

vSphere のストレージ

Update 2

変更日：2022 年 4 月 19 日

VMware vSphere 6.5

VMware ESXi 6.5

vCenter Server 6.5

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

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

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

目次

vSphere のストレージについて	14
更新情報	15
1 ストレージの概要	16
従来のストレージ仮想化モデル	16
Software-Defined Storage モデル	18
vSphere Storage API	19
2 従来のストレージ モデルでの開始	20
物理ストレージのタイプ	20
ローカル ストレージ	20
ネットワーク ストレージ	21
ターゲットとデバイスの表現	25
仮想マシンからストレージへのアクセス方法	26
ストレージ デバイスの特徴	27
ストレージのタイプの比較	30
サポート対象のストレージ アダプタ	31
ストレージ アダプタ情報の表示	31
データストアの特性	32
データストア情報の表示	34
3 ESXi と SAN の併用の概要	36
ESXi と SAN の使用例	37
SAN ストレージを ESXi と併用する場合の特性	37
ESXi ホストと複数のストレージ アレイ	38
LUN の決定	38
予測型スキームを使用した LUN の決定	39
適合型スキームを使用した LUN の決定	39
仮想マシンの場所の選択	40
サードパーティ製の管理アプリケーション	40
SAN ストレージ バックアップに関する考慮事項	41
サードパーティ製のバックアップ パッケージの使用	41
4 ESXi とファイバ チャネル SAN との併用	43
ファイバ チャネル SAN の概念	43
ファイバ チャネル SAN のポート	44
ファイバ チャネル ストレージ アレイのタイプ	44

ゾーニングとファイバ チャネル SAN との併用	45
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	45

5 ファイバ チャネル ストレージの構成 47

ESXi ファイバ チャネル SAN の要件	47
ESXi ファイバ チャネル SAN の制限	48
LUN 割り当ての設定	48
ファイバ チャネル HBA の設定	48
インストールおよびセットアップの手順	49
N-Port ID の仮想化	49
NPIV ベースの LUN アクセスの作動方法	49
NPIV 使用の要件	50
NPIV の機能と制限事項	51
仮想マシンへの WWN の割り当て	51
WWN 割り当ての変更	52

6 ファイバ チャネル オーバー イーサネットの構成 53

ファイバ チャネル オーバー イーサネット アダプタ	53
ソフトウェア FCoE の構成ガイドライン	54
ソフトウェア FCoE 用のネットワークの設定	55
ソフトウェア FCoE アダプタの追加	55

7 ファイバ チャネル SAN からの ESXi の起動 57

SAN ブートのメリット	57
ファイバ チャネル SAN から起動する場合の要件と考慮事項	58
SAN から起動するための準備	58
SAN コンポーネントとストレージ システムの構成	59
SAN から起動するストレージ アダプタの構成	59
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	59
SAN から起動する Emulex HBA の構成	60
BootBIOS プロンプトの有効化	60
BIOS の有効化	60
SAN ブートを使用するように QLogic HBA を構成	61

8 ソフトウェア FCoE による ESXi のブート 63

ソフトウェア FCoE 起動の要件と考慮事項	63
ソフトウェア FCoE ブートのベスト プラクティス	64
ソフトウェア FCoE ブートの設定	64
ソフトウェア FCoE ブート パラメータの構成	65
ソフトウェア FCoE LUN からの ESXi のインストールと起動	65
ESXi ホストのソフトウェア FCoE からの起動のトラブルシューティング	66

9 ファイバ チャンネル ストレージのベスト プラクティス 67

- ファイバ チャンネル SAN の問題の防止 67
- 自動ホスト登録の無効化 68
- 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 68
 - ストレージ アレイ パフォーマンス 69
 - ファイバ チャンネルによるサーバ パフォーマンス 69

10 iSCSI SAN と ESXi との併用 71

- iSCSI SAN の概念 71
 - iSCSI SAN のポート 72
 - iSCSI 命名規則 72
 - iSCSI イニシエータ 73
 - iSCSI 接続の確立 74
 - iSCSI ストレージ システムのタイプ 74
 - 検出、認証、およびアクセス コントロール 75
 - エラー訂正 76
- 仮想マシンから iSCSI SAN 上のデータへのアクセス方法 76

11 iSCSI アダプタおよびストレージの構成 78

- ESXi iSCSI SAN の要件 79
- ESXi iSCSI SAN の制限 79
- iSCSI の LUN 割り当ての設定 79
- ネットワーク構成と認証 80
- 独立型ハードウェア iSCSI アダプタの設定 80
 - 独立型ハードウェア iSCSI アダプタの表示 81
 - iSCSI アダプタの全般プロパティの変更 82
 - ハードウェア iSCSI のネットワーク設定の編集 83
 - iSCSI の動的または静的検出の設定 84
- 依存型ハードウェア iSCSI アダプタについて 84
 - 依存型ハードウェア iSCSI に関する考慮事項 85
 - 依存型ハードウェア iSCSI アダプタの構成 85
- ソフトウェア iSCSI アダプタについて 88
 - ソフトウェア iSCSI アダプタの構成 89
 - ソフトウェア iSCSI アダプタの無効化 91
- iSCSI アダプタの全般プロパティの変更 92
- iSCSI ネットワークの設定 93
 - iSCSI ポート バインドの要件 96
 - ソフトウェア iSCSI とのネットワーク通信設定のベスト プラクティス 96
 - iSCSI ポートのバインドの設定 100
 - iSCSI ネットワークの管理 104
 - iSCSI ネットワークのトラブルシューティング 105

iSCSI でのジャンボ フレームの使用	105
ソフトウェア iSCSI と依存型ハードウェア iSCSI でジャンボ フレームを有効にする	106
独立型のハードウェア iSCSI のジャンボ フレームを有効にする	106
iSCSI アダプタの検出アドレスの構成	107
iSCSI の動的または静的検出の設定	107
動的および静的 iSCSI ターゲットの削除	108
iSCSI アダプタの CHAP パラメータの構成	108
CHAP 認証方法の選択	109
iSCSI アダプタの CHAP の設定	110
ターゲットの CHAP の設定	111
CHAP の無効化	112
iSCSI 詳細パラメータの構成	112
iSCSI の詳細パラメータの構成	114
iSCSI セッションの管理	114
iSCSI セッションの確認	115
iSCSI セッションの追加	115
iSCSI セッションの削除	116

12 iSCSI SAN からの起動 118

iSCSI SAN ブートに関する一般的な推奨事項	118
iSCSI SAN の準備	119
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 起動の設定	120
iBFT iSCSI 起動の概要	121
iBFT iSCSI 起動に関する検討事項	122
SAN からの iBFT 起動の構成	122
ネットワークのベスト プラクティス	124
iBFT iSCSI 起動設定の変更	125
iBFT iSCSI 起動のトラブルシューティング	125

13 iSCSI ストレージのベスト プラクティス 127

iSCSI SAN の問題発生の防止	127
iSCSI SAN ストレージ パフォーマンスの最適化	128
ストレージ システムのパフォーマンス	128
iSCSI でのサーバ パフォーマンス	128
ネットワーク パフォーマンス	129
イーサネット スイッチ統計情報の確認	132

14 ストレージ デバイスの管理 133

ストレージ デバイスの特徴	133
ホストのストレージ デバイスの表示	134

- アダプタのストレージ デバイスの表示 135
- ストレージ デバイスの命名について 136
 - ストレージ デバイスの名前の変更 137
- ストレージの再スキャン操作 138
 - ストレージの再スキャンの実行 138
 - アダプタの再スキャンの実行 139
 - スキャンするストレージ デバイスの数の変更 139
- デバイス接続問題の確認 140
 - PDL 状態の検出 140
 - 予定されるストレージ デバイスの削除の実行 141
 - PDL 状態からのリカバリ 143
 - 一時的な APD 状態の処理 143
 - ストレージ デバイスの接続状態の確認 145
 - デバイスの接続問題と高可用性 146
- 構成ファイルのパラメータの編集 146
- 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 147
- ストレージ デバイスでの消去 147

15 フラッシュ デバイスの操作 148

- ESXi でのフラッシュ デバイスの使用 148
 - フラッシュ仮想ディスクの特定 149
- ストレージ デバイスのマーク 150
 - ストレージ デバイスをフラッシュとしてマーク 150
 - ストレージ デバイスをローカルとしてマーク 151
- フラッシュ デバイスの監視 151
- フラッシュ デバイスのベスト プラクティス 152
 - フラッシュ デバイスの有効期間の推定 152
- 仮想フラッシュ リソースについて 153
 - 仮想フラッシュ リソースの考慮事項 153
 - 仮想フラッシュ リソースの設定 154
 - 仮想フラッシュ リソースの削除 154
 - 仮想フラッシュの詳細設定 155
- ホスト スワップ キャッシュの構成 155
 - VMFS データストアによるホスト キャッシュの構成 156
 - 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 156

16 VMware vSphere Flash Read Cache について 158

- フラッシュ読み取りキャッシュの DRS サポート 159
- vSphere High Availability の Flash Read Cache のサポート 159
- 仮想マシンの Flash Read Cache の設定 159
- Flash Read Cache とともに仮想マシンを移行 160

17 データストアでの作業 162

- データストアのタイプ 162
- VMFS データストアについて 163
 - VMFS データストアのバージョン 164
 - ストレージ デバイス フォーマットと VMFS データストア 166
 - VMFS データストアとリポジトリ 167
 - ホスト間の VMFS データストアの共有 167
 - VMFS メタデータ アップデート 168
 - VMFS のロック メカニズム 168
 - VMFS でのスナップショットのフォーマット 173
- ネットワーク ファイル システム データストアについて 173
 - NFS プロトコルと ESXi 174
 - NFS ストレージのガイドラインと要件 176
 - NFS ストレージのファイアウォール構成 179
 - 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 181
 - NFS 4.1 用 Kerberos の使用 181
 - NFS ストレージ環境のセットアップ 182
 - Kerberos 認証用 ESXi ホストの構成 183
- データストアの作成 185
 - VMFS データストアの作成 186
 - NFS データストアの作成 188
 - Virtual Volumes データストアの作成 189
- 重複 VMFS データストアの管理 189
 - 既存のデータストア署名の保持 190
 - VMFS データストア コピーの再署名 190
- VMFS データストアのキャパシティの拡張 191
 - VMFS データストア キャパシティの増加 192
- データストアの管理操作 193
 - データストア名の変更 194
 - データストアのアンマウント 194
 - データストアのマウント 195
 - VMFS データストアの削除 195
 - データストア ブラウザの使用 196
 - ストレージ フィルタのオフ 200
- 動的なディスクミラーリングの設定 202
- ストレージ デバイスでの ESXi ホストの診断情報の収集 203
 - 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 203
 - コア ダンプの場所としてのファイルの設定 205
- VOMA によるメタデータの整合性の確認 207
- VMFS ポインタ ブロック キャッシュの構成 209
 - ホストの詳細属性の設定 210

VMFS ポインタ ブロック キャッシュの情報の取得 210

18 マルチパスとフェイルオーバーについて 212

ファイバ チャネルを使用したフェイルオーバー 212

iSCSI でのホスト ベースのフェイルオーバー 213

iSCSI でのアレイ ベースのフェイルオーバー 215

パスのフェイルオーバーと仮想マシン 216

Windows ゲスト OS にタイムアウトを設定 216

複数のパスの管理 217

VMware マルチパス モジュール 218

VMware SATP 219

VMware PSP 220

I/O の VMware NMP フロー 221

パスのスキャンと要求 221

パス情報の表示 222

データストア パスの表示 222

ストレージ デバイス パスの表示 223

パス選択ポリシーの設定 223

パス選択ポリシーの変更 224

ストレージ パスの無効化 224

ストレージ パスおよびマルチパス プラグインの管理 225

マルチパスの考慮事項 225

ホストのマルチパスの要求ルールの一覧表示 226

マルチパス モジュールの表示 227

ホストの SATP の表示 228

NMP ストレージ デバイスの表示 228

マルチパスの要求ルールの追加 229

マルチパスの要求ルールの削除 230

パスのマスク 231

パスのマスク解除 233

NMP SATP ルールの定義 234

仮想マシン I/O のキューのスケジュール設定 235

ファイル I/O ごとのスケジュールの編集 235

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 236

19 Raw デバイス マッピング 237

RAW デバイス マッピングについて 237

Raw デバイス マッピングのメリット 238

RDM の注意事項と制限事項 240

Raw デバイス マッピングの特性 241

RDM の仮想および物理互換モード 241

- 動的名前解決 241
- 仮想マシン クラスタでの Raw デバイス マッピング 241
- 利用可能な SCSI デバイス アクセス モードの比較 242
- RDM を使用する仮想マシンの作成 242
- マッピング済み LUN のパス管理 244

20 Software-Defined ストレージとストレージ ポリシー ベースの管理 245

- ストレージ ポリシー ベースの管理について 245
- 仮想マシン ストレージ ポリシー 246
- 仮想マシン ストレージ ポリシーの操作 246
- 仮想マシン ストレージ ポリシー インターフェイスの入力 247
 - ストレージ プロバイダを使用した仮想マシン ストレージ ポリシー インターフェイスへの入力 249
 - データストアへのタグの割り当て 249
- デフォルト ストレージ ポリシー 251
 - VMware によって提供されるデフォルト ポリシー 251
 - 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 252
- 仮想マシン ストレージ ポリシーの作成と管理 253
 - データストア固有および共通のルール セットについて 253
 - ルールについて 254
 - ストレージ ポリシー コンポーネントについて 255
 - 仮想マシンのストレージ ポリシーの定義 259
 - 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
 - 仮想マシンへのストレージ ポリシーの割り当て 265
 - 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 266
 - 仮想マシンのストレージ コンプライアンスの監視 268
 - 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 268
 - 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 269
 - 仮想マシン ストレージ ポリシーの再適用 270

21 ストレージ プロバイダの使用 272

- ストレージ プロバイダについて 272
- ストレージ プロバイダおよびデータの表現 273
- ストレージ プロバイダの要件および考慮事項 274
- ストレージ プロバイダの登録 274
- ストレージ プロバイダ情報の表示 275
- ストレージ プロバイダの登録解除 276
- ストレージ プロバイダの更新 276
- ストレージ プロバイダ証明書の更新 277

22 Virtual Volumes の操作 278

- Virtual Volumes について 278
- Virtual Volumes の概念 279
 - Virtual Volumes 280
 - Virtual Volumes とストレージ プロバイダ 281
 - ストレージ コンテナ 282
 - プロトコル エンドポイント 282
 - Virtual Volumes とプロトコル エンドポイントのバインドおよびバインド解除 283
 - Virtual Volumes データストア 283
 - Virtual Volumes と仮想マシン ストレージのポリシー 284
- Virtual Volumes とストレージ プロトコル 284
- Virtual Volumes のアーキテクチャ 285
- Virtual Volumes と VMware 認証局 287
- スナップショットと Virtual Volumes 288
- Virtual Volumes を有効にする前に 288
 - 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 289
- Virtual Volumes の構成 290
 - Virtual Volumes のストレージ プロバイダの登録 291
 - Virtual Volumes データストアの作成 291
 - プロトコル エンドポイントの確認と管理 292
 - プロトコル エンドポイントのパス選択ポリシーの変更 293
- Virtual Volumes データストア上の仮想マシンのプロビジョニング 293
 - Virtual Volumes の仮想マシン ストレージ ポリシーの定義 294
 - 仮想マシンへの Virtual Volumes ストレージ ポリシーの割り当て 296
 - Virtual Volumes データストアのデフォルト ストレージ ポリシーの変更 297
- Virtual Volumes およびレプリケーション 298
 - Virtual Volumes でのレプリケーションの要件 298
 - Virtual Volumes とレプリケーション グループ 299
 - Virtual Volumes および障害ドメイン 300
 - Virtual Volumes レプリケーションのワークフロー 302
 - レプリケーションのガイドラインと考慮事項 302
- vSphere Virtual Volumes の操作のベスト プラクティス 303
 - vSphere Virtual Volumes の使用上のガイドラインと制限事項 304
 - ストレージ コンテナのプロビジョニングのベスト プラクティス 305
 - vSphere Virtual Volumes のパフォーマンスのベスト プラクティス 306

23 仮想マシン I/O のフィルタリング 308

- I/O フィルタについて 308
 - I/O フィルタのタイプ 309
 - I/O フィルタリング コンポーネント 309
 - I/O フィルタのストレージ プロバイダ 311

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	311
I/O フィルタのシステム要件	312
vSphere 環境での I/O フィルタの設定	313
クラスタでの I/O フィルタのインストール	313
I/O フィルタとストレージ プロバイダの表示	314
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	315
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	315
I/O フィルタの管理	319
クラスタからの I/O フィルタのアンインストール	319
クラスタでの I/O フィルタのアップグレード	320
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	320
I/O フィルタによる仮想マシンの移行	321
24 ストレージのハードウェア アクセラレーション	322
ハードウェア アクセラレーションのメリット	322
ハードウェア アクセラレーションの要件	323
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	323
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	323
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	324
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	324
NAS デバイスでのハードウェア アクセラレーション	330
NAS プラグインのインストール	330
NAS プラグインのアンインストール	331
NAS プラグインの更新	332
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	332
ハードウェア アクセラレーションについての考慮事項	333
25 シン プロビジョニングと容量再利用	334
仮想ディスク シン プロビジョニング	334
仮想ディスクのプロビジョニング ポリシーについて	335
シン プロビジョニング仮想ディスクの作成	336
仮想マシン ストレージ リソースの表示	337
仮想マシンのディスク フォーマットの判別	337
シン仮想ディスクの拡張	337
データストアのオーバーサブスクリプションの処理	338
ESXi とアレイ シン プロビジョニング	339
容量の使用の監視	339
シン プロビジョニング ストレージ デバイスの識別	340
ストレージ容量の再利用	341
VMFS データストアからの容量再利用の要求	342
ゲスト OS からの容量の再利用の要求	346

26 vmkfstools の使用 347

vmkfstools コマンドの構文 347

vmkfstools コマンドのオプション 348

-v サブオプション 348

ファイル システムのオプション 349

仮想ディスクのオプション 351

ストレージ デバイス オプション 358

vSphere のストレージについて

vSphere のストレージでは、VMware ESXi™ および VMware vCenter Server® が提供する仮想化および software-defined ストレージ テクノロジーについて説明し、これらのテクノロジーの構成方法と使用方法を説明します。

対象読者

本書は、仮想マシンおよびストレージ仮想化テクノロジー、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。

vSphere Web Client および vSphere Client

このガイドのタスクの手順は、vSphere Web Client に基づいています。このガイドのタスクのほとんどは、新しい vSphere Client を使用して実行することもできます。新しい vSphere Client のユーザー インターフェイスの用語、トポロジ、およびワークフローは、vSphere Web Client ユーザー インターフェイスの同じ要素や項目とほとんど一致しています。特に記載がない限り、vSphere Web Client の手順を新しい vSphere Client に適用できます。

注： vSphere 6.5 リリースの vSphere Client には、vSphere Web Client のすべての機能が実装されているわけではありません。サポートされていない機能を記載した最新のリストについては、「vSphere Client ガイドの機能の更新」(<http://www.vmware.com/info?id=1413>) を参照してください。

更新情報

『vSphere のストレージ』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 のストレージ』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。
2021 年 1 月 04 日	ファイバ チャネル HBA の設定 で、ESXi が 32 Gbps ファイバ チャネルをサポートしていることを示すように更新。
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 15 日	マイナー改訂。
2018 年 8 月 13 日	動的なディスクミラーリングの設定 を更新し、詳細を追加。
2018 年 7 月 12 日	マイナー改訂。
2018 年 6 月 18 日	VMFS データストアの作成 で、VMFS6 データストアに必要な最小サイズが 2 GB であると示しました。
2018 年 5 月 21 日	データストア名の変更 で、VMware Host Client からホストに直接アクセスしている場合、vCenter Server で管理されているデータストアの名前を変更できないという説明を追加。
2018 年 5 月 3 日	初期リリース。

ストレージの概要

1

vSphere は、従来の環境と Software-Defined ストレージ環境で、さまざまなストレージ オプションと機能をサポートします。vSphere ストレージの要素と特長に関する概要を把握することで、仮想データセンターのための適切なストレージ戦略を計画できます。

この章には、次のトピックが含まれています。

- [従来のストレージ仮想化モデル](#)
- [Software-Defined Storage モデル](#)
- [vSphere Storage API](#)

従来のストレージ仮想化モデル

一般的に、ストレージ仮想化とは、物理ストレージ リソースと、仮想マシンとそのアプリケーションのキャパシティの論理的な抽象化を指します。ESXi では、ホストレベルのストレージ仮想化が提供されます。

vSphere 環境の従来のモデルは、次のストレージ テクノロジーと、ESXi および vCenter Server の仮想化機能に関連して構築されます。

ローカル ストレージおよびネットワーク ストレージ

従来のストレージ環境では、ESXi ストレージ管理プロセスは、ストレージ管理者が異なるストレージ システムに対して事前に割り当てたストレージ容量から使用します。ESXi では、ローカル ストレージとネットワーク ストレージがサポートされます。

[物理ストレージのタイプ](#)を参照してください。

ストレージ エリア ネットワーク

ストレージ エリア ネットワーク (SAN) は、コンピュータ システム (ESXi ホスト) を高性能なストレージ 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。ESXi では、ファイバ チャネルまたは iSCSI プロトコルを使用して、ストレージ システムに接続します。

[3 章 ESXi と SAN の併用の概要](#)を参照してください。

ファイバ チャネル

ファイバ チャンネル (FC) は、ESXi ホスト サーバから共有ストレージにデータ トラフィックを転送するために SAN が使用するストレージ プロトコルです。このプロトコルでは、SCSI コマンドが FC フレームにパッケージ化されます。FC SAN に接続するために、ホストではファイバ チャンネル ホスト バス アダプタ (HBA) を使用します。

[4 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

インターネット SCSI (iSCSI) は、コンピュータ システム (ESXi ホスト) と高パフォーマンスなストレージ システムの間でイーサネット接続を使用できる SAN 転送です。ストレージ システムに接続するために、ホストでは標準のネットワーク アダプタ付きのハードウェア iSCSI アダプタまたはソフトウェア iSCSI イニシエータを使用します。

[10 章 iSCSI SAN と ESXi との併用](#)を参照してください。

ストレージ デバイスまたは LUN

ESXi のコンテキストでは、デバイスと LUN という用語は交換可能なものとして使用されます。通常、両方の用語は、ブロック ストレージ システムからホストに提供される、フォーマット可能なストレージ ボリュームを意味します。

[ターゲットとデバイスの表現](#) および [14 章 ストレージ デバイスの管理](#)を参照してください。

仮想ディスク

ESXi ホスト上の仮想マシンは、仮想ディスクを使用してオペレーティング システム、アプリケーション 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。仮想ディスクは大きな物理ファイル (一連のファイル) で、他のファイルと同様に、コピー、移動、アーカイブ、およびバックアップを行えます。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 パラレル、LSI Logic パラレル、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、通常、仮想マシンのゲスト OS システムおよびアプリケーションに対して透過的です。

VMware vSphere® VMFS

ブロック ストレージ デバイスでデプロイするデータストアは、ネイティブ vSphere 仮想マシン ファイル システム (VMFS) フォーマットを使用します。VMFS フォーマットは、仮想マシンの格納に最適化された専用の高性能ファイル システム フォーマットです。

[VMFS データストアについて](#)を参照してください。

NFS

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 サーバ上にある NFS ボリュームにアクセスします。ESXi ホストは、ボリュームをマウントして NFS データストアとして使用できます。

[ネットワーク ファイル システム データストア](#)についてを参照してください。

Raw デバイス マッピング

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、[19 章 Raw デバイス マッピング](#) を参照してください。

Software-Defined Storage モデル

Software-Defined Storage では、従来のストレージ モデルのように、基盤となるストレージ容量を仮想マシンから抽象化するだけでなく、ストレージ機能を抽象化します。

Software-Defined Storage モデルでは、仮想マシンがストレージ プロビジョニングの単位となり、柔軟性のあるポリシー ベースのメカニズムを通じて仮想マシンを管理することができます。このモデルには、次の vSphere テクノロジーが使用されています。

ストレージ ポリシー ベースの管理

ストレージ ポリシー ベースの管理 (SPBM) は、vSAN や Virtual Volumes など、さまざまなデータ サービスおよびストレージ ソリューションに対して単一の制御パネルを実現するフレームワークです。このフレームワークでは、仮想マシンに対するアプリケーションの要求とストレージ エンティティの機能とがストレージ ポリシーを通じて調整されます。

[20 章 Software-Defined ストレージとストレージ ポリシー ベースの管理](#)を参照してください。

VMware vSphere[®] Virtual Volumes[™]

Virtual Volumes 機能により、データストア内部の容量の管理から、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。Virtual Volumes での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。また仮想ディスクのコンテンツ、レイアウト、管理は、すべてストレージのハードウェアによって制御されます。

[22 章 Virtual Volumes の操作](#)を参照してください。

VMware vSAN

vSAN はハイパーバイザーの一部としてネイティブに実行するソフトウェアの分散レイヤーです。vSAN は ESXi ホスト クラスターのローカル ディスクまたは直接接続されたキャパシティ デバイスを統合し、vSAN クラスターのすべてのホストで共有される単一のストレージ プールを作成します。

VMware vSAN の管理 を参照してください。

I/O フィルタ

I/O フィルタは、ESXi ホストにインストールできるソフトウェア コンポーネントで、仮想マシンに追加のデータ サービスを提供できます。実装によっては、このサービスに複製、暗号化、キャッシュなどが含まれる場合もあります。

[23 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。

vSphere 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 のファミリーです。

このストレージに関するドキュメントでは、ご使用のストレージ環境に役立ついくつかの Storage API について説明します。このファミリーの他の API (vSphere APIs - Data Protection など) の詳細については、VMware Web サイトを参照してください。

vSphere APIs for Storage Awareness

サードパーティ ベンダーまたは VMware から提供される VASA と呼ばれるこれらの API を使用すると、vCenter Server と基盤となるストレージ間の通信が可能になります。ストレージ エンティティは、VASA を使用して、設定、機能、ストレージの健全性、イベントに関する情報を vCenter Server に通知することができます。また VASA は、vCenter Server の仮想マシン ストレージ要件をストレージ エンティティに提供することができ、これによりストレージ レイヤーが確実に要件を満たすことができるようになります。

Virtual Volumes、vSAN、vSphere APIs for I/O Filtering (VAIO) およびストレージ仮想マシン ポリシーを使用するときは、VASA が必ず必要になります。21 章 [ストレージ プロバイダの使用](#)を参照してください。

vSphere APIs for Array Integration

VAAI と呼ばれるこれらの API には、次のコンポーネントが含まれています。

- ハードウェア アクセラレーション API。vSphere にアレイを統合して、特定のストレージ操作をアレイに対してオフロードできるようにします。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。24 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 アレイの容量の使用状況を監視して、容量不足を防止し、容量を再利用を支援します。ESXi とアレイ シン プロビジョニングを参照してください。

マルチパス用の vSphere API

プラグイン可能なストレージ アーキテクチャ (PSA) と呼ばれるこれらの API を使用すると、ストレージ パートナーは、アレイごとに最適化されたマルチパスおよびロードバランシング プラグインを作成して提供できます。プラグインはストレージ アレイと通信し、最適なパスの選択方法を決定して、ESXi ホストからストレージ アレイへの I/O のパフォーマンスと信頼性を向上させます。詳細については、[複数のパスの管理](#)を参照してください。

従来のストレージ モデルでの開始

2

従来の環境での ESXi ストレージの設定には、ストレージ システムとデバイスの構成、ストレージ アダプタの有効化、データストアの作成が含まれます。

この章には、次のトピックが含まれています。

- 物理ストレージのタイプ
- 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

物理ストレージのタイプ

従来のストレージ環境では、ESXi ストレージ管理プロセスは、ストレージ管理者が異なるストレージ システムに対して事前に割り当てたストレージ容量から使用します。ESXi では、ローカル ストレージとネットワーク ストレージがサポートされます。

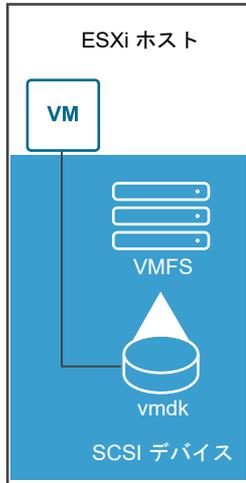
ローカル ストレージ

ESXi ホスト内の内蔵ハード ディスクをローカル ストレージにすることができます。外部に配置され、SAS や SATA などのプロトコルで直接ホストに接続される外部ストレージ システムを含めることもできます。

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 2-1. 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、ESXi ホストがストレージ デバイスへの接続を 1 つ使用しています。このデバイスで、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、ベスト プラクティスではありません。ストレージ デバイスとホスト間で単一の接続を使用すると、接続の信頼性低下や障害発生が起きた場合に、単一点障害 (SPOF) が発生し、動作が中断することがあります。ただし、ローカル ストレージ デバイスのほとんどは複数の接続をサポートしていないので、複数のバ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 ストレージ システムなど、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) は使用できません。

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、vSAN を実装できます。vSAN は、ローカル ストレージ リソースを ソフトウェア定義の共有ストレージ (Software-Defined Shared Storage) に変換します。vSAN を使用すると、共有ストレージを必要とする機能を使用できます。詳細については、『VMware vSAN 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(vSAN など) もサポートしています。vSAN 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 vSAN 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 チャンネルのみ、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。

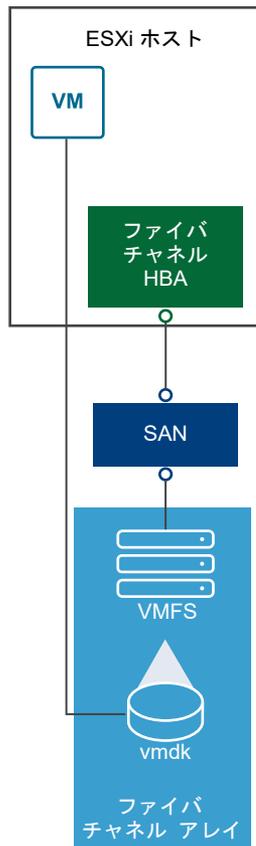
ファイバ チャンネル (FC)

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 チャンネル 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 2-2. 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。

ファイバチャネル SAN の設定の詳細については、[4 章 ESXi とファイバチャネル 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。

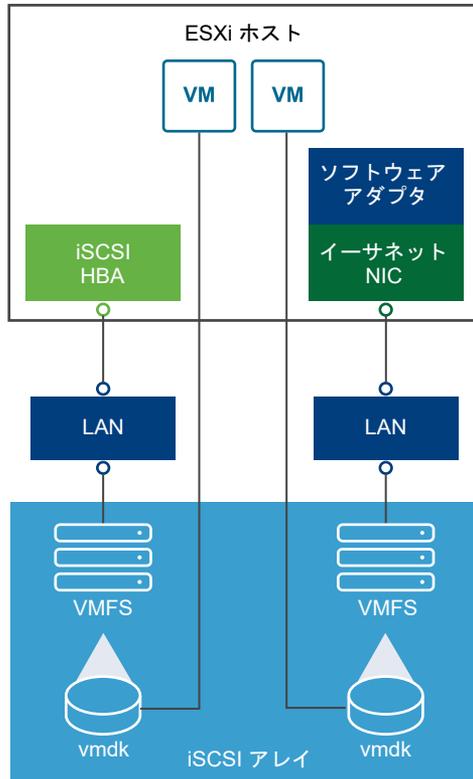
ソフトウェア iSCSI

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 2-3. 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、ホストで使用できるようになります。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、[10 章 iSCSI SAN と ESXi との併用](#)を参照してください。

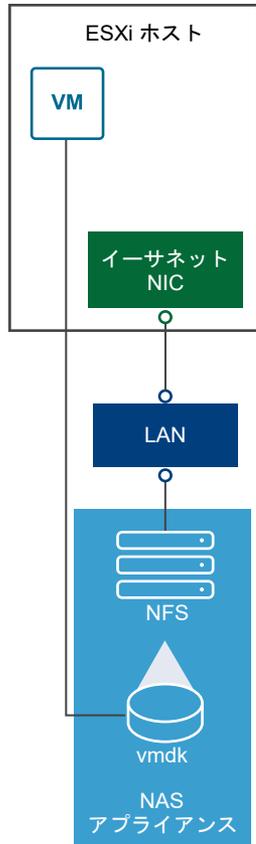
ネットワーク接続型ストレージ (NAS)

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。

ESXi ホストには直接 NFS ボリュームをマウントできます。その後、NFS データストアを使用して、VMFS データストアを使用する場合と同様に、仮想マシンを格納および管理できます。

NFS ストレージは、NFS データストア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 NAS 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 2-4. 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)

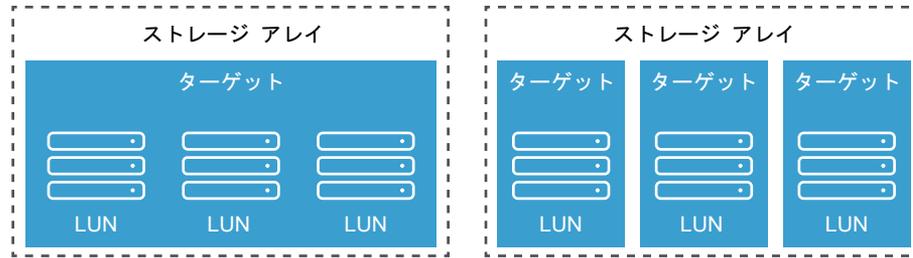
直接に接続され、複数のホストに共有アクセスを提供する SAS ストレージ システムに仮想マシンを格納します。このタイプのアクセスでは、複数のホストが、LUN の同じ VMFS データストアにアクセスできます。

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。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。ESXi の文脈では、どちらの語も、ストレージ ターゲットからホストに提供されてフォーマットの対象となりうるストレージ ボリュームを意味しています。多くの場合、ストレージ デバイスと LUN は同義です。

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 2-5. 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 つのターゲットに接続し、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、ホストが 3 つの異なるターゲットを検出し、それぞれのターゲットに 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。

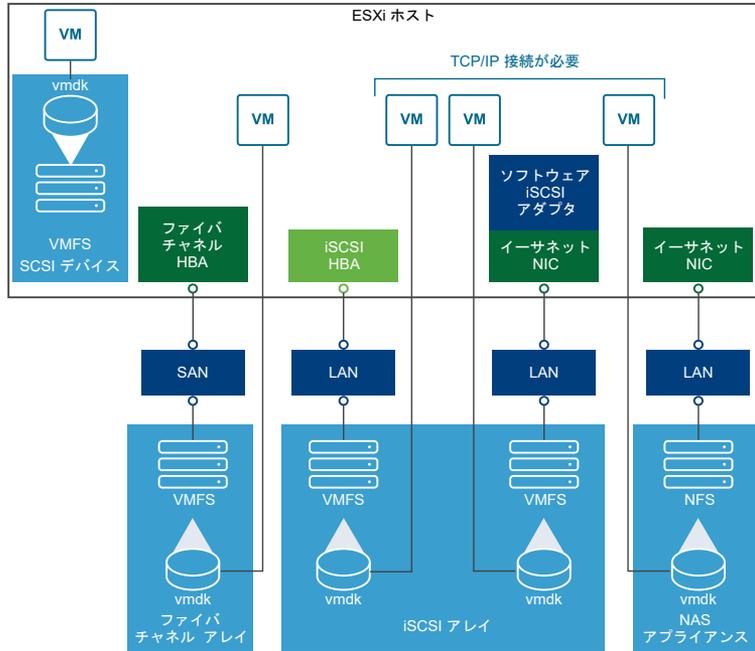
仮想マシンからストレージへのアクセス方法

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 2-6. 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 デバイスの特徴

ESXi ホストがブロックベースのストレージ システムに接続する場合、ESXi をサポートする LUN またはストレージ デバイスをホストで使用できるようになります。すべてのローカル デバイスおよびネットワーク デバイスを含む、すべてのストレージ デバイスを表示することができます。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 2-1. 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。
動作状態	デバイスが接続されているか、接続解除されているかを示します。詳細については、 ストレージ デバイスの分離 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、 15 章 フラッシュ デバイスの操作 を参照してください。

表 2-1. 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
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。物理ストレージのタイプを参照してください。
容量	ストレージ デバイスのキャパシティの合計。
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、 複数のバスの管理 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、 24 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。
セクター フォーマット	デバイスで従来の 512n が使用されるか、512e などのアドバンスド セクター フォーマットが使用されるかを示します。詳細については、 ストレージ デバイス フォーマットと VMFS データストア 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。マスタ ブート レコード (MRB) または GUID パーティション テーブル (GPT) 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、 ストレージ デバイス フォーマットと VMFS データストア 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、 18 章 マルチバスとフェイルオーバー について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] テーブル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 アイコンを使用して基本的なストレージ管理タスクを行います。

実際に使用できるアイコンは、デバイスの種類と構成によって異なります。

アイコン	説明
	ストレージ アダプタ、トポロジ、ファイル システムについての情報を更新します。
	ホスト上のすべてのストレージ 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 デバイスや VMFS データストアを検出します。
	選択したデバイスをホストから切断します。
	選択したデバイスをホストに接続します。
	選択したデバイスの表示名を変更します。
	選択したデバイスのロケータ LED をオンにします。
	選択したデバイスのロケータ LED をオフにします。
	選択したデバイスをフラッシュ ディスクとしてマークします。
	選択したデバイスを HDD ディスクとしてマークします。

- 6 [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。デバイスのマルチパス 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] で、[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] テーブル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。
- 5 アイコンを使用して基本的なストレージ管理タスクを行います。
実際に使用できるアイコンは、デバイスの種類と構成によって異なります。

アイコン	説明
	ストレージ アダプタ、トポロジ、ファイル システムについての情報を更新します。
	ホスト上のすべてのストレージ 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 デバイスや VMFS データストアを検出します。
	選択したデバイスをホストから切断します。
	選択したデバイスをホストに接続します。
	選択したデバイスの表示名を変更します。
	選択したデバイスのロケータ LED をオンにします。
	選択したデバイスのロケータ LED をオフにします。
	選択したデバイスをフラッシュ ディスクとしてマークします。
	選択したデバイスを HDD ディスクとしてマークします。
	選択したデバイスをホストのローカルとしてマークします。
	選択したデバイスをホストのリモートとしてマークします。
	選択したデバイスのパーティションを消去します。

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 2-2. 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 チャンネル	FC/SCSI	データ / LUN のブロック アクセス	FC HBA
ファイバ チャンネル 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"> ■ 統合ネットワーク アダプタ (ハードウェア FCoE) ■ FCoE をサポートする NIC (ソフトウェア FCoE)
iSCSI	IP/SCSI	データ / LUN のブロック アクセス	<ul style="list-style-type: none"> ■ iSCSI HBA または iSCSI が有効な NIC (ハードウェア iSCSI) ■ ネットワーク アダプタ (ソフトウェア iSCSI)
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 2-3. 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 のリソース管理』ドキュメントを参照してください。

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せん。

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、6 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、11 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情報の表示

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。

前提条件

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。アダプタを設定するには、次を参照してください。

- [11 章 iSCSI アダプタおよびストレージの構成](#)
- [6 章 ファイバチャネル オーバー イーサネットの構成](#)

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。
- 4 アイコンを使用して、ストレージ アダプタのタスクを実行します。

特定のアイコンが使用できるかどうかは、ストレージの構成によって異なります。

アイコン	説明
	ストレージ アダプタを追加します。ソフトウェア iSCSI およびソフトウェア FCoE に適用されます。
	ホスト上のストレージ アダプタ、トポロジ、およびファイル システムに関する情報を更新します。
	ホスト上のすべてのストレージ 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 デバイスや VMFS データストアを検出します。
	選択した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。

- 5 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。
- 6 [アダプタの詳細情報] タブを使用すると、選択したアダプタ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]	一般的なアダプタのプロパティを確認します。通常、アダプタの名前およびモデルと、特定のストレージの標準に準拠した形式の一意の識別子が含まれます。iSCSI および FCoE アダプタの場合は、このタブを使用して、追加のプロパティ（認証など）を設定します。
[デバイス]	アダプタがアクセスできるストレージ デバイスを表示します。タブを使用して、基本的なデバイス管理タスクを実行します。 アダプタのストレージ デバイスの表示 を参照してください。
[パス]	ストレージ デバイスにアクセスするためにアダプタが使用するすべてのパスを一覧表示および管理します。
[ターゲット] (ファイバ チャネルおよび iSCSI)	アダプタを介してアクセスするターゲットを確認および管理します。
[ネットワーク ポートのバインド] (iSCSI のみ)	ソフトウェアおよび依存型ハードウェアの iSCSI アダプタ用のポートのバインドを構成します。
[詳細オプション] (iSCSI のみ)	iSCSI の詳細パラメータを設定します。

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。ホストで使用でき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、VMFS データストア、NFS バージョン 3 または 4.1 データストア、Virtual Volumes データストアを作成できます。vSAN を有効にすると、vSAN データストアは自動的に作成されます。
- ESXi ホストを vCenter Server に追加すると、その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 2-4. 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 vSAN Virtual Volumes	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、 データストア名の変更 を参照してください。
ファイル システムのタイプ	VMFS NFS vSAN Virtual Volumes	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、 17 章 データストアでの作業 を参照してください。 vSAN データストアの詳細については、『VMware vSAN の管理』のドキュメントを参照してください。 Virtual Volumes の詳細については、 22 章 Virtual Volumes の操作 を参照してください。
デバイス バックアップ	VMFS NFS vSAN	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 (vSAN) 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	Virtual Volumes	対応するプロトコル エンドポイントに関する情報。 プロトコル エンドポイント 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キャパシティ。
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 ドライブなど)。詳細については、 15 章 フラッシュデバイスの操作 を参照してください。
キャパシティ	VMFS NFS vSAN Virtual Volumes	合計キャパシティ、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 vSAN Virtual Volumes	ホストの /vmfs/volumes/ ディレクトリのデータストアへのパス。

表 2-4. 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
機能セット	VMFS 注: 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 vSAN Virtual Volumes	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 のリソース管理』ドキュメントを参照してください。
ハードウェア アクセラレーション	VMFS NFS vSAN Virtual Volumes	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、24 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。 注: 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 NFS vSAN Virtual Volumes	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、データストアへのタグの割り当てを参照してください。
ホストとの接続	VMFS NFS Virtual Volumes	データストアがマウントされたホスト。
マルチパス	VMFS Virtual Volumes	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、18 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。

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。

データストア ビューを使用すると、vSphere 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の一覧表示、情報の分析、プロパティの変更を行うことができます。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。

手順

- 次のいずれかの方法で、データストアに移動します。
 - vSphere Web Client ナビゲータで、[vCenter Server のインベントリ リスト] - [データストア] の順に選択します。
 - データセンター、クラスタ、ホストなど、データストアの有効な親オブジェクトを参照し、[データストア] タブをクリックします。

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。

特定のアイコンの可用性は、データストアとその構成のタイプによって異なります。

アイコン	説明
	既存の仮想マシンをインベントリに登録します。
	データストアを作成します。
	データストア キャパシティを増加させます。
	データストア ファイル ブラウザに移動します。
	ストレージ プロバイダを管理します。
	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。

- 3 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。
- 4 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。
[設定]	データストアのプロパティを表示および変更します。表示されるメニュー項目は、データストアのタイプによって異なります。
[権限]	選択したデータストアに権限を割り当てたり、権限を編集します。
[ファイル]	データストア ファイル ブラウザに移動します。
[ホスト]	データストアがマウントされたホストを表示します。
[仮想マシン]	データストア上に存在する仮想マシンを表示します。

ESXi と SAN の併用の概要

3

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択](#)

- 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 レイアウトの簡素化

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ます。外部ストレージが必要になる可能性もあります。SAN には、システム アーキテクチャが単純化されるなどの利点があります。

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。理想的な使用とは、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たものです。必要に応じて、仮想マシンの移行が実行（または推奨）されます。

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できます。仮想マシンで実行されるアプリケーションは、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得ることができます。

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 システムを購入したときは、Storage vMotion を使用して既存のストレージから新しいターゲットに仮想マシンをライブ移行できます。移行は、仮想マシンを停止することなく実行できます。

SAN ストレージを ESXi と併用する場合の特性

SAN と ESXi ホストとの併用は、従来の SAN の使用方法とさまざまな点で異なります。

SAN ストレージを ESXi と併用する場合、次の点を考慮してください。

- ストレージ上に存在する仮想マシンのオペレーティング システムに、SAN 管理ツールを使用して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 SATP を使用している場合は、その SATP のデフォルトの PSP を変更するときに注意します。すべてのアレイに変更が適用されます。SATP および PSP については、[18 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 台のアレイの設定を変更すると、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> で会社のナレッジ 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 を検討する際は、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 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、プロビジョニングする LUN の数とサイズを決めるのが難しい場合があります。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択

仮想マシンのパフォーマンスを最適化する場合、ストレージの場所が重要な要因になります。ストレージの要件に応じて、高いパフォーマンスと高可用性を提供するストレージを選択する場合や、パフォーマンスが低いストレージを選択する場合があります。

いくつかの要件に応じて、ストレージは異なる階層に分けることができます。

- **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。下位の SCSI ドライブまたは SATA を使用します。

すべての仮想マシンがライフ サイクル全体で最高のパフォーマンスと可用性を備えたストレージに配置される必要があるわけではありません。

仮想マシンを配置する場所を決定するときは、次の考慮事項が適用されます。

- 仮想マシンの重要度
- パフォーマンスと可用性の要件
- PiT リストア要件
- バックアップおよびレプリケーションの要件

仮想マシンは、重要度またはテクノロジーの変更のために、ライフ サイクルを通じて階層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。

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 ホストと一緒に使用できます。

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、仮想マシンのメリットが得られます。ただし、より間接的になるため、管理ソフトウェアで SAN を検出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ル設定は、いくつかの要因によって異なります。

- 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、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対する全体的な影響。
- 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。
- データをアーカイブするためのリソース可用性 (オフライン メディア アクセスなど)。

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。

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、オンライン ストレージにあるリカバリ ボリュームの使用を必須とすることができます。このプロセスにより、失われたデータ コンポーネントのために低速なオフライン メディアにアクセスする必要性を低減または排除できます。

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、ユーザーデータを保護します。

VMware が提供する Storage APIs - Data Protection は、サードパーティの製品と連携させることができます。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、データの整合性を確保します。

Storage APIs - Data Protection は、VMFS のスナップショット機能を使用するため、バックアップで仮想マシンを停止する必要はありません。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、バックアップ時間枠を拡大する必要はありません。

Storage APIs - Data Protection とバックアップ製品との連携の詳細については、VMware Web サイトをご覧ください。ご利用の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

4

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おいてください。

SAN（ストレージエリアネットワーク）は、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 が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トリ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 へのアクセスをサポートします。パスが機能しない場合を除き、すべてのパスはアクティブです。

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、ホストはターゲット 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 コマンドを送信すると、SCSI 仮想化レイヤーがこれらのコマンドを VMFS ファイル処理に変換します。

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 ディスクの読み取りまたは書き込みを行うとき、仮想ディスクに対して SCSI コマンドが送信されます。
- 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 VMFS ボリュームで適切な仮想ディスク ファイルを特定します。
 - 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基づいて、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ます。その要求が、スイッチによって適切なストレージ デバイスにルーティングされます。

ファイバチャネルストレージの構成

5

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。

- ESXi システムが、使用する 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をサポートしていることを確認します。最新のリストについては、『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 ブートのディスクレスサーバを使用する場合は、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、[19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 のキュー深度は、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深度の変更の詳細は、『vSphere の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 を実行している仮想マシンで、SCSI TimeoutValue パラメータの値を 60 に増やします。この値の増大によって、Windows はパスのフェイルオーバーから生じる遅延した I/O を許容できます。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 が連携する場合の LUN の割り当て方法に関する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。

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。このアクションにより、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 32 Gbps 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的なエンティ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 チャンネル 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。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。

仮想マシンには WWN が割り当てられており、WWN のペアを含めるように、仮想マシンの設定ファイル (.vmx) が更新されます。WWN のペアは、World Wide Port Name (WWPN) と、World Wide Node Name (WWNN) から構成されます。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、物理 HBA として FC ファブリックに表示される仮想 HBA です。VPORT には一意の識別子があり、これは仮想マシンに割り当てられた WWN ペアです。

各 VPORT は仮想マシンに特有のもので、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、ターゲット ホスト上で開きます。

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。各物理パスによって、LUN へのアクセスに使用する仮想パスが決まります。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ます。

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 チャンネル NPIV の三角形をクリックして、NPIV のメニュー項目を展開します。
- 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

新しく作成した WWN をファブリックに登録します。

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

6

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します。

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専用におフロードされた統合ネットワーク 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、このアダプタを構成する必要はありません。

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、スパンニング 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 アダプタを作成します。

この手順では、単一の FCoE 物理ネットワーク アダプタに vSphere Standard 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します。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 のネットワーク』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 [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 Standard 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、分離されたネットワークが必要です。入力する VLAN ID が、ホストで通常のネットワークに対して使用されるものとは異なることを確認します。詳細については、『vSphere のネットワーク』ドキュメントを参照してください。
- 8 設定が完了したら情報を確認して、[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 Standard 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にソフトウェア 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

7

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 ブートのメリット
- ファイバチャネル SAN から起動する場合の要件と考慮事項
- 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 ブートを使用するように QLogic HBA を構成

SAN ブートのメリット

SAN ブートには、ESXi 環境に対して多くのメリットがあります。ただし、SAN ブートがホストに適していない場合もあります。SAN ブートを使用するようにシステムを設定する前に、SAN ブート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 ブートを使用する場合、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 ブートを使用した場合、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 から起動する場合の要件と考慮事項

ESXi 起動構成は、特定の要件を満たす必要があります。

表 7-1. 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を実行します。
アダプタの要件	アダプタを設定することで、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"> ■ 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 だけにアクセスできる必要があります。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。 ■ 複数のサーバで診断のパーティションを共有できます。この設定を行うには、アレイ固有の LUN マスキングを使用できます。
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認定されていない場合、SAN 接続はスイッチ 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認定されている場合、SAN をアレイに直接接続できます。SAN ブートは、両方のスイッチ トポロジと直接接続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 ブート用に ESXi ホストを準備するときは、いくつかのタスクを実行します。

本セクションでは、ラック マウント サーバで SAN ブート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 サーバで SAN ブート オプションを有効にする方法については、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。インストール メディアから起動するには、BIOS 設定でシステムの起動シーケンスを変更します。

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 このプロセスは、オブジェクトの作成とも呼ばれます。
 - 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： スクリプトによるインストール プロセスを使用して、SAN ブート 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。
起動アダプタの設定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。インストール メディアから起動するには、BIOS 設定でシステムの起動シーケンスを変更します。

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 システムをパワーオンして、システムの BIOS 設定/設定ユーティリティに移動します。
- 2 [起動オプション] を選択して Enter キーを押します。
- 3 [起動シーケンス オプション] を選択して Enter キーを押します。
- 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 を設定するには、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 を設定するには、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設定するには、Emulex のプロンプトで ALT + E キーを押して次の手順を実行します。
 - 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 ブートを使用するように QLogic HBA を構成

この例では、ESXi を SAN ブートするように QLogic HBA を設定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	HBA が 1 つだけの場合、Fast!UTIL Options ページが表示されます。手順 手順 3 に進みます。
複数の HBA	複数の HBA がある場合は、HBA を手動で選択します。 <ol style="list-style-type: none"> 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 にポインタを移動します。 b [Enter] を押します。

- 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 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] キーを押します。
ファイバ チャネル デバイスの選択ページが開きます。

- 8 特定のストレージ プロセッサを選択し、[Enter] キーを押します。

アクティブ-パッシブ ストレージ アレイを使用する場合、選択したストレージ プロセッサを起動 LUN への優先 (アクティブな) パスに置く必要があります。どちらのストレージ プロセッサがアクティブなパ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 ストレージ プロセッサに接続されている 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 の選択ページを使用する必要はありません。
LUN が複数の場合	LUN の選択ページが開きます。ポインタを使用して起動 LUN を選択し、[Enter] キーを押します。

- 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

8

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。

ほとんどの設定は、ネットワーク アダプタの option ROM を介して実行できます。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。

設定パラメータはアダプタの option 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](#)
- [ESXi ホストのソフトウェア FCoE からの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 からシステムを起動するときの具体的なガイドラインは次のとおりです。

- 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設定します。
 - 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 アダプタおよびネットワーク 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、いくつかの設定を行います。

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。

- 部分的な 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) のいずれかを含む。

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 option ROM を設定し、ターゲット起動 LUN が参照先となるようにします。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 ブートが有効に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] ページで、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 option 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 画面の指示を見ながらインストールを行います。

- 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。

ESXi ホストのソフトウェア FCoE からの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 ESXi をインストールまたは起動する際、インストールまたは起動プロセスが機能しません。使用する FCoE 設定に、VMware ソフトウェア FCoE アダプタおよび部分的な FCoE オフロード機能を持つネットワーク アダプタが含まれています。

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

9

ESXi をファイバチャネル SAN と使用するときは、パフォーマンスの問題を回避するための推奨事項を実行します。

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 のリソース管理』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、ベンダーのドキュメントを参照して、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してください。詳細については、[24 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 と共に使用する場合は、専用のガイドラインに合わせて SAN の問題を回避してください。

SAN 構成に関する問題を防ぐには、以下のヒントを参考にしてください。

- 各 LUN には、VMFS データストアを 1 つだけ配置します。
- パス 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パス 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確認します。
 - 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。サーバで使用できるバス間で、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。
- LUN の ID を変更した後、ストレージを再スキャンして、ホスト上の ID をリセットします。再スキャンについては、[ストレージの再スキャン操作](#)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

この操作によって、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発生した場合は、ストレージ アレイ ベンダーのドキュメントで関連情報を確認してください。

次の一般的なガイドラインで説明するように実行すると、vSphere 環境でアレイのパフォーマンスを向上させることができます。

- LUN を割り当てるときは、複数のホストがその LUN にアクセスする可能性があり、各ホストで複数の仮想マシンが実行されることがある点を考慮に入れます。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、通常、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 は含めません。
- 読み取り/書き込みキャッシュが使用でき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 パスの間でロード 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。

静的にロード バランシングされたストレージ アレイの調整は、1 秒あたりの I/O 操作、1 秒あたりのブロック数、応答時間など、特定のパフォーマンス統計の監視の問題になります。すべての SP 間でワークロードが分散されるように LUN ワークロードを分散させることも重要です。

注： 動的ロード バランシングは、ESXi では現在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、次のガイドラインを実行します。

- 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の使用を監視します。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。

- ホストにあるアプリケーションのピーク期間のスループットを向上させるために、各ホストに十分な 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、それぞれのアプリケーションでスループットが向上し、待ち時間が短くなります。
- HBA の潜在的な障害に対する冗長性を確保するために、ホスト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、そのリソースが複数のオペレーティング システムで使用および共有されることを念頭に置く。ESXi ホストで必要になる LUN のパフォーマンスは、通常の物理マシンを使用する場合よりも大幅に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。
- vCenter Server で複数の ESXi システムを使用する場合、ストレージ サブシステムのパフォーマンス要件はそれに応じて高くなる。
- 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 数は、HBA およびストレージ アレイで処理できる I/O 数と一致させる必要がある。

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。ホスト側の SAN コンポーネントには、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) があります。また、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ー、ケーブル、ストレージ プロセッサ (SP)、ストレージ ディスク システムなどが含まれます。

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 エミュレータがターゲットとして使用される場合もあります。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 に対する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、[18 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。

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

iSCSI 修飾名 (IQN) の形式は、`iqn.yyyy-mm.naming-authority:unique name` です。

- `yyyy-mm` は、命名機関が設立された年と月です。
- `naming-authority` は、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` という命名機関は、`iqn.1998-01.com.vmware.iscsi` という形式の iSCSI 修飾名になります。この名前は、ドメイン名 `vmware.com` が 1998 年 1 月に登録され、`iscsi` がサブドメインであり、`vmware.com` が管理していることを示します。

- *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形式

エンタープライズ一意識別子 (EUI) の形式は、`eui.16_hex_digits` です。

例えば、`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 を持つエンティティが割り当て、一意であることが必要です。

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、[11 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。ソフトウェア iSCSI アダプタを使用して、ホストは、標準のネットワーク アダプタを介して iSCSI ストレージ デバイスに接続できます。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。

通常、独立型ハードウェア iSCSI アダプタは 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です。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。

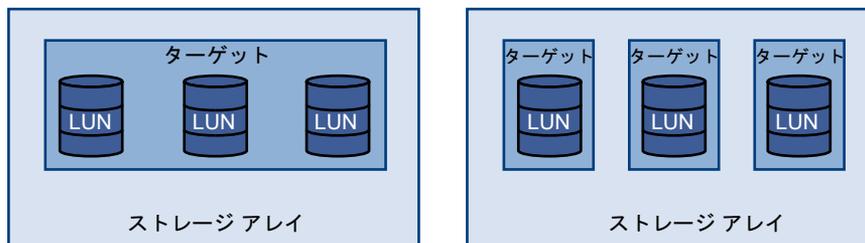
ハードウェア iSCSI アダプタではライセンスが必要になる場合があります。そうしない場合、クライアントまたは vSphere CLI には表示されない可能性があります。ライセンス情報については、ベンダーにお問い合わせください。

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 ユニットの表し方を示します。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 10-1. 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、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 へのアクセスをサポートします。すべてのパスは、パスが失敗しない限り常にアクティブです。

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、ホストはターゲット 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。仮想ポート ストレージ システムは、アクティブ-アクティブのストレージ デバイスですが、単一ポートによって複数接続を隠します。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。この機能は、透過的なフェイルオーバーと呼ばれます。

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一連のターゲットを返します。ESXi では、動的検出と静的検出の 2 種類の検出方法があります。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ます。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にのみアクセスできます。

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 CHAP 認証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 を有効にする方法の詳細は、[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 つのうち 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間で双方向に伝送されるヘッダおよび SCSI データにそれぞれに含まれます。

ヘッダおよびデータのダイジェストは、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に加え、暗号化されていないデータの整合性を検査します。ここでは、ルーター、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。

SCSI 接続が確立されたときに、ダイジェストの有無と種類の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の双方がダイジェスト設定を受け入れた場合、そのイニシエータとターゲット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追加処理が発生するため、スループットおよび CPU 使用率に影響する場合があります。

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低減されます。

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 コマンドを送信すると、SCSI 仮想化レイヤーがこれらのコマンドを VMFS ファイル処理に変換します。

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 ディスクの読み取りまたは書き込みを行うとき、仮想ディスクに対して SCSI コマンドが送信されます。
- 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 VMFS ボリュームから適切な仮想ディスク ファイルを特定します。
 - 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 ネットワーク上のイーサネット スイッチとルーターが、適切なストレージ デバイスに要求を転送します。

iSCSI アダプタおよびストレージの構成

11

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。

次の表は、ESXi がサポートする iSCSI アダプタ (vmhbas) 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 11-1. 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です。	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

SAN と正常に連携するには、ESXi ホストは、いくつかの要件を満たしている必要があります。

- ESXi システムが、SAN ストレージ ハードウェアとファームウェアをサポートしていることを確認します。最新のリストについては、『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 ブートに関する一般的な推奨事項](#)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、[19 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深度の変更の詳細は、『vSphere のトラブルシューティング』を参照してください。
- Microsoft Windows を実行している仮想マシンで、SCSI TimeoutValue パラメータの値を増やします。このパラメータの設定によって、Windows 仮想マシンがパスのフェイルオーバーから生じる遅延した I/O を許容する度合いが向上します。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 コマンドの使用の詳細については、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 IP アドレス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.設定.ストレージ パーティション設定

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。

アダプタのデフォルトの詳細が表示されます。

アダプタ情報	説明
モデル	アダプタのモデル。
iSCSI 名	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 名を編集することができます。
iSCSI エイリアス	iSCSI 名のかわりに使用される、わかりやすい名前。iSCSI エイリアスを編集することができます。
IP アドレス	iSCSI HBA に割り当てられているアドレス。
ターゲット	アダプタを介してアクセスしたアクセス先数。
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。

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 アドレス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、必ずその名前および IP アドレスに適切な形式を使用してください。

前提条件

必要な権限：ホスト.設定.ストレージ パーティション設定

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 (オプション) 以下の全般プロパティを変更します。

オプション	説明
iSCSI 名	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。名前を変更する場合、入力した名前が世界中で一意であり、適切な形式であることを確認してください。そうしないと、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。
iSCSI エイリアス	iSCSI 名の代わりに使用する、わかりやすい名前。

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 を無効にするか、IP アドレスを取得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 を無効にします。
IPv4 設定を自動的に取得します	DHCP を使用して IP アドレス設定を取得します。
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 を無効にするか、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 を無効にします。
IPv6 を有効にする	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。
ルーターの通知を使用して IPv6 アドレスを自動的に取得	ルーターの通知を使用して 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 プリフィックス長を入力し、[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] 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、[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。

検出方法	説明
動的検出	<ol style="list-style-type: none"> a [動的検出] をクリックし、[追加] をクリックします。 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。 c iSCSI アダプタを再スキャンします。 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。
静的検出	<ol style="list-style-type: none"> a [静的検出] をクリックし、[追加] をクリックします。 b ターゲットの情報を入力し、[OK] をクリックします。 c iSCSI アダプタを再スキャンします。

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 アダプタはデフォルトで有効です。これが機能するには、仮想 VMkernel アダプタ (vmk) を介して、アダプタと関連付けられた物理ネットワーク アダプタ (vmnic) 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 アダプタを設定すると、ネットワーク接続を介して検出および認証データが渡されます。iSCSI トラフィックは、ネットワークをバイパスして、iSCSI エンジンを通過します。

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 IP アドレス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 ネットワークの設定

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。

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 アドレス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、必ずその名前および IP アドレスに適切な形式を使用してください。

前提条件

必要な権限：ホスト.設定.ストレージ パーティション設定

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 (オプション) 以下の全般プロパティを変更します。

オプション	説明
iSCSI 名	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。名前を変更する場合、入力した名前が世界中で一意であり、適切な形式であることを確認してください。そうしないと、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。
iSCSI エイリアス	iSCSI 名の代わりに使用する、わかりやすい名前。

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 ネットワークの設定

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。

詳細については、[iSCSI ネットワークの設定](#) を参照してください。

iSCSI 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] 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、[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。

検出方法	説明
動的検出	<ol style="list-style-type: none"> a [動的検出] をクリックし、[追加] をクリックします。 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。 c iSCSI アダプタを再スキャンします。 <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"> a [静的検出] をクリックし、[追加] をクリックします。 b ターゲットの情報を入力し、[OK] をクリックします。 c iSCSI アダプタを再スキャンします。

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 を実装すると、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。

ソフトウェア iSCSI アダプタを使用する場合は、次の考慮事項に留意してください。

- 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。

- スクリプト内でソフトウェア アダプタの名前 (vmhbaXX) はハードコーディングしないでください。名前が ESXi のリリースごとに変更される可能性があります。ハードコーディングされた古い名前を使用している場合、変更によって既存のスクリプトでエラーが発生する可能性があります。名前の変更は、iSCSI ソフトウェア アダプタの動作には影響しません。

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 アダプタを有効にする

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 アドレス設定も変更できます。

3 iSCSI ネットワークの設定

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。

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 アダプタを有効にする

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になります。

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]、[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 アドレス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、必ずその名前および IP アドレスに適切な形式を使用してください。

前提条件

必要な権限：ホスト.設定.ストレージ パーティション設定

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 (オプション) 以下の全般プロパティを変更します。

オプション	説明
iSCSI 名	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。名前を変更する場合、入力した名前が世界中で一意であり、適切な形式であることを確認してください。そうしないと、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。
iSCSI エイリアス	iSCSI 名の代わりに使用する、わかりやすい名前。

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。

詳細については、[iSCSI ネットワークの設定](#)を参照してください。

iSCSI 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] 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、[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。

検出方法	説明
動的検出	a [動的検出] をクリックし、[追加] をクリックします。 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。 c iSCSI アダプタを再スキャンします。 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。
静的検出	a [静的検出] をクリックし、[追加] をクリックします。 b ターゲットの情報を入力し、[OK] をクリックします。 c iSCSI アダプタを再スキャンします。

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] 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] タブをクリックします。
- 5 [無効化] をクリックして、アダプタの無効化を確認します。
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 アドレス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、必ずその名前および IP アドレスに適切な形式を使用してください。

前提条件

必要な権限：ホスト.設定.ストレージ パーティション設定

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 (オプション) 以下の全般プロパティを変更します。

オプション	説明
iSCSI 名	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。名前を変更する場合、入力した名前が世界中で一意であり、適切な形式であることを確認してください。そうしないと、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。
iSCSI エイリアス	iSCSI 名の代わりに使用する、わかりやすい名前。

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 ネットワーク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。

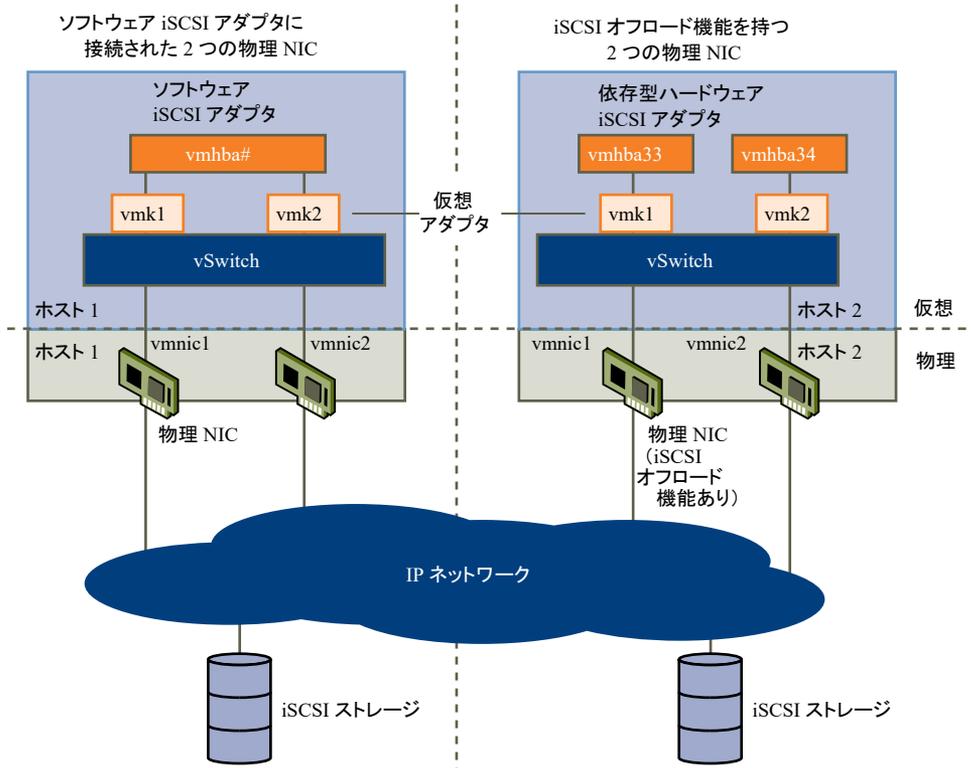
iSCSI 構成での複数のネットワーク アダプタ

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 11-1. iSCSI を使用したネットワーク



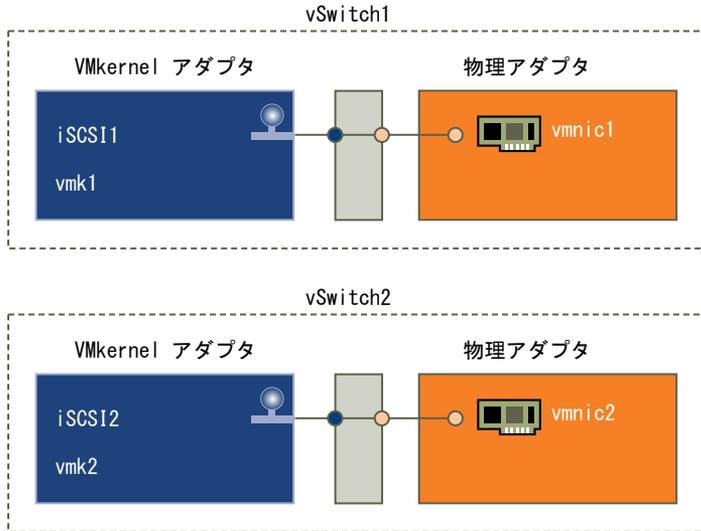
iSCSI アダプタと物理 NIC は、仮想ネットワーク アダプタまたは VMkernel ポートとも呼ばれる、仮想 VMkernel アダプタを介して接続されます。それぞれの仮想ネットワーク アダプタと物理ネットワーク アダプタ間で 1:1 のマッピングを使用して、VMkernel アダプタ (vmk) を vSphere スイッチ (vSwitch) に作成します。

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 アダプタで接続の問題が発生する場合があります、ホストは iSCSI LUN を検出できません。

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 のネットワーク』ドキュメントを参照してください。

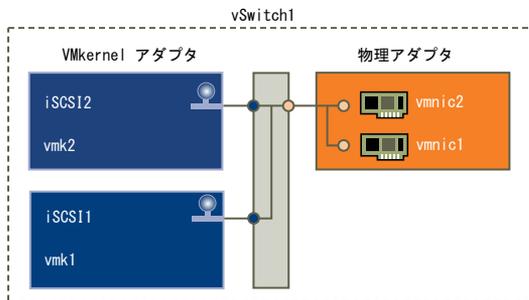
図 11-2. 個別の vSphere Standard Switch での 1 対 1 のアダプタ マッピング



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にある場合は、単一の vSwitch 構成を使用します。

図 11-3. 単一の vSphere Standard Switch 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 11-2. 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		
vmhbaX2	vmk1	vmnic1
	vmk2	vmnic2
依存型ハードウェア iSCSI		
vmhbaX3	vmk1	vmnic1
vmhbaX4	vmk2	vmnic2

iSCSI ポート バインドの要件

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。

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。

ソフトウェア iSCSI とのネットワーク通信設定のベスト プラクティス

ソフトウェア iSCSI とのネットワーク通信を設定する際には、次のベスト プラクティスを考慮してください。

ソフトウェア iSCSI ポートのバインド

ESXi ホスト上のソフトウェア iSCSI イニシエータを 1 つ以上の VMkernel ポートにバインドすると、バインドされたポートのみを使用して iSCSI トラフィックがやり取りされるようになります。ポートのバインドを設定すると、バインドされたすべてのポートから、設定されたすべてのターゲット ポータルへの iSCSI セッションが iSCSI イニシエータにより確立されます。

次の例を参照してください。

VMkernel ポート	ターゲット ポータル	iSCSI セッション
バインドされた VMkernel ポート × 2	ターゲット ポータル × 2	4 つのセッション (2 × 2)
バインドされた VMkernel ポート × 4	ターゲット ポータル × 1	4 つのセッション (4 × 1)
バインドされた VMkernel ポート × 2	ターゲット ポータル × 4	8 つのセッション (2 × 4)

注： ポートのバインドを使用する場合は、すべての VMkernel ポートからすべてのターゲット ポータルに到達可能であることを確認してください。到達可能でない場合は、iSCSI セッションの確立に失敗する可能性があります。その結果、再スキャン処理に予想以上の時間がかかる場合があります。

ポートのバインドを使用しない場合

ポートのバインドを使用しない場合は、ESXi ネットワーク レイヤーのルーティング テーブルに従って最適な VMkernel ポートが選択されます。ホストはこのポートを使用してターゲット ポータルとの iSCSI セッションを確立します。ポートのバインドを使用しない場合、確立されるセッションは、1 つのターゲット ポータルにつき 1 つのみです。

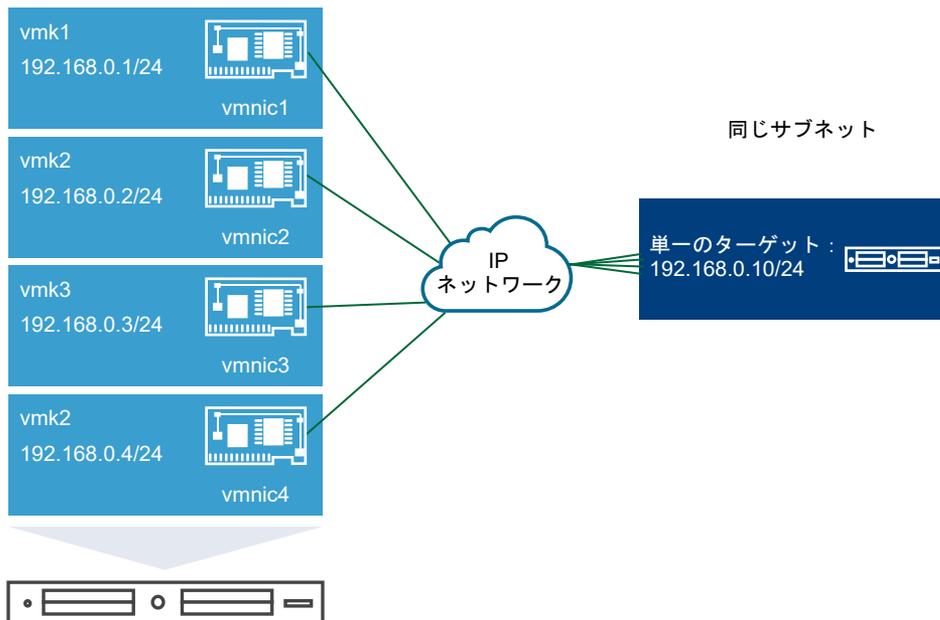
次の例を参照してください。

VMkernel ポート	ターゲット ポータル	iSCSI セッション
バインドされていない VMkernel ポート x 2	ターゲット ポータル x 2	2 つのセッション
バインドされていない VMkernel ポート x 4	ターゲット ポータル x 1	1 つのセッション
バインドされていない VMkernel ポート x 2	ターゲット ポータル x 4	4 つのセッション

ソフトウェア iSCSI でのマルチパスの使用

例 1：ネットワーク ポータルが 1 つだけの場合の iSCSI ターゲットへのマルチパス

ターゲットにネットワーク ポータルが 1 つしか存在しない場合は、ESXi ホストで複数の VMkernel ポートを追加し、それらのポートを iSCSI イニシエータにバインドすることで複数のパスを作成できます。

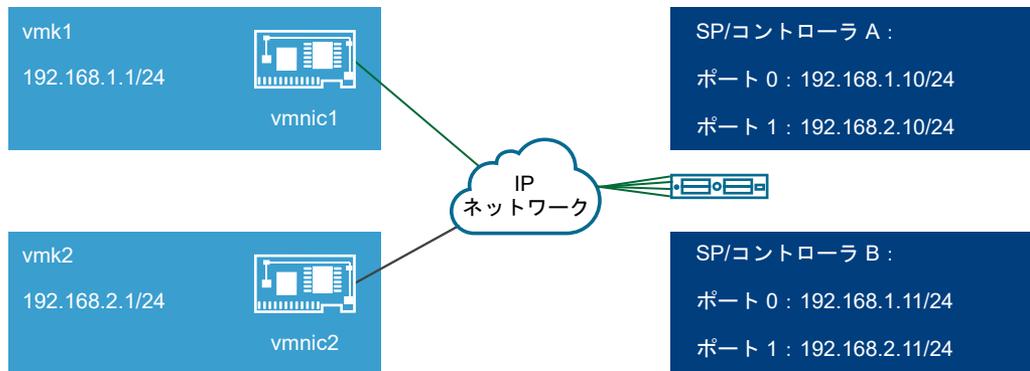


この例では、すべてのイニシエータ ポートとターゲット ポータルが同じサブネットに属しています。また、バインドされているすべてのポートを通じてターゲットに到達できます。VMkernel ポートが 4 つ、ターゲット ポータルが 1 つ存在するため、合計 4 つのパスが作成されます。

ポートのバインドを使用しない場合、作成されるパスは 1 つのみです。

例 2：VMkernel ポートが異なるサブネットに属する場合のマルチパス

異なる IP サブネットに属する複数のポートとターゲット ポータルを設定することで、複数のパスを作成できます。イニシエータとターゲット ポートを異なるサブネットに分けておくと、特定のポートを経由するパスが ESXi により作成されます。ポートのバインドを設定するにはすべてのイニシエータとターゲット ポートが同じサブネットに属している必要があるため、この構成ではポートのバインドを使用しません。



3つのポートがすべて同じサブネットに属しているため、ESXiはコントローラAとコントローラBのポート0に接続する際にvmk1を選択します。同様に、コントローラAとコントローラBのポート1に接続する際にはvmk2が選択されます。この構成ではNICチーミングを使用できます。

合計4つのパスが作成されます。

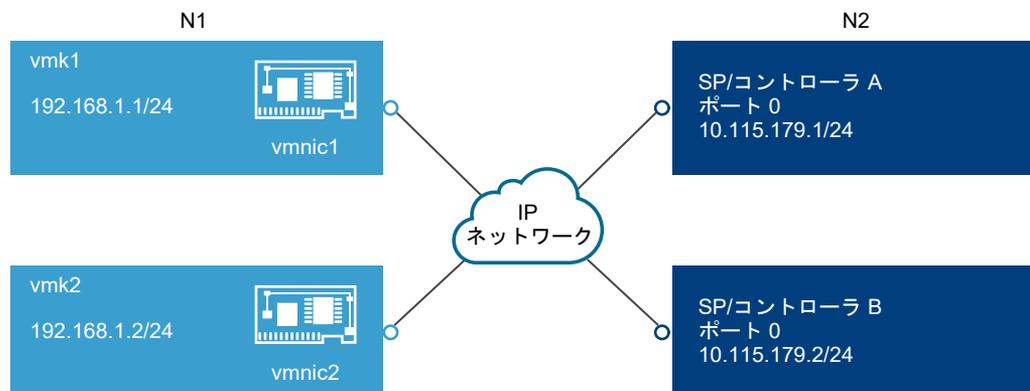
パス	説明
パス 1	vmk1 とコントローラ A のポート 0
パス 2	vmk1 とコントローラ B のポート 0
パス 3	vmk2 とコントローラ A のポート 1
パス 4	vmk2 とコントローラ B のポート 1

ソフトウェア iSCSI によるルーティング

iSCSI トラフィック用のスタティック ルートを追加するには、`esxcli` コマンドを使用します。スタティック ルートを設定すると、異なるサブネットに属すイニシエータとターゲット ポートの間で通信を行えるようになります。

例 1: ポートのバインドを使用する場合のスタティック ルートの使用例

この例では、バインドされるすべての vmkernel ポートを1つのサブネット (N1) に残し、すべてのターゲット ポータルを別のサブネット (N2) に設定します。その後、ターゲット サブネット (N2) のスタティック ルートを追加できます。

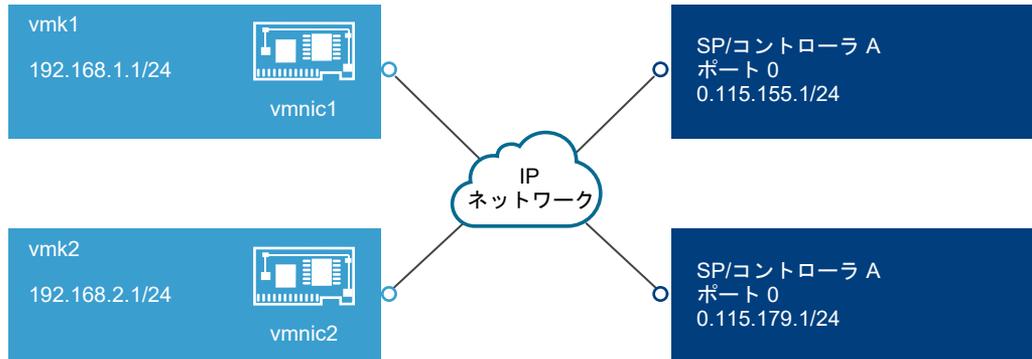


次のコマンドを使用します。

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.179.0/24
```

例 2：複数のバスを作成する場合のスタティック ルートの使用例

この構成では、異なるサブネットを使用するときにスタティック ルートを使用します。この構成では、ポートのバインドを使用できません。



vmk1 と vmk2 を別々のサブネット（192.168.1.0 と 192.168.2.0）に設定します。ターゲット ポータルも別々のサブネット（10.115.155.0 と 10.115.179.0）に属しています。

vmk1 から 10.115.155.0 のスタティック ルートを追加できます。vmk1 からゲートウェイに到達可能であることを確認してください。

```
# esxcli network ip route ipv4 add -gateway 192.168.1.253 -network
10.115.155.0/24
```

その後、vmk2 から 10.115.179.0 のスタティック ルートを追加できます。vmk2 からゲートウェイに到達可能であることを確認してください。

```
# esxcli network ip route ipv4 add -gateway 192.168.2.253 -network
10.115.179.0/24
```

コントローラ A のポート 0 に接続する際には vmk1 が使用されます。

コントローラ B のポート 0 に接続する際には vmk2 が使用されます。

例 3：vmkernel ポートごとに異なるゲートウェイを使用する場合のルーティング

vSphere 6.5 以降では、VMkernel ポートごとに異なるゲートウェイを設定できます。DHCP を使用して VMkernel ポートの IP アドレス設定を取得する場合は、DHCP を使用してゲートウェイ情報も取得できます。

VMkernel ポートごとのゲートウェイ情報を表示するには、次のコマンドを使用します。

```
# esxcli network ip interface ipv4 address list
```

Name	IPv4 Address	IPv4 Netmask	IPv4 Broadcast	Address Type	Gateway	DHCP	DNS
vmk0	10.115.155.122	255.255.252.0	10.115.155.255	DHCP	10.115.155.253	true	true
vmk1	10.115.179.209	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	true	true
vmk2	10.115.179.146	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	true	true

VMkernel ポートごとに異なるゲートウェイを使用する場合は、ポートのバインドを使用して異なるサブネットに属するターゲットに到達できます。

iSCSI ポートのバインドの設定

iSCSI ポートのバインドを設定すると、ソフトウェアまたは依存型ハードウェア iSCSI アダプタと物理ネットワークアダプタの間でトラフィックをやり取りするための接続が作成されます。

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。

iSCSI ポートのバインド設定では、VMware vSphere[®] Distributed Switch™ と VMware NSX[®] Virtual Switch™ も使用できます。NSX 仮想スイッチの詳細については、『VMware NSX』ドキュメントを参照してください。

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。分散スイッチの詳細については、『vSphere のネットワーク』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 の物理ネットワーク アダプタを 2 つ以上使用する場合に、このタスクを利用します。物理アダプタはすべて 1 台の vSphere Standard スイッチに接続する必要があります。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 台の 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、その構成のネットワーク ポリシーを設定します。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 ポリシーを設定してください。

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 Standard 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 の物理ネットワーク アダプタを 2 つ以上使用する場合に、このタスクを利用します。物理アダプタはすべて 1 台の vSphere Standard スイッチに接続する必要があります。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] タブをクリックします。
- 3 [ネットワーク] で、[仮想スイッチ] をクリックし、変更する vSphere スイッチをリストから選択します。
- 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 台の 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、その構成のネットワーク ポリシーを設定します。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 ポリシーを設定してください。

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] タブをクリックします。
- 3 [ネットワーク] で、[仮想スイッチ] をクリックし、変更する vSphere スイッチをリストから選択します。
- 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] を選択します。
- 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 [未使用のアダプタ] vmnic2
vmk2	[有効なアダプタ] vmnic2 [未使用のアダプタ] 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 ポリシーを設定してください。

必要な権限：ホスト.設定.ストレージ パーティション設定

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] アイコン (+) 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 アダプタは、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 VMkernel アダプタを 1 つのみ使用できます。

- 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] で、[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、[詳細の表示] アイコンをクリックします。
- 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 のネットワーク接続を作成した後、vSphere Web Client の iSCSI インジケータが有効になります。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にある iSCSI ポートを検出した場合でも、これらの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。これらのアダプタのいずれか、またはそれらを接続する vSphere スイッチを削除すると、関連付けを解除できます。または、それらの接続の 1 対 1 のネットワーク ポリシーを変更した場合も解除できます。

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 11-3. 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 でジャンボ フレームを有効にする

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 のネットワーク』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] タブをクリックします。
- 3 [ネットワーク] で、[仮想スイッチ] をクリックし、変更する vSphere スイッチをリストから選択します。
- 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 フレームを有効にする

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] で [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 では、最大 9,000 バイトの MTU サイズがサポートされます。

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] 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、[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。

検出方法	説明
動的検出	a [動的検出] をクリックし、[追加] をクリックします。 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。 c iSCSI アダプタを再スキャンします。 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。
静的検出	a [静的検出] をクリックし、[追加] をクリックします。 b ターゲットの情報を入力し、[OK] をクリックします。 c iSCSI アダプタを再スキャンします。

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] で、[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を確認します。また、システムがサポートする CHAP 認証方法についての情報を入手してください。CHAP が有効になっている場合、イニシエータ用に構成して、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。

一方方向 CHAP

一方方向の 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 認証は、セキュリティのレベルが強化されています。この認証方法では、イニシエータがターゲットを認証することもできます。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 11-4. 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。認証が有効になっている場合は、このオプションを使用して無効にしてください。	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
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
双方向 CHAP を使用する	ホストおよびターゲットは双方向 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、一方向 CHAP を構成するか、双方向 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、双方向 CHAP をサポートしません。
- ストレージ側で設定された CHAP パラメータを確認します。設定するパラメータは、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]
 - [ターゲットで要求された場合は一方向 CHAP を使用]
 - [ターゲットで禁止されていない場合は一方向 CHAP を使用]
 - [一方向 CHAP を使用]
 - [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。
- 4 送信 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、使用する送信 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。

送信 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 を構成するかを決定します。
- 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]
 - [ターゲットで要求された場合は一方向 CHAP を使用]
 - [ターゲットで禁止されていない場合は一方向 CHAP を使用]
 - [一方向 CHAP を使用]
 - [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 送信 CHAP 名を指定します。

指定する名前が、ストレージ側で設定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送信 CHAP シークレットを入力します。ストレージ側で入力したシークレットと同じもの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。
送信 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、ログアウトしてログインし直すまで、新しい設定は使用されません。

CHAP の無効化

ストレージ システムで CHAP が必要ない場合は、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 を無効にする場合は、既存の iSCSI セッションは、次のいずれかのアクションが実行されるまでアクティブなままになります。

- ホストを再起動します。
- コマンド ラインからセッションを終了します。
- ストレージ システムによって強制的にログアウトされます。

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 を無効にして一方 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 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 CHAP を無効にすると、相互 CHAP は [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 を使用して設定できる 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 サポートまたはストレージのベンダーの指示で iSCSI の詳細設定を変更する場合を除き、これらの設定は変更しないでください。

表 11-5. 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 パラメータが有効なときは、システムは iSCSI Protocol Data Unit (PDU) の各ヘッダ部分に対してチェックサムを実行します。システムは CRC32C アルゴリズムを使用してデータを確認します。	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。ヘッダ ダイジェスト パラメータが有効なときは、システムは各 PDU のデータ部分に対してチェックサムを実行します。システムは CRC32C アルゴリズムを使用してデータを確認します。 注： 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 ダイジェスト計算はオフロードされます。このオフロードによって、パフォーマンスに与える影響を低減できます。	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 バースト長	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
最大バースト長	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。iSCSI ターゲットは NOP-Out 要求に応じてメッセージを送信します。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
ARP リダイレクト	このパラメータを有効にすると、ストレージ システムは、ポート間で iSCSI トラフィックを動的に移動できます。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 パラメータが必要です。	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	このパラメータを有効にすると、ストレージ システムは受信データ パケットの確認を遅延できます。	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。この機能は、1 つのターゲット ポートのみをイニシエータに提示する、単一ポートのストレージ システムにホストが接続している場合に便利です。システムは、追加のセッションを別のターゲット ポートにリダイレクトします。iSCSI イニシエータと別のターゲット ポート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。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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
-A --adapter=str	たとえば、iSCSI アダプタ名は <code>vmhba34</code> です。
-s --isid=str	iSCSI セッションの識別子。
-n --name=str	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せん。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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
<code>-A --adapter=str</code>	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。
<code>-s --isid=str</code>	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。
<code>-n --name=str</code>	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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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
<code>-A --adapter=str</code>	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。
<code>-s --isid=str</code>	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。
<code>-n --name=str</code>	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 SAN からの起動

12

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 12-1. 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、 SAN 起動のための独立型ハードウェア iSCSI アダプタの構成 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、 iBFT iSCSI 起動の概要 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 ブートに関する一般的な推奨事項](#)
- [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 ブートに関する一般的な推奨事項

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を実行します。

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ます。

- VMFS データストアに LUN を使用する場合は、複数のホストが LUN を共有できます。
- 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 に配置できません。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に独立した LUN を使用する場合は、複数のホストが LUN を共有できます。
 - 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 Dump Collector 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 のネットワーク』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。

ストレージ ネットワークのあらゆるルーターまたはスイッチが適切に構成されていることを確認してください。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。

この手順には、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 ブートするようにアダプタを設定できます。

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ため、CD/DVD-ROM から起動するようにホストを設定します。

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 Crtl + q キーを押し、QLogic iSCSI HBA 設定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] の順に選択します。
 - b (オプション) 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 を設定します。
- 6 iSCSI 設定を構成します。
[iSCSI 起動の設定](#)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 起動の設定

iSCSI 起動パラメータを構成して ESXi ホストが iSCSI LUN から起動できるようにします。

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 [起動 LUN] パラメータと [iSCSI 名] パラメータを構成します。
 - ターゲット アドレスで1つの iSCSI ターゲットと1つの LUN しか利用できない場合は、[起動 LUN] と [iSCSI 名] は空のままにしてください。
ホストがターゲット ストレージ システムに到達すると、これらのテキスト ボックスに適切な情報が設定されます。
 - 複数の iSCSI ターゲットと LUN が利用できる場合は、[起動 LUN] と [iSCSI 名] の値を指定します。
 - 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。
HBA の自動再スキャンによって新しいターゲット LUN が検出されます。
- 5 iSCSI ターゲットを選択します。
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] キーを押すと、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] フィールドに値が設定されます。[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 および iSCSI SAN ブートをデプロイするには、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。このアダプタは、iSCSI Boot Firmware Table (iBFT) 形式 (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) をサポートする必要があります。

ESXi と iSCSI SAN ブートをインストールする前に、ネットワーク アダプタでネットワークと iSCSI 起動パラメータを設定します。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。

iSCSI からの起動をはじめて実行するときに、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 接続に成功した後は、iSCSI 起動ファームウェアはネットワークと iSCSI 起動パラメータを iBFT に書き込みます。ファームウェアは、システム メモリにそのテーブルを格納します。

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くない場合には、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 キーを押して 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 キーを押します。
- 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 キーを押して Boot Sequence メニューを終了します。
- 6 Esc キーを押して 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りません。
 - 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せん。

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、更新された起動設定を使用し、iSCSI ターゲットに接続して ESXi イメージをロードします。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 ホスト上の iSCSI とネットワーク パラメータを再設定し、iBFT のパラメータと一致させます。
- 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

13

ESXi を iSCSI SAN と使用する場合には、問題を回避するために VMware が提供する推奨事項を遵守してください。

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、ベンダーのドキュメントを参照して、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してください。詳細については、[24 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 の問題発生防止](#)
- [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 の問題発生防止

ESXi を SAN と併用する場合、SAN の問題を回避するためのガイドラインを遵守してください。

次の点に注意してください。

- 各 LUN には、VMFS データストアを 1 つのみ配置します。
- 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、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を記載します。
- 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。エレメントに障害が発生した場合の SAN への影響をエレメントごとに検討します。
 - 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確認します。
- 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。サーバで使用可能なバス間で、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、ストレージ ネットワークのさまざまな監視ポイントに精通しておきます。
- LUN ID の変更は、LUN にデプロイされている VMFS データストアで、いずれの仮想マシンも実行されていないときのみ行ってください。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。
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貫しており、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

ESXi ホストの最適なパフォーマンスを確保するために、いくつかの要因を考慮します。

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 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、次のガイドラインを実行します。

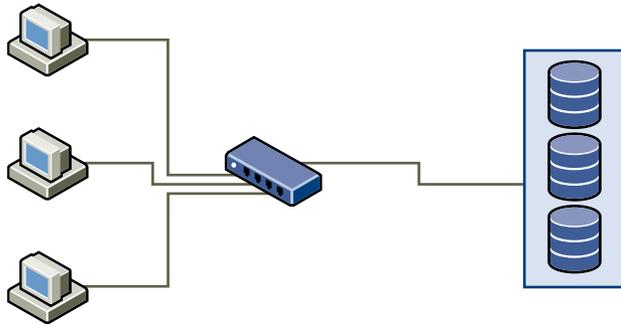
- 各 LUN を、必要なパフォーマンス レベルを提供する RAID グループに配置する。割り当てられた RAID グループにあるほかの LUN のアクティビティおよびリソースの使用を監視します。I/O を行うアプリケーションが多すぎる高性能 RAID グループは、ESXi ホストで実行されるアプリケーションで要求されるパフォーマンス目標を達成できないことがあります。
- ピーク期間中にホスト上のすべてのアプリケーションで最大のスループットを実現するために、十分なネットワーク アダプタまたは iSCSI ハードウェア アダプタをインストールします。I/O を複数のポートに分散させることで、それぞれのアプリケーションでスループットが向上し、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 アダプタにイニシエータ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、そのリソースが複数のオペレーティング システムで使用および共有されることを念頭に置く。ESXi ホストで必要になる LUN のパフォーマンスは、通常の物理マシンを使用する場合よりも大幅に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。
- vCenter Server で複数の ESXi システムを使用すると、ストレージ パフォーマンスの要件が増加する。
- 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 数と一致させる必要がある。

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。

次の図は、複数のコンピュータ システムがイーサネット スイッチ経由でストレージ システムに接続している状況を示しています。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います。このスイッチから 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。

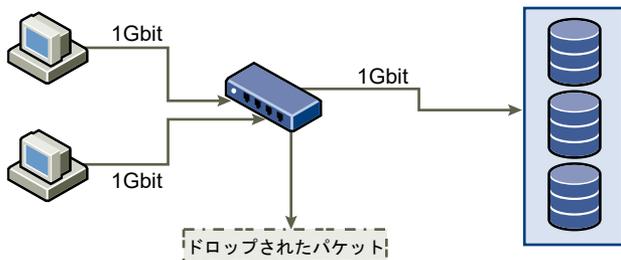
図 13-1. ストレージへの単一のイーサネット リンク



システムがストレージからデータを読み取る時、ストレージからのレスポンスでは、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を最大限に使うってデータが送信されます。1 台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ほとんどありません。しかし、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、次の状況が想定されます。

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します。これが原因で、システムとストレージ システムとの間にあるスイッチが、ネットワーク パケットをドロップする場合があります。通常、データのドロップが発生するのは、ストレージ システムに送信されるトラフィックが1つのリンクで転送できる容量を超えているためです。スイッチが送信できるデータ量は、その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ます。

図 13-2. ドロップされたパケット



ドロップされたネットワーク パケットのリカバリによって、パフォーマンスは著しく低下します。データがドロップされると判別する時間に加え、再送信するときに、次の処理に使う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 は信頼性の高い転送プロトコルで、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低下します。ネットワークの輻輳は、データ再送信リクエストや再送パケットなどによって発生します。輻輳のないネットワークと比べて、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 スイッチはデータをバッファに格納 (つまり一時保存) することができます。データの送信を試みるすべてのデバイスには、この手法により、宛先に到達する機会が均等に与えられます。この転送データの一部バッファできる点と、多くのシステムで未処理のコマンド数を制限しているため、トラフィックのバーストは小さくなります。複数のシステムで発生したバーストは、順番にストレージ システムに送信されます。

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、バッファ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が32KBまでバッファ可能な場合、サーバが256KBのデータ量をストレージデバイスに送信すると、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 13-1. 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

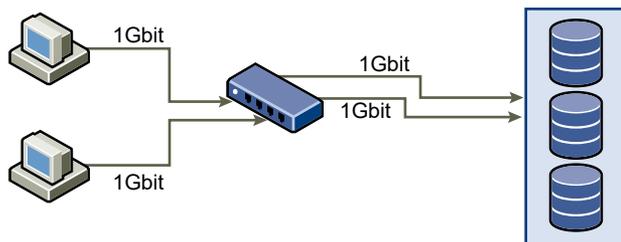
この Cisco のスイッチの例では、使用しているバンド幅が476,303,000ビット/秒で、ケーブル速度の半分未満です。ポートは受信パケットをバッファしますが、一部のパケットをドロップしています。このインターフェイスの最終行にある概要情報を見ると、IQD列で、このポートではすでに約10,000の受信パケットがドロップされているとわかります。

この問題を回避するには、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設定し、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。

一般に、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でください。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」では、スイッチからストレージへの複数接続を示しています。

図 13-3. 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 などのネットワークの仮想パーティショニングを利用すると、ネットワークを論理的に設計できます。ただし、スイッチ間のリンクやトランクの物理的な機能は変更されません。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物理接続を共有する場合、オーバーサブスクリプションや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有する 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

14

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
- ストレージの再スキャン操作
- デバイス接続問題の確認
- 構成ファイルのパラメータの編集
- 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 デバイスでの消去

ストレージ デバイスの特徴

ESXi ホストがブロックベースのストレージ システムに接続する場合、ESXi をサポートする LUN またはストレージ デバイスをホストで使用できるようになります。すべてのローカル デバイスおよびネットワーク デバイスを含み、すべてのストレージ デバイスを表示することができます。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 14-1. 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。
動作状態	デバイスが接続されているか、接続解除されているかを示します。詳細については、 ストレージ デバイスの分離 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）。

表 14-1. 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
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、 15 章 フラッシュ デバイスの操作 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。 物理ストレージのタイプ を参照してください。
容量	ストレージ デバイスのキャパシティの合計。
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、 複数のバスの管理 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、 24 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。
セクター フォーマット	デバイスで従来の 512n が使用されるか、512e などのアドバンスド セクター フォーマットが使用されるかを示します。詳細については、 ストレージ デバイス フォーマットと VMFS データストア 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。マスタ ブート レコード (MRB) または GUID パーティション テーブル (GPT) 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、 ストレージ デバイス フォーマットと VMFS データストア 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、 18 章 マルチバスとフェイルオーバー について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] テーブル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 アイコンを使用して基本的なストレージ管理タスクを行います。

実際に使用できるアイコンは、デバイスの種類と構成によって異なります。

アイコン	説明
	ストレージ アダプタ、トポロジ、ファイル システムについての情報を更新します。
	ホスト上のすべてのストレージ 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 デバイスや VMFS データストアを検出します。
	選択したデバイスをホストから切断します。
	選択したデバイスをホストに接続します。
	選択したデバイスの表示名を変更します。
	選択したデバイスのロケータ LED をオンにします。
	選択したデバイスのロケータ LED をオフにします。
	選択したデバイスをフラッシュ ディスクとしてマークします。
	選択したデバイスを HDD ディスクとしてマークします。

- 6 [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。デバイスのマルチパス 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] で、[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] テーブル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。
- 5 アイコンを使用して基本的なストレージ管理タスクを行います。
実際に使用できるアイコンは、デバイスの種類と構成によって異なります。

アイコン	説明
	ストレージ アダプタ、トポロジ、ファイル システムについての情報を更新します。
	ホスト上のすべてのストレージ 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 デバイスや VMFS データストアを検出します。
	選択したデバイスをホストから切断します。
	選択したデバイスをホストに接続します。
	選択したデバイスの表示名を変更します。
	選択したデバイスのロケータ LED をオンにします。
	選択したデバイスのロケータ LED をオフにします。
	選択したデバイスをフラッシュ ディスクとしてマークします。
	選択したデバイスを HDD ディスクとしてマークします。
	選択したデバイスをホストのローカルとしてマークします。
	選択したデバイスをホストのリモートとしてマークします。
	選択したデバイスのパーティションを消去します。

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、次のいずれかの形式で指定されています。

- `naa.number`
- `t10.number`
- `eui.number`

これらの形式は T10 技術委員会の規格に基づいています。T10 技術委員会の 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。

デバイスから 83 ページの情報が入手できない場合は、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 が識別する方法と同じように使用できます。

mpx. 識別子は、パス名が一意であることを前提に、ローカル デバイス向けに作成されます。ただし、この識別子は一意でも永続的でもないため、システムを再起動した後に毎回変わる可能性があります。

通常、デバイスへのパスの形式は次の通りです。

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示します。

- **TTarget** はターゲットの番号です。ターゲットの番号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、番号も変わることがあります。複数のホストが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 を介してアクセスするターゲット 3 上の LUN1 を表します。

レガシー識別子

ESXi は、SCSI INQUIRY または mpx. 識別子に加えて代替のレガシー名をデバイスごとに生成します。識別子の形式は次のとおりです。

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、その一部は 83 ページの情報から派生する可能性があります。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。出力例は次のとおりです。

```
# 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

ESXi ホストは、ストレージ タイプとメーカーに基づいて、ストレージ デバイスに表示名を割り当てています。デバイスのこの表示名は変更できます。

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 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。

ストレージの再スキャン操作

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、エクステントの追加、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、またはフォルダ、クラスタ、およびデータセンターのすべてのホスト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] で、[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 ホストのスキャンする LUN ID の範囲は、0 から 16,383 までです。ESXi は、16,383 より大きい LUN ID は無視します。設定可能な `Disk.MaxLUN` パラメータを使用して、スキャンされる LUN ID の範囲を管理します。パラメータのデフォルト値は 1024 です。

また、`Disk.MaxLUN` パラメータは、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、SCSI スキャン コードが個々の `INQUIRY` コマンドを使用して検出を試みる 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。たとえば使用している環境に、LUN ID が 1 から 100 の少数のストレージ デバイスがある場合は、値を 101 に設定します。その結果、`REPORT_LUNS` をサポートしていないターゲット上でデバイス検出スピードを上げることができます。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] テーブルで、[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、1～100 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 Permanent Device Loss (PDL) 状態とストレージの一時的な All Paths Down (APD) 状態は、ホストによって区別されます。

Permanent Device Loss (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せん。

All Paths Down (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。認識コードを受け取ると、ホストはデバイスを障害発生として認識し、デバイスの状態を PDL として登録します。デバイスが永続的に失われたと見なされるには、そのすべてのバスで認識コードを受信する必要があります。

デバイスの PDL 状態の登録後は、ホストは接続の再構築を停止し、デバイスへのコマンドの送信を停止します。

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。
- すべてのパスが Dead と表示されます。
- デバイス上のデータストアは使用できません。

デバイスへの開かれた接続がない場合、または最新の接続が閉じた後は、ホストは PDL デバイスと、デバイスに対するすべてのパスを削除します。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： 適切な SCSI 認識コードまたは iSCSI のログイン拒否を送信することなく、デバイスに障害が発生すると、ホストは PDL 状態を検出できません。この場合、デバイスに永続的な障害が発生した場合でも、ホストはデバイス接続の問題を APD として処理し続けます。

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 の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 アレイでは、iSCSI ログインの障害によって 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 Target Unavailable 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 状態の登録後は、ホストは仮想マシンからのすべての I/O を閉じます。vSphere HA は PDL を検出し、障害の発生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、Permanent Device Loss (PDL) または All Paths Down (APD) の状況を回避できます。ストレージ デバイスの予定される削除と再接続を実行します。

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。

タスク	説明
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 およびホストの管理
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。
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。
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。
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。	ベンダーのドキュメントを参照してください。
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。
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 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 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 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 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、次の作業を行います。

タスク	説明
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。	vSphere の仮想マシン管理 を参照してください。
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。
デバイスにアクセスしていたすべての ESXi ホストを再スキャンします。	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。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。たとえば仮想マシンやテンプレート、ISO イメージ、RAW デバイス マッピングが該当します。	

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 APD (All Path Down) 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、長期にわたって再試行に成功しない場合、ホストにパフォーマンスの問題が発生している可能性があります。ホストおよびその仮想マシンは、応答しなくなる可能性があります。

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、ホストはタイマーをオンにします。タイマーがオンの状態では、ホストは仮想マシン以外のコマンドの再試行を一定期間のみ続行します。

デフォルトで、APD タイムアウトは 140 秒に設定されます。通常この値は、ほとんどのデバイスが接続の切断から回復するために必要な時間を超えています。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。

後でデバイス パスが機能するようになったら、ホストはデバイスへの I/O を再開でき、特別な APD 処理を終了します。

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 All Paths Down (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] テーブルで、[Misc.APDHandlingEnable] パラメータを選択し、Edit 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、APD (All Paths Down) 状態の場合に、ESXi ホストがストレージ デバイスに対して I/O コマンドを再試行する秒数を制御します。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、すぐにタイムアウト期間が始まります。タイムアウトが終了すると、ホストは APD デバイスをアクセス不可としてマークします。ホストは、仮想マシンから発生していない I/O の再試行を停止し、仮想マシンの I/O の再試行を継続します。

デフォルトでは、ホストのタイムアウト パラメータは 140 秒に設定されています。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： デバイスが使用不可能になった後にタイムアウト パラメータを変更すると、その特定の APD インシデントに対して変更が適用されません。

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] テーブルで、[Misc.APDTimeout] パラメータを選択し、Edit 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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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 [Status:] 領域の接続状態を確認します。
 - 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 の可用性』ドキュメントを参照してください。

構成ファイルのパラメータの編集

VMware の技術サポート担当者による指示があった場合、あるいは システムの問題を修正するためにパラメータの追加または変更を指示する VMware の文章を参照した場合は、仮想マシンの構成パラメータの変更または追加を行うことができます。

重要： システムに問題がないときにパラメータを変更したり追加したりすると、システムのパフォーマンスが低下したり不安定な状態となる場合があります。

次の条件が適用されます。

- パラメータを変更するには、キーワードと値のペアの既存の値を変更します。たとえば、「`keyword/value`」というキーワードと値のペアを「`keyword/value2`」に変更すると、結果は「`keyword=value2`」になります。
- 構成パラメータのエントリを削除することはできません。

注意： 構成パラメータのキーワードに値を割り当てる必要があります。値を割り当てない場合、キーワードは `0`、`false`、または `disable` という値を返す可能性があるため、結果として仮想マシンをパワーオンできないことがあります。

手順

- 1 インベントリで仮想マシンを右クリックし、[設定の編集] を選択します。
- 2 [仮想マシン オプション] タブをクリックし、[詳細] を展開します。
- 3 [構成パラメータの編集] をクリックします。
- 4 (オプション) パラメータを追加するには、[行の追加] をクリックし、パラメータの名前と値を入力します。
- 5 (オプション) パラメータを変更するには、そのパラメータの [値] テキスト ボックスに新しい値を入力します。
- 6 [OK] をクリックします。

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。

ストレージ デバイスでの消去

vSAN や仮想フラッシュ リソースなどの一部の機能では、クリーンなデバイスを使用する必要があります。HHD またはフラッシュ デバイスで消去を行い、既存のデータをすべて削除できます。

前提条件

- ホストが接続状態にあることを確認します。
- 消去を行うデバイスが使用中でないことを確認します。
- 必要な権限 : Host.Config.Storage

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 1 つ以上のデバイスを選択して、[すべてのアクション] - [パーティションを消去] の順にクリックします。
単一のデバイスで消去を行う場合、パーティション情報のダイアログ ボックスが開きます。
- 5 単一のデバイスの場合は、消去するパーティション情報が重要でないことを確認します。
- 6 [OK] をクリックして変更を確定します。

フラッシュ デバイスの操作

15

通常のストレージ ハードディスク ドライブ (HDD) に加えて、ESXi 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。

可動部品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、可動部品がありません。通常、フラッシュ デバイスは回復力が高く、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。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、ストレージ アレイのメーカーにお問い合わせください。

ホストが検出したフラッシュ デバイスは、いくつかのタスクや機能で使用できます。

この章には、次のトピックが含まれています。

- [ESXi 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](#)

ESXi でのフラッシュ デバイスの使用

ESXi 環境では、いくつかの機能を持つフラッシュ デバイスを使用できます。

表 15-1. ESXi でのフラッシュ デバイスの使用

機能	説明
vSAN	vSAN には、フラッシュ デバイスが必要です。詳細については、『VMware vSAN 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	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。 <ul style="list-style-type: none"> ■ 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。 フラッシュ仮想ディスクの特定を参照してください。 ■ ESXi ホスト スワップ キャッシュ用のデータストア容量を割り当てます。 ホスト スワップ キャッシュの構成を参照してください。
仮想フラッシュ リソース (VFFS)	仮想フラッシュ リソースを設定し、次の機能で使用します。 <ul style="list-style-type: none"> ■ 仮想マシンで、仮想 Flash Read Cache を使用します。 16 章 VMware vSphere Flash Read Cache についてを参照してください。 ■ 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。この方法は、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 キャッシュ設定の代替方法です。 仮想フラッシュ リソースを使用したホスト スワップ キャッシュの構成を参照してください。 ■ 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 リソースを使用します。 23 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。

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。

vSAN の構成や仮想フラッシュ リソースの設定を行う場合は、ストレージ環境にローカル フラッシュ デバイスを含める必要があります。

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。その他の場合では、特定のデバイスがローカルとして検出されない場合があります。ESXi はこれらのデバイスをリモートとしてマークします。ローカル フラッシュ デバイスとして認識されない場合、デバイスは、vSAN 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、vSAN 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 デバイスをフラッシュとしてマークすると、それらのデバイス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。それらのデバイスがフラッシュ デバイスであることが確実な場合にのみ、デバイスをフラッシュ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 [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 デバイスの一覧から、フラッシュ デバイスとしてマークする HDD デバイスを 1 つ以上選択し、[フラッシュ ディスクとしてマーク] (F) 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。

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。この操作は、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 [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、1 つ以上のリモート デバイスを選択してローカルとしてマークし、[すべてのアクション] アイコンをクリックします。
- 5 [ローカルとしてマーク] をクリックし、[はい] をクリックして変更内容を保存します。

フラッシュ デバイスの監視

Media Wearout Indicator、Temperature、Reallocated Sector Count などの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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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、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.aaaaaaaaaaaaaaaa
Device: t10.aaaaaaaaaaaaaaaa
Successful Commands: xxxxxxxx
Blocks Read: xxxxxxxx
Blocks Written: 629145600
Read Operations: xxxxxxxx
```

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。

$$\text{ベンダーから提供された 1 日あたりの書き込み数} \times \text{ベンダーから提供された耐用年数} \div \text{1 日あたりの実際} \\ \text{の書き込み平均数}$$

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。16 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)。23 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使用する仮想フラッシュ リソースを設定する場合には、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 vSAN 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 リソースの合計使用可能容量は、ホスト スワップ キャッシュとして ESXi ホストが使用でき、読み取りキャッシュとして仮想マシンが使用できます。
- スワップ キャッシュ用または読み取りキャッシュ用に個別のフラッシュ 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する必要があります。仮想フラッシュ リソースを vSAN 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 [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 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 の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。

前提条件

- 仮想フラッシュ リソースがホスト スワップ キャッシュで構成されていないことを確認します。

- Flash Read Cache で構成された仮想マシンが、ホスト上でパワーオン状態でないことを確認します。

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 [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 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 リソースの詳細パラメータを変更できます。

手順

- 1 vSphere Web Client で、ホストに移動します。
- 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 変更する設定を選択して、[編集] ボタンをクリックします。

パラメータ	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、Host vFlash resource usage アラームがトリガされます。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遅延ディスク上のファイルから構成されます。ホストで実行されているすべての仮想マシンがキャッシュを共有します。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 デバイス容量を有効活用します。

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 キャッシュの容量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容量を確保します。
- 仮想フラッシュ リソースを設定するための 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

ESXi ホストがホスト キャッシュにスワップできるようにします。ホスト キャッシュに割り当てられる容量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 [ストレージ] で [ホスト キャッシュの設定] をクリックします。
- 4 フラッシュ 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容量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

16

Flash Read Cache™ は、ホスト常駐型のフラッシュ デバイスをキャッシュとして使用して仮想マシン パフォーマンスを高速化できます。

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ます。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、キャッシュを移行できます。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。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 などのバッキング ストレージにディスパッチされます。バッキング ストレージから読み取り、またはバッキング 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のために Flash Read Cache を設定すると、I/O リソースが共有ストレージでさらに使用できるようになります。その結果、Flash Read Cache を使用するように設定されていないワークロードのパフォーマンスも向上する可能性があります。

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 Flash Read Cache のサポート

- 仮想マシンの Flash Read Cache の設定
- 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 Flash Read Cache のサポート

HA (High Availability) では、Flash Read Cache がサポートされています。

Flash Read Cache が備わっている仮想マシンが vSphere HA によって再起動されるときは、Flash Read Cache、CPU、メモリ、オーバーヘッド予約が適合したターゲット ホスト上の仮想マシンが再起動されます。予約されていないフラッシュが仮想フラッシュ予約を満たしていない場合、仮想マシンは再起動されません。利用できる仮想フラッシュ リソースがターゲット ホストに十分存在しない場合は、仮想マシンを再構成して Flash Read Cache を減らすかドロップしてください。

仮想マシンの Flash Read Cache の設定

仮想マシンには Flash Read Cache を設定できます。

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』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。

手順

- 1 仮想マシンへ移動します。

- 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] タブで、[ハード ディスク] を展開してディスク メニュー項目を表示します。
- 4 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。
- 5 [詳細] をクリックして次のパラメータを指定します。

パラメータ	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。

- 6 [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。
 - a [[詳細]] をクリックします。
 - b 移行設定を変更する仮想ディスクを選択します。
 - c [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。

この章には、次のトピックが含まれています。

- データストアのタイプ
- 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 データストアのキャパシティの拡張
- 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

データストアのタイプ

使用するストレージに応じて、使用できるデータストアのタイプは異なります。

vCenter Server および ESXi は、次のタイプのデータストアをサポートします。

表 17-1. データストアのタイプ

データストア タイプ	説明
VMFS (バージョン 3、5、および 6)	ブロック ストレージ デバイスでデプロイするデータストアは、vSphere 仮想マシン ファイル システム (VMFS) フォーマットを使用します。VMFS は、仮想マシンを格納するために最適化された、専用の高性能ファイル システム フォーマットです。 VMFS データストアについて を参照してください。
NFS (バージョン 3 および 4.1)	ESXi に組み込まれた NFS クライアントは、TCP/IP 接続経路で、ネットワーク ファイル システム (NFS) プロトコルを使用して、指定された NFS ボリュームにアクセスします。ボリュームは、NAS サーバに配置されます。ESXi ホストは、ボリュームを NFS データストアとしてマウントし、ストレージのニーズに応じて使用します。ESXi は、バージョン 3 および 4.1 の NFS プロトコルをサポートします。 ネットワーク ファイル システム データストアについて を参照してください。
vSAN	vSAN は、ホストで使用可能なすべてのローカル キャパシティ デバイスを、vSAN クラスタのすべてのホストが共有する単一のデータストアに集約します。『VMware vSAN の管理』ドキュメントを参照してください。
Virtual Volumes	Virtual Volumes データストアは、vCenter Server および vSphere Web Client 内のストレージ コンテナを表します。 22 章 Virtual Volumes の操作 を参照してください。

vSphere Web Client を使用して、特定のタイプのデータストアを作成できます。データストアで管理操作を実行することもできます。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複数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。データストアをグループ化したら、グループのデータストアに同じ権限と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、ストレージ 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 のリソース管理』ドキュメントを参照してください。

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。データストアは、仮想マシンから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する論理コンテナです。ブロック ストレージ デバイスでデプロイするデータストアは、ネイティブ vSphere 仮想マシン ファイル システム (VMFS) フォーマットを使用します。VMFS フォーマットは、仮想マシンの格納に最適化された専用の高性能ファイル システム フォーマットです。

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 デバイス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。

仮想マシンがデータストア上で実行されている間に、データストアのキャパシティを拡張できます。この機能によって、仮想マシンが新しい容量を要求するたびに、VMFS データストアにその容量を追加できます。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。

VMFS データストアのバージョン

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。ESXi は VMFS3、VMFS5、および VMFS6 をサポートしています。

すべての VMFS バージョンで、ESXi は読み取りおよび書き込みを完全にサポートします。VMFS のすべてのバージョンで、仮想マシンを作成してパワーオンできます。

表 17-2. ホスト アクセスと VMFS のバージョン

VMFS	ESXi
VMFS 6	読み取りおよび書き込み
VMFS5	読み取りおよび書き込み
VMFS3	読み取りおよび書き込み

注： 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、仮想マシンを VMFS6 データストアに移行します。

次の表では、VMFS5 と VMFS6 の主な特性を比較しています。詳細については、「構成の上限」を参照してください。

表 17-3. VMFS5 と VMFS6 の比較

機能	VMFS5	VMFS 6
ESXi 6.5 ホストへのアクセス	はい	はい
バージョン 6.0 以前の ESXi ホストへのアクセス	はい	いいえ
ホストあたりのデータストア	512	512
512n ストレージ デバイス	可 (デフォルト)	はい
512e ストレージ デバイス	可。ローカル 512e デバイスではサポートされません。	可 (デフォルト)
容量の自動再利用	いいえ	はい
esxcli コマンドを使用した手動による容量再利用。蓄積されたストレージ容量の手動による再利用を参照してください。	はい	はい
ゲスト OS からの容量の再利用	制限あり	はい
GPT ストレージ デバイスのパーティショニング	はい	はい

表 17-3. VMFS5 と VMFS6 の比較 (続き)

機能	VMFS5	VMFS 6
MBR ストレージ デバイスのパーティショニング	はい 以前に VMFS3 からアップグレードした VMFS5 データストア向け。	いいえ
各 VMFS エクステンツにつき 2 TB を超えるストレージ デバイス	はい	はい
大容量の仮想ディスク、または 2 TB を超えるディスクを持つ仮想マシンのサポート	はい	はい
1 KB の小さなファイルのサポート	はい	はい
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。VMFS のロック メカニズムを参照してください。	はい	はい
ブロック サイズ	標準の 1 MB	標準の 1 MB
デフォルトのスナップショット	2 TB より小さい仮想ディスクの場合は VMFSsparse。 2 TB より大きい仮想ディスクの場合は SEsparse。	SEsparse
仮想ディスクのエミュレーションのタイプ	512n	512n
vMotion	はい	はい
異なるデータストア タイプ間の Storage vMotion	はい	はい
High Availability および Fault Tolerance	はい	はい
DRS および Storage DRS	はい	はい
RDM	はい	はい

VMFS5 データストアおよび VMFS6 データストアを使用するときは、次の点に注意してください。

- アップグレード。ESXi ホストをバージョン 6.5 にアップグレードした後でも、既存の VMFS5 データストアを使用し続けることができます。VMFS6 の機能を活用するには、VMFS6 データストアを作成し、仮想マシンを VMFS5 データストアから VMFS6 データストアに移行します。VMFS5 データストアを VMFS6 にアップグレードすることはできません。
- データストア エクステンツ。複数にまたがる VMFS データストアでは、同種のストレージ デバイスである 512n または 512e のみを使用する必要があります。複数にまたがるデータストアは、異なる形式のデバイスに拡張できません。
- ブロック サイズ。VMFS データストアのブロック サイズにより、最大ファイル サイズとファイルが占める容量が定義されます。VMFS5 データストアと VMFS6 データストアは、1 MB のブロック サイズをサポートしています。

- Storage vMotion。Storage vMotion は、VMFS データストア、vSAN データストア、Virtual Volumes データストア間の移行をサポートしています。vCenter Server は互換性チェックを実行し、異なるタイプのデータストア間の Storage vMotion を検証します。
- ストレージ DRS:VMFS5 と VMFS6 は、同じデータストア クラスタに共存できます。ただし、クラスタ内のすべてのデータストアでは、同種のストレージ デバイスである 512n または 512e のいずれかを使用する必要があります。同じデータストア クラスタ内で異なる形式のデバイスを混在させないでください。

ストレージ デバイス フォーマットと VMFS データストア

512n および 512e ストレージ デバイスに VMFS データストアをデプロイできます。新しい VMFS データストアを設定するときは、GPT を使用してデバイスのフォーマットが行われます。場合によっては、VMFS は MBR フォーマットをサポートできます。

デバイス セクター フォーマットと VMFS バージョン

ESXi は、従来のセクター フォーマットとアドバンスド セクター フォーマットを使用するストレージ デバイスをサポートします。

ストレージ内のセクターは、ストレージ ディスクまたはデバイスのトラックを細分化したものです。各セクターには、固定量のデータが格納されます。従来の 512n ストレージ デバイスは、512 バイトのネイティブ セクター サイズを使用してきました。それに加え、より大きいキャパシティに対する要望が増えてきたため、ストレージ業界は 512 バイト エミュレーション (512e) などのアドバンスド フォーマットを導入しました。512e は、物理セクター サイズが 4,096 バイトであるが、論理セクター サイズが 512 バイトのセクター サイズをエミュレートする、アドバンスド フォーマットです。512e フォーマットを使用するストレージ デバイスは、レガシー アプリケーションとゲスト OS をサポートできます。

512e ストレージ デバイスでデータストアを設定すると、VMFS6 がデフォルトで選択されます。512n ストレージ デバイスの場合、デフォルトのオプションは VMFS5 ですが、VMFS6 を選択することもできます。

次の表は、ネイティブの 512 バイト ストレージ デバイスとアドバンスド 512e フォーマットを使用するデバイスを比較したものです。

ストレージ デバイスのフォーマット	論理セクター サイズ	物理セクター サイズ	VMFS データストア
512n	512	512	VMFS5 (デフォルト) と VMFS6
512e	512	4,096	VMFS6 (デフォルト) と VMFS5

注： ローカルの 512e ストレージ デバイスは VMFS5 をサポートしません。

デバイス パーティションのフォーマットと VMFS バージョン

新しい VMFS5 または VMFS6 データストアは、GUID パーティション テーブル (GPT) を使用して、ストレージ デバイスのフォーマットを行います。GPT フォーマットを使用すると、2 TB より大きいデータストアを作成できます。VMFS5 データストアは、以前に VMFS3 からアップグレードされている場合、VMFS3 の特徴であるマスター ブート レコード (MBR) パーティション フォーマットを続けて使用します。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。

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。

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維持されます。

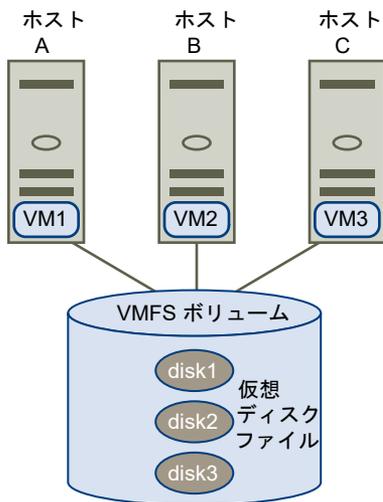
複数の仮想マシンを実行するときは、VMFS が仮想マシン ファイルの特定のロック メカニズムを提供します。その結果、仮想マシンは、複数の ESXi ホストが同じ VMFS データストアを共有する SAN 環境で安全に動作できます。

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 17-1. 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 のリソース管理』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 の可用性』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 およびホストの管理』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、拡張、ロック
- ファイルの属性の変更
- 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。

設定と基盤となるストレージのタイプに応じて、VMFS データストアはさまざまなタイプのロック メカニズムを使用できます。VMFS は独占的にアトミック テストを使用して、ロック メカニズム (ATS のみ) を設定できます。あるいは ATS 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。基盤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 および VMFS6 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 エクステント 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 または VMFS6 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 または VMFS6 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 の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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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 17-4. 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-only	データストアは ATS のみのロック モード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 モードを使用するように構成されています。ATS に障害が発生するか、ATS がサポートされていない場合は、データストアを SCSI に戻すことができます。
	ATS upgrade pending	データストアは、ATS のみのモードへのオンライン アップグレードを進行中です。
	ATS downgrade pending	データストアは、ATS+SCSI モードへのオンライン ダウングレードを進行中です。
ATS 互換		データストアは、ATS のみのモード用に構成できるかできないかを示します。
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。
	None	データストアは ATS のみとの互換性がありません。
	Online	ATS のみのモードへのアップデート中にデータストアを使用できます。
	Offline	ATS のみのモードへのアップデート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、この項目は非互換の理由を示します。

ATS のみへの VMFS ロックの変更

VMFS 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、以前に 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 メカニズムを継続して使用します。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、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 アップグレードのメカニズムは、ほとんどの単一のエクステンツ 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 のみのロック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 ATS のみのタイプへのロック メカニズムのアップグレード

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 のみのロック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。

次のサンプル出力は、データストアがアップグレード対象であることを示します。現在のロック メカニズムと、データストアに対して使用できるアップグレード モードも示します。

Locking Mode	ATS Compatible	ATS Upgrade Modes
ATS+SCSI	true	Online or Offline

- 3 データストアで使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。

ATS のみのタイプへのロック メカニズムのアップグレード

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。

複数のエクステント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 メカニズムを使用します。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などに、ATS+SCSI ロック メカニズムへの切り替えが必要になる場合があります。または、ファームウェアのアップデートが失敗して、デバイスで ATS がサポートされなくなった場合も想定されます。

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。

VMFS でのスナップショットのフォーマット

スナップショットの作成時、仮想ディスクの状態は維持されます。これにより、ゲスト OS による書き込みが阻止され、差分ディスクまたは子ディスクが作成されます。差分ディスクは、仮想ディスクの現在の状態と、以前スナップショットを作成したときの状態の違いを示します。VMFS データストアでは、差分ディスクはスパース ディスクです。

スパース ディスクは、書き込み操作を使用してデータがコピーされるまでは、コピーオンライト メカニズム（仮想ディスクにデータを保存しない）を使用します。これにより、ストレージ容量を節約できます。

データストアのタイプによって、差分ディスクは異なるスパース フォーマットを使用します。

VMFSsparse

VMFS5 は 2 TB より小さい仮想ディスクに VMFSsparse フォーマットを使用します。

VMFSsparse は VMFS の上に実装されます。VMFSsparse レイヤーでは、スナップショット仮想マシンに発行された I/O を処理します。技術的には、VMFSsparse は仮想マシンのスナップショットが作成された直後に作成される空の REDO ログです。この REDO ログは、仮想マシンのスナップショット作成後に vmdk 全体が新しいデータで再書き込みされると、その基本 vmdk のサイズまで拡張します。この REDO ログは、VMFS データストア内のファイルです。スナップショット作成時に、仮想マシンに接続された基本 vmdk は新規作成されたスパース vmdk に変更されます。

SEsparse

SEsparse は、VMFS6 データストアのすべての差分ディスクのデフォルト フォーマットです。VMFS5 では、SEsparse は 2 TB 以上のサイズの仮想ディスクに使用されます。

SEsparse は VMFSsparse に似たフォーマットで、いくつかの機能が強化されています。このフォーマットは容量効率が高く、容量の再利用をサポートしています。容量の再利用により、ゲスト OS が削除するブロックがマークされます。システムは、ハイパーバイザーの SEsparse レイヤーにコマンドを送信して、それらのブロックのマッピングを解除します。このマッピング解除により、SEsparse によって割り当てられた容量のデータがゲスト OS によって削除された後で、その容量を再利用できるようになります。容量の再利用の詳細については、[ストレージ容量の再利用](#)を参照してください。

スナップショットの移行

スナップショットを持つ仮想マシンは異なるデータストア間で移行できます。次の考慮事項が適用されます。

- VMFSsparse スナップショットを持つ仮想マシンを VMFS6 に移行する場合、スナップショットのフォーマットが SEsparse に変更される。
- vmdk のサイズが 2 TB より小さい仮想マシンを VMFS5 に移行すると、スナップショットのフォーマットが VMFSsparse に変更される。
- VMFSsparse の REDO ログと SEsparse の REDO ログを同じ階層で混在させることはできない。

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、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 ポリ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。VMFS などのローカル ファイル システムで NFS ポリリュームをフォーマットする必要はありません。代わりに、ポリリュームを 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します。

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、仮想マシンの CD-ROM デバイスをデータストア上の ISO ファイルに接続できます。次に、その ISO ファイルからゲスト OS をインストールできます。

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。ESXi は、両方のバージョンをサポートするために、2 つの異なる NFS クライアントを使用します。

NFS クライアントのバージョンの比較

次の表に、NFS バージョン 3 および 4.1 でサポートされる機能を示します。

特性	NFS バージョン 3	NFS バージョン 4.1
セキュリティ メカニズム	AUTH_SYS	AUTH_SYS および Kerberos (krb5 および krb5i)
Kerberos による暗号化アルゴリズム	該当なし	AES256-CTS-HMAC-SHA1-96 および AES128-CTS-HMAC-SHA1-96
マルチパス機能	サポート対象外	セッション トランクを使用してサポート
ロック メカニズム	専用のクライアント側ロック	サーバ側ロック
ハードウェア アクセラレーション	サポート	サポート
シック仮想ディスク	サポート	サポート
IPv6	サポート	AUTH_SYS および Kerberos の場合にサポート
仮想マシンに CD-ROM として表示される ISO イメージ	サポート	サポート
仮想マシンのスナップショット	サポート	サポート
仮想ディスクが 2 TB を超える仮想マシン	サポート	サポート

NFS プロトコルと vSphere ソリューション

次の表に、NFS バージョンでサポートされる主要な vSphere ソリューションを示します。

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
Storage DRS	はい	いいえ
Storage I/O Control	はい	いいえ
Site Recovery Manager	はい	いいえ
Virtual Volumes	はい	はい
vSphere Replication	はい	はい
vRealize Operations Manager	はい	はい

NFS 4.1 と Fault Tolerance

NFS v4.1 上の仮想マシンは、vSphere 6.0 で導入された新しい Fault Tolerance のメカニズムをサポートしません。

NFS v4.1 上の仮想マシンは、古いレガシー Fault Tolerance のメカニズムをサポートしていません。

vSphere 6.0 では、Fault Tolerance メカニズムは最大で 4 つの vCPU を持つ対称型マルチプロセッサ (SMP) 仮想マシンに対応できます。vSphere の以前のバージョンは、異なる要件や特性で Fault Tolerance のためにさまざまなテクノロジーを使用していました。

NFS アップグレード

ESXi をバージョン 6.5 にアップグレードすると、既存の NFS 4.1 データストアは、以前の ESXi リリースで利用できなかった機能のサポートを自動的に開始します。このような機能には、Virtual Volumes、ハードウェア アクセラレーションなどがあります。

ESXi 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。

- 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します。
- 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。

- NFS 3 データストアをアンマウントしてから、NFS 4.1 データストア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 ストレージのガイドラインと要件

NFS ストレージを使用する場合は、NFS サーバの設定、ネットワーク、NFS データストアなどに関連する個別のガイドラインに従ってください。

■ NFS サーバの構成

ESXi と連携するように NFS サーバを構成する場合は、ストレージ ベンダーの推奨に従ってください。これらの一般的な推奨事項に加えて、vSphere 環境の NFS に適用される個別のガイドラインを使用してください。

■ NFS のネットワーク

ESXi ホストは、TCP/IP ネットワーク接続を使用してリモート NAS サーバにアクセスします。一部のガイドラインおよびベスト プラクティスは、NFS ストレージを使用する場合にネットワークを設定するためのものです。

■ NFS のファイル ロック

ファイル ロック メカニズムは、サーバに保存されたデータへのアクセスを一度に 1 人のユーザーまたは 1 つのプロセスに制限するために使用されます。NFS 3 と NFS 4.1 で使用しているファイル ロック メカニズムには互換性がありません。

■ NFS のセキュリティ

NFS 3 および NFS 4.1 と組み合わせることで、ESXi は AUTH_SYS セキュリティをサポートします。さらに、NFS 4.1 では、Kerberos セキュリティ メカニズムがサポートされます。

■ NFS のマルチパス

NFS 3 と ESXi の組み合わせではマルチパスはサポートされませんが、NFS 4.1 は複数のパスをサポートしています。

■ NFS とハードウェア アクセラレーション

NFS データストアで作成された仮想ディスクは、デフォルトでシンプロビジョニングです。シックプロビジョニングの仮想ディスクを作成するには、容量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する必要があります。

■ NFS データストア

NFS データストアを作成する際は、必ずいくつかのガイドラインに従ってください。

NFS サーバの構成

ESXi と連携するように NFS サーバを構成する場合は、ストレージ ベンダーの推奨に従ってください。これらの一般的な推奨事項に加えて、vSphere 環境の NFS に適用される個別のガイドラインを使用してください。

ガイドラインには、以下の項目が含まれます。

- 使用する NAS 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 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。
- NAS 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ことを確認します。NAS サーバが、同じ共有に両方のプロトコル バージョンを提供することはできません。ESXi では異なる NFS バージョン間でも同じ共有がマウントされるため、NAS サーバはこのポリシーを強制する必要があります。
- NFS 3 および非 Kerberos (AUTH_SYS) 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。ストレージベンダーによって、この機能を有効にするために使用する方式が異なりますが、通常、NAS サーバでは `no_root_squash` オプションが使用されます。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、そのデータストアで仮想マシンを作成することはできません。
- 基盤となる NFS ボリュームが読み取り専用の場合、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ることを確認します。または、ボリュームを読み取り専用のデータストアとして ESXi ホストにマウントします。それ以外の場合、ホストはデータストアを読み取り/書き込み可能と認識し、ファイルを開かない場合があります。

NFS のネットワーク

ESXi ホストは、TCP/IP ネットワーク接続を使用してリモート NAS サーバにアクセスします。一部のガイドラインおよびベスト プラクティスは、NFS ストレージを使用する場合にネットワークを設定するためのものです。

詳細については、『vSphere のネットワーク』ドキュメントを参照してください。

- ネットワーク接続については、ESXi ホストで標準的なネットワーク アダプタを使用します。
- 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 ストレージの VMkernel ポート グループを設定します。既存の仮想スイッチ (vSwitch) または新規の vSwitch で、IP ストレージの VMkernel ポート グループを作成できます。vSwitch は、vSphere Standard 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。
- NFS 3 と NFS 4.1 は IPv6 をサポートしています。

NFS のファイル ロック

ファイル ロック メカニズムは、サーバに保存されたデータへのアクセスを一度に 1 人のユーザーまたは 1 つのプロセスに制限するために使用されます。NFS 3 と NFS 4.1 で使用しているファイル ロック メカニズムには互換性はありません。

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 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 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 プロトコルは異なるため、異なる NFS バージョンを使用して複数のホストに同じデータストアをマウントすることはできません。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 のセキュリティ

NFS 3 および NFS 4.1 と組み合わせることで、ESXi は AUTH_SYS セキュリティをサポートします。さらに、NFS 4.1 では、Kerberos セキュリティ メカニズムがサポートされます。

NFS 3 は AUTH_SYS セキュリティ メカニズムをサポートしています。このメカニズムを使用すると、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 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。Kerberos を使用すると、root 以外のユーザーがファイルにアクセスできます。詳細については、[NFS 4.1 用 Kerberos の使用](#)を参照してください。

Kerberos に加えて、NFS 4.1 では AUTH_SYS セキュリティを使用した従来の Kerberos 以外のマウントをサポートしています。この場合は、NFS バージョン 3 の root アクセス権のガイドラインを使用してください。

注： 複数のホストで共有される 1 つの NFS 4.1 データストアには、2 つのセキュリティ メカニズム (AUTH_SYS と Kerberos) を使用できません。

NFS のマルチパス

NFS 3 と ESXi の組み合わせではマルチパスはサポートされませんが、NFS 4.1 は複数のパスをサポートしています。

NFS 3 では、I/O で 1 つの TCP 接続を使用します。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で別々のネットワーク接続を使用する必要があります。

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 とハードウェア アクセラレーション

NFS データストアで作成された仮想ディスクは、デフォルトでシンプロビジョニングです。シックプロビジョニングの仮想ディスクを作成するには、容量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する必要があります。

NFS 3 および NFS 4.1 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。

NFS データストア

NFS データストアを作成する際は、必ずいくつかのガイドラインに従ってください。

NFS データストアのガイドラインおよびベスト プラクティスには、以下の項目が含まれます。

- 異なる NFS バージョンを使用して、異なるホストに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 クライアントは互換性がなく、使用しているロック プロトコルが異なります。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。
- ESXi は自動的に NFS バージョン 3 をバージョン 4.1 にアップグレードすることはできませんが、ほかの変換方式は使用できます。詳細については、[NFS プロトコルと ESXi](#) を参照してください。
- 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 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と、ポートおよびプロトコルとの関係が含まれています。

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。

ファイアウォール構成の詳細については、『vSphere のセキュリティ』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もあります。

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 [設定] タブをクリックします。
- 3 [システム] で、[セキュリティ プロファイル] をクリックし、[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 ルーターで Cisco のホット スタンバイ ルーター プロトコル (HSRP) を使用してください。Cisco 以外のルーターを使用している場合は、代わりに仮想ルーター冗長プロトコル (VRRP) を使用します。
- バンド幅が制限されているネットワークや、輻輳が発生しているネットワークで NFS L3 トラフィックを優先するには、Quality of Service (QoS) を使用します。詳細については、お使いのルーター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提供されるルート設定された NFS L3 の推奨事項を実行します。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。
- 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 4.1 用 Kerberos 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。

RPCSEC_GSS Kerberos メカニズムは認証サービスです。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 セキュリティでは、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。

ESXi の NFS 4.1 用の Kerberos 実装には、krb5 と krb5i の 2 つのセキュリティモデルがあり、それぞれが異なるセキュリティレベルを提供します。

- 認証のみの Kerberos (krb5) では ID 検証がサポートされます。
- 認証とデータ整合性用の Kerberos (krb5i) では、ID 検証に加えて、データの整合性サービスも提供されます。これらのサービスを使用すると、データパケットが改変されている可能性がないかがチェックされ、NFS トラフィックの改ざん保護に役立ちます。

Kerberos は暗号化アルゴリズムをサポートし、認証されていないユーザーによる NFS トラフィックへのアクセスを防止します。ESXi の NFS 4.1 クライアントは、NAS サーバ上の共有へのアクセスに、AES256-CTS-HMAC-SHA1-96 または AES128-CTS-HMAC-SHA1-96 アルゴリズムの使用を試みます。NFS 4.1 データストアを使用する前に、NAS サーバで AES256-CTS-HMAC-SHA1-96 または AES128-CTS-HMAC-SHA1-96 が有効にされていることを確認します。

次の表に、ESXi がサポートする Kerberos セキュリティ レベルの比較を示します。

表 17-5. Kerberos セキュリティのタイプ

		ESXi 6.0	ESXi 6.5
認証のみの Kerberos (krb5)	RPC ヘッダーの整合性チェックサム	あり (DES)	あり (AES)
	RPC データの統合チェックサム	なし	なし
認証とデータ整合性用 Kerberos (krb5i)	RPC ヘッダーの整合性チェックサム	なし (krb5i)	あり (AES)
	RPC データの統合チェックサム		あり (AES)

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 ドメインで Kerberos 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 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。割り当てプロセスを自動化するには、ホスト プロファイル内にユーザーを設定し、そのプロファイルをすべての ESXi ホストに適用します。
- 複数のホストで共有される 1 つの NFS 4.1 データストアには、2 つのセキュリティ メカニズム (AUTH_SYS と Kerberos) を使用できません。

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。
- Kerberos を使用する場合は、AES256-CTS-HMAC-SHA1-96 または AES128-CTS-HMAC-SHA1-96 が NAS サーバで有効化されていることを確認します。

手順

- 1 NFS サーバで、NFS ボリュームを構成し、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。
 - 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 のネットワーク』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。
[Kerberos 認証用 ESXi ホストの構成](#)を参照してください。

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。

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 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。この割り当てプロセスは、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と、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。
- Active Directory で AES256-CTS-HMAC-SHA1-96 または AES128-CTS-HMAC-SHA1-96 暗号化モードを有効にします。NFS 4.1 クライアントでは、DES-CBC-MD5 暗号化モードはサポートされていません。
- 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**

NFS 4.1 で Kerberos を使用する場合は、ESXi ホストの DNS 設定を変更する必要があります。設定は、Kerberos Key Distribution Center (KDC) に DNS レコードを配布するように設定された DNS サーバを参照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、Active Directory 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

NFS 4.1 で Kerberos を使用する場合は、ESXi ホストの DNS 設定を変更する必要があります。設定は、Kerberos Key Distribution Center (KDC) に DNS レコードを配布するように設定された DNS サーバを参照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、Active Directory サーバのアドレスを使用します。

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 [設定] タブをクリックします。
- 3 [ネットワーク] で [TCP/IP 設定] > [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 Domain Name
優先 DNS サーバ	AD Server IP
ドメインの検索	AD Domain Name

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。

ベスト プラクティスは NTP サーバとして Active Domain サーバを使用することです。

手順

- 1 vSphere インベントリでホストを選択します。
- 2 [設定] タブをクリックします。
- 3 [システム] で [時間の設定] 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 NTP サーバと同期するには、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、Active Directory (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 vSphere Web Client ナビゲータで、ホストを参照して移動します。
- 2 [設定] タブをクリックします。
- 3 [システム] で [認証サービス] をクリックします。
- 4 ESXi ホストを Active Directory ドメインに追加します。
 - a [認証サービス] ペインで [ドメインへの参加] をクリックします。
 - b ドメイン設定を指定して、[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。
- 5 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] ペインで [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 Virtual Volumes データストアを作成できます。

vSAN を有効にすると、vSAN データストアは自動的に作成されます。詳細については、『VMware vSAN 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 チャンネル、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。

■ Virtual Volumes 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、Virtual Volumes 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 チャンネル、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 データストアは、ESXi ホストで作成できません。既存の VMFS3 データストアは引き続き利用できるため、仮想マシンを VMFS5 または VMFS6 データストアに移行できます。

前提条件

- 1 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。
- 2 新しく追加されたストレージ デバイスを検出するには、再スキャンを実行します。[ストレージの再スキャン操作](#)を参照してください。
- 3 データストアでの使用を計画しているストレージ デバイスが使用可能であることを確認します。[ストレージ デバイスの特徴](#)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。
- 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 データストアのバージョンを指定します。

オプション	説明
VMFS 6	これは、512e ストレージ デバイスのデフォルトのオプションです。バージョン 6.0 以前の ESXi ホストは、VMFS6 データストアを認識できません。クラスタに、データストアを共有する ESXi 6.0 および ESXi 6.5 ホストが含まれている場合、このバージョンは適切でない可能性があります。
VMFS5	これは、512n ストレージ デバイスのデフォルトのオプションです。VMFS5 データストアは、バージョン 6.5 以前の ESXi ホストからのアクセスをサポートしています。

7 データストアの設定の詳細を定義します。

a パーティション構成を指定します。

注： VMFS6 データストアに必要な最小サイズは、2 GB です。

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。

b 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。

c VMFS6 について、ブロック サイズを指定し、容量再利用のパラメータを定義します。

オプション	説明
ブロック サイズ	VMFS データストアのブロック サイズでは、最大ファイル サイズとファイルが使用する容量を定義します。VMFS6 では、1 MB のブロック サイズをサポートしています。
容量再利用の精度	マッピング解除操作の精度を指定します。マッピング解除の精度はブロック サイズ (1 MB) に対応します。 1 MB より小さいサイズのストレージ セクターは再利用されません。
容量再利用の優先度	次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> ■ 低 (デフォルト)。マッピング解除操作を低率で処理します。 ■ なし。データストアで容量再利用の操作を無効にする場合は、このオプションを選択します。

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。
IPv6 形式または IPv4 形式を使用できます。
NFS 4.1 では、NFS 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。ESXi 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。
- 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 セキュリティを使用するには、Kerberos を有効にして適切な Kerberos モデルを選択します。

オプション	説明
認証にのみ Kerberos を使用 (krb5)	ID 検証のサポート
認証とデータの整合性に Kerberos を使用 (krb5i)	ID 検証に加え、データ整合性サービスを提供する。これらのサービスを使用すると、データバケットが改変されている可能性がないかがチェックされ、NFS トラフィックの改ざん保護に役立ちます。

Kerberos を有効にしない場合、データストアはデフォルトの AUTH_SYS セキュリティを使用します。

- 9 データセンターまたはクラスタ 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 設定オプションを確認し、[終了] をクリックします。

Virtual Volumes 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、Virtual Volumes 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 データベースの配置場所を指定します。
- 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、データストア名を入力します。
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 Virtual Volumes 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。
- 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

Virtual Volumes 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。

Virtual Volumes 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 デバイスに作成された各 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 デバイスを複製する場合、またはそのスナップショットをアレイ側で作成する場合、コピーされたデバイス コピーは元のデバイスとバイト単位で同じになります。たとえば、UUIDX を持つ VMFS データストアが元のストレージ デバイスに含まれている場合、コピーは、同じ UUIDX のデータストア コピーを格納しているように表示されます。

LUN のスナップショットとレプリケーションに加え、次の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データストアをマークします。

- 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。データストア コピーを元の UUID を使用してマウントする、または UUID を変更できます。UUID を変更するプロセスは、データストア再署名と呼ばれます。

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、再署名が最適な方法です。

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ない場合、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ト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 データストアのマウントは、その UUID が、デバイス スナップショット階層の他のデータストアの UUID と競合することなく行えます。

前提条件

- データストア コピーをアンマウントします。
- ホストでストレージの再スキャンを実行します。

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 データストアのキャパシティの拡張

VMFS データストアでより多くの容量が必要な場合は、データストアのキャパシティを増やすことができます。データストア エクステントを拡張するか、エクステントを追加することにより、キャパシティを動的に増やすことができます。

次のいずれかの方法で、データストアのキャパシティを拡張します。

- データストア エクステントが拡張可能な場合、これを動的に拡張し、隣接するキャパシティを使用できるようにする基盤となるストレージ デバイスで、エクステントの直後に空き容量がある場合、そのエクステントは拡張可能だとみなされます。

- エクステントを動的に追加する。データストアでは、最小要件 2 TB のエクステントを最大 32 個に拡張することができます。これは単一のボリュームとして扱われます。複数のエクステントにまたがる VMFS データストアでは、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の容量を使い切る必要はありません。

注： データストアが、アトミック テスト アンド セット (ATS) メカニズムとも呼ばれる Hardware Assisted Locking のみをサポートしている場合は、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 キャパシティの増加

VMFS データストアの容量は動的に増やすことができます。データストアに仮想マシンを追加するとき、またはデータストアで実行されている仮想マシンがより多くの容量を必要とするときに、追加の容量が必要になることがあります。

共有データストアが仮想マシンをパワーオンしており、100% いっぱいになった場合、データストアの容量を増やすことができます。この操作は、パワーオン状態の仮想マシンが登録されているホストからのみ実行できます。

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容量がある場合、そのストレージ デバイスは拡張可能です。
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 [パーティション レイアウト] で使用可能な設定を確認します。
- 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、表示されるメニュー項目が変わる場合があります。

メニュー項目	説明
空き容量を使用してデータストアを拡張	既存のエクステントに必要なキャパシティまで拡張します。
空き容量の使用	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。このメニュー項目は、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使います。このメニュー項目は、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 エクステントのキャパシティを設定します。

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 デバイスの空き容量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。

注： ホストが vCenter Server で管理されている場合、VMware Host Client からホストに直接アクセスしてデータストアの名前を変更することはできません。データストアの名前は vCenter Server から変更する必要があります。

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右クリックし、[名前の変更] を選択します。
- 3 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。
- Storage DRS は、データストアを管理しません。
- そのデータストアに対してストレージ I/O コントロール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は、データストアをアンマウントするホストを選択します。
- 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 データストアまたは Virtual Volumes 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。アンマウントした VMFS データストアはマウントできません。インベントリから削除された NFS データストアまたは Virtual Volumes 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。

次のステップ

ストレージ削除手順の一環として VMFS データストアをアンマウントした場合は、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 デバイスを分離できます。[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 つ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 データストアまたは Virtual Volumes 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 データストアまたは Virtual Volumes 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が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。
- すべてのホストからデータストアをアンマウントします。
- データストア用の Storage 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、[データストアの削除] を選択します。
- 3 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。

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
	データストアにファイルをアップロードします。データストアへのファイルのアップロードを参照してください。
	データストアからダウンロードします。データストアからのファイルのダウンロード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。データストア フォルダまたはファイルのコピー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。データストア フォルダまたはファイルの移動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。データストア フォルダまたはファイルの名前変更を参照してください。

アイコンとオプション	説明
	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。シン仮想ディスクの拡張を参照してください。

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

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。

データストアからのファイルのダウンロード

データストア ファイル ブラウザを使用して、ESXi ホストで使用可能なデータストアからローカル コンピュータにファイルをダウンロードします。

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 ダウンロードするファイルに移動し、[データストアからのダウンロード] アイコン (📄) をクリックします。
- 3 プロンプトに従ってファイルをローカル コンピュータに保存します。

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。

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。ただし、ターゲット データストアが、ソース ホストとは異なるホストに属する場合は、仮想ディスクへの変換が必要なことがあります。そうしないと、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。] チェック ボックスを選択します。
- 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。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。

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 [データストア] タブをクリックします。

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。
 - c データストアを選択して、[ファイルの参照] 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 フォルダを展開し、変換する仮想ディスク 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 [設定] 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

注: 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 17-6. 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 のリソース管理』ドキュメントを参照してください。

表 17-6. ストレージ フィルタ (続き)

フィルタ名	説明
config.vpxd.filter.sameHostsAndTranportsFilter (同じホストと転送フィルタ)	<p>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。</p> <ul style="list-style-type: none"> ■ 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。 ■ 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 チャネル エクステントを追加することはできません。
config.vpxd.filter.hostRescanFilter (ホストの再スキャン フィルタ)	<p>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イトします。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。</p> <p>注: 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。</p>

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 LUN 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できます。ミラーリングを行うことで、予期しないストレージ 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。
ディスクを別のデータストアに配置します。
- 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
<code>scsi#.returnNoConnectDuringAPD</code>	True
<code>scsi#.returnBusyOnNoConnectStatus</code>	False

- e ESXi 6.7 以降のバージョンを使用する場合は、ソフトウェア RAID-1 構成に参加している各仮想ディスクの追加パラメータを含めます。

パラメータは、ストレージ デバイスが故障した場合の、ゲスト OS の I/O 処理の失敗を回避します。

名前	値
<code>scsi#:1.passthruTransientErrors</code>	True
<code>scsi#:2.passthruTransientErrors</code>	True

- f [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十分でない場合、診断情報用のファイルを使用するように 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 ブートに関する一般的な推奨事項](#) を参照してください。

- ソフトウェア FCoE を介してアクセスされる LUN に診断パーティションを作成することはできません。
- 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 2 番目のホストで障害が発生した場合に、コア ダンプが保存される可能性があります。

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。

このメニュー項目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。

メニュー項目	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。複数のホストが、このパーティションにアクセスできます。1 台以上のホストに関する障害情報を保存することができます。

- 4 [次へ] 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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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 の概念と範例 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十分でない場合、診断情報用のファイルを使用するように 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 datastore_UUID or datastore_name</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 file_name</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 file_size_MB</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
<code>--path -p</code>	使用するコア ダンプ ファイルのパスです。ファイルは、事前に割り当てられている必要があります。
<code>--smart -s</code>	このフラグは <code>[--enable -e=true]</code> 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。 <pre>esxcli system coredump file set --smart --enable true</pre>

- 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 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` パラメータ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 コア ダンプ ファイルをリストします。

```
esxcli system coredump file list
```

- 2 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
```

- 3 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
<code>--file -f</code>	削除するダンプ ファイルのファイル名を入力します。名前を入力しない場合、コマンドは、デフォルト設定されているコア ダンプ ファイルを削除します。
<code>--force -F</code>	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 On-disk Metadata Analyzer (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 リソースで問題が発生した場合は、メタデータの整合性を確認できます。たとえば、次のいずれかの問題が発生した場合は、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` ファイルに、次のようなメタデータ エラーが記録されている。

```
cpu11:268057)WARNING: HBX: 599: Volume 50fd60a3-3aae1ae2-3347-0017a4770402
("<Datastore_name>") may be damaged on disk. Corrupt heartbeat detected at offset 3305472:
[HB state 0 offset 6052837899185946624 gen 15439450 stampUS 5 $
```

- 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 リソースの小さい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 サポートにお問い合わせください。

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 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.000000000000000000000000000000703	3

- 2 VMFS エラーをチェックします。

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.000000000000000000000000000000703:3
```

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 17-7. VOMA コマンド オプション

コマンド オプション	説明
-m --module	実行するモジュールには次のようなものがあります。
vmfs	モジュールの名前を指定しない場合は、このオプションがデフォルトで使用されます。 VMFS ファイル システムと、仮想フラッシュ リソースをバックアップするファイル システムを確認することができます。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。
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。
pttbl	MBR、GPT などの VMFS パーティションを確認して検証します。パーティションが存在しない場合は、パーティションが必要かどうかを判断します。
-f --func	実行される機能には次のようなものがあります。
query	モジュールでサポートされる機能をリストします。
check	エラーの有無を確認します。
-d --device	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、/vmfs/devices/disks/naa.00000000000000000000000000000000:1。
-s --logfile	結果を出力するログ ファイルを指定します。
-v --version	VOMA のバージョンを表示します。
-h --help	VOMA コマンドのヘルプ メッセージを表示します。

詳細については、VMware のナレッジベースの記事 [KB 2036767](#) を参照してください。

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 17-8. 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
VMFS3.MaxAddressableSpaceTB	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。
VMFS3.MinAddressableSpaceTB	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： 詳細オプションの変更はサポート外とみなされます。通常、デフォルトの設定で最適な結果になります。詳細オプションの変更は、VMware テクニカル サポートまたはナレッジベースの記事から具体的な手順を確認した場合にのみ行います。

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 [設定] 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] から適切な項目を選択します。
- 5 [編集] ボタンをクリックして、値を変更します。
- 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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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
<code>get</code>	VMFS ポインタ ブロック キャッシュ統計情報を取得する。
<code>reset</code>	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

18

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。マルチパスでは、ホストと外部ストレージ デバイス間でデータを転送する複数の物理パスを使用できます。

アダプタ、スイッチ、ケーブルなどの SAN ネットワーク内の要素のいずれかで障害が発生した場合に、ESXi は別の実行可能な物理パスに切り替えることができます。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ている間に、仮想マシンの I/O は最大で 60 秒遅延することがあります。この遅延時間を利用して、SAN はトポロジの変更後に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。

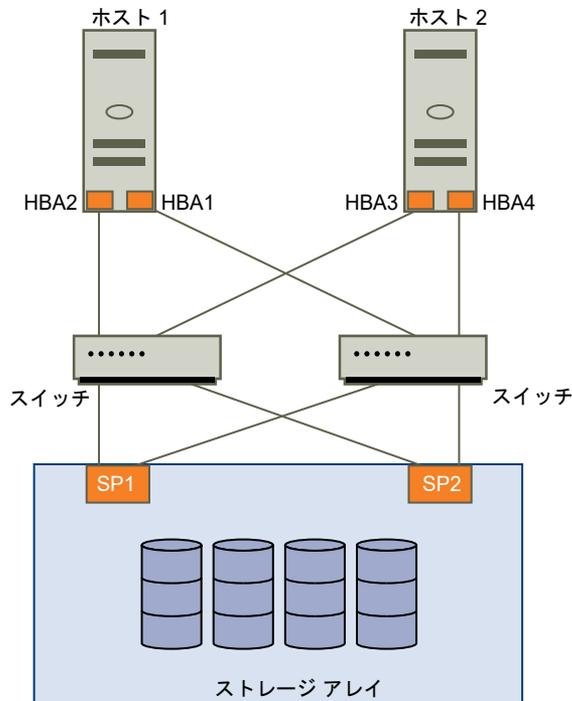
- ファイバ チャネルを使用したフェイルオーバー
- iSCSI でのホスト ベースのフェイルオーバー
- iSCSI でのアレイ ベースのフェイルオーバー
- パスのフェイルオーバーと仮想マシン
- 複数のパスの管理
- VMware マルチパス モジュール
- パスのスキャンと要求
- ストレージ パスおよびマルチパス プラグインの管理
- 仮想マシン I/O のキューのスケジューリング設定

ファイバ チャ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。一般的に、SAN のマルチパスでは SAN ファブリックに 1 台以上のスイッチ、およびストレージ アレイ デバイス自体に 1 個以上のストレージ 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、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 18-1. 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した場合、SP2 が引き継ぎます。SP2 は、スイッチとストレージ デバイスの間の接続を提供します。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 HBA フェイルオーバーと SP フェイルオーバーの両方をサポートしています。

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、複数の iSCSI HBA を使用するか、または複数の NIC とソフトウェア iSCSI アダプタとを組み合わせることができます。

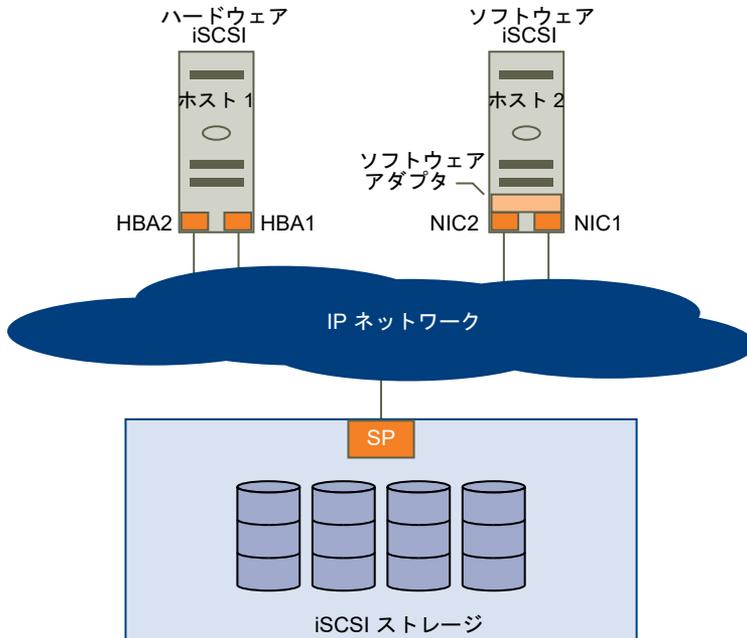
さまざまなタイプの iSCSI アダプタの詳細については、[iSCSI イニシエータ](#)を参照してください。

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 18-2. ホスト ベースのパス フェイルオーバー



ハードウェア iSCSI とフェイルオーバー

ハードウェア iSCSI を備えているホストは通常、複数のハードウェア iSCSI アダプタも備えています。ホストは、これらのアダプタを使用し、1 台以上のスイッチを介してストレージシステムにアクセスすることができます。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、アダプタが異なるパ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。

図のホスト 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パスが 2 つ提供されます。VMkernel NMP であるかサードパーティ製の MPP であるかにかかわらず、ホストのマルチパス プラグインはデフォルトでパスにアクセスできます。このプラグインで、各物理パ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、マルチパス プラグインでパスを HBA2 に切り替えることができます。

ソフトウェア iSCSI とフェイルオーバー

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、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。

マルチパス プラグインはホストの物理 NIC に直接アクセスすることができません。したがって、この設定では最初に各物理 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。別個の NIC に接続された各 VMkernel ポートは別々のパスになり、iSCSI ストレージ スタックと iSCSI ストレージ対応のマルチパス 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 でのマルチパスの構成については、[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。

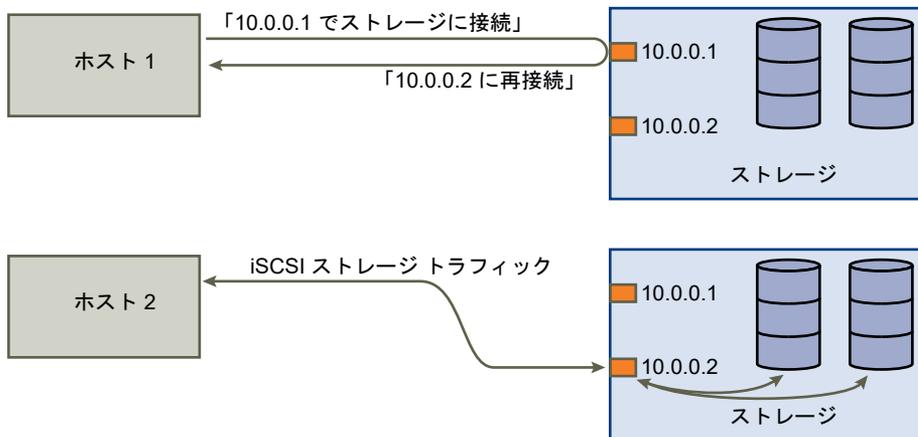
このようなストレージ システムを利用している場合、ホストはストレージ上の複数のポートを認識しないため、接続先のストレージのポートを選択できません。このようなシステムには、ホストが最初に通信を行う単一の仮想ポートアドレスがあります。この最初の通信中にストレージ システムはホストをリダイレクトして、ストレージ システム上の別のポートと通信するようになります。ホストの iSCSI イニシエータはこの再接続要求に従い、システム上の別のポートに接続します。ストレージ システムはこの技術を使用して、利用可能なポートに負荷を分散します。

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。

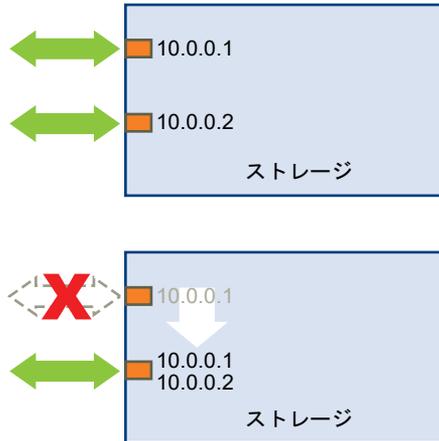
注： ストレージ システムが接続をリダイレクトしないことがあります。10.0.0.1 のポートはトラフィック用にも利用できます。

図 18-3. 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 18-4. 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

LUN へのアクティブなパスが、あるパスから別のパスに変更されると、パスのフェイルオーバーが発生します。通常、パスのフェイルオーバーは、現在のパスでの SAN コンポーネントの障害の結果として発生します。

パスに障害が発生すると、ホストがリンクがダウンしていると判断し、フェイルオーバーを実行するまで、ストレージ I/O が 30~60 秒間停止する場合があります。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。フェイルオーバー後、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。

フェイルオーバーに時間がかかりすぎると、Windows 仮想マシンが I/O を中断し、障害につながる場合があります。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 フェイルオーバー中に中断を回避するには、Windows のゲスト 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] - [Services] - [Disk] の順に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少なくとも 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) とも呼ばれる 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 を使用することで、サードパーティ製ソフトウェアの開発者は、特定のストレージ アレイに対する独自のロード バランシング技術やフェイルオーバー メカニズムを設計できます。ESXi ストレージの I/O パスには、サードパーティ コードを直接挿入できます。

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 18-1. 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 が組み込み形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。

マルチパス機能が必要な場合、サードパーティによる MPP も利用できます。サードパーティ製の MPP は、デフォルトの NMP に追加して実行することも、代替として実行することもできます。

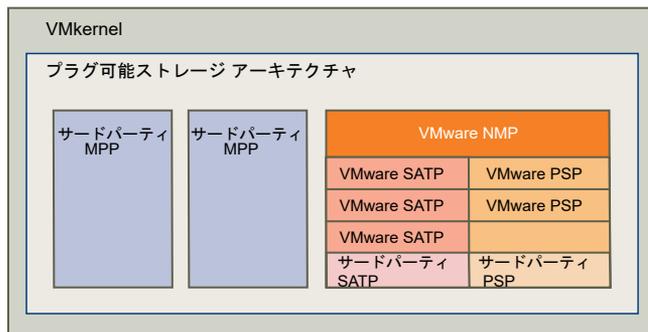
VMware NMP およびインストールされたサードパーティ製の MPP を調整する場合、PSA は次のタスクを実行します。

- 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 バランシングを制御します。

図 18-5. 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

Storage Array Type Plug-in (SATP) は、アレイに固有の処理を行います。SATP は、VMware NMP のサブモジュールです。

ESXi は、VMware がサポートするすべてのタイプのアレイの SATP を提供します。ESXi はまた、アクティブ-アクティブ、アクティブ-パッシブ、ALUA (Asymmetric Logical Unit Access)、およびローカルの非固有デバイスをサポートする、デフォルトの SATP も提供します。

各 SATP は、それぞれ特定のクラスのストレージ アレイの特性に対応しています。SATP は、パスの状態の検出と無効なパスを有効にするための、アレイに固有の処理を実行できます。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。

通常、NMP は特定のストレージ デバイスに対してどの SATP を使用するかを決定し、そのストレージ デバイスの物理パスに SATP を関連付けます。SATP では、次のようなタスクを行います。

- 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。

ESXi には、ストレージ アレイ用の一般的な SATP モジュールが含まれています。

VMW_SATP_LOCAL

ローカルの直接接続されたデバイスの SATP です。

vSphere 6.5 Update 2 リリース時点で、VMW_SATP_LOCAL は、4K ネイティブ フォーマットのデバイスを除いたローカル デバイスに対し、マルチパスのサポートを提供します。以前の vSphere リリースのように、ローカル デバイスへの複数のパスを要求するために、別の SATP を使用する必要はありません。

VMW_SATP_LOCAL は、VMW_PSP_MRU および VMW_PSP_FIXED パス選択プラグインをサポートしていますが、VMW_PSP_RR はサポートしていません。

VMW_SATP_DEFAULT_AA

アクティブ-アクティブ アレイの一般的な SATP です。

VMW_SATP_DEFAULT_AP

アクティブ-パッシブ アレイの一般的な SATP です。

VMW_SATP_ALUA

ALUA に準拠したアレイの SATP です。

詳細については、『VMware 互換性ガイド』および『vSphere Command-Line Interface リファレンス』ドキュメントを参照してください。

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、VMware 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

指定されている場合、ホストは優先パスを使用します。指定されていない場合、システムの起動時に検出された、使用可能な最初のパスを選択します。ホストで特定の優先パスを使用するには、手動で指定してください。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 デバイス用を使用するストレージ アレイ タイプ ポリシー (SATP) およびパス選択ポリシー (PSP) を確認することができます。また、このストレージ デバイスに対して使用可能なすべてのパスのステータスを表示することもできます。

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。

Active (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。

パスごとに、パ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 というパ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、パ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： パ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 というパスを記述する 3 つのパラメータすべてを指定します。

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 [設定] 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] で、[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、要求ルールに基づいて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)

指定されている場合、ホストは優先パスを使用します。指定されていない場合、システムの起動時に検出された、使用可能な最初のパスを選択します。ホストで特定の優先パスを使用するには、手動で指定してください。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] で [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] で、[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。サードパーティ製 MPP に加え、ホストの NMP および SATP 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、NMP マルチパス プラグイン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どうかを指定します。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）

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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の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。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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

各 SATP について、出力にストレージ アレイのタイプを示す情報または SATP がサポートするシステムを示す情報が表示されます。出力には、その SATP を使用するすべての LUN のデフォルトの PSP も表示されます。[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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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` パラメータを使用して、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、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。

PSA 要求ルールを追加するときの例は次のとおりです。

- 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ります。
- 新規のパスを追加して、既存の MPP を使用してこれらのパスを要求する。

注意： 要求ルールを作成するときは、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、この設定はパフォーマンス上の問題を起こす可能性があります。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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
<code>-A --adapter=<str></code>	パスのアダプタを指定します。
<code>-u --autoassign</code>	システムが自動的にルール ID を割り当てます。
<code>-C --channel=<long></code>	パスのチャンネルを指定します。
<code>-c --claimrule-class=<str></code>	要求ルール クラスを指定します。 有効な値：MP, Filter, VAAI。
<code>-d --device=<str></code>	デバイス UID を指定します。
<code>-D --driver=<str></code>	パスのドライバを指定します。
<code>-f --force</code>	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。
<code>--if-unset=<str></code>	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。
<code>-i --iqn=<str></code>	ターゲットの iSCSI 修飾名を指定します。
<code>-L --lun=<long></code>	パスの LUN を指定します。
<code>-M --model=<str></code>	パスのモデルを指定します。

オプション	説明
<code>-P --plugin=<str></code>	PSA プラグインを指定します。(必須)
<code>-r --rule=<long></code>	ルール ID を指定します。
<code>-T --target=<long></code>	バスのターゲットを指定します。
<code>-R --transport=<str></code>	バスの転送を指定します。 有効な値: block, fc, iscsi, iscsivendor, ide, sas, sata, usb, parallel, unknown。
<code>-t --type=<str></code>	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)
<code>-V --vendor=<str></code>	バスのベンダーを指定します。
<code>--wwnn=<str></code>	ターゲットのワールドワイド ノード番号を指定します。
<code>--wwpn=<str></code>	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パ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：マルチパスの要求ルールの定義

次の例では、ルール番号 500 を追加してロードします。このルールはモデル文字列に 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。

次の出力は、要求ルール 500 がシステムにロードされていて、アクティブなことを示します。

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	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		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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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
<code>-c --claimrule-class=<str></code>	要求ルールのクラスを指定します (MP、Filter、VAAI)。
<code>-P --plugin=<str></code>	プラグインを指定します。
<code>-r --rule=<long></code>	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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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 があ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。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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 やベンダーなどのデバイス 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 パ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 デバイスへのパスごとに

```
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、特定のストレージ デバイスをどの SATP で管理するのかを定義します。通常、NMP SATP ルールのデフォルト設定を使用できます。ルールを変更する必要がある場合は、`esxcli` コマンドを使用して、特定の 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ります。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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
<code>-b --boot</code>	このルールは、起動時に追加されるシステムのデフォルト ルールです。 <code>esx.conf</code> を変更する、またはホスト プロファイルに追加しないでください。
<code>-c --claim-option=string</code>	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。
<code>-e --description=string</code>	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。
<code>-d --device=string</code>	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。
<code>-D --driver=string</code>	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。
<code>-f --force</code>	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。
<code>-h --help</code>	ヘルプ メッセージを表示します。
<code>-M --model=string</code>	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。
<code>-o --option=string</code>	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。

オプション	説明
<code>-P --psp=string</code>	SATP 要求ルールのデフォルトの PSP を設定します。
<code>-O --psp-option=string</code>	SATP 要求ルールの PSP オプションを設定します。
<code>-s --satp=string</code>	新規ルールを追加する SATP です。
<code>-R --transport=string</code>	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。
<code>-t --type=string</code>	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。
<code>-V --vendor=string</code>	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リング設定

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リング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、特定の仮想マシン ファイルの I/O が専用の別個のキューに送られ、他のファイルの I/O からの干渉が防止されます。

この機能はデフォルトで有効です。この機能を無効にするには、システムの詳細設定で `VMkernel.Boot.isPerFileSchedModelActive` パラメータを調整してください。

ファイル I/O ごとのスケジューリングの編集

`VMkernel.Boot.isPerFileSchedModelActive` 詳細パラメータでは、ファイル I/O ごとのスケジューリング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 [設定] 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 次のいずれかのアクションを実行します。

- 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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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
<pre>esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE</pre>	ファイルごとの I/O スケジュールの無効化
<pre>esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE</pre>	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。

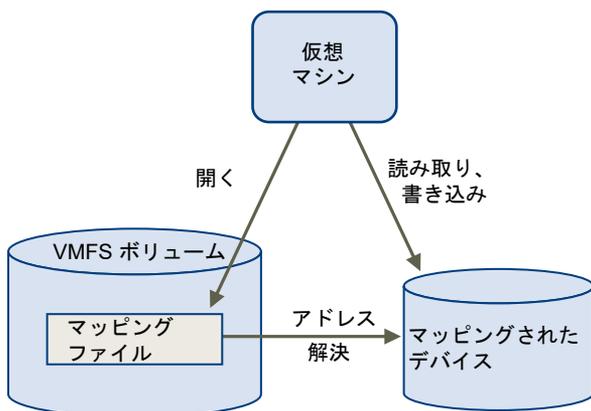
- RAW デバイス マッピングについて
- Raw デバイス マッピングの特性
- RDM を使用する仮想マシンの作成
- マッピング済み LUN のパス管理

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 があることで、仮想マシンはストレージ デバイスに直接アクセスして、ストレージ デバイスを使用することができます。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。

図 19-1. Raw デバイス マッピング



通常、仮想ディスクのストレージには VMFS データストアを使用します。しかし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) を使用する場合があります。

たとえば、次の場合に RDM で Raw LUN を使用します。

- 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バックアップ負荷軽減システムを実現します。
- 複数の物理ホストにまたがる MSCS クラスタリングの場合 (仮想-仮想クラスタ、物理-仮想クラスタなど)。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 として構成されます。

RDM は、VMFS ポリリュームから 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 ポリ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 で、次の 2 つの互換モードを使用できます。

- 仮想互換モードの RDM は、仮想ディスク ファイルに似た働きをします。RDM でスナップショットを使用できます。
- 物理互換モードの RDM 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的 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、マッピング済みのポリシーを保護するため、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、マッピング済みのポリシーで、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。

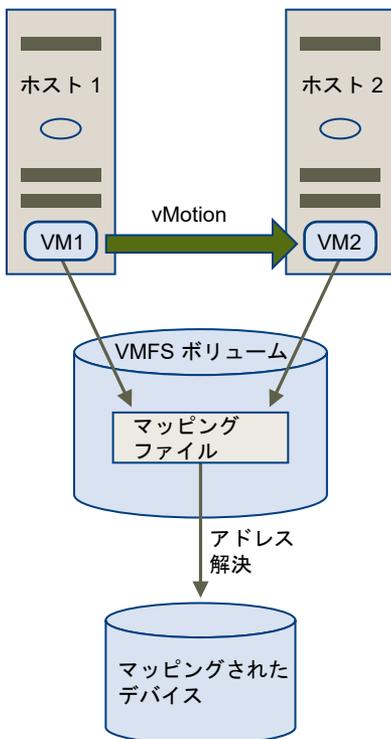
スナップショット

マッピング済みのポリシー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 19-2. 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。

当社では、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する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 および VMFS6 は仮想モードと物理モードの RDM で 2 TB 以上のディスク サイズをサポートします。

動的名前解決

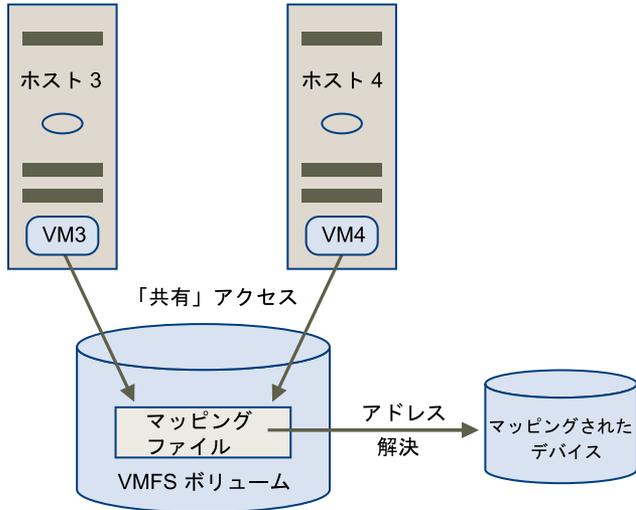
RDM ファイルでは、Raw デバイスへのパスが変更されたときに動的名前解決が可能です。

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 19-3. 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。

次の表に、それぞれのモードで使用可能な機能の比較を示します。

表 19-1. 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	いいえ	いいえ	はい REPORT LUNs はバススルーされ ない
vCenter Server のサポート	はい	はい	はい
スナップショット	はい	はい	いいえ
分散ロック	はい	はい	はい
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	いいえ	いいえ	はい

筐体内クラスタ タイプのクラスタリングの仮想ディスク ファイルを使用します。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 の仮想マシン管理』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、[18 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。

Software-Defined ストレージとストレージ ポリシー ベースの管理

20

ストレージ ポリシー ベースの管理 (SPBM) は、software-defined ストレージ環境の主要な要素です。これは、広範なデータ サービスおよびストレージ ソリューション間で単一の統合されたコントロール パネルを提供するストレージ ポリシー フレームワークです。

このフレームワークは、ストレージで仮想マシンのアプリケーションのニーズを満たすのに役立ちます。

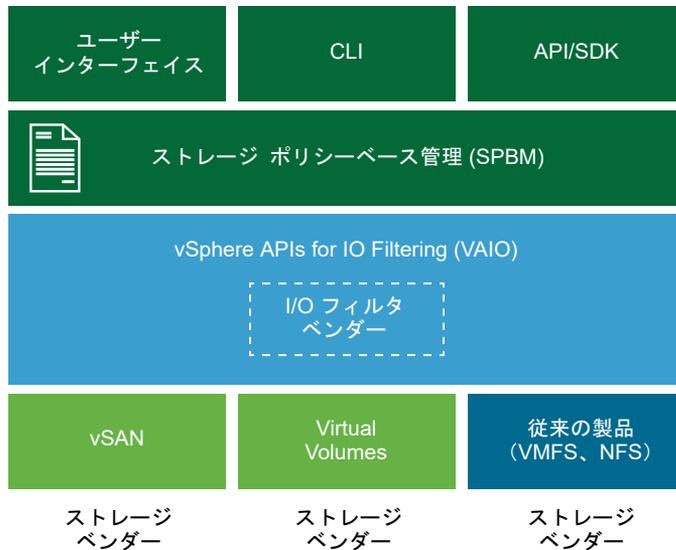
この章には、次のトピックが含まれています。

- ストレージ ポリシー ベースの管理について
- 仮想マシン ストレージ ポリシー
- 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 インターフェイスの入力
- デフォルト ストレージ ポリシー
- 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

ストレージ ポリシー ベースの管理について

SPBM は抽象レイヤーとして、Virtual Volumes、vSAN、I/O フィルタ、またはその他のストレージ エンティティによって提供されるストレージ サービスを抽象化します。

多くのパートナーおよびベンダーが、Virtual Volumes、vSAN、または I/O フィルタをサポートしています。個別のベンダー、あるいは特定のタイプのストレージやデータ サービスと統合するのではなく、SPBM は多くのタイプのストレージ エンティティ用の汎用フレームワークとなります。



SPBM は、次のメカニズムを提供します。

- ストレージ アレイや、I/O フィルタなどのその他のエンティティが提供するストレージ機能やデータ サービスのアドバタイズ。
- ESXi および vCenter Server と、ストレージ アレイ側と、エンティティ側との間で行われる双方向通信。
- 仮想マシン ストレージ ポリシーに基づいた仮想マシンのプロビジョニング。

仮想マシン ストレージ ポリシー

SPBM の特徴の 1 つは、仮想マシンのプロビジョニングに不可欠な仮想マシン ストレージ ポリシーです。ポリシーによって、仮想マシンに提供されるストレージのタイプと、仮想マシンに対するストレージ内での配置方法が管理されます。さらに仮想マシンが使用できるデータ サービスも決定されます。

vSphere は、デフォルトのストレージ ポリシーを提供しています。それに加え、ユーザーはポリシーを定義して、そのポリシーを仮想マシンに割り当てることができます。

ストレージ ポリシーを作成するには、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ます。ポリシーを定義する際は、仮想マシンで実行するアプリケーション用に、さまざまなストレージ要件を指定します。ストレージ ポリシーは、キャッシュ、レプリケーションなどの仮想ディスクの特定のデータ サービスを要求するために使用することもできます。

仮想マシンの作成、クローン作成、または移行の際に、ストレージ ポリシーを適用します。ストレージ ポリシーの適用後は、適合するデータストア内に仮想マシンを配置する際に SPBM メカニズムが役立ちます。特定のストレージ環境では、必要なサービスのレベルを確保するために、ストレージ リソース内で仮想マシン ストレージ オブジェクトをプロビジョニングして割り当てる方法が、SPBM によって決定されます。SPBM はさらに、仮想マシンに対して要求されたデータ サービスを有効にし、ポリシーのコンプライアンスの監視をサポートします。

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のプロセス全体には、通常、いくつかのステップが関係しています。

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。

手順	説明
仮想マシン ストレージ ポリシー インターフェイスに適切なデータを入力します。	<p>仮想マシン ストレージ ポリシー インターフェイスに、ストレージ環境で使用可能なデータストアとデータ サービスに関する情報が入力されていることを確認します。この情報は、ストレージ プロバイダとデータストア タグから取得されます。</p> <ul style="list-style-type: none"> ■ ストレージ プロバイダによって表されるエンティティについて、適切なプロバイダが登録されていることを確認します。 <p>ストレージ プロバイダを使用するエンティティには、vSAN、Virtual Volumes、I/O フィルタなどがあります。ストレージ エンティティのタイプに応じて、一部のプロバイダの自己登録が行われます。他のプロバイダは手動で登録する必要があります。</p> <p>ストレージ プロバイダ情報の表示および Virtual Volumes のストレージ プロバイダの登録を参照してください。</p> <ul style="list-style-type: none"> ■ 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をタグ付けします。タグを使用して、地理的場所や管理グループなどのストレージ プロバイダで伝送されないプロパティを示すこともできます。 <p>データストアへのタグの割り当てを参照してください。</p>
事前定義のストレージ ポリシー コンポーネントを作成します。	<p>ストレージ ポリシー コンポーネントは、レプリケーションなど、仮想マシンに提供する必要がある単一のデータ サービスを記述します。コンポーネントを前もって定義し、複数の仮想マシン ストレージ ポリシーに関連付けることができます。コンポーネントは再利用と交換が可能です。</p> <p>ストレージ ポリシー コンポーネントの作成を参照してください。</p>
仮想マシン ストレージ ポリシーを作成します。	<p>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。</p> <p>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。</p>
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。	<p>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。</p> <p>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。</p>
仮想マシン ストレージ ポリシーのコンプライアンスを確認します。	<p>仮想マシンが、割り当てられたストレージ ポリシーに順守したデータストアを使用していることを確認します。</p> <p>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。</p>

仮想マシン ストレージ ポリシー インターフェイスの入力

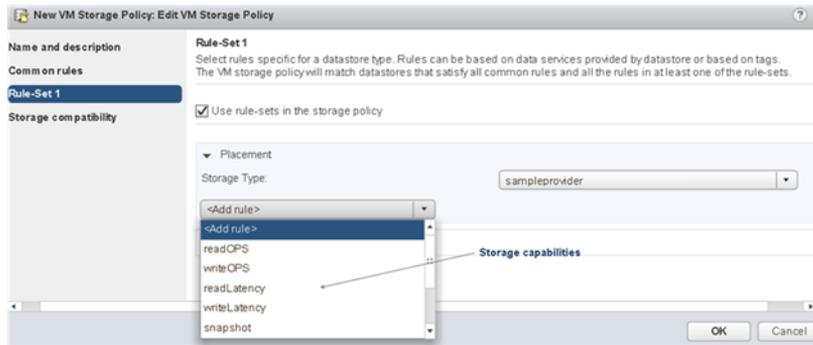
仮想マシン ストレージ ポリシーを定義するには、仮想マシン ストレージ ポリシー インターフェイスを使用します。このインターフェイスを使用するには、あらかじめストレージ環境で使用可能なストレージ エンティティとデータ サービスに関する情報を入力しておく必要があります。

この情報は、VASA プロバイダとも呼ばれるストレージ プロバイダから取得されます。もう 1 つのソースはデータストア タグです。

ストレージ機能とデータ サービス

たとえば Virtual Volumes や vSAN など、一部のデータストアはストレージ プロバイダによって表されます。ストレージ プロバイダを通じて、データストアはその機能を仮想マシン ストレージ ポリシー インターフェイスにアドバタイズできます。データストア機能、データ サービス、さまざまな値を持つその他の特性のリストが仮想マシン ストレージ ポリシー インターフェイスに入力されます。

これらの特性は、ストレージ ポリシーに機能ベースの配置ルールを定義するときに使用します。



ストレージ プロバイダは、ホストにインストールされた I/O フィルタも表示します。ストレージ プロバイダを通じて、フィルタ サービスに関する情報が仮想マシン ストレージ ポリシー インターフェイスに入力されます。特定のデータ サービスを仮想マシン ストレージ ポリシーの共通ルールに含めます。ストレージ固有の配置ルールとは異なり、共通ルールでは仮想マシンのストレージ配置および配置要件が定義されません。代わりに、仮想マシンについて要求された I/O フィルタ データ サービスが有効化されます。

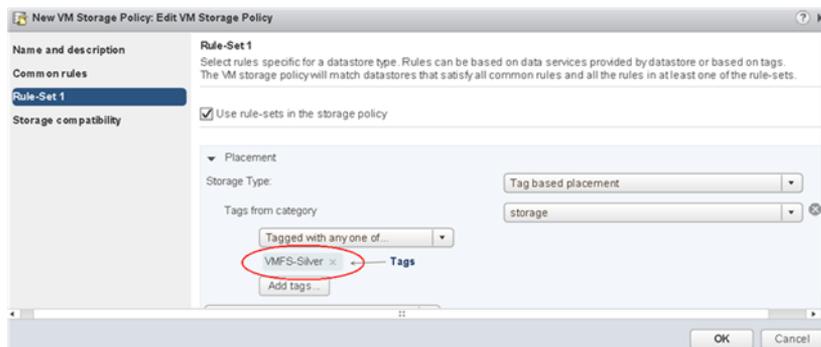


Tags

一般的に、VMFS および NFS データストアはストレージ プロバイダによって表されません。これらの機能やデータ サービスは、仮想マシン ストレージ ポリシー インターフェイスに表示されません。これらのデータストアに関する情報をエンコードするためにタグを使用できます。たとえば、VMFS データストアを VMFS-Gold および VMFS-Silver としてタグ付けし、異なるサービスのレベルを表すことができます。

また、タグを使用して、地理的場所 (Palo Alto) や管理グループ (会計) など、ストレージ プロバイダによってアドバタイズされない情報をエンコードすることもできます。

ストレージ機能や特性と同じように、データストアに関連付けられたすべてのタグが仮想マシン ストレージ ポリシー インターフェイスに表示されます。タグは、タグベースの配置ルールを定義する際に使用できます。



ストレージ プロバイダを使用した仮想マシン ストレージ ポリシー インターフェイスへの入力

ストレージ (VASA) プロバイダによって表されるエンティティについて、適切な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 プロバイダが登録されたら、そのプロバイダが表すデータストアおよびデータ サービスに関する情報が仮想マシン ストレージ ポリシー インターフェイスに入力されます。

ストレージ プロバイダを使用するエンティティには、vSAN、Virtual Volumes、I/O フィルタなどがあります。エンティティのタイプによって、一部のプロバイダは自動で登録されます。Virtual Volumes ストレージ プロバイダなど、その他のプロバイダは手動で登録する必要があります。ストレージ プロバイダが登録されたら、以下のデータを仮想マシン ストレージ ポリシー インターフェイスに提供します。

- Virtual Volumes や vSAN などのデータストアのストレージ機能および特性
- I/O フィルタの特性

前提条件

手動での登録が必要なストレージ プロバイダを登録します。詳細については、適切なドキュメントを参照してください。

- VMware vSAN の管理
- [22 章 Virtual Volumes の操作](#)
- [23 章 仮想マシン I/O のフィルタリング](#)

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 プロバイダを確認します。
このリストには、ストレージ プロバイダの名前、その URL およびステータス、プロバイダが表すストレージ エンティティなどの全般的な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 プロバイダまたはそのコンポーネントを選択します。

データストアへのタグの割り当て

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。データストアがストレージ プロバイダで示されず、仮想マシン ストレージ ポリシー インターフェイスでそのサービスをアダプタイズしない場合に、タグが役立ちます。ストレージ プロバイダ経由で通信されないプロパティ（地理的場所や管理グループなど）を示す際に、タグを使用することもできます。

一般的な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。

前提条件

必要な権限：

- ルート vCenter Server インスタンス上の vSphere タグ付け.vSphere タグの作成
- ルート vCenter Server インスタンス上の vSphere タグ付け.vSphere タグ カテゴリの作成
- ルート vCenter Server インスタンス上の vSphere タグ付け.vSphere タグの割り当てまたは割り当て解除

手順

- 1 ストレージ タグ用のカテゴリを作成します。
 - a vSphere Web Client のホーム ページで、[タグとカスタム属性] をクリックします。
 - b [タグ] タブ、[カテゴリ] の順にクリックします。
 - c [新しいカテゴリ] アイコンをクリックします ()。
 - d カテゴリ プロパティを指定します。次の例を参照してください。

カテゴリ プロパティ	例
カテゴリ名	ストレージの場所
説明	ストレージの場所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]

- e [OK] をクリックします。
- 2 ストレージ タグを作成します。
 - a [タグ] タブで、[タグ] をクリックします。
 - b [新しいタグ] アイコンをクリックします ()。
 - c タグのプロパティを指定します。次の例を参照してください。

タグのプロパティ	例
名前	テキサス
説明	テキサスにあるデータストア
カテゴリ	ストレージの場所

- d [OK] をクリックします。
- 3 タグをデータストアに適用します。
 - a vSphere Web Client ナビゲータで、データストアを参照して移動します。
 - b データストアを右クリックして、[タグとカスタム属性] - [タグの割り当て] の順に選択します。

- c [カテゴリ] ドロップダウン メニューから、ストレージの場所カテゴリを選択します。
- d 該当するタグ（テキサスなど）を選択して、[割り当て] 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

仮想マシン ストレージ ポリシーを作成するときは、タグを参照して、互換性のあるストレージ リソースのリストにタグ付けされたデータストアを含めることができます。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を参照してください。

または、タグ付けされたデータストアを仮想マシン ストレージ ポリシーから除外できます。たとえばテキサスおよびカリフォルニアにある Virtual Volumes データストアは仮想マシン ストレージ ポリシーに含め、ネバダにあるデータストアは仮想マシン ストレージ ポリシーから除外できます。

仮想マシン ストレージ ポリシーでタグを使用する方法の詳細については、次のビデオをご覧ください。



(Using Tags in Storage Policies in the vSphere Web Client)

デフォルト ストレージ ポリシー

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、互換性のある仮想マシン 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。オブジェクトベースのデータストアには vSAN や Virtual Volumes 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、Virtual Volumes または vSAN 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。

VMware は、vSAN と Virtual Volumes を対象とするデフォルト ストレージ ポリシーを提供します。または、デフォルト ポリシーを定義できます。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、vSAN と Virtual Volumes 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。

vSAN のデフォルト ストレージ ポリシー

vSAN ポリシーを選択しない場合は、vSAN データストアにプロビジョニングされているすべての仮想マシン オブジェクトに、デフォルトのストレージ ポリシーが適用されます。

VMware によって提供されるデフォルトの vSAN 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 vSAN 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、別のストレージ ポリシーを作成するためのテンプレートとしてそのコピーを使用できます。
- vSAN デフォルト ポリシーは、vSAN データストアとのみ互換性があります。
- vSAN 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。

Virtual Volumes のデフォルト ストレージ ポリシー

Virtual Volumes (VVol) 用として、VMware では、ルールやストレージ要件を何も含んでおらず、VVol 要件なしのポリシーと呼ばれるデフォルト ストレージ ポリシーを提供しています。vSAN の場合と同様、このポリシーは、Virtual Volumes データストアの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要件なしのポリシーには、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。
- ポリシーは、Virtual Volumes データストアとのみ互換性があります。
- Virtual Volumes 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

vSAN または Virtual Volumes 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。次に、このポリシーを vSAN データストアおよび Virtual Volumes データストアのデフォルトに指定できます。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 vSAN および Virtual Volumes データストアには、一度に 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 vSAN および Virtual Volumes データストアに一致するように、複数のルール セットを持つ単一のストレージ ポリシーを作成できます。このポリシーをすべてのデータストアのデフォルト ポリシーに指定できません。

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

Virtual Volumes と vSAN 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 Virtual Volumes または vSAN 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。

注： レプリケーション ルールが含まれるストレージ ポリシーは、デフォルトのストレージ ポリシーとして指定しないでください。指定すると、レプリケーション グループを選択できなくなります。

前提条件

Virtual Volumes または vSAN 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 [設定] タブをクリックします。
- 4 [設定] で、[全般] をクリックします。
- 5 [デフォルト ストレージ ポリシー] ペインで [編集] をクリックします。
- 6 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 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 ポリシーを作成および管理するには、vSphere Web Client の仮想マシン ストレージ ポリシー インターフェイスを使用します。

仮想マシン ストレージ ポリシー インターフェイスに適切なデータが入力されたら、ストレージ ポリシーの作成を開始できます。ストレージ ポリシーを作成する場合、配置ルールおよびデータ サービス ルールを定義します。ルールは仮想マシン ストレージ ポリシーの基本要素です。ポリシー内で、ルールはルールのコレクション、つまりルール セットにグループ化されます。

場合によっては、事前にルールをストレージ ポリシー コンポーネントにパッケージ化できます。コンポーネントは、前もって定義し、複数のストレージ ポリシーで参照できるモジュール式のビルディング ブロックです。

ストレージ ポリシーを作成したら、編集やクローン作成、さらに使用しないポリシーの削除を行うことができます。

データストア固有および共通のルール セットについて

仮想マシン ストレージ ポリシー インターフェイスに適切なデータが入力されたら、ストレージ ポリシーの定義を開始できます。仮想マシン ストレージ ポリシーの基本要素はルールです。個々のルールは、仮想マシン ストレージとデータ サービスに関する 1 つの要件が記述されたステートメントです。ポリシー内では、ルールはルールのコレクションにグループ化されます。2 種類のコレクション（通常のルール セットと共通のルール セット）が存在します。

通常のルール セット

通常のルール セットはデータストア固有です。各ルール セットには、仮想マシン ストレージ リソースの要件を記述する配置ルールが含まれている必要があります。1 つのルール セット内のすべての配置ルールは、1 つのストレージ エンティティを表します。これらのルールは、タグまたはストレージ機能に基づきます。さらに通常のルール セットには、仮想マシンに提供されるデータ サービスを示すオプションのストレージ ポリシー コンポーネントを含めることができます。

ストレージ ポリシーを定義するには、通常のルール セットが1つ必要です。追加のルール セットはオプションです。1つのポリシーで複数のルール セットを使用して、通常は複数のストレージ プロバイダから代替用のストレージ配置パラメータを定義できます。

共通のルール セット

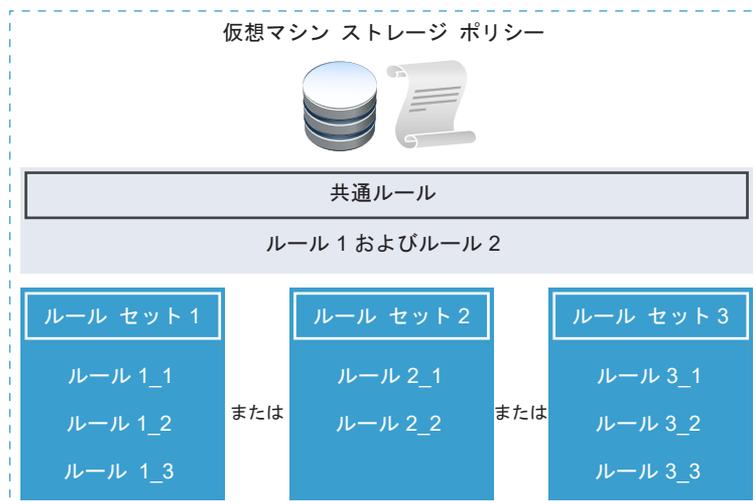
共通のルール セットでは、データストア固有の通常のルール セットとは異なり、仮想マシンのストレージ配置を定義することも、配置ルールを含むこともありません。共通のルール セットは、すべてのタイプのストレージ用の一般的なルール セットであり、データストアには依存しません。このルール セットでは、仮想マシンに対するデータ サービスを有効化します。共通のルール セットには、暗号化またはレプリケーションなどの特定のデータ サービスを示すルール、またはストレージ ポリシー コンポーネントが含まれます。

表 20-1. 仮想マシン ストレージ ポリシーの構造

共通ルール	通常のルール セット
ESXi ホストにインストールされているデータ サービスを有効にするルール、または事前定義のストレージ ポリシー コンポーネント。たとえば、I/O フィルタによるレプリケーション。	仮想マシン ストレージ リソースの要件を記述する配置ルール。たとえば、Virtual Volumes の配置。
	ストレージによって提供されるデータ サービスを有効にするルール、または事前定義のストレージ ポリシー コンポーネント。たとえば、Virtual Volumes によるキャッシュ。

ルールとルール セットの関係

ブール演算子 OR は、ポリシー内の通常のルール セット間の関係を定義します。AND 演算子は、1つのルール セット内のすべてのルール間の関係を定義します。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。共通ルールが存在しない場合は、1つの通常のルール セット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。共通ルールがある場合、ポリシーは、共通ルールと、通常のルール セットのいずれかのすべてのルールを満たすデータ ストアに一致します。



ルールについて

ルールは、仮想マシン ストレージ ポリシーの基本要素です。個々のルールは、仮想マシン ストレージとデータ サービスに関する1つの要件が記述されたステートメントです。

通常、各ルールは配置ルール（機能ベースおよびタグベース）とデータ サービス ルールのいずれかのカテゴリに分類できます。ストレージ ポリシー内では、個々のルールはルールのコレクション（ルール セット）で構成されています。

配置ルール：機能ベース

配置ルールでは、仮想マシンの特定のストレージ要件を指定し、SPBM がインベントリ内のすべてのデータストアの中から互換性のあるデータストアを区別できるようにします。これらのルールでは、必要なレベルのサービスを受けるために、データストア内で仮想マシン ストレージ オブジェクトを割り当てる方法を記述します。たとえば、ルールではターゲットとして Virtual Volumes の一覧を表示し、Virtual Volumes オブジェクトの最大目標復旧時点 (RPO) を定義できます。仮想マシンをプロビジョニングするとき、SPBM が仮想マシンの配置について決定する際にこれらのルールが指針となります。SPBM は、ルールに一致し、仮想マシンのストレージ要件を満たす Virtual Volumes データストアを見つけます。

配置ルール：タグベース

タグベースのルールでは、データストアのタグを参照します。これらのルールは、仮想マシンの配置を定義できます。たとえば、VMFS-Gold タグを含むすべてのデータストアをターゲットとして要求できます。タグベースのルールを使用すると、仮想マシンの配置要求を微調整することもできます。たとえば、Palo Alto タグのあるデータストアを Virtual Volumes データストアのリストから除外できます。

データ サービス ルール

データ サービス ルールは配置ルールとは異なり、仮想マシンのストレージ配置およびストレージ要件を定義しません。代わりに、仮想マシンに対して特定のデータ サービス（キャッシュ、レプリケーションなど）を有効化できます。ストレージ システムや他のエンティティが、これらのサービスを提供できます。これらのサービスは、ホストや vCenter Server にインストールすることもできます。データ サービス ルールはストレージ ポリシー コンポーネントに含めます。データ サービスがストレージ システムから提供される場合は、コンポーネントを通常のルール セットに追加します。データ サービスが I/O フィルタから提供される場合は、コンポーネントを共通のルール セットに追加します。

ストレージ ポリシー コンポーネントについて

仮想マシン ストレージ ポリシーには、ストレージ ポリシー コンポーネントと呼ばれる再利用および交換可能な構築要素を 1 つ以上含めることができます。各コンポーネントは、仮想マシンに提供される特定のデータ サービスを示します。あらかじめ定義したポリシー コンポーネントを複数の仮想マシン ストレージ ポリシーに関連付けることができます。

事前定義されたコンポーネントを仮想マシンまたは仮想ディスクに直接割り当てることはできません。代わりに、コンポーネントを仮想マシン ストレージ ポリシーに追加して、そのポリシーを仮想マシンに割り当てる必要があります。

コンポーネントは、1 つのサービス プロバイダの 1 つのサービス タイプを示します。サービスは、使用するプロバイダに応じて異なる可能性があります。通常は次のカテゴリのいずれかに属しています。

- 圧縮
- キャッシュ
- 暗号化

■ レプリケーション

ストレージ ポリシー コンポーネントを作成するときは、1つの特定のタイプおよびレベルのサービスに対してルールを定義します。

次の例は、仮想マシン VM1 および VM 2 は同じ配置要件を持つが、異なるレベルのレプリケーション サービスが必要であることを示しています。さまざまなレプリケーション パラメータを使用してストレージ ポリシー コンポーネントを作成し、そのコンポーネントを関連するストレージ ポリシーに追加できます。

表 20-2. ストレージ ポリシー コンポーネント

仮想マシン	仮想マシン ストレージ ポリシー	ストレージ ポリシー コンポーネント
VM1 は 2 時間ごとのレプリケーションが必要	SP1	2 時間のレプリケーション
VM2 は 4 時間ごとのレプリケーションが必要	SP2 (SP1 のクローン)	4 時間のレプリケーション

サービスのプロバイダには、ストレージ システム、I/O フィルタ、または別のエンティティがあります。コンポーネントが I/O フィルタを参照する場合、コンポーネントはストレージ ポリシーの共通のルール セットに追加されます。I/O フィルタ以外のエンティティ、たとえばストレージ システムを参照するコンポーネントは、配置ルールのある通常のルール セットに追加されます。

コンポーネントを操作するときは、次のガイドラインに従ってください。

- 各コンポーネントに含めることができるのは、1つのルール セットのみです。このルール セットのすべての特性は、データ サービスの単一のプロバイダに属します。
- コンポーネントが仮想マシン ストレージ ポリシー内で参照されている場合は、コンポーネントを削除できません。コンポーネントを削除する前に、そのコンポーネントをストレージ ポリシーから除外するか、ストレージ ポリシーを削除する必要があります。
- コンポーネントをポリシーに追加するときは、ルール セットごとに同じカテゴリ（キャッシュなど）のコンポーネントを1つのみ使用できます。

ストレージ ポリシー コンポーネントの作成

ストレージ ポリシー コンポーネントは、レプリケーションなど、仮想マシンに提供する必要がある単一のデータ サービスを記述します。コンポーネントを前もって定義し、複数の仮想マシン ストレージ ポリシーに関連付けることができます。コンポーネントは再利用と交換が可能です。

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 コンポーネント] タブをクリックし、[ストレージ ポリシー コンポーネントの作成] 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 たとえば「4 時間のレプリケーション」などの名前を入力し、ポリシー コンポーネントの説明を入力します。名前がほかのコンポーネントやストレージ ポリシーと競合しないようにしてください。

- 5 サービスのカテゴリ ([レプリケーション] など) を選択します。
- 6 サービス プロバイダを選択します。
- 7 選択したカテゴリのルールを定義します。

たとえば、4 時間のレプリケーションを設定している場合は、目標復旧時点 (RPO) の値を 4 に設定します。

I/O フィルタに基づいた暗号化については、[暗号化の前に I/O フィルタを許可] パラメータを設定します。ストレージによって提供される暗号化ではこのパラメータは必要ありません。

オプション	説明
False (デフォルト)	暗号化フィルタの前に他の I/O フィルタを使用できません。
True	暗号化フィルタの前に他の I/O フィルタを使用できます。暗号化の前に、他のフィルタ (レプリケーションなど) でクリア テキスト データを分析できます。

- 8 [OK] をクリックします。

結果

新しいコンポーネントがストレージ ポリシー コンポーネントのリストに表示されます。

次のステップ

コンポーネントを仮想マシン ストレージ ポリシーに追加できます。レプリケーションなど、コンポーネントが参照するデータ サービスが I/O フィルタによって提供される場合、コンポーネントを共通ルール セットに追加します。データ サービスがストレージ システムによって提供される場合、コンポーネントを通常のルール セットに追加します。

ストレージ ポリシー コンポーネントの表示

ストレージ ポリシー コンポーネントを作成したら、その詳細情報を表示し、その他の管理タスクを実行できます。

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 [ストレージ ポリシー コンポーネント] タブをクリックします。
- 3 選択したストレージ ポリシー コンポーネントの詳細情報を表示します。
 - a コンポーネントを選択します。
 - b 次のタブを切り替えます。

メニュー項目	説明
内容	ルールおよびルールに関連する値を表示します。
次で使用	コンポーネントを参照する仮想マシン ストレージ ポリシーの一覧を表示します。

次のステップ

[ストレージ ポリシー コンポーネント] タブを使用して、選択したストレージ ポリシー コンポーネントの編集、クローン作成、または削除を行います。

ストレージ ポリシー コンポーネントの編集またはクローン作成

既存のストレージ ポリシー コンポーネントを変更できます。また、クローン作成することにより、既存のコンポーネントのコピーを作成できます。

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 [ストレージ ポリシー コンポーネント] タブをクリックし、編集またはクローン作成するコンポーネントを選択します。
- 3 次のいずれかのアイコンをクリックします。
 - [設定の編集]
 - [クローン作成]
- 4 適切な値を変更します。

編集する際には、データ サービスおよびプロバイダのカテゴリは変更できません。たとえば、元のコンポーネントが I/O フィルタによって提供されるレプリケーションを参照する場合、これらの設定は変更しないままにする必要があります。クローン作成する際には、元のコンポーネントのすべての設定をカスタマイズできます。

- 5 変更内容を保存するには、[OK] をクリックします。
- 6 仮想マシンに割り当てられた仮想マシン ストレージ ポリシーが編集するポリシー コンポーネントを参照する場合、ストレージ ポリシーを仮想マシンに再適用します。

メニュー項目	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。 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。
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 コンポーネントの削除

使用しないストレージ ポリシー コンポーネントは削除できます。

前提条件

コンポーネントが仮想マシン ストレージ ポリシーで使用されていないことを確認します。使用されている場合、ポリシーからコンポーネントを削除するかポリシーを削除します。コンポーネントの [次で使用] タブで、そのコンポーネントを参照する仮想マシン ストレージ ポリシーが一覧表示されます。

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 コンポーネント] タブをクリックし、リストから削除するコンポーネントを選択します。複数のコンポーネントを選択できます。
- 3 [削除] アイコンをクリックし、コンポーネントの削除を確定します。

結果

コンポーネントがストレージ ポリシー コンポーネントのリストから削除されます。

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ストレージ機能を参照できます。または、データストア タグを参照できます。ポリシーには、レプリケーションやキャッシュなど、I/O フィルタ、ストレージ システム、またはその他のエンティティによって提供されるデータ サービスを有効にするコンポーネントを含めることができます。

前提条件

- 仮想マシン ストレージ ポリシー インターフェイスに、ストレージ環境で使用可能なストレージ エンティティとデータ サービスに関する情報が入力され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 インターフェイスの入力](#) を参照してください。
- 適切なストレージ ポリシーのコンポーネントを定義します。[ストレージ ポリシー コンポーネントの作成](#) 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] ページで、仮想マシン ストレージ ポリシーに含めるデータ サービスを指定します。データ サービスは、ESXi ホストと vCenter Server にインストールされたソフトウェア コンポーネントによって提供されます。共通ルールが含まれる仮想マシン ストレージ ポリシーにより、仮想マシンの指定されたデータ サービスが有効にされます。
- 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](#)
[ルール セット] ページを使用してストレージ配置ルールを定義します。ストレージでレプリケーションなどの追加のデータ サービスが提供される場合、このページを使用して仮想マシン ストレージ ポリシーに含めるデータ サービスを指定します。

4 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。vSAN や Virtual Volumes 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] 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] タブをクリックします。
- 3 [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。
- 4 vCenter Server インスタンスを選択します。
- 5 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] ページで、仮想マシン ストレージ ポリシーに含めるデータ サービスを指定します。データ サービスは、ESXi ホストと vCenter Server にインストールされたソフトウェア コンポーネントによって提供されます。共通ルールが含まれる仮想マシン ストレージ ポリシーにより、仮想マシンの指定されたデータ サービスが有効にされます。

データ サービスはすべてのストレージのタイプに汎用であり、データストアに依存しません。環境によっては、データ サービスが暗号化、キャッシュ、レプリケーションなど、複数のカテゴリに属する場合があります。暗号化など、一部のデータ サービスは VMware によって提供されます。サードパーティ製の I/O フィルタによって提供されるデータ サービスもあります。

前提条件

- 仮想マシンの暗号化については、『vSphere のセキュリティ』のドキュメントを参照してください。
- I/O フィルタについては、[23 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 ポリシー コンポーネントについては、[ストレージ ポリシー コンポーネントについて](#)を参照してください。

手順

- 1 [仮想マシン 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 [コンポーネントの追加] (+) アイコンをクリックし、ドロップダウン メニューからデータ サービス カテゴリを選択します (レプリケーションなど)。
- 3 ルールに対して適切なプロバイダと値を指定することによって、データ サービス カテゴリのルールを定義します。または、事前定義済みコンポーネントのリストからデータ サービスを選択します。

オプション	説明
 Component Name	このオプションは、データベースにストレージ ポリシーのコンポーネントを事前定義している場合に使用できます。使用するコンポーネントがわかっている場合は、リストでそれを選択して仮想マシン ストレージ ポリシーに追加します。
すべて表示	カテゴリで使用できるすべてのコンポーネントを確認します。特定のコンポーネントを含める場合は、リストでそれを選択し、[OK] をクリックします。
カスタム	ルールに対して適切なプロバイダと値を指定して、データ サービス カテゴリのカスタム ルールを定義します。

- 4 さらにコンポーネントを追加して、他のデータ サービスを要求します。
共通または通常のルール セットごとに、同じカテゴリ (キャッシュなど) から使用できるコンポーネントは1つのみです。
- 5 [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

[ルール セット] ページを使用してストレージ配置ルールを定義します。ストレージでレプリケーションなどの追加のデータ サービスが提供される場合、このページを使用して仮想マシン ストレージ ポリシーに含めるデータ サービスを指定します。

前提条件

- 使用する環境に vSAN や Virtual Volumes 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 vSAN の管理』ドキュメントおよび、[22 章 Virtual Volumes の操作](#)を参照してください。
- 事前定義済みストレージ ポリシー コンポーネントを設定するには、[ストレージ ポリシー コンポーネントについて](#)を参照してください。

手順

- 1 [ストレージ ポリシーでのルール セットの使用] チェック ボックスが選択されていることを確認します。

2 配置ルールを定義します。

配置ルールでは、特定のストレージ エンティティが仮想マシンのターゲットとして要求されます。機能ベースの配置ルールもタグベースの配置ルールも使用できます。機能ベースのルールは、vSAN や Virtual Volumes などのストレージ エンティティがストレージ (VASA) プロバイダ経由でアダプタイズするデータ サービスに基づいています。タグベースのルールは、データストアに割り当てたタグを参照します。

オプション	説明
ストレージ機能に基づく配置	<ul style="list-style-type: none"> a [ストレージ タイプ] ドロップダウン メニューから、Virtual Volumes などのターゲット ストレージ エンティティを選択します。 b [ルールの追加] ドロップダウン メニューから、機能を選択してその値を指定します。 たとえば、Virtual Volumes オブジェクトの 1 秒あたりの読み取り操作数を指定できます。選択したストレージ エンティティに必要な数のルールを含めることができます。入力する値が、ストレージ リソースがアダプタイズする値の範囲内にあることを確認します。 c 配置要求を微調整する必要がある場合は、タグベースのルールを追加します。 タグベースのルールでは、特定の配置基準を含めたり除外したりできます。たとえば、ターゲット Virtual Volumes データストアのリストから Palo Alto タグの付いたデータストアを除外することができます。
タグに基づく配置	<ul style="list-style-type: none"> a [ストレージ タイプ] ドロップダウン メニューから、[タグ ベースの配置] 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、[カテゴリからのタグ] を選択します。 c タグベースの配置基準を定義します。 たとえば、VMFS-Gold タグの付いたすべてのデータストアをターゲットとして要求できます。

- 3 (オプション) 仮想マシン ストレージ ポリシーに含めるデータ サービスを選択します。

[ルール セット] ページで参照するデータ サービスはストレージによって提供されます。データ サービスを参照する仮想マシン ストレージ ポリシーは、仮想マシンについてこれらのデータ サービスを要求します。

- a [コンポーネントの追加] (+) アイコンをクリックし、ドロップダウン メニューからデータ サービス カテゴリを選択します (レプリケーションなど)。
- b ルールに対して適切なプロバイダと値を指定することによって、データ サービス カテゴリのルールを定義します。または、事前定義済みコンポーネントのリストからデータ サービスを選択します。

オプション	説明
 Component Name	このオプションは、データベースにストレージ ポリシーのコンポーネントを事前定義している場合に使用できます。使用するコンポーネントがわかっている場合は、リストでそれを選択して仮想マシン ストレージ ポリシーに追加します。
すべて表示	カテゴリで使用できるすべてのコンポーネントを確認します。特定のコンポーネントを含める場合は、リストでそれを選択し、[OK] をクリックします。
カスタム	ルールに対して適切なプロバイダと値を指定して、データ サービス カテゴリのカスタムルールを定義します。

- c さらにコンポーネントを追加して、他のデータ サービスを要求します。

共通または通常のルール セットごとに、同じカテゴリ (キャッシュなど) から使用できるコンポーネントは 1 つのみです。

- 4 (オプション) 別のルール セットを定義するには、[別のルール セットの追加] をクリックしてステップ 2 からステップ 3 を繰り返します。

複数のルール セットで、単一のポリシーが代替用のストレージ配置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)。

- 5 [次へ] をクリックします。

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 [設定の確認] ページで、ストレージ ポリシー設定を確認します。

設定を変更する必要がある場合、[戻る] をクリックして関連するページに戻ります。

- 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

ストレージ ポリシーを使用する予定がない場合、ポリシーは削除できます。

VVol の要件なしのポリシーと vSAN のデフォルト ポリシーは削除できません。

前提条件

- 削除するポリシーがデフォルトとして使用されている場合、データストアから関連付けを解除します。[データストアのデフォルト ストレージ ポリシーの変更](#)を参照してください。
- ポリシーが仮想マシンによって使用されている場合、仮想マシン ポリシーの割り当てを変更します。[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。

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] タブをクリックします。
- 3 削除するポリシーを指定し、[削除] アイコン (✖) をクリックします。
複数のポリシーを選択できます。
- 4 [はい] をクリックしてアクションを確定します。

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 [仮想マシン ストレージ ポリシー] タブをクリックします。
- 3 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]
- 4 (オプション) ポリシーを変更し、[OK] をクリックします。
 - 5 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。 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。
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。ポリシーは、仮想マシンの最適なデータストアを選択し、必要なレベルのサービスを強制できます。または、仮想マシンおよびそのディスクの特定のデータ サービスを有効にできます。

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。

仮想マシンへのストレージ ポリシーの割り当て

仮想マシンの初期導入時、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 の仮想マシン管理』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 (Virtual Volumes 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。このオプションは、キャッシュ、レプリケーションなどの I/O フィルタを仮想ディスクで有効にするために使用することもできます。

- 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られたストレージ 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。異なるストレージ ポリシーを仮想マシン構成ファイルおよび仮想ディスクと関連付けることもできます。たとえば、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に、異なるポリシーを適用することがあります。

手順

- 1 仮想マシンを参照します。
 - a 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。
 - b 変更するストレージ ポリシーをクリックします。
 - c [仮想マシン] タブ > [仮想マシン] の順にクリックします。
このストレージ ポリシーを使用する仮想マシンのリストを確認できます。
 - d リストから、ポリシーを変更する仮想マシンを選択します。
- 2 [構成] タブをクリックし、[ポリシー] をクリックします。
- 3 [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。
- 4 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	操作
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。	<ol style="list-style-type: none"> 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。	<ol style="list-style-type: none"> 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] 列で、ドロップダウン メニューからポリシーを選択します。

- 5 Virtual Volumes ポリシーでレプリケーションを使用する場合は、レプリケーション グループを構成します。
レプリケーション グループは、ターゲット サイトにまとめてレプリケートする必要のある仮想マシンと仮想ディスクを示します。
 - a [設定] をクリックして [仮想マシン レプリケーション グループの設定] ページを開きます。
 - b レプリケーション グループを指定します。

オプション	操作
同じレプリケーション グループをすべての仮想マシン オブジェクトに割り当てます。	[共通のレプリケーション グループ] を選択し、ドロップダウン メニューから事前設定済み グループまたは自動グループを選択します。
さまざまなレプリケーション グループを、仮想マシン ホーム オブジェクトおよび仮想ディスクに割り当てます。	<ol style="list-style-type: none"> 1 [ストレージ オブジェクトごとのレプリケーション グループ] を選択します。 2 変更するオブジェクトを選択します。 3 [レプリケーション グループ] 列で、ドロップダウン メニューからレプリケーション グループを選択します。

- c [OK] をクリックします。
- 6 [OK] をクリックして、仮想マシン ストレージ ポリシーの変更を保存します。

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

仮想マシンと仮想ディスクが、仮想マシン ストレージ ポリシーに準拠したデータストアを使用しているかどうかを確認できます。

ホストまたはクラスタに無効なストレージ ポリシーがある仮想マシンをチェックすると、非準拠というチェック結果が返されます。

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] (🚩) アイコンをクリックします。

[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、必要な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、データストアの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、必要な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、データストアの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。

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 [構成] 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 [すべての期限切れエンティティに仮想マシン ストレージ ポリシーを再適用します] アイコン (🔄) をクリックします。

5 コンプライアンスの状態を確認します。

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。 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。
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。

ストレージ プロバイダとは、VMware から提供されるか、vSphere APIs for Storage Awareness (VASA) を使用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、VASA プロバイダとも呼ばれます。ストレージ プロバイダはさまざまなストレージ エンティティと連携します。これらのエンティティには、外部の物理ストレージのほか、vSAN や Virtual Volumes などのストレージ抽象化が含まれます。ストレージ プロバイダは、I/O フィルタなどのソフトウェア ソリューションをサポートすることもできます。

この章には、次のトピックが含まれています。

- ストレージ プロバイダについて
- ストレージ プロバイダおよびデータの表現
- 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 プロバイダの登録
- 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 プロバイダ証明書の更新

ストレージ プロバイダについて

一般に vCenter Server および ESXi 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設定、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。この情報により、仮想マシンの配置について適切に決定し、ストレージ要件の設定やストレージ環境の監視を行うことができます。

パーシステンス ストレージ プロバイダ

アレイとストレージ抽象化を管理するストレージ プロバイダは、パーシステンス ストレージ プロバイダと呼ばれます。Virtual Volumes または vSAN をサポートするプロバイダは、ここに分類されます。パーシステンス プロバイダは、ストレージの他に、レプリケーションなどのデータ サービスを提供できます。

データ サービス プロバイダ

プロバイダの別のカテゴリは、I/O フィルタ ストレージ プロバイダまたはデータ サービス プロバイダです。これらのプロバイダは、ホスト ベースのキャッシュ、圧縮、暗号化などのデータ サービスを提供します。

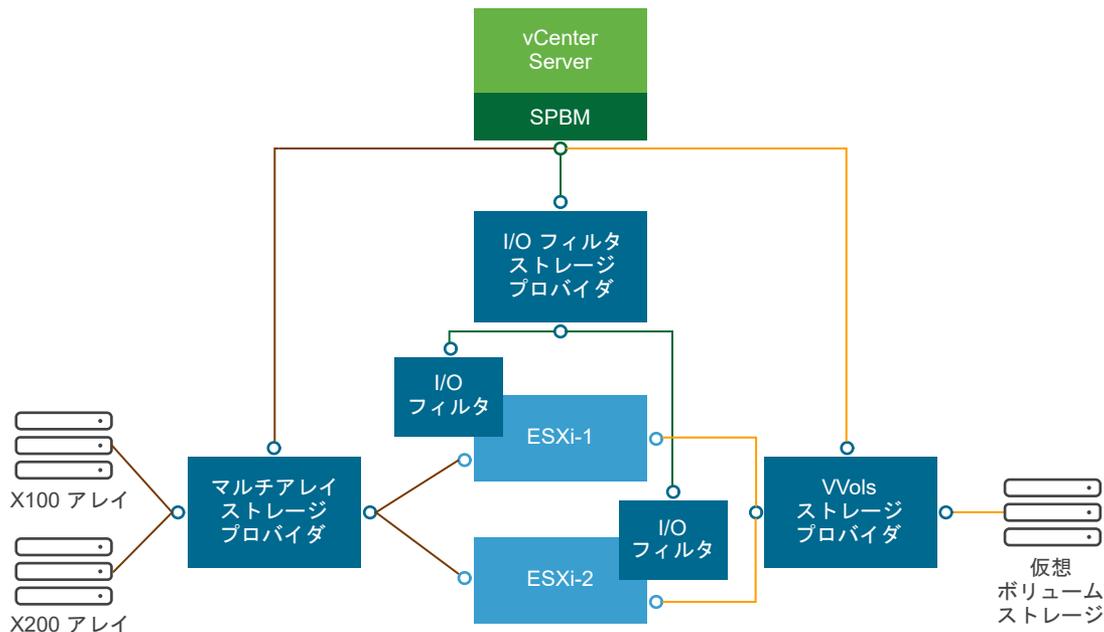
組み込みストレージ プロバイダ

組み込みストレージ プロバイダは VMware によって提供されます。通常、登録は必要ありません。たとえば I/O フィルタをサポートするストレージ プロバイダは自動的に登録されます。

サードパーティのストレージ プロバイダ

サードパーティからプロバイダが提供される場合は、通常、プロバイダを登録する必要があります。そのようなプロバイダには、Virtual Volumes プロバイダなどがあります。vSphere Web Client を使用して、各ストレージ プロバイダのコンポーネントを登録して管理します。

次の図は、さまざまなタイプのストレージ プロバイダが、vCenter Server、ESXi、およびストレージ環境のその他のコンポーネントの間の通信を促進する方法を示します。これらのコンポーネントには、ストレージ アレイ、Virtual Volumes のストレージ、および I/O フィルタなどが含まれる場合があります。



ストレージ プロバイダおよびデータの表現

vCenter Server と ESXi は、基盤となる物理ストレージおよび Software-Defined Storage 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、vSAN、Virtual Volumes、および I/O フィルタなどの機能に不可欠です。これらの機能を表すストレージ プロバイダは、ストレージ ポリシーベース管理 (SPBM) メカニズムと統合されます。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。SPBM メカニズムを使用すると、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、仮想ディスクで特定のデータ 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 ストレージ ポリシーの作成と管理](#) 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。

- ブロック デバイスまたはファイル システムの Distributed Resource Scheduling に関する Storage DRS 情報。この情報は、Storage DRS による決定事項と、ストレージ システム内部のリソース管理による決定事項の互換性を確保するために役立ちます。

ストレージ プロバイダの要件および考慮事項

サードパーティのストレージ プロバイダを使用する場合は、特定の要件と考慮事項が適用されます。

通常は、ベンダーがストレージ プロバイダを提供します。VMware VASA プログラムはサードパーティのストレージ プロバイダを vSphere 環境に統合するアーキテクチャを定義するため、vCenter Server ホストおよび ESXi ホストはストレージ プロバイダと通信できます。

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 ベンダーにお問い合わせください。
- ストレージ プロバイダが vCenter Server および ESXi のバージョンと互換性があることを確認します。VMware 互換性ガイド を参照してください。
- vCenter Server と同じシステムに VASA プロバイダをインストールしないでください。
- ご使用の環境に古いバージョンのストレージ プロバイダが含まれている場合、既存の機能は継続して動作します。ただし、新しい機能を使用する場合は、ストレージ プロバイダを新しいバージョンにアップグレードしてください。
- ストレージ プロバイダを新しい VASA バージョンにアップグレードする場合は、プロバイダを登録解除してから、再度登録する必要があります。登録後、vCenter Server では新しい VASA バージョンの機能を検出し、使用できます。

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。

ストレージ プロバイダを新しい VASA バージョンにアップグレードする場合は、プロバイダを登録解除してから、再度登録する必要があります。登録後、vCenter Server では新しい VASA バージョンの機能を検出し、使用できます。

注： vSAN を使用する場合、自動的に vSAN 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。vSAN 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 vSAN 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 セキュリティ方法を指定します。

アクション	説明
vCenter Server にストレージ プロバイダ証明書をを使用するように指示する	[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する	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際に vCenter Server 証明書をトラストストアに追加します。

- 6 [OK] をクリックします。

結果

vCenter Server はストレージ プロバイダを登録し、プロバイダとのセキュアな SSL 接続を確立します。

次のステップ

ストレージ プロバイダの登録のトラブルシューティングについては、VMware ナレッジベースの記事 <https://kb.vmware.com/s/article/49798> を参照してください。

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。ストレージ プロバイダが表すエンティティ（vSAN、I/O フィルタなど）を設定すると、そのストレージ プロバイダの自己登録が行われ、自動的にリストに表示されます。

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 プロバイダを確認します。
リストには、ストレージ プロバイダの名前、その URL とステータス、VASA API のバージョン、プロバイダが表すストレージ エンティティなどの一般的な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 プロバイダまたはそのコンポーネントを選択します。

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 システムをサポートできます。

ストレージ プロバイダの登録解除

使用しないストレージ プロバイダを登録解除することができます。

ストレージ プロバイダを新しい VASA バージョンにアップグレードする場合は、プロバイダを登録解除してから、再度登録する必要があります。登録後、vCenter Server では新しい VASA バージョンの機能を検出し、使用できます。

注： vSAN ストレージ プロバイダなどの VMware が提供する一部のストレージ プロバイダは、手動で登録解除することができません。

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、[選択したストレージ プロバイダを登録解除します] (✖) アイコンをクリックします。

結果

vCenter Server により接続が終了され、その構成からストレージ プロバイダが削除されます。

ストレージ プロバイダの更新

vCenter Server はその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 とやり取りした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。

ストレージ プロバイダ証明書の更新

vCenter Server は、ストレージ プロバイダに割り当てられている証明書の有効期限が間もなく終了することを示す警告を表示します。証明書を更新すると、引き続きプロバイダを使用できます。

期限切れ前に証明書を更新しなければ、vCenter Server はプロバイダの使用を終了します。

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 リストからプロバイダを選択し、[証明書の更新] (🔄) アイコンをクリックします。

Virtual Volumes 機能により、データストア内部の容量の管理から、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。

この章には、次のトピックが含まれています。

- Virtual Volumes について
- Virtual Volumes の概念
- Virtual Volumes とストレージ プロトコル
- Virtual Volumes のアーキテクチャ
- Virtual Volumes と VMware 認証局
- スナップショットと Virtual Volumes
- Virtual Volumes を有効にする前に
- Virtual Volumes の構成
- Virtual Volumes データストア上の仮想マシンのプロビジョニング
- Virtual Volumes およびレプリケーション
- vSphere Virtual Volumes の操作のベスト プラクティス

Virtual Volumes について

Virtual Volumes 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し合います。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。従来の方では、個々の仮想マシンの要件を満たすことは困難です。

Virtual Volumes の機能は、きめ細かな設定を行うのに役立ちます。Virtual Volumes は、これまでになく方法でストレージを管理しており、仮想マシンのサービスをアプリケーション レベルで変更することが可能です。Virtual Volumes 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。

Virtual Volumes 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 Virtual Volumes 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て、ストレージ システムに伝えることができます。ストレージ システムは、これらの要件に基づいて、仮想ディスクを適切に作成します。たとえば、仮想マシンでアクティブ - アクティブのストレージアレイが必要な場合でも、アクティブ - アクティブ モデルに対応した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 Virtual Volumes を個々に作成します。

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 Virtual Volumes データストアによって表されます。Virtual Volumes データストアには、仮想マシン ファイルをカプセル化したオブジェクトである Virtual Volumes が保存されます。

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)

■ Virtual Volumes

Virtual Volumes 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。

■ Virtual Volumes とストレージ プロバイダ

VASA プロバイダとも呼ばれる Virtual Volumes 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 ベースのストレージとは異なり、Virtual Volumes 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、Virtual Volumes では、ストレージ コンテナが使用されます。このコンテナは、ストレージ システムが Virtual Volumes 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。

■ Virtual Volumes とプロトコル エンドポイントのバインドおよびバインド解除

作成時、Virtual Volumes はパッシブ エンティティで、すぐには I/O 可能にはなりません。ESXi または vCenter Server は、Virtual Volumes にアクセスするためにバインド要求を送信します。

■ Virtual Volumes データストア

Virtual Volumes (VVol) 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。

■ Virtual Volumes と仮想マシン ストレージのポリシー

Virtual Volumes 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。

Virtual Volumes

Virtual Volumes 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。

Virtual Volumes は、イーサネットまたは SAN を介して ESXi ホストに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、Virtual Volumes は一意の GUID によって識別されず、Virtual Volumes 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 Virtual Volumes 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 Virtual Volumes を作成します。

- data-VVol. 各仮想ディスクの .vmdk ファイルに直接対応するデータ Virtual Volumes。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、Virtual Volumes は仮想マシンに対して SCSI ディスクとして示されます。data-VVol は、シック プロビジョニングすることも、シン プロビジョニングすることもできます。
- config-VVol. 構成 Virtual Volumes 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 Virtual Volumes 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 Virtual Volumes は VMFS でフォーマットされます。NFS プロトコルを持つ構成 Virtual Volumes は、NFS ディレクトリとして表示されます。通常は、シン プロビジョニングされます。
- swap-VVol. 仮想マシンを最初にパワーオンしたときに作成されます。これは、メモリに保持できない仮想マシン メモリ ページのコピーを保持する Virtual Volumes です。そのサイズは、仮想マシンのメモリ サイズによって決まります。デフォルトでは、シック プロビジョニングされます。
- snapshot-VVol. スナップショットのために仮想マシンのメモリ内容を保持する仮想メモリ ボリューム。シック プロビジョニングされます。

- その他。特定の機能用の Virtual Volumes。たとえば、CBRC (Content-Based Read Cache) 用には、ダイジェスト Virtual Volumes が作成されます。

通常、仮想マシンでは、最低限、data-VVol、config-VVol、および swap-VVol という 3 つの Virtual Volumes が作成されます。作成される Virtual Volumes の最大数は、仮想マシンに存在している仮想ディスクおよびスナップショットの数によって決まります。

たとえば、次の SQL サーバには、6 つの Virtual Volumes があります。

- config-VVol
- オペレーティング システム用の data-VVol
- データベース用の data-VVol
- ログ用の data-VVol
- パワーオン時の swap-VVol
- snapshot-VVol

異なる仮想マシン コンポーネントに対して異なる Virtual Volumes 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、仮想ディスクを含む Virtual Volumes には、仮想マシン起動ディスクの Virtual Volumes よりも豊富なサービスを含めることができます。同様に、スナップショット Virtual Volumes では、現在の Virtual Volumes と異なるストレージ階層を使用できます。

Virtual Volumes とストレージ プロバイダ

VASA プロバイダとも呼ばれる Virtual Volumes 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、Virtual Volumes 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 コンテナからの情報を提供します。ストレージ コンテナの容量は、vCenter Server および vSphere Web Client に表示されます。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 Virtual Volumes 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、Virtual Volumes 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。Virtual Volumes ストレージ プロバイダをデプロイし、現在の ESXi リリースと互換性のあるバージョンにアップグレードする方法については、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 ベースのストレージとは異なり、Virtual Volumes 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、Virtual Volumes では、ストレージ コンテナが使用されます。このコンテナは、ストレージ システムが Virtual Volumes 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 Virtual Volumes 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 Virtual Volumes を含めることができます。各ストレージ コンテナは Virtual Volumes ストアとして機能し、Virtual Volumes 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。ストレージ システムごとに少なくとも 1 つのコンテナが必要です。

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 コンテナが、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 コンテナに含めることができます。

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 Virtual Volumes 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 システムには、わずかなプロトコル エンドポイントしか必要ありません。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 ファブリックの一部です。ストレージ システムは、プロトコル エンドポイントを、関連するストレージ コンテナと一緒にストレージ プロバイダを介してエクスポートします。そのストレージ コンテナを Virtual Volumes データストアにマッピングすると、プロトコル エンドポイントは ESXi ホストによって検出され、vSphere Web Client に表示されます。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検出することもできます。複数のホストが、プロトコル エンドポイントを検出し、マウントすることができます。

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プロキシ 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。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。

プロトコル エンドポイントは、アレイごとに管理されます。ESXi と vCenter Server では、アレイに対して報告されたすべてのプロトコル エンドポイントが、そのアレイ上のすべてのコンテナに関連付けられていることを前提としています。たとえば、アレイに2つのコンテナと3つのプロトコル エンドポイントがある場合、ESXi では、両方のコンテナの Virtual Volumes が、3つのプロトコル エンドポイントすべてにバインドできるものと見なします。

Virtual Volumes とプロトコル エンドポイントのバインドおよびバインド解除

作成時、Virtual Volumes はパッシブ エンティティで、すぐには I/O 可能にはなりません。ESXi または vCenter Server は、Virtual Volumes にアクセスするためにバインド要求を送信します。

この要求に対するストレージ システムの応答には、Virtual Volumes へのアクセス ポイントとなるプロトコル エンドポイント ID が含まれます。プロトコル エンドポイントは、Virtual Volumes へのすべての I/O 要求を受け入れます。このバインドは、ESXi が、Virtual Volumes に対するバインド解除要求を送信するまで存在します。

その後、同じ Virtual Volumes でバインド要求が送信されると、ストレージ システムは、別のプロトコル エンドポイント ID を返すことができます。

Virtual Volumes への同時バインド要求を複数の ESXi ホストから受け取ると、ストレージ システムは、同じエンドポイント バインドまたはさまざまなエンドポイント バインドを、要求の送信元である ESXi ホストそれぞれに返すことができます。つまり、ストレージ システムは、同時要求を行ったさまざまなホストを、さまざまなエンドポイントを使用して同じ Virtual Volumes にバインドできます。

バインド解除操作により、Virtual Volumes の I/O アクセス ポイントが削除されます。ストレージ システムは、Virtual Volumes のバインドを、プロトコル エンドポイントからすぐに、または後から解除して、他のアクションを実行できます。バインドされた Virtual Volumes を削除するには、まず、バインドを解除する必要があります。

Virtual Volumes データストア

Virtual Volumes (VVOL) 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。

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 vCenter Server が検出した後は、それらを Virtual Volumes データストアとしてマウントする必要があります。Virtual Volumes データストアは、VMFS データストアなどの従来の方法ではフォーマットされていません。ただし、vSphere のすべての機能 (FT、HA、DRS など) を使用するにはデータストア構成が正常に機能する必要があるため、依然として Virtual Volumes データストアを作成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 Virtual Volumes データストアにマッピングします。作成する Virtual Volumes 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ます。データストアは、vCenter Server および vSphere Web Client におけるコンテナです。

vSphere 管理者の観点からすると、Virtual Volumes 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、Virtual Volumes データストアは、参照することができ、仮想マシン名別に Virtual Volumes の一覧が表示されます。また従来のデータストアと同様、Virtual Volumes 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、Virtual Volumes データストアには適用できません。Virtual Volumes データストアのキャパシティは、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 vSAN を使用する Virtual Volumes データストアを使用できません。

注： Virtual Volumes 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。このため、Virtual Volumes 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。Virtual Volumes 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拡張します。

Virtual Volumes と仮想マシン ストレージのポリシー

Virtual Volumes 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、Virtual Volumes 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、Virtual Volumes 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、Virtual Volumes ストレージの要件準拠が強制されます。

Virtual Volumes 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 Virtual Volumes ポリシーです。このポリシーでは、Virtual Volumes 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。

Virtual Volumes とストレージ プロトコル

Virtual Volumes ベースのストレージ システムは、物理ストレージ ファブリック上で検出可能なプロトコル エンドポイントです。ESXi ホストは、プロトコル エンドポイントを使用して、ストレージ上の Virtual Volumes に接続します。プロトコル エンドポイントの操作は、エンドポイントを ESXi ホストに公開するストレージ プロトコルによって異なります。

Virtual Volumes では、NFS バージョン 3 とバージョン 4.1、iSCSI、ファイバ チャネル、FCoE がサポートされます。

使用されているストレージ プロトコルにかかわらず、プロトコル エンドポイントを経由すると、SAN と NAS のどちらのストレージにも同じ方法でアクセスできます。他の従来型データストアのファイルと同様、Virtual Volumes は、仮想マシンでは SCSI ディスクとして認識されます。

注： ストレージ コンテナは、SCSI または NAS 専用であるため、これらのプロトコル タイプで共有することはできません。1つのアレイでは、SCSI プロトコル エンドポイントを含む1つのストレージ コンテナと、NFS プロトコル エンドポイントを含む別の1つのコンテナを提供できます。コンテナでは、プロトコル エンドポイントの SCSI と NFS を組み合わせて使用することはできません。

Virtual Volumes および SCSI ベースの転送

ディスク アレイで Virtual Volumes は、ファイバ チャネル、FCoE、および iSCSI プロトコルをサポートします。

SCSI ベースのプロトコルを使用すると、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プロキシ LUN を表します。

ブロックベースの LUN と同様に、プロトコル エンドポイントは標準の LUN 検出コマンドを使用して検出されません。ESXi ホストは、新しいデバイスがないか定期的に再スキャンを実行し、ブロックベースのプロトコル エンドポイントを非同期で検出します。プロトコル エンドポイントは、複数のパスでアクセスできます。これらのパスのトラフィックは、LUN で標準的な既知のパス選択ポリシーに従います。

SCSI ベースのディスク アレイで、仮想マシンの作成時、ESXi は、Virtual Volumes を作成し、VMFS としてフォーマットします。この小さな Virtual Volumes は、すべての仮想マシン メタデータ ファイルを保存するもので、config-VVol と呼ばれます。config-VVol は、vSphere の仮想マシン ストレージ ロケータとして機能します。

ディスク アレイ上の Virtual Volumes 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。

Virtual Volumes および NFS の転送

NAS ストレージの場合、プロトコル エンドポイントは、ESXi ホストが IP アドレスまたは DNS 名と共有名を使用してマウントする NFS 共有です。Virtual Volumes では、NAS ストレージにアクセスするために NFS バージョン 3 とバージョン 4.1 がサポートされています。IPv4 および IPv6 の両方の形式がサポートされています。

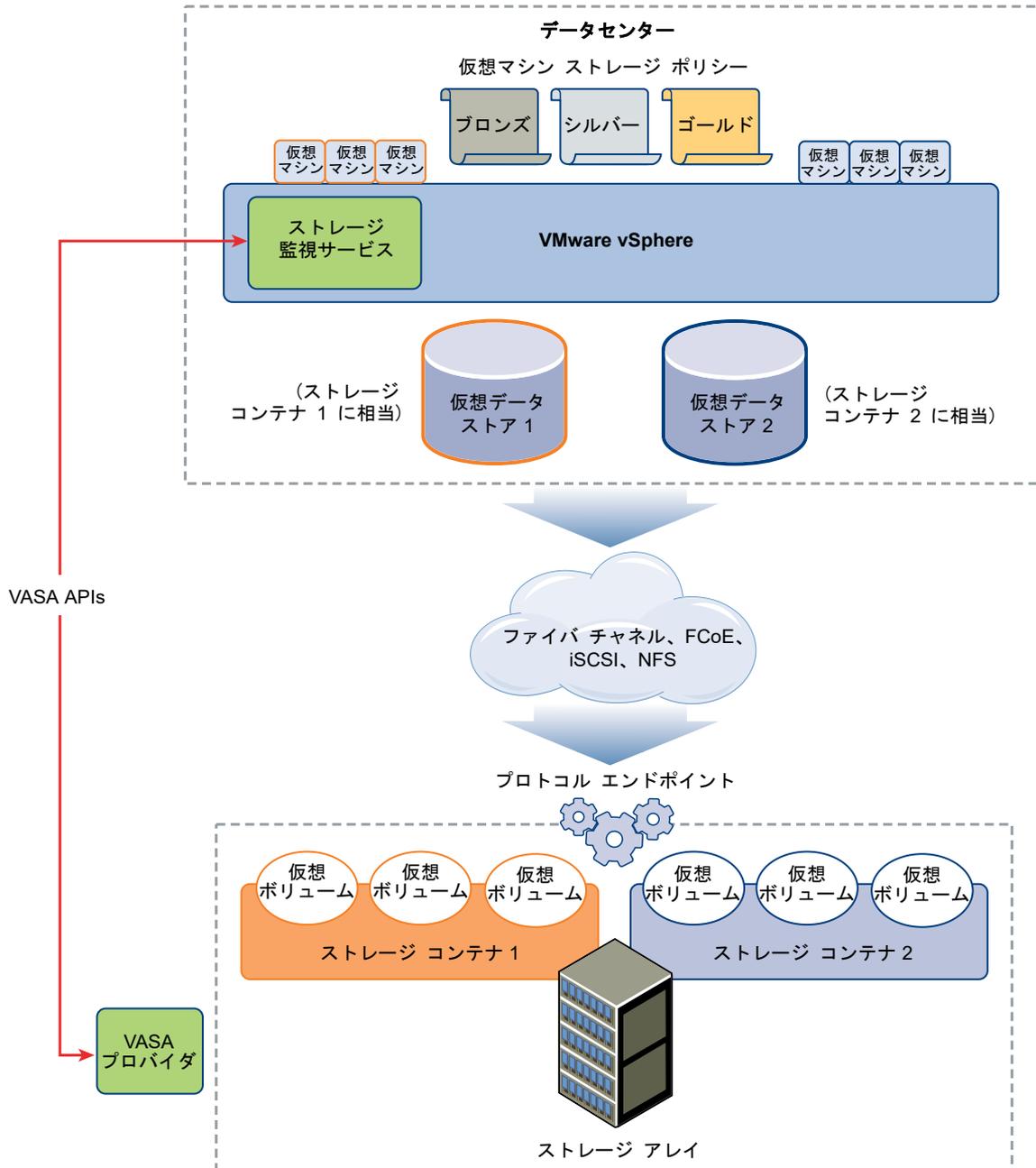
使用するバージョンに関係なく、ストレージ アレイでは、可用性を高める目的で複数のプロトコル エンドポイントを提供できます。

NAS デバイス上の Virtual Volumes では、NFS マウント ポイントへの接続時に ESXi ホストが使用するのと同じ NFS リモート プロシージャ コール (RPC) がサポートされます。

NAS デバイスで、config-VVol は、config-VVolID に対応するディレクトリ サブツリーです。config-VVol は、NFS で必要なディレクトリやその他の操作をサポートする必要があります。

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 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 エンドポイントは、仮想マシンから各 Virtual Volumes へのデータ パスを要求に応じて確立します。プロトコル エンドポイントは、ESXi ホストとストレージ システム間の直接的なインバンド 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。vCenter Server および ESXi の側では、ストレージ コンテナは、Virtual Volumes データストアとして表されます。単一のストレージ コンテナで、複数のストレージ機能セットをエクスポートし、さまざまなレベルのサービスを各種の Virtual Volumes に提供できます。

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)

Virtual Volumes と VMware 認証局

証明書は、自己生成および自己署名されたものか、外部の認証局から取得したものを使用します。vSphere には、VMware 認証局 (VMCA) が含まれています。デフォルトでは、vSphere 環境で使用されるすべての内部証明書は VMCA が作成します。新しく追加された ESXi ホスト向け、および Virtual Volumes ストレージ システムを管理または提供するストレージ VASA プロバイダ向けに証明書を生成します。

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。

- 長期にわたって使用する証明書は、VASA プロバイダから直接取得することを検討してください。証明書は、自己生成および自己署名されたものか、外部の認証局から取得したものを使用します。
- VASA プロバイダで使用する証明書は、VMCA で生成できます。

ホストまたは VASA プロバイダが登録されている場合、VMCA は vSphere 管理者の介入なしで、これらを自動的に使用します。

- 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 CSR を VMCA に渡し、CA 署名証明書を要求します。

VMCA はスタンドアロン認証局 (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 は完全な証明書チェーンで CSR に署名します。

- 4 ルート証明書によって署名された証明書が、VASA プロバイダに渡されます。VASA プロバイダは、vCenter Server 上および ESXi ホスト上にある SMS からの今後すべてのセキュアな接続を認証することができます。

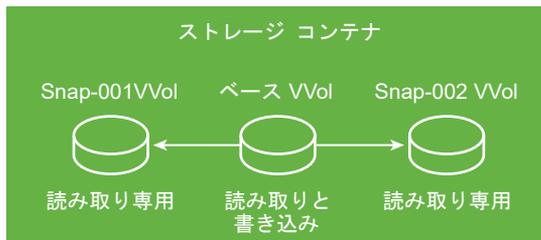
スナップショットと Virtual Volumes

スナップショットには、スナップショット作成時の仮想マシンの状態とデータが保存されます。スナップショットは、繰り返し同じ状態の仮想マシンに戻る必要があるが、複数の仮想マシンを作成したくないという場合に便利です。

Virtual Volumes スナップショットには目的が多数あります。バックアップやアーカイブの目的で静止コピーを作成したり、アプリケーションのテストおよびロールバック環境を作成したりすることができます。また、アプリケーションイメージを短時間でプロビジョニングする目的に使用することもできます。

Virtual Volumes 環境では、スナップショットを管理するのは ESXi と vCenter Server ですが、実行するのはストレージ アレイです。

各スナップショットによって、追加の Virtual Volumes オブジェクト、スナップショット（メモリ）Virtual Volumes が作成され、これに仮想マシンのメモリのコンテンツが保存されます。元の仮想マシンのデータはこのオブジェクトにコピーされ、読み取り専用の状態が保持されるため、ゲスト OS はスナップショットに書き込まれません。スナップショット Virtual Volumes のサイズは変更できません。また、このスナップショット Virtual Volumes は、仮想マシンがスナップショットに戻されたときにのみ読み取ることができます。通常は、仮想マシンをレプリケートすると、そのスナップショット Virtual Volumes もレプリケートされます。



基本 Virtual Volumes はアクティブのままです。つまり、読み取り/書き込みが可能です。他のスナップショットが作成されると、そのスナップショットには、新しい状態と、スナップショットを作成したときの仮想マシンのデータが保持されます。

スナップショットを削除すると、最新状態の仮想マシンを表す基本 Virtual Volumes が残り、スナップショット Virtual Volumes は破棄されます。従来のデータストアのスナップショットとは異なり、Virtual Volumes スナップショットは、そのコンテンツを基本 Virtual Volumes にコミットする必要はありません。



スナップショットの作成と管理の詳細については、『vSphere の仮想マシン管理』ドキュメントを参照してください。

Virtual Volumes を有効にする前に

Virtual Volumes 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。

Virtual Volumes のストレージ システムを準備する

Virtual Volumes のストレージ システム環境を準備するには、次のガイドラインに従います。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。

- 使用するストレージ システムまたはストレージ アレイは、Virtual Volumes をサポートし、vSphere APIs for Storage Awareness (VASA) を介して vSphere コンポーネントと統合する必要があります。ストレージ アレイは、シン プロビジョニングおよびスナップショットの作成をサポートする必要があります。
- Virtual Volumes 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。
- 次のコンポーネントが、ストレージ側で構成されている必要があります。
 - プロトコル エンドポイント
 - ストレージ コンテナ
 - ストレージ プロファイル
 - レプリケーションで Virtual Volumes を使用する場合は、レプリケーション構成。Virtual Volumes でのレプリケーションの要件を参照してください。

vSphere 環境を準備する

- 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、Virtual Volumes ストレージ システムの 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。
- 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。

詳細については、ベンダーにお問い合わせするか、VMware 互換性ガイドを参照してください。

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 を使用する場合は、ネットワーク タイム 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 Web Client ナビゲータで、ホストを参照して移動します。
- 2 [設定] タブをクリックします。
- 3 [システム] で [時間の設定] 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。

Virtual Volumes の構成

Virtual Volumes 環境を構成するには、いくつかの手順に従います。

前提条件

Virtual Volumes を有効にする前のガイドラインに従います。

手順

1 Virtual Volumes のストレージ プロバイダの登録

Virtual Volumes 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、Virtual Volumes を操作できるようにする必要があります。

2 Virtual Volumes 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、Virtual Volumes 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、Virtual Volumes および Virtual Volumes 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 Virtual Volumes 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、Virtual Volumes 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 の仮想マシン管理』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 の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。

Virtual Volumes のストレージ プロバイダの登録

Virtual Volumes 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、Virtual Volumes を操作できるようにする必要があります。

登録後、Virtual Volumes プロバイダは vCenter Server と通信します。ストレージ システムが提供するレプリケーションなどの基盤のストレージ サービスとデータ サービスの特性がプロバイダによってレポートされます。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、Virtual Volumes 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 Virtual Volumes ストレージにプッシュされます。このポリシーにより、Virtual Volumes 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。ストレージがキャッシュやレプリケーションなどの追加のサービスを提供する場合は、ポリシーを通じてこれらのサービスが仮想マシンに対して有効になります。

前提条件

ストレージ側に適切なバージョンの Virtual Volumes ストレージ プロバイダがインストールされていることを確認します。ストレージ プロバイダの認証情報を取得します。

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 セキュリティ方法を指定します。

アクション	説明
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する	[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する	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際に vCenter Server 証明書をトラストストアに追加します。

- 6 登録を完了するには、[OK] をクリックします。

結果

vCenter Server は、Virtual Volumes ストレージ プロバイダを検出して登録します。

Virtual Volumes 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、Virtual Volumes 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 データベースの配置場所を指定します。
- 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、データストア名を入力します。
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 Virtual Volumes 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。
- 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

Virtual Volumes 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。

Virtual Volumes 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 プロキシを使用して、Virtual Volumes および Virtual Volumes 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 Virtual Volumes 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 [ストレージ] で、[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 Virtual Volumes 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 [ストレージ] で、[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。

選択できるパス ポリシーは、ストレージ ベンダーのサポート状況によって異なります。

- 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。

Virtual Volumes データストア上の仮想マシンのプロビジョニング

Virtual Volumes 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： Virtual Volumes 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。

Virtual Volumes 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 の仮想マシン管理』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 の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

Virtual Volumes のストレージ ポリシーはデフォルトで [要件なし] に設定されています。必要な場合は、Virtual Volumes と互換性のあるカスタム ストレージ ポリシーを作成できます。

2 仮想マシンへの Virtual Volumes 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、Virtual Volumes 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、Virtual Volumes ストレージ ポリシーを仮想マシンに関連付けます。

3 Virtual Volumes 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、Virtual Volumes 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

Virtual Volumes のストレージ ポリシーはデフォルトで [要件なし] に設定されています。必要な場合は、Virtual Volumes と互換性のあるカスタム 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。Virtual Volumes のストレージ プロバイダの登録を参照してください。
- 仮想マシン ストレージ ポリシー インターフェイスに、ストレージ環境で使用可能なストレージ エンティティとデータ サービスに関する情報が入力され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 インターフェイスの入力を参照してください。
- 適切なストレージ ポリシーのコンポーネントを定義します。ストレージ ポリシー コンポーネントの作成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 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] タブをクリックします。
- 3 [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。
- 4 vCenter Server インスタンスを選択します。
- 5 ストレージ ポリシーの名前と説明を入力します。

6 [ルール セット] ページで、配置ルールを定義します。

- a [ストレージ タイプ] ドロップダウン メニューから、Virtual Volumes などのターゲット ストレージ エンティティを選択します。
- b [ルールの追加] ドロップダウン メニューから、機能を選択してその値を指定します。

たとえば、Virtual Volumes オブジェクトの 1 秒あたりの読み取り操作数を指定できます。選択したストレージ エンティティに必要な数のルールを含めることができます。入力する値が、ストレージ リソースがアダプタイズする値の範囲内であることを確認します。

- c (オプション) 配置要求を微調整するには、タグベースのルールを追加します。

タグベースのルールでは、特定の配置基準を含めたり除外したりできます。たとえば、ターゲット Virtual Volumes データストアのリストから Palo Alto タグの付いたデータストアを除外することができます。

7 (オプション) 仮想マシン ストレージ ポリシーに含めるデータ サービスを選択します。

[ルール セット] ページで参照するデータ サービスはストレージによって提供されます。データ サービスを参照する仮想マシン ストレージ ポリシーは、仮想マシンについてこれらのデータ サービスを要求します。

- a [コンポーネントの追加] (+) アイコンをクリックし、ドロップダウン メニューからデータ サービス カテゴリを選択します (レプリケーションなど)。
- b ルールに対して適切なプロバイダと値を指定することによって、データ サービス カテゴリのルールを定義します。または、事前定義済みコンポーネントのリストからデータ サービスを選択します。

オプション	説明
 Component Name	このオプションは、データベースにストレージ ポリシーのコンポーネントを事前定義している場合に使用できます。使用するコンポーネントがわかっている場合は、リストでそれを選択して仮想マシン ストレージ ポリシーに追加します。
すべて表示	カテゴリで使用できるすべてのコンポーネントを確認します。特定のコンポーネントを含める場合は、リストでそれを選択し、[OK] をクリックします。
カスタム	ルールに対して適切なプロバイダと値を指定して、データ サービス カテゴリのカスタムルールを定義します。

- c さらにコンポーネントを追加して、他のデータ サービスを要求します。

共通または通常のルール セットごとに、同じカテゴリ (キャッシュなど) から使用できるコンポーネントは 1 つのみです。

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

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 Virtual Volumes 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、Virtual Volumes 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、Virtual Volumes ストレージ ポリシーを仮想マシンに関連付けます。

Virtual Volumes 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 Virtual Volumes ストレージ ポリシーを割り当てす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 の仮想マシン管理』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 Virtual Volumes 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 Virtual Volumes データストアを選択します。
 - c Virtual Volumes でレプリケーション サービスを使用する場合は、レプリケーション グループを指定します。

レプリケーション グループは、ターゲット サイトにまとめてレプリケートする必要のある仮想マシンと仮想ディスクを示します。

オプション	説明
事前構成済みレプリケーション グループ	ストレージ側で事前に構成されたレプリケーション グループ。vCenter Server および ESXi では、レプリケーション グループは検出されますが、レプリケーション グループのライフサイクルは管理されません。
自動レプリケーション グループ	Virtual Volumes によって、レプリケーション グループが作成され、すべての仮想マシン オブジェクトがこのグループに割り当てられます。

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。
- c レプリケーションの場合は、レプリケーション グループを指定するか、変更します。仮想マシンの自動レプリケーション グループを使用している場合は、グループを仮想ディスクの事前構成済みグループに変更することはできません。

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。

Virtual Volumes 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、Virtual Volumes 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

Virtual Volumes 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 Virtual Volumes データストアを参照します。
- 2 [設定] タブをクリックします。
- 3 [設定] で、[全般] をクリックします。
- 4 [デフォルト ストレージ ポリシー] ペインで [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 ポリシーが Virtual Volumes データストアのデフォルト ポリシーになります。vSphere では他のポリシーが明示的に選択されていない場合に、Virtual Volumes 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。

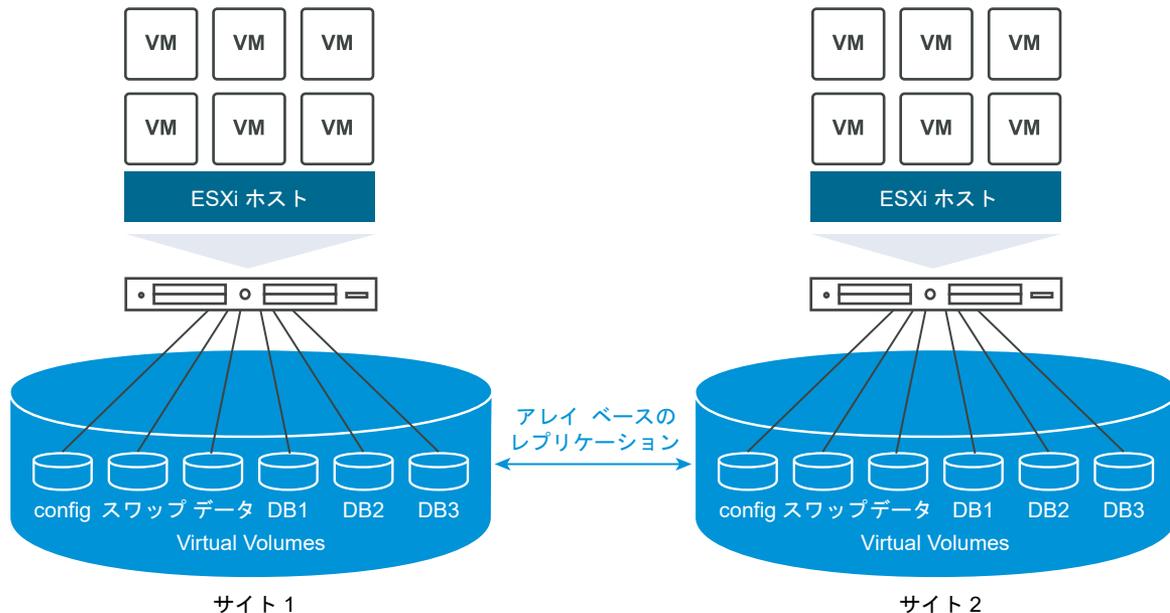
Virtual Volumes およびレプリケーション

Virtual Volumes では、レプリケーションとディザスタ リカバリがサポートされています。アレイベースのレプリケーションでは、仮想マシンのレプリケーションをストレージ アレイにオフロードし、そのアレイのすべてのレプリケーション機能を利用できます。仮想ディスクなど、単一の仮想マシン オブジェクトをレプリケートすることができます。また、複数の仮想マシン オブジェクトや仮想マシンをグループ化して、それらを単一のユニットとしてレプリケートすることもできます。

アレイ ベースのレプリケーションは、ポリシーに基づいて実行されます。Virtual Volumes ストレージをレプリケーション用に構成した後、アレイから、レプリケーション機能およびレプリケーション グループに関する情報がストレージ プロバイダによって送信されます。この情報は、vCenter Server 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。

仮想マシン ストレージ ポリシーは、仮想マシンのレプリケーション要件を記述するために使用します。ストレージ ポリシーに指定するパラメータは、アレイのレプリケーションの実装方法によって異なります。たとえば、仮想マシン ストレージ ポリシーでは、レプリケーションのスケジュール、レプリケーションの頻度、目標復旧時点 (RPO) などのパラメータを指定します。また、レプリケーション ターゲット (仮想マシンのレプリケート先のセカンダリ サイト) や、レプリカを削除する必要があるかどうかも指定します。

仮想マシンのレプリケーション サービスを要求するには、仮想マシンのプロビジョニング時にレプリケーション ポリシーを割り当てます。この操作が行われた後、アレイは、すべてのレプリケーションのスケジュールとプロセスの管理を引き継ぎます。



Virtual Volumes でのレプリケーションの要件

Virtual Volumes でレプリケーションを行えるようにする場合は、Virtual Volumes の一般的な要件のほかに、特定の要件をいくつか満たす必要があります。

Virtual Volumes の要件については、[Virtual Volumes を有効にする前に](#)を参照してください。

ストレージ要件

Virtual Volumes レプリケーションの実装はアレイに依存しており、ストレージ ベンダーによって異なる場合があります。すべてのベンダーに適用される一般的な要件を次に示します。

- レプリケーションの実装に使用するストレージ アレイが、Virtual Volumes に対応していなければなりません。
- Virtual Volumes レプリケーションと互換性があるストレージ (VASA) プロバイダに、アレイが統合されている必要があります。
- ストレージ アレイがレプリケーションに対応しており、ベンダーが提供するレプリケーション メカニズムを使用するように構成されている必要があります。標準的な構成には、通常、1つ以上のレプリケーション ターゲットが含まれます。レプリケートされたサイトとターゲット サイトのペアリングなど、必要な構成すべてをストレージ側で行う必要があります。
- 該当する場合は、Virtual Volumes のレプリケーション グループとフォールト ドメインを、ストレージ側で事前構成する必要があります。

詳細については、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。

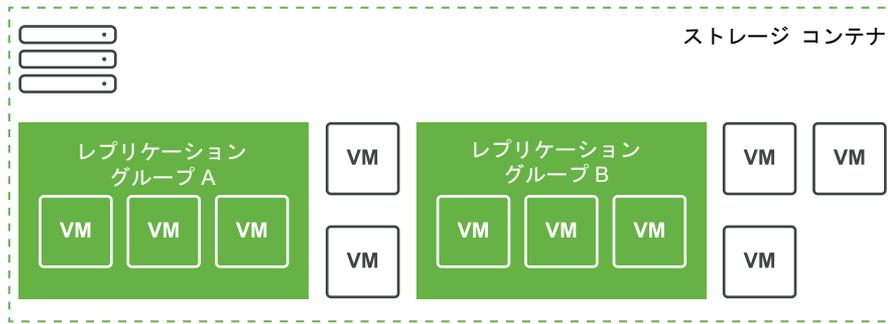
vSphere の要件

- Virtual Volumes のストレージ レプリケーションをサポートする vCenter Server および ESXi バージョンを使用します。6.5 リリースより前の vCenter Server および ESXi ホストでは、レプリケートされた Virtual Volumes ストレージがサポートされません。レプリケートされた仮想マシンを互換性のないホストで作成しようとすると、エラーが発生します。詳細については、『VMware 互換性ガイド』を参照してください。
- 仮想マシンを移行する場合は、ESXi ホスト、Virtual Volumes データストアなどのターゲット リソースによって、ストレージ レプリケーションがサポートされていることを確認します。

Virtual Volumes とレプリケーション グループ

ストレージ コンテナとプロトコル エンドポイントのほかに、レプリケーション サービスがストレージに用意されている場合、ストレージ管理者は、ストレージ側でレプリケーション グループを構成できます。

vCenter Server および ESXi では、レプリケーション グループを検出できますが、レプリケーション グループのライフサイクルは管理されません。コンシステンシ グループとも呼ばれるレプリケーション グループは、どの仮想マシンと仮想ディスクを、ターゲット サイトにまとめてレプリケートする必要があるかを示します。同じ仮想マシンにある仮想マシン構成ファイル、仮想ディスクなどのコンポーネントを、さまざまな事前構成済みレプリケーション グループに割り当てることができます。または、レプリケーションから特定の仮想マシン コンポーネントを除外します。



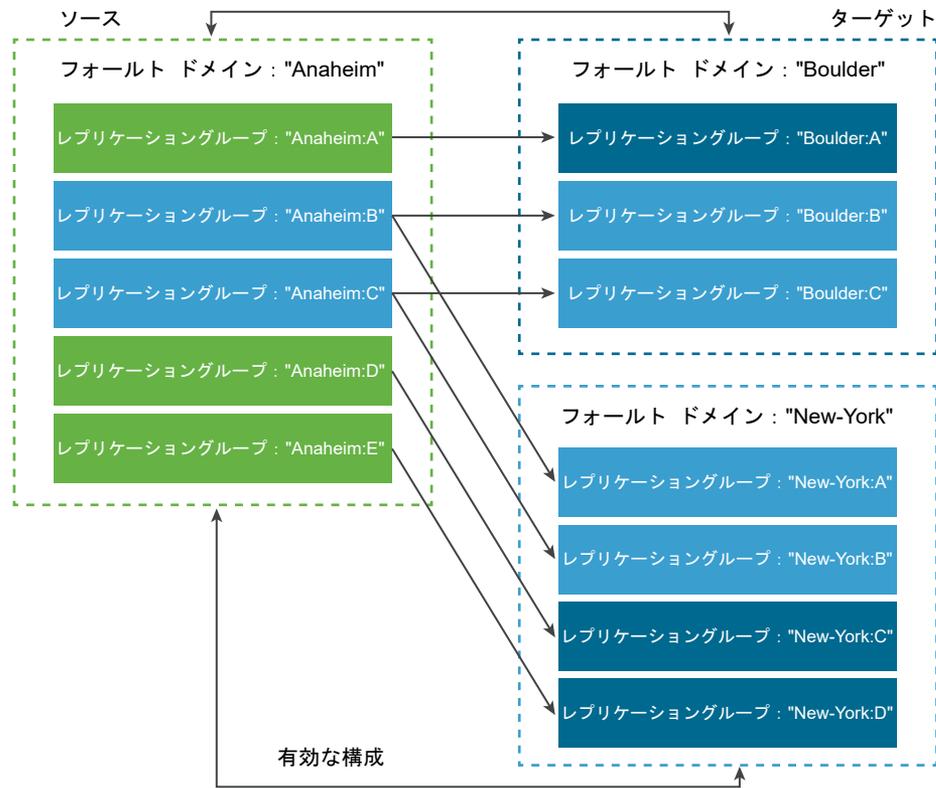
使用できる事前構成済みグループがない場合、Virtual Volumes は自動オプションを使用できます。自動オプションを使用すると、レプリケーション グループが、Virtual Volumes によって必要に応じて作成され、プロビジョニング中の Virtual Volumes オブジェクトに関連付けられます。自動レプリケーション グループを使用すると、そのグループには、仮想マシンのすべてのコンポーネントが割り当てられます。同じ仮想マシンのコンポーネントで、事前構成済みレプリケーション グループと自動レプリケーション グループを混在させることはできません。

Virtual Volumes および障害ドメイン

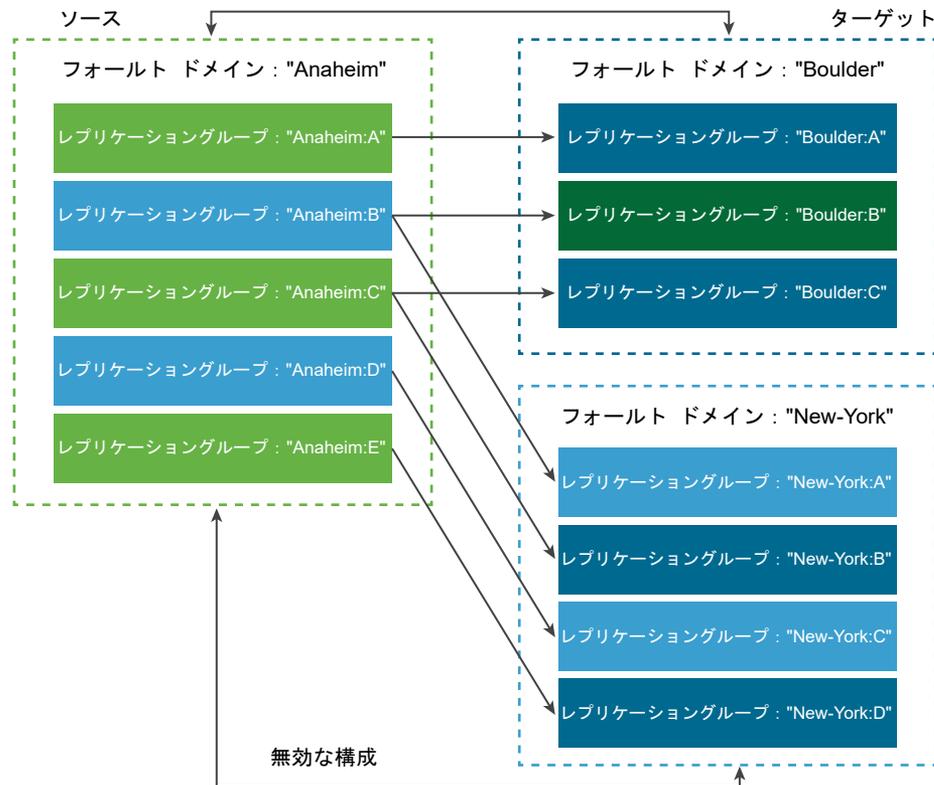
Virtual Volumes 環境の場合、障害ドメインでは、ソースからターゲット サイトへのレプリケート時に特定のレプリケーション グループをどのように組み合わせる必要があるかを定義します。

障害ドメインは、ストレージ アレイによって構成および報告されます。vSphere Web Client では公開されません。仮想マシンの作成時、SPBM (Storage Policy Based Management) メカニズムにより、障害ドメインが検出され、それを使用して検証が行われます。

たとえば、1 台の仮想マシンと 2 台のディスクをプロビジョニングします。一方のディスクはレプリケーション グループ Anaheim:B に、もう一方のディスクはレプリケーション グループ Anaheim:C に関連付けられています。両方のディスクが同じターゲット障害ドメインにレプリケートされるため、SPBM はプロビジョニングを検証します。



次に、別の 1 台の仮想マシンと 2 台のディスクをプロビジョニングします。一方のディスクはレプリケーショングループ Anaheim:B に、もう一方のディスクはレプリケーショングループ Anaheim:D に関連付けられています。この構成は無効です。両方のレプリケーショングループがニューヨークの障害ドメインにレプリケートされますが、1つのレプリケーショングループのみボルダーの障害ドメインにレプリケートされます。



Virtual Volumes レプリケーションのワークフロー

Virtual Volumes ストレージ アレイのレプリケーション機能に関する情報が vCenter Server に表示されている場合は、仮想マシンのレプリケーションをアクティベートできます。

仮想マシンのレプリケーションをアクティベートするワークフローには、Virtual Volumes ストレージにおける仮想マシンの標準的なプロビジョニング手順が含まれます。

- 1 レプリケーション ストレージと互換性のある仮想マシン ストレージ ポリシーを定義します。ポリシーには、[ルール セット] ページのレプリケーション コンポーネントを含める必要があります。Virtual Volumes の仮想マシン ストレージ ポリシーの定義を参照してください。

レプリケーションが含まれるストレージ ポリシーを構成すると、使用できるレプリケーション グループが vCenter Server によって検出されます。

- 2 レプリケーション ポリシーを仮想マシンに割り当てます。構成されている場合は、互換性のあるレプリケーション グループを選択するか、自動割り当てを使用します。仮想マシンへの Virtual Volumes ストレージ ポリシーの割り当てを参照してください。

レプリケーションのガイドラインと考慮事項

Virtual Volumes でレプリケーションを使用する場合は、特定の考慮事項が適用されます。

- レプリケーション ストレージ ポリシーは、構成 Virtual Volumes とデータ Virtual Volumes にのみ適用できます。他の仮想マシン オブジェクトについては、次の方法でレプリケーション ポリシーを継承します。
 - メモリ Virtual Volumes は、構成 Virtual Volumes のポリシーを継承します。

- ダイジェスト Virtual Volumes は、データ Virtual Volumes のポリシーを継承します。
- スワップ Virtual Volumes は、仮想マシンがパワーオンのときに存在し、レプリケーションから除外されます。
- レプリケーション ポリシーを仮想マシンに割り当てない場合、ディスクはレプリケートされません。
- レプリケーション ストレージ ポリシーは、データストアのデフォルトのストレージ ポリシーとして使用しないでください。指定すると、レプリケーション グループを選択できなくなります。
- レプリケーションには、スナップショットの履歴が保持されます。スナップショットが作成され、レプリケートされると、アプリケーション コンシステントなスナップショットに復旧できます。
- リンク クローンをレプリケートできます。親なしでリンク クローンがレプリケートされると、そのリンク クローンは完全クローンになります。
- ディスクリプタ ファイルが、ある仮想マシンの仮想ディスクに属していながら、別の仮想マシンの仮想マシン ホームに配置されている場合は、両方の仮想マシンが同じレプリケーション グループに属している必要があります。仮想マシンがそれぞれ別のレプリケーション グループに配置されている場合は、両方のレプリケーション グループが同時にフェイルオーバーしなければなりません。そうしないと、ディスクリプタは、フェイルオーバーの後に使用できなくなる可能性があります。結果として、仮想マシンがパワーオンにならない場合があります。
- レプリケーション環境が構成された Virtual Volumes では、フェイルオーバー後にリカバリされたワークロードが確実に機能できるようにするために、テスト フェイルオーバー ワークフローを定期的に行うことができます。

テスト フェイルオーバー中に作成されたテスト仮想マシンは、一般的な管理操作では正常に機能して安定しますが、以下の考慮事項があります。

- テスト フェイルオーバー中に作成された仮想マシンは、テスト フェイルオーバーが停止する前にすべて削除する必要があります。これにより、仮想マシンに含まれているスナップショットや、スナップショット Virtual Volumes などのスナップショット関連の Virtual Volumes が、テスト フェイルオーバーの停止を妨げるのを回避できます。
- テスト仮想マシンの完全クローンを作成できます。
- 高速クローンを作成できるのは、新規の仮想マシンに適用されるポリシーに、クローン作成元の仮想マシンと同じレプリケーション グループ ID が含まれている場合に限られます。親仮想マシンのレプリケーション グループの外に子仮想マシンを配置しようとすると失敗します。

vSphere Virtual Volumes の操作のベスト プラクティス

ESXi と vCenter Server で Virtual Volumes を使用する場合、次の推奨事項を確認してください。

- [vSphere Virtual Volumes の使用上のガイドラインと制限事項](#)
vSphere Virtual Volumes 機能を最大限活用するには、特定のガイドラインに従う必要があります。
- [ストレージ コンテナのプロビジョニングのベスト プラクティス](#)
ストレージ コンテナを vSphere Virtual Volumes アレイ側にプロビジョニングする場合、次のベスト プラクティスに従ってください。
- [vSphere Virtual Volumes のパフォーマンスのベスト プラクティス](#)
vSphere Virtual Volumes で最適なパフォーマンスを確保するには、次の推奨事項を実行します。

vSphere Virtual Volumes の使用上のガイドラインと制限事項

vSphere Virtual Volumes 機能を最大限活用するには、特定のガイドラインに従う必要があります。

Virtual Volumes では、次の機能と VMware 製品がサポートされます。

- Virtual Volumes を使用すると、レプリケーション、暗号化、重複解除、圧縮などの高度なストレージ サービスを個々の仮想ディスクで使用できます。Virtual Volumes で対応するサービスについては、ストレージ メーカーにお問い合わせください。
- Virtual Volumes 機能では、vSphere APIs - Data Protection 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。Virtual Volumes は仮想ディスク上でモデル化されます。vSphere APIs - Data Protection を使用するバックアップ製品は、LUN の VMDK ファイル上と同様に Virtual Volumes でも完全にサポートされます。vSphere APIs - Data Protection を使用してバックアップソフトウェアで作成されるスナップショットは、vSphere とバックアップソフトウェアに非 VVol スナップショットとして認識されます。

注: vSphere Virtual Volumes では、SAN 転送モードがサポートされていません。vSphere APIs - Data Protection によって別のデータ転送方法が自動的に選択されます。

vSphere Storage APIs - Data Protection と利用中のバックアップソフトウェアの連携の詳細については、ソフトウェアのメーカーにご確認ください。

- Virtual Volumes では、vSphere vMotion、Storage vMotion、スナップショット、リンク クローン、vSphere Flash Read Cache、および DRS などの vSphere 機能がサポートされています。
- Virtual Volumes では、Oracle Real Application Clusters などのクラスタリング製品を使用できます。これらの製品を使用するには、VVol データストアに保存された仮想ディスクの複数書き込み設定を有効化します。

詳細については、<http://kb.vmware.com/kb/2112039> のナレッジベースの記事を参照してください。Virtual Volumes の機能でサポートされる機能と製品の一覧については、『VMware 製品の相互運用性マトリックス』を参照してください。

vSphere Virtual Volumes の制限事項

vSphere Virtual Volumes を活用するために、次の制限事項を確認してください。

- Virtual Volumes 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 Virtual Volumes を使用することはできません。
- Virtual Volumes 機能は、RDM をサポートしません。
- Virtual Volumes ストレージ コンテナは、複数の物理アレイにまたがることはできません。ベンダーの中には、複数の物理アレイを 1つのアレイとして提供しているところがあります。このような場合は、引き続き 1つの論理アレイを技術的に使用します。
- Virtual Volumes データストアが含まれるホスト 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場合、そのプロファイルは、リファレンス 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。

ストレージ コンテナのプロビジョニングのベスト プラクティス

ストレージ コンテナを vSphere Virtual Volumes アレイ側にプロビジョニングする場合、次のベスト プラクティスに従ってください。

制限に基づいたコンテナの作成

Virtual Volumes をグループ分けする際にストレージ コンテナによって論理的制限が適用されるため、コンテナを適用する境界と一致する必要があります。

例として、マルチテナント デプロイのテナント用に作成されたコンテナや、エンタープライズ デプロイの部門向けのコンテナが挙げられます。

- 組織または部門（人事、経理など）
- グループまたはプロジェクト（チーム A、赤チームなど）
- 顧客

1つのコンテナへの全ストレージ機能の集約

ストレージ コンテナは個別のデータストアです。1つのストレージ コンテナで、複数のストレージ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 コンテナに含めることができます。

ストレージ プロファイルの変更は、別のコンテナへのストレージ移行ではなく、アレイ側の操作である必要があります。

ストレージ コンテナのオーバープロビジョニングの回避

ストレージ コンテナをプロビジョニングする際に、コンテナ構成の一環として適用する容量制限は、単なる論理的制限です。予想される使用に必要な容量を上回るコンテナをプロビジョニングしないようにしてください。後でコンテナのサイズを拡大する場合、フォーマットまたはパーティショニングをやり直す必要はありません。

ストレージ固有の管理ユーザー インターフェイスを使用したプロトコル エンドポイントのプロビジョニング

どのストレージ コンテナにも、ESXi ホストからアクセス可能なプロトコル エンドポイント (PE) が必要です。

ブロック ストレージを使用する場合、PE は T10 ベースの LUN WWN によって定義されたプロキシ LUN を表します。NFS ストレージの場合、PE は、IP アドレスまたは DNS 名、共有名などのマウント ポイントです。

通常、PE の構成はアレイ固有です。PE を構成するときに、固有のストレージ プロセッサまたは特定のホストへの関連付けが必要な場合があります。PE 作成時のエラーを回避するために、設定を手動で行わないようにし、可能であれば、ストレージ固有の管理ツールを使用してください。

プロトコル エンドポイント LUN に対する、Disk.MaxLUN を超える ID の割り当て回避

デフォルトでは、ESXi ホストがアクセスできる LUN ID は、0 から 1,023 までの範囲です。プロトコル エンドポイント LUN の ID を 1,024 以上に設定した場合、ホストは PE を無視する場合があります。

環境内で 1,023 を超える LUN ID が使用されている場合、スキャンされる LUN の数を Disk.MaxLUN パラメータで変更してください。[スキャンするストレージ デバイスの数の変更](#)を参照してください。

vSphere Virtual Volumes のパフォーマンスのベスト プラクティス

vSphere Virtual Volumes で最適なパフォーマンスを確保するには、次の推奨事項を実行します。

個々の Virtual Volumes に異なる仮想マシン ストレージ ポリシーを使用

デフォルトでは、Virtual Volumes 環境内にある仮想マシンのすべてのコンポーネントに、単一の仮想マシン ストレージ ポリシーが適用されます。しかし、データベース仮想ディスクとそれに対応するログ仮想ディスクなど、コンポーネントごとにパフォーマンス特性が異なる場合があります。パフォーマンス要件によっては、個々の仮想ディスクと仮想マシン ホーム ファイル、または config-VVol に、異なる仮想マシン ストレージ ポリシーを割り当てることができます。

vSphere Web Client を使用する場合、swap-VVol、memory-VVol、または snapshot-VVol に対する仮想マシン ストレージ ポリシーの割り当ては変更できません。

[仮想マシンへの Virtual Volumes ストレージ ポリシーの割り当て](#)を参照してください。

Virtual Volumes でのホスト プロファイルの取得

Virtual Volumes でホスト プロファイルを取得する場合、最適な方法として、リファレンス ホストを構成してから、そのプロファイルを抽出します。vSphere Web Client で既存のホスト プロファイルを手動で編集し、そのプロファイルを新しいホストに使用すると、コンプライアンス エラーが発生することがあります。また、他にも予期しない問題が生じる可能性があります。詳細については、[VMware ナレッジベースの記事 KB2146394](#) を参照してください。

個々のプロトコル エンドポイントにおける I/O ロードの監視

- Virtual Volumes I/O は、必ずプロトコル エンドポイント (PE) を通過します。アレイは、ESXi ホストからアクセス可能な複数の PE の中からプロトコル エンドポイントを選択します。アレイはロード バランシングを行って、Virtual Volumes と PE とを結ぶパスを変更できます。[Virtual Volumes とプロトコル エンドポイントのバインドおよびバインド解除](#)を参照してください。
- ブロック ストレージでは Virtual Volumes 数が多くなる可能性があるため、ESXi によって I/O のキュー深度が大きくなります。PE に対してキューに登録できる I/O の数は、Scsi.ScsiVVolPESNRO パラメータで制御されます。このパラメータは、vSphere Web Client の [システムの詳細設定] ページで構成できます。[ホストの詳細属性の設定](#)を参照してください。

アレイ制限の監視

1 台の仮想マシンが複数の Virtual Volumes を占有する場合があります。[Virtual Volumes](#) を参照してください。

仮想マシンに 2 台の仮想ディスクがあり、メモリで 2 つのスナップショットを作成するとします。仮想マシンによっては、最大で 10 個の VVol オブジェクトを占有する場合があります (1 つの config-VVol、1 つの swap-VVol、2 つの data-VVol、4 つの snapshot-VVol、2 つのメモリ snapshot-VVol)。

ストレージ プロバイダの可用性の確保

vSphere Virtual Volumes ストレージにアクセスするには、ESXi ホストにストレージ プロバイダ (VASA プロバイダ) が必要です。ストレージ プロバイダの可用性を常に確保するために、次のガイドラインに従ってください。

- ストレージ プロバイダ仮想マシンを Virtual Volumes ストレージに移行しない。

- ストレージ プロバイダ仮想マシンをバックアップする。
- vSphere HA または Site Recovery Manager を使用してストレージ プロバイダ仮想マシンを保護する（適切である場合）。

I/O フィルタは、ESXi ホストにインストールできるソフトウェア コンポーネントで、仮想マシンに追加のデータ サービスを提供できます。フィルタは、仮想マシンのゲスト OS と仮想ディスクの間を移動する I/O リクエストを処理します。

I/O フィルタは VMware から提供されるか、vSphere APIs for I/O Filtering (VAIO) を使用してサードパーティによって作成されます。

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
- I/O フィルタのシステム要件
- vSphere 環境での I/O フィルタの設定
- 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

I/O フィルタは、仮想マシンの I/O パスに直接アクセスできます。個々の仮想ディスク レベルで I/O フィルタを有効にできます。I/O フィルタは、ストレージ トポロジから独立しています。

VMware は、I/O フィルタの特定のカテゴリを提供します。またサードパーティ ベンダーは、I/O フィルタを作成できます。通常、I/O フィルタはパッケージとして配布され、インストーラを使用して、vCenter Server と ESXi ホスト クラスタにフィルタ コンポーネントをデプロイします。

I/O フィルタをデプロイすると、vCenter Server は VASA プロバイダとも呼ばれる I/O フィルタ ストレージ プロバイダを、クラスタ内のホストごとに設定して登録します。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。これらのデータ サービスは、仮想マシン ポリシーの共通ルールを作成する際に参照できます。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。

データストアのサポート

I/O フィルタでは、次のようなすべてのデータストア タイプがサポートされます。

- VMFS

- NFS 3
- NFS 4.1
- Virtual Volumes (VVOL)
- vSAN

I/O フィルタのタイプ

ESXi ホストにインストールされる特定のカテゴリの I/O フィルタが用意されています。それに加え、VMware パートナーは、vSphere APIs for I/O Filtering (VAIO) 開発者プログラムを使用して I/O フィルタを作成できます。I/O フィルタは複数の目的を果たすことができます。

サポート対象のフィルタのタイプには次のようなものがあります。

- 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。
- 暗号化。VMware から提供されます。仮想マシンの暗号化メカニズムを提供します。詳細については、『vSphere のセキュリティ』ドキュメントを参照してください。
- 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。
- Storage I/O control。VMware から提供されます。データベースへの I/O ロードを調整し、I/O が輻輳状態にあるときに、仮想マシンに割り当てられるストレージ I/O の量を制御します。詳細については、『vSphere のリソース管理』ドキュメントを参照してください。

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

ユーザー環境と ESXi によって提供される VMkernel インフラストラクチャの組み合わせです。このフレームワークを使用して、仮想ディスクとの間の I/O パスにフィルタ プラグインを追加できます。インフラストラクチャには I/O フィルタ ストレージ プロバイダ (VASA プロバイダ) が含まれています。プロバイダは、ストレージ ポリシー ベース管理 (SPBM) システムと統合され、フィルタ機能を vCenter Server にエクスポートします。

I/O フィルタ プラグイン

VMware によって提供されるか、VMware パートナーによって開発されるソフトウェア 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

VMware パートナーが I/O フィルタを開発する場合、パートナーは I/O フィルタ プラグインを設定および管理するオプションのコンポーネントを提供できます。

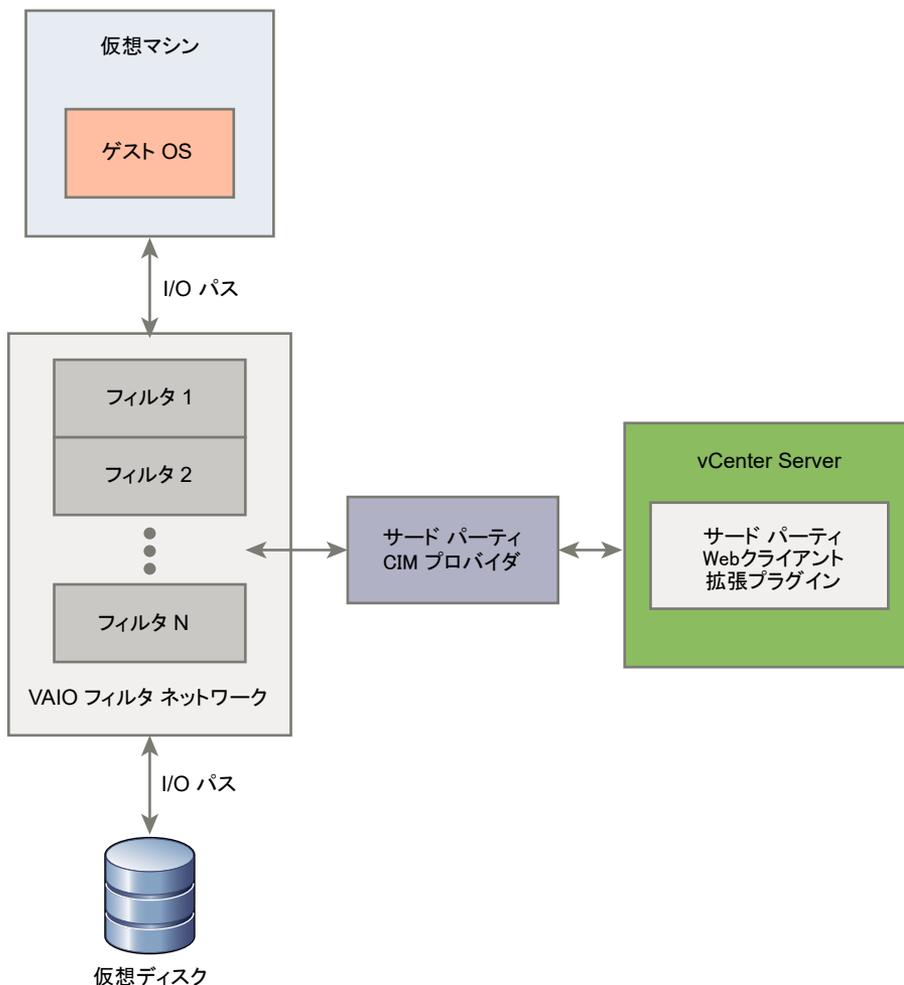
vSphere Web Client プラグイン

I/O フィルタを開発するとき、VMware パートナーはこのオプションのプラグインを含めることができます。vSphere 管理者は、このプラグインを使用し、I/O フィルタの CIM プロバイダと通信して、I/O フィルタ ステータスに関する監視情報を受信できます。さらに、CIM プロバイダに構成コマンドを送信して I/O フィルタを設定することもできます。

I/O フィルタ デーモン

VMware パートナーが開発できるオプションのコンポーネントです。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、ホスト間でのネットワーク通信チャン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。またフィルタは、実行中の仮想マシンの外で発生する仮想ディスクへの I/O アクセスを傍受します。

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。

特定のディスクに対応しているすべてのフィルタが I/O リクエストを確認したら、リクエストはそのターゲット（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。

I/O フィルタのストレージ プロバイダ

I/O フィルタが ESXi ホストにインストールされると、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）の設定と登録が行われます。

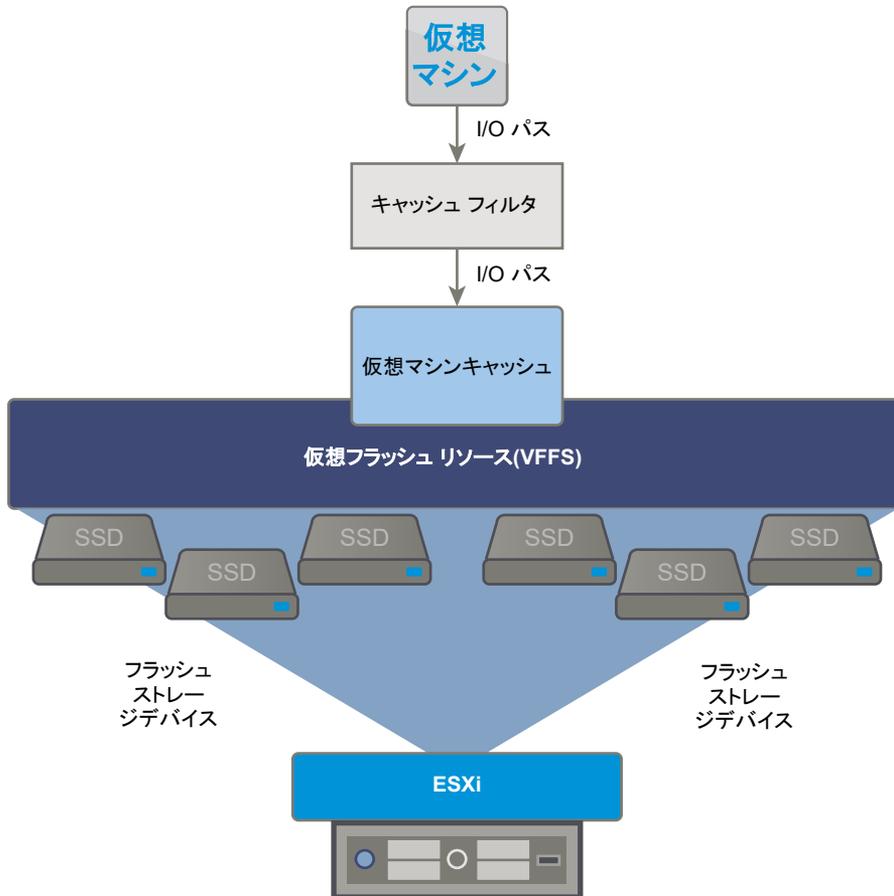
I/O フィルタのストレージ プロバイダは、vSphere によって提供されるソフトウェア コンポーネントです。ストレージ プロバイダは、I/O フィルタや、I/O フィルタが vCenter Server に対してサポートするレポート データ サービス機能と統合されます。

この機能は、仮想マシン ストレージ ポリシー インターフェイスに配置され、仮想マシン ストレージ ポリシーで参照できます。このポリシーを仮想ディスクに適用すると、I/O フィルタはディスクの I/O を処理できます。

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、仮想フラッシュ リソース（VFFS ボリュームとも呼ばれる）を設定する必要があります。ESXi ホストでリソースを設定してから、フィルタを有効化します。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 ボリュームに配置します。



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 リソースのキャパシティを拡張するために、フラッシュ ドライブを追加できます。フラッシュ ドライブは、仮想フラッシュ リソース専用個別に割り当てる必要があります。vSAN 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的の関係にあります。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。

I/O フィルタのシステム要件

環境で I/O フィルタを使用できるようにするには、いくつかの要件に従う必要があります。

次の要件が適用されます。

- I/O フィルタと互換性がある ESXi および vCenter Server の最新バージョンを使用する。古いバージョンでは、I/O フィルタがサポートされていない、または部分的にしかサポートされていない場合があります。
- 個別のパートナー ソリューションに追加の要件がないか確認する。場合によっては、フラッシュ デバイス、追加の物理メモリ、またはネットワーク接続やバンド幅が環境に必要なこともあります。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。

- フィルタ インストール用のパートナー パッケージをホストする Web サーバ。このサーバは最初のインストール後も引き続き使用できる必要があります。新しいホストがクラスタに参加すると、このサーバは適切な I/O フィルタ コンポーネントをホストにプッシュします。

vSphere 環境での I/O フィルタの設定

I/O フィルタが仮想マシン用に提供するデータ サービスを設定するには、いくつかの手順を実行します。

前提条件

- 少なくとも 1 つの ESXi ホストが含まれるクラスタを作成します。
- VMware は、I/O フィルタを提供しています。さらに、VMware パートナーが vSphere API for I/O Filtering (VAIO) を通じて作成するフィルタを使用することができます。通常、パートナー フィルタ パッケージは vSphere インストール バンドル (VIB) として配布され、I/O フィルタ デーモン、CIM プロバイダ、その他の関連付けられたコンポーネントを含むことができます。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

サードパーティによって提供された I/O フィルタを使用する場合、その 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 フィルタとストレージ プロバイダの表示

環境で使用できる I/O フィルタを確認し、I/O フィルタ プロバイダが想定どおりに表示され、アクティブな状態であることを確認できます。

3 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、仮想フラッシュ リソース (VFFS ポリュームとも呼ばれる) を設定する必要があります。ESXi ホストでリソースを設定してから、フィルタを有効化します。

4 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 の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

サードパーティによって提供された I/O フィルタを使用する場合、その 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。

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 フィルタを作成します。フィルタ パッケージは通常、vSphere インストール バンドル (VIB) として配布されます。VIB パッケージには、I/O フィルタ デモン、CIM プロバイダ、およびその他の関連付けられたコンポーネントを含めることができます。

通常、フィルタをデプロイするには、ベンダーによって提供されたインストーラを実行します。インストールは ESXi クラスタ レベルで実行されます。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。

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。

手順

- ◆ 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 にデプロイされ、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。

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すると、システムはホストでアラームを発生させます。

I/O フィルタとストレージ プロバイダの表示

環境で使用できる I/O フィルタを確認し、I/O フィルタ プロバイダが想定どおりに表示され、アクティブな状態であることを確認できます。

サードパーティの I/O フィルタをインストールすると、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すると、システムはホストでアラームを発生させます。

手順

- 1 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、アクティブな状態であることを確認します。
 - a vSphere Web Client ナビゲータで、vCenter Server に移動して参照します。
 - b [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。
 - c 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 プロバイダが適切に登録されると、フィルタが提供する機能とデータ 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ます。

- 2 I/O フィルタ コンポーネントのリストがクラスタおよび ESXi ホストに表示されていることを確認します。

オプション	操作
クラスタの I/O フィルタの表示	a クラスタに移動します。 b [設定] タブをクリックします。 c [設定] で [I/O フィルタ] をクリックして、クラスタにインストールされているフィルタを確認します。
ホストの I/O フィルタの表示	a ホストに移動します。 b [構成] タブをクリックします。 c [ストレージ] で [I/O フィルタ] をクリックして、ホストにインストールされているフィルタを確認します。

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、仮想フラッシュ リソース (VFFS ボリュームとも呼ばれる) を設定する必要があります。ESXi ホストでリソースを設定してから、フィルタを有効化します。

前提条件

仮想フラッシュ リソースを有効化する必要があるかどうかを決定するには、I/O フィルタ ベンダーに確認してください。

手順

- 1 vSphere Web Client で、ホストに移動します。
- 2 [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 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 リソースを設定します。

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。

次のステップ

後で仮想マシンの I/O フィルタを無効にする場合、仮想マシン ストレージ ポリシーからフィルタ ルールを削除してポリシーを再適用できます。[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](#)を参照してください。または、仮想マシンの設定を編集し、そのフィルタが含まれない別のストレージ ポリシーを選択できます。

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。I/O フィルタを有効にするポリシーには共通ルールを含める必要があります。ただし、追加の配置ルールはオプションです。

環境にインストールされている I/O フィルタによっては、データ サービスがキャッシュ、レプリケーションなど、複数のカテゴリに属する場合があります。ストレージ ポリシーの特定のカテゴリを参照することで、仮想マシンのサービスを要求することになります。

I/O フィルタとストレージで暗号化など、同じサービス カテゴリが提供される場合、ポリシーはこのサービスを両方のプロバイダから要求できます。その結果、仮想マシン データが 2 回、I/O フィルタとストレージによって暗号化されることになります。ただし、Virtual Volumes によって提供されるレプリケーションと I/O フィルタによって提供されるレプリケーションは、同じストレージ ポリシーに共存することができません。

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 フィルタとストレージ プロバイダの表示](#)を参照してください。
- 適切なストレージ ポリシーのコンポーネントを定義します。[ストレージ ポリシー コンポーネントの作成](#)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 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] タブをクリックします。

- 3 [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。
- 4 vCenter Server インスタンスを選択します。
- 5 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。
- 6 [共通ルール] ページで、I/O フィルタを定義します。
 - 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 [コンポーネントの追加] (+) アイコンをクリックし、ドロップダウン メニューからデータ サービス カテゴリを選択します（レプリケーションなど）。
 - c ルールに対して適切なプロバイダと値を指定することによって、データ サービス カテゴリのルールを定義します。または、事前定義済みコンポーネントのリストからデータ サービスを選択します。

オプション	説明
 Component Name	このオプションは、データベースにストレージ ポリシーのコンポーネントを事前定義している場合に使用できます。使用するコンポーネントがわかっている場合は、リストでそれを選択して仮想マシン ストレージ ポリシーに追加します。
すべて表示	カテゴリで使用できるすべてのコンポーネントを確認します。特定のコンポーネントを含める場合は、リストでそれを選択し、[OK] をクリックします。
カスタム	ルールに対して適切なプロバイダと値を指定して、データ サービス カテゴリのカスタムルールを定義します。

注： 他の I/O フィルタと一緒に暗号化を使用する場合は、[暗号化の前の I/O フィルタを許可する] パラメータを [True] に設定します。これにより、暗号化の前に、レプリケーションなどのフィルタでクリアテキスト データを分析できるようになります。

- d さらにコンポーネントを追加して、他のデータ サービスを要求します。
共通または通常のルール セットごとに、同じカテゴリ（キャッシュなど）から使用できるコンポーネントは 1 つのみです。
 - e [次へ] をクリックします。
- 7 ポリシーに配置ルールが含まれる場合、[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： 異なるタイプのデータストア間で I/O フィルタをもつ仮想マシンを移行する場合は、ポリシーにすべてのターゲット データストアの配置ルールが含まれていることを確認してください。たとえば、VMFS と Virtual Volumes のデータストア間で仮想マシンを移行する場合は、混合仮想マシン ストレージ ポリシーを作成します。ポリシーには、VMFS データストアのタグベースのルールと Virtual Volumes データストアのルールが含まれている必要があります。

- 8 [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。
- 9 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。

仮想マシンの初期導入時に 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 の仮想マシン管理』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 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。
 - b 互換性のある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。
- 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。
仮想ディスクに対してのみ I/O フィルタを有効にするには、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

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。vCenter Server によって 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。

- 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

- フィルタをアップグレードするには、ベンダーが提供するインストーラを実行します。

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。

- 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 フィルタはデータストアに依存しないため、VMFS、NFS、Virtual Volumes、vSAN を含むすべてのタイプのデータストアが I/O フィルタに対応しています。
- I/O フィルタは仮想互換モードの RDM をサポートしています。物理互換モードの RDM はサポートされていません。
- 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的の関係にあります。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。
- 仮想マシンの移行中またはクローン作成中に 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。移行またはクローン作成の完了後にポリシーを変更できます。

- I/O フィルタ ポリシーが含まれる仮想マシンをクローン作成する、または 1 台のホストからほかのホストに移行するときは、ターゲット ホストに互換性のあるフィルタがインストールされていることを確認してください。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 サイトに 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再接続する必要があります。
- 仮想マシンの作成時に、暗号化 I/O フィルタを新しい仮想ディスクに接続できます。暗号化フィルタを既存の仮想ディスクに接続することはできません。
- 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 の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 Virtual Volumes 間のように、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。この操作を行う場合は、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 セットが含まれていることを確認してください。たとえば、VMFS と Virtual Volumes のデータストア間で仮想マシンを移行する場合は、以下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。

- 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。
- Virtual Volumes 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 I/O フィルタの共通ルールのみを定義する場合、システムはデータストアのデフォルトのストレージ ポリシーを適用します。

ストレージのハードウェア アクセラレーション

24

ハードウェア アクセラレーション機能により、ESXi ホストを互換性のあるストレージ システムと統合できます。ホストは、特定の仮想マシンとストレージ管理の操作をストレージ システムにオフロードできます。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。

ブロック ストレージ デバイス、ファイバ チャネルと iSCSI、および NAS デバイスは、ハードウェア アクセラレーションをサポートします。

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 24-1. 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	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

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をサポートし、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、[ESXi とアレイ シン プロビジョニング](#) 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 [設定] 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 アレイを統合するため、vSphere は Storage APIs - Array Integration (VAAI) と呼ばれる ESXi の拡張機能を使用します。この統合により、vSphere はアレイのハードウェア操作を使用できます。

vSphere 5.x 以降のリリースでは、これらの拡張は T10 SCSI 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か、部分的にしかサポートしていない場合、ESXi は、ホストにインストールされている VAAI プラグインを使用する設定に戻ります。ホストは、T10 SCSI コマンドとプラグインを組み合わせて使用することもできます。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か、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お問い合わせください。

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には、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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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、次のパラメータ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。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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.XXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
Multipath Plugin: NMP
XXXXXXXXXXXXXXXXXX
Attached Filters: VAAI_FILTER
VAAI Status: supported
XXXXXXXXXXXXXXXXXX
```

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、ブロック ストレージ デバイスがハードウェア アクセラレーションをサポートするかどうかを照会します。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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。

VAAI プラグインがデバイスを管理する場合、出力には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.XXXXXXXXXXXXX4c
naa.XXXXXXXXXXXXX4c
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リスト表示

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 デバイスには、2 つの要求ルールが必要です。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ています。

```
# 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、VAAI プラグインが要求するデバイスを指定しています。

```
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します。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。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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_VAAIP_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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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、vSphere APIs 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にします。

VAAI NAS フレームワークは、NFS ストレージの両方のバージョン、NFS 3 と NFS 4.1 をサポートしています。

VAAI NAS は、ホストからアレイへのストレージ操作の負荷をオフロードするために、ストレージ プリミティブのセットを使用します。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。仮想ディスク ファイルのクローンを作成するため、NAS デバイスの機能をサポートします。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。
- 容量の予約。シック フォーマットで仮想ディスク ファイルの容量を割り当てるため、ストレージ アレイの機能をサポートします。

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の作成負荷は、アレイにオフロードできます。
- 拡張された統計。NAS デバイスでの容量使用量の可視化をサポートします。この機能は、シン プロビジョニングに役立ちます。

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 サイトから 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、いくつかのツールを利用できます。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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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
```

ホストの許容レベルに対する制限は、ホストに追加する VIB の許容レベルと同程度か少なくなければなりません。*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:、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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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 には、更新する VIB パッケージの URL を指定します。http:、https:、ftp:、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。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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。

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容量が提供されます。ただし、容量は未使用のままとなり、ストレージのキャパシティ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容量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。

シン プロビジョニングによって、実際に存在する物理容量以上の仮想ストレージ容量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、物理ストレージ容量が不足する状態を回避します。

この章には、次のトピックが含まれています。

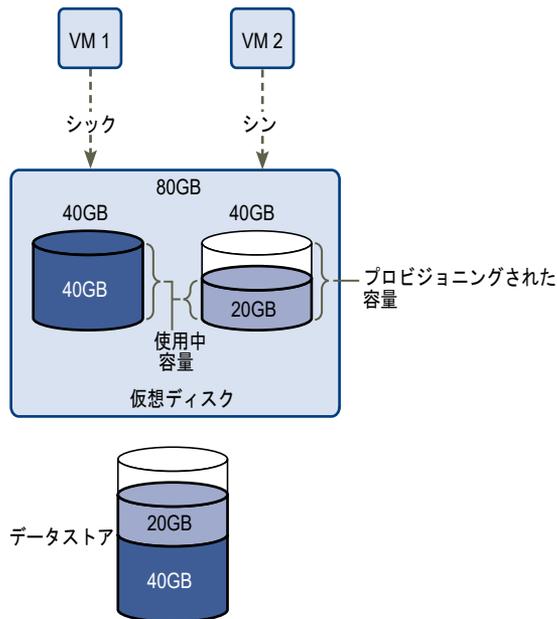
- [仮想ディスク シン プロビジョニング](#)
- [ESXi とアレイ シン プロビジョニング](#)
- [ストレージ容量の再利用](#)

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容量が仮想ディスク 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、仮想マシンの仮想ディスクに固定のストレージ容量 (たとえば 40 GB) を事前にプロビジョニングします。プロビジョニングされた容量全体が仮想ディスクにコミットされます。プロビジョニングされた容量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容量全体 (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容量に限定されます。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。ディスクで追加の容量が必要な場合は、プロビジョニングされた容量の 40 GB 全体にまで拡張できます。



仮想ディスクのプロビジョニング ポリシーについて

特定の仮想マシン管理操作を実行するときは、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。操作には、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があります。

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、仮想マシンへ初めて書き込みを行うときに必要に応じてゼロアウトされます。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ゼロアウトされます。このフォーマットで仮想ディスクを作成する場合、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。シン ディスクでさらに多くの容量が必要になったら、最大容量まで拡張して、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、最も短時間で仮想ディスクを作成できます。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アウトは行われません。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アウトが行われます。

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 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 の仮想マシン管理』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、仮想ディスクはプロビジョニングされた容量全体は使用しない場合があります。実際のストレージ使用の値には、仮想ディスクのサイズよりも小さい値を指定できます。

- 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、使用済みストレージ容量にはスワップ 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の値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 [データストア] タブをクリックします。
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。
 - c データストアを選択して、[ファイルの参照] 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 フォルダを展開し、変換する仮想ディスク 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 およびホストの管理』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 キャパシティの増加](#) を参照してください。

ESXi とアレイ シン プロビジョニング

ESXi でシン プロビジョニング ストレージ アレイを使用できます。

ESXi ホストはブロックベースのストレージと連携し、これらのタスクを実行できます。

- ホストは基礎となるシン プロビジョニング LUN を認識し、ストレージ使用状態を監視して、物理容量の不足を回避できます。たとえば、VMFS データストアが増大した場合、または Storage vMotion を使用してシン プロビジョニング LUN に仮想マシンを移行する場合、LUN 容量は変更される可能性があります。ホストは、物理 LUN 容量の違反と容量不足状態について警告します。
- ホストは VMFS6 および仮想マシン ゲスト OS からの自動 T10 unmap コマンドを発行して、アレイの未使用容量を再利用できます。VMFS5 は、手動による容量再利用方法をサポートします。

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 レポートと容量再利用の機能を使用するには、次の要件を満たす必要があります。

- 適切な ESXi バージョンを使用します。

表 25-1. ESXi バージョンとシン プロビジョニングのサポート

サポート対象のシン プロビジョニング コンポーネント	ESXi 6.0 以前	ESXi 6.5
シン プロビジョニング	はい	はい
VMFS から発行される Unmap コマンド	VMFS5 の場合は手動。 esxcli storage vmfs unmap を使用します。	VMFS6 の場合は自動
ゲスト OS から発行される Unmap コマンド	可。限定的なサポート。	可 (VMFS6)

- T10 ベースの vSphere Storage APIs - Array Integration (VAAI) をサポートするストレージ システムを使用します (シン プロビジョニングと容量再利用を含む)。詳細は、ストレージ プロバイダに連絡して、VMware 互換性ガイドをご確認ください。

容量の使用の監視

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 の容量使用を監視し、容量不足を回避することができます。

次のサンプル フローは、シン プロビジョニングされた LUN で、容量の違反および不足の警告を生成するために ESXi ホストとストレージ アレイが連携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容量が増加して、設定されたソフトしきい値に到達した場合、次のようなアクションを実行します。

- 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。

物理容量を増やすように、ストレージ管理者に連絡します。または、Storage vMotion を使用して、LUN の容量がなくなる前に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 に割り当てられた容量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、ホストに容量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、容量不足アラームを生成します。

ストレージ管理者に物理容量を要求することによって、永久的な容量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。

プロシージャの **--server=server_name** は、ターゲット サーバを指定します。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
-----
```

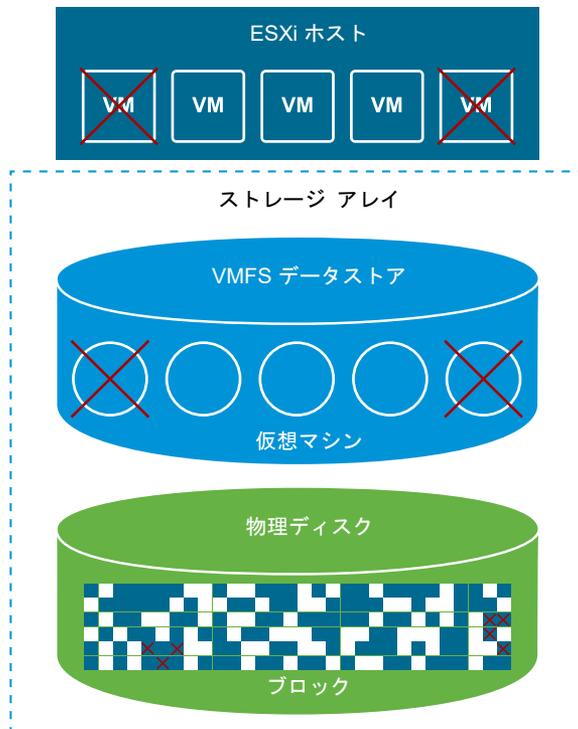
不明なステータスは、ストレージ デバイスがシックであることを示します。

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 ペンダーにご確認ください。

ストレージ容量の再利用

ESXi は、VMFS データストアまたは仮想マシン ゲスト OS から発行される、SCSI unmap コマンドとも呼ばれる容量再利用コマンドをサポートしています。このコマンドを使用すると、シン プロビジョニング ストレージ アレイで、VMFS データストアおよびデータストア上のシン仮想ディスクの未使用容量を再利用できるようになります。VMFS6 データストアは、容量再利用コマンドを自動的に送信できます。VMFS5 データストアでは、ストレージ容量を手動で再利用できます。

仮想マシンの削除または移行、スナップショットの統合などを行うときは、VMFS データストア内部のストレージ容量を解放します。仮想マシン内部では、シン仮想ディスクのファイルを削除すると、ストレージ容量が解放されます。これらの操作では、ストレージ アレイの未使用容量のブロックが残されます。しかし、ブロックからデータが削除されたことをアレイが認識しない場合、データストアがブロックを解放するまで、ブロックはアレイによって割り当てられたままになります。VMFS は SCSI unmap コマンドを使用して、ストレージ ブロックに削除されたデータが含まれていることをアレイに通知するため、アレイはこれらのブロックの割り当てを解除できます。



コマンドは、ゲスト OS から直接発行することもできます。VMFS5 および VMFS6 両方のデータストアは、ゲスト OS から処理する unmap コマンドをサポートできます。ただし、VMFS5 ではサポート レベルが制限されています。

VMFS データストアのタイプに応じて、さまざまな方法を使用して、データストアおよび仮想マシンで容量再利用を設定できます。

容量再利用の仕組みの詳細については、次のビデオをご覧ください。



(Space Reclamation with VMFS in vSphere 6.5)

■ VMFS データストアからの容量再利用の要求

VMFS データストアからファイルを削除すると、ファイル システム内の容量が解放されます。この空き容量は、ファイル システムが解放またはマッピング解除するまで、ストレージ デバイスにマッピングされます。ESXi は、マッピング解除操作とも呼ばれる空き容量の再利用をサポートしています。

■ ゲスト OS からの容量の再利用の要求

ESXi は、ストレージ容量を再利用するためにゲスト OS から直接発行される unmap コマンドをサポートしています。サポートのレベルおよび要件は、仮想マシンが存在するデータストアのタイプによって異なります。

VMFS データストアからの容量再利用の要求

VMFS データストアからファイルを削除すると、ファイル システム内の容量が解放されます。この空き容量は、ファイル システムが解放またはマッピング解除するまで、ストレージ デバイスにマッピングされます。ESXi は、マッピング解除操作とも呼ばれる空き容量の再利用をサポートしています。

この操作により、ストレージ アレイは未使用の空き容量を再利用できるようになります。マッピング解除された容量は、他のストレージ割り当て要求やニーズに使用できます。

VMFS6 データストアでの空き容量の非同期再利用

ESXi は、VMFS6 データストアで、空き容量の自動の非同期再利用をサポートしています。VMFS6 は、マッピング解除操作をサポートするシンプロビジョニング ストレージ アレイで、unmap コマンドを実行し、ストレージの空き容量をバックグラウンドで解放できます。

非同期のマッピング解除処理には、いくつかの利点があります。

- マッピング解除要求は一定速度で送信されるため、バックグラウンドでの短期間のロードを回避できます。
- 解放された領域は一括処理され、同時にマッピング解除されます。
- マッピング解除処理と I/O パスの切り詰めは分離されているため、I/O パフォーマンスに影響を受けることはありません。

VMFS6 データストアの場合、データストア作成時に、次の容量再利用パラメータを設定できます。

容量再利用の精度

精度では、基盤となるストレージが再利用できる、解放される最小サイズのセクターを定義します。ストレージは、指定した精度より小さいサイズのセクターを再利用できません。

VMFS6 の場合、再利用の精度はブロック サイズと同じです。1 MB のブロック サイズを指定すると、精度も 1 MB になります。1 MB より小さいサイズのストレージ セクターは再利用されません。

注： 特定のストレージ アレイでは、最適なマッピング解除の精度が推奨されます。推奨されたマッピング解除の精度が 1 MB より大きい（たとえば 16 MB）場合、ESXi は、これらのアレイで自動のマッピング解除処理をサポートしません。最適な精度が 1 MB 以下のアレイでは、精度が 1 MB の倍数である場合、マッピング解除処理がサポートされます。たとえば、1 MB は 512 バイト、4 K、64 K などです。

容量再利用の優先度

このパラメータでは、容量再利用の操作が実行される頻度を定義します。通常 VMFS6 は、ワークロードと設定に応じて、一斉にまたは散発的に unmap コマンドを送信できます。VMFS6 データストアを作成するとき、次のいずれかのオプションを指定できます。

- なし。データストアでマッピング解除操作を無効にします。オプションは vSphere Web Client で設定できます。
- 低（デフォルト）。unmap コマンドを低頻度で送信します。オプションは vSphere Web Client で設定できます。

容量の再利用を有効にした後、VMFS6 データストアは、少なくとも 1 つのファイルが開いている場合にのみ、未使用の容量のブロック解放を開始できます。たとえば、データストア上の仮想マシンのうち 1 台をパワーオンすると、この条件を満たすことができます。

VMFS5 データストアでの空き容量の手動再利用

VMFS5 以前のファイル システムでは、空き容量を自動的にマッピング解除しませんが、`esxcli storage vmfs unmap` コマンドを使用して、容量を手動で再利用できます。コマンドを使用する場合は、多数のマッピング解除要求が一度に送信される可能性があることに注意してください。このアクションにより、操作中に一部のリソースがロックされる場合があります。

VMFS6 データストアの容量再利用の設定

VMFS6 データストアを作成するとき、自動的な容量の再利用のデフォルト パラメータを変更することができます。また、VMFS6 データストアの容量の再利用を無効にしたり、詳細設定や優先順位を変更することもできます。

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 [新規データストア] アイコンをクリックします。
- 3 VMFS6 データストアの作成に必要な手順を実行します。

- 4 [パーティション設定] ページで、容量再利用のパラメータを指定します。

パラメータでは、精度と容量再利用の操作が実行される率を定義します。このページを使用して、データストアの容量再利用を無効にすることもできます。

オプション	説明
ブロック サイズ	VMFS データストアのブロック サイズでは、最大ファイル サイズとファイルが使用する容量を定義します。VMFS6 では、1 MB のブロック サイズをサポートしています。
容量再利用の精度	マッピング解除操作の精度を指定します。マッピング解除の精度はブロック サイズ (1 MB) に対応します。 1 MB より小さいサイズのストレージ セクターは再利用されません。
容量再利用の優先度	次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> ■ 低 (デフォルト)。マッピング解除操作を低率で処理します。 ■ なし。データストアで容量再利用の操作を無効にする場合は、このオプションを選択します。

- 5 データストアの作成プロセスを完了します。

結果

容量の再利用を有効にした後、VMFS6 データストアは、少なくとも 1 つのファイルが開いている場合にのみ、未使用の容量のブロック解放を開始できます。たとえば、データストア上の仮想マシンのうち 1 台をパワーオンすると、この条件を満たすことができます。

容量再利用の優先度の変更

容量再利用の優先度では、VMFS6 データストアから削除されたブロックを、データストアをバックアップしている LUN で再利用する方法を定義します。デフォルトでは、LUN は容量再利用の操作を低い率で実行します。デフォルト設定を変更して、データストアに対する操作を無効にできます。

手順

- 1 vSphere Web Client ナビゲータで、データストアを参照して移動します。
- 2 右クリック メニューから [領域再利用の編集] を選択します。
- 3 容量再利用の設定を変更します。

オプション	説明
なし	データストアで容量再利用の操作を無効にする場合は、このオプションを選択します。
低 (デフォルト)	容量再利用を低率で実行します。

- 4 [OK] をクリックして、新しい設定を保存します。

結果

容量再利用の優先度の変更された値が、データストアの [全般] ページに表示されます。

容量の自動再利用に関する設定の確認

VMFS6 データストアの容量再利用のパラメータを設定または編集後、その設定内容を確認できます。

手順

- 1 データストアに移動します。
- 2 [設定] タブをクリックします。
- 3 [全般] をクリックして、容量再利用の設定を確認します。
 - a プロパティで [ファイル システム] を展開し、容量再利用の精度の値を確認します。
 - b [領域の再利用] で、容量再利用の優先度の設定を確認します。

例：VMFS6 の容量再利用のパラメータの取得

`esxcli storage vmfs reclaim config get -l=VMFS_label|-u=VMFS_uuid` コマンドを使用して、容量再利用の設定情報を取得することもできます。

```
# esxcli storage vmfs reclaim config get -l my_datastore
Reclaim Granularity: 1048576 Bytes
Reclaim Priority: low
```

蓄積されたストレージ容量の手動による再利用

容量の自動再利用をサポートしていない VMFS データストアでは、`esxcli` コマンドを使用して、未使用のストレージ容量を手動で再利用できます。

プロシージャの `--server=server_name` は、ターゲット サーバを指定します。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 シン プロビジョニング デバイスの未使用のストレージ ブロックを再利用するには、次のコマンドを実行します。

```
esxcli --server=server_name storage vmfs unmap
```

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
<code>-l --volume-label=volume_label</code>	マップ解除する VMFS ボリュームのラベル。必須の引数です。この引数を指定した場合、 <code>-u --volume-uuid=volume_uuid</code> は使用しないでください。
<code>-u --volume-uuid=volume_uuid</code>	マップ解除する VMFS ボリュームの UUID。必須の引数です。この引数を指定した場合、 <code>-l --volume-label=volume_label</code> は使用しないでください。
<code>-n --reclaim-unit=number</code>	反復ごとにマップ解除する VMFS ブロックの数。オプションの引数です。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。

- マッピング解除処理が完了したかどうかを確認するには、`vmkernel.log` ファイルでマッピング解除を検索します。

ゲスト OS からの容量の再利用の要求

ESXi は、ストレージ容量を再利用するためにゲスト OS から直接発行される `unmap` コマンドをサポートしています。サポートのレベルおよび要件は、仮想マシンが存在するデータストアのタイプによって異なります。

仮想マシン内部でストレージ容量が解放されるのは、たとえばシン仮想ディスクでファイルを削除したときなどです。ゲスト OS は `unmap` コマンドを送信して、解放された容量について VMFS に通知します。ゲスト OS から送信された `unmap` コマンドにより、VMFS データストア内の容量が解放されます。このコマンドはその後、アレイが解放された容量のブロックを再利用できるようにアレイに渡されます。

VMFS6 仮想マシンの容量の再利用

VMFS6 は、一般にゲスト OS から生成される容量の自動再利用の要求をサポートしており、これらの要求をアレイに渡します。多くのゲスト OS は `unmap` コマンドを送信でき、追加の設定は必要ありません。自動マッピング解除をサポートしないゲスト OS では、ユーザーの介入が必要な場合もあります。VMFS6 の容量の自動再利用をサポートするゲスト OS の詳細については、ベンダーにお問い合わせください。

通常、ゲスト OS はアダプタイズするマッピング解除の精度に基づいて `unmap` コマンドを送信します。詳細については、ゲスト OS に付属するドキュメントを参照してください。

VMFS6 は、再利用する容量が 1 MB または 1 MB の倍数の場合のみ、ゲスト OS からのマッピング解除の要求を処理します。容量が 1 MB 未満、または 1 MB の倍数になっていない場合、マッピング解除の要求は処理されません。

VMFS5 仮想マシンの容量の再利用

通常、VMFS5 上のゲスト OS から生成される `unmap` コマンドを直接アレイに渡すことはできません。アレイのマッピング解除をトリガするには `esxcli storage vmfs unmap` コマンドを実行する必要があります。

ただし、ごく一部のゲスト OS については、VMFS5 が容量の自動再利用の要求をサポートしています。

ゲスト OS からマッピング解除要求をアレイに送信するには、仮想マシンが次の前提条件を満たしている必要があります。

- 仮想マシンはシンプロビジョニングである必要があります。
- 仮想マシンのハードウェアはバージョン 11 (ESXi 6.0) 以降である必要があります。
- 詳細設定の `EnableBlockDelete` を 1 に設定する必要があります。
- ゲスト OS が仮想ディスクをシンとして識別できる必要があります。

vmkfstools は、VMFS ボリューム、ストレージ デバイス、および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してください。

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 コマンドのオプション

vmkfstools コマンドの構文

vmkfstools コマンドを実行する場合、通常は 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は、root ユーザーとして実行する必要があります。

vmkfstools コマンドでは、次のコマンド構文をサポートします。

```
vmkfstools 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	vmkfstools で実行するアクティビティを指定するために使用する、1 つ以上のコマンドライン オプションと関連する引数です。たとえば、新しい仮想ディスクを作成するときにディスク フォーマットを選択します。 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、 <code>disk_ID:P</code> 形式を使用します。 <code>disk_ID</code> はストレージ アレイから返されるデバイス ID で、 <code>P</code> 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"> ■ <code>/vmfs/devices/disks</code> (ローカルまたは SAN ベース ディスク)。 ■ <code>/vmfs/devices/lvm</code> (ESXi 論理ボリューム)。 ■ <code>/vmfs/devices/generic</code>(一般的な SCSI デバイス)。
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"> ■ 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。 <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"> ■ 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。 <pre>/vmfs/volumes/file_system_label file_system_UUID/[dir]/myDisk.vmdk</pre> <p>現在の作業ディレクトリが <code>myDisk.vmdk</code> の親ディレクトリの場合は、パス全体を入力しません。</p>

vmkfstools コマンドのオプション

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 vmfs6 --blocksize 1m disk_ID:P
vmkfstools -C vmfs6 -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 データストアの属性の一覧表示

VMFS データストア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 データストア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、指定されたデータストアの属性が一覧表示されます。一覧表示される属性には通常、ファイル システム ラベル、データストアのエクステンツの数、UUID、各エクステンツが存在するデバイス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、エクステンツ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|--humanreadable` 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さらにわかりやすい形式で表示されます。

例：VMFS 属性の一覧表示の例

```
~ vmkfstools -P -h /vmfs/volumes/my_vmfs
VMFS-5.81 (Raw Major Version: 14) file system spanning 1 partitions.
File system label (if any): my_vmfs
Mode: public
Capacity 99.8 GB, 97.5 GB available, file block size 1 MB, max supported file size 62.9 TB
UUID: 571fe2fb-ec4b8d6c-d375-XXXXXXXXXXXX
Partitions spanned (on "lvm"):
    eui.3863316131XXXXXX:1
Is Native Snapshot Capable: YES
```

VMFS データストアまたはスクラッチ パーティションの作成

VMFS データストアまたはスクラッチ パーティションを作成するには、`vmkfstools` コマンドを使用します。

```
-C|--createfs [vmfs5|vmfs6|vfat]
```

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 VMFS データストアを作成します。このパーティションがデータストアのヘッド パーティションになります。VMFS5 と VMFS6 では、使用可能なブロック サイズは 1 MB のみです。

-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 オプションとともに使用します。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。この操作によって、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。

- -Y|--unmapGranularity #[bBsSkKmMgGtT] - このサブオプションは VMFS6 のみに適用されます。マッピング解除操作の精度を定義します。デフォルトの精度は 1 MB です。ブロック サイズの場合と同様に、単位のタイプを入力します。
- -O|--unmapPriority <none|low|medium|high> - このサブオプションは VMFS6 のみに適用されます。マッピング解除操作の優先順位を定義します。

例：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 VMFS6 データストアを作成します。

```
~ vmkfstools -C vmfs6 -S my_vmfs /vmfs/devices/disks/naa.ID:1
```

VMFS データストアへのエクステントの追加

VMFS データストア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。

エクステントを追加するときに、`span_partition` で指定されたパーティション全体で、ヘッド パーティションから VMFS データストアを拡張します。

```
-Z|--spanfs span_partitionhead_partition
```

ヘッドパーティションとスパンパーティションのフルパス名（例：/vmfs/devices/disks/disk_ID:1）を指定する必要があります。このオプションを使用するときには必ず、データストアが複数のパーティションにまたがるようにエクステントを VMFS データストアに追加します。

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。

例：VMFS データストアを拡張する例

この例では、VMFS データストアの既存のヘッドパーティションを新しいパーティションに拡張します。

```
~ vmkfstools -Z /vmfs/devices/disks/naa.disk_ID_2:1 /vmfs/devices/disks/naa.disk_ID_1:1
```

拡張されたデータストアは、*naa.disk_ID_1:1* と *naa.disk_ID_2:1* の 2 つのパーティションにまたがります。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。

VMFS データストアの拡張

VMFS データストアにエクステントを追加する代わりに、既存のデータストアのサイズを増大できます。

`vmkfstools -G` コマンドを使用します。

基盤となるストレージの容量を増やした後で、データストアのサイズを増やす場合があります。

このコマンドでは、次のオプションを使用します。

```
-G|--growfs devicedevice
```

このオプションは、VMFS データストアまたはその特定のエクステントを拡張します。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。

データストアのアップグレード時に、以下のオプションを使用します。

```
-T|--upgradevmfs /vmfs/volumes/UUID
```

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。

仮想ディスクのオプション

仮想ディスク オプションを使用して、データストアに格納されている仮想ディスクの設定、移行、管理を行うことができます。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、仮想マシンへ初めて書き込みを行うときに必要に応じてゼロアウトされます。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、必要に応じて割り当てられ、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` : 最大エクステント サイズ 2 GB のスパース ディスクです。VMware Fusion 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。

NFS データストアでのディスク 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、[24 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[bB|sS|kK|mM|gG]
-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 KB として認識します。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せん。

-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。

- -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 vSAN 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。

例：仮想ディスクを作成する例

この例は、disk.vmdk という名前の 2 GB の仮想ディスク ファイルの作成方法を示しています。myVMFS という名前の VMFS データストアにディスクを作成します。このディスク 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/disk.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。

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。

この例に従ってください。

```
vmkfstools --eagerzero /vmfs/volumes/myVMFS/VMName/disk.vmdk
```

ゼロクリアされたブロックの削除

vmkfstools コマンドを使用して、ゼロクリアされたブロックを削除します。

```
-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。

仮想ディスクの削除

vmkfstools コマンドを使用して、VMFS ボリューム上の指定されたパスで仮想ディスク ファイルを削除します。

次のオプションを使用します。

```
-U|--deletevirtualdisk
```

仮想ディスクの名前の変更

vmkfstools コマンドを使用して、VMFS ボリュームの指定されたパスにある仮想ディスク 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 oldName newName
```

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。

非 root ユーザーは、仮想ディスクまたは RDM にクローン作成できません。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|2gbsparse]
  -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 vSAN 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 ネイティブ 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、プライマリ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-primary.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-primary.vmdk /vmfs/volumes/myVMFS/myOS.vmdk -d thin
```

仮想ディスクの拡張

仮想マシン作成後、`vmkfstools` コマンドを使用して、仮想マシンに割り当てられたディスクのサイズを拡張できます。

```
-X|--extendvirtualdisk newSize[bBsSkKmMgGtT]
```

`newSize` パラメータを指定し、末尾に適切な単位を追加します。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 `KB` として認識します。単位のタイプを指定しない場合、`vmkfstools` ではデフォルトで `KB` 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、`4 g` の仮想ディスクを `1 g` 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。

-X オプションを使用する場合は、次の考慮事項が適用されます。

- 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。
- ディスクの拡張後、ディスクのファイル システムの更新が必要な場合があります。その結果、ゲスト OS はディスクの新しいサイズを認識し、使用できるようになります。

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。

タイプが LEGACYSPARSE、LEGACYPLAIN、LEGACYVMFS、LEGACYVMFS_SPARSE、LEGACYVMFS_RDM の仮想ディスクを変換するにはこのオプションを使用します。

```
-M|--migratevirtualdisk
```

仮想互換モードの Raw デバイス マッピングの作成

vmkfstools コマンドを使用して、VMFS ボリューム上で Raw デバイス マッピング (RDM) ファイルを作成し、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
```

例：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

vmkfstools コマンドを使用して、パススルー Raw デバイスを VMFS ボリューム上のファイルにマッピングします。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 deviceexample.vmdk
```

このタイプのマッピングが完了すると、それを使用して、他の 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 パスを指定する場合は、次の形式を使用してください。

```
/vmfs/devices/disks/device_ID
```

.vmdk 名に、この形式を使用します。コマンドを使用する前にデータストアを作成することを確認してください。

```
/vmfs/volumes/datastore_name/example.vmdk
```

次に例を示します。

```
vmkfstools -z /vmfs/devices/disks/naa.600a000000000000... /vmfs/volumes/datastore1/  
mydisk.vmdk
```

RDM の属性の一覧表示

vmkfstools コマンドを使用して、Raw ディスク マッピングの属性を一覧表示します。これらの属性は、RDM ファイルがマップするストレージ デバイスを識別するのに役立ちます。

```
-q|--queryrdm my_rdm.vmdk
```

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。

例：RDM 属性の一覧表示の例

```
# vmkfstools -q /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk  
  
Disk /vmfs/volumes/VMFS/my_vm/my_rdm.vmdk is a Passthrough Raw Device Mapping  
  
Maps to: vml.02000000006005076801900207700000000000005323134352020
```

仮想ディスク構造の表示

vmkfstools コマンドを使用して、仮想ディスクの構造に関する情報を取得します。

```
-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。ディスク構造の不整合によって、ゲスト OS をロードしたり新規作成された仮想マシンを実行したりすると、問題が発生する場合があります。

仮想ディスクの確認と修復

vmkfstools コマンドを使用して仮想ディスクをチェックし、仮想ディスクが破損している場合は修復します。

```
-x|--fix [check|repair]
```

次に例を示します。

```
vmkfstools -x check /vmfs/volumes/my_datastore/my_disk.vmdk
```

整合性のためのディスク チェーンのチェック

vmkfstools コマンドを使用して、スナップショット チェーン全体を確認します。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

vmkfstools コマンドのデバイス 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

vmkfstools コマンドを使用して、ESXi ホスト専用として SCSI LUN を予約します。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、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もできます。

```
-L|--lock [reserve|release|lunreset|targetreset|busreset|readkeys|readresv] 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せん。ほかのサーバがその LUN にアクセスしようすると、予約エラーが表示されます。
- `-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。

- `-L readkeys` : LUN に登録した予約キーを読み取ります。SCSI-III の Persistent Group Reservation 機能に適用されます。
- `-L readresv` : LUN での予約状態を読み取ります。SCSI-III の Persistent Group Reservation 機能に適用されます。

`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

`vmkfstools` コマンドを使用して、特定のパーティションのデバイス ロックを解除します。

```
-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
```

データストアの拡張、エクステンツの追加、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。このコマンドを実行するときには、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。