

# vSphere のストレージ

Update 1

変更日：2022 年 4 月 19 日

VMware vSphere 6.0

VMware ESXi 6.0

vCenter Server 6.0

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>)

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

**ヴィエムウェア株式会社**  
〒108-0023 東京都港区芝浦 3-1-1  
田町ステーションタワー N 18 階  
[www.vmware.com/jp](http://www.vmware.com/jp)

Copyright © 2009-2022 VMware, Inc. All rights reserved. 著作権および商標情報。

# 目次

vSphere Storage について 13

更新情報 14

## 1 ストレージの概要 15

ストレージ仮想化 15

物理ストレージのタイプ 16

ローカル ストレージ 16

ネットワーク ストレージ 17

ターゲットとデバイスの表現 20

ストレージ デバイスの特徴 21

ホストのストレージ デバイスの表示 22

アダプタのストレージ デバイスの表示 23

サポート対象のストレージ アダプタ 23

ストレージ アダプタの特徴 23

ストレージ アダプタ情報の表示 24

データストアの特性 24

データストア情報の表示 26

インフラストラクチャ オブジェクトのデータストアを一覧表示する 27

仮想マシンからストレージへのアクセス方法 28

ストレージのタイプの比較 28

## 2 ESXi と SAN の併用の概要 30

ESXi と SAN の使用例 31

SAN ストレージを ESXi と併用する場合の特性 31

ESXi ホストと複数のストレージ アレイ 32

LUN の決定 32

予測型スキームを使用した LUN の決定 33

適合型スキームを使用した LUN の決定 33

仮想マシンの場所の選定 34

レイヤー化されたアプリケーション 34

アレイ ベース (サードパーティ) のソリューション 35

ファイル ベース (VMFS) のソリューション 35

サードパーティ製の管理アプリケーション 36

SAN ストレージ バックアップに関する考慮事項 36

サードパーティ製のバックアップ パッケージの使用 37

## 3 ESXi とファイバ チャネル SAN との併用 38

ファイバ チャンネル SAN の概念	38
ファイバ チャンネル SAN のポート	39
ファイバ チャンネル ストレージ アレイのタイプ	39
ゾーニングとファイバ チャンネル SAN との併用	40
仮想マシンからファイバ チャンネル SAN 上のデータへのアクセス方法	40

## 4 ファイバ チャンネル ストレージの構成 42

ESXi ファイバ チャンネル SAN の要件	42
ESXi ファイバ チャンネル SAN の制限	43
LUN 割り当ての設定	43
ファイバ チャンネル HBA の設定	43
インストールおよびセットアップの手順	44
N-Port ID の仮想化	44
NPIV ベースの LUN アクセスの作動方法	44
NPIV 使用の要件	45
NPIV の機能と制限事項	46
仮想マシンへの WWN の割り当て	46
WWN 割り当ての変更	47

## 5 ファイバ チャンネル オーバー イーサネットの構成 48

ファイバ チャンネル オーバー イーサネット アダプタ	48
ソフトウェア FCoE の構成ガイドライン	49
ソフトウェア FCoE 用のネットワークの設定	50
ソフトウェア FCoE アダプタの追加	50

## 6 ファイバ チャンネル SAN からの ESXi の起動 52

SAN から起動のメリット	52
ファイバ チャンネル SAN からの起動の要件と考慮事項	53
SAN から起動するための準備	53
SAN コンポーネントとストレージ システムの構成	54
SAN から起動するストレージ アダプタの構成	54
インストール メディアから起動するためのシステムの設定	54
SAN から起動する Emulex HBA の構成	55
BootBIOS プロンプトの有効化	55
BIOS の有効化	55
SAN から起動する QLogic HBA の構成	56

## 7 ソフトウェア FCoE による ESXi のブート 58

ソフトウェア FCoE 起動の要件と考慮事項	58
ソフトウェア FCoE ブートのベスト プラクティス	59
ソフトウェア FCoE ブートの設定	59

- ソフトウェア FCoE ブート パラメータの構成 60
- ソフトウェア FCoE LUN からの ESXi のインストールと起動 60
- ソフトウェア FCoE からのインストールおよび起動のトラブルシューティング 61

## 8 ファイバ チャンネル ストレージのベスト プラクティス 62

- ファイバ チャンネル SAN の問題の防止 62
- 自動ホスト登録の無効化 63
- ファイバ チャンネル SAN ストレージ パフォーマンスの最適化 63
  - ストレージ アレイ パフォーマンス 64
  - ファイバ チャンネルによるサーバ パフォーマンス 64

## 9 iSCSI SAN と ESXi との併用 66

- iSCSI SAN の概念 66
  - iSCSI SAN のポート 67
  - iSCSI 命名規則 67
  - iSCSI イニシエータ 68
  - iSCSI 接続の確立 69
  - iSCSI ストレージ システムのタイプ 69
  - 検出、認証、およびアクセス コントロール 70
  - エラー訂正 71
- 仮想マシンから iSCSI SAN 上のデータへのアクセス方法 72

## 10 iSCSI アダプタおよびストレージの構成 73

- ESXi iSCSI SAN の要件 74
- ESXi iSCSI SAN の制限 74
- iSCSI の LUN 割り当ての設定 74
- ネットワーク構成と認証 75
- 独立型ハードウェア iSCSI アダプタの設定 75
  - 独立型ハードウェア iSCSI アダプタの表示 76
  - iSCSI アダプタの全般プロパティの変更 77
  - ハードウェア iSCSI のネットワーク設定の編集 77
  - iSCSI の動的または静的検出の設定 78
- 依存型ハードウェア iSCSI アダプタについて 79
  - 依存型ハードウェア iSCSI に関する考慮事項 79
  - 依存型ハードウェア iSCSI アダプタの構成 80
- ソフトウェア iSCSI アダプタについて 87
  - ソフトウェア iSCSI アダプタの構成 87
  - ソフトウェア iSCSI アダプタの無効化 94
- iSCSI アダプタの全般プロパティの変更 95
- iSCSI ネットワークの設定 96
  - ESXi で iSCSI ポート バインドを使用する際のガイドライン 99

iSCSI のネットワーク接続の作成	99
iSCSI ネットワークの管理	103
iSCSI ネットワークのトラブルシューティング	104
iSCSI でのジャンボ フレームの使用	104
ソフトウェア iSCSI と依存型ハードウェア iSCSI でのジャンボ フレームの有効化	105
独立型のハードウェア iSCSI のジャンボ フレームの有効化	105
iSCSI アダプタの検出アドレスの構成	106
iSCSI の動的または静的検出の設定	106
動的および静的 iSCSI ターゲットの削除	107
iSCSI アダプタの CHAP パラメータの構成	107
CHAP 認証方法の選択	108
iSCSI アダプタの CHAP の設定	109
ターゲットの CHAP の設定	110
CHAP の無効化	111
iSCSI 詳細パラメータの構成	112
iSCSI の詳細パラメータの構成	113
iSCSI セッションの管理	113
iSCSI セッションの確認	114
iSCSI セッションの追加	115
iSCSI セッションの削除	115

## 11 iSCSI SAN からの起動 117

iSCSI SAN からの起動に関する一般的推奨事項	117
iSCSI SAN の準備	118
SAN 起動のための独立型ハードウェア iSCSI アダプタの構成	119
iSCSI 起動設定の構成	119
iBFT iSCSI 起動の概要	120
iBFT iSCSI 起動に関する検討事項	121
SAN からの iBFT 起動の構成	121
ネットワークのベスト プラクティス	123
iBFT iSCSI 起動設定の変更	124
iBFT iSCSI 起動のトラブルシューティング	124

## 12 iSCSI ストレージのベスト プラクティス 126

iSCSI SAN の問題の防止	126
iSCSI SAN ストレージ パフォーマンスの最適化	127
ストレージ システムのパフォーマンス	127
iSCSI でのサーバ パフォーマンス	127
ネットワーク パフォーマンス	128
イーサネット スイッチ統計情報の確認	131

## 13 ストレージ デバイスの管理 132

- ストレージ デバイスの特徴 132
  - ホストのストレージ デバイスの表示 133
  - アダプタのストレージ デバイスの表示 134
- ストレージ デバイスの命名について 134
  - ストレージ デバイスの名前の変更 135
- ストレージの更新操作および再スキャン操作 136
  - ストレージの再スキャンの実行 136
  - アダプタの再スキャンの実行 137
  - スキャンするストレージ デバイスの数の変更 137
- デバイス接続問題の確認 138
  - PDL 状態の検出 138
  - 予定されるストレージ デバイスの削除の実行 139
  - PDL 状態からのリカバリ 141
  - 一時的な APD 状態の処理 141
  - ストレージ デバイスの接続状態の確認 143
  - デバイスの接続問題と高可用性 144
- ストレージ デバイスのロケータ LED の有効化または無効化 144

## 14 フラッシュ デバイスの操作 145

- vSphere でのフラッシュ デバイスの使用 145
  - フラッシュ仮想ディスクの特定 146
- ストレージ デバイスのマーク 147
  - ストレージ デバイスをフラッシュとしてマーク 147
  - ストレージ デバイスをローカルとしてマーク 148
- フラッシュ デバイスの監視 148
- フラッシュ デバイスのベスト プラクティス 149
  - フラッシュ デバイスの有効期間の推定 149
- 仮想フラッシュ リソースについて 150
  - 仮想フラッシュ リソースの考慮事項 150
  - 仮想フラッシュ リソースの設定 151
  - 仮想フラッシュ リソースの削除 151
  - 仮想フラッシュの詳細設定 152
- ホスト スワップ キャッシュの構成 152
  - VMFS データストアによるホスト キャッシュの構成 153
  - 仮想フラッシュ リソースを使用したホスト スワップ キャッシュの構成 153

## 15 VMware vSphere Flash Read Cache について 155

- フラッシュ読み取りキャッシュの DRS サポート 156
- vSphere High Availability のフラッシュ読み取りキャッシュのサポート 156
- 仮想マシンの Flash Read Cache を構成 156

Flash Read Cache とともに仮想マシンを移行 157

## 16 データストアでの作業 159

VMFS データストアについて 160

VMFS5 データストアの特性 161

VMFS データストアとストレージ ディスク フォーマット 161

VMFS データストアとリポジトリ 162

ホスト間の VMFS データストアの共有 162

VMFS メタデータ アップデート 163

VMFS のロック メカニズム 164

ネットワーク ファイル システム データストアについて 168

NFS ストレージのガイドラインと要件 169

NFS プロトコルと ESXi 170

NFS ストレージのファイアウォール構成 172

NFS ストレージにアクセスするためのレイヤー 3 のルート設定された接続 174

NFS ストレージ環境のセットアップ 175

NFS 4.1 用 Kerberos 認証情報の使用 175

データストアの作成 178

VMFS データストアの作成 179

NFS データストアの作成 180

仮想データストアの作成 180

重複 VMFS データストアの管理 181

既存のデータストア署名の保持 182

VMFS データストア コピーの再署名 182

VMFS データストアのアップグレード 183

データストアの VMFS5 へのアップグレード 184

VMFS データストア容量の増加 185

VMFS データストア容量の増加 185

データストアの管理操作 186

データストア名の変更 187

データストアのアンマウント 187

データストアのマウント 188

VMFS データストアの削除 189

データストア ブラウザの使用 189

ストレージ フィルタのオフ 194

動的なディスクミラーリングの設定 195

ストレージ デバイスでの ESXi ホストの診断情報の収集 196

コア ダンプの場所としてのデバイス パーティションの設定 196

コア ダンプの場所としてのファイルの設定 198

VOMA によるメタデータの整合性の確認 200

VMFS ポインタ ブロック キャッシュの構成 202



ホストの詳細属性の設定	203
VMFS ポインタ ブロック キャッシュの情報の取得	203

## 17 マルチパスとフェイルオーバーについて 205

ファイバ チャネルを使用したフェイルオーバー	205
iSCSI でのホスト ベースのフェイルオーバー	206
iSCSI でのアレイ ベースのフェイルオーバー	208
パスのフェイルオーバーと仮想マシン	209
Windows ゲスト OS にタイムアウトを設定	209
複数のパスの管理	210
VMware マルチパス モジュール	211
VMware SATP	212
VMware PSP	212
I/O の VMware NMP フロー	213
パスのスキャンと要求	213
パス情報の表示	214
データストア パスの表示	215
ストレージ デバイス パスの表示	215
パス選択ポリシーの設定	215
パス選択ポリシーの変更	216
ストレージ パスの無効化	217
ストレージ パスおよびマルチパス プラグインの管理	217
マルチパスの考慮事項	217
ホストのマルチパスの要求ルールの一覧表示	218
マルチパス モジュールの表示	219
ホストの SATP の表示	220
NMP ストレージ デバイスの表示	220
マルチパスの要求ルールの追加	221
マルチパスの要求ルールの削除	223
パスのマスク	224
パスのマスク解除	225
NMP SATP ルールの定義	226
仮想マシン I/O のキューのスケジュール設定	228
ファイル I/O ごとのスケジュールの編集	228
esxcli コマンドを使用したファイル I/O ごとのスケジュールの有効化または無効化	228

## 18 Raw デバイス マッピング 230

Raw デバイス マッピングについて	230
Raw デバイス マッピングのメリット	231
RDM の注意事項と制限事項	234
Raw デバイス マッピングの特性	234

- RDM の仮想および物理互換モード 234
- 動的名前解決 235
- 仮想マシン クラスタでの Raw デバイス マッピング 235
- 利用可能な SCSI デバイス アクセス モードの比較 235
- RDM を使用する仮想マシンの作成 236
- マッピング済み LUN のバス管理 237

## 19 仮想ボリュームの操作 239

- Virtual Volumes の概念 240
  - 仮想ボリューム 240
  - 仮想ボリュームとストレージ プロバイダ 241
  - ストレージ コンテナ 242
  - プロトコル エンドポイント 242
  - 仮想データストア 243
  - 仮想ボリュームと仮想マシン ストレージのポリシー 243
- 仮想ボリュームを使用するときのガイドライン 244
- 仮想ボリュームとストレージ プロトコル 244
- Virtual Volumes のアーキテクチャ 245
- 仮想ボリュームと VMware Certificate Authority 247
- 仮想ボリュームを有効化する前に 247
  - ネットワーク タイム サーバによる vSphere のストレージ環境の同期 248
- 仮想ボリュームの構成 248
  - 仮想ボリュームのストレージ プロバイダの登録 249
  - 仮想データストアの作成 250
  - プロトコル エンドポイントの確認と管理 251
  - プロトコル エンドポイントのバス選択ポリシーの変更 251
- 仮想データストア上の仮想マシンのプロビジョニング 252
  - Virtual Volumes の仮想マシン ストレージ ポリシーの定義 252
  - 仮想マシンへの仮想ボリューム ストレージ ポリシーの割り当て 253
  - 仮想データストアのデフォルト ストレージ ポリシーの変更 254

## 20 仮想マシン ストレージ ポリシー 255

- レガシー ストレージ プロファイルのアップグレード 255
- 仮想マシンのストレージ ポリシーについて 256
  - ストレージ ポリシーとルール 257
  - データストア固有および共通のルール セットについて 258
- 仮想マシン ストレージ ポリシーの操作 259
- 仮想マシン ストレージ ポリシーの作成と管理 259
  - データストアへのタグの割り当て 260
  - 仮想マシンのストレージ ポリシーの定義 261
  - 仮想マシン ストレージ ポリシーの削除 264

仮想マシン ストレージ ポリシーの編集またはクローン作成	264
ストレージ ポリシーと仮想マシン	265
デフォルト ストレージ ポリシー	265
仮想マシンへのストレージ ポリシーの割り当て	267
仮想マシンのファイルとディスク用ストレージ ポリシー割り当ての変更	268
仮想マシンのストレージ コンプライアンスの監視	269
仮想マシン ストレージ ポリシーのコンプライアンスの確認	270
互換性のない仮想マシン向けの互換性のあるストレージ リソースの検索	271
仮想マシン ストレージ ポリシーの再適用	272

## 21 仮想マシン I/O のフィルタリング 273

I/O フィルタについて	273
I/O フィルタのタイプ	273
I/O フィルタリング コンポーネント	274
VAIO フィルタのストレージ プロバイダ	275
フラッシュ ストレージ デバイスとキャッシュ I/O フィルタの併用	276
vSphere 環境での I/O フィルタのデプロイと構成	277
クラスタでの I/O フィルタのインストール	278
I/O フィルタのストレージ プロバイダの表示	278
I/O フィルタの機能の確認	278
キャッシュ I/O フィルタの仮想フラッシュ リソースの構成	279
仮想ディスクでの I/O フィルタ データ サービスの有効化	279
I/O フィルタの管理	282
クラスタからの I/O フィルタのアンインストール	283
クラスタでの I/O フィルタのアップグレード	283
I/O フィルタのガイドラインおよびベスト プラクティス	284
I/O フィルタによる仮想マシンの移行	285

## 22 VMkernel とストレージ 286

Storage API	287
-------------	-----

## 23 ストレージのハードウェア アクセラレーション 289

ハードウェア アクセラレーションのメリット	289
ハードウェア アクセラレーションの要件	290
ハードウェア アクセラレーションのサポート ステータス	290
ブロック ストレージ デバイスのハードウェア アクセラレーション	290
ブロック ストレージ デバイスのハードウェア アクセラレーションの無効化	291
ブロック ストレージ デバイスでのハードウェア アクセラレーションの管理	291
NAS デバイスでのハードウェア アクセラレーション	296
NAS プラグインのインストール	297
NAS プラグインのアンインストール	298

NAS プラグインの更新 298

NAS のハードウェア アクセラレーション ステータスの検証 299

ハードウェア アクセラレーションについての考慮事項 300

## 24 ストレージ シック プロビジョニングとストレージ シン プロビジョニング 301

ストレージ オーバーサブスクリプション 301

仮想ディスク シン プロビジョニング 301

仮想ディスクのプロビジョニング ポリシーについて 302

シン プロビジョニング仮想ディスクの作成 303

仮想マシン ストレージ リソースの表示 304

仮想マシンのディスク フォーマットの判別 304

シン仮想ディスクの拡張 305

データストアのオーバーサブスクリプションの処理 305

アレイ シン プロビジョニングおよび VMFS データストア 306

領域使用の監視 306

シン プロビジョニング ストレージ デバイスの識別 307

蓄積されたストレージ領域の再要求 308

## 25 ストレージ プロバイダの使用 310

ストレージ プロバイダおよびストレージ データの表現 311

ストレージ プロバイダの要件および考慮事項 311

ストレージ ステータス レポート 312

ストレージ プロバイダの登録 312

ストレージ プロバイダとの通信のセキュリティ強化 313

ストレージ プロバイダ情報の表示 313

ストレージ プロバイダの登録解除 314

ストレージ プロバイダの更新 314

## 26 vmkfstools の使用 315

vmkfstools コマンドの構文 315

vmkfstools オプション 316

-v サブオプション 316

ファイル システムのオプション 317

仮想ディスクのオプション 319

ストレージ デバイス オプション 326

# vSphere Storage について

vSphere Storage では、VMware® ESXi で使用可能なストレージ オプションについて、およびさまざまなタイプのストレージを使用および管理できるように ESXi システムを構成する方法を説明します。さらに、vSphere Storage では、ストレージ オプションとしてファイバ チャネル® および iSCSI ストレージ エリア ネットワーク (SAN) を重点的に取り上げ、ファイバ チャネルおよび iSCSI 環境で ESXi を使用する際の具体的な項目について説明します。

## 対象読者

本書は、仮想マシン テクノロジー、データセンターの運用、SAN ストレージの概念に詳しいシステム管理者としての経験をお持ちのユーザーを対象としています。

# 更新情報

『vSphere ストレージ』は、製品のリリースごとに、または必要に応じて更新されます。

『vSphere ストレージ』の更新履歴については、次の表をご確認ください。

リビジョン	説明
2022 年 4 月 19 日	マイナー改訂。
2020 年 8 月 15 日	VMware では、多様性の受け入れを尊重しています。弊社のお客様、パートナー、内部コミュニティにおいてこの原則を推進するため、弊社のコンテンツに含まれている用語の見直しを行っています。不適切な表現を削除するため、このガイドを更新しました。
2019 年 6 月 27 日	マイナー改訂。
2018 年 11 月 27 日	マイナー改訂。
2018 年 7 月 12 日	マイナー改訂。
2018 年 4 月 18 日	マイナー改訂。
2018 年 3 月 20 日	マイナー改訂。
2018 年 2 月 14 日	マイナー改訂。
JP-001799-07	<a href="#">データストア フォルダまたはファイルのコピー</a> ：データストア ブラウザが vCenter Server 間での仮想マシン ファイルのコピーをサポートしないことを記載。
JP-001799-06	<a href="#">データストア ブラウザの使用</a> ：詳細情報を追加。
JP-001799-05	<ul style="list-style-type: none"><li>■ <a href="#">I/O フィルタのガイドラインおよびベスト プラクティス</a>：I/O フィルタとスナップショット ツリーに関する記述を追加。</li><li>■ <a href="#">ストレージ フィルタリング</a>：同じホストと転送フィルタの値を訂正。正しい値は <code>config.vpxd.filter.sameHostsAndTransportsFilter</code> です。</li></ul>
JP-001799-04	<a href="#">フラッシュ デバイスの有効期間の推定</a> ：詳細情報を追加。
JP-001799-03	<a href="#">Flash Read Cache</a> とともに仮想マシンを移行：vSphere Web Client で使用可能なオプションと一致するように修正。
JP-001799-02	<a href="#">VMFS ポインタ ブロック キャッシュの情報の取得</a> ： <code>esxcli storage vmfs pbcache</code> コマンドを追加。
JP-001799-01	マイナー改訂。
JP-001799-00	初期リリース。

# ストレージの概要

# 1

ここでは、vSphere で使用できるストレージ オプションについて、およびさまざまなタイプのストレージを使用および管理できるようにホストを構成する方法について説明します。

この章には、次のトピックが含まれています。

- ストレージ仮想化
- 物理ストレージのタイプ
- ターゲットとデバイスの表現
- ストレージ デバイスの特徴
- サポート対象のストレージ アダプタ
- データストアの特性
- 仮想マシンからストレージへのアクセス方法
- ストレージのタイプの比較

## ストレージ仮想化

vSphere ストレージ仮想化は、仮想マシン、Virtual SAN、仮想ボリューム、ポリシー ベースのストレージ管理などの機能をサポートします。

ESXi はホスト レベルのストレージ仮想化を行います。これは、仮想マシンから物理ストレージレイヤーを論理的に抽象化します。ESXi 仮想マシンは仮想ディスクを使用して、オペレーティング システム、プログラム ファイル、およびアクティビティに関連するその他のデータを格納します。仮想ディスクは、サイズの大きな物理ファイルまたはファイルのセットであり、ほかのファイル同様、容易にコピー、移動、アーカイブ、バックアップできます。複数の仮想ディスクを持つ仮想マシンを構成できます。

仮想マシンは仮想 SCSI コントローラを使用して仮想ディスクにアクセスします。これらの仮想コントローラには BusLogic 平行、LSI Logic 平行、LSI Logic SAS、および VMware 準仮想化が含まれます。これらのコントローラは、仮想マシンが参照およびアクセスできる唯一の SCSI コントローラ タイプです。

各仮想ディスクは、物理ストレージにデプロイされているデータストアに存在します。仮想マシンの観点からは、仮想ディスクは SCSI コントローラに接続された SCSI ドライブとして認識されます。ホスト上で実際の物理ストレージへのアクセスがストレージのアダプタを経由しているか、ネットワーク アダプタを経由しているかは、ゲスト OS システムおよび仮想マシンで実行しているアプリケーションに対し通常、透過的です。

仮想ディスクに加え、vSphere は、Raw デバイス マッピング (RDM) と呼ばれるメカニズムを提供します。RDM は、仮想マシン内のゲスト OS がストレージ デバイスへの直接アクセスを必要とする場合に有効です。RDM の詳細については、[18 章 Raw デバイス マッピング](#) を参照してください。

vSphere が提供するその他のストレージ仮想化機能には、Virtual SAN、仮想フラッシュ、仮想ボリューム、ポリシー ベースのストレージ管理などもあります。Virtual SAN の詳細については、『VMware Virtual SAN の管理』ドキュメントを参照してください。

## 物理ストレージのタイプ

ESXi ストレージ管理プロセスは、ストレージ管理者が別々のストレージ システムに対して事前に割り当てたストレージ領域から使用します。

ESXi は、次のタイプのストレージをサポートしています。

### ローカル ストレージ

内部のストレージ ディスク、または直接接続された外部のストレージ ディスク上に、仮想マシン ファイルを格納します。

### ネットワーク ストレージ

ホストに直接接続されたか、高速ネットワークを介して接続された外部のストレージ ディスクまたはアレイ上に、仮想マシン ファイルを格納します。

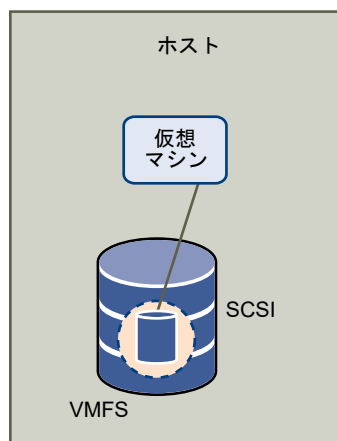
## ローカル ストレージ

ローカル ストレージは、ESXi ホスト内にある内部ハード ディスク、またはホスト外にあり、SAS や SATA などのプロトコルによってホストに直接接続されている外部ストレージ システムです。

ローカル ストレージには、ホストと通信するストレージ ネットワークが必要ありません。ストレージ ユニットに接続するケーブルと、必要に応じて互換性のある HBA がホスト内に必要です。

次の図に、ローカル SCSI ストレージを使用する仮想マシンを示します。

図 1-1. ローカル ストレージ





この例のローカル ストレージ トポロジでは、ホストはストレージ ディスクへの接続を 1 つ使用しています。このディスクで、仮想マシンのディスク ファイルの格納に使用する VMFS データストアを作成できます。

このストレージ構成は可能ですが、推奨するトポロジではありません。ストレージ アレイとホスト間で単一の接続を使用すると、接続の信頼性が低下したり障害が発生したりした場合に、単一点障害（SPOF）が発生し、動作が中断されることがあります。ただし、ローカル ストレージ デバイスの大半は複数の接続をサポートしていないので、複数のパスを使用してローカル ストレージにアクセスすることはできません。

ESXi は、SCSI、IDE、SATA、USB、および SAS など、さまざまなローカル ストレージ デバイスをサポートしています。使用するストレージのタイプにかかわらず、ホストは仮想マシンから物理ストレージ レイヤーを隠蔽します。

---

**注：** IDE/ATA または USB ドライブを使用して仮想マシンを格納することはできません。

---

ローカル ストレージは、複数のホスト間での共有をサポートしません。1 台のホストのみがローカル ストレージ デバイスのデータストアにアクセスできます。そのため、ローカル ストレージを使用して仮想マシンを作成できますが、共有ストレージが必要な VMware 機能（HA や vMotion など）を使用できません。

ただし、ローカル ストレージ デバイスのみを持つホストのクラスタを使用すると、Virtual SAN を実装できます。Virtual SAN を利用して、ローカル ストレージ リソースをソフトウェア定義による共有ストレージに変換し、共有ストレージが必要な機能を使用できます。詳細については、『VMware Virtual SAN の管理』ドキュメントを参照してください。

## ネットワーク ストレージ

ネットワーク ストレージとは、ESXi ホストが仮想マシン ファイルをリモートに格納するために使用する外部ストレージ システムからなります。通常、ホストは高速ストレージ ネットワークを介して、これらのシステムにアクセスします。

ネットワーク ストレージ デバイスは共有されます。ネットワーク ストレージ デバイスにあるデータストアは、複数のホストから同時にアクセスできます。ESXi は、複数のネットワーク ストレージ テクノロジーをサポートしています。

本トピックで説明する従来のネットワーク ストレージに加え、VMware は仮想化を利用した共有ストレージ（Virtual SAN など）もサポートしています。Virtual SAN は ESXi ホストの内部ストレージ リソースを、仮想マシンの High Availability や vMotion のような機能を備えた共有ストレージに変換します。詳細については、『VMware Virtual SAN の管理』ドキュメントを参照してください。

---

**注：** 同一の LUN を、異なるストレージ プロトコルを通じて ESXi ホストまたは複数のホストに表示することはできません。ホストが LUN にアクセスするには、ファイバ チャネルのみ、あるいは iSCSI のみなど、常に単一のプロトコルを使用する必要があります。

---

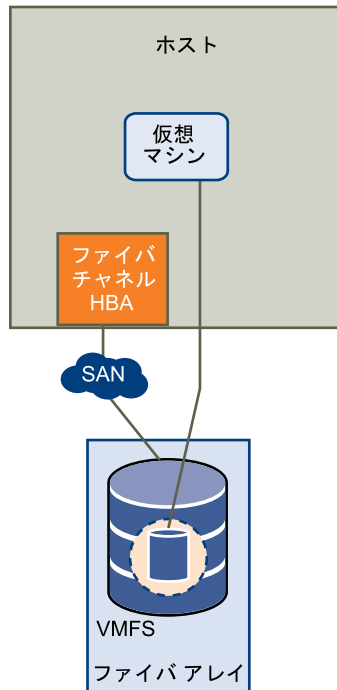
## ファイバ チャネル（FC）

FC ストレージ エリア ネットワーク（SAN）上でリモートに仮想マシン ファイルを格納します。FC SAN は、ホストを高性能なストレージ デバイスに接続する特別な高速ネットワークです。このネットワークは、ファイバ チャネル プロトコルを使用して、仮想マシンから FC SAN デバイスに SCSI トラフィックを転送します。

FC SAN に接続するには、ホストにファイバ チャンネル HBA（ホスト バス アダプタ）が搭載されている必要があります。また、ファイバ チャンネルの直接接続ストレージを使用する場合を除き、ストレージ トラフィックのルーティングにファイバ チャンネル スイッチが必要です。ホストに FCoE（Fibre Channel over Ethernet）アダプタがある場合は、イーサネット ネットワークを使用して、共有ファイバ チャンネル デバイスに接続できます。

ファイバ チャンネル ストレージは、ファイバ チャンネル ストレージを使用して仮想マシンを示します。

図 1-2. ファイバ チャンネル ストレージ



この構成では、ホストは、ファイバ チャンネル アダプタを使用して、SAN ファブリックに接続します。SAN ファブリックは、ファイバ チャンネル スイッチおよびストレージ アレイで構成されています。ストレージ アレイの LUN が、ホストで使用できるようになります。これらの LUN にアクセスし、ストレージが必要とするデータストアを作成できます。データストアには、VMFS フォーマットを使用します。

ファイバ チャンネル SAN の設定の詳細については、[3 章 ESXi とファイバ チャンネル SAN との併用](#)を参照してください。

## インターネット SCSI (iSCSI)

リモート iSCSI ストレージ デバイスに仮想マシン ファイルを格納します。iSCSI は、TCP/IP プロトコルに SCSI ストレージ トラフィックをパッケージ化することにより、専用の FC ネットワークではなく、標準 TCP/IP ネットワークを介して送信できるようにします。iSCSI 接続では、ホストは、リモート iSCSI ストレージ システムに配置されているターゲットと通信するイニシエータとして機能します。

ESXi は、次のタイプの iSCSI 接続をサポートしています。

### ハードウェア iSCSI

ホストは、iSCSI とネットワーク処理の負荷を軽減できるサードパーティ製のアダプタを介してストレージに接続します。ハードウェア アダプタは依存型と独立型にできます。

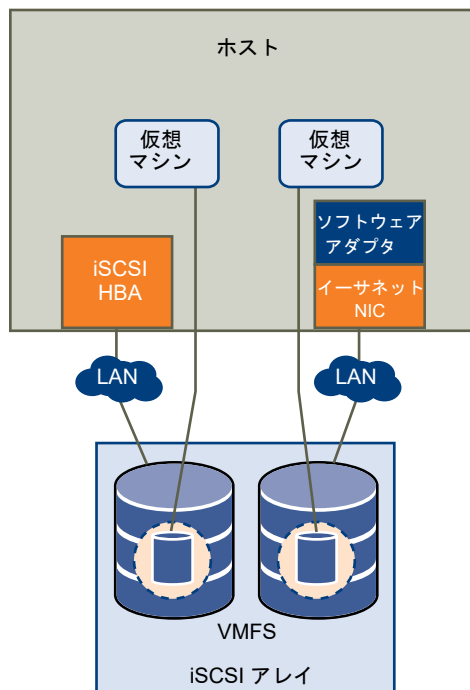
## ソフトウェア iSCSI

ホストは、VMkernel のソフトウェア ベースの iSCSI イニシエータを使用してストレージに接続します。このタイプの iSCSI 接続では、ホストはネットワーク接続のために標準ネットワーク アダプタのみを必要とします。

ホストが iSCSI ストレージ デバイスにアクセスして表示できるように iSCSI イニシエータを構成する必要があります。

iSCSI ストレージに、異なるタイプの iSCSI イニシエータを示しています。

図 1-3. iSCSI ストレージ



左側の例では、ホストがハードウェア iSCSI アダプタを使用して iSCSI ストレージ システムに接続しています。

右側の例では、ホストがソフトウェア iSCSI アダプタとイーサネット NIC を使用して iSCSI ストレージに接続しています。

ストレージ システムの iSCSI ストレージ デバイスを、ホストで使用するようになります。これらのストレージ デバイスにアクセスし、ストレージの必要に応じて、使用する VMFS データストアを作成できます。

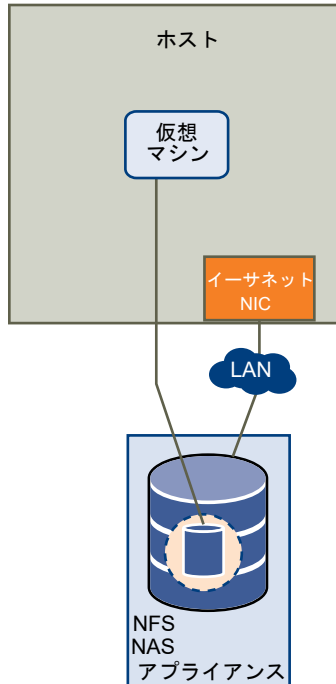
iSCSI SAN の設定の詳細については、[9 章 iSCSI SAN と ESXi との併用](#)を参照してください。

## ネットワーク接続型ストレージ (NAS)

標準 TCP/IP ネットワークを介してアクセスするリモート ファイル サーバ上に、仮想マシン ファイルを格納します。ESXi に組み込まれた NFS クライアントは、NFS (Network File System) プロトコル バージョン 3 および 4.1 を使用して NAS/NFS サーバと通信します。ネットワーク接続するには、ホストで標準ネットワーク アダプタが必要です。

NFS ストレージに、NFS ボリュームを使用してファイルを格納する仮想マシンを示します。この構成では、ホストは、仮想ディスク ファイルが格納されている NFS サーバに、通常のネットワーク アダプタを介して接続しています。

図 1-4. NFS ストレージ



NFS ストレージの設定の詳細については、[ネットワーク ファイル システム データストアについて](#)を参照してください。

## 共有のシリアル接続 SCSI (SAS)

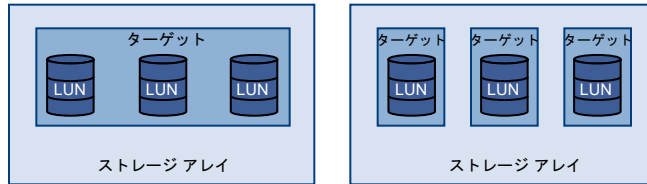
直接に接続され、複数のホストに共有アクセスを提供する SAS ストレージ システムに仮想マシンを格納します。このタイプのアクセスでは、複数のホストが、LUN の同じ VMFS データストアにアクセスできます。

## ターゲットとデバイスの表現

ESXi の文脈では、ターゲットという語は、ホストがアクセスできる 1 つのストレージ ユニットを表します。デバイスおよび LUN という語は、ターゲット上のストレージ領域を表す論理ボリュームを意味しています。一般的に ESXi の文脈では、デバイスおよび LUN という語は、ストレージ ターゲットからホストに表示されるストレージ ボリュームを意味しており、フォーマットに使用できます。

ストレージ ベンダーが異なると、ESXi ホストに対して異なる方法でストレージ システムを表示します。複数のストレージ デバイスまたは LUN を 1 つのターゲットで表示するベンダーもありますが、1 つの LUN を複数のターゲットで表示するベンダーもあります。

図 1-5. ターゲットと LUN の表現



この図では、各構成において3つのLUNを使用できます。一方のケースでは、ホストから1つのターゲットが見え、そのターゲットには使用可能なLUNが3つあります。それぞれのLUNは、個別のストレージボリュームを意味します。もう一方の例では、ホストから3つの異なるターゲットが見え、それぞれにLUNが1つあります。

ネットワークを介してアクセスされるターゲットには、ストレージシステムによって提供される一意の名前があります。iSCSI ターゲットは iSCSI 名を使用しますが、ファイバ チャネル ターゲットは、World Wide Name (WWN) を使用します。

**注：** ESXi では、異なる転送プロトコル（iSCSI とファイバ チャネルなど）を使用して同じ LUN にアクセスすることはサポートされていません。

デバイス、つまり LUN は、UUID 名で識別されます。LUN が複数のホストで共有される場合は、すべてのホストに同じ UUID で表示される必要があります。

## ストレージ デバイスの特徴

ローカル デバイスやネットワーク デバイスもすべて含めて、ホストで利用できるすべてのストレージ デバイスまたは LUN を表示できます。サードパーティ製のマルチパス プラグインを使用している場合は、プラグインを介して利用できるストレージ デバイスもリストに表示されます。

各ストレージ アダプタについて、このアダプタで利用できるストレージ デバイスの個別のリストを表示できます。

一般的に、ストレージ デバイスを確認する場合には、次の情報が表示されます。

表 1-1. ストレージ デバイスの情報

ストレージ デバイスの情報	説明
名前	表示名とも呼ばれます。これは ESXi ホストがストレージ タイプおよびメーカーに基づいてデバイスに割り当てた名前です。この名前は任意の名前に変更できます。
識別子	デバイスに固有な、あらゆる場所において一意の ID。
操作状態	デバイスがマウントされているか、マウントされていないかを示します。詳細については、 <a href="#">ストレージ デバイスの分離</a> を参照してください。
LUN	SCSI ターゲット内の LUN（論理ユニット番号）。LUN 番号は、ストレージ システムによって提供されます。ターゲットに1つのLUNしかない場合、LUN 番号は常にゼロ（0）になります。
タイプ	デバイスのタイプ（ディスク、CD-ROM など）。
ドライブの種類	デバイスがフラッシュ ドライブか、通常の HDD ドライブかに関する情報。フラッシュ ドライブの詳細については、 <a href="#">14 章 フラッシュ デバイスの操作</a> を参照してください。
転送	ホストがデバイスにアクセスするために使用する転送プロトコル。プロトコルは、使用しているストレージのタイプによって異なります。 <a href="#">物理ストレージのタイプ</a> を参照してください。

表 1-1. ストレージ デバイスの情報（続き）

ストレージ デバイスの情報	説明
容量	ストレージ デバイスの容量の合計。
所有者	NMP やサードパーティ製のプラグインなど、ホストがストレージ デバイスへのバスを管理するために使用するプラグイン。詳細については、 <a href="#">複数のバスの管理</a> を参照してください。
ハードウェア アクセラレーション	ストレージ デバイスが仮想マシン管理操作を行なってホストを支援しているかどうかに関する情報。ステータスは、「サポート」、「未サポート」、または「不明」です。詳細については、 <a href="#">23 章 ストレージのハードウェア アクセラレーション</a> を参照してください。
場所	/vmfs/devices/ ディレクトリにあるストレージ デバイスへのバス。
パーティションのフォーマット	ストレージ デバイスによって使用されるパーティションのスキーム。MBR（マスタ ブート レコード）または GPT（GUID パーティション テーブル）フォーマットにすることができます。GPT デバイスは 2TB より大きいデータストアをサポートします。詳細については、 <a href="#">VMFS データストアとストレージ ディスク フォーマット</a> を参照してください。
パーティション	プライマリおよび論理パーティション（構成されている場合は、VMFS データストアを含む）。
マルチバス ポリシー（VMFS データストア）	ホストがストレージへのバスの管理に使用しているバス選択ポリシーおよびストレージ アレイ タイプ ポリシー。詳細については、 <a href="#">17 章 マルチバスとフェイルオーバーについて</a> を参照してください。
バス（VMFS データストア）	ストレージへのアクセスに使用されているバスとそのステータス。

## ホストのストレージ デバイスの表示

ホストで使用可能なすべてのストレージ デバイスを表示します。サードパーティ製のマルチバス プラグインを使用している場合は、プラグインを介して使用できるストレージ デバイスもリストに表示されます。

[ストレージ デバイス] ビューでは、ホストのストレージ デバイスの一覧表示、それらの情報の分析、プロパティの修正を行うことができます。

### 手順

1 vSphere Web Client ナビゲータで、ホストを参照して移動します。

2 [構成] タブをクリックします。

3 [ストレージ] で、[ストレージ デバイス] をクリックします。

ホストで使用可能なすべてのストレージ デバイスが [ストレージ デバイス] に一覧表示されます。

4 特定のデバイスの詳細情報を表示するには、リストからデバイスを選択します。

5 [デバイスの詳細情報] タブを使用すると、選択したデバイスの追加情報にアクセスしたり、プロパティを修正したりできます。

タブ	説明
プロパティ	デバイスのプロパティと特性を表示します。デバイスのマルチバス ポリシーを表示、修正できます。
バス	デバイスで使用可能なバスを表示します。選択したバスを有効/無効にします。

## アダプタのストレージ デバイスの表示

ホスト上の特定のストレージ アダプタを通じてアクセスできるストレージ デバイスのリストを表示します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックします。

ホストにインストールされているすべてのストレージ アダプタが [ストレージ アダプタ] に一覧表示されます。

- 4 リストからアダプタを選択し、[デバイス] タブ をクリックします。

ホストがアダプタを通じてアクセスできるストレージ デバイスが表示されます。

## サポート対象のストレージ アダプタ

ストレージ アダプタは、ESXi ホストに、特定のストレージ ユニットまたはネットワークに対する接続を提供します。

ESXi は、SCSI、iSCSI、RAID、ファイバ チャネル、FCoE（Fibre Channel over Ethernet）、イーサネットなど、さまざまなクラスのアダプタをサポートしています。ESXi は、VMkernel のデバイス ドライバを介してアダプタに直接アクセスします。

使用しているストレージのタイプによっては、ホスト上でストレージ アダプタを有効にして構成しなければならない場合があります。

ソフトウェア FCoE アダプタの設定の詳細については、[5 章 ファイバ チャネル オーバー イーサネットの構成](#)を参照してください。

さまざまなタイプの iSCSI アダプタの構成の詳細については、[10 章 iSCSI アダプタおよびストレージの構成](#)を参照してください。

## ストレージ アダプタの特徴

ホストでストレージ アダプタを使用して、さまざまなストレージ デバイスにアクセスします。使用可能なストレージ アダプタの詳細を表示して、これらの情報を確認できます。

特定のアダプタ（ソフトウェア iSCSI や FCoE など）の情報を表示する前に、それらのアダプタを有効にする必要があります。

表 1-2. ストレージ アダプタの情報

アダプタ情報	説明
モデル	アダプタのモデル。
アクセス先（ファイバ チャネルおよび SCSI）	アダプタを介してアクセスしたアクセス先数。
接続中のアクセス先（iSCSI）	iSCSI アダプタ上で接続中のアクセス先の数。

表 1-2. ストレージ アダプタの情報（続き）

アダプタ情報	説明
WWN（ファイバ チャネル）	FC アダプタを一意に識別する、ファイバ チャネルの基準に従って形式化された World Wide Name。
iSCSI 名（iSCSI）	iSCSI アダプタを識別する iSCSI の基準に従って形式化された一意の名前。
iSCSI エイリアス（iSCSI）	iSCSI 名のかわりに使用される、わかりやすい名前。
IP アドレス（独立型ハードウェア iSCSI）	iSCSI HBA に割り当てられているアドレス。
デバイス	アダプタがアクセスできるすべてのストレージ デバイスまたは LUN。
バス	アダプタが使用してストレージ デバイスにアクセスするためのすべてのバス。
プロパティ	アダプタに追加の構成が必要であることを示すリンク。iSCSI および FCoE のアダプタにこのリンクが表示されます。

## ストレージ アダプタ情報の表示

ホストで使用するストレージ アダプタを表示して、これらの情報を確認します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックします。
- 4 特定のアダプタの詳細を表示するには、リストからアダプタを選択します。

## データストアの特性

データストアとは、ファイル システムに似た論理コンテナで、各ストレージ デバイスの仕様を隠し、仮想マシン ファイルを格納するための一貫したモデルを提供します。ホストで使用するすべてのデータストアを表示し、それらのプロパティを分析できます。

データストアは、次の方法で vCenter Server に追加されます。

- 新しいデータストア ウィザードを使用して、VMFS5 データストア、NFS バージョン 3 または 4.1 データストア、仮想データストアを作成できます。Virtual SAN データストアは、Virtual SAN を有効にすると自動的に作成されます。
- vCenter Server にホストを追加すると、ホストのすべてのデータストアが vCenter Server に追加されます。

次の表に、vSphere Web Client でデータストアを確認するときに表示されるデータストアの詳細情報を示します。一部のタイプのデータストアでしか使用または適用できない機能もあります。



表 1-3. データストア情報

データストア情報	適用可能なデータストア タイプ	説明
名前	VMFS NFS Virtual SAN VVOL	データストアに割り当てられた編集可能な名前。データストアの名前変更の詳細については、 <a href="#">データストア名の変更</a> を参照してください。
ファイル システムのタイプ	VMFS NFS Virtual SAN VVOL	データストアが使用するファイル システム。VMFS および NFS データストアに関する情報とその管理方法については、 <a href="#">16 章 データストアでの作業</a> を参照してください。  Virtual SAN データストアの詳細については、『VMware Virtual SAN の管理』のドキュメントを参照してください。  仮想ボリュームの詳細については、 <a href="#">19 章 仮想ボリュームの操作</a> を参照してください。
デバイス バックিং	VMFS NFS Virtual SAN	データストアがデプロイされているストレージ デバイス(VMFS)、サーバおよびフォルダ(NFS)、またはディスク グループ (Virtual SAN) など、基盤となるストレージに関する情報。
プロトコル エンドポイント	VVOL	対応するプロトコル エンドポイントに関する情報。 <a href="#">プロトコル エンドポイント</a> を参照してください。
エクステント	VMFS	データストアがまたがる個々のエクステントとその容量。
ドライブの種類	VMFS	基盤となるストレージ デバイスのタイプ (フラッシュ ドライブまたは通常の HDD ドライブ)。詳細については、 <a href="#">14 章 フラッシュ デバイスの操作</a> を参照してください。
容量	VMFS NFS Virtual SAN VVOL	合計容量、プロビジョニング済み容量、および空き容量を含みます。
マウント ポイント	VMFS NFS Virtual SAN VVOL	ホストの /vmfs/volumes/ ディレクトリ内のデータストアへのパス。
機能セット	VMFS  <b>注:</b> マルチ エクステント VMFS データストアでは、1 つのエクステントのみの機能を想定しています。  NFS Virtual SAN	基盤となるストレージ エンティティが提供するストレージ データ サービスに関する情報。修正できません。
Storage I/O Control	VMFS NFS	クラスタ全体のストレージ I/O の優先順位付けが有効かどうかに関する情報。『vSphere リソース管理』ドキュメントを参照してください。

表 1-3. データストア情報（続き）

データストア情報	適用可能なデータストア タイプ	説明
ハードウェア アクセラレーション	VMFS	基盤となるストレージ エンティティがハードウェア アクセラレーションをサポートしているかどうかに関する情報。ステータスは、「サポート」、「未サポート」、または「不明」です。詳細については、 <a href="#">23 章 ストレージのハードウェア アクセラレーション</a> を参照してください。
	NFS	
	Virtual SAN	
	VVOL	
	<b>注：</b> NFS 4.1 では、ハードウェア アクセラレーションはサポートされていません。	
タグ	VMFS	タグ形式でユーザーが定義しデータストアに関連付けるデータストア機能。詳細については、 <a href="#">ストレージ ポリシーとルール</a> を参照してください。
	NFS	
	Virtual SAN	
	VVOL	
ホストとの接続	VMFS	データストアがマウントされたホスト。
	NFS	
	VVOL	
マルチパス機能	VMFS	ホストがストレージへのアクセスに使用しているパス選択ポリシー。詳細については、 <a href="#">17 章 マルチパスとフェイルオーバーについて</a> を参照してください。
	VVOL	




## データストア情報の表示

vSphere Web Client ナビゲータで、データストア ビューにアクセスします。ナビゲータで表示されるデータストア ビューでは、vSphere のインフラストラクチャ インベントリで使用できるすべてのデータストアが一覧表示されます。ここで、情報を分析し、プロパティを変更することができます。このビューを使ってデータストアを作成することもできます。

データセンター、クラスタ、またはホストといった特定の親オブジェクトのデータストアを一覧表示するには、[インフラストラクチャ オブジェクトのデータストアを一覧表示する](#)を参照してください。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。インベントリで使用可能なデータストアが、中央の [データストア] パネルに表示されます。
- 2 アイコンを使用してデータストアを作成するか、選択したデータストアについて基本的なタスクを実行します。

アイコン	説明
	データストアを作成します。
	データストア容量を増加させます。
	特定のホストにデータストアをマウントします。
	データストアの削除。
	特定のホストからデータストアをアンマウントします。

- 特定のデータストアの詳細を表示するには、選択したデータストアをクリックします。
- タブを使用して追加情報にアクセスし、データストア プロパティを修正します。

タブ	説明
[はじめに]	概要情報を表示し、基本アクションにアクセスできます。
[サマリ]	選択したデータストアの統計情報および構成を表示します。
[監視]	データストアに関するアラーム、パフォーマンス データ、リソース割り当て、イベント、その他のステータス情報を表示します。
[管理]	データストアのプロパティ、アラーム定義、タグ、権限を表示し変更します。このタブを使用し、データストアをバックアップしているストレージ デバイスにアクセスし、データストア デバイスのマルチパス詳細を表示し編集します。
[関連オブジェクト]	データストアに関連するオブジェクトを表示します。オブジェクトには、データストア上にある仮想マシンおよびデータストアがマウントされているホストが含まれます。

## インフラストラクチャ オブジェクトのデータストアを一覧表示する

データセンター、クラスタまたはホストといった特定の親オブジェクトのデータストアを表示します。






### 手順

- vSphere Web Client オブジェクト ナビゲータを使用し、データセンター、クラスタ、またはホストといったデータストアの有効な親オブジェクトであるオブジェクトに移動して参照します。

- [関連オブジェクト] タブをクリックし、[データストア]をクリックします。

このオブジェクトについて構成されているデータストアがあれば、中央の [データストア] パネルに表示されます。

- アイコンを使用してデータストアを作成するか、選択したデータストアについて基本的なタスクを実行します。

アイコン	説明
	データストアを作成します。
	データストア容量を増加させます。
	特定のホストにデータストアをマウントします。
	データストアの削除。
	特定のホストからデータストアをアンマウントします。

- タブを使用して追加情報にアクセスし、データストア プロパティを修正します。

タブ	説明
[はじめに]	概要情報を表示し、基本アクションにアクセスできます。
[サマリ]	選択したデータストアの統計情報および構成を表示します。
[監視]	データストアに関するアラーム、パフォーマンス データ、リソース割り当て、イベント、その他のステータス情報を表示します。

タブ	説明
[管理]	データストアのプロパティ、アラーム定義、タグ、権限を表示し変更します。このタブを使用し、データストアをバックアップしているストレージ デバイスにアクセスし、データストア デバイスのマルチパス詳細を表示し編集します。
[関連オブジェクト]	データストアに関連するオブジェクトを表示します。オブジェクトには、データストア上にある仮想マシンおよびデータストアがマウントされているホストが含まれます。

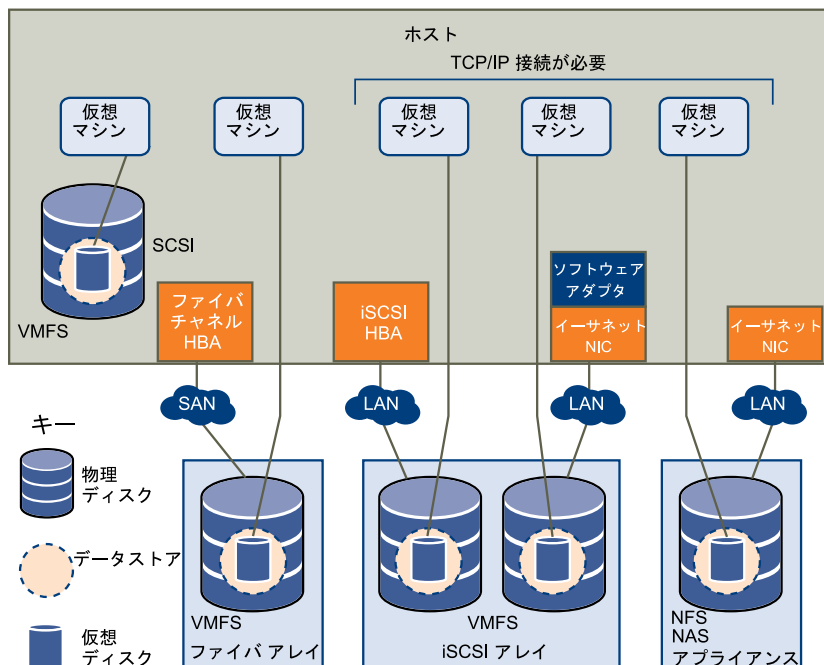
## 仮想マシンからストレージへのアクセス方法

仮想マシンは、データストアに格納された仮想ディスクと通信する際に、SCSI コマンドを発行します。データストアは、さまざまなタイプの物理ストレージに存在するため、これらのコマンドは、ESXi ホストがストレージ デバイスへの接続に使用するプロトコルに応じて、別の形式にカプセル化されます。

ESXi はファイバ チャネル (FC)、インターネット SCSI (iSCSI)、FCoE (Fibre Channel over Ethernet)、および NFS プロトコルをサポートしています。ホストで使用するストレージ デバイスのタイプにかかわらず、仮想ディスクは、仮想マシンでは常にマウントされた SCSI デバイスとして表示されます。仮想ディスク環境では、仮想マシンのオペレーティング システムから物理ストレージ レイヤーを隠蔽します。これにより、SAN などの特定のストレージ装置で認定されていないオペレーティング システムを、仮想マシン内で実行できます。

次の図に、異なるタイプのストレージを使用する 5 台の仮想マシンから、各タイプの違いを示します。

図 1-6. さまざまなタイプのストレージにアクセスする仮想マシン



**注：** この図は、概念を示す目的で使用します。推奨する構成ではありません。

## ストレージのタイプの比較

vSphere の特定の機能がサポートされるかどうかは、使用するストレージのテクノロジーによって決まります。

次の表で、ESXi がサポートするネットワーク ストレージ テクノロジーを比較します。

表 1-4. ESXi がサポートするネットワーク ストレージ

テクノロジー	プロトコル	転送	インターフェイス
ファイバ チャネル	FC/SCSI	データ / LUN のブロック アクセス	FC HBA
ファイバ チャネル オーバーイーサネット	FCoE/SCSI	データ / LUN のブロック アクセス	<ul style="list-style-type: none"> <li>■ 統合ネットワーク アダプタ (ハードウェア FCoE)</li> <li>■ FCoE をサポートする NIC (ソフトウェア FCoE)</li> </ul>
iSCSI	IP/SCSI	データ / LUN のブロック アクセス	<ul style="list-style-type: none"> <li>■ iSCSI HBA または iSCSI が有効な NIC (ハードウェア iSCSI)</li> <li>■ ネットワーク アダプタ (ソフトウェア iSCSI)</li> </ul>
NAS	IP/NFS	ファイル (直接 LUN アクセスなし)	ネットワーク アダプタ

次の表は、さまざまなタイプのストレージでサポートしている vSphere の機能について比較しています。

表 1-5. ストレージでサポートされる vSphere の機能

ストレージ タイプ	仮想マシンの起動	vMotion	データストア	RDM	仮想マシン クラスタ	VMware HA および DRS	Storage APIs - Data Protection
ローカル ストレージ	はい	いいえ	VMFS	いいえ	はい	いいえ	はい
ファイバ チャネル	はい	はい	VMFS	はい	はい	はい	はい
iSCSI	はい	はい	VMFS	はい	はい	はい	はい
NAS over NFS	はい	はい	NFS 3 および NFS 4.1	いいえ	いいえ	はい	はい

**注：** ローカル ストレージは、単一ホスト (筐体内クラスタとも言われる) で仮想マシンのクラスタをサポートしません。共有の仮想ディスクが必要です。この構成の詳細については、『vSphere リソース管理』ドキュメントを参照してください。

# ESXi と SAN の併用の概要

## 2

ESXi を SAN と併用すると、柔軟性、効率、信頼性が高まります。また ESXi を SAN と併用すると、統合管理、フェイルオーバー、およびロード バランシングのテクノロジーもサポートされます。

ESXi と SAN を併用すると、次のようなメリットがあります。

- データを安全に格納し、ストレージへのパスを複数構成することで、単一点障害を除去できます。
- SAN を ESXi システムと併用すると、サーバの耐障害性が得られます。SAN ストレージを使用すると、ホストで障害が発生した場合に、すべてのアプリケーションを別のホストですぐに再起動できます。
- VMware vMotion を使用すると、仮想マシンをライブ移行できます。
- VMware HA (High Availability) を SAN と併用すると、ホストで障害が発生した場合に、仮想マシンを最後の既知の状態別のサーバ上で再起動できます。
- VMware Fault Tolerance (FT) を使用すると、保護対象の仮想マシンを 2 台の異なるホストに複製できます。プライマリ ホストで障害が発生した場合、仮想マシンは中断せずにセカンダリ ホストで動作し続けます。
- VMware DRS (Distributed Resource Scheduler) を使用すると、あるホストから別のホストに仮想マシンを移行してロード バランシングを実行できます。ストレージは共有 SAN アレイにあるため、アプリケーションはシームレスに実行を継続できます。
- VMware DRS クラスタを使用している場合は、ESXi ホストをメンテナンス モードに切り替えて、すべての実行中の仮想マシンを別の ESXi ホストに移行します。その後、元のホストでアップグレードまたはその他のメンテナンス操作を実行できます。

このストレージが共有されているという特徴は、VMware 仮想マシンの移植性およびカプセル化でさらに強化されます。仮想マシンが SAN ベースのストレージにある場合、即座にあるサーバで仮想マシンをシャットダウンして別のサーバで起動したり、あるサーバで仮想マシンをサスペンドして同じネットワークの別のサーバで動作をレジュームしたりできます。この機能によって、共有アクセスを整合性のとれた状態で維持したまま、コンピューティング リソースを移行できます。

この章には、次のトピックが含まれています。

- [ESXi と SAN の使用例](#)
- [SAN ストレージを ESXi と併用する場合の特性](#)
- [ESXi ホストと複数のストレージ アレイ](#)
- [LUN の決定](#)
- [仮想マシンの場所の選定](#)

- レイヤー化されたアプリケーション
- サードパーティ製の管理アプリケーション
- SAN ストレージ バックアップに関する考慮事項

## ESXi と SAN の使用例

SAN と使用されると、ESXi は、Storage vMotion、DRS (Distributed Resource Scheduler)、High Availability などをはじめとする複数の vSphere の機能の利点を活用できます。

ESXi を SAN と併用すると、次のタスクの実行に効果的です。

### ストレージ統合とストレージ レイアウトの簡略化

複数のホストを使用していて、各ホストが複数の仮想マシンを実行している場合、ホストのストレージは不足し、外部ストレージが必要です。外部ストレージとして SAN を選択すると、システム アーキテクチャが単純化される点に加え、その他のメリットもあります。

### ダウンタイムなしのメンテナンス

ESXi ホストまたはインフラストラクチャのメンテナンスを実行するとき、vMotion を使用して、仮想マシンをほかのホストに移行します。共有ストレージが SAN にある場合、仮想マシンのユーザーの操作を停止することなく、メンテナンスを実行できます。移行の間、仮想マシンの作業プロセスは続行します。

### ロード バランシング

DRS クラスタにホストを追加でき、ホストのリソースはクラスタのリソースの一部になります。クラスタ内にあるすべてのホストおよび仮想マシンの CPU およびメモリ リソースの配分と使用率を継続的に監視します。DRS は理想的なリソースの使用とこれらのメトリックを比較します。理想的な使用は、クラスタのリソース プールと仮想マシンの属性、現在の需要、および不均衡なターゲットを考慮します。次に、それに応じて仮想マシンへの移行を実行 (または推奨) します。

### ディザスタ リカバリ

VMware High Availability を使用して、複数の ESXi ホストをクラスタとして構成して、仮想マシンで実行中のアプリケーションに、システム停止からの迅速なリカバリと、費用対効果に優れた高可用性を提供します。

### アレイの移行とストレージのアップグレードの簡素化

新しいストレージ システムまたはアレイを購入した場合、Storage vMotion を使用して、仮想マシンのユーザーの操作を停止することなく、既存のストレージから新しいターゲットに、仮想マシンのディスク ファイルを自動的にライブ移行できます。

## SAN ストレージを ESXi と併用する場合の特性

SAN を ESXi ホストと併用する場合は、さまざまな点で従来の SAN の使用方法と異なります。

SAN ストレージを ESXi と併用する場合は、次の点に留意してください。

- SAN 管理ツールを使用して、ストレージを使用する仮想マシンのオペレーティング システムに直接アクセスすることはできません。従来のツールで監視できるのは VMware ESXi オペレーティング システムのみです。仮想マシンを監視するには、vSphere Web Client を使用します。
- SAN 管理ツールで参照できる HBA は、仮想マシンの一部ではなく、ESXi システムの一部です。
- 通常、ESXi システムは、マルチパス機能を実行します。

## ESXi ホストと複数のストレージ アレイ

ESXi ホストは、複数のストレージ アレイ（異なるベンダーからのアレイを含む）から提供されるストレージ デバイスにアクセスできます。

異なるベンダーからの複数のアレイを使用するとき、次の点に注意してください。

- ホストが複数のアレイに同じストレージ アレイ タイプ プラグイン（SATP）を使用している場合、その SATP のデフォルトのパス選択ポリシー（PSP）の変更が必要なときには注意してください。変更は、すべてのアレイに適用されます。SATP および PSP については、[17 章 マルチパスとフェイルオーバーについて](#) を参照してください。
- 一部のストレージ アレイには、キューの深さやその他の設定に関する推奨があります。通常、これらの設定は ESXi ホスト レベルでグローバルに構成されます。1 台のアレイに変更を行うと、ホストへの LUN を提供する他のアレイにも影響を及ぼします。キューの深さの変更については、<http://kb.vmware.com/kb/1267> で当社のナレッジ ベースの記事を参照してください。
- ファイバ チャネル アレイに対して ESXi ホストをゾーニングする場合には、1 ターゲット 1 イニシエータ ゾーニングを使用します。このタイプの構成では、1 台のアレイで発生したファブリックに関するイベントは他のアレイに影響を及ぼしません。ゾーニングに関する詳細は、[ゾーニングとファイバ チャネル SAN との併用](#) を参照してください。

## LUN の決定

VMFS データストアを使用して LUN をフォーマットする場合は、まず ESXi システムのストレージのセットアップ方法を検討する必要があります。

LUN を決定するとき、次の点を考慮してください。

- 各 LUN には、その LUN を使用する仮想マシンで実行されるアプリケーションに適した RAID レベルとストレージ特性が必要です。
- 各 LUN に含めることができる VMFS データストアは 1 つだけです。
- 複数の仮想マシンが同じ VMFS にアクセスする場合、ディスク シェアを使用して仮想マシンに優先順位を付けます。

少数の大きな LUN を設定すると、次のようなメリットがあります。

- 仮想マシンをより柔軟に作成でき、ストレージ管理者にディスク領域の拡張を依頼する必要がありません。
- 仮想ディスクのサイズ変更、スナップショットの操作などをより柔軟に実行できます。



- 管理する VMFS データストアの数が少なくなります。

多数の小さな LUN を設定すると、次のようなメリットがあります。

- 無駄になるストレージ領域が減ります。
- アプリケーションが異なると、必要な RAID 特性が異なる場合があります。
- マルチパス ポリシーやディスク共有を LUN ごとに設定すると、より柔軟性が高くなります。
- Microsoft Cluster Service を使用する場合、各クラスター ディスク リソースが専用 LUN に存在する必要があります。
- 1 つのボリュームに対する競合が緩和されるのでパフォーマンスが向上します。

仮想マシンのストレージ特性がわからないときは、プロビジョニングする LUN の数とサイズを決定する単純な方法は通常ありません。予測型スキームや適合型スキームで試行できます。

## 予測型スキームを使用した LUN の決定

ESXi システムのストレージを設定するときは、VMFS データストアを作成する前に、プロビジョニングする LUN のサイズと数を決定する必要があります。予測型スキームを使用して試行できます。

### 手順

- 1 ストレージ特性が異なる複数の LUN をプロビジョニングします。
- 2 各 LUN に VMFS データストアを作成し、各データストアに、その特性に応じてラベルを付けます。
- 3 仮想マシン アプリケーションのデータを、アプリケーションの要件に合わせた適切な RAID レベルで LUN 上の VMFS データストアに格納できるように、仮想ディスクを作成します。
- 4 ディスク シェアを使用して、優先順位の高い仮想マシンと優先順位の低い仮想マシンを区別します。

---

**注：** ディスク シェアは、指定されたホスト内でのみ有効です。あるホストの仮想マシンに割り当てられたシェアは、別のホストの仮想マシンでは無効です。

---

- 5 アプリケーションを実行し、仮想マシンのパフォーマンスが許容できる状態かどうかを判断します。

## 適合型スキームを使用した LUN の決定

ESXi ホストのストレージを設定するときは、VMFS データストアを作成する前に、プロビジョニングする LUN の数とサイズを決定する必要があります。適合型スキームを使用して試行できます。

### 手順

- 1 書き込みキャッシュを有効にして、大きな LUN (RAID 1+0 または RAID 5) をプロビジョニングします。
- 2 その LUN に VMFS を作成します。
- 3 その VMFS 上に 4 ～ 5 の仮想ディスクを作成します。
- 4 アプリケーションを実行し、ディスク パフォーマンスが許容できる状態かどうかを判断します。

## 結果

パフォーマンスが許容可能な場合、VMFS に追加の仮想ディスクを配置できます。パフォーマンスが条件にあっていない場合は、新しく大きな LUN を作成（おそらく別の RAID レベルで）し、このプロセスを繰り返します。移行を実行し、LUN を再作成しても仮想マシンのデータが失われないようにします。

## 仮想マシンの場所の選定

仮想マシンのパフォーマンスを最適化する場合、ストレージの選定が重要な要因になります。高いパフォーマンスと高い可用性を提供する高価なストレージと、より安価でパフォーマンスが劣るストレージとの間では、常にトレードオフが発生します。

多くの要因に応じて、ストレージは異なる階層に分けられます。

- **ハイティア**：高いパフォーマンスと高い可用性を提供します。バックアップとポイント イン タイム（PiT）リストアが容易になる組み込み型スナップショットを備えていることがあります。レプリケーション、完全なストレージ プロセッサの冗長性、および SAS ドライブをサポートします。高価なスピンドルを使用しています。
- **ミッドティア**：ミッドレンジのパフォーマンス、やや低い可用性、一部のストレージ プロセッサの冗長性、および SCSI ドライブまたは SAS ドライブを備えています。スナップショットを提供することもあります。中位の価格のスピンドルを使用しています。
- **ローティア**：パフォーマンスは低く、内部ストレージの冗長性はほとんどありません。ローエンド SCSI ドライブまたは SATA（低価格のスピンドル）を使用しています。

必ずしもすべてのアプリケーションが、最高のパフォーマンスと可用性を備えたストレージを必要とするわけではありません。

---

**注：** 少なくとも、アプリケーションのライフサイクル全体で必要となるわけではありません。スナップショットなどハイティアの機能の一部が必要だが費用をかけたくない場合は、ソフトウェアで高いパフォーマンス機能を実現できることがあります。たとえば、ソフトウェアでスナップショットを作成できます。

---

どのような仮想マシンを選定するかを決定するには、次の事項について考えます。

- その仮想マシンは、どの程度重要か。
- パフォーマンスと可用性の要件はどの程度か。
- PiT リストア要件は何か。
- バックアップ要件は何か。
- レプリケーション要件は何か。

仮想マシンでは、重要度の変化、またはハイティア機能をローティアに取り込むようなテクノロジーの変化によって、ライフサイクルを通じてティアが変わることがあります。重要度は相対的で、組織、運用プロセス、規制条件、災害計画などの変更を含め、さまざまな理由で変わることがあります。

## レイヤー化されたアプリケーション

SAN 管理者は一般的に、特別なアレイ ベースのソフトウェアを使用して、バックアップ、ディザスタ リカバリ、データ マイニング、フォレンジック、および構成テストを行います。

ストレージ業者は通常、LUN について 2 種類の上級サービスを提供しています。スナップショットとレプリケーションです。

- スナップショットでは、データのブロックが共通である LUN を効率的にコピーして容量を作成します。一般的に、スナップショットはプライマリ LUN と同じストレージ システムでローカルに利用され、短時間でのバックアップ、アプリケーション テスト、フォレンジック、またはデータ マイニングを行います。
- レプリケーションでは、LUN 全体のコピーを作成します。レプリカは通常、ストレージ システムを分離させるのに使用します。場合によっては、アレイやサイト全体の機能停止または破壊を招くような大規模な停電から、サイトを保護するために分離します。

ESXi システムを SAN と組み合わせて使用する場合は、アレイ ベースとホスト ベースのツールのどちらがその状況に適しているかを判断する必要があります。

## アレイ ベース（サードパーティ）のソリューション

ESXi システムを SAN と組み合わせて使用する場合は、アレイ ベースのツールがその状況に適しているかどうかを判断する必要があります。

アレイ ベースのソリューションについて検討するときは、次の点に留意してください。

- アレイ ベースのソリューションは、通常、より広範囲な統計情報を提供します。RDM では、データは常に同じバスを通るため、パフォーマンス管理が簡単になります。
- RDM とアレイ ベースのソリューションを使用すると、ストレージ管理者にとってセキュリティがよりわかりやすくなります。これは、RDM を使用すると、仮想マシンはより物理マシンに近くなるためです。
- アレイ ベースのソリューションを使用する場合、仮想マシンのストレージには物理的に互換性のある RDM がよく利用されます。RDM を使用する計画がない場合は、ストレージ ベンダーのドキュメントを確認して、VMFS ボリュームのある LUN での操作がサポートされているかどうか確認してください。VMFS LUN でアレイ操作を行う場合、再署名のセクションを注意して読んでください。

## ファイル ベース（VMFS）のソリューション

ESXi システムを SAN と組み合わせて使用する場合は、ファイル ベースのツールがその状況に適しているかどうかを判断する必要があります。

アレイツールの代わりに VMware Tools と VMFS を使用するファイル ベースのソリューションについて検討するときは、次の点を考慮してください。

- プロビジョニングについては、VMware Tools と VMFS の使用がより適しています。1 つの大きな LUN が割り当てられ、複数の .vmdk ファイルをその LUN に配置できます。RDM では、各仮想マシンに新しい LUN が必要です。
- スナップショットは ESXi ホストに無償で含まれています。
- ESXi 管理者にとっては、VMFS を使用するほうが簡単です。
- ファイル ベースのソリューションを使用すると、ESXi 管理者の SAN 管理者に対する依存度が減ります。

## サードパーティ製の管理アプリケーション

サードパーティ製の管理アプリケーションを ESXi ホストと組み合わせて使用できます。

ほとんどの SAN ハードウェアには、ストレージ管理ソフトウェアが付属しています。多くの場合、このソフトウェアは Web アプリケーションで、ネットワークに接続された Web ブラウザから利用できます。その他の場合では、このソフトウェアは通常、ストレージ システムまたは単一サーバで実行されます。サーバが SAN をストレージとして使用しているかどうかは関係ありません。

このサードパーティ製の管理ソフトウェアを使用すると、次のタスクが実行できます。

- ストレージ アレイの管理（LUN の作成、アレイ キャッシュの管理、LUN のマッピング、LUN のセキュリティなど）
- レプリケーション、チェック ポイント、スナップショット、ミラーリングの設定

仮想マシンで SAN 管理ソフトウェアを実行する場合、vMotion や VMware HA を使用したフェイルオーバーなど、仮想マシンを実行するメリットが得られます。ただし、より間接的になるため、管理ソフトウェアを SAN を認識できないことがあります。この場合は RDM を使用できます。

---

**注：** 仮想マシンで管理ソフトウェアを正常に実行できるかどうかは、ストレージ アレイに依存します。

---

## SAN ストレージ バックアップに関する考慮事項

適切なバックアップ戦略をとることは、SAN 管理にとって最重要事です。SAN 環境では、バックアップの目的は 2 つあります。最初の目的は、オンライン データをオフライン メディアにアーカイブすることです。このプロセスは、すべてのオンライン データに対して、定期的にスケジュールに従って繰り返されます。もう 1 つの目的は、問題からリカバリするために、オフラインデータへのアクセスを提供することです。たとえば、データベースのリカバリでは、現在オンラインではないアーカイブされたログ ファイルの取得がしばしば必要となります。

バックアップのスケジューリングは、次のような多くの要因に依存します。

- 一定の期間内により頻繁なバックアップ サイクルを必要とする重要なアプリケーションの特定。
- リカバリ ポイントとリカバリ時間の目標。必要なリカバリ ポイントの正確さと、リカバリを待つことができる時間の長さについて考えます。
- データに関連付けられた変更率（RoC）。たとえば、同期/非同期レプリケーションを使用している場合、RoC が、プライマリ ストレージ デバイスとセカンダリ ストレージ デバイスの間で必要なバンド幅の量に影響を与えます。
- SAN 環境、（バックアップ中の）ストレージ パフォーマンス、およびその他のアプリケーションに与える全体的な影響。
- SAN のピーク トラフィック時間の特定（ピーク時間にスケジュールされたバックアップは、アプリケーションおよびバックアップ プロセスの速度を低下させることがあります）。
- データセンター内のすべてのバックアップをスケジュールする時間。
- 個別のアプリケーションをバックアップするために必要な時間。
- データのアーカイブに使用できるリソース。通常はオフライン メディア アクセス（テープ）です。

バックアップ計画を立てるときには、アプリケーションごとのリカバリ時間の目標を含めます。つまり、バックアップを実行するために必要な時間とリソースについて考慮します。たとえば、スケジュール設定したバックアップで大量のデータが保管されるためにリカバリに長時間かかる場合は、バックアップ スケジュールを検討してみてください。バックアップの実行回数を増やすと、1 回にバックアップされるデータの量が少なくなり、リカバリ時間が短縮されます。

特定のアプリケーションを特定の時間枠でリカバリする必要がある場合は、この要件を満たすために、バックアッププロセスでタイム スケジュールと特別なデータ処理を指定する必要があります。高速リカバリでは、失われたデータコンポーネントに低速なオフライン メディアでアクセスする必要性を最小限にする、またはなくすために、オンライン ストレージにあるリカバリ ボリュームを使用する必要があります。

## サードパーティ製のバックアップ パッケージの使用

サードパーティ製のバックアップ ソリューションを使用して、仮想マシンのシステム、アプリケーション、ユーザ データを保護します。

VMware は、サードパーティの製品と組み合わせて動作させるために Storage APIs - Data Protection を提供しています。API を使用するとき、サードパーティのソフトウェアはバックアップ タスクの処理で ESXi ホストをロードすることなく、バックアップを実行できます。

Storage APIs - Data Protection を使用するサードパーティの製品は、次のバックアップ タスクを実行できます。

- 仮想マシンのフル、差分および増分イメージ バックアップおよびリストアを実行します。
- サポートされる Windows および Linux オペレーティング システムを使用する仮想マシンのファイル レベルのバックアップを実行します。
- サポートされる Microsoft Windows オペレーティング システムを実行する仮想マシンのために Microsoft Volume Shadow Copy Services (VSS) を使用することによって、データの整合性を保証します。

Storage APIs - Data Protection が VMFS のスナップショット機能を活用しているために、実行可能なバックアップでは、仮想マシンのためのダウンタイムは必要とされません。これらのバックアップは無停止であり、いつでも実行可能であるため、拡張されたバックアップ ウィンドウは不要です。

Storage APIs - Data Protection とバックアップ製品との統合の詳細については、VMware Web サイトをご覧ください。いただくか、バックアップ製品のベンダーにお問い合わせください。

# ESXi とファイバ チャネル SAN との併用

## 3

FC SAN ストレージ アレイを使用するように ESXi ホストを設定するときは、特別な考慮が必要になります。このセクションでは、ESXi を FC SAN アレイと併用する方法の概要について説明します。

この章には、次のトピックが含まれています。

- ファイバ チャネル SAN の概念
- ゾーニングとファイバ チャネル SAN との併用
- 仮想マシンからファイバ チャネル SAN 上のデータへのアクセス方法

## ファイバ チャネル SAN の概念

ESXi のシステム管理者として、SAN と連携するようにホストを設定しようとする場合は、SAN の概念について実用的な知識が必要です。SAN に関する情報は、印刷物またはインターネットで入手できます。この業界は常に変化しているので、これらの関連資料を頻繁にチェックしてください。

はじめて SAN テクノロジーを使用する場合は、基本的な用語について理解してください。

SAN（ストレージ エリア ネットワーク）は、コンピュータ システム（すなわちホスト サーバ）を高性能なストレージ サブシステムに接続するための専用の高速ネットワークです。SAN コンポーネントには、ホスト サーバ内のホスト バス アダプタ（HBA）、ストレージ トラフィックのルーティングを支援するスイッチのほか、ケーブル、ストレージ プロセッサ（SP）、ストレージ ディスク アレイなどが含まれます。

ネットワークに1つ以上のスイッチを持つ SAN トポロジは、SAN ファブリックを形成します。

トラフィックをホスト サーバから共有ストレージに転送するために、SAN は、SCSI コマンドを FC（ファイバ チャネル）フレームにパッケージ化する FC プロトコルを使用します。

サーバに割り当てられていないストレージ アレイへのサーバ アクセスを制限するために、SAN はゾーニングを使用します。通常、ストレージ デバイスおよび LUN の共有グループにアクセスするサーバ グループごとにゾーンを作成します。ゾーンは、どの HBA がどの SP に接続できるかを定義します。ゾーン外のデバイスは、ゾーン内のデバイスから参照できません。

ゾーニングは、アクセス権の管理に広く使用されている LUN マスキングに似ています。LUN マスキングは、LUN をあるホストからは使用できるようにして、別のホストからは使用できないようにする処理です。

ホスト サーバとストレージの間でデータを転送するとき、SAN はマルチパスとよばれる手法を使用します。マルチパスによって、ESXi ホストからストレージ システム上の LUN への複数の物理パスを確保できます。

一般的に、ホストから LUN への 1 つのパスは、HBA、スイッチ ポート、接続用ケーブル、およびストレージ コントローラ ポートから構成されます。パスのコンポーネントで障害が発生した場合、ホストは I/O に使用可能な別のパスを選択します。障害が発生したパスを検出し、別のパスに切り替えるプロセスは、パスのフェイルオーバーと呼ばれます。

## ファイバチャネル SAN のポート

このドキュメントでは、ポートとはデバイスから SAN への接続を指します。SAN の各ノード、たとえばホスト、ストレージ デバイス、またはファブリック コンポーネントには、それぞれを SAN に接続する 1 つ以上のポートがあります。ポートは、いくつかの方法で識別できます。

### WWPN (World Wide Port Name)

グローバルで一意なポート ID であり、特定のアプリケーションがポートにアクセスできるようにします。FC スイッチは、デバイスまたはホストの WWPN を検出し、ポート アドレスをデバイスに割り当てます。

### Port\_ID (またはポート アドレス)

SAN では各ポートに一意のポート ID があり、ポートの FC アドレスとして機能します。この一意の ID によって、SAN 経由でそのポートにデータをルーティングできます。デバイスがファブリックにログインしたときに、FC スイッチはポート ID を割り当てます。ポート ID は、デバイスがログインしている間だけ有効です。

NPIV (N-Port ID Virtualization) を使用する場合、いくつかの WWPN を使用して 1 つの FC HBA ポート (N-port) をファブリックに登録できます。この方法により、N-port は複数のファブリック アドレスの獲得が可能で、それぞれのアドレスは固有のエンティティとして認識されます。ESXi ホストが SAN を使用している場合、これらの複数の一意の ID によって、構成の一環として各仮想マシンに WWN を割り当てることができます。

## ファイバチャネルストレージアレイのタイプ

ESXi では、さまざまなストレージ システムとアレイをサポートしています。

ホストでサポートされるストレージのタイプは、アクティブ-アクティブ、アクティブ-パッシブ、および ALUA 準拠です。

### アクティブ-アクティブのストレージ システム

大幅にパフォーマンスを低下させることなく、使用可能なすべてのストレージ ポートを通じて同時に LUN にアクセスできます。すべてのパスが常にアクティブな状態です (パスに障害が発生したときを除く)。

### アクティブ-パッシブのストレージ システム

1 つのストレージ プロセッサが特定の LUN にアクティブにアクセスを提供しているシステム。その他のプロセッサは、その LUN のバックアップとして機能し、ほかの LUN I/O にアクティブにアクセスを提供します。I/O は、特定の LUN のアクティブなポートにのみ送信できます。アクティブなストレージ ポートを経由したアクセスで障害が発生した場合、パッシブ ストレージ プロセッサの 1 つが、そこにアクセスしているサーバによってアクティブになります。

### 非対称ストレージ システム

非対称論理ユニット アクセス (ALUA) をサポートします。ALUA 準拠のストレージ システムは、ポートごとに異なるアクセス レベルを設定できます。ALUA を使用すると、ホストがターゲット ポートの状態を判別

し、バスに優先順位を付けることができます。ホストはプライマリとしてアクティブ バスのいくつかを使用し、その他をセカンダリとして使用します。

## ゾーニングとファイバ チャネル SAN との併用

ゾーニングは、SAN トポロジでのアクセス制御を提供します。ゾーニングは、どの HBA がどのターゲットに接続できるかを定義します。ゾーニングを使用して SAN を構成すると、ゾーン外のデバイスはゾーン内のデバイスから参照できなくなります。

ゾーニングには次の効果があります。

- ホストに提供されるターゲットと LUN の数が減ります。
- ファブリック内のバスを制御し隔離します。
- ESXi 以外のシステムが特定のストレージ システムにアクセスしないようにし、また VMFS データの破壊を予防できます。
- 異なる環境の分離に使用できます（テスト環境と本番環境など）。

ESXi ホストでは、1 イニシエータ ゾーニングまたは 1 ターゲット 1 イニシエータ ゾーニングを使用します。後者のゾーニングを推奨します。制約が多いゾーニングを使用すると、SAN で発生する可能性がある問題や構成エラーを防止できます。

詳細な手順およびゾーニングのベスト プラクティスについては、ストレージ アレイまたはスイッチのベンダーにお問い合わせください。

## 仮想マシンからファイバ チャネル SAN 上のデータへのアクセス方法

ESXi は、SAN ストレージ デバイスにある VMFS データストア内に、仮想マシンのディスク ファイルを格納します。仮想マシンのゲスト OS が仮想ディスクに SCSI コマンドを発行すると、SCSI 仮想化レイヤーがこれらのコマンドを VMFS ファイル操作に変換します。

仮想マシンが SAN 上の仮想ディスクと通信するとき、次の処理が実行されます。

- 1 仮想マシンのゲスト OS が SCSI ディスクに読み書きするとき、仮想ディスクに対して SCSI コマンドが発行されます。
- 2 仮想マシンのオペレーティング システムのデバイス ドライバが仮想 SCSI コントローラと通信します。
- 3 仮想 SCSI コントローラは、コマンドを VMkernel に転送します。
- 4 VMkernel は次の処理を実行します。
  - a ゲスト仮想マシン ディスクに対応する VMFS ボリュームにファイルを配置します。
  - b 仮想ディスクに対するブロックの要求を、適切な物理デバイスのブロックにマッピングします。
  - c 変更した I/O 要求を VMkernel のデバイス ドライバから物理 HBA に送信します。
- 5 物理 HBA は次の処理を実行します。
  - a FC プロトコルのルールに従い、I/O 要求をパッケージ化します。
  - b 要求を SAN に転送します。



- 6 HBA がファブリックへの接続に使用するポートに応じて、SAN スイッチのいずれかが要求を受信し、ホストがアクセスするストレージ デバイスにその要求をルーティングします。

# ファイバ チャネル ストレージの構成

# 4

SAN ストレージを使用した ESXi システムを使用する場合、特定のハードウェアおよびシステム要件があります。

この章には、次のトピックが含まれています。

- [ESXi ファイバ チャネル SAN の要件](#)
- [インストールおよびセットアップの手順](#)
- [N-Port ID の仮想化](#)

## ESXi ファイバ チャネル SAN の要件

SAN を構成し、ESXi システムを設定して SAN ストレージの使用準備をするときに、要件および推奨事項を確認してください。

- 使用する SAN ストレージのハードウェアとファームウェアの組み合わせが、ESXi システムとの併用でサポートされているか確認してください。最新のリストは、『VMware 互換性ガイド』を参照してください。
- 1 つの LUN につき 1 つの VMFS ボリュームのみ持つようシステムを構成してください。
- ディスクレス サーバを使用している場合を除き、SAN LUN に診断パーティションを設定しないでください。  
SAN から起動するディスクレス サーバの場合は、共有診断パーティションが適しています。
- RDM を使用して Raw ディスクにアクセスします。詳細については、[18 章 Raw デバイス マッピング](#) を参照してください。
- マルチパスが適切に機能するには、すべての ESXi ホストに対して、各 LUN が同じ LUN ID 番号を提示する必要があります。
- ストレージ デバイス ドライバが、十分に大きなキューを指定していることを確認します。物理 HBA のキューの深さは、システム セットアップで設定できます。HBA および仮想マシンのキューの深さの変更の詳細は、『vSphere トラブルシューティング』ドキュメントを参照してください。
- Microsoft Windows を実行する仮想マシンでは、SCSI の TimeoutValue パラメータの値を 60 に増やします。この増加により、Windows はパスのフェイルオーバーによって発生する遅延 I/O をさらに許容できます。詳細については、[Windows ゲスト OS にタイムアウトを設定](#) を参照してください。

## ESXi ファイバ チャンネル SAN の制限

ESXi と SAN を併用するときは、特定の制限が適用されます。

- ESXi は、FC 接続されたテープ デバイスをサポートしません。
- 仮想マシン内のマルチパス ソフトウェアを使用して、単一物理 LUN の I/O ロード バランシングを実行することはできません。ただし、Microsoft Windows 仮想マシンでダイナミック ディスクを使用している場合、この制限は適用されません。ダイナミック ディスクの構成方法については、[動的なディスクミラーリングの設定](#)を参照してください。

## LUN 割り当ての設定

ここでは、ESXi と SAN を組み合わせて使用する場合に、LUN を割り当てる方法の全般的な情報について説明します。

LUN 割り当てを設定するときは、次のことに注意してください。

### ストレージのプロビジョニング

起動時に ESXi システムが LUN を認識するように、SAN を ESXi システムに接続する前に、すべての LUN を適切な HBA にプロビジョニングします。

すべての LUN をすべての ESXi HBA に同時にプロビジョニングすることをお勧めします。HBA フェイルオーバーは、すべての HBA が同じ LUN を参照している場合にのみ機能します。

複数のホストで LUN を共有する場合は、すべてのホストで LUN ID が同じである必要があります。たとえば、LUN 5 は、ホスト 1、ホスト 2、およびホスト 3 に LUN 5 としてマッピングします。

### vMotion および VMware DRS

vCenter Server と vMotion または DRS を使用する場合は、仮想マシンの LUN がすべての ESXi ホストにプロビジョニングされていることを確認します。このようにすると、仮想マシンを移動する機能が最大になります。

### アクティブ-パッシブ アレイと比較したアクティブ-アクティブ アレイ

アクティブ-パッシブの SAN ストレージ デバイスで vMotion または DRS を使用する場合は、すべての ESXi システムが、すべてのストレージ プロセッサへの一貫したパスを保持するようにします。そうしない場合、vMotion の移行が行われるときに、パスのスラッシングが生じることがあります。

『ストレージ/SAN 互換性』にないアクティブ-パッシブ ストレージ アレイでは、ストレージ ポートのフェイルオーバーはサポートされません。この場合、サーバをストレージ アレイのアクティブなポートに接続する必要があります。この構成によって、LUN が ESXi ホストに確実に提供されます。

## ファイバ チャンネル HBA の設定

一般的に、ESXi ホストで使用する FC HBA は、デフォルト構成設定で問題なく動作します。

ストレージ アレイ ベンダーから提供される構成ガイドラインに従います。FC HBA をセットアップするときは、次について検討します。

- 1 台のホストでベンダーの異なる FC HBA を併用しないでください。同一の HBA でモデルが異なるものについてはサポートされていますが、2 つの異なる HBA タイプを介して 1 つの LUN にアクセスすることはできません。同じタイプからのみアクセスできます。
- 各 HBA のファームウェア レベルが同じであることを確認します。
- フェイルオーバー検出のタイムアウト値を設定します。最適なパフォーマンスを確保するには、デフォルト値を変更しないでください。
- ESXi は、エンドツーエンドの 16 GB ファイバ チャンネル接続をサポートしています。

## インストールおよびセットアップの手順

ここでは、SAN 環境を構成して ESXi システムと組み合わせるための、インストールとセットアップの手順の概要について説明します。

ESXi SAN 環境を構成するには、次の手順に従います。

- 1 SAN を構成していない場合、設計する。ほとんどの既存の SAN は、小さな変更だけで、ESXi と組み合わせることができます。
- 2 すべての SAN コンポーネントが要件を満たしていることを確認する。
- 3 ストレージ アレイに対して必要な変更を行う。  
  
VMware ESXi と組み合わせて動作するように SAN をセットアップする方法については、ほとんどのベンダーがベンダー固有のドキュメントを提供しています。
- 4 SAN に接続したホストの HBA を設定する。
- 5 ホストに ESXi をインストールする。
- 6 仮想マシンを作成し、ゲスト OS をインストールする。
- 7 (オプション) VMware HA フェイルオーバーまたは Microsoft Clustering Service を使用するように、システムをセットアップする。
- 8 必要に応じて環境をアップグレードまたは変更する。

## N-Port ID の仮想化

N-Port ID の仮想化 (NPIV) は ANSI T11 標準であり、これはいくつかの WWPN (World Wide Port Name) を使用して 1 つのファイバ チャンネル HBA ポートをファブリックに登録する方法について説明しています。これにより、ファブリックに接続した N-Port が複数のファブリック アドレスを要求できるようになります。各アドレスは、ファイバ チャンネル ファブリックで一意のエントリティとして認識されます。

## NPIV ベースの LUN アクセスの作動方法

NPIV は 1 つの FC HBA ポートを有効にして、複数の一意な WWN をファブリックに登録します。それぞれの WWN は各仮想マシンに割り当てることができます。

スイッチ、HBA、ストレージ デバイス、仮想マシンのような SAN オブジェクトには、WWN（World Wide Name）識別子を割り当てることができます。WWN はファイバ チャネル ファブリックにあるそれらのオブジェクトを一意的に識別します。仮想マシンに WWN が割り当てられている場合、仮想マシンはすべての RDM トラフィックに対してそれらの WWN 割り当てを使用します。こうすることで、仮想マシンの任意の RDM が参照する LUN が、WWN に対してマスクされないようにします。仮想マシンに WWN が割り当てられていない場合、仮想マシンは、ホストの物理 HBA の WWN を使用してストレージ LUN にアクセスします。ただし、NPIV を使用して、SAN のシステム管理者は仮想マシン 1 台ごとにストレージ アクセスの監視と経路設定ができます。次のセクションでは、この動作について説明します。

仮想マシンに WWN が割り当てられたときに、仮想マシンの構成ファイル（.vmx）は WWN のペア（WWPN（World Wide Port Name）と WWNN（World Wide Node Name））を含むようにアップデートされます。VMkernel は、仮想マシンをパワーオンしたときに、LUN へのアクセスで使用する物理 HBA で仮想ポート（VPORT）のインスタンスを作成します。VPORT は仮想 HBA であり、FC ファブリックには物理 HBA として認識されます。つまり、VPORT には一意の識別子（仮想マシンに割り当てられた WWN のペア）があります。各 VPORT は仮想マシンに特有のものです。仮想マシンをパワーオフすると、VPORT はホストで無効化され、FC ファブリックに認識されなくなります。仮想マシンが 1 つのホストから別のホストに移行すると、VPORT が最初のホスト上で閉じられ、ターゲット ホスト上で開かれます。

NPIV を有効にすると、作成時に各仮想マシンに対して WWN のペア（WWPN と WWNN）が指定されます。NPIV を使用している仮想マシンをパワーオンすると、仮想マシンはこれらの WWN ペアをそれぞれ順次使用して、ストレージへのアクセス パスを検出しようとします。インスタンス作成された VPORT の数は、ホストにある物理 HBA の数と同じです。VPORT は、物理パスが検出された各物理 HBA に作成されます。各物理パスを使用して、LUN へのアクセスに使用する仮想パスを決定します。NPIV に対応していない HBA は、HBA 上で VPORT をインスタンス作成できないため、この検出プロセスでスキップされることに注意してください。

## NPIV 使用の要件

NPIV を仮想マシン上で有効にする予定であれば、特定の要件に注意してください。

次の要件があります。

- NPIV は、RDM ディスクを使用する仮想マシンだけが使用できます。通常の仮想ディスクを使用する仮想マシンは、ホストの物理 HBA の WWN を使用します。
- ホストの HBA は NPIV をサポートしている必要があります。

詳細については、『VMware 互換性ガイド』およびベンダーのドキュメントを参照してください。

- 同じタイプの HBA、すべての QLogic とすべての Emulex のいずれかを使用してください。VMware では、同じホストにある異種の HBA から同じ LUN へのアクセスはサポートされていません。
- ホストが、ストレージへのパスとして複数の物理 HBA を使用している場合、すべての物理パスを仮想マシンにゾーニングする必要があります。一度に 1 つのパスだけがアクティブになる場合でも、マルチ パスをサポートする必要があります。
- ホスト上の物理 HBA が、そのホストで実行されている NPIV 対応の仮想マシンがアクセスするすべての LUN にアクセスできる必要があります。
- ファブリック内のスイッチは NPIV に対応している必要があります。

- ストレージ レベルでの NPIV アクセスに LUN を構成する場合、NPIV LUN の番号および NPIV ターゲット ID が、物理 LUN およびターゲット ID と一致していることを確認します。

## NPIV の機能と制限事項

ESXi で NPIV を使用する際の特定の機能と制限事項について説明します。

ESXi で NPIV を使用すると、次の項目がサポートされます。

- NPIV では vMotion がサポートされます。vMotion を使用して仮想マシンを移行するとき、割り当てられている WWN が維持されます。

NPIV 対応の仮想マシンを、NPIV をサポートしていないホストに移行すると、VMkernel は物理 HBA を使用した I/O の送信に戻ります。

- FC SAN 環境で、アクティブ-アクティブ アレイのディスクへの同時 I/O がサポートされている場合は、2 つの異なる NPIV ポートへの同時 I/O もサポートされます。

ESXi で NPIV を使用する場合は、次の制限事項が適用されます。

- NPIV テクノロジーは FC プロトコルの拡張であるので、FC スイッチを必要とし、直接接続の FC ディスクには使用できません。
- WWN が割り当てられている仮想マシンまたはテンプレートをクローン作成する場合、そのクローンは WWN を保持しません。
- NPIV で Storage vMotion はサポートされません。
- 仮想マシンの実行中に FC スイッチの NPIV 機能を無効にしてから再度有効にすると、FC リンクに障害が発生し、I/O が停止することがあります。

## 仮想マシンへの WWN の割り当て

WWN 設定を RDM ディスクを持つ仮想マシンに割り当てます。

1 ～ 16 個の WWN ペアを作成し、ホストの最初の 1 ～ 16 個の物理 FC HBA にマッピングできます。

### 前提条件

RDM ディスクを持つ仮想マシンを作成します。[RDM を使用する仮想マシンの作成](#) を参照してください。

### 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 仮想マシンを右クリックし、[設定の編集] を選択します。
- 3 [仮想マシン オプション] をクリックします。
- 4 ファイバ チャネル NPIV の三角形をクリックして、NPIV オプションを展開します。
- 5 [この仮想マシンのチェック ボックスの NPIV を] 一時的に無効にします。
- 6 [新しい WWN を生成する] を選択します。

## 7 WWNN と WWPN の数を指定します。

NPIV を使用したフェイルオーバーをサポートするには最低 2 つの WWPN が必要です。通常は各仮想マシンに WWNN を 1 つだけ作成します。

### 結果

ホストによって仮想マシンの WWN 割り当てが作成されます。

### 次のステップ

仮想マシンがスイッチにログインできるように、新規に作成した WWN をファブリックに登録し、ストレージ LUN を WWN に割り当てます。

## WWN 割り当ての変更

RDM を使用する仮想マシンについて、WWN 割り当てを変更できます。

通常は、仮想マシンの既存の WWN 割り当てを変更する必要はありません。ただし、手動で割り当てた WWN が原因で SAN で競合が発生している場合などの特定の状況では、WWN を変更または削除する必要があることがあります。

### 前提条件

既存の WWN を編集する場合、必ず仮想マシンをパワーオフしてください。

仮想マシンの ESXi ホストがストレージ LUN ACL にアクセスできるよう、SAN の管理者がストレージ LUN ACL をプロビジョニングしていることを事前に確認します。

### 手順

- 1 選択した仮想マシンの [設定の編集] リンクをクリックし、仮想マシンのプロパティ ダイアログ ボックスを開きます。
- 2 [オプション] タブをクリックし、[ファイバ チャネル NPIV] を選択します。  
仮想マシンのプロパティ ダイアログ ボックスが開きます。
- 3 次のいずれかのオプションを選択して、WWN の割り当てを編集します。

オプション	説明
この仮想マシンの NPIV を一時的に無効にする	仮想マシンの WWN の割り当てを無効にします。
変更しない	既存の WWN 割り当てを保持します。このダイアログ ボックスの読み取り専用の WWN の割り当てセクションに、既存の WWN 割り当てのノードとポートの値が表示されます。
新しい WWN を生成	新しい WWN を生成して仮想マシンに割り当て、既存の WWN を上書きします (HBA の WWN には影響しません)。
WWN 割り当ての削除	仮想マシンに割り当てられた WWN は削除され、仮想マシンは HBA WWN を使用してストレージ LUN にアクセスします。このオプションは、仮想マシンを新規作成する場合は利用できません。

- 4 [OK] をクリックして、変更内容を保存します。

# ファイバ チャンネル オーバー イーサネットの構成

# 5

ファイバ チャンネル ストレージにアクセスするために、ESXi ホストは FCoE (Fibre Channel over Ethernet) プロトコルを使用できます。

FCoE プロトコルは、ファイバ チャンネル フレームをイーサネット フレームにカプセル化します。その結果、ホストは特別なファイバ チャンネル リンクを使用してファイバ チャンネル ストレージに接続する必要がなくなり、10 Gbit ロスレス イーサネットを使用してファイバ チャンネル トラフィックを送信することができます。

この章には、次のトピックが含まれています。

- [ファイバ チャンネル オーバー イーサネット アダプタ](#)
- [ソフトウェア FCoE の構成ガイドライン](#)
- [ソフトウェア FCoE 用のネットワークの設定](#)
- [ソフトウェア FCoE アダプタの追加](#)

## ファイバ チャンネル オーバー イーサネット アダプタ

ファイバ チャンネル オーバー イーサネット (FCoE) を使用するには、ホストに FCoE アダプタをインストールする必要があります。

VMware がサポートするアダプタは通常、ハードウェア FCoE アダプタと、ESXi でネイティブの FCoE スタックを使用するソフトウェア FCoE アダプタの 2 つのカテゴリに分類されます。

### ハードウェア FCoE アダプタ

このカテゴリには、ネットワークおよびファイバ チャンネル機能が同じカードに搭載されている完全にオフロードされた専用の統合ネットワーク アダプタ (CNA) が含まれます。

このようなアダプタを取り付けると、ホストで両方の CNA コンポーネントが検出され、使用できます。クライアントでは、ネットワーク コンポーネントは標準ネットワーク アダプタ (vmnic) として、ファイバ チャンネル コンポーネントは FCoE アダプタ (vmhba) として表示されます。ハードウェア FCoE アダプタを使用するためには構成する必要がありません。



## ソフトウェア FCoE アダプタ

ソフトウェア FCoE アダプタはプロトコル処理に ESXi でネイティブの FCoE プロトコル スタックを使用します。ソフトウェア FCoE アダプタは、Data Center Bridging (DCB) と I/O オフロード機能を提供する NIC と使用されます。Intel X520 はこのような NIC の一例です。ソフトウェア FCoE をサポートする NIC については、『VMware 互換性ガイド』を参照してください。

ソフトウェア FCoE アダプタの場合は、ネットワークを適切に構成してからアダプタを有効にする必要があります。

---

**注：** 有効にするソフトウェア FCoE アダプタの数は、物理 NIC ポートの数に相当します。ESXi は、1 台のホスト上で最大 4 つのソフトウェア FCoE アダプタをサポートします。

---

## ソフトウェア FCoE の構成ガイドライン

ESXi ソフトウェア FCoE で作業をするようにネットワーク環境を設定するときに、VMware が提供するガイドラインとベスト プラクティスに従ってください。

### ネットワーク スイッチ ガイドライン

ソフトウェア FCoE 環境のためにネットワーク スイッチを構成するときは次のガイドラインに従ってください。

- ESXi ホストと通信するポートで、スパニング ツリー プロトコル (STP) を無効にします。STP を有効にすると、スイッチで FCoE Initialization Protocol (FIP) の応答が遅延し、APD (すべてのパスがダウン) 状態が発生する場合があります。  
  
FIP は、イーサネット上で FCoE エンティティを検出して初期化するために FCoE が使用するプロトコルです。
- Priority-based Flow Control (PFC) をオンにして AUTO に設定します。
- FCoE スイッチに互換性のあるファームウェア バージョンがあることを確認します。

### ネットワーク アダプタのベスト プラクティス

ネットワーク アダプタで作業をするためにソフトウェア FCoE アダプタを有効にする予定がある場合には、特定の考慮事項が適用されます。

- 最新のマイクロコードが FCoE ネットワーク アダプタにインストールされていることを確認します。
- ネットワーク アダプタにポートが複数ある場合に、ネットワークを構成するときは、各ポートを個別の vSwitch に追加します。この方法によって、MTU 変更などの障害が発生したときに APD 状態を回避することができます。
- FCoE トラフィックがアクティブのときに 1 つの vSwitch から別の vSwitch にネットワーク アダプタ ポートを移動しないでください。この変更が必要な場合には、あとでホストを再起動します。
- ネットワーク アダプタ ポートのために vSwitch を変更して障害が発生した場合には、ポートを元の vSwitch に戻すと問題は解決します。

## ソフトウェア FCoE 用のネットワークの設定

ソフトウェア FCoE アダプタを有効にする前に、ホストにインストールされているすべての物理 FCoE NIC に VMkernel ネットワーク アダプタを作成する必要があります。

この手順は、単一の FCoE 物理ネットワークアダプタに vSphere 標準スイッチを介して接続された単一の VMkernel ネットワーク アダプタの作成方法を説明するものです。ホストに複数のネットワーク アダプタがある場合、またはアダプタに複数のポートがある場合、それぞれの FCoE NIC を別々の標準スイッチに接続します。詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

---

**注：** ESXi では、ソフトウェア FCoE で使用するネットワーク アダプタ ポートを最大で 4 つサポートします。

---

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [アクション] - [ネットワークの追加] の順にクリックします。
- 3 [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
- 4 [新しい標準スイッチ] を選択して、vSphere 標準スイッチを作成します。
- 5 [請求されていないアダプタ] で、FCoE をサポートするネットワーク アダプタ (vmnic#) を選択して、[割り当て] をクリックします。  
  
[アクティブ アダプタ] にアダプタが割り当てられていることを確認します。
- 6 ネットワーク ラベルを入力します。  
  
ネットワーク ラベルは、「FCoE」など、作成する VMkernel アダプタを識別する分かりやすい名前です。
- 7 VLAN ID を指定し、[次へ] をクリックします。  
  
FCoE トラフィックには分離されたネットワークが必要であるため、入力する VLAN ID は、ホスト上で通常のネットワークに使用されるものとは異なっている必要があります。詳細については、『vSphere ネットワーク』ドキュメントを参照してください。
- 8 構成を完了し、情報を確認して、[終了] をクリックします。

### 結果

これで、ホストにインストールされた物理 FCoE ネットワーク アダプタ用の仮想 VMkernel アダプタが作成されました。

---

**注：** FCoE トラフィックの中断を防ぐため、FCoE ネットワークを設定した後は、FCoE ネットワーク アダプタ (vmnic#) を vSphere 標準スイッチから外さないでください。

---

## ソフトウェア FCoE アダプタの追加

ホストがファイバ チャネル ストレージにアクセスする際に使用できるようソフトウェア FCoE アダプタを有効にする必要があります。

有効にできるソフトウェア FCoE アダプタの数は、ホスト上にある物理的な FCoE NIC ポートの数に相当します。ESXi は、1 台のホスト上で最大 4 つのソフトウェア FCoE アダプタをサポートします。

#### 前提条件

ソフトウェア FCoE アダプタについてネットワークを設定します。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ]、[追加] アイコン (➕) の順にクリックします。
- 4 [ソフトウェア FCoE アダプタ] を選択します。
- 5 [ソフトウェア FCoE アダプタの追加] ダイアログ ボックスで、物理ネットワーク アダプタのドロップダウン リストから適切な vmnic を選択します。

FCoE トラフィックで使用されていないアダプタのみがリストに表示されます。

- 6 [OK] をクリックします。

ソフトウェア FCoE アダプタが、ストレージ アダプタのリストに表示されます。

#### 結果

ソフトウェア FCoE アダプタを有効にすると、そのプロパティを表示できます。アダプタを使用しない場合は、そのアダプタをアダプタ リストから削除できます。

# ファイバ チャネル SAN からの ESXi の起動

# 6

SAN から起動するようにホストを設定すると、ホストの起動イメージが SAN ストレージ システム内の 1 つ以上の LUN に格納されます。ホストが起動するとき、ローカル ディスクではなく、SAN の LUN から起動します。

ESXi は、ファイバ チャネル ホスト バス アダプタ (HBA) または FCoE (Fibre Channel over Ethernet) 統合ネットワーク アダプタ (CNA) を通した起動をサポートしています。

この章には、次のトピックが含まれています。

- SAN から起動のメリット
- ファイバ チャネル SAN からの起動の要件と考慮事項
- SAN から起動するための準備
- SAN から起動する Emulex HBA の構成
- SAN から起動する QLogic HBA の構成

## SAN から起動のメリット

SAN からの起動には、環境に対して多くのメリットがあります。ただし、SAN からの起動が ESXi ホストに適していない場合もあります。SAN から起動するようにシステムを設定する前に、SAN からの起動が使用中の環境に適しているかどうかを判断します。

---

**注意：** 複数の ESXi ホストと一緒に SAN からの起動を使用する場合、ホストごとに独自の起動 LUN が必要です。複数のホストが同じ起動 LUN を共有するように構成すると、ESXi イメージが破損する可能性があります。

---

SAN からの起動を使用した場合、環境には次のメリットがあります。

- サーバが安価になる。内部ストレージが不要になるため、サーバの密度を高くしたり動作時の温度を抑えたりできます。
- サーバの交換が簡単になる。サーバを交換して、新しいサーバが古い起動場所を参照するようにできます。
- 無駄になる領域が減る。ローカル ディスクがないサーバは一般に使用領域が少なくなります。
- バックアップ プロセスが簡単になる。SAN のシステム起動イメージは、SAN 全体のバックアップ プロシージャの一部としてバックアップできます。また、起動イメージに対して、スナップショットなどの高度なアレイ機能を使用することもできます。
- 管理がしやすくなる。オペレーティング システム イメージの作成と管理が簡単になり、より効率的になります。

- 信頼性が向上する。複数のバスを使用して起動ディスクにアクセスできるので、ディスクが単一点障害になりません。

## ファイバ チャネル SAN からの起動の要件と考慮事項

ESXi 起動構成は、特定の要件を満たす必要があります。

表 6-1. SAN からの起動の要件

要件	説明
ESXi システム要件	SAN から起動するサーバに対するベンダーの推奨事項に従います。
アダプタの要件	アダプタを有効にし、適切に構成することで、起動 LUN にアクセスできるようにします。ベンダーのドキュメントを参照してください。
アクセス コントロール	<ul style="list-style-type: none"> <li>■ 各ホストは、ほかのホストの起動 LUN ではなく、自分の起動 LUN だけにアクセスする必要があります。ストレージ システム ソフトウェアを使用して、ホストが、指定した LUN だけにアクセスすることを確認します。</li> <li>■ 複数のサーバで診断のパーティションを共有できます。これは、アレイ固有の LUN マスキングを使用して可能です。</li> </ul>
マルチバスのサポート	アクティブ-パッシブ アレイでは、起動 LUN へのマルチバスはサポートされていません。BIOS でマルチバスはサポートされず、スタンバイ バスをアクティブにできないからです。
SAN に関する考慮事項	アレイで直接接続トポロジが保証されていない場合、SAN 接続はスイッチ ファブリック トポロジを経由する必要があります。アレイで直接接続トポロジが保証されている場合、SAN をアレイに直接接続できます。SAN からの起動は、スイッチ トポロジと直接接続トポロジが特定のアレイで保障されている場合、両方のトポロジでサポートされています。
ハードウェア固有の考慮事項	IBM eServer BladeCenter を実行し、SAN からの起動を使用する場合、ブレードの IDE ドライブを無効にする必要があります。

## SAN から起動するための準備

SAN から起動する環境を設定する場合は、いくつかの作業を行います。

本セクションでは、ラック マウント サーバで SAN からの起動を有効にするための一般的な手順を示します。Cisco Unified Computing System FCoE ブレード サーバにおける SAN からの起動の有効化については、Cisco のドキュメントを参照してください。

### 手順

#### 1 SAN コンポーネントとストレージ システムの構成

SAN LUN から起動するように ESXi ホストを設定する前に、SAN コンポーネントとストレージ システムを構成します。

#### 2 SAN から起動するストレージ アダプタの構成

SAN から起動するようにホストを設定する場合は、ホスト BIOS で起動アダプタを有効にします。その後、ターゲット起動 LUN への初期接続を開始するように起動アダプタを構成します。

#### 3 インストール メディアから起動するためのシステムの設定

SAN から起動するようにホストを設定するときは、最初に VMware のインストール メディアからホストを起動します。そのためには、BIOS セットアップでシステムの起動シーケンスを変更する必要があります。

## SAN コンポーネントとストレージ システムの構成

SAN LUN から起動するように ESXi ホストを設定する前に、SAN コンポーネントとストレージ システムを構成します。

SAN コンポーネントの構成はベンダーによって異なるので、各コンポーネントの製品ドキュメントを参照してください。

### 手順

- 1 ネットワーク ケーブルを接続します。現在の環境に該当する配線ガイドを参照してください。  
スイッチの接続がある場合、確認します。
- 2 ストレージ アレイを構成します。
  - a SAN ストレージ アレイから、SAN で ESXi ホストを参照できるようにします この操作をオブジェクトの作成と呼びます。
  - b SAN ストレージ アレイから、ホストのアダプタの WWPN がポート名またはノード名になるようにホストを設定します。
  - c LUN を作成します。
  - d LUN を割り当てます。
  - e スイッチとストレージ アレイの IP アドレスを記録します。
  - f 各 SP の WWPN を記録します。

---

**注意：** インストール スクリプトを使用して、SAN からの起動モードで ESXi をインストールする場合は、誤ってデータが失われないように特別な手順を実行する必要があります。

---

## SAN から起動するストレージ アダプタの構成

SAN から起動するようにホストを設定する場合は、ホスト BIOS で起動アダプタを有効にします。その後、ターゲット起動 LUN への初期接続を開始するように起動アダプタを構成します。

### 前提条件

ストレージ アダプタの WWPN を確認します。

### 手順

- ◆ SAN から起動するようストレージ アダプタを構成します。  
起動アダプタの構成はベンダーによって異なるので、ベンダーのドキュメントを参照してください。

## インストール メディアから起動するためのシステムの設定

SAN から起動するようにホストを設定するときは、最初に VMware のインストール メディアからホストを起動します。そのためには、BIOS セットアップでシステムの起動シーケンスを変更する必要があります。

BIOS で起動シーケンスを変更する方法はベンダーによって異なるので、変更手順については、ベンダーのドキュメントを参照してください。次の手順では、IBM のホストで起動シーケンスを変更する方法を示します。

#### 手順

- 1 システムを起動するときに、システムの BIOS 構成または設定のユーティリティに入ります。
- 2 [起動オプション] を選択し、[Enter] を押します。
- 3 [起動シーケンス オプション] を選択し、[Enter] を押します。
- 4 [最初の起動デバイス] を [CD-ROM] に変更します。

#### 結果

これで、ESXi をインストールできます。

## SAN から起動する Emulex HBA の構成

SAN から起動するように Emulex HBA BIOS を構成するには、BootBIOS プロンプトの有効化および BIOS の有効化を行います。

#### 手順

##### 1 BootBIOS プロンプトの有効化

SAN から ESXi を起動するよう Emulex HBA BIOS を構成するには、BootBIOS プロンプトを有効にする必要があります。

##### 2 BIOS の有効化

SAN から ESXi を起動するよう Emulex HBA BIOS を構成するには、BIOS を有効にする必要があります。

## BootBIOS プロンプトの有効化

SAN から ESXi を起動するよう Emulex HBA BIOS を構成するには、BootBIOS プロンプトを有効にする必要があります。

#### 手順

- 1 `lputil` を実行します。
- 2 [3. ファームウェアのメンテナンス] を選択します。
- 3 アダプタを選択します。
- 4 [6. 起動 BIOS のメンテナンス] を選択します。
- 5 [1. 起動 BIOS の有効化] を選択します。

## BIOS の有効化

SAN から ESXi を起動するよう Emulex HBA BIOS を構成するには、BIOS を有効にする必要があります。

#### 手順

- 1 ホストを再起動します。

- 2 アダプタのパラメータを構成するには、Emulex のプロンプトで [ALT] + [E] を押して次の手順に従います。
  - a アダプタ（および BIOS サポート）を選択します。
  - b [2. このアダプタのパラメータを構成] を選択します。
  - c [1. BIOS の有効化または無効化] を選択します。
  - d [1] を選択して BIOS を有効にします。
  - e [x] を選択して終了し、[Esc] を選択して前のメニューに戻ります。
- 3 起動デバイスを構成するには、Emulex のメイン メニューから次の手順に従います。
  - a 同じアダプタを選択します。
  - b [1. 起動デバイスの構成] を選択します。
  - c 起動エントリーの場所を選択します。
  - d 2 桁の起動デバイスを入力します。
  - e 2 桁（16 進数）の起動 LUN を入力します（08 など）。
  - f 起動 LUN を選択します。
  - g [1. WWPN] を選択します（DID ではなく WWPN を使用してこのデバイスを起動します）。
  - h [x] を選択して終了し、[Y] を選択して再起動します。
- 4 起動してシステム BIOS に入り、起動コントローラ シーケンスで Emulex を先頭に移動します。
- 5 SAN LUN で再起動し、インストールします。

## SAN から起動する QLogic HBA の構成

この手順の例では、ESXi を SAN から起動するように QLogic HBA を構成する方法を説明します。この手順では、QLogic HBA BIOS を有効にし、選択可能な起動を有効にし、起動 LUN を選択します。

### 手順

- 1 サーバが起動する間に、[Ctrl] + [Q] を押して Fast!UTIL 構成ユーティリティを開始します。
- 2 HBA の数に応じて、適切な操作を実行します。

オプション	説明
1つの HBA	ホスト バス アダプタ（HBA）が 1 つだけの場合、Fast!UTIL Options ページが表示されます。 <a href="#">手順 手順 3</a> に進みます。
複数の HBA	<p>複数の HBA がある場合は、HBA を手動で選択します。</p> <ol style="list-style-type: none"> <li>a ホスト アダプタの選択ページで矢印キーを使用して、適切な HBA にカーソルを移動します。</li> <li>b [Enter] を押します。</li> </ol>

- 3 Fast!UTIL Options ページで、[構成設定] を選択し、[Enter] を押します。
- 4 構成設定ページで、[アダプタの設定] を選択し、[Enter] を押します。



- 5 SCSI デバイスを検索する BIOS を設定します。
  - a ホスト アダプタの設定ページで [ホスト アダプタ BIOS] を選択します。
  - b [Enter] を押して値を有効に切り替えます。
  - c [Esc] を押して終了します。
- 6 選択可能な起動を有効にします。
  - a [選択可能な起動の設定] を選択して [Enter] を押します。
  - b 選択可能な起動の設定ページで [選択可能な起動] を選択します。
  - c [Enter] を押して値を [有効] に切り替えます。
- 7 カーソル キーを使用して、ストレージ プロセッサ (SP) のリストで起動ポート名のエントリを選択し、[Enter] を押してファイバ チャネル デバイスの選択画面を開きます。
- 8 カーソル キーを使用して、特定の SP を選択し、[Enter] を押します。
 

アクティブ-パッシブ ストレージ アレイを使用する場合、選択した SP を起動 LUN への優先 (アクティブな) バスに置く必要があります。どちらの SP がアクティブなバスにあるかわからない場合は、ストレージ アレイ管理ソフトウェアを使用して調べます。ターゲット ID は BIOS で作成され、再起動ごとに変わる可能性があります。
- 9 SP に接続されている LUN の数に応じて、適切な操作を実行します。

オプション	説明
LUN が 1 つの場合	その LUN が起動 LUN として選択されます。LUN の選択画面を使用する必要はありません。
LUN が複数の場合	LUN の選択画面が開きます。カーソルを使用して起動 LUN を選択し、[Enter] を押します。

- 10 その他のストレージ プロセッサがリストに表示される場合は、[C] を押してデータをクリアします。
- 11 [Esc] を 2 回押して終了し、[Enter] を押して設定を保存します。

# ソフトウェア FCoE による ESXi のブート

# 7

ESXi は、FCoE 対応のネットワーク アダプタからのブートをサポートしています。

ESXi をインストールして FCoE LUN からブートを行う場合は、ホストは VMware software FCoE アダプタおよび FCoE 機能を持つネットワーク アダプタを使用することができます。ホストには専用の FCoE HBA は必要ありません。

ほとんどの構成は、ネットワーク アダプタのオプション ROM から実行できます。ネットワーク アダプタは次のいずれかの形式をサポートしている必要があります。この形式を使用して FCoE ブート デバイスに関するパラメータが VMkernel に送信されます。

- FCoE Boot Firmware Table (FBFT)。FBFT は Intel の登録商標です。
- FCoE Boot Parameter Table (FBPT)。FBPT は、サードパーティ ベンダーがソフトウェア FCoE ブートを実装するために VMware によって定義されたものです。

構成パラメータはアダプタのオプション ROM に設定されます。ESXi インストールまたはその後のブートの間に、これらのパラメータが FBFT 形式または FBPT 形式でシステム メモリにエクスポートされます。VMkernel は構成設定を読み取り、それらを使用してブート LUN にアクセスします。

この章には、次のトピックが含まれています。

- [ソフトウェア FCoE 起動の要件と考慮事項](#)
- [ソフトウェア FCoE ブートのベスト プラクティス](#)
- [ソフトウェア FCoE ブートの設定](#)
- [ソフトウェア FCoE からのインストールおよび起動のトラブルシューティング](#)

## ソフトウェア FCoE 起動の要件と考慮事項

ソフトウェア FCoE を使用して SAN から ESXi ホストを起動する場合は、一定の要件と考慮事項が適用されます。

### 要件

- ESXi 5.1 以降 である必要があります。
- ネットワーク アダプタは次の機能を持つ必要があります。
  - FCoE に対応している。
  - ESXi オープン FCoE スタックをサポートしている。

- FBFT 形式または FBPT 形式で起動情報をエクスポートできる FCoE ブート ファームウェアを搭載している。

## 考慮事項

- ESXi からソフトウェア FCoE ブート構成を変更することはできません。
- コアダンプは、起動 LUN を含めて、すべてのソフトウェア FCoE LUN でサポートされていません。
- 起動前のマルチパスはサポートされていません。
- 起動 LUN は、共有ストレージ上であっても他のホストと共有できません。

## ソフトウェア FCoE ブートのベスト プラクティス

ソフトウェア FCoE LUN からシステムをブートするには、推奨のベスト プラクティスがいくつかあります。

- ホストがブート LUN 全体にアクセスできることを確認します。共有ストレージ上であっても、ブート LUN は別のホストと共有できません。
- Intel 10 ギガビット イーサネット コントローラ (Niantec) を Cisco スイッチで使用している場合、スイッチポートを次のように構成します。
  - スパニング ツリー プロトコル (STP) を有効にする。
  - FCoE に使用している VLAN の `switchport trunk native vlan` をオフにする。

## ソフトウェア FCoE ブートの設定

ESXi ホストは、ソフトウェア FCoE アダプタ、ネットワークアダプタを使用して FCoE LUN から起動できます。

ホストをソフトウェア FCoE ブート用に構成するには、いくつかの作業を行います。

### 前提条件

ネットワーク アダプタには次の機能があります。

- 部分的 FCoE オフロードをサポート (ソフトウェア FCoE)。
- FCoE ブート ファームウェア テーブル (FBFT) または FCoE ブート パラメータ テーブル (FBPT) の何れかを含む。

ソフトウェア FCoE ブートをサポートするネットワーク アダプタについては、『VMware 互換性ガイド』を参照してください。

### 手順

#### 1 ソフトウェア FCoE ブート パラメータの構成

ソフトウェア FCoE ブート プロセスをサポートするには、ホスト上のネットワーク アダプタに、特別に構成された FCoE ブート ファームウェアが必要です。ファームウェアを構成するとき、アダプタでソフトウェア FCoE ブートを有効にし、起動 LUN パラメータを指定します。

## 2 ソフトウェア FCoE LUN からの ESXi のインストールと起動

ソフトウェア FCoE LUN から起動するようにシステムを設定するとき、ESXi イメージをターゲット LUN にインストールします。LUN からホストを起動できるようになります。

### ソフトウェア FCoE ブート パラメータの構成

ソフトウェア FCoE ブート プロセスをサポートするには、ホスト上のネットワーク アダプタに、特別に構成された FCoE ブート ファームウェアが必要です。ファームウェアを構成するとき、アダプタでソフトウェア FCoE ブートを有効にし、起動 LUN パラメータを指定します。

#### 手順

- ◆ ネットワーク アダプタのオプションの ROM で、ソフトウェア FCoE ブート パラメータを指定します。

これらのパラメータには、起動ターゲット、起動 LUN、VLAN ID などが含まれます。

ネットワーク アダプタの構成はベンダーによって異なるので、構成方法についてはベンダーのドキュメントを参照してください。

### ソフトウェア FCoE LUN からの ESXi のインストールと起動

ソフトウェア FCoE LUN から起動するようにシステムを設定するとき、ESXi イメージをターゲット LUN にインストールします。LUN からホストを起動できるようになります。

#### 前提条件

- ネットワーク アダプタのオプション ROM が、起動 LUN として使用するターゲット LUN を参照するように設定します。起動可能な LUN についての情報を保有していることを確認します。
- システム BIOS の起動順を次のシーケンスに変更します。

a ソフトウェア FCoE ブートに使用するネットワーク アダプタ。

b ESXi インストール メディア。

システムのベンダーが提供するドキュメントを参照してください。

#### 手順

- 1 ESXi のインストール CD/DVD から、対話形式のインストールを開始します。

ESXi インストーラは、BIOS で FCoE ブートが有効化されていることを確認し、必要に応じて FCoE 対応のネットワーク アダプタの標準仮想スイッチを作成します。vSwitch の名前は、VMware\_FCoE\_vSwitch です。その後インストーラは、事前構成済みの FCoE ブート パラメータを使用し、使用可能なすべての FCoE LUN を検出し、表示します。

- 2 [ディスクの選択] 画面で、起動パラメータ設定で指定したソフトウェア FCoE LUN を選択します。

このメニューに起動 LUN が表示されない場合は、ネットワーク アダプタのオプション ROM の起動パラメータが正しく構成されていることを確認してください。

- 3 プロンプトの指示に従って、インストールを完了します。

- 4 ホストを再起動します。

- 5 FCoE ブート LUN が起動可能な最初のデバイスとなるようにシステム BIOS の起動順を変更します。

ESXi は、使用の準備が整うまで、ソフトウェア FCoE LUN から起動を続けます。

#### 次のステップ

必要に応じて、VMware\_FCoE\_vSwitch の名前を変更し、インストーラが自動的に作成されるように変更することができます。シスコ検出プロトコル (CDP) モードが [待機] または [両方] に設定されていることを確認します。

## ソフトウェア FCoE からのインストールおよび起動のトラブルシューティング

ソフトウェア FCoE LUN からの ESXi のインストールまたは起動が失敗した場合、いくつかのトラブルシューティングの方法を使用できます。

#### 問題

FCoE ストレージから VMware ソフトウェア FCoE アダプタおよび部分的な FCoE オフロード機能を搭載したネットワーク アダプタを使用して ESXi をインストールまたは起動すると、インストールまたは起動プロセスが失敗します。

#### 解決方法

- FCoE ネットワーク アダプタのオプション ROM の起動パラメータが正しく構成されていることを確認します。
- インストール中に、FCoE ネットワーク アダプタの BIOS にエラーがないか監視します。
- 可能であれば、VMkernel ログにエラーがないか確認します。
- `esxcli` コマンドを使用して、起動 LUN が存在するかどうかを確認します。

```
esxcli conn_options hardware bootdevice list
```

# ファイバチャネルストレージのベストプラクティス

## 8

ESXi をファイバチャネル SAN と使用する場合には、パフォーマンスの問題を回避するために VMware が提供するベストプラクティスに従ってください。

vSphere Web Client は、パフォーマンス情報を収集するための幅広い機能を提供します。情報がグラフィカルに表示され、頻繁に更新されます。

resxtop または esxtop コマンドラインユーティリティを使用することも可能です。このユーティリティでは、ESXi がリアルタイムでリソースをどのように使用するかについての詳細情報が提示されます。詳細については、『vSphere リソース管理』ドキュメントを参照してください。

ストレージシステムが Storage API - Array Integration ハードウェアアクセラレーション機能をサポートしているかどうかを、ストレージの担当者にご確認ください。サポートしている場合には、ハードウェアアクセラレーションのサポートをストレージシステム側で有効にする方法はベンダーのドキュメントを参照してください。詳細については、[23 章 ストレージのハードウェアアクセラレーション](#) を参照してください。

この章には、次のトピックが含まれています。

- [ファイバチャネル SAN の問題の防止](#)
- [自動ホスト登録の無効化](#)
- [ファイバチャネル SAN ストレージパフォーマンスの最適化](#)

## ファイバチャネル SAN の問題の防止

ESXi をファイバチャネル SAN と併用する場合、SAN の問題を回避するために特別なガイドラインに従う必要があります。

SAN 構成に関する問題を防止するためのいくつかのヒントを示します。

- 各 LUN には、VMFS データストアを 1 つだけ配置します。
- バスポリシーの変更について熟知していない場合は、システムで設定されているバスポリシーをそのまま使用します。
- すべてを文書化します。これには、ゾーニング、アクセスコントロール、ストレージ、スイッチ、サーバと FC HBA の構成、ソフトウェアとファームウェアのバージョン、およびストレージケーブル計画に関する情報が含まれます。

- 障害に対する計画を立てます。
  - トポロジ マップの複製をいくつか作成します。エレメントごとに、エレメントに障害が発生した場合の SAN への影響を検討します。
  - 設計上の重大な障害を見落とさないように、さまざまなリンク、スイッチ、HBA、およびその他のエレメントを削除します。
- ファイバ チャンネル HBA が、スロットとバス速度を基準として、ホストの正しいスロットにインストールされていることを確認します。サーバで利用できるバス間で、PCI バスの負荷を分散します。
- ホストのパフォーマンス チャート、FC スイッチ統計情報、ストレージ パフォーマンス統計情報など、すべての参照できるポイントで、ストレージ ネットワークのさまざまな監視ポイントに関する情報を得ます。
- ESXi ホストで使用されている VMFS データストアを持つ LUN の ID の変更時には、注意が必要です。ID を変更すると、データストアは非アクティブとなり、仮想マシンは停止します。データストアを再署名して再度アクティブにすることができます。[重複 VMFS データストアの管理](#) を参照してください。

VMFS データストア上で実行中の仮想マシンがない場合、LUN の ID を変更したあとで、再スキャンを実行してホストの ID をリセットする必要があります。再スキャンについては、[ストレージの更新操作および再スキャン操作](#) を参照してください。

## 自動ホスト登録の無効化

特定のストレージ アレイでは、ESXi ホストがアレイに登録されている必要があります。ESXi は、アレイにホスト名と IP アドレスを送信することによって、ホストを自動的に登録します。ストレージ管理ソフトウェアを使用して手動で登録する場合は、ESXi の自動登録機能を無効にします。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [システム] メニューの [システムの詳細設定] をクリックします。
- 4 [システムの詳細設定] で、[Disk.EnableNaviReg] パラメータを選択し、[編集] アイコンをクリックします。
- 5 値を 0 に変更します。

### 結果

これによって、デフォルトで有効になっている自動ホスト登録が無効になります。

## ファイバ チャンネル SAN ストレージ パフォーマンスの最適化

一般的な SAN 環境の最適化には、いくつかの要因があります。

環境が適切に構成されている場合、SAN ファブリック コンポーネント（特に SAN スイッチ）は、サーバやストレージ アレイと比べて待ち時間が低いため、あまり影響を与えません。スイッチ ファブリックのバスが飽和していない、つまりスイッチ ファブリックが最高のスループットで動作していることを確認してください。

## ストレージ アレイ パフォーマンス

ストレージ アレイのパフォーマンスは、SAN 環境全体のパフォーマンスに影響する主要な要因の 1 つです。

ストレージ アレイのパフォーマンスに問題がある場合は、ストレージ アレイのベンダーのドキュメントで関連情報を調べてください。

vSphere 環境でアレイのパフォーマンスを向上させるためには、次の全般的なガイドラインに従ってください。

- LUN を割り当てるときは、各 LUN が多くのホストからアクセスされ、各ホストで多くの仮想マシンが実行される可能性があることに注意してください。1 つのホストで使用される 1 つの LUN が、異なるオペレーティング システムで実行される多様なアプリケーションからの I/O を提供する可能性があります。このような場合はさまざまなワークロードが発生するため、ESXi LUN を含む RAID グループには、ESXi を実行していないその他のサーバが使用する LUN を含めないでください。
- 読み取り/書き込みキャッシュが有効であることを確認します。
- SAN ストレージ アレイは、I/O がすべてのストレージ アレイ パス間でロード バランシングされるように、継続的な再設計と調整を必要とします。この要件を満たすために、すべての SP 間で LUN へのパスを分散し、最適なロード バランシングを提供します。詳細な監視によって、LUN の分散を再調整する必要がある時期が示されます。

静的にバランスがとられたストレージ アレイの調整は、特定のパフォーマンス統計情報（1 秒あたりの I/O 動作数、1 秒あたりのブロック数、応答時間など）を監視し、LUN のワークロードをすべての SP に分散して行います。

---

**注：** 現在、ESXi ではダイナミック ロード バランシングはサポートされていません。

---

## ファイバ チャネルによるサーバ パフォーマンス

サーバ パフォーマンスを最適にするために考慮しなければならない点がいくつかあります。

各サーバ アプリケーションは、次の条件を満たしながら、目的のストレージにアクセスできる必要があります。

- 高い I/O レート（1 秒あたりの I/O 処理数）
- 高いスループット（1 秒あたりのメガバイト数）
- 最小限の待ち時間（応答時間）

アプリケーションごとに要件は異なるため、ストレージ アレイの適切な RAID グループを選択することで、これらの目標を達成できます。パフォーマンスの目標を達成するには、次のようにします。

- 各 LUN を、必要なパフォーマンス レベルを提供する RAID グループに配置する。割り当てられた RAID グループにあるほかの LUN のアクティビティおよびリソース使用率に注意してください。I/O を行うアプリケーションが多すぎる高性能 RAID グループは、ESXi ホストで実行されるアプリケーションで要求されるパフォーマンス目標を達成できないことがあります。
- 各サーバに、サーバがホスティングするすべてのアプリケーションでピーク時に最大のスループットが得られるだけの十分な数の HBA があることを確認する。I/O を複数の HBA に分散させることで、どのアプリケーションでもスループットが高くなり、待ち時間が短くなります。



- HBA に障害が発生した場合に備えて冗長性を提供するために、サーバが二重冗長ファブリックに接続されていることを確認する。
- ESXi システムに LUN または RAID グループを割り当てるときは、複数のオペレーティング システムがそのリソースを使用および共有する。結果として、ESXi システムを使用する場合にストレージ サブシステムの各 LUN で要求されるパフォーマンスは、物理マシンを使用する場合よりも高くなる場合があります。たとえば、I/O の多いアプリケーションを 4 つ実行しようとする場合は、ESXi LUN に 4 倍のパフォーマンス キャパシティを割り当てます。
- 複数の ESXi システムを vCenter Server と組み合わせて使用する場合は、それに対応して、ストレージ サブシステムのパフォーマンスを高くする。
- ESXi システムで実行されるアプリケーションが要求する未実行 I/O 数を、HBA およびストレージ アレイで処理できる I/O 数と一致させる。

# iSCSI SAN と ESXi との併用

# 9

ESXi は、ストレージ エリア ネットワーク (SAN) で使用できます。SAN は、高性能ストレージ サブシステムにコンピュータ システムを接続することに特化した高速ネットワークです。ESXi を SAN で使用すると、ストレージが統合され、信頼性が向上し、ディザスタ リカバリ時に役立ちます。

ESXi と SAN を効果的に使用するには、ESXi システムと SAN の概念について、実用的な知識が必要です。また、インターネット SCSI (iSCSI) SAN ストレージ システムを使用するように ESXi ホストを設定するときは、特別な考慮を必要とするものがあることに注意してください。

この章には、次のトピックが含まれています。

- iSCSI SAN の概念
- 仮想マシンから iSCSI SAN 上のデータへのアクセス方法

## iSCSI SAN の概念

管理者として、iSCSI SAN と連携するように ESXi ホストを設定しようとする場合は、iSCSI の概念について実用的な知識が必要です。

iSCSI SAN は、コンピュータ システム (ホスト サーバ) と高性能ストレージ サブシステムとの間でイーサネット接続を使用します。SAN コンポーネントには、ホスト サーバで使用する iSCSI ホスト バス アダプタ (HBA) またはネットワーク インターフェイス カード (NIC)、ストレージ トラフィックを転送するスイッチおよびルータ、ケーブル、ストレージ プロセッサ (SP)、ストレージ ディスク システムが含まれます。

iSCSI SAN では、クライアント サーバ アーキテクチャが使用されます。クライアントは iSCSI イニシエータと呼ばれ、ホストで動作します。クライアントは iSCSI コマンドを発行し、iSCSI プロトコルでカプセル化してサーバに送信することで、iSCSI セッションを開始します。サーバは iSCSI ターゲットと呼ばれます。iSCSI ターゲットは、ネットワーク上の物理ストレージ システムを表します。仮想 iSCSI SAN、たとえば仮想マシン内で実行されている iSCSI ターゲット エミュレータで表すこともできます。iSCSI ターゲットは、必要な iSCSI データを送信することで、イニシエータのコマンドに応答します。

## iSCSI マルチパス

ホスト サーバとストレージの間でデータを転送するとき、SAN はマルチパスとよばれる手法を使用します。マルチパスによって、ESXi ホストからストレージ システム上の LUN への複数の物理パスを確保できます。

一般的に、ホストから LUN への 1 つのパスは、iSCSI アダプタまたは NIC、スイッチ ポート、接続用ケーブル、およびストレージ コントローラ ポートから構成されます。パスのコンポーネントで障害が発生した場合、ホストは I/O に使用可能な別のパスを選択します。障害が発生したパスを検出し、別のパスに切り替えるプロセスは、パスのフェイルオーバーと呼ばれます。

マルチパスの詳細については、[17 章 マルチパスとフェイルオーバーについて](#)を参照してください。

## iSCSI SAN のポート

iSCSI SAN 上の単一の検出可能なエンティティ、たとえばイニシエータやターゲットは、iSCSI ノードを表します。各ノードには、そのノードを SAN に接続する 1 つ以上のポートがあります。

iSCSI ポートは、iSCSI セッションのエンドポイントです。各ノードは、いくつかの方法で識別できます。

### IP アドレス

各 iSCSI ノードには関連付けられた IP アドレスがあるため、ネットワーク上のルーティングおよびスイッチングの機器はサーバとストレージとの間の接続を確立できます。このアドレスは、企業内のネットワークやインターネットにアクセスするときにコンピュータに割り当てる IP アドレスと同様です。

### iSCSI 名

ノードを識別するための世界中で一意的な名前。iSCSI では、iSCSI 修飾名 (IQN) および拡張された一意識別子 (EUI) を使用します。

デフォルトで、ESXi は iSCSI イニシエータに `iqn.1998-01.com.vmware:iscsitestox-68158ef2` のような一意の iSCSI 名を生成します。通常、デフォルトの値を変更する必要はありませんが、変更する場合は、新しい iSCSI 名が世界中で一意的であることを確認してください。

### iSCSI エイリアス

iSCSI 名の代わりに使用する、iSCSI デバイスまたはポートのより管理しやすい名前。iSCSI エイリアスは一意的ではなく、ポートとの関連付けを単にわかりやすくするための名前です。

## iSCSI 命名規則

iSCSI は、iSCSI ノード (ターゲットまたはイニシエータ) を識別するために、特殊な一意の名前を使用します。この名前はファイバ チャネル デバイスに関連付けられた WWN (WorldWide Name) に似ており、ノードを包括的に識別する手段として使用されます。

iSCSI 名は 2 つの異なる形式で付けられます。もっとも一般的な形式は IQN 形式です。

iSCSI 命名要件と文字列プロファイルについては、IETF Web サイトの RFC 3721 と RFC 3722 を参照してください。

### iSCSI 修飾名 (IQN) 形式

IQN 形式は、`iqn.yyyy-mm.naming-authority:unique name` という形式になります。

- `yyyy-mm` は、命名機関が設立された年と月です。

- *naming-authority* は通常、命名機関のインターネット ドメイン名の逆の構文です。たとえば、iscsi.vmware.com という命名機関で、iSCSI 修飾名形式が iqn.1998-01.com.vmware.iscsi とします。この名前は、vmware.com のドメイン名が 1998 年 1 月に登録され、サブドメインが iscsi で、vmware.com によって管理されているということを表します。
- *unique name* は、使用する任意の名前です（ホスト名など）。命名機関は、コロン（:）の後ろに割り当てた名前が、次のように一意であることを確認する必要があります。
  - iqn.1998-01.com.vmware.iscsi:name1
  - iqn.1998-01.com.vmware.iscsi:name2
  - iqn.1998-01.com.vmware.iscsi:name999

## エンタープライズ一意識別子（EUI）形式

EUI 形式は、*eui.16 hex digits* という形式になります。

たとえば、eui.0123456789ABCDEF です。

16 桁の 16 進数は、IEEE EUI（拡張された一意識別子）形式による 64 ビットの数字を文字で表現したものです。上位 24 ビットは IEEE が特定の企業に対して登録した企業 ID です。下位 40 ビットは企業 ID を保有するエンティティが割り当て、一意である必要があります。

## iSCSI イニシエータ

iSCSI ターゲットにアクセスするには、ホストで iSCSI イニシエータを使用します。イニシエータは、iSCSI プロトコルにカプセル化した SCSI 要求と応答を、ホストと iSCSI ターゲット間で転送します。

ホストは、異なるタイプのイニシエータをサポートします。

iSCSI アダプタの構成と使用の詳細は、[10 章 iSCSI アダプタおよびストレージの構成](#)を参照してください。

## ソフトウェア iSCSI アダプタ

ソフトウェア iSCSI アダプタは VMkernel に内蔵された VMware コードです。標準的なネットワーク アダプタを経由して、使用しているホストが iSCSI ストレージ デバイスに接続できるようにします。ネットワーク アダプタと通信するとき、ソフトウェア iSCSI アダプタが iSCSI 処理を行います。ソフトウェア iSCSI アダプタの使用により、特殊なハードウェアを購入せずに、iSCSI テクノロジーを使用できます。

## ハードウェア iSCSI アダプタ

ハードウェア iSCSI アダプタは、ホストからの iSCSI およびネットワーク処理を軽減するサードパーティ製アダプタです。ハードウェア iSCSI アダプタはカテゴリに分類されます。

### 依存型ハードウェア iSCSI アダプタ

VMware が提供する iSCSI の構成および管理用インターフェイスと、VMware ネットワークに依存します。

このタイプのアダプタとして、同じポートに対して標準ネットワーク アダプタと iSCSI オフロード機能を提供するカードが利用できます。iSCSI オフロード機能は、iSCSI セッションで使用する IP、MAC、およびその他

のパラメータを取得するのに、ホストのネットワーク構成に依存します。依存型アダプタの例として、ライセンス取得済みの iSCSI 対応 Broadcom 5709 NIC が挙げられます。

### 独立型ハードウェア iSCSI アダプタ

独自のネットワークと、iSCSI の構成インターフェイスおよび管理インターフェイスを実装しています。

独立型ハードウェア iSCSI アダプタの例として、iSCSI オフロード機能のみを提供するカード、または iSCSI オフロード機能と標準の NIC 機能を提供するカードが挙げられます。iSCSI オフロード機能には、iSCSI セッションで使用する IP、MAC、およびその他のパラメータを割り当てる独立構成管理機能があります。独立型アダプタの例として、QLogic QLA4052 アダプタがあります。

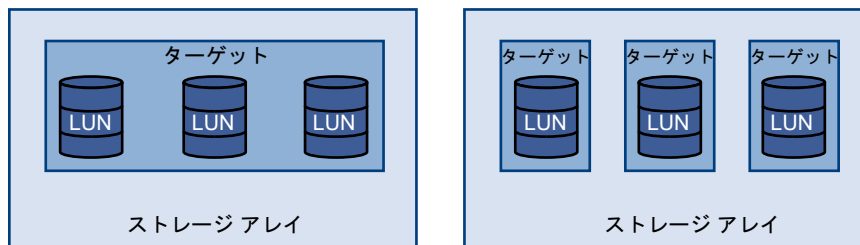
ハードウェア iSCSI アダプタではライセンスが必要になる場合があります。そうしない場合、クライアントまたは vSphere CLI には表示されません。ライセンス情報については、ベンダーにお問い合わせください。

## iSCSI 接続の確立

ESXi の文脈では、ターゲットという語は、ホストがアクセスできる 1 つのストレージ ユニットを表します。ストレージ デバイスおよび LUN という語は、ターゲット上のストレージ領域を表す論理ボリュームを意味しています。一般的に ESXi の文脈では、デバイスおよび LUN という語は、ストレージ ターゲットからホストに表示される SCSI ボリュームを意味しており、フォーマットに使用できます。

iSCSI ストレージのベンダーにより、ストレージをサーバに見せる方法が異なります。一部のベンダーは複数の LUN を単一のターゲットで表示し、別のベンダーは複数のターゲットをそれぞれ 1 つの LUN で表示します。ESXi がストレージを使用する方法は似ているものの、管理ツール上での情報の表現方法は異なります。

図 9-1. ターゲットと LUN との対応表現



次の構成において、それぞれ 3 つの LUN が利用可能です。最初の例の場合、ホストは 1 つのターゲットを検出しますが、そのターゲットには使用できる LUN が 3 つあります。各 LUN は、個々のストレージ ボリュームを意味します。2 つ目の例では、ホストはそれぞれ 1 つの LUN を持つ 3 つの異なるターゲットを検出します。

ホスト ベースの iSCSI イニシエータは、各ターゲットに対して接続を確立します。複数の LUN が 1 つのターゲット内にあるストレージ システムの場合、すべてのトラフィックは単一の接続で行われます。3 つのターゲットにそれぞれ 1 つずつ LUN があるシステムの場合は、ホストと 3 つの LUN との間には、個別の接続が 3 つ存在します。これは、複数の iSCSI HBA があるホストからの複数の接続上のストレージ トラフィックを集約する場合に役立つ情報です。この場合、1 つのターゲットに対するトラフィックにはある HBA が設定され、別のターゲットに対するトラフィックには異なる HBA が使用されています。

## iSCSI ストレージ システムのタイプ

ESXi では、さまざまなストレージ システムとアレイをサポートしています。

ホストでサポートされるストレージのタイプは、アクティブ-アクティブ、アクティブ-パッシブ、および ALUA 準拠です。

### アクティブ-アクティブのストレージ システム

大幅にパフォーマンスを低下させることなく、使用可能なすべてのストレージ ポートを通じて同時に LUN にアクセスできます。すべてのパスが常にアクティブな状態です（パスに障害が発生したときを除く）。

### アクティブ-パッシブのストレージ システム

1つのストレージ プロセッサが特定の LUN にアクティブにアクセスを提供しているシステム。その他のプロセッサは、その LUN のバックアップとして機能し、ほかの LUN I/O にアクティブにアクセスを提供します。I/O は、特定の LUN のアクティブなポートにのみ送信できます。アクティブなストレージ ポートを経由したアクセスで障害が発生した場合、パッシブ ストレージ プロセッサの1つが、そこにアクセスしているサーバによってアクティブになります。

### 非対称ストレージ システム

非対称論理ユニット アクセス（ALUA）をサポートします。ALUA 準拠のストレージ システムは、ポートごとに異なるアクセス レベルを設定できます。ALUA を使用すると、ホストがターゲット ポートの状態を判別し、パスに優先順位を付けることができます。ホストはプライマリとしてアクティブ パスのいくつかを使用し、その他をセカンダリとして使用します。

### 仮想ポート ストレージ システム

1つの仮想ポートを経由して、使用可能なすべての LUN へアクセスできます。アクティブ-アクティブのストレージ デバイスもありますが、単一ポート経由の複数接続であることが隠されます。ESXi マルチパスは、デフォルトで特定のポートからストレージに複数接続を行いません。一部のストレージ ベンダーはストレージへの複数の接続を確立および管理するためにセッション マネージャを提供しています。このストレージ システムでは、ポートのフェイルオーバーと接続バランスの調整を透過的に行います。これは透過的フェイルオーバーと呼ばれることがよくあります。

## 検出、認証、およびアクセス コントロール

ストレージの検出と、アクセスの制限には、複数のメカニズムを使用できます。

使用しているストレージ アクセス制御ポリシーに対応させるには、ホストおよび iSCSI ストレージ システムを構成する必要があります。

### 検出

検出セッションは iSCSI プロトコルの一部で、iSCSI ストレージ システムでアクセスできるターゲット セットを返します。ESXi で利用できる 2 種類の検出方法は、動的検出と静的検出です。動的検出ではアクセス可能なターゲットのリストを iSCSI ストレージ システムから取得し、静的検出ではターゲット名とアドレスを使用して特定のターゲット 1 つのみにアクセスできます。

詳細については、[iSCSI アダプタの検出アドレスの構成](#) を参照してください。

## 認証

iSCSI ストレージ システムは、名前と鍵のペアでイニシエータを認証します。ESXi は、SAN の実装に推奨される CHAP プロトコルをサポートします。CHAP 認証を使用するには、ESXi ホストと iSCSI ストレージ システムで CHAP を有効にし、証明書を共通にしておく必要があります。

CHAP の有効化の詳細は、[iSCSI アダプタの CHAP パラメータの構成](#)を参照してください。

## アクセス コントロール

アクセス コントロールとは iSCSI ストレージ システムで設定するポリシー。ほとんどの実装環境で、次に示す 3 つうちの 1 つ以上のアクセス コントロール機能をサポートしています。

- イニシエータ名によるアクセス コントロール
- IP アドレスによるアクセス コントロール
- CHAP プロトコルによるアクセス コントロール

すべてのルールを満たすイニシエータのみが iSCSI ボリュームにアクセスできます。

アクセス コントロールに CHAP だけを使用すると、再スキャンの速度が低下する可能性があります。ESXi ホストはすべてのターゲットを検出できますが、認証段階で失敗するためです。認証できるターゲットのみをホストが検出する場合は、iSCSI の再スキャンは 高速で実行されます。

## エラー訂正

iSCSI ヘッダおよびデータの整合性を保護するために、iSCSI プロトコルにはヘッダ ダイジェストおよびデータ ダイジェストというエラー訂正方法が規定されています。

パラメータは両方ともデフォルトで無効になっていますが、有効にできます。これらのダイジェストは、iSCSI イニシエータとターゲットとの間を両方向に伝送されるヘッダおよび SCSI データにそれぞれ関連しています。

ヘッダおよびデータのダイジェストでは、TCP やイーサネットなどのほかのネットワーク レイヤーが提供する整合性検査に加え、暗号化されていないエンドツーエンドのデータの整合性を検査します。ここでは、ルータ、スイッチ、プロキシなどのネットワークレベルのトラフィックを変動させる要素も含め、通信経路全体を検査します。

ダイジェストの有無と種類については、iSCSI 接続が確立されたときにネゴシエーションが行われます。イニシエータとターゲットとの間でダイジェスト構成について一致した場合、その二者間の全トラフィックにそのダイジェストを使用する必要があります。

ヘッダおよびデータのダイジェストを有効にすると、イニシエータおよびターゲットの両方に対して追加処理が発生するため、スループットおよび CPU 使用率が影響を受けることがあります。

---

**注：** Intel Nehalem プロセッサを使用しているシステムは、iSCSI ダイジェストの計算をオフロードするため、パフォーマンスへの影響が減少します。

---

ヘッダー ダイジェストとデータ ダイジェストの詳細は、[iSCSI 詳細パラメータの構成](#)を参照してください。

## 仮想マシンから iSCSI SAN 上のデータへのアクセス方法

ESXi は、SAN ストレージ デバイスにある VMFS データストア内に、仮想マシンのディスク ファイルを格納します。仮想マシンのゲスト OS が仮想ディスクに SCSI コマンドを発行すると、SCSI 仮想化レイヤーがこれらのコマンドを VMFS ファイル操作に変換します。

仮想マシンが SAN 上の仮想ディスクと通信するとき、次の処理が実行されます。

- 1 仮想マシンのゲスト OS が SCSI ディスクに読み書きするとき、仮想ディスクに対して SCSI コマンドが発行されます。
- 2 仮想マシンのオペレーティング システムのデバイス ドライバが仮想 SCSI コントローラと通信します。
- 3 仮想 SCSI コントローラは、コマンドを VMkernel に転送します。
- 4 VMkernel は次の処理を実行します。
  - a ゲスト仮想マシン ディスクに対応するファイルを VMFS ボリュームに配置します。
  - b 仮想ディスクに対するブロックの要求を、適切な物理デバイスのブロックにマッピングします。
  - c 変更した I/O 要求を VMkernel のデバイス ドライバから iSCSI イニシエータ（ハードウェアまたはソフトウェア）に送信します。
- 5 iSCSI イニシエータがハードウェア iSCSI アダプタ（独立型または依存型）の場合、アダプタは次の処理を行います。
  - a I/O 要求を iSCSI PDU（Protocol Data Unit）にカプセル化します。
  - b iSCSI PDU を TCP/IP パケットにカプセル化します。
  - c イーサネット経由で iSCSI ストレージ システムに IP パケットを送信します。
- 6 iSCSI イニシエータがソフトウェア iSCSI アダプタの場合、次の処理が実行されます。
  - a iSCSI イニシエータが I/O 要求を iSCSI PDU にカプセル化します。
  - b イニシエータは TCP/IP 接続経由で iSCSI PDU を送信します。
  - c VMkernel の TCP/IP スタックは TCP/IP パケットを物理 NIC に中継します。
  - d 物理 NIC はイーサネット経由で iSCSI ストレージ システムに IP パケットを送信します。
- 7 iSCSI イニシエータがネットワークへの接続に使用するポートに応じて、イーサネット スイッチとルータは、ホストがアクセスするストレージ デバイスにその要求を伝送します。



# iSCSI アダプタおよびストレージの構成

# 10

ESXi を SAN と連携させるには、iSCSI アダプタおよびストレージを設定する必要があります。

これを行うには、まず基本的な要件を満たし、次にベスト プラクティスに従って、ハードウェアまたはソフトウェア iSCSI アダプタをインストールおよび設定して SAN にアクセスします。

次の表は、ESXi がサポートする iSCSI アダプタ (vmhba) をリストして、VMkernel ネットワーク構成が必要かどうかを示します。

表 10-1. サポートされる iSCSI アダプタ

iSCSI アダプタ (vmhba)	説明	VMkernel ネットワーク
ソフトウェア	標準的な NIC を使用して、IP ネットワーク上のリモート iSCSI ターゲットにホストを接続します。	必須
独立型ハードウェア	iSCSI およびネットワークの処理と管理をホストからオフロードするサードパーティのアダプタ。	必須ではない
依存型ハードウェア	VMware ネットワークおよび iSCSI 構成および管理インターフェイスに依存するサードパーティのアダプタ。	必須

iSCSI アダプタを設定したあとで、iSCSI ストレージでデータストアを作成できます。データストアの作成および管理方法の詳細は、[データストアの作成](#) を参照してください。

この章には、次のトピックが含まれています。

- [ESXi iSCSI SAN の要件](#)
- [ESXi iSCSI SAN の制限](#)
- [iSCSI の LUN 割り当ての設定](#)
- [ネットワーク構成と認証](#)
- [独立型ハードウェア iSCSI アダプタの設定](#)
- [依存型ハードウェア iSCSI アダプタについて](#)
- [ソフトウェア iSCSI アダプタについて](#)
- [iSCSI アダプタの全般プロパティの変更](#)
- [iSCSI ネットワークの設定](#)

- [iSCSI でのジャンボ フレームの使用](#)
- [iSCSI アダプタの検出アドレスの構成](#)
- [iSCSI アダプタの CHAP パラメータの構成](#)
- [iSCSI 詳細パラメータの構成](#)
- [iSCSI セッションの管理](#)

## ESXi iSCSI SAN の要件

ESXi ホストを SAN と正常に連携させるには、いくつかの要件を満たす必要があります。

- SAN ストレージ ハードウェアとファームウェアの組み合わせが、ESXi システムとの併用でサポートされていることを確認します。最新のリストは、『VMware 互換性ガイド』を参照してください。
- LUN ごとに VMFS データストアが 1 つのみ存在するようにシステムを構成します。
- ディスクレス サーバを使用していない場合には、ローカル ストレージで診断パーティションを設定します。iSCSI SAN から起動するディスクレス サーバを使用する場合には、iSCSI による診断パーティションの詳細については、[iSCSI SAN からの起動に関する一般的推奨事項](#)を参照してください。
- Raw ディスクへのアクセスには RDM を使用します。詳細については、[18 章 Raw デバイス マッピング](#)を参照してください。
- ゲスト OS の SCSI コントローラ ドライバを、十分に大きなキューに設定します。iSCSI アダプタと仮想マシンのキューの深さの変更の詳細は、『vSphere トラブルシューティング』を参照してください。
- Microsoft Windows を実行する仮想マシンでは、Windows がバスのフェイルオーバーによって発生する遅延 I/O をさらに許容できるように、SCSI の TimeoutValue パラメータの値を増やします。詳細については、[Windows ゲスト OS にタイムアウトを設定](#)を参照してください。

## ESXi iSCSI SAN の制限

ESXi を iSCSI SAN と使用するときには多数の制限が存在します。

- ESXi は、iSCSI 接続されたテープ デバイスをサポートしません。
- 仮想マシンのマルチパス ソフトウェアを使用して、単一物理 LUN の I/O ロード バランシングを実行することはできません。
- 独立型ハードウェア アダプタをソフトウェアまたは依存型ハードウェア アダプタと組み合わせると、ESXi はマルチパスをサポートしません。

## iSCSI の LUN 割り当ての設定

ESXi システムで iSCSI SAN ストレージを使用する準備をする場合、LUN 割り当てを設定する必要があります。

次の点に注意してください。

- ストレージのプロビジョニング。起動時にホストが LUN を認識するようにするために、すべての iSCSI ストレージ ターゲットを構成し、ホストがターゲットにアクセスして利用できるようにします。またホストを構成し、使用可能な iSCSI ターゲットをすべて検出できるようにします。
- vMotion および VMware DRS。vCenter Server と vMotion または DRS を使用する場合は、仮想マシンの LUN がすべてのホストにプロビジョニングされていることを確認します。この構成によって、仮想マシンの移動の自由度が最大になります。
- アクティブ-アクティブ アレイとアクティブ-パッシブ アレイ。アクティブ-パッシブの SAN ストレージ デバイスで vMotion または DRS を使用する場合は、すべてのホストが、すべてのストレージ プロセッサへの一貫したパスを保持するようにします。そうしない場合、vMotion の移行が行われるときに、パスのスラッシングが生じることがあります。

『ストレージ/SAN 互換性』にないアクティブ-パッシブ ストレージ アレイでは、ストレージ ポートのフェイルオーバーはサポートされません。サーバをストレージ システムのアクティブなポートに接続する必要があります。この構成によって、LUN がホストに確実に提供されます。

## ネットワーク構成と認証

ESXi ホストで iSCSI ストレージを検出するには、あらかじめ iSCSI イニシエータを構成しておく必要があります。場合によっては、認証も設定しておく必要があります。

- ソフトウェア iSCSI と依存型ハードウェア iSCSI の場合、VMkernel 用のネットワークを構成する必要があります。vmkping ユーティリティを使用して、ネットワーク構成を確認できます。ソフトウェア iSCSI および依存型 iSCSI では、IPv4 および IPv6 プロトコルがサポートされています。
- 独立型ハードウェア iSCSI の場合、IP アドレス、サブネット マスク、およびデフォルト ゲートウェイなどのネットワーク パラメータを HBA で構成する必要があります。また、アダプタのネットワーク プロトコル、IPv4、または IPv6 を指定することもできます。
- 必要に応じて、デフォルトのイニシエータ名を確認および変更します。
- ストレージ システムの動的検出アドレスまたは静的検出アドレスおよびターゲット名を設定する必要があります。ソフトウェア iSCSI および依存型 iSCSI の場合には、vmkping を使用して、アドレスを ping 可能にします。
- CHAP 認証については、イニシエータおよびストレージ システム側で有効にします。認証を有効にすると、未検出のターゲットすべてに対して適用されますが、検出済みのターゲットに対しては適用されません。検出アドレスが設定されると、新しく検出されたターゲットが公開され、その時点で使用できるようになります。

vmkping コマンドの使用方法的詳細については、当社のナレッジ ベースを検索してください。

## 独立型ハードウェア iSCSI アダプタの設定

独立型ハードウェア iSCSI アダプタとは、TCP/IP で iSCSI ストレージにアクセスできる、サードパーティ製の専用アダプタのことです。この iSCSI アダプタは、ESXi システムにおける、iSCSI とネットワークのすべてのプロセスおよび管理を行います。

**前提条件**

- アダプタにライセンスが必要かどうかを確認します。
- アダプタをインストールします。

ライセンス、インストール、およびファームウェアの更新については、ベンダーのドキュメントを参照してください。

**手順****1 独立型ハードウェア iSCSI アダプタの表示**

独立型ハードウェア iSCSI アダプタを表示して、インストールが正しく行われ、構成する準備が整っていることを確認します。

**2 iSCSI アダプタの全般プロパティの変更**

iSCSI アダプタに割り当てられたデフォルト iSCSI 名およびエイリアスを変更できます。独立ハードウェア iSCSI アダプタの場合は、デフォルトの I P 設定も変更できます。

**3 ハードウェア iSCSI のネットワーク設定の編集**

独立型ハードウェア iSCSI アダプタのインストール後は、アダプタが iSCSI SAN 用に適切に構成されるようにするため、デフォルトのネットワーク設定の変更が必要になることがあります。

**4 iSCSI の動的または静的検出の設定**

動的検出では、イニシエータが指定された iSCSI ストレージ システムに接続するたびに、SendTargets 要求がシステムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供することで応答します。動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。

**次のステップ**

必要に応じて、CHAP パラメータおよびジャンボ フレームを構成します。

**独立型ハードウェア iSCSI アダプタの表示**

独立型ハードウェア iSCSI アダプタを表示して、インストールが正しく行われ、構成する準備が整っていることを確認します。

ホストに独立型ハードウェア iSCSI アダプタをインストールすると、構成に使用可能なストレージ アダプタのリストに表示されます。プロパティを表示できます。

**前提条件**

必要な権限：ホスト.構成.ストレージ パーティション構成

**手順**

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックします。

ハードウェア iSCSI アダプタがインストールされている場合は、ストレージ アダプタのリストに表示されます。

#### 4 表示するアダプタを選択します。

モデル、iSCSI 名、iSCSI エイリアス、IP アドレス、ターゲットとパスの情報など、アダプタのデフォルトの詳細が表示されます。

## iSCSI アダプタの全般プロパティの変更

iSCSI アダプタに割り当てられたデフォルト iSCSI 名およびエイリアスを変更できます。独立ハードウェア iSCSI アダプタの場合は、デフォルトの IP 設定も変更できます。

---

**重要：** iSCSI アダプタのデフォルトのプロパティを変更する際は、その名前および IP アドレスの形式が適切なことを確認します。

---

#### 前提条件

必要な権限： ホスト .構成.ストレージ パーティション構成

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックし、設定するアダプタ (vmhba#) を選択します。
- 4 [アダプタの詳細] で、[プロパティ] タブをクリックし、[全般] パネルの [編集] をクリックします。
- 5 アダプタのデフォルト iSCSI 名を変更するには、新しい名前を入力します。

入力した名前が世界中で一意であることと、形式が適切であることを確認します。これが正しく行われないと、一部のストレージ デバイスで iSCSI アダプタが認識されない場合があります。

- 6 (オプション) iSCSI エイリアスを入力します。

エイリアスは、iSCSI アダプタの識別に使用する名前です。

#### 結果

iSCSI 名を変更すると、新しい iSCSI セッションで使用されます。既存のセッションでは、ログアウトして再ログインするまで、新しい設定は使用されません。

## ハードウェア iSCSI のネットワーク設定の編集

独立型ハードウェア iSCSI アダプタのインストール後は、アダプタが iSCSI SAN 用に適切に構成されるようにするため、デフォルトのネットワーク設定の変更が必要になることがあります。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックし、設定するアダプタ (vmhba#) を選択します。
- 4 [アダプタの詳細] で、[ネットワーク設定] タブをクリックし、[編集] をクリックします。

- 5 [IPv4 設定] セクションで、IPv6 を無効化するか、IP アドレスを取得するために使用する方法を選択します。

**注：** 自動 DHCP オプションと固定オプションは相互に排他的です。

オプション	説明
IPv4 設定がありません	IPv4 を無効化します。
IPv4 設定を自動的に取得します	DHCP を使用して IP 設定を取得します。
固定 IPv4 設定を使用します	iSCSI アダプタの IPv4 IP アドレス、サブネット マスク、およびデフォルト ゲートウェイを入力します。

- 6 [IPv6 設定] セクションで、IPv6 を無効化するか、IPv6 アドレスを取得するための適切なオプションを選択します。

**注：** 自動オプションと固定オプションは相互に排他的です。

オプション	説明
IPv6 設定なし	IPv6 を無効化します。
IPv6 の有効化	IPv6 アドレスを取得するためのオプションを選択します。
DHCP を使用して IPv6 アドレスを自動的に取得	DHCP を使用して IPv6 アドレスを取得します。
ルータの通知を使用して IPv6 アドレスを自動的に取得	ルータの通知を使用して IPv6 アドレスを取得します。
IPv6 のリンク ローカル アドレスのオーバーライド	固定 IP アドレスを構成することによって、リンク ローカル IP アドレスをオーバーライドします。
固定 IPv6 アドレス	a [追加] をクリックして新しい IPv6 アドレスを追加します。 b IPv6 アドレスとサブネット プリフィックスの長さを入力し、[OK] をクリックします。

- 7 [DNS 設定] セクションで、優先 DNS サーバおよび代替 DNS サーバの IP アドレスを入力します。

両方の値を入力する必要があります。

## iSCSI の動的または静的検出の設定

動的検出では、イニシエータが指定された iSCSI ストレージ システムに接続するたびに、SendTargets 要求がシステムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供することで応答します。動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。

静的検出または動的検出を設定する場合は、新しい iSCSI ターゲットしか追加できません。既存のターゲットのパラメータは変更できません。これを変更するには、既存のターゲットを削除して新しいターゲットを追加します。

### 前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。

- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、構成する iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ターゲット] タブをクリックします。
- 5 検出方法を構成します。

オプション	説明
動的検出	<ol style="list-style-type: none"> <li>a [動的検出] をクリックし、[追加] をクリックします。</li> <li>b ストレージ システムの IP アドレスまたは DNS 名を入力し、[OK] をクリックします。</li> <li>c iSCSI アダプタを再スキャンします。</li> </ol> <p>iSCSI システムとの SendTargets セッションが確立された後、ホストは新たに検出されたすべてのターゲットで静的検出リストを作成します。</p>
静的検出	<ol style="list-style-type: none"> <li>a [静的検出] をクリックし、[追加] をクリックします。</li> <li>b ターゲットの情報を入力し、[OK] をクリックします。</li> <li>c iSCSI アダプタを再スキャンします。</li> </ol>

## 依存型ハードウェア iSCSI アダプタについて

依存型ハードウェア iSCSI アダプタは、VMware が提供する iSCSI 構成インターフェイスおよび管理インターフェイスと、VMware ネットワークに依存するサードパーティ製アダプタです。

依存型 iSCSI アダプタの例として、Broadcom 5709 NIC が挙げられます。ホストにインストールされると、標準的なネットワーク アダプタと iSCSI エンジンの 2 つのコンポーネントを同じポートに提供します。ストレージ アダプタのリストで iSCSI エンジンは iSCSI アダプタ (vmhba) として表示されます。iSCSI アダプタがデフォルトでは有効になっていますが、機能させるためには、仮想の VMkernel アダプタ (vmk) から、関連付けられた物理的ネットワーク アダプタ (vmnic) に最初に接続する必要があります。これで、iSCSI アダプタを構成できます。

依存型ハードウェア iSCSI アダプタを構成したあとは、検出および認証データはネットワーク接続を通して渡されません。一方、iSCSI トラフィックは iSCSI エンジンを通して移動し、ネットワークをバイパスします。

## 依存型ハードウェア iSCSI に関する考慮事項

依存型ハードウェア iSCSI アダプタを ESXi で使用する場合、特定の考慮事項が適用されます。

- 依存型ハードウェア iSCSI アダプタを使用すると、iSCSI トラフィックが多い場合でも、アダプタに関連付けられている NIC のパフォーマンスに関するレポートに、アクティビティがほとんど、またはまったく表示されない場合があります。これは、iSCSI トラフィックが通常のネットワーク スタックをバイパスするために発生します。
- Cisco Nexus 1000V DVS のようなサードパーティ仮想スイッチを使用する場合には、自動固定を無効にします。代わりに手動による固定を使用して、VMkernel アダプタ (vmk) を適切な物理 NIC (vmnic) に接続していることを確認します。詳細は、仮想スイッチ ベンダーのドキュメントを参照してください。
- Broadcom iSCSI アダプタは、ハードウェアでデータの再アセンブリを実行しますが、これにはバッファ スペースに制限があります。Broadcom iSCSI アダプタを輻輳が発生しているネットワーク、または多大な負荷を受けている状態で使用する場合、パフォーマンス低下を回避するためにフローの制御を有効にします。

フローの制御は、2 つのノード間でのデータ転送率を管理し、高速な送信者が低速な受信者をオーバーランさせてしまうことを防ぎます。最適な結果を得るには、ホストおよび iSCSI ストレージ システムの I/O パスのエンド ポイントでフローの制御を有効にします。

ホストのフロー制御を有効にするには、`esxcli system module parameters` コマンドを使用します。詳細は、<http://kb.vmware.com/kb/1013413> にある VMware ナレッジ ベースの記事を参照してください。

- 依存型ハードウェア アダプタでは、IPv4 および IPv6 がサポートされています。

## 依存型ハードウェア iSCSI アダプタの構成

依存型ハードウェア iSCSI アダプタの設定および構成はすべて、いくつかの手順を実行します。アダプタの設定後に、CHAP パラメータおよびジャンボ フレームの構成が必要になる場合があります。

### 手順

#### 1 依存型ハードウェア iSCSI アダプタの表示

依存型ハードウェア iSCSI アダプタを表示して、それが正しくロードされていることを確認します。

#### 2 iSCSI アダプタの全般プロパティの変更

iSCSI アダプタに割り当てられたデフォルト iSCSI 名およびエイリアスを変更できます。独立ハードウェア iSCSI アダプタの場合は、デフォルトの I P 設定も変更できます。

#### 3 iSCSI アダプタとネットワーク アダプタとの間の関連性の特定

ネットワーク接続を作成して、依存型 iSCSI アダプタと物理ネットワーク アダプタをバインドできます。接続を正しく作成するには、依存型ハードウェア iSCSI アダプタと関連付けられている物理 NIC の名前を判断する必要があります。

#### 4 iSCSI のネットワーク接続の作成

ソフトウェアまたは依存型ハードウェア iSCSI アダプタと物理的ネットワーク アダプタの間のトラフィックのために接続を構成します。

#### 5 iSCSI の動的または静的検出の設定

動的検出では、イニシエータが指定された iSCSI ストレージ システムに接続するたびに、SendTargets 要求がシステムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供することで応答します。動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。

### 次のステップ

必要に応じて、CHAP パラメータおよびジャンボ フレームを構成します。

## 依存型ハードウェア iSCSI アダプタの表示

依存型ハードウェア iSCSI アダプタを表示して、それが正しくロードされていることを確認します。

依存型ハードウェア iSCSI アダプタ (vmhba#) がインストールされている場合は、ストレージ アダプタのリストで Broadcom iSCSI アダプタなどのカテゴリに表示されます。依存型ハードウェア アダプタがストレージ アダプタのリストに表示されない場合、ライセンスが必要かどうか確認する必要があります。ベンダーのドキュメントを参照してください。



**手順**

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックします。
- 4 表示するアダプタ (vmhba#) を選択します。

iSCSI 名、iSCSI エイリアス、およびそのステータスを含む、アダプタのデフォルトの詳細が表示されます。

**次のステップ**

依存型 iSCSI アダプタはデフォルトで有効になっていますが、機能させるためには、iSCSI トラフィックのネットワークを設定し、アダプタを適切な VMkernel iSCSI ポートにバインドする必要があります。そのあとで、検出アドレスと CHAP パラメータを構成します。

**iSCSI アダプタの全般プロパティの変更**

iSCSI アダプタに割り当てられたデフォルト iSCSI 名およびエイリアスを変更できます。独立ハードウェア iSCSI アダプタの場合は、デフォルトの IP 設定も変更できます。

---

**重要：** iSCSI アダプタのデフォルトのプロパティを変更する際は、その名前および IP アドレスの形式が適切なことを確認します。

---

**前提条件**

必要な権限： ホスト .構成.ストレージ パーティション構成

**手順**

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックし、設定するアダプタ (vmhba#) を選択します。
- 4 [アダプタの詳細] で、[プロパティ] タブをクリックし、[全般] パネルの [編集] をクリックします。
- 5 アダプタのデフォルト iSCSI 名を変更するには、新しい名前を入力します。

入力した名前が世界中で一意であることと、形式が適切であることを確認します。これが正しく行われないと、一部のストレージ デバイスで iSCSI アダプタが認識されない場合があります。

- 6 (オプション) iSCSI エイリアスを入力します。

エイリアスは、iSCSI アダプタの識別に使用する名前です。

**結果**

iSCSI 名を変更すると、新しい iSCSI セッションで使用されます。既存のセッションでは、ログアウトして再ログインするまで、新しい設定は使用されません。

## iSCSI アダプタとネットワーク アダプタとの間の関連性の特定

ネットワーク接続を作成して、依存型 iSCSI アダプタと物理ネットワーク アダプタをバインドできます。接続を正しく作成するには、依存型ハードウェア iSCSI アダプタと関連付けられている物理 NIC の名前を判断する必要があります。

### 前提条件

vSphere Web Client で、依存型ハードウェア iSCSI アダプタ (vmhba#) を参照します。[依存型ハードウェア iSCSI アダプタの表示](#) を参照してください。

### 手順

- 1 iSCSI アダプタ (vmhba#) を選択し、[アダプタの詳細] の [ネットワーク ポートのバインド] タブをクリックします。
- 2 [追加] をクリックします。

依存型 iSCSI アダプタに対応するネットワーク アダプタ (vmnic#) が [物理ネットワーク アダプタ] 列に一覧表示されます。

### 次のステップ

[VMkernel アダプタ] 列が空の場合、物理ネットワーク アダプタ (vmnic#) の VMkernel アダプタ (vmk#) を作成し、関連する依存型ハードウェア iSCSI にバインドします。[iSCSI ネットワークの設定](#) を参照してください。

## iSCSI のネットワーク接続の作成

ソフトウェアまたは依存型ハードウェア iSCSI アダプタと物理的ネットワーク アダプタの間のトラフィックのために接続を構成します。

次のタスクは、vSphere の標準スイッチによる iSCSI ネットワーク構成について説明します。

複数のアップリンク ポートがある vSphere Distributed を使用している場合は、ポートのバインドに、物理 NIC ごとに個別の分散ポート グループを作成します。次に、各分散ポート グループのアクティブなアップリンク ポートが 1 つだけになるようにチーム ポリシーを設定します。vSphere Distributed Switch の詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

### 手順

#### 1 iSCSI 用の単一 VMkernel アダプタの作成

iSCSI ストレージ用にサービスを実行する VMkernel を物理ネットワーク アダプタに接続します。

#### 2 iSCSI 用の追加 VMkernel アダプタの作成

iSCSI 用の物理ネットワーク アダプタが複数あり、すべての物理アダプタを単一の vSphere 標準スイッチに接続する場合は、このタスクを使用します。このタスクでは、物理アダプタおよび VMkernel アダプタを既存の vSphere 標準スイッチに追加します。

#### 3 iSCSI のネットワーク ポリシーの変更

1 つの vSphere 標準スイッチを使用して複数の VMkernel アダプタを複数のネットワーク アダプタに接続する場合は、それぞれの VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが 1 つだけになるようネットワーク ポリシーを設定します。

#### 4 iSCSI および VMkernel アダプタのバインド

iSCSI アダプタと VMkernel アダプタをバインドします。

#### 5 ポート バインドの詳細の確認

iSCSI アダプタにバインドされた VMkernel アダプタのネットワーク詳細を確認します。

### iSCSI 用の単一 VMkernel アダプタの作成

iSCSI ストレージ用にサービスを実行する VMkernel を物理ネットワーク アダプタに接続します。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [アクション] - [ネットワークの追加] の順にクリックします。
- 3 [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
- 4 [新しい標準スイッチ] を選択して、vSphere 標準スイッチを作成します。
- 5 [アダプタの追加] アイコンをクリックし、iSCSI に使用するネットワーク アダプタ (vmnic#) を選択します。  
[アクティブ アダプタ] にアダプタが割り当てられていることを確認します。

---

**重要：** 依存型ハードウェア iSCSI 用の VMkernel アダプタを作成する場合は、iSCSI コンポーネントに対応するネットワーク アダプタを選択します。[iSCSI アダプタとネットワーク アダプタとの間の関連性の特定](#) を参照してください。

---

- 6 ネットワーク ラベルを入力します。  
ネットワーク ラベルは、「iSCSI」 など、作成する VMkernel アダプタを識別するわかりやすい名前です。
- 7 IP 設定を指定します。
- 8 情報を確認し、[終了] をクリックします。

#### 結果

これで、ホスト上の物理ネットワーク アダプタ (vmnic#) 用に、仮想 VMkernel アダプタ (vmk#) が作成されました。

#### 次のステップ

ホストに iSCSI トラフィック用の物理ネットワーク アダプタが 1 つある場合は、作成した仮想アダプタを iSCSI アダプタにバインドする必要があります。

複数のネットワーク アダプタがある場合は、追加の VMkernel アダプタを作成してから、iSCSI とのバインドを実行します。仮想アダプタの数は、ホスト上の物理アダプタの数に対応している必要があります。

### iSCSI 用の追加 VMkernel アダプタの作成

iSCSI 用の物理ネットワーク アダプタが複数あり、すべての物理アダプタを単一の vSphere 標準スイッチに接続する場合は、このタスクを使用します。このタスクでは、物理アダプタおよび VMkernel アダプタを既存の vSphere 標準スイッチに追加します。

**前提条件**

iSCSI トラフィック用に指定された単一の物理ネットワーク アダプタに iSCSI VMkernel アダプタをマッピングする vSphere 標準スイッチを作成します。

**手順**

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックし、[ネットワーク] をクリックします。
- 3 [仮想スイッチ] をクリックし、リストから、変更する vSphere スイッチを選択します。
- 4 追加のネットワーク アダプタをスイッチに接続します。
  - a [ホスト ネットワークの追加] アイコンをクリックします。
  - b [物理ネットワーク アダプタ] を選択し、[次へ] をクリックします。
  - c 既存のスイッチを使用していることを確認し、[次へ] をクリックします。
  - d [アダプタの追加] アイコンをクリックし、iSCSI に使用する 1 つ以上のネットワーク アダプタ (vmnic#) を選択します。  
  
依存型ハードウェア iSCSI アダプタの場合は、対応する iSCSI コンポーネントがある NIC だけを選択します。
  - e 構成を完了し、[終了] をクリックします。
- 5 追加したすべての物理ネットワーク アダプタに iSCSI VMkernel アダプタを作成します。  
  
VMkernel インターフェイスの数は、vSphere 標準スイッチ上の物理ネットワーク アダプタの数に対応している必要があります。
  - a [ホスト ネットワークの追加] アイコンをクリックします。
  - b [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
  - c 既存のスイッチを使用していることを確認し、[次へ] をクリックします。
  - d 構成を完了し、[終了] をクリックします。

**次のステップ**

すべての VMkernel アダプタ用のネットワーク ポリシーを変更して、各 VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが 1 つのみになるようにします。そのあとで、iSCSI VMkernel アダプタをソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタにバインドできます。

**iSCSI のネットワーク ポリシーの変更**

1 つの vSphere 標準スイッチを使用して複数の VMkernel アダプタを複数のネットワーク アダプタに接続する場合は、それぞれの VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが 1 つだけになるようネットワーク ポリシーを設定します。

デフォルトでは、vSphere 標準スイッチ上の VMkernel アダプタごとに、すべてのネットワーク アダプタがアクティブなアダプタとして表示されます。この設定をオーバーライドして、各 VMkernel アダプタが、対応する 1 つのアクティブな物理アダプタのみにマッピングするようにしてください。たとえば、vmk1 は vmnic1 にマッピングし、vmk2 は vmnic2 にマッピングする、というようにします。

#### 前提条件

VMkernel を iSCSI トラフィック用に指定された物理ネットワーク アダプタに接続する vSphere 標準スイッチを作成します。VMkernel アダプタの数は、vSphere 標準スイッチ上の物理アダプタの数に対応している必要があります。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックし、[ネットワーク] をクリックします。
- 3 [仮想スイッチ] をクリックし、リストから、変更する vSphere スイッチを選択します。
- 4 vSwitch 図で VMkernel アダプタを選択し、[設定の編集] アイコンをクリックします。
- 5 [設定の編集] ウィザードで、[チーミングおよびフェイルオーバー] をクリックし、[フェイルオーバーの順序] で [オーバーライド] をクリックします。
- 6 1 つの物理アダプタのみをアクティブなアダプタとして指定し、残りのすべてのアダプタを [未使用のアダプタ] カテゴリに移動します。
- 7 vSphere 標準スイッチ上の各 iSCSI VMkernel インターフェイスについて、[手順 4](#) から [手順 6](#) までを繰り返します。

#### 例：iSCSI ネットワーク ポリシー

次の表は、正しい iSCSI マッピングを示しています。ここでは、VMkernel アダプタごとのアクティブな物理ネットワーク アダプタが 1 つのみとなっています。

VMkernel アダプタ (vmk#)	物理ネットワーク アダプタ (vmnic#)
vmk1	[有効なアダプタ]
	vmnic1
	[未使用アダプタ]
	vmnic2
vmk2	[有効なアダプタ]
	vmnic2
	[未使用アダプタ]
	vmnic1

#### 次のステップ

このタスクを実行したあと、仮想 VMkernel アダプタを、ソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタにバインドします。

#### iSCSI および VMkernel アダプタのバインド

iSCSI アダプタと VMkernel アダプタをバインドします。

## 前提条件

ホスト上の各物理ネットワーク アダプタ用に、仮想 VMkernel アダプタを作成します。複数の VMkernel アダプタを使用する場合は、正しいネットワーク ポリシーを設定します。

必要な権限：ホスト.構成.ストレージ パーティション構成

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックして、構成するソフトウェア iSCSI アダプタまたは依存型 iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ネットワーク ポートのバインド] タブをクリックし、[追加] をクリックします。
- 5 iSCSI アダプタとバインドする VMkernel アダプタを選択します。

---

**注：** VMkernel アダプタのネットワーク ポリシーがバインド要件に準拠していることを確認してください。

---

ソフトウェア iSCSI アダプタを、1 つ以上の VMkernel アダプタにバインドできます。依存型ハードウェア iSCSI アダプタの場合は、正しい物理 NIC と関連付けられた 1 つの VMkernel アダプタのみ使用できます。

- 6 [OK] をクリックします。

## 結果

ネットワーク接続が、iSCSI アダプタの VMkernel ポート バインドのリストに表示されます。

## ポート バインドの詳細の確認

iSCSI アダプタにバインドされた VMkernel アダプタのネットワーク詳細を確認します。

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、リストからソフトウェア iSCSI アダプタ または依存型 iSCSI アダプタを選択します。
- 4 [アダプタの詳細] で、[ネットワーク ポートのバインド] タブをクリックし、[詳細の表示] をクリックします。
- 5 利用可能なタブを切り替えて、VMkernel アダプタ情報を確認します。

## iSCSI の動的または静的検出の設定

動的検出では、イニシエータが指定された iSCSI ストレージ システムに接続するたびに、SendTargets 要求がシステムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供することで応答します。動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。

静的検出または動的検出を設定する場合は、新しい iSCSI ターゲットしか追加できません。既存のターゲットのパラメータは変更できません。これを変更するには、既存のターゲットを削除して新しいターゲットを追加します。

**前提条件**

必要な権限：ホスト.構成.ストレージ パーティション構成

**手順**

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、構成する iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ターゲット] タブをクリックします。
- 5 検出方法を構成します。

オプション	説明
動的検出	<ol style="list-style-type: none"> <li>a [動的検出] をクリックし、[追加] をクリックします。</li> <li>b ストレージ システムの IP アドレスまたは DNS 名を入力し、[OK] をクリックします。</li> <li>c iSCSI アダプタを再スキャンします。</li> </ol> <p>iSCSI システムとの SendTargets セッションが確立された後、ホストは新たに検出されたすべてのターゲットで静的検出リストを作成します。</p>
静的検出	<ol style="list-style-type: none"> <li>a [静的検出] をクリックし、[追加] をクリックします。</li> <li>b ターゲットの情報を入力し、[OK] をクリックします。</li> <li>c iSCSI アダプタを再スキャンします。</li> </ol>

## ソフトウェア iSCSI アダプタについて

ソフトウェア ベースの iSCSI 実装では、標準の NIC を使用して、ホストを IP ネットワーク上のリモート iSCSI ターゲットに接続できます。ESXi に組み込まれたソフトウェア iSCSI アダプタは、ネットワーク スタックを介して物理 NIC と通信することにより、このような接続が容易になります。

ソフトウェア iSCSI アダプタを使用する前に、ネットワークを設定し、アダプタを有効にし、検出アドレスや CHAP などのパラメータを構成する必要があります。

**注：** iSCSI の個別のネットワーク アダプタを指定します。速度が 100Mbps 以下のアダプタでは、iSCSI を使用しないでください。

## ソフトウェア iSCSI アダプタの構成

ソフトウェア iSCSI アダプタの構成は、次の手順で行います。

**手順**

### 1 ソフトウェア iSCSI アダプタの有効化

ソフトウェア iSCSI アダプタを有効にして、ホストが iSCSI ストレージへのアクセスに使用できるようにする必要があります。

## 2 iSCSI アダプタの全般プロパティの変更

iSCSI アダプタに割り当てられたデフォルト iSCSI 名およびエイリアスを変更できます。独立ハードウェア iSCSI アダプタの場合は、デフォルトの IP 設定も変更できます。

## 3 iSCSI のネットワーク接続の作成

ソフトウェアまたは依存型ハードウェア iSCSI アダプタと物理的ネットワーク アダプタの間のトラフィックのために接続を構成します。

## 4 iSCSI の動的または静的検出の設定

動的検出では、イニシエータが指定された iSCSI ストレージ システムに接続するたびに、SendTargets 要求がシステムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供することで応答します。動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。

### 次のステップ

必要に応じて、CHAP パラメータおよびジャンボ フレームを構成します。

## ソフトウェア iSCSI アダプタの有効化

ソフトウェア iSCSI アダプタを有効にして、ホストが iSCSI ストレージへのアクセスに使用できるようにする必要があります。

有効にできるソフトウェア iSCSI アダプタは 1 つだけです。

### 前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

---

**注：** ソフトウェア iSCSI アダプタを使用して iSCSI から起動する場合、最初の起動時にアダプタが有効になり、ネットワーク構成が作成されます。アダプタを無効にした場合、ホストを起動するたびに再度有効化されます。

---

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ]、[追加] アイコン (+) の順にクリックします。
- 4 [ソフトウェア iSCSI アダプタ] を選択し、アダプタを追加することを確定します。

### 結果

ソフトウェア iSCSI アダプタ (vmhba#) が有効になり、ストレージ アダプタのリストに表示されます。アダプタを有効にすると、ホストによってデフォルトの iSCSI 名が割り当てられます。デフォルトの名前を変更する必要がある場合は、iSCSI の命名規則に従ってください。

### 次のステップ

アダプタを選択し、[アダプタの詳細] セクションを使用して構成を完了します。



## iSCSI アダプタの全般プロパティの変更

iSCSI アダプタに割り当てられたデフォルト iSCSI 名およびエイリアスを変更できます。独立ハードウェア iSCSI アダプタの場合は、デフォルトの IP 設定も変更できます。

**重要：** iSCSI アダプタのデフォルトのプロパティを変更する際は、その名前および IP アドレスの形式が適切なことを確認します。

### 前提条件

必要な権限： ホスト .構成.ストレージ パーティション構成

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックし、設定するアダプタ (vmhba#) を選択します。
- 4 [アダプタの詳細] で、[プロパティ] タブをクリックし、[全般] パネルの [編集] をクリックします。
- 5 アダプタのデフォルト iSCSI 名を変更するには、新しい名前を入力します。

入力した名前が世界中で一意的であることと、形式が適切であることを確認します。これが正しく行われないと、一部のストレージ デバイスで iSCSI アダプタが認識されない場合があります。

- 6 (オプション) iSCSI エイリアスを入力します。

エイリアスは、iSCSI アダプタの識別に使用する名前です。

### 結果

iSCSI 名を変更すると、新しい iSCSI セッションで使用されます。既存のセッションでは、ログアウトして再ログインするまで、新しい設定は使用されません。

## iSCSI のネットワーク接続の作成

ソフトウェアまたは依存型ハードウェア iSCSI アダプタと物理的ネットワーク アダプタの間のトラフィックのために接続を構成します。

次のタスクは、vSphere の標準スイッチによる iSCSI ネットワーク構成について説明します。

複数のアップリンク ポートがある vSphere Distributed を使用している場合は、ポートのバインドに、物理 NIC ごとに個別の分散ポート グループを作成します。次に、各分散ポート グループのアクティブなアップリンク ポートが 1 つだけになるようにチーム ポリシーを設定します。vSphere Distributed Switch の詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

### 手順

- 1 [iSCSI 用の単一 VMkernel アダプタの作成](#)

iSCSI ストレージ用にサービスを実行する VMkernel を物理ネットワーク アダプタに接続します。

## 2 iSCSI 用の追加 VMkernel アダプタの作成

iSCSI 用の物理ネットワーク アダプタが複数あり、すべての物理アダプタを単一の vSphere 標準スイッチに接続する場合は、このタスクを使用します。このタスクでは、物理アダプタおよび VMkernel アダプタを既存の vSphere 標準スイッチに追加します。

## 3 iSCSI のネットワーク ポリシーの変更

1 つの vSphere 標準スイッチを使用して複数の VMkernel アダプタを複数のネットワーク アダプタに接続する場合は、それぞれの VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが 1 つだけになるようネットワーク ポリシーを設定します。

## 4 iSCSI および VMkernel アダプタのバインド

iSCSI アダプタと VMkernel アダプタをバインドします。

## 5 ポート バインドの詳細の確認

iSCSI アダプタにバインドされた VMkernel アダプタのネットワーク詳細を確認します。

## iSCSI 用の単一 VMkernel アダプタの作成

iSCSI ストレージ用にサービスを実行する VMkernel を物理ネットワーク アダプタに接続します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [アクション] - [ネットワークの追加] の順にクリックします。
- 3 [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
- 4 [新しい標準スイッチ] を選択して、vSphere 標準スイッチを作成します。
- 5 [アダプタの追加] アイコンをクリックし、iSCSI に使用するネットワーク アダプタ (vmnic#) を選択します。  
[アクティブ アダプタ] にアダプタが割り当てられていることを確認します。

---

**重要：** 依存型ハードウェア iSCSI 用の VMkernel アダプタを作成する場合は、iSCSI コンポーネントに対応するネットワーク アダプタを選択します。[iSCSI アダプタとネットワーク アダプタとの間の関連性の特定](#) を参照してください。

---

- 6 ネットワーク ラベルを入力します。  
ネットワーク ラベルは、「iSCSI」 など、作成する VMkernel アダプタを識別するわかりやすい名前です。
- 7 IP 設定を指定します。
- 8 情報を確認し、[終了] をクリックします。

### 結果

これで、ホスト上の物理ネットワーク アダプタ (vmnic#) 用に、仮想 VMkernel アダプタ (vmk#) が作成されました。

## 次のステップ

ホストに iSCSI トラフィック用の物理ネットワーク アダプタが 1 つある場合は、作成した仮想アダプタを iSCSI アダプタにバインドする必要があります。

複数のネットワーク アダプタがある場合は、追加の VMkernel アダプタを作成してから、iSCSI とのバインドを実行します。仮想アダプタの数は、ホスト上の物理アダプタの数に対応している必要があります。

## iSCSI 用の追加 VMkernel アダプタの作成

iSCSI 用の物理ネットワーク アダプタが複数あり、すべての物理アダプタを単一の vSphere 標準スイッチに接続する場合は、このタスクを使用します。このタスクでは、物理アダプタおよび VMkernel アダプタを既存の vSphere 標準スイッチに追加します。

## 前提条件

iSCSI トラフィック用に指定された単一の物理ネットワーク アダプタに iSCSI VMkernel アダプタをマッピングする vSphere 標準スイッチを作成します。

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックし、[ネットワーク] をクリックします。
- 3 [仮想スイッチ] をクリックし、リストから、変更する vSphere スイッチを選択します。
- 4 追加のネットワーク アダプタをスイッチに接続します。
  - a [ホスト ネットワークの追加] アイコンをクリックします。
  - b [物理ネットワーク アダプタ] を選択し、[次へ] をクリックします。
  - c 既存のスイッチを使用していることを確認し、[次へ] をクリックします。
  - d [アダプタの追加] アイコンをクリックし、iSCSI に使用する 1 つ以上のネットワーク アダプタ (vmnic#) を選択します。  
  
依存型ハードウェア iSCSI アダプタの場合は、対応する iSCSI コンポーネントがある NIC だけを選択します。
  - e 構成を完了し、[終了] をクリックします。
- 5 追加したすべての物理ネットワーク アダプタに iSCSI VMkernel アダプタを作成します。  
  
VMkernel インターフェイスの数は、vSphere 標準スイッチ上の物理ネットワーク アダプタの数に対応している必要があります。
  - a [ホスト ネットワークの追加] アイコンをクリックします。
  - b [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
  - c 既存のスイッチを使用していることを確認し、[次へ] をクリックします。
  - d 構成を完了し、[終了] をクリックします。

## 次のステップ

すべての VMkernel アダプタ用のネットワーク ポリシーを変更して、各 VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが1つのみになるようにします。そのあとで、iSCSI VMkernel アダプタをソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタにバインドできます。

## iSCSI のネットワーク ポリシーの変更

1 つの vSphere 標準スイッチを使用して複数の VMkernel アダプタを複数のネットワーク アダプタに接続する場合は、それぞれの VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが1つだけになるようネットワーク ポリシーを設定します。

デフォルトでは、vSphere 標準スイッチ上の VMkernel アダプタごとに、すべてのネットワーク アダプタがアクティブなアダプタとして表示されます。この設定をオーバーライドして、各 VMkernel アダプタが、対応する1つのアクティブな物理アダプタのみにマッピングするようにしてください。たとえば、vmk1 は vmnic1 にマッピングし、vmk2 は vmnic2 にマッピングする、というようにします。

## 前提条件

VMkernel を iSCSI トラフィック用に指定された物理ネットワーク アダプタに接続する vSphere 標準スイッチを作成します。VMkernel アダプタの数は、vSphere 標準スイッチ上の物理アダプタの数に対応している必要があります。

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックし、[ネットワーク] をクリックします。
- 3 [仮想スイッチ] をクリックし、リストから、変更する vSphere スイッチを選択します。
- 4 vSwitch 図で VMkernel アダプタを選択し、[設定の編集] アイコンをクリックします。
- 5 [設定の編集] ウィザードで、[チーミングおよびフェイルオーバー] をクリックし、[フェイルオーバーの順序] で [オーバーライド] をクリックします。
- 6 1 つの物理アダプタのみをアクティブなアダプタとして指定し、残りのすべてのアダプタを [未使用のアダプタ] カテゴリに移動します。
- 7 vSphere 標準スイッチ上の各 iSCSI VMkernel インターフェイスについて、[手順 4](#) から [手順 6](#) までを繰り返します。

## 例：iSCSI ネットワーク ポリシー

次の表は、正しい iSCSI マッピングを示しています。ここでは、VMkernel アダプタごとのアクティブな物理ネットワーク アダプタが1つのみとなっています。

VMkernel アダプタ (vmk#)	物理ネットワーク アダプタ (vmnic#)
vmk1	[有効なアダプタ] vmnic1
	[未使用アダプタ] vmnic2
vmk2	[有効なアダプタ] vmnic2
	[未使用アダプタ] vmnic1

#### 次のステップ

このタスクを実行したあと、仮想 VMkernel アダプタを、ソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタにバインドします。

#### iSCSI および VMkernel アダプタのバインド

iSCSI アダプタと VMkernel アダプタをバインドします。

#### 前提条件

ホスト上の各物理ネットワーク アダプタ用に、仮想 VMkernel アダプタを作成します。複数の VMkernel アダプタを使用する場合は、正しいネットワーク ポリシーを設定します。

必要な権限：ホスト.構成.ストレージ パーティション構成

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックして、構成するソフトウェア iSCSI アダプタまたは依存型 iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ネットワーク ポートのバインド] タブをクリックし、[追加] をクリックします。
- 5 iSCSI アダプタとバインドする VMkernel アダプタを選択します。

**注：** VMkernel アダプタのネットワーク ポリシーがバインド要件に準拠していることを確認してください。

ソフトウェア iSCSI アダプタを、1 つ以上の VMkernel アダプタにバインドできます。依存型ハードウェア iSCSI アダプタの場合は、正しい物理 NIC と関連付けられた 1 つの VMkernel アダプタのみ使用できます。

- 6 [OK] をクリックします。

#### 結果

ネットワーク接続が、iSCSI アダプタの VMkernel ポート バインドのリストに表示されます。

#### ポート バインドの詳細の確認

iSCSI アダプタにバインドされた VMkernel アダプタのネットワーク詳細を確認します。

**手順**

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、リストからソフトウェア iSCSI アダプタ または依存型 iSCSI アダプタを選択します。
- 4 [アダプタの詳細] で、[ネットワーク ポートのバインド] タブをクリックし、[詳細の表示] をクリックします。
- 5 利用可能なタブを切り替えて、VMkernel アダプタ情報を確認します。

**iSCSI の動的または静的検出の設定**

動的検出では、イニシエータが指定された iSCSI ストレージ システムに接続するたびに、SendTargets 要求がシステムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供することで応答します。動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。

静的検出または動的検出を設定する場合は、新しい iSCSI ターゲットしか追加できません。既存のターゲットのパラメータは変更できません。これを変更するには、既存のターゲットを削除して新しいターゲットを追加します。

**前提条件**

必要な権限：ホスト.構成.ストレージ パーティション構成

**手順**

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、構成する iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ターゲット] タブをクリックします。
- 5 検出方法を構成します。

オプション	説明
動的検出	<ol style="list-style-type: none"> <li>[動的検出] をクリックし、[追加] をクリックします。</li> <li>ストレージ システムの IP アドレスまたは DNS 名を入力し、[OK] をクリックします。</li> <li>iSCSI アダプタを再スキャンします。</li> </ol> <p>iSCSI システムとの SendTargets セッションが確立された後、ホストは新たに検出されたすべてのターゲットで静的検出リストを作成します。</p>
静的検出	<ol style="list-style-type: none"> <li>[静的検出] をクリックし、[追加] をクリックします。</li> <li>ターゲットの情報を入力し、[OK] をクリックします。</li> <li>iSCSI アダプタを再スキャンします。</li> </ol>

**ソフトウェア iSCSI アダプタの無効化**

ソフトウェア iSCSI アダプタが必要なくなった場合は、それを無効にすることができます。

ソフトウェア iSCSI アダプタを無効にすると削除用のマークが付きます。次回のホストの再起動の際に、ホストからアダプタが削除されます。削除した後は、このアダプタに関連するストレージ デバイス上のすべての仮想マシンとその他のデータはホストにアクセスできなくなります。

#### 前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックして、ソフトウェア iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で [プロパティ] タブをクリックします。
- 5 [無効化] をクリックして、アダプタの無効化を確定します。  
ステータスは、アダプタが無効にされていることを示します。
- 6 ホストを再起動します。  
再起動後、アダプタはストレージ アダプタのリストに表示されなくなります。

#### 結果

iSCSI ソフトウェア アダプタが使用できなくなり、それに関連するストレージ デバイスにはアクセスできなくなります。後でアダプタを有効化することもできます。

## iSCSI アダプタの全般プロパティの変更

iSCSI アダプタに割り当てられたデフォルト iSCSI 名およびエイリアスを変更できます。独立ハードウェア iSCSI アダプタの場合は、デフォルトの IP 設定も変更できます。

---

**重要：** iSCSI アダプタのデフォルトのプロパティを変更する際は、その名前および IP アドレスの形式が適切なことを確認します。

---

#### 前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックし、設定するアダプタ (vmhba#) を選択します。
- 4 [アダプタの詳細] で、[プロパティ] タブをクリックし、[全般] パネルの [編集] をクリックします。

- 5 アダプタのデフォルト iSCSI 名を変更するには、新しい名前を入力します。

入力した名前が世界中で一意であることと、形式が適切であることを確認します。これが正しく行われないと、一部のストレージ デバイスで iSCSI アダプタが認識されない場合があります。

- 6 (オプション) iSCSI エイリアスを入力します。

エイリアスは、iSCSI アダプタの識別に使用する名前です。

## 結果

iSCSI 名を変更すると、新しい iSCSI セッションで使用されます。既存のセッションでは、ログアウトして再ログインするまで、新しい設定は使用されません。

## iSCSI ネットワークの設定

ソフトウェアおよび依存型ハードウェア iSCSI アダプタは、VMkernel ネットワーキングによって異なります。ソフトウェアまたは依存型ハードウェアの iSCSI アダプタを使用する場合は、iSCSI コンポーネントと物理ネットワーク アダプタとのトラフィック用に接続を構成する必要があります。

ネットワーク接続の構成には、各物理ネットワーク アダプタへの仮想 VMkernel アダプタの作成が含まれます。その際に、VMkernel アダプタを適切な iSCSI アダプタと関連付けます。このプロセスをポート バインドと呼びます。

ソフトウェア iSCSI でのネットワーク接続の使用時機と方法に関する特別の考慮事項については、<http://kb.vmware.com/kb/2038869> にある VMware ナレッジ ベースの記事を参照してください。

## iSCSI 構成での複数のネットワーク アダプタ

ソフトウェアおよび依存型ハードウェア iSCSI でホストが複数の物理ネットワーク アダプタを使用している場合、マルチパス用のアダプタを使用します。

ソフトウェア iSCSI アダプタは、ホストで使用可能な物理 NIC で接続できます。依存型 iSCSI アダプタを接続する場合は、必ず固有の物理 NIC へ接続する必要があります。

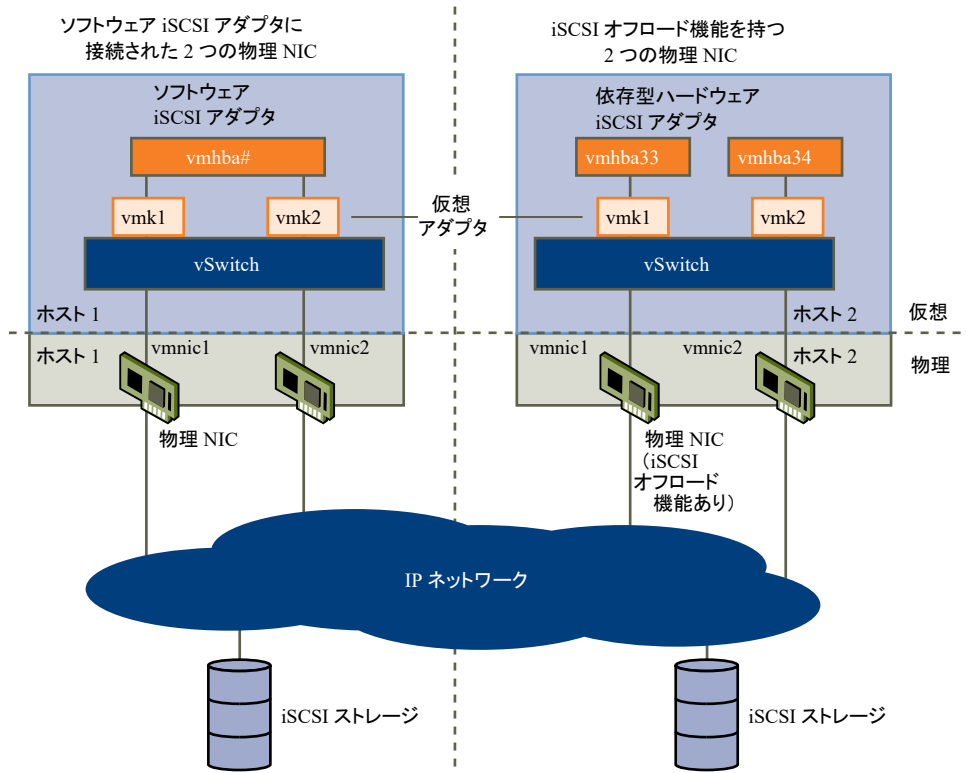
---

**注：** 物理 NIC は、接続対象の iSCSI ストレージ システムと同じサブネット上になければなりません。

---



図 10-1. iSCSI を使用したネットワーク



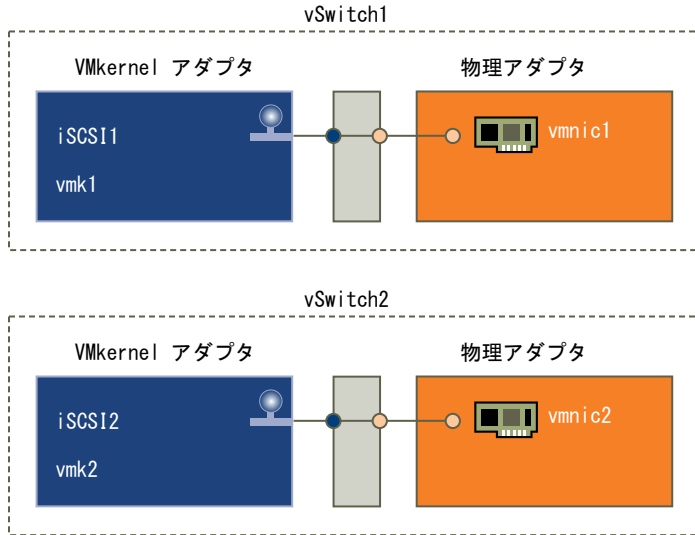
iSCSI アダプタと物理 NIC は、仮想ネットワーク アダプタまたは VMkernel ポートとも呼ばれる、仮想 VMkernel アダプタを介して接続されます。それぞれの仮想ネットワーク アダプタと物理ネットワーク アダプタ間で 1:1 のマッピングを使用して、VMkernel アダプタ (vmk) を vSphere スイッチ (vSwitch) に作成します。

複数の NIC を使用している場合に 1:1 のマッピングを実行する 1 つの方法は、仮想 - 物理アダプタの組み合わせごとに個別の vSphere スイッチを指定することです。

**注：** 個別の vSphere スイッチを使用する場合、それらを異なる IP サブネットに接続する必要があります。そうしなければ、VMkernel アダプタで接続問題が発生する場合があります、ホストは iSCSI LUN を検出できなくなります。

次の例は、vSphere 標準スイッチを使用する構成を示していますが、Distributed Switch も使用できます。vSphere Distributed Switch の詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

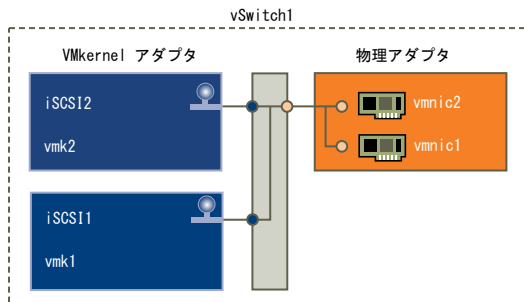
図 10-2. 個別の vSphere 標準スイッチでの 1 対 1 のアダプタ マッピング



代わりに、すべての NIC と VMkernel アダプタをひとつの vSphere 標準スイッチに追加する方法があります。この場合、デフォルトのネットワーク設定をオーバーライドし、唯一の対応するアクティブな物理アダプタに各 VMkernel アダプタをマップする必要があります。

**注：** VMkernel アダプタが同じサブネット上にある場合、単一 vSwitch 構成を使用する必要があります。

図 10-3. 1 つの vSphere 標準スイッチでの 1 対 1 のアダプタ マッピング



次の表にこのトピックで説明した iSCSI 管理ネットワークを要約します。

表 10-2. iSCSI のネットワーク構成

iSCSI アダプタ	VMkernel アダプタ (ポート)	物理アダプタ (NIC)
ソフトウェア iSCSI		
vmhba32	vmk1	vmnic1
	vmk2	vmnic2
依存型ハードウェア iSCSI		
vmhba33	vmk1	vmnic1
vmhba34	vmk2	vmnic2

## ESXi で iSCSI ポート バインドを使用する際のガイドライン

iSCSI にバインドした複数の VMkernel アダプタを使用して、単一の IP アドレスをブロードキャストする iSCSI アレイへのパスを複数持つことができます。

マルチパスにポート バインドを使用する場合は、次のガイドラインに従ってください。

- アレイ ターゲットの iSCSI ポートは VMkernel アダプタと同じブロードキャスト ドメインおよび IP サブネットに存在する必要があります。
- iSCSI ポート バインドに使用する VMkernel アダプタはすべて、同じブロードキャスト ドメインおよび IP サブネットに存在する必要があります。
- iSCSI 接続に使用する VMkernel アダプタはすべて、同じ仮想スイッチに存在する必要があります。
- ポート バインドはネットワーク ルーティングをサポートしていません。

以下の条件が存在するときには、ポート バインドは使用しないでください。

- アレイ ターゲットの iSCSI ポートが別のブロードキャスト ドメインおよび IP サブネットに存在する。
- iSCSI 接続に使用する VMkernel アダプタが、別のブロードキャスト ドメイン、IP サブネットに存在するか、異なる仮想スイッチを使用している。
- iSCSI アレイへのアクセスにルーティングが必須である。

## iSCSI のネットワーク接続の作成

ソフトウェアまたは依存型ハードウェア iSCSI アダプタと物理的ネットワーク アダプタの間のトラフィックのために接続を構成します。

次のタスクは、vSphere の標準スイッチによる iSCSI ネットワーク構成について説明します。

複数のアップリンク ポートがある vSphere Distributed を使用している場合は、ポートのバインドに、物理 NIC ごとに個別の分散ポート グループを作成します。次に、各分散ポート グループのアクティブなアップリンク ポートが 1 つだけになるようにチーム ポリシーを設定します。vSphere Distributed Switch の詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

### 手順

#### 1 iSCSI 用の単一 VMkernel アダプタの作成

iSCSI ストレージ用にサービスを実行する VMkernel を物理ネットワーク アダプタに接続します。

#### 2 iSCSI 用の追加 VMkernel アダプタの作成

iSCSI 用の物理ネットワーク アダプタが複数あり、すべての物理アダプタを単一の vSphere 標準スイッチに接続する場合は、このタスクを使用します。このタスクでは、物理アダプタおよび VMkernel アダプタを既存の vSphere 標準スイッチに追加します。

#### 3 iSCSI のネットワーク ポリシーの変更

1 つの vSphere 標準スイッチを使用して複数の VMkernel アダプタを複数のネットワーク アダプタに接続する場合は、それぞれの VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが 1 つだけになるようネットワーク ポリシーを設定します。

#### 4 iSCSI および VMkernel アダプタのバインド

iSCSI アダプタと VMkernel アダプタをバインドします。

#### 5 ポート バインドの詳細の確認

iSCSI アダプタにバインドされた VMkernel アダプタのネットワーク詳細を確認します。

### iSCSI 用の単一 VMkernel アダプタの作成

iSCSI ストレージ用にサービスを実行する VMkernel を物理ネットワーク アダプタに接続します。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [アクション] - [ネットワークの追加] の順にクリックします。
- 3 [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
- 4 [新しい標準スイッチ] を選択して、vSphere 標準スイッチを作成します。
- 5 [アダプタの追加] アイコンをクリックし、iSCSI に使用するネットワーク アダプタ (vmnic#) を選択します。  
[アクティブ アダプタ] にアダプタが割り当てられていることを確認します。

---

**重要：** 依存型ハードウェア iSCSI 用の VMkernel アダプタを作成する場合は、iSCSI コンポーネントに対応するネットワーク アダプタを選択します。[iSCSI アダプタとネットワーク アダプタとの間の関連性の特定](#) を参照してください。

---

- 6 ネットワーク ラベルを入力します。  
ネットワーク ラベルは、「iSCSI」 など、作成する VMkernel アダプタを識別するわかりやすい名前です。
- 7 IP 設定を指定します。
- 8 情報を確認し、[終了] をクリックします。

#### 結果

これで、ホスト上の物理ネットワーク アダプタ (vmnic#) 用に、仮想 VMkernel アダプタ (vmk#) が作成されました。

#### 次のステップ

ホストに iSCSI トラフィック用の物理ネットワーク アダプタが 1 つある場合は、作成した仮想アダプタを iSCSI アダプタにバインドする必要があります。

複数のネットワーク アダプタがある場合は、追加の VMkernel アダプタを作成してから、iSCSI とのバインドを行います。仮想アダプタの数は、ホスト上の物理アダプタの数に対応している必要があります。

### iSCSI 用の追加 VMkernel アダプタの作成

iSCSI 用の物理ネットワーク アダプタが複数あり、すべての物理アダプタを単一の vSphere 標準スイッチに接続する場合は、このタスクを使用します。このタスクでは、物理アダプタおよび VMkernel アダプタを既存の vSphere 標準スイッチに追加します。

## 前提条件

iSCSI トラフィック用に指定された単一の物理ネットワーク アダプタに iSCSI VMkernel アダプタをマッピングする vSphere 標準スイッチを作成します。

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックし、[ネットワーク] をクリックします。
- 3 [仮想スイッチ] をクリックし、リストから、変更する vSphere スイッチを選択します。
- 4 追加のネットワーク アダプタをスイッチに接続します。
  - a [ホスト ネットワークの追加] アイコンをクリックします。
  - b [物理ネットワーク アダプタ] を選択し、[次へ] をクリックします。
  - c 既存のスイッチを使用していることを確認し、[次へ] をクリックします。
  - d [アダプタの追加] アイコンをクリックし、iSCSI に使用する 1 つ以上のネットワーク アダプタ (vmnic#) を選択します。

依存型ハードウェア iSCSI アダプタの場合は、対応する iSCSI コンポーネントがある NIC だけを選択します。
  - e 構成を完了し、[終了] をクリックします。
- 5 追加したすべての物理ネットワーク アダプタに iSCSI VMkernel アダプタを作成します。

VMkernel インターフェイスの数は、vSphere 標準スイッチ上の物理ネットワーク アダプタの数に対応している必要があります。

  - a [ホスト ネットワークの追加] アイコンをクリックします。
  - b [VMkernel ネットワーク アダプタ] を選択し、[次へ] をクリックします。
  - c 既存のスイッチを使用していることを確認し、[次へ] をクリックします。
  - d 構成を完了し、[終了] をクリックします。

## 次のステップ

すべての VMkernel アダプタ用のネットワーク ポリシーを変更して、各 VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが 1 つのみになるようにします。そのあとで、iSCSI VMkernel アダプタをソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタにバインドできます。

## iSCSI のネットワーク ポリシーの変更

1 つの vSphere 標準スイッチを使用して複数の VMkernel アダプタを複数のネットワーク アダプタに接続する場合は、それぞれの VMkernel アダプタに対してアクティブな物理ネットワーク アダプタが 1 つだけになるようネットワーク ポリシーを設定します。

デフォルトでは、vSphere 標準スイッチ上の VMkernel アダプタごとに、すべてのネットワーク アダプタがアクティブなアダプタとして表示されます。この設定をオーバーライドして、各 VMkernel アダプタが、対応する 1 つのアクティブな物理アダプタのみにマッピングするようにしてください。たとえば、vmk1 は vmnic1 にマッピングし、vmk2 は vmnic2 にマッピングする、というようにします。

#### 前提条件

VMkernel を iSCSI トラフィック用に指定された物理ネットワーク アダプタに接続する vSphere 標準スイッチを作成します。VMkernel アダプタの数は、vSphere 標準スイッチ上の物理アダプタの数に対応している必要があります。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックし、[ネットワーク] をクリックします。
- 3 [仮想スイッチ] をクリックし、リストから、変更する vSphere スイッチを選択します。
- 4 vSwitch 図で VMkernel アダプタを選択し、[設定の編集] アイコンをクリックします。
- 5 [設定の編集] ウィザードで、[チーミングおよびフェイルオーバー] をクリックし、[フェイルオーバーの順序] で [オーバーライド] をクリックします。
- 6 1 つの物理アダプタのみをアクティブなアダプタとして指定し、残りのすべてのアダプタを [未使用のアダプタ] カテゴリに移動します。
- 7 vSphere 標準スイッチ上の各 iSCSI VMkernel インターフェイスについて、[手順 4](#) から [手順 6](#) までを繰り返します。

#### 例：iSCSI ネットワーク ポリシー

次の表は、正しい iSCSI マッピングを示しています。ここでは、VMkernel アダプタごとのアクティブな物理ネットワーク アダプタが 1 つのみとなっています。

VMkernel アダプタ (vmk#)	物理ネットワーク アダプタ (vmnic#)
vmk1	[有効なアダプタ]
	vmnic1
	[未使用アダプタ]
	vmnic2
vmk2	[有効なアダプタ]
	vmnic2
	[未使用アダプタ]
	vmnic1

#### 次のステップ

このタスクを実行したあと、仮想 VMkernel アダプタを、ソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタにバインドします。

### iSCSI および VMkernel アダプタのバインド

iSCSI アダプタと VMkernel アダプタをバインドします。

## 前提条件

ホスト上の各物理ネットワーク アダプタ用に、仮想 VMkernel アダプタを作成します。複数の VMkernel アダプタを使用する場合は、正しいネットワーク ポリシーを設定します。

必要な権限：ホスト.構成.ストレージ パーティション構成

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックして、構成するソフトウェア iSCSI アダプタまたは依存型 iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ネットワーク ポートのバインド] タブをクリックし、[追加] をクリックします。
- 5 iSCSI アダプタとバインドする VMkernel アダプタを選択します。

---

**注：** VMkernel アダプタのネットワーク ポリシーがバインド要件に準拠していることを確認してください。

---

ソフトウェア iSCSI アダプタを、1 つ以上の VMkernel アダプタにバインドできます。依存型ハードウェア iSCSI アダプタの場合は、正しい物理 NIC と関連付けられた 1 つの VMkernel アダプタのみ使用できます。

- 6 [OK] をクリックします。

## 結果

ネットワーク接続が、iSCSI アダプタの VMkernel ポート バインドのリストに表示されます。

## ポート バインドの詳細の確認

iSCSI アダプタにバインドされた VMkernel アダプタのネットワーク詳細を確認します。

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、リストからソフトウェア iSCSI アダプタ または依存型 iSCSI アダプタを選択します。
- 4 [アダプタの詳細] で、[ネットワーク ポートのバインド] タブをクリックし、[詳細の表示] をクリックします。
- 5 利用可能なタブを切り替えて、VMkernel アダプタ情報を確認します。

## iSCSI ネットワークの管理

iSCSI アダプタと関連付けられた物理と VMkernel の両方のネットワーク アダプタに特別な考慮事項が適用されます。

iSCSI にネットワーク接続した後は、多数のネットワーク ダイアログ ボックスの iSCSI インジケータは有効になります。このインジケータは、特定の仮想または物理ネットワーク アダプタが iSCSI バインドであることを示します。iSCSI トラフィックで中断を回避するには、iSCSI バインドの仮想および物理ネットワーク アダプタを管理するときこれらのガイドラインおよび考慮事項に従います。

- VMkernel ネットワーク アダプタに接続先の iSCSI ストレージ ポータルと同じサブネットでアドレスが割り当てられていることを確認します。
- VMkernel アダプタを使用する iSCSI アダプタは、異なるサブネット上の iSCSI ポートが iSCSI アダプタによって検出されたとしても、これらの iSCSI ポートに接続できません。
- 個別の vSphere スイッチを使用して、物理ネットワーク アダプタと VMkernel アダプタに接続するとき、vSphere スイッチが異なる IP サブネットに接続していることを確認します。
- VMkernel アダプタが同じサブネットにある場合、それらは 1 つの vSwitch に接続されている必要があります。
- VMkernel アダプタを異なる vSphere スイッチに移行する場合には、関連する物理アダプタを移動します。
- iSCSI バインドの VMkernel アダプタまたは物理ネットワーク アダプタに構成変更を行わないでください。
- VMkernel アダプタおよび物理ネットワーク アダプタの関連付けを解除する可能性がある変更を行わないでください。アダプタの 1 つまたはアダプタに接続する vSphere スイッチを削除する場合に関連付けを解除する、または接続の 1:1 ネットワーク ポリシーを変更できます。

## iSCSI ネットワークのトラブルシューティング

警告サインは、iSCSI バインドの VMkernel アダプタの非準拠のポート グループ ポリシーを示します。

### 問題

VMkernel アダプタのポート グループ ポリシーは、次のケースで非準拠と見なされます。

- VMkernel アダプタがアクティブな物理ネットワーク アダプタに接続されていない。
- VMkernel アダプタが複数の物理ネットワーク アダプタに接続されている。
- VMkernel アダプタが 1 つまたは複数のスタンバイ物理アダプタに接続されている。
- アクティブな物理アダプタが変更されている。

### 解決方法

[iSCSI のネットワーク ポリシーの変更](#)の手順に従い、iSCSI バインドの VMkernel アダプタに正しいネットワーク ポリシーを設定します。

## iSCSI でのジャンボ フレームの使用

ESXi は iSCSI と ジャンボ フレーム との併用をサポートします。

ジャンボ フレーム は 1500 バイトを超えるサイズのイーサネット フレームです。最大転送ユニット (MTU) パラメータは ジャンボ フレーム のサイズを測定するために通常使用されます。ESXi によって、ジャンボ フレーム を MTU が 最大 9000 バイトまでに指定できます。



iSCSI トラフィックに ジャンボ フレーム を使用するとき、次の点に注意してください。

- ジャンボ フレームを有効にするには、ネットワークがジャンボ フレームのエンド ツー エンドをサポートしている必要があります。
- ご使用の物理 NIC および iSCSI HBA がジャンボ フレームを確実にサポートしていることをベンダーにご確認ください。
- ジャンボ フレーム の物理ネットワーク スイッチを設定して検証するには、ベンダーのドキュメントを参照してください。

以下の表では、ESXi が ジャンボ フレーム に提供するサポートのレベルを説明します。

表 10-3. ジャンボ フレームのサポート

iSCSI アダプタのタイプ	ジャンボ フレームのサポート
ソフトウェア iSCSI	サポート
依存型ハードウェア iSCSI	サポートあり。ベンダーに確認。
独立型ハードウェア iSCSI	サポートあり。ベンダーに確認。

## ソフトウェア iSCSI と依存型ハードウェア iSCSI でのジャンボ フレームの有効化

vSphere Web Client 内のソフトウェア iSCSI アダプタおよび依存型ハードウェア iSCSI アダプタでジャンボ フレームを有効にするには、最大転送ユニット (MTU) パラメータのデフォルト値を変更してください。

iSCSI トラフィックに使用している vSphere スイッチの MTU パラメータを変更できます。詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックし、[ネットワーク] をクリックします。
- 3 [仮想スイッチ] をクリックし、リストから、変更する vSphere スイッチを選択します。
- 4 [設定の編集] アイコンをクリックします。
- 5 [プロパティ] ページで、MTU パラメータを変更します。

この手順は、その標準スイッチ上のすべての物理 NIC に対して MTU を設定します。MTU 値は、標準スイッチに接続されているすべての NIC 間で最大の MTU サイズに設定されます。ESXi は、最大 9,000 バイトまでの MTU サイズをサポートします。

## 独立型のハードウェア iSCSI のジャンボ フレームの有効化

vSphere Web Client 内の独立型ハードウェア iSCSI アダプタでジャンボ フレームを有効にするには、最大転送ユニット (MTU) パラメータのデフォルト値を変更してください。

[詳細設定オプション] 設定を使用し、iSCSI HBA の MTU パラメータを変更します。

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、アダプタのリストから独立型ハードウェア iSCSI アダプタを選択します。
- 4 [アダプタの詳細] で、[詳細オプション] タブをクリックし、[編集] をクリックします。
- 5 MTU パラメータの値を変更します。

ESXi 最大 9,000 バイトまでの MTU サイズをサポートします。

## iSCSI アダプタの検出アドレスの構成

iSCSI アダプタがネットワーク上のアクセス可能なストレージ リソースを特定できるように、ターゲット検出アドレスを設定する必要があります。

ESXi システムは、次の検出方法をサポートしています。

### 動的検出

SendTargets 検出とも呼ばれます。イニシエータが指定された iSCSI サーバに接続するたびに、イニシエータはターゲットの SendTargets 要求をサーバに送信します。サーバは、使用可能なターゲットのリストをイニシエータに提供することで応答します。これらのターゲットの名前および IP アドレスは、[静的検出] タブに表示されます。動的検出で追加された静的ターゲットを削除する場合、このターゲットは、次の再スキャン実行時、iSCSI アダプタのリセット時、またはホストの再起動時にリストに戻すことができます。

---

**注：** ESXi は、ソフトウェア iSCSI および依存型ハードウェア iSCSI を使用して、指定した iSCSI サーバアドレスの IP ファミリーに基づいてターゲット アドレスをフィルタリングします。アドレスが IPv4 の場合、iSCSI サーバからの SendTargets 応答で取得される可能性のある IPv6 アドレスは除外されます。iSCSI サーバを指定するために DNS 名が使用されている場合や、iSCSI サーバからの SendTargets 応答に DNS 名が含まれている場合、ESXi は、DNS ルックアップで最初に解決されたエントリの IP ファミリーを使用します。

---

### 静的検出

動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。iSCSI アダプタは、提供したターゲットのリストを使用して、iSCSI サーバに接続して通信します。

## iSCSI の動的または静的検出の設定

動的検出では、イニシエータが指定された iSCSI ストレージ システムに接続するたびに、SendTargets 要求がシステムに送信されます。iSCSI システムは、使用可能なターゲットのリストをイニシエータに提供することで応答します。動的検出方法の他に、静的検出を使用して、ターゲットの情報を手動で入力することも可能です。

静的検出または動的検出を設定する場合は、新しい iSCSI ターゲットしか追加できません。既存のターゲットのパラメータは変更できません。これを変更するには、既存のターゲットを削除して新しいターゲットを追加します。

### 前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、構成する iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ターゲット] タブをクリックします。
- 5 検出方法を構成します。

オプション	説明
動的検出	<ol style="list-style-type: none"> <li>a [動的検出] をクリックし、[追加] をクリックします。</li> <li>b ストレージ システムの IP アドレスまたは DNS 名を入力し、[OK] をクリックします。</li> <li>c iSCSI アダプタを再スキャンします。</li> </ol> <p>iSCSI システムとの SendTargets セッションが確立された後、ホストは新たに検出されたすべてのターゲットで静的検出リストを作成します。</p>
静的検出	<ol style="list-style-type: none"> <li>a [静的検出] をクリックし、[追加] をクリックします。</li> <li>b ターゲットの情報を入力し、[OK] をクリックします。</li> <li>c iSCSI アダプタを再スキャンします。</li> </ol>

## 動的および静的 iSCSI ターゲットの削除

ターゲットのリストに表示される iSCSI サーバを削除します。

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、変更する iSCSI アダプタをリストから選択します。
- 4 [アダプタの詳細] で、[ターゲット] タブをクリックします。
- 5 [動的検出] と [静的検出] を切り替えます。
- 6 削除する iSCSI サーバを選択し、[削除] をクリックします。
- 7 iSCSI アダプタを再スキャンします。

動的に検出された静的ターゲットを削除する場合は、再スキャンを実行する前にそのターゲットをストレージ システムから削除する必要があります。そうしないと、アダプタを再スキャンするときに、ホストが自動的にターゲットを検出し、静的ターゲットのリストに追加することになります。

## iSCSI アダプタの CHAP パラメータの構成

リモート ターゲットへの接続に iSCSI テクノロジーで使用する IP ネットワークでは、転送するデータが保護されないため、接続のセキュリティを確保する必要があります。iSCSI の実装するプロトコルの 1 つに、CHAP（チャレンジ ハンドシェイク認証プロトコル）があります。CHAP は、ネットワーク上のターゲットにアクセスするイニシエータの正当性を検証します。

CHAP は、三方向ハンドシェイク アルゴリズムを使用してホストの ID を検証します。また該当する場合、ホストとターゲットが接続を確立するときに iSCSI ターゲットの ID を検証します。検証は、イニシエータとターゲットで共有する事前定義されたプライベート値、すなわち CHAP シークレットに基づいています。

ESXi は、アダプタ レベルで CHAP 認証をサポートします。この場合、すべてのターゲットが、iSCSI イニシエータから同じ CHAP 名およびシークレットを受信します。また、ソフトウェア iSCSI アダプタおよび依存型ハードウェア iSCSI アダプタの場合、ESXi はターゲットごとの CHAP 認証もサポートしています。これにより、ターゲットごとに異なる証明書を構成して、セキュリティのレベルを向上させることができます。

## CHAP 認証方法の選択

ESXi は、すべてのタイプの iSCSI イニシエータに対して一方向 CHAP をサポートし、ソフトウェア iSCSI および依存型ハードウェア iSCSI に対して双方向 CHAP をサポートします。

CHAP を構成する前に、iSCSI ストレージ システムで CHAP が有効になっているかどうかと、システムがサポートする CHAP 認証方法を確認します。CHAP が有効になっている場合、イニシエータ用に有効にして、CHAP の認証証明書が iSCSI ストレージの認証証明書と一致することを確認します。

ESXi は、次の CHAP 認証方法をサポートします。

### 一方向 CHAP

一方向の CHAP 認証では、ターゲットはイニシエータを認証しますが、イニシエータはターゲットを認証しません。

### 双方向 CHAP

双方向の CHAP 認証では、セキュリティのレベルが強化され、イニシエータがターゲットを認証できます。この方法は、ソフトウェア iSCSI アダプタおよび依存型ハードウェア iSCSI アダプタに対してのみサポートされます。

ソフトウェア iSCSI アダプタおよび依存型ハードウェア iSCSI アダプタでは、一方向 CHAP および双方 CHAP を各アダプタに対して設定するか、ターゲット レベルで設定できます。独立型ハードウェア iSCSI は、アダプタ レベルでのみ CHAP をサポートします。

CHAP パラメータを設定する場合、CHAP のセキュリティ レベルを指定します。

**注：** CHAP のセキュリティ レベルを指定する場合、ストレージ アレイの応答方法は、そのアレイの CHAP の実装によって異なり、また、ベンダーによって異なります。さまざまなイニシエータおよびターゲット構成における CHAP 認証の動作については、アレイのドキュメントを参照してください。

表 10-4. CHAP のセキュリティ レベル

CHAP のセキュリティ レベル	説明	サポート
なし	ホストは CHAP 認証を使用しません。現在有効な場合、このオプションを選択すると認証は無効になります。	ソフトウェア iSCSI 依存型ハードウェア iSCSI 独立型ハードウェア iSCSI
ターゲットによって要求されている場合は一方向 CHAP を使用する	ホストは CHAP 以外の接続を優先しますが、ターゲットが要求する場合は CHAP 接続を使用できます。	ソフトウェア iSCSI 依存型ハードウェア iSCSI

表 10-4. CHAP のセキュリティ レベル（続き）

CHAP のセキュリティ レベル	説明	サポート
ターゲットで禁止されていない場合は一方方向 CHAP を使用する	ホストは CHAP を優先しますが、ターゲットが CHAP をサポートしていない場合は CHAP 以外の接続を使用できます。	ソフトウェア iSCSI 依存型ハードウェア iSCSI 独立型ハードウェア iSCSI
一方方向 CHAP を使用する	ホストは正常な CHAP 認証を要求します。CHAP ネゴシエーションに失敗した場合、接続に失敗します。	ソフトウェア iSCSI 依存型ハードウェア iSCSI 独立型ハードウェア iSCSI
双方方向 CHAP を使用する	ホストおよびターゲットは双方方向 CHAP をサポートしています。	ソフトウェア iSCSI 依存型ハードウェア iSCSI

## iSCSI アダプタの CHAP の設定

iSCSI アダプタ レベルで CHAP 名およびシークレットを設定すると、すべてのターゲットがアダプタから同じパラメータを受け取ります。デフォルトでは、すべての検出アドレスまたは静的ターゲットは、アダプタ レベルで設定された CHAP パラメータを継承します。

CHAP 名は英数字で 511 文字を超えないようにし、CHAP シークレットは英数字で 255 文字を超えないようにします。一部のアダプタでは、この上限の値がさらに小さい場合があります。たとえば、QLogic アダプタの上限値は、CHAP 名では 255 文字、CHAP シークレットでは 100 文字です。

### 前提条件

- ソフトウェア iSCSI または依存型ハードウェア iSCSI の CHAP パラメータを設定する前に、一方方向 CHAP を構成するか、双方方向 CHAP を構成するかを決めます。独立型ハードウェア iSCSI アダプタは、双方方向 CHAP をサポートしません。
- ストレージ側で構成された CHAP パラメータを確認します。構成するパラメータは、ストレージ側のものと一致している必要があります。
- 必要な権限：ホスト.構成.ストレージ パーティション構成

### 手順

- 1 ストレージ アダプタを表示し、構成する iSCSI アダプタを選択します。
- 2 [アダプタの詳細] で、[プロパティ] タブをクリックし、[認証] パネルの [編集] をクリックします。
- 3 認証方法を指定します。
  - [なし]
  - [ターゲットによって要求されている場合は一方方向 CHAP を使用する]
  - [ターゲットで禁止されていない場合は一方方向 CHAP を使用する]
  - [一方方向 CHAP を使用する]
  - [双方方向 CHAP を使用する]。双方方向 CHAP を構成するには、このオプションを選択する必要があります。

#### 4 発信 CHAP 名を指定します。

指定する名前が、ストレージ側で構成した名前と一致するようにします。

- iSCSI アダプタ名に CHAP 名を設定するには、[イニシエータ名の使用] を選択します。
- CHAP 名を iSCSI イニシエータ名以外の名前に設定するには、[イニシエータ名の使用] を選択解除し、[名前] テキスト ボックスに名前を入力します。

#### 5 認証の一部として、使用する発信 CHAP シークレットを入力します。ストレージ側で入力するのと同じシークレットを使用してください。

#### 6 双方向 CHAP を構成する場合は、受信する CHAP 証明書を指定します。

発信 CHAP と受信 CHAP には、別々のシークレットを使用してください。

#### 7 [OK] をクリックします。

#### 8 iSCSI アダプタを再スキャンします。

### 結果

CHAP のパラメータを変更した場合、そのパラメータは新しい iSCSI セッションで使用されます。既存のセッションでは、ログアウトして再ログインするまで、新しい設定は使用されません。

## ターゲットの CHAP の設定

ソフトウェア iSCSI アダプタおよび依存型ハードウェア iSCSI アダプタを使用する場合、検出アドレスまたは静的ターゲットごとに異なる CHAP 証明書を構成できます。

CHAP 名は英数字で 511 文字以内に、CHAP シークレットは英数字で 255 文字以内にしてください。

### 前提条件

- ソフトウェア iSCSI または依存型ハードウェア iSCSI の CHAP パラメータを設定する前に、一方向 CHAP を構成するか、双方向 CHAP を構成するかを決めます。
- ストレージ側で構成された CHAP パラメータを確認します。構成するパラメータは、ストレージ側のものと一致している必要があります。
- ストレージ アダプタにアクセスします。
- 必要な権限：ホスト.構成.ストレージ パーティション構成

### 手順

- 1 構成する iSCSI アダプタを選択し、[アダプタの詳細] の [ターゲット] タブをクリックします。
- 2 [動的検出] または [静的検出] をクリックします。
- 3 使用可能なターゲットのリストから、構成するターゲットを選択し、[認証] をクリックします。
- 4 [親から継承] を選択解除し、認証方法を指定します。
  - [なし]
  - [ターゲットによって要求されている場合は一方向 CHAP を使用する]

- [ターゲットで禁止されていない場合は一方向 CHAP を使用する]
- [一方向 CHAP を使用する]
- [双方向 CHAP を使用する]。双方向 CHAP を構成するには、このオプションを選択する必要があります。

## 5 発信 CHAP 名を指定します。

指定する名前が、ストレージ側で構成した名前と一致するようにします。

- iSCSI アダプタ名に CHAP 名を設定するには、[イニシエータ名の使用] を選択します。
- CHAP 名を iSCSI イニシエータ名以外の名前に設定するには、[イニシエータ名の使用] を選択解除し、[名前] テキスト ボックスに名前を入力します。

## 6 認証の一部として、使用する発信 CHAP シークレットを入力します。ストレージ側で入力するのと同じシークレットを使用してください。

## 7 双方向 CHAP を構成する場合は、受信する CHAP 証明書を指定します。

発信 CHAP と受信 CHAP には、別々のシークレットを使用してください。

## 8 [OK] をクリックします。

## 9 iSCSI アダプタを再スキャンします。

### 結果

CHAP のパラメータを変更した場合、そのパラメータは新しい iSCSI セッションで使用されます。既存のセッションでは、ログアウトして再ログインするまで、新しい設定は使用されません。

## CHAP の無効化

CHAP は、ストレージ システムで必要とされない場合には、無効にすることができます。

CHAP 認証を必要とするシステムで CHAP を無効にすると、ホストが再起動されるか、コマンド ラインでセッションを終了するか、またはストレージ システムで強制ログアウトが行われるまで、既存の iSCSI セッションは有効なままとなります。セッションの終了後は、CHAP を必要とするターゲットには接続できなくなります。

必要な権限： ホスト.構成.ストレージ パーティション構成

### 手順

#### 1 CHAP 認証情報ダイアログ ボックスを開きます。

#### 2 ソフトウェア iSCSI アダプタと依存型ハードウェア iSCSI アダプタの場合、相互 CHAP だけを無効にして一方向 CHAP を残すには、相互 CHAP 領域で [CHAP を使用しない] を選択します。

#### 3 一方向 CHAP を無効にするには、[CHAP] 領域で [CHAP を使用しない] を選択します。

相互 CHAP が設定されている場合、一方向 CHAP を無効にすると、相互 CHAP は自動的に [CHAP を使用しない] に変更されます。

#### 4 [OK] をクリックします。

## iSCSI 詳細パラメータの構成

iSCSI イニシエータに追加パラメータを構成することが必要になる場合があります。たとえば、一部の iSCSI ストレージ システムでは、ポート間で iSCSI トラフィックを動的に移動するために ARP（アドレス解決プロトコル）リダイレクトが必要です。この場合、ホストで ARP リダイレクトを有効にする必要があります。

次の表に、vSphere Web Client を使用して構成できる iSCSI の詳細パラメータを示します。また、vSphere CLI コマンドを使用すると、この詳細パラメータの一部を構成できます。詳細については、『vSphere Command-Line Interface スタート ガイド』ドキュメントを参照してください。

**重要：** VMware サポート チームまたはストレージのベンダーの指示がない限り、iSCSI の詳細設定を変更しないでください。

表 10-5. iSCSI イニシエータの追加パラメータ

詳細パラメータ	説明	構成可能な対象
ヘッダ ダイジェスト	データの整合性を高めます。ヘッダ ダイジェストが有効な場合、システムは CRC32C アルゴリズムを使用して各 iSCSI PDU（Protocol Data Unit）のヘッダ部分でチェックサムを実行し、検証を行います。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
データ ダイジェスト	データの整合性を高めます。データ ダイジェストが有効な場合、システムは CRC32C アルゴリズムを使用して各 PDU のデータ部分でチェックサムを実行し、検証を行います。  <b>注：</b> Intel Nehalem プロセッサを使用するシステムでは、ソフトウェア iSCSI の iSCSI ダイジェスト計算が軽減されるため、パフォーマンスへの影響が小さくなります。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
最大 R2T 残数	ACK の PDU が受信されるまで移行中の状態にしてもよい R2T（Ready to Transfer）PDU を定義します。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
第 1 パースト長	単一の SCSI コマンドの実行時に iSCSI イニシエータがターゲットに送信できる非請求データの最大量（バイト単位）を指定します。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
最大パースト長	Data-In または請求 Data-Out の iSCSI シーケンスでの最大 SCSI データ ペイロード（バイト単位）です。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
最大受信データ セグメント長	iSCSI PDU で受信できる最大データ セグメント長（バイト単位）です。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
セッション リカバリ タイムアウト	セッション リカバリの実行中に、セッション リカバリを無効にする時間を秒単位で指定します。タイムアウトの制限を超えると、iSCSI イニシエータはセッションを終了します。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
No-Op 間隔	iSCSI イニシエータから iSCSI ターゲットに送信される NOP-Out 要求の間隔を秒単位で指定します。NOP-Out 要求は、iSCSI イニシエータと iSCSI ターゲット間の接続が有効かどうかを確認するための ping メカニズムとして機能します。	ソフトウェア iSCSI 依存型ハードウェア iSCSI
No-Op タイムアウト	ホストが NOP-In メッセージを受け取るまでの時間を秒単位で指定します。メッセージは NOP-Out 要求に対応して iSCSI ターゲットから送信されます。No-Op タイムアウトの制限を超えると、イニシエータは現在のセッションを終了して、新しいセッションを開始します。	ソフトウェア iSCSI 依存型ハードウェア iSCSI



表 10-5. iSCSI イニシエータの追加パラメータ（続き）

詳細パラメータ	説明	構成可能な対象
ARP リダイレクト	ストレージシステムで、ポート間で iSCSI トラフィックを動的に移動できるようにします。アレイ ベースのフェイルオーバーを実行するストレージ システムでは ARP が必要です。	ソフトウェア iSCSI 依存型ハードウェア iSCSI 独立型ハードウェア iSCSI
遅延 ACK	システムで、受信データ パケットの ACK を遅延させることができますようにします。	ソフトウェア iSCSI 依存型ハードウェア iSCSI

## iSCSI の詳細パラメータの構成

iSCSI の詳細設定では、ヘッダ ダイジェスト、データ ダイジェスト、ARP リダイレクト、遅延 ACK などのパラメータを制御します。

**注意：** VMware サポート チームと作業をしているか、iSCSI の詳細設定に指定する値についての十分な情報がある場合を除き、この詳細設定を変更しないでください。

### 前提条件

必要な権限：ホスト.構成.ストレージ パーティション構成

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ アダプタ] をクリックし、設定するアダプタ (vmhba#) を選択します。
- 4 詳細パラメータを構成します。
  - アダプタ レベルで詳細パラメータを構成するには、[アダプタの詳細] の [詳細オプション] タブで [編集] をクリックします。
  - ターゲット レベルで詳細パラメータを構成します。
    - a [ターゲット] タブで、[動的検出] または [静的検出] のいずれかをクリックします。
    - b 使用可能なターゲットのリストから、構成するターゲットを選択し、[詳細オプション] をクリックします。
- 5 変更する詳細パラメータに必要な値を入力します。

## iSCSI セッションの管理

iSCSI イニシエータとターゲットは、相互に通信するために iSCSI セッションを確立します。iSCSI セッションは、vSphere CLI を使用して確認および管理できます。

ソフトウェア iSCSI および依存型ハードウェア iSCSI イニシエータは、各イニシエータ ポートと各ターゲット ポートの間に iSCSI セッションをデフォルトで 1 つ開始します。iSCSI イニシエータまたはターゲットに複数のポートがある場合は、ホストで複数のセッションを確立できます。各ターゲットのデフォルトのセッション数は、iSCSI アダプタのポート数にターゲットのポート数をかけた数値になります。

vSphere CLI を使用すると、現在のセッションをすべて表示し、分析およびデバッグできます。ストレージ システムへのパスを追加で作成するには、iSCSI アダプタとターゲット ポートの間の既存のセッションを複製することで、デフォルトのセッション数を増加できます。特定のターゲット ポートへのセッションを確立することもできます。

この方法は、単一ポートのストレージ システムにホストを接続する場合に役立ちます。この方法は、単一ポートのストレージ システムにホストを接続する場合に役立ちます。単一ポートのストレージ システムは、デフォルトではイニシエータにターゲット ポートを 1 つのみ表示しますが、別のターゲット ポートに追加のセッションをリダイレクトできます。iSCSI イニシエータと別のターゲット ポートの間に新しいセッションを確立すると、ストレージ システムへの追加パスが作成されます。

次の考慮事項が iSCSI セッション管理に適用されます。

- 一部のストレージ システムは、同じイニシエータ名またはエンドポイントからの複数のセッションをサポートしていません。このようなターゲットへのセッションを複数作成しようとすると、iSCSI 環境で予期しない動作が発生する可能性があります。
- ストレージ ベンダーは自動的なセッション マネージャを提供できます。自動的なセッション マネージャを使用してセッションを追加または削除することが持続的な結果を保証しないため、ストレージのパフォーマンスを妨害する可能性があります。

## iSCSI セッションの確認

vCLI コマンドを使用して、iSCSI アダプタとストレージ システム間の iSCSI セッションを表示します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

- ◆ iSCSI セッションをリスト表示するには、次のコマンドを実行します。

```
esxcli --server=server_name iscsi session list
```

このコマンドには次のオプションがあります。

オプション	説明
<b>-A --adapter=</b> <i>str</i>	たとえば、iSCSI アダプタ名は <code>vmhba34</code> です。
<b>-s --isid=</b> <i>str</i>	iSCSI セッションの識別子。
<b>-n --name=</b> <i>str</i>	iSCSI ターゲット名、たとえば、 <code>iqn.X</code> 。

## iSCSI セッションの追加

vCLI を使用して、指定するターゲットについて iSCSI セッションを追加する、または既存のセッションを複製します。セッションを複製すると、デフォルトのセッション数が増え、ストレージ システムへの追加パスが作成されます。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

- ◆ iSCSI セッションを追加または複製するには、次のコマンドを実行します。

```
esxcli --server=server_name iscsi session add
```

このコマンドには次のオプションがあります。

オプション	説明
<b>-A --adapter=</b> <i>str</i>	たとえば、iSCSI アダプタ名は <code>vmhba34</code> です。このオプションが必要とされます。
<b>-s --isid=</b> <i>str</i>	複製するセッションの ISID。すべてのセッションを一覧表示することで確認できます。
<b>-n --name=</b> <i>str</i>	iSCSI ターゲット名、たとえば、 <code>iqn.X</code> 。

### 次のステップ

iSCSI アダプタを再スキャンします。

## iSCSI セッションの削除

vCLI コマンドを使用して、iSCSI アダプタとターゲット間の iSCSI セッションを削除します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

## 手順

- ◆ セッションを削除するには、次のコマンドを実行します。

```
esxcli --server=server_name iscsi session remove
```

このコマンドには次のオプションがあります。

オプション	説明
<b>-A --adapter=</b> <i>str</i>	たとえば、iSCSI アダプタ名は vmhba34 です。このオプションが必要とされます。
<b>-s --isid=</b> <i>str</i>	削除するセッションの ISID。すべてのセッションを一覧表示することで確認できます。
<b>-n --name=</b> <i>str</i>	iSCSI ターゲット名、たとえば、iqn.X。

## 次のステップ

iSCSI アダプタを再スキャンします。

# iSCSI SAN からの起動

# 11

SAN から起動するようにホストを設定すると、ホストの起動イメージが SAN ストレージ システム内の 1 つ以上の LUN に格納されます。ホストが起動するとき、ローカル ディスクではなく、SAN の LUN から起動します。

SAN からの起動は、ローカル ストレージのメンテナンスを行いたくない場合や、ブレード システムのようなディスクレス ハードウェア構成の場合に使用できます。

ESXi はさまざまな方法の iSCSI SAN からの起動がサポートされています。

表 11-1. iSCSI SAN からの起動のサポート

独立型ハードウェア iSCSI	ソフトウェア iSCSI および依存型のハードウェア iSCSI
SAN から起動するよう iSCSI HBA を構成します。HBA の構成の詳細については、 <a href="#">SAN 起動のための独立型ハードウェア iSCSI アダプタの構成</a> を参照してください。	iBFT をサポートしているネットワーク アダプタを使用します。詳細については、 <a href="#">iBFT iSCSI 起動の概要</a> を参照してください。

この章には、次のトピックが含まれています。

- [iSCSI SAN からの起動に関する一般的推奨事項](#)
- [iSCSI SAN の準備](#)
- [SAN 起動のための独立型ハードウェア iSCSI アダプタの構成](#)
- [iBFT iSCSI 起動の概要](#)

## iSCSI SAN からの起動に関する一般的推奨事項

ホストの起動デバイスとして iSCSI LUN を設定し、使用する場合は、一般的なガイドラインに従う必要があります。

次のガイドラインは、独立型ハードウェア iSCSI および iBFT からの起動に適用されます。

- 起動構成で使用するハードウェアに関するベンダーの推奨事項を確認してください。
- インストールの前提条件と要件については、『vSphere Installation and Setup』を参照してください。
- DHCP の競合を避けるためには、固定 IP アドレスを使用します。
- VMFS データストアとブート パーティションに、異なる LUN を使用します。

- ストレージ システムで適切な ACL を構成します。
  - 起動 LUN は、その LUN を使用するホストからのみ認識できるようにします。その SAN のほかのホストからその起動 LUN を参照できないようにしてください。
  - VMFS データストアに LUN を使用した場合、LUN を複数のホストで共有できます。ストレージ システムの ACL はこれを可能にします。
- 診断パーティションを構成します。
  - 独立型のハードウェア iSCSI のみを使用している場合は、診断パーティションを起動 LUN に配置できます。診断パーティションを起動 LUN に構成する場合、この LUN は複数のホストで共有できません。診断パーティションで単独の LUN を使用する場合は、その LUN を複数のホストで共有できます。
  - iBFT を使用して SAN から起動する場合は、SAN LUN 上に診断パーティションを設定できません。ホストの診断情報を収集するには、リモート サーバ上で vSphere の ESXi ダンプ コレクタを使用します。ESXi ダンプ コレクタの詳細については、『vSphere のインストールとセットアップ』および『vSphere ネットワーク』を参照してください。

## iSCSI SAN の準備

iSCSI LUN から起動するようにホストを構成する前に、ストレージ エリア ネットワークの準備と構成を行います。

---

**注意：** SAN から起動する場合、ESXi をインストールするためにスクリプトによるインストールを使用するときは、誤ってデータが失われないように、特別な手順を実行する必要があります。

---

### 手順

- 1 ネットワーク ケーブルを接続します。現在の環境に該当する配線ガイドを参照してください。
- 2 ストレージ システムとサーバ間の IP 接続を確認します。

これには、ストレージ ネットワークのあらゆるルータまたはスイッチが適切に構成されていることも含まれます。ストレージ システムでは、ホストの iSCSI アダプタに ping が通っている必要があります。

- 3 ストレージ システムを構成します。

- a ストレージ システムでホストの起動元となるボリューム（または LUN）を作成します。
- b ストレージ システムを構成して、ホストが、割り当てた LUN にアクセスできるようにします。

これには、ホストで使用する、IP アドレスによる ACL、iSCSI 名、および CHAP 認証パラメータのアップデートが含まれることがあります。一部のストレージ システムでは、ESXi ホストにアクセス情報を指定するだけでなく、割り当てた LUN をそのホストに明示的に関連付ける必要もあります。

- c LUN がホストで正しく認識されていることを確認します。
- d ほかのシステムが構成済みの LUN にアクセスしないことを確認します。
- e ホストに割り当てられたターゲットの iSCSI 名と IP アドレスを記録します。

この情報は iSCSI アダプタの構成時に必要です。

## SAN 起動のための独立型ハードウェア iSCSI アダプタの構成

ESXi ホストが QLogic HBA などの独立型ハードウェア iSCSI アダプタを使用する場合には、SAN から起動するようにアダプタを構成する必要があります。

この手順では、QLogic iSCSI HBA が SAN から起動できるように構成する方法を説明します。QLogic アダプタ構成設定の詳細および最新の情報については、QLogic の Web サイトを参照してください。

### 前提条件

最初に VMware インストール メディアから起動する必要があるため、CD/DVD-ROM から起動するようにホストを設定します。そのためには、システム BIOS セットアップのシステム起動シーケンスを変更します。

### 手順

- 1 インストール CD/DVD を CD/DVD-ROM ドライブに挿入し、ホストを再起動します。
- 2 BIOS を使用して、最初に CD/DVD-ROM ドライブから起動するようにホストを設定します。
- 3 サーバが POST で送信中に [Ctrl] + [q] を押し、QLogic iSCSI HBA 構成メニューに入ります。
- 4 構成する I/O ポートを選択します。  
デフォルトで、アダプタの起動モードは無効に設定されます。
- 5 HBA を構成します。
  - a [Fast!UTIL オプション] メニューから、[構成設定] - [ホスト アダプタの設定] を選択します。
  - b ホスト アダプタのイニシエータ IP アドレス、サブネット マスク、ゲートウェイ、イニシエータ iSCSI 名、および CHAP（必要に応じて）の設定を構成します。
- 6 iSCSI 設定を構成します。  
[iSCSI 起動設定の構成](#) を参照してください。
- 7 変更内容を保存し、システムを再起動します。

## iSCSI 起動設定の構成

iSCSI から起動するように ESXi ホストを設定するときには、iSCSI 起動の設定を構成する必要があります。

### 手順

- 1 [Fast!UTIL オプション] メニューから、[構成設定] - [iSCSI 起動設定] を選択します。
- 2 SendTargets を設定する前に、アダプタの起動モードを [手動] に設定します。

- 3 [プライマリ起動デバイス設定] を選択します。
  - a 検出する [ターゲット IP] および [ターゲット ポート] を入力します。
  - b 指定したアドレスに、起動元となる iSCSI ターゲットと LUN がそれぞれ 1 つのみ存在する場合、[起動 LUN] および [iSCSI 名] フィールドは空のままにできます。そのほかの場合、ほかのシステムのポリシーから起動しないように、これらのフィールドを指定する必要があります。これらのフィールドは、ターゲット ストレージ システムまで到達して再スキャンしたあとに使用できるようになります。
  - c 変更内容を保存します。
- 4 [iSCSI 起動設定] メニューからプライマリ起動デバイスを選択します。新しいターゲット LUN を検出するために、HBA の自動再スキャンが実行されます。
- 5 iSCSI ターゲットを選択します。

---

**注：** 複数の LUN がターゲット内にある場合は、iSCSI デバイスを見つけてから、[Enter] を押すと、特定の LUN ID を選択できます。

---

- 6 [プライマリ起動デバイス設定] メニューに戻ります。再スキャン後、[起動 LUN] および [iSCSI 名] フィールドが使用できます。[起動 LUN] の値を目的の LUN ID に変更します。

## iBFT iSCSI 起動の概要

ESXi ホストは、ソフトウェア iSCSI アダプタまたは依存型ハードウェア iSCSI アダプタとネットワーク アダプタを使用して、iSCSI SAN から起動できます。

ESXi をデプロイし、iSCSI SAN から起動するには、iBFT (iSCSI Boot Firmware Table) 形式をサポートしている、iSCSI 起動対応のネットワーク アダプタがホストに必要です。iBFT は、iSCSI 起動デバイスに関するパラメータをオペレーティング システムに伝える方法です。

ESXi をインストールし、iSCSI SAN から起動する前に、ネットワーク アダプタでネットワークと iSCSI 起動パラメータを構成し、アダプタで iSCSI 起動を有効にします。ネットワーク アダプタの構成はベンダーによって異なるので、構成方法についてはベンダーのドキュメントを参照してください。

iSCSI からはじめて起動するとき、システム上の iSCSI 起動ファームウェアが iSCSI ターゲットに接続します。ログインに成功すると、ファームウェアはネットワークと iSCSI 起動のパラメータを iBFT に保存し、システムのメモリにそのテーブルを格納します。システムはこのテーブルを使用して、その iSCSI 接続とネットワークの構成、および起動を行います。

次のリストに、iBFT iSCSI 起動手順を示します。

- 1 再起動時に、システム BIOS がネットワーク アダプタで iSCSI 起動ファームウェアを検出します。
- 2 iSCSI 起動ファームウェアが、事前構成済みの起動パラメータを使用して、指定された iSCSI ターゲットに接続します。
- 3 iSCSI ターゲットへの接続に成功したら、iSCSI 起動ファームウェアがネットワークと iSCSI 起動パラメータを iBFT に書き込み、そのテーブルをシステム メモリに格納します。

---

**注：** システムはこのテーブルを使用して、その iSCSI 接続とネットワークの構成、および起動を行います。

---



- 4 BIOS が起動デバイスを起動します。
- 5 VMkernel がロードを開始し、起動処理を引き継ぎます。
- 6 iBFT の起動パラメータを使用して、VMkernel は iSCSI ターゲットに接続します。
- 7 iSCSI 接続が確立されたら、システムが起動します。

## iBFT iSCSI 起動に関する検討事項

iBFT 対応のネットワーク アダプタを使用して iSCSI から ESXi ホストを起動するときは、一定の考慮事項が適用されます。

- VMware ESXi をインストールし、起動する前に、ベンダーが提供するツールを使用して NIC の起動コードと iBFT ファームウェアを更新します。VMware ESXi iBFT 起動でサポートされている起動コードと iBFT ファームウェアのバージョンについては、ベンダーのドキュメントと VMware の HCL を参照してください。
- iBFT iSCSI 起動では、iBFT 対応ネットワーク アダプタのフェイルオーバーはサポートされていません。
- iBFT iSCSI から起動するようにホストを設定したら、次の制限事項が適用されます。
  - ソフトウェア iSCSI アダプタを無効にできません。iBFT 構成が BIOS 内にある場合、ホストは再起動のたびにソフトウェア iSCSI アダプタを再度有効にします。

---

**注：** iSCSI 起動に iBFT 対応のネットワーク アダプタを使用せず、ソフトウェア iSCSI アダプタを常に有効にしたい場合には、ネットワーク アダプタから iBFT 構成を削除します。

---

- vSphere Web Client を使用して iBFT iSCSI 起動ターゲットを削除することはできません。ターゲットはアダプタの静的ターゲットのリストに表示されます。

## SAN からの iBFT 起動の構成

ソフトウェア iSCSI アダプタ、または依存型のハードウェア iSCSI アダプタおよびネットワーク アダプタを使用して iSCSI SAN から起動できます。ネットワーク アダプタは iBFT をサポートしている必要があります。

ホストを iBFT から起動するように設定する場合は、いくつかの作業を行います。

### 手順

#### 1 iSCSI 起動パラメータの構成

iSCSI 起動プロセスを開始するには、ホスト上のネットワーク アダプタに、特別に構成された iSCSI 起動ファームウェアが必要です。ファームウェアを構成するとき、ネットワークと iSCSI のパラメータを指定し、アダプタで iSCSI 起動を有効にします。

#### 2 BIOS での起動シーケンスの変更

iBFT iSCSI から起動するようにホストを設定する場合は、ホストが適切な順序で起動するように起動シーケンスを変更します。

#### 3 iSCSI ターゲットへの ESXi のインストール

iBFT iSCSI から起動するようにホストを設定するとき、ESXi イメージをターゲット LUN にインストールします。

## 4 iSCSI ターゲットからの ESXi の起動

iBFT iSCSI 起動のためにホストを準備し、ESXi イメージを iSCSI ターゲットにコピーしたら、実際の起動を実行します。

### iSCSI 起動パラメータの構成

iSCSI 起動プロセスを開始するには、ホスト上のネットワーク アダプタに、特別に構成された iSCSI 起動ファームウェアが必要です。ファームウェアを構成するとき、ネットワークと iSCSI のパラメータを指定し、アダプタで iSCSI 起動を有効にします。

ネットワーク アダプタの構成には、動的構成と静的構成があります。動的構成を使用した場合、すべてのターゲットとイニシエータの起動パラメータが、DHCP を使用して取得されます。静的構成の場合、ホストの IP アドレスとイニシエータの IQN、およびターゲット パラメータなどのデータを手動で入力します。

#### 手順

- ◆ iSCSI からの起動に使用するネットワーク アダプタで、ネットワークと iSCSI パラメータを指定します。

ネットワーク アダプタの構成はベンダーによって異なるので、構成方法についてはベンダーのドキュメントを参照してください。

### BIOS での起動シーケンスの変更

iBFT iSCSI から起動するようにホストを設定する場合は、ホストが適切な順序で起動するように起動シーケンスを変更します。

BIOS 起動シーケンスを次のように変更します。

- iSCSI
- DVD-ROM

BIOS で起動シーケンスを変更する方法はベンダーによって異なるので、変更手順については、ベンダーのドキュメントを参照してください。次の手順の例では、Broadcom のネットワーク アダプタを備えた Dell のホストで起動シーケンスを変更する方法を示します。

#### 手順

- 1 ホストを起動します。
- 2 POST (Power-On Self-Test) 中に [F2] を押して BIOS セットアップを開始します。
- 3 BIOS セットアップで [Boot Sequence] を選択し、[Enter] を押します。
- 4 Boot Sequence メニューで、iSCSI が DVD-ROM の前になるように起動可能な項目の順序を変更します。
- 5 [Esc] を押して Boot Sequence メニューを終了します。
- 6 [Esc] を押して BIOS セットアップを終了します。
- 7 [Save Changes] を選択し、[Exit] をクリックして BIOS セットアップのメニューを終了します。

### iSCSI ターゲットへの ESXi のインストール

iBFT iSCSI から起動するようにホストを設定するとき、ESXi イメージをターゲット LUN にインストールします。

**前提条件**

- 起動 NIC で、iSCSI 起動ファームウェアが、起動 LUN として使用するターゲット LUN を参照するように設定します。
- iSCSI が DVD-ROM より優先されるように BIOS で起動シーケンスを変更します。
- Broadcom 社のアダプタを使用している場合は、[iSCSI ターゲットから起動] を [無効] に設定します。

**手順**

- 1 インストール メディアを CD/DVD-ROM ドライブに挿入し、ホストを再起動します。
- 2 インストーラが開始したら、標準のインストール手順に従います。
- 3 プロンプトが表示されたら、インストール ターゲットとして iSCSI LUN を選択します。  
インストーラが、ESXi 起動イメージを iSCSI LUN にコピーします。
- 4 システムが再起動したら、インストール DVD を取り出します。

**iSCSI ターゲットからの ESXi の起動**

iBFT iSCSI 起動のためにホストを準備し、ESXi イメージを iSCSI ターゲットにコピーしたら、実際の起動を実行します。

**前提条件**

- 起動 NIC で、起動 LUN を参照するように iSCSI 起動ファームウェアを構成します。
- iSCSI が起動デバイスより優先されるように BIOS で起動シーケンスを変更します。
- Broadcom 社のアダプタを使用している場合は、[iSCSI ターゲットから起動] を [有効] に設定します。

**手順**

- 1 ホストを再起動します。  
ホストは、iBFT データを使用して iSCSI LUN から起動します。最初の起動時に、iSCSI 初期化スクリプトによってデフォルトのネットワークが設定されます。ネットワークの設定は、再起動しても保持されます。
- 2 (オプション) vSphere Web Client を使用してネットワーク構成を調整します。

**ネットワークのベスト プラクティス**

iBFT を使用して iSCSI から ESXi ホストを起動するには、適切にネットワークを構成する必要があります。

安全性を高め、かつパフォーマンスを改善するために、ホストに冗長ネットワーク アダプタを持つようにします。

すべてのネットワーク アダプタをどのように設定するかは、その環境で、iSCSI トラフィックおよびホスト管理トラフィック用に共有ネットワークを使用しているか分離されたネットワークを使用しているかによって異なります。

**iSCSI ネットワークと管理ネットワークが共有されたネットワーク**

ホストのプライマリ ネットワーク アダプタでネットワークおよび iSCSI パラメータを構成します。ホストを起動したあと、デフォルトのポート グループにセカンダリ ネットワーク アダプタを追加できます。

## iSCSI ネットワークと管理ネットワークが分離されたネットワーク

iSCSI ネットワークと管理ネットワークが分離して構成する場合、バンド幅の問題を避けるために次のガイドラインに従ってください。

- 分離されたネットワークはそれぞれ異なるサブネット上にある必要があります。
- ネットワークの分離に VLAN を使用している場合は、ルーティング テーブルが適切に設定されるように、それぞれのネットワークが異なるサブネットを持つ必要があります。
- iSCSI アダプタとターゲットを同じサブネット上に構成することを推奨します。iSCSI アダプタとターゲットを異なるサブネット上に設定すると、次のような制限が適用されます。
  - デフォルトの VMkernel ゲートウェイは、管理および iSCSI の両方のトラフィックの経路選択が可能でなければならない。
  - ホストの起動後、iBFT が有効なネットワーク アダプタは iBFT 用にのみ使用可能。その他の iSCSI トラフィックにはそのアダプタは使用できません。
- 管理ネットワークには、プライマリ物理ネットワーク アダプタを使用してください。
- iSCSI ネットワークに 2 番目の物理ネットワーク アダプタを使用します。必ず iBFT を構成します。
- ホストの起動後に、管理ネットワークと iSCSI ネットワークの両方にセカンダリ ネットワーク アダプタを追加できます。

## iBFT iSCSI 起動設定の変更

iSCSI ストレージやホストで IQN 名、IP アドレスなどの設定を変更する場合は、iBFT を更新します。この作業では、起動 LUN と、LUN に格納されているデータをそのまま残すことを想定しています。

### 手順

- 1 ESXi ホストをシャットダウンします。
  - 2 iSCSI ストレージ設定を変更します。
  - 3 ホストにある iBFT を新しい設定で更新します。
  - 4 ホストを再起動します。
- ホストは、iBFT に格納されている新しい情報を使用して起動します。

## iBFT iSCSI 起動のトラブルシューティング

このセクションのトピックは、iBFT iSCSI 起動の使用時に発生する可能性がある問題の特定と解決に役立ちます。

### システム ゲートウェイの消失によるネットワーク接続の切断

iBFT ネットワーク アダプタに関連付けられているポート グループを削除すると、ネットワーク接続が切断されます。

### 問題

ポート グループを削除したあとに、ネットワーク接続が切断されます。

## 原因

ESXi のインストール時に iBFT 対応のネットワーク アダプタでゲートウェイを指定すると、このゲートウェイがシステムのデフォルト ゲートウェイになります。ネットワーク アダプタに関連付けられているポート グループを削除すると、システムのデフォルト ゲートウェイが失われます。この操作でネットワーク接続が切断されます。

## 解決方法

必要な場合を除いて、iBFT ゲートウェイを設定しないでください。ゲートウェイが必要な場合は、インストール後に、管理ネットワークが使用しているゲートウェイをシステムのデフォルト ゲートウェイとして手動で設定します。

## iSCSI 起動パラメータの変更によって発生する ESXi のステートレス モードでの起動

最初の起動後にネットワーク アダプタで iSCSI 起動パラメータを変更しても、ESXi ホストの iSCSI とネットワークの構成は更新されません。

## 問題

iSCSI から最初に ESXi を起動したあとに、ネットワーク アダプタで iSCSI 起動パラメータを変更した場合、ホストはステートレス モードで起動します。

## 原因

ファームウェアは、更新された起動構成を使用し、iSCSI ターゲットに接続して ESXi イメージをロードできます。ただし、ロード時にシステムは新しいパラメータは取得せずに、前回起動したときのネットワークと iSCSI のパラメータを引き続き使用します。その結果、ホストはターゲットに接続できず、ステートレス モードで起動します。

## 解決方法

- 1 vSphere Web Client を使用して ESXi ホストに接続します。
- 2 iBFT のパラメータに合わせて、ホストで iSCSI とネットワークを再構成します。
- 3 再スキャンを実行します。

# iSCSI ストレージのベスト プラクティス

# 12

ESXi を iSCSI SAN と使用する場合には、問題を回避するために VMware が提供するベスト プラクティスに従ってください。

ストレージ システムが Storage API - Array Integration ハードウェア アクセラレーション機能をサポートしているかどうかを、ストレージの担当者にご確認ください。サポートしている場合には、ハードウェア アクセラレーションのサポートをストレージ システム側で有効にする方法はベンダーのドキュメントを参照してください。詳細については、[23 章 ストレージのハードウェア アクセラレーション](#) を参照してください。

この章には、次のトピックが含まれています。

- [iSCSI SAN の問題の防止](#)
- [iSCSI SAN ストレージ パフォーマンスの最適化](#)
- [イーサネット スイッチ統計情報の確認](#)

## iSCSI SAN の問題の防止

ESXi を SAN と併用する場合、SAN の問題を回避するために特別なガイドラインに従う必要があります。

SAN 構成に関する問題を回避するためのいくつかのヒントを示します。

- 各 LUN には、VMFS データストアを 1 つだけ配置します。1 つの LUN に複数の VMFS データストアを配置することはお勧めしません。
- バス ポリシーの変更について熟知していない場合は、システムで設定されているバス ポリシーをそのまま使用します。
- すべてを文書化します。これには、構成、アクセス コントロール、ストレージ、スイッチ、サーバと iSCSI HBA の構成、ソフトウェアとファームウェアのバージョン、およびストレージ ケーブル計画に関する情報が含まれます。
- 障害に対する計画を立てます。
  - トポロジ マップの複製をいくつか作成します。エレメントごとに、エレメントに障害が発生した場合の SAN への影響を検討します。
  - 設計上の重大な障害を見落とさないように、さまざまなリンク、スイッチ、HBA、およびその他のエレメントを削除します。
- iSCSI HBA が、スロットとバス速度を基準として、ESXi ホストの正しいスロットにインストールされていることを確認します。サーバで使用できるバス間で、PCI バスの負荷を分散します。

- ESXi パフォーマンス チャート、イーサネット スイッチ統計情報、ストレージ パフォーマンス統計情報など、すべての参照できるポイントで、ストレージ ネットワークのさまざまな監視ポイントに関する情報を得ます。
- ホストで使用されている VMFS データストアを持つ LUN の ID の変更時には、注意が必要です。ID を変更すると、VMFS データストアで実行中の仮想マシンが停止します。

VMFS データストア上で実行中の仮想マシンがない場合、LUN の ID を変更したあとで、再スキャンを実行してホストの ID をリセットする必要があります。再スキャンについては、[ストレージの更新操作および再スキャン操作](#) を参照してください。

- iSCSI アダプタのデフォルトの iSCSI 名を変更する必要がある場合には、入力する名前が世界中で一意であり、適切にフォーマットされていることを確認します。ストレージ アクセスの問題を回避するには、異なるホスト上でも、同じ iSCSI 名を異なるアダプタに決して割り当てないでください。

## iSCSI SAN ストレージ パフォーマンスの最適化

一般的な SAN 環境の最適化には、いくつかの要因があります。

ネットワーク環境が適切に構成されている場合、iSCSI コンポーネントは優れたスループットを発揮し、iSCSI イニシエータおよびターゲットの待ち時間は十分短くなります。ネットワーク輻輳が発生し、リンク、スイッチ、またはルータが飽和した場合、iSCSI のパフォーマンスが低下し、ESXi 環境に適さなくなることもあります。

### ストレージ システムのパフォーマンス

ストレージ システムのパフォーマンスは、iSCSI 環境全体のパフォーマンスに影響する主要な要因の 1 つです。

ストレージ システムのパフォーマンスに問題が発生した場合、これに関連する情報はストレージ システム ベンダーが提供するドキュメントを参照してください。

LUN を割り当てるときは、複数のホストから各共有 LUN にアクセスでき、各ホストで複数の仮想マシンを実行できる点に注意してください。ESXi ホストで使用される 1 つの LUN が、異なるオペレーティング システムで実行される多様なアプリケーションからの I/O を提供する可能性があります。このような場合はさまざまなワークロードが発生するため、ESXi を I/O の頻繁なアプリケーションに使用していない別のホストの LUN を、ESXi LUN のある RAID グループに含めないでください。

読み取りキャッシュおよび書き込みキャッシュを有効にします。

ロード バランシングは、サーバの I/O 要求を使用可能なすべての SP およびそれに関連付けられているホスト サーババスに分散するプロセスです。目的は、スループットの観点からパフォーマンスを最適化することにあります（1 秒あたりの I/O 数、1 秒あたりのメガバイト数、またはレスポンス タイム）。

SAN ストレージ システムには、I/O がすべてのストレージ システム バスの間でバランスがとられるように、継続的な再設計と調整が必要です。この要件を満たすために、すべての SP 間で LUN へのバスを分散し、最適なロード バランシングを提供します。詳細な監視によって、手動で LUN の分散を再調整する必要がある時期が示されます。

静的にバランスがとられたストレージ システムの調整は、特定のパフォーマンス統計情報（1 秒あたりの I/O 処理数、1 秒あたりのブロック数、応答時間など）を監視し、LUN のワークロードをすべての SP に分散して行います。

### iSCSI でのサーバ パフォーマンス

サーバ パフォーマンスを最適にするために考慮しなければならない点がいくつかあります。

各サーバ アプリケーションは、次の条件を満たしながら、目的のストレージにアクセスできる必要があります。

- 高い I/O レート (1 秒あたりの I/O 処理数)
- 高いスループット (1 秒あたりのメガバイト数)
- 最小限の待ち時間 (応答時間)

アプリケーションごとに要件が異なるため、ストレージ システムの適切な RAID グループを選択することで、これらの目的を達成できます。パフォーマンスの目標を達成するには、次のタスクを実行します。

- 各 LUN を、必要なパフォーマンス レベルを提供する RAID グループに配置する。割り当てられた RAID グループにあるほかの LUN のアクティビティおよびリソース使用率に注意してください。I/O を行うアプリケーションが多すぎる高性能 RAID グループは、ESXi ホストで実行されるアプリケーションで要求されるパフォーマンス目標を達成できないことがあります。
- 各サーバに十分な数のネットワーク アダプタまたは iSCSI ハードウェア アダプタを装備し、サーバがホスティングするすべてのアプリケーションでピーク時に最大のスループットが得られるようにする。I/O を複数のポートに分散させることで、各アプリケーションでスループットが高くなり、待ち時間が短くなります。
- ソフトウェア iSCSI の冗長性を確保するために、iSCSI 接続に利用するすべてのネットワーク アダプタにイーサネットが接続されていることを確認する。
- ESXi システムに LUN または RAID グループを割り当てるときは、複数のオペレーティング システムがそのリソースを使用および共有する。結果として、ESXi システムを使用する場合にストレージ サブシステムの各 LUN で要求されるパフォーマンスは、物理マシンを使用する場合よりも高くなることがあります。たとえば、I/O の多いアプリケーションを 4 つ実行しようとする場合は、ESXi LUN に 4 倍のパフォーマンス キャパシティを割り当てます。
- 複数の ESXi システムを vCenter Server と組み合わせて使用する場合は、それに対応して、ストレージ サブシステムのパフォーマンスを高くする。
- ESXi システムで実行されるアプリケーションが要求する未実行 I/O 数を、SAN で処理できる I/O 数と一致させる。

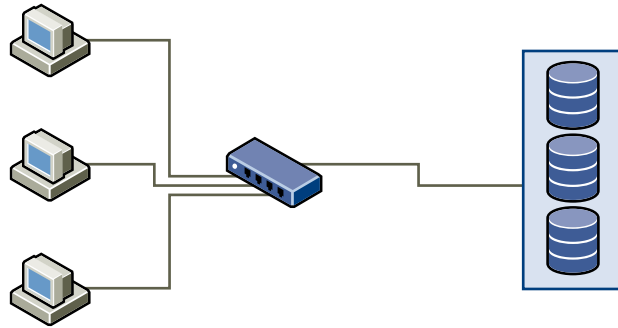
## ネットワーク パフォーマンス

一般的な SAN は、スイッチのネットワークを通じてストレージ システムの集合体に接続されたコンピュータの集合体で構成されています。複数のコンピュータが同じストレージにアクセスすることは頻繁にあります。

ストレージへの単一のイーサネット リンクはイーサネット スイッチを介してストレージ システムに接続された複数のコンピュータ システムを示します。この構成では、各システムはそれぞれ 1 つのイーサネット リンクを経由してスイッチに接続されており、スイッチからまた 1 つのイーサネット リンクを経由してストレージ システムに接続されています。ほとんどの構成 (比較的新しいスイッチと標準トラフィックを備えている) では、これで問題はありません。



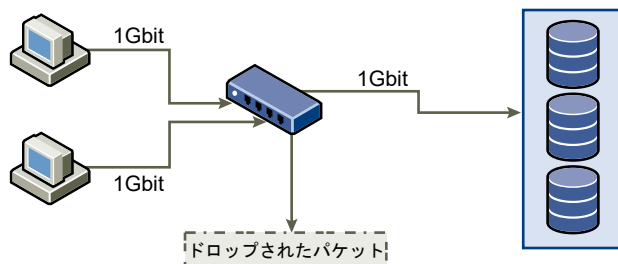
図 12-1. ストレージへの単一のイーサネット リンク



システムがストレージからデータを読み取る場合、ストレージから得られる最大のレスポンスは、ストレージ システムとイーサネット スイッチとの間のリンクで送信できるデータ量です。1つのシステムまたは仮想マシンがネットワーク スピードを占有してしまう可能性は少ないですが、複数のシステムが1つのストレージ デバイスを共用する場合には起こる可能性のある状況です。

ストレージにデータを書き込むとき、複数のシステムまたは仮想マシンがリンクを利用しようとすることがあります。これが発生すると、ドロップされたパケットに示すとおり、システムとストレージ システムとの間のスイッチでデータをドロップせざるを得なくなります。このようなことが発生するのは、ストレージ デバイスへの接続が1つしかないにもかかわらず、ストレージ システムへ送信するトラフィックが1つのリンクが送信できる容量を超えているためです。この場合、送信可能なデータ量はスイッチとストレージ システムとの間のリンク速度に制限されるので、スイッチがネットワーク パケットをドロップします。

図 12-2. ドロップされたパケット



ドロップされたネットワーク パケットをリカバリさせると、パフォーマンスが著しく低下します。データがドロップされたと判別する時間に加え、再送信するときに、次の処理に使えたはずのネットワークのバンド幅を消費します。

iSCSI のトラフィックは、ネットワーク上を TCP (Transmission Control Protocol) で送信されます。TCP は信頼性の高い伝送プロトコルで、ドロップされたパケットを再送信し、確実に最終目的地まで届けます。TCP はドロップされたパケットを回復し、すばやくシームレスに再送信するよう設計されています。ただし、スイッチがパケットを頻繁に廃棄してしまう場合、ネットワークのスループットは著しく低下します。ネットワークはデータ再送信リクエストや再送パケットなどで輻輳し、実際にネットワーク上を円滑に転送されるデータは少なくなります。

ほとんどのイーサネット スイッチはデータのバッファ (つまり一時保存) が可能なため、データを目的地に送信する機会は各デバイスに均等に与えられます。その代わり、この転送データを一部バッファできるという点と、多くのシステムでコマンド残数を制限しているという点で、複数のシステムからストレージ システムに小規模なデータが一斉に送信される可能性があります。

処理が膨大で、かつ複数のサーバが1つのスイッチ ポートからデータを送信しようとする、1つのリクエストをバッファしつつ別のリクエストを転送するスイッチの容量を超えてしまう場合があります。この場合、スイッチは送信できないデータをドロップし、ストレージ システムはドロップされたパケットの再送信を要求しなければなりません。たとえば、イーサネット スイッチは 32KB しか入力ポートにバッファできないのに、そのスイッチに接続したサーバが 256KB をストレージ デバイスに送信できると判断した場合、一部データがドロップされます。

正しく管理されているスイッチであれば、ドロップしたパケットについて次のような情報を表示します。

```
*: interface is up IHQ:pkts in input hold queue      IQD:pkts dropped from input queue
OHQ:pkts in output hold queue      OQD:pkts dropped from output queue RXBS:rx rate (bits/
sec)      RXPS:rx rate (pkts/sec) TXBS:tx rate (bits/sec)      TXPS:tx rate (pkts/
sec) TRTL:throttle count
```

表 12-1. サンプルのスイッチ情報

インターフェイス	IHQ	IQD	OHQ	OQD	RXBS	RXPS	TXBS	TXPS	TRTL
* GigabitEthernet0/1	3	9922	0	0	476303000	62273	477840000	63677	0

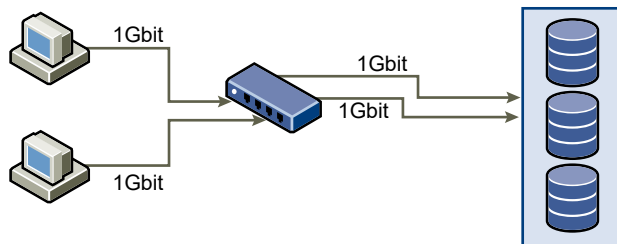
この Cisco のスイッチの例では、使用しているバンド幅が 476,303,000 ビット/秒で、ケーブル速度の半分未満です。それにもかかわらずポートは受信パケットをバッファリングし、多数のパケットをドロップしています。このインターフェイスの最終行にある概要情報を見ると、このポートではすでに約 10,000 の受信パケットがドロップされていると IQD 列からわかります。

この問題を回避するための構成変更としては、複数の入力イーサネット リンクが1つの出力リンクに集中しないようにし、結果的にリンクのオーバーサブスクリプションを防止する方法があります。最大容量に近い転送を行う多数のリンクの数を減らすと、オーバーサブスクリプションが発生する可能性があります。

一般的に言って、データの取得や処理を記録するシステムなど、大量のデータをストレージに書き込むアプリケーションやシステムでは、ストレージ デバイスのイーサネット リンクを共用しないほうがよいでしょう。このようなタイプのアプリケーションでは、ストレージ デバイスへの接続を複数にしておくことで最高のパフォーマンスを発揮します。

スイッチからストレージへの複数の接続は、スイッチからストレージへの複数接続を示します。

図 12-3. スイッチからストレージへの複数の接続



共有構成でのリンクのオーバーサブスクリプションの問題は、VLAN または VPN を使用しても解決されません。VLAN やその他のネットワーク仮想分割を利用すると、論理的なネットワーク設計は可能になりますが、スイッチ間のリンクやトランクの物理的容量が改善されるわけではありません。VPN のように、ストレージ トラフィックやその他のネットワーク トラフィックが最終的に物理接続を共用する場合、オーバーサブスクリプションおよびパケット消失が起こる可能性があります。スイッチ間のトランクを共用する VLAN にも同じことが言えます。SAN のパフォーマンス設計をする場合、ネットワークの論理的な割り当てではなく、ネットワークの物理的な制限を考慮する必要があります。

## イーサネット スイッチ統計情報の確認

多くのイーサネット スイッチには、スイッチの健全性を監視するさまざまな手段が備わっています。

稼働時間の大部分でスループットが最大限に近い状態のポートのあるスイッチでは、最大のパフォーマンスは発揮できません。最大限近くで稼働しているポートが使用中の iSCSI SAN にあれば、負荷を減らしてください。そのポートが ESXi システムや iSCSI ストレージに接続されている場合、手動ロード バランシングを利用することで負荷を軽減できます。

そのポートが複数のスイッチまたはルータ同士を接続している場合、それらのコンポーネント間にリンクを追加して処理量を増やすことも検討してください。イーサネット スイッチは通常、転送エラー、キュー状態のパケット、およびドロップされたイーサネット パケットに関する情報も通知します。iSCSI トラフィックで利用しているポートがこのような状態であるとスイッチが頻繁にレポートする場合、iSCSI SAN のパフォーマンスは低くなります。

# ストレージ デバイスの管理

# 13

ESXi ホストがアクセスするローカルおよびネットワーク上のストレージ デバイスを管理します。

この章には、次のトピックが含まれています。

- ストレージ デバイスの特徴
- ストレージ デバイスの命名について
- ストレージの更新操作および再スキャン操作
- デバイス接続問題の確認
- ストレージ デバイスのロケータ LED の有効化または無効化

## ストレージ デバイスの特徴

ローカル デバイスやネットワーク デバイスもすべて含めて、ホストで使用できるすべてのストレージ デバイスまたは LUN を表示できます。サードパーティ製のマルチパス プラグインを使用している場合は、プラグインを介して使用できるストレージ デバイスもリストに表示されます。

各ストレージ アダプタについて、このアダプタで使用できるストレージ デバイスの個別のリストを表示できます。

一般的に、ストレージ デバイスを確認する場合には、次の情報が表示されます。

表 13-1. ストレージ デバイスの情報

ストレージ デバイスの情報	説明
名前	表示名とも呼ばれます。これは ESXi ホストがストレージ タイプおよびメーカーに基づいてデバイスに割り当てた名前です。この名前は任意の名前に変更できます。
識別子	デバイスに固有な、あらゆる場所において一意の ID。
操作状態	デバイスがマウントされているか、マウントされていないかを示します。詳細については、 <a href="#">ストレージ デバイスの分離</a> を参照してください。
LUN	SCSI ターゲット内の LUN（論理ユニット番号）。LUN 番号は、ストレージ システムによって提供されます。ターゲットに 1 つの LUN しかない場合、LUN 番号は常にゼロ（0）になります。
タイプ	デバイスのタイプ（ディスク、CD-ROM など）。
ドライブの種類	デバイスがフラッシュ ドライブか、通常の HDD ドライブかに関する情報。フラッシュ ドライブの詳細については、 <a href="#">14 章 フラッシュ デバイスの操作</a> を参照してください。
転送	ホストがデバイスにアクセスするために使用する転送プロトコル。プロトコルは、使用しているストレージのタイプによって異なります。 <a href="#">物理ストレージのタイプ</a> を参照してください。

表 13-1. ストレージ デバイスの情報（続き）

ストレージ デバイスの情報	説明
容量	ストレージ デバイスの容量の合計。
所有者	NMP やサードパーティ製のプラグインなど、ホストがストレージ デバイスへのバスを管理するために使用するプラグイン。詳細については、 <a href="#">複数のバスの管理</a> を参照してください。
ハードウェア アクセラレーション	ストレージ デバイスが仮想マシン管理操作を行なってホストを支援しているかどうかに関する情報。ステータスは、「サポート」、「未サポート」、または「不明」です。詳細については、 <a href="#">23 章 ストレージのハードウェア アクセラレーション</a> を参照してください。
場所	/vmfs/devices/ ディレクトリにあるストレージ デバイスへのバス。
パーティションのフォーマット	ストレージ デバイスによって使用されるパーティションのスキーム。MBR（マスタ ブート レコード）または GPT（GUID パーティション テーブル）フォーマットにすることができます。GPT デバイスは 2TB より大きいデータストアをサポートします。詳細については、 <a href="#">VMFS データストアとストレージ ディスク フォーマット</a> を参照してください。
パーティション	プライマリおよび論理パーティション（構成されている場合は、VMFS データストアを含む）。
マルチバス ポリシー（VMFS データストア）	ホストがストレージへのバスの管理に使用しているバス選択ポリシーおよびストレージ アレイ タイプ ポリシー。詳細については、 <a href="#">17 章 マルチバスとフェイルオーバーについて</a> を参照してください。
バス（VMFS データストア）	ストレージへのアクセスに使用されているバスとそのステータス。

## ホストのストレージ デバイスの表示

ホストで使用可能なすべてのストレージ デバイスを表示します。サードパーティ製のマルチバス プラグインを使用している場合は、プラグインを介して使用できるストレージ デバイスもリストに表示されます。

[ストレージ デバイス] ビューでは、ホストのストレージ デバイスの一覧表示、それらの情報の分析、プロパティの修正を行うことができます。

### 手順

1 vSphere Web Client ナビゲータで、ホストを参照して移動します。

2 [構成] タブをクリックします。

3 [ストレージ] で、[ストレージ デバイス] をクリックします。

ホストで使用可能なすべてのストレージ デバイスが [ストレージ デバイス] に一覧表示されます。

4 特定のデバイスの詳細情報を表示するには、リストからデバイスを選択します。

5 [デバイスの詳細情報] タブを使用すると、選択したデバイスの追加情報にアクセスしたり、プロパティを修正したりできます。

タブ	説明
プロパティ	デバイスのプロパティと特性を表示します。デバイスのマルチバス ポリシーを表示、修正できます。
バス	デバイスで使用可能なバスを表示します。選択したバスを有効/無効にします。

## アダプタのストレージ デバイスの表示

ホスト上の特定のストレージ アダプタを通じてアクセスできるストレージ デバイスのリストを表示します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックします。

ホストにインストールされているすべてのストレージ アダプタが [ストレージ アダプタ] に一覧表示されます。

- 4 リストからアダプタを選択し、[デバイス] タブ をクリックします。

ホストがアダプタを通じてアクセスできるストレージ デバイスが表示されます。

## ストレージ デバイスの命名について

各ストレージ デバイスまたは LUN はいくつかの名前で識別されます。

### デバイス識別子

ストレージのタイプによって、ESXi ホストは異なるアルゴリズムと規則を使用して、ストレージ デバイスごとに識別子を生成します。

#### SCSI INQUIRY 識別子。

ホストは SCSI INQUIRY コマンドを使用して、ストレージ デバイスを照会し、結果データ (特に 83 ページの情報) を使用して、一意の識別子を生成します。83 ページに基づくデバイス識別子はすべてのホストで一貫かつ永続的で、次のいずれかのフォーマットが指定されています。

- *naa.number*
- *t10.number*
- *eui.number*

これらのフォーマットは T10 委員会の規格に従っています。T10 委員会の Web サイトで SCSI-3 のドキュメントを参照してください。

#### パス ベースの識別子。

デバイスによって 83 ページの情報が提供されない場合には、ホストで *mpx.path* 名が生成されます。*path* は、*mpx.vmhba1:C0:T1:L3* のようにデバイスへの最初のパスを表します。この識別子は、SCSI INQUIRY が識別するのと同じ方法で使用できます。

*mpx.* 識別子は、パス名が一意であることを前提として、ローカル デバイスのために作成されます。ただし、この識別子は一意でも永続的でもなく、起動した後毎回変わる可能性があります。

通常、デバイスへのパスのフォーマットは次の通りです。

*vmhbaAdapter:CChannel:TTarget:LLUN*

- *vmhbaAdapter* はストレージ アダプタの名前です。この名前は、仮想マシンで使用される SCSI コントローラではなく、ホストの物理アダプタを表します。
- *CChannel* はストレージ チャンネルの番号です。

ソフトウェア iSCSI アダプタと依存型ハードウェア アダプタは、チャンネル番号を使用して、同じターゲットへの複数のパスを表します。

- *TTarget* はターゲットの番号です。ターゲットの番号付けはホストによって決定されますが、ホストに表示されるターゲットのマッピングが変わると、番号付けも変わることがあります。複数のホストで共有しているターゲットは、同じターゲット番号を持たないことがあります。
- *LLUN* は、ターゲット内の LUN の場所を表す、LUN の番号です。LUN 番号は、ストレージ システムによって提供されます。ターゲットに 1 つの LUN しかない場合、LUN 番号は常にゼロ (0) になります。

たとえば *vmhba1:C0:T3:L1* は、ストレージ アダプタ *vmhba1* とチャンネル 0 を介してアクセスされるターゲット 3 上の LUN1 を表します。

## レガシー識別子

SCSI INQUIRY または *mpx.* 識別子に加えて、デバイスごとに、ESXi は代替のレガシー名を生成します。識別子のフォーマットは次のとおりです。

*vml.number*

レガシー識別子には、デバイスに一意の一連の数字が含まれており、使用可能な場合には 83 ページの情報からある程度派生できます。83 ページの情報をサポートしない非ローカル デバイスでは、*vml.* 名が唯一の使用可能な一意の識別子として使用されます。

## 例：vSphere CLI でデバイス名を表示

**esxcli --server=server\_name storage core device list** コマンドを使用して、vSphere CLI ですべてのデバイス名を表示できます。出力は次の例のとおりです。

```
# esxcli --server=server_name storage core device list
naa.number
    Display Name: DGC Fibre Channel Disk(naa.number)
    ...
    Other UIDs:vml.number
```

## ストレージ デバイスの名前の変更

ストレージ デバイスの表示名を変更できます。表示名は、ESXi によって割り当てられます。ストレージ タイプおよびメーカーに基づくホスト

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ デバイス] をクリックします。

- 4 名前を変更するデバイスを選択し、[名前の変更] をクリックします。
- 5 デバイスの名前を分かりやすい名前に変更します。

## ストレージの更新操作および再スキャン操作

データストア、ストレージ デバイス、およびストレージ アダプタを更新すると、vSphere Web Client に表示されるリストとストレージ情報が更新されます。たとえば、データストアの容量などの情報が更新されます。ストレージ管理作業を実行したり、SAN 構成を変更したりすると、ストレージの再スキャンが必要になる場合があります。

VMFS データストアや RDM の作成、エクステンツの追加、VMFS データストアの拡張または縮小など、VMFS データストアの管理操作を実行すると、ホストまたは vCenter Server によって、ストレージが自動的に再スキャンおよび更新されます。自動再スキャン機能は、ホストの再スキャン フィルタをオフにすることで無効にできます。[ストレージ フィルタのオフ](#) を参照してください。

場合によっては、手動で再スキャンを実行する必要があります。ホストで使用可能なすべてのストレージを再スキャンできます。また、vCenter Server を使用している場合は、フォルダ、クラスタ、およびデータセンター内のすべてのホストで使用可能なすべてのストレージを再スキャンできます。

特定のアダプタを介して接続されているストレージに対してのみ変更を行う場合、そのアダプタの再スキャンを実行します。

次のいずれかの変更を行う場合は、その都度、手動で再スキャンを実行します。

- SAN の新しいディスク アレイをゾーニングした場合。
- SAN に新しい LUN を作成した場合。
- ホスト上でパスのマスキングを変更した場合。
- ケーブルを接続しなおした場合。
- CHAP 設定を変更した場合 (iSCSI のみ)。
- 検出アドレスまたは固定アドレスを追加または削除した場合 (iSCSI のみ)。
- vCenter Server ホストおよび単一ホストによって共有されているデータストアを編集または vCenter Server から削除したあと、vCenter Server に単一ホストを追加した場合。

---

**重要：** パスが使用できないときに再スキャンすると、デバイスのパスのリストからホストはそのパスを削除します。パスが使用可能になり、機能し始めると、リストに再び表示されます。

---

## ストレージの再スキャンの実行

SAN 構成を変更すると、ストレージの再スキャンが必要になる場合があります。ホスト、クラスタ、またはデータセンターで利用できるすべてのストレージを再スキャンできます。特定のホストを介してアクセスしているストレージに対してのみ変更を行う場合、そのホストだけの再スキャンを実行します。

### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、ホスト、クラスタ、データセンター、またはホストを含むフォルダを参照します。



- 2 右クリック メニューから、[ストレージ] - [ストレージの再スキャン] を選択します。
- 3 再スキャンの範囲を指定します。

オプション	説明
新規ストレージ デバイスのスキャン	すべてのアダプタを再スキャンして、新しいストレージ デバイスを検出します。新しいデバイスが検出されると、デバイス リストに表示されます。
新規 VMFS ボリュームのスキャン	前回のスキャン以降に追加された新しいデータストアを検出するため、すべてのストレージ デバイスを再スキャンします。見つかった新しいデータストアは、データストア リストに表示されます。

## アダプタの再スキャンの実行

SAN 構成を変更し、これらの変更が特定のアダプタを介してアクセスしているストレージに対してのみ限定される場合、このアダプタだけの再スキャンを実行します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ アダプタ] をクリックし、再スキャンするアダプタをリストから選択します。
- 4 [アダプタの再スキャン] アイコンをクリックします。

## スキャンするストレージ デバイスの数の変更

ESXi ホストがアクセスできる SCSI ストレージ デバイスの台数が 256 台に制限されている場合、LUN ID は 0 ～ 1023 の範囲で設定できます。ESXi は、LUN ID 1024 以降を無視します。この制限は、Disk.MaxLUN（デフォルト値 1024）によって制御されます。

また、Disk.MaxLUN の値は、SCSI ターゲットが REPORT\_LUNS を使用した直接検出をサポートしていない場合に、個々の INQUIRY コマンドを使用して SCSI スキャン コードが検出を試みる LUN の数を指定します。

Disk.MaxLUN パラメータは、必要に応じて変更できます。たとえば、環境内で使用するストレージ デバイスの台数が少なく、LUN ID が 0 ～ 100 に設定されている場合、このパラメータの値を 101 に設定すると、REPORT\_LUNS をサポートしていないターゲットでのデバイス検出速度が向上します。この値を小さくすると、再スキャンの時間と起動時間を短縮できます。ただし、ストレージ デバイスを再スキャンする時間は、ストレージ システムのタイプや、ストレージ システムの負荷など、いくつかの要因によって異なる場合があります。

また、1023 より大きな LUN ID を環境内で使用しているときは、このパラメータの値を増やさなければならない場合があります。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [システム] メニューの [システムの詳細設定] をクリックします。
- 4 システムの詳細設定で、[Disk.MaxLUN] を選択し、[編集] アイコンをクリックします。

- 5 既存の値を目的の数値に変更し、[OK] をクリックします。

検出したい最後の LUN ID の次の LUN ID を指定します。

たとえば、0 ～ 100 の LUN ID を検出するには、[Disk.MaxLUN] を 101 に設定してください。

## デバイス接続問題の確認

ESXi ホストがストレージ デバイスへの接続中に問題を経験すると、ホストは特定の要因に従ってその問題を永続的なものまたは一時的なものとして扱います。

ストレージ接続の問題は、さまざまな要因によって発生します。ESXi がストレージ デバイスやバスが使用できない理由を常に判断することはできませんが、デバイスの永続的なデバイス損失 (PDL) 状態とストレージの一時的な全バス ダウン (APD) 状態は、ホストによって区別されます。

### 永続的なデバイスの損失 (PDL)

ストレージ デバイスが永続的に失敗するか、管理者により削除または除外されている場合に発生する状態です。使用可能になることは期待できません。デバイスが永続的に使用できなくなると、ESXi は、該当する認識コードまたはストレージ アレイからのログイン拒否を受信し、デバイスが永続的に損失していることを認識できます。

### 全バス ダウン (APD)

ストレージ デバイスがホストに対してアクセス不能となり、デバイスへのバスが使用できなくなった場合に発生する状態です。通常デバイスのこの問題は一時的なものであり、デバイスが再び使用できるようになることが期待できるため、ESXi は、これを一時的な状態として扱います。

## PDL 状態の検出

ストレージ デバイスが ESXi ホストで永続的に使用できなくなると、そのストレージ デバイスは永続的なデバイス損失 (PDL) 状態であるとみなされます。

通常、デバイスが誤って削除された場合、一意の ID が変更された場合、デバイスに修復不可能なハードウェア エラーが発生した場合に、PDL 状態が発生します。

ストレージ アレイによりデバイスが永続的に使用できないと判断されると、SCSI 認識コードが ESXi ホストに送信されます。認識コードにより、ホストはデバイスに障害が発生していることを認識し、デバイスの状態が PDL であると登録します。認識コードは、永続的な損失であるとみなされるデバイスへのすべてのバスで受信される必要があります。

デバイスの PDL 状態が登録された後は、ホストは接続の再構築の試みやデバイスへのコマンドの発行を停止し、ブロックまたは未応答状態になるのを回避します。

vSphere Web Client にはデバイスに関する次の情報が表示されます。

- デバイスの動作状態が Lost Communication に変わります。
- すべてのバスが Dead と表示されます。
- デバイス上のデータストアはグレイアウトされます。

デバイスへの開かれた接続が存在しない場合、または最後の接続が閉じた後、ホストは PDL デバイスとデバイスへのすべてのパスを自動的に削除します。パスの自動削除は、ホストの詳細パラメータ `Disk.AutoremoveOnPDL` を 0 に設定することで無効にできます。[ホストの詳細属性の設定](#) を参照してください。

デバイスが PDL 状態から復帰した場合、ホストによって検出されても新しいデバイスと見なされます。リカバリされたデバイス上に存在する仮想マシンのデータの整合性は保証されません。

**注：** ストレージ デバイスに永続的な障害が発生し、適切な SCSI 認識コードや iSCSI ログイン拒否を返せない場合は、ホストは PDL 状態を検出できず、デバイスの接続性の問題を APD であると処理し続けます。

## 永続的なデバイス損失と SCSI 認識コード

次の VMkernel ログは、デバイスが PDL 状態になったことを表す SCSI 認識コードの例です。

```
H:0x0 D:0x2 P:0x0 Valid sense data: 0x5 0x25 0x0 or Logical Unit Not Supported
```

SCSI 認識コードの詳細については、『vSphere トラブルシューティング』の「ストレージのトラブルシューティング」を参照してください。

## 永続的なデバイス損失と iSCSI

ターゲットごとに単一の LUN を持つ iSCSI アレイの場合は、iSCSI ログインの失敗によって PDL が検出されます。iSCSI セッションを開始しようとするホストの試みは、iSCSI ストレージ アレイによってターゲット使用不可との理由で拒否されます。認識コードを使用する場合は、この応答が、永続的な損失であるとみなされるデバイスへのすべてのパスで受信される必要があります。

## 永続的なデバイス損失と仮想マシン

デバイスの PDL 状態の登録後、ホストは仮想マシンからのすべての I/O を終了します。vSphere HA で PDL を検出して失敗した仮想マシンを再起動できます。詳細については、[デバイスの接続問題と高可用性](#) を参照してください。

## 予定されるストレージ デバイスの削除の実行

ストレージ デバイスが正しく機能していないとき、永続的なデバイスの損失 (PDL) または全パス ダウン (APD) の状況を回避し、ストレージ デバイスの予定される削除と再接続を実行できます。

予定されるデバイスの削除とは、ストレージ デバイスを計画的に切断することです。デバイスの削除は、ハードウェアのアップグレードやストレージ デバイスの再構成などの理由で計画することがあります。ストレージ デバイスの削除と再接続を正しく実行するとき、さまざまなタスクを完了させます。

- 1 分離を計画しているデバイスから仮想マシンを移行します。

『vCenter Server およびホスト管理』ドキュメントを参照してください。

- 2 デバイスにデプロイされているデータストアをアンマウントします。

[データストアのアンマウント](#)を参照してください。

- 3 ストレージ デバイスを分離します。

[ストレージ デバイスの分離](#)を参照してください。

- 4 1つのターゲットあたりに1つの LUN のある iSCSI デバイスでは、ストレージ デバイスへのパスのある各 iSCSI HBA から静的ターゲット項目を削除します。

[動的および静的 iSCSI ターゲットの削除](#)を参照してください。

- 5 アレイ コンソールを使用することで、必要なストレージ デバイスの再構成を実行します。
- 6 ストレージ デバイスを再接続します。

[ストレージ デバイスの接続](#)を参照してください。

- 7 データストアをマウントし、仮想マシンを再起動します。 [データストアのマウント](#)を参照してください。

## ストレージ デバイスの分離

ホストからストレージ デバイスを安全に取り外します。

ホストからデバイスにアクセスできないようにするため、デバイスを分離する必要がある場合があります。たとえば、ストレージ側でハードウェアのアップグレードを実行する場合などです。

### 前提条件

- デバイスにはデータストアは含まれていません。
- デバイスを RDM ディスクとして使用している仮想マシンはありません。
- デバイスには、診断パーティションまたはスクラッチ パーティションは含まれていません。

### 手順

- 1 vSphere Web Client で、ストレージ デバイスを表示します。
- 2 分離するデバイスを選択し、[分離] アイコンをクリックします。

### 結果

デバイスがアクセス不能になります。デバイスの動作状態がアンマウント済みに変わります。

### 次のステップ

複数のホストでデバイスを共有している場合は、各ホストでそのデバイスを分離してください。

## ストレージ デバイスの接続

以前に取り外したストレージ デバイスを再接続します。

### 手順

- 1 vSphere Web Client で、ストレージ デバイスを表示します。
- 2 分離されたストレージ デバイスを選択し、[接続] をクリックします。

### 結果

デバイスがアクセス可能になります。

## PDL 状態からのリカバリ

予期しない永続的なデバイスの損失 (PDL) 状態は、ESXi ホストから適切に切り離されずに、ストレージ デバイスが永続的に使用できなくなったときに発生します。

vSphere Web Client 内の次の項目は、デバイスが PDL 状態にあることを示します。

- デバイスにデプロイされているデータストアが使用できない。
- デバイスの動作状態が Lost Communication に変わる。
- すべてのバスの表示が Dead になる。
- VMkernel ログ ファイルに、デバイスが永続的にアクセス不能になっているという警告が表示される。

予期せぬ PDL 状態から復旧し、使用できないデバイスをホストから削除するには、いくつかの作業が必要です。

- 1 PDL 状態の影響を受けているデータストア上で実行されているすべての仮想マシンをパワーオフし、登録解除します。
- 2 データストアをアンマウントします。

[データストアのアンマウント](#) を参照してください。

- 3 デバイスにアクセスしていたすべての ESXi ホストで再スキャンを実行します。

[ストレージの再スキャンの実行](#) を参照してください。

---

**注：** 再スキャンが正常に行われず、ホストが引き続きデバイスを一覧表示し続ける場合は、一部の保留中の I/O またはデバイスに対するアクティブ リファレンスがまだ存在している可能性があります。仮想マシン、テンプレート、ISO イメージ、RAW デバイス マッピングなど、デバイスまたはデータストアに対するアクティブ リファレンスがまだ存在する可能性があるものがないか確認してください。

---

## 一時的な APD 状態の処理

ストレージ デバイスが不特定の期間にわたって ESXi ホストで使用できない状態になると、そのデバイスは全バスダウン (APD) 状態にあるとみなされます。

APD 状態の原因としては、スイッチの不具合またはストレージ ケーブルの切断などが考えられます。

永続的なデバイスの損失 (PDL) 状態の場合とは異なり、ホストは APD 状態を一時的なものとして扱い、デバイスが再び使用可能になることを期待します。

ホストは無制限で、デバイスとの接続性を再び確立する試みの中で、発行されたコマンドを試行し続けます。ホストのコマンドが長期間にわたって再試行を失敗し続ける場合、ホストおよびその仮想マシンにパフォーマンスの問題が生じ、応答不能となるリスクがあります。

これらの問題を回避するために、ホストではデフォルトの APD 処理機能を使用します。デバイスが APD 状態になると、システムはすみやかにタイマーをオンにし、ホストがある一定期間にわたって非仮想マシン コマンドを再試行し続けることを許可します。

デフォルトで、APD タイムアウトは 140 秒に設定されています。これは、ほとんどのデバイスが接続の損失を回復するために必要な時間よりも長い設定となっています。デバイスがこの期間内に使用可能になると、ホストおよび仮想マシンは、問題なく実行を継続します。

デバイスが回復せずタイムアウトが終了した場合、ホストは再試行の試みを停止し、非仮想マシン I/O を終了します。仮想マシン I/O が再試行を継続します。vSphere Web Client には、APD タイムアウトに至ったデバイスについての次の情報が表示されます。

- デバイスの動作状態が `Dead or Error` に変わります。
- すべてのパスが `Dead` と表示されます。
- デバイス上のデータストアが淡色表示されます。

デバイスおよびデータストアは使用できなくても、仮想マシンは応答し続けます。仮想マシンをパワーオフするか、別のデータストアまたはホストに移行することができます。

後で 1 つまたは複数のデバイス パスが操作可能となった場合、通常はデバイスへの次の I/O が発行され、特殊な APD 処理がすべて終了します。

## ストレージ APD 処理の無効化

ESXi ホスト上でのストレージの全パス ダウン (APD) の処理は、デフォルトで有効になっています。有効になっていると、ホストは、APD 状態になっているストレージ デバイスに対して、非仮想マシン I/O コマンドを一定期間実行し続けます。一定時間が経過すると、ホストは再試行を停止し、すべての非仮想マシン I/O を終了します。ホストでの APD 処理機能を無効にすることもできます。

APD 処理を無効にすると、ホストは APD デバイスへの再接続のために発行したコマンドを永久的に実行し続けます。再試行し続ける動作は、ESXi バージョン 5.0 と同じです。この動作が原因となり、ホスト上の仮想マシンがその内部 I/O タイムアウトを超過し、応答しなくなる、または失敗する可能性があります。ホストが vCenter Server から切断されることも考えられます。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [システム] メニューの [システムの詳細設定] をクリックします。
- 4 [システムの詳細設定] で、[Misc.APDHandlingEnable] パラメータを選択し、編集 アイコンをクリックします。
- 5 値を 0 に変更します。

### 結果

APD 処理を無効にした場合でも、デバイスが APD 状態になった場合に処理を再度有効にすることができます。内部 APD 処理機能はすぐにオンになり、APD 状態の各デバイスに対して現在のタイムアウト値でタイマーが起動します。

## ストレージ APD のタイムアウト制限の変更

タイムアウト パラメータは、全パス ダウン (APD) 状態の場合に、ESXi ホストがストレージ デバイスに対して非仮想マシン I/O コマンドを再試行する秒数を制御します。必要に応じて、デフォルトのタイムアウト値を変更できます。

デバイスが APD 状態になると、タイマーがすぐに起動します。タイムアウトになると、APD デバイスにはホストにより、アクセスできない、保留中または新規の非仮想マシン I/O に失敗したとマークが付けられます。仮想マシン I/O は引き続き再試行されます。

ホストのデフォルトのタイムアウト パラメータは 140 秒です。たとえば、ESXi ホストに接続されているストレージ デバイスが接続の喪失から復旧するのに 140 秒以上かかる場合は、タイムアウトの値を増やすことができます。

---

**注：** APD 中にタイムアウト値を変更しても、その APD のタイムアウトには影響しません。

---

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [システム] メニューの [システムの詳細設定] をクリックします。
- 4 [システムの詳細設定] で、[Misc.APDTimeout] パラメータを選択し、編集 アイコンをクリックします。
- 5 デフォルト値を変更します。

値は 20 ~ 99999 秒の範囲で入力できます。

## ストレージ デバイスの接続状態の確認

`esxcli` コマンドを使用して、特定のストレージ デバイスの接続状態を確認します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

#### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

#### 手順

- 1 **`esxcli --server=server_name storage core device list -d=device_ID`** コマンドを実行します。
- 2 ステータス: で接続ステータスを確認します。 フィールドに最大 255 文字の英数字で名前を入力します。
  - on - デバイスが接続されています。
  - dead - デバイスが APD 状態になりました。 APD タイマーが起動します。
  - dead timeout - APD タイムアウトになりました。
  - not connected - デバイスは PDL 状態です。

## デバイスの接続問題と高可用性

デバイスが永続的なデバイス損失 (PDL) 状態や全バス ダウン (APD) 状態になると、vSphere High Availability (HA) は、接続問題を検出し、影響を受けた仮想マシンの自動回復処理を実行します。

vSphere HA は、仮想マシン コンポーネント保護 (VMCP) を使用して、vSphere HA クラスタ内のホストで実行されている仮想マシンをアクセス障害から保護します。VMCP の詳細および APD または PDL 状態が発生した場合のデータストアと仮想マシンの対応の構成方法については、『vSphere 可用性ガイド』ドキュメントを参照してください。

## ストレージ デバイスのロケータ LED の有効化または無効化

ロケータ LED を使用して特定のストレージ デバイスを識別し、それらのデバイスをその他のデバイスの中で特定できるようにします。ロケータ LED はオンまたはオフにできます。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ] で、[ストレージ デバイス] をクリックします。
- 4 ストレージ デバイスのリストからディスクを 1 つ以上選択し、ロケータ LED インジケータを有効または無効にします。

オプション	説明
有効化	[ロケータ LED をオンにする] アイコンをクリックします。
無効化	[ロケータ LED をオフにする] アイコンをクリックします。



# フラッシュ デバイスの操作

# 14

通常のストレージ ハードディスク ドライブ (HDD) に加えて、vSphere はフラッシュ ストレージ デバイスをサポートしています。

駆動パーツを含む磁気デバイスである通常の HDD とは異なり、フラッシュ デバイスはストレージ媒体として半導体を使用し、駆動パーツがありません。通常、フラッシュ デバイスは非常に回復力が高く、データに高速でアクセスできます。

フラッシュ デバイスを検出するため、ESXi では、T10 規格に基づく照会メカニズムを使用します。ESXi ホストは、いくつかのストレージ アレイでフラッシュ デバイスを検出できます。ご使用のストレージ アレイが ESXi のフラッシュ デバイス検出メカニズムをサポートしているかどうかについては、ベンダーにお問い合わせください。

ホストがフラッシュ デバイスを検出した後は、さまざまなタスクや機能でそれらを使用できます。

この章には、次のトピックが含まれています。

- [vSphere でのフラッシュ デバイスの使用](#)
- [ストレージ デバイスのマーク](#)
- [フラッシュ デバイスの監視](#)
- [フラッシュ デバイスのベスト プラクティス](#)
- [仮想フラッシュ リソースについて](#)
- [ホスト スワップ キャッシュの構成](#)

## vSphere でのフラッシュ デバイスの使用

vSphere 環境では、フラッシュ デバイスをさまざまな機能に利用できます。

表 14-1. vSphere でのフラッシュ デバイスの使用

機能	説明
Virtual SAN	Virtual SAN にはフラッシュ デバイスが必要です。詳細については、『VMware Virtual SAN の管理』ドキュメントを参照してください。
VMFS データストア	<p>フラッシュ デバイス上に VMFS データストアを作成できます。データストアは、次の目的で使用します。</p> <ul style="list-style-type: none"> <li>■ 仮想マシンを保存します。特定のゲスト OS では、これらのデータストアに保存されている仮想ディスクをフラッシュ仮想ディスクとして識別できます。 <a href="#">フラッシュ仮想ディスクの特定</a> を参照してください。</li> <li>■ ESXi ホスト スワップ キャッシュ用のデータストア領域を割り当てます。を参照してください。 <a href="#">ホスト スワップ キャッシュの構成</a></li> </ul>
仮想フラッシュ リソース (VFFS)	<p>仮想フラッシュ リソースを設定し、次の機能で 사용합니다。</p> <ul style="list-style-type: none"> <li>■ 仮想マシンで、仮想 Flash Read Cache を 사용합니다。 <a href="#">15 章 VMware vSphere Flash Read Cache について</a> を参照してください。</li> <li>■ ESXi ホスト スワップ キャッシュ用に仮想フラッシュ リソースを割り当てます。これは、VMFS データストアの代わりに VFFS ボリュームを使用するホスト キャッシュ構成の代替方法です。 <a href="#">仮想フラッシュ リソースを使用したホスト スワップ キャッシュの構成</a> を参照してください。</li> <li>■ ベンダーによって要求される場合は、I/O キャッシュ フィルタに仮想フラッシュ リソースを 사용합니다。 <a href="#">21 章 仮想マシン I/O のフィルタリング</a> を参照してください。</li> </ul>

## フラッシュ仮想ディスクの特定

ゲスト OS では、フラッシュベースのデータストアにフラッシュ仮想ディスクとして存在する仮想ディスクを識別することができます。

この機能が有効かどうかを検証するには、ゲストのオペレーティング システムは SCSI デバイスに SCSI VPD Page (B1h) および IDE デバイスに ATA IDENTIFY DEVICE (Word 217) などの標準的照会コマンドを使用できます。

リンク クローン、ネイティブのスナップショット、デルタ ディスクの場合には、照会コマンドによってベース ディスクの仮想フラッシュ ステータスが報告されます。

オペレーティング システムは、任意の仮想ディスクがフラッシュ ディスクであることを次の条件で検出できます。

- フラッシュ仮想ディスクの検出は、ESXi 5.x 以降のホストと仮想ハードウェア バージョン 8 以降でサポートされます。
- フラッシュ仮想ディスクの検出は、VMFS5 以降でのみサポートされます。
- フラッシュ デバイス エクステントによる共有 VMFS データストアに仮想ディスクが配置されている場合は、すべてのホストでデバイスにフラッシュのマークを付ける必要があります。
- 仮想ディスクが仮想フラッシュとして識別されるためには、基盤となるすべての物理エクステントをフラッシュベースにする必要があります。

## ストレージ デバイスのマーク

vSphere Web Client を使用して、ローカル フラッシュ デバイスとして自動的に認識されないストレージ デバイスにマークを付けることができます。

Virtual SAN を構成したり、仮想フラッシュ リソースを設定したりする場合は、ストレージ環境にローカル フラッシュ デバイスが含まれている必要があります。

ただし、ESXi は、デバイスのベンダーが自動フラッシュ デバイス検出をサポートしていない場合、特定のストレージ デバイスをフラッシュ デバイスとして認識しない可能性があります。その他、特定の非 SATA SAS フラッシュ デバイスがローカルとして検出されない可能性もあります。デバイスは、ローカル フラッシュとして認識されない場合、Virtual SAN または仮想フラッシュ リソースに提供されるデバイスのリストから除外されます。これらのデバイスにローカル フラッシュとしてマークを付けると、仮想 SAN および仮想フラッシュ リソースで使用可能になります。

## ストレージ デバイスをフラッシュとしてマーク

ESXi がデバイスを自動的にフラッシュと認識しない場合には、デバイスをフラッシュ デバイスとしてマークします。

デバイスのベンダーが自動フラッシュ ディスク検出をサポートしていないと、ESXi は特定のデバイスをフラッシュとして認識しません。デバイスの [ドライブのタイプ] 列に、デバイスのタイプとして HDD が表示されます。

---

**注意：** HDD ディスクをフラッシュ ディスクとしてマークすると、それらのディスクを使用するデータストアおよびサービスのパフォーマンスが低下することがあります。それらのディスクがフラッシュ ディスクであることが確実な場合にのみ、フラッシュ ディスクとしてマークしてください。

---

### 前提条件

デバイスが使用中ではないことを確認します。

### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[ストレージ] をクリックします。
- 3 [ストレージ デバイス] をクリックします。
- 4 ストレージ デバイスの一覧から、フラッシュ デバイスとして認識される必要がある HDD デバイスを 1 個以上選択し、[フラッシュ ディスクとしてマーク] アイコン (F) をクリックします。
- 5 [はい] をクリックして変更を保存します。

### 結果

デバイスのタイプがフラッシュに変更されます。

### 次のステップ

マークするフラッシュ デバイスを複数のホストで共有する場合には、デバイスを共有するすべてのホストでデバイスがマークされていることを確認します。

## ストレージ デバイスをローカルとしてマーク

ESXi により、デバイスをローカルとしてマークすることができます。これは、ESXi で特定のデバイスがローカルかどうかを判別できない場合に役立ちます。

### 前提条件

- デバイスが共有されていないことを確認します。
- デバイ스에 常駐する仮想マシンをパワーオフし、関連データストアをアンマウントします。

### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、ホストに移動して参照します。
- 2 [管理] タブをクリックして、[ストレージ] をクリックします。
- 3 [ストレージ デバイス] をクリックします。
- 4 ストレージ デバイスのリストから、ローカルとしてマークする必要があるリモート デバイスを 1 つ以上選択し、[ホストのローカルとしてマーク] アイコンをクリックします。
- 5 [はい] をクリックして変更を保存します。

## フラッシュ デバイスの監視

メディア消費指数、温度、および再割り当てセクター カウントなど特定の重要なフラッシュ デバイス パラメータを ESXi ホストから監視できます。

esxcli コマンドを使用してフラッシュ デバイスを監視します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- ◆ 次のコマンドを実行し、フラッシュ デバイスの統計情報を表示します。

```
esxcli server=server_name storage core device smart get -d=flash device_ID
```

## フラッシュ デバイスのベスト プラクティス

vSphere 環境でフラッシュ デバイスを使用するときは、ベスト プラクティスに従ってください。

- フラッシュ デバイスを含む最新のファームウェアを使用してください。更新がないか、ストレージのベンダーからの情報を頻繁に確認してください。
- フラッシュ デバイスの使用頻度を注意して監視し、耐用年数の推定値を算出します。耐用年数の推定値は、どの程度フラッシュ デバイスを使用し続けたかによって異なります。

## フラッシュ デバイスの有効期間の推定

フラッシュ デバイスを使用する場合は、その使用頻度を監視して、耐用年数の推定値を算出します。

通常、ストレージのベンダーは理想的な条件下でのフラッシュ デバイスの信頼性のある耐用年数推定値を提供しています。たとえば、ベンダーによって、1 日あたり 20GB の書き込みが行われるという条件下で、5 年間の耐用年数が保証されている場合があるかもしれません。しかし、デバイスのより現実的な寿命は ESXi ホストで実際に行われる 1 日あたりの書き込み数によって左右されます。次の手順に従って、フラッシュ デバイスの耐用年数を算出してください。

### 前提条件

前回 ESXi ホストを再起動してからの経過日数を書き留めます。たとえば、10 日などです。

### 手順

- 1 前回の再起動以降にフラッシュ デバイスに書き込まれたブロックの合計数を割り出します。

**esxcli storage core device stats get -d=device\_ID** コマンドを実行します。例：

```
~ # esxcli storage core device stats get -d t10.000000000000000000
Device: t10.000000000000000000
Successful Commands: 1
Blocks Read: 0
Blocks Written: 629145600
Read Operations: 0
```

出力の [書き込みブロック] の項目は、前回の再起動以降にデバイスに書き込まれたブロック数を示します。この例では、値は 629,145,600 です。再起動のたびに、値が 0 にリセットされます。

- 2 書き込みの合計数を計算し、GB に変換します。

1 ブロックは 512 バイトです。書き込みの合計数を計算するには、[書き込みブロック] の値を 512 倍し、その計算結果を GB に変換します。

この例で、前回の再起動以降の書き込みの合計数は約 322 GB です。

- 3 1 日あたりの書き込みの平均数を GB 単位で推定します。

書き込みの合計数を前回の再起動からの経過日数で割ります。

前回の再起動が 10 日前の場合、1 日あたりの書き込み数は 32 GB となります。この期間にわたって、この数字の平均値を取ることができます。

#### 4 次の公式を使用して、デバイスの耐用年数を見積もります。

ベンダーから提供された 1 日あたりの書き込み数 × ベンダーから提供された耐用年数 ÷ 1 日あたりの実際の書き込み平均数

たとえば、ベンダーが 1 日あたり 20 GB の書き込みが行われる条件下で 5 年間の耐用年数を保証している場合、1 日あたりの実際の書き込み平均数が 30 GB であれば、フラッシュ デバイスの耐用年数はおよそ 3.3 年になります。

## 仮想フラッシュ リソースについて

ESXi ホスト上のローカル フラッシュ デバイスは、仮想フラッシュ リソースと呼ばれる 1 つの仮想化キャッシュ レイヤーに集約することができます。

仮想フラッシュ リソースの設定時には、新しいファイル システムとして仮想フラッシュ ファイル システム (VFFS) を作成します。VFFS は VMFS からの派生システムで、フラッシュ デバイス用に最適化されており、物理フラッシュ デバイスを 1 つのキャッシュ リソース プールにグループ化するために使用されます。読み取り専用リソースであるため、仮想マシンの保存先として使用することはできません。

次の vSphere の各機能には、仮想フラッシュ リソースが必要です。

- 仮想マシンの読み取りキャッシュ。15 章 [VMware vSphere Flash Read Cache について](#) を参照してください。
- ホスト スワップ キャッシュ。仮想フラッシュ リソースを使用したホスト スワップ キャッシュの構成を参照してください。
- I/O キャッシュ フィルタ (ベンダーによって要求されている場合)。21 章 [仮想マシン I/O のフィルタリング](#) を参照してください。

仮想フラッシュ リソースを設定する前に、『VMware 互換性ガイド』で認定されているデバイスを使用していることを確認してください。

## 仮想フラッシュ リソースの考慮事項

ESXi ホストと仮想マシンが消費する仮想フラッシュ リソースを構成する場合には、いくつかの考慮事項が適用されます。

- 仮想フラッシュ リソースは VFFS ボリュームとも呼ばれ、1 つの ESXi ホストに 1 つだけ配置できます。仮想フラッシュ リソースは、ホストのレベルでのみ管理されます。
- 仮想フラッシュ リソースを使用して仮想マシンを保存することはできません。仮想フラッシュ リソースは、キャッシュ レイヤーのみです。
- 仮想フラッシュ リソースとして使用できるのは、ローカル フラッシュ デバイスのみです。
- 仮想フラッシュ リソースは、混在するフラッシュ デバイスで作成することができます。すべてのデバイス タイプが同様の方法で扱われ、SAS、SATA、または PCI Express 接続の区別はありません。混在するフラッシュ デバイスからリソースを作成する場合は、性能が似ているデバイスをまとめてグループ化し、確実にパフォーマンスが最大化されるようにしてください。

- 仮想フラッシュ リソースと Virtual SAN で同じフラッシュ デバイスを使用することはできません。それぞれに、独自の排他的かつ専用のフラッシュ デバイスが必要です。
- 仮想フラッシュ リソースの設定後は、ESXi ホストによりホスト スワップ キャッシュとして、また仮想マシンにより読み取りキャッシュとして使用可能な合計容量が使用され、消費されるようにすることができます。
- スワップ キャッシュまたは読み取りキャッシュのいずれかとして使用するために個々のフラッシュ デバイスを選択することはできません。すべてのフラッシュ デバイスは、単一のフラッシュ リソース エンティティに結合されます。

## 仮想フラッシュ リソースの設定

仮想フラッシュ リソースを設定したり、既存の仮想フラッシュ リソースに容量を追加したりできます。

仮想フラッシュ リソースを設定するには、ホストに接続されたローカル フラッシュ デバイスを使用します。仮想フラッシュ リソースの容量を増やすため、『構成の上限』ドキュメントに示されている最大数までデバイスを追加することができます。個々のフラッシュ デバイスは、仮想フラッシュ リソース専用割り当てが必要があり、Virtual SAN や VMFS などの他の vSphere サービスと共有することはできません。

### 手順

- 1 vSphere Web Client で、ホストに移動します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [仮想フラッシュ] で [仮想フラッシュ リソース管理] を選択し、[容量を追加] をクリックします。
- 4 使用可能なフラッシュ デバイスのリストから、仮想フラッシュ リソースで使用するデバイスを 1 つ以上選択し、[OK] をクリックします。

特定の状況下では、リストにフラッシュ デバイスが表示されないことがあります。詳細については、『vSphere トラブルシューティング』ドキュメントの「フラッシュ デバイスのトラブルシューティング」セクションを参照してください。

### 結果

仮想フラッシュ リソースが作成されます。[デバイスの補助] 領域に、仮想フラッシュ リソースとして使用するすべてのデバイスが一覧表示されます。

### 次のステップ

仮想フラッシュ リソースはホストのキャッシュ構成や仮想ディスクの Flash Read Cache 構成で使用できます。さらに、vSphere APIs for I/O Filtering で開発された I/O キャッシュ フィルタで仮想フラッシュ リソースが必要になることがあります。

容量は、仮想フラッシュ リソースにフラッシュ デバイスを追加することによって増加できます。

## 仮想フラッシュ リソースの削除

デバイスを他のサービスに解放するために、ローカル フラッシュ デバイスにデプロイされた仮想フラッシュ リソースの削除が必要になることがあります。

仮想フラッシュ リソースは、ホスト スワップ キャッシュで構成されている場合、またはフラッシュ読み取りキャッシュで構成されパワーオンされた仮想マシンがホストにある場合は、削除できません。

#### 手順

- 1 vSphere Web Client で、仮想フラッシュが構成されているホストに移動します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [仮想フラッシュ] で、[仮想フラッシュ リソース管理] を選択し、[すべてを削除する] をクリックします。

#### 結果

仮想フラッシュ リソースを削除し、フラッシュ デバイスを消去したら、他の操作でデバイスを利用できるようになります。

## 仮想フラッシュの詳細設定

仮想フラッシュの詳細オプションを変更できます。

#### 手順

- 1 vSphere Web Client で、ホストに移動します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [[システム]] メニューの [[システムの詳細設定]] をクリックします。
- 4 変更する設定を選択して、[編集] ボタンをクリックします。

オプション	説明
[VFLASH.VFlashResourceUsageThreshold]	仮想フラッシュ リソース使用量がしきい値を超えた場合は、ホストの vFlash リソース使用量アラームがトリガーされます。デフォルトのしきい値は 80% です。このしきい値を適切な値に変更できます。仮想フラッシュ リソース使用量がしきい値を下回ると、アラームは自動的にクリアされます。
[VFLASH.MaxResourceGBForVmCache]	ESXi ホストは、Flash Read Cache のメタデータを RAM に格納します。ホスト上の仮想マシンの合計キャッシュ サイズは、デフォルトで 2TB に制限されます。この設定は再構成できます。新しい設定を有効にするには、ホストを再起動する必要があります。

- 5 [[OK]] をクリックします。

## ホスト スワップ キャッシュの構成

ESXi ホストでは、フラッシュバックされたストレージ エンティティの一部を、すべての仮想マシンによって共有されるスワップ キャッシュとして使用できます。

ホストレベルのキャッシュは、ESXi が仮想マシン スワップ ファイルの書き込み戻しキャッシュとして使用する低待ち時間のディスク上のファイルから構成されます。このキャッシュは、このホスト上で実行されているすべての仮想マシンで共有されます。仮想マシン ページのホストレベルのスワップは、容量に限りがある可能性があるフラッシュ デバイス領域を有効活用します。



環境およびライセンス パッケージに応じ、次の方法を使用してホストレベルのスワップ キャッシュを構成することができます。両方の方法で同様の結果が得られます。

- フラッシュ デバイスで VMFS データストアを作成し、そのデータストアを使用してホスト キャッシュの領域を割り当てることができます。ホストは、ホスト キャッシュへのスワップ用に一定量の領域を確保します。
- 仮想フラッシュ リソースを設定および管理するための適切な vSphere ライセンスがある場合は、リソースを使用してホストでスワップ キャッシュを構成することができます。ホスト スワップ キャッシュは、仮想フラッシュ リソースの部分から割り当てられます。

## VMFS データストアによるホスト キャッシュの構成

ホスト キャッシュにスワップするホストの機能をオンにします。ホスト キャッシュに割り当てられる領域の割合を変更することもできます。

仮想フラッシュ リソースをセットアップして管理できる適切なライセンスを持っていない場合は、このタスクを使用します。ライセンスがある場合は、仮想フラッシュ リソースを使用して、ホスト キャッシュを構成します。

### 前提条件

フラッシュバック VMFS データストアを作成します。[VMFS データストアの作成](#) を参照してください。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ホスト キャッシュの構成] をクリックします。
- 4 データストアをリストから選択し、[[ホスト キャッシュに領域を割り当て]] アイコンをクリックします。
- 5 データストアごとにホスト スワップ キャッシュを有効化するには、[ホスト キャッシュに領域を割り当て] チェック ボックスを選択します。

デフォルトでは、ホスト キャッシュには使用可能な最大領域が割り当てられます。

- 6 (オプション) ホスト キャッシュ サイズを変更するには、[カスタム サイズ] を選択して、適切に調整します。
- 7 [OK] をクリックします。

## 仮想フラッシュ リソースを使用したホスト スワップ キャッシュの構成

ホスト スワップ キャッシュ用に一定量の仮想フラッシュ リソースを予約できます。

### 前提条件

仮想フラッシュ リソースを設定します。[仮想フラッシュ リソースの設定](#)。

---

**注：** 仮想フラッシュを使用して構成された ESXi ホストがメンテナンス モードになっている場合、ホスト スワップ キャッシュを追加または変更できません。ホスト スワップ キャッシュを構成する前に、まずホストのメンテナンス モードを終了する必要があります。

---

## 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [仮想フラッシュ] で、[仮想フラッシュ ホスト スワップ キャッシュ構成] を選択し、[編集] をクリックします。
- 4 [仮想フラッシュ ホスト スワップ キャッシュの有効化] チェック ボックスを選択します。
- 5 ホスト スワップ キャッシュ用に予約する仮想フラッシュ リソースの容量を指定します。
- 6 [OK] をクリックします。

# VMware vSphere Flash Read Cache について

# 15

Flash Read Cache™ を使うと、ホスト上のフラッシュ デバイスをキャッシュとして使用するため、仮想マシンのパフォーマンスを向上できます。

各仮想ディスクに Flash Read Cache を予約できます。Flash Read Cache は、仮想マシンがパワーオンになったときにのみ作成され、仮想マシンがサスペンド状態またはパワーオフ状態になると破棄されます。仮想マシンを移行するときには、キャッシュを移行するオプションがあります。デフォルトでは、ソースおよびターゲット ホストの仮想フラッシュ モジュールに互換性があればキャッシュは移行されます。キャッシュを移行しない場合、キャッシュはターゲット ホストでリウォームされます。仮想マシンがパワーオンされている間はキャッシュのサイズを変更できます。このインスタンスでは、既存のキャッシュが破棄され、新しいライトスルー キャッシュが作成され、キャッシュのウォーム アップ期間となります。新しいキャッシュを作成するメリットは、キャッシュのサイズがアプリケーションのアクティブ データと良く一致することです。

Flash Read Cache は、ライトスルーまたは読み取りキャッシュをサポートしています。ライト バックまたは書き込みキャッシュはサポートされていません。キャッシュがある場合には、データの読み取りはキャッシュから実行されます。データの書き込みは SAN または NAS などのバックング ストレージにディスパッチされます。バックング ストレージから読み取り、またはバックング ストレージに書き込みされるすべてのデータは、無条件にキャッシュに格納されます。

Flash Read Cache は物理互換の RDM をサポートしていません。仮想互換の RDM は Flash Read Cache でサポートされています。

Flash Read Cache の詳細については、ビデオをご覧ください。



( vSphere Flash Read Cache の構成 )

**注：** すべてのワークロードで Flash Read Cache によるメリットがあるわけではありません。パフォーマンスがどの程度向上するかは、ワークロードのパターンと作業セットのサイズによって異なります。読み取りを多用するワークロードにキャッシュに合わせた作業セットを組み合わせると、Flash Read Cache 構成のメリットを最大限に生かすことができます。読み取りを多用するワークロードに Flash Read Cache を構成することにより、追加の I/O リソースが共有ストレージで使用可能になり、Flash Read Cache を使用しない構成の他のワークロードでもパフォーマンスの向上が期待できます。

この章には、次のトピックが含まれています。

- フラッシュ読み取りキャッシュの DRS サポート
- vSphere High Availability のフラッシュ読み取りキャッシュのサポート

- 仮想マシンの Flash Read Cache を構成
- Flash Read Cache とともに仮想マシンを移行

## フラッシュ読み取りキャッシュの DRS サポート

DRS はリソースとして仮想フラッシュをサポートします。

DRS はフラッシュ読み取りキャッシュ予約で仮想マシンを管理します。DRS を実行するたびに、ESXi ホストによって報告された使用可能な仮想フラッシュ容量が表示されます。各ホストは 1 つの仮想フラッシュ リソースをサポートします。DRS は、仮想マシンの起動に十分な仮想フラッシュ容量のあるホストを選択します。DRS は、フラッシュ読み取りキャッシュを備えたパワーオン状態の仮想マシンが、その現在のホストに対してソフト アフィニティがあるものと見なされ、どうしても必要な理由がある場合、またはホストの高すぎる使用率の修正に必要な場合にのみ、これらのマシンを移動します。

## vSphere High Availability のフラッシュ読み取りキャッシュのサポート

HA (High Availability) では、フラッシュ読み取りキャッシュがサポートされています。

vSphere HA がフラッシュ読み取りキャッシュで構成された仮想マシンを再起動するときは、フラッシュ読み取りキャッシュ、CPU、メモリとオーバーヘッド予約が適合したクラスターのホスト上の仮想マシンが再起動されます。vSphere HA は、予約されていないフラッシュが仮想フラッシュの予約に十分でない場合には仮想マシンを再起動しません。ターゲットのホストに使用可能な仮想フラッシュ リソースが十分でない場合は、仮想マシンを手動で再構成してフラッシュ読み取りキャッシュを減らすかドロップする必要があります。

## 仮想マシンの Flash Read Cache を構成

ESXi 5.5 以降と互換性がある仮想マシンに Flash Read Cache を構成できます。

Flash Read Cache を有効にするとブロック サイズとキャッシュ サイズを指定して予約ができます。

ブロック サイズとはキャッシュに格納される連続したバイトの最小数です。ブロック サイズは公称のディスクのブロック サイズ 512 バイトよりも大きく、4 KB と 1024 KB の間に設定できます。ゲスト OS が単一の 512 バイトのディスク ブロックに書き込む場合、周囲のキャッシュ ブロック サイズのバイトがキャッシュされます。キャッシュ ブロック サイズとディスク ブロック サイズを混同しないでください。

予約とはキャッシュ ブロックの予約サイズです。256 キャッシュ ブロックの最小数があります。キャッシュ ブロック サイズが 1 MB の場合、最小キャッシュ サイズは 256 MB になります。キャッシュ ブロック サイズが 4 KB の場合、最小キャッシュ サイズは 1 MB になります。

サイズ設定のガイドラインについては、VMware Web サイトのホワイト ペーパー『Performance of vSphere Flash Read Cache in VMware vSphere (VMware vSphere の vSphere Flash Read Cache のパフォーマンス)』を参照してください。

### 前提条件

- 仮想フラッシュ リソースを設定します。

- 仮想マシンが ESXi 5.5 以降と互換性があることを確認します。

#### 手順

- 1 仮想マシンを見つけるには、データセンター、フォルダ、クラスタ、リソース プール、ホスト、または vApp を選択します。
- 2 [関連オブジェクト] タブで、[仮想マシン]をクリックします。
- 3 仮想マシンを右クリックし、[設定の編集] を選択します。
- 4 [仮想ハードウェア] タブで、[ハード ディスク] を展開してディスク オプションを表示します。
- 5 仮想マシンの Flash Read Cache を有効にするには、[仮想 Flash Read Cache] テキスト ボックスに値を入力します。
- 6 [詳細] をクリックして次のパラメータを指定します。

オプション	説明
予約	キャッシュ サイズの予約を選択します。
ブロック サイズ	ブロック サイズを選択します。

- 7 [OK] をクリックします。

## Flash Read Cache とともに仮想マシンを移行

パワーオンされた仮想マシンを、あるホストから別のホストに移行する際に、仮想ディスクとともに Flash Read Cache コンテンツを移行するかどうかを指定できます。

#### 前提条件

Flash Read Cache コンテンツを移行する場合は、ターゲット ホストで十分な仮想フラッシュ リソースを設定します。

#### 手順

- 1 実行中の仮想マシンを右クリックして [移行] を選択します。
- 2 移行タイプを指定します。

オプション	説明
コンピューティング リソースのみ変更します	仮想マシンを別のホストまたはクラスタに移行します。
コンピューティング リソースとストレージの両方を変更します	仮想マシンを特定のホストまたはクラスタに移行し、そのストレージを特定のデータストアまたはデータストア クラスタに移行します。

- 3 ターゲット ホストを選択して、[次へ] をクリックします。

- 4 仮想 Flash Read Cache で設定されたすべての仮想ディスクの移行設定を指定します。この移行パラメータは、ホストを変更せずにデータストアの変更のみを行う場合には表示されません。

フラッシュ読み取りキャッシュ移行設定	説明
常にキャッシュ コンテンツを移行	ターゲット ホストにすべてのキャッシュ コンテンツを移行できる場合にのみ、仮想マシンの移行は処理されます。このオプションは、キャッシュが小さいときやキャッシュのサイズがアプリケーションのアクティブ データにきわめて近いときに役立ちます。
キャッシュ コンテンツを移行しない	ライトスルー キャッシュを削除します。キャッシュはターゲット ホストで再作成されます。このオプションは、キャッシュが大きいときやキャッシュのサイズがアプリケーションのアクティブ データよりも大きいときに役立ちます。

- 5 Flash Read Cache を持つ仮想ディスクが複数存在する場合、個別のディスクごとに移行設定を調整できます。
- [詳細] をクリックします。
  - 移行設定を変更する仮想ディスクを選択します。
  - [仮想 Flash Read Cache 移行設定] 列のドロップダウン メニューから、適切なオプションを選択します。
- 6 移行設定を完了し、[終了] をクリックします。

#### 次のステップ

仮想マシンの [サマリ] タブを調べて、移行が成功したことを確認します。

- このタブでターゲット ホストの IP アドレスが正しく表示されていることを確認します。
- [仮想マシンのハードウェア] パネルに各仮想ディスクの仮想 Flash Read Cache 情報が正しく表示されていることを確認します。

# データストアでの作業

# 16

データストアとは、ファイル システムに似た論理コンテナで、物理ストレージの仕様を隠し、仮想マシン ファイルを格納するための一貫したモデルを提供します。データストアは、ISO イメージ、仮想マシン テンプレート、およびフロッピー イメージの格納にも使用できます。

使用するストレージによって、データストアは次のタイプに分けることができます。

- 仮想マシン ファイル システム フォーマットに支持された VMFS データストア。[VMFS データストアについて](#) を参照してください。
- ネットワーク ファイル システム NFS に支持された NFS データストア。[ネットワーク ファイル システム データストアについて](#) を参照してください。
- Virtual SAN データストア。『VMware Virtual SAN の管理』ドキュメントを参照してください。
- 仮想ボリューム データストア。[19 章 仮想ボリュームの操作](#) を参照してください。

データストアの作成後、データストアでいくつかの管理操作を実行できます。すべてのタイプのデータストアで、データストアの名前変更などの特定の操作を実行できます。一方、その他の操作は特定のタイプのデータストアに適用されます。

データストアは、別の方法で編成することもできます。たとえば、業務の内容に応じて、データストアをフォルダにグループ化できます。これにより、グループ内のデータストアに対して同じ権限およびアラームを同時に割り当てることができます。

データストアはデータストア クラスタに追加することもできます。データストア クラスタは、リソースと管理インターフェイスが共有されたデータストアの集まりです。データストア クラスタを作成すると、Storage DRS を使用してストレージ リソースを管理できます。データストア クラスタの詳細については、『vSphere リソース管理』ドキュメントを参照してください。

この章には、次のトピックが含まれています。

- [VMFS データストアについて](#)
- [ネットワーク ファイル システム データストアについて](#)
- [データストアの作成](#)
- [重複 VMFS データストアの管理](#)
- [VMFS データストアのアップグレード](#)
- [VMFS データストア容量の増加](#)
- [データストアの管理操作](#)

- 動的なディスクミラーリングの設定
- ストレージ デバイスでの ESXi ホストの診断情報の収集
- VOMA によるメタデータの整合性の確認
- VMFS ポインタ ブロック キャッシュの構成

## VMFS データストアについて

仮想ディスクを格納するために、ESXi はデータストアを使用します。データストアとは、仮想マシンから物理ストレージの特性を隠し、仮想マシン ファイル格納用の一貫したモデルを提供する論理コンテナです。ブロック ストレージ デバイスにデプロイされたデータストアは、vSphere VMFS フォーマットを使用します。vSphere VMFS フォーマットとは、仮想マシンの格納用に最適化された特殊な高性能ファイル システム フォーマットです。

VMFS ファイル システムには、その導入時以降、いくつかのバージョンが公開されています。次の表では、ホストと VMFS のバージョンの関係を示します。

表 16-1. ホスト アクセスと VMFS のバージョン

VMFS	ESX/ESXi 3.x ホスト	ESX/ESXi 4.x ホスト	ESXi 5.x ホスト	ESXi 6.x ホスト
VMFS2	RO	RO	N	N
VMFS3	RW	RW	RW	RW
<b>注：</b> 既存の VMFS3 データストアは引き続き使用できますが、新しい VMFS3 データストアを作成することはできません。既存の VMFS3 データストアが存在する場合、VMFS5 にアップグレードします。				
VMFS5	N	N	RW	RW

- RW：読み書きを完全にサポート。仮想マシンを作成し、パワーオンできます。
- RO：読み取り専用をサポート。仮想マシンの作成およびパワーオンはできません。
- N：アクセスなし。ESXi 5.x 以降のホストでは VMFS2 はサポートされません。データストアが VMFS2 でフォーマットされていた場合は、始めにレガシー ホストを使用してデータストアを VMFS3 にアップグレードしてください。

vSphere Web Client を使用して、ESXi ホストが検出するブロック ベースのストレージ デバイス上に、VMFS データストアをあらかじめ設定します。VMFS データストアは、SAN LUN やローカル ストレージなどの複数の物理ストレージ エクステンツにまたがって拡張できます。この機能によってストレージのプール操作が可能になり、仮想マシンに必要なデータストアを柔軟に作成できます。

**注：** ATS 対応ハードウェアをプールすると、ATS 専用ロック メカニズムを使用できる、複数にまたがる VMFS データストアが作成されます。いずれかのデバイスが ATS 対応でない場合、データストアは ATS 専用になることはできませんが、ATS+SCSI ロックが使用されます。



仮想マシンがデータストア上で実行されている間に、データストアの容量を拡張できます。この機能によって、仮想マシンが新しい領域を要求するたびに、VMFS データストアにその領域を追加できます。VMFS は複数の物理マシンから同時にアクセスできるように設計されており、仮想マシン ファイルへのアクセス制御を適切に実行します。

## VMFS5 データストアの特性

VMFS5 は、スケーラビリティとパフォーマンスの面で多くの点が強化されています。

VMFS5 には、次の特性があります。

- 各 VMFS5 エクステンツで 2TB を超えるストレージ デバイス。
- 大容量の仮想ディスク、または 2TB を超えるディスクを持つ仮想マシンのサポート。
- ファイル記述子などでリソース制限を拡大。
- 1MB のファイル システム ブロック サイズを標準とし、2TB の仮想ディスクをサポート。
- RDM 用の 2TB を超えるディスク サイズ。
- 1 KB の小さなファイルをサポート。
- VMFS5 データストアにあるあらゆるファイルを、最大 32 台のホストによる共有モードで開くことが可能。
- ハードウェア アクセラレーションをサポートするストレージ デバイスでスケーラビリティを向上。詳細については、[23 章 ストレージのハードウェア アクセラレーション](#) を参照してください。
- ATS をサポートするストレージ デバイスで ATS のみのロック メカニズムをデフォルトで使用。ATS のみのロックと ATS のみのロックへのアップグレードを行う方法については、[VMFS のロック メカニズム](#) を参照してください。
- シン プロビジョニングされたストレージ デバイスでの物理ストレージ領域の解放が可能。詳細については、[アレイ シン プロビジョニングおよび VMFS データストア](#) を参照してください。
- 実行中のホストや仮想マシンを中断せずに、既存のデータストアをアップグレードする、オンライン アップグレード プロセス。詳細については、[VMFS データストアのアップグレード](#) を参照してください。

VMFS データストアのブロック サイズ制限に関する情報については、VMware のナレッジ ベースの記事 <http://kb.vmware.com/kb/1003565> を参照してください。

## VMFS データストアとストレージ ディスク フォーマット

ホストでサポートされているストレージ デバイスでは、マスタ ブート レコード (MBR) フォーマットまたは GUID パーティション テーブル (GPT) フォーマットを使用できます。

新しい VMFS5 データストアを作成すると、デバイスは GPT でフォーマットされます。GPT フォーマットにより、単一のエクステンツについて、2TB より大きい、最大 64TB のデータストアを作成できます。

VMFS3 データストアでは、ストレージ デバイス用に MBR フォーマットが引き続き使用されます。VMFS3 データストアで作業する際は、次の点を考慮してください。

- VMFS3 データストアでは、ストレージ デバイスの容量が 2TB を超えていても、2TB の制限が引き続き適用されます。ストレージの領域全体を使用するには、VMFS3 データストアを VMFS5 にアップグレードします。MBR フォーマットから GPT への変換は、データストアを 2TB を超えるサイズに拡張したあとでのみ可能です。

- VMFS3 データストアを VMFS5 にアップグレードすると、データストアでは MBR フォーマットが使用されます。GPT への変換は、データストアを 2TB を超えるサイズに拡張したあとでのみ可能です。
- VMFS3 データストアをアップグレードする場合は、ESXi で認識されないパーティションをストレージ デバイスから削除してください。たとえば、EXT2 または EXT3 フォーマットを使用するパーティションです。そうしないと、ホストはデバイスを GPT でフォーマットできず、アップグレードは失敗します。
- GPT パーティション フォーマットのあるデバイス上の VMFS3 データストアは拡張できません。

## VMFS データストアとリポジトリ

ESXi は、SCSI ベースのストレージ デバイスを VMFS データストアとしてフォーマットできます。VMFS データストアは、主に仮想マシンのリポジトリとして機能します。

VMFS5 では、ホスト 1 台あたり最大 256 個の VMFS データストア（サイズは最大 64TB）を設定できます。1 つの VMFS データストアに必要な領域は 1.3GB ですが、少なくとも 2GB を確保することをお勧めします。

---

**注：** 各 LUN に作成できる VMFS データストアは 1 つだけです。

---

1 つの VMFS データストアに複数の仮想マシンを格納できます。各仮想マシンは、ファイル セットにカプセル化され、1 つの独立したディレクトリに格納されます。VMFS は、仮想マシン内のオペレーティング システム向けに、内部ファイルシステムのセマンティックを保持します。これにより、仮想マシンで動作するアプリケーションの正常な動作やデータの整合性が保障されます。

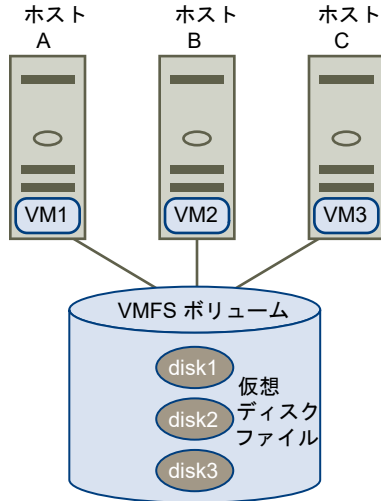
複数の仮想マシンを実行する場合、VMFS では仮想マシン ファイルに対する特別なロック メカニズムが提供されます。これにより仮想マシンは、複数の ESXi ホストが同じ VMFS データストアを共有する SAN 環境で安全に動作できます。

仮想マシンに加え、VMFS データストアに、仮想マシン テンプレートや ISO イメージなどのほかのファイルを格納することもできます。

## ホスト間の VMFS データストアの共有

VMFS はクラスタ ファイル システムであるため、複数の ESXi ホストが同じ VMFS データストアへ同時にアクセスすることが可能です。

図 16-1. ホスト間の VMFS データストアの共有



1 つの VMFS データストアに接続できるホストの最大数については、『構成の上限』ドキュメントを参照してください。

複数のホストが同時に同じ仮想マシンにアクセスするのを防ぐために、VMFS にはオンディスク ロック機能があります。

複数のホスト間で VMFS ボリュームを共有すると、次のようなメリットがあります。

- VMware Distributed Resource Scheduling (DRS) および VMware High Availability (HA) を使用できます。

仮想マシンを複数の物理サーバに分散できます。つまり、各サーバ上で複数の仮想マシンを実行できるため、同時に同じ領域に大きな負荷が集中することがなくなります。サーバに障害が発生しても、別の物理サーバ上で仮想マシンを再起動できます。障害が発生すると、各仮想マシンのオンディスク ロックは解除されます。

VMware DRS の詳細については、『vSphere リソース管理』ドキュメントを参照してください。VMware HA の詳細については、『vSphere 可用性ガイド』ドキュメントを参照してください。

- vMotion を使用して、稼働中の仮想マシンを物理サーバ間で移行できます。仮想マシンの移行の詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。

共有データストアを作成するには、データストアへのアクセスが必要な ESXi ホストにデータストアをマウントします。 [データストアのマウント](#)を参照してください。

## VMFS メタデータ アップデート

VMFS データストアは、仮想マシンのファイル、ディレクトリ、シンボリック リンク、RDM 記述子ファイルなどを保持します。また、データストアは、これらのオブジェクトに関するすべてのマッピング情報について、一貫した表示を維持します。このマッピング情報は、メタデータと呼ばれます。

メタデータは、データストアまたは仮想マシンの管理操作を実行するたびに更新されます。メタデータの更新が必要となる操作の例を次に示します。

- 仮想マシンのファイルの作成、増大、ロック
- ファイル属性の変更

- 仮想マシンのパワーオンまたはパワーオフ
- VMFS データストアの作成または削除
- VMFS データストアの拡張
- テンプレートの作成
- テンプレートからの仮想マシンのデプロイ
- vMotion での仮想マシンの移行

共有ストレージ環境でメタデータが変更されると、VMFS は特別なロック メカニズムを使用して、データを保護し、メタデータへの書き込みが複数のホストで同時に行われないようにします。

## VMFS のロック メカニズム

共有ストレージ環境では、複数のホストが同じ VMFS データストアにアクセスすると、特定のロック メカニズムが使用されます。これらのロック メカニズムは、複数のホストによるメタデータへの同時書き込みを防ぎ、データ破損の発生を阻止します。

基礎となるストレージの構成とタイプに応じて、VMFS データストアはアトミック テストだけを使用してロック メカニズム（ATS のみ）を設定するか、ATS 予約と SCSI 予約の組み合わせ (ATS+SCSI) を使用できます。

### ATS のみのメカニズム

T10 標準ベースの VAAI 仕様をサポートするストレージ デバイスの場合、VMFS は Hardware Assisted Locking と呼ばれる ATS ロックを使用します。この ATS アルゴリズムでは、ディスク セクタ単位での異なるロックに対応します。基礎となるストレージが ATS のみのメカニズムをサポートしている場合は、新しくフォーマットされたすべての VMFS5 データストアは ATS のみのメカニズムを使用し、SCSI 予約は使用しません。

ATS が使用されるマルチ エクステンツ データストアを作成した場合、vCenter Server は ATS 以外のデバイスを除外します。このフィルタリングによって、ATS プリミティブをサポートするデバイスのみを使用できるようになります。

場合によっては、VMFS5 データストアに対して ATS のみの設定をオフにする必要があります。詳細については、[ロック メカニズムの ATS+SCSI への変更](#) を参照してください。

### ATS+SCSI メカニズム

ATS+SCSI メカニズムをサポートする VMFS データストアは、ATS を使用するように構成され、可能な場合は ATS を使用します。ATS が失敗すると、VMFS データストアは SCSI 予約に戻ります。ATS ロックとは対照的に、SCSI 予約では、メタデータの保護を必要とする操作を実行しているときに、ストレージ デバイス全体がロックされます。操作が完了すると、VMFS により予約が解放され、ほかの操作を続行できます。

ATS+SCSI メカニズムを使用するデータストアには、VMFS3 からアップグレードされた VMFS5 データストアがあります。また ATS をサポートしないストレージ デバイス上の新しい VMFS5 データストアも、ATS+SCSI メカニズムを使用します。

VMFS データストアが SCSI 予約に戻ると、過剰な SCSI 予約によりパフォーマンスの低下が発生する場合があります。SCSI 予約を低減する方法については、『vSphere トラブルシューティング』ドキュメントを参照してください。

## VMFS ロック情報の表示

VMFS データストアが使用するロック メカニズムに関する情報を取得するには、`esxcli` コマンドを使用します。

手順中、`--server=server_name` で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

- ◆ VMFS ロック メカニズムに関する情報を表示するには、次のコマンドを実行します。

```
esxcli --server=server_name storage vmfs lockmode list
```

### 結果

次の表に、コマンドの出力に含まれる項目を一覧表示します。

表 16-2. VMFS ロック情報

フィールド	値	説明
ロック モード		データストアのロック構成を示します。
	ATS のみ	データストアは ATS のみを使用するように構成されています。
	ATS+SCSI	データストアは ATS を使用するように構成されていますが、ATS でエラーが発生するか、ATS がサポートされていない場合は、SCSI に戻ることができます。
	ATS アップグレードを保留中	データストアは、ATS のみへのオンライン アップグレードを進行中です。
	ATS ダウングレードを保留中	データストアは、ATS+SCSI へのオンライン ダウングレードを進行中です。
ATS 互換		データストアを ATS のみに構成できるかどうかを示します。
ATS アップグレード モード		データストアがサポートするアップグレードのタイプを示します。
	なし	データストアは ATS のみとの互換性がありません。
	オンライン	ATS のみへのアップグレード中にデータストアを使用できます。

表 16-2. VMFS ロック情報（続き）

フィールド	値	説明
	オフライン	ATS のみへのアップグレード中にデータストアを使用できません。
ATS 非互換の理由		データストアが ATS のみと互換性がない場合は、非互換の理由を示します。

## ATS のみへの VMFS ロックの変更

VMFS5 データストアで ATS+SCSI ロック メカニズムを使用する場合は、ATS のみのロックに変更することができます。

通常、VMFS3 からアップグレードされた VMFS5 データストアでは、ATS+SCSI ロック メカニズムを使用します。データストアは、ATS が有効なハードウェアにデプロイされている場合、通常は ATS のみのロックへのアップグレードで使用可能です。vSphere 環境に応じて、次のアップグレード モードのいずれかを使用できます。

- ATS のみへのオンライン アップグレードは、ほとんどの単一のエクステント VMFS5 データストアで使用できます。ホストのいずれかでオンライン アップグレードを実行する間、その他のホストはそのデータストアを使用し続けることができます。
- ATS のみへのオフライン アップグレードは、複数の物理エクステントをまたぐ VMFS5 データストアで使用する必要があります。複数のエクステントで構成されるデータストアは、オンライン アップグレードでは使用できません。これらのデータストアでは、アップグレードの要求時に、どのホストもデータストアをアクティブに使用しないようにする必要があります。

### 手順

#### 1 ATS のみへのアップグレードを開始する前に

ATS のみのロックへオンラインまたはオフライン アップグレードするための環境を準備するには、いくつかの手順を実行する必要があります。

#### 2 ロック メカニズムの ATS のみへのアップグレード

VMFS データストアの互換性が ATS のみの場合は、ATS+SCSI から ATS のみにロック メカニズムをアップグレードできます。

### ATS のみへのアップグレードを開始する前に

ATS のみのロックへオンラインまたはオフライン アップグレードするための環境を準備するには、いくつかの手順を実行する必要があります。

### 手順

- 1 VMFS5 データストアにアクセスするすべてのホストを、最新バージョンの vSphere にアップグレードします。

- 2 `esxcli storage vmfs lockmode list` コマンドを実行して、データストアが、現在のロック メカニズムのアップグレード対象であるかどうかを判断します。

次の出力フィールドの例では、データストアがアップグレード対象であることを示し、現在のロック メカニズムと、データストアで利用できるアップグレード モードを表示しています。

```
Locking Mode   ATS Compatible   ATS Upgrade Modes-----
-----ATS+SCSI           true           Online or Offline
```

- 3 データストアで利用できるアップグレード モードに応じて、次のアクションのいずれかを実行します。

アップグレード モード	アクション
オンライン	すべてのホストに、VMFS データストアへの一貫したストレージ接続があることを確認します。
オフライン	データストアをアクティブに使用しているホストが存在しないことを確認します。

### ロック メカニズムの ATS のみへのアップグレード

VMFS データストアの互換性が ATS のみの場合は、ATS+SCSI から ATS のみにロック メカニズムをアップグレードできます。

複数のエクステンツをまたぐことのないほとんどのデータストアは、オンライン アップグレードで使用可能です。ESXi ホストのいずれかでオンライン アップグレードを実行する間、その他のホストはデータストアを使用し続けることができます。オンライン アップグレードは、すべてのホストでデータストアを閉じた後にのみ完了します。

#### 前提条件

データストアをメンテナンス モードにすることによってロック メカニズムのアップグレードを完了する予定の場合は、Storage DRS を無効にします。前提条件は、オンライン アップグレードにのみ適用されます。

#### 手順

- 1 次のコマンドを実行することにより、ロック メカニズムのアップグレードを実行します。

```
esxcli storage vmfs lockmode set -a|--ats -l|--volume-label= VMFS label -u|--volume-uuid= VMFS UUID
```

## 2 オンライン アップグレードの場合は、追加の手順を実行します。

- a データストアにアクセスすることができるすべてのホストでデータストアを閉じ、ホストで変更を認識できるようにします。

次の方法のいずれかを使用できます。

- データストアをアンマウントおよびマウントします。
- データストアをメンテナンス モードにしてから、メンテナンス モードを終了します。

- b 次のコマンドを実行して、データストアのロック モード ステータスが ATS のみに変更されたことを確認します。

```
esxcli storage vmfs lockmode list
```

- c ロック モードが、ATS UPGRADE PENDING などの別のステータスで表示された場合は、次のコマンドを実行して、アップグレードをまだ処理していないホストを調べます。

```
esxcli storage vmfs host list
```

## ロック メカニズムの ATS+SCSI への変更

アトミック テスト アンド セット (ATS) のロックをサポートするデバイスで VMFS5 データストアを作成する場合、データストアは ATS 専用ロック メカニズムを使用するように設定されます。特定の状況では、ATS 専用ロックを ATS+SCSI にダウングレードにすることが必要になります。

ストレージ デバイスがダウングレードされた場合、ファームウェアの更新に失敗した場合、デバイスで ATS がサポートされなくなった場合などに ATS+SCSI ロック メカニズムに切り替える必要があります。

ダウングレード プロセスは、ATS 専用アップグレードと似ています。アップグレードと同様に、ストレージ構成に応じて、オンライン モードまたはオフライン モードでダウングレードを実行できます。

### 手順

- 1 次のコマンドを実行して、ロック メカニズムを ATS+SCSI に変更します。

```
esxcli storage vmfs lockmode set -s|--scsi -l|--volume-label= VMFS label
-u|--volume-uuid= VMFS UUID
```

- 2 オンライン モードの場合、ホストで変更を認識できるように、データストアへのアクセス権があるすべてのホストでデータストアを終了します。

## ネットワーク ファイル システム データストアについて

ESXi に組み込まれた NFS クライアントは、TCP/IP 接続で NFS (Network File System) プロトコルを使用して、NAS サーバ上に存在する指定された NFS ボリュームにアクセスします。ESXi ホストは、そのボリュームをマウントし、ストレージとして使用することができます。vSphere では、NFS プロトコルのバージョン 3 および 4.1 をサポートしています。

通常、NFS ボリュームまたはディレクトリは、ストレージ管理者によって作成され、NFS サーバからエクスポートされます。NFS ボリュームは、VMFS などのローカル ファイル システムによってフォーマットする必要はありません。ボリュームを ESXi ホストに直接マウントし、VMFS データストアを使用する場合と同じ方法で仮想マシンを保存および起動できます。



NFS は、NFS データストアに仮想ディスクを格納するほかに、ISO イメージや仮想マシンのテンプレートなどの中央リポジトリとして使用できます。ISO イメージ用のデータストアを使用する場合は、仮想マシンの CD-ROM デバイスをデータストアの ISO ファイルに接続し、ISO ファイルからゲスト OS をインストールできます。

ESXi は、ほとんどの NFS ボリュームで次のストレージ機能をサポートしています。

- vMotion および Storage vMotion
- High Availability (HA) および Distributed Resource Scheduler (DRS)
- Fault Tolerance (FT) およびホスト プロファイル

---

**注：** NFS 4.1 では、レガシー Fault Tolerance をサポートしません。

---

- 仮想マシンに CD-ROM として表示される ISO イメージ
- 仮想マシンのスナップショット
- 大容量の仮想ディスク、または 2TB を超えるディスクを持つ仮想マシン。NFS データストアに作成される仮想ディスクは、領域の予約操作をサポートするハードウェア アクセラレーションを使用している場合を除いて、デフォルトでシン プロビジョニングされます。NFS 4.1 では、ハードウェア アクセラレーションはサポートされていません。詳細については、[NAS デバイスでのハードウェア アクセラレーション](#) を参照してください。

## NFS ストレージのガイドラインと要件

NFS ストレージを使用する場合、次の固有の構成、ネットワーク、および NFS データストア ガイドラインに従う必要があります。

### NFS サーバ構成ガイドライン

- 使用する NFS サーバが『VMware HCL』に記載されていることを確認します。サーバ ファームウェアの正しいバージョンを使用します。
- NFS ストレージを構成する場合、ストレージ ベンダーの推奨事項に従います。
- NFS ボリュームが NFS over TCP を使用してエクスポートされていることを確認します。
- NFS サーバが NFS 3 または NFS 4.1 として特定の共有をエクスポートするが、同じ共有に両方のプロトコルバージョンを提供していないことを確認します。ESXi では、異なる NFS バージョンで同じ共有をマウントできるため、サーバでこのポリシーを適用する必要があります。
- NFS 3 および非 Kerberos NFS 4.1 は、root 以外の認証情報を使用して NFS ボリュームにアクセスできるようにするデリゲート ユーザー機能をサポートしていません。NFS 3 または非 Kerberos NFS 4.1 を使用する場合、各ホストにボリュームへの root アクセス権があることを確認します。この機能を有効にする方法はストレージ ベンダーごとに異なりますが、NAS サーバで `no_root_squash` オプションを使用して行う方法が一般的です。NAS サーバから root アクセス権が付与されていない場合でも、NFS データストアをホストにマウントできます。ただし、そのデータストア上に仮想マシンを作成することはできません。
- ファイルが格納される基盤となる NFS ボリュームが読み取り専用の場合は、そのボリュームが NFS サーバによって読み取り専用の共有としてエクスポートされていることを確認するか、そのボリュームを ESXi ホスト上の読み取り専用のデータストアとして構成します。それ以外の場合、ホストはデータストアが読み取り/書き込み可能であると認識し、ファイルを開くことができない可能性があります。

## NFS ネットワーク ガイドライン

- ネットワーク接続するには、ホストで標準ネットワーク アダプタが必要です。
- ESXi は、レイヤー 2 およびレイヤー 3 ネットワーク スイッチをサポートしています。レイヤー 3 スイッチを使用する場合、ESXi ホストと NFS ストレージ アレイのサブネットは異なっている必要があります。ネットワーク スイッチでルーティング情報を処理する必要があります。
- NFS ストレージには VMkernel ポート グループが必要です。すでに存在している仮想スイッチ (vSwitch) に、または新しい vSwitch の構成時に IP ストレージの新しい VMkernel ポート グループを作成できます。vSwitch は、vSphere 標準スイッチ (VSS) または vSphere Distributed Switch (VDS) になります。
- NFS トラフィックに複数のポートを使用する場合、仮想スイッチと物理スイッチを正しく構成していることを確認します。詳細については、『vSphere ネットワーク』ドキュメントを参照してください。
- NFS 3 と非 Kerberos NFS 4.1 は、IPv4 と IPv6 をサポートします。

## NFS データストア ガイドライン

- NFS 4.1 を使用するには、vSphere 環境をバージョン 6.x にアップグレードします。バージョン 4.1 をサポートしていないホストに NFS 4.1 データストアをマウントすることはできません。
- 異なる NFS バージョンを使用して、同じデータストアをマウントすることはできません。NFS 3 クライアントと NFS 4.1 クライアントで使用するロック プロトコルは異なります。そのため、互換性のない 2 つのクライアントから同じ仮想ディスクにアクセスすると、不適切な動作やデータの破損が発生する可能性があります。
- NFS 3 と NFS 4.1 のデータストアは同じホスト上に共存できます。
- vSphere は、NFS バージョン 3 からバージョン 4.1 へのデータストアのアップグレードをサポートしていません。
- 異なるホスト上で同じ NFS 3 ボリュームをマウントする場合、サーバ名とフォルダ名がホスト間で同一であることを確認してください。名前が一致しない場合、ホストは同じ NFS バージョン 3 ボリュームを 2 つの異なるデータストアと見なします。このエラーによって、vMotion などの機能が失敗する場合があります。たとえば、1 つのホストでサーバ名を「filer」と入力し、別のホストで「filer.domain.com」と入力した場合に、このような不一致が見られます。このガイドラインは NFS バージョン 4.1 には適用されません。
- ASCII 以外の文字を使用してデータストアと仮想マシンに命名する場合には、基盤となる NFS サーバが国際化サポートを提供することを確認します。サーバが国際文字をサポートしない場合には、ASCII 文字のみを使用します。そうでないと、予測できない障害が発生する場合があります。

## NFS プロトコルと ESXi

ESXi は、NFS プロトコルのバージョン 3 および 4.1 をサポートしています。両方のバージョンをサポートするため、ESXi は 2 つの異なる NFS クライアントを使用します。

## NFS プロトコル バージョン 3

vSphere は、TCP で NFS バージョン 3 をサポートしています。このバージョンを使用する場合には、次の考慮事項が適用されます。

- NFS バージョン 3 を使用する場合、ストレージ トラフィックは暗号化されない形式で LAN 内を転送されます。このセキュリティ上の制約があるため、信頼できるネットワークでのみ NFS ストレージを使用し、トラフィックを別々の物理スイッチ上で隔離します。プライベート VLAN を使用することもできます。
- NFS 3 では、I/O で 1 つの TCP 接続のみを使用します。そのため、ESXi は NFS サーバの 1 つの IP アドレスまたはホスト名での I/O のみをサポートしており、複数のパスをサポートしていません。ネットワークのインフラストラクチャおよび構成に応じて、ネットワーク スタックを使用してストレージ ターゲットへの複数の接続を構成することができます。この場合は複数のデータストアを使用し、各データストアでは、ホストとストレージの間に別々のネットワーク接続を使用する必要があります。
- NFS 3 を使用する場合、ESXi では、root 以外の認証情報を使用して NFS ボリュームにアクセスできるようにするデリゲート ユーザー機能をサポートしていません。必ず、各ホストにボリュームへの root アクセス権があるようにする必要があります。
- NFS 3 ではハードウェア アクセラレーションがサポートされており、これによりホストでは、NAS デバイスと統合し、NAS ストレージが提供するいくつかのハードウェア操作を使用できます。詳細については、[NAS デバイスでのハードウェア アクセラレーション](#) を参照してください。
- ハードウェア アクセラレーションがサポートされている場合は、NFS 3 データストアにシック プロビジョニングされた仮想ディスクを作成できます。
- ESXi の NFS 3 ロックでは、ネットワーク ロック マネージャ (NLM) プロトコルを使用しません。代わりに VMware は、独自のロック プロトコルを使用できるようにしています。NFS 3 ロックは、NFS サーバでロック ファイルを作成することによって実装されます。ロック ファイルには、`.lck-file_id.` という名前が付けられます。

## NFS プロトコル バージョン 4.1

NFS 4.1 を使用する場合は、次の考慮事項が適用されます。

- NFS 4.1 では、セッション トランクをサポートするサーバの場合にマルチパスを使用できます。トランク機能が使用可能な場合は、複数の IP アドレスを使用して 1 つの NFS ボリュームにアクセスすることができます。クライアント ID トランクはサポートされていません。
- NFS 4.1 では、ハードウェア アクセラレーションはサポートされていません。この制限のため、NFS 4.1 データストアでシック仮想ディスクを作成することはできません。
- NFS 4.1 では、NFS サーバとの通信の安全性を確保するため、Kerberos 認証プロトコルがサポートされています。詳細については、[NFS 4.1 用 Kerberos 認証情報の使用](#) を参照してください。
- NFS 4.1 では、ロック メカニズムとして共有の予約を使用します。
- NFS 4.1 では、組み込みのファイル ロックがサポートされています。
- NFS 4.1 では、Kerberos と併用される場合に、root 以外のユーザーのファイルへのアクセスがサポートされています。

- NFS 4.1 では、従来の Kerberos 以外のマウントがサポートされています。この場合は、NFS バージョン 3 の場合に推奨されるセキュリティおよび root アクセス権のガイドラインに従ってください。
- AUTH\_SYS と Kerberos の同時マウントはサポートされていません。
- NFS 4.1 と Kerberos の組み合わせでは IPv6 がサポートされません。NFS 4.1 と AUTH\_SYS の組み合わせでは、IPv4 と IPv6 の両方がサポートされます。

## NFS プロトコルと vSphere ソリューション

vSphere 機能	NFS バージョン 3	NFS バージョン 4.1
vMotion および Storage vMotion	はい	はい
High Availability (HA)	はい	はい
フォールトトレランス (FT)	はい	はい
DRS (Distributed Resource Scheduler)	はい	はい
ホスト プロファイル	はい	はい
ストレージ DRS	はい	いいえ
Storage I/O Control	はい	いいえ
Site Recovery Manager	はい	いいえ
仮想ボリューム	はい	いいえ

## NFS バージョンのアップグレード

vSphere では、NFS バージョン 3 から NFS 4.1 への自動データストア変換がサポートされていません。NFS 3 データストアをアップグレードする場合は、次のオプションを選択できます。

- 新しい NFS 4.1 データストアを作成してから、Storage vMotion を使用して古いデータストアから新しいデータストアに仮想マシンを移行することができます。
- NFS ストレージ サーバによって提供される変換方式を使用します。詳細については、ストレージベンダーにお問い合わせください。
- 1 つのバージョンからアンマウントし、次に別のバージョンとしてマウントします。

**注意：** このオプションを使用する場合は、データストアにアクセスできるすべてのホストから確実にデータストアをアンマウントしてください。データストアは、同時に両方のプロトコルを使用してマウントすることはできません。

## NFS ストレージのファイアウォール構成

ESXi では、管理インターフェイスとネットワークの間にファイアウォールが含まれています。このファイアウォールはデフォルトで有効になっています。インストール時、ESXi ファイアウォールは、NFS などのデフォルトサービスのトラフィック以外の受信トラフィックと送信トラフィックをブロックするように構成されています。

NFS を含むサポート対象サービスについては、ESXi ファイアウォールのディレクトリ `/etc/vmware/firewall/` にあるルール セットの構成ファイルに記述されています。このファイルにはファイアウォールのルールが含まれているほか、各ルールについてのポートおよびプロトコルとの関係が記述されています。

NFS クライアントのルール セット (`nfsClient`) の動作は、ほかのルール セットとは異なります。NFS クライアントのルール セットが有効な場合、すべての送信 TCP ポートは、許可された IP アドレス一覧のターゲット ホストに対して開かれます。

NFS 4.1 のルール セットは、接続バージョン 4.1 プロトコルの仕様で指名されているターゲット ポート 2049 への発信接続を開きます。この発信接続は、最初のマウント時にすべての IP アドレスに対して開きます。このポートは、ESXi ホストが再起動されるまで開いたままになります。

ファイアウォール構成の詳細については、『vSphere セキュリティ』ドキュメントを参照してください。

## NFS クライアント ファイアウォールの動作

NFS クライアントのファイアウォール ルール セットの動作は、他の ESXi ファイアウォール ルール セットとは異なります。ESXi では、NFS データストアをマウントまたはアンマウントするときに NFS クライアント設定が構成されます。動作は、NFS のバージョンによって異なります。

NFS データストアの追加、マウント、アンマウントを行ったときの動作は、NFS のバージョンによって異なります。

### NFS v3 ファイアウォールの動作

NFS v3 データストアを追加またはマウントする際、ESXi は、NFS クライアント (`nfsClient`) のファイアウォール ルール セットの状態を確認します。

- `nfsClient` のルール セットが無効な場合、ESXi はこのルール セットを有効にし、`allowedAll` フラグを `FALSE` に設定することで、すべての IP アドレスを許可するポリシーを無効にします。NFS サーバの IP アドレスが発信 IP アドレスの許可リストに追加されます。
- `nfsClient` のルール セットが有効な場合、ルール セットの状態と、許可される IP アドレスのポリシーは変更されません。NFS サーバの IP アドレスが発信 IP アドレスの許可リストに追加されます。

**注：** `nfsClient` のルール セットを手動で有効にするか、すべての IP アドレスを許可するポリシーを手動で設定すると、NFS v3 データストアをシステムに追加する前または後で、以前の NFS v3 データストアがアンマウントされる際に設定がオーバーライドされます。すべての v3 NFS データストアがアンマウントされると、`nfsClient` のルール セットは無効になります。

NFS v3 データストアを削除またはアンマウントすると、ESXi によって次のいずれかの操作が実行されます。

- 残りの NFS v3 データストアのいずれもアンマウントされるデータストアのサーバからマウントされない場合、ESXi はサーバの IP アドレスを発信 IP アドレスのリストから削除します。
- アンマウント操作後にマウントされている NFS v3 データストアが残っていない場合、ESXi は、`nfsClient` ファイアウォール ルール セットを無効にします。

## NFS v4.1 ファイアウォールの動作

最初の NFS v4.1 データストアをマウントすると、ESXi は `nfs41client` のルール セットを有効にし、`allowedAll` フラグを `TRUE` に設定します。この操作により、すべての IP アドレスに対してポート 2049 が開きます。NFS v4.1 データストアをアンマウントしても、ファイアウォールの状態には影響しません。つまり、最初の NFS v4.1 のマウントでポート 2049 が開き、そのポートは、明示的に閉じられない限り、有効な状態を維持します。

## NFS クライアントのファイアウォール ポートの確認

ESXi は、NFS ストレージへのアクセスを有効にするために、ユーザーが NFS データストアをマウントするときに自動的に NFS クライアントのファイアウォール ポートを開きます。トラブルシューティングのために、ポートが開いていることを確認しなければならない場合があります。

### 手順

- 1 vSphere Web Client で、ESXi ホストを選択します。
- 2 [管理] タブをクリックし、[設定] をクリックします。
- 3 [システム] 領域で [セキュリティ プロファイル] を選択し、[編集] をクリックします。
- 4 適切なバージョンの NFS までスクロール ダウンし、ポートが開いていることを確認します。

## NFS ストレージにアクセスするためのレイヤー 3 のルート設定された接続

レイヤー 3 (L3) のルート設定された接続を使用して NFS ストレージにアクセスする場合は、特定の要件および制約を検討してください。

環境が次の要件を満たしていることを確認します。

- IP ルータで Cisco のホット スタンバイ ルータ プロトコル (HSRP) を使用してください。Cisco 以外のルータを使用している場合は、替わりに仮想ルータ冗長プロトコル (VRRP) を使用していることを確認してください。
- サービスの品質 (QoS) を使用し、バンド幅が制限されているネットワーク、あるいは輻輳を経験しているネットワーク上の NFS L3 トラフィックを優先順位付けしてください。詳細については、お使いのルータのドキュメントを参照してください。
- ストレージ ベンダーによって推奨される経路指定された NFS L3 のベスト プラクティスに従ってください。詳細については、ストレージ ベンダーにお問い合わせください。
- ネットワーク I/O リソース管理 (NetIORM) を無効にしてください。
- トップオブラック スイッチあるいはスイッチ依存の I/O デバイス パーティショニングを使用する予定がある場合は、互換性とサポートについてシステム ベンダーにお問い合わせください。

L3 環境では、以下の制限が適用されます。

- この環境は VMware Site Recovery Manager をサポートしません。
- この環境は NFS プロトコルのみをサポートします。同じ物理ネットワーク上で FCoE などの他のストレージ プロトコルを使用しないでください。
- この環境の NFS トラフィックは IPv6 をサポートしません。

- この環境の NFS トラフィックは LAN 上でのみ経路指定することができます。WAN などのその他の環境はサポートされていません。

## NFS ストレージ環境のセットアップ

vSphere で NFS データストアをマウントする前に、いくつかの構成手順を実行する必要があります。

### 前提条件

- [NFS ストレージのガイドラインと要件](#)にあるガイドラインについて理解しておく必要があります。
- NFS ストレージの構成方法の詳細については、ストレージ ベンダーのドキュメントを参照してください。

### 手順

- 1 NFS サーバで、NFS ポリュームを構成し、エクスポートして ESXi ホストにマウントします。
  - a NFS サーバの IP アドレスまたは DNS 名、および NFS 共有のフル パスまたはフォルダ名を書き留めます。

NFS 4.1 の場合は、複数の IP アドレスまたは DNS 名を収集して、NFS 4.1 データストアで提供されるマルチパス サポートを利用できます。NFS 3 と非 Kerberos NFS 4.1 は、IPv4 および IPv6 アドレスをサポートします。
  - b NFS 4.1 で Kerberos 認証を使用する場合は、ESXi が認証処理で Kerberos 認証情報を使用するように指定します。

- 2 各 ESXi ホストで、NFS トラフィックの VMkernel ネットワーク ポートを構成します。

詳細については、『vSphere ネットワーク』ドキュメントを参照してください。

- 3 NFS 4.1 データストアで Kerberos 認証を使用する場合は、Kerberos 認証を使用するように ESXi ホストを構成します。

このデータストアをマウントする各ホストが Active Directory ドメインの一部になっており、その NFS 認証の認証情報が設定されていることを確認します。

### 次のステップ

これで、ESXi ホストで NFS データストアを作成できます。

## NFS 4.1 用 Kerberos 認証情報の使用

NFS バージョン 4.1 を使用する場合、ESXi は Kerberos 認証メカニズムをサポートします。

Kerberos は認証サービスの 1 つで、これにより ESXi にインストールされている NFS 4.1 クライアントは、NFS 共有をマウントする前に、NFS サーバに対してその ID を証明することができます。Kerberos では、セキュリティ保護のないネットワーク接続で使用できるよう暗号化を使用します。NFS 4.1 用の Kerberos の vSphere 実装では、クライアントおよびサーバの実在性認証のみをサポートしており、データの整合性サービスや機密保持サービスは提供しません。



Kerberos 認証を使用する場合は、次の考慮事項が適用されます。

- ESXi は、Active Directory ドメインおよび Key Distribution Center (KDC) で Kerberos バージョン 5 を使用します。
- vSphere 管理者として Active Directory 認証情報を指定し、NFS ユーザーが NFS 4.1 Kerberos データストアにアクセスできるようにします。認証情報の単一セットを使用して、そのホストにマウントされているすべての Kerberos データストアにアクセスします。
- 複数の ESXi ホストが同じ NFS 4.1 データストアを共有する場合は、共有データストアにアクセスするすべてのホストで同じ Active Directory 認証情報を使用する必要があります。この動作は、ホスト プロファイルでユーザーを設定し、すべての ESXi ホストにプロファイルを適用することによって、自動化することができます。
- NFS 4.1 は、AUTH\_SYS と Kerberos の同時マウントをサポートしていません。
- NFS 4.1 と Kerberos の組み合わせでは IPv6 がサポートされません。IPv4 のみがサポートされています。

## Kerberos 認証用 ESXi ホストの構成

NFS 4.1 と Kerberos を組み合わせて使用する場合、いくつかのタスクを実行して Kerberos 認証用のホストを設定する必要があります。

複数の ESXi ホストが同じ NFS 4.1 データストアを共有する場合は、共有データストアにアクセスするすべてのホストで同じ Active Directory 認証情報を使用する必要があります。この動作は、ホスト プロファイルでユーザーを設定し、すべての ESXi ホストにプロファイルを適用することによって、自動化することができます。

### 前提条件

- Kerberos を使用するように Microsoft Active Directory (AD) および NFS サーバが構成されていることを確認します。
- AD で DES-CBC-MD5 暗号化モードを有効にします。NFS 4.1 クライアントでは、この暗号化モードのみがサポートされています。
- Kerberos ユーザーにフル アクセスを付与するように NFS サーバのエクスポートが構成されていることを確認します。

### 手順

#### 1 Kerberos を使用する NFS 4.1 用 DNS の構成

Kerberos と NFS 4.1 を組み合わせて使用する場合、Kerberos Key Distribution Center (KDC) の DNS レコードを配布するように構成された DNS サーバを参照するように、ESXi ホストの DNS 設定を変更する必要があります。たとえば、Active Directory が DNS サーバとして使用されている場合、AD サーバのアドレスを使用します。

#### 2 Kerberos を使用する NFS 4.1 用 Network Time Protocol の構成

Kerberos で NFS 4.1 を使用する場合は、ネットワーク時間プロトコル (NTP) を構成して、vSphere ネットワークのすべての ESXi ホストが確実に同期されるようにします。



### 3 Active Directory での Kerberos 認証の有効化

Kerberos が使用可能な NFS 4.1 を使用する場合は、各 ESXi ホストを Active Directory ドメインに追加し、Kerberos 認証を有効化することができます。Kerberos では、Active Directory との統合によって Single Sign-On が有効化され、セキュリティ保護のないネットワーク接続で使用されるときに追加のセキュリティ レイヤーを提供します。

#### 次のステップ

Kerberos のホストを構成すると、Kerberos 対応の NFS 4.1 データストアを作成できます。

#### Kerberos を使用する NFS 4.1 用 DNS の構成

Kerberos と NFS 4.1 を組み合わせて使用する場合、Kerberos Key Distribution Center (KDC) の DNS レコードを配布するように構成された DNS サーバを参照するように、ESXi ホストの DNS 設定を変更する必要があります。たとえば、Active Directory が DNS サーバとして使用されている場合、AD サーバのアドレスを使用します。

#### 手順

- 1 vSphere Web Client で、ホストに移動します。
- 2 [管理] タブをクリックし、[ネットワーク] をクリックして、[TCP/IP 構成] を選択します。
- 3 [TCP/IP 構成] を選択し、[編集] アイコンをクリックします。
- 4 DNS 設定情報を入力します。

オプション	説明
ドメイン	AD ドメイン名
優先 DNS サーバ	AD サーバ IP
ドメインの検索	AD ドメイン名

#### Kerberos を使用する NFS 4.1 用 Network Time Protocol の構成

Kerberos で NFS 4.1 を使用する場合は、ネットワーク時間プロトコル (NTP) を構成して、vSphere ネットワークのすべての ESXi ホストが確実に同期されるようにします。

#### 手順

- 1 vSphere インベントリでホストを選択します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] セクションで、[時間の構成] を選択します。
- 4 [編集] をクリックし、NTP サーバを設定します。
  - a [Network Time Protocol を使用 (NTP クライアントの有効化)] を選択します。
  - b NTP サービス起動ポリシーを設定します。
  - c 同期する NTP サーバの IP アドレスを入力します。
  - d [NTP サービス ステータス] セクションで [起動] または [再起動] をクリックします。

## 5 [[OK]] をクリックします。

ホストが NTP サーバと同期します。

### Active Directory での Kerberos 認証の有効化

Kerberos が使用可能な NFS 4.1 を使用する場合は、各 ESXi ホストを Active Directory ドメインに追加し、Kerberos 認証を有効化することができます。Kerberos では、Active Directory との統合によって Single Sign-On が有効化され、セキュリティ保護のないネットワーク接続で使用されるときに追加のセキュリティ レイヤーを提供します。

#### 前提条件

ホストをドメインに追加する権限により、AD ドメインおよびドメイン管理者アカウントを設定します。

#### 手順

- 1 ESXi ホストを Active Directory ドメインに追加します。
  - a vSphere Web Client で、ESXi ホストを選択します。
  - b [管理] タブをクリックして、[設定] をクリックします。
  - c [システム] で、[認証サービス] を選択します。
  - d [ドメインへの参加] をクリックし、ドメイン設定を入力して [OK] をクリックします。

ディレクトリ サービスのタイプが Active Directory に変更されます。

- 2 NFS Kerberos ユーザーの認証情報を構成または編集します。
  - a [NFS Kerberos 認証情報] で、[編集] をクリックします。
  - b ユーザー名とパスワードを入力します。

すべての Kerberos データストアに保存されているファイルには、これらの認証情報を使用してアクセスします。

NFS Kerberos 認証情報の状態が [有効] に変わります。

## データストアの作成

新しいデータストア ウィザードを使用して、データストアを作成します。使用中の環境にあるストレージのタイプおよびストレージの要件に応じて、VMFS、NFS または仮想データストアを作成できます。

Virtual SAN データストアは、Virtual SAN を有効にすると自動的に作成されます。詳細については、『VMware Virtual SAN の管理』ドキュメントを参照してください。

新しいデータストア ウィザードを使用して、VMFS データストアのコピーを管理することもできます。

### ■ VMFS データストアの作成

VMFS データストアは、仮想マシンのリポジトリとして機能します。ファイバ チャネル、iSCSI、およびローカル ストレージ デバイスなど、ホストが検出する SCSI ベースのストレージ デバイス上に、VMFS データストアを設定できます。

## ■ NFS データストアの作成

[新しいデータストア] ウィザードを使用すると、NFS ボリュームをマウントできます。

## ■ 仮想データストアの作成

[新しいデータストア] ウィザードを使用して、仮想データストアを作成します。

# VMFS データストアの作成

VMFS データストアは、仮想マシンのリポジトリとして機能します。ファイバ チャネル、iSCSI、およびローカルストレージ デバイスなど、ホストが検出する SCSI ベースのストレージ デバイス上に、VMFS データストアを設定できます。

**注：** VMFS3 データストアを vSphere 6.x に作成することはできません。既存の VMFS3 データストアが引き続き利用可能で利用できるであっても、それらを VMFS5 にアップグレードする必要があります。

## 前提条件

ストレージに必要なアダプタをインストールおよび構成する必要があります。アダプタを再スキャンして、新しく追加されたストレージ デバイスを検出します。

## 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 [新規データストア] アイコンをクリックします。
- 3 データストア名を入力し、必要に応じてデータストアの配置場所を選択します。  
vSphere Web Client ではデータストア名が強制的に 42 文字に制限されます。
- 4 データストア タイプに VMFS を選択します。
- 5 データストアに使用するデバイスを選択します。

**重要：** 選択するデバイスは、[スナップショット ボリューム] 列に値が表示されていない必要があります。値が表示されている場合、デバイスには既存の VMFS データストアのコピーが含まれています。データストアのコピーの管理については、[重複 VMFS データストアの管理](#)を参照してください。

- 6 パーティション構成を指定します。

オプション	説明
すべての利用可能なパーティションを利用	ディスク全体を 1 つの VMFS データストア専用にしします。このオプションを選択すると、現在このデバイスに保存されているすべてのファイル システムやデータは消去されます。
空き容量の使用	ディスクの残りの空き容量に VMFS データストアをデプロイします。

- 7 (オプション) データストアに割り当てられた容量が大きすぎる場合は、[データストア サイズ] フィールドで容量の値を調整します。

デフォルトでは、ストレージ デバイスの空き容量がすべて割り当てられます。

- 8 [設定の確認] ページで、データストア構成情報を確認し、[終了] をクリックします。

## 結果

SCSI ベースのストレージ デバイス上にデータストアが作成されます。デバイスへのアクセス権を持つすべてのホストがそれを使用できます。

## NFS データストアの作成

[新しいデータストア] ウィザードを使用すると、NFS ボリュームをマウントできます。

### 前提条件

- NFS ストレージ環境を設定します。
- NFS 4.1 データストアで Kerberos 認証を使用する場合、Kerberos 認証用の ESXi ホストを構成します。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 [新規データストア] アイコンをクリックします。
- 3 データストア名を入力し、必要に応じてデータストアの配置場所を選択します。  
vSphere Web Client ではデータストア名が強制的に 42 文字に制限されます。
- 4 データストア タイプに NFS を選択します。
- 5 NFS バージョンを指定します。

- NFS 3
- NFS 4.1

---

**重要：** 複数のホストが同じデータストアにアクセスする場合、すべてのホストで同じプロトコルを使用する必要があります。

---

- 6 サーバ名または IP アドレス、およびマウント ポイント フォルダ名を入力します。  
  
NFS 4.1 では、サーバでトランクがサポートされている場合、複数の IP アドレスまたはサーバ名を追加できます。ホストはこれらの値を使用して、NFS サーバのマウント ポイントへのマルチパスを実現します。  
  
NFS 3 と非 Kerberos NFS 4.1 には、IPv4 または IPv6 アドレスを使用できます。
- 7 ボリュームが NFS サーバによって読み取り専用としてエクスポートされている場合、[読み取り専用の NFS マウント] を選択します。
- 8 NFS 4.1 で Kerberos 認証を使用する場合、データストアで Kerberos を有効にします。
- 9 データセンターまたはクラスターレベルでデータストアを作成する場合は、データストアをマウントするホストを選択します。
- 10 構成オプションを確認し、[終了] をクリックします。

## 仮想データストアの作成

[新しいデータストア] ウィザードを使用して、仮想データストアを作成します。

**手順**

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 [新規データストア] アイコンをクリックします。
- 3 データストア名を入力し、必要に応じてデータストアの配置場所を選択します。  
必ず、データセンター環境内の別のデータストア名と重複しない名前を使用してください。  
同じ仮想データストアをいくつかのホストにマウントする場合は、すべてのホストで一貫したデータストアの名前を使用する必要があります。
- 4 データストア タイプとして [VVOL] を選択します。
- 5 ストレージ コンテナのリストから、バックアップ ストレージ コンテナを選択します。
- 6 データストアへのアクセスが必要なホストを選択します。
- 7 構成オプションを確認し、[終了] をクリックします。

**次のステップ**

仮想データストアを作成した後は、データストアの名前変更、データストア ファイルの参照、データストアのアンマウントなどのデータストア操作を実行できます。

仮想データストアをデータストア クラスタに追加することはできません。

## 重複 VMFS データストアの管理

ストレージ デバイスに VMFS データストアのコピーが含まれている場合、既存の署名を使用してデータストアをマウントするか、新たに署名を割り当てることができます。

ストレージ ディスク内に作成された各 VMFS データストアには一意の 署名 (UUID と呼ばれる) があり、ファイル システム スーパーブロックに格納されています。ストレージ ディスクを複製する場合、またはそのスナップショットをストレージ側で作成する場合、コピーされたディスク コピーは元のディスクとバイト単位で同じになります。その結果、元のストレージ ディスクに UUID X を持つ VMFS データストアが含まれている場合、ディスク コピーには、まったく同じ UUID X を持つ VMFS データストア (つまり VMFS データストアのコピー) が表示されます。

LUN のスナップショットとレプリケーションに加えて、次のストレージ デバイス操作によって、ESXi が元のデータストアのコピーとしてデバイス上の既存のデータストアをマークする場合があります。

- LUN ID の変更
- SCSI デバイス タイプは SCSI-2 から SCSI-3 のように変わります。
- SPC-2 準拠の有効化

ESXi では、VMFS データストアのコピーを検出して vSphere Web Client に表示することができます。元の UUID でデータストアのコピーをマウントする、または UUID を変更してデータストアを再署名するというオプションがあります。

再署名するか、再署名をせずにマウントするかは、ストレージ環境内での LUN のマスク方法によって異なります。ホストが LUN の両方のコピーを表示できる場合は、再署名を推奨します。それ以外の場合は、マウントを選んでも構いません。

## 既存のデータストア署名の保持

VMFS データストアのコピーに再署名する必要がある場合、その署名を変えずにマウントできます。

ディザスタ リカバリ プランの一環として、仮想マシンの同期済みコピーをセカンダリ サイトで管理する場合などは、署名を維持できます。プライマリ サイトでディザスタが発生した場合は、セカンダリ サイトでデータストアのコピーをマウントして仮想マシンをパワーオンします。

### 前提条件

- ホストのストレージ再スキャンを実行し、ホストに提示されるストレージ デバイスのビューを更新します。
- マウントしようとしているコピーと同じ UUID を持つ元の VMFS データストアをアンマウントします。VMFS データストアのコピーをマウントできるのは、元の VMFS データストアと競合しない場合だけです。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 [新規データストア] アイコンをクリックします。
- 3 データストア名を入力し、必要に応じてデータストアの配置場所を選択します。
- 4 データストア タイプに VMFS を選択します。
- 5 ストレージ デバイスのリストから、[スナップショット ボリューム] 列に特定の値が表示されているデバイスを選択します。  
  
[スナップショット ボリューム] 列に表示された値は、デバイスが既存の VMFS データストアのコピーを含むコピーであることを示します。
- 6 マウント オプションで、[既存の署名を保持] を選択します。
- 7 データストアの構成情報を確認し、[終了] をクリックします。

### 次のステップ

マウントしたデータストアにあとで再署名する場合、まずアンマウントする必要があります。

## VMFS データストア コピーの再署名

VMFS データストア コピー上に保存されたデータを保持したい場合は、データストア再署名を使用してください。

VMFS コピーの再署名を行うとき、ESXi は新しい署名（UUID）をコピーに割り当て、コピー元とは別のデータストアとしてマウントします。仮想マシン構成ファイルから元の署名への参照はすべて更新されます。

データストアの再署名を行うとき、次の点を考慮してください。

- データストアの再署名は取り消しできません。
- 再署名の後、VMFS コピーを格納していたストレージ デバイス レプリカは、レプリカとして扱われなくなります。

- 複数にまたがるデータストアは、そのすべてのエクステンツがオンラインである場合のみ再署名が可能です。
- 再署名は、耐クラッシュ性および耐障害性のある処理です。処理が中断したとしても、あとで再開できます。
- 新しい VMFS データストアをマウントする際に、その UUID がストレージ デバイス スナップショット階層中の親または子などほかのデータストアの UUID と競合する危険を冒すことなく、マウントできます。

#### 前提条件

- データストア コピーをアンマウントします。
- ホストのストレージ再スキャンを実行し、ホストに提示されるストレージ デバイスのビューを更新します。

#### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 [新規データストア] アイコンをクリックします。
- 3 データストア名を入力し、必要に応じてデータストアの配置場所を選択します。
- 4 データストア タイプに VMFS を選択します。
- 5 ストレージ デバイスのリストから、[スナップショット ボリューム] 列に特定の値が表示されているデバイスを選択します。  
  
[スナップショット ボリューム] 列に表示された値は、デバイスが既存の VMFS データストアのコピーを含むコピーであることを示します。
- 6 マウント オプションで、[新しい署名の割り当て] を選択し、[次へ] をクリックします。
- 7 データストアの構成情報を確認し、[終了] をクリックします。

## VMFS データストアのアップグレード

データストアが VMFS2 または VMFS3 でフォーマットされていた場合は、そのデータストアを VMFS5 にアップグレードする必要があります。

データストアのアップグレードを実行する際は、次の点を考慮してください。

- VMFS2 データストアをアップグレードするには、最初に VMFS2 を VMFS3 にアップグレードする手順を伴う、2 段階の手順を使用します。VMFS2 データストアにアクセスして、VMFS2 から VMFS3 への変換を実行するには、ESX/ESXi 4.x 以前のホストを使用します。  
  
VMFS2 データストアを VMFS3 にアップグレードすると、データストアは ESXi 6.x ホストで使用可能になり、このホストで VMFS5 へのアップグレード プロセスを完了します。
- データストアの使用中で仮想マシンのパワーがオンの状態で、VMFS3 から VMFS5 へのアップグレードを実行できます。
- アップグレードの実行中に、ホストはデータストアのすべてのファイルを保存します。
- データストアのアップグレードは一方方向のプロセスです。データストアをアップグレードしたあとで、以前の VMFS フォーマットに戻すことはできません。

アップグレードされた VMFS5 データストアは、新しくフォーマットされた VMFS5 とは異なります。

表 16-3. アップグレードされた VMFS5 データストアと新しくフォーマットされた VMFS5 データストアの比較

特徴	アップグレードされた VMFS5	フォーマットされた VMFS5
ファイル ブロック サイズ	1、2、4、および 8MB	1MB
サブブロック サイズ	64KB	8KB
パーティションのフォーマット	MBR。GPT への変換は、データストアを 2TB を超えるサイズに拡張したあとでのみ可能です。	GPT
データストア制限	VMFS3 データストアの制限がそのまま適用されます。	
VMFS のロック メカニズム	ATS+SCSI	ATS のみ (ATS をサポートするハードウェア) ATS+SCSI (ATS をサポートしないハードウェア)

VMFS ロック メカニズムと ATS のみへのアップグレード方法の詳細については、[VMFS のロック メカニズム](#)を参照してください。

## データストアの VMFS5 へのアップグレード

VMFS3 データストアを使用している場合は、それらを VMFS5 にアップグレードする必要があります。

データストアの使用中で仮想マシンのパワーがオンの状態で、アップグレードを実行できます。

### 前提条件

- VMFS2 データストアがある場合、最初に ESX/ESXi 3.x または ESX/ESXi 4.x ホストを使用して、VMFS3 にアップグレードする必要があります。vSphere Host Client を使用して、ホストにアクセスします。
- データストアにアクセスするホストはすべて、VMFS5 をサポートする必要があります。
- アップグレードするボリュームに 2 MB 以上の空き容量があることを確認します。この情報については、データストアの [サマリ] タブで確認できます。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 データストアをクリックして、アップグレードします。
- 3 [構成] タブをクリックします。
- 4 [VMFS5 へのアップグレード] をクリックします。
- 5 データストアにアクセスしているホストが VMFS5 をサポートすることを確認します。
- 6 [OK] をクリックしてアップグレードを開始します。
- 7 データストアに関連付けられたすべてのホストで再スキャンを実行します。

### 結果

データストアは VMFS5 にアップグレードされ、データストアに関連付けられているすべてのホストに対して使用可能になります。



## VMFS データストア容量の増加

VMFS データストアがより多くの領域を必要とする場合は、データストア容量を増やすことができます。データストア エクステントを増やすか、新しいエクステントを追加することにより、容量を動的に増やすことができます。

次のいずれかの方法で、データストアの容量を増加します。

- 拡張可能なデータストア エクステントを動的に増やし、近接する利用可能な領域に格納する。基になるストレージ デバイスで、エクステントの直後に空き容量があるときに、そのエクステントは拡張可能だとみなされます。
- 新しいエクステントを動的に追加します。データストアは、それぞれ 2TB を超えるサイズを持つ最大 32 個のエクステントに拡張できますが、単一のボリュームとして扱われます。複数のまたがる VMFS データストアは、任意のエクステントまたはすべてのエクステントを随時使用できます。次のエクステントを使用する前に、特定のエクステントをいっぱいにする必要はありません。

**注：** Hardware Assisted Locking（アトミックテスト アンド セット（ATS） ロックとも呼ばれる）メカニズムのみをサポートしているデータストアは、ATS 以外のデバイスに拡張することはできません。詳細については、[VMFS のロック メカニズム](#)を参照してください。

## VMFS データストア容量の増加

データストアに仮想マシンを追加する必要がある場合、またはデータストア上で実行している仮想マシンの容量を増やす必要がある場合、VMFS データストアの容量を動的に増加できます。

共有のデータストアにはパワーオンされた仮想マシンがあり、完全に容量が使用されている場合、パワーオンされている仮想マシンが登録されているホストからのみデータストアの容量を拡大できます。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 拡大するデータストアを選択し、[データストア容量の増加] アイコンをクリックします。
- 3 ストレージ デバイスのリストからデバイスを選択します。

選択内容は、拡張可能なストレージ デバイスを使用できるかどうかによって異なります。

オプション	説明
既存のエクステントを拡張する	拡張可能列が「はい」になっているデバイスを選択します。拡張後すぐに使用できる領域がある場合、そのストレージ デバイスは拡張可能であると報告されます。
新しいエクステントを追加する	拡張可能列が「いいえ」になっているデバイスを選択します。

- 4 [現在のディスク レイアウト] で使用可能な構成を確認し、[次へ] をクリックします。

## 5 下部のパネルから、構成オプションを選択します。

現在のディスク レイアウトと以前の選択状況により、表示されるオプションが変わる場合があります。

オプション	説明
フリー スペースを使用して新規エクステントを追加	このディスク上の空き容量を、新しいエクステントとして追加します。
空き容量を使用して既存のエクステントを拡張	既存のエクステントを必要な容量まで拡張します。
空き領域の使用	ディスクの残りの空き容量にエクステントをデプロイします。このオプションは、エクステントを追加するときにだけ使用できます。
すべての利用可能なパーティションを利用	ディスク全体を 1 つのエクステント専用にします。このオプションは、エクステントを追加する場合、およびフォーマットするディスクが空ではない場合にのみ使用できます。ディスクが再フォーマットされ、データストア、およびそれに含まれているすべてのデータが消去されます。

## 6 エクステントの容量を設定します。

エクステントの最小サイズは 1.3 GB です。デフォルトでは、ストレージ デバイスの空き領域がすべて使用可能です。

## 7 [次へ] をクリックします。

## 8 提案されるレイアウトと、新しいデータストアの構成を確認して [終了] をクリックします。

# データストアの管理操作

データストアの作成後、データストアでいくつかの管理操作を実行できます。すべてのタイプのデータストアで、データストアの名前変更などの特定の操作を実行できます。その他の操作は、特定のタイプのデータストアに適用されます。

### ■ データストア名の変更

既存のデータストアの名前を変更できます。システムに悪影響を及ぼさずに、仮想マシンが実行されているデータストアの名前を変更することができます。

### ■ データストアのアンマウント

データストアをアンマウントするとそのまま残りますが、指定したホストからは見えなくなります。マウントされたままの状態になっている別のホストでは、データストアは引き続き表示されます。

### ■ データストアのマウント

前にアンマウントしたデータストアをマウントすることができます。また、共有データストアにするために追加のホストにデータストアをマウントすることもできます。

### ■ VMFS データストアの削除

再署名せずにマウントされたコピーなど、あらゆるタイプの VMFS データストアを削除できます。データストアを削除すると、データストアが破棄され、そのデータストアへアクセスできるすべてのホストから消失します。

## ■ データストア ブラウザの使用

データストア ファイル ブラウザを使用して、データストアのコンテンツを管理します。データストアに格納されたフォルダとファイルを参照できます。また、ブラウザを使用して、ファイルをアップロードしたり、フォルダやファイルに対して管理タスクを実行したりすることもできます。

## ■ ストレージ フィルタのオフ

VMFS データストアの管理操作を行うとき、vCenter Server はデフォルトのストレージ保護フィルタを使用します。フィルタを使用すると、特定の操作に使用できるストレージ デバイスののみを取得できるため、ストレージの破損を防ぐことができます。不適切なデバイスは選択肢として表示されません。すべてのデバイスを表示するには、フィルタをオフにします。

# データストア名の変更

既存のデータストアの名前を変更できます。システムに悪影響を及ぼさずに、仮想マシンが実行されているデータストアの名前を変更することができます。

## 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] > [データストア] の順に選択します。
- 2 名前を変更するデータストアを選択します。
- 3 右クリック メニューから [名前の変更] を選択します。
- 4 新しいデータストア名を入力します。

vSphere Web Client ではデータストア名が強制的に 42 文字に制限されます。

## 結果

新しい名前は、データストアへのアクセス権のあるすべてのホストに表示されます。

# データストアのアンマウント

データストアをアンマウントするとそのまま残りますが、指定したホストからは見えなくなります。マウントされたままの状態になっている別のホストでは、データストアは引き続き表示されます。

アンマウントの処理中は、データストアへの I/O が発生する可能性がある構成操作を行わないでください。

---

**注：** データストアが vSphere HA ハートビートで使用されていないことを確認してください。vSphere HA ハートビートによってデータストアのアンマウントができなくなることはありません。ただし、データストアがハートビートのために使用されている場合、そのデータストアをアンマウントするとホストに障害が発生し、アクティブな仮想マシンが再起動されることがあります。

---

## 前提条件

データストアをアンマウントする前に、次の前提条件を満たしていることを適宜確認してください。

- そのデータストア上に仮想マシンが存在しない。
- そのデータストアが Storage DRS で管理されていない。
- そのデータストアに対して Storage I/O Control が無効化されている。

## 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 アンマウントするデータストアを右クリックして [データストアのアンマウント] を選択します。
- 3 データストアが共有されている場合、データストアへのアクセスが不要なホストを指定します。
- 4 データストアをアンマウントすることを確認します。

## 結果

すべてのホストから VMFS データストアをアンマウントした後、データストアはアクティブでないとしてマークが付けられます。NFS または仮想データストアをすべてのホストからアンマウントすると、データストアがインベントリに表示されなくなります。

## 次のステップ

正しいストレージ取り出し手順の一部として VMFS データストアをアンマウントした場合、これでデータストアをバックアップしているストレージ デバイスを取り出せます。[ストレージ デバイスの分離](#) を参照してください。

## データストアのマウント

前にアンマウントしたデータストアをマウントすることができます。また、共有データストアにするために追加のホストにデータストアをマウントすることもできます。

すべてのホストからアンマウントされた VMFS データストアは、インベントリに残されますが、アクセス不可のマークが付けられています。このタスクを使用して、指定した 1 台のホストまたは複数のホストに VMFS データストアをマウントすることができます。

NFS または仮想データストアをすべてのホストからアンマウントした場合、そのデータストアはインベントリに表示されなくなります。インベントリから削除された NFS または仮想データストアをマウントするには、[新しいデータストア] ウィザードを使用します。

一部のホストからアンマウントされても、ほかのホストにマウントされたままのデータストアは、インベントリでは有効なデータストアとして表示されます。

## 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 マウントするデータストアを右クリックし、次のいずれかのオプションを選択します。
  - [データストアのマウント]
  - [追加ホストでのデータストアのマウント]1 つまたは別のオプションが表示されるかどうかは、使用するデータストアのタイプによって決まります。
- 3 データストアにアクセスする必要のあるホストを選択します。

## VMFS データストアの削除

再署名せずにマウントされたコピーなど、あらゆるタイプの VMFS データストアを削除できます。データストアを削除すると、データストアが破棄され、そのデータストアへアクセスできるすべてのホストから消失します。

**注：** データストアの削除操作により、仮想マシンに関連する、データストア上のすべてのファイルが永久に削除されます。アンマウントしなくてもデータストアを削除することはできますが、最初にデータストアをアンマウントすることをお勧めします。

### 前提条件

- すべての仮想マシンをデータストアから削除または移行します。
- データストアにアクセスしているホストがないことを確認してください。
- データストア用のストレージ DRS を無効にします。
- データストアに対して Storage I/O control を無効にします。
- データストアが vSphere HA ハートビートに使用されていないことを確認してください。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 削除するデータストアを右クリックします。
- 3 [データストアの削除] を選択します。
- 4 データストアを削除することを確認します。

## データストア ブラウザの使用

データストア ファイル ブラウザを使用して、データストアのコンテンツを管理します。データストアに格納されたフォルダとファイルを参照できます。また、ブラウザを使用して、ファイルをアップロードしたり、フォルダやファイルに対して管理タスクを実行したりすることもできます。

### ■ データストアへのファイルのアップロード

データストア ファイル ブラウザを使用して ESXi ホストにアクセスできるデータストアにファイルをアップロードします。

### ■ データストア フォルダまたはファイルのコピー

データストア ブラウザを使用して、同じデータストアまたは別のデータストア上の新しい場所にフォルダまたはファイルをコピーします。

### ■ データストア フォルダまたはファイルの移動

データストア ブラウザを使用して、同じデータストアまたは別のデータストア上の新しい場所にフォルダまたはファイルを移動します。

### ■ データストア フォルダまたはファイルの名前変更

データストア ブラウザを使用してフォルダ名またはファイル名を変更します。

## ■ シン仮想ディスクの拡張

シン フォーマットで仮想ディスクを作成した場合は、シン ディスクをシック プロビジョニング フォーマットの仮想ディスクに変換できます。

### 手順

- 1 データストア ブラウザを開きます。
  - a インベントリにデータストアを表示します。
  - b データストアを右クリックし、[ファイルの参照] (🔍) を選択します。
- 2 既存のフォルダやファイルに移動して、データストアのコンテンツを参照します。
- 3 アイコンとオプションを使用して、管理タスクを実行します。

アイコンとオプション	説明
	クライアント統合プラグインをインストールするか、またはデータストアにファイルをアップロードします。 <a href="#">データストアへのファイルのアップロード</a> を参照してください。
	データストアにフォルダを作成します。
	選択したフォルダまたはファイルを、同じデータストアまたは別のデータストア上の新しい場所にコピーします。 <a href="#">データストア フォルダまたはファイルのコピー</a> を参照してください。
	選択したフォルダまたはファイルを、同じデータストアまたは別のデータストア上の新しい場所に移動します。 <a href="#">データストア フォルダまたはファイルの移動</a> を参照してください。
	選択したフォルダまたはファイルの名前を変更します。 <a href="#">データストア フォルダまたはファイルの名前変更</a> を参照してください。
	選択したフォルダまたはファイルを削除します。
拡張	選択したシン仮想ディスクをシックに変換します。このオプションは、シンプロビジョニングディスクのみに適用されます。 <a href="#">シン仮想ディスクの拡張</a> を参照してください。

### 次のステップ

詳細については、次のビデオをご覧ください。



(Using the Datastore Browser in the vSphere Web Client )

## データストアへのファイルのアップロード

データストア ファイル ブラウザを使用して ESXi ホストにアクセスできるデータストアにファイルをアップロードします。

データストアは、仮想マシンのファイルのストレージとして従来どおりに使用するだけでなく、仮想マシン関連のデータやファイルの保存にも使用できます。たとえば、オペレーティング システムの ISO イメージをローカル コンピュータからホストのデータストアにアップロードできます。これらのイメージを使用して新しい仮想マシンにゲスト OS をインストールします。

---

**注：** Virtual Volumes データストアにファイルを直接アップロードすることはできません。先に Virtual Volumes データストアにフォルダを作成してから、フォルダにファイルをアップロードする必要があります。ブロック ストレージの Virtual Volume データストアに作成されたフォルダには、4 GB のストレージ容量しかありません。vVol データストアはフォルダの直接アップロードをサポートしています。

---

#### 前提条件

- 必要な権限：データストア.データストアの参照
- アイコン (📁) をポイントし、そのラベルを確認します。ラベルに「クライアント統合プラグインのインストール」と表示される場合は、ファイルをアップロードするためにプラグインをインストールする必要があります。アイコンをクリックし、表示される指示に従ってください。インストール後は、ラベルが「データストアにファイルをアップロード」に変わります。

#### 手順

- 1 データストア ブラウザを開きます。
  - a インベントリにデータストアを表示します。
  - b データストアを右クリックし、[ファイルの参照] (📁) を選択します。
- 2 (オプション) ファイルを保存するフォルダを作成します。
- 3 ターゲット フォルダを選択し、[データストアにファイルをアップロード] アイコン (📁) をクリックします。
- 4 ローカル コンピュータ上でアップロードする項目を検索し、[開く] をクリックします。
- 5 データストア ファイル ブラウザを更新し、アップロードしたファイルがリストにあることを確認します。

#### 次のステップ

前にエクスポートしてからデータストアにアップロードした OVF テンプレートをデプロイする場合、問題が発生する可能性があります。詳細および回避策については、VMware のナレッジベースの記事 [KB 2117310](#) を参照してください。

### データストア フォルダまたはファイルのコピー

データストア ブラウザを使用して、同じデータストアまたは別のデータストア上の新しい場所にフォルダまたはファイルをコピーします。

仮想ディスク ファイルは、フォーマット変換することなく移動またはコピーされます。ソース ホストとは異なるホストに属するデータストアに仮想マシンを移動する場合、仮想ディスクの変換が必要になる場合があります。変換しなければ、ディスクを使用できない可能性があります。

vCenter Server 間で仮想マシン ファイルをコピーすることはできません。

### 前提条件

必要な権限：データストア.データストアの参照

### 手順

- 1 データストア ブラウザを開きます。
  - a インベントリにデータストアを表示します。
  - b データストアを右クリックし、[ファイルの参照] (🔍) を選択します。
- 2 コピーするオブジェクト（フォルダまたはファイルのいずれか）を参照します。
- 3 オブジェクトを選択し、[選択項目を新しい場所へコピー] アイコンをクリックします。
- 4 コピー先を指定します。
- 5 （オプション）[ターゲットで名前が一致するファイルおよびフォルダを上書きします。] を選択します。
- 6 [OK] をクリックします。

### データストア フォルダまたはファイルの移動

データストア ブラウザを使用して、同じデータストアまたは別のデータストア上の新しい場所にフォルダまたはファイルを移動します。

---

**注：** 仮想ディスク ファイルは、フォーマット変換することなく移動またはコピーされます。移動元ホストとは異なるタイプのホストにあるデータストアに仮想ディスクを移動した場合、その仮想ディスクを使用するには変換する必要があります。

---

### 前提条件

必要な権限：データストア.データストアの参照

### 手順

- 1 データストア ブラウザを開きます。
  - a インベントリにデータストアを表示します。
  - b データストアを右クリックし、[ファイルの参照] (🔍) を選択します。
- 2 移動するオブジェクト（フォルダまたはファイルのいずれか）を参照します。
- 3 オブジェクトを選択し、[選択項目を新しい場所へ移動] アイコンをクリックします。
- 4 コピー先を指定します。
- 5 （オプション）[ターゲットで名前が一致するファイルおよびフォルダを上書きします。] を選択します。
- 6 [[OK]] をクリックします。

### データストア フォルダまたはファイルの名前変更


データストア ブラウザを使用してフォルダ名またはファイル名を変更します。



**前提条件**

必要な権限：データストア.データストアの参照

**手順**

- 1 データストア ブラウザを開きます。
  - a インベントリにデータストアを表示します。
  - b データストアを右クリックし、[ファイルの参照] () を選択します。
- 2 名前を変更するオブジェクト（フォルダまたはファイル）を参照します。
- 3 オブジェクトを選択して、[選択項目の名前変更] アイコンをクリックします。
- 4 新しい名前を指定して、[OK] をクリックします。

**シン仮想ディスクの拡張**


シン フォーマットで仮想ディスクを作成した場合は、シン ディスクをシック プロビジョニング フォーマットの仮想ディスクに変換できます。

データストア ブラウザを使用して、仮想ディスクを拡張します。

**前提条件**

- 仮想マシンが存在するデータストアに十分な容量があることを確認します。
- 仮想ディスクがシンであることを確認します。
- スナップショットを削除します。
- 仮想マシンをパワーオフします。

**手順**

- 1 拡張する仮想ディスクのフォルダに移動します。
  - a vSphere Web Client で、仮想マシンを参照します。
  - b 情報を表示する仮想マシンをダブルクリックします。
  - c [関連オブジェクト] > [データストア] の順にクリックします。  
仮想マシン ファイルを保存するデータストアが一覧表示されます。
  - d データストアを選択し、[データストア ファイル ブラウザに移動します。] アイコンをクリックします。  
データストア ブラウザに、データストアのコンテンツが表示されます。
- 2 仮想マシン フォルダを開き、変換したい仮想ディスク ファイルを参照します。  
このファイルには .vmdk 拡張子が含まれており、仮想ディスク () アイコンが表示されます。
- 3 仮想ディスク ファイルを右クリックし、[拡張] を選択します。

---

**注：** 仮想ディスクがシックの場合、または仮想マシンが実行中の場合、このオプションは使用できない場合があります。

---

## 結果

拡張された仮想ディスクは、最初にプロビジョニングされたデータストア容量全体を専有します。

## ストレージ フィルタのオフ

VMFS データストアの管理操作を行うとき、vCenter Server はデフォルトのストレージ保護フィルタを使用します。フィルタを使用すると、特定の操作に使用できるストレージ デバイスのみを取得できるため、ストレージの破損を防ぐことができます。不適切なデバイスは選択肢として表示されません。すべてのデバイスを表示するには、フィルタをオフにします。

### 前提条件

デバイス フィルタを変更する場合は、事前に VMware のサポート チームに相談してください。ほかにデバイスの破損を防ぐ方法がある場合のみ、フィルタをオフにできます。

### 手順

- 1 vSphere Web Client オブジェクト ナビゲータで、vCenter Server を参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [設定] で、[詳細設定] をクリックし、[編集] をクリックします。
- 4 無効にするフィルタを指定します。
  - a ページの下部にある [名前] テキスト ボックスに適切なフィルタ名を入力します。

名前	説明
config.vpxd.filter.vmfsFilter	VMFS フィルタ
config.vpxd.filter.rdmFilter	RDM フィルタ
config.vpxd.filter.sameHostsAndTranportsFilter	同じホストと転送フィルタ
config.vpxd.filter.hostRescanFilter	ホストの再スキャン フィルタ
<b>注：</b> このフィルタをオフにしても、ホストでは引き続き、ホストまたはクラスタに新しい LUN を提供するたびに再スキャンが実行されます。	

- b [値] テキスト ボックスに、指定キーとして **False** と入力します。

- 5 [追加] をクリックし、[OK] をクリックして変更内容を保存します。

vCenter Server システムを再起動する必要はありません。

## ストレージ フィルタリング

vCenter Server には、サポートされていないストレージ デバイスの使用で発生する可能性のある、ストレージ デバイスの破損やパフォーマンスの低下を回避するためのストレージ フィルタが用意されています。これらのフィルタはデフォルトで使用できます。

表 16-4. ストレージ フィルタ

フィルタ名	説明
config.vpxd.filter.vmfsFilter (VMFS フィルタ)	vCenter Server が管理する任意のホストの VMFS データストアによってすでに使用されているストレージ デバイスや LUN をフィルタリングします。LUN は、別の VMFS データストアでフォーマットされる候補、または RDM として使用される候補として表示されません。
config.vpxd.filter.rdmFilter (RDM フィルタ)	vCenter Server が管理する任意のホストの RDM によってすでに参照されている LUN をフィルタリングします。LUN は、VMFS でフォーマットされる候補、または別の RDM によって使用される候補として表示されません。  複数の仮想マシンが同じ LUN にアクセスする場合、これらの仮想マシンは同一の RDM マッピング ファイルを共有する必要があります。このタイプの構成については、『vSphere リソース管理』ドキュメントを参照してください。
config.vpxd.filter.sameHostsAndTransportsFilter (同じホストと転送フィルタ)	ホストまたはストレージ タイプに互換性がないため VMFS データストア エクステントとして使用できない LUN をフィルタリングします。次の LUN はエクステントとして追加できません。 <ul style="list-style-type: none"> <li>■ 元の VMFS データストアを共有するすべてのホストに公開されていない LUN。</li> <li>■ 元の VMFS データストアが使用するものと異なるタイプのストレージを使用する LUN。たとえば、ローカル ストレージ デバイス上の VMFS データストアに、ファイバ チャンネル エクステントを追加することはできません。</li> </ul>
config.vpxd.filter.hostRescanFilter (ホストの再スキャン フィルタ)	データストアの管理操作を行なったあと、自動的に VMFS データストアを再スキャンおよびアップデートします。フィルタは、vCenter Server が管理するすべてのホスト上にある、すべての VMFS データストアの一貫した表示を提供します。  <b>注：</b> ホストまたはクラスタに新しい LUN を提供した場合、ホストの再スキャン フィルタがオンであるか、オフであるかに関係なく、ホストによって自動的に再スキャンが実行されます。

## 動的なディスクミラーリングの設定

通常、仮想マシン上の論理ボリューム マネージャ ソフトウェアを使用して仮想ディスクをミラーリングすることはできません。ただし、Microsoft Windows の仮想マシンがダイナミック ディスクをサポートしている場合は、2 つの SAN LUN 間で仮想ディスクをミラーリングすることで、予定しないストレージ デバイスの損失から仮想マシンを保護することができます。

### 前提条件

- ダイナミック ディスクをサポートする Windows 仮想マシンを使用してください。
- 必要な権限： 詳細

### 手順

- 1 2 つの仮想ディスクを持つ仮想マシンを作成します。  
これらのディスクは、別々のデータストアに配置してください。
- 2 仮想マシンにログインし、ディスクを動的にミラーリングされたディスクとして構成します。  
詳細については、Microsoft のドキュメントを参照してください。
- 3 ディスクの同期後、仮想マシンをパワーオフします。

4 動的なディスク ミラーリングの使用を許可するように、仮想マシンの設定を変更します。

- a 仮想マシンを右クリックし、[設定の編集] を選択します。
- b [仮想マシン オプション] タブをクリックして、[詳細設定] メニューを展開します。
- c 構成パラメータの横にある [構成パラメータの編集] をクリックします。
- d [行の追加] をクリックして次のパラメータを追加します。

名前	値
scsi#.returnNoConnectDuringAPD	True
scsi#.returnBusyOnNoConnectStatus	False

- e [OK] をクリックします。

## ストレージ デバイスでの ESXi ホストの診断情報の収集

診断やテクニカル サポートを行うために、ESXi では、ホスト障害時に診断情報を事前構成済みの場所に保存できるようになっている必要があります。

通常、診断情報を収集するパーティション (VMkernel コア ダンプとも呼ばれる) は、ESXi のインストール中にローカル ストレージ デバイスに作成されます。このデフォルトの動作は、たとえば、ローカル ストレージの代わりに共有ストレージ デバイスを使用する場合に上書きできます。ローカル デバイスの自動フォーマットを防ぐには、ESXi をインストールしてホストを最初にパワーオンする前に、デバイスをホストから切り離します。診断情報を収集する場所は、後でローカルまたはリモート ストレージ デバイスで設定できます。

ストレージ デバイスを使用する場合、コア ダンプの収集を設定するのに 2 つの選択肢があります。ストレージ デバイスの事前構成済みの診断パーティションを使用するか VMFS データストアのファイルを使用することができます。

### ■ コア ダンプの場所としてのデバイス パーティションの設定

ESXi ホストに診断パーティションを作成します。

### ■ コア ダンプの場所としてのファイルの設定

使用可能なコア ダンプ パーティションのサイズが不十分な場合は、コア ダンプをファイルとして生成するように ESXi を構成できます。

## コア ダンプの場所としてのデバイス パーティションの設定

ESXi ホストに診断パーティションを作成します。

診断パーティションを作成するときは、次の考慮事項が適用されます。

- 診断パーティションは、ソフトウェア iSCSI または依存型ハードウェア iSCSI アダプタを介してアクセスする iSCSI LUN には作成できません。iSCSI を使った診断パーティションの詳細については、[iSCSI SAN からの起動に関する一般的推奨事項](#) を参照してください。
- 診断パーティションは、ソフトウェア FCoE LUN には作成できません。
- ディスクレス サーバを使用していない場合には、ローカル ストレージで診断パーティションを設定します。

- 各ホストには 2.5 GB の診断パーティションが必要です。複数のホストが SAN LUN で診断パーティションを共有する場合、パーティションには、すべてのホストのコア ダンプを収容できるサイズが必要です。
- 共有診断パーティションを使用するホストで障害が発生した場合は、ホストを再起動して、障害発生直後にログ ファイルを抽出してください。そうしないと、最初のホストの診断データを収集する前に別のホストで障害が発生した場合に、コア ダンプを保存できない可能性があります。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 ホストを右クリックして、[診断パーティションの追加] を選択します。

このオプションが表示されていない場合は、すでにホストに診断パーティションがあります。

- 3 診断パーティションのタイプを指定します。

オプション	説明
プライベート ローカル	ローカル ディスクに診断パーティションを作成します。このパーティションには、使用しているホストのみに関する障害情報が格納されます。
プライベート SAN ストレージ	SAN を共有しない LUN に診断パーティションを作成します。このパーティションには、使用しているホストのみに関する障害情報が格納されます。
共有 SAN ストレージ	共有 SAN LUN に診断パーティションを作成します。このパーティションは複数のホストによってアクセスされ、複数のホストに関する障害情報を格納できます。

- 4 [Next] をクリックします。
- 5 診断パーティションに使用するデバイスを選択し、[次へ] をクリックします。
- 6 パーティションの構成情報を確認し、[終了] をクリックします。

### 診断パーティションの確認

esxcli コマンドを使用して、診断パーティションが設定されているかどうかを確認します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

#### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

#### 手順

- ◆ 診断パーティションが設定されているかどうかを確認するために、パーティションをリストします。

```
esxcli --server=server_name system coredump partition list
```

## 結果

診断パーティションが設定されている場合、コマンドはそれに関する情報を表示します。そうでない場合、コマンドは有効化および構成されているパーティションがないことを表示します。

## 次のステップ

ホストの診断パーティションを管理するには、vCLI コマンドを使用します。vSphere Command-Line Interface の例 を参照してください。

## コア ダンプの場所としてのファイルの設定

使用可能なコア ダンプ パーティションのサイズが不十分な場合は、コア ダンプをファイルとして生成するように ESXi を構成できます。

通常、ESXi のインストール時には、2.5 GB のコア ダンプ パーティションが作成されます。ESXi 5.0 以前からのアップグレードでは、コア ダンプ パーティションが 100 MB に制限されます。このタイプのアップグレードの場合は、起動プロセス中にシステムが VMFS データストアにコア ダンプ ファイルを作成する可能性があります。コア ダンプ ファイルが作成されない場合は、そのファイルを手動で作成することができます。

**注：** ソフトウェア iSCSI とソフトウェア FCoE は、コア ダンプ ファイルの場所としてサポートされていません。

## 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

## 手順

- 1 次のコマンドを実行して、VMFS データストア コア ダンプ ファイルを作成します。

```
esxcli system coredump file add
```

このコマンドには次のオプションがありますが、これらのオプションは必須ではないので省略できます。

オプション	説明
<code>--datastore   -d <i>datastore_UUID または datastore_name</i></code>	指定しない場合は、十分なサイズを持つデータストアがシステムによって選択されます。
<code>--file   -f <i>file_name</i></code>	指定しない場合は、コア ダンプ ファイルの一意の名前がシステムによって指定されます。
<code>--size   -s <i>file_size_MB</i></code>	指定しない場合は、ホストに装着されているメモリに対して適切なサイズのファイルがシステムによって作成されます。

- 2 次のコマンドを実行して、ファイルが作成されたことを確認します。

```
esxcli system coredump file list
```

次のような出力が表示されます。

Path	Active	Configured	Size
-----	-----	-----	-----
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	false	false	104857600

- 3 ホストのコア ダンプ ファイルを有効にします。

**esxcli system coredump file set**

このコマンドには次のオプションがあります。

オプション	説明
<b>--path   -p</b>	使用するコア ダンプ ファイルのパスです。これは事前割り当て済みのファイルでなければなりません。
<b>--smart   -s</b>	このフラグは --enable   -e=true 指定時にのみ使用できます。その場合は、洗練された選択アルゴリズムを使用してファイルが選択されます。 次に例を示します。 <b>esxcli system coredump file set --smart --enable true</b>

- 4 次のコマンドを実行して、コア ダンプ ファイルがアクティブであり、構成されていることを確認します。

**esxcli system coredump file list**

次のような出力は、コア ダンプ ファイルがアクティブであり、構成されていることを示します。

Path	Active	Configured	Size
-----	-----	-----	-----
/vmfs/volumes/52b021c3-.../vmkdump/test.dumpfile	True	True	104857600

#### 次のステップ

コア ダンプ ファイルの管理で利用できるその他のコマンドの詳細については、『vSphere Command-Line Interface のリファレンス』ドキュメントを参照してください。

## コア ダンプ ファイルの無効化と削除

構成済みのコア ダンプ ファイルを無効化し、必要に応じて、VMFS データストアから削除します。

一時的にコア ダンプ ファイルを無効化することができます。無効化したファイルを使用する予定がない場合、VMFS データストアから削除できます。無効化されていないファイルを削除するには、**esxcli system coredump file remove** コマンドを **--force | -F** オプションと一緒に使用します。

#### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で **esxcli** コマンドを実行します。

## 手順

- 1 次のコマンドを実行して、コア ダンプ ファイルを無効化します。

```
esxcli system coredump file set --unconfigure | -u
```

- 2 ファイルを VMFS データストアから削除します。

```
esxcli system coredump file remove --file | -f file_name
```

このコマンドには次のオプションがあります。

オプション	説明
--file   -f	削除するダンプ ファイルのファイル名を指定します。ファイル名を指定しないと、構成済みのコア ダンプ ファイルが削除されます。
--force   -F	削除するダンプ ファイルを無効化し、構成解除します。このオプションは、ファイルが今までに無効化されておらず、アクティブな場合に必要です。

## 結果

コア ダンプ ファイルは無効になり、VMFS データストアから削除されます。

# VOMA によるメタデータの整合性の確認

vSphere Ondisk Metadata Analyser (VOMA) を使用して、ファイル システムまたは基盤となる論理ボリュームに影響するメタデータの破損インシデントを特定および修正します。

## 問題

VMFS データストアまたは仮想フラッシュ リソースのさまざまな機能で問題が発生した場合は、ファイル システムまたはファイル システムをバックアップする論理ボリュームでのメタデータの整合性を確認する必要があります。たとえば、状況が次のいずれかである場合、メタデータの確認を行います。

- ストレージが停止する。
- RAID を再構築した後またはディスク交換を行った後。
- vmkernel.log ファイルでメタデータのエラーが確認された場合。
- VMFS 上のファイルにアクセスできない。
- vCenter Server のイベント タブに、データストアが破損したことが表示される。

## 解決方法

メタデータの整合性を確認するには、ESXi ホストの CLI から VOMA を実行します。VOMA を使用して、VMFS データストアまたは仮想フラッシュ リソースのメタデータの不整合問題を確認し、修正します。VOMA によって報告されるエラーを解決するには、VMware サポートに問い合わせてください。

VOMA ツールを使用するときは、これらのガイドラインに従います。

- 分析する VMFS データストアが複数のエクステントにまたがっていないことを確認します。VOMA は、単一のエクステントのデータストアのみに対して実行できます。



- 実行中の仮想マシンをパワーオフするか、それらを別のデータストアに移行します。

次の例は、VOMA を使用して VMFS メタデータの整合性を確認する方法を示しています。

- 1 確認する必要がある VMFS データストアをバックアップするデバイスの名前とパーティション番号を取得します。

```
#esxcli storage vmfs extent list
```

出力されたデバイス名およびパーティション列によりデバイスを特定します。例：

Volume Name	XXXXXXXXX	Device Name	Partition
1TB_VMFS5	XXXXXXXXX	naa.600508e000000000b367477b3be3d703	3

- 2 VMFS エラーがないか確認するために VOMA を実行します。

VMFS データストアをバックアップするデバイス パーティションへの絶対パスを指定し、パーティション番号をデバイス名とともに指定します。例：

```
# voma -m vmfs -f check -d /vmfs/devices/disks/  
naa.600508e000000000b367477b3be3d703:3
```

出力リストに可能性のあるエラーが表示されます。たとえば、次の出力は、ハートビート アドレスが無効であることを示しています。

```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXX  
Phase 2: Checking VMFS heartbeat region  
ON-DISK ERROR: Invalid HB address  
Phase 3: Checking all file descriptors.  
Phase 4: Checking pathname and connectivity.  
Phase 5: Checking resource reference counts.  
  
Total Errors Found:          1
```

VOMA ツールで指定できるコマンド オプションを次に示します。

表 16-5. VOMA コマンド オプション

コマンド オプション	説明
-m   --module	実行モジュール： <ul style="list-style-type: none"> <li>■ vmfs:これは、デフォルトのオプションです。VMFS 3 および VMFS 5 のデータストアを確認できます。このモジュールを指定すると、LVM の最小確認も同様に行われます。</li> <li>■ vmfsl:仮想フラッシュ ボリュームをバックアップするファイル システムを確認します。</li> <li>■ lvm:VMFS データストアをバックアップする論理ボリュームを確認します。</li> </ul>
-f   --func	実行される機能： <ul style="list-style-type: none"> <li>■ query:モジュールでサポートされる機能をリストします。</li> <li>■ check:エラーの有無を確認します。</li> <li>■ fix:エラーを確認して修正します。</li> </ul>

表 16-5. VOMA コマンド オプション （続き）

コマンド オプション	説明
<code>-d --device</code>	検査されるデバイスまたはディスク。VMFS データストアをバックアップするデバイス パーティションへの絶対パスを指定します。例、 <code>/vmfs/devices/disks/naa.00000000000000000000000000000000:1</code> 。
<code>-s   --logfile</code>	結果を出力するログ ファイルを指定します。
<code>-v   --version</code>	VOMA のバージョンを表示します。
<code>-h --help</code>	VOMA コマンドのヘルプ メッセージを表示します。

## VMFS ポインタ ブロック キャッシュの構成

ポインタ ブロック キャッシュの設定には VMFS の詳細パラメータを使用できます。

VMFS データストアにある仮想マシン ファイルのサイズが増加すると、それらのファイルで使用されるポインタ ブロック数も増加します。ポインタ ブロックは、VMFS データストアの大きい仮想マシン ファイルおよび仮想ディスクのファイル ブロックに対応するために使用されます。

各 ESXi ホストで、ポインタ ブロック キャッシュの最小サイズと最大サイズを構成できます。ポインタ ブロック キャッシュのサイズが設定された最大サイズに近づくと、削除メカニズムによってキャッシュから一部のポインタ ブロック エントリが削除されます。

ポインタ ブロック キャッシュの最大サイズは、VMFS データストアに存在する、開いているすべての仮想ディスク ファイルの作業サイズに基づきます。ホストのすべての VMFS データストアは 1 つのポインタ ブロック キャッシュを使用します。

最小値は、システムでのキャッシュの割り当てに保証された最小メモリに基づきます。開いているファイルの容量が 1 TB の場合、約 4 MB のメモリが必要です。

ポインタ ブロック キャッシュの最小値および最大値を設定するには、vSphere Web Client の [システムの詳細設定] ダイアログ ボックスを使用します。

表 16-6. ポインタ ブロック キャッシュを制御するための詳細パラメータ

パラメータ	値	説明
<code>VMFS3.MaxAddressableSpaceTB</code>	デフォルト値は 32 (TB) です。	VMFS キャッシュでサポートされる、削除が開始されるまでの開いているすべてのファイルの最大サイズ。
<code>VMFS3.MinAddressableSpaceTB</code>	デフォルト値は 10 (TB) です。	VMFS キャッシュでサポートが保証される、開いているすべてのファイルの最小サイズ。

`esxcli storage vmfs pbcache` コマンドを使用して、ポインタ ブロック キャッシュのサイズに関する情報とその他の統計情報を取得できます。この情報は、ポインタ ブロック キャッシュの最小サイズおよび最大サイズを調整する際に役立つため、最大のパフォーマンスを得ることができます。

## ホストの詳細属性の設定

ホストの詳細属性を設定できます。

**注意：** VMware テクニカル サポートまたはナレッジ ベースの記事で特に指示がない限り、詳細オプションの変更はサポートされていないと見なされます。その他の場合はすべて、これらのオプションの変更はサポートされていないと見なされます。ほとんどの場合、デフォルトの設定で最適な結果が得られます。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム]メニューの[システムの詳細設定]をクリックします。
- 4 [詳細設定] から適切な項目を選択します。
- 5 [編集]をクリックして、値を編集します。
- 6 [OK] をクリックします。

## VMFS ポインタ ブロック キャッシュの情報の取得

VMFS ポインタ ブロック キャッシュの使用量に関する情報を取得できます。この情報は、ポインタ ブロック キャッシュがどの程度の容量を消費するかを理解するのに役立ちます。また、ポインタ ブロック キャッシュの最小サイズと最大サイズを調整する必要があるかどうかを判断することもできます。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

- ◆ ポインタ ブロック キャッシュ統計情報を取得またはリセットするには、次のコマンドを使用します。

```
esxcli storage vmfs pbcache
```

オプション	説明
取得	VMFS ポインタ ブロック キャッシュ統計情報を取得する。
リセット	VMFS ポインタ ブロック キャッシュ統計情報をリセットする。

**例：ポインタ ブロック キャッシュの統計情報の取得**

```
#esxcli storage vmfs pbcache get
Cache Capacity Miss Ratio: 0 %
Cache Size: 0 MiB
Cache Size Max: 132 MiB
Cache Usage: 0 %
Cache Working Set: 0 TiB
Cache Working Set Max: 32 TiB
Vmfs Heap Overhead: 0 KiB
Vmfs Heap Size: 23 MiB
Vmfs Heap Size Max: 256 MiB
```

# マルチパスとフェイルオーバーについて

# 17

ホストとそのストレージ間の常時接続を維持するため、ESXi はマルチパスをサポートしています。マルチパスは、複数の物理パスを使用できる技術で、ホストと外部のストレージ デバイス間におけるデータの送信を行います。

アダプタ、スイッチ、またはケーブルなど、SAN ネットワーク内の要素に障害が発生した場合、ESXi は、障害の発生したコンポーネントを使用していない別の物理パスにフェイルオーバーできます。この、障害の発生したコンポーネントを避けるためのパスの切り替え手順は、パスのフェイルオーバーと呼ばれます。

パスのフェイルオーバーのほかに、マルチパスによるロード バランシングもあります。ロード バランシングは、複数の物理パス間で I/O 負荷を割り当てる処理です。ロード バランシングによって、潜在的なボトルネックが軽減または排除されます。

---

**注：** パスのフェイルオーバーが発生した場合、仮想マシン I/O は最大 60 秒遅延することがあります。この遅延時間があるために、トポロジが変わったあとで SAN は構成を安定させることができます。一般的に、I/O 遅延はアクティブ-パッシブ アレイでは長くなり、アクティブ-アクティブ アレイでは短くなります。

---

この章には、次のトピックが含まれています。

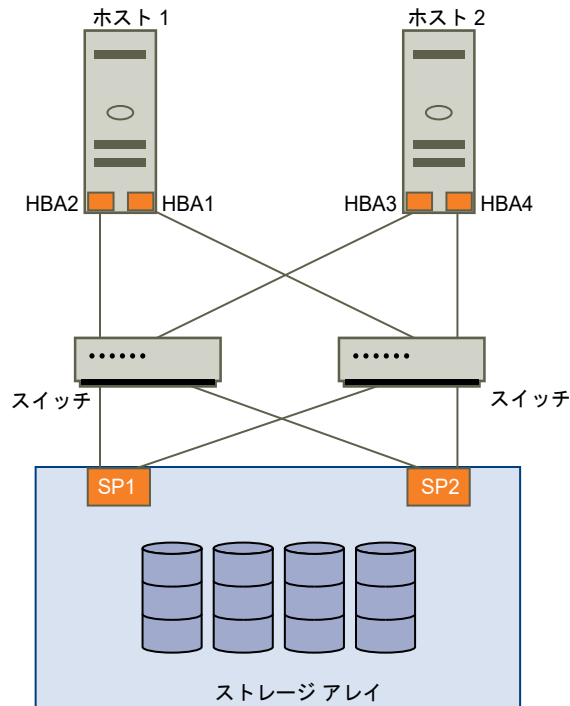
- ファイバ チャンネルを使用したフェイルオーバー
- iSCSI でのホスト ベースのフェイルオーバー
- iSCSI でのアレイ ベースのフェイルオーバー
- パスのフェイルオーバーと仮想マシン
- 複数のパスの管理
- VMware マルチパス モジュール
- パスのスキャンと要求
- ストレージ パスおよびマルチパス プラグインの管理
- 仮想マシン I/O のキューのスケジュール設定

## ファイバ チャンネルを使用したフェイルオーバー

マルチパスをサポートするため、ホストには通常複数の使用可能な HBA が装備されています。この構成は SAN のマルチパス構成を補完します。SAN のマルチパス構成では一般的に、SAN ファブリックに 1 つ以上のスイッチ、およびストレージ アレイ デバイス自体に 1 つ以上のストレージ プロセッサを提供します。

以下の図では、複数の物理パスで各サーバとストレージ デバイスを接続しています。たとえば、HBA1 または HBA1 と FC スイッチ間のリンクに障害が発生した場合、サーバとスイッチ間の接続は、HBA2 に引き継がれて実行されます。別の HBA に引き継ぐプロセスは、HBA フェイルオーバーと呼ばれます。

図 17-1. ファイバ チャンネルを使用したマルチパスとフェイルオーバー



同様に、SP1 に障害が発生するか、SP1 とスイッチ間のリンクが切断された場合、スイッチとストレージ デバイス間の接続は、SP2 に引き継がれて実行されます。このプロセスは SP フェイルオーバーと呼ばれます。VMware ESXi は、マルチパス機能により、HBA フェイルオーバーと SP フェイルオーバーをサポートします。

## iSCSI でのホスト ベースのフェイルオーバー

ESXi ホストをマルチパスおよびフェイルオーバー用に設定する場合、ホストの iSCSI アダプタのタイプによって、複数の iSCSI HBA、または複数の NIC を使用できます。

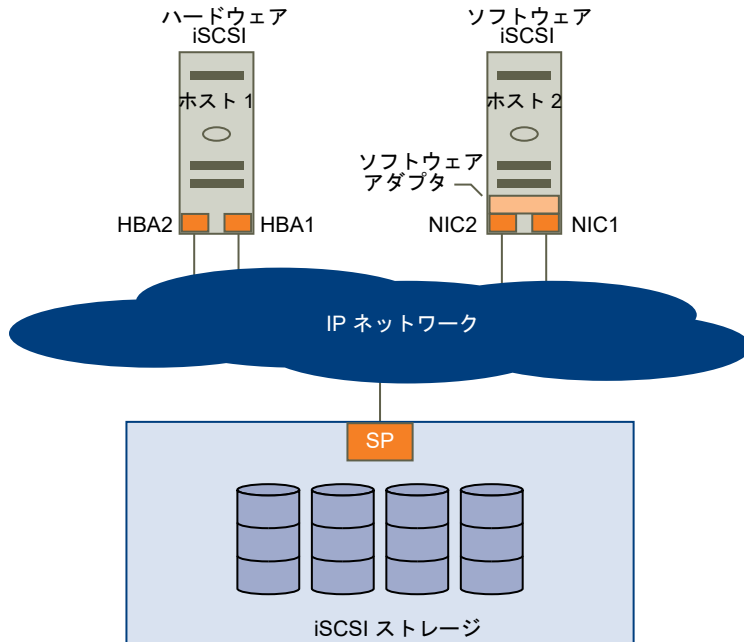
さまざまなタイプの iSCSI アダプタの詳細については、[iSCSI イニシエータ](#)を参照してください。

マルチパスを使用する場合は、特定の考慮事項が適用されます。

- 同じホストで独立型ハードウェア アダプタをソフトウェア iSCSI アダプタまたは依存型 iSCSI アダプタと結合する場合は、ESXi はマルチパスをサポートしません。
- 同じホスト内のソフトウェア アダプタと依存型アダプタ間のマルチパスはサポートされます。
- 異なるホストで、依存型アダプタと独立型アダプタの両方をミックスできます。

次の図は、さまざまなタイプの iSCSI イニシエータで使用可能なマルチパスの設定を示しています。

図 17-2. ホスト ベースのバス フェイルオーバー



## ハードウェア iSCSI のフェイルオーバー

ハードウェア iSCSI を使用すると、ホストには通常複数の使用可能なハードウェア iSCSI アダプタがあり、この iSCSI アダプタから 1 つ以上のスイッチを使用してストレージ システムにアクセスできます。または、アダプタを 1 つ、ストレージ プロセッサを 2 つ設定し、アダプタが異なるバスを使用してストレージ システムにアクセスできるようにします。

ホスト ベースのバス フェイルオーバーの図で、ホスト 1 には HBA1 と HBA2 の 2 つのハードウェア iSCSI アダプタがあり、ストレージ システムへの物理バスが 2 つ提供されます。VMkernel NMP であるかサードパーティ製の MPP であるにかかわらず、ホストのマルチバス プラグインはデフォルトでバスにアクセスでき、各物理バスの健全性を監視できます。たとえば、HBA1 自体、または HBA1 とネットワークとの間のリンクに障害が発生した場合、マルチバス プラグインでバスを HBA2 に切り替えることができます。

## ソフトウェア iSCSI のフェイルオーバー

ホスト ベースのバス フェイルオーバーの図のホスト 2 に示すように、ソフトウェア iSCSI を使用すると複数の NIC を使用でき、ホストとストレージ システム間の iSCSI 接続にフェイルオーバー機能とロード バランシング機能が提供されます。

この設定を行う場合、マルチバス プラグインはホストの物理 NIC に直接アクセスできないため、最初に各物理 NIC を個別の VMkernel ポートに接続する必要があります。その後、ポートのバインド技術を使用して、すべての VMkernel ポートとソフトウェア iSCSI イニシエータを関連付けます。その結果、別個の NIC に接続された各 VMkernel ポートは別々のバスになり、iSCSI ストレージ スタックと iSCSI ストレージ対応のマルチバス プラグインで使用できるようになります。

ソフトウェア iSCSI でのマルチバスの構成方法については、[iSCSI ネットワークの設定](#) を参照してください。

## iSCSI でのアレイ ベースのフェイルオーバー

一部の iSCSI ストレージ システムでは、ポートでのパス利用を自動的、また ESXi に対して透過的に管理します。

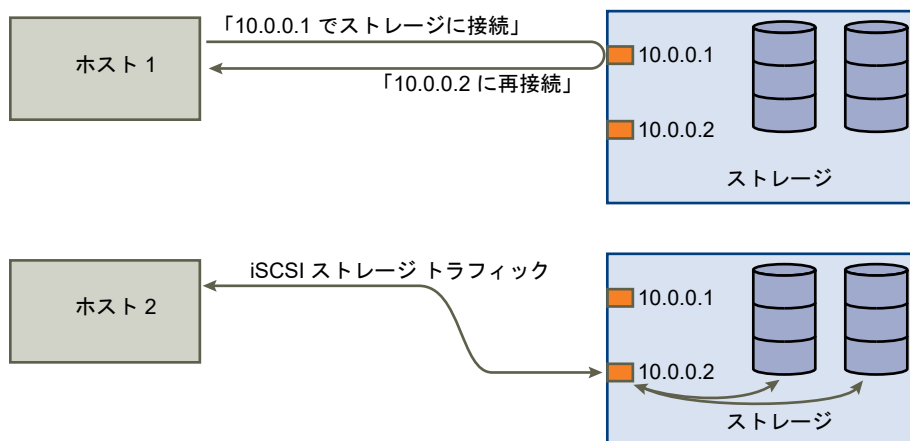
このようなストレージ システムを利用している場合、ホストはストレージ上の複数のポートを認識しないため、接続先のストレージのポートを選択できません。このようなシステムには、ホストが最初に通信を行う単一の仮想ポートアドレスがあります。この最初の通信中にストレージ システムはホストをリダイレクトして、ストレージ システム上の別のポートと通信するようにできます。ホストの iSCSI イニシエータはこの再接続要求に従い、システム上の別のポートに接続します。ストレージ システムはこの技術を使用して、利用可能なポートに負荷を分散します。

ESXi ホストは、あるポートに対する接続が途切れてしまった場合、ストレージ システムの仮想ポートへの再接続を自動的に試み、有効で利用可能なポートにリダイレクトされます。この再接続とリダイレクトは短時間で行われるため、通常は実行中の仮想マシンで中断が発生することはありません。このようなストレージ システムでは iSCSI イニシエータに対し、システムに再接続するよう要求して、接続先のストレージ ポートを変更することもできます。これにより、複数のポートを最大限有効に活用できます。

ポート リダイレクトの図は、ポート リダイレクトの例を示します。ホストは 10.0.0.1 の仮想ポートに接続しようとしています。このリクエストはストレージ システムから 10.0.0.2 にリダイレクトされます。クライアントは 10.0.0.2 に接続され、このポートが I/O 通信で使用されます。

**注：** ストレージ システムが接続をリダイレクトしないことがあります。10.0.0.1 のポートはトラフィック用にも利用できます。

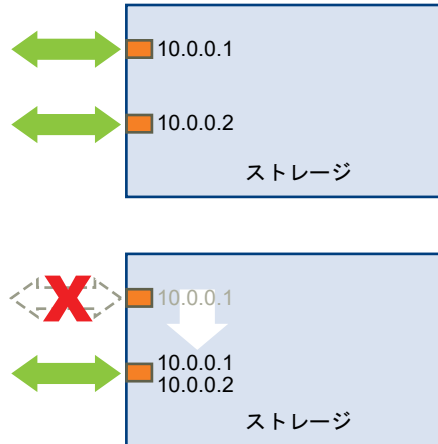
図 17-3. ポート リダイレクト



仮想ポートとして動作しているストレージ システムのポートが利用不可になった場合、ストレージ システムは仮想ポートのアドレスをシステム上にある別のポートに再割り当てします。ポート リダイレクトに、このタイプのポート再割り当ての例を示します。この場合、仮想ポート 10.0.0.1 は利用不可になり、ストレージ システムはその仮想ポートの IP アドレスを別のポートに再割り当てします。両方のアドレスに対し、2 つ目のポートが応答します。



図 17-4. ポート再割り当て



この形式のアレイ ベースのフェイルオーバーでは、ESXi ホストで複数のポートを使用している場合にのみ、ストレージに対して複数のパスを設定できます。これらのパスはアクティブ-アクティブです。詳細については、[iSCSI セッションの管理](#)を参照してください。

## パスのフェイルオーバーと仮想マシン

パスのフェイルオーバーは、LUN へのアクティブなパスが別のパスに変更されると発生します。通常、現在のパスの SAN コンポーネントに発生した障害が原因です。

パスに障害が発生すると、リンクがダウンしているとホストが判断し、フェイルオーバーが終了するまでストレージ I/O は 30 ～ 60 秒間停止する可能性があります。ホスト、ストレージ デバイス、またはアダプタを表示しようとすると、動作が停止したように見えることがあります。仮想マシン（および SAN にインストールされているその仮想ディスク）が応答しないように見えることがあります。フェイルオーバーが完了すると、I/O は正常にレジュームして、仮想マシンは実行を継続します。

ただし、フェイルオーバーの完了に時間がかかると、Windows の仮想マシンは I/O を中断して最終的に障害が発生する場合があります。失敗を回避するには、Windows の仮想マシンのディスク タイムアウト値を少なくとも 60 秒に設定します。

## Windows ゲスト OS にタイムアウトを設定

パスのフェイルオーバー時に中断しないように、Windows ゲスト OS で標準ディスク タイムアウト値を増やします。

この手順は、Windows レジストリを使用してタイムアウト値を変更する方法を説明します。

### 前提条件

Windows レジストリをバックアップします。

### 手順

- 1 [スタート] - [ファイル名を指定して実行] を選択します。
- 2 `regedit.exe` と入力して、[OK] をクリックします。

3 左パネルの階層表示で、[HKEY\_LOCAL\_MACHINE,] - [System,] - [CurrentControlSet,] - [サービス,] - [ディスク] の順にをダブルクリックします。

4 [TimeOutValue] をダブルクリックします。

5 データ値を 0x3c (16 進数) または 60 (10 進数) に設定し、[OK] をクリックします。

このように変更すると、Windows は遅延したディスク処理の完了を 60 秒間待機してから、エラーを生成するようになります。

6 ゲスト OS を再起動して、変更内容を有効にします。

## 複数のパスの管理

ストレージ マルチパスを管理するには、ESXi は、プラグイン可能なストレージ アーキテクチャ (PSA) と呼ばれる Storage API の集合を使用します。PSA は、複数のマルチパス プラグイン (MPP) の動作を同時に調整するオープン モジュラー フレームワークです。PSA によって、サードパーティのソフトウェア開発者は特定のストレージ アレイのために固有のロード バランシング方法とフェイルオーバー メカニズムを設計して、コードを ESXi ストレージ I/O パスに直接挿入することができます。

パスの管理を説明するトピックでは、次の略語を使用します。

表 17-1. マルチパスに関する略語

略語	定義
PSA	プラグ可能ストレージ アーキテクチャ
NMP	ネイティブ マルチパス プラグイン。汎用的な VMware のマルチパス モジュールです。
PSP	パス選択プラグイン。パス選択ポリシーとも呼ばれます。指定したデバイスに対するパスの選択を処理します。
SATP	ストレージ アレイ タイプ プラグイン。ストレージ アレイ タイプ ポリシーとも呼ばれます。指定したストレージ アレイに対するパスのフェイルオーバーを処理します。

ESXi がデフォルトで提供する VMkernel マルチパス プラグインは、VMware ネイティブ マルチパス プラグイン (NMP) です。NMP は、サブプラグインを管理する拡張可能なマルチパス モジュールです。NMP のサブプラグインには、ストレージ アレイ タイプ プラグイン (SATP) およびパス選択プラグイン (PSP) の 2 種類があります。SATP および PSP は、VMware が組み込み式で提供するものと、サードパーティが提供するものがあります。

さらにマルチパス機能が必要であれば、デフォルトの NMP への追加またはその代替として、サードパーティ製の MPP も利用できます。

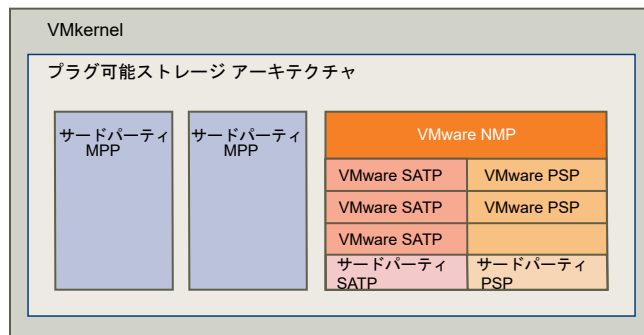
VMware NMP およびインストールされたサードパーティ製の MPP を調整する場合、PSA は次のタスクを実行します。

- マルチパス プラグインをロードおよびアンロードします。
- 仮想マシンの特性を特定のプラグインで非表示にします。
- 特定の論理デバイスに対する I/O 要求を、そのデバイスを管理する MPP にルーティングします。

- 論理デバイスへの I/O キューを処理します。
- 仮想マシン間で論理デバイスのバンド幅共有を実現します。
- 物理ストレージの HBA への I/O キューを処理します。
- 物理バスの検出と削除を処理します。
- 論理デバイスおよび物理バスの I/O 統計を提供します。

プラグ可能ストレージ アーキテクチャの図に示すように、VMware NMP と並行して複数のサードパーティ製 MPP を実行できます。サードパーティ製の MPP をインストールすると、その MPP が NMP に代わって特定のストレージ デバイスに関するバス フェイルオーバーおよびロード バランシングを完全に制御します。

図 17-5. プラグ可能ストレージ アーキテクチャ



マルチパス モジュールは次の操作を行います。

- 物理バスの要求および要求解除を管理します。
- 論理デバイスの作成、登録、および登録解除を管理します。
- 物理バスを論理デバイスに関連付けます。
- バスの障害検出および修正をサポートします。
- 論理デバイスへの I/O 要求を処理します。
  - 要求にとって最適な物理バスを選択します。
  - ストレージ デバイスによっては、バスの障害や I/O コマンドの再試行を処理するのに必要となる特殊なアクションを実行します。
- 論理デバイスのリセットなど、管理タスクをサポートします。

## VMware マルチパス モジュール

デフォルトで ESXi は、ネイティブ マルチパス プラグイン (NMP) と呼ばれる拡張可能なマルチパス モジュールを備えています。

通常、VMware NMP は VMware ストレージ HCL に示されているすべてのストレージ アレイをサポートし、アレイ タイプに基づいてデフォルトのパス選択アルゴリズムを提供します。NMP は、一連の物理パスを特定のストレージ デバイスすなわち LUN に関連付けます。特定のストレージ アレイに対するパスのフェイルオーバーの処理については、ストレージ アレイ タイプ プラグイン (SATP) に具体的な詳細が委ねられます。I/O 要求をストレージ デバイスに発行するためにどの物理パスを使用するか決定については、具体的な詳細はパス選択プラグイン (PSP) によって処理されます。SATP および PSP は、NMP モジュール内のサブプラグインです。

ESXi で、使用しているアレイに適切な SATP が自動的にインストールされます。SATP の入手やダウンロードは必要ありません。

## VMware SATP

ストレージ アレイ タイプ プラグイン (SATP) は VMware NMP と一緒に実行され、アレイ固有の操作を行います。

ESXi は、当社がサポートするすべてのタイプのアレイに対して SATP を提供します。また、非固有のアクティブ-アクティブ ストレージ アレイおよび ALUA ストレージ アレイをサポートするデフォルトの SATP、および直接接続デバイス用のローカル SATP も提供します。各 SATP は特定のクラスのストレージ アレイの特性に対応しており、パスの状態を検出し、無効なパスを有効にするために必要なアレイ固有の操作を実行できます。このため、NMP モジュール自体は、ストレージ デバイスの特性を認識しなくても、複数のストレージ アレイと連携できます。

NMP が、特定のストレージ デバイスに使用する SATP を判断し、その SATP をストレージ デバイスの物理パスに関連付けたあと、SATP は次のようなタスクを実施します。

- 各物理パスの健全性を監視します。
- 各物理パスの状態の変化を報告します。
- ストレージのフェイルオーバーに必要なアレイ固有のアクションを実行します。たとえば、アクティブ-パッシブ デバイスでは、パッシブ パスを有効にできます。

## VMware PSP

パス選択プラグイン (PSP) は VMware NMP のサブ プラグインで、I/O 要求の物理パスの選択を行います。

各論理デバイスに対し、VMware NMP はそのデバイスの物理パスに関連付けられた SATP に基づいて、デフォルトの PSP を割り当てます。デフォルトの PSP はオーバーライドできます。詳細については、[パスのスキャンと要求](#) を参照してください。

デフォルトで、VMware NMP は次の PSP をサポートします。

### VMW\_PSP\_MRU

ホストは最近使用したパスを選択します。パスが使用できなくなると、ホストは代替パスを選択します。元のパスが再び使用できるようになっても、ホストは元のパスに戻りません。MRU ポリシーでは優先パスの設定はありません。MRU はほとんどのアクティブ-パッシブのストレージ デバイスのデフォルト ポリシーです。

VMW\_PSP\_MRU ランク付け機能により、個々のパスにランクを割り当てることができます。個々のパスにランクを設定するには、`esxcli storage nmp psp generic pathconfig set` コマンドを使用します。詳細については、当社のナレッジ ベースの記事 <http://kb.vmware.com/kb/2003468> を参照してください。

最近の使用 (VMware) のパス選択ポリシーとしてクライアントにポリシーが表示されます。

## VMW\_PSP\_FIXED

指定された優先パスが構成されている場合は、ホストはそれを使用します。構成されていない場合、システムの起動時に検出された、機能している最初のパスを選択します。ホストで特定の優先パスが使用されるようにするには、手動で指定します。アクティブ-アクティブのストレージ デバイスのデフォルト ポリシーは固定です。

---

**注：** ホストでデフォルトの優先パスが使用されるときに、そのパスの状態が「非活動」になると、新しいパスが優先パスとして選択されます。ただし、優先パスを明示的に設定すると、パスがアクセス不可になっていても優先パスのままになります。

---

固定 (VMware) のパス選択ポリシーとしてクライアントに表示されます。

## VMW\_PSP\_RR

ホストは、自動パス選択アルゴリズムを使用します。アクティブ-パッシブ アレイに接続しているときはすべてのアクティブなパス、アクティブ-アクティブ アレイに接続しているときはすべての使用可能なパスを巡回します。RR は多数のアレイのデフォルトで、アクティブ-アクティブおよびアクティブ-パッシブ アレイの両方と併用して、異なる LUN のパスでロード バランシングを実装できます。

ラウンド ロビン (VMware) のパス選択ポリシーとしてクライアントに表示されます。

## I/O の VMware NMP フロー

仮想マシンが、NMP によって管理されるストレージ デバイスに I/O 要求を発行するとき、次の処理が実行されます。

- 1 NMP が、このストレージ デバイスに割り当てられた PSP を呼び出します。
- 2 PSP が、I/O の発行先として最適な物理パスを選択します。
- 3 NMP が、PSP で選択されたパスに I/O 要求を発行します。
- 4 I/O 操作に成功した場合、NMP がその完了を報告します。
- 5 I/O 操作でエラーが報告された場合、NMP が適切な SATP を呼び出します。
- 6 SATP が I/O コマンド エラーを解釈し、無効なパスを適宜に有効にします。
- 7 PSP が呼び出され、I/O の発行先となる新しいパスを選択します。

## パスのスキャンと要求

ESXi ホストを起動またはストレージ アダプタを再スキャンすると、ホストは利用可能なストレージ デバイスへのすべての物理パスを検出します。要求ルール セットに基づき、ホストはどのマルチパス プラグイン (MPP) が特定のデバイスへの複数のパスを要求し、そのデバイスのマルチパス サポートを管理すべきかを判断します。

デフォルトでは、ホストは 5 分おきに周期的なパス評価を行い、要求を受けていないパスがあれば、適切な MPP が要求するようにします。

要求ルールには番号がつけられています。各物理パスに対し、ホストは最も小さい番号から要求ルールを調べていきます。物理パスの属性が、要求ルールのパス仕様と比較されます。一致すると、ホストは要求ルールに指定された MPP を物理パスの管理に割り当てます。これは、すべての物理パスが、対応する MPP（サードパーティ製またはネイティブのマルチパス プラグイン（NMP））によって要求されるまで続けられます。

NMP モジュールにより管理されているパスについては、別の要求ルール セットが適用されます。これらの要求ルールにより、特定のアレイ タイプのパスの管理にどのストレージ アレイ タイプ プラグイン（SATP）を使用し、各ストレージ デバイスに対しどのパス選択プラグイン（PSP）を使用すべきかを判断します。

vSphere Web Client を使用して、ホストが特定のストレージ デバイスに対してどの SATP と PSP を使用しているのかを表示し、そのストレージ デバイスに使用可能なすべてのパスの状態を表示します。デフォルトの VMware PSP は、必要に応じてクライアントで変更できます。デフォルトの SATP を変更するには、vSphere CLI を使用して要求ルールを変更する必要があります。

要求ルールの変更については、[ストレージ パスおよびマルチパス プラグインの管理](#) を参照してください。

PSA の管理に使用できるコマンドの詳細については、『vSphere Command-Line Interface スタート ガイド』を参照してください。

ストレージ アレイの完全なリストと対応する SATP および PSP については、『vSphere の互換性ガイド』の「SAN Array Model Reference」（SAN アレイ モデル リファレンス）を参照してください。

## パス情報の表示

ESXi ホストが特定のストレージ デバイスに対して使用しているストレージ アレイ タイプ ポリシー (SATP) およびパス選択ポリシー (PSP)、および当該ストレージ デバイスで利用可能なすべてのパスの状態を確認することができます。データストア ビューおよびデバイス ビューどちらからもパス情報にアクセスできます。データストアの場合、そのデータストアが展開されているデバイスに接続するパスが表示されます。

パス情報には、デバイスを管理するために割り当てられた SATP、PSP、パスのリストおよび各パスのステータスが含まれています。次のパス状態情報が表示されます。

### アクティブ

I/O を LUN に発行するのに使用できるパス。現在データの転送に使用されている単一または複数の機能しているパスはアクティブ（I/O）とマークされます。

### スタンバイ

アクティブなパスに障害が発生すると、パスは素早く作動状態になり、I/O に使用できます。

### 無効

パスが機能しておらず、データを転送できません。

### 非活動

ソフトウェアはこのパス経由でディスクに接続できません。

[固定] パス ポリシーを使用している場合、どのパスが優先パスであるかを確認できます。優先パスには、優先の列がアスタリスク（\*）でマークされます。

バスごとに、バスの名前を表示することも可能です。名前には、アダプタ ID、ターゲット ID、デバイス ID というバスを記述するパラメータが含まれます。アダプタ ID、ターゲット ID およびデバイス ID。通常、バス名は次のようなフォーマットになっています。

```
fc.adapterID-fc.targetID-naa.deviceID
```

---

**注：** バスを編集するためにホスト プロファイル エディタを使用するときは、アダプタ ID、ターゲット ID、デバイス ID というバスを記述するすべての 3 つのパラメータを指定する必要があります。

---

## データストア パスの表示

データストアをバックアップしているストレージ デバイスに接続するパスを確認します。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 データストアをクリックして、その情報を表示します。
- 3 [構成] タブをクリックします。
- 4 [接続およびマルチパス] をクリックします。
- 5 データストアが共有されている場合は、デバイスのマルチパスの詳細を表示するホストを選択します。
- 6 マルチパスの詳細で、データストアをバックアップしているストレージ デバイスのマルチパス ポリシーおよびパスを確認します。

## ストレージ デバイス パスの表示

ホストが特定のストレージ デバイスで使用するマルチパス ポリシー、当該ストレージ デバイスで利用可能なすべてのパスの状態を表示します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ デバイス] をクリックします。
- 4 パスを表示するストレージ デバイスを選択します。
- 5 マルチパス ポリシーで [プロパティ] タブをクリックして、詳細を確認してください。
- 6 ストレージ デバイスで利用可能なすべてのパスを確認するには、[パス] タブをクリックします。

## パス選択ポリシーの設定

ストレージ デバイスごとに、ESXi ホストは、要求ルールに基づきパス選択ポリシーを設定します。

デフォルトで、次のパス選択ポリシーがサポートされます。ホストにサードパーティ製の PSP をインストールしている場合、そのポリシーもリストに表示されます。

### 固定 (VMware)

指定された優先パスが構成されている場合は、ホストはそれを使用します。構成されていない場合、システムの起動時に検出された、機能している最初のパスを選択します。ホストで特定の優先パスが使用されるようにするには、手動で指定します。アクティブ-アクティブのストレージ デバイスのデフォルト ポリシーは固定です。

**注：** ホストでデフォルトの優先パスが使用されるときに、そのパスの状態が「非活動」になると、新しいパスが優先パスとして選択されます。ただし、優先パスを明示的に設定すると、パスがアクセス不可になっていても優先パスのままになります。

## 最近の使用 (VMware)

ホストは最近使用したパスを選択します。パスが使用できなくなると、ホストは代替パスを選択します。元のパスが再び使用できるようになっても、ホストは元のパスに戻りません。MRU ポリシーでは優先パスの設定はありません。MRU はほとんどのアクティブ-パッシブのストレージ デバイスのデフォルト ポリシーです。

## ラウンド ロビン (VMware)

ホストは、自動パス選択アルゴリズムを使用します。アクティブ-パッシブ アレイに接続しているときはすべてのアクティブなパス、アクティブ-アクティブ アレイに接続しているときはすべての使用可能なパスを巡回します。RR は多数のアレイのデフォルトで、アクティブ-アクティブおよびアクティブ-パッシブ アレイの両方と併用して、異なる LUN のパスでロード バランシングを実装できます。

## パス選択ポリシーの変更

一般的に、ホストが特定のストレージ デバイスに使用しているデフォルトのマルチパス設定を変更する必要はありません。ただし変更する場合、[マルチパス ポリシーの編集] ダイアログ ボックスを使用してパス選択ポリシーを変更し、固定ポリシーで優先するパスを指定できます。このダイアログ ボックスを使用して、SCSI ベースのプロトコル エンドポイントのマルチパスを変更することもできます。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ デバイス] または [プロトコル エンドポイント] をクリックします。
- 4 パスを変更するアイテムを選択して、[プロパティ] タブをクリックします。
- 5 [マルチパス ポリシー] で、[マルチパスの編集] をクリックします。
- 6 パス ポリシーを選択します。

デフォルトで、次のパス選択ポリシーがサポートされます。ホストにサードパーティ製の PSP をインストールしている場合、そのポリシーもリストに表示されます。

- 固定 (VMware)
- 最近の使用 (VMware)
- ラウンド ロビン (VMware)

- 7 固定ポリシーでは、優先パスを指定します。
- 8 [OK] をクリックして設定内容を保存し、ダイアログ ボックスを閉じます。



## ストレージ パスの無効化

メンテナンスなどの目的で、一時的にパスを無効にできます。

パス パネルを使用して、パスを無効化できます。パス パネルにアクセスするにはさまざまな方法があります。データストア、ストレージ デバイス、またはアダプタ ビューからアクセスできます。このタスクは、ストレージ デバイス ビューを使用してパスを無効化する方法を説明します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [ストレージ デバイス] をクリックします。
- 4 無効化するパスのストレージ デバイスを選択して、[パス] タブをクリックします。
- 5 無効化するパスを選択して、[無効] をクリックします。

## ストレージ パスおよびマルチパス プラグインの管理

`esxcli` コマンドを使用して、PSA マルチパス プラグインとそれに割り当てられたストレージ パスを管理できます。

ホストで使用可能なすべてのマルチパス プラグインを表示できます。ホストの NMP および SATP に加え、サードパーティ製 MPP をリスト表示し、要求されるパスを確認できます。新しいパスを定義し、どのマルチパス プラグインがそのパスを要求するのかを指定することもできます。

PSA の管理に使用可能なコマンドの詳細については、『Getting Started with vSphere Command-Line Interfaces』を参照してください。

### マルチパスの考慮事項

ストレージ マルチパス プラグインと要求ルールを管理するとき、特定の考慮事項が適用されます。

次の考慮事項がマルチパスに役立ちます。

- 要求ルールによってデバイスに割り当てられる SATP が存在しない場合、iSCSI デバイスまたは FC デバイスのデフォルト SATP は `VMW_SATP_DEFAULT_AA` になります。デフォルト PSP は `VMW_PSP_FIXED` です。
- システムが SATP ルールを検索して、あるデバイスの SATP を見つけ出す場合、最初にドライバ ルールを検索します。マッチしなければベンダー ルールまたはモデル ルールを検索し、最後にトランスポート ルールを検索します。マッチしなければ、NMP はそのデバイスのデフォルトの SATP を選択します。
- `VMW_SATP_ALUA` が特定のストレージ デバイスに割り当てられていて、そのデバイスが ALUA 対応ではない場合、このデバイスにマッチする要求ルールはありません。そのデバイスは、デバイスのトランスポート タイプに基づき、デフォルト SATP が要求します。
- `VMW_SATP_ALUA` が要求するすべてのデバイスのデフォルト PSP は `VMW_PSP_MRU` です。`VMW_PSP_MRU` は、`VMW_SATP_ALUA` が報告する有効/最適化状態のパス、または有効/最適化状態

のパスがない場合は、有効/非最適化状態のパスを選択します。これよりも状態の良いパスが見つかるまで、このパスが使用されます (MRU)。たとえば現在 VMW\_PSP\_MRU が有効/非最適化状態のパスを使用していて、有効/最適化状態のパスが使用可能になったとすると、VMW\_PSP\_MRU は現在のパスを有効/最適化状態のパスにスイッチします。

- デフォルトでは通常、ALUA アレイに VMW\_PSP\_MRU が選択されていますが、特定の ALUA ストレージアレイでは VMW\_PSP\_FIXED を使用する必要があります。使用しているストレージアレイで VMW\_PSP\_FIXED が必要かどうかを確認するには、『VMware 互換性ガイド』を参照するか、ストレージベンダーにお問い合わせください。ALUA アレイで VMW\_PSP\_FIXED を使用するときは、優先パスを明示的に指定する場合を除き、ESXi ホストで機能している最適なパスを選択してそのパスをデフォルトの優先パスに設定します。ホストで選択したパスが使用できなくなると、ホストは使用可能な代替パスを選択します。ただし、優先パスを明示的に設定すると、ステータスにかかわらず優先パスが使用されます。
- デフォルトでは、PSA 要求ルール 101 は、Dell アレイ擬似デバイスをマスクします。このデバイスのマスクを解除する場合以外は、このルールを削除しないでください。

## ホストのマルチパスの要求ルールの一覧表示

esxcli コマンドを使用して、使用可能なマルチパスの要求ルールをリスト表示します。

要求ルールでは、どのマルチパス プラグイン、NMP、またはサードパーティ製 MPP が特定の物理パスを管理するかを指定します。各要求ルールでは、次のパラメータに基づいてパスのセットを識別します。

- ベンダーまたはモデルの文字列
- SATA、IDE、ファイバ チャネルなどのトランスポート
- アダプタ、ターゲット、または LUN の場所
- デバイス ドライバ (たとえば Mega-RAID)

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- ◆ **esxcli --server=server\_name storage core claimrule list --claimrule-class=MP** コマンドを実行して、マルチパス要求ルールをリスト表示します。

### 例：esxcli storage core claimrule list コマンドのサンプル出力

Rule	Class	Rule	Class	Type	Plugin	Matches	MP	0	runtime
transport	NMP		transport=usb	MP	1	runtime	transport	NMP	
transport=sata	MP		2	runtime	transport	NMP	transport=ide	MP	

3	runtime	transport	NMP	transport=block	MP	4	runtime	transport
NMP	transport=unknown	MP	101	runtime	vendor	MASK_PATH	vendor=DELL	
model=Universal	Xport	MP	101	file	vendor	MASK_PATH	vendor=DELL	
model=Universal	Xport	MP	200	runtime	vendor	MPP_1	vendor=NewVend	
model=* MP	200	file	vendor	MPP_1	vendor=NewVend	model=* MP		
201	runtime	location	MPP_2	adapter=vmhba41	channel=* target=* lun=* MP			
201	file	location	MPP_2	adapter=vmhba41	channel=* target=* lun=* MP			
202	runtime	driver	MPP_3	driver=megaraid	MP	202	file	driver
MPP_3	driver=megaraid	MP	65535	runtime	vendor	NMP	vendor=* model=*	

この例は次のような意味です。

- NMP は、USB、SATA、IDE、およびブロック SCSI トランスポートを使用するストレージ デバイスに接続されているすべてのパスを要求します。
- MASK\_PATH モジュールを使用して、使用されていないデバイスをホストから隠します。デフォルトで、PSA 要求ルール 101 は、DELL のベンダー文字列と Universal Xport のモデル文字列で Dell アレイ擬似デバイスをマスクします。
- MPP\_1 モジュールは、NewVend ストレージ アレイの任意のモデルに接続されているすべてのパスを要求します。
- MPP\_3 モジュールは、Mega-RAID デバイス ドライバが制御するストレージ デバイスへのパスを要求します。
- 前述のルールに記載されていないすべてのパスは、NMP が要求します。
- 出力の Rule Class 列は、要求ルールのカテゴリを示します。カテゴリは、MP（マルチパス プラグイン）、Filter（フィルタ）、または VAAI のいずれかです。
- Class 列は、定義されているルールとロードされているルールを示します。Class 列の file パラメータは、ルールが定義されていることを表します。runtime パラメータは、ルールがシステムにロードされたことを表します。ユーザー定義の要求ルールを有効にするには、同じルール番号の行が 2 つ存在しなければなりません。1 つは file パラメータの行で、もう 1 つは runtime の行です。数字が小さいルールのいくつかでは、Class が runtime となっている 1 行だけの行があります。これらはシステム定義の要求ルールで、ユーザーが変更することはできません。

## マルチパス モジュールの表示

esxcli コマンドを使用して、システムにロードされているすべてのマルチパス モジュールをリスト表示します。マルチパス モジュールは、ホストとストレージとを接続する物理パスを管理します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

## 手順

- ◆ マルチパス モジュールをリスト表示するには、次のコマンドを実行します。

```
esxcli --server=server_name storage core plugin list --plugin-class=MP
```

## 結果

このコマンドは通常、NMP を表示し、ロードされている場合には MASK\_PATH モジュールを表示します。何らかのサードパーティ製 MPP がロードされている場合、それもリスト表示されます。

## ホストの SATP の表示

esxcli コマンドを使用して、システムにロードされている VMware NMP SATP をリスト表示します。SATP に関する情報を表示します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

## 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

## 手順

- ◆ VMware SATP をリスト表示するには、次のコマンドを実行します。

```
esxcli --server=server_name storage nmp satp list
```

## 結果

この出力は各 SATP について、その SATP がサポートするストレージ アレイまたはシステムのタイプや、その SATP を使用しているすべての LUN のデフォルト PSP に関する情報を表示します。[説明] 列の Placeholder (plugin not loaded) は、SATP がロードされていないことを示します。

## NMP ストレージ デバイスの表示

esxcli コマンドを使用して、VMware NMP が制御するすべてのストレージ デバイスをリスト表示し、各デバイスに関連する SATP および PSP の情報を表示します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

## 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

## 手順

- ◆ すべてのストレージ デバイスを一覧表示するには、次のコマンドを実行します。

```
esxcli --server=server_name storage nmp device list
```

**--device** | **-d=device\_ID** オプションを使用して、このコマンドの出力をフィルタして、単一のデバイスを表示します。

## マルチパスの要求ルールの追加

`esxcli` コマンドを使用して、新規のマルチパス PSA 要求ルールをシステムの要求ルール セットに追加します。新規の要求ルールを有効にするには、まずルールを定義し、次にそれを使用しているシステムにロードします。

新規の PSA 要求ルールを追加するのは、たとえば、新規のマルチパス プラグイン (MPP) をロードし、このモジュールが要求するパスを定義する必要がある場合です。新規のパスを追加して、既存の MPP にそのパスを要求させる場合は、要求ルールの作成が必要になることがあります。

**注意：** 要求ルールを新規作成するときは、複数の MPP が同一 LUN に対して異なる物理パスを要求しないように注意してください。MPP の 1 つが MASK\_PATH MPP である場合を除いて、この構成はパフォーマンス上の問題を起こします。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

## 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

## 手順

- 1 新規の要求ルールを定義するには、次のコマンドを実行します。

```
esxcli --server=server_name storage core claimrule add
```

このコマンドには次のオプションがあります。

オプション	説明
<b>-A --adapter=&lt;str&gt;</b>	この操作で使用するパスのアダプタを指定します。
<b>-u --autoassign</b>	システムが自動的にルール ID を割り当てます。
<b>-C --channel=&lt;long&gt;</b>	この操作で使用するパスのチャネルを指定します。

オプション	説明
<b>-c --claimrule-class=&lt;str&gt;</b>	この操作で使用する要求ルールのクラスを指定します。 有効な値：MP, Filter, VAAI。
<b>-d --device=&lt;str&gt;</b>	この操作で使用するデバイス Uid を指定します。
<b>-D --driver=&lt;str&gt;</b>	この操作で使用するバスのドライバを指定します。
<b>-f --force</b>	要求ルールで妥当性チェックを無視し、ルールを設定するように強制します。
<b>--if-unset=&lt;str&gt;</b>	この上級ユーザー変数が 1 に設定されていない場合にはこのコマンドを実行します。
<b>-i --iqn=&lt;str&gt;</b>	この操作で使用するターゲットの iSCSI 修飾名を指定します。
<b>-L --lun=&lt;long&gt;</b>	この操作で使用するバスの LUN を指定します。
<b>-M --model=&lt;str&gt;</b>	この操作で使用するバスのモデルを指定します。
<b>-P --plugin=&lt;str&gt;</b>	この操作で使用する PSA プラグインを指定します。(必須)
<b>-r --rule=&lt;long&gt;</b>	この操作で使用するルール ID を指定します。
<b>-T --target=&lt;long&gt;</b>	この操作で使用するバスのターゲットを指定します。
<b>-R --transport=&lt;str&gt;</b>	この操作で使用するバスのトランスポートを指定します。 有効な値：block、fc、iscsi、iscsivendor、ide、sas、sata、usb、parallel、unknown
<b>-t --type=&lt;str&gt;</b>	claim、unclaim、または claimrule で使用する一致のタイプを指定します。 有効な値：vendor、location、driver、transport、device、target。(必須)
<b>-V --vendor=&lt;str&gt;</b>	この操作で使用するバスのベンダーを指定します。
<b>--wwnn=&lt;str&gt;</b>	この操作で使用するターゲットのワールド ワイド ノード番号を指定します。
<b>--wwpn=&lt;str&gt;</b>	この操作で使用するターゲットのワールド ワイド ポート番号を指定します。

- 2 システムに新規の要求ルールをロードするには、次のコマンドを実行します。

```
esxcli --server=server_name storage core claimrule load
```

このコマンドは、新規作成されたマルチバスの要求ルールすべてを、システムの構成ファイルからロードします。

### 例：マルチバスの要求ルールの定義

次の例では、ルール番号 500 を追加およびロードして、モデル文字列に NewMod およびベンダー文字列に NewVend を持つすべてのバスを NMP プラグインに要求します。

```
# esxcli --server=server_name storage core claimrule add -r 500 -t vendor -V  
NewVend -M NewMod -P NMP
```

```
# esxcli --server=server_name storage core claimrule load
```

**esxcli --server=server\_name storage core claimrule list** コマンドを実行すると、リストに新規の要求ルールが表示されることを確認できます。

**注：** この要求ルールの 2 つの行（1 つは runtime クラスで、もう 1 つは file クラス）は、新規の要求ルールがシステムにロードされてアクティブであることを表します。

Rule	Class	Rule	Class	Type	Plugin	Matches	MP	0	runtime
transport	NMP		transport=usb	MP		1	runtime	transport	NMP
transport=sata	MP		2	runtime	transport	NMP		transport=ide	MP
3	runtime	transport	NMP		transport=block	MP		4	runtime
NMP		transport=unknown	MP		101	runtime	vendor	MASK_PATH	vendor=DELL
model=Universal	Xport	MP		101	file	vendor		MASK_PATH	vendor=DELL
model=Universal	Xport	MP		500	runtime	vendor	NMP		vendor=NewVend
model=NewMod	MP		500	file	vendor	NMP		vendor=NewVend	model=NewMod

## マルチパスの要求ルールの削除

esxcli コマンドを使用して、マルチパス PSA 要求ルールをシステムの要求ルール セットから削除します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- 1 ある要求ルールを要求ルール セットから削除します。

**esxcli --server=server\_name storage core claimrule remove**

**注：** デフォルトでは、PSA 要求ルール 101 は、Dell アレイ擬似デバイスをマスクします。このデバイスのマスクを解除する場合以外は、このルールを削除しないでください。

このコマンドには次のオプションがあります。

オプション	説明
<b>-c --claimrule-class=&lt;str&gt;</b>	この操作で使用する要求ルールのクラスを指定します（MP、Filter、VAAI）。
<b>-P --plugin=&lt;str&gt;</b>	この操作で使用するプラグインを指定します。
<b>-r --rule=&lt;long&gt;</b>	この操作で使用するルール ID を指定します。

この手順は、File クラスから要求ルールを削除します。

- 2 システムから要求ルールを削除します。

```
esxcli --server=server_name storage core claimrule load
```

この手順は、Runtime クラスから要求ルールを削除します。

## パスのマスク

ホストがストレージ デバイスや LUN にアクセスできないよう、または LUN への個々のパスを使用できないように設定できます。esxcli コマンドを使用して、パスをマスクします。パスをマスクする場合、指定したパスに MASK\_PATH プラグインを割り当てる要求ルールを作成します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- 1 次に使用可能なルール ID を確認します。

```
esxcli --server=server_name storage core claimrule list
```

パスのマスクに使用する要求ルールでは、ルール ID を 101 ~ 200 の範囲とします。前述のコマンドでルール 101 と 102 がすでに存在していることが判明したら、追加するルールとして 103 を指定できます。

- 2 プラグインの新しい要求ルールを作成し、MASK\_PATH プラグインをパスに割り当てます。

```
esxcli --server=server_name storage core claimrule add -P MASK_PATH
```

- 3 MASK\_PATH 要求ルールをシステムにロードします。

```
esxcli --server=server_name storage core claimrule load
```

- 4 MASK\_PATH 要求ルールが正しく追加されたことを確認します。

```
esxcli --server=server_name storage core claimrule list
```

- 5 マスクされたパスに要求ルールがある場合は、そのルールを削除します。

```
esxcli --server=server_name storage core claiming unclaim
```

- 6 パス要求ルールを実行します。

```
esxcli --server=server_name storage core claimrule run
```

### 結果

MASK\_PATH プラグインをパスに割り当てると、パスの状態が不明になり、ホストで管理できなくなります。その結果、マスクされているパスの情報を表示するコマンドを使用すると、パスの状態は非活動であると表示されます。



## 例：LUN のマスキング

この例では、ストレージ アダプタ vmhba2 および vmhba3 を介してアクセスされるターゲット T1 および T2 の LUN 20 をマスクします。

```
1 #esxcli --server=server_name storage core claimrule list

2 #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 109 -t location -A vmhba2 -C 0 -T 1 -L 20 #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 110 -t location -A vmhba3 -C 0 -T 1 -L 20 #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 111 -t location -A vmhba2 -C 0 -T 2 -L 20 #esxcli --server=server_name storage core claimrule add -P MASK_PATH -r 112 -t location -A vmhba3 -C 0 -T 2 -L 20

3 #esxcli --server=server_name storage core claimrule load

4 #esxcli --server=server_name storage core claimrule list

5 #esxcli --server=server_name storage core claiming unclaim -t location -A vmhba2 #esxcli --server=server_name storage core claiming unclaim -t location -A vmhba3

6 #esxcli --server=server_name storage core claimrule run
```

## パスのマスク解除

ホストがマスクされたストレージ デバイスにアクセスする必要がある場合、そのデバイスのパスのマスクを解除します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

**注：** デバイス ID、ベンダー、モデルなどのデバイス プロパティを使用して要求解除操作を実行したとき、MASK\_PATH プラグインによるパスの要求は解除されません。MASK\_PATH プラグインは、要求したパスのデバイス プロパティを追跡しません。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- 1 MASK\_PATH 要求ルールを削除します。

```
esxcli --server=server_name storage core claimrule remove -r rule#
```

- 2 要求ルールが正しく削除されたことを確認します。

```
esxcli --server=server_name storage core claimrule list
```

- 3 バスの要求ルールを構成ファイルから VMkernel に再ロードします。

```
esxcli --server=server_name storage core claimrule load
```

- 4 マスクされたストレージ デバイスへのバスごとに

```
esxcli --server=server_name storage core claiming unclaim
```

 コマンドを実行します。

例：

```
esxcli --server=server_name storage core claiming unclaim -t location -A
vmhba0 -C 0 -T 0 -L 149
```

- 5 バス要求ルールを実行します。

```
esxcli --server=server_name storage core claimrule run
```

## 結果

これで、ホストは、今までマスクされていたストレージ デバイスにアクセスできます。

## NMP SATP ルールの定義

NMP SATP 要求ルールでは、あるストレージ デバイスをどの SATP で管理するのかを指定します。通常、NMP SATP ルールを修正する必要はありません。必要がある場合は `esxcli` コマンドを使用して、指定の SATP 要求ルールのリストにルールを追加します。

特定のストレージ アレイ用にサードパーティ製の SATP をインストールする場合は、SATP ルールを作成する必要がある場合があります。

手順中、`--server=server_name` で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

## 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

## 手順

- 1 特定の SATP 用の要求ルールを追加するには、

**esxcli --server=server\_name storage nmp satp rule add** コマンドを実行します。このコマンドには次のオプションがあります。

オプション	説明
<b>-b --boot</b>	これは、起動時に追加されるシステムのデフォルト ルールです。esx.conf を修正したり、ホスト プロファイルに追加しないでください。
<b>-c --claim-option=string</b>	SATP 要求ルールを追加するときに、要求のオプション文字列を設定します。
<b>-e --description=string</b>	SATP 要求ルールを追加するときに、要求ルールの説明を設定します。
<b>-d --device=string</b>	SATP 要求ルールを追加するときに、デバイスを設定します。デバイスのルールは、ベンダーまたはモデルのルール、およびドライバのルールと相互に排他的です。
<b>-D --driver=string</b>	SATP 要求ルールを追加するときに、ドライバ文字列を設定します。ドライバのルールは、ベンダーまたはモデルのルールと相互に排他的です。
<b>-f --force</b>	要求ルールで妥当性チェックを無視し、ルールを設定するように強制します。
<b>-h --help</b>	ヘルプ メッセージを表示します。
<b>-M --model=string</b>	SATP 要求ルールを追加するときに、モデル文字列を設定します。ベンダーまたはモデルのルールは、ドライバのルールと相互に排他的です。
<b>-o --option=string</b>	SATP 要求ルールを追加するときに、オプション文字列を設定します。
<b>-P --psp=string</b>	SATP 要求ルールのデフォルトの PSP を設定します。
<b>-O --psp-option=string</b>	SATP 要求ルールの PSP オプションを設定します。
<b>-s --satp=string</b>	新規ルールを追加する SATP です。
<b>-R --transport=string</b>	SATP 要求ルールを追加するときに、要求のトランスポート タイプ文字列を設定します。
<b>-t --type=string</b>	SATP 要求ルールを追加するときに、要求タイプを設定します。
<b>-V --vendor=string</b>	SATP 要求ルールを追加するときに、ベンダー文字列を設定します。ベンダーまたはモデルのルールは、ドライバのルールと相互に排他的です。

**注：** SATP ルールを検索して、あるデバイスの SATP を見つけ出す場合、NMP は最初にドライバ ルールを検索します。マッチしなければベンダー ルールまたはモデル ルールを検索し、最後にトランスポート ルールを検索します。ここでもマッチしなければ、NMP はそのデバイスのデフォルトの SATP を選択します。

- 2 ホストを再起動します。

## 例： NMP SATP ルールの定義

次のサンプル コマンドでは、VMW\_SATP\_INV プラグインを割り当て、ベンダー文字列に NewVend およびモデル文字列に NewMod を持つストレージ アレイを管理します。

```
# esxcli --server=server_name storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

**esxcli --server=server\_name storage nmp satp list -s VMW\_SATP\_INV** コマンドを実行すると、VMW\_SATP\_INV ルールのリストに追加された新しいルールを参照できます。

## 仮想マシン I/O のキューのスケジュール設定

vSphere には、デフォルトで、すべての仮想マシン ファイルのキューのスケジュールを作成するメカニズムが用意されています。たとえば、.vmdk などの各ファイルには、それ独自のバンド幅制御が適用されます。

このメカニズムにより、.vmdk などの特定の仮想マシン ファイルの I/O が独自の別個のキューに送られ、他のファイルからの I/O と干渉することのないようにします。

この機能はデフォルトで有効化されています。この機能は、システムの詳細設定で `VMkernel.Boot.isPerFileSchedModelActive` パラメータの値を調整することによって、必要に応じて無効化できます。

### ファイル I/O ごとのスケジュールの編集

`VMkernel.Boot.isPerFileSchedModelActive` 詳細パラメータでは、ファイル I/O ごとのスケジュールメカニズムが制御されます。このメカニズムはデフォルトで有効になっています。

#### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [システム] メニューの [システムの詳細設定] をクリックします。
- 4 [システムの詳細設定] で [VMkernel.Boot.isPerFileSchedModelActive] パラメータを選択して、[編集] アイコンをクリックします。
- 5 以下のいずれかのオプションを選択します：
  - ファイルごとのスケジュール メカニズムを無効にするには、値を [いいえ] に変更します。

---

**注：** ファイル I/O ごとのスケジュール モデルを無効にすると、ホストは、1 つの I/O キューを使用する以前のスケジュール メカニズムに戻ります。ホストは、仮想マシンとストレージ デバイスの各ペアに 1 つの I/O キューを保持します。仮想マシンとストレージ デバイスに格納されている仮想ディスクとの間のすべての I/O が、このキューに移動されます。その結果、バンド幅の共有時にさまざまな仮想ディスクからの I/O が互いに干渉し、互いのパフォーマンスに影響を及ぼす可能性があります。

---

- ファイルごとのスケジュール メカニズムを再度有効にするには、値を [はい] に変更します。

- 6 ホストを再起動して、変更内容を有効にします。

### esxcli コマンドを使用したファイル I/O ごとのスケジュールの有効化または無効化

esxcli コマンドを使用して、I/O のスケジュール機能を変更できます。この機能はデフォルトで有効化されています。

手順中、`--server=server_name` で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

## 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

## 手順

- ◆ ファイルごとの I/O スケジュールを有効または無効にするには、次のコマンドを実行します。

オプション	説明
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE</code>	ファイルごとの I/O スケジュールの無効化
<code>esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE</code>	ファイルごとの I/O スケジュールの有効化

Raw デバイス マッピング (RDM) を使用すると、仮想マシンから物理ストレージ サブシステム上の LUN に直接アクセスできるようになります。

次のトピックには、RDM に関する情報が含まれています。また、RDM を作成および管理する方法についても記載されています。

この章には、次のトピックが含まれています。

- Raw デバイス マッピングについて
- Raw デバイス マッピングの特性
- RDM を使用する仮想マシンの作成
- マッピング済み LUN のパス管理

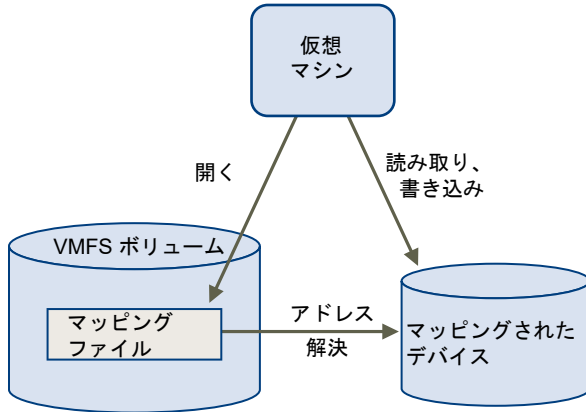
## Raw デバイス マッピングについて

RDM は別個の VMFS ボリュームにあるマッピング ファイルであり、Raw 物理ストレージ デバイスのプロキシとして機能します。RDM によって、仮想マシンはストレージ デバイスに直接アクセスして使用できるようになります。RDM には、物理デバイスへのディスク アクセスを管理およびリダイレクトするためのメタデータが格納されています。

このファイルを使用すると、VMFS 内の仮想ディスクを利用できると同時に、物理デバイスに直接アクセスできます。したがって、このファイルによって VMFS の管理性と Raw デバイス アクセスとが結合されます。

RDM は、「Raw デバイスのデータストアへのマッピング」、「システム LUN のマッピング」、「ディスク ファイルの物理ディスク ボリュームへのマッピング」などの言葉で表すことができます。これらの言葉はすべて、RDM を表しています。

図 18-1. Raw デバイス マッピング



ほとんどの場合、仮想ディスクのストレージには VMFS データストアを使用することをお勧めしますが、ある特定の状況においては Raw LUN（SAN 内にある論理ディスク）を使用する必要がある場合があります。

たとえば、次の場合に RDM で Raw LUN を使用する必要があります。

- SAN スナップショットまたはその他のレイヤー アプリケーションを仮想マシンで実行している場合。RDM は、SAN 固有の機能を使用することによって拡張性の高いバックアップ負荷軽減システムを実現します。
- 仮想クラスタから仮想クラスタ、および物理クラスタから仮想クラスタに、物理ホストを展開する MSCS クラスタリングの場合。この場合、クラスタ データおよびクォーラム ディスクは、共有 VMFS の仮想ディスクではなく RDM として構成する必要があります。

RDM は、VMFS ボリュームから Raw LUN へのシンボル リンクとして考えます。マッピングにより、LUN は VMFS ボリューム内のファイルとして認識されるようになります。Raw LUN ではない RDM は、仮想マシン構成で参照されます。RDM には、Raw LUN への参照が含まれています。

RDM を使用すると、次の処理を実行できます。

- vMotion を使用して、Raw LUN で仮想マシンを移行する。
- vSphere Web Client を使用して、RAW LUN を仮想マシンに追加する。
- 分散ファイル ロック、許可、ネーミングなどのファイル システム機能を使用する。

RDM で、次の 2 つの互換モードを使用できます。

- 仮想互換モードでは、スナップショットの使用など、仮想ディスク ファイルと同様に RDM が機能します。
- 物理互換モードでは、低レベル制御が必要なアプリケーションで、SCSI デバイスの直接アクセスが可能です。

## Raw デバイス マッピングのメリット

RDM には多くのメリットがありますが、すべての状況に該当するわけではありません。通常、仮想ディスク ファイルは、管理性の面で RDM よりも優れています。ただし、Raw デバイスが必要な場合、RDM を使用する必要があります。

RDM には、いくつかのメリットがあります。

### わかりやすく永続的な名前

マッピング済みのデバイスに、わかりやすい名前を提供します。RDM を使用する場合、デバイスをそのデバイス名で示す必要はありません。参照するには、マッピング ファイルの名前を使用します。次に例を示します。

```
/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
```

### 動的名前解決

マッピング済みの各デバイスの一意の ID 情報を保存します。VMFS は、アダプタ ハードウェアの変更、バスの変更、デバイスの移動などによりサーバの物理構成に変更が発生しても、現在の SCSI デバイスと各 RDM を関連付けます。

### 分散ファイル ロック

Raw SCSI デバイスの VMFS 分散ロックを使用できます。RDM で分散ロックを使用することにより、別のサーバにある 2 個の仮想マシンが同じ LUN にアクセスしようとしても、データを消失することなく、共有の Raw LUN を安全に使用できます。

### ファイル権限

ファイル権限を使用できます。マッピング ファイルの権限は、マッピング済みのボリュームを保護するため、ファイルを開くときに使用されます。

### ファイル システムの操作

マッピング ファイルをプロキシとして使用して、マッピング済みのボリュームで、ファイル システム ユーティリティを使用できます。通常のファイルに有効なほとんどの操作は、マッピング ファイルに適用でき、マッピング済みのデバイスで機能するようにリダイレクトされます。

### スナップショット

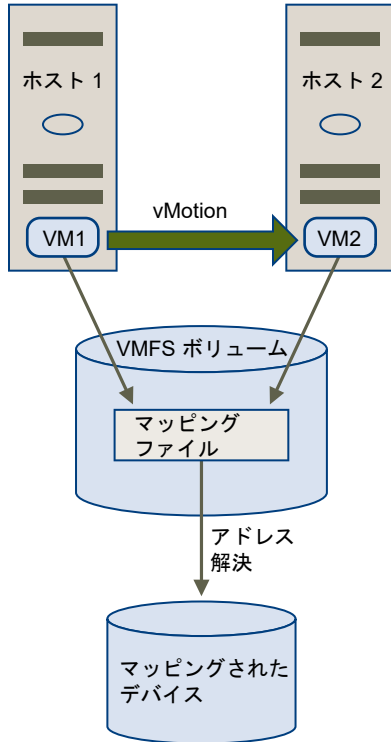
マッピング済みのボリュームで仮想マシンのスナップショットを使用できます。RDM が物理互換モードで使用されている場合、スナップショットは使用できません。

### vMotion

vMotion を使用して仮想マシンの移行ができます。マッピング ファイルはプロキシとして機能し、仮想ディスク ファイルの移行と同じメカニズムを使用することで、vCenter Server が仮想マシンを移行できるようにします。



図 18-2. Raw デバイス マッピングを使用した仮想マシンの vMotion



### SAN 管理エージェント

仮想マシン内で一部の SAN 管理エージェントを実行できます。同様に、ハードウェア固有の SCSI コマンドを使用することにより、デバイスにアクセスする必要があるソフトウェアも仮想マシン内で実行できます。このようなソフトウェアは、「SCSI ターゲット ベース ソフトウェア」と呼ばれます。SAN 管理エージェントを使用する場合、RDM で物理互換モードを選択します。

### N-Port ID 仮想化 (NPIV)

複数の Worldwide ポート名 (WWPN) を使用して 1 つのファイバチャネル HBA ポートをファイバチャネル ファブリックに登録できる NPIV テクノロジーを使用できます。これによって HBA ポートは、それぞれが独自の ID と仮想ポート名を持つ複数の仮想ポートとして表示されます。仮想マシンは、各仮想ポートを要求し、すべての RDM トラフィックに使用できます。

**注：** NPIV は、RDM ディスクを使用している仮想マシンにのみ使用できます。

当社は、ストレージ管理ソフトウェアのベンダーと協力して、ESXi を含む環境でのソフトウェアの正常な動作を実現しています。このようなアプリケーションのいくつかを次に示します。

- SAN 管理ソフトウェア
- ストレージ リソース管理 (SRM) ソフトウェア
- スナップショット ソフトウェア
- レプリケーション ソフトウェア

このようなソフトウェアでは、SCSI デバイスに直接アクセスできるように RDM で物理互換モードを使用します。

さまざまな管理製品が（ESXi マシン上でなく）統合されて最適な状態で実行される一方、別の製品は仮想マシン上で最適に実行されます。当社では、このようなアプリケーションについては保証せず、互換性マトリックスを提供していません。SAN 管理アプリケーションが ESXi 環境でサポートされているかどうかを確認するには、SAN 管理ソフトウェア プロバイダにお問い合わせください。

## RDM の注意事項と制限事項

RDM を使用する場合には、いくつかの注意事項と制限事項があります。

- RDM は直接接続ブロック デバイスまたは特定の RAID デバイスに使用できません。RDM は SCSI シリアル番号を使用して、マップされたデバイスを識別します。ブロック デバイスおよび一部の直接接続 RAID デバイスはシリアル番号をエクスポートしないので、このようなデバイスは RDM を使用できません。
- 物理互換モードで RDM を使用している場合には、ディスクとスナップショットを併用できません。物理互換モードでは、仮想マシンで、独自のストレージ ベース、スナップショットまたはミラーリング処理を管理できません。

仮想マシン スナップショットは、仮想互換モードで RDM に使用可能です。

- ディスク パーティションにマップできません。RDM ではマップされたデバイスが LUN 全体であることが求められます。
- vMotion で RDM を使用する仮想マシンを移行する場合、参加するすべての ESXi ホストで RDM の一貫した LUN ID を維持するようにしてください。
- フラッシュ読み取りキャッシュは物理互換の RDM をサポートしていません。仮想互換の RDM はフラッシュ読み取りキャッシュでサポートされています。

## Raw デバイス マッピングの特性

RDM は、マッピング済みのデバイスのメタデータを管理する VMFS ボリュームに含まれる特別なマッピング ファイルです。マッピング ファイルは、通常のファイル システムの操作に使用できる、通常のディスク ファイルとして管理ソフトウェアに提供されます。仮想マシンには、ストレージ仮想化レイヤーにより、マッピング済みのデバイスが仮想 SCSI デバイスとして提供されます。

マッピング ファイルのメタデータの主な内容には、マッピング済みのデバイスの場所（名前解決）、およびマッピング済みのデバイスのロック状態、権限などが含まれます。

## RDM の仮想および物理互換モード

RDM は、仮想互換モードまたは物理互換モードで使用できます。仮想モードは、マッピング済みのデバイスの完全な仮想化を指定します。物理モードは、マッピング済みのデバイスの最小 SCSI 仮想化を指定して、SAN 管理ソフトウェアの柔軟性を最大にします。

仮想モードでは、VMkernel はマッピング済みのデバイスに READ と WRITE だけを送信します。マッピング済みのデバイスは、ゲスト OS では、VMFS ボリュームの仮想ディスク ファイルとまったく同じものとして認識されます。実際のハードウェア特性は表示されません。Raw ディスクを仮想モードで使用している場合、データを保護する詳細ファイル ロックや、開発プロセスを簡単にスナップショットなどの VMFS のメリットを利用できます。また、仮想モードは、ストレージ ハードウェアでは物理モード比べてよりポータブルなため、仮想ディスク ファイルとも同じ動作を行います。

物理モードでは、VMkernel がすべての SCSI コマンドをデバイスに渡します。ただし、例外が 1 つあります。REPORT LUN コマンドは、VMkernel が所有する仮想マシンから LUN を分離できるように、仮想化されます。仮想化されない場合、基本となるハードウェアのすべての物理特性が公開されます。物理モードは、SAN 管理エージェントまたはほかの SCSI ターゲット ベース ソフトウェアを仮想マシンで実行するときに便利です。また、物理モードでは、コスト効率および可用性の高い、仮想と物理間のクラスタリングが可能になります。

VMFS5 は仮想モードと物理モードの RDM で 2TB 以上のディスク サイズをサポートします。VMFS5 以外のデータストアに 2TB より大きい RDM を再配置できません。

## 動的名前解決

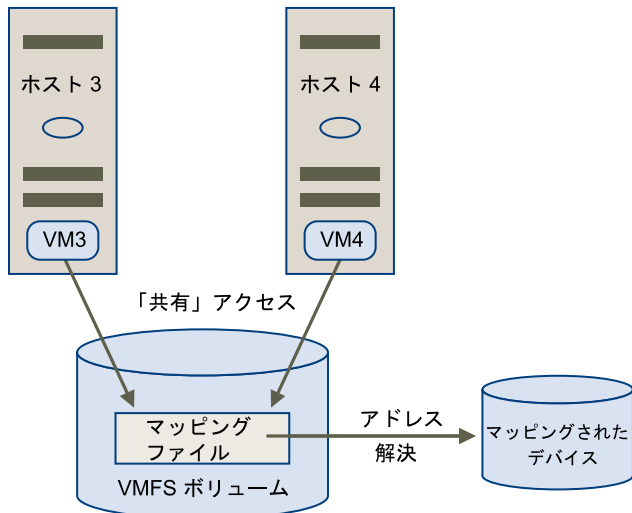
RDM ファイルでは、Raw デバイスへのパスが変更されたときに動的名前解決が可能です。

マッピングされたストレージ デバイスはすべて、VMFS で一意に識別されます。ID は、その内部データ構造に保存されます。ファイバ チャネル スイッチ障害や新しい HBA の追加など、Raw デバイスへのパスが変更されると、デバイス名も変わる可能性があります。動的名前解決によって、これらの変更が解明され、元のデバイスが新しい名前に自動的に関連付けられます。

## 仮想マシン クラスタでの Raw デバイス マッピング

フェイルオーバーが生じた場合に、同一の Raw LUN にアクセスする必要がある仮想マシン クラスタで RDM を使用します。設定は、同一の仮想ディスク ファイルにアクセスする仮想マシン クラスタの場合と似ていますが、RDM では仮想ディスク ファイルを置き換えます。

図 18-3. クラスタリングされた仮想マシンからのアクセス



## 利用可能な SCSI デバイス アクセス モードの比較

SCSI ベースのストレージ デバイスにアクセスする方法として、VMFS データストアの仮想ディスク ファイル、仮想モード RDM、および物理モード RDM があります。

SCSI デバイスで使用できるアクセス モードから選択するときの参考に、それぞれのモードで使用できる機能の簡単な比較を以下の表に示します。

表 18-1. 仮想ディスクおよび Raw デバイス マッピングで使用できる機能

ESXi 機能	仮想ディスク ファイル	仮想モード RDM	物理モード RDM
バス スルー SCSI コマンド	不可	不可	可 REPORT LUN はバス スルーされません
vCenter Server のサポート	可	可	可
スナップショット	可	可	不可
分散ロック	可	可	可
クラスタリング	筐体内クラスタのみ	筐体内クラスタ 筐体間クラスタ	物理マシンと仮想マシンのクラスタリング 筐体間クラスタ
SCSI ターゲット ベース ソフトウェア	不可	不可	可

筐体内クラスタ タイプのクラスタリングには、仮想ディスク ファイルを使用することをお勧めします。筐体内クラスタを筐体間クラスタとして再構成する計画がある場合は、筐体内クラスタに仮想モードの RDM を使用します。

## RDM を使用する仮想マシンの作成

仮想マシンから Raw SAN LUN に直接アクセスできるようにするときは、VMFS データストアに配置され、LUN を参照する RDM ディスクを作成します。RDM は、新規仮想マシンの初期ディスクとして作成したり、既存の仮想マシンに追加したりすることができます。RDM を作成するときに、マッピングする LUN、および RDM を保存するデータストアを指定します。

RDM ディスク ファイルの拡張子は通常の仮想ディスク ファイルと同じ .vmdk ですが、RDM に含まれるのはマッピング情報だけです。実際の仮想ディスクのデータは、LUN に直接格納されます。

この手順では、新しい仮想マシンを作成すると想定します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。

### 手順

- 1 仮想マシンの有効な親オブジェクトである任意のインベントリ オブジェクト（データセンター、フォルダ、クラスタ、リソース プール、ホストなど）を右クリックして、[新規仮想マシン] を選択します。
- 2 [新規仮想マシンの作成] を選択し、[次へ] をクリックします。
- 3 仮想マシンの作成に必要な手順すべてを実行します。
- 4 [ハードウェアのカスタマイズ] ページで、[仮想ハードウェア] タブをクリックします。
- 5 （オプション） システムがお使いの仮想マシン用に作成したデフォルトのハードディスクを削除するには、カーソルをディスクの上に移動し、[削除] アイコンをクリックします。
- 6 ページ下部の[新規] ドロップダウン メニューから、[RDM ディスク] を選択し、[追加] をクリックします。

- 7 SAN デバイスまたは LUN のリストから、仮想マシンが直接アクセスする Raw LUN を選択して、[OK] をクリックします。

仮想マシンをターゲット LUN にマッピングする RDM ディスクが作成されます。RDM ディスクが仮想デバイスのリストに新しいハード ディスクとして表示されます。

- 8 [新規ハード ディスク] の三角形をクリックして、RDM ディスクのプロパティを展開します。
- 9 RDM ディスクの場所を選択します。

RDM は、仮想マシンの構成ファイルと同じデータストアまたは異なるデータストアに配置できます。

**注：** NPIV を有効にした仮想マシンで vMotion を使用するには、RDM ファイルと仮想マシン ファイルが同じデータストアにあることを確認してください。NPIV が有効なときに Storage vMotion を実行できません。

- 10 互換モードを選択します。

オプション	説明
物理	ゲスト OS がハードウェアに直接アクセスできるようにします。物理互換モードは、仮想マシンで SAN 認識アプリケーションを使用している場合に便利です。ただし、物理互換 RDM のある仮想マシンはクローン作成、テンプレートへの変換、または移行（移行時にそのディスクのコピーを伴う場合）することはできません。
仮想	RDM を仮想ディスクのように機能させることができるため、スナップショット作成やクローン作成などの機能を使用できます。ディスクのクローンの作成またはディスクからのテンプレートの作成を行うと、LUN のコンテンツが .vmdk 仮想ディスク ファイルにコピーされます。仮想互換モードの RDM を移行するときは、マッピング ファイルを移行するか、LUN のコンテンツを仮想ディスクにコピーできます。

- 11 仮想互換モードを選択した場合は、ディスク モードを選択します。

ディスク モードは、物理互換モードを使用する RDM ディスクには使用できません。

オプション	説明
依存型	依存型ディスクはスナップショットに含まれます。
独立型：通常	通常モードのディスクは、物理コンピュータ上の従来のディスクと同様に動作します。通常モードのディスクに書き込まれたすべてのデータは、永続的にこのディスクに書き込まれます。
独立型：読み取り専用	読み取り専用モードのディスクへの変更は、仮想マシンをパワーオフまたはリセットしたときに破棄されます。読み取り専用モードでは、仮想マシンを再起動するときに仮想ディスクが常に同じ状態になります。ディスクへの変更は REDO ログ ファイルに書き込まれ、このファイルから読み取られます。REDO ログ ファイルはパワーオフまたはリセット時に削除されます。

- 12 [OK] をクリックします。

## マッピング済み LUN のパス管理

RDM で仮想マシンを使用すると、マッピング済みの Raw LUN のパスを管理できます。

## 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 仮想マシンを右クリックし、[設定の編集] を選択します。
- 3 [仮想ハードウェア] タブをクリックして、[ハード ディスク] をクリックしてディスク オプション メニューを展開します。
- 4 [パスの管理] をクリックします。
- 5 [マルチパス ポリシーの編集] ダイアログ ボックスを使用して、パスの有効化または無効化、マルチパス ポリシーの設定、および優先パスの指定を行います。

パスの管理については、[17 章 マルチパスとフェイルオーバーについて](#) を参照してください。

仮想ボリューム機能により、データストア内部の領域の管理から、ストレージ アレイで処理される抽象的なストレージ オブジェクトの管理へとストレージ管理のパラダイムが変わります。仮想ボリュームを使用すると、ストレージ管理の単位はデータストアではなく個々の仮想マシンになりますが、仮想ディスクのコンテンツ、レイアウト、および管理はストレージ ハードウェアで完全に制御されます。

これまで、vSphere のストレージ管理では、データストアを中心としたアプローチを行ってきました。このアプローチの場合、ストレージ管理者と vSphere 管理者は、仮想マシンの基盤となるストレージ要件について事前に話合います。その後、ストレージ管理者は、LUN または NFS 共有を設定し、ESXi ホストに提供します。vSphere 管理者は、LUN または NFS に基づいてデータストアを作成し、これらのデータストアを仮想マシン ストレージとして使用します。通常、ストレージの観点からデータを管理する最小の精度レベルは、データストアになります。ただし、1つのデータストアに、要件の異なる複数の仮想マシンが含まれる場合があります。従来のアプローチでは、仮想マシン レベルごとに区別することは困難です。

仮想ボリューム機能では、ストレージ管理への新しいアプローチを提供することで、精度が向上し、アプリケーション レベルごとに仮想マシン サービスを区別できます。仮想ボリュームでは、ストレージ システムの機能に基づいてストレージを配置するのではなく、個々の仮想マシンのニーズに基づいてストレージを配置します。これにより、ストレージ仮想マシンが中心となります。

仮想ボリュームでは、仮想ディスクとその派生ディストリビューション、クローン、スナップショット、およびレプリカが、ストレージ システムの仮想ボリュームと呼ばれるオブジェクトに直接マップされます。このマッピングにより、vSphere はスナップショット、クローン作成、およびレプリケーションなどの大量のストレージ操作の負荷をストレージ システムに移すことができます。

仮想ディスクごとにボリュームを作成することで、最適なレベルでポリシーを設定できます。アプリケーションのストレージ要件を事前に決定し、これらの要件に基づいて適切な仮想ディスクを作成できるように、要件をストレージ システムに通知することができます。たとえば、仮想マシンにアクティブ-アクティブ ストレージ アレイが必要な場合、アクティブ-アクティブ モデルをサポートするデータストアを選択する必要はありません。代わりに、アクティブ-アクティブ アレイに自動的に配置される個々の仮想ボリュームを作成します。

この章には、次のトピックが含まれています。

- [Virtual Volumes の概念](#)
- [仮想ボリュームを使用するときのガイドライン](#)
- [仮想ボリュームとストレージ プロトコル](#)
- [Virtual Volumes のアーキテクチャ](#)
- [仮想ボリュームと VMware Certificate Authority](#)

- [仮想ボリュームを有効化する前に](#)
- [仮想ボリュームの構成](#)
- [仮想データストア上の仮想マシンのプロビジョニング](#)

## Virtual Volumes の概念

Virtual Volumes を使用すると、抽象ストレージ コンテナでは、LUN または NFS 共有に基づいて従来のストレージ ボリュームを置き換えます。vCenter Server では、ストレージ コンテナが仮想データストアによって表されます。仮想データストアにより、従来のデータストアの人為的な境界を取り除き、Virtual Volumes（仮想マシン ファイルをカプセル化するオブジェクト）を保存します。

Virtual Volumes 機能の各種コンポーネントの詳細については、ビデオをご覧ください。



( Virtual Volumes パート 1 : 概念 )

- [仮想ボリューム](#)

仮想ボリュームは、仮想マシンのファイル、仮想ディスク、およびその派生物をカプセル化したものです。

- [仮想ボリュームとストレージ プロバイダ](#)

VASA プロバイダとも呼ばれる仮想ボリューム ストレージ プロバイダは、vSphere の Storage Awareness サービスとして動作するソフトウェア コンポーネントです。プロバイダは、一方の側を vCenter Server ホストと ESXi ホスト、もう一方の側をストレージ システムとする、アウトオブバンド通信を仲介します。

- [ストレージ コンテナ](#)

従来の LUN および NFS ベースの vSphere ストレージとは異なり、仮想ボリューム機能では、ストレージ側でボリュームの事前構成を行う必要がありません。代わりに仮想ボリュームでは、ストレージ コンテナを使用します。このコンテナは、ストレージ システムが仮想ボリュームに提供する RAW ストレージ容量のプールまたはストレージ機能の集約です。

- [プロトコル エンドポイント](#)

ストレージ システムは Virtual Volumes のすべての側面を管理しますが、ESXi ホストは、ストレージ側の Virtual Volumes に直接アクセスできません。ESXi ホストは、代わりに、プロトコル エンドポイントと呼ばれる論理 I/O プロキシを使用して、Virtual Volumes および Virtual Volumes によってカプセル化された仮想ディスク ファイルと通信します。ESXi は、プロトコル エンドポイントを使用し、要求に応じて、仮想マシンから各 Virtual Volumes へのデータ パスを確立します。

- [仮想データストア](#)

仮想データストアは、vCenter Server および vSphere Web Client におけるストレージ コンテナです。

- [仮想ボリュームと仮想マシン ストレージのポリシー](#)

仮想データストアで実行される仮想マシンには、仮想マシン ストレージ ポリシーが必要です。

## 仮想ボリューム

仮想ボリュームは、仮想マシンのファイル、仮想ディスク、およびその派生物をカプセル化したものです。



仮想ボリュームは、イーサネットまたは SAN を介して接続されているストレージ システムの内部にネイティブに格納されます。準拠ストレージ システムによってオブジェクトとしてエクスポートされ、ストレージ側のハードウェアによって全体的に管理されます。通常、仮想ボリュームは一意の GUID によって識別されます。仮想ボリュームは事前にプロビジョニングされませんが、仮想マシンの管理操作を実行するときに自動的に作成されます。これらの操作には、VM 作成、クローン作成、およびスナップショットの作成などがあります。ESXi および vCenter Server は、1 つ以上の仮想ボリュームを 1 つの仮想マシンに関連付けます。システムは、仮想マシンを構成するコア要素として、次のタイプの仮想ボリュームを作成します。

- 各仮想ディスクの .vmdk ファイルに直接対応するデータ仮想ボリューム。仮想ディスク ファイルは従来のデータストア上にあるため、仮想ボリュームは仮想マシンに対して SCSI ディスクとして示されます。
- 構成仮想ボリュームまたはホーム ディレクトリは、仮想マシンのメタデータ ファイルに含まれる小さいディレクトリを表します。ファイルには .vmx ファイル、仮想ディスクの記述子ファイル、ログ ファイルなどがあります。構成仮想ボリュームは、ファイル システムでフォーマットされます。ESXi が SCSI プロトコルを使用してストレージに接続されている場合、構成仮想ボリュームは VMFS でフォーマットされます。NFS プロトコルを持つ構成仮想ボリュームは、NFS ディレクトリとして表示されます。

クローン、スナップショット、レプリカなど、他の仮想マシンのコンポーネントおよび仮想ディスクの派生物用に、仮想ボリュームを追加で作成できます。これらの仮想ボリュームには、仮想マシン スワップ ファイルを保持するためのスワップ仮想ボリュームと、スナップショットの仮想マシン メモリの内容を保持する仮想メモリ ボリュームが含まれます。

異なる仮想マシン コンポーネントに対して異なる仮想ボリュームを使用することにより、最大限に細分化された精度レベルでストレージ ポリシーを適用および操作できます。たとえば、1 つの仮想ディスクを含む 1 つの仮想ボリュームには、仮想マシン 起動ディスクの仮想ボリュームよりも豊富なデータ サービスとパフォーマンス レベルのセットを含めることができます。同様に、スナップショット仮想ボリュームでは、現在の仮想ボリュームと異なるストレージ階層を使用できます。

## 仮想ボリュームとストレージ プロバイダ

VASA プロバイダとも呼ばれる仮想ボリューム ストレージ プロバイダは、vSphere の Storage Awareness サービスとして動作するソフトウェア コンポーネントです。プロバイダは、一方の側を vCenter Server ホストと ESXi ホスト、もう一方の側をストレージ システムとする、アウトオブバンド通信を仲介します。

ストレージ プロバイダは、VMware APIs for Storage Awareness (VASA) によって実装され、仮想ボリューム ストレージのすべての側面を管理するために使用されます。ストレージ プロバイダは、vSphere に付属するストレージ監視サービス (SMS) と統合され、vCenter Server および ESXi ホストと通信します。

ストレージ プロバイダは、基盤となるストレージから、または仮想ボリュームの場合にはストレージ コンテナから情報を配信し、ストレージ コンテナの機能を vCenter Server および vSphere Web Client に表示できるようにします。次にストレージ プロバイダは、仮想マシンのストレージ要件をストレージ レイヤーに伝達します。要件は、ストレージ ポリシーの形式で定義できます。この統合プロセスにより、ストレージ レイヤーで作成される仮想ボリュームが、ポリシーで規定されている要件を必ず満たすようになります。

通常、ベンダーには、vSphere と統合可能なストレージ プロバイダを供給し、仮想ボリュームをサポートする責任があります。すべてのストレージ プロバイダは、VMware によって認定され、適切にデプロイされる必要があります。仮想ボリューム ストレージ プロバイダのデプロイの詳細については、ストレージ ベンダーにお問い合わせください。

ストレージ プロバイダのデプロイ後は、そのプロバイダを vCenter Server で登録し、SMS を経由して vSphere と通信できるようにする必要があります。

## ストレージ コンテナ

従来の LUN および NFS ベースの vSphere ストレージとは異なり、仮想ボリューム機能では、ストレージ側でボリュームの事前構成を行う必要がありません。代わりに仮想ボリュームでは、ストレージ コンテナを使用します。このコンテナは、ストレージ システムが仮想ボリュームに提供する RAW ストレージ容量のプールまたはストレージ機能の集約です。

ストレージ コンテナは論理ストレージ ファブリックの一部であり、基盤となるハードウェアの論理ユニットです。ストレージ コンテナは、管理および運用上の必要に基づいて仮想ボリュームを論理的にグループ化します。たとえば、ストレージ コンテナには、マルチテナント デプロイのテナント用か、エンタープライズ デプロイの部門用に作成されたすべての仮想ボリュームを含めることができます。各ストレージ コンテナは仮想ボリューム ストアとして機能し、仮想ボリュームがストレージ コンテナの容量から割り当てられます。

通常は、ストレージ側のストレージ管理者がストレージ コンテナを定義します。ストレージ コンテナの数、その容量、およびサイズは、ベンダーに固有の実装方法によって決まりますが、ストレージ システムごとにコンテナが少なくとも 1 つは必要です。

---

**注：** 1 つのストレージ コンテナが複数の物理アレイをまたぐことはできません。

---

ストレージ システムに関連付けられているストレージ プロバイダを登録すると、vCenter Server は、すべての構成済みストレージ コンテナを、そのストレージ機能プロファイル、プロトコル エンドポイント、およびその他の属性とともに検出します。1 つのストレージ コンテナで複数の機能プロファイルをエクスポートできます。そのため、多様なニーズとさまざまなストレージ ポリシー設定が関係する仮想マシンを同じストレージ コンテナの一部にすることができます。

最初は、検出されたストレージ コンテナによっては任意の特定のホストに接続されないものもあり、それらのコンテナは vSphere Web Client に表示されません。ストレージ コンテナをマウントするには、そのコンテナを仮想データストアにマッピングする必要があります。

## プロトコル エンドポイント

ストレージ システムは Virtual Volumes のすべての側面を管理しますが、ESXi ホストは、ストレージ側の Virtual Volumes に直接アクセスできません。ESXi ホストは、代わりに、プロトコル エンドポイントと呼ばれる論理 I/O ブロキシを使用して、Virtual Volumes および Virtual Volumes によってカプセル化された仮想ディスク ファイルと通信します。ESXi は、プロトコル エンドポイントを使用し、要求に応じて、仮想マシンから各 Virtual Volumes へのデータ パスを確立します。

各 Virtual Volumes は、特定のプロトコル エンドポイントにバインドされています。ホスト上の仮想マシンが I/O 操作を実行すると、プロトコル エンドポイントによって I/O が適切な Virtual Volumes に送られます。通常、ストレージ システムが必要とするのはごく少数のプロトコル エンドポイントです。1 つのプロトコル エンドポイントが、何百、何千もの Virtual Volumes に接続できます。

ストレージ側では、ストレージ管理者が、ストレージ コンテナごとに1つまたは複数のプロトコル エンドポイントを構成します。プロトコル エンドポイントは物理ストレージ ファブリックに属し、ストレージ プロバイダ経由で、ストレージ システムによって関連するストレージ コンテナとともにエクスポートされます。ストレージ コンテナを仮想データストアにマッピングすると、プロトコル エンドポイントが ESXi によって検出され、vSphere Web Client で認識されるようになります。プロトコル エンドポイントは、ストレージの再スキャン時にも検出できます。

vSphere Web Client では、利用可能なプロトコル エンドポイントのリストは、ホスト ストレージ デバイスのリストに似ています。さまざまなストレージの転送を使用して、プロトコル エンドポイントを ESXi に公開できます。SCSI ベースの転送を使用すると、プロトコル エンドポイントは T10 ベースの LUN WWN によって定義されたブロック LUN を表します。NFS プロトコルの場合、プロトコル エンドポイントは IP アドレス、共有名などのマウント ポイントです。SCSI ベースのプロトコル エンドポイントではマルチパスを構成できますが、NFS ベースのプロトコル エンドポイントでは構成できません。ただし、使用しているプロトコルに関わらず、ストレージ アレイでは、可用性の目的で複数のプロトコル エンドポイントを使用できます。

## 仮想データストア

仮想データストアは、vCenter Server および vSphere Web Client におけるストレージ コンテナです。

vCenter Server がストレージ システムによってエクスポートされたストレージ コンテナを検出した後は、それらをマウントして使用できるようにする必要があります。vSphere Web Client のデータストア作成ウィザードを使用して、ストレージ コンテナを仮想データストアにマッピングします。作成する仮想データストアは、特定のストレージ コンテナに直接対応し、vCenter Server および vSphere Web Client におけるコンテナの表現となります。

vSphere 管理者の観点からすると、仮想データストアはその他の任意のデータストアに似ており、仮想マシンを保持するために使用されます。他のデータストアと同様に、仮想データストアは、参照することができ、仮想マシン名別に仮想ボリュームの一覧が表示されます。また従来のデータストアと同様、仮想データストアはアンマウントとマウントをサポートします。ただし、アップグレードやサイズ変更などの操作は、仮想データストアには適用されません。仮想データストアの容量は、vSphere の外部のストレージ管理者が構成できます。

従来の VMFS および NFS データストア、および Virtual SAN を使用する仮想データストアを使用できます。

---

**注：** 仮想ボリュームのサイズは、1 MB の倍数（最低 1 MB 以上）でなければなりません。そのため、仮想データストア上でのプロビジョニングまたはその仮想データストア以外の任意のデータストアからの移行を行うすべての仮想ディスクは、サイズが 1 MB の偶数倍になるはずで、仮想データストアに移行する仮想ディスクが 1 MB の偶数倍になっていない場合は、1 MB の偶数倍にできるだけ近づくようにディスクを手動で拡張します。

---

## 仮想ボリュームと仮想マシン ストレージのポリシー

仮想データストアで実行される仮想マシンには、仮想マシン ストレージ ポリシーが必要です。

仮想マシン ストレージ ポリシーは、仮想マシンの配置要件とサービス品質要件を含むルール セットです。このポリシーにより、仮想ボリューム ストレージ内に仮想マシンが適切に配置され、ストレージが仮想マシンの要件を確実に満たすことができます。

仮想マシン ストレージ ポリシー インターフェイスを使用して、仮想ボリューム ストレージ ポリシーを作成します。新しいポリシーを仮想マシンに割り当てると、そのポリシーにより、仮想ボリューム ストレージの要件準拠が強制されます。

仮想データストアと互換性のある仮想マシン ストレージ ポリシーを作成しない場合、システムではデフォルトの要件なしポリシーが使用されます。要件なしポリシーは、ルールまたはストレージの仕様が含まれない汎用的な仮想ボリューム ポリシーです。このポリシーでは、仮想ボリューム ストレージ アレイで仮想マシン オブジェクトの最適な配置を決定できます。

## 仮想ボリュームを使用するときのガイドライン

仮想ボリューム機能には、いくつかのメリットがあります。仮想ボリュームを操作するときは、次の固有のガイドラインに従う必要があります。

仮想ボリュームには次の特性があります。

- ストレージ ハードウェアに対するさまざまな操作の負荷を軽減できます。このような操作には、スナップショット作成、クローン作成、および Storage DRS が含まれます。
- 個々の仮想ディスクのレプリケーション、暗号化、デデュープ、および圧縮などの高度なストレージ サービスを使用できます。
- vMotion、Storage vMotion、スナップショット、リンク クローン、Flash Read Cache、および DRS などの vSphere 機能がサポートされています。
- ストレージ ベンダーは、ネイティブ スナップショット機能を使用して、vSphere スナップショットのパフォーマンスを向上させることができます。
- vSphere APIs for Array Integration (VAAI) をサポートするストレージ アレイで仮想ボリュームを使用できます。
- vSphere APIs for Data Protection (VADP) を使用するバックアップ ソフトウェアがサポートされています。

## 仮想ボリュームのガイドラインおよび制限事項

仮想ボリュームを使用するときは、これらのガイドラインに従います。

- 仮想ボリューム環境では、vCenter Server が必要であるため、スタンドアロン ホストで仮想ボリュームを使用することはできません。
- 仮想ボリュームでは、RDM はサポートされていません。
- 仮想ボリューム ストレージ コンテナは、異なる物理アレイにまたがることはできません。
- 仮想データストアを含むホスト プロファイルは、vCenter Server に固有です。このタイプのホスト プロファイルを抽出したら、参照ホストと同じ vCenter Server によって管理されるホストおよびクラスタにのみ接続できます。

## 仮想ボリュームとストレージ プロトコル

仮想ボリュームの機能により、ファイバ チャネル、FCoE、iSCSI、および NFS がサポートされます。ストレージの転送では、ESXi ホストに対してプロトコル エンドポイントが公開されます。

SCSI ベースのプロトコルを使用する場合、プロトコル エンドポイントは、T10 ベースの LUN WWN によって定義された LUN を表します。NFS プロトコルの場合、プロトコル エンドポイントは、IP アドレスや DNS 名、および共有名などのマウント ポイントです。

使用するストレージ プロトコルに関係なく、仮想ボリュームは、他の従来のデータストア上のファイルと同様に、仮想マシンに対して SCSI ディスクとして示されます。ディスク アレイ上の仮想ボリュームは、VMFS と同じ SCSI コマンド セットをサポートし、ATS をロック メカニズムとして使用します。

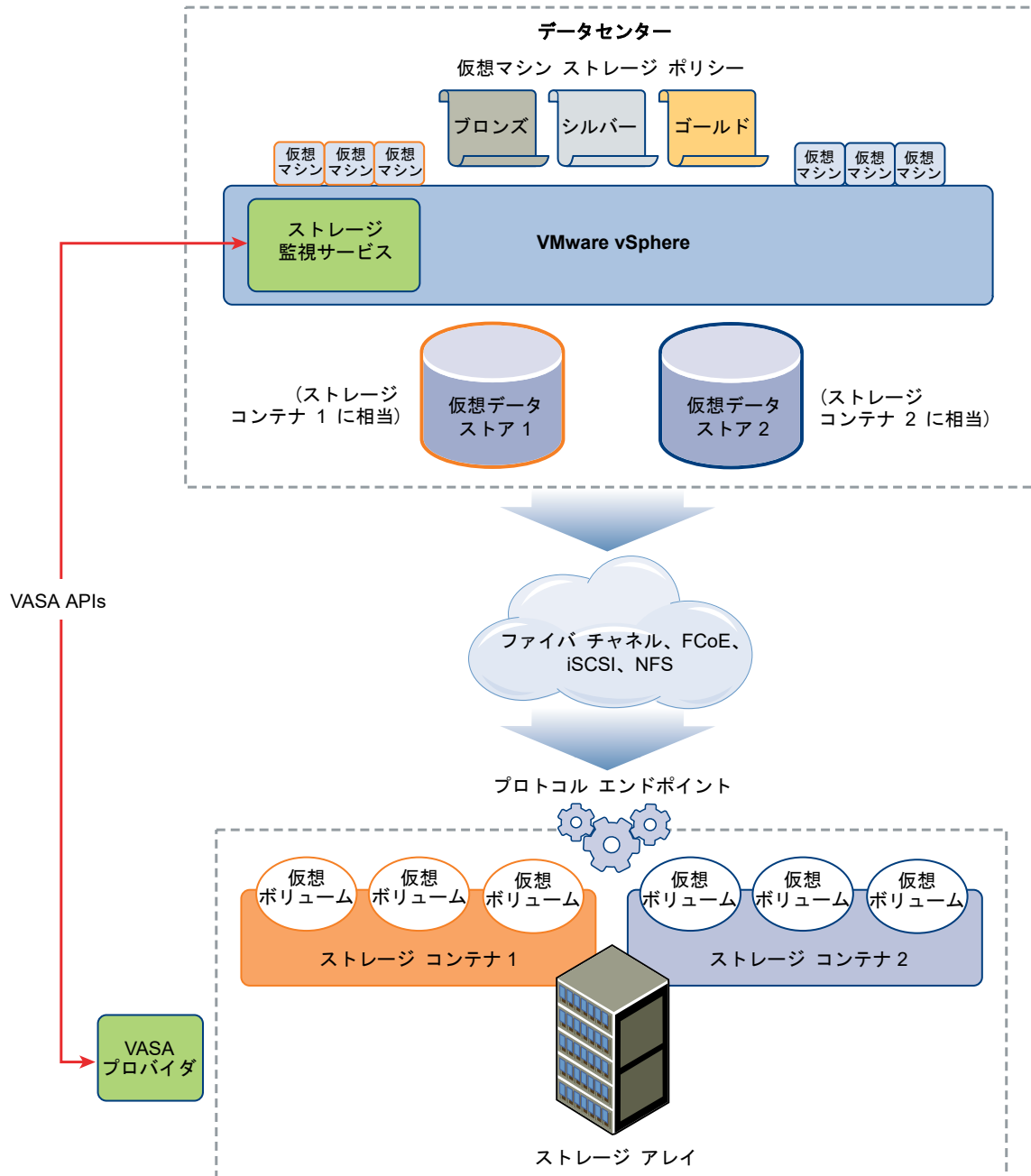
NAS デバイス上の仮想ボリュームは、NFS マウント ポイントに接続するために ESXi ホストで必要とされるのと同じ NFS リモート プロシージャ コール (RPC) をサポートします。

次の考慮事項とガイドラインは、異なるストレージ プロトコルを使用する場合に適用されます。

- NFS については、バージョン 3 を使用できます。仮想ボリュームは NFS 4.1 をサポートしていません。
- IPv6 形式はサポートされません。
- iSCSI の場合は、ソフトウェア iSCSI アダプタを有効化する必要があります。動的検出を構成し、仮想ボリューム ストレージ プロバイダの IP アドレスを入力します。[ソフトウェア iSCSI アダプタの構成](#) を参照してください。
- SCSI ベースのプロトコル エンドポイントではマルチパスを構成できますが、NFS ベースのプロトコル エンドポイントでは構成できません。使用するプロトコルに関係なく、ストレージ アレイでは、可用性を高める目的で複数のプロトコル エンドポイントを提供できます。

## Virtual Volumes のアーキテクチャ

アーキテクチャ図には、Virtual Volumes 機能のすべてのコンポーネントが相互作用する仕組みの概要が示されています。



Virtual Volumes は、準拠ストレージ システムによってエクスポートされるオブジェクトで、通常、仮想マシン ディスクや他の仮想マシン関連ファイルに 1 対 1 で対応します。Virtual Volumes は、VASA プロバイダにより、データ パス内ではなくアウトオブバンドで作成および操作されます。

VASA プロバイダ、つまりストレージ プロバイダは、vSphere APIs for Storage Awareness で開発されます。ストレージ プロバイダにより、一方の vSphere スタック (ESXi ホスト、vCenter Server、および vSphere Web Client) ともう一方のストレージ システム間の通信が可能になります。VASA プロバイダは、ストレージ側で実行され、vSphere ストレージ監視サービス (SMS) と統合されて Virtual Volumes ストレージのすべての側面を管理します。VASA プロバイダは、仮想ディスク オブジェクトとその派生物 (クローン、スナップショット、およびレプリカなど) をストレージ システム上の Virtual Volumes に直接マッピングします。

ESXi ホストには、Virtual Volumes ストレージに直接アクセスする権限がありません。代わりにホストは、プロトコル エンドポイントと呼ばれるデータ パス内の中間ポイントを介して Virtual Volumes にアクセスします。プロトコル エンドポイントでは、仮想マシンからそれぞれの Virtual Volumes へのデータ パスがオンデマンドで確立され、ESXi ホストとストレージ システムの間の直接インバンド I/O のゲートウェイとして機能します。ESXi では、インバンド通信で、ファイバ チャネル、FCoE、iSCSI、および NFS の各プロトコルを使用できます。

Virtual Volumes はストレージ コンテナ内部に存在し、論理的にストレージ システム上の物理ディスクのプールを表します。vSphere スタックにおいて、ストレージ コンテナは仮想データストアとして表されます。1つのストレージ コンテナ単体で、複数のストレージ機能セットをエクスポートできます。そのため、仮想データストアで仮想マシンを作成する場合は、異なるストレージ ポリシーを使用して、仮想マシンのさまざまなストレージのニーズを満たすように、同じストレージ コンテナの内部に Virtual Volumes を配置することができます。

Virtual Volumes アーキテクチャの詳細については、ビデオをご覧ください。



( Virtual Volumes パート 2 : アーキテクチャ )

## 仮想ボリュームと VMware Certificate Authority

vSphere 6.0.x には VMware 認証局 (VMCA) が含まれます。デフォルトでは、VMCA は vSphere 環境で使用するすべての内部証明書を生成します。これには、仮想ボリューム ストレージ システムを管理または示す、新たに追加された ESXi ホストおよびストレージ VASA プロバイダの証明書が含まれます。

VASA プロバイダとの通信は SSL 証明書によって保護されます。これらの証明書は VASA プロバイダからまたは VMCA から取得できます。

- 証明書は、長期の使用のために VASA プロバイダから直接取得することも、自己生成および自己署名証明書を使用することも、外部の認証局から取得することもできます。
- VASA プロバイダで使用するために VMCA で証明書を生成できます。

ホストまたは VASA プロバイダが登録されている場合、VMCA は自動的にこれらの手順に従い、vSphere 管理者が介入することはありません。

- 1 VASA プロバイダが最初に vCenter Server ストレージ管理サービス (SMS) に追加されたときに、自己署名証明書が生成されます。
- 2 証明書を検証した後、SMS は VASA プロバイダから証明書署名要求 (CSR) を要求します。
- 3 CSR を受け取って検証した後、SMS は VASA プロバイダの代わりにそれを VMCA に呈示して、CA 署名証明書を要求します。

VMCA はスタンドアロン CA として、またはエンタープライズ CA の従属局として機能するように構成できます。VMCA を従属 CA として設定する場合、VMCA は完全なチェーンで CSR に署名します。

- 4 vCenter Server および ESXi ホスト上で SMS から生成された、以降のすべての安全な接続を認証できるように、署名証明書がルート証明書とともに VASA プロバイダに渡されます。

## 仮想ボリュームを有効化する前に

仮想ボリュームを使用できるようにするには、ストレージと vSphere 環境を正しく設定する必要があります。

次のガイドラインに従って、仮想ボリュームのストレージ システム環境を準備します。詳細については、ストレージ ペンダーにお問い合わせください。

- 使用するストレージ システムまたはストレージ アレイでは、仮想ボリュームをサポートし、vSphere APIs for Storage Awareness (VASA) を介して vSphere と統合できるようになっている必要があります。
- 仮想ボリュームのストレージ プロバイダをデプロイする必要があります。
- ストレージ側で、プロトコル エンドポイント、ストレージ コンテナ、およびストレージ プロファイルを構成する必要があります。

vSphere 環境を準備します。

- 必ず、使用するストレージのタイプ（ファイバ チャネル、FCoE、iSCSI、または NFS）に応じた適切なセットアップのガイドラインに従ってください。必要な場合は、ESXi ホストにストレージ アダプタをインストールして構成します。  
  
iSCSI を使用する場合は、ESXi ホストでソフトウェア iSCSI アダプタを有効化します。動的検出を構成し、仮想ボリューム ストレージ システムの IP アドレスを入力します。
- ストレージ アレイのすべてのコンポーネントを、vCenter Server およびすべての ESXi ホストと同期します。この同期処理には、ネットワーク時間プロトコル (NTP) を使用します。

## ネットワーク タイム サーバによる vSphere のストレージ環境の同期

Virtual Volumes を有効にする前に、vSphere ネットワーク上のすべてのマシンの時計が同期されていることを確認します。

### 手順

- 1 vSphere インベントリでホストを選択します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [システム] セクションで、[時間の構成] を選択します。
- 4 [編集] をクリックし、NTP サーバを設定します。
  - a [Network Time Protocol を使用（NTP クライアントを有効にする）] を選択します。
  - b NTP サービス起動ポリシーを設定します。
  - c 同期する NTP サーバの IP アドレスを入力します。
  - d [NTP サービス ステータス] セクションで [起動] または [再起動] をクリックします。
- 5 [OK] をクリックします。  
  
ホストが NTP サーバと同期します。

## 仮想ボリュームの構成

仮想ボリューム環境を構成するには、一連の手順を実行する必要があります。



## 前提条件

仮想ボリュームを有効化する前にのガイドラインに従います。

## 手順

### 1 仮想ボリュームのストレージ プロバイダの登録

仮想ボリューム環境には、VASA プロバイダとも呼ばれるストレージ プロバイダが含まれている必要があります。通常、サードパーティ ベンダーが VMware APIs for Storage Awareness (VASA) を使用してストレージ プロバイダを開発します。ストレージ プロバイダにより、vSphere とストレージ側との通信が円滑になります。ストレージ プロバイダを vCenter Server に登録して、仮想ボリュームを操作できるようにする必要があります。

### 2 仮想データストアの作成

[新しいデータストア] ウィザードを使用して、仮想データストアを作成します。

### 3 プロトコル エンドポイントの確認と管理

ESXi ホストは、プロトコル エンドポイントと呼ばれる論理 I/O プロキシを使用して、仮想ボリュームおよび仮想ボリュームがカプセル化する仮想ディスク ファイルと通信します。プロトコルのエンドポイントは、ストレージ プロバイダを介したストレージ システムにより、関連付けられたストレージ コンテナと一緒にエクスポートされます。プロトコル エンドポイントは、ストレージ コンテナを仮想データストアにマップした後、vSphere Web Client で表示可能になります。プロトコル エンドポイントのプロパティを確認し、特定の設定を変更することができます。

### 4 (オプション) プロトコル エンドポイントのパス選択ポリシーの変更

ESXi ホストが SCSI ベースの転送を使用してストレージ アレイを表すプロトコル エンドポイントと通信する場合は、プロトコル エンドポイントに割り当てられたデフォルトのマルチパス ポリシーを変更できます。[マルチパス ポリシーの編集] ダイアログ ボックスを使用して、パス選択ポリシーを変更します。

## 次のステップ

これで、仮想データストアに仮想マシンをプロビジョニングできます。仮想マシンの作成の詳細については、『vSphere 仮想マシン管理』のドキュメントを参照してください。

トラブルシューティングの詳細については、『vSphere トラブルシューティング』ドキュメントを参照してください。

## 仮想ボリュームのストレージ プロバイダの登録

仮想ボリューム環境には、VASA プロバイダとも呼ばれるストレージ プロバイダが含まれている必要があります。通常、サードパーティ ベンダーが VMware APIs for Storage Awareness (VASA) を使用してストレージ プロバイダを開発します。ストレージ プロバイダにより、vSphere とストレージ側との通信が円滑になります。ストレージ プロバイダを vCenter Server に登録して、仮想ボリュームを操作できるようにする必要があります。

登録後、仮想ボリューム プロバイダは vCenter Server と通信し、基盤となるストレージの特性を報告します。特性は、仮想マシン ストレージ ポリシーのインターフェイスに表示され、仮想データストアと互換性のある仮想マシン ストレージ ポリシーを作成するために使用できます。このストレージ ポリシーを仮想マシンに適用すると、そのポリシーは仮想ボリューム ストレージにプッシュされます。このポリシーにより、仮想ボリューム ストレージ内に仮想マシンが適切に配置され、ストレージが仮想マシンの要件を確実に満たすことができます。

**前提条件**

ストレージ プロバイダ コンポーネントがストレージ側にインストールされていることを確認して、その証明書をストレージ管理者から取得します。詳細については、ベンダーにお問い合わせください。

**手順**

- 1 vSphere Web Client ナビゲータで、vCenter Server に移動して参照します。
- 2 [構成] タブをクリックし、[ストレージ プロバイダ] をクリックします。
- 3 [新しいストレージ プロバイダの登録] アイコンをクリックします。
- 4 (オプション) vCenter Server にストレージ プロバイダの証明書を参照させるには、[ストレージ プロバイダ 証明書を使用する] オプションを選択して、証明書の場所を指定します。  
  
このオプションを選択しない場合、証明書のサムプリントが表示されます。サムプリントを確認して承認することができます。
- 5 [OK] をクリックして、登録を完了します。

**結果**

vCenter Server は、仮想ボリューム ストレージ プロバイダを検出して登録します。

**仮想データストアの作成**

[新しいデータストア] ウィザードを使用して、仮想データストアを作成します。

**手順**

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 [新規データストア] アイコンをクリックします。
- 3 データストア名を入力し、必要に応じてデータストアの配置場所を選択します。  
  
必ず、データセンター環境内の別のデータストア名と重複しない名前を使用してください。  
  
同じ仮想データストアをいくつかのホストにマウントする場合は、すべてのホストで一貫したデータストアの名前を使用する必要があります。
- 4 データストア タイプとして [VVOL] を選択します。
- 5 ストレージ コンテナのリストから、バックアップ ストレージ コンテナを選択します。
- 6 データストアへのアクセスが必要なホストを選択します。
- 7 構成オプションを確認し、[終了] をクリックします。

**次のステップ**

仮想データストアを作成した後は、データストアの名前変更、データストア ファイルの参照、データストアのアンマウントなどのデータストア操作を実行できます。

仮想データストアをデータストア クラスタに追加することはできません。

## プロトコル エンドポイントの確認と管理

ESXi ホストは、プロトコル エンドポイントと呼ばれる論理 I/O ブロキシを使用して、仮想ボリュームおよび仮想ボリュームがカプセル化する仮想ディスク ファイルと通信します。プロトコルのエンドポイントは、ストレージ プロバイダを介したストレージ システムにより、関連付けられたストレージ コンテナと一緒にエクスポートされます。プロトコル エンドポイントは、ストレージ コンテナを仮想データストアにマップした後、vSphere Web Client で表示可能になります。プロトコル エンドポイントのプロパティを確認し、特定の設定を変更することができます。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [プロトコル エンドポイント] をクリックします。
- 4 特定の項目の詳細を表示するには、リストからその項目を選択します。
- 5 [プロトコル エンドポイントの詳細] の下のタブを使用して追加情報にアクセスし、選択したプロトコル エンドポイントのプロパティを変更します。

タブ	説明
プロパティ	項目のプロパティと特性を表示します。SCSI (ブロック) 項目の場合は、マルチパス ポリシーを表示および編集します。
パス (SCSI プロトコル エンドポイントのみ)	プロトコル エンドポイントの使用可能なパスを表示します。選択したパスを有効/無効にします。パス選択ポリシーを変更します。
データストア	対応する仮想データストアを表示します。データストアの管理操作を実行します。

## プロトコル エンドポイントのパス選択ポリシーの変更

ESXi ホストが SCSI ベースの転送を使用してストレージ アレイを表すプロトコル エンドポイントと通信する場合は、プロトコル エンドポイントに割り当てられたデフォルトのマルチパス ポリシーを変更できます。[マルチパス ポリシーの編集] ダイアログ ボックスを使用して、パス選択ポリシーを変更します。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [プロトコル エンドポイント] をクリックします。
- 4 パスを変更するプロトコル エンドポイントを選択して、[プロパティ] タブをクリックします。
- 5 [マルチパス ポリシー] で、[マルチパスの編集] をクリックします。
- 6 パス ポリシーを選択します。
  - 固定 (VMware)
  - 最近の使用 (VMware)
  - ラウンド ロビン (VMware)

- 7 固定ポリシーでは、優先パスを指定します。
- 8 [OK] をクリックして設定内容を保存し、ダイアログ ボックスを閉じます。

## 仮想データストア上の仮想マシンのプロビジョニング

仮想データストアに仮想マシンをプロビジョニングできます。

---

**注：** 仮想データストアにプロビジョニングするすべての仮想ディスクは 1 MB の偶数倍である必要があります。

---

仮想データストアで実行される仮想マシンには、適切な仮想マシン ストレージ ポリシーが必要です。

仮想マシンをプロビジョニングしたら、一般的な仮想マシン管理タスクを実行できます。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。

トラブルシューティングの詳細については、『vSphere トラブルシューティング』ドキュメントを参照してください。

### 手順

#### 1 Virtual Volumes の仮想マシン ストレージ ポリシーの定義

仮想データストアと互換性のある仮想マシン ストレージ ポリシーを作成できます。

#### 2 仮想マシンへの仮想ボリューム ストレージ ポリシーの割り当て

仮想マシンを割り当てるときに、仮想データストアが特定のストレージ要件を満たすよう保証するには、仮想ボリューム ストレージ ポリシーを仮想マシンに関連付けます。

#### 3 仮想データストアのデフォルト ストレージ ポリシーの変更

VMware では、仮想データストアにプロビジョニングされた仮想マシンについて、デフォルトの要件なしポリシーを提供しています。このポリシーは編集できませんが、新規作成したポリシーをデフォルトとして指定できます。

## Virtual Volumes の仮想マシン ストレージ ポリシーの定義

仮想データストアと互換性のある仮想マシン ストレージ ポリシーを作成できます。

### 前提条件

Virtual Volumes ストレージ プロバイダを使用できることと、アクティブであることを確認します。[仮想ボリュームのストレージ プロバイダの登録](#)を参照してください。

### 手順

- 1 vSphere Web Client のホームで、[ポリシーおよびプロファイル] - [仮想マシン ストレージ ポリシー] の順にクリックします。
- 2 [仮想マシン ストレージ ポリシーを新規作成します] アイコンをクリックします。
- 3 vCenter Server インスタンスを選択します。
- 4 ストレージ ポリシーの名前と説明を入力して、[次へ] をクリックします。

- 5 [ルール セット] ページで、[データ サービスに基づくルール] ドロップダウン メニューから Virtual Volumes ストレージ プロバイダを選択します。

ページが展開され、Virtual Volumes ストレージ リソースによって提供されるデータ サービスが表示されます。

- 6 含めるデータ サービスを選択し、その値を指定します。

指定する値が、Virtual Volumes プロファイルによって通知される値の範囲内であることを確認します。

ストレージ消費量メカニズムによって、仮想データストアに配置される仮想ディスクに必要な容量が入力に基づいて計算されます。

- 7 ストレージ ポリシーの作成を完了させて、[終了] をクリックします。

## 結果

Virtual Volumes と互換性のある新しい仮想マシン ストレージ ポリシーがリストに表示されます。

## 次のステップ

これで、このポリシーを仮想マシンに関連付けたり、デフォルトとしてポリシーを指定したりできます。

## 仮想マシンへの仮想ボリューム ストレージ ポリシーの割り当て

仮想マシンを割り当てるときに、仮想データストアが特定のストレージ要件を満たすよう保証するには、仮想ボリューム ストレージ ポリシーを仮想マシンに関連付けます。

仮想ボリューム ストレージ ポリシーを割り当てることができるのは、仮想マシンの初期デプロイ中か、またはクローン作成や移行などのその他の仮想マシンの操作を実行するときです。このトピックでは、新しい仮想マシンの作成時に仮想ボリューム ストレージ ポリシーを割り当てる方法を説明します。仮想マシンのその他のプロビジョニング方法については、『vSphere 仮想マシン管理』ドキュメントを参照してください。

同じストレージ ポリシーを、仮想マシンの構成ファイルとそのすべての仮想ディスクに適用することができます。仮想ディスクと構成ファイルのストレージ要件が異なる場合は、別のストレージ ポリシーを仮想マシンの構成ファイルおよび選択した仮想ディスクに関連付けることができます。

## 手順

- 1 vSphere Web Client で、仮想マシンのプロビジョニング プロセスを開始し、次の該当するステップに従います。
- 2 すべての仮想マシンのすべてのファイルおよびディスクに同じストレージ ポリシーを割り当てます。
  - a [ストレージの選択] ページの [仮想マシン ストレージ ポリシー] ドロップダウン メニューで、VVols Silver などの仮想ボリュームに適合するストレージ ポリシーを選択します。
  - b 使用可能なデータストアのリストから仮想データストアを選択し、[次へ] をクリックします。

そのデータストアは、仮想マシン構成ファイルとすべての仮想ディスクのターゲット ストレージ リソースとなります。

### 3 仮想ディスクのストレージ ポリシーを変更します。

仮想ディスクごとにストレージ配置の要件が異なる場合は、このオプションを使用します。

- a [ハードウェアのカスタマイズ] ページで、[新規ハードディスク] ペインを展開します。
- b [仮想マシン ストレージ ポリシー] ドロップダウン メニューで、仮想ディスクに割り当てる VVol Gold などの適切なストレージ ポリシーを選択します。

### 4 仮想マシンのプロビジョニング プロセスを完了します。

#### 結果

仮想マシンの作成後は、[サマリ] タブに、割り当てられたストレージ ポリシーとそのコンプライアンス ステータスが表示されます。

#### 次のステップ

構成ファイルまたは仮想ディスクのストレージ配置要件を変える場合は、後で仮想ポリシー割り当てを変更できます。[仮想マシンのファイルとディスク用ストレージ ポリシー割り当ての変更](#) を参照してください。

## 仮想データストアのデフォルト ストレージ ポリシーの変更

VMware では、仮想データストアにプロビジョニングされた仮想マシンについて、デフォルトの要件なしポリシーを提供しています。このポリシーは編集できませんが、新規作成したポリシーをデフォルトとして指定できます。

#### 前提条件

仮想ボリュームと互換性のあるストレージ ポリシーを作成します。

#### 手順

- 1 デフォルト ストレージ ポリシーを変更する仮想データストアを参照します。
- 2 [管理] タブをクリックし、[設定] をクリックします。
- 3 [全般] をクリックし、[デフォルト ストレージ ポリシー] ペインの [編集] をクリックします。
- 4 使用可能なストレージ ポリシーのリストから、デフォルトとして指定するポリシーを選択し、[OK] をクリックします。

#### 結果

選択したストレージ ポリシーが、仮想データストアのデフォルト ポリシーになります。他のポリシーが明示的に選択されていない場合、仮想データストアにプロビジョニングする仮想マシン オブジェクトにこのポリシーが割り当てられます。

# 仮想マシン ストレージ ポリシー

# 20

仮想マシンのストレージ ポリシーは、仮想マシンのプロビジョニングに不可欠です。これらのポリシーにより、仮想マシンのストレージ要件を定義し、仮想マシン用に準備するストレージのタイプ、仮想マシンをストレージ内に配置する方法、および仮想マシンに提供するデータ サービスを管理することができます。

ストレージ ポリシーを定義するときには、仮想マシンで実行するアプリケーションのストレージ要件を指定します。このストレージ ポリシーを仮想マシンに適用すると、仮想マシンは、ストレージ要件を満たすことができる特定のデータストアに配置されます。Virtual SAN や仮想ボリュームなどのソフトウェア定義のストレージ環境では、ストレージ ポリシーにより、必要なサービス レベルを保証するためにストレージ リソース内で仮想マシンのストレージ オブジェクトがどのようにしてプロビジョニングされて割り当てられるかも決定されます。サードパーティ I/O フィルタがインストールされている環境では、ストレージ ポリシーを使用して、仮想ディスクのキャッシュやレプリケーションなどのデータ サービスの追加レベルを有効にできます。

この章には、次のトピックが含まれています。

- [レガシー ストレージ プロファイルのアップグレード](#)
- [仮想マシンのストレージ ポリシーについて](#)
- [仮想マシン ストレージ ポリシーの操作](#)
- [仮想マシン ストレージ ポリシーの作成と管理](#)
- [ストレージ ポリシーと仮想マシン](#)

## レガシー ストレージ プロファイルのアップグレード

vSphere 5.x では、仮想マシン ストレージ ポリシーはストレージ プロファイルと呼ばれ、異なる形式で記述されていました。vSphere 環境をバージョン 5.x から vSphere 6.x にアップグレードすると、前のバージョンで作成したストレージ プロファイルはストレージ ポリシーに変換されます。

レガシー ストレージ プロファイルのコンポーネントすべてが、新しい形式またはオブジェクトに変換されます。すべてのシステム定義ストレージ機能は、メタデータを基にストレージ固有のデータ サービスに変換されます。ユーザー定義機能はデータストア タグになります。

表 20-1. ストレージ ポリシーの新旧形式

vSphere 5.x	vSphere 6.x
仮想マシン ストレージ プロファイル	仮想マシン ストレージ ポリシー
システム定義機能	ストレージ固有のデータ サービス

表 20-1. ストレージ ポリシーの新旧形式（続き）

vSphere 5.x	vSphere 6.x
ユーザー定義機能	データストア タグ
該当なし	共通データ サービス

## 仮想マシンのストレージ ポリシーについて

仮想マシンのストレージ ポリシーにより、仮想マシン内でアプリケーションを実行するために、仮想マシンのホーム ファイルと仮想ディスクで必要とされるストレージ特性を取得します。ストレージ ポリシーをいくつか作成して、ストレージ要件のタイプおよびクラスを定義できます。

各ストレージ ポリシーは同時に適用する制約のセットというだけではありません。1つのポリシーには、データストアに固有で、同等に許容可能なストレージ要件を表す、代替のサブポリシーのセット（ルール セット）を含めることができます。vSphere APIs for I/O Filtering を使用する場合、ストレージ ポリシーにすべてのストレージ タイプに共通のルールを含めることができます。このポリシーには、共通ルールのみ、またはデータストア固有のルール セットのみ、あるいはその両方を含めることができます。

仮想マシンを作成、クローン作成、または移行するときに、ストレージ ポリシーを仮想マシンに適用できます。ポリシー要件に適合するデータストアの 1 つに仮想マシンを配置することができます。データストアがポリシー要件に適合するには、次のガイドラインを満たす必要があります。

- I/O フィルタリングおよび共通ルールを使用できない場合、少なくとも 1 つのデータストア固有のルール セットのすべてのルールを、そのデータストアが満たす必要がある。
- 共通ルールが有効になっている場合、すべての共通ルールおよび少なくとも 1 つのルール セットのすべてのルールを、そのデータストアが満たす必要がある。

仮想マシンのホーム ファイル（.vmx、.vmsd、.nvram、.log など）と仮想ディスク（.vmdk）は、別個のストレージ ポリシーを持つことができます。

表 20-2. 仮想マシンのストレージ ポリシーの例

仮想マシン ファイルの例	ストレージ ポリシーの例	ストレージ ポリシーに準拠したデータストアの例
<code>windows_2008r2_test.vmx</code>		
<code>windows_2008r2_test.vmx</code>		
<code>windows_2008r2_test.log</code>		
<code>windows_2008r2_test.nvram</code>	ストレージ ポリシー 2	datastore02、datastore05、datastore10
<code>windows_2008r2_test.vmem</code>		
<code>windows_2008r2_test.vmsd</code>		
<code>windows_2008r2_test.vmdk</code>	ストレージ ポリシー 3	データストア 05
<code>windows_2008r2_test_1.vmdk</code>	ストレージ ポリシー 5	データストア 10



## ストレージ ポリシーとルール

ストレージ ポリシーに追加するルールは、ストレージ固有のデータ サービスおよびタグに基づくルール、または共通ルールにできます。

### ■ 共通ルール

共通ルールは、すべてのタイプのストレージ用の一般的なデータ サービスに基づいており、データストアには依存しません。これらの追加サービスは、vSphere APIs for I/O Filtering を介して開発されたサードパーティ製 I/O フィルタをインストールすると、仮想マシン ストレージ ポリシー インターフェイスで使用可能になります。これらのデータ サービスは、仮想マシン ストレージ ポリシー内で参照できます。

### ■ ストレージ固有のデータ サービスに基づくルール

これらのルールは、Virtual SAN や仮想ボリュームなどのストレージ エンティティがアダプタイズするデータ サービスに基づいています。

### ■ タグに基づくルール

タグに基づくルールは、特定のデータストアに関連付けられたデータストア タグを参照します。複数のタグをデータストアに適用できます。

## 共通ルール

共通ルールは、すべてのタイプのストレージ用の一般的なデータ サービスに基づいており、データストアには依存しません。これらの追加サービスは、vSphere APIs for I/O Filtering を介して開発されたサードパーティ製 I/O フィルタをインストールすると、仮想マシン ストレージ ポリシー インターフェイスで使用可能になります。これらのデータ サービスは、仮想マシン ストレージ ポリシー内で参照できます。

ストレージ固有のルールとは異なり、共通ルールは仮想マシンのストレージの配置やストレージ要件を定義するものではなく、I/O フィルタなどの追加のデータ サービスを仮想マシンで使用可能にします。使用可能になったフィルタは、仮想マシンが稼働しているデータストアに関係なく、次のサービスを提供できます。

- キャッシュ。仮想ディスク データのキャッシュを構成します。このフィルタは、ローカル キャッシュまたはフラッシュ ストレージ デバイスを使用してデータをキャッシュでき、仮想ディスクの IOPS（1 秒あたりの I/O 処理数）やハードウェア使用率を増やすことができます。
- レプリケーション。仮想マシンまたは仮想ディスクを、別のホストやクラスタなどの外部ターゲットにレプリケートします。

I/O フィルタの詳細については、[21 章 仮想マシン I/O のフィルタリング](#)を参照してください。

## ストレージ固有のデータ サービスに基づくルール

これらのルールは、Virtual SAN や仮想ボリュームなどのストレージ エンティティがアダプタイズするデータ サービスに基づいています。

基盤となるストレージに関する情報を vCenter Server に提供するため、Virtual SAN と仮想ボリュームは、VASA プロバイダとも呼ばれるストレージ プロバイダを使用します。ストレージ情報およびデータストアの特性は、特定のデータストア タイプによって提供されるデータ サービスとして、vSphere Web Client の仮想マシン ストレージ ポリシー インターフェイスに表示されます。

1つのデータストアで複数のサービスを提供できます。データ サービスは、データストアで実現可能なサービス品質の概要を示すデータストア プロファイルにグループ化されます。

仮想マシン ストレージ ポリシーのルールを作成する場合は、特定のデータストアがアダプタイズするデータ サービスを参照します。データストアは、このポリシーを使用する仮想マシンに対して、仮想マシンのストレージ要件を満たすことができることを保証します。また、データストアは容量、パフォーマンス、可用性、冗長性などの特定の特性セットを仮想マシンに提供します。

ストレージ プロバイダの詳細については、[25 章 ストレージ プロバイダの使用](#) を参照してください。

## タグに基づくルール

タグに基づくルールは、特定のデータストアに関連付けられたデータストア タグを参照します。複数のタグをデータストアに適用できます。

通常、タグは次の目的を果たします。

- ストレージ プロバイダによって表されないデータストア（VMFS データストア、NFS データストアなど）に、広範なストレージ レベルの定義を適用する。
- 地理的場所や管理グループなど、vSphere API for Storage Awareness (VASA) を介して通知されないポリシー関連情報をエンコードする。

ストレージ固有のサービスと同様に、データストアに関連付けられたすべてのタグは、仮想マシン ストレージ ポリシーのインターフェイスに表示されます。ストレージ ポリシーのルールを定義するときは、これらのタグを使用できます。

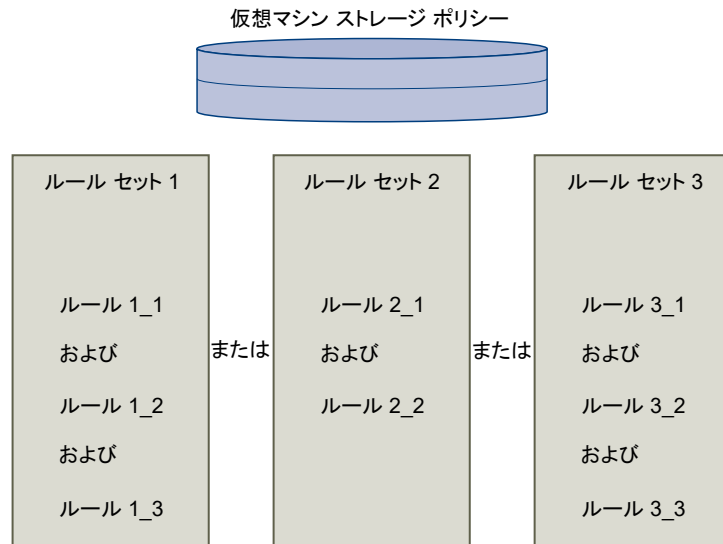
## データストア固有および共通のルール セットについて

ストレージ ポリシーには、仮想マシン ストレージ リソースの要件を記述した 1 つ以上のルール セットを含めることができます。また、共通ルールを含めることもできます。

共通ルールを使用できない環境の場合や共通ルールが定義されていない場合、データストア固有のルール セットを含むポリシーを作成できます。ポリシーを定義するには、1 つのルール セットが必須です。追加のルール セットはオプションです。複数のルール セットで、単一のポリシーが代替用の選択パラメータを定義できるようになります（通常は複数のストレージ プロバイダから）。

単一のルール セットには 1 つ以上のルールが含まれます。各ルールは、ストレージ エンティティで保証される、基盤となる単一のデータ サービスに基づいて定義できます。ルールには、ストレージ リソースが提供しなければならない一定の質および量を記述します。ルールでは、ユーザー定義のデータストア タグも参照できます。1 つのデータストア固有のルール セットには単独のストレージ エンティティからのルールのみを含めることができます。

ポリシー内のすべてのルール セット間の関係はブール演算子 OR で定義されていますが、単一のルール セット内のすべてのルール間関係は AND で定義されています。1 つのルール セット内のすべてのルールを満たせば、ポリシー全体を満たしたことになります。各ルール セットは同等に許容可能な制約のセットを表します。



共通ルールが有効になっている場合、共通ルールまたは 1 つ以上のデータストア固有のルール セットのいずれかを含めるにはポリシーが必要です。共通ルールとデータストア固有のルールの両方を定義する場合、ストレージ ポリシーは、すべての共通ルールと 1 つ以上のルール セットのすべてのルールを満たすデータストアに一致します。

## 仮想マシン ストレージ ポリシーの操作

ストレージ ポリシーの作成および管理を行う場合、通常はそのプロセスで、いくつかの手順を実行します。特定の手順を実行するかどうかは、使用環境で提供されるストレージまたはデータ サービスのタイプによって決まります。

- 1 ストレージ プロバイダでストレージ ポリシーを使用する場合は、適切なストレージ プロバイダが登録されていることを確認します。ストレージ プロバイダを必要とするエンティティには、仮想マシンに追加のソフトウェアデータ サービスを提供する Virtual SAN、Virtual Volumes、I/O フィルタが含まれます。

[25 章 ストレージ プロバイダの使用](#)を参照してください。

- 2 ストレージ タグをデータストアに適用します。 [データストアへのタグの割り当て](#)を参照してください。
- 3 ストレージ ポリシーを作成し、仮想マシンで実行するアプリケーションの要件を定義します。 [仮想マシンのストレージ ポリシーの定義](#)を参照してください。
- 4 仮想マシン ストレージ ポリシーを仮想マシンに適用します。仮想マシンをデプロイする場合、またはその仮想ディスクを構成する場合は、ストレージ ポリシーを適用します。 [仮想マシンへのストレージ ポリシーの割り当て](#)を参照してください。
- 5 仮想マシンのホーム ファイルまたは仮想ディスクのストレージ ポリシーを変更します。 [仮想マシンのファイルとディスク用ストレージ ポリシー割り当ての変更](#)を参照してください。
- 6 仮想マシンと仮想ディスクが、割り当てられたストレージ ポリシーに準拠するデータストアを使用していることを確認します。 [仮想マシン ストレージ ポリシーのコンプライアンスの確認](#)を参照してください。

## 仮想マシン ストレージ ポリシーの作成と管理

仮想マシンのストレージ ポリシーを有効化、作成、および管理するには、通常、vSphere Web Client の仮想マシン ストレージ ポリシーのインスタンスを使用できます。

Virtual SAN、仮想ボリューム、または I/O フィルタでストレージ ポリシーを使用する場合は、詳細について次のドキュメントを参照してください。

- VMware Virtual SAN の管理
- 19 章 仮想ボリュームの操作
- 21 章 仮想マシン I/O のフィルタリング

## データストアへのタグの割り当て

ストレージ プロバイダでデータストアが表示されず、その機能とデータ サービスが仮想マシン ストレージ ポリシー インターフェイスに表示されない場合は、タグを使用してデータストアに関する情報をエンコードします。これらのタグは、仮想マシンのストレージ ポリシーを定義するときに参照できます。

ストレージ情報を含む新しいタグをデータストアに適用できます。タグ、タグのカテゴリ、およびタグの管理方法の詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。

### 手順

- 1 vSphere Web Client ナビゲータで、データストアを参照します。
- 2 [管理] タブをクリックし、[タグ] をクリックします。
- 3 [新しいタグ] アイコンをクリックします。
- 4 [vCenter Server] ドロップダウン メニューで、タグを作成する vCenter Server インスタンスを選択します。
- 5 タグの名前と説明を入力します。

たとえば、Gold Storage などのストレージ レベルの広範囲な定義を指定するか、地理的な場所や管理グループなどのストレージ プロバイダ経由ではやり取りしないプロパティを指定することができます。

タグのプロパティ 例	
名前	Fault Tolerance
説明	2 TB を超える容量とフォールト トレランス機能を持つストレージ。

- 6 [カテゴリ] ドロップダウン メニューで、既存のカテゴリを選択するか、カテゴリを作成します。
- 7 (オプション) カテゴリを作成します。
  - a [新しいカテゴリ] を選択します。
  - b カテゴリ オプションを指定します。

カテゴリ プロパティ	例
カテゴリ名	ストレージ カテゴリ
説明	ストレージに関連するタグのカテゴリ
カーディナリティ	[オブジェクトあたりに多数のタグ]
関連付け可能なオブジェクト タイプ	[データストア]および[データストア クラス]

- 8 [OK] をクリックします。

## 結果

新しいタグがデータストアに割り当てられ、[タグ] ペインのデータストアの [サマリ] タブに表示されます。

## 次のステップ

タグ ベースのルールをストレージ ポリシーに追加するときに、タグを参照できます。[タグ ベースのルールの追加または編集](#)を参照してください。データストアは、ポリシーを使用する仮想マシンに対して互換性のあるストレージ リソースのリストに表示されます。

## 仮想マシンのストレージ ポリシーの定義

仮想マシンのストレージ ポリシーを定義する場合は、その仮想マシンで実行されるアプリケーションのストレージ要件を指定します。

ストレージ ポリシーは、ストレージ エンティティによってアダプタイズされるデータ サービスに基づいて、またはデータストア タグに基づいて定義できます。ポリシーは、I/O フィルタ フレームワークで提供される共通データ サービスを参照することもできます。

## 前提条件

- ストレージ プロバイダで仮想マシンのストレージ ポリシーを使用する場合は、適切なストレージ プロバイダが登録されていることを確認します。[25 章 ストレージ プロバイダの使用](#)を参照してください。
- 必要な権限：仮想マシン ストレージ ポリシー.更新および仮想マシン ストレージ ポリシー.表示

## 手順

### 1 [仮想マシン ストレージ ポリシー作成プロセスの開始](#)

仮想マシンのストレージ ポリシーを定義するには、[仮想マシン ストレージ ポリシーの新規作成] ウィザードを使用します。

### 2 [仮想マシン ストレージ ポリシーの共通ルールの定義](#)

共通ルールは、すべてのタイプのストレージ用の一般的なデータ サービスに基づいており、データストアには依存しません。vSphere APIs for I/O Filtering を使用して開発したサードパーティの I/O フィルタをインストールすると、[仮想マシン ストレージ ポリシー] インターフェイスでこれらのデータ サービスが使用可能になります。これらのデータ サービスはストレージ ポリシーで参照できます。

### 3 [仮想マシン ストレージ ポリシーのストレージ固有ルールの作成](#)

データストアに固有のルールは、Virtual SAN や仮想ボリュームなどのストレージ エンティティがアダプタイズするデータ サービスに基づいています。データストアは、このポリシーを使用する仮想マシンに対して、仮想マシンのストレージ要件を満たすことができることを保証します。また、データストアは、容量、パフォーマンス、可用性、冗長性などについて、特定の特性セットを提供することも保証します。

### 4 [タグ ベースのルールの追加または編集](#)

仮想マシンのストレージ ポリシーを定義または編集するときに、特定のデータストアに使用したタグを参照するルールを作成または変更できます。データストアはそのタイプのストレージ ポリシーと互換性を持つようになります。

## 5 仮想マシン ストレージ ポリシー作成の完了

仮想マシン ストレージ ポリシーとの互換性があるデータストアのリストを確認し、任意のストレージ ポリシー設定を変更することができます。

### 次のステップ

このストレージ ポリシーは、仮想マシンに適用できます。Virtual SAN や仮想ボリュームなどのオブジェクトベースのストレージを使用する場合は、このストレージ ポリシーをデフォルトに指定できます。

## 仮想マシン ストレージ ポリシー作成プロセスの開始

仮想マシンのストレージ ポリシーを定義するには、[仮想マシン ストレージ ポリシーの新規作成] ウィザードを使用します。

### 手順

- 1 vSphere Web Client の [ホーム] で、[ポリシーおよびプロファイル] - [仮想マシン ストレージ ポリシー] をクリックします。
- 2 [仮想マシン ストレージ ポリシーを新規作成します] アイコンをクリックします。
- 3 vCenter Server インスタンスを選択します。
- 4 ストレージ ポリシーの名前と説明を入力します。

## 仮想マシン ストレージ ポリシーの共通ルールの定義

共通ルールは、すべてのタイプのストレージ用の一般的なデータ サービスに基づいており、データストアには依存しません。vSphere APIs for I/O Filtering を使用して開発したサードパーティの I/O フィルタをインストールすると、[仮想マシン ストレージ ポリシー] インターフェイスでこれらのデータ サービスが使用可能になります。これらのデータ サービスはストレージ ポリシーで参照できます。

### 手順

- 1 [共通ルール] ページで [ストレージ ポリシーでの共通ルールの使用] を選択して、共通ルールを有効にします。
- 2 [ルールの追加] ドロップダウン メニューから、ルールに含めるデータ サービスを選択します。
- 3 データ サービスのプロバイダを選択します。

同じデータ サービス（レプリケーションなど）が異なるプロバイダによって提供される場合、このデータ サービスを参照する複数のルールを追加することはできません。

- 4 ルールの値を指定して [次へ] をクリックします。

## 仮想マシン ストレージ ポリシーのストレージ固有ルールの作成

データストアに固有のルールは、Virtual SAN や仮想ボリュームなどのストレージ エンティティがアダプタイズするデータ サービスに基づいています。データストアは、このポリシーを使用する仮想マシンに対して、仮想マシンのストレージ要件を満たすことができることを保証します。また、データストアは、容量、パフォーマンス、可用性、冗長性などについて、特定の特性セットを提供することも保証します。

1つのデータストア固有のルール セットには単独のストレージ エンティティからのルールのみを含めることができます。

## 前提条件

使用する環境に Virtual SAN や仮想ボリュームなどのストレージ エンティティが含まれる場合は、それらの機能について再確認してください。詳細については、『VMware Virtual SAN の管理』ドキュメントおよび [19 章 仮想ボリュームの操作](#)を参照してください。

## 手順

- 1 [ルール セット] ページの [データ サービスに基づくルール] ドロップダウン メニューで、Virtual SAN や仮想ボリュームなどのストレージ プロバイダを選択します。

ページが展開され、ストレージ リソースによって提供されるデータ サービスが表示されます。

- 2 含めるデータ サービスを選択し、その値を指定します。

入力する値が、ストレージ リソースがアダプタイズするデータ サービス プロファイルの値の範囲内にあることを確認します。

ユーザー入力に基づき、ストレージ消費メカニズムによって、このストレージ エンティティに存在する仮想ディスクで必要とされる領域のサイズが計算されます。

- 3 (オプション) タグ ベースのルールを追加します。

- 4 [次へ] をクリックします。

## タグ ベースのルールの追加または編集

仮想マシンのストレージ ポリシーを定義または編集するときに、特定のデータストアに使用したタグを参照するルールを作成または変更できます。データストアはそのタイプのストレージ ポリシーと互換性を持つようになります。

ストレージ固有のルールが含まれるルール セットにタグ ベースのルールを追加したり、タグ ベースのルールのみが含まれる個別のルール セットを作成したりできます。ポリシーでタグを使用する場合は、次のガイドラインに従ってください。

- ルール セットに他のストレージ固有ルールが含まれている場合、割り当てられたタグを含むデータストアはルール セット内のすべてのルールを満たす必要があります。
- 同じカテゴリの複数のタグを同じルールに追加すると、それらのタグは代替制限として処理されます。どちらかのタグを満たすことができます。
- 同じルール セット内の別個のルールにタグを追加する場合は、すべてのタグが満たされる必要があります。

## 前提条件

ストレージ タグを作成し、データストアに適用します。 [データストアへのタグの割り当て](#) を参照してください。

## 手順

- 1 [ルール セット] ページで、タグ ベースのルールを追加または編集します。

- ルールを追加するには、[タグ ベースのルールの追加] ボタンをクリックします。
- 既存のルールを変更するには、ルールを選択して[ルールの変更] アイコンをクリックします。

- 2 カテゴリを指定してください。

- 3 タグを選択するか、既存の選択内容を編集します。

## 結果

選択されたタグを使用するデータストアは、ストレージ ポリシーと互換性があります。

## 仮想マシン ストレージ ポリシー作成の完了

仮想マシン ストレージ ポリシーとの互換性があるデータストアのリストを確認し、任意のストレージ ポリシー設定を変更することができます。

## 手順

- 1 [ストレージ互換性] ページでこのポリシーに適合するデータストアのリストを確認し、[次へ] をクリックします。

使用可能にするには、データストアが少なくとも 1 つのルール セットおよびそのセット内のすべてのルールを満たしている必要があります。

- 2 ストレージ ポリシーの設定を確認し、[戻る] をクリックして関連するページに戻って変更を行います。
- 3 [終了] をクリックします。

## 結果

仮想マシンのストレージ ポリシーがリストに表示されます。

## 仮想マシン ストレージ ポリシーの削除

どの仮想マシンまたは仮想ディスクにも使用していないストレージ ポリシーを削除できます。

## 手順

- 1 vSphere Web Client のホームで、[ポリシーおよびプロファイル] - [仮想マシン ストレージ ポリシー] の順にクリックします。
- 2 [仮想マシン ストレージ ポリシー] インターフェイスで、削除するポリシーを選択し、[仮想マシン ストレージ ポリシーを削除します] アイコン (✖) をクリックします。
- 3 [Yes] をクリックします。

## 結果

ポリシーがインベントリから削除されます。

## 仮想マシン ストレージ ポリシーの編集またはクローン作成

仮想マシンと仮想ディスクのストレージ要件を変える場合は、既存のストレージ ポリシーを変更できます。また、クローン作成することにより、既存の仮想マシン ストレージ ポリシーのコピーを作成できます。クローン作成中に、必要に応じて元のストレージ ポリシーをカスタマイズする選択ができます。

## 前提条件

必要な権限 : StorageProfile.View



## 手順

- 1 vSphere Web Client のホームで、[ポリシーおよびプロファイル] - [仮想マシン ストレージ ポリシー] の順にクリックします。
- 2 ストレージ ポリシーを選択し、次のいずれかのアイコンをクリックします。
  - [仮想マシン ストレージ ポリシーを編集します]
  - [仮想マシン ストレージ ポリシーのクローンを作成します]
- 3 (オプション) ポリシーを変更し、[OK] をクリックします。
- 4 仮想マシンが使用するストレージ ポリシーを編集する場合は、その仮想マシンにポリシーを再適用します。

オプション	説明
後で手動で行う	このオプションを選択すると、ストレージ ポリシーに関連付けられたすべての仮想ディスクと仮想マシンのホーム オブジェクトのコンプライアンス状態は期限切れに変更されます。構成とコンプライアンスを更新するには、関連付けられたすべてのエンティティにストレージ ポリシーを手動で再適用します。 <a href="#">仮想マシン ストレージ ポリシーの再適用</a> を参照してください。
今すぐ	ストレージ ポリシーを編集した後すぐに、仮想マシンとコンプライアンス ステータスを更新します。

## ストレージ ポリシーと仮想マシン

仮想マシン ストレージ ポリシーを定義したら、そのストレージ ポリシーを仮想マシンに適用できます。仮想マシンのプロビジョニングまたはその仮想ディスクの構成時に、ストレージ ポリシーを適用します。ポリシーはそのタイプと構成に応じて、さまざまな役割を果たします。ポリシーを使用すると、仮想マシンに最も適したデータストアを選択し、必要なレベルのサービスを適用できます。また仮想マシンとそのディスクで、特定のデータ サービスを有効にすることができます。

ストレージ ポリシーを指定しない場合は、データストアに関連付けられているデフォルトのストレージ ポリシーが使用されます。仮想マシン上のアプリケーションに対するストレージ要件が変わると、最初に仮想マシンに適用されたストレージ ポリシーを変更できます。

## デフォルト ストレージ ポリシー

Virtual SAN や仮想ボリュームなどのオブジェクトベースのデータストア上で仮想マシンをプロビジョニングする場合は、データストアと互換性のある適切な仮想マシン ストレージ ポリシーを仮想マシンに割り当てる必要があります。この割り当てにより、オブジェクトベースのストレージ内に仮想マシン オブジェクトが適切に配置されます。仮想マシンにストレージ ポリシーを明示的に割り当てない場合は、データストアに関連付けられているデフォルトのストレージ ポリシーが使用されます。割り当てたポリシーに、仮想ボリュームまたは Virtual SAN 固有のルールが含まれていない場合にも、デフォルト ポリシーが使用されます。

Virtual SAN および仮想ボリュームのデフォルトのストレージ ポリシーは、VMware から提供される場合も、ユーザーによって定義される場合もあります。VMFS および NFS データストアには、デフォルトのポリシーはありません。

## VMware によって提供されるデフォルト ポリシー

VMware では、Virtual SAN と仮想データストアを対象とするデフォルト ストレージ ポリシーを提供しています。

### Virtual SAN のデフォルト ストレージ ポリシー

VMware が提供するデフォルト ストレージ ポリシーは、他の Virtual SAN ポリシーを選択しない場合に、Virtual SAN データストアでプロビジョニングされるすべての仮想マシン オブジェクトに適用されます。

VMware によって提供されるポリシーには、次の特性があります。

- ポリシーを削除することはできません。
- ポリシーは編集可能です。ポリシーを編集するには、表示権限と更新権限が含まれるストレージ ポリシー権限が必要です。
- ポリシーを編集する場合、ポリシーの名前や Virtual SAN ストレージ プロバイダの仕様を変更することはできません。ルールを含む他のすべてのパラメータを編集できます。
- デフォルト ポリシーのクローンを作成し、ストレージ ポリシーを作成するためのテンプレートとして使用できます。
- Virtual SAN のデフォルト ポリシーは、Virtual SAN データストアとのみ互換性があります。
- Virtual SAN の仮想マシン ストレージ ポリシーを作成し、そのポリシーをデフォルトに指定できます。

### 仮想ボリュームのデフォルト ストレージ ポリシー

仮想ボリューム用として、VMware では、ルールやストレージ要件を何も含んでいないデフォルト ストレージ ポリシーを提供しています。Virtual SAN の場合と同様、このポリシーは、仮想データストアに配置する仮想マシンに別のポリシーを指定しない場合に、仮想マシン オブジェクトに適用されます。要件なしのポリシーにより、ストレージ アレイでは、仮想マシン オブジェクトの最適な配置を決定できます。

VMware によって提供されるデフォルトの仮想ボリューム ポリシーには、次の特性があります。

- このポリシーは、削除、編集、およびクローン作成できません。
- 仮想ボリュームのデフォルト ポリシーは、仮想データストアとのみ互換性があります。
- 仮想ボリュームの仮想マシン ストレージ ポリシーを作成し、そのポリシーをデフォルトに指定できます。

### 仮想マシン ストレージのユーザー定義のデフォルト ポリシー

Virtual SAN または仮想ボリュームと互換性のある仮想マシン ストレージ ポリシーを作成して、そのポリシーを Virtual SAN および仮想データストアのデフォルト ポリシーとして指定できます。VMware が提供するデフォルト ストレージ ポリシーは、ユーザー定義のデフォルト ポリシーに置き換えられます。

各 Virtual SAN および仮想データストアには、1 度に 1 つのデフォルト ポリシーのみを設定できます。ただし、複数の Virtual SAN および仮想ボリュームのデータストアに対応する単一のストレージ ポリシーを作成して、そのポリシーを、すべてのデータストアのデフォルト ポリシーとして指定できます。

仮想マシン ストレージ ポリシーがデータストアのデフォルト ポリシーになると、そのポリシーは、データストアとの関連付けを解除しなければ、削除できません。

## データストアのデフォルト ストレージ ポリシーの変更

仮想ボリュームと Virtual SAN データストアには、仮想マシンのプロビジョニング中にデフォルトとして使用されるストレージ ポリシーが用意されています。選択した仮想ボリュームまたは Virtual SAN データストアのデフォルトのストレージ ポリシーは、変更することができます。

### 前提条件

仮想ボリュームまたは Virtual SAN に適合するストレージ ポリシーを作成します。両方のタイプのストレージに適合するポリシーを作成できます。

### 手順

- 1 vSphere Web Client ナビゲータで、[グローバル インベントリ リスト] - [データストア] の順に選択します。
- 2 データストアをクリックします。
- 3 [管理] タブをクリックして、[設定] をクリックします。
- 4 [全般] をクリックし、[デフォルト ストレージ ポリシー] ペインの [編集] をクリックします。
- 5 選択可能なストレージ ポリシーの一覧から、デフォルトとして指定するポリシーを選択し、[OK] をクリックします。

### 結果

選択したストレージ ポリシーは、データストアのデフォルトのポリシーとなります。vSphere は、他に選択されたポリシーがない場合、データストアでプロビジョニングするすべての仮想マシン オブジェクトにこのポリシーを割り当てます。

## 仮想マシンへのストレージ ポリシーの割り当て

仮想マシンの初回デプロイ時、またはクローン作成や移行などの他の仮想マシン操作の実行時に、仮想マシン ストレージ ポリシーを割り当てることができます。

ここでは、仮想マシンの作成時に仮想マシン ストレージ ポリシーを割り当てる方法を説明します。クローン作成、テンプレートからのデプロイなど、他のデプロイ方法の詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。

同じストレージ ポリシーを、仮想マシンの構成ファイルとそのすべての仮想ディスクに適用することができます。仮想ディスクと構成ファイルのストレージ要件が異なる場合は、別のストレージ ポリシーを仮想マシンの構成ファイルおよび選択した仮想ディスクに関連付けることができます。

### 手順

- 1 vSphere Web Client で、仮想マシン プロビジョニング プロセスを開始し、適切な手順に従ってください。

## 2 すべての仮想マシンのすべてのファイルおよびディスクに同じストレージ ポリシーを割り当てます。

- a [ストレージの選択] ページで、[仮想マシン ストレージ ポリシー] ドロップダウン メニューからストレージ ポリシーを選択します。

ストレージ ポリシーでは、その構成に基づいて、すべてのデータストアを互換性のあるセットと互換性のないセットにわけます。ポリシーが特定のストレージ エンティティ（仮想ボリュームなど）から提供されるデータ サービスを参照する場合、互換性リストには、そのタイプのストレージのみを示すデータストアが含まれます。

- b 互換性のあるデータストアのリストから適切なデータストアを選択して、[次へ] をクリックします。

そのデータストアは、仮想マシン構成ファイルとすべての仮想ディスクのターゲット ストレージ リソースとなります。

## 3 仮想ディスクの仮想マシン ストレージ ポリシーを変更します。

仮想ディスクごとにストレージ配置の要件が異なる場合は、このオプションを使用します。キャッシュや複製などのソフトウェア データ サービスを仮想ディスクで有効化する必要がある場合にも、このオプションを使用できます。

- a [ハードウェアのカスタマイズ] ページで、[新規ハード ディスク] ペインを展開します。
- b [仮想マシン ストレージ ポリシー] ドロップダウン メニューから、仮想ディスクに割り当てるストレージ ポリシーを選択します。
- c （オプション） 仮想ディスクのストレージの場所を変更します。

仮想マシン構成ファイルが格納されているデータストア以外のデータストアに仮想ディスクを格納する場合は、このオプションを使用します。

## 4 仮想マシンのプロビジョニング プロセスを完了します。

### 結果

仮想マシンの作成後は、[サマリ] タブに、割り当てられたストレージ ポリシーとそのコンプライアンス ステータスが表示されます。

### 次のステップ

構成ファイルまたは仮想ディスクのストレージ配置要件を変える場合は、後で仮想ポリシー割り当てを変更できます。

## 仮想マシンのファイルとディスク用ストレージ ポリシー割り当ての変更

仮想マシン上のアプリケーションに対するストレージ要件が変わった場合、最初に仮想マシンに適用されたストレージ ポリシーを編集できます。

パワーオフ状態またはパワーオン状態の仮想マシンのストレージ ポリシーを編集できます。

仮想マシン ストレージ ポリシーの割り当てを変更する際、同じストレージ ポリシーを仮想マシン構成ファイルと、そのすべての仮想ディスクに適用できます。仮想ディスクと構成ファイルのストレージ要件が異なる場合は、別のストレージ ポリシーを仮想マシンの構成ファイルおよび選択した仮想ディスクに関連付けることができます。

**手順**

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 [管理] タブをクリックし、[ポリシー] をクリックします。
- 3 [ストレージ] をクリックします。
- 4 [仮想マシン ストレージ ポリシーの編集] をクリックします。
- 5 仮想マシンの仮想マシン ストレージ ポリシーを指定します。

オプション	説明
同じストレージ ポリシーをすべての仮想マシン オブジェクトに適用します。	a [仮想マシン ストレージ ポリシー] ドロップダウン メニューから、ポリシーを選択します。 b [すべてに適用] をクリックします。
さまざまなストレージ ポリシーを、仮想マシン ホーム オブジェクトおよび仮想ディスクに適用します。	a オブジェクトを選択します。 b [仮想マシン ストレージ ポリシー] ドロップダウン メニューから、オブジェクトのポリシーを選択します。

- 6 [OK] をクリックします。

**結果**

ストレージ ポリシーが仮想マシンとそのディスクに割り当てられます。

## 仮想マシンのストレージ コンプライアンスの監視

仮想マシン オブジェクトにポリシーを関連付け、仮想マシンおよび仮想ディスクを実行するデータストアを選択すると、仮想マシンおよび仮想ディスクがポリシーに準拠しているデータストアを使用しているかどうかを確認できます。

仮想マシンのホストまたはクラスタでストレージ ポリシーが無効にされている場合に仮想マシンのコンプライアンスを確認すると、機能が無効であるため確認の結果は非準拠となります。

**前提条件**

ストレージ ポリシーのコンプライアンス チェックを実行するには、そのポリシーを少なくとも 1 つの仮想マシンまたは仮想ディスクと関連付けます。

**手順**

- 1 vSphere Web Client のホームで、[ポリシーおよびプロファイル] - [仮想マシン ストレージ ポリシー] の順にクリックします。
- 2 ストレージ ポリシーをダブルクリックします。
- 3 [監視] タブをクリックし、[仮想マシンと仮想ディスク] をクリックします。
- 4 [仮想マシン ストレージ ポリシーのコンプライアンス チェックのトリガ] をクリックします。  
  
[コンプライアンス ステータス] 列に仮想マシンおよびポリシーのストレージのコンプライアンス ステータスが表示されます。

コンプライアンス ステータス	説明
準拠	仮想マシンまたは仮想ディスクが使用するデータストアには、ポリシーで必要とされるストレージ機能があります。
コンプライアンスに非準拠	データストアは特定のストレージ要件をサポートしますが、現在は仮想マシン ストレージ ポリシーを満たすことができません。たとえば、データストアをバックアップする物理リソースが使用不可またはすべて使用済みの場合に、ステータスが「非準拠」になることがあります。ホストやディスクをクラスタに追加する方法などで、物理構成を変更するとデータベースを準拠させることができます。その他のリソースが仮想マシン ストレージ ポリシーを満たす場合は、ステータスが「準拠」に変わります。
旧バージョン	このステータスは、ポリシーが編集されており、新しい要件が仮想マシン オブジェクトが存在するデータストアに伝送されていないことを示しています。変更を伝送するには、ポリシーを旧バージョンのオブジェクトに再適用します。
該当なし	ストレージ ポリシーが、仮想マシンが存在するデータストアにサポートされていないデータストア機能を参照しています。

### 次のステップ

非準拠データストアを準拠データストアにできない場合は、ファイルまたは仮想ディスクを互換性のあるデータストアに移行します。[互換性のない仮想マシン向けの互換性のあるストレージ リソースの検索](#) を参照してください。

ステータスが「期限切れ」の場合には、ポリシーをオブジェクトに再適用します。[仮想マシン ストレージ ポリシーの再適用](#) を参照してください。

## 仮想マシン ストレージ ポリシーのコンプライアンスの確認

仮想マシン ストレージ ポリシーで指定されたストレージ要件と互換性のあるデータストアが仮想マシンで使用されているかどうかを確認できます。

### 前提条件

仮想マシンに関連付けられたストレージ ポリシーがあることを確認します。

### 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 右クリック メニューから、[仮想マシン ポリシー] - [仮想マシン ストレージ ポリシーのコンプライアンスのチェック] を選択します。  
  
システムによりコンプライアンスが検証されます。
- 3 仮想マシンの [サマリ] タブをクリックします。
- 4 [仮想マシン ストレージ ポリシー] ペインでコンプライアンス ステータスを確認します。

コンプライアンス ステータス	説明
準拠	仮想マシンまたは仮想ディスクが使用するデータストアには、ポリシーで必要とされるストレージ機能があります。
コンプライアンスに非準拠	データストアは特定のストレージ要件をサポートしますが、現在は仮想マシン ストレージ ポリシーを満たすことができません。たとえば、データストアをバックアップする物理リソースが使用不可またはすべて使用済みの場合に、ステータスが「非準拠」になることがあります。ホストやディスクをクラスタに追加する方法などで、物理構成を変更するとデータベースを準拠させることができます。その他のリソースが仮想マシン ストレージ ポリシーを満たす場合は、ステータスが「準拠」に変わります。

#### コンプライア ンス ステータ ス

#### 説明

旧バージョン	このステータスは、ポリシーが編集されており、新しい要件が仮想マシン オブジェクトが存在するデータストアに伝送されていないことを示しています。変更を伝送するには、ポリシーを旧バージョンのオブジェクトに再適用します。
該当なし	ストレージ ポリシーが、仮想マシンが存在するデータストアにサポートされていないデータストア機能を参照しています。

#### 次のステップ

非準拠データストアを準拠データストアにできない場合は、ファイルまたは仮想ディスクを互換性のあるデータストアに移行します。[互換性のない仮想マシン向けの互換性のあるストレージ リソースの検索](#) を参照してください。

ステータスが「期限切れ」の場合には、ポリシーをオブジェクトに再適用します。[仮想マシン ストレージ ポリシーの再適用](#) を参照してください。

## 互換性のない仮想マシン向けの互換性のあるストレージ リソースの検索

どのデータストアが仮想マシンに関連付けられているストレージ ポリシーと互換性があるかを判断します。

場合によっては、仮想マシンに割り当てられたストレージ ポリシーが非準拠の状態になっていることがあります。この状態は、仮想マシンまたはそのディスクがポリシーと互換性のないデータストアを使用していることを示します。仮想マシン ファイルおよびその仮想ディスクを、互換性のあるデータストアに移行できます。

このタスクを使用してどのデータストアがポリシーの要件を満たしているかを判断します。

#### 前提条件

仮想マシンの [サマリ] タブの [仮想マシン ストレージ ポリシーのコンプライアンス] フィールドに「非準拠」の状態が表示されていることを確認します。

#### 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 [サマリ] タブをクリックします。  
[仮想マシン ストレージ ポリシー] ペインの [仮想マシン ストレージ ポリシーのコンプライアンス] パネルに「非準拠」の状態が表示されます。
- 3 [仮想マシン ストレージ ポリシー] パネルにあるポリシーのリンクをクリックします。
- 4 [監視] タブをクリックし、[仮想マシンと仮想ディスク] をクリックしてどの仮想マシンのファイルが非準拠であるか判断します。
- 5 [ストレージ互換性] をクリックします。  
ポリシーの要件に一致するデータストアのリストが表示されます。

#### 次のステップ

仮想マシンまたはそのディスクをリストのいずれかのデータストアに移行できます。

## 仮想マシン ストレージ ポリシーの再適用

仮想マシン オブジェクトにすでに関連付けられているストレージ ポリシーを編集した後は、ポリシーを再適用する必要があります。ポリシーを再適用することにより、新しいストレージ要件を仮想マシン オブジェクトが存在するデータストアに伝送します。

### 前提条件

仮想マシンのコンプライアンス ステータスが「期限切れ」です。このステータスは、ポリシーが編集されており、新しい要件がデータストアに伝送されていないことを示しています。

### 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 [管理] タブをクリックし、[ポリシー] をクリックします。
- 3 コンプライアンス ステータスが「期限切れ」になっていることを確認します。
- 4 [仮想マシン ストレージ ポリシーの再適用] アイコンをクリックします。
- 5 [仮想マシン ストレージ ポリシー] ペインでコンプライアンス ステータスを確認します。

コンプライアンス ステータス	説明
準拠	仮想マシンまたは仮想ディスクが使用するデータストアには、ポリシーで必要とされるストレージ機能があります。
コンプライアンス に非準拠	仮想マシンまたは仮想ディスクが使用するデータストアには、ポリシーで必要とされるストレージ機能がありません。仮想マシン ファイルおよびその仮想ディスクを、準拠するデータストアに移行できます。  非準拠データストアを準拠データストアにできない場合は、ファイルまたは仮想ディスクを互換性のあるデータストアに移行します。 <a href="#">互換性のない仮想マシン向けの互換性のあるストレージ リソースの検索</a> を参照してください。
該当なし	ストレージ サービス レベルでは、仮想マシンが存在するデータストアにサポートされていないデータストア機能を参照します。



vSphere APIs for I/O Filtering (VAIO) は、サードパーティが I/O フィルタと呼ばれるソフトウェア コンポーネントを作成できるようにするフレームワークを提供します。

フィルタは ESXi ホストにインストールして、仮想マシンのゲスト OS と仮想ディスク間を移動する I/O 要求を処理することで、仮想マシンに追加のデータ サービスを提供することができます。

この章には、次のトピックが含まれています。

- I/O フィルタについて
- フラッシュ ストレージ デバイスとキャッシュ I/O フィルタの併用
- vSphere 環境での I/O フィルタのデプロイと構成
- I/O フィルタの管理
- I/O フィルタのガイドラインおよびベスト プラクティス

## I/O フィルタについて

仮想ディスクに関連付けられている I/O フィルタは、基盤となるストレージ トポロジに関係なく、仮想マシンの I/O パスへの直接アクセスを取得します。

I/O フィルタは、サードパーティ ベンダーによって作成され、パッケージとして配布されます。このパッケージでは、フィルタ コンポーネントを vCenter Server および ESXi ホスト クラスタにデプロイするためのインストーラが提供されます。

I/O フィルタをインストールし、そのコンポーネントを ESXi クラスタにデプロイしたら、vCenter Server によって、クラスタ内のホストごとに I/O フィルタのストレージ プロバイダ（VASA プロバイダとも呼ばれる）が自動的に構成および登録されます。ストレージ プロバイダは、vCenter Server と通信し、I/O フィルタによって提供されるデータ サービスを仮想マシン ストレージ ポリシー インターフェイスに表示できるようにします。仮想マシン ポリシーの共通ルールを作成するときにこれらのデータ サービスを参照できます。仮想ディスクをこのポリシーに関連付けると、仮想ディスクで I/O フィルタが有効になります。

## I/O フィルタのタイプ

通常、I/O フィルタは VMware パートナーによって vSphere APIs for I/O Filtering (VAIO) 開発者プログラムを介して作成されます。サードパーティ ベンダーは、多目的の I/O フィルタを開発できます。

このリリースでは、次のようなタイプのフィルタがサポートされています。

- キャッシュ。仮想ディスク データのキャッシュを実装します。このフィルタは、ローカル フラッシュ ストレージ デバイスを使用してデータをキャッシュでき、仮想ディスクの IOPS やハードウェア使用率を増やすことができます。キャッシュ フィルタを使用する場合、仮想フラッシュ リソースの構成が必要になることがあります。
- レプリケーション。すべての書き込み I/O 操作を外部ターゲットの場所（別のホストやクラスタなど）にレプリケートします。

---

**注：** 同じカテゴリ（キャッシュなど）の複数のフィルタを ESXi ホストにインストールできます。ただし、同じカテゴリのフィルタは仮想ディスクごとに 1 つしか設定できません。

---

## I/O フィルタリング コンポーネント

I/O フィルタリング プロセスは複数のコンポーネントで構成されています。

I/O フィルタリングのコンポーネントは次のとおりです。

### VAIO フィルタ ネットワーク

ユーザー ワールドと ESXi によって実現された VMkernel インフラストラクチャを組み合わせたもので、これにより、VMware パートナーは、仮想ディスクへの I/O パスおよび仮想ディスクからの I/O パスにフィルタ プラグインを追加できます。

### I/O フィルタ プラグイン

VMware パートナーによって開発されたソフトウェア コンポーネントで、仮想ディスクとゲスト OS 間で通信中の I/O データを傍受およびフィルタリングします。

### CIM プロバイダ

I/O フィルタ プラグインを構成および管理する、VMware パートナーによって開発されたオプションのコンポーネント。

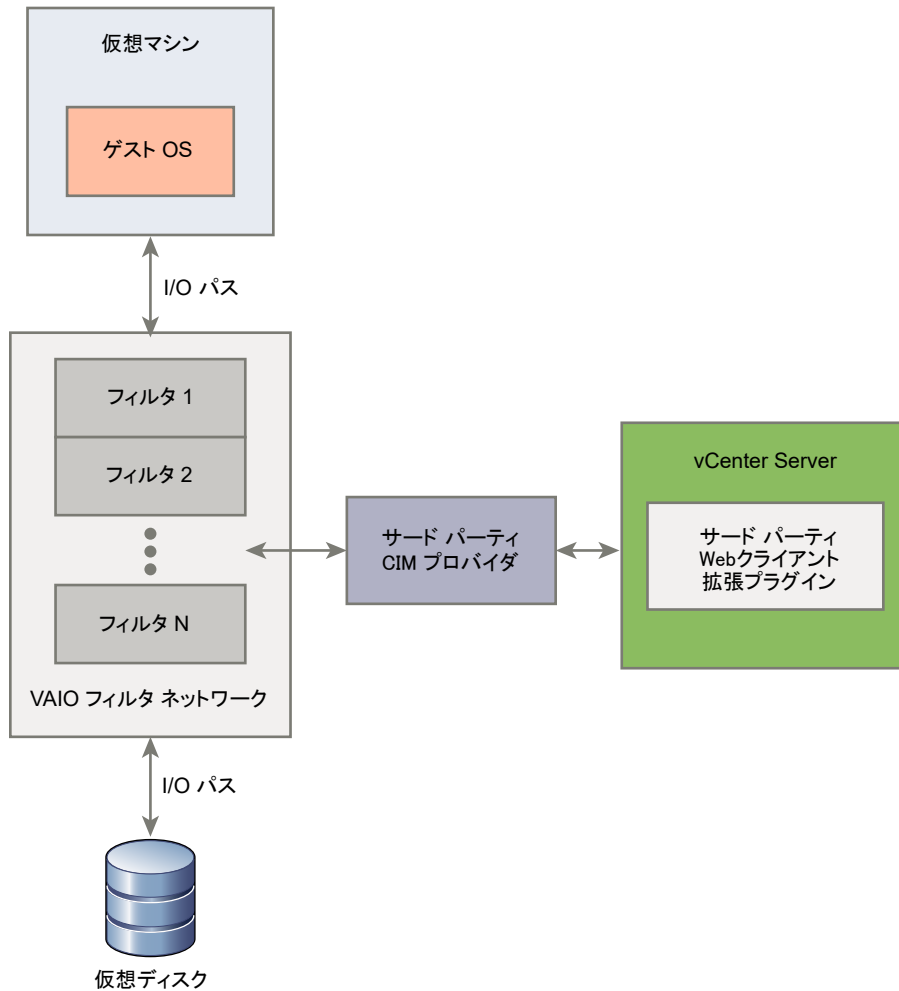
### vSphere Web Client プラグイン

VMware パートナーによって開発されたオプションのコンポーネント。このコンポーネントを使用して、vSphere 管理者は、I/O フィルタの CIM プロバイダと通信できます。具体的には、I/O フィルタ ステータスに関する監視情報を受信したり、CIM プロバイダに構成コマンドを送信して I/O フィルタを構成したりできます。

### I/O フィルタ デーモン

VMware パートナーによって開発されたオプションのコンポーネント。ホスト上で動作する個々のフィルタ インスタンスとやり取りする追加サービスとして使用できます。このサービスは、クロス ホスト ネットワーク 通信チャネルを確立できます。

次の図に、I/O フィルタリングの各コンポーネント、およびゲスト OS と仮想ディスク間の I/O フローを示します。



仮想マシンの各仮想マシン実行可能 (VMX) コンポーネントには、仮想ディスクに接続された I/O フィルタ プラグインを管理するフィルタ フレームワークが含まれています。I/O リクエストがゲスト OS と仮想ディスク間を移動するとき、このフィルタ フレームワークによってフィルタが起動されます。また、実行中の仮想マシンの外で仮想ディスクに対する I/O アクセスが発生した場合、それらの I/O アクセスもこのフィルタによって傍受されます。

フィルタは特定の順序で逐次的に実行されます。たとえば、レプリケーション フィルタの後にキャッシュ フィルタが実行されます。特定の仮想ディスクを 2 つ以上のフィルタでフィルタリングできますが、各カテゴリに対して使用できるフィルタは 1 つだけです。

I/O リクエストは、特定のディスクのすべてのフィルタによってフィルタリングされると、宛先、すなわち、仮想マシンまたは仮想ディスクに移動します。

フィルタはユーザー スペース内で実行されるため、いずれかのフィルタでエラーが発生しても影響を受けるのは仮想マシンだけであり、ESXi ホストが影響を受けることはありません。

## VAIO フィルタのストレージ プロバイダ

I/O フィルタをインストールし、それらを ESXi ホストにデプロイすると、I/O フィルタ フレームワークによってクラスタ内の各ホストのストレージ プロバイダ (VASA プロバイダとも呼ばれる) の構成と登録が行われます。

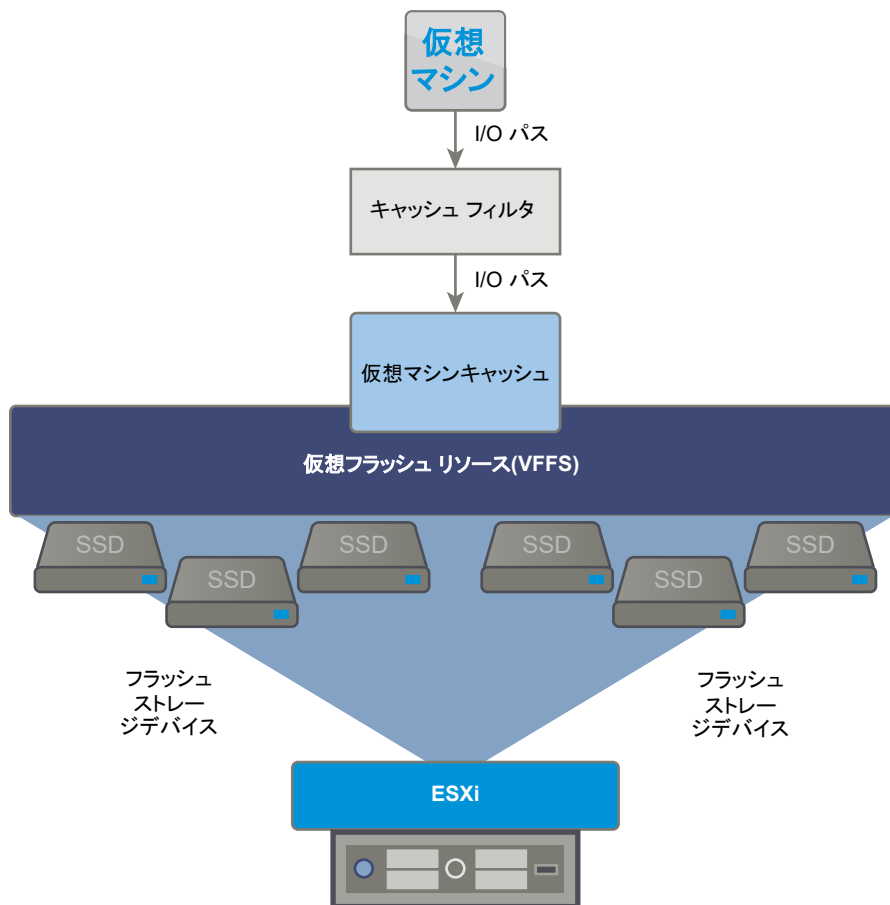
I/O フィルタのストレージ プロバイダは、vSphere によって提供されるソフトウェア コンポーネントです。ストレージ プロバイダは、I/O フィルタや、I/O フィルタが vCenter Server に対してサポートするレポート データ サービス機能と統合されます。

これらのデータ サービスは、仮想マシン ストレージ ポリシー インターフェイスで表示できるほか、仮想マシン ポリシーで参照することもできます。続いて、フィルタによってディスクの I/O を処理できるように、このポリシーを仮想ディスクに適用します。

## フラッシュ ストレージ デバイスとキャッシュ I/O フィルタの併用

キャッシュ I/O フィルタは、ローカル フラッシュ デバイスを使用して仮想マシン データをキャッシュできます。

キャッシュ I/O フィルタでローカル フラッシュ デバイスを使用している場合、フィルタを有効化する前に、仮想フラッシュ リソース (VFFS ポリウムとも呼ばれる) を ESXi ホストに構成する必要があります。仮想マシン読み取り I/O の処理中に、フィルタは仮想マシン キャッシュを作成し、VFFS ポリウムに配置します。



仮想フラッシュ リソースを設定するには、ホストに接続されたフラッシュ デバイスを使用します。仮想フラッシュ リソースの容量を拡張するために、フラッシュ ドライブを追加できます。個々のフラッシュ ドライブは、仮想フラッシュ リソース専用に割り当てる必要があり、Virtual SAN や VMFS などの他の vSphere サービスと共有することはできません。

フラッシュ読み取りキャッシュとキャッシュ I/O フィルタは相互排他に関係にあります。これは、いずれの機能もホストの仮想フラッシュ リソースを使用するためです。キャッシュ I/O フィルタが構成された仮想ディスクではフラッシュ読み取りキャッシュを有効にすることはできません。同様に、仮想マシンにフラッシュ読み取りキャッシュが構成されている場合は、キャッシュ I/O フィルタを使用することはできません。

## vSphere 環境での I/O フィルタのデプロイと構成

vSphere 環境に I/O フィルタをインストールすると、I/O フィルタが提供するデータ サービスを仮想マシンで有効にすることができます。

### 前提条件

VMware パートナーは、vSphere APIs for I/O Filtering (VAIO) 開発者プログラムを通じて I/O フィルタを作成し、フィルタ パッケージとして配布しています。vSphere インストール バンドル (VIB) として提供されているパッケージには、I/O フィルタ デーモン、CIM プロバイダ、およびその他の関連コンポーネントが含まれている場合があります。詳細については、ベンダーまたは VMware の担当者にお問い合わせください。

### 手順

#### 1 クラスタでの I/O フィルタのインストール

ベンダーから提供されたインストーラを実行して、I/O フィルタを ESXi ホスト クラスタにインストールします。

#### 2 I/O フィルタのストレージ プロバイダの表示

I/O フィルタをデプロイすると、クラスタ内の ESXi ホストごとに、ストレージ プロバイダ (VASA プロバイダとも呼ばれる) が自動的に登録されます。I/O フィルタ ストレージ プロバイダが想定どおりに表示されてアクティブな状態であることを確認できます。

#### 3 I/O フィルタの機能の確認

vSphere 環境に I/O フィルタをインストールすると、フィルタが提供する機能およびデータ サービスに登録され、仮想マシン ストレージ ポリシー インターフェイスに表れます。これらのサービスと機能およびそのデフォルト値を確認できます。

#### 4 キャッシュ I/O フィルタの仮想フラッシュ リソースの構成

キャッシュ I/O フィルタでローカル フラッシュ デバイスを使用している場合、フィルタを有効化する前に、仮想フラッシュ リソース (VFFS ボリュームとも呼ばれる) を ESXi ホストに構成する必要があります。

#### 5 仮想ディスクでの I/O フィルタ データ サービスの有効化

I/O フィルタが提供するデータ サービスの有効化は、2 段階のプロセスです。まず、I/O フィルタが提供するデータ サービス機能に基づいて仮想マシン ポリシーを作成し、次に、そのポリシーを仮想マシンに接続します。

### 次のステップ

I/O フィルタのトラブルシューティングの詳細については、『vSphere トラブルシューティング』のドキュメントを参照してください。

## クラスタでの I/O フィルタのインストール

ベンダーから提供されたインストーラを実行して、I/O フィルタを ESXi ホスト クラスタにインストールします。

### 前提条件

- 必要な権限 : Host.Configuration.Query パッチ
- I/O フィルタ ソリューションが vSphere ESX Agent Manager と統合されていて、VMware によって認定されていることを確認します。
- クラスタに ESXi 6.0 Update 1 ホストが含まれていることを確認します。
- クラスタの DRS を有効にします。

### 手順

- 1 ベンダーから提供されたインストーラを実行します。

インストーラにより、適切な I/O フィルタ拡張機能が vCenter Server にインストールされ、フィルタ コンポーネントがクラスタ内のすべてのホストにデプロイされます。選択したホストにフィルタをインストールすることはできません。

- 2 I/O フィルタ コンポーネントが ESXi ホストに適切にインストールされていることを確認します。

```
esxcli --server=server_name software vib list
```

フィルタが VIB パッケージのリストに表示されます。

## I/O フィルタのストレージ プロバイダの表示

I/O フィルタをデプロイすると、クラスタ内の ESXi ホストごとに、ストレージ プロバイダ（VASA プロバイダとも呼ばれる）が自動的に登録されます。I/O フィルタ ストレージ プロバイダが想定どおりに表示されてアクティブな状態であることを確認できます。

I/O フィルタ ストレージ プロバイダの自動登録が正常に完了した場合は、ホスト レベルでイベントがトリガされます。ストレージ プロバイダが自動登録に失敗した場合は、システムによってホストのアラームが表示されます。

### 手順

- 1 vSphere Web Client ナビゲータで、vCenter Server に移動して参照します。
- 2 [構成] タブをクリックし、[ストレージ プロバイダ] をクリックします。
- 3 I/O フィルタのストレージ プロバイダを確認します。

## I/O フィルタの機能の確認

vSphere 環境に I/O フィルタをインストールすると、フィルタが提供する機能およびデータ サービスに登録され、仮想マシン ストレージ ポリシー インターフェイスに表れます。これらのサービスと機能およびそのデフォルト値を確認できます。

#### 手順

- 1 vSphere Web Client のホームで、[ポリシーおよびプロファイル] - [仮想マシン ストレージ ポリシー] の順にクリックします。
- 2 [仮想マシン ストレージ ポリシーを新規作成します] アイコンをクリックします。
- 3 vCenter Server インスタンスを選択します。
- 4 「キャッシュ I/O フィルタ」などの名前およびポリシーの説明を入力して、[次へ] をクリックします。
- 5 [共通ルール] ページで [ストレージ ポリシーでの共通ルールの使用] を選択します。
- 6 [ルールの追加] ドロップダウン メニューから、キャッシュなど I/O フィルタのカテゴリを選択します。
- 7 [値の選択] ドロップダウン メニューから、機能を確認するフィルタを選択します。

パネルが展開され、I/O フィルタが提供するデータ サービスおよび対応するデフォルト値が表示されます。

## キャッシュ I/O フィルタの仮想フラッシュ リソースの構成

キャッシュ I/O フィルタでローカル フラッシュ デバイスを使用している場合、フィルタを有効化する前に、仮想フラッシュ リソース（VFFS ボリュームとも呼ばれる）を ESXi ホストに構成する必要があります。

#### 前提条件

I/O フィルタ ベンダーに問い合わせ、仮想フラッシュ リソースを有効にする必要があるかどうかを確認してください。

#### 手順

- 1 vSphere Web Client で、ホストに移動します。
- 2 [管理] タブをクリックして、[設定] をクリックします。
- 3 [仮想フラッシュ] で [仮想フラッシュ リソース管理] を選択し、[容量を追加] をクリックします。
- 4 使用可能なフラッシュ ドライブのリストから、仮想フラッシュ リソースで使用するドライブを 1 つ以上選択し、[OK] をクリックします。

#### 結果

仮想フラッシュ リソースが作成されます。[デバイス バッキング] 領域に仮想フラッシュ リソースに使用しているすべてのドライブが表示されます。

## 仮想ディスクでの I/O フィルタ データ サービスの有効化

I/O フィルタが提供するデータ サービスの有効化は、2 段階のプロセスです。まず、I/O フィルタが提供するデータ サービス機能に基づいて仮想マシン ポリシーを作成し、次に、そのポリシーを仮想マシンに接続します。

**前提条件**

I/O フィルタのキャッシングを行う場合は、ESXi ホスト上で仮想フラッシュ リソースを構成します。

**手順****1 I/O フィルタの機能に基づいた仮想マシン ポリシーの定義**

仮想マシンの I/O フィルタを有効にするには、まず、その I/O フィルタによって提供されるデータ サービス機能がリストされた仮想マシン ポリシーを作成する必要があります。

**2 仮想マシンへの I/O フィルタ ポリシーの割り当て**

I/O フィルタから提供されるデータ サービスを有効化するには、I/O フィルタ ポリシーを仮想ディスクに関連付けます。仮想マシンを作成または編集する場合、ポリシーを割り当てることができます。

**I/O フィルタの機能に基づいた仮想マシン ポリシーの定義**

仮想マシンの I/O フィルタを有効にするには、まず、その I/O フィルタによって提供されるデータ サービス機能がリストされた仮想マシン ポリシーを作成する必要があります。

I/O フィルタ機能は、仮想マシン ストレージ ポリシー ウィザードの [共通ルール] ページに表示されます。

**前提条件**

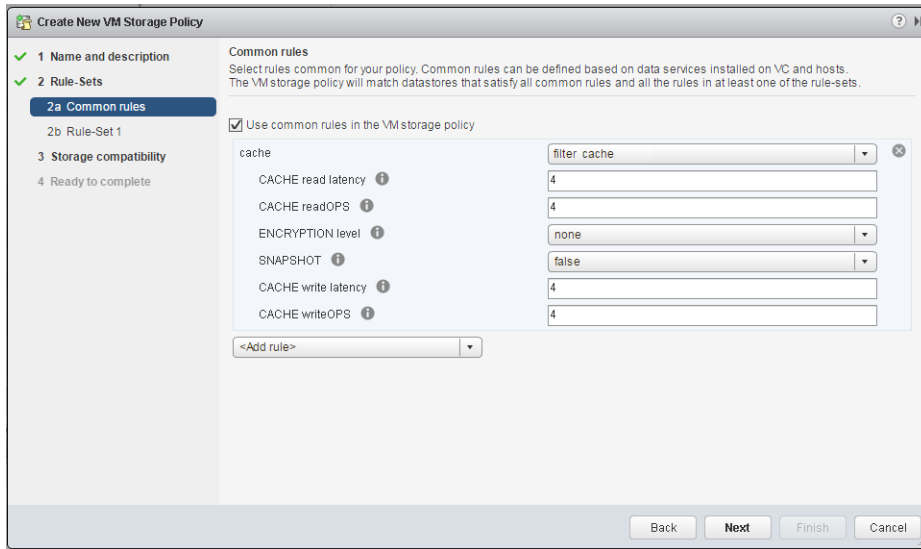
- I/O フィルタ ストレージ プロバイダが使用可能であり、アクティブであることを確認します。[I/O フィルタのストレージ プロバイダの表示](#) を参照してください。

**手順**

- 1 vSphere Web Client のホームで、[ポリシーおよびプロファイル] - [仮想マシン ストレージ ポリシー] の順にクリックします。
- 2 [仮想マシン ストレージ ポリシーを新規作成します] アイコンをクリックします。
- 3 vCenter Server インスタンスを選択します。
- 4 仮想マシン ポリシーの名前（例：I/O フィルタ）と説明を入力して、[次へ] をクリックします。
- 5 [共通ルール] ページで、特定の仮想マシンに対して有効化される I/O フィルタ サービスを指定します。

1 つのストレージ ポリシー内で異なるカテゴリ（例：レプリケーションとキャッシング）に属する I/O フィルタを組み合わせ使用できます。または、カテゴリごとに異なるポリシーを作成します。特定のストレージ ポリシー内で、同じカテゴリ（例：キャッシング）に属するフィルタを複数使用することはできません。





- a [ストレージ ポリシーでの共通ルールの使用] を選択します。
- b [ルールの追加] ドロップダウン メニューから、I/O フィルタ カテゴリを選択します。

オプション	説明
レプリケーション	仮想マシン ゲスト OS と仮想ディスク間のすべての書き込み I/O 操作を外部ターゲットの場所（別のホストやクラスタなど）にレプリケートします。
キャッシュ	仮想ディスク データのキャッシュを構成します。ローカル フラッシュ ストレージ デバイスを使用してデータをキャッシュし、仮想ディスクの IOPS やハードウェア使用率を増やします。

- c [値の選択] ドロップダウン メニューで、フィルタを選択します。  
ページが展開され、フィルタがサポートするデータ サービス機能とデフォルト値が表示されます。
  - d ルールの値を指定して [次へ] をクリックします。
- 6 [ルール セット] ページで、ストレージ配置要件を指定し、[次へ] をクリックします。

**注：** I/O フィルタを使用する仮想マシンを異なるタイプのデータストア（例：VMFS と仮想ボリューム）間で移行する場合は、仮想マシン ストレージ ポリシーに、使用するすべてのタイプのデータストアのルール セットが指定されていることを確認してください。たとえば、仮想マシンを VMFS と仮想ボリューム データストア間で移行する場合は、VMFS データストアのタグベースのルールと、仮想ボリューム データストアのルールを含む混合仮想マシン ストレージ ポリシーを作成します。

- 7 [ストレージ互換性] ページで、使用可能なデータストアのリストを確認し、[次へ] をクリックします。  
I/O フィルタ ポリシーとの互換性を維持するため、データストアは I/O フィルタを使用するホストと接続されており、なおかつポリシーのストレージ要件を満たしている必要があります。
- 8 ストレージ ポリシーの作成を完了させて、[終了] をクリックします。

## 結果

新しいポリシーがリストに追加されます。

## 仮想マシンへの I/O フィルタ ポリシーの割り当て

I/O フィルタから提供されるデータ サービスを有効化するには、I/O フィルタ ポリシーを仮想ディスクに関連付けます。仮想マシンを作成または編集する場合、ポリシーを割り当てることができます。

仮想マシンの最初のデプロイ時に I/O フィルタ ポリシーを割り当てることができます。このトピックでは、新しい仮想マシンの作成時にポリシーを割り当てる方法を説明します。その他のデプロイ方法については、『vSphere 仮想マシン管理』ドキュメントを参照してください。

---

**注:** 仮想マシンの移行またはクローン作成を行うときに I/O フィルタ ポリシーを変更または割り当てることはできません。

---

### 前提条件

仮想マシンが実行される ESXi ホストに I/O フィルタがインストールされていることを確認します。

### 手順

- 1 vSphere Web Client で、仮想マシン プロビジョニング プロセスを開始し、適切な手順に従ってください。
- 2 [ストレージの選択] ページで、[仮想マシン ストレージ ポリシー] ドロップダウン メニューから I/O フィルタ ポリシーを選択します。
- 3 使用可能なデータストアのリストからデータストアを選択し、[次へ] をクリックします。  
そのデータストアは、仮想マシン構成ファイルとすべての仮想ディスクのターゲット ストレージ リソースとなります。ポリシーは、仮想ディスクの I/O フィルタ サービスも有効化します。
- 4 仮想マシンのプロビジョニング プロセスを完了します。

### 結果

仮想マシンの作成後は、[サマリ] タブに、割り当てられたストレージ ポリシーとそのコンプライアンス ステータスが表示されます。

### 次のステップ

仮想ポリシー割り当ては後で変更できます。[仮想マシンのファイルとディスク用ストレージ ポリシー割り当ての変更](#) を参照してください。

## I/O フィルタの管理

ベンダーによって提供されたインストーラを実行し、I/O フィルタのインストール、アンインストール、またはアップグレードを実行できます。

I/O フィルタの処理では、次のことを考慮する必要があります。

- vCenter Server は、ESX Agent Manager (EAM) を使用して I/O フィルタのインストールとアンインストールを行う。管理者は、vCenter Server が作成または使用する EAM エージェントのために EAM API を直接呼び出してはならない。I/O フィルタ関連の操作はすべて VIM API を通して行う必要がある。vCenter

Server によって作成された EAM エージェントを誤って変更した場合は、その変更を取り消す必要がある。  
I/O フィルタが使用する EAM エージェントを誤って壊した場合は、  
`Vim.IoFilterManager#uninstallIoFilter` を呼び出し、影響を受けた I/O フィルタをアンインストールする必要がある。アンインストール後、フレッシュ再インストールを実行する。

- I/O フィルタを持つクラスタに新しいホストが加わる時には、そのクラスタにインストールされているフィルタがそのホストにデプロイされる。vCenter Server によって、そのホストの I/O フィルタ ストレージ プロバイダが登録される。クラスタに何か変更があった場合には、vSphere Web Client の仮想マシン ストレージ ポリシーのインターフェイスでその変更を確認できる。
- クラスタ外へホストを移動したりホストを vCenter Server から削除したりすると、そのホストから I/O フィルタがアンインストールされる。フィルタがアンインストールされた後、vCenter Server によって、ホストの I/O フィルタ ストレージ プロバイダの登録が解除される。
- ステートレス ESXi ホストを使用する場合には、再起動中にホストがその I/O フィルタ VIB を失うことがある。ホストが再起動した後で、vCenter Server が、ホストにインストールされているバンドルをチェックし、必要に応じて I/O フィルタ VIB をホストにプッシュする。

## クラスタからの I/O フィルタのアンインストール

ESXi ホスト クラスタにデプロイされている I/O フィルタをアンインストールできます。

### 前提条件

- 必要な権限：ホスト.構成.パッチ。

### 手順

- 1 ベンダーが提供するインストーラを実行し、I/O フィルタをアンインストールします。

アンインストール中は、vSphere ESX Agent Manager によってホストが自動的にメンテナンス モードに切り替えられます。

アンインストールが正常に実行されると、フィルタと関連コンポーネントがすべてホストから削除されます。

- 2 ESXi ホストから I/O フィルタ コンポーネントが確実にアンインストールされたことを確認します。

```
esxcli --server=server_name software vib list
```

アンインストールしたフィルタは今後リストに表示されなくなります。

## クラスタでの I/O フィルタのアップグレード

I/O フィルタ ベンダーから提供されたインストーラを使用して、ESXi ホスト クラスタにデプロイされた I/O フィルタをアップグレードします。

アップグレードは、古いフィルタ コンポーネントのアンインストールと、新しいフィルタ コンポーネントとの置き換えで構成されています。インストールがアップグレードであるかどうかを判断するために、vCenter Server により、既存のフィルタの名前とバージョンがチェックされます。既存のフィルタ名が新しいフィルタ名と一致するが、バージョンが異なる場合、インストールがアップグレードだとみなされます。

## 前提条件

- 必要な権限：ホスト.構成.パッチ。

## 手順

- 1 ベンダーから提供されたインストーラを実行してフィルタをアップグレードします。

アップグレード中、vSphere ESX Agent Manager により自動的にホストがメンテナンス モードになります。

インストーラにより、新しいフィルタ コンポーネントのインストール前に既存のフィルタ コンポーネントが識別されて削除されます。

- 2 ESXi ホストから I/O フィルタ コンポーネントが確実にアンインストールされたことを確認します。

```
esxcli --server=server_name software vib list
```

## 結果

アップグレード後、vSphere ESX Agent Manager によりホストが操作モードに戻ります。

# I/O フィルタのガイドラインおよびベスト プラクティス

環境内で I/O フィルタを使用する場合は、具体的なガイドラインとベスト プラクティスに従ってください。

- I/O フィルタは物理互換モードの RDM はサポートしません。
- フラッシュ読み取りキャッシュとキャッシュ I/O フィルタは相互排他関係にあります。これは、いずれの機能もホストの仮想フラッシュ リソースを使用するためです。キャッシュ I/O フィルタが設定された仮想ディスクではフラッシュ読み取りキャッシュを有効にすることはできません。同様に、仮想マシンにフラッシュ読み取りキャッシュが設定されている場合は、キャッシュ I/O フィルタを使用することはできません。
- 仮想マシンの移行またはクローン作成を行うときに、I/O フィルタ ポリシーの変更または割り当てを行うことはできません。
- I/O フィルタ ポリシーが設定された仮想マシンのクローン作成や移行を行う場合は、互換性のあるフィルタがターゲット ホストにインストールされている必要があります。この要件は、管理者、または HA や DRS などの機能によって開始される移行に適用されます。
- テンプレートを仮想マシンに変換する場合、そのテンプレートに I/O フィルタ ポリシーが設定されているときには、互換性のある I/O フィルタがターゲット ホストにインストールされている必要があります。
- vCenter Site Recovery Manager を使用して仮想ディスクをレプリケートする場合、リカバリ サイト上に生成されるディスクに I/O フィルタ ポリシーは含まれません。リカバリ サイトで I/O フィルタ ポリシーを作成し、レプリケートされたディスクにポリシーを追加する必要があります。
- 仮想マシンにスナップショット ツリーが関連付けられている場合、その仮想マシンの I/O フィルタの追加、変更、または削除を行うことはできません。

I/O フィルタのトラブルシューティングの詳細については、『vSphere トラブルシューティング』のドキュメントを参照してください。

## I/O フィルタによる仮想マシンの移行

I/O フィルタを使用している仮想マシンを移行する場合には、特定の考慮事項が適用されます。

Storage vMotion を使用して I/O フィルタを用いる仮想マシンを移行する場合は、ターゲット データストアが、互換性のある I/O フィルタがインストールされているホストに接続されている必要があります。

I/O フィルタを使用している仮想マシンを、たとえば VMFS と仮想ボリューム間、VMFS と Virtual SAN 間というように、タイプの異なるデータストア間で移行しなければならない場合があります。この場合は、I/O フィルタ ポリシーを記述する共通ルールに加え、仮想マシン ストレージ ポリシーに、使用するすべてのタイプのデータストアのルール セットが含まれていることを確認します。たとえば、VMFS と仮想ボリュームのデータストア間で仮想マシンを移行する場合は、以下を含む混合仮想マシン ストレージ ポリシーを作成します。

- I/O フィルタの共通ルール
- VMFS データストアのルール セット 1。ストレージ ポリシー ベース管理では明示的な VMFS ポリシーを提供していないため、このルール セットに VMFS データストアのタグベースのルールを含める必要があります。
- 仮想ボリューム データストアのルール セット 2

Storage vMotion では仮想マシンを移行する際に、ターゲット データストアに対応した正しいルール セットが選択されます。I/O フィルタ ルールは変更されません。

データストアのルールを指定せずに、I/O フィルタの共通ルールだけを定義すると、Virtual SAN、仮想ボリューム、VMFS/NFS のデータストアにはデフォルトのストレージ ポリシーが選択されます。

VMkernel は、ESXi ホストで直接実行する高パフォーマンスのオペレーティング システムです。VMkernel は、メモリ、物理プロセッサ、ストレージ、ネットワーク コントローラなどの、ハードウェア上の物理リソースの大部分を管理します。

ストレージを管理するには、VMkernel にはパラレル SCSI、SAS、ファイバ チャネル、FCoE および iSCSI をはじめとするいくつかの HBA (ホスト バス アダプタ) をサポートするストレージ サブシステムがあります。これらの HBA は、VMkernel と使用するために認定されている広範なアクティブ-アクティブ、アクティブ-パッシブおよび ALUA ストレージ アレイに接続します。サポートされる HBA とストレージ アレイのリストについては、『vSphere の互換性ガイド』を参照してください。

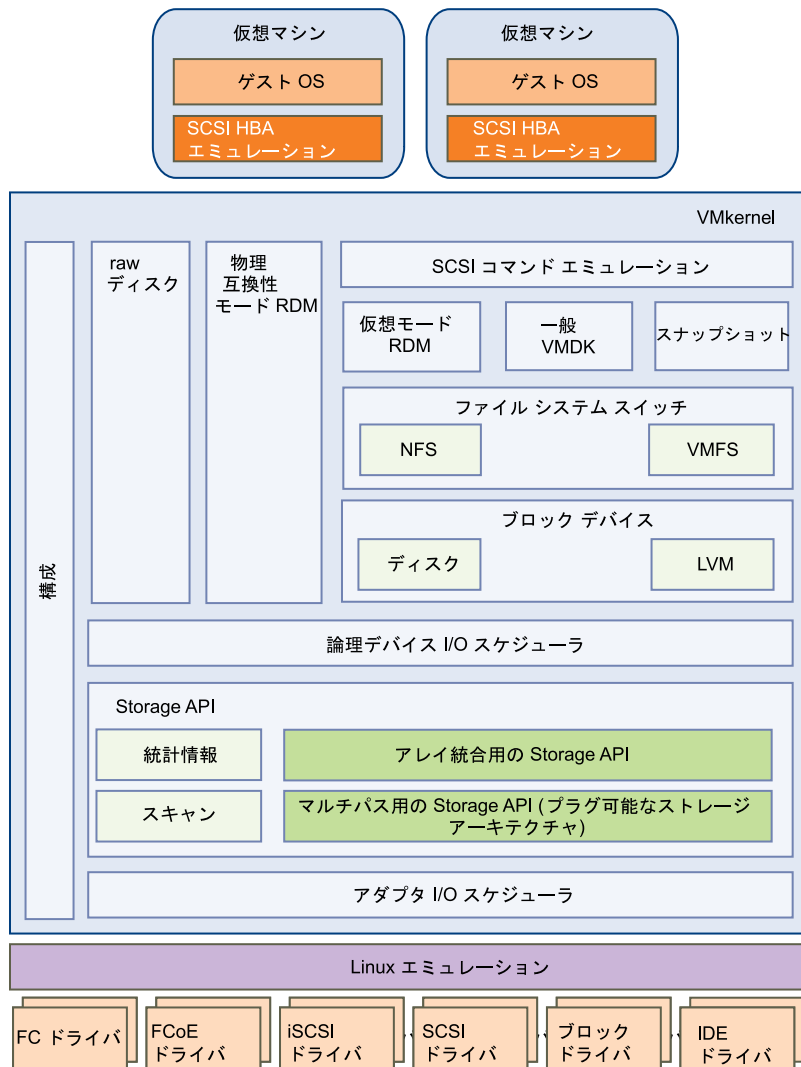
VMkernel が使用するプライマリ ファイル システムは VMFS (VMware Virtual Machine File System) です。VMFS は仮想ディスクやスワップ ファイルなどの大きいファイルをサポートするために設計され最適化されたクラスタ ファイル システムです。VMkernel は NFS ファイル システムで仮想ディスクのストレージもサポートします。

ストレージ I/O パスは、デバイス エミュレーションによるストレージ デバイスへのアクセスを仮想マシンに提供します。このデバイス エミュレーションによって、仮想マシンは SCSI デバイスであるかのように VMFS または NFS ファイル システム上のファイルにアクセスできます。VMkernel は複数の仮想マシンおよびマルチパスからの I/O 要求のスケジュールなどストレージ仮想化機能を提供します。

さらに、VMkernel はストレージ パートナーが vSphere のために製品の統合および最適化することを可能にするいくつかの Storage API を提供します。

次の図は、ストレージ スタックに特別な注意を払い、VMkernel コアの基本を示しています。ストレージ関連のモジュールは、論理デバイス I/O スケジューラとアダプタ I/O スケジューラ レイヤー間に存在します。

図 22-1. VMkernel とストレージ



この章には、次のトピックが含まれています。

## ■ Storage API

# Storage API

Storage API は、いくつかの vSphere 機能およびソリューションを拡張するコンポーネントを開発するためにサードパーティのハードウェア、ソフトウェアおよびストレージ プロバイダによって使用される API のファミリです。

本書では、以下のとおり Storage API のセットについて、またこれらがストレージ環境でどのように役立つかを説明します。Storage API - Data Protection および Storage API - Site Recovery Manager をはじめとするこのファミリのその他の API の詳細については、VMware の Web サイトを参照してください。

- Storage APIs - Multipathing (旧 PSA (プラグイン可能なストレージ アーキテクチャ))。PSA は VMkernel API の集合で、この集合を使用することで、ストレージ パートナーは、ESXi リリース スケジュールと非同期のアレイを有効にして認証するだけでなく、アレイごとに最適化されるパフォーマンスの強化、マルチパスおよびロード バランシング動作を提供することを可能にします。詳細については、[複数のパスの管理](#) を参照してください。
- Storage APIs- Array Integration (旧 VAAI) には次の API が含まれます。
  - ハードウェア アクセラレーション API。アレイは vSphere と統合して、特定のストレージ操作の負荷をアレイに透過的に移行することができます。この統合は、ホストでの CPU オーバーヘッドを大幅に軽減します。[23 章 ストレージのハードウェア アクセラレーション](#) を参照してください。
  - アレイ シン プロビジョニング API。シン プロビジョニング ストレージ アレイで領域使用を監視して、領域不足の状況を防止し領域の再利用を実行するのに役立ちます。[アレイ シン プロビジョニングおよび VMFS データストア](#) を参照してください。
- Storage API - Storage Awareness。これらの vCenter Server ベースの API によって、ストレージ アレイは構成、機能、ストレージの健全性とイベントについて vCenter Server に通知できます。[25 章 ストレージ プロバイダの使用](#) を参照してください。



# ストレージのハードウェア アクセラレーション

# 23

ハードウェア アクセラレーション機能によって、ESXi ホストで互換性のあるストレージ アレイと統合したり、特定の仮想マシンおよびストレージ管理操作の負荷をストレージ ハードウェアに移すことができます。ストレージ ハードウェア アシストにより、ホストはこれらの操作をより短時間で実行できます。また、CPU、メモリ、およびストレージ ファブリック バンド幅の使用量を削減できます。

ハードウェア アクセラレーションは、ブロック ストレージ デバイス、ファイバ チャネルおよび iSCSI ならびに NAS デバイスでサポートされます。

追加の詳細情報は、<http://kb.vmware.com/kb/1021976> にある VMware ナレッジ ベースの記事を参照してください。

この章には、次のトピックが含まれています。

- ハードウェア アクセラレーションのメリット
- ハードウェア アクセラレーションの要件
- ハードウェア アクセラレーションのサポート ステータス
- ブロック ストレージ デバイスのハードウェア アクセラレーション
- NAS デバイスでのハードウェア アクセラレーション
- ハードウェア アクセラレーションについての考慮事項

## ハードウェア アクセラレーションのメリット

ハードウェア アクセラレーション機能がサポートされている場合、ホストはハードウェア アシストにより、いくつかのタスクをより短時間で効率よく実行できます。

ホストは次のアクティビティによりアシストを得ることができます。

- Storage vMotion での仮想マシンの移行
- テンプレートからの仮想マシンのデプロイ
- 仮想マシンまたはテンプレートのクローン作成
- VMFS による仮想マシン ファイルのクラスタ ロックとメタデータ操作
- シック仮想ディスクのプロビジョニング
- フォールト トレランス対応の仮想マシンの作成

- NFS データストアでのシック ディスクの作成およびクローン作成

## ハードウェア アクセラレーションの要件

ハードウェア アクセラレーション機能は、ホストとストレージ アレイの適切な組み合わせを使用した場合にのみ機能します。

表 23-1. ハードウェア アクセラレーション ストレージの要件

ESXi	ブロック ストレージ デバイス	NAS デバイス
ESXi バージョン 6.0	T10 SCSI 規格、またはアレイ統合用のブロック ストレージ プラグイン (VAAI) のサポート	アレイ統合用の NAS プラグインをサポート <b>注：</b> NFS 4.1 では、ハードウェア アクセラレーションはサポートされていません。

**注：** SAN または NAS ストレージ ファブリックがハードウェア アクセラレーションをサポートするストレージ システムの前で中間アプライアンスを使用する場合には、中間アプライアンスはハードウェア アクセラレーションとサポートし、適切な認定を受けていることも必要です。中間アプライアンスはストレージ仮想化アプライアンス、I/O アクセラレーション アプライアンス、暗号化アプライアンスなどがあります。

## ハードウェア アクセラレーションのサポート ステータス

vSphere Web Client では、各ストレージ デバイスとデータストアについて、ハードウェア アクセラレーションのサポート ステータスが表示されます。

ステータスの値は、「不明」、「サポート」、および「未サポート」です。初期値は「不明」です。

ブロック デバイスの場合、ホストで負荷の軽減が正常に実行されると、ステータスが「サポート」に変わります。負荷の軽減に失敗した場合、ステータスは「未サポート」に変わります。デバイスが部分的にハードウェア アクセラレーションをサポートする場合、ステータスは「不明」のままです。

NAS を使用すると、ストレージがハードウェアの負荷軽減を少なくとも 1 回実行できるときには、ステータスは「サポート」になります。

ストレージ デバイスがホスト操作をサポートしていないか、部分的にサポートしている場合、ホストは、サポートされていない操作を実行するために元のメソッドに戻ります。

## ブロック ストレージ デバイスのハードウェア アクセラレーション

ハードウェア アクセラレーションによって、ホストはブロック ストレージ デバイス、ファイバ チャネルまたは iSCSI と統合して、特定のストレージ アレイ操作を使用できます。

ESXi ハードウェア アクセラレーションは次のアレイ操作をサポートします。

- Full Copy. クローン ブロックまたはコピー オフロードとも呼ばれます。ホストにデータの読み込みや書き出しを実行させることなく、ストレージ アレイはアレイ内のデータをフル コピーできます。この操作によって、仮想マシンのクローン作成、テンプレートからのプロビジョニング、vMotion を使用した移行のときに、時間が短縮され、ネットワークの負荷が軽減されます。

- Block Zeroing。Write Same と呼ばれます。以前に書き込まれたデータが存在しない、新たに割り当てられたストレージを提供するために、ストレージ アレイは多数のブロックをゼロクリアできます。この操作によって、仮想マシンの作成と仮想ディスクのフォーマットのときに、時間が短縮し、ネットワークの負荷が軽減されます。
- Hardware Assisted Locking。Atomic Test and Set (ATS) と呼ばれています。SCSI 予約を使用することなく、個別の仮想マシンのロックをサポートします。この操作によって、SCSI 予約のときのように LUN 全体ではなく、セクターごとにディスクをロックできます。

ハードウェア アクセラレーションのサポートについては、ベンダーにご確認ください。一部のストレージ アレイは、ストレージ側でサポートを有効にする必要があります。

ホストでは、ハードウェア アクセラレーションはデフォルトで有効になっています。ストレージがハードウェア アクセラレーションをサポートしない場合には、無効にできます。

ハードウェア アクセラレーションに加えて、ESXi ではアレイ シン プロビジョニングをサポートしています。詳細については、[アレイ シン プロビジョニングおよび VMFS データストア](#) を参照してください。

## ブロック ストレージ デバイスのハードウェア アクセラレーションの無効化

ホストでは、ブロック ストレージ デバイスのハードウェア アクセラレーションはデフォルトで有効になっています。vSphere Web Client の詳細設定を使用して、ハードウェア アクセラレーション操作を無効化できます。

ほかの詳細設定と同様に、ハードウェア アクセラレーションを無効にする前に、VMware のサポート チームに相談してください。

### 手順

- 1 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [構成] タブをクリックします。
- 3 [システム] メニューの [システムの詳細設定] をクリックします。
- 4 オプションの値を 0 (disabled) に変更します。
  - VMFS3.HardwareAcceleratedLocking
  - DataMover.HardwareAcceleratedMove
  - DataMover.HardwareAcceleratedInit

## ブロック ストレージ デバイスでのハードウェア アクセラレーションの管理

ブロック ストレージ アレイと統合して、アレイ ハードウェア操作の利点を活用するには、vSphere は Storage APIs - Array Integration (以前は VAAI と呼ばれていた) という ESXi 拡張を使用します。

vSphere 5.x 以降のリリースでは、これらの拡張は T10 SCSI ベースのコマンドとして実装されています。その結果、T10 SCSI 規格をサポートするデバイスを使用すれば、ESXi ホストは直接通信することができるため、VAAI プラグインを必要としません。

デバイスが T10 SCSI をサポートしていない、または部分的にサポートする場合には、ESXi はホストにインストールされた VAAI プラグインの使用に戻るか、T10 SCSI コマンドとプラグインの組み合わせを使用します。VAAI プラグインはベンダー固有で、VMware またはパートナーによって開発可能です。VAAI 対応のデバイスを管理するには、ホストは VAAI フィルタとベンダー固有の VAAI プラグインをデバイスに接続します。

ストレージが VAAI プラグインを必要とする、それとも T10 SCSI コマンドによるハードウェア アクセラレーションをサポートするかの詳細については、『VMware 互換性ガイド』を参照するか、ストレージベンダーにご確認ください。

いくつかの `esxcli` コマンドを使用して、ハードウェア アクセラレーションのサポート情報をストレージデバイスに照会できます。VAAI プラグインを必要とするデバイスには、要求ルール コマンドも使用できます。`esxcli` コマンドの詳細については、『vSphere Command-Line Interface スタートガイド』を参照してください。

## ハードウェア アクセラレーション プラグインおよびフィルタの表示

T10 SCSI 規格をサポートしないデバイスと通信するために、ホストは単一の VAAI フィルタとベンダー固有の VAAI プラグインを組み合わせで使用します。`esxcli` コマンドを使用して、システムに現在ロードされているハードウェア アクセラレーション フィルタとプラグインを表示します。

手順中、`--server=server_name` で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタートガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタートガイドを参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

- ◆ `esxcli --server=server_name storage core plugin list --plugin-class=value` コマンドを実行します。

`value` には、次のオプションのいずれかを入力します。

- VAAI と入力してプラグインを表示します。

このコマンドの出力は、次の例のようになります。

```
#esxcli --server=server_name storage core plugin list --plugin-class=VAAI Plugin
name          Plugin class VMW_VAAIP_EQL          VAAI VMW_VAAIP_NETAPP    VAAI
VMW_VAAIP_CX   VAAI
```

- Filter と入力してフィルタを表示します。

このコマンドの出力は、次の例のようになります。

```
esxcli --server=server_name storage core plugin list --plugin-class=Filter Plugin
name  Plugin class VAAI_FILTER  Filter
```

## ハードウェア アクセラレーションのサポート ステータスの検証

`esxcli` コマンドを使用して、特定のストレージ デバイスのハードウェア アクセラレーションのサポート ステータスを確認します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

- ◆ **`esxcli --server=server_name storage core device list -d=device_ID`** コマンドを実行します。

出力に、ハードウェア アクセラレーション (VAAI) のステータスが表示されます。ステータスは、「不明」、「サポート」、または「未サポート」のいずれかです。

```
# esxcli --server=server_name storage core device list -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c Display Name:XXXX Fibre Channel Disk(naa.XXXXXXXXXXX4c) Size:20480
Device Type:Direct-Access Multipath Plugin:NMP XXXXXXXXXXXXXXXX Attached
Filters:VAAI_FILTER VAAI Status:supported XXXXXXXXXXXXXXXX
```

## ハードウェア アクセラレーションのサポート詳細の検証

`esxcli` コマンドを使用して、デバイスが提供するハードウェア アクセラレーションのサポートに関してブロックストレージ デバイスを照会します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

## 手順

- ◆ **esxcli --server=server\_name storage core device vaai status get -d=device\_ID** コマンドを実行します。

デバイスが VAAI プラグインによって管理される場合、出力にデバイスに添付されたプラグイン名が表示されます。出力には、T10 SCSI ベースのプリミティブ（使用可能な場合）のサポート ステータスが表示されます。出力は次の例の通りです。

```
# esxcli --server=server_name storage core device vaai status get -d naa.XXXXXXXXXXXXXc
naa.XXXXXXXXXXXXXc VAAI Plugin Name:VMW_VAAIP_SYMM ATS Status:supported Clone
Status:supported Zero Status:supported Delete Status:unsupported
```

## ハードウェア アクセラレーションの要求ルールの一覧表示

VAAI プラグインによって管理される各ブロック ストレージ デバイスは、2 つの要求ルールを必要とします。1 つの要求ルールはハードウェア アクセラレーション フィルタを指定し、もう 1 つの要求ルールはデバイス用のハードウェア アクセラレーション プラグインを指定します。esxcli コマンドを使用して、ハードウェア アクセラレーションのフィルタとプラグインの要求ルールをリスト表示できます。

## 手順

- 1 フィルタ要求ルールをリスト表示するには、  
**esxcli --server=server\_name storage core claimrule list --claimrule-class=Filter** コマンドを実行します。

この例では、フィルタの要求ルールは、VAAI\_FILTER フィルタが要求するデバイスを指定します。

```
# esxcli --server=server_name storage core claimrule list --claimrule-class=Filter Rule
Class Rule Class Type Plugin Matches Filter 65430 runtime vendor
VAAI_FILTER vendor=EMC model=SYMMETRIX Filter 65430 file vendor VAAI_FILTER
vendor=EMC model=SYMMETRIX Filter 65431 runtime vendor VAAI_FILTER vendor=DGC
model=* Filter 65431 file vendor VAAI_FILTER vendor=DGC model=*
```

- 2 VAAI プラグイン要求ルールをリスト表示するには、  
**esxcli --server=server\_name storage core claimrule list --claimrule-class=VAAI** コマンドを実行します。

この例では、VAAI の要求ルールは、特定の VAAI プラグインが要求するデバイスを指定します。

```
esxcli --server=server_name storage core claimrule list --claimrule-class=VAAI Rule
Class Rule Class Type Plugin Matches VAAI 65430 runtime vendor
VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX VAAI 65430 file vendor
VMW_VAAIP_SYMM vendor=EMC model=SYMMETRIX VAAI 65431 runtime vendor
VMW_VAAIP_CX vendor=DGC model=* VAAI 65431 file vendor VMW_VAAIP_CX
vendor=DGC model=*
```

## ハードウェア アクセラレーションの要求ルールの追加

新しいアレイのハードウェア アクセラレーションを構成するには、VAAI フィルタ用と VAAI プラグイン用に 1 つずつ要求ルールを追加する必要があります。新規の要求ルールをアクティブにするには、まずルールを定義し、次にそれをシステムにロードします。

これは、T10 SCSI コマンドをサポートせずに、代わりに VAAI プラグインを使用するブロック ストレージ デバイスのための手順です。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で **esxcli** コマンドを実行します。

### 手順

- 1 **esxcli --server=server\_name storage core claimrule add --claimrule-class=Filter --plugin=VAAI\_FILTER** コマンドを実行して、VAAI フィルタ用に新規要求ルールを定義します。
- 2 **esxcli --server=server\_name storage core claimrule add --claimrule-class=VAAI** コマンドを実行して、VAAI フィルタ用に新規要求ルールを定義します。
- 3 次のコマンドを実行して、2 つの要求ルールをロードします。  
  
**esxcli --server=server\_name storage core claimrule load --claimrule-class=Filter**  
  
**esxcli --server=server\_name storage core claimrule load --claimrule-class=VAAI**
- 4 **esxcli --server=server\_name storage core claimrule run --claimrule-class=Filter** コマンドを実行して、VAAI フィルタ要求ルールを実行します。

---

**注：** 実行が必要なのはフィルタ クラスのルールだけです。VAAI フィルタがデバイスを要求するとき、添付に適した VAAI プラグインが自動的に検索されます。

---

### 例：ハードウェア アクセラレーションの要求ルールの定義

この例では、VMW\_VAAI\_T10 プラグインを使用して、IBM アレイのハードウェア アクセラレーションを構成する方法を示します。次のコマンド シーケンスを使用します。コマンドが取得するオプションについては、[マルチパスの要求ルールの追加](#) を参照してください。

```
# esxcli --server=server_name storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign
```

```
# esxcli --server=server_name storage core claimrule add --claimrule-
class=VAAI --plugin=VMW_VAAIP_T10 --type=vendor --vendor=IBM --autoassign

# esxcli --server=server_name storage core claimrule load --claimrule-
class=Filter

# esxcli --server=server_name storage core claimrule load --claimrule-
class=VAAI

# esxcli --server=server_name storage core claimrule run --claimrule-
class=Filter
```

## ハードウェア アクセラレーションの要求ルールの削除

esxcli コマンドを使用して、既存のハードウェア アクセラレーションの要求ルールを削除します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- ◆ 次のコマンドを実行します。

```
esxcli --server=server_name storage core claimrule remove -r claimrule_ID
--claimrule-class=Filter

esxcli --server=server_name storage core claimrule remove -r claimrule_ID
--claimrule-class=VAAI
```

## NAS デバイスでのハードウェア アクセラレーション

ハードウェア アクセラレーションにより、ESXi ホストでは、NAS デバイスと統合してその NAS ストレージによって提供されるいくつかのハードウェア操作を使用できます。ハードウェア アクセラレーションでは、VMware vSphere Storage for Array Integration (VAAI) を使用して、ホストとストレージ デバイスの間の通信を有効化します。

この API では、ホストが特定のストレージ操作の負荷をアレイにオフロードできるようにする、ストレージ プリミティブのセットが定義されています。次のリストにサポートされる NAS 操作を示します。

- ファイルのフル クローン。NAS デバイスで仮想ディスク ファイルのクローンを作成できるようにします。この操作は、NAS デバイスがファイル セグメントではなく、ファイル全体のクローンを作成する点を除き、VMFS のブロック クローン作成と似ています。



- 領域の予約。ストレージ アレイがシック フォーマットで仮想ディスク ファイルの領域を割り当てることを可能にします。

通常、仮想ディスクを NFS データストアで作成するときに、NAS サーバは割り当てポリシーを決定します。ほとんどの NAS サーバのデフォルトの割り当てポリシーはシンですが、ストレージをファイルに戻すことは保証されません。ただし、スペースの予約操作によって、ベンダー固有のメカニズムを使用して仮想ディスク用のスペースを予約するように NAS デバイスに指示が行われる場合があります。この結果、NFS データストアにシック仮想ディスクを作成してしまう可能性があります。

- ネイティブ スナップショットのサポート。仮想マシンのスナップショットを作成する負荷がアレイにオフロードされるようにします。
- 拡張された統計。NAS デバイスでの領域使用量を可視化することができ、シン プロビジョニングにおいて役立ちます。

NAS ストレージ デバイスによって、ハードウェア アクセラレーションの統合は、ベンダー固有の NAS プラグインによって実装されます。これらのプラグインは通常、ベンダーによって作成され、Web ページから VIB パッケージとして配布されます。NAS プラグインが動作するための要求ルールは不要です。

VIB パッケージのインストールおよびアップグレードに使用可能なツールがいくつかあります。ツールには `esxcli` コマンドと vSphere Update Manager が含まれています。詳細については、『vSphere のアップグレード』および『VMware vSphere Update Manager のインストールと管理』ドキュメントを参照してください。

## NAS プラグインのインストール

ベンダーが配布したハードウェア アクセラレーション NAS プラグインをホストにインストールします。

このトピックでは `esxcli` コマンドを使用した VIB パッケージのインストールの例を紹介します。詳細については、『vSphere のアップグレード』ドキュメントを参照してください。

手順中、`--server=server_name` で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

- 1 ホストをメンテナンス モードにします。
- 2 ホストの許容レベルを次のように設定します。

```
esxcli --server=server_name software acceptance set --level=value
```

このコマンドは、どの VIB パッケージがホストで許容されるかを制御します。*value* は次のいずれかに指定できます。

- VMwareCertified

- VMwareAccepted
- PartnerSupported
- CommunitySupported

3 VIB パッケージをインストールします。

```
esxcli --server=server_name software vib install -v|--viburl=URL
```

URL は URL をインストールする VIB パッケージに指定します。http:、https:、ftp:、および file: がサポートされます。

4 プラグインがインストールされたことを検証します。

```
esxcli --server=server_name software vib list
```

5 ホストを再起動して、インストールを有効にします。

## NAS プラグインのアンインストール

NAS プラグインをアンインストールするには、VIB パッケージをホストから削除します。

このトピックでは、`esxcli` コマンドを使用して、VIB パッケージをアンインストールする方法を説明します。詳細については、『vSphere のアップグレード』ドキュメントを参照してください。

手順中、`--server=server_name` で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

### 手順

1 プラグインをアンインストールするには、次の通りに実行します。

```
esxcli --server=server_name software vib remove -n|--vibName=name
```

`name` は削除する VIB パッケージ名です。

2 プラグインが削除されたことを検証します。

```
esxcli --server=server_name software vib list
```

3 ホストを再起動して、変更を有効にします。

## NAS プラグインの更新

ストレージ ベンダーが新しいバージョンのプラグインをリリースするときにホストでハードウェア アクセラレーション NAS プラグインをアップグレードします。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

#### 前提条件

このトピックは、`esxcli` コマンドを使用して、VIB パッケージを更新する方法を説明します。詳細については、『vSphere のアップグレード』ドキュメントを参照してください。

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

#### 手順

- 1 新しいバージョンのプラグインをアップグレードします。

```
esxcli --server=server_name software vib update -v|--viburl=URL
```

*URL* は更新する VIB パッケージに URL を指定します。http:、https:、ftp: および file: がサポートされます。

- 2 正しいバージョンがインストールされたことを検証します。

```
esxcli --server=server_name software vib list
```

- 3 ホストを再起動します。

## NAS のハードウェア アクセラレーション ステータスの検証

クライアントに加えて、`esxcli` コマンドを使用して、NAS デバイスのハードウェア アクセラレーションのステータスを検証できます。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

#### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で `esxcli` コマンドを実行します。

#### 手順

- ◆ **esxcli --server=server\_name storage nfs list** コマンドを実行します。

出力のハードウェア アクセラレーション列にステータスが表示されます。

## ハードウェア アクセラレーションについての考慮事項

ハードウェア アクセラレーション機能を使用する場合には、特定の考慮事項が適用されます。

いくつかの理由が原因となってハードウェア アクセラレーションが失敗する場合があります。

アレイが実装しないプリミティブの場合、アレイはエラーを返します。エラーが発生すると、ESXi ホストはネイティブ メソッドを使用して操作を試行します。

次のいずれかが発生すると、VMFS データ ムーバーはハードウェア オフロードを活用せずに、代わりにソフトウェアによるデータ移動を使用します。

- ソースおよびターゲットの VMFS データストアにはさまざまなブロック サイズがあります。
- ソースのファイル タイプは RDM でターゲットのファイル タイプは非 RDM（通常のファイル）です。
- ソースの VMDK タイプは eagerzeroedthick でターゲットの VMDK タイプはシンです。
- ソースまたはターゲットの VMDK はスパースまたはホスト フォーマットです。
- ソースの仮想マシンにはスナップショットがあります。
- 要求された操作の論理アドレスと転送の長さは、ストレージ デバイスによって要求される最小整列に整列されません。vSphere Web Client で作成されたすべてのデータストアは自動的に整列されます。
- VMFS には複数の LUN またはエクステンツがあり、これらは異なるアレイにあります。

同じ VMFS データストア内であっても、アレイ間でのハードウェアのクローン作成は機能しません。

# ストレージ シック プロビジョニング とストレージ シン プロビジョニング

# 24

vSphere では、シック プロビジョニングとシン プロビジョニングの 2 つのストレージ プロビジョニング モデルがサポートされています。

## シック プロビジョニング

従来のストレージ プロビジョニング モデルです。シック プロビジョニングを使用すると、将来のストレージの必要性を事前に予測して大量のストレージ領域が提供されます。ただし、領域は未使用のままとなり、ストレージの容量を十分に利用できない場合があります。

## シン プロビジョニング

この方法はシック プロビジョニングとは対照的で、オンデマンドで柔軟にストレージ領域を割り当てることによって、ストレージを十分に利用できない問題を解消するのに役立ちます。ESXi によって、シン プロビジョニングの 2 つのモデルのアレイ レベルおよび仮想ディスク レベルを使用できます。

この章には、次のトピックが含まれています。

- [ストレージ オーバーサブスクリプション](#)
- [仮想ディスク シン プロビジョニング](#)
- [アレイ シン プロビジョニングおよび VMFS データストア](#)

## ストレージ オーバーサブスクリプション

シン プロビジョニングによって、実際に存在する物理領域以上の仮想ストレージ領域をレポートすることができま  
す。この違いは、ストレージ オーバーサブスクリプション (オーバー プロビジョニングとも呼ばれる) を引き起こす  
可能性があります。

シン プロビジョニングを使用する場合、実際のストレージ使用率を監視して、物理ストレージ領域が不足する状態を  
回避する必要があります。

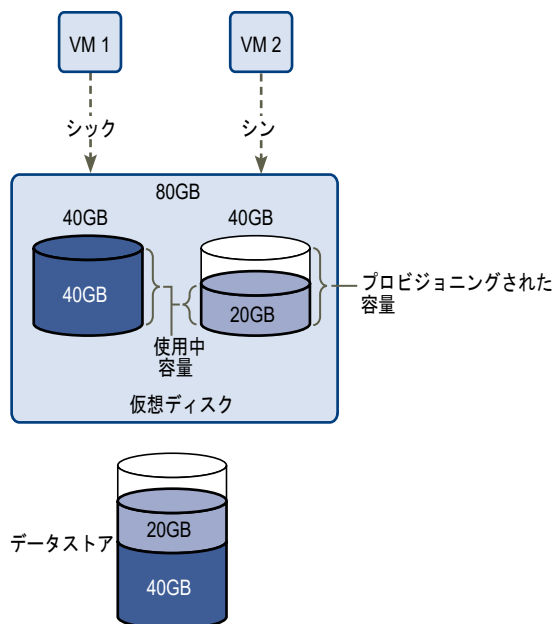
## 仮想ディスク シン プロビジョニング

仮想マシンを作成する場合には、データストア上の一定量のストレージ領域が仮想ディスク ファイルにプロビジョニ  
ングされます。

デフォルトで、ESXi は仮想マシンの従来のストレージ プロビジョニング方法を提供します。この方法によって、仮想マシンがライフサイクル全体で必要とするストレージの量を最初に見積もります。次に仮想ディスクに固定されたストレージの容量 (たとえば 40GB) を事前にプロビジョニングし、プロビジョニングされた領域全体を仮想ディスクにコミットします。プロビジョニングされた領域全体をすぐに占有する仮想ディスクはシック ディスクです。

ESXi では仮想ディスクのシン プロビジョニングがサポートされます。ディスク レベルのシン プロビジョニング機能を使用すると、シン フォーマットの仮想ディスクを作成できます。シン仮想ディスクの場合、ESXi はディスクの現在および将来のアクティビティに必要な領域全体 (たとえば 40GB) をプロビジョニングします。ただし、シン ディスクが初期の操作で使用するのは、ディスクが必要とするストレージ領域に限定されます。この例では、シン プロビジョニング ディスクが使用するストレージは 20GB のみです。ディスクがさらなる領域を必要とすると、プロビジョニングされた領域全体の 40GB に増やすことができます。

図 24-1. シックおよびシン仮想ディスク



## 仮想ディスクのプロビジョニング ポリシーについて

仮想ディスクの作成、テンプレートへの仮想マシンのクローン作成、仮想マシンの移行など、仮想マシンの特定の管理操作を実行する際には、仮想ディスク ファイルのプロビジョニング ポリシーを指定できます。

ハードウェア アクセラレーションに対応する NFS データストアおよび VMFS データストアでは、次のディスク プロビジョニング ポリシーをサポートします。ハードウェア アクセラレーションに対応しない NFS データストアでは、シン フォーマットのみを使用できます。

Storage vMotion またはクロス ホスト Storage vMotion を使用して、仮想ディスクのフォーマットを変換することができます。

### シック プロビジョニング (Lazy Zeroed)

仮想ディスクをデフォルトのシック フォーマットで作成します。ディスクの作成時に、仮想ディスクに必要な容量が割り当てられます。物理デバイスに残っているデータは、作成中には消去されませんが、あとで仮想マシンにはじめて書き込むときにオン デマンドで消去されます。仮想マシンが物理デバイスから古いデータを読み取ることはありません。

### シック プロビジョニング (Eager Zeroed)

Fault Tolerance などのクラスタリング機能をサポートする、シック仮想ディスクのタイプ。仮想ディスクに必要な容量は、作成時に割り当てられます。シック プロビジョニング (Lazy Zeroed) フォーマットの場合とは異なり、物理デバイスに残っているデータは、仮想ディスクの作成時に消去されます。このフォーマットでの仮想ディスクの作成には、他のタイプのディスクに比べて長い時間がかかることがあります。

### シン プロビジョニング

このフォーマットを使用してストレージ容量を節約します。シン ディスクの場合、入力した仮想ディスク サイズの値に応じて、ディスクに必要な容量と同じデータストア容量をプロビジョニングします。ただし、シン ディスクは最初は小さく、初期処理に必要なデータストア容量のみを使用します。あとでシン ディスクでさらに多くの容量が必要になると、その最大容量まで拡張し、プロビジョニングされたデータストア容量全体を占有できます。

シン プロビジョニングではヘッダ情報のみのディスクを作成するため、最も速く仮想ディスクを作成することができます。また、シン プロビジョニングでは、ストレージ ブロックの割り当ておよびゼロ クリアは行われません。ストレージ ブロックは、最初にアクセスされたときに割り当ておよびゼロ クリアが行われます。

---

**注：** 仮想ディスクが Fault Tolerance などのクラスタ ソリューションをサポートしている場合は、シン ディスクを作成しないでください。

---

シン ディスクは、プロビジョニングされた容量全体を占有するように手動で拡張することができます。物理ストレージ領域が枯渇し、シン プロビジョニングしたディスクを拡張できない場合は、仮想マシンが使用できなくなります。

## シン プロビジョニング仮想ディスクの作成

ストレージ容量を節約するために、シン プロビジョニング フォーマットの仮想ディスクを作成できます。シン プロビジョニング仮想ディスクは、最初は小さく、必要なディスク容量が増加するにつれて拡大します。シン ディスクは、ディスク レベルのシン プロビジョニングに対応したデータストアのみに作成できます。

この手順では、新しい仮想マシンを作成すると想定します。詳細については、『vSphere 仮想マシン管理』ドキュメントを参照してください。

#### 手順

- 1 仮想マシンの有効な親オブジェクトである任意のインベントリ オブジェクト（データセンター、フォルダ、クラスタ、リソース プール、ホストなど）を右クリックして、[新規仮想マシン] を選択します。
- 2 [新規仮想マシンの作成] を選択し、[次へ] をクリックします。
- 3 仮想マシンの作成に必要な手順すべてを実行します。
- 4 [ハードウェアのカスタマイズ] ページで、[仮想ハードウェア] タブをクリックします。
- 5 [新規ハード ディスク] の三角形をクリックして、ハード ディスク オプションを展開します。

## 6 (オプション) デフォルトのディスク サイズを調整します。

シン仮想ディスクでは、ディスク サイズ値は、ディスクにプロビジョニングされ、保証される容量を示します。最初は、仮想ディスクがプロビジョニングされた領域全体を使用せず、実際のストレージ使用量が仮想ディスクのサイズよりも小さくなる場合があります。

## 7 ディスク プロビジョニングに [シン プロビジョニング] を選択します。

## 8 仮想マシンの作成を終了します。

### 結果

シン フォーマットのディスクを持つ仮想マシンを作成しました。

### 次のステップ

シン フォーマットの仮想ディスクを作成した場合は、あとでフル サイズまで拡張できます。

## 仮想マシン ストレージ リソースの表示

仮想マシン用に割り当てられているデータストアのストレージ容量を表示できます。

ストレージ使用量は、構成ファイル、ログ ファイル、スナップショット、仮想ディスクなどの仮想マシン ファイルが占有しているデータストア容量を示します。仮想マシンが実行中の場合は、使用済みストレージ領域にはスワップ ファイルも含まれます。

シン ディスクを持つ仮想マシンでは、実際のストレージ使用量は仮想ディスクのサイズよりも小さい場合があります。

### 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 仮想マシンをダブルクリックし、[サマリ] タブをクリックします。
- 3 [サマリ] タブ右上部のストレージ使用量情報を確認します。

## 仮想マシンのディスク フォーマットの判別

仮想ディスクが、シック フォーマットかシン フォーマットかを特定できます。

### 手順

- 1 vSphere Web Client で、仮想マシンを参照します。
- 2 仮想マシンを右クリックし、[設定の編集] を選択します。
- 3 [仮想ハードウェア] タブをクリックします。
- 4 [ハード ディスク] の三角形をクリックして、ハード ディスク オプションを展開します。

[タイプ] テキスト ボックスに仮想ディスクのフォーマットが表示されます。

### 次のステップ

仮想マシンがシン フォーマットの場合は、フル サイズまで拡張できます。



## シン仮想ディスクの拡張

シン フォーマットで仮想ディスクを作成した場合は、シン ディスクをシック プロビジョニング フォーマットの仮想ディスクに変換できます。

データストア ブラウザを使用して、仮想ディスクを拡張します。

### 前提条件

- 仮想マシンが存在するデータストアに十分な容量があることを確認します。
- 仮想ディスクがシンであることを確認します。
- スナップショットを削除します。
- 仮想マシンをパワーオフします。

### 手順

- 1 拡張する仮想ディスクのフォルダに移動します。
  - a vSphere Web Client で、仮想マシンを参照します。
  - b 情報を表示する仮想マシンをダブルクリックします。
  - c [関連オブジェクト] > [データストア] の順にクリックします。  
仮想マシン ファイルを保存するデータストアが一覧表示されます。
  - d データストアを選択し、[データストア ファイル ブラウザに移動します。] アイコンをクリックします。  
データストア ブラウザに、データストアのコンテンツが表示されます。
- 2 仮想マシン フォルダを開き、変換したい仮想ディスク ファイルを参照します。  
このファイルには .vmdk 拡張子が含まれており、仮想ディスク (🗑️) アイコンが表示されます。
- 3 仮想ディスク ファイルを右クリックし、[拡張] を選択します。

---

**注：** 仮想ディスクがシックの場合、または仮想マシンが実行中の場合、このオプションは使用できない場合があります。

---

### 結果

拡張された仮想ディスクは、最初にプロビジョニングされたデータストア容量全体を専有します。

## データストアのオーバーサブスクリプションの処理

シン ディスクに対してプロビジョニングされる領域は、コミット領域よりも多いことがあるため、データストアのオーバーサブスクリプションが発生することがあります。このため、データストア上の仮想マシン ディスクに対してプロビジョニングされた容量の合計が、実際の容量よりも多くなる、という結果になります。

通常、シン ディスクを備えているすべての仮想マシンが、プロビジョニングされたデータストア全体の領域を同時に必要とするわけではないため、オーバーサブスクリプションが可能な場合があります。ただし、データストアのオーバーサブスクリプションが発生しないようにするには、プロビジョニングした領域が特定のしきい値に達した場合にユーザーにアラームを通知するよう設定できます。

アラームの設定の詳細については、『vCenter Server およびホスト管理』ドキュメントを参照してください。

仮想マシンに追加の領域が必要な場合は、先着順にデータストア領域が割り当てられます。データストアの領域が不足している場合、物理ストレージを追加してデータストアを増やすことができます。

[VMFS データストア容量の増加](#) を参照してください。

## アレイ シン プロビジョニングおよび VMFS データストア

ESXi は、シン プロビジョニング ストレージ アレイと使用できます。

アレイによって ESXi ホストに提示される従来の LUN はシン プロビジョニングです。各 LUN をバックするために必要な物理領域全体が事前に割り当てられます。

ESXi はシン プロビジョニング LUN もサポートします。LUN がシン プロビジョニングのとき、ストレージ アレイは LUN の論理サイズをレポートします（このサイズは、その LUN をバックアップする本当の物理容量よりも大きい場合があります）。

シン プロビジョニング LUN でデプロイする VMFS データストアで検出できるのは、LUN の論理サイズのみです。たとえば、実際にアレイで提供されるのが 1TB のみであるのに、ストレージが 2TB であるとアレイによってレポートされる場合、データストアは LUN のサイズが 2TB であると見なします。データストアが大きくなると、物理領域の実際の量が必要に対してまだ十分であるかどうか判断できなくなります。

ただし、Storage APIs - Array Integration を使用すると、ホストは物理ストレージと統合できるため、基盤となるシン プロビジョニング LUN と領域の使用状況が認識されるようになります。

シン プロビジョニング統合を使用すると、ホストは次のタスクを実行できます。

- シン プロビジョニング LUN で領域の使用状況を監視し、物理領域の不足を回避します。データストアが大きくなる場合や、Storage vMotion を使用して仮想マシンをシン プロビジョニング LUN に移行する場合には、ホストは LUN と通信して物理領域の侵害や領域外の状態について警告します。
- Storage vMotion によってファイルがデータストアから削除されたときに解放されるデータストア領域についてアレイに対して通知が行われます。こうすることでアレイは解放された領域のブロックを再要求できます。

---

**注：** ESXi は、ストレージ デバイスでのシン プロビジョニングの有効化と無効化をサポートしません。

---

## 要件

シン プロビジョニング レポート機能を使用するには、ホストとストレージ アレイは次の要件を満たす必要があります。

- ESXi バージョン 5.0 以降。
- ストレージ アレイに T10 ベースの Storage APIs - Array Integration（シン プロビジョニング）をサポートする適切なファームウェアがある。詳細は、ストレージ プロバイダに連絡して、HCL をご確認ください。

## 領域使用の監視

シン プロビジョニング統合機能によって、シン プロビジョニングされた LUN の領域使用を監視し、領域不足を回避することができます。

次のサンプル図は、ESXi ホストとストレージ アレイが、基盤となるシン プロビジョニングされた LUN で、データストアの領域の違反および不足の警告を生成するために動作する方法を示しています。Storage vMotion を使用して、仮想マシンをシン プロビジョニング LUN に移行する場合、同じメカニズムが適用されます。

- 1 ストレージ固有のツールを使用して、ストレージ管理者はシン LUN をプロビジョニングし、ソフトしきい値の制限を設定し、しきい値に達するとアラームを発するように設定します。この手順はベンダー固有です。
- 2 vSphere Web Client を使用して、シン プロビジョニング LUN で VMFS データストアを作成します。データストアは、LUN がレポートする論理サイズ全体にまたがります。
- 3 データストアで使用される領域が増加して、指定したソフトしきい値に到達した場合、次のような操作を実行します。

- a ストレージ アレイはホストに違反をレポートします。
- b ホストはデータストアの警告アラームを発します。

ストレージ管理者に連絡して、LUN の容量がなくなる前に物理領域を増やすように求めたり、Storage vMotion を使用して仮想マシンを退避させることができます。

- 4 シン プロビジョニング LUN に割り当てられた領域が残っていない場合、次のような操作を実行します。
- a ストレージ アレイは、ホストに領域不足状態をレポートします。

---

**注意：** 場合によって、LUN がいっぱいになると、オフラインになるか、ホストからのマッピングが解除される場合があります。

---

- b ホストは仮想マシンを休止し、領域不足アラームを生成します。

ストレージ管理者に物理領域を要求することによって、永久的な領域不足状態を解決できます。

## シン プロビジョニング ストレージ デバイスの識別

esxcli コマンドを使用して、特定のストレージ デバイスがシン プロビジョニングかどうかを検証します。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- ◆ **esxcli --server=server\_name storage core device list -d=device\_ID** コマンドを実行します。

## 結果

次のシン プロビジョニングのステータスは、ストレージ デバイスがシン プロビジョニングであることを示します。

```
# esxcli --server=server_name storage core device list -d naa.XXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXX4c Display Name:XXXX Fibre Channel Disk(naa.XXXXXXXXXXXXX4c) Size:20480 Device
Type:Direct-Access Multipath Plugin:NMP ----- Thin Provisioning Status:yes
Attached Filters:VAAI_FILTER VAAI Status:supported -----
```

不明なステータスは、ストレージ デバイスがシックであることを示します。

**注：**一部のストレージ システムは、デバイスがシンまたはシックのいずれにかかわらず、すべてのデバイスをシン プロビジョニングとして提供します。シン プロビジョニングのステータスは常に yes です。詳細は、ストレージ ベンダーにご確認ください。

## 蓄積されたストレージ領域の再要求

VMFS データストアがシン プロビジョニング LUN に存在するとき、esxcli コマンドを使用して未使用のストレージ ブロックを再要求できます。

手順中、**--server=server\_name** で接続先サーバーを指定します。指定された接続先サーバーはユーザー名とパスワードの入力を促します。構成ファイルやセッション ファイルなど、他の接続オプションもサポートされています。接続オプションのリストについては、『vSphere Command-Line Interface スタート ガイド』を参照してください。

### 前提条件

vCLI をインストールするか、vSphere Management Assistant (vMA) 仮想マシンを導入します。vSphere Command-Line Interface スタート ガイド を参照してください。トラブルシューティングするには、ESXi Shell で esxcli コマンドを実行します。

### 手順

- ◆ 次のコマンドを実行して、シン プロビジョニングされたデバイスのために VMFS5 データストア上の未使用のストレージ ブロックを再要求します。

```
esxcli --server=server_name storage vmfs unmap --volume-label=volume_label|--volume-uuid=volume_uuid --reclaim-unit=number
```

このコマンドには次のオプションがあります。

オプション	説明
<b>-l --volume-label=volume_label</b>	マップ解除する VMFS ボリュームのラベル。これは必須の引数です。この引数を指定した場合、 <b>-u --volume-uuid=volume_uuid</b> は使用しないでください。
<b>-u --volume-uuid=volume_uuid</b>	マップ解除する VMFS ボリュームの UUID。これは必須の引数です。この引数を指定した場合、 <b>-l --volume-label=volume_label</b> は使用しないでください。
<b>-n --reclaim-unit=number</b>	反復ごとにマップ解除する VMFS ブロックの数。これは省略可能な引数です。指定されていない場合、コマンドはデフォルト値の 200 を使用します。

#### 次のステップ

---

**重要:** 追加の詳細情報は、<http://kb.vmware.com/kb/2014849> にある VMware ナレッジ ベースの記事を参照してください。

---

# ストレージ プロバイダの使用

# 25

ストレージ プロバイダとは、vSphere によって提供されるか、vStorage APIs for Storage Awareness (VASA) を介してサードパーティによって開発されたソフトウェア コンポーネントです。ストレージ プロバイダはさまざまなストレージ エンティティと統合され、それらのエンティティには、Virtual SAN や仮想ボリュームなどの外部の物理ストレージやストレージ抽象化が含まれます。ストレージ プロバイダを使用してソフトウェア ソリューションを実現することもできます（例：vSphere APIs for I/O Filtering を介して開発された I/O フィルタ）。

一般に vSphere は、ストレージ プロバイダを使用して、使用環境で提供されるストレージ トポロジ、ステータス、およびストレージ データの各サービスに関する情報を取得します。この情報は、vSphere Web Client で表示されます。表示される情報により、仮想マシンの配置について適切に決定し、ストレージ環境を監視することができます。

通常、サードパーティのストレージ プロバイダはストレージ側にインストールされ、vSphere 環境内の Storage Awareness サービスとして動作します。

ご使用のストレージがストレージ プロバイダのプラグインをサポートしているかの確認は、ストレージ ベンダーにお問い合わせください。ストレージでサードパーティのストレージ プロバイダがサポートされている場合、vSphere Web Client を使用して、各ストレージ プロバイダ コンポーネントを登録および管理します。

組み込みストレージ プロバイダは、通常、ESXi ホストで実行され、登録する必要はありません。たとえば、Virtual SAN をサポートするストレージ プロバイダは、Virtual SAN を有効にすると自動で登録されます。詳細については、『VMware Virtual SAN の管理』ドキュメントを参照してください。

この章には、次のトピックが含まれています。

- ストレージ プロバイダおよびストレージ データの表現
- ストレージ プロバイダの要件および考慮事項
- ストレージ ステータス レポート
- ストレージ プロバイダの登録
- ストレージ プロバイダとの通信のセキュリティ強化
- ストレージ プロバイダ情報の表示
- ストレージ プロバイダの登録解除
- ストレージ プロバイダの更新

## ストレージ プロバイダおよびストレージ データの表現

vCenter Server と ESXi は、基盤となる物理ストレージおよびソフトウェア定義によるストレージから、または使用可能な I/O フィルタからストレージ プロバイダが収集する情報を取得するストレージ プロバイダと通信します。これで vCenter Server は vSphere Web Client でストレージ データを表示できます。

ストレージ プロバイダが提供する情報は、次のカテゴリに区分できます。

- ストレージ データ サービスおよび機能。このタイプの情報は、Virtual SAN、仮想ボリューム、および I/O フィルタなどの機能に不可欠です。ストレージ プロバイダは、基盤となるストレージ エンティティまたは使用可能な I/O フィルタが提供するデータ サービスに関する情報を収集します。

ストレージ ポリシーの仮想マシンおよび仮想ディスクのストレージ要件を定義するときに、これらのデータ サービスを参照します。ストレージ ポリシーを使用すると、使用環境に応じて仮想マシンのストレージを適切に配置したり、仮想ディスクの特定のデータ サービスを有効にしたりできます。詳細については、[仮想マシンのストレージ ポリシーについて](#) を参照してください。

- ストレージ ステータス。このカテゴリには、さまざまなストレージ エンティティのステータスに関するレポートが含まれています。構成の変更に関して通知するアラームやイベントも含まれています。

このタイプの情報は、ストレージの接続やパフォーマンスの問題を解決するのに役立ちます。アレイ生成イベントおよびアラームをアレイ上での対応するパフォーマンスおよびロードの変化と関連付ける場合も役に立ちます。

- Storage DRS 情報。ブロック デバイスまたはファイル システムの Distributed Resource Scheduling (DRS) で使用されます。ストレージ プロバイダによりストレージ システムに関する追加情報が提供されるため、Storage DRS による決定とストレージ システム内部のリソース管理の決定の整合性は確保されます。

## ストレージ プロバイダの要件および考慮事項

ストレージ プロバイダ機能を使用するときに、特定の要件と考慮事項が適用されます。

通常、vSphere と統合するストレージ プロバイダは、ベンダーから提供されます。ストレージ プロバイダは、VMware APIs for Storage Awareness (VASA) によって実装されます。VASA アーキテクチャは、vSphere に付属するストレージ監視サービス (SMS) を拡張し、vCenter Server および ESXi ホストが VASA プロバイダと通信するために使用できる機能セットを定義します。

ストレージ プロバイダを使用するには、次の要件に従います。

- 使用するすべてのストレージ プロバイダが VMware によって認定され、適切にデプロイされていることを確認します。ストレージ プロバイダのデプロイの詳細については、ストレージ ベンダーに問い合わせるか、『VMware 互換性ガイド』を参照してください。
- ストレージ プロバイダが vSphere バージョンと互換性があることを確認してください。を参照してください。VMware 互換性ガイド

ストレージ プロバイダを使用する場合は、次の考慮事項が適用されます。

- ブロック ストレージとファイル システム ストレージ デバイスの両方でストレージ プロバイダを使用できません。

- ストレージ プロバイダは、vCenter Server を除き、どこでも実行できます。通常、サードパーティのストレージ プロバイダは、ストレージ アレイ サービス プロセッサまたはスタンドアロン ホストのいずれかで実行されます。
- 複数の vCenter Server はストレージ プロバイダの単一のインスタンスに同時に接続できます。
- 単一の vCenter Server は複数の異なるストレージ プロバイダに同時に接続できます。ホストから使用可能な物理ストレージ デバイスのタイプごとに異なるストレージ プロバイダを指定できます。

## ストレージ ステータス レポート

ストレージ プロバイダを使用している場合、vCenter Server は物理ストレージ デバイスのステータス特性を収集し、この情報を vSphere Web Client に表示できます。

ステータス情報には、イベントやアラームが含まれます。

- イベントには、ストレージ構成の重要な変更点が表示されます。そのような変更には LUN の作成および削除、または LUN が LUN のマスキングのためにアクセス不可になったことが含まれる場合があります。
- アラームは、ストレージ システムの可用性における変更を示します。たとえば、プロファイル ベースのストレージ管理を使用している場合、仮想マシンのストレージ要件を指定できます。基盤となるストレージに対する変更によって、仮想マシンのストレージ要件に違反する可能性が生じたときに、アラームが出されます。

イベントとアラームに関する詳細は、『vSphere の監視とパフォーマンス』ドキュメントを参照してください。

シン プロビジョニング LUN には特別なレポート要件があります。シン プロビジョニング LUN の領域監視については、[アレイ シン プロビジョニング](#)および [VMFS データストア](#)を参照してください。

## ストレージ プロバイダの登録

vCenter Server とストレージ プロバイダとの間に接続を確立するには、ストレージ プロバイダを登録する必要があります。クラスタの各ホストで個別のストレージ プロバイダを登録してください。

---

**注：** Virtual SAN を使用する場合、自動的に Virtual SAN のストレージ プロバイダが登録されて、ストレージ プロバイダのリストに表示されます。Virtual SAN では、ストレージ プロバイダを手動で登録することはできません。『VMware Virtual SAN の管理』ドキュメントを参照してください。

---

### 前提条件

ストレージ プロバイダ コンポーネントがストレージ側にインストールされていることを確認して、その証明書をストレージ管理者から取得します。

### 手順

- 1 vSphere Web Client ナビゲータで、vCenter Server に移動して参照します。
- 2 [構成] タブをクリックし、[ストレージ プロバイダ] をクリックします。
- 3 [新しいストレージ プロバイダの登録] アイコンをクリックします。
- 4 ストレージ プロバイダの接続情報（名前、URL、認証情報など）を入力します。



- 5 (オプション) vCenter Server にストレージ プロバイダの証明書を承認させるには、[ストレージ プロバイダ 証明書を使用する] オプションを選択して、証明書の場所を指定します。

このオプションを選択しない場合、証明書のサムプリントが表示されます。サムプリントを確認して承認することができます。

- 6 [OK] をクリックして、登録を完了します。

#### 結果

vCenter Server はストレージ プロバイダを登録し、セキュアな SSL 接続を確立しました。

#### 次のステップ

ストレージ プロバイダを登録できない場合は、VMware のナレッジベースの記事 <http://kb.vmware.com/kb/2079087> を参照してください。Virtual SAN ストレージ プロバイダ登録の問題については、<http://kb.vmware.com/kb/2105018> を参照してください。

## ストレージ プロバイダとの通信のセキュリティ強化

ストレージ プロバイダと通信するために、vCenter Server はセキュリティの高い SSL 接続を使用します。SSL 認証メカニズムでは vCenter Server とストレージ プロバイダの両方で SSL 証明書を交換し、SSL 証明書をトラストストアに追加する必要があります。

vCenter Server は、ストレージ プロバイダ証明書をストレージ プロバイダのインストールの一部としてトラストストアに追加できます。インストール中に証明書が追加されない場合には、次のいずれかの方法を使用して、ストレージ プロバイダの登録時に追加します。

- vCenter Server にストレージ プロバイダ証明書を使用するように指示します。[新規ストレージ プロバイダ] ダイアログ ボックスで、[ストレージ プロバイダ証明書を使用する] オプションを選択し、証明書の場所を指定します。
- ストレージ プロバイダ証明書のサムプリントを使用します。vCenter Server にプロバイダ証明書を使用するように指示しない場合には、証明書のサムプリントが表示されます。サムプリントを確認して承認することができます。vCenter Server は証明書をトラストストアに追加し、接続を開始します。

ストレージ プロバイダは、vCenter Server が初めてプロバイダに接続するときに vCenter Server 証明書をトラストストアに追加します。

## ストレージ プロバイダ情報の表示

ストレージ プロバイダ コンポーネントを vCenter Server に登録すると、ストレージ プロバイダ リストにそのストレージ プロバイダが表示されます。

一般的なストレージ プロバイダ情報と各ストレージ コンポーネントの詳細を表示します。

#### 手順

- 1 vSphere Web Client ナビゲータで、vCenter Server に移動して参照します。
- 2 [構成] タブをクリックし、[ストレージ プロバイダ] をクリックします。

- 3 [ストレージ プロバイダ] リストで、vCenter Server に登録されたストレージ プロバイダ コンポーネントを表示します。

リストには、名前、URL、およびビューの最終更新時間を含めた一般的なベンダー情報が表示されます。

- 4 その他の詳細を表示する場合は、リストから特定のストレージ プロバイダを選択します。

詳細には、ストレージ アレイのベンダーおよびプロバイダによってサポートされるアレイ モデルが表示されます。

---

**注：** 単一のストレージ プロバイダで、複数の異なるベンダーのストレージ アレイをサポートできます。

---

## ストレージ プロバイダの登録解除

必要のないストレージ プロバイダを登録解除することができます。

---

**注意：** Virtual SAN ストレージ プロバイダなどの VMware が提供するストレージ プロバイダを手動で登録解除することはできません。

---

### 手順

- 1 vSphere Web Client ナビゲータで、vCenter Server に移動して参照します。
- 2 [構成] タブをクリックし、[ストレージ プロバイダ] をクリックします。
- 3 ストレージ プロバイダのリストから、登録解除するストレージ プロバイダを選択して、[ストレージ プロバイダの登録解除] アイコンをクリックします。

### 結果

vCenter Server が接続を終了し、その構成からストレージ プロバイダを削除します。

## ストレージ プロバイダの更新

vCenter Server では、データベース内のストレージ データを定期的に更新します。更新は部分的に行われ、ストレージ プロバイダが vCenter Server に対してやり取りしたストレージの変更分のみが反映されます。必要に応じて、選択したストレージ プロバイダに対して、データベースの完全同期を行うことができます。

### 手順

- 1 vSphere Web Client ナビゲータで、vCenter Server に移動して参照します。
- 2 [構成] タブをクリックし、[ストレージ プロバイダ] をクリックします。
- 3 リストから、同期するストレージ プロバイダを選択して、[ストレージ プロバイダの再スキャン] アイコンをクリックします。

### 結果

vSphere Web Client により、プロバイダのストレージ データが更新されます。

vmkfstools は、VMFS ボリュームと仮想ディスクを管理するための ESXi Shell コマンドの 1 つです。vmkfstools コマンドを使用して多くのストレージ操作を実行できます。たとえば、物理パーティションで VMFS データストアを作成および管理する、または VMFS または NFS データストアに格納されている仮想ディスク ファイルを操作できます。

**注：** vmkfstools を使用して変更した後、vSphere Web Client がすぐに更新されない場合があります。クライアントの更新または再スキャン操作を使用する必要があります。

ESXi Shell の詳細については、『Getting Started with vSphere Command-Line Interfaces』を参照してください。

この章には、次のトピックが含まれています。

- vmkfstools コマンドの構文
- vmkfstools オプション

## vmkfstools コマンドの構文

一般的に、vmkfstools コマンドを実行するために root ユーザーとしてログインする必要はありません。ただし、ファイル システム コマンドなどの一部のコマンドでは、root ユーザーでのログインが必要な場合もあります。

vmkfstools コマンドは次のコマンド構文をサポートします。

vmkfstools *conn\_options options target*.

ターゲットはコマンド オプションを適用するパーティション、デバイスまたはパスを指定します。

表 26-1. vmkfstools コマンド引数

引数	説明
オプション	1 つ以上のコマンドライン オプションで、vmkfstools で実行するアクティビティ（たとえば、新規仮想ディスク作成時のディスク フォーマットの選択など）を指定するために関連付けられている引数です。 オプションを入力したら、操作を実行するターゲットを指定します。ターゲットはパーティション、デバイスまたはパスを示すことができます。
パーティション	ディスク パーティションを指定します。この引数は、 <i>disk_ID:P</i> 形式を使用します。 <i>disk_ID</i> はストレージ アレイから返されるデバイス ID で、 <i>P</i> はパーティション番号を表す整数です。パーティションの数字は 0 よりも大きく、有効な VMFS パーティションに対応している必要があります。

表 26-1. vmkfstools コマンド引数（続き）

引数	説明
デバイス	<p>デバイスまたは論理ボリュームを指定します。この引数は、ESXi のデバイス ファイル システムのパス名を使用します。パス名は <code>/vmfs/devices</code> で始まります。これは、デバイス ファイル システムのマウント ポイントです。</p> <p>異なるタイプのデバイスを指定する場合、次の形式を使用します。</p> <ul style="list-style-type: none"> <li>■ <code>/vmfs/devices/disks</code>（ローカルまたは SAN ベース ディスク）。</li> <li>■ <code>/vmfs/devices/lvm</code> (ESXi 論理ボリューム)。</li> <li>■ <code>/vmfs/devices/generic</code>(一般的な SCSI デバイス)。</li> </ul>
パス	<p>VMFS ファイル システムまたはファイルを指定します。この引数は、ディレクトリ シンボリック リンク、Raw デバイス マッピング、または <code>/vmfs</code> 下のファイルを示す絶対パスまたは相対パスです。</p> <ul style="list-style-type: none"> <li>■ VMFS ファイル システムを指定するには、次の形式を使用します。</li> </ul> <pre>/vmfs/volumes/file_system_UUID</pre> <p>または</p> <pre>/vmfs/volumes/file_system_label</pre> <ul style="list-style-type: none"> <li>■ VMFS データストア上のファイルを指定するには、次の形式を使用します。</li> </ul> <pre>/vmfs/volumes/file_system_label file_system_UUID/[dir]/myDisk.vmdk</pre> <p>現在作業中のディレクトリが <code>myDisk.vmdk</code> の親ディレクトリの場合、パス全体を入力する必要はありません。</p>

## vmkfstools オプション

vmkfstools コマンドにはいくつかのオプションがあります。オプションには、上級ユーザーのみに推奨されるものが含まれています。

長形式のオプションと 1 文字のオプションは同等です。たとえば、次のコマンドは同一です。

```
vmkfstools --createfs vmfs5 --blocksize 1m disk_ID:P vmkfstools -C vmfs5 -b 1m disk_ID:P
```

### -v サブオプション

-v サブオプションは、コマンド出力の詳細さのレベルを示します。

このサブオプションの形式は次のとおりです。

```
-v --verbose number
```

*number* の値は、1 ～ 10 の整数で指定します。

すべての `vmkfstools` オプションで `-v` サブオプションを指定できます。オプションの出力が `-v` サブオプションの使用に適していない場合、`vmkfstools` は `-v` を無視します。

**注：** `-v` サブオプションは、任意の `vmkfstools` コマンドラインに含めることができるので、各オプションの説明には `-v` がサブオプションとして含まれていません。

## ファイル システムのオプション

ファイル システムのオプションを使用すると、VMFS データストアを作成し、管理できます。これらのオプションは、NFS には適用されません。これらのタスクの多くは、vSphere Web Client を使用して実行できます。

### VMFS ボリュームの属性の一覧表示

VMFS ボリュームの属性を一覧表示するには、`vmkfstools` コマンドを使用します。

```
-P --queryfs -h --humanreadable
```

VMFS ボリューム上にあるファイルまたはディレクトリに対してこのオプションを使用すると、指定されたボリュームの属性が一覧表示されます。リスト表示された属性には、ファイル システム ラベル（ある場合には）、指定した VMFS ボリュームを構成するエクステントの数、UUID、および各エクステントが属しているデバイス名のリストが含まれます。

**注：** VMFS ファイル システムを支援する任意のデバイスがオフラインになると、それに従い、エクステントおよび使用可能な容量が変化します。

`-P` オプションとともに、`-h` サブオプションを指定できます。このようにする場合は、`vmkfstools` にボリュームの容量が、5k、12.1M、2.1G のように、さらにわかりやすい形式で表示されます。

### VMFS データストアの作成

VMFS データストアを作成するには、`vmkfstools` コマンドを使用します。

```
-C --createfs [vmfs5]
-S --setfsname datastore
```

このオプションにより、`disk_ID:P` などの指定された SCSI パーティションで VMFS5 データストアを作成します。パーティションは、ファイル システムのヘッド パーティションになります。

**注：** 新しい VMFS3 データストアを作成することはできませんが、既存の VMFS3 データストアを使用することはできます。VMFS3 データストアを VMFS5 にアップグレードします。

`-C` オプションとともに、次のサブオプションを指定できます。

- `-S --setfsname` – 作成している VMFS データストアのボリューム ラベルを定義します。このサブオプションは、必ず `-C` オプションと組み合わせて使用します。指定するラベルは、最大 128 文字で、先頭または末尾にスペースを含めることはできません。

**注：** vCenter Server ではすべてのエンティティの文字数が 80 文字に制限されています。データストア名がこの制限を超える場合は、このデータストアを vCenter Server に追加する際に名前が短縮されます。

ボリューム ラベルを定義したら、それを使用していつでも `vmkfstools` コマンドに VMFS データストアを指定できます。ボリューム ラベルは、`ls -l` コマンドで生成されるリストに、`/vmfs/volumes` ディレクトリの下にある VMFS ボリュームへのシンボリック リンクで表示されます。

VMFS ボリューム ラベルを変更するには、`ln -sf` コマンドを使用します。次に例を示します。

```
ln -sf /vmfs/volumes/UUID /vmfs/volumes/datastore
```

`datastore` は `UUID` の VMFS に使用する新しいボリューム ラベルです。

---

**注：** ホストが vCenter Server に登録されると、VMFS ボリューム ラベルに行う変更は、vCenter Server によって上書きされます。これによって、VMFS ラベルがすべての vCenter Server ホスト全体で一致することが保証されます。

---

## VMFS ファイル システムを作成する例

この例では、`naa.ID:1` パーティションで `my_vmfs` という名前の新しい VMFS5 データストアを作成します。ファイルのブロック サイズは 1MB です。

```
vmkfstools -C vmfs5 -S my_vmfs /vmfs/devices/disks/naa.ID:1
```

## 既存の VMFS ボリュームの拡張

VMFS ボリュームにエクステントを追加するには、`vmkfstools` コマンドを使用します。

```
-Z --spanfs span_partitionhead_partition
```

このオプションは、`span_partition` で指定されたパーティション全体にスパンすることによって、指定されたヘッド パーティションで VMFS ファイル システムを拡張します。`/vmfs/devices/disks/disk_ID:1` のようなフルパス名を指定する必要があります。このオプションを使用するたびに、VMFS ボリュームに新しいエクステントが追加され、ボリュームが複数のパーティション上に拡張されます。

---

**注意：** このオプションを実行すると、`span_partition` で指定した SCSI デバイスに以前に存在したデータはすべて失われます。

---

## VMFS ボリュームを拡張する例

この例では、論理ファイル システムを新しいパーティションに広げることによって拡張します。

```
vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

拡張されたファイル システムは、2 つのパーティション (`naa.disk_ID_1:1` および `naa.disk_ID_2:1`) をまたいで配置されます。この例では、`naa.disk_ID_1:1` は、ヘッド パーティションの名前です。

## 既存のエクステントの拡張

新しいエクステントを VMFS データストアに追加する代わりに、`vmkfstools -G` コマンドを使用して既存のエクステントを拡張できます。

次のオプションを使用して、基盤となるストレージの容量を増やした後で、VMFS データストアのサイズを増やします。

```
-G --growfs devicedevice
```

このオプションによって、既存の VMFS データストアまたはエクステントが拡張されます。次に例を示します。

```
vmkfstools --growfs /vmfs/devices/disks/disk_ID:1 /vmfs/devices/disks/disk_ID:1
```

## VMFS データストアのアップグレード

VMFS3 データストアを使用している場合は、VMFS5 にアップグレードする必要があります。

**注意：** アップグレードは一方方向のプロセスです。VMFS3 データストアを VMFS5 に変換したあと、VMFS3 に戻すことはできません。

データストアのアップグレードでは、次のオプションを使用します。 `vmkfstools -T|-- upgradevmfs /vmfs/volumes/UUID`

**注：** データストアにアクセスするホストはすべて、VMFS5 をサポートする必要があります。ESX/ESXi ホストバージョン 4.x 以前が VMFS3 データストアを使用している場合には、アップグレードは失敗し、データストアをアクティブに使用しているホストの MAC アドレスが表示されます。

## 仮想ディスクのオプション

仮想ディスクのオプションを使用すると、VMFS および NFS ファイル システムに格納された仮想ディスクを設定、移行、および管理できます。これらのタスクのほとんどは、vSphere Web Client から実行できます。

### サポートされているディスク フォーマット

仮想ディスクを作成またはクローン作成する場合、`-d --diskformat` サブオプションを使用して、ディスク フォーマットを指定できます。

次のフォーマットから選択します。

- `zeroedthick`（デフォルト）：仮想ディスクに必要な容量は、作成中に割り当てられます。物理デバイスに残っているあらゆるデータは、作成中には消去されませんが、あとで仮想マシンにはじめて書き込むときにオン デマンドで消去されます。仮想マシンがディスクから古いデータを読み取ることはありません。
- `eagerzeroedthick`：仮想ディスクに必要な容量は、作成時に割り当てられます。`zeroedthick` フォーマットの場合とは異なり、物理デバイスに残っているデータは、作成時に消去されます。ほかのタイプのディスクに比べて、ディスクの作成に非常に長い時間がかかることがあります。
- `thin`：シン プロビジョニング仮想ディスクです。`thick` フォーマットの場合と異なり、仮想ディスクに必要な容量は作成時に割り当てられませんが、あとで必要なときに割り当てられ、消去されます。
- `rdm: device` – 仮想互換モードの Raw ディスク マッピングです。
- `rdmp: device` – 物理互換モード（パス スルー）の Raw ディスク マッピングです。

- `2gbsparse`: エクステント サイズが最大 2GB のスパース ディスクです。VMware Fusion、Player、Server または Workstation などのホスト型 VMware 製品でこのフォーマットのディスクを使用できます。ただし、`thick` または `thin` などの互換性フォーマットで `vmkfstools` でディスクを最初に再インポートしない場合には、ESXi ホストでスパース ディスクをパワーオンにできません。

異なる VMware 製品間での仮想マシンの移行 を参照してください。

## NFS ディスク フォーマット

NFS に使用できるディスク フォーマットは `thin`、`thick`、`zeroedthick`、および `2gbsparse` のみです。

ESXi ホストではなく NFS サーバが割り当てポリシーを決定するため、`Thick`、`zeroedthick`、および `thin` フォーマットは、通常、同様に動作します。ほとんどの NFS サーバのデフォルトの割り当てポリシーは `thin` です。ただし、Storage APIs - Array Integration をサポートする NFS サーバで、仮想ディスクを `zeroedthick` フォーマットで作成できます。予約スペース操作により、NFS サーバはスペースを割り当てて保証することが可能となります。

アレイ統合 API の詳細については、[23 章 ストレージのハードウェア アクセラレーション](#) を参照してください。

## 仮想ディスクの作成

仮想ディスクを作成するには、`vmkfstools` コマンドを使用します。

```
-c --createvirtualdisk size[kK|mM|gG]
-a --adaptype [buslogic|lsilogic|ide|lsisas|pvscsi] srcfile
-d --diskformat [thin|zeroedthick|eagerzeroedthick]
-W --objecttype [file|vsan|vvol]
--policyFile fileName
```

このオプションは、データストア上の指定したパスに仮想ディスクを作成します。仮想ディスクのサイズを指定します。サイズの値を入力する際、末尾に `k`（キロバイト）、`m`（メガバイト）、または `g`（ギガバイト）を追加すると、単位のタイプを指定できます。単位のタイプに大文字と小文字の区別はありません。 `vmkfstools` は、`k` と `K` のいずれもキロバイトとして認識されます。単位のタイプを指定しない場合、`vmkfstools` ではデフォルトでバイトに設定されます。

`-c` オプションとともに、次のサブオプションを指定できます。

- `-a` は、仮想マシンが仮想ディスクとの通信に使用するコントローラを指定します。BusLogic、LSI Logic、IDE、LSI Logic SAS、VMware 準仮想化 SCSI を選択できます。
- `-d` は、ディスク フォーマットを指定します。
- `-w` は、仮想ディスクが VMFS 上のファイルか NFS データストアか、または Virtual SAN 上のオブジェクトか仮想ボリューム データストアかを指定します。
- `--policyFile fileName` はディスクの仮想マシン ストレージを指定します。



## 仮想ディスクを作成する例

この例では、myVMFS という名前の VMFS ファイル システムに、rh6.2.vmdk という名前の 2GB の仮想ディスク ファイルを作成します。このファイルは、仮想マシンがアクセスできる空の仮想ディスクです。

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```

## 仮想ディスクの初期化

仮想ディスクを初期化するには、vmkfstools コマンドを使用します。

```
-w --writezeros
```

このオプションは、すべてのデータにゼロを書き込むことで、仮想ディスクをクリーンアップします。仮想ディスクのサイズおよびその仮想ディスクをホストするデバイスへの I/O バンド幅によっては、このコマンドの完了に時間がかかることがあります。

---

**注意：** このコマンドを使用する場合、仮想ディスクにある既存のデータはすべて消失されます。

---

## シン仮想ディスクの拡張

シン仮想ディスクを拡張するには、vmkfstools コマンドを使用します。

```
-j --inflatedisk
```

このオプションは、すべての既存データを保持したまま、thin 仮想ディスクを eagerzeroedthick に変換します。このオプションは、まだ割り当てられていないブロックの割り当ておよび消去を行います。

## ゼロクリアされたブロックの削除

任意の zeroedthick または eagerzeroedthick のシン仮想ディスクを、シン ディスクに変換してゼロクリアされたブロックを削除するには、vmkfstools コマンドを使用します。

```
-K --punchzero
```

このオプションは、ゼロクリアされたすべてのブロックの割り当てを解除し、割り当て済みで有効なデータを含むブロックだけを残します。処理後の仮想ディスクはシン フォーマットになります。

## Zeroedthick 仮想ディスクから Eagerzeroedthick ディスクへの変換

任意の zeroedthick 仮想ディスクを eagerzeroedthick ディスクに変換するには、vmkfstools コマンドを使用します。

```
-k --eagerzero
```

変換の実行中に仮想ディスク上の任意のデータを保持します。

## 仮想ディスクの削除

このオプションは、VMFS ボリューム上の指定したパスにある仮想ディスク ファイルを削除します。

```
-U --deletevirtualdisk
```

## 仮想ディスクの名前の変更

このオプションは、VMFS ボリュームで指定されたパスの仮想ディスク ファイルの名前を変更します。

元のファイル名またはファイル パスである *oldName* と、新しいファイル名またはファイル パスである *newName* を指定する必要があります。

```
-E --renamevirtualdisk oldNamenewName
```

## 仮想ディスクまたは RDM のクローン作成または変換

vmkfstools コマンドを使用して、指定した仮想ディスクまたは Raw ディスクのコピーを作成します。

root ユーザー以外のユーザーは、仮想ディスクまたは RDM のクローンを作成できません。元のファイル名またはファイル パスである *oldName* と、新しいファイル名またはファイル パスである *newName* を指定する必要があります。

```
-i|--clonevirtualdisk oldName newName
-d|--diskformat [thin|zeroedthick|eagerzeroedthick|rdm:device|rdmp:device]
-W|--objecttype [file|vsan|vvol]
--policyFile fileName
-N|--avoidnativeclone
```

作成したコピーに対応するパラメータを変更するには、次のサブオプションを使用します。

- `-d|--diskformat` は、ディスク フォーマットを指定します。
- `-W|--objecttype` は、仮想ディスクが VMFS 上のファイルか NFS データストアか、または Virtual SAN 上のオブジェクトか Virtual Volumes データストアかを指定します。
- `--policyFile fileName` はディスクの仮想マシン ストレージ ポリシーを指定します。

デフォルトでは、ESXi はネイティブの方法を使用してクローン作成操作を実行します。使用しているアレイでクローン作成テクノロジーがサポートされている場合は、操作をアレイにオフロードできます。ESXi のネイティブのクローン作成を回避するには、`-N|--avoidnativeclone` オプションを指定します。

### 例：仮想ディスクのクローン作成または変換例

この例では、templates リポジトリから、ファイル システム myVMFS にある myOS.vmdk という名前の仮想ディスク ファイルに、ゴールド仮想ディスクの内容のクローンを作成します。

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold.vmdk /vmfs/volumes/myVMFS/myOS.vmdk
```

次の例のように、仮想マシンの構成ファイルに数行追加すると、この仮想ディスクを使用するように仮想マシンを構成できます。

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

ディスクのフォーマットを変更する場合は、`-d|--diskformat` サブオプションを使用します。

このサブオプションは、ESXi と互換性のないフォーマット（2gbsparse フォーマットなど）で仮想ディスクをインポートする際に役立ちます。ディスクの変換後、ESXi に作成した新しい仮想マシンにこのディスクを接続できます。

例：

```
vmkfstools -i /vmfs/volumes/myVMFS/templates/gold.vmdk /vmfs/volumes/myVMFS/myOS.vmdk -d thin
```

## 異なる VMware 製品間での仮想マシンの移行

通常、VMware Converter を使用して、仮想マシンをその他の VMware 製品から ESXi システムに移行します。ただし、`vmkfstools -i` コマンドを使用して、2gbsparse フォーマットの仮想ディスクを ESXi にインポートして、次にこのディスクを ESXi で作成する新しい仮想マシンに接続できます。

ESXi ホスト上で 2gbsparse フォーマットでディスクをパワーオンできないため、最初に仮想ディスクをインポートする必要があります。

### 手順

- 1 次のコマンドを実行することによって、2gbsparse フォーマットでディスクを ESXi ホストにインポートします。ESXi と互換性のあるディスク フォーマットを選択してください。

```
vmkfstools -i <input> <output> -d <format>
```

- 2 vSphere Web Client を使用して、インポートしたディスクを ESXi 内の仮想マシンに添付します。

詳細については、『vSphere 仮想マシン管理』を参照してください。

## 仮想ディスクの拡張

このオプションは、仮想マシンの作成後、その仮想マシンに割り当てられたディスクのサイズを拡張します。

```
-X --extendvirtualdisk newSize [kK|mM|gG]
```

このコマンドを入力する前に、このディスク ファイルを使用する仮想マシンをパワーオフする必要があります。ディスク上のファイル システムを更新することで、ゲスト OS がディスクの新しいサイズを認識して使用し、追加された領域を利用できるようにする必要があります。

**注：** 拡張後の容量が 2TB 以上になる場合は、仮想 SATA ディスクまたは任意の仮想ディスクをホット拡張できません。

`newSize` パラメータをキロバイト、メガバイト、またはギガバイトで指定するには、末尾に `k`（キロバイト）、`m`（メガバイト）、または `g`（ギガバイト）を追加します。単位のタイプに大文字と小文字の区別はありません。`vmkfstools` は、`k` と `K` のいずれもキロバイトとして認識されます。単位のタイプを指定しない場合、`vmkfstools` ではデフォルトでキロバイトに設定されます。

`newSize` パラメータは、ディスクに追加するサイズではなく、新しいサイズ全体を定義します。

たとえば、4g の仮想ディスクを 1g 分拡張するには、次のように入力します。 `vmkfstools -X 5g disk name`。  
`-d eagerzeroedthick` オプションを使用することによって、仮想ディスクを `eagerzeroedthick` フォーマットに拡張できます。

---

**注：** スナップショットが関連付けられている仮想マシンの基本ディスクを拡張しないでください。拡張すると、スナップショットのコミットや、ベース ディスクの元のサイズへの復元ができなくなります。

---

## 仮想ディスクのアップグレード

このオプションは、指定した仮想ディスク ファイルを ESX Server 2 フォーマットから ESXi フォーマットに変換します。

```
-M --migratevirtualdisk
```

## 仮想互換モードの Raw デバイス マッピングの作成

このオプションは、RDM（Raw デバイス マッピング） ファイルを VMFS ボリュームに作成し、Raw LUN をこのファイルにマッピングします。このマッピングが完了すると、通常の VMFS 仮想ディスクにアクセスする場合と同じように LUN にアクセスできます。マッピングするファイルの長さは、参照する Raw LUN のサイズと同じです。

```
-r --createrdm device
```

`device` パラメータを指定する場合は、次の形式を使用してください。

```
/vmfs/devices/disks/disk_ID:P
```

## 仮想互換モードの RDM を作成する例

この例では、`my_rdm.vmdk` という名前の RDM ファイルを作成し、そのファイルに `disk_ID` Raw ディスクをマッピングします。

```
vmkfstools -r /vmfs/devices/disks/disk_ID my_rdm.vmdk
```

仮想マシンの構成ファイルに次の行を追加すると、`my_rdm.vmdk` マッピング ファイルを使用するように仮想マシンを構成できます。

```
scsi0:0.present = TRUE scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

## 物理互換モードの Raw デバイス マッピングの作成

このオプションを使用して、パススルー モードの Raw デバイスを VMFS ボリューム上のファイルにマッピングできます。このマッピングによって、仮想マシンが仮想ディスクにアクセスするときに、ESXi SCSI コマンド フィルタリングをバイパスできます。このタイプのマッピングは、仮想マシンが企業独自の SCSI コマンドを送信する必要がありますがある場合に役に立ちます。たとえば、SAN 対応のソフトウェアを仮想マシンで実行する場合などです。

```
-z --createrdmpassthru device
```

このタイプのマッピングが完了すると、それを使用して、ほかの VMFS 仮想ディスクにアクセスする場合と同じように Raw ディスクにアクセスできます。

*device* パラメータを指定する場合は、次の形式を使用してください。

```
/vmfs/devices/disks/disk_ID
```

## RDM の属性の一覧表示

このオプションを使用して、Raw ディスク マッピングの属性を一覧表示できます。

```
-q --queryrdm
```

このオプションは、Raw ディスク RDM の名前を出力します。このオプションは、その Raw ディスクに関するほかの識別名情報（ディスク ID など）も出力します。

## 仮想ディスク構造の表示

このオプションは、仮想ディスクの構造の情報を取得します。

```
-g --geometry
```

出力形式は、Geometry information C/H/S です。ここで C はシリンダ数、H はヘッド数、S はセクタ数を表します。

**注：** ホストされた VMware 製品から仮想ディスクを ESXi ホストにインポートすると、ディスク構造の不整合を示すエラー メッセージが表示される場合があります。また、ディスク構造の不整合によって、ゲスト OS のロードまたは新規作成した仮想マシンの実行に問題が生じる場合もあります。

## 仮想ディスクの確認と修復

クリーン シャットダウンできなかった場合に、このオプションを使用して仮想ディスクを確認または修復します。

```
-x , --fix [check|repair]
```

## 整合性のためのディスク チェーンのチェック

このオプションによって、ディスク チェーン全体をチェックできます。チェーン内のリンクが壊れているかどうか、または無効な親子関係が存在するかどうかを判断できます。

```
-e --chainConsistent
```

## ストレージ デバイス オプション

デバイス オプションを使用して、物理ストレージ デバイスの管理タスクを実行できます。

### LUN の SCSI 予約の管理

-L オプションを使用して、ESXi ホスト専用として SCSI LUN を予約したり、ほかのホストがその LUN にアクセスできるように予約を解放したり、またはターゲットからの予約をすべて強制的に解除して予約をリセットしたりすることが可能です。

```
-L --lock [reserve|release|lunreset|targetreset|busreset] device
```

**注意：** -L オプションを使用すると、SAN 上のほかのサーバの操作を中断できます。-L オプションは、クラスタリング設定のトラブルシューティング時のみ使用してください。

当社から特別な指示がないかぎり、VMFS ボリュームをホストする LUN ではこのオプションは使用しないでください。

-L オプションには、複数の指定方法があります。

- -L reserve：指定した LUN を予約します。予約後は、その LUN を予約したサーバだけがアクセスできます。ほかのサーバがその LUN にアクセスしようとすると、予約エラーが発生します。
- -L release：指定した LUN の予約を解放します。ほかのサーバが、その LUN に再びアクセスできます。
- -L lunreset：指定した LUN の予約をすべて消去し、その LUN をすべてのサーバで再び使用できるようにすることで、LUN をリセットします。リセットすることによって、デバイス上のその他の LUN に影響を与えることはありません。デバイス上でほかの LUN が予約されている場合、その予約は引き続き有効です。
- -L targetreset：ターゲット全体をリセットします。リセットすると、ターゲットに関連付けられたすべての LUN の予約を消去し、すべてのサーバが再びそれらの LUN を使用できるようになります。
- -L busreset：バス上のアクセス可能なすべてのターゲットをリセットします。リセットすると、バスからアクセスできるすべての LUN の予約が消去され、すべてのサーバが再びそれらの LUN を使用できるようになります。

device パラメータを入力する場合は、次の形式を使用してください。

```
/vmfs/devices/disks/disk_ID:P
```

### デバイス ロックの解除

-B オプションによって、特定のパーティションでデバイス ロックを強制的に解除できます。

```
-B --breaklock device
```

device パラメータを入力する場合は、次の形式を使用してください。

```
/vmfs/devices/disks/disk_ID:P
```

エクステントの拡張、エクステントの追加、再署名など、データストア操作中にホストに障害が発生した場合にこのコマンドを使用できます。このコマンドを発行するときには、その他のホストがロックを保持していないことを確認してください。