

**IBM System Storage DS ストレージ・
マネージャー バージョン 10.8**



インストールおよびホスト・サポートのガイド

お願い

本書および本書で紹介する製品をご使用になる前に、349 ページの『特記事項』に記載されている情報をお読みください。

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。

本書は、IBM DS ストレージ・マネージャー バージョン 10 モディフィケーション 83、および新しい版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

本書は、GA32-2221-01 の改訂版です。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： GA32-2221-02

IBM System Storage DS Storage Manager Version 10.8
Installation and Host Support Guide

発行： 日本アイ・ピー・エム株式会社

担当： トランスレーション・サービス・センター

第1刷 2012.11

© Copyright IBM Corporation 2012.

目次

図	vii

表	ix

本書について	xi

このリリースの新機能	xii

関連資料	xvii

IBM Web サイト上のストレージ・マネージャ ー資料	xviii

ストレージ・マネージャのオンライン・ヘル プおよび診断	xviii

ストレージ・マネージャ・ソフトウェア、コン トローラー・ファームウェア、および README ファイルの検出	xix

IBM System Storage Productivity Center	xix

サポート情報に必須の Web サイト	xx

情報、ヘルプ、およびサービスの入手	xxi

依頼する前に	xxi

資料の使用	xxi

ソフトウェアのサービスとサポート	xxii

ハードウェアのサービスとサポート	xxii

本書の注意および注記	xxii

製品更新およびサポート通知の受け取り	xxii

第 1 章 インストールの準備	1

紹介	1

ストレージ・マネージャ・ソフトウェア	1

ストレージ・マネージャのソフトウェア・コンポ ーネント	2

サポートされるコントローラー・ファームウェア	2

インストール構成のタイプ	2

ネットワーク構成	3

サンプル・ネットワーク構成の検討	4

管理ステーションのセットアップ	4

ネットワーク管理 (アウト・オブ・バンド) 構成 のセットアップ	4

ホスト・エージェント管理 (インバンド) 構成の セットアップ	5

直接接続および SAN 接続の構成	6

直接接続構成のセットアップ	6

SAN 接続の構成のセットアップ	6

ソフトウェアのインストールのためのコントローラー のアドレスのセットアップ	7

ストレージ・サブシステム・コントローラーの IP アドレスのセットアップ	7

DHCP/BOOTP サーバーでの IP アドレスのセット アップ	8

イーサネット MAC アドレスの識別	8

出荷時のデフォルト値の管理ポート TCP/IP アドレ スを使用する静的 TCP/IP アドレスのストレージ・ サブシステムへの割り当て	9

インバンド管理接続を使用する静的 TCP/IP アド レスのストレージ・サブシステムへの割り当て	10

ストレージ・サブシステム・コントローラー・シ リアル・ポートのサービス・インターフェースを 使用する静的 TCP/IP アドレスの割り当て	11

第 2 章 ストレージ・マネージャのイン ターフェース	13

「Enterprise Management (エンタープライズ管理)」 ウィンドウ	13

「Devices (デバイス)」タブの使用	15

「Setup (セットアップ)」タブの使用	19

「Subsystem Management (サブシステム管理)」ウィ ンドウ	20

「Subsystem Management (サブシステム管理)」ウ ィンドウのオープン	21

「Summary (要約)」タブの使用	21

「Storage and Copy Services (ストレージおよびコ ピー・サービス)」タブの使用	22

「Host Mappings (ホスト・マッピング)」タブの 使用	25

「Hardware (ハードウェア)」タブの使用	27

「Setup (セットアップ)」タブの使用	27

複数のソフトウェア・バージョンの管理	27

第 3 章 ストレージ・マネージャのイン ストール	29

プリインストール要件	30

インストール・ウィザードを使用するストレージ・ マネージャ・パッケージの自動インストール	30

Linux、AIX、HP-UX、および Solaris でのコンソ ール・ウィンドウを使用したストレージ・マネー ジャーのインストール	33

ストレージ・マネージャ・パッケージの手動イン ストール	34

ソフトウェア・インストール・シーケンス	34

ストレージ・マネージャの手動インストール	35

ストレージ・マネージャのアンインストール	36

Windows オペレーティング・システムでのストレ ージ・マネージャのアンインストール	36

Linux、AIX、または Solaris オペレーティング・ システムでのストレージ・マネージャのアンイ ンストール	36

ストレージ・マネージャのインストールの完了	36

ストレージ・サブシステムの自動ディスカバリー の実行	37

ストレージ・サブシステムの手動ディスカバリー の実行	39

ストレージ・サブシステムの管理パスワードの設 定	39

ストレージ・サブシステムの命名	39	ディスク・プールの作成	79
アラート通知の設定	40	アレイの作成	81
iSCSI 設定の管理	42	新磁気ディスク制御機構 (RAID)	81
ターゲット認証の変更	43	標準論理ドライブの作成	84
相互認証許可の入力	43	シン論理ドライブの作成	85
ターゲット ID の変更	43	動的容量拡張の概要	86
ターゲット・ディスクバリーの変更	43	進行中の操作の表示	86
iSCSI ホスト・ポートの構成	43	グローバル・ホット・スペア・ドライブの構成	87
iSCSI セッションの表示または終了	44	デフォルト・ホスト・オペレーティング・システム	
iSCSI 統計の表示	44	の定義	88
iSNS サーバーの使用	44	ホスト・グループの定義	90
DHCP の使用	44	異機種ホストの定義	91
サポートされるハードウェア・イニシエーター		ホストおよびホスト・ポートの定義	91
の使用	44	LUN のマッピング	92
IPv6 の使用	45	新規のホストまたはホスト・グループへの LUN	
iSCSI ホスト接続のためのネットワーク設定の		マッピング	92
構成	45	既存のホストまたはホスト・グループへの LUN	
最大伝送単位の設定の構成	46	の追加	92
Microsoft iSCSI ソフトウェア・イニシエーター		IBM i の IBMSystem Storage の構成	93
の考慮事項	46	オプションのプレミアム・フィーチャーの構成および	
コントローラー・ファームウェア、		使用	94
NVSRAM、ESM ファームウェアのダウンロード	46	Enhanced FlashCopy の概要	94
ファームウェア・レベルの判別	47	FlashCopy の概要	95
コントローラーおよび NVSRAM のファーム		VolumeCopy の使用	96
ウェアのダウンロード	49	拡張リモート・ミラーリングの使用	96
IBM System Storage コントローラー・ファーム		拡張グローバル・ミラーリングの使用	96
ウェア・アップグレード・ツールの使用	50	パフォーマンス読み取りキャッシュの使用	97
ESM ファームウェア・ダウンロード	52	フル・ディスク暗号化の使用	97
ドライブ・ファームウェア・ダウンロード	53	その他の機能の使用	98
ストレージ・マネージャーのプレミアム・フィー		コントローラーのキャッシュ・メモリーの使用	98
チャー	55	永続的予約の使用	99
プレミアム・フィーチャー試用版の使用可能化	56	メディア・スキャンの使用	99
パーマナント・プレミアム・フィーチャーの使用		メディア・スキャンにより報告されるエラー	101
可能化	56	メディア・スキャン設定	102
プレミアム・フィーチャー使用可能化 ID の取得	56	メディア・スキャン期間	103
フィーチャー・キー・ファイルの生成	57	ストレージ・サブシステムのチューニング	104
プレミアム・フィーチャーの使用可能化	58	ロード・バランシングによるスループットの最大	
プレミアム・フィーチャーの使用不可化	59	化	104
ストレージ・サブシステムのプロファイルを保管		ファイバー・チャンネルの入出力負荷の平衡化	106
する	59	入出力転送速度の最適化	106
		入出力要求速度の最適化	106
		入出力アクセス・パターンおよび入出力サイ	
		ズの決定	107
		書き込みキャッシュの使用可能化	107
		キャッシュ・ヒット率の最適化	107
		適切な RAID レベルの選択	107
		最適な論理ドライブ変更優先順位の設定の選	
		択	108
		アレイの最適なセグメント・サイズの選択	108
		ファイルのデフラグによるディスク・アクセ	
		スの最小化	108
		ストレージ・マネージャーのコマンド行インター	
		フェースおよびスクリプト・エディターの使用	109
		ストレージ・マネージャーのコマンド行インター	
		フェース	109
		スクリプト・エディターの使用	109

第 4 章 ストレージの構成 61

ストレージの区画化の概説	61
タスク・アシスタントの使用	62
IBM System Storage DS ストレージ・マネージャー	
によりサポートされるドライブ	63
RAID アレイ作成時のドライブ選択規則	64
ソリッド・ステート・ドライブ (SSD) 属性	66
T10PI 対応ドライブ属性	67
T10PI 機能の使用可能化の規則	68
T10PI 対応のアレイの作成	69
T10PI 対応ディスク・プールの作成	69
T10PI 対応 RAID アレイの使用可能化および	
使用不可化	69
フル・ディスク暗号化 (FDE) 属性	73
ディスク・ストレージの構成	74

第 5 章 ホストの構成 113

SAN ブートを使用したホスト・オペレーティング・システムのブート	113
マルチパス・ドライバの概要	115
論理ドライブのフェイルオーバーおよびフェイルバックを自動的に管理するためのマルチパス・ドライバの使用	127
ホスト・バス・アダプターの使用	130
ホスト・バス・アダプターについて	130
ファイバー・チャネル・スイッチ環境における HBA の接続	130
マルチパス・ドライバのインストール	132
Windows MPIO または MPIO/DSM マルチパス・ドライバ	132
Storport ミニポート HBA デバイス・ドライバ	135
SCSIport ミニポート HBA デバイス・ドライバ	136
dsmUtil の使用	137
Veritas DMP DSM ドライバ	139
AIX マルチパス・ドライバ	139
Linux Device Mapper Multipath ドライバ	140
Linux RDAC (MPP) ドライバ	149
MAC OS マルチパス・ドライバ	154
Veritas DMP ドライバ	154
HP-UX PV-links	154
PV-links の使用: 方法 1	155
PV-links の使用: 方法 2	156
HP-UX 固有のマルチパス	158
Solaris フェイルオーバー・ドライバ	159
MPxIO ドライバのインストール	159
Solaris への RDAC フェイルオーバー・ドライバのインストールおよび構成ファイルの変更	165
Veritas DMP ドライバのインストールの計画と準備	168
デバイスの識別	170
SMdevices ユーティリティの使用	171
Windows オペレーティング・システムでの SMdevices の使用	171
UNIX タイプ・オペレーティング・システムでの SMdevices の使用	171
AIX ホストにおけるデバイスの識別	172
デバイスの構成	174
hot_add ユーティリティの使用	174
SMrepassist ユーティリティの使用	174
ホスト・エージェント・ソフトウェアの停止と再開	175
hdisk デバイスのキュー項目数の設定	176
キューの最大長の計算	176
Windows のキュー項目数の変更	177
AIX のキュー項目数の変更	177
キャッシュのミラーリングの使用不可化	177
動的容量拡張および動的論理ドライブ拡張の使用	177
SUSE Linux Enterprise Server での Veritas Storage Foundation	178

Red Hat Enterprise Linux での Veritas Storage

Foundation 5.0	179
LUN サイズの確認	180
論理ドライブの再配分	181
AIX での論理ドライブの再配分	181
HP-UX での論理ドライブの再配分	182
Solaris での論理ドライブの再配分	182
ホット・スワップ HBA の交換	183
AIX でのホット・スワップ HBA の交換	183
Linux での IBM HBA の交換	187
PCI ホット・プラグ HBA の交換	190
AIX および Linux 用ストレージ・サブシステムへの新しい WWPN のマッピング	191
HBA ホット・スワップ手順の完了	191
Windows DSM および Linux RDAC の設定	193
パス輻輳検出およびオンライン/オフライン・パス状態の設定の構成	199
T10PI をサポートするための DS5000 ストレージ・システムおよび AIX ホストのセットアップの詳細	201
DS5K ストレージ・ボックスのセットアップ	201
AIX ホストのセットアップ	202

第 6 章 フル・ディスク暗号化の処理 205

フル・ディスク暗号化	206
侵害に対するデータの保護	206
ローカル・セキュリティ・キー管理または外部セキュリティ・キー管理の選択	207
セキュリティ・キーの使用	208
ローカル・セキュリティ・キー管理でのセキュリティ・キーの変更	212
外部セキュリティ・キー管理でのセキュリティ・キーの変更	212
ストレージ・サブシステムのセキュリティ・キー・ファイルの識別	212
ローカル・セキュリティ・キー管理モードでのセキュア・ドライブのアンロック	219
外部セキュリティ・キー管理モードでのセキュア・ドライブのアンロック	219
セキュア消去の使用	220
FDE セキュリティ許可	221
FDE の用語	223
開始する前に	224
DS TKLM プロキシ・コード・サーバーのインストールおよび構成	224
DS TKLM プロキシ・コード・サーバーの始動、停止、および再始動	225
DS TKLM プロキシ・コード・サーバーの構成ファイルの変更	226
DS TKLM プロキシ・コードのインストール	229
Windows 環境での DS TKLM プロキシ・コード・サーバーのインストール	229
AIX または Linux 環境での DS TKLM プロキシ・コード・サーバーのインストール	230
FDE ドライブを使用したディスク暗号化の構成	231
FDE ドライブの取り付け	231
プレミアム・フィーチャーの使用可能化	232

RAID アレイのセキュア化	240
ディスク・ドライブのアンロック	246
FDE ドライブを使用するストレージ・サブシス テムのマイグレーション (ヘッド・スワップ)	249
ディスク・ドライブの消去	253
グローバル・ホット・スペア・ディスク・ドライ ブ	256
ログ・ファイル	257
よくある質問	258
アレイの保護	258
セキュア消去	259
ローカル・セキュリティ・キー管理	259
外部セキュリティ・キー管理	259
プレミアム・フィーチャー	260
グローバル・ホット・スペア・ドライブ	260
ブート・サポート	261
ロックおよびアンロック状態	261
バックアップおよびリカバリー	261
その他	261

第 7 章 Troubleshooting (トラブルシ ューティング) 263

重大イベントの問題解決	263
トレース・バッファの取り出し	283
構成データベース検証	284
データベースの保存/復元	285
DS 診断データ・キャプチャー (DDC)	286
リカバリー手順	287
DDC MEL イベント	288
AIX でのディスク・アレイのエラーの解決	289

付録 A. ホスト・バス・アダプターの設 定 295

HBA 設定の調整	295
Fast!UTIL による HBA 設定へのアクセス	295
デフォルトのホスト・バス・アダプター設定値	296
拡張 HBA 設定	297
QLogic ホスト・バス・アダプターの設定	298
JNI および QLogic ホスト・バス・アダプター設定 値	305
JNI HBA カード設定値	305
FCE-1473/FCE-6460/FCX2-6562/FCC2-6562 の 構成設定値	306
FCE-1063/FCE2-1063/FCE-6410/FCE2-6410 の 構成設定値	307
FCI-1063 の構成設定値	308
FC64-1063 の構成設定値	309
QLogic HBA 設定値	310

付録 B. VMware ESX Server 構成での ストレージ・サブシステムの使用 313

構成の例	313
ソフトウェア要件	314
管理ステーション	314
ホスト (VMware ESX Server)	314

ハードウェア要件	315
VMware ESX Server に関する制限	315
その他の VMware ESX Server ホストに関する情報	317
VMware ESX Server 用のストレージ・サブシステ ムの構成	317
VMware 接続の相互接続構成	317
VMware ESX Server での LUN のストレージ区 画へのマッピング	318
VMware のストレージ構成の検査	319

付録 C. 高可用性クラスター・サービス を備えたストレージ・マネージャーの使 用 321

一般情報	321
AIX システムにおけるクラスター・サービスの使用	321
High-Availability Cluster Multi-Processing	322
ソフトウェア要件	322
構成の制限	322
その他の HACMP の使用上の注	323
Parallel System Support Programs および General Parallel File System	323
ソフトウェア要件	323
構成の制限	323
その他の PSSP および GPFS の使用上の注	324
GPFS、PSSP、および HACMP クラスター構成 図	324
HP-UX システムにおけるクラスター・サービスの 使用	330
Solaris システムでのクラスター・サービスの使用	331
一般的な Solaris 要件	331
システムの依存関係	331
RDAC ID の追加	331
Single points of failure	331

付録 D. AIX オブジェクト・データ・マ ネージャー (ODM) 属性の表示および設 定 333

属性定義	333
ODM 属性を表示する lsattr コマンドの使用	338

付録 E. VDS/VSS プロバイダーについ て 341

付録 F. SMI-S プロバイダーのインスト ール 343

付録 G. アクセシビリティ 345

特記事項	349
商標	351
重要事項	351

用語集 353

索引 369



1. ネットワーク管理およびホスト・エージェント管理ストレージ・サブシステムを使用するサンプル・ネットワーク	3
2. 「Enterprise Management (エンタープライズ管理)」ウィンドウの各部	15
3. ディスク・プール自動構成	66
4. 保護情報 (P) チェック箇所	68
5. 論理ドライブ上での T10 PI の使用可能化	70
6. RAID ドライブ - 保護情報 (T10 PI) - 使用可能	71
7. 例 - RAID アレイ 4 の論理ドライブ 4 - T10PI 使用不可	72
8. T10PI の使用不可化	73
9. FDE 対応 RAID アレイ - セキュリティーの詳細	74
10. IBM i 用のポート ID の割り当て	93
11. ホスト・タイプとしての IBM i の選択	94
12. 「Script Editor (スクリプト・エディター)」ウィンドウ	110
13. 最適の単一パスの入出力フロー	116
14. 最適の 2 つのパスの入出力フロー	117
15. 一方のパスに障害が起きた場合、もう一方のパスを使用	118
16. 単一パス環境での入出力のフェイルオーバー	119
17. マルチパス環境での入出力のフェイルオーバー	120
18. AVT/ADT および RDAC フェイルオーバー・モードでコントローラーへのすべてのパスに障害	122
19. ALUA フェイルオーバー・モードでコントローラーへのすべてのパスに障害。フェイルオーバーの最初の 5 分間	123
20. ALUA モードでコントローラーへのすべてのパスに障害。障害が起きてから 5 分後	124
21. AIX fcp_array および Solaris RDAC を除くすべてのマルチパス・ドライバーに関する、ホスト HBA からストレージ・サブシステム・コントローラーへのマルチパス構成の例	128
22. AIX fcp_array および Solaris RDAC マルチパス・ドライバーに関する、ホスト HBA からストレージ・サブシステム・コントローラーへのマルチパス構成の例	129
23. 1 対 1 のゾーニング方式	131
24. 1 対 2 のゾーニング方式	131
25. セキュリティー有効 FDE ドライブ: 適切な正しい権限によって、アンロック状態でのデータの読み取りおよび書き込みが発生します	211
26. セキュリティー有効 FDE ドライブは、ストレージ・サブシステムから取り外されました: 正しい権限がない場合、盗まれた FDE ディスクはアンロックできず、データは暗号化されたままです	211
27. セキュリティー・キーの変更	213
28. セキュリティー・キーの変更 - 完了	214
29. ドライブのプロパティー - セキュア FDE ドライブ	215
30. ファイルの選択 - LockKeyID	217
31. ドライブのプロパティー - 非セキュア FDE ドライブ	218
32. セキュア消去プロセス	221
33. 外部セキュリティ・キー管理トポロジー	225
34. VMware ESX Server 構成の例	314
35. VMware 接続の相互接続構成	318
36. 単一のストレージ・サブシステム - 1 つから 4 つの区画が含まれるクラスター構成	325
37. 3 つのストレージ・サブシステム (サブシステムごとに 1 つの区画) が含まれるクラスター構成	326
38. 4 つのストレージ・サブシステム (サブシステムごとに 1 つの区画) が含まれるクラスター構成	327
39. 2 つのストレージ・サブシステム (サブシステムごとに 2 つの区画) が含まれる RVSD クラスター構成	328
40. 1 つのストレージ・サブシステム - 1 つの区画を持つ HACMP/GPFS クラスター構成	329
41. 2 つのストレージ・サブシステム (サブシステムごとに 2 つの区画) が含まれる HACMP/GPFS クラスター構成	330

表

1. テーブル・ビューに表示されるデータ	17	27. multipath.conf ファイルの属性およびパラメーター値	146
2. ストレージ・サブシステムの追加	18	28. multipath コマンドのオプションおよびパラメーター	148
3. ストレージ・サブシステムの除去	19	29. デバイス・マッパーのトラブルシューティング	148
4. 複数のサブシステムを同時に除去	19	30. mppUtil パラメーターの説明	152
5. 「Logical (論理)」タブのノード	22	31. 論理ドライブの優先パスおよび代替パスのサンプル・レコード	157
6. 「Topology (トポロジー)」ペイン内のノードのタイプ	25	32. フェイルオーバー・ドライバーの構成パラメーター	194
7. 「Defined Mappings (定義済みマッピング)」ペインのノード情報	26	33. 待ち時間設定のパラメーター	198
8. ストレージ・マネージャーのソフトウェア・パッケージのインストール・シーケンス	35	34. パス輻輳検出の構成設定	199
9. ストレージ・マネージャー・パッケージのインストール・コマンドの例	35	35. セキュリティー許可	221
10. ストレージ・マネージャー・パッケージのインストール検証コマンド	35	36. フル・ディスク暗号化の用語	223
11. サポートされるドライブ・タイプ、ドライブ・インターフェース、およびドライブ機能の要約	64	37. プロキシの構成ファイル・プロパティー	226
12. 保護情報メタデータ (8 バイト)	67	38. 重大イベント	264
13. アレイおよびディスク・プールに使用できるドライブのタイプ	75	39. リカバリー・ステップ 2	287
14. アレイおよびディスク・プールでサポートされるコピー・サービス	75	40. リカバリー・ステップ 4	287
15. ディスク・プールの予約済み容量	77	41. リカバリー・ステップ 5	288
16. アレイまたはディスク・プールでサポートされる機能のリスト	77	42. DDC MEL イベント	288
17. RAID レベルの説明	82	43. ディスク・アレイ・エラー	289
18. インストールされたコントローラー・キャッシュごとにサポートされるパフォーマンス読み取りキャッシュの最大サイズ	97	44. QLogic モデル QLA234x、QLA24xx、QLE2462、QLE2460、QLE2560、QLE2562、QMI2572、QMI3572、QMI2582	299
19. メディア・スキャン中に検出されるエラー	102	45. オペレーティング・システム別の QLogic モデル QL220x (BIOS V1.81 の場合) ホスト・バス・アダプターの設定	303
20. 「Subsystem Management (サブシステム管理)」ウィンドウのパフォーマンス・モニター・チューニング・オプション	104	46. FCE-1473/FCE-6460/FCX2-6562/FCC2-6562 の構成設定値	306
21. オペレーティング・システムでサポートされるロード・バランシング・ポリシー	105	47. FCE-1063/FCE2-1063/FCE-6410/FCE2-6410 の構成設定値	307
22. 各オペレーティング・システムのフェイルオーバー・モード	125	48. FCI-1063 の構成設定値	308
23. オペレーティング・システム別のマルチパス・ドライバー	127	49. FC64-1063 の構成設定値	309
24. オペレーティング・システム別の、各マルチパス・ドライバーがサポートするパスの数	129	50. QL2342 の構成設定値	310
25. dsmUtil パラメーター	137	51. dar デバイス属性	333
26. 各コンポーネントの最小必須バージョン	141	52. dac デバイス属性	335
		53. hdisk デバイス属性	335
		54. 例 1: dar の属性設定値の表示	338
		55. 例 2: dac の属性設定値の表示	338
		56. 例 3: hdisk の属性設定値の表示	339
		57. ストレージ・マネージャーの代替キーボード操作	346

本書について

本書では、IBM®System Storage® DS ストレージ・マネージャー バージョン 10.83 以降、およびコントローラー・ファームウェア・バージョン 7.8x.xx.xx 以降を使用したストレージ・サブシステム向け。IBM DS ストレージ・マネージャーが 10.83 より前の場合、「IBM System Storage DS ストレージ・マネージャー バージョン 10 インストールおよびホスト・サポートのガイド」を参照してください。本書は、ストレージ管理ソフトウェアをインストールする責任を持つシステム管理者およびストレージ管理者を対象としています。ストレージ・マネージャーを使用してストレージ・サブシステムをインストールおよび管理するには、RAID、SCSI、ファイバー・チャネル、および SATA テクノロジーについて理解している必要があります。また、管理ソフトウェアと共に使用される該当オペレーティング・システムの実務経験を持っている必要があります。

注： 本書に記載するスクリーン・ショットは説明の目的で示されており、ストレージ・マネージャーおよびコントローラー・ファームウェアのバージョンによっては、実際の UI と異なる場合があります。

本書において、ストレージ・マネージャー という用語は、すべてのホスト・ソフトウェア・リリース・レベルを指すものとします。

本書は、以下のタスクを行う場合に使用してください。

- ストレージ・マネージャーをインストールするために必要なハードウェアとソフトウェアを判別する。
- 必要なハードウェア・コンポーネントをネットワークに統合する。
- ストレージ・マネージャー ソフトウェアをインストールする。
- 必要に応じて、コントローラーのファームウェアをアップグレードする。
- インストール済み環境に固有のストレージ管理機能を識別して使用する。

重要： サポートされるオペレーティング・システムのリストに更新があるかどうかについては、ストレージ・マネージャーの README ファイルを確認してください。Web 上のストレージ・マネージャーの README ファイルにアクセスする方法については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

用語について詳しくは、ストレージ・マネージャー の「Enterprise Management (エンタープライズ管理)」ウィンドウまたは「Subsystem Management (サブシステムの管理)」ウィンドウのヘルプ・セクション、または 353 ページの『用語集』を参照してください。

この資料を読むときには、次の 2 つの用語の違いについて理解しておくことが重要です。

管理ステーション

管理ステーションは、ストレージ・サブシステムを管理するために使用されるシステムです。管理ステーションは、次のいずれかの方法を使用してストレージ・サブシステムに接続できます。

- ストレージ・サブシステムのコントローラーに対する TCP/IP イーサネット接続を通して。
- ホスト・コンピューター上にインストールされたホスト・エージェント・ソフトウェアとの TCP/IP 接続を介して。この場合も、ファイバー・チャネル入出力 (I/O) パスまたはコントローラーへの TCP/IP イーサネット接続のいずれかを介して、ストレージ・サブシステムに直接接続されます。

ホスト・コンピューター

ホスト・コンピューターは、ファイバー・チャンネル I/O パスを通してストレージ・サブシステムに直接接続されているシステムです。このシステムは、以下のタスクを実行するために使用されます。

- ストレージ・サブシステムからのデータを提供します (通常はファイルの形式で)。
- リモート管理ステーションのためのストレージ・サブシステムに対する接続ポイントとして機能します。

注:

1. この資料では、ホストと ホスト・コンピューター は同じ意味で使用されています。
2. ホスト・コンピューターは、管理ステーションとして機能することもできます。

このリリースの新機能

DS ストレージ・マネージャー バージョン 10.84 で提供される機能は、以下にリストされています。

- DS5020、DS5100、および DS5300 ストレージ・サブシステムで使用可能にされた VMware VAAI
- DS3500 および DCS3700 ストレージ・サブシステムで使用可能にされたパフォーマンス読み取りキャッシュ、拡張グローバル・ミラーリング (iSCSI 接続)、および拡張リモート・ミラーリング
- DS3500 サブシステムでサポートされる Solaris オペレーティング・システム
- プレミアム・フィーチャー・キット構成を以下に簡単にまとめます。
 - FlashCopy 論理ドライブ
 - パフォーマンス読み取りキャッシュ
 - 災害復旧オプション
 - 拡張グローバル・ミラーリング
 - 拡張リモート・ミラーリング
 - バックアップおよびリストア・オプション
 - Enhanced FlashCopy
 - スーパー・キー
 - パフォーマンス読み取りキャッシュ
 - 拡張グローバル・ミラーリング
 - 拡張リモート・ミラーリング
 - Enhanced FlashCopy

以下の表は、DS ストレージ・マネージャーのバージョン 10.83 で提供される機能について説明しています。

新機能	説明
ディスク・プール	アレイと同様に、ディスク・プールは、論理ドライブの作成元となる、論理的にグループ化されたディスク・ドライブの集合です。アレイとは異なり、ホット・スペア・ディスク・ドライブ、RAID レベル、およびセグメント・サイズを選択する必要はありません。ディスク・プールがこれらの属性を管理するからです。1 つのディスク・プールは、最小 11 個の SAS ハード・ディスク (HDD) で構成され、何百ものディスク・ドライブを含めることが可能です。ディスク・プールとアレイは 1 つのストレージ・サブシステム内に共存できます。 ディスク・プール論理ドライブ内のデータおよび冗長情報は、そのディスク・プール内のすべてのディスク・ドライブ間に分散されています。ディスク・プールのこの方法でのデータ分散により、次のようないくつかの利点が得られます。 • 構成の単純化 • ディスク・ドライブの使用効率の向上 • 保守の軽減 • シン・プロビジョニングの使用 ディスク・プールが使用可能なのは、DS3500 と DCS3700 ストレージ・サブシステム、および Performance Module Controller 搭載の DCS3700 ストレージ・サブシステム上に限定されます。これらのサブシステム上のコントローラー・ファームウェア・バージョンは、7.8x.xx.xx 以降でなくてはなりません。ディスク・プールについて詳しくは、74 ページの『ディスク・ストレージの構成』を参照してください。また、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプのトピック『Learn About Disk Pools and Disk Pool logical drives (ディスク・プールおよびディスク・プール論理ドライブの概要)』も参照してください。
シン論理ドライブ	標準論理ドライブの他に、シン論理ドライブも作成できるようになりました。シン論理ドライブの場合、容量はデータが書き込まれるにつれて割り振られます。シン・プロビジョニングを使用すると、標準論理ドライブで生じる可能性がある大量の未使用容量を除去することができ、先行投資コスト、フロア・スペース、エネルギー・コスト、および管理時間を最小限に抑えることができます。シン論理ドライブは、ディスク・プールからのみ作成することができ、アレイからは作成できません。 シン論理ドライブが使用可能なのは、DS3500 と DCS3700 ストレージ・サブシステム、および Performance Module Controller 使用の DCS3700 ストレージ・サブシステム上に限定されます。これらのサブシステム上のコントローラー・ファームウェア・バージョンは、7.8x.xx.xx 以降でなくてはなりません。シン論理ドライブについて詳しくは、85 ページの『シン論理ドライブの作成』を参照してください。また、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプのトピック『Thin logical drives (シン論理ドライブ)』も参照してください。

新機能	説明
Enhanced FlashCopy、Enhanced FlashCopy グループ、および Enhanced FlashCopy 論理ドライブ	Enhanced FlashCopy イメージは、論理ドライブの特定時点における論理的なイメージです。Enhanced FlashCopy イメージ機能は FlashCopy 機能に似ていますが、次のような相違点があります。 • 基本論理ドライブの特定時点のイメージが複数ある場合、新規の Enhanced FlashCopy イメージ機能ではパフォーマンスが向上します。FlashCopy 機能では、基本論理ドライブの FlashCopy ごとに 1 つのリポジトリ論理ドライブを使用します。新規の Enhanced FlashCopy イメージ機能では、基本論理ドライブに関連付けられた Enhanced FlashCopy イメージのグループごとに 1 つのリポジトリ論理ドライブを使用します。したがって、基本論理ドライブへの書き込み時に、新規の Enhanced FlashCopy イメージ機能では、Enhanced FlashCopy グループ内の Enhanced FlashCopy イメージごとに複数の順次書き込み操作を行う代わりに、1 回だけの書き込み操作で済みます。 • 新規の Enhanced FlashCopy イメージ機能には、Enhanced FlashCopy グループの概念が追加されています。複数の Enhanced FlashCopy イメージに対して 1 つだけリポジトリが存在するため、このリポジトリは、FlashCopy 機能の場合のように Enhanced FlashCopy イメージに関連付けられるのではなく、Enhanced FlashCopy グループに関連付けられます。 • FlashCopy 論理ドライブとは異なり、新規の Enhanced FlashCopy イメージは基本論理ドライブの変更データを保存するためにのみ使用されるため、ホストから直接 Enhanced FlashCopy イメージに読み取り/書き込みアクセスすることはできません。ホストに Enhanced FlashCopy イメージへの読み取り/書き込みアクセスを提供するには、最初に Enhanced FlashCopy イメージの Enhanced FlashCopy 論理ドライブを作成する必要があります。 基本論理ドライブから FlashCopy イメージまたは Enhanced FlashCopy イメージのいずれかを作成することができますが、両方を作成することはできません。 Enhanced FlashCopy イメージ、Enhanced FlashCopy グループ、および Enhanced FlashCopy 論理ドライブが使用可能なのは、DS3500 と DCS3700 ストレージ・サブシステム、および Performance Module Controller 搭載の DCS3700 ストレージ・サブシステム上に限定されます。これらのサブシステム上のコントローラー・ファームウェア・バージョンは、7.8x.xx.xx 以降でなくてはなりません。Enhanced FlashCopy イメージ、Enhanced FlashCopy グループ、および Enhanced FlashCopy 論理ドライブについて詳しくは、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプで、トピック『About Enhanced FlashCopy Operations (Enhanced FlashCopy 操作の概要)』を参照してください。コピー・サービス機能の詳細については、「<i>IBM System Storage DS Storage Manager Copy Services User's Guide</i>」を参照してください。
整合性グループ	複数の論理ドライブ上で同じ Enhanced FlashCopy イメージ操作を頻繁に実行する場合、整合性グループを作成することができます。整合性グループは、1 つのエンティティとして扱う、論理ドライブのグループです。整合性グループに対して実行する操作は、その整合性グループ内のすべての論理ドライブに対して同時に実行されます。整合性グループに対して実行できる Enhanced FlashCopy イメージ操作には、作成、スケジューリング、およびロールバックがあります。 整合性グループが使用可能なのは、DS3500 と DCS3700 ストレージ・サブシステム、および Performance Module Controller 搭載の DCS3700 ストレージ・サブシステム上に限定されます。これらのサブシステム上のコントローラー・ファームウェア・バージョンは、7.8x.xx.xx 以降でなくてはなりません。整合性グループについて詳しくは、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプで、トピック『Creating Consistency Groups (整合性グループの作成)』を参照してください。コピー・サービス機能の詳細については、「<i>IBM System Storage DS Storage Manager Copy Services User's Guide</i>」を参照してください。

新機能	説明
「Subsystem Management (サブシステム管理)」ウィンドウのメニュー構造	「Subsystem Management (サブシステム管理)」ウィンドウのメニュー構造が、より直観的に分かるように再配置されました。ストレージ・サブシステム・タスクは、「Storage subsystem (ストレージ・サブシステム)」、「Monitor (モニター)」、および「Upgrade (アップグレード)」の各メニュー下に配置されています。「Storage subsystem (ストレージ・サブシステム)」メニューには、ストレージ・サブシステムのセキュリティー、設定、および構成に関連したコマンドが含まれています。「Monitor (モニター)」メニューには、パフォーマンス、トラブルシューティング、およびレポート生成に関連したコマンドが含まれています。「Upgrade (アップグレード)」メニューには、ファームウェアのアップグレードに関連したコマンドが含まれています。 サンプル・コマンドを以下にいくつか示します。 • ストレージ・サブシステムを構成するには、「Storage subsystem (ストレージ・サブシステム)」 > 「Configuration (構成)」を選択します。 • ストレージ・サブシステム・プロファイルを表示するには、「Monitor (モニター)」 > 「Reports (レポート)」 > 「Storage subsystem profile (ストレージ・サブシステム・プロファイル)」を選択します。 • パフォーマンス・モニターを表示するには、「Monitor (モニター)」 > 「Health (ヘルス)」 > 「Monitor Performance (パフォーマンスのモニター)」を選択します。 • Recovery Guru を開くには、「Monitor (モニター)」 > 「Health (ヘルス)」 > 「View Health (Recovery Guru) (ヘルス (Recovery Guru) の表示)」を選択します。 • ファームウェアをアップグレードするには、「Upgrade (アップグレード)」 > 「Controller Firmware (コントローラー・ファームウェア)」 > 「Upgrade (アップグレード)」を選択します。 ディスク・プール、アレイ、および論理ドライブに関連した基本タスクは、「Storage (ストレージ)」メニューの下に配置されています。 論理ドライブのコピー、Enhanced FlashCopy イメージ、整合性グループ、FlashCopy、および同期ミラーリングに関連したコピー・サービス・タスクは、「Copy Services (コピー・サービス)」メニューの下に配置されています。 ホストおよびマッピング・タスクは、「Host Mappings (ホスト・マッピング)」メニューの下に配置されています。 エンクロージャー、コントローラー、およびディスク・ドライブに関連したハードウェア・タスクは、「Hardware (ハードウェア)」メニューの下に配置されています。 コピー・サービス機能の詳細については、「<i>IBM System Storage DS Storage Manager Copy Services User's Guide</i>」を参照してください。

新機能	説明
「Subsystem Management (サブシステム管理)」ウィンドウのタブ	「Subsystem Management (サブシステム管理)」ウィンドウの一部のタブが、以下のように名前変更または削除されています。 「Logical (論理)」タブは、「Storage & Copy Services (ストレージおよびコピー・サービス)」に名前変更されています。 「Mappings (マッピング)」タブは、「Host Mappings (ホスト・マッピング)」に名前変更されています。 「Physical (物理)」タブは、「Hardware (ハードウェア)」に名前変更されています。 「Support (サポート)」タブは削除されました。このタブ上の機能は、「Summary (要約)」タブに移動されました。 「Subsystem Management (サブシステム管理)」ウィンドウのタブについて詳しくは、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプで、トピック『Learn About the Subsystem Management Window (「Subsystem Management (サブシステム管理)」ウィンドウの概要)』を参照してください。コピー・サービス機能の詳細については、「IBM System Storage DS Storage Manager Copy Services User's Guide」を参照してください。
ストレージ・エンクロージャー・オブジェクトの検索およびフィルター	「Storage & Copy Services (ストレージおよびコピー・サービス)」タブでは、ストレージ・サブシステム・オブジェクトのツリー構造ビューに検索ボックスが含まれるようになり、オブジェクトを名前で簡単に検索できます。また、オブジェクトをタイプ別 (論理ドライブ、アレイ、ディスク・プール、Enhanced FlashCopy イメージ、リポジトリ、およびその他のタイプ) にフィルターに掛けることもできます。オブジェクトをフィルターに掛けるには、新規の「All Logical Objects (すべての論理オブジェクト)」ノードを選択し、表示するオブジェクト・タイプをドロップダウン・リストから選択します。 詳しくは、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプで、トピック『Using the Storage & Copy Services Tab (「Storage & Copy Services (ストレージおよびコピー・サービス)」タブの使用)』を参照してください。
サポート・データ収集のスケジュール	ストレージ・マネージャー・ソフトウェアを使用して、サポート・データの収集をスケジュールすることができます。サポート・データを定期的に収集し、週次または月次のレポートを生成できます。日次、週次、または月次で実行するスケジュールを作成できます。スケジュールリングをより簡単にするために、複数のストレージ・サブシステムを対象に同じスケジュールを同時に作成することができます。 サポート・データ収集のスケジュールリングについて詳しくは、「Enterprise Management (エンタープライズ管理)」ウィンドウのオンライン・ヘルプで、トピック『Scheduling Support Data Collection (サポート・データ収集のスケジュールリング)』を参照してください。

新機能	説明
デュアル・コントローラー・システムに対してサポートされる Asymmetric Logical Unit Access (ALUA)	論理ドライブを作成するときに、その論理ドライブの論理装置番号 (LUN) をマップします。この LUN に関連付けられたコントローラーは、その論理ドライブの優先所有者と呼ばれます。ホスト・オペレーティング・システムは常に、特定の論理ドライブに指定されたデータ入出力を、その論理ドライブの優先所有者であるコントローラーを介して送信しようと試みます。 ALUA は、デュアル・コントローラー・システムで使用可能なフェイルオーバーおよびフェイルバック・メカニズムです。コントローラー上で ALUA がサポートされているときに、ストレージ・サブシステム内の論理ドライブに対するデータ入出力アクセスが失われた場合、ホスト・オペレーティング・システムは自動的にデータ入出力を、優先所有者のコントローラーから非所有コントローラーに転送します。優先所有者のコントローラーが短期間内に作動可能になった場合、ALUA により、ホスト・オペレーティング・システムは自動的にデータ入出力処理を、非所有コントローラーから優先所有者コントローラーにフェイルバックします。 また、ホストが優先所有コントローラーと非所有コントローラーの両方から論理ドライブに入出力を送信することも許可します。非所有コントローラーに送信される入出力は、優先所有コントローラーが稼働しており最適の状態の場合、処理のために内部で優先所有コントローラーに送信されます。論理ドライブが 5 分間にわたって優先所有コントローラーよりも非所有コントローラーを介して 75 % を超えるデータ入出力を受け取る場合、論理ドライブの所有権が非所有コントローラーに移転されます。今度は、このコントローラーが入出力の処理の責任を持つことになります。優先コントローラーへの入出力は、代わりに、処理のために内部でこのコントローラーに送信されるようになります。非所有コントローラーは、論理ドライブの現行の所有者になりますが、優先所有者にはなりません。優先コントローラーが 5 分間にわたって論理ドライブへの 75 % を超える入出力を受け取るようになると、論理ドライブの所有権が変更されて優先コントローラーに戻ります。ALUA メカニズムについて、よりよく理解するためには、115 ページの『マルチパス・ドライバーの概要』を参照してください。
サポート・データの自動収集	ストレージ・マネージャー・ソフトウェアは、クライアント・モニター・プロセスがイベントを検出したときに、サポート・データのコピーを自動的に保存することができます。この機能は、「Subsystem Management (サブシステム管理)」ウィンドウから「Enterprise Management (エンタープライズ管理)」ウィンドウに移動され、一度に複数のストレージ・サブシステムに対してこの機能をセットアップできるようになりました。 サポート・データの自動収集について詳しくは、「Enterprise Management (エンタープライズ管理)」ウィンドウのオンライン・ヘルプで、トピック『Automatically Collect All Support Data (すべてのサポート・データの自動収集)』を参照してください。
試用版	試用版を使用すると、フィーチャーをご購入いただく前に評価することができます。特定の日数の間、フィーチャーをご使用いただけます。フィーチャーの機能に関する制限はありません。 試用版が使用可能なのは、DS3500 と DCS3700 ストレージ・サブシステム、および Performance Module Controller 使用の DCS3700 ストレージ・サブシステム上に限定されます。これらのサブシステム上のコントローラー・ファームウェア・バージョンは、7.8x.xx.xx 以降でなくてはなりません。試用版について詳しくは、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプで、トピック『Using a Trial Version of a Premium Feature (プレミアム・フィーチャーの試用版の使用)』を参照してください。

関連資料

本書の情報に加えて、下記のセクションで説明されているリソースを使用できます。

IBM Web サイト上のストレージ・マネージャー資料

以下の資料は、IBMWeb サイトからダウンロードできます (PDF)。

- *IBM System Storage DS® Storage Manager Command Line Interface and Script Commands Programming Guide*
- *IBM System Storage DS ストレージ・マネージャー コピー・サービスのユーザー・ガイド*
- *IBM System Storage DS4000® ファイバー・チャネルおよびシリアル ATA 混合使用でのプレミアム・フィーチャーのインストール概説*

これらの資料およびその他の IBM System Storage 資料に IBM サポート・ポータルからアクセスするには、以下の手順を実行します。

注: IBM サポート・ポータルに初めてアクセスする際、ご使用のストレージ・サブシステムの製品カテゴリ、製品ファミリー、および型式番号を選択する必要があります。次回、IBM サポート・ポータルにアクセスすると、最初を選択した製品が Web サイトによってプリロードされ、ご使用の製品用のリンクのみが表示されます。製品リストを変更するか、製品リストに追加するには、「**Manage my product lists (My プロダクト・リストの管理)**」リンクをクリックします。

1. <http://www.ibm.com/support/entry/portal> に進みます。
2. 「**Choose your products (製品の選択)**」で、「**Hardware (ハードウェア)**」を展開します。
3. 「**System Storage**」 > 「**Disk systems (ディスク・システム)**」 > 「**Mid-range disk systems (ミッドレンジ・ディスク・システム)**」 (DS4000 または DS5000 ストレージ・サブシステムの場合) または 「**Entry-level disk systems (エントリー・レベル・ディスク・システム)**」 (DS3000 ストレージ・サブシステムの場合) をクリックして、ご使用のストレージ・サブシステムのボックスにチェック・マークを付けます。
4. 「**Choose your task (タスクの選択)**」で、「**Documentation (資料)**」をクリックします。
5. 「**See your results (結果の表示)**」で、「**View your page (ページの表示)**」をクリックします。
6. 「**Product documentation (製品資料)**」ボックスで、アクセスしたい資料のリンクをクリックします。

ストレージ・マネージャーのオンライン・ヘルプおよび診断

ツールバーの「**Help (ヘルプ)**」をクリックするか、F1 キーを押すと、ストレージ・マネージャーの「**Enterprise Management (エンタープライズ管理)**」ウィンドウおよび「**Subsystem Management (サブシステム管理)**」ウィンドウからヘルプ・システムにアクセスできます。

「Enterprise Management (エンタープライズ管理)」ヘルプ・ウィンドウ

管理ドメイン全体の処理についてさらに知りたい場合は、このオンライン・ヘルプ・システムを使用してください。

「Subsystem Management (サブシステム管理)」ヘルプ・ウィンドウ

個々のストレージ・サブシステムの管理についてさらに知りたい場合は、このオンライン・ヘルプ・システムを使用してください。

ストレージ・マネージャーをインストールした後で、ホスト・バス・アダプター (HBA) 管理および診断アプリケーション (使用可能な場合) のインストールを検討してください。QLogic SANsurfer および Emulex HBAnyware アプリケーションは、ストレージ・サブシステムを使用する前に入出力接続の状況を検査するのに使用できる診断プログラムです。

ご使用のストレージ・サブシステムが、SAN 環境内でホスト・サーバーのファイバー・チャネル HBA に接続されている場合は、SAN 管理およびトラブルシューティングに役立つ IBM Tivoli® Storage Manager ソフトウェア・アプリケーションの購入をご検討ください。

ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出

ストレージ・マネージャー・ソフトウェアおよびコントローラー・ファームウェアは、ストレージ・マネージャー DVD から入手できます。また、Web からダウンロードすることもできます。

重要: ストレージ・マネージャーをインストールする前に、README ファイルをお読みください。更新済みの README ファイルには、最新バージョンのデバイス・ドライバー、ファームウェア・レベル、制限、および本書には記載されていないその他の情報が含まれています。

IBM IBM サポート・ポータルでファームウェアおよび README ファイルを検索するには、以下の手順を実行します。

注: IBM サポート・ポータルに初めてアクセスする際、ご使用のストレージ・サブシステムの製品カテゴリ、製品ファミリー、および型式番号を選択する必要があります。次回、IBM サポート・ポータルにアクセスすると、最初を選択した製品が Web サイトによってプリロードされ、ご使用の製品用のリンクのみが表示されます。製品リストを変更するか、製品リストに追加するには、「**Manage my product lists (My プロダクト・リストの管理)**」リンクをクリックします。

1. <http://www.ibm.com/support/entry/portal> に進みます。
2. 「**Choose your products (製品の選択)**」で、「**Hardware (ハードウェア)**」を展開します。
3. 「**System Storage**」 > 「**Disk systems (ディスク・システム)**」 > 「**Mid-range disk systems (ミッドレンジ・ディスク・システム)**」をクリックしてから、ご使用のストレージ・サブシステムのチェック・ボックスを選択します。
4. 「**Select OS (OS の選択)**」をクリックして、ご使用のオペレーティング・システムに対応するボックスにチェック・マークを付け、「**Submit (送信)**」をクリックします。
5. 「**Choose your task (タスクの選択)**」で、「**Downloads (ダウンロード)**」をクリックします。
6. 「**See your results (結果の表示)**」で、「**View your page (ページの表示)**」をクリックします。
7. 「**Product documentation (製品資料)**」ボックスで、アクセスしたい資料のリンクをクリックします。

IBM System Storage Productivity Center

IBM System Storage Productivity Center (SSPC) は、統合されたハードウェアおよびソフトウェアのソリューションの 1 つであり、IBM System Storage DS3000 システム、DS4000 システム、DS5000 システム、DS8000® システム、IBM System Storage SAN ボリューム・コントローラー・クラスター、およびご使用のデータ・ストレージ・インフラストラクチャーのその他のコンポーネントを管理するための単一の入り口を提供します。そのため、IBM System Storage Productivity Center を使用して、単一の管理インターフェースから複数の IBM System Storage 製品構成を管理することができます。

ストレージ・マネージャーを IBM System Storage Productivity Center に組み込む方法については、次の Web サイトにある IBM System Storage Productivity Center インフォメーション・センターを参照してください。

publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp

サポート情報に必須の Web サイト

ご使用の IBM ストレージ・サブシステムおよび DS ストレージ・マネージャーに関する資料、最新のソフトウェア、ファームウェア、および NVSRAM ダウンロードを含めた最新情報は、以下の Web サイトにあります。

IBM System Storage Disk Storage Systems

ソフトウェアおよびファームウェアのダウンロード、README ファイルへのリンク、および、すべての IBM System Storage ディスク・ストレージ・システムのサポート・ページへのリンクについては、次のサイトを参照してください。

<http://www.ibm.com/systems/support/storage/disk>

IBM System Storage Interoperation Center (SSIC)

ご使用のシステムの最新のファームウェア・バージョンを含めて、特定のストレージ・サブシステムおよびホスト構成の技術サポート情報については、次のサイトにある対話式 Web ベース・ユーティリティを使用して検索してください。

<http://www.ibm.com/systems/support/storage/config/ssic>

IBM DS3000、DS4000、DS5000、および BladeCenter® Boot Disk System プレミアム・フィーチャーの活化 プレミアム・フィーチャーを活動化するには、次のサイトにある Web ベースのユーティリティを使用してください。

<http://www.ibm.com/storage/fasttkeys>

IBM System Storage Productivity Center

IBM System Storage Productivity Center (IBM System Storage DS3000、DS4000、DS5000、DS8000、および SAN ボリューム・コントローラーに対して中央管理コンソールを提供するために設計された新しいシステム) の最新資料は、次のサイトにあります。

publib.boulder.ibm.com/infocenter/tivihelp/v4r1/index.jsp

IBM System Storage Support

ホスト・オペレーティング・システム、HBA、クラスタリング、ストレージ・エリア・ネットワーク (SAN)、ストレージ・マネージャー・ソフトウェアおよびコントローラー・ファームウェアの最新のサポート情報は、次のサイトにあります。

www.ibm.com/systems/support/storage

Storage Area Network (SAN) Support

SAN スイッチの使用に関する情報 (SAN 資料へのリンクなど) は、次の Web サイトにあります。

www.ibm.com/systems/support/storage/san

IBM System p® AIX 5L™ および Linux サーバー

System p AIX®、Linux、BladeCenter、および i5/OS® サーバーの最新のサポート情報については、次のサイトを参照してください。

www.ibm.com/systems/support/supportsite.wss/brandmain?brandind=5000025

IBM System x® サーバーのサポート

System x Intel および AMD ベースのサーバーの最新のサポート情報については、次のサイトを参照してください。

<http://www.ibm.com/systems/support/>

System p and AIX インフォメーション・センター

System p および POWER® サーバーでの AIX を使用方法に関する情報は、次の Web サイトにあります。

publib.boulder.ibm.com/infocenter/pseries/index.jsp?

IBM System Storage 製品

すべての IBM System Storage 製品に関する情報は、以下のサイトを参照してください。

www.ibm.com/systems/storage

IBM Publications Center

IBM 関連の資料は、以下のサイトを参照してください。

www.ibm.com/shop/publications/order/

情報、ヘルプ、およびサービスの入手

ヘルプ、サービス、技術支援、または IBM 製品に関する詳しい情報が必要な場合は、IBM がさまざまな形で提供している支援をご利用いただけます。このセクションでは、IBM および IBM 製品についての追加情報の入手先、システムで問題が発生した場合に行うべきこと、サービスが必要になった場合の連絡先などについて説明します。

依頼する前に

依頼する前に、以下の手順を実行して、お客様自身で問題の解決を試みてください。

- ケーブルがすべて接続されていることを確認します。
- 電源スイッチをチェックして、システムの電源がオンになっていることを確認します。
- ご使用のシステムに付属の資料に記載のトラブルシューティング情報を参照するか、診断ツールを使用します。
- このセクションにリストされている IBM System Storage Disk Support Web サイトに、技術情報、ヒント、および新しいデバイス・ドライバがあるか確認します。
- IBM Web サイトの IBM ディスカッション・フォーラムを使用して質問する。

IBM が提供しているストレージ・マネージャー・オンライン・ヘルプまたはご使用のシステムおよびソフトウェアに付属の資料の中にあるトラブルシューティング手順を実行することで、多くの問題は外部の支援を受けずに解決することができます。ご使用のシステムに付属の資料には、ユーザーが実行できる診断テストについても記載しています。大部分のサブシステム、オペレーティング・システム、およびプログラムには、トラブルシューティング手順およびエラー・メッセージおよびエラー・コードに関する説明書が付属しています。ソフトウェアの問題だと考えられる場合は、オペレーティング・システムまたはプログラムの資料を参照してください。

資料の使用

IBM システムおよびブリインストール・ソフトウェア (ある場合) に関する情報は、ご使用のシステムに付属の資料に記載されています。これには、印刷された資料、オンライン資料、README ファイル、およびヘルプ・ファイルが含まれます。診断プログラムの使用方法については、システム資料にあるトラブルシューティングに関する情報を参照してください。トラブルシューティング情報または診断プログラムを使用した結果、デバイス・ドライバの追加や更新、あるいは他のソフトウェアが必要になることがあります。

ソフトウェアのサービスとサポート

IBM サポート・ラインを利用すれば、有料で、使用法、構成、およびソフトウェアの問題について、電話での支援を受けることができます。使用する国または地域で、サポート・ラインがサポートする製品について詳しくは、以下の Web サイトをご覧ください。

www.ibm.com/services/sl/products

IBM サポート・ラインおよびその他の IBM サービスについて詳しくは、以下の Web サイトをご覧ください。

- www.ibm.com/services
- www.ibm.com/planetwide

ハードウェアのサービスとサポート

IBM Integrated Technology Services を通して、または IBM 販売店が保証サービスの提供を IBM から許可されている場合には販売店を通して、ハードウェア・サービスを受けることができます。サポートの電話番号については、以下の Web サイトをご覧ください。

www.ibm.com/planetwide

米国およびカナダでは、ハードウェア・サービスおよびサポートは、1 日 24 時間、週 7 日ご利用いただけます。英国では、これらのサービスは、月曜から金曜までの午前 9 時から午後 6 時までご利用いただけます。

本書の注意および注記

本書では、重要な情報を強調表示する以下の注記を使用しています。

- **注:** この注記は、重要なヒント、ガイダンス、またはアドバイスを示します。
- **重要:** この注記は、不都合な状況または問題のある状況を避けるのに役立つ可能性のある情報を提供します。
- **注意:** プログラム、装置、またはデータに損傷をもたらす可能性を示します。「注意」という注記は、損傷が発生する可能性がある説明または状況の直前に記載してあります。
- **警告:** これらの注記は、人身に危険をもたらす可能性がある状態を示します。「警告」の注記は、危険が発生する可能性がある手順のステップまたは状態の説明の直前に記載されます。

製品更新およびサポート通知の受け取り

以下のパッケージの最新バージョンを、初期インストール時および製品の更新が利用可能になったときにダウンロードしてください。

- ストレージ・マネージャー・ホスト・ソフトウェア
- ストレージ・サブシステム・コントローラー・ファームウェア
- ドライブ・ストレージ拡張エンクロージャー ESM ファームウェア
- ドライブ・ファームウェア

重要: サポート通知を受け取るためのサブスクリプションにより、最新のファームウェアおよびその他の製品更新を使用して、ご使用のシステムを最新の状態に保ってください。サポート通知を受け取るための登録方法については、次の Web サイトにアクセスして「**My notifications**」をクリックしてください。

<http://www.ibm.com/systems/support>

また、下記の IBM サポート・ポータル Web サイトを使用すると、製品更新およびサポート通知を見ることができます。

<http://www.ibm.com/support/entry/portal>

第 1 章 インストールの準備

以下の情報は、ストレージ・マネージャー・ソフトウェアを正常にインストールするために準備する上で役立ちます。

- 『ストレージ・マネージャー・ソフトウェア』
- 2 ページの『サポートされるコントローラー・ファームウェア』
- 2 ページの『インストール構成のタイプ』
- 7 ページの『ソフトウェアのインストールのためのコントローラーのアドレスのセットアップ』

紹介

IBM System Storage DS ストレージ・マネージャーは、管理ステーションから IBM DS3000、DS4000、および DS5000 ストレージ・サブシステムを管理するために使用できるクライアントとホストの一組のツールで構成されています。

ストレージ・マネージャーは、以下のオペレーティング・システムでサポートされます。

- AIX
- Windows Server 2003、Windows Server 2008、および Windows Server 2012
- Linux (RHEL および SLES)
- HP-UX
- Solaris

DS3000、DS4000、および DS5000 ストレージ・サブシステムは、Apple Mac OS、VMware ESX Server、および System p Virtual IO Server (VIOS) ホストに接続されている場合にもサポートされます。また、i5/OS でも VIOS 上のゲスト・クライアントとしてサポートされます。IBM では、これらのオペレーティング・システム用のホスト・ソフトウェアを提供していません。お客様は、上記にリストされたオペレーティング・システムのいずれかがインストールされている管理ステーションに IBM DS ストレージ・マネージャーをインストールする必要があります。

i5/OS サポートについては、以下の Web サイトを参照してください。

www.ibm.com/systems/i/os/

追加情報については、以下の Web サイトにある System Storage Interoperation Center を参照してください。

<http://www.ibm.com/systems/support/storage/config/ssic>

ストレージ・マネージャー・ソフトウェア

ストレージ・マネージャーは、ストレージ・サブシステムの構成、管理、およびトラブルシューティングに使用されます。このソフトウェアは主として、ディスク・プールまたは RAID アレイおよび論理ドライブの構成、ホストへの論理ドライブの割り当て、故障したディスク・ドライブの交換および再ビルド、ディスク・プール、アレイ、および論理ドライブのサイズの拡張、ならびに、ある RAID レベルから別の RAID レベルへの変換のために使用されます。ストレージ・マネージャーにより、ストレージ・サブシステム・コ

ンポーネントの状況の確認、RAID コントローラーのファームウェアの更新、ストレージ・サブシステムの管理など、トラブルシューティングおよび管理のタスクを実行することができます。最後に、ストレージ・マネージャーは、FlashCopy®、VolumeCopy、および拡張リモート・ミラーリングなどのプレミアム・フィーチャーへのアクセスを提供します。

各ストレージ・サブシステム・モデルでサポートされる最新ファームウェア・バージョンについては、ご使用のオペレーティング・システムの README ファイルを参照してください。

ストレージ・マネージャーのソフトウェア・コンポーネント

ストレージ・マネージャーには、以下のクライアント・ソフトウェア・コンポーネントが含まれています。

注: ストレージ・マネージャー・コンポーネントは、オペレーティング・システムによって異なる場合があります。ストレージ・マネージャー バージョン 10.77.xx.xx 以降では、Microsoft MPIO DSM インストーラーは、以下にリストされたコンポーネントをインストールするためのストレージ・マネージャー・インストーラーから分離されています。ただし、ストレージ・マネージャー・インストーラーと Microsoft MPIO DSM インストーラーは 1 つのコード・パッケージにバンドルされています。このコード・パッケージは、IBM サポート・ポータルで入手できます。

SMruntime ソフトウェア

ストレージ・マネージャー Java™ コンパイラー

SMesm ソフトウェア

ストレージ・マネージャー ESM ファームウェア・デリバリー・パッケージ

SMclient ソフトウェア

ストレージ・マネージャーのクライアント・パッケージ

SMagent ソフトウェア

ストレージ・マネージャーのエージェント・パッケージ

SMutil ソフトウェア

ストレージ・マネージャーのユーティリティ・パッケージ

サポートされるコントローラー・ファームウェア

コントローラー・ファームウェアのすべてのバージョンを、IBM Web サイトで無料で使用できます。

最高レベルの互換性とエラー・フリー操作を確保するには、ストレージ・サブシステムのコントローラー・ファームウェアを、必ずそのストレージ・サブシステム・モデル用の最新のファームウェア・バージョンにしておいてください。

重要: ストレージ・マネージャーのバージョン 10.84.xx.xx 以降では、6.50.xx.xx 以降のコントローラー・ファームウェアが必要です。

最新のファームウェア・バージョン・レベルをダウンロードする方法については、46 ページの『コントローラー・ファームウェア、NVSRAM、ESM ファームウェアのダウンロード』を参照してください。

インストール構成のタイプ

管理ステーションは、以下の構成のいずれかにすることができます。

ネットワーク構成 (アウト・オブ・バンド)

イーサネット・ネットワークに接続され、1 つ以上のストレージ・サブシステムを管理するために使用されるリモート・システム。

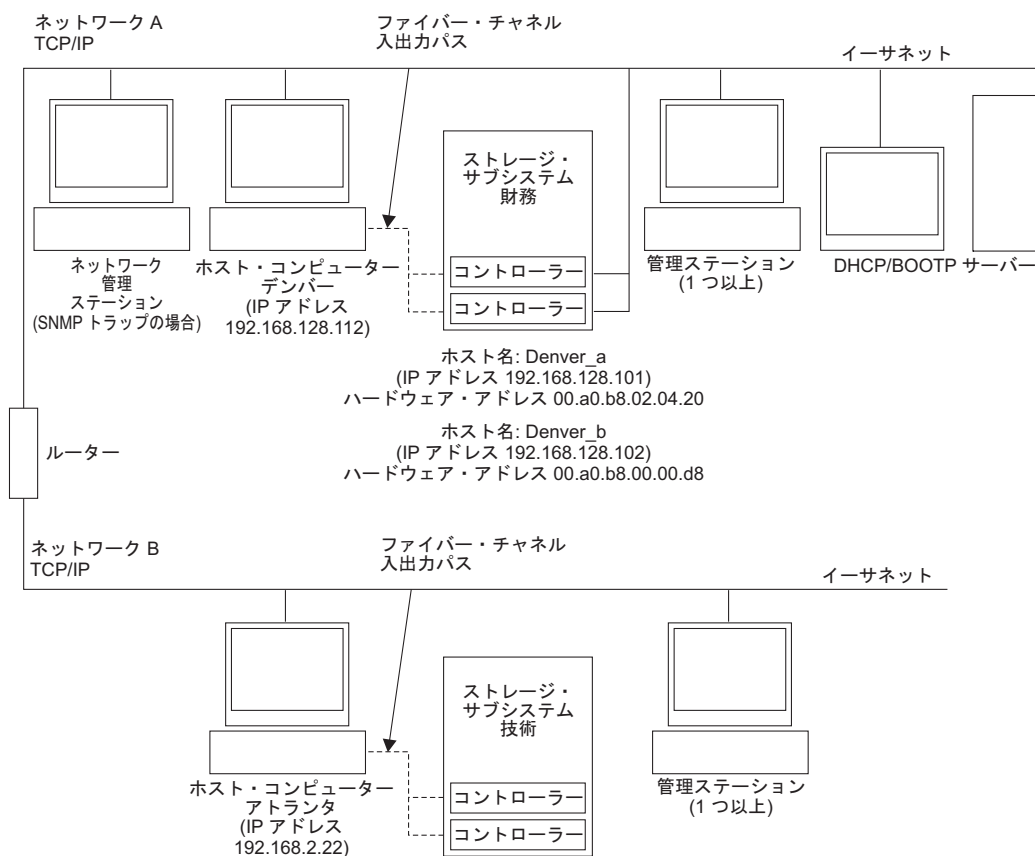
直接接続または SAN 接続構成 (インバンドまたはアウト・オブ・バンド)

ファイバー・チャネル、iSCSI、または SAS 入出力 (I/O) パスを通じてストレージ・サブシステムに接続されたホスト。このホストは、入出力パス (インバンド) またはイーサネット・ネットワーク・ポート (アウト・オブ・バンド) のいずれかを使用できます。

ネットワーク構成

ストレージ・マネージャー・ソフトウェアのインストールを開始する前に、ネットワーク・コンポーネントがセットアップされて正しく動作していること、およびソフトウェアを正しく動作させるために必要なホストとコントローラーに関するすべての情報が用意されていることを確認してください。

注: ストレージ・サブシステムをイーサネット・スイッチに接続する場合は、スイッチ・ポートの設定値を自動折衝に設定します。



SJ000882

図 1. ネットワーク管理およびホスト・エージェント管理ストレージ・サブシステムを使用するサンプル・ネットワーク

サンプル・ネットワーク構成の検討

3 ページの図 1 は、ネットワーク管理されるストレージ・サブシステム (ネットワーク A) とホスト・エージェントで管理されるストレージ・サブシステム (ネットワーク B) の両方を含むネットワークの例です。

ネットワーク管理ストレージ・サブシステム: ネットワーク A は、ネットワーク管理されるストレージ・サブシステムです。管理ステーションとストレージ・サブシステムの両方がイーサネット・ネットワークに接続されます。ネットワーク A には、以下のコンポーネントが含まれています。

- DHCP/BOOTP サーバー
- Simple Network Management Protocol (SNMP) トラップのためのネットワーク管理ステーション
- ファイバー・チャネル入出力パスを介してストレージ・サブシステムに接続されるホスト
- イーサネット・ケーブルでストレージ・サブシステム・コントローラーに接続される管理ステーション

注: コントローラーの静的 TCP/IP アドレス、またはデフォルト TCP/IP アドレスを使用する場合は、DHCP/BOOTP サーバーをセットアップする必要はありません。

ホスト・エージェント管理ストレージ・サブシステム: ネットワーク B は、ホスト・エージェントで管理されるストレージ・サブシステムです。ホスト・サーバーにインストールされたストレージ・マネージャー・エージェント・ソフトウェアを使用し、ホスト・サーバーがホストとストレージ・サブシステムの間で入出力を送信するために使用するのと同じパス (ファイバー・チャネルまたは SAS) を使用して、ストレージ・サブシステムを管理することができます。通常、ストレージ・サブシステムのイーサネット管理ポートは、イーサネット・ネットワークに接続されていません。

ストレージ・マネージャーのエージェントは、特別な LUN がホスト区画に割り当てられるかまたはマップされることを必要とします。この LUN は、アクセス LUN または UTM LUN と呼ばれ、ストレージ・マネージャー・エージェントおよびコントローラーによって管理情報を渡すために使用されます。この LUN は、論理ドライブがホスト区画に最初に割り当てられるときに、LUN 31 として自動的にホスト区画に割り当てられます。LUN は、ホストに割り当てることができる LUN/論理ドライブの最大数を 1 つ削減しているので、ストレージ・サブシステムがアウト・オブ・バンド方式のみを通じて管理されている場合、ストレージ・サブシステム管理 GUI を使用して、それを割り当て解除します。

注: ストレージ・サブシステムは、同時にインバンドおよびアウト・オブ・バンドで管理できます。ネットワーク B には、以下のコンポーネントが含まれています。

- サポートされている入出力パスを介してストレージ・サブシステムに接続されるホスト
- イーサネット・ケーブルでホスト・コンピューターに接続される管理ステーション

管理ステーションのセットアップ

管理ステーション は、すべてのストレージ・ネットワーク、またはその一部の管理を担当するサーバーです。これは、Simple Network Management Protocol (SNMP) といったネットワーク管理プロトコルを使用して、管理対象ノードのネットワーク管理エージェントと通信します。

ストレージ管理コマンドは、ストレージ・サブシステム・コントローラーに送信され、そこでコントローラー・ファームウェアがコマンドを検証および実行してから、クライアント・ソフトウェアに状況と構成情報を戻します。

ネットワーク管理 (アウト・オブ・バンド) 構成のセットアップ

以下の手順では、ネットワーク管理 (アウト・オブ・バンド) 構成のインストール済み環境向けにネットワークをセットアップするために必要な作業の概要について説明します。

重要: 最大 8 つの管理ステーションが同時にアウト・オブ・バンド管理ストレージ・サブシステムをモニターできます。この制限は、インバンド管理方式でストレージ・サブシステムを管理するサーバーには適用されません。

1. ネットワークに接続するすべてのハードウェア・コンポーネント (ホスト・コンピューター、ストレージ・サブシステム、ケーブル) を取り付け。ハードウェア・コンポーネントの取り付けについて詳しくは、ハードウェア・コンポーネントに付属の資料を参照してください。
2. ネットワークに接続される予定のストレージ・サブシステムに対する命名規則を設定する。
3. ストレージ・サブシステムの名前と管理タイプを記録する。

注: 以下の手順では、ハードウェアのイーサネット・アドレスや IP アドレスなどの情報を将来使用するために記録する必要があります。

4. ネットワークに接続されているストレージ・サブシステム内の各コントローラーに対するハードウェア・イーサネット MAC アドレスを決定する。デフォルト・コントローラー IP アドレスを使用する場合は、ステップ 6 に進みます。それ以外の場合は、ネットワーク上のストレージ・サブシステムの各コントローラーに対する TCP/IP アドレスとホスト名を、ネットワーク管理者から取得します。
5. 特定のコントローラーに対するネットワーク構成情報を提供するための DHCP/BOOTP サーバーをセットアップする。コントローラーの静的 IP アドレスを使用する場合は、このステップをスキップします。
6. TCP/IP ソフトウェアがインストールされていることを確認する。
7. ホスト・テーブルまたはドメイン・ネーム・サーバー (DNS) テーブルをセットアップする。
8. ネットワークに接続する装置の電源を入れる。

ホスト・エージェント管理 (インバンド) 構成のセットアップ

以下の手順では、ホスト・エージェント管理 (インバンド) 構成のインストール済み環境をセットアップするために必要な作業の概要について説明します。

1. 管理するすべてのハードウェア・コンポーネント (ホスト・コンピューター、ストレージ・サブシステム、およびケーブル) を取り付け。ハードウェア・コンポーネントの取り付けについて詳しくは、ハードウェア・コンポーネントに付属の資料を参照してください。ホスト・コンピューターで、ストレージ・サブシステムへの入出力接続が構成されている必要があります (例えば、ホストには、オペレーティング・システムがホスト・バス・アダプターに適切なデバイス・ドライバと共にインストールされている必要があります)。
2. ストレージ・マネージャー・ホスト・ソフトウェアおよびストレージ・マネージャー・エージェント・ソフトウェアをインストールする。
3. ネットワークに接続される予定のストレージ・サブシステムに対する命名規則を設定する。
4. ストレージ・サブシステムの名前と管理タイプを記録する。

注: 以下の手順では、ハードウェアのイーサネット・アドレスや IP アドレスなどの情報を将来使用するために記録する必要があります。

5. ホスト・エージェント・ソフトウェアを実行するホスト・コンピューターの IP アドレスとホスト名を、ネットワーク管理者から取得します。

注: SMagent は、ストレージ・マネージャー・ソフトウェア・パッケージの一部であり、サポートされるインターフェースを介してストレージ・サブシステムに接続されるホストで必要です。

6. TCP/IP ソフトウェアがインストールされていることを確認する。
7. ネットワークに接続する装置の電源を入れる。

注: ホストおよびストレージ・サブシステムの管理イーサネット・ポートをネットワークに接続しない場合でも、ホストは、ホスト・エージェントと通信するために TCP/IP を使用します。ホスト・エージェントは、アクセス・ボリューム を使用したファイバー・チャネル接続経由で、コントローラーと通信します。

直接接続および SAN 接続の構成

ストレージ・マネージャーは、直接接続構成、またはスイッチ経由の SAN 環境で、ストレージ・サブシステムのインバンド管理をサポートします。

直接接続構成のセットアップ

重要: iSCSI ポートを備えたストレージ・サブシステムは、ホスト・システムからストレージ・サブシステムの iSCSI ポートへの直接接続をサポートしません。

開始する前に、以下のことを確認してください。

- 1 つまたは 2 つのサーバーをストレージ・サブシステムに接続できます。
- 外部スイッチまたは外部ファイバー・チャネル・ハブを使用しません。
- 詳しくは、ご使用のストレージ・サブシステムの「*Installation and User's Guide*」を参照してください。

以下の手順を完了して、直接接続の構成をセットアップします。

1. ストレージ・サブシステムのコントローラー・ポートに、HBA を接続します。
2. ストレージ・マネージャーの自動ディスカバリー機能を使用して、ストレージ・サブシステムが検出されることを確認します。

SAN 接続の構成のセットアップ

SAN 接続の構成は、ファイバー・チャネル、SAS、または iSCSI 接続で構成することができます。

ご使用の SAN 接続構成でファイバー・チャネル HBA を使用する場合、HBA 接続とストレージ・サブシステム・ホスト・ポート接続をファブリック・ゾーン内で分離して、SAN ファブリック環境でのポート間の相互作用の可能性を最小限に抑える必要があります。ファイバー・チャネル、SAS、またはイーサネット・スイッチを介して、同一の HBA セットに対して複数のストレージ・サブシステムを構成できます。ファイバー・チャネルのゾーニング・スキームについて詳しくは、130 ページの『ファイバー・チャネル・スイッチ環境における HBA の接続』を参照してください。SAS スイッチおよびイーサネット・スイッチでも、同様のゾーニング・スキームを実装できます。

重要: 単一の HBA 構成では、パスに障害があるとデータ・アクセスの喪失につながる場合があります。SAN 接続構成内に単一の HBA がある場合は、ストレージ・サブシステムの両方のコントローラーは、スイッチ経由でその HBA に接続する必要があります。また、両方のコントローラーがその HBA と同じ SAN ゾーン内に存在している必要があります。

以下の手順を完了して、SAN 接続の構成をセットアップします。

1. HBA をスイッチ (複数の場合もある) に接続します。
2. ストレージ・サブシステムをスイッチ (複数の場合もある) に接続します。
3. ファイバー・チャネル・スイッチまたはイーサネット・スイッチ上に必要なゾーニングまたは VLAN を設定します (該当する場合)。
4. ストレージ・マネージャーの自動ディスカバリー機能を使用して、ストレージ・サブシステムが検出されることを確認します。

ソフトウェアのインストールのためのコントローラーのアドレスのセットアップ

ストレージ・サブシステムの管理方法が異なると、ソフトウェア・コンポーネントをインストールする場所が異なります。ソフトウェア・コンポーネントをインストールするには、事前にストレージ・コントローラーに IP アドレスを割り当てる必要があります。

注:

1. コントローラーを、データ速度を自動折衝するよう設定された LAN ポートに接続する必要があります。コントローラーは、固定レートに設定されたスイッチ・ポートに接続されていると、正しく機能しません。
2. ファイアウォールを介してストレージ・サブシステムを管理するには、ファイアウォールを構成して、ポート 2463 を TCP データに開きます。

ストレージ・サブシステム・コントローラーの IP アドレスのセットアップ

SMruntime および SMclient をインストールした後で、ホスト・オペレーティング・システムのインストール・セクションで説明されているように、以下の手順を完了してください。

DHCP または BOOTP サーバーおよび以下のコンポーネントをもつネットワークをセットアップする必要があります。

- DHCP サーバーまたは BOOTP サーバー
- Simple Network Management Protocol (SNMP) トラップのためのネットワーク管理ステーション
- ファイバー・チャネル入出力パスを介してストレージ・サブシステムに接続されるホスト
- イーサネット・ケーブルでストレージ・サブシステム・コントローラーに接続される管理ステーション

注: 静的 IP アドレスをコントローラーに割り当てることによって、DHCP/BOOTP サーバーおよびネットワーク・タスクを回避することができます。9 ページの『出荷時のデフォルト値の管理ポート TCP/IP アドレスを使用する静的 TCP/IP アドレスのストレージ・サブシステムへの割り当て』に示されているようにストレージ・サブシステムのデフォルト TCP/IP アドレスを使用して静的 TCP/IP アドレスをストレージ・マネージャーに割り当てることを望まない場合は、ストレージ・サブシステムへのインバンド管理接続を確立して、「Subsystem Management (サブシステム管理)」ウィンドウで管理ポートの IP アドレスを変更します。

コントローラーに 2 つの管理ポートがある場合、同じゲートウェイ・アドレスが 2 つのポート間で共有されます。最後に取得または指定されたゲートウェイ・アドレスが両方のポートに使用されます。そのため、一方のポートの構成を変更した結果として、もう一方のポートのアクセスが失われる可能性があります。両方のポートが手動で構成されている場合、最後に指定されたゲートウェイ・アドレスが使用されます。一方のポートが手動で構成されており、もう一方のポートで DHCP が使用可能になっている場合、最後に指定または取得されたゲートウェイ・アドレスが使用されます。一般的に、これは、もう一方のポートの手動構成が変更される場合を除き、DHCP サーバーによって指定されたゲートウェイ・アドレスになります。この場合、ゲートウェイ・アドレスは、コントローラーによって指定される値に設定される必要があります。この値は、DHCP サーバーから取得したゲートウェイ・アドレスと一致する必要があります。両方のポートで DHCP が使用可能になっている場合、2 つのポートに接続された DHCP サーバーは同じゲートウェイ・アドレスを指定するように構成される必要があります。DHCP サーバーが別々のゲートウェイ・アドレスを適用する場合、最後に取得されたゲートウェイ・アドレスが両方のポートに使用されます。

リモート・ログイン・アクセスに対する変更は、両方のポートに影響を与えます。つまり、一方のポートでリモート・ログイン・アクセスが使用可能または使用不可に設定されると、もう一方のポートでも使用可能

または使用不可に設定されます。ゲートウェイ・アドレスと同様、リモート・ログインに最後に適用された構成が両方のポートに適用されます。例えば、ポート 1 でリモート・ログイン・アクセスが手動で使用可能に設定されると、ポート 2 でも使用可能に設定されます。後で、DHCP サーバーが、リモート・ログイン・アクセスの使用不可化を含む構成パラメーターをポート 2 に指定した場合、両方のポートで使用不可になります。

コントローラーに 2 つの管理ポートがある場合、2 つのイーサネット・ポートは別々のサブネット上になければなりません。両方のポートが同じサブネット上にある場合、またはネットワーク・アドレス (IP アドレスとサブネット・マスクの論理積) が同じである場合、サブネット構成エラー・イベント通知が発生します。

DHCP/BOOTP サーバーでの IP アドレスのセットアップ

以下の手順を完了して、DHCP/BOOTP サーバーおよびネットワークをセットアップします。

1. それぞれのストレージ・サブシステム・コントローラーから MAC アドレスを入手します。(『イーサネット MAC アドレスの識別』の手順を参照してください。)
2. 以下の手順のうち、サーバーに適切な方を完了します。
 - DHCP サーバーで、それぞれの MAC アドレスの DHCP レコードを作成します。リース期間を可能な限り長い時間に設定します。
 - BOOTP サーバーで、bootptab ファイルを編集して、MAC アドレス・タブを TCP/IP アドレスに関連付ける項目を追加します。
3. DS3000/DS4000/DS5000 ストレージ・サブシステムのイーサネット・ポートをネットワークに接続します。
4. ストレージ・サブシステムをブートします。

イーサネット MAC アドレスの識別

直接管理 (アウト・オブ・バンド) 方式を使用してストレージ・サブシステムを管理するには、各コントローラーに対するハードウェア・イーサネット・メディア・アクセス制御 (MAC) アドレスを識別する必要があります。

すべてのストレージ・サブシステムには、ハードウェア・イーサネット MAC アドレス番号が記載されたラベルがあります。この番号の形式は `xx.xx.xx.xx.xx.xx` です。ここで、`x` は文字または数字を表します。例えば、イーサネット MAC アドレスは `00.a0.b8.20.00.d8` になる場合があります。

特定のストレージ・サブシステムの説明およびラベルの位置は、以下のセクションにリストされています。

DS4800、DS5100、または DS5300 ストレージ・サブシステムでのイーサネット MAC アドレスの識別:

マシン・タイプ、型式番号、およびシリアル番号は、各 RAID コントローラー・ユニットの上部に記載されています。MAC アドレスは、各 RAID コントローラーのイーサネット・ポートの近くにあります。

注: コントローラーには、DS4800、DS5100、または DS5300 のシャーシの背面からアクセスできます。

DS3000、DS3500、DCS3700、DS3950、DS4200、DS4700、DS5020、または Performance Module

Controller 使用の DCS3700 ストレージ・サブシステムのイーサネット MAC アドレスの識別: これらのストレージ・サブシステムの MAC アドレスは、各 RAID コントローラーのイーサネット・ポートの近くにあります。

注: コントローラーには、ストレージ・サブシステムのシャーシの後ろ側からアクセスできます。

DS4400、または DS4500 ストレージ・サブシステムでのイーサネット MAC アドレスの識別: DS4400 および DS4500 ストレージ・サブシステムでのハードウェア・イーサネット MAC アドレスを識別するには、以下の手順を実行してください。

1. ストレージ・サブシステムから前面ベゼルを取り外し、注意しながらベゼルの下部を外側に引いて、ピンを外します。その後、ベゼルを下方にスライドさせます。
2. 各コントローラーの前面で、ハードウェア・イーサネット MAC アドレスが記載されたラベルを探す。番号は `xx.xx.xx.xx.xx.xx` のような形式になっています (例: 00.a0.b8.20.00.d8)。
3. 各イーサネット MAC アドレスを記録してください。
4. ベゼルの元に戻すには、上端をシャーシのリップの下に滑り込ませる。その後、ベゼルの下部を押して、ピンを取り付け穴にはめ込む。

DS4100、または DS4300 ストレージ・サブシステムでの Ethernet MAC アドレスの識別: マシン・タイプ 3542 (DS4100、または 1722 (DS4300) に対するハードウェア・イーサネット MAC アドレスを識別するには、以下の手順を実行します。

1. 装置の背面の、コントローラー・ファイバー・チャンネル・ホスト・ポートの下で、イーサネット MAC アドレスを探す。番号は `xx.xx.xx.xx.xx.xx` のような形式になっています (例: 00.a0.b8.20.00.d8)。
2. 各イーサネット MAC アドレスを記録してください。

出荷時のデフォルト値の管理ポート TCP/IP アドレスを使用する静的 TCP/IP アドレスのストレージ・サブシステムへの割り当て

製造時にコントローラーに割り当てられたデフォルト TCP/IP アドレスを使用して、ストレージ・サブシステム・コントローラーに静的 TCP/IP アドレスを割り当てるには、以下の手順を実行します。

1. コントローラーのデフォルト TCP/IP アドレスを使用して、ストレージ・サブシステムへの直接管理接続を行います。ご使用のストレージ・サブシステムのデフォルト TCP/IP アドレスを見つけるために、#1 とラベルされたコントローラー管理ポートに取り付けられたハードウェアと共に出荷される「*Installation and User's Guide*」を参照してください。
 - コントローラー A: 192.168.128.101
 - コントローラー B: 192.168.128.102
 - サブネット・マスク: 255.255.255.0

注: コントローラーごとに 2 つのイーサネット・ポートを実装したストレージ・サブシステム (DCS3700、Performance Module Controller を装備した DCS3700、DS5020、DS3500、DS5100 および DS5300) の場合、#2 とラベルされたイーサネット・ポートを使用します。2 番目のイーサネット・ポートのデフォルト IP アドレスは、以下の通りです。

- コントローラー A: 192.168.129.101
 - コントローラー B: 192.168.129.102
 - サブネット・マスク: 255.255.255.0
2. SMclient を開始します。「Enterprise Management (エンタープライズ管理)」ウィンドウが開きます。
 3. 「Enterprise Management (エンタープライズ管理)」ウィンドウで、デフォルトのストレージ・サブシステムの名前をクリックします。「Subsystem Management (サブシステム管理)」ウィンドウが開きます。
 4. 「Subsystem Management (サブシステム管理)」ウィンドウで、コントローラー・アイコンを右クリックして、メニューで、「Change (変更)」 > 「Network Configuration (ネットワーク構成)」を選択します。「Change Network Configuration (ネットワーク構成の変更)」ウィンドウが開きます。

5. 「Change Network Configuration (ネットワーク構成の変更)」ウィンドウで、**コントローラー A** および **コントローラー B** のタブをクリックして、新規の TCP/IP アドレスを該当するフィールドに入力します。「OK」をクリックします。
6. 「Subsystem Management (サブシステム管理)」ウィンドウを閉じて、5 分待ち、それから「Enterprise Management (エンタープライズ管理)」ウィンドウの、デフォルト ストレージ・サブシステム項目を削除します。
7. 新規 TCP/IP アドレスを使用して、新規ストレージ・サブシステム項目を「Enterprise Management (エンタープライズ管理)」ウィンドウに追加します。

インバンド管理接続を使用する静的 TCP/IP アドレスのストレージ・サブシステムへの割り当て

ファイバー・チャネル入出力パスを介してストレージ・サブシステムに接続されるホストの場合は、以下の手順を完了して、静的 TCP/IP アドレスを、ストレージ・サブシステム・ファイバー・チャネル・ホスト・ポートへ接続しているホストを介してストレージ・サブシステム・コントローラーに割り当てます。

この手順を完了するには、以下のコンポーネントを持っていない必要ありません。

- ファイバー・チャネル入出力パスを介してストレージ・サブシステムに接続されるホスト
- イーサネット・ケーブルでストレージ・サブシステム・コントローラーに接続される管理ステーション

注: ストレージ・サブシステムに iSCSI 接続しているホストを使用したインバンド管理は、この構成が完了するまでは実行できません。代わりに、このセクションの他の方法を使用して、静的 TCP/IP アドレスをストレージ・サブシステム・コントローラー管理ポートへ割り当てます。

1. ホストに DS ストレージ・マネージャー・クライアント・ソフトウェアをインストールし、SMagent ソフトウェアがインストールされて稼働していることを確認します。
2. DS ストレージ・マネージャー・クライアント・ソフトウェアを開始します。「Enterprise Management (エンタープライズ管理)」ウィンドウが開きます。
3. ストレージ・サブシステムへファイバー・チャネル接続しているホストの IP アドレスを使用して、ストレージ・サブシステムをエンタープライズ管理ドメインに追加します。
4. 「Enterprise Management (エンタープライズ管理)」ウィンドウで、新しくディスカバリーされたストレージ・サブシステムの名前をクリックします。「Subsystem Management (サブシステム管理)」ウィンドウが開きます。
5. 「Subsystem Management (サブシステム管理)」ウィンドウで、コントローラー・アイコンを右クリックして、ドロップダウン・メニューで、「Change (変更)」 > 「Network Configuration (ネットワーク構成)」を選択します。「Change Network Configuration (ネットワーク構成の変更)」ウィンドウが開きます。
6. 「Change Network Configuration (ネットワーク構成の変更)」ウィンドウで、コントローラー A およびコントローラー B のタブをクリックして、新規の TCP/IP アドレスを該当するフィールドに入力します。
7. 「OK」をクリックします。
8. 「Subsystem Management (サブシステム管理)」ウィンドウを閉じます。
9. 最低 5 分待ちます。
10. 「Enterprise Management (エンタープライズ管理)」ウィンドウで、既存のストレージ・サブシステム項目を削除します。
11. 該当する場合には、管理ステーションでイーサネット・ポートの IP アドレスを、割り当てたばかりのコントローラー・イーサネット・ポート IP アドレスと同じ TCP/IP サブネット上の値に変更します。

12. DS ストレージ・マネージャーを終了します。
13. 再始動します。
14. コントローラー管理ポートへのイーサネット・ケーブル接続を行います。
15. 新規に割り当てられた IP アドレスを使用して、「Enterprise Management (エンタープライズ管理)」ウィンドウで、新規ストレージ・サブシステム項目を追加します。

ストレージ・サブシステム・コントローラー・シリアル・ポートのサービス・インターフェースを使用する静的 TCP/IP アドレスの割り当て

注: ファイアウォールを介してストレージ・サブシステムを管理するには、ファイアウォールを構成して、ポート 2463 を TCP データに開きます。

この手順を完了するには、以下のコンポーネントを持っていないけません。

- ホストのシリアル・ポートをコントローラーのシリアル・ポートに接続するのに使用される、両端に DB-9 メス・コネクタのあるヌル・モデムのケーブル。
- ホスト・システムにインストールされる、Procomm または Microsoft Windows Hyperterm といった、端末エミュレーション・ソフトウェア・アプリケーション。

注:

1. 端末セッションの設定には、以下の値が必要です。すなわち、38400 BAUD、8 つのデータ・ビット、1 つのストップ・ビット、パリティなし。
2. コントローラーのボー・レート設定が端末の設定と異なる場合は、「ブレイク」文字を送信して、コントローラーが次に使用可能なボー・レート設定に切り替わるようにします。「Press space to set the BAUD rate (スペースを押してボー・レートを設定する)」というメッセージが表示されるまで、ブレイク文字の送信を繰り返します。
- コントローラー・ファームウェア・バージョン 7.77.xx.xx 以降およびそれに関連する NVSRAM ファイルがインストールされます。

以下の手順を実行して、新規 IP アドレスを表示し、それをコントローラー管理ポートに割り当てます。

1. **Enter** キーを押します。次の文字 (->) が表示された場合には、**Exit (終了)** を入力し、**Enter** キーを押します。そうでない場合には、次のステップに進み続行します。
2. 端末エミュレーター・セッションで、ブレイク文字を送信します。例えば、Microsoft Windows Hyperterm に対して **CNTL+BREAK** を、Procomm に対して **ALT+B** を使用します。
3. 次のメッセージ「Press within 5 seconds: for <S> Service Interface, <BREAK> for baud rate (サービス・インターフェースの場合は <S> を、ボー・レートの場合は <BREAK> を、5 秒以内に押します)」が表示されたときに、大文字 **S** を入力し、**Enter** キーを押します。
4. 次のメッセージ「Enter the password to access the Service Interface (60 second timeout) (サービス・インターフェースにアクセスするためにパスワードを 60 秒以内に入力します (60 秒のタイムアウト))」が表示されてから 60 秒以内にパスワード **DSSStorage** (大/小文字の区別) を入力します。

注: コントローラーに、コントローラー・ファームウェア・バージョン 7.77.xx.xx 以降およびそれに関連する NVSRAM ファイルがインストールされていない場合、このパスワードは受け付けられず、ユーザーは以下の 2 つのうちいずれかに従って、コントローラー・イーサネット・ポートの IP 構成を変更する必要があります。詳細については、9 ページの『出荷時のデフォルト値の管理ポート TCP/IP アドレスを使用する静的 TCP/IP アドレスのストレージ・サブシステムへの割り当て』および 10 ページの『インバンド管理接続を使用する静的 TCP/IP アドレスのストレージ・サブシステムへの割り当て』を参照してください。

5. 以下のメニューが表示された場合には、1 または 2 を入力して、IP 構成を表示または変更します。

```
Service Interface Main Menu
=====
1) Display IP Configuration
2) Change IP Configuration
3) Reset Storage Array Administrator Password
Q) Quit Menu
```

オプション 2 を選択した場合には、プロンプトに従って、選択したポートの IP 構成を設定します。設定を有効にするためには、コントローラーをリブートする必要があります。

注: これらの手順を、両方のコントローラーに対して実行する必要があります。

第 2 章 ストレージ・マネージャーのインターフェース

この章では、サブシステム上のストレージ・マネージャー・ソフトウェアの基本的なレイアウトについて説明します。ここで、ストレージ・マネージャーのバージョンは 10.84.xx.xx、コントローラー・ファームウェアのバージョンは 7.84.xx.xx です。

ストレージ・マネージャーには、ストレージ・サブシステムの管理機能とグラフィカル表現を提供する 2 つのウィンドウがあります。すなわち、「Enterprise Management (エンタープライズ管理)」ウィンドウと「Subsystem Management (サブシステム管理)」ウィンドウです。

管理およびモニターするストレージ・サブシステムを追加するには、「Enterprise Management (エンタープライズ管理)」ウィンドウを使用します。「Enterprise Management (エンタープライズ管理)」ウィンドウでは、ストレージ・サブシステムに影響を与えているクリティカル・エラーのアラート通知を受け取ります。

「Enterprise Management (エンタープライズ管理)」ウィンドウでストレージ・サブシステムが「Optimal (最適)」状態にないという通知を受け取った場合、影響を受けたストレージ・サブシステム用の「Subsystem Management (サブシステム管理)」ウィンドウを開いて、ストレージ・サブシステムの状態についての詳細情報を表示することができます。

重要: ご使用のストレージ・マネージャーおよびコントローラー・ファームウェアのバージョンに応じて、ビュー、メニュー・オプション、および機能が、本書内の情報と異なる場合があります。使用可能な機能に関する情報は、ストレージ・マネージャーのオンライン・ヘルプ・トピックを参照してください。

「Enterprise Management (エンタープライズ管理)」ウィンドウ

「Enterprise Management (エンタープライズ管理)」ウィンドウは、ストレージ・マネージャーの開始時に最初に開くウィンドウです。「Enterprise Management (エンタープライズ管理)」ウィンドウを使用して、以下の管理タスクを実行します。

- ローカル・サブネットワーク上のインバンド・ホストおよびアウト・オブ・バンド・ストレージ・サブシステムを自動的に検出する
- インバンド・ホストおよびストレージ・サブシステムを手動で追加および削除する
- ストレージ・サブシステムの正常性をモニターし、該当するアイコンを使用してハイレベル状況を報告する
- E メールまたは Simple Network Management Protocol (SNMP) を使用したアラート通知を構成し、構成されたアラート宛先に重大イベントを報告する

注: 追加したストレージ・サブシステムおよび構成した E メール宛先または SNMP トラップに関する情報はすべて、ローカル構成ファイルに保管されます。

- 選択されたストレージ・サブシステムに適用できる「Subsystem Management (サブシステム管理)」ウィンドウを開いて、詳細な構成操作および管理操作を実行する
- 特定のストレージ・サブシステム上でバッチ管理タスクを実行するためのスクリプトを実行する。

注: 例えば、新規論理ドライブを作成したり、新しいコントローラー・ファームウェアをダウンロードするためのスクリプトを実行できます。スクリプトの実行についての詳細は、「IBM System Storage DS

Storage Manager Command Line Interface and Script Commands Programming Guide」または「Enterprise Management (エンタープライズ管理)」ウィンドウのオンライン・ヘルプ・トピックを参照してください。

- クライアント・モニター・プロセスが重大イベントを検出した場合、サポート・データのコピーの保存をスケジュールする、または自動的に保存する。
- メジャー・コントローラー・ファームウェア・バージョン間でコントローラー・ファームウェアをアップグレードする (例えば、コントローラー・ファームウェアをバージョン 6.xx.xx.xx から 7.xx.xx.xx にアップグレードする)。この機能は、スタンドアロンの IBM System Storage コントローラー・ファームウェア・アップグレード・ツールの機能と同じです。このツールは、IBM DS Storage Manager クライアント・バージョン 10.50.xx.xx 以降に組み込まれています。
- 定義された間隔で 1 つまたはすべてのストレージ・サブシステム上のすべてのサポート情報の収集をスケジュールする。
- すべてのストレージ・サブシステムのファームウェア・インベントリを取り出す。

ツールバーおよびステータス・バーを表示または非表示にするには、メニューから「View (表示)」を選択し、「Tool (ツール)」オプションまたは「Status (ステータス)」オプションを選択またはクリアします。

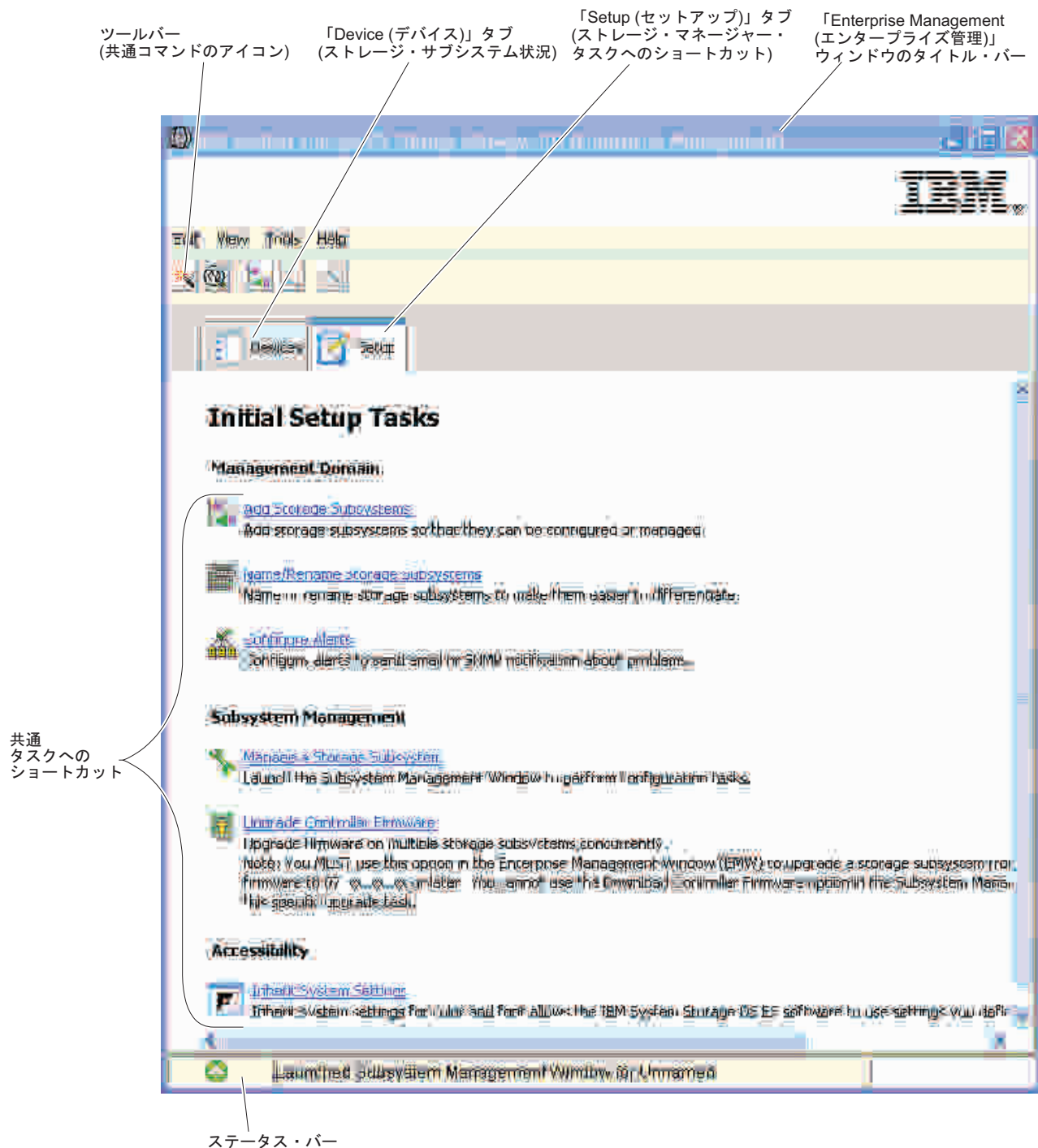


図 2. 「Enterprise Management (エンタープライズ管理)」ウィンドウの各部

「Devices (デバイス)」タブの使用

「Enterprise Management (エンタープライズ管理)」ウィンドウの「Devices (デバイス)」タブは、管理セッションによって管理されているストレージ・サブシステムのツリー・ビューとテーブル・ビューの 2 つのビューを表示します。

ツリー・ビュー

ツリー・ビューは、ストレージ・サブシステム内のノードの階層ビューを表示します。ツリー・ビューには、2 つのタイプのノードが表示されます。

- Discovered Storage Subsystems (検出されたストレージ・サブシステム)
- Unidentified Storage Subsystems (未確認のストレージ・サブシステム)

「Discovered Storage Subsystems (検出されたストレージ・サブシステム)」ノードと「Unidentified Storage Subsystems (未確認のストレージ・サブシステム)」ノードは、「Management Station (管理ステーション)」ノードの下位ノードです。

「Discovered Storage Subsystems (検出されたストレージ・サブシステム)」ノードには、管理ステーションによって現在管理されているストレージ・サブシステムを表す下位ノードがあります。各ストレージ・サブシステムは、マシン名でラベル付けされ、ツリー・ビューに常に存在します。ストレージ・サブシステムおよびストレージ・サブシステムが接続されたホストが「Enterprise Management (エンタープライズ管理)」ウィンドウに追加されると、そのストレージ・サブシステムは「Discovered Storage Subsystems (検出されたストレージ・サブシステム)」ノードの下位ノードになります。

注: 「Discovered Storage Subsystems (検出されたストレージ・サブシステム)」ノード上にマウスを移動すると、コントローラー IP アドレスを表示したツールチップが現れます。

「Unidentified Storage Subsystems (未確認のストレージ・サブシステム)」ノードには、ネットワーク接続の問題、サブシステムが電源オフ、または存在しない名前が原因で管理ステーションがアクセスできないストレージ・サブシステムが表示されます。

ツリー・ビュー内のノードに対して、以下のアクションを実行できます。

- 管理ステーション・ノードおよび「Discovered Storage Subsystems (検出されたストレージ・サブシステム)」ノードをダブルクリックして、下位ノードの表示を拡張または縮小する。
- ストレージ・サブシステム・ノードをダブルクリックして、そのストレージ・サブシステム用の「Subsystem Management (サブシステム管理)」ウィンドウを起動する。
- 「Discovered Storage Subsystems (検出されたストレージ・サブシステム)」ノードをダブルクリックして、そのノードに適用できるアクションが含まれているメニューを開く。

「Discovered Storage Subsystems (検出されたストレージ・サブシステム)」ノード用のメニューを右クリックすると、以下のオプションが含まれています。

- **Add Storage Subsystem** (ストレージ・サブシステムの追加)
- **Automatic Discovery** (自動ディスカバリー)
- **Refresh** (最新表示)
- **Collect Support Data** (サポート・データの収集)
 - automatically (自動)
 - create/edit schedule (スケジュールの作成/編集)

ストレージ・サブシステム・ノードのメニューを右クリックすると、以下のオプションが含まれています。

- **Manage storage subsystem** (ストレージ・サブシステムの管理)
- **Locate storage subsystem** (ストレージ・サブシステムの検索)
- **Execute script** (スクリプトの実行)
- **Load storage subsystem configuration** (ストレージ・サブシステム構成のロード)

- Upgrade controller firmware (コントローラー・ファームウェアのアップグレード)
- Refresh (最新表示)
- Remove storage subsystem (ストレージ・サブシステムの除去)
- Remove management connection (管理接続の除去)
- Configure Alerts (アラートの構成)
- Collect support data automatically (サポート・データの自動収集)
- Create/Edit Collect support data schedule (サポート・データ収集スケジュールの作成/編集)
- Rename the storage subsystem (ストレージ・サブシステムの名前変更)
- Comment (コメント)

これらのオプションは、「**Edit (編集)**」および「**Tools (ツール)**」のメニュー・オプション内の他のオプションにも含まれています。詳細については、「*Using the Enterprise Management Window (エンタープライズ管理ウィンドウの使用)*」オンライン・ヘルプ・トピックを参照してください。

テーブル・ビュー

テーブル・ビューでは、各ストレージ・サブシステムはテーブル内の単一行で表されます。テーブル・ビューの列は、管理対象ストレージ・サブシステムに関するデータを表示します。

表 1. テーブル・ビューに表示されるデータ

列	説明
Name (名前)	管理対象ストレージ・サブシステムの名前。 注: 管理対象ストレージ・サブシステムが無名の場合、デフォルト名は Unnamed です。
Type (タイプ)	アイコンによって示される、管理対象ストレージ・サブシステムのタイプ
Status (状況)	管理対象ストレージ・サブシステムの真の状況を報告する、アイコンとテキスト・ラベル
Management Connections (管理接続)	以下の接続タイプを使用できます。 • Out-of-Band (アウト・オブ・バンド): このストレージ・サブシステムはアウト・オブ・バンド・ストレージ・サブシステムです。 • In-Band (インバンド): このストレージ・サブシステムは、単一ホストを介して管理されるインバンド・ストレージ・サブシステムです。 • Out-of-Band, In-Band (アウト・オブ・バンド、インバンド): このストレージ・サブシステムは、アウト・オブ・バンドとインバンドの両方のストレージ・サブシステムです。 これらの接続について詳しい情報を見るには、「 Details (詳細) 」をクリックします。
Comment (コメント)	特定の管理対象ストレージ・サブシステムについてユーザーが入力したコメント

テーブル・ビュー内の行を昇順または降順でソートするには、列見出しをクリックするか、以下のメニュー・オプションのいずれかを選択します。

- 「**View (表示)**」 > 「**By Name (名前別)**」
- 「**View (表示)**」 > 「**By Status (状況別)**」

- 「View (表示)」 > 「By Management Connection (管理接続別)」
- 「View (表示)」 > 「By Comment (コメント別)」

管理対象ストレージ・サブシステムをテーブル・ビューに表示する方法を変更するには、以下のいずれかの処置を実行します。

- 既知のすべての管理対象ストレージ・サブシステムをテーブル・ビューに表示するには、「Management Station (管理ステーション)」ノードを選択します。
- そのストレージ・サブシステムのみをテーブル・ビューに表示するには、ツリー・ビューでそのストレージ・サブシステム・ノードを選択します。

注: ツリー・ビュー内の「Unidentified (未確認)」ノードを選択すると、空のテーブル・ビューが表示されます。

テーブル・ビューの管理対象サブシステムの表示

管理対象ストレージ・サブシステムをテーブル・ビューに表示する方法を変更することができます。

- ストレージ・マネージャー・ノードを選択すると、既知のすべての管理対象ストレージ・サブシステムがテーブル・ビューに表示されます。
- ツリー・ビューで「Discovered Storage Subsystem (検出されたストレージ・サブシステム)」ノードまたは「Undiscovered Storage Subsystem (未確認のストレージ・サブシステム)」ノードを選択すると、その特定のホストに接続されているすべてのストレージ・サブシステムがテーブル・ビューに表示されます。

注: ストレージ・サブシステムを何も追加していない場合は、テーブル・ビューは空です。

- ツリー・ビューでストレージ・サブシステム・ノードを選択すると、そのストレージ・サブシステムのみがテーブル・ビューに表示されます。

注: ツリー・ビュー内の「Unidentified (未確認)」ノードを選択すると、空のテーブル・ビューが表示されます。

ストレージ・サブシステムの追加と除去

ストレージ・サブシステムを追加するには、ストレージ・マネージャーで以下のいずれかを実行します。

表 2. ストレージ・サブシステムの追加

場所	手順
ツリー・ビュー	ツリー・ビューでルート・ノードを右クリックし、ポップアップ・メニューから「Add Storage Subsystem (ストレージ・サブシステムの追加)」を選択する
ツールバー	アイコンをクリックして、ストレージ・サブシステムを追加する
「Edit (編集)」メニュー	「Edit (編集)」 > 「Add Storage Subsystem (ストレージ・サブシステムの追加)」を選択する
「Setup (セットアップ)」タブ	「Add Storage Subsystem (ストレージ・サブシステムの追加)」を選択する

ストレージ・サブシステムを削除するには、ストレージ・マネージャーで以下のいずれかを実行します。サブシステムを除去するとアイコンのみが除去され、サブシステムは削除されません。一度に複数のサブシステムを選択できます。

表 3. ストレージ・サブシステムの除去

場所	手順
ツリー・ビュー	ツリー・ビューから除去するストレージ・サブシステムを右クリックし、ポップアップ・メニューから「 Remove (除去) 」 > 「 Storage Subsystem (ストレージ・サブシステム) 」を選択します。
ツールバー	ツリー・ビューまたはテーブル・ビューから除去するストレージ・サブシステムを選択し、アイコンをクリックして、そのストレージ・サブシステムを除去します。
「Edit (編集)」メニュー	ツリー・ビューまたはテーブル・ビューから除去するストレージ・サブシステムを選択し、「 Edit (編集) 」 > 「 Remove (除去) 」 > 「 Storage subsystem (ストレージ・サブシステム) 」を選択します。

複数のストレージ・サブシステムを同時に除去

多数のストレージ・サブシステムを管理している場合、テーブル・ビューを使用して、複数の連続するまたは不連続のストレージ・サブシステムを同時に除去することができます。

注: ツリー・ビューまたはテーブル・ビューからアイコンのみ除去され、ストレージ・サブシステムは除去されません。

表 4. 複数のサブシステムを同時に除去

場所	手順
ツリー・ビュー	「Discovered Storage Subsystem (検出されたストレージ・サブシステム)」ノードをクリックして、管理しているストレージ・サブシステムを表示します。
テーブル・ビュー	連続するストレージ・サブシステムを除去するには、除去する最初のストレージ・サブシステムをクリックします。シフト・キーを押したまま、除去する最後のストレージ・サブシステムをクリックします。選択したストレージ・サブシステムがテーブル・ビューで強調表示されている状態で、右クリックし、ポップアップ・メニューから「 Remove (除去) 」を選択します。不連続のストレージ・サブシステムを除去するには、Ctrl キーを押したまま、除去するストレージ・サブシステムをクリックします。選択したストレージ・サブシステムがテーブル・ビューで強調表示されている状態で、右クリックし、ポップアップ・メニューから「 Remove (除去) 」を選択します。

「Setup (セットアップ)」タブの使用

「Enterprise Management (エンタープライズ管理)」ウィンドウの「**Setup (セットアップ)**」タブは、ストレージ・サブシステムのセットアップ時に実行できるタスクへのゲートウェイです。「Enterprise Management (エンタープライズ管理)」ウィンドウの「**Setup (セットアップ)**」タブを使用して、以下の作業を実行できます。

- ストレージ・サブシステムを追加する
- ストレージ・サブシステムの命名または名前変更を行う

- アラートを構成する
- ストレージ・サブシステムを管理するために「Subsystem Management (サブシステム管理)」ウィンドウを開く
- コントローラー・ファームウェアをアップグレードする
- 「Inherit Systems Settings (システムの設定の継承)」ウィンドウを開く

「Subsystem Management (サブシステム管理)」ウィンドウ

「Subsystem Management (サブシステム管理)」ウィンドウは、「Enterprise Management (エンタープライズ管理)」ウィンドウから起動される Java テクノロジー・ベースのソフトウェアです。各「Subsystem Management (サブシステム管理)」ウィンドウは、単一のストレージ・サブシステムに対する管理機能を提供します。複数の「Subsystem Management (サブシステム管理)」ウィンドウを開いて、異なるストレージ・サブシステムを管理することも可能です。「Subsystem Management (サブシステム管理)」ウィンドウには、次の機能があります。

- ストレージ・サブシステムの配置、ストレージ・サブシステムの構成、ストレージ・サブシステムの名前変更、またはパスワードの変更など、ストレージ・サブシステムのオプションにアクセスする
- ストレージ・サブシステムの容量からディスク・プールまたはアレイと、標準論理ドライブまたはシン論理ドライブを構成し、ホストおよびホスト・グループを定義し、ホストまたはホスト・グループに対して、ストレージ区画と呼ばれる標準論理ドライブまたはシン論理ドライブのセットへのアクセス権限を付与する
- ストレージ・サブシステム・コンポーネントの正常性をモニターし、該当するアイコンを使用して詳細状況を報告する
- 障害が起きた論理コンポーネントまたは障害が起きたハードウェア・コンポーネントに適用できるリカバリー手順にアクセスする
- ストレージ・サブシステムのイベント・ログを表示する
- コントローラーやドライブなどのハードウェア・コンポーネントに関するプロファイル情報を表示し、ハードウェア・エンクロージャー内のドライブの物理ビューを取得する
- 論理ドライブの所有権を変更したり、コントローラーをオンラインまたはオフラインにするなど、コントローラー管理オプションにアクセスする
- ホット・スペアの割り当ておよびドライブの配置など、ドライブ管理オプションにアクセスする
- ストレージ・サブシステムのパフォーマンスをモニターする
- Enhanced Flashcopy、Flashcopy、VolumeCopy、およびリモート・ミラーリングのようなコピー・サービスを構成する

ストレージ・サブシステムがコントローラー・ファームウェア・バージョン 7.70.xx.xx を使用している場合、強力なパスワードを指定しない限り、「Subsystem Management (サブシステム管理)」ウィンドウを開くことができません。強力なパスワードは、8 文字から 30 文字でなければならず、少なくとも 1 文字の数字、1 文字の小文字、1 文字の大文字、および 1 文字の非英数字 (例えば、< > ! @ + #) が含まれている必要があります。スペースは使用できません。また、大/小文字の区別があります。

7.70.xx.xx 以外のコントローラー・ファームウェアを搭載したストレージ・サブシステムでは、そのストレージ・サブシステム用のパスワードが指定されていない場合、このストレージ・サブシステムの

「Subsystem Management (サブシステム管理)」ウィンドウを開こうとするたびに、このパスワードの指定を求めるプロンプトが出されます。IBM は、サブシステム管理構成に対する無許可の変更を防止するために、サブシステム管理パスワードを作成することをお勧めします。

「Subsystem Management (サブシステム管理)」ウィンドウのオープン

「Enterprise Management (エンタープライズ管理)」ウィンドウから「Subsystem Management (サブシステム管理)」ウィンドウを開くには、以下のいずれかの処置を実行します。

- 「Devices (デバイス)」タブをクリックし、管理するストレージ・サブシステムの名前をダブルクリックする。
- 「Devices (デバイス)」タブをクリックし、管理するストレージ・サブシステムの名前を右クリックして、「Manage Storage Subsystem (ストレージ・サブシステムの管理)」を選択する。
- 「Devices (デバイス)」タブをクリックし、「Tools (ツール)」 > 「Manage Storage Subsystem (ストレージ・サブシステムの管理)」を選択する。
- 「Setup (セットアップ)」タブをクリックし、「Manage Storage Subsystem (ストレージ・サブシステムの管理)」を選択する。「Select Storage Subsystem (ストレージ・サブシステムの選択)」ウィンドウで、管理するストレージ・サブシステムの名前を選択して、「OK」をクリックします。

「Subsystem Management (サブシステム管理)」ウィンドウでは、1 つのストレージ・サブシステムのみを管理できます。ただし、「Enterprise Management (エンタープライズ管理)」ウィンドウから複数の「Subsystem Management (サブシステム管理)」ウィンドウを開いて、同時に複数のストレージ・サブシステムを管理することも可能です。

「Subsystem Management (サブシステム管理)」ウィンドウは、ストレージ・サブシステムを管理するための以下のオプションを備えています。

IBM System Storage DS ストレージ・マネージャー バージョン 10.83 以降では、コントローラー・ファームウェア・バージョン 7.83.xx.xx 以降とともに、「Subsystem Management (サブシステム管理)」ウィンドウの画面レイアウトおよびメニュー・オプションが変更されています。以前のバージョンに実装されていたすべてのサブシステム管理機能が引き続き有効です。ただし、メニュー・オプションは異なる場合があります。ソフトウェアを調べて、オンライン・ヘルプを参照し、確認してください。

「Summary (要約)」タブの使用

「Subsystem Management (サブシステム管理)」ウィンドウの「Summary (要約)」タブは、ストレージ・サブシステムに関する情報を表示します。「Summary (要約)」タブには、「Storage Subsystem Profile (ストレージ・サブシステム・プロファイル)」ウィンドウ、関連のオンライン・ヘルプ・トピック、およびストレージ概念チュートリアルへのリンクも表示されます。さらに、ストレージ・サブシステムに注意する必要がある場合、Recovery Guru ウィンドウへのリンクも表示されます。

「Summary (要約)」タブでは、以下の情報を表示できます。

- ストレージ・サブシステムの状況
- IBM DS ストレージ・マネージャー・ソフトウェアおよびコントローラー・ファームウェアのバージョン情報
- ストレージ・サブシステムの容量
- ストレージ・サブシステム内のディスク・プールおよびアレイ、論理ドライブ、およびコピー・サービスの構成 (FlashCopy、VolumeCopy、および拡張リモート・ミラーリングなど)
- ストレージ・サブシステム内のホスト、マッピング、およびストレージ区画
- ストレージ・サブシステムに対して選択可能、アクティブ、使用可能、または使用不可のプレミアム・フィーチャーの数
- ストレージ・サブシステム内のハードウェア・コンポーネント
- ストレージ・サブシステムについての学習に使用できるオンライン資料

「Storage and Copy Services (ストレージおよびコピー・サービス)」タブの使用

「Storage & Copy Services (ストレージおよびコピー・サービス)」タブは、論理ノードのツリー構造ビューを提供します。ノードに隣接するプラス (+) 符号またはマイナス (-) 符号をクリックして、ビューを拡張または縮小します。ノードをダブルクリックして、そのノードに適用できるアクションが含まれているメニューを開きます。

「Logical (論理)」タブのノード

ストレージ・サブシステム (つまり、ルート・ノード) には、次の表に示されているタイプの下位ノードがあります。

表 5. 「Logical (論理)」タブのノード

ルート・ノードの下位ノード	下位ノードの説明
All Logical Objects (すべての論理オブジェクト)	このノードでは、ストレージ・サブシステムを構成するすべての論理オブジェクトに関する情報を表示できます。「View (表示)」ペインの「Object Type (オブジェクト・タイプ)」ドロップダウン・メニューを使用して、特定のオブジェクト・タイプを選択します。これは、ディスク・プールまたはアレイの状況および容量情報の表示、あるいは Flashcopy イメージ、Enhanced Flashcopy イメージ、および整合性グループの各プレミアム・フィーチャーで使用された基本論理ドライブに関連付けられた、または関連付けられていないすべてのリポジトリ論理ドライブの表示を行うために便利な方法です。
Total Unconfigured Capacity (未構成容量の合計)	このノードは、ディスク・プール内またはアレイ内にないすべての未割り当てドライブの容量の合計を表します。
Unconfigured Capacity (未構成容量)	このノードは、アレイに構成されていないストレージ・サブシステム容量を表します。ストレージ・サブシステムに、異なるメディア・タイプを持つドライブ (ハード・ディスクまたはソリッド・ステート・ドライブ) および異なるインターフェース・タイプが含まれている場合、複数の「Unconfigured (未構成)」ノードが表示されます。ドライブ・エンクロージャー内に使用可能な未割り当てドライブがある場合、ドライブ・タイプごとに関連の「Unconfigured Capacity (未構成容量)」ノードが「Total Unconfigured Capacity (合計未構成容量)」ノードのもとに表示されます。

表 5. 「Logical (論理)」 タブのノード (続き)

ルート・ノードの下位ノード	下位ノードの説明
Disk Pools (ディスク・プール)	ストレージ・サブシステムに 1 つ以上のディスク・プールが構成されている場合、IBM ストレージ・マネージャーは「Disk Pools (ディスク・プール)」ノードを表示します。「Disk Pool (ディスク・プール)」ノードを展開すると、個々のディスク・プールが表示されます。Flashcopy プレミアム・フィーチャーが使用可能になっている場合、Flashcopy イメージ下位ノードを持つことができます。ディスク・プール・ノードには、以下のようないくつかのタイプの下位ノードがあります。 • Logical Drive (論理ドライブ) — このノードは、構成および定義済みの論理ドライブ (標準論理ドライブまたはシン論理ドライブのいずれか) を表します。「Disk Pools (ディスク・プール)」ノードのもとには、複数の「Logical drive (論理ドライブ)」ノードが存在することがあります。 • Free Capacity (空き容量) — このノードは、ディスク・プール内に 1 つ以上の論理ドライブを作成するために使用できる領域の容量を表します。各「Disk Pool (ディスク・プール)」ノードのもとに、「Free Capacity (空き容量)」ノードが存在することがあります。 • Enhanced Flashcopy Images (Enhanced Flashcopy イメージ) — このノードは、選択された基本論理ドライブの特定時点の論理イメージを表します。基本論理ドライブは、Enhanced Flashcopy イメージのソースである標準論理ドライブまたはシン論理ドライブです。 • Enhanced Flashcopy Groups (Enhanced FlashCopy グループ) — このノードは、同じ基本論理ドライブの Enhanced FlashCopy イメージのシーケンスを表します。 • Enhanced Flashcopy logical drives (Enhanced FlashCopy 論理ドライブ) — このノードは、Enhanced FlashCopy イメージのビューが作成されていることを示します。Enhanced FlashCopy 論理ドライブは、ホストが Enhanced FlashCopy イメージに、それが論理ドライブであるかのようにしてアクセスできるようにするために作成します。 • Primary and Secondary logical drives (1 次および 2 次論理ドライブ) — このノードは、拡張リモート・ミラーリングの論理ドライブ・ペア内の論理ドライブが 1 次であるか 2 次であるかを示します。

表 5. 「Logical (論理)」 タブのノード (続き)

ルート・ノードの下位ノード	下位ノードの説明
Arrays (アレイ)	「Logical drive (論理ドライブ)」ノードおよび「Free Capacity (空き容量)」ノードは、標準下位ノードです。「Enhanced Flashcopy Image (Enhanced Flashcopy イメージ)」プレミアム・フィーチャーが使用可能になっている場合、Enhanced FlashCopy イメージ下位ノードを持つことができます。 • Logical Drive (論理ドライブ) — このノードは、構成および定義済みの論理ドライブを表します。アレイは、標準論理ドライブのみをサポートします。「Array (アレイ)」ノードのもとには、複数の論理ドライブ・ノードが存在することがあります。 • Free Capacity (空き容量) — このノードは、アレイ内に 1 つ以上の論理ドライブを作成するために使用できる領域の容量を表します。アレイ・ノードのもとには、複数の「Free Capacity (空き容量)」ノードが存在することがあります。 • Enhanced Flashcopy Images (Enhanced Flashcopy イメージ) — このノードは、選択された基本論理ドライブの特定時点の論理イメージを表します。基本論理ドライブは、Enhanced Flashcopy イメージのソースである標準論理ドライブまたはシン論理ドライブです。 • Enhanced Flashcopy Groups (Enhanced FlashCopy グループ) — このノードは、同じ基本論理ドライブの Enhanced FlashCopy イメージのシーケンスを表します。 • Enhanced Flashcopy Logical Drives (Enhanced FlashCopy 論理ドライブ) — このノードは、ホストに表示される基本論理ドライブの Enhanced FlashCopy イメージを表します。 • Primary and Secondary logical drives (1 次および 2 次論理ドライブ) — このノードは、拡張リモート・ミラーリングの論理ドライブ・ペア内の論理ドライブが 1 次であるか 2 次であるかを示します。 • Flashcopy Logical Drive (FlashCopy 論理ドライブ) — 関連付けられている基本論理ドライブの下位ノードです。
Consistency Groups (整合性グループ)	Enhanced Flashcopy プレミアム・フィーチャーが使用可能になっている場合、以下の整合性グループ下位ノードを持つことができます。 • Consistency Group (整合性グループ) — このノードは、この整合性グループ用に作成されたすべての下位ノードを含むグループ化ノードを表します。このノードを展開すると、下位ノードが表示されます。 • Enhanced Flashcopy Images (Enhanced FlashCopy イメージ) — このノードは、整合性グループのメンバー論理ドライブの特定時点の論理イメージの集合を表します。 • Member logical drives (メンバー論理ドライブ) — このノードは、この整合性グループのメンバーである論理ドライブの集合です。 • Enhanced Flashcopy logical drives (Enhanced FlashCopy 論理ドライブ) — このノードは、ホストに表示されるメンバー論理ドライブの Enhanced FlashCopy イメージを表します。

表 5. 「Logical (論理)」 タブのノード (続き)

ルート・ノードの下位ノード	下位ノードの説明
Enhanced Global Mirror Groups (拡張グローバル・ミラー・グループ)	これらは、ローカル・ストレージ・サブシステムとリモート・ストレージ・サブシステムの両方の各コントローラーのリソースとして作成される、ストレージ・サブシステム内の特殊論理ドライブです。コントローラーは、重複する情報をミラー・リポジトリ論理ドライブに保管します。これには、まだ 2 次論理ドライブに書き込まれていないリモート書き込みに関する情報が含まれます。

「Host Mappings (ホスト・マッピング)」タブの使用

「Subsystem Management (サブシステム管理)」ウィンドウの「Mappings (マッピング)」タブには、2 つのペイン (「Host Mappings (ホスト・マッピング)」ペインと「Defined Mappings (定義済みマッピング)」ペイン)が含まれています。

「Host Mappings (ホスト・マッピング)」ペイン

「Host Mappings (ホスト・マッピング)」ペインは、ストレージ区画に関連した論理ノードのツリー構造ビューを表示します。ノードに隣接するプラス (+) 符号またはマイナス (-) 符号をクリックして、ビューを拡張または縮小します。ノードを右クリックすると、そのノードに適用できるアクションが含まれたポップアップ・メニューが開きます。

ストレージ・サブシステム (つまり、ルート・ノード) には、以下のタイプの下位ノードがあります。

表 6. 「Topology (トポロジー)」ペイン内のノードのタイプ

ルート・ノードの下位ノード	下位ノードの説明
Undefined Mappings (未定義マッピング)	「Undefined Mappings (未定義マッピング)」ノードには、1 つのタイプの下位ノードがあります。 • Individual Undefined Mapping (個別未定義マッピング): 未定義マッピングをもつ論理ドライブを表します。「Undefined Mappings (未定義マッピング)」ノードのもとには、複数の「Logical Drive (論理ドライブ)」ノードが存在することがあります。
Default Group (デフォルト・グループ)	注: Storage Manager ストレージの区画化プレミアム・フィーチャーが使用不可の場合、作成された論理ドライブはすべて「Default Group (デフォルト・グループ)」に入れられます。 「Default Group (デフォルト・グループ)」ノードには、2 つのタイプの下位ノードがあります。 • Host Group (ホスト・グループ): 特定のマッピングに関与していない定義済みホスト・グループがリストされます。このノードは「ホスト」下位ノードを持つことができ、「ホスト」下位ノードは「ホスト・ポート」下位ノードを持つことができます。 • Host (ホスト): 特定のホスト・グループの一部ではなく、「Default Group (デフォルト・グループ)」の一部であり、かつ特定のマッピングに関与していない、定義済みホストがリストされます。このノードは、「ホスト・ポート」下位ノードを持つことができます。

表 6. 「Topology (トポロジー)」 ペイン内のノードのタイプ (続き)

ルート・ノードの下位ノード	下位ノードの説明
Unassociated Host Port Identifier (非関連ホスト・ポート ID)	「Unassociated Host Port Identifier (非関連ホスト・ポート ID)」 ノードには、1 つのタイプの下位ノードがあります。 • Host Port Identifier (ホスト・ポート ID) – どのホストにも関連付けられていないホスト・ポート ID。
Host Group (ホスト・グループ)	「Host Group (ホスト・グループ)」 ノードには、1 つのタイプの下位ノードがあります。 • Host (ホスト) - この定義済みホスト・グループに属する定義済みホストがリストされます。このノードは、「ホスト・ポート」下位ノードを持つことができます。 注: このホスト・グループの下位ノードであるホスト・ノードは、ホスト・グループではなく個別ホストに固有のマッピングに関与することもできます。
Host (ホスト)	「Host (ホスト)」 ノードには、1 つのタイプの下位ノードがあります。 • Host Ports (ホスト・ポート): このノードには、このホストに関連付けられたホスト・アダプター上のすべてのホスト・ポートまたは単一ポートを表す下位ノードがあります。

「ストレージ区画」アイコンが「Host Mappings (ホスト・マッピング)」ペインに表示されている場合、ホスト・グループまたはホスト用のストレージ区画が定義されていることを示します。この機能が使用可能になっている場合、このアイコンはステータス・バーにも表示されます。

「Defined Mappings (定義済みマッピング)」 ペイン

「Defined Mappings (定義済みマッピング)」ペインは、「Topology (トポロジー)」ペインで選択されたノードに関連付けられているマッピングを表示します。

表 7. 「Defined Mappings (定義済みマッピング)」ペインのノード情報

列名	説明
Logical Drive name (論理ドライブ名)	ユーザー提供の論理ドライブ名。 工場で構成されたアクセス論理ドライブもこの列に表示されます。 注: アクセス論理ドライブ・マッピングは、IBM ストレージ・マネージャーがストレージ・サブシステムと通信できるようにするために、インバンド接続を使用するストレージ・サブシステムの場合に必要です。アウト・オブ・バンド接続を使用するストレージ・サブシステムの場合は、アクセス論理ドライブ・マッピングを削除できます。
Accessible by (アクセス可能)	マッピング内の論理ドライブへのアクセス権限が付与されている「Default Group (デフォルト・グループ)」、定義済みホスト・グループ、または定義済みホスト。
LUN	1 つ以上のホストが論理ドライブにアクセスするために使用する、特定の論理ドライブに割り当てられた LUN。
Logical Drive Capacity (論理ドライブ容量)	GB 単位の論理ドライブの容量。
Type (タイプ)	標準論理ドライブ、FlashCopy 論理ドライブなど、論理ドライブのタイプ。

「Defined Mappings (定義済みマッピング)」ペインの論理ドライブ名を右クリックして、メニューを開くことができます。メニューには、マッピングを変更および除去するためのオプションが含まれています。

「Hardware (ハードウェア)」タブの使用

「Hardware (ハードウェア)」タブには、2 つのペインが含まれています。左側が「Hardware placement (ハードウェアの配置)」または「Hardware layout (ハードウェア・レイアウト)」ペインで、右側が「Properties (プロパティ)」ペインです。「Hardware placement (ハードウェアの配置)」ペインでは、ストレージ・サブシステムのハードウェア・コンポーネント (その状況を含む) のビューが提供されます。

「Hardware placement (ハードウェアの配置)」ペインでは、「Hardware (ハードウェア)」ペインで選択されたハードウェア・コンポーネントの情報が提供されます。「Properties (プロパティ)」ペインの情報は、各ハードウェア・コンポーネントに固有です。「Hardware (ハードウェア)」ペインでコントローラー・アイコンを選択すると、そのコントローラー用のプロパティのリストが「Properties (プロパティ)」ペインに表示されます。「Hardware (ハードウェア)」ペインでドライブ・アイコンを選択すると、そのドライブ用のプロパティのリストが「Properties (プロパティ)」ペインに表示されます。

View (表示)

各エンクロージャーに対して **View Enclosure Components** コマンドを使用すると、そのエンクロージャー内の 2 次コンポーネント (電源機構、ファン、および温度センサーなど) の状況が表示されます。「**Drive type (ドライブ・タイプ)**」から選択し、「Hardware placement (ハードウェアの配置)」ペインの「**Show (表示)**」をクリックして、ドライブの特定タイプ、速度、および容量を識別できます。関連のドライブの先頭に緑色の三角形が表示されます。

「Setup (セットアップ)」タブの使用

「Subsystem Management (サブシステム管理)」ウィンドウの「**Setup (セットアップ)**」タブには、以下のタスクへのリンクがあります。

- Locate Storage subsystem (ストレージ・サブシステムの検索)
- Rename Storage subsystem (ストレージ・サブシステムのリネーム)
- Change Hardware View Order (ハードウェア・ビュー・オーダーの変更)
- Set a Storage subsystem password (ストレージ・サブシステム・パスワードの設定)
- Manage Premium features (プレミアム・フィーチャーの管理)
- Create Storage (ストレージの作成)
- Save Configuration (構成の保存)

オプション・タスク:

- Manually Define Host (ホストの手動定義)
- Map Logical Drives (論理ドライブのマッピング)
- Configure Ethernet Management Ports (イーサネット・マネジメント・ポートの構成)

リンクをクリックすると、対応するウィンドウが開きます。

複数のソフトウェア・バージョンの管理

ストレージ・サブシステムを管理するために「Subsystem Management (サブシステム管理)」ウィンドウを開くと、ファームウェアのバージョンに適用可能なバージョンのストレージ・マネージャー・ソフトウェアが開きます。例えば、ストレージ・マネージャー・ソフトウェアを使用する 2 つのストレージ・サブシ

テム (一方のストレージ・サブシステムはファームウェア・バージョン 6.14 を使用し、他方はファームウェア・バージョン 7.5x を使用) を管理することができます。いずれか 1 つのストレージ・サブシステムの「Subsystem Management (サブシステム管理)」ウィンドウを開くと、正しいバージョンの「Subsystem Management (サブシステム管理)」ウィンドウが使用されます。ファームウェア・バージョン 6.14 を持つストレージ・サブシステムはバージョン 9.14 のストレージ・マネージャー・ソフトウェアを使用し、ファームウェア・バージョン 7.5x を持つストレージ・サブシステムはバージョン 10.5x のストレージ・マネージャー・ソフトウェアを使用します。「Subsystem Management (サブシステム管理)」ウィンドウの「**Help (ヘルプ)**」 > 「**About (バージョン情報)**」をクリックすると、現在使用されているバージョンを確認することができます。

注: 複数のサブシステムを管理しており、これらのサブシステムが異なるバージョンのコントローラー・ファームウェアを使用している場合、サブシステム管理ウィンドウは、コントローラー・ファームウェア・バージョンによってロック・アンド・フィールドが異なることがあります。

第 3 章 ストレージ・マネージャーのインストール

この章では、ストレージ・マネージャー・ソフトウェアをインストールするための要件および手順について説明します。

ストレージ・マネージャーを UNIX タイプのオペレーティング・システムにインストールする場合、インストール・ウィザードを使用するために、システムがグラフィックス機能を備えている必要があります。システムにグラフィックス機能がない場合は、シェル・コマンドを使用すれば、グラフィックスなしでストレージ・マネージャーをインストールできます。詳しくは、33 ページの『Linux、AIX、HP-UX、および Solaris でのコンソール・ウィンドウを使用したストレージ・マネージャーのインストール』を参照してください。このセクションをスキップして、スタンドアロンのホスト・ソフトウェア・パッケージをインストールすることもできます。35 ページの『ストレージ・マネージャーの手動インストール』を参照し、示されている手順に従ってください。すべてのパッケージがインストール DVD に組み込まれています。ストレージ・マネージャーでサポートされる管理ステーションのオペレーティング・システムは次のとおりです。

- AIX
- Windows 7、Windows Vista、Windows XP (Service Pack 2)、Windows Server 2003、Windows Server 2008、および Windows Server 2012
- Linux: RHEL および SLES (x86、x86_64、および Linux on POWER)
- HP-UX (PA-RISC および IA64 版)
- Oracle Solaris (SPARC および x86 版)

注: IA64 バージョンのストレージ・マネージャーは、IA64 エディションの Microsoft Windows および Linux オペレーティング・システムでは使用できません。バージョンが 6.50.xx.xx より前のコントローラー・ファームウェアを使用したサブシステムを管理する場合、別の管理ワークステーションにインストールされている、前のバージョンのストレージ・マネージャー・ソフトウェアを使用する必要があります。

インストールの説明は、以下のセクションで構成されています。

- 30 ページの『プリインストール要件』
- 30 ページの『インストール・ウィザードを使用するストレージ・マネージャー・パッケージの自動インストール』
- 34 ページの『ストレージ・マネージャー・パッケージの手動インストール』
- 36 ページの『ストレージ・マネージャーのインストールの完了』

ストレージ・マネージャーをアンインストールするには、36 ページの『ストレージ・マネージャーのアンインストール』を参照してください。

重要: クラスタ構成では、2 番目のホストまたはクラスタ・サーバーでストレージ・マネージャー・ソフトウェアをインストールする前に、ストレージ・サブシステムごとにすべての該当する構成手順を完了してください。

プリインストール要件

注: ストレージ・マネージャー・バージョン 10.84.xx.xx 以降を使用する場合は、最小コントローラー・ファームウェア・バージョンは 6.50.xx.xx 以降でなければなりません。 6.50.xx.xx より前のコントローラー・ファームウェア・バージョンは、サポートも管理もされなくなりました。

また管理ステーションは、次のハードウェア、ソフトウェア、および構成の要件を満たす必要があります。

- 2 GHz 以上のマイクロプロセッサ速度
- 最小 2 GB のシステム・メモリー。他のアプリケーションが管理ステーションにインストールされている場合、追加のメモリーが必要な場合があります。
- ツールおよび保存されているサポート・バンドル用に最小 1.5 GB のフリー・ディスク・スペース。
- TCP/IP スタックが使用可能でなければなりません。

インストール・ウィザードを使用するストレージ・マネージャー・パッケージの自動インストール

ストレージ・マネージャー・インストール・ウィザードを使用して、ストレージ・マネージャー・ソフトウェアを自動的にインストールするか、それぞれのパッケージを手動でインストールすることができます。このセクションでは、ストレージ・マネージャー・インストール・ウィザードのインストール・プロセスについて説明します。

ストレージ・マネージャー・ソフトウェアをインストールする前に、『Windows でのストレージ・マネージャーのインストール』または 32 ページの『Linux、AIX、HP-UX または Solaris でのストレージ・マネージャーのインストール』のいずれかのセクションをお読みください。

Windows でのストレージ・マネージャーのインストール

ご使用の管理ステーションで Windows オペレーティング・システムを使用している場合は、以下の手順を実行し、インストール・ウィザードを使用してストレージ・マネージャーをインストールします。

1. ストレージ・マネージャー DVD または System Storage Disk Support Web サイトから、ファイルをご使用のシステムのディレクトリーにダウンロードします。Windows のデフォルト・ドライブは C です。
2. 「**IBM DS Storage Manager package (IBM DS ストレージ・マネージャー・パッケージ)**」(または SMIA) 実行可能プログラム・アイコンをダブルクリックします。
3. インストール・ウィザードの指示に従って、ストレージ・マネージャー・ソフトウェアをインストールします。デフォルト・ディレクトリーは、

C:\Program Files\IBM_DS

または

C:\Program Files(x86)\IBM_DS

4. インストール・タイプを選択するときは、以下のオプションから 1 つを選択することができます。

重要: SMIA パッケージが Microsoft Windows オペレーティング・システムのサーバー・バージョンにインストールされている場合、ストレージ・マネージャー SMIA パッケージ・バージョン 10.77.xx.xx 以降は、ホスト・インストール・タイプでの、または典型的インストール・タイプでのマルチパスをサポートするための MPIO DSM ドライバーをインストールしません。MPIO DSM をインストールするための別個の SMIA パッケージがあります。ストレージ・マネージャー・インストーラーと MPIO DSM インストーラーは、1 つのコード・パッケージにバンドルされています。このコード・パッケージは、IBM サポート・ポータルで入手できます。

- **標準 (フル) インストール:** ホストからストレージ・サブシステムを管理し、ストレージ・サブシステムへの入出力接続を提供するのに必要なストレージ・マネージャー・ソフトウェア・パッケージをインストールします。
 - **管理ステーション:** ストレージ・サブシステムの管理およびモニターに必要なパッケージ (SMclient) をインストールします。
 - **ホスト:** ストレージ・サブシステムへの入出力接続を提供するのに必要なパッケージ (SMagent および SMutil) をインストールします。
 - **カスタム:** インストールしたいパッケージを選択することができます。
5. IBM DS Storage Manager MPIO DSM パッケージをダブルクリックし、インストール・ウィザードの手順に従って、マルチパスをサポートするのに必要な MPIO DSM ドライブをインストールします。

注: このステップは、ストレージ・マネージャー・バージョン 10.77.xx.xx 以降にのみ適用されます。

6. 「スタート」 > 「すべてのプログラム」 > 「DS Storage Manager 10 client (DS ストレージ・マネージャー 10 クライアント)」 > 「Storage Manager 10 client (ストレージ・マネージャー 10 クライアント)」をクリックして、ストレージ・マネージャー・クライアント・プログラムを開始します。ストレージ・マネージャー・クライアント・プログラムの「Enterprise Management (エンタープライズ管理)」ウィンドウで、管理とモニターを行う対象のストレージ・サブシステムを追加します。
7. サブシステムを右クリックして、「Collect Support Data (サポート・データの収集)」 > 「Create/Edit Schedule (スケジュールの作成/編集)」を選択します。「Schedule Support Data Collection (サポート・データ収集のスケジュール)」ウィンドウが開きます。
8. ここで、スケジュール/時間を設定し、追加したストレージ・サブシステム用の自動サポート・データ収集時にサポート・データを保管する場所を指定します。

注: 自動サポート・データ収集の日 (1 から 31) または曜日 (月曜日から日曜日) のいずれかをスケジュールできます。1 つのサブシステムには、1 つだけスケジュールを設定できます。同一のスケジュールを設定する複数のサブシステムを選択できます。サポート・データ・レポートは、ローカル・ドライブの指定された場所に保存されます。レポート名には、そのレポートが生成された日付が含まれます。このシステムでは、最大 5 つのサポート・データ・レポートが許可されます。既に 5 つのレポートが存在するときに新たなレポートが生成された場合、最も古いレポートが削除され、新しいレポートが保存されます。

9. 「Collect Support Data (サポート・データの収集)」 > 「Automatically (自動)」を選択します。「Automatic Support Data Collection (自動サポート・データ収集)」ウィンドウが開きます。

注: 自動サポート・データ収集のためには、ストレージ・マネージャーのモニター・サービスが使用可能になっている必要があります。

10. 重大イベントが発生した場合の自動報告するサブシステムを選択し、レポートを保存するローカル・ドライブ上の場所を指定します。

インストールの際に、「Automatically Start Monitor? (モニターを自動的に開始しますか?)」という質問が表示されます。これは、Microsoft Windows イベント・モニター・サービスを指しています。ESM の自

動同期と重大なイベントのサポート・バンドル自動収集の両方を行うには、イベント・モニターを使用可能にする必要があります。イベント・モニターを使用可能にするには、「**Automatically Start Monitor (モニターを自動的に開始する)**」を選択します。

ストレージ・マネージャーのインストールを完了するには、36 ページの『ストレージ・マネージャーのインストールの完了』を参照してください。

Linux、AIX、HP-UX または Solaris でのストレージ・マネージャーのインストール

ご使用の管理ステーションで UNIX ベースのオペレーティング・システム (Linux、AIX、HP-UX、または Solaris など) を使用している場合は、以下の手順を実行し、インストール・ウィザードを使用してストレージ・マネージャーをインストールします。

1. ストレージ・マネージャー DVD または System Storage Disk Support Web サイトから、ファイルをご使用のシステムのルート・ファイル・システムにダウンロードします。
2. root としてログインします。
3. ストレージ・マネージャー・ソフトウェア・パッケージの .bin ファイルに実行可能な許可がない場合、`chmod +x` コマンドを使用して実行可能にします。
4. .bin ファイルを実行し、インストール・ウィザードの指示に従ってソフトウェアをインストールします。デフォルト・ディレクトリーは、
`/opt/IBM_DS`

インストール・タイプを選択するときは、以下のオプションから 1 つを選択することができます。

- **標準 (フル) インストール:** 当該ホストからストレージ・サブシステムを管理し、ストレージへの入出力接続を提供するのに必要なストレージ・マネージャー・ソフトウェア・パッケージをすべてインストールします。
 - **管理ステーション:** ストレージ・サブシステムの管理およびモニターに必要なパッケージ (SMruntime および SMclient) をインストールします。
 - **ホスト:** ストレージ・サブシステムへの入出力接続を提供するのに必要なパッケージ (SMruntime、SMagent、および SMutil) をインストールします。
 - **カスタム:** インストールしたいパッケージを選択することができます。
5. コンソール・ウィンドウに SMclient と入力し、Enter キーを押してストレージ・マネージャー・クライアント・プログラムを開始します。ストレージ・マネージャー・クライアント・プログラムの「Enterprise Management (エンタープライズ管理)」ウィンドウに、管理とモニターを行う対象のストレージ・サブシステムを追加します。
 6. サブシステムを右クリックして、「**Collect Support Data (サポート・データの収集)**」 > 「**Create/Edit Schedule (スケジュールの作成/編集)**」を選択します。「**Schedule Support Data Collection (サポート・データ収集のスケジュール)**」ウィンドウが開きます。
 7. ここで、スケジュール/時間を設定し、追加したストレージ・サブシステム用の自動サポート・データ収集時にサポート・データを保管する場所を指定します。

注: 自動サポート・データ収集の日 (1 から 31) または曜日 (月曜日から日曜日) のいずれかをスケジュールできます。1 つのサブシステムには、1 つだけスケジュールを設定できます。同一のスケジュールを設定する複数のサブシステムを選択できます。サポート・データ・レポートは、ローカル・ドライブの指定された場所に保存されます。レポート名には、そのレポートが生成された日付が含まれます。このシステムでは、最大 5 つのサポート・データ・レポートが許可されます。既に 5 つのレポートが存在するときに新たなレポートが生成された場合、最も古いレポートが削除され、新しいレポートが保存されます。

8. サブシステムを右クリックします。「**Collect Support Data (サポート・データの収集)**」
>「**Automatically (自動)**」を選択します。「**Automatic Support Data Collection (自動サポート・データ収集)**」ウィンドウが開きます。

注: 自動サポート・データ収集のためには、ストレージ・マネージャーのモニター・サービスが使用可能になっている必要があります。

9. 重大イベントが発生した場合の自動報告するサブシステムを選択し、レポートを保存するローカル・ドライブ上の場所を指定します。
10. ストレージ・サブシステムからマップ済み論理ドライブへのパスを管理するために、マルチパス・ドライバを構成するか、あるいはインストールして構成します。

インストールの際に、「**Automatically Start Monitor? (モニターを自動的に開始しますか?)**」という質問が表示されます。これは、イベント・モニター・サービスを指しています。ESM の自動同期と重大なイベントのサポート・バンドル自動収集の両方を行うには、イベント・モニターを使用可能にする必要があります。イベント・モニターを使用可能にするには、「**Automatically Start Monitor (モニターを自動的に開始する)**」を選択します。

ストレージ・マネージャーのインストールを完了するには、36 ページの『ストレージ・マネージャーのインストールの完了』を参照してください。

Linux、AIX、HP-UX、および Solaris でのコンソール・ウィンドウを使用したストレージ・マネージャーのインストール

グラフィックス・アダプターを備えていない管理ステーションの場合、`-i silent` または `-i console` オプションを使用してストレージ・マネージャー・ソフトウェア・パッケージを自動的にインストールできます。このインストール方式は、Windows オペレーティング・システム環境でも使用できます。

`-i silent` オプションを使用すると、デフォルトのインストーラー設定を使用してストレージ・マネージャーのソフトウェア・インストーラー・パッケージがインストールされます。`-i console` オプションを使用すると、インストール・ウィザードと同じように、ソフトウェアのインストールを開始する前に、インストールされるオプションを指定するよう求めるプロンプトがユーザーに出されます。ただし、これらのプロンプトは、グラフィカル・ウィンドウではなく、コンソール・ウィンドウのテキストで表示されます。

次の例では、`-i silent` および `-i console` オプションを指定したストレージ・マネージャー・コンソール・ウィンドウ・インストールの一部を示しています。

```
[usr@RHManStation ~]# ./SMIA-LINUX-10.60.A5.17.bin -i console
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system environment...

Launching installer...

Preparing CONSOLE Mode Installation...

=====
Choose Locale...
-----

1- Deutsch
->2- English
3- Español
4- Français
```



```

5- Italiano
6- Português (Brasil)

CHOOSE LOCALE BY NUMBER:
2
... ..

...
[usr@RHManaStation ~]# ./SMIA-LINUX-10.60.A5.17.bin -i silent
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system environment...

Launching installer...

Preparing SILENT Mode Installation...

=====
IBM System Storage DS Storage Manager 10(created with InstallAnywhere by Macrovision)
=====

Installing...

[=====|=====|=====|=====]
[-----|-----|-----|-----]
... ..

```

ストレージ・マネージャー・パッケージの手動インストール

UNIX タイプのオペレーティング・システム (AIX、Linux、Sun Solaris、HP-UX など) の場合、個別のストレージ・マネージャー・ソフトウェア・パッケージが提供されています。個別のソフトウェア・パッケージのインストール・シーケンスについては、35 ページの表 8 を参照してください。

ストレージ・マネージャー・ソフトウェアを管理ステーションに手動でインストールする場合は、このセクションの手順を使用します。必ず、パッケージを正しい順序でインストールするようにしてください。

重要:

1. Windows オペレーティング・システム用の手動インストール・オプションはありません。Windows でストレージ・マネージャーのインストールの場合はすべて、個々のソフトウェア・パッケージは単一のストレージ・マネージャー・ソフトウェア・インストーラーに組み込まれています。

ソフトウェア・インストール・シーケンス

ストレージ・マネージャーのソフトウェア・パッケージを、35 ページの表 8 に示されている順序でインストールします。

注: これらのパッケージは、グラフィカル・ユーザー・インターフェースなしの UNIX サーバーで使用できます。

表 8. ストレージ・マネージャーのソフトウェア・パッケージのインストール・シーケンス

ステップ	パッケージ
1	SMruntime
2	SMesm
3	SMclient ¹
4	SMagent
5	SMutil

¹SMclient は SMclient の Java コンパイラーである SMruntime に依存しています。そこで、まず SMruntime をインストールする必要があります。

ストレージ・マネージャーの手動インストール

ストレージ・マネージャー・ソフトウェアをインストールする前に、ストレージ・マネージャーのファイルがシステムのディレクトリーで使用可能になっていることを確認してください。

インストールが必要な場合は、以下のコマンドを変更してください。インストール・プロセス中は、再始動は必要ありません。検証プロセスによって、インストール・パッケージのファイル名、バージョン番号、アクション、およびアクションの状況を含む、ソフトウェアのインストールを説明するテーブルが戻されます。

1. ご使用のオペレーティング・システムに適したコマンドを入力して、<SMpackage> をインストールします。

注: 次の表にリストされている手動インストール・コマンドは、UNIX ベースのオペレーティング・システム専用 です。

表 9. ストレージ・マネージャー・パッケージのインストール・コマンドの例

オペレーティング・システム	パッケージ名	インストール・コマンド
AIX	SMruntime.AIX-10.xx.xx.bff	#installp -a -d /path_name/SMruntime.AIX-10.xx.xx.bff SMruntime.aix.rte
HP-UX	SMruntime_10.xx.xx.xx.depot	#swinstall -s /cdrom/HP-UX/SMruntime_10.xx.xx.xx.depot
Solaris	SMruntime-SOL-10.xx.xx.xx.pkg	#pkgadd -d path/SMruntime-SOL-10.xx.xx.xx.pkg
Linux on POWER	SMruntime-LINUX-10.xx.xx.xx-x.i586.rpm	#rpm -ihv SMruntime-LINUX-10.xx.xx.xx-x.i586.rpm

2. ご使用のオペレーティング・システムに適したコマンドを入力して、インストールが正常に行われたことを確認します。

表 10. ストレージ・マネージャー・パッケージのインストール検証コマンド

オペレーティング・システム	検証コマンド
AIX	# ls1pp -ah <SMpackage>.aix.rte
HP-UX	# swverify -v <SMpackage>
Solaris	# pkginfo -l <SMpackage>
Linux on POWER	# rpm -qa grep <SMpackage>

検証プロセスによってエラーが戻された場合は、IBM サービス担当員に連絡してください。

ストレージ・マネージャーのアンインストール

Windows または UNIX タイプのオペレーティング・システムでストレージ・マネージャーをアンインストールするには、このセクションの該当する手順を使用してください。

Windows オペレーティング・システムでのストレージ・マネージャーのアンインストール

Windows オペレーティング・システムでこのソフトウェアをアンインストールするには、以下の手順を完了してください。

1. 「コントロール パネル」ウィンドウを開きます。
2. Windows 2003 または Windows XP を使用している場合は、「プログラムの追加と削除」をダブルクリックします。Windows 2008 または Windows 2012 を使用している場合、「**Program and Features (プログラムと機能)**」をダブルクリックします。新しいウィンドウが開きます。
3. 「**IBM DS Storage Manager Host Software version 10.8x (IBM DS ストレージ・マネージャー・ホスト・ソフトウェア バージョン 10.8x)**」を選択します。ここで、*x* は、ご使用のソフトウェアに該当するバージョン番号です。
4. 「変更と削除」をクリックし、「Uninstall Storage Manager 10 (ストレージ・マネージャー 10 のアンインストール)」ウィザードの指示に従って、ストレージ・マネージャー・ソフトウェアをアンインストールします。このソフトウェアをアンインストールするプロセスでは、インストールが完了した後にストレージ・マネージャーによって作成されたファイルが残る場合があります。これらのファイルには、トレース・ファイル、リポジトリ・ファイル、およびその他の管理ファイルが含まれる場合があります。ストレージ・マネージャーを完全に削除するには、これらのファイルを手動で削除してください。

Linux、AIX、または Solaris オペレーティング・システムでのストレージ・マネージャーのアンインストール

UNIX タイプのオペレーティング・システムでこのソフトウェアをアンインストールするには、以下の手順を完了してください。

1. アンインストーラー・バイナリーが入っている `/opt/IBM_DS/Uninstall IBM System Storage DS Storage Manager 10` ディレクトリーを開きます。
2. コンソール・ウィンドウで `Uninstall_IBM_System_Storage_DS_Storage_Manager_10` スクリプトを実行して、ストレージ・マネージャー・ソフトウェアをアンインストールします。このソフトウェアをアンインストールするプロセスでは、オリジナルのインストールに含まれていなかったファイルが残る場合があります。これらのファイルには、トレース・ファイル、リポジトリ・ファイル、およびその他の管理ファイルが含まれる場合があります。ストレージ・マネージャーを完全に削除するには、これらのファイルを手動で削除してください。

ストレージ・マネージャーのインストールの完了

このセクションでは、ストレージ・マネージャーのエンタープライズ管理機能およびサブシステム管理機能を使用して、すべてのホスト・オペレーティング・システムについてストレージ・マネージャーをインストールする手順を説明します。

ストレージ・マネージャーのインストールを完了するには、以下の手順を実行する必要があります。

- ストレージ・サブシステムの初期自動ディスカバリーの実行
- ストレージ・サブシステムの初期手動ディスカバリーの実行
- ストレージ・サブシステムの名前
- アラート通知のセットアップ
- 管理対象ストレージ・サブシステムのサポート・データを自動的に収集するためのスケジュールの作成
- 重大イベントの場合のサポート・データ収集の使用可能化
- iSCSI ポートを持つストレージ・サブシステムの iSCSI 設定の構成
- コントローラー・コード、ESM、およびディスク・ドライブ・ファームウェアの確認、および IBM サポート・ポータルに指定されている最新バージョンへのアップグレード
- ストレージ・サブシステムのプレミアム・フィーチャーの使用可能化
- ストレージ・サブシステム・プロファイルおよびサポート・データの保存

これらの各手順については、以下のセクションで詳しく説明されています。

ストレージ・マネージャーを開始すると、「Enterprise Management (エンタープライズ管理)」ウィンドウが開きます。このウィンドウでは、以下のタスクを行うことができます。

- ストレージ・サブシステムを追加および認識する
- 管理ドメインにあるすべてのストレージ・サブシステムを表示する
- スクリプト・エディターを使用して、ストレージ・サブシステムのバッチ管理タスクを実行する

ストレージ・サブシステムの自動ディスカバリーの実行

以下の手順を完了して、ストレージ・サブシステムの初期自動ディスカバリーを実行します。

1. Windows オペレーティング・システムの場合は、「スタート」 > 「すべてのプログラム」 > 「DS Storage Manager 10 Client (DS ストレージ・マネージャー 10 クライアント)」 > 「DS Storage Manager 10 Client (DS ストレージ・マネージャー 10 クライアント)」をクリックする。UNIX タイプのオペレーティング・システムの場合は、コンソール・ウィンドウを開く。SMclient と入力して、Enter キーを押す。ストレージ・マネージャー・クライアント・ソフトウェアが開始し、「Enterprise Management (エンタープライズ管理)」ウィンドウおよび「Confirm Initial Automatic Discovery (初期自動ディスカバリーの確認)」ウィンドウが表示される。
2. 「Yes (はい)」をクリックして、ローカル・サブネットワークに接続されているホストおよびストレージ・サブシステムの初期自動ディスカバリーを開始する。

初期自動ディスカバリーが完了すると、ローカル・サブネットワークに接続されているすべてのホストとストレージ・サブシステムが「Enterprise Management (エンタープライズ管理)」ウィンドウに表示されます。

注: 「Enterprise Management (エンタープライズ管理)」ウィンドウは、初期自動ディスカバリーの後、最新表示するのに約 1 分間かかることがあります。ストレージ・サブシステムが自動的にディスカバリーされない場合、ネットワーク接続 (アウト・オブ・バンド管理)、またはサーバーの HBA ポートからストレージ・サブシステムのホスト・ポートへの接続を確認してください。手動でのサブシステムの追加を試行するには、「Edit (編集)」 > 「Add Storage Subsystem (ストレージ・サブシステムの追加)」をクリックします。

3. 各ホストおよびストレージ・サブシステムが「Enterprise Management (エンタープライズ管理)」ウィンドウに表示されることを確認する。
 - ホストまたはストレージ・サブシステムが表示されない場合は、以下のタスクを行います。

- a. ハードウェアおよびハードウェア接続で、起こりうる問題を調べます。具体的な手順については、ご使用のストレージ・サブシステムの「インストール、メンテナンスおよびユーザーのガイド」を参照してください。
- b. ストレージ・サブシステムの認識に関する追加情報については、エンタープライズ管理のオンライン・ヘルプを参照してください。
- c. ネットワーク管理方式（一般にはアウト・オブ・バンド管理と呼ばれる）を使用している場合は、すべてのホストとストレージ・サブシステムが同じサブネット・ネットワークに接続されていること、およびイーサネット・ポートに対してゲートウェイ情報が定義されていることを確認します。ストレージ・サブシステムのイーサネット管理ポートについて詳しくは、7 ページの『ストレージ・サブシステム・コントローラーの IP アドレスのセットアップ』を参照してください。ホスト・エージェント方式（一般にはインバンド管理と呼ばれる）を使用している場合は、ホストとストレージ・サブシステムの間がファイバー・チャネル、SAS、または iSCSI で接続されていることを確認します。
- d. ネットワーク管理システムに対してストレージ・サブシステムをセットアップするための準備ステップがすべて完了していることを確認します。「**Add Device (装置の追加)**」オプションを使用して、ストレージ・サブシステムの IP アドレスを追加します。コントローラーの両方の IP アドレスを追加します。そのようにしないと、ストレージ・サブシステムを管理しようとしたときに、「partially-managed device (部分的に管理されたデバイス)」というエラー・メッセージが表示されます。

注: オートディスカバリー方式を使用するには、ストレージ・サブシステムとこのホストが同一サブネット上になければなりません。同一サブネット上にない場合は、手動方式を使用してストレージ・サブシステムを追加します。

- ホスト・エージェント管理方式を使用している場合は、以下のステップを実行します。
 - a. ホストに SMagent がインストールされていることを確認する。
 - b. ストレージ・サブシステムと、SMagent がインストールされているホストの間が、ファイバー・チャネル、SAS、または iSCSI で接続されていることを確認する。必要に応じて、SAN スイッチのゾーニングまたは VLAN の構成を確認してください。
 - c. 準備ステップがすべて完了していることを確認する。
 - 1) hot_add ユーティリティーを実行する。
 - 2) SMagent を再始動する。
 - 3) 「Enterprise Management (エンタープライズ管理)」ウィンドウで、ホストを右クリックし、「Tools (ツール)」 > 「Rescan Hosts (ホストの再スキャン)」をクリックする。

注: 特定の状況では、自動ディスカバリーの後で、1 つのストレージ・サブシステムが「**Device (デバイス)**」タブのツリー・ビューで重複して表示される場合があります。重複するストレージ管理アイコンを装置ツリーから除去するには、「Enterprise Management (エンタープライズ管理)」ウィンドウの「**Remove Device (装置の除去)**」オプションを使用します。

4. 各ストレージ・サブシステムの状況が「Optimal (最適)」であることを確認する。装置の状況が「Unresponsive (非応答)」である場合は、装置を右クリックして「**Remove Device (装置の除去)**」を選択し、管理ドメインからその装置を削除します。ストレージ・サブシステムがパワーアップされて、その日の始動プロセスを完了していることを確認します。その後、「**Add Device (装置の追加)**」オプションを使用して、その装置を再び管理ドメインに追加します。装置を除去および追加する手順については、「Enterprise Management (エンタープライズ管理)」ウィンドウのオンライン・ヘルプを参照してください。

ストレージ・サブシステムの手動ディスカバリーの実行

ホストまたはストレージ・サブシステムを手動で追加することができます。このオプションを使用すると、SMclient からストレージ・サブシステムのグループを選択的に管理できます。また、このオプションを使用すると、SMclient の初期認識の際に検出されなかった装置を追加して、管理することもできます。

「Enterprise Management (エンタープライズ管理)」ウィンドウで、「Edit (編集)」 > 「Add Storage Subsystem (ストレージ・サブシステムの追加)」をクリックします。「Add New Storage Subsystem - Manual (新規ストレージ・サブシステムの追加 - 手動)」ウィンドウが開きます。管理用のストレージ・サブシステムを追加することができます。サブシステムを追加する方法については、オンライン・ヘルプを参照してください。

重要:

1. ホスト・エージェント・ソフトウェアを通して管理される SAN の既存のストレージ・サブシステムに新しいストレージ・サブシステムを追加するときには、ホスト・エージェント・サービスを停止してから再始動する必要があります。ホスト・エージェント・サービスが再始動すると、新しいストレージ・サブシステムが検出されます。その後、「Enterprise Management (エンタープライズ管理)」ウィンドウに移動し、「Tools (ツール)」 > 「Rescan (再スキャン)」をクリックして、新しいストレージ・サブシステムを管理ドメインに追加します。
2. 直接管理 (アウト・オブ・バンド) 方式を使用して管理されている既存のストレージ・サブシステムに新しいストレージ・サブシステムを追加するときには、両方のコントローラーに対する IP アドレスを指定してください。

ストレージ・サブシステムの管理パスワードの設定

ストレージ・サブシステムの管理パスワードの機能は、ストレージ・マネージャーとコントローラー・ファームウェア・バージョンの特定の組み合わせによって異なります。

パスワードがまだ設定されていないストレージ・サブシステムの「Subsystem Management (サブシステム管理)」ウィンドウを開始するたびに、プロンプトが出され、サブシステム管理パスワードを設定するためのウィンドウが表示されます。さらに、一定期間にわたって「Subsystem Management (サブシステム管理)」ウィンドウでアクティビティがない状態が続くと、パスワードはタイムアウトになります。パスワードは 8 文字から 30 文字でなければならず、少なくとも 1 文字の数字、1 文字の小文字、1 文字の大文字、および 1 文字の非英数字 (例えば、< > ! @ + #) が含まれている必要があります。スペースは使用できません。また、大/小文字の区別があります。サブシステム管理パスワードが設定されていない場合、コントローラー・ファームウェア・バージョン 7.70.xx.xx を使用するストレージ・サブシステムでは、「Subsystem Management (サブシステム管理)」ウィンドウを開くことができません。他のコントローラー・ファームウェア・バージョンに関しては、このような制限はありません。

重要: パスワード情報は必ず、安全でしかもアクセス可能な場所に保管してください。ストレージ・サブシステムのパスワードを忘れた場合は、IBM 技術サポートに連絡してください。

ストレージ・サブシステムの命名

ネットワークをセットアップするときには、ストレージ・サブシステムに対する命名規則を決定します。例えば、デバイス・タイプを使用し、その後にシリアル番号を続けると、1815 1312345 XXXX xxx xxxx のようになります。ストレージ・マネージャー・ソフトウェアをインストールした後で初めて開始すると、管理ドメイン内のすべてのストレージ・サブシステムは <unnamed> と表示されます。「Subsystem Management (サブシステム管理)」ウィンドウを使用して、個々のストレージ・サブシステムの名前を変更します。

ストレージ・サブシステムに名前を付けるときには、以下の要因を考慮します。

- 30 文字の制限があります。先頭と末尾のスペースはすべて名前から削除されます。
- 簡単に理解できて覚えられる、固有で意味のある命名方式を使用します。
- 無原則な名前、またはすぐに意味が失われるような名前は避けます。
- ストレージ・サブシステム名を表示する際には、ソフトウェアは「Storage Subsystem」というプレフィックスを追加します。例えば、ストレージ・サブシステムを「Engineering」という名前にする場合、「Storage Subsystem Engineering」と表示されます。

ストレージ・サブシステムの名前を設定するには、以下の手順を完了します。

1. 「Enterprise Management (エンタープライズ管理)」ウィンドウでストレージ・サブシステムを右クリックし、「**Rename (名前変更)**」を選択します。「Rename Storage Subsystem (ストレージ・サブシステムの名前変更)」ウィンドウが開きます。

注: いずれかのホストがパス・フェイルオーバー・ドライバを実行している場合、ホスト・システムをリブートする前に、パス・フェイルオーバー・ドライバの構成ファイル内のストレージ・サブシステム名を更新して、そのストレージ・サブシステムへのアクセスが中断されないようにします。

2. ストレージ・サブシステムの名前を入力して、「**OK**」をクリックします。
3. 警告画面の「**Yes (はい)**」をクリックします。
4. 名前が設定されていないストレージ・サブシステムごとに、この手順を繰り返す。詳しくは、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプで、ストレージ・サブシステムの名前変更に関するトピックを参照してください。
5. 『アラート通知の設定』に進む。

アラート通知の設定

管理ドメインにデバイスを追加した後、ストレージ・サブシステムでの重大なイベントを報告するためのアラート通知を設定できます。以下のアラート通知オプションを使用できます。

- Simple Network Management Protocol (SNMP) トラップを使用する、指定したネットワーク管理ステーションへの通知
- 指定した E メール・アドレスへの通知
- 指定した英数字ポケットベルへの通知 (E メール・メッセージを変換するため、別に提供されているソフトウェアが必要です)

注: モニターできるのは、管理ドメイン内のストレージ・サブシステムだけです。イベント・モニター・サービスをインストールしていない場合は、「Enterprise Management (エンタープライズ管理)」ウィンドウを開いたままにしておく必要があります。ウィンドウを閉じておくと、管理対象のストレージ・サブシステムからアラート通知を受け取りません。追加情報については、「Enterprise Management (エンタープライズ管理)」ウィンドウのオンライン・ヘルプを参照してください。

SNMP トラップを使用するアラート通知

SNMP トラップを使用してネットワーク管理ステーションにアラート通知をセットアップするには、以下のステップを実行します。

1. ネットワーク管理ステーションの DVD ドライブにストレージ・マネージャー DVD を挿入する。指定された管理ステーションに一度だけセットアップする必要があります。
2. SMxx.x.MIB ファイルを、SMxxMIB ディレクトリーからネットワーク管理ステーションにコピーする。

3. ネットワーク管理ステーションで要求されているステップに従って、管理情報ベース (MIB) ファイルをコンパイルする。(詳しくは、ネットワーク管理者に問い合わせるか、ご使用のストレージ管理製品の資料を参照してください。)

SNMP トラップを使用しないアラート通知

SNMP トラップを使用せずにアラート通知をセットアップするには、「Enterprise Management (エンタープライズ管理)」ウィンドウで「Storage subsystem (ストレージ・サブシステム)」>「Edit (編集)」>「Configure alerts (アラートの構成)」をクリックする。

自動サポート・バンドル収集

ストレージ・マネージャー バージョン 10.83 以降、管理対象ストレージ・サブシステムから定期的にサポート・データを自動的に収集する機能は、ストレージ管理クライアント・ソフトウェアに組み込まれています。保存されたサポート・データ収集の情報は、壊滅的な障害が発生した場合にストレージ・サブシステムのトラブルシューティングおよびリカバリーに役立つことがあります。サポート・データを自動的に収集するためのスケジュールを作成するには、「Enterprise Management (エンタープライズ管理)」ウィンドウで「Tools (ツール)」>「Collect Support Data (サポート・データの収集)」>「Create/Edit (作成/編集)」を選択します。「Schedule Support Data Collection (サポート・データ収集のスケジュール)」ウィンドウが開いたら、ストレージ・サブシステムを選択して「Create/Edit (作成/編集)」をクリックし、日次、週次、月次、または年次でサポート・データを収集するスケジュールを作成します。Ctrl キーを押したままサブシステムを選択することにより、同時に複数のサブシステムのスケジュールを作成することができます。ただし、IBM では、複数のサブシステムを管理する場合にデータ収集時間をずらすことをお勧めしません。定期的なサポート・データ収集について詳しくは、オンライン・ヘルプを参照してください。定期的な自動サポート・データ収集に加えて、ストレージ・マネージャー・クライアントには、管理対象ストレージ・サブシステムに重大イベントが発生したときにサポート・データを収集する機能もあります。これを構成するには、「Enterprise Management (エンタープライズ管理)」ウィンドウで「Tools (ツール)」>「Collect Support Data (サポート・データの収集)」>「Automatically (自動)」を選択します。「Automatic Support Data Collection (自動サポート・データ収集)」ウィンドウが開いたら、必要に応じて変更を行います。詳しくは、オンライン・ヘルプを参照してください。

スケジュールは、それが定義されている管理ステーションに保管されます。サポート・バンドルを自動的に作成するには、管理ステーションが稼働中であり、ストレージ・サブシステムへの管理接続が確立されている必要があります。保存されたファイルのファイル名には、日付も含まれます。ストレージ・マネージャー・コードには、最大 5 つのファイルが維持されます。5 つのファイルが既に存在する場合、コードは新しいファイルを保存する前に、最も古いファイルを削除します。新規ファイルを保存するためのディスク・スペースが十分でない場合、ストレージ・マネージャー・コードは、十分なスペースが生じるまで、最も古いファイルから始めてファイルを削除していきます。

注: サポート・データを収集するためにストレージ・マネージャー・クライアントが稼働中である必要はありません。ただし、IBM DS ストレージ・マネージャーのサポート・モニター・サービスが実行されている必要があります。また、リポジトリ・ディレクトリーがいっぱいになったときにサポート・データが削除されるのを防ぐために、リポジトリ用に適切なスペースがある場所を選択してください。

SM スクリプトを使用した自動サポート・バンドル収集の構成と管理

「Enterprise Management (エンタープライズ管理)」ウィンドウでメニュー・オプションを使用する代わりに、管理ステーションのコマンド行インターフェースから自動サポート・バンドル収集の構成、現行スケジュールの表示、および収集のスケジュールを行うことができます。これらのコマンドについての詳細は、「IBM System Storage DS3000、DS4000、および DS5000 コマンド行インターフェースおよびスクリプト・コマンドのプログラミング・ガイド」またはオンライン・ヘルプを参照してください。これらのコマンド

は、ストレージ・マネージャーの「Enterprise Management (エンタープライズ管理)」ウィンドウで起動されるスクリプト・ウィンドウからではなく、ストレージ・マネージャーをインストールした管理ステーションから実行する必要があります。また、ストレージ・サブシステム IP アドレスを `SMcli` コマンドの一部として指定したり、`supportBundle` コマンドの前に「-c」パラメーターを指定したりしないでください。スクリプト・コマンド値には、管理対象ストレージ・サブシステムの `subsystemName` を使用します。`subsystemName` を調べるには、次の `smcli` コマンドに `-d` パラメーターを付けて実行してください。

```
C:\Program Files (x86)\IBM_DS\client>smcli -d
DS3400A          fe80:0:0:0:2a0:b8ff:fe5a:ae42
DS3524-DTL139140 ds3524dta.net.com ds3524dtb.net.com
DS3524-DTL       ds3524dt1.net.com ds3524dt2.net.com
DS5100-DTL       ds5k-a.net.com   ds5k-b.net.com
```

DS3400A、DS3524-DTL139140、DS3524-DTL、および DS5100-DTL は、ストレージ・サブシステムの名前です。ストレージ・サブシステム DS3524-DTL139140 上で毎週日曜日と火曜日の午前 2 時にサポート・バンドルを自動収集するスケジュールを使用可能にするには、次のように指定します。

```
C:\Program Files (x86)\IBM_DS\client>smcli -supportBundle schedule enable DS3524-DTL139140
daysofweek=[Sunday Tuesday] startTime=02:00
```

これらのコマンドは両方とも管理ステーションのコマンド行インターフェースから実行します。

注: 管理ステーションが Windows オペレーティング・システム上にある場合は、管理者としてこれらのコマンドを実行する必要があります。

iSCSI 設定の管理

「Subsystem Management (サブシステム管理)」ウィンドウで、「**Setup (セットアップ)**」タブをクリックします。

注: 「Subsystem Management (サブシステム管理)」ウィンドウの「**iSCSI Manage settings (iSCSI 管理設定)**」または「**Configure iSCSI Host Ports (iSCSI ホスト・ポートの構成)**」へのリンクは、iSCSI ホスト接続をサポートするストレージ・サブシステムの場合のみ選択可能です。本書の作成時点で、以下のストレージ・サブシステムが iSCSI ホスト接続をサポートしています。

- DS3300
- DS3500
- Performance Module Controller 搭載の DCS3700
- DS3950
- DS5020
- DS5100/5300

以下の iSCSI オプションが「**Storage Subsystem management (ストレージ・サブシステム管理)**」メニューから選択可能です。これらについては、以下のセクションで説明します。

注: これらの iSCSI オプションのメニュー選択は、コントローラー・ファームウェアのバージョンに応じて変更されます。該当するメニュー・オプションについては、オンライン・ヘルプを参照してください。

- 43 ページの『ターゲット認証の変更』
- 43 ページの『相互認証許可の入力』
- 43 ページの『ターゲット ID の変更』
- 43 ページの『ターゲット・ディスカバリーの変更』
- 43 ページの『iSCSI ホスト・ポートの構成』

- 44 ページの『iSCSI セッションの表示または終了』
- 44 ページの『iSCSI 統計の表示』

ターゲット認証の変更

「**Change Target Authentication (ターゲット認証の変更)**」を選択して、iSCSI ログインのセキュリティー折衝フェーズ中にイニシエーターが使用する必要がある、ターゲットのチャレンジ・ハンドシェイク認証プロトコル (CHAP) シークレットを指定します。デフォルトでは、「**None (なし)**」が選択されています。選択を変更するには、「**CHAP**」をクリックして CHAP シークレットを入力します。ランダム・シークレットを生成するオプションを選択することもできます。これによって 1 方向 CHAP が使用可能になります。

相互認証許可の入力

「**Enter Mutual Authentication Permissions (相互認証許可の入力)**」を選択する前に、イニシエーター用のホスト・ポートを定義し、ターゲット認証を使用可能にする必要があります。ホスト・ポートがリストされた後、リストからホストを選択して「**Chap Secret (CHAP シークレット)**」をクリックし、ターゲットからイニシエーターに渡されるシークレットを指定して認証します。これによって相互 CHAP (双方向) が使用可能になります。

ターゲット ID の変更

「**Change Target Identification (ターゲット ID の変更)**」を選択して、デバイス・ディスカバリー中に使用されるターゲットの別名を指定します。30 文字未満の固有の名前を、ターゲット用に指定する必要があります。

注: 別名の上にリストされている完全修飾の IQN を使用してターゲットに接続します。

ターゲット・ディスカバリーの変更

「**Change Target Discovery (ターゲット・ディスカバリーの変更)**」を選択して、iSNS (iSCSI Simple Naming Service) を使用してデバイス・ディスカバリーを実行します。このオプションを選択した後、

「**Use iSNS Server (iSNS サーバーの使用)**」チェック・ボックスを選択します。iSNS サーバーのディスカバリーにネットワーク上の DHCP サーバーを使用するかどうか選択することもできます。さらに、インターネット・プロトコル・バージョン 4 (IPv4) または IPv6 アドレスを手動で指定することができます。

「**Advanced (拡張)**」タブをクリックすると、セキュリティー強化のために iSNS サーバーに別の TCP/IP ポートを割り当てることができます。

注: 正しいデバイス・ディスカバリーに必要なポート・ログイン情報を提供するには、すべての iSCSI ポートが同じ iSNS サーバーと通信可能であることが必要です。

iSCSI ホスト・ポートの構成

「**Configure iSCSI Host Ports (iSCSI ホスト・ポートの構成)**」を選択して、すべての TCP/IP 設定を構成します。すべてのポートについて IPv4 および IPv6 の使用可能または使用不可を選択することができます。静的 IP アドレスを割り当てるか、DHCP を使用して IP アドレスを検出することも可能です。

「**Advanced IPv4 Settings (拡張 IPv4 設定)**」では、「**VLAN Tags (VLAN タグ)**」(802.1Q) を割り当てるか、または「**Ethernet Priority (イーサネット優先順位)**」(802.1P) を設定することができます。「**Advanced Host Port Settings (拡張ホスト・ポート設定)**」では、そのターゲット・ポートに対する固有の iSCSI TCP/IP ポートを指定することができます。このオプションから「**Jumbo Frames (ジャンボ・フレーム)**」を使用可能にすることもできます。サポートされるフレーム・サイズは 1500 および 9000 です。

iSCSI セッションの表示または終了

「View/End iSCSI Sessions (iSCSI セッションの表示/終了)」を選択して、ターゲットに接続されたすべての iSCSI セッションを表示します。このページから、イニシエーター・セッションのターゲット ASYNC ログアウトを強制することで、既存のセッションを閉じることも可能です。

iSCSI 統計の表示

「View iSCSI Statistics (iSCSI 統計の表示)」を選択して、すべての iSCSI セッションのデータ (例えば、ヘッダー・ダイジェスト・エラーの数、データ・ダイジェスト・エラーの数、および正常なプロトコル・データ単位数) のリストを表示します。修正処置の後のベースライン・カウントを設定することで、問題が解決したかを判別することもできます。

iSNS サーバーの使用

iSNS サーバーを正しく使用するためには、多くの考慮事項があります。イニシエーターまたはターゲットの DHCP リース・ディスカバリーの間に提供される iSNS サーバー・アドレスが正しく割り当てられていることを確認してください。これにより、イニシエーター・ベースのソリューションを使用する場合に、ディスカバリーが容易になります。このようにできずに、iSNS サーバーを手動でソフトウェアまたはハードウェア・イニシエーターに割り当てる必要がある場合は、ストレージ・サブシステムの iSCSI ポートおよび iSCSI イニシエーターがすべて同一のネットワーク・セグメント内にあることを確認する必要があります (または、別々のネットワーク・セグメント間のルーティングが正しいことを確認します)。このようにしない場合、iSCSI ディスカバリー・プロセス中にすべてのポートをディスカバリーできずに、コントローラーまたはパスのフェイルオーバーが正しく実行されない可能性があります。

DHCP の使用

ターゲット・ポータルに DHCP を使用しないでください。DHCP を使用する場合は、ストレージ・サブシステムの再始動の際にリースが一貫して維持されるように、DHCP 予約を割り当てる必要があります。静的 IP 予約ができない場合、イニシエーター・ポートはコントローラーと通信できなくなり、そのデバイスへの再接続ができなくなる可能性があります。

サポートされるハードウェア・イニシエーターの使用

これらのアダプターを取り付けて構成する前に、管理アプリケーションと最新のファームウェアがインストールされていることを確認してください。その後で、各アダプターを一度に 1 つずつ構成します。iSCSI アダプターとターゲット・ポートが同じネットワーク・セグメント内にある単一コントローラー・サブシステムの構成では、各アダプターをどのターゲット・ポートにでも接続できます。複合構成では、各アダプターを 1 つのコントローラー装置に接続できます。フェイルオーバーが正常に実行されるように、次のいずれかの方法で、サーバー内の各 iSCSI アダプターを接続します。

- **サーバー内の単一 iSCSI アダプター** - iSCSI アダプター・ポートは、コントローラー A および B の両方の iSCSI ホスト・ポートにログインできる必要があります。iSCSI ポートは、コントローラー A および B の iSCSI ポート・サブネットを持つマルチホームとして構成されます。
- **サーバー内の複数の iSCSI アダプター** - 各アダプター・ポートは、各コントローラーの iSCSI ホスト・ポートへの単一パスを持つことができます。各 iSCSI アダプター・ポートとそれに関連付けられた iSCSI コントローラー・ホスト・ポートは、他の iSCSI アダプター・ポートとコントローラー・ホスト・ポートのペアとは別のサブネット上になければなりません。

Qlogic ハードウェア・イニシエーター・アダプターを使用する場合、以下の手順を実行して、ハードウェア・イニシエーターからすべての使用可能なターゲット・ポートにログインできるようにします。その他のハードウェア・イニシエーター・アダプターの場合は、該当するハードウェア・イニシエーター・アダプターの資料を参照して、すべての使用可能なターゲット・ポートへのログインに関する情報を確認してください。

サポートされるハードウェア・イニシエーターのリストについては、<http://www.ibm.com/systems/support/storage/config/ssic> にアクセスしてください。

QLogic ハードウェア・イニシエーターからすべての使用可能なターゲット・ポートにログインするには、以下の手順を実行します。

注: 以下の手順内のステップの実行に失敗すると、パス・フェイルオーバーの不整合およびストレージ・サブシステムの不正な動作が発生する可能性があります。

1. SANsurfer 管理ユーティリティを開始する。
2. qlremote エージェントを実行しているシステムに接続する。
3. 構成するアダプターを選択する。
4. アダプターのポート 0 またはポート 1 を選択する。
5. 「**Target Settings (ターゲットの設定)**」をクリックする。
6. ウィンドウの右端にある正符号 (+) をクリックする。
7. 接続するターゲット・ポートの IPv4 または IPv6 アドレスを入力する。
8. 「**OK**」をクリックします。
9. 「**Config Parameters (構成パラメーター)**」を選択する。
10. ISID が見えるまでスクロールする。接続 0 では、リストされている最後の文字は 0 でなければなりません。同様に、接続 1 では 1、接続 2 では 2 でなければなりません。
11. 作成するターゲットへの各接続に対して、ステップ 6 から 10 を繰り返す。
12. すべてのセッションが接続されたら、「**Save Target Settings (ターゲット設定の保存)**」を選択する。
IPv6 をサポートするために、IBM System x 用 QLogic iSCSI 単一ポートまたはデュアル・ポート PCIe HBA を使用する場合は、ホスト・バス・アダプターのファームウェアがローカル・リンク・アドレスを割り当てできるようにする必要があります。

IPv6 の使用

ストレージ・サブシステムの iSCSI ポートは、インターネット・プロトコル・バージョン 6 (IPv6) TCP/IP をサポートします。ローカル・リンク・アドレスを手動で割り当てる場合は、最後の 4 つのオクテットのみが構成可能であることに注意してください。最初の 4 つのオクテットは、fe80:0:0:0 です。イニシエーターからターゲットへ接続を試みる場合は、完全な IPv6 アドレスが必要になります。完全な IPv6 アドレスを指定しない場合は、イニシエーターの接続が失敗する場合があります。

iSCSI ホスト接続のためのネットワーク設定の構成

複雑なネットワーク・トポロジで iSCSI ホスト接続をサポートするストレージ・サブシステムを使用する場合には、いくつかの課題に対応する必要があります。可能な場合、iSCSI トラフィックを専用のネットワークに分離してください。これが可能ではなく、ハードウェア・ベースのイニシエーターを使用する場合は、Keep Alive timeout (キープアライブ・タイムアウト) を 120 秒に設定する必要があります。Keep Alive timeout (キープアライブ・タイムアウト) を設定するには、以下の手順を実行してください。

1. SANsurfer 管理ユーティリティを開始して、サーバーに接続する。
2. 構成するアダプターとアダプター・ポートを選択する。
3. ポート・オプションとファームウェアを選択する。

デフォルトの接続タイムアウトは 60 秒です。この設定は、単純なネットワーク・トポロジでは適切です。ただし、より複雑な構成で、ネットワーク収束が発生し、「Fast Spanning Tree (高速スパンニング・ツリー)」および別のスパンニング・ツリー・ドメインを使用していない場合は、入出力タイムアウトが発

生する可能性があります。Linux iSCSI ソフトウェア・イニシエーターを使用している場合は、スパンニング・ツリーの問題点に対応するために、ConnFailTimeout パラメーターを変更します。ConnFailTimeout 値は 120 秒に設定する必要があります。

最大伝送単位の設定の構成

リンク上で相互に通信する必要があるすべてのデバイス (同一 VLAN 上のデバイスなど) は、同じ最大伝送単位 (MTU) サイズで構成されなければなりません。MTU サイズは、構成項目であるか、デバイスにハードコーディングされているかのいずれかです。ログインまたは接続の確立時にエンドポイント間で折衝されません。MTU サイズより大きいパケットをデバイスが受信する場合、デバイスはそのパケットを除去します。ルーターが受信するパケットが、受信に使用されたリンクの MTU サイズを超えないものの、転送リンクの MTU サイズを超える場合、そのルーターはパケットをフラグメント化するか (IPv4)、あるいは「packet too large (パケットが大きすぎます)」ICMP エラー・メッセージを返します。ネットワーク・リンク上のすべてのコンポーネントが同じ MTU サイズ値を使用していることを確認してください。

iSCSI をサポートするストレージ・システムの場合、デフォルトの MTU 設定は 1500 バイトです。ジャンボ・フレーム用に 9000 バイトを選択するオプションがあります。エンドツーエンドのジャンボ・フレームが有効に機能するために、すべてのコンポーネント (ホスト、スイッチ、ルーター、およびターゲット) でジャンボ・フレーム (大きい MTU) が使用可能でなければなりません。ジャンボ・フレームが一部のコンポーネントで使用可能でない場合、次の項目の 1 つ以上が発生する可能性があります。

- フレームが除去される。
- 大きすぎるパケットに関するエラー・メッセージが出されるため、接続は除去されない。
- ジャンボ・フレームがフラグメント化される。

Microsoft iSCSI ソフトウェア・イニシエーターの考慮事項

Microsoft iSCSI ソフトウェア・イニシエーター (バージョン 2.03 以降) に付属の固有マルチパス入出力 (MPIO) は、サポートされません。正常なフェイルオーバーおよび入出力アクセスを確実にするには、ストレージ・マネージャーに付属の DSM を使用する必要があります。Microsoft iSCSI ソフトウェア・イニシエーターに付属の固有 MPIO を使用すると、予期しない影響を引き起こします。

コントローラー・ファームウェア、NVSRAM、ESM ファームウェアのダウンロード

このセクションでは、ストレージ・サブシステム・コントローラー・ファームウェア、NVSRAM、ストレージ・エンクロージャー ESM ファームウェア、およびドライブ・ファームウェアのダウンロード方法について説明します。通常、ストレージ・サブシステムのファームウェアをダウンロードする順序は次のとおりです。

1. コントローラー・ファームウェア
2. コントローラー NVSRAM
3. ESM ファームウェア
4. ドライブ・ファームウェア

更新されたコントローラー・ファームウェア、NVSRAM、ESM ファームウェア、およびドライブ・ファームウェアに付属の Readme ファイルを調べて、ファームウェアのダウンロード順序に必要な変更があるかどうかを確認してください。

重要:

1. 以下の手順では、最新のコントローラー・ファームウェア・バージョンを使用していることが想定されています。IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) 上の最新バージョンの

ストレージ・サブシステム・コントローラー・ファームウェア、NVS RAM、およびストレージ・エンクロージャー ESM ファームウェアにアクセスします。ご使用のオペレーティング・システムの最新のストレージ・マネージャー README ファイルについては、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

2. IBM では、一部のストレージ・サブシステムで、入出力を処理しながらのストレージ・サブシステム・コントローラーおよび ESM のファームウェア・ダウンロード (並行ファームウェア・ダウンロードとも呼ばれます) をサポートしています。並行ファームウェア・ダウンロードを進める前に、ファームウェア・コードまたはご使用のオペレーティング・システムのストレージ・マネージャーのホスト・ソフトウェアに同梱されている README ファイルで制限事項を確認してください。
3. 単一コントローラーのストレージ・サブシステムにファームウェアおよび NVSRAM をダウンロードする間は、すべての入出力アクティビティを中断してください。入出力アクティビティを中断しない場合、ホスト・サーバーとストレージ・サブシステムの間に冗長性のあるコントローラー接続があるため、ホスト・サーバーで入出力要求は失敗します。
4. ファームウェア更新をストレージ・サブシステムに適用する前に、必ずストレージ・サブシステム・コントローラー・ファームウェアの README ファイルを読んで、コントローラー・ファームウェアの依存関係および前提条件を確認してください。依存関係および前提条件を満たさない条件下でストレージ・サブシステム・ファームウェアのコンポーネントを更新すると、ダウン時間が (問題の修正またはリカバリーのために) 発生することがあります。
5. コントローラー・ファームウェアのダウングレードは、サポートされている機能ではありません。このオプションは、IBM サポートの指示の下でのみ使用する必要があります。ファームウェア・レベル 07.xx から 06.xx へのダウングレードはサポートされておらず、試行するとエラーが返されます。

既存のコントローラー・ファームウェアが 06.1x.xx.xx 以降の場合は、新しいコントローラー・ファームウェアをアップグレードまたはダウンロードすると同時に、NVSRAM をダウンロードするよう選択するオプションがあります。さらに、ファームウェアと NVSRAM をすぐにダウンロードし、後で都合のいいときに活動化するオプションもあります。詳しくは、オンライン・ヘルプを参照してください。

注: 後の時点でファームウェアを活動状態にするためのオプションは、DS4400 ストレージ・サブシステムではサポートされていません。

ファームウェア・レベルの判別

ファームウェア・アップグレードをダウンロードする前に、現在のファームウェア・バージョンを確認します。ストレージ・サブシステム、ストレージ・エンクロージャー、ドライブ、および ESM のファームウェア・バージョンを確認するには、3 つの方法があります。どちらの方法でも、ストレージ・サブシステムとそれに接続されたストレージ・エンクロージャーを管理するストレージ・マネージャー・クライアントを使用します。

方法 1:

「Subsystem Management (サブシステム管理)」ウィンドウに進み、ストレージ・サブシステム・プロファイルを表示するためのメニュー・オプションを選択します。「Storage Subsystem Profile (ストレージ・サブシステム・プロファイル)」ウィンドウが開いたら、「Summary (サマリー)」タブをクリックし、「Monitor (モニター)」ページをスクロールして、以下の情報を見つけます。「View Firmware Inventory or View Storage Subsystem Profile (ファームウェア・インベントリ表示またはストレージ・サブシステム・プロファイル表示)」ページには、ストレージ・サブシステム全体のすべてのプロファイル情報 (ファームウェア・バージョン番号など) が含まれます。以下に例を示します。

ストレージ・サブシステム・コントローラー・ファームウェア・バージョン

ストレージ・サブシステム・プロファイルの表示

以下のプロファイル情報の例を参照してください。

```
FIRMWARE INVENTORY
IBM DS Storage Manager 10
  SMW Version:      10.84.G5.21
  Report Date:      Tue Oct 09 21:13:34 CST 2012
```

```
Storage Subsystem
Storage Subsystem Name: DCS3700
Current Package Version: 07.84.39.00
Current NVSRAM Version: N1818D37R0784V04
Staged Package Version: None
Staged NVSRAM Version: None
```

コントローラー

```
Location:      Enclosure 1, Slot A
Current Package Version: 07.84.39.00
Current NVSRAM Version: N1818D37R0784V04
Board ID:      2660
Sub-Model ID:  162
```

```
Location:      Enclosure 1, Slot B
Current Package Version: 07.84.39.00
Current NVSRAM Version: N1818D37R0784V04
Board ID:      2660
Sub-Model ID:  162
```

電源機構

```
Location:      Enclosure 1 Right
Firmware Version: Not Available

Location:      Enclosure 1 UNKNOWN
Firmware Version: Not Available
```

ドライブ

```
Enclosure, Drawer, Slot:      Manufacturer:
Product ID:      Drive Type:      Capacity:
Drive Firmware Version:      FPGA Version: (SSD only)

Enclosure 1, Drawer 1, Slot 2      IBM-ESXS
ST9300603SS F Serial Attached SCSI (SAS) 278.896 GB
B53B Not Available
Enclosure 1, Drawer 1, Slot 3      IBM-ESXS
CBRCA300C3ETS0 N Serial Attached SCSI (SAS) 278.896 GB
C610 Not Available
```

方法 2:

以下のオプションから適切な手順を実行して、指定されているファームウェア・バージョンを取得します。

コントローラー・ファームウェア・バージョンの取得

「Subsystem Management (サブシステム管理)」ウィンドウの「**Hardware (ハードウェア)**」タブにある「**Controller (コントローラー)**」アイコンをクリックします。新規ウィンドウに、コントローラーの情報が表示されます。

個々のコントローラーごとに、この処置を実行する必要があります。

ドライブ・ファームウェアのバージョンを取得するには:

「Subsystem Management (サブシステム管理)」ウィンドウの「**Hardware (ハードウェア)**」タブにある「**Controller (コントローラー)**」アイコンをクリックします。新規ウィンドウに、ドライブ・ファームウェアの情報が表示されます。

個々のコントローラーごとに、この処置を実行する必要があります。

ESM ファームウェア・バージョンの取得

「Subsystem Management (サブシステム管理)」ウィンドウの「**Hardware (ハードウェア)**」タブにある「**Controller (コントローラー)**」アイコンをクリックします。新規ウィンドウに、ESM ファームウェア情報が表示されます。

個々のコントローラーごとに、この処置を実行する必要があります。

コントローラーおよび NVSRAM のファームウェアのダウンロード

注: コントローラー・ファームウェアおよび NVSRAM をアップグレードする前に、「Collect All Support Data (すべてのサポート・データの収集)」操作を実行してください。データ収集手順については、263 ページの『重大イベントの問題解決』を参照してください。

このセクションでは、ストレージ・サブシステム・コントローラー・ファームウェアおよび NVSRAM のダウンロード方法を説明します。通常、ストレージ・サブシステムのファームウェアをダウンロードするときは、まずコントローラー・ファームウェアから開始し、NVSRAM、ESM ファームウェア、そしてドライブ・ファームウェアをダウンロードするという順序になります。

重要: 06.xx から 07.xx にアップグレードする場合、コントローラー・ファームウェア・アップグレード・ツールを使用する必要があります。50 ページの『IBM System Storage コントローラー・ファームウェア・アップグレード・ツールの使用』を参照してください。既に 07.xx ファームウェア・レベルを使用している場合は、別の 07.xx レベルにアップグレードするためにコントローラー・ファームウェア・アップグレード・ツールを使用する必要はありません。ただし、アップグレード・ツールには有用な診断機能があります。

ファームウェア バージョン 06.1x.xx.xx 以降および NVSRAM をダウンロードするには、次の手順を実行します。

1. 「Enterprise Management (エンタープライズ管理)」ウィンドウから、ストレージ・サブシステムを選択します。
2. 「Tools (ツール)」 > 「Upgrade Controller Firmware (コントローラー・ファームウェアのアップグレード)」をクリックします。「Upgrade Controller Firmware (コントローラー・ファームウェアのアップグレード)」ウィンドウが開きます。

注: コントローラー・ファームウェアが 7.77.xx.xx 以降の場合、システムは事前アップグレード・チェックを自動的に実行し、これに数分かかります。この事前アップグレード・チェックを満たしている場合にのみ、コントローラー・ファームウェア・アップグレードが進められます。ストレージ・サブシステムに、コントローラー・ファームウェア・バージョン 06.1x.xx.xx 以降がインストールされている場合、ファームウェア・ファイルと共に NVSRAM ファイルをダウンロードできます。このダウンロード機能は、コントローラー・ファームウェア 05.4x.xx.xx 以前を使用するストレージ・サブシステムではサポートされていません。既存のコントローラー・ファームウェアのバージョンが 05.4x.xx.xx 以前の場合、ファームウェアをダウンロードするためのウィンドウのみが表示されます。

ストレージ・マネージャー・ソフトウェアは各ストレージ・サブシステムの状況を確認し、アップデートが必要なストレージ・サブシステムのリストを表示します。

3. アップグレードするストレージ・サブシステムをすべて選択します。「Firmware (ファームウェア)」をクリックします。「Download Firmware (ファームウェア・ダウンロード)」ウィンドウが開きます。

注: 同時に複数のサブシステムをアップグレードする場合、それらすべてのサブシステムは同じタイプである必要があります。

IBM System Storage コントローラー・ファームウェア・アップグレード・ツールの使用

ここでは、IBM System Storage コントローラー・ファームウェア・アップグレード・ツールを使用して、ご使用の DS4800、DS4700、または DS4200 Express® コントローラー・ファームウェアを 06.xx から 07.xx にアップグレードする方法について説明します。

重要:

- コントローラー・ファームウェア・アップグレード・ツールは、DS4800、DS4700、および DS4200 コントローラーをバージョン 06.xx からバージョン 07.xx にマイグレーションする場合にのみ使用してください。
- このツールは、コントローラー、ESM、またはドライブ・ファームウェアの標準アップグレード (6.xx.xx.xx コード・スレッド内または 7.xx..xx.xx コード・スレッド内でのアップグレード) を対象としていません。コントローラー、ESM、またはドライブ・ファームウェアの標準アップグレードを実行する場合は、46 ページの『コントローラー・ファームウェア、NVS RAM、ESM ファームウェアのダウンロード』を参照してください。
- ストレージ・マネージャー・バージョン 10.50 以降から、コントローラー・ファームウェア・アップグレード・ツールは「Enterprise Management (エンタープライズ管理)」ウィンドウの一部となり、別個のツールではなくなりました。「Tools (ツール)」 > 「Upgrade Controller Firmware (コントローラー・ファームウェアのアップグレード)」をクリックして、「Controller Firmware Upgrade (コントローラー・ファームウェアのアップグレード)」ウィンドウを開きます。

重要: ダウンロードするファームウェアに、ご使用のストレージ・サブシステムにインストールされているストレージ・マネージャー・ソフトウェアとの互換性があることを確認してください。互換性のないファームウェアをダウンロードすると、ストレージ・サブシステム内のドライブへのアクセスが失われる可能性があります。必要な場合、IBM System Storage コントローラー・ファームウェア・アップグレード・ツールを使用する前に、ストレージ・マネージャーをアップグレードしてください。

IBM System Storage コントローラー・ファームウェア・アップグレード・ツールを使用する前に、以下のガイドラインを必ず理解しておいてください。

- DS4800、DS4700、および DS4200 ストレージ・サブシステムのすべてのデータをバックアップして、既存のシステム構成を保存しておいてください。ツールがアップグレードを完了した後、コントローラーを以前のファームウェア・バージョン・レベルに戻すことはできません。
- アップグレードはオフラインで実行する必要があります。ストレージ・マネージャーを既存のホスト環境にインストールするときは、その全体をオンラインで実行してください。ほとんどのフェイルオーバー・ドライバーは、有効にするためにホストのリブートを必要とします。
- ファームウェアをダウンロードする前に、すべてのデバイスが「Optimal (最適)」状況でなければなりません。ヘルス・チェック・ユーティリティを使用して、デバイスの「Optimal (最適)」状況を検証してください。
- また、ファームウェアの現行レベルを確認する必要があります。
- アップグレード処理中は、構成を変更したり、ドライブまたはエンクロージャーを取り外したりしないでください。
- ファームウェアの現行バージョンについては、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照して、Web で最新のストレージ・マネージャー README ファイルにアクセスする方法を調べてください。

デバイスのヘルス状態の確認: デバイスのヘルス状態を判別するには、以下の手順を実行します。

1. ストレージ・マネージャーの「サブシステム管理」ウィンドウで、ストレージ・サブシステムを右クリックします。ストレージ・マネージャーは、管理対象の各デバイスとの通信を確立して、現行デバイスの状況を判別します。

次の 6 つの状況条件の可能性があります。

- **Optimal (最適):** 管理対象デバイス内のすべてのコンポーネントが最適な動作状態にある。
 - **Needs Attention (要注意):** 管理対象デバイスに問題があり、それを訂正するために介入が必要である。
 - **Fixing (修正中):** 「Needs Attention (要注意)」状態が訂正され、管理対象デバイスは現在「Optimal (最適)」状態に変化している。
 - **Unresponsive (応答なし):** 管理ステーションが、デバイスと、あるいはストレージ・サブシステム内の一方または両方のコントローラーと通信できない。
 - **Contacting Device (デバイスに接続中):** ストレージ・マネージャーがデバイスとの接続を確立中である。
 - **Needs Upgrade (要アップグレード):** ストレージ・サブシステムが、ストレージ・マネージャーで現在サポートされていないレベルのファームウェアを実行している。
2. 状態が「Optimal (最適)」でない場合、ファームウェアのダウンロード前に、「サブシステム管理」ウィンドウから「**Recovery Guru** (リカバリー・グループ)」をクリックして、システム・リカバリーに関する詳しい情報を確認してください。うまくシステム・リカバリーができない場合は、障害の解決方法について IBM 技術サポート担当者にお問い合わせください。

コントローラー・ファームウェア・アップグレード・ツールのオープンおよび使用: コントローラー・ファームウェア・アップグレード・ツールを使用するには、「Enterprise Management (エンタープライズ管理)」ウィンドウで「**Tools (ツール)**」 > 「**Firmware Upgrade (ファームウェア・アップグレード)**」をクリックします。「Firmware Upgrade (ファームウェア・アップグレード)」ウィンドウが開きます。ファームウェア・アップグレード・ツールは、自動的にこれらのサブシステムに対して診断検査を実行し、コントローラー・ファームウェアのアップグレードを実行するのに適切な状態であるかどうかを判別します。

注:

- 「Optimal (最適)」以外の状態の場合は、IBM サポートに連絡して支援を得る必要があります。詳しくは、xxii ページの『ソフトウェアのサービスとサポート』を参照してください。
- このツールでは、メジャー・リリースからメジャー・リリース (例えば、06.xx. から 07.xx) へのアップグレードのみを実行できます。「Subsystem Management (サブシステム管理)」ウィンドウでは、このタイプのファームウェア・アップグレードの実行を試行しないでください。
- 07.xx ファームウェア・レベルにアップグレードした後は、ファームウェア・アップグレード・ツールを使用する必要はありません。以降のファームウェア・アップグレードを実行するには、「Subsystem Management (サブシステム管理)」ウィンドウを使用してください。

このツールの使用についての詳細情報を見るには、コントローラー・ファームウェア・アップグレード・ツールの「**Help (ヘルプ)**」ボタンをクリックしてください。

ストレージ・サブシステムの追加: コントローラー・ファームウェア・アップグレード・ツールを使用してストレージ・サブシステムを追加するには、以下の手順を実行します。

1. 「**Add (追加)**」をクリックします。「Select Addition Method (追加方式の選択)」ウィンドウが開きます。
2. 「**Automatic (自動)**」または「**Manual (手動)**」をクリックします。
3. 「**OK**」をクリックして、ストレージ・サブシステムの追加を開始します。

4. ファームウェア・アップグレードを妨げる可能性がある、追加したストレージ・サブシステムの問題を表示するには、「**View Log (ログの表示)**」をクリックします。

ファームウェア・ダウンロード:

1. 活動化するストレージ・サブシステムを選択します。「**Download (ダウンロード)**」ボタンが選択可能になります。
2. 「Enterprise Management (エンタープライズ管理)」ウィンドウのツールバーから、「**Tools (ツール)**」>「**Upgrade Firmware (ファームウェアのアップグレード)**」をクリックします。「Download Firmware (ファームウェア・ダウンロード)」ウィンドウが開きます。
3. 「**Browse (参照)**」をクリックして、ディレクトリーからダウンロードしたいコントローラー・ファームウェア・ファイルを選択します。
4. 「**Browse (参照)**」をクリックして、ディレクトリーから NVSRAM ファイルを選択します。
5. 「**OK**」をクリックします。ファームウェア・ダウンロードが開始されます。「Controller Firmware Upgrade (コントローラー・ファームウェアのアップグレード)」ウィンドウにステータス・バーが表示されます。

IBM System Storage コントローラー・ファームウェア・アップグレード・ツールのログ・ファイルの表示 : コントローラー・ファームウェア・アップグレード・ツールのログ・ファイルには、ファームウェアの更新を妨げる可能性がある、ストレージ・システムの問題がすべて記録されます。ファームウェアのアップグレード中に問題が発生した場合、「**View Log (ログの表示)**」をクリックしてログ・ファイルを開きます。ファームウェアのダウンロードを再試行する前に、ログ・ファイル内の問題を修正します。

ESM ファームウェア・ダウンロード

このセクションでは、ストレージ・エンクロージャー ESM ファームウェアのダウンロード方法を説明します。通常、ストレージ・サブシステムのファームウェアをダウンロードするときは、まずコントローラー・ファームウェアから開始し、NVSRAM、ESM ファームウェア、そしてドライブ・ファームウェアをダウンロードするという順序になります。

ESM ファームウェアをダウンロードするには、以下の手順を実行します。

1. 「System Management (システム管理)」ウィンドウで、「**Upgrade (アップグレード)**」>「**ESM firmware (ESM ファームウェア)**」を選択する。「Download Environmental Card Firmware (環境カード・ファームウェアのダウンロード)」ウィンドウが開きます。
2. 「**Select All (すべて選択)**」をクリックし、すべてのストレージ・エンクロージャーのダウンロードを指定する。また、1 つのストレージ・エンクロージャーを選択することも、Ctrl キーを押しながらエンクロージャーを選択して複数のエンクロージャーを選択することもできます。

注: 複数のエンクロージャーを選択した場合、ESM ファームウェアのダウンロード中はすべての入出力アクティビティーを中断してください。一度に 1 つのエンクロージャーだけを選択した場合は、サーバーが I/O 活動を実行している間でも、ESM ファームウェアをダウンロードできます。

3. 「**Browse (参照)**」をクリックして、ESM ファームウェア・ファイルのファイル名を識別して選択し、「**Start (スタート)**」をクリックして ESM ファームウェアのダウンロードを開始する。
4. 「Confirm Download (ダウンロードの確認)」ウィンドウで、yes と入力して「**OK**」をクリックし、ダウンロード・プロセスを開始する。
5. 選択したすべてのエンクロージャーに ESM ファームウェアがダウンロードされた後、「**Cancel (キャンセル)**」をクリックしてウィンドウを閉じる。

新規 ESM を、ESM ファームウェアの自動同期をサポートするストレージ・サブシステム内の既存のストレージ・エンクロージャーに取り付けるとき、新規 ESM 内のファームウェアは自動的に既存 ESM 内のファームウェアに同期化されます。これにより、ESM ファームウェアのミスマッチ条件はすべて自動的に解決されます。

ESM ファームウェアの自動同期を使用可能にするには、ご使用のシステムが以下の要件を満たしていることを確認してください。

- ストレージ・マネージャーのイベント・モニターがインストールされ、実行されている必要がある
- ストレージ・サブシステムが、ストレージ・マネージャー・クライアント (SMclient) の「Enterprise Management (エンタープライズ管理)」ウィンドウで定義されている必要がある

注: 本書の作成時点で、ストレージ・マネージャーは、EXP710 および EXP810 ストレージ・エンクロージャーでのみ ESM ファームウェアの自動同期をサポートします。将来、他のタイプのストレージ・エンクロージャーをサポートするかどうかについては、IBM にお問い合わせください。ESM ファームウェア自動同期サポートを使用せずにストレージ・エンクロージャー内で ESM ミスマッチ条件を訂正するには、SMclient の「Subsystem Management (サブシステム管理)」ウィンドウにある ESM ファームウェアのダウンロード・メニュー機能を使用して、正しい ESM ファームウェア・ファイルをダウンロードする必要があります。

ドライブ・ファームウェア・ダウンロード

このセクションでは、ドライブ・ファームウェア・ダウンロードの指示を記載します。最大で 4 種類のドライブ・タイプで、同時にドライブ・ファームウェアを更新することができます。照会の際にドライブが別々の製品 ID を報告する場合、ドライブは異なるドライブ・タイプであると見なされます。追加情報については、オンライン・ヘルプを参照してください。

重要:

1. 以下の手順では、最新のコントローラー・ファームウェア・バージョンがあることを想定しています。これより前のファームウェア・バージョンを使用している場合は、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照して、該当するファームウェア・バージョンの資料を取得してください。
2. IBM は、I/O でのファームウェア・ダウンロード (並行ファームウェア・ダウンロード ともいいます) をサポートしています。この機能は、ドライブ・ファームウェアの場合はサポートされません。ドライブおよび ATA 変換機構のファームウェア・アップグレードのためのダウン時間をスケジュールに入れる必要があります。

ストレージ・マネージャーのドライブ・ファームウェアをダウンロードするには、以下の手順を実行します。

1. ドライブ・ファームウェア・ダウンロード・プロセスを開始する前に、以下の作業を完了してください。
 - a. ドライブ・ファームウェアをストレージ・サブシステムにダウンロードする前に、すべての入出力アクティビティを停止します。
 - b. ファームウェア・アップグレードのために選択したドライブ上のすべてのデータのフルバックアップを完了させます。
 - c. ファームウェアのアップグレードのために選択したドライブにアクセスしているすべての論理ドライブ上のファイル・システムをアンマウントします。
2. 「Enterprise Management (エンタープライズ管理)」ウィンドウから、ストレージ・サブシステムを選択します。

3. 「Subsystem Management (サブシステム管理)」ウィンドウのメニュー・バーで、「**Upgrade (アップグレード)**」 > 「**Drive firmware (ドライブ・ファームウェア)**」をクリックします。「Introduction (概要)」ページが開きます。指示を読み、「**Next (次へ)**」をクリックします。

注: ストレージ・マネージャーを使用すると、最大 4 つの異なったファームウェア・パッケージを同時にダウンロードおよびアップデートできます。

4. 「**Add (追加)**」をクリックし、ダウンロードする予定のファームウェアを含むサーバー・ディレクトリを見つけます。
5. ダウンロードする計画のファームウェア・ファイルを選択して、「**OK**」をクリックします。「Selected Packages (選択済みパッケージ)」ウィンドウにファイルがリストされます。
6. ファームウェアのダウンロードを予定する最大 4 つのパッケージについて、手順 4 および 5 を繰り返し、「**Next (次へ)**」をクリックします。「Selected Packages (選択済みパッケージ)」ウィンドウに追加のファイルがリストされます。
7. ダウンロードするファームウェア・パッケージを指定した後、「**Next (次へ)**」をクリックします。
8. 「**Compatible Drives (互換性のあるドライブ)**」ページには、選択したファームウェア・パッケージ・タイプと互換性のあるドライブのリストが表示されます。このリストから、ドライブ・ファームウェアをダウンロードする先として計画しているドライブを選択します。Ctrl キーを押したまま複数のドライブを個別に選択するか、Shift キーを押したまま連続してリストされている複数のドライブを選択することができます。「**Select All (すべて選択)**」をクリックして、すべてのドライブを選択します。

注: ダウンロードを計画しているファームウェアは、「Compatible Drives (互換ドライブ)」ページにリストされているものでなければなりません。ご使用のドライブのプロダクト ID がファームウェア・タイプと一致していても、このページに互換性があるドライブのリストとして表示されない場合、IBM 技術サポート担当員に連絡して追加の指示を受けてください。

9. 「**Finish (完了)**」をクリックして、ステップ 10 で選択したそれぞれの互換ドライブへのドライブ・ファームウェア・ダウンロードを開始します。
10. 「Download Drive Firmware - Are you sure you wish to continue? (ドライブ・ファームウェアのダウンロード - 確かに処理を続けますか?)」ウィンドウが開いたら、yes (はい) を入力し「**OK**」ボタンをクリックして、ドライブ・ファームウェアのダウンロードを開始します。「Download Progress (ダウンロードの進行)」ウィンドウが開きます。ダウンロード処理が完了するまで待ちます。ファームウェア・ダウンロードがスケジュールされている各ドライブは、successful (成功) または failed (失敗) が示されるまで、in progress (進行中) として示されます。
11. ドライブが failed (失敗) として示される場合、以下の手順を実行します。
 - a. 「**Save as (別名保存)**」をクリックしてエラー・ログを保存します。
 - b. 「Subsystem Management (サブシステム管理)」ウィンドウのメニュー・バーで、ストレージ・サブシステム・イベント・ログを表示するメニュー・オプションをクリックし、イベント・ログを保存するために必要な以下の作業を行った後、IBM サービス担当員に連絡して、次のステップに進みます。
 - 1) 「**Select all (すべて選択)**」をクリックします。
 - 2) 「**Save the Storage Subsystem Event Log (ストレージ・サブシステムのイベント・ログの保存)**」をクリックします。
12. 「**Close (閉じる)**」ボタンがアクティブになったら、ドライブ・ファームウェア・ダウンロード・プロセスは完了しています。「**Close (閉じる)**」をクリックして、「Download Progress (ダウンロードの進行)」ウィンドウを閉じます。
13. 以下のいずれかの手順を使用して、特定のドライブにあるドライブ・ファームウェアのレベルを判別または検証します。

- 「Subsystem Management (サブシステム管理)」ウィンドウの「Logical (論理)」または「Physical (物理)」ページでドライブを右クリックし、「**Properties (プロパティ)**」をクリックします。関連するドライブ・ファームウェアのバージョンが、ドライブ・プロパティ・テーブルにリストされます。
- 「Subsystem Management (サブシステム管理)」ウィンドウの「Logical (論理)」ページまたは「Physical (物理)」ページで、「Select (選択)」 「**Monitor (モニター)**」 > 「**Reports (レポート)**」 > 「**Storage Subsystem Profile (ストレージ・サブシステム・プロファイル)**」をします。

ストレージ・マネージャーのプレミアム・フィーチャー

ストレージ・マネージャーは、IBM または IBM ビジネス・パートナーから個別に購入可能な、以下のプレミアム・フィーチャーをサポートしています。

コピー・サービス

以下のコピー・サービスがストレージ・マネージャーで使用可能です。

- Enhanced FlashCopy および FlashCopy
- VolumeCopy
- 拡張リモート・ミラー・オプション
- 拡張グローバル・ミラー・オプション

コピー・サービス機能の詳細については、「*IBM System Storage DS Storage Manager Copy Services User's Guide*」を参照してください。

ストレージの区画化

ストレージの区画化は、DS3000/DS4000/DS5000 コントローラー・ファームウェアのバージョンでサポートされるすべてのストレージ・サブシステムでの標準機能です。ストレージの区画化の詳細については、61 ページの『ストレージの区画化の概説』を参照してください。

FC/SATA 混合使用プレミアム・フィーチャー

IBM System Storage DS3000/DS4000/DS5000 ファイバー・チャネルおよびシリアル ATA 混合使用プレミアム・フィーチャーは、ファイバー・チャネルおよび SATA ストレージ・エンクロージャーの単一ストレージ・サブシステム・コントローラー構成への並行接続をサポートします。この混合使用プレミアム・フィーチャーを使用して、ファイバー・チャネル・ディスクまたは SATA ディスクから構築する個別のアレイを作成および管理し、単一のストレージ・サブシステムを使用して論理ドライブを該当のアプリケーションに割り振ることができます。

構成、特定の混合使用構成に必要なファームウェアのバージョン、セットアップ要件など、混合使用プレミアム・フィーチャーの使用に関する重要な情報について、「*IBM System Storage DS Storage Manager Fibre Channel and Serial ATA Intermix Premium Feature Installation Overview*」を参照してください。将来のストレージ・サブシステムによる FC/SATA 混合使用プレミアム・フィーチャーのサポートに関する情報は、IBM 担当員または販売店にお問い合わせください。

ハードウェア機能強化プレミアム・フィーチャー

これらは、下記の例のような特定のストレージ・ハードウェア構成に対するサポートを提供するプレミアム・フィーチャーです。

- ストレージ・サブシステムでサポートされる特定数のドライブ・スロット
- 特定タイプのストレージ・エンクロージャー (例えば、EXP810 接続機構、または 8 つのすべての EXP5060 接続機構)
- 特定タイプのドライブ (例えば、ソリッド・ステート・ドライブ)

このプレミアム・フィーチャー・カテゴリには、コントローラー・パフォーマンス向上プレミアム・フィーチャーも含まれます。

フル・ディスク暗号化

フル・ディスク暗号化 (FDE) を使用すると、FDE ドライブが所有者の制御下にないときにデータが脅威から保護されます。

ご使用のストレージ・サブシステムでプレミアム・フィーチャーを使用可能にするには、以下のタスクを実行します。

- 『プレミアム・フィーチャー使用可能化 ID の取得』
- 57 ページの『フィーチャー・キー・ファイルの生成』
- 58 ページの『プレミアム・フィーチャーの使用可能化』

注: プレミアム・フィーチャーを使用可能にする手順は、ご使用のストレージ・マネージャーのバージョンによって異なります。

- 59 ページの『プレミアム・フィーチャーの使用不可化』

ストレージ・サブシステムのプレミアム・フィーチャーの ID スtring を取得するには、ご使用のコントローラー・ユニットとストレージ・エンクロージャーが接続され、電源がオンになっており、それらが SMclient を使用して管理されていることを確認します。

プレミアム・フィーチャー試用版の使用可能化

注: この試用版が提供されるのは、DS3500 と DCS3700 ストレージ・サブシステム、および Performance Module Controller 搭載の DCS3700 ストレージ・サブシステム用に限定されます。

ファームウェア・バージョン 7.83 以降を搭載した IBM ストレージ・サブシステムでは、最大 90 日間、特定のプレミアム・フィーチャーの試用版が提供されます。30 日間の完了後と試用有効期限の 3 日前にアラートが送信されます。90 日間の試用期間中のいつでも、永続プレミアム・フィーチャーをご購入いただき、活動化することができます。試用期間中に永続プレミアム・フィーチャーが活動化された場合、プレミアム・フィーチャーの試用版で作成されたストレージ・サブシステムの構成は引き続き有効です。プレミアム・フィーチャーを購入されない場合は、プレミアム・フィーチャーの試用版を使用して作成したストレージ・サブシステムの構成は削除していただく必要があります。削除されないと、ストレージ・サブシステムは、試用のプレミアム・フィーチャーについて「非準拠」状態に置かれます。プレミアム・フィーチャーの試用版を使用可能にするには、「Premium Feature and Feature Pack (プレミアム・フィーチャーおよびフィーチャー・パック)」 ウィンドウで「Try Now (いますぐ試用)」をクリックします。

パーマネント・プレミアム・フィーチャーの使用可能化

まず、パーマネント・プレミアム・フィーチャーを入手し、そのための固有キーを生成しなくてはなりません。その後、パーマネント・プレミアム・フィーチャーを使用可能化します。また、パーマネント・プレミアム・フィーチャーを使用不可にすることもできます。

プレミアム・フィーチャー使用可能化 ID の取得

各ストレージ・サブシステムには固有のプレミアム・フィーチャー使用可能化 ID があります。この ID により、特定のフィーチャー・キー・ファイルを確実にそのストレージ・サブシステムのみに適用できます。

フィーチャー使用可能化 ID を取得する前に、以下の前提条件を完了してください。

1. プレミアム・フィーチャーの Web アクティベーション・カードからフィーチャー・アクティベーション・コードが入手可能であり、さらにストレージ・サブシステムのモデル、マシン・タイプ、およびシリアル番号も入手可能であることを確認します。
2. コントローラー・ユニットとストレージ拡張エンクロージャーが接続され、電源がオンになっており、それらが構成済みであることを確認します。

フィーチャー使用可能化 ID を取得するには、以下の手順を完了します。

1. 「**Start (スタート)**」 > 「**Programs (プログラム)**」 > 「**Storage Manager xx Client (ストレージ・マネージャー xx クライアント)**」をクリックします。「Enterprise Management (エンタープライズ管理)」ウィンドウが開きます。
2. 「Enterprise Management (エンタープライズ管理)」ウィンドウで、プレミアム・フィーチャーを使用可能にしたいストレージ・サブシステムをダブルクリックします。選択したストレージ・サブシステムについて「Subsystem Management (サブシステム管理)」ウィンドウが開きます。
3. ご使用のストレージ・マネージャーのバージョンに応じて、以下のアクションのいずれか 1 つを完了します。
 - ストレージ・マネージャーのバージョン 9.x 以前を使用している場合は、「**Storage Subsystem (ストレージ・サブシステム)**」 > 「**Premium Features (プレミアム・フィーチャー)**」 > 「**List (リスト)**」をクリックします。「List Premium Features (プレミアム・フィーチャーのリスト)」ウィンドウが開いて、フィーチャー使用可能化 ID が表示されます。
 - ストレージ・マネージャーのバージョン 10.x 以降を使用している場合は、「**Storage Subsystem (ストレージ・サブシステム)**」 > 「**Premium Features (プレミアム・フィーチャー)**」をクリックします。「Premium Features and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウが開きます。新しいウィンドウの下部にフィーチャー使用可能化 ID が表示されます。
4. フィーチャー使用可能化 ID を記録します。

注: フィーチャー使用可能化 ID を記録する場合に間違わないように、32 文字の ID をコピーし、「premium feature key request (プレミアム・フィーチャー・キー要求)」フィールドに貼り付けてください。

5. 「**Close (閉じる)**」をクリックしてウィンドウを閉じます。
6. 『フィーチャー・キー・ファイルの生成』に進みます。

注: ストレージ・マネージャー・バージョン 9.x 以前の既存のプレミアム・フィーチャーの状況を確認するには、メニューから「**Storage Subsystem (ストレージ・サブシステム)**」 > 「**Premium Features (プレミアム・フィーチャー)**」 > 「**List (リスト)**」を選択します。

フィーチャー・キー・ファイルの生成

<http://www.ibm.com/storage/fasttkeys> にある Premium Feature Activation ツールを使用して、フィーチャー・キー・ファイルを生成することができます。

1. Web サイトの手順を完了します。

注: プロンプトが出された後で正しいプレミアム・フィーチャーまたはフィーチャー・パックを選択したことを確認してください。

フィーチャー・キー・ファイルは、Web ページでダウンロードでき、また、E メールで送信することができます。

2. ハード・ディスクに、新規ディレクトリーを作成します (例えば、ディレクトリーに `FlashCopyfeaturekey` という名前を付けます)。
3. プレミアム・フィーチャー・キー・ファイルを新規ディレクトリーに保存します。

プレミアム・フィーチャー・キーが失われたり、プレミアム・フィーチャー ID が変更されてプレミアム・フィーチャーが準拠しなくなった場合、<http://www.ibm.com/storage/fasttkeys> でプレミアム・フィーチャー再活動化キー・ファイルを要求できます。最初にプレミアム・フィーチャー・キー・ファイルの生成に使用したのと同じマシン・タイプ、モデル、およびシリアル番号の情報を用意する必要があります。

プレミアム・フィーチャーの使用可能化

プレミアム・フィーチャーを使用可能にするには、ご使用のストレージ・マネージャーのバージョンに該当する手順に従います。

ストレージ・マネージャー 10.x 以降のプレミアム・フィーチャーおよびフィーチャー・パックの使用可能化

ストレージ・マネージャー・バージョン 10.x 以降のプレミアム・フィーチャーを使用可能にするには、以下のステップを完了してください。

1. 「Subsystem Management (サブシステム管理)」ウィンドウで、「Storage Subsystem (ストレージ・サブシステム)」 > 「Premium Features (プレミアム・フィーチャー)」をクリックします。「Premium Features and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウが開きます。
2. リストの中からプレミアム・フィーチャーを使用可能にするには、コントローラー・ファームウェアのバージョンに応じて、「Enable (使用可能)」または「Use key file (キー・ファイルの使用)」をクリックします。プレミアム・フィーチャーを使用可能にするプレミアム・フィーチャー・キー・ファイルを選択できるウィンドウが開きます。画面の指示に従います。
3. 「Premium Features and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウで表示されているプレミアム・フィーチャーのリストを検査することによって、プレミアム・フィーチャーが使用可能になっているかどうかを確認します。
4. 「Close (閉じる)」をクリックして、「Premium Features and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウを閉じます。

フィーチャー・パックの使用可能化

1. 「Premium Feature and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウで「Change (変更)」をクリックします。
2. フィーチャー・パックのキー・ファイルを選択するためのウィンドウが開きます。キー・ファイルを選択して、「OK」をクリックします。
3. 「Feature Pack installed on storage subsystem (ストレージ・サブシステムにインストールされているフィーチャー・パック)」フィールドの内容を検討して、フィーチャー・パックがインストールされているかどうかを確認します。

重要: プレミアム・フィーチャー・パックを使用可能にするには、コントローラーの再始動が必要です。プレミアム・フィーチャー・パックを使用可能にする対象のストレージ・サブシステムが実行中である場合、コントローラーを再始動するためのダウン時間を必ずスケジュールしてください。

プレミアム・フィーチャーの使用不可化

通常のシステムの動作状態では、プレミアム・フィーチャーを使用不可にする必要はありません。ただし、プレミアム・フィーチャーを使用不可にする場合は、キー・ファイルがあるか、またはキー・ファイルを生成するためのプレミアム・フィーチャー・アクティベーション・コードが記載されているプレミアム・フィーチャーのライセンス・カードがあることを確認してください。このキー・ファイルは、後でプレミアム・フィーチャーを再び使用可能にする際に必要になります。

注:

1. 将来、プレミアム・フィーチャーを使用可能にする場合は、そのフィーチャーに対して再びフィーチャー・キー・ファイルを適用する必要があります。
2. フィーチャーを非アクティブにせずに、リモート・ミラー・オプションを使用不可にできます。フィーチャーが使用不可にされているがアクティブである場合、既存のリモート・ミラーですべてのミラーリング操作を実行できます。ただし、フィーチャーが使用不可である場合はリモート・ミラーを新規作成することができません。リモート・ミラー・オプションの活動化について詳しくは、「*IBM System Storage DS Storage Manager Copy Services User's Guide*」を参照するか、またはストレージ・マネージャーのオンライン・ヘルプで『Using the Activate Remote Mirroring Wizard (リモート・ミラーリングの活動化ウィザードの使用)』を参照してください。
3. プレミアム・フィーチャーが使用不可になっている場合は、Web サイトにアクセスして、プレミアム・フィーチャー・オプションを再びアクティブにしてから、このプロセスを繰り返すことができます。

ストレージ・マネージャー 10.x 以降のプレミアム・フィーチャーの使用不可化

ストレージ・マネージャー・バージョン 10.x 以降のプレミアム・フィーチャーを使用不可にするには、以下のステップを完了してください。

1. 「Subsystem Management (サブシステム管理)」ウィンドウで、「Storage Subsystem (ストレージ・サブシステム)」 > 「Premium Features (プレミアム・フィーチャー)」をクリックします。「Premium Features and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウが開きます。
2. 使用不可にするプレミアム・フィーチャーを選択し、「Disable (使用不可化)」をクリックします。

詳しくは、お近くの IBM サービス・プロバイダーにお問い合わせください。

ストレージ・サブシステムのプロファイルを保管する

重要: ストレージ・サブシステムのアレイと論理ドライブを変更したときには常に、ストレージ・サブシステムのプロファイルを保存する必要があります。この保存済みプロファイルには、重大な突発的障害が発生した場合に構成のリカバリーに役立つ、論理的および物理的なディスク構成情報を含む詳細なコントローラー情報が入っています。ストレージ・サブシステムのプロファイルを、同じストレージ・サブシステム上に保存しないようにしてください。

ストレージ・サブシステムのプロファイルを保存するには、「System Management (システム管理)」ウィンドウにサブシステム・プロファイルを表示するメニュー・オプションを選択し、「Storage Subsystem Profile (ストレージ・サブシステム・プロファイル)」ウィンドウが開いたら「Save As (別名保存)」をクリックします。フル・プロファイルを保存するには、「All (すべて)」タブを選択します。さらに、サポート・データを保存するメニュー・オプションを選択して、このストレージ・サブシステムからさまざまなタイプのインベントリ、状況、診断、およびパフォーマンスのデータをすべて収集し、それらを 1 つの圧縮ファイルに保存することもできます。

第 4 章 ストレージの構成

ストレージ・マネージャーがインストールされた後、ストレージ・サブシステムを構成する必要があります。この章の以下のトピックでは、構成に必要な作業について説明します。

- 『ストレージの区画化の概説』
- 62 ページの『タスク・アシスタントの使用』
- 87 ページの『グローバル・ホット・スペア・ドライブの構成』
- 74 ページの『ディスク・ストレージの構成』
- 88 ページの『デフォルト・ホスト・オペレーティング・システムの定義』
- 90 ページの『ホスト・グループの定義』
- 91 ページの『異機種ホストの定義』
- 91 ページの『ホストおよびホスト・ポートの定義』
- 92 ページの『LUN のマッピング』
- 97 ページの『パフォーマンス読み取りキャッシュの使用』

この章の終わり近くにある以下のトピックには、ストレージ・サブシステムの構成に適用される可能性があるオプション情報が記載されています。

- 93 ページの『IBM i の IBMSystem Storage の構成』

注: このセクションは、IBM i オペレーティング・システムを使用するストレージ構成にのみ適用されます。

- 94 ページの『オプションのプレミアム・フィーチャーの構成および使用』

注: このセクションは、プレミアム・フィーチャーを使用するストレージ・サブシステムにのみ適用されます。

- 98 ページの『その他の機能の使用』
- 104 ページの『ストレージ・サブシステムのチューニング』

注: デフォルトでは、ストレージ・マネージャーを開始すると、「Enterprise Management (エンタープライズ管理)」ウィンドウの「**Setup (セットアップ)**」タブが最初にあります。「Enterprise Management (エンタープライズ管理)」ウィンドウの詳しい説明については、13 ページの『「Enterprise Management (エンタープライズ管理)」ウィンドウ』を参照してください。

ストレージの区画化の概説

ストレージ区画を作成する前に、以下の情報に留意してください。

- ストレージ・マネージャーのタスク・アシスタントで「Storage Partitioning (ストレージの区画化)」ウィザードが提供されます。このウィザードを使用して、ホストおよびホスト・ポートを定義し、LUN をストレージ区画にマップできます。ストレージ・サブシステムがコントローラー・ファームウェア 05.xx.xx.xx を実行している場合、このウィザードは使用できません。両方のタイプの手順が、このセクションで文書化されています。
- 以下の手順は、ホストとストレージ・サブシステム・コントローラー間の物理接続を作成済みであり、さらにスイッチ (該当する場合) を接続してゾーニングしてあることを前提としています。これらの接続

が完了していない場合、ストレージ・マネージャーは、以下の手順の実行中に HBA のワールドワイド・ポート名 (WWPN) または iSCSI iqn 名をリストできません。この場合は、91 ページの『ホストおよびホスト・ポートの定義』で説明されている手順の実行中に WWPN を該当フィールドに入力する必要があります。

- ストレージ・サブシステム・レベルでホスト・グループを作成します。デフォルト・グループ・レベルでホスト・グループを作成しないでください。

注: DS4100 または DS4300 構成で区画化を使用可能にしていない場合は、デフォルト・ホスト・グループを使用することができます。

- ホスト内の複数の HBA がストレージ・サブシステムに接続されている場合は、それらのすべての HBA を含む単一のホスト区画を作成します。ホスト・グループ定義は、同じ論理ドライブ・セットを共有するホスト・セットをグループ化するためにのみ使用します。
- クラスタ区画では、すべてのホストが同じストレージを認識できるように、ホスト・グループ・レベルで論理ドライブのマッピングを行います。通常の区画では、ホスト・レベルで論理ドライブのマッピングを実行します。
- ウィザードを使用して DS5300 および DS5100 ストレージ・サブシステムで IBM i LUN のセットアップと割り当てを行うには、IBM i 構成に固有の情報について 93 ページの『IBM i の IBMSystem Storage の構成』を参照してください。

タスク・アシスタントの使用

ストレージ・マネージャーのタスク・アシスタントは、セントラル・ロケーションを提供し、ユーザーは「Enterprise Management (エンタープライズ管理)」ウィンドウおよび「Subsystem Management (サブシステム管理)」ウィンドウからほとんどの共通タスクの実行を選択できます。タスク・アシスタントを使用して、本セクションで説明する多数の手順を完了することができます。

重要: バージョン 7.50 以降のコントローラー・ファームウェアを使用している場合、ストレージ・マネージャーのタスクの説明が、以下のリストにあるタスクとやや異なる場合があります。

「Subsystem Management (サブシステム管理)」ウィンドウでは、「Setup (セットアップ)」タブ (コントローラー・ファームウェアのバージョンによって異なります) のタスク・アシスタントは、以下のタスクへのショートカットで構成されています。

- ストレージ・サブシステムの構成
- ホストの定義
- 新規ストレージ区画の作成
- 追加の論理ドライブのマッピング
- 構成の保存

ストレージ・サブシステムで問題が発生すると、Recovery Guru へのショートカットが表示されます。Recovery Guru を使用して、問題の詳細を確認し、問題を訂正するための解決策を見つけることができます。

重要: バージョン 7.50 以降のコントローラー・ファームウェアを使用している場合、ストレージ・マネージャーからタスク・アシスタントの機能にアクセスする手順がやや異なります。ボタンがなく、タスク・アシスタント用に別個のウィンドウはありません。「Subsystem Management (サブシステム管理)」ウィンドウの「Setup (セットアップ)」タブをクリックして、「Initial Setup Tasks (初期セットアップ・タスク)」ウィンドウの「Task Assistant (タスク・アシスタント)」メニューにアクセスしてください。

注: タスク・アシスタントは、「Subsystem Management (サブシステム管理)」ウィンドウ下部の「**Don't show the task assistant at startup again** (今後、開始時にタスク・アシスタントを表示しない)」チェック・ボックスを選択しない限り、このウィンドウを開くたびに自動的に呼び出されます。

IBM System Storage DS ストレージ・マネージャーによりサポートされるドライブ

DS サブシステムは、ハード・ディスクおよびソリッド・ステート・ディスク・ドライブのメディア・タイプをサポートします。

モデルに応じて、DS サブシステムは以下のディスク・ドライブ・インターフェースのすべてあるいはいくつかをサポートします。

SATA 特定のエンクロージャーでは、SATA ディスク・ドライブは、FC コネクタを使用してドライブをドライブ・スロットに挿入するのに役立つ ATA 変換機構または FC-SATA インターポーザーを必要とします。

注: SATA ドライブおよび ATA 変換機構または FC-SATA インターポーザーは、個別に識別される単一の物として販売されます。

ファイバー・チャネル (FC)

FC ドライブについての特別な要件はありません。

SAS FC ミッドプレーンをもつエンクロージャーの場合、SAS ドライブは、FC コネクタを使用してドライブ・スロットに挿入するのに役立つ FC-SAS インターポーザーを必要とします。このカテゴリには、NL SAS ドライブも含まれます。

注: SAS ドライブおよび FC-SAS インターポーザーは、個別に識別される単一の物として販売され、FC-SAS ドライブとして知られています。

ディスク・ドライブのタイプ間およびインターフェース間の相違に加えて、T10 保護情報 (T10PI) またはフル・ディスク暗号化/自己暗号化 (FDE/SED) 機能といったドライブ機能に関するいくつかの相違があります。サポートされるドライブ・メディア・タイプ、ドライブ・インターフェース、およびドライブ機能の大部分に対して、ドライブ・キャパシティーが使用可能です。DS サブシステムは、すべてのタイプのドライブ・メディアをサポートするわけではありません。特定のストレージ・サブシステムに対して使用可能でありサポートされるドライブのタイプに関する詳細については、**DS サブシステム RFA** を参照してください。特定のストレージ・サブシステムのモデルでサポートされるドライブの FRU パーツ・リストに関する詳細については、DS ストレージ・サブシステムの「取り付け、メンテナンスおよびユーザーのガイド」も参照することができます。サポートされるドライブ・タイプ、ドライブ・インターフェース、およびドライブ機能の要約が、64 ページの表 11 に示されています。

表 11. サポートされるドライブ・タイプ、ドライブ・インターフェース、およびドライブ機能の要約

IBM DS ストレージ・マネージャーによってサポートされるドライブ	ドライブ・インターフェース	T10PI 機能	SED 対応	SED 非対応
ハード・ディスク	SATA	N/A	N/A	N/A
	ファイバー・チャンネル (FC)	はい	はい	はい
		N/A	はい	はい
	NL SAS/SAS	はい	はい	はい
		N/A	はい	はい
ソリッド・ステート・ドライブ	FC	N/A	N/A	はい
	SAS	N/A	N/A	はい

「Subsystem Management (サブシステム管理)」では、コントローラー・ファームウェア・バージョンに応じて、「Physical (物理)」タブまたは「Hardware (ハードウェア)」タブに、特定のエンクロージャー内のさまざまなドライブ・タイプを識別するのに役立つボタンまたはドロップダウン・リストがあります。このボタンをクリックするか、ドロップダウン・リストから選択すると、ボタンの定義に適合するすべてのドライブが「物理ビュー」ペインに強調表示されます。エンクロージャーで、すべてのドライブがボタンの定義に合致していると、ボタンは使用不可になります。

RAID アレイ作成時のドライブ選択規則

以下に記載することは、RAID アレイ用にドライブを選択する際に考慮すべき事柄です。

- RAID アレイは、同じドライブ・インターフェースを使用するドライブのみを使用して作成することができます。

例えば、SATA および SAS ドライブが FC ドライブと同じように動作できるようにするインターポーザーを持っている場合でも、FC、SAS および SATA ドライブを使用して RAID アレイを作成することはできません。また、特定のドライブ・インターフェースを備えているドライブは、異なるドライブ・インターフェースをもつ RAID アレイ内のドライブのスペアとして使用することはできません。

- RAID アレイは、スピン・ハード・ディスク・ドライブとソリッド・ステート・ドライブとの組み合わせを持つことはできません。
- NL-SAS ドライブと SAS ドライブは異なる回転速度で作動するので、NL-SAS ドライブと SAS ドライブを同じ RAID アレイ内で混用しないでください。NL-SAS は 7200 回転/分で作動し、SAS ドライブは 10K または 15K 回転/分で作動します。SAS ドライブと NL-SAS ドライブで構成される RAID アレイでは、障害が起こった SAS ドライブを置き換えるのに NL-SAS を使用し、障害が起こった NL-SAS ドライブを置き換えるのに SAS ドライブを使用することが可能です。
- 同じドライブ・インターフェースをもつ異なる回転速度で作動する複数のドライブを、同じ RAID アレイ内で混用しないでください。ストレージ・マネージャー GUI または SM コマンド行インターフェースは、このような構成を防止しません。適切なドライブがない場合、コントローラー・ファームウェアは、異なる回転速度をもつ使用可能なホット・スペア・ドライブを、障害が起きたドライブのスペアとして選択することがあります。ホット・スペア・ドライブの回転速度が低い場合は、できるだけ早く障害ドライブを交換してください。
- 必要な回転速度のドライブを入手できない場合、IBM では交換用 FRU としてより高い回転速度を持つ類似のドライブを提供することがあります。より高い回転速度のドライブを交換用として使用しても、アレイまたはディスク・プールのパフォーマンスには影響がありません。

- 1 つの RAID アレイ内の T10PI または FDE といった異なる機能のドライブを、(ドライブ機能の内の 1 つが該当の RAID アレイに対して使用可能になっていない場合に限り) 同じ RAID アレイ内でそれらの機能を持っていないドライブと混用することができます。例えば、T10PI がサポートされているドライブと、T10PI がサポートされていないドライブの両方を持つ RAID アレイを作成することができます。ただし、作成されたアレイは、T10PI 機能を使用可能にして作動することはできません。
- 回転速度の小さいドライブは、より大きい回転速度のドライブをもつアレイのスペアとして使用することができます。同じ RAID アレイ内で異なる回転速度のドライブを混用しないことをお勧めします。これは低い回転速度のドライブによって、アレイまたはディスク・プールのパフォーマンスが低下する可能性があるためです。
- 1 つの RAID アレイ内で、異なるサイズのドライブを混用することができます。ただし、アレイは、すべてのドライブが、RAID アレイ内の最小のドライブ・サイズと同じサイズになって作成されます。
- FDE および T10PI のような追加機能が使用可能になっている RAID アレイは、その RAID アレイ内で障害の起こったドライブのスペアとして使用される使用可能機能を備えていないドライブを持つことはできません。例えば、T10PI および FDE が使用可能な RAID アレイは、T10PI および FDE 機能を持っているドライブをホット・スペア・ドライブとして必要とします。
- ディスク・プールは、SAS ディスク・インターフェースを備えたスピン・ハード・ディスクでのみ構成できます。ディスク・プールは、Enhanced FlashCopy、メトロ・ミラーリング、およびグローバル・ミラーリングをサポートしますが、レガシー FlashCopy はサポートしません。1 つのディスク・プール内に、異なる容量および異なるスピンドルのドライブを含めることはできません。
- 2 TB NL-SAS ドライブ (FC#3450、3451) では、T10PI はサポートされません。これらのドライブを Performance Module Controller を搭載した DCS3700 サブシステムで使用している場合、アレイまたはディスク・プールを手動で作成し、T10PI 使用可能化を避ける必要があります。ディスク・プールを手動で作成する場合、「**Disk Pool Automatic Configuration (ディスク・プール自動構成)**」ウィンドウで「**No (いいえ)**」をクリックして、「**Filter drive selection to show T10 PI (T10 Protection Information) capable drives only (T10PI (保護情報) 機能付きドライブのみを表示するようにドライブ選択をフィルターする)**」チェック・ボックスをクリアします。アレイに T10PI 対応の論理ドライブを作成するには、すべてのドライブを T10PI 対応にする必要があります。

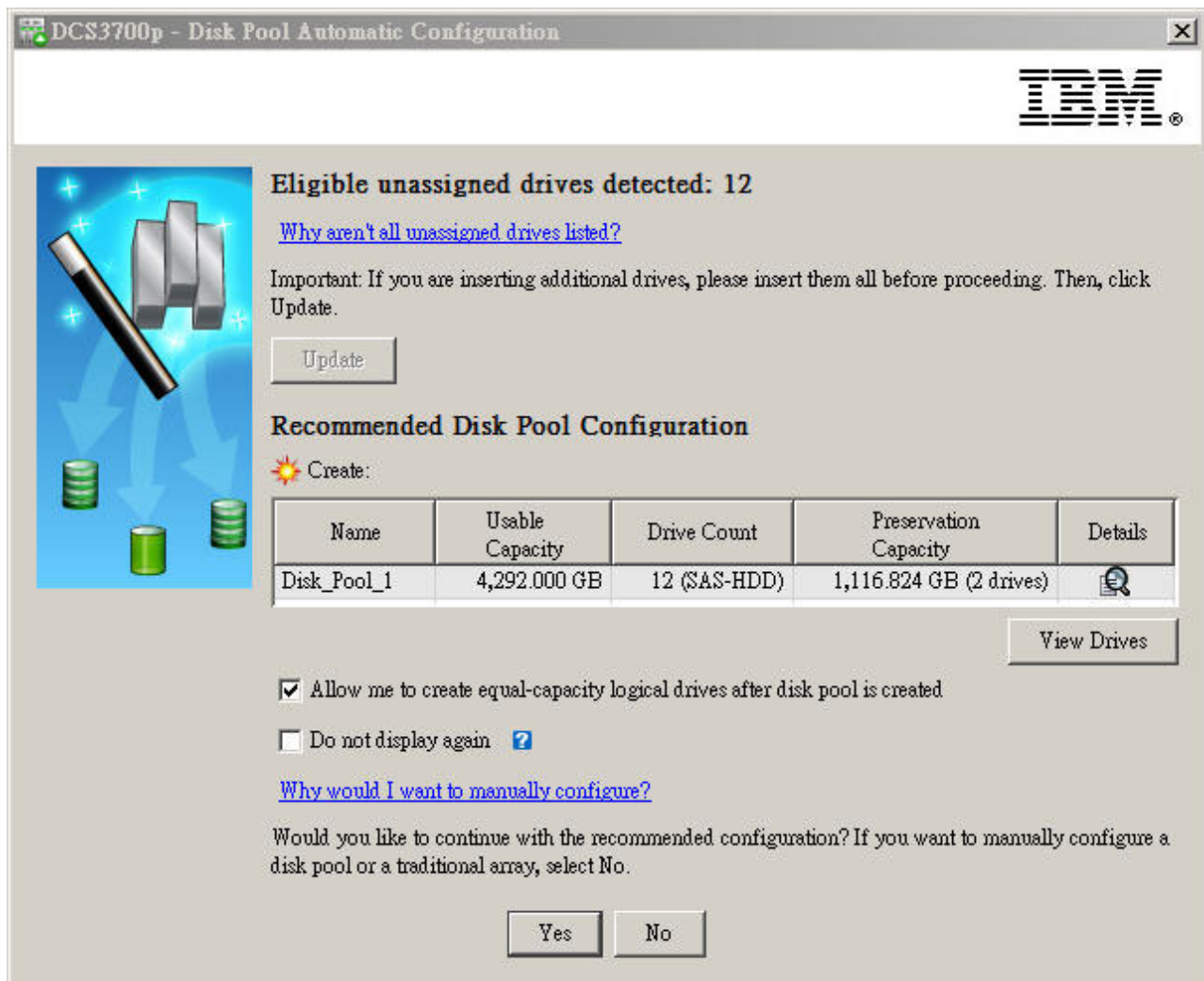


図 3. ディスク・プール自動構成

ソリッド・ステート・ドライブ (SSD) 属性

ソリッド・ステート・ドライブは、回転するハード・ディスク面ではなしにフラッシュ・メモリー・チップにデータを保管するドライブであり、結果としてハード・ディスク・ドライブよりも速いランダム・アクセス書き込み/読み取り速度が得られます。

フラッシュ・デバイスには特定の書き込みサイクル数の制限があるため、これらのドライブには、ドライブ保証期間中の書き込みサイクル使用をサポートする追加のスペア・フラッシュ・メモリー・チップが含まれています。は、SSD ディスク・ドライブおよび SSD ドライブ内の残余のスペア・ブロックの比率を示しています。SSD は、コントローラー・ファームウェア・バージョン 7.60.xx.xx 以降でサポートされます。その理由は、このバージョンが、SSD ドライブで構成される RAID アレイ内の論理ドライブのメディア・スキャンをサポートしているからです。ただし、コントローラー・ファームウェア・バージョン 7.77.xx.xx 以降をお勧めします。

コントローラー・ファームウェア バージョン 7.8x.xx.xx 以降を搭載したサブシステムの場合、DS5100/5300 および DS5020 ストレージ・サブシステムでは、所定のストレージ・サブシステム構成で最

大 20 個の SSD ドライブを持つことができます。DS3500 と DCS3700 ストレージ・サブシステム、および Performance Module Controller 搭載の DCS3700 ストレージ・サブシステムでは、最大 24 個のドライブを持つことができます。また、DS5100/5300 サブシステムの場合は、ドライブ拡張エンクロージャー当たり 4 個を超える SSD を含めてはならず、できるだけ多くの異なるドライブ・チャンネル上のドライブ・エンクロージャー間に SSD を分散させる必要があります。これは、ストレージ・サブシステムの最適のパフォーマンスを確保するために必要です。

T10PI 対応ドライブ属性

T10PI 対応ドライブは、SCSI プロトコルに関して指定された業界標準の拡張 T10 保護情報 (T10 PI または T10PI) をサポートします。T10PI 標準は、T10 DIF (Data Integrity Field) と呼ばれることもあります。

この標準は、ストレージ・コントローラーと T10PI 初期化ディスク・ドライブ間でデータが転送されるときに、8 バイトの保全性メタデータを持つ各ユーザー・データ・ブロックを保護することによって、追加レベルのデータ保全性を提供するように設計されています。この追加レベルのデータ保全性は、ストレージ・サブシステムが AIX オペレーティング・システムを稼働させている IBM Power サーバーへ入出力接続している場合に、サーバーへも拡張されます。AIX オペレーティング・システム内の T10 PI サポートには、AIX サーバーとストレージ・コントローラー間で転送されるユーザー・データに伴う保護情報メタデータが含まれます。T10PI 標準は、エンドツーエンド保護、およびサイレント・データ破損 (デバイス・ドライバー・エラー、ファイル・システム・エラーまたは宛先誤りの書き込み、失われた書き込み、ファントム書き込み、あるいは分割書き込みに起因) に対する修正を、ユーザーに提供するように設計されています。

T10PI 対応ドライブは、タイプ 2 T10PI ドライブとして初期化されます。これらのドライブは、標準の 512 バイトのセクターではなしに 520 バイトのセクターを持っています。追加の 8 バイトには、表 12 で説明されている、伝送途中のデータまたは静止しているデータを検証するのに使用できる保護情報メタデータが含まれています。

表 12. 保護情報メタデータ (8 バイト)

バイト #1	バイト #2	バイト #3	バイト #4	バイト #5	バイト #6	バイト #7	バイト #8
論理ブロック・ガード (2 バイト)		論理ブロック・アプリケーション・タグ (2 バイト)		論理ブロック参照タグ (4 バイト)			
16 ビット CRC - 受信側は、受信したデータの CRC を計算し、受信した CRC と比較します。 - セクターのデータ部分を保護します。		- アプリケーション・クライアント (イニシエーター) またはデバイス・サーバー (ターゲット) が所有することが可能 - 所有者によってのみチェックされます		- 受信側はオプションで期待した値と突き合わせてチェックします - 順序が正しくない書き込み、および宛先誤りの書き込みを防止するというシナリオ			

DS ストレージ・サブシステムは、T10PI タイプ 1 ホスト保護方式をサポートします。68 ページの図 4 は、ホストのアプリケーションからストレージ・サブシステムのドライブまでの間で保護情報メタデータがチェックされる個所を示しています。

Protection Information (PI) Check Points

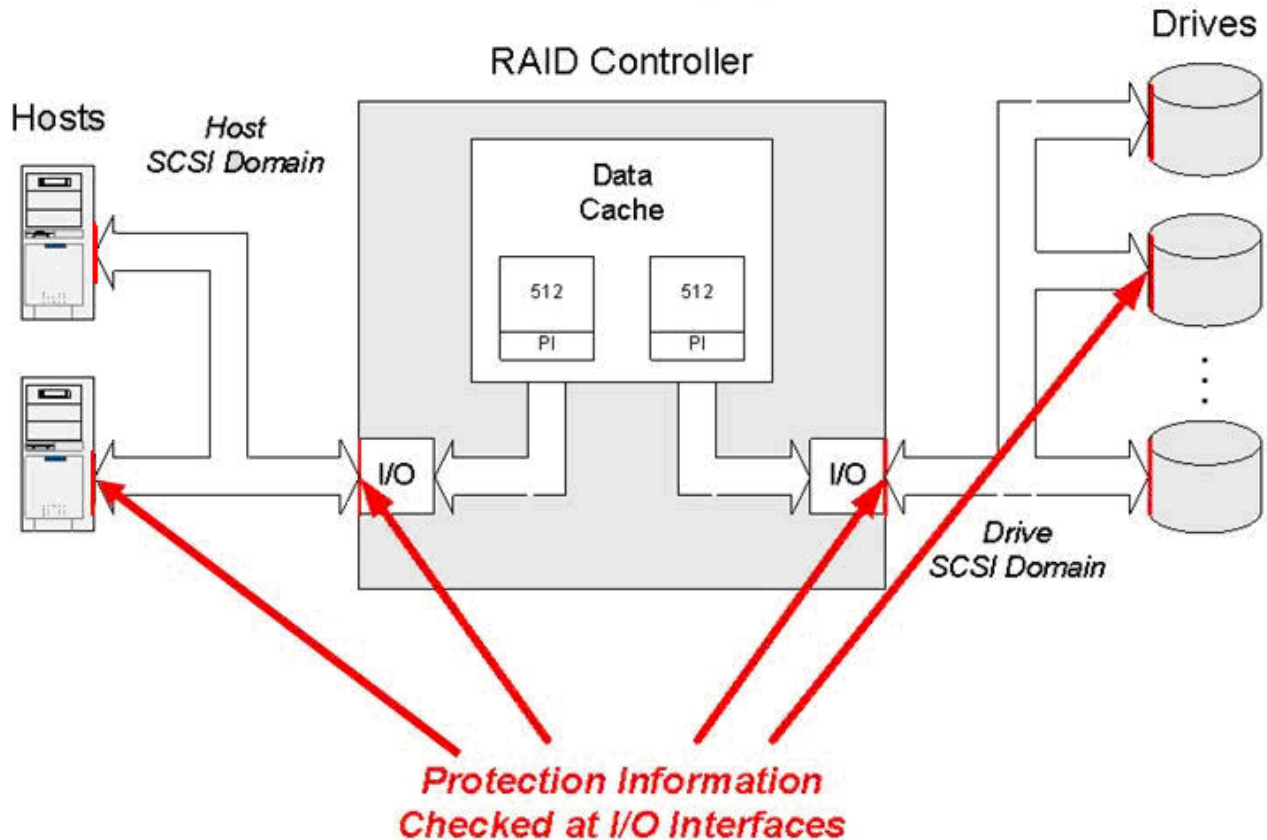


図 4. 保護情報 (P) チェック箇所

T10PI 機能の使用可能化の規則

DS ストレージ・サブシステムで T10PI 機能を使用可能にするには、以下の条件を満たしている必要があります。

T10PI 機能がサポートされるコントローラー・ファームウェア

T10PI 機能は、プレミアム・フィーチャーではなしにコントローラー・ファームウェアによって使用可能にされます。T10PI をサポートするコントローラー・ファームウェアは 7.77.xx.xx 以降です。現在、DS3950、DS5020、DCS3700、および DS5100/DS5300 サブシステムのみが、T10PI をサポートします。Performance Module Controller を装備した DCS3700 ストレージ・サブシステムは、コントローラー・ファームウェア・バージョンが 7.83.xx.xx 以降の場合、T10PI をサポートします。他の DS ストレージ・サブシステムにおける将来の T10PI のサポートについては、IBM 販売店またはサービス担当員にお問い合わせください。

注: T10PI ドライブは、T10PI 機能をサポートしないコントローラー・ファームウェアを持つストレージ・サブシステムで使用することができます。そのような場合、T10PI ドライブは T10PI 非対応ドライブとして扱われます。

ファイバー・チャンネル・ホスト・インターフェース

ファイバー・チャンネル・ホスト・インターフェースは DS ストレージ・サブシステムにインストールする必要があります。さらに、T10PI 使用可能論理ドライブは、DS ストレージ・サブシステム

のファイバー・チャンネル・ポートを介してディスカバーされたホスト・ポートにマッピングされる必要があります。例えば、コントローラーに FC、iSCSI、または SAS ホスト・インターフェースが同時にインストールされている場合、T10PI 使用可能論理ドライブは、FC ポートのみを介してディスカバーされたホスト・ポートにマッピングできます。iSCSI または SAS インターフェースを介してディスカバーされたホスト・ポートに T10PI 使用可能論理ドライブをマッピングしようとすると、エラーが発生します。

(AIX サーバーの場合) T10PI 使用可能ホスト・タイプの NVSRAM ファイル

コントローラー・ファームウェア・バージョン 7.77.xx.xx 以降に提供された NVSRAM ファイルを、ストレージ・サブシステムにインストールする必要があります。これらの NVSRAM ファイルは、T10PI 使用可能ビットを、AIX および AIXAVT ホスト・タイプ領域に設定して、T10PI 機能をサーバーに拡張します。このビットがホスト・タイプ領域に設定されていないと、T10PI 機能はサブシステム・コントローラーとドライブの間でのみ使用可能になります。

注: 必要なデバイス・ドライバー、ファームウェア・バージョン、およびサーバーで T10PI サポートを提供する AIX オペレーティング・システムのバージョンならびにサポートされる FC アダプターのタイプに関する情報については、SSIC を参照してください。

T10PI 対応のアレイの作成

T10PI 対応のアレイを作成する前に、以下の手順を完了します。

1. 「**Total Unconfigured Capacity (未構成容量の合計)**」をクリックします。「**Create Array (アレイの作成)**」ウィンドウが開きます。
2. ドライブのタイプを複数使用している場合、「**Drive type (ドライブ・タイプ)**」の「**HDD-SAS**」を選択します。
3. 「**Filter drive selection to show T10 PI (Protection Information) capable drives only (T10PI (保護情報) 機能付きドライブのみを表示するようにドライブ選択をフィルターする)**」チェック・ボックスを選択します。
4. 81 ページの『アレイの作成』に進みます。

T10PI 対応ディスク・プールの作成

T10PI 対応のディスク・プールを作成する前に、以下の手順を完了します。

1. 「**Total Unconfigured Capacity (未構成容量の合計)**」をクリックします。
2. ドライブのタイプを複数使用している場合、「**Drive type (ドライブ・タイプ)**」の「**HDD-SAS**」を選択します。
3. 「**Data assurance (データ保障)**」の「**Only T10 PI-capable drives (T10PI 対応ドライブのみ)**」を選択します。
4. 79 ページの『ディスク・プールの作成』に進みます。

T10PI 対応 RAID アレイの使用可能化および使用不可化

T10PI 対応 RAID アレイを作成するためには、RAID アレイ内のすべてのドライブが T10PI 対応でなければなりません。

このタスクでは、アレイを定義するためにサブシステム管理インターフェースを使用していることを前提にしています。

RAID アレイ上で T10PI 機能を使用可能にするには、次のようにします。

注: このセクションに記載するスクリーン・ショットは説明のみを目的としており、ストレージ・マネージャーおよびコントローラー・ファームウェアのバージョンによっては、実際の UI と異なる場合があります。

- 図 5 に示されているように、「Specify Capacity/Name (Create Logical Drive) (キャパシティー/名前の指定 (論理ドライブ作成))」ダイアログで、「**Enable T10 PI (Protection Information) (T10 PI) on the new logical drive (新規論理ドライブでの T10 PI (保護情報) (T10 PI) の使用可能化)**」をクリックします。

注: T10PI 機能を持っていない論理ドライブを作成すると、それを後で T10PI 対応の論理ドライブに変換することはできません。

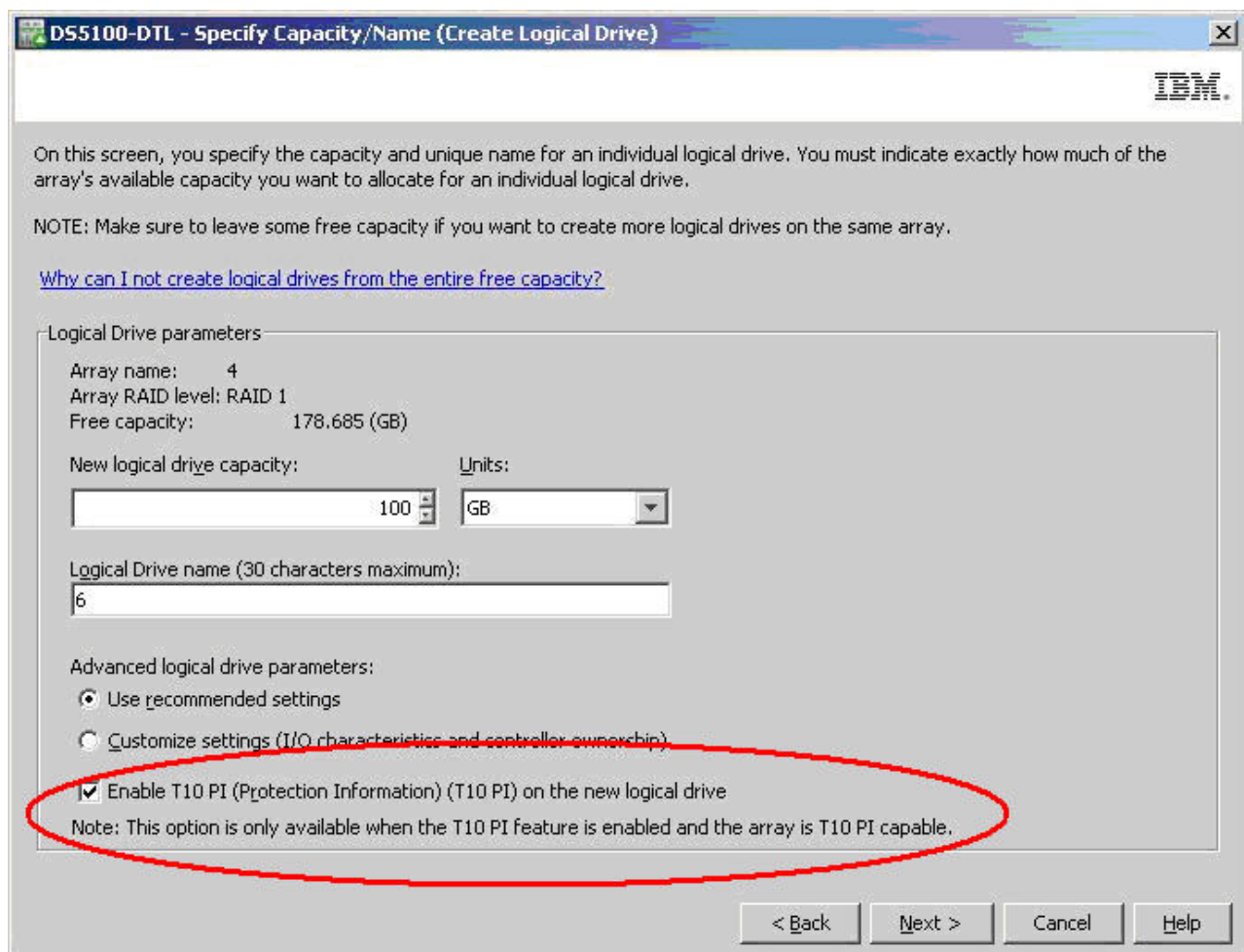


図 5. 論理ドライブ上での T10 PI の使用可能化

注: 論理ドライブが T10PI を使用可能にして作成されるかどうかを示すために、該当する SMcli コマンドで使用する追加のパラメーターも存在します。

71 ページの図 6 は、T10PI 機能を使用可能にした RAID アレイとその論理ドライブを示しています。シールド・アイコンは、アレイが T10PI 対応 RAID アレイであることを示しています。

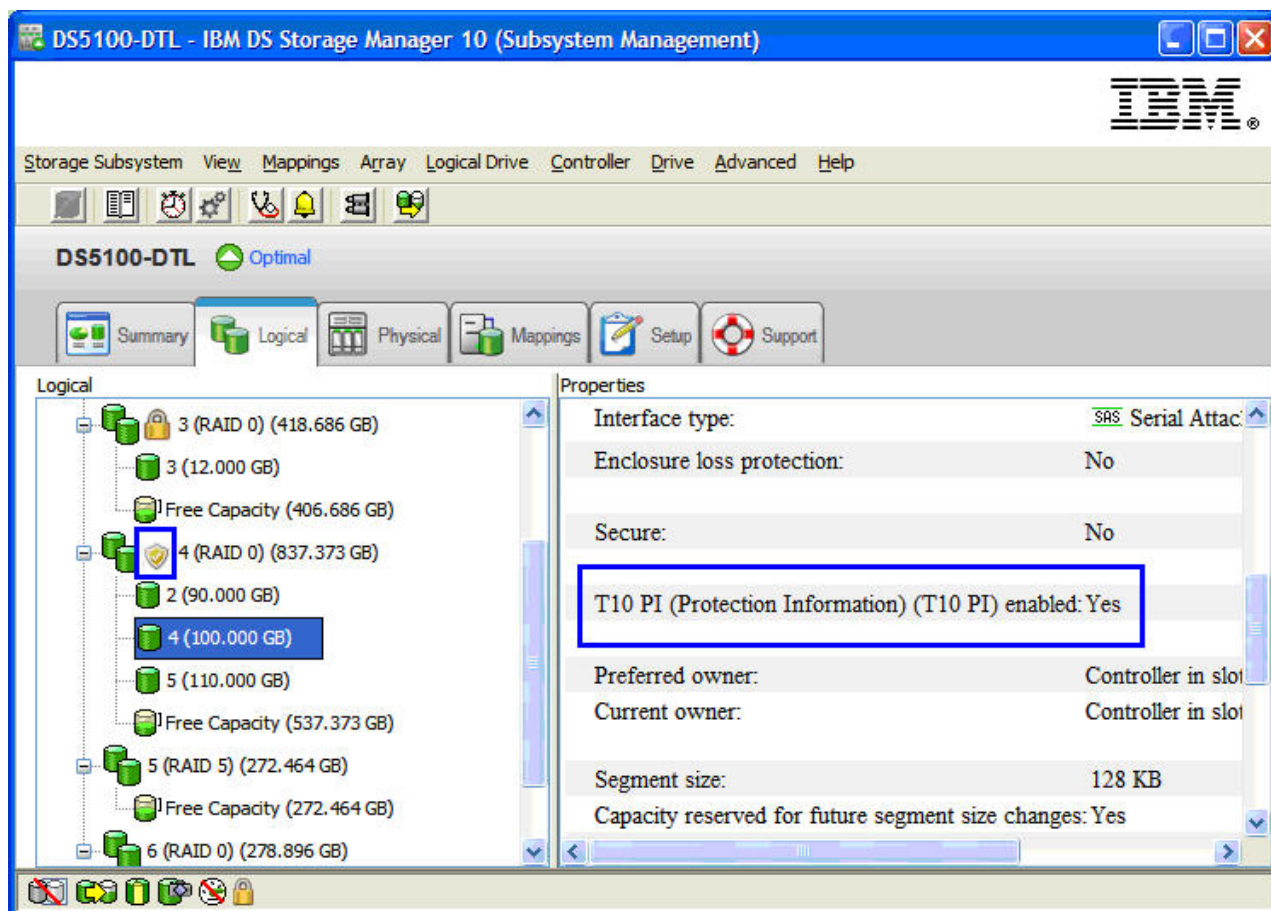


図 6. RAID ドライブ - 保護情報 (T10 PI) - 使用可能

注: T10PI 使用可能 RAID アレイ内のすべての論理ドライブを、T10PI を使用可能にして作成する必要はありません。例えば、72 ページの図 7 に示すように、RAID アレイ 4 の論理ドライブ 4 は T10PI 使用可能ではないが、論理ドライブ 2 および 5 は T10PI 使用可能です。ただし、T10PI 機能を使用可能にできるのはドライブ作成時のみなので、論理ドライブを T10PI 使用可能にして作成しておき、必要であれば後になってそれを使用不可にすることをお勧めします。

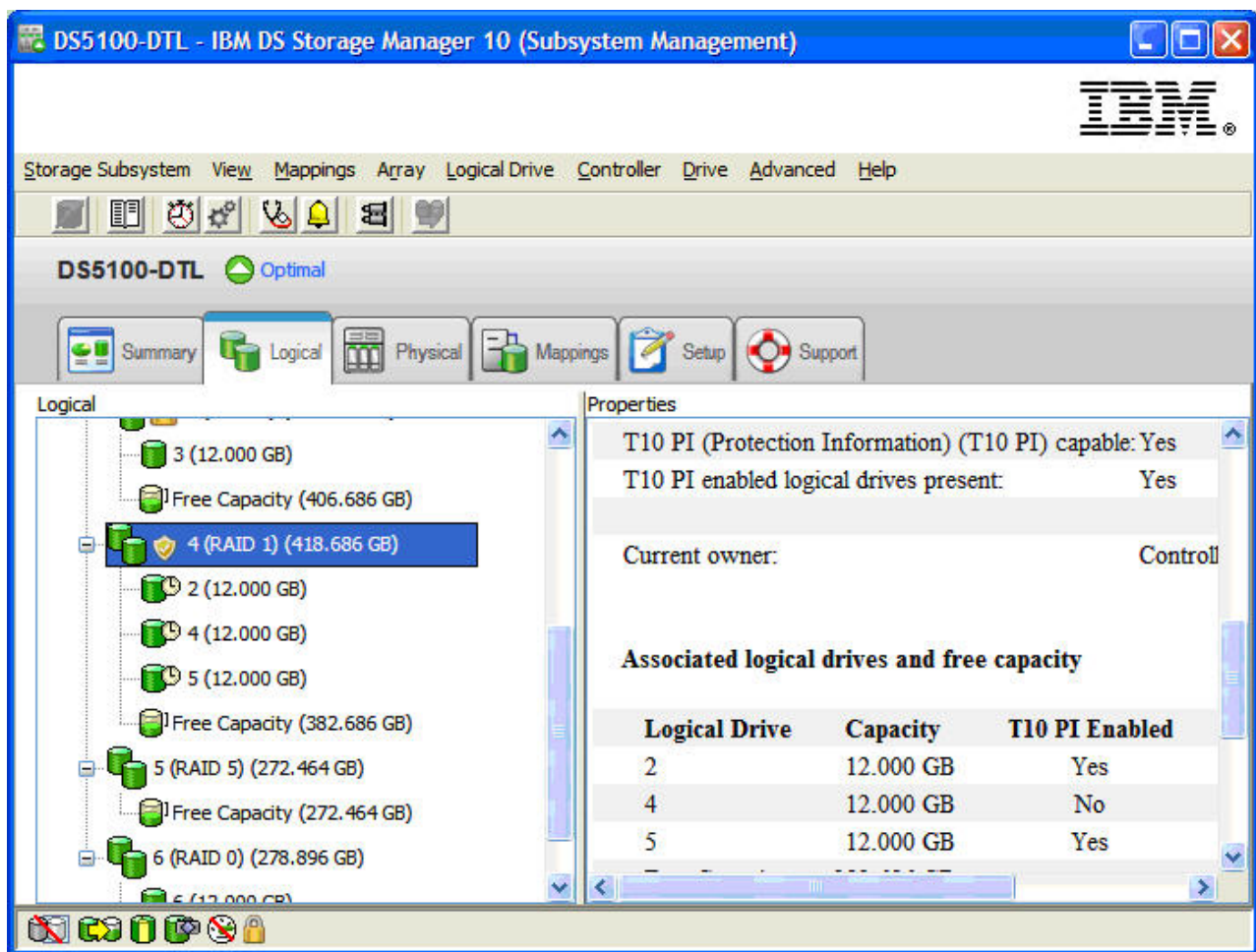


図7. 例 - RAID アレイ 4 の論理ドライブ 4 - T10PI 使用不可

RAID アレイの T10PI 機能を使用不可にするには、次のようにします。

- 73 ページの図 8 に示されているように、T10PI 機能を使用不可にしようとしているドライブを右クリックして、「**Disable T10PI (Protection Information) (T10PI) (T10PI 使用不可 (保護情報) (T10PI))**」を選択します。

注:

- また、T10PI 機能を使用不可にする SMcli コマンドもあります。
- 論理ドライブの T10PI 機能を使用不可にした場合、同じ論理ドライブで T10PI を単純に使用可能にすることはできません。ドライブを削除してから、T10PI を使用可能にしてドライブを再作成する必要があります。

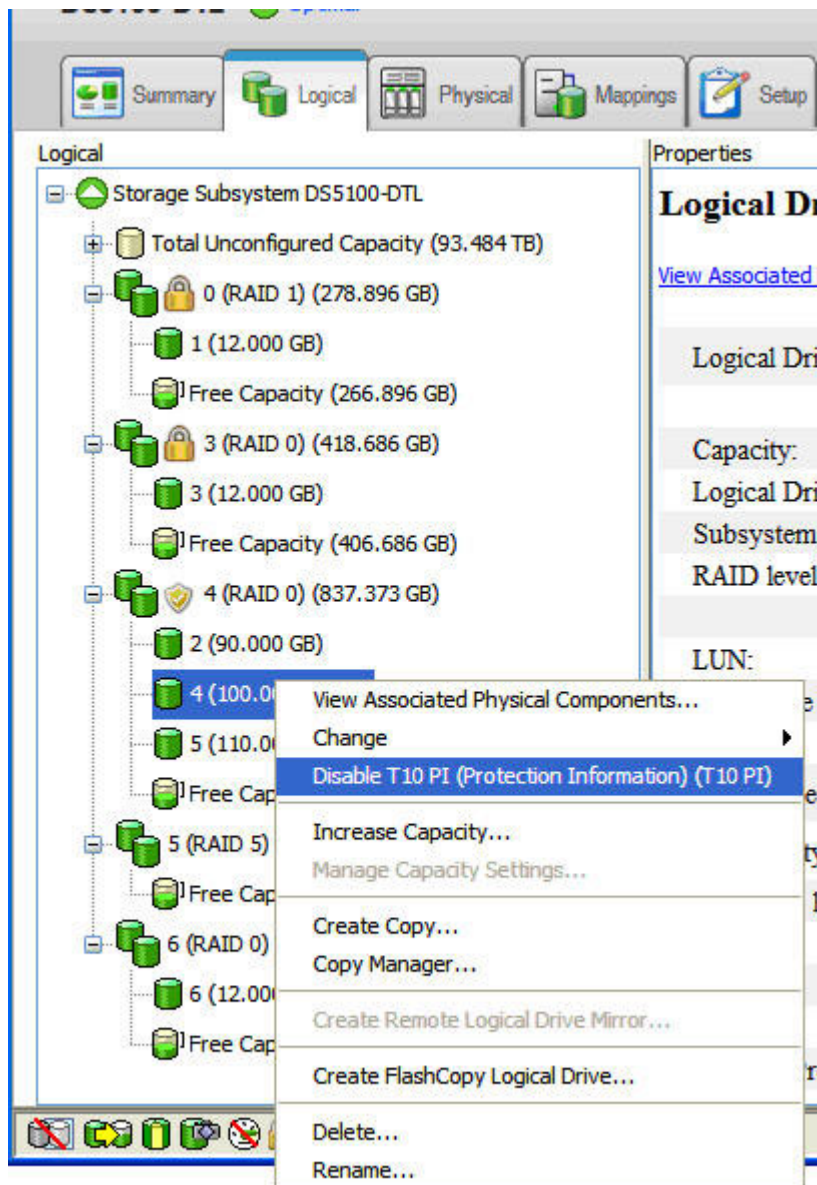


図 8. T10PI の使用不可化

フル・ディスク暗号化 (FDE) 属性

フル・ディスク暗号化 (FDE) または自己暗号化 (SED) ドライブは、DS ストレージ・サブシステムの外部からの無許可アクセスからドライブ情報を保護するための組み込み暗号化メカニズムを備えています。

保護された FDE/SED ドライブは、電源にスイッチが入れると、ロックされます。コントローラーからドライブへ該当するセキュリティ・キーを送信することによって、ドライブをアンロックします。セキュリティ・キーの管理は、コントローラーの内部でローカルに行うか、または IBM Tivoli Key Lifecycle Manager (TKLM) といった外部のキー・マネージャーによって行います。追加のセキュリティについては、ドライブはそれを書き出される前に暗号化して、ドライブに障害が起こったときまたはドライブがアクティブに使用されなくなったときにディスク面上のデータがスキャンされるのを防止します。図 10 に示さ

れているように、FDE 対応 RAID アレイ/ディスク・プールは、アレイ/ディスク・プールが保護されていない場合はアンロック・アイコンで表示され、アレイ/ディスク・プールが保護されている場合は、ロック・アイコンで表示されます。FDE ドライブに関する詳細については、205 ページの『第 6 章 フル・ディスク暗号化の処理』を参照してください。

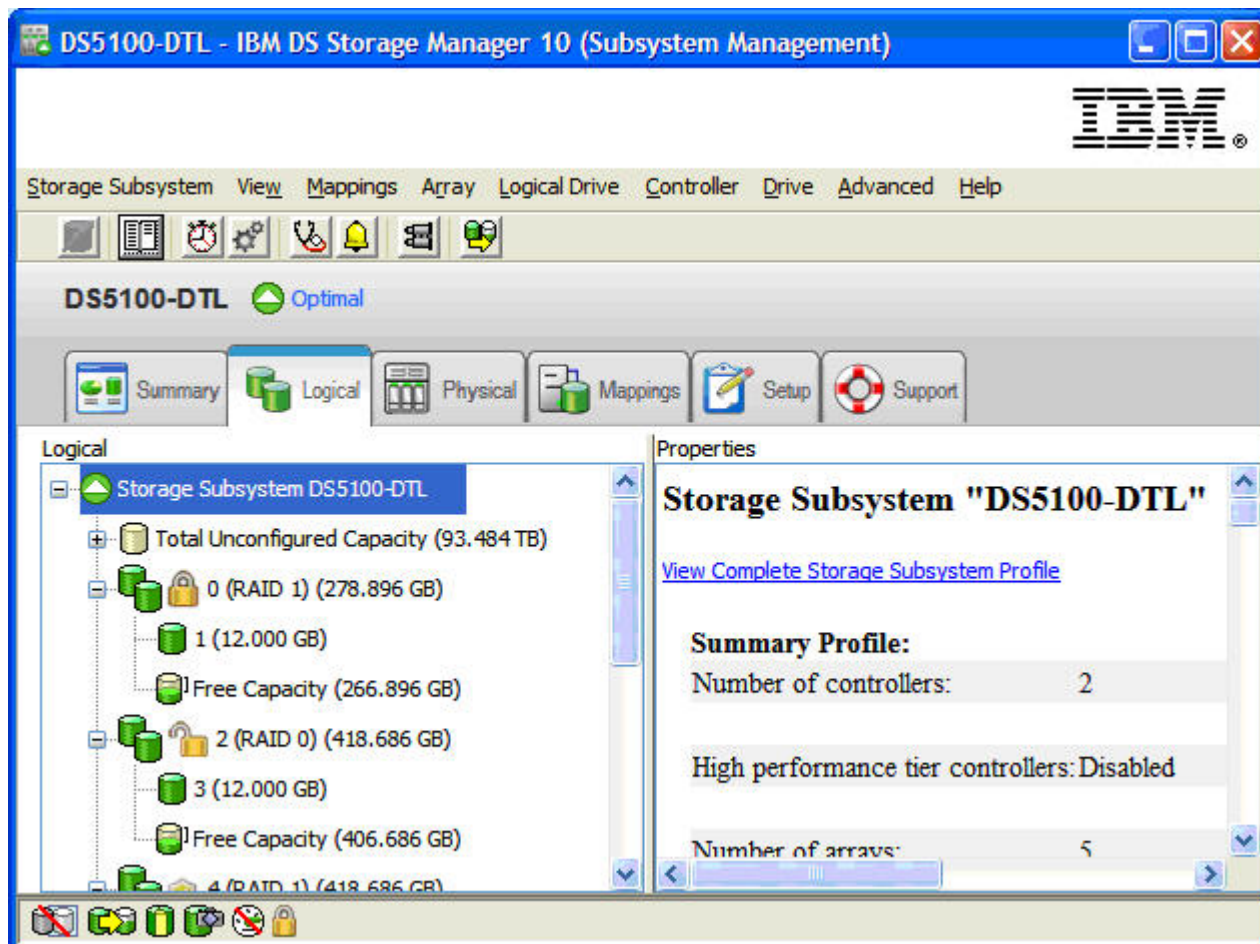


図 9. FDE 対応 RAID アレイ - セキュリティーの詳細

ディスク・ストレージの構成

IBM DS ストレージ・マネージャー バージョン 10.83 をコントローラー・ファームウェア・バージョン 7.83 と共に使用すると、ディスク・プール、アレイ、またはその両方にドライブの集合を構成できます。ディスク・プールまたはアレイには、同じ特性または類似した特定を持つドライブが入れられます。類似したドライブを判別するために使用される特性には、以下のものがあります。

- **ドライブ・タイプ** — アレイ用にサポートされるドライブのタイプは、ファイバー・チャネル、SATA、FC-SAS、または SAS です。ディスク・プールは、SAS ドライブのみで構成できます。
- **ドライブ・メディア・タイプ** — アレイ用にサポートされるドライブ・メディアは、ハード・ディスク (HDD) またはソリッド・ステート・ディスク (SSD) です。ディスク・プールには、SAS HDD ドライブのみを入れることができます。ディスク・プールでは、SAS SSD ドライブはサポートされません。

表 13. アレイおよびディスク・プールに使用できるドライブのタイプ

ドライブ・タイプ	アレイ	ディスク・プール
SAS ディスク	はい	はい
SAS ディスク - T10PI	はい	はい
SAS ディスク - SED	はい	はい
SATA ディスク	はい	はい
FC ディスク	はい	なし
FC ディスク - SED	はい	なし
FC-SAS ディスク	はい	なし
SSD	はい	なし

- **回転速度** — 1 つのディスク・プールまたはアレイ内のドライブの回転速度は同じでなければなりません。異なる回転速度のドライブを持つアレイまたはディスク・プールを作成することは可能ですが、そのような構成は最適ではありません。

注: ストレージ・マネージャー・ユーザー・インターフェースからは、回転速度が異なるドライブを持つディスク・プールを作成することはできません。回転速度が異なるドライブで構成されたディスク・プールを作成するには、SMCLI コマンドを使用する必要があります。

- **セキュリティ・レベル** — ディスク・プール全体またはアレイ全体を指定のセキュリティ・レベルで保護する場合は、すべてのドライブのドライブ・セキュリティが同じである必要があります。
- **容量** — ディスク・プールまたはアレイ内のドライブを効率的に使用するには、それらのドライブの容量を同じにする必要があります。ディスク・プールまたはアレイ内のドライブの容量が異なっている場合、ストレージ管理ソフトウェアは、ディスク・プールまたはアレイ内の最小のドライブの容量と同じ容量のみを使用します。例えば、ディスク・プールがいくつかの 4 GB ドライブと 8 GB ドライブで構成されている場合、DS ストレージ・マネージャーは各ドライブで最大 4 GB のみ使用し、8 GB ドライブの 4 GB は未使用のまま残されます。

アレイ はファイバー・チャネル、SAS、SATA、またはソリッド・ステート・ドライブの集合であり、論理的に一緒にグループ化されて RAID を形成します。ストレージ・システムには、必要に応じて、異なる RAID 特性 (RAID レベル、セグメント・サイズ、およびストライプ幅) を持つ異なるアレイを作成できます。アレイは、標準またはセキュア (フル・ディスク暗号化を使用) のいずれかです。

ディスク・プール は、ストレージ・サブシステム内の SAS ディスクを論理ディスク装置に編成して、それらのディスクをホストに示す代替方式です。ディスク・プールは、標準またはセキュア (フル・ディスク暗号化を使用) のいずれかです。IBM DS ストレージ・マネージャー バージョン 10.83 をコントローラー・ファームウェア・バージョン 7.83 と共に使用すると、ディスク・プール、アレイ、またはその両方にドライブの集合を構成できます。コントローラー・ファームウェア・バージョンが 7.83 以降の場合、ディスク・プールをサポートするストレージ・サブシステムは、現行では DS3500 と DCS3700、および Performance Module Controller 搭載の DCS3700 です。

表 14. アレイおよびディスク・プールでサポートされるコピー・サービス

コピー・サービス	アレイ	ディスク・プール
FlashCopy 論理ドライブ	はい	なし
Enhanced FlashCopy	はい	はい
VolumeCopy	はい	はい
リモート・ミラーリング	はい	はい
グローバル・ミラー	はい	はい

ディスク・プールとアレイの比較

ディスク・プールは、多くの点でアレイと異なります。

RAID 保護 - アレイは、RAID レベル 0、1、10、3、5、または 6 のいずれかを使用して作成できます。データ・セグメントとパリティ・セグメントは RAID レベルの定義に従ってドライブ間にストライピングされます。表 14 には、アレイ用に選択する必要がある RAID レベルについての情報が記載されています。アレイ内では、RAID ストライプは RAID アレイの一部である各ドライブ内の 1 セグメントをカバーします。RAID アレイの LBA とアレイ内のディスク上のデータの物理位置の間には、ほぼ直接の関係があります。

ディスク・プールには RAID レベルを指定できません。ディスク・プールは、4 GB チャンク (D チャンクと呼ばれる) のディスク・スペースに分割されています。各 D チャンクは、512 MB の断片 (D 断片と呼ばれる) 10 個で構成されます。D チャンクの 10 個の D 断片は、10 台の異なるディスクに書き込まなければなりません。それが不可能な場合、ディスク・プールは機能低下するか (10 個の断片のいずれかを個別のディスクに書き込めない場合)、または障害が起こります (10 個の断片のうちの 2 つ以上を個別のディスクに書き込めない場合)。各 D 断片は、4096 個のセグメントで構成され、1 つのセグメントは 128 KB です。10 個の D 断片のそれぞれからの 1 セグメントが RAID 6 8D+P+Q ストライプを形成します。言い換えると、4 GB の D チャンク内で、データと RAID パリティが 4096 個の 8D+P+Q RAID-6 ストライプに保管されます。データは、RAID ストライプおよび D チャンクと隣接して保管されます。ディスク・プール内の論理ドライブは、1 つ以上の 4 GB チャンクのディスク・スペースで作成されます。ディスク・プール内に 11 台を超えるディスクがある場合、データは 4 GB チャンクの倍数として、すべてのドライブに分散されます。ディスク・ドライブ間の D チャンクの割り振りパターンにより、ディスク・プールの LBA とディスク上のデータの物理位置の間には明確な直接的関係はありません。ディスク・プール上のドライブ数が多いほど、データはドライブ間により広く分散されます。

RAID アレイ特性 - アレイの作成時に、アレイ内のドライブの数、RAID レベル、および各ドライブ内のデータのセグメント・サイズに応じて、RAID ストライプをどのようにするかを決めることができます。一部のアプリケーションでは、セグメント・サイズおよび RAID ストライプ幅を調整して、特定の RAID ストライプを持つアレイを作成することができます。これにより、コントローラーのフルストライプ書き込み機能が使用可能になり、その結果、書き込みパフォーマンスが向上することがあります。ただし、現行の実装のディスク・プールでは、セグメント・サイズおよび RAID ストライプ幅の特性を調整することはできません。ディスク・プールは、所定の最小ドライブ数 11 台を超えるドライブで作成できます。ただし、ドライブ間に分散される RAID データは、常にセグメント・サイズ 128 KB の RAID 6 8D+P+Q の RAID 特性を持ちます。

ホット・スワッピング - ドライブ障害が起こった場合、アレイではアレイの再構成のために専用のグローバル・ホット・スペアを使用します。一方、ディスク・プールでは、各ドライブの一定の割合がディスク・プールの再構成用に予約されています。77 ページの表 15 には、各種ディスク・プール・サイズについて、予約済みドライブ容量に相当するドライブ数が示されています。再構成用の予約容量にはホット・スペアに比べて、以下のような利点があります。

1. **再構成時間の改善** - ディスク・プール内の各ドライブが再構成済みデータ用の予約容量を持っているため、ディスク・プール内のすべてのドライブを再構成データの書き込みに使用できます。アレイおよびホット・スペア・ドライブの場合、再構成済みデータの書き込みに使用できるドライブは 1 台のみであるため、再構成プロセスでのボトルネックの原因になります。
2. **スタンバイ状態のドライブがない。** ディスク・プッター損傷の増大などのハードウェア欠陥やドライブが非活動状態であるために、再構成中にホット・スペア・ドライブに障害が起きるという事例がこれ

までに起きています。ディスク・プールでは、どのドライブも再構成済みデータ専用にしなないことにより、すべてのドライブをどの時点でも使用できます。

3. コピー・バック時間の改善 障害の起きたドライブの交換時には、すべてのドライブがコピーバック処理に参加するため、コピーバック時間も幾分改善されます。ディスク・プールでは、再構成済みセグメントがさまざまなドライブから取り出され、複数の交換ドライブに書き込まれます。アレイでは、再構成済みデータが 1 台のドライブから取り出され、該当する 1 台の交換済みドライブにコピーバックされます。

表 15. ディスク・プールの予約済み容量

ディスク・プールのドライブ数	予約済みドライブ数
11	1
12-31	2
32-63	3
64-127	4
128-191	6
192	7

ストレージ効率 - アレイが複数の論理ドライブに分割されている場合、各論理ドライブにアレイの一定のスライスが割り当てられます。一部の論理ドライブに未使用の容量があっても、その容量を別の論理ドライブの追加容量として使用したり、新しい論理ドライブの作成に使用したりすることはできません。ディスク・プール内の論理ドライブはまとめて管理されます。論理ドライブごとに固定された容量の割り振りは行われません。したがって、論理ドライブはディスク・プールの自身の割り当て分を使用し、ディスク・プールの未使用の容量全体を、ディスク・プール内の容量を必要とする他の論理ドライブに提供したり、追加の論理ドライブ作成のために提供したりすることができます。アレイが複数の論理ドライブに分割される場合、各論理ドライブはアレイの一定部分を占有します。論理ドライブのサイズは、アレイ内に使用可能なスペースがあれば、必要に応じて増やすことができます。しかし、論理ドライブ内の未使用容量を解放して、アレイ内の新しい論理ドライブの作成に使用したり、別の論理ドライブの追加容量として使用したりすることはできません。既存の論理ドライブ内のスペースを解放する唯一の方法は、論理ドライブ内のデータのバックアップをとり、その論理ドライブを削除し、より小さい容量で論理ドライブを再作成して、その小さい論理ドライブにバックアップ・データをリストアするという方法です。ディスク・プールを複数の論理ドライブに分割する場合、論理ドライブをシン論理ドライブとして作成することができます。シン論理ドライブは、論理ドライブの作成時にディスク・プールのハード・ディスク上に物理的に割り振られた論理ドライブ・スペースの一部分のみを使用します。論理ドライブに物理スペースがさらに必要になると、その論理ドライブにはディスク・プールの空き容量から追加スペースが 4 GB D チャンク単位で割り振られ、論理ドライブに未使用の空き容量がないように適切にプロビジョンされます。

表 16. アレイまたはディスク・プールでサポートされる機能のリスト

フィーチャー	アレイ	ディスク・プール
エンクロージャー破損保護	はい ¹	はい ²
ドロー破損保護	はい ¹	はい ²
動的論理ドライブ拡張	はい	はい
動的アレイ/ディスク・プール拡張	はい	はい
シン・プロビジョニング	なし	はい

注:

1. エンクロージャーまたはドロワー破損保護用のアレイのドライブの最大数は、アレイの RAID レベルによって異なります。RAID 1、10、3、および 5 アレイの場合、エンクロージャーまたはドロワー破損保護のために、エンクロージャーまたはドロワー当たり 1 つのドライブです。RAID 6 アレイの場合は、エンクロージャーまたはドロワー当たり 2 つのドライブが必要です。
2. エンクロージャーまたはドロワー破損保護のために必要な、エンクロージャーまたはドロワー当たりのディスク・プールのドライブの最大数は、2 ドライブです。

論理ドライブ

ディスク・プールまたはアレイの内部で、ドライブはさらに論理ドライブに編成されます。論理ドライブとは、ホストがストレージ・サブシステム上のデータ・ストレージを編成するために使用する論理コンポーネントです。データはディスク・プール内またはアレイ内の複数の物理ドライブにわたって書き込まれますが、ホスト・オペレーティング・システムは論理ドライブを単一ドライブと見なします。各論理ドライブはそれぞれ論理装置番号 (LUN) にマップされ、ホストはこの番号を使用して論理ドライブにアクセスします。ストレージ・サブシステムに接続されたホストは、論理ドライブにデータを書き込み、論理ドライブからデータを読み取ります。論理ドライブは、複数のディスク・プールまたはアレイにまたがることはできません。ディスク・プールまたはアレイは、必要に応じて、ディスク・プールまたはアレイ当たり 1 つまたは複数の論理ドライブを持つことができます。また、アレイ内の論理ドライブのサイズに制限はありません。論理ドライブをアレイ自体と同じ大きさにすることができます。ただし、ディスク・プールの現行の実装では、ディスク・プール内に作成できる論理ドライブの最大サイズは 64 TB です。この制限を変更するには、IBM 販売店または担当者にお問い合わせください。

コントローラー・ファームウェア・バージョン 7.83 以降では、ディスク・プールをサポートできる IBM DS ストレージ・サブシステム上で、「シン・ボリューム」または「シン論理ドライブ」と呼ばれる新しいタイプの論理ドライブを作成できます。シン論理ドライブは、実際の物理ディスク割り振りによって作成することができ、論理ドライブのサイズの一定の割合を占めるにすぎません。この論理ドライブは、フル容量のディスクとしてホストに提示されます。実際の物理ディスクの割り振りは、必要に応じて 4 GB の割り振りの倍数で増大します。リポジトリの使用量が一定レベルに達すると、使用量レベル・アラートが表示されます。その場合、ユーザーは必要に応じて追加容量を構成できます。標準論理ドライブは、ディスク・プールにもアレイにも作成できます。しかし、シン論理ドライブは、ディスク・プールにしか作成できません。シン・プロビジョニングは、サブシステムにシン論理ドライブを作成する機能です。この機能は、ご使用の IBM DS ストレージ・サブシステムに、必要なバージョンのコントローラー・ファームウェアと共に無料で提供されます。現在、DS3500 ストレージ・サブシステムおよび DCS3700 ストレージ・サブシステム、ならびに Performance Module Controller 使用の DCS3700 ストレージ・サブシステムのみが、シン・プロビジョニングをサポートします。

標準論理ドライブの作成時に、使用可能なストレージの割り振りを前もって行い、データ可用性および入出力パフォーマンスに関するアプリケーションのニーズを満たすように標準論理ドライブの容量を構成します。ホストの入出力データ書き込みに使用できるストレージを増やすには、ディスク・プールまたはアレイにドライブを追加する必要があります。シン論理ドライブを使用すると、少量の物理ストレージの割り振りで大容量の仮想論理ドライブを作成することができ、時とともに増大する容量要求を満たすために割り振りを増やすことができます。ストレージ要求が増大すれば、物理ストレージ容量を必要なだけ増やすことができます。シン論理ドライブを使用すると、ディスク・プールに未使用の余分な容量が存在する可能性を減らすことができます。

シン論理ドライブは、ホスト入出力データの書き込みに使用できる大きな仮想容量を持つ論理ドライブですが、仮想容量のすべてが、割り振られた物理容量に関連付けられるわけではありません。シン論理ドライブの構成時に、2 つのタイプの容量を指定します。すなわち、仮想容量と物理 (優先) 容量です。仮想容量はホストに報告される容量です。仮想容量に指定できる最小値は 32 MB、最大は 64 TB です。物理容量

(プロビジョン容量および優先容量とも呼ばれる) は、データの書き込み用に現在割り振られている物理ドライブ・スペースの量です。管理者は、容量の要求が増えるにつれて物理容量を増やすことができます。物理容量は、手動で増やすことも、物理容量の最大サイズを指定して自動的に増やすこともできます。コントローラーは、必要とする物理容量を 4 GB の増分で自動的に増やします。手動方式を選択した場合、物理容量に指定できる最小値は 4 GB、最大は 64 TB です。物理容量は 4 GB の増分で指定する必要があります。IBM DS ストレージ・マネージャーは、指定された物理容量を、シン論理ドライブに割り振られる仮想容量のパーセンテージとして変換します。通常、割り振られた物理容量は、シン論理ドライブの作成時に仮想容量に指定される量よりかなり小さくなります。物理容量を自動的に増加するのが優先方式です。

シン論理ドライブの作成時に、それに関連付けられたリポジトリ論理ドライブも作成されます。リポジトリ論理ドライブの初期サイズは、「create logical drive (論理ドライブの作成)」ウィザードで指定する優先容量です。リポジトリ論理ドライブのデフォルトの優先容量は 4 GB です。管理者は、リポジトリ論理ドライブの容量使用率をモニターして容量不足のためにホスト書き込み要求が失敗するのを防止するために、2 つの属性を構成できます。管理者は、IBM DS ストレージ・マネージャーに対してリポジトリ論理ドライブ使用率の警告しきい値パーセンテージを設定して、指定されたパーセンテージの容量が使用されるとアラートを生成するようにすることができます。リポジトリ使用率が警告しきい値に達したときにサブシステムがプロビジョンされた容量を指定量だけ自動的に拡張できるように、管理者は、自動拡張ポリシー用の最大拡張値を指定します。

標準論理ドライブとシン論理ドライブの相違点を、以下にいくつか示します。

- **RAID レベル** — ディスク・プールまたはアレイの RAID レベルは、冗長データを論理ドライブ間に分散させる方法と場所を決定します。ストレージ管理ソフトウェアは、ディスク・プール内のすべての論理ドライブに 10+P+Q RAID 6 を自動的に割り当てます。アレイの論理ドライブの場合は、ストレージ管理ソフトウェアはサポートされる RAID サポート論理ドライブ・タイプのいずれかをユーザーに選択させます。標準論理ドライブは、ディスク・プールにもアレイにも作成できます。シン論理ドライブは、ディスク・プールにのみ作成できます。
- **容量の割り振り** — 標準論理ドライブでは、使用可能なストレージ容量を前もって割り振ります。シン論理ドライブでは、仮想容量と優先容量を指定し、時とともに実際の容量要求を満たすように物理容量を増やします。
- **容量の拡張** — 標準論理ドライブの容量は、任意の増分で増やすことができます。ディスク・プールは 4 GB ディスク・スペースの倍数で作成されるため、シン論理ドライブの場合は 4 GB の増分で容量を割り振る必要があります。
- **ホット・スペアの使用** — ドライブ障害の状態から復旧するために、アレイ内の論理ドライブではホット・スペア・ドライブを指定できます。ディスク・プールでは、ホット・スペア・ドライブを使用しません。ディスク・プールでドライブ障害が発生した場合のデータの再構成用として、ディスク・プール内の各ディスク・ドライブの一定のパーセンテージが予約されています。

ディスク・プールの作成

未構成容量ノードからディスク・プールを作成するには、「Subsystem Management (サブシステム管理)」ウィンドウで以下の手順を実行します。

注: Performance Module Controller を装備した DCS3700 サブシステムの 2 TB NL-SAS ドライブでは、T10PI はサポートされません。したがって、これらのドライブを使用している場合、ディスク・プールを手動で作成する必要があります。この手順を使用すると、T10PI の使用可能化を回避できます。ディスク・プールを手動で作成するには、「Disk Pool Automatic Configuration (ディスク・プール自動構成)」ウィンドウで「No (いいえ)」をクリックします。

1. ディスク・プールを作成するには、以下の手順のうち 1 つを完了します。

- 「Storage & Copy Services (ストレージおよびコピー・サービス)」タブで、「**Unconfigured Capacity (HDD, SAS)** (未構成容量 (HDD、SAS))」を右クリックして、「**Create Disk pool (ディスク・プールの作成)**」を選択します。
- 「Storage & Copy Services (ストレージおよびコピー・サービス)」タブで、「**Total Unconfigured Capacity** (未構成容量の合計)」を選択して、「サブシステム管理」ウィンドウで「**Storage (ストレージ)**」>「**Disk pool (ディスク・プール)**」>「**Create (作成)**」を選択します。

「Create Disk Pool (ディスク・プールの作成)」ウィンドウが開きます。

2. 「**Disk pool name (ディスク・プール名)**」にディスク・プールの新規名を入力し、リストから必要なディスク・プールを選択します。
3. セキュア・ディスク・プールが必要な場合は、「**Create secured disk pool (セキュア・ディスク・プールの作成)**」を選択します。

注: セキュア・ディスク・プールを作成できるのは、FDE ドライブがあり、FDE プレミアム・フィーチャが使用可能になっている場合のみです。

4. 「**View the notification settings (通知設定の表示)**」をクリックします。重大な警告および早期警告の通知しきい値を表示および変更することができます。
5. 「**Create (作成)**」をクリックします。ディスク・プールが作成されるまで待ちます。

「Subsystem Management (サブシステム管理)」ウィンドウを開いた時点で、あるいは論理ドライブ、ディスク・プール、またはアレイを削除した時点で、以下の状態にある場合、「**Disk Pool Automatic Configuration (ディスク・プール自動構成)**」ウィンドウがポップアップします。

- ディスク・プールが作成されておらず、サブシステム内に未割り当てドライブがある。
- 1 つのディスク・プールが作成されており、そのディスク・プール内のドライブと同じタイプの未割り当てドライブがサブシステム内にある。
- 複数のディスク・プールが作成されており、それらのディスク・プール内のドライブと同じタイプの未割り当てドライブがサブシステム内にある。

既存のディスク・プールへの容量の追加

既存のディスク・プールに容量を追加することができます。「Storage & Copy Services (ストレージおよびコピー・サービス)」タブで、容量を追加するディスク・プールを選択し、以下のいずれかを実行します。

- 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Storage (ストレージ)**」>「**Disk pool (ディスク・プール)**」>「**Add Drives (ドライブの追加)**」を選択する。
- ドライブを追加するディスク・プールを右クリックして、「**Add Drives (ドライブの追加)**」を選択します。

ディスク・プールの設定の変更

既存のディスク・プールの重大な警告および早期警告の通知しきい値、再構成優先順位、およびディスク・プール保存容量を変更することができます。「Storage & Copy Services (ストレージおよびコピー・サービス)」タブで、ディスク・プールを選択して、以下のいずれかを実行します。

- 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Storage (ストレージ)**」>「**Disk pool (ディスク・プール)**」>「**Change (変更)**」>「**Settings (設定)**」を選択する。
- 設定を変更するディスク・プールを右クリックして、「**Change (変更)**」>「**Settings (設定)**」を選択します。

「**Change Disk Pool Settings (ディスク・プール設定の変更)**」ウィンドウが開きます。重大な警告および早期警告のしきい値制限 (ディスク・プール容量のパーセンテージで表される) を、増やしたり減らしたりすることができます。ルーラーをスライドさせて、「**Degraded (機能低下)**」再構成優先順位、「**Critical (重大)**」再構成優先順位、およびバックグラウンド操作優先順位を変更します。

「**OK**」をクリックして、設定を保存します。

アレイの作成

未構成容量ノードからアレイを作成するには、「**Subsystem Management (サブシステム管理)**」ウィンドウで以下の手順を実行します。

1. 次の 2 つの方式のいずれかを使用して、新規アレイを作成します。

- 「**Total Unconfigured Capacity (未構成容量の合計)**」を選択し、「**Array (アレイ)**」 > 「**Create (作成)**」をクリックする。
- 「**Total Unconfigured Capacity (未構成容量の合計)**」を選択し、右クリックしてから「**Create Array (アレイの作成)**」をクリックする。

「**Introduction (Create Array) (紹介 (アレイの作成))**」ウィンドウが開きます。

2. 「**Next (次へ)**」をクリックします。「**Array Name & Drive Selection (Create Array) (アレイ名およびドライブ選択 (アレイの作成))**」ウィンドウが開きます。

注: Performance Module Controller を装備している DCS3700 ストレージ・サブシステムで 2 TB NL-SAS ドライブを使用している場合、「**Drive Selection (ドライブの選択)**」で「**Manual (手動)**」を選択します。

3. 下記のフィールドに対して、適切な処置を実行します。

- **Array name (アレイ名):** 新規アレイ名を入力します。名前は最大 30 文字です。
- **Drive selection (ドライブの選択):** 「**Automatic (自動)**」または「**Manual (Advanced) (手動 (拡張))**」を選択します。

自動 自動的に生成されたドライブおよび容量のオプションのリストから選択する。このオプションは、デフォルトで事前選択されています。

手動 (拡張)

特定のドライブを選択して、新規アレイ用の容量を取得する。

- 「**Next (次へ)**」をクリックします。「**RAID Level and Capacity (Create Array) (RAID レベルと容量 (アレイの作成))**」ウィンドウが開きます。

4. RAID レベル (冗長保護) を指定します。

5. 新規アレイ用のドライブ数 (全容量) を選択します。

6. 「**Finish(完了)**」をクリックします。「**Array Created (アレイ作成済み)**」ウィンドウが開きます。

7. 論理ドライブの作成処理を続行する場合は、「**Yes (はい)**」をクリックし、論理ドライブの作成を後で行う場合は「**No (いいえ)**」をクリックします。

新磁気ディスク制御機構 (RAID)

新磁気ディスク制御機構 (Redundant array of independent disks: RAID) は、すべてのオペレーティング・システムで使用可能であり、レベル と呼ばれる一連の構成によって、ドライブでのユーザー・データや冗長データの書き込みおよび検索方法が決定されます。ストレージ・サブシステム・コントローラーのファームウェアでは、以下の 6 つの RAID レベル構成がサポートされます。

- RAID-0

- RAID-1
- RAID-3
- RAID-5
- RAID-6
- RAID-10

各レベルでは、異なるパフォーマンスおよび保護機構が提供されます。RAID-1、RAID-3、RAID-5、および RAID-6 では、冗長データをドライブ・メディアに書き込むことで、フォールト・トレランスを実現します。冗長データは、データのコピー（ミラーリングされたデータ）、またはデータから派生したエラー訂正コードの場合があります。ドライブに障害が発生した場合、保護対象のデータからの冗長データが別のドライブ上に保管されます。その冗長データを使用して、ホット・スペア交換ドライブ上にドライブ情報が再構成されます。RAID-1 では、冗長性を得るためにミラーリングが使用されます。RAID-3、RAID-5、および RAID-6 では、データ・バイトを基に構成されて各ディスクにデータと共にストライピングされる、冗長情報（パリティー ともいいます）が使用されます。

表 17. RAID レベルの説明

RAID レベル	簡単な説明	詳しい説明
RAID-0 注: RAID-0 は、データの冗長性は提供しません。	非冗長、ストライピング・モード	RAID-0 は簡便ですが、データの冗長性は提供されません。RAID-0 アレイでは、アレイ内のすべてのドライブにデータが分散されます。通常、これが最高のパフォーマンスを発揮しますが、単一ドライブ障害に対する保護は何も提供しません。アレイの中の 1 つのドライブに障害が発生すると、そのアレイ内のすべての論理ドライブに障害が発生することになります。この RAID レベルは、高度なデータ可用性が必要な環境で使用してはなりません。RAID-0 は、あまり重要でないデータに適しています。
RAID-1 または RAID-10	ストライピング/ミラーリング・モード	• RAID-1 には少なくとも 2 つのドライブが必要です。1 つはユーザー・データ用で、もう 1 つはミラーリングされるデータ用です。DS3000/DS4000/DS5000 ストレージ・サブシステムの RAID-1 実装は、RAID-1 と RAID-10 の組み合わせで、選択するドライブの数に応じて決まります。選択したドライブが 2 つだけの場合は、RAID-1 が実装されます。4 つ以上のドライブを (2 の倍数で) 選択した場合は、アレイ全体にわたって RAID 10 が自動的に構成されます。この場合、2 ドライブはユーザー・データ専用で、2 ドライブはミラーリングされたデータ専用です。 • RAID-1 は、ハイパフォーマンスと最良のデータ可用性を提供します。RAID-1 論理ドライブでは、データは 2 つの重複ディスクに同時に書き込まれます。RAID-10 論理ドライブでは、データはミラーリングされたペアにまたがってストライピングされます。 • RAID-1 では、ディスク・ミラーリングを使用して、1 つのドライブから別のドライブへと正確なデータのコピーを作成します。RAID-1 アレイ内の 1 つのドライブに障害が発生すると、ミラーリングされたドライブが処理を引き継ぎます。 • RAID-1 および RAID-10 は、容量という点から見るとコストがかかります。ドライブの半分が冗長データに使用されるからです。

表 17. RAID レベルの説明 (続き)

RAID レベル	簡単な説明	詳しい説明
RAID-3	高帯域幅モード	- RAID-3 では、論理ドライブに、冗長情報 (パリティ) を保持するための専用ディスクが 1 つ必要です。ユーザー・データは、残りのドライブに分散してストライピングされます。 - 大量の順次データの読み取りおよび書き込みを行うマルチメディアまたは医療用画像処理などのアプリケーションには、RAID-3 をお勧めします。このようなアプリケーションでは、入出力サイズが大きく、単一の要求に対してサービスを提供するためにすべてのドライブが並行して作動し、高い入出力転送速度を実現します。
RAID-5	高入出力モード	- RAID-5 では、ユーザー・データと冗長情報 (パリティ) の両方が、論理ドライブ内のすべてのドライブに分散してストライピングされます。 - RAID-5 では、冗長情報用に 1 ドライブ分の容量と同じ容量を使用します。 - 入出力サイズが小さくて読み取りアクティビティの比率が高い、データベースやファイル・システム・ストレージなどのマルチユーザー環境の場合は、RAID-5 をお勧めします。入出力サイズが小さい場合、セグメント・サイズを選択が適切であれば、1 つの読み取り要求は 1 つの個別ドライブから取り出されます。その他のドライブは、他の入出力読み取り要求に対して並行してサービスを提供するために使用できるので、高速の読み取り入出力要求速度が実現します。
RAID-6	二重分散パリティによるブロック・レベル・ストライピング	RAID-6 は RAID-5 が進化したもので、2 セットの分散パリティを保管することによって 2 つのディスク・ドライブ障害が同時に発生した場合にも耐えられるように設計されています。 - RAID レベル 6 は、冗長データのために (1 つのアレイ内で) 2 つのドライブに相当する容量を使用します。 - RAID レベル 6 は、2 セットの分散パリティを保管することにより、2 つのドライブに同時に障害が起きるのを防止します。 注: すべての DS ストレージ・サブシステムが RAID-6 をサポートするわけではありません。ご使用のストレージ・サブシステムの発表レターまたは「インストール、メンテナンスおよびユーザーのガイド」を調べて、RAID-6 および必要なコントローラー・ファームウェアの最小バージョンがご使用のストレージ・サブシステムでサポートされているかどうかを判別してください。

注: 1 つのアレイでは単一の RAID レベルが使用され、このアレイのすべての冗長データはこのアレイ内部に保管されます。

アレイの容量は、メンバー・ドライブの総計容量から、冗長データ用に確保される容量を引いたものです。冗長データ用に必要な容量は、使用する RAID レベルによって異なります。

冗長検査を行うには、「**Advanced (拡張)**」 > 「**Recovery (リカバリー)**」 > 「**Check array redundancy (アレイの冗長検査)**」をクリックします。冗長検査では、以下のいずれかのアクションが実行されます。

- RAID-3、RAID-5、または RAID-6 論理ドライブのブロックをスキャンし、各ブロックの冗長情報を検査する。

- RAID-1 のミラーリングされたドライブのデータ・ブロックを比較する。

重要: 「**Check array redundancy (アレイの冗長検査)**」を選択すると、Recovery Guru によって指示された場合にのみこのオプションを使用するよう注意する警告メッセージが開きます。また、リカバリー以外の理由で冗長検査を行う必要がある場合には、メディア・スキャンを使用して冗長検査を使用可能することができますことも示されています。

標準論理ドライブの作成

標準論理ドライブ は、ストレージ・サブシステムにデータを保管するために作成する基本的な構造である、論理構造です。オペレーティング・システムは、論理ドライブを単一のドライブとして認識します。アレイまたはディスク・プールから論理ドライブを作成することができます。データの可用性に関するアプリケーションのニーズを満たし、ファイバー・チャネルの入出力パフォーマンスが最大になるように (アレイから論理ドライブを作成した場合)、RAID レベルを選択してください。

注: クラスター構成で、論理ドライブを追加または削除する場合は、論理ドライブをノード A と B の両方に対して認識させておく必要があります。

論理ドライブを作成するには、「Subsystem Management (サブシステム管理)」ウィンドウで以下の手順を実行します。

1. 「Introduction (Create Logical Drive) (紹介 (論理ドライブの作成))」ウィンドウの「Logical (論理)」ページまたは「Physical (物理)」ページで、新規論理ドライブを作成するアレイまたはディスク・プールの「Free Capacity (空き容量)」をクリックし、アレイまたはディスク・プールを右クリックして、「Create Logical Drive (論理ドライブの作成)」をクリックします。
2. 「Specify Capacity/Name (Create Logical Drive) (容量/名前の指定 (論理ドライブの作成))」ウィンドウで、作成する論理ドライブについて、以下のパラメーターを指定します。

New logical drive capacity (新規の論理ドライブの容量)

容量として、アレイ内の未構成容量の全体またはアレイの容量の一部を指定できます。

Units (単位)

使用可能な容量に応じて、GB、MB、または TB を選択します。

Name (名前)

ストレージ・サブシステム内で固有の名前を入力します (最大 30 文字)。

3. 「Advanced logical drive parameters (拡張論理ドライブ・パラメーター)」ウィンドウで、適切な入出力特性 (特性のタイプ、セグメント・サイズ、およびキャッシュ先読み乗数) を指定してから、「Next (次へ)」をクリックします。「Specify Logical Drive-to-LUN Mapping (Create Logical Drive) (論理ドライブから LUN へのマッピングの指定 (論理ドライブの作成))」ウィンドウが開きます。

注: 入出力特性の設定値は、自動的に設定するか、論理ドライブの用途 (ファイル・システム、データベース、またはマルチメディア) のうちの 1 つに基づいて手動で指定することができます。

4. 「Specify Logical Drive-to-LUN Mapping (Create Logical Drive) (論理ドライブから LUN へのマッピングの指定 (論理ドライブの作成))」ウィンドウで、論理ドライブから LUN へのマッピングを指定します。

論理ドライブから LUN へのマッピングの設定は、次の 2 つのいずれかの設定値にすることができます。

Default mapping (デフォルト・マッピング)

自動設定を指定すると、デフォルトのホスト・グループ内で次に使用可能な LUN を使用して、論理ドライブに LUN が自動的に割り当てられます。この設定により、論理ドライブに

は、特定の論理ドライブと LUN のマッピング (「Topology (トポロジー)」ビューにおいてデフォルト・ホスト・グループ・ノードにより指定されているもの) が指定されていないホスト・グループまたはホスト・コンピューターに対するアクセスが認可されます。ストレージ区画機能が使用可能になっていない場合は、自動設定を指定する必要があります。さらに、ホスト・オペレーティング・システムに合わせてホスト・タイプを変更することもできます。

Map later using the Mappings View (マッピング・ビューを使用して後でマップする)

この設定値は、作成時に LUN を論理ドライブに割り当てないことを指定します。この設定値を使用すると、特定の論理ドライブから LUN へのマッピングを作成し、「**Mappings Defined (定義済みのマッピング)**」オプションを使用してストレージ区画を作成できます。ストレージの区画化を使用可能にする場合は、この設定値を指定してください。

5. 「**Finish (完了)**」をクリックして論理ドライブを作成します。「**Creation Successful (Create Logical Drive) (作成成功 (論理ドライブの作成))**」ウィンドウが開きます。
6. 別の論理ドライブを作成する場合は、「**Creation Successful (Create Logical Drive) (作成成功 (論理ドライブの作成))**」ウィンドウで、「**Yes (はい)**」をクリックしてステップ 9 に進みます。別の論理ドライブを作成しない場合は、「**No (いいえ)**」をクリックします。「**Completed (Create Logical Drive) (完了 (論理ドライブの作成))**」ウィンドウが開いたら、「**OK**」をクリックしてステップ 10 に進みます。
7. 「**Allocate Capacity (Create Logical Drive) (容量の割り振り (論理ドライブの作成))**」ウィンドウで、同じアレイの空き容量から新しい論理ドライブを作成するか、別のアレイの空き容量から作成するか、あるいは未構成の容量から作成する (新しいアレイを作成する) かを選択します。ステップ 1 から開始して、上記のプロセスを繰り返します。「**Completed (Create Logical Drive) (完了 (論理ドライブの作成))**」ウィンドウが開きます。
8. 「**OK**」をクリックします。
9. 論理ドライブをオペレーティング・システムに登録します。

論理ドライブから LUN への自動マッピングを指定して論理ドライブを作成した後、170 ページの『デバイスの識別』のご使用のオペレーティング・システムに該当する指示に従って、新しい論理ドライブをディスカバーします。

シン論理ドライブの作成

コントローラー・ファームウェア が 7.8x.xx.xx 以降の DS3500 または DCS3700 ストレージ・サブシステム上、あるいは Performance Module Controller 搭載の DCS3700 ストレージ・サブシステム上では、シン論理ドライブを作成する場合、以下のようにします。

1. 次のいずれかを実行します。
 - ディスク・プール内の「Free Capacity (空き容量)」ノードを右クリックして、「**Create Logical Drive (論理ドライブの作成)**」を選択する。
 - メインメニューから、ディスク・プール内の「Free Capacity (空き容量)」ノードを選択し、「**Storage (ストレージ)**」 > 「**Create (作成)**」 > 「**Logical Drive (論理ドライブ)**」を選択する。

「**Create Logical Drive:Specify Parameters (論理ドライブの作成: パラメーターの指定)**」ウィンドウが開きます。
2. 論理ドライブに名前を付けて、初期容量を指定した後、シン論理ドライブを作成するために「**Create thin logical drive (シン論理ドライブの作成)**」チェック・ボックスを選択します。

注: シン論理ドライブでは、動的読み取りキャッシュ (dynamic read cache) は使用できません。

3. 「**Next (次へ)**」をクリックします。「**Create Logical Drive:Choose Physical capacity (論理ドライブの作成: 物理容量の選択)**」ウィンドウが開きます。

4. デフォルト設定のシン論理ドライブを作成する場合は、「**Finish (完了)**」をクリックします。デフォルト設定のいずれかを変更する場合は、「**Customize capacity settings(advanced) (容量設定のカスタマイズ (拡張))**」を選択して、「**Next (次へ)**」をクリックします。「**Create Logical Drive:Customize settings (論理ドライブの作成: 設定のカスタマイズ)**」ウィンドウが開きます。
5. 独自の優先拡張容量、最大拡張容量、および使用率警告しきい値を選択できます。「**Finish(完了)**」をクリックします。

これで、シン論理ドライブが作成されました。

動的容量拡張の概要

動的容量拡張 (DCE) は、アレイまたはディスク・プールの容量を増やす、ストレージ管理ソフトウェアの変更操作です。この変更操作を使用して、未割り当てのドライブをアレイまたはディスク・プールに追加することができます。未割り当てのドライブを追加すると、アレイまたはディスク・プールの空き容量が増えます。この空き容量を使用して、ディスク・プールまたはアレイに対して、追加の論理ドライブを作成したり、予約容量を追加したりすることができます。操作全体を通してアレイ内のデータに継続的にアクセスできるため、この操作は動的と見なされます。未割り当てドライブをアレイまたはディスク・プールに追加する際には、以下のガイドラインに留意してください。

- DCE 変更操作のために選択できる未割り当てドライブの数は、コントローラー・ファームウェアによって制限されます。アレイに対しては、一度に 2 個の未割り当てドライブを追加できます。ディスク・プールに対しては、一度に最大 12 個のドライブを追加できます。ただし、1 つの DCE 操作が完了した後、必要な容量に達するまで、再度ドライブを追加できます。
- 空き容量を拡張するために未割り当てドライブを追加しても、アレイ内またはディスク・プール内の既存の論理ドライブのサイズは増えません。この操作は、アレイ内またはディスク・プール内の既存の論理ドライブ容量を、より多数のドライブにわたって再配分します。
- アレイまたはディスク・プールに追加する未割り当てドライブは、同一のメディア・タイプおよびインターフェース・タイプでなければなりません。1 つのアレイ内またはディスク・プール内で異なるドライブ・タイプを混用することは許可されません。可能な場合は常に、アレイまたはディスク・プール内の現行ドライブの容量と同じ容量をもつドライブを選択してください。現在ディスク・プール内にあるドライブの容量以上の容量をもつドライブを、動的容量拡張操作の一部として追加することは可能です。ただし、現在ディスク・プールにあるドライブより大きい容量のドライブが追加された場合、ディスク・プール内の最小ドライブを超える容量は使用されず、未使用の量は「**unusable (使用不能)**」容量として報告されます。
- RAID レベル 1 アレイには、データの冗長性が構成されるようにするために、2 つのドライブを追加する必要があります。
- セキュリティーが有効にされているアレイまたはディスク・プール、つまりセキュリティー対応アレイまたはディスク・プールには、セキュリティー対応ドライブのみ追加できます。
- T10PI 有効論理ドライブが入っている T10PI 対応アレイまたはディスク・プールには、T10PI 対応ドライブのみ追加できます。

進行中の操作の表示

「Operations in Progress (進行中の操作)」ウィンドウには、ストレージ・サブシステムで現在実行中の、長時間実行される操作がすべて表示されます。これは表示専用のウィンドウで、進行をモニターすることができます。「Operations in Progress (進行中の操作)」ウィンドウを開いたまま、「Subsystem Management (サブシステム管理)」ウィンドウで他のタスクを実行することができます。

以下の進行状況を表示できます。

- 動的容量拡張 (DCE) – アレイに容量を追加中

- 動的 RAID マイグレーション (DRM) – アレイの RAID レベルを変更中
- アレイのデータの冗長性を検査中
- アレイのデフラグ中
- 論理ドライブの初期化中
- 動的論理ドライブ拡張 (DVE) – 論理ドライブに容量を追加中
- 動的セグメント・サイズ (DSS) – 論理ドライブのセグメント・サイズを変更中
- 再構成 – 読めないセクターまたは障害が起きたドライブのため、パリティからデータを再構成中
- コピー・バック – ホット・スペア・ドライブから新規の交換用ドライブにデータをコピー中
- VolumeCopy
- リモート・ミラーの同期化中

詳しくは、オンライン・ヘルプを参照してください。

グローバル・ホット・スペア・ドライブの構成

データをいつでも使用可能な状態にしておくために、ストレージ・サブシステム内で使用可能な物理ドライブをグローバル・ホット・スペア・ドライブとして割り当てることができます。グローバル・ホット・スペアは、データを収容しておらず、RAID 1、RAID 10、RAID 3、RAID 5、または RAID 6 アレイ内のドライブに障害が発生した場合にスタンバイとしての役目を果たします。グローバル・ホット・スペアは、ディスク・プール用のスペアとしては使用されません。ディスク・プールは、ドライブに障害が起きた場合の再構成データ用に、ディスク・プール内のすべてのドライブ間に予約容量を分散させて作成されます。アレイ内のドライブに障害が発生すると、ストレージ・サブシステムが稼働した状態でコントローラーが自動的にホット・スペア・ドライブを使用し、障害が起きた物理ドライブと置き換えます。コントローラーは、冗長データを使用して、障害が起きた物理ドライブからデータを取り出し、置換 (ホット・スペア) ドライブにデータを自動的に再構成します。これを再構成 といいます。ホット・スペア・ドライブにより、ストレージ・サブシステムに新しいレベルの冗長性が追加されます。ストレージ・サブシステム内で物理ドライブに障害が発生すると、ホット・スペア・ドライブが自動的に代替ドライブとして使用されるので、物理的に交換する必要がありません。

ホット・スペア・ドライブの割り当て

ストレージ・サブシステムに定義されたアレイにホット・スペア・ドライブを割り当てるには、次の 2 つの方法があります。

- 「Automatically assign drives (ドライブの自動割り当て)」: このオプションを選択すると、使用可能なドライブを使用して、最良のホット・スペア範囲でホット・スペア・ドライブが自動的に作成されます。このオプションは、常に使用可能です。
- 個々のドライブの手動割り当て: このオプションを選択した場合、ホット・スペア・ドライブは、以前に選択したドライブ以外に作成されます。

ホット・スペア・ドライブの手動割り当てを選択した場合、ホット・スペアを使用してカバーするドライブの合計容量に等しいか、またはそれより大きい容量のドライブを選択してください。例えば、18 GB のドライブがあり、構成済み容量が 8 GB の場合は、9 GB 以上のドライブをホット・スペアとして使用することができます。通常、ストレージ・サブシステム内の最大ドライブの容量に等しいか、またはそれより大きい容量のドライブ以外は、ホット・スペアとして割り当てないでください。異なる容量のハード・ディスクが混在する構成では、データ保護を最大限に確保するには、最大容量のドライブのみをホット・スペア・ドライブとして使用する必要があります。また、個々のドライブを手動で割り当て解除するオプションもあります。

アレイ内のドライブに障害が発生した場合、ユーザーの介入を必要とせずに、障害が起きたドライブの代わりに自動的にホット・スペアに置き換えることができます。ドライブに障害が起きたときにホット・スペアが使用可能であれば、コントローラーは冗長データを使用してホット・スペア上にデータを再構成します。

注: インターフェース・プロトコルまたはテクノロジーが異なるドライブは、相互にホット・スペアとして使用できません。例えば、SATA ドライブとファイバー・チャネル・ドライブは、相互にホット・スペアとして動作することはできません。

1. ホット・スペア・ドライブを割り当てるには、以下の手順のうち 1 つを完了します。
 - 「Storage & Copy Services (ストレージおよびコピー・サービス)」タブで、ストレージ・サブシステムを右クリックして、「**Configuration (構成)**」 > 「**Hot Spare Coverage (ホット・スペア・カバレッジ)**」を選択します。
 - 「Setup (セットアップ)」タブでは、「**Create Storage (ストレージの作成)**」 > 「**Configure hot spares (ホット・スペアの構成)**」を選択します。
2. 「Automatic (自動)」または「Manual (手動)」を選択します。「Automatic (自動)」を選択した場合、ストレージ・サブシステムは 1 つのドライブをホット・スペアとして自動的に割り当てます。後で、ホット・スペアの適用範囲を参照および変更できます。
3. 手動でホット・スペア・ドライブを選択するには、アレイを選択し「**Assign (割り当て)**」をクリックします。
4. ドライブをホット・スペアとして選択し「**OK**」をクリックします。

ホット・スペア・ドライブからのデータの復元

障害のあるドライブを物理的に交換した後で、以下のいずれかのオプションを使用してデータを復元できます。

- 障害が起きたドライブの交換が完了すると、データはホット・スペアから交換後の新しいドライブへとコピーし戻されます。このアクションをコピー・バックといいます。
- ホット・スペアをアレイの永続メンバーとして割り当てることができます。このオプションの場合、コピー・バック機能を実行する必要はありません。

注: コントローラー・ファームウェア・バージョンが 10.84 以降の場合、ホット・スペア・ドライブはコピーバック・モードで動作します。

ホット・スペアがない場合でも、アレイの作動中に障害のあるドライブを置き換えることができます。ドライブが RAID レベル 1、RAID レベル 3、RAID レベル 5、RAID レベル 6、または RAID レベル 10 アレイの一部である場合、コントローラーは冗長データを使用して、置き換えられたドライブ上に自動的にデータを再構成します。

「**Manually unassign drives (ドライブの手動割り当て解除)**」を選択すると、「Physical (物理)」タブで選択したホット・スペア・ドライブが割り当て解除されます。「Physical (物理)」タブでドライブを選択していない場合は、このオプションは使用できません。

デフォルト・ホスト・オペレーティング・システムの定義

ホスト・コンピューターで論理ドライブを使用する前に、正しいホスト・タイプを指定する必要があります。ホスト・タイプにより、ストレージ・サブシステムが接続するホストの各オペレーティング・システムと、ストレージ・サブシステム・コントローラーがどのように連動するかが決まります。同じストレージ・サブシステムに接続されるすべてのホスト・コンピューターが同じオペレーティング・システムを使用し、区画の分割を定義しない場合は、デフォルトのホスト・タイプを定義できます。

現在のデフォルト・ホスト・タイプを確認するには、以下の手順を実行します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウで、「**View Storage Subsystem Profile (ストレージ・サブシステム・プロファイルの表示)**」をクリックします。「Storage Subsystem Profile (ストレージ・サブシステム・プロファイル)」ウィンドウが開きます。
2. 「**Host Mappings (ホスト・マッピング)**」タブをクリックします。「**Default Group (デフォルト・グループ)**」を右クリックして、「**Change Default Host Operating System (デフォルト・ホスト・オペレーティング・システムの変更)**」を選択します。インデックスの隣に Base という語が表示されているホスト・タイプ名が、デフォルトのホスト・タイプです。
3. 「**Close (クローズ)**」をクリックする。

注: Asymmetric Logical Unit Access (ALUA) マルチパス機能を使用可能にするには、ホスト区画またはデフォルトのホスト・グループに対して ALUA ホスト・タイプが選択されている必要があります。

ストレージ・マネージャーの構成時に指定するホスト・タイプの設定によって、ストレージ・サブシステム・コントローラーが、接続されたホストのオペレーティング・システムとどのように連動するかが決まります。同一のホスト・タイプにより定義されたファイバー・チャネル HBA ポートはすべて、ストレージ・サブシステム・コントローラーでは同じ方法で処理されます。この判定は、ホスト・タイプにより定義されている指定に基づいて行われます。ホスト・タイプ設定によって異なる指定の中には、以下のようなオプションがあります。

自動ドライブ転送/ALUA

自動論理ドライブ転送機能 (ADT) を使用可能または使用不可にします。コントローラー・ファームウェア・バージョン 7.83.xx.xx からは、この設定は代わりに ALUA 機能を使用可能または使用不可にするために使用されます。

所有されていない LUN での予約許可

コントローラーが所有していない LUN について受け取った予約/解放コマンドに対する、コントローラーの応答を判別します。

据え置きエラーの報告

ストレージ・サブシステム・コントローラーの据え置きエラーをホストに報告する方法を決定します。

ベンダー固有の装置アテンションをチェック条件として報告しない

コントローラーがベンダー固有の装置アテンション条件をチェック条件状況として報告するかどうかを決定します。

標準照会におけるワールドワイド・ネーム

拡張標準照会を使用可能または使用不可にします。

UTM LUN 所有権を無視

ユニバーサル・アクセス LUN (UTM LUN) に対する照会の報告方法を決定します。UTM LUN は、ストレージ・マネージャーがインバンド管理構成においてストレージ・サブシステムと通信するために使用されます。

標準照会データでの LUN 優先パスの報告

標準照会データのバイト 6 のビット 4 および 5 に入れて、LUN 優先パスを報告します。

T10PI のためのホスト・サポートを使用可能にします

T10PI のためのホスト・サポートを使用可能または使用不可にします。使用不可にする場合には、コントローラーは、データをホストに送信する前に、T10PI 情報を持つ追加の 8 バイトを剥奪します。

ほとんどのストレージ・サブシステム構成では、特定のオペレーティング・システム環境についてサポートされる各ホスト・タイプの NVSRAM 設定は、ホストをストレージ・サブシステムに接続するために十分な設定になっています。したがって、NVSRAM のホスト・タイプ設定は何も変更する必要はありません。NVSRAM 設定の変更が必要だと考える場合は、変更を開始する前に、IBM サポート担当員に連絡してください。

デフォルトのホスト・タイプを定義するには、以下の手順を実行します。

1. 「**Host Mappings (ホスト・マッピング)**」 > 「**Default Group (デフォルト・グループ)**」 > 「**Change Default Host Operating System (デフォルト・ホスト・オペレーティング・システムの変更)**」をクリックします。「Default Host-type (デフォルト・ホスト・タイプ)」ウィンドウが開きます。
2. リストからホスト・タイプを選択する。
3. 「**OK**」をクリックします。

注:

Veritas Storage Foundation Linux 環境では、デフォルト・ホスト・タイプは 13 に設定されなければなりません。

追加のホスト・タイプとして、NVSRAM にホスト・タイプ VMWARE が追加されました。DS4200 および DS4700 はインデックス 21 を使用します。

他のすべてのサポートされるシステムは、インデックス 16 を使用します。

必須ではありませんが、VMWARE ホストに Linux ホスト・タイプを使用する場合、VMWARE ホスト・タイプに移ることをお勧めします。その理由は、コントローラー・ファームウェアおよび NVSRAM のいずれのアップグレードでも、スクリプトの稼働が継続して必要になるのに対して、VMWARE ホスト・タイプの使用ではスクリプトの稼働が必要にはならないからです。

- ホスト・タイプの変更の後で、コントローラーはリブートする必要はありません。
- ホストはリブートする必要があります。
- ホスト・タイプの変更は、低い入出力状態で行われるべきです。

ホスト・グループの定義

ホスト・グループは、1 つ以上の新規論理ドライブへの共有アクセスを必要とするホスト・コンピューターの論理集合を定義する、ストレージの区画化トポロジー内のエンティティです。定義されているホスト・グループ内の個々のホストに、ホスト・グループとは関係なく、ストレージ区画へのアクセス権を付与できます。論理ドライブから LUN へのマッピングを、ホスト・グループまたはホスト・グループ内の個々のホストに対して行うことができます。

ホスト・グループはストレージ・サブシステム・レベルで作成する必要があります。デフォルト・グループ・レベルでホスト・グループを作成しないでください。ただし、区画化を使用可能にせずにストレージ・サブシステム構成を実行している場合は、デフォルトのホスト・グループを使用することができます。

ホスト・グループを定義するには、以下の手順を実行します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「**Host Mappings (ホスト・マッピング)**」タブをクリックします。
2. 「Host Mappings (ホスト・マッピング)」ページの「Topology (トポロジー)」セクションで、ストレージ・サブシステムまたは「Default Group (デフォルト・グループ)」を強調表示して、「**Define (定義)**」 > 「**Host Group (ホスト・グループ)**」を右クリックします。

注: ストレージ・サブシステムが「Subsystem Management (サブシステム管理)」ウィンドウの左ペイン内で強調表示されていることを確認します。「Undefined Mappings (未定義のマッピング)」は強調表示しないでください。

3. 新規ホスト・グループの名前を入力する。「OK」をクリックします。

異機種ホストの定義

異機種ホスト機能を使用すると、複数の異なるオペレーティング・システムを実行している複数のホストが、単一のストレージ・サブシステムにアクセスすることができます。ストレージ・マネージャーは、一部のサブシステムでは最大 512 のストレージ区画をサポートします。これによって、複数のホスト・タイプのストレージ・サブシステムで、ストレージ容量の共有、ストレージの統合、およびストレージ管理コストの削減が可能になります。

ホスト・コンピューターは、異なるオペレーティング・システム、あるいは同じオペレーティング・システムのバリエーションを実行することができます。「Define New Host Port (新規ホスト・ポートの定義)」ウィンドウでホスト・タイプを定義するとき、異機種ホスト機能は、ストレージ・サブシステムのコントローラーの動作を、情報を送信するオペレーティング・システムまたはホストのバリエーションのニーズ (LUN の報告およびエラー条件など) に合わせます。

注:

1. 各コントローラー上のファームウェアがホストに正しく応答できるよう、ホスト・ポートの定義の際に、各ホスト・タイプに適切なオペレーティング・システムを設定する必要があります。
2. プレミアム・フィーチャーであるストレージの区画化を使用可能にする必要があります。インストール時に保存した区画キーを使用するか、または IBM Web ページを参照してフィーチャー・コードを再活性化し、新規フィーチャー・キーを取得してください。プレミアム・フィーチャーの詳細については、55 ページの『ストレージ・マネージャーのプレミアム・フィーチャー』を参照してください。
3. サーバーからストレージ・サブシステムに接続されているすべての HBA ポートが、単一のホスト区画内で定義されている必要があります。

注: Asymmetric Logical Unit Access (ALUA) マルチパス機能を使用可能にするには、ホスト区画またはデフォルトのホスト・グループに対して ALUA ホスト・タイプが選択されている必要があります。

ホストおよびホスト・ポートの定義

「Define a host and host ports (ホストおよびホスト・ポートの定義)」ウィザードを使用してホストおよびホスト・ポートを定義するには、以下の手順を実行します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「Mappings (マッピング)」ビューの「Topology (トポロジー)」セクションで、新規ホスト・グループを右クリックして、「**Define Host (ホストの定義)**」を選択します。「Introduction (Define Host) (紹介 (ホストの定義))」ウィンドウが開きます。
2. 「**Next (次へ)**」をクリックします。「Specify Host Port Identifiers (Define Host) (ホスト・ポート ID の指定 (ホストの定義))」ウィンドウが開きます。
3. 「**Choose a host interface type (ホスト・インターフェース・タイプの選択)**」で、希望するホスト・ポート・インターフェースを選択します。

注: IBM i のストレージを構成している場合、最初のアダプターにあるポートを使用します。IBM i には、有効な構成のために 2 つのアダプターが必要です。

4. HBA 接続が適切にセットアップされた場合、「**Add by selecting a known unassociated host port identifier** (既知の関連付けられていないホスト・ポート ID の選択による追加)」を選択しホスト・ポートを追加します。WWPN を手動で入力するには、「**Add by creating a new host port identifier** (新規のホスト・ポート ID の作成による追加)」を選択します。
5. 「**Alias (エイリアス)**」にホスト・ポート ID を入力し、「**Add (追加)**」をクリックします。「Host Group (ホスト・グループ)」リストに追加されます。「**Next (次へ)**」をクリックします。
6. 手順 3 (91 ページ) および 4 を繰り返し、すべてのホストを追加します。
7. 追加したホスト・ポート ID を削除するには、「**Host port identifiers to be associated with the host** (ホストに関連付けられるホスト・ポート ID)」のホスト・ポート ID を選択して、「**Remove (削除)**」をクリックします。
8. ホスト・タイプを選択して、「**Next (次へ)**」をクリックします。
9. 別のホストと同じ論理ドライブのアクセスを共有するか、「**Yes (はい)**」または「**No (いいえ)**」を選択します。「**Next (次へ)**」をクリックします。
10. 情報を見直して、正確であることを確認します。「**Finish (完了)**」をクリックして作業を完了します。別のホストを定義する必要がある場合、「**Yes (はい)**」を選択して手順を再び繰り返します。

LUN のマッピング

このセクションでは、以下の手順を使用して、LUN をストレージ区画にマップする方法を説明します。

- 『新規のホストまたはホスト・グループへの LUN のマッピング』
- 『既存のホストまたはホスト・グループへの LUN の追加』

新規のホストまたはホスト・グループへの LUN のマッピング

新たに作成した区画に LUN をマップするには、以下の手順を実行します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「Mappings (マッピング)」ビューを選択します。
2. 「Topology (トポロジー)」セクションで、LUN をマップしたいホストを右クリックして、「**Define Storage Partitioning (ストレージの区画化の定義)**」を選択します。「Define Storage Partitioning (ストレージの区画化の定義)」ウィンドウが開きます。
3. 「Define Storage Partitioning (ストレージ区画の定義)」ウィンドウで、「**Host (ホスト)**」または「**Host Group (ホスト・グループ)**」を選択して「**Next (次へ)**」をクリックします。
4. 論理ドライブを選択します。
5. デフォルトの LUN ID を受け入れるか、あるいは変更してから、「**Add (追加)**」をクリックします。
6. 区画にマップしたい各 LUN ごとに、ステップ 5 を繰り返します。

注: また、ストレージ・マネージャー・タスク・アシスタントの「Storage Partitioning (ストレージの区画化)」ウィザード機能を使用して、LUN を新規ストレージ区画にマップすることもできます。

既存のホストまたはホスト・グループへの LUN の追加

新規 LUN を既存の区画にマップするには、以下の手順を完了します。区画に追加したい LUN ごとに、これらの手順を繰り返します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「**Host Mappings (ホスト・マッピング)**」タブをクリックします。

2. 「Topology (トポロジー)」セクションで、LUN をマップしたいホストあるいはホスト・グループを右クリックして、「**Define Additional Mappings (追加のマッピングの定義)**」を選択します。「Define Additional Mapping (追加のマッピングの定義)」ウィンドウが開きます。
3. 「Define Additional Mapping (追加のマッピングの定義)」ウィンドウで以下のオプションを選択して、「**Add (追加)**」をクリックします。
 - ホスト・グループまたはホスト
 - 論理装置番号 (LUN)(0-255)
 - 論理ドライブ

IBM i の IBMSystem Storage の構成

ストレージ・マネージャー・ソフトウェアを備えた DS5100 および DS5300 ストレージ・サブシステムで IBM i LUN をセットアップし、割り当てるには、74 ページの『ディスク・ストレージの構成』および 90 ページの『ホスト・グループの定義』セクションと一緒に、以下のセクションの情報を使用してください。

IBM i 用のポート ID の割り当て

ストレージ・マネージャーを使用して IBM i 用のポート ID を入力する場合、そのポートは最初のアダプターにあります。有効な構成を作成するには、IBM i では 2 つのアダプターが必要です。次の図は、ポート ID を割り当てるセットアップ・ウィンドウを示しています。

DS4700_DtL - Specify Host Port Identifiers (Define Host)

The host communicates with the storage subsystem through its host bus adapters (HBAs) or its iSCSI initiators where each physical port has a unique host port identifier. In this step, select or create an identifier, give it an alias or user label, then add it to the list to be associated with host Series.

[How do I match a host port identifier to a host?](#)

Choose a method for adding a host port identifier to a host:

☒ Add by selecting a known unassociated host port identifier

Known unassociated host port identifier: 21:01:00:e0:8b:a3:ec:cc Refresh

☐ Add by creating a new host port identifier

New host port identifier (16 characters required):

Alias (30 characters maximum): test-hostPort1

Add ? Remove ?

Host port identifiers to be associated with the host:

Host Port Identifier	Alias / User Label

< Back Next > Cancel Help

図 10. IBM i 用のポート ID の割り当て

ホスト・タイプとしての IBM i の定義

ストレージ・マネージャーを使用してホスト・タイプを定義する場合、「**Host type (operating system) (ホスト・タイプ (オペレーティング・システム))**」リストから **IBM i** を選択してください。

重要: 拡張セットアップでは、ホスト・タイプとして **IBM i** を許可しないホスト・グループまたはホスト定義に **LUN 0** が割り当てられる可能性があります。この問題を解決するには、**LUN 0** 設定を除去し、オペレーティング・システムを **IBM i** に変更してから、前に除去した **LUN** を追加してください。

次の図は、**IBM i** をホスト・タイプとして定義するセットアップ・ウィンドウを示しています。

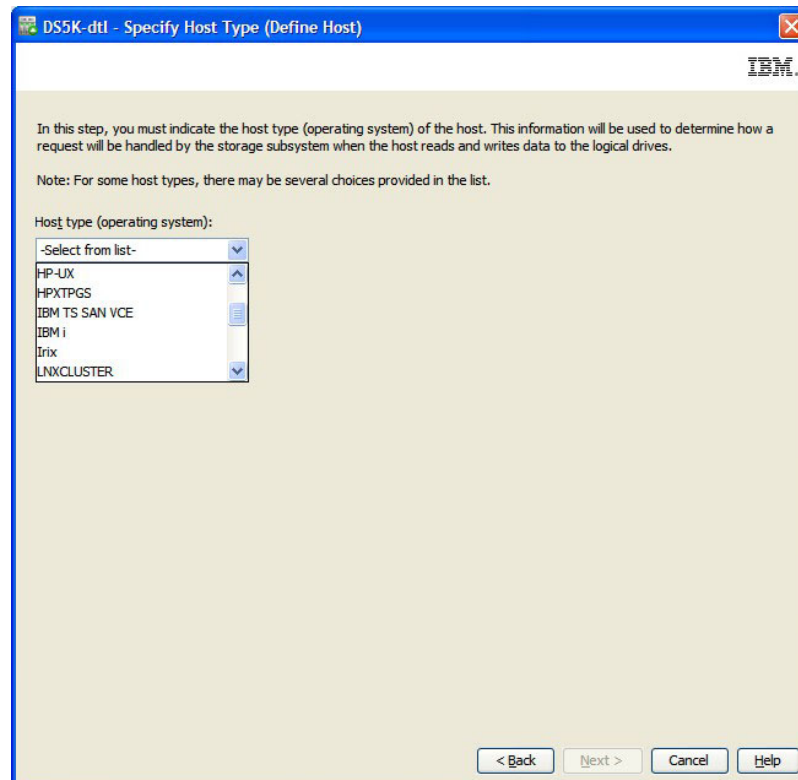


図 11. ホスト・タイプとしての **IBM i** の選択

オプションのプレミアム・フィーチャーの構成および使用

このセクションでは、FlashCopy、VolumeCopy、Enhanced FlashCopy、リモート・ミラー、およびフル・ディスク暗号化などのオプションのプレミアム・フィーチャーについて説明します。

注: これらのオプションのプレミアム・フィーチャーについて詳しくは、「*IBM System Storage DS Storage Manager Copy Services User's Guide*」を参照するか、IBM 販売店または IBM 営業担当員にお問い合わせください。

Enhanced FlashCopy の概要

コントローラー・ファームウェア・バージョン 7.8x.xx.xx 以降が搭載された DS ストレージ・マネージャーは、Enhanced FlashCopy 機能を提供します。この機能を使用すると、標準論理ドライブまたはシン論理

ドライブの特定時点の内容の論理コピーを作成できます。これらの論理ドライブの特定時点のイメージは、Enhanced FlashCopy イメージと呼ばれます。Enhanced FlashCopy イメージを作成すると、特定時点の既知の正常なデータ・セットまでロールバックできるようにする必要がある場合に役立ちます。例えば、リカバリ操作中に使用できるバックアップの 1 つとして、Enhanced FlashCopy イメージを作成することができます。基本論理ドライブの Enhanced FlashCopy イメージは、Enhanced FlashCopy グループのメンバーとして管理されます。1 つの Enhanced FlashCopy グループには最大 32 個の Enhanced FlashCopy イメージを含めることができ、1 つの基本論理ドライブは最大 4 つの Enhanced FlashCopy グループを作成できます。

論理ドライブの Enhanced FlashCopy イメージを作成すると、DS ストレージ・マネージャーはその Enhanced FlashCopy イメージを、Enhanced FlashCopy グループに関連付けられたリポジトリに保存します。Enhanced FlashCopy グループ・リポジトリ内に格納された Enhanced FlashCopy イメージへのホスト・アクセスを提供するには、その Enhanced FlashCopy イメージの Enhanced FlashCopy 論理ドライブを作成する必要があります。

Enhanced FlashCopy イメージ、Enhanced FlashCopy グループ、および Enhanced FlashCopy 論理ドライブの間の関係について、念頭に置く必要がある重要な詳細事項を以下にいくつか示します。

- 各 Enhanced FlashCopy イメージは、正確に 1 つの Enhanced FlashCopy グループとの関連で作成されます。
- 1 つの Enhanced FlashCopy グループは、1 つの関連付けられた標準論理ドライブまたはシン論理ドライブの一連の Enhanced FlashCopy イメージです。Enhanced FlashCopy イメージを作成するために使用される論理ドライブは、基本論理ドライブと呼ばれます。
- 1 つの Enhanced FlashCopy グループは、その Enhanced FlashCopy グループの一部である Enhanced FlashCopy イメージを保存するために使用する、正確に 1 つのリポジトリを持っています。
- 1 つの Enhanced FlashCopy グループ・リポジトリ内のすべての Enhanced FlashCopy イメージは、その Enhanced FlashCopy グループと直接関連があります。
- 1 つの Enhanced FlashCopy グループは、1 つの論理ドライブと関連があります。
- 各 Enhanced FlashCopy 論理ドライブは、1 つの Enhanced FlashCopy イメージと直接関連があります。
- 各 Enhanced FlashCopy 論理ドライブは、その Enhanced FlashCopy 論理ドライブが最初に作成されたときの Enhanced FlashCopy イメージの基本論理ドライブと永続的な関係があります。
- Enhanced FlashCopy 論理ドライブに関連付けられたリポジトリは、1 つの Enhanced FlashCopy グループと関連があります。

FlashCopy の概要

FlashCopy 論理ドライブとは、基本論理ドライブと呼ばれる論理ドライブの特定時点における論理的なイメージです。FlashCopy 論理ドライブには、以下のような特徴があります。

- 短時間で作成され、必要なディスク・スペースが実際の論理ドライブほど大きくありません。
- 基本論理ドライブがオンラインでアクセス可能な状態のときには FlashCopy 論理ドライブを使用してバックアップを実行できるよう、ホスト・アドレスを割り当てることができます。
- FlashCopy 論理ドライブを使用すると、アプリケーションのテストまたは開発と分析の両方のシナリオを実行できます。実際の実稼働環境には影響を与えません。
- 許可される FlashCopy 論理ドライブの最大数は、コントローラー・モデルでサポートされている論理ドライブ総数の半分です。

注: ストレージ・サブシステムでは、FlashCopy 機能と Enhanced FlashCopy 機能を同時に使用できます。ただし、各基本論理ドライブでは、FlashCopy または Enhanced FlashCopy のどちらかを使用できますが、

両方を使用することはできません。

FlashCopy 機能および FlashCopy 論理ドライブの管理方法に関する追加情報については、ストレージ・マネージャーの「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプを参照してください。

重要: Windows 2000、Windows Server 2003、または NetWare の環境では、FlashCopy 論理ドライブの基本論理ドライブが存在している同じサーバーに、FlashCopy ドライブを追加またはマップすることはできません。FlashCopy 論理ドライブを別のサーバーにマップする必要があります。

FlashCopy 論理ドライブを作成するには、以下の手順を実行します。

1. 基本論理ドライブの正確な特定時点イメージが作成されるようにするため、アプリケーションを停止し、キャッシュ I/O を基本論理ドライブにフラッシュする。
2. 「Subsystem Management (サブシステム管理)」ウィンドウを開く。「Logical (論理)」ページで、基本論理ドライブを右クリックします。
3. 「**Create FlashCopy Logical Drive (FlashCopy 論理ドライブの作成)**」を選択する。「Create FlashCopy Logical Drive (FlashCopy 論理ドライブの作成)」ウィザードが開始されます。
4. 画面の指示に従う。
5. FlashCopy 論理ドライブをホストに追加する手順については、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプを参照してください。

VolumeCopy の使用

VolumeCopy 機能は、ストレージ・サブシステム内の論理ドライブ・データを複製するための、ファームウェア・ベースのメカニズムです。この機能は、ハードウェアのアップグレードやパフォーマンス管理のためにデータを他のドライブに再配置したり、データをバックアップしたり、スナップショット論理ドライブ・データを復元したりするタスク用のシステム管理ツールとして設計されています。互換性のある 2 つのドライブを指定して、VolumeCopy の要求を実行依頼します。一方のドライブをソースとして指定し、他方のドライブをターゲットとして指定します。コピー処理に関連して生じるすべての結果をユーザーに通知できるよう、VolumeCopy 要求は終了しないで保持されます。この機能について詳しくは、IBM 販売店または営業担当員にお問い合わせください。

拡張リモート・ミラーリングの使用

拡張リモート・ミラーリングは、プレミアム・フィーチャーであり、別々の場所にあるストレージ・サブシステム間でオンラインかつリアルタイムでデータを複製するために使用されます。リモート・ミラー・オプションを使用することで、1 番目のストレージ・サブシステムに障害が起きた場合に、2 番目のストレージ・サブシステムが正常な入出力操作を処理するように指定できます。この機能について詳しくは、「*IBM System Storage DS ストレージ・マネージャー バージョン 10 コピー・サービスのユーザー・ガイド*」を参照するか、または IBM 販売店または営業担当員にお問い合わせください。

拡張グローバル・ミラーリングの使用

拡張グローバル・ミラーリングは、プレミアム・フィーチャーであり、非同期シナリオでローカル・サイトとリモート・サイト間のデータ複製に使用されます。この機能では、低コストのファブリック接続 (iSCSI) が使用でき、1 次論理ドライブで一時的イメージを作成します。この機能では、2 次論理ドライブと定期的に同期することで、ピーク時における非高速ネットワークへのシステム・パフォーマンスの影響を最小限に

します。この機能について詳しくは、「*IBM System Storage DS ストレージ・マネージャー バージョン 10 コピー・サービスのユーザー・ガイド*」を参照するか、または IBM 販売店または営業担当員にお問い合わせください。

パフォーマンス読み取りキャッシュの使用

パフォーマンス読み取りキャッシュ (Performance Read Cache) は、プレミアム・フィーチャーであり、論理ドライブから直近に読み取ったデータをキャッシュするために使用されます。この機能を使用すると、キャッシュされたデータのデータ読み取りスループットが著しく増加します。使用に関して、追加の設定や管理は不要です。パフォーマンス読み取りキャッシュのサイズは、インストールされたコントローラーのキャッシュ・サイズによって決定されます。

注: 現在、この機能は、ソリッド・ステート・ドライブを装備した DS3500 および DCS3700 ストレージ・サブシステムでサポートされます。

表 18. インストールされたコントローラー・キャッシュごとにサポートされるパフォーマンス読み取りキャッシュの最大サイズ

インストールされたコントローラー・キャッシュ・サイズ	サポートされるパフォーマンス読み取りキャッシュの最大サイズ (コントローラーごと)
1 GB	1 TB
2 GB	2 TB
4 GB	4 TB
>4 GB	5 TB

フル・ディスク暗号化の使用

フル・ディスク暗号化 (FDE) は、ストレージ・サブシステムから物理的に取り外されたドライブ上のデータへの無許可アクセスを防止するプレミアム・フィーチャーです。ストレージ・サブシステム内のコントローラーは、セキュリティ・キーを持っています。セキュア・ドライブは、正しいセキュリティ・キーを持つコントローラーを介してのみデータへのアクセスを提供します。FDE は、ストレージ管理ソフトウェアのプレミアム・フィーチャーで、ユーザーまたはストレージのベンダーが使用可能にする必要があります。

注: すべての DS ストレージ・サブシステムが FDE をサポートするわけではありません。ご使用のストレージ・サブシステムの発表レターまたは「インストール、メンテナンスおよびユーザーのガイド」を調べて、ご使用のストレージ・サブシステムで FDE がサポートされているかどうかを判別してください。

FDE プレミアム・フィーチャーは、セキュリティ対応ドライブを必要とします。セキュリティ対応ドライブは、書き込み操作時にデータを暗号化して、読み取り操作時にデータを暗号化解除します。セキュリティ対応ドライブごとに固有のドライブ暗号鍵があります。

セキュリティ対応ドライブからセキュア・アレイを作成すると、そのアレイ内のドライブはセキュリティが有効になります。セキュリティ対応ドライブのセキュリティが有効になった場合、ドライブはデータの読み取りまたは書き込みのために、正しいセキュリティ・キーを入手する必要があります。セキュリティ対応ドライブは、セキュリティ有効になるまでは他のドライブと同じように動作します。

FDE の構成方法および使用方法については、205 ページの『第 6 章 フル・ディスク暗号化の処理』を参照してください。

その他の機能の使用

このセクションでは、ストレージ・マネージャーで使用可能なその他の機能について説明します。

コントローラーのキャッシュ・メモリーの使用

書き込みキャッシュによって、コントローラーのキャッシュ・メモリーに、ホスト・コンピューターからの書き込み操作を保管することができます。これにより、システム・パフォーマンスが向上します。ただし、コントローラーのキャッシュにまだ論理ドライブに転送されていないユーザー・データがあるときに、コントローラーに障害が発生する可能性があります。また、まだ書き込みが済んでいないデータがあるときに、キャッシュ・メモリーに障害が発生する可能性もあります。書き込みキャッシュ・ミラーリングを使用することによって、これらの障害の可能性からシステムを保護することができます。書き込みキャッシュ・ミラーリングでは、キャッシュ・サイズが同じ 2 つの冗長コントローラーにキャッシュ・データをミラーリングすることができます。片方のコントローラーのキャッシュ・メモリーに書き込まれたデータは、もう一方のコントローラーのキャッシュ・メモリーにも書き込まれます。つまり、一方のコントローラーに障害が発生した場合には、そのとき未処理になっている書き込み操作はすべて、もう一方のコントローラーによって完了されます。

注: それぞれの論理ドライブごとに書き込みキャッシュ・ミラーリング・パラメーターを使用可能にできます。ただし、書き込みキャッシュ・ミラーリングを使用可能にすると、各コントローラーでは、合計キャッシュ・サイズの半分がもう一方のコントローラーからのキャッシュ・データのミラーリング用に予約済みになります。

コントローラーは、データの損失または損傷を防ぐために、定期的にキャッシュ・データを論理ドライブに書き込みます。キャッシュに保持されている未書き込みデータが指定の開始パーセントに達すると、コントローラーは、キャッシュ・データを論理ドライブに書き込みます。キャッシュがフラッシュされ、指定した停止パーセントにまで下がると、フラッシュが停止します。例えば、論理ドライブのデフォルトの開始設定は合計キャッシュ・サイズの 80% であり、停止設定は 20% です。この設定では、コントローラーは、キャッシュが 80% に達するとキャッシュ・データのフラッシュを開始し、キャッシュがフラッシュされて 20% に下がると、フラッシュを停止します。

データの安全性を最大限に確保するには、低い開始パーセントと停止パーセントを選択します。例えば、開始設定に 25%、停止設定に 0% を選択します。ただし、開始設定と停止設定が低い場合、ホスト・コンピューターによる読み取りに必要なデータがキャッシュ内にないという状況が生じる可能性が高まります。キャッシュ内に十分なデータがない場合、キャッシュ・ヒット率が低くなるため、入出力要求速度も低くなります。また、これにより、キャッシュ・レベルの維持に必要なディスク書き込み回数が多くなるため、システム・オーバーヘッドが増え、パフォーマンスがさらに低下します。

電源異常が発生した場合、論理ドライブに書き込まれていないキャッシュ内のデータは、両方のコントローラーのキャッシュ・メモリーにミラーリングされている場合でも失われます。そのため、コントローラー・エンクロージャーには、電源異常からキャッシュを保護するバックアップ・バッテリーが備わっています。

注: DS4000 ストレージ・サブシステム DS4100、DS4300、および DS4400 の全モデルについてのみ、コントローラーのバックアップ・バッテリー CRU の交換間隔は、バックアップ・バッテリー CRU を取り付けた日付から 3 年になります。その他の DS4000 ストレージ・サブシステムのキャッシュ・バッテリー・バックアップ CRU には交換期間はありません。

ストレージ・マネージャー・ソフトウェアには、バッテリーの交換時期を設定できるバッテリー存続期間クロックが備えられています。このクロックによって、バッテリーの存続期間（日付単位）が追跡されるため、バッテリーの交換時期が分かります。

注:

1. DS4100、および DS4300 または DS4300 ターボ・ディスク・システムの場合、バッテリー CRU は各コントローラー CRU の内部にあります。
2. DS4800、DS5100、および DS5300 の場合、バッテリー CRU は相互接続されたバッテリー CRU の内部にあります。書き込みキャッシュは、バッテリーが少なくなったり放電した場合には使用不可になります。論理ドライブで「write-caching without batteries (バッテリーを使用しない書き込みキャッシュ)」と呼ばれるパラメーターを使用可能にすると、コントローラー・エンクロージャーのバッテリーを取り外しても書き込みキャッシュは継続されます。

重要: データ保全性を最大限に確保するには、「write-caching without batteries (バッテリーを使用しない書き込みキャッシュ)」パラメーターを使用可能にしないでください。コントローラー・エンクロージャーに稼働中のバッテリーがないと、電源異常が発生した場合にキャッシュ内のデータが失われてしまうからです。IBM サービス部門に連絡して、できるだけ早くバッテリーを交換し、ストレージ・サブシステムが書き込みキャッシュ使用不可のまま稼働する時間を最小限に抑えるようにしてください。

永続的予約の使用

重要: 永続的予約オプションは、IBM 技術サポート担当員によるガイダンスがあった場合にのみ使用してください。

永続的予約オプションを使用すると、論理ドライブの予約や関連した登録を表示および消去することができます。永続的予約は、クラスター・サーバー・ソフトウェアを使用して構成および管理します。永続的予約によって、他のホストが特定の論理ドライブにアクセスできないようにすることができます。

他のタイプの予約とは異なり、永続的予約は、以下の機能を実行する場合に使用されます。

- 複数のホスト・ポートへのアクセスの予約、およびさまざまなレベルのアクセス制御の提供
- ストレージ・サブシステムに登録済みのポートおよび予約の照会
- ストレージ・システムの電源遮断時における予約の永続性の提供

ストレージ・マネージャー・ソフトウェアを使用すると、「Subsystem Management (サブシステム管理)」ウィンドウで永続的予約を管理することができます。永続的予約オプションを使用して、以下のタスクを実行できます。

- ストレージ・サブシステムのすべての論理ドライブに関する登録および予約情報の表示
- 論理ドライブの予約および登録に関する詳細情報の保存
- ストレージ・サブシステムの単一論理ドライブまたはすべての論理ドライブに対するすべての登録および予約の消去

手順について詳しくは、「Subsystem Management (サブシステム管理)」ウィンドウのオンライン・ヘルプを参照してください。永続的予約は、スクリプト・エンジンおよびコマンド行インターフェースを使用して管理することもできます。詳しくは、「Enterprise Management (エンタープライズ管理)」ウィンドウのオンライン・ヘルプを参照してください。

メディア・スキンの使用

メディア・スキン は、この機能が使用可能になっているストレージ・サブシステム内のすべての論理ドライブ上で実行されるバックグラウンド・プロセスで、ドライブ・メディア上でのエラー検出機能を提供します。メディア・スキン機能では、ディスクの生データを読み取ることにより物理ディスクに問題がないかどうかを調べます。エラーを検出した場合は、このエラーを書き込みます。メディア・スキンを使用可

能にすると、論理ドライブの正常な読み取りおよび書き込み機能を妨害するようなメディア・エラーがこのプロセスによって事前に検出されるという利点があります。メディア・スキャン・プロセスでは、すべての論理ドライブ・データをスキャンして、データがアクセス可能であるかどうかを検証します。

注: バックグラウンド・メディア・スキャン操作では、ホット・スペア・ドライブまたは未使用の最適なハード・ディスク (定義済み論理ドライブの一部ではないドライブ) はスキャンしません。ホット・スペア・ドライブまたは未使用の最適なハード・ディスクでメディア・スキャン操作を実行するには、スケジュールされている特定の間隔でこれらのドライブを論理ドライブに変換し、スキャンを実行した後に、これらのドライブを再度ホット・スペア状態または未使用状態に戻す必要があります。

メディア・スキャンを実行するには、以下の 2 つの方法があります。

論理ドライブの冗長検査を使用可能にしない

バックグラウンド・メディア・スキャンを使用可能にして、論理ドライブの冗長データ検査は使用可能にしなかった場合、ストレージ・サブシステムは、冗長ブロックを含め論理ドライブ内のすべてのブロックをスキャンしますが、冗長データが正確であるかどうかについては検査しません。

この設定は、ストレージ・マネージャーを使用して論理ドライブを作成する場合のデフォルト設定です。

論理ドライブの冗長検査を使用可能にする

バックグラウンド・メディア・スキャンを使用可能にして、論理ドライブの冗長データ検査を RAID-3、RAID-5、または RAID-6 論理ドライブに対して使用可能にした場合、冗長データ検査では、データ・ブロックをスキャンし、冗長データを計算して、各ブロックについて読み取られた冗長情報と比較します。次に、必要に応じて冗長エラーを修復します。RAID-1 論理ドライブの場合、冗長データ検査では、ミラーリングされたドライブ上のデータ・ブロックを比較して、データの不整合があるときはこれを訂正します。

この設定を、以前の DS ストレージ・サブシステム (DS4500、DS4400、DS4300、または DS4100 など) で使用しないでください。冗長検査はストレージ・サブシステムのパフォーマンスにマイナスの影響を与えます。

新しいストレージ・サブシステム (DS5100、DS5300、DS5020、または DS3950 など) では、この設定は性能低下を引き起こしません。

メディア・スキャンを使用可能にすると、ストレージ・サブシステム内の以下の条件を満たすすべての論理ドライブでメディア・スキャンが実行されます。

- 論理ドライブが最適の状態である。
- 変更操作が進行中ではない。
- メディア・スキャン・パラメーターが使用可能になっている。

注: メディア・エラーによる障害から論理ドライブを保護するためには、ストレージ・サブシステム全体に対して、およびストレージ・サブシステム内の各論理ドライブ上で、メディア・スキャンを使用可能にする必要があります。

メディア・スキャンでは、問題が発生しない限り、データ・ストライプのみを読み取ります。ストライプ内のブロックを読み取ることができない場合、読み取りコマンドが特定の回数だけ再試行されます。読み取りが引き続き失敗する場合、コントローラーは、このブロックの本来の状態を計算し、このストライプに対して書き込みおよび検証コマンドを発行します。ディスクがこの書き込みコマンドを実行しようとしたときにブロックが書き込み不可能であった場合、ドライブは、データの書き込みが可能になるまでセクターの再割り振りを行います。ドライブから書き込みの成功が報告されると、メディア・スキャンが再度読み取りを行って検査します。ストライプには追加の問題があってはなりません。追加の問題がある場合は、書き込みが

成功するか、または連続して書き込みが失敗した結果としてドライブに障害が発生してホット・スペア・ドライブが処理を引き継ぐまで、上記のプロセスが繰り返されます。修復は、書き込みが成功した場合にのみ行うことができ、修復を行うのはドライブです。コントローラーは、書き込みおよび検証コマンドを発行するだけです。したがって、データ・ストライプの読み取りが繰り返して行われ、無効なセクターが報告されますが、コントローラーでは RAID を使用して欠落情報を計算します。

デュアル・コントローラー・ストレージ・サブシステムには、入出力を処理する 2 つのコントローラー (コントローラー A および B) があります。作成した各論理ドライブには、通常時にその論理ドライブの入出力を処理する優先コントローラーがあります。コントローラーに障害が発生すると、障害が発生したコントローラーが所有していた 論理ドライブの入出力は、もう一方のコントローラーにフェイルオーバーされます。メディア・スキャン入出力は、コントローラーの障害による影響を受けません。アクティブなコントローラーが 1 つしか残っていない場合でも、使用可能なすべての論理ドライブでスキャンが継続されます。

メディア・スキャン・プロセスの実行中にエラーが原因でドライブに障害が発生した場合、コントローラーのオペレーティング・システムで通常の再構成タスクが開始され、メディア・スキャンは、ホット・スペア・ドライブを使用してアレイを再構成しようとします。この再構成プロセスが実行されている間は、アレイに対するメディア・スキャン・プロセスはもう行われません。

注: メディア・スキャン用の追加の入出力読み取りが生成されるため、以下の要因に応じてパフォーマンスへの影響がある場合があります。

- ストレージ・サブシステムでの構成済みの記憶容量ストレージ・サブシステムでの構成済みの記憶容量が大きいほど、パフォーマンスへの影響も大きくなります。
- メディア・スキャン操作について構成済みのスキャン期間。スキャン期間が長いほど、パフォーマンスへの影響が少なくなります。
- 冗長検査オプションの状況 (使用可能または使用不可) 冗長検査を使用可能にした場合、パフォーマンスへの影響が大きくなります。

メディア・スキャンにより報告されるエラー

メディア・スキャン・プロセスは、使用可能にした場合はバックグラウンドで継続的に実行されます。ストレージ・サブシステム内のすべての論理ドライブのメディア・スキャンが完了するたびに、スキャンが即時に再開します。メディア・スキャン・プロセスでは、エラーが検出され、ストレージ・サブシステムのメジャー・イベント・ログ (MEL) にこれらのエラーが報告されます。次の表に、メディア・スキャンの実行時に検出されるエラーをリストします。

表 19. メディア・スキャン中に検出されるエラー

エラー	説明	結果
未回復メディア・エラー	ドライブは、最初の試行でも後続の試行でも、データを読み取ることができませんでした。	冗長保護されている論理ドライブまたはアレイ (RAID-1、RAID-3、および RAID-5) の場合、データは再構成されてドライブに書き込まれ、検証されます。エラーはイベント・ログに報告されます。 冗長保護されていない論理ドライブまたはアレイ (RAID-0、低下 RAID-1、RAID-3、RAID-5、および RAID-6 論理ドライブ) の場合、エラーは訂正されませんが、イベント・ログに報告されます。
回復済みメディア・エラー	ドライブは、最初の試行でデータを読み取ることができませんでした。後続の試行ではデータの読み取りに成功しました。 注: メディア・スキャンでは、不良ブロックの読み取りが 3 回試行されます。	データは、ドライブに再書き込みされ、検証されます。エラーはイベント・ログに報告されます。
冗長不一致	冗長エラーが検出されました。 注: このエラーが発生する可能性があるのは、オプションの冗長チェック・ボックスが選択されて、メディア・スキャン機能が使用可能になっており、論理ドライブまたはアレイが RAID-0 ではない場合のみです。	論理ドライブ上で検出された最初の 10 件の冗長不一致が、イベント・ログに報告されます。
修正不能エラー	データの読み取りができず、データを再生成するためのパリティまたは冗長情報が使用できません。例えば、機能低下した論理ドライブ上のデータを再構成するために、冗長情報を使用することができません。	エラーはイベント・ログに報告されます。

メディア・スキャン設定

最大限の保護を確保し、入出力パフォーマンスへの影響を最小限に抑えるために、ストレージ・サブシステムは、メディア・スキャンが以下のデフォルトに設定された状態で製造メーカーから出荷されます。

- メディア・スキャン・オプションは、ストレージ・サブシステムのすべての論理ドライブに対して使用可能になっています。したがって、論理ドライブを作成すると、常に、メディア・スキャン・オプションが使用可能になった状態で論理ドライブが作成されます。メディア・スキャンを使用不可にするには、それぞれの論理ドライブごとに手動で使用不可にする必要があります。
- メディア・スキャン期間は、30 日に設定されています。ストレージ・サブシステム・コントローラーは、この期間内に論理ドライブのメディア・スキャンを完了する必要があります。コントローラーは、メディア・スキャン期間、およびスキャンの対象となる論理ドライブについての情報を使用して、メディア・スキャン・アクティビティーを実行する一定の間隔を決定します。メディア・スキャン期間は、ホストの入出力アクティビティーに関係なく維持されます。

30 日は、設定できる最大期間です。もっと頻繁にメディアをスキャンするには、この値を手動で変更する必要があります。この設定は、ストレージ・サブシステムのすべての論理ドライブに適用されます。

例えば、1 つの論理ドライブのメディア・スキャン期間を 2 日に設定し、その他の論理ドライブのメディア・スキャン期間を 30 日に設定することはできません。

- 7.60.39.00 より前のコントローラー・ファームウェア・バージョンでは、デフォルトで冗長検査オプションが使用可能になっていません。7.60.39.00 より前のコントローラー・ファームウェア・バージョンの場合、このオプションは、冗長データの検査対象とする論理ドライブごとに、手動で設定する必要があります。

7.60.39.00 以降のコントローラー・ファームウェア・バージョンの場合、新たに作成される任意の論理ドライブに対して、冗長検査オプションはデフォルト設定として使用可能になります。7.60.39.00 以降のバージョンをインストールする前に作成された既存の論理ドライブで冗長検査オプションを使用可能にしたい場合、手動でそのオプションを使用可能にする必要があります。

冗長検査を使用可能にしていない場合、コントローラーは、データ・ストライプを読み取ってすべてのデータが読み取り可能かどうかを確認します。すべてのデータを読み取ると、コントローラーは、そのデータを破棄して次のストライプに移動します。読み取れないデータ・ブロックがあった場合、コントローラーは、残りのブロックおよびパリティ・ブロックからデータを再構成し、読み取れなかったブロックに対して、書き込みおよび検証コマンドを発行します。ブロックにデータ・エラーがなかった場合、メディア・スキャンは、更新済み情報を受け取ってブロックが修正済みであるかどうかを検証します。ブロックの再書き込みができない場合、ドライブは、データを受け取る別のブロックを割り振ります。データが正常に書き込まれた場合は、コントローラーは、ブロックが修正済みであるかどうかを検証して次のストライプに移動します。

注: 冗長検査を行う場合、メディア・スキャンでは冗長検査を行わない場合と同じプロセスが実行されますが、パリティ・ブロックの再計算と検証が追加で行われます。パリティにデータ・エラーがある場合、パリティの再書き込みが行われます。パリティ・データの再計算と比較には追加の入出力が必要となります。そのため、パフォーマンスに影響を与える可能性があります。

重要: メディア設定に加えた変更は、現行のメディア・スキャン・サイクルが完了した後でなければ有効にはなりません。

ストレージ・サブシステム全体のメディア・スキャン設定を変更するには、以下のステップを実行します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「Logical(論理)」タブまたは「Physical (物理)」タブで、ストレージ・サブシステム項目を選択する。
2. 「Storage Subsystem (ストレージ・サブシステム)」 > 「Change (変更)」 > 「Media Scan Settings (メディア・スキャン設定)」の順にクリックする。

論理ドライブのメディア・スキャン設定を変更するには、以下のステップを完了します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「Logical(論理)」タブまたは「Physical (物理)」タブで、論理ドライブ項目を選択する。
2. 「Storage Subsystem (ストレージ・サブシステム)」 > 「Change (変更)」 > 「Media Scan Settings (メディア・スキャン設定)」の順にクリックする。

メディア・スキャン期間

メディア・スキャンを使用可能にした場合は、期間帯を (日数で) 指定します。この期間帯は、該当のすべての論理ドライブを検査するために、ストレージ・サブシステムがメディア・スキャン・プロセスに与える期間を示します。期間帯は、お客様の要件に合わせて短縮することも延長することもできます。期間が短いほど、ドライブのスキャンが頻繁に行われるので、より堅固な状態を実現できます。ただし、ドライブのスキャンが頻繁になるほど、パフォーマンスへの影響も大きくなります。

ストレージ・サブシステムにアイドル時間が生じた場合は常に、メディア・スキャン操作が開始または継続されます。アプリケーションで生成されたディスク入出力処理要求を受け取ると、その処理が優先されます。したがって、メディア・スキャン・プロセスは、処理要求の変化に応じてスローダウンしたり、高速になったり、場合によっては中断されたりします。ストレージ・サブシステムが大量のアプリケーション生成ディスク入出力を受け取った場合は、メディア・スキャンのスキャン操作が遅れる可能性があります。ストレージ・サブシステムがメディア・スキャンを終了すべき期間帯の終わりが近づくにつれて、バックグラウンド・アプリケーションの優先順位が上がり始めます (つまり、メディア・スキャン・プロセス専用に使われる時間が増えます)。ストレージ・サブシステムではアプリケーション生成のディスク入出力の処理が優先されるので、これは一定レベルの優先順位までしか上がりません。この場合、メディア・スキャン期間がその設定値より長くなる可能性もあります。

注: メディア・スキャン期間の設定を変更した場合、現行のメディア・スキャン・サイクルが完了するか、またはコントローラーがリセットされるまで、変更は有効になりません。

ストレージ・サブシステムのチューニング

このセクションの情報では、パフォーマンス・モニター・データ、およびストレージ・サブシステムとアプリケーションのパフォーマンスを最適化するためにストレージ・マネージャーで利用できるチューニング・オプションについて説明します。リアルタイムでストレージ・サブシステムのパフォーマンスをモニターし、パフォーマンス・データをファイルに保存して後で分析する場合は、「Subsystem Management (サブシステム管理)」ウィンドウのパフォーマンス・モニターを使用します。モニター対象の論理ドライブとコントローラー、およびポーリング間隔を指定することができます。ストレージ・サブシステムの合計値を受け取ることもできます。この合計値とは、アクティブ/アクティブ接続のコントローラー・ペアの両コントローラーの統計を結合したデータです。

表 20. 「Subsystem Management (サブシステム管理)」ウィンドウのパフォーマンス・モニター・チューニング・オプション

データ・フィールド	説明
Total I/Os (入出力の合計)	ポーリング・セッションの開始以降にこのデバイスが実行した入出力の合計数
Read percentage (読み取り率)	このデバイスに対する読み取り操作が入出力合計に占める割合。書き込み率を計算するには、100 からこの値を引きます。
Cache-hit percentage (キャッシュ・ヒット率)	論理ドライブからの読み取りを必要とせず、キャッシュからのデータを使用して処理された読み取り操作の割合。
Current KB per second (現行 KB/秒)	転送速度 は、ポーリング間隔の間に、ファイバー・チャネルの入出力パスを経由して 1 秒間に移動したデータ量 (KB) です (スループットともいいます)。
Maximum KB per second (最大 KB/秒)	パフォーマンス・モニターのポーリング・セッション中に達成された最大転送速度。
Current I/O per second (現行入出力/秒)	現行のポーリング間隔の間に、毎秒処理される入出力要求の平均数 (入出力要求速度ともいいます)。
Maximum I/O per second (最大入出力/秒)	ポーリング・セッション全体に渡り、1 秒間の間隔中に処理される入出力要求の最大数。

ロード・バランシングによるスループットの最大化

ロード・バランシングとは、サーバーとストレージ・サブシステム間のスループットを最大化するために読み取り要求および書き込み要求を再分配することです。ロード・バランシングは、高い作業負荷の設定など、一貫性のあるサービス・レベルが不可欠な場合に非常に重要です。マルチパス・ドライバは、管理者の介入を必要とせずに、透過的に入出力ワークロードのバランスを取ります。マルチパス・ソフトウェアを

使用しない場合、入出力要求を複数のパスに送信するサーバーは、一部のパスに重い作業負荷がかかる一方で、他のパスは効率的に使用されない状態で稼働する可能性があります。

マルチパス・ドライバーは、1 つのデバイスへの複数のパスについて、どのパスがアクティブ状態にあり、ロード・バランシングのために使用できるかを判別します。ロード・バランシング・ポリシーは、ラウンドロビン、最小キュー項目数、最小パス重み の 3 つのアルゴリズムのいずれかを使用します。混合ホスト・インターフェースが構成されている場合、ロード・バランス・ポリシーを設定するための複数のオプションを使用して、入出力パフォーマンスを最適化することができます。選択できるロード・バランシング・ポリシーは、オペレーティング・システムによって異なります。ロード・バランシングは、同じコントローラーへの複数のパスに対して実行されますが、両方のコントローラー間に渡っては実行されません。

表 21. オペレーティング・システムでサポートされるロード・バランシング・ポリシー

オペレーティング・システム	マルチパス・ドライバー	ロード・バランシング・ポリシー
AIX	MPIO	ラウンドロビン、選択可能パス優先順位
Red Hat Enterprise Linux 4 Update 7	RDAC	ラウンドロビン、最小キュー項目数
Solaris	MPxIO	ラウンドロビン
SUSE Linux Enterprise 9 Service Pack 4	RDAC	ラウンドロビン、最小キュー項目数
Windows	MPIO	ラウンドロビン、最小キュー項目数、最小パス重み

サブセット付きラウンドロビン

サブセット付きラウンドロビン方式の入出力ロード・バランシング・ポリシーは、論理ドライブを所有するコントローラーへの使用可能な各データ・パスに対して、順番に、入出力要求を経路指定します。このポリシーは、論理ドライブを所有するコントローラーへのすべてのパスを入出力アクティビティーのために平等に取り扱います。2 次コントローラーへのパスは、所有権が変更されるまで無視されます。ラウンドロビン・ポリシーの基本的な前提は、すべてのデータ・パスが同等であるということです。混合ホストをサポートしている場合、データ・パスは異なる帯域幅あるいは異なるデータ転送速度を持っている可能性があります。

サブセット付き最小キュー項目数

サブセット付き最小キュー項目数ポリシーは、最小入出力数または最小要求数ポリシーとも呼ばれます。このポリシーは、キューに入れられた未処理の入出力要求数が最小であるデータ・パスに、次の入出力要求を経路指定します。このポリシーの場合、入出力要求は、単にキューの中にあるコマンドだけです。コマンドのタイプやコマンドに関連付けられたブロックの数は考慮されません。サブセット付き最小キュー項目数ポリシーは、大規模なブロック要求と小規模なブロック要求を同等に扱います。選択されるデータ・パスは、論理ドライブを所有するコントローラーのパス・グループ内のパスの 1 つです。

サブセット付き最小パス重み

サブセット付き最小パス重みポリシーは、1 つの論理ドライブへの各データ・パスに重み係数を割り当てます。入出力要求は、論理ドライブを所有するコントローラーへの最低の重み値をもつパスに経路指定されます。その論理ドライブへの複数のデータ・パスが同じ重み値をもつ場合、同じ重み値をもつパス間での入出力要求の経路指定には、サブセット付きラウンドロビン方式のパス選択ポリシーが使用されます。

ファイバー・チャネルの入出力負荷の平衡化

「Subsystem Management (サブシステム管理)」ウィンドウの「**Total I/O (入出力の合計)**」データ・フィールドは、特定のコントローラーおよび特定の論理ドライブに対するファイバー・チャネルの入出力アクティビティをモニターするために使用します。このフィールドは、入出力ホット・スポットが発生する可能性を識別するのに役立ちます。

個々の論理ドライブに対するファイバー・チャネルの入出力パターンを識別し、アプリケーションに基づいてそれらを期待値と比較することができます。コントローラーへの入出力アクティビティが予想より多い場合は、「**Array (アレイ)**」 > 「**Change Ownership (所有権の変更)**」をクリックして、ストレージ・サブシステム内の他のコントローラーにアレイを移動します。

入出力負荷は絶えず変動するので、ファイバー・チャネルの入出力負荷をコントローラーおよび論理ドライブ全体にわたって平衡化するのは困難です。ポーリング・セッション中にアクセスされる論理ドライブおよびデータは、その期間の間にアクティブになっているアプリケーションおよびユーザーに応じて異なります。さまざまな時間枠でパフォーマンスをモニターし、定期的にデータを収集して、パフォーマンスの傾向を判別することが重要です。パフォーマンス・モニターを使用すると、データをコンマ区切りのテキスト・ファイルに保存し、それをスプレッドシートにインポートして、さらに詳しい分析を行うことができます。

ストレージ・サブシステム全体にわたる作業負荷 (ファイバー・チャネルの入出力統計の合計) が時間とともに増え続けるのに対し、アプリケーションのパフォーマンスが低下している場合は、ストレージ・サブシステムをエンタープライズに追加することが必要な場合があります。

入出力転送速度の最適化

コントローラーの転送速度は、アプリケーションの入出力サイズおよび入出力要求速度によって決まります。アプリケーションの入出力要求のサイズが小さい場合、転送速度は低下しますが、入出力要求速度が高速になり、応答時間が短くなります。アプリケーションの入出力要求サイズが大きくなると、より高いスループット率が可能になります。アプリケーションの入出力パターンを理解しておくと、特定のストレージ・サブシステムで可能な最大入出力転送速度を最適化するのに役立ちます。

入出力転送速度を向上させる方法の 1 つは、入出力要求速度を改善することです。ホスト・コンピューターのオペレーティング・システムのユーティリティを使用して、入出力サイズに関するデータを収集し、可能な最大転送速度を理解します。次に、ストレージ・マネージャーで使用可能なチューニング・オプションを使用して、到達可能な最大転送速度になるように入出力要求速度を最適化します。

入出力要求速度の最適化

入出力要求速度は、以下の要因により影響を受けます。

- 入出力アクセス・パターン (ランダムまたは順次) および入出力サイズ
- 書き込みキャッシュの状況 (使用可能または使用不可)
- キャッシュ・ヒット率
- RAID レベル
- 論理ドライブ変更優先順位
- セグメント・サイズ
- アレイまたはストレージ・サブシステム内の論理ドライブの数
- ファイルのフラグメント化

注: フラグメント化は、入出力アクセス・パターンが順次の場合は論理ドライブに影響しますが、入出力アクセス・パターンがランダムの場合は影響しません。

入出力アクセス・パターンおよび入出力サイズの決定

入出力アクセスが順次特性を持っているかどうかを判断するには、「**Logical Drive (論理ドライブ)**」 > 「**Properties (プロパティ)**」をクリックして、キャッシュ先読み乗数を控えめに (例えば 4 に) 設定します。次に、論理ドライブのキャッシュ・ヒット率を調べて、それが改善されたかどうかを確認します。改善が見られた場合は、その入出力パターンは順次パターンです。論理ドライブの標準的な入出力サイズを決定するには、ホスト・コンピュータのオペレーティング・システムのユーティリティを使用します。

書き込みキャッシュの使用可能化

書き込みキャッシュを使用可能にすると、入出力アクセス・パターンが順次の場合は特に、入出力書き込み速度が高速になります。入出力速度を最大にし、アプリケーションの応答時間を短くするために、入出力アクセス・パターンに関係なく、必ず書き込みキャッシュを使用可能にしてください。

キャッシュ・ヒット率の最適化

最適なアプリケーション・パフォーマンスを得るには、キャッシュ・ヒット率が高い方が望ましく、これとファイバー・チャンネルの入出力要求速度との間には正の相関関係があります。

すべての論理ドライブのキャッシュ・ヒット率が低いか、または下がる傾向を示しており、コントローラーに現在取り付けられているキャッシュ・メモリーの量が最大量より少ない場合は、メモリーの増設が必要になる可能性があります。

個々の論理ドライブのキャッシュ・ヒット率が低い場合、その論理ドライブのキャッシュ先読みを使用可能にすることができます。キャッシュ先読みにより、順次入出力ワークロードのキャッシュ・ヒット率が向上する可能性があります。キャッシュ先読みを使用可能にすると、キャッシュが (通常はドライブ上の隣接するデータ・ブロックから) 取り出すデータ量が増加します。この機能により、要求されたデータのみでなく、データに対する後続の要求もキャッシュからの入出力で処理できる確率が高くなり、したがって論理ドライブにアクセスする必要性が減少します。

キャッシュ先読み乗数の値は、どれだけの追加データ・ブロックをキャッシュに読み込むかを決定するために使用される乗数です。キャッシュ先読み乗数に大きい値を選択するほど、キャッシュ・ヒット率が向上します。

ファイバー・チャンネルの入出力へのアクセス・パターンが順次特性であることが判別できた場合は、キャッシュ先読み乗数を高めに (例えば 8 に) 設定してください。次に、論理ドライブのキャッシュ・ヒット率を調べて、その値が改善されているかどうかを見ます。最適な乗数に到達するまで、論理ドライブのキャッシュ先読みをカスタマイズしてください (入出力パターンがランダムの場合は、最適な乗数は 0 です)。

適切な RAID レベルの選択

アプリケーションの動作を判別するには、論理ドライブの読み取り率を使用します。読み取り率が高いアプリケーションは、RAID-5 の論理ドライブを使用すると優れたパフォーマンスを示します。これは、RAID-5 構成の読み取りパフォーマンスがきわめて優れているためです。

注: これは従来のアレイにのみ適用できます。ディスク・プールは常に RAID 6 および 8D+P+Q で作成されます。

読み取り率が低い (書き込みの比重が高い) アプリケーションの場合は、RAID-5 論理ドライブではパフォーマンスがよくありません。これは、コントローラーが、データおよび冗長データを RAID-5 論理ドライブ内のドライブに書き込むからです。書き込みアクティビティと比較して読み取りアクティビティの割合が低い場合には、論理ドライブの RAID レベルを RAID-5 から RAID-1 に変更すると、高速のパフォーマンスが得られます。

最適な論理ドライブ変更優先順位の設定の選択

変更優先順位は、論理ドライブの変更操作およびシステム・パフォーマンスのそれぞれに対して、どれだけの処理時間を割り振るかを定義するものです。優先順位が高いほど、論理ドライブの変更操作の完了は速くなりますが、システム入出力のアクセス・パターンへのサービス速度は低下します。

論理ドライブの変更操作には、再構成、コピーバック、初期化、メディア・スキャン、デフラグ、RAID レベルの変更、およびセグメント・サイズの変更があります。変更優先順位は、「Logical Drive - Properties (論理ドライブ - プロパティ)」ウィンドウのスライダー・バーを使用して、論理ドライブごとに設定します。再構成速度のスライダー・バーには、「Low (低)」から「Highest (最高)」までの範囲の 5 つの相対設定値があります。各設定値の実際の速度は、コントローラーによって決まります。ファイバー・チャネルの入出力要求速度を最大にするには、設定値として「Low (低)」を選択します。コントローラーは、アイドル状態になっている (どの入出力要求速度にもサービスを提供していない) 場合は、個々の論理ドライブの速度設定を無視して論理ドライブの変更操作を可能な限り高速に処理します。

アレイの最適なセグメント・サイズの選択

セグメントは、コントローラーがデータを次のドライブに書き込む前に、単一の論理ドライブに書き込むデータ量 (KB) です。データ・ブロックは 512 バイトのデータで、ストレージの最小単位です。セグメントのサイズにより、それに含まれるデータ・ブロック数が決まります。例えば、8 KB のセグメントは 16 個のデータ・ブロックを保持でき、64 KB のセグメントは 128 個のデータ・ブロックを保持できます。

注: ディスク・プールの場合、セグメント・サイズは常に 128 KB です。DS ストレージ・マネージャーのセグメント・サイズは、KB で表されます。

論理ドライブを作成する場合は、予想される論理ドライブの使用状況に対して、デフォルトのセグメント・サイズを選択するのもよい方法です。デフォルトのセグメント・サイズを変更するには、「**Logical Drive (論理ドライブ)**」 > 「**Change Segment Size (セグメント・サイズの変更)**」をクリックします。

入出力サイズがセグメント・サイズよりも大きい場合は、セグメント・サイズを増やして、入出力要求を満たすのに必要なドライブ数が最小になるようにしてください。この手法は、入出力アクセス・パターンがランダムの場合はさらに役立ちます。1 つの要求に対して 1 つの論理ドライブを使用すれば、その他の論理ドライブが解放され、その他の要求に同時にサービスを提供するために使用可能になります。

入出力が大きい単一ユーザー環境 (マルチメディア・アプリケーションなど) で論理ドライブを使用する場合は、単一のアレイ・データ・ストライプ (入出力要求に使用されるアレイ内の論理ドライブ数をセグメント・サイズに掛けた値) を使用して単一の入出力要求に対してサービスを提供すると、ストレージのパフォーマンスが最適になります。この場合、同一要求に対して複数の論理ドライブが使用されますが、各論理ドライブへのアクセスは一度だけです。

ファイルのデフラグによるディスク・アクセスの最小化

ドライブにアクセスしてファイルの読み取りやファイルへの書き込みを行うたびに、読み取り/書き込みヘッドが移動します。論理ドライブ上のファイルがデフラグされているかチェックしてください。ファイルがデフラグされていると、ファイルを構成しているデータ・ブロックが互いに隣接しており、ファイル検索時に読み取り/書き込みヘッドの余分な移動がなくなります。ファイルがフラグメント化されていると、順次入出力アクセス・パターンの論理ドライブの場合、パフォーマンスが低下します。

ストレージ・マネージャーのコマンド行インターフェースおよびスクリプト・エディターの使用

このセクションでは、ストレージ・マネージャーのコマンド行インターフェースおよびスクリプト・エディターについて説明します。

ストレージ・マネージャーのコマンド行インターフェース

重要: コマンド行インターフェース (CLI) には、誤ってストレージ・サブシステムに望ましくない変更を加えることを防止するためのメカニズムはありません。スクリプト・コマンドは、正しく使用されない場合、構成を損傷してデータ・アクセスの損失を引き起こす可能性があります。ストレージ構成またはデータに対する損傷の影響を回避するために、ストレージ・サブシステム構成の管理にはストレージ・マネージャー・クライアントのグラフィカル・ユーザー・インターフェース (GUI) を使用してください。

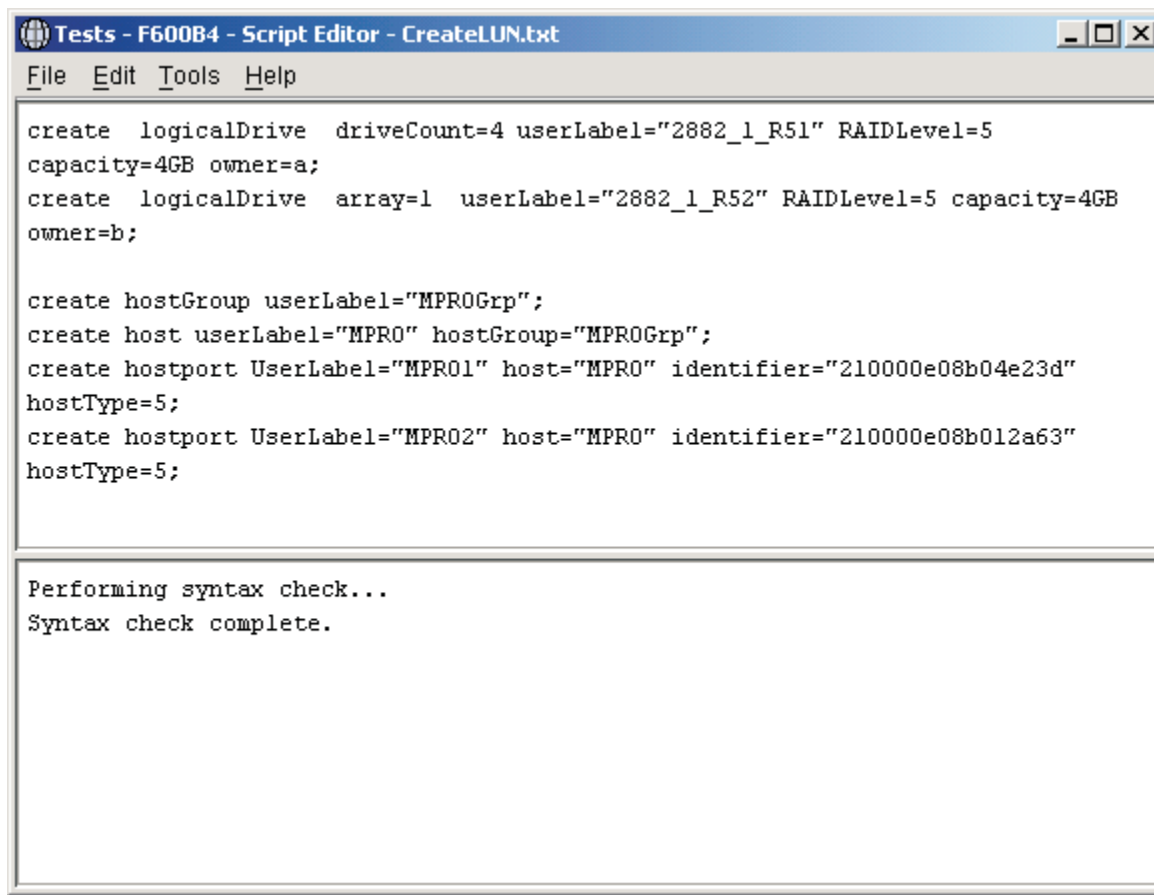
コマンド行インターフェースは、スクリプト・コマンドを使用してストレージ・サブシステムを構成およびモニターすることができるソフトウェア・ツールです。CLI を使用すると、Windows コマンド・プロンプト、Linux オペレーティング・システム・コンソール、または Solaris オペレーティング・システム・コンソールなどのオペレーティング・システム・プロンプトからコマンドを実行することができます。IBM DS ストレージ・マネージャー・クライアントの「Enterprise (エンタープライズ)」ウィンドウから呼び出されるスクリプト・ウィンドウまたは SMcli プログラムを使用するコマンド行インターフェースのいずれかからスクリプト・コマンドを実行するには、IBM DS ストレージ・マネージャー・クライアントをインストールする必要があります。スクリプト・コマンド・エンジンは、IBM DS ストレージ・マネージャー・クライアントのインストールの一部として自動的にインストールされます。

各コマンドは、ストレージ・サブシステムを管理するための特定のアクションを実行するか、ストレージ・サブシステムの状況に関する情報を返します。個別のコマンドを入力するか、複数回にわたって操作を実行する必要がある場合はスクリプト・ファイルを実行することができます。例えば、同じ構成を複数のストレージ・サブシステムにインストールしたい場合にスクリプト・ファイルを実行できます。CLI では、ディスクからスクリプト・ファイルをロードして、スクリプト・ファイルを実行できます。CLI は、複数のネットワーク・ストレージ・サブシステム上でストレージ管理コマンドを実行するための手段を提供します。CLI は、インストール場所と開発環境の両方で使用できます。

ストレージ・マネージャー CLI についての詳細は、「*IBM System Storage DS3000, DS4000, and DS5000 コマンド行インターフェースおよびスクリプト・コマンドのプログラミング・ガイド*」を参照してください。

スクリプト・エディターの使用

グラフィカル・ユーザー・インターフェースを使用してストレージ・サブシステム管理機能を実行する代わりに、スクリプト化された管理コマンドを実行するための「Script Editor (スクリプト・エディター)」ウィンドウを使用することができます。コントローラー・ファームウェア・バージョンが 5.4x.xx.xx 以前の場合、グラフィカル・ユーザー・インターフェースのいくつかの管理機能をスクリプト・コマンドで使用することができません。ストレージ・マネージャー 10.xx は、コントローラー・ファームウェア・バージョン 07.xx.xx.xx 以降と組み合わせて使用した場合に、SMcli コマンドによりすべての管理機能に対する完全サポートを提供します。



ds50_001138

図 12. 「Script Editor (スクリプト・エディター)」ウィンドウ

重要: スクリプト・エディターでは、破壊的な操作 (アレイの削除やストレージ・サブシステム構成のリセットのコマンドなど) の場合にも、確認のプロンプトは表示されません。したがって、コマンドを実行する場合には十分に注意してください。

すべてのスクリプト・コマンドがすべてのバージョンのコントローラー・ファームウェアで実装されているわけではありません。ファームウェア・バージョンが古いほど、使用可能なスクリプト・コマンドのセットは小さくなります。スクリプト・コマンドおよびファームウェア・バージョンについては詳しくは、ストレージ・マネージャーの「Enterprise Management (エンタープライズ管理)」ウィンドウを参照してください。

使用可能なコマンドとその構文のリストについては、オンラインの「Command Reference (コマンド解説)」ヘルプを参照してください。

「Script Editor (スクリプト・エディター)」を開くには、以下の手順を実行します。

1. 「**Device (デバイス)**」タブのツリー・ビューまたはテーブル・ビューでストレージ・サブシステムを選択します。
2. 「**Tools (ツール)**」 > 「**Execucrypt (スクリプトの実行)**」をクリックします。
3. スクリプト・エディターが開きます。「**Script (スクリプト)**」ビューおよび「**Output (出力)**」ビューがウィンドウに表示されています。スプリッター・バーによって、ウィンドウが「**Script (スクリプト)**」ビューと「**Output (出力)**」ビューに分割されています。ビューのサイズを変更する場合は、スプリッター・バーをドラッグします。

「Script (スクリプト)」ビューで、スクリプト・コマンドを入力および編集することができます。「Output (出力)」ビューには、操作の結果が表示されます。「Script (スクリプト)」ビューは、以下の編集キー・ストロークをサポートしています。

Ctrl+A

ウィンドウ内のすべてを選択します。

Ctrl+C

ウィンドウ内でマークされているテキストを Windows のクリップボード・バッファにコピーします。

Ctrl+V

Windows のクリップボード・バッファからウィンドウにテキストを貼り付けます。

Ctrl+X

ウィンドウ内でマークされているテキストを削除 (切り取り) します。

Ctrl+Home

カーソルをスクリプト・ウィンドウの先頭に移動します。

Ctrl+End

カーソルをスクリプト・ウィンドウの最後に移動します。

スクリプト・エディターを使用する際の一般ガイドラインを、以下のリストに示します。

- すべてのステートメントは、セミコロン (;) で終わらせる必要があります。
- 各コマンドおよびそれに関連する 1 次および 2 次パラメーターは、スペースで区切る必要があります。
- スクリプト・エディターでは、大/小文字の区別はありません。
- 個々の新しいステートメントは、別の行から書き始める必要があります。
- スクリプトにはコメントを追加できます。コメントがあれば、自分自身や後で使用する他のユーザーがコマンド・ステートメントの目的を理解しやすくなります。

スクリプト・エディターは、以下の 2 つのコメント書式をサポートしています。

- 2 つのスラッシュ (//) の後ろから行末文字までの間に含まれるテキスト

例えば、以下のとおりです。

```
//The following command assigns hot spare drives.  
set drives [1,2 1,3] hotspare=true;
```

コメント「//The following command assigns hot spare drives.」は、説明のために組み込まれるだけで、スクリプト・エディターでは処理されません。

重要: // で始まるコメントは行末文字で終了する必要があります。行末文字を挿入するには、Enter キーを押します。コメントの処理後にスクリプト・エンジンがスクリプト内に行末文字を検出できなかった場合は、エラー・メッセージが表示され、そのスクリプトは異常終了します。

- 文字 /* と */ の間に含まれたテキスト

例えば、以下のとおりです。

```
/* The following command assigns hot spare drives.*/  
set drives [1,2 1,3] hotspare=true;
```

コメント「 /*The following command assigns hot spare drives.*/」は、説明のために組み込まれるだけで、スクリプト・エディターでは処理されません。

重要: コメントは、`/*` で始まり `*/` で終わる必要があります。スクリプト・エンジンがコメントの開始表記および終了表記の両方を検出できなかった場合は、エラー・メッセージが表示され、そのスクリプトは異常終了します。

第 5 章 ホストの構成

ストレージ・サブシステムを構成した後、この章の情報を使用して、すべてのホストをストレージ・サブシステムに接続できるようにします。この章は、以下のセクションで構成されています。

- 『SAN ブートを使用したホスト・オペレーティング・システムのブート』
- 127 ページの『論理ドライブのフェイルオーバーおよびフェイルバックを自動的に管理するためのマルチパス・ドライバーの使用』
- 170 ページの『デバイスの識別』
- 174 ページの『デバイスの構成』

SAN ブートを使用したホスト・オペレーティング・システムのブート

SAN ブートは、ストレージ・エリア・ネットワーク (SAN) デバイスからホスト・オペレーティング・システムをブートする機能です。この場合、デバイスは DS3000/DS4000/DS5000 ストレージ・サブシステムからの LUN です。SAN ブートは、リモート・ブート と呼ばれます。この場合、ブート LUN はサーバー・エンクロージャー内部ではなくストレージ・サブシステム内にあり、サーバーは SAN のストレージ・サブシステムに接続されます。接続は、直接接続、または SAN ファブリック - SAS、FC、または iSCSI を介します。

SAN ブートを使用する利点として、以下が挙げられます。

サーバー統合

各サーバーは、SAN 上のオペレーティング・システムのイメージからブートできます。

サーバー障害からのリカバリーの簡素化

オペレーティング・システムの再インストールは不要です。

迅速な災害復旧

ストレージ・サブシステムをリモート・リカバリー・サイトで複製できます。

SAN ブートには以下の条件が必要です。

- SAN 構成、ブート・デバイスのゾーニング、マルチパス構成 (該当する場合)
- ブート LUN への単一のアクティブ・パス。インストール・プロセスの実行時に、マルチパス・ドライバーをインストールして使用可能にする前に、ブート LUN へのパスを 1 つだけ使用可能にする必要があります。
- HBA BIOS。選択可能ブート (すなわち、ブート BIOS) を使用可能にする必要があります。

ストレージ・サブシステムを SAN ブート用に構成するには、以下のガイドラインを使用してください。

1. SAN ファブリックの構成:

- a. SAN ゾーニングを作成し、ファブリックの物理構成上の論理グループ内へファイバー・チャネル・デバイスを配置します。SAN 内の各デバイスは複数のゾーンに配置されることになります。
- b. サーバーの HBA ポートから、1 つを除き、ブート LUN へのパスをすべて除去します。これを行うには、その他の物理パスのスイッチでポートを使用不可に設定します。

2. ストレージ・サブシステムを構成します。

- a. LUN を作成します。

- b. LUN をホストに LUN 0 としてマップします。

注: HBA WWNN を知っている必要があります。これは、HBA ラベルに記載されています。

3. SAN からのブートのために HBA を構成します。

- a. ホスト用に構成された HBA デバイスでブート BIOS が使用可能になっていることを検証します。
- b. ホストの始動中に、HBA デバイスのブート BIOS を開始します。
- c. SAN ブートに使用する HBA を選択して、ブート LUN が優先ブート・デバイスとして指定されるように BIOS を構成します。ストレージ・サブシステムが HBA WWPN をディスカバリーした後、ホスト・マッピング手順を使用して、それらをブート LUN への HBA として構成する必要があります。

注:

- 1) HBA がストレージ・サブシステムにログインしている必要があります。その時点でまだ使用可能な LUN がない場合でも、BIOS を使用してそのストレージ・サブシステムをディスカバリーすることができます。
- 2) 詳細については、ご使用の HBA に付属の資料を参照してください。
- d. 変更内容を保存して、BIOS を終了し、サーバーを再始動します。これで BIOS を使用して、新たに構成された LUN を見つけることができます。

4. インストール・メディアからのブートによるインストールを開始します。

- a. インストール時に、オペレーティング・システム・メディアは、どのドライブ (または LUN) でインストールを実行するか尋ねます。ご使用のストレージ・サブシステム・デバイスに該当するドライブを選択してください。

注: サード・パーティー・デバイス・ドライバのインストール中にプロンプトが出された場合、別の形式のメディア上の使用可能な HBA ドライバを選択します。

- b. ディスク区画化のデフォルト・オプションを選択します。

注: 選択した LUN がオペレーティング・システム用として十分な大きさであることを確認してください。Linux、および他のほとんどのオペレーティング・システムでは、ブート・デバイス用に 20 GB あれば十分です。スワップ区画の場合、サイズは少なくともご使用のサーバーの物理メモリー・サイズ以上になるようにしてください。

5. インストールを完了して、SAN ブート手順を終了します。

- a. 再びサーバーを再始動して、ブート・オプション・メニューを開きます。セットアップしたブート・デバイスは既に使用できるように準備されています。
- b. ハード・ディスク/SAN からブートするオプションを選択して、インストールが完了した SAN ディスク・デバイスに関連した HBA を選択します。インストール・ブート・デバイスは、選択した HBA 上でディスカバリーされたブート可能デバイスにリストされます。
- c. 適切なデバイスを選択してブートします。
- d. インストール済みブート・デバイスをシステムのデフォルト・ブート・デバイスとして設定します。

注: このステップは必須ではありません。ただし、この手順が完了した後で無人リブートを使用可能にするには、インストール済みブート・デバイスがデフォルトのブート・デバイスでなければなりません。

- e. **Linux の場合のみ – Linux でインストールを完了するには、以下の手順を実行します。**

- 1) /var/mpp/devicemapping の永続バインディングが最新であることを確認する。
/var/mpp/devicemapping ファイルは、RDAC にどのストレージ・サブシステムを最初に構成す

るかを伝えます。サーバーにストレージ・サブシステムを追加する場合は、ブート/ルート・ボリュームを備えたストレージ・サブシステムが常にデバイス・マッピング・ファイルの最初になるようにします。このファイルを更新するには、次のコマンドを実行してください。

```
# mppUpdate
```

- 2) # mppUpdate コマンドの実行後、次のコマンドを使用して /var/mpp/devicemapping ファイルを戻す。

```
# cat /var/mpp/devicemapping 0:<DS4x00 SAN Boot Device>
```

ブート/ルート・ボリュームのストレージ・サブシステムはエントリー 0 になければなりません。ブート/ルート・ボリュームがエントリー 0 にはない場合は、ファイルを編集してストレージ・サブシステム・エントリーを再配列し、ブート/ルート・ボリュームがエントリー 0 になるようにします。

- 3) # mppUpdate コマンドを実行する。これでインストールは完了です。

これでストレージ・サブシステムとサーバー間にパスを追加することができます。ストレージ・サブシステムの管理にサーバーを使用する予定の場合は、ここでそのサーバーにストレージ・マネージャーをインストールできます。

マルチパス・ドライバーの使用について詳しくは、127 ページの『論理ドライブのフェイルオーバーおよびフェイルバックを自動的に管理するためのマルチパス・ドライバーの使用』を参照してください。

マルチパス・ドライバーの概要

フェイルオーバー・フィーチャーの主要な機能の 1 つは、パス管理を提供することです。サーバーからコントローラーへのパスが複数ある場合、一部のマルチパス・ドライバーでは、パス間で I/O (入出力) を分散させることもできます。このサポートについては、マルチパス・フェイルオーバー・ドライバーに付属の資料で確認してください。

注: 以下の図に示されたホストとストレージ・サブシステム間の接続は、マルチパス・ドライバーの概念を説明するためのものです。これらは推奨ではありません。

116 ページの図 13 と 117 ページの図 14 は、サーバーからコントローラー環境への最適の単一パスと 2 つのパスについて、入出力がどのように流れるかを示しています。

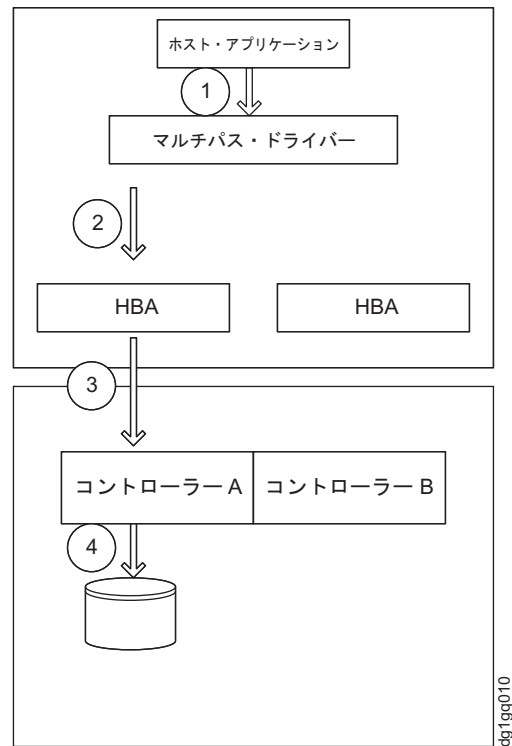


図 13. 最適の単一パスの入出力フロー

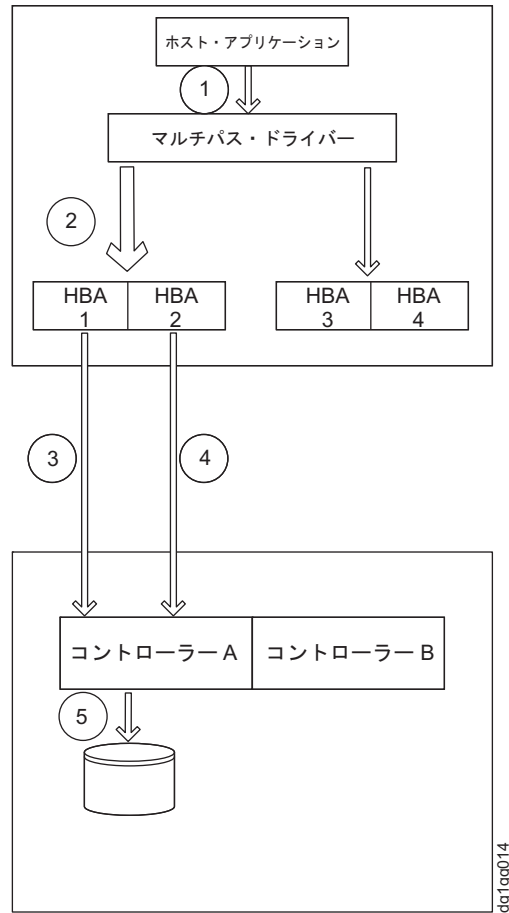


図 14. 最適の 2 つのパスの入出力フロー

また、図 14 は、マルチパス・ドライバーがサポートしている場合、論理ドライブへの入出力をすべての使用可能なパスを介してラウンドロビン方式で経路指定できることも示しています。

フェイルオーバー

マルチパス・ドライバーは、ストレージ・サブシステムへのデータ・パスが正常に動作していない場合、あるいは複数のリンク・エラーが発生した場合に備えて、ストレージ・サブシステムへのデータ・パスをモニターします。マルチパス・ドライバーは、これらの状態のいずれかを検出すると、パス・テーブルをチェックして、冗長パスおよび冗長コントローラーの有無を確認します。同じコントローラーへの代替パスが使用可能な場合、フェイルオーバー・ドライバーはパス・フェイルオーバーを実行します。118 ページの図 15 は、マルチパス・ドライバーがコントローラーへの 2 つのパスのうちの 1 つだけを使用することを示しています。もう一方のパスには障害が起きているためです。1 つのコントローラーへのすべてのパスに障害が起きている場合、マルチパス・ドライバーは、119 ページの図 16 と 120 ページの図 17 に示されているように、コントローラー・フェイルオーバーを実行します。この例では、コントローラー A に障害が起きると、マルチパス・ドライバーは論理ドライブの所有権をコントローラー A からコントローラー B に移動します。その後、コントローラー B はその論理ドライブへのすべての入出力を受け取って処理します。

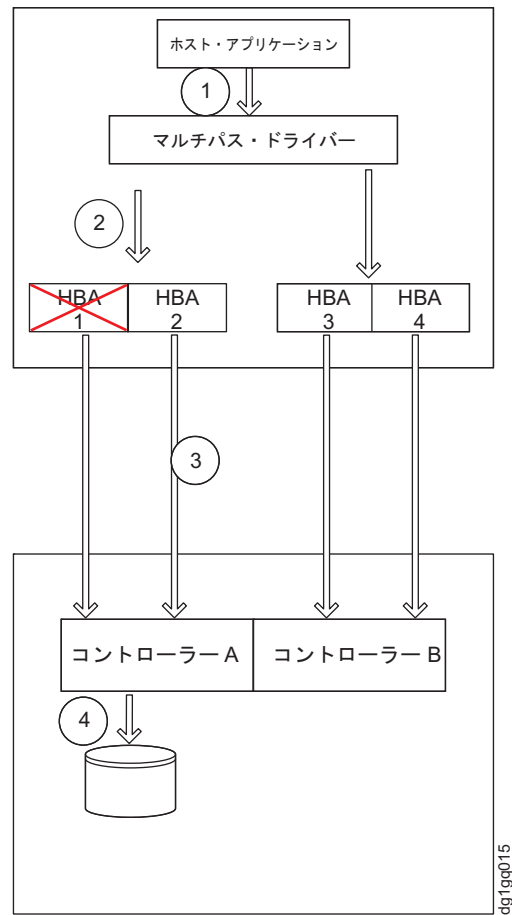


図 15. 一方のパスに障害が起きた場合、もう一方のパスを使用。

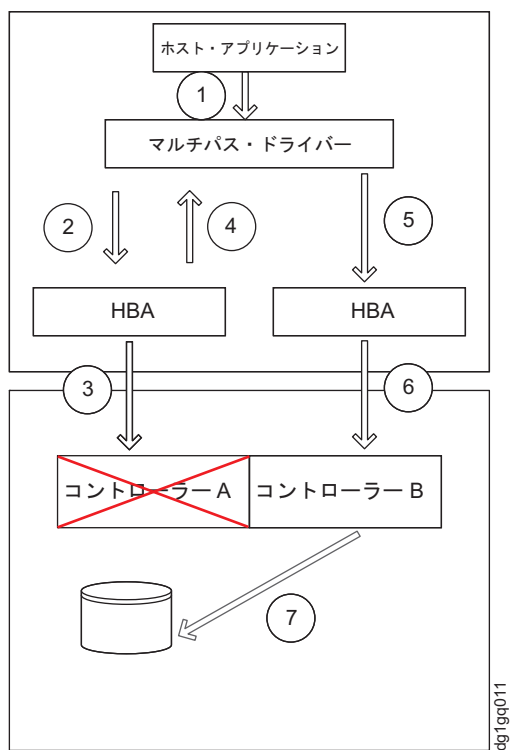


図 16. 単一パス環境での入出力のフェイルオーバー

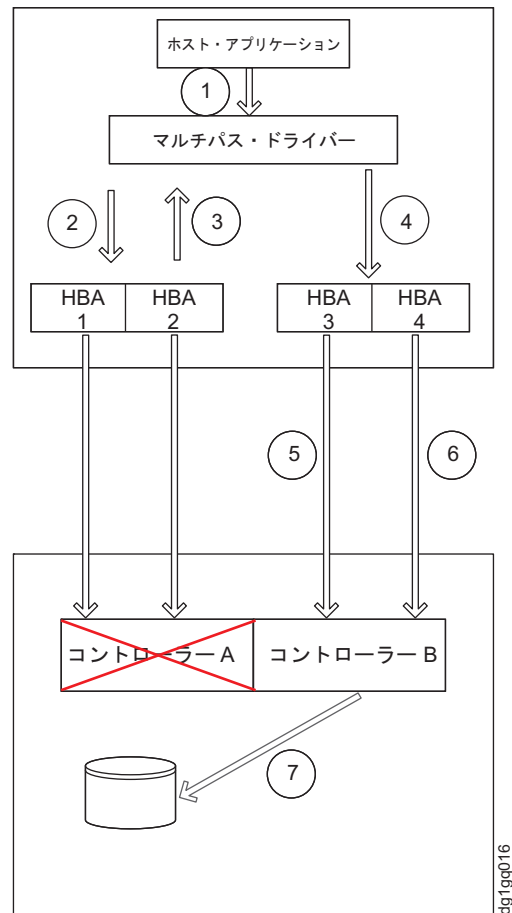


図 17. マルチパス環境での入出力のフェイルオーバー

コントローラー・ファームウェアおよびマルチパス・ドライバー・コードに応じて、マルチパス・ドライバーは、コントローラー・フェイルオーバーに対して異なるアクションを実行します。実行されるアクションは、使用可能なフェイルオーバー・モードによって決まります。フェイルオーバー・モードは、125 ページの表 22 に示されているように、該当するホストを選択することによって設定されます。コントローラー・ファームウェアのバージョンに応じて、以下の 3 つのコントローラー・フェイルオーバー・モードがあります。

1. Automatic Volume Transfer (AVT/ADT) フェイルオーバー・モード - ホスト・タイプが AVT/ADT フェイルオーバー・モードを使用できるように設定されている場合、マルチパス・ドライバーは存続しているコントローラーに入出力を転送します。存続しているコントローラーが論理ドライブの所有権を取得し、入出力を処理するように設定できます。所有権は、障害のあるコントローラーが稼働中かどうかにかかわらず設定できます。これは、コントローラーへのすべてのパスに障害が起こっているか、またはコントローラー自体に障害が起こっている場合に類似しています。コントローラー・ファームウェア・バージョンが 7.77.xx.xx 以前で、このフェイルオーバー・モードがサポートされます。
2. RDAC フェイルオーバー・モード - ホスト・タイプが **disable AVT/ADT** または **non-ALUA** に設定されている場合、マルチパス・ドライバーは、存続しているコントローラーに対してモード・ページ 2C を発行して、存続しているコントローラーに論理ドライブの所有権を移動します。これにより、存続しているコントローラーは論理ドライブの所有権を取得し、それ自体の上で入出力を処理します。他方のコントローラーが稼働中であるかどうか (そのコントローラーへのすべてのパスに障害が発生した場合のように)、あるいはコントローラー自体が故障しているのかどうかに関係なく、存続しているコントローラー

ラーは論理ドライブの所有権を取得します。このフェイルオーバー・モードは、コントローラー・ファームウェアのすべてのバージョンでサポートされます。

3. Asymmetric Logical Unit Access (ALUA) モード - コントローラー・ファームウェア・バージョン 7.83.xx.xx 以降を使用し、ホスト・タイプが「enable ALUA (ALUA 使用可能)」に設定されている場合、マルチパス・ドライバーは、存続しているコントローラーに入出力を転送するだけです。コントローラーへのパスに障害が起きたがコントローラー自体はまだ最適状態である場合のように、「FAILED (障害)」コントローラーが稼働中である場合、存続しているコントローラーは、論理ドライブの所有権を取得して自身で入出力を処理する代わりに、処理のために入出力を「FAILED (障害)」コントローラーにシップします。この状態が 5 分を超えて続く場合、存続しているコントローラーは、処理のために他方のコントローラーに入出力をシップするのを停止し、論理ドライブの所有権を取得して、論理ドライブへの入出力の処理を引き受けます。

ALUA の利点には、以下のものがあります。

- 「SAN からのブート」サーバーは、ブート中に障害が起こりません。これは、ブート LUN は、サーバーのブート・プロセス中にサーバーが最初にスキャンするパスに存在しないか、そのパスにあるコントローラーによって所有されていないためです。「SAN からのブート」サーバーは、そのオペレーティング・システム・ディスクが、サーバー・シャーシ内部にあるのではなく、ストレージ・サブシステムのいずれかの論理ドライブ内にあるサーバーです。
- 偶発的に短時間 (<5 分) のパス中断がある場合に、不必要な論理ドライブのフェイルオーバー/フェイルバックを除去します。
- 論理ドライブがクラスター環境内のサーバーにマップされている特定条件下での「LUN ピンポン」を防止します。
- デュアル・コントローラー構成で、論理ドライブがアクティブ・アクティブとして動作します。どちらのコントローラーが論理ドライブを所有しているかに関係なく、処理のために入出力を両方のコントローラーに送信できます。RDAC または AVT/ADT フェイルオーバー・モードでは、論理ドライブを所有しているコントローラーのみが、その論理ドライブへの入出力を処理できます。これは、デュアル・コントローラー構成のアクティブ・パッシブ操作モードとも呼ばれます。

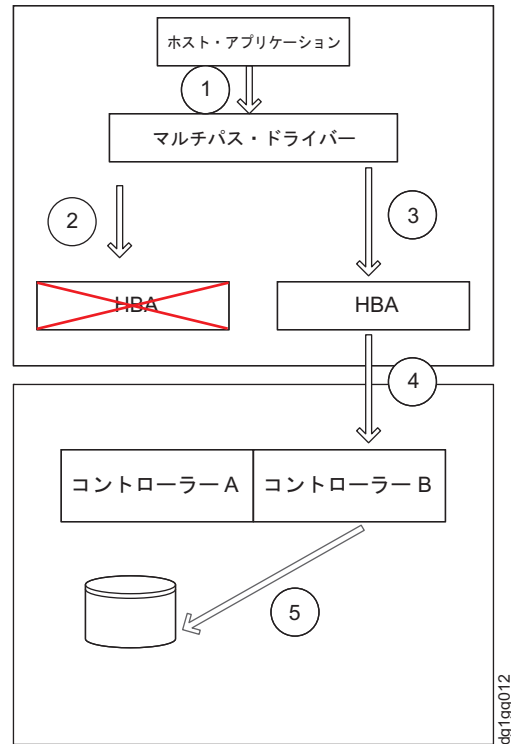


図 18. AVT/ADT および RDAC フェイルオーバー・モードでコントローラーへのすべてのパスに障害

図 18は、コントローラーへのすべてのパスに障害が起きたが、コントローラー自体は AVT/ADT および RDAC のフェイルオーバー・モードで最適状態にある場合のフェイルオーバーを示しています。このフェイルオーバー・シナリオでは、コントローラー A は稼働中で最適状態にあり、障害の原因はホストからコントローラー A へのパス障害にのみにある場合でも、論理ドライブの所有権はコントローラー B に移転され、コントローラー B が論理ドライブへのすべての入出力を処理します。123 ページの図 19 と 124 ページの図 20 は、コントローラーへのすべてのパスに障害があるが、コントローラー自体は ALUA フェイルオーバー・モードで最適状態にある場合のフェイルオーバーを示しています。

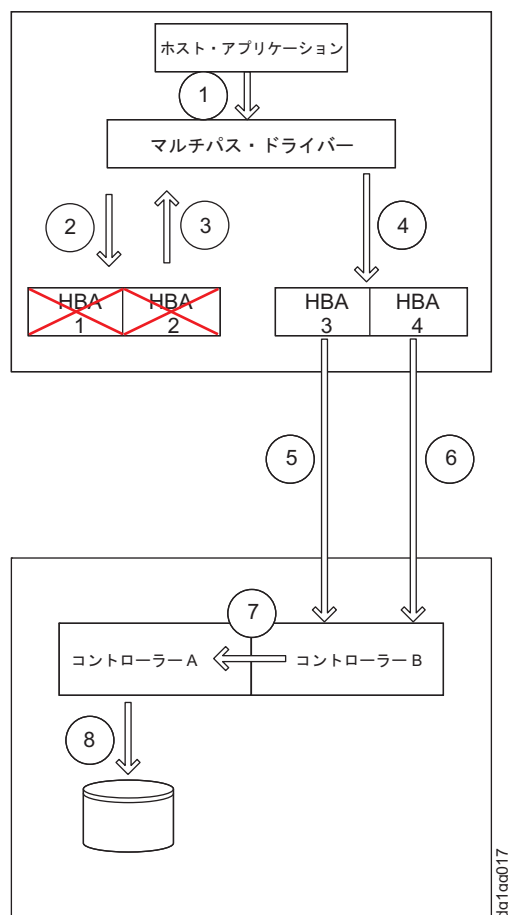


図 19. ALUA フェイルオーバー・モードでコントローラーへのすべてのパスに障害。フェイルオーバーの最初の 5 分間。

フェイルオーバーの最初の 5 分間は、図 19 に示されているように、論理ドライブへの入出力は、処理のためにコントローラー A に内部でシップされます。コントローラー A はまだ論理ドライブの所有者です。5 分後に、コントローラー A へのパスにまだ障害がある場合は、124 ページの図 20 に示されているように、コントローラー B が所有権を取得し、論理ドライブへの入出力の処理を引き受けます。

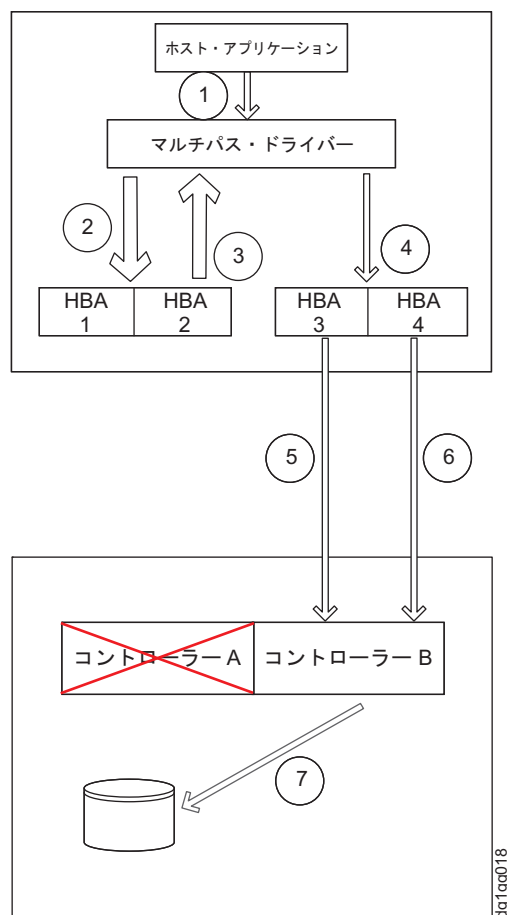


図 20. ALUA モードでコントローラーへのすべてのパスに障害。障害が起きてから 5 分後

上記のフェイルオーバー・モード 1 と 2 で動作している場合、ストレージ・サブシステム内のデュアル・コントローラーは、マップされた LUN の観点からアクティブ・パッシブの組み合わせで動作します。これは、マップされた LUN を所有するコントローラーにのみ、処理のために入出力を送信できることを意味しています。他方のコントローラーは、LUN を所有するコントローラーに障害が起きるか、LUN を所有するコントローラーへのすべてのパスに障害が起きるまで、待機モードになります。マップされた LUN を所有していないコントローラーに入出力が送信されると、LUN はそのコントローラーにフェイルオーバーするか (AVT/ADT モード)、コントローラーによって失敗させられるか (RDAC モード) のいずれかになります。ALUA フェイルオーバー・モードでは、デュアル・コントローラーは、マップされた LUN の観点からアクティブ・アクティブの組み合わせとして動作するようになりました。入出力は、所有するコントローラーだけでなく、処理のために両方のコントローラーに送信することができます。LUN を所有していないコントローラーは、LUN を所有するコントローラーに障害が起きるまでスタンバイ/パッシブ・モードで動作する必要はありません。入出力は、処理のために、LUN を所有するコントローラーに内部で自動的に経路指定されます。また、LUN の所有権の変更は、ALUA モードでの 5 分間内に一方のコントローラーが LUN への入出力の 75% を超える量を処理している場合にのみ実行されます。

コントローラー・ファームウェア・バージョン 7.77.xx.xx 以前では、AVT/ADT および RDAC のフェイルオーバー・モードをサポートしています。コントローラー・ファームウェア・バージョン 7.83.xx.xx 以降は、RDAC および ALUA のフェイルオーバー・モードのみをサポートします。コントローラー・ファームウェア・バージョン 7.83.xx.xx 以降では、AVT/ADT モードはサポートされません。AVT/ADT または ALUA を使用可能にするために、ホスト・タイプ領域内の同じコントローラー NVSRAM ビットが使用されることに注意してください。コントローラー・ファームウェアのバージョンに応じて、このビットは

AVT/ADT または ALUA のいずれかのフェイルオーバー・モードを使用可能にします。どのフェイルオーバー・モードを使用可能にするかは、該当するホスト・タイプがサーバー・ホスト区画で選択されている必要があります。次の表は、各種 OS のホスト・タイプと、そのホスト・タイプに対して使用可能にされているフェイルオーバー・モードをリストしています。

表 22. 各オペレーティング・システムのフェイルオーバー・モード

ホスト・インデックス	ホスト・タイプ (フルネーム)	ホスト・タイプ (ショート・ネーム) ₁	ADT/AVT ₂	RDAC	ALUA ₂
0	デフォルト	Base	なし	はい	なし
1	MacOS	MacOS	なし	はい	なし
2	Windows Server 2003/Server 2008 Non-Clustered <Windows>	W2KNETNCL/Windows	なし	はい	なし
3	Windows Server 2003/Server 2008 Non-Clustered <Windows>	W2KNETNCL/Windows Clustered	なし	はい	なし
4	AIX with Veritas DMP	AIXAVT	はい	なし	なし
5	Linux/ Linux with Veritas DMP	LNHAVT/Linux	はい	なし	なし
6	AIX	AIX	なし	はい	なし
7	HP-UX	HPX	はい	なし	なし
8	Solaris (Spare) <Solaris (with or without MPXIO)>	SOL	なし	はい	なし
9	Windows Server 2003/Server 2008 Clustered Non-Clustered (DMP support)	W2KNETNCLDMP <Windows DMP>	はい	なし	なし
10	Unused 10/Irix ³	Unused10/Irix	なし	はい	なし
11	Unused 11/Netware Failover ³	Unused11/Netware	なし	はい	なし
12	IBM TS SAN VCE	IBM TS SAN VCE	はい	なし	なし
13	Linux Cluster	LNXC LUSTER / LNXC LVMWARE <Linux Cluster>	なし	はい	なし
14	Solaris (with Veritas DMP)	SOLAVT	はい	なし	なし
15	Windows Server 2003/Server 2008 Clustered Clustered (DMP Support)	W2KNETCLDMP	はい	なし	なし

表 22. 各オペレーティング・システムのフェイルオーバー・モード (続き)

ホスト・インデックス	ホスト・タイプ (フルネーム)	ホスト・タイプ (ショート・ネーム) ₁	ADT/AVT ₂	RDAC	ALUA ₂
16	VMWARE <VMWare>	VMWARE	はい	なし	なし
17	HP-UX TPGS	HPXTPGS	なし	はい	なし
18	Linux <Linux Non-ADT>	LNX <Linux Non-ADT>	なし	はい	なし
19	IBM I/Os	IBM i	なし	はい	なし
20	Onstor	Onstor	はい	なし	なし
21	Windows ALUA	W2KALUA	なし	なし	はい
22	Linux ALUA	LNXALUA	なし	なし	はい
23	AIX ALUA w/ TPGS	AIXATPGSALUA	なし	なし	はい
24	VMWARE ALUA w/ TPGS	VMWareTPGSALUA	なし	なし	はい
25	Mac OS ALUA w/ TPGS	MacOSTPGSALUA	なし	なし	はい
26	HP-UX ALUA w/ TPGS	HPXTPGSALUA	なし	なし	はい
27	Solaris ALUA w/ TPGS	SOLTPGSALUA	なし	なし	はい

注:

1. 実際の名前は、ロードされた NVSRAM ファイルのバージョンによって多少異なることがあります。ただし、ホスト・タイプ・インデックスは、すべてのバージョン間で同一であるはずです。
2. コントローラー・ファームウェアに応じて、同じ NVSRAM ビットが ADT/AVT のいずれかを使用可能にしますが、ALUA のみは、ALUA 固有の追加設定が必要であるため、ALUA フェイルオーバー・タイプを使用可能にするには、ホスト・タイプ (ホスト・インデックス 21 から 27) を使用する必要があります。
3. コントローラー・ファームウェア・バージョン 7.77.xx.xx 以前の場合、Irix および Netware のフェイルオーバー・ホスト・タイプは、NVSRAM ファイルで定義されます。コントローラー・ファームウェア 7.83.xx.xx 以降では、Netware サーバーおよび Irix サーバーはホスト接続としてサポートされません。そのため、これらのホスト・タイプは「Unused (未使用)」に変更されました。

フェイルバック

マルチパス・ドライバーは、障害が起きたパスの状況も定期的にモニターし、障害が起きたパスが復元されると、論理ドライブを優先コントローラーにフェイルバックします。コントローラーへの複数のパスのいくつかに障害が起きた後、復元した場合、マルチパス・ドライバーは、再び復元したパスを使用して入出力の送信を開始します。マルチパス・ドライバーは、フェイルオーバー・セクションで説明されているのと同じモード (AVT/ADT、RDAC、または ALUA) を使用して、論理ドライブを移動して優先コントローラーに戻します。

サーバー・クラスター構成では、特定のフェイルオーバー・シナリオでのコントローラー間の「LUN ピンポン」問題を防止するために、マルチパス・ドライバーの自動論理ドライブ・フェイルバック機能を使用不可にすることも可能です。

論理ドライブのフェイルオーバーおよびフェイルバックを自動的に管理するためのマルチパス・ドライバーの使用

入出力アクティビティー用に DS3000/DS4000/DS5000 ストレージ・サブシステムに接続されるホスト・システムには、ファイバー・チャネル・パスの冗長性を確保するために、マルチパス・ドライバー (RDAC またはフェイルオーバー・ドライバーともいいます) が必要です。マルチパス・ドライバーは、入出力パスをモニターします。ファイバー・チャネル・パスのいずれか 1 つでコンポーネントの障害が発生すると、マルチパス・ドライバーがすべての入出力を別のパスに転送します。マルチパス・ドライバーは、インストールしたオペレーティング・システムによって異なります。

Microsoft Windows 環境では、Windows RDAC と呼ばれる他のマルチパス・ドライバーがストレージ・マネージャー・ホスト・ソフトウェアの 9 以前のバージョンで提供されていました。Windows RDAC のサポートは、コントローラー・ファームウェアの 7.xx.xx.xx 以降のバージョンと、それに対応するストレージ・マネージャー・ホスト・ソフトウェアの 10 以降のバージョンで終了しました。さらに、AIX fcp_array のサポートも終了しました。AIX fcp_array ユーザーは、できるだけ早く AIX MPIO マルチパス・ドライバーに移行する必要があります。

IBM ファイバー・チャネル・ホスト・バス・アダプター (HBA) は、ホスト・サーバーとストレージ・サブシステム間のインターフェースを提供します。ストレージ・サブシステムのファイバー・チャネル HBA は、ハイエンド・システム用に設計された、直接メモリー・アクセスを行うバス・マスターの高性能ホスト・アダプターです。これらの HBA は、プライベート・ループ、直接接続、およびファブリック・ループ接続をサポートする、すべてのファイバー・チャネル周辺装置をサポートします。IBM ホスト・アダプター・デバイス・ドライバーを使用することで、オペレーティング・システムはファイバー・チャネル HBA と通信することができます。

表 23 に、さまざまなオペレーティング・システムでサポートされているマルチパス・ドライバーをリストします。特定のストレージ・サブシステム・モデルの特定の OS バージョンでサポートされているマルチパス・ドライバーを判別するには、SSIC を参照してください。

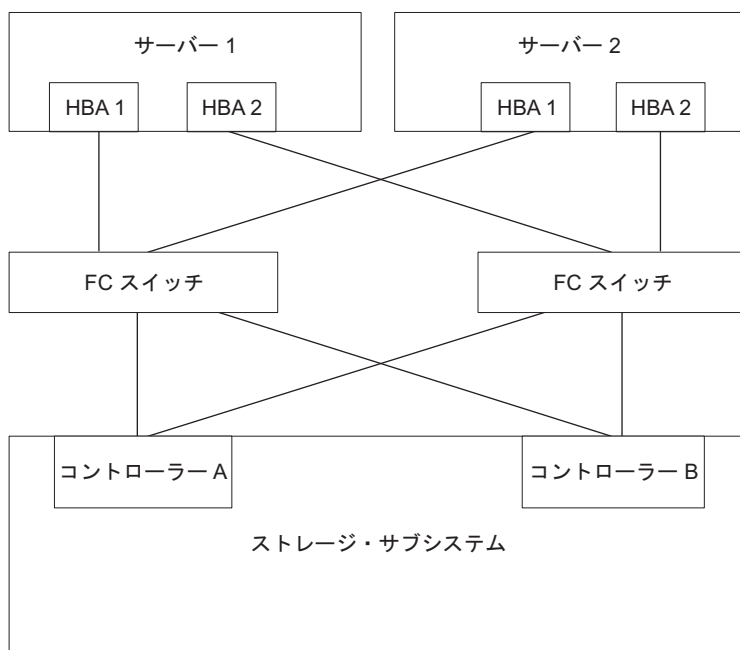
表 23. オペレーティング・システム別のマルチパス・ドライバー

オペレーティング・システム	マルチパス・ドライバー
AIX	fcp_array (RDAC と呼ばれる)、MPIO、あるいは SDDPCM
HP-UX	LVM、ネイティブ・マルチパス、または IBM SDD
Linux	MPP (Linux RDAC または RDAC と呼ばれます)、Veritas DMP、またはネイティブ (ディストリビューション内の) Linux Device Mapper Multipath (DM-Multipath)
Mac OS	HBA メーカーによって提供される
NetWare	Novell MPE
Solaris	RDAC、MPxIO または Veritas DMP
SVC	SDD
VMware	NMP
Windows	MPIO DSM または Veritas DMP DSM

Windows MPIO は例外ですが、マルチパス・ドライバー・ファイルは、ストレージ・マネージャ DVD には含まれていません。SSIC およびストレージ・マネージャー README ファイルで、オペレーティング・システムに必要な最小ファイル・セット・バージョンを確認してください。README ファイルを Web で検索する方法については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。マルチパス・ドライバーをインストールするには、132 ページの『マルチパス・ドライバーのインストール』の指示に従ってください。

マルチパスとは、ストレージ・デバイスへの複数のパスを認識するホストの機能を指す表現です。これは、SAN ファブリック・スイッチに接続されているホスト・サーバー内の複数の HBA ポートまたはデバイスを使用し、これらの SAN ファブリック・スイッチがストレージ・デバイスの複数のポートにも接続するという方法で実現されます。DS3000/DS4000/DS5000 として表されるストレージ製品の場合、これらのデバイスには、ストレージ・サブシステム内で、ディスク・ドライブの管理および制御を行う 2 つのコントローラーがあります。これらのコントローラーは、アクティブ方式またはパッシブ方式のいずれかで動作します。特定の LUN の所有権を持っていて制御を行うのは、片方のコントローラーです。もう 1 つのコントローラーは、障害が発生するまではパッシブ・モードになっていますが、障害の発生時には LUN の所有権がこのコントローラーに転送されます。各コントローラーは、SAN ファブリックへの接続を提供するためのファブリック・ポートを複数持つことができます。

図 21 は、AIX fcp_array と Solaris RDAC マルチパス構成を除く、すべてのサポートされるオペレーティング・システムに関するマルチパス構成の例を示しています。129 ページの図 22 は、AIX fcp_array、Microsoft Windows RDAC (すでにサポートを終了しています)、および Solaris RDAC マルチパス構成に関するマルチパス構成の例を示しています。



詳しくは、63 ページの『IBM System Storage DS ストレージ・マネージャーによりサポートされるドライブ』を参照してください。

図 21. AIX fcp_array および Solaris RDAC を除くすべてのマルチパス・ドライバーに関する、ホスト HBA からストレージ・サブシステム・コントローラーへのマルチパス構成の例

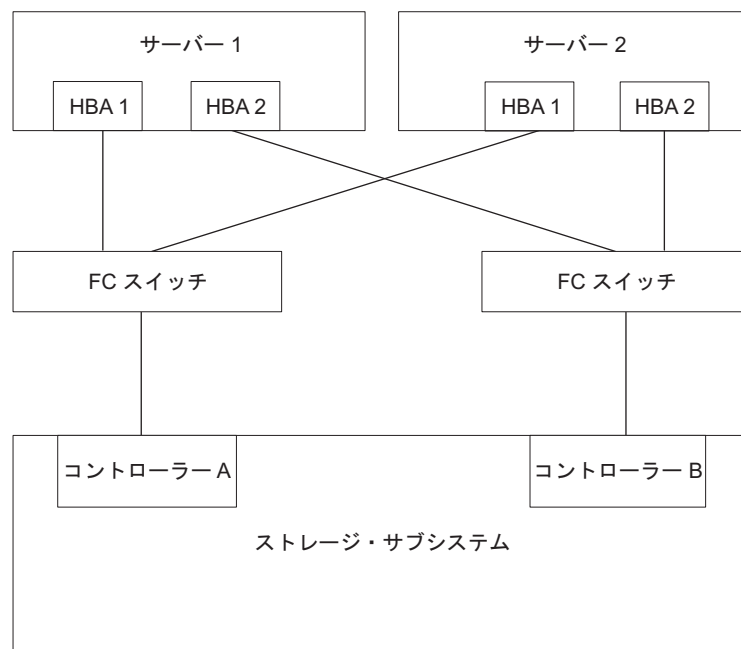


図 22. AIX *fcp_array* および Solaris RDAC マルチパス・ドライバーに関する、ホスト HBA からストレージ・サブシステム・コントローラーへのマルチパス構成の例

ほとんどのマルチパス・ドライバーが、複数のパスをサポートできます。表 24 に、各ドライバーがサポートできるパスの数を示します。AIX *fcp_array* および Solaris RDAC がサポートできるのは 2 つのパスのみ (各コントローラーに 1 つずつ) です。

表 24. オペレーティング・システム別の、各マルチパス・ドライバーがサポートするパスの数

ドライバー	パスの数	デフォルト
AIX MPIO	無制限	該当なし
AIX RDAC	2	該当なし
HP-UX ネイティブ	65,536	該当なし
HP-UX PVlinks	8,192	該当なし
Linux MPP	無制限	4
Linux Veritas DMP	無制限	該当なし
Mac OS	無制限	該当なし
Solaris MPxIO	無制限	該当なし
Solaris RDAC	2	該当なし
Solaris Veritas DMP	無制限	該当なし
SVC	32	該当なし
VMware	無制限 - 最適なパフォーマンスを確保するには 8 以下	該当なし
Windows MPIO DSM	LUN ごとに 32 のパス、コントローラーごとに 16 のパス	4
Windows Veritas DMP DSM	無制限	該当なし

ホスト・バス・アダプターの使用

このセクションでは、ホスト・バス・アダプター (HBA) の基本的な概要、およびファイバー・チャネル・スイッチ環境で HBA を接続するための手順について説明します。

ホスト・バス・アダプターについて

ホスト・バス・アダプター (HBA) は、サーバーをファイバー・チャネル・トポロジに接続するために使用されます。HBA の機能は、LAN リソースにアクセスするために使用されるネットワーク・アダプターの機能に似ています。HBA 用のデバイス・ドライバは、通常、ファイバー・チャネル・トポロジ (ポイント・ツー・ポイント、ループ、またはファブリック) に対するサポートを提供します。

DS3000、DS4000、および DS5000 ストレージ・サブシステムでは、ホスト・サーバーをストレージ・サブシステムに接続するために、ファイバー・チャネル (FC)、Serial Attached SCSI (SAS)、Fibre Channel over Ethernet (FCoE)、および iSCSI の各ホスト・バス・アダプター (HBA) をサポートしています。これらのストレージ・サブシステムでは、通常のイーサネット NIC アダプター経由の iSCSI もサポートしています。ただし、すべての HBA が DS3000、DS4000、および DS5000 ストレージ・サブシステムでサポートされるわけではありません。HBA サポートの詳細情報は、<http://www.ibm.com/systems/support/storage/config/ssic>に進みます。

特定のオペレーティング・システム環境用にカスタマイズできる HBA の設定について詳しくは、資料を参照してください。この資料には、これらの設定の変更方法についても記載されています。設定を誤ると、パフォーマンスの低下または偶発的な障害の原因となるため、これらの設定を変更する際は十分に注意してください。また、設定に関する最新の変更情報については、ホスト・バス・アダプター BIOS、ファームウェア、またはデバイス・ドライバのパッケージに含まれている README ファイルを参照してください。295 ページの『付録 A. ホスト・バス・アダプターの設定』の表に、さまざまな HBA ベンダーの選択された設定の必須値が示されています。

ファイバー・チャネル・スイッチ環境における HBA の接続

ホスト・サーバー内のファイバー・チャネル・ホスト・バス・アダプター (HBA) を、ファイバー・チャネル・スイッチ環境内のストレージ・サブシステムのホスト・ポートに接続する場合に使用できる、2 つの主なゾーニング方式があります。1 対 1 のゾーニング方式では、各 HBA ポートは 1 つのコントローラー・ホスト・ポートにゾーニングされます。1 対 2 のゾーニング方式では、各 HBA ポートは 2 つのコントローラー・ホスト・ポートにゾーニングされます。

一般に、SAN ファブリック環境におけるポート間で起こり得る相互作用を最小限に抑えるために、HBA およびストレージ・サブシステムのホスト・ポート接続はゾーニングされなければなりません。1 対 1 のゾーニング方式は、必須ではありませんが、1 つの HBA ポートをたった 1 つのサーバー・ホスト・ポートに接続するので、相互作用を最小限に抑えます。ただし、どのゾーニング方式を選択するかは、ご使用のホスト・ストレージ SAN ファブリック・トポロジとご使用のファイバー・チャネル・スイッチの機能によって異なります。

ご使用のホスト・ストレージ SAN ファブリック・トポロジとファイバー・チャネル・スイッチの機能に応じて、131 ページの図 23 と 131 ページの図 24 にある以下の 2 つのゾーニング方式のどちらかを実装することができます。

注: ゾーニングのベスト・プラクティスと要件について詳しくは、「*Fibre Channel Switch Hardware Reference Guide*」、またはファイバー・チャネル・スイッチに付属のその他の資料を参照してください。IBM Web サイトにあるスイッチの資料へのリンクについては、次のサイトにアクセスしてください。

www.ibm.com/servers/storage/support/san/index.html

このゾーニング方式 (半透明のバーで示されている) では、1 つの HBA ポートが 1 つのコントローラー・ホスト・ポートにゾーニングされています。

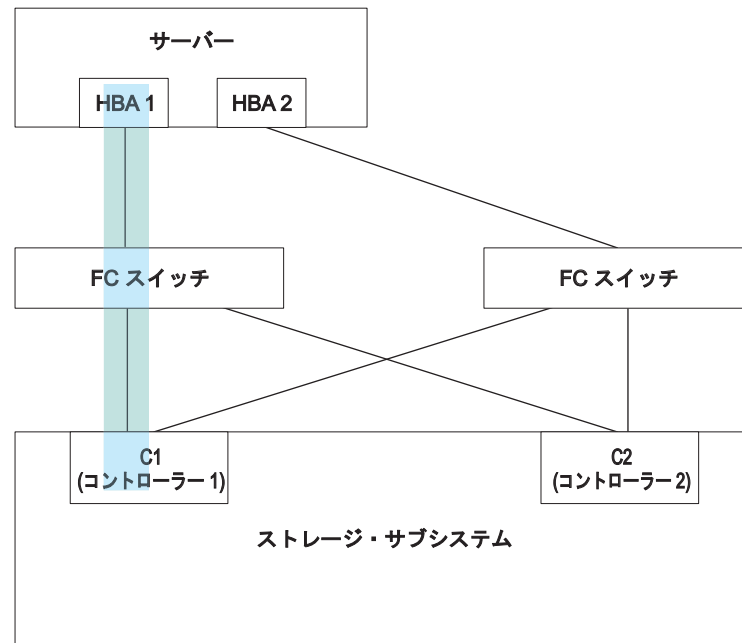


図 23. 1 対 1 のゾーニング方式

このゾーニング方式 (半透明のバーで示されている) では、1 つの HBA ポートが 2 つのコントローラー・ホスト・ポートにゾーニングされています。

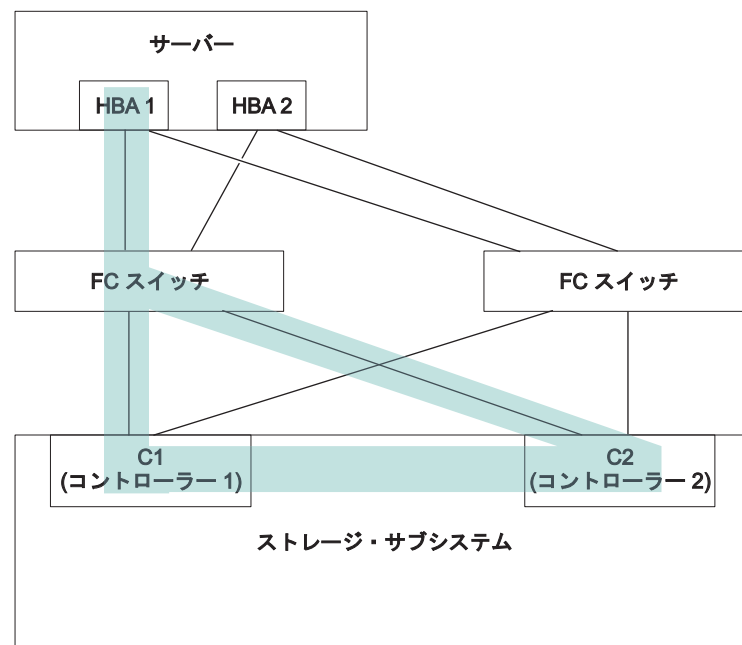


図 24. 1 対 2 のゾーニング方式

マルチパス・ドライバーのインストール

ご使用のストレージ・サブシステムに接続するホストがストレージ・サブシステムに対して複数のパスを持つかどうかに関係なく、これらのホストすべてにマルチパス・ドライバーをインストールする必要があります。このセクションでは、さまざまなマルチパス・ドライバー、マルチパス・ドライバー・プログラムの現行のドライバー・バージョン・レベルの確認方法、マルチパス・デバイス・ドライバーの更新方法、およびマルチパスの更新の完了の検証方法について説明します。

Windows MPIO または MPIO/DSM マルチパス・ドライバー

概要

このマルチパス・ドライバーは、Windows 版のストレージ・マネージャーのホスト・ソフトウェア・パッケージに含まれています。MPIO は、マルチパス・デバイスの管理コードを開発するための、Microsoft 提供の DDK キットです。DDK キットには、ストレージ・サブシステムのデバイス固有モジュール (DSM) と共にインストールされるバイナリー・ドライバーのコア・セットが含まれています。これらのドライバーは、Microsoft プラグ・アンド・プレイに依存する透過的システム・アーキテクチャーを提供するように設計されています。これらのバイナリー・ドライバーは、LUN マルチパス機能を提供すると同時に、既存の Microsoft Windows デバイス・ドライバー・スタックとの互換性を維持します。Windows Server 2003 の場合、MPIO は MPIO DSM と共にインストールされます。Windows Server 2008 では、MPIO DSM のみがインストールされます。Windows 2008 は、MPIO がインストールされた状態で出荷されるためです。

MPIO ドライバーは、以下のタスクを実行します。

- ベンダーまたは製品 ID スtringに基づいて、ストレージ・サブシステムから提示される物理ディスク・デバイスの検出および要求を行い、物理デバイスへの論理パスを管理する。
- 各 LUN の単一インスタンスを、Windows オペレーティング・システムの他の部分に対して提供する。
- WMI を介して、ユーザー・モードのアプリケーションで使用するオプションのインターフェースを提供する。
- ストレージ・サブシステムの動作に関する以下の情報を、ベンダー (IBM) のカスタマイズ済みデバイス固有モジュール (DSM) に応じて判別する。
 - 入出力ルーティング情報
 - 要求の再試行、失敗、フェイルオーバーまたはフェイルバックが必要となる条件 (例えば、ベンダー固有のエラー)
 - リリースまたは予約コマンドなどの各種機能

異なるディスク・ストレージ・サブシステム用の複数の DSM は、同一のディスク・デバイスを要求しない限り、同一のホスト・サーバーにインストールできます。

マルチパス環境でのネイティブ SCSI-2 解放/予約コマンド

単一コントローラーへの複数のパスが存在する場合に、ある論理ドライブに対する SCSI-2 解放/予約 (R/R) を受け取った場合、MPIO DSM ドライバーは各コントローラーへの 1 つのパスを選択し (予約パスと呼ばれる)、要求を繰り返します。この機能が必要な理由は、特定の論理ドライブに対する SCSI-2 R/R 要求が複数のパスを通して出された場合、コントローラーはそれらの要求を受け入れることができないからです。予約パスが確立されると、以降の論理ドライブに対する入出力要求は、SCSI-2 解放コマンドを受け取るまで、そのパスに限定されます。複数の論理ドライブがホストにマップされている場合、MPIO DSM ドライバーは予約パスを分散させます。これにより、負荷は、同一コントローラーへの複数のパス間に分散されます。

注: この SCSI 予約処理方式は、コントローラーの ALUA 機能とは両立しません。ALUA 機能が使用可能になっているときは、この方式は使用しないでください。

SCSI-2 解放/予約コマンドの SCSI-3 永続予約への変換

MPIO DSM ドライバーは、SCSI-2 R/R コマンドを SCSI-3 永続予約に変換する機能もサポートしています。この機能により、論理ドライブは、単一の予約パスに限定されずに、すべての使用可能なコントローラー・パスにわたって、前述のロード・バランシング・ポリシーのいずれかを使用できます。この機能では、MPIO DSM ドライバーはホストごとに固有の「予約キー」を設定する必要があります。このキーは、レジストリーに格納され、S2toS3Key と呼ばれます。このキーが存在する場合は変換が実行され、存在しない場合は「クローン作成」方式が使用されます。

プロトコル別入出力タイムアウト値

非パススルー入出力要求（読み取り/書き込み要求など）に関連付けられたタイムアウト値は、レジストリーで定義されている Microsoft ディスク・ドライバーの **TimeOutValue** パラメーターに基づきます。DSM 内の機能により、パスで使用されるプロトコル（ファイバー・チャネル、SAS、または iSCSI）に基づいて、カスタマイズされたタイムアウト値を適用することができます。プロトコル別タイムアウト値には、次のような利点があります。

- プロトコル別タイムアウト値がないと、**TimeOutValue** 設定はグローバルになり、すべてのストレージに影響します。
- **TimeOutValue** は通常、HBA ドライバーがアップグレードされるとリセットされます。
- Windows Server 2003 では、入出力要求のサイズに基づいて、デフォルトのディスク・タイムアウト値を調整できます。デフォルトのディスク・タイムアウト値の調整は、レガシー SCSI デバイスのサポートに役立ちます。
- DSM カスタマイズ・タイムアウト機能により、Windows Server 2003 環境ではタイムアウト設定がさらに予測可能になります。カスタマイズ・タイムアウト機能の構成可能パラメーターについては、『Windows DSM および Linux RDAC の構成設定値』を参照してください。

プロトコル別タイムアウト値機能により、**SynchTimeout** パラメーターの評価方法が多少変更されます。

SynchTimeout パラメーターは、DSM ドライバーによって生成される同期要求の入出力タイムアウトを決定します。

この例としては、SCSI-2 から SCSI-3 への PR 変換や、デバイス・ディスクバリー中に使用される照会コマンドが含まれます。DSM ドライバーからの要求のタイムアウト値は、少なくともプロトコル別入出力タイムアウト値と同じ大きさであることが重要です。ホストのブート時に、DSM ドライバーは以下のアクションを実行します。

- **SynchTimeout** パラメーターの値が DSM ドライバーのレジストリー・キーで定義されている場合、現行値を記録します。
- Microsoft ディスク・ドライバーの **TimeOutValue** パラメーターの値がレジストリーに定義されている場合、現行値を記録します。
- この 2 つの値の大きい方を、**SynchTimeout** パラメーターの初期値として使用します。
- どちらの値も定義されていない場合、デフォルト値の 10 秒を使用します。
- 同期入出力要求ごとに、プロトコル別入出力タイムアウトまたは **SynchTimeout** パラメーターのいずれか大きい方の値が使用されます。例えば、以下のとおりです。
 - **SynchTimeout** パラメーターの値が 120 秒で、**TimeOutValue** パラメーターの値が 60 秒の場合、初期値として 120 秒が使用されます。

- **SynchTimeout** パラメーターの値が 120 秒で、**TimeOutValue** パラメーターの値が 180 秒の場合、DSM ドライバーの同期入出力要求の初期値として 180 秒が使用されます。
- 別のプロトコル (例えば、SAS) の入出力タイムアウト値が 60 秒で、初期値が 120 秒の場合、入出力は 120 秒のタイムアウトを使用して送信されます。

選択 LUN 転送

この機能では、DSM ドライバーが LUN を代替コントローラーに移動する条件が以下の 3 つのケースに限定されます。

1. 1 つのコントローラーのみへのパス (非優先パス) を持つ DSM ドライバーが、代替コントローラーへのパスをディスカバーした場合。
2. 優先パスによって所有される LUN に入出力要求が送信されたが、DSM ドライバーが非優先パスにのみ接続されている場合。
3. 非優先パスによって所有される LUN に入出力要求が送信されたが、DSM ドライバーが優先パスにのみ接続されている場合。

ケース 2 とケース 3 の場合、この機能の動作を調整するために設定できる、以下のユーザー構成可能パラメーターがあります。

- LUN 転送が実行される最大回数。このパラメーター設定値により、LUN が現行コントローラーに所有されている必要がある別のホストにコントローラー・エンクロージャーまたはコントローラー・ドライブ・エンクロージャーが接続されている場合に、所有権の連続スラッシング状態が発生するのが防止されます。
- LUN 転送が試行される前の時間遅延。このパラメーターは、偶発的な入出力パス・リンク・エラーを抑えるために使用されます。この時間遅延の間、別のホストが LUN を現行コントローラーに移行する可能性を利用するために、入出力要求は現行コントローラー上で再試行されます。

これらの 2 つのパラメーターの詳しい情報については、『Windows DSM および Linux RDAC の構成設定値』を参照してください。

ホスト・システムが両方のコントローラーに接続されていて、入出力が 94/01 状況 (LUN が所有されておらず、所有できる) で戻された場合、DSM ドライバーは、その LUN のためにどちらのコントローラーを使用するかに関する内部データを変更して、他方のコントローラーに対してコマンドを再発行します。コントローラー・エンクロージャーまたはコントローラー・ドライブ・エンクロージャーに接続されている可能性がある他のホストとの干渉を回避するために、DSM ドライバーはそのコントローラー・エンクロージャーまたはコントローラー・ドライブ・エンクロージャーには LUN 転送コマンドを発行しません。

DSM は、論理ドライブの転送操作が必要であることを検出しても、即時にフェイルオーバー/フェイルバック・コマンドを発行しません。デフォルト設定では、ストレージ・サブシステムにコマンドを送信する前に 3 秒間の遅延があります。この遅延により、他の LUN に対する論理ドライブ転送操作をできるだけ多くまとめてバッチ処理するための時間が提供されます。コントローラーは、論理ドライブ転送操作を単一スレッドで実行するため、現在処理中の操作が完了するまで、追加の転送コマンドを拒否します。その結果、ストレージ・サブシステムが入出力を正常にサービスできない期間が生じます。遅延を導入し、その間に複数の論理ドライブ転送操作を 1 つのバッチ操作に集約できるようにすることで、DSM は論理ドライブ転送操作が再試行限度を超える可能性を減らします。大規模なシステム構成では、構成内により多くのホストがあり、より多くの論理ドライブ転送コマンドが送信される可能性があるため、デフォルトの 3 秒の遅延値を増やす必要がある場合があります。

遅延値は、次の場所にあります。

HKEY_LOCAL_MACHINE¥SYSTEM¥CurrentControlSet¥Services¥<DSM_Driver>¥Parameters¥LunFailoverDelay。

この機能は、以下の条件が存在するときに使用可能になります。

- コントローラー・エンクロージャーまたはコントローラー・ドライブ・エンクロージャーで AVT が使用可能になっていない。
- DSM ドライバーの構成可能パラメーター **ClassicModeFailover** が 1 に設定されている。
- DSM ドライバーの構成可能パラメーター **DisableLunRebalance** が 4 に設定されている。

Windows フェイルオーバー・クラスター

Windows Server 2008 OS および Windows Server 2008 R2 OS のクラスタリングでは、ネイティブで SCSI-3 永続予約を使用します。その結果、DSM ドライバーはどの SCSI-2 R/R コマンドについても変換を実行せず、すべてのコントローラー・パスにわたって前述のロード・バランシング・ポリシーのいずれかを使用できます。DSM ドライバーが Windows Server 2003 OS ベースの環境で実行されている場合は、引き続き変換が行われます。クラスター環境で操作していて、CFW の入出力シッパ機能または DSM の選択 LUN 転送機能を利用しない場合は、**DisableLunRebalance** パラメーターを 3 に設定してください。このパラメーターについては、『Windows DSM および Linux RDAC 構成設定値』を参照してください。

Asymmetric Logical Unit Access (ALUA) の入出力シッパ機能

入出力シッパ機能は、ALUA のサポートを実装します。コントローラー・ファームウェア (CFW) の以前のリリースでは、デバイス固有モジュール (DSM) は特定の論理ドライブに対する入出力 (I/O) 要求を、その論理ドライブを所有するコントローラーに送信する必要がありました。コントローラーは、所有していない論理ドライブに対する要求を受け取ると、その要求を拒否していました。この動作は、ストレージ・サブシステムが論理ドライブ内のデータの整合性を維持するために必要でした。しかし、この同じ動作が、システム・ブート時およびマルチホスト・パス障害状態時に、いくつかの領域で競合が起こる原因になっていました。

入出力シッパ機能を使用すると、ストレージ・サブシステムは二重構成内のどちらのコントローラーを介しても入出力要求を処理することができます。非所有コントローラーが論理ドライブにアクセスすると、パフォーマンスが低下します。サブシステムの入出力パフォーマンスを最良に維持するために、DSM は CFW と相互作用して、所有コントローラーが使用可能であればそのコントローラーに入出力要求が送信されるようにします。

DSM をインストールまたは更新すると、デフォルトでは、選択 LUN 転送 (SLT) 機能が使用可能になり、入出力シッパをサポートします。前のバージョンで SLT が使用可能になっていなかった場合、DSM の更新中に一部のレジストリー値が変更されます。ストレージ・サブシステムが入出力シッパ機能を使用しないで動作するように SLT の使用可能化を防ぐには、レジストリーを編集して以下の設定にしてください。

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<DSM_Driver>\Parameters\DisableLunRebalance ここで、<DSM_Driver> は、ストレージ・サブシステムで使用される DSM ドライバーの名前です。
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<DSM_Driver>\Parameters\ClassicModeFailover ここで、<DSM_Driver> は、ストレージ・サブシステムで使用される DSM ドライバーの名前です。

Storport ミニポート HBA デバイス・ドライバー

Windows オペレーティング・システムの場合、ストレージ・マネージャーは、Microsoft Storport ミニポート・デバイス・ドライバー・モデルをベースにした MPIO DSM デバイス・ドライバーを提供します。

Storport ミニポート・デバイス・ドライバー・モデルは、SCSIport ミニポート・デバイス・ドライバー・モデルの代わりに Microsoft Windows Server 2003 リリースに導入されました。これは、AMD64 および EM64T サーバーをサポートする、Windows Server 2003 および Windows Server 2008 用に唯一サポートされるデバイス・ドライバー・モデルです。Microsoft Windows オペレーティング・システムのプラグ・アンド・プレイ・ドライバーをバイパスするための `buschange=0` パラメーターはサポートしません。代わりに、プラグ・アンド・プレイ・ドライバーと共に動作して、ファイバー・チャネル・ホスト・バス・アダプター・ポートでのデバイスの取り外しおよび挿入を検出します。

DS4100、DS4200、DS4300 (標準またはターボ・モデル)、DS4400、DS4500、DS4700、および DS4800 ストレージ・サブシステムのみが、この Storport ベースのデバイス・ドライバーをサポートします。DS4100、DS4300 (標準またはターボ・モデル)、DS4400、および DS4500 ストレージ・サブシステム・モデルには、コントローラー・ファームウェア・バージョン 6.12.27.xx 以降が必要です。

コントローラー・ファームウェアのバージョンまたは更新情報など、コントローラー・ファームウェアのバージョンまたは更新情報など、追加要件については、Microsoft Windows オペレーティング・システムに関するストレージ・マネージャーの README ファイルを参照してください。

SCSIport ミニポート HBA デバイス・ドライバー

Windows 2000 オペレーティング・システム環境では、SCSIport ミニポート・デバイス・ドライバー (Storport モデルではない) をベースにしたデバイス・ドライバーのみがサポートされています。

SCSIport デバイス・ドライバーの前のリリースでは、Microsoft プラグ・アンド・プレイ・デバイス・ドライバが HBA ポートを管理しないようにすることにより、`buschange=0` パラメーターによって、RDAC マルチパス・ドライバーがデバイスの HBA ポートへの挿入と取り外しを制御し、モニターするのを許可しています。この新しい SCSIport デバイス・ドライバーのバージョンでは、`buschange=0` パラメーターをサポートしません。

重要: 必ずしもすべての DS4000/DS5000 コントローラー・ファームウェアのバージョンがこの機能をサポートするものではありません。DS4300 標準またはターボ・モデルと DS4500 ストレージ・サブシステム用 DS4000 および DS5000 コントローラー・ファームウェア・バージョン 06.12.27.xx (およびそれ以降)、あるいは DS4200、DS4700、および DS4800 ストレージ・サブシステム用バージョン 6.16.8x.xx (およびそれ以降) のみが、SCSIport ミニポート・デバイス・ドライバーをサポートします。

デバイス・ドライバーをインストールする前に、デバイス・ドライバーのパッケージ・ファイルに付属の README ファイルおよび Windows のストレージ・マネージャー・ホスト・ソフトウェアに付属の README ファイルを参照して、どのデバイス・ドライバーおよびコントローラー・ファームウェア・バージョンが DS3000、DS4000、または DS5000 ストレージ・サブシステムでサポートされているかを確認してください。Web 上で最新のストレージ・マネージャーの README ファイルにアクセスする方法については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。ご使用のオペレーティング・システムに対応したデバイス・ドライバーのインストールの説明については、README ファイルを参照してください。

注: 最適なパフォーマンスを得るために必要な、デフォルトの HBA BIOS およびホスト・オペレーティング・システムのレジストリー設定に対する変更については、デバイス・ドライバーの README ファイルをお読みください。HBA BIOS の設定を変更した場合、その変更を有効にするにはサーバーをリブートする必要があります。

詳細については、ご使用のファイバー・チャネル HBA に付属の資料を参照してください。

dsmUtil の使用

dsmUtil ユーティリティは、マルチパス入出力 (MPIO) デバイス固有モジュール (DSM) ソリューションでのみ機能する、コマンド行駆動型ユーティリティです。このユーティリティは、主に各種のメンテナンス・タスクの実行を DSM ドライバーに指示するための手段として使用されますが、必要な場合には、トラブルシューティング・ツールとしての役目も果たすことができます。

dsmUtil ユーティリティを使用するには、次のコマンドを入力して、Enter キーを押します。

```
dsmUtil [[-a [target_id]]
[-c array_name | missing]
[-d debug_level] [-e error_level] [-g
virtual_target_id]
[-o [[feature_action_name[=value]] |
[feature_variable_name=value]][, SaveSettings]] [-M]
[-P [GetMpioParameters | MpioParameter=value | ...]]
[-R]
[-s "failback" | "avt" | "busscan" | "forcerebalance"]
[-w target_wwn, controller_index]
```

パラメーターを何も指定せずに dsmUtil と入力すると、使用情報が表示されます。dsmUtil パラメーターについては、以下の表を参照してください。

表 25. dsmUtil パラメーター

パラメーター	説明
-a [target_id]	DSM によって認識されるすべてのストレージ・サブシステムの要約を表示します。要約には、target_id、ストレージ・サブシステム WWID、およびストレージ・サブシステム名が表示されます。target_id が指定されている場合、そのストレージ・サブシステムについての DSM の特定時点の状態情報が表示されます。UNIX オペレーティング・システムでは、仮想 HBA がストレージ・サブシステムごとに固有のターゲット ID を指定します。Windows MPIO 仮想 HBA ドライバーは、ターゲット ID を使用しません。このオプションのパラメーターは、DSM 情報構造へのオフセットと見なすことができ、各オフセットは異なるストレージ・サブシステムを表します。お客様サポート担当員および技術サポート担当員専用です。
-c array_name missing	WWN ファイルの項目をクリアします。このファイルは、Program Files\DSMDrivers\mppdsm\WWN_FILES にあり、拡張子.wwn が付いています。subsystem_name キーワードが指定されている場合、その特定のストレージ・サブシステム用の WWN ファイルが削除されます。missing キーワードが使用されている場合、前に接続されていたストレージ・サブシステム用のすべての WWN ファイルが削除されます。どちらのキーワードも使用されていない場合、現在接続されているストレージ・サブシステムと前に接続されていたストレージ・サブシステムの両方のすべての WWN ファイルが削除されます。

表 25. *dsmUtil* パラメーター (続き)

パラメーター	説明
<code>-d debug_level</code>	現行のデバッグ・レポート・レベルを設定します。このオプションは、デバッグを有効にして RDAC ドライバーをコンパイルした場合にのみ使用できます。デバッグ・レポートは、2 つのセグメントで構成されます。最初のセグメントは、機能の特定の領域を示し、2 番目のセグメントは、その領域内のレポートのレベルを示します。debug_level は、以下の 16 進数のいずれかです。 • 0x20000000 – RDAC ドライバーの初期化ルーチンからのメッセージを表示します。 0x10000000 – RDAC ドライバーのディスカバリー・ルーチンからのメッセージを表示します。 • 0x08000000 – RDAC ドライバーの ioctl() ルーチンからのメッセージを表示します。 0x04000000 – RDAC ドライバーのデバイス・オープン・ルーチンからのメッセージを表示します (Linux プラットフォームのみ)。 • 0x02000000 – RDAC ドライバーのデバイス読み取りルーチンからのメッセージを表示します (Linux プラットフォームのみ)。 • 0x01000000 – HBA コマンドに関連したメッセージを表示します。 • 0x00800000 – 異常終了したコマンドに関連したメッセージを表示します。 • 0x00400000 – パニック・ダンプに関連したメッセージを表示します。 • 0x00200000 – 同期出力アクティビティに関連したメッセージを表示します。 • 0x00100000 – フェイルオーバー・アクティビティに関連したメッセージを表示します。 • 0x00080000 – フェイルバック・アクティビティに関連したメッセージを表示します。 • 0x00040000 – フェイルバック・アクティビティに関連した追加メッセージを表示します。 • 0x00010000 – デバイスの取り外しに関連したメッセージを表示します。 • 0x00001000 – SCSI 予約アクティビティに関連したメッセージを表示します。 • 0x00000400 – パス検証アクティビティに関連したメッセージを表示します。 • 0x00000001 – デバッグ・レベル 1。 • 0x00000002 – デバッグ・レベル 2。 • 0x00000004 – デバッグ・レベル 3。 • 0x00000008 – デバッグ・レベル 4。 必要に応じて、これらのオプションを論理 OR 演算子を使用して結合し、複数の領域およびレベルのレポートを提供することができます。お客様サポート担当員および技術サポート担当員専用です。

表 25. *dsmUtil* パラメーター (続き)

パラメーター	説明
-e <i>error_level</i>	現行のエラー・レポート・レベルを <i>error_level</i> に設定します。以下のいずれかの値を指定できます。 • 0 – すべてのエラーを表示します。 • 1 – パス・フェイルオーバー、コントローラー・フェイルオーバー、再試行可能エラー、致命的エラー、およびリカバリー済みエラーを表示します。 • 2 – パス・フェイルオーバー、コントローラー・フェイルオーバー、再試行可能エラー、および致命的エラーを表示します。 • 3 – パス・フェイルオーバー、コントローラー・フェイルオーバー、および致命的エラーを表示します。これがデフォルトの設定値です。 • 4 – コントローラー・フェイルオーバーおよび致命的エラーを表示します。 • 5 – 致命的エラーを表示します。 お客様サポート担当員および技術サポート担当員専用です。
-g <i>target_id</i>	指定されたストレージ・サブシステムの各コントローラー、パス、および LUN の状態についての詳細情報を表示します。 <i>target_id</i> は、<i>dsmUtil -a</i> コマンドを実行することにより検索できます。
-M	DSM の MPIO ディスクからドライブへのマッピングを表示します。出力は、SMdevices ユーティリティの検索結果に似ています。お客様サポート担当員および技術サポート担当員専用です。
-o [[<i>feature_action_name</i> [=value]] [<i>feature_variable_name</i> =value]], SaveSettings]	機能のトラブルシューティングを行うか、構成設定を変更します。SaveSettings キーワードを指定しない場合、変更はその変数のメモリー内の状態にのみ影響を与えます。SaveSettings キーワードは、メモリー内の状態と永続的状態の両方を変更します。コマンドの例を以下にいくつか示します。 • <i>dsmUtil -o</i> – すべての使用可能な機能アクション名を表示します。 • <i>dsmUtil -o DisableLunRebalance=0x3</i> – DSM 開始のストレージ・サブシステム LUN 再バランスをオフにします (メモリー内の状態にのみ影響を与えます)。
-P [GetMpioParameters MpioParameter= value ...]	MPIO パラメーターの表示および設定を行います。お客様サポート担当員および技術サポート担当員専用です。
-R	非アクティブ・デバイスのロード・バランシング・ポリシー設定を除去します。
-s ["failback" "avt" "busscan" "forcerebalance"]	DSM ドライバーのいずれかのスキャン・タスクを手動で開始します。「failback」スキャンでは、DSM ドライバーは障害が起きたコントローラーとの通信を再試行します。「avt」スキャンでは、DSM ドライバーはストレージ・サブシステム全体について、AVT が使用可能または使用不可になっているかどうかを検査します。「busscan」スキャンでは、DSM ドライバーは未構成装置のリストをスキャンして、構成済みになっている装置があるかどうかを調べます。「forcerebalance」スキャンでは、DSM ドライバーはストレージ・サブシステムの論理ドライブをそれらの優先コントローラーに移動し、DSM ドライバーの DisableLunRebalance 構成パラメーターの値を無視します。
-w <i>target_wnn</i> , <i>controller_index</i>	お客様サポート担当員および技術サポート担当員専用です。

Veritas DMP DSM ドライバー

Veritas DMP DSM ドライバーのインストール方法については、<http://www.symantec.com/business/support/> で Symantec Storage Foundation for Windows の資料を参照してください。

AIX マルチパス・ドライバー

AIX ホスト・システムは、ファイバー・チャネル・パスの冗長性を確保するために、AIX 冗長ディスク・アレイ・コントローラー (RDAC) かまたは MPIO フェイルオーバー・ドライバーのどちらかを必要とします。サポートされる Veritas 環境では、サポートされるフェイルオーバー・ドライバーは RDAC です。

フェイルオーバー・ドライバーは、入出力パスをモニターします。ファイバー・チャンネル・パスのいずれか 1 つでコンポーネントの障害が発生すると、フェイルオーバー・ドライバーがすべての入出力を別のパスに転送します。

注: AIX は、冗長ディスク・アレイ・コントローラー (RDAC) およびマルチパス入出力の両方をサポートします。これらのマルチパス・ドライバーは、AIX オペレーティング・システムに組み込まれています。これらのドライバーのインストールについての詳細は、AIX 資料を参照してください。

Linux Device Mapper Multipath ドライバー

Device Mapper Multipath (DMMP または DM-MP) は、Linux オペレーティング・システムで提供されるブロック・デバイス用の汎用フレームワークです。これは、連結、ストライピング、スナップショット、ミラーリング、およびマルチパスをサポートします。マルチパス機能は、カーネル・モジュールとユーザー・スペース・ツールを組み合わせた機能です。

重要: Linux Device Mapper Multipath ドライバーをインストールするホストは、Linux 非 AVT/非 ADT (Linux) または LinuxCluster (LNXCLUSTER) のいずれかであることが必要です。ADT または AVT の状況は、ストレージ・サブシステム・プロファイルにあるホスト・タイプ情報の中で検証できます。Linux Device Mapper Multipath ドライバーがインストールされているホストの ADT または AVT 状況は、「使用不可」でなければなりません。

Device Mapper Multipath ドライバーは、以下の働きをします。

- マルチパス論理装置に単一のブロック・デバイス・ノードを提供します。
- パスの障害発生時に、使用可能なパスに入出力が確実に再経路指定されるようにします。
- 障害が起こったパスができるだけ速やかに再検証されるようにします。
- パフォーマンスを最大化するためにマルチパスを構成します。
- イベント発生時にマルチパスを自動的に再構成します。
- 新しく追加された論理装置に DMMP 機能のサポートを提供します。
- /dev/mapper/ のもとで DMMP デバイスのデバイス名の永続化を行います。
- マルチパス論理装置で OS をインストールおよびリブートできるように、リブートの早い段階でマルチパスを自動的に構成します。

Device Mapper Multipath (DMMP または DM-MP) は、SLES11、SLES11 SP1、RHEL 6.0、RHEL 6.1、またはそれらの以降のバージョンでサポートされます。

Device Mapper MultiPath ドライバーのインストール

Device Mapper Multipath (DMMP または DM-MP) は、SLES11、SLES11 SP1、RHEL 6.0、RHEL 6.1、またはそれらの以降のバージョンでサポートされます。

DMMP でサポートされている DS3000/DS5000 サブシステムおよびコントローラーのファームウェア・バージョンについては、<http://www.ibm.com/systems/support/storage/config/ssic> を参照してください。

SLES11 base への Device Mapper MultiPath のインストール

注: ALUA 機能は、SLES 11 base ではサポートされません。SLES 11 SP1 以降 (コントローラー・ファームウェア・バージョン 7.8x.xx.xx 以降を搭載) にアップグレードする必要があります。

SLES 11 base オペレーティング・システムには、IBM DS ストレージ・サブシステム用のデバイス・マッパーをサポートするためのパッケージが、すべて含まれているわけではありません。可能であれば、以下の

コンポーネントは最新バージョンのものを使用することをお勧めします。可能でない場合、少なくとも以下のバージョンのコンポーネントを使用する必要があります。

表 26. 各コンポーネントの最小必須バージョン

コンポーネント	最小バージョン	ダウンロード場所
カーネル	kernel-default-2.6.27.29-0.1.1	http://download.novell.com/patch/finder
scsi_dh_rdac driver	lsi-scsi_dh_rdac-kmp-default-0.0_2.6.27.19_5-1	http://drivers.suse.com/driver-process/pub/update/LSI/sle11/common/x86_64/
デバイス・マッパー・ライブラリー	device-mapper-1.02.27-8.6	http://download.novell.com/patch/finder
Kpartx	kpartx-0.4.8-40.6.1	http://download.novell.com/patch/finder
Multipath_tools	multipath-tools-0.4.8-40.6.1	http://download.novell.com/patch/finder

先に進む前に、必ずすべての従属パッケージをインストールしてください。詳しくは、Novel/SuSe Web サイトにある「SUSE Linux Enterprise Server 11 Installation and Administration Guide」を参照してください。

SLES11 base に Device Mapper Multipath をインストールするには、以下の手順を実行します。

1. オペレーティング・システムのベンダーが提供するメディアを使用して、SLES 11 のインストールを完了します。
2. エラッタ・カーネル 2.6.27.29-0.1 をダウンロードし、インストールします。
3. リブートして 2.6.27.29-0.1 カーネルを有効にします。
4. device-mapper-1.02.27-8.6 をインストールします。
5. kpartx-tools-0.4.8-40.6.1 をインストールします。
6. multipath-tools-0.4.8-40.6.1 をインストールします。
7. /etc/multipath.conf を更新および構成します。サンプル・ファイルは /usr/share/doc/packages/multipath-tools/multipath.conf.synthetic に格納されています。このファイルをコピーして /etc/multipath.conf に名前変更します。詳しくは、143 ページの『Multipath.conf ファイルの処理』を参照してください。
8. コマンド `#chkconfig multipathd on` を使用してマルチパス・サービスを使用可能にします。
9. /etc/sysconfig/kernel ファイルを編集して、scsi_dh_rdac を INITRD_MODULES リストに追加します。これで、scsi_dh_rdac が initrd に追加されるはずです。
10. lsi-scsi_dh_rdac-kmp-default-0.0_2.6.27.19_5-1 をインストールします。
11. ホストをリブートします。

SLES11 sp1 以降への Device Mapper MultiPath のインストール

DMMP に必要なすべてのコンポーネントが、SUSE Linux Enterprise Server (SLES) バージョン 11.1 sp1 インストール・メディアに含まれています。SLES では、DMMP はデフォルトで使用不可になっています。ホストで DMMP コンポーネントを使用可能にするには、以下の手順を実行します。

注: Asymmetric Logical Unit Access (ALUA) は、コントローラー・ファームウェア 7.83.xx.xx 以降でサポートされています。SLES sp2 以降では、ALUA 用に必要なパッチがカーネルの配布の一部として提供されます。

1. オペレーティング・システムのベンダーが提供するメディアを使用して、SLES11 sp1 のインストールを完了します。

2. SLES 11 sp2 以降をインストール済みの場合は、このステップをスキップしてください。それ以外の場合は、`perform rpm -qa | grep <name of the package>` を実行して、以下のパッケージがインストールされているかどうかを確認します。

- `kpartx-0.4.8-40.21.1.1.09.00.0000.0006`
- `multipath-tools-0.4.8-40.21.1.1.09.00.0000.0000`
- `scsi_dh_rdac-kmp-default-09.00.0000.0006_2.6.32.12_0.7-sles11.1`

その後、ALUA 機能を使用可能にするために、次の `rpm` コマンドを使用してパッケージをインストールします。

- `rpm -ivh kpartx-0.4.8-40.21.1.1.00.00.0000.0005.<arch>.rpm --force`
- `rpm -ivh multipath-tools-0.4.8-40.21.1.1.00.00.0000.0005.<arch>.rpm --force`
- `rpm -ivh scsi_dh_rdac-kmp-default-00.00.0000.000<X>_2.6.32.12_0.7-sles11.1.<arch>.rpm --force`

ここで、<arch> は、適切なアーキテクチャー (x86、x86_x64、または PPC64) で置き換えてください。

3. `/etc/multipath.conf` を更新および構成します。サンプル・ファイルは `/usr/share/doc/packages/multipath-tools/multipath.conf.synthetic` に格納されています。このファイルをコピーして `/etc/multipath.conf` に名前変更します。詳しくは、143 ページの『Multipath.conf ファイルの処理』を参照してください。
4. コマンド `#chkconfig multipathd on` を使用してマルチパス・サービスを使用可能にします。
5. ファイル `/etc/sysconfig/kernel` を編集して、`scsi_dh_rdac` を `INITRD_MODULES` リストに追加します。これで、`scsi_dh_rdac` が `initrd` に追加されるはずです。
6. コマンド `# mkinitrd -k /boot/vmlinux-$(uname -r) -i /boot/initrd-$(uname -r)-scsi_dh -M /boot/System.map-$(uname -r)` を使用して、新しい `initrd` イメージを作成します。
7. 新しく作成した `initrd` を使用して、ブート・ローダー構成ファイル (`grub.conf`、`lilo.conf`、または `yaboot.conf`) を更新します。
8. ホストをリブートし、新しい `initrd` イメージでブートします。

RHEL 6.0、RHEL 6.1 以降への Device Mapper MultiPath のインストール

DMMP に必要なコンポーネントはすべて、RHEL 6 および 6.1 のインストール・メディアに含まれています。デフォルトでは、DMMP は使用不可になっています。ホストで DMMP コンポーネントを使用可能にするには、以下の手順を実行します。

注: Asymmetric Logical Unit Access (ALUA) は、RHEL 6.0 ではサポートされません。RHEL 6.1 以降にアップグレードする必要があります。また、コントローラー・ファームウェアは 7.83.xx.xx 以降でなければなりません。

1. オペレーティング・システムのベンダーが提供するメディアを使用して、RHEL 6.0、RHEL 6.1 以降のインストールを完了します。
2. RHEL 6 更新 2 をインストール済みの場合、RHEL 6 更新 2 以降には ALUA をサポートするために必要なパッチが既に含まれているため、このステップをスキップしてください。これらのパッチは、カーネルの配布の一部として提供されます。それ以外の場合は、`perform rpm -qa | grep <name of the package>` を実行して、以下のパッケージがインストールされているかどうかを確認します。

- `kpartx-0.4.8-40.21.1.1.09.00.0000.0006`
- `multipath-tools-0.4.8-40.21.1.1.09.00.0000.0000`
- `scsi_dh_rdac-kmp-default-09.00.0000.0006_2.6.32.12_0.7-sles11.1`

その後、ALUA 機能を使用可能にするために、次の rpm コマンドを使用してパッケージをインストールします。

- **rpm -ivh kpartx-0.4.8-40.21.1.1.00.00.0000.0005.<arch>.rpm --force**
- **rpm -ivh device-mapper-multipath-libs-0.4.9-41.1.el6.00.00.0000.0005.<arch>.rpm --force**
- **rpm -ivh device-mapper-multipath-0.4.9-41.1.el6.00.00.0000.000<X>.<arch>.rpm --force**
- **rpm -ivh scsi_dh_rdac-kmod-00.00.0000.0005-el6.<arch>.rpm**

ここで、<arch> は、適切なアーキテクチャー (x86、x86_x64、または PPC64) で置き換えてください。

3. /etc/multipath.conf を更新および構成します。サンプル・ファイルは /usr/share/doc/packages/multipath-tools/multipath.conf.synthetic に格納されています。このファイルをコピーして /etc/multipath.conf に名前変更します。詳しくは、『Multipath.conf ファイルの処理』を参照してください。
4. コマンド **#chkconfig multipathd on** を使用して、マルチパス・サービスを使用可能にします。
5. 以下のように、scsi_dh_rdac ドライバーを使用して initramfs イメージを作成します。
 - a. ファイル scsi_dh_alua.conf を /etc/modprobe.d/ ディレクトリーに作成します。
 - b. このファイルに **alias scsi_hostadapter99 scsi_dh_rdac** を追加します。
6. コマンド **#dracut -f /boot/initrd-\$(uname -r)-scsi_dh \$(uname -r)** を実行して、initramfs イメージを作成します。
7. initramfs を使用して、ブート・ローダー構成ファイル (grub.conf、lilo.conf、または yaboot.conf) を更新します。
8. ホストをリブートして、新しい initramfs イメージでブートします。

Multipath.conf ファイルの処理

Multipath.conf は、マルチパス・デーモン multipathd の構成ファイルです。このファイルは、multipathd の組み込み構成テーブルをオーバーライドします。ファイル内で、先頭に非空白文字 # がある行はすべてコメント行です。空の行は無視されます。

デフォルトでは、DMMP は IBM DS3000/DS5000 サブシステムの特定のマシン・タイプ・モデルでサポートされます。ただし IBM では、DMMP の設定が確実に以下になるよう、multipath.conf ファイルを使用してデフォルト設定をオーバーライドすることを推奨します。

multipath.conf ファイルをセットアップするには、以下の手順を実行します。

1. Linux オペレーティング・システムが Redhat RHEL か Novell SLES のどちらであるかに応じて、該当するディレクトリーからサンプル・ファイル multipath.conf を /etc ディレクトリーにコピーします。
 - SLES の場合、このファイルは multipath.conf.synthetic という名前であり、/usr/share/doc/packages/multipath-tools/ ディレクトリーに格納されています。
 - RHEL の場合、このファイルは multipath.conf.defaults という名前であり、/usr/share/doc/device-mapper-multipath-0.4.9/ ディレクトリーに格納されています。
2. ファイル multipath.conf を名前変更します。
3. 新しい /etc/multipath.conf ファイルに対して、このセクションで説明されている構成変更を行います。サンプル・ファイル multipath.conf の内容は、それが SLES または RHEL のどちらのカーネルからのものであるかによって異なります。

注: マルチパス・デバイスのすべてのエントリーは最初にコメント化されます。コメントを外すには、そのセクションの先頭文字 (#) を削除します。default、blacklist、および devices の 3 つのセクションのコメントを外す必要があります。
構成ファイルは、次のように 5 つのセクションに分割されます。

defaults

すべてのデフォルト値を指定します。

blacklist

新規インストールをブラックリストに記載します。デフォルトのブラックリストは、/etc/multipath.conf ファイルのコメント化されたセクションにリストされます。この機能を使用しない場合、デバイス・マッパー・マルチパスを WWID ごとにブラックリストに入力します。

blacklist_exceptions

blacklist セクション内の項目に対する例外をすべて指定します。

デバイス

すべてのマルチパス・デバイスを、それに対応するベンダーおよび製品の値と共にリストします。

multipaths

すべてのマルチパス・デバイスを、それに対応する WWID 値と共にリストします。

マルチパス・デバイスの属性を判別するには、/etc/ multipath.conf ファイルの multipaths セクション、続いて devices セクション、defaults セクションの順に調べます。Linux カーネルのバージョンによっては、サンプル・ファイル multipath.conf の devices セクションで、ご使用のストレージ・サブシステム・モデルの製品 ID 用の設定が定義済みになっている場合があります。必要な作業は、その設定が以下にリストされた推奨設定と一致しているかどうかを確認することのみです。まだ設定が定義されていない場合は、ご使用のサブシステム・モデルの製品 ID のデバイス設定を手動で入力する必要があります。それぞれ異なる製品 ID を持つ複数のストレージ・サブシステムが Linux ホストに接続されている場合、各ストレージ・サブシステムの製品 ID のデバイス設定を /etc/ multipath.conf ファイルの devices セクションに追加してください。SLES オペレーティング・システムにおける、multipath.conf ファイルの devices セクションの DS3500 (製品 ID 1746) と DS5100/DS5300 (製品 ID 1818) のサンプル設定を、以下に示します。

注: 製品 ID が 4 文字を超える場合、最初の 4 文字のみを使用してください。次の例の場合、製品 ID は「1746 FAStT」ですが、製品は「1746」として指定されています。同様に、「1818 FAStT」は「1818」として指定されています。

```
Devices {
  device {

        vendor                "IBM"
        product                "1746"
        path_grouping_policy    group_by_prio
        getuid_callout          "/lib/udev/scsi_id -g -u -d /dev/%n"
        path_selector           "round-robin 0"
        path_checker            rdac
        features                "2 pg_init_retries 50"
        hardware_handler        "1 rdac"
        prio                    rdac
        failback                immediate
        no_path_retry           15
        rr_min_io               100
        rr_weight               priorities
    }
}
```



```

device {

    vendor                "IBM"
    product               "1818"
    path_grouping_policy  group_by_prio
    getuid_callout        "/lib/udev/scsi_id -g -u -d /dev/%n"
    path_selector         "round-robin 0"
    path_checker          rdac
    features              "2 pg_init_retries 50"
    hardware_handler      "1 rdac"
    prio                  rdac
    failback              immediate
    no_path_retry         15
    rr_min_io             100
    rr_weight             priorities
}

```

RHEL オペレーティング・システムにおける、multipath.conf ファイルの devices セクションの DS3500 (製品 ID 1746) と DS5100/DS5300 (製品 ID 1818) のサンプル設定を、以下に示します。

```

Devices {
    device {

        vendor                "IBM"
        product               "1746"
        path_grouping_policy  group_by_prio
        getuid_callout        "/lib/udev/scsi_id --whitelisted --device=/dev/%n"
        path_selector         "round-robin 0"
        path_checker          rdac
        features              "2 pg_init_retries 50"
        hardware_handler      "1 rdac"
        prio                  rdac
        failback              immediate
        no_path_retry         15
        rr_min_io             100
        rr_weight             priorities
    }

    device {

        vendor                "IBM"
        product               "1818"
        path_grouping_policy  group_by_prio
        getuid_callout        "/lib/udev/scsi_id --whitelisted --device=/dev/%n"
        path_selector         "round-robin 0"
        path_checker          rdac
        features              "2 pg_init_retries 50"
        hardware_handler      "1 rdac"
        prio                  rdac
        failback              immediate
        no_path_retry         15
        rr_min_io             100
        rr_weight             priorities
    }
}

```

アクセス LUN (UTM LUN と呼ばれることもあります) がホスト区画にマップされている場合、/etc/multipath.conf ファイルの blacklist セクションにエントリーを含めて、このファイルが DMMP によって管理されないようにします。ストレージ・マネージャーのホスト・ソフトウェアは、アクセス LUN を使用してストレージ・サブシステムのインバンド管理を行います。エントリーは、次の例のパターンに従っている必要があります。

```

blacklist {
  device {
    vendor "*"
    product "Universal Xport"
  }
}

```

次の表では、`/etc/multipath.conf` ファイルの `devices` セクションの属性と値を説明します。

表 27. `multipath.conf` ファイルの属性およびパラメーター値

属性	パラメーター値	説明
<code>path_grouping_policy</code>	<code>group_by_prio</code>	この属性は、この特定のベンダーおよび製品ストレージに適用されるバス・グループ化ポリシーを決定します。
<code>prio</code>	<code>rdac</code>	この属性は、バス優先順位ルーチンを判別するためのプログラムおよび引数を設定します。指定されるルーチンは、このバスの相対優先順位を指定する数値を返します。数値が高いほど、優先順位が高くなります。
<code>getuid_callout</code>	SLES の場合は <code>"/lib/udev/scsi_id -g -u -d /dev/%n"</code> 、RHEL の場合は <code>"/lib/udev/scsi_id --whitelisted--device=/dev/%n"</code>	この属性は、固有バス ID のコールアウトおよび取得のためのプログラムおよび引数を決定します。
<code>polling_interval</code>	<code>5</code>	この属性は、2 つのバス検査の間隔 (秒単位) を決定します。
<code>path_checker</code>	<code>rdac</code>	この属性は、バスの状態を判別するために使用される方式を設定します。
<code>path_selector</code>	<code>"round-robin 0"</code>	この属性は、バス・グループに複数のバスがある場合に使用するバス・セレクター・アルゴリズムを決定します。
<code>hardware_handler</code>	<code>"1 rdac"</code>	この属性は、デバイス固有情報を処理するために使用するハードウェア・ハンドラーを決定します。
<code>failback</code>	<code>immediate</code>	この属性は、デーモンがバス・グループ・フェイルバックを管理する方法を決定します。この例では、パラメーターが 10 秒に設定されているため、デバイスがオンラインになった 10 秒後にフェイルバックが行われます。フェイルバックを使用不可にするには、このパラメーターを <code>manual</code> に設定します。フェイルバックが即時に行われるように強制するには、 <code>immediate</code> に設定します。
フィーチャー	<code>"2 pg_init_retries 50"</code>	この属性は、フィーチャーを使用可能にします。この例では、カーネル・パラメーター <code>pg_init_retries</code> が 50 に設定されています。パラメーター <code>pg_init_retries</code> は、モード選択コマンドを再試行するために使用されます。

表 27. *multipath.conf* ファイルの属性およびパラメーター値 (続き)

属性	パラメーター値	説明
<code>no_path_retry</code>	30	この属性は、キューイングが使用不可になる前の再試行回数を決定します。即時の失敗 (キューイングなし) の場合、このパラメーターを <code>fail</code> に設定します。このパラメーターが <code>queue</code> に設定されている場合、キューイングは永久に続行されます。
<code>rr_min_io</code>	100	同じバス・グループ内の次のバスに切り替える前に、バスに経路指定する入出力の数。
<code>rr_weight</code>	<code>priorities</code>	<code>priorities</code> に設定すると、マルチバス・コンフィギュレーターはバスの重みを「 <code>path prio * rr_min_io</code> 」として割り当てます。

デバイス・マッパー・デバイスの使用

マルチバス・デバイスは、`/dev/` ディレクトリ一下で接頭部 `dm-` を付けられて作成されます。これらのデバイスは、ホスト上のその他のブロック・デバイスと同じです。すべてのマルチバス・デバイスをリストするには、**`multipath -ll`** コマンドを実行します。次の例は、非 ALUA フェイルオーバー・モードのマルチバス・デバイスのいずれかに対する **`multipath -ll`** コマンドからのシステム出力を示しています。

```
mpathp (3600a0b80005ab177000017544a8d6b92) dm-0 IBM, 1746 FASTT
[size=5.0G][features=3 queue_if_no_path pg_init_retries
50][hwhandler=1 rdac][rw]
_ round-robin 0 [prio=6][active]
_ 5:0:0:0 sdc 8:32 [active][ready]
_ round-robin 0 [prio=1][enabled]
_ 4:0:0:0 sdb 8:16 [active][ghost]
```

次の例は、ALUA フェイルオーバー・モードのマルチバス・デバイスのいずれかに対する **`multipath -ll`** コマンドからのシステム出力を示しています。

```
mpathf (3600a0b800047516e00006d864f70696c) dm-11 IBM, 1746 FASTT
size=1.0G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1 rdac' wp=rw
| -+- policy='round-robin 0' prio=14 status=active
|   ^- 9:0:0:3 sdac 65:192 active ready running
| -+- policy='round-robin 0' prio=9 status=enabled
|   ^- 10:0:0:3 sds 65:32 active ready running
```

これは、優先順位が 14 と 9 (LUN が優先コントローラー上にある場合) の 2 つのアクティブな作動可能バスを表示します。代替の非優先コントローラーが LUN を所有している場合は、次のように優先順位が 12 と 11 として表示されます。

```
mpathe (3600a0b800029e8320000623d4f70486a) dm-15 IBM, 1746 FASTT
size=1.0G features='3 queue_if_no_path pg_init_retries 50' hwhandler='1 rdac' wp=rw
| -+- policy='round-robin 0' prio=12 status=active
|   ^- 16:0:0:6 sdah 66:16 active ready running
| -+- policy='round-robin 0' prio=11 status=enabled
|   ^- 15:0:0:6 sdat 66:208 active ready running
```

上記の例で、このデバイスのマルチバス・デバイス・ノードは `/dev/mapper/mpathp` および `/dev/dm-0` です。次の表に、**`multipath`** コマンドの基本的なオプションとパラメーターをいくつかリストします。

表 28. **multipath** コマンドのオプションおよびパラメーター

コマンド	説明
<code>multipath -h</code>	使用法の情報を印刷します
<code>multipath -ll</code>	使用可能なすべての情報 (sysfs、デバイス・マッパー、パス・チェッカーなど) からの現行マルチパス・トポロジーを表示します。
<code>multipath -f map</code>	マップが使用されていない場合に、 <i>map</i> オプションによって指定されたマルチパス・デバイス・マップをフラッシュします。
<code>multipath -F</code>	使用されていないすべてのマルチパス・デバイス・マップをフラッシュします。

デバイス・マッパーのトラブルシューティング

デバイス・マッパーのトラブルシューティングを行うには、次の表の情報を使用してください。

表 29. デバイス・マッパーのトラブルシューティング

状態	アクション
マルチパス・デーモン <code>multipathd</code> が実行中であるかどうかを検査します。	コマンド・プロンプトで、コマンド <code>/etc/init.d/multipathd status</code> を実行します。
multipath -ll コマンドの実行時にデバイスがリストされない理由を判別します。	コマンド・プロンプトで、コマンド <code>#cat /proc/scsi/scsi</code> を実行します。システム出力に、既にディスクカバーされたすべてのデバイスが表示されます。 <code>multipath.conf</code> ファイルが適切な設定で更新されていることを確認します。

既知の問題と制限

- ストレージが ADT/AVT モードを使用して構成されている場合、デバイスのディスクバリーで遅延が生じる可能性があります。デバイス・ディスクバリーで遅延が生じると、オペレーティング・システムのブート時に遅延が長くなる場合があります。
- `no_path_retry` または `queue_if_no_path` 機能が使用可能な場合の特定のエラー状態においては、アプリケーションがハングしたままになる可能性があります。これらの状態を解決するには、影響が及ぶすべてのマルチパス・デバイスにコマンド `dmsetup message device 0 "fail_if_no_path"` を入力する必要があります。ここで、`device` はマルチパス・デバイス名です。
- 最初に DM デバイスを削除せずに論理ドライブをマップ解除すると、入出力のハングが発生する可能性があります。この制限が適用されるのは、SLES11 base のみです。これは、後のバージョンで修正されます。
- 最初に DM デバイスとその基礎にあるパスを削除せずに論理ドライブをマップ解除または削除すると、`multipath -ll` の出力に無効なエントリーが生じる可能性があります。この制限が適用されるのは、SUSE 11 base OS のみです。
- デバイス・マッパーでは、モード選択コマンドは各 LUN で同期的に発行されます。大規模な LUN 構成では、モード選択コマンドの完了に遅延が発生すると、DM マルチパス・デバイスのフェイルオーバーが遅くなる可能性があります。この制限が適用されるのは、SUSE 11 base OS のみです。これは、後のバージョンで解決済みになっています。
- `scsi_dh_rdac` モジュールが `initrd` に含まれていない場合、デバイスのディスクバリーが遅くなる可能性があります。また、`syslog` にバッファ入出力エラー・メッセージが書き込まれる場合があります。

- ストレージのベンダーとモデルが `scsi_dh_rdac` デバイス・ハンドラーに含まれていない場合、デバイスのディスカバリーが遅くなる可能性があります、`syslog` にバッファ入出力エラー・メッセージが書き込まれる場合があります。
- 同じホスト上で DMMP と RDAC のフェイルオーバー・ソリューションを一緒に使用することはサポートされません。一度に 1 つのソリューションのみを使用してください。

Linux RDAC (MPP) ドライバー

このセクションでは、Linux 構成用 RDAC (MPP) ドライバーをインストールする方法について説明します。ALUA 機能は、SLES SP1、RHEL 6.1 以降のバージョンでサポートされます。IBM では、新しいサーバーおよびストレージ・サブシステムの構成に Linux Device Mapper Multipath ドライバーを使用することをお勧めします。Linux RDAC (MPP) マルチパス・ドライバーのサポートは、コントローラー・ファームウェア・バージョン 7.8x.xx.xx で打ち切られることになっています。

重要: MPP をインストールする前に、区画および LUN が構成され、割り当てられており、正しい HBA ドライバーがインストールされていることを確認してください。

MPP をインストールするには、以下の手順を完了します。

1. MPP ドライバー・パッケージを IBM System Storage Disk サポート・ポータルからダウンロードします。
2. ホスト上にディレクトリを作成し、そのディレクトリに MPP ドライバー・パッケージをダウンロードします。
3. 次のコマンドを入力して、ファイルを解凍します。

```
# tar -zxvf rdac-LINUX-package_version-source.tar.gz
```

ここで、`package_version` は SLES または RHEL パッケージのバージョン番号です。結果として、`linuxrdac-version#` または `linuxrdac` というディレクトリが作成されます。

4. `linuxrdac-version#` ディレクトリにある README を開きます。
5. README の中で、ドライバーの作成およびインストールの説明を見つけ、すべての手順を完了します。

注: 次のステップに進む前に、必ずサーバーを再始動してください。

6. 次のコマンドを入力して、インストール済みのモジュールを表示します。

```
# lsmod
```

7. モジュール項目が次の `lsmod` リストに組み込まれていることを検証します。

SLES または RHEL 用のモジュール項目

- `scsi_mod`
- `sd_mod`
- `sg`
- `mppVhba`
- `mppUpper`
- `lpfc` (または BladeCenter 構成用の `qla2xxx`)
- `lpfcdfc` (`ioctl` モジュールがインストール済みの場合)

注: mpp_Vhba モジュールが見えない場合、その原因として、LUN が割り当てられる前にサーバーがリブートされたために、mpp_Vhba モジュールがインストールされていないことが考えられます。このような場合は、この時点で LUN を割り当ててからサーバーを再始動して、このステップを繰り返します。

8. 次のコマンドを入力して、ドライバーのバージョンを検証します。

```
# mppUtil -V
```

Linux マルチパス・ドライバー・バージョンが表示されます。

9. 次のコマンドを入力して、デバイスが RDAC ドライバーにより構成されていることを検証します。

```
# ls -lR /proc/mpp
```

次の例と同様の出力が表示されます。

```
# ls -lR /proc/mpp
/proc/mpp:
total 0
dr-xr-xr-x    4 root    root          0 Oct 24 02:56 DS4100-sys1
crwxrwxrwx    1 root    root        254,  0 Oct 24 02:56 mppVBusNode

/proc/mpp/ DS4100-sys1:
total 0
dr-xr-xr-x    3 root    root          0 Oct 24 02:56 controllerA
dr-xr-xr-x    3 root    root          0 Oct 24 02:56 controllerB
-rw-r--r--    1 root    root          0 Oct 24 02:56 virtualLun0
-rw-r--r--    1 root    root          0 Oct 24 02:56 virtualLun1
-rw-r--r--    1 root    root          0 Oct 24 02:56 virtualLun2
-rw-r--r--    1 root    root          0 Oct 24 02:56 virtualLun3
-rw-r--r--    1 root    root          0 Oct 24 02:56 virtualLun4
-rw-r--r--    1 root    root          0 Oct 24 02:56 virtualLun5

/proc/mpp/ DS4100-sys1/controllerA:
total 0
dr-xr-xr-x    2 root    root          0 Oct 24 02:56 lpfc_h6c0t2

/proc/mpp/ DS4100-sys1/controllerA/lpfc_h6c0t2:
total 0
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN0
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN1
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN2
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN3
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN4
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN5

/proc/mpp/ DS4100-sys1/controllerB:
total 0
dr-xr-xr-x    2 root    root          0 Oct 24 02:56 lpfc_h5c0t0

/proc/mpp/ DS4100-sys1/controllerB/lpfc_h5c0t0:
total 0
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN0
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN1
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN2
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN3
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN4
-rw-r--r--    1 root    root          0 Oct 24 02:56 LUN5
```

10. RDAC ドライバーが使用可能な物理論理ドライブとそれ用に作成された仮想論理ドライブを確実に検出できるようにする別の方法として、コマンド `/opt/mpp/lsvdev` を入力して **Enter** キーを押すこともできます。ここで、入出力を論理ドライブに送信することができます。
11. RDAC 構成ファイル (`/etc/mpp.conf`) または永続バインディング・ファイル (`/var/mpp/devicemapping`) に変更を加えた場合は、mppUpdate コマンドを実行して、新規ファイルを組み込むた

めに RAMdisk イメージを再作成します。これにより、次のシステム再始動時に、新しい構成ファイル (または、永続バインディング・ファイル) を使用できます。

12. システムを再始動せずにドライバー・スタック (mppUpper、物理 HBA ドライバー・モジュール、mppVhba) を動的に再ロードするには、以下の手順を実行します。
 - a. mppVhba ドライバーをアンロードするために、コマンド `rmmod mppVhba` を入力して、**Enter** キーを押します。
 - b. 物理 HBA ドライバーをアンロードするために、コマンド `modprobe -r "physical hba driver modules"` を入力して、**Enter** キーを押します。
 - c. mppUpper ドライバーをアンロードするために、コマンド `rmmod mppUpper` を入力して、**Enter** キーを押します。
 - d. mppUpper ドライバーを再ロードするために、コマンド `modprobe mppUpper` を入力して、**Enter** キーを押します。
 - e. 物理 HBA ドライバーを再ロードするために、コマンド `modprobe "physical hba driver modules"` を入力して、**Enter** キーを押します。
 - f. mppVhba ドライバーを再ロードするために、コマンド `modprobe mppVhba` を入力して、**Enter** キーを押します。
13. システムを再始動して、ドライバー・スタックをアンロードします。

注: RDAC ドライバーがインストールされると、以下のコマンドおよびページが使用可能になります。

- mppUtil
- mppBusRescan
- mppUpdate
- RDAC

mppUtil の概要

mppUtil ユーティリティーは、MPP ベースの RDAC ソリューションでのみ機能する、汎用コマンド行駆動型ユーティリティーです。このユーティリティーは、RDAC による各種のメンテナンス・タスクの実行を指示するだけでなく、必要な場合はトラブルシューティング・ツールとしての役目も果たします。

mppUtil ユーティリティーを使用するには、以下のコマンドを入力して、**Enter** キーを押します。

```
mppUtil [-a target_name] [-c wwn_file_name] [-d
debug_level]
[-e error_level] [-g virtual_target_id] [-I host_num]
[-o feature_action_name[=value][, SaveSettings]]
[-s "failback" | "avt" | "busscan" | "forcerebalance"]
[-S] [-U]
[-V] [-w target_wwn,controller_index]
```

注: パラメーターは二重引用符で囲む必要があります。

mppUtil ユーティリティーはクロスプラットフォーム・ツールです。各パラメーターの説明を以下に示します。

表 30. mppUtil パラメーターの説明

パラメーター	説明
-a <i>target_name</i>	指定された仮想 <i>target_name</i> (ストレージ・サブシステム名) に関する RDAC ドライバーの内部情報を表示します。 <i>target_name</i> 値が含まれていない場合、-a パラメーターは、このホストによって現在検出されているすべてのストレージ・サブシステムに関する情報を表示します。
-c <i>wnn_file_name</i>	WWN ファイルの項目をクリアします。このファイルは、/var/mpp にあり、拡張子 .wnn が付いています。
-d <i>debug_level</i>	現行のデバッグ・レポート・レベルを設定します。このオプションは、デバッグを有効にして RDAC ドライバーをコンパイルした場合にのみ使用できます。デバッグ・レポートは、2 つのセグメントで構成されます。最初のセグメントは、機能の特定の領域を示し、2 番目のセグメントは、その領域内のレポートのレベルを示します。<i>debug_level</i> は、以下の 16 進数のいずれかです。 • 0x20000000- RDAC ドライバーの init() ルーチンからのメッセージを表示します。 • 0x10000000- RDAC ドライバーの attach() ルーチンからのメッセージを表示します。 • 0x08000000- RDAC ドライバーの ioctl() ルーチンからのメッセージを表示します。 • 0x04000000- RDAC ドライバーの open() ルーチンからのメッセージを表示します。 • 0x02000000- RDAC ドライバーの read() ルーチンからのメッセージを表示します。 • 0x01000000- HBA コマンドに関連したメッセージを表示します。 • 0x00800000- 異常終了したコマンドに関連したメッセージを表示します。 • 0x00400000- パニック・ダンプに関連したメッセージを表示します。 • 0x00200000- 同期入出力アクティビティに関連したメッセージを表示します。 • 0x00000001- デバッグ・レベル 1。 • 0x00000002- デバッグ・レベル 2。 • 0x00000004- デバッグ・レベル 3。 • 0x00000008- デバッグ・レベル 4。 必要に応じて、これらのオプションを論理 AND 演算子を使用して結合し、複数の領域およびレベルのレポートを提供することができます。お客様サポート担当員および技術サポート担当員専用です。

表 30. mppUtil パラメーターの説明 (続き)

パラメーター	説明
-e <i>error_level</i>	現行のエラー・レポート・レベルを <i>error_level</i> に設定します。以下のいずれかの値を指定できます。 • 0 - すべてのエラーを表示します。 • 1 - パス・フェイルオーバー、コントローラー・フェイルオーバー、反復可能エラー、致命的エラー、およびリカバリー済みエラーを表示します。 • 2 - パス・フェイルオーバー、コントローラー・フェイルオーバー、反復可能エラー、および致命的エラーを表示します。 • 3 - パス・フェイルオーバー、コントローラー・フェイルオーバー、および致命的エラーを表示します。これがデフォルトの設定値です。 • 4 - コントローラー・フェイルオーバーおよび致命的エラーを表示します。 • 5 - 致命的エラーを表示します。 お客様サポート担当員および技術サポート担当員専用です。
-g <i>target_id</i>	指定されたストレージ・サブシステムの各コントローラー、パス、および LUN の状態についての詳細情報を表示します。 <i>target_id</i> は、dsmUtil -a コマンドを実行することにより検索できます。
-M	DSM の MPIO ディスクからドライブへのマッピングを表示します。出力は、SMdevices ユーティリティの検索結果に似ています。お客様サポート担当員および技術サポート担当員専用です。
-o [[<i>feature_action_name</i> [= <i>value</i>]] [<i>feature_variable_name</i> = <i>value</i>]][, SaveSettings]	機能のトラブルシューティングを行うか、構成設定を変更します。SaveSettings キーワードを指定しない場合、変更はその変数のメモリー内の状態にのみ影響を与えます。SaveSettings キーワードは、メモリー内の状態と永続的状态の両方を変更します。コマンドの例を以下にいくつか示します。 • dsmUtil -o - すべての使用可能な機能アクション名を表示します。 • dsmUtil -o DisableLunRebalance=0x3 - DSM 開始のストレージ・サブシステム LUN 再バランスをオフにします (メモリー内の状態にのみ影響を与えます)。
-P [GetMpioParameters MpioParameter= <i>value</i> ...]	MPIO パラメーターの表示および設定を行います。お客様サポート担当員および技術サポート担当員専用です。
-R	非アクティブ・デバイスのロード・バランシング・ポリシー設定を除去します。

表 30. mppUtil パラメーターの説明 (続き)

パラメーター	説明
-s ["failback" "avt" "busscan" "forcerebalance"]	DSM ドライバーのいずれかのスキャン・タスクを手動で開始します。「failback」スキャンでは、DSM ドライバーは障害が起きたコントローラーとの通信を再試行します。「avt」スキャンでは、DSM ドライバーはストレージ・サブシステム全体について、AVT が使用可能または使用不可になっているかどうかを検査します。「busscan」スキャンでは、DSM ドライバーは未構成装置のリストをスキャンして、構成済みになっている装置があるかどうかを調べます。「forcerebalance」スキャンでは、DSM ドライバーはストレージ・サブシステムの論理ドライブをそれらの優先コントローラーに移動し、DSM ドライバーの DisableLunRebalance 構成パラメーターの値を無視します。
-w target_wwn, controller_index	お客様サポート担当員および技術サポート担当員専用です。

MAC OS マルチパス・ドライバー

サポートされている唯一の MAC OS マルチパス・ドライバーは、HBA ベンダーである ATTO Corporation が提供するマルチパス・ドライバーです。MAC OS マルチパス・ドライバーをインストールする説明については、ATTO IBM Solutions Web サイトにアクセスしてください。その Web サイトで、*ATTO Celerity MultiPaxath Director Installation and Operation Manual* の Celerity HBA ドライバーのインストールおよび ATTO Configuration Tool のインストールに関する情報を参照してください。

重要: LUN を構成した後、LUN が検出されるようにするには、サーバーをリブートする必要があります。

Veritas DMP ドライバー

Veritas DMP ドライバーのインストール方法については、<http://www.symantec.com/business/support/> で Symantec Storage Foundation for Windows の資料を参照してください。

注: ストレージ・サブシステムで DMP をサポートする Array Support Library (ASL) のロードが必要な場合があります。Storage Foundation のバージョンによって、ASL は Symantec から入手可能な別個のファイルであるか、Volume Manager に組み込まれている場合があります。

HP-UX PV-links

HP-UX システムが 2 つのホスト・バス・アダプターを使用しストレージ・サブシステムに接続している場合は、HP-UX オペレーティング・システムの 1 機能である物理ボリューム・リンク (PV-links) を使用して、ストレージに対して冗長アクセスを確立できます。PV-links は、同じデバイスへの基本パスおよび 2 次パスの両方を持つデバイスを使用することによって、アクセス冗長性を実現します。

重要:

- PV-links の使用によるストレージへの冗長アクセスの確立には、以下のような 2 つの方法があります。
 - コントローラー・ファームウェア・バージョンが 07.xx.xx.xx、06.xx.xx.xx、または 05.xx.xx.xx の場合、155 ページの『PV-links の使用: 方法 1』に記載されている方法を使用します。

- コントローラー・ファームウェア・バージョンが 04.xx.xx.xx の場合、156 ページの『PV-links の使用: 方法 2』に記載されている方法を使用します。
- いずれの方法の場合も、SMutil がホストにインストールされている必要があります。

PV-links の使用: 方法 1

コントローラー・ファームウェア・バージョンが 05.xx.xx.xx 以降の場合、以下の手順を使用して、PV リンクによるマルチパス入出力を使用可能にします。

1. シェル・プロンプトで、HP-UX から **hot_add** コマンドを実行します。このコマンドは、作成または追加された任意の新規デバイスを更新します。ダンプが生成されます。**hot_add** コマンドが実行されると、「Subsystem Management (サブシステム管理)」ウィンドウで作成された各新規論理ドライブは、オペレーティング・システムにディスク・デバイスとして表されます。
2. 「**SMdevices**」コマンドを実行します。システムは、以下の表の例と同様のダンプを提供します。すべての論理ドライブおよび論理ドライブのアクセス・ユニットには、論理装置番号 (LUN) が割り当てられていることに注意してください。各論理ドライブにはパスが 2 つあります。各ストレージ・サブシステム・コントローラーには論理ドライブ・アクセスが 1 つあります。

```
/dev/rdisk/cl66t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0,
Logical Drive WWN <600a0b80000f56d00000001e3eae2b>,
Preferred Path (Controller-B): In Use]
/dev/rdisk/cl66t0d1 [Storage Subsystem DS4000, Logical Drive HR, LUN 1,
Logical Drive WWN <600a0b80000f5d6c000000273eae30>,
Alternate Path (Controller-B): Not In Use]
/dev/rdisk/cl66t0d2 [Storage Subsystem DS4000, Logical Drive Finance,
LUN 2, Logical Drive WWN <600a0b80000f5d6c000000253eae30>,
Alternate Path (Controller-B): Not In Use]
/dev/rdisk/cl66t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing,
LUN 3, Logical Drive WWN <600a0b80000f5d6c000000243eae30>,
Alternate Path (Controller-B): Not In Use]
/dev/rdisk/cl66t0d4 [Storage Subsystem DS4000, Logical Drive Development,
LUN 4, Logical Drive WWN <600a0b80000f56d00000001d3eae30>,
Preferred Path (Controller-B): In Use]
/dev/rdisk/cl66t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f56d00000001b00000000>]
```

```
/dev/rdisk/cl72t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0,
Logical Drive WWN <600a0b80000f56d00000001e3eae2b>,
Alternate Path (Controller-A): Not In Use]
/dev/rdisk/cl72t0d1 [Storage Subsystem DS4000, logical Drive HR, LUN 1,
Logical Drive WWN <600a0b80000f5d6c000000273eae30>,
Preferred Path (Controller-A): In Use]
/dev/rdisk/cl72t0d2 [Storage Subsystem DS4000, Logical Drive Finance, LUN 2,
Logical Drive WWN <600a0b80000f5d6c000000253eae30>,
Preferred Path (Controller-A): In Use]
/dev/rdisk/cl72t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing, LUN 3,
Logical Drive WWN <600a0b80000f5d6c000000243eae30>,
Preferred Path (Controller-A): In Use]
/dev/rdisk/cl72t0d4 [Storage Subsystem DS4000, Logical Drive Development, LUN 4,
Logical Drive WWN <600a0b80000f56d00000001d3eae30>,
Alternate Path (Controller-A): Not In Use]
/dev/rdisk/cl72t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f5d6c0000002200000000>]
```

注: **hot_add** および **SMdevices** コマンドを実行した後に論理ドライブおよび論理ドライブ・アクセスが表示されない場合は、**reboot** コマンドを使用して HP-UX ホストを再始動してください。

3. 前の例に示されているように、**SMdevices** コマンドの出力を調べて、各論理ドライブの優先パスおよび代替パスを判別します。各デバイスは 2 回リストされることに注意してください。最初の例は優先パス、2 番目の例は代替パスです。

優先パス

下に示されている出力例では、優先パスは `/dev/rdisk/c166t0d0` です。

```
/dev/rdisk/c166t0d0 [Storage Subsystem DS4000, Logical Drive
Accounting, LUN 0, Logical Drive WWN <600a0b80000f56d00000001e3eae2b>,
Preferred Path (Controller-B): In Use]
```

代替パス

下に示されている出力例では、代替パスは `/dev/rdisk/c172t0d0` です。

```
/dev/rdisk/c172t0d0 [Storage Subsystem DS4000, Logical Drive
Accounting, LUN 0, Logical Drive WWN <600a0b80000f56d00000001e3eae2b>,
Alternate Path (Controller-A): NotIn Use]
```

PV-links の使用: 方法 2

コントローラー・ファームウェア・バージョンが 4.xx.xx.xx の場合、以下の手順を使用して、PV リンクによるマルチパス入出力を使用可能にします。

- 優先パスおよび代替パスを判別します
- 論理ドライブおよびアレイを作成します

優先パスおよび代替パスの判別

1. シェル・プロンプトで、HP-UX から **hot_add** コマンドを実行します。このコマンドは、作成または追加された任意の新規デバイスを更新します。ダンプが生成されます。**hot_add** コマンドが実行されると、「Subsystem Management (サブシステム管理)」ウィンドウで作成された各新規論理ドライブは、オペレーティング・システムにディスク・デバイスとして表されます。
2. 「**SMdevices**」コマンドを実行します。システムは、下記の例と同様のダンプを提供します。すべての論理ドライブおよび論理ドライブのアクセス・ユニットには、論理装置番号 (LUN) が割り当てられていることに注意してください。各論理ドライブにはパスが 2 つあります。各ストレージ・サブシステム・コントローラーには論理ドライブ・アクセスが 1 つあります。

```
/dev/rdisk/c166t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0,
Logical Drive WWN <600a0b80000f56d00000001e3eae2b>]
/dev/rdisk/c166t0d1 [Storage Subsystem DS4000, Logical Drive HR, LUN 1,
Logical Drive WWN <600a0b80000f5d6c000000273eae30>]
/dev/rdisk/c166t0d2 [Storage Subsystem DS4000, Logical Drive Finance, LUN 2,
Logical Drive WWN <600a0b80000f5d6c000000253eaeadf8>]
/dev/rdisk/c166t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing, LUN 3,
Logical Drive WWN <600a0b80000f5d6c000000243eaeadeb>]
/dev/rdisk/c166t0d4 [Storage Subsystem DS4000, Logical Drive Development, LUN 4,
Logical Drive WWN <600a0b80000f56d00000001d3eaeacef>]
/dev/rdisk/c166t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f56d00000001b00000000>]
```

```
/dev/rdisk/c172t0d0 [Storage Subsystem DS4000, Logical Drive Accounting, LUN 0,
Logical Drive WWN <600a0b80000f56d00000001e3eae2b>]
/dev/rdisk/c172t0d1 [Storage Subsystem DS4000, Logical Drive HR, LUN 1,
Logical Drive WWN <600a0b80000f5d6c000000273eae30>]
/dev/rdisk/c172t0d2 [Storage Subsystem DS4000, Logical Drive Finance, LUN 2,
Logical Drive WWN <600a0b80000f5d6c000000253eaeadf8>]
/dev/rdisk/c172t0d3 [Storage Subsystem DS4000, Logical Drive Purchasing, LUN 3,
Logical Drive WWN <600a0b80000f5d6c000000243eaeadeb>]
/dev/rdisk/c172t0d4 [Storage Subsystem DS4000, Logical Drive Development, LUN 4,
Logical Drive WWN <600a0b80000f56d00000001d3eaeacef>]
/dev/rdisk/c172t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,
Logical Drive WWN <600a0b80000f5d6c0000002200000000>]
```

注: **hot_add** および **SMdevices** コマンドを実行した後に論理ドライブおよび論理ドライブ・アクセスが表示されない場合は、**reboot** コマンドを使用して HP-UX ホストを再始動してください。

3. 上記の例に示されているように、**SMdevices** コマンドの出力を調べて、各論理ドライブの優先パスおよび代替パスを判別します。

各デバイスは 2 回リストされることに注意してください。最初の例は優先パス、2 番目の例は代替パスです。また、各デバイスはワールドワイド・ネーム (WWN) を持っていることに注意してください。各論理ドライブの WWN の一部は、ストレージ・サブシステム内の各コントローラーにごとに固有になっています。上記の例の論理ドライブ・アクセスの WWN は、**f56d0** と **f5d6c** の 5 桁のみが異なります。

上記の例のデバイスは、コントローラー **c166** および **c172** から表示されます。オペレーティング・システムで表示される特定の論理ドライブの優先パスを判別するには、以下の手順を実行します。

- a. 各論理ドライブ・アクセスの WWN を見つけます。この場合、論理ドライブ・アクセス 1 は **c166** に関連しており、WWN は **f56d0** です。

```
/dev/rdisk/c166t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,  
Logical Drive WWN <600a0b80000f56d00000001b00000000>]
```

論理ドライブ・アクセス 2 は **c172** に関連しており、WWN は **f5d6c** です。

```
/dev/rdisk/c172t3d7 [Storage Subsystem DS4000, Logical Drive Access, LUN 31,  
Logical Drive WWN <600a0b80000f5d6c0000002200000000>]
```

- b. 論理ドライブ WWN を論理ドライブ・アクセス WWN と突き合わせて、接続されているストレージ・デバイスの優先デバイス・パス名を識別します。この場合、**LUN 0** の WWN はコントローラー **c166** および **c172** に関連しています。したがって、**LUN 0** の優先パスは **/dev/rdisk/c166t0d0** です。これは、コントローラー **c166** です。

```
/dev/rdisk/c166t0d0 [Storage Subsystem DS4000, Logical Drive  
Accounting, LUN 0, Logical Drive g<600a0b80000f56d00000001e3eae2b>]
```

代替パスは **/dev/rdisk/c172t0d0** です。これは、コントローラー **c172** です。

```
/dev/rdisk/c172t0d0 [Storage Subsystem DS4000, Logical Drive  
Accounting, LUN 0, Logical Drive WWN <600a0b80000f5d6c0000001e3eae2b>]
```

- c. 将来の参照のためにレコードを保持するには、LUN 0 についてのこのパス情報を (表 31 のものと同様の) マトリックスに入力します。

表 31. 論理ドライブの優先パスおよび代替パスのサンプル・レコード

LUN	論理ドライブ名	優先パス	代替パス
0	Accounting (経理)	/dev/rdisk/c166t0d0	/dev/rdisk/c172t0d0
1	HR (人事)	/dev/rdisk/c172t0d1	/dev/rdisk/c166t0d1
2	Finance (財務)	dev/rdisk/c172t0d2	/dev/rdisk/c166t0d2
3	Purchasing (購買)	/dev/rdisk/c172t0d3	/dev/rdisk/c166t0d3
4	Development (開発)	/dev/rdisk/c166t0d4	/dev/rdisk/c172t0d4

- d. オペレーティング・システムで表示される各論理ドライブごとに、ステップ 3.a からステップ 3.c を繰り返します。

論理ドライブおよびアレイの作成

優先パスおよび代替パスを判別し、将来の参照のためにマトリックスに記録した後に、以下の手順を実行して、論理ドライブおよびアレイを作成します。

重要: DS3000、DS4000、または DS5000 ストレージ構成で HP System Administration Management (SAM) アプリケーションを使用しないでください。使用すると、予期しない結果が生じる場合があります。

注: この手順の個々のステップについては、157 ページの表 31 の LUN 0 を参照してください。

1. 物理論理ドライブを作成して、接続されているストレージ・デバイスの基本パスを定義します。基本パスは優先パスになります。シェル・プロンプトで次のコマンドを入力します。

```
#pvcreate /dev/rdisk/c166t0d0
```

システムは、新規物理論理ドライブの作成を確認します。

2. アレイを作成します。

注: アレイの作成方法の詳細については、HP-UX 資料または man ページを参照してください。

- a. 次のコマンドを入力して、アレイのディレクトリを作成します。このディレクトリは、/dev ディレクトリに存在する必要があります。

```
#cd /dev  
#mkdir /vg1
```

- b. 次のコマンドを入力して、/dev ディレクトリに、アレイのグループ特殊ファイルを作成します。

```
#mknod /dev/vg1/group c 64 0x010000
```

- c. 次のコマンドを入力して、アレイを作成し、接続されているストレージ・デバイスの物理論理ドライブ名 (1 次リンク) を定義します。

```
#vgcreate /dev/vg1/ /dev/dsk/c166t0d0
```

- d. 次のコマンドを入力して、接続されているストレージ・デバイスの 2 次パス名 (代替パス) を定義します。

```
#vgextend vg1 /dev/dsk/c172t0d0
```

注: **vgextend** コマンドを使用して、追加のストレージ・デバイスを既存のアレイに追加することもできます。次の例に示されているように、まず基本パスを追加し、その後に代替パスを追加します。

- 1) LUN1 の基本パスを追加します。

```
#vgextend vg1 /dev/dsk/c172t0d1
```

- 2) LUN1 の 2 次パスを追加します。

```
#vgextend vg1 /dev/dsk/c166t0d1
```

3. 論理ドライブを作成します。詳細については、HP-UX 資料を参照してください。
4. 論理ドライブのファイル・システムを作成します。
5. 追加のアレイを作成するには、ステップ 1 からステップ 4 を繰り返します。詳細については、HP-UX 資料を参照してください。
6. 次のコマンドを入力して、各デバイスの 1 次 (優先) パスおよび 2 次 (代替) パスを検証します。

```
#vgdisplay -v vgname
```

ここで、*vgname* はアレイ・グループ名です。

HP-UX 固有のマルチパス

マルチパスは HP-UX 11i v3 固有のものです。このマルチパスは、大容量ストレージ・サブシステム内で作成され、特殊な構成を持たないアプリケーションに使用することができます。

HP-UX 11iv3 固有のマルチパスについて詳しくは、<http://docs.hp.com/en/oshpux11iv3.html> にある資料を参照してください。

Solaris フェイルオーバー・ドライバー

フェイルオーバー・ドライバーは、入出力パスをモニターします。ファイバー・チャネル・パスのいずれか 1 つでコンポーネントの障害が発生すると、フェイルオーバー・ドライバーがすべての入出力を別のパスに転送します。

Solaris ホスト・システムは、以下のフェイルオーバー・ドライバーのいずれかを必要とします。

- Solaris Multiplexed I/O (MPxIO)
- RDAC
- Dynamic Multipathing (DMP) を備えた Veritas VolumeManager

注:

1. RDAC は、Solaris 10 ではサポートされません。Solaris MPxIO または Veritas DMP フェイルオーバー・ドライバーを使用する必要があります。
2. Solaris 10 では、MPxIO 機能が組み込まれています。Solaris の以前のバージョンで MPxIO を使用したい場合は、SUN StorEdge SAN Foundation Suite をインストールする必要があります。
3. Asymmetric Logical Unit Access (ALUA) をサポートするには、Solaris 11 以降が必要です。

このセクションには、以下の手順が記載されています。

- 『MPxIO ドライバーのインストール』
- 165 ページの『Solaris への RDAC フェイルオーバー・ドライバーのインストールおよび構成ファイルの変更』
- 168 ページの『Veritas DMP ドライバーのインストールの計画と準備』

MPxIO ドライバーのインストール

Multiplexed I/O (MPxIO) は、Sun Solaris マルチパス・ドライバー・アーキテクチャーです。このフェイルオーバー・ドライバーにより、ストレージ・サブシステムの単一インスタンスから、複数のホスト・コントローラー・インターフェースを通じて、ストレージ・サブシステムにアクセスできるようになります。

MPxIO は、コントローラーの障害が原因でストレージ・サブシステムが停止しないよう保護するのに役立ちます。1 つのコントローラーに障害が起こると、MPxIO は自動的に代替コントローラーに切り替えます。

MPxIO は Solaris 10 オペレーティング・システムに完全に統合されています。Solaris 8 および 9 オペレーティング・システムの場合、MPxIO は Sun StorEdge SAN Foundation Suite の一部として使用可能ですが、別々にインストールする必要があります。

Sun StorEdge SAN Foundation Suite のサポートされる最新バージョン、最新の Solaris カーネル・パッチ、および MPxIO の使用に関する最新の更新情報については、ストレージ・マネージャーの Solaris の README ファイルを参照してください。Web で README ファイルを検索する手順については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

このセクションでは、以下のトピックについて説明します。

- 160 ページの『MPxIO のデバイス名の変更に関する考慮事項』
- 160 ページの『MPxIO ドライバーの最新バージョンの獲得』
- 160 ページの『MPxIO フェイルオーバー・ドライバーの使用可能化』
- 165 ページの『MPxIO マルチパス・ドライバーの使用不可化』

注: 詳しくは、Sun Web サイト (<http://docs.sun.com>) にある「*Sun StorEdge SAN Foundation Software Installation Guide*」、「*Sun StorEdge SAN Foundation Software Configuration Guide*」、および「*Sun Solaris Fibre Channel and Storage Multipathing Administration Guide*」を参照してください。

MPxIO のデバイス名の変更に関する考慮事項:

MPxIO が使用可能な場合、`/dev` および `/devices` ツリーで、デバイスにはその元の名前とは異なる名前が付けられます。下記の例を参照してください。

MPxIO が使用不可の場合のデバイス名:

```
/dev/dsk/clt1d0s0
```

MPxIO が使用可能な場合のデバイス名:

```
/dev/rdsd/c0t600A0B800011121800006B31452CC6A0d0s2
```

MPxIO 構成が使用可能または使用不可になる場合は必ず、デバイスに直接関与するアプリケーションを、新規名を使用するように構成する必要があります。

さらに、`/etc/vfstab` ファイルおよびダンプ構成にも、デバイス名への参照が含まれます。 **stmsboot** コマンドを使用して MPxIO を使用可能または使用不可にすると、次のセクションで説明するように、`/etc/vfstab` およびダンプ構成は新規デバイス名によって自動的に更新されます。

MPxIO ドライバーの最新バージョンの獲得: MPxIO の獲得方式は、お客様が Solaris のどのバージョンをインストールしているかによって異なります。

Solaris 10

MPxIO は、Solaris 10 オペレーティング・システムに統合されているため、別々にインストールする必要はありません。Solaris 10 パッチを使用して、Solaris 10 の MPxIO を更新します。パッチは、Sun Technical Support Web サイト (<http://sunsolve.sun.com>) で入手できます。

注: 正規のカーネル・ジャンボ・パッチをインストールする必要があります。その理由は、ドライバー・スタックを構成する各種のパッチ間に依存関係があるからです。

Solaris 8 および 9

MPxIO は Solaris 8 および 9 には組み込まれていないので、必要な SAN suite (Sun StorEdge SAN Foundation Suite) を、Sun Technical Support Web サイト (<http://sunsolve.sun.com>) からダウンロードする必要があります。この Web ページで、「**SAN 4.4 release Software/Firmware Upgrades**」 & 「**Documentation**」をクリックします。

注: 提供されている **install_it.ksh** スクリプトを使用して、ソフトウェアをインストールします。

MPxIO フェイルオーバー・ドライバーの使用可能化: このセクションでは、**stmsboot** コマンドを使用して MPxIO を使用可能にする方法を説明します。MPxIO を使用可能化することに加えて、このコマンドは、次のリブート時に `/etc/vfstab` ファイルおよびダンプ構成ファイル内のデバイス名を更新します。

注: Solaris 10 では、**stmsboot** コマンドを使用して、すべてのデバイス上の MPxIO を使用可能または使用不可にします。

開始する前に:

1. Solaris オペレーティング・システム、および最新のパッチをインストールします。
2. ホストの定義時に、Solaris ホスト・タイプが選択されていることを確認します。

Solaris 8 および 9 上の MPxIO の使用可能化

1. **Sun StorEdge install_it** スクリプトを使用して、Sun StorEdge SAN Foundation Suite の最新バージョンおよび必要なパッチをインストールします。詳細については、「*Sun StorEdge SAN Foundation Suite x.xx Installation Guide*」を参照してください (ここで、x.xx は StorEdge ソフトウェアのバージョンです)。
2. `/kernel/drv/scsi_vhci.conf` 構成ファイルを編集して、このファイルに VID/PID が指定されていないことを確認します。また、以下のエントリーがこのファイルにあることを確認します。

```
mpxio-disable="no";  
load-balance="none";  
auto-failback="enable";
```

注: 論理ドライブ (LUN) が複数の Sun サーバーで共有されるクラスター環境では、auto-failback パラメーターを `disable` に設定して、次のような現象が発生しないようにする必要がある場合があります。この現象は、サーバーの 1 つから共有 LUN の 1 つへのパスに障害がある場合に発生することがあります。

クラスター・サーバー構成内のホストがストレージ・サブシステム・コントローラーへの物理パスを失うと、クラスター・グループにマップされる LUN は、障害を起こしたパスが復元するまでクラスター・ノード間で周期的にフェイルオーバーとフェイルバックを繰り返すことがあります。この動作は、マルチパス・ドライバの論理ドライブ自動フェイルバック機能によるものです。ストレージ・サブシステム・コントローラーへのパスに障害のあるクラスター・ノードは、クラスター・グループにマップされたすべての LUN に対して、アクセス可能なコントローラーへのフェイルオーバー・コマンドを出します。プログラムに組み込まれた一定時間間隔の後、パスに障害がなかったノードは、両方のコントローラーの LUN にアクセスできるので LUN に対してフェイルバック・コマンドを出します。パスに障害のあるクラスター・ノードは、特定の LUN にアクセスすることができません。このクラスター・ノードは次に、すべての LUN に対してフェイルオーバー・コマンドを出し、LUN のフェイルオーバー/フェイルバック・サイクルを繰り返します。

サポートされるクラスター・サービスについては、System Storage Interoperation Center (www.ibm.com/systems/support/storage/config/ssic) を参照してください。

3. 前のステップで `/kernel/drv/scsi_vhci.conf` ファイルに何らかの変更を加えた場合は、そのファイルを保存し、次のコマンドを使用してサーバーを再始動します。

```
# shutdown -g0 -y -i6
```

4. 必要なら、ファイバー・チャネル HBA ファームウェアを更新します。
5. ストレージ・サブシステム論理ドライブを作成し、それらを Sun サーバー内のファイバー・チャネル HBA ポートにマップします。

Solaris 10 上の MPxIO の使用可能化

`stmsboot -e [enable] -d [disable] and -u [update]` についての以下の考慮事項に留意してください。

- **stmsboot** コマンドを実行する場合、デフォルトの `Reboot the system now` を受け入れます。
- **stmsboot** コマンドは、元の `/kernel/drv/fp.conf` および `/etc/vfstab` ファイルのコピーを変更前に保存するので、予期しない問題が生じたときに、保存されたファイルを使用してリカバリーすることができます。
- **eeprom** ブート・デバイスが現行ブート・デバイスからブートするように設定されていることを確認してください。

すべてのファイバー・チャネル・デバイスで MPxIO を使用可能にするには、以下の手順を実行します。

1. **stmsboot -e** コマンドを実行し、デフォルトの [y] を選択してサーバーを再始動します。

```
# stmsboot -e
```

```
WARNING: This operation will require a reboot.
Do you want to continue ? [y/n] (default: y) y
The changes will come into effect after rebooting the system.
Reboot the system now ? [y/n] (default: y) y
```

注: リブート中に、/etc/vfstab およびダンプ構成はデバイス名の変更を反映するように更新されます。

2. リブート後、160 ページの『MPxIO のデバイス名の変更に関する考慮事項』で説明したとおり、新規デバイス名を使用するようにアプリケーションを構成します。
3. 必要であれば、/kernel/drv/fp.conf 構成ファイルを編集して、次のパラメーターが以下に示すように設定されていることを確認します。

```
mpxio-disable="no";
```

/kernel/drv/scsi_vhci.conf 構成ファイルを編集して、次のパラメーターが以下に示すように設定されていることを確認します。

```
load-balance="none";
auto-failback="enable";
```

4. 前のステップで構成ファイルに何らかの変更を加えた場合は、そのファイルを保存し、次のコマンドを使用してサーバーを再始動します。

```
# shutdown -g0 -y -i6
```

5. 必要なら、ファイバー・チャネル HBA ファームウェアを更新します。
6. ストレージ・サブシステム論理ドライブを作成し、それらを Sun サーバー内のファイバー・チャネル HBA ポートにマップします。

マップされた LUN のためのデバイスの検査とフェイルオーバー/フェイルバック・パスの構成

マップされた LUN のためにデバイスを検査し、フェイルオーバー・パスを構成するには、以下の手順を完了します。

1. **cfgadm -al** コマンドを使用して、デバイスを検証します。**cfgadm -al** コマンドを実行して、ホスト・ポートおよびそれに接続されたデバイスに関する情報を表示します。

```
# cfgadm -al
```

Ap_Id	Type	Receptacle	Occupant	Condition
PCI0	vgs8514/hp	connected	configured	ok
PCI1	unknown	empty	unconfigured	unknown
PCI2	unknown	empty	unconfigured	unknown
PCI3	mult/hp	connected	configured	ok
PCI4	unknown	empty	unconfigured	unknown
PCI5	unknown	empty	unconfigured	unknown
PCI6	unknown	empty	unconfigured	unknown
PCI7	mult/hp	connected	configured	ok
PCI8	mult/hp	connected	configured	ok
c0	scsi-bus	connected	configured	unknown
c0::dsk/c0t6d0	CD-ROM	connected	configured	unknown
c1	fc-private	connected	configured	unknown
c1::500000e0106fca91	disk	connected	configured	unknown
c1::500000e0106fcde1	disk	connected	configured	unknown
c1::500000e0106fcf31	disk	connected	configured	unknown
c1::500000e0106fd061	disk	connected	configured	unknown
c1::500000e0106fd7b1	disk	connected	configured	unknown
c1::500000e0106fdaa1	disk	connected	configured	unknown
c1::50800200001d9841	ESI	connected	configured	unknown
c2	fc-fabric	connected	configured	unknown

c2::201400a0b811804a	disk	connected	configured	unusable
c2::201400a0b8118098	disk	connected	configured	unusable
c2::201700a0b8111580	disk	connected	configured	unusable
c3	fc-fabric	connected	configured	unknown
c3::201500a0b8118098	disk	connected	configured	unusable
c3::201600a0b8111580	disk	connected	configured	unusable
c3::202500a0b811804a	disk	connected	configured	unusable
c4	fc-fabric	connected	configured	unknown
c4::200400a0b80f1285	disk	connected	configured	unknown
c4::200400a0b8127a26	disk	connected	configured	unusable
c5	fc-fabric	connected	configured	unknown
c5::200400a0b82643f5	disk	connected	unconfigured	unknown
c5::200500a0b80f1285	disk	connected	configured	unknown
c5::200500a0b8127a26	disk	connected	configured	unusable
c5::200c00a0b812dc5a	disk	connected	configured	unknown
usb0/1	usb-kbd	connected	configured	ok
usb0/2	usb-mouse	connected	configured	ok
usb0/3	unknown	empty	unconfigured	ok
usb0/4	unknown	empty	unconfigured	ok
#				

2. サーバー上の接続点に関する情報を表示することもできます。次の例で、c0 はファブリック接続ホスト・ポートを表し、c1 はプライベートの、ループ接続ホスト・ポートを表します。ファブリック接続ホスト・ポート上のデバイス構成を管理するには、**cfgadm** コマンドを使用します。デフォルトで、プライベートの、ループ接続ホスト・ポート上のデバイス構成は Solaris ホストによって管理されます。

注: **cfgadm -l** コマンドは、ファイバー・チャネル・ホスト・ポートに関する情報を表示します。また、**cfgadm -al** コマンドを使用すると、ファイバー・チャネル・デバイスに関する情報が表示されます。c0 に関連付けられた Ap_Id フィールド内のポートのワールドワイド・ネーム (WWN) を含む行は、ファブリック・デバイスを表します。**cfgadm configure** および **cfgadm unconfigure** コマンドを使用して、これらのデバイスを管理し、Solaris ホストでできるようにしてください。

```
# cfgadm -l
Ap_Id      Type      Receptacle  Occupant    Condition
c0         fc-fabric connected   unconfigured unknown
c1         fc-private connected   configured  unknown
```

3. 次のコマンドを使用して、デバイスを構成します。

```
cfgadm -c configure Ap-Id
```

Ap_ID パラメーターは、構成されたファイバー・チャネル・デバイスの接続点 ID を指定します。この ID はコントローラー番号とデバイスの WWN でも構いません (例えば、c3::50020f230000591d)。

ステップ 1 の出力例を参照してください。また、接続点の説明は、*cfgadm man* ページを参照してください。

注: fc-private タイプの Ap_Id を構成解除することはできません。fc-fabric タイプのみが構成および構成解除可能です。

4. **luxadm probe** コマンドを使用して、マップされた LUN をすべてリストします。

```
# luxadm probe
luxadm probe
No Network Array enclosures found in /dev/es

Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006ADE452CBC62d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006ADF452CBC6Ed0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE0452CBC7Ad0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE1452CBC88d0s2
```

```

Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE2452CBC94d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE3452CBCA0d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE4452CBCACd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE5452CBCB8d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE6452CBCB4d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE7452CBCD2d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE8452CBCDEd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AE9452CBCAd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AEA452CBCF8d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AEB452CBD04d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AEC452CBD10d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006AED452CBD1Ed0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006B2A452CC65Cd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006B2B452CC666d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006B2C452CC670d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006B2D452CC67Ad0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c0t600A0B800011121800006B32452CC6ACd0s2
Node WWN:200400a0b8111218 Device Type:Disk device
Logical Path:/dev/rdisk/c8t201400A0B8111218d7s2

```

5. **luxadm display** 論理パス コマンドを使用して、マップされた各 LUN に関する詳細 (各 LUN へのパス数を含む) をリストします。次の例は、前の例の論理パスを使用しています。

```

# luxadm display /dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
DEVICE PROPERTIES for disk: /dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
Vendor: IBM
Product ID: 1742-900
Revision: 0914
Serial Num: 1T51207691
Uninitialized capacity: 1024.000 MBytes
Write Cache: Enabled
Read Cache: Enabled
Minimum prefetch: 0x0
Maximum prefetch: 0x0
Device Type: Disk device
Path(s):

/dev/rdisk/c0t600A0B800011121800006B31452CC6A0d0s2
/devices/scsi_vhci/ssd@g600a0b800011121800006b31452cc6a0:c,raw
Controller /devices/pci@7c0/pci@0/pci@8/SUNW,qlc@0,1/fp@0,0
Device Address 201400a0b8111218,1e
Host controller port WWN 210100e08ba0fca0
Class secondary
State STANDBY
Controller /devices/pci@7c0/pci@0/pci@8/SUNW,qlc@0,1/fp@0,0
Device Address 201500a0b8111218,1e
Host controller port WWN 210100e08ba0fca0
Class primary
State ONLINE

```



```

Controller          /devices/pci@7c0/pci@0/pci@8/SUNW,q1c@0/fp@0,0
Device Address       201400a0b8111218,1e
Host controller port WWN 210000e08b80fca0
Class                secondary
State                STANDBY
Controller          /devices/pci@7c0/pci@0/pci@8/SUNW,q1c@0/fp@0,0
Device Address       201500a0b8111218,1e
Host controller port WWN 210000e08b80fca0
Class                primary
State                ONLINE
#

```

フェイルオーバー/フェイルバック・パスの構成解除

フェイルオーバー/フェイルバック・パスを構成解除するには、以下の手順を完了します。

1. ファブリック・デバイスを構成解除する前に、このデバイスへのすべてのアクティビティを停止し、ファブリック・デバイス上のファイル・システムをすべてアンマウントします (アンマウントの手順については、Solaris 管理資料を参照してください)。
2. **cfgadm -al** コマンドを実行して、ホスト・ポートおよびそれに接続されたデバイスに関する情報を表示します。
3. 次のコマンドを実行して、LUN を構成解除します。

```
cfgadm -c unconfigure Ap-Id
```

ここで、Ap-Id は構成解除する LUN です。

4. **cfgadm -al** コマンドを再度実行して、LUN が現在構成解除されているか検証します。
5. 必要に応じて、**newfs** コマンドを使用してファイル構造を定義します。 /etc/vfstab ファイルにエントリーを追加します。
6. 次のコマンドを入力して、サーバーを再始動します。

```
shutdown -g0 -y -i6
```

MPxIO マルチパス・ドライバーの使用不可化: MPxIO マルチパス・ドライバーを使用不可にするには、ご使用の Solaris のバージョンに該当する処置を実行します。

- Solaris 10 の場合は、**cfgadm -c unconfigure AP-id Ap-id** コマンドを使用してすべてのデバイスを構成解除します。次に、**stmsboot -d** コマンドを実行して、デフォルトの Reboot the system now を受け入れます。
- Solaris 8 および 9 の場合は、**cfgadm -c unconfigure AP-id Ap-id** コマンドを使用してすべてのデバイスを構成解除し、/kernel/drv/scsi_vhci.conf 構成ファイルを編集して **mpxio-disable** パラメーターの値を **yes** に設定します。サーバーを再始動します。

パッチの復帰方法または StorEdge ソフトウェアの使用方法については、<http://docs.sun.com> にある「*Sun StorEdge SAN Foundation Installation Software Guide*」を参照してください。

Solaris への RDAC フェイルオーバー・ドライバーのインストールおよび構成ファイルの変更

このセクションでは、RDAC を Solaris ホストにインストールする方法について説明します。

開始する前に:

1. RDAC は Solaris 8 および 9 でのみサポートされます。

2. RDAC と MPxIO の両方を実行することはできないので、必ず MPxIO を使用不可にしてください。構成ファイル (/kernel/drv/scsi_vhci.conf、/kernel/drv/fp.conf、または両方) を調べて、mpxio-disable パラメーターの値が Yes に設定されていることを確認します。
3. RDAC をインストールする前に、HBA ドライバー・パッケージをインストールする必要があります。SAN 接続の構成を使用する場合は、RDAC をインストールする前に、HBA の構成ファイルを変更することも必要です。この順序で手順を実行しないと、問題が発生する可能性があります。
4. RDAC のインストール後に HBA 構成ファイルのフェイルオーバー設定値を変更する場合は、ホストから RDAC を除去する必要があります。

重要: 一部の構成では、RDAC が正常に機能するためにパッチが必要です。RDAC のインストールを始める前に、Solaris 用のストレージ・マネージャー README ファイルで、ご使用の特定の構成でパッチが必要であるかどうかを確認してください。README ファイルでは、最新の RDAC バージョンおよびその他の重要な情報を見つけることもできます。README ファイルを Web で検索する方法について詳しくは、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

RDAC フェイルオーバー・ドライバーのインストール

RDAC フェイルオーバー・ドライバーをインストールするには、以下の手順を実行します。

1. Solaris インストール DVD を DVD ドライブに挿入します。

注: この手順では、インストール DVD は /cdrom/SM91 にマウントされています。ユーザーのインストールで必要であれば、これらのコマンドを変更してください。ディスクがマウントされた方法に応じて、「cdrom」または「dvdrom」になります。

2. 次のコマンドを入力して、RDAC パッケージのインストールを開始します。

```
# pkgadd -d path/filename.pkg
```

ここで、*path/filename* は、インストールしたいパッケージのディレクトリー・パスと名前です。

インストール・プロセスが開始されます。

以下の例のように、指定されたディレクトリーにインストールできるパッケージに関する情報が、コマンド行に表示されます。

The following packages are available:

```
1 RDAC                               Redundant Disk Array Controller
                                   (sparc) version number
```

```
Select package(s) you wish to process (or 'all' to process all
packages). (default:all) [?,??.q]:
```

3. インストールするパッケージの値を入力し、Enter キーを押します。インストール・プロセスが開始されます。
4. ソフトウェアが、パッケージの競合を自動的に検査します。競合が検出されると、いくつかのファイルが既にインストールされていて、別のパッケージによって使用中であることを示すメッセージが表示されます。次のプロンプトが表示されます。

```
Do you want to install these conflicting files [y, n, ?]
```

y を入力して、Enter キーを押します。次のプロンプトが表示されます。

This package contains scripts which will be executed with super-user permission during the process of installing this package.

Do you want to continue with the installation of <RDAC>

[y, n, ?]

5. `y` を入力して、Enter キーを押します。インストール・プロセスが続行されます。RDAC パッケージが正常にインストールされると、次のメッセージが表示されます。

Installation of <RDAC> was successful.

6. JNI アダプター・カードの構成ファイルの変数が、正しい値に設定されていることを確認します。
7. 次のコマンドを入力して、Solaris ホストを再始動します。

```
# shutdown -g0 -y -i6
```

構成ファイルの変更

重要: `jnic146x.conf` 構成ファイルの永続バインディングに変更を加える場合には、RDAC を除去する必要があります。RDAC を除去した後、`jnic146x.conf` ファイルの永続バインディングを変更し、RDAC を再インストールすることができます。

以下の手順を完了して、`sd.conf` または `jnic146x.conf` ファイルを変更します。

1. 次のコマンドを入力して、RDAC を除去します。

```
# pkgrm RDAC_driver_pkg_name
```

ここで、`RDAC_driver_pkg_name` は、除去したい RDAC ドライバー・パッケージの名前です。

2. 次のコマンドを入力して、RDAC ドライブ・パッケージが除去されたことを検証します。

```
# pkginfo RDAC_driver_pkg_name
```

ここで、`RDAC_driver_pkg_name` は、除去した RDAC ドライバー・パッケージの名前です。

3. 次のコマンドを入力して、Solaris ホストを再始動します。

```
# shutdown -g0 -y -i6
```

4. 次のコマンドを入力して、`sd.conf` ファイルの永続バインディングを変更するか、`sd.conf` ファイルを編集します。

```
# vi /kernel/drv/jnic146x.conf or sd.conf
```

5. 変更が終了したら、次のコマンドを入力して変更を保存します。

```
# :wq
```

6. 次のコマンドを入力して、RDAC ドライバー・パッケージをインストールします。

```
# pkgadd -d RDAC_driver_pkg_name
```

ここで、`RDAC_driver_pkg_name` は、インストールしたい RDAC ドライバー・パッケージの名前です。

7. 次のコマンドを入力して、パッケージのインストールを検証します。

```
# pkginfo RDAC_driver_pkg_name
```

ここで、`RDAC_driver_pkg_name` は、インストールした RDAC ドライバー・パッケージの名前です。

8. 次のコマンドを入力して、Solaris ホストを再始動します。

```
# shutdown -g0 -y -i6
```

注: jnic146x.conf ドライバーはブート・プロセスでのみ読み取られるので、jnic146x.conf ファイルを変更した後、ホストを再始動する必要があります。ホストを再始動しないと、一部のデバイスがアクセス不能になる可能性があります。

Veritas DMP ドライバーのインストールの計画と準備

このセクションでは、Veritas Dynamic Multipathing (DMP) ドライバーのインストールを計画および準備する方法について説明します。Veritas DMP ドライバーは、Solaris ホスト用のフェイルオーバー・ドライバです。DMP フェイルオーバー・ドライバは、Symantec 製の Storage Foundation 製品のコンポーネントである Veritas Volume Manager の機能です。RDAC では 32 の LUN のみを持つことができますが、DMP を使用すると、256 までの LUN を持つことができます。

重要: 本書では、Veritas 製品のインストール方法については説明しません。詳細については、<http://www.symantec.com/business/support/> にある Symantec 資料を参照してください。

システム要件

ご使用のサーバーが Veritas DMP をインストールするための以下の要件を満たしていることを確認してください。

- Solaris オペレーティング・システム
- Veritas Volume Manager 4.0、4.1、5.0、または 5.1
- Array Support Library (ASL)。Solaris が DS3000、DS4000、または DS5000 マシン・タイプを認識できるようにします。

注: Storage Foundation のバージョンによって、ASL は Symantec から入手可能な別個のファイルであるか、Volume Manager に組み込まれている場合があります。

Veritas DMP のインストールの概説

ご使用のサーバーが Veritas DMP をインストールするための以下の前提条件を満たしていることを確認してください。

- HBA が Solaris ホストにインストール済みである。
- HBA 構成ファイルのパラメーター設定値 (例えば、qla2300.conf) が変更済みである。
- SAN 環境で、バインディングが構成済みである。
- Solaris 区画でゾーンが作成済みであり、使用可能になっている。
- ストレージが Solaris 区画にマップされている。

Veritas DMP インストールを完了するには、以下の順序で手順を実行します。

1. 『Veritas DMP インストールの準備』
2. 170 ページの『ASL パッケージのインストール』

Veritas DMP インストールの準備

Veritas DMP をインストールするためにホストを準備するには、以下の手順を実行します。

1. DMP をインストールしたい Solaris ホストを選択します。
2. 以下の手順を実行して、/kernel/drv/sd.conf ファイルでターゲットと LUN を手動で定義します。

注: デフォルトでは、/kernel/drv/sd.conf ファイルは、ターゲット 0、1、2、および 3 を定義します。また、LUN0 は、ターゲット 0、1、2、および 3 に対して定義されます。各ターゲットは、スト

レージ・サブシステムに対するコントローラーを表し、各 LUN は、論理ドライブを表します。追加のターゲットまたは LUN の定義を、既存の DMP 構成の `/kernel/drv/sd.conf` ファイルに追加する場合は、必ず Solaris ホストをリブートしてください。

- a. 次のコマンドを入力して、vi エディターで `/kernel/drv/sd.conf` ファイルを開きます。

```
# vi /kernel/drv/sd.conf
```

ファイルは、次の例と同様になります。

```
#
# Copyright (c) 1992, Sun Microsystems, Inc.
#
# ident "@(#)sd.conf 1.9 98/01/11 SMI"

name="sd" class="scsi" class_prop="atapi"
target=0 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=1 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=2 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=3 lun=0;
```

- b. vi エディターを使用して、ターゲットおよび LUN の定義を追加します。次の例では、Solaris ホストが、ストレージ・サブシステム区画にマップされた 3 つの LUN を備えた 1 つのストレージ・サブシステムに接続されていることを想定しています。さらに、アクセス LUN を区画にマップする必要があります。

```
#
# Copyright (c) 1992, Sun Microsystems, Inc.
#
# ident "@(#)sd.conf 1.9 98/01/11 SMI"

name="sd" class="scsi" class_prop="atapi"
target=0 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=1 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=2 lun=0;

name="sd" class="scsi" class_prop="atapi"
target=3 lun=0;

name="sd" class="scsi" target=0 lun=1;
name="sd" class="scsi" target=0 lun=2;
name="sd" class="scsi" target=0 lun=3;
name="sd" class="scsi" target=0 lun=31;
name="sd" class="scsi" target=1 lun=1;
name="sd" class="scsi" target=1 lun=2;
name="sd" class="scsi" target=1 lun=3;
name="sd" class="scsi" target=1 lun=31;
```

- c. 次のコマンドを入力して、`/kernel/drv/sd.conf` ファイルの新規エントリーを保存します。

```
# :wq
```

3. 次のコマンドを入力して、RDAC がホストにインストールされていないことを検証します。

```
# pkginfo -l RDAC
```

4. RDAC がインストールされている場合は、次のコマンドを入力して削除します。

```
# pkgrm RDAC
```


5. ホスト区画が作成済みであることを検証します。

重要: ホスト・タイプを **DMP** として **Solaris** に設定します。設定しないと、32 の LUN の RDAC 制限を超えた場合にマップできなくなり、その他の予期しない結果が発生します。

6. すべてのパスが最適になっていて、SMclient からの優先パスの状態にあることを確認します。
7. DMP を備えた Veritas Volume Manager を含めて、Veritas Storage Foundation Solaris をインストールします。

重要: Veritas Volume Manager および DMP を伴う Veritas Storage Foundation Solaris のインストールをする前に、必要なライセンス・キーがあることを確実にしてください。本書では、Veritas 製品のインストール方法については説明しません。詳細については、<http://www.symantec.com/business/support/> にある Symantec 資料を参照してください。

8. 次のコマンドを入力して、Solaris ホストを再始動します。

```
# shutdown -g0 -y -i6
```

ASL パッケージのインストール

必要に応じて、以下の手順を実行して ASL パッケージをインストールします。

注: VxVM 4.x バージョンの ASL パッケージは、SMibmasl と呼ばれます (詳細は、<http://seer.entsupport.symantec.com/docs/284913.htm> を参照してください)。VxVM バージョン 5.0 以降の場合、複数の ASL が組み込まれているので、インストールする必要はありません。VxVM バージョン 5.0 以降では、ASL パッケージは「VRTSLSIas1」と呼ばれます (<http://seer.entsupport.symantec.com/docs/340469.htm> を参照)。以下の例では、VxVM 4.x をインストールすることを前提としています。

1. 次のコマンドを入力して、**SMibmasl** パッケージをインストールします。

注: デフォルト (all) を選択するか、オプション 1 を選択することができます。

```
# pkgadd -d SMibmasl_pkg
```

2. 次のコマンドを入力して、Solaris ホストを再始動します。

```
# shutdown -g0 -y -i6
```

以下のタスクの完了方法については、Symantec Veritas 資料を参照してください。

- Veritas Volume Manager の開始
- ディスク・グループのセットアップ
- ボリュームの作成
- ファイル・システムの作成
- ファイル・システムのマウント

デバイスの識別

マルチパス・ドライバをインストールした後で、またはマルチパス・ドライバが既にインストールされていることを確認した後で、SMdevices ユーティリティを使用して、オペレーティング・システムのデバイスに関連付けられたストレージ・サブシステムの論理ドライブを識別します。

SMdevices ユーティリティの使用

SMutil ソフトウェアに含まれる SMdevices という名前のユーティリティを使用すると、特定のオペレーティング・システム装置名に関連付けられているストレージ・サブシステム論理ドライブを表示できます。このユーティリティは、ディスク・アドミニストレーターを使用してドライブ名または区画を作成するときに便利です。

Windows オペレーティング・システムでの SMdevices の使用

ストレージ・サブシステム上に論理ドライブを作成した後、ストレージ・サブシステムに接続されたホストで、SMdevices を Windows で使用するための以下の手順を実行します。

1. DOS またはコマンド・プロンプトで、ディレクトリー <installation_directory>%Util に変更する。

installation_directory は、SMutil がインストールされているディレクトリーです。

デフォルトのディレクトリーは c:\Program Files\IBM_DS4000\Util です。

2. SMdevices と入力して、Enter キーを押す。

UNIX タイプ・オペレーティング・システムでの SMdevices の使用

SMdevices を使用して、LUN ごとにホストで割り当てられたデバイス名を、対応するストレージ・サブシステム・デバイスにマップし直すことができます。SMdevices の出力では、SMclient に示されるように、以下のストレージ・サブシステム情報を表示できます。

注: リスト内の例は、SMdevices の出力例を参照しています。

- ホストが割り当てた名前 (/dev/sdh)
- DS3000/DS4000/DS5000 ストレージ・サブシステム名 (DS4500_Storage_Server-A)
- 論理ドライブ名 (Raid-5-0A)
- LUN ID (LUN 4)
- 優先コントローラー所有者、およびそのコントローラーが論理ドライブを制御しているかどうか

以下の例では、DS4500_Storage_Server-A ストレージ・サブシステムに対する SMdevices の出力例が示されています。

```
# SMdevices
IBM FAStT Storage Manager Devices, Version 09.12.A5.00
Built Fri Jan 14 16:42:15 CST 2005
(C) Copyright International Business Machines Corporation,
2004 Licensed Material - Program Property of IBM. All rights reserved.

/dev/sdh (/dev/sg10) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-5-0A, LUN 4, Logical Drive ID
<600a0b80000f0fc30000004412e2dbf>, Preferred Path (Controller-A): In Use]
/dev/sdd (/dev/sg6) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-5-1A, LUN 0, Logical Drive ID
<600a0b80000f13ec00000016412e2e86>, Preferred Path (Controller-B): In Use]
/dev/sde (/dev/sg7) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-0-0A, LUN 1, Logical Drive ID
<600a0b80000f0fc30000003c412e2d59>, Preferred Path (Controller-A): In Use]
/dev/sdf (/dev/sg8) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-1-0A, LUN 2, Logical Drive ID
<600a0b80000f0fc30000003e412e2d79>, Preferred Path (Controller-A): In Use]
/dev/sdg (/dev/sg9) [Storage Subsystem DS4500_Storage_Server-A,
Logical Drive Raid-3-0A, LUN 3, Logical Drive ID
<600a0b80000f13ec00000012412e2e4c>, Preferred Path (Controller-A): In Use]
```

AIX ホストにおけるデバイスの識別

このセクションの情報では、AIX でのデバイス・ディスカバリーについて説明します。AIX のディスク・アレイ・エラーに関するトラブルシューティング情報については、263 ページの『第 7 章 Troubleshooting (トラブルシューティング)』の 289 ページの『AIX でのディスク・アレイのエラーの解決』を参照してください。

AIX ホストにおけるデバイスについて

マルチパス・ドライバーは、ストレージ・サブシステム構成を表す以下のデバイスを作成します。

dar ディスク・アレイ・ルーター (dar) デバイスは、すべての LUN (hdisk) への現行パスおよび据え置きパスを含む、アレイ全体を表します。

dac ディスク・アレイ・コントローラー (dac) デバイスは、ストレージ・サブシステム内のコントローラーを表します。ストレージ・サブシステム内には、2 つの dac が存在します。MPIO では、dac デバイスが表示されるのは UTM デバイスが割り当てられている場合のみです。

hdisk 各 hdisk デバイスは、アレイ上の個々の LUN を表します。

utm ユニバーサル・トランスポート・メカニズム (utm) デバイスは、SMagent とストレージ・サブシステム間の通信チャネルとして、インバンド管理構成でのみ使用されます。

注: インバンド管理構成が存在するかどうかに関係なく、utm デバイスはコマンド出力にリストされる場合があります。例えば、**lsattr** コマンドを dac 上で実行したときに utm がリストされる場合があります。

デバイスの初期ディスカバリーの実行

デバイスの初期ディスカバリーを実行するには、以下の手順を実行してください。

1. ストレージ・サブシステムがセットアップされていること、LUN がホストに割り当てられていること、およびマルチパス・ドライバーがインストールされていることを確認してください。
2. 次のコマンドを入力して、新規デバイスを厳密に調べます。

```
# cfgmgr -v
```

注: SAN 構成では、デバイスは **cfgmgr** コマンドが実行されるまでは、SAN スイッチにログインしません。

3. 次のコマンドを入力します。

```
# lsdev -Cc disk
```

4. **lsdev -Cc disk** コマンドの出力を調べて、以下のリストに示されているように、RDAC ソフトウェアがストレージ・サブシステム論理ドライブを認識することを確認します。

- 各 DS4200 論理ドライブが「1814 DS4200 Disk Array Device」として認識される。
- 各 DS4300 論理ドライブが「1722-600 (600) Disk Array Device」として認識される。
- 各 DS4400 論理ドライブが「1742-700 (700) Disk Array Device」として認識される。
- 各 DS4500 論理ドライブが「1742-900 (900) Disk Array Device」として認識される。
- 各 DS4700 論理ドライブが「1814 DS4700 Disk Array Device」として認識される。
- 各 DS4800 論理ドライブが「1815 DS4800 Disk Array Device」として認識される。

重要: 構成プロセスによって、1 つのストレージ・サブシステム上に 2 つの dac と 2 つの dar が作成されることに気付く場合があります。この状況は、関連する LUN が存在しない区画をホストが使用し

ているときに発生する場合があります。この状況が発生した場合、システムは正しい dar の下で 2 つの dac を関連付けることができません。LUN が存在しない場合は、システムは予想通り 2 つの dac を生成しますが、2 つの dar も生成します。

以下のリストは、最も一般的な原因を示しています。

- 区画を生成して LUN を区画に接続しているが、ホスト・ポートを区画に追加していません。そのため、ホスト・ポートはデフォルトの区画に残っています。
- 1 つ以上の HBA を交換後、区画の HBA の worldwide name (WWN) を更新していません。
- 再構成の一部として、あるセットの HBA から別のセットにストレージ・サブシステムを切り替えた後、WWN を更新していません。

それぞれの場合において問題を解決して、**cfgmgr** を再実行します。システムは余分な dar を除去するか、または Available 状態から Defined 状態に移します。(システムが dar を Defined 状態に移すと、これを削除することができます。)

注: デバイスの初期識別を実行すると、各デバイスのオブジェクト・データ・マネージャー (ODM) 属性がデフォルト値で更新されます。ほとんどの場合およびほとんどの構成において、デフォルト値で十分です。ただし、パフォーマンスと可用性を最大にするために、変更できる値もあります。AIX システムで **lsattr** コマンドを使用して属性の設定値を表示することに関する情報については、333 ページの『付録 D. AIX オブジェクト・データ・マネージャー (ODM) 属性の表示および設定』を参照してください。

MPIO による初期ディスクバリーの例

以下の例は、MPIO による初期ディスクバリーを示しています。

```
# lsdev -C |grep hdisk10
hdisk10    Available 05-08-02      MPIO Other DS4K Array Disk

# lscfg -vpl hdisk10
hdisk10    U787F.001.DPM0H2M-P1-C3-T1-W200400A0B8112AE4-L9000000000000
MPIO Other DS4K Array Disk
  Manufacturer.....IBM
  Machine Type and Model.....1814      FAStT
  ROS Level and ID.....30393136
  Serial Number.....
  Device Specific.(Z0).....0000053245004032
  Device Specific.(Z1).....

# mpio_get_config -A
Storage Subsystem worldwide name: 60ab8001122ae000045f7fe33
Storage Subsystem Name = 'Kinks-DS-4700'
  hdisk      LUN #
  hdisk2      1
  hdisk3      2
  hdisk4      3
  hdisk5      4
  hdisk6      5
  hdisk7      6
  hdisk8      7
  hdisk9      8
  hdisk10     9
  hdisk11    10
```

デバイスの構成

ストレージ・サブシステムのパフォーマンスを最大化するために、ご使用の `hdisk` のキュー項目数を設定し、キャッシュのミラーリングを使用不可にし、動的容量拡張および動的論理ドライブ拡張 (DVE) を使用し、LUN のサイズを確認することができます。

hot_add ユーティリティの使用

`hot_add` ユーティリティを使用すると、システムを再始動せずに、新しい論理ドライブを追加できます。このユーティリティは、新しい論理ドライブをオペレーティング・システムに登録し、ディスク・アドミニストレーターを使用して区画の作成や装置名の追加を行うことができますようにします。`hot_add` ユーティリティは、`SMutil` ソフトウェア・パッケージに含まれています。プログラムを 2 回実行しても新しい論理ドライブがディスク・アドミニストレーターのウィンドウに表示されない場合は、ファイバー・チャンネルの診断を実行するか、またはホストを再始動する必要があります。

`hot_add` ユーティリティを使用するには、特定のストレージ・サブシステムで論理ドライブを作成した後、そのストレージ・システムに接続されているホストで次の手順を実行します。

1. DOS またはコマンド・プロンプトから、次のディレクトリーに変更する。

```
<installation_directory>%Util
```

`installation_directory` は、`SMutil` がインストールされているディレクトリーです。

注: デフォルトのディレクトリーは `c:\Program Files\IBM_DS4000\Util` です。

2. DOS またはコマンド・プロンプトで、次のコマンドを入力する。

```
hot_add
```

3. Enter キーを押します。新しい論理ドライブがディスク・アドミニストレーターで使用できるようになります。

SMrepassist ユーティリティの使用

`SMrepassist` ユーティリティを使用して、論理ドライブのキャッシュ・データをフラッシュします。

重要: Windows 2000、Windows Server 2003、Windows Server 2008、または NetWare の環境では、FlashCopy 論理ドライブの基本論理ドライブが存在している同じサーバーに、FlashCopy ドライブを追加またはマップすることはできません。FlashCopy 論理ドライブを別のサーバーにマップする必要があります。

論理ドライブにおいてキャッシュされているデータをフラッシュするには、次の手順を完了します。

1. DOS またはコマンド・プロンプトから、ディレクトリーに変更する。

```
<installation_directory>%Util
```

`installation_directory` は、`SMutil` がインストールされているディレクトリーです。

注: デフォルトのディレクトリーは `c:\Program Files\IBM_DS4000\Util` です。

2. 次のコマンドを入力します。

```
smrepassist -f logical_drive_letter:
```

`logical_drive_letter` は、論理ドライブ上のディスク区画に割り当てられている、オペレーティング・システムのドライブ名です。

3. Enter キーを押します。

ホスト・エージェント・ソフトウェアの停止と再開

ホスト・エージェント・ソフトウェアの管理ドメインにストレージ・サブシステムを追加する場合は、ホスト・エージェント・ソフトウェアを停止して再び開始する必要があります。サービスを再開すると、ホスト・エージェント・ソフトウェアが新しいストレージ・サブシステムをディスカバーして、管理ドメインに追加します。

注: 再開した後でアクセス論理ドライブが検出されない場合には、ホスト・エージェント・ソフトウェアは自動的に実行を停止します。ホストと、ストレージ・サブシステムが接続されている SAN の間がファイバー・チャネルで接続されていることを確認してから、ホストまたはクラスター・ノードを再始動して、新しいホスト・エージェント管理ストレージ・サブシステムがディスカバーされるようにします。

このセクションに記載されている、ご使用のオペレーティング・システムに該当する手順を使用してください。

Windows 2000

Windows 2000 でホスト・エージェント・ソフトウェアを停止して再開するには、次の手順を実行します。

1. 「スタート」 > 「プログラム」 > 「管理ツール」 > 「サービス」をクリックする。「サービス」ウィンドウが開きます。
2. 「IBM DS Storage Manager Agent (IBM DS ストレージ・マネージャー・エージェント)」を右クリックする。
3. 「再起動」をクリックする。ストレージ・マネージャー・エージェントが停止して、再び開始します。
4. 「サービス」ウィンドウを閉じる。

Windows Server 2003 および 2008

Windows Server 2003 および 2008 でホスト・エージェント・ソフトウェアを停止して再開するには、次の手順を実行します。

1. 「スタート」 > 「管理ツール」 > 「サービス」をクリックする。「サービス」ウィンドウが開きます。
2. 「IBM DS Storage Manager Agent (IBM DS ストレージ・マネージャー・エージェント)」を右クリックする。
3. 「再起動」をクリックする。ストレージ・マネージャー・エージェントが停止して、再び開始します。
4. 「サービス」ウィンドウを閉じる。

Windows Server 2012

Windows Server 2012 のホスト・エージェント・ソフトウェアを停止および再開するには、以下の手順を完了します。

1. 「Server Manager (サーバー・マネージャー)」 > 「Tools (ツール)」 > 「Services (サービス)」をクリックします。「サービス」ウィンドウが開きます。
2. 「IBM DS Storage Manager Agent (IBM DS ストレージ・マネージャー・エージェント)」を右クリックする。
3. 「再起動」をクリックする。ストレージ・マネージャー・エージェントが停止して、再び開始します。
4. 「サービス」ウィンドウを閉じる。

hdisk デバイスのキュー項目数の設定

queue_depth 属性を適切な値に設定することは、最適なシステム・パフォーマンスを確保する上で重要なことです。ストレージ・サブシステム構成の規模が大きく、多数の論理ドライブとホストが接続されている場合は、この設定を使用します。

このセクションでは、キューの最大長を計算する方法を記載します。これは、ご使用の構成に最も適したキューの最大長の設定値を決めるのに役立つガイドラインとして使用できます。

キューの最大長の計算

システムのキューの最大長を計算する数式は、コントローラー上にどのファームウェア・バージョンがインストールされているかによって異なります。以下の数式のいずれか 1 つを使用して、使用するシステムのキューの最大長を計算してください。

重要:

1. キューの最大長は、すべての事例で最適な設定になるとは限りません。キューの最大長をガイドラインとして使用し、使用する特定の構成の必要に応じて、設定を調整してください。
2. 1 つ以上の SATA デバイスを接続したシステムでは、queue_depth 属性をキューの最大長より小さい値に設定することが必要になる場合があります。

コントローラー・ファームウェア・バージョン 07.10.xx.xx 以降用の数式

ストレージ・サブシステム・コントローラー・ファームウェア・バージョン 07.10.xx.xx 以降を実行している DS4800 および DS4700 または DS4200 ストレージ・システムでは、次の数式を使用して、キューの最大長を判別します。

DS4800: $4096 / (\text{ホスト数} * \text{ホストごとの LUN 数})$ 。例えば、それぞれ 32 の LUN を備えたホストが 4 つある DS4800 システムでは、キューの最大長は、次のように **32** になります。 $4096 / (4 * 32) = 32$ 。

DS4700 または DS4200: $2048 / (\text{ホスト数} * \text{ホストごとの LUN 数})$ 。例えば、それぞれ 32 の LUN を備えたホストが 4 つある DS4700 システムまたは DS4200 システムの場合、キューの最大長は、次のように **16** になります。 $2048 / (4 * 32) = 16$ 。

コントローラー・ファームウェアのバージョン 05.4x.xx.xx または 06.1x.xx.xx から 06.6x.xx.xx 用の数式

ストレージ・サブシステム・コントローラー・ファームウェア・バージョン 05.4x.xx.xx、または 06.1x.xx.xx から 06.6x.xx.xx を実行している DS4000 または DS5000 ストレージ・システムでは、次の数式を使用して、キューの最大長を判別します。 $2048 / (\text{ホスト数} * \text{ホストごとの LUN 数})$ 。例えば、それぞれ 32 の LUN を備えたホストが 4 つあるシステムでは、キューの最大長は、次のように **16** になります。 $2048 / (4 * 32) = 16$ 。

コントローラー・ファームウェアのバージョン 05.30.xx.xx 用の数式

ストレージ・サブシステム・コントローラー・ファームウェア・バージョン 05.30.xx.xx 以前を実行している DS4000 または DS5000 ストレージ・システムでは、次の数式を使用して、キューの最大長を判別します。 $512 / (\text{ホスト数} * \text{ホストごとの LUN 数})$ 。例えば、それぞれ 32 の LUN を備えたホストが 4 つあるシステムでは、キューの最大長は、次のように **4** になります。 $512 / (4 * 32) = 4$ 。

Windows のキュー項目数の変更

QLogic SANsurfer プログラムを使用して、Windows オペレーティング・システム環境から「Host Adapter Settings (ホスト・アダプターの設定)」および「Advanced Adapter Settings (拡張アダプター設定)」プリファレンスを変更することができます。ただし、変更を有効にするにはサーバーを再始動する必要があります。

Microsoft Windows オペレーティング・システム環境で QLogic アダプターのキュー項目数の設定を変更するには、Fast!UTIL の「**Configuration Settings (設定の構成)**」メニューを選択し、次に「**Advanced Adapter Settings (拡張アダプター設定)**」選択して、**Execution Throttle** にアクセスする必要があります。

AIX のキュー項目数の変更

AIX の `queue_depth` 属性を変更するには、次の例に示すように、**chdev -l** コマンドを使用します。

```
# chdev -l hdiskX -a queue_depth=y -P
```

ここで、*X* は `hdisk` の名前で、*y* はキュー項目数の設定です。

注: 変更を Customized Devices オブジェクト・クラス内で永続的なものにするには、**-P** フラグを使用します。

キャッシュのミラーリングの使用不可化

重要: キャッシュのミラーリングを使用不可にしているときに、コントローラーに障害が起こったり、コントローラーの電源がオフになると、データを失う可能性があります。キャッシュのミラーリングを使用不可にする前に、すべてのデータをバックアップしてください。

ストレージ・マネージャーでキャッシュのミラーリングを使用不可にするには、以下の手順を実行します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「**Logical (論理)**」または「**Physical (物理)**」タブで、キャッシュのミラーリングを使用不可にしたい論理ドライブを右クリックして、「**Change (変更)**」 > 「**Cache Settings (キャッシュ設定)**」を選択します。
2. 「Change Cache Settings (キャッシュ設定値の変更)」ウィンドウで、「**Enable write caching with mirroring (書き込みキャッシングのミラーリングの使用可能化)**」チェック・ボックスをクリアします。
3. 「**OK**」をクリックします。

注: AIX オペレーティング・システムの場合、書き込みキャッシュを使用可能にし、キャッシュのミラーリングを使用不可にして実行している LUN がオープンされると、FCP アレイ警告メッセージが表示されます。警告は、キャッシュのミラーリングが再度使用可能になるまで、24 時間ごとに表示されます。

動的容量拡張および動的論理ドライブ拡張の使用

動的論理ドライブ拡張 (DVE) は、論理ドライブのサイズを増加させます。DVE を実行するには、アレイ内に使用可能な空き容量が必要です。それがなければ、動的容量拡張 (DCE) を実行し、ドライブを追加してアレイの容量を増加させることができます。アレイ内に十分な空き容量が存在することを確認した後、DVE の操作を実行することができます。

動的容量拡張の実行

アレイの容量を増やすには、以下の手順を完了して DCE を実行します。

注: この手順について詳しくは、ストレージ・マネージャーのオンライン・ヘルプを参照してください。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「**Logical (論理)**」または「**Physical (物理)**」タブで、アレイを右クリックして、「**Add Free Capacity (Drives) (空き容量 (ドライブ) の追加)**」を選択します。
2. 「Add Free Capacity (Drives) (空き容量 (ドライブ) の追加)」ウィンドウで、1 つまたは 2 つの使用可能なドライブを選択し、「**Add (追加)**」をクリックします。

動的論理ドライブ拡張の実行

動的論理ドライブ拡張 (DVE) を実行する前に、アレイ内に使用可能な空き容量が存在することを確認してください。「Subsystem Management (サブシステム管理)」ウィンドウの「**Logical (論理)**」または「**Physical (物理)**」タブで、使用可能な空き容量を確認してください。十分な空き容量がない場合でも、追加のドライブが使用可能である場合は、DVE 操作を実行する前に動的容量拡張 (DCE) 操作を実行して、アレイに 1 つ以上のドライブを追加することができます。

注:

1. アレイが標準モードまたは拡張並行モードで活動化されている間は、論理ドライブをサイズ変更することはできません。
2. ルート・アレイのサイズ変更は行えません。

論理ドライブのサイズを増やすには、以下の手順を完了して DVE を実行します。

注: この手順について詳しくは、ストレージ・マネージャーのオンライン・ヘルプを参照してください。

1. 「Subsystem Management (サブシステム管理)」ウィンドウの「**Logical(論理)**」タブまたは「**Physical (物理)**」タブで、論理ドライブを右クリックして、「**Increase Capacity (容量の増加)**」を選択します。
「Increase Logical Drive Capacity – Additional Instructions (論理ドライブ容量の増加 – 追加指示)」ウィンドウが開きます。
2. 追加指示を読み、「**OK**」をクリックします。「Increase Logical Drive Capacity (論理ドライブ容量の増加)」ウィンドウが開きます。
3. 増加させたい論理ドライブの量を入力し、「**OK**」をクリックします。アレイ内のすべての論理ドライブ上に、クロック・アイコンが表示されます。何らかのホストの介入を開始する前に、このプロセスが完了するまで待つ必要があります。

注: ストレージ・サブシステムがビジーの場合は、プロセスに数時間かかる場合があります。

4. 次のコマンドを入力して、ホスト上の論理ドライブを再スキャンします。

```
# cd /sys/block/sdXX/device  
# echo 1 > rescan
```

XX はデバイス名です。

5. 180 ページの『LUN サイズの確認』で説明されている手順を使用し、論理ドライブのサイズを確認します。
6. 論理ドライブを再マウントします。

SUSE Linux Enterprise Server での Veritas Storage Foundation

LVM スキャンが原因でブート時間が長くなることがあります。Veritas Storage Foundation 環境では LVM スキャンは必要ありません。そのため、SLES 10 SP2 以降では LVM スキャンを使用不可にする必要があります。LVM スキャンを使用不可にするには、次の手順を使用します。

注:

- Veritas Storage Foundation Linux 環境では、デフォルト・ホスト・タイプは 13 (コントローラー・ファームウェア・バージョンに応じて LNXCLVMWARE または LNXCLUSTER) に設定されている必要があります。
 - IBM は DMP A/P-F ASL/APM のみをサポートし、A/P-C ASL はサポートしません。
 - ブート時、DMP がロードされる前に、入出力プローブが非所有コントローラーに進むと、タイムアウト・エラーが生じます。これらのブート時エラーは避けられませんが、重大なエラーではありません。
1. ファイル `/etc/lvm/lvm.conf` で行フィルター = ["a./"] をフィルター = ["r|/dev./*/by-path/*|", "r|/dev./*/by-id/*|", "r|/dev/sd.*|", "a./"] に変更します。
 2. `root/swap` が LVM ボリューム内にある場合は、次のタスクを実行します。
 - ステップ 1 のフィルターに特定のデバイスを追加して、該当するボリュームがスキャンされることを確認します。
 - ステップ 1 を完了した後、`mkinitrd` を実行し、今後のブートに新しい `initrd` イメージを使用します。

Red Hat Enterprise Linux での Veritas Storage Foundation 5.0

以下の手順は、Storage Foundation 5.0 の場合にのみ、RHEL 5.3 で RDAC モジュールを使用可能にするために必要です。このモジュールは、Storage Foundation 5.1 以降には組み込まれています。`scsi_dh_RDAC` モジュールは、RDAC デバイスに対するサポートを提供します。遅延時間をなくし、ブートまたはプローブ・プロセスの実行時のいくつかのエラー・メッセージをなくします。

注:

1. Veritas Storage Foundation Linux 環境では、デフォルト・ホスト・タイプは 13 (コントローラー・ファームウェア・バージョンに応じて LNXCLVMWARE または LNXCLUSTER) に設定されている必要があります。
2. IBM は DMP A/P-F ASL/APM のみをサポートし、A/P-C ASL はサポートしません。
3. ブート時、DMP がロードされる前に、入出力プローブが非所有コントローラーに進むと、タイムアウト・エラーが生じます。これらのブート時エラーは避けられませんが、重大なエラーではありません。
4. 以下の手順は、IBM NVSRAM で機能します。`scsi_dh_RDAC` モジュールは VID/PID に依存しているためです。

Storage Foundation 5.0 の場合の RHEL 5.3 での RDAC モジュールの使用可能化

Storage Foundation 5.0 の場合に RHEL 5.3 で RDAC モジュールを使用可能にするには、以下の手順を実行します。

1. HBA が検出できないように、すべてのストレージ・サブシステム・ストレージ・ポートを使用不可にします。
2. Storage Foundation をインストールします。
3. 次のように `mkinitrd` を実行して、`scsi_dh_rdac` モジュールを組み込みます。

```
mkinitrd $resultant_initrd_image_file $kernel_version --preload=scsi_dh_rdac
```

例えば、以下のとおりです。

```
mkinitrd /boot/my_image 2.6.18-118.el5 --preload=scsi_dh_rdac
```

注: `uname -r` コマンドはカーネル・バージョンを示します。

4. 新しい `initrd` イメージを使用するようにブート・ローダーを変更します。IBM i および System p サーバーの場合、`initrd` イメージ名は `yaboot` です。System x サーバーの場合、イメージ名は `grub` です。
5. ホスト・サーバーをシャットダウンします。
6. HBA がストレージ構成を認識するように、ストレージ・サブシステムを使用可能にします。
7. ホスト・サーバーを開始します。

Storage Foundation 5.0 の場合の RHEL 5.3 での RDAC モジュールのアンロード

デバイスのプローブおよび接続プロセスの後でモジュールをアンロードするには、システム・ブート・プロセス中に以下の手順を実行します。

1. 次の例に示すように、`/etc/rc3.d` スクリプトを作成します。

```
# vi /etc/init.d/rm_rdac

-----
## this script is used for detaching the scsi_dh_rdac module for each LUN
## this script has dependency on lsscsi command and this lsscsi should be available for this
## script to successfully execute.
#!/bin/bash
echo "detaching the scsi_dh_rdac module"
for i in /sys/block/sd*/device/dh_state
do
if [[ "`cat $i`" = "rdac" ]]
then
echo detach > $i
fi
done

modprobe -r scsi_dh_rdac
echo "detached successfully"
-----
```

2. `/etc/rc3.d` の下で、VCS VxFen ドライバーの始動スクリプト (VxFen ドライバーのデフォルトの始動スクリプトは `/etc/rc2.d/S68vxfen`) の前の正しい場所にスクリプトを挿入します。システムが VCS を実行していない場合は、このスクリプトを `/etc/rc3.d/S50vxvm-recover` スクリプトの後に挿入します。

```
# ln -s /etc/init.d/rm_rdac /etc/rc.d/rc3.d/S57rm_rdac
# ln -s /etc/init.d/rm_rdac /etc/rc.d/rc5.d/S57rm_rdac
```

LUN サイズの確認

AIX で LUN のサイズを確認するには、以下の手順を実行します。

1. 以下のコマンドを入力します。

```
#cd /sys/block/sdXX
# cat size
```

XX はデバイス名です。次の例に示すように、数値が表示されます。

```
8388608
```

2. 次の例に示されているように、この数値に 512 (バイト) を乗算して、LUN のサイズを計算します。

```
8388608 * 512 = 4294967296 (~ 4GB)
```

この例では、LUN サイズは約 4 GB です。

論理ドライブの再配分

論理ドライブがその 2 次コントローラー・パスにフェイルオーバーしている状態では、一部の構成は、エラーが解決した後で、これらのドライブを元に戻すための手動操作が必要となります。この介入が必要かどうかは、インストールされているホスト・マルチパス・ドライバーと、ADT (自動ドライブ転送) が使用可能かどうかによって決まります。AIX および Windows ではデフォルトで ADT が使用不可に設定されていますが、それらのマルチパス・ドライバーは自動リカバリーが可能です。Linux ではデフォルトで ADT が使用可能に設定されていますが、MPP ドライバーは同様の自動リカバリーが可能です。このドライバーを使用する際は、ADT を使用不可に設定してください。

「Subsystem Management (サブシステム管理)」ウィンドウで論理ドライブを手動で優先パスに再配分するには、「**Advanced (拡張)**」 > 「**Recovery (リカバリー)**」 > 「**Redistribute Logical Drives (論理ドライブの再配分)**」をクリックします。

AIX、HP-UX、または Solaris で論理ドライブを再配分するには、このセクションの該当する手順を実行してください。

AIX での論理ドライブの再配分

AIX ホストで自動リカバリーを使用可能にした場合は、コントローラーのフェイルオーバー後に論理ドライブを手動で再配分する必要はありません。ただし、異機種混合ホスト環境の場合は、論理ドライブの手動による再配布が必要な場合があります。ある種の形式の自動リカバリーをサポートしないホスト、または自動リカバリーが使用不可になっている AIX ホストは、論理ドライブを優先パスに自動的にリダイレクトすることはありません。

AIX のディスク・アレイ・エラーに関するトラブルシューティング情報については、263 ページの『第 7 章 Troubleshooting (トラブルシューティング)』の 289 ページの『AIX でのディスク・アレイのエラーの解決』を参照してください。

以下の手順を完了して、手動で論理ドライブを所定のパスに再配分します。

1. 障害のあるコンポーネントを修復するかまたは交換します。詳しくは、ストレージ・サブシステムに付属の「インストール、メンテナンスおよびユーザーのガイド」を参照してください。
2. 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Advanced (拡張)**」 > 「**Recovery (リカバリー)**」 > 「**Redistribute Logical Drives (論理ドライブの再配分)**」をクリックして、論理ドライブを優先パスに再配分します。

注: 多数の LUN がストレージ・サブシステム上に構成されている場合、論理ドライブの再配分に 60 分以上かかることがあります。

3. 次の例に示されているように、**fget_config** コマンドを実行して、アクティブ・パスを検証します。

```
# fget_config -l dar0
dac0 ACTIVE dac1 ACTIVE
dac0-hdisk1
dac0-hdisk2
dac0-hdisk3
dac1-hdisk4
dac1-hdisk5
dac1-hdisk6
dac1-hdisk7
dac0-hdisk8
```

HP-UX での論理ドライブの再配分

HP-UX ホストでは、自動ドライブ転送 (ADT) がデフォルトで使用可能になっています。コントローラーのフェイルオーバーを開始させる障害が発生した場合、ADT は使用可能なコントローラーに入出力をリダイレクトします。ADT では手動による再配分は不要です。

重要: 異機種混合のホスト環境で障害が発生した場合、ADT を使用可能にした HP-UX ホストは、パスが使用可能になると LUN を自動的に再配分します。ただし、ADT が使用可能になっていないホストでは、手動で論理ドライブを再配分する必要があります。そうしないと、ストレージ・サブシステムは「Needs Attention (要注意)」状態のままになります。その理由は、ADT をサポートしないホストおよび ADT を使用不可にしたホストは、入出力を自動的に優先されるコントローラーにリダイレクトしないためです。この場合、ストレージ・マネージャーの Recovery Guru は、どのホスト・プラットフォームが、フェイルオーバー状態にある LUN に関連付けられているかを示します。

注: DS5000 ストレージ・サブシステムは ALUA 対応ではありません。DS5000 サブシステムには、ターゲット・ポート・グループ・サポート (TPGS) があります。これは、優先ポートに入出力を転送する類似の SCSI プロトコルです。HP-UX 11.31 の場合、デフォルトの HP-UX ホスト・タイプを TPGS ホスト・タイプ HPXTPGS に変更する必要があります。

TPGS サポートをオンにし、ホスト・タイプを変更するには、以下の手順を完了します。

1. DS5000 ストレージ・サブシステムのオペレーティング・システム・タイプを HP-UX から HPXTPGS に変更します。
2. ロード・バランシングを「**Default, round-robin (デフォルト、ラウンドロビン)**」に変更します。
3. 変更内容が正しいことを確認します。次の例は、正しい 4 つのアクティブ・パスと 4 つのスタンバイ・パスがある LUN の 1 つを示しています。

```
# scsimgr get_info all_lpt -D /dev/rdisk/asmlai|grep -e STATUS -e 'Open close state'
```

```
STATUS INFORMATION FOR LUN PATH : lunpath306
Open close state                  = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath344
Open close state                  = STANDBY
STATUS INFORMATION FOR LUN PATH : lunpath420
Open close state                  = STANDBY
STATUS INFORMATION FOR LUN PATH : lunpath326
Open close state                  = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath346
Open close state                  = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath213
Open close state                  = ACTIVE
STATUS INFORMATION FOR LUN PATH : lunpath273
Open close state                  = STANDBY
STATUS INFORMATION FOR LUN PATH : lunpath179
Open close state                  = STANDBY
```

4. SAN ファイバー・チャンネル・スイッチ・モニター・ツールを使用して、入出力負荷が適切に配分されていることを確認します。

Solaris での論理ドライブの再配分

ホストおよびホスト・ポートを定義するときにホスト・タイプとして Solaris を選択した場合は、自動ドライブ転送 (ADT) は Solaris ホスト上で使用不可になります。この場合、コントローラーのフェイルオーバーを開始させる障害が発生した場合は、優先パスに論理ドライブを手動で再配分する必要があります。

論理ドライブを優先パスに手動で再配分するには、以下の手順を実行します。

1. 障害のあるコンポーネントを修復するかまたは交換します。詳しくは、ストレージ・サブシステムに付属の「インストール、メンテナンスおよびユーザーのガイド」を参照してください。

2. 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Advanced (拡張)**」 > 「**Recovery (リカバリー)**」 > 「**Redistribute Logical Drives (論理ドライブの再配分)**」をクリックして、論理ドライブを優先パスに再配分します。

ホット・スワップ HBA の交換

重要: ここに記載されている手順に従わない場合、データの可用性が失われる可能性があります。HBA ホット・スワップ手順を開始する前に、このセクションの手順をすべて読み、理解しておく必要があります。

このセクションでは、System p サーバー上でファイバー・チャネル・ホスト・バス・アダプター (HBA) をホット・スワップする手順について説明します。

次のリストに、このセクションの概要を示します。

- 『AIX でのホット・スワップ HBA の交換』
- 187 ページの『Linux での IBM HBA の交換』
- 190 ページの『PCI ホット・プラグ HBA の交換』
- 191 ページの『AIX および Linux 用ストレージ・サブシステムへの新しい WWPN のマッピング』
- 191 ページの『HBA ホット・スワップ手順の完了』

AIX でのホット・スワップ HBA の交換

重要: これらの注と手順から逸脱すると、データの可用性が失われるおそれがあります。

AIX でホット・スワップ操作を実行する前に、下記の問題と制約事項のリストを確認してください。

- dar の autorecovery 属性は、no に設定する必要があります。autorecovery は、ホット・スワップ手順が完了した後オンに戻ることができる、動的に設定される機能です。ホット・スワップ手順のときに autorecovery モードを使用不可にできないと、データへのアクセスが失われるおそれがあります。
- HBA 交換が成功したことで、後続の構成が正しく行われたことを確認するまで、論理ドライブを優先パスへ再配分しないでください。ホット・スワップと構成の成功を確認する前に論理ドライブを再配分すると、データへのアクセスが失われるおそれがあります。
- 唯一のサポートされるホット・スワップ・シナリオでは、障害のある HBA を同じ HBA モデルに、しかも同じ PCI スロットで交換します。欠陥のある HBA は、たとえその HBA が欠陥がないとわかった場合でも、他のシステムに挿入しないでください。必ず、その HBA を IBM に返品してください。

重要: 本書の作成時点では、交換シナリオのこれ以外のバリエーションはサポートされていません。

- ホット・スワップは、単一 HBA 構成ではサポートされません。

AIX での HBA ホット・スワップの準備:

ホット・スワップを準備するには、以下の手順を完了します。

システム・データの収集

システムからデータを収集するには、以下の手順を完了します。

1. 次のコマンドを入力します。

```
# lsdev -C |grep fcs
```

出力は、次の例と同様になります。

```
fcs0      Available 17-08      FC Adapter
fcs1      Available 1A-08      FC Adapter
```

2. 次のコマンドを入力します。

```
# lsdev -C |grep dac
```

出力は、次の例と同様になります。

```
dac0      Available 17-08-02    1815    DS4800 Disk Array Controller
dac1      Available 1A-08-02    1815    DS4800 Disk Array Controller
```

3. それぞれの fcs デバイスについて、次のコマンドを入力します。

```
# lscfg -vpl fcsX
```

ここで、*X* は fcs デバイスの番号です。出力は、次の例と同様になります。

```
lscfg -vpl fcs0
fcs0      U0.1-P1-I1/Q1  FC Adapter

Part Number.....09P5079
EC Level.....A
Serial Number.....1C21908D10
Manufacturer.....001C
Feature Code/Marketing ID...2765
FRU Number.....09P5080
Network Address.....10000000C92D2981
ROS Level and ID.....02C03951
Device Specific.(Z0).....2002606D
Device Specific.(Z1).....00000000
Device Specific.(Z2).....00000000
Device Specific.(Z3).....03000909
Device Specific.(Z4).....FF401210
Device Specific.(Z5).....02C03951
Device Specific.(Z6).....06433951
Device Specific.(Z7).....07433951
Device Specific.(Z8).....20000000C92D2981
Device Specific.(Z9).....CS3.91A1
Device Specific.(ZA).....C1D3.91A1
Device Specific.(ZB).....C2D3.91A1
Device Specific.(YL).....U0.1-P1-I1/Q1
```

PLATFORM SPECIFIC

```
Name: Fibre Channel
Model: LP9002
Node: Fibre Channel@1
Device Type: fcp
Physical Location: U0.1-P1-I1/Q1
```

4. 次のコマンドを入力します。

```
# lsdev -C |grep dar
```

出力は、次の例と同様になります。

```
# dar0      Available      1815    DS4800 Disk Array Router
dar1      Available      1815    DS4800 Disk Array Router
```

5. 次のコマンドを入力して、システム上で検出された各 dar の属性をリストします。

```
# lsattr -El darX
```

ここで、*X* は dar の番号です。出力は、次の例と同様になります。

```
lsattr -El dar0
act_controller  dac0,dac2  Active Controllers      False
all_controller  dac0,dac2  Available Controllers  False
```


held_in_reset	none	Held-in-reset controller	True
load_balancing	no	Dynamic Load Balancing	True
autorecovery	no	Autorecover after failure is corrected	True
hlthchk_freq	600	Health check frequency in seconds	True
aen_freq	600	Polled AEN frequency in seconds	True
balance_freq	600	Dynamic Load Balancing frequency in seconds	True
fast_write_ok	yes	Fast Write available	False
cache_size	1024	Cache size for both controllers	False
switch_retries	5	Number of times to retry failed switches	True

autorecovery が使用不可であることの確認

ホット・スワップを行う前に、ホット・スワップしたい HBA に関与するすべての dar 上で autorecovery が使用不可になっていることを確認するために、以下の手順を実行します。

1. その HBA に関与するすべての dac を識別するため、次のコマンドを入力します。

```
# lsdev -C|grep 11-08
```

出力は、次の例と同様になります。

```
# lsdev -C|grep 11-08
fcs0      Available 11-08      FC Adapter
fscsi0    Available 11-08-01    FC SCSI I/O Controller Protocol Device
dac0      Available 11-08-01    1742      (700) Disk Array Controller
hdisk1    Available 11-08-01    1742      (700) Disk Array Device
hdisk3    Available 11-08-01    1742      (700) Disk Array Device
hdisk5    Available 11-08-01    1742      (700) Disk Array Device
hdisk7    Available 11-08-01    1742      (700) Disk Array Device
hdisk8    Available 11-08-01    1742      (700) Disk Array Device
```

2. 183 ページの『システム・データの収集』の手順のステップ 5 で収集した **lsattr** コマンド出力を参照します。 **lsattr** 出力の中で、この手順のステップ 1 で識別した dac をリストしている dar を識別します。
3. ステップ 2 で識別した dar ごとに、次のコマンドを入力します。

```
# lsattr -El darX |grep autorecovery
```

ここで、*X* は dar の番号です。出力は、次の例と同様になります。

```
# lsattr -El dar0 |grep autorecovery
autorecovery  no      Autorecover after failure is corrected      True
```

4. **lsattr** コマンド出力の中で、2 番目のワードが no であることを検証します。2 番目のワードが yes である場合、autorecovery は現在使用可能になっています。

重要: autorecovery が使用可能になっている各 dar ごとに、それを使用不可にするために、autorecovery ODM 属性を no に設定します。属性の設定値を変更する方法については、338 ページの『ODM 属性を表示する lsattr コマンドの使用』を参照してください。このステップが完了し、autorecovery が使用不可であることを確認するまで、ホット・スワップ手順を進めないでください。

ホット・スワップ HBA の交換:

重要: ここに記載されている手順に従わない場合、データの可用性が失われる可能性があります。HBA ホット・スワップ手順を開始する前に、このセクションの手順をすべて読み、理解しておく必要があります。

ホット・スワップ HBA を交換するには、以下の手順を実行します。

1. 次のコマンドを入力して、交換したい HBA を Defined 状態にします。

```
# rmdev -Rl fcsX
```

ここで、*X* は HBA の番号です。出力は、次の例と同様になります。

```
rmdev -Rl fcs0
fcnet0 Defined
dac0 Defined
fscsi0 Defined
fcs0 Defined
```

Linux オペレーティング・システムの場合は、次のコマンドを入力して、PCI ホット・プラグ・スロットを識別します。

```
# drslot_chrp_pci -i -s slot-name
```

ここで、*slot-name* は、交換する HBA のスロットの名前です (例えば、U7879.001.DQD014E-P1-C3)。

スロット *slot-name* の LED が明滅して、次のメッセージが表示されます。

```
The visual indicator for the specified
PCI slot has been set to the identify
state. Press Enter to continue or
enter x to exit.
```

2. AIX smit メニューで、「smit」 > 「Devices (デバイス)」 > 「PC Hot Plug Manager (PC ホット・プラグ・マネージャー)」 > 「Replace/Remove a PCI Hot Plug Adapter (PCI ホット・プラグ・アダプターの交換/取り外し)」をクリックして、HBA のホット・スワップに必要なプロセスを開始します。
3. 「Replace/Remove a PCI Hot Plug Adapter (PCI ホット・プラグ・アダプターの交換/取り外し)」ウィンドウで、ターゲットとなる HBA を選択します。ウィンドウが開き、HBA を交換するための指示が表示されます。
4. smit の指示に従って、HBA を交換してください。

注: この時点では、ファイバー・チャネル・ケーブルの再取り付けをしないでください。

5. この手順のステップがこの時点まで正常に完了した場合、次の結果が得られます。

- 障害のある HBA がシステムから取り外された。
- 交換用 FC HBA の電源がオンになる。
- 関連する fcsX デバイスが Defined 状態になる。

先へ進む前に、これらの結果が得られたかどうかを検証してください。

6. 置き換えの HBA にファイバー・チャネル・ループをインストールします。
7. 次のコマンドを入力して、その HBA を Active 状態にします。

```
# cfgmgr
```

注: 新規 HBA はデフォルト・グループに置かれます。hdisk がデフォルト・グループに割り当てられている場合、HBA は新規 dar および dac を生成します。これにより、分割が行われます。WWPN をマップした後、**rmdev** コマンドを出して新規 dar および dac を除去してください。

8. 次のコマンドを入力して、fcs デバイスが使用可能になったことを検証します。

```
# lsdev -C |grep fcs
```

9. 次のコマンドを入力して、置き換えの HBA のファームウェアを検証するか、正しいレベルまでアップグレードします。

```
# lscfg -vpl fcsX
```

ここで、*X* は fcs の番号です。

10. Network Address に関連した 16 桁の数値を記録してください。この数値は、ステップ 9 で使用したコマンドの出力の中に表示されたものです。このネットワーク・アドレス番号は、次の手順の 191 ページの『AIX および Linux 用ストレージ・サブシステムへの新しい WWPN のマッピング』で使用されます。

11. 次のコマンドを入力して、HBA を Defined 状態に戻します。

```
# rmdev -Rl fcsX
```

この手順を完了した後、191 ページの『AIX および Linux 用ストレージ・サブシステムへの新しい WWPN のマッピング』に進みます。

Linux での IBM HBA の交換

このセクションでは、System p サーバー内の IBM ホスト・バス・アダプターを PCI ホット・プラグ・ツールを使用して交換するための要件と手順を記載します。

Linux での IBM HBA ホット・スワップの準備: ホット・スワップを準備するには、以下の手順を完了します。

PCI ホット・プラグ・ツールの確認

以下のツールが /usr/sbin ディレクトリーにインストールされていることを確認します。

- lsslot
- drslot_chrp_pci

これらのツールがインストールされていない場合は、以下の手順を完了してインストールします。

1. rdist-6.1.5-792.1 および compat-2004.7.1-1.2 が SLES 9 メディアからインストールされていることを確認します。
2. PCI ホット・プラグ・ツールの rpm ファイルを見つけるには、<http://www14.software.ibm.com/webapp/set2/sas/f/lopdiags/> にアクセスします。
3. この Web サイトで、ご使用のオペレーティング・システムの該当リンクを選択します。以下の rpm ファイルをダウンロードし、インストールします。

- librtas-1.3.1-0.ppc64.rpm
- rpa-pci-hotplug-1.0-29.ppc64.rpm

4. 次のコマンドを入力して、それぞれの rpm ファイルをインストールします。

```
# rpm -Uvh <filename>.rpm
```

ここで<filename> は rpm ファイルの名前です。

PCI コアがインストール済みであることの確認

PCI コアがシステム上にインストールされている必要があります。次のコマンドを入力して、インストールされていることを確認します。

```
# ls -l /sys/bus/pci/slots
```

PCI コアがインストールされている場合、出力は次の例のようになります。

```
elml7c224:/usr/sbin # ls -l /sys/bus/pci/slots
total 0
drwxr-xr-x  8 root root 0 Sep  6 04:29 .
drwxr-xr-x  5 root root 0 Sep  6 04:29 ..
drwxr-xr-x  2 root root 0 Sep  6 04:29 0000:00:02.0
drwxr-xr-x  2 root root 0 Sep  6 04:29 0000:00:02.4
```

```
drwxr-xr-x 2 root root 0 Sep 6 04:29 0000:00:02.6
drwxr-xr-x 2 root root 0 Sep 6 04:29 0001:00:02.0
drwxr-xr-x 2 root root 0 Sep 6 04:29 0001:00:02.6
drwxr-xr-x 2 root root 0 Sep 6 04:29 control
```

/sys/bus/pci/slots ディレクトリが存在しない場合、PCI コアはインストールされていません。

rpaphp ドライバーがインストール済みであることの確認

rpaphp ドライバーがシステム上にインストールされている必要があります。次のコマンドを入力して、インストールされていることを確認します。

```
ls -l /sys/bus/pci/slots/*
```

rpaphp ドライバーがインストールされている場合、出力は次の例のようになります。

```
elm17c224:/usr/sbin # ls -l /sys/bus/pci/slots/*
/sys/bus/pci/slots/0000:00:02.0:
total 0
drwxr-xr-x 2 root root 0 Sep 6 04:29 .
drwxr-xr-x 8 root root 0 Sep 6 04:29 ..
-r--r--r-- 1 root root 4096 Sep 6 04:29 adapter
-rw-r--r-- 1 root root 4096 Sep 6 04:29 attention
-r--r--r-- 1 root root 4096 Sep 6 04:29 max_bus_speed
-r--r--r-- 1 root root 4096 Sep 6 04:29 phy_location
-rw-r--r-- 1 root root 4096 Sep 6 04:29 power
```

スロット情報をリストするための lsslot ツールの使用: PCI ホット・プラグを使用して HBA を交換する前に、lsslot ツールを使用して入出力スロットに関する情報をリストすることができます。このセクションでは、lsslot の使用方法を説明し、例を記載します。lsslot ツールは、以下のガイドラインに従って使用します。

lsslot ツールの構文

lsslot 構文を、次の例に示します。

```
lsslot [ -c slot | -c pci [ -a | -o ] ] [ -s drc-name ] [ -F delimiter ]
```

lsslot ツールのオプション

lsslot オプションを、次のリストに示します。

オプションなし

すべての DR スロットを表示します。

-c slot すべての DR スロットを表示します。

-c pci すべての PCI ホット・プラグ・スロットを表示します。

-c pci -a

使用可能な (空いている) すべての PCI ホット・プラグ・スロットを表示します。

-c pci -o

占有されているすべての PCI ホット・プラグ・スロットを表示します。

-F 区切り文字を使用して列を区切ります。

lsslot コマンドを使用する PCI ホット・プラグ・スロットのリスト表示

このセクションでは、すべての PCI ホット・プラグ・スロット、空いているすべての PCI ホット・プラグ・スロット、または占有されているすべての PCI ホット・プラグ・スロットをリストするために使用できるコマンド行を示します。また、PCI ホット・プラグ・デバイスに関する詳細情報を表示することもできます。

注: コマンド行出力の「*Device(s)* (デバイス)」列には、スロット内の PCI デバイスが *xxxx:yy:zz.t* の形式でリストされます (例えば、0001:58:01.1)。

すべての PCI ホット・プラグ・スロットをリストするには、次のコマンドを入力します。

```
# lsslot -c pci -a
```

結果出力は、次の例と同様になります。

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C1	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C2	PCI-X capable, 64 bit, 133MHz slot	0002:58:01.0
U7879.001.DQD014E-P1-C3	PCI-X capable, 64 bit, 133MHz slot	0001:40:01.0
U7879.001.DQD014E-P1-C4	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C5	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C6	PCI-X capable, 64 bit, 133MHz slot	0001:58:01.0

空いているすべての PCI ホット・プラグ・スロットを表示するには、次のコマンドを入力します。

```
# lsslot -c pci -a
```

結果出力は、次の例と同様になります。

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C1	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C4	PCI-X capable, 64 bit, 133MHz slot	Empty
U7879.001.DQD014E-P1-C5	PCI-X capable, 64 bit, 133MHz slot	Empty

占有されているすべての PCI ホット・プラグ・スロットをリストするには、次のコマンドを入力します。

```
# lsslot -c pci -o
```

結果出力は、次の例と同様になります。

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C2	PCI-X capable, 64 bit, 133MHz slot	0002:58:01.0
U7879.001.DQD014E-P1-C3	PCI-X capable, 64 bit, 133MHz slot	0001:40:01.0
U7879.001.DQD014E-P1-C6	PCI-X capable, 64 bit, 133MHz slot	0001:58:01.0

PCI ホット・プラグ・デバイスに関する詳細情報を表示するには、以下の手順を実行します。

1. 前の出力例に見られるような、# `lsslot -c pci -o` の出力からデバイス番号を選択します。
2. デバイスに関する詳細情報を表示するには、次のコマンドを入力します。

```
# lspci | grep xxxx:yy:zz.t
```

ここで、*xxxx:yy:zz.t* は、PCI ホット・プラグ・デバイスの番号です。結果出力は、次の例と同様になります。

```
0001:40:01.0 Ethernet controller: Intel Corp. 82545EM Gigabit  
Ethernet Controller (Copper) (rev 01)
```


PCI ホット・プラグ HBA の交換

`drslot_chrp_pci` コマンドを使用して PCI ホット・プラグ HBA を交換するには、次の手順を完了します。

重要: HBA を取り外す前に、HBA に接続されているファイバー・チャンネル・ケーブルを取り外す必要があります。すべての入出力アクティビティが代替パスに転送されたことを確認するために、ファイバー・チャンネル・ケーブルは、少なくとも 5 分間接続しないままにしておく必要があります。ファイバー・チャンネル・ケーブルの取り外しが失敗すると、望ましくない結果を引き起こす可能性があります。

注: これらの手順で、変数 `slot-name` は、交換する HBA が入っているスロットを指します。

1. 次のコマンドを入力して、PCI ホット・プラグ・スロットを識別します。

```
# drslot_chrp_pci -i -s slot-name
```

ここで、`slot-name` は、交換する HBA のスロットの名前です (例えば、U7879.001.DQD014E-P1-C3)。

スロット `slot-name` の LED が明滅を開始し、次のメッセージが表示されます。

```
The visual indicator for the specified
PCI slot has been set to the identify
state. Press Enter to continue or
enter x to exit.
```

2. 次のようにして、スロットから HBA をホット・アンプラグ (取り外し) します。

- a. HBA に接続されているファイバー・チャンネル・ケーブルを取り外し、フェイルオーバーの完了を待ちます。
- b. フェイルオーバーが完了したら、次のコマンドを入力します。

```
# drslot_chrp_pci -r -s slot-name
```

次のメッセージが表示されます。

```
The visual indicator for the specified
PCI slot has been set to the identify
state. Press Enter to continue or
enter x to exit.
```

- c. Enter キーを押します。次のメッセージが表示されます。

```
The visual indicator for the specified
PCI slot has been set to the action state.
Remove the PCI card from the identified slot
and press Enter to continue.
```

- d. Enter キーを押します。
- e. スロットから HBA を物理的に取り外します。
- f. 次のコマンドを入力して、スロットが空になったことを検証します。

```
# lsslot -c pci -s slot-name
```

スロットが空の場合、結果出力は以下の例と同様になります。

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C3	PCI-X capable, 64 bit, 133MHz slot	Empty

3. スロットへの HBA のホット・プラグを行うには、以下の手順を完了します。

- a. 次のコマンドを入力します。

```
# drslot_chrp_pci -a -s slot-name
```

次のメッセージが表示されます。

The visual indicator for the specified
PCI slot has been set to the identify
state. Press Enter to continue or
enter x to exit.

- b. Enter キーを押します。次のメッセージが表示されます。

The visual indicator for the specified
PCI slot has been set to the action state.
Insert the PCI card into the identified slot,
connect any devices to be configured
and press Enter to continue. Enter x to exit.

- c. 新しい HBA をスロットに挿入します。
d. 次のコマンドを入力して、スロットが空でなくなったことを検証します。

```
# lsslot -c pci -s      slot-name
```

スロットが空でない場合、結果出力は以下の例と同様になります。

# Slot	Description	Device(s)
U7879.001.DQD014E-P1-C3	PCI-X capable, 64 bit, 133MHz slot	0001:40:01.0

AIX および Linux 用ストレージ・サブシステムへの新しい WWPN のマッピング

ホット・スワップによって影響を受ける各ストレージ・サブシステムごとに、以下の手順を実行して、HBA のワールドワイド・ポート名 (WWPN) をストレージ・サブシステムへマップします。

1. ストレージ・マネージャーを開始し、「Subsystem Management (サブシステム管理)」ウィンドウを開きます。
2. 「Subsystem Management (サブシステム管理)」ウィンドウの「Mappings (マッピング)」タブで、「Mappings (マッピング)」 > 「Show All Host Port Information (ホスト・ポート情報をすべて表示)」をクリックします。「Host Port Information (ホスト・ポート情報)」ウィンドウが開きます。
3. 欠陥のある HBA (取り外した HBA) の WWPN に一致する「Host Port Information (ホスト・ポート情報)」ウィンドウ内の項目を見つけ、その別名を記録します。その後、「Host Port Information (ホスト・ポート情報)」ウィンドウを閉じます。
4. 「Mappings (マッピング)」タブで、記録したばかりの HBA ホスト・ポートの別名を選択します。
5. 「Mappings (マッピング)」 > 「Replace Host Port (ホスト・ポートの置換)」をクリックします。「Replace Host Port (ホスト・ポートの置換)」ウィンドウが開きます。
6. 「Replace Host Port (ホスト・ポートの置換)」ウィンドウで、ウィンドウの上部にリストされている現在の HBA ホスト・ポート ID が、取り外した HBA の WWPN に一致することを検証します。
7. 置き換えの HBA の 16 桁からなる WWPN (コロン (:) は含まない) を「New Identifier (新しい ID)」フィールドに入力し、「OK」をクリックします。

上記の手順を完了した後、『HBA ホット・スワップ手順の完了』に進みます。

HBA ホット・スワップ手順の完了

HBA ホット・スワップ手順を完了させるには、このセクションに記載されている、AIX または Linux のいずれかの該当する手順を実行します。

AIX での HBA ホット・スワップ手順の完了

1. ファイバー・チャネル・ループバック・プラグを取り外し、取り外した HBA に前に接続していたファイバー・チャネル・ケーブルを差し込みます。

注: HBA をストレージ・サブシステムに直接接続している場合、またはファイバー・チャンネル・スイッチのゾーニングが WWPN でなくポート番号に基づいている場合は、以下のステップをスキップしてください。ゾーニングを変更する必要がある場合は、正しく変更できないと、HBA がストレージ・サブシステムにアクセスできなくなります。

2. HBA がファイバー・チャンネル・スイッチに接続されており、しかも、ゾーニングが WWPN に基づいている場合は、ゾーニング情報を変更し、以前の HBA の WWPN を置き換えの HBA の WWPN に置換します。
3. ファイバー・チャンネル・ループバック・プラグを取り外し、取り外した HBA に前に接続していたファイバー・チャンネル・ケーブルを差し込みます。

注: HBA をストレージ・サブシステムに直接接続している場合、またはファイバー・チャンネル・スイッチのゾーニングが WWPN でなくポート番号に基づいている場合は、以下のステップをスキップしてください。ゾーニングを変更する必要がある場合は、正しく変更できないと、HBA がストレージ・サブシステムにアクセスできなくなります。

4. HBA がファイバー・チャンネル・スイッチに接続されており、しかも、ゾーニングが WWPN に基づいている場合は、ゾーニング情報を変更し、以前の HBA の WWPN を置き換えの HBA の WWPN に置換します。
5. **cfgmgr** コマンドを実行して、HBA が WWPN をファイバー・チャンネル・スイッチに登録できるようにします。
6. 次のコマンドを入力し、交換した fcsX デバイスとそれに関連する dac が Available 状態にあることを検証します。

```
# lsdev -C |grep fcs
```

```
lsdev -C |grep dac
```

7. 次のコマンドを入力して、追加の dar が作成されておらず、予期した dar が Available 状態にあることを検証します。

注: MPIO では、dac デバイスが表示されるのは UTM LUN が割り当てられている場合のみです。

```
# lsdev -C |grep dar
```

重要: lsdev の出力に追加の dar が存在することは、構成に問題があることを示しています。これが起きた場合は、問題を訂正するまで、この手順を続行しないでください。そうしないと、データの可用性が失われる可能性があります。

8. それぞれの dar ごとに次のコマンドを入力し、影響を受けた dar 属性が 2 つのアクティブな dac の存在を示していることを検証します。

```
# lsattr -El darX|grep act_controller
```

ここで、X は dar の番号です。

出力は、次の例と同様になります。

```
lsattr -El dar0|grep act_controller
act_controller dac0,dac2 Active Controllers False
```

重要: 影響を受けたそれぞれの dar ごとに 2 つの dac が報告されない場合は、データの可用性が失われるおそれがあります。それぞれの dar ごとに dac が 2 つずつ報告されない場合は、この手順を続行しないでください。先へ進む前に、問題を訂正してください。

9. 優先パスへ手動でボリュームを再配分します。

10. 次のいずれか、または両方の方法によって、各ディスクが優先パス上に留まっていることを検証します。

AIX システムの使用

`mpio_get_config -Av` コマンドを実行し、ドライブが予期されるパス上にあることを検証します。

ストレージ・マネージャーの使用

「Enterprise Management (エンタープライズ管理)」ウィンドウで、ストレージ・サブシステムが「Optimal (最適)」状態であることを検証します。「Optimal (最適)」状態でない場合は、ホット・スワップ・プロセスに関与したサブシステムに属するドライブが、いずれも Recovery Guru にリストされていないことを検証します。

11. 必要に応じて、影響を受けた dar の autorecovery を使用可能に設定します。属性の設定値を変更する方法については、333 ページの『付録 D. AIX オブジェクト・データ・マネージャー (ODM) 属性の表示および設定』を参照してください。

これで、ファイバー・チャンネル HBA のホット・スワップが完了しました。

Linux での HBA ホット・スワップ手順の完了

1. ファイバー・チャンネル・ループバック・プラグを取り外し、取り外した HBA に前に接続していたファイバー・チャンネル・ケーブルを差し込みます。
2. HBA がファイバー・チャンネル・スイッチに接続されており、しかも ゾーニングが WWPN に基づいている場合は、ゾーニング情報を変更し、以前の HBA の WWPN を置き換えの HBA の WWPN に置換します。

注: HBA をストレージ・サブシステムに直接接続している場合、またはファイバー・チャンネル・スイッチのゾーニングが WWPN でなくポート番号に基づいている場合は、このステップをスキップしてください。ゾーニングを変更する必要がある場合は、正しく変更できないと、HBA がストレージ・サブシステムにアクセスできなくなります。

3. RDAC がインストールされている場合は、次のコマンドを入力して新しい HBA を認識します。

```
# mppBusRescan
```

これで、ファイバー・チャンネル HBA のホット・スワップが完了しました。

Windows DSM および Linux RDAC の設定

このトピックは、Windows オペレーティング・システムと Linux オペレーティング・システムの両方に適用されます。IBM ストレージ・マネージャーで提供されるフェイルオーバー・ドライブの構成設定は、ドライブを変更します。

- Linux の場合、構成設定は `/etc/mpp.conf` ファイルにあります。
- Windows の場合、構成設定は `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\<DSM_Driver>\Parameters` レジストリー・キー内にあります。ここで、<DSM_Driver> は OEM 固有のドライバーの名前です。

デフォルトのフェイルオーバー・ドライバーは、`mppdsm.sys` です。変更を有効にするには、ホストをリブートする必要があります。以下の表にリストされているデフォルト値は、Windows と Linux の両方のオペレーティング・システムに適用されます。Windows と Linux でデフォルト値が異なる場合は、そのことが明記されています。これらの値の多くは、Linux または Windows のフェイルオーバー・インストーラーによってオーバーライドされます。

重要: これらの設定を構成値から変更した場合、ストレージ・サブシステムへのアクセスが失われる可能性があります。

表 32. フェイルオーバー・ドライバーの構成パラメーター

パラメーター名	デフォルト値	説明
MaxPathsPerController	4	コントローラー当たりのサポートされるパス (論理エンドポイント) の最大数。ストレージ・サブシステムへのパスの総数は、MaxPathsPerController 値にコントローラーの数を乗算した値です。許容値は、Windows OS の場合は 0x1 (1) から 0x20 (32) までの範囲、Linux RDAC の場合は 0x1 (1) から 0xFF (255) までの範囲です。お客様サポート担当員および技術サポート担当員専用です。
ScanInterval	1 (Windows) 60 (Linux)	フェイルオーバー・ドライバーが以下の条件を検査する時間間隔 (秒単位)。 • LUN の優先所有権の変更 • LUN の優先パスへの再バランスの試行 • AVT 使用可能の状況または AVT 使用不可の状況の変更 Windows の場合、許容値は 0x1 から 0xFFFFFFFF までの範囲で、分単位で指定する必要があります。Linux の場合、許容値は 0x1 から 0xFFFFFFFF までの範囲で、秒単位で指定する必要があります。お客様サポート担当員および技術サポート担当員専用です。

表 32. フェイルオーバー・ドライバーの構成パラメーター (続き)

パラメーター名	デフォルト値	説明
ErrorLevel	3	この設定は、どのエラーをログに記録するかを決定します。以下の値が有効です。 • 0 – すべてのエラーを表示します • 1 – パス・フェイルオーバー・エラー、コントローラー・フェイルオーバー・エラー、再試行可能エラー、致命的エラー、および回復済みエラーを表示します • 2 – パス・フェイルオーバー・エラー、コントローラー・フェイルオーバー・エラー、再試行可能エラー、および致命的エラーを表示します • 3 – パス・フェイルオーバー・エラー、コントローラー・フェイルオーバー・エラー、および致命的エラーを表示します • 4 – コントローラー・フェイルオーバー・エラー、および致命的エラーを表示します お客様サポート担当員および技術サポート担当員専用です。
SelectionTimeoutRetryCount	0	パスが失敗する前に入出力要求の選択タイムアウトが再試行される回数。同一コントローラーへの別のパスが存在する場合、入出力が再試行されます。同一コントローラーへのパスが他に存在しない場合、フェイルオーバーが実行されます。代替コントローラーへの有効なパスが存在しない場合、入出力は失敗します。許容値は 0x0 から 0xFFFFFFFF までの範囲です。お客様サポート担当員および技術サポート担当員専用です。

表 32. フェイルオーバー・ドライバーの構成パラメーター (続き)

パラメーター名	デフォルト値	説明
CommandTimeoutRetryCount	1	バスが失敗する前に入出力要求のコマンド・タイムアウトが再試行される回数。同一コントローラーへの別のバスが存在する場合、入出力が再試行されます。同一コントローラーへの別のバスが存在しない場合、フェイルオーバーが実行されます。代替コントローラーへの有効なバスが存在しない場合、入出力は失敗します。許容値は、Windows の場合は 0x0 から 0xa (10) までの範囲、Linux RDAC の場合は 0x0 から 0xFFFFFFFF までの範囲です。お客様サポート担当員および技術サポート担当員専用です。
UaRetryCount	10	LUN からの装置アテンション (UA) 状況が再試行される回数。このパラメーターは、静止中 (Quiescence In Progress) による UA 状態には適用されません。許容値は、Windows OS の場合は 0x0 から 0x64 (100) までの範囲、Linux RDAC の場合は 0x0 から 0xFFFFFFFF までの範囲です。お客様サポート担当員および技術サポート担当員専用です。
SynchTimeout	120	フェイルオーバー・ドライバーによって内部で生成される同期入出力要求のタイムアウト (秒単位)。内部要求の例には、再バランス、バス検証、およびフェイルオーバー・コマンドの発行に関連した要求が含まれます。許容値は 0x1 から 0xFFFFFFFF までの範囲です。お客様サポート担当員および技術サポート担当員専用です。

表 32. フェイルオーバー・ドライバーの構成パラメーター (続き)

パラメーター名	デフォルト値	説明
DisableLunRebalance	0	このパラメーターは、LUN を再バランスして優先パスに戻すという LUN フェイルバック動作に対する制御を提供します。以下の値を指定できます。 • 0 – LUN 再バランスを、AVT モードと非 AVT モードの両方に対して使用可能にします。 • 1 – LUN 再バランスを、AVT モードに対して使用不可にし、非 AVT モードに対して使用可能にします。 • 2 – LUN 再バランスを、AVT モードに対して使用可能にし、非 AVT モードに対して使用不可にします。 • 3 – LUN 再バランスを、AVT モードと非 AVT モードの両方に対して使用不可にします。 • 4 – AVT モードがオフで、ClassicModeFailover が LUN レベル 1 に設定されている場合、選択 LUN 転送機能を使用可能にします。
S2ToS3Key	固有キー	この値は、フェイルオーバー・ドライバーのインストール中に生成される SCSI-3 予約キーです。お客様サポート担当員および技術サポート担当員専用です。
LoadBalancePolicy	1	このパラメーターは、Windows DSM および Linux RDAC のフェイルオーバー・ドライバーによって管理されるすべての論理ドライブで使用されるロード・バランシング・ポリシーを決定します。以下の値が有効です。 • 0 – サブセット付きラウンドロビン。 • 1 – サブセット付き最小キュー項目数。 • 2 – サブセット付き最小パス重み (Windows のみ)

表 32. フェイルオーバー・ドライバーの構成パラメーター (続き)

パラメーター名	デフォルト値	説明
ClassicModeFailover	0	このパラメーターは、DSM によるフェイルオーバー状態の処理方法に対する制御を提供します。以下の値が有効です。 • 0 – コントローラー・レベルのフェイルオーバーを実行します (すべての LUN が代替コントローラーに移動されます)。 • 1 – LUN レベルのフェイルオーバーを実行します (エラーを示している LUN のみが代替コントローラーに移動されます)。
SelectiveTransferMaxTransferAttempts	3	このパラメーターは、選択 LUN 転送モードが使用可能になっている場合、ホストが LUN の所有権を代替コントローラーに移転する最大回数を設定します。この設定は、複数のホストが絶えずコントローラー間で LUN を転送するのを防止します。
SelectiveTransferMinIOWaitTime	5	このパラメーターは、選択 LUN 転送モードが使用可能になっている場合、DSM が LUN を代替コントローラーに転送する前に待つ最小待ち時間 (秒単位) を設定します。このパラメーターは、偶発的なリンク・エラーによる過度の LUN 転送を制限するために使用されます。

待ち時間の設定

フェイルオーバー・ドライバーは、初めて入出力要求を受け取ったときに、その要求のタイム・スタンプ情報をログに記録します。要求がエラーを返し、フェイルオーバー・ドライバーがその要求を再試行することに決定した場合、現在時刻が元のタイム・スタンプ情報と比較されます。エラーおよび経過時間の長さに応じて、要求は LUN を現在所有しているコントローラーに対して再試行されるか、あるいはフェイルオーバーが実行されて要求が代替コントローラーに送信されます。このプロセスは、待ち時間と呼ばれます。NotReadyWaitTime 値、BusyWaitTime 値、および QuiescenceWaitTime 値が、ControllerIoWaitTime 値より大きい場合、それらの値は無効です。

表 33. 待ち時間設定のパラメーター

パラメーター名	デフォルト値	説明
NotReadyWaitTime	300 (Windows)、270 (Linux)	フェイルオーバーが実行される前の作動不能 (Not Ready) 状態 (SK 0x06、ASC/ASCQ 0x04/0x01) が許容される時間 (秒単位)。有効な値は 0x1 から 0xFFFFFFFF までの範囲です。

表 33. 待ち時間設定のパラメーター (続き)

パラメーター名	デフォルト値	説明
BusyWaitTime	600 (Windows) 270 (Linux)	フェイルオーバーが実行される前の使用中 (Busy) 状態が許容される時間 (秒単位)。有効な値は 0x1 から 0xFFFFFFFF までの範囲です。
QuiescenceWaitTime	600 (Windows) 270 (Linux)	フェイルオーバーが実行される前の静止 (Quiescence) 状態が許容される時間 (秒単位)。有効な値は 0x1 から 0xFFFFFFFF までの範囲です。
ControllerIoWaitTime	600 (Windows) 120 (Linux)	フェイルオーバーが実行される前の再試行状況に関係なく、コントローラー上で入出力が再試行される時間の上限 (秒単位) を指定します。代替コントローラー上でこの制限を超えると、入出力は元のコントローラー上で再試行されます。ArrayIoWaitTime 制限の値に達するまで、このプロセスが続行されます。有効な値は 0x1 から 0xFFFFFFFF までの範囲です。
ArrayIoWaitTime	600	どのコントローラーで要求が試行されるかに関係なく、ストレージ・サブシステムに対して入出力が再試行される時間の上限 (秒単位) を指定します。この制限を超えると、入出力は障害状態で返されます。有効な値は 0x1 から 0xFFFFFFFF までの範囲です。

バス輻輳検出およびオンライン/オフライン・バス状態の設定の構成

以下の構成設定は、ユーティリティ `dsmUtil -o` オプション・パラメーターを使用して適用されます。

表 34. バス輻輳検出の構成設定

パラメーター	デフォルト値	説明
CongestionDetectionEnabled	0x0	バス輻輳 (ふくそう) 検出が使用可能であるかどうかを示すブール値。このパラメーターが定義されていないか、0x0 に設定されている場合、値は false であり、バス輻輳機能は使用不可で、他のパラメーターはすべて無視されます。0x1 に設定されている場合、バス輻輳機能は使用可能です。有効な値は 0x0 または 0x1 です。

表 34. パス輻輳検出の構成設定 (続き)

パラメーター	デフォルト値	説明
CongestionResponseTime	0x0	CongestionIoCount が 0x0 であるか、定義されていない場合、このパラメーターは、入出力要求に許容される平均応答時間 (秒単位) を表します。CongestionIoCount パラメーターの値がゼロ以外の場合、このパラメーターは、入出力要求に許容される絶対時間を示します。有効な値は 0x1 から 0x10000 (約 18 時間) までの範囲です。
CongestionIoCount	0x0	CongestionTimeFrame パラメーターの値の範囲内で CongestionResponseTime パラメーターの値を超過した入出力要求の数。有効な値は、0x0 から 0x10000 (約 4000 個の要求) までの範囲です。
CongestionTimeFrame	0x0	秒単位で評価される時間枠を定義するスライディング・ウィンドウ。このパラメーターが定義されていないか、0x0 に設定されている場合、時間フレームが定義されていないため、パス輻輳機能は使用不可になります。有効な値は 0x1 から 0x1C20 (約 2 時間) までの範囲です。
CongestionSamplingInterval	0x0	n 番目の要求が平均応答時間の計算に使用される前にパスに送信される必要がある入出力要求の数。例えば、このパラメーターが 100 に設定されている場合、パスに送信された 100 番目ごとの要求が、平均応答時間の計算に使用されます。このパラメーターが 0x0 に設定されているか、定義されていない場合、すべての入出力要求で計算が行われることになり、パフォーマンス上の理由でパス輻輳機能は使用不可になります。有効な値は 0x1 から 0xFFFFFFFF (約 40 億個の要求) までの範囲です。
CongestionMinPopulationSize	0x0	平均応答時間が計算される前に収集される必要があるサンプル入出力要求の数。有効な値は 0x1 から 0xFFFFFFFF (約 40 億個の要求) までの範囲です。

表 34. パス輻輳検出の構成設定 (続き)

パラメーター	デフォルト値	説明
CongestionTakeLastPathOffline	0x0	輻輳しきい値を超過した場合に、DSM ドライバーがストレージ・サブシステムへの使用可能な最後のパスをオフラインにするかどうかを示すブール値。このパラメーターが定義されていないか、0x0 に設定されている場合、値は false です。有効な値は 0x0 または 0x1 です。 注: この値の設定に関係なく、dsmUtil ユーティリティでのパス・オフラインの設定は成功します。

パス輻輳検出機能の構成設定の例

以下のセクションに、概念の簡単な例を示します。

注: パス輻輳検出を使用可能にする前に、CongestionResponseTime、CongestionTimeFrame、および CongestionSamplingInterval の各パラメーターを有効な値に設定する必要があります。

パス輻輳入出力応答時間を 10 秒に設定するには、dsmUtil -o CongestionResponseTime=10,SaveSettings と指定します。

パス輻輳サンプリング間隔を 1 分に設定するには、dsmUtil -o CongestionSamplingInterval=60 と指定します。

パス輻輳検出を使用可能にするには、dsmUtil -o CongestionDetectionEnabled=0x1,SaveSettings と指定します。

dsmUtil -o コマンドを使用して、管理者へのパスをオフラインに設定するには、dsmUtil -o SetPathOffline=0x77070001 と指定します。

dsmUtil -o コマンドを使用して、パスをオンラインに設定するには、dsmUtil -o SetPathOnline=0x77070001 と指定します。

注: パス ID (この例では、0x77070001) は、dsmUtil -g コマンドを使用して検索します。

T10PI をサポートするための DS5000 ストレージ・システムおよび AIX ホストのセットアップの詳細

AIX ホストから DS5000 ストレージ・サブシステム内のドライブに T10PI 機能をサポートするには、以下の手順を使用して、ご使用の DS5000 ストレージ・システムおよび AIX ホストをセットアップする必要があります。

DS5K ストレージ・ボックスのセットアップ

1. T10PI をサポートするファームウェアを使用して DS5000 ストレージ・システムをアップグレードします。
2. T10PI をサポートする論理装置番号 (LUN) を作成し、エクスポートします。

注: このステップを実行するには、T10PI をサポートするディスクを持っている必要があります。これらのディスクは通常、520 バイトのブロックに事前に初期化されています。詳しくは、67 ページの『T10PI 対応ドライブ属性』を参照してください。

AIX ホストのセットアップ

注: SSIC を使用して、すべての適用可能パッチとともに、サポートされる HBA、HBA ドライバーおよびファームウェア・バージョン、およびご使用の AIX オペレーティング・システムのバージョンをチェックする必要があります。

1. AIX 61 TL6 SP5 または AIX 71 TL0 SP3 をインストールします。AIX マシンは、T10PI をサポートする最新のファームウェアのある最低 1 つの 8Gb PCIe FC アダプター (フィーチャー・コード 5735 または 5273) を備えている必要があります。これは、少なくともバージョン df1000f114108a03.200305 を持っている必要があります。8Gb PCIe FC アダプター (フィーチャー・コード 5735 または 5273) ファームウェアをダウンロードするのに AIX 診断ユーティリティを使用することができます。
 - 2 ポート 8Gb PCIe ファイバー・チャネル・アダプターを使用する必要があります。
 - ファームウェアの 200307 レベルまたはそれ以上のレベルが必要とされます。
 - フィーチャー・コード 5735 またはロー・プロファイル・フィーチャー・コード 5273 が必要です。
 - Power Blade についてのサポートはありません。
 - アダプター・ファームウェアをダウンロードするには、**diag -T download -d fcs#** コマンド (ここで、# は fcs 装置番号) を使用します。
 - Coho アダプター上の現行のファームウェア・バージョンを検索するには、**lsmcode -cd fcs#** または **lscfg -vl fcs#** コマンドを使用します。
2. 8Gb PCIe FC アダプター (フィーチャー・コード 5735 または 5273) (fcs デバイスの DIF 使用可能属性) での保護を使用可能にします。
 - FC アダプターでの保護を使用可能にするには、**chdev -l fcs# -a DIF_enabled=yes** コマンドを使用することができます。
 - fcs# での保護を使用可能/使用不可にするには、**smit fcsa** コマンドを使用することもできます。

注: FC アダプターでの保護を使用不可にするには、**chdev -l fcs# -a DIF_enabled=no** を使用します。

3. ステップ 1 で指定されているようにファームウェアを更新し、ディスクのパスの開始個所であるすべての 8Gb PCIe FC アダプター (フィーチャー・コード 5735 または 5273) でステップ 2 を実行することを確認します。
 - a. ディスクのパスで FC アダプターを検出するのに **lspath -l hdisk#** コマンドを使用します。これは、fscsi# デバイス (FC プロトコル・デバイス) を示します。
 - b. fscsi# デバイスの親を検出するのに、**lsdev -l fscsi# -F'name parent'** コマンドを使用します。
 - c. 保護を使用可能にします。
4. ディスク上で T10 保護を使用可能にするのに、**chdev -l hdisk# -a DIF_protection=yes** コマンドを使用します。ディスクは、「タイプ 1」T10 保護をサポートする必要があります。

注: hdisk# 上で保護を使用可能/使用不可にするのに、**smit disk** コマンドを使用することもできます。

注: ディスク上で T10 保護を使用不可にするのに **chdev -l hdisk# -a DIF_protection=no** コマンドを使用することができます。

5. 保護を使用可能にした後、**lsattr -El hdisk#** コマンドを使用してこの属性の現行値をチェックします。少なくとも 1 つのパスが保護をサポートしていない場合、ディスク上で保護を使用可能にすることはできません。この属性が「サポートされない」という値を持っている場合、それは以下のことを意味しています。

- ディスクへのいくつかのパスまたはすべてのパスが保護をサポートしないか、あるいは
- ディスクが保護をサポートしない

hdisk2 には 3 つのパスがあります。これらの 3 つのパスは、fcs0、fcs2 おび fcs3 からのものです。これら 3 つのアダプター上の保護を使用可能にしようとしています。それを行うには、以下のことを行います。

1. 上述のすべての fcs デバイス上のファームウェアをアップグレードします。それらはすべて 8Gb PCIe FC アダプター (フィーチャー・コード 5735 または 5273) でなければなりません。
2. 子デバイス (fscsi0、fscsi2 および fscsi3) を構成解除します。
3. **chdev** コマンド (**chdev -l fcs0 -a DIF_enabled=yes**) を使用して、fcs0、fcs2 および fcs3 アダプター上の保護を使用可能にします。
4. すべてのデバイスが使用可能な状態になるように、**cfgmgr** を実行します。
5. hdisk2 上で **chdev** コマンドを使用して、保護を使用可能または使用不可にします (**chdev -l hdisk2 -a DIF_protection=yes**)。ディスクが保護をサポートし、すべてのパスが保護をサポートする場合には、属性値は「はい」に設定されます。そうでない場合には、属性値は「サポートされない」に設定されます。

注: 属性値が「サポートされない」に設定された場合には、すべてのパス (すべての fcs アダプター属性) をチェックし、DS5000 ストレージ上で LUN が作成されたときに LUN 上で保護が使用可能にされたかどうかをチェックします。場合によっては、fcs アダプター上の属性は「はい」を示すが、T10 保護 (BlockGuard フィーチャー) をサポートしない古い 8Gb PCIe FC アダプター (フィーチャー・コード 5735 または 5273) ファームウェアが原因で、それがサポートされないことがあります。

第 6 章 フル・ディスク暗号化の処理

この章では、フル・ディスク暗号化 (FDE) ディスク・ドライブの機能および利点と、FDE ディスクを装備した FDE 互換ストレージ・サブシステムでセキュリティーを実装する方法について説明します。

この章の情報に加えて、「*IBM Full Disk Encryption Best Practices*」資料で、FDE ドライブを装備したストレージ・サブシステムでセキュリティーを維持するためのベスト・プラクティスについて説明しています。この資料にアクセスするには、<http://www-947.ibm.com/support/entry/portal/docdisplay?lnodocid=MIGR-5081492&brandind=5000028> にアクセスするか、以下の手順を実行します。

1. IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) にアクセスします。
2. Web ページの下部にある「**Search within all of support & downloads (サポート & ダウンロードの全体を検索)**」フィールドに「FDE」と入力して、Enter キーを押します。
3. 検索結果のリストで、「**IBM Full Disk Encryption Best Practices - IBM System Storage (IBM フル・ディスク暗号化ベスト・プラクティス - IBM System Storage)**」リンクをクリックします。
4. PDF ファイルへのリンクをクリックして、「*IBM Full Disk Encryption Best Practices (IBM フル・ディスク暗号化ベスト・プラクティス)*」資料を開くか、ダウンロードします。

注: ディスク・プールに FDE ディスクがある場合は、ディスク・プールもセキュアにすることができません。240 ページの『RAID アレイのセキュア化』を参照してください。手順は完全に同じです。

注: このセクションに記載するスクリーン・ショットは説明のみを目的としており、ストレージ・マネージャーおよびコントローラー・ファームウェアのバージョンによっては、実際の UI と異なる場合があります。

この章では、以下のトピックが扱われています。

- 206 ページの『フル・ディスク暗号化』
 1. 206 ページの『侵害に対するデータの保護』
 2. 207 ページの『ローカル・セキュリティー・キー管理または外部セキュリティー・キー管理の選択』
 3. 224 ページの『開始する前に』
 4. 208 ページの『セキュリティー・キーの使用』
 5. 220 ページの『セキュア消去の使用』
 6. 221 ページの『FDE セキュリティー許可』
 7. 223 ページの『FDE の用語』
- 224 ページの『DS TKLM プロキシ・コード・サーバーのインストールおよび構成』
 1. 226 ページの『DS TKLM プロキシ・コード・サーバーの構成ファイルの変更』
 2. 229 ページの『DS TKLM プロキシ・コードのインストール』
- 231 ページの『FDE ドライブを使用したディスク暗号化の構成』
 1. 231 ページの『FDE ドライブの取り付け』
 2. 232 ページの『プレミアム・フィーチャーの使用可能化』
 3. 240 ページの『RAID アレイのセキュア化』
 4. 246 ページの『ディスク・ドライブのアンロック』

5. 249 ページの『FDE ドライブを使用するストレージ・サブシステムのマイグレーション (ヘッド・スワップ)』
 6. 253 ページの『ディスク・ドライブの消去』
 7. 256 ページの『グローバル・ホット・スペア・ディスク・ドライブ』
 8. 257 ページの『ログ・ファイル』
- 258 ページの『よくある質問』

注: すべての IBM DS ストレージ・サブシステムが FDE をサポートするわけではありません。FDE の互換性について詳しくは、ご使用のストレージ・サブシステムに付属の資料を参照してください。

フル・ディスク暗号化

このセクションの情報では、FDE の動作方法の概要を示します。この章の後続のセクションでは、内部セキュリティ・キー管理および外部セキュリティ・キー管理を使用してディスク暗号化を構成する方法について説明します。

フル・ディスク暗号化 (FDE) を使用すると、FDE ドライブが所有者の制御下でないときにデータが脅威から保護されます。FDE ドライブは、データ・センター内またはネットワーク上で発生する脅威からはデータを保護しません。アタッカーがサーバーへのアクセス権を取得し、アンロックされたドライブにアクセスできる場合、アタッカーはドライブから平文を読み取ることができます。ドライブ・レベルの暗号化テクノロジーは、データ・センターのアクセス制御の代替ではなく、補完するためのものであることを忘れないでください。

フル・ディスク暗号化 (FDE) ディスク・ドライブによって、保管データのセキュリティぜい弱性を削減することができます。Trusted Storage Group (TCG) エンタープライズ・セキュリティ・サブシステム・クラスの規格を順守した FDE ディスク・ドライブは、National Security Agency (国家安全保障局) が認定しており、政府クラスの暗号化によるセキュリティを提供します。

注: 単一のセキュリティ実装では、すべての脅威からすべてのレベルのデータを効果的に保護することはできません。

ハード・ディスクに保管されたデータを異なる脅威から保護するためには、異なるテクノロジーが必要です。FDE ドライブは、以下の方法によって保管データのセキュリティを保護します。

侵害に対するデータの保護

不正なユーザーが暗号化されたデータを含むディスク・ドライブの所有権を取得した場合、あるいはドライブがデータ・センターから取り外されたり、電源がオフにされた場合、データは保護されます。

セキュア消去の使用

セキュアな消去は、再利用あるいは処分する予定のドライブ上のデータを高速に、永久的に消去します。

侵害に対するデータの保護

フル・ディスク暗号化テクノロジーを備えたドライブは、セキュリティ対応です。各 FDE ドライブは、セキュリティ対応 (セキュリティ無効) 状態で出荷されます。この状態では、FDE ドライブは非 FDE ドライブと同じように動作します。この状態のドライブに保管されたデータは、ドライブがストレージ・サブシステムから取り外された場合には保護されません。このドライブは、セキュリティ・キー・ファイルによってアンロックすることなく、1 つのストレージ・サブシステムから他のストレージ・サブシステムに移動させることができます。また、非暗号化 (非 FDE) のディスクで構成された RAID アレイの一部とし

て使用することもできます。ただし、セキュリティ対応 FDE と非 FDE ドライブによって構成された RAID アレイは、後でセキュア RAID アレイに変換することはできず、ストレージ・サブシステムから取り外された場合は FDE ドライブ上のデータは非セキュア状態で残されます。

IBM ストレージ・サブシステム・コントローラーは、FDE ドライブのみで構成されている RAID アレイ内のすべての FDE ドライブに、セキュリティを適用することができます。ご使用のセキュリティ・キー管理方式 (ローカルまたは外部) に応じて、コントローラー・ファームウェアは、セキュリティ・キーを作成するか、外部キー・マネージャー (IBM Tivoli Key Lifecycle Manager ソフトウェアなど) からセキュリティ・キーを取得します。ファームウェアは、セキュリティ・キーを用意した後、ドライブの暗号化機能を活動化します。これによって、各 FDE ディスク・ドライブは、ディスクに組み込むランダムな暗号鍵を生成します。

セキュリティが有効な場合、FDE ドライブは書き込み操作および読み取り操作のためにフル・ディスク暗号化を自動的に実行します。書き込み操作が実行されると、平文がディスクに入り、ディスク暗号鍵を使用して暗号化されてからメディアに書き込まれます。読み取り操作が実行されると、メディアから読み取られた暗号化されたデータは暗号化解除されてから、ドライブから取り出されます。

通常の運用中には、FDE ドライブがセキュリティ対応状態あるいはセキュリティ有効状態のいずれであっても、ストレージ・サブシステムには非暗号化ディスクと同様に動作します。セキュリティ有効 FDE ドライブは、常にデータを暗号化しています。ディスク暗号化は、誤ってオフにされることはありません。ディスク暗号鍵はドライブ自身によって生成され、ディスク上に保管され、ディスクから出ることはなく、そのドライブのみに固有です。セキュリティが絶対に暗号漏えいすることがないように、暗号化された暗号鍵はそのディスク・ドライブのみに保管されます。ディスク暗号鍵がディスクから出ることはないため、オペレーティング・システムのパスワードを定期的に変更するように暗号鍵を定期的に変更する必要はありません。

ローカル・セキュリティ・キー管理または外部セキュリティ・キー管理の選択

ストレージ・サブシステムのセキュリティ・キーを管理するには、ローカル・セキュリティ・キー管理と外部セキュリティ・キー管理の 2 つの方式があります。

ローカル・セキュリティ・キー管理

ローカル・セキュリティ・キー管理では、セキュリティ・キーは、ストレージ・サブシステム・コントローラー内部に作成および収容されます。ローカル・セキュリティ・キー管理には、別のソフトウェアは必要ありません。セキュア・ドライブをストレージ・サブシステム間で移動するには、元のストレージ・サブシステムに保存したセキュリティ・キー・ファイルを使用してドライブをアンロックする必要があります。

ローカル・セキュリティ・キー管理を使用可能にするには、以下の作業を実行します。

1. FDE プレミアム・フィーチャーの Web 上の活動化手順に従います。
2. ストレージ・マネージャーを使用して、ストレージ・サブシステム・コントローラーに対してセキュリティ・キーを作成するためのコマンドを出します。

外部セキュリティ・キー管理

外部セキュリティ・キー管理では、ストレージ・サブシステム・コントローラーによって作成されたセキュリティ・キーを使用する代わりに、ネットワーク上のセントラル・キー・ロケーションを使用してさまざまなストレージ・サブシステム用のキーを管理します。外部セキュリティ・キー管理は、IBM Tivoli

Key Lifecycle Manager (TKLM) などの外部キー・ライセンス・マネージャー・ソフトウェアによって容易に行うことができます。このソフトウェアがまだない場合は、ソフトウェアを購入してインストールし、プロキシ・サーバーを構成する必要があります。

外部セキュリティ・キー管理では、コントローラーが外部セキュリティ・キー管理ソースからセキュリティ・キーを取得します。その後、このキーは、ストレージ・サブシステムの電源がオンになっている間、将来の使用のためにコントローラーの揮発性メモリーで難読化されます。ストレージ・サブシステムの電源がオフになると、このキーは揮発性メモリーから消去されます。キーがストレージ・サブシステム内に保管されないため、ストレージ・サブシステムが正常にブートするには、構成内に非 FDE ドライブが必要です。ストレージ・サブシステムは、FDE ドライブをアンロックするために、外部キー管理サーバーからのセキュリティ・キーを要求します。

この方式は、一貫性のある共通のキー管理インターフェースを提供します。外部キー・ライセンス・マネージャー・ソフトウェアは、セキュア・テープ・ドライブなどの他のストレージ・ハードウェア用のセキュリティ・キーも管理します。セキュア・ドライブを 1 つのストレージ・サブシステムから 2 台目のストレージ・サブシステムに移動するために、保存したセキュリティ・キー・ファイルにアクセスする必要はありません。ドライブの挿入時に 2 台目のストレージ・サブシステムがキー・ライセンス・マネージャーに接続されている場合、外部キー・ライセンス・マネージャー・ソフトウェアが、ドライブを自動的にアンロックするセキュリティ・キーを提供します。

外部セキュリティ・キー管理を使用可能にするには、以下の作業を実行します。

1. 外部キー・ライセンス・マネージャー・ソフトウェアをインストールおよび構成します。詳しくは、ソフトウェアに付属の資料を参照してください。
2. DS TKLM プロキシ・コードをインストールおよび構成します。
3. 外部キー要求を受け取るように外部キー管理ソフトウェアを構成します。
4. ローカル・セキュリティ・キーを生成するのではなく、ストレージ・マネージャーを使用して、ストレージ・サブシステム・コントローラーに対して外部キー・ライセンス・マネージャーからのセキュリティ・キーを要求するためのコマンドを出します。
5. 外部キー要求を受け取るように外部キー・ライセンス・マネージャー・ソフトウェアを構成します。

重要:

1. Tivoli Key Lifecycle Manager は、IBM DS ストレージ・サブシステムでサポートされている唯一の外部セキュリティ・キー管理ソフトウェアです。
2. 外部セキュリティ・キー管理を使用する場合、少なくとも 1 つの非 FDE ドライブがストレージ・サブシステムに取り付けられていることを確認してください。そうでないと、ストレージ・サブシステムの電源がオフになってから、再びオンになった場合、ストレージ・サブシステムは、セキュア FDE ドライブをアンロックしてブート・プロセスを完了するために、保存されたファイルから手動でセキュリティ・キーを提供するよう要求することがあります。

セキュリティ・キーの使用

フル・ディスク暗号化を使用すると、ドライブをセキュアにするプロセスではストレージ・サブシステムのセキュリティを使用可能にし、次にデータが保管されているセキュリティ対応の特定の RAID アレイをセキュアにします。

セキュリティ・キーを生成するプロセスは、使用しているセキュリティ・キー管理方式のタイプによって異なります。ストレージ・サブシステムのセキュリティの使用可能化のプロセスは、後日セキュリティ・キーの変更やキー管理方式の変更を行うのでなければ、一度だけ行えばよいものです。各 FDE ドライブが固有の暗号鍵を持っている場合でも、個々のドライブごとに個別のセキュリティ・キーは必要ありま

せん。ストレージ・サブシステムのセキュリティーを使用可能にするには、FDE ドライブ・オプションおよび IBM DS ディスク暗号化プレミアム・フィーチャーを購入し、プレミアム・フィーチャー・キー・ライセンス・キットに付属の手順を使用して、ストレージ・サブシステムでフィーチャーを使用可能にする必要があります。

セキュリティー・キーがコントローラーによって作成された後、あるいは外部キー管理ソフトウェアから取得された後、暗号化されたバージョンのセキュリティー・キーはストレージ・サブシステム内で難読化され、直接的に表示できなくなります。

ストレージ・サブシステムでセキュリティー・キーを作成した後、暗号化されたバージョンのセキュリティー・キーを、指定した場所にあるバックアップ・セキュリティー・キー・ファイルに保存するよう求められます。必ず、セキュリティー・キー・ファイルおよびファイルに関連付けられているパスフレーズを保護してください。指定した保存場所に加えて、ストレージ・マネージャーもファイルのコピーをデフォルトの場所に保存しています。これは Microsoft Windows 環境では `...¥IBM_DS¥client¥data¥securityLockKey`、AIX、Linux、Solaris、および HP-UX 環境では `/var/opt/SM/securityLockkey` です。

ローカル・セキュリティー・キー管理方式では、セキュリティー・キー ID およびパスフレーズのプロンプトが出されます。セキュリティー・キーが関連付けられているストレージ・サブシステムを識別できるように、このセキュリティー・キー ID はストレージ・サブシステムのワールドワイド ID に追加されます。外部セキュリティー・キー管理方式では、パスフレーズのみのプロンプトが出されます。コントローラーは、ストレージ・サブシステムのワールドワイド ID を使用して、セキュリティー・キー・ファイルが関連付けられているストレージ・サブシステムを識別します。

セキュリティー・キー・ファイルには、暗号化されたセキュリティー・キーとセキュリティー・キー ID が含まれます。セキュリティー・キーの保存操作中にパスフレーズを指定する必要があります。パスフレーズは、ストレージ・サブシステムあるいはセキュリティー・キー・ファイルには保管されません。コントローラーは、パスフレーズを使用してセキュリティー・キーを暗号化してから、セキュリティー・キーをセキュリティー・キー・ファイルにエクスポートします。セキュリティー・キー ID はセキュリティー・キー・ファイルに保管されるため、そのセキュリティー・キー・ファイルが関連付けられているストレージ・サブシステムを識別することができます。必ず、セキュリティー・キー・ファイルおよびファイルに関連付けられているパスフレーズを保護してください。これらの 2 つの情報を使用すると、セキュア FDE ドライブをアンロックできるためです。

セキュリティー・キー・ファイル内のセキュリティー・キーを暗号化解除するには、セキュリティー・キー・ファイルの生成時に入力したものと同一パスフレーズを入力する必要があります。次にドライブは、そのセキュリティー・キーとストレージ・サブシステムが提供したセキュリティー・キーが同一であるかを判別します。それらのセキュリティー・キーが同一であった場合は、セキュリティー有効 FDE ドライブに対してデータの読み取りおよび書き込みが可能です。

重要: パスフレーズは、セキュリティー・キー・ファイル内のセキュリティー・キーを保護するためにのみ使用されます。「Subsystem Management (サブシステム管理)」ウィンドウにアクセスできる人であれば誰でも、新しいパスフレーズを使用してセキュリティー・キー・ファイルのコピーを保存することができます。セキュリティー・キーの作成および変更を含めたあらゆる構成変更の際にパスワードを指定する必要があります。ストレージ・サブシステムごとに、ストレージ・サブシステム・パスワードを設定します。ストレージ・サブシステム・パスワードの設定の手順については、39 ページの『ストレージ・サブシステムの管理パスワードの設定』を参照してください。

ローカル・セキュリティー・キー管理を使用する場合、セキュリティー・キー・ファイルは、破損したセキュリティー・キーあるいはストレージ・サブシステムの両方のコントローラーの障害に対して保護を提供します。セキュリティー・キー・ファイルは、セキュリティー有効 FDE ドライブが 1 つのストレージ・サ

ブシステムから別のストレージ・サブシステムに移動された場合に、そのドライブをアンロックするためにも必要です。これらの場合、セキュリティ・キー・ファイルに保管されているセキュリティ・キーによってドライブがアンロックされるまで、セキュリティ有効 FDE ドライブはロックされたままです。セキュリティ・キー・ファイル内のセキュリティ・キーを暗号化解除するには、セキュリティ・キー・ファイルの生成時に入力したものと同一パスフレーズを入力する必要があります。次にドライブは、そのセキュリティ・キーとストレージ・サブシステムが提供したセキュリティ・キーが同一であることを判別します。それらのセキュリティ・キーが同一であった場合は、セキュリティ有効 FDE ドライブに対してデータの読み取りおよび書き込みが可能です。

外部セキュリティ・キー管理を使用する場合、セキュリティ・キー・ファイルは以下の状況に対する保護を提供します。

1. コントローラーがセキュア FDE ドライブをアンロックするときにプロキシ・サーバーまたは外部キー・ライセンス・サーバーへの通信が失われた場合
2. セキュア FDE ドライブが、同じ外部キー・ライセンス・マネージャーによって管理されていないストレージ・サブシステムとの間で移動された場合
3. 構成内にセキュア FDE ドライブのみがあり、非セキュア FDE ドライブまたは非 FDE ドライブがないストレージ・サブシステム構成の電源再投入後にドライブをアンロックする必要がある場合

ストレージ・サブシステム・コントローラーがセキュリティ・キーを作成した後、RAID アレイを「Security Capable (セキュリティ対応)」状態から「Security Enabled (セキュリティ有効)」状態に変更することができます。「Security Enabled (セキュリティ有効)」状態では、ドライブの電源がオンになった後で、そのドライブに保管されたデータにアクセスするためのセキュリティ・キーを使用して、RAID アレイ FDE ドライブがアンロックされている必要があります。RAID アレイ内のドライブに電源が投入されると必ず、ドライブはすべて「Security Locked (セキュリティ・ロック)」状態になります。これらのドライブは、ドライブの初期化中のみ、ストレージ・サブシステムのセキュリティ・キーを使用してアンロックされます。「Security Unlocked (セキュリティ・アンロック)」状態では、ドライブは読み取りおよび書き込みアクティビティについてアクセス可能になります。ドライブがアンロックされると、ドライブの電源がオフにされるか、ドライブがドライブ・ベイから取り外されて再挿入されるか、あるいはストレージ・サブシステムの電源サイクルが行われるまでは、そのドライブはアンロックされた状態のままです。

ドライブがセキュア状態になると、電源がオフにされるか電源が取り外された場合、ドライブはロック状態になります。ドライブをコントローラーによってアンロックされるまで読み取り不能にすることで、そのドライブ内の暗号鍵によってデータが暗号化あるいは暗号化解除されることはありません。

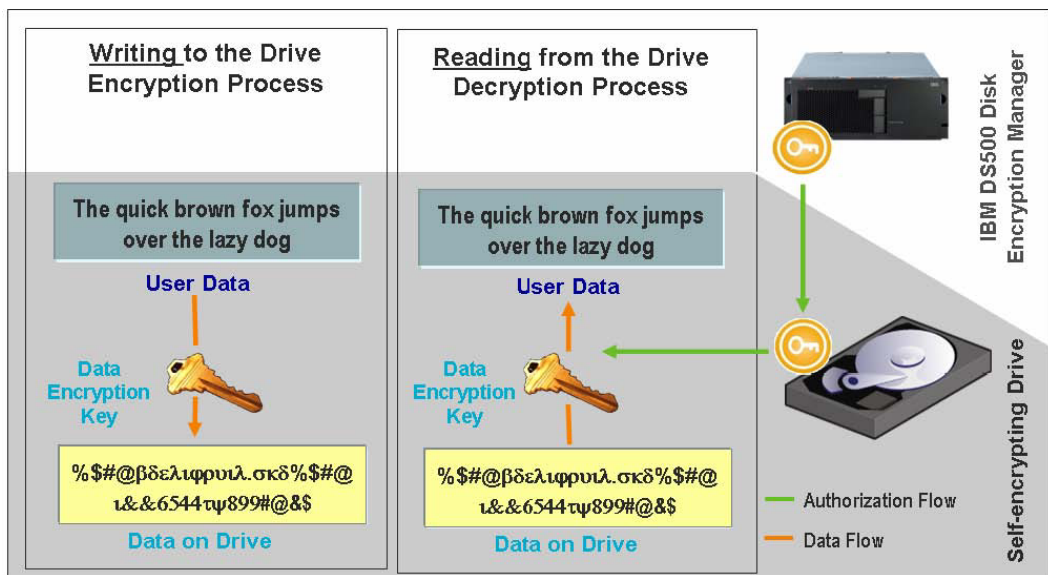


図 25. セキュリティ有効 FDE ドライブ: 適切な正しい権限によって、アンロック状態でのデータの読み取りおよび書き込みが発生します。

認証が設定されてストレージ・サブシステム上でセキュリティが有効になると、FDE ドライブ内部で行われる書き込み操作の暗号化および読み取り操作の暗号化解除は、ユーザーあるいはストレージ・サブシステム・コントローラーからは認識できません。ただし、セキュアなドライブが脱落、取り外し、あるいは盗まれた場合は、ドライブはロック状態になり、そのディスクに保管されているデータは暗号化された読み取り不能状態のまま維持されます。許可されていないユーザーはセキュリティ・キー・ファイルおよびパズルフレーズを所有していないため、保管されたデータにアクセスすることはできません。

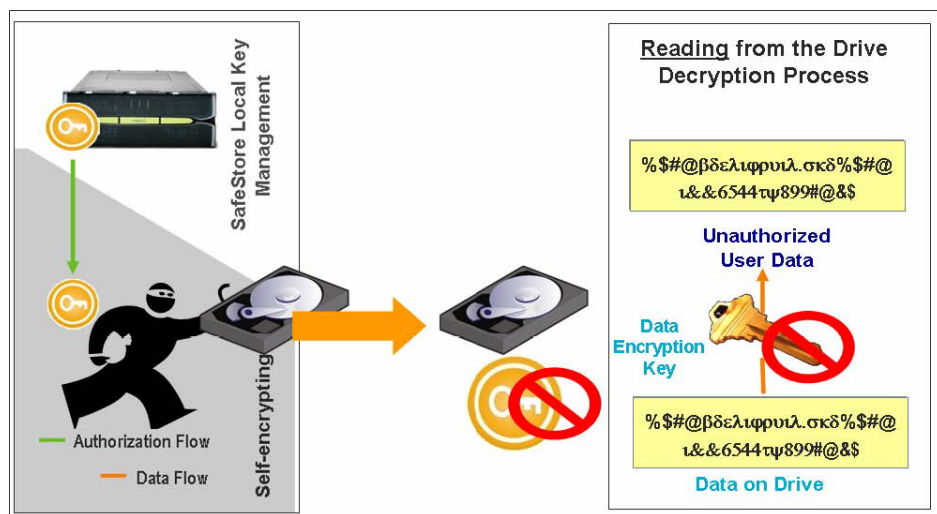


図 26. セキュリティ有効 FDE ドライブは、ストレージ・サブシステムから取り外されました: 正しい権限がない場合、盗まれた FDE ディスクはアンロックできず、データは暗号化されたままです。

ローカル・セキュリティ・キー管理でのセキュリティ・キーの変更

セキュリティ・キーを変更するプロセスは、使用しているセキュリティ・キー管理方式のタイプによって異なります。このセクションの情報では、ローカル・セキュリティ・キー管理構成でのセキュリティ・キーの変更について説明します。

ユーザーがセキュリティ・キーを変更すると、新しいセキュリティ・キーがストレージ・サブシステム・コントローラーのファームウェアによって生成されます。新しいセキュリティ・キーはストレージ・サブシステム内で暗号化されており、セキュリティ・キーを直接参照することはできません。ストレージ・サブシステム内のセキュリティ有効 FDE ドライブをアンロックするために使用されている以前のキーは、新しいセキュリティ・キーに置き換わります。コントローラーは、新しいキーについてすべてのセキュリティ有効 FDE ドライブと折衝します。

セキュリティ・キー・ファイルのバックアップ・コピーはセキュリティ・キーを変更する際には必ず生成され、コントローラー障害や他のストレージ・サブシステムへの転送に備えて、別のストレージ・メディアに保管しておく必要があります。セキュリティ・キーを変更する場合、ユーザーは、セキュリティ・キー ID、パスフレーズ、セキュリティ・キー・ファイルの名前および場所の作成に関与します。パスフレーズは、ストレージ・サブシステムあるいはセキュリティ・ファイルには保管されません。コントローラーは、パスフレーズを使用してセキュリティ・キーを暗号化してから、セキュリティ・キーをセキュリティ・キー・ファイルにエクスポートします。

外部セキュリティ・キー管理でのセキュリティ・キーの変更

このセクションの情報では、外部セキュリティ・キー管理構成でのセキュリティ・キーの変更について説明します。

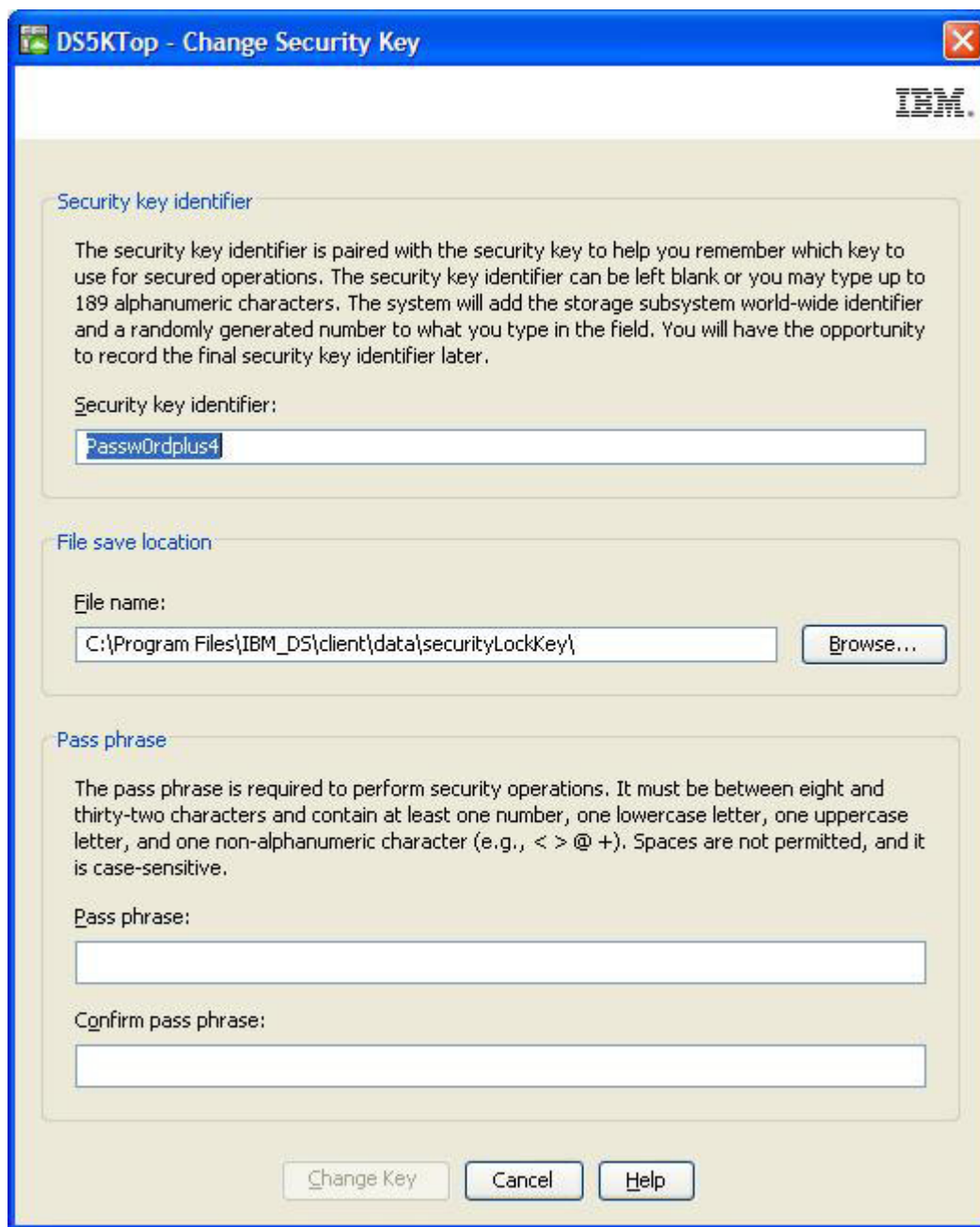
セキュリティ・キーを変更すると、ストレージ・サブシステム・コントローラーは、新規セキュリティ・キーを取得するために外部キー・ライセンス・マネージャーに接続します。次に、コントローラーは、セキュリティ有効 FDE ドライブと新規セキュリティ・キーを折衝します。新規キーは、コントローラー内部では難読化されません。キーをセキュリティ・キー・ファイルに保存するようプロンプトが出されます。セキュリティ・キーをバックアップするには、パスフレーズとセキュリティ・キー・ファイルの名前および場所が必要です。パスフレーズは、ストレージ・サブシステムあるいはセキュリティ・キー・ファイルには保管されません。コントローラーは、パスフレーズを使用してセキュリティ・キーを暗号化してから、セキュリティ・キーをセキュリティ・キー・ファイルにエクスポートします。

ストレージ・サブシステムのセキュリティ・キー・ファイルの識別

追加の保護として、FDE ドライブのアンロックに使用するセキュリティ・キーは、ユーザーには表示されません。セキュリティ・キー ID は、どのセキュリティ・キー・ファイルが各ストレージ・サブシステムに関連付けられているかを識別する上で役立ちます。ローカル・セキュリティ・キー管理方式では、最大 189 文字の英数字の値を指定できます。この値はストレージ・サブシステムのワールドワイド ID と乱数にリンクされ、セキュリティ・キー ID が形成されます。外部セキュリティ・キー管理方式では、セキュリティ・キー ID の一部として使用される値を指定するよう求められません。セキュリティ・キーの作成あるいは変更のような、ドライブ・セキュリティ・キー・ファイルを必要とする操作中に、セキュリティ・キー ID を参照することができます。

213 ページの図 27 は、セキュリティ・キー変更操作の実行時のセキュリティ・キー ID フィールドの例を示しています。

注: 外部セキュリティ・キー管理方式では、ローカル・セキュリティ・キー管理とは異なり、ユーザーがセキュリティ・キー ID を変更することはできません。



The image shows a Windows-style dialog box titled "DS5KTop - Change Security Key". It features the IBM logo in the top right corner. The dialog is divided into three main sections: "Security key identifier", "File save location", and "Pass phrase".

- Security key identifier:** Contains a text box with the value "Passw0rdplus4". Above the text box is explanatory text: "The security key identifier is paired with the security key to help you remember which key to use for secured operations. The security key identifier can be left blank or you may type up to 189 alphanumeric characters. The system will add the storage subsystem world-wide identifier and a randomly generated number to what you type in the field. You will have the opportunity to record the final security key identifier later."
- File save location:** Contains a "File name:" label and a text box with the path "C:\Program Files\IBM_DS\client\data\securityLockKey\". To the right of the text box is a "Browse..." button.
- Pass phrase:** Contains two text boxes labeled "Pass phrase:" and "Confirm pass phrase:". Above the first text box is explanatory text: "The pass phrase is required to perform security operations. It must be between eight and thirty-two characters and contain at least one number, one lowercase letter, one uppercase letter, and one non-alphanumeric character (e.g., < > @ +). Spaces are not permitted, and it is case-sensitive."

At the bottom of the dialog are three buttons: "Change Key", "Cancel", and "Help".

図 27. セキュリティー・キーの変更

「Change Security Key Complete (セキュリティ・キー変更の完了)」ウィンドウは、セキュリティ・キー・ファイルに書き込まれていたセキュリティ・キー ID が 図 27 で入力したセキュリティ・キー ID とストレージ・サブシステムのワールドワイド ID に乱数を追加したものであることを示しています。214 ページの図 28 は、セキュリティ・キー ID の乱数部分の例を示しています。



図 28. セキュリティー・キーの変更 - 完了

「FDE Drive Properties (FDE ドライブのプロパティ)」ウィンドウの**セキュリティー・キー ID** フィールドには、ユーザーがセキュリティー・キーを作成あるいは変更する際にコントローラーが生成する乱数が含まれます。215 ページの図 29 は、乱数の例を示しています。現在の乱数は 27000000 が接頭部です。ストレージ・サブシステムのすべてのセキュア FDE ドライブがセキュリティー・キー ID フィールドに同じ値を持っている場合、それらは同じセキュリティー・キー ID でアンロックすることができます。

注: 「Drive Properties (ドライブのプロパティ)」ウィンドウの「**Security Capable (セキュリティー対応)**」および「**Secure (セキュア)**」フィールドは、ドライブがセキュア対応であるかどうか、およびドライブがセキュア (Yes) 状態あるいは非セキュア (No) 状態のどちらであることを示します。



図 29. ドライブのプロパティ - セキュア FDE ドライブ

217 ページの図 30 は、ストレージ・サブシステム内のセキュア・ドライブをアンロックするためにセキュリティー・キー・バックアップ・ファイルを選択した場合に、**ファイル情報**フィールドに表示されるセキュ

リティー・キー ID の例を示しています。セキュリティー・キー ID あるいは LockKeyID (ファイル情報フィールドに表示されます) は、ユーザーがセキュリティー・キーを作成あるいは変更した際にセキュリティー・キー ID フィールドに入力した文字と一緒に、ストレージ・サブシステムのワールドワイド ID とランダムに生成された数値を含みます。これはすべてのセキュア FDE ドライブのセキュリティー・キー ID に表示されます。この情報はコロン (:) で区切られています。例えば、以下のような LockKeyID になります。

Passw0rdplus3:600a0b800029ece6000000004a2d0880:600a0b800029ed8a00001aef4a2e4a73

以下の情報を含んでいます。

- 指定したセキュリティー・キー ID、例えば Passw0rdplus3

注: 外部セキュリティー・キー管理方式では、ローカル・セキュリティー・キー管理とは異なり、ユーザーがセキュリティー・キー ID を変更することはできません。したがって、この情報は表示されません。

- ストレージ・サブシステムのワールドワイド ID、例えば 600a0b800029ece6000000004a2d0880
- ランダムに生成された数値 600a0b800029ed8a00001aef4a2e4a73

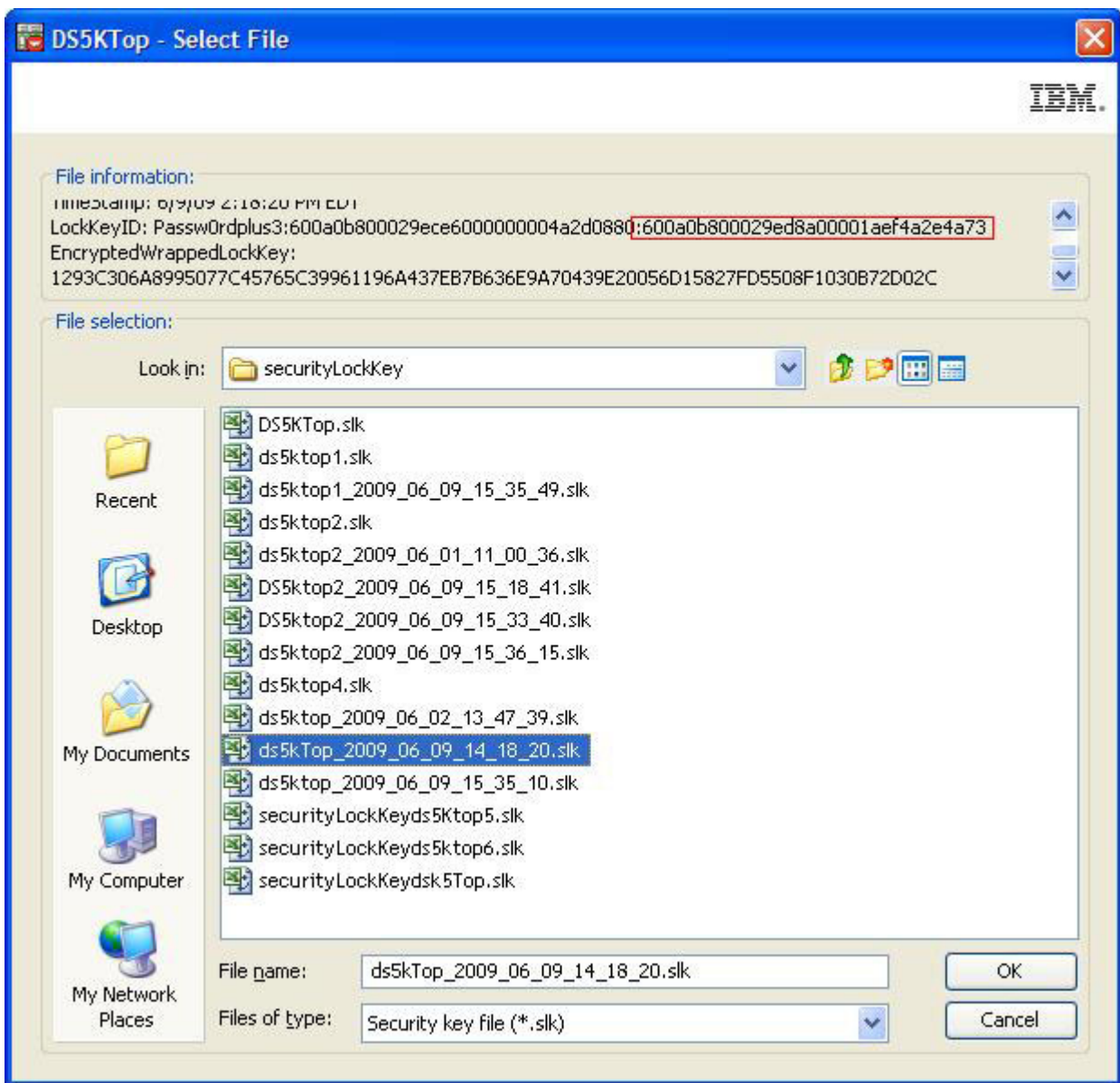


図 30. ファイルの選択 - LockKeyID

218 ページの図 31 は、非セキュア FDE ドライブのドライブ・プロパティの例を示しています。非セキュア FDE ドライブのセキュリティー・キー ID フィールドは、0 になっていることを確認してください。

「Security Capable (セキュリティー対応)」フィールドの値が「Yes」、「Secure (セキュア)」フィールドが「No」で、これがセキュリティー対応だが非セキュア FDE ドライブであると示していることを確認してください。

218 IBM System Storage DS ストレージ・マネージャー パージョン 10.8: インストールおよびホスト・サポートのガイド

ローカル・セキュリティ・キー管理モードでのセキュア・ドライブのアンロック

セキュリティ有効 FDE ドライブを使用した RAID アレイを、別のストレージ・サブシステムにエクスポートすることができます。これらのドライブを新しいストレージ・サブシステムに取り付けた後、セキュリティ有効 FDE ドライブをアンロックしないと、ドライブからのデータの読み取りやデータの書き込みができません。新しいストレージ・サブシステムのセキュリティ・キーは前のものとは異っており、ドライブをアンロックすることはできません。元のストレージ・サブシステムに保存したセキュリティ・キー・ファイルから、セキュリティ・キーを提供する必要があります。さらに、セキュリティ・キー・ファイルからセキュリティ・キーを取り出すには、そのセキュリティ・キーを暗号化するために使用したパスフレーズを提供する必要があります。セキュリティ・キー・ファイルのセキュリティ・キーを使用してドライブをアンロックした後、コントローラーは 1 つのバージョンのセキュリティ・キーのみがストレージ・サブシステム内のドライブをアンロックするのに使用されるように、これらのドライブ用の既存のセキュリティ・キーと交渉します。

コントローラーが常にこれらのドライブをアンロックするための現行および以前 ($n-1$) のセキュリティ・キーの値を保持しているため、ユーザーはストレージ・サブシステムの電源サイクルあるいは同じストレージ・サブシステム内でのドライブの取り外しと再挿入のたびに、ストレージ・サブシステム内のセキュリティ有効ドライブをアンロックするためにセキュリティ・キー・ファイルを提供する必要はありません。ただし、ドライブがストレージ・サブシステムから取り外され、同じストレージ・サブシステム内で 3 回以上セキュリティ・キーが変更された場合、そのドライブが同じストレージ・サブシステムに再挿入されたときにドライブをアンロックするためのセキュリティ・キーはコントローラーにありません。

重要: 悪意のある行為、自然災害、異常なハードウェア障害、あるいは FDE セキュリティ・キーの消失によってデータが失われないように、常にストレージ・サブシステム内のデータを機密保護機能のあるテープにバックアップしてください。

外部セキュリティ・キー管理モードでのセキュア・ドライブのアンロック

セキュリティ有効 FDE ドライブを使用した RAID アレイを、別のストレージ・サブシステムにエクスポートすることができます。ドライブの移動先が元のサブシステムと同じ外部キー・ライセンス・マネージャーによって管理されている別のサブシステムである場合、ドライブをアンロックするために、保存したセキュリティ・キー・ファイルを提供する必要はありません。

セキュリティ・キー・ファイルのセキュリティ・キーを使用してドライブをアンロックした後、コントローラーは 1 つのバージョンのセキュリティ・キーのみがストレージ・サブシステム内のドライブをアンロックするのに使用されるように、これらのドライブ用の既存のセキュリティ・キーと交渉します。これが行われない場合、元のストレージ・サブシステムに保存したセキュリティ・キー・ファイルからセキュリティ・キーを提供する必要があります。また、セキュリティ・キー・ファイルからセキュリティ・キーを取り出すには、そのセキュリティ・キーを暗号化するために使用したパスフレーズを提供する必要があります。セキュリティ・キー・ファイルのセキュリティ・キーを使用してドライブをアンロックした後、コントローラーは 1 つのバージョンのセキュリティ・キーのみがストレージ・サブシステム内のドライブをアンロックするのに使用されるように、これらのドライブ用の既存のセキュリティ・キーと交渉します。

注: FDE ドライブを移動する前に、元のサブシステムからアレイをエクスポートする必要があります。アレイは、ドライブを取り外しのために構成してサブシステム構成を更新する際に必要です。

サブシステム構成に非セキュア・ドライブまたは非 FDE ドライブがない場合、新規サブシステムの電源がオンになるときに、元のストレージ・サブシステムに保存したセキュリティ・キー・ファイルからセキュリティ・キーを提供する必要があります。サブシステム構成に最適な非セキュア・ドライブまたは非

FDE ドライブがある場合、サブシステムは始動して、外部セキュリティー・キー・マネージャーと接続し、セキュア FDE ドライブをアンロックするキーを取得します。

重要: 悪意のある行為、自然災害、異常なハードウェア障害、あるいは FDE セキュリティー・キーの消失によってデータが失われないように、常にストレージ・サブシステム内のデータを機密保護機能のあるテープにバックアップしてください。

セキュア消去の使用

セキュア消去は、FDE ドライブが将来的に使用を終えたり、返却、廃棄、あるいは目的を変更される際に、セキュリティーの脅威からドライブを保護します。これらのドライブがデータ・センターから移されたり、あるいは再利用されるときに、ディスク上のデータを永久的に消去してリカバリーに対してぜい弱でないようにすることが重要です。廃棄されたドライブには、許可されていないユーザーによって再構成可能なデータが残留している可能性があります。セキュア消去は、データを暗号的に消去することでこの脅威から保護します。

データを永久的に消去するために使用された従来の方法は、多くの場合で費用と時間がかかり、高水準のデータ消去を提供できないことが判明しました。従来の方法は、ドライブがコントロールの範囲外になる場合があります。それによってデータ侵害の危険にさらされる可能性もあります。セキュア消去には、従来の方法と比較して次のような利点があります。

- 即時の暗号的なデータ消去
- 全体のコストの削減
- 米国連邦情報・技術局 (NIST) に従った、より高水準なメディア・サニテーション

重要: セキュア消去操作は、取り消すことができません。セキュア消去操作が実行されると、ドライブ上のすべてのデータは永久的に消去されます。ドライブ上のデータがバックアップされているか、破棄しても構わないことを確認してください。

FDE ドライブを使用したセキュア消去によって、ドライブをデータ・センターから取り外す必要なく、データの即時消去が可能になります。数回のクリックのみで、すぐにドライブを再利用または廃棄することができます。セキュア消去により、ドライブを消去して再使用することができます。これによってドライブを破壊する必要がなくなり、同時に保証および有効期限切れのリースの返却を保護したり、ドライブをセキュアに再利用できるようになります。NIST によって、セキュア消去はデータ・パージの一種であると見なされており、これは従来の方法より高水準なデータ・サニテーションであると考えられています。

セキュア消去は FDE ドライブに対して、ドライブ内の既存の暗号鍵を消去して新しくランダムに生成した暗号鍵と置き換えるように指示します。ドライブ暗号鍵は、ディスク上のすべてのデータをエンコードおよびデコードするために使用されます。暗号鍵が変更されると、以前にディスクに書き込まれていたデータはすべて解読不能になります。以前の暗号鍵によって暗号化されていたデータは、新規の暗号鍵を使用して暗号化解除する場合は解読不能です。これは、すべてのビット、ヘッダー、およびディレクトリーも含まれます。データは完全に、そして永久にアクセス不能です。

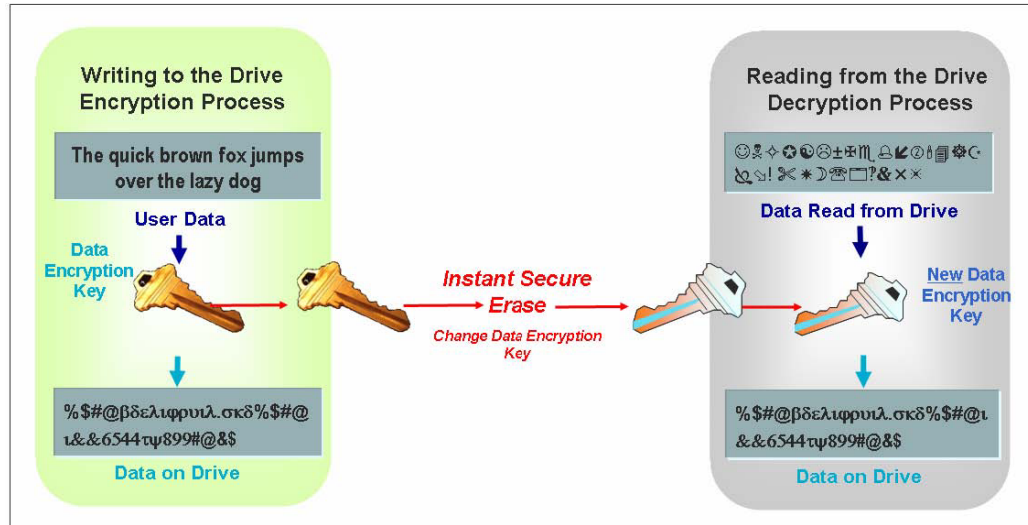


図 32. セキュア消去プロセス

FDE セキュリティー許可

次の表で、FDE 互換ストレージ・サブシステムにセキュリティーを実装するために使用する許可パラメーターを示して説明します。

表 35. セキュリティー許可

パラメーター	説明	どこに配置および管理されていますか？	どのように生成されますか？
暗号鍵	暗号鍵は、FDE ディスク・ドライブ上のデータを暗号化および暗号化解除するために使用されます。	FDE ディスク・ドライブに保管および管理されます。 - ドライブから転送されることはありません。 - 各ドライブごとに固有の暗号鍵があります。	暗号鍵はドライブの製造時に生成され、使用前にキーが漏えいしていないことを確実にするために、お客様のサイトで (コントローラーからドライブへのコマンドによって) 再生成されます。
セキュリティー・キー	セキュリティー・キーは、暗号化および暗号化解除を行うための暗号鍵のアンロックに必要です。ストレージ・サブシステム上のすべての FDE ドライブ用に 1 つのセキュリティー・キーが作成されます。セキュリティー・キーはロック・キーと呼ばれる場合もあります。	コントローラーに保管および管理されます。単一のセキュリティー・キーがストレージ・サブシステム内のすべてのコントローラー用に同期されます。	セキュリティー・キーはストレージ・サブシステムによって生成され、ストレージ・サブシステム内では暗号化されて非表示となります。

表 35. セキュリティー許可 (続き)

パラメーター	説明	どこに配置および管理されていますか?	どのように生成されますか?
セキュリティー・キー ID	セキュリティー・キー ID はセキュリティー・キーと対になり、セキュア操作に使用するキーを思い出すのに役立ちます。ローカル・セキュリティー・キー管理でのみ、ストレージ・サブシステムによって生成されたセキュリティー・キー ID にリンクされた最大 189 文字の英数字を指定するオプションがあります。	セキュリティー・キー ID はディスクの特別な領域に保管されます。 - いつでもディスクから読み取ることができます。 - セキュリティーが有効にされており、ドライブがアンロック状態の場合にのみディスクに書き込むことができます。	ユーザー指定の英数字ストリング (ローカル・セキュリティー・キー管理のみ)。ストレージ・サブシステムは、ストレージ・サブシステムのワールドワイド ID とランダムに生成した数値を、入力された文字に追加します。
パスフレーズ	パスフレーズはセキュリティー・キーとセキュリティー・キー ID を暗号化するために使用します。パスフレーズは、最小で 8 文字、最大で 32 文字のユーザー指定の英数字ストリングです。少なくとも 1 つの数値、1 つの小文字、1 つの大文字、および 1 つの非英数字文字 (例: <, >, &, @, +, または -) を含んでいる必要があります。スペースは使用できません。また大/小文字の区別があります。	ユーザー指定の英数字ストリングで、ストレージ・サブシステム上あるいはセキュリティー・キー・ファイルには保管されません。パスフレーズは、セキュリティー・キーがセキュリティー・キー・ファイルにエクスポートされる際に、セキュリティー・キーを暗号化するために使用されます。セキュリティー有効 FDE ドライブをストレージ・サブシステム内にインポートする際に使用される、セキュリティー・ファイル内のキーを暗号化解除するためにも使用されます。	ユーザー指定の英数字ストリング。
セキュリティー・キー・ファイル	セキュリティー・キー ID と暗号化されたセキュリティー・キーと一緒に保存されているファイル。	ファイルの名前と場所は管理者が決定します。管理者指定の場所に加えて、ストレージ・マネージャーもデフォルトの場所にセキュリティー・キー・バックアップ・ファイルのコピーを保存します。詳しくは、「 <i>IBM Full Disk Encryption Best Practices</i> 」資料を参照してください。	セキュリティー・キーの作成、変更、あるいは保存操作の開始後に、ストレージ・サブシステムによって生成されます。

FDE の用語

次の表に、この章で使用されている FDE の用語の定義を示します。

表 36. フル・ディスク暗号化の用語

用語	説明
FDE	フル・ディスク暗号化。暗号化および暗号化解除の開始を許可するためのセキュリティ・キーを必要とするディスク・ドライブ上のカスタム・チップまたは ASIC (アプリケーション固有の集積回路)。 FDE ディスク・ドライブはディスク上のすべてのデータを暗号化します。セキュア・ドライブでは、読み取りまたは書き込み操作が発生する前にセキュリティ・キーが供給される必要があります。データの暗号化および暗号化解除は、すべてがドライブによって処理され、ストレージ・サブシステムには認識されません。
セキュア消去	ドライブの暗号鍵の変更による永久的なデータの消滅。セキュア消去が実行されると、以前にディスクに書き込まれていたデータは解読不能になります。このフィーチャーは FDE ディスクのセキュリティ機能を活用して、暗号鍵をランダムに生成された値に変更することでデータを消去します。暗号鍵は誰にも知られることがないため、これによってセキュア消去が実現できます。セキュア消去が実行されると、ドライブはアンロック状態になり、誰でもディスクに読み取りあるいは書き込みが可能になります。セキュア消去は、ドライブ・リプロビジョニングと呼ばれる場合もあります。
ローカル・キー管理	ストレージ・サブシステム・コントローラーに作成され、収容されているセキュリティ・キーを使用するキー管理方式。セキュア・ドライブをストレージ・サブシステム間で移動するには、元のストレージ・サブシステムに保存したセキュリティ・キー・ファイルを使用してドライブをアンロックする必要があります。セキュリティ・キーは、電源オフ時に、ストレージ・サブシステム内で難読化されて保管されます。
外部キー管理	さまざまなストレージ・デバイスのキーを管理するためにネットワーク上のセントラル・キー・ロケーション (ストレージ・サブシステムの外部にある 1 つ以上のサーバー) を使用するキー管理方式。プロキシ・サーバーにより、セキュリティ・キーの要求および受け入れが容易になります。セキュリティ・キーは、電源オフ時にストレージ・サブシステム内に保管されません。 注: 1. 外部セキュリティ・キー管理を行うには、専用ソフトウェア (IBM Tivoli Key Lifecycle Manager (TKLM) など) が必要です。
ロック状態	セキュリティ有効 FDE ドライブがストレージ・サブシステムから取り外された後で再挿入された場合、あるいはストレージ・サブシステムが電源オフされたときに、そのドライブが示す状態。ストレージ・サブシステムの電源が復元されても、ドライブはロック状態のままです。セキュリティ・キーを使用してコントローラーがアンロックするまでは、ロック状態のディスクへのデータの書き込みあるいは読み取りはできません。コントローラーがセキュリティ・キーを持っていない場合、読み取りおよび書き込み操作のためにドライブをアンロックするには、セキュリティ・キー・ファイルとパスフレーズが必要です。
リパーバシング (目的変更)/リプロビジョニング (再提供)	ドライブを再利用するために、セキュア状態から非セキュア状態に変更すること。ドライブのリプロビジョニングは、セキュア消去によって完了します。
セキュア・アレイ	セキュリティ有効 FDE ドライブ上のアレイ。
セキュリティ対応ドライブ	暗号化対応だが非セキュア状態 (セキュリティが有効にされていない) の FDE ドライブ。
セキュリティ有効ドライブ	セキュリティが有効にされた FDE ドライブ。セキュリティ有効 FDE ドライブは、ドライブの電源がオンになった後で、読み取りまたは書き込み操作が発生する前に、セキュリティ・キーを使用してアンロックされる必要があります。

表 36. フル・ディスク暗号化の用語 (続き)

用語	説明
アンロック状態	ディスク上のデータに読み取りおよび書き込み操作のためにアクセス可能な、セキュリティ有効 FDE ドライブの状態。

開始する前に

外部セキュリティ・キー管理を使用する場合、以下の手順を実行する必要があります。

1. 外部キー・ライセンス・マネージャー・ソフトウェアの IBM Tivoli Key Lifecycle Manager (TKLM) をインストールおよび構成します。詳しくは、ソフトウェアに付属の資料を参照してください。
2. DS TKLM プロキシ・コードを IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) からダウンロードします。
3. DS TKLM プロキシ・コードをインストールおよび構成します。『DS TKLM プロキシ・コード・サーバーのインストールおよび構成』を参照してください。
4. ストレージ・マネージャーでフル・ディスク暗号化および外部キー管理プレミアム・フィーチャーを使用可能にします。232 ページの『プレミアム・フィーチャーの使用可能化』を参照してください。
5. TKLM およびストレージ・サブシステムを DS TKLM プロキシ用に構成して、外部キー管理のセキュリティ許可を作成します。232 ページの『プレミアム・フィーチャーの使用可能化』で 235 ページの『外部セキュリティ・キー管理を使用するセキュリティ許可の作成』を参照してください。

ローカル・セキュリティ・キー管理を使用する場合は、最初に、231 ページの『FDE ドライブを使用したディスク暗号化の構成』の情報をお読みください。

DS TKLM プロキシ・コード・サーバーのインストールおよび構成

このセクションでは、DS TKLM プロキシ・コード・サーバーをインストールするために必要な手順について説明します。DS TKLM プロキシ・コードは、以下のオペレーティング・システムをサポートします。

- AIX 5.x
- AIX 6.x
- Red Hat Enterprise Linux 4.x
- Red Hat Enterprise Linux 5.5
- SUSE Linux Enterprise Server 10.3
- SUSE Linux Enterprise Server 11
- Windows 2008 R2
- Windows 2008 Service Pack 2
- Windows 2008 Standard Edition
- Windows 2008 Enterprise Edition

重要: DS TKLM プロキシ・コード・サーバーに影響を与える可能性がある環境変更または構成変更を行う場合は、サーバーを再始動する必要があります。例えば、ストレージ・マネージャー・コントローラーの交換、**sysWipe** コマンドの発行、または IP アドレスの変更を行うには、DS TKLM プロキシ・コード・サーバーを再構成して再始動する必要があります。また、ストレージ・マネージャー・コントローラーの交換または **sysWipe** コマンドの発行など、セキュリティ・キー ID を変更する場合は、235 ページの『外部セキュリティ・キー管理を使用するセキュリティ許可の作成』で説明されているように、新しい

セキュリティー・キー ID を認識するように TKLM を変更する必要があります。詳しくは、『DS TKLM プロキシ・コード・サーバーの始動、停止、および再始動』を参照してください。

次の図は、外部セキュリティー・キー管理構成のコンポーネント間の関係を示しています。

注:

1. 1 つのプロキシ・サーバーによって最大 4 つのストレージ・サブシステム・コントローラーをモニターできます。
2. 1 つのプロキシ・サーバーに最大 4 つの TKLM サーバーを接続できます。

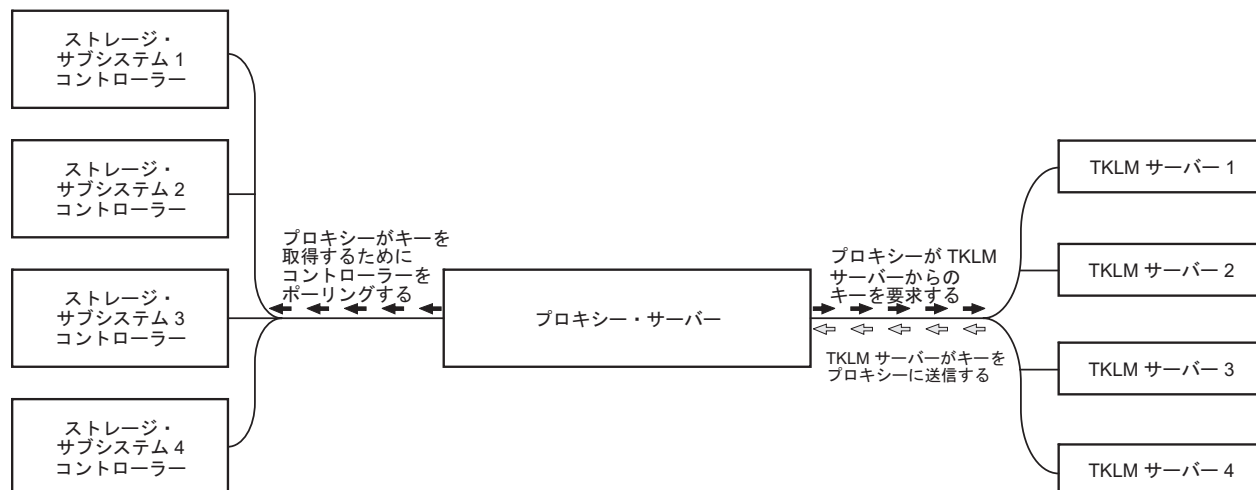


図 33. 外部セキュリティー・キー管理トポロジー

外部セキュリティー・キー管理構成を設定するには、DS TKLM プロキシ・コードを IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) からダウンロードして、以下の手順を実行します。

1. 226 ページの『DS TKLM プロキシ・コード・サーバーの構成ファイルの変更』
2. 229 ページの『DS TKLM プロキシ・コードのインストール』

重要: 手順を順番どおりに実行する必要があります。IBM Tivoli Key Lifecycle Manager (TKLM) ソフトウェアがインストールされていることを確認します。詳しくは、ソフトウェアに付属の資料を参照してください。

DS TKLM プロキシ・コード・サーバーの始動、停止、および再始動

プロキシに影響を与える可能性がある環境変更または構成変更（例えば、ネットワークの変更）を行うには、プロキシを再始動する必要があります。次のユーティリティを使用できます。

AIX の場合:

```
start_DS_TKLM_Proxy_Code_AIX.sh
stop_DS_TKLM_Proxy_Code_AIX.sh
restart_DS_TKLM_Proxy_Code_AIX.sh
```

Linux の場合:

```
start_DS_TKLM_Proxy_Code_Linux.sh
stop_DS_TKLM_Proxy_Code_Linux.sh
restart_DS_TKLM_Proxy_Code_Linux.sh
```

stop_DS_TKLM_Proxy_Code_*.sh スクリプトにより、/etc/inittab から項目が削除され、プロセスが終了します。

DS TKLM プロキシ・コード・サーバーの構成ファイルの変更

プロキシの構成ファイルは、DS_TKLM_Proxy_Code.config です。構成ファイル名、およびパラメーターとそれらの定義は、サポートされるすべてのオペレーティング・システム (Windows、AIX、および Linux) で同じです。ただし、一部のパラメーター値の形式が Windows と AIX または Linux で異なります。

Windows で構成ファイルを作成および編集する方法は、AIX または Linux の方法と異なります。Windows では、DS_TKLM_Proxy_Code_Windows*.zip ファイルに含まれているテンプレートを使用して、DS_TKLM_Proxy_Code.config を手動で作成する必要があります。プロキシをインストールする前に、パラメーターの定義を割り当てる必要があります。

重要: Windows オペレーティング・システム環境で作業している場合、DS TKLM プロキシ・コード・サーバーをインストールする前に、構成ファイルを作成および変更する必要があります。

AIX および Linux では、インストール時に DS_TKLM_Proxy_Code.config が作成され、パラメーターの定義が割り当てられます。プロンプトが出されたら、構成ファイル・パラメーターに定義を割り当てる必要があります。

各パラメーターの定義について次の表で説明します。

表 37. プロキシの構成ファイル・プロパティ

プロパティ名	説明	例
LogLevel	このプロパティは、次の 4 つのロギング・レベルのいずれか 1 つを指定します。 • UserInfo: イベントに関する基本的な情報 • UserWarning: 潜在的な問題に関する警告情報 • UserError: システム障害およびプロキシ・サーバー出口に関するエラー情報 • Debug: さまざまな位置のストリングの長さおよびプロパティ値など、デバッグに役立つ情報	LogLevel = debug
DebugPath	このプロパティは、デバッグ・ファイルの場所を指定します。ディレクトリー /DS_TKLM_Proxy_Code/bin への相対パスまたは絶対パスのいずれかで、ファイル・システム内のパスを指定する必要があります。 注: パス・ディレクトリーに対する読み取りおよび書き込み許可があることを確認します。	AIX または Linux の例: DebugPath = ./Log/Debug/debug.log Windows の例: DebugPath = .¥Log¥Debug¥debug.log
AuditPath	このプロパティは、監査ファイルの場所を指定します。ディレクトリー /DS_TKLM_Proxy_Code/bin への相対パスまたは絶対パスのいずれかで、ファイル・システム内のパスを指定する必要があります。 注: パス・ディレクトリーに対する読み取りおよび書き込み許可があることを確認します。	AIX または Linux の例: AuditPath = ./Log/Audit/audit.log Windows の例: AuditPath = .¥Log¥Audit¥audit.log

表 37. プロキシの構成ファイル・プロパティ (続き)

プロパティ名	説明	例
ThresholdSize	このプロパティは、各ログ・ファイルの最大サイズをバイト単位で指定します。サイズのしきい値に達すると、元のファイル名と同じ名前の末尾に番号 01 が追加されたファイル名で新規ファイルが作成されます。新規ログ・ファイルがサイズのしきい値に達すると、元のファイルが上書きされます。 注: 後でしきい値のサイズを増やす場合、既存のログ・ファイルを削除してください。そうしないと、新しいサイズのしきい値が以前のサイズのしきい値より大きい場合、プロキシはログ情報を以前のファイルに書き込みます。	Threshold size = 100000000000
KeyinformationPath	このプロパティは、セキュリティ証明書ファイルの場所 (KeyPassword プロパティで指定されるファイルと一致します) を指定します。/DS_TKLM_Proxy_Code/bin への相対パスまたは絶対パスのいずれかで、ファイル・システム内のパスを入力します。パスが Windows または AIX および Linux のディレクトリ指定の規則に従っていること、および指定するディレクトリおよびファイルが存在することを確認します。 注: このプロパティは、外部キー管理プレミアム・フィーチャーを使用可能にした後で E メールで受信したセキュリティ証明書ファイルおよびパスワードを参照します。セキュリティ証明書ファイルを受信していない場合、またはこのファイルがなくなった場合は、IBM Premium Features Web サイトでキー再活動化プロセスを使用して、別のファイルとパスワードを要求できます。	AIX または Linux の例: KeyinformationPath = ./CertFile/ibmproxycert.p12 Windows の例: KeyinformationPath = .%CertFile%ibmproxycert.p12
KeyPassword	このプロパティは、セキュリティ証明のパスワード (KeyinformationPath プロパティで指定されるファイルと一致します) を指定して、読み取りが行われた後に難読化されます。難読化された後でパスワードを変更する必要がある場合は、最初に KeyPasswordHex プロパティ値を削除してプロキシ・サーバーを再始動する必要があります。そうしないと、新規パスワードは無視されます。 注: このプロパティは、外部キー管理プレミアム・フィーチャーを使用可能にした後で E メールで受信したセキュリティ証明書ファイルおよびパスワードを参照します。セキュリティ証明書ファイルを受信していない場合、またはこのファイルがなくなった場合は、IBM Premium Features Web サイトでキー再活動化プロセスを使用して、別のファイルとパスワードを要求できます。	最初の読み取りが行われる前の KeyPassword プロパティの例: KeyPassword = password 最初の読み取りが行われ、パスワードが難読化された後の KeyPassword プロパティの例: KeyPasswordHex = 47558BADDI3321FC KeyPassword = *****

表 37. プロキシの構成ファイル・プロパティ (続き)

プロパティ名	説明	例
SYMServer.x	<i>SYMServer</i> という用語は、ストレージ・サブシステムとそのコントローラーを表します。 注: 1 つのプロキシ・サーバーによって最大 4 つのストレージ・サブシステム・コントローラーをモニターできます。このプロパティは、構成内のすべてのストレージ・サブシステム、またはシンボル・サーバー (<i>SYMServer.1</i> から <i>SYMServer.n</i>) に関する情報を指定します。SYMServer ごとに 2 つのコントローラー IP アドレス、2 つのポート (2463)、1 つの SSID、1 つのパスワード標識、および 1 つのパスワードが必要です。したがって、それぞれの SYMServer プロパティ値は次の形式のパターンと一致する必要があります。変数はイタリック体で示されています。 <i>SYMServer.x = Controller A IP address , Controller B IP address , port number , port number , SSID , password indicator , password</i> パスワード標識は、パスワードが平文で指定されている場合は <i>false</i> に設定され、パスワードが難読化されている場合は <i>true</i> に設定される必要があります。パスワードは、ストレージ・サブシステムを管理するために使用されます。パスワードは、読み取りが行われた後で、プロキシによって自動的に難読化され、暗号化された形式で保管されます。 このプロパティでは、値の各部分の間にスペースを使用できます。SSID は 16 進値でなければなりません。プロキシは、DS_TKLM_Proxy_Code.config ファイルの SSID を、ストレージ・サブシステムから取得する SSID と比較します。これらが等しくない場合、プロキシは、ストレージ・サブシステムのモニターを停止します。 注: ストレージ・マネージャーの「Storage Subsystem Profile (ストレージ・サブシステム・プロファイル)」ウィンドウからストレージ・サブシステムの SSID を取得する必要があります。	構成ファイルが最初に読み取られる前の例: <pre>SYMServer.1 = 9.37.117.35 , 9.37.117.36 , 2463 , 2463 ,600A0B8000339848000000004B72851F, false, SymPasswd</pre> 構成ファイルが最初に読み取られた後の例: <pre>SYMServer.1 = 9.37.117.35 , 9.37.117.36 , 2463 , 2463 , 600A0B8000339848000000004B72851F, true , 6408D5D0C596979894AA8F</pre>

表 37. プロキシの構成ファイル・プロパティ (続き)

プロパティ名	説明	例
TKLMServer.x	このプロパティは、構成内のすべての TKLM サーバーに関する情報を指定します。 注: 1 つのプロキシ・サーバーに最大 4 つの TKLM サーバーを接続できます。TKLM サーバーごとに 1 つの IP アドレスおよび 1 つのポートがあるため、それぞれの TKLM サーバー・プロパティ値は次の形式のパターンと一致する必要があります。変数はイタリック体で示されています。 <i>TKLMServer.x = IP address , port number</i> このプロパティでは、値の各部分の間にスペースを使用できます。このプロパティの値を入力しない場合、プロキシ・サーバーはデフォルト値 (localhost, 3801) を使用します。ポート番号は、Tivoli Lifecycle Key Manager ソフトウェアの「Key Serving Ports (キー・サービス・ポート)」ウィンドウで見つかります。	TKLMServer.1 = 9.41.18.161 , 3801
TcpTimeout	このプロパティは、サーバーへの TCP 接続のタイムアウト期間の長さを秒単位で指定します。	TcpTimeout = 1000
RpcTimeout	このプロパティは、サーバー上のリモート・プロシージャ・コールのタイムアウト期間の長さを秒単位で指定します。	RpcTimeout = 10
TimeBetween-SymbolServer-Queries	このプロパティは、プロキシ・サーバーによるアテンション状態の検査間の待機期間を秒単位で指定します。	TimeBetweenSymbolServerQueries = 10

DS TKLM プロキシ・コードのインストール

外部セキュリティー・キー管理で使用するために DS TKLM プロキシ・コードをインストールするには、以下のいずれかの手順を実行します。Windows 環境の場合、『Windows 環境での DS TKLM プロキシ・コード・サーバーのインストール』を参照してください。AIX または Linux 環境の場合、230 ページの『AIX または Linux 環境での DS TKLM プロキシ・コード・サーバーのインストール』を参照してください。

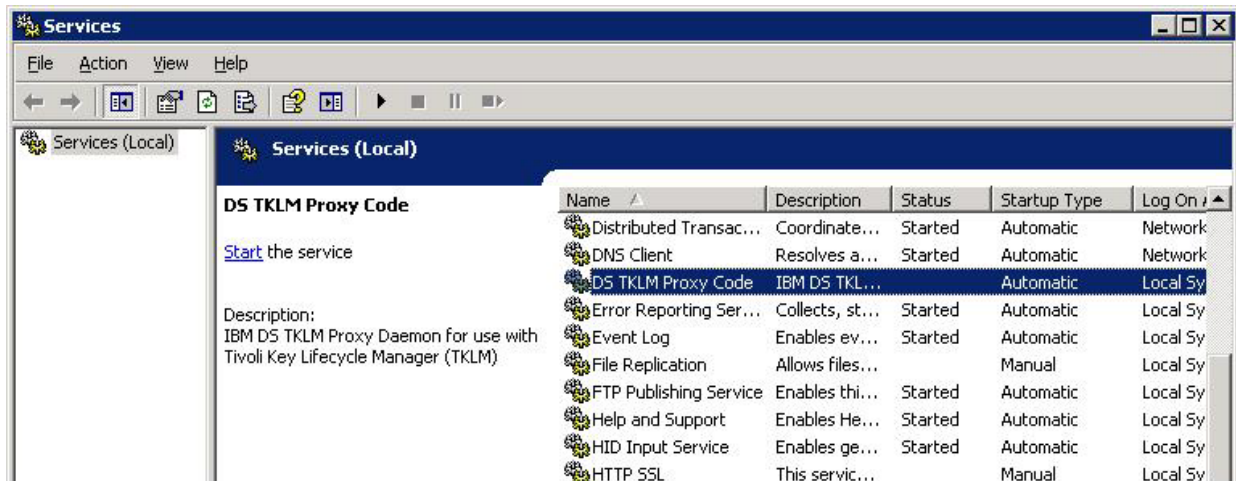
Windows 環境での DS TKLM プロキシ・コード・サーバーのインストール

Windows 環境でプロキシをインストールするには、以下の手順を実行します。

1. IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) にアクセスして、ポータルの「Downloads and fixes (ダウンロードおよびフィックス)」エリアから、ご使用のバージョンの Windows 用の該当ファイルをダウンロードします。ファイル名は、DS_TKLM_Proxy_Code-Windows-V*.zip のようになっています。
2. 圧縮ファイルをローカル・ディレクトリー (例えば、c:\¥DS_TKLM_Proxy_Code) に解凍します。
3. DS_TKLM_Proxy_Code.config ファイルが変更されていることを確認します (変更する必要があるプロパティについては、226 ページの『DS TKLM プロキシ・コード・サーバーの構成ファイルの変更』を参照してください)。
4. プロキシ・サーバーを始動する前に、IBM から取得した、構成ファイルの KeyInformationPath プロパティで指定されている証明書ファイルが存在することを確認します。

注: 「DS_TKLM_Proxy_Code_WinService.exe - Application Error」メッセージが表示された場合、Microsoft Visual C++ Redistributable Package をダウンロードしてインストールすることが必要になる可能性があります。Windows 2008 と互換性のあるパッケージを入手するには、<http://www.microsoft.com/downloads/details.aspx?familyid=A5C84275-3B97-4AB7-A40D-3802B2AF5FC2&displaylang=en> にアクセスしてください。

5. DOS プロンプト・ウィンドウで、コマンド `DS_TKLM_Proxy_Code_WinService.exe -i` を入力します。「Services (サービス)」ウィンドウにプロキシーが追加されます。プロキシーを開始するには、「Services (サービス)」ウィンドウの「Start (開始)」をクリックします。



注: プロキシーをアンインストールするには、DOS プロンプト・ウィンドウを開き、コマンド `DS_TKLM_Proxy_Code_WinService.exe -u` を入力して実行します。Windows を再始動します。

AIX または Linux 環境での DS TKLM プロキシー・コード・サーバーのインストール

DS TKLM プロキシー・コードは、AIX または Linux (RedHat および SUSE) 向けに RPM フォーマットでパッケージされています。AIX または Linux 環境でプロキシー・サーバーをインストールするには、以下の手順を実行します。

1. IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) にアクセスして、ポータルの「Downloads and fixes (ダウンロードおよびフィックス)」エリアから、ご使用のオペレーティング・システム・バージョン用の該当ファイルをダウンロードします。例えば、AIX 用のファイル名は `DS_TKLM_Proxy_Code-AIX-V2.01_90.70.60.04.ppc.rpm`、Linux 用のファイル名は `DS_TKLM_Proxy_Code-Linux-V2.01_90.70.60.04.i386.rpm` のようになっています。

注: 必ず、ご使用のオペレーティング・システム用の正しいファイルをダウンロードしてください。オペレーティング・システムは、RPM ファイル名の一部になっています。

2. rpm コマンドを使用して、ダウンロードしたファイルを解凍し、インストール・プロセスを開始します。例えば、以下のとおりです。

```
rpm -ivh --nodeps DS_TKLM_Proxy_Code-AIX-V1_.ppc.rpm
```

注: コマンドの `--nodeps` の部分は、AIX でのインストールにのみ必要です。

RPM コマンドを実行する際、シンボリック・リンクを作成して、IBM によって提供される証明書ファイルの場所を指定し、`/etc/inittab` のバックアップを作成して、インストール・スクリプトの実行時に使用するパスを指定します。

3. RPM コマンドを実行した後、インストール・スクリプト (/DS_TKLM_Proxy_Code/bin/install.sh) を実行します。
4. プロンプトが出されたら、すべての構成ファイル・プロパティーを入力します。プロパティーおよびそれらの値の説明については、226 ページの『DS TKLM プロキシ・コード・サーバーの構成ファイルの変更』を参照してください。

TKLM およびストレージ・サブシステムをプロキシ用に構成して、外部キー管理のセキュリティ許可を作成するには、232 ページの『プレミアム・フィーチャーの使用可能化』の 235 ページの『外部セキュリティ・キー管理を使用するセキュリティ許可の作成』に進みます。

FDE ドライブを使用したディスク暗号化の構成

このセクションでは、ストレージ・サブシステム上で FDE を使用可能にする手順およびセキュア・アレイを作成する手順について説明しています。FDE ディスクを使用してディスク暗号化を構成するには、以下のタスクを実行します。

1. FDE ドライブを取り付けます (『FDE ドライブの取り付け』を参照)。
2. フル・ディスク暗号化フィーチャーを使用可能にします (232 ページの『プレミアム・フィーチャーの使用可能化』を参照)。
3. アレイを作成し、アレイ・セキュリティを使用可能にします (240 ページの『RAID アレイのセキュア化』を参照)。ディスク・プールに対してもセキュリティを使用可能にすることができます。手順は、アレイの場合と完全に同じです。

注: このセクションに記載するスクリーン・ショットは説明のみを目的としており、ストレージ・マネージャーおよびコントローラー・ファームウェアのバージョンによっては、実際の UI と異なる場合があります。

セキュリティ有効 FDE ドライブは、電源がオフにされたりストレージ・サブシステムから取り外されるとロックされます。ロックされたドライブをアンロックするには、246 ページの『ディスク・ドライブのアンロック』を参照してください。

一部のストレージ・サブシステムでは、ドライブを別のストレージ・サブシステムに完全なアレイとしてマイグレーションすることができます。セキュア・アレイをマイグレーションするには、249 ページの『FDE ドライブを使用するストレージ・サブシステムのマイグレーション (ヘッド・スワップ)』を参照してください。

FDE ドライブの取り付け

このセクションでは、本書の作成時点で FDE 互換の IBM DS ストレージ・サブシステムがサポートする FDE ディスク・ドライブをリストしています。インストール手順および最新のサポート情報については、「*IBM System Storage DS3000、DS4000、および DS5000 ハード・ディスク・ドライブおよびストレージ拡張エンクロージャーの取り付けとマイグレーションのガイド*」および「*DS5000 Interoperability Guide*」を参照してください。

IBM DS ストレージ・サブシステムによってサポートされている FDE ドライブは、その特定のストレージ・サブシステムの発表レターに記載されています。また、ご使用のストレージ・サブシステム用の互換性のある FDE ドライブについて IBM 販売店または IBM 営業担当員にお問い合わせいただくこともできます。

注: FDE ドライブが「Security Enabled (セキュリティ有効)」状態で、ドライブにデータを保持したくない場合は、各ドライブでセキュア消去を実行してから新規 RAID アレイの一部として使用してください。

セキュア消去は、強制的にドライブに新しい暗号鍵を生成し、ドライブを非セキュア状態にし、以前にディスクに保管されていたすべてのデータを確実に消去します。詳しくは、220 ページの『セキュア消去の使用』を参照してください。

プレミアム・フィーチャーの使用可能化

IBM DS ディスク暗号化プレミアム・フィーチャー・キー・ライセンス・キットに付属の手順を使用して、ストレージ・サブシステムで FDE プレミアム・フィーチャーを使用可能にする必要があります。フル・ディスク暗号化が使用可能にされていることを確認するには、「Setup (セットアップ)」ページで「**View/Enable Premium Features (プレミアム・フィーチャーの表示/使用可能化)**」を選択します。

「Premium Features and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウで「Full Disk Encryption: Enabled (フル・ディスク暗号化: 使用可能)」および「External Key Management: Enabled (外部キー管理: 使用可能)」が表示されている場合は、FDE プレミアム・フィーチャーが使用可能にされています。

重要: 外部キー管理では、セキュリティ証明書ファイルおよびそのパスワードが必要です。このファイルとパスワードは、外部キー管理プレミアム・フィーチャーを使用可能にした後で E メールによってユーザーに送信されます。IBM Premium Feature Web サイトで外部キー管理プレミアム・フィーチャーを使用可能にする際、次の図に示されているフィールドに有効な E メール・アドレスを入力する必要があります。そうしないと、「**Continue (続行)**」をクリックした後で、E メール・アドレスを入力するようプロンプトが出されます。

Your activation key file will be provided via a link once the information above is verified and submitted. In addition, if you would like the activation key file sent to you, please provide your email address below:

Email address

Verify email address

E-mail: Stay informed about IBM products, services, and other offerings! If you want to stay informed by e-mail, please let us know by checking the box below.

☐ e-mail: Yes, please have IBM or an affiliate send me e-mail.

Other communications: IBM or an affiliate or selected organizations may keep you informed about IBM related products, services and other offerings through ways other than e-mail, for example, by telephone or postal mail. If you do not want us to use the information you provided here to keep you informed through other ways, please indicate in the box below.

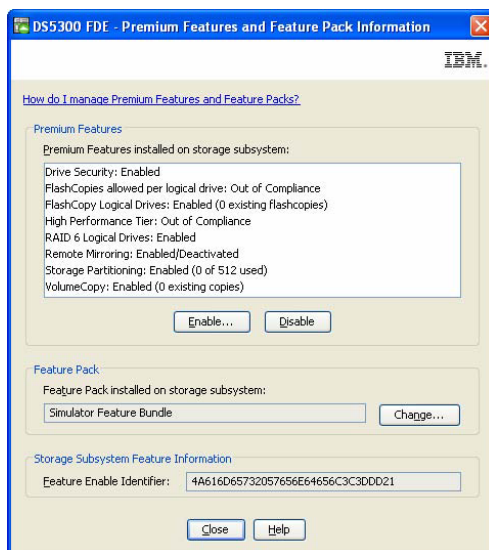
☐ Other communications: Please do not use the information I have provided here.

By clicking "Continue", you agree that IBM may process your data in the manner indicated above and as described in our Privacy policy.

セキュリティ証明書ファイルとパスワードを受信するまで最大で 1 日かかることがあります。ファイルを受信していない場合、またはファイルが添付された E メールがなくなった場合は、IBM Premium Features Web サイトでキー再活動化プロセスを使用して、別のファイルとパスワードを要求できます。セキュリティ証明書ファイルと、KeyinformationPath および KeyPassword プロパティの構成 (Windows

オペレーティング・システムのみ) について詳しくは、226 ページの『DS TKLM プロキシ・コード・サーバーの構成ファイルの変更』を参照してください。

コントローラー・ファームウェア 7.70.xx.xx 以降を使用するストレージ・サブシステムの場合、2010 年 11 月より後に FDE フィーチャーを使用可能にすると、「Premium Features and Feature Pack Information (プレミアム・フィーチャーおよびフィーチャー・パック情報)」ウィンドウに「External Key Management: Enabled (外部キー管理: 使用可能)」および「Full Disk Encryption: Enabled (フル・ディスク暗号化: 使用可能)」が表示されます。



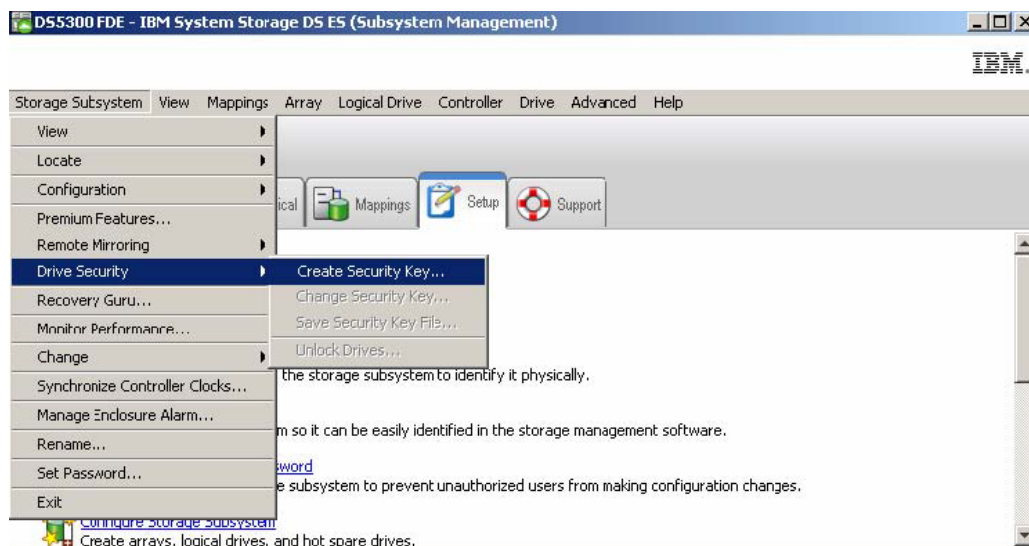
フル・ディスク暗号化の使用可能化には、電源がオフにされたりストレージ・サブシステムから取り外されたセキュアな FDE ドライブをアンロックするために後で必要な、セキュリティ許可の作成が含まれます。これらの許可には、セキュリティ・キー ID、パスフレーズ、およびセキュリティ・キー・ファイルが含まれます。セキュリティ許可は、ストレージ・サブシステム内のすべての FDE ドライブに適用され、電源をオンにした後でドライブをアンロックする必要がある場合に重要です。

セキュリティ許可を作成するプロセスは、使用しているキー管理方式によって異なります。ローカルまたは外部セキュリティ・キー管理の該当セクションを参照してください。

ローカル・セキュリティ・キー管理を使用するセキュリティ許可の作成

ローカル・キー管理を使用してフル・ディスク暗号化用のセキュリティ許可を作成するには、以下の手順を実行します。外部キー管理のセキュリティ許可については、235 ページの『外部セキュリティ・キー管理を使用するセキュリティ許可の作成』を参照してください。

1. 「ストレージ・マネージャーの「Subsystem Management (サブシステム管理)」ウィンドウから、「Storage Subsystem (ストレージ・サブシステム)」をクリックして、「Drive Security (ドライブ・セキュリティ)」をクリックし、「Create Security Key (セキュリティ・キーの作成)」をクリックします。



2. 次のように「Create Security Key (セキュリティ・キーの作成)」ウィンドウで、セキュリティ・キー ID、セキュリティ・キー・ファイルの名前および場所、パスフレーズを入力します。
 - **セキュリティ・キー ID:** セキュリティ・キー ID はストレージ・サブシステム・ワールドワイド ID とランダムに生成された数値の組み合わせで、セキュリティ・キー・ファイルを一意的に識別するために使用します。セキュリティ・キー ID は、ブランクあるいは最大で 189 文字が可能です。
 - **パスフレーズ:** パスフレーズは、セキュリティ・キー・ファイルからセキュリティ・キーを読み取る際に、セキュリティ・キーを暗号化解除するために使用します。ここで、パスフレーズを入力および記録します。パスフレーズを確認してください。
 - **セキュリティ・キー・バックアップ・ファイル:** ファイル名の横の「**Browse (参照)**」をクリックして、セキュリティ・キー・ファイルの名前と場所を選択するか、フィールドに値を直接入力します。「**Create Key (キーを作成)**」をクリックします。

注: 安全な場所にセキュリティ・キー・ファイルを保存します。ベスト・プラクティスは、セキュリティ・キー・ファイルとキー管理ポリシーと一緒に保管することです。ドライブを 1 つのストレージ・サブシステムから別のストレージ・サブシステムに移動する際や、ストレージ・サブシステムの両方のコントローラーが同時に交換される際にセキュリティ・キー・ファイルが必要なため、このファイルの保管場所を記録および記憶しておくことが重要です。

3. 「Create Security Key Complete (セキュリティ・キー作成の完了)」ウィンドウで、セキュリティ・キー ID およびセキュリティ・キー・ファイルの名前を記録して「OK」をクリックします。ストレージ・サブシステムで FDE ドライブのセキュリティを使用可能にするために必要な許可が設定されました。これらの許可は、ストレージ・サブシステムの両方のコントローラー間で同期されます。これらの適切な許可によって、ストレージ・サブシステムの FDE ドライブ上のアレイは保護されます。

重要: さらにセキュリティを強固にするには、複数のパスフレーズとセキュリティ・キー・ファイルを保管します。セキュリティ・キー・ファイルのコピーの保管場所として、デフォルトのセキュリティ・ファイル・ディレクトリーを指定しないようにしてください。セキュリティ・キー・ファイルの保存場所としてデフォルトのディレクトリーを指定した場合、セキュリティ・キー・ファイルのコピーは 1 つしか保存されません。同じストレージ・サブシステムからマップされている論理ドライブに、セキュリティ・キー・ファイルを保管しないようにしてください。詳しくは、「IBM Full Disk Encryption Best Practices」資料を参照してください。



外部セキュリティ・キー管理を使用するセキュリティ許可の作成

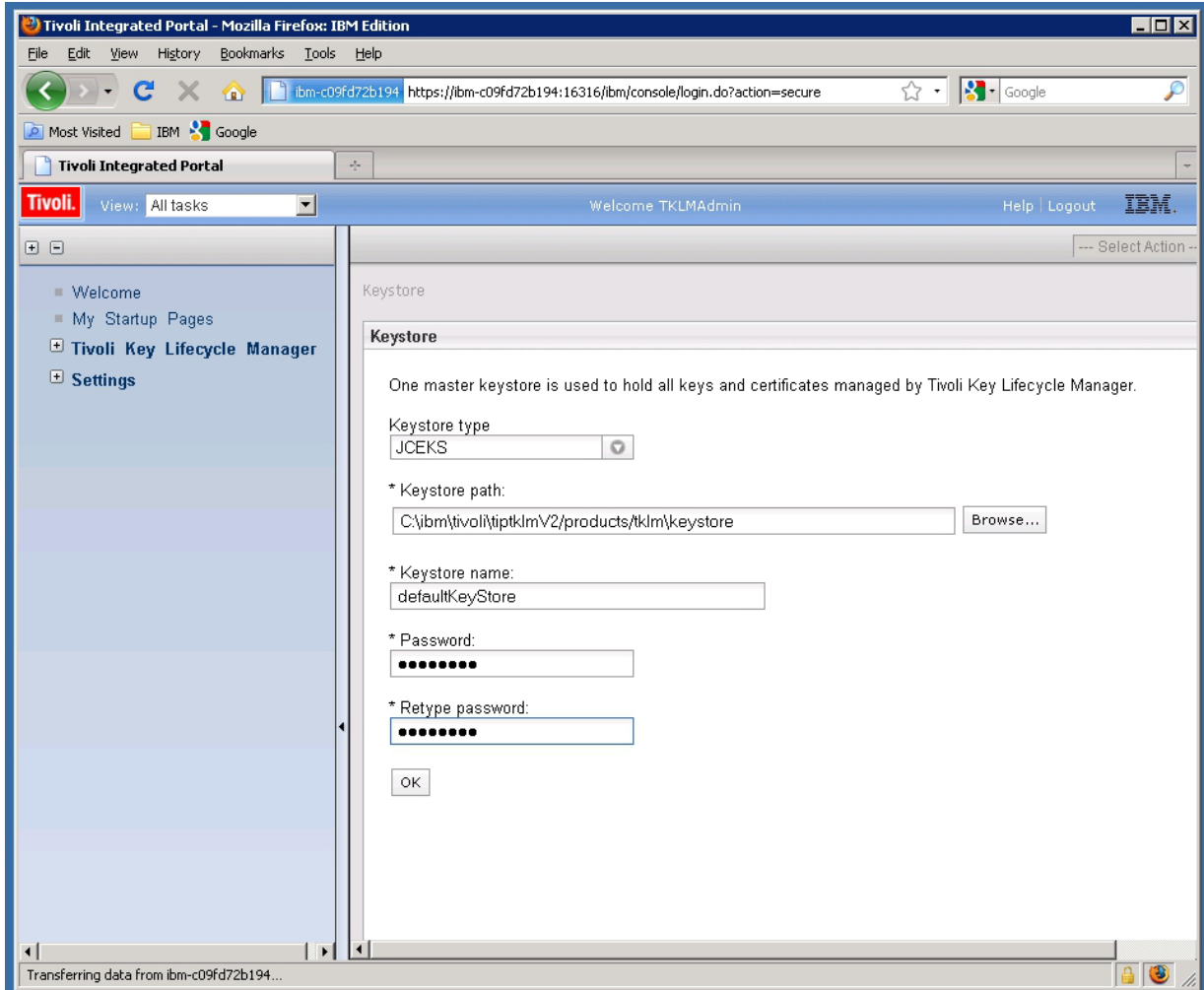
重要:

外部キー管理を使用してフル・ディスク暗号化用のセキュリティ許可を作成する前に、224 ページの『DS TKLM プロキシ・コード・サーバーのインストールおよび構成』の手順を完了しておく必要があります。

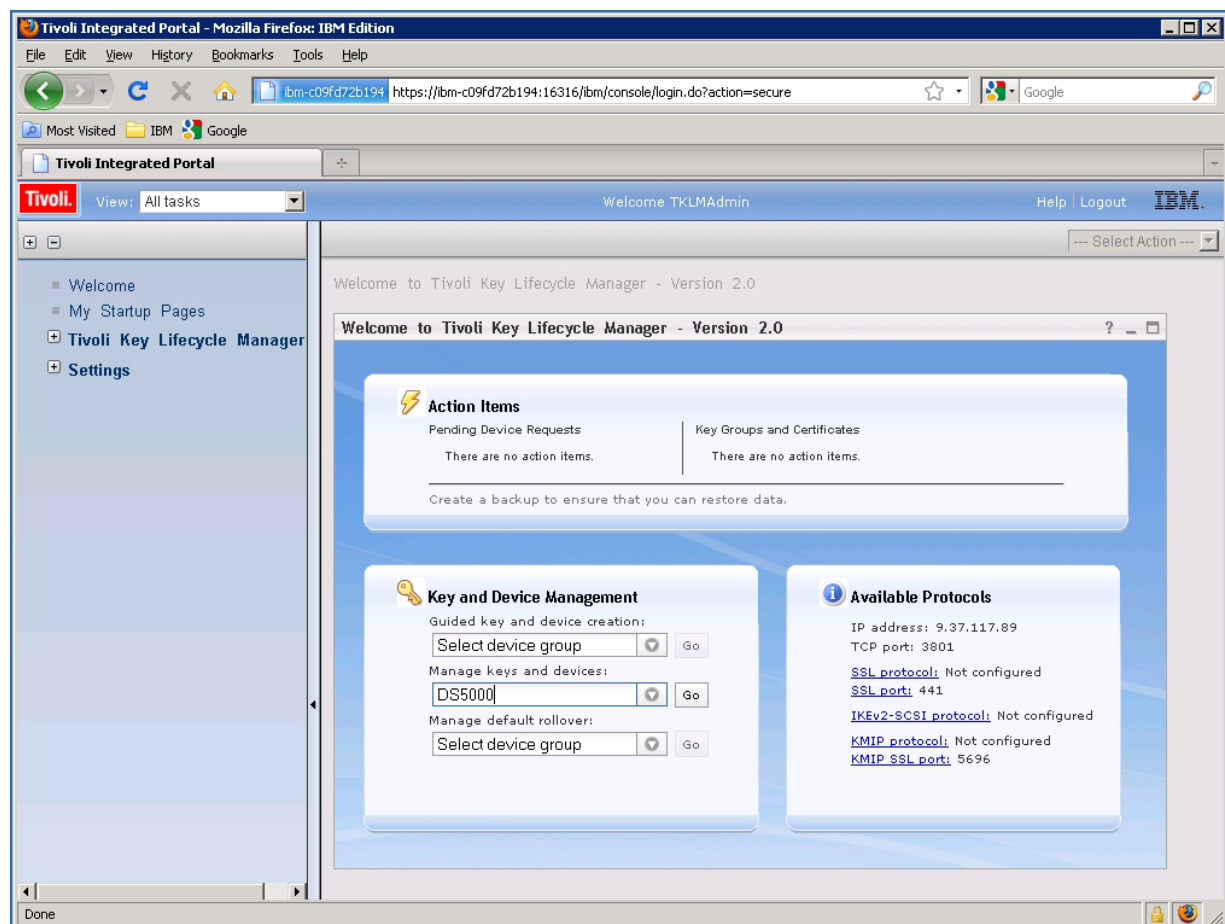
Tivoli Key Lifecycle Manager (TKLM) は、インストールされた後に、DS TKLM プロキシ・コード・サーバーからのキー要求に対応するよう構成される必要があります。TKLM を構成するには、以下の手順を完了します。

1. TKLM を開き、TKLAdmin ID を使用してログインします。
2. 「[click here to create the master keystore](#) (マスター鍵ストアを作成するにはここをクリックします)」をクリックします。「Keystore settings (鍵ストア設定)」ウィンドウが表示されます。

3. 鍵ストア用のパスワードを入力して、再入力します。その他の鍵ストア設定についてはデフォルト値のままにして、「OK」をクリックします。

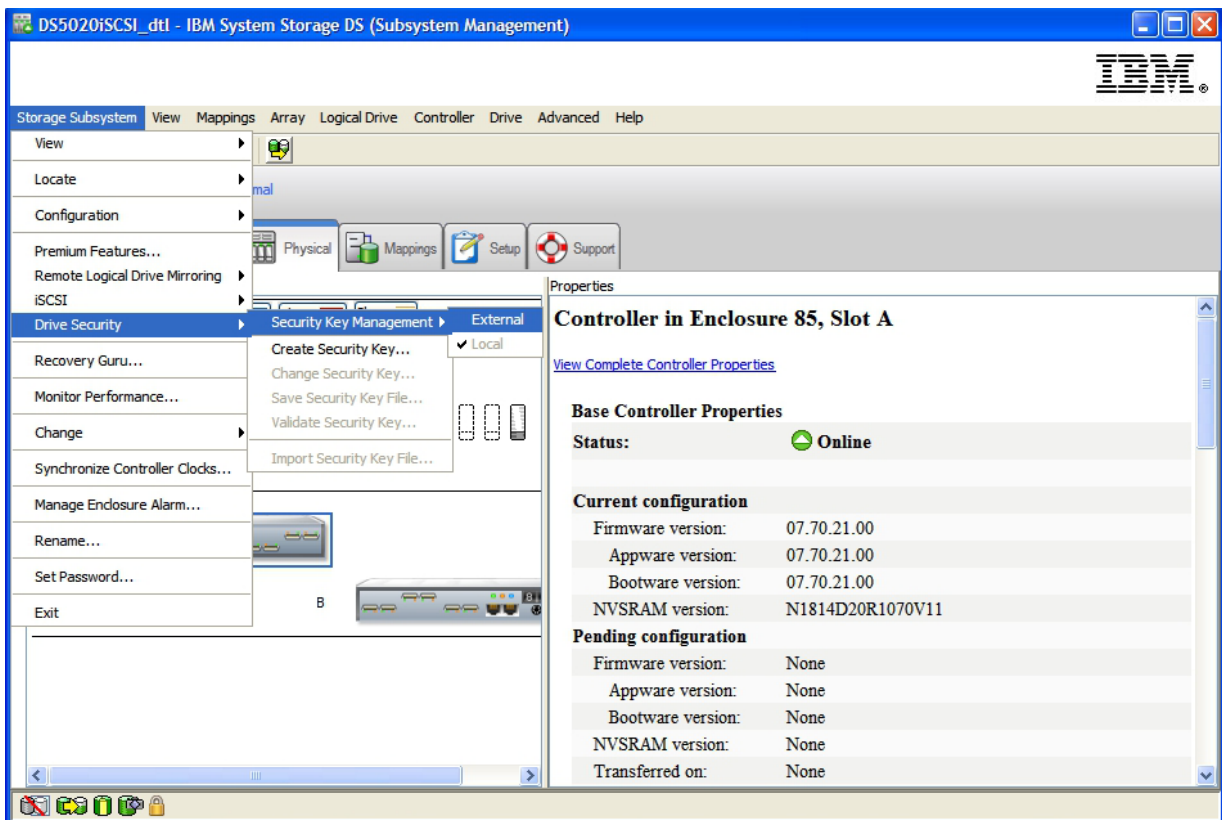


4. ウィンドウの左側にある「Welcome (ようこそ)」リンクをクリックします。「Welcome (ようこそ)」ウィンドウが開きます。
5. 「Key and Device Management (キーおよびデバイスの管理)」ボックスで、「Manage keys and devices (キーおよびデバイスの管理)」メニューから「DS5000」を選択して、「Go (実行)」をクリックします。「Key and Device Management (キーおよびデバイスの管理)」ウィンドウが開きます。

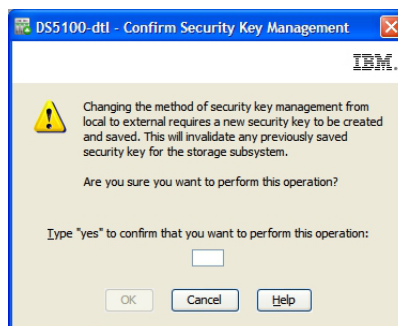


6. 「Confirm (確認)」プロンプトが表示されたら、「Cancel (キャンセル)」をクリックします。
7. ウィンドウの下部にあるドロップダウン・メニューで、「**Hold new device requests pending my approval (承認が保留中の新規デバイス要求を保持する)**」を選択します。
8. ストレージ・マネージャーを開いてログインし、構成しているストレージ・サブシステム用の「Subsystem Management (サブシステム管理)」ウィンドウを開きます。
9. 「Storage Subsystem (ストレージ・サブシステム)」 > 「Drive Security (ドライブ・セキュリティー)」 > 「Security Key Management (セキュリティー・キー管理)」 > 「External (外部)」をクリックします。

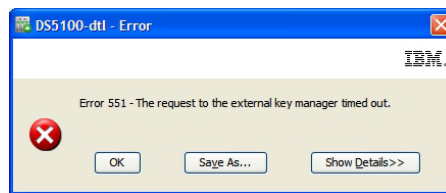
注: 外部キー管理プレミアム・フィーチャーが使用可能になっていない場合、「Storage Subsystem (ストレージ・サブシステム)」 > 「Drive Security (ドライブ・セキュリティー)」をクリックしたときにメニュー・オプション「Security Key Management (セキュリティー・キー管理)」は表示されません。



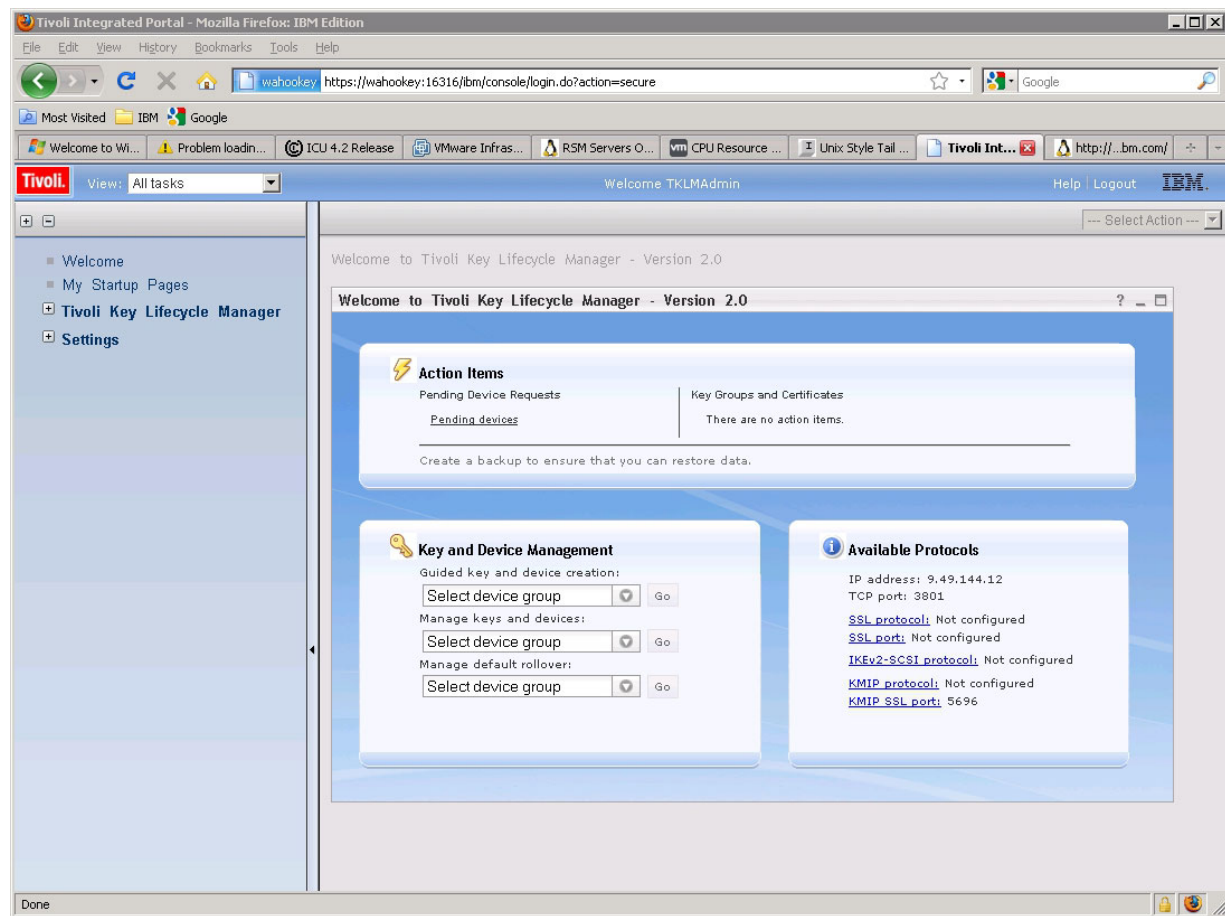
10. 「Confirm Security Key Management (セキュリティー・キー管理の確認)」ウィンドウでプロンプトが出されたら、yes と入力して、「OK」をクリックします。



11. プロンプトが出されたら、セキュリティー・キーのコピーを保存します。パスフレーズ、ファイル名、およびファイルの場所を入力して、「OK」をクリックします。コントローラーは、セキュリティー・キーを取得するために外部キー・マネージャーへの接続を試行します。失敗した場合、次のメッセージが表示されます。

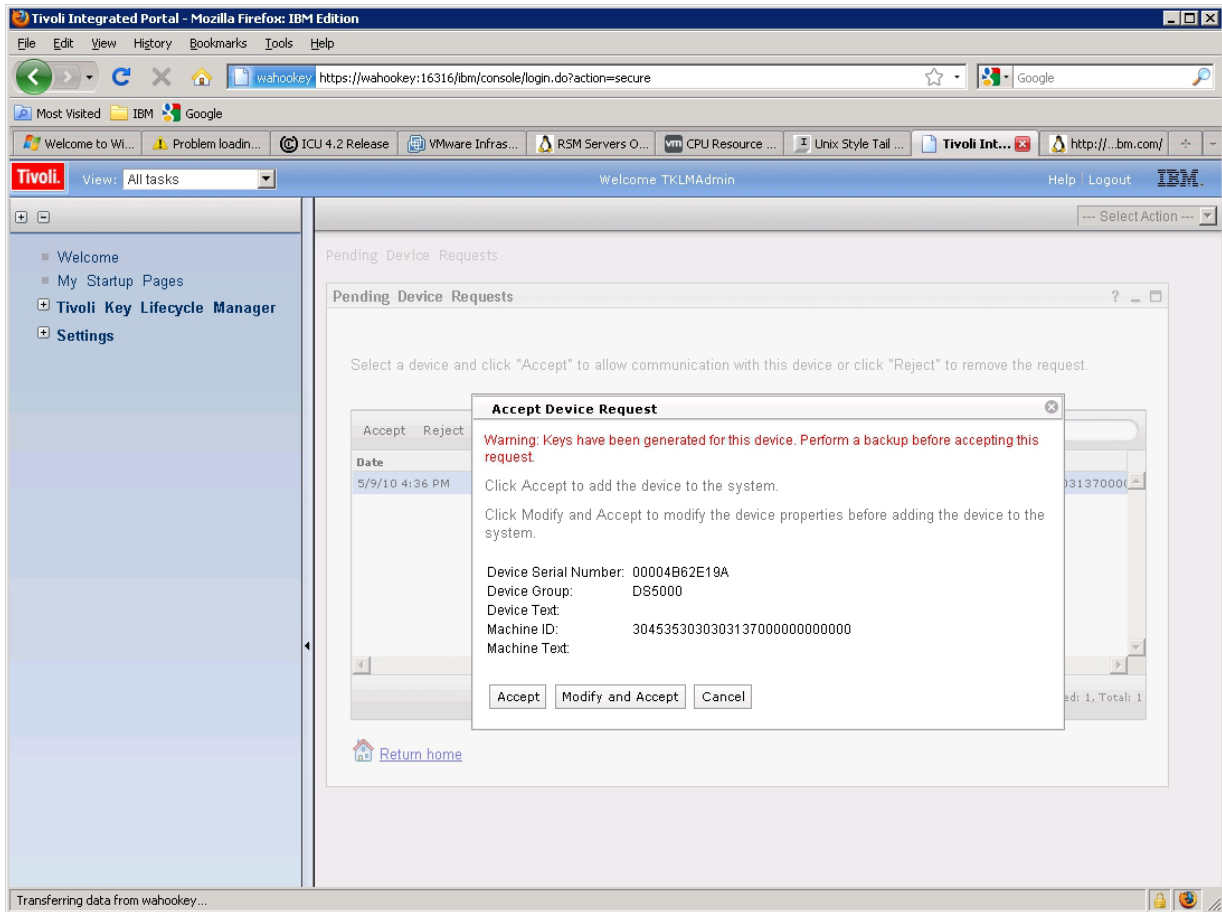


12. TKLM アプリケーションに戻り、「Action Items (アクション項目)」ボックスの「Pending devices (保留中のデバイス)」リンクをクリックします。



「Pending Device Request (保留中のデバイス要求)」ウィンドウが開きます。

13. リストからデバイスを選択して、「**Accept (受け入れる)**」をクリックします。「Accept Device Request (デバイス要求の受け入れ)」ウィンドウが開きます。
14. 「Accept Device Request (デバイス要求の受け入れ)」ウィンドウの「**Accept (受け入れる)**」をクリックします。



これで、TKLM サーバーはキーを DS TKLM プロキシ・コード・サーバーに送信する準備ができました。

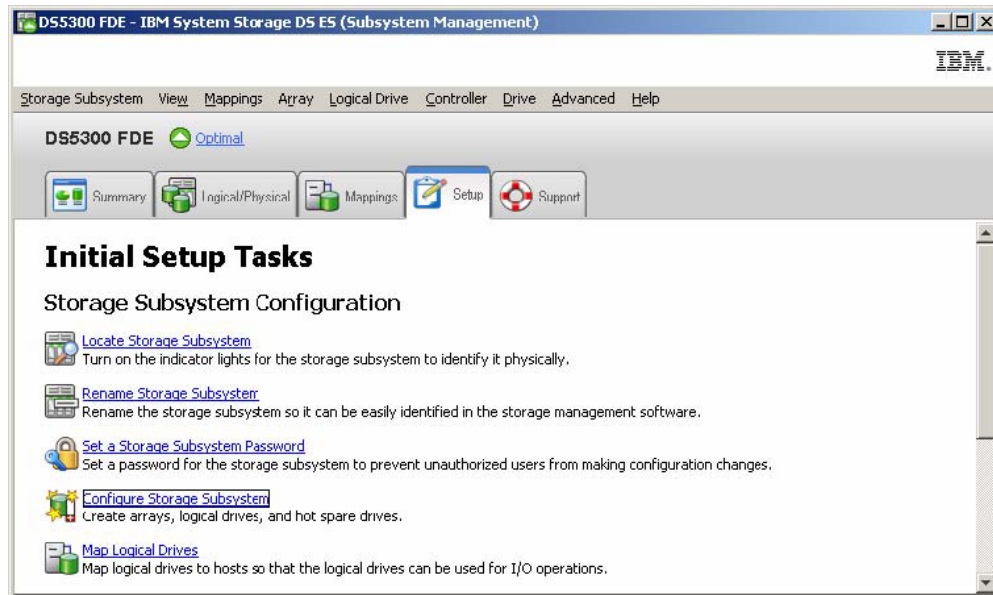
RAID アレイのセキュア化

アレイ内の FDE ドライブがセキュリティー有効にされている場合、アレイは保護されています。セキュア・アレイ内の FDE ドライブは、電源がオフにされたりストレージ・サブシステムから取り外されると、ロック状態になります。

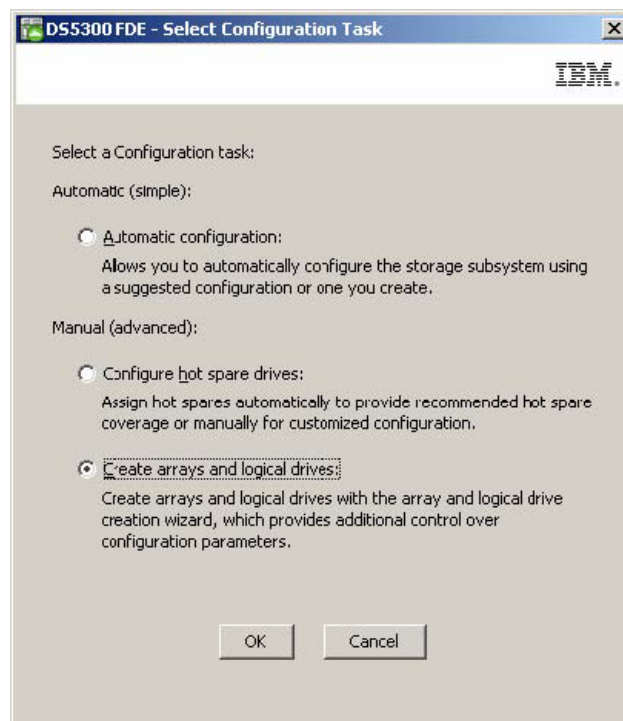
アレイ内のすべてのドライブは、セキュリティーが有効にされていないセキュリティー対応 FDE ドライブである必要があります。アレイには FlashCopy ベースの論理ディスク、あるいは FlashCopy リポジトリ論理ディスクを含むことはできません。基本論理ディスクおよび FlashCopy 論理ディスクは、セキュリティーが有効にされた後にのみ、ディスクへの書き込みが可能です。

RAID アレイを作成してセキュアにするには、次の手順を完了します。

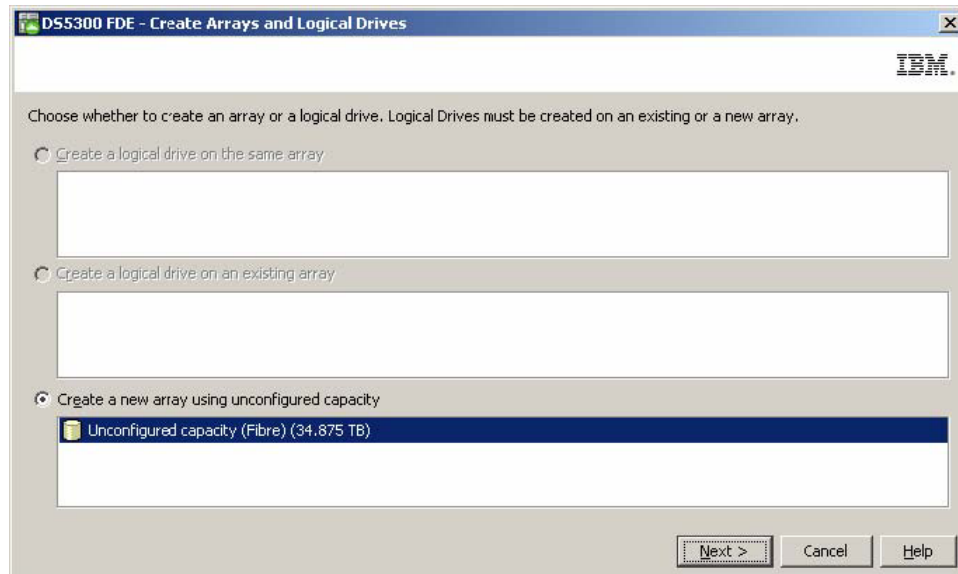
1. ストレージ・サブシステムで使用可能な FDE ドライブから RAID アレイを作成し、セキュアにします。「Setup (セットアップ)」ページから「**Configure Storage Subsystem (ストレージ・サブシステムの構成)**」をクリックします。



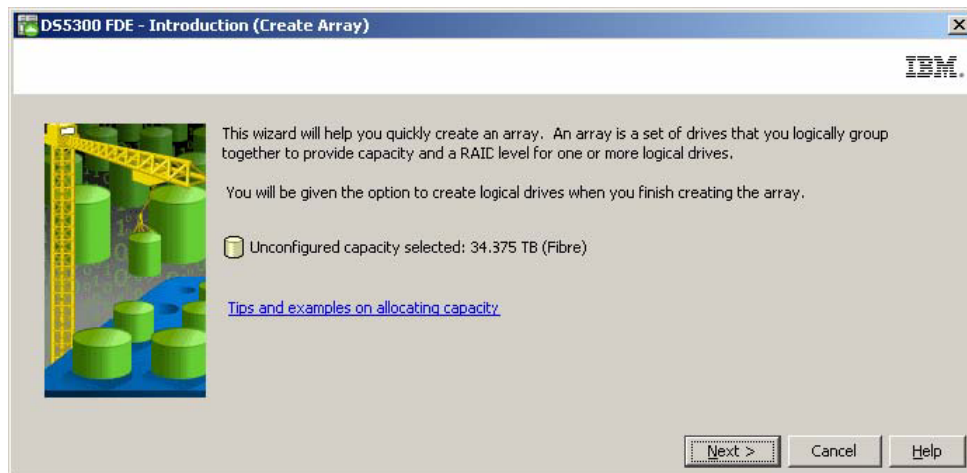
2. 「Select Configuration Task (構成タスクの選択)」ウィンドウで「**Manual (advanced) (手動 (拡張))**」、「**Create arrays and logical drives (アレイおよび論理ドライブの作成)**」、「**OK**」を順番にクリックします。



3. 「Create Arrays and Logical Drives (アレイおよび論理ドライブの作成)」ウィンドウで「**Create a new array using unconfigured capacity (未構成の容量を使用して新規アレイを作成)**」を選択します。DS5000 に他の (非 FDE) ドライブ・タイプが取り付けられている場合は、ファイバー・チャネル FDE ドライブのみを選択することを確認してください。「**Next (次へ)**」をクリックして先に進みます。

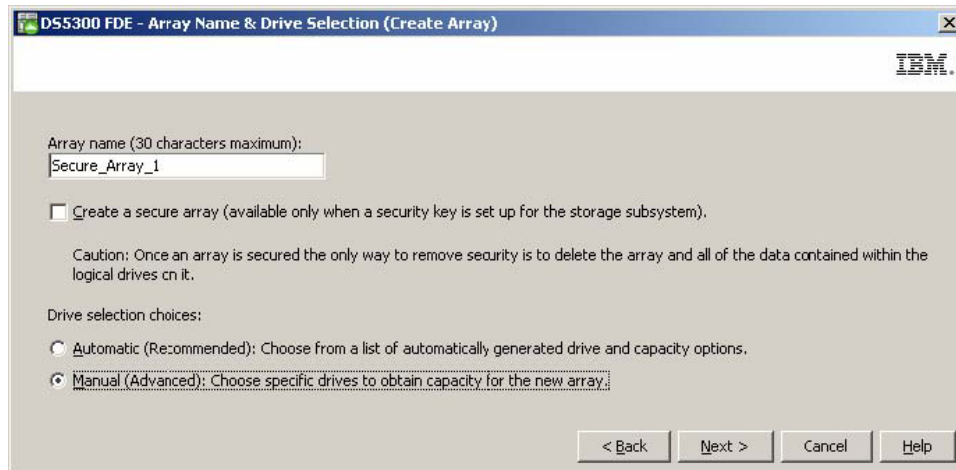


4. 「Create Array (アレイの作成)」ウィザードを使用してアレイを作成します。「**Next (次へ)**」をクリックして先に進みます。



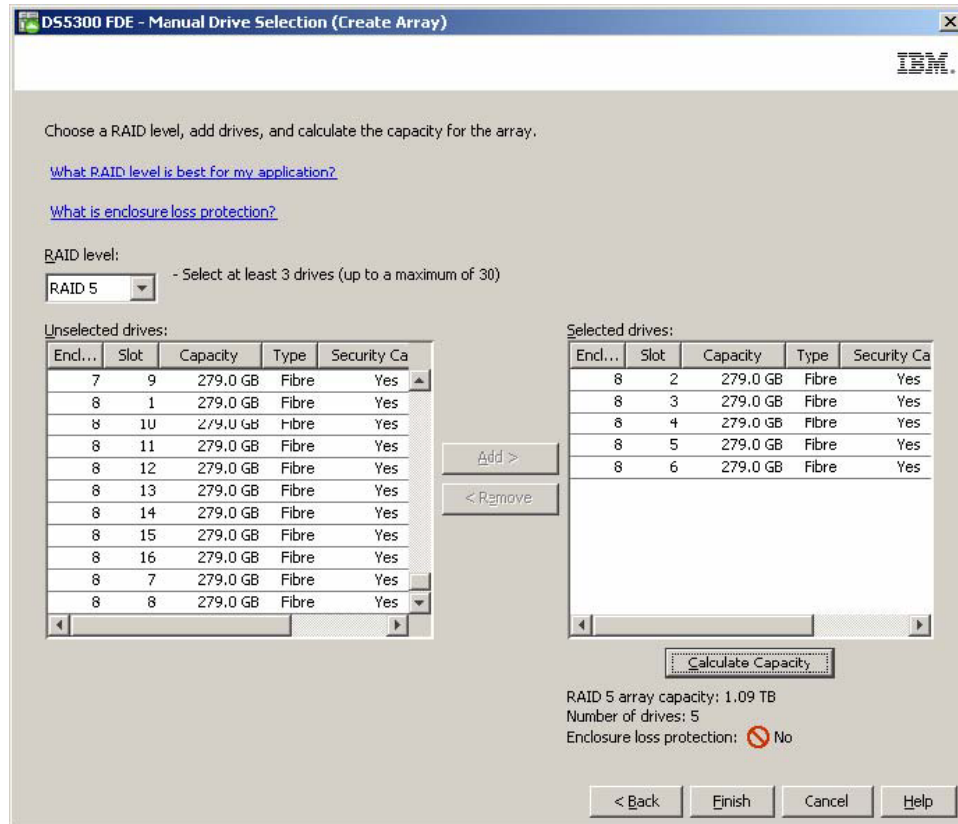
5. 「Array Name & Drive Selection (アレイ名およびドライブの選択)」ウィンドウで、アレイ名 (例: Secure_Array_1) を入力します。「**Create a secure array (セキュア・アレイの作成)**」チェック・ボックスが、このウィンドウで事前選択されていることに注意してください。「**Create a secure array (セキュア・アレイの作成)**」チェック・ボックスのチェックを外し、「**Disk selection choices (ディスク選択)**」の下の「**Manual (Advanced) (手動 (拡張))**」を選択します。「**Next (次へ)**」をクリックして先に進みます。

注: 「**Create a secure array (セキュア・アレイの作成)**」チェック・ボックスが表示され、フル・ディスク暗号化プレミアム・フィーチャーが使用可能にされている場合にのみ選択されています。アレイの作成時にこのチェック・ボックスを選択すると、作成されるアレイはセキュアになり、アレイをセキュアにするために「**Manual (Advanced) (手動 (拡張))**」オプションは必要ではなくなります。

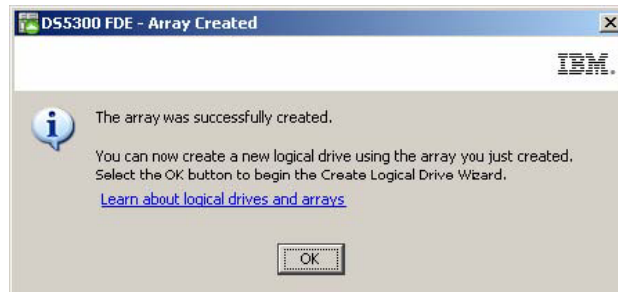


6. 「Manual Drive Selection (手動ドライブ選択)」ウィンドウでアレイ用のドライブを次のように構成します。
 - a. RAID レベルを選択します (例: RAID 5)。
 - b. 「**Unselected drives (未選択ドライブ)**」リストから使用したいセキュリティー対応ドライブを選択して「**Add (追加)**」をクリックし、「**Selected drives (選択済みドライブ)**」リストに追加します (例: ストレージ拡張エンクロージャー 8 から、スロット 2 から 6 のディスク・ドライブを選択します)。
 - c. 「**Calculate Capacity (容量の計算)**」をクリックして選択したドライブの総容量を計算します。
 - d. 「**Finish (完了)**」をクリックしてアレイを完成します。

注: これらのドライブはまだセキュアではありません。ドライブはこの後のプロセスでセキュアになります。

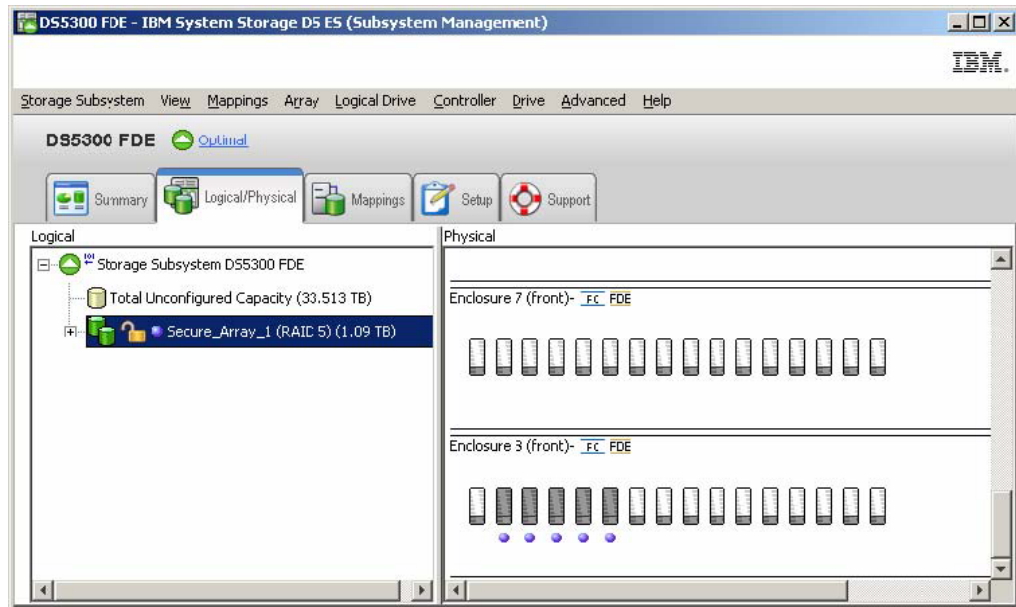


7. 「Array Created (アレイ作成完了)」ウィンドウで、「OK」をクリックしてアレイが正常に作成されたことを確認します。

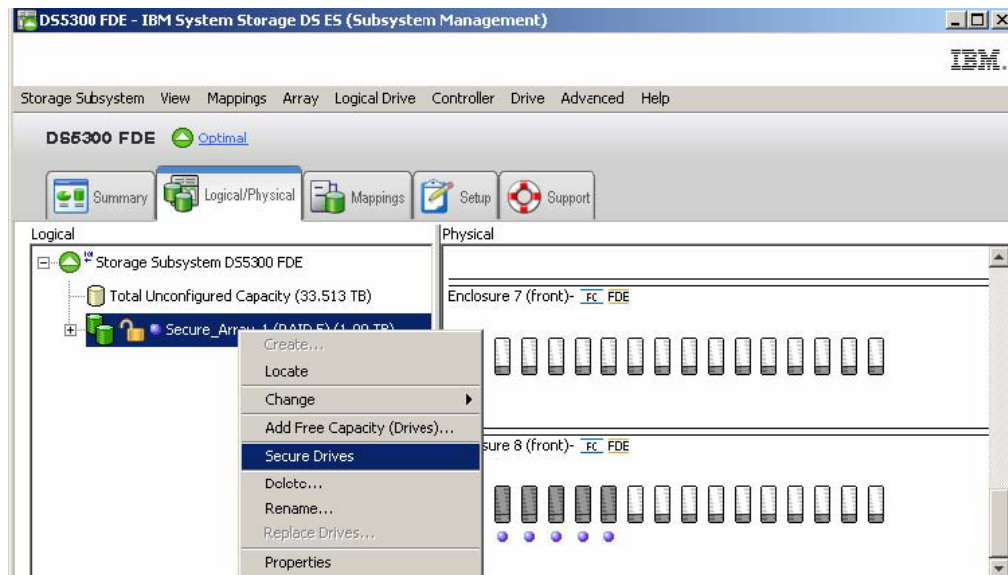


8. ウィザードでアレイ内に論理ドライブを作成するプロンプトが出されたら、ウィザードを使用して論理ドライブを作成します。論理ドライブが作成されたら、次のステップに進みます。論理ドライブの作成について詳しくは、61 ページの『第 4 章 ストレージの構成』を参照してください。
9. 作成したアレイを以下の手順でセキュアにします。
 - a. 「Subsystem Management (サブシステム管理)」ウィンドウで、「Logical/Physical (論理/物理)」タブをクリックします。

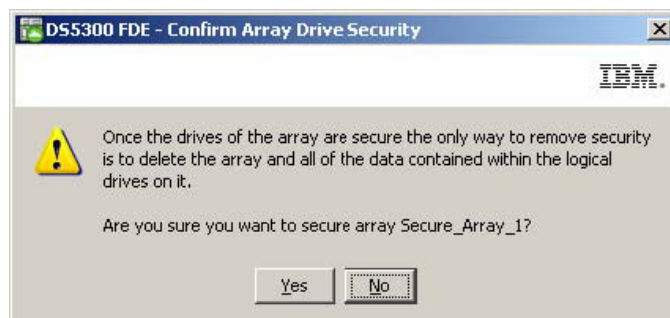
注: ウィンドウの右側にあるディスクのアイコンの下青色の点は、アレイを構成しているディスクを示しています。



- b. アレイのセキュリティーを有効にするには、アレイ名を右クリックし、次に「**Secure Drives** (ドライブのセキュア化)」をクリックします。

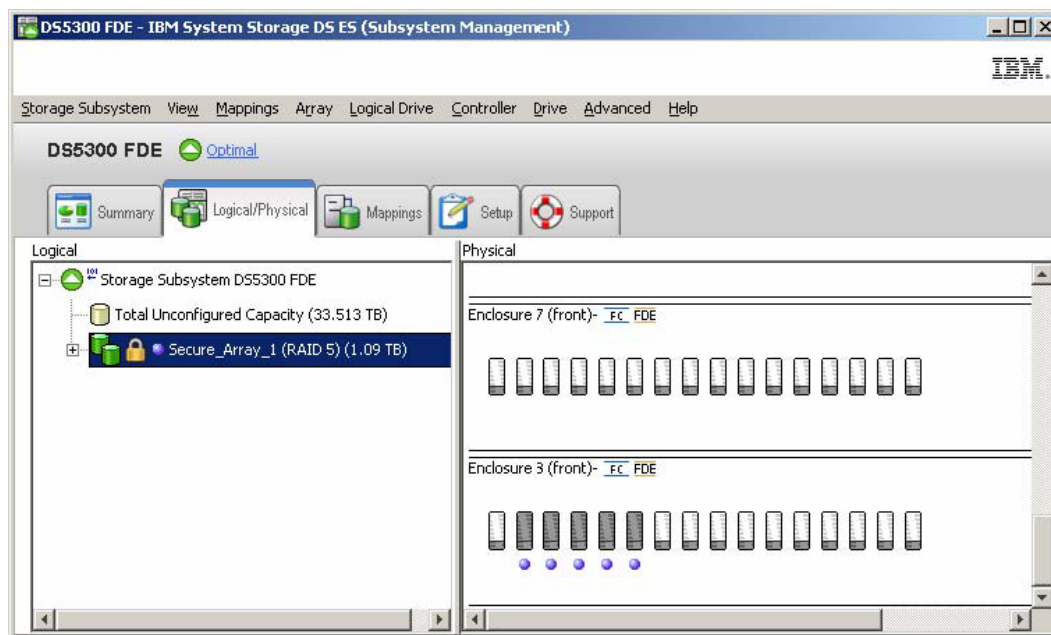


- c. 「Confirm Array Drive Security (アレイ・ドライブ・セキュリティーの確認)」ウィンドウで、「**Yes** (はい)」をクリックしてアレイをセキュアにします。



注:

- 1) ドライブを別のストレージ・サブシステムに移動させたり、ドライブがストレージ・サブシステムから取り外されている間に現行のストレージ・サブシステムで 3 回以上セキュリティー・キーを変更すると、ドライブをアンロックしてデータを読み取り可能に戻すために、パスフレーズ、セキュリティー・キー、およびセキュリティー・キー・ファイルが必要になります。
 - 2) アレイがセキュアになると、セキュリティーを除去する唯一の方法はアレイを削除することです。アレイの VolumeCopy を作成して他のディスクに保存することで、データへのアクセスを継続することができます。
10. 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Logical/Physical (論理/物理)**」タブをクリックし、アレイがセキュアであることを確認します。これはアレイ名の左のロック記号によって示されています。



ディスク・ドライブのアンロック

セキュリティー有効 FDE ドライブは、電源がオフにされたりストレージ・サブシステムから取り外されるとロックされます。これは、ストレージ・サブシステムのディスク暗号化および FDE ドライブの重要な機能です。ロック状態により、許可されていないユーザーに対してデータは読み取り不能になります。

重要: ストレージ・サブシステムが外部キー管理モードであり、サブシステム構成に最適な非 FDE ドライブまたは非セキュア FDE ドライブがない場合、ストレージ・サブシステムが正常にブートするためには、バックアップ・セキュリティー・ファイルおよび関連するパスフレーズを指定してドライブをアンロックする必要があります。

FDE ドライブがロック状態になる原因の条件は、使用しているセキュリティー・キー管理のタイプによって異なります。ローカル・セキュリティー・キー管理では、キーはコントローラー内部に保管されます。コントローラーが常に現行および以前のセキュリティー・キーを保持しているため、セキュリティー・キー・ファイルはストレージ・サブシステムの電源サイクルのたびに、あるいはドライブを同じストレージ・サブシステム内で取り外しと再挿入をするたびに、毎回必要なわけではありません。ただし、ドライブが他のストレージ・サブシステムに移された場合、あるいはストレージ・サブシステムからディスクが取り外されて

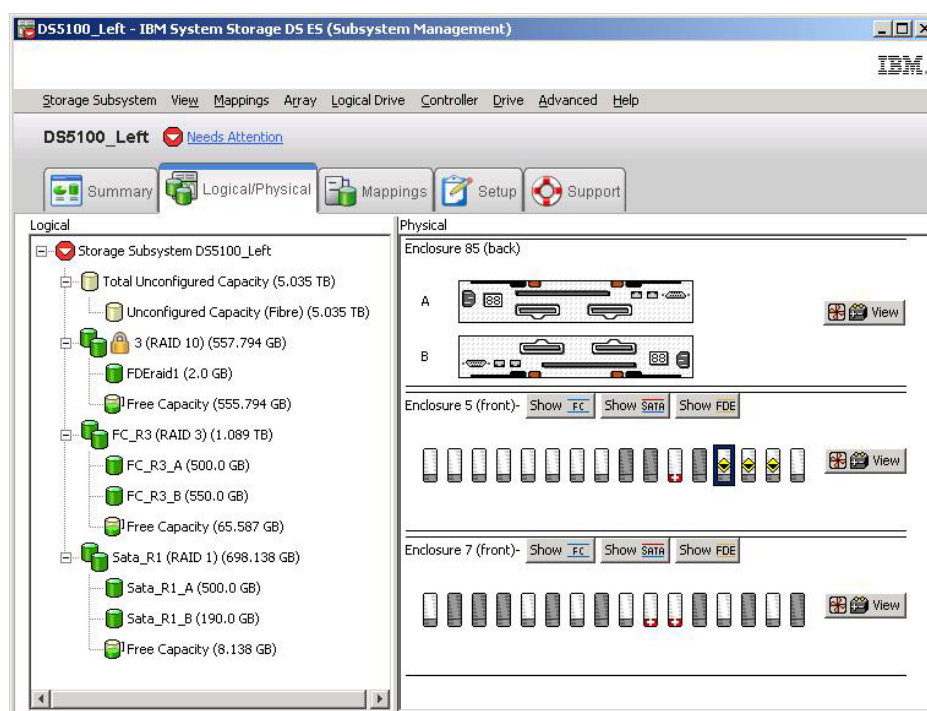
いる間に同じストレージ・サブシステム内のセキュリティー・キーが 3 回以上変更された場合は、ドライブをアンロックするにはパスフレーズとセキュリティー・ファイルが必要です。

注: セキュリティー有効 FDE ドライブは、ファームウェア更新中あるいはコンポーネントの交換中はアンロック状態のままです。これらのドライブがロック状態になるのは、電源がオフあるいはストレージ・サブシステムから取り外されているときのみです。

外部セキュリティー・キー管理では、外部キー・マネージャー・アプリケーションが、元のサブシステムから新しいサブシステムに移動されたドライブをアンロックするためのセキュリティー・キーを提供します。ただし、新しいサブシステムがアプリケーションからアクセス可能であることが条件です。移動されたドライブをアンロックするためには、新しいサブシステムが外部キー・マネージャー・アプリケーションに接続されている必要があります。外部キー・マネージャー・アプリケーションとストレージ・サブシステムとの通信が中断された場合、通信が再確立されるか、あるいはバックアップ・セキュリティー・キー・ファイルによってドライブがアンロックされるまで、ドライブをアンロックできません。

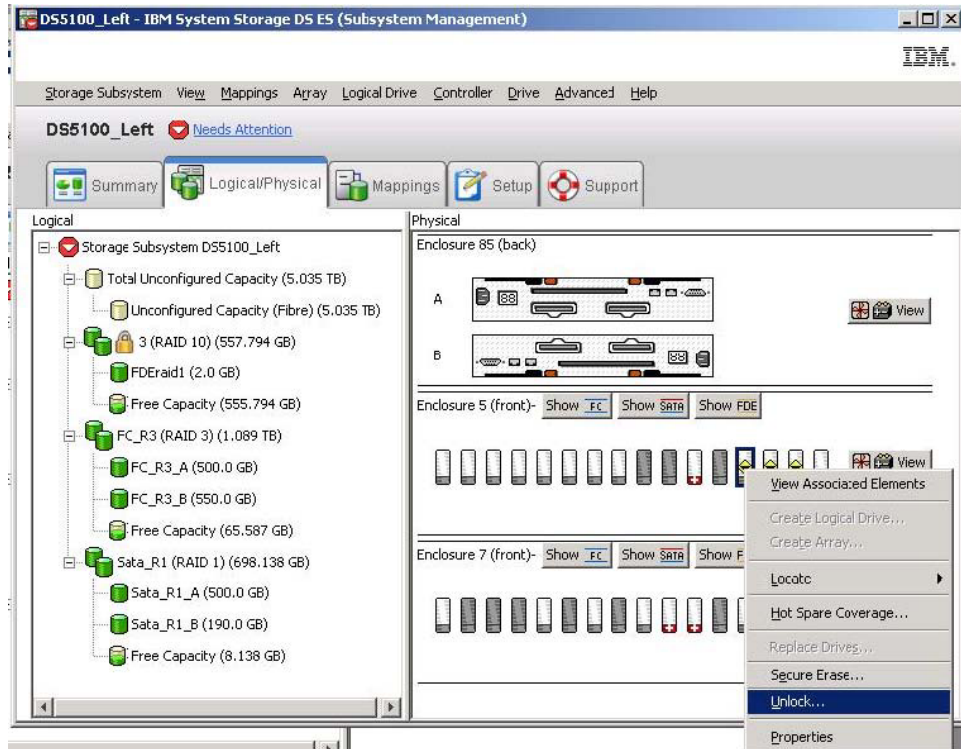
バックアップ・セキュリティー・キー・ファイルを使用してロック状態の FDE ドライブをアンロックするには、以下の手順を実行します。

1. 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Logical/Physical (論理/物理)**」タブをクリックします。



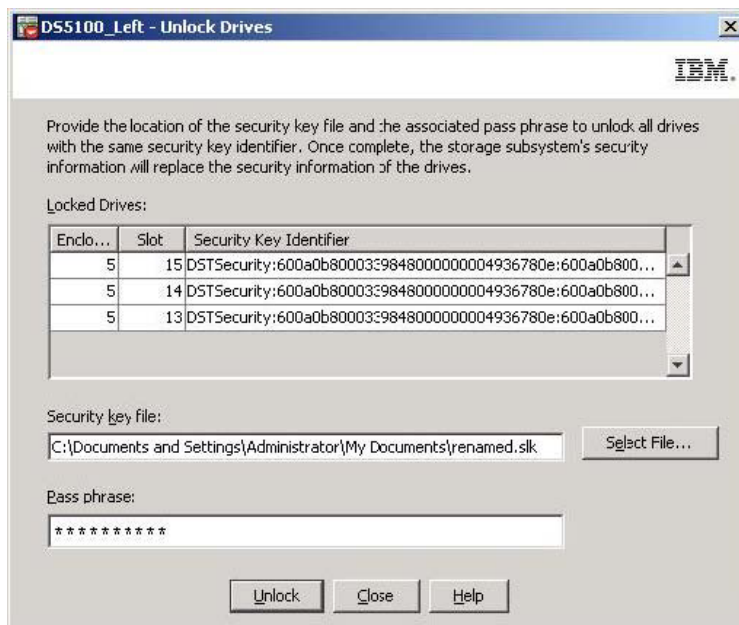
2. アンロックしたいドライブを右クリックし、「**Unlock (アンロック)**」をクリックします。

注: 複数のドライブをアンロックする場合でも、1 つのドライブを選択するだけですみます。ストレージ・マネージャーは自動的にストレージ・サブシステム内でロック状態のドライブをすべてリストし、提供されたセキュリティー・キー・ファイルに対して各ドライブを検査してセキュリティー・キー・ファイルのキーが使用できるかを判別します。



3. 「Unlock Drives (ドライブのアンロック)」ウィンドウで、選択したロック状態のドライブがリストされます。これらのドライブをアンロックするには、セキュリティ・キー・ファイルを選択してパスフレーズを入力し、「Unlock (アンロック)」をクリックします。ストレージ・サブシステムは、パスフレーズを使用してセキュリティ・キー・ファイルからセキュリティ・キーを暗号化解除します。次にストレージ・サブシステムは、暗号化解除したセキュリティ・キーをドライブ上のセキュリティ・キーと比較し、セキュリティ・キーが一致したすべてのドライブをアンロックします。

注: ドライブは電源遮断が起きた後に電源オンされているため、認証プロセスはドライブがロック状態のときにのみ発生します。読み取りおよび書き込み操作のたびに繰り返すことはありません。



4. 「Unlock Drives Complete (ドライブのアンロックの完了)」ウィンドウで、「OK」をクリックしてドライブがアンロックされたことを確認します。これでアンロックされたドライブは、インポートされる準備ができました。

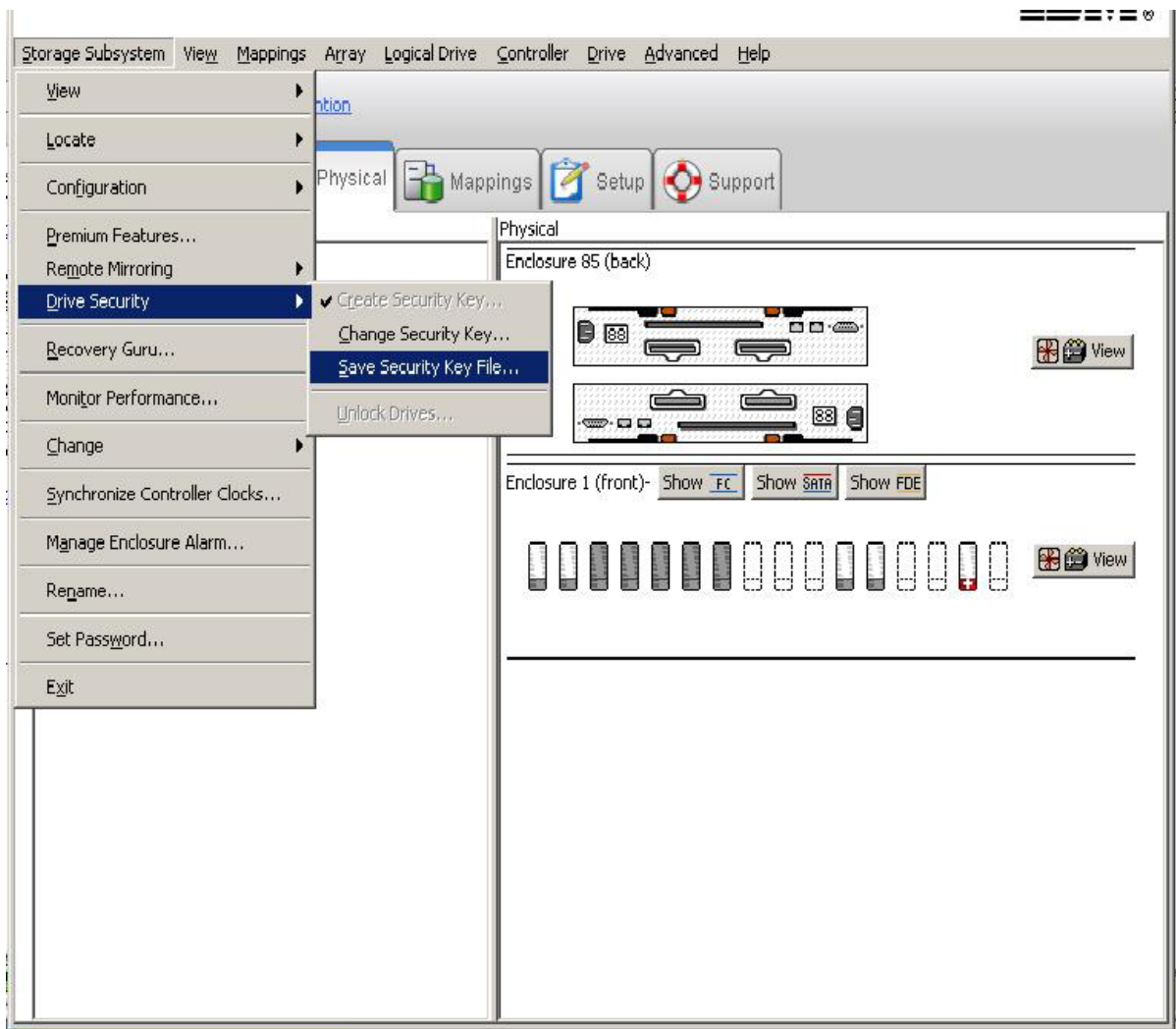


FDE ドライブを使用するストレージ・サブシステムのマイグレーション (ヘッド・スワップ)

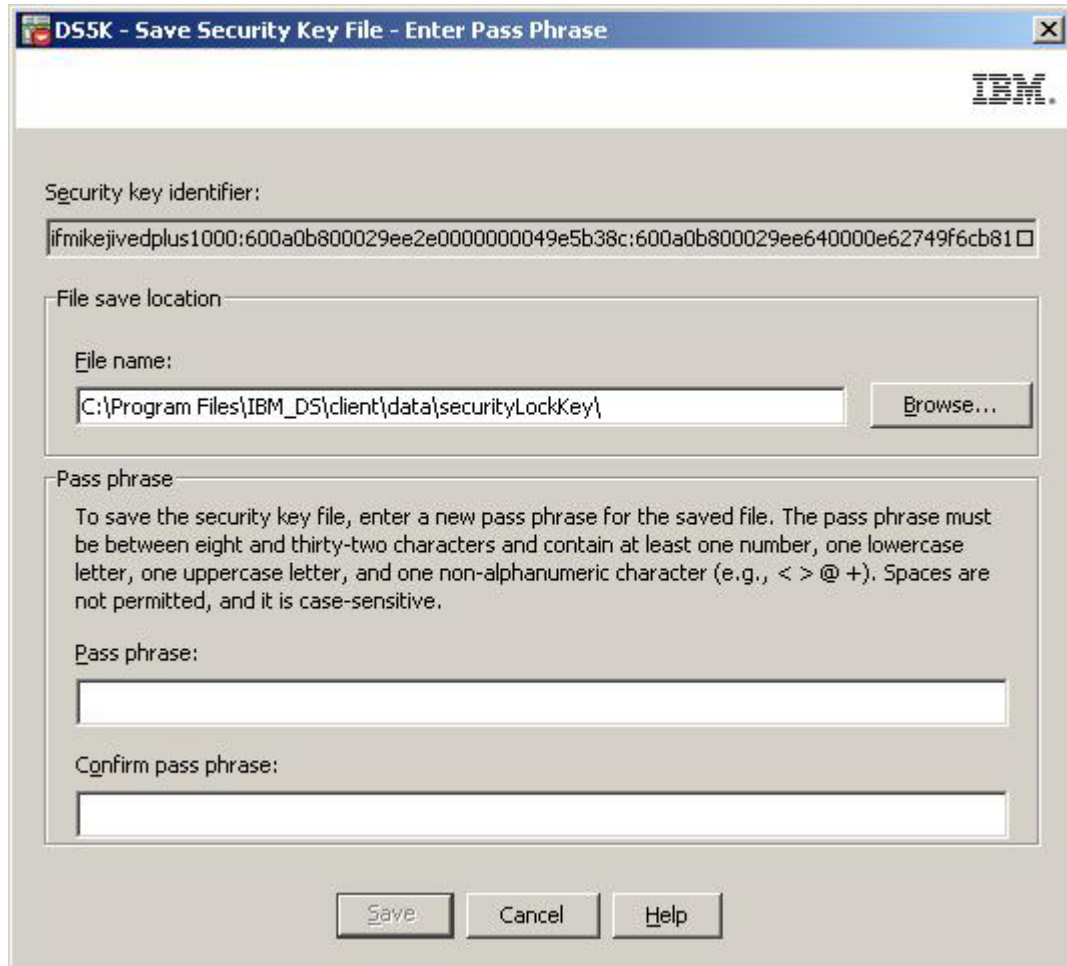
FDE 互換ストレージ・サブシステムでは、既存のディスク・グループのマイグレーション技法を使用して、ドライブを完全なストレージ・サブシステムとして別の FDE 互換ストレージ・サブシステムにマイグレーションすることができます。構成メタデータがストレージ・サブシステムのすべてのドライブに保管されているため、ユーザー・データはディスクにそのまま残ります。このセクションで説明されているいくつかの追加手順を使用することで、FDE セキュリティー有効ドライブをマイグレーションし、セキュアのまま残すことも可能です。

注:

1. 以下の手順では、セキュア・アレイに必要な追加のデータ・マイグレーションの手順についてのみ説明します。完全な情報および手順については、「IBM System Storage DS3000、DS4000、および DS5000 ハード・ディスク・ドライブおよびストレージ拡張エンクロージャーの取り付けとマイグレーションのガイド」を参照してください。
2. 以下のデータ・マイグレーション手順は、ストレージ・サブシステムの両方のコントローラーを交換する際にも適用されます。そのストレージ・サブシステム内のすべてのドライブが含まれます。両方のコントローラーを交換する場合は、部分的なマイグレーションはサポートされません。この場合、セキュリティー・ファイルが必要です。両方のコントローラーを交換する必要がある場合、現行のセキュリティー・キーをエクスポートするためのストレージ・サブシステムへの管理アクセス権限を持っていない可能性があります。
1. 既存のストレージ・サブシステムでドライブをアンロックするために使用しているセキュリティー・キーをセキュリティー・キー・ファイルに保存してから、既存のストレージ・サブシステムからドライブを取り外します。セキュリティー・キー、パズフレーズ、およびセキュリティー・キー・ファイルをエクスポートした後、セキュリティー・キー・ファイルを 1 つのストレージ・サブシステムから他のストレージ・サブシステムに転送することができます。
 - a. 「Subsystem Management (サブシステム管理)」ウィンドウで、「Storage Subsystem (ストレージ・サブシステム)」、「Drive Security (ドライブ・セキュリティー)」、「Save Security Key File (セキュリティー・キー・ファイルの保存)」を順番にクリックします。

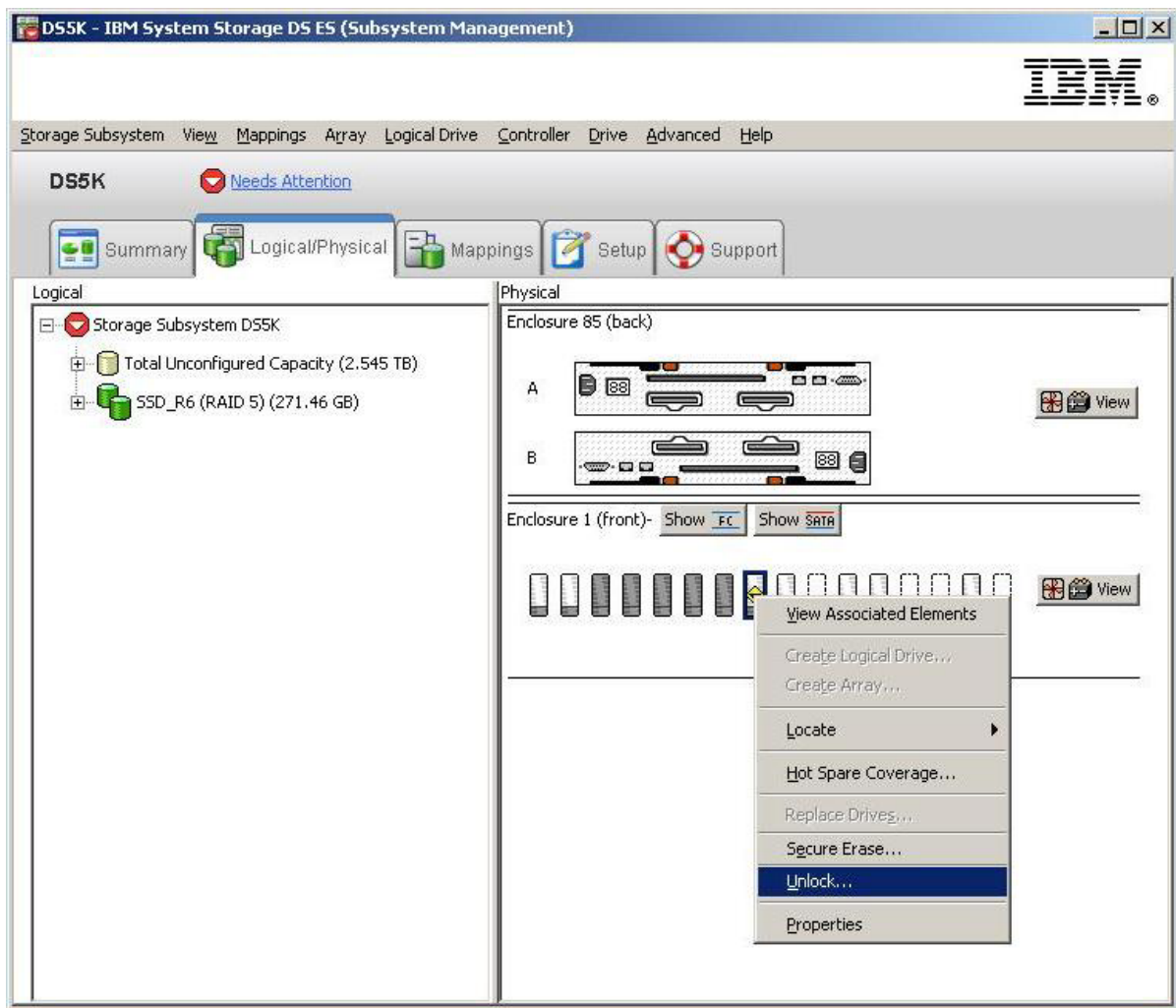


- b. 「Save Security Key File (セキュリティー・キー・ファイルの保存)」で「Pass Phrase (パスフレーズ)」ウィンドウに入り、ファイルの保存場所を選択し、パスフレーズを入力および確認して、「**Save (保存)**」をクリックします。

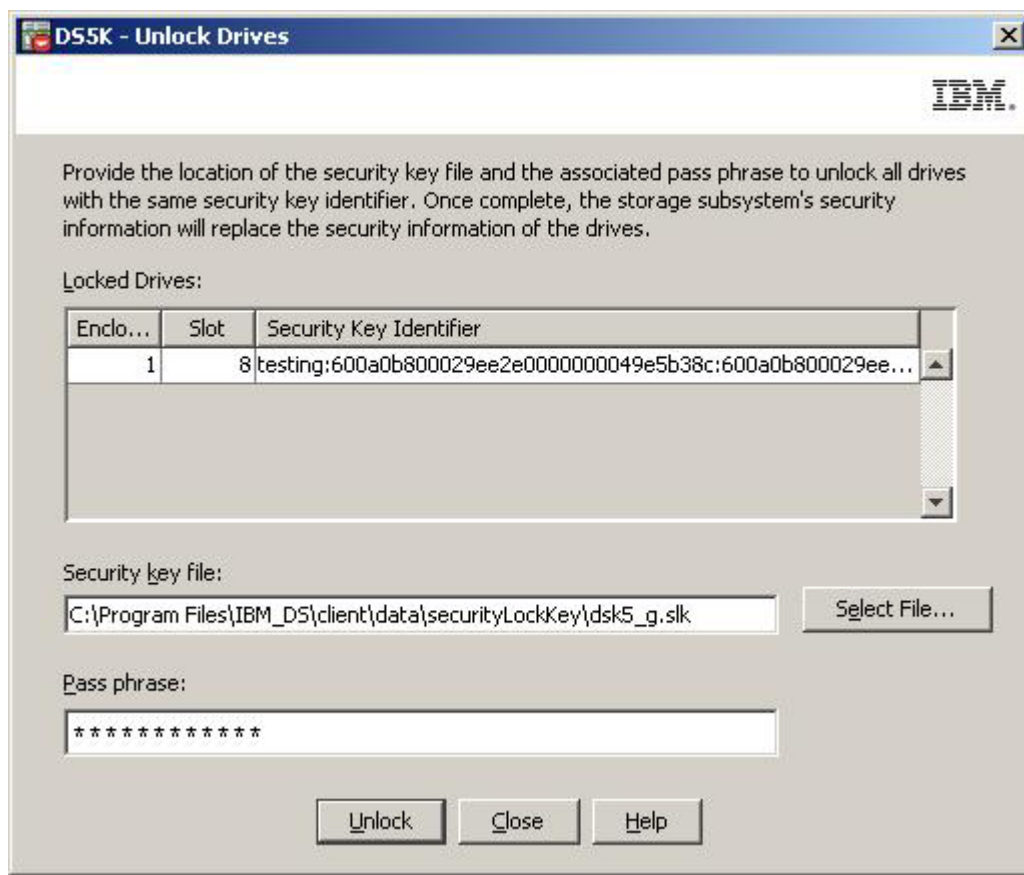


- c. 元のストレージ・サブシステムの定義済みアレイをエクスポートします。
 - d. サブシステムの電源をオフにして、以前のストレージ・サブシステム・コントローラー・エンクロージャーを新しいコントローラー・エンクロージャーに取り替えます。
 - e. 新しいストレージ・サブシステムの電源をオンにします。
2. 既存のストレージ・サブシステムのコントローラー格納装置を新しいコントローラー格納装置と交換した後、セキュリティ有効 FDE ドライブをアンロックしてから RAID アレイをインポートします。
 - a. 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Logical/Physical (論理/物理)**」タブをクリックします。
 - b. アンロックしたいドライブを右クリックし、「**Unlock (アンロック)**」をクリックします。

注: フル・ディスク暗号化プレミアム・フィーチャーが承諾されない可能性があります。ストレージ・サブシステムの FDE 機能を使用可能にするために、新しい FDE プレミアム・フィーチャー・キー・ファイルを生成します。



- c. 選択したドライブ用のセキュリティー・キー・ファイルを選択し、セキュリティー・キーのバックアップ・ファイルを保存した際に入力したパスフレーズを入力して、「**Unlock (アンロック)**」をクリックします。



ディスク・ドライブの消去

重要: セキュリティー有効 FDE ドライブのセキュア消去操作が完了すると、ディスク上のすべてのデータは永久的に消去されます。データを消去したいことが確実ではない場合は、この処置を実行しないでください。

セキュア消去は、従来の他の方法と比較して高水準のデータ消去を提供します。ストレージ・マネージャーを使用してセキュア消去を開始すると、暗号消去を実行するためのコマンドが FDE ドライブに送信されます。暗号消去によって既存のデータ暗号鍵が消去され、新しい暗号鍵をドライブ内部に生成することで、データの暗号化解除ができなくなります。暗号鍵が変更されると、変更前の暗号鍵によって暗号化されてディスクに書き込まれたすべてのデータは解読不能です。これは、すべてのビット、ヘッダー、およびディレクトリも含まれます。

セキュア消去が行われると、以下の処置が発生します。

- データは完全に、そして永久的にアクセス不能になり、ドライブは工場出荷時の状態に戻ります。
- ドライブ・セキュリティは使用不可になり、必要な場合はもう一度使用可能にする必要があります。

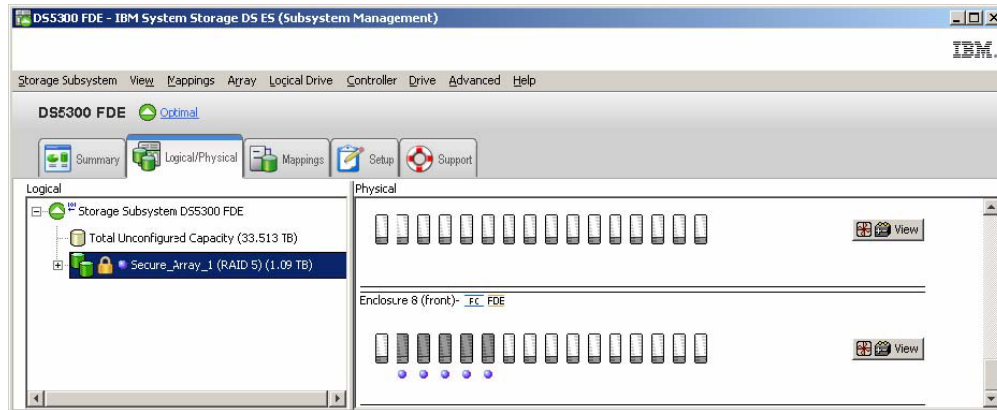
セキュア消去を開始する前に、セキュリティ有効 FDE ドライブをアンロックし、割り当て済みのアレイを削除する必要があります。

重要: 後でデータにアクセスしたい場合は、FDE ドライブをセキュア消去する前に、セキュリティ有効 FDE ドライブ内のデータを他のドライブまたはセキュア・テープにバックアップする必要があります。セキュリティ有効 FDE ドライブのセキュア消去操作が完了すると、ディスク上のすべてのデータは永久的

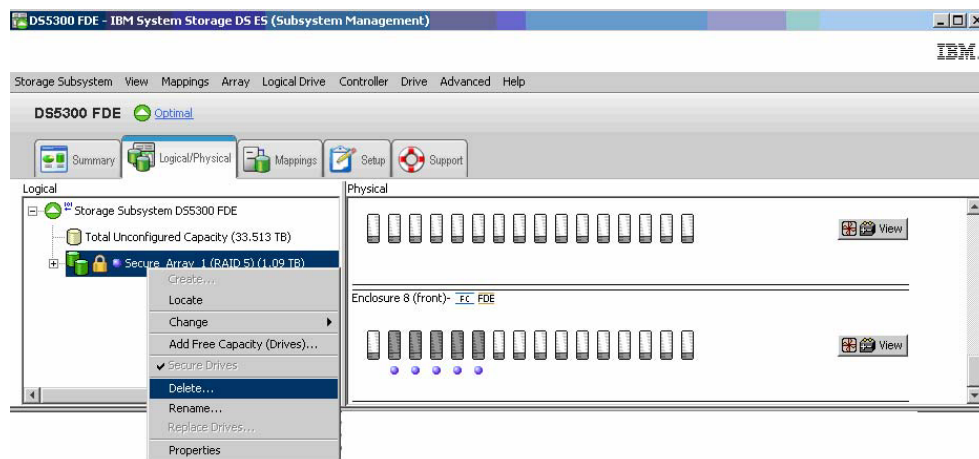
に消去されます。データを消去したいことが確実ではない場合は、この処置を実行しないでください。セキュア消去の不適切な使用は、データの消失をもたらします。

1. 次のようにドライブが関連する RAID アレイを削除し、ドライブを「Unassigned (未割り当て)」状態に戻すと、ドライブをセキュア消去することができます。

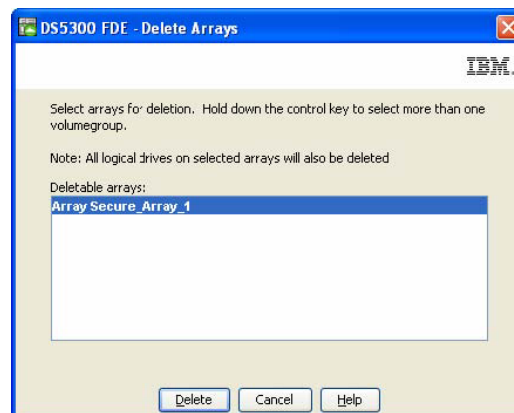
- a. 「Subsystem Management (サブシステム管理)」ウィンドウで、「**Logical/Physical (論理/物理)**」タブをクリックします。



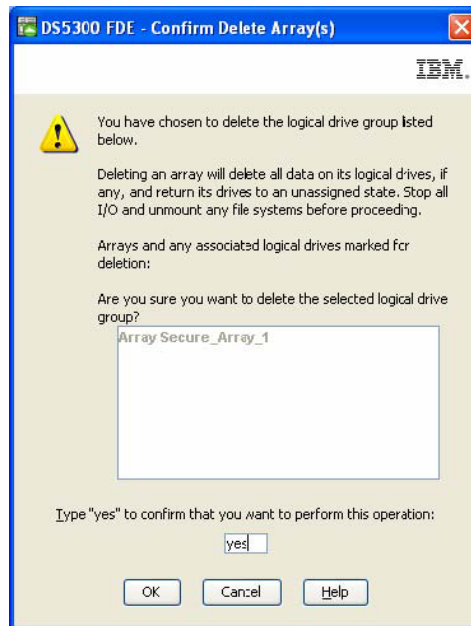
- b. アレイ名を右クリックし、次に「**Delete (削除)**」をクリックします。



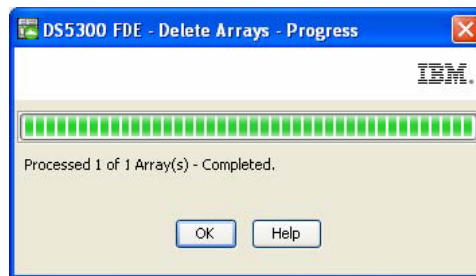
- c. 削除したいアレイを選択するようにプロンプトが表示されたら、アレイ名をクリックして「**Delete (削除)**」をクリックします。



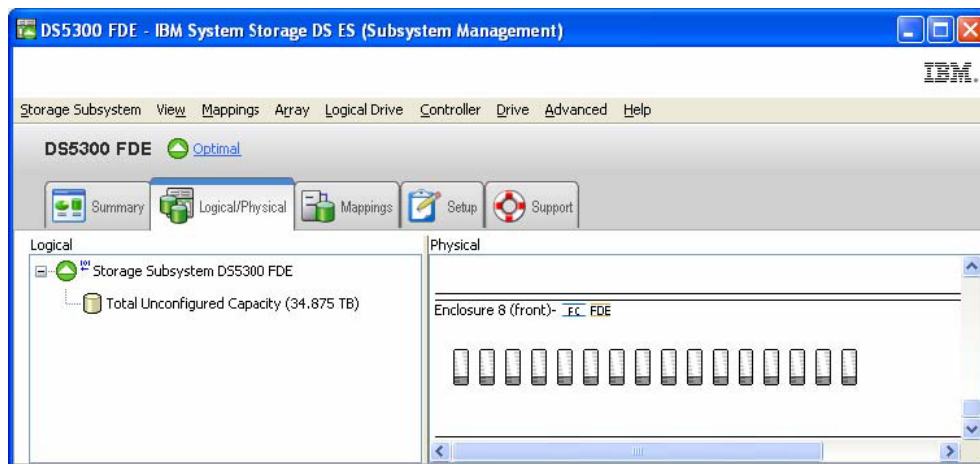
- d. アレイの削除を確認するために、フィールドに「yes」を入力して「OK」をクリックします。



- e. アレイの削除プロセスが完了するのを待ちます。「Processed 1 of array(s) - Complete」という確認が表示されたら、「OK」をクリックします。

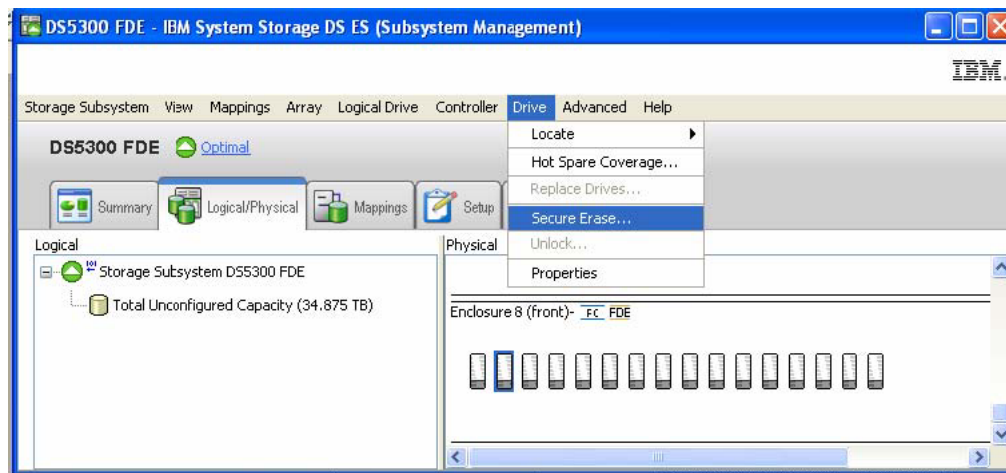


2. 「Subsystem Management (サブシステム管理)」ウィンドウで、「Logical/Physical (論理/物理)」タブをクリックします。

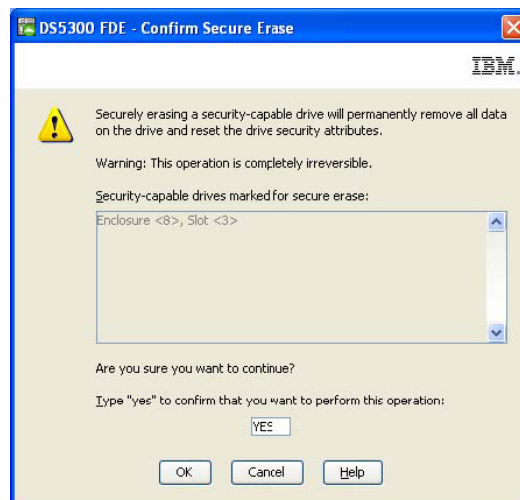


3. セキュア消去を実行したいドライブを選択します。Ctrl キーを押したまま選択することで、消去する複数のドライブを選択することができます。上部のメニュー・バーで、「Drive (ドライブ)」をクリック

クし、次に「Secure Erase (セキュア消去)」をクリックします。



4. ディスク上のすべてのデータを永久的に消去することを確認するために、フィールドに「yes」を入力して「OK」をクリックします。これで、ドライブは再利用あるいは廃棄することができます。



グローバル・ホット・スペア・ディスク・ドライブ

FDE 互換ストレージ・サブシステムでディスク・ドライブが故障すると、コントローラーは冗長データを使用して、故障したドライブ上のデータをグローバル・ホット・スペア・ドライブに再構成します。グローバル・ホット・スペア・ドライブは、介入操作なしで自動的に故障したドライブと置換されます。障害が起きたドライブの交換が完了すると、データはホット・スペア・ドライブから交換後の新しいドライブにコピーされて戻ります。

ホット・スペア・ドライブは、アレイのホット・スペア要件を満たしている必要があります。セキュア機能のあるアレイが構成されている場合は、ホット・スペア・ドライブとして以下のドライブ・タイプが必要です。ドライブが故障すると、ストレージ・マネージャーは故障したドライブのタイプに応じて、どのホット・スペア・ドライブと置換するかを自動的に判別します。

- セキュア FDE ドライブを持つアレイでは、そのドライブ以上の容量がある非セキュア FDE ドライブを、ホット・スペア・ドライブとする必要があります。非セキュア FDE ホット・スペア・ドライブが、セキュア RAID アレイで故障したドライブのスペアとして使用されると、セキュリティーが有効なドライブになります。

- ・ 非セキュア FDE ドライブを持つアレイでは、ホット・スペア・ドライブには非セキュア FDE ドライブあるいは非 FDE ドライブのいずれかを使用することができます。

注: 非セキュア FDE ホット・スペア・ドライブが、セキュア FDE が使用されていないアレイでスペアとして使用され、データがコピーして戻された後にアレイがセキュアにされた場合は、非セキュア FDE ホット・スペア・ドライブは保護されていないまま残り、ドライブがストレージ・サブシステムから取り外されるとドライブ内のデータは危険にさらされます。

未構成のセキュア FDE ドライブは、グローバル・ホット・スペアとして使用することはできません。グローバル・ホット・スペアがセキュア FDE ドライブの場合、セキュア・アレイのスペア・ドライブとしてのみ使用することができます。グローバル・ホット・スペア・ドライブが非セキュア FDE ドライブの場合、FDE ドライブを使用したセキュア・アレイまたは非セキュア・アレイ、あるいは非 FDE ドライブを使用したアレイでスペア・ドライブとして使用することができます。FDE ドライブをグローバル・ホット・スペア・ドライブと使用できるようにするために、非セキュア状態に変更するには、FDE ドライブをセキュア消去する必要があります。未構成のセキュア FDE ドライブをグローバル・ホット・スペアとして割り当てると、次のエラー・メッセージが生成されます。

Return code: Error 2 - The operation cannot complete because either (1) the current state of a component does not allow the operation to be completed, (2) the operation has been disabled in NVSRAM (example, you are modifying media scan parameters when that option (offset 0x31, bit 5) is disabled), or (3) there is a problem with the storage subsystem. Please check your storage subsystem and its various components for possible problems and then retry the operation.Operation when error occurred: PROC_assignSpecificDrivesAsHotSpares

グローバル・ホット・スペア・ドライブがセキュア・アレイで故障したドライブのスペアとして使用される際は、セキュア FDE ドライブになり、セキュア・アレイでスペアとして使用されている限りセキュア状態を維持します。セキュア・アレイの故障したドライブが交換され、グローバル・ホット・スペア・ドライブ内のデータが交換されたドライブにコピーされて戻ると、グローバル・ホット・スペア・ドライブはコントローラーによって自動的に再準備され、非セキュア FDE グローバル・ホット・スペア・ドライブになります。

セキュリティー非対応 SATA ドライブ、セキュリティー非対応のファイバー・チャネル・ドライブ、および FDE ファイバー・チャネル・ドライブ (セキュリティーが有効にされたドライブ、あるいは有効にされていないドライブ) の混用ディスク環境でのベスト・プラクティスとして、少なくとも 1 つのタイプのグローバル・ホット・スペア・ドライブ (FDE ファイバー・チャネルおよび SATA ドライブ) をアレイ内の最大容量で使用してください。セキュア対応の FDE ファイバー・チャネルおよび SATA ホット・スペア・ドライブが含まれている場合、すべてのアレイが保護されます。

87 ページの『グローバル・ホット・スペア・ドライブの構成』の標準ホット・スペア・ドライブ構成のガイドラインに従ってください。ホット・スペア構成のガイドラインは FDE ドライブについても同じです。

ログ・ファイル

ストレージ・マネージャーの主要イベント・ログ (MEL) には、ストレージ・サブシステムにおけるすべてのセキュリティーの変更について示すメッセージが含まれます。

よくある質問

このセクションでは、FDE に関するよくある質問をリストします。質問と回答は以下のカテゴリーで編成されています。

- 『アレイの保護』
- 259 ページの『セキュア消去』
- 259 ページの『ローカル・セキュリティ・キー管理』
- 259 ページの『外部セキュリティ・キー管理』
- 260 ページの『プレミアム・フィーチャー』
- 260 ページの『グローバル・ホット・スベア・ドライブ』
- 261 ページの『ブート・サポート』
- 261 ページの『ロックおよびアンロック状態』
- 261 ページの『バックアップおよびリカバリー』
- 261 ページの『その他』

アレイの保護

- FDE ドライブを使用した非セキュア・アレイを、セキュア・アレイに変更することはできますか？
 - はい。この処理を完了するための手順は 240 ページの『RAID アレイのセキュア化』で説明しています。DS5000 の暗号化フィーチャーが使用可能にされ、セキュリティ・キー・ファイルおよびパスフレーズが設定済みである必要があります。詳しくは、232 ページの『プレミアム・フィーチャーの使用可能化』を参照してください。
- アレイ上でセキュリティを有効にする際、そのアレイにすでに書き込まれているデータは消失あるいは消去されますか？
 - いいえ。アレイ・ディスク・ドライブでセキュア消去を実行しない限りは、データはそのまま残ります。
- FDE ドライブを使用したセキュア・アレイを、非セキュア・アレイに変更することはできますか？
 - いいえ。このオプションはサポートされません。非セキュア・アレイをセキュア・アレイに変更すると、セキュリティ有効 FDE ドライブ内のデータを破棄せずに非セキュア・アレイに戻すことはできません。VolumeCopy (ボリューム・コピー) を使用してセキュア・データを非セキュア・アレイにコピーするか、セキュア・テープにデータをバックアップしてください。セキュア・データを非セキュア・アレイに VolumeCopy する場合、ドライブを物理的に保護する必要があります。次に、オリジナルのアレイを削除し、アレイ・ドライブをセキュア消去する必要があります。そのドライブを使用して新しい非セキュア・アレイを作成し、VolumeCopy (ボリューム・コピー) を使用してオリジナルのドライブにデータをコピーして戻すか、あるいはセキュア・テープからデータをリストアします。
- セキュア FDE ドライブを使用したアレイがある場合に、同じドライブを使用してセキュリティを有効にしない別のアレイを作成することはできますか？ストレージ・サブシステムは、これが発生しないようにコントロールしますか？
 - いいえ。これらの機能はサポートされません。論理ドライブがあるドライブのセキュリティが有効なため、アレイ内のあらゆる論理ドライブは必ずセキュアになります。
- セキュア・アレイが削除される際、ディスクのセキュリティは有効のまま残りますか？
 - はい。セキュリティを無効にする唯一の方法は、セキュア消去またはドライブのリプロビジョニングを実行することです。
- 未割り当て/未構成のセキュリティ有効 FDE ディスクのセット上に新しいアレイを作成する場合、自動的にセキュアになりますか？

- はい。

セキュア消去

- セキュア消去を使用すると、何を消去することができますか? (個々のドライブですか? アレイですか?)
 - セキュア消去は個々のドライブ上で実行されます。アレイを構成しているセキュア・ドライブを消去することはできません。最初にアレイを削除する必要があります。アレイが削除されてドライブが未割り当て状態になると、Ctrl キーを押したままセキュア消去するドライブを選択することで、一度の操作で複数のディスクを消去することができます。
- セキュア消去機能のみを使用したい場合でも、セキュリティー・キー ID とパスフレーズのセットアップが必要ですか?
 - はい。フル・ディスク暗号化機能を使用可能にしなければ、セキュア消去を使用することはできません。
- ドライブ上でセキュア消去が実行された後、そのドライブのセキュリティーは有効ですか、無効ですか?
 - セキュア消去の後、ドライブはセキュリティー対応 (非セキュア) 状態に戻ります。ドライブ上でセキュリティーは無効です。
- 不注意でドライブをセキュア消去した場合、ドライブ内のデータをリカバリーすることはできますか?
 - いいえ。ドライブがセキュア消去されると、ドライブ内のデータをリカバリーすることはできません。消失したデータはバックアップ・コピーからリカバリーする必要があります。セキュア消去の前に、データをセキュア・ドライブにバックアップしてください。

ローカル・セキュリティー・キー管理

- ストレージ・マネージャーまたはコントローラーからセキュリティー・キーを取得することはできますか?
 - いいえ。セキュリティー・キーはストレージ・サブシステム内で暗号化されています。セキュリティー・キーの保存操作を使用して、暗号化されたキーのみをセキュリティー・キー・ファイルにエクスポートすることができます。実際のセキュリティー・キーを表示することはできません。ストレージ・サブシステムには用心深いセキュリティー機能が実装されています。ストレージ・マネージャーは強力なパスワードを強制しますが、管理者権限には適切で厳しいコントロールが必要です。
- アンロック状態またはセキュリティー無効のドライブを紛失した場合、データが暗号化されていてもアクセスすることができますか?
 - はい。ドライブでセキュリティーが有効にされていないため、ドライブはアンロック状態のままで、データはアクセス可能です。
- セキュリティー・キーが悪意のある人の手に渡った場合、データを損失することなくセキュリティー・キーを変更することはできますか?
 - はい。セキュリティー・キーの変更手順を使用して、ドライブのキーを再設定することが可能です。

外部セキュリティー・キー管理

- 外部セキュリティー・キー管理は、ローカル・セキュリティー・キー管理とどのように違うのでしょうか。
 - 外部セキュリティー・キー管理では、ストレージ・サブシステム・コントローラー内部で収容され、難読化されたセキュリティー・キーを使用する代わりに、ネットワーク上のセントラル・キー・ロケーションを使用してさまざまなストレージ・サブシステム用のキーを管理します。外部セキュリティー・キー管理は、IBM Tivoli Key Lifecycle Manager (TKLM) などの外部キー・ライセンス・マネー

ジャー・ソフトウェアによって容易に行うことができます。このソフトウェアがまだない場合は、ソフトウェアを購入してインストールし、プロキシ・サーバーを構成して外部セキュリティ・キー管理をセットアップする必要があります。

- セキュア・ドライブをストレージ・サブシステム間で移動する際、保存されたセキュリティ・ファイルにアクセスする必要がありますか？
 - いいえ、新しいストレージ・サブシステムがプロキシ・サーバーおよび外部キー管理ソフトウェアによって接続されて認識されている場合、ソフトウェアが自動的にドライブをアンロックするためのセキュリティ・キーを提供します。
- なぜ、サブシステムの電源を入れ直した後に、ストレージ・サブシステムにより、保存したセキュリティ・ファイルから手動でセキュリティ・キーを提供することを要求されるのですか？
 - サブシステムに少なくとも 1 つの非 FDE ドライブが取り付けられていないためです。

プレミアム・フィーチャー

- ミラーリングされたデータがセキュアであることをどのように確認しますか？ リモート・サイトでのデータの保護についてのベスト・プラクティスは何ですか？
 - 1 次および 2 次サイトの両方でセキュリティ有効 FDE ドライブを使用することで、データを保護します。また、1 次および 2 次サイトの間でデータを転送中に、そのデータが保護されていることを確認する必要があります。
- セキュア論理装置番号 (LUN) から非セキュア LUN へのコピーに VolumeCopy (ボリューム・コピー) を使用できますか？ 可能な場合、何者かによってコピーが行われること、および非セキュア・コピーを盗まれることをどのように防止しますか？
 - はい。この方法を使用して何者かがデータを盗難することを防ぐには、DS5000 ストレージ・サブシステム用の用心深いセキュリティ機能を実装します。ストレージ・マネージャーは強力なパスワードを強制しますが、管理者権限には適切で厳しいコントロールが必要です。
- FlashCopy および VolumeCopy データはセキュアですか？
 - はい。FlashCopy では、ターゲット FlashCopy データがセキュアな場合、FlashCopy リポジトリ論理ドライブもセキュアである必要があります。ストレージ・マネージャーは、この規則を実行します。同様に、VolumeCopy ペアのソース・アレイがセキュアな場合、VolumeCopy ペアのターゲット・アレイもセキュアである必要があります。

グローバル・ホット・スペア・ドライブ

- 未構成の FDE ドライブをグローバル・ホット・スペア・ドライブとして使用することはできますか？
 - はい。ただしドライブが非セキュア (セキュリティが有効ではない) 場合のみです。未構成の FDE ドライブの状況を確認してください。ドライブがセキュアな場合、グローバル・ホット・スペア・ドライブとして使用する前にセキュア消去するか、あるいはリプロビジョニングする必要があります。
- セキュア・アレイ内のホット・スペア・ドライブが非セキュア FDE ドライブの場合、セキュア FDE ドライブが故障してそのデータがホット・スペア・ドライブに書き込まれる際に、このドライブは自動的にセキュアになりますか？
 - はい。故障したドライブが RAID グループから削除されると、ホット・スペア・ドライブに対して再ビルドが自動的に開始されます。再ビルドが開始される前に、ホット・スペア・ドライブのセキュリティは有効になります。セキュア・アレイの再ビルドは、非 FDE ドライブには開始されません。セキュア・アレイの故障したドライブが交換され、グローバル・ホット・スペア・ドライブ内のデータが交換されたドライブにコピーされて戻ると、グローバル・ホット・スペア・ドライブはコントローラーによって自動的に再準備され、非セキュア FDE グローバル・ホット・スペア・ドライブになります。

ブート・サポート

- セキュリティー有効ドライブからのブートについて特別なプロセスはありますか?
 - いいえ。唯一の要件は、ストレージ・サブシステムが稼働していることです (これはすべてのブート・プロセスに必要です)。
- FDE ドライブはコールド・ブート・アタックに影響を受けやすいですか?
 - いいえ。サーバーへのアクセス権を得るためのブート・イメージを個人が作成可能なため、この問題はサーバー側に多く当てはまります。FDE ドライブには当てはまりません。FDE ドライブはコールド・ブート・アタックに影響を受けやすいタイプのメモリーを使用しません。

ロックおよびアンロック状態

- セキュリティー有効ドライブは、いつロック状態になりますか?
 - ドライブは、ディスクの電源がオフになると必ずロックされます。FDE ドライブが電源オフになるか切断されると、ディスク上のデータをロックして終了します。

バックアップおよびリカバリー

- 保存したデータがセキュアであることをどのように確認できますか?
 - 保存したデータのセキュア化については、本書の有効範囲外です。セキュア・テープ・バックアップに関する Storage Networking Interface Association (SNIA) のガイドラインを参照してください。具体的な解説については、「*IBM Full Disk Encryption Best Practices*」資料を参照してください。IBM Web サイト上のこの資料にアクセスするには、<http://www-947.ibm.com/support/entry/portal/docdisplay?lnocid=MIGR-5081492&brandind=5000028> にアクセスするか、以下の手順を実行します。
 1. IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) にアクセスします。
 2. Web ページの下部にある「**Search within all of support & downloads (サポート & ダウンロードの全体の検索)**」フィールドに「FDE」と入力して、Enter キーを押します。
 3. 検索結果のリストで、「**IBM Full Disk Encryption Best Practices - IBM System Storage (IBM フル・ディスク暗号化ベスト・プラクティス - IBM System Storage)**」リンクをクリックします。
 4. PDF ファイルへのリンクをクリックして、「*IBM Full Disk Encryption Best Practices (IBM フル・ディスク暗号化ベスト・プラクティス)*」資料を開くか、ダウンロードします。

その他

- DACstore 情報は引き続きディスクに書き込まれていますか?
 - はい。ただし、ドライブがセキュアな場合、コントローラーによってアンロックされるまでは DACstore 情報を読み取ることはできません。コントローラーのセキュリティー・キーが破損したり、両方のコントローラーが交換されるような頻度の低いことが起きたときには、セキュリティー・キー・ファイルを使用してドライブをアンロックする必要があります。
- コントローラー・キャッシュ上のデータは FDE および IBM ディスク暗号化によってセキュアですか? セキュアではない場合、ベスト・プラクティスがありますか?
 - いいえ。これはハードウェアへの物理アクセスのセキュリティー問題です。管理者には、ストレージ・サブシステム自身の物理的なコントロールおよびセキュリティーが必要です。
- セキュア対応ディスクを持っているが IBM ディスク暗号化プレミアム・フィーチャー・キーを購入していない場合、引き続きユーザー・インターフェースからセキュア対応ディスクを認識することができますか?

- はい。この情報は、ストレージ・マネージャー・インターフェースの複数のウィンドウから使用可能です。
- データ種別は何ですか?
 - データ種別に関する詳細は、SNIA ベスト・プラクティスを参照してください。具体的な解説については、「*IBM Full Disk Encryption Best Practices*」資料を参照してください。IBM Web サイト上のこの資料にアクセスするには、<http://www-947.ibm.com/support/entry/portal/docdisplay?lnocid=MIGR-5081492&brandind=5000028> にアクセスするか、以下の手順を実行します。
 1. IBM サポート・ポータル (<http://www.ibm.com/support/entry/portal>) にアクセスします。
 2. Web ページの下部にある「**Search within all of support & downloads (サポート & ダウンロードの全体の検索)**」フィールドに「FDE」と入力して、Enter キーを押します。
 3. 検索結果のリストで、「**IBM Full Disk Encryption Best Practices - IBM System Storage (IBM フル・ディスク暗号化ベスト・プラクティス - IBM System Storage)**」リンクをクリックします。
 4. PDF ファイルへのリンクをクリックして、「*IBM Full Disk Encryption Best Practices (IBM フル・ディスク暗号化ベスト・プラクティス)*」資料を開くか、ダウンロードします。
- ドライブを保護しない場合、FDE および非 FDE ドライブの両方を使用することはできますか?
 - はい。ただし、FDE と非 FDE ドライブの両方を使用することは、コスト効率の良い FDE ドライブの使用ではありません。FDE と非 FDE ドライブの両方を使用しているアレイは、後でセキュア・アレイに変換することはできません。
- FDE ディスク・ドライブの使用可能容量は、データの暗号化あるいは暗号化エンジンおよびキーのために必要な容量によって減少しますか?
 - いいえ。非 FDE ディスク・ドライブと FDE ディスク・ドライブで使用可能な容量は同じです (非暗号化 1 GB = 暗号化 1 GB)。

第 7 章 Troubleshooting (トラブルシューティング)

この章の情報をを使用して、ストレージ・マネージャーに関連した問題を診断および解決してください。ヘルプ、サービス、またはその他の技術支援の入手について詳しくは、xxi ページの『情報、ヘルプ、およびサービスの入手』を参照してください。

この章では、以下のトピックが扱われています。

- 『重大イベントの問題解決』
-
- 286 ページの『DS 診断データ・キャプチャー (DDC)』
- 289 ページの『AIX でのディスク・アレイのエラーの解決』

重大イベントの問題解決

重大イベントが発生した場合は、そのイベントがイベント・ログに記録されて、構成済みのすべての E メールおよび SNMP トラップの宛先に送信されます。重大イベントのタイプとセンス・キー、ASC、および ASCQ データがイベント・ログの詳細に表示されます。

重大イベントが発生して IBM サポートに連絡しようとする場合、カスタマー・サポート・バンドル機能を使用して、リモート・トラブルシューティングに役立つ各種データを収集して 1 つにまとめて添付することができます。カスタマー・サポート・バンドル機能を使用するには、以下の手順を実行してください。

1. 問題を示している論理ドライブの「Subsystem Management (サブシステム管理)」ウィンドウから、「Advanced (拡張)」 > 「Troubleshooting (トラブルシューティング)」 > 「Advanced (拡張)」 > 「Collect All Support Data (すべてのサポート・データの収集)」をクリックします。「Collect All Support Data (サポート・データをすべて収集)」ウィンドウが開きます。
2. 収集したデータの保存先のファイル名を入力するか、参照してファイルを選択します。「Start (開始)」をクリックします。

注: 収集されるデータの量によっては、圧縮ファイルの作成に数分かかります。

3. プロセスが完了したら、圧縮ファイルを電子メールで IBM サポートに送信して、トラブルシューティングを行ってもらうことができます。

264 ページの表 38 で、「Subsystem Management (サブシステム管理)」ウィンドウのイベント・ログに示される重大な優先順位のイベントについて、詳しく説明します。

表 38. 重大イベント

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 1001 - Channel failed (イベント 1001 - チャネルに障害が発生しました)	6/3F/C3	説明: コントローラーがチャネルに障害が発生したと判断したので、これ以上このチャネルのドライブにアクセスできません。センス・データの FRU グループ限定子 (バイト 26) に、障害のあるチャネルの相対チャネル番号が示されています。この状態が生じる原因は、通常、コントローラー宛先チャネルの 1 つに SCSI プロトコルを無視しているドライブがあることです。チャネルに対してリセットを発行し、ドライブがそのチャネルで SCSI バス・リセットを無視する状態が続いていることを検出すると、コントローラーは、そのチャネルに障害が発生したものとみなします。 処置: Recovery Guru を開始して、「Failed Drive SCSI Channel (障害のあるドライブの SCSI チャネル)」リカバリ手順にアクセスします。IBM サポートに連絡して、この手順を完了してください。
Event 1010 - Impending drive failure (PFA) detected (イベント 1010 - まもなくドライブ障害 (PFA) が発生する可能性があることを検出しました)	6/5D/80	説明: ドライブから、障害予測しきい値を超えたことが報告されました。これは、24 時間以内にこのドライブに障害が発生する可能性があることを示しています。 処置: Recovery Guru を開始して、「Impending Drive Failure (まもなくドライブ障害が発生する可能性があることを検出しました)」リカバリ手順をクリックします。指示に従って、障害を訂正してください。
Event 1015 - Incorrect mode parameters set on drive (ドライブに間違ったモード・パラメーターが設定されています)	6/3F/BD	説明: ドライブの現在の重大モード・ページの設定値について、コントローラーがそのドライブに照会できないか、それらの設定値を正しい設定値に変更できません。これは、「Request Sense data (センス・データの要求)」の「FRU」フィールドで指定されているドライブに対する Qerr ビットの設定が間違っていることを示しています。 処置: コントローラーには、まだ障害は発生していません。IBM サポートに連絡して、この重大イベントからリカバリするための指示を受けてください。
Event 1207 - Fibre Channel link errors - threshold exceeded (イベント 1207 - ファイバー・チャネル・リンク・エラー - しきい値を超えました)	なし	説明: ファイバー・チャネル・シグナルで無効文字が検出されました。ギガビット・インターフェース・コンバーター (GBIC) またはメディア・インターフェース・アダプターにおけるレーザーの劣化、ファイバー・チャネル・ケーブルの損傷または障害、またはループにおけるコンポーネント間のケーブル接続不良が、このエラーの原因と考えられます。 処置: メインの「Subsystem Management (サブシステム管理)」ウィンドウで、「Help (ヘルプ)」→「Recovery Procedures (リカバリ手順)」をクリックします。この障害からのリカバリについての詳細は、「Fibre Channel Link Errors Threshold Exceeded (ファイバー・チャネル・リンク・エラーしきい値を超えました)」をクリックしてください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 1208 - Data rate negotiation failed (イベント 1208 - データ速度の折衝に失敗しました)	なし	説明: コントローラーは転送リンク速度について自動折衝を行うことができません。コントローラーが作業日の最初の始動時に折衝を試行するまで、または信号が消失した後で再び信号を検出するまで、コントローラーはリンクがダウンしていると思なします。 処置: Recovery Guru を開始して「Data rate negotiation failed (データ速度の折衝に失敗しました)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。
Event 1209 - Drive channel set to Degraded (イベント 1209 - ドライブ・チャンネルが「劣化」に設定されました)	なし	説明: 入出力エラーが多すぎるため、または技術サポート担当員がアレイ管理者に、診断上またはその他のサポート上の理由でドライブ・チャンネルの状況を手動で設定するようにアドバイスしたために、ドライブ・チャンネルの状況が「劣化」に設定されました。 処置: Recovery Guru を開始して「Degraded Drive Channel (ドライブ・チャンネルの劣化)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。
Event 150E - Controller loopback diagnostics failed (イベント 150E - コントローラーのループバック診断が失敗しました)	なし	説明: コントローラーがドライブ側のファイバー・チャンネル・ループを初期化できません。診断ルーチンが実行されてコントローラーの問題であることが確認されたので、コントローラーがオフラインにされました。このイベントは、特定のコントローラー・モデルのみで発生します。 処置: Recovery Guru を開始して「Offline Controller (コントローラーのオフライン化)」リカバリー手順にアクセスし、その指示に従ってコントローラーを交換してください。
Event 150F - Channel miswire (イベント 150F - チャンネルの配線ミス)	なし	説明: 複数のドライブ・チャンネルが、同一のファイバー・チャンネル・ループに接続されています。これは、ストレージ・サブシステムが予想外の動作をする原因になることがあります。 処置: Recovery Guru を開始して「Channel Miswire (チャンネルの配線ミス)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。
Event 1510 - ESM blade miswire (イベント 1510 - ESM ブレードの配線ミス)	なし	説明: 同一のストレージ拡張エンクロージャー内の 2 つの ESMブレードが、同一のファイバー・チャンネル・ループに接続されています。冗長のレベルが失われ、このストレージ拡張エンクロージャーの入出力パフォーマンスが低下しています。 処置: Recovery Guru を開始して「ESM blade Miswire (ESM ブレードの配線ミス)」リカバリー手順にアクセスし、その指示に従って障害を修正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 1513 - Individual Drive - Degraded Path (イベント 1513 - 個別ドライブ - パスの機能低下)	なし	説明: 単一のドライブまたは複数のドライブへのパス上で、指定されたドライブ・チャンネルに偶発的なエラーが発生しています。 処置: Recovery Guru を開始して「Individual Drive - Degraded Path (個別ドライブ - パスの機能低下)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 1600 - Uncertified drive detected (イベント 1600 - 未認証のドライブを検出しました)	なし	説明: 未認証のドライブがストレージ・サブシステムに挿入されています。 処置: Recovery Guru を開始して「Uncertified Drive (未認証ドライブ)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 1601 - Reserved blocks on ATA drives cannot be discovered (イベント 1601 - ATA ドライブ上の予約済みブロックを検出できません)	なし	説明: ATA ドライブ上の予約済みブロックを認識できません。 処置: IBM サポートに連絡し、このイベントからリカバリーするための指示を受けてください。
Event 200A - Data/parity mismatch detected on logical drive (イベント 200A - 論理ドライブで、データ/パリティの不一致が検出されました)	なし	説明: メディア・スキャン操作で、論理ドライブ上のデータ・ブロックの一部とそれに関連付けられているパリティ・ブロックの間に不整合が検出されました。論理ドライブのこの部分のユーザー・データが失われた可能性があります。 処置: アプリケーション固有のツールが使用可能な場合はそれを選択して、論理ドライブ上のデータが正しいか検証してください。そのようなツールを使用できない場合、またはユーザー・データに問題があることが報告されている場合は、データが重要であれば、最新のバックアップから論理ドライブの内容全体をリストアしてください。
Event 202E - Read drive error during interrupted write (イベント 202E - 書き込みへの割り込み中に、ドライブ読み取りエラーが発生しました)	3/11/8A	説明: 書き込みへの割り込み中に、読み取り操作でメディア・エラーが発生しました。 処置: Recovery Guru を開始して、「Unrecovered Interrupted Write (リカバリーされなかった、割り込みが発生した書き込み)」リカバリー手順にアクセスします。IBM サポートに連絡して、この手順を完了してください。
Event 2109 - Controller cache not enabled - cache sizes do not match (イベント 2109 - コントローラー・キャッシュが使用不能です - キャッシュ・サイズが一致しません)	6/A1/00	説明: 両方のコントローラーの代替コントローラー・キャッシュ・サイズが同一でない場合は、コントローラーはミラーリングを使用可能にできません。両方のコントローラーのキャッシュ・サイズが同一であることを確認してください。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 210C - Controller cache battery failed (イベント 210C - コントローラー・キャッシュ・バッテリーに障害が発生しました)	6/0C/80	説明: バッテリーが物理的に存在していないか、完全に消耗しているか、または有効期限に達しているか、そのいずれかであることを、コントローラーが検出しました。 処置: Recovery Guru を開始して「Failed Battery CRU (バッテリー CRU の障害)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。
Event 210E - Controller cache memory recovery failed after power cycle or reset (イベント 210E - 電源再投入後またはリセット後に、コントローラー・キャッシュ・メモリーのリカバリーが失敗しました)	6/0C/81	説明: データ・キャッシュ・エラーからのリカバリーが正常に終了しませんでした。ユーザー・データが失われた可能性があります。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。
Event 2110 - Controller cache memory initialization failed (イベント 2110 - コントローラー・キャッシュ・メモリーの初期化に失敗しました)	6/40/81	説明: コントローラーが、内部のコントローラー・コンポーネント (RAID バッファ) の障害を検出しました。その内部コントローラー・コンポーネントの障害は、動作中またはオンボード診断ルーチンの実行中に検出された可能性があります。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。
Event 2113 - Controller cache battery nearing expiration (イベント 2113 - コントローラー・キャッシュのバッテリーがまもなく期限切れになります)	6/3F/D9	説明: 6 週間以内にキャッシュ・バッテリーの有効期限が切れます。 処置: Recovery Guru を開始して「Battery Nearing Expiration (バッテリーがまもなく期限切れになります)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。
Event 211B - Batteries present but NVSRAM configured for no batteries (イベント 211B - バッテリーは存在しますが、どのバッテリーに対しても NVSRAM が構成されていません)	なし	説明: ストレージ・サブシステムにバッテリーは存在していますが、バッテリーを組み込まないように NVSRAM が設定されています。 処置: IBM 技術サポート担当員に連絡して、この障害からリカバリーするための指示を受けてください。
Event 2229 - Drive failed by controller (イベント 2229 - コントローラーがドライブに障害が発生していると判断しました)	なし	説明: ドライブに問題があるため、コントローラーがそのドライブに障害があると判断しました。 処置: Recovery Guru を開始して「Drive Failed by Controller (コントローラーがドライブに障害が発生していると判断しました)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 222D - Drive manually failed (イベント 222D - ドライブを手動で障害発生状態にしました)	6/3F/87	説明: ユーザーがドライブを手動で障害発生状態にしました。 処置: Recovery Guru を開始して「Drive Manually Failed (ドライブを手動で障害発生状態にしました)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。
Event 2247 - Data lost on the logical drive during unrecovered interrupted write (イベント 2247 - リカバリーされなかった書き込みへの割り込み中に、論理ドライブのデータが失われました)	6/3F/EB	説明: その日の始動ルーチンの実行時に、書き込み処理への割り込み中にエラーが発生しました。これにより、論理ドライブが障害状態になりました。 処置: Recovery Guru を開始して、「Unrecovered Interrupted Write (リカバリーされなかった、割り込みが発生した書き込み)」リカバリー手順にアクセスし、その手順に従って障害を修正します。IBM サポートに連絡して、この手順を完了してください。
Event 2248 - Drive failed - write failure (イベント 2248 - ドライブ障害 - 書き込み障害です)	6/3F/80	説明: 書き込みコマンドの実行中に、ドライブに障害が発生しました。ドライブには、障害発生マークが付けました。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 2249 - Drive capacity less than minimum (イベント 2249 - ドライブ容量が最小容量未満です)	6/3F/8B	説明: ドライブを交換しましたが、新規のドライブの容量が、そのドライブ上に再構成する必要がある論理ドライブをすべてサポートするのに十分な大きさではありません。 処置: ドライブをもっと大きい容量のドライブと交換してください。
Event 224A - Drive has wrong block size (イベント 224A - ドライブのブロック・サイズが間違っています)	6/3F/8C	説明: ドライブのブロック・サイズが、論理ドライブ内の他のドライブのブロック・サイズと一致しません。ドライブには、障害発生マークが付けました。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 224B - Drive failed - initialization failure (イベント 224B - ドライブ障害 - 初期化障害です)	6/3F/86	説明: ドライブに障害が発生しました。原因は、(論理ドライブの初期化時に発行された) Format Unit コマンドまたは Write 操作です。ドライブには、障害発生マークが付けました。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 224D - Drive failed - no response at start of day (イベント 224D - ドライブ障害 - その日の始動時の応答がありません)	6/3F/85	説明: その日の始動ルーチン実行中に、ドライブが容量の読み取り コマンドまたは読み取り コマンドに失敗しました。コントローラーは、そのドライブに保管されている構成情報を読み取ることができません。ドライブには、障害発生マークが付けました。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 224E - Drive failed - initialization/reconstruction failure (イベント 224E - ドライブ障害 - 初期化/再構成障害です)	6/3F/82	説明: 以下のいずれかの理由で、以前に障害を起こしたドライブに障害発生マークが付いています。 - ドライブに対して発行された Format Unit コマンドが失敗した。 - コントローラーがドライブを復元できなかったために、そのドライブの再構成が失敗した (例えば、再構成に必要な別のドライブにエラーが発生していた場合)。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 2250 - Logical drive failure (イベント 2250 - 論理ドライブ障害)	6/3F/E0	説明: コントローラーが、論理ドライブに障害発生マークを付けました。ユーザー・データおよび冗長情報 (パリティ) を保持することができなくなりました。原因として最も可能性が高いのは、非冗長構成内の単一ドライブに障害が発生したか、または 1 つのドライブで保護されている構成内の 2 番目の非冗長ドライブに障害が発生したことです。 処置: Recovery Guru を開始して、「Failed Logical Drive Failure (論理ドライブ障害)」リカバリー手順にアクセスし、その指示に従って障害を訂正してください。
Event 2251 - Drive failed - reconstruction failure (イベント 2251 - ドライブ障害 - 再構成障害)	6/3F/8E	説明: その日の始動ルーチンの実行中に発生した再構成障害が原因で、ドライブに障害が発生しました。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 2252 - Drive marked offline during interrupted write (イベント 2252 - 書き込みへの割り込み中に、ドライブにオフラインのマークが付けました)	6/3F/98	説明: 書き込み処理中への割り込み中にエラーが発生したため、論理ドライブに障害発生マークが付けました。読み取りエラーが発生しなかったアレイ内のドライブはオフライン状態になり、このエラーがログに記録されます。 処置: Recovery Guru を開始して、「Unrecovered Interrupted Write (リカバリーされなかった、割り込みが発生した書き込み)」リカバリー手順にアクセスします。IBM サポートに連絡して、この手順を完了してください。
Event 2254 - Redundancy (parity) and data mismatch is detected (イベント 2254 - 冗長情報 (パリティ) とデータの不一致が検出されました)	6/8E/01	説明: パリティの検査中に、コントローラーが、冗長情報 (パリティ) またはデータに不整合があることを検出しました。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 2255 - Logical drive definition incompatible with ALT mode - ALT disabled (イベント 2255 - 論理ドライブ定義は ALT モードと互換性がありません - ALT は使用不可になりました) 注: このイベントは DS4800 には適用されません。	6/91/3B	説明: 自動 LUN 転送 (ALT) は、論理ドライブが 1 つだけ定義されているアレイでしか動作しません。現在、ストレージ・サブシステムには複数の論理ドライブが定義されたアレイが存在しています。そのため、ALT モードが使用不可になっています。コントローラーは標準の冗長コントローラー・モードで動作しています。問題がある場合、コントローラーは、個々の論理ドライブを転送する代わりに、アレイ上のすべての論理ドライブを転送します。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。
Event 2260 - Uncertified drive (イベント 2260 - 未認証ドライブ)	ASC/ASCQ: なし	説明: ストレージ・サブシステムに未認証ドライブがあります。 処置: Recovery Guru を開始して、「Uncertified Drive (未認証ドライブ)」リカバリー手順にアクセスします。
Event 2602 - Automatic controller firmware synchronization failed (イベント 2602 - コントローラー・ファームウェアの自動同期化が失敗しました)	02/04/81	説明: コントローラー・ファームウェアの自動同期化が失敗したため、各冗長コントローラーのファームウェアのバージョンが同一ではありません。ファームウェアのバージョンに互換性のないコントローラーが原因で、予期しない結果を生じる場合があります。 処置: 再度、ファームウェアをダウンロードしてください。問題が解決しない場合には、IBM サポートに連絡してください。
Event 2801 - Storage subsystem running on uninterruptible power supply battery (イベント 2801 - ストレージ・サブシステムは、無停電電源装置のバッテリーで稼働しています)	6/3F/C8	説明: 無停電電源装置が、AC 電源が供給されなくなったために予備電源に切り替わったことを示しました。今すぐ対応が必要な原因は何もありませんが、突然のバッテリー切れに備えて、データを頻繁に保存してください。 処置: Recovery Guru を開始して、「Lost AC Power (AC 電源断)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 2803 - Uninterruptible power supply battery - two minutes to failure (イベント 2803 - 無停電電源装置バッテリー - 障害発生まであと 2 分)	6/3F/C9	説明: 無停電電源装置が、予備電源が切れかかっていることを示しました。 処置: コントローラーへの入出力アクティビティを停止する処置を取ってください。通常、コントローラーは、ライトバック・キャッシュ・モードからライトスルー・モードに切り替わります。
Event 2804 - Uninterruptible power supply battery failed (イベント 2804 - 無停電電源装置のバッテリーに障害が発生しました)	なし	説明: 無停電電源装置のバッテリーに障害が発生しました。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 2807 - Environmental service module failed (イベント 2807 - 環境サービス・モジュールに障害が発生しました)	なし	説明: ESM に障害が発生しました。 処置: Recovery Guru を開始して、「Failed Environmental Service Module CRU (環境サービス・モジュール CRU の障害)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 2808 - storage expansion enclosure ID not unique (イベント 2808 - ストレージ拡張エンクロージャー ID が固有ではありません)	6/98/01	説明: コントローラーが、同じ ID が選択されている複数のストレージ拡張エンクロージャーを検出しました。各ストレージ拡張エンクロージャーの ID 設定値が固有であるかどうか検査してください。 処置: Recovery Guru を開始して、「Enclosure ID Conflict (エンクロージャー ID の競合)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 280A - Controller enclosure component missing (イベント 280A - コントローラー・エンクロージャーのコンポーネントが欠落しています)	6/3F/C7	説明: コントローラー以外のコンポーネント (例えば、ファン、電源機構、バッテリー) が、コントローラー・エンクロージャーに欠落しています。FRU コードに、障害のあるコンポーネントが示されています。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 280B - Controller enclosure component failed (イベント 280B - コントローラー・エンクロージャーのコンポーネントに障害が発生しました)	6/3F/C7	説明: コントローラー・エンクロージャー内のコントローラー以外のコンポーネント (例えば、ファン、電源機構、バッテリー) に障害が発生したか、過熱状態が発生しました。FRU コードに、障害のあるコンポーネントが示されています。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 280D - Drive storage expansion enclosures component failed (イベント 280D - ドライブ・ストレージ拡張エンクロージャー・コンポーネントで障害が発生しました)	6/3F/C7	説明: ストレージ拡張エンクロージャー内で、ドライブ以外のコンポーネント (例えば、ファン、電源機構、バッテリー) に障害が発生したか、過熱状態が発生しました。FRU コードに、障害のあるコンポーネントが示されています。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 280E - Standby power supply not fully charged (イベント 280E - 予備電源装置がフル充電されていません)	6/3F/CA	説明: 無停電電源装置が、その予備電源装置がフル充電済みの容量に達していないことを示しました。 処置: 無停電電源装置を検査して、予備電源 (バッテリー) が動作状態にあることを確認してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 280F - Environmental service module - loss of communication (イベント 280F - 環境サービス・モジュール - 通信が切断しています)	6/E0/20	説明: ストレージ拡張エンクロージャー 内の二重 ESM CRU の一方との通信が切断しました。ストレージ拡張エンクロージャーの入出力パスは 1 つしか使用できません。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 2813 - Minihub CRU failed (イベント 2813 - ミニハブ CRU に障害が発生しました)	6/3F/C7	説明: ミニハブ CRU との通信が切断しました。ミニハブ CRU か、コントローラーか、内部のバックプレーン通信ボードに障害が発生した可能性があります。1 つのミニハブだけで障害が発生している場合は、ストレージ・サブシステムはまだ作動していますが、2 番目のミニハブに障害が発生すると、影響を受けたエンクロージャーに障害が発生する可能性があります。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 2815 - GBIC failed (イベント 2815 - GBIC に障害が発生しました)	なし	説明: コントローラー・エンクロージャーまたはストレージ拡張エンクロージャーのいずれかのギガビット・インターフェース・コンバーター (GBIC) に障害が発生しました。1 つの GBIC だけで障害が発生している場合は、ストレージ・サブシステムはまだ作動していますが、2 番目の GBIC に障害が発生すると、影響を受けたエンクロージャーに障害が発生する可能性があります。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 2816 - storage expansion enclosure ID conflict - duplicate IDs across ストレージ拡張エンクロージャーs (イベント 2816 - ストレージ拡張エンクロージャー ID の競合 - 複数のストレージ拡張エンクロージャーで ID が重複しています)	6/98/01	説明: 複数のストレージ拡張エンクロージャーが同一のエンクロージャー識別番号を使用しています。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 2818 - storage expansion enclosure ID mismatch - duplicate IDs in the same ストレージ拡張エンクロージャー (イベント 2818 - ストレージ拡張エンクロージャー ID の不一致 - 同一のストレージ拡張エンクロージャー内で ID が重複しています)	6/98/02	説明: ストレージ・サブシステム内のいずれかのストレージ拡張エンクロージャーに、異なるエンクロージャー識別番号を持つ ESM が含まれています。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 281B - Nominal temperature exceeded (イベント 281B - 公称温度を超えました)	6/98/03	説明: エンクロージャーの公称温度を超えました。ファンが故障したか、室内の温度が高すぎます。エンクロージャーの温度が上昇し続けた場合、その影響を受けるエンクロージャーが自動的にシャットダウンする可能性があります。事態が深刻にならないうちに、すぐに問題を訂正してください。自動シャットダウン条件は、エンクロージャーのモデルによって異なります。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 281C- Maximum temperature exceeded (イベント 281C - 最大温度を超えました)	6/3F/C6	説明: エンクロージャーの最大温度を超えました。ファンが故障したか、室内の温度が高すぎます。この状態は重大です。すぐに問題を修正しないと、エンクロージャーがシャットダウンする可能性があります。自動シャットダウン条件は、エンクロージャーのモデルによって異なります。 処置: Recovery Guru を開始し、指示に従って障害を訂正してください。
Event 281D - Temperature sensor removed (イベント 281D - 温度センサーが取り外されました)	6/98/03	説明: 温度センサーが取り付けられているファン CRU が、ストレージ・サブシステムから取り外されました。 処置: できるだけ早く、CRU を取り替えてください。Recovery Guru を開始して、「Failed or Removed Fan CRU (障害のある、または取り外されたファン CRU)」リカバリー手順をクリックし、その指示に従って障害を訂正してください。
Event 281E - Environmental service module firmware mismatch (イベント 281E - 環境サービス・モジュール・ファームウェアの不一致)	6/98/03	説明: ストレージ・サブシステム内のストレージ拡張エンクロージャーに、別のバージョンのファームウェアを持つ ESM が含まれています。同じストレージ拡張エンクロージャー内の ESM は、同じバージョンのファームウェアを持っている必要があります。交換用サービス・モニターがない場合は、IBM サポートに連絡して、ファームウェアをダウンロードしてください。 処置: Recovery Guru を開始して、「Environmental Service Module Firmware Version Mismatch (環境サービス・モジュール・ファームウェアのバージョンの不一致)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 2821 - Incompatible Minihub (イベント 2821 - 非互換のミニハブ)	なし	説明: コントローラー・エンクロージャーで非互換のミニハブ・ブレードが検出されました。 処置: Recovery Guru を開始して、「Incompatible minihub blade (非互換のミニハブ・ブレード)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 2823 - Drive bypassed (イベント 2823 - ドライブをバイパスしました)	なし	説明: ESM が、ファイバー・チャンネル・ループの完全性を維持するためにドライブをバイパスしたことを報告しました。 処置: Recovery Guru を開始して「By-Passed Drive (バイパスされたドライブ)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 2827 - Controller was inadvertently replaced with an ESM (イベント 2827 - コントローラーが誤って ESM と交換されました)	なし	説明: コントローラー・ブレードが誤って ESM ブレードと交換されました。 処置: できるだけ早く、ESM ブレードをコントローラー・ブレードと取り替えてください。
Event 2828 - Unsupported ストレージ拡張エンクロージャー selected (イベント 2828 - 非サポートのストレージ拡張エンクロージャーが選択されました)	なし	説明: ストレージ・サブシステムに、サポートされないストレージ拡張エンクロージャーが 1 つ以上含まれています。ストレージ拡張エンクロージャーがすべて非サポートとして検出されている場合は、NVS RAM 構成ファイルに問題があるか、ファームウェアのバージョンが間違っている可能性があります。このエラー条件によって、サポートされないストレージ拡張エンクロージャー内のドライブがロックアウトされ、それが原因で定義済みアレイまたは論理ドライブに障害が発生することがあります。 処置: アレイまたは論理ドライブで障害が発生している場合は、IBM サポートに連絡してリカバリー手順を問い合わせてください。あるいは、Recovery Guru を開始して「Unsupported Drive Enclosure (非サポートドライブ・エンクロージャー)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 2829 - Controller redundancy lost (イベント 2829 - コントローラーの冗長に損失が発生しました)	6/E0/20	説明: ライブ・ループ (チャンネル) の 1 つを経由する 2 台のコントローラー間の通信が切断しました。 処置: Recovery Guru を開始して、他にも冗長性の消失の問題が報告されていないか確認してください。他の問題が報告されている場合は、そちらの方を最初に訂正してください。冗長性の問題が引き続き報告される場合は、IBM サポートに連絡してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 282B - ストレージ拡張エンクロージャー path redundancy lost (イベント 282B - ストレージ拡張エンクロージャーのパスの冗長に損失が発生しました)	6/E0/20	説明: 冗長なドライブ・ループ (チャンネル) を持つストレージ拡張エンクロージャーで、そのループのうちの 1 つを経由する通信が失われました。ストレージ拡張エンクロージャーの入出力に使用できるループは 1 つだけです。できるだけ早く、この障害を訂正してください。ストレージ・サブシステムはまだ作動していますが、パスの冗長のレベルは失われました。残りのドライブ・ループに障害が発生した場合、そのストレージ拡張エンクロージャーへの入出力はすべて失敗します。 処置: Recovery Guru を開始して、「Drive - Loss of Path Redundancy (ドライブ - パスの冗長に損失が発生しました)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 282D - Drive path redundancy lost (イベント 282D - ドライブ・パスの冗長性が失われました)	6/E0/20	説明: ドライブとの通信パスが失われました。できるだけ早く、この障害を訂正してください。ドライブはまだ作動していますが、パスの冗長のレベルは失われました。ドライブのもう一方のポート、または作動しているチャンネルの他のコンポーネントに障害が発生した場合は、ドライブ障害が発生します。 処置: Recovery Guru を開始して、「Drive - Loss of Path Redundancy (ドライブ - パスの冗長に損失が発生しました)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 282F - Incompatible version of ESM firmware detected (イベント 282F - 非互換バージョンの ESM ファームウェアが検出されました)	なし	説明: ストレージ・サブシステム内のストレージ拡張エンクロージャーに、異なるファームウェア・バージョンの ESM ブレードが搭載されています。ストレージ・サブシステム内のストレージ拡張エンクロージャーに、ハードウェアが異なる ESM ブレードが搭載されている場合も、このエラーが報告されることがあります。 処置: Recovery Guru を開始して「ESM blade Firmware Version Mismatch (ESM ブレード・ファームウェア・バージョンの不一致)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 2830 - Mixed drive types not supported (イベント 2830 - ドライブ・タイプの混在はサポートされていません)	なし	説明: ストレージ・サブシステムには現在、ファイバー・チャンネル (FC) やシリアル ATA (SATA) などの、異なるドライブ・テクノロジーのドライブが含まれています。このストレージ・サブシステムでは、異なるドライブ・テクノロジーの混在はサポートされていません。 処置: Recovery Guru を開始して「Mixed Drive Types Not Supported (ドライブ・タイプの混在はサポートされていません)」リカバリー手順にアクセスし、指示に従ってこの障害からリカバリーしてください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 2835 - Drive storage expansion enclosures not cabled together (イベント 2835 - ドライブ・ストレージ拡張エンクロージャーがケーブル接続されていません)	ASC/ASCQ: なし	説明: ストレージ・サブシステム内に、正しくケーブル接続されていないドライブ・ストレージ拡張エンクロージャーがあります。それらのエンクロージャーには、相互に順次接続する必要のある ESM ブレードが搭載されています。 処置: Recovery Guru を開始して「Drive Enclosures Not Cabled Together (ドライブ・エンクロージャーがケーブル接続されていません)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 3019 - Logical drive ownership changed due to failover (イベント 3019 - フェイルオーバーにより、論理ドライブの所有権が変更されました)	なし	説明: 特定のパス上の論理ドライブにアクセスできなかったために、マルチパス・ドライバー・ソフトウェアが、その論理ドライブの所有権をもう一方のコントローラーに変更しました。 処置: Recovery Guru を開始し、「Logical Drive Not on Preferred Path (論理ドライブが優先パスにありません)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 4011 - Logical drive not on preferred path (イベント 4011 - 論理ドライブが優先パスにありません)	なし	説明: 「Recovery Guru」領域にリストされているコントローラーにアクセスできません。このコントローラーが優先パスとして割り当てられている論理ドライブはすべて、非優先パス (代替コントローラー) に移動されます。 処置: Recovery Guru を開始し、「Logical Drive Not on Preferred Path (論理ドライブが優先パスにありません)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 5005 - Place controller offline (イベント 5005 - コントローラーをオフラインにします)	なし	説明: コントローラーがオフラインになりました。コントローラーで診断テストに失敗したことが原因になっている可能性があります。(診断は、コントローラーが内部的に開始した場合もあり、「Controller (コントローラー)」→「Run Diagnostics (診断の実行)」メニュー・オプションでユーザーが開始した場合もあります。)あるいは、「Controller (コントローラー)」→「Place Offline (オフラインにする)」メニュー・オプションを使用して、コントローラーが手動でオフラインにされました。 処置: Recovery Guru を開始し、「Offline Controller (コントローラーのオフライン化)」リカバリー手順をクリックします。指示に従って、コントローラーを交換してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 502F - Missing logical drive deleted (イベント 502F - 欠落している論理ドライブが削除されました)	なし	説明: ストレージ・サブシステムが、論理ドライブに関連付けられているドライブにアクセスできなくなっていることを検出しました。これは、アレイに関連付けられているドライブがすべて取り外された場合、または 1 つ以上のストレージ拡張エンクロージャーに電力が供給されていない場合に起こることがあります。 処置: Recovery Guru を開始し、「Missing Logical Drive (論理ドライブの欠落)」リカバリー手順をクリックしてください。指示に従って、障害を訂正してください。
Event 5038 - Controller in lockout mode (イベント 5038 - コントローラーがロックアウト・モードです)	なし	説明: パスワード認証の試行の失敗回数が、10 分間に 10 回を超えたので、両方のコントローラーが 10 分間のロックアウト・モードに入りました。ロックアウト期間中は、どのコントローラーでもすべての認証要求が拒否されます。10 分間のロックアウトが過ぎると、コントローラーは認証失敗の合計カウンターをリセットし、自身をアンロックします。 処置: 10 分間待って、もう一度パスワードを入力してください。
Event 5040 - Place controller in service mode (イベント 5040 - コントローラーをサービス・モードにします)	なし	説明: コントローラーは、診断上の理由またはリカバリー上の理由で、手動でサービス・モードにされました。 処置: Recovery Guru を開始して、「Controller in Service Mode (コントローラーはサービス・モード)」リカバリー手順にアクセスしてください。コントローラーを元のオンラインに戻すには、この手順を使用します。
Event 5405 - Gold Key - mismatched settings (イベント 5404 - ゴールド・キー - 設定の不一致)	ASC/ASCQ: なし	説明: ペアのコントローラーのそれぞれの NVSRAM ビット設定が異なります。この設定はコントローラーがゴールド・キー制限に従っているかどうかを判別するものです。 処置: IBM ストレージ・サブシステム・コントローラーまたはドライブを、誤って IBM 以外のコントローラーまたはドライブとスワッピングした場合に、このイベントが生成されることがあります。この重大イベントは、IBM DS3000、DS4000、または DS5000 ストレージ・サブシステム構成には適用されません。リカバリー手順については、IBM サポートにお問い合わせください。
Event 5406 - Mixed drive types - mismatched settings (イベント 5406 - 混合ドライブ・タイプ - 設定の不一致)	ASC/ASCQ: なし	説明: ペアのコントローラーの NVSRAM ビットの設定が互いに異なっています。この設定は混合ドライブ・タイプがプレミアム・フィーチャーであるかどうかを制御するものです。 処置: Recovery Guru を開始して「Mixed Drive Types - Mismatched Settings (混合ドライブ・タイプ - 設定の不一致)」リカバリー手順にアクセスし、その指示に従ってこのコントローラーの状態を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 5602 - This controller alternate failed - timeout waiting for results (イベント 5602 - 代替コントローラーに障害が発生しました - 結果待ちがタイムアウトになりました)	なし	説明: このコントローラーは、代替コントローラーに対して診断を開始しましたが、診断が完了したことを示す応答を受け取りませんでした。このペアの代替コントローラーは、オフラインになりました。 処置: Recovery Guru を開始し、「Offline Controller (コントローラーのオフライン化)」リカバリー手順をクリックします。指示に従って、コントローラーを交換してください。
Event 560B - CtlrDiag task cannot obtain Mode Select lock (イベント 560B - CtlrDiag タスクがモード選択ロックを取得できません)	なし	説明: このコントローラーは診断を実行しようとしていますが、他のストレージ・サブシステムの操作からテスト領域を保護できませんでした。診断は取り消されました。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。
Event 560C - CtlrDiag task on controller alternate cannot obtain Mode (イベント 560C - 代替コントローラーに対する CtlrDiag タスクがモードを取得できませんでした)	なし	説明: このペアの代替コントローラーは診断を実行しようとしていますが、他のストレージ・サブシステムの操作からテスト領域を保護できませんでした。診断は取り消されました。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。
Event 560D - Diagnostics read test failed on controller (イベント 560D - コントローラーでの診断読み取りテストが不合格になりました)	なし	説明: コントローラーが、診断の実行中に、受信された情報がそのテストに対して期待されている戻り値に一致していないことを検出しました。これは、入出力が完了しないか、読み取られているデータに不一致があることを示していることがあります。この障害の結果、コントローラーはオフラインになります。 処置: Recovery Guru を開始し、「Offline Controller (コントローラーのオフライン化)」リカバリー手順をクリックします。指示に従って、コントローラーを交換してください。
Event 560E - This controller alternate failed diagnostics read test (イベント 560E - 代替コントローラーでの診断読み取りテストが不合格になりました)	なし	説明: このコントローラーの代替コントローラーが、診断の実行中に、受信された情報がそのテストに対して期待されている戻り値に一致していないことを検出しました。これは、入出力が完了しないか、読み取られているデータに不一致があることを示していることがあります。このペアの代替コントローラーは、オフラインになります。 処置: Recovery Guru を開始し、「Offline Controller (コントローラーのオフライン化)」リカバリー手順をクリックします。指示に従って、コントローラーを交換してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 560F - Diagnostics write test failed on controller (イベント 560F - コントローラーでの診断書き込みテストが不合格になりました)	なし	説明: このコントローラーの代替コントローラーが、診断の実行中に、テスト領域にデータを書き込めませんでした。これは、入出力が完了しないか、書き込まれているデータに不一致があることを示していることがあります。コントローラーはオフラインになります。 処置: Recovery Guru を開始し、「Offline Controller (コントローラーのオフライン化)」リカバリー手順をクリックします。指示に従って、コントローラーを交換してください。
Event 5610 - This controller alternate failed diagnostics write test (イベント 5610 - 代替コントローラーに対する診断書き込みテストが不合格になりました)	なし	説明: このコントローラーの代替コントローラーが、診断の実行中に、テスト領域にデータを書き込めませんでした。これは、入出力が完了しないか、書き込まれているデータに不一致があることを示していることがあります。このペアの代替コントローラーは、オフラインになります。 処置: Recovery Guru を開始し、「Offline Controller (コントローラーのオフライン化)」リカバリー手順をクリックします。指示に従って、コントローラーを交換してください。
Event 5616 - Diagnostics rejected - configuration error on controller (イベント 5616 - 診断が拒否されました - コントローラーでの構成エラーです)	なし	説明: このコントローラーの代替コントローラーが診断を実行しようとしていますが、テストの完了に必要なテスト領域を作成できませんでした。診断は取り消されました。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。
Event 5617 - Diagnostics rejected - configuration error on controller alternate (イベント 5617 - 診断が拒否されました - 代替コントローラーでの構成エラーです)	なし	説明: このコントローラーの代替コントローラーが診断を実行しようとしていますが、テストの完了に必要なテスト領域を作成できませんでした。診断は取り消されました。 処置: IBM サポートに連絡し、この障害からリカバリーするための指示を受けてください。
Event 6101 - Internal configuration database full (イベント 6101 - 内部の構成データベースがいっぱいです)	なし	説明: ある種の構成データを保管するために必要なデータ量が原因となって、論理ドライブの最大数の見積もりが少なすぎるという状況になりました。以下のタイプのデータのいずれか、または両方が原因で、内部の構成データベースがいっぱいになった可能性があります。 • FlashCopy 論理ドライブの構成データ • グローバル/メトロ・リモート・ミラーの構成データ 処置: このイベントからリカバリーするには、ストレージ・サブシステムから 1 つ以上の FlashCopy 論理ドライブを削除するか、1 つ以上のリモートのミラー関係を除去します。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 6107 - The alternate for the controller is nonfunctional and is being held in reset 代替 (イベント 6107 - 代替コントローラーが作動しておらず、リセット状態になっています)	なし	説明: ストレージ・サブシステム内のコントローラーが、代替コントローラーがハードウェア障害のために作動しておらず、交換の必要があることを検出しました。 処置: Recovery Guru を開始して「Offline Controller (コントローラーのオフライン化)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 6200 - FlashCopy repository logical drive threshold exceeded (イベント 6200 - FlashCopy リポジトリ論理ドライブのしきい値を超えました)	なし	説明: FlashCopy リポジトリ論理ドライブ容量が、警告しきい値レベルを超えました。FlashCopy リポジトリ論理ドライブの容量がいっぱいになると、それに関連するFlashCopy 論理ドライブに障害が発生する可能性があります。これは、FlashCopy リポジトリ論理ドライブがいっぱいになる前に受け取る最後の警告です。 処置: Recovery Guru を開始して、「FlashCopy Repository Logical Drive Threshold Exceeded (FlashCopy リポジトリ論理ドライブのしきい値を超えました)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。
Event 6201 - FlashCopy repository logical drive full (イベント 6201 - FlashCopy リポジトリ論理ドライブがいっぱいです)	なし	説明: FlashCopy リポジトリ論理ドライブの使用可能な容量がすべて使用されました。FlashCopy リポジトリ論理ドライブがいっぱいになったときの処理は、FlashCopy リポジトリ論理ドライブの障害ポリシーによって決まります。障害ポリシーは、FlashCopy 論理ドライブを障害発生とみなす (デフォルト設定)、または基本論理ドライブの着信入出力を失敗させる、のいずれかに設定できます。 処置: Recovery Guru を開始して、「FlashCopy Repository Logical Drive Capacity - Full (FlashCopy リポジトリ論理ドライブ容量 - 満杯)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。
Event 6202 - Failed FlashCopy logical drive (イベント 6202 - FlashCopy 論理ドライブに障害が発生しました)	なし	説明: FlashCopy 論理ドライブに関連付けられているFlashCopy リポジトリ論理ドライブがいっぱいになったか、それに関連付けられている基本論理ドライブまたはFlashCopy リポジトリ論理ドライブが、それらのアレイの 1 つ以上のドライブ障害のために障害を起こしました。 処置: Recovery Guru を開始して、「Failed FlashCopy Logical Drive (FlashCopy 論理ドライブに障害が発生しました)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 6400 - Dual primary logical drive (イベント 6400 - 1 次論理ドライブが重複しています)	なし	説明: 役割の強制反転後に、両方の論理ドライブが 1 次論理ドライブにプロモートされました。このイベントが報告される可能性があるのは、コントローラーがリセットした場合、またはアレイからファイバー・チャンネル・スイッチへのケーブルが取り外された後に再度挿入され、もう一方の論理ドライブが 1 次論理ドライブにプロモートされていた場合です。 処置: Recovery Guru を開始して、「Dual Primary Logical Drive Conflict (重複する 1 次論理ドライブの競合)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。
Event 6401 - Dual secondary logical drive (イベント 6401 - 2 次論理ドライブが重複しています)	なし	説明: 役割の強制反転後に、リモート・ミラーの両方の論理ドライブが 2 次論理ドライブにデモートされました。このイベントが報告される可能性があるのは、コントローラーがリセットした場合、またはアレイからファイバー・チャンネル・スイッチへのケーブルが取り外された後に再度挿入され、もう一方の論理ドライブが 2 次論理ドライブにプロモートされていた場合です。 処置: Recovery Guru を開始して、「Dual Secondary Logical Drive Conflict (重複 2 次論理ドライブの競合)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。
Event 6402 - Mirror data unsynchronized (イベント 6402 - ミラー・データが同期化されていません)	イベントには記録されません	説明: これは入出力エラーが原因で発生する場合がありますが、他のイベントがその入出力エラーに関連付けられている可能性があります。リモート・ミラーの 1 次ストレージ・サブシステムおよび 2 次ストレージ・サブシステムの両方に、「Needs Attention (要注意)」アイコンが表示されます。 処置: Recovery Guru を開始して、「Mirror Data Unsynchronized (ミラー・データが同期化されていません)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 6503 - Remote logical drive link down (イベント 6503 - リモート論理ドライブ・リンクがダウンしました)	なし	説明: アレイとそのピアの間のケーブルが切断されているか、ファイバー・チャネル・スイッチに障害があるか、ピア・アレイがリセットされたかの場合に、このイベントがトリガーされます。このエラーの結果、「Mirror Data Unsynchronized (ミラー・データが同期化されていません)」(イベント 6402) が発生する場合があります。影響を受けるリモート論理ドライブには、「Unresponsive (未応答)」アイコンが表示され、カーソルをこの論理ドライブの上に動かすと、ツールチップでこの状態が選択されます。 処置: Recovery Guru を開始して、「Mirror Communication Error - Unable to Contact Logical Drive (ミラー通信エラー - 論理ドライブに接続できません)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。
Event 6505 - WWN change failed (イベント 6505 - WWN の変更が失敗しました)	なし	説明: ミラーリングによって、WWN の変更がアレイ間で通信されます。WWN の変更の失敗は、WWN が変更されたアレイと、ピアのアレイとの間の非入出力通信エラーが原因で発生します。(アレイの WWN は、ファイバー・ネットワーク上でアレイを検出するために使用される固有の名前です。アレイ内のコントローラーを両方とも交換すると、アレイの WWN が変わります。)影響を受けるリモート論理ドライブには、「Unresponsive (未応答)」アイコンが表示され、カーソルをこの論理ドライブの上に動かすと、ツールチップでこの状態が選択されます。 処置: Recovery Guru を開始して、「Unable to Update Remote Mirror (リモート・ミラーを更新できません)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。この問題の唯一の解決策は、リモート・ミラーを削除してから、別のリモート・ミラーを設定することです。
Event 6600 - Logical drive copy operation failed (イベント 6600 - 論理ドライブのコピー操作が失敗しました)	なし	説明: 「進行中」状況の論理ドライブのコピー操作が失敗しました。この失敗の原因は、ソース論理ドライブでの読み取りエラー、ターゲット論理ドライブでの書き込みエラー、あるいは、ソース論理ドライブまたはターゲット論理ドライブに影響を与えるストレージ・サブシステムで発生した障害にあります。 処置: Recovery Guru を開始し、「Logical Drive Copy Operation Failed (論理ドライブのコピー操作が失敗しました)」リカバリー手順をクリックしてください。指示に従って、この障害を訂正してください。

表 38. 重大イベント (続き)

重大イベントの番号	センス・キー/ASC/ASCQ	重大イベントの説明および必要な処置
Event 6700 - Unreadable sector(s) detected - data loss occurred (イベント 6700 - 読み取り不能セクターが検出されました - データが失われました)	なし	説明: 1 つ以上の論理ドライブで、読み取り不能セクターが検出され、データが失われました。 処置: Recovery Guru を開始して「Unreadable Sectors Detected (読み取り不能セクターが検出されました)」リカバリー手順にアクセスし、その指示に従ってこの障害からリカバリーしてください。
Event 6703 - Overflow in unreadable sector database (イベント 6703 - 読み取り不能セクター・データベースでオーバーフローが発生しました)	なし	説明: 読み取り不能セクターのログが、その最大容量に達していっぱいになりました。 処置: Recovery Guru を選択して「Unreadable Sectors Log Full (読み取り不能セクターのログが満杯になりました)」リカバリー手順にアクセスし、指示に従ってこの障害からリカバリーしてください。

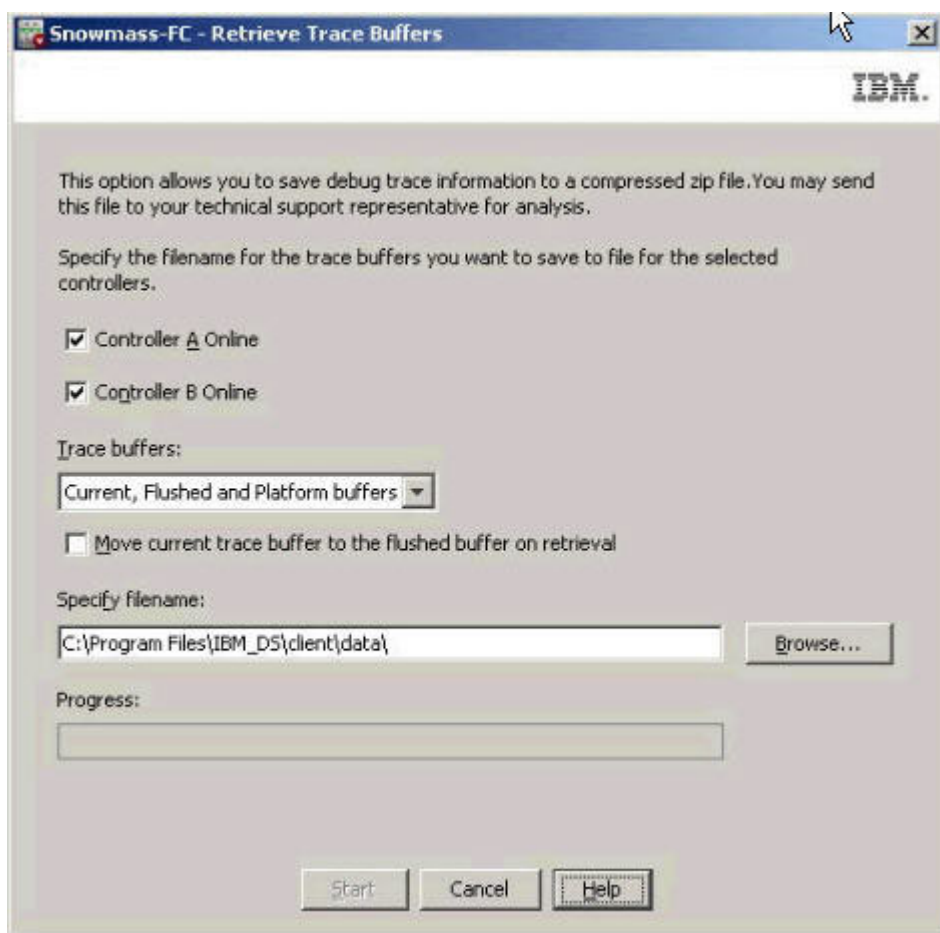
トレース・バッファの取り出し

バイナリー・トレース・バッファは、stateCaptureData.txt の以前の dqprint テキストよりも長い期間、データを提供します。

拡張トラブルシューティングおよびサポート・データは、バイナリー・フォーマットで収集され、IBM サポートによって解析される必要があります。これらのデータは、Collect All Support Data (すべてのサポート・データの収集) (CASD) サポート・バンドル (traceBuffers.zip) の部分です。

CLi での使用:

```
start controller [both] trace dataType=all forceFlush=FALSE file="C:\TBTest2.zip";
```



構成データベース検証

バージョン 10.77 では、新規の構成データベース診断フィーチャーが追加されています。

手動で検証を実行するには、「Physical (物理)」タブ上でコントローラーを選択し、次に「**Advanced (拡張)**」 > 「**Troubleshooting (トラブルシューティング)**」 > 「**Run Diagnostics (診断の実行)**」 > 「**Configuration Database (構成データベース)**」を選択します。

EMW、SubSystem Managment (サブシステム管理) ウィンドウ、または CLI を介してコントローラー・ファームウェアのダウンロードが開始する前に、自動的にデータベース・チェックが実行されます。

検証が失敗すると、エラーの説明用のテキスト・ファイルと、トラブルシューティング用の DQ ファイルを含む zip ファイルが作成されます。

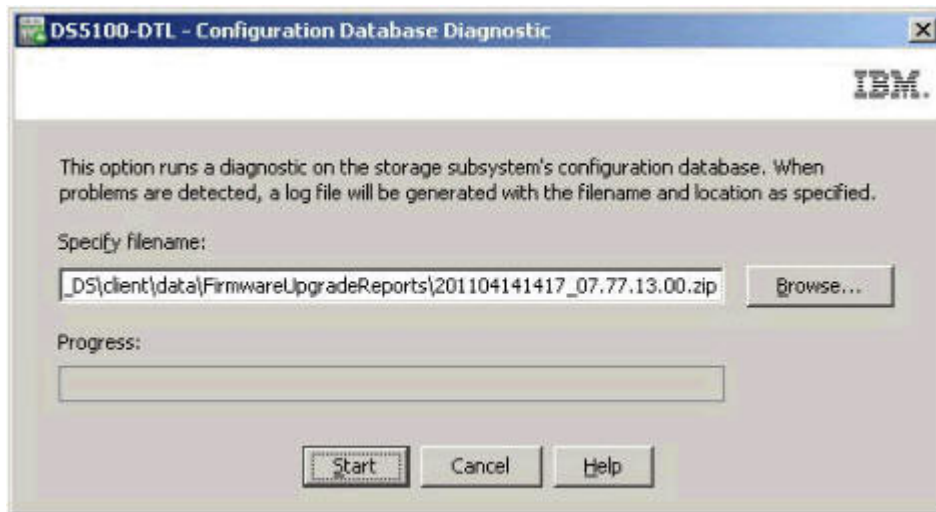
検証失敗 MEL イベント

イベント名: 生データ検索構造不整合が検出されました。

タイプ: 3408

コンポーネント・タイプ: コントローラー

新規 CLI コマンド:**start storageSubsystem configDbDiagnostic;**



データベースの保存/復元

ストレージ・モニター・サービスは、自動的にサブシステムから構成 DB を保存し、また既存の構成 DB を復元することもできます。

保存

ストレージ・モニター・サービスは、DB の変更があり、しかも直前のキャプチャー以降 125 分経過している場合、自動的にサブシステムから構成 DB を保存し、"`...client\data\monitor\dbcapture`" にファイルを保存します。

サブシステムが新規にインストールされた HSW に追加されたときに、最初の DB がキャプチャーされます。

キャプチャーされたすべての DB ファイルは zip され、以下のように名前が付けられます。

`RetrievedRecords_SSID_Date_Time.dbm`

例: `RetrievedRecords_60080e500017b8de000000004be47b12_2010_08_20_14_48_27.dbm`

コマンド `save storageSubsystem dbmDatabase file="C:\path\filename.zip"` を使用すれば、DB を手動で保存するのに CLI を使用することができます。

復元

自身の構成を失ったシステム、または故障状態から回復するために構成が除去されていたシステムを回復するのに、既存の構成 DB を復元することができます。

この機能は、以下のものが含まれているデータベースの部分で復元します。

- Lun およびアレイの構成
- Lun WWN
- コントローラー WWN
- プレミアム・フィーチャー
- マッピング

以下のものを除外します。

- MEL
- UTM
- キャッシュ

期間: 最大 45 分

ユーザーは、構成 DB を復元するためにバリデータ・ストリングを持っている必要があります。バリデータを取得するには、構成 DB zip ファイルおよびシステム・プロファイルを IBM サポートに送ります。IBM サポートは、ユーザーが提供する情報に基づいてバリデータ・ストリングを生成します。

構成データベースのロード

構成データベースをロードするには、以下のことを行います。

1. E メールを介して送信される *.key ファイルをテキスト・エディターで開きます。
2. ストリングを記録します。例: 8bbaadfa7375cb4dfcc81c15bde30ad32d814c09
3. サブシステムへの入出力を停止します。
4. GUI を介してコントローラーの 1 つをオフラインに設定します。
5. 復元は、CLI コマンド `load storageSubsystem dbmDatabase file="C:¥path¥filename.zip" validator="8bbaadfa7375cb4dfcc81c15bde30ad32d814c09";` を使用して行われます。

DS 診断データ・キャプチャー (DDC)

DDC 機能は、コントローラー・ファームウェアの異常イベントをトラブルシューティングするために IBM サポートでデータを収集する際の補助として実装されました。

注: この機能は、06.12.27.xx レベルより前のコントローラー・ファームウェアのコード・バージョンには実装されていません。

まれなケースですが、内部コントローラー・エラーにより、診断データ・キャプチャー (DDC) 機能を実行するルーチンが強制されることがあります。これが起こると、「Enterprise Management (エンタープライズ管理)」ウィンドウで、エラーのある (最適の状態ではない) ストレージ・サブシステムの名前の横に赤の停止記号が表示されます。そのストレージ・サブシステム用の「Subsystem Management (サブシステム管理)」ウィンドウを開いた後、Recovery Guru をクリックできます。Recovery Guru には、MEL (ストレージ・マネージャーのメジャー・イベント・ログ) と同様に、何が問題であるかが表示されます。MEL について詳しくは、288 ページの『DDC MEL イベント』を参照してください。

DDC 機能が実装されると、ストレージ・サブシステムの状況が「Optimal (最適)」から「Needs Attention due to DDC (DDC により要注意)」に変わります。これは、次の状況で起こります。

- ストレージ・サブシステム内のコントローラーがマスター・アボート (ファイバー・チャネル・チップによる誤ったアドレスへのアクセスの結果、PCI バス・エラーが生じたために起こる) などの異常イベントを検出した。
- コントローラーが長時間 (数分間) ホスト入出力要求を処理できない。
- 宛先装置番号レジストリーが破損している。
- ディスク・ドライブによって EDC (エラー検出コード) エラーが返される。
- 代替コントローラーが所有する論理ドライブに静止障害が発生した。
- ストレージ区画管理に関連したレコードが破損した。

「Needs Attention due to DDC (DDC により要注意)」フラグが設定されると、コントローラーのキャッシュ・バッテリーが十分に充電されているならば、電源を入れ直してコントローラーをリブートしても、このフラグは引き続き立てられたままです。さらに、異常イベントが発生した瞬間のストレージ・サブシステム・コントローラーの状態を反映するデータが、収集され、ユーザーによって取り出されるまで保存されます。「Needs Attention due to DDC (DDC により要注意)」フラグをクリアし、保存された診断データを取り出すには、『リカバリー手順』を参照してください。

現行 DDC 機能の実装では、その DDC データが保存されるまで、一度に 1 つの異常イベントについてのみ DDC データを保持するので、「Needs Attention due to DDC (DDC により要注意)」エラーが生じた場合は必ず、できるだけ迅速に **SMcli** コマンドを実行して、コントローラーが他の異常イベントに関するデータを収集できるようにする必要があります。診断データが保存され、「Needs Attention due to DDC (DDC により要注意)」フラグがクリアされるまで、他に異常イベントが発生しても、コントローラーがこれらのイベントについて診断データの収集を開始することはありません。前の DDC トリガーから少なくとも 48 時間経っている場合、またはユーザーが前の DDC 情報を正常に取り出した場合、異常イベントは DDC トリガーを呼び出します。さらに、DDC 情報は、コントローラーがオンラインの場合にのみ使用可能となります。サービス中またはロック・ダウン・モードのコントローラーは、DDC イベントを引き起こしません。DDC データを収集した後、IBM サポートに連絡して問題を報告し、その状況のトラブルシューティングの支援を求めてください。

リカバリー手順

DDC リカバリー・プロセスを実行するには、以下の手順を実行します。

1. Enterprise Management (エンタープライズ管理) ウィンドウから「Script Editor (スクリプト・エディター)」を開くか、またはコマンド行インターフェース (CLI) を開きます。

注: これらのコマンドの構文について詳しくは、「Enterprise Management (エンタープライズ管理) ウィンドウのオンライン・ヘルプを参照してください。

2. 診断データを保存するかどうかに応じて、次の表に記載されている指示に従います。

表 39. リカバリー・ステップ 2

発生した内容	対策
診断データを保存する	ステップ 3 に進みます。
診断データを保存しない	ステップ 5 に進みます。

3. 次のように入力します。

```
save storageSubsystem diagnosticData file="filename ";
```

ここで、*filename* は保存するファイルの場所と名前です。ファイルは .zip ファイルとして初期化されます。

注: コマンド構文の *esm* パラメーターはサポートされていません。

4. 診断データを処理するには、次の表に記載されている指示に従います。

表 40. リカバリー・ステップ 4

発生した内容	対策
エラーは返されませんでした	ステップ 6 に進みます。

表 40. リカバリー・ステップ 4 (続き)

発生した内容	対策	
エラーが返されました	発生した内容	対策
	エラー・メッセージは、データの保存に問題があったことを示しています。	2 分待ってから、ステップ 3 を再開します。
	エラー・メッセージは、データのリセットに問題があったことを示しています。	2 分待ってから、ステップ 5 に進みます。

5. Type (タイプ)

```
reset storageSubsystem diagnosticData;
```

表 41. リカバリー・ステップ 5

発生した内容	対策
エラーは返されませんでした	ステップ 6 に進みます。
エラーが返されました	2 分待ってから、コマンドを再度実行してください。コントローラーによる状況の更新に、さらに時間がかかる可能性があります。 注: 診断データの状況が既にリセットされている場合は、別のエラーが発生する可能性があります。 ステップ 6 に進みます。

6. 「**Recheck (再検査)**」をクリックして、Recovery Guru を再実行します。この障害はもう「**Summary (要約)**」領域には表示されません。

この処理が完了すると、DDC メッセージは自動的に削除され、Recovery Guru の再検査で DDC キャプチャーのエントリは表示されなくなります。何らかの理由でデータが削除されない場合、Recovery Guru は、データを保存せずに DDC 情報をクリアする方法の例を示します。上記の手順をスクリプト・エディターで実行するには、次のように入力します。

```
reset storageSubsystem diagnosticData;
```

DDC MEL イベント

異常イベントによって「Diagnostic Data Capture (診断データ・キャプチャー)」アクションが引き起こされると、ユーザー処置に応じて、以下のイベントのうち 1 つ以上がストレージ・サブシステムのイベント・ログに記入されます。

表 42. DDC MEL イベント

イベント番号	説明	優先度	説明
0x6900	診断データが使用可能です。	重大	これは、異常なコントローラー・イベントがきっかけとなって DDC 機能が診断データを保存した場合にログに記録されます。
0x6901	診断データの検索操作が開始されます。	通知	これは、287 ページの『リカバリー手順』のステップ 3 で説明したように、ユーザーが SMcli コマンドを実行して診断データの検索および保存を行った場合に、ログに記録されます。
0x6902	診断データの検索操作が完了しました。	通知	これは、診断データの検索および保存が完了した場合に、ログに記録されます。

表 42. DDC MEL イベント (続き)

イベント番号	説明	優先度	説明
0x6903	「Diagnostic Data Needs Attention (診断データ要注意)」状況/フラグはクリアされました。	通知	これは、ユーザーが SMcli コマンドを使用して「Needs Attention due to DDC (DDC により要注意)」フラグをリセットした場合、またはユーザーが save storageSubsystem diagnosticData SMcli コマンドを実行して開始した診断データの検索および保存が正常に完了した場合に、ログに記録されます。

AIX でのディスク・アレイのエラーの解決

このセクションでは、AIX エラー・ログで報告される場合があるディスク・アレイ・エラーについて説明します。AIX エラー・ログは、**errpt -a** コマンドを使用することによって表示することができます。また、ストレージ・マネージャーの主なイベント・ログ (MEL) を確認して、ホストと SAN とストレージ・サブシステムの間で相関関係があるかどうかを見つけることができます。

状況を訂正するために、構成を検証するかまたは障害のあるハードウェアを交換する必要がある場合があります。

注: トラブルシューティング情報については、ストレージ・サブシステムに付属の「インストール、メンテナンスおよびユーザーのガイド」を参照してください。

表 43. ディスク・アレイ・エラー

エラー番号	エラー名	エラー・タイプ	エラーの説明
1	FCP_ARRAY_ERR1	ARRAY OPERATION ERROR	ディスク・アレイ・メディア関連のハードウェアの永続エラーが発生しました。
2	FCP_ARRAY_ERR2	ARRAY OPERATION ERROR	永続ハードウェア・エラーが発生しました。
3	FCP_ARRAY_ERR3	ARRAY OPERATION ERROR	アレイ・アダプターによって永続エラーが検出されました。
4	FCP_ARRAY_ERR4	ARRAY OPERATION ERROR	アレイ、通信、またはアダプターの内部で一時的エラーが発生しました。
5	FCP_ARRAY_ERR5	UNDETERMINED ERROR	未判別エラーが発生しました。
6	FCP_ARRAY_ERR6	SUBSYSTEM COMPONENT FAILURE	ディスク・ドライブ以外で低下状態が発生しました。
7	FCP_ARRAY_ERR7	CONTROLLER HEALTH CHECK FAILURE	パッシブなコントローラー上での正常性検査が失敗しました。
8	FCP_ARRAY_ERR8	ARRAY CONTROLLER SWITCH	1 個のアレイ・コントローラーが使用できなくなったため、入出力が別のコントローラーに移動しました。
9	FCP_ARRAY_ERR9	ARRAY CONTROLLER SWITCH FAILURE	アレイ・コントローラーの切り替えで障害が発生しました。
10	FCP_ARRAY_ERR10	ARRAY CONFIGURATION CHANGED	論理装置が、あるコントローラーから別のコントローラーに移動されました (ほとんどの場合、代替ホストのアクションによります)。

表 43. ディスク・アレイ・エラー (続き)

エラー番号	エラー名	エラー・タイプ	エラーの説明
11	FCP_ARRAY_ERR11	IMPROPER DRIVE TYPE FOR DUAL ACTIVE MODE	このエラーは、2102 アレイでは発生せず、履歴の目的のためにのみ存在します。 FCP_ARRAY_ERR11 は、今後別のエラーに再利用される可能性があります。
12	FCP_ARRAY_ERR12	POLLED AEN FAILURE	自動エラー通知で障害が発生しました。
13	FCP_ARRAY_ERR13	ARRAY INTER-CONTROLLER COMMUNICATION FAILURE	コントローラーがお互いに通信できません。 このエラーは、エラー・ログの生成中にいずれか 1 つのコントローラーがリブートされたために発生する場合があります。ただし、ファイバー・チャネル接続の問題を示している可能性もあります。
14	FCP_ARRAY_ERR14	ARRAY DRIVE FAILURE	ストレージ・サブシステム内の物理ディスク上で重大エラーまたはリカバリー不能エラーが検出されました。システム・エンジニアが、センス・データを分析して正確な原因を見つけることができる場合があります。
15	FCP_ARRAY_ERR15	CACHE BATTERY LOW/DATA LOSS POSSIBLE	コントローラー・カードを交換した場合、キャッシュ・バッテリーが枯渇する可能性があります。キャッシュ・バッテリーを再充電するには、2 日かかる場合があります。この間、エラーがエラー・ログに記録されます。コントローラーを交換しないでください。
16	FCP_ARRAY_ERR16	CACHE BATTERY CHARGE BELOW 87.5%	コントローラー・カードを交換した場合、キャッシュ・バッテリーが枯渇する可能性があります。キャッシュ・バッテリーを再充電するには、2 日かかる場合があります。この間、エラーがエラー・ログに記録されます。コントローラーを交換しないでください。
17	FCP_ARRAY_ERR17	WORLDWIDE NAME CHANGED	コントローラーによって worldwide name が変更されました。このエラーは、コントローラーを最初にリセット状態にせずに交換する場合、または配線を変更し、SCSI ID が同じである別のコントローラーがループ上に存在する場合に発生することがあります。
18	FCP_ARRAY_ERR18	RESERVATION CONFLICT	ディスク・アレイ論理ドライブ (LUN) が他のホストに予約されているため、操作が失敗しました。
19	FCP_ARRAY_ERR19	SNAPSHOT VOLUME REPOSITORY FULL	リポジトリの容量が限度に達しました。このエラーを解決するには、リポジトリの容量を増やします。
20	FCP_ARRAY_ERR20	SNAPSHOT OPERATION STOPPED BY ADMIN	FlashCopy(スナップショット) 操作が使用不可になったかまたは停止されました。このエラーを解決するには、FlashCopy を再作成します。

表 43. ディスク・アレイ・エラー (続き)

エラー番号	エラー名	エラー・タイプ	エラーの説明
21	FCP_ARRAY_ERR21	SNAPSHOT REPOSITORY METADATA ERROR	FlashCopy 操作中に、FlashCopy(スナップショット) リポジトリのメタデータに問題がありました。このエラーを解決するには、FlashCopy を再作成します。
22	FCP_ARRAY_ERR22	REMOTE VOL MIRRORING: ILLEGAL I/O ORIGIN	1 次論理ドライブがリモート・アレイから入出力を受け取ったか、2 次論理ドライブが 1 次論理ドライブ以外のソースから入出力を受け取りました。このエラーを解決するには、操作を再試行します。
23	FCP_ARRAY_ERR23	SNAPSHOT OPERATION NOT ALLOWED	リポジトリの容量が限度に達し、FlashCopy (スナップショット) 操作が失敗しました。このエラーを解決するには、FlashCopy を削除または再作成します。
24	FCP_ARRAY_ERR24	SNAPSHOT VOLUME REPOSITORY FULL	リポジトリの容量が限度に達しました。このエラーを解決するには、FlashCopy (スナップショット) を削除または再作成します。
25	FCP_ARRAY_ERR25	CACHED DATA WILL BE LOST IF CONTROLLER FAILS	このメッセージは、書き込みキャッシュが使用可能で、かつキャッシュのミラーリングが使用不可という状態で、ディスク・アレイ論理ドライブ (LUN) が実行しているという警告です。警告は、LUN が開いたときに表示され、キャッシュのミラーリングが再度使用可能になるまで、24 時間ごとに表示されます。 LUN がこのモードで実行している間にコントローラーに障害が発生したか、またはコントローラーの電源がオフになった場合、書き込みキャッシュ内にある (ただし物理ディスク・メディアに書き込まれていない) データは失われる可能性があります。これは、ファイル、ファイル・システム、またはデータベースが壊れる原因になることがあります。

表 43. ディスク・アレイ・エラー (続き)

エラー 番号	エラー名	エラー・タイプ	エラーの説明
26	FCP_ARRAY_ERR26	LOGICAL VOLUME IS WRITE PROTECTED	論理ドライブの状況が読み取り専用です。予想される理由は、このドライブが FlashCopy、VolumeCopy、またはリモート・ミラー・ペアの 2 次論理ドライブであることです。この論理ドライブに、どの関係が当てはまるか判別してください。 - FlashCopy の場合、2 次論理ドライブの読み取り専用の状況は、通常、リポジトリがいっぱいであることを示しています。 - VolumeCopy の場合、コピー操作中は 1 次と 2 次の両方の論理ドライブが読み取り専用になります。2 次論理ドライブが読み取り専用になるのは、コピー操作が停止されてコピー・ペアが削除されていない場合です。 - リモート・ミラーリングの場合、2 次論理ドライブは、ミラーがアクティブである限り、常に読み取り専用です。
27	FCP_ARRAY_ERR27	SINGLE CONTROLLER RESTARTED	ストレージ・サブシステムはシングル・コントローラーとして作動しており、エラーは修復されました。エラーは、通信の問題またはハードウェア障害が原因であったか、現行ホストへのパスを持っていないコントローラーに LUN が移動されたために起きた可能性があります。 これがデュアル・コントローラー・ストレージ・サブシステムの場合は、ストレージ・サブシステムがシングル・コントローラー・モードで作動している理由を見つけ、問題を解決してください。考えられる理由として、以下の原因が挙げられます。 - 前回のシステム再始動のとき、または前回 cfgmgr コマンドを実行したときに、HBA、スイッチ・ポート、スイッチ、ストレージ・サブシステム・ポート、ストレージ・サブシステム・コントローラーのいずれかが利用不可だった。 - バス (dac) をファイバー・チャネル・アダプターのホット・スワップ操作の一部として除去した。

表 43. ディスク・アレイ・エラー (続き)

エラー番号	エラー名	エラー・タイプ	エラーの説明
28	FCP_ARRAY_ERR28	SINGLE CONTROLLER RESTART FAILURE	ストレージ・サブシステムはシングル・コントローラーとして作動しており、エラーは修復されていません。このホストとストレージ・サブシステム間のパス、またはストレージ・サブシステム自体に問題があります。ホストはストレージ・サブシステムとの通信を試みましたが、その通信が失敗しました。 ODM 属性 <code>switch_retries</code> で指定した再試行回数に到達した場合、入出力は失敗し、ユーザーへ戻されます。 エラーを修復してください。その後、これがデュアル・コントローラー・ストレージ・サブシステムの場合は、ストレージ・サブシステムがシングル・コントローラー・モードで作動している理由を見つけ、その問題を解決してください。考えられる理由として、以下の原因が挙げられます。 • 前回のシステム再始動のとき、または前回 cfgmgr コマンドを実行したときに、HBA、スイッチ・ポート、スイッチ、ストレージ・サブシステム・ポート、ストレージ・サブシステム・コントローラーのいずれかが利用不可だった。 • パス (dac) をファイバー・チャネル・アダプターのホット・スワップ操作の一部として除去した。

新規エラー・ログ `DISK_ERR7` が作成されました。これは、パスで発生した入出力エラーの数があらかじめ設定されている数に達したために、そのパスが障害発生パスとみなされたことを示すものです。通常はこの前に、パスで発生した実際のエラーを表す他のエラー・ログが作成されています。

付録 A. ホスト・バス・アダプターの設定

この章では、Windows、Linux on Intel、VMware ESX、および NetWare オペレーティング・システム用の DS3000/DS4000/DS5000 ストレージ・サブシステムでの使用に適した、さまざまなホスト・バス・アダプター (HBA) のデフォルト設定について説明します。その他のすべてのオペレーティング・システムおよびプラットフォームの場合は、デフォルト値を使用する必要があります。詳しくは、該当する製品資料を参照してください。

設定に関する最新の変更情報については、ファイバー・チャネル・ホスト・バス・アダプター BIOS またはデバイス・ドライバのパッケージに含まれている README ファイルを参照してください。

HBA は、サーバーをファイバー・チャネル・トポロジに接続するために使用されます。その機能は、LAN リソースにアクセスするためにネットワーク・アダプターによって提供される機能と似ています。HBA 用のデバイス・ドライバは、通常、ファイバー・チャネル・トポロジ (ポイント・ツー・ポイント、ループ、またはファブリック) に対するサポートを提供します。

重要: IBM は、同じ HBA を使用した同一サーバー内の DS3000、DS4000、および DS5000 ストレージ・サブシステムの共存をサポートします。ただし、アプリケーションがデバイスおよびマルチパス・ドライバのタイムアウト設定値の共通セットに対応できる場合に限りです。タイムアウト設定値の共通セットは、このセクションで DS3000、DS4000、および DS5000 ストレージ・サブシステムに関して公開されている最長の設定値で構成されます。これが可能でなくても、マルチパス・ドライバが許可する場合は、DS3000 サブシステムに使用する HBA が DS4000 または DS5000 ストレージ・サブシステムに使用するものと異なっていれば、DS3000、DS4000、および DS5000 ストレージ・サブシステムの混合を使用することができます。そうでない場合、同一サーバー内の DS3000、DS4000、および DS5000 ストレージ・サブシステムの共存は不可能です。

同一サーバー内の DS3000、DS4000、および DS5000 ストレージ・サブシステムの共存に関する制約事項については、最新の IBM DS コントローラー・ファームウェアおよびストレージ・マネージャーの README ファイルを参照してください。HBA サポートの詳細情報は、次の Web サイトを参照してください。 www.ibm.com/systems/support/storage/config/ssic。

HBA 設定の調整

装置の能力に合わせて、HBA の設定を調節することが必要な場合がよくあります。このセクションでは、これらの設定にアクセスし、必要な調整を行う方法について説明します。

Fast!UTIL による HBA 設定へのアクセス

Fast!UTIL 機能を使用すると、ホスト・バス・アダプターの設定にアクセスできます。この機能にアクセスするには、BIOS 初期化中に Alt+Q または Ctrl+Q を押します。Fast!UTIL のメニューが表示されるまでに、数秒かかる場合があります。複数のアダプターが取り付けられている場合は、構成するアダプターを選択するための Fast!UTIL のプロンプトが表示されます。アダプター設定の変更が済むと、Fast!UTIL はサーバーを再始動して、新しいパラメーターをロードします。Fast!UTIL が開始された後、「Fast!UTIL Options (Fast!UTIL オプション)」メニューでは以下の選択肢を使用できます。

- 「Configuration Settings (設定の構成)」
- 「Loopback Test (ループバック・テスト)」

- 「Select Host Adapter (ホスト・アダプターの選択)」

また、ホスト・バス・アダプターの設定にアクセスするには、Fast!UTIL の「**Configuration Settings (設定の構成)**」メニューから「**Adapter Settings (アダプターの設定)**」または「**Advanced Adapter Settings (拡張アダプター設定)**」を選択します。

注: あるいは、QLogic SANsurfer プログラムを使用して、Microsoft Windows オペレーティング・システム環境から **Host adapter settings (ホスト・アダプターの設定)** および **Advanced adapter settings (拡張アダプターの設定)** プリファレンスを変更することもできます。変更を有効にするにはサーバーを再始動する必要があります。

デフォルトのホスト・バス・アダプター設定値

ホスト・バス・アダプターの設定にアクセスするには、Fast!UTIL の「**Configuration Settings (設定の構成)**」メニューを選択し、「**Adapter Settings (アダプターの設定)**」を選択します。FC2-133 HBA に対するホスト・バス・アダプターのデフォルトの設定は、次のとおりです。

Host Adapter BIOS (ホスト・アダプター BIOS)

この設定が「Disabled (使用不可)」の場合は、FC2-133 HBA の ROM BIOS が使用不可になり、上位メモリーのスペースが使用可能になります。FC2-133 アダプターに接続されたファイバー・チャンネル・ディスク・ドライブからブートしている場合は、この設定を「Enabled (使用可能)」にする必要があります。デフォルトは「Disabled (使用不可)」です。

Frame Size (フレーム・サイズ)

この設定は、FC2-133 HBA がサポートする最大フレーム長を指定します。デフォルトのサイズは 2048 で、F-Port (ポイント・ツー・ポイント) 接続の最高のパフォーマンスを提供します。

Loop Reset Delay (ループ・リセット遅延)

ループをリセットすると、ファームウェアは、この設定で指定されている秒数の間、いかなるループ活動も行いません。デフォルトは 5 秒です。

Adapter Hard Loop ID (アダプター・ハード・ループ ID)

この設定は、「Hard Loop ID (ハード・ループ ID)」設定で指定されている ID の使用をアダプターが試みるように強制します。デフォルトは「Enabled (使用可能)」です。

Hard Loop ID (ハード・ループ ID)

「Adapter Hard Loop ID (アダプター・ハード・ループ ID)」の設定が「Enabled (使用可能)」の場合、アダプターは、この設定で指定されている ID の使用を試みます。デフォルトの ID は 125 です。複数のアダプターが FC-AL に接続されていて、「Adapter Hard Loop ID (アダプター・ハード・ループ ID)」の設定が「Enabled (使用可能)」の場合は、この ID に 0 - 125 の範囲の固有値を設定します。

Spin Up Delay (スピンアップ遅延)

このビットがセットされていると、BIOS は、最初のドライブを検出するまでに最大で 5 分間待ちます。デフォルトの設定は「Disabled (使用不可)」です。

Connection Options (接続オプション)

この設定は、接続のタイプ (ループまたはポイント・ツー・ポイント) または接続のプリファレンスを定義します。デフォルトは 2 で、ポイント・ツー・ポイントよりループが優先されることを意味します。

Fibre Channel Tape Support (ファイバー・チャネル・テープ・サポート)

この設定は、FCP-2 リカバリーを使用可能にします。デフォルトは「Enabled (使用可能)」です。HBA が磁気テープ装置に接続されていない場合は、この設定を「Disabled (使用不可)」に変更します。

Data Rate (データ速度)

この設定はデータの速度を決定します。この設定が 0 の場合、FC2-133 HBA は 1 Gbps で動作します。この設定を 1 にすると、FC2-133 HBA は 2 Gbps で動作します。この設定を 2 にすると、システムが対応できる速度を Fast!UTIL が判断し、それに従って速度を設定します。デフォルトは 2 (自動構成) です。

拡張 HBA 設定

以下の拡張ホスト・バス・アダプター設定にアクセスするには、Fast!UTIL の「**Configuration Settings (設定の構成)**」メニューを選択し、「**Advanced Adapter Settings (拡張アダプター設定)**」を選択します。FC2-133 HBA に対するデフォルトの設定は、次のとおりです。

Execution Throttle (実行スロットル)

この設定では、1 つのポートで実行されるコマンドの最大数を指定します。ポートの実行スロットルに達すると、現行のコマンドが終了するまで、新しいコマンドは実行されません。この設定に対する有効なオプションは 1 から 256 です。デフォルトは 255 です。

LUNs per Target (ターゲット当たり LUN 数)

この設定は、ターゲットごとの LUN の数を指定します。通常、複数 LUN のサポートは、ドライブをマップするために LUN を使用する新磁気ディスク制御機構 (RAID) システムのためです。デフォルトは 0 です。Microsoft Windows 以外のホスト・オペレーティング・システムでは、この設定を 0 以外の値に変更して、ホストがストレージ・サブシステムから複数の論理ドライブを認識できるようにすることが必要な場合があります。

Enable LIP Reset (LIP リセットの使用可能化)

この設定は、オペレーティング・システムがバス・リセット・ルーチンを開始するときに使用される、ループ初期化プロセス (LIP) リセットのタイプを決定します。この設定が Yes の場合には、ドライバーはグローバル LIP リセットを開始してターゲット装置の予約をクリアします。この設定が no のときには、ドライバーはフル・ログインでグローバル LIP リセットを開始します。デフォルトは「No」です。

Enable LIP Full Login (LIP フル・ログインの使用可能化)

この設定は、ISP チップに対し、LIP の後ですべてのポートに再ログインするよう指示します。デフォルトは Yes です。

Enable Target Reset (ターゲット・リセット使用可能化)

この設定は、SCSI バス・リセット・コマンドが実行されたときに、ドライバーがループ上のすべての装置に対してターゲット・リセット・コマンドを実行できるようにします。デフォルトは Yes です。

Login Retry Count (ログイン再試行カウント)

この設定は、ソフトウェアが装置へのログインを試みる回数を指定します。デフォルトは 30 回です。

Port Down Retry Count (ポート・ダウン再試行カウント)

この設定は、ポート・ダウン状況を戻すポートに対してソフトウェアがコマンドを再試行するまでに経過する秒数を指定します。デフォルトは 30 秒です。MSCS 構成の Microsoft Windows サーバーの場合、ポート・ダウン再試行カウント BIOS パラメーターはデフォルトの 30 から 70 に変更する必要があります。

Link Down Timeout (リンクダウン・タイムアウト)

この設定は、ソフトウェアがリンクダウンの回復を待つ秒数を指定します。デフォルトは 60 秒です。

Extended Error Logging (拡張エラー・ログ)

この設定は、エラーとデバッグに関する追加情報をオペレーティング・システムに提供します。使用可能にすると、Windows NT のイベント・ビューアーにイベントが記録されます。デフォルトは「Disabled (使用不可)」です。

RIO Operation Mode (RIO 動作モード)

この設定は、ソフトウェア・ドライバがサポートしている場合には、縮小割り込み動作 (RIO) モードを指定します。RIO モードを使用すると、単一の割り込みで複数のコマンド完了を通知できます。デフォルトは 0 です。

Interrupt Delay Timer (割り込み遅延タイマー)

この設定には、タイマーがハンドルのセットにアクセスして (DMA) 割り込みを生成する間の待ち時間を設定するために使用される値 (100 マイクロ秒単位) が含まれます。デフォルトは 0 です。

QLogic ホスト・バス・アダプターの設定

重要: IBM は、同じ HBA を使用した同一サーバー内の DS3000、DS4000、および DS5000 ストレージ・サブシステムの共存をサポートします。ただし、アプリケーションがデバイスおよびマルチパス・ドライバのタイムアウト設定値の共通セットに対応できる場合に限りです。タイムアウト設定値の共通セットは、このセクションで DS3000、DS4000、および DS5000 ストレージ・サブシステムに関して公開されている最長の設定値で構成されます。これが可能でなくても、マルチパス・ドライバが許可する場合は、DS3000 サブシステムに使用する HBA が DS4000 または DS5000 ストレージ・サブシステムに使用するものと異なっていれば、DS3000、DS4000、および DS5000 ストレージ・サブシステムの混合を使用することができます。そうでない場合、同一サーバー内の DS3000、DS4000、および DS5000 ストレージ・サブシステムの共存は不可能です。

同一サーバー内の DS3000、DS4000、および DS5000 ストレージ・サブシステムの共存に関する制約事項については、最新の IBM DS コントローラー・ファームウェアおよびストレージ・マネージャーの README ファイルを参照してください。HBA サポートの詳細情報は、次の Web サイトを参照してください。www.ibm.com/systems/support/storage/config/ssic.

注: Windows 列の BIOS 設定は、IBM FC-2 (QLA2310)、FC2-133 (QLA2340)、および単一ポートとデュアル・ポート 4 Gbps (QLx2460 と QLx2462) ファイバー・チャネル・ホスト・バス・アダプターとして IBM にアダプターを注文した場合に設定される、デフォルト値です。IBM にアダプターを注文しない場合は、デフォルトの BIOS 設定が Microsoft Windows 列で定義されているものと異なる可能性があります。例外が 1 つあり、ファイバー・チャネル・テープ・サポートに対するデフォルトの設定は使用可能です。

299 ページの表 44 は、オペレーティング・システムごとの IBM ファイバー・チャネル FC-2 および FC2-133 (QLogic アダプター・モデル QLA2310 および QLA2340) ホスト・バス・アダプターの設定 (BIOS V1.35 以降の場合) および Microsoft Windows オペレーティング・システムのデフォルトのレジストリー設定を示しています。DS3000/DS4000/DS5000 製品では、これらのアダプターに対して BIOS V1.43 以降が必要です。さらに、これらの値は、新規の DS3000/DS4000/DS5000 4 Gbps 単一およびデュアル・ポート・ホスト・バス・アダプター (QLogic アダプター・モデル QLx2460 および QLx2462) 用のデフォルトの BIOS 設定です。4 Gbps ホスト・バス・アダプターの BIOS バージョンは 1.12 以降です。これらの値に対する最新の更新情報については、該当する README ファイルを参照してください。

表 44. QLogic モデル QLA234x、 QLA24xx、 QLE2462、 QLE2460、 QLE2560、 QLE2562、 QMI2572、 QMI3572、 QMI2582

項目	デフォルト	VMware	Windows 2000	Windows 2003 および Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
BIOS の設定								
ホスト・アダプターの設定								
Host Adapter BIOS (ホスト・アダプター BIOS)	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Frame Size (フレーム・サイズ)	2048	2048	2048	2048	2048	2048	2048	2048
Loop Reset Delay (ループ・リセット遅延)	5	5	8	8	8	8	8	8
Adapter Hard Loop ID (アダプター・ハード・ループ ID) - (アービトレーテッド・ループ・トポロジーのみ)	使用不可	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能
Hard Loop ID (ハード・ループ ID) (HBA ごとに固有でなければなりません) - (アービトレーテッド・ループ・トポロジーのみ)	0	125 ¹	125 ¹	125 ¹	125 ¹	125 ¹	125 ¹	125 ¹
Spin-up Delay (スピンアップ遅延)	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Connect Options (接続オプション)	2	2	2	2	2	2	2	2
Fibre Channel Tape Support (ファイバー・チャネル・テープ・サポート)	使用不可	使用不可 ³	使用不可 ³	使用不可 ³	使用不可 ³	使用不可 ³	使用不可 ³	使用不可 ³
Data Rate (データ速度)	2	2 (自動)	2 (自動)	2 (自動)	2 (自動)	2 (自動)	2 (自動)	2 (自動)
拡張アダプターの設定								
Execution Throttle (実行スロットル)	16	256	256	256	256	256	256	256
LUNs per Target (ターゲット当たり LUN 数)	8	0	0	0	0	0	0	32
Enable LIP Reset (LIP リセットの使用可能化)	なし	なし	なし	なし	なし	なし	なし	なし
Enable LIP Full Login (LIP フル・ログインの使用可能化)	はい	はい	はい	はい	はい	はい	はい	はい

表 44. QLogic モデル QLA234x、 QLA24xx、 QLE2462、 QLE2460、 QLE2560、 QLE2562、 QMI2572、 QMI3572、 QMI2582 (続き)

項目	デフォルト	VMware	Windows 2000	Windows 2003 および Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
Enable Target Reset (ターゲット・リセット使用可能化)	はい	はい	はい	はい	はい	はい	はい	はい
Login Retry Count (ログイン再試行カウント)	8	30	30	30	30	30	30	30
Port Down Retry Count (ポート・ダウン再試行カウント) (5.30 以前のコントローラー・ファームウェア)	8	30	30	30	30	12	12	70
Port Down Retry Count (ポート・ダウン再試行カウント)	8	70	DS3K: 144 DS4K/5K: 70 ²	DS3K: 144 DS4K/5K: 70 ²	70	DS3K: 70 DS4K/5K: 35	10	70
Link Down Timeout (リンクダウン・タイムアウト)	30	60	DS3K:144 DS4K/5K: 60	DS3K:144 DS4K/5K: 60	60	DS3K:144 DS4K/5K: 60	NA	60
Extended Error Logging (拡張エラー・ログ)	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
RIO Operation Mode (RIO 動作モード)	0	0	0	0	0	0	0	0
Interrupt Delay Timer (割り込み遅延タイマー)	0	0	0	0	0	0	0	0
IOCB Allocation (IOCB 割り振り)	256	256	256	256	256	256	256	256
>4 GB Addressing (4 GB を超えるアドレッシング)	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Drivers Load RISC Code (ドライバーが RISC コードをロード)	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能
Enable Database Updates (データベース更新の使用可能可)	なし	なし	なし	なし	なし	なし	なし	なし
Disable Database Load (データベース・ロードの使用不可化)	なし	なし	なし	なし	なし	なし	なし	なし
Fast Command Posting (高速コマンド通知)	使用不可	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能

拡張ファームウェア設定 (1.34 以前)

表 44. QLogic モデル QLA234x、 QLA24xx、 QLE2462、 QLE2460、 QLE2560、 QLE2562、 QMI2572、 QMI3572、 QMI2582 (続き)

項目	デフォルト	VMware	Windows 2000	Windows 2003 および Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
Extended Control Block (拡張制御ブロック)	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能	使用可能
RIO Operation Mode (RIO 動作モード)	0	0	0	0	0	0	0	0
Connection Options (接続オプション)	2	2	2	2	2	2	2	2
Class 2 Service (クラス 2 サービス)	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
ACK0	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Fibre Channel Tape Support (ファイバー・チャネル・テープ・サポート)	使用可能	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Fibre Channel Confirm (ファイバー・チャネル確認)	使用可能	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Command Reference Number (コマンド参照番号)	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Read Transfer Ready (読み取り転送レディー)	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可	使用不可
Response Timer (応答タイマー)	0	0	0	0	0	0	0	0
Interrupt Delay Timer (割り込み遅延タイマー)	0	0	0	0	0	0	0	0
Data Rate (データ速度)	2	2 (自動)	2 (自動)	2 (自動)	2 (自動)	2 (自動)	2 (自動)	2 (自動)

レジストリー設定 ⁵ (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\QL2300\Parameters\Device)

LargeLuns	1	1	N/A	N/A	N/A	N/A	N/A	N/A
MaximumSGList	0x21	0xff	0xff	0xff	N/A	N/A	N/A	N/A

O/S レジストリー設定 ⁵ (HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\QL2300\Parameters\Device)

DriverParameter 変数の下

注:

1. QLogic ドライバーのバージョン 9.1.x.x より前は、使用される変数名は、DriverParameter ではなく、DriverParameters でした。
2. DriverParameter のタイプは REG_SZ であり、以下のパラメーターが DriverParameters スtringに追加されます。パラメーターごとに別々のキーを作成しないでください。

UseSameNN	1	1	1	1	N/A	N/A	N/A	N/A

表 44. QLogic モデル QLA234x、QLA24xx、QLE2462、QLE2460、QLE2560、QLE2562、QMI2572、QMI3572、QMI2582 (続き)

項目	デフォルト	VMware	Windows 2000	Windows 2003 および Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare
BusChange (SCSI Port ミニポート 9.0.1.60 以前 – 9.1.1.11 以降には適用されません)	2	N/A	0	0	N/A	N/A	N/A	N/A
TimeoutValue 4 (REG_DWORD)	0x3C	N/A	DS3K: xA0 DS4K/5K: x78	DS3K: xA0 DS4K/5K: x78	N/A	N/A	N/A	N/A

レジストリー設定⁵ (HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\<FAILOVER>\parameters。ここで、MPP または RDAC インストールの場合は <FAILOVER>=Rdacadisk、もしくは MPIO インストールの場合は <FAILOVER>=mppdsm、ds4dsm、md3dsm、sx3dsm、csmdsm、または tpsdsm です。Mppdsm は汎用バージョン用であり、ご使用のインストールでは異なる場合があります。)

SynchTimeout (REG_DWORD)	0x78	N/A	DS3K: xA0 DS4K/5K: x78	DS3K: xA0 DS4K/5K: x78				
DisableLunRebalance (クラスター構成のみに適用。ファームウェア・バージョン 6.xx.xx.xx 以降。)	0x00	N/A	0x03	0x03				

SuSE 7.3 固有の変更:

- アレイ・コントローラーの NVSRAM の Linux 領域 (6) におけるオフセット 0x11 は、デフォルトの 0x20 から 0x7f に変更されなければなりません。以下のコマンドはスクリプト・エンジンから実行できます。
 - controller[a] HOSTNVSRAMByte[6,0x11]=0x7f を設定する
 - controller[b] HOSTNVSRAMByte[6,0x11]=0x7f を設定する
- SuSE で使用されるシンボリック・リンクを反映するように、QLogic ドライバー・ソースが変更されなければなりません。
 - vi makefile
 - OSVER を検出し、それを OSVER=linux-2.4 から OSVER=linux に変更する
 - 保存して終了する

Red Hat Linux Advanced Server 2.1 / SuSE Linux Enterprise Server 8.0 (6.x シリーズのフェイルオーバー・ドライバー [RDAC なし] のみ)。/etc/modules.conf ファイルの HBA ドライバー・オプション・ストリングに以下を追加します。ql2xretrycount=60 ql2xsuspendcount=40

QLogic インボックス・ドライバーを実行している場合、ストリング options qla2xxx qlport_down_retry=144 (PB1-3) または options qla2xxx qlport_down_retry=70 (PB4-6) が、/etc/modprobe.conf (RHEL の場合) または /etc/modprobe.conf.local (SLES の場合) で追加されなければなりません。以前のすべての (RH3/4 SLES8/9) Linux バージョン (および非インボックス・ドライバー) の場合、代わりにストリング options qla2xxx qlport_down_retry=72 (PB1-3) または options qla2xxx qlport_down_retry=35 (PB4-6) が追加されなければなりません。

表 44. QLogic モデル QLA234x、QLA24xx、QLE2462、QLE2460、QLE2560、QLE2562、QMI2572、QMI3572、QMI2582 (続き)

項目	デフォルト	VMware	Windows 2000	Windows 2003 および Windows 2008	Solaris	LINUX MPP	LINUX DMMP	NetWare

注:

1. FC-AL ループに複数のファイバー・チャネル装置がある場合は、この設定を固有の AL-PA 値に変更する必要があります。
2. I/O 負荷の重い大規模な構成や Microsoft クラスタ・サービス (MSCS) 環境の場合は、この値が増える可能性があります。
3. HBA が磁気テープ装置にだけ接続されている場合は、この設定を「Enabled (使用可能)」または「Supported (サポート)」に変更します。DS3000、DS4000、または DS5000 ストレージ・サブシステムに接続するときは、「Disabled (使用不可)」に設定します。
4. 特定のストレージ・サブシステムの最大構成インストール済み環境では、TimeOutValue を 120 (10 進) に設定することが必要になる場合があります。この値を大きくすると、特に特定の時間内にディスク I/O 完了応答を必要とするアプリケーションに影響する場合があります。
5. 「スタート」をクリックし、「ファイル名を指定して実行」を選択し、「名前」フィールドに「regedit」と入力して、「OK」をクリックすると、レジストリー設定にアクセスすることができます。
重要: Windows のレジストリーを変更する際には注意が必要です。間違ったレジストリー項目を変更したり、正しくない値を設定したりすると、サーバーがブートしなくなったり、正しく動作しなくなるエラーが発生する可能性があります。

注: Windows 列の下に BIOS 設定は、IBM ファイバー・チャネル・ホスト・バス・アダプターとして IBM にアダプターを注文した場合に設定される、デフォルト値です。IBM にアダプターを注文しない場合は、デフォルトの BIOS 設定が Microsoft Windows 列のものと異なる可能性があります。例外が 1 つあり、ファイバー・チャネル・テープ・サポートに対するデフォルトの設定は使用可能です。

表 45 に示すのは、さまざまな IBM DS3000/DS4000/DS5000 ファイバー・チャネル・ホスト・バス・アダプター (QLogic アダプター QL220x) モデル (BIOS V1.81 の場合) に対するオペレーティング・システム別のデフォルト設定です。これらの値に対する最新の更新情報については、該当する README ファイルを参照してください。

表 45. オペレーティング・システム別の QLogic モデル QL220x (BIOS V1.81 の場合) ホスト・バス・アダプターの設定

項目	Windows		Linux	NetWare
	NT	2000 / Server 2003		
BIOS の設定				
ホスト・アダプターの設定				
Host Adapter BIOS (ホスト・アダプター BIOS)	使用不可	使用不可	使用不可	使用不可
Frame Size (フレーム・サイズ)	2048	2048	2048	2048
Loop Reset Delay (ループ・リセット遅延)	5	5	8	5

表 45. オペレーティング・システム別の QLogic モデル QL220x (BIOS V1.81 の場合) ホスト・バス・アダプターの設定 (続き)

Adapter Hard Loop ID (アダプター・ハード・ループ ID)	使用可能	使用可能	使用可能	使用可能
Hard Loop ID (ハード・ループ ID) (HBA ごとに固有でなければなりません)	125 ¹	125 ¹	125 ¹	125 ¹
Spin Up Delay (スピンアップ遅延)	使用不可	使用不可	使用不可	使用不可
拡張アダプターの設定				
Execution Throttle (実行スロットル)	256	256	256	256
>4 Gbyte Addressing (4 Gbyte を超えるアドレッシング)	使用不可	使用不可	使用不可	使用不可
LUNs per Target (ターゲット当たり LUN 数)	0	0	0	32
Enable LIP Reset (LIP リセットの使用可能化)	なし	なし	なし	なし
Enable LIP Full Login (LIP フル・ログインの使用可能化)	はい	はい	はい	はい
Enable Target Reset (ターゲット・リセット使用可能化)	はい	はい	はい	はい
Login Retry Count (ログイン再試行カウント)	30	30	30	30
Port Down Retry Count (ポート・ダウン再試行カウント)	30	30	12	30 ²
IOCB Allocation (IOCB 割り振り)	256	256	256	256
Extended Error Logging (拡張エラー・ログ)	使用不可	使用不可	使用不可	使用不可
拡張ファームウェア設定				
Extended Control Block (拡張制御ブロック)	使用可能	使用可能	使用可能	使用可能
RIO Operation Mode (RIO 動作モード)	0	0	0	0
Connection Options (接続オプション)	3	3	3	3
Class 2 Service (クラス 2 サービス)	使用不可	使用不可	使用不可	使用不可
ACK0	使用不可	使用不可	使用不可	使用不可
Fibre Channel Tape Support (ファイバー・チャネル・テープ・サポート)	サポート ³	サポート ³	サポート ³	サポート ³
Fibre Channel Confirm (ファイバー・チャネル確認)	使用不可	使用不可	使用不可	使用不可

表 45. オペレーティング・システム別の QLogic モデル QL220x (BIOS V1.81 の場合) ホスト・バス・アダプターの設定 (続き)

Command Reference Number (コマンド参照番号)	使用不可	使用不可	使用不可	使用不可
Read Transfer Ready (読み取り転送レディー)	使用不可	使用不可	使用不可	使用不可
Response Timer (応答タイマー)	0	0	0	0
Interrupt Delay Time (割り込み遅延時間)	0	0	0	0
レジストリー設定 ⁴ (HKEY_LOCAL_MACHINE → System → CurrentControlSet → Services → QL2200 → Parameters → Device)				
LargeLuns		1		
MaximumSGList	0x21	0x21		
レジストリー設定 ⁴ (HKEY_LOCAL_MACHINE → System → CurrentControlSet → Services → Disk)				
TimeOutValue ⁴ (REG_DWORD)	0x3C	0x3C		
レジストリー設定 ⁴ (HKEY_LOCAL_MACHINE → System → CurrentControlSet → Services → QL2200 → Parameters → Device) DriverParameter 変数の下				
BusChange		0		

注:

1. FC-AL ループに複数のファイバー・チャネル装置がある場合は、この設定を固有の AL-PA 値に変更する必要があります。
2. I/O 負荷の重い大規模な構成の場合は、この値を 70 に変更します。
3. HBA が磁気テープ装置にだけ接続されている場合は、この設定を「Enable (使用可能)」または「Supported (サポート)」に変更します。DS3000、DS4000、または DS5000 ストレージ・サブシステムに接続するときは、「Disabled (使用不可)」に設定します。
4. レジストリー設定にアクセスするには、「スタート」をクリックし、「ファイル名を指定して実行」を選択し、「名前」フィールドに「regedit」と入力して、「OK」をクリックします。

重要: Windows のレジストリーを変更する際には注意が必要です。間違ったレジストリー項目を変更したり、正しくない値を設定したりすると、サーバーがブートしなくなったり、正しく動作しなくなるエラーが発生する可能性があります。

JNI および QLogic ホスト・バス・アダプター設定値

以下の表に、Sun Solaris 用のさまざまなホスト・バス・アダプター (HBA) の設定値が列挙されています。

注: JNI ホスト・バス・アダプターは Solaris 8 および 9 でのみサポートされます。Solaris 10 ではサポートされません。

JNI HBA カード設定値

JNI カードは自動構成によるプラグ・アンド・プレイではありません。自動構成の代わりに、設定値またはバインディングの変更が必要な場合があります。

FCE-1473/FCE-6460/FCX2-6562/FCC2-6562 の構成設定値

JNI ホスト・バス・アダプター・モデル FCE-1473、FCE-6460、FCX2-6562、および FCC2-6562 は、現在サポートされているすべてのレベルのストレージ・サブシステム・コントローラー・ファームウェアでサポートされています。

重要: 表 46 にリストされているそれぞれの設定値で行のコメントを外す必要があります。これは、デフォルトの設定値および変更が必要な設定値の両方にあてはまります。

表 46. FCE-1473/FCE-6460/FCX2-6562/FCC2-6562 の構成設定値

元の値	新規の値
FcLoopEnabled = 1	FcLoopEnabled = 0 (非ループ、自動トポロジの場合) FcLoopEnabled = 1 (ループの場合)
FcFabricEnabled = 0	FcFabricEnabled = 0 (非ファブリック、自動トポロジの場合) FcFabricEnabled = 1 (ファブリックの場合)
FcEngHeartbeatInterval = 5	元の値と同じ (秒単位)
FcLinkUpRecoveryTime = 1000	元の値と同じ (ミリ秒単位)。
BusRetryDelay = 5000	元の値と同じ (ミリ秒単位)。
TargetOfflineEnable = 1	TargetOfflineEnable = 0 (使用不可) TargetOfflineEnable = 1 (使用可能)
FailoverDelay = 30;	FailoverDelay = 60 (秒単位)
FailoverDelayFcTape = 300	元の値と同じ (秒単位)
TimeoutResetEnable = 0	元の値と同じ
QfullRetryCount = 5	元の値と同じ
QfullRetryDelay = 5000	元の値と同じ (ミリ秒単位)。
LunRecoveryInterval = 50	元の値と同じ (ミリ秒単位)。
FcLinkSpeed = 3	元の値と同じ
JNICreationDelay = 1	JNICreationDelay = 10 (秒単位)
FlogiRetryCount = 3	元の値と同じ
FcFlogiTimeout = 10	元の値と同じ (秒単位)
PlogiRetryCount = 3	元の値と同じ
PlogiControlSeconds = 30	元の値と同じ (秒単位)
LunDiscoveryMethod = 1	元の値と同じ (LUN のレポート)
CmdTaskAttr = 0	CmdTaskAttr = 0 (シンプル・キュー) CmdTaskAttr = 1 (タグなし)
automap = 0	automap = 1 (使用可能)
FclpEnable = 1	FclpEnable = 0 (使用不可)
OverrunFailoverCount = 0	元の値と同じ
PlogiRetryTime = 50	元の値と同じ
SwitchGidPtSyncEnable = 0	元の値と同じ
target_throttle = 256	元の値と同じ

表 46. FCE-1473/FCE-6460/FCX2-6562/FCC2-6562 の構成設定値 (続き)

元の値	新規の値
lun_throttle = 64	元の値と同じ
これらの設定値を追加します。	target0_hba = 『jnic146x0』;
	target0_wwpn = 『<controller wwpn>』
	target1_hba = 『jnic146x1』;
	target1_wwpn = 『<controller wwpn>』

注: Solaris のシェルから /etc/raid/bin/genjnicconf 再構成スクリプトを実行する必要がある場合があります。

```
# /etc/raid/bin/genjnicconf
```

FCE-1063/FCE2-1063/FCE-6410/FCE2-6410 の構成設定値

JNI ホスト・バス・アダプター・モデル FCE-1063、FCE2-1063、FCE-6410、および FCE2-6410 は、現在サポートされているすべてのレベルのストレージ・サブシステム・コントローラー・ファームウェアでサポートされています。

注: 表 47 にリストされているそれぞれの設定値で行のコメントを外す必要があります。これは、デフォルトの設定値および変更が必要な設定値の両方にあてはまります。

表 47. FCE-1063/FCE2-1063/FCE-6410/FCE2-6410 の構成設定値

元の値	新規の値
FcLoopEnabled = 1	FcLoopEnabled = 0 (非ループの場合) FcLoopEnabled = 1 (ループの場合)
FcFabricEnabled = 0	FcFabricEnabled = 0 (非ファブリックの場合) FcFabricEnabled = 1 (ファブリックの場合)
FcPortCfgEnable = 1	FcPortCfgEnable = 0 (ポートの再構成は必要ありません) FcPortCfgEnable = 1 (ポートの再構成が必要です)
FcEngHeartbeatInterval = 5	元の値と同じ (秒単位)
FcLrrTimeout = 100	元の値と同じ (ミリ秒単位)。
FcLinkUpRecoverTime = 1000	元の値と同じ (ミリ秒単位)。
BusyRetryDelay = 5000	元の値と同じ (ミリ秒単位)。
FailoverDelay = 30;	FailoverDelay = 60;
TimeoutResetEnable = 0	元の値と同じ
QfullRetryCount = 5	元の値と同じ
QfullRetryDelay = 5000	元の値と同じ (ミリ秒単位)。
IoRecoveryDelay = 50	元の値と同じ (ミリ秒単位)。
JniCreationDelay = 5;	JniCreationDelay = 10;
FlogiRetryCount = 3	元の値と同じ
PlogiRetryCount = 5	元の値と同じ
FcEmIdEndTcbTimeCount = 1533	元の値と同じ
target_throttle = 256	元の値と同じ (すべてのターゲットのデフォルト・スロットル)

表 47. FCE-1063/FCE2-1063/FCE-6410/FCE2-6410 の構成設定値 (続き)

元の値	新規の値
lun_throttle = 64	元の値と同じ (すべての LUN のデフォルト・スロットル)
automap = 0	automap = 0 (永続バインディング) automap = 1 (自動マッピング)
これらの設定値を追加します。	target0_hba = 『jnic146x0』 ;
	target0_wwpn = 『controller_wwpn』
	target1_hba = 『jnic146x1』 ;
	target1_wwpn = 『controller_wwpn』

- Solaris のシェルから /etc/raid/bin/genjnicconf 再構成スクリプトを実行する必要がある場合があります。

```
# /etc/raid/bin/genjnicconf
```

- JNI カードが /var/adm/messages ファイルで non-participating モードとなっている場合のみ、portEnabled = 1; を設定します。この状態では、以下の手順を実行します。

1. FcPortCfgEnabled = 1; を設定します。
2. ホストを再始動します。
3. FcPortCfgEnabled = 0; を設定します。
4. ホストを再び再始動します。

上記の作業を行った後で、/var/adm/messages を参照して、JNI カードがファブリックまたはループ・モードに設定されていることを確認します。

FCI-1063 の構成設定値

JNI ホスト・バス・アダプター・モデル FCI-1063 は、コントローラー・ファームウェアのバージョンが 05.4x.xx.xx 以前のストレージ・サブシステム構成でのみ サポートされます。

注: 表 48 にリストされているそれぞれの設定値で行のコメントを外す必要があります。これは、デフォルトの設定値および変更が必要な設定値の両方にあてはまります。

表 48. FCI-1063 の構成設定値

元の値	新規の値
scsi_initiator_id = 0x7d	元の値と同じ
fca_nport = 0;	fca_nport = 1 (ファブリックの場合) / fca_nport = 0 (ループの場合)
public_loop = 0	元の値と同じ
target_controllers = 126	元の値と同じ
ip_disable = 1;	元の値と同じ
ip_compliant = 0	元の値と同じ
qfull_retry_interval = 0	元の値と同じ
qfull_retry_interval = 1000	元の値と同じ (ミリ秒単位)。
failover = 30;	failover = 60 (秒単位)
failover_extension = 0	元の値と同じ
recovery_attempts - 5	元の値と同じ
class2_enable = 0	元の値と同じ

表 48. FCI-1063 の構成設定値 (続き)

元の値	新規の値
fca_heartbeat = 0	元の値と同じ
reset_glm = 0	元の値と同じ
timeout_reset_enable = 0	元の値と同じ
busy_retry_delay= 100;	元の値と同じ (ミリ秒単位)。
link_recovery_delay = 1000;	元の値と同じ。(ミリ秒単位)
scsi_probe_delay = 500;	scsi_probe_delay = 5000 (ミリ秒単位、10 ミリ秒の解決)
def_hba_binding = 『fca-pci*』 ;	def_hba_binding = "nonjni"; (バインディングの場合) def_hba_binding = 『fcaw』 ; (非バインディングの場合)
def_wwnn_binding = 『\$xxxxxx』	def_wwnn_binding = 『xxxxxx』
def_wwpn_binding = 『\$xxxxxx』	元の項目と同じ
fca_verbose = 1	元の項目と同じ
再構成スクリプトによって追加される	name= 『fca-pci』 parent= 『physical path』 unit-address= 『#』
再構成スクリプトによって追加される	target0_hba= 『fca-pci0』 target0_wwpn= 『controller wwpn』 ;
再構成スクリプトによって追加される	name= 『fca-pci』 parent= 『physical path』 unit-address= 『#』
再構成スクリプトによって追加される	target0_hba= 『fca-pci1』 target0_wwpn= 『controller wwpn』 ;

注: Solaris のシェルから /etc/raid/bin/genjnicnf 再構成スクリプトを実行する必要がある場合があります。

```
# /etc/raid/bin/genjnicnf
```

FC64-1063 の構成設定値

JNI ホスト・バス・アダプター・モデル FC64-1063 は、コントローラー・ファームウェアのバージョンが 05.4x.xx.xx 以前のストレージ・サブシステム構成でのみ サポートされます。

重要: 表 49 にリストされているそれぞれの設定値で行のコメントを外す必要があります。これは、デフォルトの設定値および変更が必要な設定値の両方にあてはまります。

表 49. FC64-1063 の構成設定値

元の値	新規の値
fca_nport = 0;	fca_nport =1;
ip_disable = 0;	ip_disable=1;
failover = 0;	failover =30;
busy_retry_delay = 5000;	busy_retry_delay = 5000;
link_recovery_delay = 1000;	link_recovery_delay = 1000;
scsi_probe_delay = 5000;	scsi_probe_delay = 5000;
def_hba_binding = 『fcaw*』 ;	直接接続構成: def_hba_binding = "fcaw*"; SAN 接続構成: def_hba_binding = 『nonJNI』 ;

表 49. FC64-1063 の構成設定値 (続き)

元の値	新規の値
def_wwnn_binding = 『\$xxxxxx』	def_wwnn_bindindef_hba_ binding = 『nonjni』 ; g = 『xxxxxx』
def_wwnn_binding = 『\$xxxxxx』	元の項目と同じ
再構成スクリプトによって追加される	name= 『fcaw』 parent= 『<physical path>』 unit-address= 『<#>』
再構成スクリプトによって追加される	target0_hba= 『fcaw0』 target0_wwpn= 『<controller wwpn>』 ;
再構成スクリプトによって追加される	name= 『fcaw』 parent= 『<physical path>』 unit-address= 『<#>』
再構成スクリプトによって追加される	target0_hba= 『fcaw0』 target0_wwpn= 『<controller wwpn>』 ;

注: シェル・プロンプトから /etc/raid/bin/genscsiconf 再構成スクリプトを実行する必要がある場合があります。

```
# /etc/raid/bin/genscsiconf
```

QLogic HBA 設定値

QLogic HBA は自動構成によるプラグ・アンド・プレイではありません。自動構成の代わりに、表 50 の説明のように、設定値またはバインディングの変更が必要です。

注: 表 50 では、HBA は hba0 として示されています。しかし、hba0 と hba1 の両方の QLogic HBA で設定値を変更する必要があります。

hba1 の設定値を変更する場合は、この表にリストされている値と同じ値を使用しますが、hba0 のすべてのインスタンスを次の例に示すように、hba1 に変更してください。

HBA	元の値	新規の値
hba0	hba0-execution-throttle=16;	hba0-execution-throttle=255;
hba1	hba1-execution-throttle=16;	hba1-execution-throttle=255;

vi エディターで各 QLogic HBA のループ属性のコメントを外し、表 50 で指定されている値を使用して変更します。

表 50. QL2342 の構成設定値

元の値	新規の値	コメント
max-frame-length=2048;	max-frame-length=2048	デフォルトを使用する
execution-throttle=16;	execution-throttle=255;	変更する
login-retry-count=8;	login-retry-count=30;	変更する
enable-adapter-hard-loop-ID=0;	enable-adapter-hard-loop-ID=1;	変更する
adapter-hard-loop-ID=0;	adapter-hard-loop-ID=0;	固有の数値でなければならない
enable-LIP-reset=0;	enable-LIP-reset=0;	デフォルトを使用する
hba0-enable-LIP-full-login=1;	hba0-enable-LIP-full-login=1;	デフォルトを使用する

表 50. QL2342 の構成設定値 (続き)

元の値	新規の値	コメント
enable-target-reset=0;	enable-target-reset=0;	デフォルトを使用する
reset-delay=5	reset-delay=8	変更する
port-down-retry-count=8;	port-down-retry-count=70;	変更する
maximum-luns-per-target=8;	maximum-luns-per-target=0;	変更する
connection-options=2;	connection-options=2;	デフォルトを使用する
fc-tape=1;	fc-tape=0;	変更する
loop-reset-delay = 5;	loop-reset-delay = 8;	変更する
> gbyte-addressing = disabled;	> gbyte-addressing = enabled;	変更する
link-down-timeout = 30;	link-down-timeout = 60;	変更する

付録 B. VMware ESX Server 構成でのストレージ・サブシステムの使用

ストレージ・マネージャー・ソフトウェアは現在、VMware ESX Server オペレーティング・システムでは使用できません。したがって、DS3000/DS4000/DS5000 ストレージ・サブシステムを VMware ESX Server ホストで管理するには、Windows または Linux 管理ステーションにストレージ・マネージャー・クライアント・ソフトウェア (SMclient) をインストールする必要があります。このワークステーションは、ブラウザー・ベースの VMware ESX Server 管理インターフェースに使用するものと同じです。また、Asymmetric Logical Unit Access (ALUA) を使用可能にするには、VMware ESX Server オペレーティング・システムバージョン 4.1 u2 以降および 5.0 u1 以降が必要です。

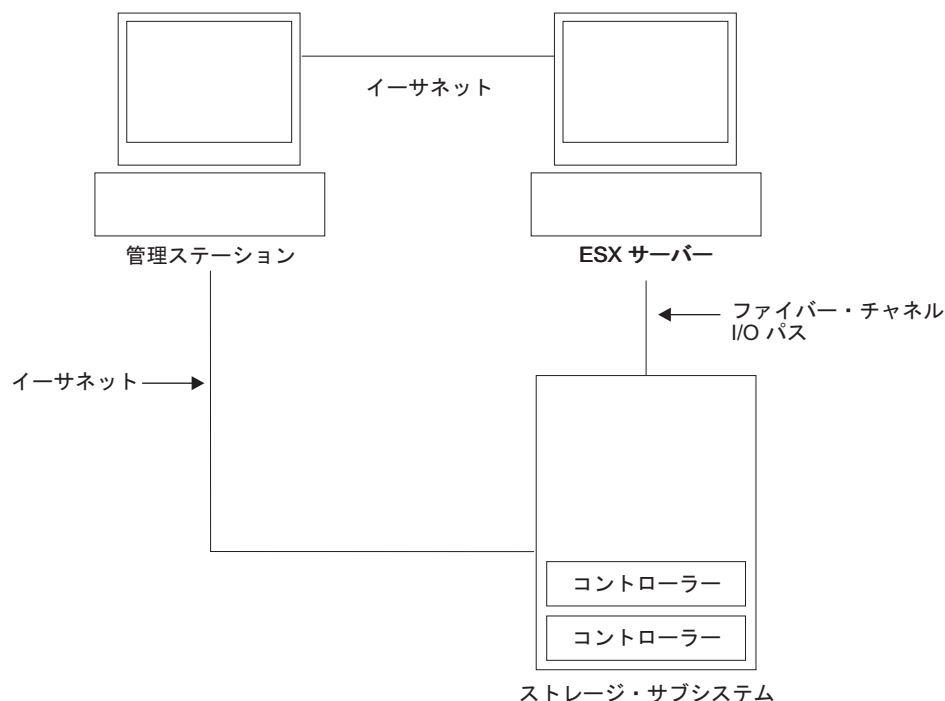
VMware ESX Server ホスト上で DS3000/DS4000/DS5000 ストレージ・サブシステムを使用する際の追加情報については、315 ページの『VMware ESX Server に関する制限』を参照してください。

また、次の Web サイトにある System Storage Interoperation Center も参照することができます。

www.ibm.com/systems/support/storage/config/ssic

構成の例

314 ページの図 34 は、VMware ESX Server の構成例を示しています。



SJ001150

ソフトウェア要件

このセクションでは、VMware ESX Server ホスト・オペレーティング・システムを DS3000/DS4000/DS5000 ストレージ・サブシステムで使用するために必要なソフトウェアを説明します。

管理ステーション

Windows または Linux の管理ステーションでは、次のソフトウェアが必要です。

1. SM Runtime (Linux のみ)
2. SMclient (Linux および Windows)

ホスト (VMware ESX Server)

VMware ESX Server では、次のソフトウェアが必要です。

- VMware ESX Server (DS3000/DS4000/DS5000 コントローラー・ファームウェアのバージョン 07.1x.xx.xx を使用する場合)
- VMware ESX Server が提供するファイバー・チャネル HBA 用のドライバー
- VMware ESX Server が提供する QLogic ドライバー・フェイルオーバー・セットアップ
- VMware ESX Server ツール (DS3000/DS4000/DS5000 論理ドライブを使用してすべての仮想マシンにインストールされたもの)

VMware ESX Server の以前のバージョン:

1. VMware ESX Server 2.1 は、DS4000/DS5000 コントローラー・ファームウェアのバージョン 06.12.xx.xx の場合のみサポートされます。
2. VMware ESX Server 2.0 は、DS4000/DS5000 コントローラー・ファームウェアのバージョン 05.xx.xx.xx の場合のみサポートされます。

ゲスト OS クラスターリング: ゲスト OS クラスター構成を作成する場合は、このセクションにリストされているホスト・ソフトウェア要件に加えて、Microsoft Cluster Services ソフトウェアを使用する必要があります。

VMware ホスト・クラスターリング: VMware ESX Server 2.5 以降は分散リソース・スケジューラーを備え、クラスターリング用に高可用性となっているので、複数のホストのリソースを 1 つのリソース・プールに集約することができます。(DRS クラスターは事実上リソース・プールを意味します。)

VMware ESX Server での Windows クラスター化に関する情報は、次の Web サイトで ESX Server 2.5 インストール・ガイドを参照してください。 <http://www.vmware.com/support/pubs/>.

ハードウェア要件

以下のタイプのストレージ・サブシステムおよびストレージ拡張エンクロージャーでは、VMware ESX Server ホスト・サーバーを使用することができます。追加情報については、以下の Web サイトにある System Storage Interoperation Center を参照してください。

<http://www.ibm.com/systems/support/storage/config/ssic>

注: 一般的なストレージ・サブシステムの要件については、1 ページの『第 1 章 インストールの準備』を参照してください。

DS5000 ストレージ・サブシステム

- DS5300
- DS5100

DS4000 ストレージ・サブシステム

- DS4100 (デュアル・コントローラー・ユニットのみ)
- DS4200
- DS4300 (デュアル・コントローラーおよびターボ・ユニットのみ)
- DS4400
- DS4500
- DS4700
- DS4800

DS5000 ストレージ拡張エンクロージャー

- EXP5000

DS4000 ストレージ拡張エンクロージャー

- EXP100
- EXP420 (DS4200 使用のみ)
- EXP500
- EXP700
- EXP710
- EXP810

VMware ESX Server に関する制限

SAN および接続の制限:

- VMware ESX Server ホストは、ホスト・エージェント (アウト・オブ・バンド) 管理のストレージ・サブシステム構成のみをサポートします。直接接続 (インバンド) 管理構成はサポートされません。
- VMware ESX Server ホストは、複数のホスト・バス・アダプター (HBA) および DS3000/DS4000/DS5000 デバイスをサポートします。ただし、単一のストレージ・サブシステムに接続できる HBA の数には制限があります。区画ごとに最大 2 つの HBA およびストレージ・サブシステムごとに最大 2 つの区画を構成できます。追加の HBA は、特定のストレージ・サブシステム・プラットフォームによって制限される数まで、追加のストレージ・サブシステムおよび他の SAN デバイスに追加できます。

- 1 台の VMware ESX Server で 2 つの HBA を使用している場合は、ストレージ・サブシステムに接続されている各 HBA について LUN の番号を同じにする必要があります。
- 単一 HBA 構成も可能ですが、各単一 HBA 構成では、ストレージ・サブシステムの両方のコントローラーをスイッチ経由で HBA に接続する必要があります。スイッチを使用して接続する場合は、両方のコントローラーは HBA と同じ SAN ゾーン内に存在する必要があります。

重要: 単一の HBA 構成では、パスに障害があるとデータ・アクセスの喪失につながる場合があります。

- 単一スイッチ構成は許可されていますが、HBA とストレージ・サブシステム・コントローラーの各組み合わせは個別の SAN ゾーンに存在する必要があります。
- 磁気テープ・デバイスまたはディスク・ストレージなどの他のストレージ・デバイスは、個別の HBA および SAN ゾーン経由で接続する必要があります。

区画の制限:

- 1 つの ストレージ・サブシステム上の VMware ESX Server ホストごとの区画の最大数は、2 です。
- VMware ESX Server に対して構成される論理ドライブはすべて、VMware ESX Server ホスト・グループにマップする必要があります。

注: コントローラー・ファームウェア・バージョンが 7.70.xx.xx より前の場合、VMware ESX サーバー固有のホスト・タイプは、DS3000、DS4000、または DS5000 ストレージ・サブシステムでは使用不可です。VMware ホストおよびホスト・グループには、LNXCLVMWARE ホスト・タイプを使用してください。デフォルトのホスト・グループを使用時は、このデフォルトのホスト・タイプを必ず LNXCLVMWARE にしてください。コントローラー・ファームウェア・バージョン 7.70.xx.xx 以降を搭載した DS ストレージ・サブシステムには、VMWARE という名前の VMware ESX サーバー固有のホスト・タイプが定義されています。VMware ホストおよびホスト・グループのホスト・タイプとして、VMWARE を使用する必要があります。

- DS4100 ストレージ・サブシステム構成では、最小番号の HBA 上でコントローラー A に LUN を最初に割り当てる必要があります。LUN の初期化後に、このパスをコントローラー B に変更可能です。(この制限は ESX Server の今後のリリースで修正されます。)
- LUN 番号 0 で始まるように、各 LUN を ESX Server に割り当てます。
- アクセス (UTM) LUN を ESX Server ホストあるいはホスト・グループのいずれにもマップしないでください。アクセス (UTM) LUN を使用するの、インバンド管理のストレージ・サブシステム構成の場合のみです。現時点では VMware ESX Server はこの構成をサポートしていません。

フェイルオーバーの制限:

- マルチパス構成に対しては、VMware ESX Server フェイルオーバー・ドライバーを使用する必要があります。他のフェイルオーバー・ドライバー (RDAC など) は VMware ESX Server 構成ではサポートされません。
- すべてのストレージ・サブシステムのデフォルトのフェイルオーバー・ポリシーは、現在は MRU (most recently used: 最後に使用されたもの) です。
- VMware ESX Server 構成 (2.0 以降) では、LNXCLVMWARE (コントローラー・ファームウェアが 7.70.xx.xx より前の場合) または VMWARE (コントローラー・ファームウェアが 7.70.xx.xx 以降の場合) ホスト・タイプを使用してください。LNXCLVMWARE または VMWARE ホスト・タイプは、自動的に自動ドライブ転送 (ADT) を使用不可にします。

相互運用性の制限:

- DS4100 および DS4300 の単一コントローラー・ストレージ・サブシステムは、VMware ESX Server ホストではサポートされません。(DS4100 および DS4300 のデュアル・コントローラー・ストレージ・サブシステムはサポートされています。)
- EXP700 ストレージ拡張エンクロージャーは、DS4800 ストレージ・サブシステムではサポートされません。EXP710 ストレージ拡張エンクロージャーにアップグレードする必要があります。

その他の制限:

- 2.5.x より前の VMware ESX Server オペレーティング・システム上の VMFS フォーマット LUN に対しては、動的論理ドライブ拡張 (DVE) はサポートされません。VMware ESX Server 2.5 サーバー以降の構成でサポートされている DS コピー・サービス機能の可用性については、IBM サポート担当員にお問い合わせください。
- SATA デバイスからは、システムをブートしないでください。

その他の VMware ESX Server ホストに関する情報

ご使用の VMware ESX Server ホストのセットアップに関する詳細は、次の Web サイトにある資料および README ファイルを参照してください。

www.vmware.com/support/pubs/

IBM サーバーへの VMware ESX Server オペレーティング・システムのインストールに関しては、次の IBM Support Web サイトを参照してください。

www-03.ibm.com/systems/i/advantages/integratedserver/vmware/

VMware ESX Server 用のストレージ・サブシステムの構成

ストレージ・サブシステムを構成する前に、ホスト・サーバー、SAN ファブリック、およびストレージ・サブシステム・コントローラーを物理的に構成する必要があります。つまり、初期 IP アドレスをコントローラーに割り当て、SMclient を Windows または Linux 管理ステーションにインストールする必要があります。ストレージ・サブシステムの構成手順については、61 ページの『第 4 章 ストレージの構成』を参照してください。

VMware 接続の相互接続構成

相互接続ストレージ・エリア・ネットワーク (SAN) 構成は、VMware ホストが DS3000/DS4000/DS5000 ストレージ・サブシステムに接続している場合に必要です。VMware ホストの各ホスト・バス・アダプター (HBA) には、ストレージ・サブシステムの各コントローラーへのバスが必要です。318 ページの図 35 は、VMware サーバー構成の相互接続を示しています。

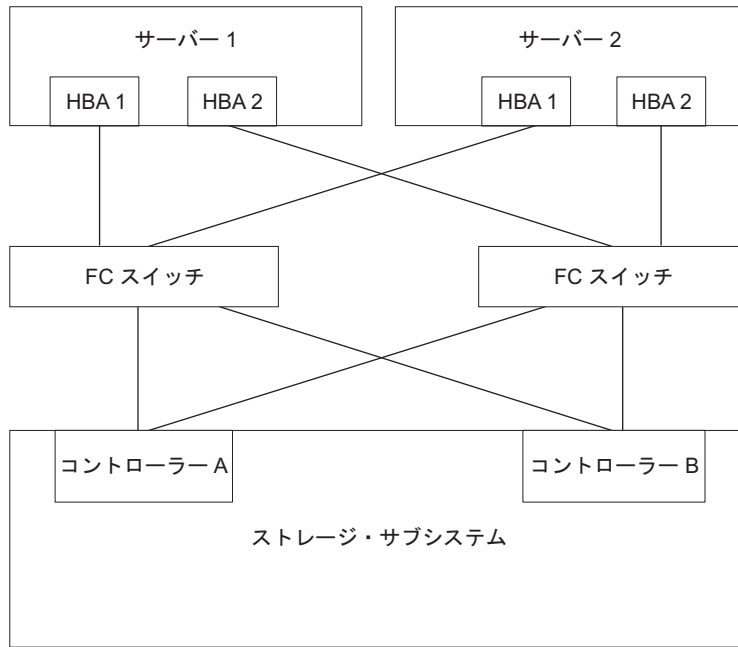


図 35. VMware 接続の相互接続構成

VMware ESX Server での LUN のストレージ区画へのマッピング

LUN を区画へマッピングする方法については、92 ページの『LUN のマッピング』に記載された手順を参照してください。このセクションには、VMware ESX Server 固有の LUN マッピングに関する注意が記載されています。

VMware ESX Server 上で各 LUN をマッピングする際には、以下の点に注意してください。

- LUN 0 で始まる連続番号を使用して LUN をマップします。例えば、LUN を 0、1、2、3、4、5 のように、番号をスキップせずにマップします。
- それぞれの区画ごとに LUN 0 をマップする必要があります。
- ご使用の構成で LUN 共有が不必要な場合 (単一または複数の独立 ESX Server、ローカル仮想クラスター)、各論理ドライブを直接ホストにマッピングするか、あるいは 1 メンバーとして単一ホストのホスト・グループにマッピングするか、どちらかにする必要があります。
- 複数の ESX サーバーにまたがった LUN 共有がサポートされるのは、VMotion 対応ホストあるいは Microsoft クラスター・ノードを構成しようとする場合に限定されます。複数の ESX サーバーにマッピングされた LUN では、アクセス・モードを「Shared (共有)」に変更する必要があります。

各 LUN を ESX Server 用のホスト・グループにマッピング可能なため、これらの LUN はホスト・グループのメンバーすべてに対して使用可能です。ESX Server での Windows クラスター化に関する追加情報は、次の Web サイトで ESX インストール・ガイド を参照してください。

www.vmware.com/support/pubs/

VMware のストレージ構成の検査

ストレージ・サブシステムが正しくセットアップされ、ストレージ・サブシステムを表示可能であることを確認するには、以下の手順を完了してください。

1. サーバーを開始します。
2. QLogic BIOS の初期化後に、Ctrl+Q を押して Fast!UTIL セットアップ・プログラムを開始する。
3. Fast!UTIL 画面に表示された最初のホスト・バス・アダプターを選択する。
4. 「**Host Adapter Settings (ホスト・アダプターの設定)**」を選択し、Enter キーを押す。
5. 「**Scan Fibre Devices (ファイバー・デバイスのスキャン)**」を選択し、Enter キーを押す。結果出力は次のようなものです。

ID	Vendor	Product	Rev	Port Name	Port ID
128	No device present		0520		
129	IBM	1742	0520	200400A0b00F0A16	610C00
130	No device present				
131	No device present				
132	No device present				
133	No device present				
134	No device present				
135	No device present				

注: 構成のケーブル接続方法によっては、複数インスタンスが表示される可能性があります。

ストレージ・サブシステム・コントローラーが見つからない場合は、ケーブル接続、スイッチのゾーニング、および LUN マッピングを検査してください。

付録 C. 高可用性クラスター・サービスを備えたストレージ・マネージャーの使用

ストレージ・マネージャーが提供するハイ・アベイラビリティ・クラスタリング・サービスを使用すれば、ハードウェアまたはソフトウェアに障害が発生した場合でも、アプリケーション・サービスの継続が可能になります。このシステムは、ソフトウェア障害だけでなく、CPU、ディスク、または LAN コンポーネントに障害がある場合にも、ユーザーを保護します。コンポーネントに障害がある場合、その冗長パートナー・コンポーネントがクラスター・サービスを引き継ぎ、コンポーネント間の転送を調整します。

一般情報

本書では、クラスター・サービスのインストール方法または構成方法については説明しません。その情報については、ご使用のクラスター・サービス製品に付属している資料を参照してください。

重要: 本書の情報には、最新のクラスター・ソフトウェア・バージョン・レベルが含まれていない可能性があります。

ストレージ・マネージャーをクラスター・サービスと一緒に使用するための最新の要件とユーザー情報については、ご使用のホスト・オペレーティング・システムのストレージ・マネージャー DVD にある README ファイルを参照するか、あるいは、オンラインで最新の README ファイルを確認してください。

オンラインで README ファイルを検索する手順については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

また、次の Web サイトにある System Storage Interoperation Center でも、詳細な情報を見つけることができます。

www.ibm.com/systems/support/storage/config/ssic

AIX システムにおけるクラスター・サービスの使用

以下のセクションには、クラスター・サービスに関する一般的なハードウェア要件、および追加情報が含まれています。

重要: 本書のこの情報は、最新のクラスター・ソフトウェア・バージョン・レベルを反映していない場合があります。AIX 用のストレージ・マネージャー README ファイルで、クラスタリング要件に関する最新情報の有無を確認してください。Web で README ファイルを検索する手順については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

AIX とクラスタリングに関する最新情報については、以下の Web サイトを参照することもできます。

www.ibm.com/systems/support/storage/config/ssic

High-Availability Cluster Multi-Processing

このセクションでは、ストレージ・マネージャーにおける High Availability Cluster Multi-Processing (HACMP™) サポートに関する一般的な要件および使用上の注意を示します。

ソフトウェア要件

サポートされる最新の HACMP バージョンについては、次の Web サイトにある System Storage Interoperation Center を参照してください。

www.ibm.com/systems/support/storage/config/ssic

構成の制限

以下の制限が、HACMP 構成に適用されます。

- 「Add a Disk to the Cluster (クラスターへのディスクの追加)」機能を使用して AIX に DS3000/DS4000/DS5000 ディスクを追加する場合、HACMP C-SPOC を使用することはできません。
- HACMP C-SPOC は、拡張並行モード・アレイをサポートしていません。
- 単一 HBA 構成も可能ですが、各単一 HBA 構成では、ストレージ・サブシステムの両方のコントローラーが、HBA と同じ SAN ゾーン内でスイッチに接続されている必要があります。

重要: 単一 HBA 構成はサポートされますが、ストレージ入出力パスに単一障害点を作ることになるので、HACMP 環境では使用しないでください。

- ホスト・ノードとストレージ・サブシステムの間ではスイッチ・ファブリック接続を使用してください。HACMP 環境でのホスト・ノードからストレージ・サブシステムへの直接接続は、次の制約事項と制限がすべて満たされた場合のみ サポートされます。
 - デュアル・コントローラー DS3000/DS4000/DS5000 ストレージ・サブシステム・バージョンのみが、ハイ・アベイラビリティ構成での直接接続でサポートされる。
 - AIX オペレーティング・システムは、バージョン 5.2 以降であることが必要。
 - HACMP クラスタリング・ソフトウェアは、バージョン 5.1 以降であることが必要。
 - ストレージ・サブシステムに直接接続されたすべてのホスト・ノードが、同じ HACMP クラスターの一部であることが必要。
 - ストレージ・サブシステムに表示されるすべての論理ドライブ (LUN) が、1 つ以上の拡張並行モード・アレイの一部である。
 - アレイ **varyon** は、HACMP 非並行リソース・グループ (1 つ以上の拡張並行モード・アレイを含む) を所有するホスト・ノード上でのみ アクティブ状態である。HACMP クラスタ内の他のすべてのホスト・ノードでは、拡張並行モード・アレイ **varyon** は、パッシブ状態にある。
 - 操作が AIX オペレーティング・システムの Logical VolumeManager (LVM) 層をバイパスする場合、拡張並行モード・アレイの論理ドライブ上の直接操作は、HACMP クラスタのどのホスト・ノードからも実行できない。例えば、root ユーザーとしてログインしている間は、DD コマンドは使用できない。
 - HACMP クラスタの各ホスト・ノードには、ストレージ・サブシステムへの 2 つのファイバー・チャネル接続がある。このうち 1 つの直接ファイバー・チャネル接続は、ストレージ・サブシステムのコントローラー A への接続とし、他方の直接ファイバー・チャネル接続は、ストレージ・サブシステムのコントローラー B への接続とする必要がある。

- HACMP クラスタ内の最大で 2 つのホスト・ノードを、DS4100 または DS4300 ストレージ・サブシステムのデュアル・コントローラー・バージョンに直接接続することができる。
- HACMP クラスタ内の最大で 2 つのホスト・ノードを、ストレージ・サブシステムに直接接続することができる。各ホスト・ノードは、ストレージ・サブシステムへの 2 つの直接ファイバー・チャンネル接続を持つ必要がある。

注: DS3000/DS4000/DS5000 ストレージ・サブシステムでは、各ホスト・ノードからの 2 つの直接ファイバー・チャンネル接続は、独立したミニハブへの接続でなければなりません。したがって、この構成では、DS3000/DS4000/DS5000 ストレージ・サブシステムに 4 つのホスト・ミニハブ (フィーチャー・コード 3507) が取り付けられていることが必要です (つまり、HACMP クラスタのホスト・ノードごとに 2 つのホスト・ミニハブが必要です)。

その他の HACMP の使用上の注

以下の表記は、HACMP 環境に固有のものです。

- HACMP クラスタは、DS3000/DS4000/DS5000 ストレージ・サブシステム区画ごとに 2 台から 32 台までのサーバーをサポートすることができます。この種類の環境を実行する場合は、176 ページの『hdisk デバイスのキュー項目数の設定』にある AIX デバイス・ドライバのキュー項目数の設定に関する説明を必ずよく読み、理解してください。
- ストレージ・マネージャーを実行しており、HACMP クラスタに接続されているストレージ・サブシステムに、クラスタ化されていない AIX ホストを接続することができます。ただし、クラスタ化されていない AIX ホストは、ストレージ・サブシステム上の別々のホスト区画で構成する必要があります。

Parallel System Support Programs および General Parallel File System

このセクションでは、DS ストレージ・マネージャーでの Parallel System Support Programs (PSSP) および General Parallel File System (GPFS™) サポートの一般的な要件および使用上の注意を示します。

ソフトウェア要件

サポートされる最新の PSSP および GPFS バージョンについては、次の Web サイトにある System Storage Interoperation Center を参照してください。

www.ibm.com/systems/support/storage/config/ssic

構成の制限

以下の制限が、PSSP と GPFS の構成に適用されます。

- ホスト・ノードと DS3000/DS4000/DS5000 ストレージ・サブシステム間の直接接続は許可されていません。スイッチ・ファブリック接続のみ、許可されています。
- RVSD クラスタは、ストレージ・サブシステム区画ごとに 2 つまで、IBM 仮想共有ディスクおよび RVSD サーバーをサポートすることができます。
- 構成で DS3000/DS4000/DS5000 ディスクを使用するデュアル・ノード GPFS クラスタでは、シングル・ノード・クォーラムはサポートされていません。
- 異機種混合の構成はサポートされていません。

その他の PSSP および GPFS の使用上の注

GPFS ファイル・システムでは、以下の DS3000/DS4000/DS5000 ストレージ・サブシステム・キャッシュ設定値がサポートされています。

- 読み取りキャッシュの使用可能化または使用不可化
- 書き込みキャッシュの使用可能化または使用不可化
- キャッシュのミラーリングの使用可能化または使用不可化（書き込みキャッシュのミラーリングの設定値によって異なる）

読み取りまたは書き込みキャッシングのパフォーマンス上の利点は、アプリケーションによって異なります。

GPFS、PSSP、および HACMP クラスタ構成図

このセクションにある図は、HBA ペアから特定の論理ドライブまたは論理ドライブ・セットへの、優先パスおよびフェイルオーバー・パスの両方を示しています。

論理ドライブへの最優先パスは、論理ドライブの作成時に決定され、ストレージ・サブシステム・コントローラー全体に分散されます。パスが割り当てられたコントローラーは、入出力転送についてどのパスが優先か、あるいはアクティブかを判別します。論理ドライブは、両方のコントローラーに割り当てることができ（またほとんどの場合は割り当てての必要があり）、そうすることで入出力の負荷を HBA とストレージ・サブシステム・コントローラー全体で平衡化することができます。

325 ページの図 36 は、1 つから 4 つの区画を持つ単一の DS ストレージ・サブシステムが含まれるクラスタ構成を示しています。

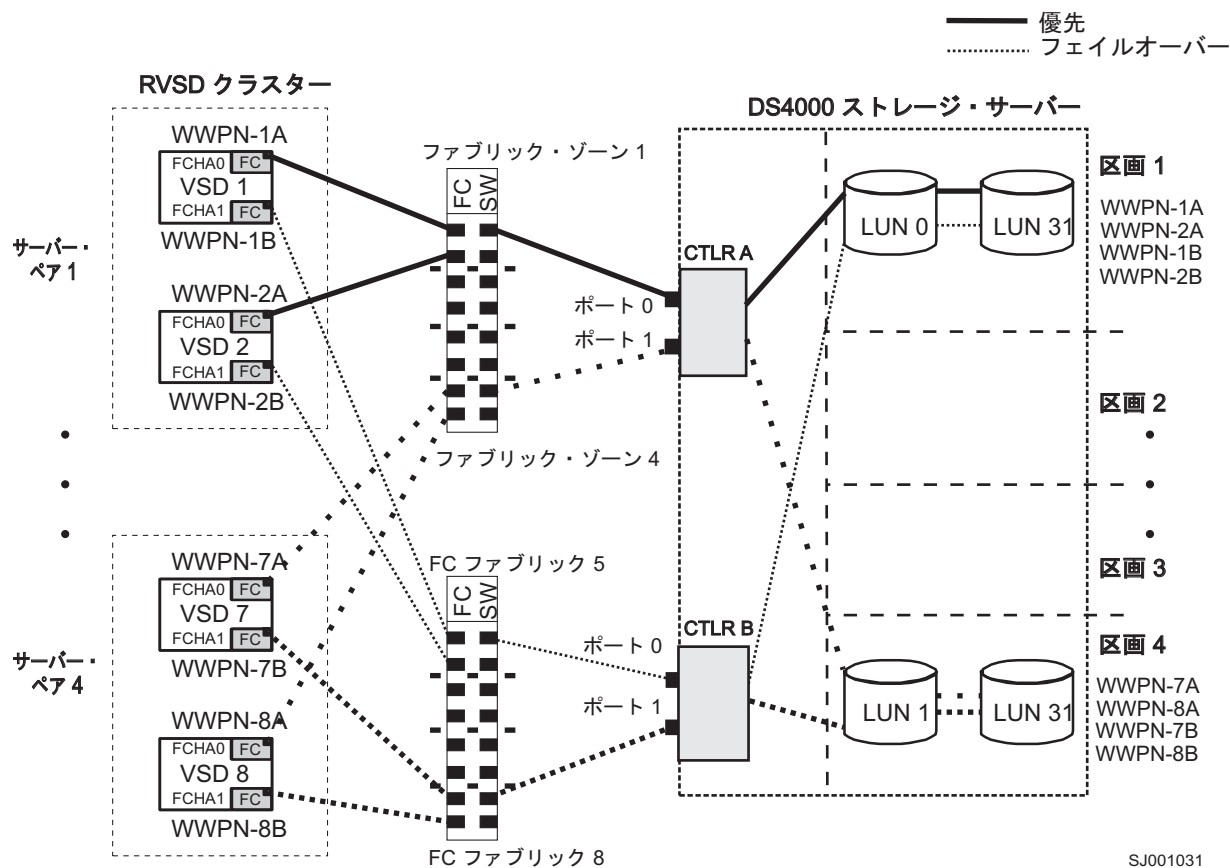


図 36. 単一のストレージ・サブシステム - 1 つから 4 つの区画が含まれるクラスター構成

326 ページの図 37 は、ストレージ・サブシステムごとに 1 つの区画を持つ、3 つの DS ストレージ・サブシステムが含まれるクラスター構成を示しています。

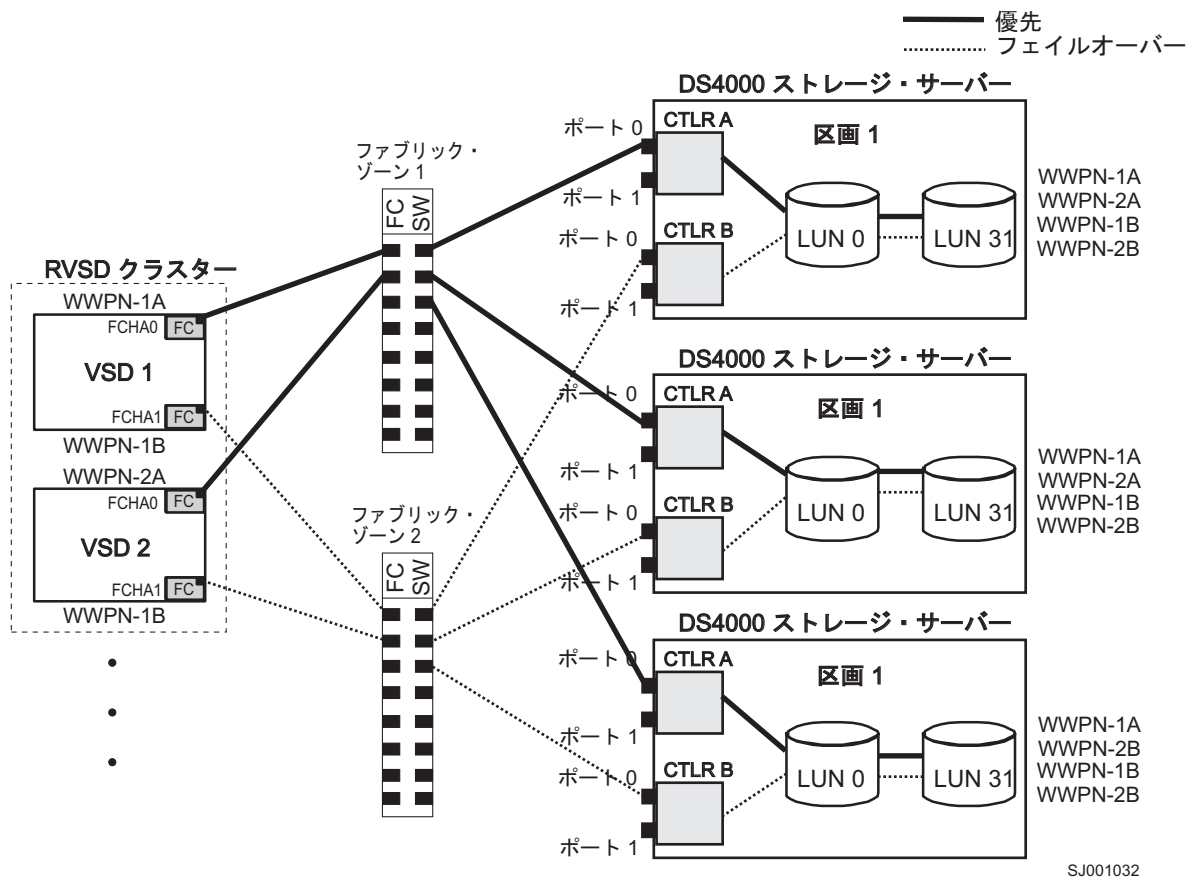
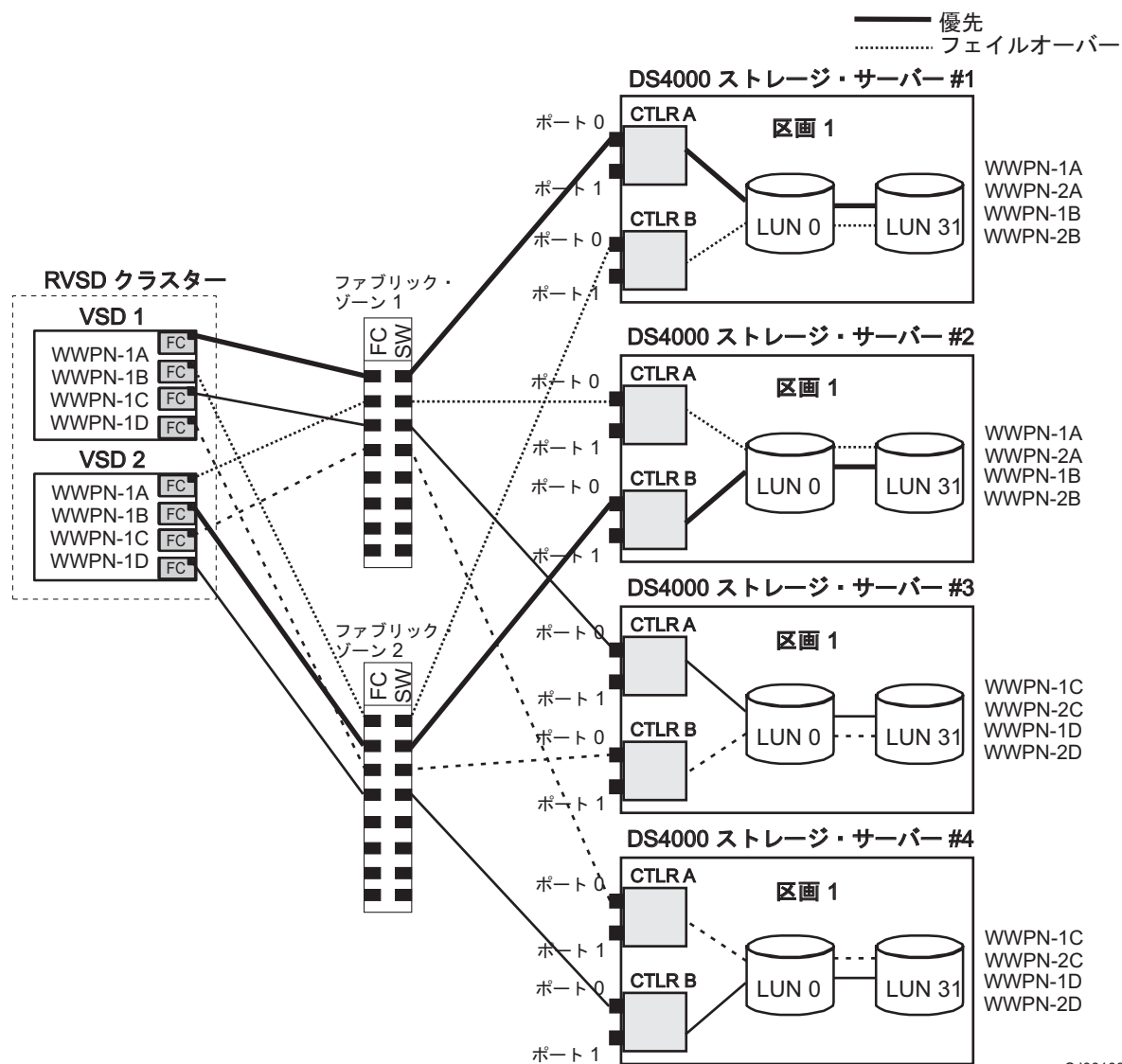


図 37. 3 つのストレージ・サブシステム (サブシステムごとに 1 つの区画) が含まれるクラスター構成

327 ページの図 38 は、ストレージ・サブシステムごとに 1 つの区画を持つ、4 つの DS ストレージ・サブシステムが含まれるクラスター構成を示しています。



SJ001033

図 38. 4 つのストレージ・サブシステム (サブシステムごとに 1 つの区画) が含まれるクラスター構成

328 ページの図 39 は、ストレージ・サブシステムごとに 2 つの区画を持つ、2 つの DS ストレージ・サブシステムが含まれるクラスター構成を示しています。

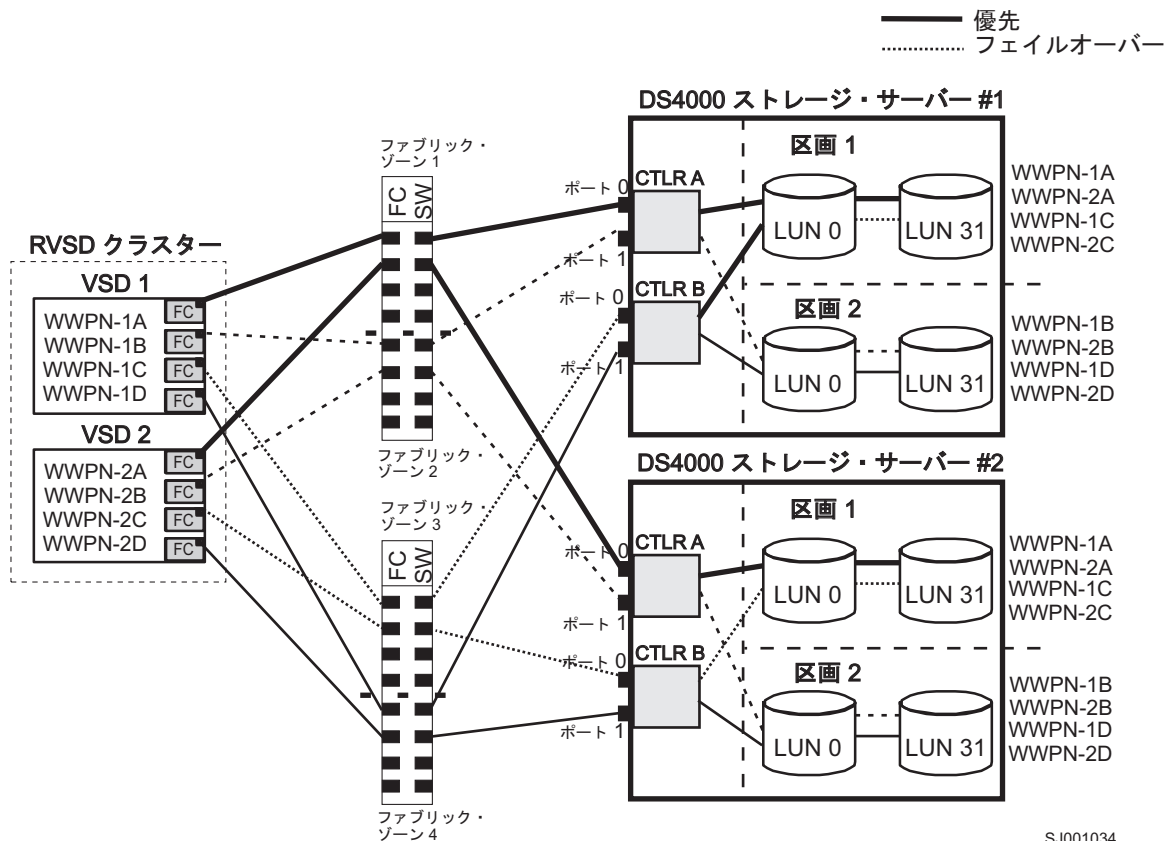


図 39. 2 つのストレージ・サブシステム (サブシステムごとに 2 つの区画) が含まれる RVSD クラスタ構成

329 ページの図 40 は、1 つの区画を持つ単一の DS ストレージ・サブシステムが含まれる HACMP/GPFS クラスタ構成を示しています。

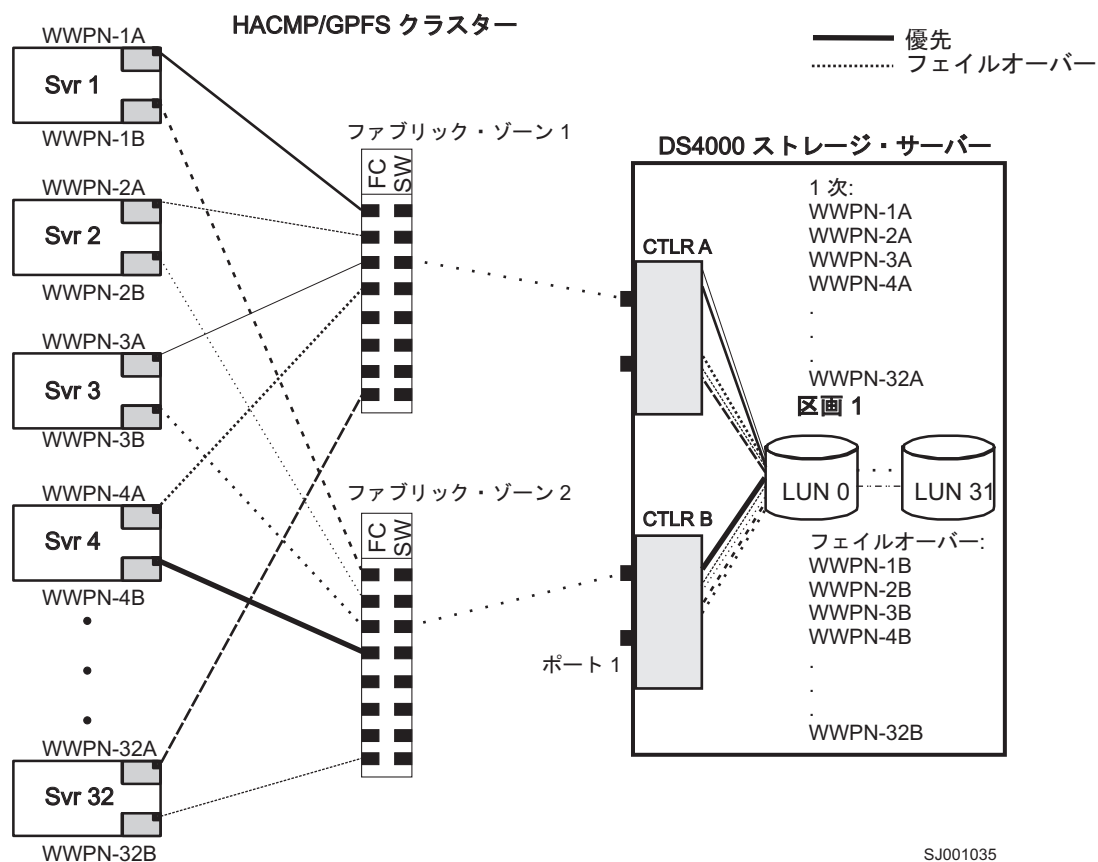


図 40. 1 つのストレージ・サブシステム - 1 つの区画を持つ HACMP/GPFS クラスタ構成

330 ページの図 41 は、ストレージ・サブシステムごとに 2 つの区画を持つ、2 つの DS ストレージ・サブシステムが含まれる HACMP/GPFS クラスタ構成を示しています。

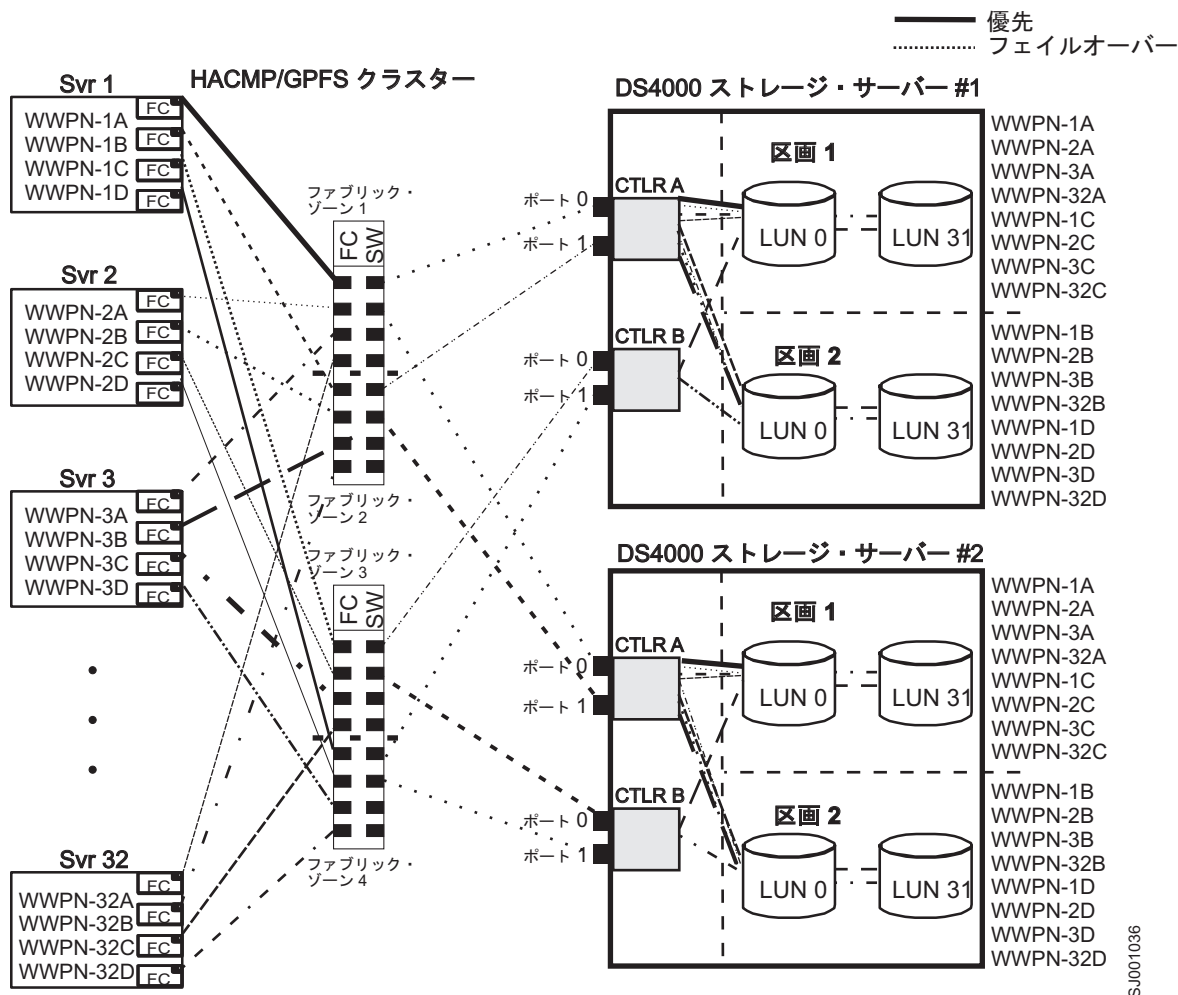


図 41. 2 つのストレージ・サブシステム (サブシステムごとに 2 つの区画) が含まれる HACMP/GPFS クラスタ構成

HP-UX システムにおけるクラスター・サービスの使用

本書のこの情報は、最新のクラスター・ソフトウェア・バージョン・レベルを反映していない場合があります。HP-UX 用のストレージ・マネージャー README ファイルで、クラスタリング要件に関する最新情報の有無を確認してください。オンラインで README ファイルを検索する手順については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

また、次の Web サイトにある System Storage Interoperation Center も参照することができます。

www.ibm.com/systems/support/storage/config/ssic

HP-UX システムでクラスタリングをセットアップする場合は、多くの構成の中から選択することができます。最小の構成は、ハートビート LAN を確立するために 1 次 LAN と 2 つのスタンバイ LAN の両方で構成された、2 つのサーバーから成り立ちます。

ホストに必要な冗長データ・バスを提供する 2 つのスイッチを通じて、ストレージ・サブシステムにファイバー・チャネル接続を提供してください。それぞれのサーバーに 2 つの HP Tachyon ホスト・バス・アダプターが存在することを確認してください。

Solaris システムでのクラスター・サービスの使用

以下のセクションには、クラスター・サービスに関する一般的なハードウェア要件、および追加情報が含まれています。

重要: 本書のこの情報は、最新のクラスター・ソフトウェア・バージョン・レベルを反映していない場合があります。Solaris 用のストレージ・マネージャー README ファイルで、サポートされる Veritas Cluster Server の最新バージョンなどの、クラスタリング要件に関する最新情報を確認してください。オンラインで README ファイルを検索する手順については、xix ページの『ストレージ・マネージャー・ソフトウェア、コントローラー・ファームウェア、および README ファイルの検出』を参照してください。

また、次の Web サイトにある System Storage Interoperation Center も参照することができます。

www.ibm.com/systems/support/storage/config/ssic

一般的な Solaris 要件

クラスター内の各 Solaris システムには、以下のハードウェアが必要です。

- 最低 3 つのイーサネット・ポート:
 - プライベート・ネットワーク接続用、2 つ
 - 公衆網接続用、最低 1 つ
- ストレージ・サブシステムへの接続用のファイバー・チャネル・ホスト・バス・アダプター 2 つ
- オペレーティング・システム・ディスク用の SCSI 接続
- 各 Veritas Cluster Server システム用に、最低 128 MB の RAM と 35 MB の空きディスク・スペース

システムの依存関係

このセクションでは、RDAC ID および Single Point of Failure に関する情報を提供します。

RDAC ID の追加

8 つまでの追加 ID を `/etc/symasm/rmparams` ファイルに追加できます。それらを追加するには、以下の手順を完了します。

1. 次のコマンドを入力して、Vi エディターで `/etc/symasm/rmparams` ファイルを開きます。

```
# vi /etc/symasm/rmparams
```

2. 以下のように `Rdac_HotAddIDs` 行を変更します。

```
Rdac_HotAddIDs:0:1:2:3:4:5:6:7:8
```

3. `/etc/symasm/rmparams` ファイルを保存してクローズします。

Single points of failure

Single Point of Failure はクラスターをその最も弱いコンポーネントと同じ強さにしてしまうため、クラスター・サービスをセットアップする場合には、Single Point of Failure を除去することが重要です。共有ス

トレイジ用にストレージ・サブシステムをセットアップします。例えば、クラスター内のすべてのノードが同じストレージを認識する必要があります。また、ホスト・タイプを正しく設定する必要があります。

付録 D. AIX オブジェクト・データ・マネージャー (ODM) 属性の表示および設定

一部の ODM 属性は、通知のみを目的としています。これらの通知のみに使用する属性は、ストレージ・サブシステムがどのように構成されているかについて、またはサーバーの現在の状態を表示します。他の属性は、SMIT または UNIX **chdev -p** コマンドを使用して変更できます。

属性定義

以下の表には、dar、dac、および hdisk の ODM 属性の定義と値がリストされています。

- 表 51: *dar* デバイス属性
- 335 ページの表 52: *dac* デバイス属性
- 335 ページの表 53: *hdisk* デバイス属性

注:

1. 変更可能列で True になっている属性は、デフォルト設定から変更できます。
2. 変更可能列で False になっている属性は、通知または状態を表す目的のためのみに使用されます。ただし、変更可能列で False になっている属性の中には、ストレージ・マネージャーを使用して変更できるものもあります。
3. **lsattr -El** (大文字の E、小文字の L) コマンドは、どの属性が変更できるかを判別する別の方法です。変更できる属性は、**lsattr -El** 出力の最後の列で True と表示されます。デフォルト値は、**lsattr -Dl** コマンドを使用することによっても表示できます。

表 51. *dar* デバイス属性

属性	定義	変更可能 (T/F)	可能な値
<i>act_controller</i>	構成時にアクティブ状態にあるコントローラーのリスト。	False	構成時に RDAC ソフトウェアによって設定されます。
<i>all_controller</i>	このアレイを構成するコントローラーのリスト。通常は 2 つの <i>dac</i> デバイスがあります。	False	構成時に RDAC ソフトウェアによって設定されます。
<i>held_in_reset</i>	構成時にリセット保留状態であったコントローラーの名前、またはその状態にあるコントローラーがなかった場合は、 none	True	構成時に RDAC ソフトウェアによって設定されます。変更しないでください。
<i>load_balancing</i>	ロード・バランシングが使用可能になっている (yes) か、または使用不可になっている (no) かを示すインディケーター。詳細については、 <i>balance_freq</i> 属性定義を参照してください。	True	Yes または No。 重要: 単一ホスト構成では、 <i>load_balancing</i> 属性は yes にのみ設定する必要があります。

表 51. dar デバイス属性 (続き)

属性	定義	変更可能 (T/F)	可能な値
<i>autorecovery</i>	デバイスがバスとコントローラーの両方が正しく作動していることを検出した場合に、アレイをデュアル・アクティブ・モードに戻す (yes) か、または戻さない (no) かを示すインディケーター。	True	Yes または No。使用についての制限を参照してください。
<i>hlthchk_freq</i>	正常性の検査を実行する頻度を指定する数 (秒単位)。	True	1 から 9999。変更しないでください。
<i>aen_freq</i>	ポーリング AEN 検査を実行する頻度を指定する数 (秒単位)。	True	1 から 9999。変更しないでください。
<i>balance_freq</i>	<i>load_balancing</i> が使用可能になっている場合、システムがアレイに対してロード・バランシングを実行する頻度を指定する数 (秒単位)。	True	1 から 9999。変更しないでください。
<i>fast_write_ok</i>	このシステムについて、高速書き込み、書き込みキャッシングが使用可能 (yes) か、または使用可能でないか (no) を示すインディケーター。	False	Yes または No。ストレージ・サブシステムの構成状態です。
<i>cache_size</i>	両方のコントローラーのキャッシュ・サイズ (MB 単位)。サイズが一致しない場合は、 0 です。	False	512 または 1024。ストレージ・サブシステムにより設定されます。
<i>switch_retries</i>	障害の発生したスイッチを再試行する回数を指定する数 (整数)。	True	0 から 255。 デフォルト: 5。 大部分の構成では、デフォルトが最良の設定です。 HACMP を使用している場合は、この値を 0 に設定すると役に立つ場合があります。 重要: デフォルト設定を変更した場合は、並行ファームウェア・ダウンロードを使用することはできません。

表 52. dac デバイス属性

属性	定義	変更可能 (T/F)	可能な値
<i>passive_control</i>	このコントローラーが構成時にパッシブ状態であった (yes) か、またはそうではなかった (no) かを示すインディケーター。	False	Yes または No。ストレージ・サブシステムの構成状態です。
<i>alt_held_reset</i>	代替コントローラーが構成時にリセット保留状態であった (yes) か、または、そうではなかった (no) かを示すインディケーター。	False	Yes または No。ストレージ・サブシステムの構成状態です。
<i>controller_SN</i>	このコントローラーのシリアル番号。	False	ストレージ・サブシステムにより設定されます。
<i>ctrl_type</i>	このコントローラーが属するアレイ・タイプ。	False	1742、 1722、 1742-900。ストレージ・サブシステムにより設定されます。
<i>cache_size</i>	このコントローラーのキャッシュ・サイズ (MB 単位)。	False	512、 1024。ストレージ・サブシステムにより設定されます。
<i>scsi_id</i>	このコントローラーの SCSI ID。	False	SAN によって設定され、AIX によって報告されます。
<i>lun_id</i>	このコントローラーの論理装置番号。	False	ストレージ・サブシステムにより設定されます。
<i>utm_lun_id</i>	このコントローラーの論理装置番号。 UTM (アクセス論理ドライブ) が使用可能になっていない場合は none 。	False	0 から 31。ストレージ・マネージャーにより設定されます。
<i>node_name</i>	ファイバー・チャネル・ノード名。	False	ストレージ・サブシステムにより設定されます。
<i>location</i>	このコントローラーのユーザー定義の場所ラベル。システムはこの値を使用しません。	True	ストレージ・マネージャーにより設定されます。
<i>ww_name</i>	このコントローラーのファイバー・チャネルの worldwide name。	False	ストレージ・サブシステムにより設定されます。
<i>GLM_type</i>	このコントローラーに使用される GLM タイプ。	False	High または Low。ストレージ・サブシステムにより設定されます。

表 53. hdisk デバイス属性

属性	定義	変更可能 (T/F)	可能な値
<i>pvid</i>	AIX 物理ボリューム ID、または設定されていない場合は、 none 。	False	AIX によって設定されます。

表 53. *hdisk* デバイス属性 (続き)

属性	定義	変更可能 (T/F)	可能な値
<i>q_type</i>	このデバイスのキューイング・タイプ。 simple に設定する必要があります。	False	AIX によって設定されます。『simple』にする必要があります。
<i>queue_depth</i>	システム構成に基づいてキュー項目数を指定する数。アレイが BUSY 状況を常に戻す場合は、この数を減らしてください。	True	1 から 64 注: この属性の設定に関する重要な情報については、176 ページの『 <i>hdisk</i> デバイスのキュー項目数の設定』を参照してください。
<i>PR_key_value</i>	デバイスが、いずれかの永続予約ポリシーをサポートする場合にのみ必要。この属性は、さまざまなホストを区別するために使用されます。	True	1 から 64、または、なし。 注: <i>reserve_policy</i> 属性を設定する前に、この属性をゼロ以外の値に設定する必要があります。
<i>reserve_policy</i>	永続予約ポリシー。これは、デバイスが開かれるときに予約の方法を採用するかどうかを定義するものです。	True	<i>no_reserve</i> <i>PR_shared</i> 、 <i>PR_exclusive</i> 、または <i>single_path</i>
<i>max_transfer</i>	最大転送サイズ。これは、入出力の送信で使用する最大転送サイズです。	True	数値。 デフォルト = 1 MB 注: 通常、非常に大きな I/O で値を大きくする必要がある場合を除いて、デフォルトを変更する必要はありません。
<i>write_cache</i>	このデバイスで、書き込みキャッシングが使用可能になっている (yes) か、または、そうっていない (no) かを示すインディケータ。詳細については、 <i>cache_method</i> 属性定義を参照してください。	False	Yes または No。
サイズ	この論理ドライブのサイズ。	False	ストレージ・サブシステムにより設定されます。
<i>raid_level</i>	このデバイスの RAID レベルを指定する数。	False	0、1、3、5。DS ストレージ・マネージャーにより設定されます。
<i>rw_timeout</i>	このアレイに対する各 read/write コマンドの読み取り/書き込みタイムアウト値を指定する数 (秒単位)。通常は、30 に設定されます。	True	30 から 180。デフォルト値を変更しないでください。

表 53. *hdisk* デバイス属性 (続き)

属性	定義	変更可能 (T/F)	可能な値
<i>reassign_to</i>	FC 再割り当て操作のタイムアウト値を指定する数 (秒単位)。通常は、120 に設定されます。	True	0 から 1000。デフォルト値を変更しないでください。
<i>scsi_id</i>	構成時の SCSI ID。	False	SAN によって設定され、AIX によって報告されます。
<i>lun_id</i>	このデバイスの論理装置番号。	False	0 から 255。ストレージ・マネージャーにより設定されます。
<i>cache_method</i>	<i>write_cache</i> が使用可能になっている場合、このアレイの書き込みキャッシング方法。以下のいずれかに設定されます。 • default。デフォルト・モード。<i>write_cache</i> が yes に設定されている場合は、ワード「default」は表示されません。 • fast_write。高速書き込み (バッテリー・バックアップされ、ミラーリングされた書き込みキャッシュ) モード。 • fw_unavail。高速書き込みモードが指定されたが、使用可能にできませんでした。書き込みキャッシングは使用されません。 • fast_load。高速ロード (バッテリー・バックアップなし、ミラーリングなしの書き込みキャッシュ) モード。 • fl_unavail。高速ロード・モードが指定されたが、使用可能にできませんでした。	False	default、fast_write、fast_load、fw_unavail、fl_unavail。
<i>prefetch_mult</i>	各ブロック読み取りで、プリフェッチされて読み取りキャッシュに入れられるブロック数。	False	0 から 100。
<i>ieee_volname</i>	この論理ドライブの IEEE 固有論理ドライブ名 ID。	False	ストレージ・サブシステムにより設定されます。

ODM 属性を表示する lsattr コマンドの使用

dar、dac、および hdisk のオブジェクト・データ・マネージャー (ODM) 属性設定値を表示するには、以下のように **lsattr** コマンドを使用します。

- デフォルト設定値を表示するには、**lsattr -DI** と入力します。
- 現在システムに設定されている属性を表示するには、**lsattr -El** と入力します。

表 54、表 55、および 339 ページの表 56 に示される **lsattr -El** 出力例は、dar、dac および hdisk の ODM 属性設定値を示しています。

表 54. 例 1: dar の属性設定値の表示

```
# lsattr -El dar0
act_controller dac0,dac1 Active Controllers          False
aen_freq      600      Polled AEN frequency in seconds      True
all_controller dac0,dac1 Available Controllers          False
autorecovery   no      Autorecover after failure is corrected  True
balance_freq   600      Dynamic Load Balancing frequency in seconds      True
cache_size    128      Cache size for both controllers          False
fast_write_ok  yes      Fast Write available          False
held_in_reset  none     Held-in-reset controller          True
hlthchk_freq   600      Health check frequency in seconds      True
load_balancing no      Dynamic Load Balancing          True
switch_retries 5        Number of times to retry failed switches      True
```

表 55. 例 2: dac の属性設定値の表示

```
# lsattr -El dac0
GLM_type      low      GLM type          False
alt_held_reset no      Alternate held in reset  False
cache_size    128      Cache Size in MBytes    False
controller_SN 1T24594458 Controller serial number False
ctrl_type     1722-600 Controller Type        False
location      Location Label          True
lun_id        0x0      Logical Unit Number     False
node_name     0x200200a0b80f14af FC Node Name          False
passive_control no      Passive controller      False
scsi_id       0x11000   SCSI ID               False
utm_lun_id    0x001f000000000000 Logical Unit Number     False
ww_name       0x200200a0b80f14b0 World Wide Name        False
```

注: # **lsattr -Rl <device> -a <attribute>** コマンドを実行すると、指定した属性について使用できる値が表示されます。MPIO を使用している場合は、hdisk 属性リストが表示されます。

注: 339 ページの表 56 では、**ieee_volname** および **lun_id** 属性値は、省略して表示されています。実際の出力では、完全な値が表示されます。

表 56. 例 3: *hdisk* の属性設定値の表示

lsattr -El hdisk174			
cache_method	fast_write	Write Caching method	False
ieee_volname	600A0B8...1063F7076A7	IEEE Unique volume name	False
lun_id	0x0069...000000	Logical Unit Number	False
prefetch_mult	12	Multiple of blocks to prefetch on read	False
pvid	none	Physical volume identifier	False
q_type	simple	Queuing Type	False
queue_depth	2	Queue Depth	True
raid_level	5	RAID Level	False
reassign_to	120	Reassign Timeout value	True
reserve_lock	yes	RESERVE device on open	True
rw_timeout	30	Read/Write Timeout value	True
scsi_id	0x11f00	SCSI ID	False
size	2048	Size in Mbytes	False
write_cache	yes	Write Caching enabled	False

付録 E. VDS/VSS プロバイダーについて

Microsoft Virtual Disk Service (VDS) および Microsoft Volume Shadow-copy Service (VSS) は、Microsoft Windows Server 2003 および Microsoft Windows Server 2008 向けの IBM DS ストレージ・マネージャー・インターフェースです。VDS および VSS により、ストレージ・サブシステムは VDS または VSS アプリケーション・プログラミング・インターフェース (API) を使用するサード・パーティー・アプリケーションと対話できます。Microsoft VDS/VSS は、Windows Server 2003 および Windows Server 2008 のインストールに含まれています。Microsoft VSS は Windows Server 2012 に含まれてサポートされますが、Windows Server 2012 では Microsoft VDS の使用は推奨されません。

注: IBM VDS/VSS ハードウェア・プロバイダーでは、Windows Server 2012 のクライアント・バージョンはサポートされません。

IBM VDS/VSS ハードウェア・プロバイダーでは、Windows Server 2012 のクライアント・バージョンはサポートされません。IBM DS ストレージ・マネージャー VDS ハードウェア・プロバイダーは、VDS がロードする Windows Dynamic Link Library (DLL) であり、ストレージ・サブシステムへの通信チャンネルとして使用されます。インストールされた IBM DS ストレージ・マネージャー VDS ハードウェア・プロバイダーを使用すると、サード・パーティー・アプリケーションによりストレージ・サブシステムに管理コマンドを送信できます。これは、論理ドライブの作成、論理ドライブの削除および論理ドライブのアンマスクなどのコマンドをサポートします。サード・パーティー・アプリケーションを使用すると、ストレージ・サブシステムの状況および構成情報が得られます。IBM DS ストレージ・マネージャー VSS ハードウェア・プロバイダーは、Windows サービス (.exe) です。Microsoft の VSS はサービスに接続され、サービスを使用してストレージ・サブシステム上の FlashCopy 論理ドライブの作成を調整します。VSS が起動した論理ドライブ FlashCopy は、「リクエスター」と呼ばれるサード・パーティーのバックアップ・ツールを介して起動できます。

以下の Web サイト から、VDS/VSS プロバイダーおよびインストール説明をダウンロードします。最初にフリー・アカウントを登録し、ログイン資格情報を入手して、インストーラーをダウンロードします。

<http://support.netapp.com/NOW/apbu/oemcp/protcd/>.

付録 F. SMI-S プロバイダーのインストール

SMIS-S (Storage Management Initiative Specification) では、異機種混合 SAN (Storage Area Network) で相互運用可能な管理のための方法を定義し、SMI-S に準拠した CIM サーバーから WBEM Client への使用可能な情報、およびオブジェクト指向の XML ベースおよびメッセージング・ベースのインターフェースについて説明します。このインターフェースは、SAN、IBM SAN ポリューム・コントローラー、Tivoli Storage Productivity Center、および Director がサポートする DS3000、DS4000 および DS5000 ストレージ・サブシステム内で、およびそれらを介して装置を管理するための特定の要件をサポートするように設計されています。詳しくは、IBM Software 相互運用性マトリックスを参照してください。

以下の Web サイト から、SMI-S プロバイダーおよびインストール説明をダウンロードします。最初にフリー・アカウントを登録し、ログイン資格情報を入手して、インストーラーをダウンロードします。

<http://support.netapp.com/NOW/apbu/oemcp/protcd/>.

付録 G. アクセシビリティ

この付録の情報では、資料のアクセシビリティおよびストレージ・マネージャーのアクセシビリティ・フィーチャーについて説明します。

文書フォーマット

本製品の資料は Adobe PDF 形式になっており、アクセシビリティ標準に準拠しています。PDF ファイルのご使用時に障害が発生したため、Web ベース形式あるいは表示可能な PDF 文書の資料をご希望される場合は、以下の住所宛に郵送でお申し込みください。

*Information Development
IBM Corporation
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
U.S.A.*

ご要望の書簡には、必ず資料のタイトルと部品番号を明記してください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

ストレージ・マネージャーのアクセシビリティ機能

このセクションには、ストレージ・マネージャーのアクセシビリティ機能の 1 つである代替キーボード・ナビゲーションについて説明します。アクセシビリティ機能は、運動障害または視覚障害など身体に障害を持つユーザーがソフトウェア・プロダクトを快適に使用できるようにサポートします。

このセクションで説明する代替キーボード操作を使用することにより、さまざまなキーまたはキーの組み合わせを使用して、ストレージ・マネージャーのタスクを実行したり、マウスを使用しても行える多数のメニュー・アクションを開始したりできます。

注: Windows 版のストレージ・マネージャー バージョン 9.14 - 10.10 (およびそれ以降) のソフトウェア・インストール・パッケージには、このセクションに示すキーボード操作に加えて、スクリーン・リーダー (読み上げ機能) ソフトウェア・インターフェースが組み込まれています。

スクリーン・リーダー (読み上げ機能) を使用可能にするには、インストール・ウィザードの使用時に、「**Custom Installation (カスタム・インストール)**」を選択して、ストレージ・マネージャー 9.14 - 10.10 以降を Windows ホスト/管理ステーションにインストールします。次に、「**Select Product Features (製品機能の選択)**」ウィンドウで、その他の必要なホスト・ソフトウェア・コンポーネントに加えて「**Java Access Bridge**」を選択します。

346 ページの表 57 は、ユーザー・インターフェース・コンポーネントのナビゲート、選択、または活動化を行うことができるようにするキーボード操作を定義しています。この表では、以下の用語を使用しています。

- ナビゲート とは、ユーザー・インターフェース・コンポーネント間で入力フォーカスを移動することです。

- **選択** とは、通常は、後続のアクションのために、1 つ以上のコンポーネントを選択することを意味します。
- **活動化** とは、特定のコンポーネントのアクションを実行することを意味します。

注: 一般に、コンポーネント間のナビゲーションには以下のキーが必要です。

- **Tab** - キーボード・フォーカスを次のコンポーネントへ移動するか、次のコンポーネント・グループの最初のメンバーへ移動します。
- **Shift+Tab** - キーボード・フォーカスを前のコンポーネントへ移動するか、前のコンポーネント・グループの最初のコンポーネントへ移動します。
- **矢印キー** - コンポーネント・グループの個々のコンポーネント内で、キーボード・フォーカスを移動します。

表 57. ストレージ・マネージャーの代替キーボード操作

ショートカット	アクション
F1	ヘルプを開きます。
F10	キーボード・フォーカスをメインメニュー・バーへ移動し、最初のメニューを表示します。矢印キーを使用して、選択可能なオプションの間をナビゲートします。
Alt+F4	管理ウィンドウを閉じます。
Alt+F6	ダイアログ (モーダル以外の) 間および管理ウィンドウ間でキーボード・フォーカスを移動します。
Alt+ 下線付きの英字	下線付きの英字へ関連付けられたキーを使用して、メニュー項目、ボタン、およびその他のインターフェース・コンポーネントにアクセスします。 メニュー・オプションの場合は、「Alt+ 下線付きの英字」の組み合わせを選択してメインメニューにアクセスした後、下線付きの英字を選択して個々のメニュー項目にアクセスします。 それ以外のインターフェース・コンポーネントでは、「Alt+ 下線付きの英字」の組み合わせを使用します。
Ctrl+F1	キーボード・フォーカスがツールバー上にあるときに、ツールチップを表示または非表示にします。
スペース・バー	項目を選択するか、ハイパーリンクを活動化します。
Ctrl+ スペース・バー (連続/不連続) AMW 論理/物理ビュー	「Physical View (物理ビュー)」内で複数のドライブを選択します。 複数のドライブを選択するには、スペース・バーを押して 1 つのドライブを選択した後、Tab を押して、次に選択したいドライブへフォーカスを移動し、Ctrl+ スペース・バーを押してドライブを選択します。 複数のドライブを選択しているときにスペース・バーを単独で押すと、すべての選択が解除されます。 複数のドライブを選択しているときに、1 つのドライブの選択を解除するには、「Ctrl+ スペース・バー」の組み合わせを使用します。 この動作は、ドライブの連続選択と不連続選択のどちらの場合も共通です。
End、Page Down	キーボード・フォーカスをリスト内の最後の項目へ移動します。
Esc	現在のダイアログを閉じます (キーボード・フォーカスは不要です)。

表 57. ストレージ・マネージャーの代替キーボード操作 (続き)

ショートカット	アクション
Home、Page Up	キーボード・フォーカスをリスト内の最初の項目へ移動します。
Shift+Tab	コンポーネント間でキーボード・フォーカスを逆方向に移動します。
Ctrl+Tab	キーボード・フォーカスをテーブルから次のユーザー・インターフェース・コンポーネントへ移動します。
Tab	コンポーネント間でキーボード・フォーカスをナビゲートするか、ハイパーリンクを選択します。
下矢印	キーボード・フォーカスをリスト内で 1 項目下へ移動します。
左矢印	キーボード・フォーカスを左へ移動します。
右矢印	キーボード・フォーカスを右へ移動します。
上矢印	キーボード・フォーカスをリスト内で 1 項目上へ移動します。

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510

東京都中央区日本橋箱崎町19番21号

日本アイ・ビー・エム株式会社

法務・知的財産

知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Corporation

Almaden Research

650 Harry Road

Bldg 80, D3-304, Department 277

San Jose, CA 95120-6099

U.S.A.

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

この文書に含まれるいかなるパフォーマンス・データも、管理環境下で決定されたものです。そのため、他の操作環境で得られた結果は、異なる可能性があります。一部の測定が、開発レベルのシステムで行われた可能性があります。その測定値が、一般に利用可能なシステムのものと同じである保証はありません。さらに、一部の測定値が、推定値である可能性があります。実際の結果は、異なる可能性があります。お客様は、お客様の特定の環境に適したデータを確かめる必要があります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。これらのサンプル・プログラムは特定物として現存するままの状態を提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年).このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。

© Copyright IBM Corp. _年を入れる_.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

商標

IBM、IBM ロゴおよび ibm.com は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。

現時点での IBM の商標リストについては、<http://www.ibm.com/legal/copytrade.shtml> をご覧ください。

以下は、International Business Machines Corporation の米国およびその他の国における商標です。

IBM
AIX
eServer
FlashCopy
Netfinity
POWER
Series p
RS/6000
TotalStorage

Adobe および PostScript は、Adobe Systems Incorporated の米国およびその他の国における登録商標または商標です。

Intel、Intel Xeon、Itanium、および Pentium は、Intel Corporation またはその関連企業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。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標です。

Linux は、Linus Torvalds の米国およびその他の国における商標です。

Microsoft、Windows、および Windows NT は、Microsoft Corporation の米国およびその他の国における商標です。

UNIX は The Open Group の米国およびその他の国における登録商標です。

他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

重要事項

プロセッサの速度とは、マイクロプロセッサの内蔵クロックの速度を意味しますが、他の要因もアプリケーション・パフォーマンスに影響します。

本製品は、いかなる方法でも直接的または間接的に公共通信ネットワークのインターフェースに接続されることを意図していません。

CD または DVD のドライブ速度は、可変読み取り速度です。実際の速度は記載された速度と異なる場合があります。最大可能な速度よりも遅いことがあります。

プロセッサ・ストレージ、実記憶域と仮想記憶域、またはチャネル転送量を表す場合、KB は 1024 バイト、MB は 1,048,576 バイト、GB は 1,073,741,824 バイトを意味します。

ハード・ディスクの容量または通信ボリュームを表す場合、MB は 1,000,000 バイト、GB は 1,000,000,000 バイトを意味します。ユーザーが利用できる容量の合計は、稼働環境によって異なります。

内蔵ハード・ディスクの最大容量は、IBM から入手可能な現在サポートされている最大のドライブを標準ハード・ディスクの代わりに使用し、すべてのハード・ディスク・ドライブ・ベイに取り付けることを想定しています。

最大メモリーは標準メモリーをオプション・メモリー・モジュールと取り替える必要があります。

IBM は、ServerProven[®] に登録されている他社製品およびサービスに関して、商品性、および特定目的適合性に関する黙示的な保証も含め、一切の保証責任を負いません。これらの製品は、第三者によってのみ提供および保証されます。

IBM は、他社製品に関して一切の保証責任を負いません。他社製品のサポートがある場合は、IBM ではなく第三者によって提供されます。

いくつかのソフトウェアは、その小売り版 (利用可能である場合) とは異なる場合があります。ユーザー・マニュアルまたはすべてのプログラム機能が含まれていない場合があります。

用語集

この用語集では、IBM System Storage の資料で使用されている用語および省略語の定義を記載しています。

お探しの用語が見つからない場合は、次の Web サイトにある「*IBM Glossary of Computing Terms*」を参照してください。

<http://www.ibm.com/ibm/terminology>

また、この用語集には、以下の刊行物に収容されている用語と定義が含まれています。

- 「*Information Technology Vocabulary*」。国際標準化機構および国際電気標準会議の第 1 合同技術委員会第 1 小委員会 (ISO/IEC JTC1/SC1) によって作成された資料。この用語集では、出版されたものの定義の後には記号 (I) が付いています。また、国際標準草案、委員会草案、および ISO/IEC JTC1/SC1 で作成中の作業文書から取られた定義の後には、記号 (T) が付いており、SC1 参加国間の最終合意がまだ得られていないことを示しています。
- 「*IBM Glossary of Computing Terms*」、New York: McGraw-Hill, 1994

この用語集では、以下の相互参照についての表記上の規則を使用しています。

を参照 (a) 省略語または頭字語の拡張された形である用語、あるいは、(b) 同義語またはより優先される用語を参照します。

も参照 関連した用語を参照します。

アービトレーテッド・ループ (arbitrated loop)

2 から 126 のポートが 1 つのループ回路内で直列に相互接続されている 3 つの既存ファイバー・チャネル・トポロジーの 1 つ。ファイバー・チャネル - アービトレーテッド・ループ (FC-AL) へのアクセスは、アービトレーション・スキームによって制御される。FC-AL トポロジーは、すべてのサービス・クラスをサポートし、さらに、発信元と応答側が同じ FC_AL にあるときは、FC フレームのイン・オーダー・デリバリーを保証する。ディスク・ア

レイのデフォルトのトポロジーは、アービトレーテッド・ループである。アービトレーテッド・ループは、ステルス・モードと呼ばれることがある。

アービトレーテッド・ループ物理アドレス (AL_PA) (arbitrated loop physical address (AL_PA))

アービトレーテッド・ループ内の関与しているデバイスを識別するために使用される 8 ビット値。ループは 1 つ以上の AL_PA を持つことができる。

アウト・オブ・バンド (out-of-band)

ファイバー・チャネル・ネットワークの外側で、通常、イーサネットを介して行われる管理プロトコルの伝送。

アクセス論理ドライブ (access logical drive)

ホスト・エージェントがストレージ・サブシステム内のコントローラーと通信できるようにする論理ドライブ。

アダプター (adapter)

ホスト・システムの内部バスと外部ファイバー・チャネル (FC) リンクとの間でユーザー・データ入出力 (I/O) を伝送するプリント回路アセンブリー。入出力アダプター、ホスト・アダプター、または、FC アダプターとも呼ばれる。

アレイ (array)

論理的にグループ化できる、ファイバー・チャネルまたは SATA ハード・ディスクの集合。アレイ内のすべてのドライブは、同一の RAID レベルを割り当てられる。アレイは、「RAID セット」と呼ばれることもある。**新磁気ディスク制御機構 (RAID) (redundant array of independent disks (RAID))**、RAID レベル (RAID level) も参照。

異機種混合のホスト環境 (heterogeneous host environment)

独自のディスク・ストレージ・サブシステム設定を持った異なるオペレーティング・システムを使用する複数のホスト・サーバ

ーが、同一の ストレージ・サブシステムに同時接続するホスト・システム。「ホスト (*host*)」も参照。

陰極線管 (CRT) (cathode ray tube (CRT))

制御された電子ビームを使用して電界発光画面上に英数字またはグラフィカル・データを表示する、ディスプレイ・デバイス。

インターネット・プロトコル (IP) (Internet Protocol (IP))

ネットワークまたは相互接続ネットワークを通じてデータの経路を定めるプロトコル。IP は、上位のプロトコル層と物理ネットワーク間の仲介としての役割を果たす。

インターネット・プロトコル (IP) アドレス (Internet Protocol (IP) address)

IP 規格を使用するネットワーク上の装置または論理装置に固有のアドレス。例えば、9.67.97.103 は IP アドレスである。

インバンド (in-band)

ファイバー・チャンネル・トランスポートを経由した管理プロトコルの伝送。

エージェント (agent)

Simple Network Management Protocol- 伝送制御プロトコル/インターネット・プロトコル (SNMP-TCP/IP) ネットワーク管理環境においてネットワーク・マネージャー (クライアント・プログラム) から仮想接続を受け取るサーバー・プログラム。

エラー訂正コード (ECC) (error correction coding (ECC))

ブロック内の複数のビット・エラーを検出して訂正する機能を持つ、データ・ブロックに付加されたコード。大部分の ECC は、検出し訂正できるエラーの最大数によって特徴付けられる。

お客様交換可能ユニット (CRU) (customer replaceable unit (CRU))

お客様が交換できるアセンブリーまたは部品。現場交換可能ユニット (*FRU*) (*field replaceable unit (FRU)*) と対比。

オブジェクト・データ・マネージャー (ODM) (Object Data Manager (ODM))

ドライブをカーネルの中に構成する作業の一環として編集される ASCII スタンザ・

ファイル用の AIX プロプラエタリー・ストレージ・メカニズム。

拡張業界標準アーキテクチャー (EISA) (Extended Industry Standard Architecture (EISA))

AT バス (ISA バス) を 32 ビットに拡張して、バス・マスターに対するサポートを提供する PC バス規格。1988 年に、既存のボードの投資を保護する、マイクロチャンネルに代わる 32 ビット版として発表された。PC および AT アダプター (ISA アダプター) を EISA バスに接続することができる。「業界標準アーキテクチャー (*Industry Standard Architecture*)」も参照。

拡張ポート (E_port) (expansion port (E_port))

大規模なスイッチ・ファブリックの建物内で、別のスイッチの E_port に接続するためのスイッチ間拡張ポートとして使用されるポート。

環境サービス・モジュール (ESM) キャニスター (environmental service module (ESM) canister)

そのエンクロージャー内のコンポーネントの環境条件をモニターする、ストレージ拡張エンクロージャー内のコンポーネント。すべてのストレージ・サブシステムが ESM キャニスターを装備しているわけではない。

管理情報ベース (MIB) (Management Information Base (MIB))

Simple Network Management Protocol (SNMP) において、ネットワーク管理システムによって照会または設定できるオブジェクトのデータベース。

ホストまたはゲートウェイから使用可能な情報および許可される操作を指定する管理情報の定義。

管理ステーション

ストレージ・サブシステムを管理するために使用されるシステム。管理ステーションは、ファイバー・チャンネル入出力 (I/O) パスを通じてストレージ・サブシステムに接続される必要はない。

ギガビット・インターフェース・コンバーター (GBIC) (gigabit interface converter (GBIC))

光ファイバー・ケーブルに接続される送受信コンセントを備えたクラス 1 レーザー・コンポーネント・アセンブリーであ

る、エンコード/デコード装置。GBIC は、順次に、光から電気、および電気から光の信号変換を行う。スイッチ内の GBIC はホット・スワップ対応である。「スモール・フォーム・ファクター・プラグブル (Small Form-Factor Pluggable)」も参照。

基本入出力システム (BIOS) (Basic Input/Output System (BIOS))

ディスク・ドライブ、ハード・ディスク・ドライブ、およびキーボードとの相互作用など、基本的なハードウェア操作を制御するコード。

業界標準アーキテクチャー (ISA) (Industry Standard Architecture (ISA))

IBM PC/XT パーソナル・コンピューターのバス・アーキテクチャーの非公式名。このバス設計には、さまざまなアダプター・ボードに接続する拡張スロットが組み込まれている。初期のバージョンは、8 ビットのデータ・バスをもち、その後 16 ビットのデータ・バスに拡張された。「Extended Industry Standard Architecture」(EISA) では更に 32 ビットのデータ・バスに拡張された。「拡張業界標準アーキテクチャー (Extended Industry Standard Architecture)」も参照。

区画化 「ストレージ区画 (storage partition)」を参照。

クライアント (client)

サーバーからサービスを要求するソフトウェア・プログラムまたはコンピューター。複数のクライアントが共通サーバーへのアクセスを共有することができる。

グラフィカル・ユーザー・インターフェース (GUI) (graphical user interface (GUI))

多くの場合、デスクトップ上の実世界の場面のビジュアル・メタフォアを、高解像度グラフィックス、ポインティング・デバイス、メニュー・バーおよび他のメニュー、重なり合うウィンドウ、アイコンおよび、オブジェクト - アクションの関係を結合することによって表すコンピューター・インターフェースの 1 つのタイプ。

グローバル・コピー (Global Copy)

書き込み整合性グループ・オプションなしの非同期書き込みモードを使用してセット

アップされるリモート論理ドライブ・ミラー・ペアを指す。これは「整合性グループを使用しない非同期ミラーリング」とも呼ばれる。グローバル・コピーは、複数の 1 次論理ドライブへの書き込み要求が、1 次論理ドライブ上と同じ順序で 2 次論理ドライブ上で実行されるよう保証はしない。1 次論理ドライブへの書き込みが、適切な 2 次論理ドライブでの順序と同じ順序で実行されることがクリティカルである場合は、グローバル・コピーでなくグローバル・ミラーリングを使用する必要がある。「非同期書き込みモード (asynchronous write mode)」、「グローバル・ミラーリング (Global Mirroring)」、「リモート・ミラーリング (remote mirroring)」、「メトロ・ミラーリング (Metro Mirroring)」も参照。

グローバル・ミラー (Global Mirror)

リモート・ミラーおよびコピー機能のオプション機能。2 サイトの拡張距離リモート・コピーを提供する。ローカル・サイトのストレージ・ユニットにホストにより書き込まれるデータは、自動的にリモート・サイトでも維持される。「非同期書き込みモード (asynchronous write mode)」、「グローバル・コピー (Global Copy)」、「リモート・ミラーリング (remote mirroring)」、「メトロ・ミラーリング (Metro Mirroring)」も参照。

現場交換可能ユニット (FRU) (field replaceable unit (FRU))

コンポーネントのいずれかに障害が起こった場合にそっくりそのまま交換されるアセンブリー。場合によっては、現場交換可能ユニットに他の現場交換可能ユニットが含まれていることもある。「お客様交換可能ユニット (CRU) (customer replaceable unit (CRU))」と対比。

コマンド (command)

アクションの開始またはサービスの開始に使用するステートメント。コマンドは、コマンド名の省略形と、適用される場合はそのパラメーターとフラグから成る。コマンドは、それをコマンド行でタイプ入力するか、メニューから選択して実行することができる。

コミュニティ・ストリング (community string)
それぞれの Simple Network Management Protocol (SNMP) のメッセージに含まれているコミュニティの名前。

サーバー (server)
他のソフトウェア・プログラムや他のコンピュータにサービスを提供する、ソフトウェア・プログラムまたはコンピュータ。

サーバー/装置イベント (server/device events)
サーバー上、またはユーザーが設定する基準を満たす指定デバイス上で起こるイベント。

先進テクノロジー (AT) バス・アーキテクチャー (advanced technology (AT) bus architecture)
IBM 互換製品用のバス規格。このアーキテクチャーは、XT バス・アーキテクチャーを 16 ビットに拡張し、バス・マスターを行えるようにするが、直接アクセスには、メイン・メモリーの最初の 16 MB しか使用できない。

サブネット (subnet)
独立した小さいサブグループに分割されたネットワークで、それらのサブグループは相互接続されている。

システム名 (system name)
ベンダーのサード・パーティー・ソフトウェアによって割り当てられたデバイス名。

自動 ESM ファームウェア同期 (automatic ESM firmware synchronization)
新規 ESM を、ESM ファームウェアの自動同期をサポートする DS3000 あるいは DS4000 ストレージ・サブシステム内の既存のストレージ拡張エンクロージャーに取り付けるとき、新規 ESM 内のファームウェアは自動的に既存 ESM 内のファームウェアに同期化される。

自動ドライブ転送 (ADT) (Auto Drive Transfer (ADT))
ストレージ・サブシステム上のコントローラーで障害が発生した場合に自動フェイルオーバーを提供する機能。

集積回路 (IC) (integrated circuit (IC))
相互接続された多くのトランジスターおよびその他のコンポーネントから成る超小型

電子技術半導体デバイス。IC は、シリコン結晶またはその他の半導体素材から切り取られた小さい長方形上に構成される。回路の小型化は、ボード・レベルの集積に比べて、高速化、電力浪費の削減、および、製造コストの削減ができる。チップとも呼ばれる。

終了後常駐型プログラム (TSR プログラム) (terminate and stay resident program (TSR program))

実行されるときに DOS の延長として、それ自身の一部をインストールするプログラム。

巡回冗長検査 (CRC) (cyclic redundancy check (CRC))

(1) 検査キーが巡回アルゴリズムによって生成される冗長検査。(2) 送受信の両方のステーションで実行されるエラー検出手法。

冗長ディスク・アレイ・コントローラー (RDAC) (redundant disk array controller (RDAC))

ハードウェアにおいては、コントローラーの予備セット (アクティブ/パッシブかアクティブ/アクティブのいずれか)。

ソフトウェアにおいて、通常の入出力操作中にアクティブなコントローラーを介して入出力 (I/O) を管理し、コントローラーまたは入出力パスが失敗した場合に、入出力を冗長セットの他のコントローラーに透過的に転送する層。

初期プログラム・ロード (IPL) (initial program load (IPL))

システム補助ストレージからシステム・プログラムをロードするプロセスで、システム・ハードウェアを検査し、ユーザー操作に備えてシステムを準備する。システム再始動、システム始動、およびブートとも呼ばれる。

シリアル ATA (serial ATA)

SCSI ハード・ディスクの高速の代替規格。SATA-1 規格は、パフォーマンスについて 10 000 RPM SCSI ドライブと同等である。

新磁気ディスク制御機構 (RAID) (Redundant Array of Independent Disks (RAID))

ホストに対して 1 つ以上の論理ディス

ク・ドライブのイメージを提示する、複数の物理ディスク・ドライブの集合 (アレイ)。物理装置に障害が起こった場合は、データの冗長性があるために、アレイ内の他のディスク・ドライブからデータを読み取ったり、再生成したりすることができる。アレイ (array)、パリティ検査 (parity check)、ミラーリング (mirroring)、RAID レベル (RAID level)、ストライピング (striping) も参照。

スイープ・メソッド (sweep method)

ネットワークの各デバイスに要求を送信することによって、情報に対する Simple Network Management Protocol (SNMP) 要求をサブネット上のすべてのデバイスに送信する方法。

スイッチ (switch)

リンク・レベル・アドレッシングを使用することによって、ポートごとの全帯域幅、およびデータの高速ルーティングを提供するファイバー・チャネル・デバイス。

スイッチ・グループ (switch group)

スイッチ、および、そのスイッチに接続されていて他のグループに属していないデバイスの集合。

スイッチ・ゾーニング (switch zoning)

「ゾーニング (zoning)」を参照。

ストライピング (striping)

「データ・ストライピング (data striping)」を参照。

ストレージ・エリア・ネットワーク (SAN)

サーバー、ストレージ製品、ネットワーク製品、ソフトウェア、およびサービスを結合して、特定の環境用に調整された、専用ストレージ・ネットワーク。「ファブリック (fabric)」も参照。

ストレージ・サブシステム ID (SAI または SA ID) (Storage Subsystem Identifier (SAI or SA Identifier))

ストレージ・サブシステム ID は各管理対象ストレージ・サーバーを一意的に識別するためにストレージ・マネージャーのホスト・ソフトウェア (SMClient) によって使用される識別値である。ストレージ・マネージャーの SMClient プログラムは、前にディスカバーされたストレージ・サーバ

ーのストレージ・サブシステム ID レコードをホスト常駐ファイル内に維持する。これにより、ディスクバリー情報を永続的に保存することが可能になる。

ストレージ拡張エンクロージャー (EXP)、またはストレージ・エンクロージャー (storage expansion enclosure (EXP) または storage enclosure)

システム・ユニットに接続して、追加のストレージおよび処理能力を提供できる機能。

ストレージ区画 (storage partition)

ホスト・コンピューターから可視であるか、またはホスト・グループの一部であるホスト・コンピューター間で共有されているストレージ・サブシステム論理ドライブ。

ストレージ区画トポロジー (storage partition topology)

ストレージ・マネージャー・クライアントにおいて、「Mappings (マッピング)」ウィンドウの「Topology (トポロジー)」ビューにデフォルト・ホスト・グループ、定義済みホスト・グループ、ホスト・コンピューター、およびホスト・ポート・ノードが表示される。ホスト・ポート、ホスト・コンピューター、およびホスト・グループのトポロジーのエレメントは、論理ドライブから LUN へのマッピングを使用してホスト・コンピューターおよびホスト・グループにアクセス認可を行えるように定義される必要がある。

スモール・フォーム・ファクター・プラグ可能 (SFP) (small form-factor pluggable (SFP))

信号を光ファイバー・ケーブルとスイッチの間で変換するために使用される光学式トランシーバー。SFP はギガビット・インターフェース・コンバーター (GBIC) より小さい。「ギガビット・インターフェース・コンバーター (gigabit interface converter)」も参照。

静的ランダム・アクセス・メモリー (SRAM) (static random access memory (SRAM))

フリップフロップと呼ばれる論理回路に基づいたランダム・アクセス・メモリー。これが「静的」と呼ばれるのは、定期的にリフレッシュが必要なダイナミック RAM

(DRAM) と異なり、電力が供給されている間は値を保持するからである。ただし、静的ランダム・アクセス・メモリーは、電源をオフにするとその内容が失われることがあるという意味で、揮発性である。

静電気の放電 (ESD)

静的帯電を持った物体が放電を起こすほどに接近した結果生じる電流の流れ。

セグメント・ループ・ポート (SL_port) (segmented loop port (SL_port))

ファイバー・チャネル・プライベート・ループを複数のセグメントへ分割できるようにするポート。各セグメントは、フレームを、独立ループとして次々に受け渡し、さらに、ファブリックを使用して同じループの別のセグメントに接続できる。

センス・データ (sense data)

否定応答とともに送信され、応答の理由を示すデータ。

入出力エラーについて説明するデータ。センス・データは、センス要求コマンドに応じてホスト・システムに提示される。

ゾーニング (zoning)

ファイバー・チャネル環境において、仮想で専用のストレージ・ネットワークを形成する複数ポートのグループ化。ゾーンのメンバーであるポートは相互に通信可能であるが、別のゾーンのポートからは分離されている。

アドレス、名前、または物理ポートによってノードのセグメンテーションをできるようにし、ファブリック・スイッチまたはハブによって提供される機能。

装置タイプ (device type)

デバイスをスイッチ、ハブ、ストレージなどの物理マップに入れるために使用する ID。

ダイナミック RAM (DRAM) (dynamic random access memory (DRAM))

保管データを保持するために、セルが、制御信号の反復適用を必要とするストレージ。

直接アクセス・ストレージ・デバイス (DASD) (direct access storage device (DASD))

アクセス時間が事実上データの位置とは関

係ないデバイス。情報は、先にアクセスされたデータを参照することなしに入力され、検索される。(例えば、データを線形の順序で保管する磁気テープ・ドライブに対して、ディスク・ドライブは DASD である。) DASD には、固定および取り外し可能なストレージ・デバイスが含まれる。

直接メモリー・アクセス (DMA) (direct memory access (DMA))

プロセッサの介入なしに行われるメモリーと入出力デバイスの間のデータの転送。

データ・ストライピング (data striping)

情報がブロック (固定量のデータ) に分割され、ブロックが並行して一連のディスクに書き込まれる (またはディスクから読み取られる) ストレージ・プロセス。

ディスク・アレイ・コントローラー (dac) (disk array controller (dac))

1 つ以上のディスク・アレイを管理して機能を提供するデバイス (RAID など)。「ディスク・アレイ・ルーター (disk array router)」も参照。

ディスク・アレイ・ルーター (dar) (disk array router (dar))

すべての論理装置番号 (LUN) (AIX 上では hdisk) への現行および据え置きのパスを含む、アレイ全体を表すルーター。

「ディスク・アレイ・コントローラー (disk array controller)」も参照。

デフォルト・ホスト・グループ (default host group)

次の要件を満たすストレージ区画トポロジー内の、ディスカバーされたホスト・ポート、定義されたホスト・コンピューター、および定義済みホスト・グループの論理集合。

- 特定の論理ドライブから LUN へのマッピングに関与していない。
- デフォルトの論理ドライブから LUN へのマッピングを使用して論理ドライブへのアクセスを共有している。

電氣的消去可能プログラマブル読み取り専用メモリー (EEPROM) (electrically erasable programmable read-only memory (EEPROM))

一貫した電源供給なしにその内容を保存できる、メモリー・チップの一種。一度だけ

プログラミングできる PROM とは異なっており、EEPROM は電氣的に消去することができる。消耗するまでに、限られた回数しか再プログラミングできないために、頻繁に変更されることがない少量のデータを保管するのに適している。

伝送制御プロトコル (TCP) (Transmission Control Protocol (TCP))

インターネットおよびインターネットワーク・プロトコルに関する Internet Engineering Task Force (IETF) 規格に従う、任意のネットワークで使用される通信プロトコル。TCP は、パケット交換通信ネットワーク内、およびそのようなネットワークの相互接続システム内で信頼性の高いホスト間プロトコルを提供する。

伝送制御プロトコル/インターネット・プロトコル (TCP/IP) (Transmission Control Protocol/Internet Protocol (TCP/IP))

ローカル・エリア・ネットワークと広域ネットワークの両方に、対等接続機能を提供する通信プロトコルのセット。

同期書き込みモード (synchronous write mode)

リモート・ミラーリングで、1 次コントローラーが 2 次コントローラーからの書き込み操作の肯定応答を待って、書き込み入出力要求の完了をホストに戻すオプション。「非同期書き込みモード (asynchronous write mode)」、「リモート・ミラーリング (remote mirroring)」、「メトロ・ミラーリング (Metro Mirroring)」も参照。

統合ドライブ・エレクトロニクス (IDE) (integrated drive electronics (IDE))

コントローラーの電子回路がドライブ自体に収容され、別個のアダプター・カードを必要としない、16 ビット IBM パーソナル・コンピューターの業界標準アーキテクチャー (ISA) に基づくディスク・ドライブ・インターフェース。Advanced Technology Attachment (ATA) インターフェースとも呼ばれる。

動的ホスト構成プロトコル (DHCP) (Dynamic Host Configuration Protocol (DHCP))

構成情報を集中管理するために使用される通信プロトコル。例えば、DHCP は自動的

にネットワーク内のコンピューターに IP アドレスを割り当てる。

トポロジー (topology)

ネットワーク内のネットワーキング・コンポーネントまたはノードのロケーションの物理または論理マッピング。共通ネットワーク・トポロジーには、バス、リング、スター、およびツリーが含まれる。ファイバー・チャネル・トポロジーには、ファブリック、アービトレーテッド・ループ、および、Point-to-Point の 3 つがある。ディスク・アレイのデフォルトのトポロジーは、アービトレーテッド・ループである。

ドメイン (domain)

ファイバー・チャネル (FC) デバイスのノード・ポート (N_port) ID における最上位バイト。ファイバー・チャネル - small computer system interface (FC-SCSI) ハードウェア・パス ID では使用されない。1 つの FC アダプターに論理的に接続されているすべての SCSI ターゲットに対して同じであることが必要である。

ドライブ・チャネル (drive channels)

DS4200、DS4700、および DS4800 サブシステムは、物理的観点からは、2 つのドライブ・ループと同じ方法で接続されるデュアル・ポート・ドライブ・チャネルを使用する。ただし、ドライブ数およびエンクロージャー数の観点からは、2 つの異なるドライブ・ループではなく、単一のドライブ・ループとして扱われる。ストレージ拡張エンクロージャーのグループは、各コントローラーからのドライブ・チャネルを使用して、DS3000 あるいは DS4000 ストレージ・サブシステムに接続される。このドライブ・チャネル・ペアは、冗長ドライブ・チャネル・ペアと呼ばれる。

ドライブ・ループ (drive loops)

ドライブ・ループは、1 つの冗長ドライブ・チャネル・ペアまたは冗長ドライブ・ループを形成するために結合された、各コントローラーの 1 つのチャネルで構成される。各ドライブ・ループは 2 つのポートに関連付けられる。(1 つのコントローラーごとに 2 つのドライブ・チャネルと 4 つの関連ポートがある。) DS4800 の場合、ドライブ・ループは一般にドライブ・

チャンネルと呼ばれる。「ドライブ・チャンネル (*drive channels*)」を参照。

トラップ (trap)

Simple Network Management Protocol (SNMP) において、例外条件を報告するために、管理対象ノード (エージェント機能) によって管理ステーションに送信されるメッセージ。

トラップ受信者 (trap recipient)

転送された Simple Network Management Protocol (SNMP) トラップの受信側。具体的には、トラップの受信側は、トラップが送信される先のインターネット・プロトコル (IP) アドレスとポートによって定義される。おそらく、実際の受信者は、その IP アドレスで実行され、そのポートを listen するソフトウェア・アプリケーションである。

トランシーバー (transceiver)

通信において、トランシーバー・ケーブルをイーサネット同軸ケーブルに接続する装置。トランシーバーは、データの送信および受信に使用される。トランシーバーは、送受信装置の省略語である。

ネットワーク管理ステーション (NMS) (network management station (NMS))

Simple Network Management Protocol (SNMP) において、ネットワーク・エレメントをモニターし制御する管理アプリケーション・プログラムを実行するステーション。

ノード (node)

ネットワーク内でデータ伝送を可能にする物理デバイス。

ノード・ポート (N_port) (node port (N_port))

ファイバー・チャンネル・リンクを介してデータ通信を行う、ファイバー・チャンネル定義のハードウェア・エンティティ。これは、固有の Worldwide Name によって識別可能である。これは、発信元としての、または応答者としての役割を果たすことである。

ハブ (hub)

ネットワークにおいて、回路が接続されるか、あるいは、切り替えられるポイント。例えば、スター型ネットワークでは、ハブ

は中央ノードであり、スター型/リング型ネットワークでは、ハブは集線装置の場所である。

パフォーマンス・イベント (performance event)

ストレージ・エリア・ネットワーク (SAN) のパフォーマンスに関して設定されたしきい値に関連したイベント。

パリティ検査 (parity check)

アレイ内のビットの 1 (または 0) の数、奇数であるか偶数であるかを判別するテスト。

2 点間で通信される情報の数値的表現における数理的な操作。例えば、パリティが奇数である場合、偶数で表されるすべての文字にはビットが 1 つ追加され、それを奇数にする。情報の受信者は情報の各単位が奇数値であることを確認する。

非同期書き込みモード (asynchronous write mode)

リモート・ミラーリングで、データが 2 次コントローラーによって正しく書き込まれる前に、1 次コントローラーが、書き込み入出力要求の完了をホスト・サーバーに戻すことができるようにするオプション。「同期書き込みモード (*synchronous write mode*)」、「リモート・ミラーリング (*remote mirroring*)」、「グローバル・コピー (*Global Copy*)」、「グローバル・ミラーリング (*Global Mirroring*)」も参照。

ブートストラップ・プロトコル (BOOTP) (Bootstrap Protocol (BOOTP))

クライアントがネットワーク上のサーバーからインターネット・プロトコル (IP) アドレスおよびファイル名の両方を検出できるようにするプロトコル。

ファイバー・チャンネル (FC) (Fibre Channel (FC))

コンピューター・デバイス間でデータを送信するためのテクノロジー。コンピューター・サーバーを共有ストレージ・デバイスに接続する場合、およびストレージ・コントローラーとドライブを相互接続する場合に特に適している。FC は、point-to-point、アービトラレーテッド・ループ、およびスイッチ・トポロジーをサポートする。

ファイバー・チャンネル・アービトレーテッド・ループ (FC-AL)

「アービトレーテッド・ループ (*arbitrated loop*)」を参照。

ファブリック (*fabric*)

接続された N_port のログインを相互接続し、使用しやすくする、ファイバー・チャンネル・エンティティ。ファブリックは、フレーム・ヘッダーでのアドレス情報を使用して、ソースおよび宛先 N_port 間のフレームのルーティングを担当する。ファブリックは、2 つの N_port 間の Point-to-Point チャンネルのように単純であることも可能であるし、または F_port 間のファブリック内に複数の予備的内部バスを備えたフレーム・ルーティング・スイッチのように複雑であることも可能である。

ファブリック・ポート (F_port) (*fabric port* (F_port))

ファブリックにおいて、ユーザーの N_port 接続のためのアクセス・ポイント。F_port は、ファブリックに接続されたノードからファブリックへの N_port ログインを容易にする。F_port は、接続される N_port によってアドレス可能である。「ファブリック (*fabric*)」も参照。

フィーチャー使用可能化 ID

プレミアム・フィーチャー・キーの生成プロセスで使用される、ストレージ・サブシステム用の固有 ID。「プレミアム・フィーチャー・キー (*premium feature key*)」も参照。

不揮発性ストレージ (NVS) (*nonvolatile storage* (NVS))

電源が切られても内容が失われないストレージ・デバイス。

プライベート・ループ (*private loop*)

ファブリックへの接続がないファイバー・チャンネル・アービトレーテッド・ループ (FC-AL)。「アービトレーテッド・ループ (*arbitrated loop*)」も参照。

ブリッジ (*bridge*)

物理およびトランスポート変換 (例えば、ファイバー・チャンネルから SCSI ブリッジへ) を提供するストレージ・エリア・ネットワーク (SAN) デバイス。

ブリッジ・グループ (*bridge group*)

ブリッジおよびそのブリッジに接続されているデバイスの集合。

プレミアム・フィーチャー・キー (*premium feature key*)

ストレージ・サブシステム・コントローラーが許可されたプレミアム・フィーチャーを使用可能にするために使用するファイル。ファイルには、プレミアム・フィーチャーが許可されるストレージ・サブシステムのフィーチャー使用可能化 ID、およびプレミアム・フィーチャーに関するデータが入っている。「機能使用可能 ID (*feature enable identifier*)」も参照。

ブロードキャスト (*broadcast*)

複数の宛先へのデータの同時伝送。

プログラム一時修正 (PTF) (*program temporary fix* (PTF))

System i、System p、および System z 製品の場合、IBM によってテストされ、すべてのお客様が使用できる修正。

並行ダウンロード (*concurrent download*)

ユーザーがプロセス中にコントローラーへの入出力を停止する必要のない、ファームウェアのダウンロードおよびインストール方法。

変換ループ・ポート (TL_port) (*translated loop port* (TL_port))

プライベート・ループに接続し、プライベート・ループ・デバイスとオフ・ループ・デバイス (その特定の TL_port に接続されていないデバイス) との間を接続できるようにするポート。

ポート (*port*)

外部デバイス (ディスプレイ装置、端末、プリンター、スイッチ、または外部ストレージ・ユニットなど) 用ケーブルが接続されるシステム・ユニット、またはリモート・コントローラーの部分。ポートはデータ入力、または終了のアクセス・ポイントである。1 つのデバイスは、1 つ以上のポートを持つことができる。

ポーリング遅延 (*polling delay*)

連続したディスクバリー・プロセスの間にディスクバリーが非アクティブになる時間 (秒数)。

ホスト (host)

ファイバー・チャネル入出力 (I/O) パスを通じてストレージ・サブシステムに直接接続されたシステム。このシステムは、ストレージ・サブシステムからのデータを (通常はファイルの形で) 提供するのに使用される。システムは、同時に管理ステーションとホストの両方になることができる。

ホスト・グループ (host group)

1 つ以上の論理ドライブへの共有アクセスを必要とするホスト・コンピューターの論理集合を定義する、ストレージ区画トポロジにおけるエンティティ。

ホスト・コンピューター (host computer)

「ホスト (host)」を参照。

ホスト・バス・アダプター (HBA) (host bus adapter (HBA))

PCI バスなどのホスト・バスをストレージ・エリア・ネットワークに接続するインターフェース・カード。

ホスト・ポート (host port)

ホスト・アダプターに物理的に存在し、ストレージ・マネージャー・ソフトウェアにより自動的にディスカバーされるポート。ホスト・コンピューターに区画へのアクセス権を与えるには、その関連ホスト・ポートが定義されている必要がある。

ホット・スワップ (hot-swap)

システムをオンにしたまま取り替えが可能なデバイスを指す。

マイクロチャネル・アーキテクチャー (MCA)

(Micro Channel architecture (MCA))

コンピューターで、サブシステムおよびアダプターがマイクロチャネル・バスを使用する方法を定義する規則。MCA は、各サブシステムが提供できる、または提供する必要があるサービスを定義する。

マスク不能割り込み (NMI) (non-maskable interrupt (NMI))

別のサービス要求が退ける (マスクする) ことができないハードウェア割り込み。

NMI は、ソフトウェア、キーボード、および他のそのようなデバイスによって生成された割り込み要求をバイパスし、それらの割り込み要求に優先し、破滅的状況 (重大なメモリー・エラーまたは差し迫った電

源障害など) においてのみマイクロプロセッサに対して出される。

ミニ・ハブ (mini hub)

短波 (Short Wave) ファイバー・チャネルの GBIC または SFP を受信する、インターフェース・カードまたはポート・デバイス。これらのデバイスを使用すると、光ファイバー・ケーブルによる、直接またはファイバー・チャネル・スイッチ/管理ハブを経由した、ホスト・コンピューターから DS3000 および DS4000 ストレージ・サーバー・コントローラーへの冗長ファイバー・チャネル接続が可能になる。各 DS3000 および DS4000 コントローラーは 2 つのミニ・ハブの管理を担当する。各ミニハブには 2 つのポートがある。4 つのホスト・ポート (各コントローラーに 2 つ) は、スイッチを使用することなくクラスター・ソリューションを提供する。2 つのホスト・サイドのミニハブが標準として配送される。「ホスト・ポート (host port)」、「ギガビット・インターフェース・コンバーター (GBIC) (gigabit interface converter (GBIC))」、「スモール・フォーム・ファクター・プラグابل (SFP) (Small Form-Factor Pluggable (SFP))」も参照。

ミラーリング (mirroring)

ハード・ディスク上の情報を追加のハード・ディスク上に複写する、フォールト・トレランス手法。リモート・ミラーリング (remote mirroring) も参照。

無停電電源装置 (uninterruptible power supply)

商用電源とシステムの間に設置されたバッテリーからの供給電源で、商用電源に障害が生じた場合にシステム処理が正常に完了するまでシステムを稼働し続ける。

メディア・アクセス制御 (MAC) (Media Access Control (MAC))

ネットワーキングにおいて、オープン・システム間相互接続モデルのデータ・リンク層の 2 つのサブレイヤーの下位のもの。MAC サブレイヤーは、共有メディアへのアクセスを処理する (例えば、トークン・パッシングを使用するか、競合を使用するか)。

メディア・スキャン (media scan)

メディア・スキャンは、この機能が使用可能になっているストレージ・サブシステム内のすべての論理ドライブ上で実行されるバックグラウンド・プロセスの 1 つであり、ドライブ・メディア上でのエラー検出を提供する。メディア・スキャン・プロセスは、すべての論理ドライブ・データをスキャンして、そのデータにアクセスできることを確認し、またオプションとして、論理ドライブの冗長情報をスキャンする。

メトロ・ミラー (metro mirror)

ソース論理ドライブに対して行われた変更内容と一致するように、論理ドライブの 2 次コピーを継続的に更新するリモート・ミラーおよびコピー機能。「リモート・ミラーリング (remote mirroring)」、「グローバル・ミラーリング (Global Mirroring)」も参照。

モデル (model)

製造メーカーによってデバイスに割り当てられたモデル識別番号。

ユーザー処置イベント (user action events)

ユーザーが取る処置、例えば、SAN 内の変更、設定の変更など。

有効範囲 (scope)

コントローラーのグループをそのインターネット・プロトコルのアドレスによって定義する。スコープは、動的 IP アドレスをネットワーク上のコントローラーに割り当てることができるように作成され、定義される必要がある。

読み取り専用メモリー (ROM) (read-only memory (ROM))

特殊な条件下の場合を除き、保管されるデータがユーザーにより変更できないメモリー。

ラベル (label)

物理マップおよびデータ・パス・マップの各デバイスの下に表示される、ディスクカバーされたあるいはユーザーが入力したプロパティ値。

ランダム・アクセス・メモリー (RAM) (random access memory (RAM))

保管場所に直接アクセスできるコンピューター・メモリー。「DASD」と対比。

リカバリー可能仮想共有ディスク (RVSD)

(recoverable virtual shared disk (RVSD))

クラスター内のデータおよびファイル・システムに連続アクセスを行うように構成された、サーバー・ノード上の仮想共有ディスク。

リモート・ミラーリング (remote mirroring)

別々のメディアに維持されているストレージ・サブシステムの間で、オンラインでリアルタイムに実行されるデータの複製操作。拡張リモート・ミラー・オプションは、リモート・ミラーリングのサポートを提供するためのプレミアム・フィーチャーである。「グローバル・ミラーリング (Global Mirroring)」、「メトロ・ミラーリング (Metro Mirroring)」も参照。

ルーター (router)

ネットワーク・トラフィック・フローのパスを決定するコンピューター。パスの選択は、特定のプロトコル、最短のまたは最良のパスを識別しようと試みるアルゴリズム、および経路距離またはプロトコル固有の宛先アドレスといったその他の基準から得られた情報に基づいて行われる。

ループ・アドレス (loop address)

ループ ID と呼ばれることもある、ファイバー・チャネル・ループ・トポロジー内のノードの固有の ID。

ループ・グループ (loop group)

1 つのループ回路内で直列に相互接続されているストレージ・エリア・ネットワーク (SAN) デバイスの集合。

ループ・ポート (loop port)

ノードをファイバー・チャネル・アービトラレーテッド・ループ (FC-AL) に接続するために使用されるポート。

ローカル・エリア・ネットワーク (LAN) (local area network (LAN))

限定された領域内 (単一のビルまたはキャンパスなど) のいくつかの装置を接続し、より大きなネットワークに接続できるネットワーク。

論理区画 (LPAR) (logical partition (LPAR))

リソース (プロセッサ、メモリー、および入出力デバイス) が含まれている単一のシステムのサブセット。論理区画は独立し

たシステムとして作動する。ハードウェア要件が満たされる場合、システム内に複数の論理区画が存在できる。

論理ドライブの固定サイズ部分。論理区画は、アレイ内の物理区画と同じサイズである。論理区画が一部となっている論理ドライブがミラーリングされない場合、各論理区画は単一の物理区画に対応し、内容は物理区画に保管される。

1 から 3 個の物理区画 (コピー)。論理ドライブ内の論理区画の数は変数である。

論理装置番号 (LUN) (logical unit number (LUN))

SCSI 標準において、それぞれが論理装置 (LU) である装置を区別するために使用される固有 ID。

論理ブロック・アドレス (LBA) (logical block address (LBA))

論理ブロックのアドレス。論理ブロック・アドレスは、通常、ホストの入出力コマンドで使用される。例えば、SCSI ディスク・コマンド・プロトコルは、論理ブロック・アドレスを使用する。

ワールドワイド・ポート名 (WWPN) (worldwide port name (WWPN))

スイッチに関連付けられた固有の 64 ビット ID。WWPN は、実装およびプロトコルに依存しない方法で割り当てられる。

割り込み要求 (IRQ) (interrupt request (IRQ))

通常の命令実行を一時的に中断して割り込みハンドラー・ルーチンの実行を開始する原因となる、プロセッサ上で検出される入力。

Abstract Windowing Toolkit (AWT)

Java プログラミングにおける、コンポーネントの独自のプラットフォーム・バージョンを使用して実装された GUI コンポーネントの集合。これらのコンポーネントは、すべてのオペレーティング・システム環境に共通の機能のサブセットを提供する。

accelerated graphics port (AGP)

低コストの 3D グラフィックス・カードに、通常の周辺コンポーネント相互接続 (PCI) バスよりも、パーソナル・コンピュ

ーター上のメイン・メモリーへのより速いアクセスを提供するバス仕様。AGP は、既存のシステム・メモリーを使用して、ハイエンドのグラフィックス・サブシステムの作成コスト全体を削減させる。

ADT 「自動ドライブ転送 (Auto Drive Transfer)」を参照。

AGP 「Accelerated Graphics Port」を参照。

AL_PA

「アービトレーテッド・ループ物理アドレス (arbitrated loop physical address)」を参照。

AT 「先進テクノロジー (AT) バス・アーキテクチャー (advanced technology (AT) bus architecture)」を参照。

AT 接続 (AT-attached)

元の IBM AT コンピューター規格と互換性のある周辺装置。その 40 ピン AT 接続 (ATA) リボン・ケーブル上の信号が、IBM PC AT コンピューターの業界標準アーキテクチャー (ISA) のシステム・バスのタイミングと制約に従っている。「統合ドライブ・エレクトロニクス (IDE)(integrated drive electronics (IDE))」と同等。

ATA 「AT 接続 (AT-attached)」を参照。

AWT 「Abstract Windowing Toolkit」を参照。

BIOS 「基本入出力システム (basic input/output system)」を参照。

BOOTP

「ブートストラップ・プロトコル (bootstrap protocol)」を参照。

CRC 「巡回冗長検査 (cyclic redundancy check)」を参照。

CRT 「陰極線管 (cathode ray tube)」を参照。

CRU 「お客様交換可能ユニット (customer replaceable unit)」を参照。

dac 「ディスク・アレイ・コントローラー (disk array controller)」を参照。

dar 「ディスク・アレイ・ルーター (disk array router)」を参照。

DASD 「直接アクセス・ストレージ・デバイス (direct access storage device)」を参照。

DHCP 「動的ホスト構成プロトコル (*Dynamic Host Configuration Protocol*)」を参照。

DMA 「直接メモリー・アクセス (*direct memory access*)」を参照。

DRAM
「ダイナミック RAM (*dynamic random access memory*)」を参照。

ECC 「エラー訂正コード (*error correction code*)」を参照。

EEPROM
「電氣的消去可能プログラマブル読み取り専用メモリー (*electrically erasable programmable read-only memory*)」を参照。

EISA 「拡張業界標準アーキテクチャー (*Extended Industry Standard Architecture*)」を参照。

ESD 「静電気の放電 (*electrostatic discharge*)」を参照。

ESM キャンISTER (ESM canister)
「環境サービス・モジュール・キャンISTER (*environmental service module canister*)」を参照。

EXP 「ストレージ拡張エンクロージャー (*storage expansion enclosure*)」を参照。

E_port 「拡張ポート (*expansion port*)」を参照。

FC 「ファイバー・チャネル (*Fibre Channel*)」を参照。

FC-AL
「アービトレーテッド・ループ (*arbitrated loop*)」を参照。

FlashCopy
データのインスタント・コピー (すなわち論理ドライブのポイント・イン・タイム・コピー) を作成できる、Storage System DS ファミリーのオプション・フィーチャー。

FRU 「現場交換可能ユニット (*field replaceable unit*)」を参照。

F_port 「ファブリック・ポート (*fabric port*)」を参照。

GBIC 「ギガビット・インターフェース・コンバーター (*gigabit interface converter*)」を参照。

GUI 「グラフィカル・ユーザー・インターフェース (*graphical user interface*)」を参照。

HBA 「ホスト・バス・アダプター (*host bus adapter*)」を参照。

hdisk アレイ上の論理装置番号 (LUN) を表す AIX 用語。

IBMSAN ドライバー (IBMSAN driver)
Novell NetWare 環境で使用され、ストレージ・コントローラーにマルチパス入出力サポートを提供するデバイス・ドライバ。

IC 「集積回路 (*integrated circuit*)」を参照。

IDE 「統合ドライブ・エレクトロニクス (*integrated drive electronics*)」を参照。

IP 「インターネット・プロトコル (*Internet Protocol*)」を参照。

IPL 「初期プログラム・ロード (*initial program load*)」を参照。

IRQ 「割り込み要求 (*interrupt request*)」を参照。

ISA 「業界標準アーキテクチャー (*Industry Standard Architecture*)」を参照。

Java ランタイム環境 (JRE) (Java runtime environment (JRE))
Java Developer Kit のサブセットであり、標準的な Java プラットフォームを構成する核となる実行可能プログラムとファイルが収められている。JRE には、Java 仮想マシン (JVM)、コア・クラス、およびサポート・ファイルが組み込まれている。

JRE 「Java ランタイム環境 (*Java Runtime Environment*)」を参照。

LAN 「ローカル・エリア・ネットワーク (*local area network*)」を参照。

LBA 「論理ブロック・アドレス (*logical block address*)」を参照。

LPAR 「論理区画 (*logical partition*)」を参照。

LUN 「論理装置番号 (*logical unit number*)」を参照。

MAC 「メディア・アクセス制御 (*Medium access control*)」を参照。

man ページ (man page)

UNIX システムにおける、1 ページのオンライン資料。それぞれの UNIX コマンド、ユーティリティ、およびライブラリー関数には man ページが関連付けられている。

MCA 「マイクロチャネル・アーキテクチャー (*micro channel architecture*)」を参照。

MIB 「管理情報ベース (*management information base*)」を参照。

Microsoft Cluster Server (MSCS)

コンピュータを MSCS クラスタにグループ化することによって高可用性を提供するテクノロジー。クラスタ内のいずれかのコンピュータが一連の問題のいずれかにヒットする場合、MSCS は、中断されたアプリケーションを所定の手順でシャットダウンして、その状態データをクラスタ内の別のコンピュータに転送し、そこでアプリケーションを再開する。

MSCS 「Microsoft Cluster Server」を参照。

NMI 「マスク不能割り込み (*non-maskable interrupt*)」を参照。

NMS 「ネットワーク管理ステーション (*network management station*)」を参照。

NVS 「不揮発性ストレージ (*nonvolatile storage*)」を参照。

NVSRAM

不揮発性ストレージ・ランダム・アクセス・メモリー (*Nonvolatile storage random access memory*)。 「不揮発性ストレージ (*nonvolatile storage*)」を参照。

N_port

「ノード・ポート (*node port*)」を参照。

ODM 「オブジェクト・データ・マネージャー (*Object Data Manager*)」を参照。

PCI ローカル・バス (PCI local bus)

「PCI ローカル・バス (*peripheral component interconnect local bus*)」を参照。

PCI ローカル・バス (Peripheral Component Interconnect local bus (PCI local bus))

Intel 提供の PC 用のローカル・バス。CPU と最大 10 個の周辺装置 (ビデオ、

ディスク、ネットワーク、など) 間の高速データ・バスを提供する。PCI バスは、Industry Standard Architecture (ISA) または、Extended Industry Standard Architecture (EISA) バスをもつ PC 内に共存する。ISA と EISA ボードは、IA または EISA スロットに接続するが、高速 PCI コントローラーは PCI スロットに接続する。「業界標準アーキテクチャー (*Industry Standard Architecture*)」、「拡張業界標準アーキテクチャー (*Extended Industry Standard Architecture*)」も参照。

PDF 「PDF (*portable document format*)」を参照。

PDF (portable document format)

文書の電子配布のために、Adobe Systems, Incorporated によって仕様が作成された規格。PDF ファイルはコンパクトで、E メール、Web、イントラネット、CD-ROM あるいは DVD-ROM でグローバルに配布でき、Acrobat Reader を使用して表示できる。

PTF 「プログラム一時修正 (*program temporary fix*)」を参照。

RAID 新磁気ディスク制御機構 (*RAID*) (*redundant array of independent disks (RAID)*) を参照。

RAID セット (RAID set)
アレイ (*array*) を参照。

RAID レベル

アレイの RAID レベルは、アレイの冗長性および耐障害性の実現に使用される方式を表す番号。アレイ (*array*)、新磁気ディスク制御機構 (*RAID*) (*redundant array of independent disks (RAID)*) も参照。

RAM 「ランダム・アクセス・メモリー (*random access memory*)」を参照。

RDAC 「冗長ディスク・アレイ・コントローラー (*redundant disk array controller*)」を参照。

ROM 「読み取り専用メモリー (*read-only memory*)」を参照。

RVSD 「リカバリー可能仮想共有ディスク (*recoverable virtual shared disk*)」を参照。

SA ID 「ストレージ・サブシステム ID (*storage subsystem Identifier*)」を参照。

SAI 「ストレージ・サブシステム ID (*Storage Subsystem Identifier*)」を参照。

SAN 「ストレージ・エリア・ネットワーク (*storage area network*)」を参照。

SATA 「シリアル ATA (*serial ATA*)」を参照。

SCSI 「*Small Computer System Interface (SCSI)*」を参照。

SCSI 用のファイバー・チャネル・プロトコル (FCP) (Fibre Channel Protocol (FCP) for small computer system interface (SCSI))

低レベルのファイバー・チャネル (FC-PH) サービスを使用して、FC リンク上の SCSI イニシエーターと SCSI ターゲット間で、FC フレームおよびシーケンス・フォーマットを用いて、SCSI コマンド、データ、および状況情報を伝送する、高水準のファイバー・チャネル・マッピング層 (FC-4)。

Serial Storage Architecture (SSA)

IBM によって実装された、ストレージ・サブシステムなどの周辺装置用の Point-to-Point 接続を提供する高速シリアル・インターフェースに関する米国規格協会 (ANSI) の規格。Small Computer System Interface (SCSI) デバイスと互換性がある SSA は、各方向に 20Mbps の速度で、全二重パケットの多重化されたシリアル・データ転送を可能にする。

SFP 「スモール・フォーム・ファクター・プラグブル (*Small Form-Factor Pluggable*)」を参照。

Simple Network Management Protocol (SNMP)

複合ネットワークでシステムとデバイスをモニターするための一連のプロトコル。管理対象装置に関する情報は、管理情報ベース (MIB) で定義および保管される。

SL_port

「セグメント・ループ・ポート (*segmented loop port*)」を参照。

SMagent

POWER ホスト・システムで Microsoft Windows、Novell NetWare、AIX、HP-

UX、Solaris、および Linux を使用することができ、ホスト・ファイバー・チャネル接続を介してストレージ・サブシステムを管理する、ストレージ・マネージャーの任意指定の Java ベースのホスト・エージェント・ソフトウェア。

Small Computer System Interface (SCSI)

ANSI 規格の電子インターフェースであり、パーソナル・コンピューターが周辺ハードウェア (ディスク・ドライブ、テープ・ドライブ、CD-ROM ドライブまたは DVD-ROM ドライブ、プリンター、スキャナーなど) との通信を、以前のインターフェースよりも高速かつ柔軟に行うことができるようにする。

各種の周辺デバイスが互いに通信できるようにする標準ハードウェア・インターフェース。

SMclient

ストレージ・サブシステムにおいて、ストレージ・サーバーおよびストレージ拡張エンクロージャーの構成、管理、およびトラブルシューティングに使用される、Java ベースのグラフィカル・ユーザー・インターフェース (GUI) である、ストレージ・マネージャーのクライアント・ソフトウェア。SMclient は、ホスト・システムまたは管理ステーションで使用できる。

SMruntime

SMclient 用の Java コンパイラー。

SMutil POWER のホスト・システムで Microsoft Windows、AIX、HP-UX、Solaris、および Linux を、新規論理ドライブのオペレーティング・システムへの登録およびマッピングに使用される、ストレージ・マネージャーのユーティリティ・ソフトウェア。Microsoft Windows の場合は、特定ドライブのオペレーティング・システムのキャッシュ付きデータを FlashCopy の作成前にフラッシュする、ユーティリティも入っている。

SNMP 「*Simple Network Management Protocol*」および「*SNMPv1*」を参照。

SNMP トラップ・イベント (SNMP trap event)

しきい値などの事前設定値を超過した状態を示す、SNMP エージェントによって送信されるイベント通知。「*Simple Network Management Protocol (SNMP)*」も参照。

SNMPv1

SNMP のオリジナルの規格は、SNMP の改訂版である SNMPv2 と対比して、現在では SNMPv1 と呼ばれる。「*Simple Network Management Protocol (SNMP)*」も参照。

SRAM 「静的ランダム・アクセス・メモリー (SRAM) (*static random access memory (SRAM)*)」を参照。

SSA 「*Serial Storage Architecture (SSA)*」を参照。

TCP 「*TCP プロトコル (Transmission Control Protocol)*」を参照。

TCP/IP

「*TCP/IP (Transmission Control Protocol/Internet Protocol)*」を参照。

TL_port

「変換ループ・ポート (*translated loop port*)」を参照。

TSR プログラム (TSR program)

「終了後常駐型プログラム (*terminate and stay resident program*)」を参照。

worldwide name (WWN)

各ファイバー・チャネル・ポートに割り当てられた、64 ビットの符号なし固有名 ID。

WORM

「*write-once read-many*」を参照。

Write Once Read Many (WORM)

データの書き込みは 1 回しかできないが、そこからの読み取りは何回でもできる、あらゆるタイプのストレージ・メディア。データが記録された後は、そのデータは変更できない。

WWN 「*Worldwide Name*」を参照。

索引

日本語, 数字, 英字, 特殊文字の順に配列されています。なお, 濁音と半濁音は清音と同等に扱われています。

【ア行】

アウト・オブ・バンド構成

参照: ネットワーク管理構成

アクセシビリティ

資料 345

ストレージ・マネージャー機能 345

アクセス・ボリューム 6, 335

アダプター (adapter)

参照: HBA

アラート通知、設定 40

アレイ 81

作成 74

定義 74

アンインストール

ストレージ・マネージャー 36

Windows での DS TKLM プロキシ
ー・コード、外部セキュリティ・
キー管理 230

イーサネット

Solaris 要件、クラスター・サービス
331

イーサネット MAC アドレス

参照: MAC アドレス

異機種環境 91

イベント

DDC MEL 288

イベント、重大

説明 263

番号 263

必要な処置 263

問題の解決 263

医療用画像処理アプリケーション 83

インストール 229

完了手順 36

構成タイプ 2

コンソール・ウィンドウ 33

準備 1

ストレージ・マネージャー 29

ストレージ・マネージャー、自動 30

ストレージ・マネージャー、手動 34,
35

ネットワーク構成 3

のシーケンス 34

マルチパス・ドライバ 132

インストール (続き)

AIX または Linux でのプロキシ、
外部セキュリティ・キー管理 230

FDE ドライブ 231

Support Monitor 29

VMware ESX Server 構成 313

Windows での DS TKLM プロキシ
ー・コード、外部セキュリティ・
キー管理 229

インバンド構成

参照: ホスト・エージェント管理構成

ウィンドウ

スクリプト・エディター 109

永続的予約 99

エラー

FCP ディスク・アレイ 289

エラー、メディア・スキャン 101

オブジェクト・データ・マネージャー

(ODM) 属性

定義 333

デバイスの初期識別 172

オペレーティング・システム

ストレージ・マネージャーでのサポー
ト 1

要件 30

DS TKLM プロキシ・コード 224

SAN ブートを使用したブート 113

Solaris 160

【カ行】

外部セキュリティ・キー管理 208, 212,
219, 224, 226, 229, 235

構成 235

DS TKLM プロキシ・コード・サー
バー 229, 230

書き込みキャッシュ

使用可能化 107

拡張グローバル・ミラーリング

使用 96

管理ステーション xi

互換性のある構成タイプ 2

説明 1, 4

VMware ESX Server 314

キー、セキュリティ (FDE)

参照: FDE

キャッシュ先読み、乗数の選択 107

キャッシュのミラーリング 291, 324

キャッシュのミラーリング、使用不可化
177

キャッシュ・ヒット

最適化 107

率 107

キュー項目数

最大、計算 176

変更、AIX 177

変更、Windows 177

キュー項目数、設定 176

区画化 61

クラスター化

VMware ESX Server 構成 314

クラスター・サービス

AIX 要件 323

HACMP ES および ESCRM 322

クラスター・サービス、高可用性

システムの依存関係 321

AIX 321

AIX 要件 322

GPFS を備えた PSSP 323

HP-UX の要件 330

MC/Service Guard 330

Solaris 331

Solaris 要件 331

更新

受け取り xxii

更新 (製品更新) xxii

構成 4, 5, 226, 235

ストレージ・サブシステム 6

ストレージ・サブシステム・パスワー
ド 39

タイプ 2

直接接続 2, 6

デバイス 174

デバイス・ドライバ、Linux

DM-Multipath ドライバ 140

ネットワーク 2, 3

ネットワーク設定、iSCSI ホスト接続
45

ネットワークの例 4

ホスト 113

ホット・スベア・ドライバ 87

リカバリー 74

DS TKLM プロキシ・コード、外部
セキュリティ・キー管理 224

DS TKLM プロキシ・コード・サー
バー、始動、停止、および再始動
225

FDE ドライブ 231

GPFS、PSSP、および HACMP クラス
ター 324

HBA 295

構成 (続き)

- IBM i 93
- iSCSI 設定 42
- iSCSI ホスト・ポート 43
- MTU 46
- SAN 接続 2, 6
- 構成タイプ
 - ストレージ・マネージャーのインストール 2
- コピー・サービス 55
- コマンド行インターフェース (CLI) 109
- コメント、スクリプト・エディター 109
- コントローラー
 - アドレス 7
 - ディスク・アレイ 172
 - 転送速度、最適化 106
 - dar 172
 - IP アドレス 7
- コントローラーのキャッシュ・メモリー 98
- コントローラー・ファームウェア
 - ダウンロード 46, 49
 - ファームウェア
 - ダウンロード 49
- コントローラー・ファームウェア・アップグレード・ツール
 - オープン 51
 - 概要 50
 - 使用 51
 - ストレージ・サブシステム、追加 51
 - デバイスのヘルス、確認 50
 - ファームウェアのダウンロード 52
 - ログ・ファイル、表示 52
- コンポーネント、ストレージ・マネージャー・ソフトウェア 2, 34

[サ行]

サービス

- 依頼 xxi
- サービス、提供、米国 IBM 349
- 最小キュー項目数ポリシー 104
- 最小バス重みポリシー 104
- 最大伝送単位
 - 参照: MTU
- サポート
 - 取得 xxi, xxii
 - 通知 xxii
 - マルチパス・ドライバ 127
 - Web サイト xx, xxii
- サポート通知 xxii
 - 受け取り xxii
- 事項、重要 351
- 自動 ESM ファームウェア同期
 - 定義済み 53

- 自動 ESM ファームウェア同期 (automatic ESM firmware synchronization)
 - イベント・モニター要件 53
- 自動ディスクバリー、ストレージ・サブシステムの 37
- 自動ホスト・ディスクバリー 37
- 重要な注意 351
- 手動ディスクバリー 39
- 紹介
 - ストレージ・マネージャー 1
- 障害サポート
 - クラスター・サービス 321
 - 論理ドライブの再配分 181, 182
 - DMP ドライバ 159
 - MPxIO 159
 - RDAC ドライバ 159
- 商標 351
- 資料
 - アクセシビリティ 345
 - 関連資料のリソース xvii
 - 使用 xxi
 - 資料 xix
 - ストレージ・マネージャー xviii
 - 説明 xi
 - 注記 xxii
 - 特記事項 xxii
 - FDE ベスト・プラクティス 261
 - Sun Solaris 159
 - Sun StorEdge 165
 - Symantec 139, 168
 - Veritas 139, 168
 - VMware 317
 - Web サイト xviii, xx
- 診断データ・キャプチャー
 - スクリプト・エディター 286
 - リカバリー手順 287
 - MEL イベント 288
 - Recovery Guru 286, 288
- スイッチ
 - ゾーニング 6
 - テクニカル・サポートの Web サイト xx
 - SAN 接続の構成で 6
- スイッチ環境 130
- スクリプト・エディター
 - ウィンドウ 109
 - 使用 109
- 診断データ・キャプチャー 286
- ストレージの区画化 55, 91
 - およびホスト・グループ 61
- ストレージ・エリア・ネットワーク (SAN)
 - 構成 6
 - テクニカル・サポートの Web サイト xx

ストレージ・サブシステム

- 新しい WWPN のマッピング、AIX および Linux 191
- 外部セキュリティ・キー管理、構成 224
- クラスター・サービス 321
- 構成、外部キー管理 235
- 手動ディスクバリー 39
- 紹介 1
- 使用可能なチューニング・オプション 104
- 初期自動ディスクバリー 37
- 静的 TCP/IP アドレス 9
- チューニング 104, 106, 107, 108
- 追加 175
- パスワードの設定 39
- ファームウェア・レベルの決定 47, 48
- プロファイルの保存 59
- 命名 39
- IP アドレス 7
- VMware ESX Server 構成 313
- ストレージ・サブシステム、外部セキュリティ・キー管理 235
- ストレージ・マネージャー 98, 99
 - アクセシビリティ 345
 - アンインストール 36
 - イベント・ログ 263
 - インストール 36
 - インストール・ウィザード 30
 - インストール・シーケンス 34
 - インターフェース・エレメント 13
 - インターフェース・エレメント、ストレージ・マネージャー 13
- コマンド行インターフェース 109
- コントローラーのアドレスのセットアップ 7
- コントローラー・ファームウェア・アップグレード・ツール
 - ツールの使用 50
- サポートされるオペレーティング・システム 1
- 手動インストール 34, 35
- スクリプト・エディター 109
- 説明 1
- その他の機能 98
- ソフトウェアの取得 xix
- ソフトウェア・コンポーネント 2, 34
- タスク・アシスタント 62
- トラブルシューティング 263
- バージョン 2
- バージョン 10.5x ドライブ・ファームウェアのダウンロード 53
- プレミアム・フィーチャー 55, 94
- 問題、解決 263

ストレージ・マネージャー (続き)
「Enterprise Management (エンタープライズ管理)」ウィンドウ 13
IBM System Storage Productivity Center
で使用するためにインストール xix
Linux、AIX、または Solaris でのアンインストール 36
「Subsystem Management (サブシステム管理)」ウィンドウ 20
Windows でのアンインストール 36
ストレージ・マネージャー ソフトウェア
新しい用語 xi
製品、作成 349
セキュア消去、FDE 220
セキュリティ許可、FDE 221
セキュリティ・キー
作成 209
変更 (外部) 212
変更 (ローカル) 212
FDE ドライブをアンロックするための
使用 246
ID 212
セキュリティ・キー、FDE
参照: FDE
セッション、iSCSI 44
設定値
拡張 HBA 297
変更優先順位 108
メディア・スキャン 102
HBA 295
HBA のデフォルト 296
MTU 46
前提条件
HP-UX
クラスター・サービス、高可用性
330
前提条件、ストレージ・マネージャー・ク
ライアント・ソフトウェア 35
ゾーニング 130
ゾーニング・スイッチ 6
相互接続
VMware ESX Server 317
相互認証許可、入力、iSCSI 43
操作の進行
表示 86
属性
dac 338
dar 338
hdisk 176, 338
LUN 176, 338
その他のよくある質問 261
ソフトウェア
キー・ライセンス管理 207
コントローラーのアドレスのセットア
ップ 7
サービスおよびサポート xxii

ソフトウェア (続き)
ストレージ・マネージャー・コンポー
ネント 2, 34
マルチパス・ドライバ 127
RDAC パッケージ 159
VMware ESX Server の要件 314
ソフトウェア・バージョン、複数
参照: 「Subsystem Management (サブ
システム管理)」ウィンドウ

[タ行]

ターゲット ID の変更、iSCSI 43
ターゲット認証の変更、iSCSI 43
ターゲット・ディスクバリアー、iSCSI の場
合の変更 43
タスク・アシスタント
ショートカット 62
説明 62
注記 xxii
直接接続構成
セットアップ 6
直接接続の構成
IP アドレスの設定 7
ツール
lsslot 188
PCI ホット・プラグ 187
通知
英数字ポケットベル 40
E メール 40
SNMP トラップの使用 40
データ
最適なセグメント・サイズ、選択 108
冗長度 81
ファイル、デフラグ 108
AIX での HBA ホット・スワップの前
の収集 183
FDE による保護 206
ディスクバリアー、自動、ストレージ・サブ
システム 37
ディスク・アクセス、最小化 108
ディスク・アレイ・コントローラー
参照: dac
ディスク・アレイ・ルーター
参照: dar
ディスク・ドライブ
ホット・スベア、構成 87
ホット・スベア、データの復元 87
ホット・スベア、割り当て 87
FDE 206
FDE ホット・スベア 256
FDE、アンロック (外部) 219
FDE、アンロック (ローカルおよび外
部) 246
FDE、アンロック (ローカル) 219
FDE、構成 231

ディスク・ドライブ (続き)
FDE、消去 253
FDE、セキュア消去 220
FDE、取り付け 231
FDE、マイグレーション 249
ディスク・プール
作成 79
デバイス
アラート通知の設定 40
構成 174
識別 170, 172
追加 39
デバイス固有モジュール
参照: DSM
デバイス・ドライバ
最新バージョンのダウンロード xi,
xix
説明 127
フェイルオーバー 127
マルチパス 127
インストール 132
DMP のインストール 168
HACMP クラスターを使用する 323
HBA 135, 136
Linux DM-Multipath ドライバ 140
RDAC 127, 159
SCSIport ミニポート 136
Solaris の RDAC フェイルオーバー・
ドライバ 165
Storport ミニポート 135
Veritas DMP DSM 139
デフォルト・ホスト・タイプの定義と確認
88
転送速度 104
統計、iSCSI 44
動的容量拡張
参照: DCE
動的論理ドライブ拡張
参照: DVE
特記事項 xxii
一般 349
ドライバ xix
rpaphp 187
参照: デバイス・ドライバ
ドライブ
参照: ディスク・ドライブ
ドライブ・ファームウェア
ダウンロード 53
レベルの決定 47, 48
トラブルシューティング 263
重大イベント 263
診断データ・キャプチャー 286

[ナ行]

名前、ストレージ・サブシステム 39

入出力
 アクセス・パターン 107
 書き込みキャッシュ 107
 サイズ 107
 要求速度、最適化 106
入出力アクセス・パターンおよび入出力サ
 イズ 107
入出力アクティビティ、モニター 127
入出力データ・フィールド 104, 106
入出力転送速度、最適化 106
入出力要求速度
 最適化 106
ネットワーク
 一般的な構成 3
 構成の例 4
 iSCSI 設定 45
ネットワーク管理、セットアップ 4
ネットワーク管理構成 4
ネットワーク・インストールの準備 3

[ハ行]

ハードウェア
 イーサネット・アドレス 5
 サービスおよびサポート xxii
 VMware ESX Server の要件 315
ハードウェア・イニシエーター、
 iSCSI 44
パスワード、設定 39
バックグラウンド・メディア・スキャン
 99
パッケージ、ストレージ・マネージャー・
 ソフトウェア 2, 34
パフォーマンス
 ODM 属性設定および 176
パフォーマンス読み取りキャッシュ
 使用 97
パフォーマンス・モニター 104
パリティ 81
ファームウェア
 コントローラー xix
 取得 xix
 ストレージ・マネージャーでのサポー
 ト 2
 ダウンロード 46, 52
 入出力と同時のダウンロード 53
 バージョン 2
 レベルの決定 47, 48
ファイバー・チャンネル
 スイッチ環境での HBA 130
ファイバー・チャンネル入出力
 キャッシュ・ヒット率 107
 ロード・バランシング 106
ファイバー・チャンネル・スイッチ・ゾーニ
 ング 130
ファイル、デフラグ 108

ファブリック・スイッチ環境 130
フィーチャー
 Fast!UTIL 295
フィーチャー、プレミアム
 参照: プレミアム・フィーチャー
フィーチャー使用可能化 ID 56
フィーチャー・キーのファイル 57
フェイルオーバー・ドライバー
 説明 127
 MPxIO 160
フェイルオーバー・モード
 自動ボリューム転送 115
 非対称論理装置アクセス (Asymmetric
 Logical Unit Access) 115
 RDAC フェイルオーバー 115
フル・ディスク暗号化
 参照: FDE
プレミアム・フィーチャー 55, 96
 キー 96, 97
 構成 94
 使用 94
 使用可能化 57, 58
 使用不可化 59
 ストレージの区画化 61, 90, 91
 説明 55
 フィーチャー使用可能化 ID 56
 フィーチャー・キーのファイル 57
 フル・ディスク暗号化
 参照: FDE
 リモート・ミラー・オプション 96
 FDE 205
 FDE および FlashCopy 260
 FDE および VolumeCopy 260
 FDE、使用可能化 232
 FlashCopy 95
 VolumeCopy 96
プロキシー、AIX または Linux でのイン
 ストール 230
プロキシー、Windows でのアンインスト
 ール 230
プロキシー、Windows でのインストール
 229
プロキシー構成ファイルの変更、外部セキ
 ュリティー・キー管理 226
プロファイル、ストレージ・サブシステム
 59
並行ファームウェア・ダウンロード 46,
 53
ヘッド・スワップ、FDE ストレージ・サ
 ブシステム 249
ヘルプ
 取得 xxi, xxii
 Web サイト xx
ヘルプ、オンライン xviii
ホスト xi
 異機種 91

ホスト (続き)
 構成 113
 自動ディスカバリー 37
 手動ディスカバリー 39
 定義 91
 プリインストール・タスク 5
 AIX、デバイス 172
 IBM i 93, 94
 iSCSI 45
 VMware ESX Server 314
ホスト・エージェント管理、セットアップ
 5
ホスト・エージェント管理構成 5
ホスト・エージェント管理方式
 UTM デバイス 172
ホスト・エージェント・ソフトウェア
 停止と再開 175
ホスト・グループ
 定義 61, 90
ホスト・コンピューター
 参照: ホスト
ホスト・タイプ
 確認 88
 デフォルトの定義 88
ホスト・バス・アダプター
 HBA
 ホスト・ポートの設定 61
 Solaris
 QLogic 設定値 310
 参照: HBA
ホスト・ポート
 定義 91
ホスト・ポート、iSCSI 43
ホット・スベア
 FDE ディスク・ドライブ 256
ホット・スベア・ドライブ 87
ホット・スワップ HBA
 参照: HBA、ホット・スワップ
ポリシー、ロード・バランシング
 最小キュー項目数ポリシー 104
 最小パス重みポリシー 104
 ラウンドロビン・ポリシー 104

[マ行]

マルチパス 46, 132, 159
 固有、HP-UX 158
 AIX での論理ドライブの再配分 181
 DMP、Solaris でのインストール 168
 HP-UX での論理ドライブの再配分
 182
 MPxIO、Solaris とともに使用 159
 PV-links、HP-UX での使用 154, 155,
 156
 Solaris での論理ドライブの再配分
 182

マルチパス (続き)

Solaris の RDAC フェイルオーバー・
ドライバ 165

マルチパス・ドライバ 115, 139, 149,
154, 170

インストール 132

説明 127

フェイルオーバー 115

マルチメディア・アプリケーション 83

マルチユーザー環境 83

ミニハブ 6

メディア・アクセス制御 (MAC) アドレス
参照: MAC アドレス

メディア・スキャン 99

概要 99

期間 103

設定値 102

設定の変更 99

パフォーマンスへの影響 101

報告されるエラー 101

問題、解決 263

問題解決、重大イベント 263

[ヤ行]

ユーティリティ

hot_add 174

SMdevices 171

SMrepassist 174

ユニバーサル・トランスポート・メカニズ
ム

参照: UTM デバイス

要件

オペレーティング・システム 30

ストレージ・マネージャー・クライア
ント・ソフトウェア 35

HP-UX

クラスター・サービス、高可用性
330

用語 xi

用語、FDE 223

用語集 353

よくある質問、その他 261

[ラ行]

ラウンドロビン・ポリシー 104

リソース

資料 xix

リモート・ブート

参照: SAN ブート

リモート・ミラー・オプション 96

ローカル・セキュリティ・キー管理
209, 212, 219

ロード・バランシング 333

ログ・ファイル 263

主要イベント・ログ 257

セキュリティ変更 257

論理ドライバ 6, 335

空きまたは未構成の容量からの作成
81

構成 84

再配分 181, 182

作成 74, 84, 85

識別 170

定義 74

変更優先順位の設定 108

予想される用途 85

[ワ行]

ワールドワイド・ポート名

参照: WWPN

A

ADT 182

AIX 139

エラー・ログ 289

オブジェクト・データ・マネージャー
(ODM) 属性

定義 333

表示および設定 333

dac デバイス 333

dar デバイス 333

hdisk デバイス 333

lsattr コマンド 338

クラスター・サービス 321

ストレージ・サブシステムへの新しい
WWPN のマッピング 191

ホット・スワップ HBA、交換 185

論理ドライバ、再配分 181

FCP ディスク・アレイ・エラー 289

HBA ホット・スワップ、完了 191

HBA ホット・スワップ、準備 183

AIX ホスト

サポート xx

AIX マルチパス・ドライバ 139

autorecovery

AIX での HBA ホット・スワップの前
の使用不可状態の確認 183

B

BIOS

設定値 295

BOOTP サーバ

サンプル・ネットワーク 4, 7

C

CHAP 43

D

dac

および RDAC 172

属性 338

dar

および RDAC 172

属性 338

DCE 177

DDC

参照: 診断データ・キャプチャ

「Devices (デバイス)」タブ

参照: 「Enterprise Management (エン
タープライズ管理)」ウィンドウ

DHCP サーバ

サンプル・ネットワーク 4, 7

DHCP、使用 44

DMP 159

インストールの計画 168

インストールの準備 168

DMP DSM ドライバ 139

DMP ドライバ 154

DS TKLM プロキシー・コード、外部セ
キュリティ・キー管理 229

DS TKLM プロキシー・コード、構成、
外部セキュリティ・キー管理 235

DS TKLM プロキシー・コード・サーバ
ー、再始動 225

DS TKLM プロキシー・コード・サーバ
ー、サポートされるオペレーティング・
システム 224

DSM 132

DVE 177

Dynamic Multipathing (DMP)

説明 159

参照: DMP

E

「Enterprise Management (エンタープライ
ズ管理)」ウィンドウ

アラート通知 40

エレメント 13

オンライン・ヘルプ xviii

装置の追加 39

ツリー・ビューの説明 15

テーブル・ビューの説明 15

「Devices (デバイス)」タブ 15

「Setup (セットアップ)」タブ 19

ESM ファームウェア

- 自動 ESM ファームウェア同期 (automatic ESM firmware synchronization) 53
- 自動 ESM ファームウェア・ダウンロード 52
- ダウンロード 46, 52
- レベルの決定 47, 48

F

- Fast!UTIL 295
- FCP ディスク・アレイ・エラー 289
- FC/SATA 混合使用プレミアム・フィチャー 55
- FDE 97, 205
 - アレイ、セキュア化 258
 - 外部セキュリティ・キー管理 207, 259
 - キー管理方式、選択 207
 - 使用可能化 232
 - 状態、ロックおよびアンロック 261
 - 侵害に対するデータの保護 206
 - セキュア消去 259
 - セキュア消去、使用 220
 - セキュア・ドライブ、アンロック (外部) 219
 - セキュア・ドライブ、アンロック (ローカル) 219
 - セキュリティ許可 221
 - セキュリティ・キー
 - 作成 208
 - 取得 208
 - 使用 208
 - セキュリティ・キー ID 212
 - セキュリティ・キー、作成 209
 - セキュリティ・キー、取得 208
 - セキュリティ・キー、変更 (外部) 212
 - セキュリティ・キー、変更 (ローカル) 212
 - セキュリティ・キー管理、FDE 207
 - 他のプレミアム・フィチャーとの使用 260
 - ディスク・ドライブ 206
 - ディスク・ドライブ、アンロック (ローカルおよび外部) 246
 - ディスク・ドライブ、構成 231
 - ディスク・ドライブ、消去 253
 - ディスク・ドライブ、取り付け 231
 - ディスク・ドライブ、マイグレーション 249
 - バックアップおよびリカバリー 261
 - ブート・サポート 261
 - ベスト・プラクティス 261

FDE (続き)

- ホット・スベア・ディスク・ドライブ 256
- ホット・スベア・ドライブ 260
- 用語 223
- よくある質問 258
- 理解 206
- ローカル・セキュリティ・キー管理 207, 259
- ログ・ファイル 257
- RAID アレイ、セキュア化 240
- FlashCopy 95
 - ディスク・アレイのエラー・メッセージ (AIX) 290, 291
- Enhanced 94

G

- General Parallel File System (GPFS) 323
- GPFS 323

H

- HACMP 322
 - 使用 323
 - 「Hardware (ハードウェア)」タブ
 - 参照：「Subsystem Management (サブシステム管理)」ウィンドウ
- HBA
 - 概要 130
 - 拡張設定 297
 - 使用 130
 - 設定値 295
 - 直接接続の構成で 6
 - デバイス・ドライバ 135, 136
 - デフォルトの設定値 296
 - ファイバー・チャンネル・スイッチ環境 130
 - ファイバー・チャンネル・スイッチ環境の接続 130
 - ホット・スワップ、完了 191
 - ホット・スワップ、交換 183
 - ホット・スワップ、交換、AIX および Linux 185
 - ホット・スワップ、AIX での交換 183
 - JNI 設定値 305
 - Linux でのホット・スワップ、準備 187
 - Linux、交換 187
 - PCI ホット・プラグ、交換 190
 - QLogic 設定値 298, 310
 - SAN 接続の構成で 6
 - Solaris での JNI 設定値 305

hdisk

- キュー項目数、設定 176
- 検証 172
- 属性 176, 338
- High Availability Cluster Multi-Processing
 - 参照：HACMP
- 「Host Mappings (ホスト・マッピング)」タブ
 - 参照：「Subsystem Management (サブシステム管理)」ウィンドウ
- hot_add ユーティリティ 174
- HP-UX
 - クラスター・サービス、高可用性の要件 330
 - 固有のマルチパス 158
 - 論理ドライブ、再配分 182
 - PV-links 154, 155, 156
 - PV-links を使用するマルチパス入出力 154, 155, 156

I

- IBM i
 - 構成 93
 - ポート ID 93
 - ホスト・タイプとしての定義 94
- IBM Power Systems 93
- IBM System Storage Productivity Center xix
- IBM System Storage コントローラー・ファームウェア・アップグレード・ツール
 - 参照：コントローラー・ファームウェア・アップグレード・ツール
- IBM Tivoli Key Lifecycle Manager 207, 235
 - 外部セキュリティ・キー管理、構成 224
- DS TKLM プロキシ・コード、インストール 229
- DS TKLM プロキシ・コード、構成 235
- DS TKLM プロキシ・コード・サーバーの構成ファイル、変更 226
- IBM サポート・ライン xxii
- Intel および AMD ベースのホストサポート xx
- IP アドレス 7
- IPv6 45
- IPv6 45
- iSCSI
 - サポートされるハードウェア・イニシエーター、使用 44
 - セッション、表示または終了 44
 - 設定、管理 42
 - 相互認証許可、入力 43

iSCSI (続き)

- ソフトウェア・イニシエーターの考慮事項、Microsoft 46
- ターゲット ID、変更 43
- ターゲット認証、変更 43
- ターゲット・ディスカバリー、変更 43
- 統計、表示 44
- ネットワーク設定 45
- ホスト・ポート 42
- ホスト・ポート、構成 43
- iSNS サーバー、使用 44
- iSNS サーバー、使用 44

J

JNI

- HBA の設定 305
- Solaris での HBA 設定値 305

L

Linux

- 交換、HBA 187
- ストレージ・サブシステムへの新しい WWPN のマッピング 191
- ホット・スワップ HBA、交換 185
- DCE 177
- DVE 177
- HBA ホット・スワップ、完了 191
- HBA、ホット・スワップの準備 187
- RHEL 5.3、Veritas Storage Foundation 5.0 179
- SUSE、Veritas Storage Foundation 178
- Linux DM-Multipath ドライバー 140
- Linux MPP ドライバー 149
- Linux ホスト
 - サポート xx
- load_balancing 属性 333, 334
- LockKeyID、FDE 212
- lsslot ツール 188
- LUN
 - 既存の区画への追加 92
 - 区画へのマッピング、VMware ESX Server 318
 - サイズの確認 180
 - 新規区画へのマッピング 92
 - 属性 176, 338

M

- MAC OS 154
- MAC アドレス
 - 識別 8
- MC/Service Guard 330

MEL

- セキュリティ変更 257
- Microsoft iSCSI ソフトウェア・イニシエーター 46
- Microsoft Windows MPIO 132
- Microsoft Windows MPIO/DSM 132
- MPIO 173
- MPP ドライバー 149
- MPxIO 159
 - 最新のドライバー・バージョン、獲得 160
 - デバイス、検証 160
 - デバイス名、変更 160
 - ドライバー、使用不可化 165
 - フェイルオーバー・ドライバー、使用可能化 160
 - フェイルオーバー・パス、構成 160
 - フェイルオーバー・パス、構成解除 160
- MTU
 - 設定値 46
- Multiplexed I/O (MPxIO)
 - 参照： MPxIO
- My Support (マイ・サポート) xxii

N

- NVSRAM ファームウェア
 - ダウンロード 46, 49

P

- Parallel System Support Program (PSSP) 323
- PCI コア 187
- PCI スロット情報 188
- PCI ホット・プラグ 188
- PCI ホット・プラグ HBA 190
- PCI ホット・プラグ・ツール 187
- PSSP 323
- PV-links
 - 参照： HP-UX

Q

- QLogic
 - 設定値 310
 - HBA の設定 295, 298, 305, 310
- QLogic SANsurfer xviii

R

- RAID
 - アプリケーションの動作、レベル別 107

RAID (続き)

- アレイのセキュア化、FDE を使用 240
 - データの冗長性 81
 - レベル 81
 - レベルの選択 107
 - RAID レベル
 - アプリケーションの動作 83
 - 構成 82
 - 選択 83
 - RAID-0
 - 説明 82
 - ドライブ障害の結果 82
 - RAID-1
 - 説明 82
 - ドライブ障害の結果 82
 - RAID-3
 - 説明 83
 - ドライブ障害の結果 83
 - RAID-5
 - 説明 83
 - ドライブ障害の結果 83
 - RAID-6
 - 二重分散パリティ 83
 - RDAC
 - ID、クラスター・サービス 331
 - ID、追加 331
 - RDAC ドライバー
 - 構成ファイル、変更 165
 - 説明 127, 159
 - Solaris、インストール 165
 - README
 - ファイルの取得 xix
 - Recovery Guru
 - 診断データ・キャプチャー 286
- ## S
- SAN 接続の構成
 - セットアップ 6
 - SAN ブート
 - ホストの構成 113
 - 要件 113
 - SCSIport ミニポート 136, 139
 - 「Setup (セットアップ)」タブ
 - 「Enterprise Management (エンタープライズ管理)」ウィンドウ 19
 - 「Subsystem Management (サブシステム管理)」ウィンドウ 27
 - Simple Network Management Protocol (SNMP) トラップ
 - SNMP トラップ 4
 - 参照： SNMP トラップ
 - SMagent
 - ソフトウェア・インストール・シーケンス 34

SMclient
ソフトウェア・インストール・シーケ
ンス 34

SMdevices ユーティリティー
使用 171
UNIX タイプのオペレーティング・シ
ステム 171
Windows 171

SMrepassist ユーティリティー 174

SMruntime
ソフトウェア・インストール・シーケ
ンス 34

SMutil
ソフトウェア・インストール・シーケ
ンス 34

SNMP トラップ 4, 7, 40

Solaris
クラスター・サービス、高可用性 331
クラスター・サービスの要件 331
論理ドライブ、再配分 182
Veritas 168

SSPC xx

SSPC (System Storage Productivity
Center) xix
「Storage and Copy Services (ストレージ
およびコピー・サービス)」タブ
参照：「Subsystem Management (サブ
システム管理)」ウィンドウ

Storport ミニポート 135
「Subsystem Management (サブシステム管
理)」ウィンドウ
イベント・ログ 263
エレメント 20, 21
オープン 21
オンライン・ヘルプ xviii
複数のソフトウェア・バージョン 27
「Hardware (ハードウェア)」タブ 27
「Host Mappings (ホスト・マッピン
グ)」タブ 25
「Setup (セットアップ)」タブ 27
「Storage and Copy Services (ストレ
ージおよびコピー・サービス)」タブ
22
「Summary (要約)」タブ 21
「Summary (要約)」タブ
参照：「Subsystem Management (サブ
システム管理)」ウィンドウ

System p ホスト
サポート xx

System Storage Interoperation Center
(SSIC) xx

System Storage Productivity Center xix

System Storage Productivity Center
(SSPC) xx

System x ホスト
サポート xx

T

TCP/IP
IPv6 45

TCP/IP アドレス、静的
ストレージ・サブシステムへの割り当
て 9

Tivoli Key Lifecycle Manager
参照：IBM Tivoli Key Lifecycle
Manager

TKLM
参照：IBM Tivoli Key Lifecycle
Manager

U

UTM デバイス 172

V

VDS/VSS プロバイダー 341

Veritas 139
DMP 168
Dynamic Multipathing (DMP) 159
File System 168
Storage Foundation 178
Storage Foundation 5.0 179
VolumeManager 159, 168

Veritas DMP DSM 139

Veritas DMP ドライバー 154

Veritas Storage Foundation
LVM スキャン、SUSE Linux
Enterprise Server での使用不可化
178
RDAC モジュール、Storage Foundation
5.0 の場合の RHEL での使用可能化
179

Veritas Storage Foundation 5.0
RDAC モジュール、アンロード 179
RDAC モジュール、使用可能化 179

VMware ESX Server 313
相互接続 317
LUN の区画へのマッピング 318

VolumeCopy 96

W

Web サイト
サービス xxii
サポート xxii
資料 xviii
スイッチ・サポート xx
通知 xxii
プレミアム・フィーチャーの活動化
xx

Web サイト (続き)
リスト xx
AIX xx
FDE ベスト・プラクティス 261
IBM Publications Center xxi
IBM System Storage 製品情報 xxi
SAN サポート xx
Solaris フェイルオーバー・ドライバ
168
SSIC xx
System p xx
System Storage Productivity Center
(SSPC) xx
System x xx
VMware 317

WWPN
ストレージ・サブシステムへのマッピ
ング、AIX および Linux 191



Printed in Japan

GA88-4765-01



日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21