先となるディレクトリの場所を示すフルパスで、ボリューム名を含みます。既存の空のディレクトリを指定する必要があります。

この操作により、`/dvol/etc` ディレクトリに格納されているすべての構成情報が、指定した場所にコピーされます。

システムの管理

コンソール管理機能を使用して、システム管理作業を行うことができます。この節では、次の作業について説明します。

- 223 ページの「TCP/IP の構成」
- 223 ページの「管理者パスワードの変更」
- 224 ページの「日付および時刻の制御」
- 224 ページの「時刻同期の設定」

- 226 ページの「コマンド行を介した、ウイルス対策保護機能の使用可能への切り替え」
- 227 ページの「コマンド行を介した言語の選択」

TCP/IP の構成

TCP/IP を構成するには、次の手順を実行します。

1. 「Configuration」メニューから「Host Name & Network」を選択します。
2. 「1. Edit fields」を選択します。
3. サーバーのホスト名を入力して、**Enter** キーを押します。
4. 最大転送単位 (MTU) を入力するか、**Enter** キーを押してデフォルトを保持します。
5. サーバーの IP アドレスを入力して、**Enter** キーを押します。
6. ネットワークの IP サブネットマスクを入力して、**Enter** キーを押します。
7. ネットワークの IP ブロードキャストを入力して、**Enter** キーを押します。
8. 「1. Setup」を選択してエイリアス IP アドレスを設定し、**Enter** キーを押します。
9. ほかのすべてのポートについて手順 3～手順 8 を繰り返します。次の処理に進むには、**Enter** キーを押します。
注: ほかのポートが存在する場合は、スペースバーを使用して画面を下にスクロールします。
10. ゲートウェイアドレスを入力して、**Enter** キーを押します。
11. 「7. Save changes」を選択します。

管理者パスワードの変更

管理者パスワードを変更するには、次の手順を実行します。

1. 「Access Control」メニューから「Admin Access」を選択します。
2. パスワード保護を使用可能にするには「Y. Yes」、使用不可にするには「N. No」を選択します。
注: 必ずパスワードを使用してシステムを保護してください。
3. 「Yes」を選択した場合は、パスワードの入力を求めるプロンプトが表示されます。管理アクセス用のパスワードを入力し、確認のためもう一度入力します。

- 「7. Save changes」を選択して、新しいパスワードを使用可能にします。

日付および時刻の制御

システムのタイムゾーン、時刻、および日付の設定を変更するには、「Timezone, Time, Date」メニューオプションを使用してください。メインボードのリアルタイムクロックは、現地時間に設定されています。

注: システムに日付および時刻をはじめて設定する際、システムの固定クロックも初期化されます。このクロックは、ライセンス管理ソフトウェアおよび Compliance Archiving Software で使用され、時間に依存する動作を制御します。

注意: 固定クロックは一度初期化されると再設定できません。したがって、システムを構成する際は、日付および時刻を正確に設定してください。

タイムゾーン、時刻、および日付を設定するには、次の手順を実行します。

- 「Configuration」メニューから「Timezone, Time, Date」を選択します。

- 適切なタイムゾーンを選択して、Enter キーを押します。

- 夏時間について「Y」または「N」を選択します。

- 新しい日付を入力して、Enter キーを押します。

形式は YYYYMMDD で、YYYY は年、MM は月、DD は日を示します。たとえば、20041001 は、2004 年 10 月 1 日を表します。

- 現在の時刻を入力して、Enter キーを押します。

システムは 24 時間時計を使用します。

- 「7. Save changes」を選択します。

注: システムに日付および時刻をはじめて設定する場合は、この手順によって固定クロックも同じ日付および時刻に設定されます。固定クロックは一度しか設定できないため、必ず日付および時刻を正確に設定してください。

時刻同期の設定

NTP プロトコルまたは RDATE サーバーのいずれかの時刻と同期をとるように、システムを構成できます。

NTP は、基準時刻のソースに接続し、コンピュータの時計を同期化するためのインターネットプロトコルです。一般的な NTP 構成には、複数台の冗長サーバーおよび各種ネットワークパスが使用できるため、高い精度と信頼性を実現できます。



RDATE サーバーは、通常 UNIX システム上に存在し、システムサーバーの時刻を RDATE サーバーの時刻に同期化できます。

時刻同期のための NTP の設定

NTP を設定するには、次の手順を実行します。

1. 「Extensions」メニューから、「NTP Configuration」を選択します。
2. 「1. Edit fields」を選択して、NTP の設定を行います。
3. 「Y. Yes」を選択して、NTP を使用可能にします。
4. NTP サーバーは 2 台まで構成できます。「Y. Yes」を選択して、1 台めの NTP サーバーを使用可能にします。
5. Sun StorageTek 5320 NAS Appliance がポーリングによって現在の時刻を取得する最初の NTP サーバーの名前または IP アドレスを入力して、Enter キーを押します。
6. 使用する認証タイプとして、「0. none」または「1. symmetric-key」を選択します。

対称鍵による認証を使用すると、Sun StorageTek 5320 NAS Appliance は、鍵と鍵識別子を使用して NTP サーバーが認識および信頼できることを確認します。メッセージを認証するには、NTP サーバーと Sun StorageTek 5320 NAS Appliance との間で鍵および鍵識別子を一致させる必要があります。

7. 前述のフィールドで認証スキーマとして「Symmetric Key」を選択した場合は、この NTP サーバーに使用される鍵ファイルの非公開鍵に関連付けられた鍵識別子を入力します。
この値の有効範囲は 1 ~ 65534 です。
8. 2 台めの NTP サーバーを構成するには、サーバー 2 に対して手順 4 ~ 手順 7 を繰り返します。
9. 「Min. Polling Interval」フィールドに、NTP メッセージの最小ポーリング率を入力します。
この値が 2 乗されてポーリング間隔の最小秒数となります。たとえば 4 を入力すると、ポーリング間隔は 16 秒になります。このフィールドの値の有効範囲は 4 ~ 17 です。
10. 「Max. Polling Interval」フィールドに、NTP メッセージの最大ポーリング率を入力します。
この値が 2 乗されてポーリング間隔の最大秒数となります。たとえば 4 を入力すると、ポーリング間隔は 16 秒になります。このフィールドの有効範囲は 4 ~ 17 ですが、最小ポーリング間隔よりも大きい値に設定してください。

11. 「Broadcast Client Enabled」フィールドで、「Y. Yes」を選択します。これによって、任意のインタフェースで受信されたサーバーのブロードキャストメッセージに Sun StorageTek 5320 NAS Appliance が応答するようになります。
12. 「Require Server authentication」フィールドで、「Y. Yes」を選択します。これによって、ブロードキャストクライアントによるサーバーの認証が行われます。認証を使用していない NTP サーバーは許可されません。
13. 「7. Save changes」を選択します。

時刻同期のための RDATE サーバーおよび許容範囲の設定

RDATE サーバーおよび許容範囲を設定するには、次の手順を実行します。

1. 「Extensions」メニューから「RDATE time update」を選択します。
2. 「1. Edit fields」を選択します。
3. RDATE サーバーの名前または IP アドレスを入力して、Enter キーを押します。
4. 許容範囲を入力します。

Sun StorageTek 5320 NAS Appliance システムの時刻と RDATE サーバーの時刻との誤差がこの秒数より小さい場合 (+ または -) は、Sun StorageTek 5320 NAS Appliance システムの時刻が RDATE サーバーの時刻に同期化されます。このような誤差の確認は、毎日午後 11 時 45 分に実行されます。Enter キーを押してください。

5. 「7. Save changes」を選択します。

ネットワーク上でウイルス対策スキャンエンジンを実行している場合は、システムにウイルス対策保護機能を構成できます。ウイルス対策保護機能の詳細は、64 ページの「ウイルス対策ソフトウェアについて」を参照してください。

コマンド行を介した、ウイルス対策保護機能の使用可能への切り替え

ウイルス対策保護機能を使用可能にするには、次の手順を実行します。

1. 「Extensions」メニューから、「Anti-Virus Configuration」を選択します。
2. 「1. Edit fields」を選択します。
3. 「AVA Enable」フィールドで「Yes」を指定して、ウイルス対策保護機能を使用可能にします。
4. 「Scan mode」フィールドでスキャンモードを選択します。

スキャンモードオプションの詳細は、65 ページの「ウイルス対策保護機能の使用可能への切り替え」を参照してください。

5. 使用するスキャンエンジンの TCP/IP アドレスを指定します。
6. ICAP サーバーが接続まで待機する TCP/IP のポート番号を指定します。通常はポート 1344 を使用します。
7. システムがスキャンエンジンに振り分ける、並行ファイルスキャン操作の最大数を指定します。通常は 2 を設定します。
8. スキャンの対象または対象外にするファイルタイプと、除外するクライアント、グループ、または共有を指定します。

指定	説明	形式
File Types Included	スキャンの対象にする各ファイルタイプの拡張子。すべてを対象とする場合は、空白にします。	3 文字以内で、コンマで区切って指定します。ワイルドカードマッチング用に ? を使用できます。
File Types Excluded	スキャンの対象外にするファイルタイプの拡張子。	3 文字以内で、コンマで区切って指定します。ワイルドカードマッチング用に ? を使用できます。
Exempt Clients	スキャンから除外する各クライアントの名前または IP アドレス。	コンマで区切って指定します。
Exempt Groups	スキャンから除外する Windows/NT または Windows Active Directory の各グループ (UNIX グループ以外) の名前。	空白文字を含めることができ、コンマで区切って指定します。
Exempt Shares	スキャンから除外する各 CIFS 共有の名前。 注: 管理共有 (x\$) は常にスキャンから除外されます。	コンマで区切って指定します。

9. 「7. Save changes」を選択します。

コマンド行を介した言語の選択

NFS および CIFS で使用する言語を指定できます。

言語を選択するには、次の手順を実行します。

1. 「Extensions」メニューから「Language Selection」を選択します。
2. 使用する言語を入力して、Enter キーを押します。
サポートされる言語は、画面の上部に表示されます。

ルートの管理

ルーティングテーブルには、指定した宛先へのネットワークパケットの送信に使用されるネットワークパスのリストが含まれます。各ルートのエントリは、宛先のアドレスおよびパスで構成されます。宛先には、ネットワークまたはホストのいずれかを指定できます。パスは、宛先へのパケットの送信に使用されるゲートウェイデバイスを示します。

ローカルネットワークの静的ルートを管理するには、次の手順を実行します。

1. 「Configuration」メニューから「Host Name & Network」を選択します。
2. 「2. Manage Routes」を選択します。
3. 「1. Add route」を選択して、「1. Edit」を選択します。
4. ルートのタイプに、ホスト、ネットワーク、ゲートウェイを経由したホスト、ゲートウェイを経由したネットワークのいずれかを選択します。
5. 宛先の IP アドレスを入力して、Enter キーを押します。
6. Sun StorageTek 5320 NAS Appliance を宛先に接続するために使用されるパスまたはゲートウェイアドレスを入力して、Enter キーを押します。
ゲートウェイデバイスは、Sun StorageTek 5320 NAS Appliance と同じサブネットに接続している必要があります。
7. 「7. Save changes」を選択します。

ネームサービス

コンソールインタフェースで使用可能なネームサービスおよび機能は、GUI で使用可能なネームサービスおよび機能とは異なります。

DNS、syslogd、およびローカルロギングの設定

ドメインネームシステム (DNS) は、ドメイン名を IP アドレスに変換する階層的なネームシステムです。syslogd は、遠隔ロギングをサポートするユーティリティーです。ネットワーク上に Sun StorageTek 5320 NAS Appliance のシステムログを受信できる syslogd ユーティリティーを持つ UNIX システムがある場合にのみ、遠隔ロギングを使用可能にできます。これらの機能はすべて同じ画面上で設定します。

syslogd ユーティリティーを設定すると、選択したサーバーにすべてのログメッセージが送信されます。これによって、すべてのサーバーからのログメッセージのレコードを、1 つのシステムに集中させることができます。

DNS、動的 DNS、syslogd、およびローカルロギングを設定するには、次の手順を実行します。

1. 「Configuration」メニューから「DNS & SYSLOGD」を選択します。
2. 「1. Edit fields」を選択します。
3. 「Y. Yes」を選択して、DNS を使用可能にします。
4. 名前解決で最初に照会される DNS サーバーの IP アドレスを入力して、Enter キーを押します。
5. 名前解決で 2 番めに照会されるサーバーの IP アドレスを入力して、Enter キーを押します。
セカンダリ DNS サーバーが存在しない場合は、このフィールドは空白のままにします。
6. DNS サーバーのドメイン名を入力して、Enter キーを押します。
7. システムが各 DNS サーバーに対して DNS 照会を試行する最大回数を入力して、Enter キーを押します。
8. 各 DNS サーバーに照会を試行する間隔を秒単位で入力して、Enter キーを押します。
9. 「Y. Yes」を選択して、遠隔ロギングを使用可能にします。ネットワーク上に syslogd サーバーが存在しない場合は「N. No」を選択して、手順 15 に進みます。
この機能を使用すると、Sun StorageTek 5320 NAS Appliance が遠隔 syslogd サーバーにログメッセージを送信できます。
10. syslogd サーバーの名前または IP アドレスを入力して、Enter キーを押します。

11. 適切な機能を選択して、**Enter** キーを押します。機能は、メッセージの生成元のアプリケーションまたはシステムコンポーネントを示します。選択できる機能を次に示します。
 - **Kern** – カーネルによって生成されるメッセージ。ユーザープロセスでは生成されないメッセージです。
 - **User** – ランダムユーザープロセスによって生成されるメッセージ。機能を指定しない場合は、この機能識別子がデフォルトで指定されます。
 - **Mail** – メールシステム。
 - **Daemon** – システムデーモンまたはネットワークデーモン。
 - **Auth** – ログインなどの認証システム。
 - **Syslog** – syslogd によって内部的に生成されるメッセージ。
 - **Local0 ~ Local7** – ローカルでの使用のために予約済み。
12. Sun StorageTek 5320 NAS Appliance ログに記録するシステムイベントのタイプを選択します。
 - a. 適切なイベントタイプを選択します。
 - b. 「Y. Yes」を選択して、そのタイプのイベントが報告されるようにします。次のイベントタイプがあります。
 - **Emerg** – 緊急メッセージであることを示します。このメッセージは一部のユーザーに送信されます。優先順位が緊急のメッセージは、確認用に別のファイルに記録できます。
 - **Alert** – ただちに対処する必要がある重要メッセージであることを示します。このメッセージはすべてのユーザーに送信されます。
 - **Crit** – ハードウェアの問題など、エラーには分類されない重大メッセージであることを示します。優先順位が重大以上のメッセージはシステムコンソールに送信されます。
 - **Err** – ディスク書き込みの失敗など、エラーの状態を示すメッセージであることを示します。
 - **Warning** – 回復可能な異常に関するメッセージであることを示します。
 - **Notice** – 重要な情報メッセージであることを示します。優先順位指定のないメッセージは、この優先順位のメッセージに割り当てられます。
 - **Info** – 情報メッセージであることを示します。このメッセージはシステムの分析に役立ちます。
 - **Debug** – デバッグに関するメッセージであることを示します。
 - c. **Enter** キーを押して、次のイベントタイプに移動します。
13. 「Y. Yes」を選択して、動的 DNS 更新を使用可能にします。

動的 DNS 更新を使用すると、セキュリティー保護されていない動的更新が起動時に実行されます。

14. セキュリティー保護された更新を可能にするには、Windows ユーザーの名前を入力し動的 DNS クライアントがこの名前によって更新を検証できるようにして、Enter キーを押します。
このユーザーには管理権限が必要です。
15. 動的 DNS ユーザーのパスワードを入力して、Enter キーを押します。
16. 「Y. Yes」を選択して、ローカルログインを使用可能にします。
17. 「Log File」フィールドに、ログファイルのパス (ディレクトリ) およびファイル名を入力します。
注: /cvol ディレクトリへのローカルログインは設定できません。
/dvol/error.txt などの別のディレクトリを指定してください。
18. 「Archives」フィールドに、アーカイブファイルの最大数を入力します。
指定可能な範囲は 1 ~ 9 です。
19. 「Archives」フィールドに、各アーカイブファイルの最大ファイルサイズを K バイト単位で入力します。
指定可能な範囲は 1000K ~ 999,999K バイトです。
20. 「7. Save changes」を選択します。

NIS および NIS+ の設定

注: NIS を設定したあと、サーバーを定期的に検査してマスターファイルの変更の有無を確認してください。変更されたファイルは NIS サーバーからローカルファイルにコピーされます。「Enable」フィールドを使用すると、設定情報を失うことなく NIS 更新を使用不可にし、再度使用可能にするときまで設定情報を保持できます。

NIS または NIS+ を使用可能にするには、次の手順を実行します。

1. 「Configuration」メニューから「NIS & NIS+」を選択します。
2. 「1. Edit fields」を選択します。
3. 「Y. Yes」を選択して、Sun StorageTek 5320 NAS Appliance による、NIS サーバーを使用したホスト、ユーザー、およびグループのファイルの定期的な更新を使用可能にします。
4. NIS ドメイン名を入力して、Enter キーを押します。
5. NIS サーバーの名前または IP アドレスを入力して、Enter キーを押します。
6. 「Y. Yes」を選択して、NIS サーバーによるホストのファイルの更新を使用可能にします。

7. 「Y. Yes」を選択して、NIS サーバーによるユーザーのファイルの更新を使用可能にします。
8. 「Y. Yes」を選択して、NIS サーバーによるグループのファイルの更新を使用可能にします。
9. 「Y. Yes」を選択して、NIS サーバーによるネットグループのファイルの更新を使用可能にします。
10. NIS 更新の間隔を 0 ～ 9 分の範囲で入力して、Enter キーを押します。
11. 「Y. Yes」を選択して、Sun StorageTek 5320 NAS Appliance に対して NIS+ を使用可能にします。
12. NIS+ ホームドメインサーバーのアドレスを入力して、Enter キーを押します。
13. NIS+ ホームドメイン名を入力して、Enter キーを押します。
14. NIS+ サーバーの、セキュリティー保護された RPC パスワードを入力します。Enter キーを押します。
15. コロンで区切ったドメインのリストの形式で検索パスを入力します。ホームドメインとその親のみを検索する場合、このフィールドは空白のままにします。Enter キーを押します。
16. 「7. Save changes」を選択します。

ネームサービスの検索順序の設定

ユーザー、グループ、およびホストの検索機能で最初に使用されるサービスを選択できます。

検索順序を設定するには、次の手順を実行します。

1. 「Configuration」メニューから「Lookup orders」を選択します。
2. 「1. Edit fields」を選択します。
3. ユーザー情報を解決する順序 (NIS または NIS+ のいずれか) を選択して、Enter キーを押します。
4. グループ情報を解決する順序 (NIS または NIS+ のいずれか) を選択して、Enter キーを押します。
5. ホスト情報を解決する 1 ～ 4 番めのサービスを選択して、Enter キーを押します。
6. 「7. Save changes」を選択します。

サーバーファイルシステムの管理

コンソールでは、いくつかの手順を実行して、サーバーファイルシステム (SFS) ボリュームを管理できます。次の節では、もっとも一般的な手順について説明します。

- 233 ページの「ドライブ文字の構成」
- 234 ページの「新しいディスクボリュームの作成」
- 234 ページの「パーティションの名前の変更」
- 235 ページの「拡張セグメントの追加」
- 235 ページの「ディスクボリュームの削除」

ドライブ文字の構成

ドライブ文字は、SMB/CIFS を使用して共有可能なファイルボリュームに自動的に割り当てられます。\`\cvol` にのみ割り当てることができるドライブ `C:` を除き、コンソールを使用してドライブ文字の割り当てを手動で行うことができます。

使用できるドライブ文字がなくなる場合もあり、その際は次のログメッセージが表示されます。

```
No drive letter available
```

このメッセージは情報提供のみを目的としています。ファイルシステムは作成されませんが、ドライブ文字を割り当てするには、現在ほかのファイルシステムに使用されているドライブ文字を割り当て直す必要があります。

ファイルボリュームへのドライブ文字の再割り当てを手動で行うには、次の手順に従います。

1. 「Configuration」メニューから「Drive Letters」を選択します。
2. 変更するドライブ文字を入力して、Enter キーを押します。
3. ドライブ文字に新たに割り当てるファイルボリューム名を入力して、Enter キーを押します。

ドライブ文字には既存のファイルボリュームのみを割り当てることができます。

4. Esc キーを押して、この画面を終了します。

新しいディスクボリュームの作成

新しいディスクボリュームを作成するには、次の手順を実行します。

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 構成するドライブの文字を入力します。
3. 「1. Edit」を選択します。
4. 「1. Create partition」を選択します。
5. ドライブのパーティションタイプを選択します。
sfs2 (一次ボリューム)、sfs2ext (セグメント) などのデフォルト設定を使用する場合は、Enter キーを押してください。
6. ディスクボリュームラベルを入力して、Enter キーを押します。
7. このボリュームで規制適合アーカイブ機能を使用可能にするかどうかを確認するプロンプトが表示された場合で、Compliance Archiving Software のライセンスを持っているときは、Y キーを押して規制適合対応ボリュームを作成します。
注: Sun StorageTek 5320 NAS Gateway システムの構成では、推奨実施の規制適合はサポートされていますが、必須実施の規制適合はサポートされていません。
注意: いったんボリュームに対して必須実施の規制適合アーカイブ機能を使用可能にすると、そのボリュームの削除、名前の変更、あるいは規制適合アーカイブの使用不可への切り替えまたは推奨実施へのダウングレードは実行できなくなります。
8. Enter キーを押してデフォルトのサイズを選択するか、ディスクボリュームのサイズを M バイト単位で入力して Enter キーを押します。
9. 「7. Proceed with create」を選択します。
「Initialization OK」および「Mount OK」というメッセージが表示されるまで待機し、Esc キーを押して「Configure Disk」メニューに戻ります。
10. 新しいファイルボリュームの作成が終了したら、メインメニューが表示されるまで Esc キーを押します。



パーティションの名前の変更

書き込み操作中にボリュームの名前を変更しようとした場合、CIFS クライアントと NFS クライアントでは動作が異なります。書き込み操作中に Windows ボリュームの名前を変更しようとする、ボリュームの名前が変更されたあとに、CIFS での入出力が停止します。NFS 共有の場合は、UNIX ボリュームの名前を変更したあとでも入出力が継続されます。

パーティションの名前を変更するには、次の手順を実行します。

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 名前を変更するドライブの文字を入力します。
3. 「1. Edit」を選択します。
4. 「3. Rename」を選択します。
5. パーティションの新しい名前を入力して、**Enter** キーを押します。
注: 厳格な規制適合対応のボリュームは、名前を変更できません。

拡張セグメントの追加

拡張セグメントを追加するには、まずそのボリューム上に `sfs2ext` パーティションを作成する必要があります。

注: `sfs` ファイルボリュームに拡張ボリュームを配置したあと、これを切り離すことはできません。これは取り消し不可能な操作です。拡張ボリュームを切り離す唯一の方法は、`sfs` ファイルボリュームを削除することです。

拡張セグメントを追加するには、次の手順を実行します。

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 構成するドライブの文字を入力します。
注: ディスクドライブ (ディスクボリューム) の数が 26 を超えている場合は、スペースバーを押して探します。
3. 変更するパーティションの横に表示されている数字を入力します。
4. 「5. Segments」を選択します。
5. 「1. Add an extension segment」を選択します。
6. 拡張ドライブの横に表示されている文字を選択します。
7. 「7. Proceed」を選択します。

ディスクボリュームの削除

注: 厳格な規制適合対応ボリュームは、削除できません。

注意: ボリュームを削除すると、ボリューム内のすべてのデータが失われます。

ディスクボリュームを削除するには、次の手順を実行します。



1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 構成するドライブの文字を入力します。
注: ディスクドライブ (ディスクボリューム) の数が 26 個を超えている場合は、スペースバーを押して探します。
3. 「1. Edit」を選択します。
4. 「8. Delete」を選択します。
5. ディスクボリューム名を入力して、Enter キーを押します。
6. 「7. Proceed with delete」を選択します。「Delete OK」および「Delpart OK」というメッセージが表示されるまで待機します。
7. Esc キーを押して「Configure Disk」メニューに戻ります。
8. メインメニューが表示されるまで Esc キーを押します。

共有および割り当て

コンソールを使用して、共有および割り当てを管理できます。

SMB/CIFS 共有

CIFS は、SMB プロトコルを使用する Windows のファイル共有サービスです。CIFS は、Windows クライアントシステムが Sun StorageTek 5320 NAS Appliance 上のファイルにアクセスするためのメカニズムを提供します。

SMB/CIFS 共有の設定

共有を設定するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「A. Domain Configuration」を選択します。
3. 「Domain」フィールドにワークグループまたはドメインの名前を入力します。
4. 必要に応じて、ドメインの適用範囲を定義します。
5. Sun StorageTek 5320 NAS Appliance サーバーの説明を入力します。

6. 必要に応じて、プライマリおよびセカンダリの WINS サーバーの IP アドレスを入力します。
7. 「Keep Alive」パラメータを割り当てます。
これは、アクティブでない接続をシステムが切断するまでの秒数です。
8. セキュリティーモードに「Secure Share Level」または「NT Domain Auto UID」を割り当てます。
9. 「NT Domain Auto UID」モードを使用する場合は、管理者ユーザーの名前およびパスワードを入力します。
10. 「7. Save changes」を選択します。
「Secure Share Level」および「NT Domain Auto UID」間でセキュリティーモードを変更した場合、Sun StorageTek 5320 NAS Appliance が再起動します。

自動ホーム SMB/CIFS 共有の設定

自動ホーム共有は、ユーザーがシステムにログインすると作成され、ログアウトすると削除される、一時的な共有です。

自動ホーム共有機能では、次に定義する状態および自動ホームパスの 2 つの構成パラメータが必要になります。

- 状態パラメータは、自動ホーム共有機能を使用可能にするか使用不可にするかを決定します。この機能の現在の状態は、環境変数 `smb.autohome.enable` によって保持されます。値は「yes」または「no」である必要があります。
- 自動ホームパスパラメータは、一時的な共有のベースディレクトリのパスを定義します。これは、`smb.autohome.path` 環境変数によって定義されます。たとえば、ユーザーのホームディレクトリが `/vol1/home/john` である場合、自動ホームパスは `/vol1/home` に設定します。一時的な共有の名前は、`john` になります。ユーザーのホームディレクトリの名前は、ユーザーのログイン名と同じである必要があります。

この機能が使用不可である場合、自動ホームパスパラメータは無効となり評価されません。

この機能が使用可能で、パスの文字列の長さが 0 である場合には、構成は無視されません。この機能が使用可能で、パスの文字列の長さが 0 でない場合は、パスが評価されます。自動ホームパスパラメータが既存のディレクトリパスを示していないと、システムログに情報メッセージが書き込まれます。たとえば、`/vol1/home` をベースパスに指定した場合は、次のようなログメッセージが書き込まれます。

```
SMB autohome: /vol1/home: no such directory
```

このログメッセージはシステム管理者に状況を通知するためのもので、構成は有効なままになります。システムは正常に動作しますが、自動ホーム共有は作成されません。そのあと指定したディレクトリパスが作成されると、その時点で、必要に応じて自動ホーム共有が追加および削除されます。

自動ホーム共有を使用可能にするには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「F. Autohome Setup」を選択します。
3. 「1. Edit fields」を選択します。
4. 「Y. Yes」を選択して、自動ホーム共有を使用可能にします。
5. 自動ホームパスを入力します。

自動ホームパスとは、共有のベースディレクトリのパスです。たとえば、ユーザーのホームディレクトリが `/usr/home/john` である場合、自動ホームパスは `/usr/home` に設定します。一時的な共有の名前は `john` になります。システムでは、ユーザーのホームディレクトリの名前は、ユーザーのログイン名と同じであると見なされます。

6. 「7. Save changes」を選択します。

共有の追加

SMB/CIFS の設定が完了したあとに、SMB/CIFS 共有を定義します。Windows ユーザーは、共有を使用して Sun StorageTek 5320 NAS Appliance 上のディレクトリにアクセスできます。

共有を追加するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「E. Shares」を選択します。
3. 「8. Add a share」を選択します。
4. 共有名を入力します。
5. ボリューム/ディレクトリの形式で、ディレクトリのパスを入力します。
6. 必要に応じて、このディレクトリに関するコメントを入力します。
7. システムがワークグループモードで構成されている場合は、次の手順を実行します。
 - 「Password Protection」プルダウンメニューで、「Yes」または「No」を選択します。

これを使用可能にすると、読み取り/書き込みまたは読み取り専用のいずれかを選択するオプションが表示されます。

- ユーザー ID、グループ ID、および umask を入力します。

8. 「7. Save changes」を選択します。

共有の編集

共有を編集するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「E. Shares」を選択します。
3. 編集する共有に対応する文字を入力します。
4. 「1. Edit fields」を選択します。
5. 新しい共有名、ディレクトリ、コメント、パスワード情報、ユーザー ID、およびグループ ID を入力します。
6. システムがワークグループモードで構成されている場合は、次の手順を実行します。
 - 「Password Protection」プルダウンメニューで、「Yes」または「No」を選択します。

これを使用可能にすると、読み取り/書き込みまたは読み取り専用のいずれかを選択するオプションが表示されます。
 - ユーザー ID、グループ ID、および umask を入力します。
7. 「7. Save changes」を選択します。

共有の削除

共有を削除するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「E. Shares」を選択します。
3. 削除する共有に対応する文字を入力します。
4. 「8. Delete」を選択します。

Active Directory サービスの設定

Active Directory サービス (ADS) を使用可能にして設定を行うと、Sun StorageTek 5320 NAS Appliance は自動的に ADS 更新を実行します。

ADS サービスを使用可能にするには、次の手順を実行します。

1. 「Extensions」メニューから「ADS Setup」を選択します。
2. 「1. Edit fields」を選択します。
3. 「Y. Yes」を選択して、ADS クライアントによる ADS への Sun StorageTek 5320 NAS Appliance 共有の公開を許可します。
4. ADS が動作している Windows ドメインを入力します。
Sun StorageTek 5320 NAS Appliance もこのドメインに属している必要があります。
5. 管理権限のある Windows ユーザーの名前を入力します。
ADS クライアントでは、このユーザーによるセキュリティー保護された ADS の更新が検証されます。
6. Windows の管理者ユーザーのパスワードを入力します。
7. 「User Container」フィールドに、Windows の管理者ユーザーの ADS パスを LDAP の DN 記法で入力します。
詳細は、77 ページの「ADS の使用可能への切り替え」を参照してください。
8. ADS ドメインがサイトを使用する場合は、「Site」フィールドに適切なサイト名を入力します。サイトを使用しない場合は、「Site」フィールドは空白のままにしてください。サイト名を指定すると、ドメインコントローラを選択したときにこのサイトが含まれるようになります。
9. ADS の識別に使用される Kerberos レalm名を大文字で入力します。
通常、これは ADS ドメインになります。
10. Kerberos 鍵配布センター (KDC) サーバーのホスト名を入力します。
通常、これは ADS ドメインのメインドメインコントローラのホスト名です。ADS クライアントまたは動的 DNS クライアントが DNS を介して KDC サーバーを検索できる場合は、このフィールドを空白のままにします。
11. 「7. Save changes」を選択します。

割り当てを使用可能および使用不可にする方法

割り当ては、それぞれのユーザーおよびグループが使用するディスク領域の量を追跡および制限します。割り当ての追跡機能をオンまたはオフにすることができます。この機能は、割り当ての使用可能または使用不可への切り替えのみを行うことができます。割り当ての制限の設定は行いません。

注: 割り当ての初期化には数分かかります。その間、ボリュームはロックされ、ユーザーが使用することはできません。

割り当てを使用可能または使用不可にするには、次の手順を実行します。

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 割り当てを使用可能にするドライブを選択します。
3. 「1. Edit」を選択します。
4. 「4. Quotas on/off」を選択します。
5. 「1. Turn quotas on」または「8. Turn quotas off」を選択します。

セキュリティ

グループと資格のマッピングを設定することで、セキュリティ保護を確実に実施できます。次の節では、それらの作業について説明します。

- 241 ページの「ユーザーグループの構成」
- 243 ページの「グループ権限の変更」
- 243 ページの「ユーザーマップとグループマップ」
- 245 ページの「マッピングおよびセキュリティ保護が可能なオブジェクト」
- 247 ページの「ホストリストの構成」
- 248 ページの「信頼できるホストの管理」
- 248 ページの「ボリュームアクセスの管理」
- 249 ページの「コンソールのロックおよびロック解除」

ユーザーグループの構成

組み込みローカルグループの要件は、Windows NT システムのローカルグループの要件とは異なります。ユーザーグループの詳細は、86 ページの「ローカルグループについて」を参照してください。

グループの追加

グループを追加するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 「8. Add a Group」を選択して、ローカルグループを追加します。
4. グループの名前を入力して、Enter キーを押します。
5. 必要に応じて、グループの説明を入力し、Enter キーを押します。
6. 「7. Save Changes」を選択して、新しいグループを保存します。

グループへのメンバーの追加

グループにメンバーを追加するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 変更するグループの文字を押します。
4. 「2. Members」を選択して、グループのメンバーシップを変更します。
5. 「8. Add」を選択して、メンバーを追加します。

6. 「ドメイン\ユーザー名」の形式でドメインおよびユーザー名を入力します。

ドメインとは、ユーザー名を認証できるドメインです。たとえば、BENCHLAB\
john と入力した場合は、john というユーザーを認証できるドメイン BENCHLAB
を指定したことになります。

7. Enter キーを押します。
8. 「7. Save Changes」を選択して、新しいメンバーを保存します。

グループからのメンバーの削除

グループからメンバーを削除するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 変更するグループの文字を押します。

4. 「2. Members」を選択して、グループのメンバーシップを変更します。
5. 削除するグループメンバーに対応する文字を押します。
6. プロンプトが表示されたら Y キーを押します。

グループ権限の変更

ユーザーグループの権限の詳細は、86 ページの「ローカルグループの権限の構成について」を参照してください。

ローカルグループの権限を変更するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「B. Local Groups」を選択します。
3. 変更するグループの文字を押します。
4. 「3. Privileges」を選択して、グループメンバーの権限を変更します。
5. 追加または削除する権限の文字を押します。
6. 「7. Save Changes」を選択して、変更内容を保存します。

ユーザーマップとグループマップ

ユーザーおよびグループの資格の詳細は、94 ページの「ユーザーおよびグループの資格のマッピングについて」を参照してください。

ユーザーマップの追加

ユーザーマップを追加するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「C. User Mapping」を選択します。
3. 「8. Add a map」を押します。
4. 「Account」フィールドに、UNIX ユーザーにマッピングする NT ユーザーのドメインおよび名前を入力します。
「ドメイン\ユーザー名」の形式を使用します。
5. 「Name」フィールドに、NT ユーザーにマッピングする UNIX ユーザーの名前を入力します。

6. 「7. Save Changes」を選択します。

ユーザーマップの編集

ユーザーマップを編集するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「C. User Mapping」を選択します。
3. 編集するマップの文字を押します。
4. 「1. Edit Fields」を押します。
5. 変更内容を入力して、Enter キーを押します。
6. 「7. Save Changes」を選択します。

ユーザーマップの削除

ユーザーマップを削除するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「C. User Mapping」を選択します。
3. 削除するユーザーマップの文字を押します。
4. 「8. Delete」を選択します。

グループマップの追加

グループマップを追加するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「D. Group Mapping」を選択します。
3. 「8. Add a map」を押します。
4. 「Account」フィールドに、UNIX グループにマッピングする NT グループのドメインおよび名前を入力します。「ドメイン\ユーザー名」の形式を使用します。
5. 「Name」フィールドに、NT グループにマッピングする UNIX グループの名前を入力します。
6. 「7. Save Changes」を選択します。

グループマップの編集

グループマップを編集するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「D. Group Mapping」を選択します。
3. 編集するグループマップの文字を押します。
4. 「1. Edit Fields」を押します。
5. 変更内容を入力して、Enter キーを押します。
6. 「7. Save Changes」を選択します。

グループマップの削除

グループマップを削除するには、次の手順を実行します。

1. 「Extensions」メニューから「CIFS/SMB Configuration」を選択します。
2. 「D. Group Mapping」を選択します。
3. 削除するグループマップの文字を押します。
4. 「8. Delete」を押します。

マッピングおよびセキュリティ保護が可能なオブジェクト

この節では、ユーザーまたはグループの資格のマッピングと、ファイルシステムに含まれるファイルやディレクトリなどの、セキュリティ保護が可能なシステム内のオブジェクトとの間の相互作用について詳細に説明します。

システム上のオブジェクトは、そのセキュリティ属性が設定されたドメインに応じて分類されます。NFS プロトコルを使用して作成されたオブジェクトは UNIX のセキュリティ属性のみを保持するため、UNIX オブジェクトとして分類されます。SMB プロトコルを使用して作成されたオブジェクトは UNIX および Windows の両方のセキュリティ属性を保持しますが、Windows オブジェクトとして分類されません。セキュリティ属性の変更に伴うドメイン間の移行をオブジェクトに許可することも可能ですが、一方向の移行のみを許可するようにポリシーで定められています。SMB を使用してセキュリティ属性を変更すると、UNIX オブジェクトは Windows オブジェクトになります。デフォルトでは、NFS を使用して Windows オブジェクトのセキュリティ属性を変更することはできません。これは、Windows セキュリティがセキュリティ記述子に基づいて設定されており、UNIX のセキュリティ

属性では必ずしも正確に表すことができないためです。Windows オブジェクトから UNIX オブジェクトへの変更を許可すると、オブジェクトを保護するアクセス制御を弱める可能性があります。

NFS を介して Windows オブジェクトの属性を変更するメカニズムには、`ch smb` コマンドと `acl.override.allowed` 環境変数の 2 つがあります。

`acl.override.allowed` が存在しないか「no」に設定されている場合は、ボリュームのデフォルトの動作が適用されるため、NFS を介して Windows オブジェクトの属性を変更することはできません。

`acl.override.allowed` 環境変数が「yes」に設定されていると、標準的な UNIX のアクセス規則に従って、`chown`、`chgrp`、`chmod` などの UNIX コマンドが許可されます。NFS を使用して Windows オブジェクトの属性を変更すると、Windows セキュリティー記述子は削除され、オブジェクトは UNIX オブジェクトになります。

`ch smb` コマンドを使用すると、単一の Windows セキュリティー記述子、または 1 つのボリューム内の Windows セキュリティー記述子データベース全体を削除できます。`ch smb` コマンドを個別のファイルまたはディレクトリに適用するには、そのオブジェクトに対する絶対パスを指定する必要があります。`ch smb` では再帰的な処理が実行されないため、このコマンドをディレクトリに適用した場合、ディレクトリに含まれるサブディレクトリやファイルは影響を受けません。`ch smb` コマンドの使用例を次に示します。

`/vol1/shared/bin/file.doc` 上のセキュリティ記述子を削除して UNIX のアクセス権に戻すには、次のコマンドを使用します。

```
ch smb /vol1/shared/bin/file.doc
```

`/vol1` 上のすべてのセキュリティ記述子を削除し、すべてのファイルをそれぞれの UNIX のアクセス権に戻すには、次のコマンドを使用します。

```
ch smb /vol1
```

`ch smb` コマンドはファイルのセキュリティに影響を及ぼすため、このコマンドを使用する際は特に注意してください。ボリュームが指定されると、`ch smb` コマンドは処理を実行する前に警告を出し、確認のプロンプトを表示します。

Windows ユーザーが Windows オブジェクトにアクセスする際は、マッピングは実行されません。同様に、UNIX ユーザーが UNIX オブジェクトにアクセスする際にも、マッピングは実行されません。これらはネイティブなアクセス状況と見なされます。また、Windows オブジェクトには Windows および UNIX の両方のセキュリティ属性が含まれるため、UNIX ユーザーが Windows オブジェクトにアクセスする際は、ネイティブなアクセス状況ではありませんが、マッピングを必要としません。これは、独立した中立のマッピングを作成するのではなく、1 つのドメインをデフォルトのマッピングとして選択する設計であることの直接的な利点です。したがって、マッピングが必要になるのは、Windows ユーザーが UNIX オブジェクトにアクセスする場合のみです。Windows ユーザーが UNIX オブジェクトにアクセスする場合は、オブジェクトの UNIX セキュリティー属性が Windows ドメインにマッピングされ、Windows のセキュリティポリシーが適用されます。

ホストリストの構成

コンソールを使用して、ホスト情報を設定できます。

ホストの追加

ホストを追加するには、次の手順を実行します。

1. 「Configuration」メニューから「Hosts」を選択します。
2. 新しいホスト名を入力して、Enter キーを押します。
システムによって、そのホスト名がまだ使用されていないことが確認されます。
3. Enter キーを押して、ホストを追加します。
4. 新しいホストの IP アドレスを入力します。
5. 「7. Save changes」を選択します。

既存のホストの編集

既存のホストを編集するには、次の手順を実行します。

1. 「Configuration」メニューから「Hosts」を選択します。
2. 編集するホストの名前を入力して、Enter キーを押します。
3. 「1. Edit」を選択します。
4. 新しいホストの名前または IP アドレスを入力します。
5. 「7. Save changes」を選択します。

ホストの削除

ホストを削除するには、次の手順を実行します。

1. 「Configuration」メニューから「Hosts」を選択します。
2. 削除するホストの名前を入力して、Enter キーを押します。
3. 「8. Delete」を選択します。

信頼できるホストの管理

「Trusted Hosts」メニューオプションを使用して、すべてのリソースへの無制限のアクセス権を持つホストを管理します。

信頼できるホストの指定

信頼できるホストを指定するには、次の手順を実行します。

1. 「Access Control」メニューから「Trusted Hosts」を選択します。
2. ホスト名を入力して、Enter キーを押します。

注: 信頼できるホストを追加するには、そのホストがホストリストまたはNISに存在している必要があります。

システムによって、そのホストの名前が信頼できるホストとしてまだ指定されていないことが確認されます。すでに信頼できるホストとして存在する場合は、ホストの情報が表示されます。ホストが信頼されていない場合は、警告が表示されます。

3. 「7. Add to list」を選択します。

新しく信頼できるホストが追加され、画面の上部に名前が表示されます。

信頼できるホストの削除

信頼できるホストを削除するには、次の手順を実行します。

1. 「Access Control」メニューから「Trusted Hosts」を選択します。
2. 削除する、信頼できるホストの名前を入力して、Enter キーを押します。
3. 「8. Delete」を選択します。

信頼できるホストがリストから削除されます。

ボリュームアクセスの管理

変更内容を保存すると、クライアントによる既存のNFSマウントが更新され、新しいパラメータが反映されます。

cvol ボリュームに対しては、読み取りおよび書き込みを含むすべてのアクセスを禁止してください。

注: 信頼できるホストには、ボリュームのアクセス権の設定にかかわらず、ファイルボリュームの読み取り/書き込みアクセス権が自動的に付与されます。

NFS クライアントのボリュームアクセスの管理

NFS クライアントのボリュームアクセスを管理するには、次の手順を実行します。

1. 「Access Control」メニューから「Volume Access」を選択します。
2. アクセス権を変更するボリュームに対応する文字を入力します。
3. 割り当てるアクセス権のタイプ、つまり読み取り/書き込み、読み取り専用、またはアクセス不可に対応する番号を入力します。

注: 信頼できるホストのリストに含まれるホストは、ボリュームアクセスパラメータの設定にかかわらず、読み取り/書き込みアクセスを許可されます。

4. 「7. Save changes」を選択します。

コンソールのロックおよびロック解除

コンソールの不正な使用を防ぐため、コンソールを使用して、ほとんどのメインメニューオプションを使用可能または使用不可に切り替えることができます。コンソールを保護するには、管理パスワードを設定する必要があります。

コンソールのロック

コンソールをロックするには、次の手順を実行します。

1. 「Operations」メニューから「Lock Console」を選択します。
2. 管理パスワードを入力します。
3. 「Y (Yes)」を選択します。

コンソールのロック解除

コンソールのロックを解除するには、次の手順を実行します。

1. メインメニューから「Unlock Console」を選択します。
2. 管理パスワードを入力します。
3. 「Y (Yes)」を選択します。

ファイルボリュームのミラー化

この節では、Sun StorageTek 5320 NAS Appliance のアクティブシステムから、Sun StorageTek 5320 NAS Appliance のミラーシステムへ、ファイルボリュームをミラー化する方法について説明します。ミラー化の詳細は、第 9 章を参照してください。

注: Sun StorageTek 5320 NAS Cluster Appliance でファイルの複製機能を使用する際、クラスタが縮退状態にある場合には役割の変更などのミラー化操作を実行しないでください。

アクティブサーバーおよびミラーサーバーの構成

アクティブサーバーおよびミラーサーバー上でプライマリ IP アドレスを構成し、Sun StorageTek 5320 NAS Appliance のミラーサーバーを相互に接続するポートの役割を指定したあとで、コンソールインタフェースを使用してアクティブサーバーおよびミラーサーバーのミラー化を構成できます。

新しいアクティブサーバーでの新しいミラーサーバーの構成

次の手順は、まずアクティブサーバーで実行し、次に Telnet を使用してミラーサーバーで実行してください。

新しいアクティブサーバーに新しいミラーサーバーを構成するには、次の手順を実行します。

1. 「Configuration」メニューから「Host Names and Network」を選択します。
2. 「1. Edit Fields」を選択します。
3. ローカルネットワークまたはサブネットに接続するポートを構成していない場合は、ポートを構成します。
コンソールを使用した TCP/IP の設定の詳細は、223 ページの「TCP/IP の構成」を参照してください。ポートの構成の詳細は、第 5 章を参照してください。
4. アクティブシステムとミラーシステムとの接続に使用するポートに、サーバー名と IP アドレスを割り当てます。
5. アクティブサーバーとミラーサーバーとの接続に使用するポートの「Role」フィールドで、「Mirror」を選択します。
6. 「Save」を選択して変更内容を保存し、メインメニューに戻ります。

7. DNS サービスおよび NIS/NIS+ サービスが使用可能である場合はこれを設定し、ネームサービスの検索順序を設定します。
ネームサービスの設定の詳細は、228 ページの「ネームサービス」を参照してください。
これで、アクティブシステムおよびミラーシステムのネットワーク接続が構成されました。続けて次の節を参照してください。

既存のアクティブサーバーでの新しいミラーサーバーの構成

既存のアクティブサーバーに新しいミラーサーバーを構成するには、次の手順を実行します。

1. アクティブサーバー上で、「Configuration」メニューから「Host Names and Network」を選択します。
2. 「1. Edit Fields」を選択します。
3. アクティブシステムとミラーシステムとの接続に使用するポートに、サーバー名と IP アドレスを割り当てます。
4. アクティブサーバーとミラーサーバーとの接続に使用するポートの「Role」フィールドで、「Mirror」を選択します。
5. Telnet ウィンドウを開いてミラーシステムにアクセスし、手順 1～手順 4 を繰り返します。
6. アクティブサーバーの Telnet ウィンドウで、次のコマンド行が表示されるまで Esc キーを押します。
`connect to (? for list) ? [menu]`
7. 管理者としてログインします。
8. 次の項目を入力します。
ping xxx.xxx.xx.xx
xxx.xxx.xx.xx は、ミラーサーバーの IP アドレスです。
9. ミラーサーバーに管理者としてログインし、アクティブサーバーの IP アドレスを入力します。
これで、アクティブシステムおよびミラーシステムのネットワーク接続が構成されました。次に進んで、ミラー化するファイルボリュームを構成してください。

ファイルボリュームの構成

ミラー化は、ボリューム単位で実行されます。使用しているボリュームの一部またはすべてをミラー化できます。

注: いったんファイルボリュームをミラー化すると、ミラー接続が保持されている間は、元のファイルボリュームの名前を変更できません。ミラー化できるのは、1G バイト以上のファイルボリュームのみです。

ミラー化するファイルボリュームの設定

ミラー化するファイルボリュームを設定するには、次の手順を実行します。

1. アクティブシステムで、ほかのボリュームを作成する前に、32M バイトなどの小さいファイルボリュームを **SYS** という名前で作成します。
アクティブシステム上にすでにファイルボリュームがある場合は、この手順は任意です。
2. アクティブシステム上で、「**Configuration**」メニューから「**Disks and Volumes**」を選択します。
3. 新しいファイルボリュームを作成するドライブを選択します。
4. 「**Create & init partition**」を選択します。次に「**1. sfs2**」を選択します。
5. 名前に「**SYS**」と入力し、サイズには **M** バイト単位で **64** と入力します。
この操作によって、**/etc** ディレクトリおよびそれに含まれる **Sun StorageTek 5320 NAS Appliance** の構成ファイルが、強制的に **SYS** ボリューム内に格納されます。
6. ミラーシステムで手順 1～手順 5 を繰り返します。
ミラーシステムには、これ以外のファイルボリュームを作成しないでください。

ファイルボリュームのミラー化

ファイルボリュームをミラー化するには、次の手順を実行します。

1. **Telnet** を使用してアクティブシステムに接続し、メインメニューを表示します。
2. 「**Operations**」メニューから「**Licenses**」を選択し、「**Mirroring**」に対応する文字を選択します。
3. ご購入先から提供された起動キーを正確に入力します。
4. メインメニューが表示されるまで、**Esc** キーを押します。

5. 「Extensions」メニューから、「Mirrors」を選択します。
6. 「Add mirror」を選択して新しいミラーを作成します。
7. ミラー化するファイルボリュームに対応する文字を入力して、ファイルボリュームを選択します。
ファイルボリュームは、1G バイト以上である必要があります。
8. ミラーシステムのホスト名を入力します。
9. 必要に応じてプライベート IP アドレスを入力します。
これは、ミラーサーバーとのミラー接続に使用される IP アドレスです。
10. 「Alt IP Address」フィールドに代替 IP アドレスを入力します。
11. ミラーサーバーへのアクセスに管理パスワードが必要な場合は、「Remote admin password」フィールドに管理パスワードを入力します。
12. トランザクションバッファの予約サイズを入力して、Enter キーを押します。
13. 「7. Proceed」を選択して、ミラー化されたファイルボリュームを追加します。
ミラーボリュームとアクティブボリュームとの同期がとれると、ミラーボリュームが読み取り専用でマウントされます。
注: ミラーの初期同期中に、アクティブサーバーに対して入出力動作を行うことはできません。
ミラーの作成中および作成後は、システムに「Mirror Creation」画面が表示されます。
14. ミラー状態を確認するには、「A」を選択します。
15. 代替 IP アドレスまたは管理者パスワードを編集するには、「1. Edit」を選択します。

警告しきい値の設定

トランザクションバッファとして予約した領域がいっぱいになり制限を超えると、ミラーは破損します。この画面では、警告が送信される使用率を設定できます。デフォルトの使用率は、70、80、および 90% です。

警告が送信される使用率のしきい値を設定するには、次の手順を実行します。

1. アクティブシステム上で、「Extensions」メニューから「Mirrors」を選択します。
2. 「3. Threshold Config」を選択します。
3. 「1. Edit」を選択して、この画面に表示される使用率を編集します。

4. 設定する使用率を入力します。
5. 「Alert Silent Period」フィールドで、システムが同じしきい値警告をふたたび送信するまで待機する時間数を入力します。
6. 「7. Proceed」を選択します。

ミラー化されたファイルボリュームのプロモート

アクティブシステムに障害が発生した場合に、ミラーシステムは高可用性を提供します。ミラー化されたファイルボリュームをネットワークユーザーが使用できるようにするには、ファイルボリュームをプロモートします。まず、アクティブファイルボリュームとミラー化されたファイルボリュームとの間のアクティブミラー接続を切断して、ミラーを切り離す必要があります。次に、ボリュームをプロモートし、ミラー化されたファイルボリュームのアクセス権を設定します。いったんミラーを切断してミラー化されたファイルボリュームをプロモートすると、2つのファイルボリュームは完全に独立した状態になります。

ミラーシステムでファイルボリュームをプロモートするには、次の手順を実行します。

1. ミラーシステム上で「Configuration」メニューから「Disks & Volumes」を選択し、ファイルボリュームの状態を表示します。

ミラー化ファイルボリュームの名前の後ろに表示される「*」（アスタリスク）は、そのファイルボリュームが現在ミラー化されていることを示します。

アクティブシステムが停止している場合のみ、ミラーシステムからミラー化ファイルボリュームを切断することをお勧めします。アクティブシステムが動作している場合にファイルボリュームをプロモートするには、ミラーシステムからではなく、アクティブシステムからミラーを切断してください。

2. 「Extensions」メニューから、「Mirrors」を選択します。
3. 切断するミラー化されたファイルボリュームに対応する文字を選択します。
4. 「8. Break」を選択します。
注: 可能な場合は、アクティブシステムからミラーを切断してください。
5. 切断を確認するプロンプトが表示されたら、「Y. Yes」を選択して次に進みます。
6. Esc キーを押して、「Mirrors」のメイン画面に戻ります。
7. 「Extensions」メニューから、「Mirrors」を選択します。
8. 「1. Promote Volume」を選択します。
9. プロモートするファイルボリュームに対応する文字を選択します。

10. 「7. Proceed」を選択して、ファイルボリュームをプロモートします。

この処理が完了するまでに数分かかる場合があります。ミラー化されたファイルボリュームをプロモートするには、少なくとも一度はそのボリュームが「In Sync」の状態になっている必要があります。
11. ファイルボリュームのプロモートが完了したら、Esc キーを押してメインメニューに戻ります。
12. (任意) NFS ファイルボリュームアクセスを構成するには、「Access Control」メニューから「Volume Access」を選択します。
13. ファイルボリュームに対応する文字を選択して、ファイルボリュームにアクセス権を設定します。
14. 「Read/write」、「Read only」、または「None」のいずれかを選択します。
15. 「7. Save changes」を選択して次に進みます。

ボリュームがプロモートされました。ミラーを再確立するには、次の節の、255 ページの「ミラーの再確立」を参照してください。

ミラーの再確立

ここでは、アクティブサーバーに障害が発生してミラーサーバー上のファイルボリュームをプロモートしたときに、ミラーを再確立する方法について説明します。プロモートしたファイルボリュームが最新のバージョンになり、アクティブシステム上の古いファイルボリュームから完全に独立して機能します。ミラーを再確立するには、最新のファイルボリュームをアクティブサーバーにミラー化し、そのファイルボリュームをミラーサーバーにミラー化して元の状態に戻す必要があります。

ミラー化されたファイルボリュームをプロモートしていない場合は、次の手順を実行しないでください。アクティブシステムがオンラインに戻ると、ミラーが自動的に「In Sync」の状態に戻されます。

次の例では、サーバー 1 がアクティブサーバー、サーバー 2 がミラーサーバーです。

ミラーを再確立するには、次の手順を実行します。

- サーバー 1 でミラーを切断
- サーバー 1 から古いファイルボリュームを削除
- サーバー 2 の最新のファイルボリュームをサーバー 1 にミラー化
- 役割の変更。サーバー 1 をふたたびアクティブにしてサーバー 2 をミラーサーバーに変更

アクティブサーバーは、オンラインになるときにミラーの再確立を試みる場合があります。そのため、サーバー 1 でミラーを切断する必要があります。

サーバー 1 でのミラーの切断

サーバー 1 でミラーを切断するには、次の手順を実行します。

1. サーバー 1 で、「Extensions」メニューから「Mirrors」を選択します。
2. ミラー化されたファイルボリュームに対応する文字を選択します。
3. 「8. Break」を選択します。
4. 「Y. Yes」を選択してミラーの切断を確認します。

サーバー 1 からの古いファイルボリュームの削除

サーバー 1 から古いファイルボリュームを削除するには、次の手順を実行します。

1. Esc キーを押して、メインメニューに戻ります。
2. 「Configuration」メニューから「Disks & Volumes」を選択します。
3. ミラー化されたファイルボリュームに対応する数字を選択します。

注意: 次の手順を実行する前に、削除しようとしているのはサーバー 1 の古いファイルボリュームであることを確認してください。また、サーバー 2 の最新のファイルボリュームを確認し、先にプロモートしておいてください。

4. 「8. Delete」を選択します。
5. 古いファイルボリュームのファイル名を入力します。
6. 「7. Proceed with delete」を選択して、古いファイルボリュームを削除します。



サーバー 2 の最新のファイルボリュームのサーバー 1 へのミラー化

サーバー 2 の最新のファイルボリュームをサーバー 1 にミラー化して戻すには、次の手順に従います。

1. サーバー 2 で、「Extensions」メニューから「Mirrors」を選択します。
2. 「8. Add mirror」を選択します。
3. ミラー化するファイルボリュームに対応する文字を選択します。
4. サーバー 1 のプライベートホスト名を入力します。
5. プライベート IP アドレスを入力し、必要に応じて管理者パスワードを入力します。

6. トランザクションバッファの予約サイズを入力します。
詳細は、252 ページの「ファイルボリュームのミラー化」を参照してください。
7. 「7. Proceed」を選択します。
8. ミラーの作成中、ミラー化された新しいファイルボリュームに対応する文字を選択します。
ミラーが「In Sync」の状態になると、サーバー 1 とサーバー 2 の両方にファイルボリュームの同一のコピーが存在するようになります。
これで、役割を変更できます。詳細は、257 ページの「役割の変更」を参照してください。

役割の変更

役割を変更するには、次の手順を実行します。

1. メインメニューから、サーバー 1 の「Mirror」オプションを選択します。
2. 該当する文字を押して、対象のボリュームを選択します。
3. たとえば、A キーを押して cvol1 ファイルボリュームを選択します。
4. 「Mirror Status」メニューから、「Change Role」オプションを選択します。
注: 役割を変更するには、あらかじめボリュームが 100% 同期した状態である必要があります。
5. 「Yes」を選択して確定します。

監視

コンソールを使用して監視機能を実行できます。次の各節では、監視機能の設定方法と使用方法について説明します。

- 258 ページの「SNMP の構成」
- 258 ページの「電子メール通知の構成」
- 259 ページの「システム情報の表示」

SNMP の構成

「SNMP」メニューでは、コミュニティ文字列、連絡先情報、および SNMP モニターの場所の変更だけでなく、遠隔の SNMP モニターにメッセージを送信できます。

SNMP を構成するには、次の手順を実行します。

1. 「Extensions」メニューから「SNMP Configuration」を選択します。
デフォルトのコミュニティ名は **public** です。任意の名前を入力できます。
2. トラップの宛先を追加、編集、または削除するには「1-5. Edit a Trap Destination」、コミュニティ文字列を編集するには「6. Edit Community」、連絡先情報を編集するには「7. Edit Contact」、遠隔 SNMP モニターの場所を編集するには「8. Edit Location」を選択します。
3. 「Y. Yes」を選択して、変更内容を保存します。

電子メール通知の構成

システムに問題が発生すると、Sun StorageTek 5320 NAS Appliance は特定の受信者に電子メールメッセージを送信します。

注: 電子メール通知が正しく機能するように DNS を構成してください。

電子メール通知を構成するには、次の手順を実行します。

1. 「Extensions」メニューから、「EMAIL Configuration」を選択します。
2. 「1. Edit fields」を選択します。
3. 各フィールドに必要な情報を入力します。フィールド間を移動するには **Enter** キーを押します。
 - **SMTP Server** — メールサーバー。すべてのメールがここに送信されます。ホストファイルまたは DOS サーバーに、このサーバー名が含まれている必要があります。
注: IP アドレスまたは名前を使用できます。名前の場合は、DNS サーバーが解釈処理できる名前を使用する必要があります。
 - **Recipient 1 ~ 4** — 問題の発生時に自動的に通知が送信される 4 人の受信者の電子メールアドレス。
 - **Notification Level** — 電子メールを使用して受信者に通知が送信される問題のレベル。次のいずれかを選択します。
Errors — エラーの発生時にのみ送信される通知。

Errors and warnings — エラーおよび優先順位が低い警告の発生時に送信される通知。

None — 通知は送信されません。

4. 現在の構成を保存するには、「7. Save Changes」を選択します。
5. Esc キーを押して、メインメニューに戻ります。

システム情報の表示

コンソールにシステム情報を表示できます。

サーバーの状態の表示

サーバーの状態を表示するには、次の手順を実行します。

1. 「Operations」メニューから「Activity Monitor」を選択します。
アクティビティモニターの画面には、次の情報が表示されます。
 - **Volume** — 最初の 22 個のファイルボリューム。
 - **Use%** — ボリューム上の使用済み容量。
 - **Reqs** — 直前の 10 秒間にボリュームに対して処理された要求の数。
 - **Device** — デバイス名。
 - **Load** — CPU の負荷 (%)。
 - **Peak** — 直前の 10 分間の 1 秒あたりの最大使用率。
 - **Client** — ユーザーの名前またはアドレス。
 - **Reqs** — 直前の 10 秒間にボリュームに対して処理された要求の数。
2. Esc キーを押して、メインメニューに戻ります。

システムログの表示

- システムログを表示するには、「Operations」メニューから「Show Log」を選択します。

ログには、次の 2 種類のエントリが表示されます。

- **システム起動時のログエントリ** — デバイスの構成、ボリューム、およびその他の関連情報
- **通常動作時のログエントリ** — デバイスのエラー、セキュリティの違反、およびルーティングの状態に関するその他の情報。リリース番号とソフトウェアのシリアル番号が最後に表示されます。

ポート結合の表示

ポート結合を表示するには、次の手順を実行します。

1. 「Configuration」メニューから「Host Name & Network」を選択します。
2. 次のページにスクロールするには、スペースバーを押します。
「bond1」列には、最初のポート結合が表示されます。この列に表示される入出力情報は、結合した2つのポートの入出力情報の合計を示します。

チェックポイント分析の表示

チェックポイント分析を表示するには、次の手順を実行します。

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. 構成するドライブに対応する文字を入力します。
3. 「Change/Delete volume name」を選択します。
4. 「6. Checkpoints」を選択します。
5. 「3. Analysis」を選択します。分析をスクロールして表示するには、スペースバーを使用します。
6. 「0. End Analysis」を選択して、この画面を終了します。

ミラー化ファイルボリュームの状態の表示

ミラー化ファイルボリュームの状態を表示するには、次の手順を実行します。

1. アクティブシステム上で、「Extensions」メニューから「Mirrors」を選択します。
2. ミラー化されたファイルボリュームを選択します。
状態画面は、次の3つのセクションに分かれています。
 - 最初の行には、ファイルボリューム名、ミラーの状態、進捗インジケータ、状態メッセージなどのミラー状態に関連する情報が表示されます。ミラーの状態には、次の10種類があります。
 - ERR — エラーが発生しました。
 - NEW — 新しいミラーを作成しています。
 - INIT — ミラーバッファを初期化しています。
 - MKPT — ミラーシステムでディスクパーティションを作成しています。
 - RDY — システムの準備が完了して、ほかのシステムの準備完了を待機しています。
 - DOWN — ネットワークリンクが停止しています。

- CRK — ミラーが破損しています。
- RPL — 複製段階が実行されています。
- OOS — ミラーは同期がとれていません。
- SYNC — ミラーは同期がとれています。

進捗インジケータによって、各状態の動作の進捗率が示されます。また、状態メッセージにも、ミラーの状態を示す短いテキストメッセージが表示されます。

- 2 番目の行には、トランザクションバッファの予約領域の状況が表示されます。ここに表示されるのは、バッファが保持できるトランザクションの最大数、次のトランザクション ID、同期トランザクション ID、本体トランザクション ID、およびアクティブシステムとミラーシステム間の同期状態を示す In Sync 率のインジケータです。

アクティブシステムでは、次の情報が表示されます。

- next xid (次のトランザクション ID) は、ファイルシステムの次のトランザクションを示します。
- sync xid (同期トランザクション ID) は、ミラーシステムに最後に転送されたトランザクションを示します。
- head xid (本体トランザクション ID) は、ミラーシステムで最後に確認されたトランザクションを示します。
- In Sync 率のインジケータが 100% になると、ミラーシステムはアクティブシステムを完全にコピーしたことになります。In Sync 率のインジケータが 0% を示す場合は、ミラーが破損しており、アクティブサーバーは自動的にブロック単位の再同期処理を実行します。ミラーの状態が「Out Of Sync」の間、ふたたびミラーの同期がとれるまで、ミラーボリュームは揮発性になります。

ミラーシステムでは、次の情報が表示されます。

- next xid (次のトランザクション ID) は、アクティブシステムから予想される次のトランザクションを示します。
- sync xid (同期トランザクション ID) は、ディスクへの書き込みが予定されていた、最後のトランザクションを示します。
- head xid (本体トランザクション ID) は、ディスクで最後に確認されたトランザクションを示します。
- In Sync 率のインジケータが 100% になると、すべてのミラートランザクションがディスクに書き込まれたことになり、ミラーシステムのボリュームはアクティブシステムのボリュームの完全なコピーになります。

3. 代替 IP アドレスまたは管理者パスワードを編集するには、「1. Edit」を選択します。
4. フィールドを編集してから「7. Proceed」を選択し、変更を保存します。
5. ミラー化されたファイルボリュームのネットワーク統計情報を参照するには、「2. Statistics」を選択します。

画面には、アクティブファイルボリュームに送信されるトランザクション数 (IN) や、アクティブシステムからミラー化されたファイルボリュームに送信されるトランザクション数 (OUT) などの、アクティブシステムの統計情報が表示されます。画面には、それぞれの 1 秒あたりトランザクション数 (t/s) の、平均値、最小値、および最大値が表示されます。

システムは、流入速度とともに、トランザクションバッファの予約領域 (Buffer) の残量を示します。流入速度が 0 より大きい場合は、すべてのネットワーク接続が正常に機能していることを確認する必要があります。この場合、アクティブシステムへのトランザクションの送信速度がミラーシステムへの送信速度を上回っているため、バッファがいっぱいになります。バッファが制限を超えると、ミラーは破損します。

すべてのミラー化ファイルボリュームのネットワーク統計情報の表示

すべてのミラー化ファイルボリュームのネットワーク統計情報を表示するには、次の手順を実行します。

1. アクティブシステム上で、「Extensions」メニューから「Mirrors」を選択します。
2. 「2. Network Statistics」を選択します。

画面には、平均応答時間および転送速度のほか、送信された RCB (要求制御ブロック) の合計数、1 秒あたりの送信 RCB 数、および RCB の平均サイズが表示されます。

3. 「1. Reset」を選択し、この画面を再起動します。

システムの保守

一部のシステム保守および設定機能は、コンソールからのみ実行できます。これには次の機能が含まれます。

- 263 ページの「ファイル転送プロトコル (FTP) アクセスの構成」
- 264 ページの「RAID コントローラの管理」
- 266 ページの「ファイルシステムのマウント」

その他の作業は、Web Administrator だけでなく、管理者コンソールからも実行できます。

- 266 ページの「システムの停止」
- 267 ページの「LUN フェイルオーバーの管理」

- 268 ページの「LUN パスの構成」
- 269 ページの「ファイルのチェックポイントのスケジュール設定」
- 269 ページの「NDMP バックアップの構成」
- 270 ページの「Compliance Archiving Software の構成」
- 271 ページの「システム監査の構成」

ファイル転送プロトコル (FTP) アクセスの構成

FTP は、クライアントとサーバー間でファイルをコピーするために使用されるインターネットプロトコルです。FTP では、サーバーへのアクセスを要求する各クライアントを、ユーザー名およびパスワードで識別する必要があります。

ユーザーのタイプ

次の 3 つのタイプのユーザーを設定できます。

- **管理者** – admin というユーザー名を持ち、GUI クライアントと同じパスワードを使用します。
管理者は、システム上のすべてのボリューム、ディレクトリ、およびファイルにスーパーユーザーでアクセスできます。管理者のホームディレクトリは「/」と定義されます。
- **ユーザー** – ローカルのパスワードファイルか、遠隔の NIS または NIS+ ネームサーバーに指定されているユーザー名およびパスワードを持ちます。
ユーザーは、自身のホームディレクトリに含まれるすべての既存のディレクトリおよびファイルへのアクセス権を持ちます。ホームディレクトリは、ユーザーのアカウント情報の一部として定義され、ネームサービスによって取得されます。
- **ゲスト** – ユーザー名 ftp またはそのエイリアス anonymous でログインします。パスワードが要求されますが、認証されません。すべてのゲストユーザーは、ftp ユーザーのホームディレクトリに含まれるすべてのディレクトリおよびファイルへのアクセス権を持ちます。
注: ゲストユーザーは、ファイルの名前の変更、上書き、または削除を行うことができません。また、ディレクトリの作成または削除、および既存のファイルまたはディレクトリのアクセス権の変更を行うこともできません。

FTP アクセスの設定

FTP アクセスを設定するには、次の手順を実行します。

1. 「Extensions」メニューから「FTP Configuration」を選択します。

2. 「1. Edit Fields」を選択します。
3. FTP を使用可能にするには「Y. Yes」、使用不可にするには「N. No」を選択します。

FTP サービスを使用可能に設定すると、FTP サーバーは受信した接続要求を受け入れます。
4. 「Allow guest access」で、「Yes」を選択して匿名ユーザーによる FTP サーバーへのアクセスを許可するか、「No」を選択して禁止します。
5. 「Allow user access」で、「Yes」を選択してすべてのユーザーによる FTP サーバーへのアクセスを許可するか、「No」を選択して禁止します。

これには、admin ユーザーまたはスーパーユーザーは含まれません。

注: ローカルのパスワードファイルまたは遠隔 NIS/NIS+ ネームサーバーでは、ユーザー名およびパスワードが指定されている必要があります。
6. 「Allow admin access」で、「Yes」を選択して Sun StorageTek 5320 NAS Appliance の管理パスワードでの、スーパーユーザーとしてのアクセスを許可するか、「No」を選択してアクセスを禁止します。管理パスワードの使用には注意が必要です。

注: 「スーパー」ユーザーとは、UID が 0 に設定されているユーザー、および Sun StorageTek 5320 NAS Appliance の特別なユーザーである「admin」を示します。
7. 「Enable logging」で、「Yes」を選択してログを使用可能にするか、「No」を選択して使用不可にします。
8. ログを使用可能にする場合は、「Log filename」にログファイル名を指定します。
9. 「7. Save changes」を選択します。

RAID コントローラの管理

raidctl コマンドを使用すると、CLI から RAID コントローラを管理できます。

いずれの raidctl コマンドを使用する場合でも、220 ページの「管理者コンソールのコマンド行インタフェースへのアクセス」の手順を実行してください。

注意: 予期しない結果を回避するため、コマンドは注意して使用してください。



サブコマンドでのヘルプの表示

サブコマンドでヘルプを表示するには、コマンド行で「**raidctl help**」と入力してください。

LED の制御

LED を制御するには、次の手順を実行します。

1. トレーのすべての LED を点滅させるには、次のように入力します。

```
raidctl locate type=lsi target=tray ctrl=0..n tray=0..n
```

2. 指定したドライブの LED を点滅させるには、次のように入力します。

```
raidctl locate type=lsi target=drive ctrl=0..n tray=0..n  
slot=1..n
```

3. 指定したコントローラの LED の点滅をやめるには、次のように入力します。

```
raidctl locate type=lsi action=stop ctrl=0..n
```

イベントおよび構成情報の取得

イベントおよび構成情報を取得するには、次の手順を実行します。

1. 指定したコントローラのすべてのイベントを取得するには、次のように入力します。

```
raidctl get type=lsi target=events ctrl=0..n
```

すべてのイベントのログが /cvol/log/2882ae.log ファイルに書き込まれます。ファイルがすでに存在する場合は、そのファイルを上書きするか、新しいファイル名を指定するか、または操作をキャンセルするかを確認するプロンプトが表示されます。

2. 指定したコントローラの重大イベントを取得するには、次のように入力します。

```
raidctl get type=lsi target=events ctrl=0..n etype=critical
```

重大イベントのログが /cvol/log/2882ce.log ファイルに書き込まれます。ファイルがすでに存在する場合は、そのファイルを上書きするか、新しいファイル名を指定するか、または操作をキャンセルするかを確認するプロンプトが表示されます。

3. 指定したコントローラの構成情報を取得するには、次のように入力します。

```
raidctl get type=lsi target=profile ctrl=0..n
```

コントローラの時刻とバッテリーの有効期限の設定

コントローラの時刻とバッテリーの有効期限を設定するには、次の手順を実行します。

1. 指定したコントローラのバッテリーの有効期限をリセットするには、次のように入力します。

```
raidctl set type=lsi target=battery-age ctrl=0..n
```

2. コントローラの時刻をサーバーの時刻と同期化させるには、次のコマンドを使用します。

```
raidctl set type=lsi target=ctrl_time-age ctrl=0..n
```

ファームウェアのダウンロード

ファームウェアをダウンロードするには、**raidctl download** コマンドを使用します。

注: ファームウェアのアップグレードの手順については、第 11 章を参照してください。

ファイルシステムのマウント

再起動を連続して複数回行うと、1 つ以上のファイルシステムのマウントが解除されることがあります。ファイルシステムをマウントするには、次のコマンドを実行します。

```
mount -f volume-name
```

システムの停止

Sun StorageTek 5320 NAS Appliance システムは連続稼働できるように設計されていますが、システムを停止する必要がある場合は、必ず **Web Administrator**、コンソール、または **LCD パネル** で停止してください。

システムを停止するには、次の手順を実行します。

1. 「Operations」メニューから「Shutdown」を選択します。
2. 該当する文字を入力して、必要なオプションを選択します。
 - **R. Reboot** — システムを再起動するには「R」と入力します。
 - **H. Halt** — システムを停止するには「H」と入力します。
 - **P. Boot Previous Version 4.x.xx.xxx** — 使用可能な以前のバージョンの OS を使用してシステムを再起動するには「P」と入力します。このオプションは、複数のバージョンの OS がインストールされているシステム上で使用できます。
 - **ESC** — 操作を取り消してメインメニューに戻るには、Esc キーを押します。

再起動、停止、または以前のバージョンの OS を使用した起動を選択すると、ディスクへのすべての遅延書き込みが完了したあとで、サーバーが再起動または停止します。

LUN フェイルオーバーの管理

2 台の本体のうちのいずれかの信頼性が失われ、その制御下にあるすべての LUN を安定している本体に移行する必要がある場合に、フェイルオーバーが発生します。「Failover」メニューでは、回復可能なエラーが発生したときのディスクリソースを管理します。

フェイルオーバーの構成

フェイルオーバーを構成するには、次の手順を実行します。

1. 「Extensions」メニューから「Failover/Move LUNs」を選択します。

注: 「Failover/Move LUNs」はクラスタ構成でのみ使用可能です。本体 1 台構成のシステムでは、LUN のフェイルオーバーを使用可能または使用不可に切り替えることはできません。
2. 「3. Edit Failover」が使用可能な場合は、このオプションを選択します。
3. 「Y. Yes」を選択して、本体のフェイルオーバーを使用可能にします。
4. クラスタ構成の Sun StorageTek 5320 NAS Cluster Appliance または Sun StorageTek 5320 NAS Gateway システムを使用する場合は、次の手順を実行します。
 - 「Y. Yes」を選択して、リンクのフェイルオーバーを使用可能にします。リンクのフェイルオーバーでは、一次リンクに障害が発生すると、代替ネットワークリンクがアクティブになります。
 - 1 つのネットワークリンクで信頼性が低下した場合に、リンクのフェイルオーバーが実行されるまでの時間を秒単位で入力します。
 - 信頼性が低下したリンクが修復または再接続される場合に、リンクが復元されるまでの時間を秒単位で入力します。
5. Sun StorageTek 5320 NAS Cluster Appliance または Sun StorageTek 5320 NAS Gateway システムクラスタ構成ユーザーの場合は、「2. Modify」を選択して、LUN の所有権をアダプタ別に並べ替えます。復元処理が実行される際に、ここで指定したように構成されます。
 - 各アダプタが所有する LUN を入力します。
 - 空白 1 文字で数字を区切ります (例: 0 2 8 10)。
 - Enter キーを押します。
6. 「Y. Yes」を選択して、変更内容を保存します。

システムの復元およびフェイルバックの開始

システムを復元して、フェイルバックを開始するには、次の手順を実行します。

1. 障害の発生したコンポーネントを交換または修復して、オンラインになっていることを確認します。
2. 「Extensions」メニューから「Failover/Move LUNs」を選択します。
注:「Failover/Move LUNs」はクラスタ構成でのみ使用可能です。本体 1 台構成のシステムでは、LUN のフェイルオーバーを使用可能または使用不可に切り替えることはできません。
3. 「1. Restore」を選択します。
4. 「Y. Yes」を選択して、復元処理を続けます。

LUN パスの構成

LUN パスと、LUN パス設定時の GUI の使用法の詳細は、15 ページの「LUN パスの設定について」を参照してください。

LUN パスを編集するには、次の手順を実行します。

1. 「Extensions」メニューで、「LUN Ownership」オプションが表示されるまでスペースバーを押し、「LUN Ownership」オプションを選択します。
「LUN Ownership」画面に、パスの変更が可能なすべての LUN が表示されません。LUN にファイルシステムが存在しない場合にのみ、LUN を割り当て直すことができます。クラスタ構成の Sun StorageTek 5320 NAS Cluster Appliance または Sun StorageTek 5320 NAS Gateway システムでは、LUN を「所有する」本体のみが、その LUN をもう 1 台の本体に割り当て直すことができます。
注: クラスタ構成の Sun StorageTek 5320 NAS Cluster Appliance または Sun StorageTek 5320 NAS Gateway システムでは、はじめてシステムを起動したときに、すべての LUN が 1 台の本体 (本体 1) に割り当てられます。LUN を均等に振り分けるために、本体 1 を使用して、一部の LUN を本体 2 に割り当て直す必要があります。
注: 「LUN Ownership」画面には、最初に、LUN パスが割り当てられていない LUN が何度も表示されることがあります。これは、複数のパスを介した複数のコントローラによってそれらの存在が通知されるためです。いったん LUN パスが割り当てられると、現在のパスの LUN が一度だけ表示されます。
2. 選択するパスの左側に表示されている文字を入力して、LUN パスを選択します。
3. 「1. Edit」を選択して、LUN パスを編集します。
「Configure LUN Path」画面では、LUN に使用できるすべてのパスが表示されません。現在の LUN パスまたはアクティブな LUN パスには、「Active」と表示されます。LUN にプライマリパスが設定されている場合は、「PRIMARY」と表示されます。
4. 変更する LUN パスの番号を入力して、Enter キーを押します。

LUN の割り当てを、2 つの使用可能なパスに均等に振り分けます。たとえば、1 つめと 3 つめの LUN をパス 1 に、2 つめと 4 つめの LUN をパス 2 に振り分けます。

5. 「Y. Yes」を選択して、変更内容を保存します。

ファイルのチェックポイントのスケジュール設定

チェックポイントは、一次ファイルボリュームの読み取り専用の仮想コピーです。チェックポイントの詳細は、165 ページの「ファイルのチェックポイントについて」を参照してください。

チェックポイントのスケジュールを作成するには、次の手順を実行します。

1. 「Configuration」メニューから「Disks & Volumes」を選択します。
2. チェックポイントのスケジュールを設定するドライブを選択します。
注: ドライブ (ディスクボリューム) の数が 26 個を超える場合は、スペースバーを押して探します。
3. 「1. Edit」を選択します。
4. 「6. Checkpoints」を選択します。
5. Enter キーを押してフィールド間を移動し、画面の下部に表示されるプロンプトに従います。
6. すべてのチェックポイント情報を入力したら、「7. Save changes」を選択します。

NDMP バックアップの構成

システムボリュームをバックアップするには、まずバックアップジョブを追加し、次にそれをスケジュール設定するか、実行する必要があります。手順を開始する前に、バックアップデバイスがオンラインになっていることを確認してください。

注: Network Data Management Protocol (NDMP) によってバックアップされるボリュームでは、チェックポイントを使用可能にしてください。詳細は、165 ページの「ファイルのチェックポイントについて」を参照してください。

NDMP を設定するには、次の手順を実行します。

1. 「Extensions」メニューから「NDMP Setup」を選択します。
2. バックアップテープドライブへのデータ転送に使用する NIC ポートを選択して、Enter キーを押します。

このフィールドの下に、使用可能なすべてのポートが表示されます。

3. NDMP ログおよびデータファイルの保存に使用する 2G バイト以上のスペアボリュームのパス、たとえば `/vol_ndmp` を選択します。

バックアップのスケジュール設定されているボリュームではなく、まったく別のファイルボリュームを使用することをお勧めします。

4. 変更を保存します。

Compliance Archiving Software の構成

Compliance Archiving Software オプションを購入し、起動して使用可能にした場合 (125 ページの「システムのオプションの起動」を参照)、コマンド行インタフェースを使用して追加設定を確立できます。

注: Sun StorageTek 5320 NAS Gateway システムの構成では、推奨実施の規制適合はサポートされていますが、必須実施の規制適合はサポートされていません。

注意: 予期しない結果を回避するため、コマンドは注意して使用してください。



デフォルトの保持期間の変更

デフォルトの保持期間を変更するには、次の手順を実行します。

1. 220 ページの「管理者コンソールのコマンド行インタフェースへのアクセス」の手順を実行します。
2. コマンド行で `fsctl compliance volume drt time` と入力します。

volume にはデフォルトの保持期間を設定するボリューム名を指定し、*time* にはデフォルトの保持期間を秒単位で指定します。

デフォルトの保持期間を「永続的」に設定するには、最大許容値である 2147483647 を使用することをお勧めします。

CIFS 規制適合の使用可能への切り替え

Compliance Archiving Software の初期構成では、NFS クライアントからのデータ保持要求のみがサポートされます。共通インターネットファイルシステム (CIFS) からのこの機能へのアクセスは、コマンド行インタフェースを使用して使用可能にできません。

注意: 予期しない結果を回避するため、コマンドは注意して使用してください。

Windows クライアントが規制適合アーカイブ機能を使用できるようにするには、次の手順を実行します。



1. 220 ページの「管理者コンソールのコマンド行インタフェースへのアクセス」の手順を実行します。
2. コマンド行で **fsctl compliance wte on** と入力します。

システム監査の構成

システム監査は、システムイベントのレコードをログファイルに格納して、管理者が特定のシステムイベントを監査できるようにするサービスです。システム監査の詳細は、151 ページの「システム監査について」を参照してください。

システム監査を構成するには、次の手順を実行します。

1. 「Extensions」メニューから「System Audit Configuration」を選択します。
2. 「1. Edit fields」を選択します。
3. 監査を使用可能にして、監査ログのパスとログファイルの最大サイズを指定します。
4. 「7. Save changes」を選択して変更内容を保存します。

Sun StorageTek 5320 NAS Appliance エラーメッセージ

この付録では、Sun StorageTek 5320 NAS Appliance システムの各種コンポーネントによって生成されるエラーメッセージについて説明します。この付録は、次の節で構成されています。

- 273 ページの「Sun StorageTek 5320 NAS Appliance のエラーメッセージについて」
 - 274 ページの「SysMon エラー通知について」
 - 274 ページの「リファレンス: UPS サブシステムエラー」
 - 276 ページの「リファレンス: ファイルシステムエラー」
 - 277 ページの「リファレンス: RAID エラー」
 - 277 ページの「リファレンス: IPMI イベント」
-

Sun StorageTek 5320 NAS Appliance のエラーメッセージについて

この付録では、システムエラー発生時に管理者に通知するために、電子メール、SNMP (ネットワーク管理プロトコル) 通知、液晶ディスプレイ (LCD) パネル、およびシステムログを介して送信される特定のエラーメッセージについて説明します。Sun StorageTek 5320 NAS Appliance ソフトウェアの監視スレッド *SysMon* で、RAID (Redundant Array of Independent Disks) デバイス、無停電電源装置 (UPS)、ファイルシステム、本体装置、格納装置サブシステム、および環境変数の状態が監視されます。監視およびエラーメッセージは、モデルおよび構成によって異なります。

注: この付録の表の列に、エントリがない場合は、そのエントリが削除されたことを示します。

SysMon エラー通知について

Sun StorageTek 5320 NAS Appliance の監視スレッド SysMon では、サブシステムのエラーによって生成されたイベントが取得されます。次に、電子メールの送信、SNMP (ネットワーク管理プロトコル) サーバーへの通知、液晶ディスプレイ (LCD) パネルでのエラーの表示、またはシステムログへのエラーメッセージの書き込みのうち、適切な処理が実行されます。これらの処理のいくつかが同時に実行される場合もあります。電子メール通知およびシステムログには、イベントの発生時刻も示されます。

リファレンス: UPS サブシステムエラー

表 B-1 に、無停電電源装置 (UPS) のエラー状態を示します。

表 B-1 UPS エラーメッセージ

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
電源障害	AC Power Failure: AC power failure.System is running on UPS battery. Action: Restore system power. Severity = Error	EnvUpsOn Battery	U20 on battery	UPS: AC power failure.System is running on UPS battery.
電源の復旧	AC power restored: AC power restored.System is running on AC power. Severity = Notice	EnvUpsOff Battery	U21 power restored	UPS: AC power restored.
バッテリー低下	UPS battery low: UPS battery is low.The system will shut down if AC power is not restored soon. Action: Restore AC power as soon as possible. Severity = Critical	EnvUpsLow Battery	U22 low battery	UPS: Low battery condition.
バッテリー充電完了	UPS battery recharged: The UPS battery has been recharged. Severity = Notice	EnvUps Normal Battery	U22 battery normal	UPS: Battery recharged to normal condition.

表 B-1 UPS エラーメッセージ (続き)

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
バッテリー交換	Replace UPS Battery: The UPS battery is faulty. Action: Replace the battery. Severity = Notice	EnvUps Replace Battery	U23 battery fault	UPS: Battery requires replacement.
UPS アラーム (周辺温度または 湿度が正常なし きい値の範囲外)	UPS abnormal temperature/humidity: Abnormal temperature/humidity detected in the system. Action: 1. Check UPS unit installation, OR 2. Contact technical support. Severity = Error	EnvUps Abnormal	U24 abnormal ambient	UPS: Abnormal temperature and/or humidity detected.
ライトバック キャッシュが 使用不可	Controller Cache Disabled: Either AC power or UPS is not charged completely. Action: 1 - If AC power has failed, restore system power.2 - If after a long time UPS is not charged completely, check UPS. Severity = Warning		Cache Disabled	write-back cache for ctrl <i>x</i> disabled
ライトバック キャッシュが 使用可能	Controller Cache Enabled: System AC power and UPS are reliable again. Write-back cache is enabled. Severity = Notice		Cache Enabled	write-back cache for ctrl <i>n</i> enabled
UPS の停止	UPS shutdown: The system is being shut down because there is no AC power and the UPS battery is depleted. Severity = Critical			!UPS: Shutting down
UPS 障害	UPS failure: Communication with the UPS unit has failed. Action: 1. Check the serial cable connecting the UPS unit to one of the CPU enclosures, OR 2. Check the UPS unit and replace if necessary. Severity = Critical	EnvUpsFail	U25 UPS failure	UPS: Communication failure.

リファレンス: ファイルシステムエラー

表 B-2 に、ファイルシステム使用量が定義された使用量しきい値を超えた場合に生成される、ファイルシステムのエラーメッセージを示します。使用量のデフォルトのしきい値は 95% です。

表 B-2 ファイルシステムエラー

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
ファイル システムの 空き領域不足	File system full: File system <name> is xx% full. Action: 1. Delete any unused or temporary files, OR 2. Extend the partition by using an unused partition, OR 3. Add additional disk drives and extend the partition after creating a new partition. (Severity=Error)	PartitionFull	F40 FileSystemName full	File system <name> usage capacity is xx%.

リファレンス: RAID エラー

表 B-3 に、RAID サブシステムのイベントおよびエラーメッセージを示します。

表 B-3 RAID エラーメッセージ

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
LUN 障害	RAID LUN failure: RAID LUN <i>N</i> failed and was taken offline.Slot <i>n</i> is offline. Action: Replace bad drives and restore data from backup. Severity = Error	RaidLunFail	R10 Lun failure	RAID LUN <i>N</i> failed and was taken offline.Slot <i>n</i> is offline. (Severity=Error)
ディスク 障害	Disk drive failure: Disk drive failure.Failed drives are: Slot no., Vendor, Product ID, Size Severity = Error	RaidDiskFail	R11 Drive failure	Disk drive failure.Failed drives are: Slot#, Vendor, Product ID, Size (Severity=Error)
コント ローラ 障害	RAID controller failure: RAID controller <i>N</i> has failed. Action: Contact technical support. Severity = Error	RaidController Fail	R12 Ctlr failure	RAID controller <i>N</i> failed.

リファレンス: IPMI イベント

Sun StorageTek 5320 NAS Appliance ソフトウェアは、環境システムの監視と、電源装置および温度の異常に関するメッセージの送信を実行する Intelligent Platform Management Interface (IPMI) ボードを搭載しています。

注: デバイスの場所については、付録 D を参照してください。

表 B-4 に、Sun StorageTek 5320 NAS Appliance ソフトウェアの IPMI エラーメッセージを示します。

表 B-4 IPMI のエラーメッセージ

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
ファン エラー	<p>Fan Failure: Blower fan xx has failed.Fan speed = xx RPM.</p> <p>Action: The fan must be replaced as soon as possible.If the temperature begins to rise, the situation could become critical. Severity = Error</p>	envFanFail trap	P11 Fan xx failed	Blower fan xx has failed!
電源 モジュール の障害	<p>Power supply failure: The power supply unit xx has failed.</p> <p>Action: The power supply unit must be replaced as soon as possible. Severity = Error</p>	envPowerFail trap	P12 Power xx failed	Power supply unit xx has failed.
電源 モジュール の温度	<p>Power supply temperature critical: The power supply unit xx is overheating.</p> <p>Action: Replace the power supply to avoid any permanent damage. Severity = Critical</p>	envPowerTemp Critical trap	P22 Power xx overheated	Power supply unit xx is overheating.

表 B-4 IPMI のエラーメッセージ (続き)

イベント	電子メールの件名: 本文	SNMP トラップ	LCD パネル	ログ
温度エラー	<p>Temperature critical: Temperature in the system is critical.It is xxx Degrees Celsius.</p> <p>Action: 1. Check for any fan failures, OR 2. Check for blockage of the ventilation, OR 3. Move the system to a cooler place.</p> <p>Severity = Error</p>	envTemperatue Error trap	P51 Temp error	The temperature is critical.
主電源 コードの 障害	<p>Power cord failure: The primary power cord has failed or been disconnected.</p> <p>Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord.</p> <p>Severity = Error</p>	envPrimary PowerFail trap	P31 Fail PWR cord 1	The primary power cord has failed.
副電源 コードの 障害	<p>Power cord failure: The secondary power cord has failed or been disconnected.</p> <p>Action: 1. Check the power cord connections at both ends, OR 2. Replace the power cord.</p> <p>Severity = Error</p>	envSecondary PowerFail trap	P32 Fail PWR cord 2	The secondary power cord has failed.

Compliance Archiving Software API

ライセンスキーを使用して「Compliance Archiving Software」と呼ばれるソフトウェア拡張機能を有効にすると、Sun StorageTek 5320 NAS Appliance 製品で規制適合対応のデータストレージがサポートされるようになります。

Compliance Archiving Software は、「必須実施」と呼ばれる厳しい形式、および「推奨実施」と呼ばれる「必須実施」よりは厳しくない形式で使用できます。Compliance Archiving Software の概要は、140 ページの「Compliance Archiving Software について」を参照してください。

この付録では、厳密な Compliance Archiving Software の機能およびプログラミングインタフェースの技術的な概要について説明します。この付録は、次の節で構成されています。

- 282 ページの「規制適合機能」
- 283 ページの「規制適合機能の使用」
- 287 ページの「UNIX システムコールの動作」
- 290 ページの「Windows クライアントの動作」
- 291 ページの「その他の API」

注: Compliance Archiving Software を適切に動作させるには、Sun StorageTek 5320 NAS Appliance システムのハードウェアが物理的に正しく構成されている必要があります。特に、Sun StorEdge 5300 RAID 拡張ユニットアレイを、NAS 本体および任意の Sun StorEdge 5300 拡張ユニット拡張格納装置へのプライベートファイバチャネル接続以外のデバイスまたはネットワークには接続しないことをお勧めします。

注: できるかぎり強力なデータ保持方針を確実に実施するには、使用している Sun StorageTek 5320 NAS Appliance システムに物理的なセキュリティも追加することをお勧めします。ソフトウェア制御によるデータ保持よりも、物理的な保護手段を使用してシステムのハードウェアへのアクセスを制御する方が強力です。

規制適合機能

Compliance Archiving Software は、ファイルの精度、完全性、および保持をストレージレベルで保証します。次に続く節では、次の 3 つの主要機能について説明します。

- 282 ページの「WORM ファイル」
- 282 ページの「ファイル別保持期間」
- 282 ページの「管理ロックダウン」

WORM ファイル

WORM ファイルは、NFS や CIFS プロトコルによって提供される従来のファイルアクセスの定義よりも強力なアクセス制御を実現します。アプリケーションによってファイルが WORM に指定されると、そのファイルは永続的に不変となります。操作を試みるクライアントまたはユーザーの識別情報または特権にかかわらず、WORM ファイルの変更、拡張、または名前の変更はできません。また、WORM ファイルは、次に説明するファイルの保持規則に準拠している場合にのみ削除できます。

注: これらのファイルは、再書き込みおよび再消去ができないストレージを指す業界用語に合わせて「WORM」と呼んでいますが、「常時読み取り専用」と呼ぶ方がよりの確です。Sun StorageTek 5320 NAS Appliance では、ファイルが WORM ファイルに変換されるまでは、ファイルの書き込み方法または内容を変更できる回数に制限はありません。

ファイル別保持期間

Compliance Archiving Software では、WORM ファイルごとに保持期間が関連付けられます。WORM ファイルは保持期間が期限切れになるまで削除できません。保持期間は延長できますが、短縮することはできません。保持期間が期限切れになったファイルには、新しい保持期間を割り当てることができます。

管理ロックダウン

WORM ファイルおよび保持期間の保持および保護を確実に保証するため、規制適合対応のファイルシステムボリュームでは、ファイルボリュームの削除、編集などの特定のシステム管理機能が使用不可になるか、または制限されます。これらの制限は、ファイルの保持を避けるために使用されるシステムの管理機能 (ファイルボリュームの削除など) に影響します。

規制適合機能の使用

Compliance Archiving Software の機能は、既存のクライアントのオペレーティングシステムおよびアプリケーションとの互換性を維持するため、Sun StorageTek 5320 NAS Appliance がサポートする既存のファイルアクセスプロトコル (NFS および CIFS) の拡張機能として実装されています。つまり、Sun StorageTek 5320 NAS Appliance は、既存のファイル属性を多重定義して、ファイルの WORM 状態および保持期間の終了を示します。これにより、標準のクライアント API およびユーティリティーを使用してメタデータフィールドを設定および参照できるため、既存の文書およびレコード管理アプリケーションの移植が容易になります。

規制適合対応のボリューム

ボリュームは、作成時に規制適合対応に指定する必要があります。既存のボリュームを規制適合対応のボリュームに変換することはできません。1 台の Sun StorageTek 5320 NAS Appliance には複数のボリュームを構成できますが、一部のボリュームのみが規制適合対応になります。

Compliance Archiving Software によって実施される、さまざまなデータ保持の定義を認識しないアプリケーションおよびユーザーが使用するボリュームでは、規制適合アーカイブ機能を使用可能にしないでください。

WORM ファイル

WORM ファイルは、変更または更新できません。いったん WORM ファイルになると、削除されるまで読み取り専用となります。

WORM ファイルの作成

Compliance Archiving Software は、WORM トリガーを使用して通常のファイルを WORM ファイルに変換します。クライアントのアプリケーションまたはユーザーがファイル上でトリガー動作を実行すると、Compliance Archiving Software は、ターゲットファイルが WORM ファイルに変換される必要があると解釈します。

UNIX クライアントの WORM トリガーでは、ファイルのアクセスモードが 4000 に設定されます。クライアントアプリケーションまたはユーザーは、`chmod` コマンドまたはシステムコールを使用してこの WORM トリガーを起動できます。この要求を受信すると、Compliance Archiving Software は、次の処理を実行して、ターゲットファイルを WORM ファイルに変換します。

- **setuid** ビットの設定
- ファイルに設定されているすべての書き込みビットのクリア
- ファイル上のすべての読み取りアクセスビットの維持

注: 実行可能ファイルは **WORM** ファイルに変換できません。Windows クライアントで作成されたファイルでは、これは、ファイルに実行権を付与するアクセス制御エントリ (**ACE**) がアクセス制御リスト (**ACL**) に存在する場合、そのファイルを **WORM** ファイルに変換できないことを意味します。

次の例では、アクセスモードが **640** のファイルを **WORM** ファイルに変換します。**WORM** トリガーが実行されると、ファイルのアクセスモードは **4440** になります。

```
$ ls -l testfile
-rw-r----- 1 smith  staff      12139 Dec  2 13:18 testfile
$ chmod 4000 testfile
$ ls -l testfile
-r-Sr----- 1 smith  staff      12139 Dec  2 13:18 testfile
```

この **WORM** トリガーは既存のアプリケーションによって使用される可能性が低い操作であるため、**Compliance Archiving Software** によって使用されます。

Windows クライアントの **WORM** トリガーでは、読み取り専用ビットおよびシステムビットの両方がファイルに設定されます。ファイルにアーカイブも隠しビットも設定されていない場合は、これらのビットが設定されたときのみ、**WORM** がトリガーされます。**WORM** トリガーによってファイルの読み取り専用ビットは設定されますが、システムビットは変更されません。

WORM ファイルに変換されたファイルは、元に戻すことはできません。Windows クライアントからは、読み取り専用ビットのクリア、およびシステムビットの変更はできません。**UNIX** クライアントからは、**setuid** ビットのクリア、およびファイルのアクセスモードへの実行権または書き込み権の追加ができません。

これらの **WORM** 設定は、規制適合対応のボリュームによって **CIFS** と **NFS** 間で変換されます。たとえば、Windows クライアントで作成された **WORM** ファイルを **UNIX** クライアントが参照すると、**WORM** のアクセスモードは前述のようになります。

WORM ファイルの動作

WORM ファイルは変更、上書き、または拡張できません。クライアントユーザーの識別情報およびアクセス権にかかわらず、**WORM** ファイルへの書き込みはすべて失敗してエラーが返されます。

WORM ファイルの所有者や管理権限を持つユーザー、およびスーパーユーザー権限を持つユーザーでさえ、**WORM** ファイルを変更できません。**WORM** ファイルの名前を変更したり、**WORM** ファイルを **WORM** ではない通常のファイルに戻したりすることはできません。

WORM ファイルのメタデータ

Compliance Archiving Software では、クライアントデータの保有、保護、記述、または名前付けを行うメタデータを変更できません。表 C-1 に示すように、オペレーティングシステムに応じて、一部の限られたメタデータフィールドのみを変更できます。

表 C-1 変更可能または変更不可能な WORM ファイルのメタデータ

オペレーティングシステム	変更可	変更不可
UNIX	<ul style="list-style-type: none">読み取りアクセス権ビットの設定またはクリアファイルおよびグループの所有者の変更	<ul style="list-style-type: none">書き込みビットおよび実行ビットの使用可能への切り替えsetuid ビットのクリアサイズまたは変更時刻 (mtime) の変更
Windows	<ul style="list-style-type: none">読み取りアクセス権ビットの設定またはクリアアーカイブビットの変更アクセス制御リストの作成および変更(ただし、ACL の設定にかかわらず、WORM ファイルは変更できない)	<ul style="list-style-type: none">読み取り専用ビット、システムビット、および隠しビットの変更サイズまたは変更時刻 (mtime) の変更

ネームスペースの制限

Compliance Archiving Software では、WORM ファイルの名前を変更できません。ディレクトリが空でない場合は、ディレクトリの名前も変更できません。この規則によって、WORM ファイルが存続する限り、ファイルのフルパス名が変更されないことが保証されます。

警告

UNIX クライアントがファイルモードを 4000 (WORM トリガーの呼び出し) に設定すると、ファイルのアクセスモードは通常 4000 にはなりません。これは、chmod コマンドおよびシステムコールの標準の定義に違反します。その結果、多くの Linux ディストリビューションで使用される GNU バージョンの chmod(1) コマンドを使用して WORM トリガーを発行すると、警告メッセージが生成されます。このメッセージは無視できます。

ファイル保持期間

WORM ファイルにはそれぞれ保持期間が設定されており、保持期間中はファイルを削除できません。保持期間は、保持期間の終了時点を表すタイムスタンプを使用して指定されます。この保持期間は、クライアントのアプリケーションまたはユーザーが明示的に設定できます。保持期間がクライアントによって指定されていない場合、**Compliance Archiving Software** は、ボリュームの作成時に指定されたデフォルトの保持期間を使用します。保持期間が終了する前に WORM ファイルを削除しようとしても失敗します。ただし、保持期間が期限切れになると、いつでもファイルを削除できます。

注: 保持期間は、ファイルを削除する機能にのみ適用されます。保持期間が期限切れになっているかどうかにかかわらず、WORM ファイルは変更できません。

保持タイムスタンプの設定

Compliance Archiving System の保持タイムスタンプは、WORM ファイルのアクセス時刻 (atime) 属性に格納されます。クライアントは、通常、ファイルを読み取り専用に変更する前に atime 属性を設定します。ファイルが WORM ファイルになると、そのファイルの atime の値が秒単位で切り捨てられ、保持タイムスタンプが決まります。

atime 属性が過去の時刻を表す場合は、ファイルシステムのデフォルト保持期間が現在の時刻に追加されて保持タイムスタンプが計算されます。

永続保持

クライアントのアプリケーションまたはユーザーは、ファイルを永続的に保持するように指定できます。永続保持を指定するには、32 ビットの符号付き整数で設定可能な最大値をファイルの atime に設定します。この値 (0x7fffffff) は、2,147,483,647 に相当します。UNIX システムでは、この値は、limits.h ヘッダーファイルで INT_MAX として定義され、タイムスタンプ 03:14:07 GMT, Jan 19, 2038 に変換されます。

保持期間の変更

保持期間は、延長できます。また、保持期間が期限切れになったファイルに新しい保持期間を設定することもできます。保持期間を変更するには、WORM ファイルの atime 属性を再設定します。新しい値が古い保持タイムスタンプよりも新しい場合、変更は許可されます。

アクセス時刻の無視

Compliance Archiving Software では、アクセス時刻 (atime) 属性を使用して保持タイムスタンプを格納します。そのため、ファイルが WORM ファイルであるかどうかに関係なく、標準的なファイルシステム操作の副作用でこの属性が更新されることはありません。

ファイル状態の確認

クライアントのアプリケーションおよびユーザーは、標準ツールおよび API を使用してファイルのメタデータを読み取り、ファイルの保持状態を確認できます。たとえば UNIX クライアントの場合、ファイル属性は `stat(2)` システムコールを介して読み取ったり、`ls` コマンドで表示したりできます。`ls -lu` コマンドを実行すると、ファイルの一覧がアクセス権および `atime` のタイムスタンプと一緒に表示されます。

UNIX システムコールの動作

UNIX クライアントのアプリケーションは、ローカルのシステムコールインタフェースを介して Compliance Archiving Software にアクセスします。これらのコールで呼び出されたクライアント NFS 実装によって、システムコールは標準の NFS プロトコル要求に変換されます。規制適合対応のファイルシステムの動作は標準の NAS ファイルシステムの動作と異なるため、クライアントシステムコールの動作もそれに応じて異なります。

この節では、標準 UNIX システムコールのなかで、規制適合対応の Sun StorageTek 5320 NAS Appliance 共有に対してクライアントが実行すると動作が異なるものについて説明します。この節に記載されていないシステムコールは通常どおり動作します。

Sun StorageTek 5320 NAS Appliance のインタフェースは、NFS および CIFS ファイルアクセスプロトコルです。したがって、この節では、標準のプロトコル要求に対応する Sun StorageTek 5320 NAS Appliance の規制適合に関する動作、およびシステムコールから NFS 要求へのマッピングの両方について説明します。これらのコールの動作は Solaris オペレーティングシステムクライアントで確認済みです。また、ほかの UNIX クライアントでも同じように動作します。

`access(2)`

`amode` 引数に `W_OK` ビットを指定した `access(2)` のコールなど、WORM ファイルの書き込み権を確認しようとする、失敗してエラー (EPERM) が返されます。

chmod(2)、fchmod(2)

ターゲットファイルが WORM ファイルではなく通常のファイルで、実行権ビットが設定されていない場合、新しいアクセス権が 4000 (S_ISUID) に設定されると、そのターゲットファイルは WORM ファイルになります。この場合、ターゲットファイルは、ファイルのアクセスモードの既存の読み取りビットに `setuid` ビットを追加して計算された新しいアクセスモードを受け取ります。具体的に説明すると、古いアクセスモードが `oldmode` の場合、WORM トリガーを受け取ったあとのファイルの新しいアクセスモードは次のように計算されます。

```
newmode = S_ISUID | (oldmode & 0444)
```

実行可能ファイルは WORM ファイルに変換できません。WORM トリガー (モード 4000) を 1 つ以上の実行権ビットが指定されたファイルに適用すると、失敗してエラー (EACCES) が返されます。

WORM ファイルの読み取りアクセスビットは、設定またはクリアできます。WORM ファイルの書き込み権または実行権の追加、`setgid` ビット (S_ISGID) または `sticky` ビット (S_ISVTX) の設定、あるいは WORM ファイルの `setuid` ビットのクリアを試みると、失敗してエラー (EPERM) が返されます。

chown(2)、fchown(2)

これらのコールは、WORM ファイルでも WORM ではないファイルでも同じように動作します。

link(2)

クライアントは、WORM ファイルへの新しいハードリンクを作成できます。WORM ファイルへのハードリンクは、ファイルの保持期間が期限切れになるまで削除できません。詳細は、289 ページの `unlink(2)` を参照してください。

read(2)、readv(2)

クライアントは、WORM ファイルを読み取ることができます。保持タイムスタンプは `atime` 属性に格納されているため、WORM ファイルへの読み取りアクセスを反映してこの値が更新されることはありません。

rename (2)

WORM ファイル、または規制適合対応のファイルシステム上の空ではないディレクトリの名前を変更しようとする、失敗してエラー (EPERM) が返されます。

stat (2)、fstat (2)

これらのコールを使用して通常のファイルに関する情報を取得すると、返される stat 構造体には規制適合に関する値が含まれます。st_mode フィールドには、通常どおり、ファイルのモードとアクセス権が含まれます。WORM ファイルには setuid ビットが設定されていますが、書き込みビットまたは実行ビットは設定されていません。st_atime フィールドには、ファイルの保持期間の終了を示すタイムスタンプが含まれます。この値が limits.h で定義される INT_MAX と同じ場合、ファイルは永続的に保持されます。

unlink (2)

Sun StorageTek 5320 NAS Appliance の固定クロックが示す現在の時間がファイルの atime 属性に格納されている日付 (保持タイムスタンプ) を過ぎている場合にのみ、WORM ファイルのリンクを解除できます。この条件が満たされない場合、unlink (2) は失敗してエラー (EPERM) が返されます。

utime (2)、utimes (2)

これらのコールは、ファイルのアクセス時刻 (atime) 属性および変更時刻 (mtime) 属性を設定するために使用します。WORM 以外のファイルに対して使用すると通常どおり動作し、ファイルが WORM に変換される前に保持タイムスタンプを指定するための手段を提供します。

これらのコールを WORM ファイルに対して呼び出すと、ファイルの保持期間を延長したり、保持期限が切れたファイルに新しい保持期間を割り当てたりすることができます。新しい atime 値がファイルの既存の atime 値よりも大きい場合 (atime 値よりあとの時刻を示している場合) は、WORM ファイルに対するこれらのコールは成功します。新しい atime 値が現在の atime 値と同じか小さい場合は、これらのコールは失敗してエラー (EPERM) が返されます。WORM ファイルに対して使用した場合、mtime 引数は無視されます。

`write(2)`、`writev(2)`

WORM ファイルへの書き込みは、すべて失敗してエラー (`EPERM`) が返されます。

Windows クライアントの動作

この節では、Windows クライアントの規制適合対応ファイルの相違点について説明します。

WORM ファイルの作成

WORM ファイルでない通常のファイルは、アーカイブおよび隠しビットが設定されていない場合にのみ Windows から WORM ファイルに変換できます。これらのビットがクリアされると、Windows クライアントは読み取り専用ビットおよびシステムビットを設定して、ファイルを WORM ファイルに変換します。この WORM トリガーによって、ファイルの読み取り専用ビットが設定されますが、ファイルのシステムビットの状態は変更されません。

WORM ファイルのメタデータの制限

Windows クライアントは、WORM ファイルのアーカイブビットを変更できますが、読み取り専用ビット、隠しビット、またはシステムビットは変更できません。Windows クライアントは WORM ファイルの ACL を変更できますが、WORM ファイルの ACL の書き込み権はすべて無視されます。ACL のアクセス権にかかわらず、WORM ファイルのデータを変更しようとするとう失敗します。

保持期間の設定

UNIX クライアントと同様、Windows クライアントは、ファイルのアクセス時刻 (`atime`) 属性に保持タイムスタンプを格納して保持期間を設定します。

Windows クライアントに対する警告

次に続く節では、Windows クライアントに関して認識する必要がある追加情報について説明します。

読み取り専用ビットに関する注意事項

規制適合対応のボリュームは、WORM ファイルの特殊な動作を認識する Windows のアプリケーションおよびユーザーのみが使用する必要があります。ファイルのコピーを行う標準的な多くの Windows ユーティリティでは、ファイルに対して読み取り専用ビットおよびシステムビットが指定されます。これらのツールを使用して規制適合対応ボリュームに WORM ファイルのコピーを作成すると、読み取り専用ビットおよびシステムビットが設定されるため、作成されたファイルが WORM ファイルになる可能性があります。

ウイルス対策ソフトウェア

多くのウイルスチェックプログラムは、検査するファイルのアクセス時刻を保持しようとします。通常、このようなプログラムは、ウイルスチェックの前にファイルの `atime` を読み取り、ウイルスチェックが終わると `atime` を走査前の値に再設定します。これによって、ほかのアプリケーションがファイルの保持期間を設定しているときに、同時にウイルスチェックプログラムがファイルを走査すると、競合状態が発生する可能性があります。その結果、ファイルに誤った保持期間が設定される場合があります。

この問題を回避する簡単な方法は、ウイルスチェックプログラムを規制適合対応のファイルシステム上で実行しないか、または WORM ファイルを作成するアプリケーションと同時に実行しないことです。

カスタムアプリケーションでは、短いデフォルト保持期間を使用し、WORM トリガーの適用後にファイルの実際の保持期間を設定することによって、この問題を回避することもできます。

その他の API

Compliance Archiving Software には、Java、Perl、C++ など、ほかにも多くの API を介してアクセスできます。これらのすべての言語は、NFS または CIFS を介してマウントされる共有にアクセスするために、基本となる同一のシステムコールに依存します。

付録 D

Sun StorageTek 5320 NAS Appliance コンポーネント

この付録では、Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance サーバー (本体) のハードウェアのコンポーネントについて説明します。この付録は、次の節で構成されています。

- 293 ページの「NAS サーバー」
- 301 ページの「RAID コントローラ格納装置および拡張格納装置コンポーネント」

顧客交換可能ユニット (CRU) として識別されるコンポーネントの詳細は、第 12 章を参照してください。

注: この付録で説明する Sun StorageTek 5320 NAS Appliance の一般的な機能は、Sun StorageTek 5320 NAS Cluster Appliance にも当てはまります。

NAS サーバー

Sun StorageTek 5320 NAS Appliance サーバーは、すべてのシステム構成の基本サーバー装置です。図 D-1 に、このサーバーの正面を示します。

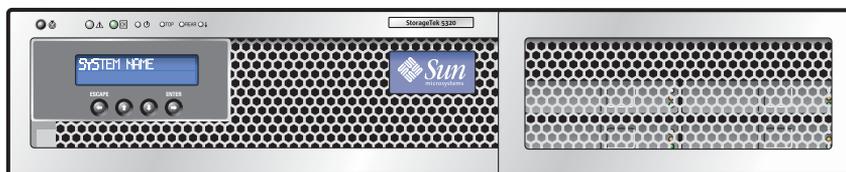


図 D-1 Sun StorageTek 5320 NAS Appliance の正面図

フロントパネルのボタンおよび LED

サーバーのフロントパネルには、液晶ディスプレイ (LCD) パネル、ボタン、および LED があります。

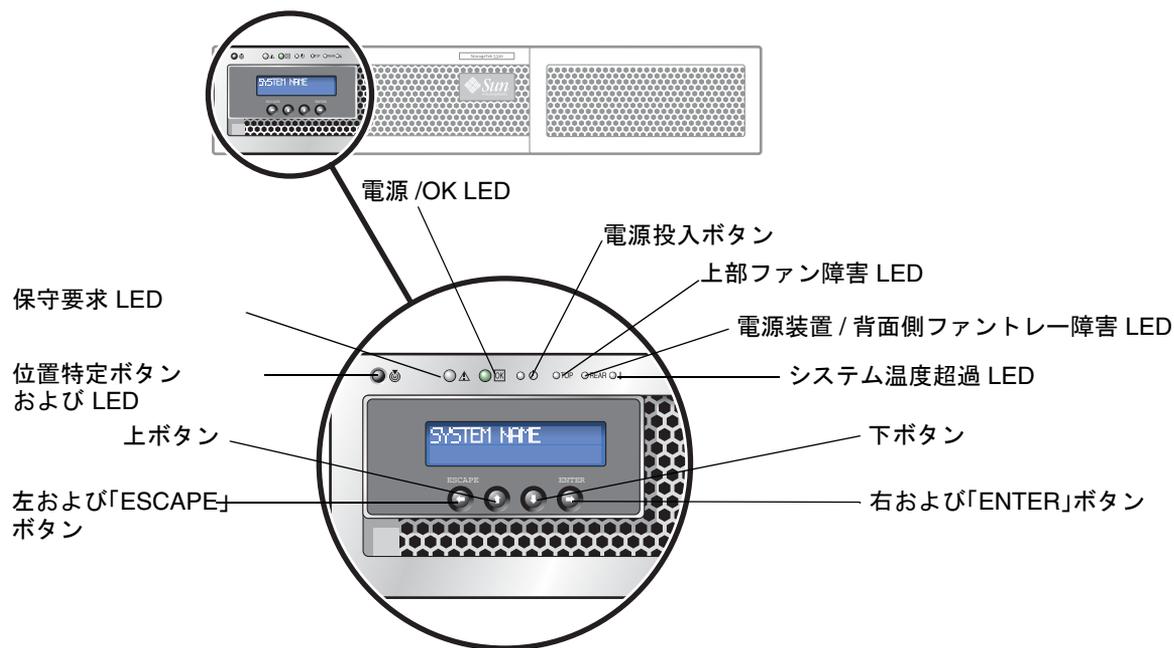


図 12-22 NAS サーバーのフロントパネルのボタンおよび LED

LCD ボタンを使用すると、LCD メニューオプション間を移動して、ローカルな基本機能を実行できます。基本機能には、システム状態の確認、ネットワーク構成設定の表示または変更、システムの停止または再起動などがあります。

LCD ボタンを使用してシステムを停止すると、オペレーティングシステムの制御下で正常な停止が実行されます。遠隔ユーザーは、Web Admin グラフィカルユーザーインターフェースを使用して、ネットワーク経由でシステムを停止できます。



注意: システムを停止する場合は、電源ボタンを使用しないでください。常に、LCD ボタンか、164 ページの「サーバーの停止」で説明している遠隔停止手順を使用してください。不適切な停止手順を実行すると、データが失われる可能性があります。

表 D-1 に、サーバーのフロントパネルにあるボタンの機能を示します。

表 D-1 NAS サーバーのフロントパネルのボタン

ボタン	説明
電源投入ボタン	NAS サーバーに電源を入れます。ペン先または同様の道具を使用して、埋め込み式のボタンを押して離してください。常に次の順序で装置に電源を入れてください。 <ol style="list-style-type: none">1. アレイの拡張ユニット。2. アレイのコントローラ装置。3. NAS サーバー。
左/「ESCAPE」ボタン	取り消し、バックスペース、エスケープ。
上ボタン	上にスクロールして、文字、ドット、スペースを選択します。
下ボタン	下にスクロールして、文字、ドット、スペースを選択します。
右/「ENTER」ボタン	確定、選択、保存、入力。

状態インジケータ LED

Sun StorageTek 5320 NAS サーバーの正面にある状態 LED は、サーバーコンポーネントの状態を示します。

表 D-2 で、システムで発生している現在の活動を示す LED 状態インジケータについて説明します。

表 D-2 正面の LED 状態インジケータ

LED	説明
位置特定ボタン/LED	<p>この LED は、ラック全体に多数のサーバーが設置されている場合に、ラック内で作業中のシステムを特定するために役立ちます。</p> <ul style="list-style-type: none"> このボタンを押して離すと、位置特定 LED が 30 分間点滅します。 このボタンを 5 秒間押し続けると、「push-to-test」モードになり、シャーシの内側と外側にあるほかのすべての LED が 15 秒間点灯します。
保守要求 LED	<p>この LED には次の 2 つの状態があります。</p> <ul style="list-style-type: none"> オフ: 正常な動作。 ゆっくり点滅: 保守の必要なイベントが検出されました。
電源/OK LED	<p>この LED には次の 3 つの状態があります。</p> <ul style="list-style-type: none"> オフ: サーバーの主電源およびスタンバイ電源が切断されています。 点滅: サーバーがスタンバイ電源モードであり、AC 電源が GRASP ボードおよび電源装置ファンのみには供給されています。 オン: サーバーが主電源モードであり、AC 電源がすべてのコンポーネントに供給されています。
上部ファン障害 LED	<p>この LED は、正面の冷却ファンモジュールに障害が発生した場合に点灯します。個々のファンモジュールの LED によって、どのモジュールに障害が発生したかが示されません。</p>
電源装置/背面側ファントレイ障害 LED	<p>この LED は、次の場合に点灯します。</p> <ul style="list-style-type: none"> システム内に 2 つの電源装置が存在するが、一方だけが AC 電源に接続されている場合。この状況を解決するには、もう一方の電源装置を AC 電源に接続するか、シャーシから取り外します。 システム内で電圧関連のイベントが発生した場合。CPU に関連する電圧エラーの場合は、関連付けられた CPU 障害 LED も点灯します。 背面側ファントレイに障害が発生したか、または背面側ファントレイが取り外されている場合。
システム温度超過 LED	<ul style="list-style-type: none"> この LED は、温度の上限が検出された場合に点灯しません。

背面パネルのポートおよび LED

Sun StorageTek 5320 NAS Appliance サーバーは、PCI スロット 1 (標準) および PCI スロット 0 (オプション) にデュアルポートファイバチャネル (FC) ホストバスアダプタ (HBA) カードを取り付けて、クラスタ構成にすることができます。図 D-2 に、サーバーの背面を示します。

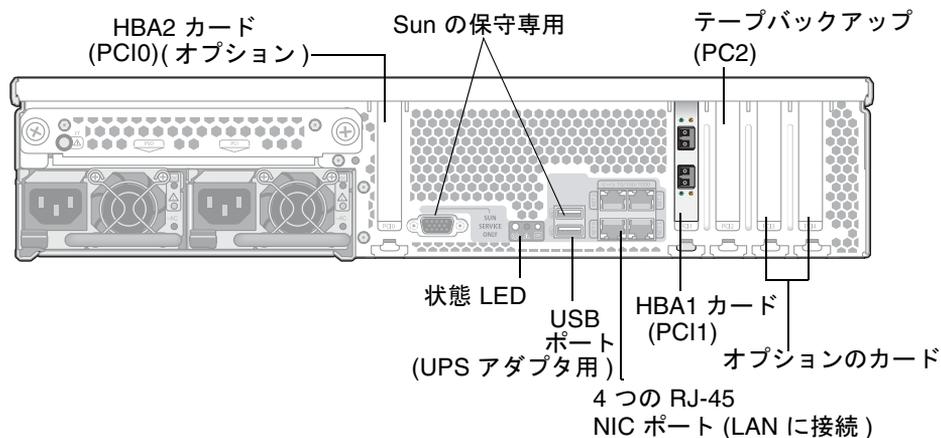


図 D-2 1 枚の HBA カードを装備した Sun StorageTek 5320 NAS Appliance の背面パネル

Sun StorageTek 5320 NAS Cluster Appliance 構成では、2 台の高可用性 (HA) サーバーが対で販売され、ソフトウェアのシリアル番号でサーバー「-H1」およびサーバー「-H2」として識別されます。各サーバーは、2 枚のデュアルポート FC HBA カードを装備しており、ほかのオプションのカードも装備できます。

補助ローカル UPS への接続

USB/シリアルポートアダプタケーブルまたは変換ケーブル (出荷キットに同梱) を使用して、サポートされるローカル UPS (無停電電源装置) デバイスに接続できます。

サポートされるローカル UPS デバイスに UPS アダプタケーブルを接続すると、NAS 機器が UPS の状態を監視できます。電源異常が発生した場合でも、UPS によりシステムの正常な停止が可能になります。詳細は、158 ページの「UPS 監視について」を参照してください。

UPS アダプタケーブルは、NAS サーバーの動作状態 (オン/オフ) に関係なく接続できます。

UPS アダプタケーブルを接続するには、次の手順を実行します。

1. UPS デバイスに付属する説明書に従って、シリアルポートコネクタ側を、サポートされる UPS のシリアルポートインタフェースに接続します。
2. ケーブルの USB コネクタ側を、NAS Appliance 背面の下側の USB コネクタに接続します。

背面パネルの LED

図 D-3 に、サーバーの背面にある LED を示します。

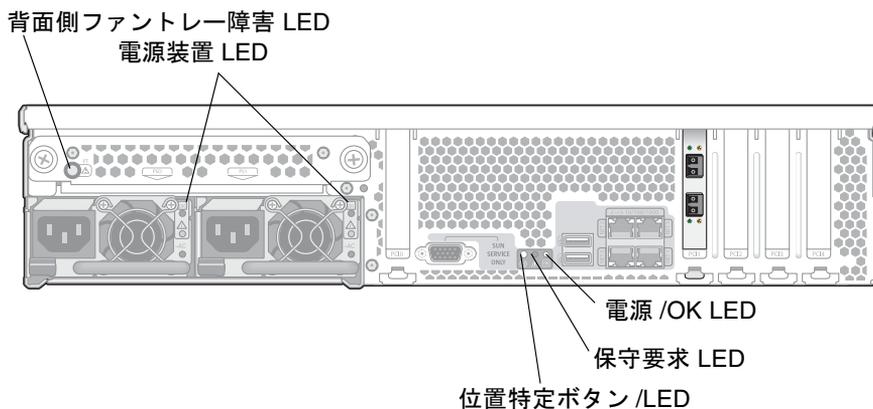


図 D-3 サーバーの背面パネルの LED

表 D-3 に、背面パネルの LED の機能を示します。

表 D-3 背面パネルの LED 状態インジケータ

LED 名	説明
背面側ファントレー障害 LED	この LED には次の 2 つの状態があります。 <ul style="list-style-type: none">• オフ: ファンモジュールは正常です。• オン (オレンジ色): ファントレーに障害が発生しました。
電源装置 LED	電源装置には次の 3 つの LED があります。 <ul style="list-style-type: none">• 上の LED (緑色): 電源装置は正常です。• 中央の LED (オレンジ色): 電源装置に障害が発生しました。• 下の LED (緑色): 電源装置への AC 電源は正常に供給されています。
位置特定ボタン/LED	この LED は、ラック全体に多数のサーバーが設置されている場合に、ラック内で作業中のシステムを特定するために役立ちます。 <ul style="list-style-type: none">• このボタンを押して離すと、位置特定 LED が 30 分間点滅します。• このボタンを 5 秒間押し続けると、「push-to-test」モードになり、シャーシの内側と外側にあるほかのすべての LED が 15 秒間点灯します。
保守要求 LED	この LED には次の 2 つの状態があります。 <ul style="list-style-type: none">• オフ: 正常な動作。• ゆっくり点滅: 保守の必要なイベントが検出されました。
電源/OK LED	この LED には次の 3 つの状態があります。 <ul style="list-style-type: none">• オフ: サーバーの主電源およびスタンバイ電源が切断されています。• 点滅: サーバーがスタンバイ電源モードであり、AC 電源が GRASP ボードおよび電源装置ファンのみに供給されています。• オン: サーバーが主電源モードであり、AC 電源がすべてのコンポーネントに供給されています。

サーバーの電源装置

システムの電源装置は、すべてのコンポーネントに電源を供給します。すべての装置に対応する電源装置システムは、電圧を 100 ~ 240 ボルト、50 ~ 60 Hz に自動的に適合させる自動検知デバイスです。

サーバーの電源装置システムは、図 D-4 に示すように、1 + 1 構成の 2 つの冗長なホットスワップ対応モジュールで構成されています。各モジュールは、500 W の負荷を維持することができます。システムが適切に動作するには 1 台以上の電源装置が必要であり、電源の冗長性を得るには 2 台の電源装置が必要です。

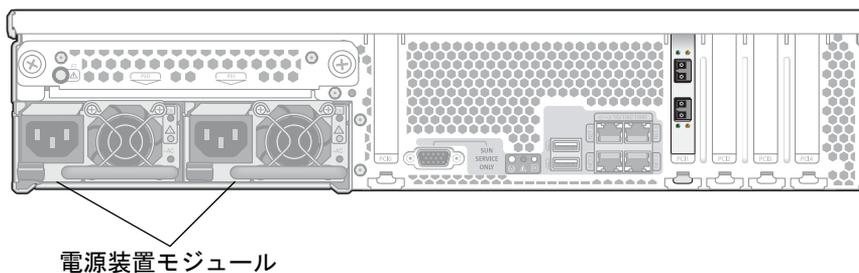


図 D-4 電源装置モジュール

電源装置には、次のような機能があります。

- 550W の出力
- 複数の速度に対応できる内部冷却ファン
- 組み込み型負荷分散機能
- 組み込み型過負荷保護機能
- 差し込み/引き出し用の一体型のハンドル

直接接続のテープライブラリ

ローカルテープバックアップ用ドライブは、サーバーの背面の左下にある SCSI ポートに接続できます。

注: サポートされているテープ装置のリストに、使用するテープドライブが含まれていることを確認してください。サポートされているテープデバイスの最新情報については、ご購入先にお問い合わせください。

テープライブラリの SCSI ID は、テープドライブの ID より小さい値である必要があります。たとえば、ライブラリ ID を 0 に設定し、ドライブ ID を 5 などの矛盾しない値に設定します。

使用するテープドライブシステムの詳細は、システムに付属するマニュアルを参照してください。

RAID コントローラ格納装置および拡張格納装置コンポーネント

コントローラ格納装置と拡張格納装置は、Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance システムにストレージを提供します。

コントローラ格納装置

Sun StorEdge 5300 RAID EU コントローラ格納装置は、ファイバチャネル拡張格納装置 (EU F) または SATA 拡張格納装置 (EU S) とともに使用できます。



注意 – 拡張格納装置を追加するか取り外すには、システムを停止する必要があります。

ファイバチャネルコントローラ格納装置のフロントパネル側には、14 台のホットスワップ対応のハードドライブが取り付けられており、6 台のドライブ (5+1) による RAID 5 グループが 2 つと、グローバルホットスペアが 2 台という構成になっています。各ドライブの未フォーマット時の容量は 146G バイトで、使用可能な容量は 133G バイトです。格納装置で使用可能な容量は、合計で 1.3T バイトになります。

300G バイトの FC ドライブの RAID 構成には、6 台のドライブ (5+1) で構成される RAID 5 グループが 1 つと、7 台のドライブ (6+1) で構成される RAID 5 グループが 1 つ、およびグローバルホットスペアが 1 台含まれます。

SATA システムで使用するコントローラ格納装置は、ハードドライブがない状態で出荷されます。代わりに、SATA ドライブはすべて EU S 拡張格納装置に取り付けられています。



注意 – コントローラ格納装置内またはアレイ内で、ファイバチャネルディスクドライブと SATA ディスクドライブを混在させないでください。

注 – デュアルアレイ構成の場合、一方のアレイにファイバチャネルディスクドライブを取り付け (コントローラ格納装置および拡張格納装置内)、もう一方のアレイに SATA ディスクドライブを取り付ける (拡張格納装置内のみ) ことができます。

拡張格納装置

拡張格納装置を使用すると、システムのストレージ容量を拡張できます。

各 EU F 拡張格納装置のフロントパネル側には、14 台のホットスワップ対応のファイバチャネルハードドライブが取り付けられており、7 台のドライブ (6+1) による RAID 5 グループが 2 つという構成になっています。各ドライブの未フォーマット時の容量は 146G バイトで、使用可能な容量は 133G バイトです。1 台の EU F 拡張格納装置で使用可能な容量は、合計で 1.6T バイトになります。

1 台めの EU S 拡張格納装置のフロントパネル側には、14 台のホットスワップ対応の SATA ドライブが取り付けられており、6 台のドライブ (5+1) による RAID 5 グループが 1 つ、7 台のドライブ (6+1) によるグループが 1 つと、1 台のグローバルホットスペアという構成になっています。各 SATA ドライブの未フォーマット時の容量は 400G バイトで、使用可能な容量は 360G バイトです。1 台めの EU S 拡張格納装置で使用可能な容量は、合計で 3.6T バイトになります。

2 台め以降の EU S 拡張格納装置には、14 台のホットスワップ対応の SATA ハードドライブが取り付けられており、7 台のドライブ (6+1) による RAID 5 グループが 2 つという構成になっています。約 4.4T バイトの使用可能な容量が追加されます。



注意 – 拡張格納装置内で、ファイバチャネルディスクドライブと SATA ディスクドライブを混在させないでください。

FC 拡張ユニットと SATA 拡張ユニットの混在

シリアル ATA (Serial Advanced Technology Attachment, SATA) とファイバチャネルが混在する拡張ユニット (EU) 構成は、現在、次の条件でサポートされています。

- それぞれの EU は、ファイバチャネルドライブのみ、または SATA ドライブのみで構成される必要があります。1 つの EU 内で複数の種類のドライブを混在させることはできません。
- EU に SATA ドライブが含まれていても、RAID EU にはファイバチャネルドライブを含めることができます。RAID EU に SATA ドライブを含めることはできません。
- SATA およびファイバチャネルの両方に対して、アレイで使用しているものと同じ容量の固有のホットスペアが 1 台必要です。
- LUN に、SATA ドライブおよびファイバチャネルドライブの両方を含めることはできません。

ドライブシャトル



注意 – Sun StorageTek 5320 NAS Appliance および Sun StorageTek 5320 NAS Cluster Appliance では、Sun が提供するファイバチャネルドライブまたは SATA ドライブのみが動作します。最新のサポート情報については、ご購入先にお問い合わせください。

ドライブは、それぞれのドライブシャトルに入っています。拡張格納装置、コントローラ格納装置、または Sun StorageTek 5320 NAS Appliance や Cluster を停止することなく、ドライブシャトルを個別に交換することができます。



注意 – 拡張格納装置内、コントローラ格納装置内、またはアレイ内で、ファイバチャネルディスクドライブと SATA ディスクドライブを混在させないでください。



注意 – ホットスワップできるのは、一度に 1 台のドライブシャトルのみです。RAID サブシステムで必要な再構築作業が完了していることを確認してから、次のドライブシャトルを取り外してください。



注意 – RAID サブシステムが危険な状態である場合や、新しい RAID セットを作成したり既存の RAID セットを再構築したりする場合には、システムソフトウェアまたは RAID ファームウェアを更新しないでください。

▼ ドライブまたは格納装置の位置を確認する

1. Web Administrator のナビゲーションパネルで、「RAID」>「Manage RAID」を選択します。
2. 「Locate Drive」または「Locate Drive Tray」ボタンをクリックします。この操作によって、ドライブまたは格納装置の LCD インジケータが点滅します。



図 D-5 ファイバチャネルドライブシャトル

▼ 交換するドライブを確認する

ディスクドライブに障害が発生した場合、ディスクを特定するにはログエントリが役立ちます。システムログおよび診断レポートのどちらの場合も、同じ方法でディスクの場所を解釈できます。次にログエントリの例を示します。

```
Controller 0 enclosure 0 row 0 column 6
```

このようなログエントリを解釈するには、次の事項に注意してください。

- チャネルおよびターゲットの番号はすべて無視してください。
- コントローラ番号は、0 から始まります。たとえば、1 番めのアレイ (RAID EU) のコントローラは 0 (スロット A) および 1 (スロット B) で、2 番めのアレイのコントローラは 2 および 3 です。
- 格納装置の番号は 0 から始まり、属するアレイに対しての番号となります。たとえば、1 番めのアレイに 2 台の格納装置がある場合は、格納装置 0 および 1 として識別されます。
- Sun StorageTek 5320 NAS Cluster Appliance の場合、行番号は常に 0 になります。
- 列番号は 0 から始まり、格納装置のスロット番号を示します。

したがって、この例は、1 番めのアレイにある 1 番めの格納装置のスロット 7 を示していると解釈できます。

注 - 1 番めのアレイと 2 番めのアレイを特定する標準的な方法はありません。通常、1 番めの HBA ポートは 1 番めのアレイ、2 番めの HBA ポートは 2 番めのアレイなどのように接続されます。

ドライブ障害メッセージ

次の表に、発生する可能性のあるドライブの問題、その意味、および修正措置を示します。

注 – 次の手順を実行する前に、Web Admin GUI およびシステムログを確認して、ドライブの再構築が完了していることを確認してください。

表 D-4 ドライブ障害メッセージ

問題	意味	修正措置
LED が赤色	ドライブの障害を示しています。	<ol style="list-style-type: none">1. ドライブの再構築が確実に完了していることを <code>syslog</code> で確認します。2. 正確で完全なシステムバックアップが使用可能であるかどうかを確認します。バックアップを確認できない場合は、すぐにシステムをバックアップします。3. Sun の保守担当者にお問い合わせ、障害が発生したドライブを交換します。
ログまたは電子メールのドライブ障害メッセージ	障害が発生したこと、または障害が発生しようとしていることを示しています。	<ol style="list-style-type: none">1. 正確で完全なシステムバックアップが使用可能であるかどうかを確認します。バックアップを確認できない場合は、すぐにシステムをバックアップします。2. Sun の保守担当者にお問い合わせ、障害が発生したドライブを交換します。
LCD パネルに「Drive failure」メッセージの表示	ドライブの障害を示します。	<p>このタイプのエラーでは LED が赤く点灯しない場合があります。</p> <ol style="list-style-type: none">1. ログまたは電子メールメッセージでドライブの位置を確認します。このメッセージには、障害が発生しているドライブのスロットが示されています。たとえば、「drive failure slot 9」と示されます。2. Sun の保守担当者にお問い合わせ、障害が発生したドライブを交換します。

電源装置

コントローラ格納装置および拡張格納装置は、同じ電源装置モジュールを使用しません。



電源装置モジュール

コントローラ格納装置



電源装置モジュール

電源装置モジュール

拡張格納装置



電源装置モジュール

電源装置モジュール

図 D-6 電源装置モジュール

診断電子メールメッセージの送信

診断電子メール機能を使用して、Sun の技術サポートチームまたはその他の任意の受信者に電子メールメッセージを送信できます。診断電子メールメッセージには、Sun StorageTek 5320 NAS Appliance のシステム構成、ディスクサブシステム、ファイルシステム、ネットワーク構成、SMB 共有、バックアップや復元処理に関する情報、/etc ディレクトリ情報、システムログ、環境データ、および管理者情報が含まれます。

送信されるすべての診断電子メールメッセージには、発生した問題にかかわらず、これらのすべての情報が含まれます。

クラスタ構成では、クラスタ内の各サーバーに診断電子メールを設定する必要があります。

診断電子メールを設定するには、次の手順を実行します。

1. **Web Administrator** グラフィカルユーザーインターフェースの一番上のツールバーで、 ボタンをクリックします。
「Diagnostic Email」ウィンドウが表示されます。
2. 「Problem Description」フィールドに問題の説明を入力します。
これは必須エントリで、256 文字まで入力できます。
3. 1 人以上の電子メール受信者の「Diagnostics」チェックボックスが選択されていることを確認します。
受信者の追加または変更が必要な場合は、32 ページの「電子メール通知の設定」を参照してください。
4. 「Send」をクリックしてメッセージを送信します。

Web Administrator のパネル

この付録では、Web Administrator グラフィカルユーザーインターフェースの各パネルのフィールドおよび要素を一覧で示します。この付録は、次の節で構成されています。

- 309 ページの「「Anti Virus Configuration」のパネル」
- 311 ページの「「Configuration Wizard」のパネル」
- 313 ページの「「File Replicator」のパネル」
- 320 ページの「ファイルボリューム操作のパネル」
- 335 ページの「「High Availability」のパネル」
- 339 ページの「「iSCSI Configuration」のパネル」
- 343 ページの「「Monitoring and Notification」のパネル」
- 351 ページの「「Network Configuration」のパネル」
- 362 ページの「「RAID」のパネル」
- 368 ページの「「System Activity」のパネル」
- 370 ページの「「System Backup」のパネル」
- 371 ページの「「System Manager」のパネル」
- 374 ページの「「System Operations」のパネル」
- 384 ページの「「UNIX Configuration」のパネル」
- 396 ページの「「Windows Configuration」のパネル」

「Anti Virus Configuration」のパネル

この節では、「Configure Anti Virus」パネルのフィールドおよび要素について説明します。

「Configure Anti Virus」パネル

このパネルでは、システムに対してウイルス対策ソフトウェアを構成できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-1 「Configure Anti Virus」パネルのフィールドおよび要素

フィールド	説明
Enable Anti Virus	システム上でウイルス対策ソフトウェアを使用可能にする場合に選択します。
Scan Mode	ウイルス対策スキャンを実行する場合のモードを選択します。 <ul style="list-style-type: none">• Scan Suspend (Quarantine Only) — 「Enable Anti Virus」チェックボックスを選択すると、すでに隔離されているファイルのスキャンは実行されず、隔離されているファイルはアクセス不可になります。ウイルス対策ソフトウェアを一時的に使用不可にする場合は、このオプションを選択することをお勧めします。それ以外の場合、「Enable Anti Virus」チェックボックスをクリアしてウイルス対策ソフトウェアを使用不可にすると、ウイルス対策ソフトウェアが完全にアクティブでなくなり、隔離されているファイルがアクセス可能になります。 注: このオプションを選択すると、ウイルス対策保護機能が無効になります。• Scan after Modify — ファイルが変更された場合にのみファイルをスキャンします。このオプションは、パフォーマンスとウイルス保護の完全性の妥協点を提供するもので、読み取りアクセスは高速ですが、ウイルスからの保護は、ファイルが変更された時点でのみ最新のウイルス定義が適用された状態になります。その後、そのファイルにアクセスした時点では、ウイルス定義が変更された可能性が考慮されません。• Scan all Access — ファイルへの何らかのアクセスが行われた場合にファイルをスキャンします。このオプションでは、ウイルスからの保護がほぼ完全に実施され、最新のウイルス定義でスキャン済みのデータへのアクセスだけが許可されます。
Scan Engine IP Address	ウイルスのスキャン用に設定するスキャンエンジンのインターネットプロトコル (IP) アドレス。最大 4 つのスキャンエンジンを使用できます。
Port #	スキャンエンジンのポート番号。
Max Conn	スキャンエンジンとの最大接続数。これは、スキャンエンジンがファイルのスキャンに使用する並行スレッドの数です。デフォルト値は 2 です。
	これをクリックすると、選択したスキャンエンジンが表から削除されるか、選択したオブジェクトが「List」メニューから削除されます。どちらが削除されるかは、パネルの「Scan Engine IP Address」セクションまたは「List」セクションのどちらでこのボタンをクリックしたかに依存します。

表 F-1 「Configure Anti Virus」パネルのフィールドおよび要素 (続き)

フィールド	説明
Type	<p>ウイルス対策ソフトウェアでスキャンするオブジェクト、または無視するオブジェクトのカテゴリ。次のいずれかのカテゴリをクリックしてから、「List」フィールドに値を入力して、スキャンまたは無視するオブジェクト (ファイル拡張子やクライアント名など) を指定します。</p> <ul style="list-style-type: none"> • File Types Included – ウイルス対策ソフトウェアでスキャンするファイルのタイプ。このフィールドを空白にすると、すべてのファイルタイプがスキャンされます。入力できる値は 3 文字以内で、ワイルドカードマッチング用の「?」を使用できます。 • File Types Excluded – ウイルス対策ソフトウェアで無視するファイルのタイプ。入力できる値は 3 文字以内で、ワイルドカードマッチング用の「?」を使用できます。 • Exempt Clients – ウイルス対策ソフトウェアで無視するクライアントの名前または IP アドレス。 • Exempt Groups – ウイルス対策ソフトウェアで無視する各 Windows/NT グループまたは Windows Active Directory グループの名前。UNIX グループではありません。入力項目には空白文字を含めることができます。 • Exempt Shares – ウイルス対策ソフトウェアで無視する共通インターネットファイルシステム (CIFS) 共有の名前。 注: 管理共有 (x\$) はウイルス対策ソフトウェアによって常に無視されます。
List	<p>「Type」メニューで選択したカテゴリに応じて、ウイルス対策ソフトウェアでスキャンするオブジェクト、または無視するオブジェクト。「List」セクションの上部にあるフィールドには、値を入力できます。リストのすぐ下にあるフィールドには、以前に入力したすべての値が一覧表示されます。</p> <p> これをクリックすると、パネルの「List」セクションの上部のフィールドに新しく入力した値が、「List」セクションの下部のフィールドに追加されます。</p>
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Configuration Wizard」のパネル

この節では、Web Administrator グラフィカルユーザーインタフェースの「Configuration Wizard」の各パネルにあるフィールドおよび要素について説明します。

- 312 ページの「「Configuration Wizard」パネル」
- 312 ページの「「Confirmation」パネル」
- 312 ページの「「Select Environment」パネル」

「Configuration Wizard」パネル

これは構成ウィザードの最初の画面です。構成ウィザードは、連続したウィンドウに情報を入力することで、新しく接続されたシステムを構成できるツールです。

各ウィンドウに必要な情報を入力し、「Next」をクリックして続行します。ウィザードの最後では、入力した情報を確認したあと、編集してから保存するか、「Cancel」をクリックして破棄できます。

「Confirmation」パネル

このパネルは構成ウィザードの最後の画面です。ここでは、構成ウィザードに入力した情報を確認または破棄できます。

このウィンドウで、次のいずれかを実行します。

- 入力した情報を変更してからシステムに保存するには、次の操作を行います。
 - a. 「Back」ボタンをクリックして、変更を行うウィンドウに戻ります。
 - b. 変更を行い、「Next」をクリックして「Confirmation」パネルに戻ります。
 - c. 「Finish」をクリックします。
変更内容がシステムに保存されます。
- 入力した構成情報をシステムに保存するには、「Finish」をクリックします。
- 情報を保存せずに構成ウィザードを閉じるには、「Cancel」をクリックします。

「Select Environment」パネル

このパネルでは、新しく接続されたシステムのネットワーク環境を構成できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-2 「Select Environment」パネルのフィールドおよび要素

フィールド	説明
Network	

表 F-2 「Select Environment」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Configure for Windows Only Networks	システムに Windows のみのネットワークを設定する場合に選択します。ネットワーク上に UNIX サーバーが構成されていない場合、このオプションを選択します。
Configure for Unix Only Networks	システムに UNIX のみのネットワークを設定する場合に選択します。ネットワーク上に Windows サーバーが構成されていない場合、このオプションを選択します。
Configure Both Windows and UNIX Networks	システムに Windows と UNIX の混在ネットワークを設定する場合に選択します。ネットワーク上に Windows サーバーと UNIX サーバーの両方が構成されている場合、このオプションを選択します。

「File Replicator」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「File Replicator」の各パネルにあるフィールドおよび要素について説明します。

- 313 ページの「「Add/Edit Mirror」 ウィンドウ」
- 314 ページの「「Manage Mirrors」 パネル」
- 316 ページの「「Promote Volume」 ウィンドウ」
- 316 ページの「「Set Threshold Alert」 パネル」
- 317 ページの「「View Mirror Statistics」 パネル」

「Add/Edit Mirror」 ウィンドウ

このウィンドウでは、ミラーを追加または編集できます。追加または編集のどちらであるかは、「Add」または「Edit」のどちらをクリックしてウィンドウにアクセスしたかに依存します。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-3 「Add/Edit Mirror」 ウィンドウのフィールドおよび要素

フィールド	説明
Volume	このフィールドは、ウィンドウが追加モードの場合にのみ編集可能です。ミラー化するファイルボリュームを選択します。

表 F-3 「Add/Edit Mirror」ウィンドウのフィールドおよび要素

フィールド	説明
Mirror Host	このフィールドは、ウィンドウが追加モードの場合にのみ編集可能です。ミラー化されたファイルボリュームのホストとなるサーバーの名前を指定します。
IP Address	ミラー接続に使用されるインターネットプロトコル (IP) アドレス。ミラー化にはプライベートネットワークリンク (ネットワーク内のほかのデバイスからアクセスできないリンク) を使用することをお勧めします。
Alternative IP Address	(省略可能) 最初の IP アドレスが使用不可になった場合にミラーを維持するために使用される IP アドレス。
Password	必要に応じて、ミラーホストサーバーへのアクセスに必要な管理パスワードを入力します。管理パスワードを設定しない場合、このフィールドは空白のままかまいません。
Mirror Buffer Size (MB)	このフィールドは、ウィンドウが追加モードの場合にのみ編集可能です。ミラーバッファのサイズを指定します。ミラーバッファには、ミラーホストサーバーへのファイルシステムの書き込みトランザクションの転送中に、これらのトランザクションが格納されます。ミラーバッファのサイズはさまざまな要因に依存しますが、100M バイト以上必要であり、ミラー化バッファボリュームのサイズは最小でも数 G バイトにしてください。ミラー化バッファボリュームの約 10% のサイズのミラーバッファを作成するとよいでしょう。選択するサイズは、ファイルボリュームサイズよりも、ソースファイルボリュームへの書き込み活動により大きく作用します。アクティブサーバー上のファイルボリュームの空き領域は、ミラーバッファに割り当てたサイズの分だけ減少することに注意してください。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、入力項目を保存せずにウィンドウが閉じます。

「Manage Mirrors」パネル

このパネルでは、アクティブサーバーとミラーサーバーの間でミラーの追加、編集、または切断を行うことができます。アクティブサーバー上でミラーが切断されると、ミラーサーバー上でミラー化されたファイルボリュームをプロモートすることができます。つまり、ミラー化されたファイルボリュームをユーザーが使用できるようにします。

注:ファイルボリュームが規制適合対応である場合、そのファイルボリュームはプロモートできません。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-4 「Manage Mirrors」パネルのフィールドおよび要素

フィールド	説明
Volume	ミラー化するファイルボリューム。
Active Server	ファイルボリュームが最初に存在しているサーバーの名前または IP アドレス。
Mirror Server	ミラー化ファイルボリュームのホストとなるサーバーの名前または IP アドレス。
Sync Status	ミラーの状態: <ul style="list-style-type: none">• New – 新しいミラーが作成されています。• Creating mirror log – ミラーバッファが初期化されています。• Connecting to host – アクティブサーバーが遠隔ミラーサーバーに接続しています。• Creating extent – ミラーサーバー上にディスクパーティションが作成されています。• Ready – システムの準備が完了して、他方のシステムの準備が完了するまで待機しています。• Down – ネットワークリンクが停止しています。• Cracked – ミラーが破損しています。• Syncing Volume – ミラーサーバー上でファイルボリュームの同期がとられています。• In Sync – ミラーは同期がとれています。• Out of Sync – ミラーは同期がとれていません。• Error – エラーが発生しました。• Mirror is out of space – ミラー上で記憶領域として使用できる容量がなくなりました。
Add	(アクティブサーバーのみ) ファイルボリュームをアクティブサーバーからミラーサーバーにミラー化する場合にクリックします。
Break	(アクティブサーバーのみ) 選択したミラーを切断する場合にクリックします。
Edit	(アクティブサーバーのみ) 選択したミラーを編集する場合にクリックします。
Promote	(ミラーサーバーのみ) これをクリックすると、「Promote Volume」ウィンドウが表示されます。このウィンドウから、ミラーサーバー上にある、プロモートするファイルボリュームを選択できます。 注: アクティブサーバー上ですでに切断されているミラーのみをプロモートできます。

表 F-4 「Manage Mirrors」パネルのフィールドおよび要素 (続き)

フィールド	説明
Change Roles	アクティブボリュームがミラーボリュームとして、またはミラーボリュームがアクティブボリュームとして機能できるようにする場合にクリックします。この場合、各ボリューム上の元の構成は変更されません。ミラーボリュームの役割を変更するには、ファイルボリュームを選択して「Change Roles」をクリックします。

「Promote Volume」ウィンドウ

このウィンドウでは、ミラーサーバー上でミラー化されたボリュームをプロモートし、ユーザーに対して使用可能にすることができます。

注: ボリュームが規制適合対応である場合、そのファイルボリュームはプロモートできません。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-5 「Promote Volume」ウィンドウのフィールドおよび要素

フィールド	説明
Available Volumes	プロモート (NBD ボリュームから SFS2 ボリュームに変換) できるボリュームを選択します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「Set Threshold Alert」パネル

このパネルでは、すべてのミラー化されたファイルボリュームのしきい値警告を設定できます。しきい値警告とは、指定された受信者に警告が送信されるミラーバッファの使用率です。

ミラーバッファには、ミラーホストサーバーへのファイルシステムの書き込みトランザクションの転送中に、これらのトランザクションが格納されます。アクティブサーバーへの書き込みアクティビティが増加したり、ネットワークリンクが損傷を受けたりすると、ミラーサーバーへの書き込みトランザクションの転送がミラーバッファ上にバックアップされる場合があります。この処理でミラーバッファが制限を超えた場合、ミラーが破損し、ミラーが再確立されるまでアクティブサーバーとミラーサーバー間でトランザクションが発生しなくなります。

この状況を回避するため、ミラーバッファの使用率が特定のしきい値に達すると、ソフトウェアは自動的に警告を送信します。

次の表で、このパネルのしきい値およびボタンについて説明します。

表 F-6 「Set Threshold Alert」 パネルのフィールドおよび要素

フィールド	説明
	このアイコンをクリックしてドラッグすると、スケール上に沿ってしきい値が移動します。このアイコンを移動させると、右側に表示されるしきい値が更新されます。
Mirroring Buffer Threshold 1 (%)	これは、最初の警告が送信されるミラーバッファの使用率です。デフォルト値は 70% です。これは、ミラーバッファの使用率が 70% に達すると、自動的に警告が送信されることを意味します。
Mirroring Buffer Threshold 2 (%)	これは、2 番めの警告が送信されるミラーバッファの使用率です。デフォルト値は 80% です。
Mirroring Buffer Threshold 3 (%)	これは、3 番めの警告が送信されるミラーバッファの使用率です。デフォルト値は 90% です。
Alert Reset Interval (Hours)	ソフトウェアがすでに送信した警告を再送信するまでに待機する時間です。たとえば、「Mirroring Buffer Threshold 1」を 10% に設定し、「Alert Reset Interval」を 2 時間に設定すると、ミラーバッファの使用率が 10% に達したときに最初の警告が送信されます。ソフトウェアは、その後 2 時間はしきい値 1 警告を再送信しません。その時点でミラーバッファの使用率がまだ 10% のしきい値を超えている場合、しきい値 1 警告が再送信されます。デフォルト値は 24 時間です。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「View Mirror Statistics」 パネル

このパネルでは、ミラー化されたファイルボリュームのネットワーク統計情報を参照できます。

次の表で、このパネルのしきい値およびボタンについて説明します。

表 F-7 「View Mirror Statistics」パネルのフィールドおよび要素

フィールド	説明
<i>Select Volume</i>	
List of Volumes	ネットワーク統計情報を表示するミラー化ファイルボリュームを選択します。
Status	ミラーの状態を記述するテキスト行。
<i>Transactions (transactions/second)</i>	
Incoming	選択したボリュームの受信トランザクション統計情報。1秒あたりのトランザクション数で表されます。 <ul style="list-style-type: none">• Avg – アクティブサーバーに送信される1秒あたりの平均トランザクション数。• Min – アクティブサーバーに送信された1秒あたりの最小トランザクション数。可能な場合は、この数のトランザクションが発生した日時が右側に表示されます。• Max – アクティブサーバーに送信された1秒あたりの最大トランザクション数。可能な場合は、この数のトランザクションが発生した日時が右側に表示されます。
Outgoing	選択したボリュームの送信トランザクション統計情報。1秒あたりのトランザクション数で表されます。 <ul style="list-style-type: none">• Avg – アクティブサーバーからミラーサーバーに送信される1秒あたりの平均トランザクション数。• Min – アクティブサーバーからミラーサーバーに送信された1秒あたりの最小トランザクション数。可能な場合は、この数のトランザクションが発生した日時が右側に表示されます。• Max – アクティブサーバーからミラーサーバーに送信された1秒あたりの最大トランザクション数。可能な場合は、この数のトランザクションが発生した日時が右側に表示されます。
<i>Mirror Buffer (transactions)</i>	
Size	ミラーバッファのサイズ。バイト数ではなく、トランザクション数で表されます。
Free	ミラーバッファ内に残っているトランザクション数。
Utilization	トランザクションを保持するために現在使用されているミラーバッファの割合。この値が100%に近づいたら、すべてのネットワークリンクが正常に機能していることを確認してください。ネットワークリンクが停止すると、バッファがいっぱいになり、最終的に制限を超えます。この場合、アクティブシステムへのトランザクションの送信速度がミラーシステムへの送信速度を上回っているため、バッファがいっぱいになります。バッファが制限を超えると、ミラーは破損しています。ネットワークリンクが修復されると、ミラー化されたファイルボリュームの同期がとれるまで、システムはミラー更新処理を自動的に開始します。

表 F-7 「View Mirror Statistics」パネルのフィールドおよび要素 (続き)

フィールド	説明
Fill Rate	ミラーバッファの流入速度、1 秒あたりのトランザクション数で表されます。流入速度が 0 より大きい場合は、すべてのネットワーク接続が正常に機能していることを確認する必要があります。ネットワークリンクが停止すると、バッファがいっぱいになり、最終的に制限を超えます。この場合、アクティブシステムへのトランザクションの送信速度がミラーシステムへの送信速度を上回っているため、バッファがいっぱいになります。バッファが制限を超えると、ミラーは破損しています。ネットワークリンクが修復されると、ミラー化されたファイルボリュームの同期がとれるまで、システムはミラー更新処理を自動的に開始します。
<i>Network Statistics</i>	
<i>Host</i>	
Hostname	ミラーバッファに使用されるホストの、ネットワークによって認識される名前。
Connected	ミラーバッファによって使用されるホストのネットワークへの接続方法を示すテキスト行。
Connected Since	ミラーバッファによって使用されるホストが最初にネットワークに接続された日付。
<i>Link</i>	
Status	ネットワーク上のミラーバッファのリンク状態。
Link Quality	ネットワーク上のミラーバッファリンクの品質。
Errors	ネットワーク上のミラーバッファリンクに関連するエラー。
Timeouts	ネットワーク上のミラーバッファリンクのタイムアウト回数。
Drops	ネットワーク上のミラーバッファリンクのドロップ数。
Time of Last Transfer	ネットワーク上でメモリーバッファの最後の転送が行われた日時。
<i>Request Control Blocks</i>	
Sent	メモリーバッファによってネットワーク上で送信された制御ブロックの数。
Total Bytes	メモリーバッファによってネットワーク上で送信された制御ブロックの合計バイト数。
Average Size	メモリーバッファの制御ブロックの平均サイズ。
Rate	メモリーバッファによってネットワーク上で送信された制御ブロックの 1 秒あたりの速度。
<i>Transfer Rate</i>	
Average (kb/s)	メモリーバッファでの転送が行われる平均速度。1 秒あたりの K バイトで表されます。

表 F-7 「View Mirror Statistics」パネルのフィールドおよび要素 (続き)

フィールド	説明
Max (kb/s)	メモリーバッファによってネットワーク上で行われた転送の最大量。1 秒あたりの K バイトで表されます。
When Max Occurred	最大量の転送が行われた日時。
<i>Response Time</i>	
Average (msec)	メモリーバッファの平均応答時間。
Max (msec)	メモリーバッファの最大応答時間。
When Max Occurred	最大応答時間が発生した日時。

ファイルボリューム操作のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースのファイルボリューム操作の各パネルにあるフィールドおよび要素について説明します。

- 321 ページの「「Add/Edit Checkpoint Schedule」ウィンドウ」
- 322 ページの「「Add/Edit DTQ Setting」ウィンドウ」
- 323 ページの「「Add/Edit Quota Setting」ウィンドウ」
- 324 ページの「「Attach Segments」パネル」
- 325 ページの「「Configure Directory Tree Quotas」パネル」
- 326 ページの「「Configure User and Group Quotas」パネル」
- 327 ページの「「Create Checkpoint」ウィンドウ」
- 328 ページの「「Create File Volumes/Segments」パネル」
- 330 ページの「「Delete File Volumes」パネル」
- 330 ページの「「Edit Volume Properties」パネル」
- 332 ページの「「Manage Checkpoints」パネル」
- 333 ページの「「Rename Checkpoint」ウィンドウ」
- 333 ページの「「Schedule Checkpoints」パネル」
- 334 ページの「「View Volume Partitions」パネル」

「Add/Edit Checkpoint Schedule」ウィンドウ

このウィンドウでは、チェックポイントスケジュールを追加または編集できます。追加または編集のどちらであるかは、「Add」または「Edit」のどちらをクリックしてこのウィンドウにアクセスしたかに依存します。

注: チェックポイントには大量の領域およびシステムメモリーが必要です。システム上のチェックポイントが多いほど、システムのパフォーマンスに対する影響が大きくなります。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-8 「Add/Edit Checkpoint Schedule」ウィンドウのフィールドおよび要素

フィールド	説明
Volume	チェックポイントスケジュールを作成または編集するボリューム。チェックポイントスケジュールを編集する場合は、このメニューで別のボリュームを選択できません。
Description	チェックポイントを記述するテキスト行。これは必須フィールドです。
Keep Days + Hours	チェックポイントが作成されたあと保持される期間 (日数と時間)。「Days」ボックスには、0 ~ 99 の整数を入力します。「Hours」ドロップダウンメニューからは、0 ~ 23 の整数値を選択します。これは必須フィールドです。
Days	チェックポイントを作成する曜日。このリストから複数の項目を選択するには、Ctrl キーを押しながら追加の曜日をクリックします。
AM Hours	チェックポイントを作成する午前の時間。このリストから複数の項目を選択するには、Ctrl キーを押しながら追加の項目をクリックします。
PM Hours	チェックポイントを作成する午後の時間。このリストから複数の項目を選択するには、Ctrl キーを押しながら追加の項目をクリックします。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Add/Edit DTQ Setting」 ウィンドウ

このウィンドウでは、ファイルシステム内のディレクトリの作成または編集と、割り当ての構成ができます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-9 「Add/Edit DTQ Setting」 ウィンドウのフィールドおよび要素

フィールド	説明
DTQ Name	このディレクトリツリー割り当ての識別に使用される名前。
Dir Name	新しいディレクトリの名前。ディレクトリ割り当ては、このフィールドで作成したディレクトリについてのみ構成できます。
Path	新しいディレクトリの読み取り専用パス。ディレクトリツリー割り当てを追加する場合は、このフィールドの下にあるボックスのフォルダをクリックして、「Path」フィールドを生成できます。このボックスには、ディレクトリが存在するファイルボリュームのディレクトリツリー構造が表示されます。このボックスのフォルダの内容を表示するには、フォルダの横の記号をクリックするか、フォルダ自体をダブルクリックします。次に、この割り当てを設定する新しいディレクトリを含むディレクトリを選択します。
Disk Space Limits	ディレクトリのディスク容量制限。「No Limit」または「Custom」を選択します。 <ul style="list-style-type: none">• No Limit — ディレクトリで使用できるディスク容量を無制限にする場合に選択します。• Custom — ディレクトリで使用できる最大ディスク容量を指定する場合に選択します。割り当てを M バイトまたは G バイトのどちらかの単位で決定するかを指定して、「Max Value」フィールドにディスク容量の制限値を入力します。0 (ゼロ) の値を入力すると、「No Limit」を選択した場合と同様に処理されます。
File Limits	このディレクトリに書き込み可能なファイルの最大数。「No Limit」または「Custom」を選択します。 <ul style="list-style-type: none">• No Limit — このディレクトリに書き込み可能なファイル数を無制限にする場合に選択します。• Custom — ディレクトリに書き込み可能なファイルの最大数を指定する場合に選択します。そのあと、「Max Value」フィールドにファイル数の制限値を入力します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Add/Edit Quota Setting」ウィンドウ

このウィンドウでは、グループ割り当てを追加または編集できます。追加または編集のどちらであるかは、「Add」または「Edit」のどちらをクリックしてこのウィンドウにアクセスしたかに依存します。割り当ては、NT および UNIX のユーザーとグループに対するディスク容量およびファイル数の制限値を指定するものです。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-10 「Add/Edit Quota Setting」ウィンドウのフィールドおよび要素

フィールド	説明
Volume	ユーザー割り当てまたはグループ割り当てを追加または編集するボリューム。
User	割り当てを追加または編集するユーザーまたはグループ。割り当てを追加する場合は、適切な「Unix」または「Windows」ラジオボタンを選択して、指定したユーザーまたはグループが UNIX または Windows 環境のどちらに属しているかを選択します。そのあと、対応するドロップダウンメニューから、ユーザー名またはグループ名 (NT ユーザーまたはグループの場合はドメイン名も) を選択します。
Disk Space Limits	選択したユーザーまたはグループのディスク容量の制限値。次のいずれかを選択します。 <ul style="list-style-type: none">• Default - 325 ページの「「Configure Directory Tree Quotas」パネル」で示すように、強い制限値および弱い制限値をデフォルトのユーザーまたはグループと同じ値に設定する場合に選択します。• No Limit - ユーザーまたはグループが使用できる容量を無制限にする場合に選択します。• Custom - ユーザーまたはグループに対して弱い制限値および強い制限値を定義する場合に選択します。割り当てを K バイト、M バイト、または G バイトのどの単位で指定するかを選択します。そのあと、ユーザーまたはグループが使用できる最大ディスク容量を「Max Value」フィールドに入力します。
File Limits	選択したボリュームにユーザーまたはグループが書き込むことができるファイルの最大数。次のいずれかを選択します。 <ul style="list-style-type: none">• Default - 325 ページの「「Configure Directory Tree Quotas」パネル」で示すように、強い制限値および弱い制限値をデフォルトのユーザーまたはグループと同じ値に設定する場合に選択します。• No Limit - ユーザーまたはグループが書き込むことができるファイルの数を無制限にする場合に選択します。• Custom - ユーザーまたはグループに対して弱い制限値および強い制限値を定義する場合に選択します。割り当てを K バイト、M バイト、または G バイトのどの単位で指定するかを選択します。そのあと、ユーザーまたはグループが書き込むことができるファイルの最大数を「Max Value」フィールドに入力します。
Apply	これをクリックすると、変更内容が保存されます。

表 F-10 「Add/Edit Quota Setting」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Attach Segments」 パネル

「Create File Volumes」 パネルを使用するか、「System Manager」オブジェクトを右クリックしてから適切なセグメント配置メニューオプションを選択することによって、選択した一次ボリュームにセグメントを配置できます。

このウィンドウまたはパネルでは、既存の一次ファイルボリュームにセグメントを配置できます。一度に配置できるセグメントは、1つのみです。

注: セグメントが配置されたあと、それを一次ファイルボリュームから切り離すことはできません。むしろ、セグメントは永続的にそのボリュームの一部となります。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-11 「Attach Segments」 パネルのフィールドおよび要素

フィールド	説明
Existing Volumes	このフィールドは、「Create File Volumes」パネルからのみ使用できます。セグメントを配置する既存のボリュームをクリックします。
Available Segments	一次ボリュームに配置できる既存のファイルセグメントのリスト。名前、LUN、およびサイズ (M バイト単位) が表示されます。セグメントが存在しない場合は、328 ページの「「Create File Volumes/Segments」 パネル」でセグメントを作成できます。詳細は、46 ページの「「Create File Volumes」 パネルを使用したファイルボリュームまたはセグメントの作成」を参照してください。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Configure Directory Tree Quotas」パネル

このパネルでは、Sun StorageTek ファイルシステムの特定のディレクトリに対する割り当てを管理できます。ディレクトリツリー割り当ては、ディレクトリで使用可能なディスク容量およびこのディレクトリに書き込み可能なファイル数を決定します。

注: このパネルで作成したディレクトリにのみ、割り当てを作成および構成することができます。以前から存在したディレクトリには、割り当てを作成および構成することはできません。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-12 「Configure Directory Tree Quotas」パネルのフィールドおよび要素

フィールド	説明
Volume	ディレクトリツリー割り当てを構成する一次ボリュームを選択します。
DTQ Name	選択したボリューム上のディレクトリに適用するディレクトリツリー割り当ての名前。
Max Size (MB)	このディレクトリで使用できる最大ディスク容量。
Size Used (%)	このディレクトリで現在使用されているディスク容量の割合。
Max File	このディレクトリに書き込むことができるファイルの最大数。
File Used	このディレクトリに現在書き込まれているファイルの数。
Path	選択したボリューム上のディレクトリのフルパス。
Refresh	これをクリックすると、選択したボリュームに関する最新の情報でパネルが更新されます。
Add	これをクリックすると、「Add DTQ Setting」ウィンドウが表示されます。このウィンドウから、選択したボリューム上に新しいディレクトリを作成し、そのディレクトリに新しいディレクトリツリー割り当てを適用できます。
Edit	これをクリックすると、「Edit DTQ Setting」ウィンドウが表示されます。このウィンドウから、選択したディレクトリツリー割り当てを編集できます。
Delete	これをクリックすると、選択したディレクトリツリー割り当てが表から削除されます。

「Configure User and Group Quotas」 パネル

このパネルでは、NT および UNIX のユーザーおよびグループに対して、ボリュームに関するユーザーおよびグループの割り当てを管理できます。ユーザーおよびグループの割り当ては、ユーザーまたはグループが使用できるディスク容量と、ユーザーまたはグループがボリュームに書き込むことができるファイルの数を決定します。ユーザーおよびグループの割り当てを設定する前に、330 ページの「「Edit Volume Properties」 パネル」で、選択したボリュームに対する割り当てを使用可能にしてください。

表には、選択したボリュームに対するスーパーユーザー、デフォルトのユーザー、および個別のユーザーの割り当てが表示されます。デフォルトでは、スーパーユーザーおよびスーパーユーザーグループには容量またはファイル数に対する強い制限値も弱い制限値も設定されていません。デフォルトのユーザーおよびデフォルトのグループの設定は、個別の割り当てが設定されていないすべてのユーザーおよびグループに対する設定です。割り当ての制限値の詳細は、115 ページの「ユーザーおよびグループの割り当ての構成について」を参照してください。

注: ユーザーおよびグループの割り当てを使用する場合は、ユーザーまたはグループのアクセスを許可する前に、デフォルトのディスク容量またはファイル数の制限値を設定することをお勧めします。これによって、ユーザーまたはグループの個々の割り当てを構成する前でも、ユーザーおよびグループは許可された制限値を超えるデータまたはファイルを書き込むことができなくなります。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-13 「Configure User and Group Quotas」 パネル

フィールド	説明
Volume	ユーザーまたはグループの割り当てを作成する既存のボリュームを選択します。
Users	これを選択すると、選択したボリュームに適用されている既存のユーザー割り当てが表示されます。
Groups	これを選択すると、選択したボリュームに適用されている既存のグループ割り当てが表示されます。
ID	ユーザーまたはグループの割り当てに指定された一意の識別子。
Name	ユーザーまたはグループの割り当ての名前。
Windows Name	Windows 環境によって認識されるユーザーまたはグループの割り当ての名前。
KB Used	ユーザーまたはグループによってボリューム上で現在使用されているディスク容量。

表 F-13 「Configure User and Group Quotas」 パネル (続き)

フィールド	説明
Soft KB Limits	「Hard KB Limits」と同じか、それより大きい値。この値を超えると7日間の猶予期間に入ります。この猶予期間が過ぎると、ユーザーまたはグループは、使用済みのディスク容量が弱い制限値を下回るまで、このボリューム上のディスク容量を使用できなくなります。
Hard KB Limits	「Soft KB Limits」と同じか、それより小さい値。選択したボリューム上でユーザーまたはグループが使用できる最大ディスク容量を決定します。
File Used	選択したボリュームにユーザーまたはグループによって書き込まれたファイルの数。
Soft File Limits	「Hard File Limits」と同じか、それより小さい値。この値を超えると7日間の猶予期間に入ります。この猶予期間が過ぎると、ユーザーまたはグループは、ボリュームにすでに書き込まれているファイルの数が弱い制限値を下回るまで、これ以上ボリュームにファイルを書き込むことができなくなります。
Hard File Limits	「Soft File Limits」と同じか、それより大きい値。選択したボリュームにユーザーまたはグループが書き込むことができるファイルの最大数を決定します。
Refresh	これをクリックすると、ユーザーまたはグループの割り当てに関する最新情報でパネルが更新されます。
Add	これをクリックすると、「Add Quota Settings」ウィンドウが表示されます。このウィンドウから、選択したボリュームに対するユーザーまたはグループの新しい割り当てを作成できます。
Edit	これをクリックすると、「Edit Quota Settings」ウィンドウが表示されます。このウィンドウから、選択したユーザーまたはグループの割り当てを編集できます。

「Create Checkpoint」ウィンドウ

このウィンドウでは、チェックポイントを作成できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-14 「Create Checkpoint」ウィンドウのフィールドおよび要素

フィールド	説明
Volume Name	チェックポイントを作成または編集するボリュームを選択します。

表 F-14 「Create Checkpoint」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Auto Delete	システムによってチェックポイントに自動的に名前が割り当てられ、「Keep Days and Hours」で指定された時間が経過したあとでチェックポイントが削除されるようにする場合に選択します。次の項目を指定します。 Keep Days + Hours — チェックポイントが保持される日数および時間。「Days」フィールドには、0 ~ 99 の整数を入力します。「Hours」ドロップダウンメニューからは、0 ~ 23 の整数値を選択します。
Backup	チェックポイントのデフォルトの名前を「Backup」として定義する場合に選択します。チェックポイントは、Sun StorageTek 5320 NAS Appliance ファイルシステムのローカルバックアップに使用されません。特定の期間が経過しても、チェックポイントは自動的に削除されません。
Manual	手で削除されるまでチェックポイントを常に保持する場合に選択します。「Name」フィールドで、チェックポイントの保存に使用する名前を指定します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Create File Volumes/Segments」 パネル

「Create File Volumes」 パネルを使用するか、ナビゲーションパネルで「System Manager」を右クリックしてから適切なメニューオプションを選択することによって、ボリュームまたはセグメントを作成できます。1 つの LUN につき最大 31 のファイルボリュームを作成できます。

注: 1 つのファイルボリュームは 256G バイトに制限されます。ただし、一次ボリュームにセグメントを配置して、より大きなボリュームを作成できます。最大 63 のファイルセグメントを配置できます。

セグメントのファイルボリュームを作成する前に、システムに新しく追加された可能性のあるディスクがないか走査します。この走査を実行するには、次のいずれかの操作を行います。

- ナビゲーションパネルで「System Manager」を右クリックし、「Scan for New Disks」を選択します。
- ナビゲーションパネルで「File Volume Operations」 > 「Create File Volumes」を選択し、「Create File Volumes」パネルの「Scan for New Disks」をクリックします。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-15 「Create File Volumes/Segments」 パネルのフィールドおよび要素

フィールド	説明
LUN	ファイルボリュームまたはセグメントを作成する論理ユニット番号 (LUN) をクリックします。1 つの LUN につき最大 31 のファイルボリュームを作成できます。LUN をクリックすると、右のフィールドが更新され、LUN の構成がグラフィカルに表示されます。このグラフィカルな表示の詳細は、パネルの「Legend」セクションを参照してください。
Name	ファイルボリュームまたはセグメントの名前。有効な文字は、英数字 (a ~ z, A ~ Z, 0 ~ 9) です。英字 (a ~ z, A ~ Z) から始まる 12 文字以内の名前を指定する必要があります。
Partition	パーティションが存在する場合、ファイルボリュームまたはセグメントを作成するパーティションを選択します。
Size	新しいファイルボリュームまたはセグメントのサイズ。ドロップダウンメニューから、「MB」または「GB」を選択します。
Type	このフィールドは、「File Volume Operations」 > 「Create File Volumes」パネルでのみ使用可能です。パーティションのタイプとして、「Primary」または「Segment」を選択します。
Compliance Archiving Software	このフィールドは、一次パーティションにファイルボリュームを作成する場合に、「File Volume Operations」 > 「Create File Volumes」パネルでのみ使用可能です。必須実施または推奨実施の規制適合ボリュームの作成を可能にする場合にクリックします。必須実施の規制適合ボリュームは、削除できません。
Legend	選択した LUN 構成のグラフィカル表示でのインジケータ： <ul style="list-style-type: none">• オレンジ - LUN 上の一次パーティションを示します。• 水色 - LUN 上のセグメント化されたパーティションを示します。• 緑色 - LUN 上のミラーを示します。• 青色 - LUN に DOS の読み取り専用属性が適用されていることを示します。この DOS の読み取り専用属性は、システムボリュームのフラッシュディスクでのみ使用されます。• 白色 - LUN 上の空き領域を示します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。
Scan for New Disks	このボタンは、「File Volume Operations」 > 「Create File Volumes」パネルでのみ使用可能です。これをクリックすると、システムに新しく追加されたディスクが検索されます。

「Delete File Volumes」 パネル

このパネルでは、選択したファイルボリュームを構成から削除できます。

注: 必須実施の規制適合ボリュームの場合は、ボリュームを削除できません。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-16 「Delete File Volumes」 パネルのフィールドおよび要素

フィールド	説明
Name	削除するボリュームの名前。
LUN	そのボリュームが存在する論理ユニット番号 (LUN)。ボリュームが、複数の LUN に存在する複数のパーティションで構成される場合があります。この状況では、LUN とパーティションのすべてのペアが表に一覧表示されます。
Partition #	ボリュームが存在する LUN パーティション。ボリュームが、複数の LUN に存在する複数のパーティションに存在する場合があります。この状況では、LUN とパーティションのすべてのペアが表に一覧表示されます。
Size (MB)	ボリュームのサイズ。
Apply	これをクリックすると、選択したボリュームが削除されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Edit Volume Properties」 パネル

このパネルでは、ボリュームの名前、チェックポイントオプション、割り当てオプションなどのボリュームのプロパティを変更できます。

注: 規制適合ボリュームでは、名前の変更または規制適合機能の使用不可への切り替えはできません。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-17 「Edit Volume Properties」 パネルのフィールドおよび要素

フィールド	説明
Volumes	編集する既存のボリュームをクリックします。
Volume Name	選択したボリュームの名前。

表 F-17 「Edit Volume Properties」パネルのフィールドおよび要素 (続き)

フィールド	説明
New Name	選択したボリュームの新しい名前。有効な文字は、英数字 (a ~ z、A ~ Z、0 ~ 9) です。英字 (a ~ z、A ~ Z) から始まる 12 文字以内の名前を指定してください。
Enable Checkpoints	ボリュームのチェックポイントを使用可能する場合にクリックします。チェックポイントの作成およびチェックポイントの自動削除オプションの詳細は、165 ページの「ファイルのチェックポイントの作成」を参照してください。
Checkpoint Configuration	<p>チェックポイントを構成できるオプション:</p> <ul style="list-style-type: none"> • Use for Backups – バックアップシステムで backup という名前のチェックポイントが作成および使用されるようにする場合にクリックします。 • Automatic – チェックポイントマネージャーによって、構成されているスケジュールに基づき、チェックポイントが自動的に作成および削除されるようにする場合にクリックします。
Enable Quotas	選択したボリュームに対する割り当てを使用可能にする場合にクリックします。
Enable Attic	<p>削除されたファイルを、このボリュームのルートにある .attic\$ ディレクトリに一時的に保存する場合に選択します。このオプションはデフォルトで使用可能に設定されています。</p> <p>ビジー状態のファイルシステム上でまれに、削除処理が終了する前に .attic\$ ディレクトリがいっぱいになり、結果として空き領域が不足してパフォーマンスが低下することがあります。このような場合は、このフィールドの選択を解除して、.attic\$ ディレクトリを使用不可にすることをお勧めします。</p>

表 F-17 「Edit Volume Properties」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Compliance Archiving	<p>これらのオプションは、ボリュームの作成時に推奨規制適合実施バージョンの規制適合アーカイブソフトウェアを使用可能にした場合のみ使用できます。規制適合アーカイブソフトウェアを構成できるオプションは、次のとおりです。</p> <ul style="list-style-type: none"> • Enabled – ボリュームで規制適合アーカイブソフトウェアが使用可能になっているかどうかを示すインジケータ。 • Mandatory (No Administrator Override) – ボリュームは必須実施の規制適合です。このボリュームを推奨実施の規制適合に構成することはできません。 • Advisory (Allow Administrator Override) – ボリュームは推奨実施の規制適合です。必須実施の規制適合を使用可能にする場合は、ソフトウェアを必須実施の規制適合バージョンにアップグレードしてください。これは一度だけ処理できます。 • Default Retention Period – クライアントに保持期間が設定されていない場合に、WORM (Write-Once, Read-Many) ファイルをボリュームに保持する期間を指定するには、このフィールドをクリックします。ファイルが保持される前に、そのファイルに対して保持期間が適用されていない場合は、ボリュームに対するデフォルトの保持期間が使用されます。ボリュームのデフォルトの保持期間を変更しても、すでに保持されているファイルには影響しません。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Manage Checkpoints」 パネル

このパネルでは、既存のチェックポイントの表示 (1 つのボリュームの 1 つのチェックポイントにつき 1 行)、新しいチェックポイントの作成、および既存のチェックポイントの編集と削除を行うことができます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-18 「Manage Checkpoints」 パネルのフィールドおよび要素

フィールド	説明
Name	チェックポイントの名前。
Volume	チェックポイントの対象となるボリューム。
Creation Date	チェックポイントが作成された日付。
Expiration Date	チェックポイントが削除された日付。

表 F-18 「Manage Checkpoints」 パネルのフィールドおよび要素

フィールド	説明
Create	これをクリックすると、「Create Checkpoint」ウィンドウが表示されます。このウィンドウから、ボリュームに対する新しいチェックポイントを作成できます。
Remove	これをクリックすると、選択したチェックポイントが表から削除されます。
Rename	これをクリックすると、「Rename Checkpoint」ウィンドウが表示されます。このウィンドウから、選択したチェックポイントの名前を編集できます。

「Rename Checkpoint」ウィンドウ

このウィンドウでは、選択したチェックポイントの名前を変更できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-19 「Rename Checkpoint」ウィンドウのフィールドおよび要素

フィールド	説明
Volume Name	このチェックポイントが作成されたボリュームの名前。このフィールドは編集できません。
Old Name	チェックポイントの名前。このフィールドは編集できません。
New Name	チェックポイントに割り当てる新しい名前。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Schedule Checkpoints」パネル

このパネルでは、既存のファイルボリュームに対するチェックポイントの作成についてスケジュールを設定できます。また、既存のチェックポイントのスケジュールを表示、編集、および削除することができます。このパネルには、チェックポイントごとに、ボリューム名、説明、スケジュール設定されたチェックポイントの日時、およびチェックポイントが保持される期間が表示されます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-20 「Schedule Checkpoints」パネルのフィールドおよび要素

フィールド	説明
Volume	チェックポイントのスケジュールを作成するボリューム。
Description	チェックポイントの説明を記述するテキスト行。
Days	チェックポイントを作成する曜日。
AM Hours	チェックポイントを作成する午前の時間。
PM Hours	チェックポイントを作成する午後および晩の時間。
Keep	チェックポイントスケジュールが作成されたあと保持される期間 (日数と時間)。
Add	これをクリックすると、「Add Checkpoint Schedule」ウィンドウが表示されます。このウィンドウから、ボリュームに対する新しいチェックポイントのスケジュールを作成できます。
Remove	これをクリックすると、選択したチェックポイントのスケジュールが表から削除されます。
Edit	これをクリックすると、「Edit Checkpoint Schedule」ウィンドウが表示されます。このウィンドウから、選択したチェックポイントのスケジュールを編集できます。

「View Volume Partitions」パネル

このパネルでは、システムで使用可能な論理ユニット番号 (LUN) と、それらの LUN に関連付けられているボリュームを表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-21 「View Volume Partitions」パネルのフィールドおよび要素

フィールド	説明
Volumes	ボリュームをクリックすると、既存の LUN 上でのボリュームの位置を表示できます。

表 F-21 「View Volume Partitions」 パネルのフィールドおよび要素

フィールド	説明
Legend	LUN 構成のグラフィカル表示でのインジケータ: <ul style="list-style-type: none"> • オレンジ – LUN 上の一次パーティションを示します。 • 水色 – LUN 上のセグメント化されたパーティションを示します。 • 緑色 – LUN 上のミラー化されたボリュームを示します。 • 青色 – LUN に DOS の読み取り専用属性が適用されていることを示します。この DOS の読み取り専用属性は、システムボリュームのフラッシュディスクでのみ使用されます。 • 白色 – LUN 上の空き領域を示します。 注: 選択したボリュームの LUN 上での位置は斜線 (///) で示されません。
Lun	選択したボリュームが存在する LUN の名前。
Partition	ボリュームが存在する LUN パーティション。
Use (%)	ボリューム上で使用されている領域の割合。
Type	一次、セグメント化など、ボリュームのタイプ。
Free (MB)	ボリューム上で記憶領域として使用できる空き容量。
Capacity (MB)	ボリューム上の記憶領域の合計容量。

「High Availability」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「High Availability」の各パネルにあるフィールドおよび要素について説明します。

- 335 ページの「「Enable Failover」パネル」
- 337 ページの「「Recover」パネル」
- 338 ページの「「Set LUN Path」パネル」
- 338 ページの「「Set Primary Path」ウィンドウ」

「Enable Failover」パネル

注: このパネルは Sun StorageTek 5320 NAS Cluster Appliance でのみ使用可能です。

このパネルでは、Sun StorageTek 5320 NAS Cluster Appliance の本体フェイルオーバーを使用可能にすることができます。フェイルオーバーは、サーバー 2 台構成のシステムで一方の本体に障害が発生した場合に実行されます。障害が発生した本体に

よってそれまで管理されていたインターネットプロトコル (IP) アドレスおよび論理ユニット番号 (LUN) は、動作している本体によって自動的に引き継がれるか、または管理されます。障害が発生した本体が手動でオンラインに戻されると、前述の LUN および IP アドレスの元の所有権または制御は、フェイルバックまたは回復と呼ばれる処理によって復元されます。フェイルオーバーの詳細は、19 ページの「フェイルオーバーの使用可能への切り替えについて」を参照してください。

注: 障害が発生したサーバー (本体) がオンラインに戻ったら、「Recover」パネルから回復処理を開始してください。詳細は、21 ページの「回復の開始」を参照してください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-22 「Enable Failover」 パネルのフィールドおよび要素

フィールド	説明
Automatic Failover	本体に障害が発生した場合に、システムによってフェイルオーバーが自動的に開始されるようにするには、これをクリックします。
Head Status	本体の健全性のインジケータ。
<i>Link Failover</i>	
Enable Link Failover	リンクのフェイルオーバーを使用可能にする場合にクリックします。これにより、「Primary」の役割が割り当てられているいずれかのネットワークインタフェースに障害が発生したときに、本体のフェイルオーバーが必ず実行されます。このタイプの障害は「リンク停止」状態と呼ばれます。パートナーのネットワークリンクが停止した場合、フェイルオーバーを実行する本体は、パートナー本体がネットワークリンクを再確立したあとで、指定された時間が経過するまで待機する必要があります。 注: リンクのフェイルオーバーを使用可能または使用不可にしたあとで、変更内容を有効にするためにシステムを再起動してください。
Down Timeout	1 台の本体のネットワークリンクの信頼性が失われ、そのパートナー本体のネットワークリンクが健全である場合に、本体がフェイルオーバーを実行するまで待機する秒数。
Restore Timeout	フェイルオーバーが行われるように、パートナー本体の一次リンクが確立されるまで待機する秒数。「Restore Timeout」は、リンク停止によって開始されたフェイルオーバーが、パートナー本体の一次リンクが切断されているために中止された場合のみ使用されません。
<i>Partner Configuration</i>	
Name	パートナーサーバーの名前。
Gateway	パートナーサーバーのゲートウェイ IP アドレス。

表 F-22 「Enable Failover」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Private IP	2 台のサーバー (本体) 間のハートビート接続用に予約されている IP アドレス。この IP アドレスは変更できません。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Recover」 パネル

注: このパネルは Sun StorageTek 5320 NAS Cluster Appliance でのみ使用可能です。

このパネルでは、障害が発生したサーバー (本体) がオンラインに戻ったあとで、回復を開始できます。回復処理を開始する前に、障害が発生した本体またはコントローラが動作可能で、オンラインになっていることを確認してください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-23 「Recover」 パネルのフィールドおよび要素

フィールド	説明
<i>Current RAID Configuration</i>	
Head 1	本体 1 として指定される、回復するサーバーの名前。
Head 2	本体 2 として指定される、回復するサーバーの名前。
<i>(NEW) Restore RAID Configuration</i>	
Controller 0/Head 1	構成に応じて、コントローラ 0 の LUN マッピング、または本体 1 の LUN マッピングのいずれかです。
Controller 1/Head 2	構成に応じて、コントローラ 1 の LUN マッピング、または本体 2 の LUN マッピングのいずれかです。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。
Apply	これをクリックすると、変更内容が保存されます。
Recover	これをクリックすると、選択したコントローラまたは本体の回復が実行されます。

「Set LUN Path」 パネル

このパネルでは、ファイルボリュームの論理ユニット番号 (LUN) のパスを定義、編集、および復元することができます。

LUN パスは、本体から RAID コントローラへのハードウェアルートを指定するもので、LUN 内のファイルボリュームへのアクセスに使用されます。ファイルボリュームごとに 2 つの LUN パスがあります。代替パスは、一次パスに障害が発生した場合に使用されます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-24 「Set LUN Path」 パネルのフィールドおよび要素

フィールド	説明
LUN	ファイルボリュームが存在する LUN。
Volumes	LUN 上の特定のファイルボリューム。
Active Path (HBA/SID)	LUN がシステムとの通信に使用する、現在アクティブなハードウェアパス。ハードウェアパスは、1 から始まるホストバスアダプタ (HBA) 番号と、LUN の最初のドライブであるコントローラの SCSI (Small Computer Systems Interface) 識別子 (ID) 番号によって識別されます。たとえば、1/1 は HBA 1 と SCSI コントローラターゲット 1 を示します。
Primary Path (HBA/SID)	LUN がシステムとの通信に使用する優先ハードウェアパス。また、一次パスは、LUN パスの復元先のパスにもなります。一次パスが指定されていない場合、システムは最初に使用可能なパスを使用します。
Alternate Path (HBA/SID)	一次パスに障害が発生した場合に LUN がシステムとの通信に使用できる代替ハードウェアパス。
Edit	これをクリックすると、「Primary Path」ウィンドウが表示されます。このウィンドウから、選択したボリュームの一次パスを編集できます。
Restore	これをクリックすると、アクティブなパスが、選択したボリュームの一次パスに復元されます。
Auto-assign LUN Paths	これをクリックすると、ソフトウェアによって、選択したボリュームに LUN パスが自動的に割り当てられます。

「Set Primary Path」 ウィンドウ

このウィンドウでは、一次パスを定義できます。このパスは、ソフトウェアが共有 LUN に情報を送信する際に使用するハードウェアルートです。二次パスは、一次パスに障害が発生した場合に使用されます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-25 「Set Primary Path」 ウィンドウのフィールドおよび要素

フィールド	説明
LUN Name	一次パスを設定する LUN の読み取り専用の名前。
Primary Path	パスを定義するホストバスアダプタ (HBA) および SCSI (Small Computer Systems Interface) 識別子 (ID)。設定するパスをドロップダウンメニューから選択します。
Volumes	選択した LUN ボリュームの読み取り専用の名前。
Text box	使用可能なパスの HBA、SID、および状態を示すテキスト行。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、入力項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「iSCSI Configuration」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「iSCSI Configuration」の各パネルにあるフィールドおよび要素について説明します。

- 339 ページの「「Add/Edit iSCSI Access」ウィンドウ」
- 340 ページの「「Add/Edit iSCSI LUN」ウィンドウ」
- 342 ページの「「Configure Access List」パネル」
- 342 ページの「「Configure iSCSI LUN for MS-Exchange」パネル」
- 343 ページの「「Configure iSNS Server」パネル」

「Add/Edit iSCSI Access」ウィンドウ

このウィンドウでは、iSCSI (Internet Small Computer Systems Interface) アクセスリストを作成または編集できます。作成または編集のどちらであるかは、「Add」または「Edit」のどちらをクリックしてこのウィンドウにアクセスしたかに依存します。iSCSI アクセスリストは、どの iSCSI イニシエータに論理ユニット番号 (LUN) へのアクセス権を付与するかを定義します。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-26 「Add/Edit iSCSI Access」 ウィンドウのフィールドおよび要素

フィールド	説明
Name	アクセスリストの名前。この名前は 1 文字以上で、英数字 (a ~ z、A ~ Z、0 ~ 9)、ピリオド (.)、ハイフン (-)、またはコロン (:) を指定できます。
CHAP Initiator Name	iSCSI イニシエータソフトウェアで構成されているチャレンジハンドシェイク認証プロトコル (CHAP) イニシエータの完全な名前。 Windows iSCSI クライアントのデフォルトの CHAP イニシエータ名の例を、次に示します。 <code>iqn.1991-05.com.microsoft:iscsi-winxp</code> このフィールドを空白にすると、CHAP 承認は不要になります。詳細は、iSCSI イニシエータのマニュアルを参照してください。
CHAP Initiator Password	CHAP イニシエータのパスワード。
Initiator IQN Name	イニシエータの iSCSI 修飾名 (IQN) の名前。このフィールドを空白にすると、すべてのイニシエータがターゲットにアクセスできるようになります。 この名前は 1 文字以上で、英数字 (a ~ z、A ~ Z、0 ~ 9)、ピリオド (.)、ハイフン (-)、またはコロン (:) を指定できます。  これをクリックすると、イニシエータの IQN 名が、ターゲット LUN にアクセスできるイニシエータのリストに追加されます。
Initiator IQN List	ターゲット LUN にアクセスできるイニシエータのリスト。  このボタンは、選択したイニシエータに関連付けられたターゲット LUN がアクティブでない場合にのみ使用可能です。これをクリックすると、選択したイニシエータがリストから削除されます。この場合、そのイニシエータは LUN にアクセスできなくなります。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Add/Edit iSCSI LUN」 ウィンドウ

このウィンドウでは、iSCSI (Internet Small Computer Systems Interface) の論理ユニット番号 (LUN) を作成または編集できます。作成または編集のどちらであるかは、「Add」または「Edit」のどちらをクリックしてこのウィンドウにアクセスしたかに依存します。iSCSI イニシエータは iSCSI LUN にアクセスできます。

iSCSI LUN を追加または編集する前に、LUN のアクセスリストを必ず作成してください。詳細は、55 ページの「iSCSI アクセスリストの作成」を参照してください。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-27 「Add/Edit iSCSI LUN」 ウィンドウのフィールドおよび要素

フィールド	説明
Name	<p>iSCSI LUN の名前。この名前は 1 文字以上で、英数字 (a ~ z、A ~ Z、0 ~ 9)、ピリオド (.)、ハイフン (-)、またはコロン (:) を指定できます。</p> <p>指定するターゲット名の先頭には、次に示す命名規則に従って、完全な iSCSI 修飾名 (IQN) が付与されます。</p> <p><code>iqn.1986-03.com.sun:01:mac-address.timestamp.user-specified-name</code></p> <p>たとえば、名前 <code>lun1</code> を入力する場合、iSCSI ターゲットの LUN の完全な名前は次のようになります。</p> <p><code>iqn.1986-03.com.sun:01:mac-address.timestamp.lun1</code></p> <p>注: <code>timestamp</code> は、1970 年 1 月 1 日からの経過秒数を表す 16 進数です。</p>
Alias	(省略可能) ターゲット LUN に関する簡単な説明。
Volume	iSCSI LUN を作成するボリュームの名前。
Capacity	バイト、K バイト、M バイト、または G バイト単位の LUN の最大サイズ。
Sparse	<p>スパース LUN を作成する場合は「Yes」チェックボックスを選択します。スパース LUN では、ファイルサイズ属性は指定された容量に設定されますが、ディスクブロックはデータがディスクに書き込まれるまで割り当てられません。詳細は、56 ページの「iSCSI のスパース LUN について」を参照してください。</p> <p>スパースでない LUN を作成する場合は、作成する LUN の容量に基づいてディスクブロックが割り当てられます。スパースでない iSCSI LUN を作成するときは、ファイルシステムのメタデータ用にボリュームに約 10% の追加領域を用意します。たとえば、100G バイトのスパースでない iSCSI LUN を作成する場合、その LUN が 110G バイトのボリュームに存在するようにしてください。</p> <p>スパース LUN とスパースでない LUN のどちらを使用するかの決定方法の詳細は、56 ページの「iSCSI のスパース LUN について」を参照してください。</p>
Access	ドロップダウンリストから、この LUN 用の既存のアクセスリストを選択します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Configure Access List」 パネル

このパネルでは、論理ユニット番号 (LUN) にアクセスできる iSCSI (Internet Small Computer Systems Interface) イニシエータを定義するアクセスリストを作成できます。また、既存のアクセスリストの表示、編集、および削除も行うことができます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-28 「Configure Access List」 パネルのフィールドおよび要素

フィールド	説明
Name	アクセスリストの名前。
CHAP Initiator Name	iSCSI イニシエータソフトウェアで構成されているチャレンジハンドシェイク認証プロトコル (CHAP) イニシエータの完全な名前を入力します。Windows iSCSI クライアントのデフォルトの CHAP イニシエータ名の例を、次に示します。 <code>iqn.1991-05.com.microsoft:iscsi-winxp</code> このフィールドを空白にすると、CHAP 承認は不要になります。詳細は、iSCSI イニシエータのマニュアルを参照してください。
Add	これをクリックすると、「Add iSCSI Access」ウィンドウが表示されます。このウィンドウから、新しいアクセスリストを追加できます。
Remove	これをクリックすると、選択したアクセスリストが「Configure Access List」の表から削除されます。
Edit	これをクリックすると、「Edit iSCSI Access」ウィンドウが表示されます。このウィンドウから、選択したアクセスリストを編集できます。

「Configure iSCSI LUN for MS-Exchange」 パネル

このパネルでは、iSCSI イニシエータがアクセスできる iSCSI (Internet Small Computer Systems Interface) 論理ユニット番号 (LUN) を追加できます。また、既存の iSCSI LUN の表示、編集、および削除もできます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-29 「Configure iSCSI LUN for MS-Exchange」 パネルのフィールドおよび要素

フィールド	説明
Name	iSCSI LUN の名前。
Alias	ターゲット LUN に関する簡単な説明。

表 F-29 「Configure iSCSI LUN for MS-Exchange」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Volume	iSCSI LUN を作成するボリュームの名前。
Add	これをクリックすると、「Add iSCSI LUN」 ウィンドウが表示されます。このウィンドウから、新しい iSCSI LUN を追加できます。
Remove	これをクリックすると、選択した iSCSI LUN が「Configure Access List」の表から削除されます。
Edit	これをクリックすると、「Edit iSCSI LUN」 ウィンドウが表示されます。このウィンドウから、選択した iSCSI LUN を編集できます。

「Configure iSNS Server」 パネル

このパネルでは、ソフトウェアで使用される iSNS (Internet Storage Name Service) サーバーを指定できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-30 「Configure iSNS Server」 パネルのフィールドおよび要素

フィールド	説明
iSNS Server	iSNS サーバーのインターネットプロトコル (IP) アドレスまたはドメインネームサービス (DNS) 名。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Monitoring and Notification」 のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「Monitoring and Notification」の各パネルにあるフィールドおよび要素について説明します。

- 344 ページの「「Configure SNMP」 パネル」
- 345 ページの「「Configure System Auditing」 パネル」
- 345 ページの「「Display System Log」 パネル」
- 346 ページの「「Set Up Email Notification」 パネル」

- 347 ページの「「Set Up Logging」パネル」
- 348 ページの「「Set Up UPS Monitoring」パネル」
- 349 ページの「「View Fan Status」パネル」
- 349 ページの「「View File Volume Usage」パネル」
- 350 ページの「「View Power Supply Status」パネル」
- 350 ページの「「View Temperature Status」パネル」
- 351 ページの「「View Voltage Regulator Status」パネル」

「Configure SNMP」パネル

このパネルでは、SNMP (Simple Network Management Protocol) 監視を構成できます。SNMP は、さまざまなネットワークデバイスの動作を調整するための業界標準規格です。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-31 「Configure SNMP」パネルのフィールドおよび要素

フィールド	説明
Enable SNMP	システムの SNMP 監視を使用可能にする場合にクリックします。
Server SNMP Community Name	システムが属する SNMP コミュニティの名前。
Contact Info	このシステムの管理者の名前。
System Location	システムのネットワーク上の場所。物理的な場所または論理的な場所のいずれでもかまいません。
Destination IP Address	システムエラーの発生時に、SNMP トラップの宛先として指定するサーバーの、TCP/IP (Transmission Control Protocol/Internet Protocol) アドレス。
Port #	システムがトラップを送信するポート。デフォルトの値は、ポート 162 です。
Version	SNMP プロトコルのバージョン (1 または 2)。
Community	トラップの宛先のコミュニティ文字列。
Enable	このターゲットアドレスをトラップの宛先にできるようにする場合にクリックします。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Configure System Auditing」パネル

このパネルでは、システム監査を構成できます。特定のシステムイベントの記録が個別の監査ログファイルに格納されるように、システム監査を設定できます。

注: Web Administrator グラフィカルユーザーインターフェースでは、監査ログの読み取りまたは削除はサポートされていません。監査ログファイルの読み取りを行うには、`praudit` コマンドを使用します。このコマンドを実行すると、監査ログのバイナリ情報が読み取り可能なテキストに変換されます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-32 「Configure System Auditing」パネルのフィールドおよび要素

フィールド	説明
Enable System Auditing	システム監査を使用可能にする場合に選択します。
<i>Log File Configuration</i>	
Store Log Files to Volume	システム監査ログファイルを格納するボリューム。 注: システムボリューム以外のボリュームを指定できます。専用の監査ボリュームを作成してください。詳細は、46 ページの「「Create File Volumes」パネルを使用したファイルボリュームまたはセグメントの作成」を参照してください。
Max Log File Size (1 to 1024)	システム監査ログファイルを拡張できる最大サイズ。1 ~ 1024M バイトのサイズを指定します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Display System Log」パネル

このパネルでは、システムログメッセージを選択的に表示、印刷、および保存できます。システムソフトウェアは、次のイベントタイプを記録および表示します。

- 緊急 (Emergency)
- 警告 (Alert)
- 重大 (Critical)
- エラー (Error)
- 警告 (Warning)
- 通知 (Notice)
- 情報 (Information)

■ デバッグ (Debug)

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-33 「Display System Log」 パネルのフィールドおよび要素

フィールド	説明
File	参照するログファイルの名前。システムログファイルを参照する場合は、このフィールドを空白にします。
Date	イベントが発生した日付。
Time	イベントが発生した時刻 (24 時間形式)。
Description	イベントの説明を記述するテキスト行。
Event Types	このパネルに表示するイベントのタイプをクリックします。選択したイベントタイプのみが表示されるようにログファイルを更新するには、「Refresh」をクリックします。
Refresh	これをクリックすると、ログが最新の情報で更新されます。
Print	これをクリックすると、ログが印刷されます。
Save As	これをクリックすると、ログが HTML ファイルとしてローカルシステム上に保存されます。
Open	これをクリックすると、別のログファイルが開き、このパネルに表示されます。
Silence Alarm	このボタンは Sun StorageTek 5210 システムでのみ使用可能です。これをクリックすると、RAID (Redundant Array of Independent Disk) アラームが表示されなくなります。

「Set Up Email Notification」 パネル

このパネルでは、メール転送プロトコル (SMTP) サーバーの名前を設定し、電子メール通知の受信者を指定することができます。システムエラーが発生すると、システムは SMTP サーバーを介して、指定された受信者に詳細な電子メールメッセージを送信します。

受信者の電子メールアドレスは「List」ボックスに表示されます。エラーが検出されると、システムによってそのエラーがシステムログファイルに記録され、リストに示されている受信者に電子メール通知および警告が送信されます。

注: 構成ウィザードからこのパネルにアクセスしている場合は、「Next」をクリックして変更内容を保存してから、次のパネルに進んでください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-34 「Set Up Email Notification」 パネルのフィールドおよび要素

フィールド	説明
SMTP Server Name	SMTP サーバーの名前。
Mail From	送信者の電子メールアドレス。
Email Address	受信者の電子メールアドレス。
Notification	電子メール受信者に通知を送信する場合にクリックします。
Diagnostics	電子メール受信者に診断情報を送信する場合にクリックします。
<i>List</i>	
	これをクリックすると、受信者のリストに新しい受信者が追加されます。
	これをクリックすると、選択した受信者が受信者リストから削除されます。
Recipient	受信者の電子メールアドレス。
Notification	電子メール受信者に通知を送信する場合にクリックします。
Diagnostics	電子メール受信者に診断情報を送信する場合にクリックします。
<i>Notification Level</i>	
Errors	受信者にシステムエラーを通知するが、システム警告は通知しない場合に選択します。
Errors and Warnings	すべてのシステム警告およびエラーを受信者に通知する場合に選択します。
None	電子メール通知を使用不可にする場合に選択します。Sun StorageTek サーバーはどの通知も送信しなくなります。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Up Logging」 パネル

このパネルでは、システムのロギングを設定できます。システムに `syslogd` UNIX サーバーが構成されている場合は、遠隔ロギングを使用可能にできます。

遠隔ロギングを使用可能にする前に、次の条件を満たす必要があります。

- システムがこの遠隔 syslogd サーバーにシステムログを送信できる必要があります。詳細は、33 ページの「ロギングの設定」を参照してください。
- DNS 設定が構成されている必要があります。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-35 「Set Up Logging」パネルのフィールドおよび要素

フィールド	説明
Enable Remote Syslogd	システムメッセージロガーとその指定サーバーを使用可能にする場合にクリックします。
Server	システムログが送信されるサーバーの名前。
機能	ログメッセージを生成するアプリケーションまたはシステムコンポーネント。syslogd サーバーに送信されるすべてのメッセージには、この機能の値が指定されます。ログメッセージを生成するイベントのタイプを選択します。 <ul style="list-style-type: none"> • 緊急 (Emergency) • 警告 (Warning) • 警告 (Alert) • 注意 (Notice) • 重大 (Critical) • 情報 (Info) • エラー (Error) • デバッグ (Debug)
Enable Local Log	ローカルシステムロギングを使用可能にして、システムがログメッセージをローカルに保存できるようにする場合にクリックします。
Local File	システムログのパスおよびファイル名。/cvol ディレクトリにはログを書き込めません。
Archives	アーカイブファイルの最大数。1～9 の数を指定します。
Size	各アーカイブファイルに許容される最大サイズ。K バイト単位で指定します。指定可能な範囲は 100K～999,999K バイトです。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Up UPS Monitoring」パネル

このパネルでは、無停電電源装置 (UPS) 監視を設定できます。UPS 管理は設定できません。監視可能な UPS イベントに関する情報は、158 ページの「UPS 監視について」を参照してください。

注: このパネルで UPS 監視を使用可能にする場合は、事前に UPS 監視サービスをシステムに接続してください。これが接続されていないと、UPS 監視システムは UPS 障害を通知します。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-36 「Set Up UPS Monitoring」パネルのフィールドおよび要素

フィールド	説明
Enable UPS Monitoring	システムの UPS 監視を使用可能にする場合にクリックします。適切に動作するには、UPS 監視サービスがシステムに接続されている必要があります。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「View Fan Status」パネル

このパネルでは、システムの本体装置にある各ファンアセンブリの状態と 1 分あたりの回転数 (RPM) を表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-37 「View Fan Status」パネルのフィールドおよび要素

フィールド	説明
Fan	状態を表示するファン。
Status	ファンの状態の視覚的インジケータ: <ul style="list-style-type: none">• 緑色のひし形 – このファンの RPM は正常です。• 赤いひし形 – このファンの RPM は許容範囲を超えています。いずれかのファンで 1 分あたりの回転数が 1800 未満になると、指定された電子メール受信者に電子メール通知が送信されます。電子メール通知の設定については、32 ページの「電子メール通知の設定」を参照してください。
RPM	ファンの RPM 数。

「View File Volume Usage」パネル

このパネルでは、各 Sun StorageTek ファイルボリュームの使用状況を表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-38 「View File Volume Usage」パネルのフィールドおよび要素

フィールド	説明
Name	ファイルボリュームの名前。
Capacity	ファイルボリュームの使用済み容量および使用可能な空き容量のグラフィカル表示。
Volume Status	ボリュームの状態。読み取り/書き込みの「r/w」または読み取り専用の「r/o」のいずれかです。
Requests	ボリュームがマウントされてから、そのボリュームに対して処理された要求の数。
Active	直前の 10 分間にそのボリュームに対して処理された要求の数。

「View Power Supply Status」パネル

このパネルでは、システムのすべての電源装置に関する現在の状態を表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-39 「View Power Supply Status」パネルのフィールドおよび要素

フィールド	説明
Power Supply	状態を表示する電源装置。
Status	電源装置の状態の視覚的インジケータ: <ul style="list-style-type: none">• 緑色のひし形 — この電源装置の電圧および温度レベルは正常です。• 赤いひし形 — 電圧および温度レベルが許容範囲を超えています。指定された電子メール受信者に、この状態を通知する電子メールが送信されます。電子メール通知の設定については、32 ページの「電子メール通知の設定」を参照してください。
Description	電源装置の状態を記述するテキスト行。

「View Temperature Status」パネル

このパネルでは、システムの本体装置内にあるセンサーの温度を表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-40 「View Temperature Status」 パネルのフィールドおよび要素

フィールド	説明
Sensor	状態を表示するセンサー。
Status	センサーの状態の視覚的インジケータ: <ul style="list-style-type: none">• 緑色のひし形 — センサーが正常な温度範囲内で動作しています。• 赤いひし形 — 温度が許容範囲を超えています。温度が 55 °C (131 ° F) を超えると、指定した電子メール受信者に電子メールが送信されます。電子メール通知の設定については、32 ページの「電子メール通知の設定」を参照してください。
値	センサーの温度。

「View Voltage Regulator Status」 パネル

このパネルでは、システム上の電圧調整器の現在の値を表示できます。電圧調整器は、マイクロプロセッサに供給される電圧を調整するデバイスまたは回路です。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-41 「View Voltage Regulator Status」 パネルのフィールドおよび要素

フィールド	説明
Voltage Regulator	状態を表示する電圧調整器。
Status	電圧調整器の状態の視覚的インジケータ: <ul style="list-style-type: none">• 緑色のひし形 — この電圧調整器の電圧レベルは正常です。• 赤いひし形 — この電圧調整器の電圧レベルが許容範囲を超えています。指定された電子メール受信者に、この状態を通知する電子メールが送信されます。電子メール通知の設定については、32 ページの「電子メール通知の設定」を参照してください。
Current Value	マイクロプロセッサに現在供給されている電圧数。

「Network Configuration」 のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「Network Configuration」の各パネルにあるフィールドおよび要素について説明します。

- 352 ページの「「Bond NIC Ports」 パネル」

- 353 ページの「「Configure Network Adapters」パネル」
- 357 ページの「「Create/Edit Port Bond」ウィンドウ」
- 359 ページの「「Set Gateway Address」パネル」
- 359 ページの「「Set Server Name」パネル」
- 360 ページの「「Set Up DNS」パネル」
- 361 ページの「「View the Routing Table」パネル」

「Bond NIC Ports」パネル

このパネルでは、ネットワークインタフェースカード (NIC) のポート結合を追加、編集、削除、および回復できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-42 「Bond NIC Ports」パネルのフィールドおよび要素

フィールド	説明
Bond ID	この結合の一意の NIC ポート結合の指定。
Type	<p>結合のタイプ。次のいずれかを指定できます。</p> <ul style="list-style-type: none"> • Port aggregation – 「チャンネル結合」または「トランキング」とも呼ばれます。NIC ポートを結合してネットワーク入出力を拡大できます。これによって、帯域幅の狭い 2 つ以上のチャンネルから、帯域幅の広い単一ネットワークチャンネルを形成できます。ポート結合には、2 つ以上の使用可能な NIC ポートが必要です。 注: 集約結合に含まれる NIC ポートは、すべて同じタイプ (たとえば、Fast Ethernet と Fast Ethernet) のインタフェースカードのポートで、同じサブネットに接続されており、隣接するポートに接続されている必要があります。スイッチを使用するシステムでは、ポート結合またはチャンネル結合をサポートするスイッチを使用してください。 • High availability – NIC ポートのフェイルオーバーが提供されます。複数の NIC ポートを、バックアップポートとして一次ポートに結合できます。一次ポートに障害が発生すると、ソフトウェアは、高可用性結合ポートのリストの一番上にあるバックアップポートに自動的に切り替えます。また、そのポートに障害が発生すると、リスト内の次のポートが順に使用されます。 注: 高可用性結合の NIC は、同じタイプのインタフェースカードである必要はなく、同じサブネットに接続されている必要もありません。

表 F-42 「Bond NIC Ports」パネルのフィールドおよび要素 (続き)

フィールド	説明
Status	<p>カラーコードで示される状態:</p> <ul style="list-style-type: none"> • 正常 (緑色) • フェイルオーバー (黄色) • 停止 (赤) – これは、ポートに障害が発生した場合、高可用性結合の一次ポートとスレーブポートに障害が発生した場合、またはフェイルオーバーが失敗した場合に表示されます。
IP Address	ポート結合用に指定されるインターネットプロトコル (IP) アドレス。
Subnet Mask	結合に関連付けられるサブネットマスク。
Broadcast Address	結合に関連付けられるブロードキャストアドレス。
Slaves	結合に含まれるスレーブポート。
Create	これをクリックすると、「Create Port Bond」ウィンドウが表示されます。このウィンドウから、新しいポート結合を作成できます。
Edit	これをクリックすると、「Edit Port Bond」ウィンドウが表示されます。このウィンドウから、選択したポート結合を編集できます。
Remove	これをクリックすると、選択したポート結合が表から削除されます。
Recover	NIC ポートのフェイルオーバーから回復する場合にクリックします。「Recover」をクリックすると、回復処理が開始されます。回復を試みる前に、障害が発生した NIC ポートをオンラインにしてください。

「Configure Network Adapters」パネル

このパネルでは、システムに対して動的ホスト構成プロトコル (DHCP) を構成するか、各ネットワークコントローラのインターネットプロトコル (IP) アドレス、ネットマスク、およびブロードキャストを指定できます。また、このパネルを使用して、各ネットワークインタフェースカード (NIC) の IP エイリアスを追加することもできます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-43 「Configure Network Adapters」 パネルのフィールドおよび要素

フィールド	説明
Enable DHCP	DHCP を使用可能にする場合にクリックします。DHCP を使用すると、システムは DHCP サーバーから IP アドレスを動的に取得できます。静的 IP アドレス、サブネットマスク、またはゲートウェイ IP、あるいはそれらすべてを手動で構成する場合は、このチェックボックスを選択しないでください。
Adapter	既存の NIC ポートのリスト。すでにポート結合が作成されている場合は、そのポート結合がこのメニューに表示されます。結合されていないポートは「Port x」というラベルで示されるのに対し、結合されているポートは「Bond x」というラベルで示されます。 注: ポートが結合されている場合、各ポートのエイリアス IP アドレスは作成できませんが、代わりに結合に対してエイリアスを作成します。たとえば、ポート 2 とポート 3 を結合して結合 1 を形成した場合、ポート 2 またはポート 3 にはエイリアス IP アドレスを追加できません。結合 1 のみにエイリアスを追加できます。
IP Address	「Adapters」メニューで選択した NIC ポートのプライマリ IP アドレス。
Netmask	IP アドレスのどの部分がネットワークアドレスを識別し、どの部分がホストアドレスを識別するかを示すインジケータ。
Broadcast	「Adapters」メニューで選択した NIC ポートの読み取り専用のブロードキャストアドレス。ブロードキャストアドレスは、ブロードキャストメッセージをサブネットに送信する際に使用される IP アドレスです。

表 F-43 「Configure Network Adapters」パネルのフィールドおよび要素 (続き)

フィールド	説明
Role	<p data-bbox="615 244 1326 296">「Adapters」メニューで選択した NIC ポートの NIC での役割。有効な役割は次のとおりです。</p> <ul data-bbox="615 305 1326 1305" style="list-style-type: none"> <li data-bbox="615 305 1326 638"> <p data-bbox="615 305 1326 638">• Primary — アクティブなネットワークポートであることを示す NIC ポートの役割で、フェイルオーバー処理の一部として統合されます。ネットワークアダプタにこの役割を割り当てると、パートナー本体 (本体 2) が、このアダプタに割り当てられた IP アドレスをバックアップ用エイリアス IP アドレスとして保持します。パートナー本体にエイリアス IP アドレスを指定すると、その逆の状態になります。パートナーの IP アドレスが、この本体 (本体 1) によってバックアップ用エイリアス IP アドレスとして保持されません。フェイルオーバーが発生すると、健全な本体はパートナー本体のエイリアス IP アドレスを使用可能にします。これによって、障害が発生した本体が依然として動作中であるかのように、ネットワークアクセスを継続できます。</p> <p data-bbox="615 644 1326 808">注: サーバー 2 台構成 (本体 2 台) システムでは、ハートビート NIC の役割は <code>private</code> です。File Replicator オプションが使用可能になっているサーバー 2 台構成のシステムでは、指定した NIC ポートの役割は <code>Mirror</code> になります。高可用性結合に含まれる NIC ポートには、<code>Main</code> または <code>Bkup1</code> ~ <code>Bkup7</code> の役割を割り当てることができます。</p> <li data-bbox="615 817 1326 1038"> <p data-bbox="615 817 1326 1038">• Independent — アクティブなネットワークポートであることを示す NIC ポートの役割ですが、フェイルオーバー処理には使用されません。<code>Independent</code> の NIC ポートは通常、遠隔バックアップに使用されます。<code>Independent</code> の NIC ポートを集約したり、エイリアス IP アドレスをこのポートに追加したりすることはできません。<code>Independent</code> の役割を割り当てる NIC ポートの数に制限はありませんが、1 台の本体に 1 つだけ割り当ててをお勧めします。</p> <li data-bbox="615 1046 1326 1156"> <p data-bbox="615 1046 1326 1156">• Mirror — このオプションは、サーバー 2 台構成のシステムでのみ使用可能です。ファイルボリュームをミラー化するために、このサーバーをほかのサーバーに接続するポートであることを示す NIC ポートの役割です。</p> <li data-bbox="615 1164 1326 1305"> <p data-bbox="615 1164 1326 1305">• Private — このオプションは Sun StorageTek 5320 NAS Cluster Appliance の構成でのみ選択できます。ハートビート用に予約される NIC ポートの役割です。これは、もう 1 台のサーバー (本体) の状態を定期的に監視する専用ネットワークリンクです。<code>Private</code> ポートは各サーバー (本体) に 1 つのみです。</p>

表 F-43 「Configure Network Adapters」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Interface	<p>選択した NIC ポートに適用される、インタフェース固有の情報で、次の項目を指定します。</p> <ul style="list-style-type: none"> • Description — 選択したアダプタの説明を記述するテキスト行。 • H/W Address — 16 進形式で示される、一意のハードウェア (H/W) アドレスまたはメディアアクセス制御 (MAC) アドレス。このネットワークカードをネットワーク上のほかのカードと区別するためにネットワークソフトウェアで使用されます。このアドレスは、出荷時にネットワークカード上で符号化されています。 • Speed — ネットワーク上のデータ転送速度 (M ビット/秒)。 • MTU/Max MTU — 選択したアダプタの現在の最大転送単位 (MTU)。MTU は物理媒体上で送信できるフレームの最大長です。MTU に指定できる最大値はデフォルト値の 1500 です。最小値には 512 を使用することをお勧めします。TCP の最大セグメントサイズは、IP の最大データグラムサイズから 40 を引いた値です。デフォルトでは、IP の最大データグラムサイズは 576 です。デフォルトでは、TCP の最大セグメントサイズは 536 です。
Statistics	<p>選択した NIC ポートに関する入出力 (I/O) 情報:</p> <ul style="list-style-type: none"> • Packets In/Out — この NIC ポートの入出力パケット数。 • Errors In/Out — この NIC ポートの入出力エラー数。 • Collisions — この NIC ポートの転送衝突数。 • Clear Counters — これをクリックすると、「Statistics」タブ上のすべてのカウント、つまりパケット、エラー、および衝突のカウントが消去されます。
IP Aliases	<p>選択した NIC ポートに適用されるエイリアス IP アドレス。サーバー 1 台構成のシステムでは最大 9 つ、サーバー 2 台構成のシステムでは最大 4 つのエイリアスを設定できます。サーバー 2 台構成のシステムの場合のみ、必要に応じて、パートナー本体の対応するポートのプライマリ IP アドレスをこのフィールドに入力できます。</p>
Partner IP Aliases	<p>このフィールドはサーバー 2 台構成のシステムでのみ使用可能です。必要に応じて、パートナー本体の対応するポートのプライマリ IP アドレスを入力します。このフィールドには、バックアップ用に予約されているパートナー本体の IP アドレスが表示されます。これらは、フェイルオーバーの発生時に、正常な本体によって使用可能にされる IP アドレスです。</p>
	<p>これをクリックすると、「IP Aliases」フィールドで入力した値が、使用可能な IP エイリアスのリストに移動します。</p>

表 F-43 「Configure Network Adapters」パネルのフィールドおよび要素 (続き)

フィールド	説明
	これをクリックすると、選択した IP エイリアスが、使用可能な IP エイリアスのリストから削除されます。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Create/Edit Port Bond」ウィンドウ

このウィンドウでは、2 つ以上のネットワークインタフェースカード (NIC) ポート間の結合を作成または編集できます。この結合は、ポート集約結合または高可用性結合のどちらかになります。

ポート集約結合では、ポートを結合することで、より広い帯域幅のポートが生成されます。このタイプの結合に含まれる NIC は、すべて同じタイプ (たとえば、Fast Ethernet と Fast Ethernet) のインタフェースカードで、同じサブネットに接続されている必要があります。高可用性結合では、ポートを結合することで、ポートのフェイルオーバー (NIC ポートの冗長性) が生成されます。このタイプの結合では、NIC は異なるタイプのインタフェースカードでもよく、異なるサブネットに接続されていてもかまいません。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-44 「Create/Edit Port Bond」ウィンドウのフィールドおよび要素

フィールド	説明
IP Address	ポート結合用に指定されるインターネットプロトコル (IP) アドレス。
Subnet Mask	このフィールドは DHCP が使用不可の場合にのみ使用可能です。ポート結合に追加する最初の NIC ポートのサブネットマスクを指定します。
Broadcast Address	結合に関連付けられるブロードキャストアドレス。このブロードキャストアドレスは、「NIC Ports in This Bond」フィールドに示される最初の NIC ポート (一次ポート) で使用されます。

表 F-44 「Create/Edit Port Bond」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Port Aggregation	<p>「チャンネル結合」または「トランキング」とも呼ばれる結合のタイプ。NIC ポートを結合してネットワーク入出力を拡大できます。これによって、帯域幅の狭い2つ以上のチャンネルから、帯域幅の広い単一ネットワークチャンネルを形成できます。ポート結合には、2つ以上の使用可能な NIC ポートが必要です。</p> <p>注: 集約結合に含まれる NIC ポートは、すべて同じタイプ (たとえば、Fast Ethernet と Fast Ethernet) のインタフェースカードのポートで、同じサブネットに接続されており、隣接するポートに接続されている必要があります。スイッチを使用するシステムでは、ポート結合またはチャンネル結合をサポートするスイッチを使用してください。</p>
High Availability	<p>NIC ポートのフェイルオーバーを提供するポート結合のタイプ。複数の NIC ポートを、バックアップポートとして一次ポートに結合できます。一次ポートに障害が発生すると、ソフトウェアは、高可用性結合ポートのリストの一番上にあるバックアップポートに自動的に切り替えます。また、そのポートに障害が発生すると、リスト内の次のポートが順に使用されます。</p> <p>注: 高可用性結合の NIC は、同じタイプのインタフェースカードである必要はなく、同じサブネットに接続されている必要もありません。</p>
Available NIC Ports	<p>結合に使用できる NIC ポート。</p> <p>上のボタンをクリックすると、選択したポートが「Available NIC Ports」ボックスから「NIC Ports in This Bond」ボックスに移動します。下のボタンをクリックすると、選択したポートが「NIC Ports in This Bond」ボックスから「Available NIC Ports」ボックスに移動します。</p>
	
NIC Ports in This Bond	<p>すでにこの結合に含まれているポート。</p> <p>高可用性結合タイプの場合は、上矢印ボタンと下矢印ボタンを使用してポートの順序を整理します。「NIC Ports in This Bond」リストの最初のポートが一次ポートとなります。2つめのポートは、フェイルオーバーが発生した場合に最初に使用されるポートです。リスト内の次のポートは、その前のポートにもまた障害が発生した場合に使用されます。</p>
	
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Set Gateway Address」 パネル

このパネルでは、Sun StorageTek のゲートウェイアドレスを指定できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-45 「Set Gateway Address」 パネルのフィールドおよび要素

フィールド	説明
Gateway	システムのゲートウェイアドレス。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Server Name」 パネル

このパネルでは、ネットワーク上の Sun StorageTek サーバーに関する基本情報を構成できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-46 「Set Server Name」 パネルのフィールドおよび要素

フィールド	説明
Server Name	ネットワーク上で Sun StorageTek サーバーの識別に使用される名前。サーバー名には、英字 (a ~ z、A ~ Z) から始まる名前を指定します。英数字 (a ~ z、A ~ Z、0 ~ 9)、 「-」 (ダッシュ)、および 「.」 (ピリオド) を使用できます。
Company Name	このシステムから送信される診断電子メールメッセージに含める会社名。
Contact Name	このシステムから送信される診断電子メールメッセージに含める連絡先の名前。
Contact Phone #	このシステムから送信される診断電子メールメッセージに含める連絡先の電話番号。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Up DNS」パネル

このパネルでは、ドメイン名の指定や DNS サーバーの追加または削除など、ドメインネームサービス (DNS) のネームサービスを設定できます。

注: 動的 DNS を使用せずに DNS を使用する場合は、このパネルで値を入力する前に、システムのホスト名とインターネットプロトコル (IP) アドレスを DNS データベースに追加してください。動的 DNS を使用する場合は、DNS データベースを手動で更新する必要はありません。詳細は、DNS のマニュアルを参照してください。

注: 構成ウィザードからこのパネルにアクセスしている場合は、「Next」をクリックして変更内容を保存してから、次のパネルに進んでください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-47 「Set Up DNS」パネルのフィールドおよび要素

フィールド	説明
Enable DNS	システム上で DNS を使用可能にする場合に選択します。
Domain Name	DNS ドメイン名。これは、ネットワーク上でドメインの識別に使用される名前です。
Server	ネットワークに対して使用可能にする DNS サーバーの IP アドレス。
Server List	ネットワークに対して使用可能である既存の各 DNS サーバー。リストの一番上にある DNS サーバーは、ドメインの名前解決の際に最初に照会されます。
	これをクリックすると、「Server」フィールドに入力したサーバーエントリが「Server List」メニューに移動します。
	これをクリックすると、選択したサーバーが「Server List」メニューから削除されます。
	これをクリックすると、選択したサーバーが「Server List」メニュー内で 1 つ上の位置に移動します。
	これをクリックすると、選択したサーバーが「Server List」メニュー内で 1 つ下の位置に移動します。

表 F-47 「Set Up DNS」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Enable Dynamic DNS	動的 DNS クライアントが DNS ネームスペースにシステムを追加できるようにする場合に選択します。動的 DNS を使用可能にする場合は、401 ページの「「Configure Domains and Workgroups」パネル」で、Kerberos レルムおよび鍵配布センター (KDC) サーバーも構成してください。セキュリティ保護されていない動的更新が DNS サーバーによって許可されている場合に、動的 DNS を使用可能にすると、セキュリティ保護されていない動的更新が自動的に実行されます。
DynDNS User Name	セキュリティ保護された動的 DNS 更新を実行するために、動的 DNS クライアントが認証できる Windows 2000 ユーザーのユーザー名。このユーザーは、401 ページの「「Configure Domains and Workgroups」パネル」で指定された Active Directory サービス (ADS) ドメインおよび Kerberos レルム内に存在する必要があります。 注: このフィールドにドメイン管理者のユーザー名が表示されても、ADS の更新が失敗する場合は、ドメインコントローラでドメイン管理者のパスワードを変更してください。パスワードの変更は、管理者ユーザーの場合にのみ必要です。また、同じパスワードを再利用することもできます。詳細は、Microsoft のサポートサービスの Web サイトで「文書番号 Q248808」を参照してください。
DynDNS Password	DynDNS ユーザーのパスワード。このフィールドを更新する場合、パスワード全体を削除してから新しいパスワードを入力します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「View the Routing Table」パネル

このパネルでは、ネットワークルートに関する次の情報を表示できます。

表 F-48 「View the Routing Table」 パネルのフィールドおよび要素

フィールド	説明
Destination	宛先のインターネットプロトコル (IP) アドレス。ネットワークまたはホストのいずれかを指定できます。デフォルトルート (0.0.0.0 など) が 1 つ、ループバックルート (127.0.0.1 など) が 1 つ、ネットワークルートが 1 つ以上、およびホストルートが 1 つ以上存在する必要があります。
Gateway	パケットが宛先に送信される際に経由するゲートウェイアドレス。
Mask	宛先ネットワークのネットマスク。

表 F-48 「View the Routing Table」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Interface	ネットワーク上でのパケット送信に使用されるインタフェースのタイプ。
Flags	ルート状態のインジケータ。状態表示の各タイプは、16 進形式の数で表されます。いくつかの一般的なフラグとその意味を次に示します。 <ul style="list-style-type: none">• 0x1 – ルートは使用可能です。• 0x2 – 宛先はゲートウェイです。• 0x4 – 宛先はホストエントリです。• 0x8 – ホストまたはネットワークが到達不可能です。• 0x10 – 宛先が動的に作成されました。• 0x20 – 宛先が動的に変更されました。 フラグには、個々のフラグの合計を示すものもあります。たとえば 0x3 は、ルートが使用可能である (0x1) ことと、ゲートウェイである (0x2) ことを示します。

「RAID」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「RAID」の各パネルにあるフィールドおよび要素について説明します。

- 362 ページの「「Add Hot Spare」ウィンドウ」
- 363 ページの「「Add LUN」ウィンドウ」
- 365 ページの「「Locate Drive Tray」ウィンドウ」
- 365 ページの「「Locate Drive」ウィンドウ」
- 366 ページの「「Manage RAID」パネル」
- 367 ページの「「View Controller/Enclosure Information」パネル」
- 368 ページの「「View LUN Information」パネル」

「Add Hot Spare」ウィンドウ

このウィンドウでは、Sun StorageTek 5320 NAS Appliance または Cluster システムに対して、ドライブをホットスペアとして指定できます。これを行うには、指定するドライブイメージをクリックします。

次の表で、このウィンドウのドライブイメージおよびボタンについて説明します。

表 F-49 「Add Hot Spare」ウィンドウのドライブイメージおよびボタン

ドライブ	意味
	このスロットのドライブは、ホットスペアとして使用できます。
	このスロットのドライブは、ホットスペアとしてすでに選択されています。
	このスロットにドライブは存在しません。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Add LUN」ウィンドウ

このウィンドウでは、システム構成に論理ユニット番号 (LUN) を追加できます。

注: このウィンドウから新しい LUN を追加するには、その LUN に含めるドライブを選択してください。これを行うには、ウィンドウに表示されている各ドライブイメージをクリックします。3 つ以上のドライブを選択してください。次の表に示すように、ドライブイメージには各ドライブの状態が示されます。

表 F-50 「Add LUN」 ウィンドウのドライブ状態のインジケータ

ドライブ	意味
	このスロットのドライブは、LUN メンバーシップに使用できます。
	このスロットのドライブは、LUN メンバーシップにすでに選択されています。
	このスロットにドライブは存在しません。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-51 「Add LUN」 ウィンドウのフィールドおよび要素

フィールド	説明
<i>New LUN Assignments</i>	
RAID Level	RAID (Redundant Array of Independent Disk) の構成。
Controller	LUN を追加するコントローラの番号。
Head Id	このフィールドはサーバー 2 台構成のシステムでのみ使用可能です。このサーバー (本体) に割り当てられる一意の識別子です。
Create New Volume	この LUN に新しいボリュームを作成する場合に選択します。ボリュームの作成には LUN 全体が使用されます。新しいボリュームの名前をフィールドに入力してください。
Grow Existing Volume	この LUN を使用して既存のボリュームにディスク容量を追加し、セグメントを作成および配置する場合に選択します。次に、拡張するボリュームをプルダウンメニューから選択します。
None	名前を割り当てずに新しい LUN を作成する場合に選択します。
Apply	これをクリックすると、変更内容が保存されます。

表 F-51 「Add LUN」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Locate Drive Tray」 ウィンドウ

このウィンドウでは、ストレージレイ内のドライブトレイの物理的な位置を確認し、そのドライブトレイを特定できます。このウィンドウでドライブトレイの位置を確認すると、ドライブトレイ内のすべてのドライブで、適切なインジケータ LED が点滅します。

次の表で、このウィンドウのドライブイメージおよびボタンについて説明します。

表 F-52 「Locate Drive Tray」 ウィンドウのイメージおよびボタン

ドライブ	意味
	ストレージレイ内のドライブトレイを検索する場合にクリックします。
	ドライブトレイの位置を確認する場合にクリックします。選択したドライブトレイまたはドライブのインジケータ LED が点滅します。
	ドライブトレイの位置を確認したあとで、ドライブトレイまたはドライブのインジケータ LED の点滅を停止する場合にクリックします。
Cancel	これをクリックすると、ウィンドウが閉じます。

「Locate Drive」 ウィンドウ

このウィンドウでは、ドライブのインジケータ LED をアクティブにして、ドライブトレイ内の 1 つ以上のドライブの物理的な位置を確認し、それらのドライブを特定できます。

次の表で、このウィンドウのドライブイメージおよびボタンについて説明します。

表 F-53 「Locate Drive」ウィンドウのドライブ状態インジケータ

ドライブ	意味
	ドライブトレイ内でこのドライブを検索する場合にクリックします。
	ドライブの位置を確認する場合にクリックします。選択したドライブのインジケータ LED が点滅します。
	ドライブの位置を確認したあとで、ドライブのインジケータ LED の点滅を停止する場合にクリックします。
Cancel	これをクリックすると、ウィンドウが閉じます。

「Manage RAID」パネル

このパネルでは、Sun StorageTek RAID (Redundant Array of Independent Disk) アレイを管理できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-54 「Manage RAID」パネルのフィールドおよび要素

フィールド	説明
Legend	Sun StorageTek RAID アレイのグラフィカル表示で示すことのできる内容は、次のとおりです。 <ul style="list-style-type: none">• 黒 — ドライブがスロット内に存在しません。• 緑 — ドライブがスロット内に存在し、機能しています。• オレンジ — ホットスペアドライブからデータがコピーされています。• 黄 — LUN が作成されています。• 赤 — ドライブに障害が発生しました。• ピンク — ドライブが交換されました。
Capacity	選択した LUN 上で記憶領域として使用できる合計容量。
Status	LUN 内のドライブの状態。
Raid Level	RAID の構成。

表 F-54 「Manage RAID」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Lun Owner	LUN を所有するユーザー。
Remove LUN	選択した LUN を Sun StorageTek RAID アレイから削除する場合にクリックします。
Add LUN	このボタンは、Sun StorageTek RAID アレイで 3 つ以上のドライブが使用可能な場合にのみ使用できます。これをクリックすると、「Add LUN」 ウィンドウが表示されます。このウィンドウから、Sun StorageTek RAID アレイに LUN を追加できます。
Remove HS	ホットスペアを Sun StorageTek RAID アレイから削除する場合にクリックします。
Add HS	これをクリックすると、「Add Hot Spare」 ウィンドウが表示されません。このウィンドウから、Sun StorageTek RAID アレイにホットスペアを追加できます。
Locate Drive	ドライブの位置を確認する場合にクリックします。このオプションをクリックすると、そのドライブの LCD インジケータが点滅します。
Locate Drive Tray	ドライブトレイの位置を確認する場合にクリックします。このオプションをクリックすると、そのドライブトレイの LCD インジケータが点滅します。

「View Controller/Enclosure Information」 パネル

このパネルでは、システム内のコントローラまたは格納装置に関する情報を表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-55 「View Controller/Enclosure Information」 パネルのフィールドおよび要素

フィールド	説明
Controller Information	Sun StorageTek RAID (Redundant Array of Independent Disk) アレイ内のコントローラのリスト。
Vendor	コントローラのベンダーの名前。
Model	コントローラのモデル番号。
Firmware Release	コントローラのファームウェアのリリースレベル。
<i>Enclosure Information</i>	
Tray IDs	格納装置に関連付けられているトレイ ID のリスト。

表 F-55 「View Controller/Enclosure Information」 パネルのフィールドおよび要素
(続き)

フィールド	説明
Vendor	格納装置のベンダーの名前。
Model	格納装置のモデル番号。
Firmware Release	格納装置のファームウェアのリリースレベル。

「View LUN Information」 パネル

このパネルでは、システム内の論理ユニット番号 (LUN) を表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-56 「View LUN Information」 パネルのフィールドおよび要素

フィールド	説明
LUNs	システム内の LUN のリスト。
Vendor	LUN のベンダーの名前。
Product	LUN 製品。
Product Revision	LUN 製品のバージョン。
Size	LUN のサイズ。
ID Type	LUN で使用される識別子のタイプ。
Vendor ID	LUN のベンダーの識別子。
Vendor Specific ID	ベンダー固有の識別子。
Vendor Specific ID Extension	ベンダー固有の識別子の拡張子。

「System Activity」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「System Activity」の各パネルにあるフィールドおよび要素について説明します。

- 369 ページの「「View Networking Activity」パネル」
- 369 ページの「「View System Activity」パネル」

「View Networking Activity」 パネル

このパネルでは、すべての Sun StorageTek クライアントの 1 秒あたりの入出力要求数を表示できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-57 「View Networking Activity」 パネルのフィールドおよび要素

フィールド	説明
Clients	Sun StorageTek クライアントのインターネットプロトコル (IP) アドレス。
Requests	1 秒あたりの入出力要求数。

「View System Activity」 パネル

このパネルでは、システムと、システムが通信する周辺デバイスとの間で送信される、1 秒あたりの入出力要求数を表示できます。このパネルに表示できる周辺デバイスは次のとおりです。

- CPU — システムの中央処理装置 (CPU)
- Memory — システムのランダムアクセスメモリー (RAM)
- Port Aggregation x — ポート集約 x
- Controller x — RAID コントローラ x
- dac1d0xx — 論理ユニット番号 (LUN) xx
- PORTx — ネットワークインタフェースカード (NIC) ポート x
- Host Adapter x — iSCSI (Internet Small Computer Systems Interface) ホストアダプタ x (テープバックアップデバイス用)

注: 監視されるデバイスの名前および番号は、Sun StorageTek のハードウェア構成によって異なります。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-58 「View System Activity」 パネルのフィールドおよび要素

フィールド	説明
デバイス	システムと通信する周辺デバイス。
Load	デバイスの現在の負荷。1 秒あたりの入出力要求数で表されます。
Peak	デバイスの最大負荷。

「System Backup」のパネル

この節では、Web Administrator の「System Backup」パネルのフィールドおよび要素について説明します。

「Set Up NDMP」パネル

このパネルでは、ネットワークベースのバックアップのオープンなプロトコルである NDMP (Network Data Management Protocol) に対するアーキテクチャーを設定できます。NDMP アーキテクチャーによって、ネットワーク接続ストレージのベンダーは、NDMP 準拠の任意のバックアップ管理アプリケーションとともに使用できる NDMP 準拠のサーバーを出荷することができます。NDMP を使用する場合、ローカルバックアップは使用できません。

注: NDMP を使用する場合は、ユーザー名「administrator」と、コンソール (コマンド行インタフェース) 管理者で使用されるパスワードを使用してログオンできるように、バックアップ管理アプリケーションを構成してください。

注: NDMP を使用してボリュームをバックアップする場合は、チェックポイントを使用可能にしてください。詳細は、165 ページの「ファイルのチェックポイントの作成」を参照してください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-59 「Set Up NDMP」パネルのフィールドおよび要素

フィールド	説明
NDMP NIC	システム内のアダプタ、結合、およびインターネットプロトコル (IP) アドレス。選択したアダプタまたは結合が NDMP に使用されません。 <ul style="list-style-type: none">• Adapter – NDMP NIC アダプタの名前。• IP Address – アダプタの IP アドレス。
Gateway	選択した NDMP NIC のゲートウェイアドレス。NDMP バックアップテープデバイスが別のネットワークに存在する場合は、適切なゲートウェイに接続する NIC を必ず選択してください。
NDMP Log	NDMP ロギング用のフルパス。このパスでは、NDMP によって使用される NDMP ログファイルとその他の一時データファイルが格納されるディレクトリを指定します。このパスは有効なシステムボリューム上に存在する必要があります。また、NDMP が機能するために、そのボリュームを書き込み可能にしてください。
Apply	これをクリックすると、変更内容が保存されます。

表 F-59 「Set Up NDMP」パネルのフィールドおよび要素 (続き)

フィールド	説明
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「System Manager」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「System Manager」の各パネルにあるフィールドおよび要素について説明します。

- 371 ページの「「Edit NFS Export」ウィンドウ」
- 372 ページの「「Server Properties」ウィンドウ」
- 372 ページの「「Volume Properties」ウィンドウ」

「Edit NFS Export」ウィンドウ

このウィンドウでは、選択した NFS エクスポートのアクセス権と、スーパーユーザーに対する UID マッピングを更新することができます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-60 「Edit NFS Export」ウィンドウのフィールドおよび要素

フィールド	説明
Hosts	選択したエクスポートが定義されているホスト。
Access	
Read/Write	エクスポートに読み取り/書き込みアクセス権限を割り当てる場合に選択します。
Read/Only	エクスポートに読み取り専用アクセス権限を割り当てる場合に選択します。
No Access	エクスポートにアクセス権限を割り当てない場合に選択します。
Map Root User	
Anonymous User	スーパーユーザー (UID が 0 のユーザー) のユーザー ID (UID) を、匿名ユーザー (ユーザー nobody) のユーザー ID に対応付ける場合に選択します。
Root User	スーパーユーザーがスーパーユーザーの UID (uid=0) を使用するよう設定する場合に選択します。

表 F-60 「Edit NFS Export」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Map to UID	スーパーユーザーの UID を、このフィールドで指定する UID に対応付ける場合に選択します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「Server Properties」 ウィンドウ

このウィンドウでは、Sun StorageTek サーバーの基本プロパティを表示できません。このウィンドウを開くには、「System Manager」の下でボリューム名を右クリックします。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-61 「Server Properties」 ウィンドウのフィールドおよび要素

フィールド	説明
Name	サーバーの名前。
Model	サーバーのモデル番号。
Serial #	サーバーのシリアル番号。
OS Version	サーバーで使用されるオペレーティングシステムのバージョン。
Cancel	これをクリックすると、ウィンドウが閉じます。

「Volume Properties」 ウィンドウ

このウィンドウでは、選択したボリュームのプロパティを表示できます。このウィンドウを開くには、「System Manager」を右クリックして「Properties」を選択します。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-62 「Edit Volume Properties」 ウィンドウのフィールドおよび要素

フィールド	説明
Label	ボリュームのラベル。
Checkpoints	ボリュームに対してチェックポイントが使用可能かどうかが表示されます。
Quotas	ボリュームに対して割り当てが使用可能かどうかが表示されます。
Capacity	ボリューム上の記憶領域の合計容量。記憶領域の使用状況を示すグラフィカル表示は、次のとおりです。 <ul style="list-style-type: none">• Used – ボリューム上の使用済み容量。• Free – ボリューム上で記憶領域として使用できる空き容量。
<i>Partitions</i>	
Legend	選択した LUN 構成のグラフィカル表示でのインジケータ： <ul style="list-style-type: none">• オレンジ – ボリューム上の一次パーティションを示します。• 水色 – ボリューム上のセグメント化されたパーティションを示します。• 緑色 – ボリューム上のミラーを示します。• 青色 – ボリュームに DOS の読み取り専用属性が適用されていることを示します。この DOS の読み取り専用属性は、システムボリュームのフラッシュディスクでのみ使用されます。• 白色 – ボリューム上の空き領域を示します。
Enable Attic	削除されたファイルを、このボリュームのルートにある <code>.attic\$</code> ディレクトリに一時的に保存する場合に選択します。このオプションはデフォルトで使用可能に設定されています。 ビジー状態のファイルシステム上でまれに、削除処理が終了する前に <code>.attic\$</code> ディレクトリがいっぱいになり、結果として空き領域が不足してパフォーマンスが低下することがあります。このような場合は、このフィールドの選択を解除して、 <code>.attic\$</code> ディレクトリを使用不可にすることをお勧めします。
Lun	選択したボリュームが存在する LUN の名前。
Partition	ボリュームが存在する LUN パーティション。
Use (%)	ボリューム上で使用されている領域の割合。
Type	一次、セグメント化など、ボリュームのタイプ。
Free (MB)	ボリューム上で記憶領域として使用できる空き容量。
Capacity (MB)	ボリューム上の記憶領域の合計容量。
Cancel	これをクリックすると、ウィンドウが閉じます。

「System Operations」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「System Operations」の各パネルにあるフィールドおよび要素について説明します。

- 374 ページの「「Activate Options」パネル」
- 375 ページの「「Add License」ウィンドウ」
- 376 ページの「「Assign Language」パネル」
- 377 ページの「「Enable Temporary Licenses」ウィンドウ」
- 377 ページの「「Import Licenses」ウィンドウ」
- 378 ページの「「Set Administrator Password」パネル」
- 378 ページの「「Set Remote Access」パネル」
- 379 ページの「「Set Time and Date」パネル」
- 380 ページの「「Set Up Time Synchronization」パネル」
- 382 ページの「「Shut Down the Server」パネル」
- 383 ページの「「Update Software」パネル」

「Activate Options」パネル

このパネルでは、システム上の既存ライセンスの表示、システムへのライセンスの追加、システムからのライセンスの削除、およびシステム上での一時ライセンスの使用可能への切り替えを行うことができます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-63 「Activate Options」パネルのフィールドおよび要素

フィールド	説明
Module	ライセンス追加可能なモジュールの名前。
State	ライセンスが有効かどうかを示されます。
Status	ライセンスがアクティブかどうかを示されます。
Origination	ライセンスがアクティブになった日付。YYYYMMDD 形式で表されます。このフィールドに 00000000 という値が表示される場合、そのライセンスはただちにアクティブになります。 注: この日付は固定クロックに対して検証されます。

表 F-63 「Activate Options」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Expiration	<p>ライセンスが期限切れになる日付。YYYYMMDD 形式で表されます。このフィールドに 00000000 という値が表示される場合、そのライセンスが期限切れになることはありません。</p> <p>注: この日付は固定クロックに対して検証されます。</p>
Key	<p>ライセンスに割り当てられている一意のライセンスキー。</p>
Add	<p>これをクリックすると、「Add License」ウィンドウが表示されます。このウィンドウから、Sun StorageTek サーバーに新しいライセンスを追加できます。</p> <p>注: 固定クロックが初期化されるまでは、システムにライセンスを追加できません。固定クロックは、システムに日付および時刻をはじめて設定したときに初期化されます。詳細は、63 ページの「日付および時刻の手動設定」を参照してください。</p> <p>固定クロックは一度しか設定できないため、必ず時刻を正確に設定してください。時刻および日付を初期設定したあとで、さらに時刻および日付を変更しても、ライセンスは影響を受けません。</p>
Remove	<p>選択したライセンスをシステムから削除する場合にクリックします。</p>
Temporary Licenses	<p>これをクリックすると、「Enable Temporary Licenses」ウィンドウが表示されます。このウィンドウから、システム上で使用可能な任意の一時ライセンスをアクティブにできます。</p>
Import	<p>ファイルからライセンス情報を読み取り (デフォルトのシステムライセンスパスが検索される)、その情報をシステムにインポートする場合にクリックします。</p>

「Add License」ウィンドウ

このウィンドウでは、パラメータを指定してライセンスをシステムに追加できます。

次の表で、このウィンドウのフィールドおよび要素について説明します。

表 F-64 「Add License」ウィンドウのフィールドおよび要素

フィールド	説明
Module	<p>ライセンス追加可能なモジュールの名前。</p>
Origination	<p>時刻が 0000:00 になるとライセンスがアクティブになる日付。</p>

表 F-64 「Add License」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Expiration	時刻が 2359:59 になるとライセンスが期限切れになる日付。 注: 日付は YYYYMMDD 形式で指定されます。特殊な日付文字列「00000000」は、制限がないことを示します。この文字列が開始日として使用されると、ライセンスはただちにアクティブになります。この文字列が有効期限として使用されると、ライセンスは期限切れになることはありません。
Key	ライセンスキー。UUID 形式「XXXXXXXX-XXXX-XXXX-XXXXXXXXXXXXXXXX」で指定します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Assign Language」パネル

このパネルでは、Web Administrator アプリケーションで表示される言語を選択できます。Web Administrator アプリケーションでは Unicode がサポートされています。Unicode は、正式には Unicode 国際文字標準として知られています。これは、国際言語および古典言語の入れ替えおよび表示用のシステムです。

注: 構成ウィザードからこのパネルにアクセスしている場合は、「Next」をクリックして変更内容を保存してから、ウィザードの次のパネルに進んでください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-65 「Assign Language」パネルのフィールドおよび要素

フィールド	説明
Codepage	Sun StorageTek サーバーの言語コードページを選択します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Enable Temporary Licenses」 ウィンドウ

このウィンドウでは、システムで使用可能な一時ライセンスを有効にすることができます。

次の表で、このウィンドウのフィールドおよび要素について説明します。

表 F-66 「Enable Temporary Licenses」 ウィンドウのフィールドおよび要素

フィールド	説明
Module	ライセンス追加可能なモジュールの名前。
Duration	この一時ライセンスが有効になる日数。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Import Licenses」 ウィンドウ

このウィンドウでは、ライセンスをファイルからインポートできます。

注: ライセンス情報をコピー&ペーストするか、手動で入力する方法を選択する場合は、ライセンス情報内に行ブレイクを誤って挿入しないでください。そのようにしないと、行が有効なエントリとして認識されなくなります。

次の表で、このウィンドウのフィールドおよび要素について説明します。

表 F-67 「Import Licenses」 ウィンドウのフィールドおよび要素

フィールド	説明
「Import License」 フィールド	インポートするライセンスのライセンス情報。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。
Browse	ライセンスをファイルからインポートする場合にクリックします。

「Set Administrator Password」 パネル

このパネルでは、システム管理者のパスワードを設定できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-68 「Set Administrator Password」 パネルのフィールドおよび要素

フィールド	説明
Old	システム管理者の既存のパスワード。パスワードが設定されていない場合は、このフィールドを空白のままにします。
New	システム管理者の新しいパスワード。パスワードは、1文字以上、21文字以内で指定してください。管理者のパスワードを使用不可にする場合は、このフィールドを空白のままにします。
Confirm	システム管理者の新しいパスワードをもう一度入力します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Remote Access」 パネル

このパネルでは、Sun StorageTek Filer の遠隔管理に使用されるネットワークサービスを設定できます。使用可能なネットワークサービスは次のとおりです。

- Telnet
- 遠隔ログイン
- リモートシェル
- ハイパーテキスト転送プロトコル (HTTP) 上での Secure Shell、Web Admin
- セキュリティー保護されたハイパーテキスト転送プロトコル (HTTPS) 上での Secure Web Admin

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-69 「Set Remote Access」 パネルのフィールドおよび要素

フィールド	説明
Secure Mode	セキュリティ保護されているとみなされるプロトコルのみを使用可能にする場合にクリックします。この場合、その他のサービスはすべて使用不可になります。セキュリティ保護されているプロトコルは次のとおりです。 <ul style="list-style-type: none">• HTTP 上で SSL (Secure Socket Layer) を使用する Secure Web Admin• Secure Shell (SSH)
Service	Sun StorageTek Filer で使用可能な既存のサービス。
Enabled	Sun StorageTek Filer への遠隔アクセスに使用される、対応するサービスを使用可能にする場合にクリックします。
Comment	サービスの説明を記述するテキスト行。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Time and Date」 パネル

このパネルでは、Sun StorageTek サーバーの時刻および日付を設定できます。

次の表で、このパネルのフィールド、要素、およびボタンについて説明します。

表 F-70 「Set Time and Date」 パネルのフィールドおよび要素

フィールド	説明
Calendar	現在の年、月、および日。グラフィカルな形式で表示されます。現在の年または月を変更するには、カレンダー上の該当するドロップダウンメニューからオプションを選択します。日を更新するには、カレンダー自体をクリックします。
Clock	現在の時刻。グラフィカル形式で表示されます。現在の時刻を変更するには、クロックのすぐ上にあるドロップダウンメニューから新しい時刻を選択します。これらのドロップダウンメニューには、時刻が 24 時間形式で表示されます。たとえば、1 時 30 分は 13:30 として表示されます。

表 F-70 「Set Time and Date」 パネルのフィールドおよび要素 (続き)

フィールド	説明
「Time Zone」 ドロップダウンメニュー	Sun StorageTek サーバーの現在のタイムゾーン。タイムゾーンを変更するには、ドロップダウンメニューから新しいタイムゾーンを選択します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Up Time Synchronization」 パネル

このパネルでは、Sun StorageTek サーバーの時刻を、時間情報プロトコル (NTP) または RDATE サーバーのいずれかと同期をとることができます。NTP は、無線、衛星受信機、モデムなどの基準時刻ソースにコンピュータのクロックを同期化させるために使用されるインターネットプロトコルです。一般的な NTP 構成には、複数台の冗長サーバーおよび各種ネットワークパスが使用できるため、高い精度と信頼性を実現できます。

RDATE 時間プロトコルは、サイトに影響を受けない日付および時刻を提供します。これは、ネットワーク上の別のマシンから時刻を取得できるプロトコルです。RDATE サーバーは一般に UNIX システム上に存在します。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-71 「Set Up Time Synchronization」 パネルのフィールドおよび要素

フィールド	説明
Manual Synchronization	NTP または RDATE の時刻同期をどちらも使用しない場合に選択します。

表 F-71 「Set Up Time Synchronization」パネルのフィールドおよび要素 (続き)

フィールド	説明
NTP Synchronization	<p>NTP 同期を使用する場合に選択します。この場合、ネットワーク上に 1 台以上の NTP サーバーが必要です。NTP 同期に固有のオプションを次に示します。</p> <ul style="list-style-type: none"> • Enable Server 1、Enable Server 2 – いずれかのチェックボックスをクリックして、その NTP サーバーを使用可能にします。最大 2 台の NTP サーバーを使用可能にできます。 • NTP Server – Sun StorageTek サーバーがポーリングによって現在の時刻を取得する NTP サーバーの名前またはインターネットプロトコル (IP) アドレス。 • Auth Type – Sun StorageTek サーバーと NTP サーバーの間で使用される認証のタイプを選択します。認証のサポートにより、Sun StorageTek サーバーは鍵と鍵識別子を使用して、NTP サーバーが既知の信頼できるサーバーであることを確認できます。メッセージを認証するには、NTP サーバーと Sun StorageTek サーバーとの間で鍵と鍵識別子を一致させます。 • Key ID – この NTP サーバーとともに使用される ntp. 鍵ファイルの非公開鍵に関連付ける鍵識別子。「Auth Type」フィールドで「Symmetric Key」を選択した場合にのみ、このフィールドに値を入力する必要があります。「Key ID」の値の有効範囲は 1 ~ 65534 です。 注: 対称鍵による認証を使用する場合は、事前に ntp. 鍵ファイルを \etc ディレクトリにコピーしてください。 • Min Poll Rate – NTP メッセージの最小ポーリング率。この値の 2 乗が、ポーリング間隔の最小秒数を示します。たとえば、6 という値は 36 秒を表します。このフィールドの有効範囲は 4 ~ 17 です。ほとんどのインストール環境では、デフォルト値の 6 で十分です。 • Max Poll Rate – NTP メッセージの最大ポーリング率。この値の 2 乗が、ポーリング間隔の最大秒数を示します。たとえば、4 という値は 16 秒を表します。このフィールドの有効範囲は 4 ~ 17 ですが、最小ポーリング間隔よりも大きい値に設定してください。ほとんどのインストールでは、デフォルト値の 10 で十分です。 • Enable Broadcast Client – Sun StorageTek サーバーが、任意のインタフェースで受信された NTP サーバーのブロードキャストメッセージに応答するように設定する場合にクリックします。これは、サーバーとの時刻同期を必要とする多数のクライアントを持つ 1 台以上の NTP サーバーが存在する構成が対象となります。 • Require Broadcast Server Authentication – Sun StorageTek サーバーにメッセージをブロードキャストしたサーバーが既知の信頼できるサーバーであることが NTP クライアントによって確認されることを必須にする場合にクリックします。

表 F-71 「Set Up Time Synchronization」パネルのフィールドおよび要素 (続き)

フィールド	説明
RDATE Synchronization	<p>Sun StorageTek サーバーとの RDATE サーバーの時刻同期を使用する場合に選択します。RDATE サーバー同期に固有のオプションを次に示します。</p> <ul style="list-style-type: none"> • RDATE Server – RDATE サーバーの名前または IP アドレス。 • Tolerance – Sun StorageTek サーバー上の時刻と、RDATE サーバーから受信する時刻のずれの最大許容範囲。0 ~ 3600 の秒数で指定します。RDATE サーバーの時刻に対する Sun StorageTek サーバーの時刻の遅れまたは進みがこの秒数より小さい場合、Sun StorageTek サーバーの時刻は RDATE サーバーの時刻に同期化されます。誤差がこの秒数より大きい場合は、Sun StorageTek サーバーの時刻は RDATE サーバーの時刻に自動的に同期化されません。この誤差の確認は、毎日午後 11 時 45 分に実行されます。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Shut Down the Server」パネル

このパネルでは、Sun StorageTek サーバーを停止または再起動できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-72 「Shut Down the Server」パネルのフィールドおよび要素

フィールド	説明
None	サーバーの停止も再起動も実行しない場合にクリックします。
Halt both heads	このフィールドはサーバー 2 台構成 (クラスタ) のシステムでのみ使用可能です。クラスタ構成の両方のサーバーを停止する場合にクリックします。クラスタ内の両方のサーバーの状態が NORMAL であることを確認してください。再起動するには、サーバーに手で電源を入れる必要があります。
Reboot both heads	このフィールドはサーバー 2 台構成 (クラスタ) のシステムでのみ使用可能です。クラスタ構成の両方のサーバーを停止して再起動する場合にクリックします。
Halt	このフィールドはサーバー 1 台構成のシステムでのみ使用可能でず。サーバーを停止する場合にクリックします。再起動するには、サーバーに手で電源を入れる必要があります。
Reboot	このフィールドはサーバー 1 台構成のシステムでのみ使用可能でず。サーバーを停止して再起動する場合にクリックします。

表 F-72 「Shut Down the Server」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Reboot Previous Version <i>version-number</i>	<p>サーバーを停止し、旧バージョンのソフトウェアで再起動する場合に選択します。ソフトウェアをアップグレードしても問題が発生した場合に、このオプションを使用します。サーバーは、アップグレードする前に最後に使用されていたソフトウェアで再起動します。</p> <p>クラスタ構成では、クラスタ内の本体ごとにこの処理を実行してください。</p> <p>注: このオプションを選択する場合は、事前にテクニカルサポートに問い合わせることをお勧めします。</p>
Halt this head	<p>このフィールドはサーバー 2 台構成のシステムでのみ使用可能です。このサーバー (現在ログオンしているサーバー) を停止する場合にクリックします。もう一方のサーバーはオンラインのままです。再起動するには、サーバーに手で電源を入れる必要があります。</p>
Reboot this head	<p>このフィールドはサーバー 2 台構成のシステムでのみ使用可能です。このサーバー (現在ログオンしているサーバー) を停止して再起動する場合にクリックします。もう一方のサーバーはオンラインのままです。</p>
Apply	<p>これをクリックすると、サーバーの停止または再起動が実行されます。</p>
Cancel	<p>これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。</p> <p>注: サーバーの停止または再起動が開始されてから、その停止または再起動を取り消すことはできません。「Cancel」をクリックしても、このパネルに入力したエントリが削除されるだけです。</p>

「Update Software」 パネル

このパネルでは、Sun StorageTek サーバーの現在の Sun StorageTek 5320 NAS Appliance ソフトウェアのバージョンが表示され、サーバーを新しいバージョンのソフトウェアを使用して更新できます。ソフトウェアを Sun の Web サイトからダウンロードするか、フロッピーまたは CD-ROM ドライブからアップロードして、サーバーを更新できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-73 「Update Software」パネルのフィールドおよび要素

フィールド	説明
The Current OS Version	Sun StorageTek サーバーの Sun StorageTek 5320 NAS Appliance ソフトウェアの現在のバージョン。
<i>Update Server from a File</i>	
Path	ワークステーション上のソフトウェアファイルのフルパス。Sun の Web サイトから入手可能なこのファイルを使用して、Sun StorageTek サーバー上の Sun StorageTek 5320 NAS Appliance ソフトウェアバージョンを更新できます。
Browse	ワークステーションからインストールするソフトウェアファイルを特定する場合にクリックします。
Update	選択したファイルからのソフトウェアのアップロードを実行する場合にクリックします。アップロード処理が完了すると、サーバーの再起動を求めるプロンプトが表示されます。再起動するには「Yes」、再起動せずに続行するには「No」をクリックします。ソフトウェアの更新は、システムを再起動するまで行われません。

「UNIX Configuration」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「UNIX Configuration」の各パネルにあるフィールドおよび要素について説明します。

- 385 ページの「「Add/Edit Comment」ウィンドウ」
- 385 ページの「「Add/Edit Host」ウィンドウ」
- 386 ページの「「Add/Edit NFS Export」ウィンドウ」
- 387 ページの「「Add Hostgroup」ウィンドウ」
- 388 ページの「「Add Hostgroup Member」ウィンドウ」
- 388 ページの「「Configure Exports」パネル」
- 390 ページの「「Configure Name Services」パネル」
- 391 ページの「「Set Up FTP」パネル」
- 392 ページの「「Set Up Hostgroups」パネル」
- 393 ページの「「Set Up Hosts」パネル」
- 393 ページの「「Set Up NIS」パネル」
- 394 ページの「「Set Up NIS+」パネル」
- 395 ページの「「Set Up NSSLDAP」パネル」

「Add/Edit Comment」 ウィンドウ

このウィンドウでは、ネットワークファイルシステム (NFS) エクスポートに関するコメントを追加または編集できます。追加または編集のどちらであるかは、388 ページの「**Configure Exports**」パネルで「Add」または「Edit」アイコンのどちらをクリックしてこのウィンドウにアクセスしたかに依存します。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-74 「Add/Edit Comment」 ウィンドウのフィールドおよび要素

フィールド	説明
Add Comment	NFS エクスポートに関するテキスト行。80 文字までの長さで指定します。# 文字でコメントテキストを始めるか、# 文字を削除して空白行を追加することができます。
Ok	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「Add/Edit Host」 ウィンドウ

このウィンドウでは、ホストを追加または編集できます。追加または編集のどちらかは、「Add」または「Edit」のどちらをクリックしてこのウィンドウにアクセスしたかに依存します。



注意: ホストに「信頼できる」の状態を割り当てる場合には注意が必要です。信頼できるホストは **Sun StorageTek** ファイルシステムにスーパーユーザーの権限でアクセスできるため、そのファイルシステムでの管理機能を実行できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-75 「Add/Edit Host」 ウィンドウのフィールドおよび要素

フィールド	説明
Host Name	ホストの名前。ホスト名には、英数字 (a ~ z、A ~ Z、0 ~ 9)、ダッシュ (-)、およびピリオド (.) を指定できます。先頭の文字は、英字 (a ~ z または A ~ Z) にします。
IP Address	ホストのインターネットプロトコル (IP) アドレス。
Trusted	ホストが信頼できるかどうかを指定します。信頼できるホストは、 Sun StorageTek ファイルシステムにスーパーユーザーの権限でアクセスできます。
Apply	これをクリックすると、変更内容が保存されます。

表 F-75 「Add/Edit Host」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Add/Edit NFS Export」 ウィンドウ

388 ページの「「Configure Exports」 パネル」の「Add」または「Edit」アイコンをクリックするか、「System Manager」項目を右クリックしてから適切な「Add Export」メニューオプションを選択することによって、ネットワークファイルシステム (NFS) エクスポートを追加または編集できます。

NFS エクスポートはボリューム全体にのみ追加できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-76 「Add/Edit NFS Export」 ウィンドウのフィールドおよび要素

フィールド	説明
Volume	このフィールドは、「Configure Exports」パネルで「Add」をクリックした場合にのみ使用可能です。NFS エクスポートを追加または編集するボリュームを選択します。ボリューム全体のみを選択できます。
Path	このフィールドは、「Configure Exports」パネルで「Add」をクリックした場合にのみ使用可能です。UNIX NFS ホストにアクセス権を付与するディレクトリを指定します。このフィールドを空白のままにすると、ボリューム全体が選択されます。
Full Path	ボリューム上のエクスポート済みディレクトリのフルパス。
Access	
Read/Write	指定したホストに、選択したボリュームに対する読み取り/書き込み権を付与する場合に選択します。
Read/Only	指定したホストに、選択したボリュームに対する読み取り専用アクセス権を付与する場合に選択します。
No Access	指定したホストに、選択したボリュームに対するアクセス権を付与しない場合に選択します。
Map Root User	
Anonymous User	このエクスポートで、スーパーユーザーのユーザー ID を匿名ユーザーのユーザー ID に割り当てる場合に選択します。
Root User	このエクスポートで、スーパーユーザーのユーザー ID をスーパーユーザーのユーザー ID (UID=0) に割り当てる場合に選択します。

表 F-76 「Add/Edit NFS Export」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Map to UID	このエクスポートで、スーパーユーザーに対して使用される特定のユーザー ID を割り当てる場合に選択し、そのユーザー ID を入力します。
<i>Hosts</i>	
Host Netgroups	このフィールドは追加モードでのみ編集可能です。ネットグループの NFS エクスポートを定義する場合に選択します。エクスポートを割り当てるネットグループをドロップダウンメニューから選択します。
Host Group	このフィールドは追加モードでのみ編集可能です。ホストグループの NFS エクスポートを定義する場合に選択します。プルダウンメニューから、すべてのホストを示す「general」、すべての信頼できるホストを示す「trusted」、またはユーザー定義のホストグループを選択します。
Known Host	このフィールドは追加モードでのみ編集可能です。「Set Up Hosts」パネルで追加したホストへのエクスポートを定義する場合に選択します。エクスポートを割り当てるホストをドロップダウンメニューから選択します。
Other Host	このフィールドは追加モードでのみ編集可能です。「Set Up Hosts」パネルで追加していない個々のホストへのエクスポートを定義する場合に選択します。右のフィールドにホストの名前を入力します。
Ok	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「Add Hostgroup」 ウィンドウ

このウィンドウでは、ホストグループを構成に追加できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-77 「Add Hostgroup」 ウィンドウのフィールドおよび要素

フィールド	説明
Add Hostgroup	追加するホストグループの名前。この名前には、英数字 (a ~ z、A ~ Z、0 ~ 9)、ダッシュ (-)、およびピリオド (.) を指定できます。先頭の文字は、英字 (a ~ z または A ~ Z のみ) にする必要があります。
Apply	これをクリックすると、変更内容が保存されます。

表 F-77 「Add Hostgroup」 ウィンドウのフィールドおよび要素 (続き)

フィールド	説明
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「Add Hostgroup Member」 ウィンドウ

このウィンドウでは、選択したホストグループにメンバーを追加できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-78 「Add Hostgroup Member」 ウィンドウのフィールドおよび要素

フィールド	説明
Host Netgroups	このオプションを選択して、メンバーとして追加する、外部 NIS サーバー上で定義されているネットグループを選択します。
Host Group	このオプションを選択して、メンバーとして追加するホストグループを選択します。
Known Host	メンバーとして追加する、「Set Up Hosts」パネルから手動で追加したホスト、または外部 NIS サーバー上に存在するホストを選択します。
Other Host	メンバーとして追加する、「Set Up Hosts」パネルから追加していないホストを入力します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、変更内容を保存せずにウィンドウが閉じます。

「Configure Exports」 パネル

このパネルでは、指定されたボリュームに対する UNIX ユーザーのアクセス権限を指定できます。このパネルの表には、各エクスポートのアクセス可能ディレクトリ、ホスト名、およびアクセスレベル (読み取り/書き込みまたは読み取り専用) など、現在のネットワークファイルシステム (NFS) エクスポートの情報が表示されます。

「@」で始まるホスト名は、ホストのグループを示します。たとえば、「@general」というホスト名は、すべてのホストを含む定義済みホストグループを示します。「@trusted」というホスト名は、信頼できるホストを含む定義済みホストグループを示します。

「&」で始まるホスト名は、ホストネットグループを示します。たとえば、「&group1」は「netgroup, group1」を示します。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-79 「Configure Exports」パネルのフィールドおよび要素

フィールド	説明
Full Path	UNIX NFS にアクセス権限を付与するディレクトリのフルパス。
Host	ボリュームに対するアクセス権限を持つホストの名前。
Access	ボリュームに対するホストのアクセス権のレベル。アクセス権には、読み取り/書き込みの「R/W」または読み取り専用の「R/O」を指定できます。
Map Root User	スーパーユーザーのユーザー ID のマッピング方法。詳細は、121 ページの「エクスポートの作成」を参照してください。
	これをクリックすると、「Add NFS Export」ウィンドウが表示されます。このウィンドウから、新しい NFS エクスポートを構成に追加できます。
	これをクリックすると、「Add Comment」ウィンドウが表示されません。このウィンドウから、「Configure Exports」表にコメントを追加できます。
	これをクリックすると、「Edit NFS Export」ウィンドウまたは「Edit Comment」ウィンドウが表示されます。このウィンドウから、選択した NFS エクスポートまたはコメントを編集できます。
	これをクリックすると、選択した NFS エクスポートまたはコメントが表から削除されます。
	これをクリックすると、選択した NFS エクスポートまたはコメントが表の一番上に移動します。
	これをクリックすると、選択した NFS エクスポートまたはコメントが表内の 1 つ上の位置に移動します。
	これをクリックすると、選択した NFS エクスポートまたはコメントが表内の 1 つ下の位置に移動します。
	これをクリックすると、選択した NFS エクスポートまたはコメントが表の一番下に移動します。

「Configure Name Services」パネル

このパネルでは、グループ、ネットグループ、ホスト、およびユーザーの検索用関数でネームサービス (NS) が使用される順序を選択できます。NS の検索順序によって、照会を解決するためにネームサービスを検索する順序が制御されます。サポートされるネームサービスは、NIS、NIS+、NSSLDAP、DNS、および Local です。名前解決にネームサービスを使用するには、事前にネームサービスを使用可能にしてください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-80 「Configure Name Services」パネルのフィールドおよび要素

フィールド	説明
Groups Order	これをクリックすると、グループの検索用関数で検索可能なネームサービスが表示されます。
Netgroup Order	これをクリックすると、ネットグループの検索用関数で検索可能なネームサービスが表示されます。
Hosts Order	これをクリックすると、ホストの検索用関数で検索可能なネームサービスが表示されます。
Users Order	これをクリックすると、ユーザーの検索用関数で検索可能なネームサービスが表示されます。
Services Not Selected	検索用関数で使用されない、使用可能なネームサービス。  上のボタンをクリックすると、「Services Not Selected」メニューで選択したネームサービスが「Services Selected」メニューに移動します。下のボタンをクリックすると、「Services Selected」メニューで選択したネームサービスが「Services Not Selected」メニューに移動します。
Services Selected	検索用関数で使用される使用可能なサービスが順に表示されます。これらのサービスを使用可能にしてください。  これらのボタンは、「Services Selected」メニューに複数のネームサービスが表示されている場合のみ使用可能です。上のボタンをクリックすると、選択したネームサービスがリスト内で上に移動します。下のボタンをクリックすると、選択したネームサービスがリスト内で下に移動します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Remove NFS Export」 ウィンドウ

このウィンドウでは、ネットワークファイルシステム (NFS) エクスポートを構成から削除できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-81 「Remove NFS Export」 ウィンドウのフィールドおよび要素

フィールド	説明
Host	ボリュームに対するアクセス権を持つホストの名前。
Access	ボリュームに対するホストのアクセス権のレベル。アクセス権には、読み取り/書き込みの「R/W」または読み取り専用の「R/O」を指定できます。
Apply	これをクリックすると、選択した NFS エクスポートが構成から削除されます。
Cancel	これをクリックすると、変更内容を保存せずにウィンドウが閉じます。

「Set Up FTP」 パネル

このパネルでは、システム上にファイル転送プロトコル (FTP) サービスを設定し、FTP を使用する場合のシステムへのユーザーアクセス権を定義できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-82 「Set Up FTP」 パネルのフィールドおよび要素

フィールド	説明
Enable FTP	システム上で FTP を使用可能にする場合に選択します。FTP サービスを使用可能にすると、FTP サーバーは受信した接続要求を受け入れます。
Allow Guest Access	匿名ユーザーによる FTP サーバーへのアクセスを可能にする場合に選択します。
Allow User Access	すべてのユーザーによる FTP サーバーへのアクセスを可能にする場合に選択します。このチェックボックスの選択を解除すると、admin ユーザーとスーパーユーザーだけが FTP サーバーにアクセスできます。
Allow Admin Access	すべてのスーパーユーザーによる FTP サーバーへのアクセスを可能にする場合に選択します。ユーザーは、Sun StorageTek の特別な admin ユーザーであるか、ユーザー識別子 (UID) が 0 に等しい場合にスーパーユーザーとみなされます。

表 F-82 「Set Up FTP」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Enable Logging	FTP ロギングを使用可能にする場合に選択します。
Log File Name	このフィールドはロギングが使用可能な場合にのみ使用可能です。FTP ログファイルの名前を指定します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Up Hostgroups」 パネル

このパネルでは、ホストグループデータベースを監視および管理できます。このデータベースでは、グループおよびグループメンバーの追加または削除を行うことができます。ホストグループは、ネットワークファイルシステム (NFS) エクスポートで使用できるホストのコレクションを定義するために使用されます。グループは、定義済みシステムグループとユーザー定義グループで構成されます。定義済みグループには、「信頼できる」と「iso8859」の2つのグループがあります。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-83 「Set Up Hostgroups」 パネルのフィールドおよび要素

フィールド	説明
Groups	「Group Members」メニューにメンバーを表示するグループをドロップダウンメニューから選択します。
	このボタンをクリックすると、「Add Hostgroup」ウィンドウまたは「Add Hostgroup Member」ウィンドウが表示されます。どちらのウィンドウが表示されるかは、パネルの「Groups」セクションまたは「Group Members」セクションのどちらでこのボタンをクリックしたかに依存します。新しいホストグループまたはホストグループメンバーの追加については、92 ページの「ホストグループの追加」または 93 ページの「ホストグループへのメンバーの追加」を参照してください。
	このボタンをクリックすると、選択したホストグループまたは選択したホストグループメンバーが削除されます。どちらが削除されるかは、パネルの「Groups」セクションまたは「Group Members」セクションのどちらでこのボタンをクリックしたかに依存します。
Group Members	選択したホストグループのメンバー。

「Set Up Hosts」 パネル

このパネルでは、システムホストファイルのホストエントリを追加、編集、または削除できます。



注意: ホストに「信頼できる」の状態を割り当てる場合には注意が必要です。信頼できるホストは **Sun StorageTek** ファイルシステムにスーパーユーザーの権限でアクセスできるため、そのファイルシステムでの管理機能を実行できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-84 「Set Up Hosts」 パネルのフィールドおよび要素

フィールド	説明
Host Name	システム上でホストの識別に使用される名前。英字の大文字または小文字、数字、ピリオド (.), またはハイフン (-) のみを使用します。先頭の文字は、英字にする必要があります。
Trusted	ホストが信頼できるかどうかを指定します。信頼できるホストは、 Sun StorageTek ファイルシステムにスーパーユーザーの権限でアクセスできます。
IP Address	ホストのインターネットプロトコル (IP) アドレス。
Add	これをクリックすると、「Add Host」ウィンドウが表示されます。このウィンドウから、システムホストファイルに新しいホストを追加できます。
Remove	これをクリックすると、ホストがシステムホストファイルから削除されます。
Edit	これをクリックすると、「Edit Host」ウィンドウが表示されます。このウィンドウから、選択したホストに関する情報を編集できます。

「Set Up NIS」 パネル

このパネルでは、システムにネットワーク情報サービス (NIS) ネームサービスを設定できます。実行中のネットワークが **Windows** のみで構成されている場合、NIS を設定する必要はありません。

注: 構成ウィザードからこのパネルにアクセスしている場合は、変更を適用してから、「Next」をクリックして次のパネルに進んでください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-85 「Set Up NIS」 パネルのフィールドおよび要素

フィールド	説明
Enable NIS	NIS を使用可能にする場合に選択します。この場合、ホスト、ユーザー、およびグループの情報を NIS データベースからインポートするようにシステムが構成されます。
Domain Name	NIS サービスに使用するドメインの名前。
Server	NIS データベースのインポート元となる NIS サーバーのインターネットプロトコル (IP) アドレスまたは名前。
Check Rate	NIS 情報が更新される頻度 (分単位)。デフォルトは 5 分です。
Use Broadcast	NIS サーバーの名前または IP アドレスを自動的に取得する場合に選択します。このオプションは、NIS ドメイン名がわかっているが、NIS サーバー名が不明な場合に便利です。
Update Hosts	NIS サーバーからシステムにホスト情報をダウンロードする場合に選択します。
Update Users	NIS サーバーからシステムにユーザー情報をダウンロードする場合に選択します。
Update Groups	NIS サーバーからシステムにグループ情報をダウンロードする場合に選択します。
Update Netgroups	NIS サーバーからシステムにネットグループ情報をダウンロードする場合に選択します。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Up NIS+」 パネル

このパネルでは、システムにネットワーク情報サービスプラス (NIS+) ネームサービスを設定できます。実行中のネットワークが Windows のみで構成されている場合、NIS+ を設定する必要はありません。

このパネルで NIS+ を使用可能にする前に、NIS+ サーバーでの構成手順を実行してください。詳細は、30 ページの「NIS+ の設定」を参照してください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-86 「Set Up NIS+」 パネルのフィールドおよび要素

フィールド	説明
Enable NIS+	システム上で NIS+ を使用可能にする場合に選択します。
Home Domain Server	NIS+ ホームドメインサーバーの名前またはインターネットプロトコル (IP) アドレス。
NIS+ Domain	NIS+ ホームドメインの名前。
Secure RPC Password	NIS+ サーバーとの通信を可能にするためにシステムによって使用されるパスワード。
Search Path	NIS+ での情報検索時に検索されるドメイン。NIS+ でホームドメインとその親のみが検索されるようにする場合、このフィールドは空白のままでもかまいません。 たとえば、NIS+ ドメインが <code>eng.sun.com</code> で「Search Path」フィールドが空白の場合、システムの名前解決では、最初に <code>eng.sun.com</code> 、次に <code>sun.com</code> が検索されます。これに対して、「Search Path」の値が <code>sun.com</code> の場合は、システムの名前解決では <code>sun.com</code> のドメインのみが検索されます。
Use Broadcast	NIS+ サーバーの名前または IP アドレスを自動的に取得する場合に選択します。このオプションは、NIS+ ホームドメイン名がわかっているが、NIS+ サーバー名が不明な場合に便利です。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Set Up NSSLDP」 パネル

このパネルでは、ユーザーアカウントの認証を使用可能にする UNIX のサービスである、NSSLDP (Name Service Switch Lightweight Data Access Protocol) を設定できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-87 「Set Up NSSLDP」 パネルのフィールドおよび要素

フィールド	説明
Enable NSSLDP	システムに対して NSSLDP を使用可能にする場合に選択します。
Domain (DN)	LDAP (Lightweight Data Access Protocol) ドメイン名。ドメイン名 (DN) 形式または LDAP 形式で指定します。
Password	NSSLDP サーバー上のバインドパスワード。

表 F-87 「Set Up NSSLDAP」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Server	NSSLDAP サーバーのインターネットプロトコル (IP) アドレス。
Proxy (DN)	NSSLDAP プロキシ (entryDN)。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Windows Configuration」のパネル

この節では、Web Administrator グラフィカルユーザーインターフェースの「Windows Configuration」の各パネルにあるフィールドおよび要素について説明します。

- 396 ページの「「Add/Edit Group」ウィンドウ」
- 397 ページの「「Add/Edit Share」ウィンドウ」
- 399 ページの「「Add/Edit SMB/CIFS User or Group Map」ウィンドウ」
- 400 ページの「「Configure Autohome」パネル」
- 401 ページの「「Configure Domains and Workgroups」パネル」
- 403 ページの「「Configure Groups」パネル」
- 404 ページの「「Configure Mapping Policy」パネル」
- 405 ページの「「Configure Maps」パネル」
- 406 ページの「「Configure Shares」パネル」
- 408 ページの「「Remove Share」ウィンドウ」
- 408 ページの「「Set Up WINS」パネル」
- 409 ページの「「System Status」パネル」

「Add/Edit Group」ウィンドウ

このウィンドウでは、グループを追加または編集できます。追加または編集のどちらであるかは、「Add Group」または「Edit Group」のどちらをクリックしてこのウィンドウにアクセスしたかに依存します。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-88 「Add/Edit Group」ウィンドウのフィールドおよびボタン

フィールド	説明
Group	共有の名前。
Comment	(省略可能) グループの説明を記述する短いテキスト行。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Add/Edit Share」ウィンドウ

「Configure Shares」パネルを使用するか、ナビゲーションパネルの「System Manager」項目を右クリックしてからメニューの適切なオプションを選択することによって、共有を追加および編集できます。

このウィンドウでは、サーバーメッセージブロック (SMB) 共有を追加または編集できます。追加または編集のどちらであるかは、追加モードまたは編集モードのどちらでこのウィンドウにアクセスしたかに依存します。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-89 「Add/Edit Share」ウィンドウのフィールドおよびボタン

フィールド	説明
Old Share Name	このフィールドは、編集モードの場合にのみ使用可能です。共有の現在の名前を入力します。
Share Name	共有の名前。これは、ネットワーク上でユーザーに対して表示される名前です。次の文字は共有名ではサポートされません。 = : ; \ " ? < > * /
Comment	(省略可能) 共有の説明を記述する短いテキスト行。60 文字以内の英数字で入力できます。
Path	このフィールドは、「Configure Shares」パネルで「Add」をクリックしてこのウィンドウにアクセスした場合には使用できません。「Configure Shares」パネルで「Edit」をクリックした場合にのみ編集可能です。選択したボリューム上の共有のフルパスを指定します。

表 F-89 「Add/Edit Share」 ウィンドウのフィールドおよびボタン (続き)

フィールド	説明
Mac Extensions	<p>「Desktop DB Calls」チェックボックスを選択して、システムが Macintosh デスクトップデータベースにアクセスして情報を設定できるようにします。このオプションを使用可能にすると、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システム上の Macintosh クライアントのファイルアクセスが高速化し、Macintosh 以外のクライアントがシステム上の Macintosh ファイルにアクセスできるようになります。</p>
Volume Name	<p>このフィールドは、「Configure Shares」パネルで「Add」をクリックしてこのウィンドウにアクセスした場合にのみ使用可能です。共有するボリュームをドロップダウンメニューから選択します。</p>
Directory	<p>このフィールドは、「Configure Shares」パネルで「Add」をクリックした場合にのみ使用可能です。既存のディレクトリパスを指定します。このフィールドではディレクトリを作成できません。ディレクトリの名前は太文字と小文字が区別されます。このフィールドは空白のままにしないでください。</p> <p>注: ディレクトリを指定しない場合は、ルートレベルの共有が作成されます。</p>
Container	<p>このフィールドは、401 ページの「「Configure Domains and Workgroups」パネル」で共有に対して Active Directory サービス (ADS) を使用可能にした場合にのみ使用できます。(省略可能) 共有を公開する ADS コンテナを指定します。</p> <p>これは、LDAP (Lightweight Directory Access Protocol) の識別名 (DN) 記法で指定される、共有の ADS パスの場所です。ユーザーや共有などのオブジェクトは、「コンテナ」オブジェクトの各レベルを含む階層パスに従って、Active Directory ドメイン内に配置されます。</p> <p>注: 共有の cn (共通名) フォルダまたは ou (組織単位) フォルダをパスとして入力します。cn コンテナは root フォルダ内のデフォルトフォルダです。その他のコンテナはすべて ou フォルダです。たとえば、共有が accounting という組織親フォルダ内の shares 組織フォルダに存在する場合、次のように入力します。</p> <p>ou=shares,ou=accounting</p> <p>パスには、ドメイン名を含めないでください。</p>
User ID	<p>このフィールドは、401 ページの「「Configure Domains and Workgroups」パネル」で、NT ドメインモードではなく Windows ワークグループモードを使用可能にした場合にのみ使用できます。指定されたディレクトリへのアクセスにこの共有を使用するユーザーのユーザー ID を入力します。このフィールドのデフォルト値は 0 (ゼロ) です。これは、UNIX のスーパーユーザーの値です。ただし、この値を割り当てる場合には注意が必要です。Windows ワークグループモードでは、このフィールドに 0 を入力すると、共有内のすべてのファイルおよびディレクトリに対するセキュリティーがすべて使用不可になります。</p>

表 F-89 「Add/Edit Share」 ウィンドウのフィールドおよびボタン (続き)

フィールド	説明
Group ID	このフィールドは、401 ページの「「Configure Domains and Workgroups」 パネル」で、NT ドメインモードではなく Windows ワークグループモードを使用可能にした場合のみ使用できます。指定されたディレクトリへのアクセスにこの共有を使用するユーザーのグループ ID を入力します。このフィールドのデフォルト値は 0 (ゼロ) です。これは、UNIX のスーパーユーザーの値です。ただし、この値を割り当てる場合には注意が必要です。Windows ワークグループモードでは、このフィールドに 0 を入力すると、共有内のすべてのファイルおよびディレクトリに対するセキュリティがすべて使用不可になります。
umask	共有に対するアクセス権パラメータ (3 桁の数字)。共有に対するアクセス権の詳細は、107 ページの「共有へのアクセス権について」を参照してください。
R/W Password	この共有に指定したディレクトリに対する読み取り/書き込みアクセス権のある Windows ワークグループのユーザーのパスワード。
Confirm R/W Password	「R/W Password」フィールドに入力したパスワードを確認するために使用されるフィールド。
R/O Password	共有に対する読み取り専用アクセス権のある Windows ワークグループユーザーのパスワード。
Confirm R/O Password	「R/O Password」フィールドに入力したパスワードを確認するために使用されるフィールド。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Add/Edit SMB/CIFS User or Group Map」 ウィンドウ

このウィンドウでは、SMB/CIFS ユーザーマップまたはグループマップを追加または編集できます。追加または編集のどちらであるかは、405 ページの「「Configure Maps」 パネル」で「Add」または「Edit」のどちらをクリックしてこのウィンドウにアクセスしたかに依存します。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-90 「Add/Edit SMB/CIFS User or Group Map」ウィンドウのフィールドおよびボタン

フィールド	説明
<i>NT Group</i>	
Account	割り当てるユーザーまたはグループの NT アカウント名。
RID	NT ドメイン内で NT ユーザーまたはグループを一意に識別する相対識別子。
<i>Unix Group</i>	
Name	指定した NT ユーザーまたはグループを割り当てる UNIX ユーザーまたはグループの名前。
ID	UNIX ドメイン内で UNIX ユーザーまたはグループを一意に識別する識別子。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、ウィンドウに最初に表示されていた値に戻ります。

「Configure Autohome」パネル

このパネルでは、自動ホーム共有を構成できます。自動ホーム共有は、ユーザーがシステムにログインすると作成され、ログアウトすると削除される、一時的な共有です。詳細は、113 ページの「自動ホーム共有について」を参照してください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-91 「Configure Autohome」パネルのフィールドおよびボタン

フィールド	説明
Enable Autohome	自動ホーム機能を使用可能にする場合に選択します。
Autohome Path	一時共有のベースディレクトリのパス。たとえば、ユーザーのホームディレクトリが /vol1/home/tom の場合、自動ホームパスの値は /vol1/home となります。このフィールドで有効な値を指定する方法については、113 ページの「自動ホーム共有の使用可能への切り替え」を参照してください。

表 F-91 「Configure Autohome」 パネルのフィールドおよびボタン (続き)

フィールド	説明
ADS Container	このフィールドは、401 ページの「「Configure Domains and Workgroups」 パネル」でシステムに対して ADS を使用可能にした場合にのみ使用できます。一時共有を公開できる Active Directory サービス (ADS) コンテナを指定します。このフィールドで有効な値を指定する方法については、113 ページの「自動ホーム共有の使用可能への切り替え」を参照してください。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Configure Domains and Workgroups」 パネル

このパネルでは、Windows NT ドメインまたはワークグループのセキュリティーモデルのいずれかに Windows ネットワーキングを構成できます。

注: セキュリティーモデルを Windows ワークグループモデルと NT ドメインモデルの間で切り替えると、サーバーの自動再起動の確認を求める確認メッセージが表示されます。システムを再起動するには「Yes」をクリックします。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-92 「Configure Domains and Workgroups」 パネル

フィールド	説明
<i>Domain</i>	
Domain	既存のドメインの名前。NetBIOS の 15 文字の制限を超えないドメイン名を指定してください。 注: Active Directory サービス (ADS) を使用可能にする場合は、ADS が動作している Windows 2000 ドメインの名前を入力します。ここでは、システムも属しているドメインを指定してください。

表 F-92 「Configure Domains and Workgroups」 パネル (続き)

フィールド	説明
User Name	<p>既存のドメインユーザーの名前。最大 16 文字のユーザー名を指定できます。</p> <p>ADS を有効にする場合は、このフィールドには管理権限のある Windows 2000 ユーザーの名前を入力してください。このユーザーには、ドメイン管理者か、ドメイン管理者グループのメンバーを指定します。ADS クライアントは、このユーザーによって、セキュリティー保護された ADS の更新を実行します。</p> <p>注: このフィールドにドメイン管理者のユーザー名が表示されても、ADS の更新が失敗する場合は、ドメインコントローラでドメイン管理者のパスワードを変更してください。パスワードの変更は、管理者ユーザーの場合にのみ必要です。また、同じパスワードを再利用することもできます。詳細は、Microsoft のサポートサービスの Web サイトで「文書番号 Q248808」を参照してください。</p>
Password	ドメインユーザーのパスワード。ADS の場合は、Windows 管理者ユーザーのパスワードを入力します。
Enable ADS	Active Directory サービス (ADS) ソフトウェアによって Sun StorageTek 共有を ADS に公開する場合、または ADS から Sun StorageTek 共有を削除する場合に選択します。ADS とその構成方法の詳細は、77 ページの「Active Directory サービスについて」を参照してください。
ADS Information	<p>Active Directory サービス固有の情報:</p> <ul style="list-style-type: none"> • Container – LDAP (Lightweight Directory Access Protocol) の識別名 (DN) 記法で、Windows 2000 管理者ユーザーの ADS のパス位置を入力します。 注: パスには、ドメイン名を含めないでください。 • Site – ローカル ADS NT ドメイン名。ADS の制御に別のサブネットが使用されることを前提とします。ローカル ADS サイトがないか、このパネルで指定したドメインまたはローカル ADS NT ドメインによって同じサブネットが使用される場合は、このフィールドを空白にしてください。
Kerberos Domain Information	<p>Kerberos ドメイン固有の情報:</p> <ul style="list-style-type: none"> • Realm – ADS の識別に使用される Kerberos レルム名 (通常は ADS ドメイン)。これは通常、ADS ドメインまたはドメインネームサービス (DNS) ドメインです。「Apply」をクリックすると、入力した値がすべて大文字に変換されます。 • Server – Kerberos 鍵配布センター (KDC) サーバーのホスト名。通常、これは ADS ドメインのプライマリドメインコントローラのホスト名です。ソフトウェアがドメインネームサービス (DNS) ソフトウェアを介して KDC サーバーを検索できる場合は、このフィールドは空白になります。
Workgroup	
Name	ワークグループの名前。

表 F-92 「Configure Domains and Workgroups」 パネル (続き)

フィールド	説明
Comments	ネットワーク構成を記述するテキスト行。
Apply	これをクリックすると、変更内容が保存されます。Windows NT ドメインの Windows ネットワーキングを構成すると、このシステムのドメイン上にアカウントが自動的に作成されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Configure Groups」 パネル

このパネルでは、ローカルグループを管理できます。権限は個々のユーザーではなく個々のローカルグループに付与されます。

注: ローカルグループは、共通インターネットファイルシステム (CIFS) ネットワークを使用する環境にのみ適用されます。ローカルグループの詳細は、86 ページの「ローカルグループについて」を参照してください。

次の表で、このパネルのフィールドおよび要素について説明します。

表 F-93 「Configure Groups」 パネルのフィールドおよび要素

フィールド	説明
Groups	システムが認識しているグループ。このメニューからグループを選択すると、「Group Members」メニューと「Group Privileges」メニューがそのグループ固有の情報で更新されます。
Group Members	選択したグループのメンバーであるユーザー。グループに対するユーザーの追加および削除については、88 ページの「グループメンバーの追加および削除と権限の構成」を参照してください。
Group Privileges	選択したグループに適用される権限。サポートされるグループ権限の詳細は、86 ページの「ローカルグループの権限の構成について」を参照してください。
Comment	グループの説明を記述するテキスト行。
Apply	これをクリックすると、変更内容が保存されます。
Add Group	これをクリックすると、「Add Group」ウィンドウが表示されます。このウィンドウから、新しいグループを作成できます。詳細は、88 ページの「グループメンバーの追加および削除と権限の構成」を参照してください。

表 F-93 「Configure Groups」 パネルのフィールドおよび要素 (続き)

フィールド	説明
Edit Group	これをクリックすると、「Edit Group」ウィンドウが表示されます。このウィンドウから、選択したグループの名前およびコメントテキストを編集できます。管理者、バックアップオペレータ、およびパワーユーザーのデフォルトグループは編集できません。
Remove Group	これをクリックすると、選択したグループが削除されます。管理者、バックアップオペレータ、およびパワーユーザーのデフォルトグループは削除できません。
Refresh	これをクリックすると、パネルが最新の情報で更新されます。 注: 変更を行なったあと、まだ「Apply」をクリックしていないときに「Refresh」をクリックすると、それらの変更内容がパネルから削除されます。

「Configure Mapping Policy」 パネル

システムに UNIX 環境と Windows 環境の両方が構成されている場合、このパネルで、UNIX のユーザーおよびグループと Windows のユーザーおよびグループとの間に対応関係の規則を確立できます。

ユーザーおよびグループのマッピングポリシーを選択すると、Sun StorageTek 5320 NAS Appliance、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システム上に資格の対応関係が確立され、いずれかの環境を使用した共通のアクセスが提供されます。詳細は、94 ページの「ユーザーおよびグループの資格のマッピングについて」を参照してください。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-94 「Configure Mapping Policy」 パネルのフィールドおよび要素

フィールド	説明
<i>Windows <_> Unix User Mapping Choice</i>	
Default Mapping	Windows ユーザーと UNIX ユーザーの間に定義済みのマッピング規則を確立しない場合に選択します。新しいユーザーには、新しく生成される一意のユーザー識別子がシステムによって割り当てられます。
Map by User Name	同一のユーザー名を持つ UNIX ユーザーと Windows ユーザーを割り当てる場合に選択します。これによって、同じユーザーが両方の環境から Sun StorageTek 5320 NAS Appliance システム、Sun StorageTek 5320 NAS Cluster Appliance、または Sun StorageTek 5320 NAS Gateway システムにアクセスできます。
Map by Full Name	同一のフルネームを持つ UNIX ユーザーと Windows ユーザーを割り当てる場合に選択します。

表 F-94 「Configure Mapping Policy」パネルのフィールドおよび要素 (続き)

フィールド	説明
<i>Windows <_> Unix Group Mapping Choice</i>	
Default Mapping	Windows グループと UNIX グループの間に定義済みのマッピングルールを確立しない場合に選択します。新しいグループには、新しく生成される一意のグループ識別子がシステムによって割り当てられます。
Map by Group Name	同一のフルネームを持つ UNIX グループと Windows グループを割り当てる場合に選択します。
Map to Primary Group	構成済みの passwd ファイルの一次グループフィールドの NFS グループに割り当てる場合に選択します。詳細は、99 ページの「グループマッピングについて」を参照してください。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「Configure Maps」パネル

このパネルでは、UNIX のユーザーおよびグループと Windows のユーザーおよびグループとの既存のマッピングを表示できます。また、UNIX のユーザーおよびグループと Windows のユーザーおよびグループとのマッピングを手動で構成できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-95 「Configure Maps」パネルのフィールドおよび要素

フィールド	説明
Users	これを選択すると、既存のユーザーマッピングが表に表示されます。
Groups	これを選択すると、既存のグループマッピングが表に表示されます。
Unix Name	UNIX 環境で定義されているユーザーまたはグループの名前。
Unix ID	UNIX 環境でユーザーまたはグループに割り当てられている一意の識別子。
Windows Name	Windows 環境で定義されているユーザーまたはグループの名前。
Windows Domain	Windows 環境でユーザーまたはグループが属するドメイン。
Windows RID	Windows 環境でユーザーまたはグループに割り当てられている相対識別子 (RID)。

表 F-95 「Configure Maps」パネルのフィールドおよび要素 (続き)

フィールド	説明
Add	これをクリックすると、「Add SMB/CIFS User Map」ウィンドウまたは「Add SMB/CIFS Group Map」ウィンドウが表示されます。どちらのウィンドウが表示されるかは、「Configure Maps」パネルの上部で「Users」または「Groups」のどちらを選択したかに依存します。このウィンドウから、新しいユーザーマッピングまたはグループマッピングを構成できます。詳細は、101 ページの「Windows のグループおよびユーザーの、UNIX のグループおよびユーザーへのマッピング」を参照してください。
Remove	これをクリックすると、選択したユーザーマッピングまたはグループマッピングが削除されます。ユーザーマッピングまたはグループマッピングのどちらであるかは、「Configure Maps」パネルの上部で「Users」または「Groups」のどちらを選択したかに依存します。
Edit	これをクリックすると、「Edit SMB/CIFS User Map」ウィンドウまたは「Edit SMB/CIFS Group Map」ウィンドウが表示されます。どちらのウィンドウが表示されるかは、「Configure Maps」パネルの上部で「Users」または「Groups」のどちらを選択したかに依存します。このウィンドウから、選択したユーザーマッピングまたはグループマッピングを編集できます。詳細は、102 ページの「Windows のグループまたはユーザーと UNIX のグループまたはユーザーとのマッピングの編集」を参照してください。

「Configure Shares」パネル

このパネルでは、静的なサーバーメッセージブロック (SMB) 共有を追加、表示、および更新できます。

このパネルの上部の表には、システム上の既存のすべての SMB 共有に関する情報が表示されます。これには、Windows ワークグループのみにに関する情報 (ユーザーおよびグループ情報、読み取り/書き込みパスワード、および読み取り専用パスワード) のほかに、共有名や共有されているディレクトリも含まれます。

注: ボリュームを作成したあとで、そのボリュームに対する共有を作成してください。その後、ユーザーはボリュームにアクセスして、ディレクトリを作成することができます。ボリューム上にディレクトリが作成されたあと、そのディレクトリに対する個別の共有を作成できます。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-96 「Configure Shares」 パネルのフィールドおよびボタン

フィールド	説明
Name	共有の名前。これは、ネットワーク上でユーザーが確認できる名前です。この名前は 15 文字以内で入力する必要があります。次の文字はサポートされていません。 = : ; \ " ? < > * /
Path	システム上の共有の位置。
Comment	共有に関する情報。
User	共有を所有するユーザーの名前。
Group	共有を所有するユーザーが属するグループ。
umask	この共有に適用されるファイル生成マスク (存在する場合)。 umask は、共有モードで作成されるファイルおよびディレクトリのセキュリティポリシーを定義します。これによって、ファイルの作成時に使用不可になるアクセス権ビットが指定されます。詳細は、107 ページの「共有へのアクセス権について」を参照してください。
Container	このフィールドは、401 ページの「「Configure Domains and Workgroups」 パネル」で共有に対して Active Directory サービス (ADS) を使用可能にした場合にのみ使用できます。共有が公開される ADS コンテナを指定します。
Desktop DB Calls	システムから Macintosh デスクトップデータベースにアクセスして情報を設定できるかどうかを指定します。このフィールドに「On」の値が表示されている場合は、Macintosh クライアントのファイルへのアクセスが高速化し、Macintosh 以外のクライアントがこの共有の Macintosh ファイルにアクセスできます。
Add	新しい共有を作成する場合にクリックします。「Add Share」ウィンドウで、すべての共有情報を指定できます。
Remove	これをクリックすると、「Remove Share」ウィンドウが表示されます。このウィンドウから、表で選択した共有を削除できます。実際に削除を実行するには、「Yes」を選択してください。
Edit	これをクリックすると、表で選択した共有に関する情報が更新されます。

「Remove Share」 ウィンドウ

このウィンドウでは、共有を構成から削除できます。

次の表で、このウィンドウのフィールドおよびボタンについて説明します。

表 F-97 「Remove Share」 ウィンドウのフィールドおよび要素

フィールド	説明
Name	共有の名前。これは、ネットワーク上でユーザーが確認できる名前です。この名前は 15 文字以内で入力する必要があります。次の文字はサポートされていません。 = : ; \ " ' ? < > * /
User	共有を所有するユーザーの名前。
Group	共有を所有するユーザーが属するグループ。
Apply	これをクリックすると、共有が構成から削除されます。
Cancel	これをクリックすると、変更内容を保存せずにウィンドウが閉じます。

「Set Up WINS」 パネル

Windows 環境または混在環境を使用する場合は、このパネルで、Sun StorageTek ソフトウェアで使用する Windows インターネットネームサービス (WINS) サーバーを設定できます。

WINS サーバーを使用すると、ネットワーク上のコンピュータが、NetBIOS (Network Basic Input/Output System) 名をインターネットプロトコル (IP) アドレスに解決することで相互に通信できるようになります。サーバーメッセージブロック (SMB) が使用可能な場合、システムには NetBIOS 名が指定されています。

純粋な UNIX 環境を使用する場合は、WINS を設定する必要はありません。

次の表で、このパネルのフィールドおよびボタンについて説明します。

表 F-98 「Set Up WINS」 パネルのフィールドおよびボタン

フィールド	説明
Enable WINS	WINS を使用可能にする場合に選択します。これによって、システムを WINS クライアントにすることができます。
Primary WINS Server	NetBIOS の名前解決で最初に照会されるサーバーの IP アドレス。

表 F-98 「Set Up WINS」 パネルのフィールドおよびボタン (続き)

フィールド	説明
Secondary WINS Server	プライマリ WINS サーバーが応答しない場合にのみ照会されるサーバーの IP アドレス。
Scope	NetBIOS の適用範囲識別子。ドメインネームサーバー (DNS) ソフトウェアでの定義に従って有効なドメイン名を指定してください。このフィールドに入力できる有効な値については、27 ページの「WINS の設定」を参照してください。
Apply	これをクリックすると、変更内容が保存されます。
Cancel	これをクリックすると、新しく入力した項目がフィールドから消去され、パネルに最初に表示されていた値に戻ります。

「System Status」 パネル

このパネルでは、ネットワーク接続ストレージ (NAS) システムの概要を表示できません。パネルの下部には、システムの最新の状態が表示されます。

次の表で、このパネルのフィールドについて説明します。

表 F-99 「System Status」 パネルのフィールド

フィールド	説明
Name	システム名。
Model	システムモデル。
Serial #	システムの一意的シリアル番号。
Up Time	システムの電源が最後に投入された時点からの経過時間。
CPU Load	中央処理装置 (CPU) の負荷の現在値および最大値。
OS Version	システムで現在動作しているオペレーティングシステムのバージョン。
Web Admin Version	グラフィカルな Web 管理アプリケーションのバージョン呼称。

索引

A

AC power failure, 274

AC 電源障害, 158

Active Directory サービス
「ADS」を参照

ADS

概要, 77

共有コンテナの更新, 81

共有の公開, 80

共有の削除, 81

構成

GUI, 77

Telnet, 240

Windows 2000 クライアント, 112

コンテナ名, 78

使用可能への切り替え, 77

設定, 26

GUI, 77

Telnet, 240

定義, 10, 76

ADS での共有の公開, 80

Alert (警告)

イベント、システムログ, 150

ALONE 状態

クラスタ, 147

C

c 点、定義, 165

CATIA V4/V5、文字変換, 173

CIFS

Compliance Archiving Software, 270

共有の名前の制限, 108, 110

クライアントの構成

DOS, 113

Windows, 112

自動ホーム共有

構成, 113

設定、Telnet, 237

静的共有

構成, 108

削除, 111

作成, 108

セキュリティー, 109

設定、Telnet, 236

追加, 108, 110, 111, 112, 113

定義, 106

編集, 110

定義, 106

ドライブ文字の割り当て, 233

Compliance Archiving Software, 140

API, 281

構成, 270

推奨実施, 141

必須実施, 141

Critical (重大) イベント、システムログ, 150

CRU

位置, 202

交換, 197

D

Debug (デバッグ) イベント、システムログ, 150

DHCP

本体のフェイルオーバーの使用不可への切り替え, 19

DIMM

サーバーの交換, 208

サポートされる構成, 208

配置規則, 208

DIMM 構成, 208

DNS

構成の確認, 79

設定

GUI, 27

Telnet, 229

定義, 76

DOS、SMB/CIFS の構成, 113

Down Timeout、定義, 20

DTQ

定義, 118

「ディレクトリツリー割り当て」を参照

E

Emergency (緊急) イベント、システムログ, 150

Error (エラー) イベント、システムログ, 150

F

File Replicator, 127

FTP

アクセス, 163, 263

構成, 162, 263

G

GID、定義, 109

GUI

コンテンツパネル, 8

使用, 3

状態パネル, 8

ツールバー, 3

ナビゲーションパネル, 5

H

HBA カード

サーバー

HBA, 297

I

Independent、ポートの役割, 68

Information (情報) イベント、システムログ, 150

Internet Storage Name Service (iSNS) サーバー, 58

IP アドレス

エイリアスの設定, 68

IP エイリアス

定義, 68

サーバー 2 台構成のシステム, 69

IPMI イベント, 277

iSCSI イニシエータ, 55

構成, 55

ソフトウェア, 54

iSCSI ターゲット

構成, 54

iSCSI ターゲットの検出方法, 58

iSCSI のスパーズ LUN, 57

iSNS サーバー, 58

L

LCD

定義, 294

LCD パネル, 198, 294

LDAP

構成, 82

使用可能への切り替え, 82

設定, 82

定義, 76

LED

位置特定, 299

サーバーの状態, 295

- サーバーの背面パネル, 299
- 電源/OK, 296
- 電源装置/背面側ファントレー障害, 296
- 電源装置の状態, 299
- 背面側ファントレー障害, 299
- 背面パネルの定義, 299
- 保守要求, 296, 299

LED 状態インジケータ, 296

LUN

- iSCSI、スパースでない, 56
- 再構築, 50
- 作成, 43
- 追加, 43
- 定義, 40

LUN パス

- サーバー 1 台構成, 15
- 自動割り当て, 17
- 設定, 17
- サーバー 2 台構成のシステム, 16

M

Macintosh

- サポート, 109, 111
- デスクトップ DB の呼び出し, 109, 111

MIB ファイル, 146

N

NDMP

- Telnet による設定, 269
- 設定, 170
- 定義, 170

Network Data Management Protocol

「NDMP」を参照

NFS

- エクスポート
- 削除, 123
- 作成, 121
- 設定, 121
- 編集, 122
- 定義, 121

NIC

- 構成, 23
- 定義, 22

NIC デュアルポートカード (ファイバ)

交換, 214

NIC デュアルポート (銅)

交換, 214

NIC ポート, 297

NIS

- 設定, 29
- Telnet, 231
- 定義, 10, 76

NIS+

- 設定, 30
- Telnet, 231
- 定義, 11, 76

NORMAL 状態

- クラスタ, 128
- クラスタの停止, 382

Notice (通知) イベント、システムログ, 150

NSSLDAP、「LDAP」を参照

NTP

- 時刻同期, 62
- Telnet, 224
- 設定, 63
- Telnet, 224
- 定義, 62

P

PCI スロットの指定, 216

Primary、ポートの役割, 68

Private、ポートの役割, 68

Q

QUIET 状態

クラスタ, 147

- R
 - RAID
 - エラーメッセージ, 277
 - 作成, 43
 - サポートされるレベル, 38
 - ストライプ化、定義, 38
 - セット, 38
 - 追加, 43
 - パリティ、定義, 39
 - ミラー化、定義, 39
 - RAID アレイ
 - ファームウェア, 176
 - RAID サブシステムエラー, 277
 - raidctl profile コマンド, 185
 - RDATE
 - 時刻同期, 63
 - Telnet, 225
 - 設定, 63
 - Telnet, 225
 - Restore Timeout
 - 定義, 20
-
- S
 - SCSI HBA カード
 - 交換, 214
 - SendTargets 要求, 58
 - SMB
 - 共有の名前の制限, 108, 110
 - 構成
 - DOS クライアント, 113
 - Windows クライアント, 112
 - クライアント, 112
 - 自動ホーム共有
 - 構成, 113
 - 使用可能への切り替え, 113
 - 静的共有
 - 構成, 108
 - 削除, 111
 - 作成, 108
 - 使用可能への切り替え, 108
 - 追加, 108, 110, 111, 112, 113
 - 定義, 106
 - 変更, 110
 - 編集, 110
 - セキュリティー、静的共有, 109
 - 設定
 - 自動ホーム共有、Telnet, 237
 - 静的共有、Telnet, 236
 - 定義, 106, 136
 - ドライブ文字の割り当て, 233
 - SMTP
 - 定義, 32
 - SNMP
 - 構成
 - GUI, 146
 - Telnet, 258
 - 定義, 146
 - Sun StorageTek 5320 NAS Appliance
 - LED 状態インジケータ, 296
 - 電源スイッチ, 295
 - Sun StorageTek ファイルのチェックポイント
 - 「チェックポイント」を参照
 - syslogd、定義, 33
 - SysMon、定義, 274
-
- T
 - TCP/IP
 - 構成
 - Telnet, 223
 - Telnet
 - 管理
 - 信頼できるホスト, 248
 - ファイルシステム, 233
 - ファイルボリュームアクセス, 249
 - フェイルオーバー, 267
 - ルート, 228
 - グループメンバーの削除, 242
 - 構成
 - SNMP, 258
 - TCP/IP, 223
 - アクティブサーバー, 250
 - ソースサーバー, 250
 - ターゲットサーバー, 250
 - 電子メール通知, 258
 - ドライブ文字, 233

- バックアップ, 269
- フェイルオーバー, 267
- フェイルバック, 267
- ミラー化するファイルボリューム, 252
- ミラーサーバー, 250
- ユーザーグループ, 241
- コンソールのロック, 249
- 再起動, 266
- 削除
 - 共有, 239
 - 信頼できるホスト, 248
 - ファイルボリューム, 235
 - ホスト, 247
 - ミラー化されたファイルボリューム, 256
- スケジュール
 - チェックポイント, 269
- 設定
 - ADS, 240
 - DNS, 229
 - NDMP, 269
 - NIS, 231
 - NIS+, 231
 - NTP, 224
 - RDATE, 225
 - 遠隔ログイン, 229
 - 警告しきい値, 253
 - 時刻, 224
 - 時刻同期, 224
 - 自動ホーム共有, 237
 - 静的共有, 236
 - タイムゾーン, 224
 - 動的 DNS, 229
 - ネームサービスの検索順序, 232
 - 日付, 224
 - ミラー, 252
 - ローカルログイン, 229
- 選択、言語, 227
- 追加
 - 共有, 238
 - グループメンバー, 242
 - 信頼できるホスト, 248
 - セグメント, 235
 - チェックポイント, 269
 - ホスト, 247

- 停止, 266
- パーティションの名前の変更, 234
- 表示
 - アクティビティモニター, 259
 - 個々のミラーの状態, 260
 - システムログ, 259
 - チェックポイント分析, 260
 - ポート結合, 260
 - ミラーの状態, 260
 - ミラーの統計情報, 262
- ファイルボリュームの作成, 234
- 編集
 - 共有, 239
 - ホスト, 247
- 編集キー, 221
- ミラー化, 250
 - 状態の表示, 260
 - ファイルボリュームのプロモート, 254
 - ミラーの切断, 255
- ミラーの再確立, 255
- ミラーの切断, 255
- メインメニュー, 221
- ログイン
 - イベント, 230
 - 機能, 230
- ロック解除、コンソール, 249
- 割り当ての使用可能への切り替え, 241

U

- UID、定義, 109
- umask, 110
- UNIX の設定
 - ネームサービスの検索順序, 31
 - マッピング, 101, 102
- UPS
 - アダプタケーブル, 297
 - アラーム, 158
 - エラーメッセージ, 274
 - 監視, 158
 - 監視の使用可能への切り替え, 158
 - 障害, 158
 - 定義, 157

バッテリー, 274
UPS サブシステムエラー, 274
USB ポート, 297

W

Warning (警告) イベント、システムログ, 150

Web Administrator

GUI, 3
コンテンツパネル, 8
状態パネル, 8
ツールバー, 3
ナビゲーション, 1
ナビゲーションパネル, 5

Windows

SMB/CIFS の構成, 112
資格のマッピング, 101
自動ホーム共有、定義, 113
静的共有、定義, 106
セキュリティー
モデル, 25
ドメイン
使用可能への切り替え, 26
ワークグループ
使用可能への切り替え, 26
セキュリティー, 109
ファイルディレクトリのセキュリティー, 103

WINS

設定, 27
定義, 76

WORM, 140

永続的なファイル保持, 286
管理ロックダウン, 282
推奨実施の規制適合の制限, 141
必須実施の制限, 141
ファイル, 282
ファイルの作成, 283
ファイルの動作, 284
ファイルのメタデータ, 285
ファイル別保持期間, 282
ファイル保持期間, 286
ファイル保持期間の変更, 286
ファイル保持タイムスタンプの設定, 286

あ

アイコン、ツールバー, 3
アクセス権、定義, 87
アクティビティモニター、表示、Telnet, 259
アクティブサーバー
構成
GUI, 128
Telnet, 250
ミラー化
Telnet, 250
定義, 127
アダプタ、ネットワーク
構成, 23
アダプタ、ネットワーク、構成
Telnet, 223

い

位置特定ボタン/LED, 296, 299
イベント
IPMI, 277
Telnet によるログイン, 230
システムログ, 150
インジケータ
LED 状態, 296

う

ウィザード
起動, 10
構成タイプ, 9
実行, 9

え

エイリアス IP アドレス
定義, 68
エクスポート
削除, 123
作成, 121
設定, 121
編集, 122

エラーメッセージ, 273
IPMI イベント, 277
RAID サブシステムエラー, 277
SysMon, 274
UPS サブシステムエラー, 274
ファイルシステムエラー, 276
遠隔ログイン
設定
Telnet, 229
「ログイン」を参照

お

オプション
Compliance Archiving Software, 140, 270
API, 281
起動, 125
ミラー化, 127
温度状態, 153

か

開始
コントローラの回復, 21
フェイルバック
GUI, 21
本体の回復, 21
回復
開始, 21
拡張格納装置
ドライブシャトル, 302
確認
DNS 構成, 79
ネームサービスの検索順序, 79
確認、ポートの位置, 22, 67
環境状態
温度, 153
システムの電源装置, 154
システムファン, 153
電圧, 154
表示, 153
監視
SNMP の構成, 146

UPS, 158
使用可能への切り替え, 158

管理
信頼できるホスト、Telnet, 248
ファイルボリュームアクセス、Telnet, 249
フェイルオーバー、Telnet, 267
ルート、Telnet, 228
割り当て, 114
管理者
グループ, 86

き

規則
サーバー名, 14
起動、オプション, 125
共通インターネットファイルシステム
「CIFS」を参照
共有
ADS からの削除, 81
ADS コンテナの更新, 81
ADS での公開, 80
自動ホーム
構成, 113
設定、Telnet, 237
定義, 113
静的
構成, 108
削除, 111
削除、Telnet, 239
作成, 108
セキュリティ、109
設定、Telnet, 236
追加、Telnet, 238
定義, 106
編集, 110
編集、Telnet, 239
チェックポイント, 169
定義, 106
ドライブ文字の割り当て, 233
名前の制限, 108, 110

く

- クライアント
 - DOS, 113
 - Windows, 112
 - 構成, 112
- クラスタ
 - 1 台のコントローラへの電源再投入, 19
 - NORMAL 状態, 128
 - サーバーの状態
 - NORMAL 状態
 - クラスタ, 147
 - ソフトウェアシリアル番号, 297
 - 停止, 382
 - ポートの役割, 24
 - ボリューム名の指定, 46
 - 本体のフェイルオーバーの使用可能への切り替え, 19
- グループ
 - 管理者, 86
 - 権限
 - GUI, 86
 - 資格、マッピング, 94, 404
 - スーパーユーザー
 - 割り当て, 115
 - バックアップオペレータ, 86
 - パワーユーザー, 86
 - メンバーの削除
 - GUI, 88
 - Telnet, 242
 - メンバーの追加
 - GUI, 88
 - Telnet, 242
 - ユーザー、定義, 86
 - 割り当て
 - 構成, 115
 - 追加, 115
 - デフォルト, 115
 - 編集, 116

け

- 警報
 - ミラーバッファースキ値, 134
- 警告しきい値

設定

- GUI, 133
- Telnet, 253
- 定義, 133
- ゲートウェイアドレス
 - 設定, 24
- 権限
 - 構成, 89
 - 所有権の割り当て, 88
 - スーパーユーザー, 90
 - 定義, 87
 - ユーザーグループ, 86
- 言語
 - 選択、Telnet, 227
 - 割り当て, 34
- 検索順序
 - Telnet による設定, 232
 - ネームサービス、確認, 79
 - 変更, 82

こ

- 高可用性、フェイルオーバー, 19
 - リンク、使用可能への切り替え, 20
- 更新
 - ADS 共有コンテナ, 81
 - ソフトウェア, 175
- 構成
 - ADS, 26
 - GUI, 77
 - Telnet, 240
 - ADS 向けの DNS の確認, 79
 - Compliance Archiving Software, 270
 - DNS
 - GUI, 27
 - Telnet, 229
 - FTP, 162, 263
 - iSCSI ターゲット, 54
 - LDAP, 82
 - NDMP
 - GUI, 170
 - Telnet, 269
 - NFS エクスポート, 121
 - NIC, 23

- NIS, 29
 - Telnet, 231
- NIS+, 30
 - Telnet, 231
- NTP, 63
 - Telnet, 224
- RDATE, 63
 - Telnet, 225
- SMB/CIFS クライアント, 112
- SMTP
 - Telnet, 258
- SNMP
 - GUI, 146
 - Telnet, 258
- TCP/IP
 - Telnet, 223
- Telnet でのドライブ文字, 233
- Windows のセキュリティー, 25
- WINS, 27
- アクティブサーバー
 - GUI, 128
 - Telnet, 250
- ウィザードでの構成タイプ, 9
- ウィザードの実行, 9
- 遠隔ログイン
 - Telnet, 229
- グループ
 - 権限, 86
 - 権限、Telnet, 243
 - 割り当て, 115
- 警告しきい値, 133
- ゲートウェイアドレス, 24
- 権限
 - GUI, 89
 - Telnet, 243
- 言語
 - GUI, 34
 - Telnet, 227
- 構成ウィザードの起動, 10
- サーバー名, 14
- 時刻, 63
 - Telnet, 224
- 時刻同期
 - GUI, 63
 - Telnet, 224
- 自動ホーム共有
 - GUI, 113
 - Telnet, 237
- 静的共有
 - GUI, 108
 - Telnet, 236
- ソースサーバー
 - GUI, 128
 - Telnet, 250
- ターゲットサーバー
 - GUI, 128
 - Telnet, 250
- タイムゾーン
 - GUI, 63
 - Telnet, 224
- ディレクトリツリー割り当て, 118
- 電子メール通知, 32
 - Telnet, 258
- 動的 DNS
 - Telnet, 229
- ネームサービス, 31
 - Telnet, 228
- ネットワークアダプタ, 23
- バックアップ
 - Telnet, 269
- 日付, 63
 - Telnet, 224
- ファイルボリュームのミラー化
 - GUI, 130
 - Telnet, 252
- フェイルオーバー
 - Telnet, 267
- フェイルバック
 - Telnet, 267
- ポート
 - GUI, 23
 - Telnet, 223
 - ミラー化, 129
- ホスト
 - GUI, 90
- ミラー化
 - Telnet, 250
- ミラーサーバー
 - GUI, 128
 - Telnet, 250
- ユーザーグループ、Telnet, 241
- ユーザーの割り当て, 115
- ローカルログイン

- Telnet, 229
 - ログイン, 33
- 構成タイプ、構成ウィザード, 9
- 個々のミラー、Telnet からの状態の表示, 260
- コマンド行インタフェース, 219
- コンソール, 219
 - ロック, 249
- コンソールのロック, 249
- コンテナ、ADS 共有の更新, 81
- コンテンツパネル
 - 使用, 8
- コントローラ
 - 情報、表示, 159

さ

- サーバー
 - CRU の交換, 197
 - DIMM 配置規則, 208
 - LED, 298
 - PCI スロットの指定, 216
 - 状態, 147
 - 電源 LED, 299
 - 電源障害, 158, 274
 - 電源切断, 198
 - 電源装置, 299
 - 名前
 - 規則, 14
 - 設定, 14
 - ファントレー障害 LED, 299
 - フェイルバック, 19
 - フロントパネルのボタン, 295
 - 本体、定義, 19
 - 本体のフェイルオーバー, 19
- サーバー 2 台構成のシステム
 - IP エイリアス, 69
 - ポートの結合, 71
 - ポートの役割, 24
 - 本体のフェイルオーバーの使用可能への切り替え, 19
 - Telnet, 267
- サーバーの停止, 164

- Telnet, 266
- サーバーメッセージブロック
 - 「SMB」を参照
- 再起動
 - Telnet, 266
 - ファームウェアのアップグレード後, 177
- 再構築、LUN, 50
- 削除
 - ADS の共有, 81
 - NFS エクスポート, 123
 - グループメンバー
 - GUI, 88
 - Telnet, 242
 - 信頼できるホスト
 - GUI, 91
 - Telnet, 248
 - スケジュール設定されたチェックポイント, 168
- 静的共有
 - GUI, 111
 - Telnet, 239
- チェックポイント, 169
- ディレクトリツリー割り当て, 120
- ファイルボリューム
 - Telnet, 235
- 古いファイルボリューム
 - GUI, 137
 - Telnet, 256
- ホスト
 - GUI, 91
 - Telnet, 247
- ミラー化されたファイルボリューム
 - Telnet, 256
- ユーザーの割り当て, 117

- 作成
 - LUN, 43
 - NFS エクスポート, 121
 - RAID, 43
 - グループの割り当て, 116
 - 信頼できるホスト
 - GUI, 91
 - Telnet, 248
 - スケジュール設定されたチェックポイント
 - Telnet, 269
 - 静的共有
 - GUI, 108
 - Telnet, 238

- セグメント, 46
 - Telnet, 235
- チェックポイント
 - GUI, 165
 - Telnet, 269
- ディレクトリツリー割り当て, 118
- ファイルボリューム, 46
 - Telnet, 234
- ホスト, 90
 - Telnet, 247
- ユーザーの割り当て, 116
- 作成、ファイルシステム, 42
- サポートされる RAID レベル, 38

し

- 資格、マッピング, 94, 404
- 時間情報プロトコル
 - 「NTP」を参照
- しきい値、設定
 - GUI, 133
 - Telnet, 253
- 時刻
 - 設定, 63
 - Telnet, 224
 - ゾーン、設定, 63
 - Telnet, 224
- 同期
 - NTP, 62
 - RDATE, 63
 - 設定, 63
 - 設定、Telnet, 224
 - 定義, 62
- システム
 - イベント
 - 表示, 150
 - 状態
 - パネル、使用, 8
 - 停止
 - GUI, 164
 - Telnet, 266
 - 電源障害, 158, 274
 - 動作状態、使用量に関する統計情報, 156
 - ログ

- 表示, 148
- 表示、Telnet, 259
- システム温度超過 LED, 296
- システム状態, 296
- 実行
 - 構成ウィザード, 9
- 自動ホーム共有
 - 構成, 113
 - 設定、Telnet, 237
 - 定義, 113
- シャトル
 - ドライブ, 302
- 集約
 - 「ポートの結合」を参照
- 使用
 - GUI, 3
 - コンテンツパネル, 8
 - 状態パネル, 8
 - ツールバー, 3
 - ナビゲーションパネル, 5
- 使用可能への切り替え
 - ADS
 - GUI, 77
 - Telnet, 240
 - DNS
 - GUI, 27
 - Telnet, 229
 - LDAP, 82
 - NIS, 29
 - Telnet, 231
 - NIS+, 30
 - Telnet, 231
 - SNMP
 - GUI, 146
 - Telnet, 258
 - UPS 監視, 158
 - WINS, 27
 - 遠隔ログイン
 - Telnet, 229
 - 外国語
 - GUI, 34
 - Telnet, 227
 - グループの割り当て
 - GUI, 115
 - Telnet, 241

- コントローラのフェイルオーバー
 - Telnet, 267
 - 自動ホーム共有
 - GUI, 113
 - Telnet, 237
 - 静的共有
 - GUI, 108
 - Telnet, 236
 - チェックポイント
 - Telnet, 269
 - 電子メール通知, 22
 - Telnet, 258
 - 動的 DNS, 28
 - Telnet, 229
 - ドメインのセキュリティー, 26
 - ネームサービス, 31
 - Telnet, 228
 - フェイルオーバー
 - GUI, 19
 - Telnet, 267
 - 本体のフェイルオーバー
 - Telnet, 267
 - ユーザーの割り当て
 - GUI, 115
 - Telnet, 241
 - リンクのフェイルオーバー
 - GUI, 20
 - Telnet, 267
 - ローカルロギング
 - Telnet, 229
 - ロギング, 33
 - ワークグループのセキュリティー, 26
 - 割り当て
 - Telnet, 241
 - 状態, 147
 - UPS, 158
 - インジケータ、LED, 296
 - 温度, 153
 - 環境、表示, 153
 - 個々のミラー、Telnet, 260
 - コントローラ情報, 159
 - システムの動作状態, 156
 - 電圧, 154
 - 電源装置, 154
 - ネットワークの動作状態, 156
 - ファイルボリュームの使用量, 155
 - ファン, 153
 - ミラー化
 - GUI, 159
 - Telnet, 260
 - ミラーの状態, 159
 - ミラーの統計情報、Telnet, 262
 - 状態表示 LED インジケータ, 296
 - 上部ファン障害 LED, 296
 - 正面側カバー
 - 取り外し, 201
 - フロントパネル
 - ボタン, 295
 - 使用量に関する統計情報
 - システムの動作状態, 156
 - ネットワークの動作状態, 156
 - ファイルボリューム, 155
 - ミラー化, 159
 - 所有権の割り当て、グループ権限, 88
 - シリアル番号
 - クラスタ用ソフトウェア, 297
 - 診断電子メールの送信, 307
 - 信頼できるホスト
 - 管理、Telnet, 248
 - 削除, 91
 - 削除、Telnet, 248
 - 追加
 - GUI, 91
 - Telnet, 248
 - 定義, 90
- ## す
- スイッチ
 - 電源, 295
 - スーパーユーザー
 - ホストの状態によって定義される権限, 90
 - 割り当て, 115
 - スーパーユーザーグループ
 - 割り当て, 115
 - スケジュール
 - チェックポイント, 166
 - Telnet, 269
 - 削除, 168

編集, 168
ストライプ化、定義, 38
スペースでない LUN, 56

せ

制限

強い, 115

名前

ADS コンテナ, 78

共有, 108, 110

コンテナ, 78

サーバー, 14

セグメント, 46

適用範囲, 27

ファイルボリューム, 46

ホスト, 91

弱い, 115

整合点, 165

定義, 165

静的共有

構成, 108

削除, 111

作成, 108

セキュリティ, 109

定義, 106

名前の制限, 108, 110

編集, 110

セキュリティ

Windows, 25

管理者パスワード, 61

コンソールのロック, 249

コンソールのロック解除, 249

静的共有, 109

設定, 104

ファイルボリュームアクセス、Telnet, 249

セグメント

作成, 46

追加、Telnet, 235

定義, 41

名前の制限, 46

配置

Telnet, 235

設定

ADS, 26

GUI, 77

Telnet, 240

Compliance Archiving Software, 270

DNS

GUI, 27

Telnet, 229

FTP, 162, 263

LDAP, 82

NDMP

GUI, 170

Telnet, 269

NFS エクスポート, 121

NIC, 23

NIS, 29

Telnet, 231

NIS+, 30

Telnet, 231

NTP, 63

Telnet, 224

RDATE, 63

Telnet, 225

SMB/CIFS クライアント, 112

SNMP

GUI, 146

Telnet, 258

TCP/IP、Telnet, 223

Windows のセキュリティ, 25

WINS, 27

アクティブサーバー

GUI, 128

Telnet, 250

遠隔ログイン

Telnet, 229

管理者パスワード, 61

グループ権限, 86

グループの割り当て, 115

警告しきい値

GUI, 133

Telnet, 253

ゲートウェイアドレス, 24

権限, 89

言語, 34

Telnet, 227

コントローラの回復, 21

- サーバー名, 14
- 時刻, 63
 - Telnet, 224
- 時刻同期, 63
 - Telnet, 224
- 自動ホーム共有
 - GUI, 113
 - Telnet, 237
- 静的共有
 - GUI, 108
 - Telnet, 236
- セキュリティ, 104
- ソースサーバー
 - GUI, 128
 - Telnet, 250
- ターゲットサーバー
 - GUI, 128
 - Telnet, 250
- タイムゾーン, 63
 - Telnet, 224
- ディレクトリツリー割り当て, 118
- 電子メール通知, 32
 - Telnet, 258
- 動的 DNS
 - Telnet, 229
- ドライブ文字, Telnet, 233
- ネームサービス, 31
- ネームサービスの検索順序, 31
 - Telnet, 232
- ネットワークアダプタ, 23
- バックアップ, Telnet, 269
- 日付, 63
 - Telnet, 224
- ファイルボリュームのミラー化, 130
- フェイルオーバー, Telnet, 267
- フェイルバック, 21
- ポート
 - GUI, 23
 - Telnet, 223
 - ミラー化, 129
- ホスト, 90
- 本体の回復, 21
- ミラー化
 - Telnet, 252
- ミラーサーバー

- GUI, 128
- Telnet, 250
- ユーザーの割り当て, 115
- ローカルログイン
 - Telnet, 229
- 選択、言語、Telnet, 227
- 専用ポート
 - ポートの役割の設定, 129
 - ミラー化, 129

そ

- 送信、診断電子メール, 307
- ソースサーバー
 - 構成
 - GUI, 128
 - Telnet, 250
 - ミラー化
 - Telnet, 250
 - 定義, 127

即時

- チェックポイント、作成, 165

ソフトウェア

- File Replicator, 127
- 更新, 175
- ミラー化, 127

た

- ターゲットサーバー
 - 構成
 - GUI, 128
 - Telnet, 250
 - 定義, 127
 - ミラー化、Telnet, 250
- タイムゾーン
 - データベースの更新, 171

ち

- チェックポイント
 - アクセス, 170
 - 共有, 169

- 削除, 169
- 作成, 165
- スケジュール
 - GUI, 166
 - Telnet, 269
- スケジュールの削除, 168
- スケジュールの編集, 168
- スケジュールへの追加
 - Telnet, 269
- 定義, 165
- 名前の変更, 168
- 分析、Telnet による表示, 260
- チャンネル結合
 - 「ポートの結合」を参照

つ

- 追加
 - LUN, 43
 - NFS エクスポート, 121
 - RAID, 43
 - グループの割り当て, 116
 - グループメンバー
 - GUI, 88
 - Telnet, 242
 - 信頼できるホスト
 - GUI, 91
 - Telnet, 248
 - 静的共有
 - GUI, 108, 110, 111, 112, 113
 - Telnet, 238
 - セグメント
 - Telnet, 235
 - チェックポイント
 - GUI, 165
 - Telnet, 269
 - ディレクトリツリー割り当て, 118
 - ファイルボリューム
 - Telnet, 234
 - ホスト, 90
 - Telnet, 247
 - ユーザーの割り当て, 116
- 通知レベル、電子メール通知, 32
- ツールバー
 - アイコン, 3

- 使用, 3
- 強い制限値, 115

て

- 定義
 - LUN, 43
 - RAID, 43
 - セグメント, 46
 - ファイルボリューム, 46
- 停止
 - Telnet, 266
 - クラスタ構成, 382
 - サーバー 1 台構成, 164
- ディレクトリツリー割り当て
 - 構成, 118
 - 削除, 120
 - 追加, 118
 - 編集, 119
- テープライブラリ
 - バックアップのための接続, 300
- デフォルトの割り当て
 - グループ, 115
 - ユーザー, 115
- デュアルポートファイバチャンネルカード
 - 交換, 214
- 電圧状態, 154
- 電源 LED
 - サーバー, 299
- 電源/OK LED, 198, 296
- 電源障害, 158, 274
 - クラスタ構成, 19
- 電源スイッチ, 295
- 電源切断
 - サーバー, 198
- 電源装置, 305
 - サーバー, 299
 - サーバーの交換, 207
 - 状態, 154
- 電源装置/背面側ファントレイ障害 LED, 296
- 電源装置の状態 LED, 299
- 電子メール通知

構成、Telnet, 258
診断、送信, 307
設定, 32
通知レベル, 32

と

同期、時刻

Telnet, 224
設定, 63
定義, 62

動的 DNS

使用可能への切り替え, 28
設定、Telnet, 229

ドメイン

セキュリティ, 26

ドライブシャトル, 302

ドライブ障害メッセージ, 305

ドライブのファームウェア、アップグレード, 176

ドライブ文字、構成、Telnet, 233

トラブルシューティング

サーバーの問題, 296, 299

ドライブ障害メッセージ, 305

トランキング

「ポートの結合」を参照

な

夏時間 (DST)、サーバーの更新, 171

ナビゲーション

Web Administrator, 1

ナビゲーションパネル

使用, 5

名前

共有の名前の制限, 108, 110

コンテナ、制限, 78

サーバー

規則, 14

セグメント, 46

適用範囲, 27

ファイルボリューム, 46

ホスト, 91

名前、サーバー
設定, 14

名前の変更

チェックポイント, 168

パーティション、Telnet, 234

ね

ネームサービス

DNS, 31

NIS, 31

NIS+, 31

検索順序の確認, 79

検索順序の設定、Telnet, 232

検索順序の変更, 82

構成, 31

ローカル, 31

ネットワーク

インタフェースカード

「NIC」を参照

動作状態、使用量に関する統計情報, 156

ルート, 157

表示, 157

ネットワーク管理プロトコル

「SNMP」を参照

ネットワーク情報サービス

「NIS」を参照

ネットワーク情報サービスプラス

「NIS+」を参照

ネットワークファイルシステム

「NFS」を参照

は

パーティション

名前の変更、Telnet, 234

配置、セグメント

Telnet, 235

背面側ファントレー障害 LED, 299

背面パネルの LED

定義, 299

パス名、ADS, 78

パスワード

- 管理者、設定, 61
- バックアップ
 - NDMP
 - GUI, 170
 - Telnet, 269
 - グループ, 86
 - 構成、Telnet, 269
- バッテリー
 - UPS
 - 低下, 274
 - 状態, 158
- パリティ、定義, 39
- パワーユーザーグループ, 86

ひ

- 日付、設定, 63
 - Telnet, 224
- 表示
 - アクティビティモニター、Telnet, 259
 - 温度状態, 153
 - 環境状態, 153
 - 個々のミラーの状態、Telnet, 260
 - コントローラ情報, 159
 - システムイベント, 150
 - システムの動作状態, 156
 - システムログ, 148
 - GUI, 148
 - Telnet, 259
 - 状態, 147
 - チェックポイント分析、Telnet, 260
 - 電圧状態, 154
 - 電源装置の状態, 154
 - ネットワークの動作状態, 156
 - ネットワークルート, 157
 - ファイルボリュームの使用量, 155
 - ファンの状態, 153
 - ポート結合、Telnet, 260
 - ミラーの状態、Telnet, 260
 - ミラーの統計情報
 - GUI, 159
 - Telnet, 262
 - ルート, 157

ふ

- ファームウェア
 - RAID アレイ, 176
 - アップグレード, 176
 - ディレクトリおよびファイル, 178
- ファームウェアのアップグレード, 176
- ファイルシステム
 - Telnet による管理, 233
 - エラーメッセージ, 276
 - 作成, 42
- ファイルシステムエラー, 276
- ファイルディレクトリのセキュリティー, 103
- ファイル転送プロトコル
 - 「FTP」を参照
- ファイルボリューム
 - アクセスの管理、Telnet, 249
 - 拡張
 - Telnet, 235
 - 最新のボリュームのミラー化
 - GUI, 138
 - Telnet, 256
 - 削除
 - Telnet, 235
 - 作成, 46
 - Telnet, 234
 - 自動ホーム共有
 - Telnet, 237
 - 定義, 113
 - 使用量に関する統計情報, 155
 - 静的共有
 - Telnet, 236
 - 定義, 106
 - 定義, 41
 - 名前の制限, 46
 - 古いボリュームの削除
 - GUI, 137
 - Telnet, 256
 - プロモート
 - GUI, 135
 - Telnet, 254
 - ミラー化
 - GUI, 130
 - Telnet, 252
 - ミラーの再確立
 - GUI, 136

- Telnet, 255
 - ファン
 - 状態, 153
 - ファンコネクタボード
 - 交換, 203
 - ファントレーアセンブリ
 - サーバーの交換, 211
 - ファントレー障害 LED (背面側), 299
 - フェイルオーバー
 - 管理、Telnet, 267
 - 構成、Telnet, 267
 - 使用可能への切り替え, 19
 - 定義, 19
 - リンク, 20
 - フェイルバック
 - 開始
 - GUI, 21
 - 構成
 - Telnet, 267
 - 定義, 19
 - プロモート
 - ファイルボリューム
 - GUI, 135
 - Telnet, 254
 - フロントパネルインジケータボード
 - 交換, 205
- へ
- ベゼル
 - 取り外し, 199
 - 変更
 - NFS エクスポート, 122
 - グループの割り当て, 116
 - 言語
 - Telnet, 227
 - スケジュール設定されたチェックポイント, 168
 - 静的共有
 - GUI, 110
 - Telnet, 239
 - ディレクトリツリー割り当て, 119
 - ネームサービスの検索順序, 82
 - Telnet, 232
 - パーティションの名前、Telnet, 235
 - ホスト, 90
 - Telnet, 247
 - ミラー, 132
 - ユーザーの割り当て, 116
 - 編集
 - NFS エクスポート, 122
 - Telnet で使用するキー, 221
 - グループの割り当て, 116
 - スケジュール設定されたチェックポイント, 168
 - 静的共有
 - GUI, 110
 - Telnet, 239
 - ディレクトリツリー割り当て, 119
 - ホスト, 90
 - Telnet, 247
 - ミラー, 132
 - ユーザーの割り当て, 116
- ほ
- ポート
 - NIC, 297
 - USB, 297
 - 位置
 - 確認, 22, 67
 - 結合, 69
 - サーバー 2 台構成のシステム, 71
 - 構成
 - Telnet, 223
 - ポート結合の表示、Telnet, 260
 - ミラー化
 - 構成, 129
 - 設定, 129
 - 役割, 68
 - Independent, 68
 - Primary, 68
 - Private, 68
 - 専用ポートの設定, 129
 - ミラー, 68
 - 割り当て, 24
 - ポートの結合, 69
 - サーバー 2 台構成のシステム, 71
 - 表示、Telnet, 260
 - 保持期間、Compliance Archiving Software, 270

- 保守要求 LED
 - サーバーの正面, 296
 - サーバーの背面, 299
- 補助ローカル UPS, 297
- ホスト
 - 構成, 90
 - 削除, 91
 - 削除、Telnet, 247
 - 信頼できる, 90
 - Telnet, 248
 - 構成, 90
 - 削除, 91
 - 削除、Telnet, 248
 - 追加、Telnet, 248
 - 追加, 90
 - Telnet, 247
 - 編集, 90
 - Telnet, 247
 - 命名, 91
 - ルート, 157
- ホットスペア
 - 割り当て, 44
- ポップアップブロッカ, 9
- 本体
 - 定義, 19
- 本体のフェイルオーバー
 - 定義, 19

ま

- マッピング
 - 資格, 94, 404
 - ドライブ文字、Telnet, 233

み

- ミラー
 - サーバー
 - 構成, 128
 - 構成、Telnet, 250
 - 設定, 128
 - 定義, 127
 - バッファ

- しきい値警告, 134
 - 定義, 127
- ポートの役割, 68
- ミラー化
 - Telnet, 250
 - アクティブサーバー、定義, 127
 - 警告しきい値の設定、Telnet, 253
 - 構成
 - アクティブサーバー、Telnet, 250
 - 専用ポート, 129
 - ソースサーバー、Telnet, 250
 - ターゲットサーバー、Telnet, 250
 - ファイルボリューム、Telnet, 252
 - ミラーサーバー、Telnet, 250
 - 準備作業, 127
 - 状態, 159
 - 使用量に関する統計情報, 159
 - 切断
 - Telnet, 255
 - ミラー, 135
 - 設定
 - Telnet, 252
 - 専用ポート, 129
 - ファイルボリューム, 130
 - ソースサーバー、定義, 127
 - ターゲットサーバー、定義, 127
 - 定義, 127
 - 表示、Telnet
 - 個々の状態, 260
 - 統計情報, 262
 - ファイルボリュームのプロモート
 - GUI, 135
 - Telnet, 254
 - ファイルボリュームの削除、Telnet, 256
 - 変更, 132
 - 編集, 132
 - ミラーサーバー、定義, 127
 - ミラーの再確立
 - GUI, 136
 - Telnet, 255
 - ミラーバッファ、定義, 127
 - 要件, 127
- ミラー化、RAID
 - 定義, 39

ミラーの再確立
GUI, 136
Telnet, 255
最新のファイルボリュームのミラー化
GUI, 138
Telnet, 256
古いファイルボリュームの削除
GUI, 137
Telnet, 256
ミラーの切断
GUI, 137
Telnet, 255
ミラーの切断
GUI, 135
Telnet, 255
サーバー 1
GUI, 137
Telnet, 255

む

無停電電源装置
「UPS」を参照

め

メインメニュー、Telnet, 221
メール転送プロトコル
「SMTP」を参照
メッセージ
表示言語, 34
メモリーモジュール
サーバーの交換, 208

ゆ

ユーザー
グループ
権限, 86
構成、Telnet, 241
定義, 86
メンバーの削除、Telnet, 242
メンバーの追加、Telnet, 242
資格

マッピング, 94, 404
スーパーユーザー
割り当て, 115
割り当て
構成, 115
削除, 117
追加, 116
デフォルト, 115
編集, 116

よ

要件
サーバー名, 14
ミラー化, 127
弱い制限値, 115

り

リンクのフェイルオーバー、使用可能への切り替え, 20

る

ルート
Telnet による管理, 228
定義, 157
表示, 157
フラグ, 157
ホスト, 157

ろ

ローカルロギング
「ロギング」を参照
ロギング
Alert (警告) イベント, 150
Critical (重大) イベント, 150
Debug (デバッグ) イベント, 150
Emergency (緊急) イベント, 150
Error (エラー) イベント, 150
Information (情報) イベント, 150

- Notice (通知) イベント, 150
- Warning (警告) イベント, 150
- イベントタイプ, 230
- 遠隔、設定
 - Telnet, 229
- 機能, 33
 - Telnet, 230
- システムイベント, 150
- システムログの表示
 - GUI, 148
 - Telnet, 259
- 設定, 33
- ローカル設定
 - GUI, 34
- ローカル、設定
 - Telnet, 229
- ログの表示, 148
- ロック解除、コンソール, 249
- 論理ユニット番号
 - LUN を参照

わ

- ワークグループ
 - セキュリティ
 - 使用可能への切り替え, 26
- 割り当て
 - 管理, 114
 - グループ
 - 構成, 115
 - 追加, 116
 - 編集, 116
- 言語, 34
- サーバー名, 14
- 使用可能への切り替え
 - Telnet, 241
- スーパーユーザー, 115
- スーパーユーザーグループ, 115
- 強い制限値, 115
- ディレクトリツリー
 - 構成, 118
 - 削除, 120
 - 追加, 118

- 編集, 119
- デフォルトのグループ, 115
- デフォルトのユーザー, 115
- ポートの役割, 24
- ホットスベア, 44
- ユーザー
 - 構成, 115
 - 削除, 117
 - 追加, 116
 - 編集, 116
- 弱い制限値, 115

