

vSphere のストレージ

2020 年 4 月 02 日
VMware vSphere 7.0
VMware ESXi 7.0
vCenter Server 7.0



vmware®

最新の技術ドキュメントは、VMware の Web サイト (<https://docs.vmware.com/jp/>) でご確認いただけます。このドキュメントに関するご意見およびご感想は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴァイムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2009-2020 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
1 ストレージの概要	15
従来のストレージ仮想化モデル	15
Software-Defined Storage モデル	17
vSphere Storage API	18
2 従来のストレージ モデルでの開始	19
物理ストレージのタイプ	19
ローカル ストレージ	19
ネットワーク ストレージ	20
ターゲットとデバイスの表現	24
仮想マシンからストレージへのアクセス方法	25
ストレージ デバイスの特徴	26
ストレージのタイプの比較	29
サポート対象のストレージ アダプタ	30
ストレージ アダプタ情報の表示	30
データストアの特性	31
データストア情報の表示	33
永続的なメモリの使用	34
PMEM データストアの統計情報の監視	36
3 ESXi と SAN の併用の概要	38
ESXi と SAN の使用例	39
SAN ストレージを ESXi と併用する場合の特性	39
ESXi ホストと複数のストレージ アレイ	40
LUN の決定	40
予測型スキームを使用した LUN の決定	41
適合型スキームを使用した LUN の決定	41
仮想マシンの場所の選択	41
サードパーティ製の管理アプリケーション	42
SAN ストレージ バックアップに関する考慮事項	43
サードパーティ製のバックアップ パッケージの使用	43
4 ESXi とファイバ チャネル SAN との併用	45
ファイバ チャネル SAN の概念	45
ファイバ チャネル SAN のポート	46
ファイバ チャネル ストレージ アレイのタイプ	46

- ゾーニングとファイバ チャネル SAN との併用 47
- 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 47

5 ファイバ チャネル ストレージの構成 49

- ESXi ファイバ チャネル SAN の要件 49
 - ESXi ファイバ チャネル SAN の制限 50
 - LUN 割り当ての設定 50
 - ファイバ チャネル HBA の設定 50
- インストールおよびセットアップの手順 51
- N-Port ID の仮想化 51
 - NPIV ベースの LUN アクセスの作動方法 51
 - NPIV 使用の要件 52
 - NPIV の機能と制限事項 52
 - WWN の割り当ての構成または変更 53

6 ファイバ チャネル オーバー イーサネットの構成 55

- ファイバ チャネル オーバー イーサネット アダプタ 55
- ソフトウェア FCoE の構成ガイドライン 56
- ソフトウェア FCoE 用のネットワークの設定 57
- ソフトウェア FCoE アダプタの追加 58

7 ファイバ チャネル SAN からの ESXi の起動 59

- SAN ブートのメリット 59
- 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 60
- SAN から起動するための準備 60
 - SAN コンポーネントとストレージ システムの構成 61
 - SAN から起動するストレージ アダプタの構成 61
 - 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 61
- SAN から起動する Emulex HBA の構成 62
 - BootBIOS プロンプトの有効化 62
 - BIOS の有効化 62
- SAN ブートを使用するように QLogic HBA を構成 63

8 ソフトウェア FCoE による ESXi のブート 65

- ソフトウェア FCoE 起動の要件と考慮事項 65
- ソフトウェア FCoE ブートの設定 66
 - ソフトウェア FCoE ブート パラメータの構成 67
 - ソフトウェア FCoE LUN からの ESXi のインストールと起動 67
- 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 68

9 ファイバ チャネル ストレージのベスト プラクティス 69

- ファイバ チャネル SAN の問題の防止 69
- 自動ホスト登録の無効化 70
- 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 70
 - ストレージ アレイ パフォーマンス 71
 - ファイバ チャネルによるサーバ パフォーマンス 71

10 iSCSI SAN と ESXi との併用 73

- iSCSI SAN について 73
- iSCSI マルチパス 74
- iSCSI SAN のノードおよびポート 74
- iSCSI 命名規則 75
- iSCSI イニシエータ 76
- VMware iSER アダプタについて 77
- iSCSI 接続の確立 77
- iSCSI ストレージ システムのタイプ 78
- 検出、認証、およびアクセス コントロール pacteriacontextmathced 79
- 仮想マシンから iSCSI SAN 上のデータへのアクセス方法 80
- エラー訂正 80

11 iSCSI アダプタおよびストレージの構成 82

- ESXi iSCSI SAN の推奨事項および制限事項 83
- アダプタの iSCSI パラメータの設定 83
- 独立型ハードウェア iSCSI アダプタの設定 84
 - 独立型ハードウェア iSCSI アダプタの表示 85
 - ハードウェア iSCSI のネットワーク設定の編集 86
- 依存型ハードウェア iSCSI アダプタの構成 87
 - 依存型ハードウェア iSCSI に関する考慮事項 88
 - 依存型ハードウェア iSCSI アダプタの表示 88
 - 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 89
- ソフトウェア iSCSI アダプタの構成 89
 - ソフトウェア iSCSI アダプタの有効化または無効化 90
- iSER アダプタの構成 91
 - VMware iSER アダプタの有効化 92
 - RDMA 対応のネットワーク アダプタの表示 93
- iSCSI または iSER アダプタの全般プロパティの変更 94
- iSCSI および iSER 用ネットワークの設定 95
 - iSCSI または iSER 構成での複数のネットワーク アダプタ 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 97
 - iSCSI または iSER のポートのバインドの設定 101
 - iSCSI ネットワークの管理 105
 - 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
ネットワークのジャンボ フレームの有効化	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 および iSER 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 または iSER アダプタの CHAP の設定	110
ターゲットの CHAP の設定	111
iSCSI 詳細パラメータの構成	112
iSCSI の詳細パラメータの構成	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	117
iSCSI SAN ブートに関する一般的な推奨事項	117
iSCSI SAN の準備	118
SAN 起動のための独立型ハードウェア iSCSI アダプタの構成	118
iSCSI 起動の設定	119
13 iSCSI ストレージのベスト プラクティス	121
iSCSI SAN の問題発生の防止	121
iSCSI SAN ストレージ パフォーマンスの最適化	122
ストレージ システムのパフォーマンス	122
iSCSI でのサーバ パフォーマンス	123
ネットワーク パフォーマンス	123
イーサネット スイッチ統計情報の確認	126
14 ストレージ デバイスの管理	127
ストレージ デバイスの特徴	127
ホストのストレージ デバイスの表示	128
アダプタのストレージ デバイスの表示	129
デバイス セクターのフォーマット	130
ストレージ デバイスの名前と識別子	132
NGUID デバイス識別子を持つ NVMe デバイス	133
NGUID 専用 NVMe デバイス搭載のステートレス ESXi ホストのバージョン 7.0 へのアップグレード	134
ストレージ デバイスの名前の変更	136
ストレージの再スキャン操作	137

ストレージの再スキャンの実行	137
アダプタの再スキャンの実行	138
スキャンするストレージ デバイスの数の変更	138
デバイス接続問題の確認	139
PDL 状態の検出	139
予定されるストレージ デバイスの削除の実行	140
PDL 状態からのリカバリ	141
一時的な APD 状態の処理	142
ストレージ デバイスの接続状態の確認	144
デバイスの接続問題と高可用性	144
ストレージ デバイスのロケータ LED の有効化または無効化	144
ストレージ デバイスでの消去	145
15 フラッシュ デバイスの操作	146
フラッシュ仮想ディスクの特定	147
ストレージ デバイスのマーク	147
ストレージ デバイスをフラッシュとしてマーク	147
ストレージ デバイスをローカルとしてマーク	148
フラッシュ デバイスの監視	149
フラッシュ デバイスのベスト プラクティス	149
フラッシュ デバイスの有効期間の推定	149
仮想フラッシュ リソースについて	150
仮想フラッシュ リソースの考慮事項	151
仮想フラッシュ リソースの設定	151
仮想フラッシュ リソースの削除	152
仮想フラッシュの詳細設定	153
VMFS データストアによるホスト キャッシュの構成	153
フラッシュ ディスクで VMFS を使用しないようにする	154
16 VMware NVMe ストレージについて	155
VMware NVMe の概念	155
基本的な VMware NVMe のアーキテクチャおよびコンポーネント	156
VMware NVMe ストレージの要件および制限事項	159
NVMe over RDMA (RoCE v2) ストレージ用のアダプタの構成	161
RDMA ネットワーク アダプタの構成	161
ソフトウェア NVMe over RDMA アダプタの有効化	163
NVMe over RDMA (RoCE v2) または FC-NVMe アダプタ用のコントローラの追加	164
ソフトウェア NVMe over RDMA アダプタの削除	165
17 データストアでの作業	166
データストアのタイプ	166

VMFS データストアについて	167
VMFS データストアのバージョン	168
VMFS データストアとリポジトリ	170
ホスト間の VMFS データストアの共有	170
VMFS メタデータ アップデート	171
VMFS のロック メカニズム	171
VMFS でのスナップショットのフォーマット	175
VMFS データストアのアップグレード	176
ネットワーク ファイル システム データストアについて	177
NFS プロトコルと ESXi	177
NFS ストレージのガイドラインと要件	179
NFS ストレージのファイアウォール構成	182
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	184
NFS 4.1 用 Kerberos の使用	184
NFS ストレージ環境のセットアップ	185
Kerberos 認証用 ESXi ホストの構成	186
データストアの作成	189
VMFS データストアの作成	189
NFS データストアの作成	191
vVols データストアの作成	192
重複 VMFS データストアの管理	192
VMFS データストア コピーのマウント	193
VMFS データストア キャパシティの増加	194
VMFS6 データストア上のクラスタ化された仮想ディスクのサポートの有効化または無効化	195
データストアの管理操作	196
データストア名の変更	197
データストアのアンマウント	197
データストアのマウント	198
VMFS データストアの削除	199
データストア ブラウザの使用	199
ストレージ フィルタのオフ	203
動的なディスクミラーリングの設定	204
VMFS データストアでの ESXi ホストの診断情報の収集	205
コア ダンプの場所としてのファイルの設定	206
コア ダンプ ファイルの有効化と削除	207
VOMA によるメタデータの整合性の確認	208
VOMA を使用したメタデータ整合性の確認	210
VMFS ポインタ ブロック キャッシュの構成	211
VMFS ポインタ ブロック キャッシュの情報の取得	212
ポインタ ブロック キャッシュのサイズ変更	213

18	マルチパスとフェイルオーバーについて	214
	ファイバ チャンネルを使用したフェイルオーバー	214
	iSCSI でのホスト ベースのフェイルオーバー	215
	iSCSI でのアレイ ベースのフェイルオーバー	217
	パスのフェイルオーバーと仮想マシン	218
	Windows ゲスト OS にタイムアウトを設定	218
	プラグ可能ストレージ アーキテクチャとパス管理	219
	プラグ可能ストレージ アーキテクチャについて	220
	VMware Native Multipathing Plug-In	221
	パス選択プラグインとポリシー	223
	VMware SATP	224
	VMware High Performance プラグインとパス選択スキーム	226
	パスの表示および管理	233
	ストレージ デバイス パスの表示	233
	データストア パスの表示	234
	パス選択ポリシーの変更	234
	遅延ラウンド ロビンのデフォルト パラメータの変更	235
	ストレージ パスの無効化	236
	要求ルールの使用	236
	マルチパスの考慮事項	237
	ホストのマルチパスの要求ルールの一覧表示	238
	マルチパスの要求ルールの追加	239
	マルチパスの要求ルールの削除	242
	パスのマスク	243
	パスのマスク解除	244
	NMP SATP ルールの定義	245
	仮想マシン I/O のキューのスケジュール設定	246
	ファイル I/O ごとのスケジュールの編集	246
	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	247
19	Raw デバイス マッピング	248
	RAW デバイス マッピングについて	248
	Raw デバイス マッピングのメリット	249
	RDM の注意事項と制限事項	252
	Raw デバイス マッピングの特性	252
	RDM の仮想および物理互換モード	252
	動的名前解決	253
	仮想マシン クラスタでの Raw デバイス マッピング	253
	利用可能な SCSI デバイス アクセス モードの比較	253
	RDM を使用する仮想マシンの作成	254
	マッピング済み LUN のパス管理	256

RDM を使用した仮想マシンで SCSI 照会キャッシュを無視する必要がある 256

20 ストレージ ポリシー ベースの管理 258

仮想マシン ストレージ ポリシー 259

仮想マシン ストレージ ポリシーのワークフロー 259

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 260

 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 261

 データストアへのタグの割り当て 262

ルールおよびルール セットについて 264

仮想マシン ストレージ ポリシーの作成と管理 266

 ホストベースのデータ サービスの仮想マシン ストレージ ポリシーの作成 266

 vVols 用の仮想マシン ストレージ ポリシーの作成 268

 タグベースの配置用に仮想マシン ストレージ ポリシーを作成 270

 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 271

ストレージ ポリシー コンポーネントについて 271

 ストレージ ポリシー コンポーネントの作成 272

 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 273

ストレージ ポリシーと仮想マシン 274

 仮想マシンへのストレージ ポリシーの割り当て 274

 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 276

 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 277

 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 277

 仮想マシン ストレージ ポリシーの再適用 278

デフォルト ストレージ ポリシー 279

 データストアのデフォルト ストレージ ポリシーの変更 280

21 ストレージ プロバイダの使用 281

ストレージ プロバイダについて 281

ストレージ プロバイダおよびデータの表現 282

ストレージ プロバイダの要件および考慮事項 283

ストレージ プロバイダの登録 283

ストレージ プロバイダ情報の表示 284

ストレージ プロバイダの管理 285

22 VMware vSphere Virtual Volumes (vVol) の操作 287

vVols について 287

vVols の概念 288

 Virtual Volumes オブジェクト 289

 vVols ストレージ プロバイダ 291

 vVols ストレージ コンテナ 291

 プロトコル エンドポイント 292

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	293
vVols データストア	293
vVols および仮想マシン ストレージ ポリシー	294
vVols とストレージ プロトコル	294
vVols アーキテクチャ	295
vVols および VMware Certificate Authority	297
Virtual Volumes スナップショット	298
vVols を有効にする前に	298
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	299
vVols の構成	300
vVols のストレージ プロバイダの登録	300
vVols データストアの作成	301
プロトコル エンドポイントの確認と管理	302
プロトコル エンドポイントのパス選択ポリシーの変更	303
vVols データストア上の仮想マシンのプロビジョニング	303
vVols およびレプリケーション	304
vVols でのレプリケーションの要件	305
vVols およびレプリケーション グループ	305
vVols およびフォルト ドメイン	306
vVols のレプリケーション ワークフロー	308
レプリケーションのガイドラインと考慮事項	308
vVols を使用する場合のベスト プラクティス	309
vVols を使用する場合のガイドラインと制限事項	310
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	310
vVols パフォーマンスのベスト プラクティス	311
vVols のトラブルシューティング	313
vVols および esxcli コマンド	313
vVols データストアにアクセスできない	313
vVols データストアへの仮想マシン移行時または Virtual Volumes データストアへの仮想マシン OVF のデプロイ時の失敗	314
23 仮想マシン I/O のフィルタリング	316
I/O フィルタについて	316
I/O フィルタのタイプ	317
I/O フィルタリング コンポーネント	317
I/O フィルタのストレージ プロバイダ	319
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	319
I/O フィルタのシステム要件	320
vSphere 環境での I/O フィルタの設定	321
クラスタでの I/O フィルタのインストール	321
I/O フィルタとストレージ プロバイダの表示	322
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	322

仮想マシンへの I/O フィルタ ポリシーの割り当て	323
I/O フィルタの管理	324
クラスタからの I/O フィルタのアンインストール	325
クラスタでの I/O フィルタのアップグレード	325
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	326
I/O フィルタによる仮想マシンの移行	326
I/O フィルタ インストール失敗の処理	327
単一の ESXi ホストへの I/O フィルタのインストール	327
24 ストレージのハードウェア アクセラレーション	328
ハードウェア アクセラレーションのメリット	328
ハードウェア アクセラレーションの要件	329
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	329
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	329
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	330
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	330
NAS デバイスでのハードウェア アクセラレーション	336
NAS プラグインのインストール	336
NAS プラグインのアンインストール	337
NAS プラグインの更新	338
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	338
ハードウェア アクセラレーションについての考慮事項	338
25 ストレージ プロビジョニングと容量の再利用	340
仮想ディスク シン プロビジョニング	340
仮想ディスクのプロビジョニング ポリシーについて	341
シン プロビジョニング仮想ディスクの作成	342
仮想マシン ストレージ リソースの表示	343
仮想マシンのディスク フォーマットの判別	344
シン仮想ディスクの拡張	344
データストアのオーバーサブスクリプションの処理	345
ESXi とアレイ シン プロビジョニング	345
容量の使用の監視	346
シン プロビジョニング ストレージ デバイスの識別	346
ストレージ容量の再利用	347
VMFS データストアからの容量再利用の要求	348
ゲスト OS からの容量の再利用の要求	353
26 クラウド ネイティブ ストレージの導入方法	355
クラウド ネイティブ ストレージの概念と用語	355
クラウド ネイティブ ストレージコンポーネント	358

ファイル ボリュームのプロビジョニング	360
クラウド ネイティブ ストレージユーザー	362
vSphere 管理者向けのクラウド ネイティブ ストレージ	362
クラウド ネイティブ ストレージの要件	362
クラウド ネイティブ ストレージロールと権限	366
ストレージ ポリシーを作成する	367
Kubernetes クラスタ仮想マシンを構成する	369
Kubernetes クラスタ間のコンテナ ボリュームの監視	370
Cloud Native Storage での暗号化の使用	371

27 vmkfstools の使用 373

vmkfstools コマンドの構文	373
vmkfstools コマンドのオプション	374
-v サブオプション	374
ファイル システムのオプション	375
仮想ディスクのオプション	377
ストレージ デバイス オプション	383

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。

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。

VMware vSphere[®]**Virtual Volumes™ (vVol)**

vVols 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。vVols 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 VMware vSphere Virtual Volumes \(vVol\) 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。

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 vVols 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 ストレージ ポリシー ベースの管理](#)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。

vVols、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、[プラグ可能ストレージ アーキテクチャとパス管理](#)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](#)
- [永続的なメモリの使用](#)

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。

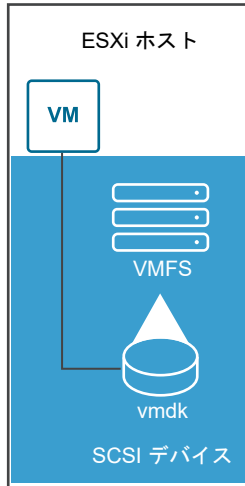
ローカル ストレージ

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、SAS、フラッシュ、および NVMe の各デバイスを含む、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。

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せん。

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。

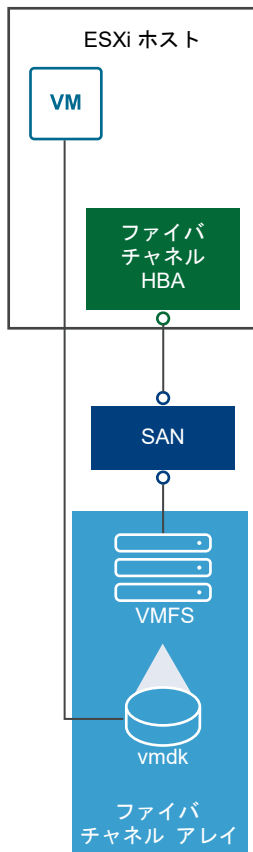
ファイバ チャンネル (FC)

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。

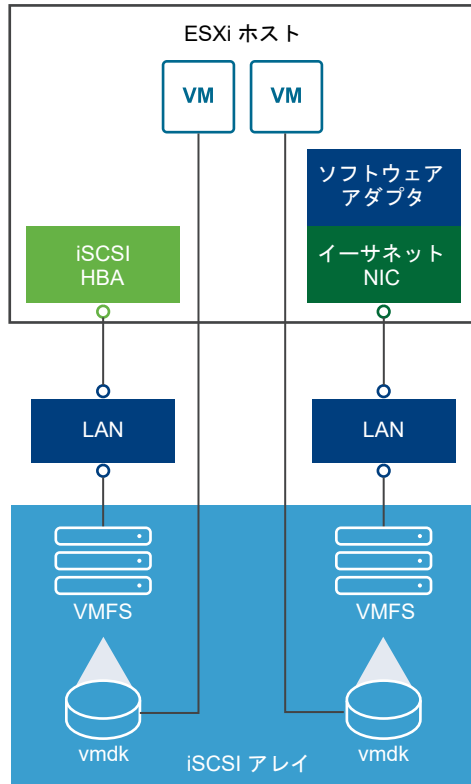
ハードウェア iSCSI ホストは、iSCSI とネットワーク処理の負荷を軽減できるサードパーティ製のアダプタを介してストレージに接続します。ハードウェア アダプタは依存型と独立型にできます。

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。

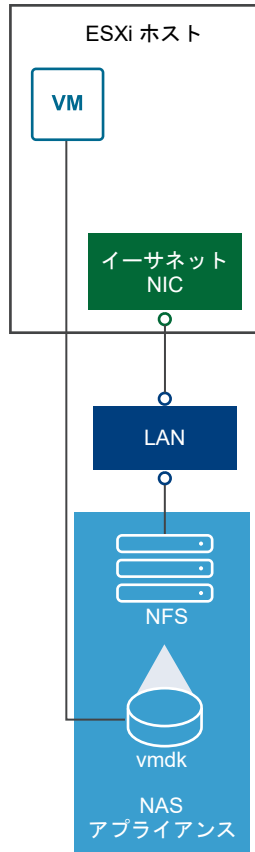
ネットワーク接続型ストレージ (NAS)

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。

NVMe over Fabrics ストレージ

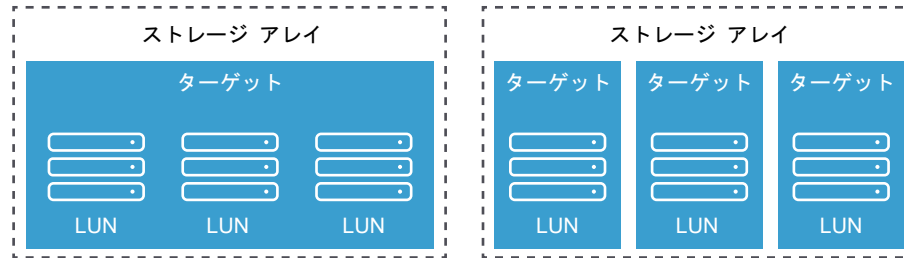
VMware NVMe over Fabrics (NVMe-oF) では、ホストと共有ストレージ アレイ上のターゲット ストレージ デバイス間の遠距離接続が可能になります。VMware は、NVMe over RDMA (RoCE v2 テクノロジーを使用) および NVMe over Fibre Channel (FC-NVMe) 転送をサポートします。詳細については、『[16 章 VMware NVMe ストレージについて](#)』を参照してください。

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。

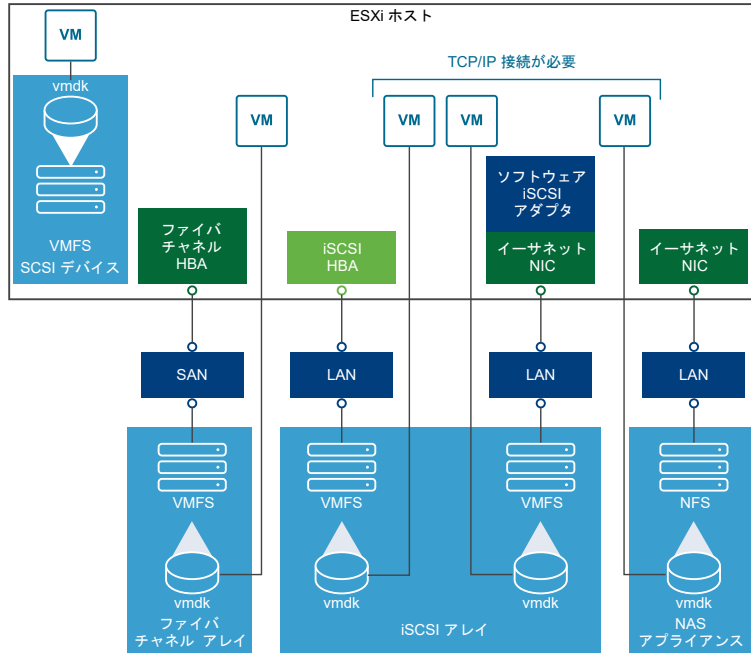
仮想マシンからストレージへのアクセス方法

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。

デバイスがホストに登録されたら、すべての利用可能なローカルおよびネットワーク デバイスを表示し、その情報を確認できます。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。

注： アレイで暗黙的な非対称論理ユニット アクセス (ALUA) がサポートされ、スタンバイ パスのみが含まれる場合、デバイスの登録は失敗します。デバイスは、ターゲットがスタンバイ パスを有効にし、ホストによりアクティブとして検出された後で、ホストに登録できます。システムの詳細 /Disk/FailDiskRegistration パラメータは、ホストのこの動作を制御します。

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。通常、この名前は任意の名前に変更できます。 ストレージ デバイスの名前の変更 を参照してください。
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。 ストレージ デバイスの名前と識別子 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
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。 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 ドライブおよび NVMe デバイスの詳細については、 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。「 プラグ可能ストレージ アーキテクチャとバス管理 」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。「 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 や 4Kn 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ています。「 デバイス セクターのフォーマット 」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。 デバイス セクターのフォーマット 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	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。 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	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。「 ストレージ バスの無効化 」を参照してください。

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 ホストに移動します。
- 2 [設定] 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
更新	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。
分離	選択したデバイスをホストから切断します。
添付	選択したデバイスをホストに接続します。
名前の変更	選択したデバイスの表示名を変更します。
LED を有効にする	選択したデバイスのロケータ LED をオンにします。
LED をオフにする	選択したデバイスのロケータ LED をオフにします。
フラッシュ ディスクとしてマーク	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。
HDD ディスクとしてマーク	選択したデバイスを HDD ディスクとしてマークします。
ローカルとしてマーク	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。
リモートとしてマーク	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。
パーティションの消去	選択したデバイスのパーティションを消去します。

- 6 次のタブを使用すると、選択したデバイスの追加情報へのアクセスや、プロパティの修正が可能になります。

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。
パーティションの詳細	パーティションとフォーマットに関する情報を表示します。

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 ホストに移動します。
- 2 [設定] 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
更新	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。
分離	選択したデバイスをホストから切断します。
添付	選択したデバイスをホストに接続します。
名前の変更	選択したデバイスの表示名を変更します。
LED を有効にする	選択したデバイスのロケータ LED をオンにします。
LED をオフにする	選択したデバイスのロケータ LED をオフにします。
フラッシュ ディスクとしてマーク	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。
HDD ディスクとしてマーク	選択したデバイスを HDD ディスクとしてマークします。
ローカルとしてマーク	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。
リモートとしてマーク	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。
パーティションの消去	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
ファイバチャネル	FC/SCSI	データ / LUN のブロック アクセス	FC HBA
ファイバチャネル オーバーイーサネット	FCoE/SCSI	データ / LUN のブロック アクセス	<ul style="list-style-type: none"> ■ 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

表 2-3. ストレージでサポートされる vSphere の機能 (続き)

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 Protectio n
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す。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す。

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

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

ソフトウェア FCoE アダプタの設定の詳細については、[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 ホストに移動します。
- 2 [設定] 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
ソフトウェア アダプタの追加	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。
更新	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。
ストレージの再スキャン	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。
アダプタの再スキャン	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。
[バス]	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バ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、vVols 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せん。
- 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 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 vVol	データストアに割り当てられた編集可能な名前。データストアの名前変更の詳細については、 データストア名の変更 を参照してください。
タイプ	VMFS NFS vSAN vVol	データストアが使用するファイル システム。VMFS および NFS データストアに関する情報とその管理方法については、 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。 vVols の詳細については、 22 章 VMware vSphere Virtual Volumes (vVol) の操作 を参照してください。
デバイス バックイング	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)、サブおよびフォルダ (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	vVol	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。
容量	VMFS NFS vSAN vVol	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 vVol	ホストの /vmfs/volumes/ ディレクトリのデータストアへのパス。
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 vVol	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。

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
ハードウェア アクセラレーション	VMFS NFS vSAN vVol	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。
Tags	VMFS NFS vSAN vVol	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 vVol	データストアがマウントされたホスト。
マルチパス	VMFS vVol	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 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。

手順

- 1 ホスト、クラスタ、データセンターなど、データストアの有効な親オブジェクトであるインベントリ オブジェクトに移動し、[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 データストアの右クリック メニューのオプションを使用して、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。

特定のオプションの可用性は、データストアとその構成のタイプによって異なります。

オプション	説明
[仮想マシンの登録]	既存の仮想マシンをインベントリに登録します。『vSphere の仮想マシン管理』を参照してください。
[データストアのキャパシティの増加]	VMFS データストアの容量を増やすか、エクステントを追加します。 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。
[ファイルの参照]	データストア ファイル ブラウザに移動します。 データストア ブラウザの使用 を参照してください。
[名前の変更]	データストアの名前を変更します。 データストア名の変更 を参照してください。
[データストアのマウント]	特定のホストにデータストアをマウントします。 データストアのマウント を参照してください。
[データストアのアンマウント]	特定のホストからデータストアをアンマウントします。 データストアのアンマウント を参照してください。

オプション	説明
[メンテナンス モード]	データストアをメンテナンス モードで使用します。『vSphere のリソース管理』を参照してください。
[Storage I/O Control の設定] (VMFS)	VMFS データストアに対して Storage I/O Control を有効にします。『vSphere のリソース管理』を参照してください。
[容量の再利用の編集] (VMFS)	VMFS データストアの容量の再利用設定を変更します。容量再利用の設定の変更を参照してください。
[データストアの削除] (VMFS)	VMFS データストアを削除します。VMFS データストアの削除を参照してください。
[タグとカスタム属性]	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。データストアへのタグの割り当てを参照してください。

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
[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。

永続的なメモリの使用

ESXi は、不揮発性メモリ (NVM) デバイスとも呼ばれる次世代の永続的なメモリ デバイスをサポートします。これらのデバイスは、メモリのパフォーマンスと速度を従来のストレージの永続性と組み合わせたものです。再起動や電源障害が発生しても、これらのデバイスに格納されたデータは保持されます。

高バンド幅、低遅延、および永続性を必要とする仮想マシンは、このテクノロジーを利用できます。たとえば、アクセラレーション データベースや分析ワークロードがある仮想マシンが該当します。

ESXi ホストで永続的なメモリを使用するには、次の概念に精通している必要があります。

PMEM データストア

ESXi ホストに永続的なメモリを追加すると、ホストは、そのハードウェアを検出し、フォーマットしてローカル PMEM データストアとしてマウントします。ESXi では、ファイル システムのフォーマットとして VMFS-L が使用されます。ホストごとに 1 つのローカル PMEM データストアのみがサポートされます。

注： 永続的な物理メモリを管理する場合は、すべての仮想マシンをホストから回避し、ホストをメンテナンス モードにしてください。

管理オーバーヘッドを軽減するために、PMEM データストアは、簡素化された管理モデルを提供します。一般に、従来のデータストア タスクはデータストアに適用されません。これは、必要なすべての操作がホストによって自動的にバックグラウン

ドで実行されるためです。管理者は、vSphere Client のデータストア ビューにデータストアを表示することも、他の通常のデータストア操作を実行することもできません。管理者が実行できる唯一の操作は、PMEM データストアの統計情報を監視することです。

PMEM データストアは、仮想 NVDIMM デバイスおよび仮想マシンの従来型の仮想ディスクを格納するために使用します。vmx および vmware.log ファイルを含む仮想マシンのホーム ディレクトリを PMEM データストアに配置することはできません。

PMEM アクセス モード

ESXi では、2 つの異なるモードで永続的なメモリが仮想マシンに公開されます。PMEM に対応する仮想マシンは、永続的なメモリに直接アクセスすることができます。従来型の仮想マシンは、PMEM データストアに格納されている高速仮想ディスクを使用できます。

直接アクセス モード

このモードでは、PMEM 領域を仮想の不揮発性デュアル インライン メモリ モジュール (NVDIMM) として仮想マシンに提示できます。仮想マシンは、NVDIMM モジュールを、電源サイクル間で維持できる標準のバイト アドレス指定可能なメモリとして使用します。

仮想マシンをプロビジョニングするときに、1 つまたは複数の NVDIMM モジュールを追加できます。

仮想マシンは、ハードウェア バージョン ESXi 6.7 以降で、PMEM に対応したゲスト OS を使用する必要があります。NVDIMM デバイスは、Windows 2016 のような、永続的なメモリをサポートする最新のゲスト OS に対応しています。

各 NVDIMM デバイスは、PMEM データストアに自動的に保存されます。

仮想ディスク モード

このモードは、従来型のすべての仮想マシンで使用可能であり、すべてのレガシーバージョンを含む、すべてのハードウェア バージョンをサポートしています。仮想マシンは、PMEM に対応している必要はありません。このモードを使用する場合は、通常の SCSI 仮想ディスクを作成し、PMEM 仮想マシン ストレージ ポリシーをディスクに適用します。ポリシーにより、ディスクが PMEM データストアに自動的に配置されます。

PMEM ストレージ ポリシ

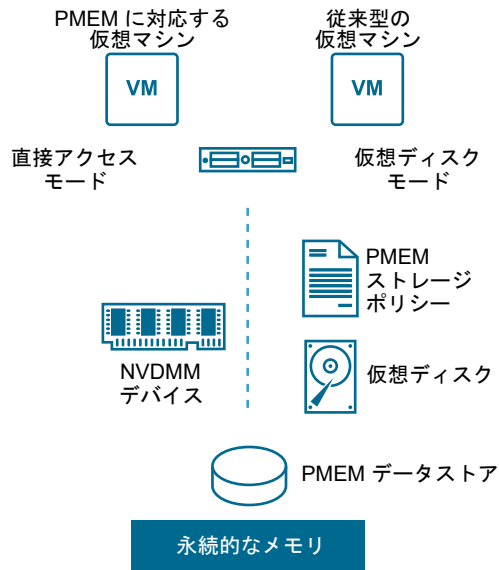
ー

PMEM データストアに仮想ディスクを配置するには、ホストのローカル PMEM のデフォルト ストレージ ポリシーをディスクに適用する必要があります。このポリシーは編集できません。

このポリシーは、仮想ディスクにのみ適用できます。仮想マシンのホーム ディレクトリは PMEM データストア上にないため、任意の標準データストアに配置してください。

PMEM ストレージ ポリシーを仮想ディスクに割り当てた後は、[仮想マシンの編集設定] ダイアログ ボックスでポリシーを変更することはできません。ポリシーを変更するには、仮想マシンを移行するかクローンを作成します。

次の図は、永続的なメモリのコンポーネントがどのように相互作用するかを示しています。



NVDIMM または仮想の永続的なメモリ ディスクを使用する仮想マシンを構成および管理する方法については、『vSphere のリソース管理』ドキュメントを参照してください。

PMEM データストアの統計情報の監視

vSphere Client および `esxcli` コマンドを使用して、PMEM データストアの容量や、その他のいくつかの属性を確認することができます。

ただし、VMFS や vVol などの通常のデータストアと異なり、PMEM データストアは vSphere Client の [データストア] ビューに表示されません。通常のデータストアの管理タスクは、PMEM データストアには適用されません。

手順

- ◆ PMEM データストアの情報を確認します。

オプション	説明
vSphere Client	a ESXi ホストに移動し、[サマリ] をクリックします。 b [ハードウェア] パネルで [永続的なメモリ] が表示されていることを確認して、その容量を確認します。
esxcli コマンド	<code>esxcli storage filesystem list</code> を使用して、PMEM データストアを一覧表示します。

例：PMEM データストアの表示

`esxcli storage filesystem list` コマンドを使用してデータストアを一覧表示すると、次のサンプル出力が表示されます。

```
# esxcli storage filesystem list
```

Mount Point	Volume Name	UUID	Mounted	Type	Size	Free
-----	-----	-----	-----	-----	-----	-----

/vmfs/volumes/5xxx...	ds01-102	5xxx...	true	VMFS-6	14227079168	12718178304
/vmfs/volumes/59ex...	ds02-102	59ex...	true	VMFS-6	21206401024	19697500160
/vmfs/volumes/59bx...		59bx...	true	vfat	4293591040	4274847744
/vmfs/volumes/pmem:5ax...	PMemDS-56ax...	pmem:5a0x...	true	PMEM	12880707584	11504975872

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での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 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> で当社のナレッジ ベースの記事を参照してください。
- ファイバ チャンネル 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 チャンネル 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。

いくつかの要因に応じて、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、定期的な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えます。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 ポ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。どうか、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 をあるホストからは使用できるようにして、別のホストからは使用できないようにする処理です。

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

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

ファイバ チャネル SAN のポート

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

WWPN (World Wide Port Name) グローバルで一意的なポート 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的なポート ID があり、ポートの FC アドレスとして機能します。この一意の ID によって、SAN 経由でそのポートにデータをルーティングできます。デバイスがファブリックにログインしたときに、FC スイッチはポート ID を割り当てます。ポート ID は、デバイスがログインしている間だけ有効です。

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

ファイバ チャネル ストレージ アレイのタイプ

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

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

アクティブ-アクティブのストレージ システム 大幅にパフォーマンスを低下させることなく、使用可能なすべてのストレージ ポートを通じて同時に LUN 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、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。

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。
- ファブリック内のパ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。
- Microsoft Windows を実行している仮想マシンで、SCSITimeoutValue 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 16 GB ファイバ チャンネル接続をサポートしています。

インストールおよびセットアップの手順

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

ESXi SAN 環境を構成するには、次の手順に従います。

- 1 SAN を構成していない場合、設計する。ほとんどの既存の SAN は、小さな変更だけで、ESXi と組み合わせることができます。
- 2 すべての SAN コンポーネントが要件を満たしていることを確認する。
- 3 ストレージ アレイに対して必要な変更を行う。

VMware ESXi と組み合わせて動作するように SAN をセットアップする方法については、ほとんどのベンダーがベンダー固有のドキュメントを提供しています。

- 4 SAN に接続したホストの HBA を設定する。
- 5 ホストに ESXi をインストールする。
- 6 仮想マシンを作成し、ゲスト OS をインストールする。
- 7 (オプション) VMware HA フェイルオーバーまたは Microsoft Clustering Service を使用するように、システムをセットアップする。
- 8 必要に応じて環境をアップグレードまたは変更する。

N-Port ID の仮想化

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

RDM を使用した仮想マシンのみが、WWN の割り当てを受け、これらの割り当てをすべての RDM トラフィックに使用できます。

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) 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。一意の識別子として、VPORT は、仮想マシンに割り当てられた WWN のペアを使用します。

各 VPORT は仮想マシンに特有のものです。仮想マシンをパワーオフすると、VPORT はホストで無効化され、FC ファブリックに認識されなくなります。仮想マシンが 1 つのホストから別のホストに移行すると、VPORT が最初のホスト上で閉じ、ターゲット ホスト上で開きます。

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 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。

- 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 を使用します。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 を検出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。
- 仮想マシンでストレージを使用しなくても、NPIV WWPN をゾーニングすると、クラスタ ホストがアクセスできるすべてのストレージ システムに接続できます。1 台以上の NPIV 対応仮想マシンが展開されているクラスタに、新しいストレージ システムを追加する場合は、NPIV WWPN が新しいストレージ システムのターゲットポートを検出できるように、新しいゾーンを追加します。

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。

WWN の割り当ての構成または変更

WWN 設定を仮想マシンに割り当てます。WWN の割り当ては後で変更できます。

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。

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、特定の状況では、WWN を変更または削除しなければならない場合があります。

前提条件

- WWN を構成する前に、アレイ側で構成されているストレージ LUN アクセス制御リスト (ACL) に ESXi ホストがアクセスできることを確認します。
- 既存の WWN を編集する場合は、仮想マシンをパワーオフします。

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] をクリックし、[ファイバ チャネル NPIV] を展開します。
- 3 次のいずれかのオプションを選択して、WWN の割り当てを作成または編集します。

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	仮想マシンの既存の WWN 割り当てを無効にしますが、削除はしないでください。
変更しない	既存の WWN 割り当てを保持します。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。

オプション	説明
新しい WWN を生成	新しい WWN を生成し、既存の WWN を上書きします。HBA の WWN は影響を受けません。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。
WWN 割り当ての削除	仮想マシンに割り当てられている WWN を削除します。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。

4 [OK] をクリックして、変更内容を保存します。

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。

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、ホストに適切なアダプタを設定します。

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。

VMware FCoE で使用可能なアダプタの詳細については、『VMware 互換性ガイド』を参照してください。

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オ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。vSphere Client 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、ESXi でネイティブの FCoE プロトコル スタックを使用して、FCoE プロセスの一部を実行します。ソフトウェア FCoE アダプタは、互換性のある NIC とともに使用する必要があります。

VMware は、ソフトウェア FCoE アダプタについて NIC の 2 つのカテゴリをサポートします。

部分的な FCoE オフロードのある NIC	オフロード機能の程度は、NIC のタイプによって異なります。一般的に NIC は、Data Center Bridging (DCB) 機能と I/O オフロード機能を提供します。
FCoE オフロードのない NIC	Data Center Bridging (DCB) 機能、および 10 Gbps 以上の速度がある NIC。ネットワーク アダプタは、FCoE オフロード機能をサポートする必要はありません。

ハードウェア FCoE アダプタとは違って、ソフトウェア アダプタは有効にする必要があります。アダプタを有効にする前に、ネットワークを適切に構成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 (All Path Down) 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および初期化するために FCoE が使用するプロトコルです。
- Priority-based Flow Control (PFC) を有効にして 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。
- vSwitch の MTU を 2500 以上に設定します。

ネットワーク アダプタのガイドラインおよびベスト 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。

- 部分的にオフロードされた NIC を使用する場合でも、FCoE に対応していない NIC を使用する場合でも、最新のマイクロコードがネットワーク アダプタにインストールされていることを確認します。
- FCoE に対応していない NIC を使用する場合は、ソフトウェア FCoE の有効にするための DCB 機能があ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、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 (All Path Down) 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。この変更を行う場合には、後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 ホストに移動します。
- 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 ジャンボ フレームを有効にするには、[MTU (バイト)] を 2,500 以上の値に変更し、[次へ] をクリックします。
- 6 [アダプタを追加] アイコンをクリックし、FCoE をサポートするネットワーク 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。

- 7 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。

- 8 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。

- 9 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 チャンネル 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 ホストに移動します。
- 2 [設定] 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]、[ソフトウェア アダプタの追加] 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、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、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。複数のパ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 だけにアクセスする必要があります。ストレージ システム ソフトウェアを使用して、ホストが、指定した LUN だけにアクセスすることを確認します。 ■ 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。
マルチパスのサポート	アクティブ-パッシブ アレイでは、起動 LUN へのマルチパスはサポートされていません。BIOS でマルチパスはサポートされず、スタンバイ パ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。

部分的 FCoE オフロードを含む NIC のみが、ソフトウェア FCoE によるブート機能をサポートしています。FCoE オフロードなしの NIC を使用する場合は、ソフトウェア FCoE によるブートがサポートされません。

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

- 互換性のあるバージョンの ESXi を使用します。

- 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。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。

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

- 障害に対する計画を立てます。
 - トポロジ マップの複製をいくつか作成します。エレメントごとに、エレメントに障害が発生した場合の SAN への影響を検討します。
 - 設計上の重大な障害を見落とさないように、さまざまなリンク、スイッチ、HBA、およびその他のエレメントを確認します。
 - ファイバ チャネル 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 ホストに移動します。
- 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、[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 ファブリックのパ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。

iSCSI SAN と ESXi との併用

10

ESXi は、インターネット SCSI (iSCSI) プロトコルを使用して、外部の SAN ストレージに接続できます。ESXi は、従来の iSCSI に加えて、iSCSI Extensions for RDMA (iSER) もサポートします。

iSER プロトコルが有効な場合、ホストは、同一の iSCSI フレームワークを使用できますが、リモート ダイレクト メモリ アクセス (RDMA) 転送を使用して、TCP/IP 転送が置き換えられます。

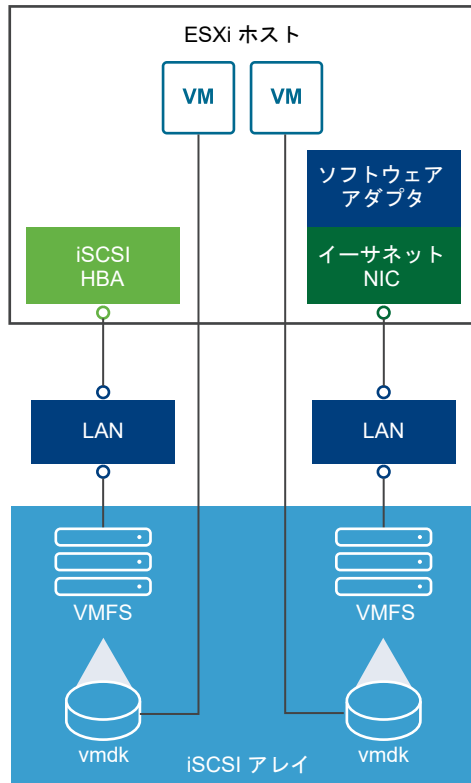
この章には、次のトピックが含まれています。

- [iSCSI SAN について](#)
- [iSCSI マルチパス](#)
- [iSCSI SAN のノードおよびポート](#)
- [iSCSI 命名規則](#)
- [iSCSI イニシエータ](#)
- [VMware iSER アダプタについて](#)
- [iSCSI 接続の確立](#)
- [iSCSI ストレージ システムのタイプ](#)
- [検出、認証、およびアクセス コントロール `pacteracontextmathced`](#)
- [仮想マシンから iSCSI SAN 上のデータへのアクセス方法](#)
- [エラー訂正](#)

iSCSI SAN について

iSCSI SAN は、ホストと高パフォーマンス 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 iSCSI 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。iSCSI ネットワークには、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 システムなども含まれます。



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、ESXi ホストで動作します。クライアントは SCSI コマンドを発行し、iSCSI プロトコルにカプセル化して iSCSI 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。通常、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 のノードおよびポート

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、ノード名が付いています。ESXi はいくつかの方法を使用してノードを識別します。

IP アドレス	各 iSCSI ノードには IP アドレスが関連付けられているため、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ホスト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 <code>iqn.1998-01.com.vmware:iscsitestox-68158ef2</code> 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	使用されている iSCSI デバイスまたはポートに付けられた管理しやすい名前です (iSCSI 名ではありません)。iSCSI エイリアスは一意ではありません。ポートに関連付けるためのわかりやすい名前です。

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。

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、ESXi ホストで iSCSI イニシエータを使用します。

このイニシエータは、ESXi ホストにインストールされたソフトウェアまたはハードウェアです。iSCSI イニシエータは、ホストと外部の iSCSI ストレージシステムとの間で通信を開始し、ストレージシステムにデータを送信します。

ESXi 環境では、ホスト上で設定された iSCSI アダプタがイニシエータの役割を果たします。ESXi は、いくつかのタイプの iSCSI アダプ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。

VMware iSER アダプタについて

ESXi は、従来の iSCSI に加えて、iSCSI Extensions for RDMA (iSER) プロトコルをサポートしています。iSER プロトコルが有効な場合、ESXi ホスト上の iSCSI フレームワークは、TCP/IP の代わりにリモートダイレクトメモリアクセス (RDMA) トランスポートを使用できます。

従来の iSCSI プロトコルは、ホスト上の iSCSI イニシエータとストレージデバイス上の iSCSI ターゲット間で TCP/IP ネットワークを介して SCSI コマンドを転送します。iSCSI プロトコルでは、コマンドをカプセル化し、そのデータを TCP/IP レイヤーのパケットに組み立てます。データが到着すると、iSCSI プロトコルは SCSI コマンドを区別してストレージデバイスに配信できるように、TCP/IP パケットを分解します。

iSER は TCP/IP データ転送モデルをリモートダイレクトメモリアクセス (RDMA) 転送に置き換えるため、従来の iSCSI とは異なります。iSER プロトコルは、RDMA の直接データ配置テクノロジーを使用して、ESXi ホストとストレージデバイスのメモリバッファ間で直接データを転送できます。この方法では、不要な TCP/IP 処理とデータの複製が必要なくなり、ストレージデバイス上の遅延と CPU 負荷も軽減できます。

iSER 環境では、iSCSI は以前と同様に動作しますが、TCP/IP ベースのインターフェイスではなく、基盤となる RDMA ファブリックインターフェイスを使用します。

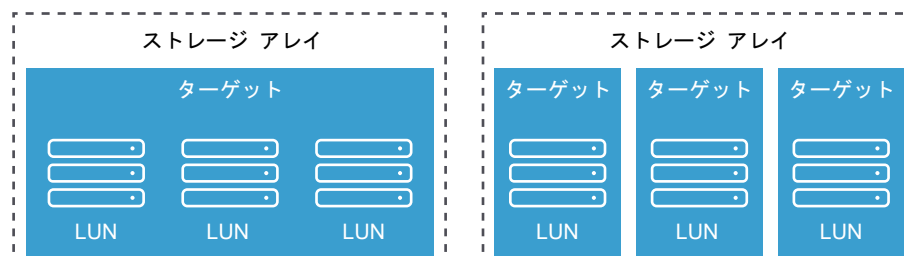
iSER プロトコルは iSCSI インフラストラクチャと互換性があるため、ESXi ホスト上で iSER を有効にするプロセスは iSCSI プロセスと似ています。[iSER アダプタの構成](#)を参照してください。

iSCSI 接続の確立

ESXi の文脈では、ターゲットという語は、ホストがアクセスできる 1 つのストレージユニットを表します。ストレージデバイスおよび LUN という語は、ターゲット上のストレージ容量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、ストレージをホスト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ます。別のベンダーは複数のターゲットにそれぞれ 1 つの LUN を表示します。

図 10-1. ターゲットと LUN との対応表現



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

ホスト ベースの iSCSI イニシエータは、各ターゲットに対して接続を確立します。複数の LUN が 1 つのターゲット内にあるストレージ システムの場合、すべてのトラフィックは単一の接続で行われます。3 つのターゲットにそれぞれ 1 つずつ LUN があるシステムの場合は、ホストと 3 つの LUN との間に個別の接続が 3 つ存在します。

この情報は、複数の iSCSI アダプタを使用して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ちます。あるターゲットへのトラフィックを特定のアダプタに設定し、別のターゲットへのトラフィックは別のアダプタに設定して使用することができます。

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 pacteracontextmathced

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。pacteracontextmathced

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。pacteracontextmathced

検出 pacteracontextmathced

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。pacteracontextmathcedESXi 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。

pacteracontextmathced 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。pacteracontextmathced 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。pacteracontextmathced

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。pacteracontextmathced

認証 pacteracontextmathced

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。pacteracontextmathcedESXi は CHAP 認証プロトコルをサポートします。pacteracontextmathcedCHAP 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。

pacteracontextmathced

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。

pacteracontextmathced

アクセス コントロール pacteracontextmathced

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。pacteracontextmathced ほとんどの実装環境で、次に示す 3 つうちの 1 つ以上のアクセス コントロール機能をサポートしています。

pacteracontextmathced

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

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。pacteracontextmathced

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。pacteracontextmathced

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。

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。

ヘッダー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。ダイジェストでは、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。

ヘッダー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。

iSCSI アダプタおよびストレージの構成

11

ESXi で iSCSI SAN を使用するためには、iSCSI 環境を設定する必要があります。

iSCSI 環境を準備するプロセスは次のとおりです。

手順	詳細
iSCSI ストレージの設定	詳細は、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。また、推奨事項は以下のとおりです。 <ul style="list-style-type: none">■ ESXi iSCSI SAN の推奨事項および制限事項■ 13 章 iSCSI ストレージのベストプラクティス
iSCSI アダプタの設定	適切なワークフローに沿ってアダプタを設定します。 <ul style="list-style-type: none">■ 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 アダプタの構成■ ソフトウェア iSCSI アダプタの構成■ iSER アダプタの構成
iSCSI ストレージでのデータストアの作成	データストアの作成

この章には、次のトピックが含まれています。

- [ESXi iSCSI SAN の推奨事項および制限事項](#)
- [アダプタの iSCSI パラメータの設定](#)
- [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 アダプタの構成](#)
- [ソフトウェア iSCSI アダプタの構成](#)
- [iSER アダプタの構成](#)
- [iSCSI または iSER アダプタの全般プロパティの変更](#)
- [iSCSI および iSER 用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 の推奨事項および制限事項

iSCSI SAN を適切に使用するには、ESXi 環境で特定の推奨事項に沿う必要があります。また、iSCSI SAN で ESXi を使用する場合は、いくつかの制限事項が適用されます。

iSCSI ストレージの推奨事項

- ESXi ホストが、iSCSI 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。
- 起動時にホストが LUN を認識できるようにするために、すべての iSCSI ストレージ ターゲットを設定し、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。ホストを設定し、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。
- 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。
- 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。
- Microsoft Windows を実行している仮想マシンで、SCSITimeoutValue 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 仮想マシンがバ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。
- 各 LUN に VMFS データストアが 1 つとなるよう、使用環境を設定します。

iSCSI ストレージの制限事項

- 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。

アダプタの iSCSI パラメータの設定

ESXi ホストが iSCSI ストレージを検出できるようにするには、iSCSI アダプタを設定する必要があります。アダプタを設定する場合は、複数の iSCSI パラメータを設定します。

iSCSI ネットワーク

特定のタイプの iSCSI アダプタに対しては、VMkernel 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。

独立型ハードウェア iSCSI アダプタでは、VMkernel ネットワークは必要ありません。独立型ハードウェア iSCSI アダプタでは、IP アドレス、サブネット マスク、デフォルト ゲートウェイなどのネットワーク パラメータを設定できます。

すべてのタイプの iSCSI アダプタで、IPv4 および IPv6 プロトコルがサポートされます。

iSCSI アダプタ (vmhba)	説明	VMkernel ネットワーク	アダプタのネットワーク設定
独立型ハードウェア iSCSI アダプタ	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。	詳細については、 ハードウェア iSCSI のネットワーク設定の編集 を参照してください。
ソフトウェア iSCSI アダプタ	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。 詳細については、 iSCSI および iSER 用ネットワークの設定 を参照してください。	該当なし
依存型ハードウェア iSCSI アダプタ	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 詳細については、 iSCSI および iSER 用ネットワークの設定 を参照してください。	該当なし
VMware iSER アダプタ	RDMA 対応のネットワーク アダプタを使用して、ホストをリモート iSCSI ターゲットに接続します。	必須 詳細については、 iSCSI および iSER 用ネットワークの設定 を参照してください。	該当なし

検出方法

すべてのタイプの iSCSI アダプタに対し、動的検出アドレスまたは静的検出アドレスを設定する必要があります。さらに、ストレージ システムのターゲット名を指定する必要があります。ソフトウェア iSCSI および依存型ハードウェア iSCSI の場合は、vmkping を使用してアドレスに ping を送信できます。

[iSCSI アダプタの検出アドレスの構成](#)を参照してください。

CHAP 認証

イニシエータおよびストレージ システム側で CHAP パラメータを有効にします。有効にした認証は、まだ検出されていないすべてのターゲットに適用されます。検出済みのターゲットには適用されません。

[iSCSI アダプタの CHAP パラメータの構成](#)を参照してください。

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 ESXi ホスト上に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。

独立型ハードウェア iSCSI アダプタの設定のプロセスには、次の手順が含まれます。

手順	説明
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。
iSCSI または iSER アダプタの全般プロパティの変更	必要に応じて、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します。独立型ハードウェア 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。
ハードウェア iSCSI のネットワーク設定の編集	デフォルトのネットワーク設定を変更して、アダプタが iSCSI SAN 用に適切に設定されるようにします。
iSCSI および iSER の動的または静的検出の設定	動的検出を設定します。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。
iSCSI または iSER アダプタの CHAP の設定	iSCSI 環境では、Challenge Handshake Authentication Protocol (CHAP) を使用する場合、それをアダプタに対して設定します。
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	iSCSI 環境がジャンボ フレームをサポートしている場合は、アダプタに対してジャンボ フレームを有効にします。

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 ホストに移動します。
- 2 [設定] 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。

アダプタ情報	説明
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。
パス	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パス。

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 ホストに移動します。
- 2 [設定] 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 [ネットワークの設定] 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。

オプション	説明
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。

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 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。

手順	説明
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。
iSCSI または iSER アダプタの全般プロパティの変更	必要に応じて、アダプタに割り当てられているデフォルトの iSCSI 名およびエイリアスを変更します。
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	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する必要があります。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。
iSCSI または iSER のポートのバインドの設定	iSCSI コンポーネントと物理ネットワーク アダプタ間のトラフィックの接続を設定します。これらの接続を設定するプロセスは、ポートのバインドと呼ばれます。
iSCSI および iSER の動的または静的検出の設定	動的検出を設定します。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。
iSCSI または iSER アダプタの CHAP の設定	iSCSI 環境では、Challenge Handshake Authentication Protocol (CHAP) を使用する場合、それをアダプタに対して設定します。
ターゲットの CHAP の設定	検出アドレスまたは静的ターゲットごとに別々の CHAP 証明書を設定できます。
ネットワークのジャンボ フレームの有効化	iSCSI 環境がジャンボ フレームをサポートしている場合は、アダプタに対してジャンボ フレームを有効にします。

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、これにはバッファ容量に制限があります。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 台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。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することをお勧めします。

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 ホストに移動します。
- 2 [設定] 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。

手順

- 1 ホストに移動します。
- 2 [設定] 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 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。
- 5 [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 および iSER 用ネットワークの設定](#)を参照してください。

ソフトウェア iSCSI アダプタの構成

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場合は、次の点を考慮してください。

- 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 アダプタの構成プロセスでは、いくつかの手順を実行します。

手順	説明
ソフトウェア iSCSI アダプタの有効化または無効化	ソフトウェア iSCSI アダプタを有効にして、ホストが iSCSI ストレージへのアクセスに使用できるようにします。
iSCSI または iSER アダプタの全般プロパティの変更	必要に応じて、アダプタに割り当てられているデフォルトの iSCSI 名およびエイリアスを変更します。

手順	説明
iSCSI または iSER のポートのバインドの設定	iSCSI コンポーネントと物理ネットワーク アダプタ間のトラフィックの接続を設定します。これらの接続を設定するプロセスは、ポートのバインドと呼ばれます。
iSCSI および iSER の動的または静的検出の設定	動的検出を設定します。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。
iSCSI または iSER アダプタの CHAP の設定	iSCSI 環境で Challenge Handshake Authentication Protocol (CHAP) を使用する場合は、アダプタに対して設定します。
ターゲットの CHAP の設定	検出アドレスまたは静的ターゲットごとに別々の CHAP 証明書を設定できます。
ネットワークのジャンボ フレームの有効化	iSCSI 環境がジャンボ フレームをサポートしている場合は、アダプタに対してジャンボ フレームを有効にします。

ソフトウェア iSCSI アダプタの有効化または無効化

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

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 ホストに移動します。
- 2 [設定] タブをクリックします。

3 アダプタを有効または無効にします。

オプション	説明
ソフトウェア iSCSI アダプタの有効化	<p>a [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。</p> <p>b [ソフトウェア iSCSI アダプタ] を選択し、アダプタを追加します。</p> <p>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。これでアダプタの設定が完了します。</p>
ソフトウェア iSCSI アダプタの無効化	<p>a [ストレージ] で、[ストレージ アダプタ] をクリックし、無効にするアダプタ (vmhba#) を選択します。</p> <p>b [プロパティ] タブをクリックします。</p> <p>c [無効化] をクリックして、アダプタを無効にします。</p> <p>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。</p> <p>d ホストを再起動します。</p> <p>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。アダプタに関連付けられているストレージ 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にすることもできます。</p>

iSER アダプタの構成

ホスト上の iSCSI フレームワークが TCP/IP の代わりにリモート ダイレクト メモリ アクセス (RDMA) トランスポートを使用できるように、ESXi ホスト上に iSER を構成します。

ホストにインストールすると、RDMA 対応のアダプタは vCenter Server でネットワーク アダプタ (vmnic) として表示されます。

アダプタを機能させるには、VMware iSER コンポーネントを有効にしてから、iSER アダプタを RDMA 対応の vmnic に接続する必要があります。その後で、iSER アダプタにターゲットや CHAP などの一般的なプロパティを設定できます。

iSER アダプタの設定および構成プロセス全体で、いくつかの手順を実行します。

手順	説明
VMware iSER アダプタの有効化	esxcli コマンドを使用して、VMware iSER アダプタを有効にします。
iSCSI または iSER アダプタの全般プロパティの変更	必要に応じて、アダプタに割り当てられているデフォルトの名前とエイリアスを変更します。
iSCSI または iSER のポートのバインドの設定	<p>iSER エンジンと RDMA 対応のネットワーク アダプタをバインドするには、ネットワーク接続を作成する必要があります。これらの接続を設定するプロセスは、ポートのバインドと呼ばれます。</p> <p>注： iSER は NIC チーミングをサポートしません。ポートのバインドを設定する場合は、vSwitch ごとに 1 つの RDMA アダプタのみを使用します。</p>
iSCSI および iSER の動的または静的検出の設定	動的検出を設定します。動的検出では、イニシエータが指定された iSER 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。iSER 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。
iSCSI または iSER アダプタの CHAP の設定	環境で Challenge Handshake Authentication Protocol (CHAP) を使用している場合は、アダプタに CHAP を構成します。

手順	説明
ターゲットの CHAP の設定	検出アドレスまたは静的ターゲットごとに別々の CHAP 証明書を設定できます。
ネットワークのジャンポ フレームの有効化	環境でジャンポ フレームがサポートされている場合は、アダプタのジャンポ フレームを有効にします。

VMware iSER アダプタの有効化

esxcli コマンドを使用して、VMware iSER アダプタを有効にします。

前提条件

- iSCSI ストレージで iSER プロトコルがサポートされていることを確認します。
- ESXi ホストに RDMA 対応アダプタをインストールします。
- RDMA 対応スイッチを使用します。
- ESXi ホストでフロー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。詳細については、VMware のナレッジ ベースの記事 <http://kb.vmware.com/kb/1013413> を参照してください。
- iSER のイニシエータとターゲット間にロスレス接続を確立するように RDMA スイッチ ポートを設定します。

手順

- 1 ESXi Shell または vSphere CLI を使用して、iSER アダプタを有効にします。

```
esxcli rdma iser add
```

2 VMware iSER アダプタが追加されていることを確認します。

- a ホストに移動します。
- b [設定] タブをクリックします。
- c [ストレージ] で [ストレージ アダプタ] をクリックして、アダプタのリストを確認します。

このアダプタが有効になっている場合は、VMware iSCSI over RDMA (iSER) アダプタのカテゴリのリストにアダプタ (vmhba#) が表示されます。

Storage Adapters

Adapter	Type	Status	Identifier	Targets	Devices	Paths
vmhba33	Block SCSI	Unknown	--	1	2	2
Model: VMware iSCSI over RDMA (iSER) Adapter						
vmhba64	iSCSI	Unbound	Iser-vmnic9(ign.1998-01.com.vmware.prim	0	0	0
vmhba65	iSCSI	Unbound	Iser-vmnic10(ign.1998-01.com.vmware.prim	0	0	0
vmhba66	iSCSI	Unbound	Iser-vmnic4(ign.1998-01.com.vmware.prim	0	0	0
vmhba67	iSCSI	Unbound	Iser-vmnic5(ign.1998-01.com.vmware.prim	0	0	0
Model: Wellburg AHCI Controller						
vmhba1	Block SCSI	Unknown	--	0	0	0
vmhba2	Block SCSI	Unknown	--	1	1	1

Properties | Devices | Paths | Dynamic Discovery | Static Discovery | Network Port Binding | Advanced Options

General

Name	vmhba64	Edit...
Model	VMware iSCSI over RDMA (iSER) Adapter	
iSCSI Name	ign.1998-01.com.vmware.prim-fcoe-005.eng.vmw	
iSCSI Alias	iser-vmnic9	
Target Discovery	Send Targets, Static Targets	

Authentication

Method	None	Edit...
--------	------	-------------------------

RDMA 対応のネットワーク アダプタの表示

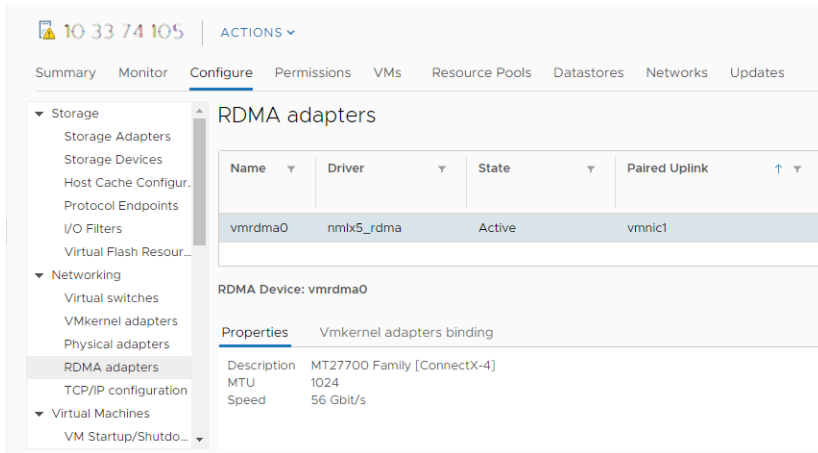
ESXi は、RDMA 対応のネットワーク アダプタ (Mellanox Technologies MT27700 Family ConnectX-4 など) をサポートします。このようなアダプタをホストにインストールすると、vSphere Client には、RDMA アダプタと物理ネットワーク アダプタの 2 つのコンポーネントが表示されます。

vSphere Client を使用して、RDMA アダプタとそれに対応するネットワーク アダプタを表示できます。

手順

- 1 ホストに移動します。
- 2 [ネットワーク] で、[RDMA アダプタ] をクリックします。

この例では、RDMA アダプタは `vmrdma0` としてリストに表示されます。[ペアリングされたアップリンク] 列には、ネットワーク コンポーネントが `vmnic1` 物理ネットワーク アダプタとして表示されます。



3 アダプタの説明を確認するには、リストから RDMA アダプタを選択し、[プロパティ] タブをクリックします。

結果

アダプタの vmnic# ネットワーク コンポーネントは、iSER や NVMe over RDMA などのストレージ設定に使用できます。iSER のポートのバインドについては、[iSCSI または iSER のポートのバインドの設定](#)を参照してください。NVMe over RDMA の詳細については、[NVMe over RDMA \(RoCE v2\) ストレージ用のアダプタの構成](#)を参照してください。

iSCSI または iSER アダプタの全般プロパティの変更

iSCSI または iSER アダプタに割り当てられたデフォルトの名前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： 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 ホストに移動します。
- 2 [設定] 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 [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。

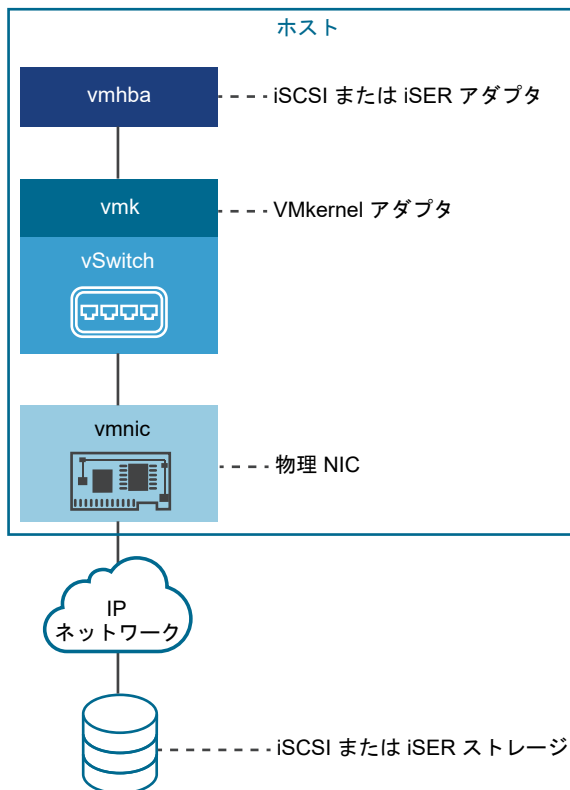
結果

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 および iSER 用ネットワークの設定

特定のタイプの iSCSI アダプタは、VMkernel ネットワークに依存します。これらのアダプタには、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、RDMA (iSER) アダプタを介する VMware iSCSI が含まれます。環境にこれらのアダプタのいずれかが含まれている場合は、iSCSI または iSER コンポーネントと物理ネットワーク アダプタの間のトラフィックの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。各仮想および物理ネットワーク アダプタ間で 1:1 のマッピングを使用します。その際に、VMkernel アダプタを適切な iSCSI または iSER 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。



ポート バインドを設定するときは、次のルールに準拠します。

- 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。
- RDMA 対応のネットワーク アダプタにのみ、iSER アダプタを接続する必要があります。

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。

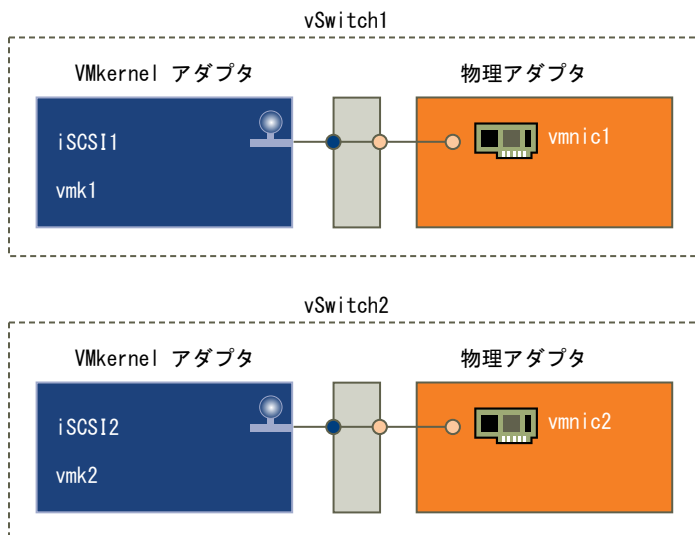
iSCSI または iSER 構成での複数のネットワーク アダプタ

ホストが iSCSI または iSER 用の複数の物理ネットワーク アダプタを使用している場合は、アダプタをマルチパスに利用できます。

複数の物理アダプタを単一スイッチ構成または複数スイッチ構成で使用できます。

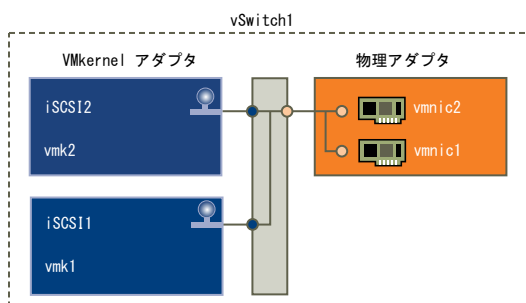
複数スイッチ構成では、仮想 - 物理アダプタのペアごとに個別の vSphere スイッチを指定します。

図 11-1. 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 1 台の vSphere スイッチに追加する方法があります。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。iSER では NIC チーミングがサポートされないため、単一スイッチ構成は iSER に適しません。

図 11-2. 単一の vSphere Standard Switch での 1 対 1 のアダプタ マッピング



このタイプの構成では、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 アダプタをマッピングする必要があります（表を参照）。

VMkernel アダプタ (vmk#)	物理ネットワーク アダプタ (vmnic#)
vmk1 (iSCSI1)	[有効なアダプタ] vmnic1 [未使用のアダプタ] vmnic2
vmk2 (iSCSI2)	[有効なアダプタ] vmnic2 [未使用のアダプタ] vmnic1

Distributed Switch を使用することもできます。vSphere Distributed Switch の詳細およびデフォルトのネットワーク ポリシーの変更方法については、『vSphere のネットワーク』ドキュメントを参照してください。

複数の物理アダプタを使用する場合の考慮事項を次に示します。

- 物理ネットワーク アダプタは、接続対象のストレージ システムと同じサブネット上になければなりません。
- (iSCSI のみ対象、iSER は非対象) 別々の vSphere スイッチを使用する場合は、異なる IP サブネットにそれらを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、ホストが LUN を検出できません。
- iSER では NIC チーミングがサポートされないため、単一スイッチ構成は iSER に適しません。

以下の条件が存在するときには、ポート バインドは使用しないでください。

- アレイ ターゲットの iSCSI ポートが別のブロードキャスト ドメインおよび IP サブネットに存在する。
- iSCSI 接続に使用する VMkernel アダプタが、別のブロードキャスト ドメイン、IP サブネットに存在するか、異なる仮想スイッチを使用している。

注： iSER 構成では、iSER 接続に使用する VMkernel アダプタを統合トラフィックに使用できません。iSER を使用した ESXi ホストと iSER ターゲットとの間の接続を有効にするために作成した VMkernel アダプタは、iSER トラフィックにのみ使用します。

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

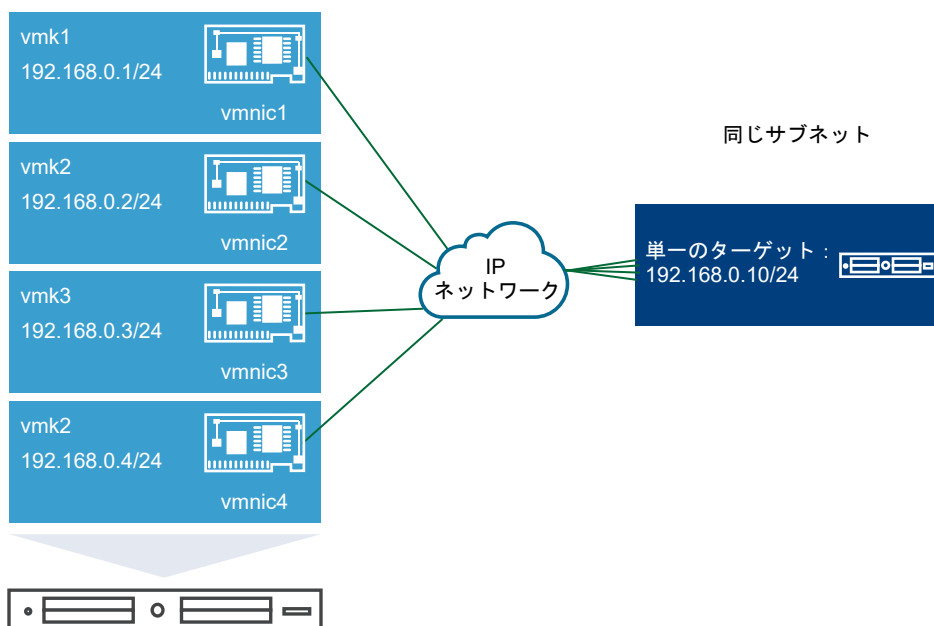
次の例を参照してください。

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。

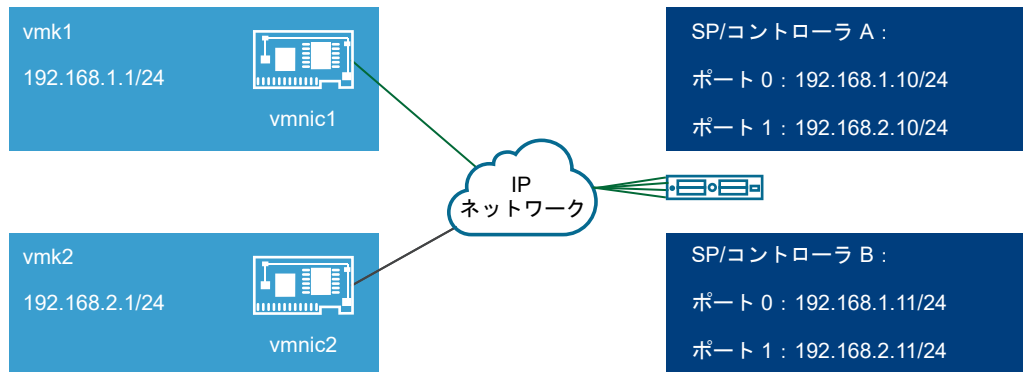


この例では、すべてのイニシエータ ポートとターゲット ポータルが同じサブネットに属しています。また、バインドされているすべてのポートを通じてターゲットに到達できます。VMkernel ポートが 4 つ、ターゲット ポータルが 1 つ存在するため、合計 4 つのパスが作成されます。

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。

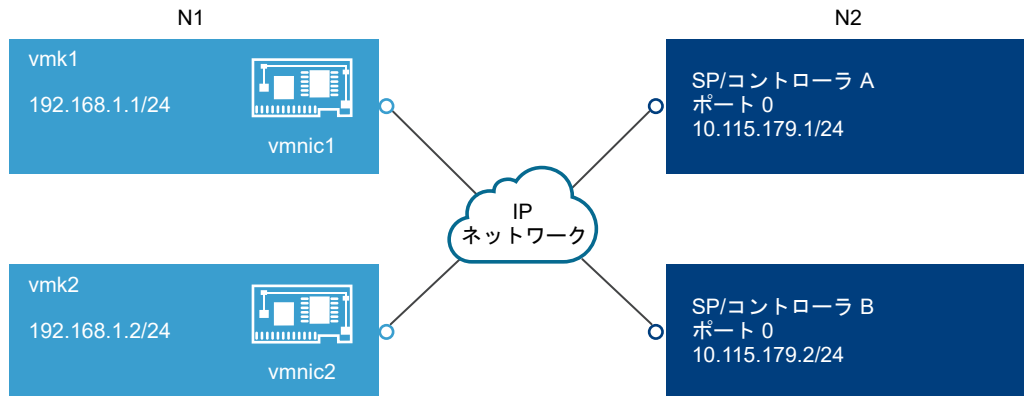
パス	説明
パス 1	vmk1 とコントローラ A のポート 0
パス 2	vmk1 とコントローラ B のポート 0
パス 3	vmk2 とコントローラ A のポート 1
パス 4	vmk2 とコントローラ B のポート 2

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る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。

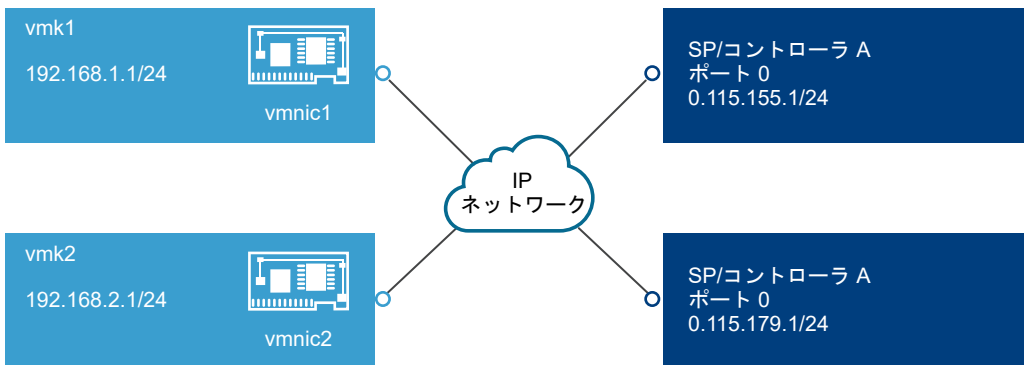


次のコマンドを使用します。

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

例 2：複数のパ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
vmk1	10.115.179.209	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	true
vmk2	10.115.179.146	255.255.252.0	10.115.179.255	DHCP	10.115.179.253	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 または iSER のポートのバインドの設定

ポートのバインドは、特定のタイプの iSCSI および iSER アダプタと物理ネットワーク アダプタ間のトラフィックの接続を作成します。

次のタイプのアダプタには、ポートのバインドが必要です。

- ソフトウェア iSCSI アダプタ
- 依存型ハードウェア iSCSI アダプタ
- VMware iSCSI over RDMA (iSER) アダプタ

次のタスクでは、vSphere 標準スイッチと単一の物理ネットワーク アダプタによるネットワーク構成について説明します。複数のネットワーク アダプタがある場合は、[iSCSI または iSER 構成での複数のネットワーク アダプタ](#)を参照してください。

注： iSER は NIC チーミングをサポートしません。iSER のポートのバインドを設定する場合は、vSwitch ごとに 1 つの RDMA 対応物理アダプタ (vmnic#) と 1 つの VMkernel アダプタ (vmk#) のみを使用します。

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 Data Center for vSphere』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 または iSER 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。作成した VMkernel アダプタは、iSCSI または iSER アダプタとともにポートのバインド設定で使用します。

2 iSCSI または iSER アダプタの VMkernel アダプタへのバインド

iSCSI または iSER アダプタと VMkernel アダプタをバインドします。

3 ポート バインドの詳細の確認

iSCSI または iSER vmhba 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 または iSER 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。作成した VMkernel アダプタは、iSCSI または iSER アダプタとともにポートのバインド設定で使

次のタイプのアダプタには、ポートのバインドが必要です。

- ソフトウェア iSCSI アダプタ
- 依存型ハードウェア iSCSI アダプタ
- VMware iSCSI over RDMA (iSER) アダプタ

前提条件

- 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物理ネットワーク アダプタ (vmnic#) を使用する必要があります。[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。
- iSER アダプタでは、適切な RDMA 対応の vmnic# を使用してください。[RDMA 対応のネットワーク アダプタの表示](#)を参照してください。

手順

- 1 ホストに移動します。
- 2 右クリック メニューから [ネットワークの追加] を選択します。
- 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 に使用する適切なネットワーク 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。

- 6 ネットワーク ラベルを入力します。

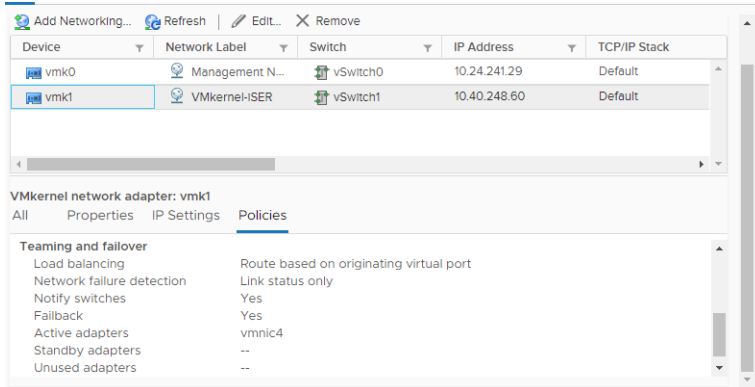
ネットワーク ラベルは、「iSCSI」や「iSER」など、作成する VMkernel アダプタを識別するわかりやすい名前です。

- 7 IP アドレス設定を指定します。
- 8 情報を確認し、[終了] をクリックします。

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。

9 設定を確認します。

- a [ネットワーク] で [VMkernel アダプタ] を選択し、リストから VMkernel アダプタ (vmk#) を選択します。
- b [ポリシー] タブをクリックし、対応する物理ネットワーク アダプタ (vmnic#) が [チームングおよびフェイルオーバー] に有効なアダプタとして表示されていることを確認します。



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 VMkernel アダプタを iSCSI または iSER vmhba アダプタにバインドします。

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できます。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。詳細については、『[iSCSI または iSER 構成での複数のネットワーク アダプタ](#)』を参照してください。

iSCSI または iSER アダプタの VMkernel アダプタへのバインド

iSCSI または iSER アダプタと VMkernel アダプタをバインドします。

次のタイプのアダプタには、ポートのバインドが必要です。

- ソフトウェア iSCSI アダプタ
- 依存型ハードウェア iSCSI アダプタ
- VMware iSCSI over RDMA (iSER) アダプタ

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 ホストに移動します。
- 2 [設定] 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、iSCSI または iSER アダプタ (vmhba#) をリストから選択します。

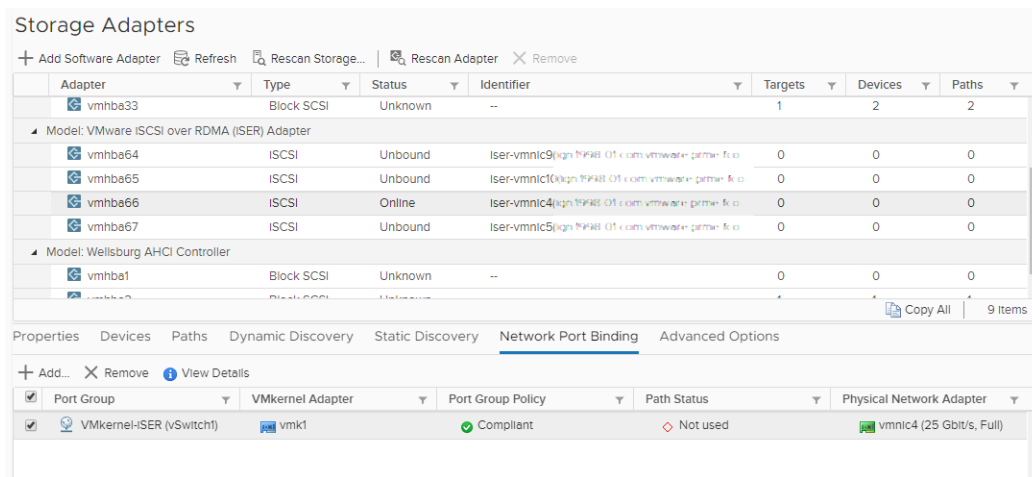
- 4 [ネットワーク ポートのバインド] タブをクリックし、[追加] アイコンをクリックします。
- 5 iSCSI または iSER アダプタとバインドする VMkernel アダプタを選択します。

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 アダプタまたは iSER 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。

ネットワーク接続が、iSCSI または iSER アダプタのネットワーク 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 または iSER vmhba 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。

次のタイプのアダプタには、ポートのバインドが必要です。

- ソフトウェア iSCSI アダプタ
- 依存型ハードウェア iSCSI アダプタ
- VMware iSCSI over RDMA (iSER) アダプタ

手順

- 1 ホストに移動します。
- 2 [設定] 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、iSCSI または iSER アダプタをリストから選択します。
- 4 [ネットワーク ポートのバインド] タブをクリックし、VMkernel アダプタをリストから選択します。
- 5 [詳細表示] アイコンをクリックします。
- 6 利用可能なタブを切り替えて、VMkernel アダプタおよび物理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せん。

iSCSI のネットワーク接続を作成した後、vSphere 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 アドレスの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 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 および iSER 用ネットワークの設定](#) を参照してください。

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。

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。

- すべてのネットワーク コンポーネントは、ジャンボ フレームをサポートする必要があります。
- ご使用の物理 NIC および iSCSI アダプタがジャンボ 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 11-1. 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。
VMware iSER	サポートあり。ベンダーに確認。

ネットワークのジャンボ フレームの有効化

トラフィックに VMkernel ネットワークを使用する iSCSI アダプタまたは iSER アダプタで、ジャンボ フレームを有効にすることができます。これらのアダプタには、ソフトウェア iSCSI アダプタ、依存型ハードウェア iSCSI アダプタ、および VMware iSER アダプタが含まれます。

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ます。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 ホストに移動します。
- 2 [設定] タブをクリックします。
- 3 [ネットワーク] で、[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 で最大の MTU サイズに設定します。ESXi では、最大 9,000 バイトの MTU サイズがサポートされます。

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 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 ホストに移動します。
- 2 [設定] 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 [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、次回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 および iSER 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 ホストに移動します。
- 2 [設定] 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 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。

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 ホストに移動します。
- 2 [設定] 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 [動的検出] と [静的検出] を切り替えます。
- 5 削除する iSCSI サーバを選択し、[削除] をクリックします。
- 6 iSCSI アダプタを再スキャンします。

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

iSCSI アダプタの CHAP パラメータの構成

リモート ターゲットへの接続に iSCSI テクノロジーで使用する IP ネットワークでは、転送するデータが保護されないため、接続のセキュリティを確保する必要があります。iSCSI の実装するプロトコルの 1 つに、CHAP (チャレ

ンジ ハンドシェイク認証プロトコル) があります。CHAP は、ネットワーク上のターゲットにアクセスするイニシエータの正当性を検証します。

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

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

CHAP 認証方法の選択

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

CHAP を構成する前に、iSCSI ストレージ システムで CHAP が有効になっているかどうかを確認します。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。

一方向 CHAP

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

双方向 CHAP

双方向の CHAP 認証は、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 11-2. 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向 CHAP を使用する	ホストは CHAP 以外の接続を優先しますが、ターゲットが要求する場合は CHAP 接続を使用できます。	ソフトウェア iSCSI 依存型ハードウェア iSCSI

表 11-2. CHAP のセキュリティ レベル (続き)

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

iSCSI または iSER アダプタの CHAP の設定

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

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

前提条件

- ソフトウェア iSCSI または依存型ハードウェア iSCSI の CHAP パラメータを設定する前に、一方方向 CHAP を構成するか、双方方向 CHAP を構成するかを決めます。独立型ハードウェア iSCSI アダプタは、双方方向 CHAP をサポートしません。
- ストレージ側で設定された 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 [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方向 CHAP を使用]
 - [一方方向 CHAP を使用]
 - [双方方向 CHAP を使用する]。双方方向 CHAP を構成するには、このオプションを選択する必要があります。

4 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、ストレージ側で構成した名前と一致するようにします。
- iSCSI アダプタ名に CHAP 名を設定するには、[イニシエータ名の使用] を選択します。
 - CHAP 名を iSCSI イニシエータ名以外の名前に設定するには、[イニシエータ名の使用] を選択解除し、[名前] テキスト ボックスに名前を入力します。
- 6 認証の一部として、使用する送信 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。
- 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。

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 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、『ESXCLI スタート ガイド』ドキュメントを参照してください。

アダプタのタイプによっては、使用できないパラメータがあります。

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 11-3. iSCSI イニシエータの追加パラメータ

詳細パラメータ	説明
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。
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。
ErrorRecoveryLevel	ホストの iSCSI イニシエータがログイン時にネゴシエートする iSCSI エラー リカバリ レベル (ERL) の値。
LoginRetryMax	ESXi iSCSI イニシエータが、ターゲットへのログインを試行する回数の最大値。
MaxOutstandingR2T	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。
FirstBurstLength	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。
MaxBurstLength	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。
MaxRecvDataSegLength	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。
MaxCommands	iSCSI アダプタ上でキューに格納できる SCSI コマンドの最大数。
DefaultTimeToWait	予期しない接続の終了またはリセットの後で、ログアウトやアクティブなタスクの再割り当てを試みるまでの最小待機時間 (秒)。
DefaultTimeToRetain	接続の終了またはリセットの後で、アクティブなタスクの再割り当てが可能な状態を維持する最大時間 (秒)。
LoginTimeout	イニシエータがログイン応答を終了させるまでの待機時間 (秒)。
LogoutTimeout	イニシエータがログアウト要求 PDU の応答を取得するまでの待機時間 (秒)。
RecoveryTimeout	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。
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。
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。
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。
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。

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 ホストに移動します。
- 2 [設定] 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。

オプション	説明
アダプタ レベルで	[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。
ターゲット レベルで	<ol style="list-style-type: none"> a [動的検出] または [静的検出] 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] をクリックします。

- 5 変更する詳細パラメータに必要な値を入力します。

iSCSI セッションの管理

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

ソフトウェア iSCSI および依存型ハードウェア iSCSI イニシエータは、各イニシエータ ポートと各ターゲット ポートのために 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。

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。ESXCLI 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 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
<code>-A --adapter=str</code>	たとえば、iSCSI アダプタ名は <code>vmhba34</code> です。
<code>-s --isid=str</code>	iSCSI セッションの識別子。
<code>-n --name=str</code>	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。

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

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。

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

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
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。	ソフトウェア iSCSI アダプタと、iSCSI Boot Firmware Table (iBFT) 形式をサポートするネットワーク アダプタを使用します。詳細については、『ESXi のインストールとセットアップ』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](#)

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、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、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、『vCenter Server 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。

手順

- 1 インストール メディアを起動し、ホストを再起動します。
- 2 BIOS を使用して、最初にインストール メディアから起動するようにホストを設定します。
- 3 サーバが POST で送信中に Ctrl + q 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。

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に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意であり、適切にフォーマットされていることを確認します。ストレージ アクセスの問題を回避するには、異なるホスト上でも、同じ iSCSI 名を異なるアダプタに決して割り当てないでください。

iSCSI SAN ストレージ パフォーマンスの最適化

一般的な SAN 環境の最適化には、いくつかの要因があります。

ネットワーク環境が適切に構成されている場合、iSCSI コンポーネントは優れたスループットを発揮し、iSCSI イニシエータおよびターゲットの待ち時間は十分短くなります。ネットワーク輻輳が発生し、リンク、スイッチ、またはルータが飽和した場合、iSCSI のパフォーマンスが低下し、ESXi 環境に適さなくなることもあります。

ストレージ システムのパフォーマンス

ストレージ システムのパフォーマンスは、iSCSI 環境全体のパフォーマンスに影響する主要な要因の 1 つです。

ストレージ システムのパフォーマンスに問題が発生した場合、これに関連する情報はストレージ システム ベンダーが提供するドキュメントを参照してください。

LUN を割り当てるときは、複数のホストから各共有 LUN にアクセスでき、各ホストで複数の仮想マシンを実行できる点に注意してください。ESXi ホストで使用される 1 つの LUN が、異なるオペレーティング システムで実行される多様なアプリケーションからの I/O を提供する可能性があります。このような場合はさまざまなワークロードが発生するため、ESXi を I/O の頻繁なアプリケーションに使用していない別のホストの LUN を、ESXi LUN のある RAID グループに含めないでください。

読み取りキャッシュおよび書き込みキャッシュを有効にします。

ロード バランシングは、サーバの I/O 要求を使用可能なすべての SP およびそれに関連付けられているホスト サーババスに分散するプロセスです。目的は、スループットの観点からパフォーマンスを最適化することにあります（1 秒あたりの I/O 数、1 秒あたりのメガバイト数、またはレスポンス タイム）。

SAN ストレージ システムには、I/O がすべてのストレージ システム バスの間でバランスがとられるように、継続的な再設計と調整が必要です。この要件を満たすために、すべての SP 間で LUN へのバスを分散し、最適なロード バランシングを提供します。詳細な監視によって、手動で LUN の分散を再調整する必要がある時期が示されます。

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

iSCSI でのサーバ パフォーマンス

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。

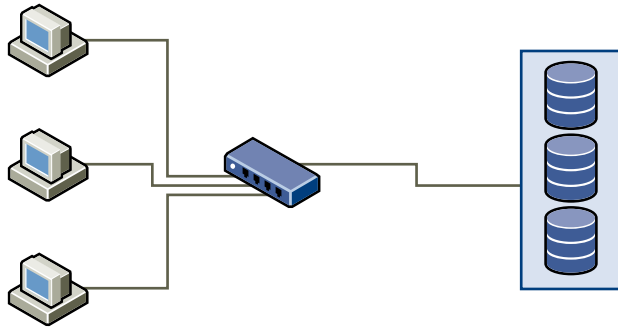
- 各 LUN を、必要なパフォーマンス レベルを提供する RAID グループに配置する。割り当てられた RAID グループにあるほかの LUN のアクティビティおよびリソースの使用を監視します。I/O を行うアプリケーションが多すぎる高性能 RAID グループは、ESXi ホストで実行されるアプリケーションで要求されるパフォーマンス目標を達成できないことがあります。
- ピーク期間中にホスト上のすべてのアプリケーションで最大のスループットを実現するために、十分なネットワーク アダプタまたは iSCSI ハードウェア アダプタをインストールします。I/O を複数のポートに分散させることで、それ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 アダプタにイーサネットアダプ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。

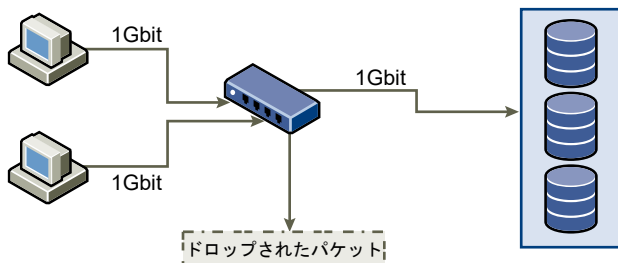
図 13-1. ストレージへの単一のイーサネット リンク



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。この転送データを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 32 KB までバッファ可能な場合、サーバが 256 KB 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	47784000	63677	0

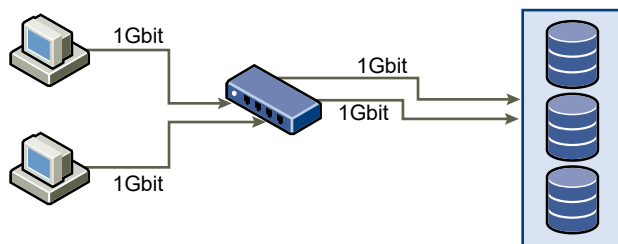
この Cisco のスイッチの例では、使用しているバンド幅が 476,303,000 ビット/秒で、ケーブル速度の半分未満です。ポートは受信パケットをバッファしますが、一部のパケットをドロップしています。このインターフェイスの最終行にある概要情報を見ると、IQD 列で、このポートではすでに約 10,000 の受信パケットがドロップされているとわかります。

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 つの出カ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 デバイスの名前と識別子](#)
- [ストレージの再スキャン操作](#)
- [デバイス接続問題の確認](#)
- [ストレージ デバイスのロケータ LED の有効化または無効化](#)
- [ストレージ デバイスでの消去](#)

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。

デバイスがホストに登録されたら、すべての利用可能なローカルおよびネットワーク デバイスを表示し、その情報を確認できます。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。

注： アレイで暗黙的な非対称論理ユニット アクセス (ALUA) がサポートされ、スタンバイ パスのみが含まれる場合、デバイスの登録は失敗します。デバイスは、ターゲットがスタンバイ パスを有効にし、ホストによりアクティブとして検出された後で、ホストに登録できます。システムの詳細 `/Disk/FailDiskRegistration` パラメータは、ホストのこの動作を制御します。

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。通常、この名前は任意の名前に変更できます。 ストレージ デバイスの名前の変更 を参照してください。
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。 ストレージ デバイスの名前と識別子 を参照してください。
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。 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 ドライブおよび NVMe デバイスの詳細については、 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。「 プラグ可能ストレージ アーキテクチャとバス管理 」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。「 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 や 4Kn 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ています。「 デバイス セクターのフォーマット 」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 デバイスへのパス。
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。 デバイス セクターのフォーマット 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	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。 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	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。「 ストレージ バスの無効化 」を参照してください。

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 ホストに移動します。

- 2 [設定] 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
更新	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。
分離	選択したデバイスをホストから切断します。
添付	選択したデバイスをホストに接続します。
名前の変更	選択したデバイスの表示名を変更します。
LED を有効にする	選択したデバイスのロケータ LED をオンにします。
LED をオフにする	選択したデバイスのロケータ LED をオフにします。
フラッシュ ディスクとしてマーク	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。
HDD ディスクとしてマーク	選択したデバイスを HDD ディスクとしてマークします。
ローカルとしてマーク	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。
リモートとしてマーク	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。
パーティションの消去	選択したデバイスのパーティションを消去します。

- 6 次のタブを使用すると、選択したデバイスの追加情報へのアクセスや、プロパティの修正が可能になります。

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。
パス	デバイスで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。
パーティションの詳細	パーティションとフォーマットに関する情報を表示します。

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 ホストに移動します。
- 2 [設定] 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
更新	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。
分離	選択したデバイスをホストから切断します。
添付	選択したデバイスをホストに接続します。
名前の変更	選択したデバイスの表示名を変更します。
LED を有効にする	選択したデバイスのロケータ LED をオンにします。
LED をオフにする	選択したデバイスのロケータ LED をオフにします。
フラッシュ ディスクとしてマーク	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。
HDD ディスクとしてマーク	選択したデバイスを HDD ディスクとしてマークします。
ローカルとしてマーク	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。
リモートとしてマーク	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。
パーティションの消去	選択したデバイスのパーティションを消去します。

デバイス セクターのフォーマット

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、一定の量のデータが格納されます。

次の表に、ESXi でサポートされているさまざまなストレージ デバイスのフォーマットを示します。

ストレージ デバイスのフォーマット	ESXi ソフトウェア エミュレーション	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	該当なし	512	512	VMFS5 および VMFS6 (デフォルト)
512e	該当なし	512	4096	VMFS5 および VMFS6 (デフォルト) 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。
4Kn	512	4096	4096	VMFS 6

512 バイトのネイティブ フォーマット

ESXi は、512 バイトのネイティブ セクター サイズを使用する従来の 512n ストレージ デバイスをサポートしています。

512 バイト エミュレーションのフォーマット

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) などのアドバンスト 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、アドバンスト 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。これらのデバイスは、4Kn セクター ドライブに移行するための中間段階として使用できます。

ソフトウェア エミュレーション機能を備えた 4K ネイティブ フォーマット

ESXi がサポートするもう 1 つのアドバンスト フォーマットは、4Kn セクター テクノロジーです。4Kn デバイスでは、物理セクターおよび論理的セクターは両方とも長さが 4,096 バイト (4 KiB) です。デバイスにはエミュレーション レイヤーがありませんが、ESXi に 4Kn 物理セクター サイズを直接公開します。

ESXi は 4Kn デバイスを検出および登録し、それらを 512e として自動的にエミュレートします。デバイスは、512e として ESXi の上位レイヤーに提供されます。ただし、ゲスト OS では常に 512n デバイスとして認識されます。4Kn デバイスを備えたホストで、レガシー ゲスト OS およびアプリケーションがインストールされた既存の仮想マシンを引き続き使用することができます。

4Kn デバイスを使用する場合は、次の考慮事項が適用されます。

- ESXi はローカルな 4Kn SAS および SATA HDD のみをサポートします。
- ESXi は、4Kn SSD および NVMe デバイスまたは 4Kn デバイスを RDM としてサポートしません。
- ESXi は、UEFI を備えた 4Kn デバイスからのみ起動できます。
- 4Kn デバイスを使用して、コアダンプ パーティションおよびコアダンプ ファイルを構成できます。
- 4Kn デバイスを要求できるのは、NMP プラグインのみです。これらのデバイスを要求するのに、HPP を使用できません。
- vSAN で使用できるのは、vSAN ハイブリッド アレイ対応の 4Kn キャパシティ HDD のみです。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。
- ソフトウェア エミュレーション レイヤーがあるため、4Kn デバイスのパフォーマンスは I/O の配置に依存します。パフォーマンスを最適化するには、主に 4K で整列された I/O を送信するワークロードを実行します。
- エミュレートされた 4Kn デバイスに Scatter-Gather I/O (SGIO) を使用して直接アクセスするワークロードの場合は、512e ディスクと互換性のある I/O を送信する必要があります。

例： デバイス フォーマットの識別

デバイスで 512n、512e、または 4Kn のいずれのフォーマットが使用されるのかを識別するには、次のコマンドを実行します。

```
esxcli storage core device capacity list
```

次のサンプル出力に、フォーマットの種類を示したものです。

Device Type	Physical Blocksize	Logical Blocksize	Logical Block Count	Size	Format
-----	-----	-----	-----	-----	-----

naa.5000xxxxxxxx36f	512	512	2344225968	1144641 MiB	512n
naa.5000xxxxxxxx030	4096	512	3516328368	1716957 MiB	4Kn SWE
naa.5000xxxxxxxx8df	512	512	2344225968	1144641 MiB	512n
naa.5000xxxxxxxx4f4	4096	512	3516328368	1716957 MiB	4Kn SWE

ストレージ デバイスの名前と識別子

ESXi 環境では、各ストレージ デバイスは複数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。

ストレージにより提供される識別子

ESXi ホストは、ターゲット ストレージ デバイスからデバイス名を照会します。返されたメタデータから、ホストはデバイスの一意の識別子を抽出または生成します。識別子は特定のストレージ標準に基づいており、すべてのホストで一貫かつ永続的なもので、次のいずれかの形式をとります。

- naa.xxx
- eui.xxx
- t10.xxx

パスベースの識別子

デバイスが識別子を提供しない場合、ホストは `mpx` を生成します。*path* の名前。ここで *path* はたとえば `mpx.vmhba1:C0:T1:L3` のようなデバイスの最初のパスを表します。この識別子は、ストレージに提供される識別子と同じように使用できます。

`mpx.path` 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

`device-provided identifiers` または `mpx.path` 識別子の他に、ESXi は各デバイスの代替のレガシー名も生成します。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、識別子は、SCSI INQUIRY コマンドで取得されたメタデータから部分的に取得することができます。SCSI INQUIRY 識別子を提供しない非ローカル デバイスの場合は `vml.number` 識別子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 storage core device list` コマンドを使用すると、vSphere CLI に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 storage core device list
naa.XXX
    Display Name: DGC Fibre Channel Disk(naa.XXX)
    ...
    Other UIDs: vml.000XXX
mpx.vmhba1:C0:T0:L0
    Display Name: Local VMware Disk (mpx.vmhba1:C0:T0:L0)
    ...
    Other UIDs: vml.0000000000XYZ
```

NGUID デバイス識別子を持つ NVMe デバイス

NVMe デバイスの場合、ESXi はデバイスから取得した情報に基づいてデバイス ID を生成します。一般に、NVMe デバイスは、EUI64 形式または NGUID 形式の識別子をサポートしているか、両方の形式を使用しています。NGUID は、EUI64 16 バイトの指定子形式を使用する名前空間グローバル一意識別子です。

NGUID 形式のみをサポートするデバイスの場合、ホストによって生成されるデバイス識別子は ESXi のバージョンによって変わります。バージョン 6.7 以前の ESXi ホストでは `t10.xxx_controller_serial_number` 識別子が作成されます。6.7 Update 1 以降では、ホストにより 2 つの識別子が作成されます。プライマリとして、`eui.xxx (NGUID)`、代替プライマリとして、`t10.xxx_controller_serial_number`。

デバイスでサポートされている ID の形式		ホストによって生成されるデバイス識別子	
EUI64 ID 形式	NGUID ID 形式	ESXi 6.7 以前	ESXi 7.0
はい	はい	t10.xxx_EUI64	t10.xxx_EUI64
はい	いいえ	t10.xxx_EUI64	t10.xxx_EUI64
いいえ	はい	t10.xxx_controller_serial_number	プライマリ ID として、eui.xxx (NGUID) 代替プライマリ ID として、t10.xxx_controller_serial_number

注： ホストに NGUID 専用デバイスが含まれていて、ホストを以前のバージョンから ESXi7.0 にアップグレードすると、デバイス識別子は、t10.xxx_controller_serial_number から euixxx (NGUID) に変更されます (ESXi 環境全体)。お客様のスクリプトのいずれかでデバイス識別子を使用する場合は、この形式の変更を反映する必要があります。

プライマリ デバイス識別子と代替デバイス識別子間のマッピングの確認

esxcli storage core device uidmap list コマンドを使用して、デバイス識別子を確認します。出力は次のようになります。

```
esxcli storage core device uidmap list
eui.0000xyz.....
  Primary UID: eui.0000xyz.....
  Alternative Primary UIDs: t10.0000abc....
  Legacy UID: vml.0000000000766d68....
  Alternative Legacy UIDs: vml.000000000080906....
```

NGUID 専用 NVMe デバイス搭載のステートレス ESXi ホストのバージョン 7.0 へのアップグレード

環境にバージョン 6.7 以前のステートレス ESXi ホストが含まれ、NGUID 形式のみをサポートする NVMe デバイスが含まれている場合は、現在のワークフローを使用してホストをバージョン 7.0 にアップグレードします。

ステートレス ホストをバージョン 6.7 以前からバージョン 7.0 にアップグレードする場合は、以下の手順を実行してストレージ構成を保持します。以下の手順を使用せずにアップグレードを実行すると、アップグレード中にホストプロファイルでキャプチャされたすべてのストレージ構成が保持されないことがあります。その結果、アップグレード後にホスト プロファイル コンプライアンス エラーが発生する可能性があります。

前提条件

- 環境には、ステートレス ESXi6.7 以前のホストが含まれています。
- 環境には、NGUID 形式のみをサポートする NVMe デバイスが含まれています。

手順

1 ホストに NGUID 専用 NVMe デバイスが含まれているかどうかを判定します。

a デバイスのベンダーが NVMe であるかどうかを確認します。

例として、次のコマンドを使用します。

```
# esxcli storage core device list -d eui.f04xxxxxxxx0000000100000001
eui.f04xxxxxxxx0000000100000001
Display Name: Local NVMe Disk (eui.f04xxxxxxxx0000000100000001)
Has Settable Display Name: true
Devfs Path: /vmfs/devices/disks/eui.f04bxxxxxxxx0000000100000001
Vendor: NVMe
```

Vendor: NVMe 行は、デバイスが NVMe であることを示します。

b どの HBA が NVMe デバイ스에 接続されているかを判定します。

```
# esxcli storage core adapter device list
HBA    Device UID
-----
vmhba2 eui.f04xxxxxxxx0000000100000001
```

c HBA と名前空間 ID を使用して、NVMe デバイスの名前空間情報を取得します。

```
# esxcli nvme device namespace get -A vmhba2 -n 1
Namespace Identify Info:
Namespace Size: 0xe8e088b0 Logical Blocks
Namespace Capacity: 0xe8e088b0 Logical Blocks
. . .
NVM Capacity: 0x1d1c1116000
Namespace Globally Unique Identifier: 0xf04xxxxxxxx0000000100000001
IEEE Extended Unique Identifier: 0x0
```

出力では、NGUID 専用 NVMe デバイスの場合、フィールド IEEE Extended Unique Identifier には 0 が含まれ、Namespace Globally Unique Identifier には 0 以外の値が含まれています。

- 2 ホスト プロファイルでキャプチャされたストレージ構成を保持するには、ステートレス ホストを 7.0 にアップグレードする際、次の手順を実行します。

- a アップグレードする前に、`esx.conf` を永続的な場所に保存してください。

たとえば、`esx.conf` ファイルを VMFS データストアにコピーできます。

```
# cp /etc/vmware/esx.conf /vmfs/volumes/datastore1/
```

- b ホストをアップグレードします。

アップグレード後、ホストがプロファイルに準拠していないため、メンテナンス モードのままになることがあります。

- c 新しい ID 形式を使用して、NGUID 専用 NVMe デバイスのデバイス設定を適用します。

`esx.conf` ファイルの場所を示すホストから、次のコマンドを実行します。

```
# python ./usr/lib/vmware/nvme-nguid-support/bin/nguidApplySettings.pyc -l /vmfs/volumes/datastore1/
```

- 3 ホストから設定をコピーし、ホストのカスタマイズをリセットします。
 - a vCenter Server で、[ホーム] - [ポリシーおよびプロファイル] - [ホスト プロファイル] の順にクリックし、ホストに添付されているプロファイルをクリックします。
 - b [設定タブ] - [ホストから設定をコピー] の順にクリックし、ホストを選択します。
 - c カスタマイズをリセットするには、vCenter Server ブラウザでホストに移動し、右クリック メニューから [ホスト プロファイル] - [ホストのカスタマイズのリセット] の順に選択します。
- 4 ホストの右クリック メニューから [ホスト プロファイル] - [修正] の順に選択します。
ホストが準拠になります。
- 5 ホストを再起動し、メンテナンス モードを終了します。
- 6 ホストが依然として準拠していない場合は、[手順 4](#) を繰り返します。

例：ストレージ構成を保持せずに ESXi ホストをアップグレードする

ホスト プロファイルでキャプチャされたストレージ構成を保持する必要がない場合は、ホストをアップグレードした後に、ホスト上で一部のコンプライアンス エラーが発生する可能性があります。この場合、ホストから設定をコピーし、ホストのカスタマイズをリセットします。[手順 3](#) を参照してください。

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。

ローカル デバイスのタイプによっては、名前を変更できないことがあります。

手順

- 1 ホストに移動します。

- 2 [設定] 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 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] の順に選択します。
- 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 ホストに移動します。
- 2 [設定] 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 ホストに移動します。
- 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] 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 デバイスやパ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、デバイスへのパ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、そのすべてのパ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 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。

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
```

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クラッチ パーティションは含まれていません。

手順

- 1 ホストに移動します。
- 2 [設定] 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 ホストに移動します。
- 2 [設定] 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 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。
- すべてのパスの表示が 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 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。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 ホストに移動します。
- 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] 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 (All Path Down) 処理を無効にした場合でも、デバイスが APD 状態になったときに処理を再度有効にして、値を 1 に設定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 ホストに移動します。
- 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] 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。

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。ESXCLI 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 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。

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 ホストに移動します。

- 2 [設定] 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	[LED をオンにする] アイコンをクリックします。
無効化	[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 ホストに移動します。
- 2 [設定] 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 つまたは複数のデバイスを選択し、[パーティションの消去] アイコンをクリックします。
- 5 消去してい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。

駆動パーツを含む磁気デバイスである通常の HDD とは異なり、フラッシュ デバイスはストレージ媒体として半導体を使用し、駆動パーツがありません。通常、フラッシュ デバイスは回復力が高く、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。

NVMe ストレージを使用する場合は、ストレージ パフォーマンスを向上するために、高性能プラグイン (HPP) を有効にします。 [VMware High Performance プラグインとパス選択スキーム](#) を参照してください。

ESXi での NVMe ストレージの使用方法の詳細については、 [16 章 VMware NVMe ストレージについて](#) を参照してください。

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 デバイス上で VMFS データストアを作成します。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。 VMFS データストアによるホスト 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)	ベンダーから要求される場合は、仮想フラッシュ リソースを設定し、I/O キャッシュ フィルタに使用します。 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。

この章には、次のトピックが含まれています。

- [フラッシュ仮想ディスクの特定](#)
- [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](#)
- [VMFS データストアによるホスト キャッシュの構成](#)
- [フラッシュ ディスクで VMFS を使用しないようにする](#)

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、仮想ハードウェア バージョン 8 以降の仮想マシンでサポートされます。
- 共有 VMFS データストアをバックアップしているデバイスは、すべてのホストでフラッシュのマークを付ける必要があります。
- VMFS データストアに複数のデバイス エクステンションが含まれている場合は、基盤となるすべての物理エクステンションがフラッシュベースである必要があります。

ストレージ デバイスのマーク

適切に検出されていないストレージ デバイスを、ローカル フラッシュ デバイスとしてマークすることができます。

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、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 ホストに移動します。
- 2 [設定] 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、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 ホストに移動します。
- 2 [設定] 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 個または複数個のリモート デバイスを選択して、[ローカルとしてマーク] アイコンをクリックします。
- 5 [はい] をクリックして変更を保存します。

フラッシュ デバイスの監視

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。

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。ESXCLI 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 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。

- VMware 互換性ガイドで承認されているフラッシュ デバイスを使用してください。
- 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](#)を参照してください。
- NVMe デバイスをストレージに使用する場合は、ストレージ パフォーマンスを向上するために、高性能プラグイン (HPP) を有効にします。NVMe デバイスの使用方法の詳細については、[VMware High Performance プラグインとパス選択スキーム](#)を参照してください。

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.xxxxxxxxxxxxxx
Device: t10.xxxxxxxxxxxxxx
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。

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

たとえば、ベンダーが 1 日あたり 20 GB の書き込みが行われる条件下で 5 年間の耐用年数を保証している場合、1 日あたりの実際の書き込み平均数が 30 GB であれば、フラッシュ デバイスの耐用年数はおよそ 3.3 年になります。

仮想フラッシュ リソースについて

ESXi ホスト上のローカル フラッシュ デバイスは、仮想フラッシュ リソースと呼ばれる 1 つの仮想化キャッシュレイヤーに集約することができます。

仮想フラッシュ リソースの設定時には、新しいファイル システムとして仮想フラッシュ ファイル システム (VFFS) を作成します。VFFS は VMFS からの派生システムで、フラッシュ デバイス用に最適化されており、物理フラッシュ デバイスを 1 つのキャッシュ リソース プールにグループ化するために使用されます。読み取り専用リソースであるため、仮想マシンの保存先として使用することはできません。

仮想フラッシュ リソースを設定したら、I/O キャッシュ フィルタに使用できます。[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。

仮想フラッシュ リソースの考慮事項

仮想フラッシュ リソースを設定する場合は、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、1 台の ESXi ホストに 1 つのみ配置できます。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、ホストまたはホスト クラスタ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の必要があります。仮想フラッシュ リソースを vSAN や VMFS などの他の vSphere 機能と共有することはできません。

手順

- 1 vSphere Client で、ホストに移動します。
- 2 [設定] タブをクリックします。
- 3 [ストレージ] で [仮想フラッシュリソース管理] をクリックします。
- 4 以下のいずれかのオプションをクリックします。

オプション	説明
キャパシティを追加	個々のホストに仮想フラッシュ リソースを作成する場合。
クラスタに容量を追加	クラスタ上に仮想フラッシュ リソースを作成する場合。

- 5 使用可能なエンティティのリストから、仮想フラッシュ リソースで使用するエンティティを 1 つ以上選択し、[OK] をクリックします。

フラッシュ デバイスがリストに表示されない場合は、[ストレージ デバイスのマーク](#)を参照してください。

オプション	説明
ローカル VMware ディスク	未要求のフラッシュ デバイスの任意の組み合わせを選択します。 ESXi は、いずれかのデバイスに VFFS ボリュームを作成してから、残りのデバイスのボリュームを拡張します。システムにより、VFFS ボリューム全体の仮想フラッシュ リソースが設定されます。 ホストに VFFS ボリュームがある場合は、既存の VFFS ボリュームを先に選択しないと、どの未要求デバイスも選択できません。
volume ID - 既存の VFFS ボリュームのエクステンションを使用して設定します	以前に vmkfstools コマンドを使用して、ホストのフラッシュ デバイス上に VFFS ボリュームを作成したことがある場合は、そのボリュームも適切なエンティティのリストに表示されます。仮想フラッシュ リソースにはこのボリュームのみを選択できます。または、これを未要求デバイスと組み合わせます。ESXi は、既存の VFFS ボリュームを使用して、他のデバイスに拡張します。

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

I/O フィルタリング用の vSphere API を介して開発された、I/O キャッシュ フィルタ用の仮想フラッシュ リソースを使用します。

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 I/O フィルタに使用されていないことを確認します。

手順

- 1 ホストまたはクラスタに移動します。
- 2 [設定] タブをクリックします。
- 3 [ストレージ] で [仮想フラッシュ リソース管理] をクリックし、[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 ホストに移動します。
- 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 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.ResourceUsageThreshold]	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。

- 5 [OK] をクリックします。

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を変更することもできます。

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。

前提条件

フラッシュ デバイスをバックアップとして使用して 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 ホストに移動します。
- 2 [設定] 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 リストからフラッシュ データストアを選択し、[編集] アイコンをクリックします。
- 5 ホスト キャッシュに適切に容量を割り当てます。
- 6 [OK] をクリックします。

フラッシュ ディスクで VMFS を使用しないようにする

ESXi のインストールまたは自動デプロイ時に自動パーティショニング起動オプションを使用すると、ホストのローカル ストレージに VMFS データストアが作成されます。場合によっては、ローカル ストレージのフラッシュ ディスクがフォーマットされないようにする必要があります。

問題

デフォルトで、自動パーティショニングを行うと、フラッシュ ディスクを含む、ホスト上のすべての未使用ローカル ストレージ ディスクに VMFS ファイル システムがデプロイされます。

ただし、VMFS でフォーマットされたフラッシュ ディスクは仮想フラッシュや vSAN などの機能で使用できなくなります。両方の機能にはフォーマットされていないフラッシュ ディスクが必要であり、いずれの機能も他のファイル システムとディスクを共有できません。

解決方法

自動パーティショニングで VMFS によってフラッシュ ディスクがフォーマットされないようにするには、ESXi をインストールするときに、または ESXi を初めて起動するときに、次の起動オプションを使用します。

- **autoPartition=TRUE**
- **skipPartitioningSsds=TRUE**

Auto Deploy を使用する場合、これらのパラメータをリファレンス ホストに設定します。

- 1 リファレンス ホストとして使用するホストに移動し、[設定] タブをクリックします。
- 2 [システム] をクリックしてシステム オプションを開き、[システムの詳細設定] をクリックします。
- 3 次の項目を設定します。

パラメータ	値
VMkernel.Boot.autoPartition	True
VMkernel.Boot.skipPartitioningSsds	True

- 4 ホストを再起動します。

仮想フラッシュ リソースと vSAN とともに使用する予定のフラッシュ ディスクに VMFS データストアがすでにある場合は、そのデータストアを削除します。

永続的なメモリを使用する不揮発性メモリ (NVM) ストレージ デバイスは、データセンターでは次第に一般的になっています。NVM Express (NVMe) は、NVM デバイスとの高パフォーマンスのマルチキュー通信専用に設計された標準化プロトコルです。ESXi は、ローカルおよびネットワーク ストレージ デバイスに接続する NVMe プロトコル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。

- [VMware NVMe の概念](#)
- [VMware NVMe ストレージの要件および制限事項](#)
- [NVMe over RDMA \(RoCE v2\) ストレージ用のアダプタの構成](#)
- [NVMe over RDMA \(RoCE v2\) または FC-NVMe アダプタ用のコントローラの追加](#)
- [ソフトウェア NVMe over RDMA アダプタの削除](#)

VMware NVMe の概念

ESXi 環境で NVMe ストレージの使用を開始する前に、NVMe の基本的な概念について理解しておく必要があります。

NVM Express (NVMe)

NVMe は、ホストとターゲット ストレージ システム間で接続およびデータ転送するための方法です。NVMe は、フラッシュ デバイスなどの不揮発性メモリを備えた高速ストレージ メディアで使用するよう設計されています。このタイプのストレージは、低遅延、少ない CPU 使用率、高パフォーマンスを実現し、通常は SCSI ストレージの代替手段として機能します。

NVMe の転送

NVMe ストレージは、PCIe インターフェイスを使用してホストに直接接続することも、異なるファブリック転送を使用して間接的に接続することもできます。VMware NVMe over Fabrics (NVMe-oF) では、ホストと共有ストレージ アレイ上のターゲット ストレージ デバイス間の遠距離接続が可能になります。

NVMe の転送については現在、次のタイプがあります。詳細については、『[VMware NVMe ストレージの要件および制限事項](#)』を参照してください。

NVMe の転送	ESXi のサポート対象
NVMe over PCIe	ローカル ストレージ。
NVMe over RDMA	共有 NVMe-oF ストレージ。RoCE v2 テクノロジーを使用します。
NVMe over Fibre Channel (FC-NVMe)	共有 NVMe-oF ストレージ。

NVMe 名前空間

NVMe ストレージ アレイでは、名前空間は、一定量の不揮発性メモリによってバックアップされるストレージ ボリュームです。ESXi のコンテキストでは、名前空間はストレージ デバイスまたは LUN の類義語です。ESXi ホストが NVMe 名前空間を検出すると、その名前空間を表すフラッシュ デバイスが vSphere Client のストレージ デバイスのリストに表示されます。そのデバイスを使用して VMFS データストアを作成し、仮想マシンを格納できます。

NVMe コントローラ

コントローラは、1 つまたは複数の NVMe 名前空間に関連付けられ、ESXi ホストとストレージ アレイ内の名前空間との間のアクセス パスを提供します。コントローラにアクセスするため、ホストはコントローラ検出とコントローラ接続の 2 つのメカニズムを使用します。詳細については、『[NVMe over RDMA \(RoCE v2\) または FC-NVMe アダプタ用のコントローラの追加](#)』を参照してください。

コントローラ検出

このメカニズムを使用すると、ESXi ホストは最初に検出コントローラに接続します。検出コントローラは、使用可能なコントローラのリストを返します。ホストがアクセスするコントローラを選択すると、このコントローラに関連付けられたすべての名前空間がホストで使用できるようになります。

コントローラ接続

ESXi ホストは、指定したコントローラに接続します。このコントローラに関連付けられたすべての名前空間がホストで使用できるようになります。

NVMe サブシステム

通常、NVMe サブシステムは、複数の NVMe コントローラ、複数の名前空間、不揮発性メモリ ストレージ媒体、およびコントローラと不揮発性メモリ ストレージ媒体間のインターフェイスを含むストレージ アレイです。このサブシステムは、サブシステムの NVMe 修飾名 (NQN) で識別されます。

VMware High-Performance Plug-in (HPP)

デフォルトでは、ESXi ホストは HPP を使用して、NVMe-oF ターゲットを要求します。I/O 要求の物理パスを選択する際、HPP は適切なパス選択スキーム (PSS) を適用します。HPP の詳細については、『[VMware High Performance プラグインとパス選択スキーム](#)』を参照してください。デフォルトのパス選択メカニズムを変更するには、『[パス選択ポリシーの変更](#)』を参照してください。

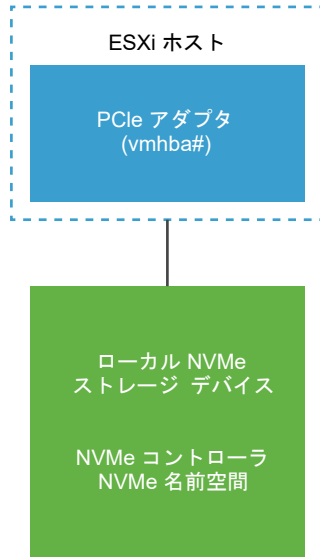
基本的な VMware NVMe のアーキテクチャおよびコンポーネント

ESXi は、NVMe over PCIe のローカル ストレージと、NVMe-oF の共有ストレージ (NVMe over Fibre Channel、NVMe over RDMA (RoCE v2) など) をサポートします。

NVMe-oF 環境では、ターゲットは SCSI の LUN に相当する名前空間を、アクティブ/アクティブまたは非対称アクセス モードのホストに提示できます。どちらの場合でも、ESXi は提示された名前空間を検出し、使用できます。ESXi は、NVMe-oF ターゲットを SCSI ターゲットとして内部でエミュレートし、アクティブ/アクティブの SCSI ターゲットまたは暗黙的な ALUA SCSI ターゲットとして提示します。

VMware NVMe over PCIe

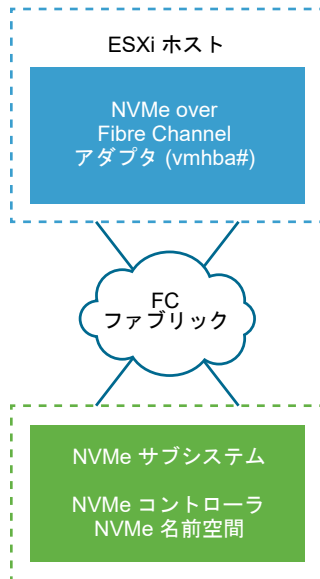
この設定では、ESXi ホストは PCIe ストレージ アダプタを使用して、1 台以上のローカルの NVMe ストレージ デバイスにアクセスします。ホストにアダプタをインストールすると、ホストは使用可能な NVMe デバイスを検出し、検出されたデバイスは vSphere Client のストレージ デバイス リストに表示されます。



VMware NVMe over FC

このテクノロジーは、NVMe をファイバ チャンネル プロトコルにマッピングして、ホスト コンピュータとターゲット ストレージ デバイス間でのデータおよびコマンドの転送を実現します。この転送では、NVMe をサポートするためにアップグレードされた既存のファイバ チャンネル インフラストラクチャを使用できます。

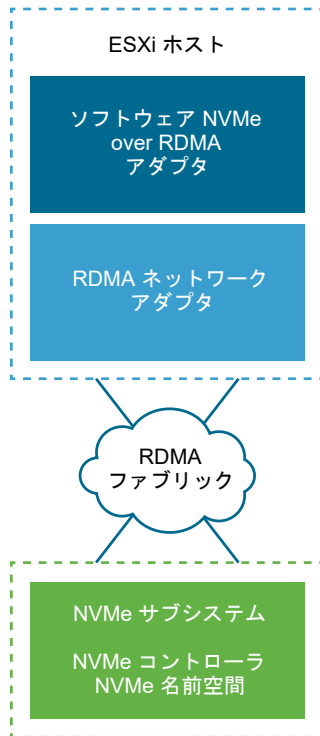
NVMe over Fibre Channel ストレージにアクセスするには、NVMe をサポートするファイバ チャンネル ストレージ アダプタを ESXi ホストにインストールします。アダプタの設定は必要ありません。アダプタは、適切な NVMe サブシステムに自動的に接続し、到達可能なすべての共有 NVMe ストレージ デバイスを検出します。後でアダプタを再設定し、コントローラの切断や、ホストの起動時には使用できなかった他のコントローラの接続を行うことができます。詳細については、『[NVMe over RDMA \(RoCE v2\) または FC-NVMe アダプタ用のコントローラの追加](#)』を参照してください。



NVMe over RDMA (RoCE v2)

このテクノロジーは、ネットワーク上の 2 台のシステム間でリモート ダイレクト メモリ アクセス (RDMA) 転送を使用します。この転送は、オペレーティング システムやいずれかのシステムのプロセッサを経由せずに、メイン メモリでのデータ交換を実現します。ESXi は、イーサネット ネットワークを介したリモート ダイレクト メモリ アクセスを実現する、RDMA over Converged Ethernet v2 (RoCE v2) テクノロジーをサポートします。

ストレージにアクセスするため、ESXi ホストは、ホストにインストールされている RDMA ネットワーク アダプタと、ソフトウェア NVMe over RDMA ストレージ アダプタを使用します。ストレージ検出のため、これらの両方のアダプタを設定する必要があります。詳細については、『[NVMe over RDMA \(RoCE v2\) ストレージ用のアダプタの構成](#)』を参照してください。



VMware NVMe ストレージの要件および制限事項

NVMe テクノロジーを VMware で使用する場合は、特定のガイドラインと要件に沿う必要があります。

NVMe over PCIe の要件

使用する ESXi ストレージ環境が次のコンポーネントを備えていることが必要です。

- ローカルの NVMe ストレージ デバイス。
- 互換性のある ESXi ホスト。
- ハードウェア NVMe over PCIe アダプタ。アダプタをインストールすると、ESXi ホストがそのアダプタを検出し、PCIe と示されたプロトコルを使用するストレージ アダプタ (vmhba) として vSphere Client に表示されます。アダプタの設定は必要ありません。

NVMe over RDMA (RoCE v2) の要件

- NVMe over RDMA (RoCE v2) 転送のサポートを備えた NVMe ストレージ アレイ。
- 互換性のある ESXi ホスト。
- ロスレス ネットワークをサポートするイーサネット スイッチ。
- RDMA over Converged Ethernet (RoCE v2) をサポートするネットワーク アダプタ。アダプタを設定する方法については、[RDMA ネットワーク アダプタの構成](#)を参照してください。

- ソフトウェア NVMe over RDMA アダプタ。このソフトウェア コンポーネントは、ESXi ホストで有効にされていること、および適切なネットワーク RDMA アダプタに接続されていることが必要です。詳細については、『[ソフトウェア NVMe over RDMA アダプタの有効化](#)』を参照してください。
- NVMe コントローラ。ソフトウェア NVMe over RDMA アダプタを設定した後でコントローラを追加する必要があります。[NVMe over RDMA \(RoCE v2\) または FC-NVMe アダプタ用のコントローラの追加](#)を参照してください。

NVMe over Fibre Channel の要件

- NVMe をサポートするファイバ チャンネル ストレージ アレイ。詳細については、『[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。
- 互換性のある ESXi ホスト。
- ハードウェア NVMe アダプタ。通常は、NVMe をサポートするファイバ チャンネル HBA です。アダプタをインストールすると、ESXi ホストがそのアダプタを検出し、NVMe と示されたストレージ プロトコルを使用するファイバ チャンネル アダプタ (vmhba) として vSphere Client に表示されます。ハードウェア NVMe アダプタを使用するために、このアダプタを設定する必要はありません。
- NVMe コントローラ。コントローラの設定は必要ありません。必要なハードウェア NVMe アダプタをインストールすると、その時点で到達可能なすべてのターゲットおよびコントローラに自動的に接続します。後で、コントローラの切断や、ホストの起動時には使用できなかった他のコントローラの接続を行うことができます。[NVMe over RDMA \(RoCE v2\) または FC-NVMe アダプタ用のコントローラの追加](#)を参照してください。

VMware NVMe over Fabrics 共有ストレージのサポート

ESXi 環境では、NVMe ストレージ デバイスは SCSI ストレージ デバイスと同じように表示され、共有ストレージとして使用できます。NVMe-oF ストレージを使用する場合は、次のルールを守ってください。

- 異なる転送タイプを使用して、同じ名前空間にアクセスしない。
- アクティブなパスがホストに提示されていることを確認する。アクティブなパスが検出されるまで、名前空間は登録できません。

共有ストレージの機能	SCSI over Fabric ストレージ	NVMe over Fabric ストレージ
RDM	サポート	サポート対象外
コア ダンプ	サポート	サポート対象外
SCSI-2 予約	サポート	サポート対象外
共有 VMDK	サポート	サポート対象外
vVols	サポート	サポート対象外
VAAI プラグインによるハードウェア アクセラレーション	サポート	サポート対象外
デフォルトの MPP	NMP	HPP (NVMe-oF ターゲットは NMP は要求できない)
制限	LUN = 1024、パス = 4096	名前空間 = 32、パス = 128 (ホスト内の名前空間あたり最大 4 つのパス)

NVMe over RDMA (RoCE v2) ストレージ用のアダプタの構成

アダプタ構成プロセスでは、RDMA ネットワーク アダプタの VMkernel バインドを設定し、その後、ソフトウェア NVMe over RDMA アダプタを有効にします。

次のビデオでは、RDMA アダプタを介して NVMe を設定する手順について説明します。



VSphere 7.0 での RDMA アダプタを介した NVMe の設定
(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_nvme_rdma)

手順

1 RDMA ネットワーク アダプタの構成

ソフトウェア NVMe over RDMA アダプタを作成する前に、RDMA ネットワーク アダプタをインストールし、その VMkernel バインドを設定します。

2 ソフトウェア NVMe over RDMA アダプタの有効化

ESXi は、ソフトウェア NVMe over RDMA アダプタをサポートしています。ソフトウェア NVMe over RDMA ストレージ アダプタを有効にするには、vSphere Client を使用します。

次のステップ

ソフトウェア NVMe over RDMA アダプタを有効にしたら、NVMe コントローラを追加して、ホストが NVMe ターゲットを検出できるようにします。[NVMe over RDMA \(RoCE v2\) または FC-NVMe アダプタ用のコントローラの追加](#)を参照してください。

RDMA ネットワーク アダプタの構成

ソフトウェア NVMe over RDMA アダプタを作成する前に、RDMA ネットワーク アダプタをインストールし、その VMkernel バインドを設定します。

手順

1 ESXi ホストで、RDMA (RoCE v2) をサポートするアダプタ (Mellanox Technologies MT27700 Family ConnectX-4 など) をインストールします。

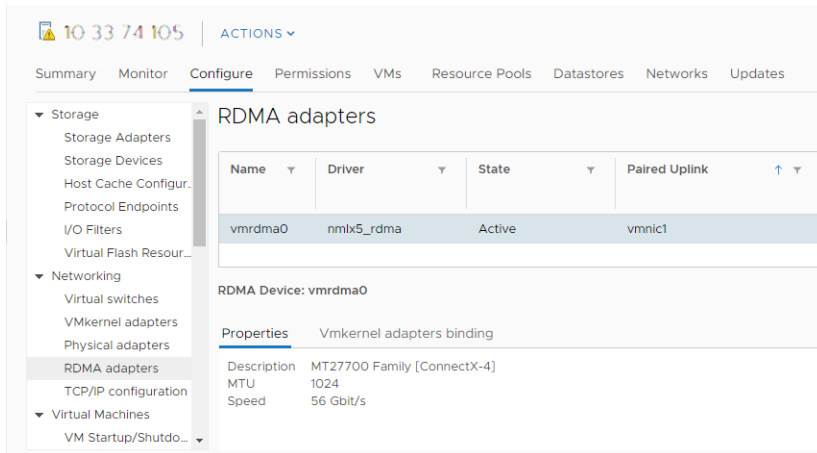
ホストはアダプタを検出し、vSphere Client は 2 つのコンポーネント (RDMA アダプタと物理ネットワーク アダプタ) を表示します。

2 vSphere Client で、RDMA アダプタがホストによって検出されていることを確認します。

- a ホストに移動します。
- b [設定] タブをクリックします。

- c [ネットワーク] で、[RDMA アダプタ] をクリックします。

この例では、RDMA アダプタは `vmrdma0` としてリストに表示されます。[ペアリングされたアップリンク] 列には、ネットワーク コンポーネントが `vmnic1` 物理ネットワーク アダプタとして表示されます。



- d アダプタの説明を確認するには、リストから RDMA アダプタを選択し、[プロパティ] タブをクリックします。

3 RDMA アダプタの VMkernel バインドを構成します。

構成では、vSphere 標準スイッチまたは vSphere Distributed Switch を使用できます。次の手順では、標準スイッチを例として使用します。

- a vSphere 標準スイッチを作成し、ネットワーク コンポーネントをスイッチに追加します。

注： RDMA アダプタに対応する物理ネットワーク アダプタを選択してください。この例では `vmnic1` アダプタです。

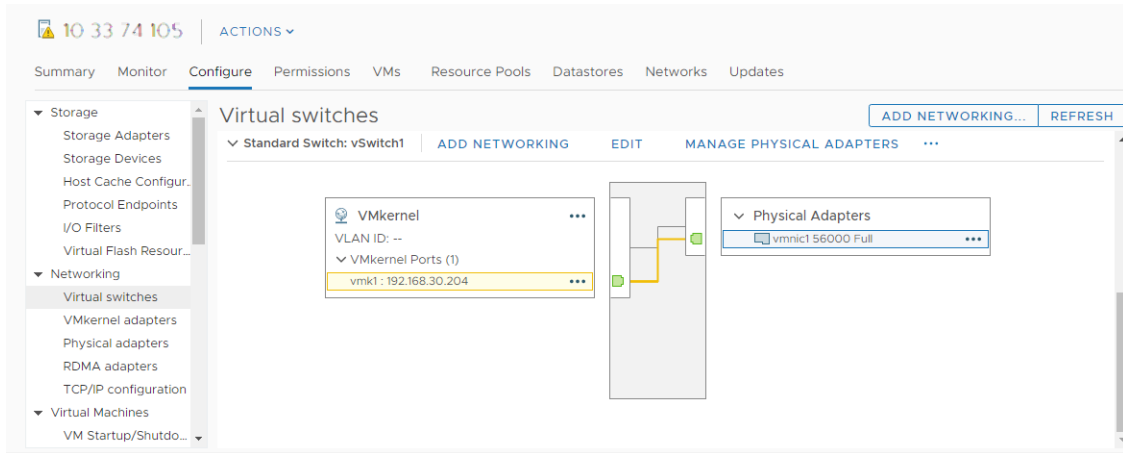
スイッチの作成に関する詳細については、『vSphere のネットワーク』ドキュメントの「vSphere 標準スイッチの作成」または「vSphere Distributed Switch の作成」を参照してください。

- b 作成した vSphere 標準スイッチに VMkernel アダプタを追加します。

VMkernel アダプタに適切な固定 IPv4 または IPv6 アドレスを割り当てて、RDMA アダプタが NVMe over RDMA を検出できるようにします。

VMkernel アダプタの追加の詳細については、『vSphere のネットワーク』ドキュメントの「VMkernel ネットワークの設定」を参照してください。

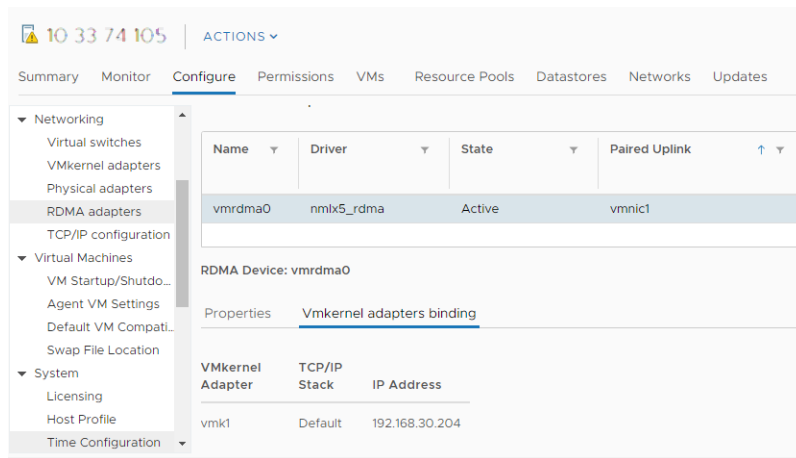
次の図は、物理ネットワーク アダプタと VMkernel アダプタが vSphere 標準スイッチに接続されていることを示しています。この接続を介して、RDMA アダプタが VMkernel アダプタにバインドされます。



4 RDMA アダプタの VMkernel バインド設定を確認します。

- a RDMA アダプタに移動します。
- b [VMkernel アダプタのバインド] タブをクリックして、関連する VMkernel アダプタがページに表示されることを確認します。

この例では、vmrmda0RDMA アダプタは vmnic1 ネットワーク アダプタとペアになっており、vmk1 VMkernel アダプタに接続されています。



次のステップ

これで、ソフトウェア NVMe over RDMA アダプタを作成できるようになりました。

ソフトウェア NVMe over RDMA アダプタの有効化

ESXi は、ソフトウェア NVMe over RDMA アダプタをサポートしています。ソフトウェア NVMe over RDMA ストレージ アダプタを有効にするには、vSphere Client を使用します。

前提条件

ESXi ホストで、RDMA (RoCE v2) をサポートするアダプタ (Mellanox Technologies MT27700 Family ConnectX-4 など) をインストールします。RDMA アダプタの VMkernel バインドを構成します。詳細については、『[RDMA ネットワーク アダプタの構成](#)』を参照してください。

手順

- 1 ホストに移動します。
- 2 [設定] 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]、[ソフトウェア アダプタの追加] アイコンの順にクリックします。
- 4 [RDMA アダプタを介したソフトウェア NVMe の追加] を選択し、適切な RDMA アダプタ (vmrdma) をドロップダウン メニューから選択します。

注： ソフトウェア NVMe over RDMA アダプタを作成できないことを示すエラー メッセージが表示される場合は、RDMA アダプタの VMkernel バインドが正しく構成されていることを確認します。詳細については、[『RDMA ネットワーク アダプタの構成』](#) を参照してください。

結果

ソフトウェア NVMe over RDMA アダプタが vmhba ストレージ アダプタとしてリストに表示されます。他の目的で、基盤となる RDMA ネットワーク アダプタを解放する必要がある場合は、アダプタを削除できます。

NVMe over RDMA (RoCE v2) または FC-NVMe アダプタ用のコントローラの追加

NVMe コントローラを追加するには、vSphere Client を使用します。コントローラを追加すると、コントローラに関連付けられている NVMe 名前空間を ESXi ホストで使用できるようになります。ESXi 環境内の名前空間を表す NVMe ストレージ デバイスが、ストレージ デバイス リストに表示されます。

NVMe over RDMA (RoCE v2) ストレージを使用する場合は、ソフトウェア NVMe over RDMA アダプタを設定した後でコントローラを追加する必要があります。FC-NVMe ストレージを使用すると、必要なアダプタをインストールした後、その時点で到達可能なすべてのターゲットへの接続が自動的に行われます。後でアダプタを再設定し、コントローラの切断や、ホストの起動時には使用できなかった他のコントローラの接続を行うことができます。

前提条件

使用しているストレージのタイプに適したアダプタが ESXi ホストにあることを確認してください。[VMware NVMe ストレージの要件および制限事項](#)を参照してください。

手順

- 1 ホストに移動します。
- 2 [設定] 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 [コントローラ] タブをクリックして、[コントローラの追加] をクリックします。

- 5 コントローラを追加するには、次のいずれかのオプションを選択し、[追加] をクリックします。

オプション	説明
コントローラを自動的に検出	この方法は、使用可能なすべてのコントローラへの接続をホストが許容できることを示します。 <ol style="list-style-type: none"> 検出コントローラについて、次のパラメータを指定します。 <ul style="list-style-type: none"> ■ NVMe over RDMA (RoCE v2) の場合は、IP アドレスと転送ポート番号。 ■ FC-NVMe の場合は、WorldWideNodeName および WorldWidePortName。 [コントローラの検出] をクリックします。 コントローラのリストから、使用するコントローラを選択します。
手動でのコントローラの詳細の入力	この方法を使用すると、ホストは次のパラメータを使用して、特定のコントローラへの接続を要求します。 <ul style="list-style-type: none"> ■ サブシステム NQN ■ コントローラの ID。NVMe over RDMA (RoCE v2) の場合は、IP アドレスと転送ポート番号。FC-NVMe の場合は、WorldWideNodeName および WorldWidePortName。 ■ 管理キューのサイズ。コントローラの管理キューのサイズを指定するオプションのパラメータ。デフォルト値は 16 です。 ■ キープアライブ タイムアウト。アダプタとコントローラ間のキープアライブ タイムアウト値を秒単位で指定するオプションのパラメータ。デフォルトのタイムアウト値は 60 秒です。

結果

コントローラがコントローラのリストに表示されます。これでホストは、コントローラに関連付けられている NVMe 名前空間を検出できるようになります。ESXi 環境内の名前空間を表す NVMe ストレージ デバイスが、vSphere Client のストレージ デバイス リストに表示されます。

ソフトウェア NVMe over RDMA アダプタの削除

ソフトウェア NVMe over RDMA アダプタを削除するには、vSphere Client を使用します。他の目的で、基盤となる RDMA ネットワーク アダプタを解放する必要がある場合は、アダプタを削除できます。

NVMe over PCIe アダプタと FC-NVMe アダプタは削除できません。

手順

- 1 ホストに移動します。
- 2 [設定] 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、削除するアダプタ (vmhba#) を選択します。
- 4 アダプタに接続されている NVMe コントローラを削除します。
 - a [コントローラ] タブをクリックします。
 - b コントローラを選択し、[削除] をクリックします。

NVMe コントローラが切断され、リストに表示されなくなります。

- 5 [削除] アイコン (ホストのストレージ アダプタを削除) をクリックして、NVMe over RDMA アダプタを削除します。

データストアでの作業

17

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](#)
- [VMFS データストアのアップグレード](#)
- [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 キャパシティの増加](#)
- [VMFS6 データストア上のクラスタ化された仮想ディスクのサポートの有効化または無効化](#)
- [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](#)
- [VMFS データストアでの 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 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 接続経由で、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。
vVol	vVols データストアは、vCenter Server および vSphere Client 内のストレージ コンテナを表します。 22 章 VMware vSphere Virtual Volumes (vVol) の操作 を参照してください。

ストレージ タイプに応じて、次のタスクの一部がデータストアで使用可能です。

- データストアの作成。vSphere 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。
- データストアでの管理操作の実行。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。
- データストアの整理。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 クラスタへのデータストアの追加。データストア クラスタは、リソースと管理インターフェイスが共有されたデータストアの集まりです。データストア クラスタを作成すると、Storage DRS を使用してストレージ リソースを管理できます。データストア クラスタの詳細については、『vSphere 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 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。現在、ESXi は VMFS5 および VMFS6 をサポートしています。

サポートされているすべての 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。サポートされている VMFS データストアで、仮想マシンを作成し、パワーオンすることができます。

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

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
バージョン 6.5 以降の ESXi 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	なし
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	はい	可 (デフォルト)
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)
4Kn ストレージ デバイス	なし	はい
容量の自動再利用	なし	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
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。	なし
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

表 17-3. VMFS5 と VMFS6 の比較 (続き)

機能	VMFS5	VMFS 6
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

VMFS 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。

- 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、512e、または 4Kn 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、vVols 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。
- Storage 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同種のストレージ デバイス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。
- デバイス パーティションのフォーマット。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。

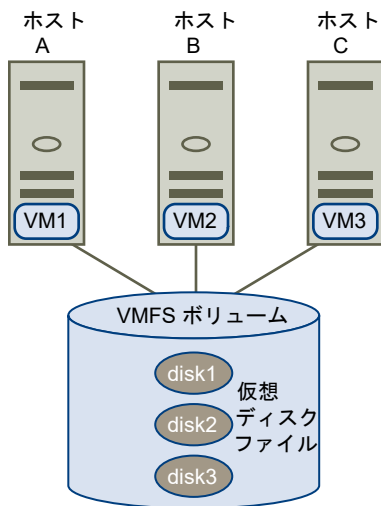
複数の仮想マシンを実行するときは、VMFS が仮想マシン ファイルの特定のロック メカニズムを提供します。その結果、仮想マシンは、複数の ESXi ホストが同じ VMFS データストアを共有する SAN 環境で安全に動作できます。

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。

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。

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。ESXCLI 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 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	ATS-only	データストアのロック構成を示します。 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。

表 17-4. VMFS ロック情報 (続き)

フィールド	値	説明
	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ト VMFS5 データストアで使用できます。ホストのいずれかでオンライン アップグレードを実行する間、その他のホストはそのデータストアを使用し続けることができます。
- ATS のみへのオフライン アップグレードは、複数の物理エクステントをまたぐ VMFS5 データストアで使用する必要があります。複数のエクステントで構成されるデータストアは、オンライン アップグレードでは使用できません。これらのデータストアでは、アップグレードの要求時に、どのホストもデータストアをアクティブに使用しないようにする必要があります。

手順

1 ATS のみ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。

複数のエクステンツをまたぐことのないほとんどのデータストアは、オンライン アップグレードで使用可能です。ESXi ホストのいずれかでオンライン アップグレードを実行する間、その他のホストはデータストアを使用し続けることができます。オンライン アップグレードは、すべてのホストでデータストアを閉じた後にのみ完了します。

前提条件

データストアをメンテナンス モードにすることによってロック メカニズムのアップグレードを完了する予定の場合は、Storage DRS を無効にします。前提条件は、オンライン アップグレードにのみ適用されます。

手順

- 1 次のコマンドを実行することにより、ロック メカニズムのアップグレードを実行します。

```
esxcli storage vmfs lockmode set -a|--ats -l|--volume-label= VMFS label -u|--volume-uuid= VMFS UUID.
```

2 オンライン アップグレードの場合は、追加の手順を実行します。

- a データストアにアクセス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。

スナップショットのフォーマット	VMFS5	VMFS 6
VMFSsparse	2 TB より小さい仮想ディスク。	該当なし
SEsparse	2 TB より大きい仮想ディスク。	すべてのディスク。

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ズ 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。

VMFS データストアのアップグレード

ESXi では、VMFS5 と VMFS3 のアップグレードで、異なるアプローチを使用します。

VMFS5 データストア

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。環境内に VMFS5 データストアがある場合、VMFS6 データストアを作成し、VMFS5 データストアから仮想マシンを VMFS6 に移行します。

VMFS3 データストア

ESXi では、VMFS3 データストアはサポートされなくなりました。ESXi ホストは、既存のデータストアをマウントするときに自動的に VMFS3 を VMFS5 にアップグレードします。ホストは、次の状況でアップグレード操作を実行します。

- ESXi7.0 以降へのアップデート後の最初の起動で、検出されたすべての VMFS3 データストアをホストがマウントするとき。
- 起動後に検出された VMFS3 データストアを手動でマウントするとき。または、アンマウントされたデータストアを永続的にマウントするとき。

ネットワーク ファイル システム データストアについて

ESXi に組み込まれた NFS クライアントは、TCP/IP 接続で NFS (Network File System) プロトコルを使用して、NAS サーバ上に存在する指定された NFS ボリュームにアクセスします。ESXi ホストは、そのボリュームをマウントし、ストレージとして使用することができます。vSphere では、NFS プロトコルのバージョン 3 および 4.1 をサポートしています。

通常、NFS ボリュームまたはディレクトリは、ストレージ管理者によって作成され、NFS サーバからエクスポートされます。VMFS などのローカル ファイル システムで NFS ボ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、ボリュームを ESXi ホストに直接マウントし、VMFS データストアを使用する場合と同じ方法で仮想マシンを保存および起動します。

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

特性	NFS バージョン 3	NFS バージョン 4.1
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 向けサポート
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

次の表は、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たものです。

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
Fault Tolerance (FT)	○	○
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	なし
Storage I/O Control	はい	なし
Site Recovery Manager	はい	X
vVols	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 メカニズムをサポートします。

NFS v4.1 上の仮想マシンは、以前のレガシー 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、異なる要件や特性に合わせて、さまざまなテクノロジーを Fault Tolerance に使用していました。

NFS アップグレード

6.5 よりも前のバージョンの ESXi をアップグレードすると、既存の NFS 4.1 データストアは、ESXi の以前のリリースでは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、vVols、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。2 つの NFS バージョンのロック メカニズムには互換性がありません。NFS 3 は独自のロックを使用し、NFS 4.1 はネイティブ プロトコルで指定されたロックを使用します。

■ 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 のマルチパス

NFS 4.1 は、プロトコルの仕様に従ってマルチパスをサポートします。NFS 3 ではマルチパスは適用できません。

■ 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 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。2 つの NFS バージョンのロック メカニズムには互換性がありません。NFS 3 は独自のロックを使用し、NFS 4.1 はネイティブ プロトコルで指定されたロックを使用します。

ESXi の NFS 3 ロックでは、ネットワーク ロック マネージャ (NLM) プロトコルを使用しません。代わりに VMware は、独自のロック プロトコルを使用できるようにしています。NFS 3 ロックは、NFS サーバでロック ファイルを作成することによって実装されます。ロック ファイルには、`.lck-file_id` という名前が付けられます。

NFS 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 4.1 は、プロトコルの仕様に従ってマルチパスをサポートします。NFS 3 ではマルチパスは適用できません。

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 ポリウ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 ポリウムを 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 ホストに移動します。

- 2 [設定] タブをクリックします。
- 3 [システム] の下で、[ファイアウォール] をクリックして [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 を使用する場合は、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 が有効であることを確認します。

次の表は、ESXi がサポートする Kerberos セキュリティ レベルの比較です。

表 17-5. Kerberos セキュリティのタイプ

		ESXi 6.0	ESXi 6.5 以降
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 データの整合性チェックサム	いいえ	いいえ
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 データの整合性チェックサム		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、ESXi ホスト、NFS サーバ、および Active Domain サーバの時刻を同期する必要があります。通常は、設定で Network Time Protocol (NTP) サーバとして Active Domain サーバが使用されます。

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 ホストに移動します。
- 2 [設定] タブをクリックします。
- 3 [ネットワーク] で、[TCP/IP 構成] をクリックします。
- 4 [デフォルト] を選択し、[編集] アイコンをクリックします。
- 5 DNS 設定を手動で入力します。

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、ESXi ホスト、NFS サーバ、および Active Domain サーバの時刻を同期する必要があります。通常は、設定で Network Time Protocol (NTP) サーバとして Active Domain サーバが使用されます。

次のタスクでは、ESXi ホストを NTP サーバと同期する方法について説明します。

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 ホストに移動します。
- 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 サーバと同期するには、IP アドレスを入力します。
 - c [NTP サービスの開始] を選択します。
 - d NTP サービス起動ポリシーを設定します。
- 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 ホストに移動します。
- 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 vVols 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。

■ vVols 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、vVols データストアを作成します。

VMFS データストアの作成

VMFS データストアは、仮想マシンのリポジトリとして機能します。ファイバチャネル、iSCSI、およびローカルストレージ デバイスなど、ホストが検出する SCSI ベースのストレージ デバイス上に、VMFS データストアを設定できます。

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 Client オブジェクト ナビゲータで、ホスト、クラスタ、またはデータセンターを参照します。
- 2 右クリック メニューで [ストレージ] - [新しいデータストア] の順に選択します。

- 3 データストア タイプに VMFS を選択します。
- 4 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。
データストア名は強制的に 42 文字に制限されます。
- 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 ポリリューム] 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	VMFS6 をサポートするすべてのホストでのデフォルト フォーマットです。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。
VMFS5	VMFS5 データストアは、バージョン 6.7 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。

注： VMFS6 データストアに必要な最小サイズは、2 GB です。

- a パーティション構成を指定します。

オプション	説明
すべての利用可能なパーティションを利用	ディスク全体を 1 つの VMFS データストア専用に使します。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。[VMFS データストアからの容量再利用の要求](#)を参照してください。
- 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。

次のステップ

VMFS データストアの作成後、次のタスクを実行できます。

- データストアの容量の変更。[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。

- 容量の再利用設定の編集。容量再利用の設定の変更 を参照してください。
- 共有 VMDK サポートの有効化。VMFS6 データストア上のクラスタ化された仮想ディスクのサポートの有効化または無効化 を参照してください。

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 Client オブジェクト ナビゲータで、ホスト、クラスタ、またはデータセンターを参照します。
- 2 右クリック メニューで [ストレージ] - [新しいデータストア] の順に選択します。
- 3 データストアのタイプとして [NFS] を選択し、NFS の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。

- 4 データストアのパラメータを入力します。

オプション	説明
データストア名	データストア名は強制的に 42 文字に制限されます。
フォルダ	マウント ポイント フォルダ名
Server	サーバ名または IP アドレス。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。

- 5 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。
- 6 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 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 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。

- 7 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。
- 8 設定オプションを確認し、[終了] をクリックします。

vVols 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、vVols データストアを作成します。

手順

- 1 vSphere Client オブジェクト ナビゲータで、ホスト、クラスタ、またはデータセンターを参照します。
- 2 右クリック メニューで [ストレージ] - [新しいデータストア] の順に選択します。
- 3 データストア タイプとして [vVol] を選択します。
- 4 データストアの名前を入力し、ストレージ コンテナのリストから、バックアップ ストレージ コンテナを選択します。
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 vVols 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。
- 5 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。
- 6 設定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

vVols 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。

vVols 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、特定のデバイス操作 (LUN ID の変更など) によって、元のデータストアのコピーが作成される場合があります。

ESXi では、VMFS データストアのコピーを検出できます。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。

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。仮想マシンの構成ファイルの元の署名へのリファレンス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。

VMFS データストア コピーのマウント

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 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。

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 Client オブジェクト ナビゲータで、ホスト、クラスタ、またはデータセンターを参照します。
- 2 右クリック メニューで [ストレージ] - [新しいデータストア] の順に選択します。
- 3 データストア タイプに VMFS を選択します。
- 4 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。

- 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 データストアをマウントします。

オプション	説明
再署名を伴うマウント	[マウント オプション] で、[新しい署名を割り当て] を選択し、[次へ] をクリックします。
再署名を伴わないマウント	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。

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を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。

共有データストアにパワーオンされた仮想マシンがあり、完全に容量が使用されている場合は、データストアの容量を増やすことができます。このアクションを実行できるのは、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です。

ストレージ構成に応じて、次のいずれかの方法でデータストア容量を増やすことができます。いずれの方法でデータストア容量を増やす場合でも、仮想マシンをパワーオフする必要はありません。

既存データストアの拡張 拡張可能なデータストアのサイズを増やします。データストアのエクステントの直後にバッキング ストレージ デバイスに空き容量がある場合、そのデータストアは拡張可能とみなされます。

エクステントの追加 データストアに新しいストレージ デバイスを追加して、既存の VMFS データストアの容量を増やします。データストアは、複数のストレージ デバイスに分散できますが、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。

前提条件

ホスト ストレージが次の条件のいずれかを満たしている場合は、データストアの容量を増やすことができます。

- 既存のデータストアのバッキング デバイスに十分な空き容量がある。
- ホストに新しいストレージ デバイスを追加した。

手順

- 1 データストアに移動します。
- 2 データストアの右クリック メニューから [データストア キャパシティの増加] を選択します。
- 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 デバイスが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
既存のデータストア 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。
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だけに使用できます。
すべての利用可能なパーティションを利用	ディスク全体を 1 つのエクステント専用にします。このメニュー項目は、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。

VMFS6 データストア上のクラスタ化された仮想ディスクのサポートの有効化または無効化

Windows Server フェイルオーバー クラスタ (WSFC) 構成で仮想ディスクを使用する場合は、VMFS6 データストアが、クラスタ化された仮想ディスクをサポートしている必要があります。クラスタ化されたディスクのサポートを有効にするには、vSphere Client を使用します。

クラスタ化された仮想ディスクを仮想マシン クラスタで使用する方法については、『Windows Server フェイルオーバー クラスタのセットアップ』のドキュメントを参照してください。

前提条件

クラスタ化された仮想ディスクにデータストアを使用する場合は、次のガイドラインに沿って行ってください。

- ストレージ アレイは、ATS、WEAR (Write Exclusive – All Registrant) SCSI-3 タイプの予約をサポートしている必要があります。
- ESXi は、このタイプの構成についてファイバ チャネル アレイのみをサポートします。
- クラスタ化されたディスクをサポートするのは、VMFS6 データストアのみです。使用するデータストアは、拡張することも、複数のエクステンツにまたがることもできません。
- ストレージ デバイスは NMP によって要求される必要があります。ESXi は、クラスタ化された仮想ディスク構成のサードパーティ製プラグイン (MPP) をサポートしていません。
- クラスタリングに使用する仮想ディスクがシック プロビジョニング (Eager Zeroed) 形式になっていることを確認します。

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、[一般] をクリックします。
- 3 [データストア機能] で、[クラスタ VMDK] 項目の横にある次のオプションのいずれかをクリックします。

オプション	説明
有効化	データストアにあるクラスタ化された仮想ディスクのサポートを有効にします。サポートを有効にすると、クラスタ化された仮想ディスクをこの VMFS データストアに配置できます。
無効化	サポートを無効にします。無効にする前に、クラスタ化された仮想ディスクがあるすべての仮想マシンをパワーオフしてください。

- 4 設定を確認します。

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するには、vSphere Client を使用します。システムに悪影響を及ぼさず、仮想マシンが実行されているデータストアの名前を変更することができます。

■ データストアのアンマウント

データストアをアンマウントするとそのまま残りますが、指定したホストからは見えなくなります。マウントされたままの状態になっている別のホストでは、データストアは引き続き表示されます。

■ データストアのマウント

前にアンマウントしたデータストアをマウントすることができます。また、共有データストアにするために追加のホストにデータストアをマウントすることもできます。

■ VMFS データストアの削除

再署名せずにマウントされたコピーなど、あらゆるタイプの VMFS データストアを削除できます。データストアを削除すると、データストアが破棄され、そのデータストアへアクセスできるすべてのホストから消失します。

■ データストア ブラウザの使用

データストア ファイル ブラウザを使用して、データストアのコンテンツを管理します。データストアに格納されたフォルダとファイルを参照できます。また、ブラウザを使用して、ファイルをアップロードしたり、フォルダやファイルに対して管理タスクを実行したりすることもできます。

■ ストレージ フィルタのオフ

VMFS データストアの管理操作を行うとき、vCenter Server はデフォルトのストレージ保護フィルタを使用します。フィルタを使用すると、特定の操作に使用できるストレージ デバイスののみを取得できるため、ストレージの破損を防ぐことができます。不適切なデバイスは選択肢として表示されません。すべてのデバイスを表示するには、フィルタをオフにします。

データストア名の変更

既存のデータストアの名前を変更するには、vSphere Client を使用します。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 データストアに移動します。
- 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。

データストア名は強制的に 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設定操作を行わないでください。

注： データストアが vSphere HA のハートビート処理に使用されていないことを確認してください。vSphere HA の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ていない。
- そのデータストアに対して Storage I/O Control が無効になっている。

手順

- 1 アンマウントするデータストアに移動します。
- 2 データストアを右クリックし、[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 または vVols 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。アンマウントした VMFS データストアはマウントできます。インベントリから削除された NFS または vVols 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 台のホストまたは複数のホストに VMFS データストアをマウントすることができます。

NFS または vVols データストアをすべてのホストからアンマウントした場合、そのデータストアはインベントリに表示されなくなります。インベントリから削除された NFS または vVols 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 データストアに移動します。

- 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。
- 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、[OK] をクリックします。
- データストアを共有するすべてのホストをリストするには、データストアに移動し、[ホスト] タブをクリックします。

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

- データストアに移動します。
- 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。
- 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

- データストア ブラウザを開きます。
 - インベントリにデータストアを表示します。
 - 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。
- 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
ファイルのアップロード	データストアにファイルをアップロードします。
フォルダのアップロード (vSphere Client でのみ利用可能)	データストアにフォルダをアップロードします。
ダウンロード	データストアからダウンロードします。
新規フォルダ	データストアにフォルダを作成します。
コピー先	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。
移動先	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。
新しい名前	選択したファイルの名前を変更します。
削除	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。

データストアへのファイルまたはフォルダのアップロード

データストア ファイル ブラウザを使用して、ESXi ホスト上のデータストアにファイルをアップロードします。vSphere Client を使用している場合は、フォルダもアップロードできます。

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： vVols 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 vVols 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 vVols 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。vVols 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) ファイルまたはフォルダを保存するフォルダを作成します。

3 ファイルまたはフォルダをアップロードします。

オプション	説明
ファイルのアップロード	<ul style="list-style-type: none"> a 保存先フォルダを選択し、[ファイルのアップロード] をクリックします。 b ローカル コンピュータ上でアップロードするアイテムを検索し、[開く] をクリックします。
フォルダのアップロード (vSphere Client でのみ可能)	<ul style="list-style-type: none"> a データストアまたはターゲット フォルダを選択して、[フォルダのアップロード] をクリックします。 b ローカル コンピュータ上でアップロードするアイテムを検索し、[OK] をクリックします。

4 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またはフォルダがリストに表示されてい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て、[ダウンロード] 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移動またはコピー

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移動またはコピーします。

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。

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 移動または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、[移動先] または [コピー先] 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 ファイル名の変更

データストア ブラウザを使用して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 名前を変更するファイルを参照します。
- 3 ファイルを選択し、[新しい名前] 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、フォーマットをシックに変更できます。

データストア ブラウザを使用して、シン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 仮想マシンへ移動します。
 - 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 データストアを右クリックし、[ファイルの参照] を選択します。
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 ファイルを選択し、[拡張] をクリックします。

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。

手順

- 1 vCenter Server インスタンスを参照します。
- 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、[設定の編集] をクリックします。
- 4 無効にするフィルタを指定します。
画面の下部にある [名前] と [値] テキスト ボックスに適切な情報を入力します。

名前	値
config.vpxd.filter.vmfsFilter	False
config.vpxd.filter.rdmFilter	False

名前	値
<code>config.vpxd.filter.sameHostsAndTransportsFilter</code>	False
<code>config.vpxd.filter.hostRescanFilter</code>	False

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。

5 [追加] をクリックし、[保存] 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
<code>config.vpxd.filter.vmfsFilter</code> (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。
<code>config.vpxd.filter.rdmFilter</code> (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。
<code>config.vpxd.filter.sameHostsAndTransportsFilter</code> (同じホストと転送フィルタ)	ホストまたはストレージ タイプに互換性がないため VMFS データストア エクステントとして使用できない LUN をフィルタリングします。次の LUN はエクステントとして追加できません。 <ul style="list-style-type: none"> ■ 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。
<code>config.vpxd.filter.hostRescanFilter</code> (ホストの再スキャン フィルタ)	データストアの管理操作を行なったあと、自動的に VMFS データストアを再スキャンおよびアップデートします。フィルタは、vCenter Server が管理するすべてのホスト上にある、すべての VMFS データストアの一貫した表示を提供します。 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。

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：仮想マシン.構成.設定

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 [設定パラメータの追加] をクリックして次のパラメータを追加します。

名前	値
scsi#.returnNoConnectDuringAPD	True
scsi#.returnBusyOnNoConnectStatus	False

- e 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
scsi#:1.passthruTransientErrors	True
scsi#:2.passthruTransientErrors	True

- f [OK] をクリックします。

VMFS データストアでの 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（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。コア ダンプをネットワーク サーバに保持するように ESXi Dump Collector を設定することもできます。ESXi Dump Collector の設定の詳細については、『ESXi のインストールとセットアップ』ドキュメントを参照してください。

また、VMFS データストア上のファイルを使用して診断情報を収集する方法もあります。

■ 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、VMFS データストア上の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 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。

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、VMFS データストア上の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。

注： ソフトウェア iSCSI およびソフトウェア FCoE ストレージの VMFS データストアは、コア ダンプ ファイルをサポートしていません。

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。ESXCLI 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>--auto -a</code>	見つからない場合は、自動的にファイルを作成します。
<code>--datastore -d <i>datastore_UUID</i> or <i>datastore_name</i></code>	ダンプ ファイルのデータストアを指定します。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>--enable -e</code>	作成後に診断ファイルを有効にします。
<code>--file -f <i>file_name</i></code>	ダンプ ファイルのファイル名を指定します。指定しない場合は、ファイルの一意の名前がシステムによって作成されます。
<code>--size -s <i>file_size_MB</i></code>	ダンプ ファイルのサイズを MB 単位で設定します。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>--enable -e</code>	ダンプ ファイルを有効または無効にします。このオプションは、ダンプ ファイルの設定を解除するときには指定できません。
<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。 esxcli system coredump file set --smart --enable true
<code>--unconfigure -u</code>	現在の VMFS ダンプ ファイルの設定を解除します。

- 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 ファイルの管理で使用できるその他のコマンドの詳細については、『ESXCLI のリファレンス』ドキュメントを参照してください。

コア ダンプ ファイルの無効化と削除

構成済みのコア ダンプ ファイルを無効化し、必要に応じて、VMFS データストアから削除します。

一時的にコア ダンプ ファイルを無効化することができます。無効化したファイルを使用する予定がない場合、VMFS データストアから削除できます。無効化されていないファイルを削除するには、`esxcli system coredump file remove` コマンドを `--force | -F` 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。ESXCLI 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 Ondisk 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および修正します。

問題

VMFS データストアまたは仮想フラッシュ リソース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 VMFS データストアをバックアップする論理ボリュームの軽微な不整合問題を確認し、修正できます。

VOMA では、次の項目を確認および修正できます。

表 17-7. VOMA の機能

VOMA の機能	説明
メタデータの確認および修正	メタデータの確認と修正の例には、次のものがあります（ただし、これらに限定されません）。 <ul style="list-style-type: none"> ■ 基本的なメタデータの整合性のための VMFS ポリリューム ヘッダーの検証。 ■ VMFS リソース ファイル（システム ファイル）の整合性の確認。 ■ すべてのファイルのパス名と接続の確認。
アフィニティ メタデータの確認および修正	VMFS6 のアフィニティ チェックを有効にするには、 <code>-a --affinityChk</code> オプションを使用します。アフィニティ メタデータの確認と修正のいくつかの例を次に示します。 <ul style="list-style-type: none"> ■ リソース タイプおよび <code>FS3_ResFileMetadata</code> のアフィニティ フラグ。 ■ SFB RC メタ (<code>FS3_ResourceClusterMDVMFS6</code>) のアフィニティ フラグの検証。 ■ 無効なエントリが含まれていないことを確認するための、RC の <code>rcMeta</code> の <code>affinityInfo</code> エントリに含まれる、オーバーフロー キーを含むすべてのエントリの検証。見つからないエントリの確認。
ディレクトリの検証	VOMA では、次のエラーを検出および修正できます。 <ul style="list-style-type: none"> ■ ディレクトリ ハッシュ ブロックの破損。 ■ 割り当てマップの破損。 ■ リンク ブロックの破損。 ■ ディレクトリ エントリ ブロックの破損。 破損の性質に基づき、VOMA は、破損したエントリのみを修正するか、ハッシュ ブロック、割り当てマップ ブロック、およびリンク ブロックの全体を再構築できます。
実体のないファイル	VOMA は、ファイルシステム チェック時に、ファイルシステム内のどこからも参照されていないファイルを検出できます。これらの実体のないファイルは有効で欠落ありませんが、システム上では名前もディレクトリ エントリもありません。 <p>VOMA は、スキャン中に実体のないファイルを検出すると、ポリリュームのルートに <code>lost+found</code> という名前のディレクトリを作成し、そこに実体のないファイルを保存します。ファイルの名前では、<code>Filesequence-number</code> の形式が使用されます。</p>

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 17-8. VOMA コマンド オプション

コマンド オプション	説明						
<code>-m --module</code>	実行するモジュールには次のようなものがあります。 <table border="1"> <tbody> <tr> <td><code>vmfs</code></td> <td>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。</td> </tr> <tr> <td><code>lvm</code></td> <td>VMFS データストアをバックアップする論理ポリリュームを確認します。</td> </tr> <tr> <td><code>ptbl</code></td> <td>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。</td> </tr> </tbody> </table>	<code>vmfs</code>	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。	<code>lvm</code>	VMFS データストアをバックアップする論理ポリリュームを確認します。	<code>ptbl</code>	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。
<code>vmfs</code>	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。						
<code>lvm</code>	VMFS データストアをバックアップする論理ポリリュームを確認します。						
<code>ptbl</code>	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。						
<code>-f --func</code>	実行される機能には次のようなものがあります。						

表 17-8. VOMA コマンド オプション (続き)

コマンド オプション	説明
	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。
	fix エラーを確認して修正します。
	dump メタデータ ダンプを収集します。
-a --affinityChk	VMFS6 向けのアフィニティ関連の確認と修正を含めます。
-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。
-x --extractDump	VOMA を使用して、収集されたダンプを抽出します。
-D --dumpfile	ファイルをダンプして、収集したメタデータ ダンプを保存します。
-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。

例

```
voma -m vmfs -f check -d /vmfs/devices/disks/naa.xxxx:x
```

```
voma -m vmfs -f dump -d /vmfs/devices/disks/naa.xxxx:x -D dumpfilename
```

VOMA を使用したメタデータ整合性の確認

ここでは、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。ESXi ホストの CLI から VOMA を実行します。

前提条件

- 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。

手順

- 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	Device Name	Partition
1TB_VMFS6	naa.xxxx	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.xxxx:x
```

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
```

VMFS ポインタ ブロック キャッシュの構成

間接的ブロックとも呼ばれるポインタ ブロックは、VMFS ファイル ブロックのアドレスが含まれるファイル システム リソースです。ESXi ホスト上の vmdk ファイルを開くと、そのファイルに関連するポインタ ブロックは、ポインタ ブロック キャッシュに格納されます。ポインタ ブロック キャッシュのサイズは、設定可能なパラメータです。

ポインタ ブロック キャッシュは、VMFS から独立したホスト全体のキャッシュです。このキャッシュは、同じ ESXi ホストからアクセスできるすべてのデータストアで共有されます。

ポインタ ブロック キャッシュのサイズは、`/VMFS3/MinAddressableSpaceTB` および `/VMFS3/MaxAddressableSpaceTB` によって決まります。各 ESXi ホストの最小サイズと最大サイズを設定できます。

/VMFS3/MinAddressableSpaceTB 最小値は、システムがポインタ ブロック キャッシュに対して確保するメモリの最小量です。たとえば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。デフォルトは 10 TB です。

/VMFS3/MaxAddressableSpaceTB このパラメータによって、メモリ内でキャッシュできるポインタ ブロックの上限を定義します。デフォルトは 32 TB です。最大値は 128 TB です。通常、`/VMFS3/MaxAddressableSpaceTB` パラメータはデフォルト値で十分です。

ただし、開いている vmdk ファイルのサイズが増加すると、それらのファイルに関連するポインタ ブロック数も増加します。その増加によってパフォーマンスの低下が発生する場合は、最大値のパラメータを変更することで、ポインタ ブロック キャッシュの容量を増やすことができます。ポインタ ブロック キャッシュの最大サイズは、作業セット、または必要なアクティブ ポインタ ブロックを基に決めます。

ポインタ ブロックの消去 `/VMFS3/MaxAddressableSpaceTB` パラメータは、ポインタ ブロック キャッシュの増加も制御します。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、ポインタ ブロックの削除プロセスが開始されます。このプロセスでは、アクティブなポインタ ブロックは残されますが、容量を再利用するため、

非アクティブまたは比較的アクティブではないブロックはキャッシュから削除されます。

ポインタ ブロック キャッシュの値を変更するには、vSphere Client の [システムの詳細設定] ダイアログ ボックスまたは `esxcli system settings advanced set -o` コマンドを使用します。

`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。

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。

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。ESXCLI 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
```

ポインタ ブロック キャッシュのサイズ変更

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 ホストに移動して参照します。
- 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。

オプション	説明
<code>VMFS3.MinAddressableSpaceTB</code>	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。
<code>VMFS3.MaxAddressableSpaceTB</code>	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。

- 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。

例：esxcli コマンドを使用してポインタ ブロック キャッシュを変更

esxcli system settings advanced set -o を使用して、ポインタ ブロック キャッシュのサイズを変更することもできます。次の例では、サイズを 128 TB の最大値に設定する方法について説明します。

- 1 `/VMFS3/MaxAddressableSpaceTB` の値を 128 TB に変更するには、次のコマンドを入力します。


```
# esxcli system settings advanced set -i 128 -o /VMFS3/MaxAddressableSpaceTB
```
- 2 値が正しく設定されていることを確認するには、このコマンドを入力します。


```
# esxcli system settings advanced list -o /VMFS3/MaxAddressableSpaceTB
```

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。

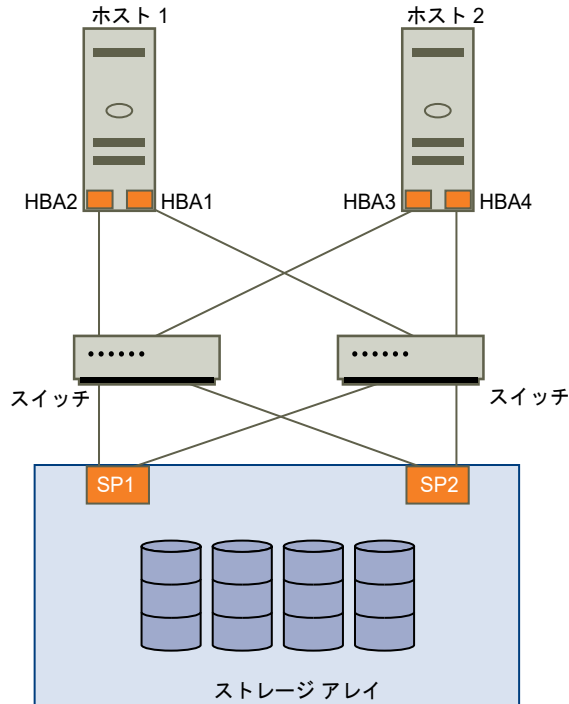
- [ファイバ チャネルを使用したフェイルオーバー](#)
- [iSCSI でのホスト ベースのフェイルオーバー](#)
- [iSCSI でのアレイ ベースのフェイルオーバー](#)
- [パスのフェイルオーバーと仮想マシン](#)
- [プラグ可能ストレージ アーキテクチャとパス管理](#)
- [パスの表示および管理](#)
- [要求ルールの使用](#)
- [仮想マシン I/O のキューのスケジューリング設定](#)

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。

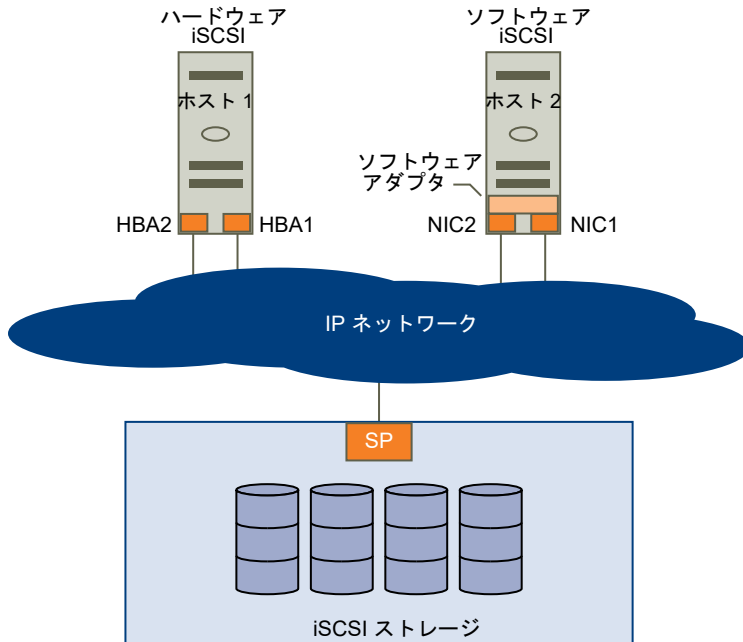
さまざまなタイプの iSCSI アダプタの詳細については、[iSCSI イニシエータ](#)を参照してください。

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、アダプタが異なるバスを使用してストレージ システムにアクセスできるようにします。

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バスにアクセスできます。このプラグインで、各物理バスの健全性を監視できます。たとえば、HBA1 自体、または HBA1 とネットワークとの間のリンクに障害が発生した場合、マルチパス プラグインでバスを HBA2 に切り替えることができます。

ソフトウェア iSCSI 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 ポートは別々のバスになり、iSCSI ストレージ スタックと iSCSI ストレージ対応のマルチパス 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 および iSER 用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、ポートでのバス利用を自動的、また ESXi に対して透過的に管理します。

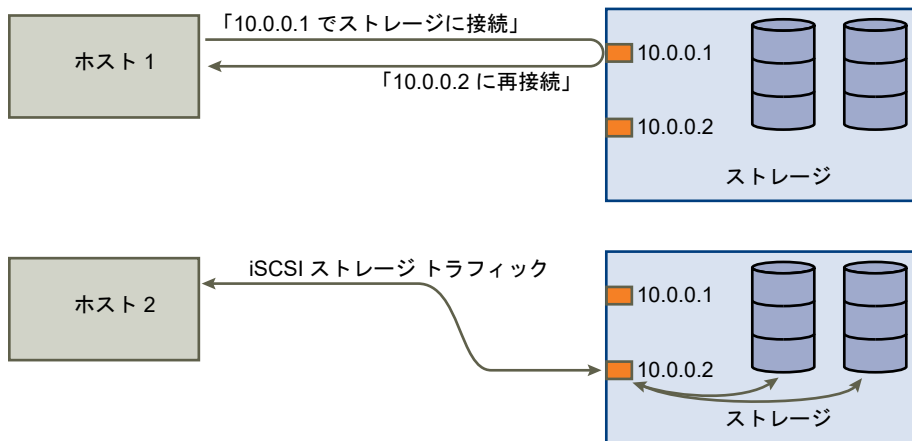
このようなストレージ システムを利用している場合、ホストはストレージ上の複数のポートを認識しないため、接続先のストレージのポートを選択できません。このようなシステムには、ホストが最初に通信を行う単一の仮想ポートアドレスがあります。この最初の通信中にストレージ システムはホストをリダイレクトして、ストレージ システム上の別のポートと通信するようになります。ホストの iSCSI イニシエータはこの再接続要求に従い、システム上の別のポートに接続します。ストレージ システムはこの技術を使用して、利用可能なポートに負荷を分散します。

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。

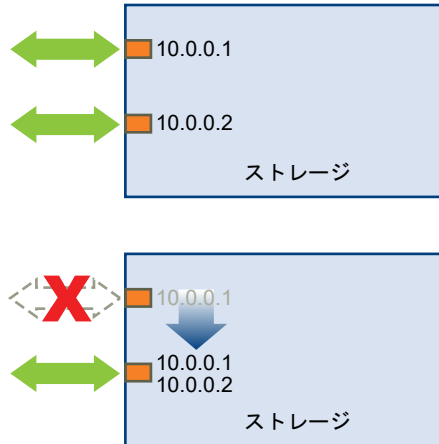
注： ストレージ システムが接続をリダイレクトしないことがあります。10.0.0.1 のポートはトラフィック用にも利用できます。

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。

プラグ可能ストレージ アーキテクチャとパス管理

このトピックでは、ESXi のストレージ マルチパスに関する主要概念について説明します。

プラグ可能ストレージ アーキテクチャ (PSA)	ESXi では、マルチパスの管理にプラグ可能ストレージ アーキテクチャ (PSA) という特殊な VMkernel レイヤーを使用します。PSA は、マルチパス操作を実行する各種のソフトウェア モジュールを調整する、オープンなモジュラ フレームワークです。これらのモジュールには、VMware によって提供される汎用マルチパス モジュールである NMP と HPP のほか、サードパーティ製のマルチパス モジュールが含まれます。
ネイティブ マルチパス プラグイン (NMP)	NMP は、ESXi がデフォルトで提供する VMkernel マルチパス モジュールです。NMP は、物理パスを特定のストレージ デバイスに関連付け、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、拡張可能であり、パス選択プラグイン (PSP) およびストレージ アレイ タイプ プラグイン (SATP) と呼ばれるその他のサブモジュールを管理します。PSP と SATP は、VMware またはサードパーティによって提供することができます。
パス選択プラグイン (PSP)	PSP は、VMware NMP のサブモジュールです。PSP は、I/O 要求の物理パスを選択します。
ストレージ アレイ タイプ プラグイン (SATP)	SATP は、VMware NMP のサブモジュールです。SATP は、アレイに固有の操作を行います。SATP は、特定のアレイに固有のパスの状態を判断し、パスのアクティベーションを実行して、パスのエラーを検出できます。
マルチパス プラグイン (MPP)	PSA は、サードパーティが独自のマルチパス プラグイン (MPP) を作成するための VMkernel API のコレクションを提供します。モジュールは、特定のストレージ アレイに対して特定のロード バランシングおよびフェイルオーバー機能を提供します。MPP は、ESXi ホストにインストールできます。MPP は、VMware ネイティブ モジュールに追加する形で実行することも、その代替として実行することもできます。
VMware High-Performance Plug-in (HPP)	HPP は、NVMe などの高速デバイスの NMP に代わる機能です。HPP により、ESXi ホスト上にローカルにインストールされている超高速のフラッシュ デバイスのパフォーマンスを向上できます。HPP は NVMe-oF のターゲットを要求するデフォルトのプラグインです。

マルチパスをサポートするため、HPP ではパス選択スキーム (PSS) を使用します。特定の PSS は、I/O 要求の物理パスを選択します。

詳細については、『[VMware High Performance プラグインとパス選択スキーム](#)』を参照してください。

要求ルール

PSA では要求ルールを使用して、特定のストレージ デバイスへのパスを所有するプラグインを判断します。

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。SCSI ストレージ デバイスで使用される汎用的な VMware のマルチパス モジュールです。
PSP	パス選択プラグイン。SCSI ストレージ 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。指定した SCSI 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。
MPP (サードパーティ)	マルチパス プラグイン。サードパーティによって開発および提供されるマルチパス モジュール。
HPP	VMware によって提供されるネイティブ高パフォーマンス プラグイン。NVMe などの超高速のローカルおよびネットワーク フラッシュ デバイスで使用されます。
PSS	パス選択スキーム。NVMe ストレージ デバイスのマルチパスを処理します。

プラグ可能ストレージ アーキテクチャについて

プラグ可能ストレージ アーキテクチャ (Pluggable Storage Architecture、PSA) は、マルチパス処理を行うさまざまなソフトウェア モジュールを調整するオープン モジュラー フレームワークです。

VMware は、VMware NMP および VMware HPP と呼ばれる汎用のネイティブ マルチパス モジュールを提供しています。また、PSA は、サードパーティの開発者が使用できる VMkernel API のコレクションを提供します。ソフトウェア開発者は、特定のストレージ アレイ用に、独自のロード バランシングおよびフェイルオーバー モジュールを作成できます。これらのサードパーティ製のマルチパス モジュール (MPP) は、ESXi ホストにインストールして、VMware ネイティブ モジュール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。

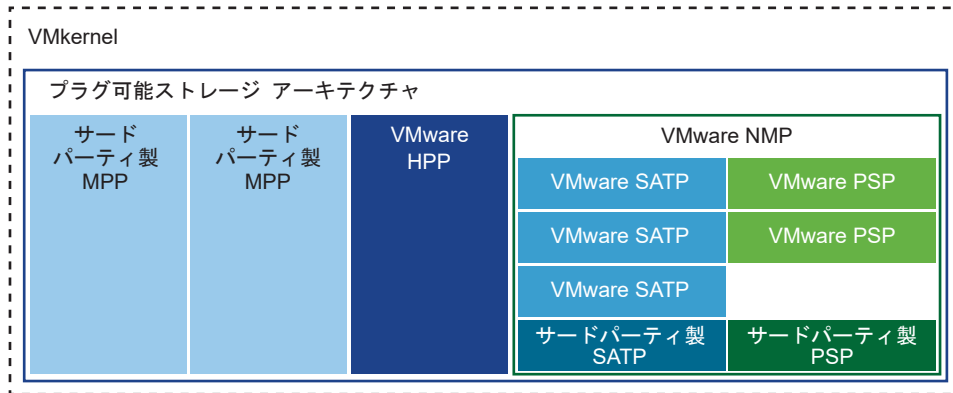
VMware のネイティブ モジュールとインストールされたサードパーティ製のマルチパス モジュールが共に機能するように調整するため、PSA は次のタスクを実行します。

- 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。
- 物理パスの検出と削除を処理します。

- 論理デバイスおよび物理パスの 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 または HPP と並行して複数のサードパーティ製のマルチパス モジュールを実行できます。サードパーティ製のマルチパス モジュールをインストールすると、これがネイティブ モジュールに代わって動作します。マルチパス モジュールは、特定のストレージ デバイスに対するパス フェイルオーバーおよびロード バランシング処理を制御します。

図 18-5. プラグ可能ストレージ アーキテクチャ



VMware Native Multipathing Plug-In

デフォルトで ESXi は、Native Multipathing Plug-In (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。

追加のマルチパス処理では、NMP は、SATP と PSP というサブモジュールを使用します。NMP は、デバイスに対するパスのフェイルオーバーの処理について、具体的な詳細を SATP に委任します。PSP は、デバイスに対するパスの選択を処理します。

通常、NMP は次の操作を実行します。

- 物理パスの要求および要求解除を管理します。
- 論理デバイスを登録および登録解除します。
- 物理パスを論理デバイスに関連付けます。
- パ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パスを選択します。
 - パスの障害や I/O コマンドの再試行を処理するために必要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。

ESXi では、使用するアレイに適した SATP を自動的にインストールします。SATP の入手やダウンロードは必要ありません。

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

- 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。

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。このモジュールには、VMware のネイティブ NMP および HPP、サードパーティ製 MPP が含まれます。

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。ESXCLI 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 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 HPP と 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。

```
Plugin name  Plugin class
-----
NMP          MP
```

このコマンドの詳細については、『ESXCLI の概念と範例』および『ESXCLI のリファレンス』ドキュメントを参照してください。

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。

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。ESXCLI 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 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。

例：NMP ストレージ デバイスの表示

```
# esxcli storage nmp device list
mpx.vmhba1:C0:T2:L0
  Device Display Name: Local VMware Disk (mpx.vmhba1:C0:T2:L0)
  Storage Array Type: VMW_SATP_LOCAL
  Storage Array Type Device Config: SATP VMW_SATP_LOCAL does not support device configuration.
  Path Selection Policy: VMW_PSP_FIXED
  Path Selection Policy Device Config: {preferred=vmhba1:C0:T2:L0;current=vmhba1:C0:T2:L0}
  Path Selection Policy Device Custom Config:
  Working Paths: vmhba1:C0:T2:L0
  Is USB: false

.....

eui.6238666462643332
  Device Display Name: SCST_BIO iSCSI Disk (eui.6238666462643332)
  Storage Array Type: VMW_SATP_DEFAULT_AA
  Storage Array Type Device Config: {action_OnRetryErrors=off}
  Path Selection Policy: VMW_PSP_FIXED
  Path Selection Policy Device Config: {preferred=vmhba65:C0:T0:L0;current=vmhba65:C0:T0:L0}
  Path Selection Policy Device Custom Config:
  Working Paths: vmhba65:C0:T0:L0
  Is USB: false
```

このコマンドの詳細については、『ESXCLI の概念と範例』および『ESXCLI のリファレンス』ドキュメントを参照してください。

パス選択プラグインとポリシー

VMware Path Selection Plug-in (PSP) は、I/O 要求の物理パスを選択します。

このプラグインは、VMware NMP のサブモジュールです。NMP は、デバイス タイプに基づいて、各論理デバイスのデフォルトの 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、「[パス選択ポリシーの変更](#)」を参照してください。

各 PSP は、対応する Path Selection Plug-In を有効にして適用します。

VMW_PSP_MRU: 最近の使用 (VMware) [最近の使用 (VMware)] ポリシーは、VMW_PSP_MRU によって適用されます。システムの起動時に検出された、使用可能な最初のパスが選択されます。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。最近の使用のポリシーでは、優先パスの設定は使用しません。このポリシーは、ほとんどのアクティブ/パッシブ ストレージ デバイスのデフォルトです。

VMW_PSP_MRU は、パスのランク付けをサポートします。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。詳細は、<http://kb.vmware.com/kb/2003468> にある VMware ナレッジベースの記事と、ESXCLI のリファレンスのドキュメントを参照してください。

VMW_PSP_FIXED：固定 (VMware)

[固定 (Vmware)] ポリシーは、VMW_PSP_FIXED によって実装されます。このポリシーは、指定された優先パスを使用します。優先パスが割り当てられていない場合、ポリシーは、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。優先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。ホストは、定義済みの優先パスが再び使用可能になると、そのパスに戻ります。アクティブ/アクティブのストレージ デバイスのデフォルト ポリシーは固定です。

VMW_PSP_RR：ラウンド ロビン (VMware)

VMW_PSP_RR は、[ラウンド ロビン (Vmware)] ポリシーを有効にします。ラウンド ロビンは、多くのアレイのデフォルト ポリシーです。このポリシーは、設定されたパスを巡回する自動パス選択アルゴリズムを使用します。

アクティブ/アクティブとアクティブ/パッシブの両方のアレイは、このポリシーを使用して異なる LUN のパス間でのロード バランシングを実装します。アクティブ/パッシブ アレイでは、このポリシーはアクティブなパスを使用します。アクティブ/アクティブ アレイでは、このポリシーは使用可能なパスを使用します。

デフォルトでポリシーに適用されている遅延メカニズムにより、適応性が向上します。ロード バランシングの結果を向上させるために、このメカニズムでは、以下のパス特性を考慮して最適なパスを動的に選択します。

- I/O 帯域幅
- パスの遅延

適合型の遅延ラウンド ロビン ポリシーのデフォルト パラメータを変更する、または遅延メカニズムを無効にする方法については、[遅延ラウンド ロビンのデフォルトパラメータの変更](#) を参照してください。

VMW_PSP_RR で構成可能なその他のパラメータを設定するには、`esxcli storage nmp psp roundrobin` コマンドを使用します。詳細については、『ESXCLI のリファレンス』を参照してください。

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『ESXCLI のリファレンス』ドキュメントを参照してください。

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。

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。ESXCLI 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 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。

例：ホストの SATP の表示

```
# esxcli storage nmp satp list
Name                Default PSP      Description
VMW_SATP_MSA        VMW_PSP_MRU     Placeholder (plugin not loaded)
VMW_SATP_ALUA        VMW_PSP_MRU     Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AP VMW_PSP_MRU     Placeholder (plugin not loaded)
VMW_SATP_SVC         VMW_PSP_FIXED   Placeholder (plugin not loaded)
VMW_SATP_EQL         VMW_PSP_FIXED   Placeholder (plugin not loaded)
VMW_SATP_INV         VMW_PSP_FIXED   Placeholder (plugin not loaded)
VMW_SATP_EVA         VMW_PSP_FIXED   Placeholder (plugin not loaded)
VMW_SATP_ALUA_CX     VMW_PSP_RR      Placeholder (plugin not loaded)
VMW_SATP_SYMM        VMW_PSP_RR      Placeholder (plugin not loaded)
VMW_SATP_CX          VMW_PSP_MRU     Placeholder (plugin not loaded)
VMW_SATP_LSI         VMW_PSP_MRU     Placeholder (plugin not loaded)
VMW_SATP_DEFAULT_AA VMW_PSP_FIXED   Supports non-specific active/active arrays
VMW_SATP_LOCAL        VMW_PSP_FIXED   Supports direct attached devices
```

このコマンドの詳細については、『ESXCLI の概念と範例』および『ESXCLI のリファレンス』ドキュメントを参照してください。

VMware High Performance プラグインとパス選択スキーム

VMware は、ESXi ホスト上の NVMe デバイスのパフォーマンスを向上させる高性能プラグイン (HPP) を提供します。

HPP は、NVMe などの高速デバイスの NMP に代わる機能です。HPP は、NVMe-oF のターゲットを要求するデフォルトのプラグインです。ESXi 内では、NVMe-oF ターゲットがエミュレートされ、ユーザーに SCSI ターゲットとして提示されます。HPP は、アクティブ/アクティブおよび暗黙的な ALUA ターゲットのみをサポートします。

ローカルの NVMe デバイスの場合、NMP はデフォルトのプラグインを残しますが、HPP に置換できます。

HPP のサポート	vSphere 7.0
ストレージ デバイス	ローカル NVMe PCIe 共有 NVMe-oF (アクティブ/アクティブおよび暗黙的な ALUA ターゲットのみ)
マルチパス	はい
第 2 レベルのプラグイン	なし パス選択スキーム (PSS)

HPP のサポート	vSphere 7.0
SCSI-3 の永続的な予約	なし
ソフトウェア エミュレーションを含む 4Kn デバイス	なし
vSAN	なし

パス選択スキーム

マルチパスをサポートするため、HPP は、I/O 要求の物理パスを選択するときにパス選択スキーム (PSS) を使用します。

デフォルトのパス選択メカニズムは、vSphere Client または `esxcli` コマンドを使用して変更できます。

vSphere Client でのパス メカニズムの設定の詳細については、[パス選択ポリシーの変更](#)を参照してください。

`esxcli` コマンドを使用して設定するには、[ESXi esxcli HPP コマンド](#)を参照してください。

ESXi は、次のパス選択メカニズムをサポートします。

固定

このスキームでは、指定した優先パスが I/O 要求に使用されます。優先パスが割り当てられていない場合、ホストは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。優先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。ホストは、定義済みの優先パスが再び使用可能になると、そのパスに戻ります。

パス選択メカニズムとして [固定] を設定する場合は、優先パスを選択します。

LB-RR (ロード バランシング - ラウンド ロビン)

これは、HPP が要求するデバイスのデフォルトのスキームです。現在のパスの、指定したバイト数または I/O を転送した後、このスキームはラウンド ロビン アルゴリズムを使用してパスを選択します。

[LB-RR] パス選択メカニズムを設定するには、次のプロパティを指定します。

- [IOPS]: デバイスのパスを切り替える基準として使用するパスの I/O 数を示します。
- [バイト]: デバイスのパスを切り替える基準として使用するパスのバイト数を示します。

LB-IOPS (ロード バランシング - IOPS)

現在のパスの、指定した数の I/O (デフォルトは 1000) を転送した後、システムは未処理の I/O が最も少ない最適なパスを選択します。

このメカニズムを設定する場合は、デバイスのパスを切り替える基準として使用されるパスの I/O 数を示す、[IOPS] パラメータを指定します。

LB-BYTES (ロード バランシング - バイト)

現在のパスで、指定したバイト数 (デフォルトは 10 MB) を転送した後、システムは未処理のバイト数が最も少ない最適なパスを選択します。

このメカニズムを設定するには、デバイスのパスを切り替える基準として使用されるパスのバイト数を示す、[バイト] パラメータを使用します。

ロード バランシング - 遅延 (LB-遅延)

ロード バランシングの結果を向上させるために、このメカニズムでは、以下のパス特性を考慮して最適なパスを動的に選択します。

- [遅延評価時間] パラメータは、パスの遅延を評価する間隔（ミリ秒）を示します。
- [パスごとのサンプリング I/O] パラメータは、パスの遅延を計算するための、各パスで発行する サンプル I/O の数を制御します。

HPP のベスト プラクティス

高速ストレージ デバイスからのスループットを最大限にするには、次の推奨事項を実行します。

- HPP をサポートするバージョンの vSphere を使用してください。
- HPP は、NVMe のローカル デバイスまたはネットワーク デバイスに対して使用してください。
- HDD または低速のフラッシュ デバイスに対し、HPP を有効にしないでください。HPP では、200,000 以上の IOPS に対応できないデバイスでは、パフォーマンスの向上は期待できません。
- NVMe over Fibre Channel デバイスを使用する場合は、ファイバ チャンネル ストレージに関する一般的な推奨事項を実行してください。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。
- NVMe-oF を使用する場合は、異なる転送タイプを使用して同じ名前空間にアクセスしないでください。
- NVMe-oF の名前空間を使用する場合は、アクティブ パスがホストに提示されていることを確認してください。アクティブなパスが検出されるまで、名前空間は登録できません。
- VMware 準仮想化コントローラを使用するように仮想マシンを構成します。『vSphere の仮想マシン管理』ドキュメントを参照してください。
- 遅延の影響を受けるしきい値を設定します。
- 単一の仮想マシンがデバイスの I/O ワークロードの大幅な共有を推進する場合、複数の仮想ディスク間で I/O を分散することを検討します。仮想マシンの個別の仮想コントローラにディスクを接続します。
そうしない場合、特定の仮想ストレージ コントローラの I/O を処理する CPU コアが飽和状態になり、I/O スループットが制限される可能性があります。

NGUID ID 形式のみをサポートする NVMe デバイスのデバイス識別子については、[NGUID デバイス識別子を持つ NVMe デバイス](#) を参照してください。

高パフォーマンス プラグインとパス選択スキームの有効化

esxcli を使用すると、ESXi ホストで高パフォーマンス プラグイン (HPP) を有効にし、パス選択スキーム (PSS) を設定できます。

HPP は、NVMe-oF のターゲットを要求するデフォルトのプラグインです。ローカルの NVMe デバイスの場合、NMP はデフォルトのプラグインを残しますが、esxcli コマンドを使用して HPP に置換できます。

ESXi Shell または vSphere CLI を使用して、HPP および PSS を設定できます。詳細については、『ESXCLI スタートガイド』および『ESXCLI のリファレンス』を参照してください。

注： PXE ブートされた ESXi ホストでは、HPP の有効化はサポートされません。

前提条件

VMware NVMe ストレージ環境を設定します。詳細については、『16 章 VMware NVMe ストレージについて』を参照してください。

手順

- 1 `esxcli storage core claimrule add` コマンドを実行して、HPP 要求ルールを作成します。

次のいずれかの方法で、要求ルールを追加します。

方法	説明
NVMe コントローラ モデルを基盤とする	<pre>esxcli storage core claimrule add --type vendor --nvme-controller-model</pre> 例： <pre>esxcli storage core claimrule add --rule 429 --type vendor --nvme-controller-model "ABCD*" --plugin HPP</pre>
PCI ベンダー ID およびサブベンダー ID を基盤とする	<pre>esxcli storage core claimrule add --type vendor --pci-vendor-id --pci-sub-vendor-id</pre> 例： <pre>esxcli storage core claimrule add --rule 429 --type vendor --pci-vendor-id 8086 --pci-sub-vendor-id 8086 --plugin HPP</pre>

- 2 PSS を設定します。

次のいずれかの方法を使用します。

方法	説明
デバイス ID に基づいて PSS を設定する	<pre>esxcli storage hpp device set</pre> 例： <pre>esxcli storage hpp device set --device=device --pss=FIXED --path=preferred path</pre>
ベンダー/モデルに基づいて PSS を設定する	<pre>--config-string</pre> オプションを <code>esxcli storage core claimrule add</code> コマンドで使用します。 例： <pre>esxcli storage core claimrule add -r 914 -t vendor -V vendor -M model -P HPP --config-string "pss=LB-Latency, latency-eval-time=40000"</pre>

- 3 ホストを再起動して、変更を有効にします。

遅延感度しきい値の設定

ストレージ デバイスに HPP を使用する場合は、I/O が I/O スケジューラを回避できるように、遅延感度しきい値を設定します。

デフォルトでは、ESXi はすべての I/O を I/O スケジューラを介して渡します。ただし、I/O スケジューラを使用すると内部キューイングが発生する可能性があるため、高速のストレージ デバイスの場合は効率的ではありません。

遅延感度しきい値を設定することにより、直接送信メカニズムを有効にして I/O がスケジューラを迂回することができます。このメカニズムを有効にすると、I/O は HPP を介して PSA からデバイス ドライバに直接渡されます。

直接送信が適切に機能するためには、観測される I/O の遅延の平均が、指定した遅延のしきい値よりも短い必要があります。I/O の遅延が遅延感度しきい値を超えると、システムは直接送信を停止し、I/O スケジューラの使用に一時的に戻ります。I/O 遅延の平均が遅延感度しきい値を再び下回ると、直接送信が再開されます。

HPP が要求したデバイス ファミリの遅延のしきい値を設定できます。ベンダーとモデルのペア、コントローラ モデル、または PCIe ベンダー ID とサブベンダー ID のペアを使用して、遅延のしきい値を設定します。

手順

- 1 デバイスの遅延感度しきい値は、次のコマンドを実行して設定します。

```
esxcli storage core device latencythreshold set -t value in milliseconds
```

次のいずれかのオプションを使用します。

オプション	例
ベンダー/モデル	指定したベンダーおよびモデルのすべてのデバイスに関する遅延感度しきい値パラメータを設定します。 esxcli storage core device latencythreshold set -v 'vendor1' -m 'model1' -t 10
NVMe コントローラ モデル	指定したコントローラ モデルのすべての NVMe デバイスに関する遅延感度しきい値を設定します。 esxcli storage core device latencythreshold set -c 'controller_model1' -t 10
PCIe ベンダー/サブベンダー ID	PCIe ベンダー ID として 0x8086、PCIe サブベンダー ID として 0x8086 を使用する、デバイスの遅延感度しきい値を設定します。 esxcli storage core device latencythreshold set -p '8086' -s '8086' -t 10

- 2 遅延感度しきい値が設定されていることを確認します。

```
esxcli storage core device latencythreshold list
```

Device	Latency Sensitive Threshold
naa.55cd2e404c1728aa	0 milliseconds
naa.500056b34036cdfd	0 milliseconds
naa.55cd2e404c172bd6	50 milliseconds

- 3 遅延感度しきい値のステータスを監視します。次のエントリの VMkernel ログを確認します。

- Latency Sensitive Gatekeeper turned on for device *device*. Threshold of *XX* msec is larger than max completion time of *YYY* msec
- Latency Sensitive Gatekeeper turned off for device *device*. Threshold of *XX* msec is exceeded by command completed in *YYY* msec

ESXi esxcli HPP コマンド

ESXi Shell または vSphere CLI のコマンドを使用して、高パフォーマンス プラグインの設定と監視ができます。

esxcli コマンドの使用の概要については『ESXCLI スタート ガイド』を、詳細については『ESXCLI のリファレンス』を参照してください。

コマンド	説明	オプション
esxcli storage hpp path list	高パフォーマンス プラグインによって現在要求されているパスを一覧表示します。	-d --device= <i>device</i> 特定のデバイスの情報を表示します。 -p --path= <i>path</i> 出力を特定のパスに制限します。
esxcli storage hpp device list	高パフォーマンス プラグインによって現在制御されているデバイスを一覧表示します。	-d --device= <i>device</i> 特定のデバイスを表示します。

コマンド	説明	オプション
<pre>esxcli storage hpp device set</pre>	<p>HPP デバイスの設定を変更します。</p>	<p><code>-B --bytes=<i>long</i></code> バスの最大バイト数。これを超えるとバスは切り替わります。</p> <p><code>-g --cfgfile</code> 構成ファイルとランタイムを新しい設定で更新します。デバイスが別の PSS によって要求されている場合、ランタイム構成に適用する際のエラーは無視してください。</p> <p><code>-d --device=<i>device</i></code> 操作対象の HPP デバイス。デバイスが報告する UID のいずれかを使用します。必須。</p> <p><code>-I --iops=<i>long</i></code> バスでの IOPS の最大値。これを超えるとバスは切り替わります。</p> <p><code>-T --latency-eval-time=<i>long</i></code> バスの遅延を評価する間隔 (ミリ秒) を制御します。</p> <p><code>-M --mark-device-ssd=<i>bool</i></code> HPP がデバイスを SSD として扱うかどうかを指定します。</p> <p><code>-p --path=<i>str</i></code> デバイスの優先バスとして設定するバス。</p> <p><code>-S --sampling-ios-per-path=<i>long</i></code> バスの遅延を計算するための、各バスで発行するサンプル I/O の数を制御します。</p> <p><code>-P --pss=<i>pss_name</i></code> デバイスに割り当てるバス選択スキーム。値を指定しない場合は、デフォルト値が選択されます。バス選択スキームの説明については、VMware High Performance プラグインとバス選択スキームを参照してください。</p> <p>次のオプションがあります。</p> <ul style="list-style-type: none"> ■ FIXED <p>優先バスを設定するには、<code>-p --path=<i>str</i></code> サブオプションを使用します。</p> ■ LB-Bytes <p>入力を指定するには、<code>-B --bytes=<i>long</i></code> サブオプションを使用します。</p> ■ LB-IOPs <p>入力を指定するには、<code>-I --iops=<i>long</i></code> サブオプションを使用します。</p> ■ LB-Latency <p>次のサブオプションがあります。</p> <p><code>-T --latency-eval-time=<i>long</i></code></p> <p><code>-S --sampling-ios-per-path=<i>long</i></code></p> ■ LB-RR (デフォルト) <p>次のサブオプションがあります。</p> <p><code>-B --bytes=<i>long</i></code></p> <p><code>-I --iops=<i>long</i></code></p>
<pre>esxcli storage hpp device usermarkedssd list</pre>	<p>ユーザーが SSD としてマークしたデバイスを一覧表示します。</p>	<p><code>-d --device=<i>device</i></code> 特定のデバイスへの出力を制限します。</p>

パスの表示および管理

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。要求ルールのセットに基づき、どのマルチパス モジュール（NMP、HPP、または MPP）が特定のデバイスへのパスを所有するかをホストが決定します。

デバイスを所有するモジュールが、デバイスのマルチパスのサポートを管理します。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を適切なモジュールに割り当てます。

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 セットが使用されます。これらのルールは、SATP および PSP のモジュールを各ストレージ デバイスに割り当て、適用するストレージ アレイ タイプ ポリシーおよびパス選択ポリシーを決定します。

vSphere Client を使用して、特定のストレージ デバイスに割り当てられている、ストレージ アレイ タイプ ポリシーとパス選択ポリシーを表示します。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確認することもできます。デフォルトのパス選択ポリシーは、必要に応じてクライアントで変更できます。

デフォルトのマルチパス モジュールまたは SATP を変更するには、vSphere CLI を使用して要求ルールを変更します。

要求ルールの変更については、[要求ルールの使用](#)を参照してください。

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 ホストに移動します。
- 2 [設定] 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 [プロパティ] タブをクリックして、NMP や HPP など、デバイスを所有しているモジュールを確認します。
[マルチパス ポリシー] に、デバイスに割り当てられた [パス選択ポリシー] および（該当する場合は）[ストレージ アレイ タイプのポリシー] も表示されます。
- 6 [パス] タブをクリックして、ストレージ デバイスで利用可能なすべてのパス、および各パスのステータスを確認します。次のパス状態情報が表示されます。

ステータス	説明
アクティブ (I/O)	現在データを転送している、機能しているパスまたは複数のパス。
スタンバイ	アクティブでないパス。アクティブなパスが使用できない場合、作動状態になり I/O の転送を開始できます。

ステータス	説明
無効	管理者によって無効にされたパス。
非活動	I/O の処理に使用できなくなったパス。物理的な中規模の障害またはアレイ構成の誤りにより、このステータスになる可能性があります。

[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。

データストア パスの表示

VMFS 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 VMFS 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 [接続およびマルチパス] をクリックします。
- 4 デバイスのマルチパス詳細を表示するホストを選択します。
- 5 マルチパス ポリシーの下で、NMP などのデバイスを所有しているモジュールを確認します。デバイスに割り当てられているパス選択ポリシーおよびストレージ アレイ タイプのポリシーも表示されます。

たとえば、次のように表示されます。

パス選択ポリシー	優先パス
ストレージ アレイ タイプのポリシー	VMW_SATP_LOCAL
所有者のプラグイン	NMP

- 6 [パス] で、デバイスのパスおよび各パスのステータスを確認します。次のパス状態情報が表示されます。

ステータス	説明
アクティブ (I/O)	現在データを転送している、機能しているパスまたは複数のパス。
スタンバイ	アクティブでないパス。アクティブなパスが使用できない場合、作動状態になり I/O の転送を開始できます。
無効	管理者によって無効にされたパス。
非活動	I/O の処理に使用できなくなったパス。物理的な中規模の障害またはアレイ構成の誤りにより、このステータスになる可能性があります。

[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。変更を加える場合は、[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

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 ホストに移動します。
- 2 [設定] 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 ポリシーを選択および設定します。オプションは、使用しているストレージ デバイスのタイプによって異なります。
 - SCSI デバイスのパス ポリシーの詳細については、[パス選択プラグインとポリシー](#)を参照してください。
 - NVMe デバイスのパス メカニズムの詳細については、[VMware High Performance プラグインとパス選択スキーム](#)を参照してください。
- 7 [OK] をクリックして設定を保存し、ダイアログ ボックスを閉じます。

遅延ラウンド ロビンのデフォルト パラメータの変更

ラウンド ロビン パス選択ポリシーに対しては、デフォルトで遅延メカニズムが有効になります。このメカニズムでは、I/O の最適なパスを選択するために、I/O のバンド幅とパスの遅延が考慮されます。遅延メカニズムを使用すると、ラウンド ロビン ポリシーは動的に最適なパスを選択して、ロード バランシングの効果を向上させることができます。

遅延メカニズムは、デフォルトのパラメータを変更したり、無効にしたりできます。

前提条件

ラウンド ロビンにパス選択ポリシーを設定します。[パス選択ポリシーの変更](#)を参照してください。

手順

- 1 遅延メカニズムを設定するには、次のコマンドを使用します。

```
esxcli storage nmp psp roundrobin deviceconfig set --type=latency --device=device ID
```

このコマンドには次のパラメータがあります。

パラメータ	説明
-S --num-sampling-cycles=sampling value	--type を latency に設定すると、各パスの平均遅延を計算するために使用する I/O の数がこのパラメータによって制御されます。このパラメータのデフォルト値は 16 です。
-T --latency-eval-time=time in ms	--type を latency に設定すると、パスの遅延が更新される頻度がこのパラメータによって制御されます。デフォルトは 3 分です。

- 遅延ラウンド ロビンとそのパラメータが正しく設定されていることを確認します。

```
esxcli storage nmp psp roundrobin deviceconfig get --device=device ID
```

または

```
esxcli storage nmp device list --device=device ID
```

次のサンプル出力で、パスの設定を示します。

```
Path Selection Policy: VMW_PSP_RR
Path Selection Policy Device Config:
{policy=latency, latencyEvalTime=180000, samplingCycles=16, curSamplingCycle=16, useANO=0;
CurrentPath=vmhba1:C0:T0:L0: NumIOsPending=0, latency=0}
```

次のステップ

遅延メカニズムを無効にするには、ホストの [システムの詳細設定] で Misc.EnablePSPLatencyPolicy パラメータを 0 に変更します。

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、パスを無効にできます。[パス] パネルには、データストア、ストレージ デバイス、アダプタ、または vVols プロトコル エンドポイントのビューからアクセスできます。

手順

- 1 ホストに移動します。
- 2 [設定] タブをクリックします。
- 3 [ストレージ] で次のいずれかをクリックします。
 - [ストレージ アダプタ]
 - [ストレージ デバイス]
 - [プロトコル エンドポイント]
- 4 右側のペインでパスを無効にするアイテム（アダプタ、ストレージ デバイス、またはプロトコル エンドポイント）を選択し、[パス] タブをクリックします。
- 5 無効にするパスを選択して、[無効] をクリックします。

パスのステータスが無効になります。

要求ルールの使用

要求ルールでは、特定のストレージ デバイスへのパスを所有するマルチパス モジュールが決定されます。また、デバイスにホストが提供するマルチパス サポートの種類が定義されます。

要求ルールはホストの /etc/vmware/esx.conf ファイルに一覧表示されます。

ルールは、次のカテゴリに分類されます。

コア要求ルール これらの要求ルールでは、どのマルチパス モジュール（NMP、HPP、またはサードパーティ製のマルチパス モジュール）が特定のデバイスを要求するのかが決定されます。

SATP 要求ルール デバイスのタイプによっては、これらのルールにより、ベンダー固有のマルチパスの管理を提供する特定の SATP サブモジュールがデバイスに割り当てられます。

esxcli コマンドを使用して、コアおよび SATP 要求ルールを追加または変更できます。通常、サードパーティ製の MPP をロードするか、ホストに LUN を非表示にする要求ルールを追加します。特定のデバイスのデフォルト設定が不十分な場合に、要求ルールの変更が必要となる場合があります。

PSA 要求ルールの管理に使用できるコマンドの詳細については、『ESXCLI スタート ガイド』を参照してください。

ストレージ アレイのリストと対応する SATP および PSP については、『vSphere Compatibility Guide』の「Storage/SAN」セクション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。

要求ルールは、NMP、HPP、またはサードパーティ製マルチパス モジュール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 チャンネルなどのトランスポート
- アダプタ、ターゲット、または LUN の場所
- デバイス ドライバ（たとえば Mega-RAID）

手順

- ◆ **esxcli 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一覧表示します。

claimrule-class オプションを使用しないは、MP ルール クラスが使用されます。

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	10	runtime	vendor	HPP	vendor=NVMe model=*	
MP	10	file	vendor	HPP	vendor=NVMe model=*	
MP	50	runtime	transport	NMP	transport=usb	
MP	51	runtime	transport	NMP	transport=sata	
MP	52	runtime	transport	NMP	transport=ide	
MP	53	runtime	transport	NMP	transport=block	
MP	54	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。
- HPP、MPP_1、MPP_2、および MPP_3 のルールが追加されたため、モジュールは指定したデバイスを要求できるようになりました。たとえば、HPP はベンダー NVMe のすべてのデバイスを要求します。インボックス nvme ドライバで処理されるすべてのデバイスが、実際のベンダーに関係なく、要求されます。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。

- 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。
- 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。いくつかのデフォルトのシステム定義要求ルールには、Class が runtime となっている行が 1 つのみあります。これらのルールは変更できません。
- デフォルト ルール 65535 は、要求を受けていないすべてのパスを NMP に割り当てます。このルールを削除しないでください。

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てから、使用しているシステムにロードします。

次のような場合に PSA 要求ルールを追加します。

- 新規のサードパーティ製マルチパス モジュールをロードしており、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。
- ネイティブの HPP を有効にする必要がある。

注意: 2 つの異なるプラグインが同じデバイスへのパスを要求するルールは作成できません。これらの要求ルールを作成すると、失敗して vmkernel.log に警告が表示されます。

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。ESXCLI 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、次のコマンドを使用します。

```
esxcli 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
-A --adapter=<adapter>	使用するパスのアダプタ。--type が location の場合にのみ有効です。
-u --autoassign	特性に基づいて要求ルールを追加します。ルール番号は不要です。
-C --channel=<channel>	使用するパスのチャネル。--type が location の場合にのみ有効です。

オプション	説明
<code>-c --claimrule-class=<cl></code>	この操作で使用する要求ルール クラス。MP (デフォルト)、Filter、または VAAI を指定できます。 新しいアレイのハードウェア アクセラレーションを設定するには、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。詳細については、 ハードウェア アクセラレーションの要求ルールの追加 を参照してください。
<code>-d --device=<device_uid></code>	デバイスの UID。--type が device の場合にのみ有効です。
<code>-D --driver=<driver></code>	使用するバスの HBA 用ドライバ。--type が driver の場合にのみ有効です。
<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>--force-reserved</code>	予約済みのルール ID 範囲の保護をオーバーライドします。 予約済みの要求ルールは、ID が 100 未満のルールです。それらを使用して、ローカル デバイスを特定のプラグインに (たとえば、NVMe デバイスを HPP に) 再割り当てすることができます。
<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=<iscsi_name></code>	ターゲットの iSCSI 修飾名。--type が target の場合にのみ有効です。
<code>-L --lun=<lun_id></code>	バスの LUN。--type が location の場合にのみ有効です。 LUN ID は、詳細設定オプション /Disk/MaxLUN の値を超えないように設定します。
<code>-M --model=<model></code>	使用するバスのモデル。--type が vendor の場合にのみ有効です。 有効な値は、SCSI INQUIRY 文字列からのモデル文字列の値です。モデル文字列の値を表示するには、各デバイスで <code>vicfg-scsidevs <conn_options> -l</code> を実行します。
<code>-P --plugin=<plugin></code>	使用する PSA プラグイン。値は NMP、MASK_PATH、または HPP です。サードパーティは、独自の PSA プラグインを指定することもできます。必須。
<code>-r --rule=<rule_ID></code>	使用する ルール ID。ルール ID は、要求ルールを評価する順序を示します。ユーザー定義の要求ルールは、101 から始まる数値順に評価されます。 使用可能なルール ID を特定するには、 <code>esxcli storage core claimrule list</code> を実行します。
<code>-T --target=<target></code>	使用するバスのターゲット。--type が location の場合にのみ有効です。
<code>-R --transport=<transport></code>	使用するバスの転送。--type が transport の場合にのみ有効です。次の値がサポートされています。 <ul style="list-style-type: none"> ■ block: ブロック ストレージ ■ fc: ファイバ チャネル ■ iscsivendor: iSCSI ■ iscsi: 現在使用されていません ■ ide: IDE ストレージ ■ sas: SAS ストレージ ■ sata: SATA ストレージ ■ usb: USB ストレージ ■ parallel: パラレル ■ fcoe: FCoE ■ unknown

オプション	説明
-t --type=<type>	処理に使用する一致タイプ。有効な値は次のとおりです。必須。 <ul style="list-style-type: none"> ■ vendor ■ location ■ driver ■ transport ■ device ■ target
-V --vendor=<vendor>	使用するバスのベンダー。--type が vendor の場合にのみ有効です。有効な値は、SCSI INQUIRY 文字列からのベンダー文字列の値です。ベンダー文字列の値を表示するには、各デバイスで <code>vicfg-scsidevs <conn_options> -l</code> を実行します。
--wwnn=<wwnn>	ターゲットの WWNN (World-Wide Node Number)。
--wwpn=<wwpn>	ターゲットの WWPN (World-Wide Port Number)。
-a --xcopy-use-array-values	アレイからレポートされた値を使用して、ストレージ アレイに送信する XCOPY コマンドを作成します。これは、VAAI の要求ルールにのみ適用されます。
-s --xcopy-use-multi-segs	XCOPY 要求を発行する場合は、複数のセグメントを使用します。--xcopy-use-array-values が指定されている場合にのみ有効です。
-m --xcopy-max-transfer-size	アレイからレポートされた値とは異なる転送サイズを使用する場合の最大データ転送サイズ (MB)。--xcopy-use-array-values が指定されている場合にのみ有効です。
-k --xcopy-max-transfer-size-kib	アレイからレポートされた値とは異なる転送サイズを使用する場合の、XCOPY コマンドの最大転送サイズ (KB)。--xcopy-use-array-values が指定されている場合にのみ有効です。

- 2 システムに新規の要求ルールをロードするには、次のコマンドを使用します。

esxcli storage core claimrule load

このコマンドは、新規作成されたマルチバスの要求ルールすべてを、`esx.conf` 構成ファイルから VMkernel にロードします。このコマンドにはオプションはありません。

- 3 ロードされている要求ルールを適用するには、次のコマンドを使用します。

esxcli storage core claimrule run

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=<adapter>	--type が location の場合に、要求ルールを実行するバスの HBA の名前。すべてのアダプタからのバスで要求ルールを実行する場合は、このオプションは省略します。
-C --channel=<channel>	--type が location の場合に、要求ルールを実行するバスの SCSI チャネル番号の値。すべてのチャネル番号を持つバスで要求ルールを実行するには、このオプションを省略します。
-c --claimrule-class=<cl>	この操作で使用する要求ルール クラス。
-d --device=<device_uid>	デバイスの UID。
-L --lun=<lun_id>	--type が location の場合の、要求ルールを実行するバスの SCSI LUN の値。すべての LUN を持つバスで要求ルールを実行するには、このオプションを省略します。
-p --path=<path_uid>	--type が path の場合、このオプションは、要求ルールを実行するバスの一意的識別子 (UID) またはランタイム名を示します。

オプション	説明
<code>-T --target=<target></code>	<code>--type</code> が <code>location</code> の場合に、要求ルールを実行するバスの SCSI ターゲット番号の値。すべてのターゲット番号を持つバスで要求ルールを実行するには、このオプションを省略します。
<code>-t --type=<location path all></code>	実行する要求のタイプ。デフォルトでは <code>all</code> が使用されます。つまり、要求ルールが特定のバスや SCSI アドレスに制限されずに実行されるということです。有効な値は、 <code>location</code> 、 <code>path</code> 、および <code>all</code> です。
<code>-w --wait</code>	このオプションは、 <code>--type all</code> も使用する場合にのみ使用できます。 このオプションが含まれている場合、要求処理を実行する前に、バスが解決されるまで待機します。その場合、システム上のすべてのバスが検出されたと考えられるまで、システムは要求プロセスを開始しません。 要求プロセスが開始された後、デバイスの登録が完了するまでコマンドは返されません。 要求中または検出中にバスを追加または削除すると、このオプションが正しく機能しない場合があります。

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 storage core claimrule add -r 500 -t vendor -V NewVend -M NewMod -P NMP
```

```
# esxcli storage core claimrule load
```

`esxcli 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		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。

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。ESXCLI 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 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 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。

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。ESXCLI 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 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 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 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 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 storage core claiming unclaim

- 6 パス要求ルールを実行します。

esxcli 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 storage core claimrule list

2 #esxcli storage core claimrule add -P MASK_PATH -r 109 -t location -A vmhba2 -C 0 -T 1 -L 20
  #esxcli storage core claimrule add -P MASK_PATH -r 110 -t location -A vmhba3 -C 0 -T 1 -L 20
  #esxcli storage core claimrule add -P MASK_PATH -r 111 -t location -A vmhba2 -C 0 -T 2 -L 20
  #esxcli storage core claimrule add -P MASK_PATH -r 112 -t location -A vmhba3 -C 0 -T 2 -L 20

3 #esxcli storage core claimrule load

4 #esxcli storage core claimrule list

5 #esxcli storage core claiming unclaim -t location -A vmhba2
  #esxcli storage core claiming unclaim -t location -A vmhba3

6 #esxcli 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。

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。ESXCLI 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 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 storage core claimrule list

- 3 バスの要求ルールを構成ファイルから VMkernel に再ロードします。

```
esxcli storage core claimrule load
```

- 4 マスクされたストレージ デバイスへのバスごとに **esxcli storage core claiming unclaim** コマンドを実行します。

例 :

```
esxcli 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 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、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。通常は、ストレージ デバイスに指定されたデフォルトの SATP を使用しても問題ありません。デフォルト設定では不十分な場合は、**esxcli** コマンドを使用して特定のデバイスの SATP を変更します。

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 ルールの作成が必要な場合があります。

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。ESXCLI 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 storage nmp satp rule add** コマンドを実行します。このコマンドには次のオプションがあります。

オプション	説明
-b --boot	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。esx.conf 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。
-c --claim-option=string	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。
-e --description=string	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。
-d --device=string	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。
-D --driver=string	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。
-f --force	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。
-h --help	ヘルプ メッセージを表示します。
-M --model=string	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。

オプション	説明
<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。
<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 storage nmp satp rule add -V NewVend -M NewMod -s VMW_SATP_INV
```

`esxcli storage nmp satp list -s VMW_SATP_INV` コマンドを実行すると、VMW_SATP_INV ルールのリストに新しいルールが表示されます。

仮想マシン I/O のキューのスケジュール設定

vSphere には、デフォルトで、すべての仮想マシン ファイルのキューのスケジュールを作成するメカニズムが用意されています。たとえば、.vmdk などの各ファイルには、それ独自のバンド幅制御が適用されます。

このメカニズムにより、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 ごとのスケジュールの編集

`VMkernel.Boot.isPerFileSchedModelActive` 詳細パラメータでは、ファイル I/O ごとのスケジュール メカニズムが制御されます。このメカニズムはデフォルトで有効になっています。

ファイルごとの I/O スケジュール モデルを無効にすると、ホストはレガシーのスケジュール メカニズムに戻ります。レガシーのスケジュールでは、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 キューのみが保持されます。仮想マシンと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。

注： HPP プラグインがあり、高速のローカル デバイスに遅延の影響を受けるしきい値パラメータが設定されている場合、ファイルごとのスケジュールを無効にしないでください。ファイルごとのスケジュールを無効にすると、予期しない動作が発生する可能性があります。

手順

- 1 ホストに移動します。
- 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 [VMkernel.Boot.isPerFileSchedModelActive] パラメータの値を編集します。

オプション	説明
False	ファイルごとのスケジュール メカニズムを無効にします。
True (デフォルト)	ファイルごとのスケジュール メカニズムを有効に戻します。

- 5 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。

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。ESXCLI 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
esxcli system settings kernel set -s isPerFileSchedModelActive -v FALSE	ファイルごとの I/O スケジュールの無効化
esxcli system settings kernel set -s isPerFileSchedModelActive -v TRUE	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。

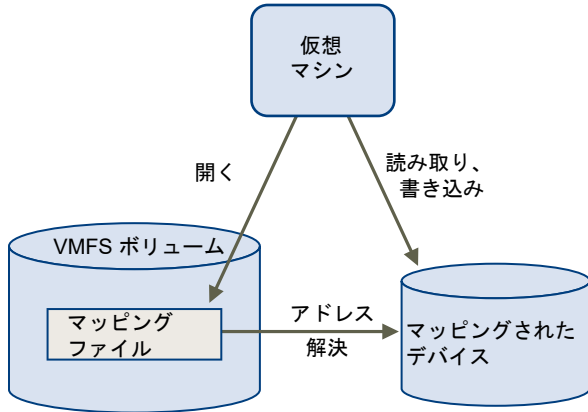
- [RAW デバイス マッピングについて](#)
- [Raw デバイス マッピングの特性](#)
- [RDM を使用する仮想マシンの作成](#)
- [マッピング済み LUN のパス管理](#)
- [RDM を使用した仮想マシンで SCSI 照会キャッシュを無視する必要がある](#)

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 ボリュームから Raw LUN へのシンボル リンクとして考えます。マッピングにより、LUN は VMFS ボリューム内のファイルとして認識されるようになります。Raw LUN ではない RDM は、仮想マシン構成で参照されます。RDM には、Raw LUN への参照が含まれています。

RDM 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の ID 情報を保存します。VMFS は、アダプタハードウェアの変更、パスの変更、デバイスの移動などによりサーバの物理構成に変更が発生しても、現在の SCSI デバイスと各 RDM を関連付けます。

分散ファイル ロック

Raw SCSI デバイスの VMFS 分散ロックを使用できます。RDM で分散ロックを使用することにより、別のサーバにある 2 個の仮想マシンが同じ LUN にアクセスしようとしても、データを消失することなく、共有の Raw LUN を安全に使用できます。

ファイル権限

ファイル権限を使用できます。マッピング ファイルの権限は、マッピング済みのボリュームを保護するため、ファイルを開くときに使用されます。

ファイル システムの操作

マッピング ファイルをプロキシとして使用して、マッピング済みのボリュームで、ファイル システム ユーティリティを使用できます。通常のファイルに有効なほとんどの操作は、マッピング ファイルに適用でき、マッピング済みのデバイスで機能するようにリダイレクトされます。

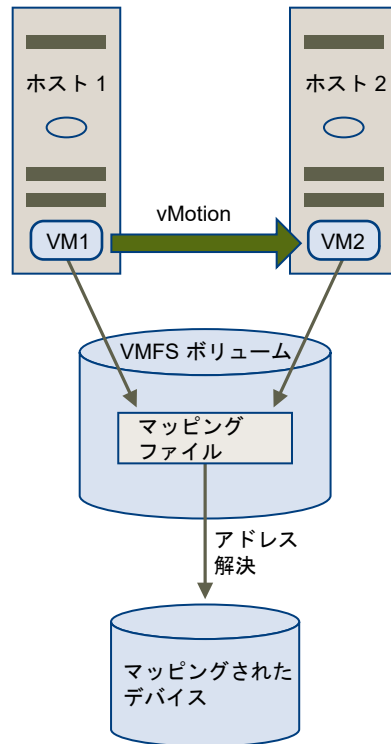
スナップショット

マッピング済みのボリュームで仮想マシンのスナップショットを使用できます。RDM が物理互換モードで使用されている場合、スナップショットは使用できません。

vMotion

vMotion を使用して仮想マシンの移行ができます。マッピング ファイルはプロキシとして機能し、仮想ディスク ファイルの移行と同じメカニズムを使用することで、vCenter Server が仮想マシンを移行できるようにします。

図 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。

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 ポリ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 ポリ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せん。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

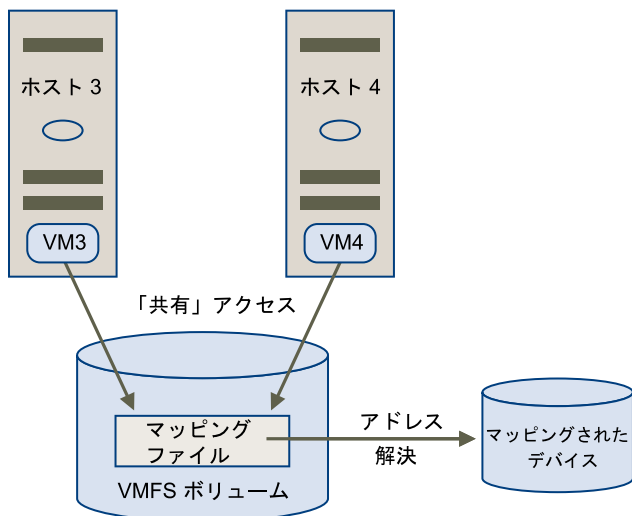
RDM ファイルでは、Raw デバイスへのパスが変更されたときに動的名前解決が可能です。

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 仮想マシンを作成します。
 - a 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。
 - b [新規仮想マシンの作成] を選択し、[次へ] をクリックします。
 - c 仮想マシンの作成に必要な手順すべてを実行します。
- 2 [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。
- 3 （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。

4 RDM ディスクを追加します。

- a [新規デバイスを追加] をクリックし、リストから [RDM ディスク] を選択します。
- b LUN のリストから、ターゲットの Raw LUN を選択し、[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。

5 RDM ディスクを設定します。

- a [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。
- b RDM 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。

- c 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。

- d 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しても、仮想ディスクの状態は常に同じです。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。

6 仮想マシンの設定を完了します。

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 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。
- 3 [物理 LUN] の横に表示されるデバイス ID をクリックして、[マルチパス ポリシーの編集] ダイアログ ボックスを開きます。
- 4 [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。

RDM を使用した仮想マシンで SCSI 照会キャッシュを無視する必要がある

RDM を使用する特定の仮想マシンは、ESXi でキャッシュされた SCSI INQUIRY データを使用するのではなく、LUN から SCSI INQUIRY 情報を取得する必要があります。

問題

RDM を使用した仮想マシンで実行している特定のゲスト OS またはアプリケーションが予期しない動作を示します。

原因

この動作は、特定のゲスト OS およびアプリケーションの妨げとなるキャッシュされた SCSI INQUIRY データによって生じる可能性があります。

ESXi は、最初にターゲットのストレージデバイスに接続したときに、デバイスから基本的な識別データを取得するために SCSI INQUIRY コマンドを発行します。デフォルトでは、ESXi は受信した SCSI INQUIRY データ（標準、ページ 80、およびページ 83）をキャッシュした後も、データは変更されません。後続の SCSI INQUIRY コマンドに対する応答がキャッシュから返されます。

ただし、RDM を使用する仮想マシンで実行している特定のゲスト OS は、ESXi によりキャッシュされた SCSI INQUIRY データを使用する代わりに LUN を照会する必要があります。このような場合は、SCSI INQUIRY キャッシュを無視するように仮想マシンを構成できます。

解決方法

- ◆ 次のいずれかの方法を使用します。

変更は、ストレージベンダーが推奨する場合のみ実行してください。

オプション	説明
RDM を使用する仮想マシンの .vmx ファイルを変更します。	<p>この方法は、ハードウェアのバージョンが 8 以降の仮想マシンに使用します。</p> <p>a ファイルに次のパラメータを追加します。</p> <pre>scsix:y.ignoreDeviceInquiryCache = "true"</pre> <p>ここで、x は SCSI コントローラ番号、y は RDM の SCSI ターゲット番号です。</p> <p>b 仮想マシンを再起動します。</p>
esxcli コマンドを使用します。	<p>ホスト レベルで設定するため、仮想マシンのハードウェアバージョンの制約は受けません。</p> <pre>esxcli storage core device inquirycache set --device device id --ignore true</pre> <p>仮想マシンの再起動は必要ありません。</p>

どの方法を使用して SCSI INQUIRY キャッシュ パラメータを true に設定しても、仮想マシンは LUN への直接接続を開始して SCSI INQUIRY データを取得します。

vmx の ignoreDeviceInquiryCache パラメータ	esxcli で inquirycache パラメータを無視します	以下から提供される照会要求
True	True	LUN
False (パラメータが存在しない場合のデフォルト値)	True	LUN
True	False	LUN
False (パラメータが存在しない場合のデフォルト値)	False	キャッシュ

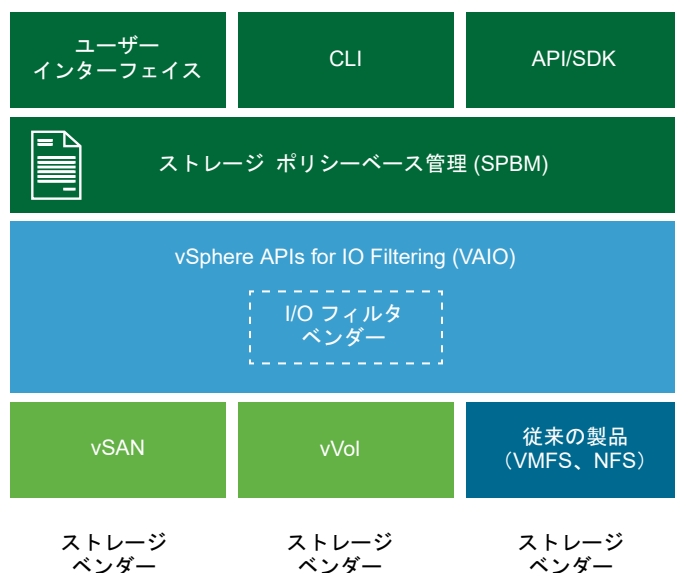
ストレージ ポリシー ベースの管理

20

Software-Defined Data Center (SDDC) 内では、ストレージを仮想マシンのアプリケーション需要に合わせる上で、ストレージ ポリシー ベース管理 (SPBM) が主要な役割を果たします。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 フレームワークが提供されます。

SPBM は抽象レイヤーとして、vVols、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。

個別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 はさまざまな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。

この章には、次のトピックが含まれています。

- [仮想マシン ストレージ ポリシー](#)
- [仮想マシン ストレージ ポリシーのワークフロー](#)
- [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](#)
- [ルールおよびルール セットについて](#)
- [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 コンポーネントについて](#)
- [ストレージ ポリシーと仮想マシン](#)
- [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

仮想マシンのストレージ ポリシーは、SPBM による仮想マシンのプロビジョニングに不可欠です。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 ポリシーのワークフロー

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、vVols、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および vVols 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のある単一のデータ 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 ストレージ ポリシーの作成と管理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>

ストレージ ポリシーを作成および管理するには、vSphere 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 インターフェイスの入力

仮想マシン ストレージ ポリシーの作成を開始する前に、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を仮想マシン ストレージ ポリシー インターフェイスにポピュレートする必要があります。

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。

ストレージ機能およびサービス

たとえば vVols 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ダプタイズできます。これらのデータストア機能、データ サービス、さまざまな値を持つその他の特性が仮想マシン ストレージ ポリシー インターフェイスにポピュレートされます。

これらの特性は、ストレージ ポリシーにデータストアの配置およびサービス ルールを定義するときに使用します。

データ サービス

ホスト上の I/O フィルタは、ストレージ プロバイダによっても表されます。ストレージ プロバイダは、フィルタのデータ サービスに関する情報を仮想マシン ストレージ ポリシー インターフェイスに提供します。この情報は、共通ルールとも呼ばれる、ホストベースのデータ サービスのルールを定義するときに使用します。データストアに固有のルールとは異なり、これらのルールでは仮想マシンのストレージ配置およびストレージ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。

vVols および vSAN データストアの場合、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、vVols、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。vVols 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。

- vVols 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 フィルタが提供するデータ サービス。

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 VMware vSphere Virtual Volumes \(vVol\) の操作](#)

■ 23 章 仮想マシン I/O のフィルタリング

手順

- 1 vCenter Server インスタンスを参照します。
- 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 ホーム メニューから、[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 [カテゴリの追加] 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
オブジェクトあたりのタグ数	[複数のタグ]
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 クラスタ]

- 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 [タグの追加] 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 データストアに移動します。
- 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 タグのリストから該当するタグを選択します。たとえば、ストレージの場所カテゴリでテキサスを選択し、[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。[タグベースの配置用に仮想マシン ストレージ ポリシーを作成](#)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 vVols 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。



ストレージ ポリシーでのタグの使用

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 vVols データストアのリストから除外できます。[タグベースの配置用に仮想マシン ストレージ ポリシーを作成](#)を参照してください。

ホストベースのサービスのルール

このルール セットは、ホストによって提供されるデータ サービスを有効にします。ホストベースのサービスのルール セットには、ルール、または暗号化やレプリケーションなどの特定のデータ サービスを示すストレージ ポリシー コンポーネントを含めることができます。

データストア固有のルールとは異なり、このセットには配置ルールは含まれません。ホストベースのサービスのルールは、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。[ホストベースのデータ サービスの仮想マシン ストレージ ポリシーの作成](#)を参照してください。

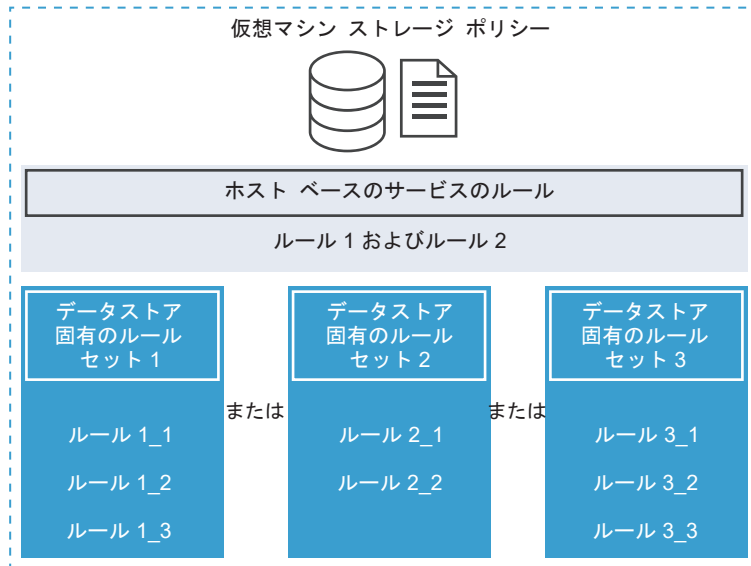
表 20-1. 仮想マシン ストレージ ポリシーの構造

ホストベースのサービスのルール	データストア固有のルール 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、機能ベースまたはタグベースの配置ルール。たとえば、vVols 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、vVols 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、ポリシー内のデータストア固有のルール 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。ポリシーには、ホストベースのサービスのルール セットと、データストア固有のルール セットの、どちらか一方のみ含めることも、両方含めることもできます。

ホストベースのサービスのルール セットが含まれていない場合、1 つのデータストア固有のルール セット内の全ルールに適合すれば、ポリシー全体を満たすことができます。ホストベースのサービスのルール セットが含まれている場合、ポリシーは、ホスト サービスのルールおよびデータストア固有のルール セット内の全ルールを満たすデータストアと一致します。



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、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。

ホストベースのデータ サービスの仮想マシン ストレージ ポリシーの作成

vSphere Client で仮想マシン 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 ポリシーの作成] ウィザードを使用します。このタスクでは、ESXi ホストによって提供されるデータ サービスのルールを作成します。これらの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。

使用可能なデータ サービスには、暗号化、I/O コントロール、キャッシュなどがあります。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。ホストにインストールしたサードパーティの I/O フィルタにより、他のデータ サービスを提供することもできます。

通常、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。データストア固有のルールをストレージ ポリシーに追加することはオプションです。

データストア固有のルールを追加し、ホストとストレージの I/O フィルタの両方が同一のタイプのサービス（暗号化など）を提供する場合、ポリシーは両方のプロバイダからこのサービスを要求できます。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、vVols 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 ポリシーに共存できません。

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。
- 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 ポリシーの作成] ウィザードを開きます。
 - a [メニュー]-[ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
 - c [仮想マシン ストレージ ポリシーの作成] をクリックします。
- 2 ポリシーの名前と説明を入力して [次へ] をクリックします。

オプション	操作
vCenter Server	vCenter Server インスタンスを選択します。
名前	ストレージ ポリシーの名前を入力します。
説明	ストレージ ポリシーの説明を入力します。

- 3 [ホスト ベースのサービス] の [ポリシー構造] ページで、ホスト ベースのルールを有効にします。
- 4 [ホスト ベースのサービス] ページで、ホストによって提供されるデータ サービスを有効にして構成するためのルールを定義します。
 - a データ サービス カテゴリのタブ ([レプリケーション] など) をクリックします。
 - b データ サービス カテゴリのカスタム ルールを定義するか、事前定義されたコンポーネントを使用します。

オプション	説明
無効	ホスト ベースのサービスは、デフォルトで無効になっています。
ストレージ ポリシー コンポーネントの使用	ドロップダウン メニューからストレージ ポリシー コンポーネントを選択します。このオプションは、データベースにコンポーネントを事前定義している場合にのみ使用できます。
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： 複数のデータ サービスを有効にすることができます。他のデータ サービス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サービスでクリア テキスト データを分析できるようになります。

- 5 [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ます。

ホスト ベースのサービスのポリシーと互換性を持たせるには、これらのサービスを提供するホストにデータストアを接続する必要があります。データストア固有のルール セットをポリシーに追加した場合は、互換性のあるデータストアもポリシーのストレージ要件を満たす必要があります。

- 6 [確認して完了] ページでポリシーの設定を確認し、[完了] をクリックします。

設定を変更するには、[戻る] をクリックして関連するページに移動します。

結果

ホスト ベースのデータサービス用の新しい仮想マシン ストレージ ポリシーがリストに表示されます。

vVols 用の仮想マシン ストレージ ポリシーの作成

vSphere Client で仮想マシン 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 ポリシーの作成] ウィザードを使用します。このタスクでは、vVols と互換性のあるカスタム ストレージ ポリシーを作成します。vVols の仮想マシン ストレージ ポリシーを定義するときは、vVols データストアによって提供されるストレージとデータ サービスを構成するためのルールを作成します。このルールは、仮想マシンが vVols データストアに配置されているときに適用されます。カスタム ストレージ ポリシーを、VMware が提供する vVols のデフォルトの要件なしのストレージ ポリシーと置き換えることができます。

この手順では、vVols 用の仮想マシン ストレージ ポリシーを作成することを前提としています。vSAN ストレージ ポリシーの詳細については、VMware vSAN の管理ドキュメントを参照してください。

前提条件

- vVols 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。[vVols 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 [仮想マシン ストレージ ポリシーの作成] ウィザードを開きます。
 - a [メニュー]-[ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
 - c [仮想マシン ストレージ ポリシーの作成] をクリックします。
- 2 ポリシーの名前と説明を入力して [次へ] をクリックします。

オプション	操作
vCenter Server	vCenter Server インスタンスを選択します。
名前	ストレージ ポリシーの名前 (vVolsStorage Policy など) を入力します。
説明	ストレージ ポリシーの説明を入力します。

- 3 [データストア固有のルール] の [ポリシー構造] ページで、vVols ストレージなどの、ターゲット ストレージ エンティティのルールを有効にします。

複数のデータストアのルールを有効にすることができます。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)。

4 Virtual Volumes ルール ページで、ターゲット vVols データストアのストレージ配置ルールを定義します。

- a [配置] タブをクリックして、[ルールの追加] をクリックします。
- b [ルールの追加] ドロップダウン メニューから、使用可能な機能を選択してその値を指定します。

たとえば、vVols 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、vVols データストア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 配置要求をさらに微調整するには、[タグ] タブをクリックし、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することで、データストアをフィルタリングできます。たとえばテキサスおよびカリフォルニアにある vVols 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。

5 (オプション) データストア固有のサービスを構成するためのルールを定義します。

暗号化、キャッシュ、レプリケーションなどのデータ サービスが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、仮想マシンが vVols データストアに配置されたときに、仮想マシン用にこれらのサービスを要求します。

- a データ サービス カテゴリのタブ ([レプリケーション] など) をクリックします。
- b データ サービス カテゴリのカスタム ルールを定義するか、事前定義されたコンポーネントを使用します。

オプション	説明
無効	データストア固有のサービスは、デフォルトで無効になっています。
ストレージ ポリシー コンポーネントの使用	ドロップダウン メニューからストレージ ポリシー コンポーネントを選択します。このオプションは、データベースにコンポーネントを事前定義している場合にのみ使用できます。
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。

6 [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ます。

ポリシーに複数のルール セットが含まれている場合は、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。

7 [確認して完了] ページでポリシーの設定を確認し、[完了] をクリックします。

設定を変更するには、[戻る] をクリックして関連するページに移動します。

結果

vVols 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。

タグベースの配置用に仮想マシン ストレージ ポリシーを作成

タグベースのルールでは、データストアに割り当てたタグを参照して、仮想マシンの配置に使用するデータストアをフィルタリングすることができます。タグベースの配置を vSphere Client で定義するには、[仮想マシン ストレージ ポリシーの作成] ウィザードを使用します。

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。
- 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 ポリシーの作成] ウィザードを開きます。
 - a [メニュー] - [ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
 - c [仮想マシン ストレージ ポリシーの作成] をクリックします。

- 2 ポリシーの名前と説明を入力して [次へ] をクリックします。

オプション	操作
vCenter Server	vCenter Server インスタンスを選択します。
名前	ストレージ ポリシーの名前を入力します。
説明	ストレージ ポリシーの説明を入力します。

- 3 [データストア固有のルール] の [ポリシー構造] ページで、タグベースの配置ルールを有効にします。
- 4 [タグベースの配置] ページで、タグ ルールを作成します。
 - a [タグ ルールの追加] をクリックし、タグ ベースの配置基準を定義します。次に例を示します。

オプション	例
タグ カテゴリ	サービスのレベル
使用量オプション	以下のタグ付けをされたストレージを使用:
Tags	ゴールド

ゴールド タグ付きのすべてのデータストアが、ストレージの配置先として互換性を持つようになります。

- b (オプション) タグベースのルールを追加します。
- 5 [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ます。
 - 6 [確認して完了] ページでポリシーの設定を確認し、[完了] をクリックします。
設定を変更するには、[戻る] をクリックして関連するページに移動します。

結果

タグ付きのデータストア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。

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 Client で、ストレージ ポリシーに移動します。
 - a [メニュー]-[ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
- 2 ストレージ ポリシーを選択し、次のいずれかのアイコンをクリックします。
 - [設定の編集]
 - [クローン作成]
- 3 (オプション) ポリシーを変更し、[OK] をクリックします。
- 4 仮想マシンが使用するストレージ ポリシーを編集する場合は、その仮想マシンにポリシーを再適用します。

オプション	説明
後で手動で行う	このオプションを選択すると、ストレージ ポリシーに関連付けられたすべての仮想ディスクと仮想マシンのホーム オブジェクトのコンプライアンス状態は期限切れに変更されます。構成とコンプライアンスを更新するには、関連付けられたすべてのエンティティにストレージ ポリシーを手動で再適用します。 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	配置ルール	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	vVols データストア	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	vVols データストア	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 ポリシーのホスト ベースのルール 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、データストア固有のルール 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 Client で、[新規ストレージ ポリシー コンポーネント] ダイアログ ボックスを開きます。
 - a [メニュー]-[ポリシーおよびプロファイル]の順にクリックします。
 - b [ポリシーおよびプロファイル]で、[ストレージ ポリシー コンポーネント]をクリックします。

- 2 [ストレージ ポリシー コンポーネントの作成] 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。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は、そのコンポーネントをストレージ ポリシーのホスト ベースのルールに追加します。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、データストア固有のルール セットに追加されます。

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 Client で、編集またはクローン作成するストレージ ポリシー コンポーネントに移動します。
 - a [メニュー] - [ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[ストレージ ポリシー コンポーネント] をクリックします。

- 2 コンポーネントを選択し、次のいずれかのアイコンをクリックします。

オプション	説明
設定の編集	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	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。

- 3 適切な値を変更し、[OK] をクリックします。
- 4 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 仮想マシンのプロビジョニング プロセスを開始し、次の該当する手順を実行します。
- 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 ポリシーは、その設定に基づいて、すべてのデータストアを互換性があるものとないものに分類します。ポリシーが特定のストレージ エンティティ (vVols 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。
- c vVols 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	vVols 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。

- 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るストレージ ポリシーを選択します。
 - c (オプション) 仮想ディスクのストレージの場所を変更します。
仮想マシン構成ファイルが格納されているデータストア以外のデータストアに仮想ディスクを格納する場合は、このオプションを使用します。
- 4 仮想マシンのプロビジョニング プロセスを完了します。

結果

仮想マシンの作成後は、[サマリ] タブに、割り当てられたストレージ ポリシーとそのコンプライアンス ステータスが表示されます。

次のステップ

構成ファイルまたは仮想ディスクのストレージ配置要件を変える場合は、後で仮想ポリシー割り当てを変更できます。

仮想マシンのファイルとディスク用ストレージ ポリシー割り当ての変更

仮想マシン上のアプリケーションに対するストレージ要件が変わった場合、最初に仮想マシンに適用されたストレージ ポリシーを編集できます。

パワーオフ状態またはパワーオン状態の仮想マシンのストレージ ポリシーを編集できます。

仮想マシン ストレージ ポリシーの割り当てを変更する際、同じストレージ ポリシーを仮想マシン構成ファイルと、そのすべての仮想ディスクに適用できます。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 vSphere Client で、仮想マシンを参照します。
 - a [メニュー]-[ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
 - c 変更するストレージ ポリシーをクリックして、[仮想マシンのコンプライアンス] をクリックします。
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 ポリシーを変更する仮想マシンをクリックします。
- 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	[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。
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 [ディスクごとに設定] オプションをオンにします。 b たとえば、仮想マシン ホーム オブジェクトを選択します。 c [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 vVols 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。
全オブジェクトに対して共通のレプリケーション グループを選択することも、ストレージ オブジェクトごとに異なるレプリケーション グループを選択することもできます。
- 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 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 仮想マシンへ移動します。
- 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 ポリシーのコンプライアンスのチェック] をクリックします。
システムによりコンプライアンスが検証されます。
- 4 コンプライアンスの状態を表示します。

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、ポリシー要件に準拠す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、ポリシー要件に準拠す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。
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、仮想マシンが配置されているデータストアで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。

手順

- 1 仮想マシンのストレージ ポリシーが非準拠の状態であることを確認します。
 - a 仮想マシンへ移動します。
 - b [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] パネルに非準拠状態が表示されます。
- 2 非準拠のストレージ ポリシーに移動します。
 - a [メニュー] - [ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
- 3 非準拠のストレージ ポリシーの互換性のあるデータストアのリストを表示します。
 - a ストレージ ポリシーをクリックします。
 - b [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 仮想マシンへ移動します。
- 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 [仮想マシン ストレージ ポリシーの再適用] 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	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 クラスターの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。たとえば、ホストまたはディスクをクラスターに追加するなどです。その他のリソースがストレージ 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。 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 ポリシーは、データストアで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。

デフォルト ストレージ ポリシー

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。仮想マシンへのストレージ ポリシーの構成と明示的な割り当てを行わない場合、システムはデフォルトのストレージ ポリシーを使用します。

VMware 提供のデフォルト ストレージ ポリシー

ESXi が提供する汎用デフォルト ストレージ ポリシーは、すべてのデータストアに適用され、ストレージ タイプに固有のルールは含まれません。

また、ESXi はオブジェクトベースのデータストア (vSAN または vVols) のデフォルト ストレージ ポリシーも提供します。これらのポリシーにより、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。

vVols のデフォルト ストレージ ポリシーの詳細については、[vVols および仮想マシン ストレージ ポリシー](#)を参照してください。

VMFS および NFS のデータストアには特定のデフォルト ポリシーはなく、汎用デフォルト ポリシーまたはデータストアに対して定義したカスタム ポリシーを使用できます。

ユーザー定義のデフォルト ストレージ ポリシー

vSAN または vVols 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 vVols 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 vVols 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 vVols データストアに一致するように、複数の配置ルール 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す。

仮想マシン ストレージ ポリシーがデータストアのデフォルト ポリシーになると、そのポリシーは、データストアとの関連付けを解除しなければ、削除できません。

データストアのデフォルト ストレージ ポリシーの変更

vVols 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 vVols 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： 複製ルールを含むストレージ ポリシーを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

vVols 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 データストアに移動します。
- 2 [設定] タブをクリックし、[一般] をクリックします。
- 3 [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。
- 4 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 ポリシーがデータストアのデフォルト ポリシーになります。他のポリシーが選択されていない場合、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、このポリシーがシステムによって割り当てられます。

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 vVols 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 プロバイダの管理](#)

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 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。vVols 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。

パーシステンス ストレージ プロバイダとデータ サービス プロバイダの両方が、これらのカテゴリのいずれかに属していることがあります。

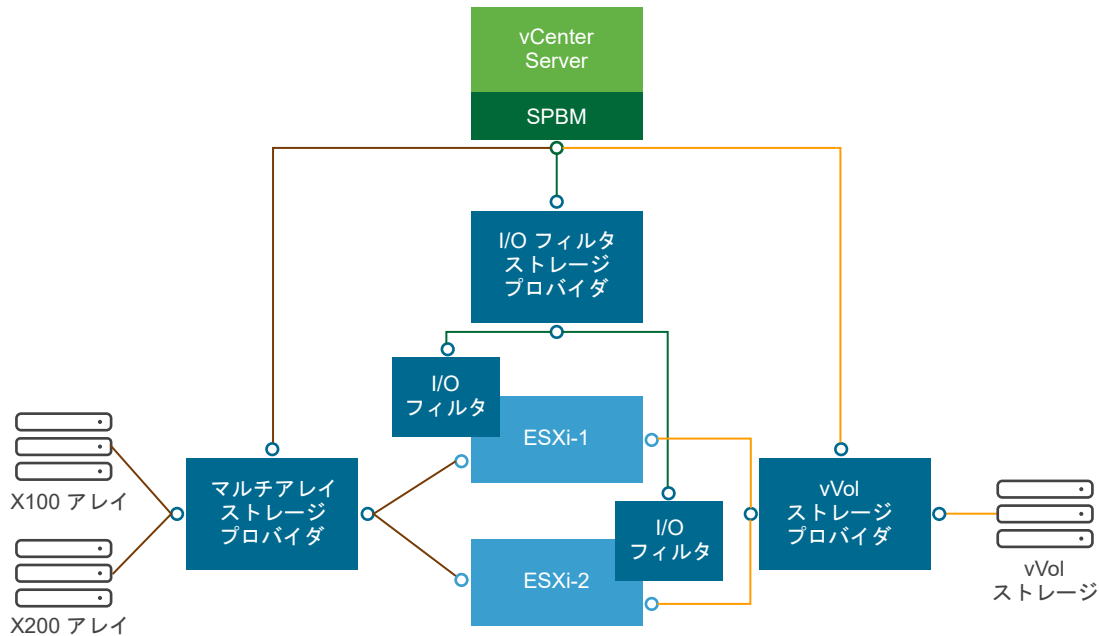
組み込みストレージ プロバイダ

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、vSAN または I/O フィルタをサポートするストレージ プロバイダが組み込まれていて、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、vVols プロバイダなどがあります。vSphere 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、vVols 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 はストレージ プロバイダと通信して、ストレージ プロバイダによって基盤の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 フィルタから収集される情報を取得します。これによって、vCenter Server は vSphere 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、vVols、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、使用できません。

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 vCenter Server に移動します。
- 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 [追加] 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指示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 vCenter Server に移動します。
- 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、プロバイダが表示するストレージ 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。

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 プロバイダの管理

登録されているストレージ プロバイダに対していくつかの管理操作を実行することができます。

手順

- 1 vCenter Server に移動します。
- 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ストレージ プロバイダを選択し、次のアイコンのいずれかをクリックします。

オプション	説明
ストレージ プロバイダの同期	現在の状態で、すべてのストレージ プロバイダと同期します。
再スキャン	プロバイダのストレージ データを更新します。 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 プロバイダがそのときに 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。
削除	使用しないストレージ プロバイダを登録解除します。この操作を実行すると、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。 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。 このオプションは、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にも役立ちます。その場合、プロバイダをいったん登録解除してから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。
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。

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。

VMware vSphere Virtual Volumes (vVol) の操作

22

VMware vSphere Virtual Volumes (vVol) は、物理ハードウェア リソースをキャパシティの論理プールに抽象化して、SAN および NAS デバイスを仮想化します。vVols 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。

- [vVols について](#)
- [vVols の概念](#)
- [vVols とストレージ プロトコル](#)
- [vVols アーキテクチャ](#)
- [vVols および VMware Certificate Authority](#)
- [Virtual Volumes スナップショット](#)
- [vVols を有効にする前に](#)
- [vVols の構成](#)
- [vVols データストア上の仮想マシンのプロビジョニング](#)
- [vVols およびレプリケーション](#)
- [vVols を使用する場合のベスト プラクティス](#)
- [vVols のトラブルシューティング](#)

vVols について

vVols 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。

vVols の機能は、きめ細かな設定を行うのに役立ちます。Virtual Volumes は、これまでにない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。vVols 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。

vVols 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ポリシーを作成することで、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。

vVols の概念

vVols を使用すると、抽象ストレージ コンテナは、LUN または NFS 共有に基づいて従来のストレージ ポリリュームを置き換えます。vCenter Server では、ストレージ コンテナは vVols データストアによって表されます。vVols 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。

vVols 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

(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vvols_part1_concepts)

- **Virtual Volumes オブジェクト**

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。

- **vVols ストレージ プロバイダ**

VASA プロバイダとも呼ばれる vVols 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。

■ vVols 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、vVols 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、vVols 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。

■ vVols データストア

vVols データストアは、vCenter Server および vSphere Client におけるストレージ コンテナです。

■ vVols および仮想マシン ストレージ ポリシー

vVols 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 オブジェクト

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 によって識別されます。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。

Virtual Volumes のタイプ

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 ポリューム。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。

ディスク プロビジョニング

vVols 機能では、仮想ディスクのシン プロビジョニングとシック プロビジョニングの両方の概念がサポートされます。ただし、I/O の観点からは、アレイによるシン プロビジョニングまたはシック プロビジョニングの実装と管理は ESXi ホストに対して透過的です。ESXi は、シン プロビジョニングに関連するすべての機能をストレージ アレイにオフロードします。データ パスでは、ESXi によるシン Virtual Volumes とシック Virtual Volumes の取り扱いの違いはありません。

仮想マシンの作成時に、仮想ディスクのタイプがシンかシックかを選択します。ディスクがシンで vVols データストア上にある場合、後からディスクを拡張することによってタイプを変更することはできません。

共有ディスク

共有ディスクは、vVols に対する SCSI の永続的な予約をサポートする vVols ストレージ上に配置できます。このディスクをクォーラム ディスクとして使用して、MSCS クラスタから RDM を排除することができます。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。

vVols ストレージ プロバイダ

VASA プロバイダとも呼ばれる vVols 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、vVols ストレージのすべての側面の管理に使用されます。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 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、vVols 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。vVols 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。

vVols 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、vVols 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、vVols 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 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 vVols 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 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。

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 vVols 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 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 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 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。

vVols データストア

vVols データストアは、vCenter Server および vSphere 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 vVols データストアとしてマウントする必要があります。vVols 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 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 vVols データストアにマッピングします。作成する vVols 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。

vSphere 管理者の観点からすると、vVols データストアは他のデータストアと似ており、仮想マシンの保持に使用されます。他のデータストアと同様に、vVols 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、vVols 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、vVols データストアには適用されません。vVols データストアの容量は、vSphere の外部のストレージ管理者が構成できます。

従来の VMFS および NFS データストア、および vSAN を使用する vVols データストアを使用できます。

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、vVols 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。vVols 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。

vVols および仮想マシン ストレージ ポリシー

vVols 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、vVols 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 ポリシーを作成するには、vVols ストレージ ポリシー インターフェイスを使用します。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、vVols ストレージの要件準拠が強制されます。

vVols のデフォルト ストレージ ポリシー

vVols 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、vVols 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。このポリシーは、vVols 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、vVols データストアとのみ互換性があります。
- vVols 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。

vVols とストレージ プロトコル

vVols 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。

vVols 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。

vVols および SCSI ベースの転送

ディスク アレイで vVols 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す。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 vVols 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。

vVols 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。vVols 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。

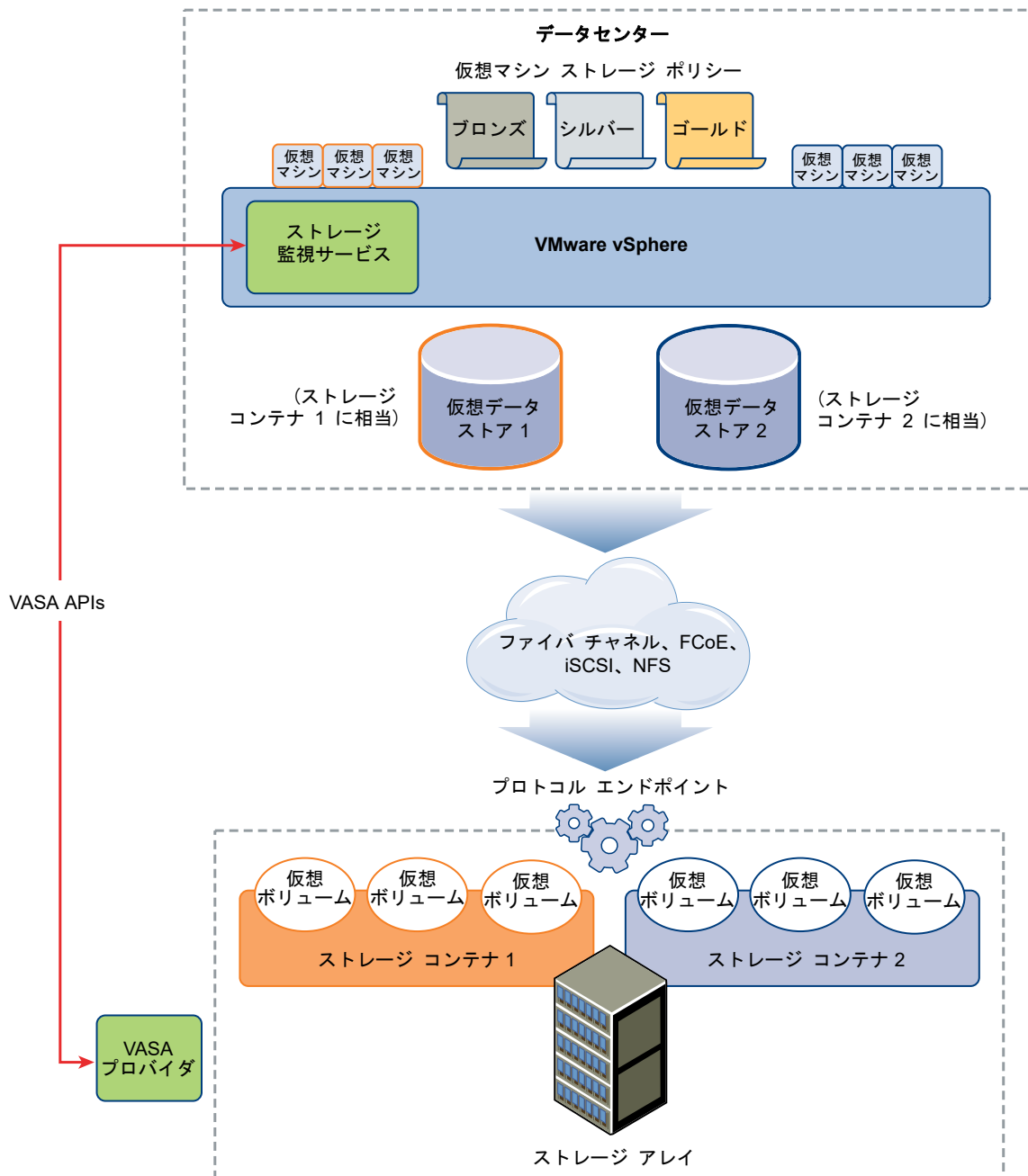
加えて NFS バージョン 4.1 では、ロード バランシングとマルチパスを実現するトランク メカニズムが導入されています。

NAS デバイス上の vVols 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。

vVols アーキテクチャ

アーキテクチャ図には、vVols 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 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 vVols 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、vVols 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。

vVols 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

(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vvols_part2_architecture)

vVols および VMware Certificate Authority

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 vVols 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。

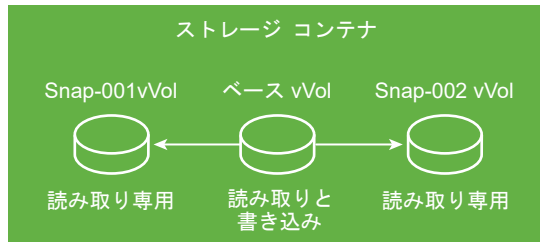
Virtual Volumes スナップショット

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。

vVols 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。

vVols を有効にする前に

vVols 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。

vVols のストレージ システムの準備

vVols 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。

- 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、vVols 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。
- vVols 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 vVols を使用する場合は、レプリケーション構成。[vVols 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、vVols 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

vVols を使用する場合は、Network Time Protocol (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 ホストに移動します。
- 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。

vVols の構成

vVols 環境を構成するには、いくつかの手順を実行します。

前提条件

[vVols を有効にする前](#)のガイドラインに従います。

手順

1 vVols のストレージ プロバイダの登録

vVols 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、vVols を操作できるようにする必要があります。

2 vVols 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、vVols 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 vVols データストアにマッピングした後、vSphere 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、vVols 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、[vVols データストア上の仮想マシンのプロビジョニング](#)および『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。

vVols のストレージ プロバイダの登録

vVols 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、vVols を操作できるようにする必要があります。

登録後、vVols 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、vVols データストアと互換性のある仮想マシン ストレージ ポリシーの作成に使用できます。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 vVols ストレージにプッシュされます。このポリシーにより、vVols 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 vVols 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 vCenter Server に移動します。
- 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 [追加] 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、vVols ストレージ プロバイダを検出して登録します。

vVols 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、vVols データストアを作成します。

手順

- 1 vSphere Client オブジェクト ナビゲータで、ホスト、クラスタ、またはデータセンターを参照します。
- 2 右クリック メニューで [ストレージ] - [新しいデータストア] の順に選択します。

- 3 データストア タイプとして [vVol] を選択します。
- 4 データストアの名前を入力し、ストレージ コンテナのリストから、バックアップ ストレージ コンテナを選択します。
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 vVols 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。
- 5 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。
- 6 設定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

vVols 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。

vVols 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 vVols データストアにマッピングした後、vSphere 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 ホストに移動します。
- 2 [設定] 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 vVols 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 ホストに移動します。
- 2 [設定] 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 ポリシーを選択および設定します。オプションは、使用しているストレージ デバイスのタイプによって異なります。

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。

- SCSI デバイスのパス ポリシーの詳細については、[パス選択プラグインとポリシー](#)を参照してください。
- NVMe デバイスのパス メカニズムの詳細については、[VMware High Performance プラグインとパス選択スキーム](#)を参照してください。

- 7 [OK] をクリックして設定を保存し、ダイアログ ボックスを閉じます。

vVols データストア上の仮想マシンのプロビジョニング

vVols 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： vVols 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。

vVols 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。

手順

- 1 vVols の仮想マシン ストレージ ポリシーを定義します。

vVols 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、vVols 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。

[vVols 用の仮想マシン ストレージ ポリシーの作成](#)を参照してください。

- 2 vVols ストレージ ポリシーを仮想マシンに適用します。

仮想マシンを割り当てるときに、vVols データストアが特定のストレージ要件を満たすようにするには、vVols ストレージ ポリシーを仮想マシンに関連付けます。

[仮想マシンへのストレージ ポリシーの割り当て](#)を参照してください。

3 vVols データストアのデフォルト ストレージ ポリシーを変更します。

VMware では、vVols 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。

[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。

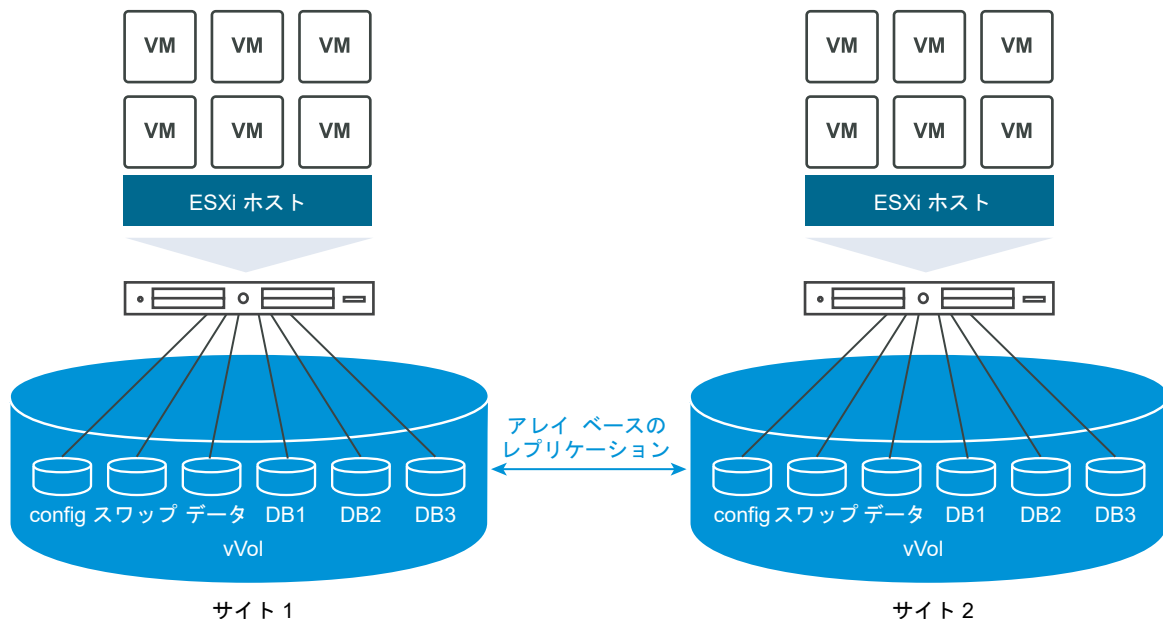
vVols およびレプリケーション

vVols 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。vVols 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。



vVols でのレプリケーションの要件

vVols でレプリケーションを行えるようにする場合は、vVols 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。

vVols の一般的な要件については、[vVols を有効にする前に](#)を参照してください。

ストレージ要件

vVols 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、vVols に対応していなければなりません。
- vVols 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、vVols のレプリケーショングループとフォルトドメインを、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。

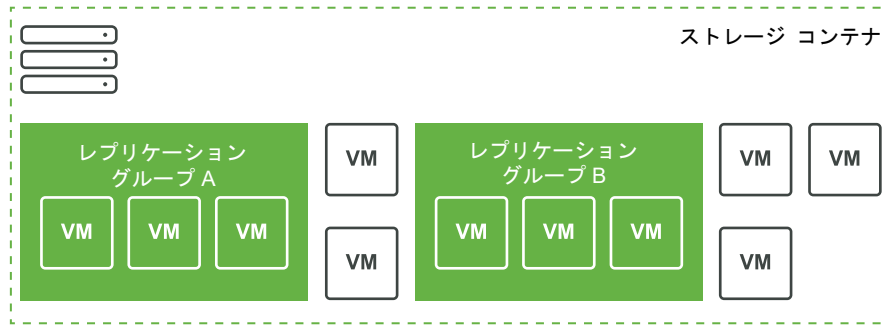
vSphere の要件

- vVols 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 vVols 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、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、vVols 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。

vVols および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。



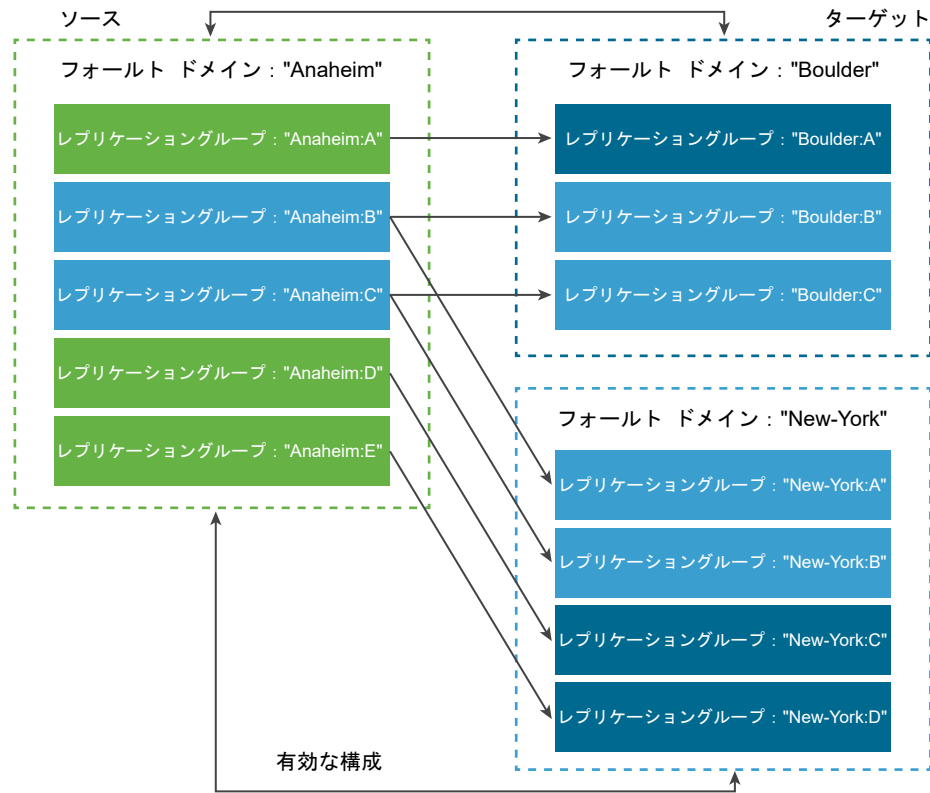
使用できる事前構成済みグループがない場合、vVols は自動オプションを使用できます。自動オプションを使用すると、レプリケーション グループが、vVols によって必要に応じて作成され、プロビジョニング中の vVols オブジェクトに関連付けられます。自動レプリケーション グループを使用すると、そのグループには、仮想マシンのすべてのコンポーネントが割り当てられます。同じ仮想マシンのコンポーネントで、事前構成済みレプリケーション グループと自動レプリケーション グループを混在させることはできません。

vVols およびフォルト ドメイン

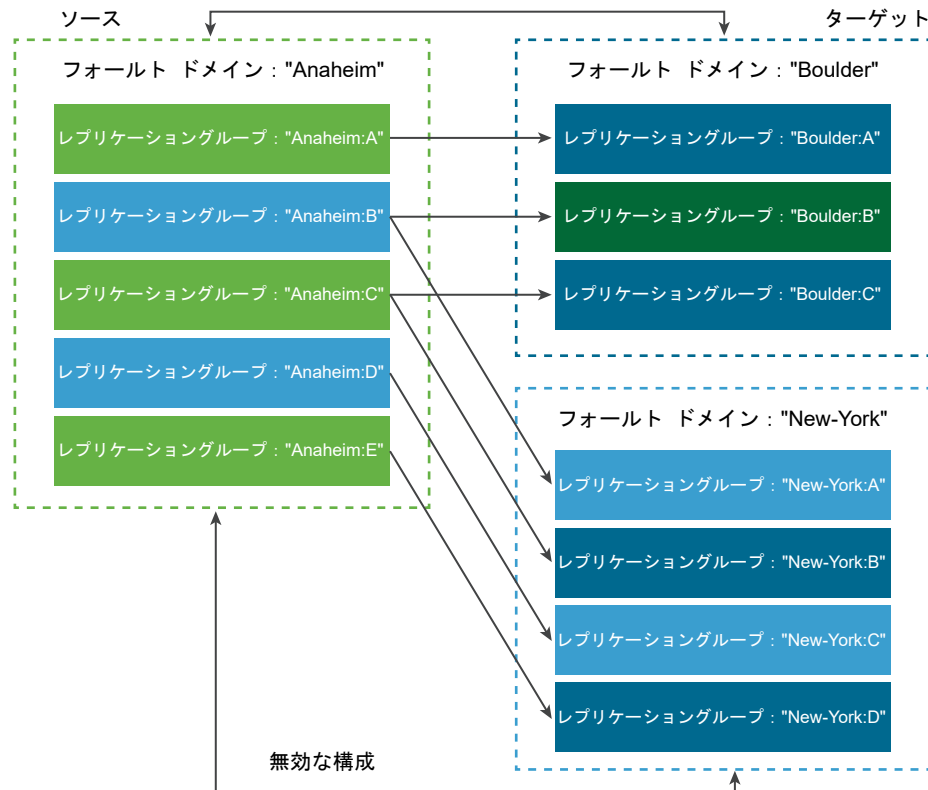
vVols 環境の場合、フォルト ドメインでは、ソースからターゲット サイトへのレプリケート時に特定のレプリケーション グループをどのように組み合わせる必要があるかを定義します。

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 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。



vVols のレプリケーション ワークフロー

vVols 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、vVols 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。ポリシーのデータストアベースのルールには、複製コンポーネントを含める必要があります。[vVols 用の仮想マシン ストレージポリシーの作成](#)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

vVols 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せん。
- 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るながら、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 vVols 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。

vVols を使用する場合のベスト プラクティス

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

- [vVols を使用する場合のガイドラインと制限事項](#)

vVols 機能を最大限活用するには、特定のガイドラインに沿う必要があります。

- [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 vVols アレイ側にプロビジョニングする場合、次のベスト プラクティスを実行してください。

- [vVols パフォーマンスのベスト プラクティス](#)

vVols で最適なパフォーマンス結果を確保するには、次の推奨事項を実行します。

vVols を使用する場合のガイドラインと制限事項

vVols 機能を最大限活用するには、特定のガイドラインに沿う必要があります。

vVols では、次の機能と VMware 製品がサポートされます。

- vVols を使用すると、レプリケーション、暗号化、重複排除、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。vVols 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。
- vVols 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： vVols 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。

- vVols では、vSphere vMotion、Storage vMotion、スナップショット、リンク クローン、DRS などの vSphere 機能がサポートされています。
- vVols 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、vVols 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にします。

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。vVols 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。

vVols の制限事項

vVols を活用するために、次の制限事項を確認してください。

- vVols 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 vVols を使用することはできません。
- vVols 機能は、RDM をサポートしません。
- vVols 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。
- vVols 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 vVols アレイ側にプロビジョニングする場合、次のベスト プラクティスを実行してください。

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ド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。

vVols パフォーマンスのベスト プラクティス

vVols で最適なパフォーマンス結果を確保するには、次の推奨事項を実行します。

個々の仮想ボリューム コンポーネント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、vVols 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せん。

vSphere 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。

[vVols 用の仮想マシン ストレージ ポリシーの作成](#)を参照してください。

vVols でのホスト プロファイルの取得

vVols 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 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.ScsiWolPESNR0 パラメータで制御されます。このパラメータは、vSphere Client の [システムの詳細設定] ページで構成できます。

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 オブジェクト](#)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 vVols 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

vVols 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 vVols 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)。

vVols のトラブルシューティング

このトラブルシューティングのトピックでは、vVols を使用しているときに生じる可能性のある問題への解決策を示します。

- **vVols および esxcli コマンド**

esxcli storage vvol コマンドを使用し、vVols 環境のトラブルシューティングを行うことができます。

- **vVols データストアにアクセスできない**

vVols データストアを作成した後、この仮想データストアにアクセスできないままです。

- **vVols データストアへの仮想マシン移行時または Virtual Volumes データストアへの仮想マシン OVF のデプロイ時の失敗**

仮想マシンを仮想データストアに移行するとき、または仮想マシン OVF を vVols データストアにデプロイするときに、処理が失敗することがあります。

vVols および esxcli コマンド

esxcli storage vvol コマンドを使用し、vVols 環境のトラブルシューティングを行うことができます。

次のコマンド オプションを使用できます。

表 22-1. esxcli storage vvol コマンド

名前空間	コマンド オプション	説明
esxcli storage core device	list	プロトコル エンドポイントを識別します。出力エントリ Is VVOL PE: true は、ストレージ デバイスがプロトコル エンドポイントであることを示します。
esxcli storage vvol daemon	unbindall	ESXi ホストで認識されているすべての VASA プロバイダから、すべての Virtual Volumes のバインドを解除します。
esxcli storage vvol protocolendpoint	list	ホストがアクセスできるすべてのプロトコル エンドポイントを一覧表示します。
esxcli storage vvol storagecontainer	list abandonedvvol scan	使用可能なすべてのストレージ コンテナを一覧表示します。 破棄された Virtual Volumes の指定されたストレージ コンテナをスキャンします。
esxcli storage vvol vasacontext	get	ホストに関連付けられている VASA コンテキスト (VC UUID) を表示します。
esxcli storage vvol vasaprovider	list	ホストに関連付けられているすべてのストレージ (VASA) プロバイダを一覧表示します。

vVols データストアにアクセスできない

vVols データストアを作成した後、この仮想データストアにアクセスできないままです。

問題

vSphere Client で、データストアがアクセス不能と表示されます。このデータストアは仮想マシン プロビジョニングには使用できません。

原因

この問題は、その仮想データストアにマッピングされている SCSI ベースのストレージ コンテナの protocols エンドポイントの構成に失敗すると発生することがあります。従来の LUN と同様に、ESXi ホストから検出できるように SCSI protocols エンドポイントを構成する必要があります。

解決方法

SCSI ベース コンテナ用の仮想データストアを作成する前に、必ずストレージ側に protocols エンドポイントを構成してください。

vVols データストアへの仮想マシン移行時または Virtual Volumes データストアへの仮想マシン OVF のデプロイ時の失敗

仮想マシンを仮想データストアに移行するとき、または仮想マシン OVF を vVols データストアにデプロイするときに、処理が失敗することがあります。

問題

非仮想データストアから移行される OVF テンプレートや仮想マシンには付加的な大サイズのファイル (ISO ディスク イメージ、DVD イメージ、イメージ ファイルなど) が含まれることがあります。これらの付加的なファイルが原因となって構成 Virtual Volumes がその 4GB 制限を超えると、仮想データストアへの移行またはデプロイが失敗します。

原因

構成 Virtual Volumes (config-vVol) には、仮想マシン関連のさまざまなファイルが含まれます。従来の非仮想データストアでは、これらのファイルは仮想マシン ホーム ディレクトリに格納されます。仮想マシン ホーム ディレクトリと同様に、config-vVol には一般に仮想マシン構成ファイル、仮想ディスクおよびスナップショットの記述子ファイル、ログ ファイル、ロック ファイルなどが含まれます。

仮想データストアでは、他の大きなサイズのファイル (仮想ディスク、メモリ スナップショット、スワップ、ダイジェストなど) はすべて別の Virtual Volumes に格納されます。

config-vVol は 4 GB Virtual Volumes として作成されます。config-vVol の一般的なコンテンツは、通常、この 4 GB 割り当てのうちのごくわずかな量しか使用しません。このため、バックアップ容量を節約する処置として、config-vVol は一般にシン プロビジョニングされます。ISO ディスク イメージ、DVD イメージ、イメージ ファイルなどの大きなサイズのファイルが他に存在すると、config-vVol がその 4 GB 制限を超える可能性があります。このようなファイルが OVF テンプレートに含まれている場合、vVols ストレージへの仮想マシン OVF のデプロイが失敗します。このようなファイルが既存の仮想マシンの一部である場合、従来のデータストアから vVols ストレージへの仮想マシンの移行も失敗します。

解決方法

- 仮想マシン移行の場合。従来のデータストアから仮想データストアに仮想マシンを移行する前に、仮想マシン ホーム ディレクトリから過剰なコンテンツを削除し、config-vVol を 4 GB 限度未満になるようにします。
- OVF デプロイの場合。過剰ファイルを含む OVF テンプレートは仮想データストアに直接デプロイすることは不可能なため、まず仮想マシンを非仮想データストアにデプロイします。仮想マシン ホーム ディレクトリから過剰コンテンツを削除し、量が少なくなった仮想マシンを vVols ストレージに移行します。

仮想マシン I/O のフィルタリング

23

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](#)
- [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 インストール失敗の処理](#)

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
- 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 フィルタリングの基本的なコンポーネントは次のとおりです。

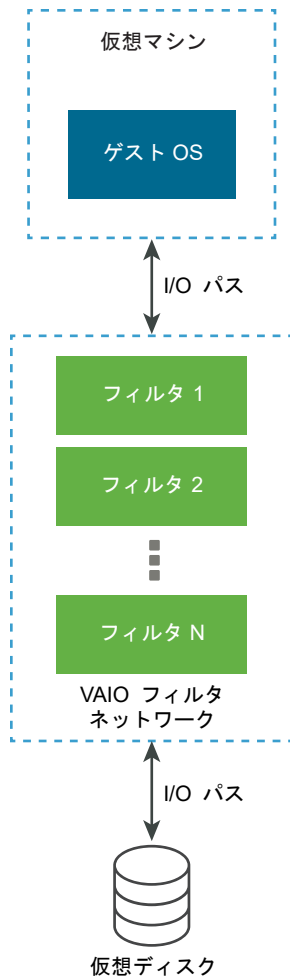
VAIO フィルタ ネットワーク ユーザー環境と ESXi によって提供される VMkernel インフラストラクチャの組み合わせです。このフレームワークを使用して、仮想ディスクとの間の I/O パスにフィルタ プラグインを追加できます。インフラストラクチャには I/O フィルタ ストレージ プロバイダ (VASA プロバイダ) が含まれています。プロバイダは、スト

レイジ 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。VMware パートナーが I/O フィルタを開発した場合、フィルタにはその構成と管理に役立つ追加のオプションのコンポーネントが含まれることがあります。

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に対して 2 つ以上のフィルタを操作できますが、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。

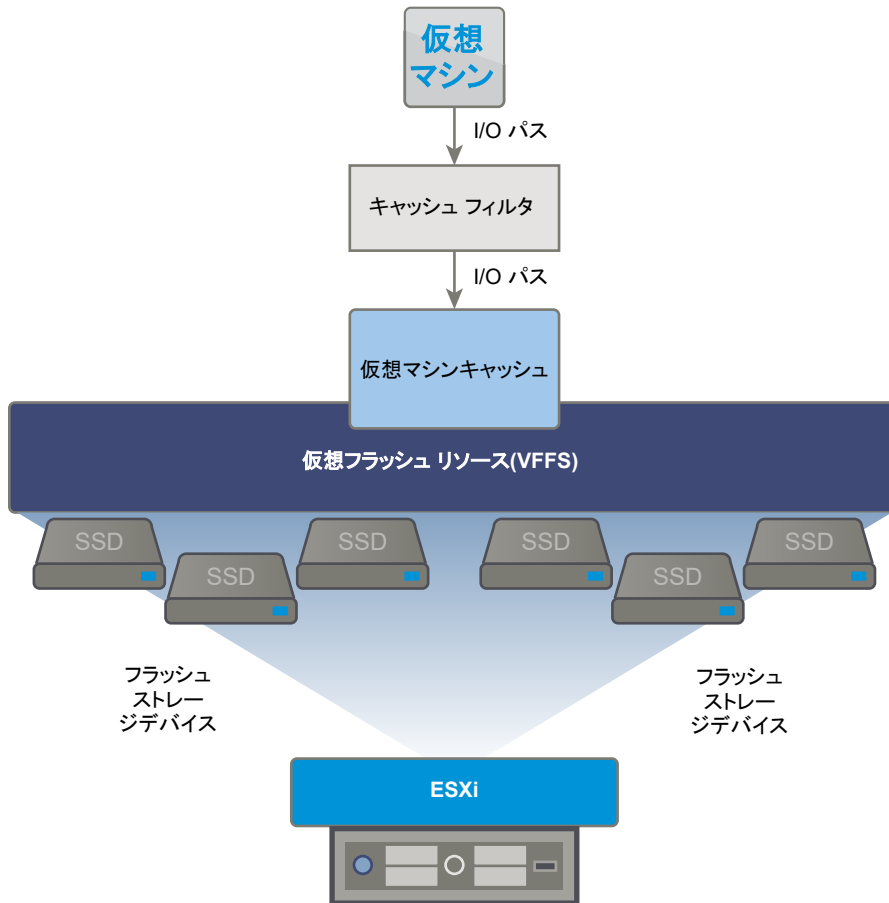
I/O フィルタのストレージ プロバイダは、vSphere によって提供されるソフトウェア コンポーネントです。ストレージ プロバイダは、I/O フィルタや、I/O フィルタが vCenter Server に対してサポートするレポート データ サービス機能と統合されます。

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。

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。
- サードパーティによって提供された I/O フィルタの詳細については、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。

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 デーモン、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せん。

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 vCenter Server に移動します。
- 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	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 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。

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、フィルタをアクティブ化する前に、ESXi ホスト上で仮想フラッシュ リソースを設定します。[仮想フラッシュ リソースの設定](#)を参照してください。

手順

1 I/O フィルタ サービスに基づいて仮想マシン ポリシーを定義します。

I/O フィルタから提供されるデータ サービスが、仮想マシン ポリシーにリストされていることを確認します。

[ホストベースのデータ サービスの仮想マシン ストレージ ポリシーの作成](#)を参照してください。

2 仮想マシンに I/O フィルタ ポリシーを割り当てます。

I/O フィルタから提供されるデータ サービスを有効にするには、I/O フィルタ ポリシーを仮想ディスクに関連付けます。ポリシーは、仮想マシンのプロビジョニング時に割り当てることができます。

[仮想マシンへの I/O フィルタ ポリシーの割り当て](#)を参照してください。

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。

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 仮想マシンのプロビジョニング プロセスを開始し、次の該当する手順を実行します。
- 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 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。

- 2 ESXi ホストから I/O フィルタ コンポーネントが確実にアンインストールされたことを確認します。

esxcli software vib list

アンインストールしたフィルタは今後リストに表示されなくなります。

クラスタでの I/O フィルタのアップグレード

I/O フィルタ ベンダーから提供されたインストーラを使用して、ESXi ホスト クラスタにデプロイされた I/O フィルタをアップグレードします。

アップグレードは、古いフィルタ コンポーネントのアンインストールと、新しいフィルタ コンポーネントとの置き換えで構成されています。インストールがアップグレードであるかどうかを判断するために、vCenter Server により、既存のフィルタの名前とバージョンがチェックされます。既存のフィルタ名が新しいフィルタ名と一致するが、バージョンが異なる場合、インストールがアップグレードだとみなされます。

前提条件

- 必要な権限：ホスト.構成.パッチ。

手順

- 1 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。

- 2 ESXi ホストから I/O フィルタ コンポーネントが確実にアンインストールされたことを確認します。

esxcli 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、vVols、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。
- 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 vVols 間のように、タイプの異なるデータストア間での移行が必要になる場合があります。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 vVols 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。
- vVols 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。

I/O フィルタ インストール失敗の処理

一般に、クラスタ内のすべての ESXi ホストには、同じ I/O フィルタ セットがインストールされています。インストール中にエラーが発生することがあります。

ホスト上で I/O フィルタのインストールに失敗すると、その失敗をレポートするイベントが生成されます。さらに、ホストのアラームで失敗の原因が示されます。失敗例として、次のようなものがあります。

- ホストから VIB URL にアクセスできない。
- VIB の形式が無効である。
- VIB で、アップグレードまたはアンインストールのためにホストをメンテナンス モードにする必要がある。
- VIB では、インストールまたはアンインストール後にホストを再起動する必要がある。
- 仮想マシンをホストから退避できないため、ホストをメンテナンス モードにしようとして失敗した。
- VIB の手動インストールまたはアンインストールが必要である。

vCenter Server は、一部の失敗を解決できます。他の失敗については、ユーザーの介入が必要になる場合があります。たとえば、VIB URL を編集したり、仮想マシンを手動で退避またはパワーオフしたり、VIB を手動でインストールまたはアンインストールする必要があります。

単一の ESXi ホストへの I/O フィルタのインストール

トラブルシューティング目的のために、I/O フィルタの ESXi コンポーネント（VIB ファイルとしてパッケージ化されている）をダウンロードして、ESXi ホストにインストールできます。esxcli コマンドを使用して、VIB ファイルをインストールします。

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。ESXCLI 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 VIB をインストールします。

```
esxcli software vib install --depot path_to_VMware_vib_ZIP_file
```

install コマンドのオプションを使用して、ドライ ラン、特定の VIB の指定、許容レベル検証のバイパスなどを行うことができます。本番システムでは検証をバイパスしないでください。『ESXCLI のリファレンス』ドキュメントを参照してください。

- 2 VIB が ESXi ホストにインストールされていることを確認します。

```
esxcli software vib list
```

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とサポートし、適切な認定を受けていることも必要です。中間アプライアンスはストレージ仮想化アプライアンス、I/O アクセラレーションアプライアンス、暗号化アプライアンスなどがあります。

ハードウェア アクセラレーションのサポート ステータス

vSphere 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** とも呼ばれます。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)** とも呼ばれています。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 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 ホストに移動します。
- 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、『ESXCLI 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。

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。ESXCLI 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 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 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 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。

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。ESXCLI 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 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 storage core device list -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
Multipath Plugin: NMP
XXXXXXXXXXXXXXXXX
Attached Filters: VAAI_FILTER
VAAI Status: supported
XXXXXXXXXXXXXXXXX
```

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。

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。ESXCLI 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 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 storage core device vaai status get -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
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 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 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 storage core claimrule list --claimrule-class=Filter
Rule Class Rule Class Type Plugin Matches XCOPY Use Array
Reported Values XCOPY Use Multiple Segments XCOPY Max Transfer Size KiB
Filter 65430 runtime vendor VAAI_FILTER vendor=EMC
model=SYMMETRIX False
False 0
Filter 65430 file vendor VAAI_FILTER vendor=EMC
model=SYMMETRIX False
False 0
Filter 65431 runtime vendor VAAI_FILTER vendor=DGC
model=* False
False 0
Filter 65431 file vendor VAAI_FILTER vendor=DGC
model=* False
False 0
```

- 2 VAAI プラグイン要求ルールをリスト表示するには、

esxcli 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 storage core claimrule list --claimrule-class=VAAI
Rule Class Rule Class Type Plugin Matches XCOPY Use Array
Reported Values XCOPY Use Multiple Segments XCOPY Max Transfer Size KiB
VAAI 65430 runtime vendor VMW_VAAIP_SYMM vendor=EMC
model=SYMMETRIX False
False 0
VAAI 65430 file vendor VMW_VAAIP_SYMM vendor=EMC
model=SYMMETRIX False
False 0
VAAI 65431 runtime vendor VMW_VAAIP_CX vendor=DGC
model=* False
False 0
VAAI 65431 file vendor VMW_VAAIP_CX vendor=DGC
model=* False
False 0
```

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。

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。ESXCLI 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 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 storage core claimrule add --claimrule-class=VAAI` コマンドを実行して、VAAI プラグイン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 storage core claimrule load --claimrule-class=Filter
```

```
esxcli storage core claimrule load --claimrule-class=VAAI
```

4 `esxcli 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 storage core claimrule add --claimrule-class=Filter --plugin=VAAI_FILTER --type=vendor --vendor=IBM --autoassign
```

```
# esxcli storage core claimrule add --claimrule-class=VAAI --plugin=VMW_VAAIP_T10 --type=vendor --vendor=IBM --autoassign
```

```
# esxcli storage core claimrule load --claimrule-class=Filter
```

```
# esxcli storage core claimrule load --claimrule-class=VAAI
```

```
# esxcli storage core claimrule run --claimrule-class=Filter
```

XCOPY パラメータの構成

XCOPY は、ストレージ アレイにタスクをオフロードするために使用される VAAI プリミティブの 1 つです。たとえば、タスクを実行するために vSphere リソースを使用するのではなく、アレイに対する仮想マシンの移行やクローン作成などの操作の負荷を軽減するのに XCOPY を使用できます。

すべてのストレージ アレイを備えた XCOPY メカニズムを使用できます。このメカニズムは、VMware が開発した SCSI T10 ベースの VMW_VAAIP_T10 プラグインです。XCOPY メカニズムを有効にするには、VAAI クラスの要求ルールを作成します。

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。ESXCLI 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

- ◆ 次のコマンドを使用して、XCOPY オプションを入力します。

```
esxcli storage core claimrule add --claimrule-class=VAAI
```

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。

オプション	説明
<code>-a --xcopy-use-array-values</code>	XCOPY コマンドに、アレイからレポートされた値を使用します。
<code>-s --xcopy-use-multi-segs</code>	XCOPY コマンドで複数セグメントを使用します。--xcopy-use-array-values が指定されている場合にのみ有効です。
<code>-m --xcopy-max-transfer-size</code>	アレイからレポートされた値とは異なる転送サイズを使用する場合の、XCOPY コマンドの最大転送サイズ (MB)。--xcopy-use-array-values が指定されている場合にのみ有効です。
<code>-k --xcopy-max-transfer-size-kib</code>	アレイからレポートされた値とは異なる転送サイズを使用する場合の、XCOPY コマンドの最大転送サイズ (KB)。--xcopy-use-array-values が指定されている場合にのみ有効です。

例：XCOPY の構成

- ```
esxcli storage core claimrule add -r 914 -t vendor -V XtremIO -M XtremApp -P VMW_VAAIP_T10 -c VAAI -a -s -k 64
```
- ```
# esxcli storage core claimrule add -r 65430 -t vendor -V EMC -M SYMMETRIX -P VMW_VAAIP_SYMM -c VAAI -a -s -m 200
```

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の削除します。

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。ESXCLI 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 storage core claimrule remove -r claimrule_ID --claimrule-class=Filter
```

```
esxcli 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、容量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容量を予約するように NAS デバイスに指示さ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。

- アレイベースのスナップショット。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。

注： Storage DRS は、NFS データストア上のアレイベースのスナップショットを検出しません。その結果、アレイベースのスナップショットを使用して仮想マシンのクローン作成などの操作を実行すると、Storage DRS からは推奨が提供されません。

- 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 Lifecycle Manager が含まれています。詳細については、『ESXi のアップグレード』および『ホストとクラスタのライフサイクルの管理』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。

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。ESXCLI 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 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 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 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。

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。ESXCLI 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 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 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。

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。ESXCLI 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 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 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。

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。ESXCLI 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 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、ハードウェア アクセラレーションがサポートされているかどうかを示されます。

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 Client で作成されたすべてのデータストアは自動的に整列されます。
- VMFS には複数の LUN またはエクステンツがあり、これらは異なるアレイにあります。

同じ VMFS データストア内であっても、アレイ間でのハードウェアのクローン作成は機能しません。

ストレージ プロビジョニングと容量の再利用

25

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。

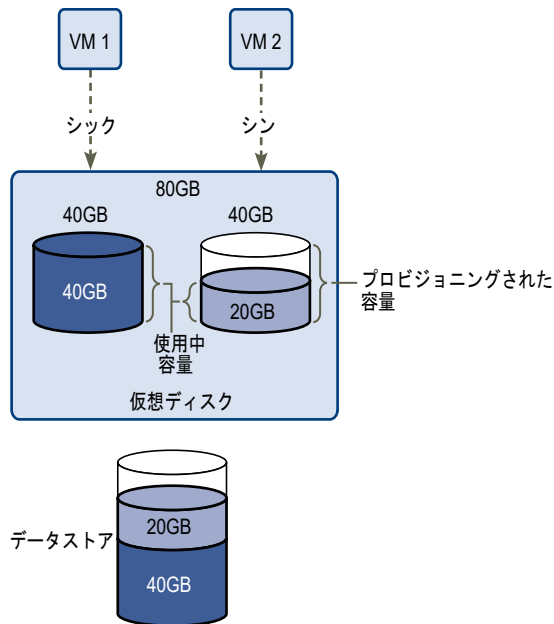
- [仮想ディスク シン プロビジョニング](#)
- [ESXi とアレイ シン プロビジョニング](#)
- [ストレージ容量の再利用](#)

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。Eager Zeroed シック仮想ディスクのサイズを増やすと、仮想マシンのサスペンド時間が著しく長くなることがあります。

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 仮想マシンを作成します。
 - a 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。
 - b [新規仮想マシンの作成] を選択し、[次へ] をクリックします。
 - c 仮想マシンの作成に必要な手順すべてを実行します。
- 2 シン仮想ディスクを設定します。
 - a [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。
 - b [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。
 - c （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。
 - d 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。
- 3 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。

手順

- 1 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。

結果

[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。

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 仮想マシンを右クリックし、[設定の編集] を選択します。
- 2 [仮想ハードウェア] タブをクリックします。
- 3 [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、フォーマットをシックに変更できます。

データストア ブラウザを使用して、シン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 仮想マシンへ移動します。
 - 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 データストアを右クリックし、[ファイルの参照] を選択します。
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 ファイルを選択し、[拡張] をクリックします。

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 T10unmap 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 以降
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 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。

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。ESXCLI 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 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 storage core device list -d naa.XXXXXXXXXXX4c
naa.XXXXXXXXXXX4c
Display Name: XXXX Fibre Channel Disk(naa.XXXXXXXXXXX4c)
Size: 20480
Device Type: Direct-Access
Multipath Plugin: NMP
-----
Thin Provisioning Status: yes
-----
```

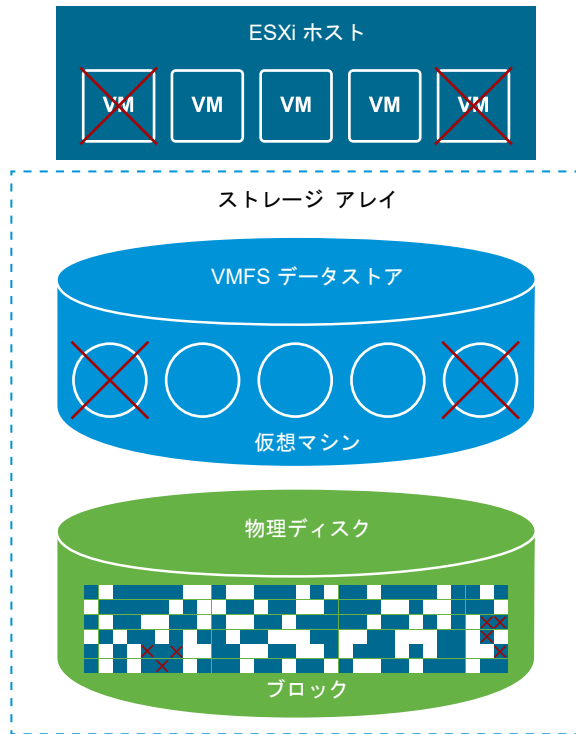
不明なステータスは、ストレージ デバイスがシックであることを示します。

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 ハ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。



VMFS の容量の再利用

(http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_space_reclamation_vmfs)

■ 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、バッキング アレイ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 パフォーマンスが影響を受けることはありません。

VMFS6 データストアでは、次の容量再利用の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。ESXi は、マッピング解除の推奨精度が 1 MB 以上（16 MB など）のアレイでの自動マッピング解除処理をサポートします。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 KB、64 KB などです。

容量の再利用方法

この方法には、優先度方式または固定方式を指定できます。優先度方式を使用する場合は、優先度を設定します。固定方式を使用する場合は、1 秒あたりのバンド幅を MB で指定する必要があります。

容量再利用の優先度

このパラメータは、優先度方式で容量再利用方法を使用する場合の処理の実行速度を定義します。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 の場合は、次のいずれかのオプションを指定できます。

容量再利用の優先度	説明	構成
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。	vSphere Client esxcli コマンド
低（デフォルト）	<code>unmap</code> コマンドを低頻度（1 秒あたり 25 ~ 50 MB）で送信します。	vSphere Client esxcli コマンド

容量再利用の		
優先度	説明	構成
中	コマンドを低速の 2 倍の速度 (1 秒あたり 50 ~100 MB) で送信します。	esxcli コマンド
高	コマンドを低速の 3 倍の速度 (1 秒あたり 100 MB 以上) で送信します。	esxcli コマンド

注： バージョン 6.5 の ESXi ホストは、優先度の中および高を認識しません。仮想マシンをホスト バージョン 6.5 に移行した場合、優先度のデフォルトは低になります。

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。

VMFS6 データストアの作成時に容量の再利用に使用できるのは、優先度方式のみです。固定方法を使用するには、既存のデータストアの容量再利用の設定を編集します。

手順

- 1 vSphere Client オブジェクト ナビゲータで、ホスト、クラスタ、またはデータセンターを参照します。
- 2 右クリック メニューで [ストレージ] - [新しいデータストア] の順に選択します。
- 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。

パラメータは、精度、および容量再利用の操作が実行される優先度を定義します。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)。容量の再利用に優先度方式を使用します。低優先度でのマッピング解除操作を有効にします。 ■ 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。

注： vSphere Client で容量再利用の優先度に使用できる設定は、[低] および [なし] です。[中] または [高] の設定を変更するには、esxcli コマンドを使用します。[容量再利用パラメータの ESXCLI コマンドを使用した変更](#)を参照してください。

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。

容量再利用の設定の変更

vSphere Client で VMFS6 データストアを作成する場合、容量の再利用方法として、優先度方式のみを指定できます。固定方式を有効にするには、既存のデータストアの容量再利用の設定を変更します。

手順

- 1 データストアに移動します。
- 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指定します。

オプション	説明
固定の再利用率で、容量の自動再利用を有効にする	容量の再利用に固定方式を使用します。再利用のバンド幅を 1 秒あたりの MB で指定します。
容量の自動再利用を無効にする	削除またはマッピング解除されたブロックは再利用されません。

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。

容量再利用パラメータの ESXCLI コマンドを使用した変更

デフォルトの容量再利用の優先度、精度、およびその他のパラメータを変更できます。

手順

- ◆ 次のコマンドを使用して、容量再利用のパラメータを設定します。

```
esxcli storage vmfs reclaim config set
```

このコマンドには次のオプションがあります。

オプション	説明
-b --reclaim-bandwidth	容量再利用の固定バンド幅 (1 秒あたりの MB)。
-g --reclaim-granularity	容量の自動再利用の最小精度 (バイト数)。
-m --reclaim-method	容量の自動再利用の方法。サポートされているオプション： <ul style="list-style-type: none"> ■ priority (優先度) ■ 固定
-p --reclaim-priority	容量の自動再利用の優先度。サポートされているオプション： <ul style="list-style-type: none"> ■ none ■ low (低) ■ medium (中) ■ high (高)
-l --volume-label	ターゲット VMFS ボリュームのラベル。
-u --volume-uuid	ターゲット VMFS ボリュームの UUID。

例：再利用方法を固定に設定

再利用方法を固定に設定して、レートを 1 秒あたり 100 MB に設定するには、次の例を使用します。

```
esxcli storage vmfs reclaim config set --volume-label datastore_name --reclaim-method fixed -b 100
```

容量自動再利用の設定の確認

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した後に、その設定内容を確認できます。

手順

- 1 vSphere Client の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。

esxcli コマンドを使用して値を設定した場合（容量再利用の優先度の中または高を設定した場合など）は、これらの値も vSphere Client に表示されます。

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。

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。ESXCLI 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 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
<i>-l --volume-label=volume_label</i>	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、 <i>-u --volume-uuid=volume_uuid</i> は使用しないでください。
<i>-u --volume-uuid=volume_uuid</i>	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、 <i>-l --volume-label=volume_label</i> は使用しないでください。
<i>-n --reclaim-unit=number</i>	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。

- 2 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 で容量の再利用を使用する際には、次の考慮事項が適用されます。

- 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。
- デフォルトの SeSparse フォーマットのスナップショットのある仮想マシンについては、VMFS6 は、ESXi ホストバージョン 6.7 以降でのみ、容量の自動再利用をサポートします。

容量の再利用は最上位のスナップショットにのみ影響し、仮想マシンをパワーオンするときに機能します。

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。

クラウド ネイティブ ストレージの導入方法

26

クラウド ネイティブ ストレージは、ステートフル アプリケーション向けの包括的なデータ管理を実現するソリューションです。クラウド ネイティブ ストレージを使用すると、再起動後や停止後にも状態を維持可能なコンテナ化されたステートフル アプリケーションを作成できます。ステートフル コンテナは、標準ボリューム、パーシステントボリューム、動的プロビジョニングなどのプリミティブを使用しながら、vSphere によって公開されるストレージを利用します。

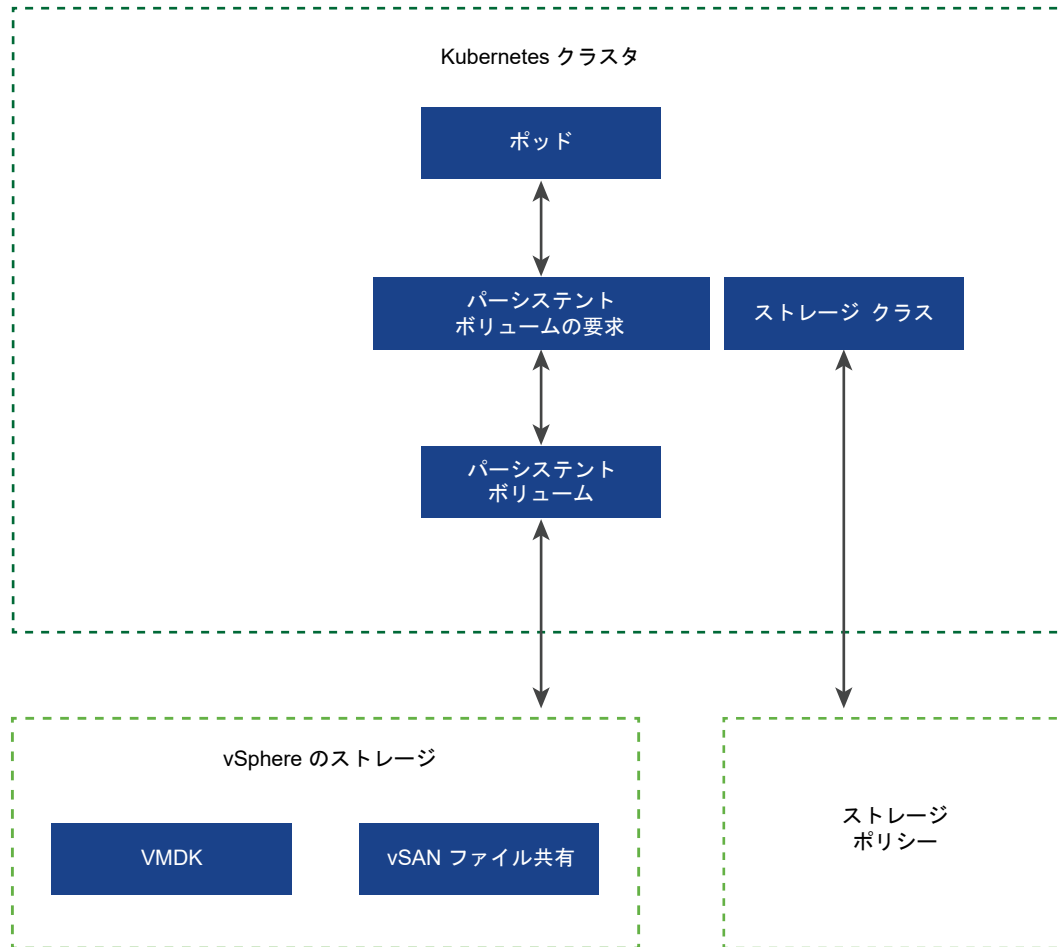
クラウド ネイティブ ストレージを使用すると、仮想マシンとコンテナ ライフサイクルに依存しないパーシステントコンテナ ボリュームを作成できます。vSphere ストレージはボリュームをバックアップするので、ボリューム上で直接ストレージ ポリシーを設定できます。ボリュームを作成したら、それらのボリュームと vSphere Client でバックアップされているストレージ オブジェクトを確認し、ストレージ ポリシー コンプライアンスを監視できます。

この章には、次のトピックが含まれています。

- [クラウド ネイティブ ストレージの概念と用語](#)
- [vSphere 管理者向けのクラウド ネイティブ ストレージ](#)

クラウド ネイティブ ストレージの概念と用語

vSphere クラウド ネイティブ ストレージ環境について重要ないくつかの概念を理解しておきます。



Kubernetes クラスタ

Kubernetes マスターおよびワーカーサービスが実行されている仮想マシンのクラスタ。Kubernetes クラスタの上部で、コンテナ化されたアプリケーションを展開します。アプリケーションには、ステートフルまたはステートレスのいずれかの状態があります。

ポッド

ポッドは、ストレージやネットワークなどのリソースを共有する 1 つ以上のコンテナ化されたアプリケーションのグループです。ポッド内のコンテナは、グループとして開始、停止、および複製されます。

コンテナ Orchestrator

ホストのクラスタ間でコンテナ化されたアプリケーションを展開、拡張、および管理するための Kubernetes などのオープンソース プラットフォーム。プラットフォームは、コンテナを中心としたインフラストラクチャを提供します。

ステートフル アプリケーション

コンテナ アプリケーションがステートレスからステートフルに発展すると、永続的なストレージが必要になります。セッション間でデータを保存しないステートレスアプリケーションとは異なり、ステートフル アプリケーションはデータを永続的なストレージに保存します。保持されたデータは、アプリケーションの状態と呼ばれます。後でデータを取得し、次のセッションで使用することができます。ほとんどのアプリケーションはステートフルです。データベースは、ステートフル アプリケーションの一例です。

PersistentVolume

ステートフル アプリケーションは、**PersistentVolumes** を使用してデータを保存します。**PersistentVolume** は、その状態とデータを保持できる Kubernetes ポリリュームです。ポッドからは独立しており、ポッドが削除または再構成されても引き続き存在できます。vSphere 環境では、**PersistentVolume** オブジェクトは vSphere の **First Class Disk (FCD)** タイプの仮想ディスク または vSAN ファイル共有をバックアップ ストレージとして使用します。

- 仮想ディスクは、**ReadWriteOnce** としてマウントされたポリリュームをサポートします。これらのポリリュームは、Kubernetes の単一ポッドでのみ使用できます。

vSphere 7.0 以降では、vSphere 暗号化テクノロジーを使用して、パーシステント ポリリュームをバックアップする FCD 仮想ディスクを保護することができます。詳細については、『[Cloud Native Storage での暗号化の使用](#)』を参照してください。

- vSAN ファイル共有は、多くのノードでマウントされている **ReadWriteMany** ポリリュームをサポートします。これらのポリリュームは、複数のポッド間、または Kubernetes ノードや Kubernetes クラスタで実行されているアプリケーション間で共有できます。ファイル共有で可能な構成の詳細については、[ファイル ポリリュームのプロビジョニング](#)を参照してください。

StorageClass

Kubernetes は、**StorageClass** を使用して、ストレージのさまざまな階層を定義し、**PersistentVolume** をバックアップするストレージの各種要件を記述します。vSphere 環境では、ストレージ クラスをストレージ ポリシーにリンクできます。vSphere 管理者は、さまざまなストレージ要件を記述したストレージ ポリシーを作成します。仮想マシン ストレージ ポリシーは、動的ポリリューム プロビジョニングの **StorageClass** 定義の一部として使用されます。

次のサンプルの YAML ファイルは、以前に vSphere Client を使用して作成した **Gold** ストレージ ポリシーを示しています。作成されたパーシステント ポリリューム VMDK は、**Gold** ストレージ ポリシー要件を満たす、互換性のあるデータストアに配置されます。

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: gold-sc
  annotations:
    storageclass.kubernetes.io/is-default-class: "true"
provisioner: csi.vsphere.vmware.com
parameters:
  storagepolicyname: "Gold"
```

PersistentVolumeClaim

通常、アプリケーションまたはポッドは **PersistentVolumeClaim** を介して永続的なストレージを要求できます。**PersistentVolumeClaim** は、タイプ、ストレージのクラス、アクセス モード (**ReadWriteOnce** または **ReadWriteMany**)、または

PersistentVolume のその他のパラメータを指定します。その後、要求によって、対応する PersistentVolume オブジェクトと、基盤となる 仮想ディスク または vSAN ファイル共有 が vSphere 環境で動的にプロビジョニングされます。

要求が作成されると、PersistentVolume が自動的に要求にバインドされます。ポッドは、要求を使用して PersistentVolume とアクセス ストレージをマウントします。

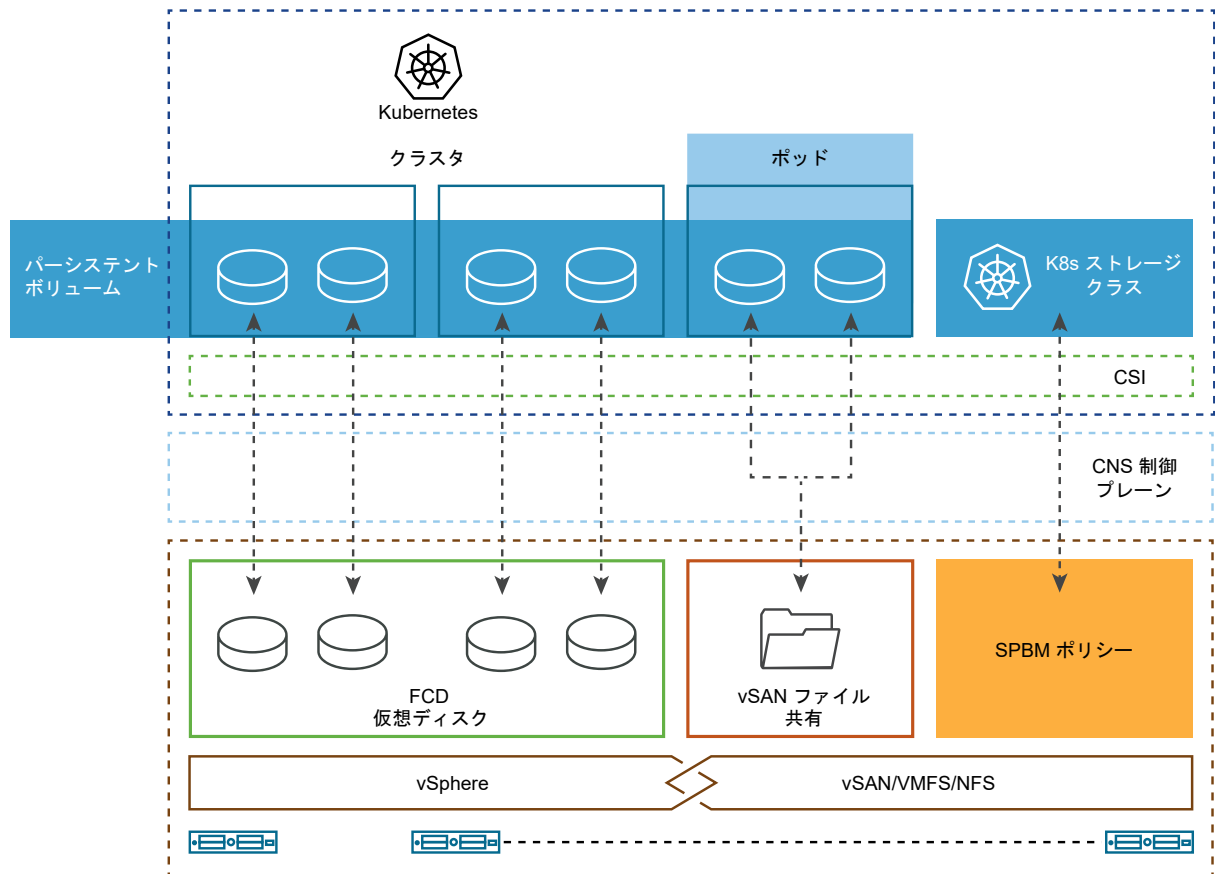
この要求を削除すると、対応する PersistentVolume オブジェクトおよび基盤となるストレージが削除されます。

```
kind: PersistentVolumeClaim
metadata:
  name: persistent-VMDK
spec:
  accessModes:
  - ReadWriteOnce
  resources:
  requests:
  storage: 5Gi
  storageClassName: gold-sc
```

クラウド ネイティブ ストレージコンポーネント

クラウド ネイティブ ストレージはいくつかのコンポーネントを使用して、vSphere ストレージと統合します。

次の図は、これらのコンポーネントの相互関係を示しています。



Kubernetes クラスタ

クラウド ネイティブ ストレージ環境では、Kubernetes クラスタは vSphere に展開された仮想マシンのクラスタまたはノードです。Kubernetes ユーザーは、クラスタと直接対話して、クラスタの上にステートフル アプリケーションを展開します。

vSphere のコンテナ ストレージ インターフェイス (CSI)

基盤となるインフラストラクチャ リソースを使用するには、クラスタに CSI ドライバが必要です。

vSphere CSI は、Kubernetes などのコンテナ Orchestrator 上のコンテナ化されたワークロードに vSphere ストレージを公開する、ツリー外のプラグインです。このプラグインにより、vSAN など各種の vSphere ストレージが有効になります。

vSphere CSI は、すべてのストレージ プロビジョニング操作で vCenter Server の CNS 制御プレーンと通信します。vSphere CSI では、以下の機能がサポートされます。

- コンテナ ボリュームの動的プロビジョニング。
- vSphere First Class Disk 機能。
- Kubernetes ゾーン。

- 従来型のマウントと raw マウント。
- 単一の vCenter Server、および複数のデータセンターとクラスタ。
- 複数のデータストアまたはデータストア クラスタからのプロビジョニング。

Kubernetes では、CSI ドライバが、ツリー外の vSphere クラウド プロバイダ インターフェイス (CPI) とともに使用されます。CSI ドライバはコンテナ イメージとして出荷されるため、クラスタ管理者がデプロイする必要があります。詳細については、[Deploying a Kubernetes Cluster on vSphere with CSI and CPI](#) セクション ([Kubernetes vSphere Cloud Provider](#) ドキュメント) を GitHub で参照してください。

クラウド ネイティブストレージサーバ コンポーネント

CNS サーバ コンポーネント、または CNS 制御プレーンは vCenter Server に配置されます。これは、コンテナ ポリ्यूームのプロビジョニングとライフサイクルの操作を実装する vCenter Server 管理の拡張機能です。

コンテナ ポリ्यूームをプロビジョニングするときに、First Class Disk 機能と通信して、ポリ्यूームをバックアップするストレージ オブジェクトを作成します。また、CNS サーバ コンポーネントは、ストレージ ポリシーベースの管理と通信して、ディスクに必要なサービス レベルを確保します。

CNS は、vCenter Server を介してコンテナ ポリ्यूームとそのバックアップ ストレージ オブジェクトを管理および監視するクエリ処理も実行します。

最初のクラス ディスク (FCD)

強化された仮想ディスクとも呼ばれます。これは、仮想マシンと関連付けられていない名前付き仮想ディスクです。これらのディスクは、VMFS、NFS、または vSAN データストア、およびバック ReadWriteOnce コンテナ ポリ्यूームに配置されます。

FCD テクノロジーにより、仮想マシンまたはポッドのライフサイクル外にあるパーシステント ポリ्यूームに関連するライフ サイクル操作を実行できます。仮想マシンが、複数のコンテナベースのアプリケーションを実行し、多くのアプリケーションに対してパーシステント ポリ्यूームと仮想ディスクを使用する Kubernetes ノードである場合、CNS は、コンテナとパーシステント ポリ्यूームの粒度でライフサイクルの操作が容易になります。

ストレージ ポリシー ベースの管理

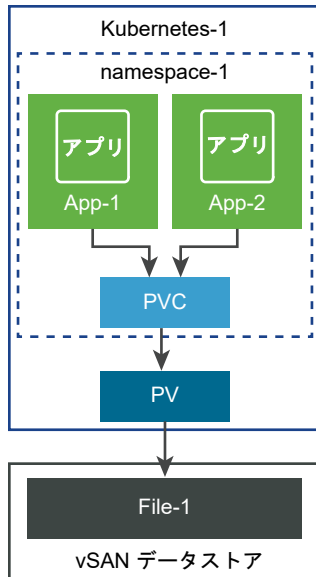
ストレージ ポリシー ベースの管理は、指定されたストレージ要件に基づき、パーシステント ポリ्यूームのプロビジョニングをサポートする vCenter Server サービスです。プロビジョニング後、サービスは、必要なポリシー特性に対するポリ्यूームのコンプライアンスを監視します。

ファイル ポリ्यूームのプロビジョニング

ファイル ポリ्यूームにはそれぞれ異なる構成を使用できます。

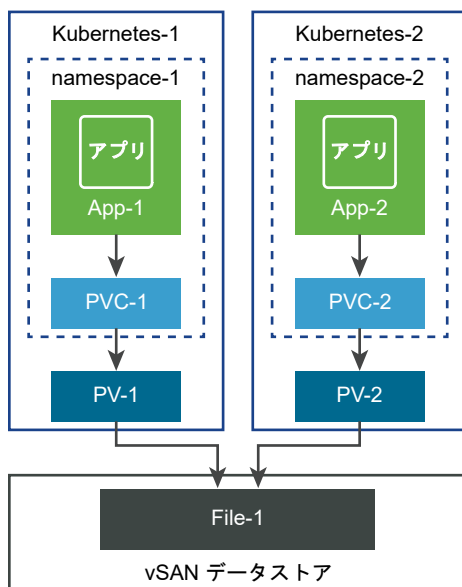
同じ名前空間内のアプリケーション間で共有される単一のファイル ボリューム

この例では、単一のファイル ボリュームが、同じ名前空間内の異なるアプリケーション間で共有ストレージとして使用されています。1つのパーシステント ボリューム要求を使用して、ファイル ボリュームをプロビジョニングします。



アプリケーションと名前空間で共有される単一のファイル ボリューム

この例では、異なるアプリケーションや名前空間で、単一のファイル ボリュームを共有ストレージとして使用しています。同じファイル ボリュームをプロビジョニングするため、名前空間ごとに個別のパーシステント ボリューム要求を作成します。



クラウド ネイティブ ストレージユーザー

vSphere クラウド ネイティブ ストレージ環境で Kubernetes ポリ्यूームを作成および監視するプロセスに関わるユーザーのタイプは通常、Kubernetes ユーザーと vSphere 管理者の 2 つのカテゴリに分類されます。どちらのタイプのユーザーも、さまざまなツールにアクセスしてさまざまなタスクを実行できます。

CNS Kubernetes ユーザー

Kubernetes ユーザーには、Kubernetes 開発者とアプリケーション所有者、Kubernetes 管理者、またはその両方を組み合わせた機能があります。Kubernetes ユーザーがクラウド ネイティブ ストレージ環境で実行するタスクには、次のようなものがあります。

- vSphere CSI をデプロイして管理する。詳細については、[Deploying a Kubernetes Cluster on vSphere with CSI and CPI](#) セクション ([Kubernetes vSphere Cloud Provider](#) ドキュメント) を GitHub で参照してください。
- ステートフル アプリケーションをデプロイして管理する。詳細については、GitHub にある、[Kubernetes vSphere Cloud Provider](#) ドキュメントの [Sample manifests to test CSI driver functionality](#) セクションを参照してください。
- パーシステント ポリ्यूームのライフ サイクルの操作を実行する。
- ストレージ クラスのライフ サイクルの操作を実行する。

CNS vSphere ユーザー

CNS vSphere ユーザーまたは vSphere 管理者は、vSphere Client にアクセスして次のタスクを実行できます。

- 仮想マシン ストレージ ポリシーのライフ サイクル操作を実行します。たとえば、Kubernetes ストレージ クラスに使用する仮想マシン ストレージ ポリシーを作成し、その名前を Kubernetes ユーザーに通知します。[ストレージ ポリシーを作成する](#) を参照してください。
- vSphere Client のクラウド ネイティブ ストレージ セクションを使用して、Kubernetes クラスタ全体のコンテナ ポリ्यूームの健全性とストレージ ポリシー コンプライアンスを監視します。[Kubernetes クラスタ間のコンテナ ポリ्यूームの監視](#) を参照してください。

vSphere 管理者向けのクラウド ネイティブ ストレージ

vSphere 管理者は、Kubernetes チームにストレージ リソースを提供し、さまざまなストレージ要件とサービスのクラスを記述する仮想マシン ストレージ ポリシーを作成します。永続性ストレージを使用する Kubernetes ワークロードがプロビジョニングされると、vSphere 管理者はバックアップ ストレージ リソースのライフサイクルおよびバックアップ ストレージ リソースの要件への準拠を監視することができます。

クラウド ネイティブ ストレージの要件

クラウド ネイティブ ストレージ環境および Kubernetes クラスタに参加する仮想マシンは、いくつかの要件を満たす必要があります。

クラウド ネイティブ ストレージの要件

- vSphere 6.7 Update 3 以降
- Kubernetes バージョン 1.14 以降。
- 1つのマスター ノードと複数のワーカー ノードを持つ Kubernetes クラスタが仮想マシンにデプロイされていること。vSphere CSI プラグインを展開し、vSphere で Kubernetes クラスタを実行する場合の詳細については、GitHub の [Kubernetes vSphere Cloud Provider](#) のドキュメントを参照してください。

Kubernetes クラスタ仮想マシンの要件

- ハードウェア バージョン 15 以降の仮想マシン。各ノードの仮想マシンに VMware Tools をインストールします。
- 仮想マシンのハードウェアに関する推奨事項：
 - ワークロード要件に基づいて、CPU とメモリを適切に設定します。
 - ノード仮想マシンのプライマリ ディスクに VMware 準仮想化 SCSI コントローラを使用します。
- すべての仮想マシンは、vSAN などの共有データストアにアクセスできる必要があります。
- 各ノードの仮想マシンで `disk.EnableUUID` パラメータを設定します。 [Kubernetes クラスタ仮想マシンを構成する](#) を参照してください。
- エラーや予期しない動作を回避するために、CNS ノード仮想マシンのスナップショットは作成しないでください。

CNS ファイル ボリュームの要件

- vSphere バージョン 7.0 以降および互換性のある Kubernetes バージョンを使用します。
- vSAN ファイル サービスを有効にして、設定します。必要なファイル サービス ドメイン、IP プール、ネットワークなどを構成する必要があります。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。
- Kubernetes ノードのゲスト OS から vSAN ファイル共有へのネットワーク アクセスを設定するには、特定のガイドラインに従ってください。 [vSAN ファイル共有へのネットワーク アクセス](#) を参照してください。

vSAN ファイル共有へのネットワーク アクセス

Kubernetes クラスタを展開する場合は、Kubernetes ノードから vSAN ファイル サービス ネットワークまで、必要なネットワーク、スイッチ、およびルーターを作成して設定する必要があります。

ネットワークのセットアップ

ネットワークを設定する場合は、次の要件に従います。

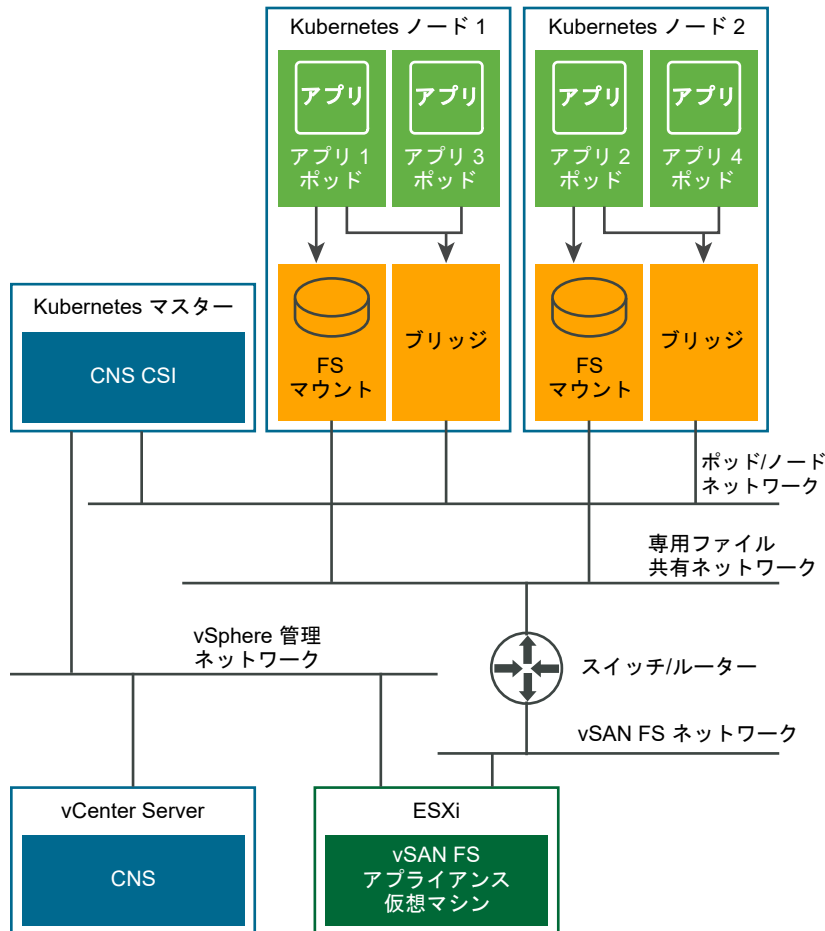
- すべての Kubernetes ノードで、vSAN ファイル共有トラフィックに専用の vNIC を使用します。
- 専用 vNIC を経由するトラフィックが、1つまたは複数の vSAN ファイル サービス ネットワークにルーティング可能であることを確認します。

- ファイル共有の IP アドレスを使用して vSAN ファイル共有に直接アクセスできるのは、各 Kubernetes ノードのゲスト OS のみであることを確認します。ノード内のポッドから vSAN ファイル共有に ping を実行したり、IP アドレスを指定してアクセスしたりすることはできません。

CNS CSI ドライバは、ゲスト OS でマウント ポイントを作成することにより、CNS ファイル ボリュームを使用するように設定されたポッドのみが vSAN ファイル共有にアクセスできるようにします。

- ノードの仮想マシンと vSAN のファイル共有の間で IP アドレスが競合しないようにしてください。

次の図に、vSAN ファイル共有サービスを使用する CNS ネットワーク構成の例を示しています。



この図のネットワーク構成の例は、次のガイドラインに従っています。

- この構成では、CNS 環境内のアイテムごとに個別のネットワークを使用します。

ネットワーク	説明
vSphere 管理ネットワーク	通常、一般的な Kubernetes クラスタでは、すべてのノードがこのネットワークにアクセスできます。
ポッドまたはノード ネットワーク	Kubernetes は、ノード間またはポッド間の通信にこのネットワークを使用します。

ネットワーク	説明
専用ファイル共有ネットワーク	CNS ファイル ボリュームのデータ トラフィックは、このネットワークを使用します。
vSAN ファイル共有ネットワーク	vSAN ファイル共有が有効になっていて、ファイル共有が使用可能なネットワーク。

- すべての Kubernetes ノードには、ファイル トラフィック専用の vNIC があります。この vNIC は、ノード間またはポッド間の通信に使用される vNIC とは異なります。
- CNS ファイル共有を使用するように設定されたアプリケーションのみが、ノードのゲスト OS のマウント ポイントを介して vSAN のファイル共有にアクセスできます。たとえば、この図では次の処理が行われます。
 - アプリケーション 1 とアプリケーション 2 のポッドはファイル ボリュームを使用するように設定されていて、CSI ドライバによって作成されたマウント ポイントを介してファイル共有にアクセスできます。
 - アプリケーション 3 とアプリケーション 4 にはファイル ボリュームが設定されておらず、ファイル共有にアクセスできません。
- vSAN ファイル共有は、ESXi ホスト上の vSAN ファイル共有アプライアンス仮想マシンにコンテナとして展開されます。Kubernetes デプロイは、Kubernetes クラスタを設定、展開、および管理できるソフトウェアまたはサービスのことで、Kubernetes ノードのゲスト OS が vSAN ファイル共有にアクセスできるように、必要なルーターとスイッチを設定できます。

セキュリティの制限

専用の vNIC によって不正なポッドがファイル共有に直接アクセスすることはできなくなりますが、特定のセキュリティ上の制限が課せられます。

- CNS ファイル機能は、CNS ファイル ボリューム ID を持つユーザーが、ボリュームに対する権限も持っていることを前提としています。CNS ファイル ボリューム ID を持つユーザーは、ボリュームに保存されているデータにアクセスできます。
- CNS ファイル ボリュームは、ユーザー ID ベース認証である AUTH_SYS 認証のみをサポートします。CNS ファイル ボリューム内のデータへのアクセスを保護するには、CNS ファイル ボリュームにアクセスするコンテナに適切なユーザー ID を使用する必要があります。
- CNS ファイル ボリュームを参照する、バインドされていない ReadWriteMany パーシステント ボリュームをバインドするには、任意の名前空間で任意の Kubernetes ユーザーによって作成されたパーシステント ボリューム要求を使用します。セキュリティ問題を回避するために、許可されたユーザーのみが Kubernetes にアクセスできるようにしてください。

vSAN ファイル サービス クラスタにアクセスするための CSI ドライバの設定

構成に応じて、CSI ドライバは、ファイル サービスが有効になっている 1 つまたは複数の vSAN クラスタでファイル ボリュームをプロビジョニングできます。

ファイル サービスが有効になっている特定の vSAN クラスタにアクセスを限定することができます。Kubernetes クラスタを展開する場合は、CSI ドライバに特定のファイル サービス vSAN クラスタへのアクセス権を設定します。その結果、CSI ドライバは、これらの vSAN クラスタでのみファイル ボリュームをプロビジョニングできるようになります。

デフォルトの構成では、CSI ドライバは、vCenter Server で使用可能な任意のファイル サービス vSAN クラスタを使用して、ファイル ボリュームのプロビジョニングを行います。CSI ドライバは、ファイル ボリュームのプロビジョニング中にアクセス可能なファイル サービス vSAN クラスタを検証しません。

クラウド ネイティブ ストレージロールと権限

クラウド ネイティブ ストレージに関連する操作を実行する場合、CNS vSphere ユーザーには特定の権限が必要です。

いくつかのロールを作成して、クラウド ネイティブ ストレージ環境に参加するオブジェクトに一連の権限を割り当てることができます。

vSphere のロールと権限の詳細、およびロールの作成方法については、『vSphere のセキュリティ』のドキュメントを参照してください。

ロール名	権限名	説明	必要とするオブジェクト
CNS-SPBM	Profile-driven storage > Profile-driven storage 更新	ストレージ仮想マシンのストレージ ポリシーの作成や更新など、仮想マシン ストレージ ポリシーへの変更を許可します。	root vCenter Server
	Profile-driven storage > Profile-driven storage ビュー	定義済みストレージ ポリシーを表示できるようにします。	
CNS-VM	仮想マシン > 設定 > 既存ディスクの追加	既存の仮想ディスクを仮想マシンに追加できるようにします。	すべてのクラスタ ノード仮想マシン
	仮想マシン > 設定 > デバイスの追加または削除	ディスク以外のデバイスを追加または削除できるようにします。	
CNS-Datastore	データストア > 低レベルのファイル操作	データストア ブラウザ内で、読み取り、書き込み、削除、および名前変更操作を実行できるようにします。	パーシステント ボリュームが配置されている共有データストア

ロール名	権限名	説明	必要とするオブジェクト
読み取り専用	デフォルトのロール	オブジェクトに対する読み取り専用ロールが割り当てられているユーザーは、オブジェクトの状態および詳細を表示できます。たとえば、このロールを持つユーザーは、すべてのノードの仮想マシンからアクセス可能な共有データストアを見つけることができます。 ゾーンとトポロジに対応した環境では、ホスト、クラスタ、データセンターなどのノード仮想マシンのすべての先祖に、CSI ドライバおよび CCM を使用するよう設定された vSphere ユーザーに対する読み取り専用ロール セットが必要です。これは、ノードのトポロジを準備するためにタグとカテゴリを読み取れるようにするために必要です。	ノードの仮想マシンが配置されているすべてのホスト データセンター
CNS ユーザー インターフェイス	privilege.Cns.label > privilege.Cns.Searchable.label	ストレージ管理者が CNS ユーザー インターフェイスを表示できるようにします。	

ストレージ ポリシーを作成する

Kubernetes コンテナ アプリケーションをバックアップする vSphere ストレージ オブジェクトは、特定のストレージ要件を満たす必要があります。vSphere ユーザーとして、Kubernetes ユーザーから提供された要件に基づいて仮想マシン ストレージ ポリシーを作成します。

ストレージ ポリシーは、Kubernetes コンテナをバックアップする仮想ディスクまたは vSAN ファイル共有に関連付けられます。

環境内に複数の vCenter Server インスタンスがある場合は、各インスタンスに仮想マシン ストレージ ポリシーを作成します。すべてのインスタンスで同じポリシー名を使用します。

前提条件

- Kubernetes ユーザーは、ステートフルのコンテナ アプリケーションが展開される Kubernetes クラスタを特定します。
- Kubernetes ユーザーは、コンテナ アプリケーションのストレージ要件を収集し、それらを vSphere ユーザーに通知します。
- 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 Client で、[仮想マシン ストレージ ポリシーの作成] ウィザードを開きます。
 - a [メニュー]-[ポリシーおよびプロファイル] の順にクリックします。
 - b [ポリシーおよびプロファイル] で、[仮想マシン ストレージ ポリシー] をクリックします。
 - c [仮想マシン ストレージ ポリシーの作成] をクリックします。

- 2 ポリシーの名前と説明を入力して [次へ] をクリックします。

オプション	操作
vCenter Server	vCenter Server インスタンスを選択します。
名前	ストレージ ポリシーの名前（容量効率の高さなど）を入力します。
説明	ストレージ ポリシーの説明を入力します。

- 3 データストア固有のルールの [ポリシー構造] ページで、[vSAN ストレージのルールの有効化] を選択し、[次へ] をクリックします。
- 4 [vSAN] ページで、ポリシー ルールセットを定義し、[次へ] をクリックします。
 - a [可用性] タブで、[サイトの耐障害性] と [許容される障害の数] を定義します。
 - b [詳細なポリシー ルール] タブで、オブジェクトあたりのディスク ストライプの数やフラッシュ読み取りキャッシュの予約などの詳細なポリシー ルールを定義します。
- 5 [ストレージ互換性] ページでこのポリシーに適合する vSAN データストアのリストを確認し、[次へ] をクリックします。

6 [確認して完了] ページでポリシーの設定を確認し、[完了] をクリックします。

次のステップ

これで、ストレージ ポリシー名を Kubernetes ユーザーに通知できるようになりました。作成した仮想マシン ストレージ ポリシーは、動的ボリューム プロビジョニングのストレージ クラス定義の一部として使用されます。

Kubernetes クラスタ仮想マシンを構成する

各ノードの仮想マシンで、disk.EnableUUID パラメータを有効にし、仮想マシンを仮想ディスクに正常にマウントできるようにします。

クラスタに参加している各仮想マシン ノードに対して、次の手順を実行します。

前提条件

- Kubernetes クラスタ用に複数の仮想マシンを作成します。仮想マシンには、k8s-master、k8s-node1、k8s-nodeX などの名前を使用できます。仮想マシンの要件については、[クラウド ネイティブ ストレージの要件](#)を参照してください。
- 必要な権限：仮想マシン.構成.設定

注： エラーや予期しない動作を回避するために、CNS ノード仮想マシンのスナップショットは作成しないでください。

手順

1 vSphere Client 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] タブをクリックして、[詳細設定] メニューを展開します。
- 3 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。
- 4 **disk.EnableUUID** パラメータを設定します。

パラメータがある場合は、その値が True に設定されていることを確認します。パラメータがない場合、追加して値を True に設定できます。

名前	値
disk.EnableUUID	True

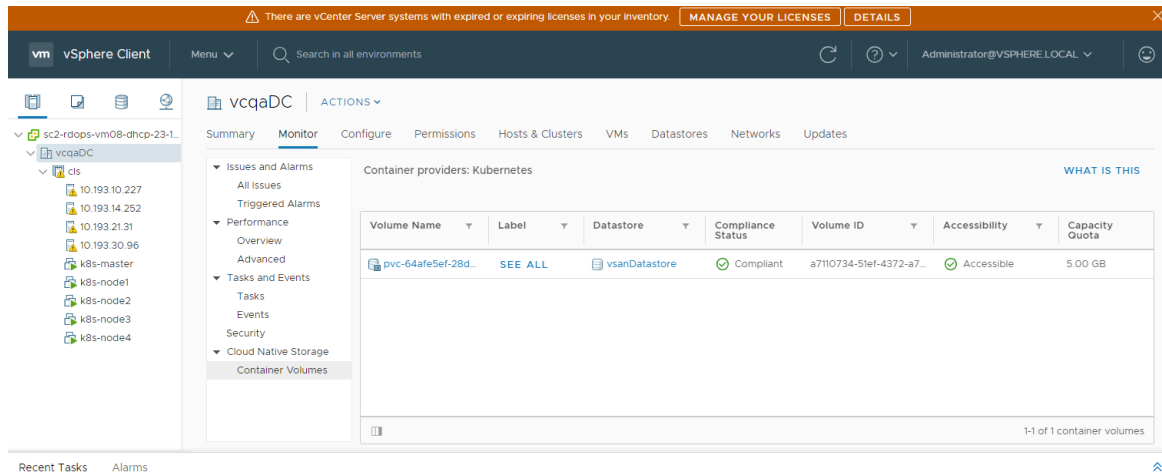
Kubernetes クラスタ間のコンテナ ボリュームの監視

ステートフル アプリケーションが Kubernetes に展開されると、ボリュームおよびそのバックアップ vSphere ストレージ オブジェクトが vSphere Client に表示されるようになります。ボリュームを表示および監視して、発生する可能性のあるストレージ問題のトラブルシューティングを行うことができます。

注： Kubernetes CNS サーバで障害が発生した場合は、完全同期が実行されるまで、vSphere Client の CNS オブジェクトが正しく表示されないことがあります。

手順

- 1 vCenter Server インスタンス、データセンター、またはデータストアに移動します。
- 2 [監視] タブをクリックし、[クラウド ネイティブ ストレージ] の下の [コンテナ ボリューム] をクリックします。
- 3 環境内で使用できるコンテナ ボリュームを確認し、ストレージ ポリシーのコンプライアンスの状態を監視します。

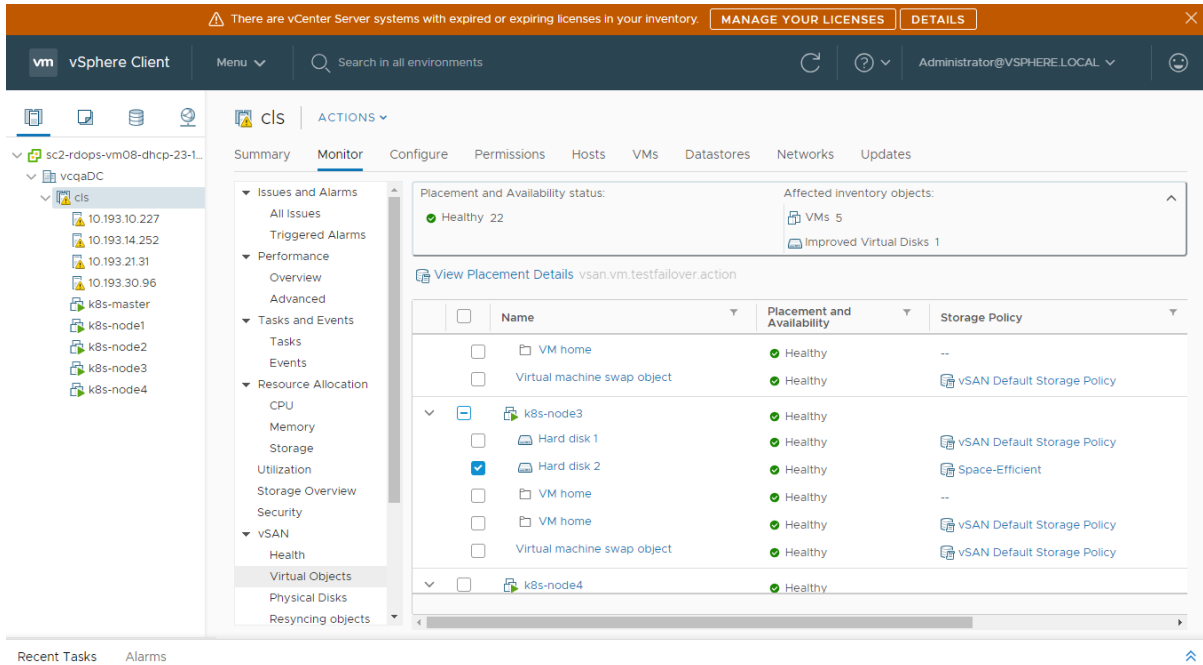


- 4 [ラベル] 列の [すべて表示] リンクをクリックし、追加の詳細を表示します。

詳細には、PersistentVolumeClaim、StorageClass などの名前が含まれていて、関連付けられている Kubernetes オブジェクトにボリュームをマッピングするのに役立ちます。

- 5 [ボリューム名] 列のリンクをクリックして、ボリュームをバックアップするさまざまなコンポーネント、および配置、コンプライアンス、ストレージ ポリシーなどの詳細を確認します。

注： [Virtual Volumes] 画面が表示されるのは、基盤となるデータストアが vSAN の場合のみです。



Cloud Native Storage での暗号化の使用

vSphere 7.0 以降では、vSphere 暗号化テクノロジーを使用して、パーシステント ボリュームをバックアップする FCD 仮想ディスクを保護することができます。

vSphere 環境で暗号化を使用するには、いくつかの準備作業が必要であり、vCenter Server とキー管理サーバ (KMS) の間の信頼できる接続の設定が含まれます。これにより、vCenter Server は必要に応じて KMS からキーを取得できるようになります。vSphere 暗号化プロセスに参加するコンポーネントの詳細については、『vSphere のセキュリティ』ドキュメントの「[vSphere 仮想マシンの暗号化のコンポーネント](#)」を参照してください。

手順

- 1 vSphere 環境で KMS クラスタを設定します。

詳細については、「[キー管理サーバ クラスタの設定](#)」を参照してください。

2 Kubernetes クラスタのすべてのノード仮想マシンを暗号化します。

vSphere Client を使用して、この手順を実行します。

- a ノード仮想マシンに移動します。
- b 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 ポリシーの編集] の順に選択します。
- c [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、[仮想マシン暗号化ポリシー] を選択し、[OK] をクリックします。

ノード仮想マシンの暗号化プロセスを迅速化するために、仮想マシン ホームのみを暗号化することができます。

3 vSphere CSI 設定を使用して、暗号化されたパーシステント ボリュームを Kubernetes クラスタに作成します。

- a 仮想マシン暗号化ストレージ ポリシーを参照する StorageClass を作成します。

例として、次の YAML ファイルを使用します。

```
kind: StorageClass
apiVersion: storage.k8s.io/v1
metadata:
  name: encryption
provisioner: csi.vsphere.vmware.com
parameters:
  storagePolicyName: "VM Encryption Policy"
  datastore: vsanDatastore
```

- b PersistentVolumeClaim を使用して、パーシステント ボリュームをプロビジョニングします。

PersistentVolumeClaim では、storageClassName フィールドに暗号化ストレージ クラスの名前を含める必要があります。

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 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、『ESXCLI スタート ガイド』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 27-1. 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 27-1. 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 システムのバス名を使用します。バス名は /vmfs/devices 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"> ■ /vmfs/devices/disks (ローカルまたは SAN ベース ディスク)。 ■ /vmfs/devices/lvm (ESXi 論理ボリューム)。 ■ /vmfs/devices/generic(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 /vmfs 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 style="background-color: #f0f0f0; padding: 5px;">/vmfs/volumes/<i>file_system_UUID</i></pre> <p>または</p> <pre style="background-color: #f0f0f0; padding: 5px;">/vmfs/volumes/<i>file_system_label</i></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 style="background-color: #f0f0f0; padding: 5px;">/vmfs/volumes/<i>file_system_label</i>/<i>file_system_UUID</i>/[<i>dir</i>]/<i>myDisk.vmdk</i></pre> <p>現在の作業ディレクトリが <i>myDisk.vmdk</i> 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 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.3863316131XXXXX: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
```

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 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。

- `-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 上または NFS データストア上のファイルであるか、または vSAN または vVols データストア上のオブジェクトであるかを指定します。
- `--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 oldNamenewName
```

仮想ディスクまたは RDM のクローン作成または変換

vmkfstools コマンドを使用して、指定した仮想ディスクまたは Raw ディスクのコピーを作成します。

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 上または NFS データストア上のファイルであるか、または vSAN または vVols データストア上のオブジェクトであるかを指定します。
- `--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 myVMFS という名前の仮想ディスク ファイルに、マスタ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-master.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-master.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 ポリ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す。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、エクステントの追加、再署名など、データストア操作中にホストに障害が発生した場合にこのコマンドを使用できます。このコマンドを実行するときには、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。