

SIOS Protection Suite for Windows

8.7.2 — 最終更新日時: 20 November 2020

SIOS TECHNOLOGY CORP.

Copyright © 2020 SIOS TECHNOLOGY CORP.

目次

1. SIOS Protection Suite for Windows 15

2. SIOS Protection Suite for Windows リリースノート 16

3. SIOS Protection Suite for Windows クイックスタートガイド 35

4. AWS Direct Connect クイックスタートガイド 38

5. AWS VPC ピア接続クイックスタートガイド 42

6. Microsoft Azure 動作検証ガイド 47

6.1. Microsoft Azure の概要 50
6.2. Azure 特有の設定について 53
6.3. 注意事項 55
6.4. Azure 上仮想環境の構築 56
6.4.1. リソースグループの作成 57
6.4.2. 仮想ネットワークの作成 59
6.4.3. クラスターノード（稼働系と待機系）の作成 65
6.4.4. クライアントの作成 74
6.4.5. ロードバランサーの作成 76
6.5. OS の設定 81
6.6. SIOS Protection Suite for Windows による HA クラスターの構築 85
6.7. Oracle固有の環境構築 92
6.7.1. ミラーボリュームリソース階層の作成 93
6.7.2. Oracleのインストールと設定 95
6.7.2.1. Oracle Databaseのインストール（稼働系） 96
6.7.2.2. Oracleリスナー設定（稼働系） 98
6.7.2.3. パスワードファイルの作成（稼働系） 108
6.7.2.4. 待機系Oracleインストール前の準備 109
6.7.2.5. Oracle Databaseのインストール（待機系） 111
6.7.2.6. Oracleリスナー設定（待機系） 112
6.7.2.7. パスワードファイルの作成（待機系） 113
6.7.2.8. 稼働系へのスイッチバック 114
6.7.3. Oracleの保護 115
6.7.4. Oracleリスナーの設定変更 117
6.7.5. 接続確認（クライアント） 121
6.7.5.1. Oracleクライアントのインストール 122
6.7.5.2. Oracleクライアントの接続確認 123
6.8. PostgreSQL固有の環境構築 126
6.8.1. PostgreSQLのインストールと設定（稼働系、待機系） 127
6.8.2. ミラーボリュームリソース階層の作成（稼働系） 129
6.8.3. PostgreSQL関連パラメーターの変更（稼働系、待機系） 131
6.8.4. PostgreSQLデータベースの保護（稼働系） 133
6.8.5. 接続確認（クライアント） 136

7. SIOS Protection Suite インストレーションガイド 140
7.1. SIOS Protection Suite 環境のプランニング 141
7.1.1. サーバ通信のプランニング 142
7.1.2. リカバリキットの要件 144
7.1.3. ストレージとアダプタの要件 145
7.1.4. サーバ仕様の確認 146
7.2. SIOS Protection Suite 環境のセットアップ 148
7.2.1. ストレージの構成 149
7.2.2. DNS リソースの要件 150
7.2.3. データベースアプリケーションのインストールと設定 151
7.2.4. 共有ディスクボリュームインスタンスの安全な作成 152
7.2.5. ネットワーク構成の確認 153
7.3. SIOS Protection Suite のインストール 157
7.3.1. SIOS Protection Suite Core ソフトウェア 158
7.3.2. SIOS Protection Suite Core ソフトウェアのインストール 159
7.3.3. ライセンスの取得とインストール 163
7.3.4. LifeKeeper for Windows ローカライズ言語サプリメントのインストール 168
7.3.5. SIOS Protection Suite の サイレントインストール 169
7.3.6. サードパーティ製品のファイル 171
7.3.7. アプリケーションディレクトリの例外事項 172
7.3.8. SIOS Protection Suite for Windows のアンインストール 173
7.3.9. SIOS Protection Suite のアップグレード 175
7.3.10. 修復 178
7.3.11. LifeKeeper の起動 179

8. SIOS Protection Suite for Windows テクニカルドキュメンテーション 180
8.1. SIOS Protection Suite for Windows について 181
8.1.1. SIOS Protection Suite Core ソフトウェア 184
8.1.2. SIOS Protection Suite Microsoft SQL Server Recovery Kit 186
8.1.3. コミュニケーションパスの概要 187
8.1.3.1. コミュニケーションパスの種類 188
8.1.3.2. SIOS Protection Suite のハートビート 190
8.1.3.3. ハートビート間隔 191
8.1.3.4. セーフティチェック 192
8.1.4. リソース階層 193
8.1.4.1. 階層の関係 194
8.1.4.2. リソース階層情報 195
8.1.4.3. リソースのステータス 196
8.1.4.4. 共有イクイバレンシ 197
8.2. 構成 198
8.2.1. SIOS Protection Suite の設定手順 199
8.2.2. アクティブ / アクティブグループ化 200
8.2.3. アクティブ / スタンバイグループ化 201
8.2.4. インテリジェントスイッチバックと自動スイッチバック 202
8.2.5. SIOS Protection Suite の設定 203

8.2.5.1. 共通ハードウェアコンポーネント 204
8.2.5.2. システムのグループ化 205
8.2.6. SPS でマルチバイト言語エンコーディングを設定する 206
8.3. SIOS Protection Suite の管理の概要 207
8.3.1. GUI による管理作業 209
8.3.1.1. サーバプロパティの編集 210
8.3.1.2. サーバのシャットダウン方法の設定 211
8.3.1.2.1. サーバプロパティ 212
8.3.1.3. 自動フェイルオーバを無効にする 217
8.3.1.4. コミュニケーションパスの作成 219
8.3.1.5. コミュニケーションパスの削除 221
8.3.2. リソース階層に関連する作業 222
8.3.2.1. リソース階層の作成 223
8.3.2.1.1. DNS リソース階層の作成 224
8.3.2.1.2. ファイル共有リストリソース階層の作成 227
8.3.2.1.3. Generic Application リソース階層の作成 229
8.3.2.1.4. LAN Manager リソース階層の作成 232
8.3.2.1.5. ボリュームリソース階層の作成 233
8.3.2.1.6. IP アドレスリソース階層の作成 235
8.3.2.1.6.1. IP ローカルリカバリのシナリオ 237
8.3.2.1.7. リソース優先度の編集 238
8.3.2.1.7.1. 不完全なリソース優先度の変更 240
8.3.2.1.8. リソースプロパティの編集 242
8.3.2.2. リソース階層の拡張 243
8.3.2.2.1. リソース階層の拡張 244
8.3.2.2.2. ファイル共有リソース階層の拡張 245
8.3.2.2.3. Generic Application リソース階層の拡張 246
8.3.2.2.4. LAN Manager リソース階層の拡張 247
8.3.2.2.5. ボリュームリソース階層の拡張 248
8.3.2.2.6. IP リソース階層の拡張 249
8.3.2.3. リソース階層の拡張解除 251
8.3.2.4. リソース依存関係の追加 252
8.3.2.5. リソース依存関係の削除 253
8.3.2.6. 全サーバのリソース階層の削除 254
8.3.3. マニュアルページ 255
8.3.3.1. LCD - その他の LCD プログラム 256
8.3.3.1.1. lcdrcp 257
8.3.3.1.2. lcdrecover 258
8.3.3.1.3. lcdremexec 260
8.3.3.1.4. lcdsync 261
8.3.3.1.5. lkstart 262
8.3.3.1.6. lkstop 263
8.3.3.2. LCDI アプリケーション 264
8.3.3.2.1. app_create 265
8.3.3.2.2. app_list 266

8.3.3.2.3. app_remove 267
8.3.3.3. LCDI インスタンス 268
8.3.3.3.1. ins_list 270
8.3.3.3.1.1. 初期化の方法 272
8.3.3.3.1.2. 初期状態 273
8.3.3.3.2. ins_create 274
8.3.3.3.3. ins_gettag 275
8.3.3.3.4. ins_remove 276
8.3.3.3.5. ins_setas 277
8.3.3.3.6. ins_setchkint 278
8.3.3.3.7. ins_setin 279
8.3.3.3.8. ins_setit 280
8.3.3.3.9. ins_setlocalrecover 281
8.3.3.3.10. ins_setst 282
8.3.3.4. LCDI 関係 283
8.3.3.4.1. dep_create 285
8.3.3.4.2. dep_list 286
8.3.3.4.3. dep_remove 287
8.3.3.4.4. eqv_create 288
8.3.3.4.5. eqv_list 289
8.3.3.4.6. eqv_remove 290
8.3.3.5. LCDI リソースタイプ 291
8.3.3.5.1. typ_create 293
8.3.3.5.2. typ_list 294
8.3.3.5.3. typ_remove 295
8.3.3.6. LCDI システム 296
8.3.3.6.1. sys_create 297
8.3.3.6.2. sys_getds 298
8.3.3.6.3. sys_getst 299
8.3.3.6.4. sys_list 300
8.3.3.6.5. sys_remove 301
8.3.3.7. LifeKeeper のフラグ 302
8.3.3.7.1. flg_create 303
8.3.3.7.2. flg_list 304
8.3.3.7.3. flg_remove 305
8.3.3.7.4. flg_test 306
8.3.3.7.5. LCDI フラグ 307
8.3.3.8. lk_chg_value 309
8.3.3.9. lk_err 312
8.3.3.10. perform_action 313
8.3.3.11. sendevent 317
8.3.3.12. volume 320
8.3.4. LKSUPPORT 322
8.3.5. ブラウザのセキュリティ設定 323
8.3.6. IP ローカルリカバリ 324

8.3.7. SNMP による SIOS Protection Suite イベント転送の概要 325
8.3.8. Java のアップグレード 329
8.4. ユーザガイド 331
8.4.1. LifeKeeper GUI 332
8.4.1.1. GUI の概要 333
8.4.1.1.1. ステータステーブル 335
8.4.1.1.2. プロパティパネル 336
8.4.1.1.3. アウトプットパネル 337
8.4.1.1.4. メッセージバー 338
8.4.1.2. ツールバー 339
8.4.1.2.1. グローバルツールバー 340
8.4.1.2.2. リソースコンテキストツールバー 341
8.4.1.2.3. サーバコンテキストツールバー 342
8.4.1.3. メニュー 343
8.4.1.3.1. リソースコンテキストメニュー 344
8.4.1.3.2. サーバコンテキストメニュー 346
8.4.1.3.3. [ファイル] メニュー 347
8.4.1.3.4. [編集] メニュー – リソース 348
8.4.1.3.5. [編集] メニュー - サーバ 349
8.4.1.3.6. [表示] メニュー 350
8.4.1.3.7. [ヘルプ] メニュー 352
8.4.1.4. LifeKeeper GUI サーバコンポーネントおよびクライアントコンポーネント 353
8.4.1.5. SIOS Protection Suite Web クライアントの実行 355
8.4.1.6. SIOS Protection Suite サーバ上の GUI アプリケーションの実行 357
8.4.1.7. LifeKeeper GUI ユーザアカウント 358
8.4.1.7.1. GUI ユーザの設定 359
8.4.2. 共通タスク 361
8.4.2.1. クラスタへの接続 362
8.4.2.2. クラスタからの切断 364
8.4.2.3. 接続先サーバの表示 365
8.4.2.4. サーバステータスの表示 366
8.4.2.5. サーバログファイルの表示 367
8.4.2.6. サーバプロパティの表示 369
8.4.2.7. リソースタグと ID の表示 370
8.4.2.8. リソースステータスの表示 371
8.4.2.9. リソースプロパティの表示 372
8.4.2.10. メッセージ履歴の表示 373
8.4.2.11. リソース階層ツリーの展開と縮小 374
8.4.3. オペレータタスク 375
8.4.3.1. リソースを起動する 376
8.4.3.2. リソースを停止する 377
8.4.3.3. ボリュームリソースの起動と停止 378
8.4.3.4. ボリュームシャドウコピー (VSS) 381
8.4.3.5. 共有 SCSI ボリュームのボリュームロック 382
8.4.4. 詳細項目 383

8.4.4.1. LifeKeeper 構成データベース (LCD) 384
8.4.4.2. LCD のディレクトリ構造 385
8.4.4.3. LCD ディレクトリの構造図 386
8.4.4.4. LCD 構成データ 387
8.4.4.5. LCD リソースタイプ 388
8.4.4.6. リソースサブディレクトリ 389
8.4.4.7. LCDI コマンド 390
8.4.4.8. LifeKeeper 通信マネージャ (LCM) 391
8.4.4.9. 通信ステータス情報 392
8.4.5. メンテナンス作業 394
8.4.5.1. LifeKeeper の起動と停止 395
8.4.5.2. IP リソース管理 396
8.4.5.3. DNS リソースの管理 398
8.4.5.4. 保護対象の共有ファイルリストの表示 399
8.4.5.5. EditFileShareResource ユーティリティ 400
8.4.5.6. リソース階層の移動 401
8.4.5.7. 共有ディスクのオフラインメンテナンス 402
8.4.5.8. SIOS Protection Suite で保護するシステムの保守 403
8.4.5.9. Generic Application スクリプトの設定 404
8.4.5.10. リソース階層の保守 406
8.4.5.11. フェイルオーバ後のリカバリ作業 407
8.4.5.12. SIOS Protection Suite for Windows のアンインストール 408
8.4.5.13. 保護対象のボリュームで CHKDSK を実行する 410
8.4.6. データレプリケーション 411
8.4.6.1. 複製ボリュームリソースの監視 412
8.4.6.2. レプリケーションの設定 414
8.4.6.3. 複製ボリュームの操作 415
8.4.6.4. スプリットブレインとは 417
8.4.6.5. スプリットブレインリカバリ 419
8.5. DataKeeper 422
8.5.1. はじめに 423
8.5.1.1. ユーザインターフェース 425
8.5.1.2. DataKeeper コンポーネント 427
8.5.1.2.1. DataKeeper サービスログオン ID とパスワードの選択 429
8.5.1.3. レプリケーションについて 434
8.5.1.3.1. SIOS DataKeeper インテントログ 435
8.5.1.3.2. インテントログの再配置 437
8.5.1.3.3. SIOS DataKeeper の再同期 438
8.5.1.3.4. 同期および非同期ミラーリング 439
8.5.1.3.5. 読み込みおよび書き込み操作 446
8.5.1.3.6. ボリュームの考慮事項 447
8.5.1.3.7. ミラーリング用ネットワークカードの指定 448
8.5.1.3.8. パフォーマンスモニタカウンタ 449
8.5.2. 構成 455
8.5.2.1. セクタサイズ 456

8.5.2.2. ネットワーク帯域 457
8.5.2.3. ネットワークアダプタ設定 459
8.5.2.4. DataKeeper サービスログオン ID とパスワードの選択 460
8.5.2.5. ファイアウォール設定 465
8.5.2.6. 高速ストレージのベストプラクティス 470
8.5.2.7. クラスタノードから外部DRサイトへのデータレプリケーション構成 472
8.5.2.8. パフォーマンスチューニング 473
8.5.2.9. 「すべてのドライブのページングファイルサイズを自動で管理する」を無効にする 474
8.5.2.10. WAN に関する考慮事項 477
8.5.2.10.1. LAN/WAN 間のデータの初期同期 478
8.5.2.10.2. 圧縮 481
8.5.2.10.3. ネットワーク帯域制限 482
8.5.3. 管理 483
8.5.3.1. DataKeeper のイベントログ通知 484
8.5.3.2. プライマリサーバのシャットダウン 486
8.5.3.3. セカンダリサーバの障害 487
8.5.3.4. 大量書き込みに対する考慮事項 488
8.5.3.5. CHKDSK に関する考慮事項 489
8.5.3.6. CLEANUPMIRROR 490
8.5.3.7. DKSUPPORT 491
8.5.3.8. DKHEALTHCHECK 492
8.5.3.9. イベントログの考慮事項 493
8.5.3.10. ディスク管理の使用 494
8.5.3.11. レジストリエントリ 495
8.5.3.12. SIOS DataKeeper で EMCMD を使用する 505
8.5.3.12.1. ミラー状態の定義 508
8.5.3.12.2. BREAKMIRROR 509
8.5.3.12.3. CHANGEMIRRORENDPOINTS 510
8.5.3.12.4. CHANGEMIRRORTYPE 515
8.5.3.12.5. CLEARBLOCKTARGET 517
8.5.3.12.6. CLEARSNAPSHOTLOCATION 518
8.5.3.12.7. CLEARSWITCHOVER 519
8.5.3.12.8. CONTINUEMIRROR 520
8.5.3.12.9. CREATEJOB 521
8.5.3.12.10. CREATEMIRROR 522
8.5.3.12.11. DELETEJOB 524
8.5.3.12.12. DELETELOCALMIRRORONLY 525
8.5.3.12.13. DELETEMIRROR 526
8.5.3.12.14. DROPSNAPSHOT 527
8.5.3.12.15. GETBLOCKTARGET 528
8.5.3.12.16. GETCOMPLETEVOLUMELIST 529
8.5.3.12.17. GETCONFIGURATION 530
8.5.3.12.18. GETEXTENDEDVOLUMEINFO 531
8.5.3.12.19. GETJOBINFO 532
8.5.3.12.20. GETJOBINFOFORVOL 533

8.5.3.12.21. GETMIRRORTYPE 534
8.5.3.12.22. GETMIRRORVOLINFO 535
8.5.3.12.23. GETREMOTEBITMAP 536
8.5.3.12.24. GETRESYNCSTATUS 537
8.5.3.12.25. GETSERVICEINFO 539
8.5.3.12.26. GETSNAPSHOTLOCATION 540
8.5.3.12.27. GETSOURCEMIRROREDVOLUMES 541
8.5.3.12.28. GETTARGETMIRROREDVOLUMES 542
8.5.3.12.29. GETVOLUMEDRVSTATE 543
8.5.3.12.30. GETVOLUMEINFO 544
8.5.3.12.31. ISBREAKUSERREQUESTED 546
8.5.3.12.32. ISPOTENTIALMIRRORVOL 547
8.5.3.12.33. LOCKVOLUME 548
8.5.3.12.34. MERGETARGETBITMAP 549
8.5.3.12.35. PAUSEMIRROR 550
8.5.3.12.36. PREPARETOBECOMETARGET 551
8.5.3.12.37. READREGISTRY 552
8.5.3.12.38. REGISTERCLUSTERVOLUME 553
8.5.3.12.39. RESTARTVOLUMEPIPE 554
8.5.3.12.40. RESYNCMIRROR 555
8.5.3.12.41. SETBLOCKTARGET 556
8.5.3.12.42. SETCONFIGURATION 557
8.5.3.12.43. SETSNAPSHOTLOCATION 558
8.5.3.12.44. STOPSERVICE 559
8.5.3.12.45. SWITCHOVERVOLUME 560
8.5.3.12.46. TAKESNAPSHOT 561
8.5.3.12.47. UNLOCKVOLUME 562
8.5.3.12.48. UPDATEJOB 563
8.5.3.12.49. UPDATEVOLUMEINFO 564
8.5.3.13. SIOS DataKeeperでDKPwrShellを使用する 566
8.5.3.13.1. New-DataKeeperMirror 567
8.5.3.13.2. New-DataKeeperJob 568
8.5.3.13.3. Remove-DataKeeperMirror 569
8.5.3.13.4. Remove-DataKeeperJob 570
8.5.3.13.5. Add-DataKeeperJobPair 571
8.5.3.13.6. Get-DataKeeperVolumeInfo 572
8.5.4. ユーザガイド 573
8.5.4.1. 入門 574
8.5.4.1.1. ディスクからディスク 575
8.5.4.1.2. 1 対 1 577
8.5.4.1.3. 1 対多 (マルチターゲット) 579
8.5.4.1.4. 多対 1 581
8.5.4.1.5. 共有ディスクを単体のディスクにレプリケーションする構成 582
8.5.4.1.6. 共有ディスク同士でレプリケーションする構成 583
8.5.4.1.7. N 個の共有ディスクターゲットへレプリケーションされる N 個の共有ディスク構成 585

8.5.4.2. SIOS DataKeeper の設定方法 587
8.5.4.2.1. SIOS DataKeeper の設定方法 588
8.5.4.2.2. サーバへ接続 589
8.5.4.2.3. サーバからの切断 590
8.5.4.2.4. ジョブの作成 591
8.5.4.3. ミラーの設定 592
8.5.4.3.1. ミラーの作成 593
8.5.4.3.2. 共有ボリュームとのミラーの作成 595
8.5.4.3.3. 共有ストレージボリュームリソースの安全な作成 598
8.5.4.3.4. 複数ターゲットとのミラーの作成 600
8.5.4.3.5. 複数ターゲットのスイッチオーバおよびフェイルオーバ 602
8.5.4.4. ジョブ操作 605
8.5.4.4.1. ジョブ 606
8.5.4.4.2. ジョブ名の変更 607
8.5.4.4.3. ジョブの削除 608
8.5.4.4.4. ジョブの再アサイン 609
8.5.4.4.5. ミラーのスイッチオーバ 610
8.5.4.5. ミラーの操作 612
8.5.4.5.1. ミラーの管理 613
8.5.4.5.2. 一時停止 / ロック解除 614
8.5.4.5.3. 再開 / ロック 615
8.5.4.5.4. 部分再同期 616
8.5.4.5.5. 中断 617
8.5.4.5.6. 再同期 618
8.5.4.5.7. ミラーの削除 619
8.5.4.5.8. ターゲットの再配置 620
8.5.4.5.9. DataKeeper ボリュームのサイズ変更 621
8.5.4.5.10. ミラープロパティ 625
8.5.4.5.11. 既存のミラーの圧縮レベルの変更 627
8.5.4.6. 共有ボリュームの操作 628
8.5.4.6.1. 共有ボリュームの管理 629
8.5.4.6.2. 共有システムの追加 630
8.5.4.6.3. 共有システムの削除 631
8.5.4.7. Windows Server 2012 上での Microsoft iSCSI ターゲットと DataKeeper の使用 632
8.5.4.7.1. iSCSI ターゲットのインストール 634
8.5.4.7.2. ミラーの作成とクラスタの構成 635
8.5.4.7.3. iSCSI 仮想ディスクの作成 638
8.5.4.7.4. Windows 2012 での iSCSI イニシエータの設定 640
8.5.4.8. DataKeeper Notification Icon 642
8.5.4.9. DataKeeper ターゲットスナップショット 644
8.5.4.10. SIOS DataKeeper Standard Edition を使用して Hyper-V 仮想マシンのディザスタリカバリを行う 655
8.5.5. よくある質問 666
8.5.5.1. Windows のファイル名およびディレクトリ名の認識 667
8.5.5.2. AWSに関する問題と回避策 668

8.5.5.3. ミラーエンドポイントの変更 669
8.5.5.4. ミラータイプの変更 670
8.5.5.5. [ミラーを作成]、[ジョブ名を変更]、[ジョブを削除] 操作がグレイアウトされる 671
8.5.5.6. データ転送ネットワークプロトコル 672
8.5.5.7. [削除] および [スイッチオーバ] 操作がグレイアウトされる 673
8.5.5.8. ミラーの削除に関する FAQ 674
8.5.5.9. サーバーに適用されているGPOの確認 675
8.5.5.10. エラーメッセージログ 676
8.5.5.11. ミラーを作成できない 677
8.5.5.12. ネットワーク切断 678
8.5.5.13. ターゲットドライブの全容量を再利用する 680
8.5.5.14. Windows Server フェールオーバークラスターロールから DataKeeper ストレージを削除する 681
8.5.5.15. ミラーボリュームのサイズ変更または拡張 682
8.5.5.16. スプリットブレインに関するFAQ 683
8.5.5.17. ソースとターゲットの間のレプリケーションの停止 686
8.5.5.18. ボリュームシャドウコピーを使用する 687
8.5.5.19. ミラーリングに使用できないボリューム 688
8.5.6. トラブルシューティング 689
8.5.6.1. 既知の問題と回避策 690
8.5.6.1.1. 指定したボリュームへのアクセス拒否 692
8.5.6.1.2. LifeKeeper および DataKeeper for Windows のアンチウイルスソフトウェアの除外リスト 693
8.5.6.1.3. DataKeeper ボリュームをクラスタリソースタイプとして使用できない 694
8.5.6.1.4. ミラーの作成に失敗する 695
8.5.6.1.5. Hyper-V ホストクラスタエラー 696
8.5.6.1.6. Live Migration の失敗 698
8.5.6.1.7. MaxResyncPasses 値 699
8.5.6.1.8. ダイナミックディスクのミラーリング 700
8.5.6.1.9. 新しいリソースはオフラインだがロック解除されている 701
8.5.6.1.10. サーバログインアカウントおよびパスワードはクラスタの各サーバで同一である必要がある 702
8.5.6.1.11. システムイベントログ – GUI でのミラー作成の失敗 703
8.5.6.1.12. 以前のインストールパスを確認できない 704
8.5.6.1.13. ユーザインターフェース – ミラーを作成できない 705
8.5.6.1.14. ユーザインターフェース – ミラーの片側しか表示されない 706
8.5.6.1.15. Windows Server 2012 固有の問題 707
8.5.6.1.15.1. Windows Server 2012 MMC スナップインのクラッシュ 708
8.5.6.1.15.2. Windows Server 2012 iSCSI Target の役割はダイナミックディスクをサポートしていない 710
8.5.6.1.15.3. ミラー作成中にWindows Server 2012のデフォルト情報が表示されない 711
8.5.6.1.15.4. Windows Server 2012 NIC チーミングの問題 713
8.5.6.1.16. Windows Server 2016 固有の問題 715
8.5.6.1.16.1. 偶発的なジョブ作成の失敗 716
8.5.6.1.16.2. ファイルサーバーの役割を作成するとサーバー マネージャーまたはフェールオー

バー クラスター マネージャーを使用して WSFC 2016 ファイル共有を作成できない 717
8.5.6.2. 制限事項 718
8.5.6.2.1. Bitlocker は DataKeeper をサポートしていない 719
8.5.6.2.2. CHANGEMIRRORENDPOINTS 720
8.5.6.2.3. CHKDSK 721
8.5.6.2.4. DataKeeper ボリュームのサイズ変更の制限事項 722
8.5.6.2.5. 再配置の前にビットマップ用ディレクトリを作成する必要がある 723
8.5.6.2.6. 同一ジョブ内で IP アドレスの重複は認められない 724
8.5.6.2.7. 同期レプリケーションによる大量の I/O 725
8.5.6.2.8. リソースタグ名の制限 726
8.6. トラブルシューティング 727
8.6.1. LifeKeeper および DataKeeper for Windows のアンチウイルスソフトウェアの除外リスト 729
8.6.2. アプレットのトラブルシューティング 730
8.6.3. LifeKeeper で OpenJDK をデプロイする 731
8.6.4. コマンドプロンプトから SIOS Protection Suite コマンドを実行しようとしたときにエラーが発生する 732
8.6.5. GUI エラーメッセージ 733
8.6.6. GUI ネットワーク関連 – サーバへの初期接続の失敗 (エラー 117) 735
8.6.7. GUI ネットワーク関連 – Windows プラットフォーム上の長期接続遅延 736
8.6.8. GUI ネットワーク関連 – 接続試行時に生成される NoRouteToHostException メッセージ 737
8.6.9. GUI ネットワーク関連 – 接続試行時に生成される不明なホスト例外メッセージ 738
8.6.10. GUI サーバのトラブルシューティング 741
8.6.11. エラーが出力されずに LifeKeeper GUI アプリケーションの起動に失敗する 742
8.6.12. Java 1.8.xのLifeKeeper GUI問題 744
8.6.13. ヘルスチェックタイムアウト 745
8.6.14. 不完全なリソースの作成 747
8.6.15. インストール – アクセス拒否 748
8.6.16. IP リソース作成問題 749
8.6.17. Java の署名があるコードとないコードの混在の警告 750
8.6.18. 参照リストに LANMAN 名が 2 回表示される場合がある 752
8.6.19. ライセンス – ライセンスされたリカバリキットリソースが起動しない 753
8.6.20. ライセンス – ライセンスキーが見つからない 754
8.6.21. SIOS Protection Suite Web クライアントがロックされる場合がある 755
8.6.22. SIOS Protection Suite Web クライアントがロックされる場合がある – 既存の階層が複数変更された 756
8.6.23. 新しい評価ライセンスキーのエラー 757
8.6.24. 1 × 1 構成における SIOS Protection Suite のサーバ障害からの復旧 758
8.6.25. サービス休止中の階層のリカバリ 766
8.6.26. LifeKeeper から DataKeeper ストレージを削除する 767
8.6.27. リカバリキットのアンインストール時に Remove がハングする 769
8.6.28. 複製ボリュームのスイッチオーバの失敗 770
8.6.29. リソースタグ名の制限 771
8.6.30. リストアおよびヘルスチェックアカウントの障害 772
8.6.31. SQL 2008 773
8.6.32. SQL Server Reporting Services (MSSQLSERVER) 774

8.6.33. 2 サーバクラスタの問題 775
8.6.34. 不明なユーザ名または誤ったパスワード 776
8.6.35. Web クライアントのトラブルシューティング 777
8.6.36. Win2008 – IIS リソース階層作成エラー 778

9. アプリケーションリカバリーキット 779
9.1. はじめに SIOS Protection Suite Microsoft SQL Server 780
9.1.1. SQL Server サービス 781
9.1.2. リカバリキットの要件 782
9.1.3. SQL Server のインストール 783
9.1.3.1. リカバリキットのインストール 784
9.1.3.2. キットの削除 785
9.1.3.3. SIOS Protection Suite とともに SQL Server をインストールおよび設定する 786
9.1.3.4. インストール – 共有ストレージシステム 787
9.1.3.5. ターゲットシステムで管理者ではないローカルシステムアカウントを使用する 789
9.1.3.6. インストール – 複製ストレージシステム 790
9.1.3.7. 拡張構成の追加のセットアップ作業 792
9.1.3.8. SQL 階層の作成 793
9.1.3.9. SQL 階層の拡張 795
9.1.3.10. SQL 階層の拡張解除 796
9.1.3.11. SQL 階層の削除 797
9.1.4. SQL Server 設定上の考慮事項 798
9.1.4.1. SQL Server の設定管理 801
9.1.4.2. プロセス設定メニュー 802
9.1.4.3. データベース設定メニュー 803
9.1.4.4. 管理操作メニュー 804
9.1.4.5. 管理ユーザメニュー 805
9.1.4.6. SQL リソース階層のテスト 806
9.1.5. SQL Server 階層の管理 807
9.1.5.1. 保護されたコミュニケーションパス経由でアクセスする 808
9.1.5.2. リモートアクセスにリソース名を使用する 809
9.1.5.3. ボリュームを SQL 専用にする 810
9.1.5.4. SQL Server 環境での手動スイッチオーバの制限について 811
9.1.5.5. Microsoft SQL Management ツールの実行 812
9.1.5.6. SQL Server の起動と停止は SIOS Protection Suite 上で実行する 813
9.1.5.7. Microsoft SQL Server ボリュームの追加 814
9.1.5.8. スイッチオーバ後にデータベースの「Suspect」状態から回復 815
9.1.5.9. Microsoft SQL Server (MSSQLServer) の一時停止 816
9.1.5.10. 切り替え可能な IP アドレスで接続するように SQL Server を設定 817
9.1.5.11. SQL Server のログインおよびパスワードの管理 818
9.1.5.12. SQL 階層の監視 819
9.1.6. トラブルシューティング 820
9.1.6.1. マスタ、あるいはユーザデータベースがシステムドライブにある場合リソースの作成や拡張に失敗する 821
9.1.6.2. SQL リソースの拡張に失敗する 822

9.1.6.3. 名前付きインスタンスで SQLAgent サービスを開始できない ... 823
9.1.6.4. SQL Server の名前付きインスタンスへの ODBC クライアントの接続 ... 824
9.2. はじめに SIOS Protection Suite PostgreSQL サーバー ... 825
9.2.1. PostgreSQL サーバーのインストール ... 826
9.2.1.1. インストールと設定の詳細 – 既存の PostgreSQL の構成に LifeKeeper を追加する ... 827
9.2.1.2. インストールと設定 – 既存の LifeKeeper 構成に PostgreSQL を追加する ... 830
9.2.1.3. 拡張設定のための追加のセットアップ作業 ... 832
9.2.2. PostgreSQL サーバーの設定に関する考慮事項 ... 834
9.2.2.1. PostgreSQL 階層の作成 ... 838
9.2.2.2. PostgreSQL 階層の拡張 ... 841
9.2.2.3. PostgreSQL 階層の拡張解除 ... 842
9.2.2.4. PostgreSQL 階層の削除 ... 843
9.2.2.5. PostgreSQL リソース階層のテスト ... 844
9.2.3. PostgreSQL サーバー階層の管理 ... 845
9.2.3.1. 保護されたコミュニケーションパス経由でのアクセス ... 846
9.2.3.2. PostgreSQL を排他的に使用するためのボリュームの予約 ... 847
9.2.3.3. SIOS Protection Suite 経由のみでの PostgreSQL サーバーの起動と停止 ... 848
9.2.3.4. 追加の PostgreSQL データベースクラスターの作成と保護 ... 849
9.2.3.5. PostgreSQL 管理ログイン ... 850
9.2.3.6. 自動接続設定 ... 851
9.2.3.7. Postmaster のポート引数設定 ... 853
9.2.3.8. PostgreSQL 階層の監視 ... 855
9.2.4. トラブルシューティング ... 856
9.2.4.1. 作成の失敗 ... 857
9.2.4.2. リストアの失敗 ... 858
9.2.5. PostgreSQL Recovery Kit の変更可能な設定 ... 859
9.3. はじめに SIOS Protection Suite Oracle ... 861
9.3.1. Oracle の概要 ... 862
9.3.2. Oracle サービス ... 864
9.3.3. Oracle リソース階層 ... 865
9.3.4. リカバリキットの要件 ... 866
9.3.5. Oracle のインストール ... 867
9.3.5.1. リカバリキットのインストール ... 868
9.3.5.2. Oracle とともに LifeKeeper をインストールおよび設定する ... 869
9.3.5.3. Oracle をインストールする前に ... 870
9.3.5.4. Oracle のインストール ... 872
9.3.6. Oracle 設定タスク ... 875
9.3.6.1. Oracle 階層の作成 ... 876
9.3.6.2. Oracle 階層の拡張 ... 878
9.3.6.3. Oracle 階層の拡張解除 ... 879
9.3.6.4. Oracle 階層の削除 ... 880
9.3.6.5. Oracle データベースの設定管理 ... 881
9.3.6.6. Oracle Multitenant 構成による Pluggable Database の設定 ... 883
9.3.6.7. Pluggable Database の移行 ... 887
9.3.6.8. Oracle リソース階層のテスト ... 890

9.3.7. Oracle 階層の管理 ... 891
9.3.7.1. Oracle 階層の管理に関するガイドライン ... 892
9.3.7.2. LifeKeeper Oracle Recovery Kit の変数 ... 893
9.3.7.3. LifeKeeper で使用する Oracle ユーザ名とパスワードの更新 ... 894
9.3.7.4. 手動による Oracle 11g DB Console の設定 ... 895
9.3.8. Oracle のトラブルシューティングのヒント ... 896
9.3.8.1. 階層の作成に失敗した ... 897
9.3.8.2. サービス開始に失敗した ... 898
9.3.8.3. Oracle TNSListener Service が必要に応じて起動または停止しない ... 899
9.3.8.4. サーバが応答しない ... 900
9.3.8.5. リモートユーザが ORA 12504、ORA 12514、ORA 12541 の理由でログインできない ... 901
9.4. はじめに SIOS Protection Suite Microsoft Internet Information Services ... 902
9.4.1. IIS の概要 ... 903
9.4.2. IIS のインストール ... 904
9.4.2.1. ハードウェアとソフトウェアの要件 ... 905
9.4.2.2. キットのインストール ... 907
9.4.2.3. キットの削除 ... 908
9.4.2.4. 構成の定義と制限 ... 909
9.4.2.5. IIS 構成の考慮事項 ... 910
9.4.2.6. LifeKeeper とともに IIS をインストールおよび設定する ... 913
9.4.2.7. SIOS Protection Suite およびリカバリキットのインストールと設定 ... 914
9.4.2.8. 全サーバでの Microsoft IIS のインストールと設定 ... 916
9.4.2.9. SMTP 仮想サーバのインストールと設定 ... 918
9.4.3. IIS の構成の定義と制限 ... 920
9.4.3.1. IIS の必要な役割、役割サービス、および機能 ... 921
9.4.3.2. IIS アクティブ / アクティブ設定 ... 922
9.4.3.3. プライマリとバックアップの指定 ... 923
9.4.3.4. 命名規約 ... 924
9.4.3.5. 同一のプライマリ/バックアップ Web サイト ... 925
9.4.3.6. 安全なサーバの構成 ... 926
9.4.3.7. IIS 設定 ... 927
9.4.3.8. ドキュメントコンテンツの場所 ... 928
9.4.3.9. 複数の IIS サイトで異なるボリュームを使用する ... 929
9.4.4. IIS リソースの設定タスク ... 930

10. IIS リソース階層の作成 ... 931

11. IIS リソース階層の拡張 ... 932

12. IIS リソース階層の削除 ... 933

13. IIS リソース階層の拡張解除 ... 934

14. IIS リソース階層のテスト ... 935
14.1. GUI からの手動スイッチオーバの実行 ... 936
14.2. リカバリ操作 ... 937

15. IIS 階層の管理 ... 938

15.1. クイックチェック間隔、ディープチェック間隔、ローカルリカバリの設定変更 939
15.2. 手動スイッチオーバ 940
15.3. IIS のフェイルオーバ 941
15.4. 匿名接続を使用できない FTP サイトを保護する場合 942
15.5. FTP ログインスクリプトを使用する 943
15.6. FTP のディープチェックを無効にする 944
15.7. LifeKeeper Microsoft IIS Recovery Kit 構成の変更 945
15.8. Microsoft IIS の削除 946
15.9. ネットワークインターフェースカード (NIC) の変更 947

16. IIS のトラブルシューティング 948
16.1. 現象と解決策 949

17. SIOS Protection Suite for Windows サポートマトリックス 950

18. プロダクトライフサイクル 956

19. LifeKeeper Single Server Protection for Windows 957
19.1. LifeKeeper Single Server Protection for Windows リリースノート 959
19.2. LifeKeeper Single Server Protection for Windowsインストレーションガイド 964

20. LifeKeeper Single Server Protection for Windows テクニカルドキュメンテーション 965
20.1. ドキュメンテーションとトレーニング 967
20.2. VMware HA との統合 969
20.3. 管理 970
20.3.1. LifeKeeper Single Server ProtectionとVMware HAの統合を有効にする 971
20.3.2. VMware HAの障害検出の有効化とリカバリシナリオ 972
20.3.3. VMware HAを使用したLifeKeeper Single Server Protectionハートビート 974
20.3.4. LifeKeeper Single Server Protection で保護されているシステムのメンテナンス 975
20.4. アプリケーションリカバリーキット 976

1. SIOS Protection Suite for Windows

SIOS Protection Suites および DataKeeper Cluster Edition の情報リソース

SIOS Technology Corp. は、SIOS Protection Suites のサポートされているすべてのバージョンのドキュメントを維持・管理しています。
私たちは、お客様からの提案やフィードバックを継続的なドキュメントの改善に役立てたいと考えています。ぜひ簡単なドキュメントフィードバック調査にご協力ください。

2. SIOS Protection Suite for Windows リリースノート

SIOS Protection Suite for Windows

リリースノート

バージョン 8.7.2

(Version 8 Update 7 Maintenance 2)

リリース日:2020/11/20

重要!!

本製品をインストールまたは使用する前に、必ずこのドキュメントをお読みください!
このドキュメントには、インストール時とその前後に留意すべき重要な項目に関する情報が記載されています。

出版物の品質を維持するために、出版物の正確さ、わかりやすさ、構成、および価値に関するお客様のご意見をお寄せください。

はじめに

このドキュメントは SIOS Protection Suite for Windows 製品のインストールや設定、管理を行う担当者向けのものであり、バージョン要件、説明や手順に対する最新の変更内容、製品の制限事項、既知の問題などの重要な情報が記載されています。SIOS Protection Suite ソフトウェアをインストールして設定する前に、必ずこのドキュメントの内容を確認してください。

SIOS Protection Suite 製品の説明

SIOS Protection Suite for Windows は、ミッションクリティカルデータおよびアプリケーションを保護し、DataKeeper (DK)、LifeKeeper (LK)、オプションのリカバリキットを含む高可用性とデータ複製機能を統合したバンドルソフトウェアです。

LifeKeeper for Windows

LifeKeeper for Windows はミッションクリティカルなアプリケーションに対して世界に通用する信頼性を提供する

という SIOS Technology Corp. の伝統を継承しています。LifeKeeper for Windows は、アプリケーションの監視およびリストアを行うために、高可用性プラットフォームに関する 10 年にわたる経験を活用して複数のサーバをクラスタ化する機能をお客様に提供します。障害が発生した場合、LifeKeeper はすべてのネットワークインターフェース、データ、およびアプリケーションを復旧します。復旧は自動的に行われ、クライアントに対しては透過的であるため、ダウンタイムと営業的損失を最小限に抑えます。

LifeKeeper for Windows は、システムまたはアプリケーションの障害時だけでなく、計画したダウンタイム時にも継続的に動作させることができます。LifeKeeper を使用すると、一般的なメンテナンス作業やアップグレードに必要なダウンタイムを大幅に軽減したり、ダウンタイムをなくしたりすることができます。

DataKeeper for Windows

SIOS DataKeeper は、最適化されたホストベースのレプリケーションソリューションとして、ソースサーバから 1 台以上のターゲットサーバにネットワーク経由で可能な限り高速かつ効率的にデータを複製します。

SIOS Protection Suite for Windows Version 8 の新機能

機能	説明
本バージョンでの新機能	
OpenJDK 15	SIOS Protection Suite for Windows は、OpenJDK15 をサポートし、同梱するようになりました
Oracle Pluggable Database Recovery Kit	Oracle プラガブルデータベースをサポートするようになりました
全体的なメンテナンス	下記の バグ修正 を参照してください。
バージョン 8.7.1 の新機能	
全体的なメンテナンス	バグ修正
バージョン 8.7 の新機能	
Microsoft SQL Server 2019 のサポート	SIOS Protection Suite for Windowsは、Microsoft SQL Server 2019をサポートするようになりました。 制限事項: • オプションの Reporting Services の保護は提供しません。 • 新しいSQL Server機能はサポートしません。 • Server 2016 プラットフォーム以上でのサポートになります。

AWS Nitro システム	SIOS Protection Suite for Windowsは、AWS Nitro システムをサポートするようになりました。
Windows 2019 対応	Secure Boot が有効になっている Windows 2019 をサポートするようになりました
64-bit Java	SIOS Protection Suite for Windows は、32ビット版と64ビット版の両方のJava ランタイム環境をサポートするようになりました
OpenJDK 12	SIOS Protection Suite for WindowsはOpenJDK 12をサポートし、同梱するようになりました
Oracle 19c	SIOS Protection Suite for Windows は Oracle 19c をサポートするようになりました
EnterpriseDB v11 と v12	SIOS Protection Suite for Windows は EnterpriseDB v11 と v12 をサポートするようになりました
全体的なメンテナンス	バグ修正
バージョン 8.6.4 の新機能	
Windows 2019 対応	SIOS Protection Suite for Windows は Windows 2019 をサポートします (v8.6.4 のみの制限事項)
書き込みキューが上限に達したときに書き込みを遅らせます	チューニング可能な BlockWritesOnLimitReached を導入しました。これは、ミラーのキューが HighWater または ByteLimit に達した場合にミラーを一時停止して再同期状態にするのではなく、書き込みを遅らせるようにします。
PostgreSQL 11 のサポート	SIOS Protection Suite for Windows は PostgreSQL 11 をサポートします
Oracle 18c のサポート	SIOS Protection Suite for Windows は Oracle 18c をサポートします
全体的なメンテナンス	バグ修正
バージョン 8.6.3 の新機能	
Queue Current Age（キューの現在の待ち時間）の追加	このパフォーマンスモニタのカウンタ値は書き込みキュー内の最も古い書き込み要求の経過時間です。
全体的なメンテナンス	バグ修正
バージョン 8.6.2 の新機能	
SIOS iQとの統合	SIOS iQにイベントを配信するDataKeeper Signalパッケージを追加しました。
全体的なメンテナンス	バグ修正
バージョン 8.6.1 の新機能	
Microsoft SQL Server 2017 のサポート	SIOS Protection Suite SQL Server Recovery KitはMicrosoft SQLServer 2017をサポートします。
全体的なメンテナンス	バグ修正
バージョン 8.6 の新機能	
VSS プロバイダ	デフォルトでは SIOS VSS プロバイダーは無効になっています。
PostgreSQL のサポート	PostgreSQLデータベースクラスターの保護を提供する、新しいSIOS Protection Suite for WindowsコアのApplication Recovery Kitを追加しました。
Windows 2016 のサポート	SIOS Protection Suite for Windowsは、Windows 2016をサポートします。
チューニング可能な書き込みキューのバイト制限	ユーザーは、WriteQueueByteLimitMB のレジストリ値を変更することにより、ミラーの書き込みキューに割り当て可能な最大バイト数を指定できます。

全体的なメンテナンス	バグ修正
バージョン 8.5 の新機能	
CHANGEMIRRORTYPE	この EMCMD コマンドを使用して、DataKeeper ジョブの一部であるミラーのミラータイプを変更します。
Microsoft SQL Server 2016 のサポート	DataKeeper は Microsoft SQL Server 2016 をサポートします。
ビットマップブロックサイズを変更可能	ユーザーは、BitmapBytesPerBlock レジストリの値を変更して、DataKeeper インテントログ（ビットマップ）のエントリーの実効サイズを変更できます。
全体的なメンテナンス	バグ修正
バージョン 8.4 の新機能	
ターゲットビットマップファイル	ターゲットの書き込みがビットマップファイルで追跡されるようになりました。
全体的なメンテナンス	バグ修正
バージョン 8.3 の新機能	
DataKeeper の通知アイコン	DataKeeper の通知アイコンは、Windows の通知トレイで DataKeeper　ミラーのサマリを表示します。また、DataKeeper ミラー管理のショートカットとして、使用可能です。
Oracle 12c と Oracle 12c Standard Edition 2	SIOS Protection Suite for Windows Version 8.3 以降、Oracle 12c および Oracle 12c Standard Edition 2 (ASM およびpluggable database を除く)　をサポートします。
Powershell cmdlet サポート	ジョブの作成、ミラーの作成、ジョブの削除、ミラーの削除、または DataKeeper (New-DataKeeperMirror、New-DataKeeperJob、Remove-DataKeeperMirror、Remove-DataKeeperJob, Add-DataKeeperJobPair, Get-DataKeeperVolumeInfo)　で使用されるボリュームについての情報を取得するのに Powershell cmdlet が使用可能になりました。
mirrorcleanup.cmd	このコマンドは、ローカルシステム上のみで、選択されたボリュームの残りすべてのミラーを削除します。SIOS サポートによって推奨された場合のみ実行してください。
DKHEALTHCHECK	ステータスと問題の識別ツールをサポートしました。基本のミラーステータスと問題検知のためのコマンドラインインターフェースを提供します。
全体的なメンテナンス	バグ修正
バージョン 8.2.1の新機能	
全体的なメンテナンス	バグ修正
バージョン 8.2の新機能	
全体的なメンテナンス	バグ修正
バージョン 8.1の新機能	
Microsoft Windows Server 2012 R2のサポート	LifeKeeper バージョン 8.1 以降で Windows Server 2012 R2 がサポートされます。
全体的なメンテナンス	バグ修正
バージョン 8.0.1の新機能	
全体的なメンテナンス	バグ修正
バージョン 8.0の新機能	

全体的なメンテナンス	バグ修正

SIOS Protection Suite for Windows v8 で廃止になった機能

機能	説明
本リリースで廃止になった機能	
	ありません
バージョン 8.7.1 で廃止になった機能	
	ありません
バージョン 8.7.0 で廃止になった機能	
	ありません
バージョン 8.6.4 で廃止になった機能	
	ありません
バージョン 8.6.3 で廃止になった機能	
データリワインド	SPS for Windows からリワインド機能を削除しました。

バグの修正

以下に、最新のバグの修正および機能強化のリストを示します。

	説明
PW-932	リソースのフェールオーバー中に削除の失敗を無視する問題を修正しました
PW-1061	SQL Server 管理者パスワードの特殊文字に対応するようにしました
PW-1280	LK SQL Optional Services は、SQL 2017 および SQL 2019 Reporting Services をサポートするようになりました
PW-1393	LK 起動時の Cygwin DLL ロードアドレスの競合の検出と解決を行います
PW-1464	ソースのサイズ変更後、ターゲット上のファイルシステムの状態が RAW になる問題を修正しました
PW-1564	ユーザーが匿名の DkSvcPipe アクセスを無効にできるようにする設定を追加しました
PW-2453	Oracle リスナーサービスが終了した場合のリカバリーアクションを改善しました
PW-2505	SQL Server のクイックチェックスクリプトがアップデートされ、誤ったサービス障害検知を回避できるようになりました
PW-2738	ボリュームにアクセスできない場合に、起動時に filesys 情報の取得を再試行するオプションを追加しました
PW-2885	lkGUIserver java プロセスでのハンドルリーク - JDK 15 にアップデートしました

製品要件

オペレーティングシステム

重要: SIOS Protection Suite を実行するすべてのサーバでローカル管理者権限を持ったドメインアカウントを使用することを推奨します。ローカルアカウントを使用している場合、ユーザ名およびパスワードは SIOS Protection Suite を実行するすべてのサーバで一致しなければなりません。これはすべてのエディションおよびすべてのプラットフォームに該当します。

注記: クラスタ内のすべてのサーバで同一バージョンの Windows を実行してください。

製品	オペレーティングシステム	追加ソフトウェア
SIOS Protection Suite (サーバコンポーネント)	SPS サポートマトリックス を参照	なし
SIOS Protection Suite (ユーザインターフェース)	SPS サポートマトリックス を参照	MMC 3.0 – こちらからダウンロードしてください。 download.cnet.com/Microsoft-Management-Console-3-0-for-Windows-XP-KB907265/3000-2206_4-10741230.html
仮想環境	上記のオペレーティングシステムは以下の仮想プラットフォーム上で動作するゲストとしてサポートされています。仮想プラットフォームOSバージョンの詳細等につきましては こちら にお問い合わせください。 • Amazon EC2 (AWS) • VMware vSphere • Microsoft Hyper-V • Citrix XenServer • KVM with Kernel	
上記の OS プラットフォームすべての 64 ビットバージョン (x64。Itanium を除く) がサポートされます。		

要件

SIOS Protection Suite を Windows 2008 にインストールするとき、以下に説明するようにシステム設定を変更するかどうかを確認するダイアログボックスが表示されます。インストーラで変更できない場合は、インストールが終了してから手動で変更する必要があります。

- Windows ファイアウォール
- **Distributed Link Tracking Client** を 無効 にする

SIOS Protection Suite for Windows および Microsoft FTP Service 7.5 for IIS 7.0 を実行するシステムの場合は、Windows 2008 R2 以降が必要です。

さらに、Windows サーバがドメイン内にない場合は、ローカルセキュリティポリシー設定 **[ネットワークアクセス: Everyone アクセス許可を匿名ユーザーに適用する]** を有効にする必要があります。サーバがドメイン内にある場合、この設定は必要ありません。

SIOS Protection Suite の要件

以下の表に、SIOS Protection Suite core およびリカバリキットに該当する要件を示します。

Core	要件
SIOS Protection Suite のライセンス	SIOS Protection Suite を実行するサーバごとに 1 つのライセンスが必要です。これは物理サーバおよび仮想サーバの両方に適用されます。
LAN Manager リカバリキット	「 **Microsoft ネットワーク用ファイルとプリンタ共有** 」コンポーネント (lanmanserver) を Windows サーバにインストールする必要があります。NetBIOS も有効にする必要があります。そうしないと、LAN Manager リソースは起動しません。
メモリ要件	SIOS Protection Suite for Windows をサポートするシステムに必要な最小メモリ容量は、使用しているオペレーティングシステム のメモリ要件に基づいて決まります。ユーザアプリケーションを実行するには SIOS Protection Suite に必要なメモリ以外に追加のメモリが必要です。
GUI	**ポート:** SIOS Protection Suite は、GUI サーバと GUI クライアントの間の Remote Method Invocation (RMI) 通信にポート 82 を使用します。 LifeKeeper GUI は管理 Web サーバにポート 81 を使用します。管理 Web サーバはパブリック Web サーバとは別のものにする必要があります。これはリモートクライアント上で Java アプレットとして実行する場合に GUI で使用されます。 既存のアプリケーションと競合する場合、これらのポートを変更するには、SIOS\LIFEKEEPER\JAVAGUI\SERVER レジストリキーの RMI_PORT または WEB_PORT エントリを編集します。

DataKeeperのシステム要件

メモリ – ミラーまたはジョブが構成されていないこと。

ベースラインメモリ使用量:

Emtray.exe = 7,560 KB
Extmirrsvc.exe = 2,504 KB
Mmc.exe = 56,944 KB
Poolmon.exe(EmDB & EmMi) = 102.704 KB
Extmirr.sys = 367 KB

プロセッサ要件 – Windowsプロセッサ要件 を参照してください。

合計 = 167,277.7KB または 167.28 MB

インストールに必要なディスク容量

667 MB

注記:メモリとCPUの使用量は、ミラーの数、サイズ、および書き込み動作に応じて増加します。

オプションのリカバリキット

SIOS Protection Suite とオプションの SIOS Protection Suite リカバリキットを連携させるにはソフトウェアライセンスキーが必要です。

ARK 名	バージョン名/要件
Microsoft SQL Server リカバリキット	SPS サポートマトリックス を参照
Oracle リカバリキット	SPS サポートマトリックス を参照

GUI の要件、プラットフォーム、およびブラウザ

LifeKeeper を使用するには、各サーバに Java Runtime Environment (JRE) をインストールする必要があります。64 ビットの Windows Java OpenJDK v15.0.1 が SIOS Protection Suite Core ソフトウェアとともにインストールされます。Java OpenJDK v15.0.1 は LifeKeeper GUI サーバおよび GUI アプリケーションコンポーネントについて十分にテストされています。

SIOS Protection Suite クラスタの外部のシステムから SIOS Protection Suite を管理するには、SIOS Protection Suite Web クライアントを実行します。以下の表に、SIOS Protection Suite Web クライアントがサポートされるプラットフォームとブラウザのリストを示します。サーバの場合と同様に Java OpenJDK v15.0.1 でテストしていますが、将来の JRE の更新でもクライアントは同様に動作するはずです。クライアントの JRE を更新してもそのマシンにしか影響しないので、安全性のテストはサーバの JRE を更新する場合ほど危険ではありません。Oracle は JRE1.9よりアプレットのサポートを廃止し、現行バージョンの JRE ではサポートされていません。Web クライアントのサポートが必要なシステムでは、バージョン JRE1.8.0_211 を使用することを推奨します。また、コミットする前に更新をテストし、問題が発生した場合にはロールバックできるよう準備することをお勧めします。

オペレーティングシステム	Internet Explorer 5.5+、6.0	Internet Explorer 7.0、8.0	Internet Explorer 9.0	Internet Explorer 10.0	Internet Explorer 11.0	Mozilla Firefox 1.5、2	Mozilla Firefox 3
Windows 2019					X		
Windows 2016				X	X		
Windows 2012 R2				X	X		
Windows 2012				X	X		
Windows 2008 R2		X					
Windows 7		X					
Linux	なし	なし	なし	なし	なし	X	X

注記: SIOS Protection Suite Web クライアントはその他の最新のプラットフォームおよびブラウザで動作すると思われますが、SIOS Technology Corp はテストしていません。

SIOS Protection Suite for Windows のインストールと削除

SIOS Protection Suite for Windows は InstallShield を使用して標準のインストールインターフェースを提供しており、**標準** 、**コンパクト** 、**カスタム** のインストールを選択できます。SIOS Protection Suite ソフトウェアのインストール、削除、またはアップグレードの詳細については、SIOS Protection Suite インストレーションガイド を参照してください。

重要

- SIOS Protection Suite スクリプトに対して行ったカスタマイズは、SIOS Protection Suite for Windows v8 のすべてのリリースでアップグレードした後に再度適用する必要があります。
- 適切なライセンスを取得していることを確認してください。古いライセンスはシステム上に残ります。ライセンスインストーラツールで削除することができます。
- SIOS では SIOS Protection Suite を 2 つ以上前のメジャーバージョンからアップグレードすることをサポートしていません。LifeKeeper for Windows v7.x よりも前のバージョンから SIOS Protection Suite for

> Windows v8.x にアップグレードする場合は、古いバージョンの LifeKeeper をアンインストールしてから SIOS Protection Suite for Windows v8.x を再インストールしてください。

技術的な注意事項

lkstart

このプログラムは、LifeKeeper が実行されていない場合に現在のシステム上で LifeKeeper を起動します。lkstart 実行すると、LifeKeeper デーモンが停止した場合に再起動されるように、LifeKeeper デーモンに属する *%LKROOT%\etc\LKinit.config* ファイルのエントリが修正されます。

–w オプションを使用すると、タイムアウト間隔を変更できます。waitperiod には、秒数を指定します。起動前の wait period (待機時間) を指定するには –w 引数を使用します。

LifeKeeper サービスは、管理ツールにある Microsoft Services mmc を使用して起動することも、コマンドプロンプトから “sc start LifeKeeper” または “net start LifeKeeper” のいずれかを使用して起動することもできます。

注記: このプログラムはコンソールから実行する必要があります。

SIOS Protection Suite によって保護されているボリュームで CHKDSK.EXE を実行する

Microsoft では、正常にシャットダウンされなかったボリュームに chkdsk.exe ユーティリティを実行して、ファイルシステムまたはディスクのエラーのチェックと修正を行うことを推奨しています。しかし、エラーの程度によっては、ユーティリティの処理が完了するまでに非常に長い時間がかかる場合があります。chkdsk でボリュームを完全にチェックするには数時間、または数日かかることもあります。また、ボリュームをチェックしている間にハングする場合もあります。このような理由により、SIOS Protection Suite は保護されているボリュームで `chkdsk` ユーティリティを実行しません。SIOS Protection Suite は、ボリュームの使用を開始する前に Microsoft の chkntfs.exe ユーティリティを実行してボリュームに不正がないかチェックします。保護されているボリュームに不正が見つかった場合、SIOS Protection Suite はイベントログにエラーを記録します。

ボリュームリソースを使用しているサーバ上の SIOS Protection Suite によって保護されているボリュームで、管理者が定期的に **chkdsk** を実行することを推奨します。chkdsk を実行する前に、ボリュームリソースを使用しているすべてのアプリケーションを終了してください。

SIOS Protection Suite で保護されたボリュームでのシステムブート中に CHKDSK.EXE を実行する

LifeKeeper と DataKeeper はボリュームをロックできることが要求されるため、SIOS Protection Suite によって保護されているボリュームで通常、システム起動時に chkdsk ユーティリティを実行するのは適切ではありません。

SIOS Protection Suite によって保護されているボリュームを起動時にチェックする必要がある場合は、アクティブノードで以下の手順を実行します。

ミラーボリュームまたは SDRS ボリュームの場合 (1 つのサイトで共有され、リモートサイトに複製される)

1. “%ExtMirrBase%\emcmd” . getconfiguration <drv> (再起動後に使用するために出力の 1 行目に表示される数を保存)
2. `"%ExtMirrBase%\emcmd" . setconfiguration <drv> 32`
3. `"%LKBIN%\lkstop" -f`
4. `sc stop ExtMirrSvc`
5. `sc config lifekeeper start= demand`
6. `sc config ExtMirrSvc start= demand`
7. `chkntfs /D`
8. `chkntfs /c <drv>`
9. reboot

   再起動後に以下の手順を実行します。
10. `sc config lifekeeper start= auto`
11. `sc config ExtMirrSvc start= auto`
12. `sc start ExtMirrSvc`
13. `"%ExtMirrBase%\emcmd" . setconfiguration <drv>` (手順 1 で emcmd getconfiguration によって報告された数)
14. reboot

共有ボリュームの場合

1. `"%LKBIN%\volume" -U <drv>`
2. `"%LKBIN%\lkstop" -f`
3. `chkntfs /c <drv>`
4. reboot

再起動後に以下の手順を実行します。

5. "%LKBIN%\volume" -p <drv>
6. "%LKBIN%\lkstop" -f
7. "%LKBIN%\lkstart"

複製ボリュームの場合

1. "%LKBIN%\lkstop" -f
2. chkntfs /D
3. chkntfs /c <drv>
4. reboot

ファイバチャネル上のコミュニケーションパス

共有ストレージを使用して SIOS Protection Suite クラスタを構築する場合、クラスタ内のノード間でコミュニケーションパスを常に使用できるようにしておくことが重要です。コミュニケーションパスは、TCP 通信プロトコルを使用して作成する必要があります。通常、TCP コミュニケーションパスはイーサネットネットワークデバイス上に構築されます。ただし、SIOS Protection Suite では、TCP プロトコルを実行できる接続であればどのような種類でも使用できます。ファイバチャネル SAN を使用して共有ストレージクラスタを作成している場合は、SIOS Protection Suite コミュニケーションパスとしてファイバチャネル SAN を使用することができます (望ましいです)。

QLogic は、QLogic ファイバチャネルストレージアダプタで TCP/IP プロトコルを実行することもできるように、Windows 用のミニポートドライバと IP ドライバを提供しています。これにより、QLogic ファイバチャネルアダプタは、実質的にストレージアダプタおよびネットワークアダプタとして動作できるようになります。このドライバが用意されていれば、QLogic カードは他のネットワークカードと同様に、標準のネットワーク設定技法を使用して設定できます。

QLogic のドライバは、以下の Web サイトからダウンロードできます。

http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/DefaultNewSearch.aspx

SIOS Protection Suite で iSCSI ストレージを使用する

iSCSI ストレージを共有ストレージとして使用して、SIOS Protection Suite で保護することができます。共有ストレージ環境では、すべてのサーバイニシエータがそのディスクにアクセスできるように iSCSI ターゲットデバイスを設定する必要があります。iSCSI ストレージデバイスのベンダは、iSCSI デバイスの設定に必要なインターフェースとコマ

ンドを提供しています。Microsoft iSCSI Initiator サービス (MSiSCSI) への依存関係を LifeKeeper サービスに追加する必要があります。これにより、LifeKeeper が共有ボリュームにアクセスしようとする前に、そのボリュームを使用できるようになります。

LifeKeeper サービス用に MSiSCSI への依存関係を作成するには、レジストリエディタ “*regedt32.exe*” を使用して、*HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LifeKeeper* で LifeKeeper サービスを表すサブキーを選択します。サービスキーは “DependOnService” という値名で “EISM” という値を 1 つ持っています。値名 “DependOnService” をダブルクリックして編集のために開きます。ダイアログボックスが表示されたら、新しい行に Microsoft iSCSI Initiator サービスのサービス名 “MSiSCSI” を追加して、**[OK]** をクリックします。

依存関係が作成されたことを確認するには、*[管理ツール]* > *[サービス]* から MMC スナップインを開きます。LifeKeeper サービスに移動してダブルクリックすると **[プロパティ]** ダイアログボックスが表示されます。ダイアログボックスが表示されたら、**[依存関係]** ページに移動して、**[このサービスが依存するシステムコンポーネント]** フィールドに **“LifeKeeper External Interface”** と共に **“Microsoft iSCSI Initiator”** サービスがリストされていることを確認します。

クイックチェックとディープチェックのシステム負荷に関する考慮事項

SIOS Protection Suite は、システム内の保護対象リソースごとに個別の監視用スレッドを起動します。これらのスレッドは互いに独立して動作します。通常、Quickcheck と Deepcheck のスクリプト実行によるシステム負荷はランダムに分散されます。SIOS Protection Suite は、Quickcheck と Deepcheck が同一リソースに対して同時に実行されるように予定されている場合に、Quickcheck の実行をスキップすることでリソース監視による負荷を分散するという処理も行っています。ただし、チェックの負荷はランダムに分散されるため、リソース監視によるシステム負荷がピークに達することがあります。システム内で保護されるリソースが増えるほど、ピークが大きくなり、ピークに達する頻度も高くなります。ピークが最大になるのは、LifeKeeper を起動して、アクティブなリソースごとの Deepcheck スクリプトを最初に起動するときです。サーバがこの最初の負荷のピークを適切に処理できる場合は、その後パフォーマンスに関する問題が発生することはありません。

VSS シャドウコピー

SIOS Protection Suite で VSS シャドウコピーをサポートするには、SIOS Protection Suite によって保護されているボリュームにシャドウコピーを保存しないようにする必要があります。ただし、保護されていない別のボリュームにシャドウコピーを保存することはできます。

制限事項と既知の問題

制限事項

SIOS AppKeeper

SIOS LifeKeeperは、AWS EC2のクラスター環境でOSおよびアプリケーションサービスを監視・修復します。このため、これらの環境でSIOS LifeKeeperに加えてSIOS AppKeeperを使用することは、推奨もサポートもされていません。

アンチウィルスソフトウェア

アンチウィルスソフトウェアは、LifeKeeper のバイナリを誤ってマルウェアとして検出する場合があります。LifeKeeper ユーティリティが誤って隔離されないように、フォルダ LKROOT（デフォルトでは C:\LK ）をウィルスチェックの対象から除外するよう設定してください。

SCVMM 2012

SCVMM 2012 で DataKeeper を使用する場合は、SCVMM 2012 SP1 を使用する必要があります。

Microsoft Failover Clustering がインストールされたサーバ

Microsoft Cluster Server 機能または Microsoft Failover Cluster 機能がインストールされた Enterprise クラスサーバまたは DataCenter クラスサーバでは、SIOS Protection Suite はサポートされません。同一グループのサーバに 2 つの「クラスタ化」ソリューションを展開しないでください。この制限の一部として、Microsoft Failover Cluster Virtual Adapter (Virtual NIC) でホストされる IP アドレス (169.254.xxx.xxx) を使用した場合、LifeKeeper コミュニケーションパスは機能しません。

FAT ファイルシステムのサポート

SIOS Protection Suite では、FAT ファイルシステムまたは FAT32 ファイルシステムを使用するボリュームの保護はサポートされません。

フォールトトレラントディスクセット

SIOS Protection Suite 複製ボリュームは Windows フォールトトレラントディスクセット (ソフトウェア RAID) を使用してサポートされますが、SIOS Protection Suite 共有ボリュームは Windows フォールトトレラントディスクセットと互換性がありません。フォールトトレラントディスクセットは動的ディスクでセットアップする必要があり、動的ディスクは 2 つのシステム間で共有できません。

ファイル共有リカバリキット

- ファイル共有リカバリキットは、アクティブドメイン環境でのみサポートされ、ワークグループ環境では動作しません。ローカルユーザ ID は元のローカルシステムでのみ有効なので、ワークグループ環境またはドメイン環境では、ローカルマシンのアカウントに付与されたファイル共有権限はフェイルオーバ時に保持されません。そのため、ローカルユーザ ID は他のシステムでは認識されません。同じローカルユーザ ID を 2 台の異なるマシンで設定した場合でも、異なるアカウントとして扱われます。つまり、ローカルユーザ ID は元のシステムでのみ有効となります。一方、ドメインアカウントは、ドメイン内の任意のシステムで識別され、使用可能です。

- システム上で定義されているファイル共有が 9999 を超えている場合、ファイル共有リカバリキットは動作しません。ユーザ定義の共有の合計数が 9999 を超えている場合、SIOS Protection Suite の対象ファイル共有を保護しようとしても失敗します。この制限はファイル共有リソースを編集する場合にも当てはまります。システム上で定義されている共有が 9999 を超えている場合、保護されている共有のリストを変更することはできません。

LAN Manager リカバリキット

Microsoft は、ネットワークインターフェースカードごとに最初の IP アドレスでしか LAN Manager の機能をサポートしません (Microsoft bug SRX#9704116-48)。このため、SIOS Protection Suite によって保護されている IP アドレスでは LAN Manager の機能を使用することができません。したがって、TCP/IP プロトコルを使用してコンピュータの別名に切り替える方法は、クライアントに対して IP アドレスから LAN Manager 名に動的にマップできるようにするしかありません。解決策としては、WINS サーバの使用を推奨します。SIOS Protection Suite サーバ (および保護対象の LAN Manager 名にアクセスするすべてのコンピュータ) を同じ WINS サーバの WINS クライアントにする必要があります。

仮想メモリが少ないとシステムの状態が悪化する

SIOS Protection Suite は必要なときにメモリが使用できることを前提としています。システムの仮想メモリが少なくなっている場合は、すぐにその状態を解消する必要があります。

仮想メモリ不足により通信機能などシステム内部の機能の性能が低下したり処理が遅延したりすると、SIOS Protection Suite が誤動作する可能性が非常に高くなります。例えば、TCP/IP 通信リソースの deepcheck によって障害が間違って検出され、バックアップサーバへのリソースのフェイルオーバが発生する可能性があります。

クラスタ内の他のサーバと SIOS Protection Suite との通信性能が低下している場合、手動による切り替えが失敗することもありえます。ただし、これによって、サーバが完全にダウンしたときに保護されたリソースをフェイルオーバする SIOS Protection Suite の機能が影響を受けることはありません。

GUI の相互運用性

LifeKeeper GUI は、Windows サーバ上の SIOS Protection Suite の管理にのみ使用できます。SIOS Protection Suite for Linux のクラスタに接続して監視できることに注意してください。ただし、リソースの作成、プロパティの編集、サーバのサービス状態の切り替えなどの管理作業は、現時点ではサポートされて **いません** 。

シリアルポートコミュニケーションパスのサポート終了

SIOS Protection Suite は、バージョン 7.2 において、TTY コミュニケーションパスのサポートを終了しました。SIOS は推奨しませんが、現在 TTY コミュニケーションパスを使用している場合は、以下に示すように */etc/lkinit.config* ファイルの TTYCA.EXE の行の「#」を削除することにより、このオプションを再び有効にすることができます。

```
# … /bin/TTYCA.EXE|-t  1  X  X  X  X  X  X    <=
(TTY コミュニケーションパス無効)
  … /bin/TTYCA.EXE|-t  1  X  X  X  X  X  X    <=
(TTY コミュニケーションパス有効)
```

TTY コミュニケーションパス機能を有効または無効にする場合は、*lkinit.config* の編集後に LifeKeeper サービスを停止し、再起動する必要があります。LifeKeeper を停止するには、コマンド {c:\lk}\bin\lkstop.exe –f (c:\lk は LifeKeeper のインストールパス) を実行してください。GUI が停止され、関連するすべてのプロセスが停止されていることを必ず確認してください。LifeKeeper を再起動するには、{c:\lk}\bin\lkstart.exe と入力します。

TTY 技術は今後使用されなくなります。TTY コミュニケーションパスはサポート対象外で、TCP/IP コミュニケーションパスに差し替える必要があります。

コンソールアプリケーションの管理

Windows Server 2008 以降では、SIOS Protection Suite からのコンソールアプリケーションの起動はサポートされません。Server 2008 において UAC やメモリ管理などのサーバのアーキテクチャとセキュリティが改善されたため、SIOS Protection Suite のようなバックグラウンドプロセスからコンソールアプリケーションを起動することはできません。

Bitlocker は DataKeeper をサポートしない

Microsoft によると、Bitlocker はソフトウェア RAID 構成との連携をサポートしません。DataKeeper は本質的にソフトウェア RAID 1 であるため、Microsoft は Bitlocker と DataKeeper の連携をサポートしません。

詳細については以下を参照してください。

http://technet.microsoft.com/en-us/library/ee449438#BKMK_R2disks

既知の問題

Microsoft SQL Server 2017 と 2019 のオプションサービスについて

- SQL Server Launchpad
- SQL Server PolyBase Data Movement
- SQL Server PolyBase Engine
- SQL Server CEIP service
- SQL Server Reporting Services

> **注意:** SIOS Protection Suite for Windows v8.6.2 ではこれらのオプションサービスを保護することができません。

既知の問題に関する詳細は SIOS Protection Suite for Windows テクニカルドキュメンテーション の「トラブルシューティング」セクションを参照してください。

よくある質問

SIOS Protection Suite の再インストールまたはリソースの再作成を行わずに、リソースの値も含め SIOS Protection Suite のデータベース設定を変更することは可能ですか。

はい。lk_chg_value.ksh コマンドを使用してください。

既存の SIOS Protection Suite 階層を旧バージョンの SIOS Protection Suite for Windows から v8 にアップグレードできますか。

既存の SIOS Protection Suite for Windows ソフトウェアを、リソース階層を維持したままアップグレードできます。正しいアップグレード手順については SIOS Protection Suite のアップグレード を参照してください。**注記** : SIOS

では SIOS Protection Suite を 2 つ以上前のメジャーバージョンからアップグレードすることをサポートしていません。LifeKeeper for Windows v7.x よりも前のバージョンから SIOS Protection Suite for Windows v8x にアップグレードする場合は、古いバージョンの LifeKeeper をアンインストールしてから SIOS Protection Suite for Windows v8.x を再インストールしてください。

Microsoft Cluster Services (Windows 2003) または Windows Server Failover Cluster (Windows 2008 以降) を使用したクラスタで SIOS Protection Suite は動作しますか。

SIOS Protection Suite v8.0.1 は、別のクラスタリング製品で、Microsoft Cluster Services と Windows Server Failover Cluster のどちらもサポートしていません。

SIOS Protection Suite では、クラスタ内のすべてのサーバの設定が同一でなければなりませんか。

いいえ。すべてのサーバが、フェイルオーバ操作後にアプリケーションを実行できるだけの処理能力があり、SIOS Protection Suite に関するそれ以外の要件をすべて満たしていれば、クラスタを構築できます。SIOS Protection Suite は、同一のハードウェアを必要としませんが、ソフトウェアについては同一のものを必要とし、同一のサービスパックで設定する必要があります。

SIOS Protection Suite for Windows は 64 ビット環境に対応していますか。

はい。SIOS Protection Suite for Windows は 64 ビットプラットフォームにのみ対応しています。

SIOS Protection Suite によって保護されているファイル共有リソースに対する権限はどのようにして変更するのですか。

EditFileShareResource ユーティリティを使用して、ファイル共有リソースを、関連するボリュームに対する現在のファイル共有および権限とともに更新することができます。このユーティリティは、ファイル共有の数が多い環境や、リソースを作成した後や権限を変更した後にファイル共有が追加または削除された環境で便利です。このユーティリティを使用すると、ファイル共有リソースを削除して再作成する必要がなくなります。EditFileShareResource ユーティリティは *%LKROOT%\bin* ディレクトリにあります。

ユーティリティを起動するには、コマンドラインから次のように入力します。

```
EditFileShareResource <Tag name>
```

< Tag name > は、現在サービス中のファイル共有リソースのタグ名です。

このユーティリティは、ファイル共有階層に関連付けたボリュームに定義されている該当の **すべて** のファイル共有を保護します。また、すでにシステムから削除された古い保護対象ファイル共有を削除し、所定の基準に従って、新たに定義したファイル共有をファイル共有リストに追加します。ファイル共有に定義されているファイル共有権限も更新します。

ドキュメント

SIOS Protection Suite for Windows のインストール、設定、管理、およびトラブルシューティングについて詳細に説明した関連ドキュメントは、SIOS Protection Suite テクニカルドキュメンテーション で参照できます。SIOS Protection Suite for Windows のあらゆる側面について、以下のセクションで説明しています。

セクション	説明
はじめに	SIOS Protection Suite for Windows 製品について、そのコンポーネントの概要を含めて説明します。
インストール	SIOS Protection Suite 環境のプランニングとセットアップ、SIOS Protection Suite のインストールとライセンスおよびリモートシステムで実行するための LifeKeeper GUI の設定方法について説明しています。
構成	クラスタ内の各サーバで SIOS Protection Suite ソフトウェアを設定するための詳細情報が記載されています。
管理	サーバを対象とする作業 (サーバプロパティの編集、リソースの作成、コミュニケーションパスの作成と削除など) とリソースを対象とする作業 (リソースの編集、拡張、削除) について説明しています。
マニュアルページ	SIOS Protection Suite 製品のリファレンスマニュアルページです。
ユーザガイド	LifeKeeper GUI で実行できる操作など、LifeKeeper GUI の詳細情報が記載されています。データレプリケーションなどの詳細項目もあります。
DataKeeper	DataKeeper のレプリケーション動作概要および DataKeeper の設定、管理に関する詳しい情報が記載されています。本トピックスには DataKeeper をインストールおよび設定するにあたって必要なネットワークに関する考慮事項、共通の設定事項や要件などが含まれています。
トラブルシューティング	SIOS Protection Suite for Windows のインストール時、設定時、または使用時に発生する可能性がある既知の問題について説明し、解決策を提示しています。
リカバリキット	LifeKeeper で特定のアプリケーションを管理できるようにするためのオプションのリカバリキット (SQL Server および Oracle) に関するプランニングとインストールの手順、管理、設定、ユーザ情報が記載されています。

クイックスタートガイド

SIOS Protection Suite for Windows を利用するにあたって、SIOS Protection Suite for Windows クイックスタートガイド および DataKeeper クイックスタートガイド を参照してください。

3. SIOS Protection Suite for Windows クイックスタートガイド

このトピックでは、以下に示すガイドにて、SIOS Protection Suite (SPS) for Windows をインストールし、設定する詳細な手順を説明しています。SIOS Protection Suite のソフトウェアバンドルには、DataKeeper (DK) 、LifeKeeper 、およびオプションの SIOS Protection Suite Microsoft SQL Server Recovery Kit があります。

一連の手順には、その手順を詳細に説明するドキュメントへのリンクがあります。

前提条件とインストール

1. SIOS Protection Suite for Windows リリースノート を読んで、最新情報を確認してください。
2. ファイアウォール設定 - ファイアウォールでどのポートを開放するかを理解します。
3. ネットワーク帯域 - WAN 上で複製する場合は、変更の割合を分析し、適切なネットワーク帯域幅を確保することが重要です。
4. DataKeeper はブロックレベルでボリュームを複製するソリューションであり、各サーバに同じサイズの追加ボリュームが必要です (システムドライブ以外)。ストレージ要件の詳細については、ボリュームの考慮事項 を参照してください。
5. レプリケーションについて のセクションを読んで、DataKeeper の仕組み、および同期と非同期のレプリケーションの違いを理解してください。
6. サーバ仕様の確認 を参照して、すべてのコンポーネントのバージョンと性能が各 SIOS Protection Suite サーバに適切であることを確認してください。*注記:* クラスタ内のすべてのサーバで同一バージョンの Windows を実行してください。
7. クラスタのコミュニケーションパスを計画します。性能を最大に発揮できるようにするには、複数のコミュニケーションパスを定義してください。追加情報については、サーバ通信のプランニング を参照してください。
8. LK は共有ストレージで使用することも、複製ストレージで使用することもできます。追加情報については、ストレージとアダプタの要件 、およびストレージの構成 を参照してください。
9. SIOS Protection Suite が正しく動作するためには、ネットワークがネットワーク構成の確認 の説明どおりに構成されていることが重要です。特に、*パブリック NIC をバインド順の最上位にする* (すべてのクラスタノードの上位にする) 必要があります。
10. アプリケーション (Oracle、SQL Server、Exchange) をインストールする前に、データベースアプリケーションのインストールと設定 を確認してください。
11. SIOS Protection Suite のインストールは、セットアップ実行可能ファイルの実行と同様に簡単です。SIOS から受け取った設定で、LK、DK、およびオプションの ARK のインストールが処理されます。セットアップの最後に、ライセンスキーの入力を求められます。評価版を使用するお客様は、SIOS 提供の期限付きキーを使用してください。ソフトウェアを購入したお客様は、ライセンスの取得とインストール の手順に従ってインストールを完了してください。詳細については、SIOS Protection Suite for Windows インストールガイド を参照してください。
12. 設定ワークグループ環境で SIOS Protection Suite (LifeKeeper および DataKeeper) を使用している場合、LifeKeeper サービスは、各システムの DataKeeper サービスログオン ID とパスワードの選択 時の DataKeeper サービスと同じアカウント (ID およびパスワード) を使用する必要があります。

設定

SIOS Protection Suite をインストールし、前提条件 の説明に従ってネットワークとストレージが設定されていることを確認したら、SIOS Protection Suite を設定してビジネスに不可欠なアプリケーションを保護しましょう。保護設定手順の詳細については SIOS Protection Suite の設定手順 を参照してください。 必要最小限の手順の概要、および詳細情報のリンクを以下に示します。

1. コミュニケーションパス を作成します。コミュニケーションパスは、ノード間のクラスタ情報、およびシステム全体に障害が発生したことの検出に使用するハートビートを伝達します。
2. リソース階層 を作成します。保護するアプリケーションに合わせて、以下のリソースを作成します。リソース作成の詳細手順については、リソースタイプをクリックしてください。

    • ボリューム - ボリュームリソースは、複製ボリュームと共有物理ディスクのいずれでもかまいません。ボリュームリソースは、ほぼすべてのクラスタ構成で使用されます。

    • IP - IP リソースは、同一サブネット内にあるクラスタノード間のクライアント転送に使用されます。

    • DNS - DNS リソースは、異なるサブネット上にあるクラスタノード間のクライアント転送に使用されます。

    • ファイル共有 - ファイル共有リソースは、Windows ファイル共有の保護とリカバリに使用されます。ファイル共有リソースは、ボリューム リソースが作成済みであることを前提にしています。

    • LAN Manager - LAN Manager リソースは、NetBIOS 名の解決が必要な環境で使用されます。別の方法として、DNS 解決が正常に機能している場合は、DNS に "A" レコードを作成し、そのレコードがクライアント転送の IP リソースに解決されるようにすることもできます。

    • Generic Application - GenApp リソースを使用すると、単純な start、stop、および recover のスクリプトを作成してアプリケーションを保護できます。GenApp リソースは、Windows のサービス保護に簡単に使用できるサンプルスクリプトに付属しています。

    • SIOS Protection Suite Microsoft SQL Server - SQL Recovery Kit を使用すると、SQL 実装の高可用性および障害リカバリを実現するソリューションを用意できます。SQL Serverクラスタの作成プロセス全体は、画面キャプチャによるデモンストレーションのオンラインビデオ デモ詳細に示されています。

3. リソースの作成後に、リソース依存関係の追加 の説明に従って依存関係を調整する必要があります。依存関係を作成することにより、その関係にある複数のリソースが必ず共にフェイルオーバし、正しい順序でそれらのリソースの開始と停止が行われます。
4. この時点で、機能するクラスタが作成されました。ドキュメンテーション では、環境で活用できるその他の高度な機能も説明しているので、参考にしてください。

管理

クラスタを使用して実行する作業は多数ありますが、まず、手動スイッチオーバをテストして、アプリケーションがアク

ティブクラスタからスタンバイクラスタに移動可能であることを確認します。このためには、スタンバイシステムの最上位リソースを右クリックし、[サービス開始] を選択してください。手動によるスイッチオーバが開始されます。

手動によるスイッチオーバが正常に完了したことを確認したら、ローカルリカバリ をテストします。SIOS Protection Suite がリソースの障害を検出すると、ローカルリカバリ が有効な場合はリソースのローカルリカバリを試行します。このテストを実行する簡単な方法の 1 つは、保護対象アプリケーションのサービスを停止することです。クイックチェック を実行すると、障害が検出され、サービスが自動的に再起動されます。

最後のテストとして、システムリカバリを実行します。アクティブサーバが完全に停止すると、コミュニケーションパス経由のハートビート がスタンバイサーバで受信されなくなるので、スタンバイサーバは障害が発生したことを検出します。タイムアウト時間を過ぎると (ハートビート間隔 X max　の機関にハートビートが受信されない)、スタンバイサーバが保護対象リソースのリカバリを開始します。システムリカバリをテストする最良の方法は、アクティブサーバの電源コードを抜くことです。アクティブサーバを単純にシャットダウンするだけでは、必ずしもフェイルオーバは発生しません。フェイルオーバするかどうかは、シャットダウン方法 の設定によって異なります。スタンバイサーバがリカバリを完了した後、障害を発生させたサーバを稼働すると、そのサーバは新しいスタンバイサーバとしてオンラインになります。

SIOS Protection Suite の管理の詳細については、SIOS Protection Suite テクニカルドキュメンテーション を参照してください。

トラブルシューティング

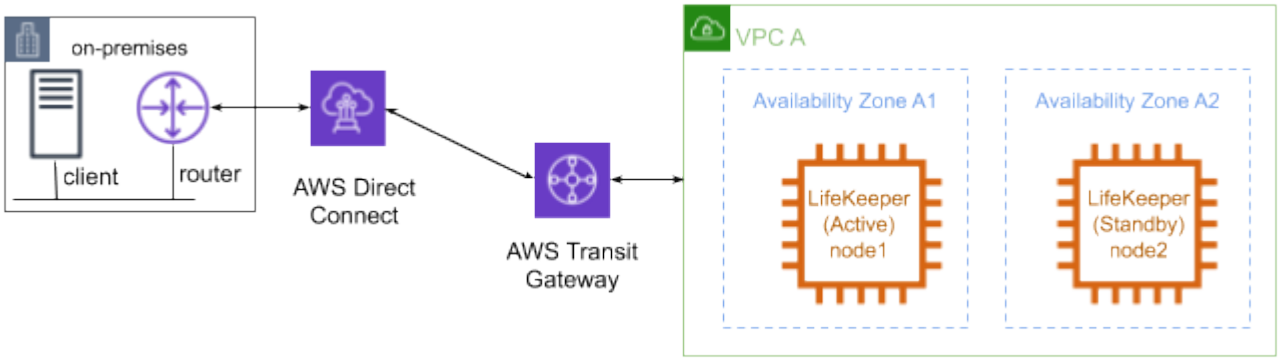
問題のトラブルシューティングでは、以下のリソースを参考にしてください。

- DataKeeper のトラブルシューティング 、およびSIOS Protection Suite のトラブルシューティング のセクション
- サポート契約を結んでいるお客様 - support.us.sios.com/aspx/SupportHome
- 評価版を使用しているお客様のみ - Pre-sales support

4. AWS Direct Connect クイックスタートガイド

目的

AWS Transit Gateway のリリースにより、AWS Direct Connect を利用したオンプレミス環境（下図の On-premises）から AWS Transit Gateway を経由して、下図の VPC A 内に配置された HA クラスターノードへ接続する構成で、Recovery Kit for EC2 のルートテーブルシナリオが利用可能になりました。



本資料は、LifeKeeper for Windows で AWS Direct Connect を利用したオンプレミス環境から接続する構成を構築するための要件や基本操作を解説するものです。

なお、本資料は LifeKeeper や Amazon Web Service (以下 AWS) の基本的な設定や操作、技術的な詳細情報を解説するものではありません。本構成の前提となる LifeKeeper や AWS に関する用語・操作・技術情報等につきましては、関連のマニュアルやユーザーサイト等であらかじめご確認ください。

> 注記: 「Amazon Web Services」、「Powered by Amazon Web Services」のロゴ、「AWS」、「Amazon EC2」、「EC2」、「Amazon Elastic ComputeCloud」、「Amazon Virtual Private Cloud」、「AWS Direct Connect」、「AWS Identity and Access Management」、「AWS Transit Gateway」および「Amazon VPC」は、米国その他の国における Amazon.com, Inc. またはその関連会社の商標です。

利用のための要件

本構成を利用するためには、環境を準備する段階で満たすべきいくつかの要件があります。以下に AWS 環境とその上に作成するインスタンスに関する要件をまとめます。

AWS 環境の要件

サービスを提供するための基盤となる環境を AWS 上に作成します。本構成を利用するための要件は以下の通りです。

Amazon Virtual Private Cloud (VPC)

- VPC を AWS 内に設定する必要があります。

- プライマリ用インスタンスを配置するサブネットとスタンバイ用インスタンスを配置するサブネットを、それぞれ異なる Availability Zone(AZ) に作成する必要があります。

Amazon Elastic Compute Cloud (EC2)

- インスタンスが 2つ以上必要です。
- プライマリ用インスタンスとスタンバイ用インスタンスがそれぞれ異なる AZ で起動するように構成する必要があります。
- インスタンスは、Elastic Network Interface (ENI) に接続されます。
- インスタンスは、LifeKeeper のインストール要件を満たす必要があります。
- AWS Command Line Interface (AWS CLI) を全ての EC2 インスタンスにインストールする必要があります。インストール方法は、「AWS Command Line Interface のインストール 」を参照してください。
- https を使用して Amazon EC2 Web サービスエンドポイントの URL (EC2 URL) に、および http を使用して Amazon EC2 メタデータの URL (http://169.254.169.254/) にアクセス可能でなければなりません。

AWS Identity and Access Management (IAM)

LifeKeeper が AWS を操作するために、以下のアクセス権を持った IAM ユーザーもしくは IAM ロールが必要です。EC2 インスタンスの root ユーザーからアクセスできるように EC2 の IAM ロール を設定するか、AWS CLI の設定 を適切に行ってください。

- ec2:DescribeRouteTables
- ec2:ReplaceRoute

AWS Transit Gateway

- クラスターノードを配置した VPC と、クライアントを配置したオンプレミス環境とは、Virtual Private Gateway で接続するのではなく、AWS Transit Gateway を経由して接続する必要があります。
- AWS Transit Gateway を作成する際に Default route table association と Default route table propagation を有効にしてください。
- VPC との接続は、Transit Gateway Attachment を作成することで行ってください。
- AWS Direct Connect との接続は Direct Connect Gateway の Gateway association の設定で、作成した AWS Transit Gateway を選択することで行なってください。この際に、Allowed prefixes には、クラスターノードを配置した VPC のネットワークアドレスと、仮想 IP アドレスの両方を設定してください。

LifeKeeper ソフトウェアの要件

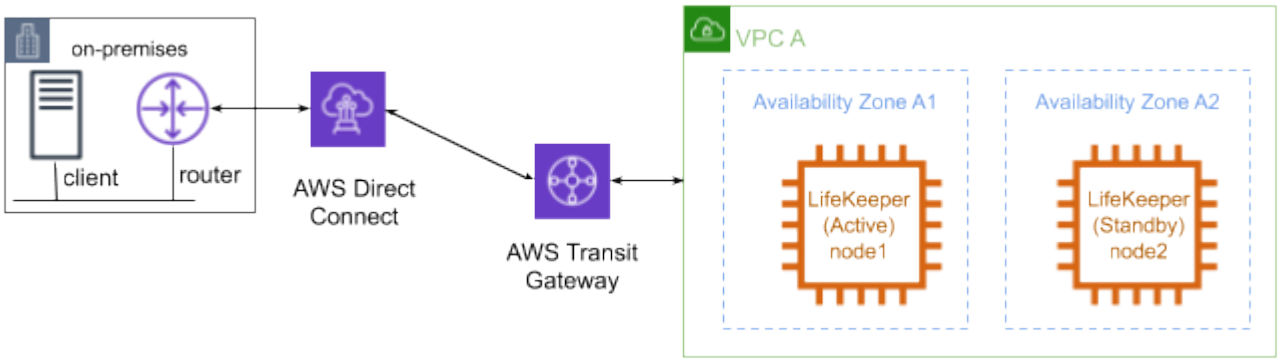
各サーバーに同じバージョンの LifeKeeper ソフトウェアとパッチをインストールする必要があります。本構成で必要な Application Recovery Kit (ARK) は以下の通りです。具体的な LifeKeeper の要件については、SPS for

Windows テクニカルドキュメンテーション および SPS for Windows リリースノート を参照してください。

- LifeKeeper IP Recovery Kit
- LifeKeeper Recovery Kit for EC2

構築手順

以下の構成図の様な環境を構築するための一般的な手順を解説します。



準備

「利用のための要件」を満たす環境を構築してください。それぞれのインスタンスに LifeKeeper をインストールして、node1/node2 間にコミュニケーションパスを作成してください。

IP リソース作成

仮想 IP リソースを作成します。IP リソースのアドレスは、VPC で管理している CIDR ブロック外である必要があります。

EC2 リソース作成

EC2 リソースを作成します。リソース作成時に要求される IP リソースは、上述の「 **IP リソース作成** 」で作成したリソースを指定してください。リソース作成時に要求される EC2 リソースタイプは Route Table (Backend Cluster) を指定してください。

保護するサービスのリソース作成

保護するサービスのためのリソースを作成してください。リソース作成に IP リソースが要求される場合は、上述の「 **IP リソース作成** 」で作成したリソースを指定してください。親リソースが保護するサービスのリソース、子リソースが EC2 リソースとなるようにリソースの依存関係を設定してください。

ルートテーブルの作成

ルートテーブルを下記のように設定してください。

- クラスターノードを配置した VPC もしくはサブネットのルートテーブルに、オンプレミス環境のネットワークへの経路情報を追加してください。

送信先	ターゲット
オンプレミス環境のネットワークアドレス	作成した Transit Gateway

- Transit Gateway のルートテーブルに、仮想 IP アドレスへの経路情報を追加してください。

送信先	ターゲット
仮想 IP アドレス	クラスターノードを配置した VPC

- オンプレミス環境のクライアントやルーターの経路情報を適切に設定し、クラスターノードを配置した VPC のネットワークアドレスや仮想 IP アドレス宛のパケットの送信先が Direct Connect となるようにしてください。

設定が完了したら、クライアントからクラスターサーバーのプライベートアドレスや仮想 IP アドレスにアクセスできることを確認してください。

既知の問題とトラブルシューティング

Windows 版 LifeKeeper Recovery Kit for EC2 には下記の既知の問題があります。

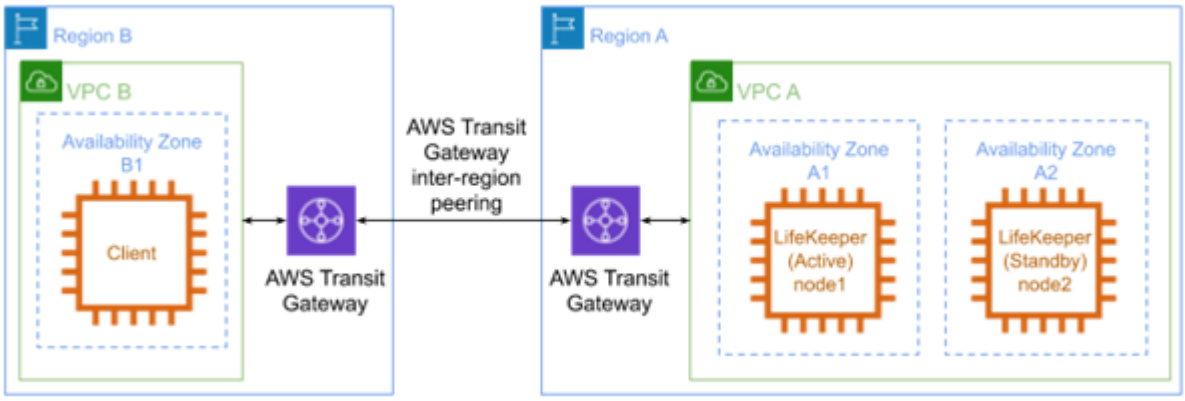
- クラスターノードを配置した VPC と同一アカウント、同一リージョン内で別 VPC のルートテーブルに仮想 IP を接続先とするエントリーも存在する場合、そのエントリーを監視と変更の対象としてしまうため、リソースの起動に失敗する。

上記問題を回避するため、仮想 IP として使用するアドレスは、同一アカウント、同一リージョンの場合、別 VPC であっても他の用途で使っている仮想 IP とは別のアドレスにしてください。

5. AWS VPC ピア接続クイックスタートガイド

目的

AWS Transit Gateway、および AWS Transit Gateway inter-region peering のリリースにより、VPC（下図の VPC A）に配置されたHAクラスターノードに、別リージョンの VPC（下図の VPC B）のクライアントから接続する構成で、Recovery Kit for EC2 のルートテーブルシナリオが利用可能になりました。



本資料は、LifeKeeper for Windows で、HA クラスターノードに、別リージョンの VPC のクライアントから接続する構成を構築するための要件や基本操作を解説するものです。

なお、本資料は LifeKeeper や Amazon Web Service (以下 AWS) の基本的な設定や操作、技術的な詳細情報を解説するものではありません。本構成の前提となる LifeKeeper や AWS に関する用語・操作・技術情報等につきましては、関連のマニュアルやユーザーサイト等であらかじめご確認ください。

> ✻ 注記: AWS Transit Gateway inter-region peering は、本ドキュメント執筆時点（2020年2月）で米国東部(バージニア北部)、米国東部(オハイオ)、米国西部(オレゴン)、欧州(アイルランド)、欧州(フランクフルト)の各リージョンで利用可能です。その他のリージョンにサーバーまたはクライアントを配置する場合には本ドキュメントの構成は利用できません。AWS Transit Gateway inter-region peering が利用できないリージョンにサーバーまたはクライアントを配置する場合は、Route53 Recovery Kit を使用して、AWS の DNS サービスの「Route53」に登録されている DNS の A レコード（ホスト名に対応する IP アドレス）を更新する構成を検討してください。

> ✻ 注記: 本ドキュメントは、単一の VPC 内にクラスターノードを配置する構成を対象としています。クラスターノードを複数のリージョンや複数の VPC にまたがって配置する構成では、ルートテーブルシナリオは利用できません。

> ✻ 注記: 「Amazon Web Services」、「Powered by Amazon Web Services」のロゴ、「AWS」、「Amazon EC2」、「EC2」、「Amazon Elastic Compute Cloud」、「Amazon Virtual Private Cloud」、「AWS Direct Connect」、「AWS Identity and Access Management」、「AWS Transit Gateway」、「AWS Transit Gateway inter-region peering」および「Amazon VPC」は、米国その他の国における Amazon.com, Inc. またはその関連会社の商標です。

利用のための要件

本構成を利用するためには、環境を準備する段階で満たすべきいくつかの要件があります。以下に AWS 環境とその上に作成するインスタンスに関する要件をまとめます。

AWS 環境の要件

サービスを提供するための基盤となる環境を AWS 上に作成します。本構成を利用するための要件は以下の通りです。

Amazon Virtual Private Cloud (VPC)

- クラスターノードを配置する VPC を AWS 内に設定する必要があります。
- クライアントを配置する VPC は、クラスターノードを配置する VPC とは別リージョンに設定される必要があります。
- クラスターノードを配置する VPC に、プライマリ用インスタンスを配置するサブネットとスタンバイ用インスタンスを配置するサブネットを、それぞれ異なる Availability Zone (AZ) に作成する必要があります。

Amazon Elastic Compute Cloud (EC2)

- クラスターノード用のインスタンスが2つ以上必要です。
- プライマリ用インスタンスとスタンバイ用インスタンスがそれぞれ異なる AZ で起動するように構成する必要があります。
- クラスターノード用インスタンスは、Elastic Network Interface (ENI) に接続されます。
- クラスターノード用インスタンスは、LifeKeeper のインストール要件を満たす必要があります。
- AWS Command Line Interface (AWS CLI) を全てのクラスター用インスタンスにインストールする必要があります。インストール方法は、「AWS Command Line Interface のインストール 」を参照してください。
- https を使用して Amazon EC2 Web サービスエンドポイントの URL (EC2 URL) に、および http を使用して Amazon EC2 メタデータの URL (http://169.254.169.254/) にアクセス可能でなければなりません。

AWS Identity and Access Management (IAM)

LifeKeeper が AWS を操作するために、以下のアクセス権を持った IAM ユーザーもしくは IAM ロールが必要です。EC2 インスタンスの管理ユーザーからアクセスできるように EC2 の IAM ロール を設定するか、AWS CLI の設定 を適切に行ってください。

- ec2:DescribeRouteTables
- ec2:ReplaceRoute

AWS Transit Gateway

- クラスターノードを配置した VPC と、クライアントを配置した VPC とは、VPC 同士を AWS Inter-Region VPC Peering で直接接続するのではなく、それぞれのリージョンで AWS Transit Gateway を作成し、AWS Transit Gateway 同士を AWS Transit Gateway inter-region peering で接続する必要があります。
- AWS Transit Gateway を作成する際に Default route table association と Default route table propagation を有効にしてください。
- VPC との接続は、Transit Gateway Attachment を作成することで行ってください。
- AWS Transit Gateway 同士の AWS Transit Gateway inter-region peering 接続は、Transit Gateway Attachment を作成することで行ってください。

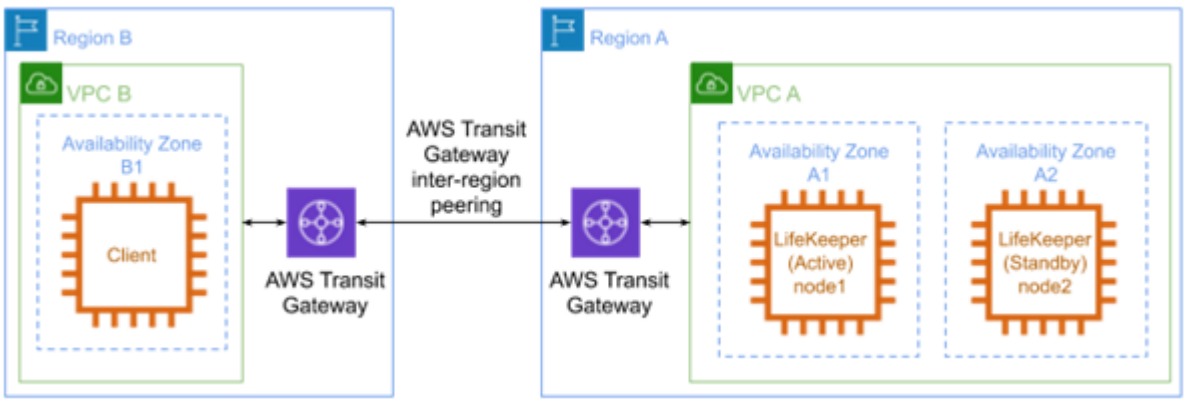
LifeKeeper ソフトウェアの要件

各サーバーに同じバージョンの LifeKeeper ソフトウェアとパッチをインストールする必要があります。本構成で必要な Application Recovery Kit (ARK) は以下の通りです。具体的な LifeKeeper の要件については、SPS for Windows テクニカルドキュメンテーション および SPS for Windows リリースノート を参照してください。

- LifeKeeper IP Recovery Kit
- LifeKeeper Recovery Kit for EC2

構築手順

以下の構成図の様な環境を構築するための一般的な手順を解説します。



準備

「利用のための要件」を満たす環境を構築してください。それぞれのインスタンスに LifeKeeper をインストールして、node1/node2 間にコミュニケーションパスを作成してください。

IP リソース作成

仮想 IP リソースを作成します。IP リソースのアドレスは、VPC で管理している CIDR ブロック外である必要があり

ます。

EC2 リソース作成

EC2 リソースを作成します。リソース作成時に要求される IP リソースは、上述の「 **IP リソース作成** 」で作成したリソースを指定してください。リソース作成時に要求される EC2 リソースタイプは Route Table (Backend Cluster) を指定してください。

保護するサービスのリソース作成

保護するサービスのためのリソースを作成してください。リソース作成に IP リソースが要求される場合は、上述の「 **IP リソース作成** 」で作成したリソースを指定してください。親リソースが保護するサービスのリソース、子リソースが EC2 リソースとなるようにリソースの依存関係を設定してください。

ルートテーブルの設定

ルートテーブルを下記のように設定してください。

- クラスターノードを配置した VPC もしくはサブネットのルートテーブルに、クライアントを配置した VPC のネットワークへの経路情報を追加してください。

送信先	ターゲット
クライアントを配置した VPC のネットワークアドレス	Transit Gateway（クラスターノード側 ）

- Transit Gateway（クラスターノード側）のルートテーブルに、クライアントを配置した VPC のネットワークへの経路情報と仮想 IP アドレスへの経路情報を追加してください。

送信先	ターゲット
クライアントを配置した VPC のネットワークアドレス	Transit Gateway（クライアント側）
仮想 IP アドレス	クラスターノードを配置した VPC

- Transit Gateway（クライアント側）のルートテーブルに、クラスターノードを配置した VPC のネットワークへの経路情報と仮想 IP アドレスへの経路情報を追加してください。

送信先	ターゲット
クラスターノードを配置した VPC のネットワークアドレス	Transit Gateway（クラスターノード側）
仮想 IP アドレス	Transit Gateway（クラスターノード側）

- クライアントを配置した VPC もしくはサブネットのルートテーブルに、クラスターノードを配置した VPC 及び仮想 IP アドレスへのネットワークへの経路情報を追加してください。

送信先	ターゲット
クラスターノードを配置した VPC のネットワークアドレス	Transit Gateway（クライアント側）

仮想 IP アドレス	Transit Gateway（クライアント側）

設定が完了したら、クライアントからクラスターサーバーのプライベートアドレスや仮想 IP アドレスにアクセスできることを確認してください。

既知の問題とトラブルシューティング

Windows 版 LifeKeeper Recovery Kit for EC2 には下記の既知の問題があります。

- クラスターノードを配置した VPC と同一アカウント、同一リージョン内で別 VPC のルートテーブルに仮想 IP を接続先とするエントリーも存在する場合、そのエントリーを監視と変更の対象としてしまうため、リソースの起動に失敗する。

上記問題を回避するため、仮想 IP として使用するアドレスは、同一アカウント、同一リージョンの場合、別 VPC であっても他の用途で使っている仮想 IP とは別のアドレスにしてください。

6. Microsoft Azure 動作検証ガイド

内容

本ガイドでは、Azure クラウド上のクラスター環境の例として、以下の構成を作成する手順をご案内します。

- SPS クラスター（2ノードクラスター）マルチ NIC 構成
- DataKeeper レプリケーションによるデータミラー型の共有データ領域
- IP リソース、Oracle リソースまたは PostgreSQL リソース

本ガイドは、当社で実際に行った検証作業の構成をベースとして記述したものです。

> **免責条項:** 本ガイドでは Microsoft Azure 環境における一般的な SIOS Protection Suite for Windows 設定の概略を述べています。また、記載のない項目は基本的にデフォルト値または任意の値を前提としています。
> 実際には、より多くの Azure インフラストラクチャーオプションを利用した構成が可能です。本ガイドに記載の設定値は、実際の要件に合わせて、適宜置き換えてご利用ください。

将来における互換性

本ガイドに記載されております内容は、2020年 7月時点の Azure 上で実施した検証に基づいています。将来における Azure 及び LifeKeeper の仕様変更について保証するものではありません。必要に応じて最新のドキュメンテーションを参照し、適切な設定を行ってください。

ライセンス

このガイドの手順を実行する際は、SIOS Protection Suite、Oracle Database、PostgreSQL など必要ソフトウェアのライセンスが必要です。

制限事項

- 本構成では、ネットワーク通信のために ILB によるネットワークアドレス変換（NAT）を用います。また、NAT の対象とする TCP ポート番号は固定の番号をあらかじめ設定しておく必要があります。そのため、固定の TCP ポート番号のみを対象とする NAT を経由した通信で不具合が発生するアプリケーションを保護対象とすることはできません。例えば下記のようなアプリケーションが該当します。
    - クライアントとの通信に複数のコネクションを用いるアプリケーションのうち、サーバー側のポート番号が動的に変化するもの（例：ftp のアクティブモード）

    - TCP 以外のプロトコル（UDP、ICMP 等）での通信を行うアプリケーション

- 本構成のアプリケーションは、仮想 IP アドレスだけでなく、正常性プローブに応答するため、稼働系と待機系それぞれのプライベート IP アドレスでも通信できなければなりません。そのため、アプリケーションが接続を待ち受けるIPアドレスは、任意の IP アドレス (INADDR_ANY) に設定可能である必要があります。

用語について

本ガイドで使用する用語について説明します。

- 内部負荷分散（Internal Load Balancing または ILB）
  Azure クラウドサービスまたは地域が限定された仮想ネットワークの内側に存在する仮想マシン間に負荷分散を実現する機能です。

- IP リソースが保護する VIP
  SPS で作成した仮想 IP アドレスです。

- ILB が設定する VIP
  Azure で作成した Internal Load Balancing の仮想 IP アドレスです。

- Azure のプライベート IP アドレス
  Azure の Virtual Network で使用するプライベートアドレスです。

スクリーンショット画像について

随所に現れるスクリーンショット画像はヒント情報です。当社が実際に環境を作るときに採取した画面が掲載されており、稼働系と待機系などの画面が混在している場合があります。

SPS を Azure で動作させるための要件

- SPS クラスターでは、保護されたアプリケーションとの通信のために Azure Internal Load Balancer (ILB) を利用します。ILB が正常に動作するためには、各クラスターノードに 2つのネットワークアダプターが必要です。クラスターノードごとに複数のネットワークインターフェースを定義してください。

- クラスターノードが Windows ドメインに属さない場合は、ノード名に小文字を含まないようにしてください。

- Azure 仮想マシンにエフェメラルディスクが含まれている場合は、そのディスクを DataKeeper のビットマップの保存に使用して、レプリケーションの性能を最適化してください。

- Azure にはアプリケーションの可用性を高めるため、**Availability zone (AS)** と **Availability set (AS)** の

2つの選択肢があります。Availability zone は Availability set より可用性が高い構成を構築可能なため、Availability zone の使用を推奨します。お使いのリージョンで Availability zone が提供されている場合、各クラスターノードは異なる Availability zone に配置してください。Availability set を使用する場合は、各クラスターノードが異なる Fault domain かつ異なる Update domain に配置されるように設定してください。

6.1. Microsoft Azure の概要

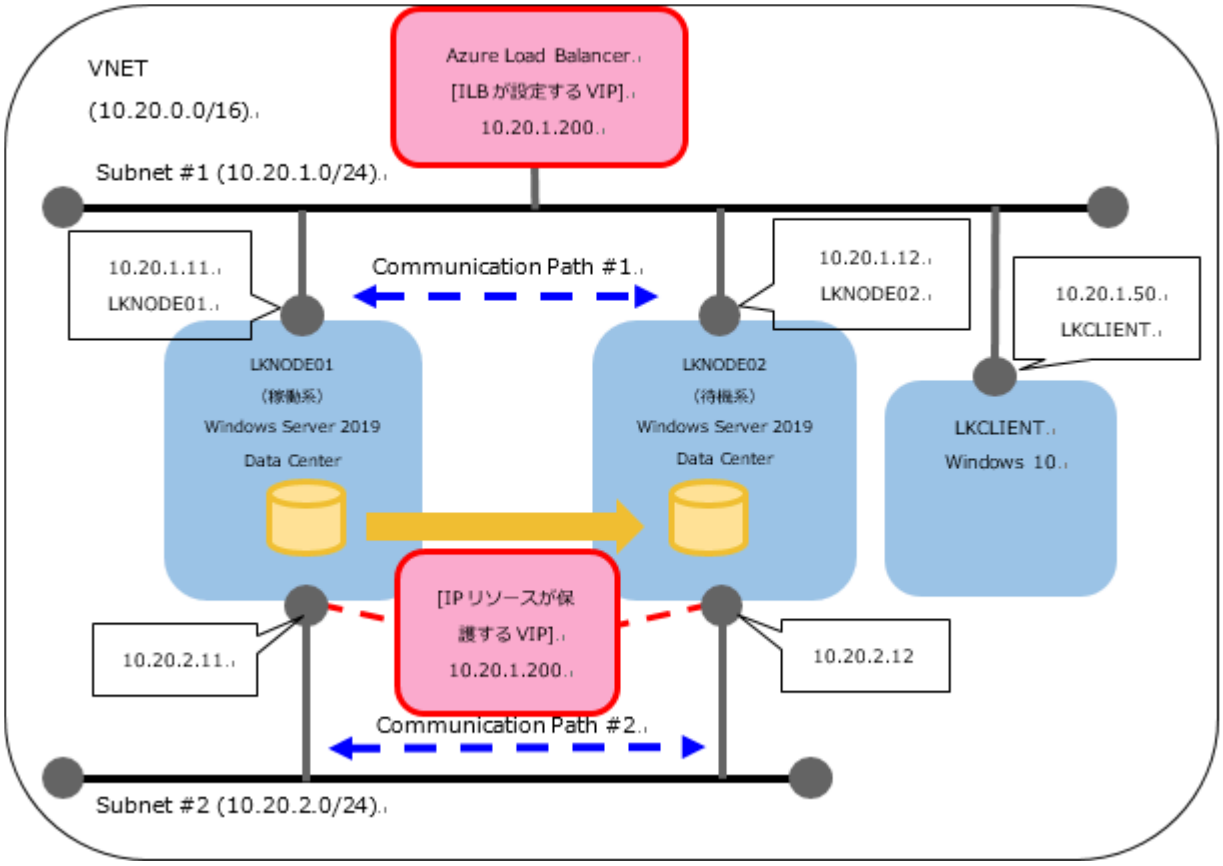
Azure は、Microsoft が提供するパブリッククラウドサービスです。ハードウェア、ネットワーク、ディスクなどのストレージ、Windows Server や Linux などのサーバー OS、Web サーバーや RDBMS などのミドルウェア、グループウェアやサーバー・アプリケーション、そして .NET Framework などのアプリケーション実行環境を、ユーザーがオンデマンドでネットワークを経由して利用可能な IT の利用形態です。

Microsoft が管理する世界中のデータセンターに、インターネット経由でサーバー・アプリケーションを簡単に作成し、展開、管理が行えます。サーバーやインフラを所有することなく、必要な時に必要な量のメモリやディスクといったコンピューティングリソースを利用することが出来ます。料金体系はリソース毎に分かれており、時間単位の従量課金での利用となります。

Azure では、Web ブラウザベースの管理ポータルを提供しており、ユーザーは直感的に操作する事が可能です。

構成情報

本構成では SPS を使って、以下の構成のアクティブ/スタンバイクラスターを構築します。



クラスターノード

	稼働系 (LKNODE01)	待機系 (LKNODE02)
仮想マシンサイズ	Standard B2ms (cpu/mem/disk=2/8g/4) ※	
データディスク	30GB（アプリケーション用） ※	
プライベート IP アドレス	10.20.1.11	10.20.1.12
[IP リソースが保護する VIP]	10.20.1.200	
[ILB が設定する VIP]	10.20.1.200	
ILB が転送するポート i.e. Oracle が Listen するポート	（Oracle の場合）1521 （PostgreSQLの場合）5432	
ILB の負荷分散対象	（Oracle の場合）10.20.1.11:1521 （PostgreSQL の場合）10.20.1.11:5432	（Oracle の場合）10.20.1.12:1521 （PostgreSQL の場合）10.20.1.12:5432
ソフトウェア	Windows Server 2019 Datacenter Edition SIOS Protection Suite for Windows v8.7.0 Oracle Database 19c (19.3) for Microsoft Windows x64 (64-bit) PostgreSQL 11.7	

※ Oracle や PostgreSQL など、保護するアプリケーションのインストール要件に合うよう、インスタンスサイズおよび仮想マシンのディスクを用意してください。

VM 構成（クライアント）

仮想マシンサイズ	Standard A2m_v2 (2/16g/4)
プライベート IP アドレス	10.20.1.50
ソフトウェア	Microsoft Windows 10 Oracle Database 19c Client (19.3) for Microsoft Windows x64 (64-bit) PostgreSQL 11.7

ネットワーク構成

Azure では、仮想マシン（VM）間での通信を行えるようにするため、"仮想ネットワーク"（VNET）を作成します。VNET は、サブネットを指定する事でこのサブネット内で VM 間での通信が行えるようにしています。

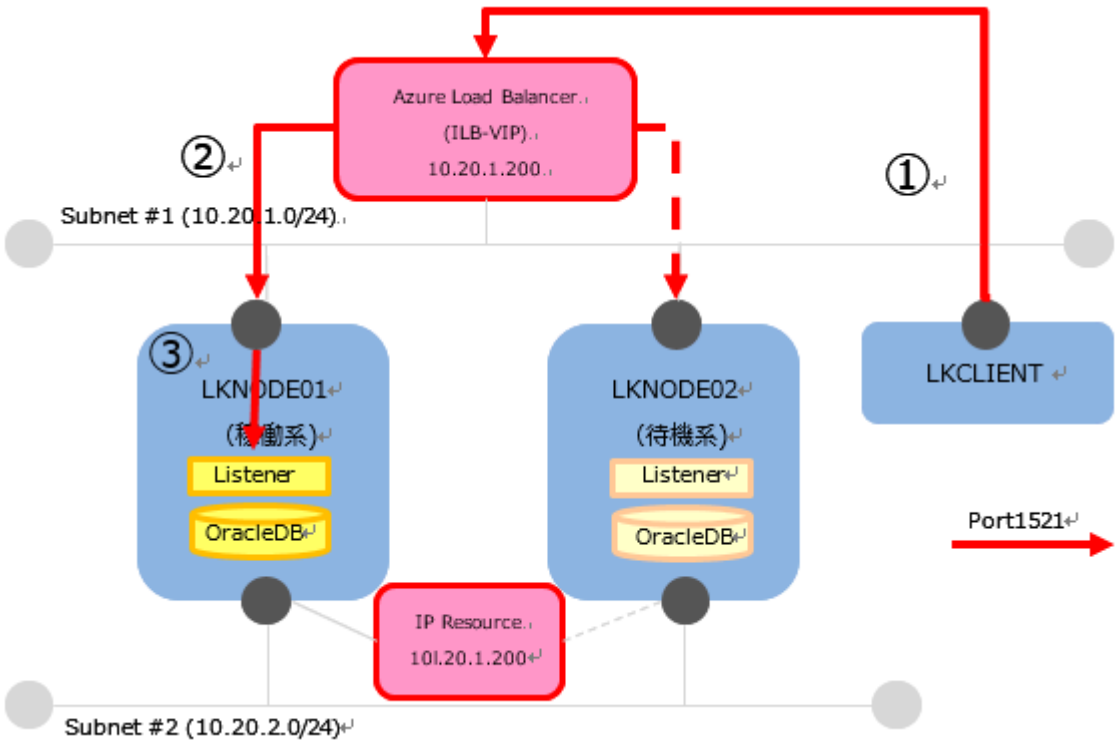
Azure で VM にネットワークを構成する場合、あらかじめ VNET を作成し、VM にこの VNET を指定するのが一般的です。VNET を使用すると、VM に仮想プライベートネットワーク (VPN) を提供できます。オプションとして、VPN をオンプレミス環境に接続して、ハイブリッドソリューションやクロスプレミスソリューションの実現もできます。VNET は管理ポータルサイトや Azure PowerShell を通して、DNS および IP アドレス範囲の構成を含むネットワークトポ

ロジーを制御できます。

6.2. Azure 特有の設定について

インターナルロードバランサー（ILB）の導入

Azure では [IP リソースが保護する VIP] を Azure の VNET で認識する事が出来ません。この影響で、通常 LifeKeeper for Windows が想定している [IP リソースが保護する VIP] によるネットワーク通信を行うことが出来ません。そのため本構成では、以下の様に ILB の導入を行い、[ILB が設定する VIP] をネットワーク通信経路として設定します。



クライアントからの接続

1. LKCLIENT が、アプリケーション（上図では Oracle Listener）へ接続するため、仮想 IP アドレスとアプリケーションのポート番号（上図では10.20.1.200:1521）で接続を試みます。

2. ILB は、負荷分散先である 10.20.1.11:1521 と 10.20.1.12:1521 のどちらかに振り分けます。アプリケーションは、LifeKeeper によってどちらか一方のマシンでのみ Active になっているため、ILB の正常性プローブは必ず Active 側のみが正常であることを検知します。結果として、ILB は常に Active 側（上図では LKNODE01 上で Active のため 10.20.1.11:1521）へ要求を振り分けます。

3. アプリケーションは、[Azure のプライベートアドレス]（を含む任意の IP アドレス）のアプリケーションポート上でも要求を待ち受けています。最終的に、LKCLIENT 上での仮想 IP アドレスとアプリケーションのポート番号（10.20.1.200:1521）への接続要求がアプリケーションに届けられます。

稼働系サーバー内部からの接続

1. ILB は NAT loopback 機能をサポートしていないため、稼働系サーバー内部から仮想 IP アドレスとアプリケーションのポート番号を指定してアプリケーションへ接続する場合は、ILB を経由することができません。この問題を解決するために、LifeKeeper の IP リソース（10.20.1.200）を作成します。

2. しかしながら、上図の通り Subnet#1 上ではすでに ILB が 10.20.1.200 を使用しているため、Subnet#1 上の NIC 上では同一の IP アドレスを Active にできません。そのため、[IP リソースが保護する VIP] には、便宜的に Subnet#2 上の NIC を設定します。

3. 稼働系サーバーから仮想 IP アドレスとアプリケーションのポート番号を指定したパケットは、稼働系サーバー内部のルーティングにより、サーバーの外部を経由することなく稼働系サーバー内部で処理されます。

4. アプリケーションは、仮想 IP アドレス（を含む任意の IP アドレス）のアプリケーションポート上でも要求を待ち受けています。最終的に、LKCLIENT 上での仮想 IP アドレスとアプリケーションのポート番号（10.20.1.200:1521）への接続要求がアプリケーションに届けられます。

IP リソースを必須とするアプリケーションの注意事項

IP リソースを必須とする ARK で保護されるアプリケーション（Oracle, Microsoft SQL Server, IIS）を Azure 環境以外で使用する場合は、接続を待ち受ける IP アドレスとして仮想 IP アドレスを設定します。しかし、上述の説明の通り、Azure 環境ではクライアントからの接続についてはそれぞれのサーバーのプライベートアドレスを使って通信し、サーバー内部からの接続については仮想 IP アドレスを使って通信します。そのため、IP リソースを必須とする ARK で保護されるアプリケーションであっても、接続を待ち受ける IP アドレスとして、任意の IP アドレス (INADDR_ANY) を設定する必要があります。このような設定が必要な例として本ガイドでは Oracle を取り上げます。

6.3. 注意事項

- 本ページ以降、**Azure のポータルサイト（管理用サイト）にログイン済み** であることを前提に、Azure リソースの作成・設定手順を説明します。

- 本ガイドの手順に従って作成された Azure リソース群の一意性を確保し、同じ目的のリソース群を複数セット作成する際の助けとなるよう、全ての Azure リソースに一意な名前を与えます。例として、SPS のクラスターノードの VM にはそれぞれ次のような名前を与えます。
  - *prefix*lknode01 → ”sios20lknode01”
  - *prefix*lknode02 → “sios20lknode02”

  ここで、*prefix* の部分は本ガイドの手順の実行者が決める任意の文字列です。説明文中では、*prefix* の例として "SIOS20" を使います。

6.4. Azure 上仮想環境の構築

リソースグループの作成

仮想ネットワークの作成

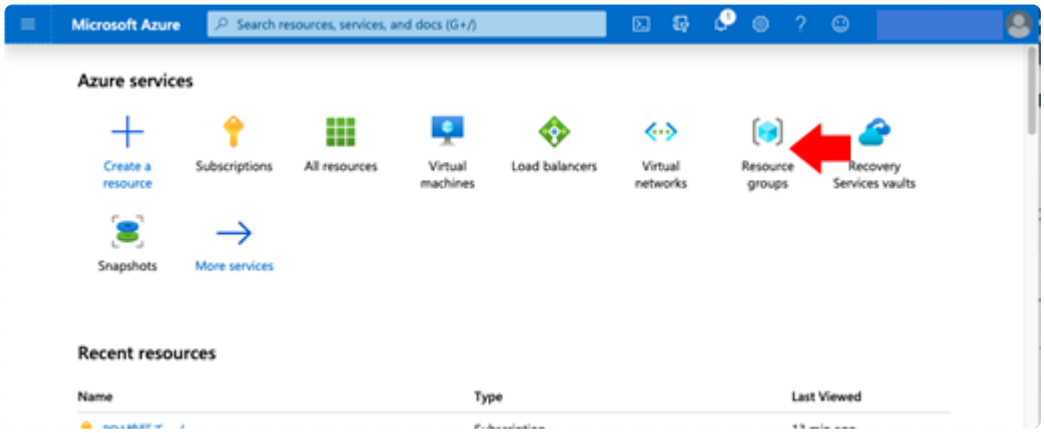
クラスターノード（稼働系と待機系）の作成

クライアントの作成

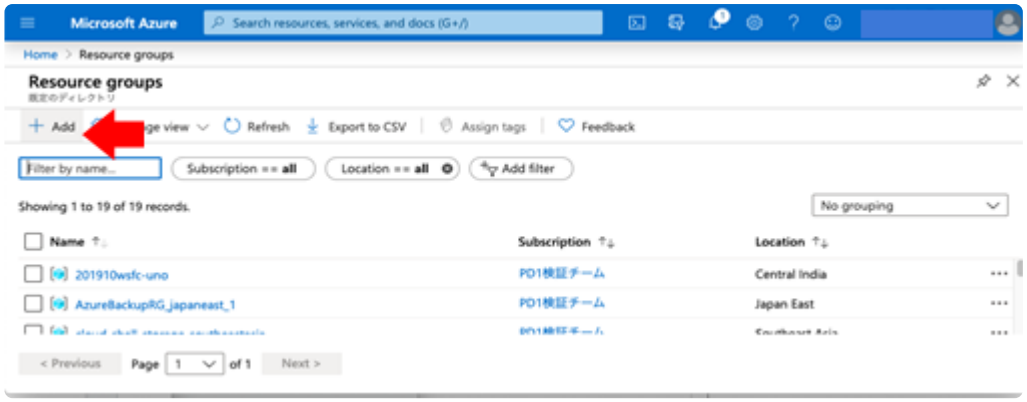
ロードバランサーの作成

6.4.1. リソースグループの作成

1. Azure にログインし、**[Azure Home]** を開きます。**[Resource groups]** アイコンをクリックします。

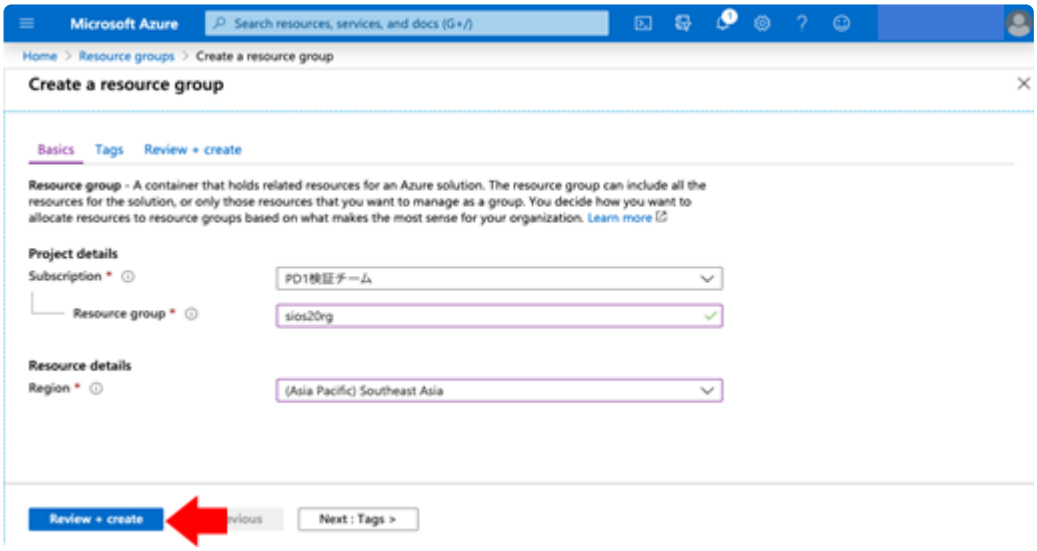


2. **[Add]** ボタンをクリックします。



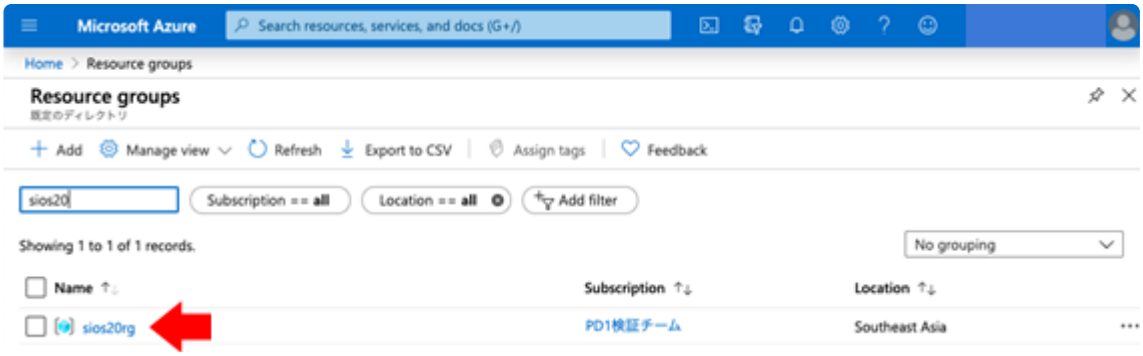
3. 次のように設定値を入力して、**[Review + Create]** をクリックします。

Resource group		
Subscription	お持ちのサブスクリプション ID	Azure サービス加入時に決められたサブスクリプション ID です。
Resource group	sios20rg	
Region	(Asia Pacific) Southeast Asia	この通りである必要はありません。



4. 確認画面で入力内容を確認して **[Create]** をクリックします。

5. リソースグループ sios20rg が作成されたのが確認できます。



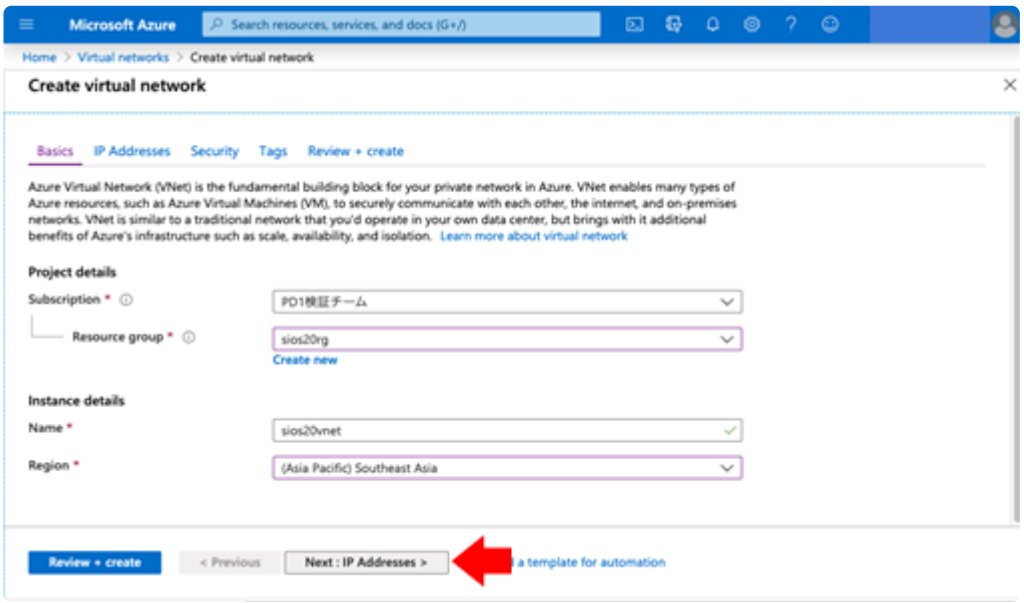
6.4.2. 仮想ネットワークの作成

本環境で使用する仮想ネットワークを作成します。今回は、アドレススペース 1つ、サブネット 2つを作成します。このうちひとつのサブネットはサービス用、もうひとつは SPS のコミュニケーションパスとレプリケーション用に使います。

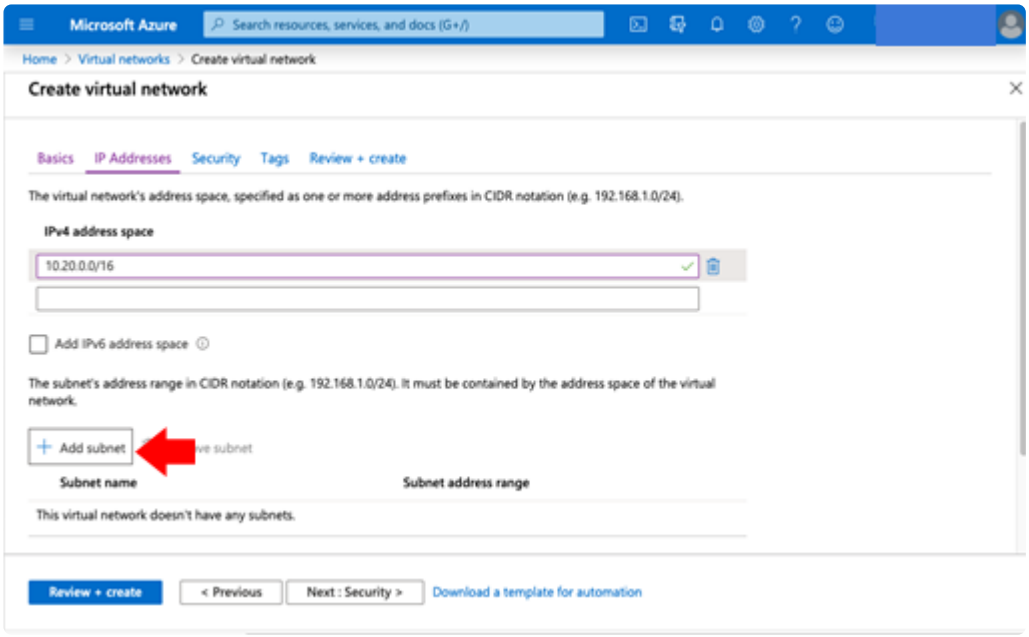
1. **Azure Home** > **[Virtual networks]** > **[Add]** を選択し、次の表にしたがって設定値を入力します。

Virtual network		
Subscription	お持ちのサブスクリプション ID	Azure サービス加入時に決められたサブスクリプション ID です。
Resource group	sios20rg	
Name	sios20vnet	
Region	(Asia Pacific) Southeast Asia	
IPv4 address space	10.20.0.0/16	
Subnet		
Name	sios20sub1	
Address range	10.20.1.0/24	
BastionHost	Disabled(default)	
DDoS protection	Basic(defaut)	
Firewall	Disabled(default)	

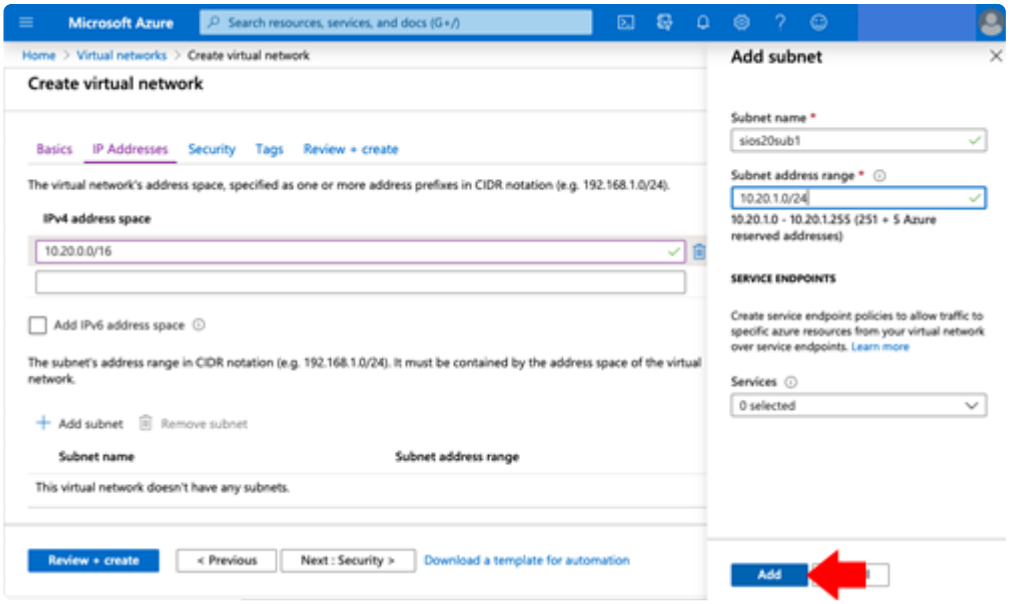
2. **[Next: IP Addresses]** をクリックします。



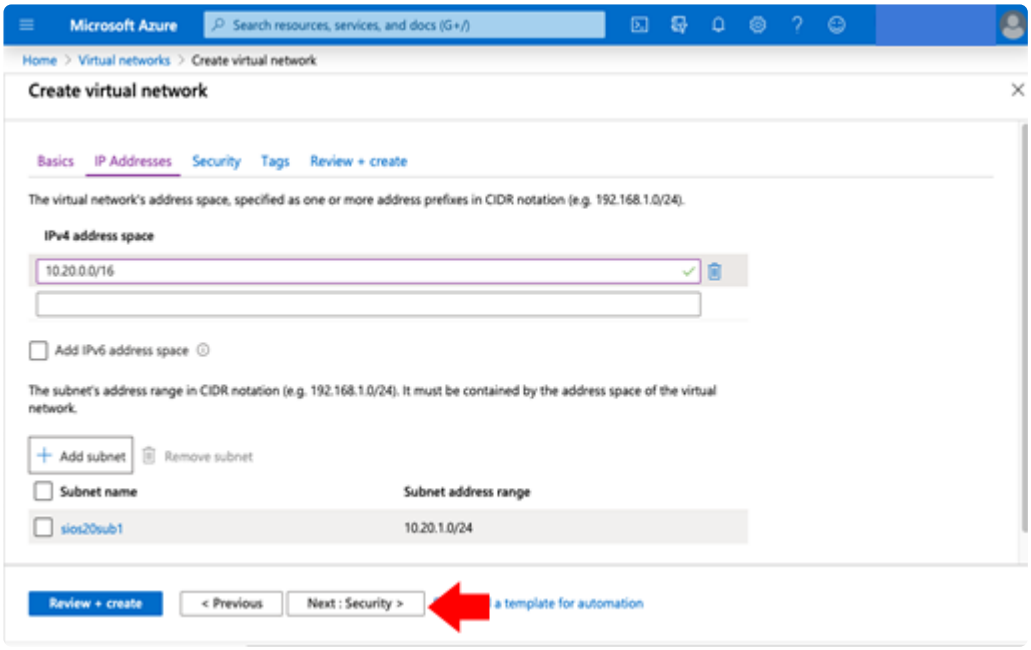
3. **[+ Add subnet]** をクリックします。



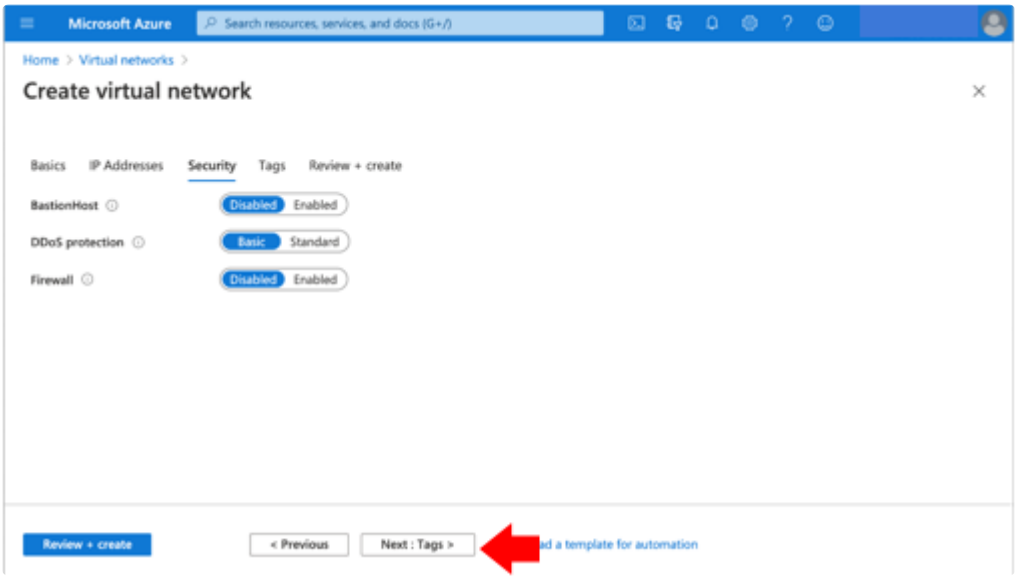
4. 右側に出てくるダイアログで一つ目のサブネットの設定値を入力し、右下の **[Add]** をクリックします。



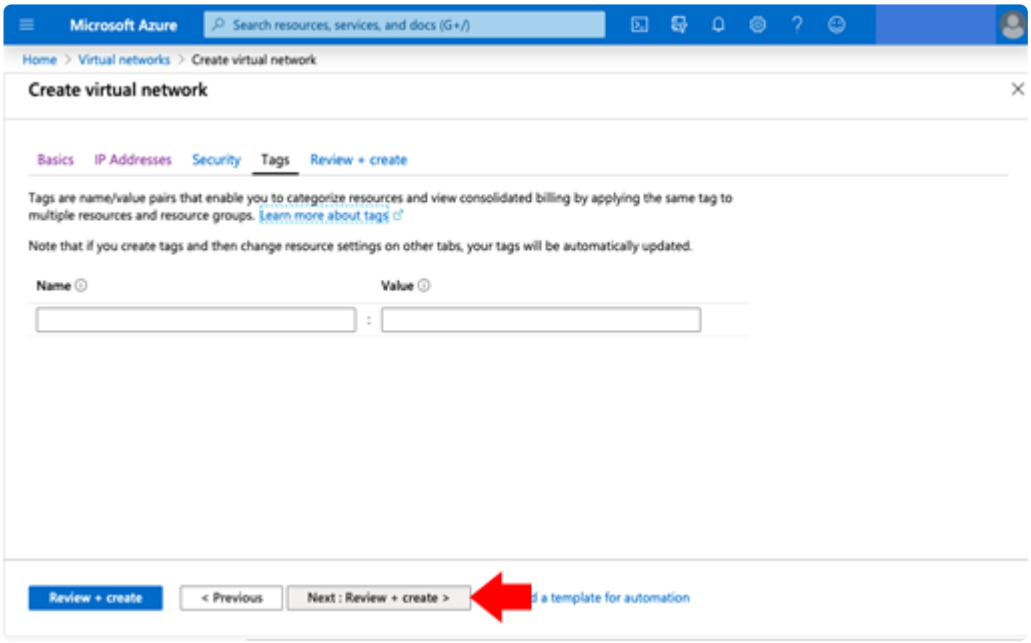
5. 新しいサブネット sios20sub1 が表示されています。**[Next: Security]** をクリックします。



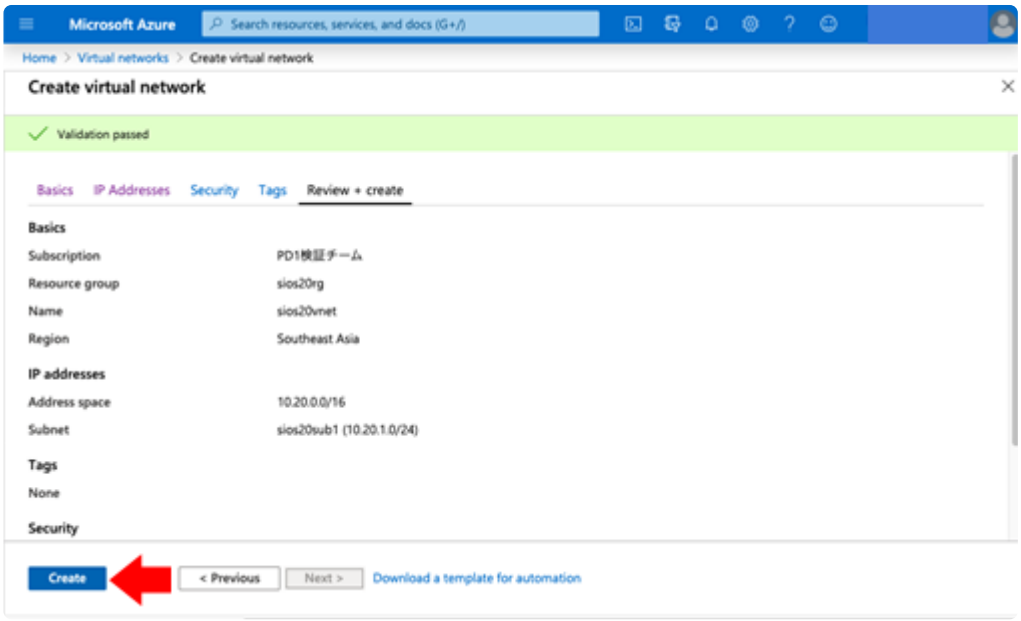
6. 何も変更せず、**[Next: Tags]** をクリックします。



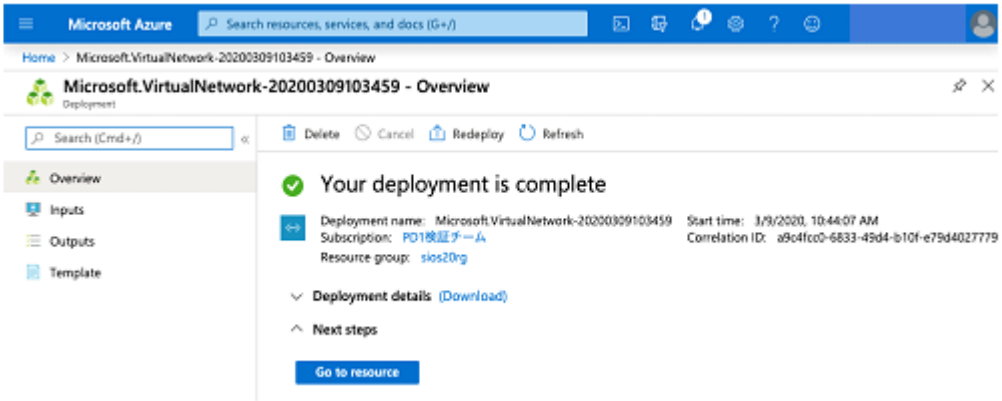
7. 何も入力せず、**[Next: Review + create]** をクリックします。



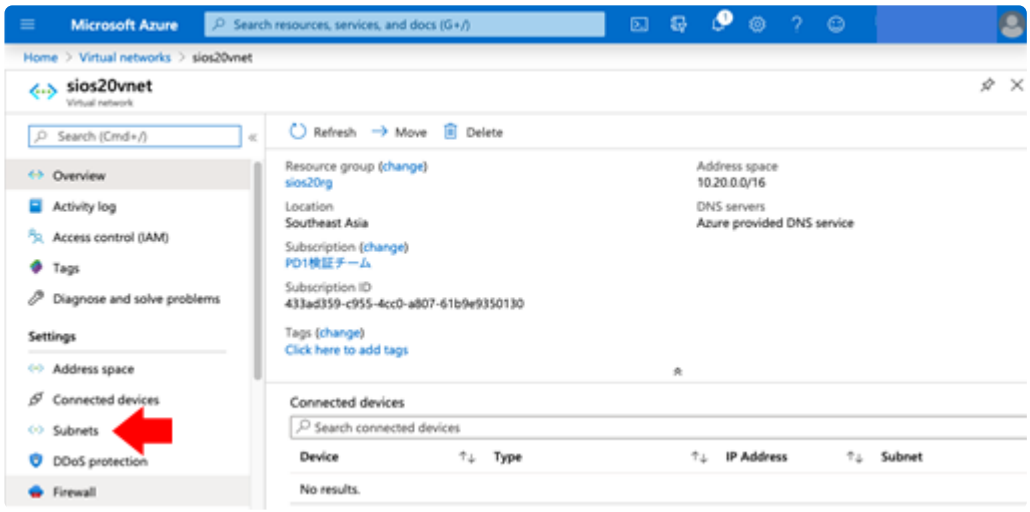
8. **[Create]** をクリックします。



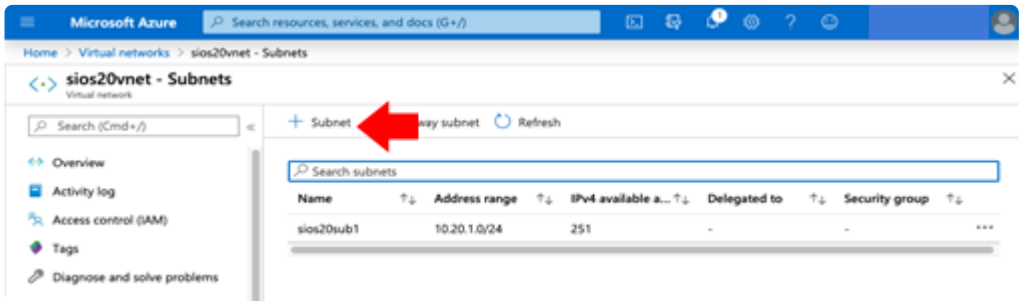
9. sios20vnet と sios20sub1 が作成され、作成が完了すると、次のような表示になります。



10. **Azure Home** > **[Virtual networks]** > sios20vnet をクリックし、左ペインの **[Settings]** > **[Subnets]** をクリックします。

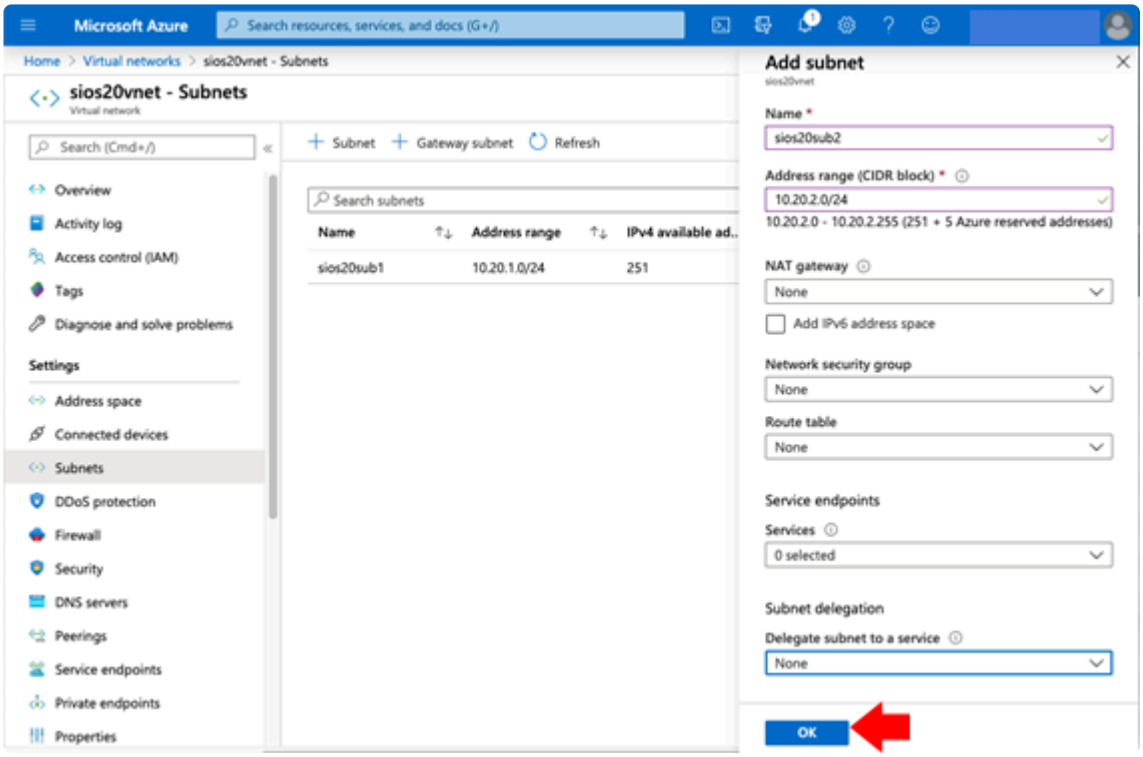


11. **[+Subnet]** アイコンをクリックします。



12. 次の表にしたがって設定値を入力し、**[OK]** をクリックします。

Subnet	
Name	sios20sub2
Address range	10.20.2.0/24
NAT gateway	None(default)
Network security group	None(default)
Route table	None(default)
Services	0 selected(default)
Delegate subnet to a service	None(default)


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Virtual networks > sios20vnet - Subnets
sios20vnet - Subnets
Virtual network
Search (Cmd+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Address space
Connected devices
Subnets
DDoS protection
Firewall
Security
DNS servers
Peerings
Service endpoints
Private endpoints
Properties
+ Subnet
+ Gateway subnet
Refresh
Search subnets
Name
Address range
IPv4 available ad..
sios20sub1
10.20.1.0/24
251
Add subnet
sios20vnet
Name *
sios20sub2
Address range (CIDR block) *
10.20.2.0/24
10.20.2.0 - 10.20.2.255 (251 + 5 Azure reserved addresses)
NAT gateway
None
Add IPv6 address space
Network security group
None
Route table
None
Service endpoints
Services
0 selected
Subnet delegation
Delegate subnet to a service
None
OK

6.4.3. クラスターノード（稼働系と待機系）の作成

重要な注意事項

- ここではクラスターを構成するノードを 2つ（稼働系と待機系）作成します。名称や IP アドレスなどの各ノード固有のパラメーターはいくつかありますが、その他の部分は作成手順も含め 2つのノードで共通です。本ページの内容を稼働系用に 1回、待機系用に 1回の計 2回実行してください。
- パラメーター表には、稼働系と待機系それぞれで設定するパラメーターが別々に記述してあります。

1. **Azure Home** > **[Virtual machines]** > **[+Add]** を選択し、次の表にしたがって設定値を入力します。

Virtual machine		
Subscription	お持ちのサブスクリプション ID	Azure サービス加入時に決められたサブスクリプション ID です。
Resource group	sios20rg	
Instance details		
Virtual machine name	SIOS20LKNODE01（稼働系） SIOS20LKNODE02（待機系）	※注1
Region	(Asia Pacific) Southeast Asia	
Availability options	Availability zone または Availability set	Availability zoneを推奨します。 ※注2
Availability zone (Availability options で Availability zone を選択した場合のみ設定)	1（稼働系） 2（待機系）	稼働系と待機系で互いに異なる Availability zone を選択してください。
Availability set (Availability options で Availability set を選択した場合のみ設定)	sios20lkcluster	稼働系のとき (create new) で作成。 待機系の時はすでに作ってあるものを参照
Image	Windows Server 2019 Datacenter	※注3
Azure Spot instance	No (default)	
Size	Standard B2ms	※注4 ※注5
Administrator account		
Username	lkadmin	
Password	XXXXXXXX	
Inbound port rules		
Public inbound ports	Allow selected ports	
Select inbound ports	RDP (3389)	

Already have a Windows Server license ?	No	Windows ライセンスを別途お持ちであれば Yes にしてください。

※注1:Virtual machine name に設定した名前が Windows のコンピューター名としても設定されます。クラスターノードが Windows ドメインに属さない場合は、Virtual machine name に小文字を含まないようにしてください。

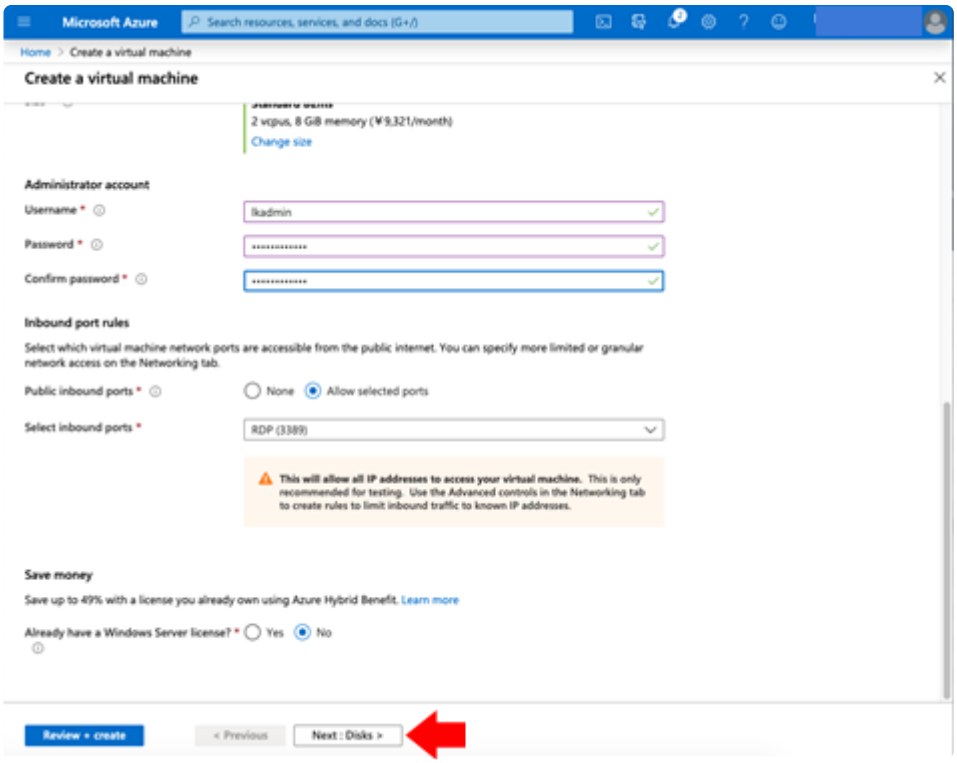
※注2:単一障害によって稼働系ノードおよび待機系ノードの両方がダウンすることを防ぐため、Availability zone または Availability set のいずれかを必ず設定してください。Availability zone を選択すると、複数のデータセンターにサーバーを分散して配置することが可能になるため、Availability set と比較してより可用性の高い設計が可能になります。ただし、利用可能なリージョンが限定されている点や、ロードバランサーやパブリック IP アドレスの SKU として安価な Basic を指定できない点に注意が必要です。

※注3:導入する LifeKeeper がサポートする OS バージョンを選択してください。LifeKeeper がサポートする OS バージョンは、各バージョンのサポートマトリクス(http://jpdocs.us.sios.com/)を参照してください。

※注4:必ず指定した Availability option が利用できるインスタンスサイズを選択してください。一部のインスタンスサイズでは Availability zone や Availability set が利用できません。

※注5:必ず負荷分散規則が利用できるインスタンスサイズを選択してください。一部のインスタンスサイズでは、負荷分散規則が利用できません。

2. 入力が終わったら、**[Next : Disks]** をクリックします。

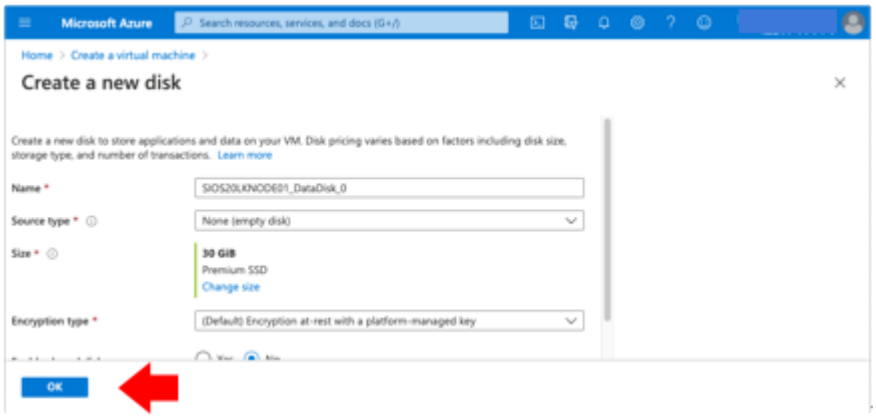


3. ディスク設定を次のように入力します。

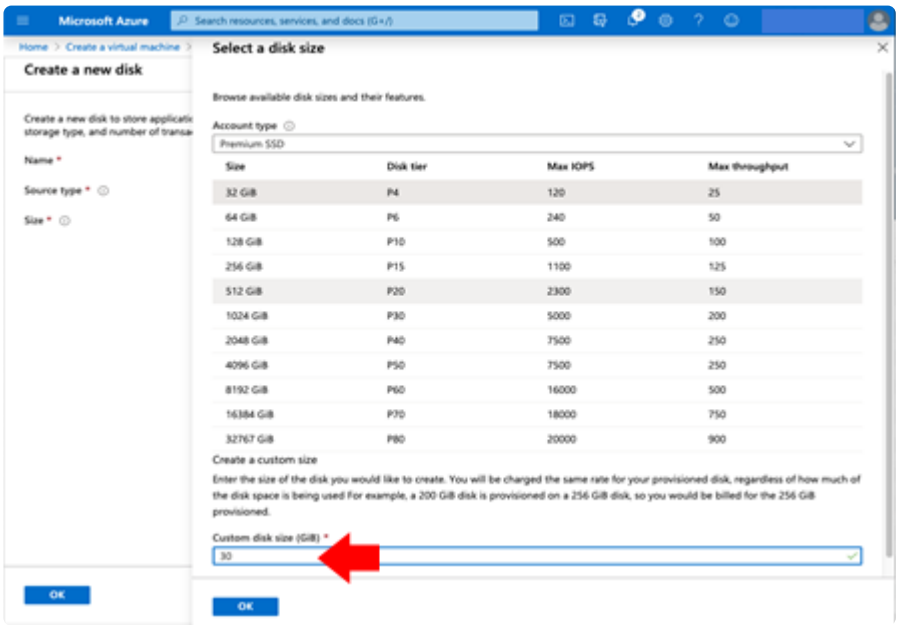
Disk

Disk options		
OS Disk type	Premium SSD (default)	
Encryption type	(Default) Encryption at-rest with a platform-managed key	
Enable Ultra Disk compatibility	No	
Data disks		
NAME	SIOS20LKNODE01_DataDisk_0（稼働系） SIOS20LKNODE02_DataDisk_0（待機系）	(create and attach a new disk) により作成
Source type	None (empty disk) (default)	
Size	30 GB	下図を参考に設定
Disk type	Premium SSD	
Encryption type	(Default) Encryption at-rest with a platform-managed key	

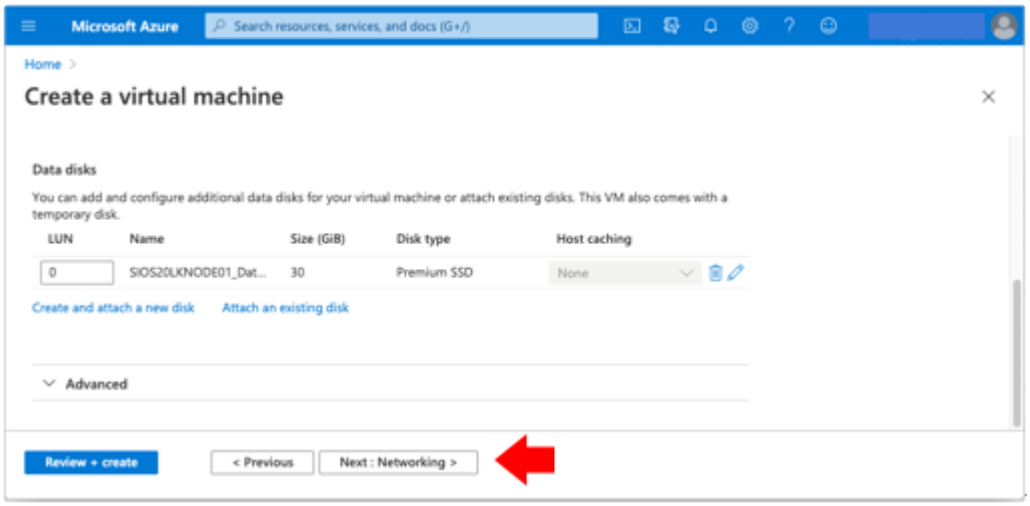
（Create and attach a new disk の画面）



（Change sizeの画面）



4. **[Next: Networking]** をクリックします。



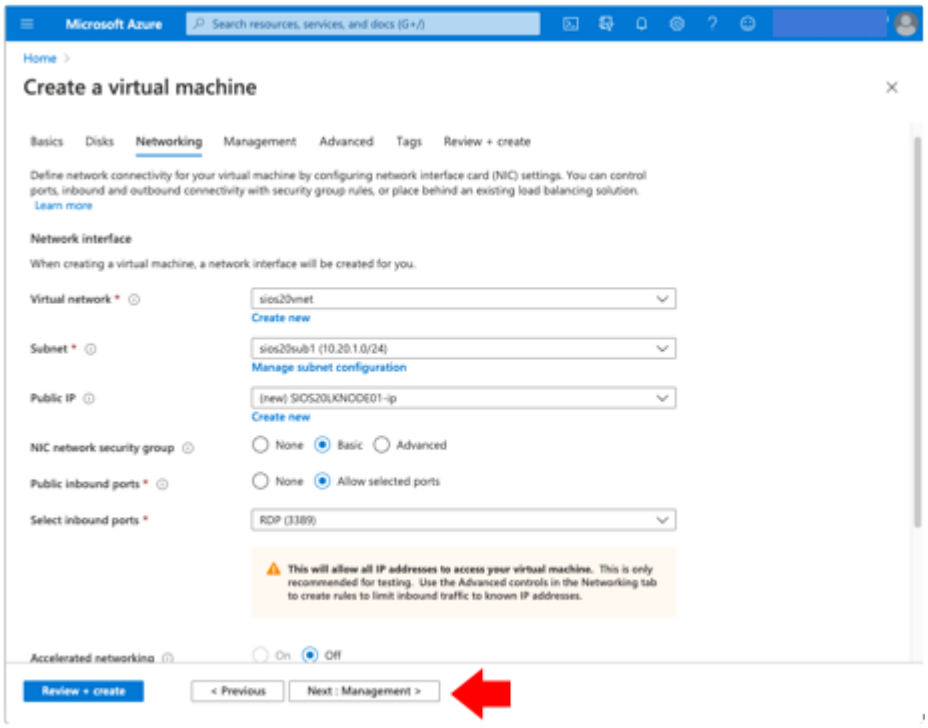
5. 次のように入力します。
作成したサブネットの 1つめ（sios20sub1）を、仮想マシンに接続します。この設定により、ネットワークインターフェースが一つ接続されます。（2つめのネットワークインターフェースは、仮想マシン作成後に作成・接続します。）

Networking			
Virtual network	sios20vnet		
Subnet	sios20sub1(10.20.1.0/24)		※注1
Public IP	Name	SIOS20LKNODE01-ip（稼働系） SIOS20LKNODE02-ip（待機系）	（create new）により作成 ※注2 設定後 OK ボタンが必要
	SKU	Standard（Availability zone を選択した場合） Basic（Availability set を選択した場合）	
	Assignment	Static	
	Availability zone （SKU に Standard を選択した場合のみ設定）	Zone 1（稼働系） Zone 2（待機系）	
NIC network security group	Basic		
Public inbound ports	Allow selected ports		
Select inbound ports	RDP (3389)		
Accelerated networking	Off (default)		
Load balancing	No (default)		

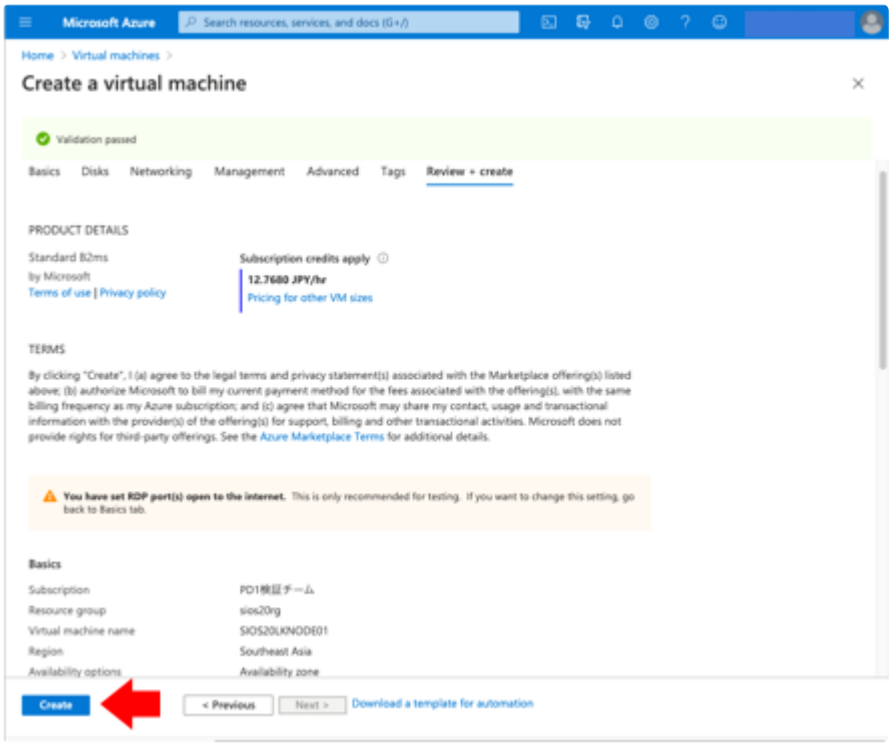
※注1：前の手順で作成した 1つめのサブネット（sios20sub1）を、仮想マシンに接続します。

※注2:本手順ではインターネット経由で各クラスターノードにアクセスするため、Public IP を設定しています。

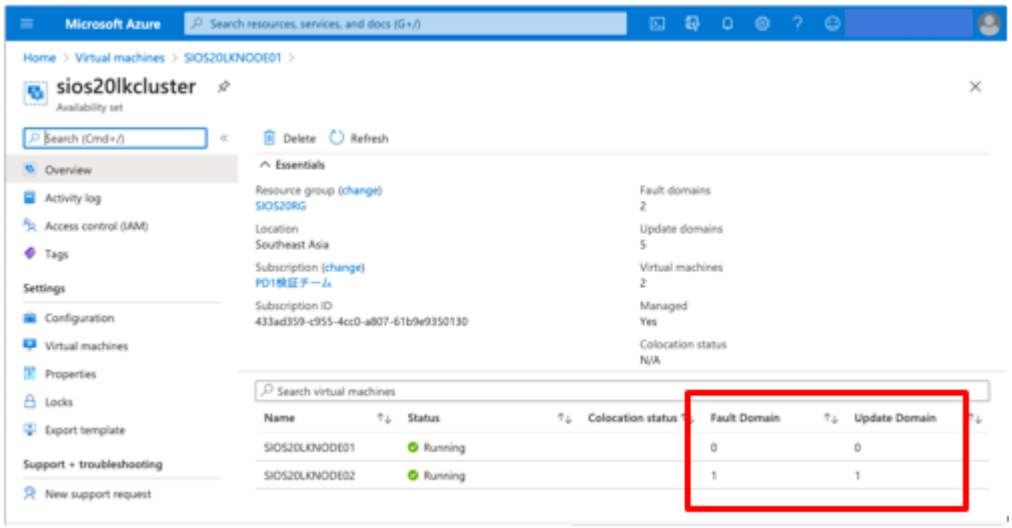
6. **[Next: Management]** 、**[Next: Advanced]** 、**[Next: Tags]** 、**[Next: Review + create]** を順にクリックします。



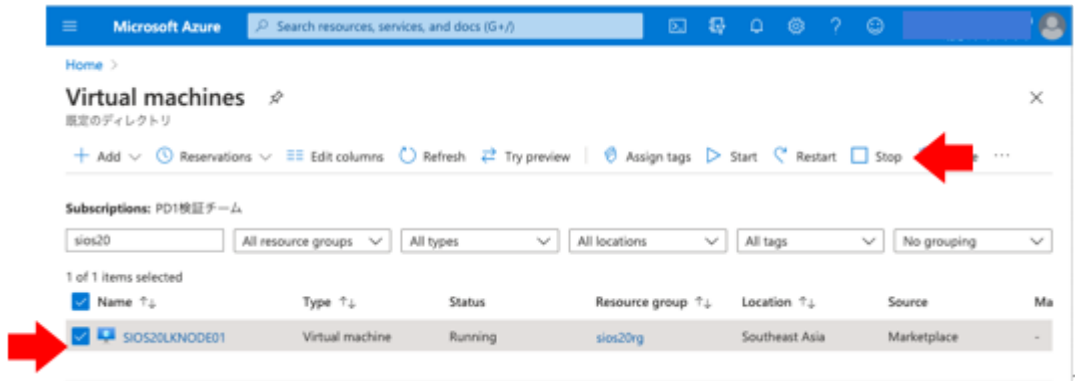
7. 設定内容が正しいことを確認し、**[Create]** をクリックします。仮想マシンの作成とデプロイメントが行われます。画面上部のメッセージが `"Your deployment is complete."` に変わるまで待ちます。



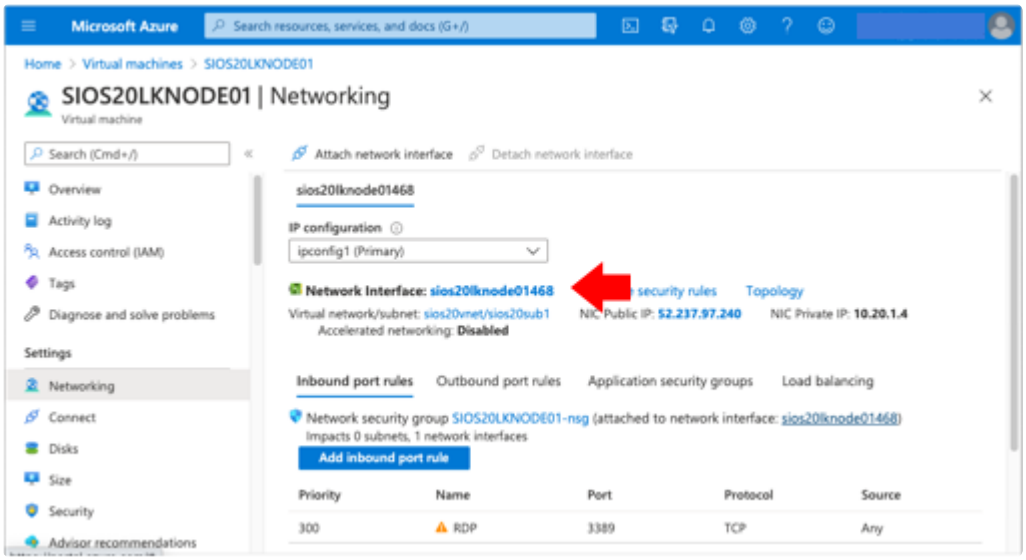
8. Availability option に Availability set を設定した場合、待機系 VM 作成後に、**Azure Home** > **[Virtual machines]** > 仮想マシン名 > **[Availability + scaling]** を開きます。Availability set 名をクリックすると Availability set に属する仮想マシンの Fault Domain と Update Domain が表示されます。待機系 VM の Fault Domain と Update Domain が稼働系 VM と異なっているかどうか確認してください。もし、同じ Fault Domain または Update Domain に待機系 VM が配置されてしまった場合は、その VM を再作成してください。



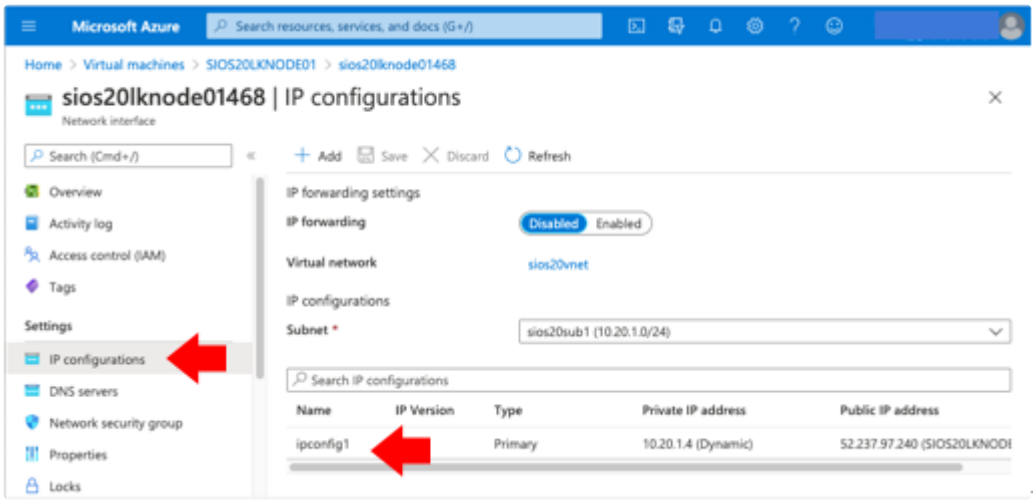
9. ネットワーク設定変更を行うため、一旦ここで作成した仮想マシンを停止します。**Azure Home** > **[Virtual machines]** で、作成したばかりの仮想マシンを選択し、**[Stop]** をクリックします。



10. **Azure Home** > **[Virtual machines]** > 仮想マシン名 > **[Networking]** を開きます。1つめのインターフェース名をクリックします。

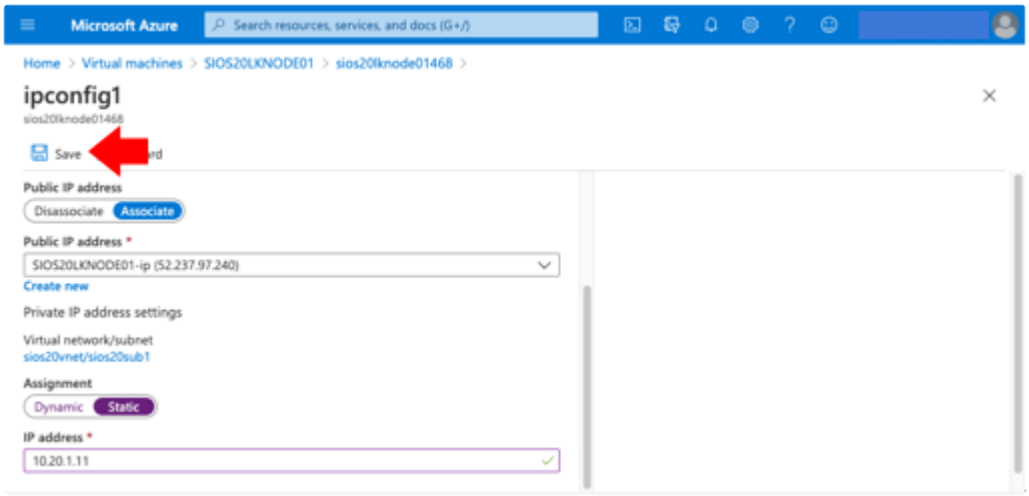


11. 左ペインの **[IP configurations]** を開いて、ipconfig1 をクリックします。



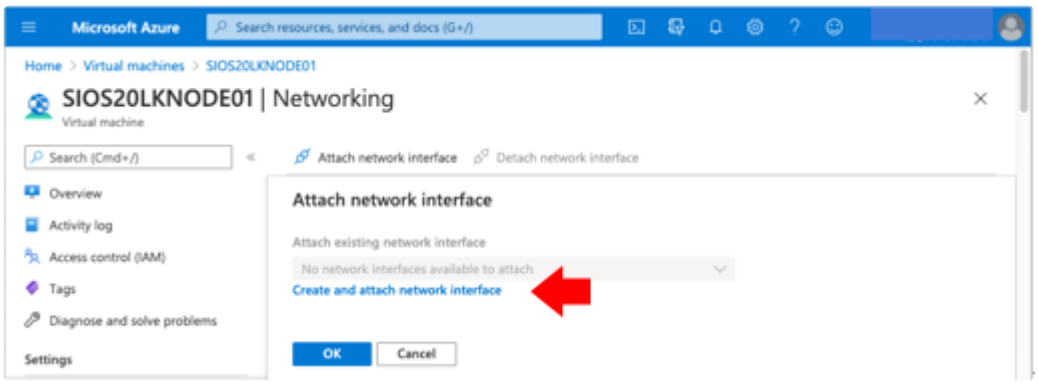
12. 次の表の通り IP アドレスのアサインモードと IP アドレスを変更して、画面上部にある **[Save]** をクリックして設定を保存します。

ipconfig	
Public IP address	Associate
Assignment	Static
IP address	稼働系：10.20.1.11 待機系：10.20.1.12



13. 次に、2つ目のネットワークインターフェースを追加します。

14. **Azure Home** > **[Virtual machines]** > 仮想マシン名 > **[Networking]** > **[Attach network interface]** をクリックし、次に **[Create and attach network interface]** をクリックします。

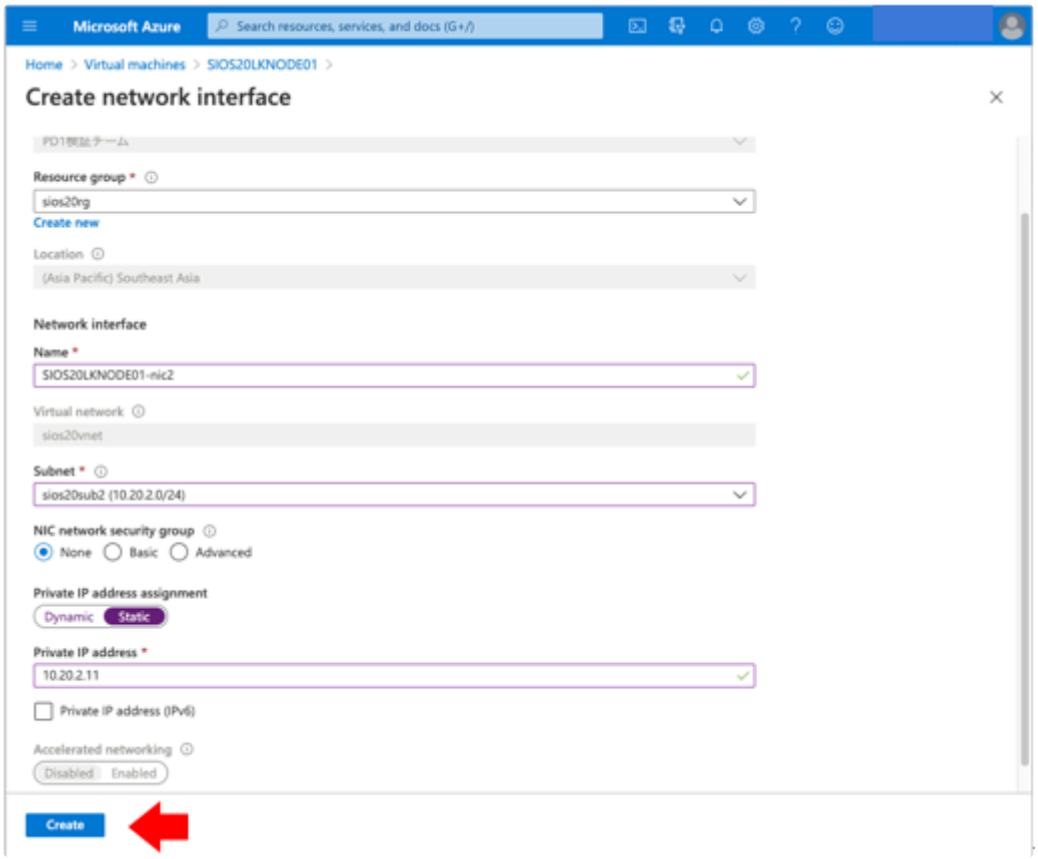


15. 次の表に従って、ネットワークインターフェースを設定し、**[Create]** ボタンを押します。

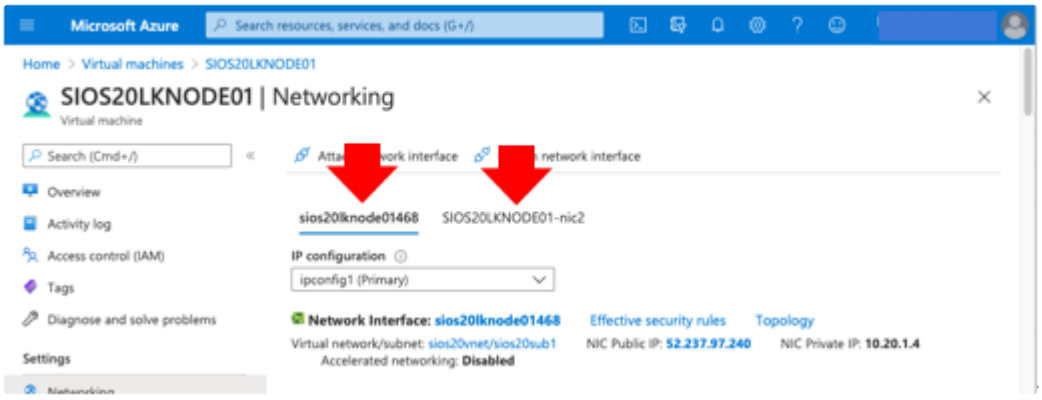
Create network interface		
Subscription	お持ちのサブスクリプション ID	Azure サービス加入時に決められたサブスクリプション ID です。(変更不可)
Resource group	sios20rg	
Location	Southeast Asia	(変更不可)
Name	稼働系: SIOS20LKNODE01-nic2 待機系: SIOS20LKNODE02-nic2	
Virtual network	sios20vnet	(変更不可)
Subnet	sios20sub2 (10.20.2.0/24)	※
NIC network security group	None	
Private IP address assignment	Static	

Private IP address	稼働系：10.20.2.11 待機系：10.20.2.12	

※：前の手順で作成した2つめのサブネット (例：sios20sub2) を、仮想マシンに対して設定します。



16. Create 及び Attach が終わったメッセージが表示されたら、インターフェースが 2つアタッチされていることを確認します。



17. **Azure Home** > **[Virtual machines]** で、作成した仮想マシンを選択し、Start をクリックして仮想マシンを起動します。

18. 本ページ(クラスターノード（稼働系と待機系）の作成)の手順を稼働系と待機系の両方について実行してください。両方が作成されたら、クライアントの作成に進みます。

6.4.4. クライアントの作成

1. **Azure Home** > **[Virtual machines]** で、**[Add]** をクリックし、次の表の通りの設定でクライアント用の仮想マシンを作成します。
   仮想マシンの作成方法はクラスターノードの場合と同じですので、スクリーンショット画像は省略します。赤の部分がクラスターノードの場合と異なっていますので、注意してください。

Basics		
Project details		
Subscription	お持ちのサブスクリプション ID	Azure サービス加入時に決められたサブスクリプション ID です。
Resource group	sios20rg	
Instance details		
Virtual machine name	SIOS20LKCLIENT	
Region	(Asia Pacific) Southeast Asia	
Availability options	No Infrastructure redundancy required (default)	
Image	Windows 10 Pro, Version 1809	
Azure spot instance	No (default)	
Size	Standard A2m_v2	
Administrator account		
Username	lkadmin	
Password	XXXXXXXX	
Inbound port rules		
Public inbound ports	Allow selected ports	
Select inbound ports	RDP (3389)	

2. **[Next: Disks]** をクリックします。ここではディスクは追加しません。

3. **[Next: Networking]** をクリックし、次のように入力します。

Networking		
Virtual network	sios20vnet	
Subnet	sios20sub1(10.20.1.0/24)	※注1
Public IP	Name:SIOS20LKCLIENT-ip SKU:Basic Assignment:Static	(create new) により作成 ※注2

		OK 必要。
NIC network security group	Basic	
Public inbound ports	Allow selected ports	
selected inbound ports	RDP (3389)	
Accelerated networking	Off (default)	
Load balancing	No (default)	

※注1:前の手順で作成したひとつめのサブネットを、仮想マシンに対して設定します。

※注2:本手順ではインターネット経由でアクセスするため、Public IP を設定しています。

4. **[Review + create]** をクリックし、内容を確認してから **[Create]** をクリックします。仮想マシンの作成とデプロイメントが行われます。画面上部のメッセージが
`"Your deployment is complete."` に変わるまで待ちます。

5. ネットワーク設定変更を行うため、一旦ここで作成した仮想マシンを停止します。**Azure Home** > **[Virtual machines]** で、作成したばかりの仮想マシンを選択し、**[Stop]** をクリックします。

6. 1つめのネットワークインターフェースを静的 IP アドレスに変更します。**Azure Home** > **[Virtual machines]** > 仮想マシン名 > **[Networking]** > 1つめのインターフェース名をクリックします。

7. 左ペインの **[IP configurations]** > ipconfig1 をクリックし、IP アドレスのアサインモードと IP アドレスを変更します。

設定値	
Public IP address	Associate
Assignment	Static
IP address	10.20.1.50

8. **[Save]** をクリックして設定を保存します。

6.4.5. ロードバランサーの作成

Azure のロードバランサーには外部ロードバランサーと内部ロードバランサーが存在しますが、今回の用途では、内部ロードバランサーを使用します。また、この内部ロードバランサーの IP アドレスの値は、後に設定する仮想 IP アドレスの値としても使用され、保護対象サービスのアクセスポイントとなります。

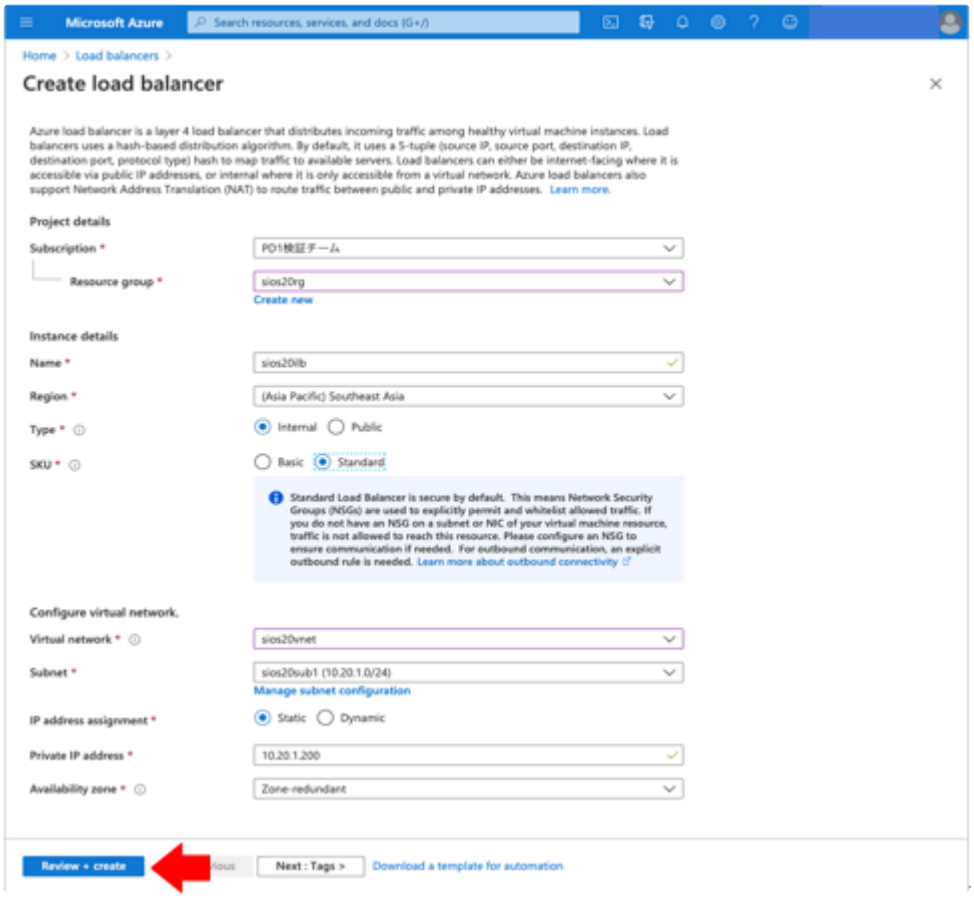
1. **Azure Home** > **[Load balancers]** > **[+Add]** を選択し、本環境で使用するロードバランサーを次の表の通り作成します。

Project details		
Subscription	お持ちのサブスクリプション ID	Azure サービス加入時に決められたサブスクリプション ID です。
Resource group	sios20rg	
Instance details		
Name	sios20ilb	
Region	(Asia Pacific) Southeast Asia	
Type	Internal	※注1
SKU	Standard（Availability zone を選択した場合） Basic（Availability set を選択した場合）	
Configure virtual network		
Virtual network	sios20vnet	
Subnet	sios20sub1 (10.20.1.0/24)	
IP address assignment	Static	
Private IP address	10.20.1.200	※注2
Availability zone（SKU に Standard を選択した場合のみ設定）	Zone-redundant	

※注1：内部ロードバランサーを作成するため、必ず **[Internal]** を選択します。

※注2：この値が後に設定する仮想 IP アドレスの値としても使用され、保護対象サービスのアクセスポイントとなります。

2. **[Review + Create]** をクリックし、内容を確認してから **[Create]** をクリックします。

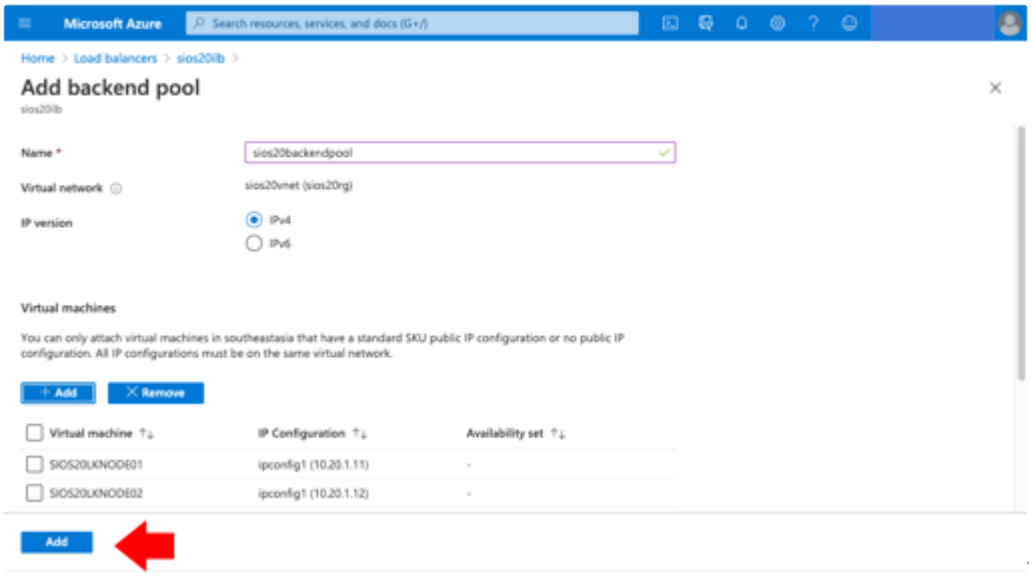


3. 作成済のクラスター用の仮想マシン 2台を内部ロードバランサーのバックエンドプールに追加します。**Azure Home** > **[Load balancers]** > ロードバランサー名 > **[Backend pools]** > **[Add]** を選択し、次のように設定します。

Add backend pool		
Name	sios20backendpool	
IP version	IPv4	
Associated to （SKU に Basic を選択した場合のみ設定）	Virtual machine	
Target #1		
Virtual machine	SIOS20LKNODE01	
IP address	ipconfig1 (10.20.1.11)	※
Target #2		
Virtual machine	SIOS20LKNODE02	
IP address	ipconfig1 (10.20.1.12)	※

※：バックエンドプールを、作成済の仮想マシンがもつプライマリー（一つめの）ネットワークインターフェースに紐づけます。

4. **[Add]** をクリックし、バックエンドプールが作成されたことを確認します。

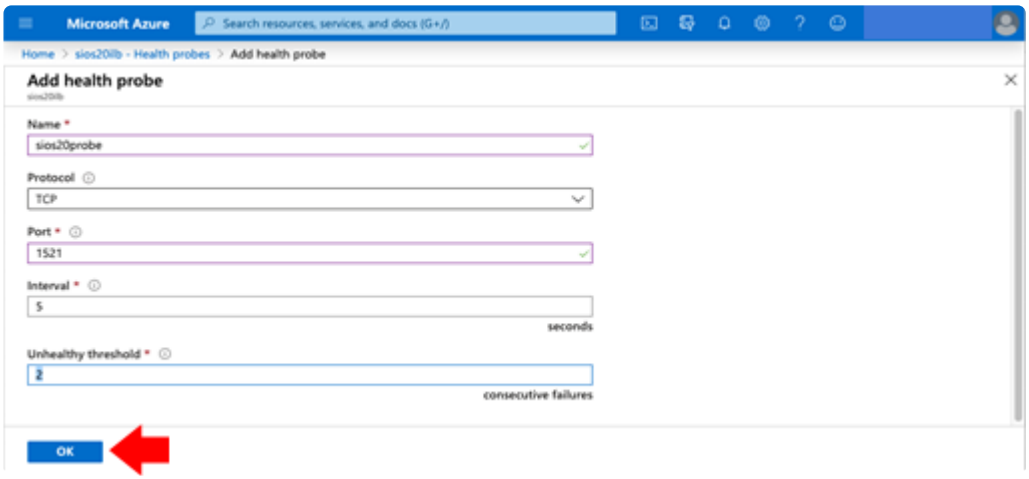


5. **Azure Home** > **[Load balancers]** > ロードバランサー名 > **[Health Probes]** > **[+Add]** をクリックし、次のように設定します。

Health probe		
Name	sios20probe	
Protocol	TCP	※
Port	1521（Oracle） 5432（PostgreSQL）	※
Interval	5	
Unhealthy threshold	2	

※：プローブ用には、アプリケーションが使用するプロトコルおよびポートを指定します。

6. **[OK]** をクリックして、プローブが作成されたことを確認します。

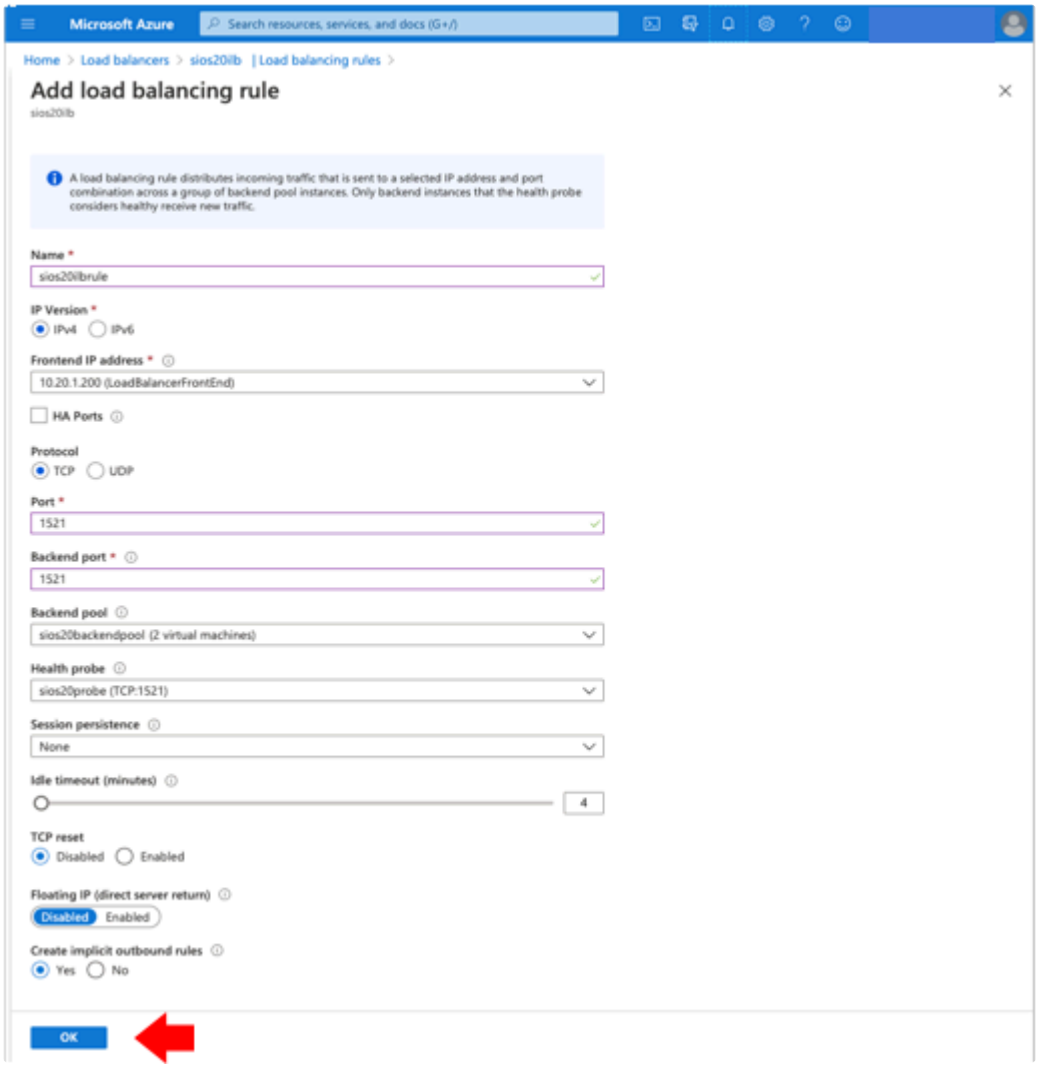


7. 続けて、負荷分散規則を設定します。**Azure Home** > **[Load balancers]** > ロードバランサー名 > **[Load balancing rules]** > **[Add]** をクリックして、次のように設定します。

Add load balancing rule		
Name	sios20ilbrule	
IP Version	IPv4	
Frontend IP address	10.20.1.200 (LoadBalancerFrontEnd)	
HA Ports （SKU に Standard を選択した場合のみ設定）	チェックしない	
Protocol	TCP	
Port	1521 (Oracle) 5432 (PostgreSQL)	※
Backend port	1521 (Oracle) 5432 (PostgreSQL)	※
Backend pool	sios20backendpool (2 virtual machines)	
Health probe	sios20probe (TCP:1521 / 5432)	
Session persistence	None (default)	
Idle timeout	4 (default)	
TCP reset （SKU に Standard を選択した場合のみ設定）	Disabled (default)	
Floating IP	Disabled (default)	
Create implicit outbound rules （SKU に Standard を選択した場合のみ設定）	Yes	

※：負荷分散用のポートには、アプリケーションが使用するポートを指定します。

8. **[OK]** をクリックして、負荷分散規則が作成されていることを確認します。



9. **Azure Home** > **[Virtual machines]** を開き、次の 3台の仮想マシンをスタートし、RDP で lkadmin としてログインしてください。ドメインをお使いの場合は、3台ともドメインに参加させ、ドメインの管理者としてログインしてください。（本ガイドではドメインへの参加手順は省きますが、以下では、sios20.local ドメインに参加し、SIOS20\lkadmin でログインするものとします。）

- SIOS20LKNODE01
- SIOS20LKNODE02
- SIOS20LKCLIENT

6.5. OS の設定

仮想マシンへのログイン（稼働系、待機系、クライアント）

1. **Azure Home** > **[Virtual machines]** > **[Overview]** > **[Connect]** を選択し、Remote Desktop（RDP）接続先情報（IP アドレス）を得ます。

2. 手元の PC などから RDP 接続します。

セキュリティ設定（稼働系、待機系）

1. IE enhanced security configuration を適切に設定します。本ガイドでは下記のように OFF に設定しています。

   [Server Manager] > **[Local Server]** > **[IE enhanced security configuration]** を off

2. Windows defender firewall を環境および使用するアプリケーションに合わせて適切に設定します。本ガイドでは下記のように OFF に設定しています。

   [Server Manager] > **[Local Server]** > **[Windows Defender Firewall]** > domain、private、public network を全て off。

セキュリティ設定（クライアント）

1. Windows defender firewall を環境および使用するアプリケーションに合わせて適切に設定します。本ガイドでは下記のように OFF に設定しています。

   [Control panel] > **[System and Security]** > **[Windows Defender and Firewall]** > **[Turn Windows Defender Firewall on or off]** で、domain、private、public network を全て off。

ディスクの設定（稼働系、待機系）

追加した 30GB のディスクを、Windows の disk manager で NTFS フォーマットして F ドライブとします。設定は下記の通りです。

New Simple Volume Wizard		
Simple volume size	30717	Maximum disk space と同じ値を指定
Assign the following drive letter	F	

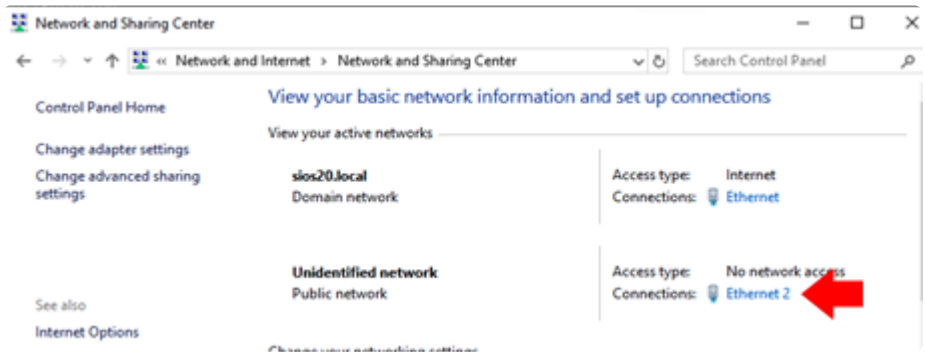
File system	NTFS	
Allocation unit size	Default	
Volume label	New Volume	
Perform a quick format	check	
Enable file and folder compression	uncheck	

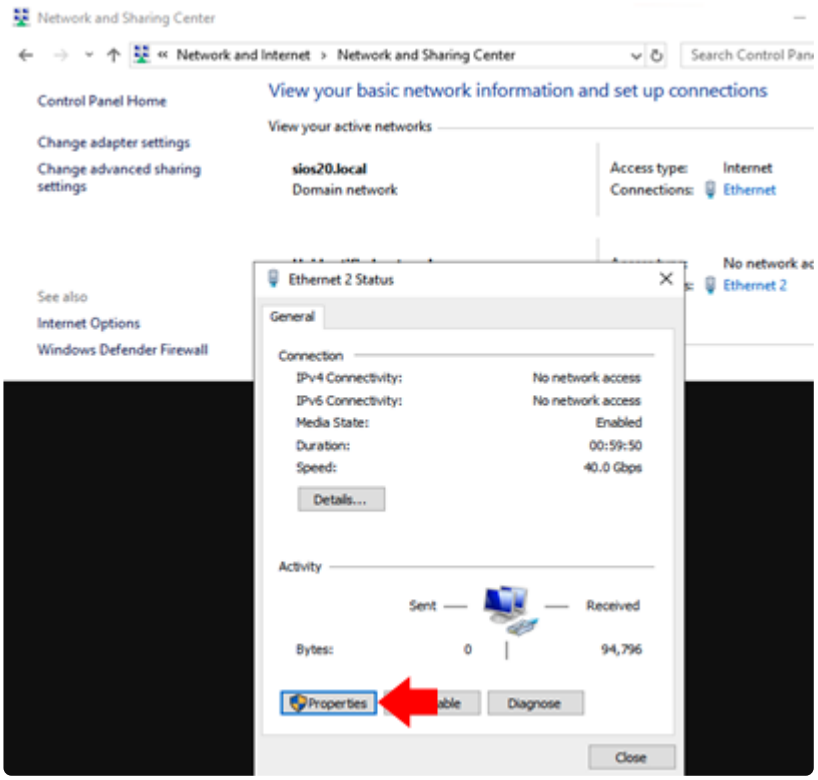
DNS 動的更新の無効化（稼働系、待機系）

LifeKeeper が（ILB の代表 IP アドレス（10.20.1.200）と同じ IP アドレスの）VIP リソースを Active にしたときに、Windows OS が自動的に VIP アドレスとコンピューター名の組を DNS サーバーに登録してしまうと、LifeKeeper GUI がコンピューター名から IP アドレスに名前解決するときに VIP アドレス（10.20.1.200）に解決してしまうなどの不都合が生じます。ここでは、それを防ぐために、LifeKeeper の VIP リソースを活性化する NIC の DNS の動的更新を無効化します。

1. **[Control Panel]** > **[Network and Internet]** > **[Network and Sharing Center]**
   10.20.2.0/24 に接続されたネットワークインターフェースをクリック

- ipconfig で、10.20.2.11 または 10.20.2.12 が活性化された NIC を探して、そのアダプター名（Ethernet、Ethernet 2など）を特定します。
- ここでは、そのアダプター名をもった NIC のリンクをクリックします。

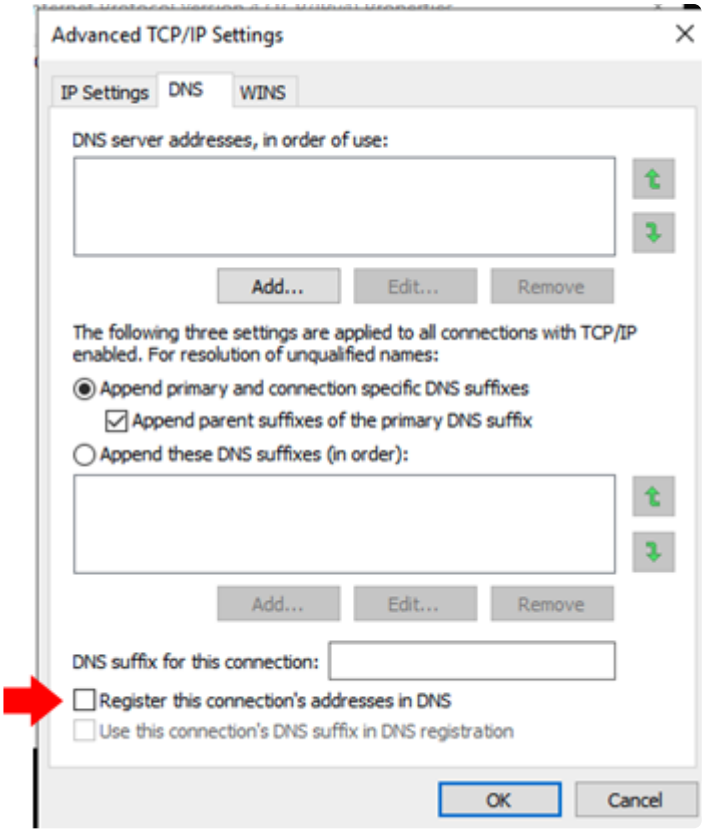




2. 次の順にダイアログを開きます。

   [Properties] > **[Internet Protocol Version 4 (TCP/IPv4)]** をクリック > **[Properties]** > **[Advanced]** > **[DNS]** タブ

3. **[Register this connection's address in DNS]** のチェックを外します。



NIC の Routing Metric の固定化（稼働系、待機系）

LifeKeeper が必要とするネットワーク設定です。

1. **[Control Panel]** > **[Network and Internet]** > **[Network and Sharing Center]**

2. 10.20.1.xx が活性化されたNIC

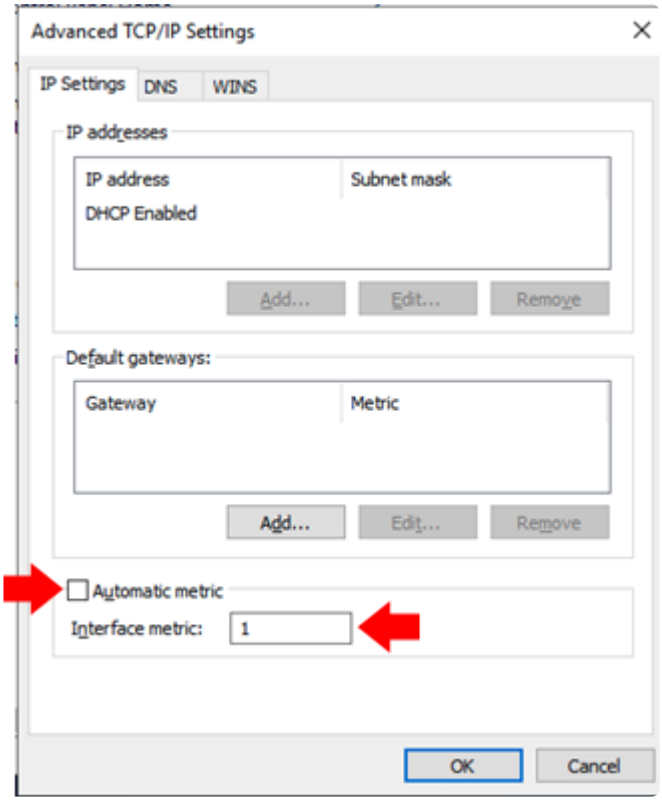
   [Ethernet] > **[Properties]** > **[Internet Protocol Version 4 (TCP/IPv4)]** をクリック > **[Properties]** > **[Advanced]**

   - **[Automatic metric]** を uncheck
   - **[Interface metric]** を 1

3. 10.20.2.xx が活性化された NIC

   [Ethernet] > **[Properties]** > **[Internet Protocol Version 4 (TCP/IPv4)]** をクリック > **[Properties]** > **[Advanced]**

   - **[Automatic metric]** を uncheck
   - **[Interface metric]** を 2



設定を有効にするため、仮想マシンを再起動します。

6.6. SIOS Protection Suite for Windows による HA クラスターの構築

SPS をインストールし、HA クラスターを構築します。

LifeKeeper のインストール（稼働系、待機系）

1. LifeKeeper v8.7.0 のインストールイメージ（ISO 形式）を入手して任意の場所に置き、ダブルクリックして開きます。インストールイメージ（製品版または評価版）の入手方法については、こちら よりお問い合わせください。

2. 開いたフォルダーの中の \Core を開き、LK-8.7.0-Setup.exe をダブルクリックして実行します。

3. ウィザードに従い、既定値でインストールします。

LifeKeeper	
Destination Folder	C:¥LK
Setup type	Typical

4. License Key Manager で、ライセンスキーを設定します。

5. **Finish** をクリックして、仮想マシンを再起動します。

アプリケーション用 ARK のインストール（稼働系、待機系）

Oracle の環境構築の場合、ここで Oracle ARK をインストールします。PostgreSQL の ARK は LifeKeeper に含まれるため、ここでは必要ありません。

1. LifeKeeper インストールイメージの中の \Recovery_Kits を開き、LKOra-8.7.0-Setup.exe をダブルクリックします。

2. ウィザードに従い、既定値でインストールします。

DataKeeper のインストール（稼働系、待機系）

1. DataKeeper v8.7.0 のインストールイメージ（ISO 形式）を入手して任意の場所に置き、ダブルクリックして開きます。インストールイメージ（製品版または評価版）の入手方法については、こちら よりお問い合わせください。

2. DataKeeper を開き、DK-8.7.0-Setup.exe をダブルクリックします。

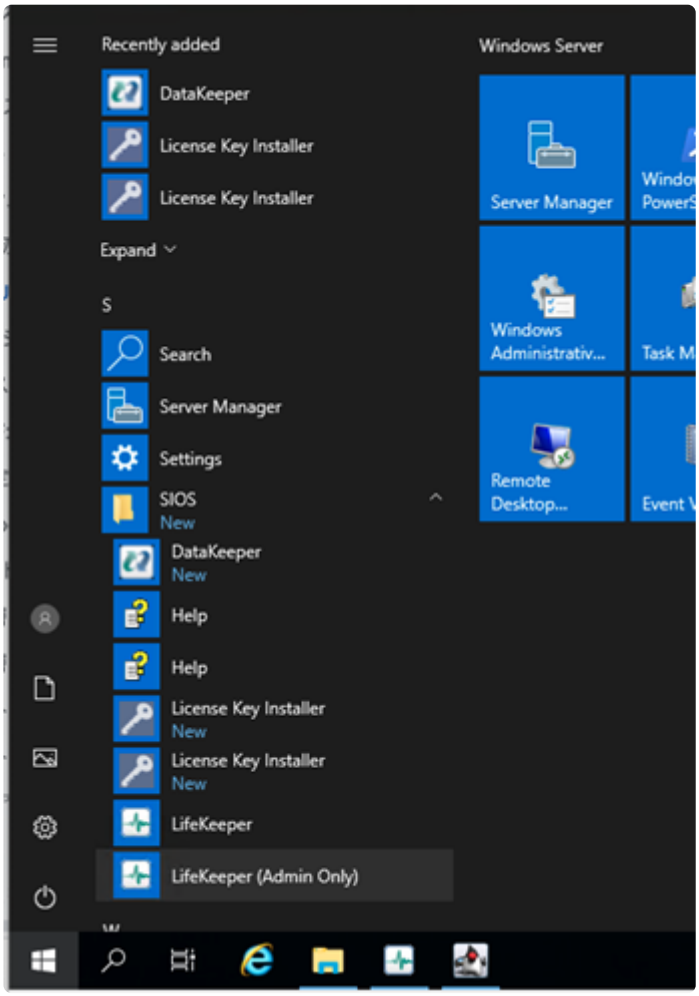
3. ウィザードに従い、インストールします。LifeKeeper および DataKeeper のサービスログオンアカウントは共に SIOS20\lkadmin とします。LifeKeeper と DataKeeper で同じサービスログオンアカウントを使用するため、途中のダイアログで「 **Synchronize LifeKeeper Account (recommended)** 」を選択してください。

4. License Key Manager で、ライセンスを設定します。それが終わったら、ライセンスマネージャーを exit して、クラスターノードを再起動します。

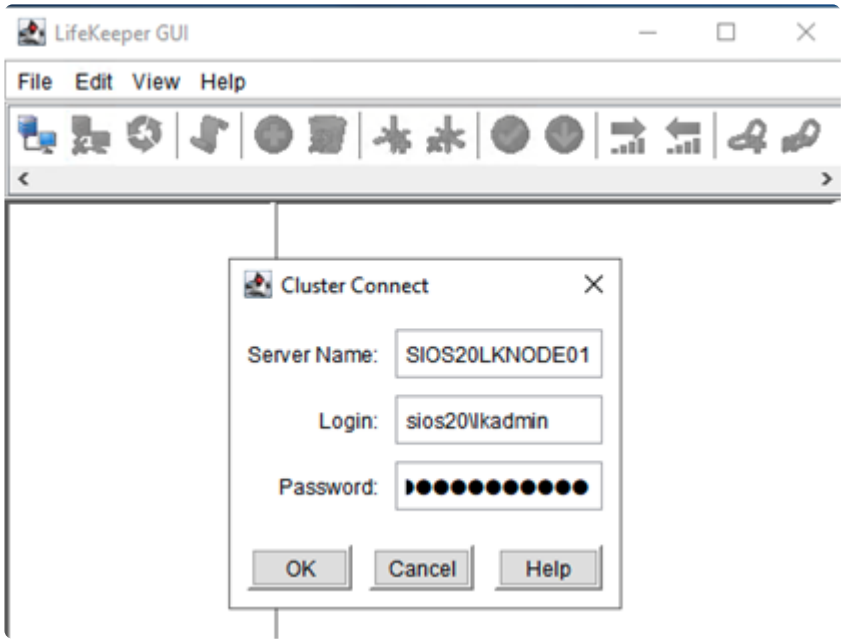
LifeKeeper GUI の初期設定

LifeKeeper GUI へのログイン

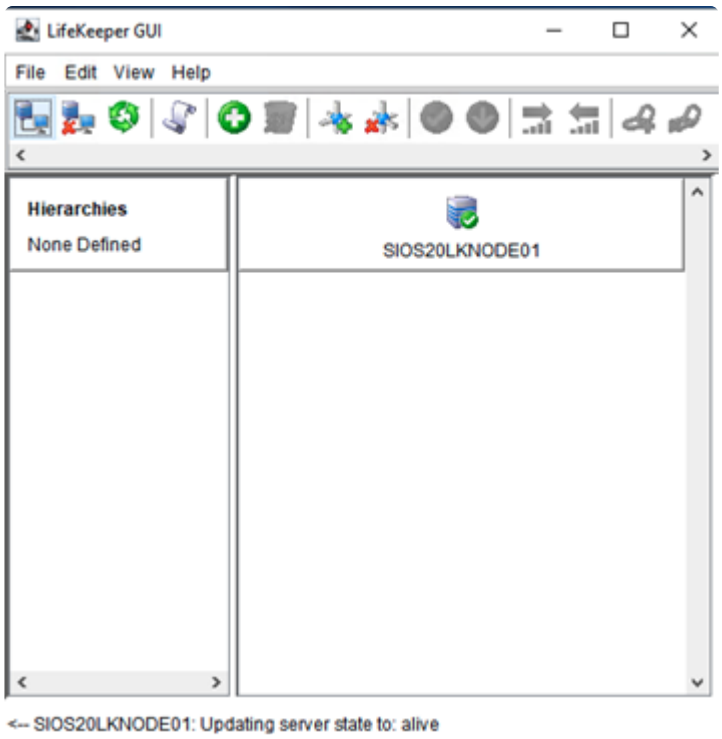
1. 1台目のクラスターノード（SIOS20LKNODE01）の Windows OSに SIOS20\lkadmin でログインします。



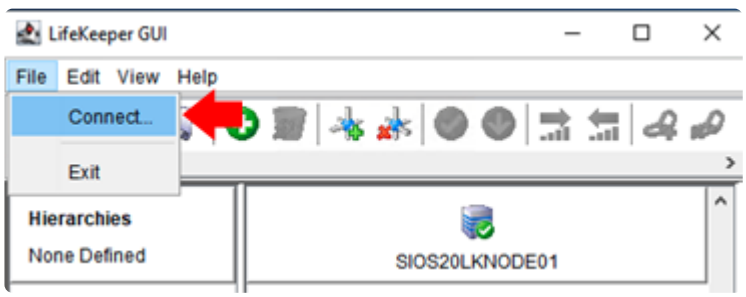
2. **[Start]** > **[SIOS]** > **[LifeKeeper (admin only)]** で、GUI を起動し、SIOS20\lkadmin でログインします。

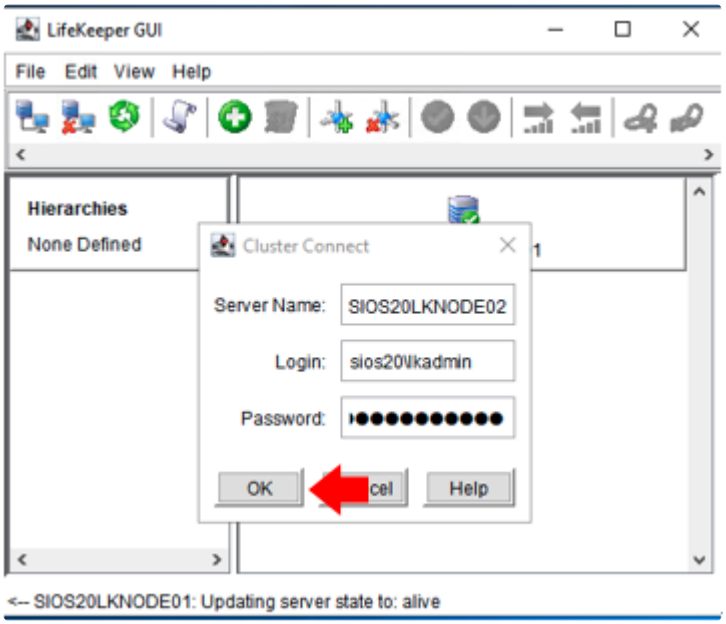


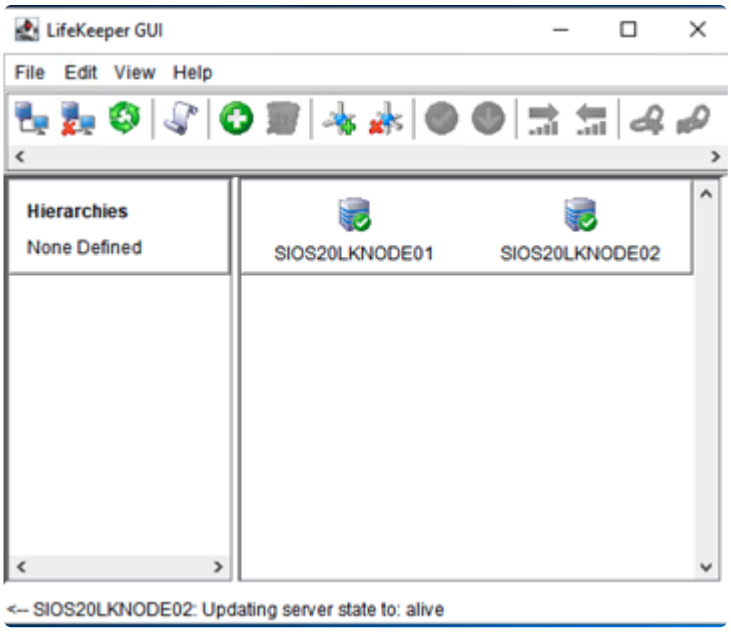
3. SIOS20LKNODE01 にログインすると、次のような画面が表示されます。



4. 次に SIOS20LKNODE02 に connect します。
   以降続くスクリーンショットは、画面の遷移を表しています。







2つのクラスターノードへのログインが完了しました。

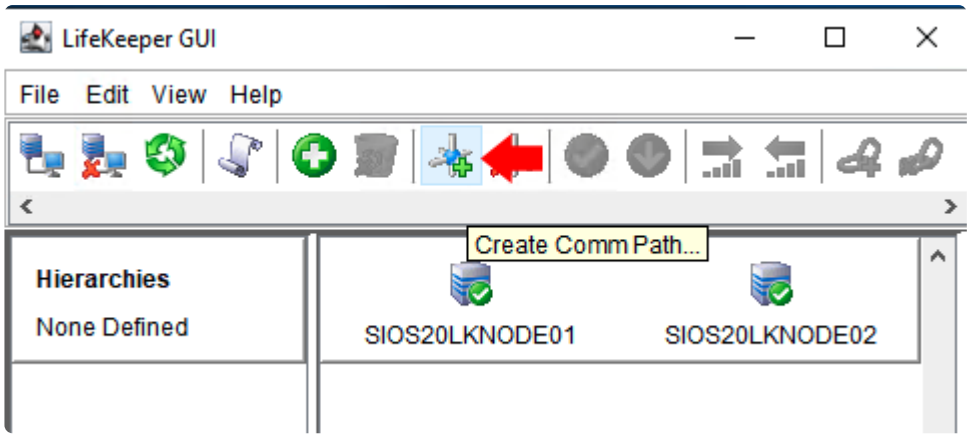
1本目のコミュニケーションパス作成

1. 続いて、クラスターノード間のコミュニケーションパスを次の表の通り作成します。

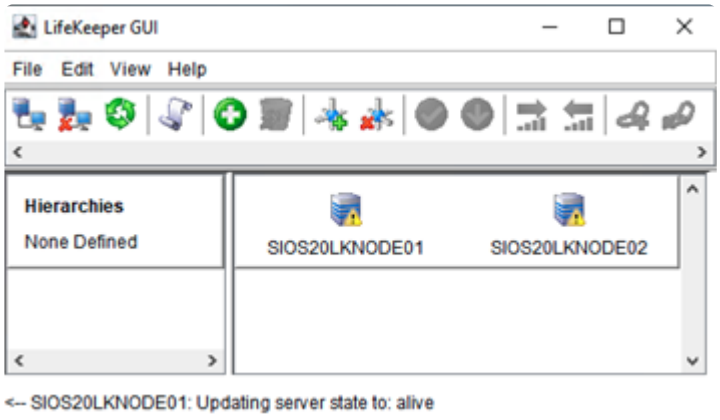
Communication path		
Local Server	SIOS20LKNODE01	
Remote Server(s)	SIOS20LKNODE02	
Device Type	TCP	
Heartbeat Interval	6	
Maximum Heartbeat	5	

Misses		
Local IP Address(es)	10.20.2.11	
Priority	1	2番目のサブネットをプライマリーコミュニケーションパスとします。
Remote IP Address	10.20.2.12	
Port#	1500	

2. **コミュニケーションパスを作成する** ボタンをクリックします。



3. ウィザードに従って設定値を入力します。作業完了すると、次のような画面が表示されます。



2本目のコミュニケーションパス作成

1. 続いて、2本目のコミュニケーションパスを作成します。
   作成の方法は、1本目のコミュニケーションパスの時と同一です。次の表に従って作成してください。

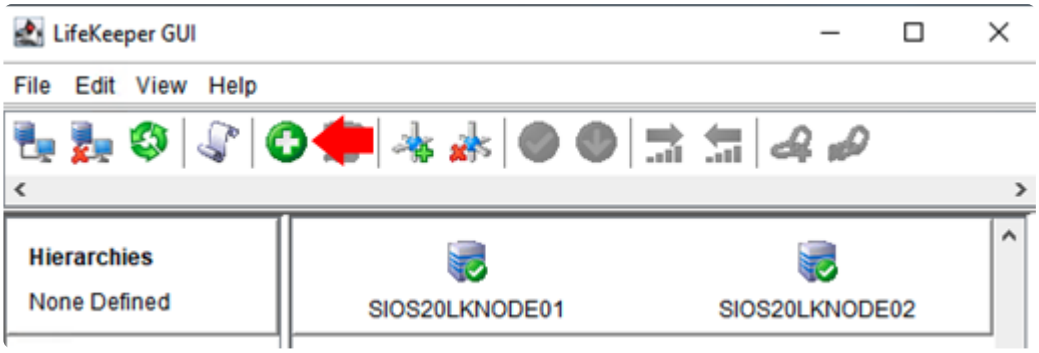
Communication path	
Local Server	SIOS20LKNODE01
Remote Server(s)	SIOS20LKNODE02
Device Type	TCP

Heartbeat Interval	6
Maximum Heartbeat Misses	5
Local IP Address(es)	10.20.1.11
Priority	2
Remote IP Address	10.20.1.12
Port#	1510

IP リソースの作成

1. 続いて、LifeKeeper GUI で IP リソースを作成します。

   [Create Resource Hierarchy]（緑色の＋ボタン）をクリックします。



2. 以降は、ウィザードに従い、次の表の通り設定値を入力します。

IP address (create)		
Primary Server	SIOS20LKNODE01	
Backup Server	SIOS20LKNODE02	
Application to protect	IP Address	
IP Address	10.20.1.200	※注1
Subnet Mask	255.255.255.255	※注2
IP Resource Tag	10.20.1.200	
Network Connection	Ethernet 2	※注3
Local Recovery	No	

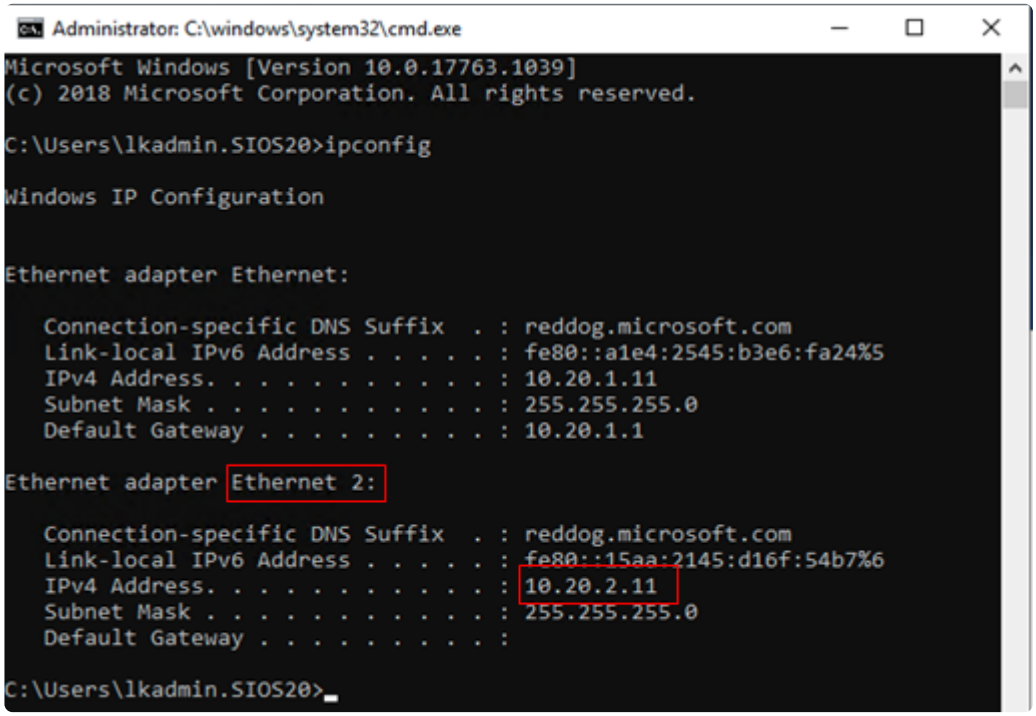
IP address (extend)		
Subnet Mask	255.255.255.255	※注2
Network Connection	Ethernet 2	※注3
Target Restore Mode	Enable	

Target Local Recovery	No	
Backup Priority	10	

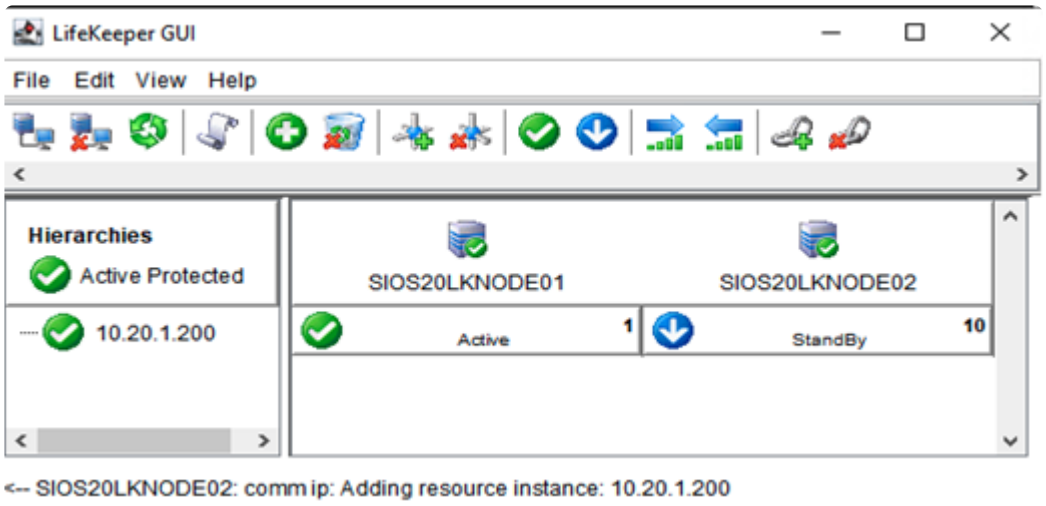
※注1:設定済の Azure ロードバランサーのフロントエンド IP と同じ値を使用します。

※注2:IPリ ソースの設定時に、Subnet Mask は、(本ガイドの例ではサブネット 10.20.1.0/24 に対する)ルーティングの競合を避けるため 255.255.255.255 を設定してください。Subnet Mask を設定する画面ではテキストボックスに値を直接入力することが可能です。

※注3:名前は異なる場合があります。10.20.2.0/24 に接続された(2つめの)NIC の名前を選択してください。IP リソース(10.20.1.200)とは「異なる」サブネット(10.20.1.0/24)に接続された NIC であることに注意してください。次のようにコマンドプロンプトで、ipconfig を実行し、10.20.2.11 または 10.20.2.12 が活性化されている NIC(図では Ethernet 2)を選びます。



IP リソースが作成されると、次のような画面が表示されます。



6.7. Oracle固有の環境構築

ミラーボリュームリソース階層の作成

Oracleのインストールと設定

Oracleの保護

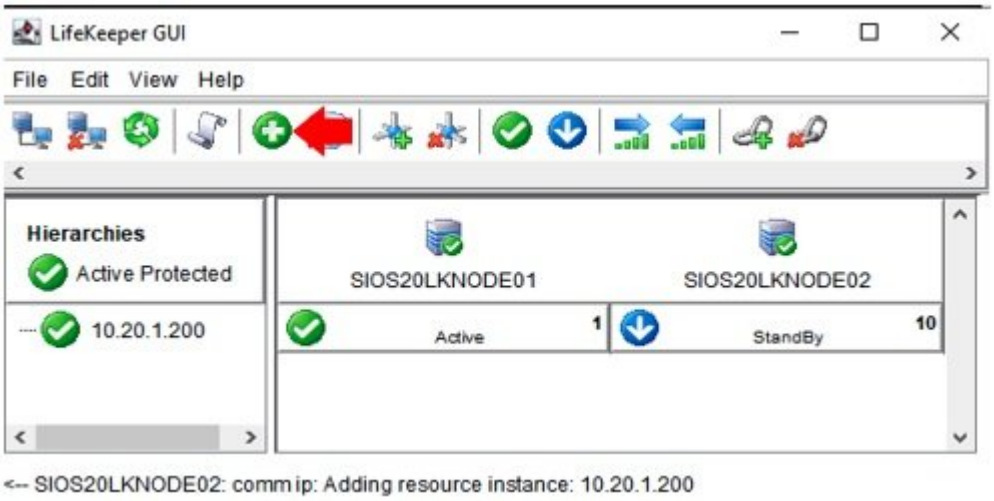
接続確認（クライアント）

6.7.1. ミラーボリュームリソース階層の作成

ここでは各クラスターノードに追加された30GBのディスク（Fドライブ）を使ってミラーボリュームを作成します。

1. SIOS20LKNODE01にログインし、LifeKeeper GUIを起動します。

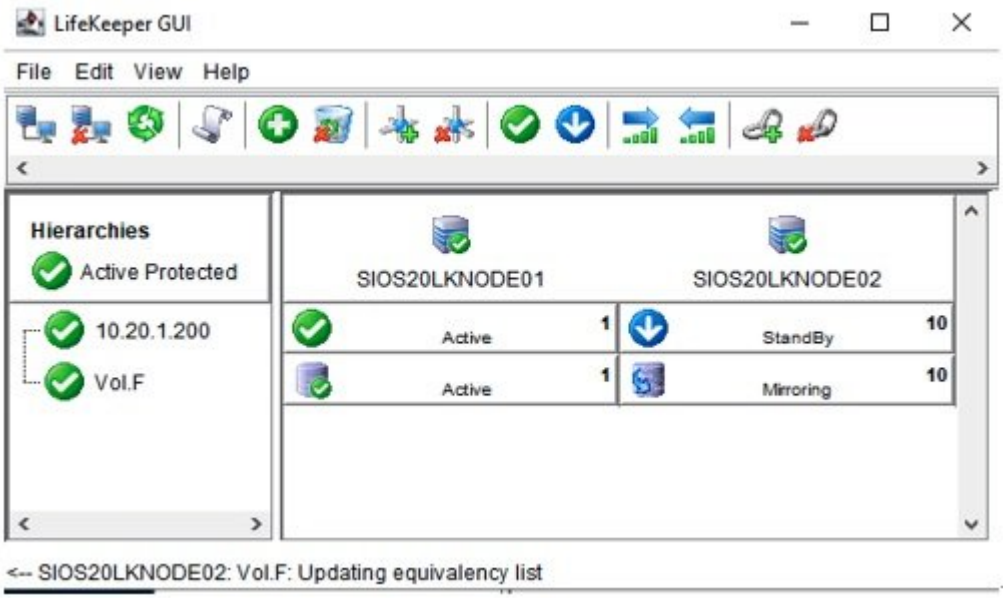
2. **[Create Resource Hierarchy]**（緑色の＋ボタン）をクリックします。



3. ウィザードに従って、次の表の通りに設定値を入力します。

IP address (create)		
Primary Server	SIOS20LKNODE01	
Backup Server	SIOS20LKNODE02	
Application to protect	Volume	スクロールしないとVolumeが見えないケースがあります。
Select Volume	F:	
Volume Tag	Vol.F	
Volume Type	Create Mirror	
Network end points (Target / Source)	10.20.2.12 / 10.20.2.11	
Mode	Asynchronous	
Backup Priority	10	

4. ミラーボリュームリソース階層が作成されると次のような画面が表示されます。


LifeKeeper GUI
File Edit View Help
Hierarchies
Active Protected
10.20.1.200
Vol.F
SIOS20LKNODE01
SIOS20LKNODE02
Active 1
StandBy 10
Active 1
Mirroring 10
<-- SIOS20LKNODE02: Vol.F: Updating equivalency list

6.7.2. Oracleのインストールと設定

Oracle Databaseのインストール（稼働系）

Oracleリスナー設定（稼働系）

パスワードファイルの作成（稼働系）

待機系Oracleインストール前の準備

Oracle Databaseのインストール（待機系）

Oracleリスナー設定（待機系）

パスワードファイルの作成（待機系）

稼働系へのスイッチバック

6.7.2.1. Oracle Databaseのインストール（稼働系）

注意: 以下の手順は、クラスターノードが属するドメインに”oracle”という名前のドメインユーザーが存在することを前提としています。存在しない場合は、以下の手順に進む前に作成するか、同等のユーザーの存在を確認しておいてください。

1. SIOS20LKNODE01にSIOS20\lkadminでログインします。

2. Oracle Databaseのインストール媒体（zipファイル）をダウンロードして任意の場所に保存します。

   - https://www.oracle.com/database/technologies/oracle19c-windows-downloads.html
   - Oracle Database 19c (19.3) for Microsoft Windows x64 (64-bit)
   - WINDOWS.X64_193000_db_home.zip

3. 次のディレクトリーを作成し、直下にzipファイルの内容を展開します。
   F:\app\oracle\product\WINDOWS.X64_193000_db_home

4. File Explorerで上のディレクトリーを開きsetup.exeをダブルクリックして実行します。

5. ウィザードに従って、次の表の通り設定値を入力します。

Oracle database		
Database Installation Options	Create and configure a single instance database.	チェックする
System Class	Server Class	
Install Type	Typical install	
Oracle Home User	Use Existing Windows User	チェックする
	User Name	SIOS20\oracle
	Password	XXXXXXXX
Typical Installation	Oracle base	F:\app\oracle
	Software location	F:\app\oracle\product\WINDOWS.X64_193000_db_home
	Storage type	File system
	Database file location	F:\app\oracle\oradata
	Database edition	Standard Edition 2
	Global database name	orcl.sios20.local

	Password	XXXXXXXX
	Create as Container database	チェックする

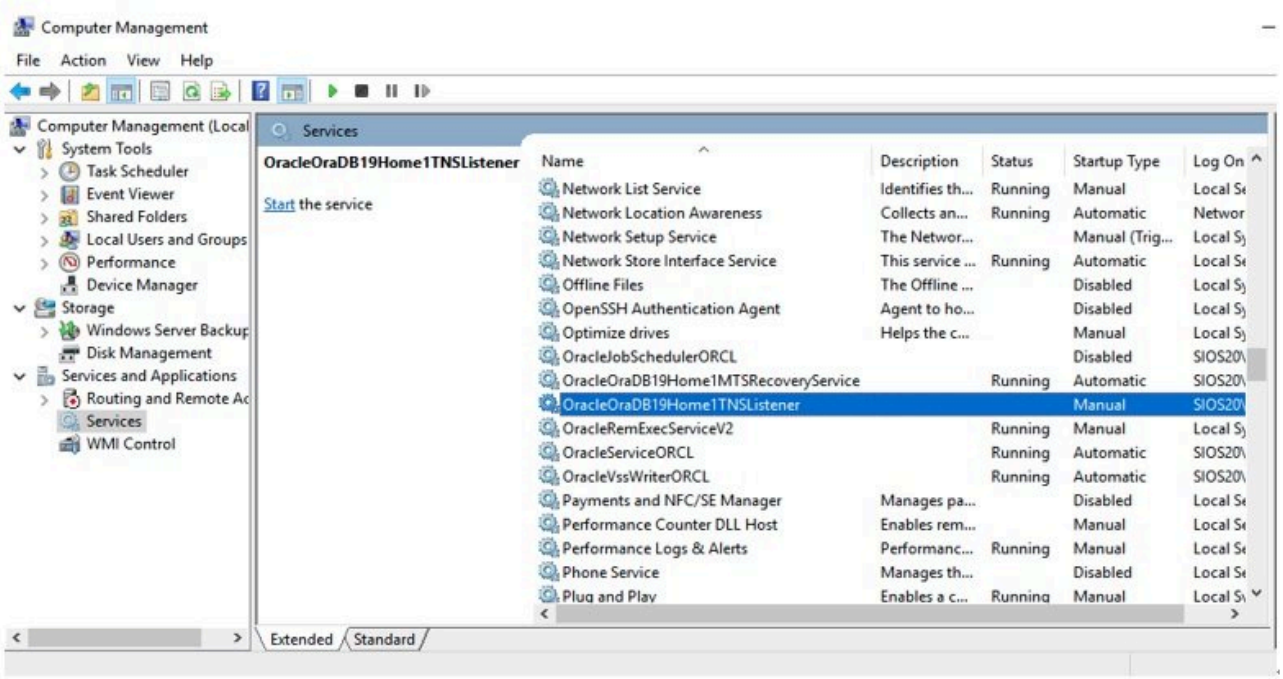
Database Configuration Assistant、Network Configuration Assistantでエラーが起こった場合は、Retryボタンをクリックして再開してください

6.7.2.2. Oracleリスナー設定（稼働系）

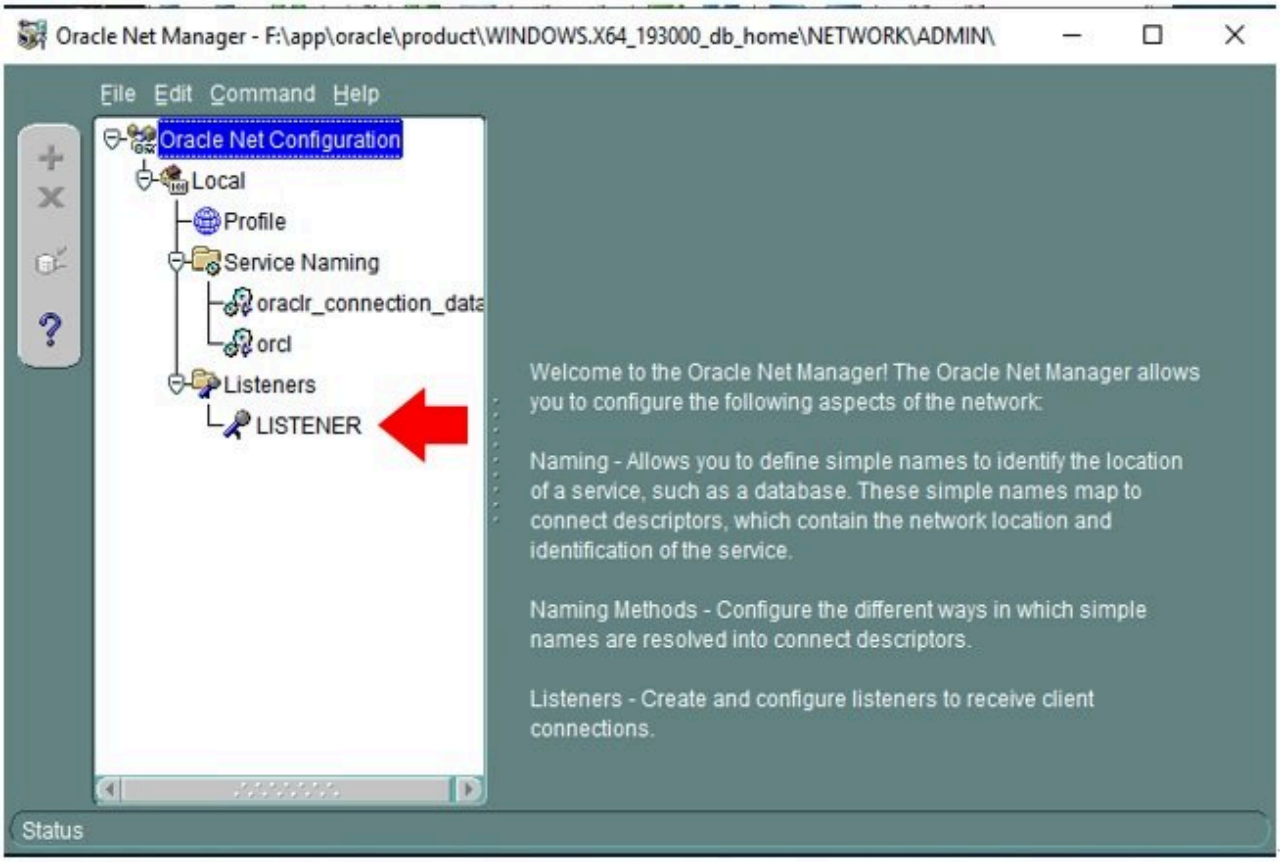
Oracleリスナーの設定をします。

1. SIOS20LKNODE01 に sios20\lkadmin でログインします。

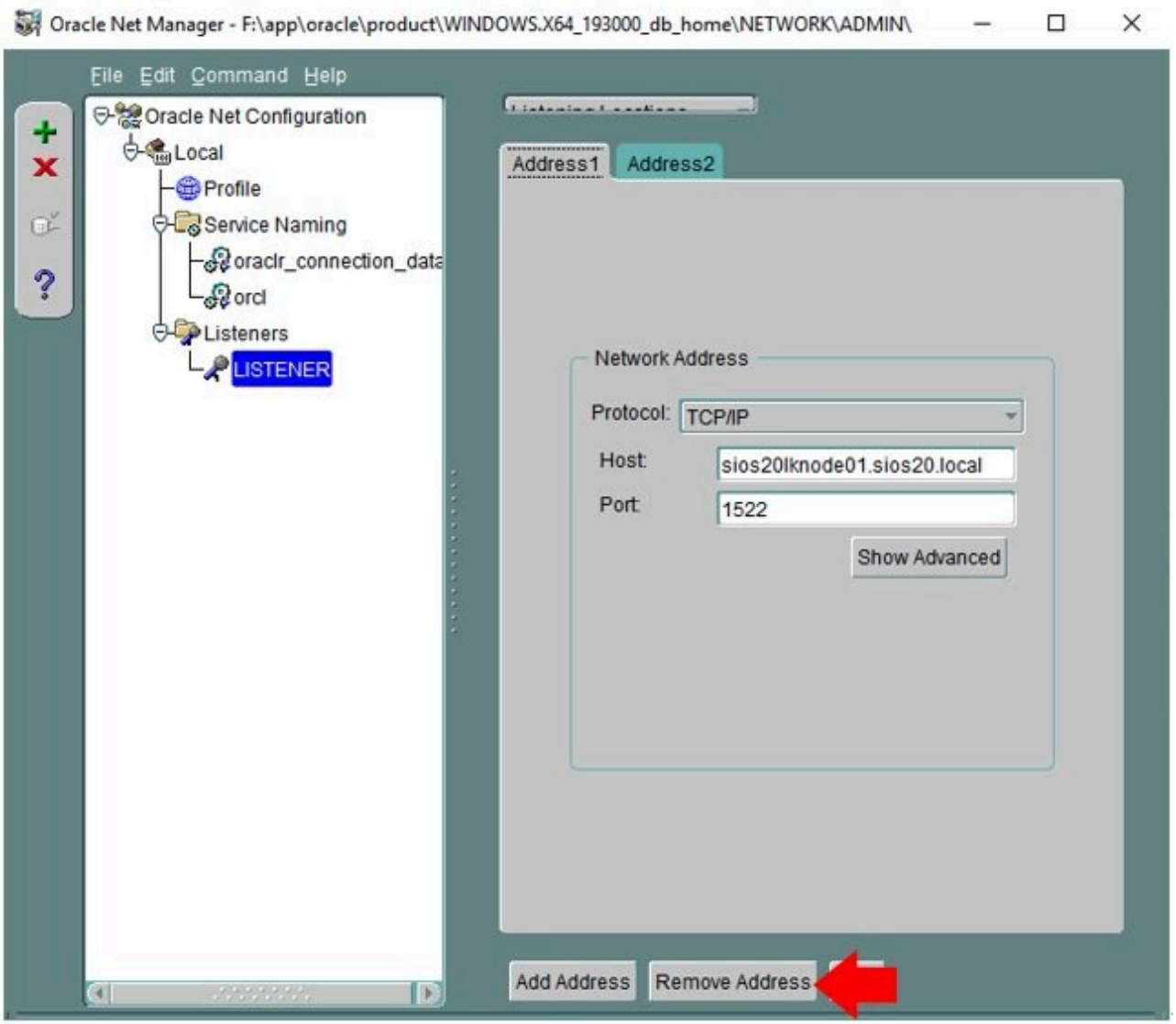
2. Windows OS のサービスコントロールマネージャーで OracleOraDB19Home1TNSListener を Stop して、Startup type を **Manual** に変更します。
   変更が終わるとこのような表示になります。



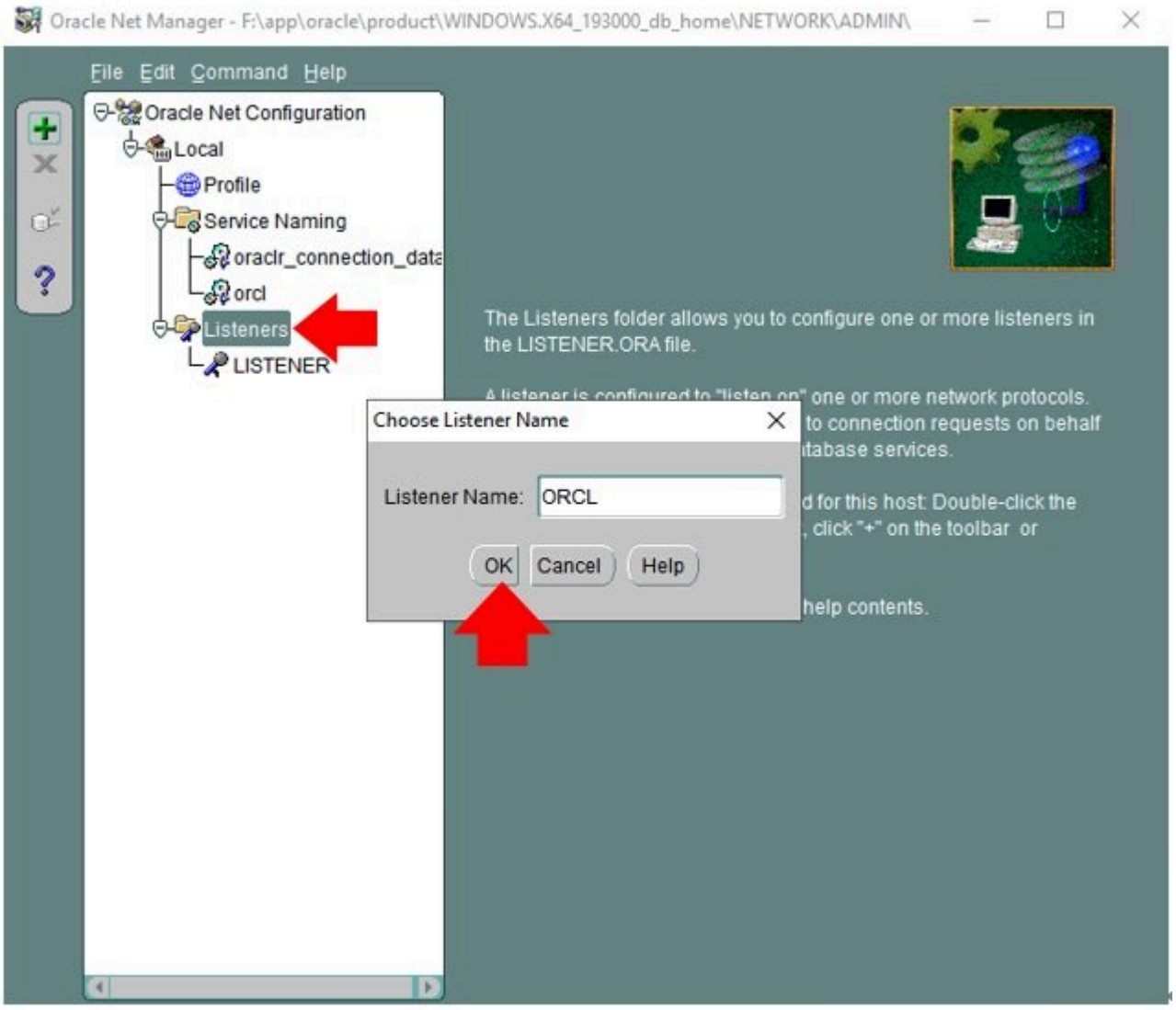
3. **Start** > **Oracle-OraDB19Home1** > **Net Manager** を起動します。
   左ペインで **Listeners** > **LISTENER** を選択し、右ペインで **Address1** を選択します。



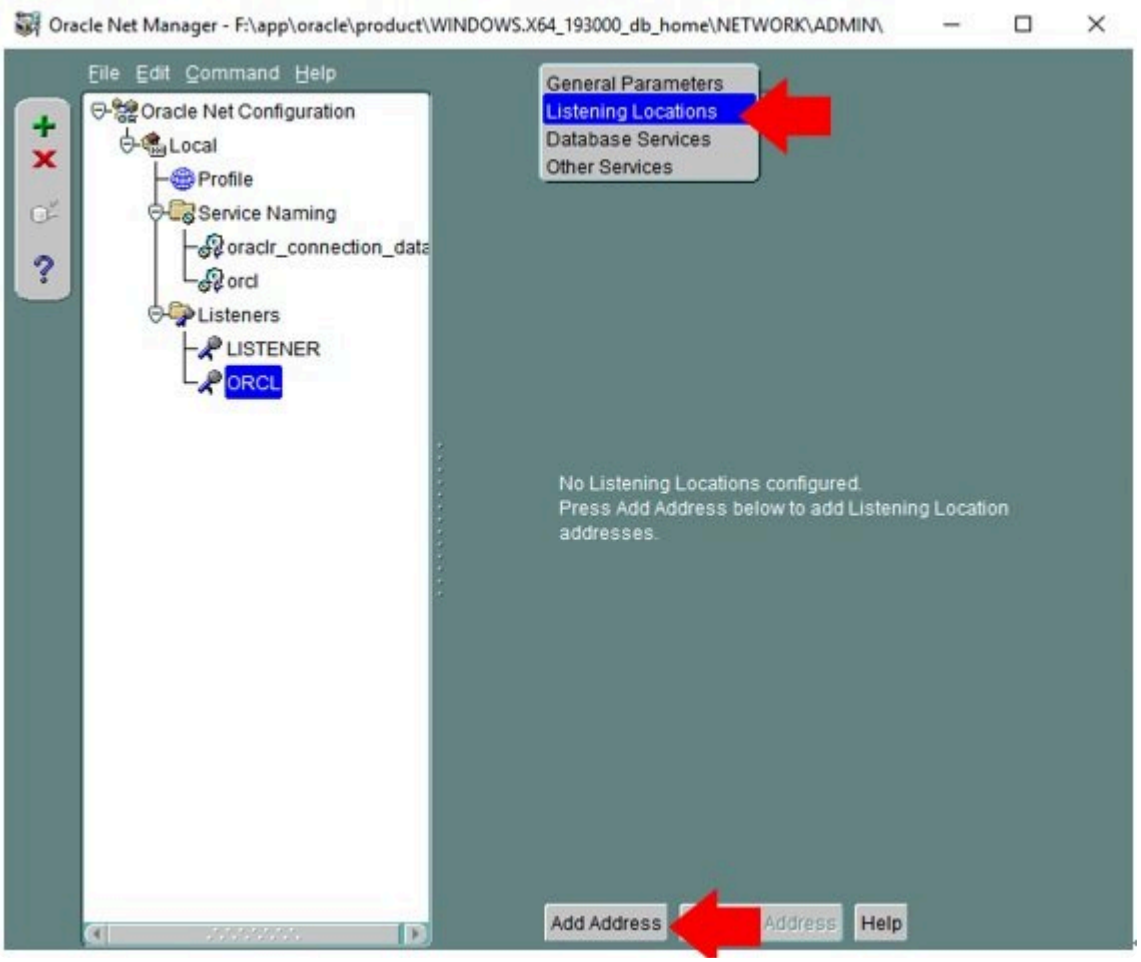
4. 下部にある **Remove Address** をクリックします。



5. 左ペインで **Listeners** を選択し、左上の ＋ ボタンをクリックして、ダイアログで **ORCL** と入力します。**OK** ボタンをクリックします。



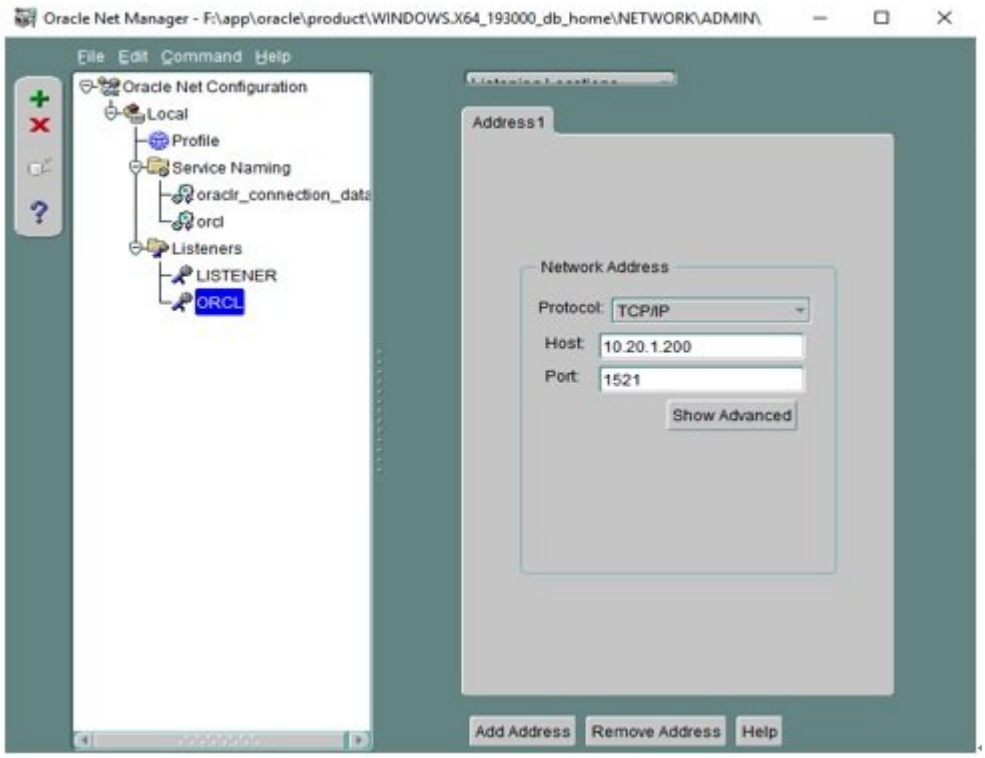
6. 左ペインで **Listeners** > **ORCL** が選択された状態で、右上のリストボックスで **Listening Locations** を選択し、下部の **Add Address** をクリックします。



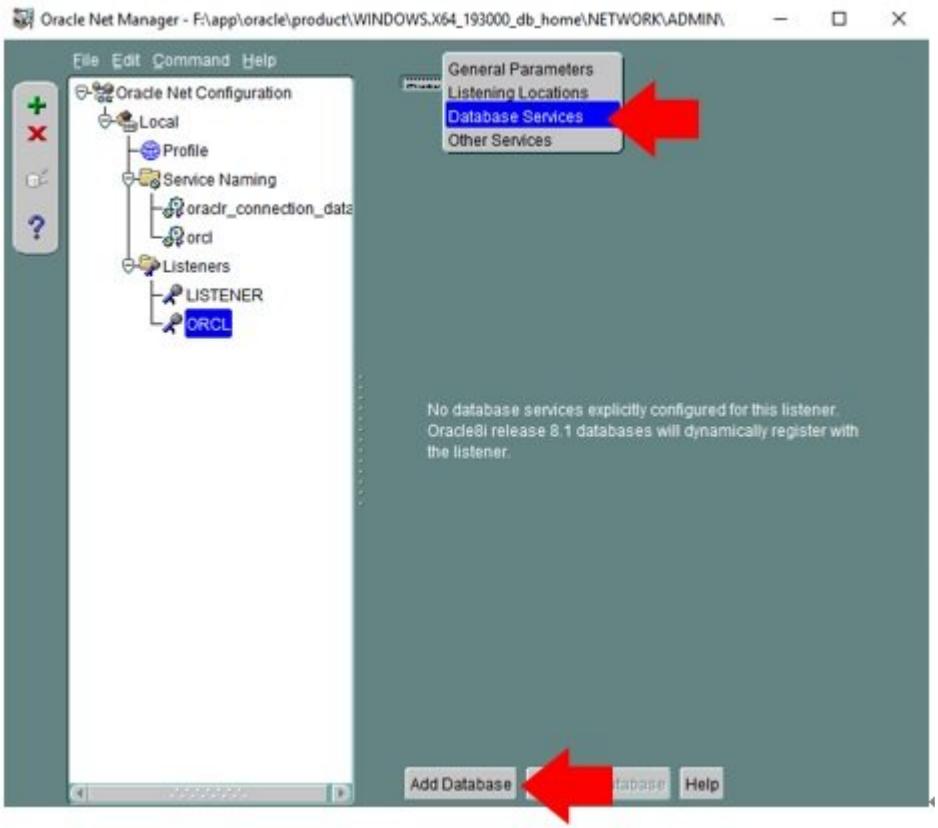
7. 次の設定値を入力します。

Net Manager Listeners / ORCL		
Protocol	TCP/IP	
Host	10.20.1.200	※
Port	1521	

※:この値はOracleリソース作成後に変更します。



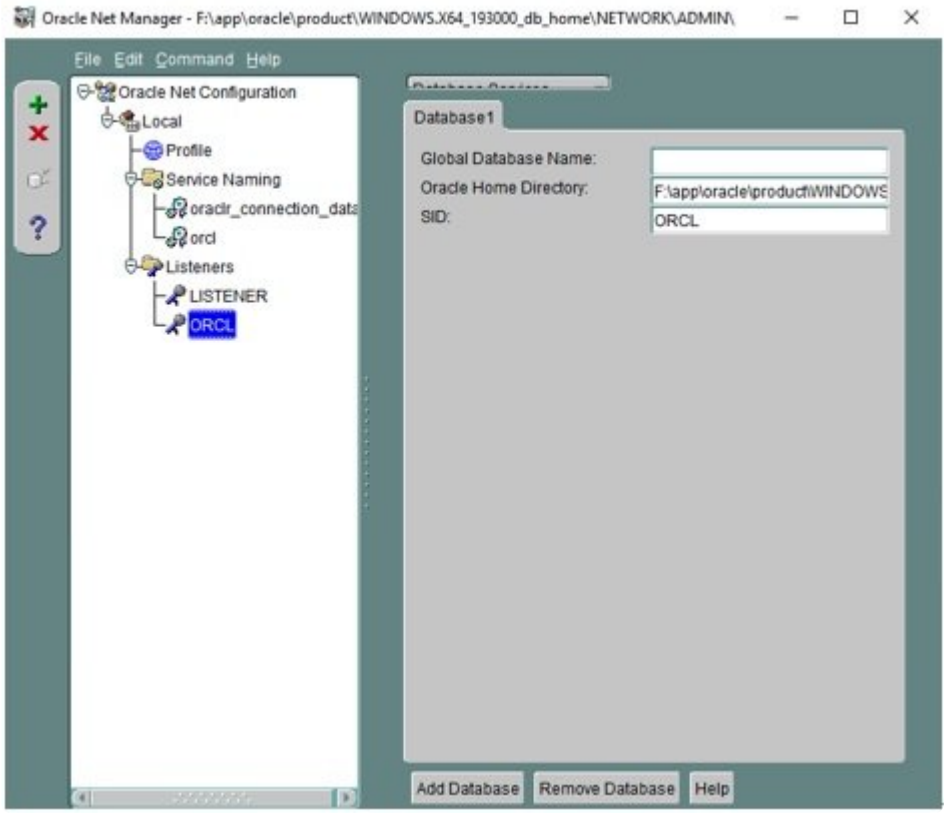
8. 右上のリストボックスを開き、**Database Services** を選択し、下部の **Add Database** をクリックします。



9. 次の表の通り設定値を入力します。

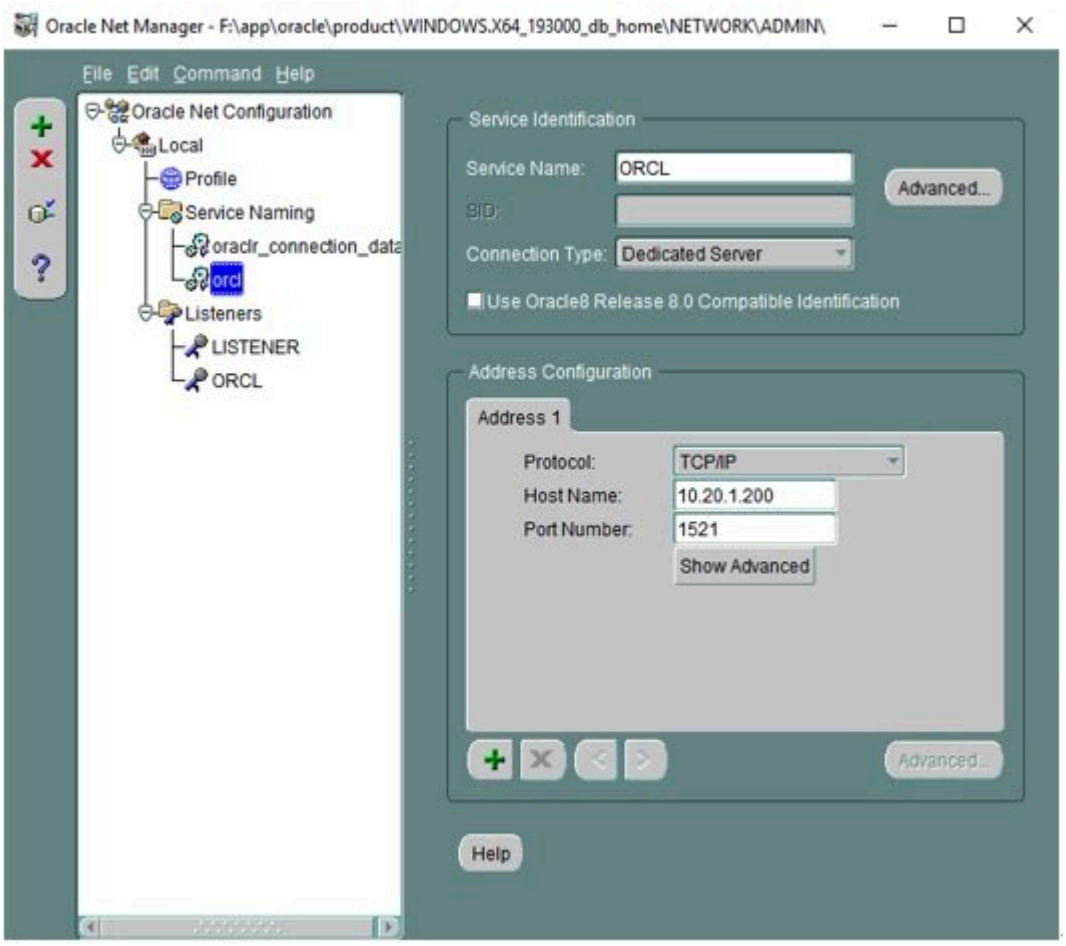
Net Manager Listeners / ORCL	
Global Database Name	空
Oracle Home Directory	F:\app\oracle\product\WINDOWS.X64_193000_db_home

SID	ORCL

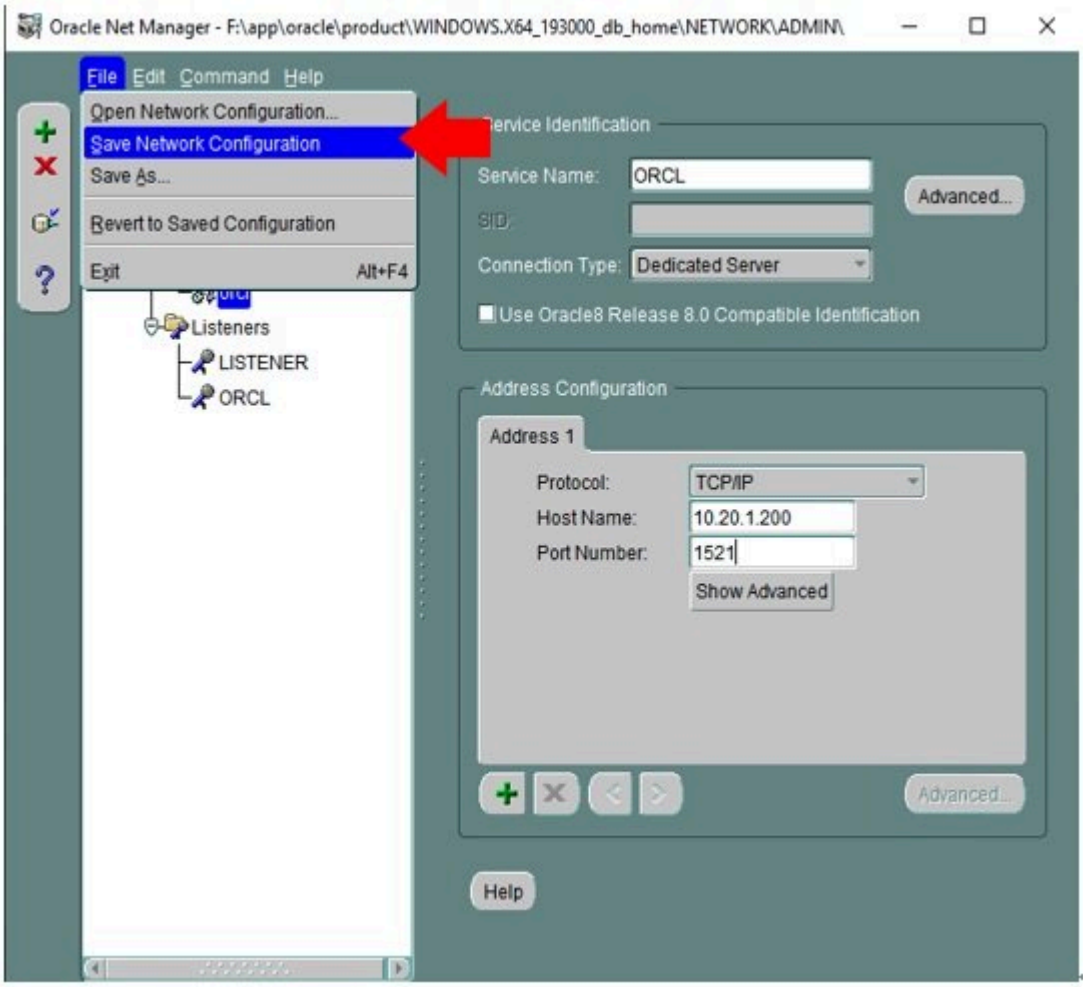


10. 左ペインで、**Service Naming** > **orcl** を選択し、次の表の通り設定値を入力します。

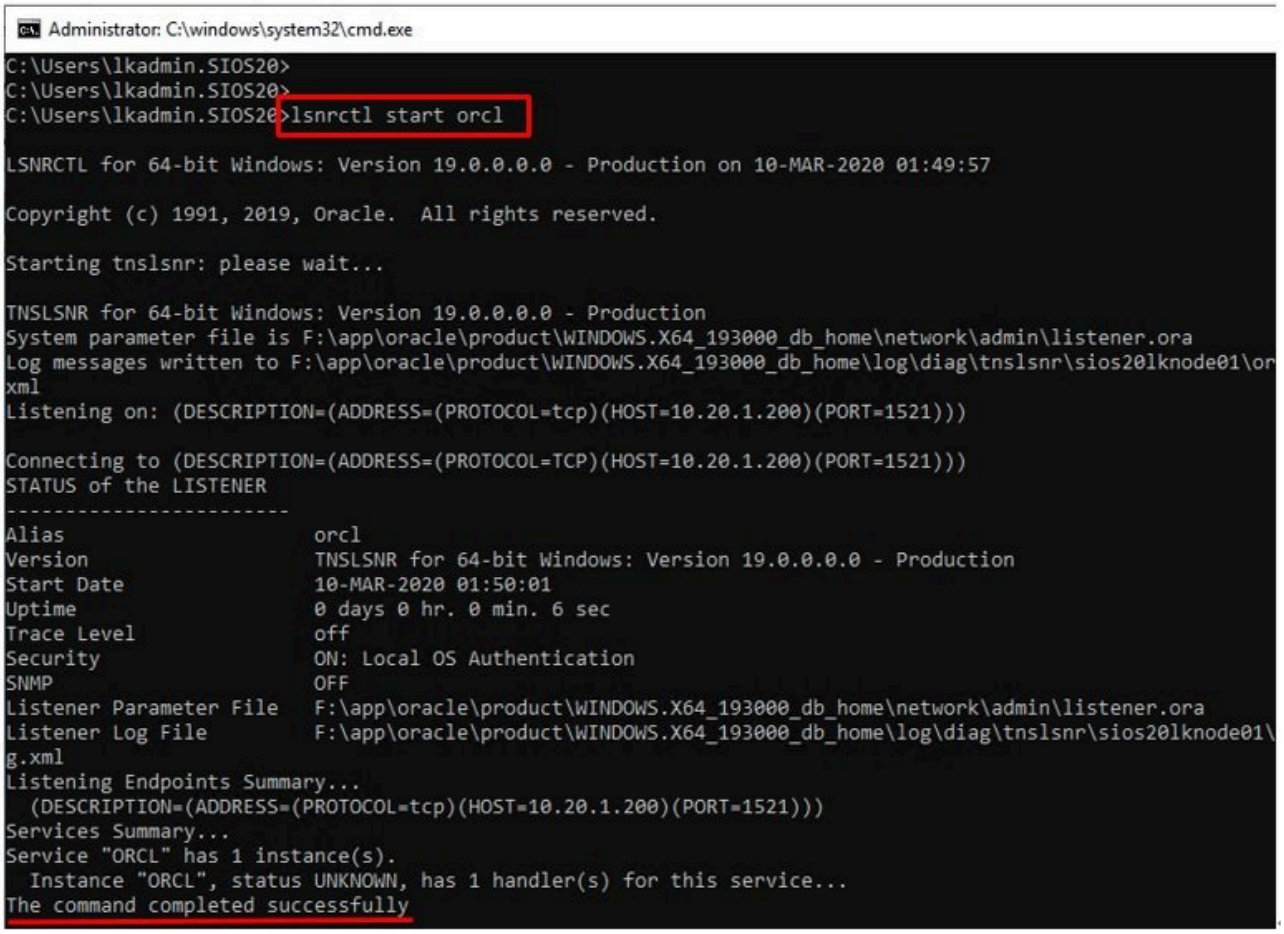
Net Manager Service Naming / orcl	
Service Identification	
Service Name	ORCL
Connection Type	Dedicated Server
Address1	
Protocol	TCP/IP
Host Name	10.20.1.200
Port Number	1521



11. **File** > **Save Network Configuration** で、設定値を保存します。



12. Oracleリスナーの設定が完了しました。コマンドプロンプトで、`lsnrctl start orcl` を実行します。


Administrator: C:\windows\system32\cmd.exe
C:\Users\lkadmin.SIOS20>
C:\Users\lkadmin.SIOS20>
C:\Users\lkadmin.SIOS20>lsnrctl start orcl
LSNRCTL for 64-bit Windows: Version 19.0.0.0.0 - Production on 10-MAR-2020 01:49:57
Copyright (c) 1991, 2019, Oracle. All rights reserved.
Starting tnslsnr: please wait...
TNSLSNR for 64-bit Windows: Version 19.0.0.0.0 - Production
System parameter file is F:\app\oracle\product\WINDOWS.X64_193000_db_home\network\admin\listener.ora
Log messages written to F:\app\oracle\product\WINDOWS.X64_193000_db_home\log\diag\tnslsnr\sios20lknode01\or
xml
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=10.20.1.200)(PORT=1521)))
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=10.20.1.200)(PORT=1521)))
STATUS of the LISTENER
Alias orcl
Version TNSLSNR for 64-bit Windows: Version 19.0.0.0.0 - Production
Start Date 10-MAR-2020 01:50:01
Uptime 0 days 0 hr. 0 min. 6 sec
Trace Level off
Security ON: Local OS Authentication
SNMP OFF
Listener Parameter File F:\app\oracle\product\WINDOWS.X64_193000_db_home\network\admin\listener.ora
Listener Log File F:\app\oracle\product\WINDOWS.X64_193000_db_home\log\diag\tnslsnr\sios20lknode01\
g.xml
Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=10.20.1.200)(PORT=1521)))
Services Summary...
Service "ORCL" has 1 instance(s).
Instance "ORCL", status UNKNOWN, has 1 handler(s) for this service...
The command completed successfully

6.7.2.3. パスワードファイルの作成（稼働系）

1. SIOS20LKNODE01にSIOS20\lkadminでログインします。

2. リスナー経由のログインで使用する、パスワードファイルを作成します。パスワードファイルの記述形式については、Oracle社の公式ドキュメントを参照してください。

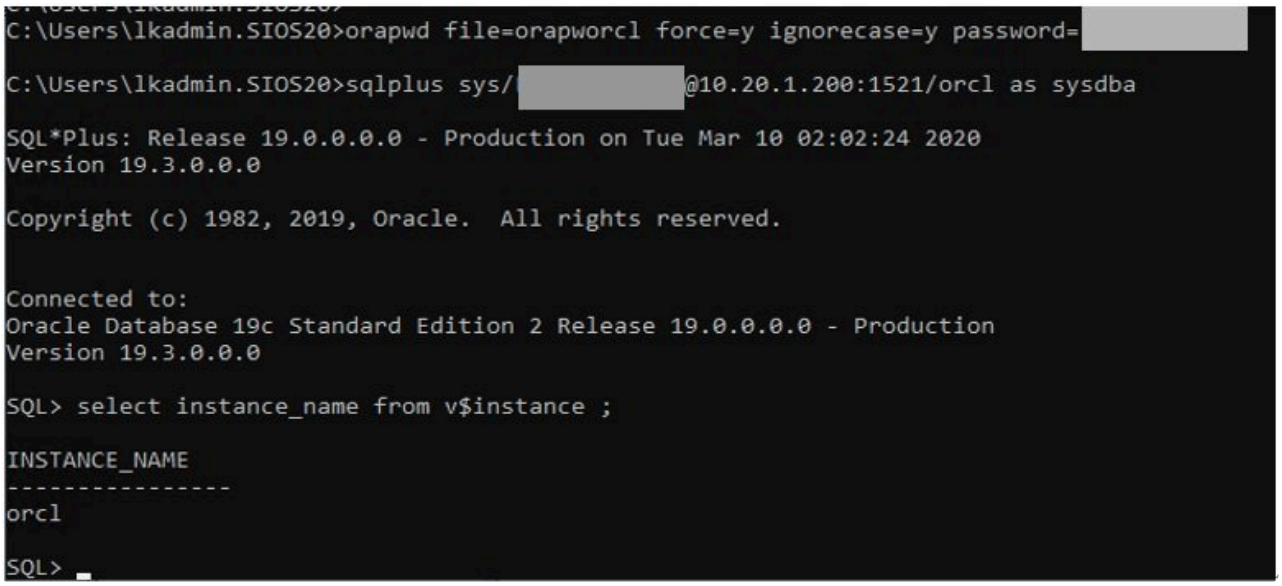
```
C:\> orapwd file=orapworcl force=y ignorecase=y password=XXXXXXXX
```

3. リスナー経由で、データベースに接続確認を行います。

```
C:\> sqlplus sys/XXXXXXXX@10.20.1.200:1521/orcl as sysdba
SQL> select instance_name from v$instance ;

INSTANCE_NAME
____________________

orcl
```

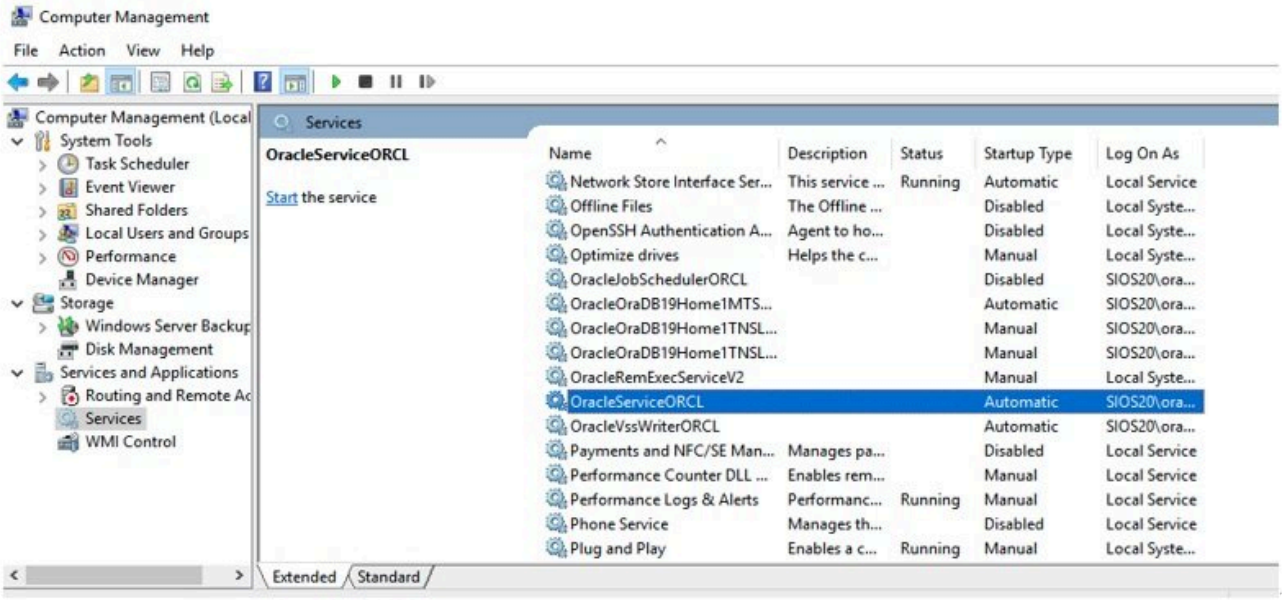


6.7.2.4. 待機系Oracleインストール前の準備

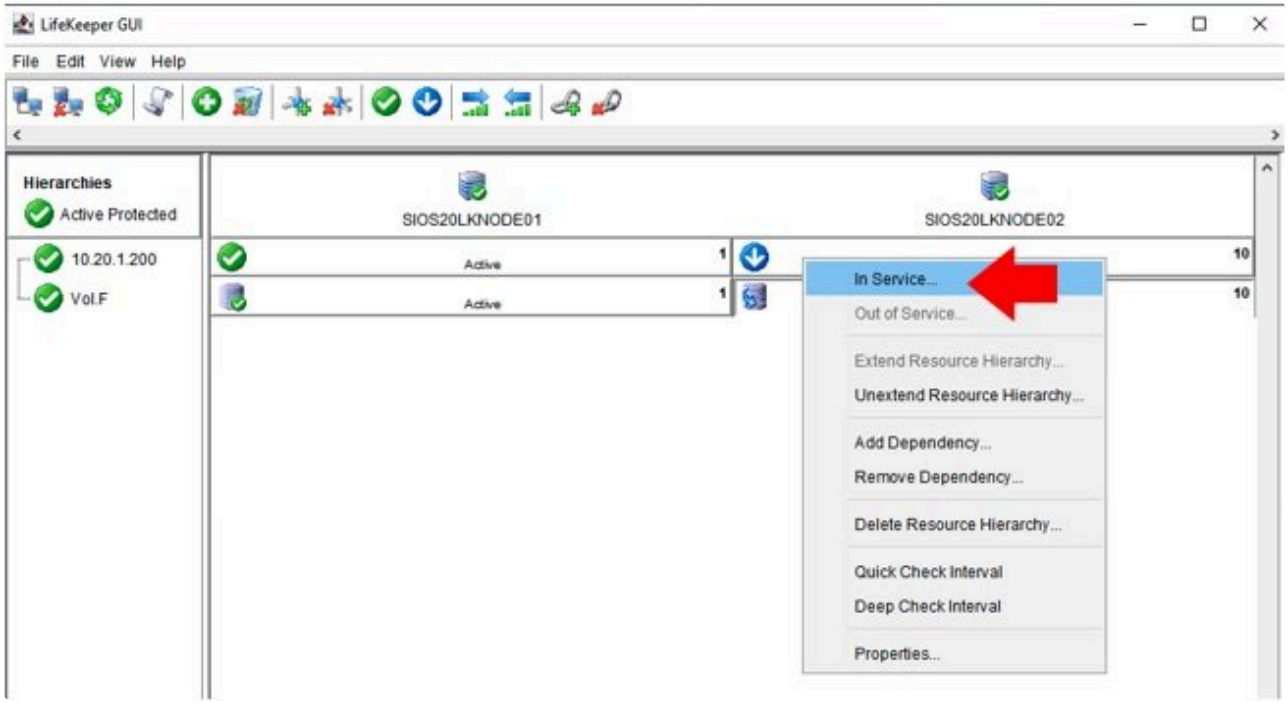
待機系でのOracleインストール・設定作業を行うために、IPリソースとボリュームリソースを待機系（SIOS20LKNODE02）でActiveとなるように操作します。

1. SIOS20LKNODE01にSIOS20\lkadminでログインします。

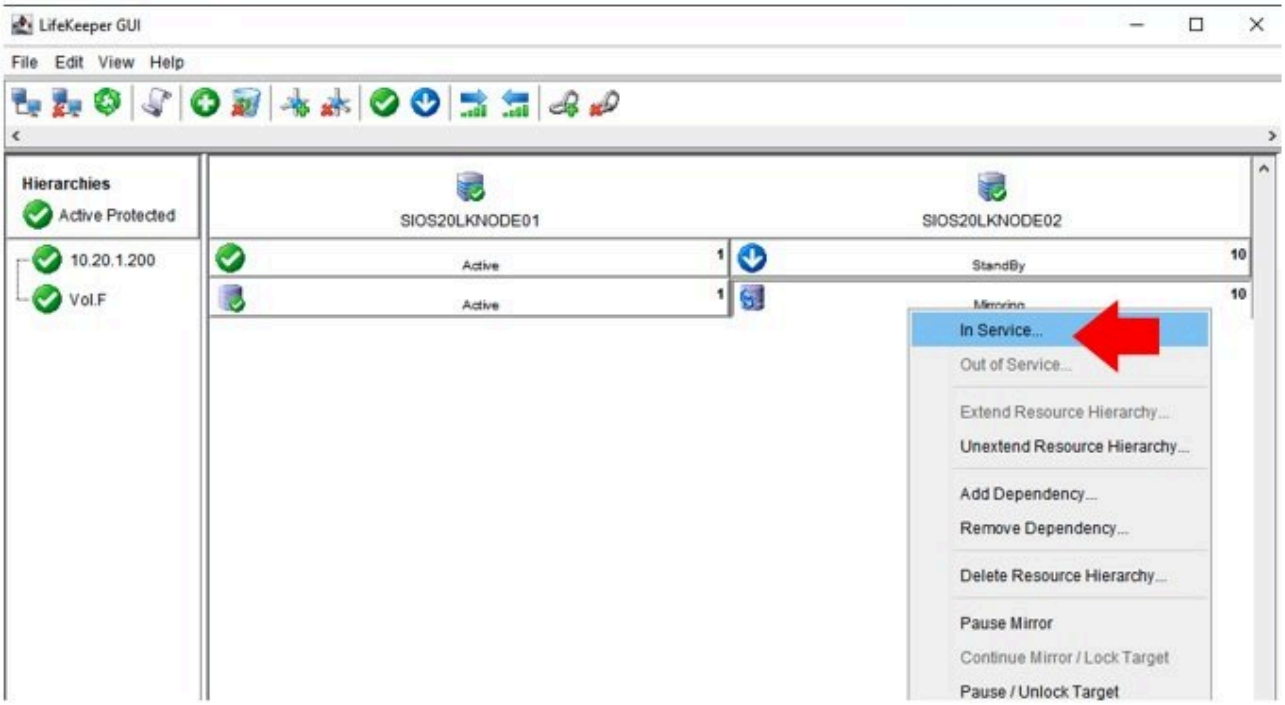
2. **サービスコントロールマネージャー** で、名前がOracleで始まるサービスを全て停止します。



3. **LifeKeeper GUI** を起動して、**SIOS20LKNODE02** のIPリソース（10.20.1.200）を右クリックし、**In Service** を選択することで、該当リソースがSIOS20LKNODE02でActiveになるようにします。



4. ボリュームリソース（Vol.F）についても、同様にSIOS20LKNODE02上でActiveとなるようにします。



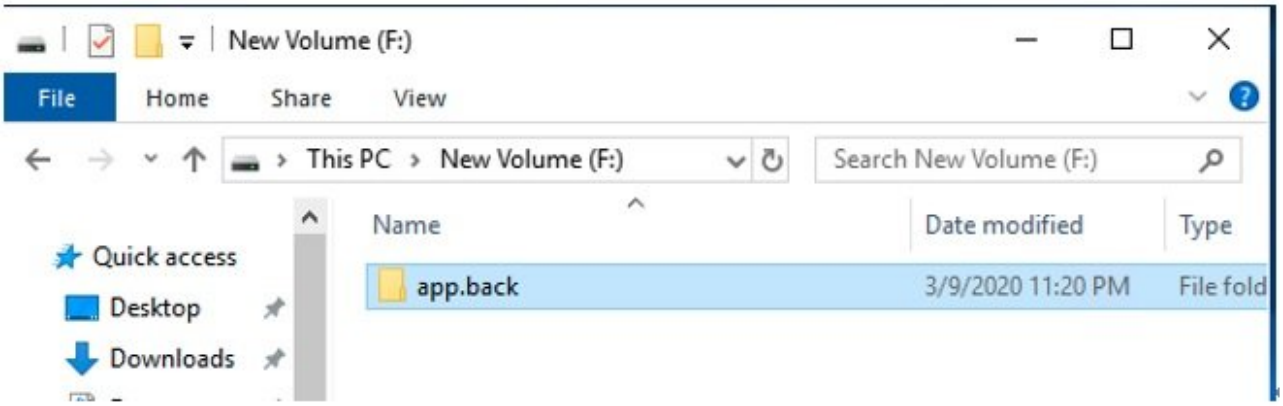
5. IPリソースとボリュームリソースがどちらもSIOS20LKNODE02上でActiveになりました。



6.7.2.5. Oracle Databaseのインストール（待機系）

1. SIOS20LKNODE02にSIOS20\lkadminでログインします。

2. **F:\app** を **F:\app.bak** にリネームします。



3. 稼働系と同一の手順で、Oracle Databaseをインストールします。

   参照：Oracle Databaseのインストール（稼働系）

6.7.2.6. Oracleリスナー設定（待機系）

稼働系で行ったときと同一の手順で、Oracleリスナーを設定します。

参照：Oracleリスナー設定（稼働系）

6.7.2.7. パスワードファイルの作成（待機系）

稼働系で行ったときと同一の手順で、パスワードファイルを作成し、リスナー経由でのデータベースへの接続確認も行います。

参照：パスワードファイルの作成（稼働系）

ここまでで、待機系でのインストール・設定作業が完了しました。

6.7.2.8. 稼働系へのスイッチバック

待機系での作業が完了しましたので、IPリソース、ボリュームリソースを稼働系にスイッチバックします（戻します）。

1. SIOS20LKNODE02に **SIOS20\lkadmin** でログインします。

2. すでに行った待機系へのスイッチオーバーの手順を参考に、IPリソースとボリュームリソースを稼働系（SIOS20LKNODE01）上でActiveとなるようにします。

   参照：待機系Oracleインストール前の準備

3. 稼働系（SIOS20LKNODE01）の **Computer Management** で、Oracleのサービスを全て開始します。

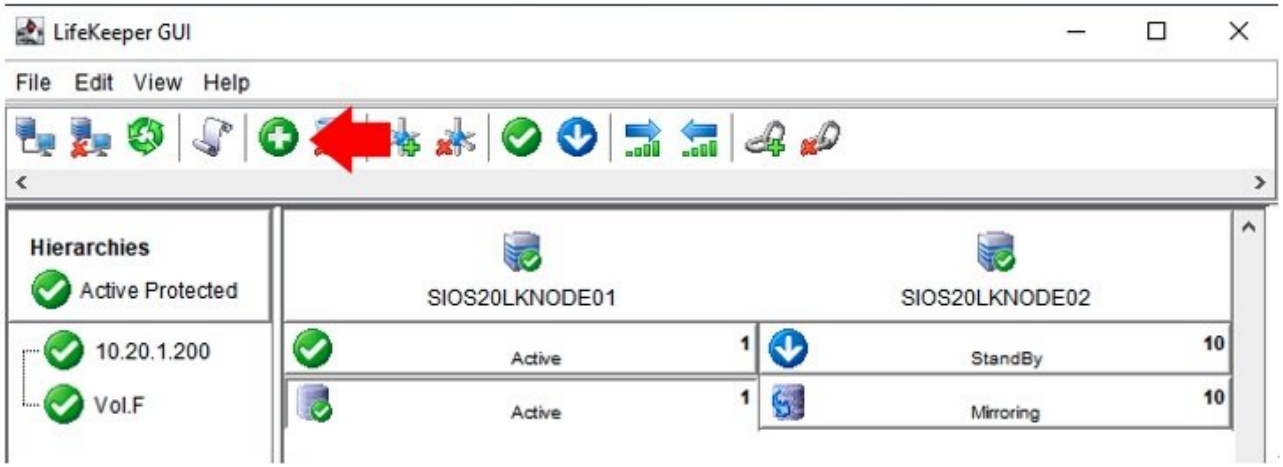
6.7.3. Oracleの保護

Oracleリソース階層の作成（稼働系）

1. 稼働系（SIOS20LKNODE01）のWindows OSに、SIOS20\lkadminでログインします。

2. LifeKeeper GUIを起動し、SIOS20\lkadminでログインします。

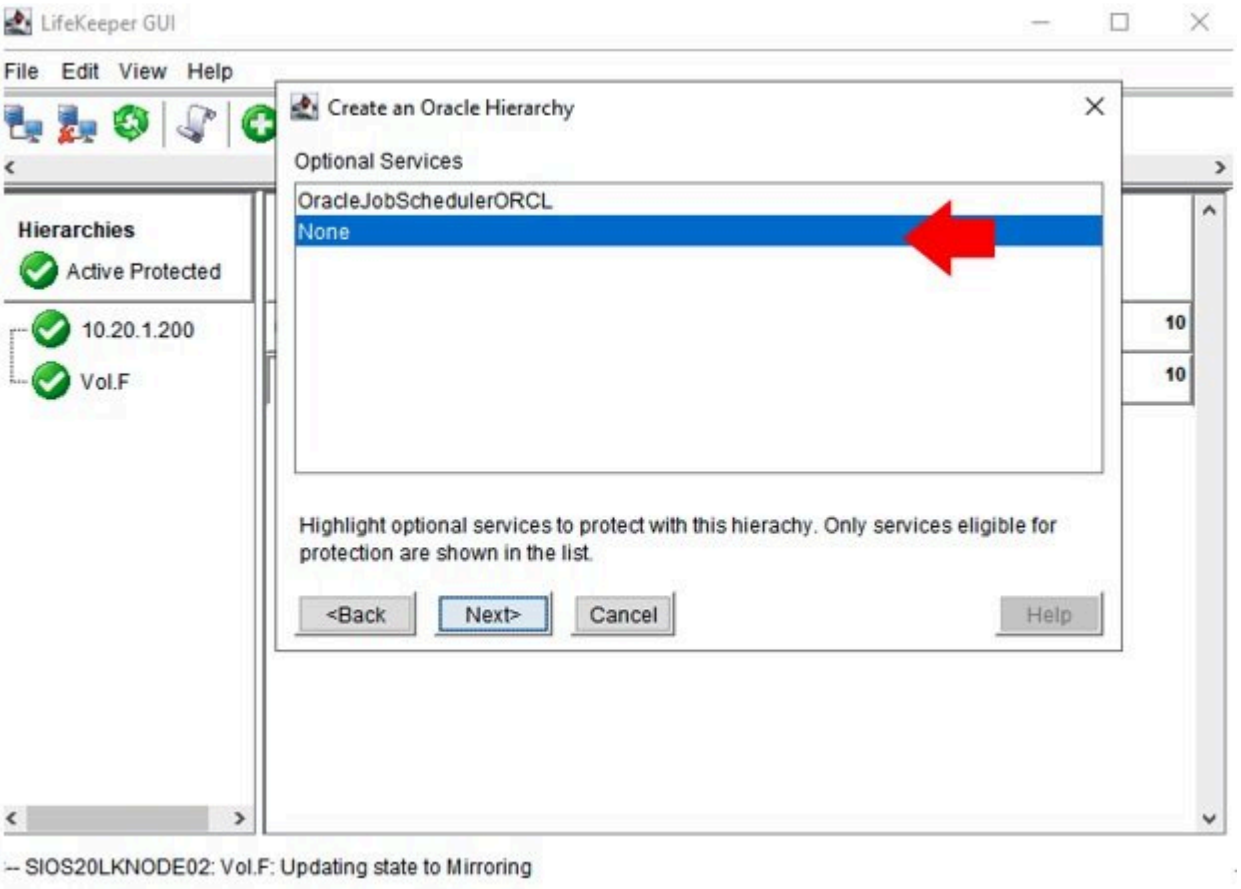
3. **リソース階層作成** アイコン（緑色の＋）をクリックし、Oracleリソース階層を作成します。



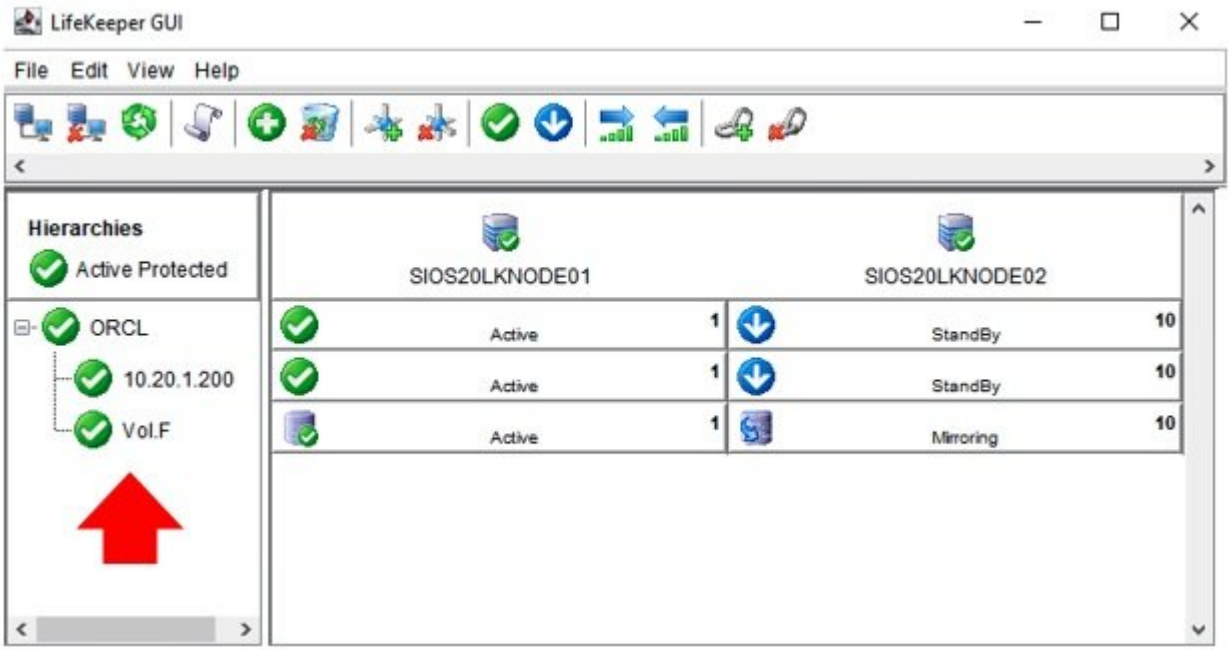
4. 次の表の通り設定値を入力します。

Oracle リソース	
Primary Server	SIOS20LKNODE01
Backup Server	SIOS20LKNODE02
Application to protect	Oracle
Oracle Home Directory	OraDB19Home1
Oracle SID	ORCL
Oracle User Name	system
Password	xxxxxxxx
Optional Services	None
Oracle Tag	ORCL

5. リソース階層作成の途中で次のような画面が表示されますが、Optional Serviceは今回必要ないので **None** を選択します。



6. Oracleのリソース階層が出来上がると次のような画面が表示されます。IPアドレスリソースとVolumeリソースが親リソース「ORCL」の子リソースになっていることに注目してください。



6.7.4. Oracleリスナーの設定変更

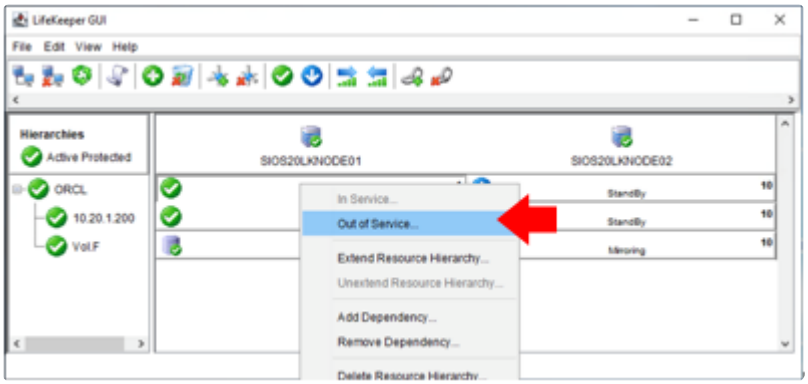
正常性プローブに稼働系と待機系それぞれのプライベートIPアドレスで応答するために、Oracleリスナーの設定を変更して、任意のIPアドレスで接続を待ち受けるようにします。具体的にはOracleリスナーのListenアドレスを0.0.0.0に設定します。

Oracleリソース階層の停止（稼働系）

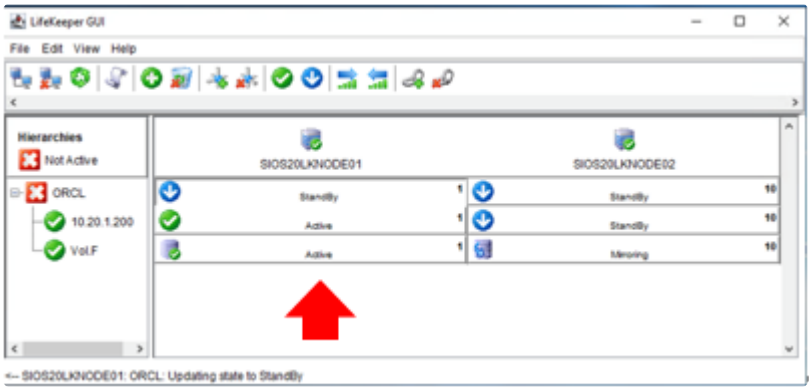
1. 稼働系（SIOS20LKNODE01）のWindows OSに、SIOS20\lkadminでログインします。

2. LifeKeeper GUIを起動し、SIOS20\lkadminでログインします。

3. 稼働系（SIOS20LKNODE01）のORCLリソースを右クリックし、**Out of Service** を選択します。



4. 完了すると次のような画面が表示されます。ORACLEリソースの状態がStandBy と表示されていること、ディスクリソースの状態がActiveと表示されていることを確認します。



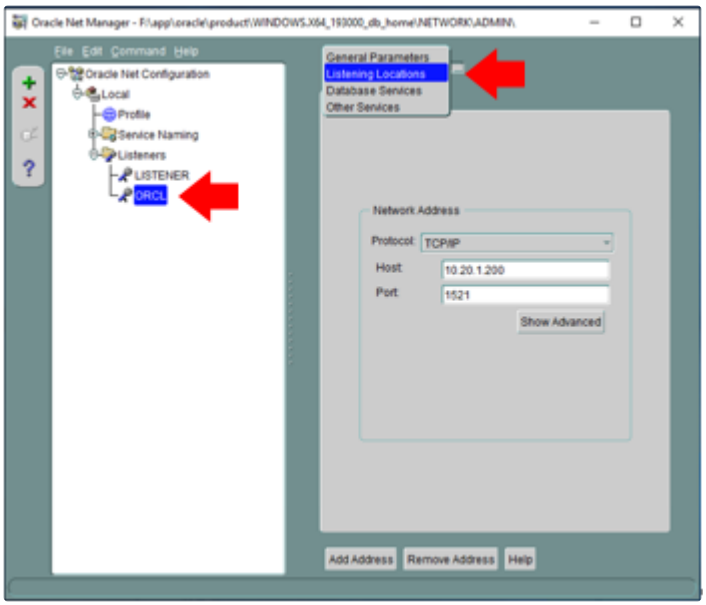
Oracleリスナー設定（稼働系）

Oracleリスナーの設定を変更します。

1. 稼働系（SIOS20LKNODE01）のWindows OSにsios20\lkadminでログインします。

2. **Start** > **Oracle-OraDB19Home1** > **Net Manager** を起動します。

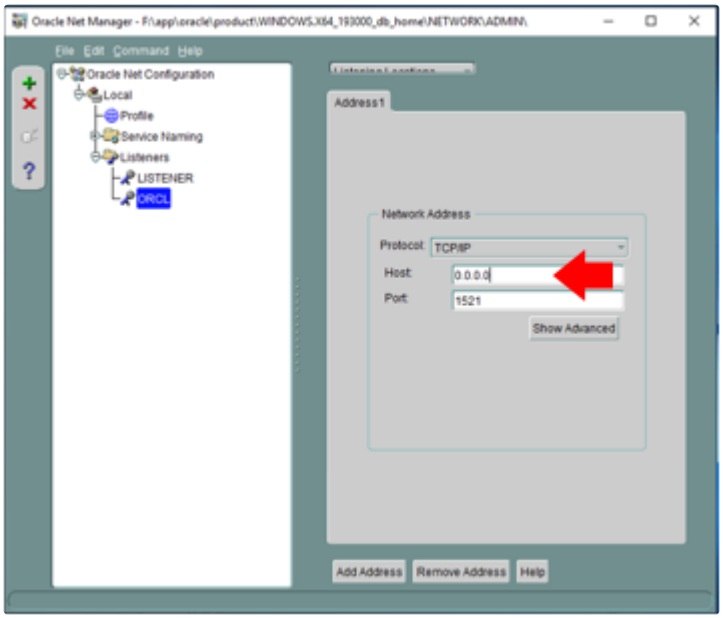
3. 左ペインで Listeners / ORCL が選択された状態で、右上のリストボックスで **Listening Locations** を選択します。



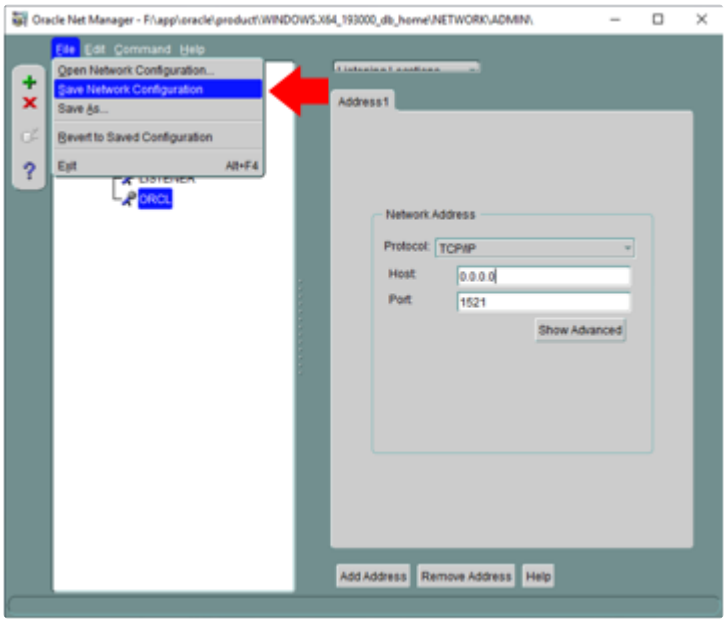
4. Hostを0.0.0.0に変更します。結果として下記の設定値になっていることを確認します。

Net Manager Listeners / ORCL		
Protocol	TCP/IP	
Host	0.0.0.0	※
Port	1521	

※:この値のみ変更します。



5. **File** > **Save Network Configuration** で、設定値を保存します。

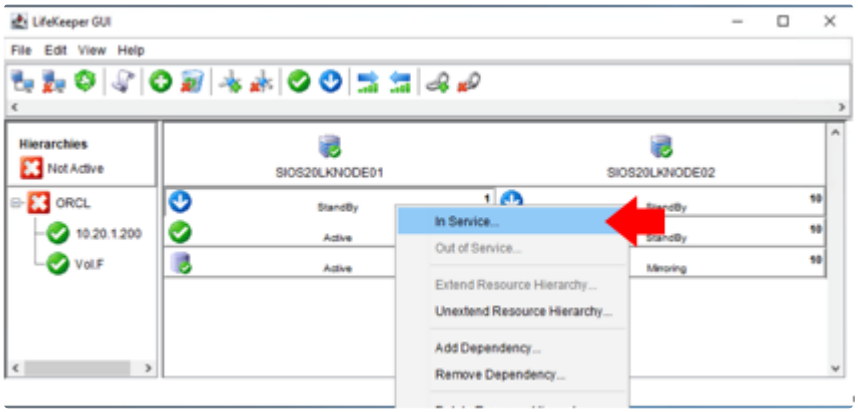


Oracleリソース階層の開始（稼働系）

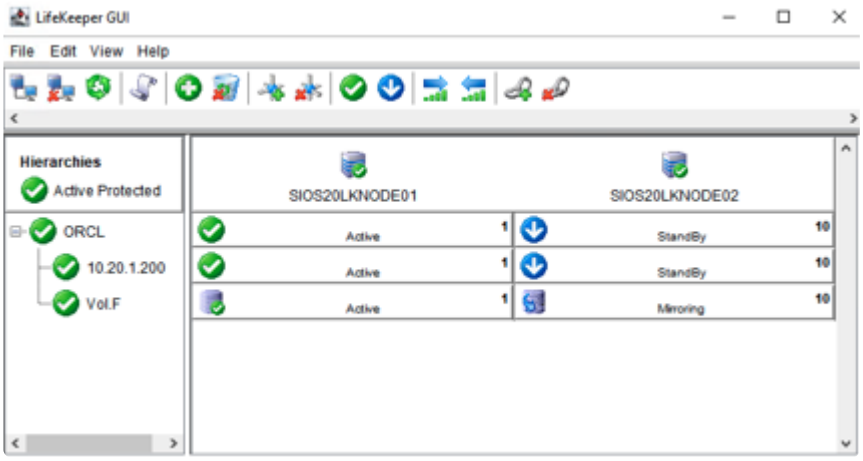
1. 稼働系（SIOS20LKNODE01）のWindows OSに、SIOS20\lkadminでログインします。

2. LifeKeeper GUIを起動し、SIOS20\lkadminでログインします。

3. 稼働系（SIOS20LKNODE01）のORCLリソースを右クリックし、**In Service** を選択します。



4. 完了すると次のような画面が表示されます。


LifeKeeper GUI
File Edit View Help
Hierarchies
Active Protected
ORCL
10.20.1.200
Vol.F
SIOS20LKNODE01
SIOS20LKNODE02
Active 1
StandBy 10
Active 1
StandBy 10
Active 1
Mirroring 10

6.7.5. 接続確認（クライアント）

Oracleクライアントのインストール

Oracleクライアントの接続確認

6.7.5.1. Oracleクライアントのインストール

1. SIOS20LKCLIENTにSIOS20\lkadminでログインします。

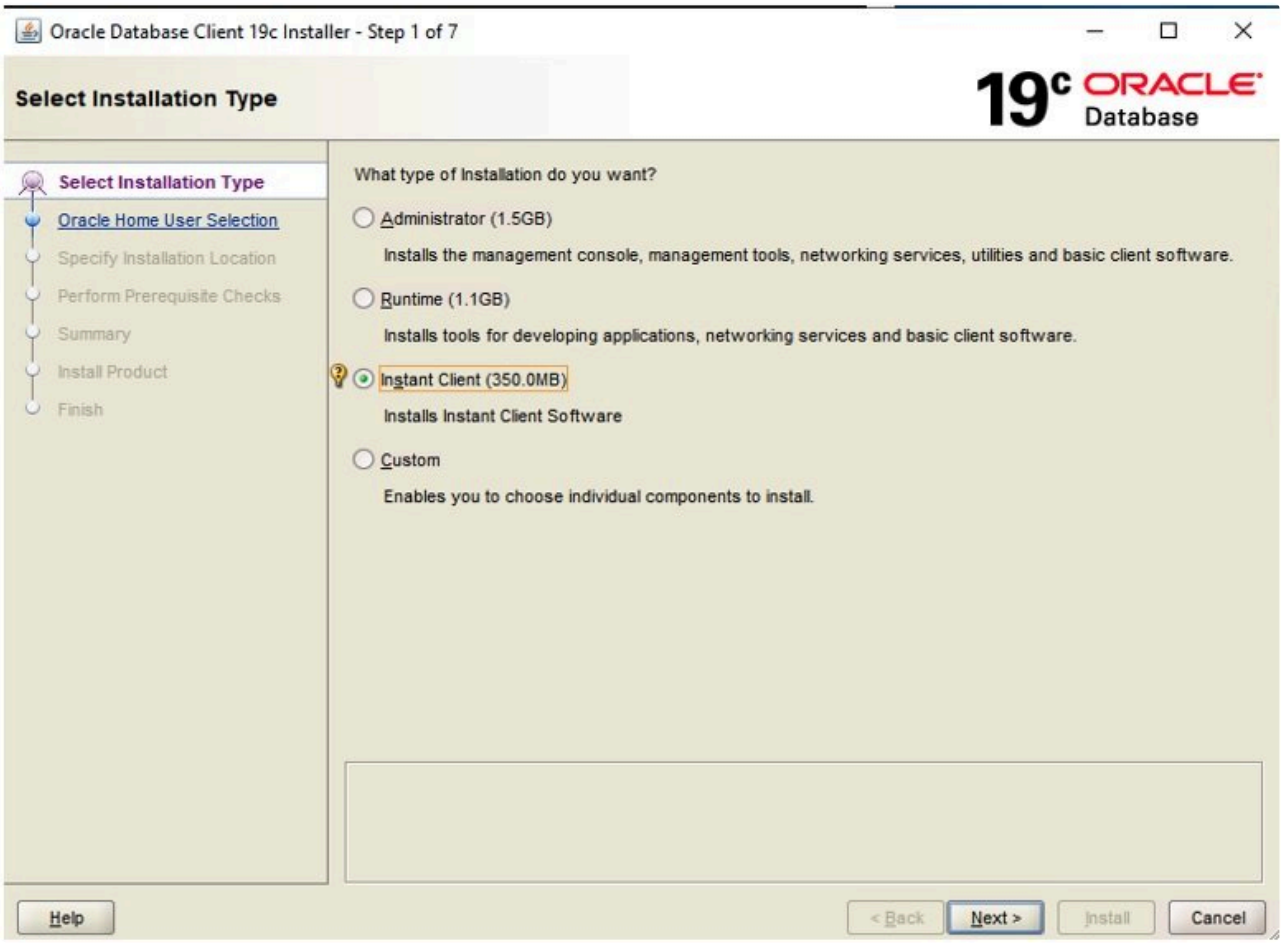
2. Oracleクライアントのインストール媒体（zipファイル）をダウンロードして任意の場所に保存します。

   - https://www.oracle.com/database/technologies/oracle19c-windows-downloads.html
   - Oracle Database 19c Client (19.3) for Microsoft Windows x64 (64-bit)
   - WINDOWS.X64_193000_client.zip

3. 次のディレクトリーを作成し、直下にzipファイルの内容を展開します。
   C:\ora

4. **File Explorer** でC:\ora\client\setup.exeをダブルクリックして実行します。

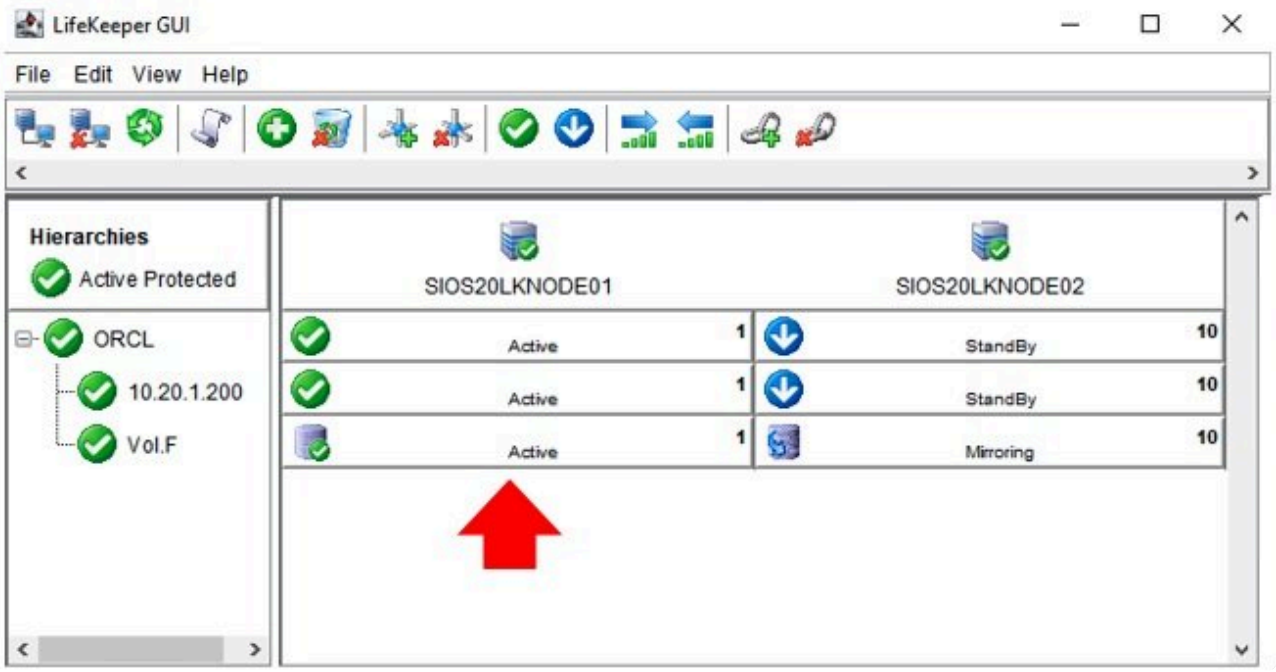
5. **Installation Type** を **Instant Client** に設定し、以降はウィザードに従って、すべて既定値でインストールします。



6.7.5.2. Oracleクライアントの接続確認

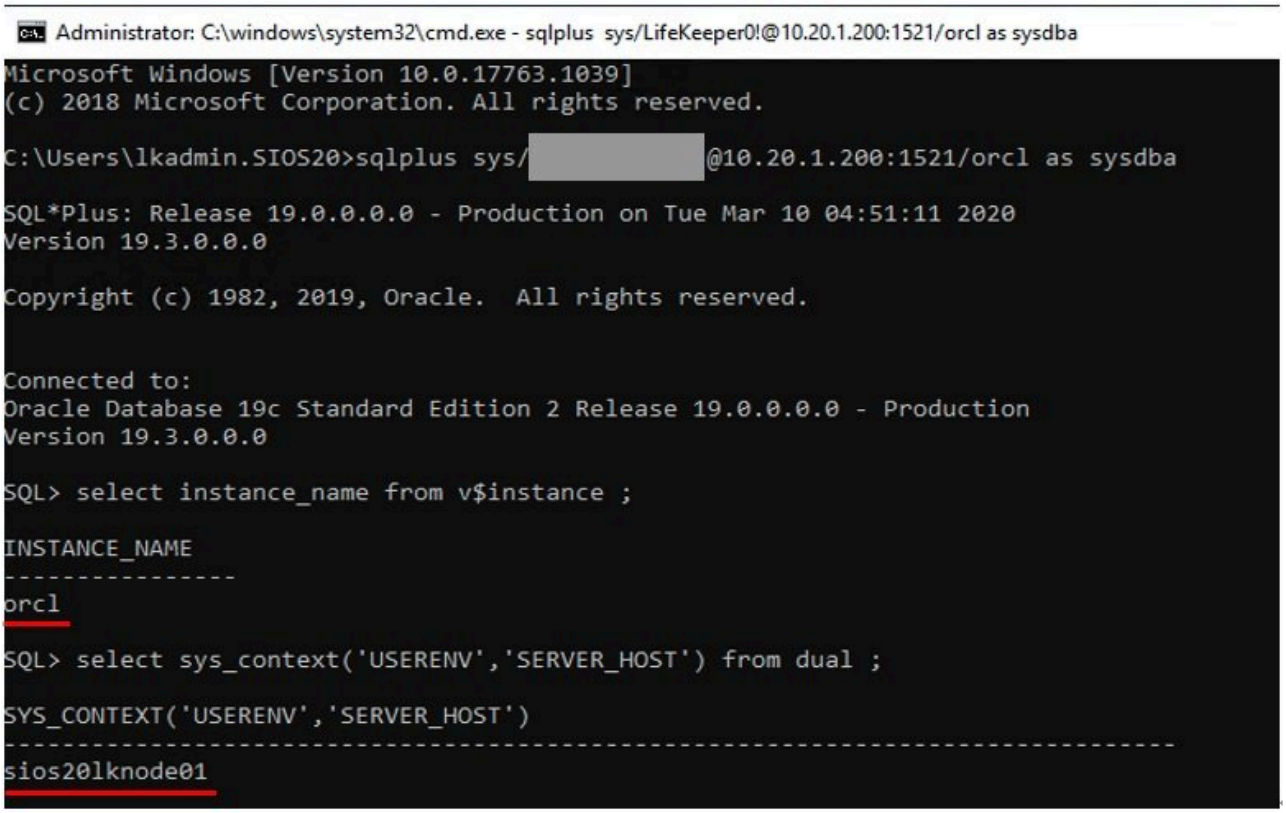
SIOS20LKCLIENT上のクライアントより、データベースへの接続確認を行います。

1. 稼働系（SIOS20LKNODE01）でOracleリソース階層がActiveであることを確認します。

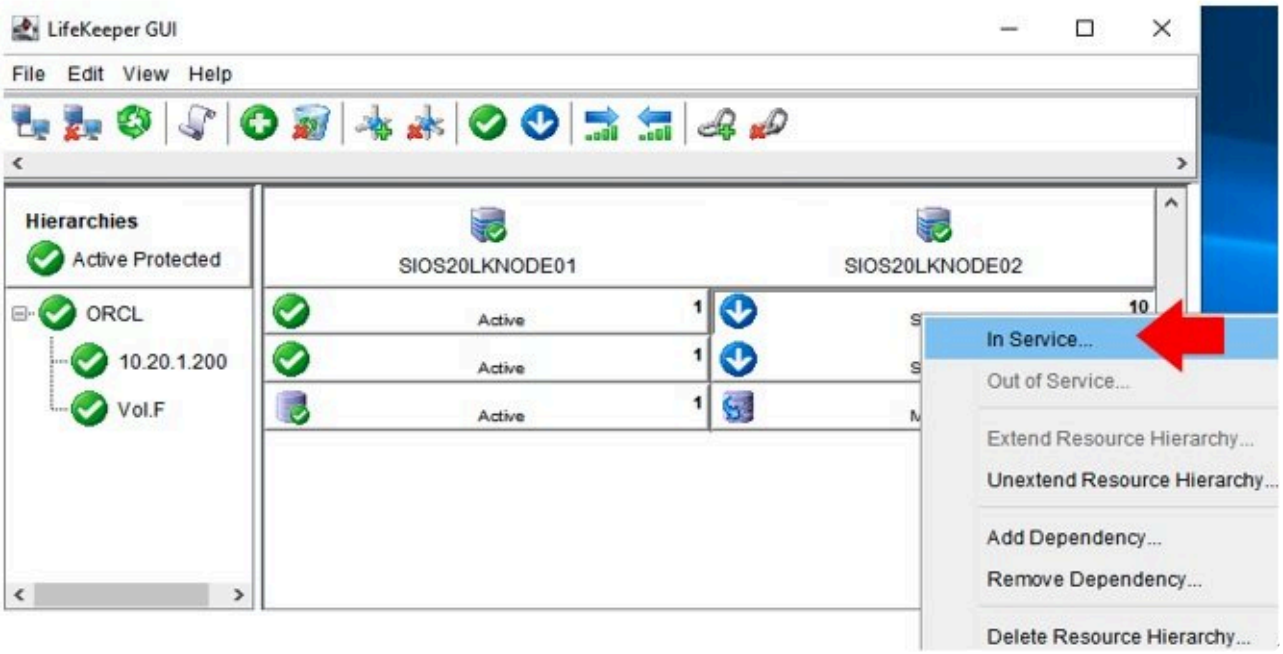


2. SIOS20LKCLIENTから、仮想IPアドレスを使ってデータベースに接続し、簡単なSQL文を実行します。

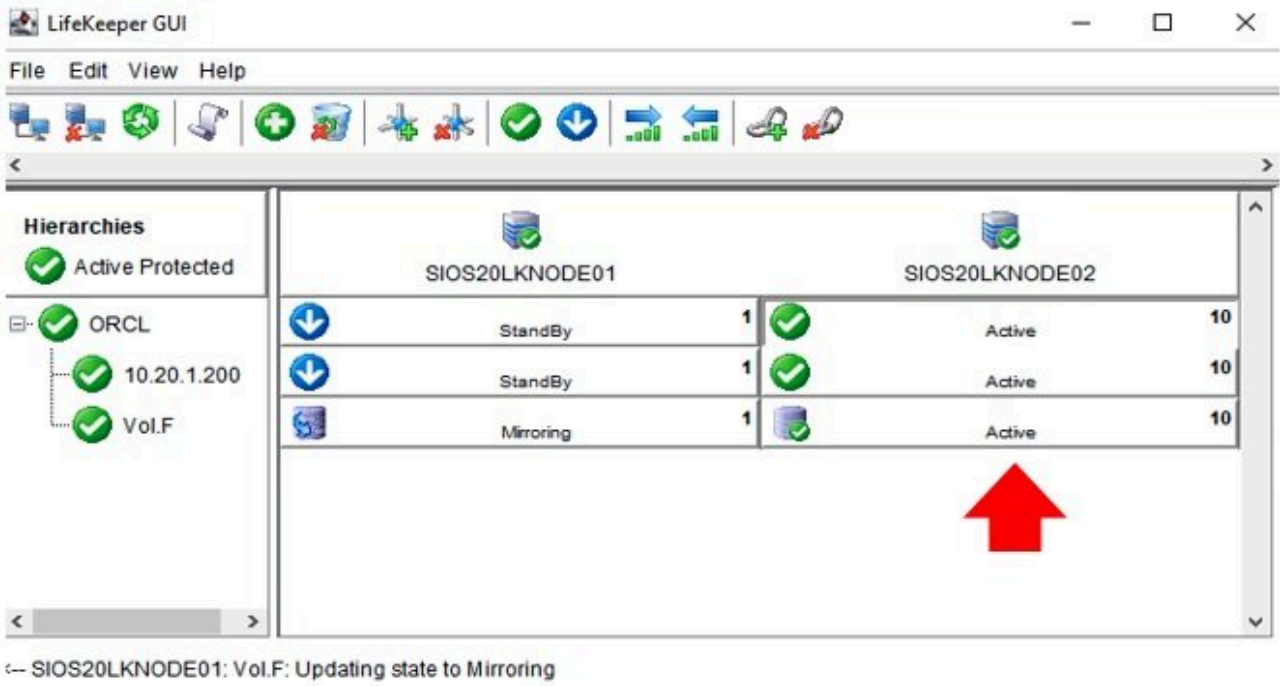
```
C:\> sqlplus sys/XXXXXXXX@10.20.1.200:1521/orcl as sysdba
SQL> select instance_name from v$instance ;
SQL> select sys_context('USERENV','SERVER_HOST') from dual ;
```



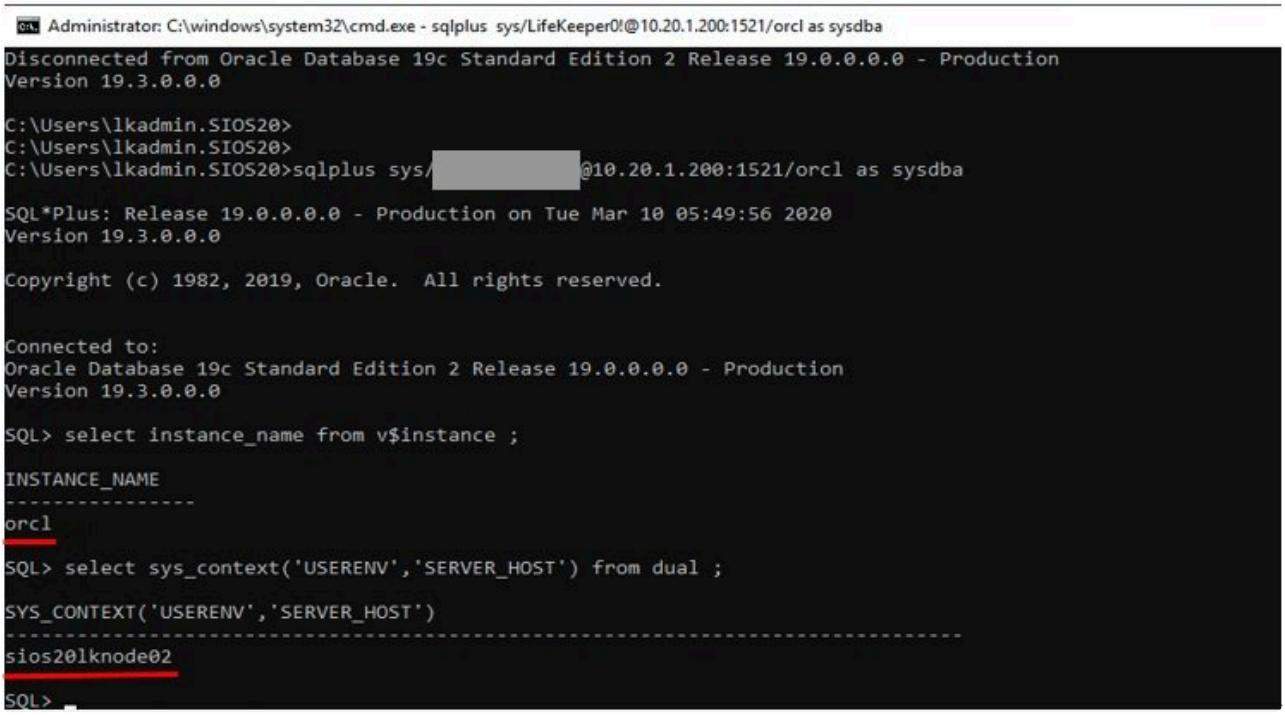
3. 待機系（SIOS20LKNODE02）のORCLリソースを右クリックし、**In Service** を選択します。ORCLリソースは待機系にスイッチオーバーします。



4. スイッチオーバーが完了すると次のような画面が表示されます。



5. SIOS20LKCLIENTから、再度仮想IPアドレスを使ってデータベースに接続します。



6. スイッチオーバーの前後で、同じIPアドレス（仮想IPアドレス）を使ってデータベースに接続できることが確認できました。

6.8. PostgreSQL固有の環境構築

PostgreSQLのインストールと設定（稼働系、待機系）

ミラーボリュームリソース階層の作成（稼働系）

PostgreSQL関連パラメーターの変更（稼働系、待機系）

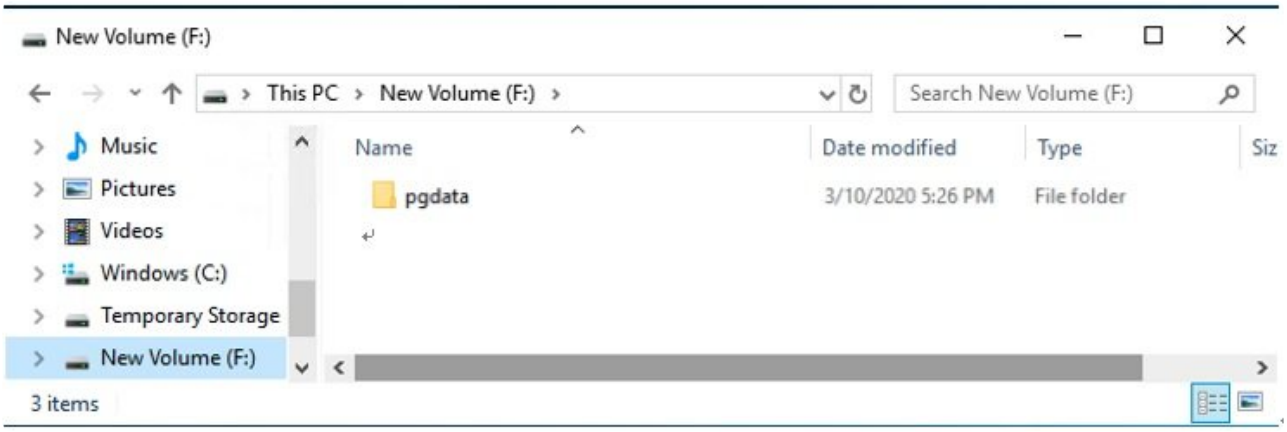
PostgreSQLデータベースの保護（稼働系）

接続確認（クライアント）

6.8.1. PostgreSQLのインストールと設定（稼働系、待機系）

データベース格納場所の作成

1. PostgreSQLのデータ格納場所として、F:\pgdataというフォルダーを作成します。



PostgreSQLのインストール

1. 次のサイトから、PostgreSQL(Windows x86-64)インストールイメージをダウンロードして任意の場所に起き、ダブルクリックして開きます。ここではバージョン11.7を使いました。
   https://www.enterprisedb.com/downloads/postgres-postgresql-downloads

2. ウィザードに従って、次の設定値を入力します。

PostgreSQL	
Installation Directory	C:\Program Files\PostgreSQL\11（既定値）
Component	（既定値）
Data Directory	F:\pgdata
Password	xxxxxxxx
Port	5432（既定値）
Locale	（既定値）

3. 最後に追加コンポーネントのインストール有無を聞かれますが、ここでは不要です。チェックを外し、**Finish**をクリックしてウィザードを終了します。

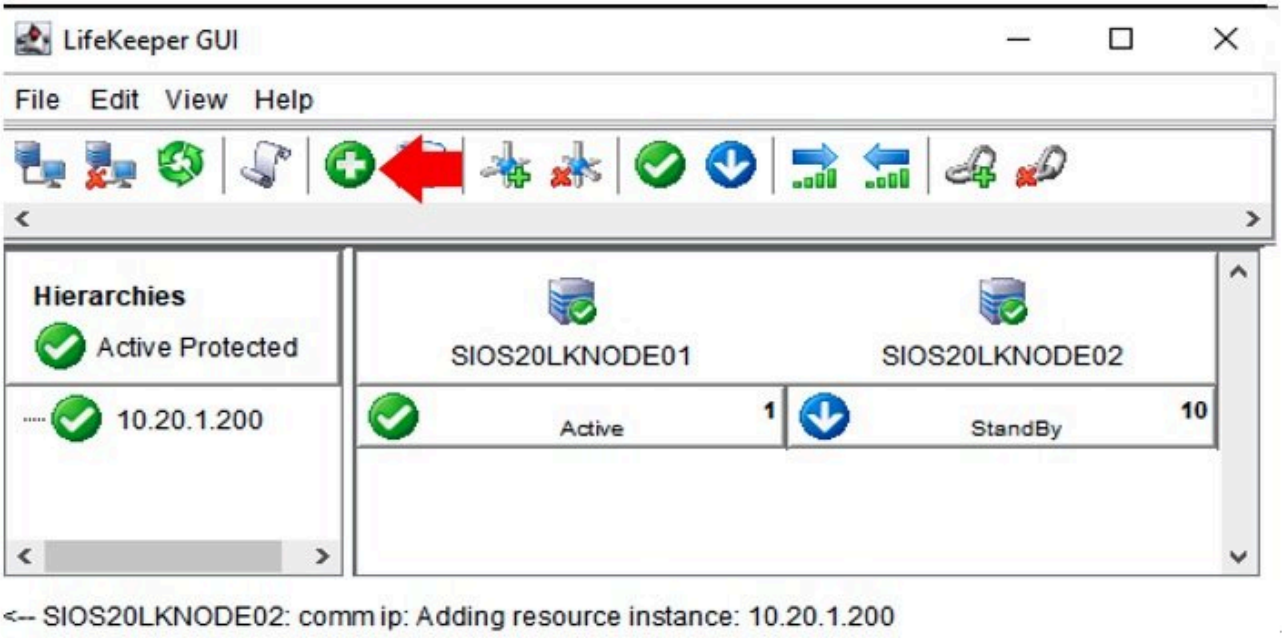

Setup
Packaged by:
EDB
POSTGRES
PostgreSQL
Completing the PostgreSQL Setup Wizard
Setup has finished installing PostgreSQL on your computer.
Launch Stack Builder at exit?
Stack Builder may be used to download and install additional tools, drivers and applications to complement your PostgreSQL installation.
< Back
Finish
Cancel

6.8.2. ミラーボリュームリソース階層の作成（稼働系）

ここでは各クラスターノードに追加された30GBのディスク（Fドライブ）を使ってミラーボリュームを作成します。

1. SIOS20LKNODE01にログインし、LifeKeeper GUIを起動します。

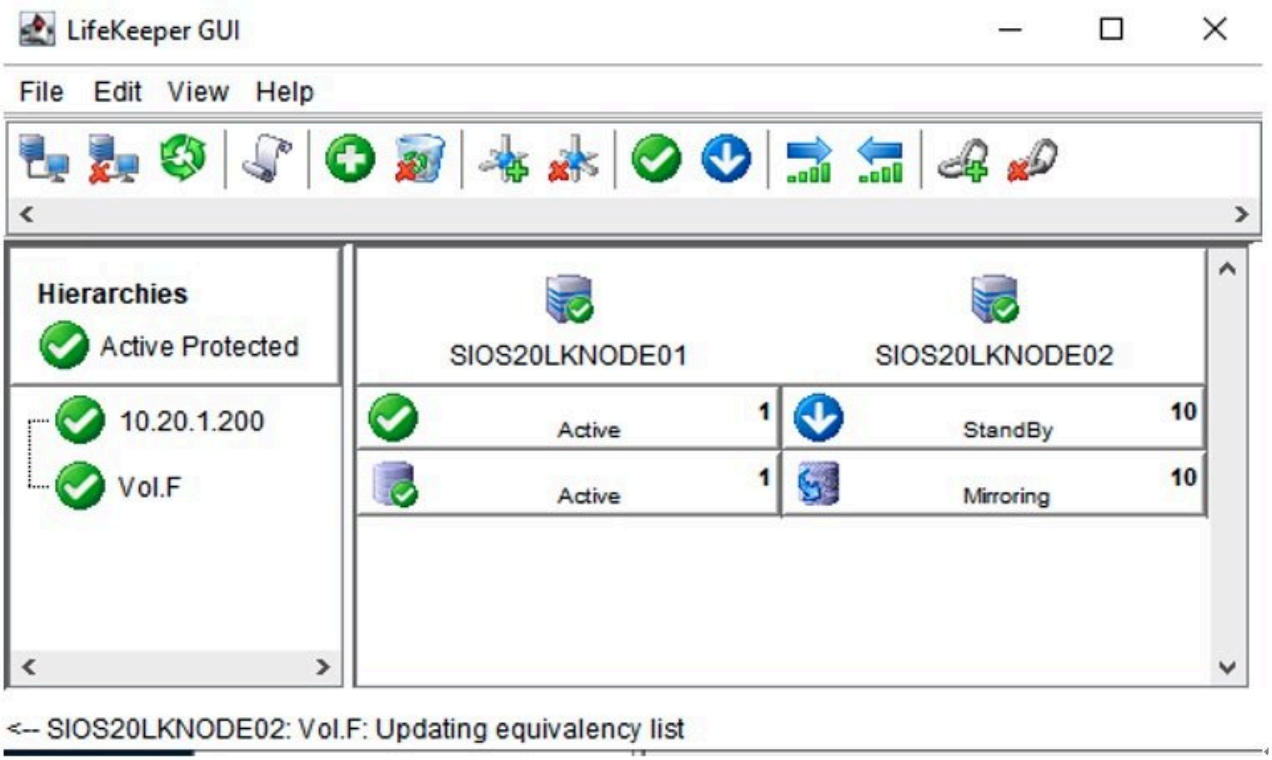
2. **[Create Resource Hierarchy]**（緑色の＋ボタン）をクリックします。



3. ウィザードに従って、次の表の通りに設定値を入力します。

IP address (create)		
Primary Server	SIOS20LKNODE01	
Backup Server	SIOS20LKNODE02	
Application to protect	Volume	スクロールしないとVolumeが見えないケースがあります。
Select Volume	F:	
Volume Tag	Vol.F	
Volume Type	Create Mirror	
Network end points (Target/Source)	10.20.2.12 / 10.20.2.11	
Mode	Asynchronous	
Backup Priority	10	

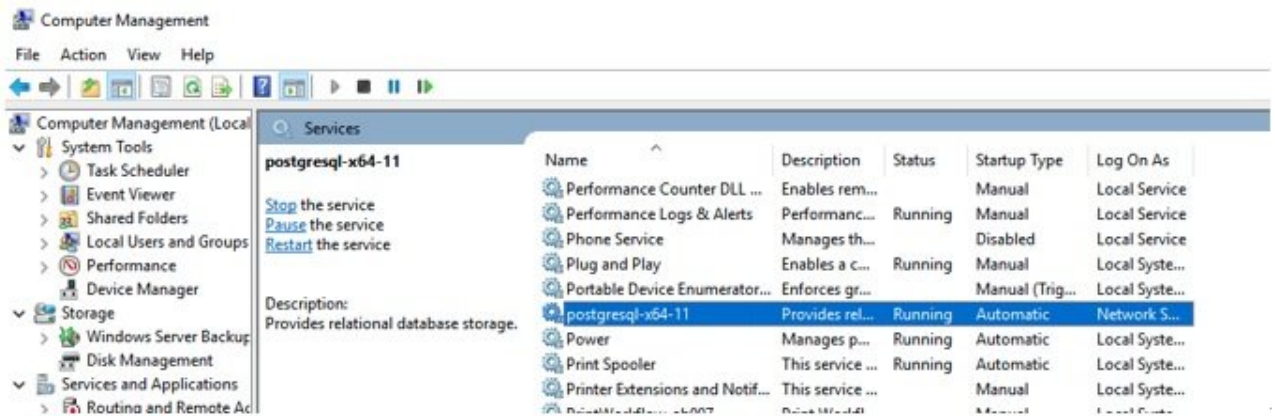
4. ミラーボリュームリソース階層が作成されると次のような画面が表示されます。



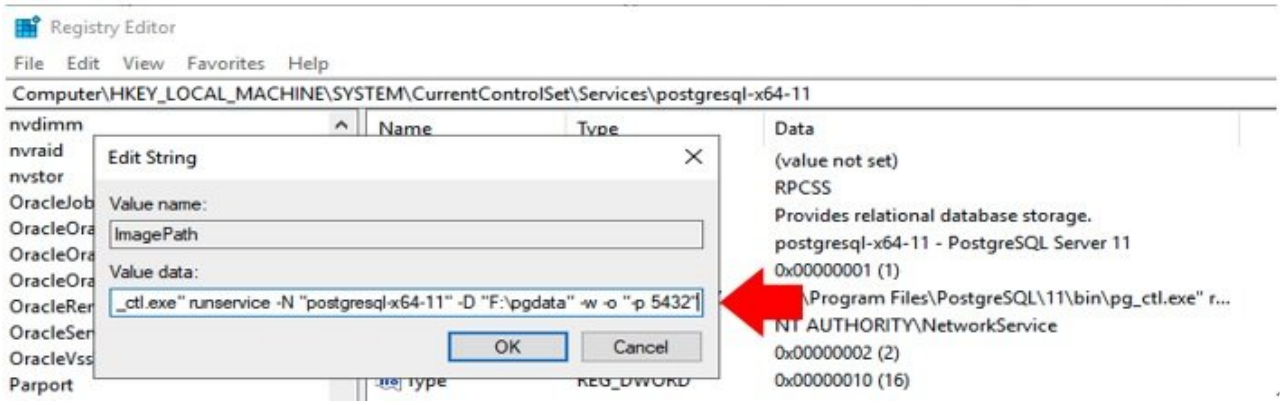
6.8.3. PostgreSQL関連パラメーターの変更（稼働系、待機系）

1. PostgreSQL起動パラメーターの追加

- サービスコントロールマネージャーで、**[postgresql-x64-11]** をStopします。



- コマンドプロンプトで `regedit` を実行します。
- 左ペインで次の階層をたどり、**[postgresql-x64-11]** を開きます。
  \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\postgresql-x64-11
- ImagePathをダブルクリックして開き、Value data（ダイアログ下部の文字列）の最後に次の文字列を追加して、OKをクリックします。
  `-o "-p 5432"`



- 先ほど停止したpostgresql-x64-11サービスをStartします。（SIOS20LKNODE01でのみ行います）。

2. F:\pgdata\pg_hba.confを編集（稼働系 SIOS20LKNODE01のみ）

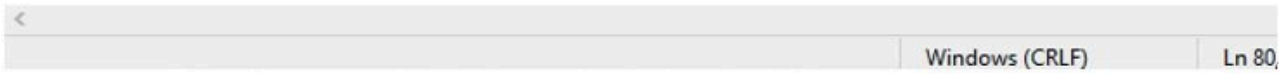
- データベースクラスターの管理ユーザーの認証方式は、「trust」に設定する必要があります。(IPv4およびIPv6) …下記①
- 接続するクライアントのネットワークアドレスを記述する必要があります。… 下記②

  以下に、編集例を示します。

```
# IPv4 local connections:
# host    all             all             127.0.0.1/32            md5
host    all             postgres        127.0.0.1/32            trust ····· ①
host    all             all             10.20.1.0/24            md5 ····· ②

# IPv6 local connections:
# host    all             all             ::1/128                 md5
host    all             postgres        ::1/128                 trust ····· ①

# Allow replication connections from localhost, by a user with the
# replication privilege.
host    replication     all             127.0.0.1/32            md5
host    replication     all             ::1/128                 md5
```



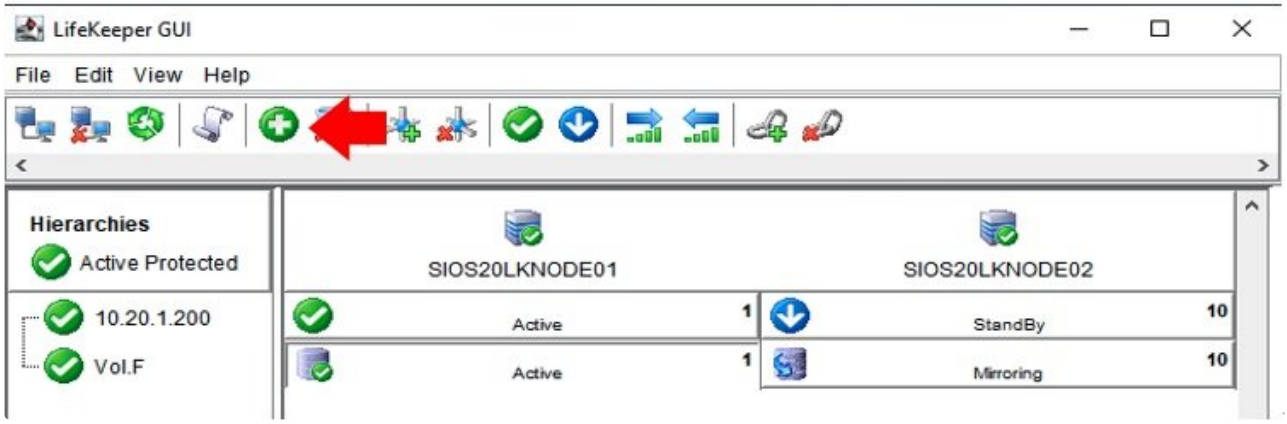
6.8.4. PostgreSQLデータベースの保護（稼働系）

PostgreSQLリソース階層の作成

1. 稼働系（SIOS20LKNODE01）のWindows OSに、SIOS20\lkadminでログインします。

2. LifeKeeper GUIを起動し、SIOS20\lkadminでログインします。

3. **リソース階層作成** アイコン（緑色の＋）をクリックし、ウィザードに従って次の表の通り設定値を入力します。

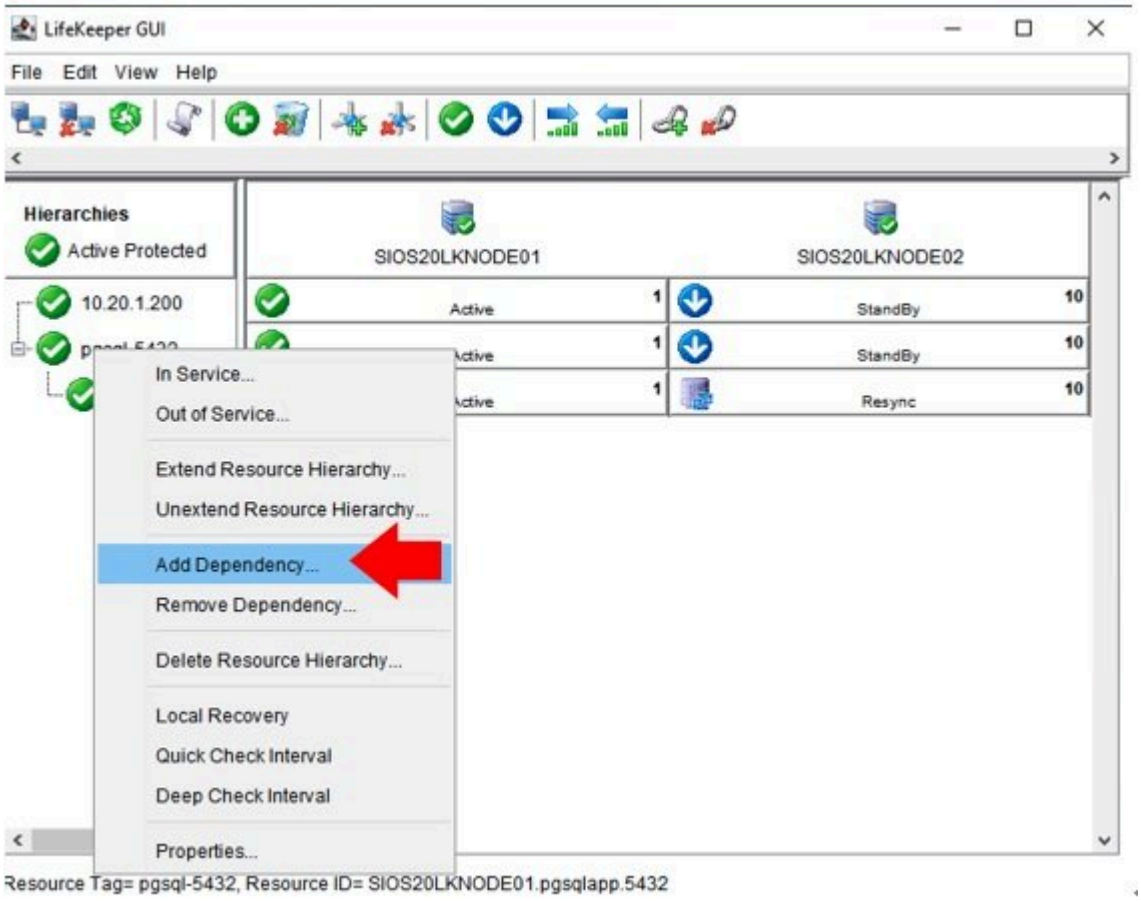


4. 次の表に従って設定値を入力します。

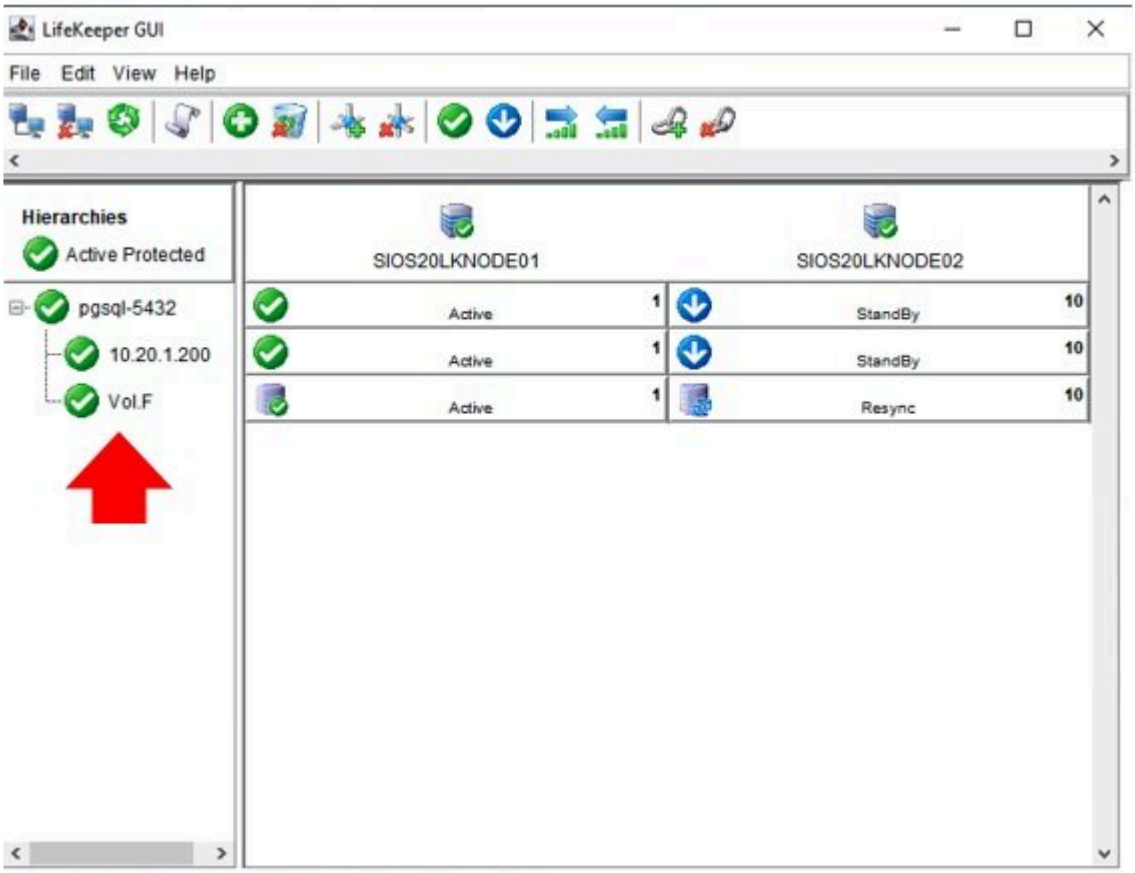
PostgreSQLリソース	
Primary Server	SIOS20LKNODE01
Backup Server	SIOS20LKNODE02
Application to protect	PostgreSQL Server
PostgreSQL Service Name	postgresql-x64-11
PostgreSQL Executable Location	C:\Program Files\PostgreSQL\11\bin（既定値）
PostgreSQL Data Directory	F:\pgdata
PostgreSQL port	5432
Database Administration User	postgres
PostgreSQL Database Tag	pgsql-5432（既定値）
Backup Priority	10（既定値）

PostgreSQLリソース依存関係の作成

1. ここでは、PostgreSQLリソース階層に、IPアドレスリソースを追加します。



2. ここまででPostgreSQLリソースに必要な依存関係の作成は完了です。次のようにリソース階層が作成されています。IPアドレスリソースとVolumeリソースが親リソース「pgsql-5432」の子リソースになっていることに注目してください。


LifeKeeper GUI
File Edit View Help
Hierarchies
Active Protected
pgsql-5432
10.20.1.200
Vol.F
SIOS20LKNODE01
SIOS20LKNODE02
Active 1
StandBy 10
Active 1
StandBy 10
Active 1
Resync 10
<-- SIOS20LKNODE02: 10.20.1.200: Adding parent: pgsql-5432

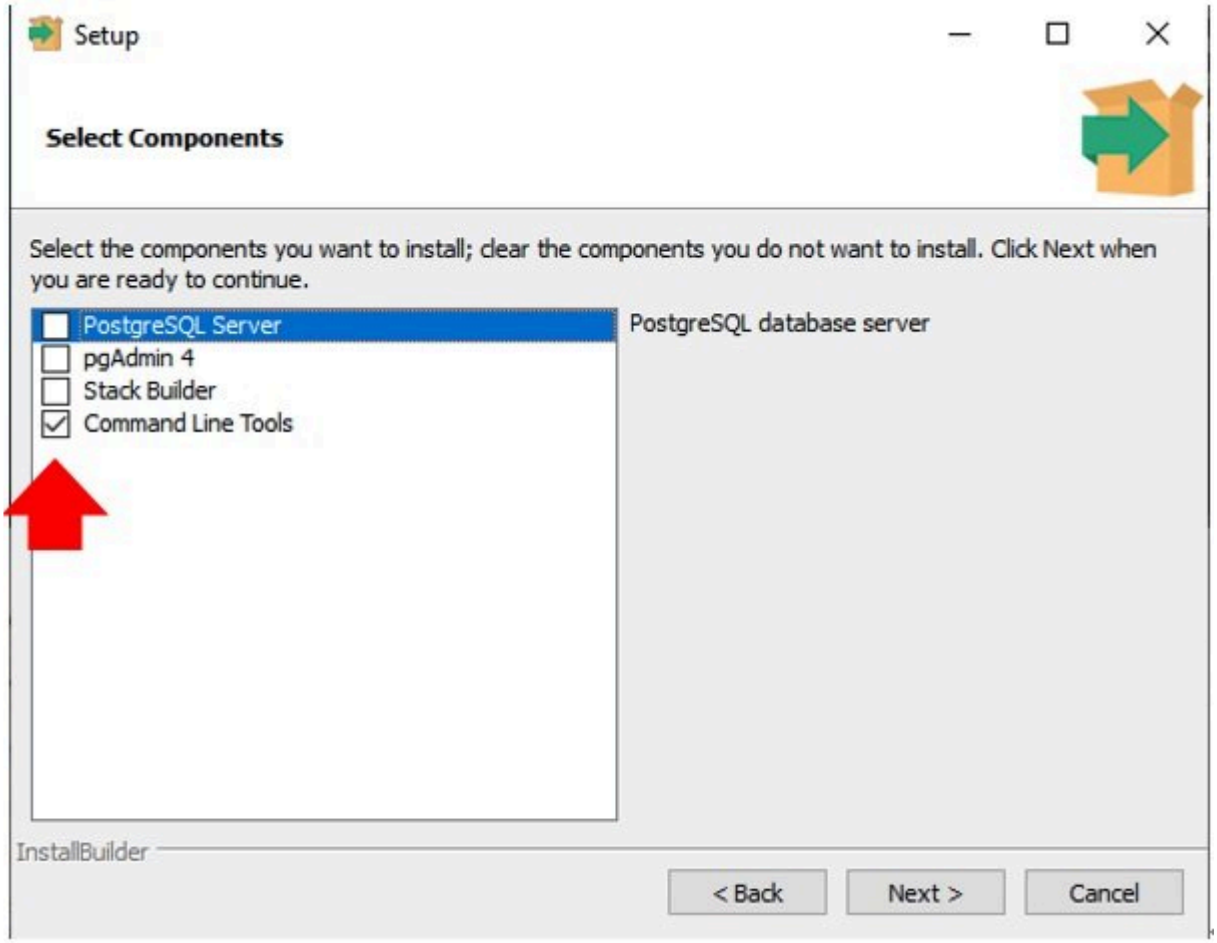
6.8.5. 接続確認（クライアント）

PostgreSQLクライアントのインストール

1. SIOS20LKCLIENTにSIOS20\lkadminでログインします。

2. 次のサイトから、PostgreSQL(Windows x86-64)インストールイメージをダウンロードして任意の場所に置き、ダブルクリックして開きます。ここではバージョン11.7を使いました。なお、このインストールイメージはPostgreSQLサーバー用のものと同一です。
   https://www.enterprisedb.com/downloads/postgres-postgresql-downloads

3. インストール対象として、**Command Line Tools** だけを選択します。

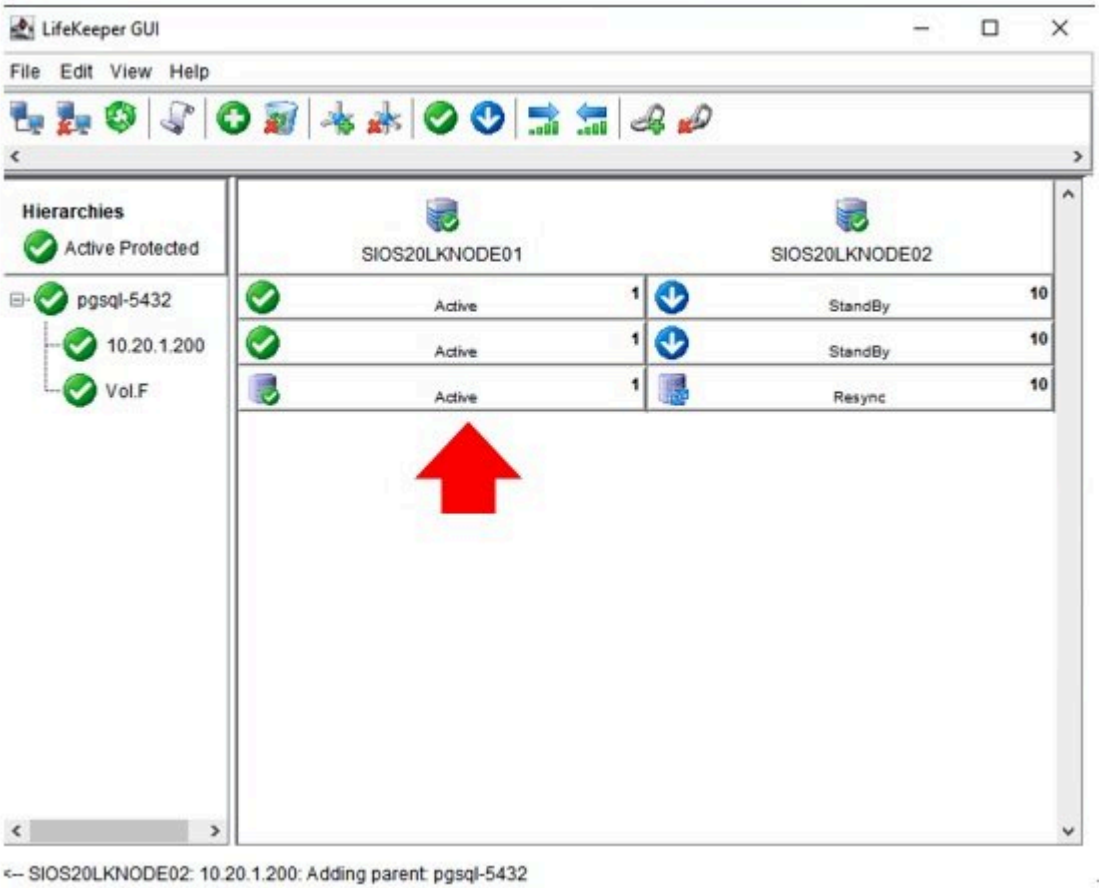


   以降は、ウィザードに従って、既定値でインストールします。

PostgreSQLクライアントの接続確認

1. SIOS20LKNODE01またはSIOS20LKNODE02に、sios20\lkadminとしてログインします。

2. LifeKeeper GUIを起動して、次のように、リソース階層がSIOS20LKNODE01上でActiveになっていることを確認します。



3. SIOS20LKCLIENTにsios20\lkadminとしてログインします。

4. コマンドプロンプトを開き、下記コマンドを実行します。

- `"\Program Files\PostgreSQL\11\bin\psql" -h 10.20.1.200 -p 5432 -U postgres -l`
  パスワードを入力してデータベース一覧が表示されれば正常動作です

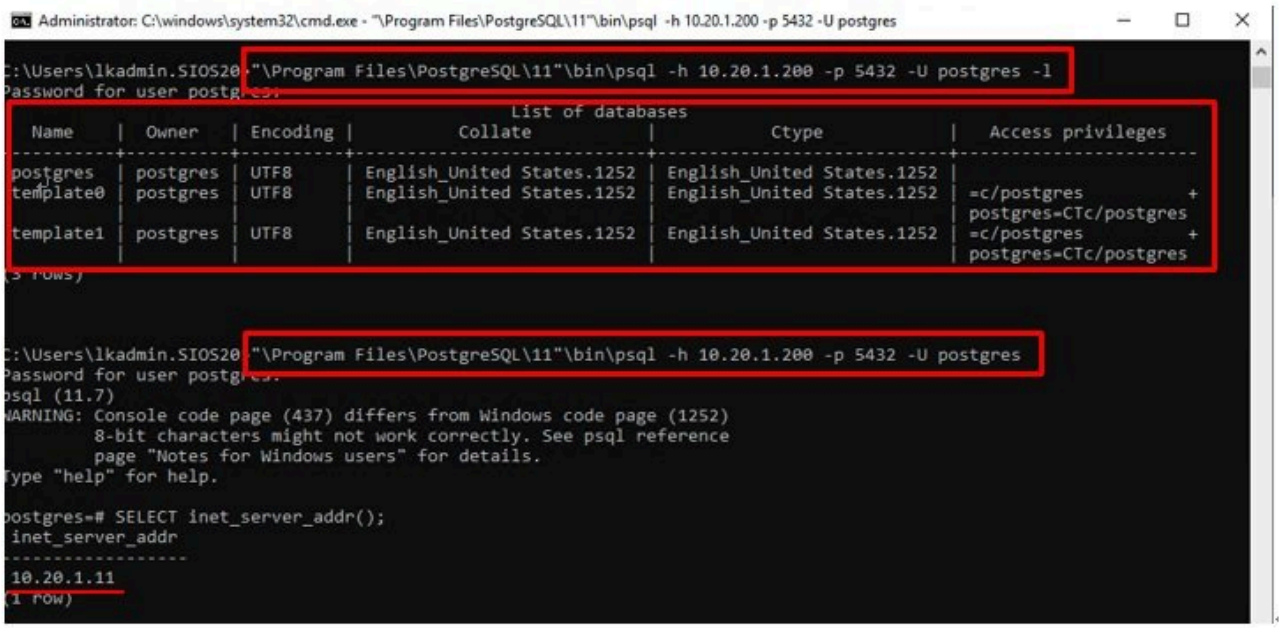
5. さらに次のコマンドを実行します。

- `"\Program Files\PostgreSQL\11\bin\psql" -h 10.20.1.200 -p 5432 -U postgres`

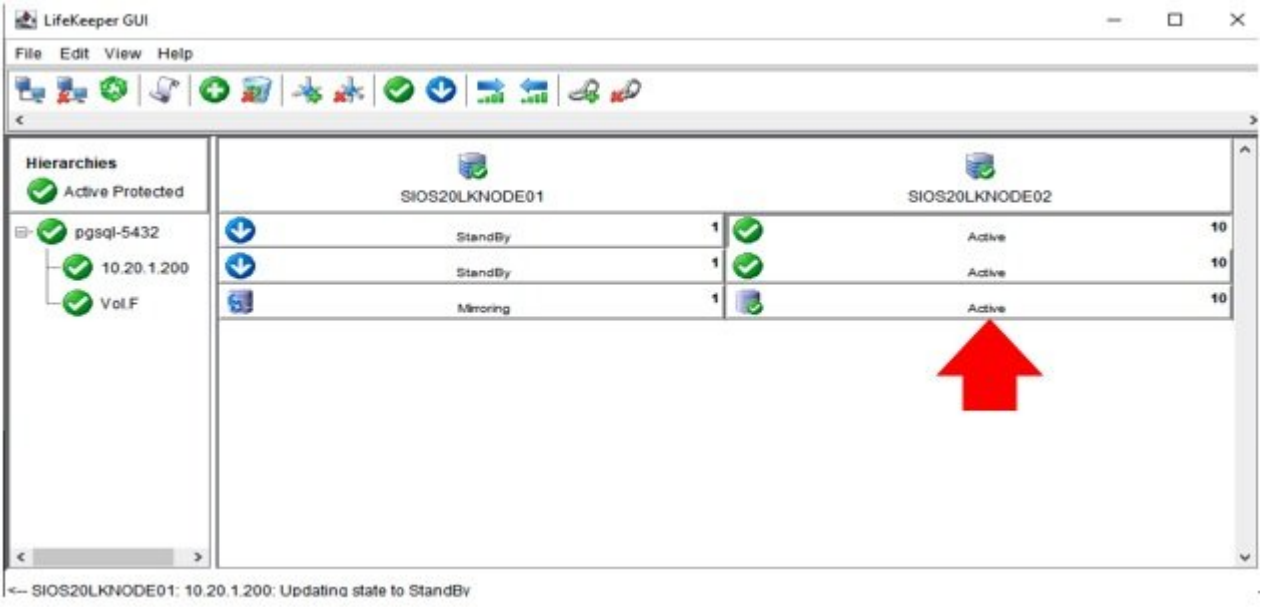
  パスワードを入力し、次の内部コマンドを実行します。

  ```
  SELECT inet_server_addr();
  ```

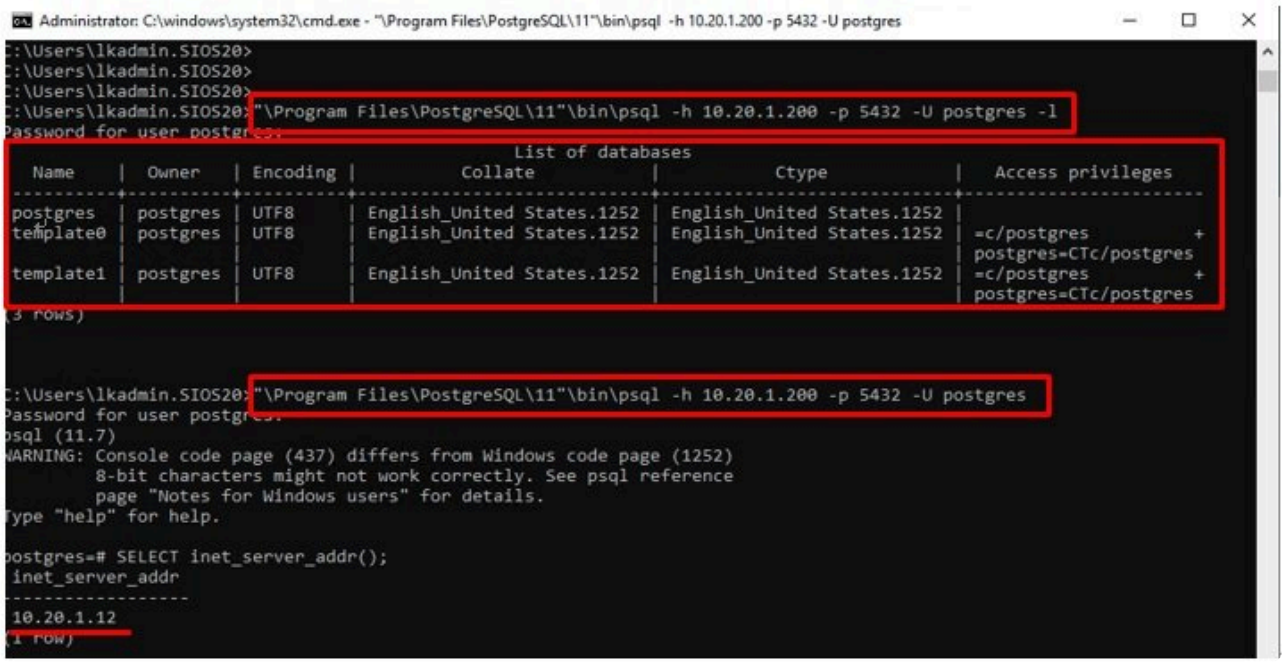
  PostgreSQLサーバーが動作しているサーバーのIPアドレスが表示されます。
  10.20.1.11(SIOS20LKNODE01)となっています。



6. 次にLifeKeeper GUIを使って、PostgreSQL関連リソースが（下の図のとおり）SIOS20LKNODE02でActiveになるようにします。



7. SIOS20LKCLIENT上で、先ほどと同じコマンドを実行します。最後に表示されるIPアドレスが10.20.1.12(SIOS20LKNODE02)となっていることに注目してください。



以上で接続確認は完了です。

7. SIOS Protection Suite インストレーションガイド

インストレーションガイドのトピックは SIOS Protection Suite cluster 環境を定義するのに役立ちます。SIOS Protection Suite 構成が確立できたら、以下のトピックが SIOS Protection Suite のセットアップやライセンス処理、インストールにおいて役立ちます。

SIOS Protection Suite 環境のプランニング

SIOS Protection Suite 環境のセットアップ

SIOS Protection Suite のインストール

7.1. SIOS Protection Suite 環境のプランニング

このセクションは、SIOS Protection Suite クラスタ環境を定義して、迅速かつ効果的に高可用性を実現するのに役立ちます。

主要なトピックは以下のとおりです。

サーバ通信のプランニング

リカバリキットの要件

ストレージとアダプタの要件

サーバ仕様の確認

7.1.1. サーバ通信のプランニング

以下のガイドラインに従って、下図のような構成マップでサーバ通信を決定して文書化してください。

- クラスタ要件: 単一障害点を作らないために、クラスタ内のサーバの間には少なくとも 2 つのコミュニケーションパス (「ハートビート」とも呼ばれます) が必要です。詳細は、下記の「コミュニケーションパスの考慮事項」を参照してください。

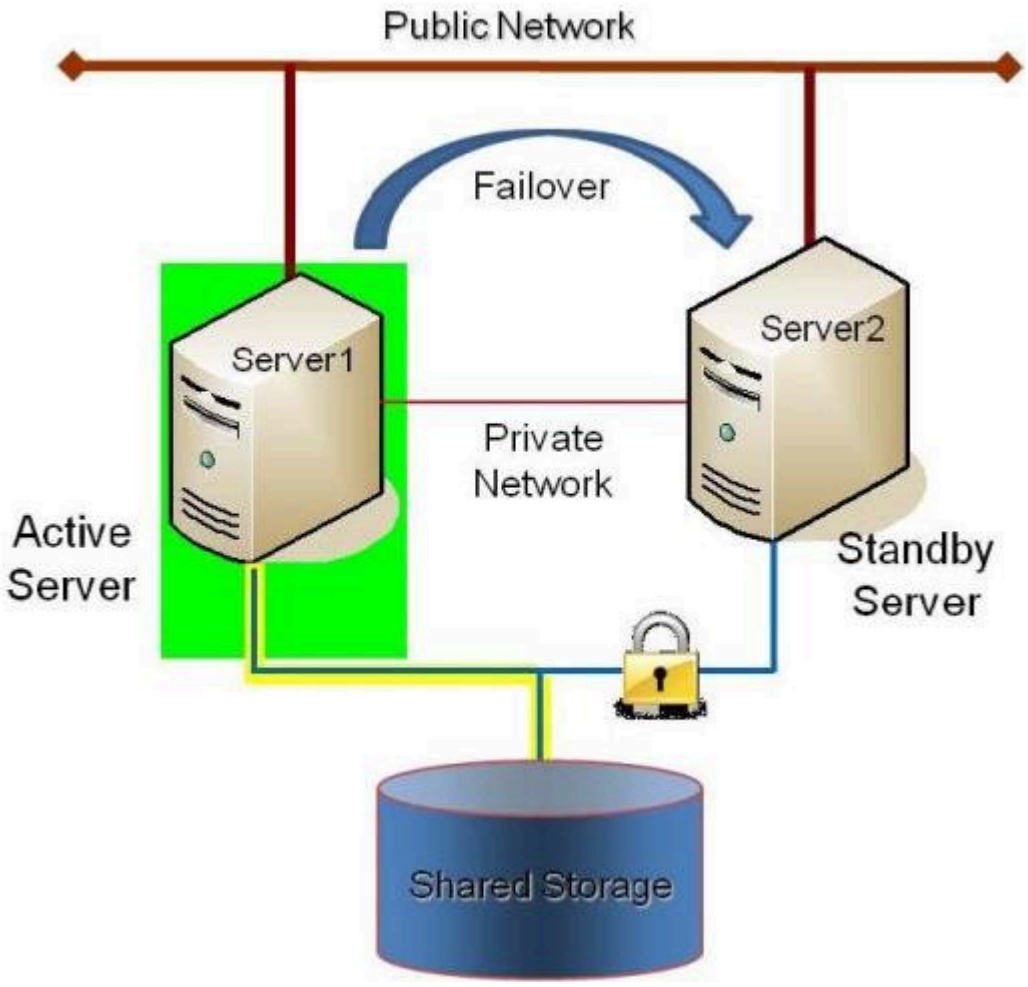


図 1: SIOS Protection Suite ペアのサンプル構成マップ

これは、ディスクアレイサブシステムを共有する SIOS Protection Suite サーバのペアを図示した非常に簡単な構成マップです。標準の状態では、Server1 でアプリケーションが実行されており、プライマリサーバ (アクティブサーバ) と見なされます。Server2 はセカンダリサーバ (スタンバイサーバ) です。この場合、ディスクアレイのボリューム全体をリザーブするのは 1 度に 1 台のサーバだけなので、ディスクリソースの競合は発生しません。

このサンプルクラスタには、パブリックネットワークおよびプライベートネットワークに構成された TCP/IP コミュニケーションパスも図示されています。構成マップには、各 TCP/IP コミュニケーションパスに関連付けられた IP アドレスを記入してください。

サーバのペアは最も簡単な SIOS Protection Suite 構成です。3 台以上のサーバで構成されるクラスタのプランニングでは、サーバ間に適切な接続が存在することを保証するために構成マップがより重要になります。カスケーディ

ングフェイルオーバ機能を提供するには、各サーバがクラスタ内の他のすべてのサーバへの物理コミュニケーションパスを持つ必要があります。

注記: 共有ストレージの代わりに複製ストレージを使用する場合は、SIOS DataKeeper のレプリケーション用ハードウェアおよびソフトウェアの構成に関する追加情報を参照してください。

コミュニケーションパスの考慮事項

SIOS Protection Suite コミュニケーションパスは、クラスタ内の保護対象リソースの状態を通信し、フェイルオーバを管理するために使用されます。各コミュニケーションパスには優先順位の数字が割り当てられており、最も小さい数字が「最も高い」優先順位を表します。

独立したサブネット上に 2 つの異なる LAN ベース (TCP/IP) コミュニケーションパスがある構成を推奨します。プライマリコミュニケーションパスはプライベートネットワーク上に構成してください。**プライマリコミュニケーションパスを伝送するネットワークインターフェースカード (NIC) には、切り替え可能な IP アドレスを構成しないでください** 。

冗長コミュニケーションパス

SIOS Protection Suite では、可能な場合は常に冗長コミュニケーションパスを構成することを強く推奨します。コミュニケーションパスを 1 本だけ使用した場合、そのコミュニケーションパスに障害が発生すると、SIOS Protection Suite のリソース階層が複数システムで同時にサービスを起動することがあります。これはフェイルオーバの誤動作または「スプリットブレイン」状態と呼ばれます。スプリットブレイン状態では、各サーバは自身がアプリケーションを管理していると認識しているので、共有ストレージデバイスにアクセスしたり、データを書き込んだりする場合があります。

プライマリコミュニケーションパス (プライベートネットワーク)

プライベート TCP/IP コミュニケーションパスは、パブリックネットワーク上で発生する通信の影響を受けず、システム間の信頼性の高い通信を提供します。このため、プライマリコミュニケーションパスをプライベートネットワーク上に構成し、セカンダリコミュニケーションパスはパブリックネットワーク上に構成することを推奨します。プライベートネットワークアドレスは DNS に登録してはいけません。プライベートネットワークアドレスについては、**[この接続のアドレスを DNS に登録する]** チェックボックスをオンにしないでください。

SIOS Protection Suite の TCP/IP コミュニケーションパスは、静的な IP アドレスおよびサブネットマスクを使用して構成されます。ケーブリングは、2 ノードクラスタの場合はクロスオーバケーブル、3 ノード以上のクラスタの場合は小型のハブを使用してください。

注記: プライベートネットワーク接続を DNS に登録しないことは非常に重要です。DNS は、通常、サーバごとのパブリックネットワーク接続のみを公開します。これは、ローカル LifeKeeper GUI 管理クライアントをリモート SIOS Protection Suite システムに接続する場合に重要になります。ネットワーク構成の詳細については、ネットワーク構成の確認 を参照してください。

7.1.2. リカバリキットの要件

SIOS Protection Suite Recovery Kit クラスタのすべてのコンポーネントのプランニングと接続において考慮する必要がある要件があります。SIOS Protection Suite for Windows リリースノート にはプログラムのバージョンやディスク容量の要件など、各キットの技術的な要件が記載されていますが、詳細な構成情報については、リカバリキットを参照してください。

Core リカバリキット (Volume、IP、LAN Manager、File Share、DNS、Microsoft Internet Information Services (IIS)、Generic Application) については、SIOS Protection Suite for Windows テクニカルドキュメンテーション を参照してください。

注記: すべてのオプションの SIOS Protection Suite Recovery kit には LifeKeeper v4.3 以降と動作させるためにライセンスが必要になります。スタート-> [すべてのプログラム] -> [SIOS] -> [LifeKeeper] -> [License Key Installer] から License key ユーティリティを起動してライセンスをインストールすることが可能です。

7.1.3. ストレージとアダプタの要件

SIOS Protection Suite 構成では、共有 SCSI ホストアダプタおよび共有ディスクハードウェアの機能を使用して、障害が発生したサーバから指定のバックアップサーバにリソースを切り替えることができます。また、ファイバチャネルストレージエリアネットワーク (SAN) を使用することもできます。

以下のガイドラインに従って、ストレージとホストアダプタの要件を判断してください。

ストレージデバイス - アプリケーションのデータストレージ要件に基づいて、構成に必要なデータストレージデバイスのタイプと数を判断する必要があります。共有ファイルはディスクアレイサブシステム (Redundant Array of Inexpensive Disks、RAID) に配置してください。SIOS Protection Suite 構成では多数のハードウェア RAID 周辺機器を使用することができます。最も重要な要件は Microsoft がサポートしていることです。Microsoft のハードウェア互換リスト を参照してください。

重要: ストレージデバイスの構成のプランニングでは、以下の問題を考慮してください。

- SIOS Protection Suite はリソースをボリューム単位で管理するので、構成内の各ボリュームのリソースを使用できるのは 1 度に 1 台のサーバだけです。そのため、SIOS Protection Suite の構成を開始する前にディスクの割り当てを計画することを推奨します。

アダプタ - 構成のタイプと周辺機器の数に基づいて、必要な SCSI ホストアダプタまたはファイバチャネルホストアダプタのタイプと数を判断してください。選択したアダプタを Microsoft がサポートしており、ドライバを入手できることが重要です。Microsoft がサポートするアダプタと周辺機器については、Microsoft のハードウェア互換リスト の「クラスタ」カテゴリを参照してください。

参照用に、構成マップにホストアダプタの仕様を追加してください。

7.1.4. サーバ仕様の確認

各 SIOS Protection Suite サーバで、以下のコンポーネントについてバージョンと性能が適切であることを確認してください。

- Windows 2008 R2、2012、2012 R2 および 2016 オペレーティングシステム (64 ビットのみ)

  注記: クラスタ内のすべてのサーバで同一バージョンの Windows を実行してください。

  注記: Lan Manager および DataKeeper 複製ボリュームで使用するために、ファイルとプリンタ共有が有効になります。必要なポートを開き、ICMP を有効にするために、SIOS Protection Suite ではインストール時に Windows 2008 ファイアウォールが自動的に構成されます。

  注記: DataKeeper 複製ボリュームを SIOS Protection Suite とともに使用する予定がある場合は、ローカルセキュリティポリシー **[ネットワークアクセス: Everyone アクセス許可を匿名ユーザに適用する]** を*有効*にする必要があります。LifeKeeper をインストールすると、このポリシーが有効になります。

  注記: インストール中、ファイアウォールの状態（有効または無効）に関係なく、LifeKeeperに必要な適切な規則がWindowsファイアウォールに追加されます。インストール中にファイアウォールのルールがインストールされなかった場合は、ファイアウォールの設定スクリプトを実行してファイアウォールの規則を追加できます。このスクリプトは、*LKROOT%\support\firewallSetup.bat* としてインストールされます。コマンドラインからコマンドを実行するには、`firewallSetup.bat %LKROOT` と入力してください。

作成されたファイアウォールルールの一覧

ルール名	ポート
LifeKeeper CommPath.1500	TCP 1500
LifeKeeper CommPath.1510	TCP 1510
LifeKeeper EISM	TCP 3279
LifeKeeper ICMPv4	ICMPv4
LifeKeeper Java	C:\LK\jre1.7.0_10\bin\java.exe – all ports
LifeKeeper lkcmserver	TCP 3278
LifeKeeper RMI	TCP 81
LifeKeeper Web Server	TCP 82
SIOS DataKeeper Dispatch port 9999	TCP 9999
SIOS	TCP 139

DataKeeper File Share port 139	
SIOS DataKeeper File Share port 445	TCP 445
SIOS DataKeeper NETBIOS port 137	UDP 137
SIOS DataKeeper NETBIOS port 138	UDP 138
SIOS DataKeeper Volumes	TCP 10000, 10001, 10002, 10003, 10004, 10005, 10006, 10007, 10008, 10009, 10010, 10011, 10012, 10013, 10014, 10015, 10016, 10017, 10018, 10019, 10020, 10021, 10022, 10023, 10024, 10025

外部ハードウェアのファイアウォール

ルール名	ポート
RMIポート	2つのエンドポイント間（サーバーAとB）の間でのみ、TCP 1024-65535 **注記:** これは、ハードウェアまたはクラウドファイアウォールでセットアップする必要があります。Windows ファイアウォールでは必要ありません。

- LAN ベースのクラスタハートビートのためのイーサネット TCP/IP 対応ネットワークインターフェースカード
- 共有ストレージを使用する場合、ディスクアレイおよびストレージアダプタ (SCSI またはファイバチャネル)
- メモリ。SIOS Protection Suite の最小メモリ要件については、SIOS Protection Suite for Windows リリースノート を参照してください。

注記: ユーザアプリケーションを実行するには、(SIOS Protection Suite に必要なメモリ以外に) さらにメモリが必要となります。

- ディスク容量。SIOS Protection Suite およびリカバリキットの最小ディスク容量要件については、SIOS Protection Suite for Windows リリースノート を参照してください。
- LifeKeeper グラフィカルユーザインターフェース (GUI) のプラットフォームおよびブラウザ
- 電源要件。SIOS Protection Suite サーバの可用性を最大にするために、無停電電源装置 (UPS) を使用するか、少なくとも各サーバの電源を分離することを強く推奨します。
- SIOS Protection Suite で保護するアプリケーションソフトウェア

構成のサーバ名、プロセッサタイプ、メモリ、およびその他の I/O デバイスを決定してください。バックアップサーバを指定する場合は、選択したサーバが、プライマリサーバで障害が発生した場合に処理を実行するための性能を備えていることを確認してください。

7.2. SIOS Protection Suite 環境のセットアップ

要件を判断して SIOS Protection Suite 構成を定義したら、SIOS Protection Suite 環境のコンポーネントのセットアップを開始できます。

このトピックの主要な作業は以下のとおりです。

- ストレージの構成
- DNS リソースの要件
- データベースアプリケーションのインストールと設定
- 共有ディスクボリュームインスタンスの安全な作成
- ネットワーク構成の確認

注記: 異なる順序で実行できるセットアップ作業もありますが、このリストの順に実行することを推奨します。

7.2.1. ストレージの構成

SIOS Protection Suite は共有ストレージで使用することも、複製ストレージで使用することもできます。構成に当てはまる指示に従ってください。

共有ストレージ構成

共有ストレージを使用する場合は、Windows 環境をインストールした後、ホストアダプタおよび共有される周辺機器のアドレス指定を設定してください。

注記: ダイナミックディスクは共有ストレージではサポート対象外です。ダイナミックディスク構成は各システム上のどこかに (文書化されていません) 保存されますが、ディスク自体には保存されないためです。現在 2 つのシステム間で構成を複製する方法が存在しません。

詳細は、アダプタおよびストレージデバイスに付属のドキュメントを参照してください。SIOS Protection Suite クラスタ内のすべてのサーバが共有ストレージにアクセスできるように設定するには、以下の作業を行ってください。

1. SIOS Protection Suite によって保護されるディスクはすべてパーティションに分割する必要があるので、Windows ディスクの管理ユーティリティを使用して、共有ディスクアレイのパーティション (ボリューム) を構成する必要があります。また、パーティションは NTFS ファイルシステムでフォーマットする必要があります。

   注記: 共有ストレージを安全に構成するために、共有ディスクボリュームインスタンスの安全な作成 の手順に従うことを推奨します。

   詳細については、ディスクアレイソフトウェアのドキュメントを参照してください。

2. 共有ディスクコミュニケーションパスを使用する予定がある場合は、コミュニケーションパスに使用する小さい raw (未フォーマット) パーティションを指定してください。サイズは 1 MB で十分です。
3. クラスタ内の他のサーバの電源を投入して、すべてのサーバが共有ディスクを認識していることを確認してください。バックアップサーバから、共有ボリュームのドライブの割り当てが最初のサーバとまったく同じになるようにしてください。ディスクの管理ユーティリティを開くのは 1 度に 1 台のサーバだけにすることを推奨します。
4. 共有ボリュームでファイル共有を作成した場合は、クラスタ内の各サーバで、これらのフォルダのファイル共有属性をオンにする必要があります。

複製ボリューム構成

SIOS DataKeeper for Windows を使用する場合は、Windows ディスクの管理ユーティリティを使用して、複製されるディスクパーティション (ボリューム) を作成してください。また、パーティションは NTFS ファイルシステムでフォーマットする必要があります。

(プライマリサーバの) ソースボリュームと (バックアップサーバの) ターゲットボリュームには同じドライブレターを割り当ててください。

7.2.2. DNS リソースの要件

SIOS Protection Suite for Windows Core 製品に付属する DNS Recovery Kit は、構成内の DNS サーバのうちプライマリサーバまたは LifeKeeper 別名の A レコードと PTR レコードを更新します。DNS リソースを使用すると、DNS プライマリサーバまたは LifeKeeper 別名の A レコードを選択することができます。フェイルオーバまたはスイッチオーバの発生時に、この A レコードと PTR レコード (存在する場合) は、バックアップサーバの IP アドレスで変更されます。DNS リソースを使用すると、フェイルオーバまたはスイッチオーバの発生時に、クライアントが WAN 環境内のサーバに接続することができます。SIOS Protection Suite サーバが異なるネットワークサブネットにある場合、切り替え可能な IP アドレスを使用することはできません。このタイプの構成では、DNS リソースを使用してクライアントを接続してください。DNS リソースの作成の詳細については、DNS リソース階層の作成 を参照してください。

制限: SIOS Protection Suite サーバをドメインコントローラまたは DNS サーバとして構成しないでください。同じシステム上の DNS サーバを指す DNS リソースを作成すると、次のエラーメッセージが表示されて失敗します。
`"User credentials cannot be used for local connections."`

DNS レコードの TTL

SIOS Protection Suite for Windows DNS Recovery Kit によって DNS プライマリサーバまたは LifeKeeper 別名の A レコードが更新されても、キャッシング DNS サーバのキャッシュの A レコードは更新されません。これらのキャッシング DNS サーバは、SIOS Protection Suite によって保護される A レコードが属するゾーンを保持していません。TTL が期限切れになるか、キャッシュを手動でクリアするまで、A レコードはキャッシュ内に残ります。そのため、これらのキャッシング DNS サーバのクライアントは、A レコードの更新された値を適切な時期に取得できません。SIOS Protection Suite によって保護される DNS リソースについては、プライマリサーバまたは LifeKeeper 別名の A レコードの TTL 値を小さい値に設定することを推奨します。

SIOS Protection Suite によって DNS リソースの A レコードと PTR レコードが作成される場合、これらのレコードの TTL は 5 分に設定されます。この値は Microsoft DNS 管理コンソール (dnsmgmt.msc) を使用して変更できます。ただし、値を大きくすると、A レコードはキャッシング DNS サーバのキャッシュ内でより長く存続します。

SIOS Protection Suite DNS リソース階層を作成する前に作成された DNS の A レコードおよび PTR レコードについては、TTL 値を 5 分程度の小さい値に設定することを推奨します。

7.2.3. データベースアプリケーションのインストールと設定

保護対象データベースアプリケーションとして SQL Server を環境に含める場合は、データベースに付属のドキュメントに従ってアプリケーションをインストールしてください。データベースおよび構成ファイルが共有ファイルシステムまたは複製ファイルシステムにあることを確認してください。実行可能ファイルは、各ローカルファイルシステムに配置することも、共有ファイルシステムに配置することもできます。SQL Server のインストールや設定の考慮事項については、SIOS Protection Suite Microsoft SQL Server Recovery Kit テクニカルドキュメンテーション を参照してください。

SIOS Protection Suite をインストールした後にアプリケーションをインストールすることもできますが、SIOS Protection Suite で保護する前に、アプリケーションが正しく設定され、正常に動作していることをテストしてください。

7.2.4. 共有ディスクボリュームインスタンスの安全な作成

共有ストレージボリュームリソースを安全に作成するには、ボリュームに対する書き込みアクセスを持つのは 1 度に 1 つのシステムだけになるようにする必要があります。これには SIOS Protection Suite インスタンスを作成する前も含まれます。

SIOS Protection Suite はインスタンスを作成する前にボリュームが共有されていることを認識できないので、ボリュームが同時に 2 つ以上のシステムで書き込み可能になることがないように、手動の手順が必要になります。

ボリュームの同時書き込みアクセスを防ぐには、以下の手順を使用してください。この例では、2 つのシステム (SYSA および SYSB) が共有ストレージに接続されています。このストレージは 2 つのボリュームで構成されており、両方のシステムでドライブレター E: および F: を割り当ててから、SIOS Protection Suite ボリュームインスタンスで保護します。

1. SYSB の電源はオフにしたまま、SYSA の電源をオンにします。
2. LifeKeeper をまだインストールしていない場合は、インストールします。
3. ボリュームにドライブレター E および F を割り当て、まだフォーマットしていない場合は NTFS でフォーマットします。
4. SYSA の電源をオフにします。
5. SYSB の電源をオンにします。
6. LifeKeeper をまだインストールしていない場合は、インストールします。
7. 共有ボリュームにドライブレター E: および F: を割り当てます。
8. コマンドプロンプトで、以下のコマンドを実行します。

```
%LKBIN%\volume -p E

%LKBIN%\volume -p F
```

9. SYSB を再起動します。E: および F: ドライブがロックされて再起動します。
10. SYSA の電源をオンにします。E: および F: ドライブが書き込み可能になって再起動します。
11. SYSA で E: および F: についてボリュームリソースを作成し、SYSB に拡張します。

システムの電源をオフにする代わりに、ディスクの管理を使用して、共有物理ディスクをオフラインにすることもできます。

7.2.5. ネットワーク構成の確認

SIOS Protection Suite をインストールする前に、ネットワークを構成し正常に動作していることを確認することが重要です。ネットワークの動作を確認するために、この時点で行う作業がいくつかあります。

1. TCP/IP コミュニケーションパスを作成したり、IP アドレスを保護したりするには、すべてのネットワークインターフェースカード (NIC) が固定 IP アドレスを 1 つ持っていることを確認する必要があります。

2. サーバに複数の NIC がある場合 (推奨)、異なるサブネット上に構成してください。アダプタが同じサブネット上にある場合、TCP/IP では 2 つ目のアダプタを効果的に使用することができません。

3. IP アドレスは以下のように構成してください。各サーバに少なくとも 2 つの NIC (プライベートネットワークに 1 つ、パブリックネットワークに 1 つ) があるものとします。

   a. [コントロール パネル] で [ネットワーク接続] をクリックしてください。[開く] を右クリックしてください。

   b. [詳細] メニューから [詳細設定] を選択してください。

   c. パブリックネットワークに接続された NIC が [接続] リストの一番上にあることを確認してください。

   d. プライベートネットワーク接続は DNS に登録しないでください。プライベートネットワークアダプタについては、以下の手順に従って [DNS] タブを開き、[この接続のアドレスを DNS に登録する] チェックボックスをオフにしてください。

   [Internet Protocol (TCP/IP) Properties]-> [詳細]-> [DNS] Tab

   プライベートネットワーク接続には DNS サーバは不要なので、リストには何も含めないでください。

   これによって、LAN Manager コンピュータ名のスイッチオーバ時にブラウザが混乱するのを防ぐことができます。

4. 各サーバから、ローカルサーバおよびクラスタ内の他のサーバに ping を実行してください。ping が失敗する場合は、続行する前に必要なトラブルシューティングと修正処置を行ってください。

5. LifeKeeper GUI サーバとクライアントコンポーネントが効果的に通信できるようにすることで、クラスタ内の各サーバが localhost を解決できるようになります。

   ・DNS が実装されていなければ、***%windir%\system32\etc\drivers\hosts*** ファイルを編集し、localhost 名を追加してください。ローカルサーバの IP アドレス、またはデフォルトエントリ (127.0.0.1) を指定できます。localhost を解決できないと、LifeKeeper GUI が動作しない場合があります。

   ・DNS を実装した場合は、構成を確認して、SIOS Protection Suite クラスタ内のサーバが DNS を使用して解決されるようにしてください。

6. 各サーバのホスト名およびネットワークアドレス指定情報が正しく、SIOS Protection Suite をインストールしても変わらないことを確認してください。SIOS Protection Suite を起動した後にホスト名を変える場合は、

`lk_chg_value` ユーティリティを実行して、SIOS Protection Suite 構成ファイル内のコンピュータ名を変更する必要があります。SIOS Protection Suite を起動した後にネットワーク構成を変える場合は、ネットワーク情報を再構成した後、`lk_chg_value` ユーティリティを実行して、既存の SIOS Protection Suite コミュニケーションパスおよびリソース階層を変更する必要があります。

注記: SIOS DataKeeper for Windows を使用している場合は、ドキュメントの SIOS DataKeeper セクションで、レプリケーションに使用するネットワークカードの指定に関する追加情報と、コミュニケーションパスの考慮事項を参照してください。

切り替え可能な IP アドレス

ほとんどの SIOS Protection Suite 構成では、IP Recovery Kit を使用して、切り替え可能な IP アドレスが定義されます。切り替え可能な IP アドレスとは、サーバ間で切り替えることができる「仮想」IP アドレスであり、各サーバのネットワークインターフェースカードに関連付けられた IP アドレスから分離されています。SIOS Protection Suite によって保護されるアプリケーションには、切り替え可能な IP アドレスが関連付けられます。その後、プライマリサーバに障害が発生した場合は、切り替え可能な IP アドレスがバックアップサーバに「切り替わり」ます。

切り替え可能な IP アドレスのリソース階層を構成する予定がある場合は、クラスタ内の各サーバで以下の操作を実行する必要があります。

- コンピュータ名が正しく、変わらないことを確認してください。
- ネットワーク上で、切り替え可能な IP アドレスが一意であることを確認してください。

注記: チーミングソフトウェアを使用するか、仮想 IP リソースを作成した後、ネットワークカードを変更すると、仮想 IP リソースがいったん削除され、ネットワークカードのインデックス番号を反映した IP リソースが再作成されます。

切り替え可能な IP アドレス、DNS、および LifeKeeper GUI の考慮事項

サーバのメイン NIC で「仮想」IP アドレスを使用するときに NIC 上で DNS 登録が有効になっている 場合は、ネットワークについて特別に考慮する必要があります。登録された NIC で SIOS Protection Suite によって「仮想」IP アドレスが作成される場合、DNS はサーバに対してこの IP アドレスを追加し、ネットワーク上のホスト名の解決に使用し始めます。ただし、SIOS Protection Suite によって保護される「仮想」IP アドレスはクラスタノード間で切り替え可能です。そのため、LifeKeeper GUI が DNS に登録された「仮想」IP アドレスを使用して、ローカルおよびリモートのクラスタノードから更新を取得するのを回避するための予防措置が必要になります。

「仮想」IP アドレスを使用する場合にローカルシステムおよびリモートシステムへの LifeKeeper GUI の接続を安定させる方法は 2 つあります。

1. 各 SIOS Protection Suite ノードのネットワーク *hosts* ファイルを使用する。
   - *hosts* ファイルで、他のすべてのリモートクラスタノードに対して固定 IP アドレスを指定してください。
   - クラスタ内のすべての SIOS Protection Suite システムでこれを実行してください。

前述のように、これらのアドレスは、LifeKeeper GUI のバインドに使用される、優先順位が最も高いネットワーク上になければなりません。

2. クラスタ内の他のすべてのノードへの LifeKeeper GUI の接続に、代替ネットワークおよび関連する代替 NIC を使用する。この方法は、上述の簡単な推奨方法とは異なります。

   - 代替ネットワークおよび NIC 上の DNS 登録を有効にしてください。
   - *[ネットワーク接続]* -> *[詳細]* -> *[詳細設定]* の順に選択して、[アダプタとバインド] タブで代替ネットワークの優先順位を最も高くしてください。LifeKeeper GUI では、この優先順位が最も高いバインドネットワークが使用されます。
   - 優先順位が最も高い SIOS Protection Suite コミュニケーションパスでも、このネットワークが使用されます。
   - クラスタ内のすべての SIOS Protection Suite システムでこれを実行してください。

     LifeKeeper GUI では、すべてのクラスタノードへの接続にこの代替ネットワークが使用されます。この代替ネットワークには仮想 IP が割り当てられておらず、アドレス登録は安定しています。DNS 登録は、必要に応じてサーバのメイン/パブリック NIC にも使用できます。

注記: ネットワーク構成を変更した後に「ipconfig /flushdns」コマンドを使用すると、キャッシュされた古い DNS 情報を削除することができます。

IP ローカルリカバリ構成

SIOS Protection Suite は切り替え可能なローカル IP アドレスを監視し、障害を検出すると、同じシステム上の別のネットワークアダプタに IP アドレスを移動します。この機能は IP ローカルリカバリと呼ばれ、システム設定に関する次の要件と制限があります。

バックアップアダプタはローカルリカバリアダプタとも呼ばれ、プライマリアダプタに障害が発生すると、切り替え可能なアドレスがアクティブになります。バックアップアダプタを設定するには、次の手順に従ってください。

- 2 つのアダプタを同じ物理サブネットに接続します。
- ローカルリカバリアダプタの全アドレスは、適切にルーティングできるように、プライマリアダプタの実アドレスと異なる論理サブネット上に置く必要があります。また、プライマリアダプタに設定して SIOS Protection Suite で保護する仮想 IP アドレスとは異なる論理サブネットに置く必要があります。
- IP ローカルリカバリ機能は、IP リソースを作成する際に有効にすることができます。IP リソースを作成した後、リソース属性を変更しても、ローカルリカバリ機能を IP リソースに追加できません。
- IP リソースの IP ローカルリカバリ機能を無効にするには、「ins_setlocalrecovery」コマンドラインユーティリティを使用してください。このユーティリティは、SIOS Protection Suite の ***bin*** ディレクトリ (デフォルトで *C:\LK\bin*) に格納されています。このユーティリティの使用方法とオプションの説明を参照するには、コマンドプロンプトから「ins_setlocalrecovery」を実行してください。

IP ローカルリカバリの動作

IP ローカルリカバリ機能を有効にした場合、定期的に実行する IP リソースのディープチェックが失敗すると、SIOS Protection Suite は次の処理を実行します。

- SIOS Protection Suite はまず現在のネットワークアダプタで IP アドレスを再起動します。
- 前記の処理に失敗すると、SIOS Protection Suite は、リソースインスタンスをチェックし、バックアップ (ローカルリカバリアダプタ) が使用できるか調べます。バックアップインターフェースが使用できる場合は、IP アドレスをバックアップインターフェースに移動します。
- ローカルリカバリが完全に失敗すると、SIOS Protection Suite は、IP アドレスと依存リソースをバックアップサーバにフェイルオーバします。

ローカルリカバリ機能は、バックアップアダプタがなくても有効にすることができます。ローカルリカバリ機能を有効にすると、SIOS Protection Suite はプライマリネットワークのインターフェースを再起動しますが、それに失敗すると、リソースをバックアップサーバにフェイルオーバします。

7.3. SIOS Protection Suite のインストール

SIOS Protection Suite 環境のプランニングと設定が完了したら、クラスタ内の各サーバに SIOS Protection Suite ソフトウェアをインストールする準備ができます。

Core ソフトウェア

Core ソフトウェアのインストール

ライセンスの取得とインストール

ローカライズ言語サプリメントのインストール:

サイレントインストール

サードパーティ製品のファイル

アプリケーションディレクトリの例外事項

SPS のアンインストール

SPS のアップグレード

修復

LifeKeeper の起動

7.3.1. SIOS Protection Suite Core ソフトウェア

SIOS Protection Suite Core ソフトウェアは FTP を用いてダウンロードすることができます。SIOS Protection Suite Core は以下で構成されています。

- 以下を含む、基本的な LifeKeeper ソフトウェア
  - Perl (CPAN v5.8.8)
  - Cygwin 2.8
  - Java OpenJDK v15.0.1
  - LifeKeeper GUI (サーバとクライアントの両方)
  - Microsoft Visual C++ 2015 Redistributable (x64) package (v14.0.23026)

- Core リカバリキット
  - ボリューム
  - IP
  - DNS
  - LAN Manager
  - ファイル共有
  - 汎用アプリケーション
  - Internet Information Services (IIS)
  - PostgreSQL Server

- DataKeeper
  - DataKeeper ドライバ (ExtMirr.sys)
  - DataKeeper サービス (ExtMirrSvc.exe)
  - コマンドラインインターフェース (EMCMD.exe)
  - DataKeeper GUI (Datakeeper.msc)
  - パッケージファイル、SIOS Protection Suite スクリプト、ヘルプファイルなど

7.3.2. SIOS Protection Suite Core ソフトウェアのインストール

SIOS Protection Suite は、Flexera InstallShield 製品を使用して標準的なインストールインターフェースを提供します。クラスタ内のサーバごとにライセンスを取得してインストールする必要があります。

SIOS Protection Suite for Windows リリースノート を読んでから SIOS Protection Suite のインストールと構成を行うことを推奨します。

SIOS Protection Suite をインストールするためには、SIOS Protection Suite for Windows 製品とともに提供されるセットアッププログラムの実行が必要です。InstallShield ウィザードはまずはじめに LifeKeeper for Windows をインストールします。LifeKeeper のインストールが完了すると SIOS DataKeeper for Windows がインストールされます。各画面でセットアップ指示に従ってください。下記のいくつかの注意点があります。

LifeKeeper インストール時の注意事項

- LifeKeeper ソフトウェアをインストールするには、管理者権限が必要です。管理者権限のないユーザもセットアッププログラムを実行することはできますが、セットアップ時に必要な特別な権限がないので、インストールはすぐに終了してしまいます。
- LifeKeeper を共有ストレージにインストールすることはサポートされて **いません** 。各サーバのローカルディスクに個別にインストールする必要があります。
- LifeKeeper のインストールプログラムから SUperior SU のインストールが呼び出されます。
- デフォルトの LifeKeeper インストールパスは *C:\LK* です。このパスを変更することはできますが、スクリプトの問題があるため、**必ず空白を含まず、8 文字以内のパスを選択してください** 。例えば、*C:\Program Files\LK* や *C:\LifeKeeper* は無効な選択であり、アプリケーションエラーが発生します。
- LifeKeeper のインストール時に、`DisableStrictNameChecking`と `DisableLoopbackCheck` の 2 つの Windows レジストリが変更されます。どちらの変更も、別名を使用してサーバにアクセスするために必要です。

Setup Typeセットアップタイプ

Typical: LifeKeeper Core およびすべての Core リカバリキットがインストールされます (推奨)。注記: DHCP Media Sense for TCP/IP はデフォルトで無効になります。

Compact: LifeKeeper Core のみがインストールされます (Volume Recovery Kit を含む)。

Custom: LifeKeeper コンポーネントのリストから、コアファイル (必須)、IP Recovery Kit、DNS Recovery Kit、LAN Manager Recovery Kit、File Share Recovery Kit、Generic Application リカバリキット、および IIS Recovery Kit を選択してインストールできます。Customオプションでは以下の質問が表示されます。

Disable DHCP Media Sense for TCP/IP?
(DHCP Media Sense for TCP/IP を無効にしますか?)

Do you wish to start the LifeKeeper Services?

(LifeKeeper サービスを起動しますか?)

詳細は、下記の LifeKeeper サービスの起動 を参照してください。

ファイアウォール変更プロンプト (Windows 2008 以降)

ソースマシンとターゲットマシンのファイアウォールが正しく設定されていない場合、LifeKeeper は正常に動作しません。LifeKeeper のインストール時に、LifeKeeper に必要なファイアウォールの規則を設定するのに加えて、LifeKeeper に必要なその他のシステム設定を設定するかどうかの確認を求められます。インストーラによる変更を許可した場合は、手動でファイアウォールを設定する必要はありません。

LifeKeeper では、以下のポート/プロセス/プロトコルを開く、または有効にする必要があります。

TCP ポート: 81、82、1500、3278、3279

プロセス: %LKROOT%\jre1.8.0_101\bin\java.exe

プロセス: %LKROOT%\jre1.8.0_101\bin\jp2launcher.exe

プロトコル: ICMP Echo

LifeKeeperサービスの起動

Customインストールオプションを選択した場合、Do you wish to start the LifeKeeper Services?が表示されます。通常は、システム起動時に LifeKeeper が自動的に起動するようにYesを選択してください。NO を選択すると、インストール後に LifeKeeper は起動せず、LifeKeeper サービスの [スタートアップの種類] は [手動] に設定されます。

いいえを選択した場合に後から LifeKeeper サービスを起動するには、Windows の [コントロール パネル] にある [サービス] ツールを使用してください。(LifeKeeper サービスと LifeKeeper External Interfaces サービスの両方を起動する必要があります)。また、[スタートアップの種類] を [自動] に設定するには、各サービスを右クリックして [プロパティ] を選択してから、[スタートアップの種類] オプションを [自動] に変更してください。これによって、システム起動時に常に LifeKeeper が起動するようになります。

質問: LifeKeeper サービスの起動に対して Noを選択するのは、どのような場合に意味を持ちますか。

回答: ステージング環境では、LifeKeeper サービスを起動しない方が便利な場合があります。ネットワークアドレスを構成する準備ができていないときに、クラスタの最終的なインストールの前に LifeKeeper をインストールしていくつかのシステムの間でレプリケーションを行う場合です。

説明: LifeKeeper を初めて起動すると、システムのネットワーク構成情報が LifeKeeper 構成データベース (LCD) に書き込まれます。LifeKeeper を起動した後にネットワーク構成を変更した場合は、コミュニケーションパスとリソース階層を削除して再作成する必要があります。そのため、インストール時に LifeKeeper サービスを起動しないように選択することで、LifeKeeper および関連リカバリキットをインストールしてからネット

ワークを構成することができます。

DataKeeper インストールノート

LifeKeeper のインストールが完了すると、InstallShield ウィザードは SIOS DataKeeper for Windows のインストールを開始します。インストールする DataKeeper の機能を選択するよう促されます。通常のインストールでは両方の機能が含まれています。

- DataKeeper サーバコンポーネント
- DataKeeper ユーザインターフェース

DataKeeper サーバーコンポーネントのインストール時:

1. ファイアウォール設定
2. DataKeeper Service log on を選択する。

   Domain or Server account を選択すると、DataKeeper Service log on ID および Password の入力が必要となります。
3. **License Manager** からライセンスのインストール を行ってください。

サーバを再起動し、DataKeeper の使用を開始してください。DataKeeper の使用に関する情報については DataKeeper テクニカルドキュメンテーション を参照してください。

SIOS DataKeeper User Interface および Server Components の機能 は個々にインストールすることが可能で、今回インストールしなかった機能を後でインストールすることも可能です。

重要: SIOS DataKeeper User Interface の機能およびターゲットスナップショット機能を使用するためには Microsoft MMC 3.0 と Microsoft .NET Framework 3.5 SP1 が必要です。.NET Framework は www.microsoft.com/net からダウンロードすることができます。これらの正しいバージョンがインストールされる前に SIOS Protection Suite Edition のインストールが実施されるとエラーが表示されインストールが中断されることがあります。SIOS Protection Suite Edition をアンインストールし SIOS Protection Suite Edition のインストール処理を再度実施する必要があります。

LifeKeeper および DataKeeper for Windows でアンチウィルスソフトウェアを使用する場合の除外リスト

LifeKeeper と DataKeeper でアンチウィルスソフトウェアを使用する場合、以下のものをウィルスチェックの対象から除外する必要があります。

- SPS の場合: *C:\LK** ディレクトリ（または LifeKeeper がインストールされているフォルダ）
- DataKeeper の場合: *C:\Program Files (x86)\SIOS\DataKeeper\directory* (または DataKeeper がイン

ストールされているフォルダ）

- ビットマップファイルの格納場所（デフォルトの格納場所は c: ドライブですが、移動されている場合もあります – *C:\Program Files (x86)\SIOS\DataKeeper\Bitmaps*）

これらの場所にはすべての実行ファイルが含まれているため、ウィルス対策ソフトウェアによって隔離されると LifeKeeper または DataKeeper が動作不能になることがあります。

LifeKeeper と DataKeeper が使用するレジストリキーのリストはこちら にあります。

また、UpperFilters レジストリキーは次の場所にあります。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}

LifeKeeper と DataKeeper の両方を使用する場合、UpperFilters キーの内容は "NCR_LKF ExtMirr" にしてください。

7.3.3. ライセンスの取得とインストール

Video

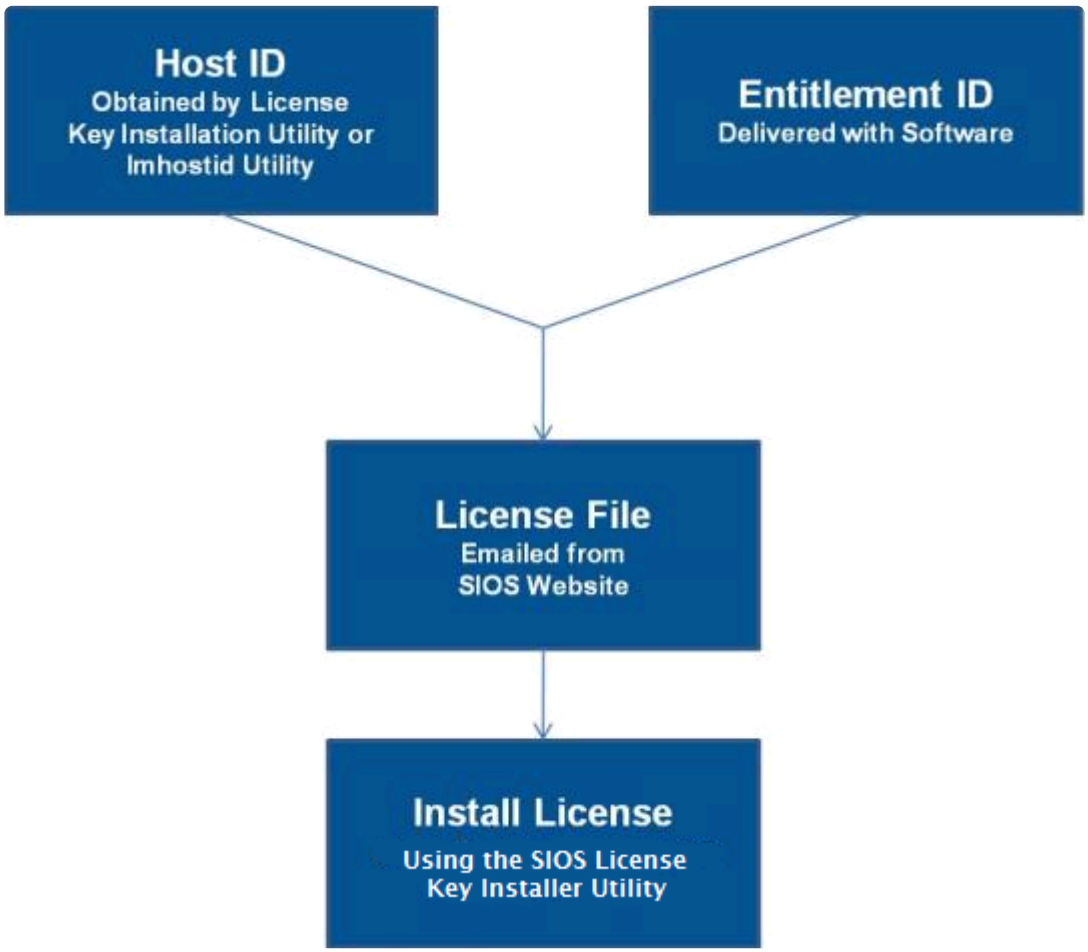
参考動画（英語）

SIOS Protection Suite ではサーバーごとに一意のライセンスが必要です。ライセンスはランタイムライセンスです。つまり、ライセンスがなくても **インストール** できますが、SIOS Protection Suite を正常に **開始** および **起動** するにはライセンスをインストールする必要があります。

インストールユーティリティー の最後の画面に、サーバーのホスト ID が表示されます。**ホスト ID** を SIOS Protection Suite ソフトウェアに付属する **Entitlement ID** (Authorization Code) とともに使用して、SIOS Protection Suite を起動するために必要なライセンスを取得してください。プロセスを以下に示します。

ライセンスキーマネージャー

SIOS Protection Suite の製品ライセンスをインストールしてから、**ライセンスキーマネージャー** を使用すると、以下の機能を実行できます。



- システムに現在インストールされているすべてのライセンスを確認する。
- 有効期限が近づいているすべてのライセンスの有効期限通知 (残り日数) を確認する。
- 現在インストールされ、無効になっているライセンスを確認する。
- インストールされているライセンスを削除する (ライセンスを右クリックして **[削除]** を選択する)。
- 期限切れのライセンスをまとめて削除する (**[期限切れライセンスを削除]** ボタンをクリックする)。
- ソフトウェアをインストールまたはアップグレードしたときに、インストール済みライセンスリストを **[更新]** する。

SIOS Protection Suite クラスタ内のサーバーごとにライセンスを取得してインストールするには、以下の手順を実行してください。

1. **ホスト ID** を取得します。SIOS Protection Suite のインストールの最後に、**ライセンスキーインストーラー** ユーティリティーに下図のように表示される **[ホスト ID]** をメモしてください。ホスト ID は、ライセンスを取得するシステム上で `%LKROOT%\bin\lmhostid` (*%LKROOT%* は LifeKeeper のインストールパス。デフォルトでは *C:\LK*) もしくは `%ExtMirrBase%\bin\lmhostid` (*%ExtMirrBase%* は DataKeeper のインストールパス。デフォルトでは *C:\Program Files (x86)\SIOS\DataKeeper*) を実行して取得することもできます (後からもう一度ホスト ID を取得する場合は、**[スタート] - [プログラム]** メニューから **ライセンスキーインストーラー** ユーティリティーを実行します。**[スタート] - [すべてのプログラム] - [SIOS] - LifeKeeper (または DataKeeper) - [ライセンスキーインストーラー]** の順にクリックします)。

2. **ホスト ID** をノートにメモするか、ファイルに保存します。ファイルに保存した場合は、そのファイルをインターネットにアクセスできるシステムにコピーしてください。それ以外の場合は、インターネットにアクセスできるシステムまでノートを持っていってください。

3. SIOS Protection Suite **Entitlement ID** (認証コード) を所有していることを確認します。ライセンスを取得するために必要な Entitlement ID が含まれた E メールをソフトウェアとともに受け取っているはずです。

4. SIOS Technology Corp. の Licensing Operations Portal からライセンスを取得します。

   a. インターネットにアクセスできるシステムを使用して SIOS Technology Corp. の Licensing Operations Portal にアクセスし、**ユーザー名** と **パスワード** を入力してログインします。(アカウントをお持ちでない場合は登録してください。)
   注記: 新規ユーザーの場合、出荷メールに記載されている資格情報　ID　を入力してください。

   b. **[Activation and Entitlements]** ドロップダウンから、**[List Entitlements]** を選択します。

   c. ライセンスを取得したい製品の左側にあるチェックボックスにチェックを入れます。

   d. **[Action]** ドロップダウンから **[Activate]** を選択し、必要な情報 (システムの HOSTNAME など) を入力して **[Next]** を選択します。

   e. **[Gray Plus Sign]** をクリックして定義済みのホストを選択するか、**[Green Plus Sign]** を選択して新し

いホストを作成します。

f. **[Node Locked Host]** の選択肢に **[ANY]** が表示されている場合には **[ANY]** を選択して **[OK]** をクリックしてください。**[ANY]** が表示されていない場合には **[ETHERNET MAC ADDRESS]** を選択し、ホストID（MACアドレス）を入力して **[OK]** をクリックし、次に **[Generate]** をクリックします。

> **注記:** hostid / mac アドレスは 12文字で、スペース、コロン、ダッシュ、フィールド区切り文字は使用できません。

g. **[Fulfillment ID]** の左側のボックスをオンにして、**[Complete]** を選択します。

h. **[License Support]** ドロップダウンから **[List Licenses]** を選択します。**[Fulfillment ID]** の左側のボックスをオンにして、**[View]** ドロップダウンから **[Send]** を選択します。

i. ライセンス送信先の有効な E メールアドレスを入力して、**[Send]** を選択します。

j. E メールを受信します。

k. ファイルを該当するシステムにコピーします。

5. ライセンスをインストールします。ライセンスをインストールするには、以下のいずれかの方法で行ってください。

- 各システム上で、ライセンスキーをC:\Windows\SysWOW64\LKLicense フォルダにコピーします。

または

- 各システム上で、**[スタート] - [プログラム]** メニューから **ライセンスキーインストーラー** を実行します（**[スタート] - [すべてのプログラム] - [SIOS] - [LifeKeeper] - [ライセンスキーインストーラー]**）の順にクリックします)。
- **ライセンスキーインストーラー** のメイン画面で **[ライセンスファイルをインストール...]** ボタンをクリックします。
- 上記の **手順 4** で保存したライセンスファイルの位置を参照します。
- ライセンスファイルの名前をクリックします。ファイルがハイライト表示されます。
- ダイアログボックスでファイル名の下に表示される **[ライセンスファイルをインストール...]** ボタンをクリックします。ライセンス検出確認ポップアップが表示されます。
  もしくは

    ライセンスファイルを該当するディレクトリに手動でコピーする。

各システム上で、*%windir%\SysWOW64\LKLicense* (*windir* は Windows のインストールパス。デフォルトでは *C:\Windows*) にライセンスファイルをコピーします。_LKLicense_ ディレクトリが存在しない場合は、ファイルをコピーする前に作成する必要があります。**注記** : ライセンスを有効にした日付を識別できるように、ファイル名を *YYYYMMDD.lic* 形式に変更することを推奨します。

6. その他のサーバーについて、上記の手順を繰り返します。他の SIOS Protection Suite サーバー上では、サーバーごとに一意のホスト ID を使用してライセンスをインストールする必要があります。

7. DataKeeper クラスターエディションを再起動します。

プライマリーネットワークインターフェースを変更すると、ライセンスの Rehost が必要になる場合がある

License Key Installer utility で使用されるホスト ID は、SIOS Protection Suite サーバーのプライマリーネットワークインターフェースカード (NIC) から取得されます。SIOS Protection Suite は、起動されるたびに有効なライセンスを確認します。将来、SIOS Protection Suite サーバーの NIC を交換してホスト ID が変わった場合は、次に LifeKeeper もしくは DataKeeper を停止したとき、再起動する前にライセンスの Rehost を実行する必要があります。SIOS Technology Corp. の Licensing Operations Portal にログインして、画面上メニューを **[License Support]** ＞ **[List Licenses]** とクリックして画面遷移させた後、目的のライセンスを選択して **[Action]** ＞ **[Rehost]** の順に選択し、Rehost を実行してください (**注記**: 製品サポートへのご連絡なしにお客様ご自身で Rehost を行うことができるのは 6 か月に 1 回です。)

サブスクリプションライセンス

サブスクリプションライセンスは、更新機能がある期間限定ライセンスです。評価ライセンスと同様に、更新しないと一定の時間で期限切れになります。この更新プロセスが自動的に実行されるように設定するには、以下の手順に従ってください。

1. 次のサブスクリプションライセンスプログラムをインストールします。

   `%LKROOT%\bin\lmSubscribe.exe` もしくは

   %ExtMirrBase%\lmSubscribe.exe

2. (**SIOS Technology Corp. カスタマ登録** から) **[ユーザー ID]** と **[パスワード]** を入力します。これらの証明書は暗号化されたファイルに保存されます。
3. **[OK]** を選択します。

上記の手順が正常に実行されると、サブスクリプション更新サービスがバックグラウンドで実行され、更新ステータスを定期的にチェックします。ライセンスが一定の日数 (90、60、30、20、10、5、4、3、2、1) で期限切れになることが検出されると、警告通知が **Windows イベントビューアー** に送信され、ライセンスを更新しようとします。新しいアクティベーションライセンスが利用できる (このシステムの資格に対して新しいアクティベーションを購入した) 場合は自動的に履行され、古いライセンスに代わって新しいライセンスがシステムにインストールされます。このシステムのライセンスが更新されている (アクティベーションを購入している) 限り、ユーザーが操作しなくてもサービスによってシ

ステム上のライセンスがアップグレードされます。

トラブルシューティング

エラーが発生した場合は、サポートに連絡する前に以下の方法を試してください。

- **Windows イベントビューアー** でエラーメッセージを確認してください。

7.3.4. LifeKeeper for Windows ローカライズ言語サプリメントのインストール

LifeKeeper for Windows ローカライズ言語サプリメントを使用すると、ローカライズされた環境で LifeKeeper を実行することができます。各ローカライズ言語サプリメントには、翻訳された LifeKeeper GUI テキスト文字列とローカライズ言語によるコンテキスト依存ヘルプが含まれています。LifeKeeper v7.2.1 以降では、日本語の言語サプリメントが利用できます。SIOS Protection Suite for Windows Core インストールプログラムによって、必要なバージョンの JRE がインストールされます。

日本語ローカライズ言語サプリメントには、LifeKeeper および DataKeeper の各製品を含む SIOS Protection Suite の言語コンテンツが含まれています。管理者は更新する製品を選択できます。また、完全にローカライズされた OS がインストールされている場合を除いて、DataKeeper MMC ベース GUI を使用するには Windows 言語パックをインストールする必要があります。

LifeKeeper for Windows ローカライズ言語サプリメントは、SIOS Protection Suite Core と同様に InstallShield を使用してインストールします。インストール時に [標準]、[コンパクト]、または [カスタム] のオプションを選択する必要はありません。LifeKeeper for Windows ローカライズ言語サプリメントをインストールするには、ローカライズ言語サプリメント製品に付属しているセットアッププログラムを実行してください。

インストール済みの LifeKeeper for Windows ローカライズ言語サプリメントを修復するには、セットアッププログラムを実行して、InstallShield オプションのリストから **[修復]** を選択してください。

LifeKeeper for Windows ローカライズ言語サプリメントを削除するには、Windows の **[コントロール パネル]** から **[プログラムの追加と削除]** を実行してください。LifeKeeper Core 製品を削除する前にローカライズ言語サプリメントを削除する必要があります。

7.3.5. SIOS Protection Suite の サイレントインストール

注記:SIOS Protection Suite for Windows をサイレントインストールするには、サポート から別々になった LifeKeeper と DataKeeper のインストールファイルを入手する必要があります。

`-silent` コマンドオプションを使用して SIOS Protection Suite for Windows をインストールすることができます。このオプションは、ウィザードおよびランチャーユーザインターフェース (UI) を使用しないので「サイレントインストール」と呼ばれています。サイレントインストールは情報を表示なしに、もしくはユーザーとの対話なしにインストールを実行する方法です。「 *オプション* 」ファイルとしても知られている **レスポンスファイル** はインストールコマンドを渡すために 使用します。通常はコマンドラインでダイアログに対しレスポンスを表示する場合および/もしくはプロパティもしくは変数の値を設定するためにオプションを指定します。**レスポンス/オプション** ファイルで指定したオプションは、コマンドラインで実行のオプションが入力された後実行されます。

LifeKeeper レスポンスファイル

LifeKeeper に対してレスポンスファイルを作成する場合は、コマンドウィンドウを開き、**LK-{version}-Setup.exe /r /f1C:\setup.iss** コマンドを使用して LifeKeeper セットアッププログラムを実行してください。ダイアログへ入力されたレスポンスは *setup.iss* ファイルへ記録されます。

作成したレスポンスファイルを使用してサイレントインストールを実行するためには、コマンドウィンドウを開き、以下のコマンドを使用して *LifeKeeper セットアッププログラム*を実行してください。

```
LK-{version}-Setup.exe /s /f1C:\setup.iss /f2C:\setup.log
```

DataKeeper レスポンスファイル

DataKeeper に対してレスポンスファイルを作成する場合は、コマンドウィンドウを開き、以下のコマンドを使用してして **SIOS DataKeeper セットアッププログラム** を実行してください。

```
DK-{version}-Setup.exe /r /f1C:\setup.iss
```

ダイアログへ入力されたレスポンスは *setup.iss* ファイルへ記録されます。

注記: 最初の *setup.iss* ファイルを作成する際にローカルユーザサーバアカウントが DataKeeper サービスに対して使用されている場合は、別サーバで使用するために *setup.iss* ファイルを編集する必要があります。メモ帳で *setup.iss* ファイルを開き、*szName* のサーバ名を変更してください(*szName=\Administrator*)。すべてのインストールにおいて **Local Service account** または **Domain account** を使用する際は *setup.iss* ファイルを変更する必要はありません。

作成したレスポンスファイルを使用してサイレントインストールを実行するためには、コマンドウィンドウを開き、以下のコマンドを使用して **SIOS DataKeeper セットアッププログラム** を実行してください。

```
DK-{version}-Setup.exe /s /f1C:\setup.iss /f2C:\setup.log
```

サイレントインストールからの結果は *setup.log* へ記録されます。"ResultCode=0" はインストールが正常に完了したことを表しています。

SIOS Protection Suite のインストールが完了次第、ライセンスキーをC:\Windows\SysWOW64\LKLicenseフォルダにコピーするか、**[スタート] - [プログラム]** メニューから **License Key Installer** ユーティリティを実行してください。

```
スタート->すべてのプログラム->SIOS->DataKeeper->License Key Installer。
```

サーバを再起動します。

7.3.6. サードパーティ製品のファイル

以下のサードパーティのファイルは SIOS Technology Corp. が開発したものではありませんが、SIOS Protection Suite/DataKeeper のインストールプロセスでインストールされます。

パスおよびファイル名	提供元	用途
<datakeeper dir>/lmdiag.exe <datakeeper dir>/lmhostid.exe <datakeeper dir>/lminstall.exe <datakeeper dir>/motdk_libFNP.dll	Flexera	ライセンス管理
<datakeeper dir>/SnapIn/IronPython.dll (.Net python 言語実装) <datakeeper dir>/SnapIn/IronPython.Modules.dll (.Net python モジュール)	github.com/IronLanguages/ironpython2 (Microsoft オープンソース)	テスト/デバッグ
<datakeeper dir>/SnapIn/J832.Common.dll <datakeeper dir>/SnapIn/J832.Wpf.BagOTricksLib.dll	Kevin Moore、http://j832.com/bagotricks/	WPF 開発用ユーティリティ/コントロール
<datakeeper dir>/SnapIn/log4net.dll (.Net ロギングライブラリ)	Apache Software Foundation	アプリケーションロギング
<datakeeper dir>/SnapIn/Microsoft.Scripting.Core.dll <datakeeper dir>/SnapIn/Microsoft.Scripting.dll	github.com/IronLanguages/ironpython2 (IronPython の一部)	
<datakeeper dir>/SnapIn/MMCFxCommon.dll <datakeeper dir>/SnapIn/microsoft.managementconsole.dll	Microsoft	MMC 管理対象スナップインライブラリ
<datakeeper dir>/VSSHelper/AlphaVSS-license.txt <datakeeper dir>/VSSHelper/AlphaVSS.Common.dll <datakeeper dir>/VSSHelper/AlphaVSS.Common.xml <datakeeper dir>/VSSHelper/AlphaVSS.x64.dll <datakeeper dir>/VSSHelper/log4net.dll <datakeeper dir>/VSSHelper/log4net.xml <datakeeper dir>/VSSHelper/cfg/log4net.Config.xml	Pete Palotas、github.com/alphaleonis/AlphaVSS	Alpha VSS 提供元
注記: デフォルトでは、<DK InstallPath> は C:\Program Files (x86)\SIOS\DataKeeper です。		

7.3.7. アプリケーションディレクトリの例外事項

以下のファイルは、DataKeeper のインストール手順で選択したデフォルトのディレクトリではないディレクトリにインストールされます。この例外は、オペレーティングシステムに パフォーマンスモニタカウンタ を設定した場合に発生します。

パスおよびファイル名	用途
/inf/ExtMirr/ExtMirrCounters.h:	パフォーマンスモニタリング。このファイルにはカウンタ名と定義が含まれます。

7.3.8. SIOS Protection Suite for Windows のアンインストール

LifeKeeper を削除する前に

LifeKeeper ソフトウェアを削除するにあたって以下の事項が必要となります。

1. **アプリケーションの移動もしくは停止。ソフトウェアを削除する前に、SIOS Protection Suite の保護が必要なアプリケーションがサーバ上にないことを確認してください。** アプリケーションリソースが In Service 中のアプリケーションが存在するサーバ上から LifeKeeper を削除しないでください。LifeKeeper を削除すると、イクイバレンシ、リソース階層の定義およびログファイルのような設定データがすべて削除されます。追加情報についてはリソース階層の移動 を参照してください。

2. **LifeKeeper が実行中である。** LifeKeeper Recovery Kit ソフトウェアを削除する場合、LifeKeeper が動作している必要があります。**サービス MMC** スナップインを使用して LifeKeeper サービスが実行中であることを確認します。LifeKeeper が実行中でない場合、クラスタ内の別の SIOS Protection Suite サーバからリソースインスタンスを削除できず、サーバに一貫性がない状態になります。

3. **リソース階層の削除。** LifeKeeper を削除するサーバからリソース階層を拡張もしくは削除してください。リソース階層がサービス中のサーバからは、絶対に Recovery Kit を削除しないでください。現在のリソース階層が壊され、Recovery Kit の再インストール時に再作成しなければならなくなります。

4. **全パッケージの削除。** LifeKeeper core を削除する場合は、最初に LifeKeeper に依存する別のパッケージを削除してください。例: SIOS Protection Suite リカバリキット。SIOS Protection Suite リカバリキットを削除する前に、関連するアプリケーションリソース階層を削除することを推奨します。

DataKeeper を削除する前に

DataKeeper のアンインストールおよび前バージョンの再インストールを実施する際は、アンインストール前に各ノードですべてのジョブ/ミラーを削除する必要があります。ソフトウェアを再インストールした時点でジョブ/ミラーを再作成する必要があります。

SIOS Protection Suite のアンインストール

- **Windows のコントロールパネル** で、インストールされたプログラムのリストから、**SIOS DataKeeper** もしくは **LifeKeeper** を選択してください。
- **アンインストール** を選択してください。

アンインストール処理が完了した時点で、再起動が必要となります。

注記: アンインストール時には自動的に SIOS DataKeeper および/または LifeKeeper サービスが停止され、レジストリエントリがクリアされます。

削除が完了しても以下のファイル群はアンインストール時に削除されません。

パスおよびファイル名	定義および特別な考慮事項
<windows dir>/SysWOW64)/LKLicense	SIOS Technology Corp. 製品の共通のライセンスファイルディレクトリです。ライセンスファイルがインストールされる場所で、複数の SIOS Technology Corp. 製品のライセンスが毎回このパスにインストールされます。インストール済みのライセンスを残しておくため、アンインストール時にこのパスは削除されません。 手動で削除することが安全ですが、そのソフトウェアを後で再インストールすることになった場合、ライセンスも同じく再インストールする必要があります。
<windows dir>/SysWOW64)/PerfStringBackup.ini	新しいパフォーマンスモニタカウンタがインストールされる時 Windows により作成されるバックアップファイルです。perfmon カウンタをインストールする際に作成されます。 このファイルは、Windows 自身により作成されるファイルなので、単体で残ります。
<windows dir>/inf/ExtMirr/0011/ExtMirrCounters.ini	このファイルは、DataKeeper パフォーマンスモニタカウンタ を記述しています。このファイルは削除またはそのまま残しておくことも可能です。これは実行ファイルではありません。

注記

- **重要**: SIOS Protection Suite ソフトウェアのアンインストールには Microsoft Visual C++ 2008 Redistributable package のインストールが必要となります。このパッケージは SIOS Protection Suite がアンインストールされるまで削除しないでください。
- SIOS Protection Suite セットアッププログラムから **[Modify]** または **[Repair]** を実行してください。
- LifeKeeper の削除では SUperior SU は削除されません。SUperior SU は **Add/Remove Programs** で個別に削除することが可能です。
- SIOS Protection Suite の削除では SIOS Protection Suite ディレクトリは削除されません。そのディレクトリは **Add/Remove Programs** 処理が完了した後、手動で削除することが可能です。
- SIOS Protection Suite を完全に削除するためにはシステムの再起動が必要となります。

7.3.9. SIOS Protection Suite のアップグレード

以下の手順を使用すると旧バージョンの SIOS Protection Suite for Windows からリソース階層およびミラーを保持したままアップグレードすることができます。

アップグレード手順

以下のシナリオでは、LifeKeeper と SIOS DataKeeper の両方をアップグレードする場合のプロセスを説明します。最初に LifeKeeper をアップグレードしてから SIOS DataKeeper をアップグレードしてください。アップグレードプロセスの間、LifeKeeper サービスと SIOS DataKeeper サービスは停止します。LifeKeeper と SIOS DataKeeper の両方をアップグレードした後にシステムの再起動が必要になります。

2 つのシステム (Sys1 および Sys2) があり、Sys1 がプライマリ (アクティブ) サーバであるとします。以下の手順に従って、LifeKeeper および SIOS DataKeeper をアップグレードしてください。

バックアップサーバのアップグレード

1. バックアップサーバ `Sys2` で LifeKeeper GUI と SIOS DataKeeper GUI を終了します。

2. コマンドウィンドウを開き、$LKROOT\bin\lkstop (`$LKROOT` は SIOS Protection Suite のインストールパス。デフォルトは `C:\LK`) を入力し、すべての LifeKeeper サービスを停止します。“ `LIFEKEEPER NOW STOPPED` ” というメッセージを確認してから次へ進んでください。

3. セットアッププログラムを実行し、バックアップサーバ `Sys2` の LifeKeeper for Windows をアップグレードしてください。**[はい]** をクリックして、LifeKeeper のアップグレードを続行します。

4. LifeKeeper をインストールすると、既存の LifeKeeper のファイルが上書きされます。SIOS DataKeeperをアップグレードするまでサーバーを再起動しないでください。

5. セットアッププログラムを実行し、バックアップサーバ `Sys2` の SIOS DataKeeper for Windows をアップグレードしてください。**はい** をクリックして SIOS DataKeeper のアップグレードを続行してください。(必要に応じて) **ライセンスマネージャ** ユーティリティを使用して新しい DataKeeper をインストールしてください。SIOS Data Replication のライセンスを使用して SIOS DataKeeper を起動させることはできません。

6. 言語サプリメントパッケージ およびオプションのリカバリキットをアップグレードする必要がある場合は、この時点で該当するインストールプログラムを実行します。

7. バックアップサーバ `Sys2` を再起動します。

クラスタ内に別のバックアップサーバがある場合は、サーバごとに上記の手順を実行してください。

注記: SIOS Protection Suite の新しいバージョンでは、インストールパッケージの代わりに SIOS テクニカルドキュメンテーションへのリンクが含まれています。オンラインプロダクトマニュアルが含まれている製品からアップグレードするときに、古いオンラインプロダクトマニュアルはアンインストールされません。これらのファイルを削除したい場合

は、手動で OLPM パッケージをアンインストールする必要があります。

プライマリサーバのアップグレード

8. バックアップサーバが再起動されるとミラーが再同期され、**[ミラーリング]** 状態に戻ります。

9. スイッチオーバを実行してください。`Sys2` でアクティブなリソース階層が In Service され、プライマリサーバ `Sys1` をアップグレードするためミラーが逆方向に実施されます。

10. 上記手順をプライマリサーバ `Sys1` で実施してください。LifeKeeper GUI と SIOS DataKeeper GUI を終了してください。

11. コマンドウィンドウを開き、`$LKROOT\bin\lkstop` (*`$LKROOT`* は LifeKeeper のインストールパス。デフォルトは `C:\LK`) を入力し、すべての LifeKeeper サービスを停止します。“ `LIFEKEEPER NOW STOPPED` ” というメッセージを確認してから次へ進んでください。

12. セットアッププログラムを実行し、プライマリサーバ `Sys1` の LifeKeeper for Windows をアップグレードしてください。**[はい]** をクリックして、LifeKeeper のアップグレードを続行します。

13. LifeKeeper をインストールすると、既存の LifeKeeper のファイルが上書きされます。SIOS DataKeeperをアップグレードするまでサーバーを再起動しないでください。

14. セットアッププログラムを実行し、プライマリサーバ `Sys1` の SIOS DataKeeper for Windows をアップグレードしてください。**はい** をクリックして SIOS DataKeeper のアップグレードを続行してください。(必要に応じて) **ライセンスマネージャ** ユーティリティを使用して新しい DataKeeper をインストールしてください。SIOS Data Replication のライセンスを使用して SIOS DataKeeper を起動させることはできません。

15. 言語サプリメントパッケージ およびオプションのリカバリキットをアップグレードする必要がある場合は、この時点で該当するインストールプログラムを実行します。

16. プライマリサーバ `Sys1` を再起動してください。

17. **[スタート]** 、**[プログラム]** 、**[LifeKeeper]** 、**[LifeKeeper GUI]** の順にクリックして `Sys1` の LifeKeeper GUI を起動し、`Sys1` にログインしてください。

SIOS Data Replication v6.2x から DataKeeper へのアップグレード

DataKeeper は "ジョブ" と呼ばれる新しい構造に組み込まれているので、SIOS Data Replication から DataKeeper へアップグレードを行う際に、DataKeeper へアップグレードする前に既存のミラーを削除し、アップグレード完了時にそれらを再作成する必要があります。その操作により DataKeeper に対して正常にジョブとミラー情報を設定することができます。

DataKeeper はライセンスの更新もまた必要になるのでライセンスマネージャが表示されたら新しい DataKeeper

用のライセンスをインストールする必要があります。この時点で古い SDR v6.2x のライセンスを削除することを推奨します。

以下の 2 つを除いては、上記アップグレード手順とまったく同じです。

アップグレード手順

1. SIOS Data Replication UI で、**すべての既存のミラーを削除してください** 。
2. 起動中の SIOS DataKeeper Replication UI があれば閉じてください。
3. 上記のアップグレード手順を実行し **各サーバに新しいライセンスを適用してください** 。
4. DataKeeper UI を起動し、ミラーを再作成してください。

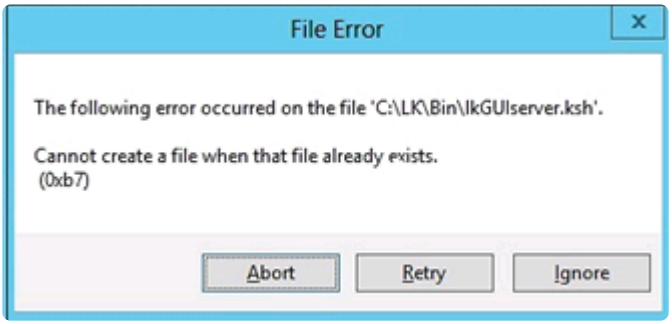
SIOS Protection Suite の再インストール

SIOS Protection Suite を再インストールするためには、上記と同じ手順を実施してください。セットアップが InstallShield オプションのリストを表示したら、**Repair** を選択してください。

7.3.10. 修復

インストールプロセスでは、SIOS Protection Suite ソフトウェアを修復することもできます。インストール済みのソフトウェアを誤って削除した場合や、部分的に修正された場合には、このオプションを使用してください。このオプションを使用すると、すべてのファイルがセットアップフォルダからコピーされ、システムの再起動を求められます。

注記: 修復時にエラーが発生する可能性があり、特に Windows 2012 でエラーが確認されています。エラーが発生した場合は、操作をやり直してください。



Windows のコントロールパネルで SIOS Protection Suite を修復する

- Windowsの **[コントロールパネル]** の **[プログラムと機能]** から、SIOS DataKeeper または LifeKeeper を選択します。
- **[修復]** を選択します。

アンインストールが完了したら、システムを再起動する必要があります。

7.3.11. LifeKeeper の起動

標準インストールでは、サーバ起動時に LifeKeeper が自動的に起動します。アプリケーションは保護された状態で起動します。

LifeKeeper の起動時に、LifeKeeper GUI サーバも起動します。LifeKeeper GUI クライアントは、Web ブラウザから起動するか、または ***[スタート] -> [すべてのプログラム] ->[SIOS]-> [LifeKeeper] -> [LifeKeeper (Admin Only)*** の順にクリックして起動します。詳細については、SIOS Protection Suite for Windows テクニカルドキュメンテーション の LifeKeeper GUI セクションを参照してください。

LifeKeeper プロセスの起動と停止

LifeKeeper はサーバを起動すると自動的に稼働します。そのため、通常は LifeKeeper を手動で起動/停止する必要はありません。LifeKeeper を手動で起動/停止する必要がある場合には、以下のいずれかの方法で行ってください。

サービス MMC スナップイン

管理タスク の*サービス MMC* スナップインを使用して LifeKeeper サービスを起動/停止することができます。

LifeKeeper には、次の 2 つのサービスがあります。

- LifeKeeper
- LifeKeeper External Interfaces

2 つのサービスは、同時に起動/停止する必要があります。ただし、LifeKeeper External Interfaces は LifeKeeper サービスに依存するため、LifeKeeper External Interfaces を停止すると、LifeKeeper サービスも停止します。そのため、LifeKeeper External Interfaces は、LifeKeeper サービスの前に起動する必要があります。

コマンドライン

LifeKeeper を停止する場合、いくつかの関連サービスも停止する必要があります。このプロセスには数秒かかる場合がありますが、すべてのサービスが停止しても [サービス] ツールには正確に反映されません。コマンドラインを使用して `$LKROOT\bin\lkstop` と入力すると、停止しようとしているサービスが表示されます。完了すると、確認のために “ `LIFEKEEPER NOW STOPPED` ” というメッセージが表示されます。

> **注意**: LifeKeeper を停止すると、保護対象のすべての階層のサービスが停止します。そのため、保護対象のアプリケーションにアクセスできなくなります。

8. SIOS Protection Suite for Windows テクニカルドキュメンテーション

8.1. SIOS Protection Suite for Windows について

SIOS Protection Suite for Windows について

SIOS Protection Suite (SPS) for Windows は、高可用性クラスタリングおよびデータ複製機能 を統合し、ミッションクリティカルなデータおよびアプリケーションを保護します。さらに SIOS Protection Suite は SQL サーバ、Oracle 製品などのアプリケーションに対応するエージェント機能を提供する SIOS のアプリケーションリカバリキットも備えているので、より正確な情報を使用して復旧することができます。

SIOS Protection Suite for Windows に統合されているコンポーネント

LifeKeeper for Windows は、データ、アプリケーション、通信リソースの高可用性を実現する耐障害ソフトウェアです。LifeKeeper では専用の耐障害ハードウェアは不要です。複数のシステムをグループ化して、サイト構成情報を定義するだけで動作します。クラスタを構築すると、LifeKeeper は障害を自動的に検出して回復します。

障害が発生すると、LifeKeeper は保護対象リソースをバックアップシステムに移動します。フェイルオーバの際、システムはわずかに中断しますが、フェイルオーバリカバリが完了すると、LifeKeeper はバックアップシステムでリソースを自動的に復元します。

SIOS DataKeeper は、最適化されたホストベースのレプリケーションソリューションであり、ソースサーバからネットワーク経由で 1 台以上のターゲットサーバに可能な限り高速かつ効率的にデータを複製します。

オプションの Microsoft SQL Server Recovery Kit を使用すると、SQL サーバの状態を詳しく知ることができます。システムがただ起動しているかどうかだけでなく、正常に応答しているかどうかを確認することができます。

保護対象リソース

SIOS Protection Suite 製品ファミリには、多様なシステムリソースをフェイルオーバにより保護するソフトウェアが用意されています。以下の図に、SIOS Protection Suite の柔軟性と共に、自動リカバリを指定できるリソースタイプを示します。

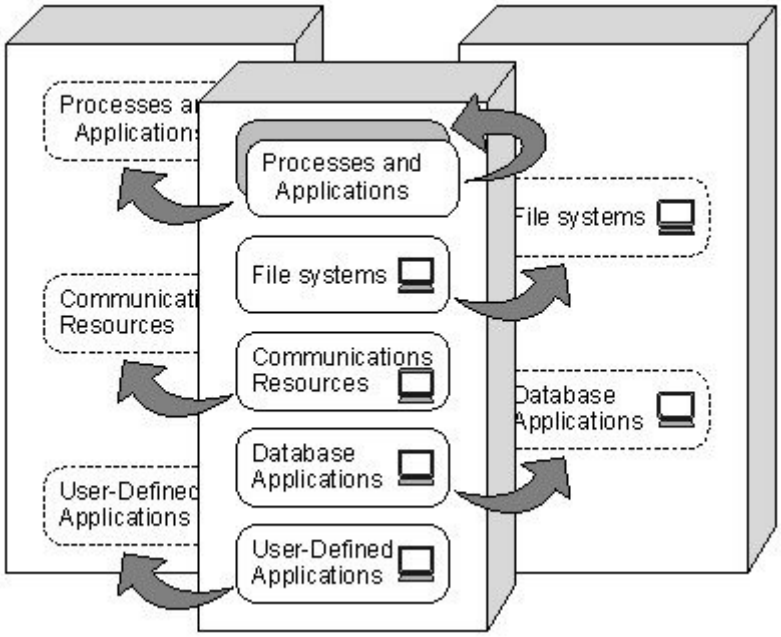
- **ボリューム:** LifeKeeper のボリュームリソースタイプを使用すると、SIOS Protection Suiteの階層にデータやアプリケーションを含むディスクボリュームのリソースを作成することで、共有 SCSI 周辺機器または複製ボリューム上にあるデータとアプリケーションを保護できます。

- **ファイル共有:** SIOS Protection Suite のファイル共有リソースは、共有ドライブ上の指定したフォルダとディレクトリを保護します。

- **コンピュータの別名:** SIOS Protection Suite の　LAN Manager Recovery Kit は、NetBEUI 経由でサーバと通信するアプリケーションのコンピュータ別名を自動的にフェイルオーバします。

- **通信リソース:**
    - SIOS Protection Suite の IP Recovery Kit を使用して、IP アドレスのスイッチオーバが可能なリソースを作成できます。
    - SIOS Protection Suite の　DNS Recovery Kit は、DNS の A レコードと PTR レコードを更新します。
- **データベースアプリケーション:** SIOS Protection Suite には、Microsoft SQL Server 用のオプションのリカバリキットがあります。
- **Generic Applications:** SIOS Protection Suite の　Generic Application Recovery Kit は、専用のリカバリキットがないアプリケーションのリソースを作成します。

SIOS Protection Suite は、さまざまなリソースタイプについて、N 方向のリカバリをサポートします。N 方向のリカバリでは、複数のリソースを複数のクラスタサーバにフェイルオーバできます。



SIOS Protection Suite の Core コンポーネントについては SIOS Protection Suite Core ソフトウェア を参照してください。

Core

MSSQL

コミュニケーションパス

コミュニケーションパスの種類

ハートビート

ハートビート間隔

セーフティチェック

リソース階層

階層の関係

リソース階層情報

リソースのステータス

共有イクイバレンシ

8.1.1. SIOS Protection Suite Core ソフトウェア

SIOS Protection Suite for Windows Core は、LifeKeeper と基本的な LifeKeeper ソフトウェアパッケージ、DataKeeperとリカバリキットを含んでいます。

- **LifeKeeper** - LifeKeeper for Windows core は基本的な LifeKeeper ソフトウェアパッケージと　Core リカバリキットを含んでいます。

  • **LifeKeeper 構成データベース (LCD)** - LifeKeeper が保護するリソースに関する情報が格納されています。リソースインスタンス、依存関係、共有イクイバレンシ、リカバリ方向、LifeKeeper 操作フラグなどの情報が格納されています。LCD データはシステムの共有メモリにキャッシュされた後、ファイルに格納されるため、システムを再起動しても、設定データは保持されます。

  • **LCD インターフェース (LCDI)** - 構成データベース (LCD) にクエリを発行し、LCD 内のデータを取得して変更できます。LCDI はアプリケーションリカバリキット (ARK) で起動し、リソース状態や各種情報を取得します。

  • **LifeKeeper 通信マネージャ(LCM)** -クラスタサーバのステータスを確認します。LifeKeeper によるプロセス間通信 (ローカルとリモート) にも使用できます。クラスタサーバのすべてのコミュニケーションパスで LCM 通信が停止すると、LifeKeeper はサーバに障害が発生したと判断します。

  • **LifeKeeper アラームインターフェース** -イベントをトリガするための基盤を提供します。LifeKeeper で保護するリソースに障害が発生すると、アプリケーションのデーモンが sendevent プログラムを呼び出します。sendevent プログラムは LCD と通信を行い、リカバリに使用できるスクリプトがあるかどうかを判断します。

  • **LifeKeeper リカバリアクション制御インターフェース(LRACI)** - リソースに実行する適切なリカバリスクリプトを決定し、適切な restore/remove スクリプトを起動します。

  • **LifeKeeper GUI** - クライアント / サーバアプリケーションです。LifeKeeper と設定データを操作するグラフィカルな管理インターフェースを提供します。LifeKeeper GUI クライアントには、スタンドアロンのアプリケーションと Web ブラウザから起動する Java アプレットがあります。

- **DataKeeper** - DataKeeper パッケージはリアルタイムのデータレプリケーション機能を装備し、複数サーバおよびデータセンターにある Windows サーバのデータを同期した状態に維持します。

SIOS Protection Suite Core Recovery Kit

Core リカバリキットは、障害検出とリカバリのあらゆるしくみを提供します。また、ボリューム (ドライブ文字)、ファイル共有、通信リソース、および Microsoft Internet Information Server を SIOS Protection Suite で保護するために必要な定義を提供します。

- **Volume Recovery Kit** - リソースを作成して、共有ドライブまたはミラー化したドライブ全体 (例: K: ドライブ) を保護します。
- **LAN Manager Recovery Kit** - コンピュータの別名と Windows ファイル共有リストを自動的にリカバリし

ます。LAN Manager リソースでは、NetBEUI 経由でサーバと通信するアプリケーションの「切り替え可能」なコンピュータ名やシステム名を作成できます。また、ファイル共有リカバリコンポーネントを含みます。

- **IP Recovery Kit** - SIOS Protection Suite 環境で、障害が発生したプライマリサーバから 1 台以上のバックアップサーバに「切り替え可能」な IP アドレスを使用して、IP アドレスを復旧します。切り替え可能な IP アドレスとは、サーバ間で切り替える仮想 IP アドレスを指します。ネットワークインターフェースカードの実アドレスとは異なります。SIOS Protection Suite で保護するアプリケーションには、切り替え可能な IP アドレスが対応付けられます。プライマリサーバに障害が発生すると、この IP アドレスがバックアップサーバに対応付けられます。IP Recovery Kit は IP リソースのローカルリカバリ機能も提供します。
- **DNS Recovery Kit** - DNS プライマリサーバまたは別名のサーバにある A レコードと PTR レコードを更新します。DNS リソースを使用した場合、バックアップサーバへのフェイルオーバやスイッチオーバが発生すると、プライマリサーバまたは別名サーバの A レコードと PTR レコード (存在する場合) が、バックアップサーバの IP アドレスで更新されます。
- **Microsoft IIS Recovery Kit** - Microsoft Internet Information Services (IIS) の Web、FTP、SMTP サービスを保護します。Web サーバの稼働状態を継続的に監視し、問題を検出すると、障害が発生した Web サーバをバックアップサーバに自動的にフェイルオーバします。
- **Generic Application Recovery Kit** - 専用のリカバリキットがないアプリケーションのリソースを作成します。

8.1.2. SIOS Protection Suite Microsoft SQL Server Recovery Kit

SIOS Protection Suite Microsoft SQL Server Application Recovery Kit は、SIOS Protection Suite が Microsoft SQL ベースのデータベースアプリケーションを管理、制御するためのツールとユーティリティを含んでいます。インストールされると、SIOS Protection Suite はアプリケーションの状態を監視したり、アプリケーションに障害が発生した場合自動的に復旧させることが可能になります。SIOS Protection Suite Recovery Kit は SIOS Protection Suite で保護するための特別な制約やアプリケーションに対する変更を必要としません。

> Microsoft によると、SQL Server failover cluster インスタンス (FCI) では、クラスターノードをドメイン参加させる必要があります。この制約により、SIOS Protection Suite for Windows は、ワークグループ環境でMicrosoft SQL Server Failover Cluster インスタンスを保護するために使用することができません。

このキットはMicrosoft SQL Server インスタンスの自動スイッチオーバに対してリソースのメニュー選択方式を提供します。簡単にリソース階層を作成できるので、リカバリ処理はSQL Serverが使用する名前付きパイプもしくはIP ソケットリソースのようなデータベースへのアクセスに使用するすべてのディスクリソースを組み込むことができます。

詳細情報については Microsoft SQL Server Recovery Kit テクニカルドキュメンテーション を参照してください。

注記: 製品要件および FAQ 情報についてはOS指定のリリースノートで確認することができます。

8.1.3. コミュニケーションパスの概要

SIOS Protection Suite はリソースの稼働状態を監視し、サーバ間に設定したコミュニケーションパスを使用してフェイルオーバを実行します。SIOS Protection Suite の障害検出機能とリソースリカバリ機能を利用するには、サーバ間の通信をアクティブに保つことが重要です。そのためには、異なるプロトコルを使用して複数のコミュニケーションパスを定義し、通信回線の障害に起因するシステムのフェイルオーバを回避する必要があります。

SIOS Protection Suite でリソースやリソース階層を定義するには、各サーバにコミュニケーションパスを定義しておく必要があります。SIOS Protection Suite は定義したコミュニケーションパスを介して、ノード間のリソース定義と状態を調整し、障害の検出とリカバリを実行します。

コミュニケーションパスの種類 では、コミュニケーションパスに関する以下の項目について説明します。

- **コミュニケーションパスの種類:** 2 台のサーバで構成するクラスタでは、2 種類のコミュニケーションパス (TCP/IP、共有ディスク) を使用できます。3 台以上のサーバで構成するクラスタでは、TCP/IP コミュニケーションパスだけを使用できます。
- **SIOS Protection Suite のハートビート:** サーバ間のコミュニケーションパスの主な機能は、SIOS Protection Suite のハートビートを通信することです。ハートビートは、接続先サーバの死活を監視するために、一定の間隔で送信される信号です。
- **セーフティチェック:** すべてのコミュニケーションパスが停止すると、SIOS Protection Suite はセーフティチェックを実行してシステム障害を検査した後、フェイルオーバを実行します。

8.1.3.1. コミュニケーションパスの種類

SIOS Protection Suite には 3 種類のコミュニケーションパスがあり、それぞれ異なるプロトコルを使用して、コミュニケーションパスを冗長化できます。同じ媒体に同じ種類のコミュニケーションパスを複数定義しても意味がありませんが、異なるプロトコルまたは異なる媒体を使用してパスを冗長化すると、コミュニケーションパス障害に起因するフェイルオーバを回避できます。

コミュニケーションパスには優先順位を設定します。SIOS Protection Suite は、優先順位を参照してノード間の通信を行います。ハートビート信号はアクティブなコミュニケーションパスすべてに送信されます。SIOS Protection Suite がサポートするコミュニケーションパス、およびコミュニケーションパスに割り当てたデフォルトの優先順位の範囲は次のとおりです。

- **TCP/IP (ソケット)** : LAN コミュニケーションパスは最も高い優先順位を持ちます。ソケットコミュニケーションパスのデフォルトの優先順位の範囲は 1 ～ 30 です。サーバペアに異なるアダプタを使用して、複数の LAN コミュニケーションパスを定義すると、フェイルオーバの誤動作を回避できます。

  注記: LifeKeeper GUI は 保護対象リソースのステータス情報の通信にTCP/IPを使用します。2 本の TCP/IP コミュニケーションパスを設定した場合、SIOS Protection Suite は優先順位の高いコミュニケーションパスを使用して、リソースのステータス情報を通信します。

- **共有ディスク:** SIOS Protection Suite では、クラスタを構成するサーバペアが通信場所として使用する共有ディスク上に raw ディスクパーティションを定義できます。共有ディスクコミュニケーションパスは、2 台のサーバが同じドライブ名を使用し、ドライブ名は同じディスクパーティションを指す必要があります。通常の場合、ディスクパーティションは 1 MB 程度で十分です。共有ディスクコミュニケーションパスのデフォルトの優先順位は 61 ～ 99 です。共有ディスクコミュニケーションパスは、2 サーバ構成だけで使用できます。

  注記: 共有ディスクコミュニケーションパスは、SIOS Protection Suite がクラスタ内の他のサーバの稼働状態を監視する目的にのみ使用されます。そのため、TCP/IP コミュニケーションパスがダウンすると、共有ディスクコミュニケーションパス、2 本目の TCP/IP コミュニケーションパスがアクティブでも、GUI には、通信先サーバの階層が UNKNOWN (不明) と表示されます。

共有ディスクコミュニケーションパスの詳細

共有ディスクコミュニケーションパスは、他のコミュニケーションパスがすべて停止した場合の最後の手段となります。共有ディスクコミュニケーションパスが停止すると、少なくとも 1 台のサーバがストレージのサブシステムにアクセスできなくなるため、2 台のサーバが同じディスクリソースに同時にアクセスする「スプリットブレイン」を回避できます。

注意:

- SIOS Protection Suite の設定には、クラスタ内の任意の 2 つのサーバ間について、共有ディスクコミュニケーションパスを複数指定することはできません。

- JBOD またはホストベースの RAID で共有ディスクコミュニケーションパスを使用する場合は、クラスタメンバがシャットダウンするか、サービスを停止した際のコミュニケーションパスの信頼性を事前にテストしてくだ

さい。JBOD またはホストベースの RAID を使用する構成では、クラスタメンバがダウンすると、コミュニケーションパスが切断されて、フェイルオーバできないことがあります。

8.1.3.2. SIOS Protection Suite のハートビート

ハートビートは、SIOS Protection Suite の主要な障害検出機構です。ハートビートとは、サーバペアのコミュニケーションパスに一定間隔で送信される信号を指します。サーバは、ハートビートを通じて、通信先サーバが稼働していることを確認します。コミュニケーションパスには、ハートビート間隔 を秒単位で定義します。また、コミュニケーションパスが稼働していると判断する、連続欠落が許容されるハートビート信号の最大数を指定します。

SIOS Protection Suite は、コミュニケーションパスが停止すると判断すると、優先順位が次に高いコミュニケーションパスを使用してノード間通信を開始します。すべてのコミュニケーションパスでハートビート信号を受信できない場合にのみ、SIOS Protection Suite は セーフティチェック を実行して、フェイルオーバリカバリを実行するかどうかを判断します。

8.1.3.3. ハートビート間隔

SIOS Protection Suite のハートビート間隔とは、サーバの稼働状態を確認するハートビート信号を送信する間隔 (秒単位) を指します。デフォルト値の 6 秒を推奨します。

- ハートビート間隔を最小の 4 秒に設定する場合は、コミュニケーションパスをプライベートネットワーク上で設定した後、十分にテストしてください。ハートビート間隔を 5 秒未満にすると、ネットワークの中断によって、フェイルオーバが誤動作することがあります。

- ハートビート間隔はハートビート最大欠落数と関係します。ハートビート最大欠落数は、デフォルトの 5 回を推奨します。ハートビート最大欠落数を最小値 (3 または 4) に設定すると、フェイルオーバが誤動作することがあります。本番環境で十分にテストしてください。

- ハートビート間隔とハートビート最大欠落数を大きな値に設定すると、SIOS Protection Suite の障害検出機能が低下します。

8.1.3.4. セーフティチェック

すべてのコミュニケーションパスが停止すると、SIOS Protection Suite は、クラスタサーバが完全に停止したと判断し、フェイルオーバを実行します。ただし、そのときに、SIOS Protection Suite　は障害がコミュニケーションパスではなく、サーバに発生したことを確認するセーフティチェックを実行します。

セーフティチェックでは、LAN Manager を使用して、サーバが稼働しているかどうかを確認します。その結果に応じて、次のいずれかのイベントが発生します。

- **システムが稼働している場合:** セーフティチェックにより、サーバがネットワークに接続していることが確認された場合、フェイルオーバを中止して、次のメッセージを LifeKeeper イベントログに出力します。

  ```
  SAFETY CHECK FAILED:COMM_DOWN ABORTED
  ```

- **システムが停止している場合:** サーバが所定のタイムアウト (デフォルトは 8 秒) 以内に応答を返さない場合、サーバが停止していると判断して、フェイルオーバを実行します。

すべてのコミュニケーションパスが停止すると、SIOS Protection Suite はセーフティチェックを 1 回のみ実行します。セーフティチェックでシステムの稼働を確認すると、SPS はフェイルオーバを中止します。また、SIOS Protection Suite が中断したフェイルオーバを再開するのは、次のすべてのイベント (1、2、3) が順番に発生したときになります。

1. 少なくとも 1 本のコミュニケーションパスが **稼働状態** に戻る。
2. すべてのコミュニケーションパスが再び **停止** する。
3. セーフティチェックが実行され、対向ノードの稼働が確認できない。

8.1.4. リソース階層

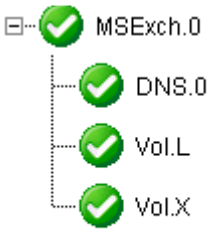
LifeKeeper GUI では、リソース階層をサーバに作成して、1 台以上のバックアップサーバに拡張できます。リソース階層は、サーバを指定すると、SIOS Protection Suite が自動的に作成します。SIOS Protection Suite は各サーバの構成データベースに階層情報を保持しています。コマンドラインインターフェースを使用する場合は、階層を各サーバに定義する必要があります。

作成したリソース階層内のリソースの停止と起動は、SIOS Protection Suite が管理します。階層定義の背景については、次の項目で説明しています。

- リソースのステータス
- 階層の関係
- 共有イクイバレンシ
- リソース階層情報

8.1.4.1. 階層の関係

SIOS Protection Suite では、リソースインスタンス間に関係を作成できます。主な関係は、依存関係です。例えば、あるリソースインスタンスが正常に機能するためには、別のリソースインスタンスの存在が前提となります。リソースインスタンスと依存関係を組み合わせたものがリソース階層です。

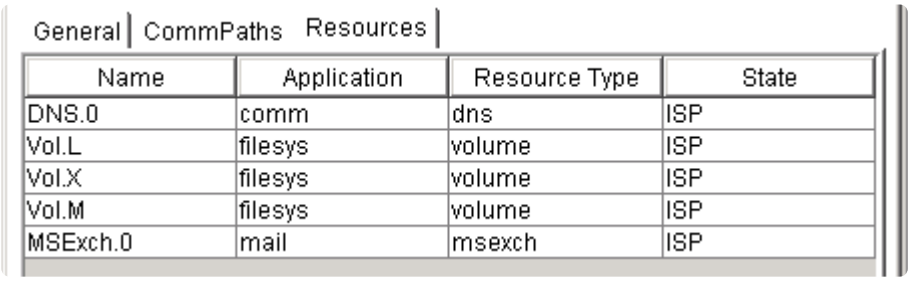


上記の例では、MSExch.0 は Exchange のリソースであり、DNS リソース (DNS.0) と 2 つのボリュームリソース (Vol.L および Vol.X) という、3 つの依存関係があります。

リソース階層に定義した依存関係によって、SIOS Protection Suite がリソースインスタンスを起動/停止する順番が決まります。この例のリソース階層では、DNS インスタンスとボリュームインスタンスが正常に起動しないと、MSExch.0 リソースのサービスを開始できません。

8.1.4.2. リソース階層情報

サーバプロパティ ダイアログボックスには、サーバに定義したリソースに関する情報のスナップショットが表示されます。


General | CommPaths | Resources

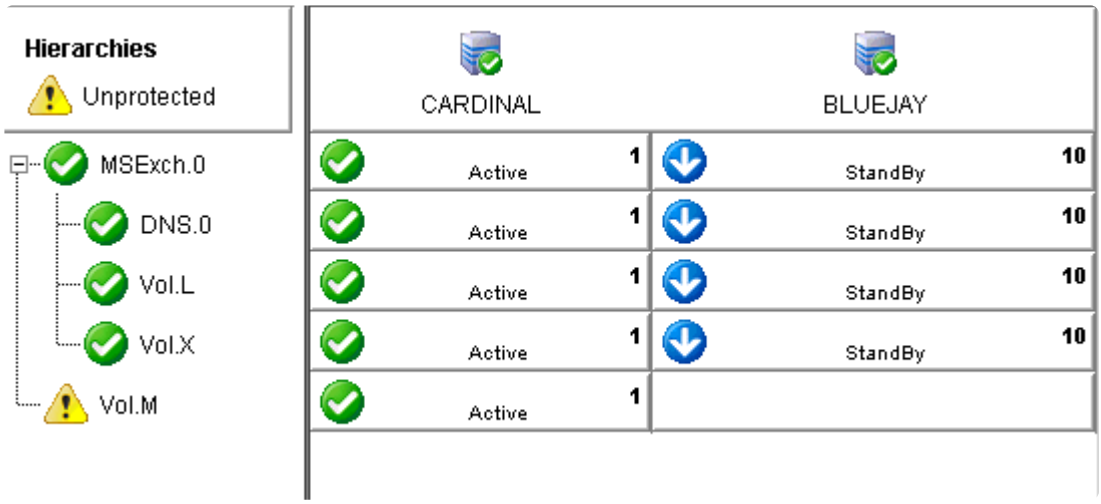
Name	Application	Resource Type	State
DNS.0	comm	dns	ISP
Vol.L	filesys	volume	ISP
Vol.X	filesys	volume	ISP
Vol.M	filesys	volume	ISP
MSExch.0	mail	msexch	ISP

リソースのその他の情報については、ステータステーブル (GUI のウィンドウ) または リソースプロパティの表示 を参照してください。

8.1.4.3. リソースのステータス

LifeKeeper GUI のステータス表示には、接続先サーバに定義したリソースが表示されます。ステータスウィンドウの左側には、**リソース階層ツリー** が表示されます。この階層ツリーは、各サーバに共通するリソースのステータス (グローバルリソースステータス) を表します。

ステータスウィンドウの右側には、各サーバのリソースのステータスが表示されます。



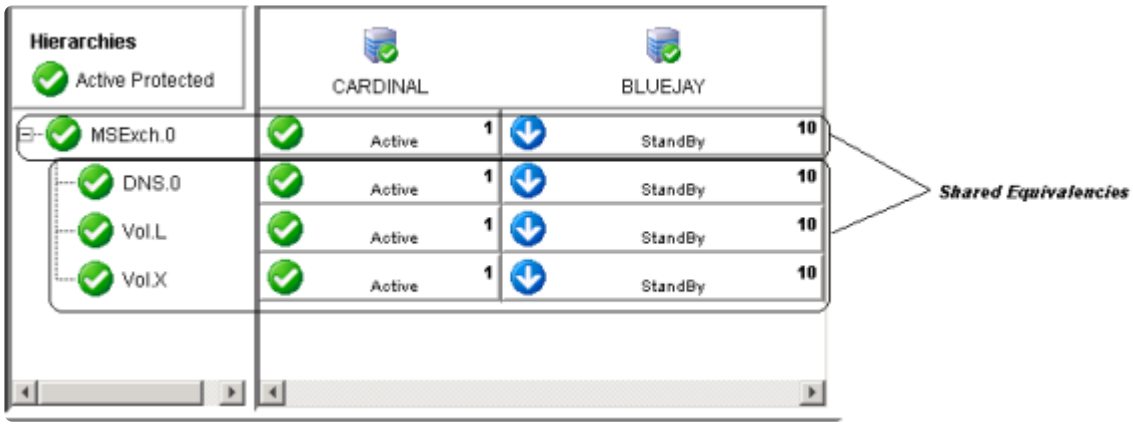
上図を例に説明すると、MSExch.0 階層はサービス中 (ISP) であり、保護されています。Vol.M リソースは、CARDINAL **だけ** に作成されています。*Vol.M* **はサービス中** ですが保護されていないため、黄色の三角形が表示されています。

リソースステータスの詳細については、リソースステータスの表示 を参照してください。

8.1.4.4. 共有イクイバレンシ

SIOS Protection Suite のリソース階層を作成するときには、プライマリサーバに階層を作成した後、その階層をバックアップサーバに拡張します。リソースインスタンスは通常、1 台のサーバだけでアクティブになります。SIOS Protection Suite では、そのようなリソースに対して共有イクイバレンシという 第 2 の種類の関係を定義します。これにより、あるサーバでサービス中のリソースが、その他の定義済みサーバではサービス停止になります。

下図では、サーバペアの各階層に共有イクイバレンシが設定されています。例えば、MSExch.0 というリソースは両方のサーバにありますが、MSExch.0 の 2 つのインスタンス間、および DNS インスタンスと 2 つのボリュームインスタンスとの間にも共有イクイバレンシが定義されています。



8.2. 構成

SIOS Protection Suite 環境をインストールしたら、クラスタ内のサーバごとに SIOS Protection Suite ソフトウェアを構成できます。このセクションでは構成の方法について説明します。

- SPS の設定手順
- アクティブ / アクティブグループ化
- アクティブ / スタンバイグループ化
- インテリジェントスイッチバックと自動スイッチバック
- SPS 構成
  - 共通ハードウェアコンポーネント
  - システムのグループ化

8.2.1. SIOS Protection Suite の設定手順

次の手順に従って設定します。リンクをクリックすると詳細な説明が表示されます。以下の作業は、クラスタ内の_各サーバ_で実行します。

1. **コントロール パネル** を開き、**[管理ツール]** の **[サービス]** で LifeKeeper の各種サービスが実行されていることを確認します。*LifeKeeper* サービスと *LifeKeeper External Interfaces* サービスの両方が稼働していることを確認します。2 つのサービスが稼働していない場合は、必要なサービスを起動してください。

   詳細については、LifeKeeperの起動と停止 を参照してください。

2. SIOS Protection Suite　サーバの管理者権限を持つユーザは、サーバ上でアプリケーションクライアントを起動できます。**[スタート]** メニューをクリックし、**[プログラム] -> [LifeKeeper] -> [LifeKeeper GUI]** の順に選択してください。

   アプリケーションを読み込むと、**LifeKeeper GUI** が開き、**[クラスタへの接続]** ダイアログボックスが開きます。接続先サーバの名前を **[サーバ名]** に入力し、**ログイン名** と **パスワード** を入力します。

3. コミュニケーションパスを作成 します。SIOS Protection Suite による保護をアクティブにする前に、LifeKeeper のコミュニケーションパス (ハートビート) を定義してください。

4. サーバーのシャットダウン方法 を設定します。システムをシャットダウンする際、リソースを切り替えるか指定します。

5. 以上の操作を実行すると、SIOS Protection Suite でアプリケーションを保護する準備が完了します。次の手順は、SIOS Protection Suite リカバリキットの種類によって異なります。

   • Core Recovery Kit を使用する場合は、ボリュームリソース階層の作成 、DNS リソース階層の作成 、IP リソース階層の作成 、ファイル共有リソース階層の作成 、LAN Manager リソース階層の作成 、または Generic Application リソース階層の作成 を参照してください。

   • オプションのMicrosoft SQL Server Recovery Kit を使用する場合は、Microsoft SQL Server Recovery Kit 管理ガイド のリソース階層の作成と拡張に関する説明を参照してください。

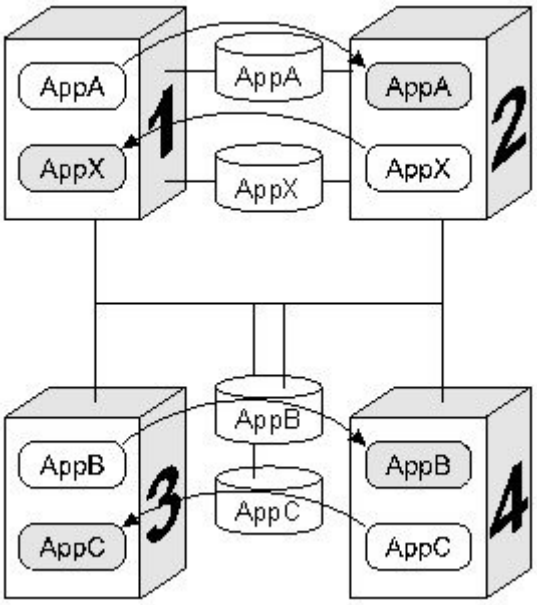
8.2.2. アクティブ / アクティブグループ化

アクティブ / アクティブグループでは、各サーバがサービスを起動します。また、各サーバは、他のリソース階層のバックアップサーバとしても動作します。

次の例では、4 台のサーバが 2 組のアクティブ / アクティブペアを構成しています。*Server 1* は *AppA* を処理し、*Server 2* で稼働する *AppX* のバックアップサーバとしても動作します。Server 2 も同様です。_Server 2_ は *AppX* を処理し、*Server 1* で稼働する *AppA* バックアップサーバとしても動作します。*Server 3* と *4* もアクティブ / アクティブ関係です。

Server 1 と *2* および *Server 3* と *4* はよく似た構成ですが、決定的な違いがあります。*AppA* アプリケーションと *AppX* アプリケーションは、*Server 1* と *Server 2* だけがグループ化のサービスを提供しています。そのため、それ以外のサーバは、共有リソースにアクセスできません。

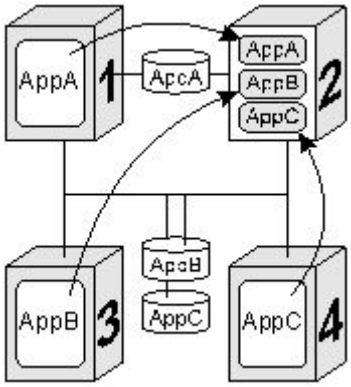
一方、*AppB* と *AppC* については、4 台のサーバが *AppB* と *AppC* 共有リソースにアクセスできるため、複数の構成が可能です。例えば、*Server 1* や *Server 2* を 3 番目と 4 番目のバックアップとして、*AppB* と *AppC* をフェイルオーバできます。



注記: SIOS Protection Suite はボリュームレベルでロックをかけるため、*AppB* と *AppC* ディスクリソースに接続しているサーバ 4 台のうち、実際にディスクリソースにアクセスできるのは 1 台だけです。この例では、Server 3 が *AppB* を処理するため、*Server 1* 、*2* 、*4* は、ディスクリソースに物理的に接続していても、実際にはアクセスできません。

8.2.3. アクティブ / スタンバイグループ化

アクティブ/スタンバイグループでは、プライマリサーバが処理を実行します。バックアップサーバは、プライマリサーバに障害が発生した場合に備えて待機します。待機系には、処理能力が低い小規模なシステムを使用できますが、稼働系に障害が発生した場合に備えて、リソースを継続的に運用する処理能力が必要になります。



スタンバイサーバは、複数のアクティブサーバをバックアップできます。例えば、上図の場合、*Server2* は 3 組のアクティブ / スタンバイペアをバックアップしています。SIOS Protection Suite リソース定義により、このアクティブ / スタンバイは、次のような組み合わせで動作します。

- *Server1* で稼働する *AppA* は、*Server2* にフェイルオーバします。
- *Server3* で稼働する *AppB* は、*Server2* にフェイルオーバします。
- *Server4* で稼働する *AppC* は、*Server2* にフェイルオーバします。

複数のアクティブ/スタンバイ構成を採用する場合は、次の点に注意してください。

- **ディスクの所有権:** アクティブアプリケーションが異なる場合、同じボリューム上のディスクスライスは使用できません。SIOS Protection Suite はボリューム単位でロックをかけます。SCSI をロックした場合、共有 SCSI バス上の 1 つのシステムだけがディスク装置のボリュームにアクセスできます。上の例では、Server3 が AppB ディスクリソースを所有しており、Server4 が AppC リソースを所有しています。
- **処理能力:** *Server1* 、*Server3* 、*Server4* が同時に故障することは希ですが、1 台のスタンバイサーバで複数のリソースをバックアップする場合は、複数サーバに障害が発生した場合を想定して、1 台のサーバで重要な処理を継続できる能力が必要になります。
- **SIOS Protection Suite の管理:** 上の例では、_Server2_ が他のサーバ 3 台をバックアップしています。SIOS Protection Suite データベースを複数の論理グループで同時に管理することは望ましくありません。最初に 1 組の稼働系と待機系にリソースを作成し、次にその待機系と他の稼働系にリソースを作成します。

8.2.4. インテリジェントスイッチバックと自動スイッチバック

リソースのスイッチバック方法は、デフォルトで *[INTELLIGENT]* に設定されます。インテリジェントスイッチバックを指定した場合、リソースが_サーバ A_ から_サーバ B_ にフェイルオーバされた後、*サーバ B* に障害が発生するか、管理者がリソースを手動で別のサーバに切り替えるまで、リソースはサーバ B にとどまります。そのため、*サーバ A* が復旧しても、リソースは *サーバ B* で稼働します。*サーバ A* はリソースのバックアップとなります。

しかし、状況によっては、プライマリサーバが障害から復旧した場合、リソースを自動的に元に戻すことが望ましいこともあります。SIOS Protection Suite では、デフォルトのインテリジェントスイッチバックを ***自動スイッチバック*** に変更できます。自動スイッチバックはリソース階層ごとに指定できます。リソース階層を稼働しているサーバに_自動スイッチバック_を指定した場合、そのサーバに障害が発生すると、リソース階層はバックアップシステムにフェイルオーバされますが、プライマリサーバが障害から復旧すると、リソース階層は自動的に元に戻ります。

注記:

- 複製データ (DataKeeper) を使用する場合は、インテリジェントスイッチバックを選択してください。複製データは自動スイッチバックに対応していません。
- スイッチバック_の確認は、LifeKeeper を起動するか、サーバをクラスタに追加すると実行されます。通常の運用時にはスイッチバックは確認されません。
- SIOS Protection Suite は、優先度の高いサーバから低いサーバには自動スイッチバックを実行しません。
- 2 つのリソースに依存関係があり、各リソースに異なるスイッチバック方法が指定されている場合、親リソースの設定が優先します。

8.2.5. SIOS Protection Suite の設定

SIOS Protection Suite は、複数のサーバに定義されたリソース階層に基づいて動作します。SIOS Protection Suite によるフェイルオーバの背景説明については、次の項目を参照してください。

共通ハードウェアコンポーネント

システムのグループ化

リソース階層

8.2.5.1. 共通ハードウェアコンポーネント

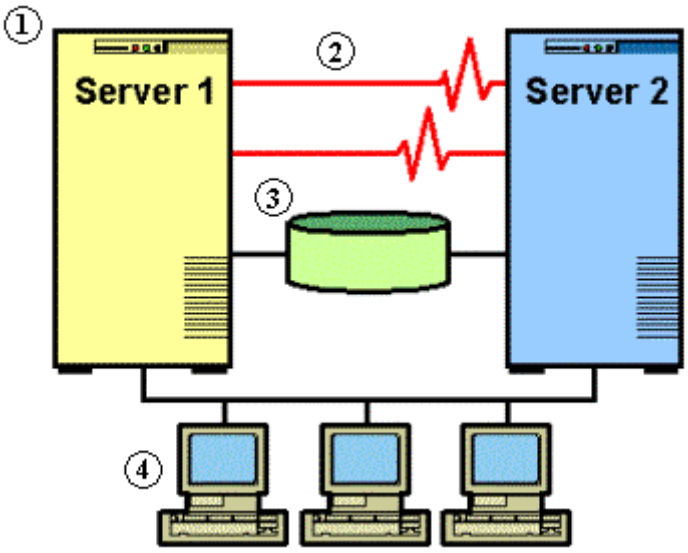
SIOS Protection Suite 構成は、次図に示すように、共通コンポーネントを共有します。

1. **サーバグループ:** SIOS Protection Suite は、Windows サーバをクラスタ化して障害回復機能を提供します。サーバ (SIOS Protection Suite ノード) のプラットフォームは、同じでなくてもかまいません。

2. **ハートビート用コミュニケーションパス:** コミュニケーションパスは最低 1 本を設定する必要がありますが、2 本のコミュニケーションパスを作成することを強く推奨します。通信障害による不要なフェイルオーバを回避するために、TCP/IP (ソケット) など、プロトコルの異なるコミュニケーションパスを作成して冗長化します。SIOS Protection Suite は、コミュニケーションパスを使用して、障害検出用のハートビートを一定間隔で送信します。サーバの死活状態を監視し、必要に応じて、リソースを切り替えます(コミュニケーションパスの概要 を参照)。

3. **共有データリソース:** SIOS Protection Suite は、共有データ、アプリケーション、通信リソースをリストアします。そして、共有ストレージデバイスの上のリソースに対して、ボリューム (ドライブ名) 単位でアクセスを制御します。サーバに障害が発生すると、SIOS Protection Suite は保護対象リソースをアクティブサーバに自動的に切り替えます。複数のシステムが共有する周辺装置は、外部のキャビネットに一括して収容してください。共有ストレージの構成方法については、ストレージの構成 を参照してください。

4. **ユーザ接続用の共有通信リソース:** SIOS Protection Suite は、IP アドレス、コンピュータの別名、ファイル共有リストなどのユーザ通信リソースを自動的に管理して切り替えます。SPS が通信リソースを自動的に切り替えることにより、ユーザは通常のパスで接続を継続できます。



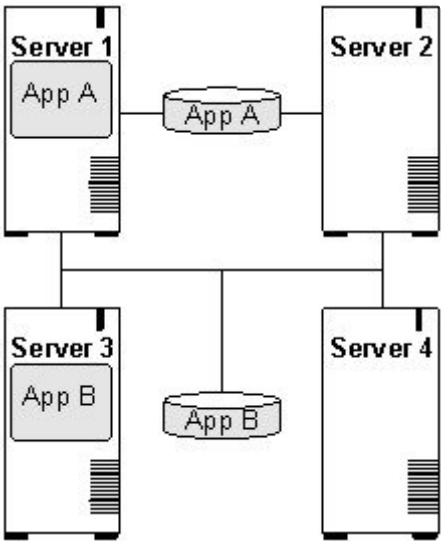
8.2.5.2. システムのグループ化

リソース階層は SIOS Protection Suite サーバのクラスタに定義します。階層を構成するサーバには、優先度を指定します。優先度が最も高いサーバには、優先度 *1* が付きます。最高の優先度が付いたプライマリサーバは、リソースを操作するコンピュータです。2 番目に高い優先度を持つサーバは、プライマリサーバに障害が発生した際にリソースの切り替え先になる SIOS Protection Suite のバックアップサーバです。

アクティブ / アクティブグループ では、すべてのサーバがリソースを起動し、同時に他のサーバのリソース階層をバックアップします。アクティブ / スタンバイグループ では、プライマリサーバが処理を実行します。バックアップサーバは、プライマリサーバに障害が発生した場合に備えて待機します。待機系には、処理能力が低い小規模なシステムを使用できますが、稼働系に障害が発生した場合に備えて、リソースを継続的に運用する処理能力が必要になります。

共有リソースへの物理的な接続とアクセス方法により、グループ化のオプションが決まります。グループ化を実行するには、ハートビートを送信するコミュニケーションパスを設定し、全サーバが共有 SCSI インターフェースまたはファイバチャネルインターフェースを介してディスクリソースにアクセスできるようにします。例えば、次図では、*Server 1* のリソース *AppA* に関して、1 つのグループを設定できます。この構成では、*AppA* データベースに共有アクセスするサーバは *Server 2* だけです。

一方、*Server 3* で稼働する *AppB* リソースは、3 台のサーバを任意に構成できます。共有 SCSI バスがサーバ 4 台に *AppB* データベースへのアクセスを提供しているためです。



8.2.6. SPS でマルチバイト言語エンコーディングを設定する

LifeKeeper は、Windows でサポートされているすべてのシステムロケールで使用できます。ただし、マルチバイト文字エンコード（日本語、中国語、韓国語など）を使用するロケールでは、システムロケールに基づいて正しいエンコードを使用するように LifeKeeper を設定する必要があります。

これを正しく行うために、設定ファイルがコアソフトウェアに含まれています。ユーザーは、システムのWindows ロケールに対応する数値であるシステムのコードページに基づいてロケール（エンコードを含む）を指定できます。ファイルは、%LKROOT%\cygwin\usr\share\locale\locale.from.codepage です。このテキストファイルは、必要に応じてカスタマイズできます。コメントされていない行は空白にするか、タブで区切られた2つの値（コードページの数値、使用するロケールの文字列）を含める必要があります。

locale.from.codepage ファイルには、すでに次の値が入力されています。

```
932 ja_JP.SJIS

936 zh_CN.GB2312
```

システムのコードページを見つけるには、次の powershell コマンドを実行してください。

```
[System.Text.Encoding]::Default.CodePage
```

LifeKeeperは、名前または値にマルチバイト文字が含まれるシステムリソースにアクセスする必要がない限り、このファイルがなくてもマルチバイトロケールで正しく動作します。たとえば、IP アドレスの作成時には NIC名が使用されますが、NIC 名がマルチバイト文字でない場合、このファイルがシステムのコードページ用に設定されているかどうかに関係なく、IP アドレスを作成できます。

8.3. SIOS Protection Suite の管理の概要

SIOS Protection Suite には、次の 2 種類の管理インターフェースがあります。

- LifeKeeper GUI
- LifeKeeper コマンドラインインターフェース

LifeKeeper 管理インターフェースは次のタスクに使用します。ここでは、SIOS Protection Suite を設定する順番に従って、各タスクを説明します。

- **コミュニケーションパスの定義:** LifeKeeper のソースインスタンスとリソース階層を定義する前に、コミュニケーションパスを定義する必要があります。コミュニケーションパスを定義するには、**[編集]** メニューまたは GUI ツールバーの **[コミュニケーションパスの作成]** を使用します。
- **リソースの定義:** リカバリキットをインストールすると、そのリカバリキットがサポートするリソースタイプが **[リソース階層の作成]** ダイアログボックスに表示されます。大半のリカバリキットは、依存関係を自動的に作成します。
- **監視:** LifeKeeper GUI のステータスには、接続先サーバの保護対象リソースのステータスがアイコンで表示されます。SIOS Protection Suite が記録するログも GUI に表示されます。
- **手動による介入:** SPS を保守管理する場合は、サーバとリソースを停止します。LifeKeeper GUI には、特定のリソースを起動/停止するメニューがあります。SIOS Protection Suite でアプリケーションを保護している場合、サービスの起動と停止は、SIOS Protection Suite からのみ実行します。

SIOS Protection Suite の初期設定については SIOS Protection Suite の設定手順 を参照してください。

GUI インターフェースを使用した SIOS Protection Suite の管理、設定、保守の手順については、GUI による管理作業 と メンテナンス作業 を参照してください。

> **注記:** SIOS Protection Suite は、各サーバのローカルシステムアカウントで SIOS Protection Suite サービスを実行するように設定されています。他のユーザアカウントで SIOS Protection Suite を実行するような変更は行わないでください。

GUI による管理作業

リソース階層に関連する作業

マニュアルページ

LKSUPPORT

ブラウザのセキュリティ設定

IP ローカルリカバリ

SNMP による SPS イベント転送の概要

Java のアップグレード

8.3.1. GUI による管理作業

サーバプロパティの編集

サーバのシャットダウン方法の設定

サーバプロパティ

自動フェイルオーバを無効にする

コミュニケーションパスの作

コミュニケーションパスの削除

8.3.1.1. サーバプロパティの編集

1. サーバプロパティを編集するには、最初に サーバプロパティを表示 します。

2. 適切なアクセス権でサーバにログインすると、次の項目を編集できます。
   - シャットダウン方式
   - 自動フェイルオーバの設定
   - サーバ設定 (特殊な構成を設定したサーバのみ)

3. 編集が完了すると、**[適用]** ボタンが有効になります。このボタンをクリックすると、変更内容が反映されます。ただし、ウィンドウは閉じません。

4. 作業が完了したら、**[OK]** をクリックして、変更内容を保存してウィンドウを閉じるか、**[キャンセル]** をクリックして、変更を適用せずに、ウィンドウを閉じます。

8.3.1.2. サーバのシャットダウン方法の設定

シャットダウン方法とは、サーバをシャットダウンする際、リソースをバックアップサーバに切り替える設定オプションを指します。次のオプションを指定できます。

リソースを切り替えない (デフォルト)	通常のシャットダウンではリソース階層を切り替えません。
リソースを切り替える	通常のシャットダウン時にすべてのリソース階層を切り替えます。

制限事項: **シャットダウン時のスイッチオーバ** の設定は SIOS DataKeeper リソースではサポートされません。

シャットダウン方法はデフォルトで **[リソースを切り替えない]** に設定されています。各サーバにシャットダウン方法を指定してください。必要に応じて、**[リソースを切り替える]** に変更します。

クラスタ内の各サーバについて、以下の操作を行ってください。

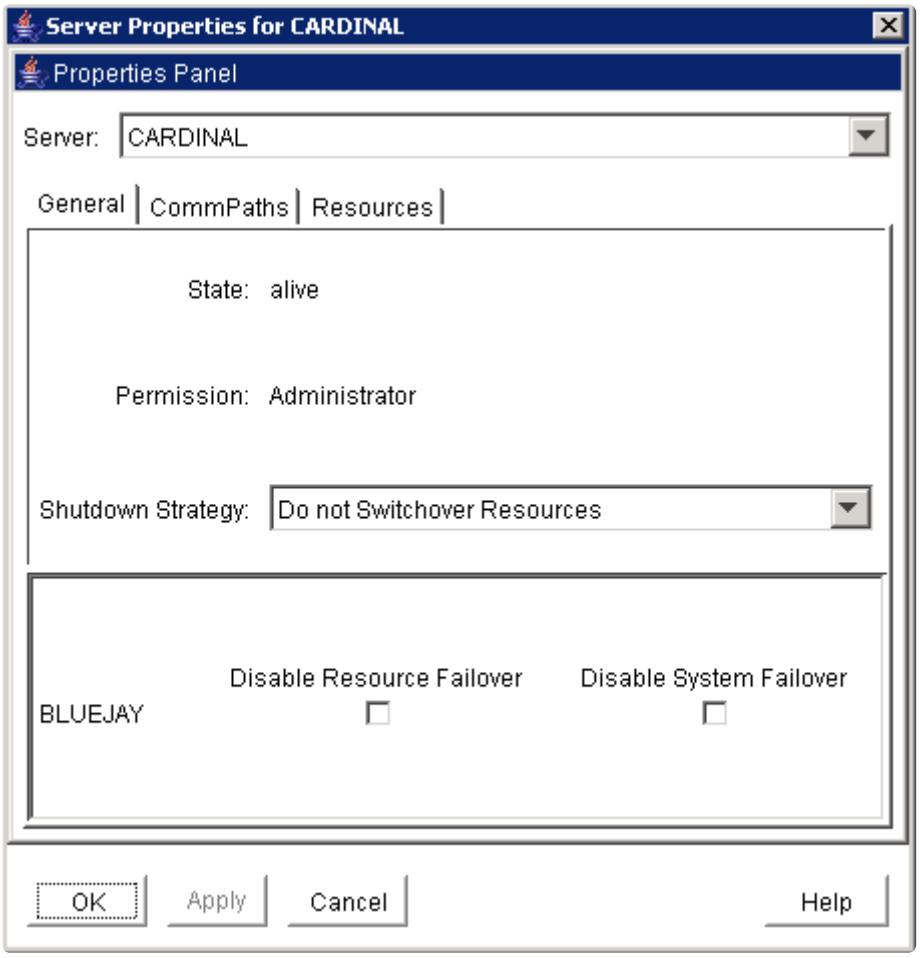
1. サーバプロパティの表示 で説明した手順に従って、**[サーバプロパティ]** ダイアログボックスを開きます。
2. **[サーバプロパティ]** ダイアログボックスの [一般]タブ で **シャットダウン方法** を選択します。

注記: ここで指定したシャットダウン方法は、通常のシャットダウン時に、SPS プロセスが稼働していないと正常に機能しません。SPS が稼働していないか、リソースサービスが停止していると、リソースは切り替えられません。

8.3.1.2.1. サーバプロパティ

[サーバプロパティ] ダイアログボックスは、メニュー またはサーバのポップアップメニューから使用できます。このダイアログボックスには、サーバのプロパティが表示されます。**[編集]** メニューを使用して、サーバを選択します。選択したサーバを変更すると、**[サーバプロパティ]** ダイアログボックスも自動的に更新されます。

[OK] をクリックすると、変更内容が適用されてウィンドウが閉じます。**[適用]** をクリックすると、変更が反映されます。**[キャンセル]** をクリックすると、**[適用]** をクリックした後に変更した内容を保存せずにウィンドウが閉じます。

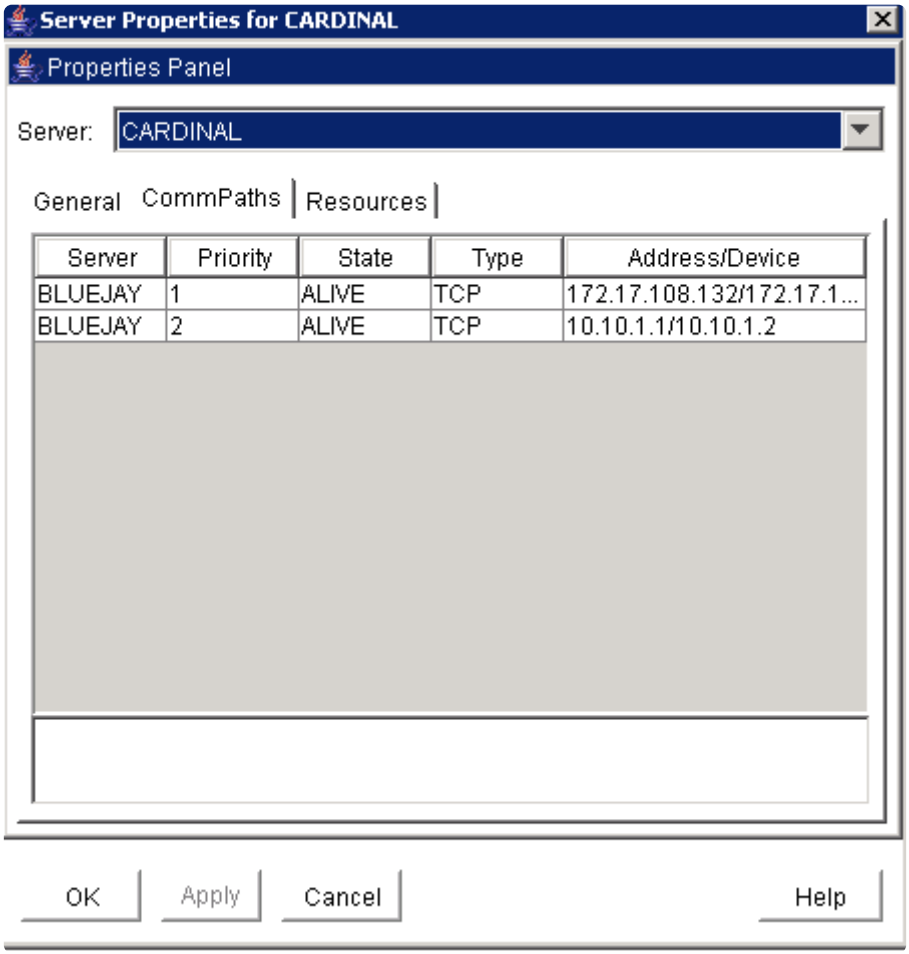


- **名前:** 選択したサーバの名前
- **権限:** サーバにログインするユーザに付与する権限です。次の権限を指定できます。
  - **管理者** - SIOS Protection Suite に関するすべてのタスクを実行できます。
  - **オペレータ** - SIOS Protection Suite のリソースとサーバの状態を監視できます。リソースを起動 / 停止できます。
  - ゲスト - SIOS Protection Suite のリソースとサーバの状態を監視できます。
- **状態:** サーバの現在の状態。サーバの状態を表す値は、次のとおりです。
  - **稼働中** - サーバは使用可能です。
  - **停止中** - サーバは使用できません。
  - **不明** - リソースの状態を特定できません。GUI サーバは使用できない可能性があります。
- **シャットダウン時の動作** (編集可能)。サーバをシャットダウンする際、稼働中のリソースをバックアップサーバに切り替える方法を制御します。**[リソースを切り替える]** を設定すると、クラスタ内のバックアップサーバでリ

ソースが起動します。**[リソースを切り替えない]** を設定すると、クラスタ内の別のサーバのリソースが起動しません。

- **サーバ名:** クラスタ内でローカルサーバからバックアップサーバに自動的にフェイルオーバする機能は、このタブで設定します。休止中のサーバはリストに表示されません。そのため、クラスタを構成しているサーバすべてが運用可能です。つまり、少なくとも、SIOS Protection Suite コミュニケーションパス 1 本がアクティブになっています。リストには、ローカルサーバを除き、クラスタでアクティブなサーバの名前が一覧表示されます。各サーバには、2 種類のフェイルオーバ機能を設定できます。すべてのフェイルオーバ機能は、デフォルトで有効に設定されます。
  - **リソースフェイルオーバ不可** - ローカルサーバのリソース階層に障害が発生した場合、バックアップとして使用しないリモートサーバを選択します。バックアップ機能を無効にしたサーバは、ローカルリソースに障害が発生しても、フェイルオーバサイトとして使用されません。フェイルオーバ機能は、設定を解除すると再び有効になります。
  - **システムフェイルオーバ不可** - ローカルサーバが完全に停止した場合、バックアップとして使用しないリモートサーバを選択します。無効に設定したサーバは、ローカルサーバが完全に停止しても、フェイルオーバサイトとして機能しません。フェイルオーバ機能は、設定を解除すると再び有効になります。

注記: すべてのリモートサーバでリソースフェイルオーバを無効にすると、障害が発生したリソースに「 **Failed** 」マークが付きます。このマークが付いたリソースは、クイックチェックとディープチェックの監視外となります。ただし、障害が発生したリソースまたは階層内の依存リソースは、サービスから削除されませんが、フェイルオーバされません。



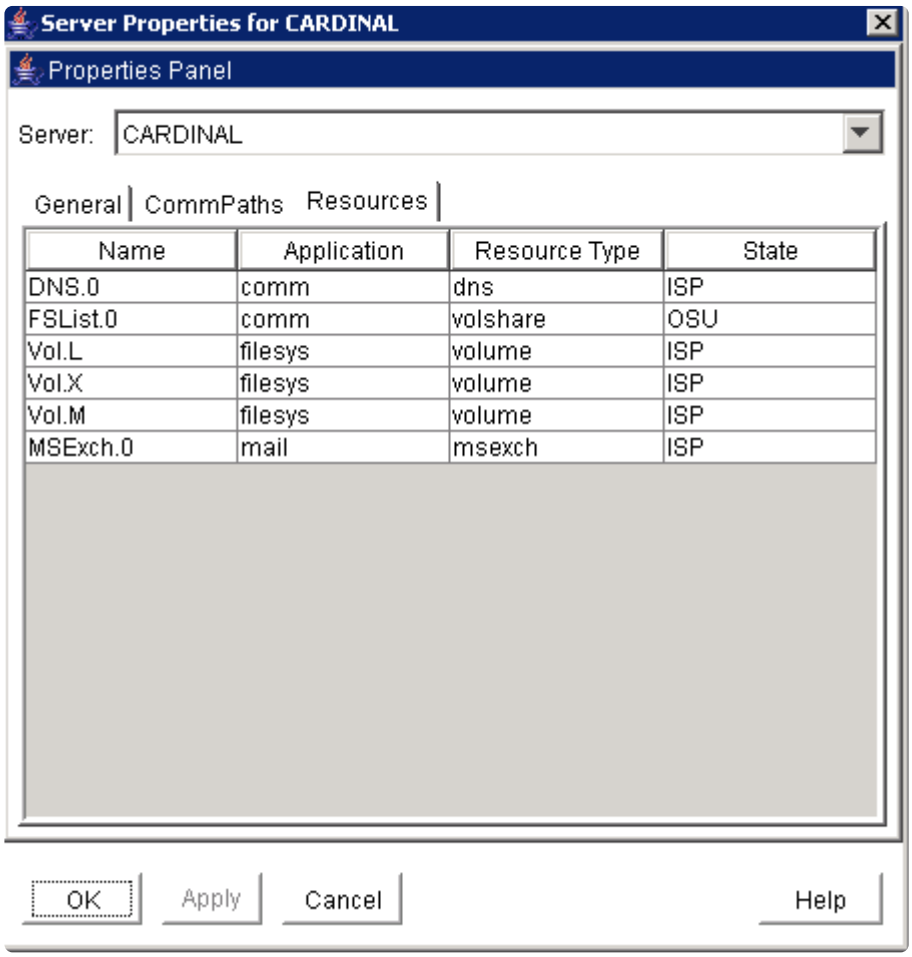
- **サーバ:** SIOS Protection Suite クラスタ内でコミュニケーションパスが接続されているその他のサーバの名前。

- **タイプ:** リストのサーバと **サーバ** フィールドで指定されているサーバ間のコミュニケーションパスの種類 (TCP/IP、共有ディスク)。

- **状態:** LifeKeeper 構成データベース (LCD) のコミュニケーションパスの状態。コミュニケーションパスの状態を表す値は、次のとおりです。
  - **稼働中** - 正常に機能しています。
  - **停止中** - 正常に機能していません。
  - **不明** - リソースの状態を特定できません。GUI サーバは使用できない可能性があります。

- **アドレス / デバイス:** このコミュニケーションパスが使用する IP アドレスまたはデバイス名。

- **コミュニケーションパスステータス:** LifeKeeper 構成データベース (LCD) のコミュニケーションパスの状態に基づき、GUI が決定したコミュニケーションパスステータスのサマリ。下側のパネルには、コミュニケーションパスのステータスが次のように表示されます。
  - **正常** - すべてのコミュニケーションパスが正常に機能しています。
  - **障害** - 特定のサーバへのすべてのコミュニケーションパスが機能していません。
  - **不明** - コミュニケーションパスの状態を特定できません。GUI サーバは使用できない可能性があります。
  - **警告** - 特定のサーバへの 1 つ以上のコミュニケーションパスが停止しているか、コミュニケーションパス 1 本だけが稼働しています。
  - **縮退** - 特定のサーバに接続した冗長コミュニケーションパスが機能していません。
  - **定義なし** - コミュニケーションパスが定義されていません。



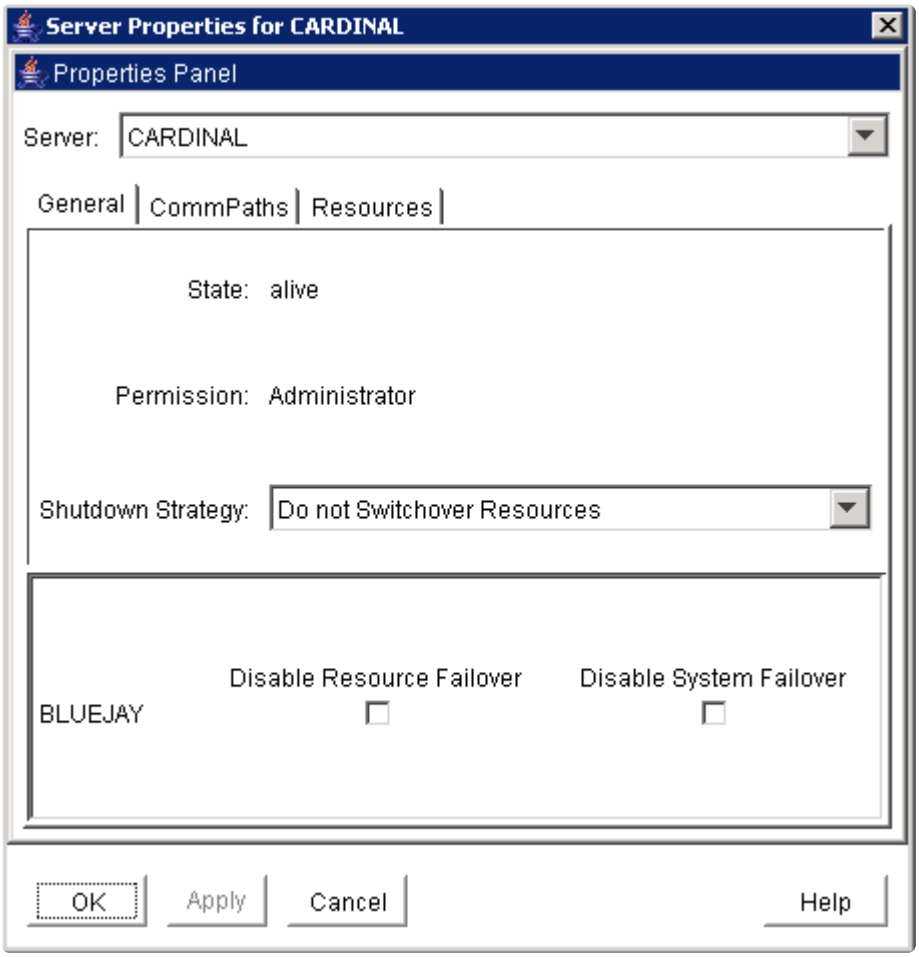
- **名前**: 選択したサーバのリソースインスタンスのタグ名。

- **アプリケーション:** リソースタイプのアプリケーション名 (gen、scsi など)。

- **リソースタイプ:** リソースタイプ。つまり、サービスを提供しているハードウェア、ソフトウェア、またはシステムエンティティのクラス (ボリュームや TCP/IP、SQL など)。

- **状態:** リソースインスタンスの現在の状態。
  - **ISP** - ローカルで稼働しており、LifeKeeper で保護されています。
  - **ISU** - ローカルで稼働していますが、ローカルリカバリは試行されません。
  - **OSF** - サービス休止中で、障害が発生しています。
  - **OSU** - サービスを休止していますが、障害は発生していません。
  - **ILLSTATE** - SIOS Protection Suite の起動シーケンスとして実行されるリソースの初期化プロセスがリソースステータスを適切に初期化していません。この状態のリソースは、SIOS Protection Suite で保護されません。
  - **UNKNOWN** - リソースの状態を特定できません。GUI サーバは使用できない可能性があります。

Server Properties – General



8.3.1.3. 自動フェイルオーバを無効にする

プライマリサーバがローカルリソースのリカバリに失敗するか、サーバが完全に停止した場合、SIOS Protection Suite は障害が発生したリソースをバックアップサーバに復元します。これが SIOS Protection Suite のデフォルトの動作です。しかし、SIOS Protection Suite で保護するリソースをリカバリサイトで自動的に起動しない方が良いこともあります。例えば、SIOS Protection Suite を WAN 環境にインストールしても、サーバ間のネットワーク接続が不安定な場合は、障害回復に不適切です。

自動フェイルオーバ機能は、デフォルトで保護対象リソースに設定されます。保護対象リソースの自動フェイルオーバを無効にするか、バックアップサーバへの自動フェイルオーバを無効にするには、［サーバプロパティ］ダイアログボックスを開き、**[一般]** タブの **[フェイルオーバ]** セクションを使用して以下の設定を行います。

クラスタ内の各サーバについて、以下の操作を行ってください。

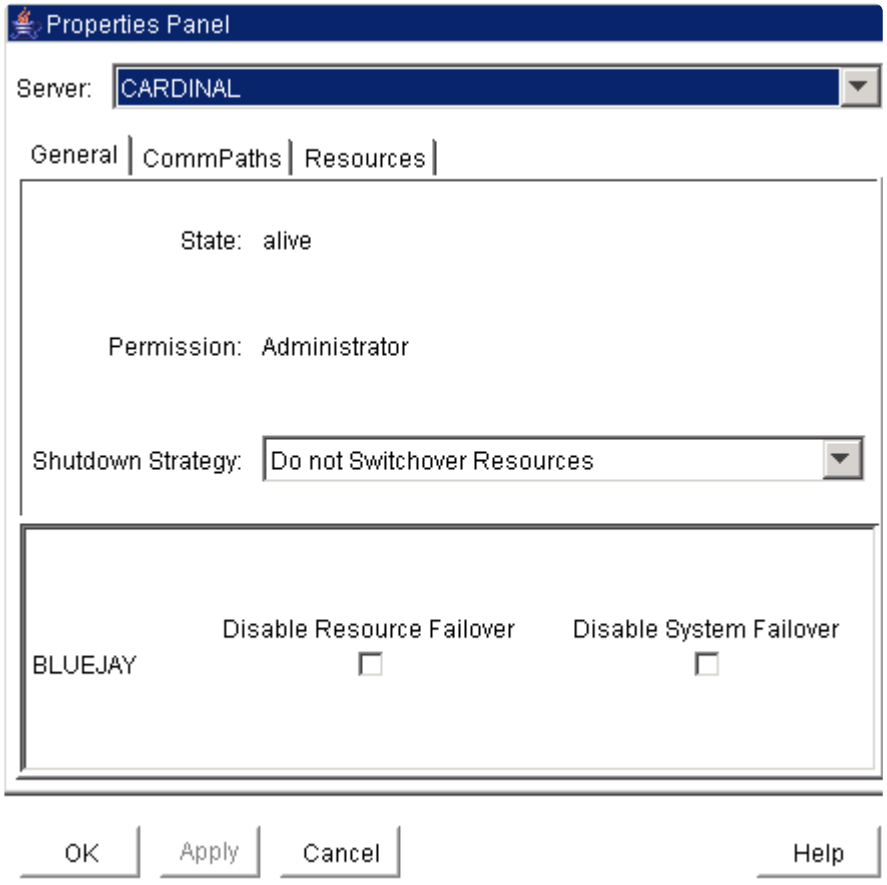
1. サーバプロパティの表示 で説明した手順に従って、**[サーバプロパティ]** ダイアログボックスを開きます。

2. **[一般]** タブをクリックします。**[サーバプロパティ]** ダイアログボックスの **[フェイルオーバ]** セクションに移動し、システムとリソースのフェイルオーバ機能を無効にするサーバを確認します。SIOS Protection Suite のフェイルオーバ機能はデフォルトで有効に設定されています。

ローカルサーバが完全に停止した際、バックアップ機能を無効にするサーバを **[システムフェイルオーバ不可]** 列から選択してください。

ローカルサーバのリソース階層に障害が発生した際、バックアップ機能を無効にするサーバを **[リソースフェイルオーバ不可]** 列から選択してください。リソースのフェイルオーバ機能は、システムのフェイルオーバ機能が無効でないと、無効に設定できません。

[適用] をクリックして、設定を反映してください。


Properties Panel
Server:
CARDINAL
General
CommPaths
Resources
State:
alive
Permission:
Administrator
Shutdown Strategy:
Do not Switchover Resources
Disable Resource Failover
Disable System Failover
BLUEJAY
OK
Apply
Cancel
Help

8.3.1.4. コミュニケーションパスの作成

SIOS Protection Suite コミュニケーションパスをサーバ間に設定する前に、ハードウェアとソフトウェアが適切にセットアップされていることを確認してください。要件については、構成 セクションを参照してください。

構成に関する注意事項

- サーバ間には、**共有ディスクコミュニケーションパスを 1 本づつ** 設定します。
- 共有ディスクコミュニケーションパスは、2 サーバ構成のクラスタだけに対応しています。
- 3 台以上のサーバでクラスタを構成する場合は、複数の TCP/IP コミュニケーションパスを使用して、ハートビートを冗長化します。TCP/IP パスには優先度を指定します。SIOS Protection Suite は優先度を参照して、リモートサーバへの TCP/IP パスを使用する順番を決定します。

重要: 通信回線 1 本に障害が発生した場合に不要なフェイルオーバが発生しないように、コミュニケーションパスを冗長化しておきます。コミュニケーションパスを 1 本だけ使用した場合、そのコミュニケーションパスに障害が発生すると、SIOS Protection Suite のリソース階層が複数サーバで同時にサービスを起動することがあります。これを「スプリットブレイン」と呼びます。また、TCP/IP コミュニケーションパスでネットワークトラフィックが増加すると、偽のフェイルオーバが発生したり、SIOS Protection Suite を正常に初期化できなくなったりするなど、予期しない問題が生じることがあります。

コミュニケーションパスの作成

1. 1 台のサーバを選択し、サーバコンテキストメニュー または サーバコンテキストツールバー の **[コミュニケーションパスの作成]** をクリックします。
2. リストボックスから 1 台以上の **リモートサーバ** を選択します。リモートサーバをクラスタに接続していないためにサーバがリストに表示されない場合は、**[サーバ追加]** をクリックして、リモートサーバを追加してください。DNS を使用するか、_/etc/hosts_ ファイルに IP アドレスを登録し、リモートとローカルのサーバの IP アドレスが解決できることを確認してください。**[次へ]** をクリックします。
3. **デバイスタイプ** として、*TCP* 、*TTY* 、または *DISK* を選択し、**[次へ]** をクリックします。
4. **デバイスタイプ** 設定に必要な情報を選択し、各手順が完了するたびに、**[次へ]** をクリックします。それぞれの設定においての詳細情報は、下記の表を参照してください。

フィールド	説明
TCP/IPコミュニケーションパス	
ハートビート間隔	ハートビート間隔 には 4 ～ 15 の値を入力して、サーバが稼働していることを確認するハートビート信号を送信する間隔を秒単位で指定します。デフォルト値は 6 です。
ハートビート最大欠落数	有効値は 3 ～ 99 です。ハートビート最大欠落数は、ハートビート信号が連続して欠落した場合、何回目でコミュニケーションパス障害と判断するかを指定します。デフォルト値は 5 です。
ローカル	コミュニケーションパスを使用するローカルサーバの IP アドレスを入力します。

IP アドレス	
優先度	ローカルサーバにおけるコミュニケーションパスの優先度を指定します。優先度は、サーバ間のコミュニケーションパスの優先順位を決定するために使用されます。優先度は 1 が最高、99 が最低です。
リモート IP アドレス	コミュニケーションパスを使用するリモートサーバの IP アドレスを入力します。
TCP ポート番号	TCP/IP サービスが使用する一意のポート番号を入力します。この番号の範囲は 1500 ～ 10000 です。SIOS Protection Suite ではデフォルト値が表示されますが、この値は変更できます。
共有ディスクコミュニケーションパス	
ハートビート間隔	ハートビート間隔 には 4 ～ 15 の値を入力して、サーバが稼働していることを確認するハートビート信号を送信する間隔を秒単位で指定します。デフォルト値は 6 です。
ハートビート最大欠落数	有効値は 3 ～ 99 です。ハートビート最大欠落数は、ハートビート信号が連続して欠落した場合、何回目でコミュニケーションパス障害と判断するかを指定します。デフォルト値は 5 です。
優先度	ローカルサーバにおけるコミュニケーションパスの優先度を指定します。優先度は、サーバ間のコミュニケーションパスの優先順位を決定するために使用されます。優先度は 1 が最高、99 が最低です。
ドライブ名	共有ディスクコミュニケーションパスに使用する共有ボリュームのドライブ名を指定します。ドライブ名は両方のサーバで統一します。

5. **[作成]** をクリックしてください。ネットワーク接続が確立したことを伝えるメッセージが表示されます。アウトプットパネルが有効な場合、メッセージはアウトプットパネルに表示されます。**[次へ]** をクリックします。

6. 複数のローカル IP アドレスまたはリモートサーバを選択し、**デバイスタイプ** に **TCP** を指定した場合は、手順 4 に戻り、次のコミュニケーションパスを作成します。複数のリモートサーバを選択し、**デバイスタイプ** を **DISK** に設定した場合は、手順 3 に戻り、次のコミュニケーションパスを設定します。

7. コミュニケーションパスの作成が完了したことを伝えるメッセージが表示されたら、**[完了]** をクリックします。

コミュニケーションパスの確認

コミュニケーションパスを確認するには、[サーバプロパティ] ダイアログボックスを使用します。ステータスが **[起動中]** であることを確認してください。

次に、GUI の右ペインにあるサーバのアイコンを確認してください。最初のコミュニケーションパスを作成した後であれば、サーバのアイコンに黄色のハートビートが表示されます。これはコミュニケーションパス 1 本が稼働中であり、冗長なコミュニケーションパスが存在しないことを示しています。	
2つのコミュニケーションパスを作成すると、サーバのアイコンが緑色のハートビートに変わります。	

コミュニケーションパスを作成してから数分が経過しても、稼働中にならない場合は、リモートサーバの名前が正しいことを確認してください。

8.3.1.5. コミュニケーションパスの削除

1. 1台のサーバを選択し、サーバコンテキストメニュー または サーバコンテキストツールバー の **[コミュニケーションパスの削除]** をクリックします。

2. 削除するコミュニケーションパスを選択し、**[コミュニケーションパスの削除]** をクリックします。

3. アウトプットパネル が有効な場合、ダイアログボックスが閉じて、コマンドの実行結果がアウトプットパネルに表示されます。すべての結果が表示されたら、**[完了]** をクリックしてダイアログボックスを閉じます。

8.3.2. リソース階層に関連する作業

このセクションでは、すべてのリソース階層に共通するタスクについて説明します。各タスクは、Core Recovery Kit とオプションのリカバリキットで共通しています。

オプションの SIOS Protection Suite リカバリキット のドキュメントは SIOS Protection Suite for Windows テクニカルドキュメンテーションから入手可能です。

リソース階層の作成

ソース階層の拡張

リソース階層の拡張解除

リソース依存関係の追加

リソース依存関係の削除

全サーバのリソース階層の削除

8.3.2.1. リソース階層の作成

1. サーバを選択します。次に、サーバコンテキストメニュー または サーバコンテキストツールバー の **[リソース階層の作成]** をクリックします。

2. **[リソース階層の作成]** ウィザードが起動し、クラスタにインストールされているリカバリキットの一覧が表示されます。リソース階層を構築してアプリケーションを保護する **リカバリキット** を選択し、**[次へ]** をクリックします。

3. 引き続きダイアログを続け、作成するリソース階層のタイプに必要なデータを入力します。

4. リソース階層が正常に作成されたことを伝えるメッセージが表示されたら、**[次へ]** をクリックして操作を続けます。問題が発生すると情報ボックスにエラーが表示され、部分的に作成されたリソース階層が削除されて、**[次へ]** ボタンが無効になります。その場合は、**[キャンセル]** をクリックして、ウィザードを終了してください。

SIOS Protection Suite のアプリケーションリソース階層

オプションのリカバリキットをインストールせずに、SIOS Protection Suite だけをインストールした場合、**[保護するアプリケーション]** の一覧には、オプションとして、**DNS** 、**共有ファイルリスト** 、**Generic Application** 、**IIS** 、**IP アドレス** 、**LAN Manager** 、**ボリューム** が表示されます。**[Generic Application]** オプションは、リカバリキットに対応していないアプリケーションを保護するときに使用してください。

選択可能なオプションについては、次の項目を参照してください。

- DNS リソース階層の作成
- ファイル共有リソース階層の作成
- Generic Application リソース階層の作成
- IP リソース階層の作成
- LAN Manager リソース階層の作成
- ボリュームリソース階層の作成

Microsoft SQL Server リカバリキット

Microsoft SQL Server Recovery Kitをインストールすると、**[保護するアプリケーション]** の一覧にエントリが追加されます。必要なリソース階層の作成方法については Microsoft SQL Server Recovery Kit 管理ガイド を参照してください。

8.3.2.1.1. DNS リソース階層の作成

DNS Recovery Kit は、仮想サーバー名のためのDNS Aレコードおよび関連するPTRレコードを生成、更新、管理する機能を提供します。DNSリソースでは、フェイルオーバまたはスイッチオーバの発生時に関連付けられる、仮想サーバー名とIPアドレスを管理された形で構成することができます。

下記の表は、サービス中の稼働系もしくはバックアップのクラスターノードで、管理下にあるサーバー名（SQLSERVER）のDNSで起きる変更の例です。この例では、稼働系ノードの公開IPアドレスは172.17.10.24で、バックアップノードの公開IPアドレスは172.16.10.25です。管理下にある仮想サーバー名、SQLSERVERは、どちらのLifeKeeper nodeが稼働しているかにしたがって、そのIPアドレスを変更します。

```
Zone: mydomain.com
```

サービスの稼働系ノード(スイッチオーバもくしくは、フェイルオーバ前)

A レコード_	SQLSERVER	172.17.10.24
PTR レコード	25.10.16.172.in-addr.arpa	SQLSERVER.mydomain.com

バックアップノードでサービス中(スイッチオーバもしくは、フェイルオーバ後)

A レコード	SQLSERVER	172.17.10.25
PTR レコード	25.10.16.172.in-addr.arpa	SQLSERVER.mydomain.com

プライマリサーバ上で DNS リソース階層を作成するには、次の手順に従ってください。

1. サーバを選択します。次に、サーバコンテキストメニュー または サーバコンテキストツールバー の **[リソース階層の作成]** をクリックします。

2. **[保護するアプリケーションを作成]** ウィンドウが起動し、**プライマリ** サーバおよび **バックアップ** サーバが表示されます。この設定を行う正しいシステムを選択します。

3. クラスタにインストールされているすべてのリカバリキットの一覧が表示されます。*DNS* を選択し、**[次へ]** をクリックします。

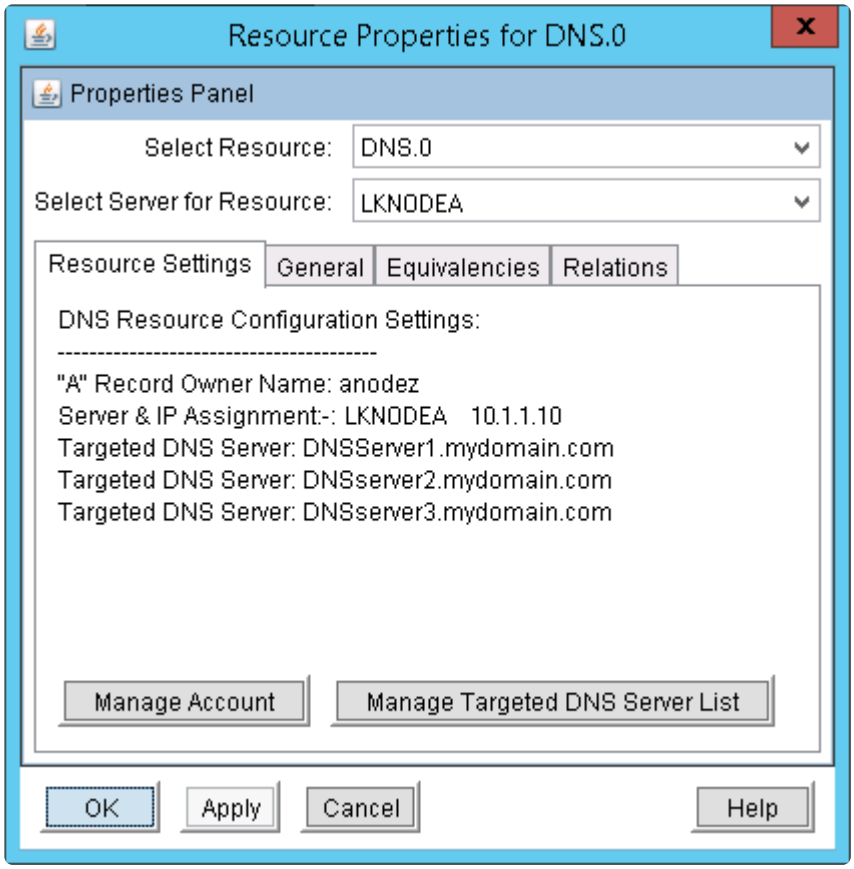
4. **[保護するアプリケーションを作成]** ウィンドウに従って、下表の情報を入力します。

5. リソース階層が無事、プライマリーノード上に生成されたとのメッセージが表示されたら、**[次へ]** をクリックし、DNSリソースをバックアップノードへも拡張します。

フィールド	説明

リソースDNSタグ	作成する DNS リソースインスタンスの一意のタグ名を選択するか入力します。このフィールドには、デフォルトのタグ名が表示されます。このタグ名は変更できます。 **注意：**タグ名に使用できる文字はASCII印字可能文字のみです。
_Aレコード_のオーナー名	DNSで更新されるAレコードとPTRレコードの仮想サーバー名を入力します。このサーバー名の入力では、サーバーの完全修飾ドメイン名ではなく、NetBIOSのコンピュータ名を使用してください。
IP アドレス	DNSリソースがこのノードでサービス中に仮想サーバー名にアサインするIPアドレスを入力してください。このIPアドレスは、通常、LifeKeeperノードの公開IPアドレスです。この IP アドレスにマップされる A レコードは、フェイルオーバまたは手動切り替え時に更新されます。
DNSサーバ名(完全修飾ドメイン名)	DNSリソースレコードを変更する DNS サーバの完全修飾ドメイン名 (FQDN) を< DNS Server Name> <mydomain.com> 形式で入力します。もし、複数のDNSサーバが構成される場合には、名前をスペースで区切ってください。サービス中は、少なくとも一つ以上のDNSサーバが、常に、プライマリ、もしくはバックアップ用のLifeKeeperノードのサーバーからアクセスできなくてはなりません。そのDNS サーバは、可能であれば、同じサイトのプライマリサーバからアクセスできるようにします。ターゲットとなるDNSサーバのリストはそれぞれのLifeKeeperノードにおいて同じ場合もあれば、異なる場合もあります。同じDNS環境の他のネームサーバ (NS) のレコードもフェイルオーバまたは手動切り替えの発生時に更新されます。 DNSサーバリソースの生成の際には、DNSサーバーの全リストを用意する必要はありません。LifeKeeperは、DNSリソースの生成時には全リストの内のサーバの一つに接続できれば、正しく構成されているほかのDNSサーバーを検出します。
DNS管理ユーザ名	Windows DNS/ドメイン管理者のユーザ名を入力します。このユーザアカウントには DNS 設定を変更する権限が必要です。ユーザは、DNS サーバと同じドメインの「Domain Admins」グループに属している必要があります。ユーザ ID は <DomainName>\<UserID> 形式で入力します。<DomainName> はドメインの NetBIOS 名です。
DNS管理者のパスワード	Windows DNS/ドメイン管理者アカウントのパスワードを入力します。

各サーバにおけるDNSリソースの構成を変更する場合は、DNSリソースを右クリックし、[プラパティ] を選択すると、現在のDNSリソース構成が下記のように表示されます。



各クラスタノードにおけるDNSリソースの構成がすぐに検出され、上記の[リソースのサーバを選択]から対象となるLifeKeeperクラスタノードを選択することで変更が可能です。

リソース構成には下記のオプションが含まれます：

・DNS/Domain Account IDおよび、もしくはDNS更新に使われるパスワード

・対象となるDNS Server Name List の管理（追加もしくは削除）

管理対象となるDNSリソースを監視するDNSのDeep Check Scriptは、対象となるDNSサーバ（最初に接続されたサーバ）の管理されるサーバー名のAレコードの有無をチェックし、その後、検出されDNS（NS）サーバについてもチェックします。もし、正しいIPアドレスへマップされたAレコードが少なくとも一つ以上のDNSサーバーについて見つからない場合、Deep Check ScriptはFailし、ローカルリカバリ（有効な場合）をトリガし、AレコードおよびPRTレコードが対象となる検出されたDNS（NS）サーバーに対して再生成されます。

もしローカルリカバリがそのDNSサーバで無効とされている場合、もしくは有効とされていて機能しなかった場合は、フェールオーバします。

8.3.2.1.2. ファイル共有リストリソース階層の作成

ファイル共有は Windows 版のファイルマネージャで定義します。SIOS Protection Suite LAN Manager Recovery Kit をインストールすると、ファイル共有を含めたファイル共有リストリソースを作成できます。

ファイル共有リストリソースの条件

利用できないファイル共有もあります。次の説明を参考にして、利用可能なファイル共有を判断してください。

- 共有名はサーバが共有するボリュームに設定します。
- 2 台のサーバにファイル共有リソースを作成すると、共有ボリュームは自動的に保護されます。しかし、3 台目以降のサーバは、ファイル共有階層を拡張しないと、ファイルを共有できません。
- 2 台目のサーバに共有名をすでに設定している場合、共有名は同じディレクトリを指す必要があります。
- いずれか一方のサーバで共有名が保護されている場合、その共有名は使用できません。
- 管理者は、作成した共有名がディレクトリを指すことを確認します。ディレクトリに共有名を作成した後でも、そのディレクトリを削除できます。ディレクトリを削除した場合は、共有名を削除したことを確認してください。

> **注記:** バックアップサーバでファイル共有リソースを起動すると、共有が有効になります。階層を削除しても、ファイル共有は削除されません。

ファイル共有リストリソースの作成

ファイル共有リソースを作成するには、次の手順に従ってください。

1. サーバを選択します。次に、サーバコンテキストメニュー または サーバコンテキストツールバー の **[リソース階層の作成]** をクリックします。
2. **[保護するアプリケーションを作成]** ウィンドウが起動し、**プライマリ** サーバおよび **バックアップ** サーバが表示されます。まだ選択していない場合は、設定のための適切なシステムを選択してください。
3. クラスタにインストールされているすべてのリカバリキットの一覧が表示されます。**[ファイル共有リスト]** を選択し、**[次へ]** をクリックします。
4. **設定ウィザード** で、以下の情報を入力します。ダイアログボックスの **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは特に、前に入力した情報の訂正が必要なエラーが発生した場合に役立ちます。階層の作成手順の間に **[キャンセル]** をクリックすると、SIOS Protection Suite は作成プロセス全体を取り消します。

フィール	説明

ド	
共有ファイルとパス名	保護する共有ファイルを選択します。複数のファイルを選択できます。ファイルが表示されない場合は、ファイル共有を指定したボリュームが SIOS Protection Suite で保護されているか確認してください。
共有ファイルリストリソースタグ	作成するファイル共有リストリソースインスタンスに一意のタグを選択または入力します。このフィールドには、デフォルトのタグ名 FSList.x が自動的に表示されます。x は SIOS Protection Suite が割り当てる値で、開始番号が自動的に入ります。タグ名は変更できます。**注意：**タグ名に使用できる文字はASCII印字可能文字のみです。

5. データの入力を完了すると、**[次へ]** ボタンが表示されます。**[次へ]** をクリックすると、リソース階層の作成と検証が実行されます。

6. リソース階層が正常に作成されたことを伝えるメッセージが表示されたら、*[次へ]* をクリックして操作を続けます。問題が発生すると情報ボックスにエラーが表示され、部分的に作成されたリソース階層が削除されて、**[次へ]** ボタンが無効になります。その場合は、**[キャンセル]** をクリックして、**ウィザード** を終了してください。

8.3.2.1.3. Generic Application リソース階層の作成

このオプションでは、対応するリカバリキットのアプリケーションを保護します。

リソース階層を作成する前に

1. 最初に、SIOS Protection Suite の 5 つの基本的な動作を制御するスクリプトを用意します。

    - restore
    - remove
    - quickchk (クイックチェック)
    - deepchk (ディープチェック)
    - ローカルリカバリ

    各スクリプトの Perl 版と VB 版のテンプレートが *$LKROOT\admin\kit\app\templates* に格納されています。テンプレートをカスタマイズしてテストするときは、*$LKROOT* と同じボリューム上の別のディレクトリにコピーしてください。

    注記: オプションの **Create** 、**Extend** 、**Delete** スクリプトを使用する場合は、他のスクリプトと一緒に前記のフォルダにコピーしてください。スクリプト選択ウィザードは、追加されたスクリプトの名前と拡張子を調べ、スクリプトを自動的に登録します。

    注記: Generic Application ソリューションでは、restore と remove スクリプトが必要です。restore または remove スクリプトが完了するまでの継続時間に制限はありませんが、この継続時間により、次の影響があります。restore スクリプトが正常に完了するまで、サービス中のリソースに対する操作を完了することができません。アクティブサーバ上のリソースに対する remove スクリプトが正常に完了するまで、リソースに対するスタンドバイサーバ上へのスイッチオーバ操作を続行することができません。

    注記: クイックチェックとディープチェックスクリプトを使用する場合、そのスクリプトはユーザ指定の時間間隔で実行されます。重複を回避するには、クイックチェックとディープチェックスクリプトの継続時間を、ユーザ指定の時間間隔より短くしてください。ローカルリカバリスクリプトも使用することができます。クイックチェックまたはディープチェックスクリプトに障害が発生し、ローカルリカバリスクリプトを使用する場合、クイックチェックまたはディープチェックの継続期間を延長し、ユーザ指定の時間間隔を超えないようにしてください。

2. ボリュームや IP アドレスなど、他のリソースに依存するアプリケーションでは、リソースを個別に作成した後、Generic Ark でリソース階層を作成します。依存関係を後から作成するには、[依存関係の追加] ダイアログボックスを使用してください。

リソース階層の作成

基本スクリプトを用意したら、Generic Ark を使用して、アプリケーションのリソース階層を作成してください。

1. サーバを選択します。次に、サーバコンテキストメニュー または サーバコンテキストツールバー の **[リソース階層の作成]** をクリックします。

2. **[保護するアプリケーションを作成]** ウィンドウが起動し、**プライマリ** サーバおよび **バックアップ** サーバが表示されます。まだ選択していない場合は、設定のための適切なシステムを選択してください。**[次へ]** をクリックします。

3. クラスタにインストールされているすべてのリカバリキットの一覧が表示されます。**[Generic Application]** を選択し、**[次へ]** をクリックします。

4. **設定ウィザード** で、以下の情報を入力します。**注記:** ダイアログボックスの **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは特に、前に入力した情報の訂正が必要なエラーが発生した場合に役立ちます。階層の作成手順の間に **[キャンセル]** をクリックすると、SIOS Protection Suite は作成プロセス全体を取り消します。

フィールド	説明
Restore スクリプト	アプリケーションに使用する **restore スクリプト** のパス名とファイル名を入力します。このスクリプトはアプリケーションを起動します。restore スクリプトのテンプレートは、templates ディレクトリにあります。restore スクリプトは、稼働中のアプリケーションに影響を与えてはなりません。
スクリプトの削除	アプリケーションに使用する **remove スクリプト** のパス名とファイル名を入力します。このスクリプトはアプリケーションを停止します。restore スクリプトのテンプレートは、templates ディレクトリにあります。
クイックチェックスクリプト [オプション]	アプリケーションに使用する **QuickCheck スクリプト** のパス名を入力します。このスクリプトはアプリケーションを監視します。quickCheck スクリプトのテンプレートは、templates ディレクトリにあります。
ディープチェックスクリプト [オプション]	アプリケーションに使用する **DeepCheck スクリプト** のパス名を入力します。deepCheck スクリプトは、quickCheck スクリプトより詳細に保護対象アプリケーションを監視します。deep check スクリプトのテンプレートは、templates ディレクトリにあります。
ローカルリカバリ [オプション]	アプリケーションで使用する **ローカルリカバリスクリプト** のパス名を入力します。このスクリプトは、障害が発生したアプリケーションをローカルサーバに復旧します。recover スクリプトのテンプレートは、templates ディレクトリにあります。
アプリケーション情報 (オプション)	任意の **アプリケーション情報** を入力します。restore、remove、recover、quickCheck スクリプトに必要なアプリケーションに関する情報をオプションとして入力します。
リソースタグ名	このフィールドには、デフォルトのタグ名 *App.x* が自動的に表示されます。x は SIOS Protection Suite が割り当てる値で 、*0* から始まります。 **注意：**タグ名に使用できる文字はASCII印字可能文字のみです。

5. データの入力を完了すると、**[インスタンスの作成]** ボタンが表示されます。**[インスタンスの作成]** をクリックすると、SIOS Protection Suite はリソース階層の作成と検証を実行します。

6. リソース階層が正常に作成されたことを伝えるメッセージが表示されたら、**[次へ]** をクリックして操作を続けます。問題が発生すると情報ボックスにエラーが表示され、部分的に作成されたリソース階層が削除されて、*[次へ]* ボタンが無効になります。その場合は、**[キャンセル]** をクリックして、**ウィザード** を終了してください。

8.3.2.1.4. LAN Manager リソース階層の作成

LAN Manager Recovery Kit は、共有ファイルを持つコンピュータに別名を作成します。コンピュータの別名とは、「切り替え可能」なコンピュータ名を指します。コンピュータの別名は「切り替え可能」なコンピュータ名として機能し、SIOS Protection Suite の LAN Manager　階層が in service であるシステム上で、対応するファイル共有が使用可能になります。IP アドレスも LAN Manager 階層の一部としてコンピュータの別名に関連付けることができます。

1. サーバを選択します。次に、サーバコンテキストメニュー または サーバコンテキストツールバー の **[リソース階層の作成]** をクリックします。

2. **[保護するアプリケーションを作成]** ウィンドウが起動し、**プライマリ** サーバおよび **バックアップ** サーバが表示されます。まだ選択していない場合は、設定のための適切なシステムを選択してください。**[次へ]** をクリックします。

3. クラスタにインストールされているすべてのリカバリキットの一覧が表示されます。**[LAN Manager]** をクリックし、**[次へ]** をクリックします。

4. **設定ウィザード** で、以下の情報を入力します。ダイアログボックスの **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは特に、前に入力した情報の訂正が必要なエラーが発生した場合に役立ちます。階層の作成手順の間に **[キャンセル]** をクリックすると、SIOS Protection Suite は作成プロセス全体を取り消します。

フィールド	説明
コンピュータの別名	コンピュータの別名を入力するか、SIOS Protection Suite から提供されるデフォルト名を使用します。
LAN Manager リソースタグ	作成している LAN Manager リソースインスタンスの一意のタグ名を選択するか入力します。このフィールドには、前記の操作で入力したコンピュータの別名がデフォルトとして表示されます。別名は変更できます。 **注意：**タグ名に使用できる文字はASCII印字可能文字のみです。

5. データの入力を完了すると、**[次へ]** ボタンが表示されます。**[次へ]** をクリックすると、SIOS Protection Suite はリソース階層の作成と検証を実行します。

6. リソース階層が正常に作成されたことを伝えるメッセージが表示されたら、**[次へ]** をクリックして操作を続けます。問題が発生すると情報ボックスにエラーが表示され、部分的に作成されたリソース階層が削除されて、**[次へ]** ボタンが無効になります。その場合は、**[キャンセル]** をクリックして、**ウィザード** を終了してください。

8.3.2.1.5. ボリュームリソース階層の作成

共有 SCSI ディスク上のリソースを保護するには、Windows のディスク管理ツールを使用して、共有ディスクを論理ボリュームに分割します。ボリュームリソースインスタンスを定義すると、SIOS Protection Suite で共有ボリュームを保護できます。インスタンスにはドライブレターを指定します (例: G:)。

SIOS Protection Suite は、ボリュームリソースインスタンスをプライマリサーバで起動した後、ソフトウェアロックをかけます。その結果、ボリュームがプライマリサーバでアクティブな限り、バックアップサーバはボリュームにアクセスできません。プライマリサーバに障害が発生すると、SIOS Protection Suite はボリュームリソースをバックアップサーバで起動し、修復中のプライマリサーバがボリュームリソースにアクセスできないようにロックします。

SIOS Protection Suite は、プライマリとバックアップを入れ替えるため、障害が発生したサーバは、ボリュームリソースにアクセスできなくなります。そのため、障害が発生したサーバを修理している間は、不適切なアクセスからリソースを保護できます。

SIOS Protection Suite のインテリジェントスイッチバック機能は、プライマリサーバとバックアップサーバを動的に再定義します。そのために、修理が完了したら、適当なタイミングを指定して、修復したサーバでリソースを起動できます。

ボリュームリソースを作成するには、次の手順に従ってください。SIOS Protection Suite はボリュームロックを保持するため、ボリュームリソースを作成した後は、SIOS Protection Suite を停止しないでください。

注記: ミラーボリュームリソースを作成して拡張する前に、SIOS Protection Suite クラスタシステムに接続している DataKeeper GUI プロセスを必ず終了してください。

1. サーバを選択します。次に、サーバコンテキストメニュー または サーバコンテキストツールバー の **[リソース階層の作成]** をクリックします。

2. **[保護するアプリケーションを作成]** ウィンドウが起動し、**プライマリ** サーバおよび **バックアップ** サーバが表示されます。まだ選択していない場合は、設定のための適切なシステムを選択してください。

3. クラスタにインストールされているすべてのリカバリキットの一覧が表示されます。ダイアログボックスの **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは特に、前に入力した情報の訂正が必要なエラーが発生した場合に役立ちます。階層の作成手順の間に **[キャンセル]** をクリックすると、SIOS Protection Suite は作成プロセス全体を取り消します。

フィールド	説明
ボリューム	保護対象のボリュームを選択します。「見つかりません」と表示される場合は、そのボリュームが SIOS Protection Suite で保護されていることを確認してください。
ボリュームタグ	ボリュームタグはリソース識別子を指定します。SIOS Protection Suite がデフォルトのボリュームタグ名「Volume.X」を割り当てます。X は、ドライブレターです。タグ名は変更できますが、一意でなければなりません。

	注意：タグ名に使用できる文字はASCII印字可能文字のみです。

4. データの入力を完了すると、**[次へ]** ボタンが表示されます。**[次へ]** をクリックすると、SIOS Protection Suite はリソース階層の作成と検証を実行します。

5. リソース階層が正常に作成されたことを伝えるメッセージが表示されたら、**[次へ]** をクリックして操作を続けます。**[ボリュームリソースの拡張ウィンドウ]** が表示されます。この手順を完了させるための詳細情報については、ヘルプトピックの ボリュームリソースの拡張 を参照してください。

6. 問題が発生すると情報ボックスにエラーが表示され、部分的に作成されたリソース階層が削除されて、**[次へ]** ボタンが無効になります。その場合は、**[キャンセル]** をクリックして、**ウィザード** を終了してください。

ボリュームリソース作成後の作業

SIOS Protection Suite ボリュームを作成するか削除した場合は、SIOS Protection Suite で保護するボリュームに次のコマンドを実行します。

```
chkntfs /x <vol_1> <vol_2> … <vol_n>
```

この Windows のコマンドは、システムの起動時に chkdsk のチェック対象となるボリュームのリストから、指定したボリュームを除外します。SIOS Protection Suite で保護するボリューム (特にバックアップシステム上のボリューム) は、LifeKeeper が起動するまでアクセスできないように、上記のコマンドで除外する必要があります。chkntfs /d コマンドは、SIOS Protection Suite ボリュームがないと、Windows のデフォルト設定を復元します。

> ! `chkntfs /x` コマンドは前回実行対象となったボリュームを記憶していないため、ユーザがこのコマンドを実行すると SIOS Protection Suite の設定が無効になります (同様に SIOS Protection Suite がユーザ設定を上書きしてしまう可能性があります)。システム起動時に SIOS Protection Suite 以外のボリュームをチェック対象から外す場合は、すべての SIOS Protection Suite ボリュームを `chkntfs /x` コマンドに指定してください。

8.3.2.1.6. IP アドレスリソース階層の作成

SIOS Protection Suite は切り替え可能なローカル IP アドレスを監視し、障害を検出すると、同じシステム上の別のネットワークアダプタに IP アドレスを移動します。切り替え可能な IP アドレスを使用すると、リソース階層全体をバックアップサーバにフェイルオーバすることを回避できます。

IP ローカルリカバリ機能には、システム設定に関する次の要件と制限があります。

IP ローカルリカバリの要件

IP ローカルリカバリでは、サーバ上で SIOS Protection Suite が保護する各 IP アドレスに *1* つ のバックアップネットワークインターフェースを指定できます。バックアップインターフェースを正常に機能させるには、プライマリインターフェースと同じ物理ネットワークに接続する必要があります。システム管理者は有効なインターフェースを選択する必要があります。バックアップインターフェースは 1 台のサーバに指定します。他のクラスタサーバに指定しても意味がありません。つまり、1 台のサーバでバックアップインターフェースを選択しても、他のサーバのバックアップインターフェースの選択には影響しません。

バックアップアダプタはローカルリカバリアダプタとも呼ばれ、プライマリアダプタに障害が発生すると、切り替え可能なアドレスがアクティブになります。バックアップアダプタを設定するには、次の手順に従ってください。

- 2 つのアダプタを同じ物理サブネットに接続します。
- ローカルリカバリアダプタの全アドレスは、適切にルーティングできるように、プライマリアダプタの実アドレスと異なる論理サブネット上に置く必要があります。また、プライマリアダプタに設定して SIOS Protection Suite で保護する仮想 IP アドレスとは異なる論理サブネットに置く必要があります。
- IP ローカルリカバリ機能を使用するには、ネットワークにゲートウェイを設置します。具体的には、システムの TCP/IP 設定の [デフォルトゲートウェイ] フィールドに、ネットワークゲートウェイのアドレスを指定します。ローカルリカバリアダプタにも同じネットワークゲートウェイを設定します。
- IP ローカルリカバリ機能は、IP リソースを作成する際に有効にすることができます。IP リソースを作成した後、リソース属性を変更しても、ローカルリカバリ機能を IP リソースに追加できません。
- IP リソースの IP ローカルリカバリ機能を無効にするには、「ins_setlocalrecovery」コマンドラインユーティリティを使用してください。このユーティリティは、LifeKeeper の *¥bin* ディレクトリ (デフォルトで `C:\LK\bin`) に格納されています。このユーティリティの使用方法とオプションの説明を参照するには、コマンドプロンプトから「 ins_setlocalrecovery 」を実行してください。

SIOS Protection Suite 階層に IP アドレスリソースを作成して使用する場合は、ネットワーク構成の確認 の説明に従ってネットワークを設定し、テストしてください。

設定が完了したら、ping を打ち、仮想 IP アドレスが一意なことを確認します。仮想 IP アドレスは必須ではありませんが、IP アドレス階層を作成すると、自動的に作成されます。

IP アドレスのリソース階層をプライマリサーバに作成するには、次の手順に従ってください。

1. サーバを選択します。次に、サーバコンテキストメニュー または サーバコンテキストツールバー の **[リソース階層の作成]** をクリックします。

2. **[保護するアプリケーションを作成]** ダイアログが起動し、クラスタにインストールされているリカバリキットの一覧が表示されます。**[IP アドレス]** をクリックし、**[次へ]** をクリックします。

3. **ウィザード** の指示に従って、以下の情報を入力します。ダイアログボックスの **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは特に、前に入力した情報の訂正が必要なエラーが発生した場合に役立ちます。階層の作成手順の間に **[キャンセル]** をクリックすると、SIOS Protection Suite は作成プロセス全体を取り消します。

フィールド	説明
IP アドレス	SIOS Protection Suite がリソースに使用する仮想 IP アドレスを指定します。クライアントアプリケーションは、この IP リソースを使用して、特定のネットワークインターフェースを介して親アプリケーションにログインします。
サブネットマスク	TCP/IP リソースがターゲットサーバで使用する IP サブネットマスクを指定します。TCP/IP リソースのアドレスクラスに対応した標準的なネットマスクを指定できます。**注記:** TCP/IP リソースが使用するサブネットは、ここで選択したサブネットマスクと前記の IP アドレスによって決まるため、ネットワーク設定を統一する必要があります。
IP リソースタグ	作成している IP リソースインスタンスの一意の IP リソースタグ名を選択するか入力します。このフィールドには、リソース名または IP アドレスに一致するデフォルトのタグ名が自動的に設定されます。タグ名は変更できます。 **注意：**タグ名に使用できる文字はASCII印字可能文字のみです。
ネットワーク接続	物理的なイーサネットカードの IP アドレスを指定します。既存のネットワーク設定、および TCP/IP リソースのアドレスやネットマスクの値をもとに、適切なカードを選択します。デフォルト値には、前のダイアログボックスで選択したアドレスとネットマスクに最も近い IP アドレスが使用されます。
ローカルリカバリのネットワーク接続	ローカルリカバリを有効にした場合、バックアップインターフェースとして使用するネットワーク接続を選択する必要があります。バックアップサーバに NIC がなければ、プライマリサーバの NIC を指定します。

4. データの入力が完了すると、**[次へ]** ボタンが表示されます。[次へ] をクリックすると、SIOS Protection Suite はリソース階層の作成と検証を実行します。

5. リソース階層が正常に作成されたことを伝えるメッセージが表示されたら、**[次へ]** をクリックして操作を続けます。問題が発生すると情報ボックスにエラーが表示され、部分的に作成されたリソース階層が削除されて、**[次へ]** ボタンが無効になります。その場合は、**[キャンセル]** をクリックして、**ウィザード** を終了してください。

注記: チーミングソフトウェアを使用するか、仮想 IP リソースを作成した後、ネットワークカードを変更すると、仮想 IP リソースがいったん削除され、ネットワークカードのインデックス番号を反映した IP リソースが再作成されます。

8.3.2.1.6.1. IP ローカルリカバリのシナリオ

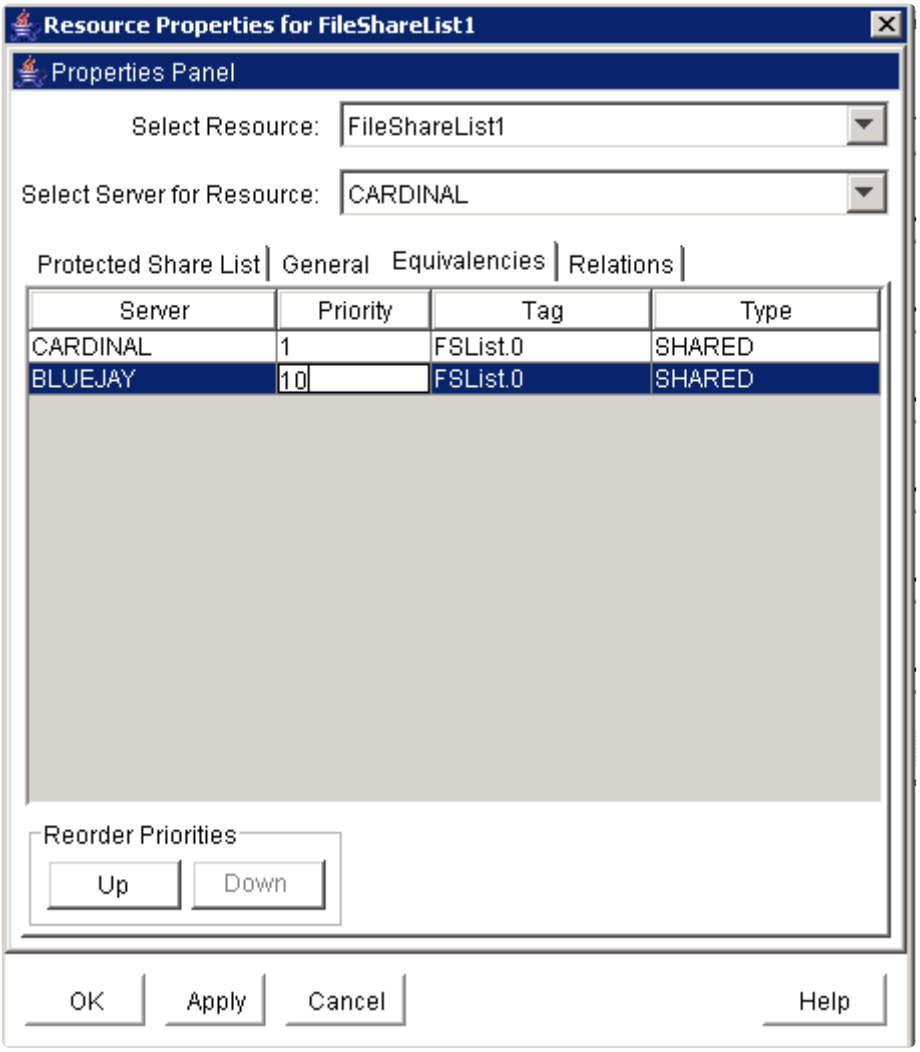
IP ローカルリカバリ機能を有効にした場合、定期的に実行する IP リソースのクイックチェック、またはディープチェックテストが失敗すると、SIOS Protection Suite は次の処理を実行します。

- 現在のネットワークインターフェースで IP アドレスを起動します。
- 前記の処理に失敗すると、リソースインスタンスをチェックし、バックアップインターフェースが使用できるかどうかを調べます。バックアップインターフェースが使用できる場合は、IP アドレスをバックアップインターフェースに移動します。
- ローカルリカバリが完全に失敗すると、SIOS Protection Suite は、IP アドレスと依存リソースをバックアップサーバにフェイルオーバします。

ローカルリカバリ機能は、バックアップアダプタがなくても有効にすることができます。ローカルリカバリ機能を有効にすると、SIOS Protection Suite はプライマリネットワークのインターフェースを再起動しますが、それに失敗すると、リソースをバックアップサーバにフェイルオーバします。

8.3.2.1.7. リソース優先度の編集

リソース階層を定義したサーバの優先度は、編集したり並び替えたりすることができます。最初に、リソースプロパティの表示 で説明した手順に従って、**[リソースのプロパティ]** ダイアログボックスを開いてください。**[リソースのプロパティ]** ダイアログボックスが開き、選択したサーバのリソースの優先度が **[イクイバレンシ]** タブに表示されます (次図)。



優先度は次の方法で変更できます。

- **[上へ]** または **[下へ]** をクリックしてイクイバレンシを移動し、優先度を並び替える。
- 優先度を直接編集する。

[上へ] ボタンと [下へ] ボタンの使用

1. **イクイバレンシ** 表の行をクリックして、イクイバレンシを選択します。選択したイクイバレンシに応じて、**[上へ]** ボタンまたは **[下へ]** ボタンが有効になります。**[上へ]** は優先度が最高のサーバ以外を選択すると有効になります。**[下へ]** は優先度が最低のサーバ以外を選択すると有効になります。

2. **[上へ]** または **[下へ]** をクリックし、イクイバレンシを優先順位リスト内で移動します。

優先度自体は変わりませんが、イクイバレンシが表内を上下に移動します。

優先度の編集

1. **イクイバレンシ** 表の **[優先度]** 列にある優先度をクリックして優先度を選択します。優先度の近くにボックスが表示され、値がハイライト表示されます。

2. 優先度を入力し、**Enter** キーを押します。

   注記: 優先度の有効値は **1** ～ **999** です。

   優先度の編集が完了すると、**イクイバレンシ** 表が並び替えられます。

変更内容の適用

イクイバレンシ 表の優先度を並び替えたら、**[適用]** または **[OK]** をクリックして、変更内容を反映してください。**[適用]** をクリックすると、変更が反映されます。**[OK]** をクリックすると、変更内容が適用されてウィンドウが閉じます。**[キャンセル]** をクリックすると、**[適用]** をクリックした後に変更した内容を保存せずにウィンドウが閉じます。

8.3.2.1.7.1. 不完全なリソース優先度の変更

SIOS Protection Suite の階層は、リソースに親子関係を割り当てて定義します。リソースが複数の親を持つ場合、階層の全ルートを表示しても、親リソースを簡単に見つけられません。階層の整合性を保持するために、SIOS Protection Suite は優先度の変更を全クラスタサーバに反映します。GUI は、**[OK]** または **[適用]** がクリックされると、選択された階層の全ルートを表示して、優先度を統一することを要求します。この時点では、すべてのルートを受け入れるか、操作を取り消します。ルートの一覧を受け入れると、新しい優先度が階層内の全リソースに適用されます。

[リソースプロパティ] ダイアログボックスが表示されている間は、階層に対してその他の変更を行わないでください。**[リソースプロパティ]** ダイアログボックスで優先度を編集する前に、SIOS Protection Suite に加えた変更は、このダイアログボックスに動的に反映されます。SIOS Protection Suite で優先度を変更しても、ダイアログボックスの値は変更されません。**[適用]** または **[OK]** をクリックすると、優先度を変更したことを伝えるメッセージが表示されて、操作が一時的に止まります。

複数の優先度を一括して変更し、回復不能なエラーが発生しないように、SPSは 1 回の操作で、サーバ 1 台に 1 件づつ優先度を変更します。また、優先度が競合しないように、ユーザが指定した変更を暫定値として扱います。暫定値として最大値 999 を超える値を許容し、ユーザが優先度を変更している間、暫定値を GUI に表示します。優先度の変更操作が完了すると、暫定値はユーザが要求した値に置換されます。エラーが発生して、優先度がロールバックできない場合、暫定値が残ることがあります。このようなエラーが発生した場合は、次の手順に従って、階層を修復してください。

階層の一貫性を復元する

優先度の変更中にエラーが発生し、操作を完了できなかった場合、優先度に矛盾が生じます。エラーは、システムやコミュニケーションパスの障害など、さまざまな原因で発生します。優先度の変更操作を開始してから、操作を完了する前にエラーが発生し、前の状態にロールバックできない場合、その旨を通知するメッセージが表示されます。こうした状態が発生した場合は、次の手順に従って、階層の一貫性を回復してください。

1. 可能な限り、問題の原因を突き止めてください。システムやコミュニケーションパスに障害が発生していないか調べてください。優先度管理プログラムの実行中に、別の操作を同時に実行しなかったことを確認してください。

2. 操作を続ける前に、問題を可能な限り解決してください。例えば、階層を復元する前に、障害が発生したシステムやコミュニケーションパスを修復します。

3. **[リソースプロパティ]** ダイアログボックスを使用して、優先度の変更を再試行してください。

4. **[リソースプロパティ]** ダイアログボックスで優先度を変更できない場合は、hry_setpri をコマンドラインから実行して、階層を修復してください。hry_setpri スクリプトを使用すると、GUI を介さずに、サーバごとに優先度を変更できます。

5. 修復作業を完了したら、すべてのクラスタサーバに eqv_list コマンドを実行し、各サーバ上の構成データベースが整合していることを確認し、各サーバが返す優先度を調べてください。

6. 以上の操作でも階層を修復できない場合は、最後の手段として、階層を削除して再作成してください。

8.3.2.1.8. リソースプロパティの編集

1. リソースのプロパティを編集するには、リソースプロパティの表示 と同じ手順で **[リソースのプロパティ]** ダイアログボックスを開きます。

2. 適切なアクセス権でサーバにログインすると、次の項目を編集できます。

    - スイッチバックタイプ
    - リソース設定 (*特殊な構成を設定したリソースのみ*)
    - リソースのプロパティ

3. 編集が完了すると、**[適用]** ボタンが有効になります。このボタンをクリックすると、変更内容が反映されます。

4. 作業が完了したら、**[OK]** をクリックして、変更内容を保存してウィンドウを閉じるか、**[キャンセル]** をクリックして、変更を適用せずに、ウィンドウを閉じます。

8.3.2.2. リソース階層の拡張

SIOS Protection Suite の [Extend Resource Hierarchy] オプションを使用すると、既存のリソース階層を別のサーバにコピーし、同じリソース階層をコピー先のサーバに作成できます。リソース階層を他のサーバに拡張すると、カスケーディングフェイルオーバが可能になります。コピー元のリソース階層を持つサーバをテンプレートサーバ、リソース階層を拡張するサーバをターゲットサーバと呼びます。

ターゲットサーバは拡張した階層を起動し、アクティブなコミュニケーションパスを介して、他のリモートサーバ上のイクイバレンシと通信できなければなりません。つまり、既存のリソース階層に関連付けたリカバリキットは、ターゲットサーバを含めて階層が常駐する全サーバにインストールする必要があります。

注記: 新しいリソース階層を作成すると、階層を拡張するかどうかを確認するメッセージが表示されます。

1. 既存のリソース階層を拡張する場合は、拡張するリソース階層を選択し、リソースコンテキストメニュー または リソースコンテキストツールバー の **[Extend Resource Hierarchy]** をクリックします。

2. **バックアップサーバ** を選択し、**[次へ]** をクリックします。

3. SIOS Protection Suite による拡張事前検査の結果がダイアログボックスに表示されます。検査に成功した場合は、拡張事前検査スクリプトが正常に実行されたことを示すメッセージが表示されます。各項目が適切なことを確認し、**[次へ]** をクリックして、拡張するリソース階層に必要なデータを指定します。

注記: 複数のルートを持つ階層は、一括して拡張する必要があります。複数ルートの階層は、単一のルート階層としては拡張できません。

8.3.2.2.1. リソース階層の拡張

このダイアログボックスは、DNS リソース階層の作成 を完了するか、既存の DNS リソース階層を拡張すると、自動的に開きます (リソース階層の拡張 を参照)。DNS リソース階層を拡張するには、次の情報を入力してください。

フィールド	説明
IP アドレス	保護するプライマリサーバまたは別名に関連付けられた *A レコード* の IP アドレスを入力します。DNS リソースがこのサーバで起動した場合、レコードはこの IP アドレスで更新されます。
DNS サーバ名 (完全修飾ドメイン名)	リソースレコードを変更する DNS サーバの完全修飾ドメイン名 (FQDN) を <DNS ServerName>.<mydomain>.com 形式で入力します。DNS サーバは、可能であれば、同じサイトのバックアップサーバからアクセスできるようにします。

8.3.2.2.2. ファイル共有リソース階層の拡張

このダイアログボックスは、ファイル共有リソース階層の作成 を完了すると自動的に開きます。既存のファイル共有リソース階層からも開けます (リソース階層の拡張 を参照)。ファイル共有リソース階層を拡張する場合、データを追加する必要はありません。

8.3.2.2.3. Generic Application リソース階層の拡張

このダイアログボックスは、Generic Application リソース階層の作成 を完了すると自動的に開きます。既存の Generic Application 階層からも開けます (リソース階層の拡張 を参照)。Generic Application で作成したリソース階層を拡張する場合、データを追加する必要はありません。

8.3.2.2.4. LAN Manager リソース階層の拡張

このダイアログボックスは、LAN Manager リソース階層の作成 を完了すると自動的に開きます。既存の LAN Manager リソース階層からも開けます (リソース階層の拡張 を参照)。LAN Manager リソース階層を拡張する場合、データを追加する必要はありません。

8.3.2.2.5. ボリュームリソース階層の拡張

このダイアログボックスは、ボリュームリソース階層の作成 を完了するか、既存のボリュームリソース階層を拡張すると、自動的に開きます (リソース階層の拡張 を参照)。ボリュームリソース階層を拡張するには、次のデータを追加してください。

フィールド	説明
ボリュームタイプ	共有ストレージを使用する場合は **[共有ディスク]** を選択します。ミラーが存在しない状態で SIOS DataKeeper を使用する場合は **[ミラーの作成]** を選択します。ミラーが存在している状態で SIOS DataKeeper を使用する場合は、**[既存のミラー]** を選択します。
ネットワークのエンドポイント (ターゲット/ソース)	ボリュームタイプとして **[ミラーの作成]** または **[既存のミラー]** を選択した場合は、ミラーのエンドポイントを選択します。エンドポイントには IP アドレスを指定します。
モード	ボリュームタイプとして **[ミラーの作成]** を選択した場合は、ミラーのモードを選択します。 **非同期ミラー:** ソースへの書き込みは、キューに入ってからターゲットに転送されます。制御は即時に戻ります。同期ミラーに比べて、信頼性は低下しますが、ソースへの書き込みは高速になります。 **同期ミラー:** ソースボリュームへの書き込みは、ターゲットボリュームで即時にコミットされます。信頼性は高くなりますが、パフォーマンスが低下します。
ボリュームリソースをクラスタ内の 3 つ目のシステムに拡張する場合は、クラスタ内のイクイバレンシシステムにボリュームタイプを指定する必要があります。	
ボリュームタイプ (共有または SIOS DataKeeper)	イクイバレンシシステム間のミラーリングには、**[共有ディスク]** またはネットワークのエンドポイントを選択します。

注記: ボリュームリソース階層を削除すると、LifeKeeper GUI で作成したミラーも削除されます。ミラー削除を回避するには、LifeKeeper ミラー削除フラグ を **False** に設定してください。

8.3.2.2.6. IP リソース階層の拡張

このダイアログボックスは、IP アドレスリソース階層の作成 を完了するか、既存の DNS リソース階層を拡張すると、自動的に開きます (リソース階層の拡張 を参照)。IP アドレスリソース階層を拡張する場合は、次の情報を入力してください。

フィールド	説明
サブネットマスク	ターゲットサーバの IP リソースに使用するサブネットマスクを入力します。テンプレートサーバのサブネットマスクがデフォルトとして表示されます。
ネットワーク接続	ターゲットサーバで使用するネットワーク接続を選択します。
ターゲットのリストアモード	IP アドレスのリストア機能は、同じサブネットにある LAN ノード 2 台と異なるサブネット上にある WAN ノード 1 台で構成する 3 ノード SIOS Protection Suite クラスタに適用されます。IP リソースのリストアモードは、LAN ノードでは **有効** 、WAN ノードでは **無効** にそれぞれ設定されます ターゲットサーバの IP リソースに適用する_リストアモード_を選択します。状況によっては、保護対象の IP アドレスがターゲットシステムで使用できないことがあります。例えば、リモートのターゲットシステムがクラスタと異なるサブネットに接続されている場合、保護対象の IP アドレスは使用できません。その場合、リストアモード「無効」で拡張することができます。リストアモード「無効」を指定すると、SIOS Protection Suite は、リソースを起動する際に、ターゲットシステムの IP アドレスを設定せず、IP リソースの監視は無効になります。このようなケースでは、ネットワーク上のリダイレクトは、SIOS Protection Suite の DNS リソースなどで実装します。ターゲットシステムの [IP リソースのプロパティ] ページを使用すると、設定を後で変更できます。詳細については、IP リソース管理 を参照してください。
ターゲットのローカルリカバリ	ターゲットサーバの IP ローカルリカバリ を有効にする場合は、**[はい]** をクリックします。有効にしない場合は、**[いいえ]** をクリックします。
ターゲットのローカルリカバリのネットワー	**ローカルリカバリ** を **有効** にした場合、バックアップインターフェースとして使用するネットワーク接続を選択する必要があります。バックアップサーバに NIC がなければ、プライマリサーバの NIC を指定します。

ク接続	

8.3.2.3. リソース階層の拡張解除

[リソース階層の拡張解除] オプションは、すべてのリソースを対象として単一のサーバからすべての階層を削除します。すべてのサーバから階層を削除する [リソース階層の削除] オプションとは、動作が異なります。

[リソース階層の拡張解除] を使用する場合、既存の階層を削除するサーバがターゲットサーバとなります。

[リソース階層の拡張解除] は、ターゲットサーバとのコミュニケーションパスがアクティブな SIOS Protection Suite サーバで使用できます。

1. 拡張を解除するサーバ固有のリソースインスタンスを選択し、リソースコンテキストメニュー または リソースコンテキストツールバー の **[リソース階層の拡張解除]** をクリックします。

2. 拡張を解除するサーバとリソース階層を確認するメッセージが表示されます。**[拡張解除]** をクリックして拡張を解除します。

3. アウトプット パネルが有効な場合は、ダイアログボックスが閉じて、リソース階層の拡張を解除した結果がアウトプットパネルに表示されます。有効でない場合は、ダイアログが表示されたままこれらの結果が表示されます。すべての結果が表示されたら、**[完了]** をクリックして終了してください。

8.3.2.4. リソース依存関係の追加

ほとんどの場合はリカバリキットで元のリソース階層の作成作業を行うときに依存関係が作成されますが、特定の状況では、新しいリソース依存関係を作成したり、既存の依存関係を削除したりする必要がある場合があります。例えば、既存の IP 依存関係を別の IP アドレスに変更する場合などです。リソース階層全体を削除してから新しく作成する代わりに、既存の IP 依存関係を削除して、別の IP アドレスで新しい依存関係を作成することができます。

1. 子の依存関係を追加する親として、サーバ固有のリソースインスタンスを選択します。次に、リソースコンテキストメニュー または リソースコンテキストツールバー から **[依存関係の作成...]** を選択します。

2. ドロップダウンボックスから **[親リソース IP アドレス]** を選択します。**[次へ]** をクリックします。

3. サーバ上の既存の有効なリソースのドロップダウンボックスから、**[子リソースタグ]** を選択します。以下のリソースを除いて、サーバ上で使用できるリソースがすべてダイアログに表示されます。
   - 親リソース、その祖先および子。
   - 親リソースと同じサーバに拡張されていないリソース。
   - 親リソースと同じ相対優先順位ではないリソース。
   - 親リソースがサービス中の場合、親と同じサーバでサービス中ではないリソース。

   [次へ] をクリックして、次のダイアログに進みます。

4. ダイアログには、依存関係を作成するために適切な親子のリソースタグを選択したかどうかの確認が表示されます。**[依存関係の追加]** をクリックして、親が拡張されたクラスタ内のすべてのサーバ上に依存関係を作成してください。

5. アウトプットパネル が有効な場合、ダイアログボックスが閉じて、依存関係作成コマンドの実行結果がアウトプットパネルに表示されます。すべての結果が表示されたら、**[完了]** をクリックしてダイアログボックスを閉じます。

8.3.2.5. リソース依存関係の削除

1. 子の依存関係を削除する親として、サーバ固有のリソースインスタンスを選択します。次に、リソースコンテキストメニュー または リソースコンテキストツールバー から **[依存関係の削除]** を選択します。

2. ドロップダウンボックスから **[子リソース]** を選択します。これは削除する依存関係の子の名前です。**[次へ]** をクリックして、次のダイアログボックスに進みます。

3. ダイアログには、依存関係を削除するために適切な親子のリソースタグを選択したかどうかの確認が表示されます。**[依存関係の削除]** をクリックすると、クラスタ内の全サーバの依存関係が削除されます。

4. アウトプットパネル が有効な場合、ダイアログボックスが閉じて、依存関係削除コマンドの実行結果がアウトプットパネルに表示されます。すべての結果が表示されたら、**[完了]** をクリックしてダイアログボックスを閉じます。

8.3.2.6. 全サーバのリソース階層の削除

1. 削除するサーバ固有のリソースインスタンスを選択し、リソースコンテキストメニュー または リソースコンテキストツールバー の **[リソース階層の削除]** をクリックします。

2. 削除するリソース階層を確認するメッセージが表示されます。**[削除]** をクリックして、リソース階層を削除します。最初に選択したサーバから順番にリソース階層が削除されます。

3. アウトプットパネル が有効な場合、ダイアログボックスが閉じて、階層削除コマンドの実行結果がアウトプットパネルに表示されます。すべての結果が表示されたら、**[完了]** をクリックしてダイアログボックスを閉じます。

8.3.3. マニュアルページ

LCD - その他の LCD プログラム

LCDI アプリケーション

LCDI インスタンス

LCDI 関係

LCDI-Resource タイプ

LCDI-Systems

LifeKeeper のフラグ

lk_chg_value

lk_err

perform_action

sendevent

volume

8.3.3.1. LCD - その他の LCD プログラム

構文

lcdremexec [-e] -d destname -- cmd [arg1 arg2 … argn]

lcdsync [-d destname]

lcdrecover -g {remote|restore|delete} -- [arg1 arg2 … argn] | -G {remote|restore|delete} -- [arg1 arg2 … argn] | -p primarytest /| [-o resource]

lcdrcp file1 file2 file3 …{dest:ofile | dest:odir}

lkstart [-w waitperiod]

lkstop [-f or -r|-n]]

説明

上記のプログラムは、アプリケーション開発者がさまざまな目的で使用できます。各プログラムは `%LKROOT%\bin` ディレクトリに格納されています。

終了コード

前記のコマンドは、次の終了コードを返します。

0	処理に成功した。
1	システムコールまたはライブラリコールが内部エラーを返した。
2	ユーザが指定した構文にエラーがある。
3	LifeKeeper の内部エラー。
4	既存のオブジェクトに対する処理を要求した。
5	不正な引数を渡した。
6	インデックスが有効な範囲を超えている。
7	存在しないオブジェクトに要求を発行した。
8	リソースインスタンスの削除を要求したが、そのリソースインスタンスには、削除していないリソースインスタンスが依存している。
9	相手のシステムと通信できない。

8.3.3.1.1. lcdrcp

```
lcdrcp file1 file2 file3 … {dest:ofile | dest:odir}
```

lcdrcp は、LifeKeeper コミュニケーションパスを使用して ASCII ファイル _file1 file2 file_3 … を別のシステムに転送する汎用プログラムです。**lcdrcp** を使用してバイナリファイルをコピーすることはできません。

ファイルは dest のディレクトリ *odir* に転送されます。送信するファイルが 1 つだけの場合には、システム dest 上の位置 *ofile* に送信先のファイル名を含めた形式を使用できます。送信先の引数に Windows のドライブ名 (D: など) を使用する場合は特に注意してください。送信先名がない場合に誤って送信先の名前として解釈される可能性があります。ただし、送信先システム名を指定した場合、ドライブ名は正常に解釈されます。

8.3.3.1.2. lcdrecover

```
lcdrecover -g {remove|restore|delete} -- [arg1 arg2 … argn] | -G
{remote|restore|delete} -- [arg1 arg2 … argn] | -p primarytest | [-o resource]
```

-g オプションは、_remove、restore、delete_ のうちいずれかの引数を取ります。このオプションによって、指定した引数に対するグローバル前処理スクリプトが実行されます。グローバル前処理スクリプトは、特定のイベントの前に実行するようにアプリケーションによって登録されます。例えば、このオプションに restore 引数を指定すると、LifeKeeper によって登録された restore 前処理スクリプトが実行されてから、すべてのアプリケーションによって登録された restore 前処理スクリプトが実行されます。通常、**perform_action** (LRACI perform_action を参照) によって restore 前処理スクリプトが自動的に実行されます。ただし、**perform_action** に *-G* オプションが指定された場合を除きます。

perform_action の *-G* オプションを使用すると、最初に **lcdrecover** *-g restore* を使用した **perform_action** の実行の前に 1 回だけグローバル前処理スクリプトを実行して、複数の **perform_action** コマンドを実行できます。アプリケーションは、以下のパスにスクリプトをインストールして、グローバル前処理スクリプトを登録できます。

```
%LKROOT%\ subsys\<appname>\actions\prerestore.ksh
```

arg1, arg2, … argn は実行時にグローバル前処理スクリプトに渡される引数です。

remove 引数についても同様のスクリプト (remove 前処理スクリプト) が存在し、**perform_action** *-G -a remove* が実行される前に実行できます。実行されるのは、**lcdrecover** *-g remove* の実行時です。

delete 前処理スクリプトも同様ですが、**ins_remove** の *-G* が省略された場合を除いて、*ins_remove * *-G* … プログラムの前に実行されます (LCDI インスタンス を参照)。

lcdrecover の *-G* オプションは *-g* に類似していますが、グローバル後処理スクリプトを実行するように指定する点が異なります。*-G* オプションは、その前の **lcdrecover** *-g arg* を実行せずに使用しないでください。また、すべての **perform_action** プログラムまたは **ins_remove** プログラムが実行された後に実行する必要があります。**getlocks** によって保護された領域内で *-G* オプションを実行する場合 (**getlocks** の後、**rlslocks** の前)、*arg1* に *-m* を設定して、**getlocks** の 2 つ目のインスタンスが実行されないようにしてください。2 つ目のインスタンスが実行されると、処理がハングします。

以下の例では、複数の **perform_action** コマンドを実行します。グローバル前処理スクリプトとグローバル後処理スクリプトは 1 回だけ実行されます。

```
lcdrecover -g restore

# run "preglobal" restore scripts

perform_action -G -a restore -t tagname

# neither scripts are run
```

```
perform_action -G -a restore -t tagname2

# neither scripts are run

lcdrecover -G restore -- -m

# run "postglobal" restore scripts

# use -m arg when in getlocks protected region of code
```

この例では、複数の restore 前処理スクリプトと restore 後処理スクリプトが実行されます。

```
perform_action -a restore -t tagname

# all scripts once

perform_action -a restore -t tagname2

# all scripts again
```

lcdrecover の *-p* オプションは、特定のリソースがプライマリシステムまたはセカンダリシステムのどちらのリソース階層にあるかを判定するために使用されます。リソースタグ名に primary test を指定すると、リソースがプライマリ階層に存在する場合は文字列 primary が、存在しない場合は secondary が標準出力に出力されます。

-o オプションを使用すると、指定したリソースタグに関連付けられたリモートシステムを取得できます。

8.3.3.1.3. lcdremexec

```
lcdremexec [-e] -d destname -- cmd [arg1 arg2 arg3 … argn]
```

このプログラムは、LifeKeeper コミュニケーションパスを介してシステム *destname* にリモート要求を送信し、引数 *arg1 arg2 arg3 …* を用いてコマンド **cmd** をリモートで実行します。また、リモートコマンドの標準出力および標準エラー出力を **lcdremexec** コマンドの標準出力に返します。リモートコマンドの終了コードは **lcdremexec** によって返されます。

注記: destname がカレントシステムである場合、メッセージは送信されず、**lcdremexec** によってローカルで実行されます。

-e オプションを指定すると、リモートコマンドの標準出力と標準エラー出力が分割され、最初にリモートコマンドの標準出力が **lcdremexec** の標準出力に出力されてから、リモートコマンドの標準エラー出力が **lcdremexec** コマンドの標準エラー出力に出力されます。このオプションはローカルコマンドには効果がなく、標準出力と標準エラー出力は変わりません。

cmd には、Korn シェルスクリプトまたは Win32 実行可能ファイルのいずれかを指定できます。*destname* の %LKROOT%を現在の作業ディレクトリとして実行されるので、%LKROOT%に対する相対パス名を指定できます。

実行前に、*destname* の PATH 変数の先頭には常にディレクトリ `%LKROOT%\BIN` が追加されます。*destname* がダウンしているか実行中にダウンした場合には、**lcdremexec** は 0 以外の終了コードを返します。

8.3.3.1.4. lcdsync

```
lcdsync [-d destname]
```

共有メモリに保存された LifeKeeper リソース階層構成とコミュニケーションパスのステータスデータが変更されているかどうかをチェックします。異なる場合、データは「同期を取って」ディスクに書き込まれます。そのため、このプログラムから復帰したとき、ディスク上に正常なデータがあることが保証されます。*destname* を指定しないと、カレントシステムが対象となります。

注記: リソース階層構成またはコミュニケーションパスの変更に使用されるコマンド (例: **ins_create** 、**dep_create** 、**ins_setit** 、**eqv_remove**) は、共有メモリセグメントのみを変更し、**lcdsync** プログラムを実行するまで、LifeKeeper の恒久的なファイルストレージには反映されません。

8.3.3.1.5. lkstart

```
lkstart [-w waitperiod]
```

このプログラムは、LifeKeeper が実行されていない場合にカレントシステム上で LifeKeeper を起動します。**lkstart** を実行すると、LifeKeeper デーモンが停止した場合に再起動されるように、LifeKeeper デーモンに属する `%LKROOT%\etc\LKinit.config` ファイルのエントリが修正されます。

-w オプションを使用すると、タイムアウト間隔を変更できます。*waitperiod* には、秒数を指定します。起動前の待機時間を指定するには *-w* 引数を使用します。

LifeKeeper サービスは、管理ツールにある Services mmc を使用して起動することも、「`sc start LifeKeeper`」または「`net start LifeKeeper`」のいずれかを使用してコマンドプロンプトから起動することもできます。

注記: このプログラムはコンソールから実行する必要があります。

8.3.3.1.6. lkstop

```
lkstop [-n] [-f] [-r]
```

このスクリプトは、LifeKeeper が実行されている場合にシステム上の LifeKeeper をシャットダウンします。LifeKeeper はシステム起動時に自動的に再起動されます。

lkstop の各オプションを入力したときの LifeKeeper の動作を以下の表に示します。

コマンドライン	動作
`lkstop`	サービス中のリソースはサービスから削除されますが、バックアップサーバにはスイッチオーバされません。
`lkstop -n`	オプションを指定しない **lkstop** と同じです。
`lkstop -f`	サービス中のリソースはサービスから削除されません。
`lkstop -r`	-f と同じです。

LifeKeeper のサービスは、Windows の [コントロール パネル] にある [管理] タスクの [サービス] ツールを使用して停止することもできます。

8.3.3.2. LCDI アプリケーション

構文

app_create [-d destsys] -a appname

app_remove [-d destsys] -a appname

app_list [-d destsys]

説明

LifeKeeper アプリケーションは、関連するリソースタイプのグループです。アプリケーションが削除されると、その下にインストールされたリソースタイプもすべて削除されます。

これらのプログラムは、構成データベースに新しいアプリケーションを生成したり、既存のアプリケーションを削除したりするためのインターフェースを提供します。失敗した場合は 0 以外のコード (「終了コード」を参照) を返し、エラーメッセージを標準エラーに出力します。

終了コード

前記のコマンドは、次の終了コードを返します。

0	処理に成功した。
1	システムコールまたはライブラリコールが内部エラーを返した。
2	ユーザが指定した構文にエラーがある。
3	LifeKeeper の内部エラー。
4	既存のオブジェクトに対する処理を要求した。
5	不正な引数を渡した。
6	インデックスが有効な範囲を超えている。
7	存在しないオブジェクトに要求を発行した。
8	リソースインスタンスの削除を要求したが、そのリソースインスタンスには、削除していないリソースインスタンスが依存している。
9	相手のシステムと通信できない。

8.3.3.2.1. app_create

```
app_create [-d destsys] -a appname
```

新しいアプリケーションを作成します。アプリケーションは、*appname* という名前を使用して、システム *destsys* に関連付けられます。*destsys* を指定しない場合、アプリケーションはローカルに作成されます。

8.3.3.2.2. app_list

```
app_list [-d destsys]
```

システム *destsys* 上で LifeKeeper と連携するようにソフトウェアをインストールしたアプリケーションのリストを、標準出力に表示します。*destsys* を指定しないと、カレントシステムが対象となります。

8.3.3.2.3. app_remove

```
app_remove [-d destsys] -a appname
```

既知のアプリケーションの構成データベースセットから、指定したアプリケーションを削除します。このアプリケーションに関連するリソースタイプ、リソースインスタンス、およびイクイバレンシも、すべて削除されます。構成データベースでアプリケーションが既知ではないためにエラーが発生する場合もあります。

8.3.3.3. LCDI インスタンス

LCDI インスタンス

構文

ins_gettag [-d destsys] -i id

ins_create [-d destsys] -a appname -r restyp [-I{AUTORES_ISP|INIT_ISP| INIT_OSU}] [-v info] -t tag -i id [-Q quickChkInt] [-DdeepChkInt] [-l localRecover{Y/N}] [-s AUTOMATIC/INTELLIGENT]

ins_remove [-d destsys] [-R roottag] [-a appname] [-r restyp] [-ttag] [-i id] [-v] [-l] [-N] [-G]

ins_setin [-d destsys] -t tag [-v info]

ins_setit [-d destsys] -t tag -I {AUTORES_ISP|INIT_ISP|INIT_OSU}

ins_setst [-d destsys] -t tag -S {ISP|ISU|OSU} [-R reason] [-A]

ins_list [-d destsys] [-fC] [-R top] [-a appname] [-r typ] [-t tag] [-i id]

ins_setchkint [-d destsys] -t tag -c {q=quick|d=deep} -vinterval

ins_setlocalrecover [-d destsys] -t tag -l {Y=enable|N=disable}

ins_setas [-d destsys] -t tag -s {INTELLIGENT|AUTOMATIC}

説明

リソースは、システムが認識しているボリューム、アプリケーション、またはシステムオブジェクトを表すために LifeKeeper によって使用されます。リソースタイプはリソースの分類です。リソースインスタンスはリソースタイプの実際のインスタンスです。例えば、リソースタイプには、ファイルシステムボリューム、ファイル共有、IP アドレス、LAN Manager 名、および SQLServer などの各種サーバが含まれます。一般のユーザ定義可能タイプを使用すると、ユーザはカスタム耐障害セットアップを構築できます。あるリソースタイプに対して、複数のインスタンスが存在する場合もあります。

リソースインスタンスは多数の様々な状態で存在します。これらの状態は以下の値と意味を持ちます。

ISP	リソースはサービス中であり、保護されています。ISP はプライマリノード上のリソースの標準状態です。
OSU	サービスを停止していますが、障害は発生していません。remove スクリプトを実行してサービスが停止されたため、このシステムではリソースを使用できません。OSU 状態は、OSF 状態または OSU 状態の子に依存関係を持つオブジェクトに対して、あるいはバックアップマシン上の同等オブジェクトが ISP 状態または ISU 状態にある場合にも使用されます。OSU はセカンダリノード上のリソースの標準状態です。
OSF	障害によりサービスを停止しています。オブジェクトを復旧しようとして障害が発生したため、このシステムで

	はリソースを使用できません。

終了コード

どのコマンドも、正常に実行された場合は 0 を返します。失敗した場合は 0 以外のコードを返し、標準エラーに出力します。前記のコマンドは、次の終了コードを返します。

0	処理に成功した。
1	システムコールまたはライブラリコールが内部エラーを返した。
2	ユーザが指定した構文にエラーがある。
3	LifeKeeper の内部エラー。
4	既存のオブジェクトに対する処理を要求した。
5	不正な引数を渡した。
6	ンデックスが有効な範囲を超えている。
7	存在しないオブジェクトに要求を発行した。
8	リソースインスタンスの削除を要求したが、そのリソースインスタンスには、削除していないリソースインスタンスが依存している。
9	相手のシステムと通信できない。

8.3.3.3.1. ins_list

```
ins_list [-d destsys] [-fC] [-R top] [-a appname] [-r typ][-t tag] [-i id]
```

このコマンドは、リソースインスタンスのセットに関する行を標準出力に表示します。各行には、特定のリソースインスタンスに関する現在の情報がすべて含まれています。行の例を以下に示します。

```
LKSYS1-filesys-volume-ISSUTILS-K:--ISP-restore action
hassucceeded-AUTORES_ISP--0-0-
```

各行のフィールドは区切り文字で区切られています。デフォルトの区切り文字は ^A (\001) です。*-fC* オプションを指定した場合、区切り文字は指定した文字に変更されます。上記の例では、区切り文字としてダッシュ (-) が表示されています。上記のコマンド例のフィールドは以下のとおりです。

LKSYS1	リソースインスタンスが存在するシステムの名前。
filesys	リソースタイプのアプリケーション名。
volume	リソースタイプ名。
ISSUTILS	ユーザ定義のリソースインスタンスタグ識別子。
K:	リソースインスタンスに対する LifeKeeper の内部識別子。
- -	このフィールドが (例のように) 空ではない場合、タイプに応じて、追加のインスタンス情報が表示されます。
ISP	リソースインスタンスの現在の 状態 。ISP、ISU、OSU、または OSF と表示されます。
restore 処理に成功した。	状態が最後に変更された理由。
AUTORES_ISP	使用可能なリソース 初期化オプション は、AUTORES_ISP、INIT_ISP、INIT_OSU です。
- -	このフィールドが (例のように) 空ではない場合、リソースが現在、以下の理由で予約されていることを示します。 RESTORE: リソースをサービス開始にする REMOVE: リソースをサービスから削除する RECOVER: リソースのローカルリカバリを実行する
0	リソースを予約したプロセスのプロセス ID。
0	予約済み。
180	クイックチェック間隔 (秒単位)。
300	ディープチェック間隔 (秒単位)。
0	ローカルリカバリオプション。0 = 無効、1 = 有効。

その他の引数を指定すると、リストに含まれるリソースインスタンスの数が制限されます。引数を使用しない場合は、

destsys のすべてのリソースが列挙されます。以下は制限するための引数です。

destsys:*destsys* を指定しないと、カレントシステムが対象となります。指定した場合は、リモートシステムのデータが表示されます。

top:*top* が空白文字列 " " の場合は、ルートリソースのみが表示されます。top に空白以外が指定された場合は、top リソースおよびその下のすべての子リソースが再帰的に表示されます。

appname:*appname* を指定した場合は、このアプリケーションで定義されたすべてのリソースタイプに関連付けられたすべてのリソースインスタンスが表示されます。appname を指定しない場合は、システム上で定義されたすべてのアプリケーションのすべてのリソースインスタンスが表示されます。

typ: *typ* を指定した場合は、アプリケーション *appname* のタイプ *typ* のリソースインスタンスがすべて表示されます。

tag または *id*: *tag* または *id* を指定した場合は、その *tag* または *id* に関連付けられたリソースインスタンスが表示されます。

8.3.3.3.1.1. 初期化の方法

デフォルトの「Auto ISP 初期化方法」を使用することを推奨します。LifeKeeper が起動時に実行する初期化を次表に示します。

Autores ISP	ペアノードでリソースが起動していないと、リソースを自動的に起動します。
Init ISP	リソースを常に ISP 状態に初期化します。
Init OSU	リソースを常に OSU 状態に初期化します。

8.3.3.3.1.2. 初期状態

状態とは、リソースの現在の処理ステータスを指します。例えば、プライマリシステムのリソースは、LifeKeeper で保護された状態「 **ISP** (サービス中)」が標準の状態です。一方、セカンダリシステムのリソースは、サービスを休止した「 **OSU** 」が標準の状態です。

デフォルトの初期状態を使用することを推奨します。初期状態を **OSU** に設定した場合は、リソースを手動で起動する必要があります。

8.3.3.3.2. ins_create

```
ins_create [-d destsys] -a appname -r restyp [-I
{AUTORES_ISP|INIT_ISP|INIT_OSU}][-v info] -t tag -i id [-Q quickChkInt][-D
deepChkInt][-l localRecover{Y|N}] [-s AUTOMATIC|INTELLIGENT]
```

destsys システムの構成データベースに新しいリソースインスタンスを定義します。リソースインスタンスは指定した引数で記述されます。_destsys_ を指定しないと、カレントシステムが対象となります。このコマンドには、次の文字列タグオプションを指定できます。

- *-a* オプションと *-r* オプションは、新しいインスタンスに関連付ける既存のアプリケーションおよびリソースタイプを指定します。
- *-I* オプションに指定する初期化タイプフィールドは、LifeKeeper が再起動する場合 (起動時など) にリソースインスタンスを初期化する方法を示します。
- *-v* オプションに指定する info 文字列には、リソースタイプに固有の追加情報を記述します。リソースタイプごとに一意である必要はありません。
- *-t* オプションに指定する文字列タグは、システム上で一意なリソースインスタンスの名前です。LifeKeeper の外部でもわかりやすい文字列を指定してください。**注意：**タグ名に使用できる文字はASCII印字可能文字のみです。
- *-i* オプションに指定する文字列 ID もシステムごとに一意ですが、LifeKeeper の内部でのみ意味を持ちます。
- *-Q* オプションに指定するクイックチェック間隔は秒単位です。リソースに対して **quickchk.ksh** スクリプトが存在しない場合には、この値に 0 を指定してください。LifeKeeper は、**quickchk.ksh** スクリプトを続けて実行するまでにこの期間だけ待機します。有効な値の範囲は 0 ～ 604800 です。
- *-D* オプションに指定するディープチェック間隔は秒単位です。リソースに対して **deepchk.ksh** スクリプトが存在しない場合には、この値に 0 を指定してください。LifeKeeper は、**deepchk.ksh** スクリプトを続けて実行するまでにこの期間だけ待機します。有効な値の範囲は 0 ～ 604800 です。
- ローカルリカバリオプションには、**recover.ksh** スクリプトによるリソースのリカバリを実行するかどうかを指定します。リソースに対して **recover.ksh** スクリプトが存在しない場合には、このオプションに「_N_」を指定してください。

8.3.3.3.3. ins_gettag

```
ins_gettag [-d destsys] -i id
```

名前が *destsys* のシステムで、内部識別子 *id* に対応するタグ名を標準出力に表示します。*destsys* を指定しないと、カレントシステムが対象となります。

注記: リソースのタグ名と *id* 名はシステム上で一意ですが、異なるシステム上の別のリソースインスタンスに再利用することができます。

リソースタグを使用して人間が読める名前 (例: `user-partition`) を付けると、リソースインスタンスの処理がわかりやすくなります。一方、_id_ は内部記述子です。リソース名 *id* は、リソースを一意に記述するために、リソースに関連付けられたアプリケーションソフトウェアで使用されます。

8.3.3.3.4. ins_remove

```
ins_remove [-d destsys] [-R roottag] [-a appname] [-r restyp][-t tag] [-i id]
[-v] [-I] [-N] [-G]
```

destsys システムの構成データベースからリソースインスタンスを削除します。このコマンドを実行すると、リソースの依存関係とイクイバレンシも削除されます。*destsys* を指定しないと、カレントシステムが対象となります。

注記: ins_remove は、指定されたリソースに直接的または間接的に依存するリソースを削除してから、指定されたリソースを削除します。

リソースインスタンスを削除する場合、削除するインスタンスのリソースタイプに削除処理が定義されていると、その削除処理はインスタンスを削除する前に実行されます。

このコマンドには、次のオプションを指定できます。

-R	*-R* オプションは下位の階層全体と、それに依存するリソースをすべて削除します。*roottag* 文字列に複数のリソースタグ名を区切り文字 ^A で区切って記述すると、指定したリソースとその下位リソースを再帰的に削除できます。削除処理は、削除対象でないリソースが依存するリソースが現れるまで続きます。
-a	*-a* オプションで指定したアプリケーションのリソースだけを削除します。
-r	*-r* オプションで指定したリソースタイプのリソースをすべて削除します。
-t (または *-i*)	*-t* (または *-i*) オプションを指定すると、一致する *タグ* 、または *ID* を持つインスタンスとその依存リソースを削除します。
-v	*-v* オプションを指定すると、削除したリソースインスタンスすべてのタグ名を標準出力に表示します (詳細モード)。
-I	*-I* オプションを指定すると、リソース階層を初期化し、**ins_remove** の適切な動作を保証します。このオプションは、**ins_remove** を最上位レベルで再帰的に呼び出す場合に使用します。例えば delete スクリプトで ins_remove を下位レベルで再帰的に呼び出す場合、このオプションは不要です。delete スクリプトから ins_remove を再帰的に呼び出す場合は、*-I* オプションを使用しないでください。
-N	*-N* オプションを指定すると、**ins_remove** はリソース階層を初期化しません。上位レベルで **ins_remove** を呼び出すと、*-I* オプションが自動的に付くためです。delete スクリプトは親である **ins_remove** から呼び出され、*-N* オプションは階層サイクルを発生しないため、*-N* オプションは delete スクリプト内部で使用する必要があります。
-G	*-G* オプションは、**ins_remove** を呼び出すときに delete 前処理スクリプトと delete 後処理スクリプトを実行しないように指示します (LCD を参照)。**ins_remove** を最上位で複数回呼び出し、**ins_remove** を呼び出す前後に LCD の **lcdrecover** *-g delete* を使用して delete 前処理スクリプトと delete 後処理スクリプトを手動で実行する場合に、このオプションが有用です。最上位で呼び出した **ins_remove** は、delete 前処理スクリプトと delete 後処理スクリプトを実行するため、delete スクリプトには *-G* オプションを指定してください。

8.3.3.3.5. ins_setas

```
ins_setas [-d destsys] -t tag -s {INTELLIGENT|AUTOMATIC}
```

destsys システムにある *tag* タグ名が付いたルートリソースのスイッチバックタイプを、*-s* オプションで指定された方法に設定します。必ずルートリソースで使用して、ルートリソースおよびそのすべての依存リソースのスイッチバックタイプを変更してください。

8.3.3.3.6. ins_setchkint

ins_setchkint

```
ins_setchkint [-d destsys] -t tag -c {q=quick|d=deep} -v interval
```

-t tag タグ名で指定されたリソースのクイックチェック間隔またはディープチェック間隔を変更します。チェック間隔は、秒単位で入力する必要があります。

例

ファイル共有リソース FSList.0 のクイックチェック間隔を 2 分間に変更する場合は、`$LKROOT\bin` から以下のコマンドを実行してください。

```
ins_setchkint-t FSList.0 -c quick -v 120
```

ファイル共有リソース FSList.0 のディープチェックを無効にする場合は、`$LKROOT\bin` から以下のコマンドを実行してください。

```
ins_setchkinst -t FSList.0 -c deep -v0
```

8.3.3.3.7. ins_setin

```
ins_setin [-d destsys] -t tag [-v info]
```

-v オプションに指定する *info* 文字列には、リソースタイプに固有の追加情報を記述します。リソースタイプごとに一意である必要はありません。例えば、ファイル共有タイプのリソースインスタンスには、このインスタンスが管理するすべての共有名を *info* に指定します。

8.3.3.3.8. ins_setit

```
ins_setit [-d destsys] -t tag -I {AUTORES_ISP | INIT_ISP | INIT_OSU}
```

LifeKeeper 自体を初期化する際 (システム起動時など) にリソースの状態を初期化する方法を LifeKeeper に指示します。このオプションを設定しない場合、LifeKeeper は初期化状態をデフォルトオプションに設定します。

指定できるリストアオプションを以下に示します。

AUTORES_ISP: リソースの初期化を *AUTORES_ISP* に設定した場合は、リソースを OSU 状態に設定してから restore 処理が実行されます。処理が正常に実行されると、リソースは ISP 状態になります。restore 処理に失敗した場合、リソースは OSF 状態になります。

INIT_ISP: *INIT_ISP* に設定した場合、LifeKeeper は他の方法でリソースを初期化するものとみなし、リソースを ISP 状態にします。

INIT_OSU: *INIT_OSU* に設定した場合、LifeKeeper は、リソースが初期化時に起動せず、システム管理者が LifeKeeper グラフィカルユーザインターフェース (GUI) アプリケーションを使用して、手動でリソースを起動するものとみなします。

8.3.3.3.9. ins_setlocalrecover

```
ins_setlocalrecover [-d destsys] -t tag -l {Y=enable|N=disable}
```

-t *tag* タグ名で指定されたリソースのローカルリカバリ設定を変更します。

例

ファイル共有リソース FSList.0 のローカルリカバリを無効にする場合は、$LKROOT\bin から以下のコマンドを実行してください。

```
ins_setlocalrecover -t FSList.0 -l N
```

8.3.3.3.10. ins_setst

```
ins_setst [-d destsys] -t tag -S {ISP|ISU|OSU} [-R reason] [-A]
```

destsys システムにある *tag* タグ名が付いたリソースを *-S* オプションで指定された状態に設定します。*destsys* を指定しないと、カレントシステムが対象となります。リソースの状態は、remove や restore などの処理スクリプトで変更されるため、このコマンドは慎重に使用してください。呼び出し側は、現在の状態がアプリケーションの実際の状態を反映していることを確認する必要があります。

-R オプションを指定すると、リソースの状態が変化した理由を説明するテキストが表示されます。*-A* オプションは、指定したリソースとその依存リソースの状態を階層を遡って再帰的に変更します。

8.3.3.4. LCDI 関係

構文

dep_create [-d destsys] -p partag -c chdtag

dep_remove [-d destsys] [-p partag] [-c chdtag]

dep_list [-d destsys] [-fC] [-C allchild | -P allparent | -c ofparenttag | -p ofchildtag] [-r typ] [-a app]

eqv_create [-d destsys] [-s sys] -t tag [-p sysPriority] [-Sothersys] -o othertag [-r othersysPriority] -e SHARED

eqv_remove [-d destsys] [-s sys] -t tag [-S othersys] -o othertag -e SHARED

eqv_list [-d destsys] [-s sys] [-t tag] [-fC]

説明

LifeKeeper リソースは、互いに対する関係の中で存在しています。2 つのリソースは、無関係である場合も依存関係がある場合もあります。階層内のリソースは、複数のリソースから依存されたり、複数のリソースに依存したりしています。各リソースは、共有イクイバレンシのペアシステム上で同様なリソースとも関連しています。この共有イクイバレンシによって、リソースは必ず、1 度に 1 つのシステムでのみアクティブになります。イクイバレンシオブジェクトは、リソースに対するシステムの優先順位も示しています。この優先順位の値によって、カスケーディングフェイルオーバの順序が決まります。リソースのリカバリ時には、優先順位の高いシステムが優先順位の低いシステムよりも優先されます。優先順位の値は 1 が最高です。数値が大きいほど優先順位は低くなります。1 つのリソースについて、2 つのシステムに同じ優先順位を割り当てることはできません。有効な範囲は 1 ～ 1024 です。

終了コード

どのコマンドも、正常に実行された場合は 0 を返します。失敗した場合は 0 以外のコードを返し、標準エラーに出力します。前記のコマンドは、次の終了コードを返します。

0	処理に成功した。
1	システムコールまたはライブラリコールが内部エラーを返した。
2	ユーザが指定した構文にエラーがある。
3	LifeKeeper の内部エラー。
4	既存のオブジェクトに対する処理を要求した。
5	不正な引数を渡した。
6	インデックスが有効な範囲を超えている。
7	存在しないオブジェクトに要求を発行した。
8	ソースインスタンスの削除を要求したが、そのリソースインスタンスには、削除していないリソースインスタンスが

	依存している。
9	相手のシステムと通信できない。

8.3.3.4.1. dep_create

```
dep_create [-d destsys] -p parent -c child
```

parent タグと *child* タグのリソースインスタンスの間に依存関係を作成します。両方のリソースが同一の *destsys* システム上にある必要があります。*destsys* を指定しないと、カレントシステムが対象となります。これは、*parent* リソースが正常に機能するには *child* リソースが必要であることを意味します。正常に機能するには、両方のリソースインスタンスが同じ状態 (ISP または OSU) で存在していなければなりません。

8.3.3.4.2. dep_list

```
dep_list [-d destsys] [-fC] [-C allchild | -P allparent | -c ofparenttag | -p ofchildtag] [-r typ] [-a appname]
```

リソースインスタンス間の依存関係を記述した文字列を標準出力に表示します。*destsys* を指定しないと、カレントシステムが対象となります。各文字列の形式は以下のとおりです。

```
LK0-LKSYS:135.66.249.201

LK0-LKSYSA:FSLIST.0

FSLIST0:fi.vo.0
```

各文字列には 2 つのフィールドがあり、区切り文字で区切られています。デフォルトの区切り文字は ^A (\001) です。*-fC* オプションを指定した場合、区切り文字は指定した文字に変更されます。上記の例では、区切り文字としてコロン (:) が表示されています。先頭のフィールドには関係の親のタグ名、右側のフィールドには子のタグ名が表示されます。

オプションを使用すると、リストの表示内容を絞り込むことができます。オプションを*使用しない*場合は、すべての依存関係が表示されます。このコマンドには、次のオプションが指定できます。

-C	-C オプションを指定した場合、*allchild* で指定したリソースの直接的および間接的な子の依存関係がすべて表示されます。
-P	-P オプションを指定した場合、*allparent* で指定したリソースの直接的および間接的な親の依存関係がすべて表示されます。
-c	-c オプションを指定した場合、*ofparenttag* で指定したリソースの直接的な子の依存関係のみが表示されます。
-p	-p オプションを指定した場合、*ofchildtag* で指定したリソースの直接的な親の依存関係のみが表示されます。
-r	-r オプションを指定すると、子 *typ* の依存関係がすべて表示されます。
-a	-a オプションを指定すると、アプリケーション *appname* の依存関係がすべて表示されます。

8.3.3.4.3. dep_remove

```
dep_remove [-d destsys] [-p parent] [-c child]
```

destsys システムのデータベースから依存関係を削除します。*destsys* を指定しないと、カレントシステムが対象となります。*child* を指定しない場合、_parent_ の依存関係がすべて削除されます。*parent* を指定しない場合、*child* タグの依存関係がすべて削除されます。両方とも指定しない場合は、すべての依存関係が削除されます。

8.3.3.4.4. eqv_create

```
eqv_create [-d destsys] [-s sys] -t tag [-p sysPriority][-S othersys] -o
othertag [-r othersysPriority] -e SHARED
```

destsys システムの構成データベースにイクイバレンシを作成します。destsys を指定しないと、ローカルシステムが対象となります。

sys または *othersys* を指定した場合は、LifeKeeper によって自動的にリモートシステムに *SHARED* イクイバレンシが追加されます。*sys* システムのタグとして指定されたリソースは、通常の状態で動作する「プライマリ」リソースであるとみなされます。*othersys* システムの *othertag* として指定されたリソースは、ペアシステム上の「セカンダリ」リソースとなります。LifeKeeper の初期化時に、リソース初期化設定に応じてプライマリリソースが設定されます (LCDI インスタンス を参照)。待機システムが起動すると、待機システム上の LifeKeeper によって、プライマリシステムが機能しているかどうかと、プライマリリソースが ISP 状態にあるかどうかがチェックされます。両方とも該当する場合、セカンダリリソースは OSU 状態になります (リソース初期化は無視されます)。いずれかが該当しない場合は、「リソース初期化」の設定に従ってセカンダリリソースが初期化されます。*-p* オプションで指定された値は、リソース *tag* についての *sys* システムの優先順位です。*-r* オプションで指定された値は、リソース *othertag* についての *othersys* システムの優先順位です。

8.3.3.4.5. eqv_list

```
eqv_list [-d destsys] [-s sys] [-t tag] [-e SHARED] [-fC]
```

この機能は、標準出力にリソースインスタンス間のイクイバレンシ関係を記述する文字列を出力します。*destsys* を指定しないと、カレントシステムが対象となります。各行のフィールドは区切り文字で区切られています。デフォルトの区切り文字は ^A (\001) です。*-fC* オプションを指定した場合、区切り文字は C に変更されます。

下記の例では、区切り文字としてコロン (:) が表示されています。

```
LKSYSA:135.66.249.201:LKSYSB:135.66.249.201:SHARED

LKSYSA:FSLIST.0:LKSYSB;FSLIST.0:SHARED

LKSYSA:LK0-LKSYSA:LKSYSB:LK0-LKSYSA:SHARED
```

`LKSYSA:fi.vo.0:LKSYSB;fi.vo.0:SHARED` を例にして、各フィールドについて説明します。

LKSYSA	リソースがあるプライマリシステムの名前。
fi.vo.0	プライマリシステムのボリュームリソースタグ。
LKSYSB	リソースイクイバレンシがあるセカンダリシステムのシステム名。
fi.vo.0	セカンダリシステム上のイクイバレンシリソースのボリュームリソースタグ。
SHARED	イクイバレンシタイプ。

残りの引数を指定すると、出力される情報が以下のように絞り込まれます。

-s sys: 引数 *sys* で指定されたシステムに関連付けられたイクイバレンシのみが出力されます。

-t tag: 引数 *tag* で指定されたタグに関連付けられたイクイバレンシのみが出力されます。

-e SHARED: すべての SHARED イクイバレンシ情報が表示されます。

8.3.3.4.6. eqv_remove

```
eqv_remove [-d destsys] [-s sys] -t tag [-S othersys]-o othertag [-e SHARED]
```

-e オプションで指定したイクイバレンシタイプを *destsys* システムの構成データベースから削除します。destsys を指定しないと、ローカルシステムが対象となります。*tag* リソースと *othertag* リソースの間にあるイクイバレンシタイプを *sys* システムと *othersys* システムから再帰的に削除します。*sys* または *othersys* を指定しないと、カレントシステムが対象となります。

8.3.3.5. LCDI リソースタイプ

LCDI リソースタイプ

構文

typ_create [-d destsys] -a appname -r restyp

typ_remove [-d destsys] -a appname -r restyp

typ_list [-d destsys] [-fC] [-a appname]

説明

リソースは、システムが認識しているボリューム、アプリケーション、またはその他のオブジェクトを表すために LifeKeeper によって使用されます。リソースタイプはリソースの分類であり、すべてのインスタンスに適用できるリカバリ手順の共通セットによって区別されます。リソースタイプの例を以下に示します。

- ファイルシステムボリューム (例: K:)
- ファイル共有 (例: UTIL_SHARE)
- IP アドレス (例: 153.66.232.21)

`typ_create` コマンドおよび `typ_remove` コマンドは、構成データベースに新しいタイプを生成するためのインターフェースを提供します。typ_list コマンドは、特定のシステムに存在するすべてのリソースタイプを一覧表示するための構成データベースへのインターフェースを提供します。

終了コード

どのコマンドも、正常に実行された場合は 0 を返します。失敗した場合は 0 以外のコード (「終了コード」を参照) を返し、標準エラーに出力します。前記のコマンドは、次の終了コードを返します。

0	処理に成功した。
1	システムコールまたはライブラリコールが内部エラーを返した。
2	ユーザが指定した構文にエラーがある。
3	LifeKeeper の内部エラー。
4	既存のオブジェクトに対する処理を要求した。
5	不正な引数を渡した。
6	インデックスが有効な範囲を超えている。
7	存在しないオブジェクトに要求を発行した。

8	リソースインスタンスの削除を要求したが、そのリソースインスタンスには、削除していないリソースインスタンスが依存している。
9	相手のシステムと通信できない。

8.3.3.5.1. typ_create

```
typ_create [-d destsys] -a appname -r restyp
```

destsys システムの構成データベースに新しいリソースタイプを作成します。destsys を指定しないと、ローカルシステムが対象となります。リソースタイプは、*restyp* という名前で、既存のアプリケーション *appname* の下にインストールされます。システムまたはアプリケーションが不明の場合、あるいはリソースタイプがすでに存在している場合には失敗します。

8.3.3.5.2. typ_list

```
typ_list [-d destsys] [-fC] [-a appname]
```

destsys システムにインストールされたアプリケーション *appname* で定義されているリソースタイプのリストを、標準出力に表示します。destsys を指定しないと、ローカルシステムが対象となります。_appname_ を指定しない場合は、すべてのアプリケーションのすべてのリソースタイプが以下の形式で表示されます。

```
filesys:volume

comm:ip

database:informix
```

区切り文字の左側はアプリケーション名、右側はリソースタイプ名です。各行のフィールドは区切り文字で区切られています。デフォルトの区切り文字は ^A (\001) です。*-fC* オプションを指定した場合、区切り文字は指定した文字に変更されます。上記の例では、区切り文字としてコロン (:) が表示されています。

8.3.3.5.3. typ_remove

```
typ_remove [-d destsys] -a appname -r restyp
```

destsys システムの既知のリソースタイプの構成データベースセットから、指定したリソースタイプを削除します。destsys を指定しないと、ローカルシステムが対象となります。このタイプに関連付けられたリソースインスタンス、依存関係、およびイクイバレンシも、すべて削除されます。指定したリソースタイプが構成データベースで不明な場合は失敗します。

8.3.3.6. LCDI システム

構文

sys_create [-d destsys] -s sys

sys_remove [-d destsys] -s sys

sys_getds [-d destsys] -s sys

sys_getst [-d destsys] -s sys

sys_list [-d destsys]

説明

LifeKeeper 構成データベースは関連システムを認識します。リソースとリソースタイプはそれらが配置されているシステムに固有のものなので、構成データベースインターフェースにシステムの概念を含める必要があります。

LCDI システムコマンドは、データベースに対して、情報を返したり、作成したり、削除したりします。

終了コード

どのコマンドも、正常に実行された場合は 0 を返します。失敗した場合は 0 以外のコードを返し、標準エラーに出力します。前記のコマンドは、次の終了コードを返します。

0	処理に成功した。
1	システムコールまたはライブラリコールが内部エラーを返した。
2	ユーザが指定した構文にエラーがある。
3	LifeKeeper の内部エラー。
4	既存のオブジェクトに対する処理を要求した。
5	不正な引数を渡した。
6	インデックスが有効な範囲を超えている。
7	存在しないオブジェクトに要求を発行した。
8	リソースインスタンスの削除を要求したが、そのリソースインスタンスには、削除していないリソースインスタンスが依存している。
9	相手のシステムと通信できない。

8.3.3.6.1. sys_create

```
sys_create [-d destsys] -s sys
```

destsys システムの構成データベースに新しいシステム定義を作成します。destsys を指定しないと、ローカルシステムが対象となります。*-s sys* オプションは、システム名を割り当てるシステムを特定するために必要です。

8.3.3.6.2. sys_getds

```
sys_getds [-d destsys] -s sys
```

destsys システムのデータベースから、システムが現在の状態になった理由を説明したオプションテキストを取得し、標準出力に表示します。destsys を指定しないと、ローカルシステムが対象となります。

8.3.3.6.3. sys_getst

```
sys_getst -s sys
```

システムの状態を、次のいずれかの文字列で、標準出力に表示します。

DEAD (停止)	システムは使用できないと思われます。
ALIVE (稼働中)	システムは使用できると思われます。
UNKNOWN (不明)	システムの状態は不明です。

8.3.3.6.4. sys_list

```
sys_list [-d destsys]
```

destsys システムのデータベースから、LifeKeeper が認識しているシステムのリストを取得し、標準出力に表示します。destsys を指定しないと、ローカルシステムが対象となります。

8.3.3.6.5. sys_remove

```
sys_remove [-d destsys] -s sys
```

destsys システムの構成データベースからシステム定義を削除します。destsys を指定しないと、ローカルシステムが対象となります。*-s sys* オプションは、システム名を割り当てたシステムを特定するために必要です。

8.3.3.7. LifeKeeper のフラグ

LifeKeeper GUI では、システムに設定されたフラグの一覧がステータス表示の最後に表示されます。ロック LCD フラグは、システム共通のフラグであり、ロックをかけたプロセスが完了するまで、他のプロセスに待機を要求します。LCD ロックの標準的な形式を次に示します。

```
!action!processID!time!machine:id
```

LCD ロックフラグの具体例を次に示します。

- **`!action!02833!701236710!<servername>:Restore_hierarchy`** - ファイルシステム階層を作成すると、この形式のロックフラグがステータスウィンドウに表示されます。filesys には、ディスクパーティション階層を持つ appdp アプリケーション、またはファイルシステム階層を持つ `appfs` アプリケーションを指定できます。

- その他の一般的なフラグには、`!nofailover!machine` と `shutdown_switchover` があります。`!nofailover!machine` フラグは、サーバのフェイルオーバを制御するために、LifeKeeper が作成または削除する一時的な内部フラグです。`shutdown_switchover` フラグは、このサーバのシャットダウン方法が switchover に設定されており、サーバをシャットダウンすると、切り替えが発生することを示します。フラグの詳細については、LCDI フラグ を参照してください。

8.3.3.7.1. flg_create

```
flg_create [-d destsys] -f flag
```

destsys システムにフラグ *flag* を作成します。

注記: この処理では、LifeKeeper 構成データベースの「共有メモリ」セグメントのみが変更されます。

共有メモリの変更内容を恒久的なストレージのディスクファイルに確実に反映するには、このコマンドの後に LifeKeeper **lcdsync** コマンドを実行してください。

8.3.3.7.2. flg_list

```
flg_list [-d destsys]
```

flg_list は、このシステム (*destsys* が指定されている場合を除く) で現在定義されているすべてのフラグについて、1 行に 1 つの短いリストを標準出力に表示します。リストの順序は不定です。

8.3.3.7.3. flg_remove

```
flg_remove [-d destsys] -f flag
```

destsys システムのフラグ *flag* を削除します。

注記: この処理では、LifeKeeper 構成データベースの共有メモリセグメントのみが変更されます。

共有メモリの変更内容を恒久的なストレージのディスクファイルに確実に反映するには、このコマンドの後に LifeKeeper **lcdsync** コマンドを実行してください。

8.3.3.7.4. flg_test

```
flg_test [-d destsys] -f flag
```

destsys システムにフラグ *flag* が存在するかどうかをチェックします。0 または 7 を返します。

8.3.3.7.5. LCDI フラグ

構文

flg_create [-d destsys] -f flag
flg_remove [-d destsys] -f flag
flg_test [-d destsys] -f flag
flg_list [-d destsys]

説明

LifeKeeper には、さまざまなタスクを実行するためにフラグを動的に設定する機能があります。以下の特殊用途のフラグが存在する場合があります。

```
!nofailover!uname
```

このフラグが存在する場合、名前が uname のシステム上のリソースはフェイルオーバが抑制されます。フラグを持つシステムはバックアップシステムとして定義されます。注記: これは一時的なフラグであり、uname システムが起動中であることを LifeKeeper が検出すると、フラグは自動的に削除されます。

```
!action!procid!timestamp!uname:identifier
```

これは「admin lock flag」の例です (getlocks を参照)。「admin lock flag」は、LifeKeeper 構成内のいずれかのシステムで他の処理が同時に実行されないようにする必要がある処理に対して使用されます。例えば、あるシステムで階層を作成しながら、別のシステムでも階層を作成することはできません。「admin lock flag」を使用すると、これらの「global」処理の 1 つについて、現在実行中の処理が完了するまで実行されないことが保証されます。

実行中の処理の種類は、「admin lock flag」の識別子フィールドによって識別されます。「admin lock flag」を要求したプロセスが実行されていたシステムは uname で指定されます。フラグは、1970 年 1 月 1 日以降の秒数のタイムスタンプで、getlocks を呼び出したプロセス ID が procid のプロセスによって作成されたものです (getlocks を参照)。

このようなフラグの例を次に示します。

```
!action!01525!701120147!cindy:Create_Hierarchy
```

このフラグは、処理 Create_Hierarchy を実行中であり、階層を作成していることを示します。プロセス ID1525 のプロセスが、cindy システムで時刻 701120147 に「admin lock flag」を要求しました。

```
!restore
```

このフラグは、restore 前処理スクリプト (LCD を参照) の実行時に LifeKeeper によって設定され、restore 後処理スクリプトを実行する必要があることを示します。通常、これは一時的な状態であり、restore 後処理スクリプト (LCD を参照) の実行時に LifeKeeper によって自動的に修正されます。唯一の例外は、以下のコマンドを使用して、明示的に restore 後処理スクリプトを実行する場合です。

```
%LKROOT%\bin\lcdrecover -G restore
```

!restore!uname

このフラグを設定すると、uname システムで restore 後処理スクリプト (LCD を参照) をリモートで実行する必要があることを示します。このシステムで restore 後処理スクリプトが実行されると、LifeKeeper は restore 後処理スクリプトを実行するように uname システムにリモート要求を送信します。通常、これは一時的な状態であり、LifeKeeper によって自動的に修正されます。唯一の例外は、`%LKROOT%\bin\lcdrecover -G restore` コマンドを使用して、明示的に restore 後処理スクリプトを実行する場合です。

!remove

このフラグは、remove 前処理スクリプト (LCD を参照) の実行時に LifeKeeper によって設定され、後から remove 後処理スクリプトを実行する必要があることを示します。通常、これは一時的な状態であり、後から remove 後処理スクリプト (LCD を参照) を実行すると LifeKeeper によって自動的に修正されます。唯一の例外は、以下のコマンドを使用して、明示的に remove 後処理スクリプトを実行する場合です。

```
%LKROOT%\bin\lcdrecover -G remove
```

!remove!uname

このフラグを設定すると、uname システムで remove 後処理スクリプト (LCD を参照) をリモートで実行する必要があることを示します。このシステムで remove 後処理スクリプトが実行されると、remove 後処理スクリプトを実行するように uname システムにリモート要求が送信されます。通常、これは一時的な状態であり、LifeKeeper によって自動的に修正されます。唯一の例外は、`%LKROOT%\bin\lcdrecover -G remove` コマンドを使用して、明示的に remove 後処理スクリプトを実行する場合です。

!delete

このフラグは、delete 前処理スクリプト (LCD を参照) の実行時に LifeKeeper によって設定され、後から delete 後処理スクリプトを実行する必要があることを示します。通常、これは一時的な状態であり、delete 後処理スクリプト (LCD (1M) を参照) の実行時に LifeKeeper によって自動的に修正されます。唯一の例外は、以下のコマンドを使用して、明示的に delete 後処理スクリプトを実行する場合です。

```
%LKROOT%\bin\lcdrecover -G delete
```

!delete!uname

このフラグを設定すると、uname システムで delete 後処理スクリプト (LCD を参照) をリモートで実行する必要があることを示します。このシステムで delete 後処理スクリプトが実行されると、delete 後処理スクリプトを実行するように uname システムにリモート要求が送信されます。通常、これは一時的な状態であり、LifeKeeper によって自動的に修正されます。唯一の例外は、以下のコマンドを使用して、明示的に delete 後処理スクリプトを実行する場合です。

```
%LKROOT%\bin\lcdrecover -G delete
```

8.3.3.8. lk_chg_value

名前

lk_chg_value.ksh --- ローカルにある LifeKeeper 構成データベースファイル内の指定された値を変更します。

構文

```
lk_chg_value.ksh {-o old_value -n new_value | -f filename} [-vFIMT]
```

説明

ローカルの LifeKeeper 構成データベースファイルに登録されている任意の値 (LifeKeeper のシステム名、コミュニケーションパスのアドレス、リソースタグ名など) を変更します。**lk_chg_value.ksh** は、LifeKeeper が稼働していないクラスタノードに管理者権限でログインして実行します。また、LifeKeeper 付属のシェル (sh.exe) を使用し、前記の構文に従って、スクリプトを呼び出します。このコマンドは、システム名やネットワークインターフェースを変更しません。LifeKeeper のシステム名やコミュニケーションパスの IP アドレスを変更する場合は、システムユーティリティを使用して、システム名とネットワークインターフェースを変更してから、このコマンドを実行します。LifeKeeper を適切に更新するには、このコマンドをすべてのクラスタサーバに実行します。

値の変更は、*-o* と *-n* オプションを指定してコマンドラインから実行することも、*-f* オプションを指定してファイルを指定することもできます。ファイルを指定する場合は、置換する値を *old_value=new_value* 形式で 1 行づつ記述します。

lk_chg_value.ksh が変更する値を変更前に確認するには、*-M* オプションを指定します。**lk_chg_value.ksh** のバージョン情報を確認するには、*-v* オプションを指定します。タグ名を変更しない場合は、*-T* オプションを指定します。リソース ID を変更しない場合は、*-I* オプションを指定します。

リソース ID は構造化された情報を含むため、**lk_chg_value.ksh** は ID フィールドの完全な置換を許可しません。この動作をオーバライドするには、*-F* オプションを指定します。

例

システム A、B、C は、LifeKeeper クラスタを構成しています。システム A と B はデータベースリソースを管理し、システム A はシステム C とのコミュニケーションパスを管理しています。システム A のシステム名とコミュニケーションパスのアドレスを変更するには、次の手順に従います。

1. 各システムに lkstop コマンドを実行して、LifeKeeper を停止します。ただし、管理対象のリソースが稼働している場合は、lkstop に -f オプションを指定します。
2. システム A のシステム名を「X」、ネットワークアドレスを「new_address」にそれぞれ変更します。置換用のファイル (/tmp/lksubs) を作成し、置換前と置換後の文字列を次の形式で記述します。

   A=X old_address=new_address

管理者でシステム A にログインし、次のコマンドを実行します。

set LKROOT=<LKROOT> (例: set LKROOT=C:\LK)

<LKROOT>\bin\sh.exe lk_chg_value.ksh -vf /tmp/lksubs

システム A にある LifeKeeper Core とリカバリキットに登録されている「A」と「old_address」すべてがシステム「X」と「new_address」に置換されます。

3. 置換ファイルをシステム A からシステム B と C にコピーします。管理者でシステム B と C にログインし、次のコマンドを実行します。

set LKROOT=<LKROOT> (例: set *LKROOT=C:\LK*)

<LKROOT>\bin\sh.exe lk_chg_value.ksh -vf /tmp/lksubs

システム B と C の構成データベースに登録されている「A」と「old_address」が「X」と「new_address」にそれぞれ置換されます。

終了コード

0 処理に成功しました。

1 割り込みが発生しました。ファイルをリストアしています。

2 不正な引数が渡りました。

3 LifeKeeper プロセスは実行中です。

4 コマンドは管理者権限で実行してください。

5 ID フィールドの変更が要求されました。-I オプションを使用しないと、ID は変更できません。

6 LKROOT 環境変数が設定されていません。

7 一致するものが見つかりません。

注記

lk_chg_value.ksh ユーティリティは、*<LKROOT>\bin* フォルダにあります。

lk_chg_value.ksh ユーティリティでは、大文字と小文字が区別されます。

前述したように、**lk_chg_value.ksh** スクリプトを起動するには、LifeKeeper 付属のシェル (sh.exe) を使用します。

<LKROOT> は LifeKeeper のホームディレクトリです。デフォルトのホームディレクトリは *C:\LK* ですが、このディレクトリは、LifeKeeper をインストールするときに変更できます。

ファイル

```
<LKROOT>\bin\lk_chg_value.ksh
```

8.3.3.9. lk_err

構文

```
lk_err -c Category -n Error number -p Process Name [-d {TO_LOG |TO_STDERR}]
”Message”
```

説明

リカバリスクリプト内で実行して、Windows のイベントログにエラーを出力します。stderr (標準出力) にもメッセージを表示します。

次の引数を指定できます。

Category: LifeKeeper のメッセージカテゴリとイベントログの分類は、次のとおりです。

LK カテゴリ	イベントカテゴリ	イベントタイプ
FRS_MES	汎用	情報
FRS_WARN	汎用	警告
FRS_ERR	汎用	エラー

Error Number: 正数を指定します。

Process Name: lk_err を呼び出すスクリプトの名前を指定します。

出力先: 省略可能です。**lk_err** が生成するイベントは、デフォルトで Windows Event Log (TO_LOG) とシステムコンソール stderr のメッセージストリーム (TO_STDERR) の両方に出力されます。*-d* オプションを指定すると、いずれか一方にエラー情報を出力できます。

ただし、LifeKeeper Core は、プログラムやスクリプトを対話形式ではなく、バックグラウンドで実行するため、LifeKeeper Core が実行するプログラムやスクリプトでメッセージを stderr (TO_STDERR) にリダイレクトすると、メッセージはシステムコンソールに出力されません。手作業でスクリプトをテストしてデバッグする場合だけ、メッセージを stderr に出力してください。

Message: テキストは ” ” で囲みます。

8.3.3.10. perform_action

構文

```
perform_action [-G] [-s] [-b] [-n] -t tag-name -a action-name [- - arg1 arg2 … argn]
```

説明

LRACI プログラム **perform_action** は、次の順序でプロセスを実行します。

- *-t* オプションの引数 tag-name で指定されるリソースを探します。
- *-a* オプションの引数 *action-name* で指定される処理スクリプトを探します。
- *tag-name* リソースインスタンス上で処理スクリプトを実行します。

-- 引数の後の引数はそのまま処理スクリプトに渡されます。これらの引数は、処理の開発者が必要に応じて要求します。

perform_action プログラムは次のアルゴリズムで処理スクリプトを探します。まず、以下のように、*tag-name* で指定されるリソースインスタンスのリソースタイプについて、actions ディレクトリを検索します。

```
%LKROOT%\subsys\appname\resources\restypname\actions\action-name.ksh
```

見つからない場合は、以下のように、リソースインスタンスが属するアプリケーションの actions ディレクトリをチェックします。

```
%LKROOT%\subsys\appname\actions\action-name.ksh
```

restore 処理と remove 処理は LRACI の特例です。restore 処理は、リモートシステムで稼働している可能性があるアプリケーション階層をローカルシステムに移動します。restore 処理では、LRACI は最初にリソースインスタンス *tag-name* が ISP 状態ではないことを確認します。ISP 状態でなければ、このリソースが依存しているすべてのリソースインスタンスが再帰的にチェックされます。このチェックは、リソースが別のリソースに依存していないか、依存しているリソースがすべて ISP 状態になっていることが判明するまで継続されます。リソースが ISU 状態だった場合は、ISP 状態になります。

リソースが OSU 状態または OSF 状態だった場合は、リモートシステム上の影響を受けるリソースに対して remove スクリプトが実行されます。これが完了すると、LRACI は上記のアルゴリズムを使用して restore 処理を検索して実行します。スクリプトが失敗した場合、リソースは OSF 状態になり、LRACI は停止します。正常に実行された場合、LRACI は *tag-name* で指定されたリソースがリストアされるまで、ツリーの上に向かってリソースを再帰的に「リストア」します。次に、LRACI は関連するルートリソースインスタンスがすべてリストアされるまで、同様の方法で再帰的に親リソースインスタンスのチェックと「リストア」を行います。どの場合でも、LRACI は上記のアルゴリズムにより、LRACI が現在スキャンしているリソースのリソースアプリケーションおよびリソースタイプを使用して適切な

restore スクリプトを検索します。*tag-name* リソースのリソースアプリケーションとリソースタイプは検索に使用しません。

remove 処理では、リソースが逆方向に再帰的に移動されます。LRACI は、*tag-name* リソースに直接的または間接的に依存しているルートリソースから下に向かって、ISP 状態または ISU 状態のすべてのリソースの remove スクリプトを呼び出します。tag-name リソースも含まれます。ISP 状態でも ISU 状態でもないリソースは無視されます。いずれかの remove スクリプトが失敗した場合、LRACI は失敗したリソースを OSF 状態にして停止します。どの場合でも、LRACI は上記のアルゴリズムにより、LRACI が現在スキャンしているリソースのリソースアプリケーションおよびリソースタイプを使用して適切な remove スクリプトを検索します。*tag-name* リソースのリソースアプリケーションとリソースタイプは検索に使用しません。

remove 処理および restore 処理では、引数 *-t tag-name* および *-i ident-field* が、対象のリソースインスタンスに対応する引数リストに自動的に追加されます。

以下に、**perform_action** に指定できる引数について説明します。

-G	action-name が remove、restore、delete の場合のみ使用します。このオプションを指定しない場合、処理を実行する前後にグローバル前処理スクリプトとグローバル後処理スクリプトが実行されます (LCD の lcdrecover を参照)。このオプションを指定した場合、グローバル前処理スクリプトとグローバル後処理スクリプトは実行されません。 このオプションは、**perform_action** を 2 回以上実行する必要があるが、グローバル前処理スクリプトとグローバル後処理スクリプトは 1 回だけ実行したいときに役立ちます。また、リソース階層を作成しながら perform_action を実行する必要がある場合にも役立ちます。階層作成スクリプトは「admin lock flag」を取得するように設定されますが (LCDI_フラグ を参照)、restore 後処理スクリプトも「admin lock flag」を要求し、これによって競合の問題が発生します。そのため、階層作成時には **perform_action** によってグローバル前処理スクリプトとグローバル後処理スクリプトが実行されないようにする必要があります。
-s	restore 処理のデフォルトの動作は、指定したタグの上および下のすべてのオブジェクトを起動します。また、remove 処理のデフォルトの動作は、指定したタグの上のすべてのオブジェクトを停止します。*-s* オプションは、指定したフラグだけに処理の範囲を制限します。
-b	restore 処理のデフォルトの動作は、指定したタグの上および下のすべてのオブジェクトを起動します。*-b* オプションは、この動作を、指定したタグの下のオブジェクトだけに変更します。このオプションは remove 処理には影響しません。
-n	*action-name* が remove または restore の場合のみ使用します。このオプションを指定した場合、リソースの予約はチェックされず、リソースが予約されているかどうかにかかわらず処理が実行されます。 **警告: このオプションの使用時は、特に注意してください。** このオプションを指定しない場合、remove スクリプトまたは restore スクリプトを実行する前に、LRACI はいずれかの処理を実行するリソースが現在別のプロセスによって予約されているかどうかを確認します。リソースの「サービスからの削除」、「サービスのリストア」、または「リカバリ」の処理を実行している間リソースを予約できます。

	いずれかのリソースが予約されている場合、プロセスがリソースの予約を解除するまで、LRACI は指定された期間だけ待機します。この期間が経過すると、LRACI は予約を解除します。いずれの場合でも、LRACI はすべてのリソースを予約してから、指定されたアルゴリズムに従って処理を実行します。
-t tag-name	最後に処理が実行されるリソースインスタンス。
-a action-name	実行されるリソース処理。
-- arg1 arg2 … argn	リソース処理開発者が必要に応じて定義して、処理スクリプトに渡すことができる引数。getlocks によって保護された領域内で *-G* オプションを使用せずに **perform_action** を実行する場合は、*arg1* に *-m* を設定して、getlocks の 2 つ目のインスタンスが実行されないようにしてください。

例

例として、以下の処理を呼び出します。

```
perform_action -t SCSI-USR-DISK -a reset-heads -- -h 7
```

LRACI プログラム **perform_action** は、reset-heads に対応する処理を検索して、以下の引数で実行します。

```
reset-heads -t SCSI-USR-DISK -h 7
```

終了コード

LRACI は、次の終了コードを返します。

0	処理に成功した。
1	システムコールまたはライブラリコールが内部エラーを返した。
2	ユーザが指定した構文にエラーがある。
3	LifeKeeper の内部エラー。
4	既存のオブジェクトに対する処理を要求した。
5	不正な引数を渡した。
6	インデックスが有効な範囲を超えている。

7	存在しないオブジェクトに要求を発行した。
8	リソースインスタンスの削除を要求したが、そのリソースインスタンスには、削除していないリソースインスタンスが依存している。
9	相手のシステムと通信できない。

8.3.3.11. sendevent

構文

```
%LKROOT%\bin\sendevent -C class-of-event -E event -m monitor-name -nname-of-obj-inst [-s severity]
```

説明

イベント通知機能は、イベント通知機構 (*%LKROOT%\bin\sendevent*) とアプリケーション登録環境で構成されています。特定のイベントやアラーム、またはすべてのイベントとアラームをイベント通知機能から受信するアプリケーションは、「登録」する必要があります。

sendevent コマンドは、モニタが監視対象のオブジェクトからイベント (障害またはリカバリ) を検出した際に、デーモン監視プロセスから起動されるプログラムです。このコマンドは、一般ユーザやシステム管理者がシェル上で使用するのではなく、デーモンプロセスや別のコマンドによって起動されます。

sendevent コマンドは、イベント発生を登録済みアプリケーションに通知します。例えば、アプリケーションは、システムのシャットダウンを事前に通知されると、ファイルとデータを保存します。また、クライアントサーバ環境では、アプリケーションは別のサービスプロバイダを使用するようにそれ自身を再設定します。アプリケーションには、イベントを処理する適切なコマンドを実装する必要があります。

sendevent コマンドは、アプリケーションのイベント応答コマンドにすべてのオプションを渡します。

アプリケーションは、イベント応答コマンドを専用の登録ディレクトリ *%LKROOT%\events* にインストールして、イベントやアラーム通知を受信します。この作業は、アプリケーションのインストール時に実行します。*%LKROOT%\events* に格納されるイベントは、イベントクラスに分類されます。アプリケーション側では、genclass (汎用イベント用) と allclass サブディレクトリを作成して、イベント発生通知の受信を登録します。

注記: アプリケーション応答コマンドを特定のイベントロケーションとすべてのロケーションの両方に配置すると、イベントが発生した際に、両方のスクリプトが実行されます。

クラスディレクトリには、そのクラスに属するイベントに対応するサブディレクトリがあります。イベントを監視し、イベント通知機構を使用するアドオンパッケージは、監視サポート対象のイベントを記録します。

アプリケーションオブジェクトモニタパッケージは、各サブディレクトリに配置した ACTIVE ファイルを保持する必要があります。ACTIVE ファイルが存在する場合、モニタが起動し、特定のイベントのオブジェクトを監視していることをアプリケーションに通知します。モニタプログラムを含むパッケージを削除すると、パッケージの削除スクリプトが監視対象イベントの ACTIVE ファイルを削除します。イベントを監視しないことをアプリケーションに通知します。パッケージを削除しても、イベント応答コマンドとイベントディレクトリは削除されません。

アプリケーションが別のアプリケーションの標準的なコマンドに依存する場合、アプリケーション登録環境は、アプリケーション用の別のアプリケーション固有のディレクトリ *%LKROOT%\subsys\application-name\actions* を提供し、「共有可能な」アクションコマンドを配置します。例えば、アプリケーション X がアプリケーション Y に依存してお

り、イベントリカバリ後に起動して実行するとします。この順番に従ってアプリケーションが起動しない場合、アプリケーション X は *LKROOT%\subsys\Y\actions\start* ディレクトリからアプリケーション Y の start コマンドを呼び出します。アプリケーション間の依存関係は、アプリケーション開発者が判断して指定します。

-C (イベントのクラス) 、_-E_ (イベント)、*-m* (モニタ名)、*-n* (オブジェクトインスタンス名) オプションは必須です。*-s* (重大度) オプションを指定しないと、sendevent にはデフォルトで MAJOR アラームが設定されます。

監視プロセスが **sendevent** コマンドを起動すると、**sendevent** は、*-C* オプションと *-E* オプションの引数を参照して、イベントが発生したクラスを識別します。*sendevent* コマンドは、クラス / イベントに対応する登録ディレクトリにあるイベント応答コマンドとすべてのディレクトリに登録されたコマンドを完全に実行するまで、バックグラウンドで動作します。

指定可能なオプションは次のとおりです。

-C class-of-event

イベントはクラス別にグループ化されます。イベントが属するクラスを指定します。これは必須オプションです。

-E event

クラス内でトリガするイベントを指定します。必須オプションです。

-m monitor-name

アラーム/イベントを送信するアプリケーションオブジェクトモニタの名前は、次の形式で記述します。

```
OM-product-name:OM-component-name
```

OM-product-name には、最大 8 文字の ASCII 文字列を記述します。これは、アラームまたはイベントをトリガするオブジェクトを監視する製品の略称です。OM-component-name には、最大 16 文字の ASCII 文字列を記述します。これは、アラームまたはイベントを検出するオブジェクトモニタのコンポーネントを識別するオブジェクトモニタ名です。

モニタ名は、1 つのオブジェクトを監視する複数の製品を識別します。

-n name-of-obj-inst

アプリケーションオブジェクトのインスタンス名です。最大 64 文字の ASCII 文字列を記述します。例えば、D: はボリュームアプリケーションオブジェクトの名前を指すのに対して、1234 はプロセスオブジェクトを指すのに使用されます。

-s severity

各アラームとイベントには、報告する問題の重大度を指定します。このオプションを指定しないと、**sendevent** はデフォルトの重大度 (MAJOR アラーム) を使用します。重大度は、次表に示すように、整数 (ASCII 文字) で指定します。

0	CLEARED アラーム: 「id-of-alarm/event」が検出したアラーム
1	INFORMATIONAL アラーム: INFO メッセージまたは cmn_err () NOTICE メッセージ
2	WARNING アラーム: 警告メッセージ
3	MINOR アラーム: 重大度の低いマイナーメッセージ
4	MAJOR アラーム: メジャーメッセージまたはエラーメッセージ (デフォルト)
5	CRITICAL アラーム: 深刻なエラーを伝えるメッセージ (cmn_err () PANIC または HALT メッセージ)

出力

sendevent コマンドは、次のいずれかの条件で出力を生成します。

- エラーメッセージが標準エラーに出力されるか、0 以外の終了コードが返った場合
- sendevent を呼び出した際に、id-of-alarm/event アラーム/イベントの識別子が標準出力に出力された場合

終了コード

sendevent は、次の終了コードを返します。

0	**sendevent** コマンドはエラーを出力せずに、処理を正常に完了した。
1	引数リストに構文エラーがある。
2	***-C*** **オプションで指定されたクラスが %LKROOT%\events ディレクトリにない。**
3	***-E*** **オプションで指定した文字列に対応するイベントが %LKROOT%\events\<class>ディレクトリにない。**
4	***-A*** **オプションは内部的に生成され、直接指定することはできない。**
5	***-s 0*** **(重大度: CLEARED) オプションを使用する場合は、_-i_ オプションを指定する必要がある。**

8.3.3.12. volume

```
volume [ -d | -D ]  [-l | -u | -p | -U   volume_letter ]
```

説明

このコマンドは、Windows サーバ上にあるボリュームのロックとロック解除を行います。LifeKeeper サービスへの登録にも使用できます。このコマンドを使用して LifeKeeper にボリュームを登録した場合、LifeKeeper によりそのボリュームが起動時に保護 (ロック) されます。ロックは、ボリュームに排他制御を適用するため、他のプロセスはボリュームにアクセスできなくなります。

このコマンドを使用するには、LifeKeeper が稼働している必要があります。このコマンドは、LifeKeeper サービスと通信して、ロック機構を提供します。

volume コマンドに指定できるオプションは、次のとおりです。_volume_letter_ には、ロック / ロック解除または保護 / 保護解除するドライブレター (C ～ Z) を指定します。

-d	ロックしているボリュームを表示します。
-D	LifeKeeper に登録されているボリュームを表示します。-p オプションで追加されたボリュームを表示します。-D を指定すると、-d オプションとは異なるリストが表示されます。
-l	ボリュームを排他的アクセスとしてロックします。リモートユーザがボリュームを開くか、ローカルアプリケーションが書き込み用にボリュームを開くと、ロックは失敗します。
-u	ボリュームの排他アクセスを解除します。
-p	LifeKeeper にボリュームを登録します。LifeKeeper を再起動すると、ボリュームは自動的にロックされます。
-U	LifeKeeper に登録したボリュームを解除します。LifeKeeper を起動しても、ボリュームは自動的にロックされません。

例

`volume` コマンドの使用例を次に示します。

```
#
```

1. ドライブボリューム e: を LifeKeeper でロックするように登録する

```
#
ret=`volume -p E`
if [ $ret -gt 0 ]
then
    # ドライブボリューム e: が保護されていないエラーを報告する
fi
#
# ボリューム e: を排他アクセス用にロックする
#
ret=`volume -l E`
if [ $ret -gt 0 ]
then
    # ドライブボリューム e: が保護されていないエラーを報告する
fi
```

終了コード

このコマンドは、次の終了コードを返します。

0	処理に成功した。
正数	処理に失敗した。エラーメッセージは標準出力に表示される。

8.3.4. LKSUPPORT

LKSUPPORT　は LK/SUPPORT ディレクトリにあり、重要な設定情報ファイルとイベントログファイルを収集して zip ファイルに圧縮するために使用されます。サポートプロセスの一環として、SIOS のサポートエンジニアが通常、この zip ファイルを必要とします。このユーティリティを実行するには、LKSUPPORT をダブルクリックしてください。同じ Support ディレクトリに zip ファイルが作成されます。

8.3.5. ブラウザのセキュリティ設定

LifeKeeper Web クライアントを実行するには、ブラウザのセキュリティを低く設定する必要があります。Internet Explorer のセキュリティを設定するには、次の手順に従ってください。

警告: セキュリティを低く設定した場合は、他のサイトへのアクセスに注意してください。

Internet Explorer

Internet Explorer を安全に使用するには、[信頼済みサイト] ゾーンに SIOS Protection Suite サーバを追加します。

1. **[ツール]** メニューの **[インターネットオプション]** をクリックします。
2. **[セキュリティ]** タブをクリックします。
3. **[信頼済みサイト]** を選択し、**[レベルのカスタマイズ]** をクリックします。
4. **[カスタム設定のリセット]** で **[中低]** を選択し、**[リセット]** をクリックします。
5. **[サイト]** をクリックします。
6. 接続する SIOS Protection Suite サーバの **サーバ名** と **ポート番号** を入力します (例: http://server1:81)。

または、次の手順に従って、セキュリティを設定します。この方法は、セキュリティが少し低下します。

1. **[ツール]** メニューの **[インターネットオプション]** をクリックします。
2. **[インターネット]** または **[イントラネット]** を選択します。どちらを選択するかは、リモートシステムと SIOS Protection Suite クラスタが同じイントラネットにあるかどうかで判断します。
3. インターネットを選択した場合は、**[セキュリティレベル]** をクリックし、**[中]** を選択します。イントラネットを選択した場合は、**[中低]** を選択します。これらのレベルは、各ゾーンのデフォルトとして設定されています。
4. **[OK]** をクリックしてください。

8.3.6. IP ローカルリカバリ

IP ローカルリカバリ機能を有効にした場合、定期的に実行する IP リソースのディープチェックが失敗すると、SIOS Protection Suite は次の処理を実行します。

- SIOS Protection Suite はまず現在のネットワークインターフェースで IP アドレスを再起動します。
- 前記の処理に失敗すると、リソースインスタンスをチェックし、バックアップインターフェースが使用できるかどうかを調べます。バックアップインターフェースが使用できる場合は、IP アドレスをバックアップインターフェースに移動します。
- ローカルリカバリが完全に失敗すると、SIOS Protection Suite は、IP アドレスと依存リソースをバックアップサーバにフェイルオーバします。

ローカルリカバリ機能は、バックアップアダプタがなくても有効にすることができます。ローカルリカバリ機能を有効にすると、SIOS Protection Suite はプライマリネットワークのインターフェースを再起動しますが、それに失敗すると、リソースをバックアップサーバにフェイルオーバします。

8.3.7. SNMP による SIOS Protection Suite イベント転送の概要

SNMP (Simple Network Management Protocol) は、デバイスから独立してネットワークを管理するフレームワークを提供します。ネットワーク上のデバイスは、製造メーカーが提供する MIB (Management Information Base) 変数で定義されます。ネットワーク上の各ノードで稼働する SNMP エージェントは、Network Manager ノードと対話します。Network Manager はエージェントにクエリを発行し、MIB 変数値を取得または設定して、エージェントのノードを監視制御します。エージェントはトラップと呼ばれるメッセージを非同期的に生成して、例外イベントをマネージャに通知します。SNMP を使用してネットワークを監視管理するアプリケーションは多数あります。

SIOS Protection Suite には、特定のイベントやアラームの送信を希望するアプリケーションを登録するイベント通知機構があります (sendevent マニュアルページを参照)。SIOS Protection Suite では、主要な SIOS Protection Suite イベントの SNMP トラップを SIOS Protection Suite の動作を監視したいサードパーティ製ネットワーク管理コンソールに簡単に送信できます。SIOS Protection Suite は MIB ファイルを、SIOS Protection Suite トラップ定義を記述した `%LKROOT%\include\LifeKeeper-MIB.txt` にインストールします。

SNMP トラップを受信するリモートの管理コンソールは、そのシステムの管理ソフトウェアであらかじめ設定しておきます。SIOS Protection Suite は外部の SNMP 設定を提供していません。リモート管理サーバは通常、SIOS Protection Suite クラスタ外にあり、SIOS Protection Suite のノードではありません。

SIOS Protection Suite のイベントの表

SIOS Protection Suite のイベントとトラップ番号を次表に示します。オブジェクト ID (OID) は、プレフィックスとトラップ番号から成り、次の形式で表示されます。

prefix.0.specific trap number

プレフィックスは、**.1.3.6.1.4.1.7359** です。MIB ツリー内で展開すると、**iso.org.dod.internet.private.enterprises.7359** となります。7359 は SIOS 社の製造メーカー番号であり、LifeKeeper を表す 1 が続きます。例えば、LifeKeeper Startup Complete イベントは、OID **.1.3.6.1.4.1.7359.1.0.100** を生成します。

SIOS Protection Suite のイベントと説明	トラップ番号	オブジェクト ID
LifeKeeper Startup Complete (LifeKeeper の起動完了) LifeKeeper を起動したノードが送信	100	.1.3.6.1.4.1.7359.1.0.100
LifeKeeper Shutdown Initiated (LifeKeeper シャットダウンの開始)	101	.1.3.6.1.4.1.7359.1.0.101

シャットダウンを開始したノードが送信		
LifeKeeper Shutdown Complete (シャットダウン完了) LifeKeeper のシャットダウンを完了したノードが送信	102	.1.3.6.1.4.1.7359.1.0.102
LifeKeeper Manual Switchover Initiated on Server (LifeKeeper の手動切り替えをサーバ上で開始) 手動切り替えを要求したノードが送信	110	.1.3.6.1.4.1.7359.1.0.110
LifeKeeper Manual Switchover Complete recovered list (LifeKeeper の手動切り替え完了 - リカバリリスト) 手動切り替えを完了したノードが送信	111	.1.3.6.1.4.1.7359.1.0.111
LifeKeeper Manual Switchover Complete failed list (LifeKeeper の手動切り替え完了 - 失敗リスト) 手動切り替えを完了したノードが送信	112	.1.3.6.1.4.1.7359.1.0.112
LifeKeeper Node Failure Detected (LifeKeeper ノードの失敗検出) 失敗を検出したクラスタノードが送信	120	.1.3.6.1.4.1.7359.1.0.120
LifeKeeper Node Recovery Complete recovered list (LifeKeeper ノードのリカバリ完了 - リカバリリスト) 失敗したノードのリソースをリカバリしたクラスタノードが送信	121	.1.3.6.1.4.1.7359.1.0.121
LifeKeeper Node Recovery Complete - failed list (LifeKeeper ノードのリカバリ完了 - 失敗リスト) 失敗したノードからのリソースのリカバリに失敗したクラスタノードが送信	122	.1.3.6.1.4.1.7359.1.0.122

LifeKeeper Resource Recovery Initiated (LifeKeeper リソースのリカバリ開始) リソースをリカバリするノードが送信。直後に 131 または 132 トラップが続き、リカバリの完了または失敗を通知	130	.1.3.6.1.4.1.7359.1.0.130
LifeKeeper Resource Recovery Failed (LifeKeeper リソースのリカバリ失敗) リソースの起動に失敗したノード (トラップ 130) が送信	131*	.1.3.6.1.4.1.7359.1.0.131
LifeKeeper Resource Recovery Complete (LifeKeeper リソースのリカバリ完了) リソースのリカバリを完了したノード (トラップ 130) が送信	132	.1.3.6.1.4.1.7359.1.0.132
Mirror State Change (ミラー状態の変更) ミラーのソースであり、ミラーの状態が変更されたノードが送信。ターゲットノードのボリュームレター、ミラーの状態、および IP アドレスを表示 有効なミラーの状態は次のとおり -1: 無効な状態 0: ミラーなし 1: ミラーリング 2: ミラーは再同期中 3: ミラーは中断 4: ミラーは一時停止 5: 再同期は待ち状態	150	.1.3.6.1.4.1.7359.1.0.150
LifeKeeper replicated volume Split Brain detected (LifeKeeper によって複製されているボリュームのスプリットブレイン検出) 両側でミラーがソースであることが LifeKeeper によって検出されたノードが送信。ターゲットノードのボリュームレターおよび IP アドレスを表示	160	.1.3.6.1.4.1.7359.1.0.160
トラップ PDU の追加情報を通知する変数は次のとおり		
トラップメッセージ	すべて	.1.3.6.1.4.1.7359.1.1
リソースタグ	130	.1.3.6.1.4.1.7359.1.2

リソースタグ	131	.1.3.6.1.4.1.7359.1.2
リソースタグ	132	.1.3.6.1.4.1.7359.1.2
リカバリ済みリソースのリスト	111	.1.3.6.1.4.1.7359.1.3
リカバリ済みリソースのリスト	121	.1.3.6.1.4.1.7359.1.3
失敗したリソースのリスト	112	.1.3.6.1.4.1.7359.1.4
失敗したリソースのリスト	122	.1.3.6.1.4.1.7359.1.4

* リカバリが複数のバックアップサーバ上で失敗した場合、このトラップは連続して表示されることがあります。

8.3.8. Java のアップグレード

SIOS Protection Suite for Windows 用の Java Runtime Environment (JRE) をアップグレードする手順

1. 適切なプロバイダーから使用するバージョンのJavaをダウンロードしてインストールします。
2. LifeKeeperクラスタノードで実行されているLifeKeeper GUIセッションを終了します。
3. バックアップノード上の LifeKeeper を停止してください。

   ```
   net stop lifekeeper
   ```

4. レジストリキーを編集します。

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SteelEye\LifeKeeper\JavaGUI`：JavaHome を現在の設定から、使用したい JRE のルートフォルダに変更します。(**注記** :このフォルダには、java.exe 実行ファイルを含むサブフォルダ「bin」が含まれている必要があります)。

   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SteelEye\LifeKeeper\JavaGUI\Server`：JavaGUI JavaHome の値と同じように、Java_Home を変更します。

5. ファイアウォールが有効の場合は、Windows ファイアウォールの受信の規則 の **[LifeKeeper Java]** を開き、プロパティの **[プログラムおよびサービス]** タブを編集して Java の実行可能ファイル (例: 使用する Java バージョンの実行ファイル) を選択します。

   説明を変更して、Java JRE <バージョン番号> 用であることがわかるようにします。

   すべてのファイアウォールルールが正しく変更されていることを確認してください。

6. LifeKeeper を起動します。

   ```
   net start lifekeeper
   ```

7. 他のバックアップノード (存在する場合) で、手順 2 ～ 6 を繰り返します。
8. SIOS Protection Suite にログインし、階層をバックアップノードに切り替えます。
9. 手順 5 ～ 8 を他のプライマリノードで繰り返してください。
10. プライマリノードで、階層を [サービス開始] にします。

これで、SIOS Protection Suite が Java の最新バージョンを使用するようにアップグレードされました。

> **注記** :インストーラー/修復オプションを使用して SIOS Protection Suite のインストールで修復

が行われた場合、修復によりレジストリ設定がリセットされるため、上記の手順2～6を繰り返してください。

8.4. ユーザガイド

ユーザガイドは、LifeKeeper GUI で実行できる多数のタスクに関する詳細情報が格納された完全かつ検索可能なリソースです。

ユーザガイドは以下の分野に分かれています。

LifeKeeper GUI - これらのトピックでは、LifeKeeper グラフィカルユーザインターフェースの概要を説明します。

共通タスク - これらのトピックでは、クラスタへの接続、サーバやリソースプロパティの表示、ログファイルの表示、GUI 設定の変更など、すべてのユーザが実行できる基本的なタスクについて説明します。

オペレータタスク - このセクションでは、リソースサービスの起動と停止など、より高度なタスクについて説明します。オペレータタスクを実行するには、オペレータ権限が必要です。

詳細項目 - このセクションでは、LifeKeeper 構成データベースと LifeKeeper の通信について説明します。

メンテナンス作業 - このセクションでは、SIOS Protection Suite のメンテナンスに必要な作業について説明します。

データレプリケーション - このセクションでは、SIOS Protection Suite とともにデータレプリケーションを使用する方法について説明します。

以下の表に、それぞれのユーザ権限で使用できるデフォルトタスクを示します。特定のリソースタイプでは追加のタスクを使用できる場合があり、これらは関連するリソースキットのドキュメントに記載されています。

タスク	権限		
	ゲスト	オペレータ	管理者
サーバおよびリソースの表示	X	X	X
サーバへの接続および接続解除	X	X	X
サーバプロパティおよびログの表示	X	X	X
サーバプロパティの変更			X
リソース階層の作成		X	
コミュニケーションパスの作成および削除			X
リソースプロパティの表示	X	X	X
リソースプロパティの変更			X
リソースサービスの起動および停止		X	X
リソース階層の拡張および拡張解除			X
リソース依存関係の作成および削除			X
リソース階層の削除			X

8.4.1. LifeKeeper GUI

LifeKeeper グラフィカルユーザインターフェース

SIOS Protection Suite Core をインストールすると GUI コンポーネントもインストールされます。

LifeKeeper GUI は、Java 技術を使用して、SIOS Protection Suite およびその構成データに対するグラフィカルユーザインターフェースを提供します。LifeKeeper GUI はクライアント/サーバアプリケーションなので、ユーザはクライアントコンポーネントを実行して SIOS Protection Suite を監視、管理します。クライアントコンポーネントとサーバコンポーネントは、同一システム上で実行される場合も、異なるシステムで実行される場合もあります。

GUI の概要

ツールバー

メニュー

LifeKeeper GUI サーバコンポーネントおよびクライアントコンポーネント

SPS Web クライアントの実行

SPS サーバ上の GUI アプリケーションの実行

LifeKeeper GUI ユーザアカウント

8.4.1.1. GUI の概要

LifeKeeper GUI では、適切なアクセス権を行使して、クラスタを構成する任意のサーバ上で他のサーバやリソースを管理、運用、監視できます。詳細については、GUI ユーザの設定 を参照してください。以降に、GUI サーバとクライアントの概要を説明します。

GUI サーバ

GUI サーバは、システムを起動すると、個々の SIOS Protection Suite サーバ上で初期化されます。GUI サーバは、HTTP (Hypertext Transfer Protocol) と RMI (Remote Method Invocation) プロトコルを使用して、GUI クライアントと通信します。

GUI クライアント

GUI クライアントは、Java 対応システム上の Web クライアント、SIOS Protection Suite サーバ上のアプリケーションとして動作します。

クライアントは次のコンポーネントで構成されています。

- ステータステーブル : 接続先サーバとリソースの詳細な状態を表示します。
- プロパティパネル : ステータステーブルで最後に選択したオブジェクトに関する詳細な情報を表示します。
- アウトプットパネル : コマンドの出力を表示します。
- メッセージバー: 処理状態に関するメッセージを表示します。
- コンテキスト (プロパティパネル) とツールバー : 使用頻度の高いタスクに素早くアクセスできます。
- コンテキスト (ポップアップ) とメニュー : すべてのタスクにアクセスできます。

LifeKeeper GUI クライアントの起動

Web クライアントの起動

SIOS Protection Suite サーバ上の Web クライアントを起動するには、**[スタート]** -> **[すべてのプログラム]** -> **[SIOS]** -> **[LifeKeeper]** -> **[LifeKeeper]** の順に選択してください。Web ブラウザが起動し、ローカルの GUI サーバ (*http://localhost:81*) に接続します。

SIOS Protection Suite クラスタ外のシステムを使用する場合は、Web ブラウザを開き、URL に http://<server name>:81 を指定してください。ここで、<server name> には、SIOS Protection Suite サーバの名前を入力します。GUI サーバから Web クライアントがロードされます。

Web クライアントのロードが完了すると、[クラスタへの接続] ダイアログボックス が表示されます。Web クライアン

トを任意の GUI サーバに接続します。

注記: Web クライアントを実行した場合、適切な Java プラグインがシステムにインストールされていないと、プラグインのダウンロードサイトに自動的にジャンプします。アップグレードの手順については、Java のアップグレード を参照してください。ブラウザのセキュリティ設定で Java を有効にする 必要もあります。

以上の手順を実行しても、クライアントがロードされない場合は、Web クライアントのトラブルシューティング を参照してください。

アプリケーションクライアントの起動

SIOS Protection Suite サーバの管理者権限を持つユーザは、サーバ上でアプリケーションクライアントを起動できます。**[スタート]** メニューをクリックし、**[プログラム]** -> **[LifeKeeper]** -> **[LifeKeeper GUI]** の順に選択してください。

以上の操作を実行しても、クライアントをロードできない場合は、ネットワーク関連のトラブルシューティング を参照してください。

GUI クライアントの終了

メニュー の **[終了]** をクリックし、すべてのサーバとの接続を切断し、GUI ウィンドウを閉じます。

8.4.1.1.1. ステータステーブル

ステータステーブルには、接続先サーバとリソースの状態がグラフィカルに表示されます。表示される項目は、次のとおりです。

- 最上位の行: サーバの状態
- 左側の列: グローバル (サーバ間) の状態とリソースの親子関係
- 残りのセル: 各サーバにあるリソースの状態

サーバとリソースの状態は、グラフィックスとテキストがさまざまな色で示されます。サーバの下にあるテーブルセルが空の場合は、そのサーバにリソースが定義されていないことを示します。

ステータステーブルでサーバまたはリソースを選択すると、詳細な状態情報とコンテキストツールバーが プロパティパネル に表示されます。セルを右クリックすると、サーバコンテキストメニュー または リソースコンテキストメニュー が表示されます。

ステータステーブルは、2 つのエリアに分かれています。左右のパネルのサイズは、ディバイダを使用して変更できます。ステータステーブルは、折りたたんで最上位の項目だけを表示できます。リソース階層ツリーを展開/縮小 すると、表内の階層も展開/縮小します。

8.4.1.1.2. プロパティパネル

プロパティパネルには、ステータステーブル で選択したサーバやリソースのプロパティが表示されます。プロパティパネルの機能は、[サーバプロパティ] ダイアログボックス 、[リソースプロパティ] ダイアログボックス 、コンテキストツールバーと同じであり、使用頻度の高いコマンドを簡単に使用できるようになっています。プロパティパネルのタイトルバーには、サーバを選択すると ***server_name*** 、リソースを選択すると ***server_name: resource_name*** がそれぞれ表示されます。

プロパティパネルのコンテキストツールバーは、サーバコンテキストツールバー と リソースコンテキストツールバー で構成されています。コンテキストツールバーはカスタマイズできます。

プロパティパネルの下にあるボタンは、次の機能を備えています。

- **適用**: パネル内で編集可能なプロパティに加えた変更を反映します。このボタンは、編集可能なプロパティを変更すると有効になります。

- **更新**: すべてのプロパティの値をサーバに問い合わせて、古い変更をクリアします。このボタンは常に有効になっています。

プロパティパネルのサイズを変更するには、パネルの左側にあるセパレータを左右にスライドしてください。プロパティパネルを表示/非表示にするには、メニュー の **プロパティパネル** チェックボックスを使用してください。

8.4.1.1.3. アウトプットパネル

アウトプットパネルは、GUI クライアントが発行したコマンドの出力を収集します。コマンドを実行すると、タイムスタンプがアウトプットパネルにラベルとして追加され、コマンドの出力がその下に追加されます。複数のサーバからコマンドを発行し、複数のコマンドを同時に実行した場合、各コマンドの出力は対応するセクションに送信されるため、結果を簡単に確認できます。

アウトプットパネルのサイズを変更するには、パネルの左側にあるセパレータを上下にスライドしてください。アウトプットパネルを表示/非表示にするには、メニュー の **アウトプットパネル** チェックボックスを使用してください。アウトプットパネルを閉じても、コマンドが起動したダイアログボックスは、そのまま表示されます。出力結果は、ユーザがクリアするまで表示されます。しかし、ダイアログボックスを閉じると、コマンドの出力は表示されなくなります。アウトプットパネルを再び開くと、GUI はデフォルトの動作に戻ります。

8.4.1.1.4. メッセージバー

メッセージバーはステータスウィンドウの下に表示されます。メッセージバーには、1 行のメッセージが表示されます。例えば、「`Connecting to Server X`」、「`Failure to connect to Server X`」などのメッセージが表示されます。

- メッセージバーを隠すには、メニュー の **[メッセージバー]** チェックボックスをオフにします。
- メッセージバーを表示するには、**[表示] メニュー** の **[メッセージバー]** チェックボックスをオンにします。
- メッセージバーに表示されたメッセージの履歴を表示する方法については、メッセージ履歴の表示 を参照してください。

8.4.1.2. ツールバー

SIOS Protection Suite for Windows ツールバー

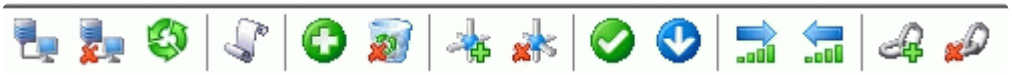
グローバル

リソースコンテキスト

サーバコンテキスト

8.4.1.2.1. グローバルツールバー

このツールバーは、デフォルトの サーバコンテキストツールバー と リソースコンテキストツールバー で構成されており、プロパティパネル に表示されます。ツールバーを使用するには、アクションを実行するサーバやリソースを選択する必要があります。



	接続 : クラスタに接続します。
	切断 : クラスタから切断します。
	更新: GUI を更新します。
	ログの表示 : ログメッセージを表示します。
	リソース階層の作成 : リソース階層を作成します。
	リソース階層の削除 : 全サーバのリソース階層を削除します。
	コミュニケーションパスの作成 : サーバ間にコミュニケーションパスを作成します。
	コミュニケーションパスの削除 : サーバからコミュニケーションパスを削除します。
	サービス開始 : リソース階層を In Service にします。
	サービス停止 : リソース階層を Out of Service にします。
	リソース階層の拡張 : フェイルオーバを実行できるように、リソース階層を別のサーバにコピーします。
	リソース階層の拡張解除 : 拡張したリソース階層を 1 台のサーバから削除します。
	依存関係の追加 : 2 つのリソースに親子関係を作成します。
	依存関係の削除 : 2 つのリソースの親子関係を削除します。

8.4.1.2.2. リソースコンテキストツールバー

リソースコンテキストツールバーは、ステータステーブル でサーバ固有のリソースを選択すると、プロパティパネル に表示されます。このページでは、デフォルトのリソースコンテキストツールバーについて説明しますが、リソースコンテキストツールバーはリソースタイプ単位でカスタマイズできます。カスタマイズの詳細については、リカバリキットに付属しているドキュメントを参照してください。

ツールバーをクリックして、所定のアクションをリソースとサーバに実行します。選択したリソースに適用できないアクションは淡色で表示されます。



	サービス開始 : リソース階層を In Service にします。
	サービス停止 : リソース階層を Out of Service にします。
	リソース階層の拡張 : フェイルオーバを実行できるように、リソース階層を別のサーバにコピーします。
	リソース階層の拡張解除 : 拡張したリソース階層を 1 台のサーバから削除します。
	依存関係の追加 : 2 つのリソースに親子関係を作成します。
	依存関係の削除 : 2 つのリソースの親子関係を削除します。
	リソース階層の削除 : 全サーバのリソース階層を削除します。

8.4.1.2.3. サーバコンテキストツールバー

サーバコンテキストツールバーは、ステータステーブル でサーバを選択すると、プロパティパネル に表示されます。ツールバーを選択して、所定のアクションをサーバに実行します。



	切断 : クラスタから切断します。
	更新: GUI を更新します。
	ログの表示 : ログメッセージを表示します。
	リソース階層の作成 : リソース階層を作成します。
	コミュニケーションパスの作成 : サーバ間にコミュニケーションパスを作成します。
	コミュニケーションパスの削除 : サーバからコミュニケーションパスを削除します。

8.4.1.3. メニュー

SIOS Protection Suite for Windows メニュー

リソースコンテキストメニュー

サーバコンテキストメニュー

［ファイル］メニュー

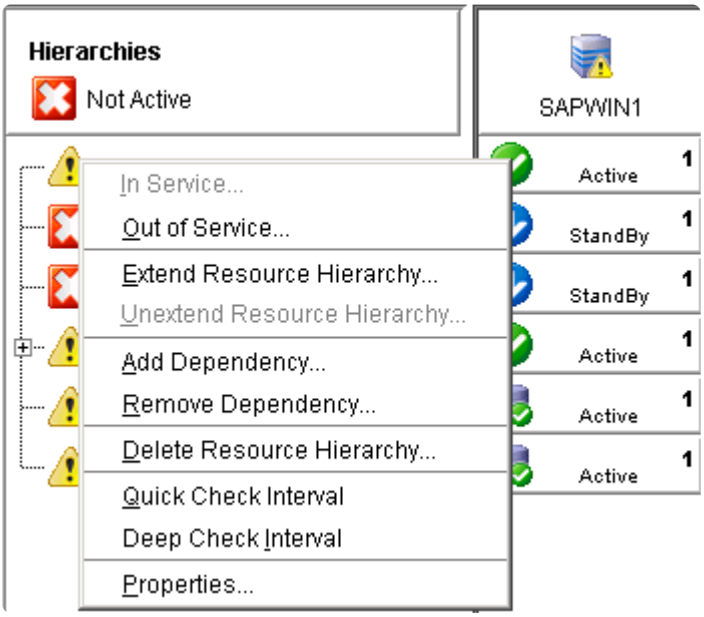
［編集］メニュー - リソース

［編集］メニュー - サーバ

［表示］メニュー

［ヘルプ］メニュー

8.4.1.3.1. リソースコンテキストメニュー



リソースコンテキストメニューは、クラスタ全体に共通するグローバルリソース (上図) またはサーバ固有のリソースインスタンス (下図) を ステータステーブル で右クリックすると表示されます。このページでは、デフォルトのリソースコンテキストメニューについて説明しますが、リソースコンテキストメニューはリソースタイプ単位でカスタマイズできます。カスタマイズの詳細については、リカバリキットに付属しているドキュメントを参照してください。

メニューを選択して、リソースに所定のアクションを実行します。特定のサーバのリソースインスタンスを選択して、アクションを実行します。また、クラスタ全体に共通するグローバルリソースを選択する場合は、アクションを実行するサーバを選択します。

サービス開始 : リソース階層を In Service にします。

サービス停止 : リソース階層を Out of Service にします。

リソース階層の拡張 : フェイルオーバを実行できるように、リソース階層を別のサーバにコピーします。

リソース階層の拡張解除 : 拡張したリソース階層を 1 台のサーバから削除します。

依存関係の追加 : 2 つのリソースに親子関係を作成します。

依存関係の削除 : 親子関係を削除します。

リソース階層の削除 : 全サーバのリソース階層を削除します。

ローカルリカバリ - リソースに対するローカルリカバリを有効にするには、[はい] を選択してください。ファイル共有のローカルリカバリは、フォルダにアクセスできなくなった場合、SIOS Protection Suite は、フォルダの再作成を行うということを意味します。

クイックチェック間隔 - リソースの基本的な状態確認の間隔を分単位で入力してください。それぞれのシステムに異なる値を指定できます。デフォルト値は 3 分です。設定値の範囲は 0 から 10080 です。間隔を 0 にするとクイックチ

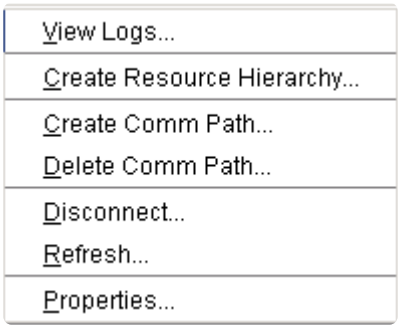
ェックは無効となります。

ディープチェック間隔 - リソースの広範囲にわたる状態確認の間隔を分単位で入力してください。ディープチェックの場合は、ディープチェックとともにクイックチェックも行います。それぞれのシステムに異なる値を指定できます。デフォルト値は 5 分です。設定値の範囲は 0 から 10080 です。間隔を 0 にするとディープチェックは無効となります。

プロパティ : [リソースプロパティ] ダイアログを表示します。

8.4.1.3.2. サーバコンテキストメニュー

サーバコンテキストメニューは、ステータステーブル でサーバを右クリックすると表示されます。メニューを選択して、所定のアクションをサーバに実行します。



ログの表示: SIOS Protection Suite ログメッセージを表示します。

リソース階層の作成 : リソース階層を作成します。

コミュニケーションパスの作成 : サーバ間にコミュニケーションパスを作成します。

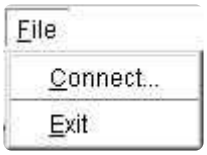
コミュニケーションパスの削除 : コミュニケーションパスを削除します。

切断 : クラスタから切断します。

更新: GUI を更新します。

プロパティ : [サーバプロパティ]ダイアログ を表示します。

8.4.1.3.3. [ファイル] メニュー

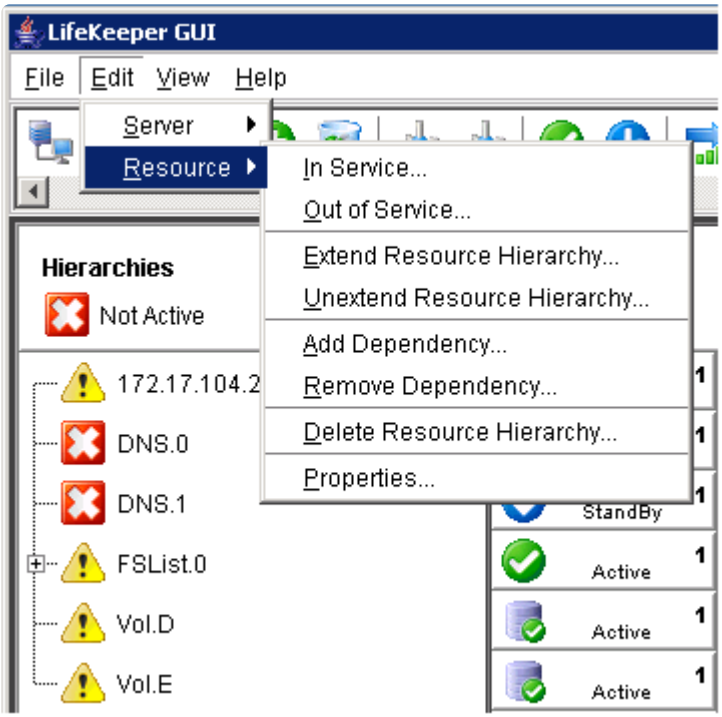


接続 : SIOS Protection Suite クラスタに接続します。サーバごとにログイン認証が必要です。

終了: すべてのサーバから切断し、GUI ウィンドウを閉じます。

8.4.1.3.4. [編集] メニュー – リソース

このメニューは、デフォルトの リソースコンテキストメニュー と基本的に同じ動作ですが、アクションを実行するリソースとサーバを選択する必要があります。**[編集]** メニューの **[リソース]** コマンドは、カスタマイズできません。



サービス開始 : リソース階層をサービス中にします。

サービス停止 : リソース階層をサービス停止にします。

リソース階層の拡張 : フェイルオーバを実行できるように、リソース階層を別のサーバにコピーします。

リソース階層の拡張解除 : 拡張したリソース階層を 1 台のサーバから削除します。

依存関係の追加 : 2 つのリソースに親子関係を作成します。

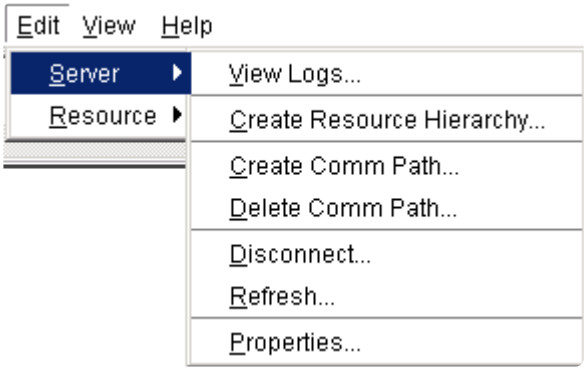
依存関係の削除 : 親子関係を削除します。

リソース階層の削除 : 全サーバのリソース階層を削除します。

プロパティ : [リソースプロパティ] ダイアログ を表示します。

8.4.1.3.5. [編集] メニュー - サーバ

このメニューは、デフォルトのサーバコンテキストメニューと基本的に同じ動作ですが、アクションを実行するサーバを選択する必要があります。**[編集] > [サーバ]** メニューは、カスタマイズできません。



ログの表示: SIOS Protection Suite ログメッセージを表示します。

リソース階層の作成: リソース階層を作成します。

コミュニケーションパスの作成: サーバ間にコミュニケーションパスを作成します。

コミュニケーションパスの削除: コミュニケーションパスを削除します。

切断: クラスタから切断します。

更新: GUI を更新します。

プロパティ [サーバプロパティ] ダイアログ を表示します。

8.4.1.3.6. [表示] メニュー



ツリーを展開：ステータステーブルを展開して、すべてのリソース階層を表示します。

ツリーを折りたたむ：ステータステーブルを折りたたみ、各階層の最上位にあるリソースだけを表示します。

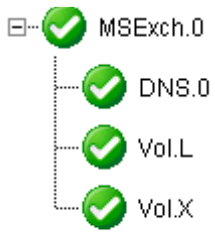
行の高さ: リソース階層ツリーおよびリソーステーブルの行の高さを修正します。表示されたリソースの数により大、中、小を選択してください。

列の幅: リソース階層ツリーおよびリソーステーブルの列幅を修正します。表示されたリソースにより **自動** 、大、中、小を選択してください。

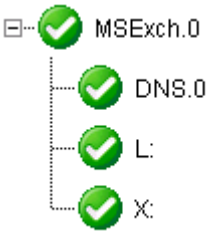
リソースラベル

このオプショングループは、リソースが、タグ名と ID のどちらでリソース階層ツリー内に表示されるか指定することができます。

タグ名



ID



ラベルでソートする: リソースラベルのみでリソースを分類します。

クラスタ単位でリソースをグループ: クラスタサーバおよびリソースラベルによって分類します。同じクラスタ内に属するリソースが同じグループになります。

コミュニケーションパスが冗長化されていない場合に警告する: サーバステータスグラフィックでコミュニケーションパスの状態についての説明を明記します。

- 選択した場合は、一組のサーバ間のコミュニケーションパスが冗長化されていない場合、サーバ警告が表示されます。
- 選択しない場合は、一組のサーバ間のコミュニケーションパスが冗長化されていない場合は無視しますが、コミュニケーションパスが切れた場合には、サーバ警告が表示されます。

ツールバー：チェックボックスをオンにするとコンポーネントが表示されます。

メッセージバー：チェックボックスをオンにするとコンポーネントが表示されます。

プロパティパネル：チェックボックスをオンにするとコンポーネントが表示されます。

アウトプットパネル：チェックボックスをオンにするとコンポーネントが表示されます。

履歴：[メッセージ履歴] ダイアログボックスのメッセージバーに最新のメッセージが表示されます。

8.4.1.3.7. [ヘルプ] メニュー



ヘルプメニュー は、**リリースノート** および **テクニカルドキュメンテーション** へリンクします。:

リリースノート: リリースノートは、新機能だけではなく製品の最終テスト時に明らかになったパッケージのバージョン、指示や手順に関する最終段階での変更点、トラブルシューティングセクションへのリンク、製品の制限、トラブル解決のヒントなどが記載されています。このドキュメントには、インストール時とその前後に留意すべき最新情報が記載されているのでソフトウェアのインストールおよび設定前に必ず確認してください。

テクニカルドキュメンテーション: オンラインドキュメントは、利用しやすいフォーマットで Steel Eye 製品に関する最新情報や詳細情報などを提供できるようデザインされています。SIOS Technology Corp. はこのサイトでサポート対象の SIOS 製品のドキュメントを管理しています。旧バージョンのドキュメントについては support@us.sios.com までご依頼ください。

About :LifeKeeper GUI のバージョン情報を表示します。

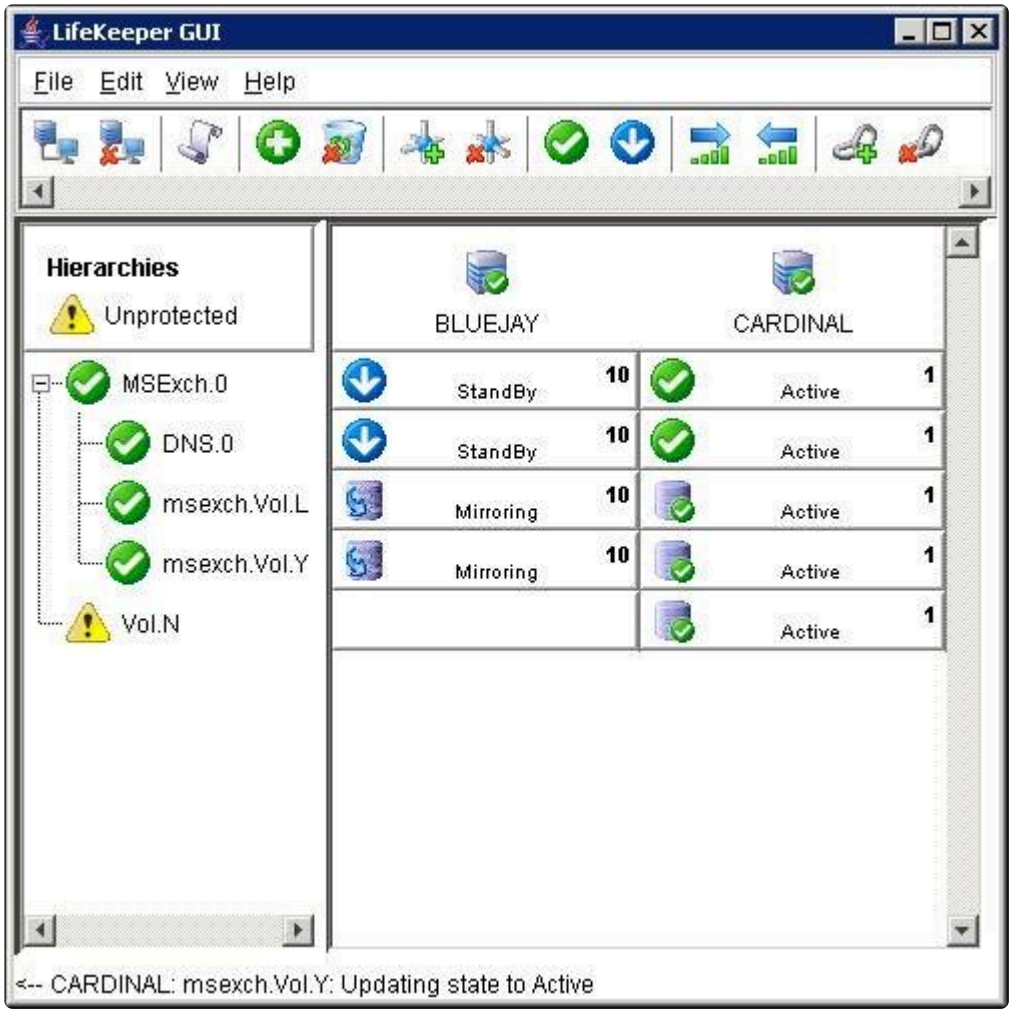
8.4.1.4. LifeKeeper GUI サーバコンポーネントおよびクライアントコンポーネント

LifeKeeper GUI サーバは、システムを起動すると、個々の SIOS Protection Suite サーバ上で初期化されます。LifeKeeper GUI サーバは、HTTP (Hypertext Transfer Protocol) と RMI (Remote Method Invocation) プロトコルを使用して、LifeKeeper GUI クライアントと通信します。

LifeKeeper GUI サーバに接続できるのは、クラスタ内のすべてのサーバのポート 81 および 82 に接続できる任意のシステムから実行できる Web クライアント、または SIOS Protection Suite に付属し、クラスタ内のサーバ上で実行するように設計されたアプリケーションクライアントです。

両方の SIOS Protection Suite クライアントに同じグラフィカルコンポーネントが含まれています。

- ポップアップのサーバコンテキストメニューおよびリソースコンテキストメニュー: サーバ関連およびリソース関連の操作にアクセスできます。
- メニューバー: LifeKeeper GUI のすべての操作にアクセスできます。
- ツールバー: 多数の SIOS Protection Suite の操作に素早くアクセスできます。
- ステータスウィンドウ: クラスタ内で接続されたサーバ、リソース階層、およびリソースとサーバのステータスがグラフィカルに表示されます。
- メッセージバー (ウィンドウの下): 処理状態が表示されます。


LifeKeeper GUI
File Edit View Help
Hierarchies
Unprotected
MSExch.0
DNS.0
msexch.Vol.L
msexch.Vol.Y
Vol.N
BLUEJAY
CARDINAL
StandBy 10
StandBy 10
Mirroring 10
Mirroring 10
Active 1
Active 1
Active 1
Active 1
Active 1
<-- CARDINAL: msexch.Vol.Y: Updating state to Active

8.4.1.5. SIOS Protection Suite Web クライアントの実行

クラスタの外部のシステムから SIOS Protection Suite を管理する場合は、Web クライアントを使用する必要があります。これは、どのオペレーティングシステムを実行するリモートシステムからでも可能です。SIOS Protection Suite for Windows は、単一セッションで Linux サーバと Windows サーバの両方を管理することはできませんが、OS に関わらず、Windows システムまたは Linux システムのいずれかを管理できます。最初に接続するサーバ OS のタイプによって、そのセッションで管理できる OS のタイプが決まります。Linux サーバと Windows サーバの両方を同時に管理する必要がある場合は、それぞれに 1 つずつ、2 つのブラウザウィンドウを開く必要があります。

リモートシステムのブラウザは、JRE 1.8 をサポートする必要があります。SIOS Protection Suite Web クライアントがサポートされるプラットフォームとブラウザについては、SIOS Protection Suite for Windows リリースノート を参照してください。以降では、リモートシステムで Web ブラウザを設定するための手順を説明します。

以下の手順に従って、SIOS Protection Suite Web クライアントを実行してください。

1. SIOS Protection Suite Web ページの URL *http://<server name>:81* (<server name> は SIOS Protection Suite サーバの名前) を開きます。Web ページには SIOS Protection Suite スプラッシュ画面とアプレットが含まれています。

   Internet Explorer を使用して Web クライアントを初めて実行した場合、適切な Java プラグインがシステムにインストールされていないと、プラグインのダウンロードサイトに自動的にジャンプします。アップグレードの手順については、Java のアップグレード を参照してください。

注記:
•プラグインをインストールした場合およびプラグインのプロパティを変更した場合は、ブラウザをいったん閉じてから再起動してください。上記の SIOS Protection Suite サーバの URL を再入力する必要があります。
Web ページが開くと、以下の処理が実行されます。
•スプラッシュ画面の表示
•アプレットの読み込み
•Java 仮想マシンの起動
•サーバファイルのダウンロード
•アプレットの初期化

ネットワークとシステムの構成によっては、これらの処理に最大 20 秒かかる場合があります。通常、アプレットの読み込み時や初期化時にはブラウザに最小限のステータスが表示されます。

注記:「証明書を確認できません。コードは未署名として扱われます」という Java プラグインのセキュリティ警告が表示される場合があります。**[OK]** をクリックしてください。

次に、スプラッシュ画面の下のアプレット領域に [起動] ボタンが表示されます。スプラッシュ画面に [起動] ボタンが表示されない場合や、アプレットの読み込みと初期化に失敗したと思われる場合は、このガイドの GUI ネットワーク関連のトラブルシューティング を参照してください。

2. **[起動]** をクリックします。SIOS Protection Suite Web クライアントが起動し、ダイアログボックス が自動的

に表示されます。接続先サーバの名前を **[サーバ名]** に入力し、**ログイン名** と **パスワード** を入力します。サーバ名を入力してクラスタへの接続が確立されると、GUI ウィンドウが表示されます。

注記: 一部のブラウザでは、アプレットによって作成されるウィンドウとダイアログに「警告: アプレットウィンドウ」が追加されます。これは正常なので、無視してください。

ブラウザのセキュリティレベルの設定

SIOS Protection Suite Web クライアントを実行するには、ブラウザのセキュリティ設定の変更が必要になる場合があります。以下の手順に従ってください。

Internet Explorer

Internet Explorer では、通常、SIOS Protection Suite サーバは自動的にローカルイントラネットゾーンに配置されます。配置されていない場合、以下のように、すべての SIOS Protection Suite サーバをローカルイントラネットゾーンに手動で追加してください。

1. [ツール] メニューの **[インターネットオプション]** をクリックします。
2. **[セキュリティ]** タブをクリックします。
3. **[ローカルイントラネット]** を選択します。
4. **[サイト]** をクリックします。
5. **[詳細設定]** をクリックします。
6. 接続する SIOS Protection Suite サーバのサーバ名とポート番号 (例: *http://server1:81*) を入力します。複数ある場合は、入力するたびに **[追加]** をクリックします。
7. 完了したら、**[OK]** をクリックします。

Mozilla Firefox

1. **[ツール]** メニューの **[オプション]** をクリックします。
2. [オプション] ダイアログボックスの **[コンテンツカテゴリ]** をクリックします。
3. **[Java を有効にする]** と **[Java スクリプトを有効にする]** オプションをオンにします。
4. **[OK]** をクリックしてください。

8.4.1.6. SIOS Protection Suite サーバ上の GUI アプリケーションの実行

LifeKeeper GUI を SIOS Protection Suite サーバ上のアプリケーションとして実行することもできます。こうすると、事実上、GUI クライアントとサーバを同一システム上で実行できます。SIOS Protection Suite サーバで管理者権限を持つユーザのみが SIOS Protection Suite アプリケーションの実行を許可されます。

1. LifeKeeper GUI を起動するには、**[スタート] -> [プログラム] -> [SIOS] -> [LifeKeeper] -> [LifeKeeper GUI]** の順にクリックします。

2. アプリケーションを読み込むと、LifeKeeper GUI が開き、ダイアログボックス が表示されます。接続先サーバの名前を **[サーバ名]** に入力し、ログイン名とパスワードを入力します。ログインの詳細は、LifeKeeper GUI ユーザアカウント を参照してください。

3. クラスタへの接続が確立されると、GUI ウィンドウが表示されます。

Web クライアントを使用して SIOS Protection Suite サーバ上で LifeKeeper GUI を実行するには、**[スタート] -> [プログラム] -> [SIOS] -> [LifeKeeper] -> [LifeKeeper]** の順にクリックしてください。Web ブラウザが起動し、*localhost:81* を使用して SIOS Protection Suite に接続します。

8.4.1.7. LifeKeeper GUI ユーザアカウント

すべての LifeKeeper GUI ユーザは SIOS Protection Suite セキュリティグループに属する必要があります。クラスタの SIOS Protection Suite 管理者は、各サーバでローカルグループとユーザアカウントを使用できます。あるいは、ドメイングループとローカルログオン権限を持ったユーザを設定できます。

ログイン

SIOS Protection Suite アカウントがクラスタ内の各サーバで同じ (同じログイン名とパスワード) である場合は、クラスタ内の 1 台のサーバにログインすると、追加のログイン手順を要求されずに他のサーバにアクセスできます。ユーザ名とともにドメイン名を入力する必要がある場合もあります (例: Southdomain\john)。

SIOS Protection Suite アカウントがクラスタ内の各サーバで異なる (ログイン名またはパスワードの少なくとも一方が異なる) 場合は、クラスタ内の最初のサーバにログインすると、クラスタ内の次のサーバにログインしようとしたときに以下のメッセージが表示されます。

```
Access denied: invalid user name or bad password.Only users with local
privileges can use LifeKeeper.Would you like to re-enter the
authentication data?
```

次のサーバにログインするためのプロンプトを表示するには、**[はい]** をクリックしてください。

8.4.1.7.1. GUI ユーザの設定

GUI ユーザには次の 3 種類があり、それぞれ異なるアクセス権が付与されます。

1. 管理者: LifeKeeper GUI を使用して、クラスタ全体を管理する権限を付与します。
2. オペレータ: 特定のサーバを対象として、構成情報とステータス情報の参照、リソースの起動と停止を実行する権限を付与します。
3. ゲスト: 特定のサーバの構成情報とステータス情報を参照する権限を付与します。

アクセス権の付与は、クラスタ全体を対象とすることを推奨します。アクセス権をサーバ単位で設定すると、ユーザが混乱し、管理作業が繁雑になります。

ユーザ管理では、各サーバのローカルユーザグループにユーザを割り当てます。ローカルの Administrators グループに割り当てたユーザは、管理者権限を持ちます。ローカルの *LK_OPERATOR* グループに割り当てたユーザは、オペレータ権限を持ちます。ローカルの *LK_GUEST* グループに割り当てたユーザは、ゲスト権限を持ちます。ローカルの Administrators グループは、Windows OS にあらかじめ設定されていますが、残り 2 つのローカルグループは、LifeKeeper 管理者が作成します。

英語版の Windows でグループ名を設定するには、*Server_RB_en.properties* ファイルのエントリを編集します。このファイルは、*$LKROOT/htdoc/com/SIOS/LifeKeeper/locale* に格納されています。グループ名をローカライズするには、同じフォルダに *Server_RB_xx.properties* ファイルを作成し、エントリを編集してください。ここで、ファイル名の「xx」には、ロケールコードを記述します。

ドメインコントローラで管理するローカルグループとユーザが未定義の場合は、信頼できるグローバルセキュリティグループとして、*LK_OPERATOR* と *LK_GUEST* グループを作成してください。次に、グループのセキュリティポリシーを作成し、ローカルからのログオンを各グループに許可してください。

ローカルの Windows サーバへのログオンを許可するには、次の手順に従ってください。

1. ローカルの管理者権限でサーバにログインします。
2. Windows の管理ツールにある **ローカルセキュリティポリシー MMC** を起動します。
3. **[ローカルポリシー]** から **[ユーザ権限の割り当て]** までスクロールします。
4. 詳細ペインに移動し、**[ローカルのログオンを許可する]** ポリシー をダブルクリックします。
5. **[ユーザとグループの追加...]** をクリックし、前記の手順で作成した *LK_OPERATOR* と *LK_GUEST* ドメイングループを [ローカルログイン権限] に追加します。

> 重要: ドメイン GPO (グループポリシーオブジェクト) によりローカルポリシーの変更が上書きされていないことを確認してください。

最後に *gpupdate* コマンド (詳細は https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpupdate を参照) を実行して、これらの変更を有効にする必要があります。一度このコマンドを実行すると、SIOS Protection Suite は、それらのグループを認識して適切なアクセス権を割り当てることができます。

注記: ローカルサーバにグループとユーザを作成した場合、アクセス権の割り当ては、そのサーバの GUI 権限だけに適用されます。ローカルサーバだけを設定した場合は、同じ操作をクラスタサーバ全体に繰り返してください。このような手順を踏むと、作業量は増えますが、ドメインコントローラにアクセスする必要がないため、クラスタがより堅牢になります。

注記: 先に説明したGUIグループ名、Administrators、LK_OPERATOR、LK_GUESTを変更することはできません。

8.4.2. 共通タスク

このセクションでは、すべてのユーザが実行できる基本的なタスクについて説明します。

クラスタへの接続

クラスタからの切断

接続されたサーバの表示

サーバステータスの表示

サーバログファイルの表示

サーバプロパティの表示

リソースタグと ID の表示

リソースステータスの表示

リソースプロパティの表示

メッセージ履歴の表示

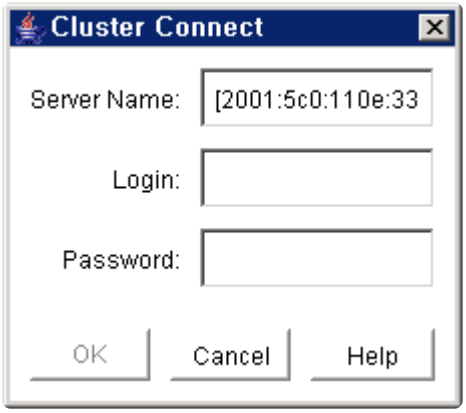
リソース階層ツリーの展開と縮小

8.4.2.1. クラスタへの接続

1. メニュー または ツールバー から **[接続]** をクリックします。

2. ダイアログボックス の **[サーバ名]** フィールドに、クラスタ内の接続先サーバの名前を入力します。

   注記: IPv6 アドレスを使用する場合は、そのアドレスを括弧 [ ] で囲む必要があります。その結果 IPv6 アドレスを通して接続が確立されます。あるいはそのアドレスに名前を割り当てると、その名前を接続に使用することができます。



3. 接続先サーバの SIOS Protection Suite を管理するユーザのログイン名とパスワードを **[ログイン]** と **[パスワード]** フィールドに入力します。

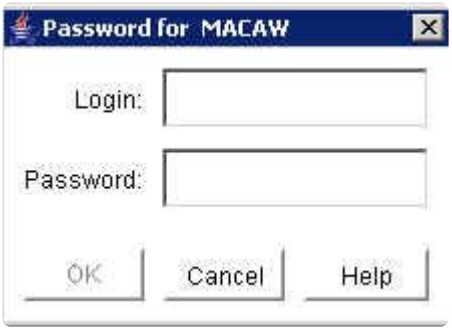
4. **[OK]** をクリックしてください。

指定したサーバに正常に接続すると、GUI は新しいサーバが検出されなくなるまでクラスタを構成する既知のサーバすべてに接続し、接続したサーバをステータス表示に追加します。

注記: クラスタ内の接続先サーバで最初に入力したログイン名とパスワードによるクライアント認証に失敗した場合、ユーザはそのサーバで使用できる別のログイン名とパスワードの入力を求められます。［パスワード］ダイアログボックス の **[キャンセル]** をクリックすると、指定したサーバへの接続は中止されますが、クラスタ内の他のサーバへの接続処理は続行されます。

パスワード ダイアログボックス

注記: このダイアログボックスは、クラスタへの接続 ダイアログボックス に無効なログイン名やパスワードを入力した場合に表示されます。



ログイン 指定したサーバにある LifeKeeper を管理するユーザのログイン名を指定します。

パスワード 接続先サーバにログインするパスワードを指定します。

8.4.2.2. クラスタからの切断

クラスタを構成する全サーバからクライアントを切断します。

1. 切断するサーバを選択し、サーバコンテキストメニュー または サーバコンテキストツールバー の **[切断]** をクリックします。

2. クラスタを構成する全サーバが **[確認]** ダイアログボックスに表示されます。**[確認]** ダイアログボックスの **[OK]** をクリックし、クラスタ内の全サーバから切断することを確認します。

クラスタを切断すると、クラスタを構成する全サーバが ステータステーブル から削除されます。

8.4.2.3. 接続先サーバの表示

サーバの状態は、GUI 画面にアイコンで表示されます (次図)。アイコンの意味については、サーバステータスの表示 を参照してください。



8.4.2.4. サーバステータスの表示

サーバステータスは、次図に示すように、テーブルヘッダにアイコンで表示されます。



サーバの状態	アイコン	表示状態
ALIVE (稼働中)		クライアントはサーバに接続しています。 サービスを提供しているリモートサーバとのコミュニケーションパスは稼働しています。 停止中のサーバは独自のアイコンで表示されるため、停止中のコミュニケーションパスとサーバは無視されます。
ALIVE (稼働中)		クライアントはサーバに接続しています。 リモートサーバ間のコミュニケーションパスは、1 本以上が停止しています。 リモートサーバとの間に冗長なコミュニケーションパスがありません。
DEAD (停止)		他のクラスタサーバから停止が報告されています。
UNKNOWN (不明)		ネットワークが切断されました。「不明」になる前は、「稼働中」でした。

8.4.2.5. サーバログファイルの表示

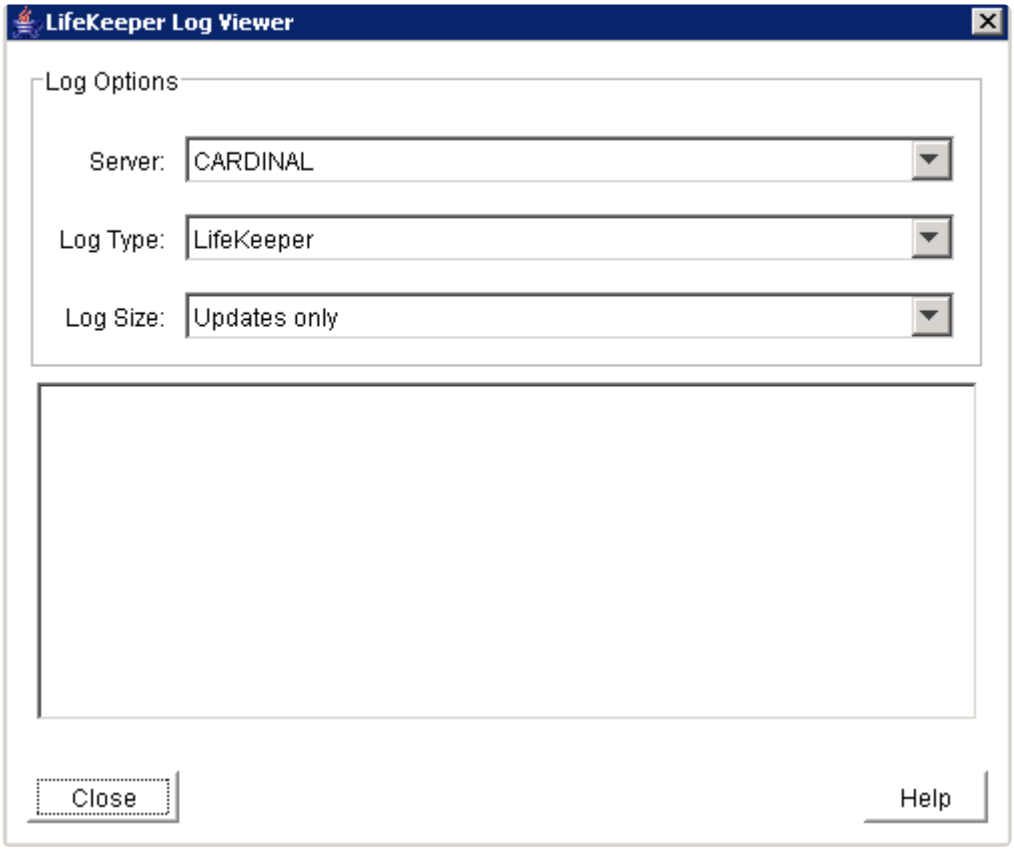
サーバログファイルを表示するには、以下の操作を実行してください。

1. サーバを選択し、サーバコンテキストメニュー または サーバコンテキストツールバー の **[ログの表示]** をクリックします。ダイアログボックス が開きます。

2. ログを閲覧したら、**[OK]** をクリックして、ダイアログボックスを閉じます。

ログビューア ダイアログボックス

ログビューア ダイアログボックスを開くには、サーバコンテキストメニューまたはツールバーを使用します。ログビューア ダイアログボックスには、LifeKeeper が管理しているログファイルの一部が表示されます。ツールバーを使用してダイアログボックスを開いた場合、サーバの一覧からサーバを選択すると、サーバのログファイルを参照できます。



サーバ: クラスタに接続したサーバの一覧がドロップダウンリストに表示されます。参照するログファイルが保存されているサーバを選択します。ただし、サーバコンテキストメニュー を使用して ログビューア ダイアログボックスを開いた場合、この一覧は表示されません。

ログタイプ: 選択したサーバに保存されているログファイルの一覧がドロップダウンリストに表示されます。参照するログファイルを指定するオプションを選択します。

- LifeKeeper

ログサイズ: 4 つのオプションがドロップダウンリストに表示されます。表示するログファイルの行数を指定します。

- 更新のみ
- 最後の 100 行
- 最後の 500 行
- 最後の 1000 行

8.4.2.6. サーバプロパティの表示

サーバプロパティを表示するには、以下の操作を実行してください。

- プロパティパネル が有効な場合、ステータステーブル からサーバを選択すると、**プロパティパネル** にサーバのプロパティが表示されます。
- プロパティパネルが無効な場合は、サーバを選択し、サーバコンテキストメニュー の **[プロパティ]** をクリックしてください。

8.4.2.7. リソースタグと ID の表示

リソースのタグと ID を表示するには、ステータスウィンドウのリソースアイコン上にマウスカーソルを移動し、マウスを左クリック (シングルクリック) してください。優先順位が最も低いサーバのタグと ID がメッセージバーに表示されます。サーバを指定して、リソースタグと ID を表示するには、テーブルでリソースインスタンスのセルをシングルクリックしてください。

次のようなメッセージがメッセージバーに表示されます。

```
Resource Tag = F-Drive, Resource ID = F:
```

状況によっては、GUI がリソース ID を特定できないことがあります。その場合は、リソースタグだけがメッセージバーに表示されます。

8.4.2.8. リソースステータスの表示

リソースのステータス (状態) は次の 2 種類の形式で表示されます。**グローバルリソースステータス** (すべてのサーバのリソース) と **サーバリソースステータス** (サーバ単体のリソース) です。グローバルリソースステータスは、ステータスウィンドウの左側のペインにある **リソース階層ツリー** に表示されます。サーバリソースステータスは、表内でリソース行とサーバ列が交差するセルに表示されます。

サーバリソースのステータス

サーバリソースの状態	アイコン	表示状態
アクティブ		このサーバでは、リソースが稼働しており、LifeKeeper で保護されています (ISP)。
縮退		リソースは稼働していますが、バックアップリソースで保護されていません (ISU)。
スタンバイ		バックアップリソースは、アクティブなリソースをフェイルオーバできる状態にあります (OSU)。
障害		障害が発生しています。例えば、リソースの起動に失敗したことが考えられます (OSF)。
不明		リソースが初期化されていないか (ILLSTATE)、SIOS Protection Suite が稼働していません。
	(表示なし)	リソースが定義されていません。

グローバルリソースのステータス

説明	アイコン	意味/原因
正常		リソースがアクティブであり (ISP)、バックアップもすべてアクティブです。
警告		リソースはアクティブです (ISP)。1 つ以上のバックアップが不明であるか、障害が発生しています (OSF)。
失敗 いずれかのサーバでリソースがアクティブではありません (OSF)		リソースは正常な理由によりサービスが停止されています。 リソースは異常な方法で停止されました。 リカバリは完了していないか、失敗しています。
不明 現在のデータだけではリソースの状態を判定できません		複数のサーバでリソースが起動しています。 サーバとの接続が切断されています。 すべてのサーバリソースインスタンスが不明な状態です。

8.4.2.9. リソースプロパティの表示

リソースプロパティを表示するには、以下の操作を実行してください。

- プロパティパネル が有効な場合、サーバ固有のリソースインスタンスを ステータステーブル から選択すると、**プロパティパネル** にプロパティが表示されます。

- プロパティパネルが無効な場合は、サーバ固有のリソースインスタンスを選択し、リソースコンテキストメニュー の **[プロパティ]** をクリックしてください。

8.4.2.10. メッセージ履歴の表示

1. メニュー の **[履歴]** をクリックします。**[メッセージ履歴]** ダイアログボックスが開きます (次図)。
2. 履歴を完全にクリアするには、**[クリア]** をクリックします。
3. **[OK]** をクリックしてダイアログボックスを閉じます。

[メッセージ履歴] ダイアログボックスには、メッセージバーに表示された最新のメッセージが表示されます。履歴には 1,000 行まで表示できます。新しいメッセージが到着し、メッセージが 1,000 行を超えると、古いメッセージから削除されます。

メッセージは、クライアントとサーバ間のアクションだけを表示します。リストでは最新のメッセージが一番上に表示されます。

メッセージ履歴の読み方

<-- : サーバが送信したメッセージです。次の形式で表示されます。

```
<--"server name":"action"
<--"server name":"app res": "action"
<--"server name":"res instance":"action"
```

--> : クライアントが送信したメッセージです。次の形式で表示されます。

```
-->"server name":"action"
-->"server name":"app res": "action"
-->"server name":"res instance":"action"
```

[クリア] をクリックすると、履歴がクリアされますが、ダイアログボックスは閉じません。

[OK] をクリックすると、履歴をクリアせずに、ダイアログボックスが閉じます。

8.4.2.11. リソース階層ツリーの展開と縮小

	*MSExch.0* リソースは折りたたまれています。 *MSExch.0* リソースは展開されています。 は、折りたたまれている場合に表示されます。 は、ツリーを展開すると、リソースアイコンの左側に表示されます。

リソース階層を展開するには、以下のいずれかの操作を行います。

-  をクリックする。
-  の右側にあるリソースアイコンをダブルクリックする。

リソース階層をすべて展開するには、以下のいずれかの操作を行います。

- 「表示」メニュー の **[ツリーを展開]** をクリックする。
- ステータステーブル の左上隅にある **[階層]** をダブルクリックする。

注記: リソース階層に表示されるリソースタグ (または ID) は、優先度が最も低いサーバのものです。サーバを指定して、リソースタグや ID を表示するには、表内のリソースインスタンスのセルを左クリックします。指定したサーバのタグと ID がメッセージバーに表示されます。

リソース階層を縮小するには、以下のいずれかの操作を行います。

-  をクリックする。
-  の右側にあるリソースアイコンをダブルクリックする。

リソース階層をすべて縮小するには、以下のいずれかの操作を行います。

- 「表示」メニュー の **[ツリーを折りたたむ]** をクリックする。
- ステータステーブル の左上隅にある **[階層]** をダブルクリックする。

8.4.3. オペレータタスク

このセクションでは、リソースサービスの起動と停止など、より高度なタスクについて説明します。オペレータタスクを実行するには、オペレータ権限が必要です。

リソースを起動する

リソースを停止する

ボリュームリソースの起動と停止

ボリュームシャドウコピー

共有 SCSI ボリュームのボリュームロック

8.4.3.1. リソースを起動する

リソースを起動するには、以下の操作を実行してください。

1. サービスを起動するサーバ固有のリソースインスタンスを選択し、リソースコンテキストメニュー または リソースコンテキストツールバー の **[サービス開始]** をクリックします。

2. サービスを開始するサーバとリソースを確認するダイアログボックスが表示されます。親リソースを起動せずに、依存する子リソースだけを起動すると、ダイアログボックスに警告メッセージが表示されます。**[サービス開始]** をクリックし、依存する子リソースとともに、リソースを起動します。

3. アウトプットパネル が有効な場合は、ダイアログボックスが閉じて、リソースを起動した結果がアウトプットパネルに表示されます。すべての結果が表示されたら、**[完了]** をクリックしてダイアログボックスを閉じます。

4. リソースを起動する際に発生したエラーは、LifeKeeper ログおよびリソースを起動したサーバの GUI ログに記録されます。

8.4.3.2. リソースを停止する

リソースを停止するには、以下の操作を実行してください。

1. サービスを停止するサーバ固有のリソースインスタンスを選択し、リソースコンテキストメニュー または リソースコンテキストツールバー の **[サービス停止]** をクリックします。

2. 停止するリソースを確認するダイアログボックスが表示されます。親リソースを停止せずに、依存する子リソースを停止すると、ダイアログボックスに警告メッセージが表示されます。**[サービス停止]** をクリックし、リソースを停止します。

3. アウトプットパネル が有効な場合は、ダイアログボックスが閉じて、リソースを停止した結果がアウトプットパネルに表示されます。アウトプットパネルが無効な場合は、ダイアログボックスに結果が表示されます。すべての結果が表示されたら、**[完了]** をクリックしてダイアログボックスを閉じます。

4. リソースを停止する際に発生したエラーは、LifeKeeper ログ、およびリソースを停止するサーバの GUI ログに記録されます。

8.4.3.3. ボリュームリソースの起動と停止

ウイルススキャナや Windows サービスなど、バックグラウンドで動作するプロセスは、共有ボリュームに書き込み権限を要求します。こうしたプロセスはアプリケーションの実行に不可欠であり、長期的に停止させられません。

バックグラウンドで動作するアプリケーションは通常、SIOS Protection Suite ボリュームの手動切り替えに影響しません。しかし、手動切り替え時に次のエラーメッセージが表示される場合、実際のフェイルオーバには影響が出ませんが、後述するボリューム削除時の停止と再起動機能で修正します。

```
*ERROR*  [No. 12035]  Unable to lock volume <volume ID> on <system name>
machine at this time as it may be in use by some application. Please free
this volume and try again.
```

書き込み権限のないユーザがボリュームにアクセスし、リモートリンクやローカルオープンを実行している場合、ボリュームの削除は、他のシステムへのボリュームのリストアと同様に成功します。既存ユーザのオープン操作は、当然ながら、無効となります。ただし、元のシステムにボリュームをリストアする操作は、手動切り替えでも、自動的なフェイルオーバでも失敗します。こうした操作を実行すると、次のエラーメッセージが表示されます。

```
*ERROR* [No. 12046] LifeKeeper RESTORE VOLUME <volume ID> FAILED.
```

ローカルユーザ (またはリモートユーザ) がボリュームにアクセスすると、ボリュームの削除とリストア、バックアップサーバへのボリュームの切り替え、ボリュームリソースを含む階層の切り替えは失敗します。

また、システムの PATH 変数には、SIOS Protection Suite で保護するボリュームにファイル共有を指定できません。PATH 変数にファイル共有を指定すると、ボリューム操作が失敗することがあります。SIOS Protection Suite でボリュームリソースを作成する前に、ファイル共有を削除してください。PATH 変数を変更するには、**[コントロール パネル]** を開き、**[システム]** - **[環境]** を選択します。

ボリューム削除時のプログラムとサービスの停止と再起動

SIOS Protection Suite では、レジストリキーを編集すると、ボリューム削除時に停止して再起動するプログラムとサービスを指定できます。SIOS Protection Suite は、ユーザがボリュームを削除してサービスを停止した場合、そのボリュームにオープンハンドルがあれば、指定されたプログラムとサービスを停止します。しかしサービスから削除されるボリュームのオープンハンドルを SIOS Protection Suite が検知しないと、プログラムとサービスを停止しません。ボリュームを削除するときに、プログラムとサービスを停止するには、次の手順に従います。

1. 削除するボリュームにアクセスし、フェイルオーバをブロックしているプログラムとサービスを探します。

2. 以下の各プログラムのサブキーを追加し、停止して再起動するプログラムを指定します。

- **64ビット: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SIOS\LifeKeeper\VolumeRemoveStopPrograms\*`**
  例えば、「myapp.exe」というプログラムを停止するには、次のサブキーを追加します。
  `HKEY_LOCAL_MACHINE\SOFTWARE\SIOS\LifeKeeper\VolumeRemoveStopPrograms\`

myapp.exe

3. 各プログラムのサブキーに次の値 (REG_SZ) を追加します。

ProgramName	プログラム名のみ (注記: 手順 2 で指定したサブキー名を使用します。)
ProgramPath	プログラム名 (絶対パス)
Restart	プログラムを再起動しない場合は、0 を指定します。再起動する場合は、1 を指定します。
StartCmdLine	プログラム起動時に渡すコマンドラインオプションを指定します。
WasRunning	SIOS Protection Suite によって、プログラム停止前に稼働していたインスタンス数を記憶します。0 に初期化します。

例えば、`myapp.exe /a /t /p` を停止して再起動する場合は、次のようにレジストリを編集します。

ProgramName	myapp.exe
ProgramPath	C:\mydir\myapp.exe
Restart	1
StartCmdLine	/a /t /p
WasRunning	0

注記: SIOS Protection Suite はデフォルトで `perfmon.exe` を停止するサブキーをレジストリに書き込むため、再起動オプションは無効になります。

1. 以下の各サービスにサブキーを追加し、停止して再起動するサービスを指定します。

- **64 ビット:HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SIOS\LifeKeeper\VolumeRemoveStopServices**
  例えば、「mysvc」というサービスを停止するには、次のサブキーを追加します。
  HKEY_LOCAL_MACHINE\SOFTWARE\SIOS\LifeKeeper\VolumeRemoveStopServices\mysvc

2. 各サービスのサブキーに次の値 (REG_SZ) を追加します。

ServiceName	サービス表示名 (注記: 手順 4 のサブキー名と一致する必要があります。)
Restart	プログラムを再起動しない場合は、0 を指定します。再起動する場合は、1 を指定します。
WasRunning	SIOS Protection Suite によって、プログラム停止前に稼働していたインスタンス数を記憶します。0 に初期化します。
StopWait	サービスが STOPPED 状態になるまで待機する秒数。StopWait に負数を指定すると、サービスとフェイルオーバは、STOPPED 状態に達するまで無制限に待機します。
StartWait	サービスが RUNNING 状態になるまで待機する秒数。サービスが指定した時間内に RUNNING 状態に達しないと、エラーがイベントログに記録されます。StartWait に負数を指定すると、フェイルオーバはサービスが起動するまで無制限に待機します。0 を設定すると、サービスは起動しますが、RUNNING 状態になるまで待機しません。そのため、サービスが再起動しなくても、イベントログメッセージは生成されません。

例えば、`mysvc` を停止して起動するには、次のように設定します。

ServiceName	mysvc
Restart	1
WasRunning	0
StopWait	120
StartWait	120

ボリューム復元時のプログラムとサービスの停止と再起動

SIOS Protection Suite では、レジストリキーを編集すると、ボリュームを復元するときにシステム上で停止して再起動するプログラムとサービスを指定できます。この機能は、前述したボリューム削除時のプログラムとサービスの停止と再起動と基本的に同じですが、次の点が異なります。

- 停止して再起動するプログラムは、以下のサブキーに指定します。
  - **64ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SIOS\LifeKeeper\VolumeStopPrograms**

- 停止して再起動するサービスは、以下のサブキーに指定します。
  - **64ビット: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SIOS\LifeKeeper\VolumeStopServices**

8.4.3.4. ボリュームシャドウコピー (VSS)

DataKeeper/SIOS Protection Suite ボリュームでボリュームシャドウコピー (VSS) を使用する

Windows 2008 R2 では、SIOS Protection Suite によって保護される (共有または複製) ボリュームで VSS シャドウコピーを有効にすることができます。ただし、以下のガイドラインが適用されます。

- SIOS Protection Suite によって保護されるボリュームには VSS スナップショットイメージを保存できません。SIOS Protection Suite によって保護されるボリュームに VSS スナップショットを保存すると、SIOS Protection Suite はボリュームをロックして別のノードにスイッチオーバすることができません。

- SIOS Protection Suite によって保護されるボリュームがスイッチオーバまたはフェイルオーバした場合、SIOS Protection Suite によって保護されるボリュームから取得された以前のスナップショットは破棄され、再利用することができません。

- VSS スナップショットスケジュールは SIOS Protection Suite サーバ間でコピーされません。プライマリサーバで 1 日 2 回スナップショットを取得するように予定されているときにスイッチオーバが発生した場合、このスケジュールはバックアップサーバには渡されず、バックアップサーバで再定義する必要があります。

- スナップショットが以前有効になっていたサーバに切り替えられた場合、動作にわずかな違いがあります。
    - ボリュームが共有ボリュームである場合は、VSS スナップショットを再度有効にする必要があります。
    - ボリュームが複製ボリュームである場合は、VSS スナップショットは自動的に有効になります。

8.4.3.5. 共有 SCSI ボリュームのボリュームロック

共有 SCSI ディスク上のリソースを保護するには、**Windows のディスク管理** ツールを使用して、共有ディスクを論理ボリュームに分割します。ボリュームリソースインスタンスを定義すると、SIOS Protection Suite で共有ボリュームを保護できます。インスタンスにはドライブレターを指定します (例: G:)。

SIOS Protection Suite は、ボリュームリソースインスタンスをプライマリサーバで起動した後、ソフトウェアロックをかけます。その結果、ボリュームがプライマリサーバでアクティブな限り、バックアップサーバはボリュームにアクセスできません。プライマリサーバに障害が発生すると、SIOS Protection Suite はボリュームリソースをバックアップサーバで起動し、修復中のプライマリサーバがボリュームリソースにアクセスできないようにロックします。

SIOS Protection Suite は、プライマリとバックアップを入れ替えるため、障害が発生したサーバは、ボリュームリソースにアクセスできなくなります。そのため、障害が発生したサーバを修理している間は、不適切なアクセスからリソースを保護できます。

SIOS Protection Suite のインテリジェントスイッチバック機能は、プライマリサーバとバックアップサーバを動的に再定義します。そのために、修理が完了したら、適当なタイミングを指定して、修復したサーバでリソースを起動できます。

ボリュームがロックされているときは、SIOS Protection Suite を停止しないでください。SIOS Protection Suite を停止するとロックが無効になります。

8.4.4. 詳細項目

このセクションでは、LifeKeeper 構成データベースと LifeKeeper の通信について説明します。

LifeKeeper 構成データベース

LCD のディレクトリ構造

LCD ディレクトリの構造図

LCD 構成データ

LCD リソースタイプ

リソースサブディレクトリ

LCDI コマンド

LifeKeeper 通信マネージャ

通信ステータス情報

8.4.4.1. LifeKeeper 構成データベース (LCD)

LifeKeeper 構成データベース (LCD) は、オブジェクト指向のリソース階層情報を保持しています。SIOS Protection Suite が保護するリソースタイプのリカバリ方向に関する情報も格納しています。LCD データはシステムの共有メモリにキャッシュされてから、ファイルに格納されるため、システムを再起動しても構成データは保持されます。LCD にはリカバリに必要なリソースインスタンスに関する状態情報や詳細なデータも格納されています。

LCD のディレクトリ構造、格納するデータの種類、利用可能なリソースタイプ、アプリケーションスクリプトの使用方法などについては、次の項目を参照してください。

- LCD のディレクトリ構造
- LCD ディレクトリの構造図 $lkroot/LifeKeeper
- LCD 構成データ

8.4.4.2. LCD のディレクトリ構造

$LKROOT (デフォルトは *c:\LK*) には、次のサブディレクトリがあります。

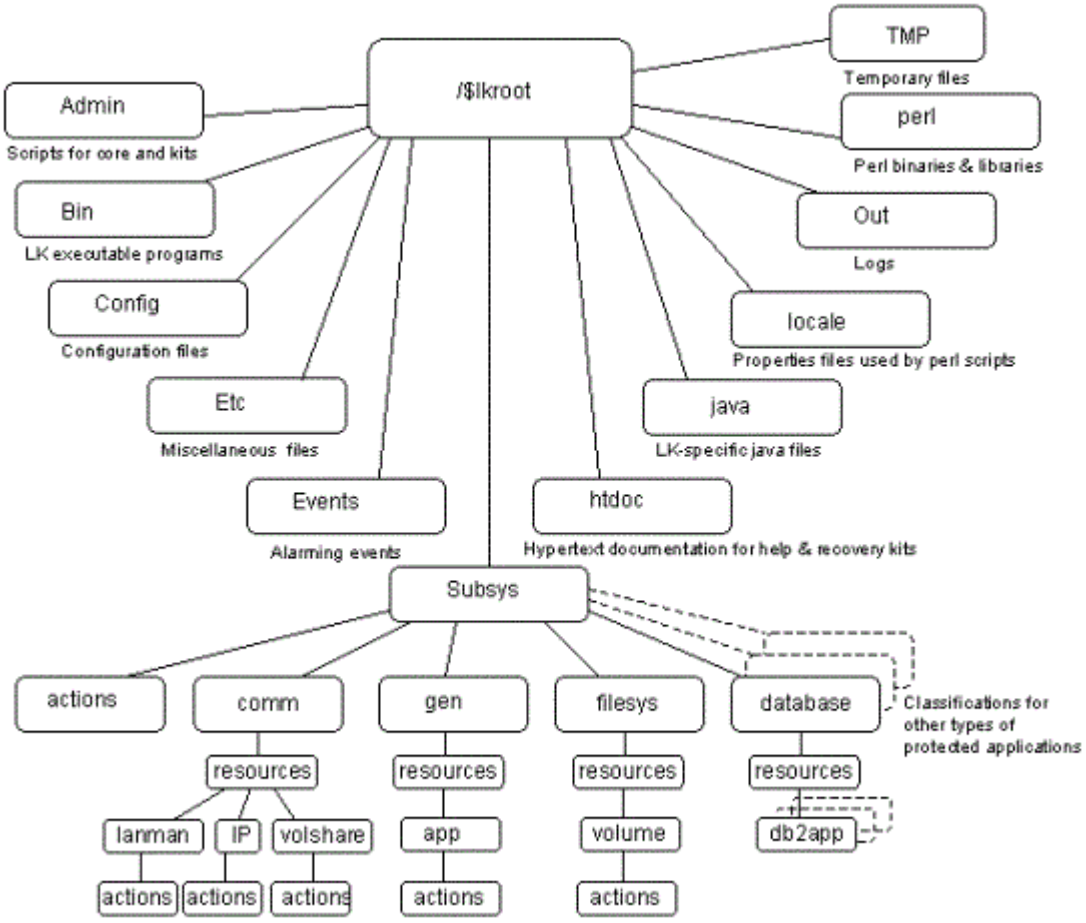
- **Admin**: SIOS Protection Suite Core とリカバリキットのスクリプトが格納されています。
- **Config**: 共有イクイバレンシなどの SIOS Protection Suite 構成ファイルが格納されています。
- **Bin**: SIOS Protection Suite の実行ファイルが格納されています。
- **Subsys**: リソースとタイプに関する情報が格納されています。SIOS Protection Suite は Subsys サブディレクトリの下にリソースとタイプの定義を格納します。例えば、通信リソースは comm、ボリュームリソースは filesys、Generic Application のリソースは gen にそれぞれ格納されます。オプションのリカバリキットは、固有のリソースタイプを別のディレクトリに作成します。例えば、データベースアプリケーションのリソースは database ディレクトリに格納されます。
- **Events**: イベントアラームが格納されています。
- **Out**: LifeKeeper のログが格納されています。SIOS Protection Suite は、エラーとメッセージの種類に応じて、ログをディレクトリに送ります。
- **perl**:Perl の実行可能プログラム (バイナリ) とライブラリが格納されています。

$LKROOT 以下の LCD ディレクトリ構造については、LCD ディレクトリの構造図 を参照してください。

注記: サブディレクトリの場所は、環境変数 LKROOT の値を編集すると変更できます。

8.4.4.3. LCD ディレクトリの構造図

$lkroot のディレクトリ構造を次図に示します。



8.4.4.4. LCD 構成データ

LCD には次のデータが格納されています。

- 依存関係に関する情報
- リソースステータスに関する情報
- サーバ間のイクイバレンシに関する情報

依存関係に関する情報

SIOS Protection Suite は、依存元と依存先のリストを定義済みリソースごとに保持しています。他のリソースに依存するリソースを依存元と呼びます。詳細については、マニュアルページの LCDI 関係 と LCDI インスタンス を参照してください。

リソースステータスに関する情報

LCD にはリソースインスタンスのステータス情報が格納されています。LCD には、リソースの状態 として、**ISP** 、**OSF** 、**OSU** 、**ILLSTATE** が記録されています。リソースの状態は、システムイベントが発生するか、管理者が特定の作業を実行すると変化します。リソースの状態が変化すると、その情報がローカルサーバとバックアップサーバの LCD に反映されます。

サーバ間のイクイバレンシに関する情報

複数のサーバが保持するリソースには、一定の関係があります。共有イクイバレンシ とは、同じ物理エンティティである複数のサーバが保持する 2 つのリソースの関係を指します。2 台のサーバが共有イクイバレンシ関係を持つリソースを保持する場合、SIOS Protection Suite は一方のサーバが保持するリソースインスタンスだけを「サービス中 (ISP)」にして、スプリットブレインを回避します。2 台のサーバのリソースインスタンスは、両方ともサービス休止状態 (OSU または OSF) にできますが、リソースをサービス中 (ISP) にする場合は、一方のサーバだけでリソースを起動して、データの完全性を保証します。

イクイバレンシリソースには、SCSI バスで接続したディスクなどがあります。

LifeKeeper は、階層内に依存関係を設定して、共有ファイルなど、ボリュームに依存する全リソースが一方のサーバだけで稼働することを保証します。

8.4.4.5. LCD リソースタイプ

LifeKeeper 構成データベース (LCD) は、共有メモリと *$LKROOT* ディレクトリで保持されています。LifeKeeper 構成データベース (LCD) の ディレクトリ構造図 に示したように、subsys にはアプリケーションインターフェースを定義する次のアプリケーションリソースセットが格納されています。

- filesys - ボリュームなどのファイルシステム関連リソース
- comm - IP、共有ボリューム (共有ファイル)、LAN Manager などの通信関連リソース
- database - Oracle などのデータベースリソース

サブディレクトリの詳細については、リソースサブディレクトリ を参照してください。

8.4.4.6. リソースサブディレクトリ

filesys 、*comm* 、*WebServer* 、*database* 、*mail* 、*appsuite* の各ディレクトリには、*resources* サブディレクトリがあります。resources ディレクトリには、SIOS Protection Suite に定義して管理するリソースタイプのリストが格納されています。

- **ファイルシステムリソースタイプ**: *$LKROOT\LifeKeeper\subsys\filesys\resources* ディレクトリに格納されています。
  - **ボリューム**: ディスクパーティションまたは仮想ディスクデバイスです。
- **通信リソースタイプ**: */$LKROOT/LifeKeeper/subsys/comm/resources* ディレクトリに格納されています。
  - **IP**: IP リカバリキットで作成するリソースです。
  - **DNS**: DNS リカバリキットで作成するリソースです。
  - **volshare**: LAN Manager リカバリキットが作成するファイル共有リソースです。
  - **lanman**: LAN Manager リカバリキットが作成するコンピュータの別名です。
- **WebServer リソースタイプ**: *$LKROOT\LifeKeeper\subsys\WebServer\resources* ディレクトリに格納されています。
  - **IIS**: IIS リカバリキットで作成するリソースです。
- **データベースリソースタイプ**: *$LKROOT\LifeKeeper\subsys\database\resources* ディレクトリに格納されています。
  - **Microsoft SQL Server**
  - **PostgreSQL**
- **メールリソースタイプ**: *$LKROOT\LifeKeeper\subsys\mail\resources* ディレクトリに格納されています。

各リソースタイプディレクトリには、次のサブディレクトリがあります。

- ***instances***: LifeKeeper 構成データベース (LCD) に格納されたリソースインスタンスに関する恒久的な情報を保存するファイルです。このリソースタイプに関連するリソースインスタンスの説明が記述されています。

- ***actions***: 特定のリソースタイプのリソースインスタンスで動作する一連のリカバリアクションプログラムが格納されています。アプリケーションのすべてのリソースタイプに適用するアクションは、*リソースタイプ_ディレクトリではなく、_アプリケーション_ディレクトリの _actions* サブディレクトリに配置します。リカバリディレクションソフトウェアは、リソースインスタンスを変更または修復します。

リソースタイプの *actions* ディレクトリには、**remove** と **restore** スクリプトをセットで格納する必要があります。

リソース操作

リソースタイプの *actions* ディレクトリには、特定のアプリケーション機能を記述するプログラム (通常はシェルスクリプト) があります。リソースタイプには restore と remove スクリプトが必要です。

remove と restore スクリプトは、互いに逆の機能を実行し、一方が他方の処理を取り消します。スクリプトは手動で実行しないでください。スクリプトは、LifeKeeper リカバリ制御インターフェース (LRACI) の perform_action シェルプログラムから実行します。詳細については、LRACI-perform_action マニュアルページを参照してください。

8.4.4.7. LCDI コマンド

SIOS Protection Suite では、次の 2 種類の方法でアプリケーションのリソース階層を定義できます。

- LifeKeeper GUI
- LifeKeeper 構成データベースインターフェース (LCDI) のコマンド

LCDI は、SIOS Protection Suite が提供する一連のインターフェースコマンドです。LCDI を使用すると、ユーザのアプリケーション要件に従って、リソース階層を作成してカスタマイズできます。例えば、アプリケーションが複数のリソース (ファイルシステムなど) に依存する場合は、コマンドインターフェースを使用します。

コマンドの詳細については、LCDI のマニュアルページ を参照してください。ここでは、GUI とコマンドの両方を使用して、リソース階層を作成する開発シナリオについて説明します。

8.4.4.8. LifeKeeper 通信マネージャ (LCM)

LifeKeeper 通信マネージャ (LCM) は、SIOS Protection Suite サーバに高信頼性のプロセス間通信を提供します。コミュニケーションパスを冗長化すると、1 本のコミュニケーションパスに障害が発生しても、SIOS Protection Suite と保護対象リソースは停止しません。LCM は、RS-232 (TTY)、TCP/IP、共有ディスク接続をサポートしています。

LCM は次の機能を提供します。

- **SIOS Protection Suite ハートビート**:SIOS Protection Suite システムに定期的に信号を送信し、他のシステムの死活状態を確認します。SIOS Protection Suite は、ハートビート信号が停止すると、システム全体に障害が発生したと解釈します。この機能は他の手段では実現できません。

- **管理サービス**:SIOS Protection Suite は、LCM を使用して、クラスタサーバをリモートから管理します。LCM を使用すると、クラスタサーバの一元管理、クラスタ構成の検証、管理アクションの健全性検査を実行できます。

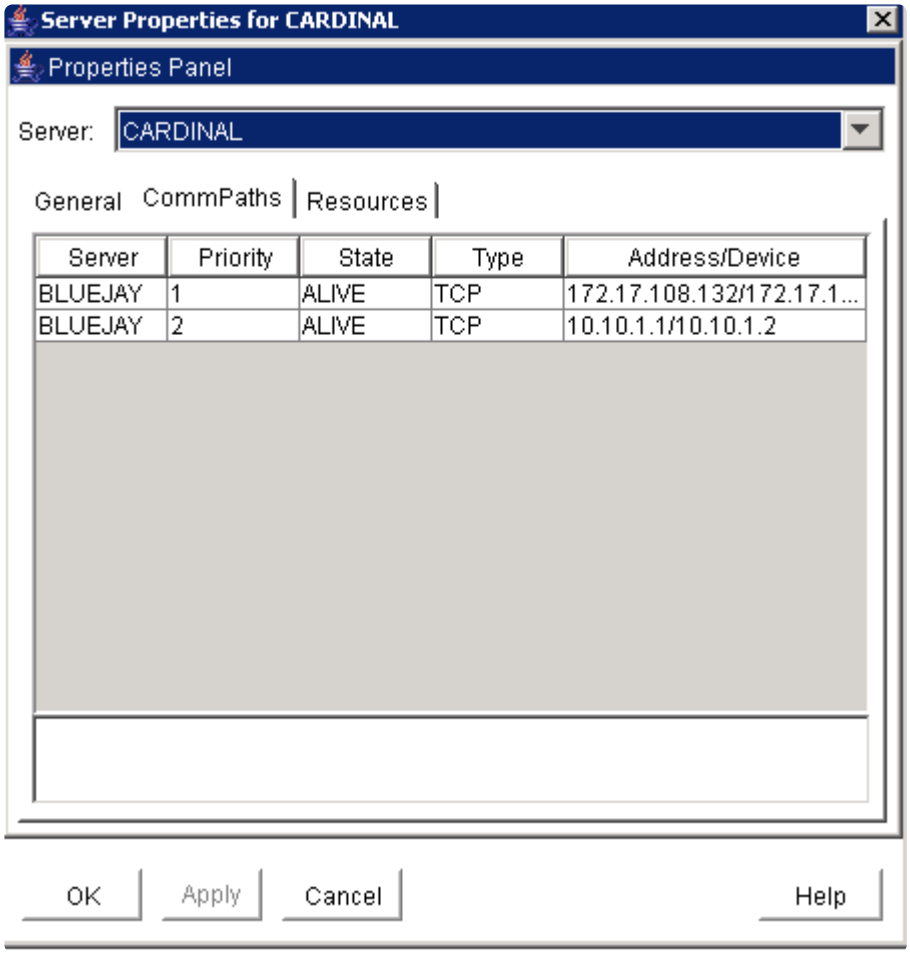
- **クラスタ構成とステータス通信**:LifeKeeper 構成データベース (LCD) は、LCM を介して、リソースのステータス、可用性、クラスタ構成を追跡し、LCD におけるプライマリサーバとバックアップサーバ間でリソース情報の整合性を保証します。

- **フェイルオーバリカバリ**:システム上のリソースに障害が発生すると、LCM は、リソースをバックアップシステムで起動するように SIOS Protection Suite に通知します。

8.4.4.9. 通信ステータス情報

ダイアログボックス の **[通信]** タブには、SIOS Protection Suite に登録したサーバの一覧、カレントステータス、コミュニケーションパスに関する情報が表示されます。

サーバプロパティ – コミュニケーションパス タブ



8.4.5. メンテナンス作業

このセクションでは、SIOS Protection Suite のメンテナンスに必要な作業について説明します。

LifeKeeper の起動と停止

IP リソース管理

DNS リソースの管理

保護されるファイル共有のリストの表示

EditFileShareResource ユーティリティ

リソース階層の移動

共有ディスクのオフラインメンテナンス

LifeKeeper で保護するシステムの保守

Generic Application スクリプトの設定

リソース階層の保守

フェイルオーバ後のリカバリ作業

SPS のアンインストール

保護対象のボリュームでCHKDSKを実行する

8.4.5.1. LifeKeeper の起動と停止

LifeKeeper は、インストールを完了して、サーバを起動すると、自動的に稼働します。そのため、通常は、LifeKeeper を手動で起動/停止する必要はありません。ただし、カスタムインストールを実行し、LifeKeeper のインストール後に自動起動しないことを選択した場合は、手動で操作する必要があります。

LifeKeeper を手動で起動または停止するには、Windows の [コントロール パネル] にある **[管理]** タスクの **[サービス]** ツールを使用してください。

LifeKeeper の起動

LifeKeeper には、次の 2 つのサービスがあります。

- LifeKeeper
- LifeKeeper External Interfaces

2 つのサービスは、同時に起動/停止する必要があります。ただし、LifeKeeper External Interfaces は LifeKeeper サービスに依存するため、LifeKeeper External Interfaces を停止すると、LifeKeeper サービスも停止します。そのため、LifeKeeper External Interfaces は、LifeKeeper サービスの前に起動する必要があります。

[LifeKeeper] を選択し、**[起動]** をクリックします。**[LifeKeeper External Interfaces]** サービスが自動的に起動します。

LifeKeeper の停止

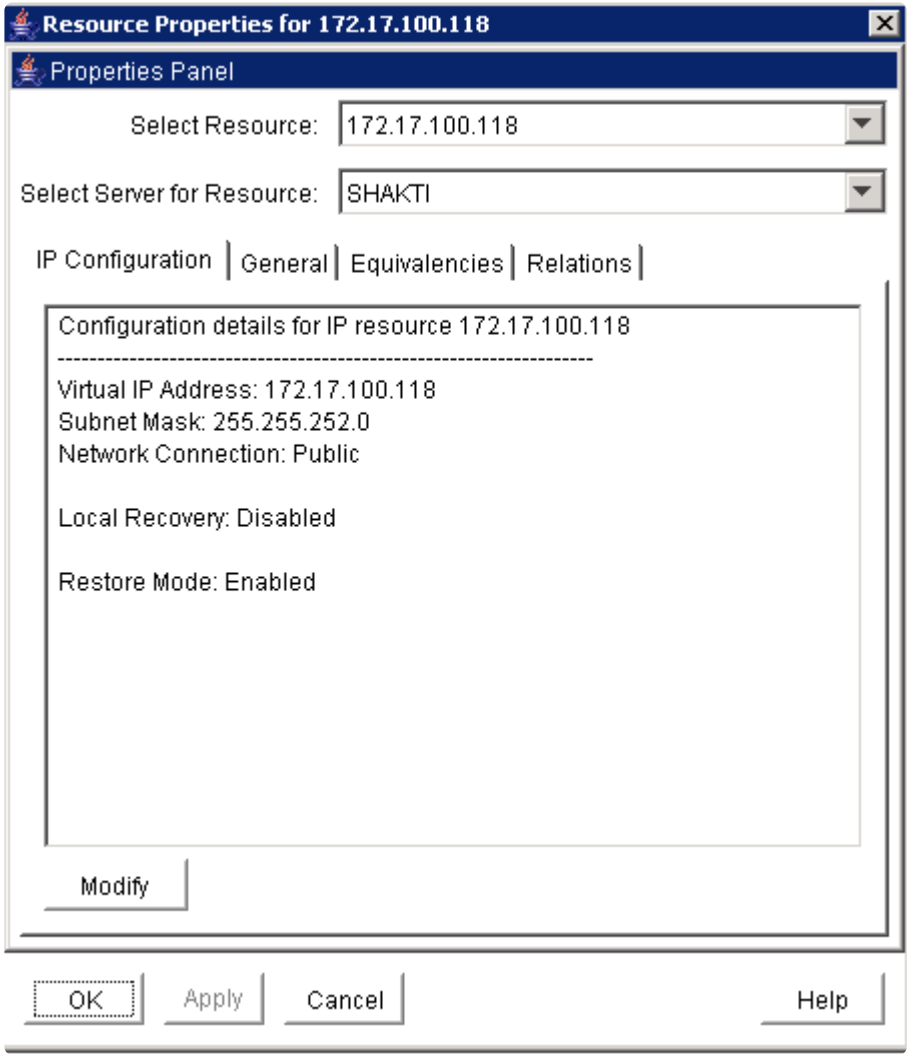
Windows の **サービス** アプリケーションを起動し、**[LifeKeeper External Interfaces]** を選択し、**[停止]** を選択します。両方のサービスが停止します。[サービス] ツールでは直ちに停止されたかのように表示されますが、LifeKeeper の停止にかかる時間は階層の設定によって異なります。

コマンドラインから $LKROOT\bin\lkstop を実行すると、サービス停止を正確に確認できます LIFEKEEPER NOW STOPPED というメッセージが表示されます)。

注記: LifeKeeper を停止すると、保護対象のすべての階層のサービスが休止します。そのため、保護対象のアプリケーションにアクセスできなくなります。

8.4.5.2. IP リソース管理

LifeKeeper で保護する IP リソースの設定情報を GUI に表示するには、右側のペインで IP リソースを右クリックし、**[プロパティ] - [IP 設定]** タブを選択してください。SIOS Protection Suite が保護する IP リソース (172.17.100.118) の詳細を次図に示します。



SIOS Protection Suite IP リソースを起動した状態で、選択したサーバの IP アドレスリストア機能を有効/無効に設定するには、**[変更]** をクリックし、**[有効] または [無効]** を選択して、リストアモードを設定してください。IP アドレスのリストア機能は、同じサブネットにある LAN ノード 2 台と異なるサブネット上にある WAN ノード 1 台で構成する 3 ノード SIOS Protection Suite クラスタに適用されます。IP リソースのリストアモードは、LAN ノードでは有効、WAN ノードでは無効にそれぞれ設定されます。

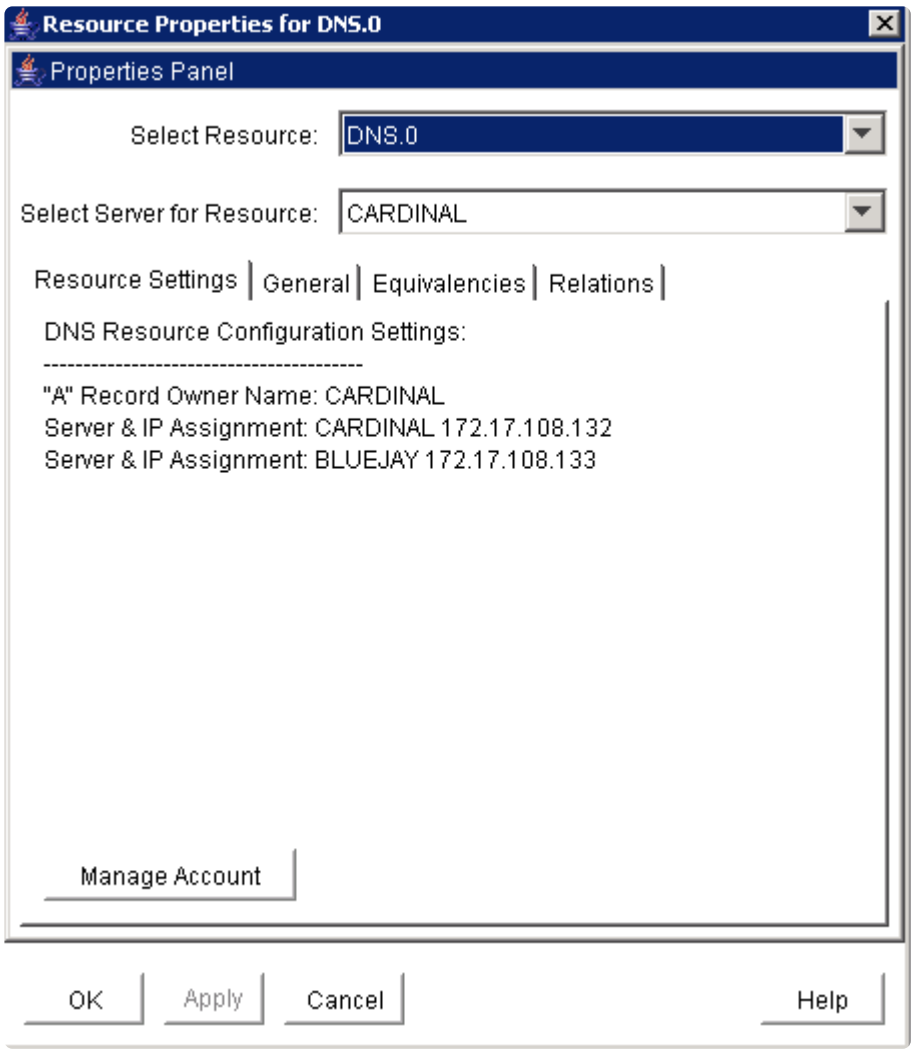
有効な IP アドレスを含むファイルを作成することで、Pinglist 機能を有効にできます。この機能は、ファイル内のアドレスへの ping を試行します。IP アドレスのいずれかが ping に応答すると成功し、応答しない場合は失敗します。IP リストア操作の終了時および IP Quick Check 中に pinglist チェックが実行されます。pinglist はオプションなので、ファイルが見つからない場合、リストアと Quick Check はこのテストをスキップします。

この機能を有効にするために必要なファイルは %LKROOT%/Subsys/comm/resources/ip/ に配置し、"pinglist.<tag>" という名前にする必要があります。<tag> は保護されている IP リソースの名前です。IP アドレスは、ファイル内の 1行に 1つずつ入力する必要があります。使用される IP アドレスは、保護された IP アドレスのサ

ブネットから到達可能であり、ICMP PING 要求に応答する必要があります。

8.4.5.3. DNS リソースの管理

LifeKeeper GUI を使用して、保護対象の DNS リソースに関連付けたドメイン管理ユーザとグループを変更するには、右側のペインにある DNS リソースを右クリックし、**[プロパティ]** をクリックし、**[リソース設定]** タブをクリックしてください。[リソース設定] ページの **[管理アカウント]** をクリックし、DNS リソースのドメイン管理ユーザとグループとパスワードを変更してください。

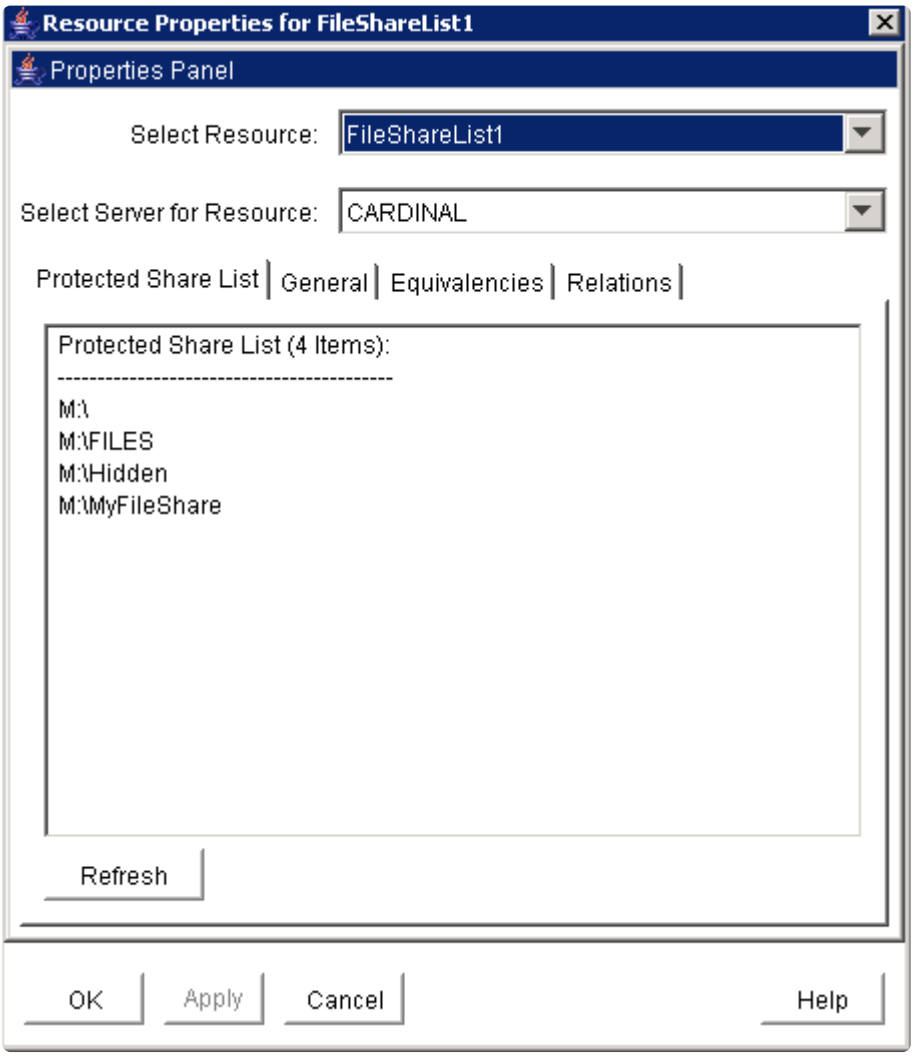


管理アカウント

フィールド	説明
ユーザ ID の入力 (Domain/UserID)	Windows DNS/ドメイン管理者のユーザ名を入力します。このユーザアカウントには DNS 設定を変更する権限が必要です。ユーザは、DNS サーバと同じドメインの「Domain Admins」グループに属している必要があります。ユーザ ID は *<DomainName>**<UserID>* 形式で入力します。*<DomainName>* はドメインの NetBIOS 名です。
パスワードの入力	前記の手順で作成したアカウントのパスワードを入力します。

8.4.5.4. 保護対象の共有ファイルリストの表示

保護対象の共有リソースに関連付けた共有ファイルの一覧を表示するには、GUI の右側にある共有ファイルリソースを右クリックして **[プロパティ]** を選択し、**[保護対象の共有リスト]** タブをクリックしてください。



8.4.5.5. EditFileShareResource ユーティリティ

EditFileShareResource ユーティリティを使用すると、関連ボリューム上にあるすべての現在のファイル共有でファイル共有リソースを更新できます。このユーティリティは、多数のファイル共有があり、リソースを作成した後で、ファイル共有を追加または削除するときに使用します。このユーティリティを使用すると、ファイル共有リソースを削除して再作成する必要がなくなります。

ユーティリティを起動するには、コマンドラインから次のように入力します。

```
EditFileShareResource <Tag name>
```

<Tag name> は、現在サービス中のファイル共有リソースのタグ名です。

このユーティリティは、ファイル共有階層に関連付けた保護対象ボリュームに定義されている **すべてのファイル共有** を保護します。また、すでにシステムから削除された古い保護対象ファイル共有を削除し、所定の基準に従って、新たに定義したファイル共有をファイル共有リストに追加します。ファイル共有に定義されているファイル共有パーミッションも更新します。

8.4.5.6. リソース階層の移動

SIOS Protection Suite サーバを定期的に保守する場合は、LifeKeeper GUI を使用して、稼働中のリソースを別のサーバに移動します。リソース階層をサーバ A からサーバ B に移動するには、LifeKeeper GUI を使用して、サーバ B でリソース階層を起動します。サーバ A のリソース階層すべてをバックアップサーバで起動するまで、この操作を繰り返してください。詳細については、リソースを起動する を参照してください。

サーバ A の全リソースをバックアップサーバで起動すると、サーバ A をシャットダウンしても、アプリケーション操作に影響しません。ただし、クラスタを構成するサーバ数によっては、保守作業を行っている間は、リソースを SIOS Protection Suite で保護できないことがあります。

8.4.5.7. 共有ディスクのオフラインメンテナンス

共有 SCSI ホストアダプタや共有バス上のディスクをオフラインで保守する場合は、LifeKeeper を停止した後、すべてのサーバと共有ディスクの電源をオフにします。保守管理作業は、次の順序で行ってください。

1. **LifeKeeper を停止します。[サービス]** ツールを使用して、SIOS Protection Suite サーバで稼働している LifeKeeper サービスと LifeKeeper External Interfaces サービスを停止します。リソース保護が解除されます。

2. **Windows をシャットダウンします。** クラスタサーバで稼働している Windows オペレーティングシステムをすべてシャットダウンします。

3. **サーバの電源をオフにします。**

4. **共有ディスクの電源をオフにします。**

5. **保守作業を行います。** 共有 SCSI ホストアダプタや共有ディスクを保守します。

6. **共有ディスクの電源をオンにします。**

7. **サーバの電源を 1 台づつ順番に入れます。** Windows オペレーティングシステムが完全に起動したら、次のサーバの電源をオンにします。

8. **LifeKeeper を起動します。** Administrator 権限でログオンし、**[サービス]** ツールを使用して、各 SIOS Protection Suite サーバの LifeKeeper サービスと LifeKeeper External Interfaces サービスを起動します。SIOS Protection Suite は、共有ファイルシステムをマウントした後、共有ディスク上のデータベースを再起動してサービスを開始します。

8.4.5.8. SIOS Protection Suite で保護するシステムの保守

SIOS Protection Suite で保護するサーバをシャットダウンして保守する場合は、作業を始める前に、リソース階層をバックアップサーバで起動します。リソース階層をバックアップサーバで起動すると、保守するシステム上の共有ディスクは完全に停止します。共有ディスクのオフラインメンテナンスについては、共有ディスクのオフラインメンテナンスを参照してください。

保守作業は次の手順に従って行います。ここで、保守するプライマリサーバをサーバ A、バックアップサーバをサーバ B とします。

1. **サーバ B でリソース階層を起動します** 。バックアップサーバ (サーバ B) の LifeKeeper GUI を使用して、サーバ A で稼働しているリソース階層をサーバ B で起動します。保護対象の共有ディスクに常駐し、サーバ A にマウントしているファイルシステムが解除されます。詳細については、リソースを起動する を参照してください。

2. **サーバ A の LifeKeeper を停止します** 。Windows の **サービス** アプリケーションを起動し、**[LifeKeeper External Interfaces]** を選択し、**[停止]** を選択します。両方のサービスが停止します。リソース保護が解除されます。

3. **サーバ A をシャットダウンします** 。サーバ A の Windows オペレーティングシステムをシャットダウンし、電源をオフにします。

4. **保守作業を行います。** サーバ A を保守します。

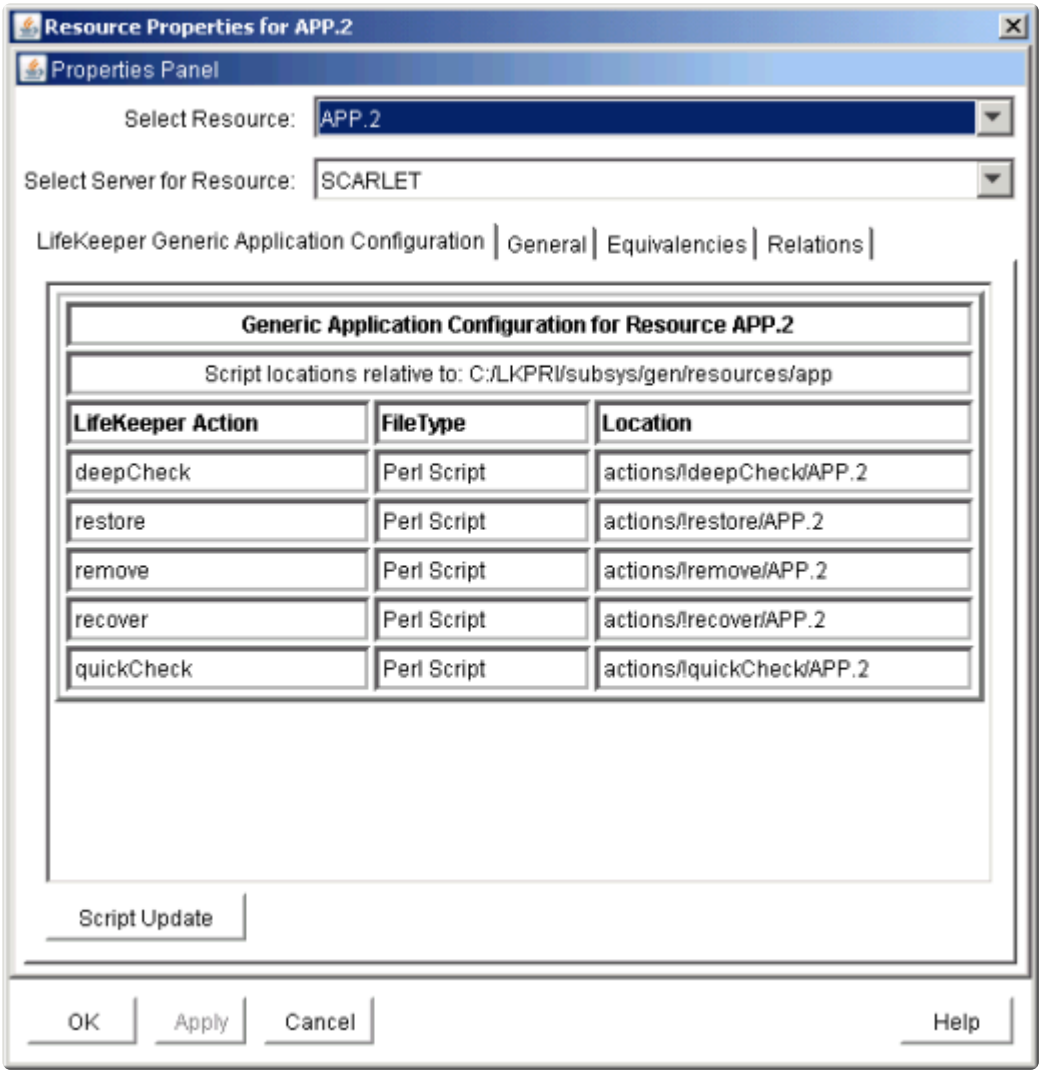
5. **サーバ A の電源をオンにします** 。サーバ A の電源をオンにし、Windows オペレーティングシステムを起動します。

6. **サーバ A でリソース階層を起動します (必要な場合)。** LifeKeeper GUI を使用して、サーバ B に切り替えたリソース階層をサーバ A で起動します。

8.4.5.9. Generic Application スクリプトの設定

この機能は、SIOS Protection Suite リカバリキットと関係のない、アプリケーションを保護するために作成されたスクリプトをアップデートします。

1. Generic Application リソースを右クリックし、**[プロパティ]** を選択します。そして、**[SIOS Protection Suite 汎用スクリプトアップデート]** タブを選択します。



2. **[スクリプトアップデート]** ボタンを選択します。Generic Application 設定手順を行うために、次の表を使用してフィールドに必要なデータを指定します。

フィールド	説明
アップデートするアクションを選択してください	アップデートされるリソースに対する SIOS Protection Suite アクションネームを、以下の中から選択します。 • **restore**:「サービス開始」スクリプトをアップデートします。 • **remove**:「サービス停止」スクリプトをアップデートします。

	• **quickCheck**: アプリケーションを監視するスクリプトをアップデートします。 • **deepCheck**: アプリケーションを詳細な部分まで監視するスクリプトをアップデートします。 • **recover**: リソースを再起動するスクリプトをアップデートします。 • **delete**: LifeKeeper の保護から削除するスクリプトをアップデートします。 • **extend**: ターゲットサーバ上の SIOS Protection Suite でアプリケーションを保護するために必要なスクリプトをアップデートします。
新しいスクリプトへのフルパス	シェルスクリプトまたはアプリケーションのオブジェクトプログラムに対するパス名を入力します。 • **restore** スクリプトは保護されたアプリケーションリソースを in-service にします (必須)。 • **recover** スクリプトは、リソースを再起動するスクリプトのアップデートを実行します (必須)。 • **quichCheck** スクリプトは、保護されたアプリケーションリソースを監視します。 • このスクリプトまたはプログラムのコピーが、サーバ上のリソース階層で SIOS Protection Suite によって保存されます。 • SIOS Protection Suite が remove、monitoring、または recover などのパス名を認証する間多少時間を要する場合があります。 • シェルスクリプトやオブジェクトプログラムを特定する必要はありません。 • スクリプトのパス名には、英字、数字、および特殊文字 - _ ! . / を使用できます。

3. **BasicFileStatistics** ダイアログは現在のスクリプトについての新旧の設定情報を表示します。**[続行]** をクリックします。

4. **[すべてのシステムを更新]** ダイアログが表示されます。該当のクラスタ内のすべてのシステムを更新する場合は、**[はい]** を選択してください。現在のシステムのみをアップデートする場合は、**[いいえ]** を選択してください。**[いいえ]** を選択した場合、バックアップサーバ上で設定するために、一致するファイルを個別にアップデートしてください。**[次へ]** をクリックします。

5. **[完了]** ボタンをクリックすると、完了します。

8.4.5.10. リソース階層の保守

リソース階層は、SIOS Protection Suite による保護を維持した状態で保守できます。保守を行う場合は、保守するリソース階層を最初に停止します。保守が完了したら、リソース階層を再び起動します。

リソース階層を保守するには、次の手順に従います。

1. **リソース階層を停止します。** LifeKeeper GUI を使用して、保守するリソース階層を完全に停止します。詳細については、リソースを停止する を参照してください。

2. **保守作業を行います。** リソース階層を保守します。

3. **リソース階層をリストアします。** LifeKeeper GUI を使用して、リソース階層を再び起動します。詳細については、リソースを起動する を参照してください。

8.4.5.11. フェイルオーバ後のリカバリ作業

SIOS Protection Suite がリソースをプライマリサーバ (サーバ A) からバックアップサーバ (サーバ B) にフェイルオーバした場合、リカバリ作業は、次の手順に従って実行してください。

1. **フェイルオーバを監視します。** サーバ B 上の SIOS Protection Suite が、サーバ A からのフェイルオーバリカバリを実行すると、ステータスメッセージが表示されます。ステータスメッセージは、次の文で終わります。

   ```
   FAILOVER RECOVERY OF MACHINE Server A

   FINISHED AT: date time year
   ```

   メッセージの出力内容はクラスタ構成によって異なります。マウントまたはマウント解除の失敗が通知されても、リカバリが失敗したわけではありません。サーバ B でリソースを起動したエラーは、ステータスメッセージと一緒にログに記録されます。

2. **保守作業を行います。** サーバ A で障害が発生した原因を調べて解決してください。保守作業はサーバ A の電源をオフにして行ってください。

3. **サーバ A を再起動します (必要な場合)。** 保守が完了したら、必要に応じて、サーバ A を再起動します。

4. **LifeKeeper を起動します (必要な場合)。** LifeKeeper がサーバ A で稼働していない場合は、**Windows のサービスアプリケーション** を起動し、**[LifeKeeper]** を選択し、**[開始]** を選択します。**[LifeKeeper External Interfaces]** サービスが自動的に起動します。

5. **アプリケーションをサーバ A に戻します。** 必要に応じて、LifeKeeper GUI を使用し、リソース階層をサーバ A で起動します。詳細については、リソースを起動する を参照してください。サーバ A のスイッチバック方法が [Automatic] に設定されている場合、この操作は不要です。

8.4.5.12. SIOS Protection Suite for Windows のアンインストール

LifeKeeper を削除する前に

LifeKeeper ソフトウェアを削除するにあたって以下の事項が必要となります。

1. **アプリケーションの移動もしくは停止。ソフトウェアを削除する前に、SIOS Protection Suite の保護が必要なアプリケーションがサーバ上にないことを確認してください。** アプリケーションリソースが In Service 中のアプリケーションが存在するサーバ上から LifeKeeper を削除しないでください。LifeKeeper を削除すると、イクイバレンシ、リソース階層の定義およびログファイルのような設定データがすべて削除されます。追加情報については リソース階層の移動 を参照してください。

2. **LifeKeeper が実行中である。** LifeKeeper Recovery Kit ソフトウェアを削除する場合、LifeKeeper が動作している必要があります。**サービス MMC** スナップインを使用して LifeKeeper サービスが実行中であることを確認します。LifeKeeper が実行中でない場合、クラスタ内の別の SIOS Protection Suite サーバからリソースインスタンスを削除できず、サーバに一貫性がない状態になります。

3. **リソース階層の削除。** LifeKeeper を削除するサーバからリソース階層を拡張もしくは削除してください。リソース階層がサービス中のサーバからは、絶対に Recovery Kit を削除しないでください。現在のリソース階層が壊され、Recovery Kit の再インストール時に再作成しなければならなくなります。

4. **全パッケージの削除。** LifeKeeper core を削除する場合は、最初に LifeKeeper に依存する別のパッケージを削除してください。例: SIOS Protection Suite リカバリキット。SIOS Protection Suite リカバリキットを削除する前に、関連するアプリケーションリソース階層を削除することを推奨します。

DataKeeper を削除する前に

DataKeeper のアンインストールおよび前バージョンの再インストールを実施する際は、アンインストール前に各ノードですべてのジョブ/ミラーを削除する必要があります。ソフトウェアを再インストールした時点でジョブ/ミラーを再作成する必要があります。

SIOS Protection Suite のアンインストール

- **Windows のコントロールパネル** で、インストールされたプログラムのリストから、**SIOS DataKeeper** もしくは **LifeKeeper** を選択してください。

- **アンインストール** を選択してください。

アンインストール処理が完了した時点で、再起動が必要となります。

注記: アンインストール時には自動的に SIOS DataKeeper および/または LifeKeeper サービスが停止され、レジストリエントリがクリアされます。

削除が完了しても以下のファイル群はアンインストール時に削除されません。

パスおよびファイル名	定義および特別な考慮事項
<windows dir>/SysWOW64)/LKLicense	SIOS Technology Corp. 製品の共通のライセンスファイルディレクトリです。ライセンスファイルがインストールされる場所で、複数の SIOS Technology Corp. 製品のライセンスが毎回このパスにインストールされます。インストール済みのライセンスを残しておくため、アンインストール時にこのパスは削除されません。 手動で削除することが安全ですが、そのソフトウェアを後で再インストールすることになった場合、ライセンスも同じく再インストールする必要があります。
<windows dir>/SysWOW64)/PerfStringBackup.ini	新しいパフォーマンスモニタカウンタがインストールされる時 Windows により作成されるバックアップファイルです。perfmon カウンタをインストールする際に作成されます。 このファイルは、Windows 自身により作成されるファイルなので、単体で残ります。
<windows dir>/inf/ExtMirr/0011/ExtMirrCounters.ini	このファイルは、DataKeeper パフォーマンスモニタカウンタ を記述しています。このファイルは削除またはそのまま残しておくことも可能です。これは実行ファイルではありません。

注記

- **重要**: SIOS Protection Suite ソフトウェアのアンインストールには Microsoft Visual C++ 2008 Redistributable package のインストールが必要となります。このパッケージは SIOS Protection Suite がアンインストールされるまで削除しないでください。
- SIOS Protection Suite セットアッププログラムから **[Modify]** または **[Repair]** を実行してください。
- LifeKeeper の削除では SUperior SU は削除されません。SUperior SU は **Add/Remove Programs** で個別に削除することが可能です。
- SIOS Protection Suite の削除では SIOS Protection Suite ディレクトリは削除されません。そのディレクトリは **Add/Remove Programs** 処理が完了した後、手動で削除することが可能です。
- SIOS Protection Suite を完全に削除するためにはシステムの再起動が必要となります。

8.4.5.13. 保護対象のボリュームで CHKDSK を実行する

LifeKeeper の保護下にあるディスクボリュームでは、自動ブート時間 CHKDSK が実行されません。管理者はボリュームに対し手動で CHKDSK を実行する必要があります。これは次の手順で実施してください。

1. ボリュームに依存しているすべてのリソースを停止します。CHKDSK の間ボリュームはロックされてアクセス不能になるため、ボリュームを使用しているアプリケーションはすべてサービス停止状態にする必要があります。

2. ボリュームリソースを起動したままにします。CHKDSK はボリュームを開くことができる必要があるため、リソースを起動した状態でアンロックします。

3. ボリュームが DataKeeper ミラーボリュームの場合は、ミラーを一時停止状態にすることを推奨します。

4. ボリュームをチェックするノードのコマンドラインから次のコマンドを実行して、ボリュームリソースをメンテナンスモードにします。

- `cd LKBIN`
- `flg_create -f Maintenance_<drvletter>`
    - `<drvletter>` はボリュームのドライブレターです。ボリューム F: をメンテナンスモードにするには、次のコマンドを実行します。
      `flg_create -f Maintenance_F`

  ボリュームがメンテナンスモードの間、ボリュームチェックスクリプトはヘルスチェックを実行しません。

5. ボリュームを確認し、エラーを修正します（例: "`chkdsk.exe /f F:`" を実行する、等）。

CHKDSKが完了したら、

1. chkdsk が完了したノードのコマンドラインから次のコマンドを実行して、ボリュームリソースのメンテナンスモードを解除します。

- `cd LKBIN`
- `flg_remove -f Maintenance_<drvletter>`
    - `<drvletter>` はボリュームのドライブレターです。ボリューム F: メンテナンスモードを解除するには、次のコマンドを実行します。
      `flg_remove -f Maintenance_F`

2. chkdsk の実行を容易にするために一時停止していたミラーを続行します。これにより、ファイルシステムの変更をターゲットノードと再同期させることができます。

3. リソース階層をサービス開始にします。これらはミラーがまだ再同期している間にオンラインにすることができます。

8.4.6. データレプリケーション

このセクションでは、SIOS Protection Suite とともにデータレプリケーションを使用する方法について説明します。

複製ボリュームリソースの監視

レプリケーションの設定

複製ボリュームの操作

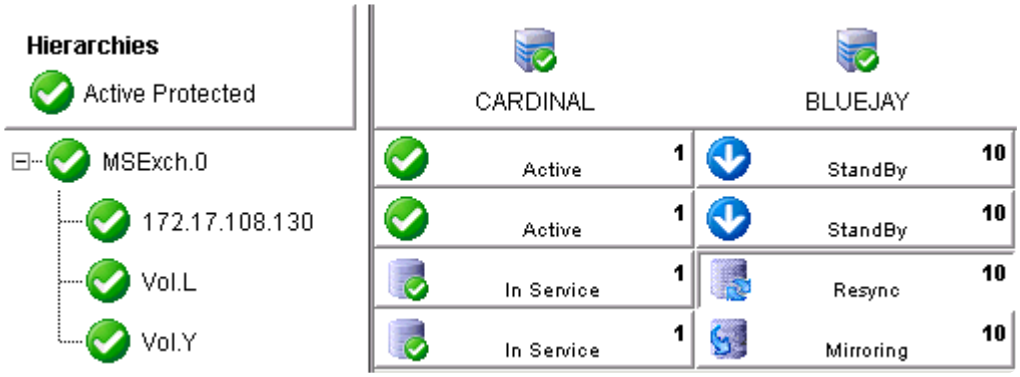
スプリットブレインとは

スプリットブレインリカバリ

8.4.6.1. 複製ボリュームリソースの監視

SIOS Protection Suite で保護する複製ボリュームリソースの状態は、LifeKeeper GUI に表示されます。ミラー状態の詳細については、SIOS DataKeeper のトピック ミラー状態の定義 を参照してください。

次図の例では、複製ボリュームリソースのミラー状態は、Vol.L が **再同期** 、Vol.Y が **ミラーリング** になっています。

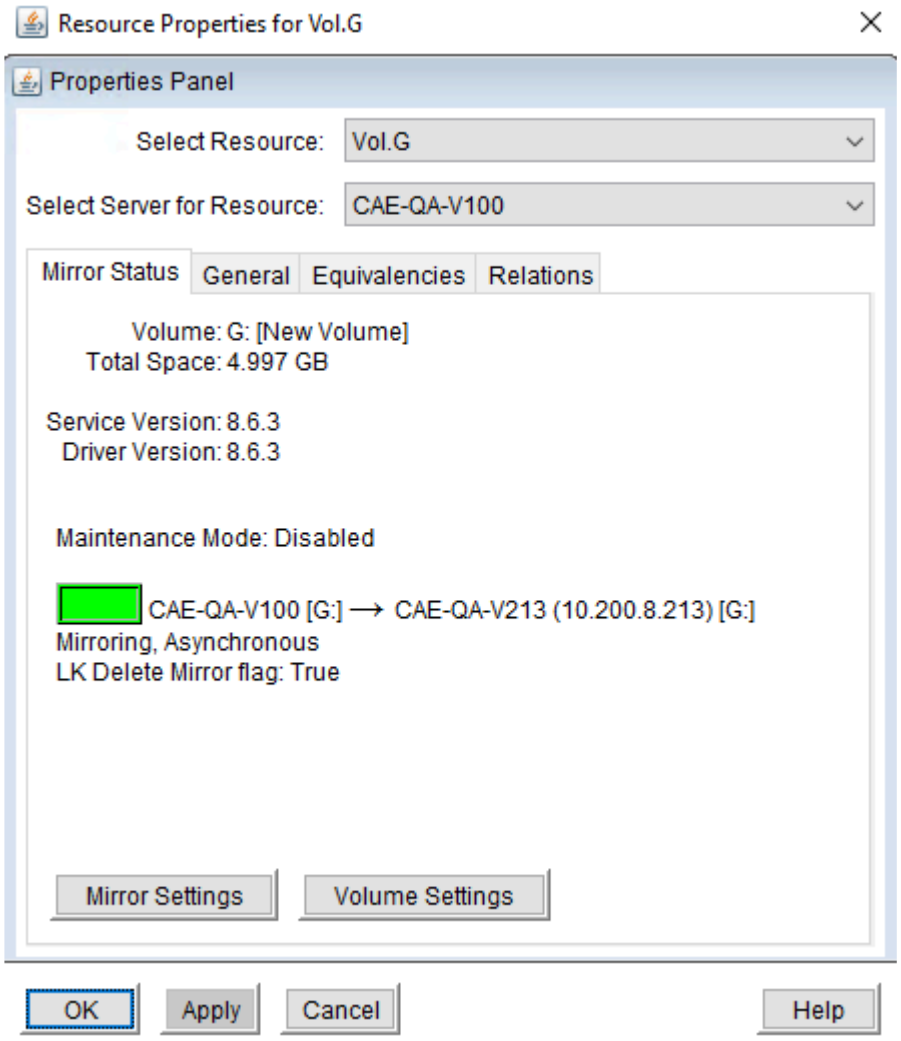


複製ボリュームリソースの状態と意味を次表に示します。

リソースの状態	アイコン	表示状態
アクティブ		プライマリサーバで稼働しており、保護されています (ISP)。
縮退		プライマリサーバで稼働していますが、バックアップサーバでは保護されていません (ISU)。
不明		リソースが初期化されていないか (ILLSTATE)、SIOS Protection Suite が稼働していません。
障害		障害が発生しています。リソースの稼働に失敗した場合。(OSF)
オフライン		リソースが稼働していません。ボリュームの読み書き操作はできません。
再同期 (ペンディング)		バックアップサーバ上のリソースステータスは、*再同期 (ペンディング)* です。
ミラーリング		バックアップサーバ上のリソースステータスは、**ミラーリング** です。
一時停止		バックアップサーバ上のリソースステータスは、**一時停止** です。
再同期		バックアップサーバ上のリソースステータスは、**再同期** です。
中断		バックアップサーバ上のリソースステータスは、**中断** です。

複製ボリュームリソースの設定状態を LifeKeeper GUI に表示するには、ボリュームリソースを右クリックし、**[プロパ**

ティ] をクリックし、**[SDR ステータス]** タブをクリックしてください。次図の例では、Vol.G が CAE-QA-V100 上のソースで、ターゲットサーバ (10.200.8.213) が 1 台あり、ターゲットサーバ CAE-QA-V213 に対して再同期が実行されています。



8.4.6.2. レプリケーションの設定

[ボリュームリソースのプロパティ] ページを開き、**[レプリケーション設定]** をクリックすると、複製ボリュームの圧縮レベル、ネットワーク帯域制限、SIOS Protection Suite 削除ミラーフラグを設定できます。

フィールド	説明
ターゲットの選択	操作を実行するターゲットサーバを選択します。
圧縮レベルの設定	レプリケーションボリュームの圧縮レベルを指定します。 有効値は 0 ～ 9 です。レベル 0 は「圧縮なし」です。1 から 9 の値で圧縮の CPU の集中レベルを増分的に指定します。圧縮レベル 1 は高速圧縮です。データを圧縮する CPU 時間は最短ですが、パケットサイズが最大になります。レベル 9 は圧縮時間が最長ですが、圧縮率は最大になります。つまり、CPU 時間は長くなりますが、パケットサイズは最小になります。ご使用のシステム、ネットワーク、作業負荷を考えて、CPU 使用率とネットワーク転送速度のバランスを取れるように、1 ～ 9 までの値を選択してください。 デフォルト: 0
ネットワーク帯域制限の設定	ネットワーク帯域設定では、レプリケーションボリュームの再同期と通常のボリューム書き込みに使用するネットワーク帯域を KB 単位で指定します。 デフォルト: 0
SIOS Protection Suite デリートミラーフラグの設定	SIOS Protection Suite デリートミラーフラグは、レプリケーションボリュームの SIOS Protection Suite リソースを削除する動作を制御します。このフラグを **[True]** に設定した場合、SIOS Protection Suite ボリュームリソースを削除すると、ミラーが削除されます。[True] を指定しないと、ミラーは削除されません。 ボリュームリソースの拡張を解除するか、SIOS Protection Suite から削除する場合は、**[True]** を選択します。 ミラーを削除しない場合は、**[False]** を選択します。 LifeKeeper GUI でミラーを作成している場合は、**[True]** が既定値となります。LifeKeeper GUI を使用せずにミラーを作成している場合、既定値は **[False]** になります。

8.4.6.3. 複製ボリュームの操作

LifeKeeper GUI を使用して、複製ボリュームリソースを操作するには、複製ボリュームリソースを右クリックし、実行する操作をコンテキストメニューから選択してください。[表示] メニューから [プロパティパネル] をクリックして、**[プロパティパネル]** を有効にした場合、ボリュームを選択すると、リソースツールバーが表示されます。

操作	アイコン	説明
ターゲットの選択		操作を実行するターゲットシステムを選択します。
ミラー一時停止		**[ミラー一時停止]** をクリックすると、データのミラー化が一時停止します。**[続行]** をクリックしてミラーリングを再開すると、部分再同期が実行されます。ミラーリングを一時停止した後、**[ターゲットのロック解除]** をクリックすると、ターゲットボリュームのロックを解除できます。
ミラー再開/ターゲットロック		ミラーリングを一時停止した後に再開するには、**[続行/ターゲットのロック]** をクリックします。このボタンをクリックすると、一時停止が解除されます。ターゲットボリュームがロックされている場合、ロックが解除してミラーリングが再開されます。 ミラーリングを一時停止した場合は、その間の書き込みデータが記録されます。ミラーリングを再開すると、記録されたデータがターゲットボリュームに送信され、部分再同期が自動的に実行されます。
ターゲットのロック解除		ミラーのターゲットボリュームのロックを解除するには、**[ターゲットのロック解除]** をクリックします。このボタンをクリックした場合、ミラーリングが一時停止して、ターゲットシステム上のミラーボリュームのロックが解除されます。その結果、ボリューム上のデータを読み書きできるようになります。 **[ミラー続行]** をクリックすると、ターゲットボリュームが再びロックされます。部分再同期の実行後にミラーリングが再開されます。 **警告**: ロック解除中のターゲットボリュームへのどの書き込みも、ミラーの再同期時に失われます。
ミラー中断/ターゲットロック解除		ミラーリングを中断すると、選択したボリュームのミラーリングが中断され、ターゲットボリュームのロックが解除されます。ただし、ミラーはボリュームリストから削除されません。**[ミラー中断/ターゲットロック解除]** を選択した場合は、その後で完全な再同期を実行して、ミラーリングを再確立する必要があります。 **警告**: ロック解除中のターゲットボリュームへのどの書き込みも、ミラーの再同期時に失われます。

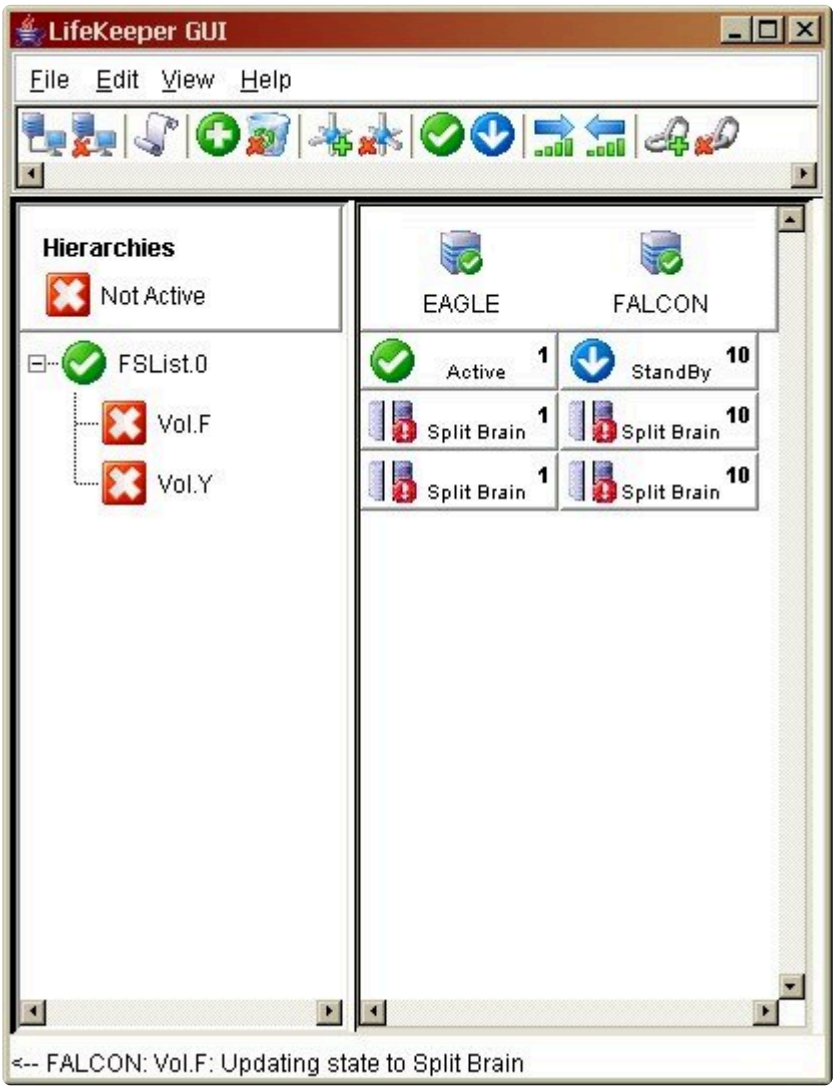
ミラー再同期/ターゲットロック		中断したミラーリングを再確立するには、**[ミラー再同期/ターゲットロック]** をクリックします。完全な再同期が実行されます。

8.4.6.4. スプリットブレインとは

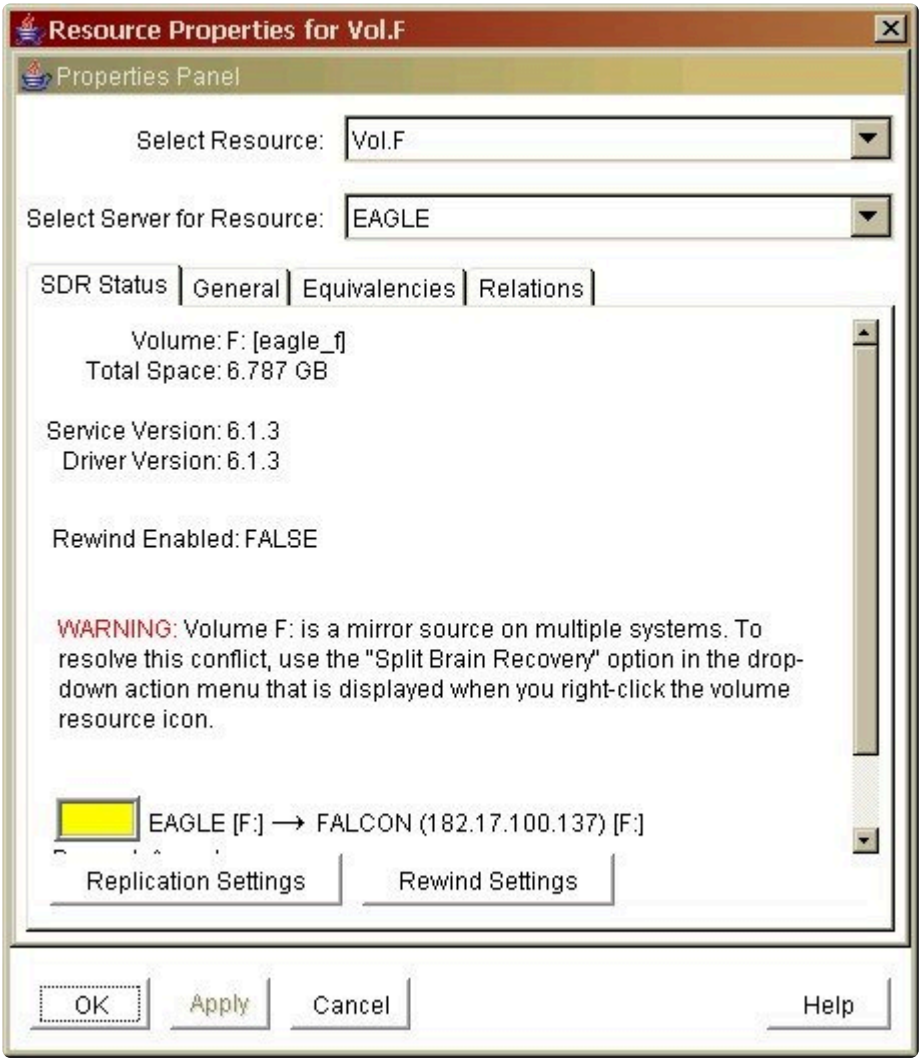
SIOS Protection Suite のすべてのコミュニケーションパスが切断された場合、**自動ノードフェイルオーバ** が有効になっていると、SIOS Protection Suite のそれぞれの側がもう一方を停止したものと見なし、すべてのリソースを起動しようとします。SIOS DataKeeper リソースの場合、両側がミラーソースになり、ボリュームにデータを書き込めるようになります。この状態は「スプリットブレイン状態」と定義され、LifeKeeper GUI では以下のアイコンが表示されます。



この状態を解決するために必要な手順については、スプリットブレインリカバリ を参照してください。



選択したボリュームの **プロパティパネル** に、スプリットブレイン状態に関する追加情報と、この問題を解決するための手順が表示されます。


Resource Properties for Vol.F
Properties Panel
Select Resource:
Vol.F
Select Server for Resource:
EAGLE
SDR Status
General
Equivalencies
Relations
Volume: F: [eagle_f]
Total Space: 6.787 GB
Service Version: 6.1.3
Driver Version: 6.1.3
Rewind Enabled: FALSE
WARNING: Volume F: is a mirror source on multiple systems. To resolve this conflict, use the "Split Brain Recovery" option in the drop-down action menu that is displayed when you right-click the volume resource icon.
EAGLE [F:] → FALCON (182.17.100.137) [F:]
Replication Settings
Rewind Settings
OK
Apply
Cancel
Help

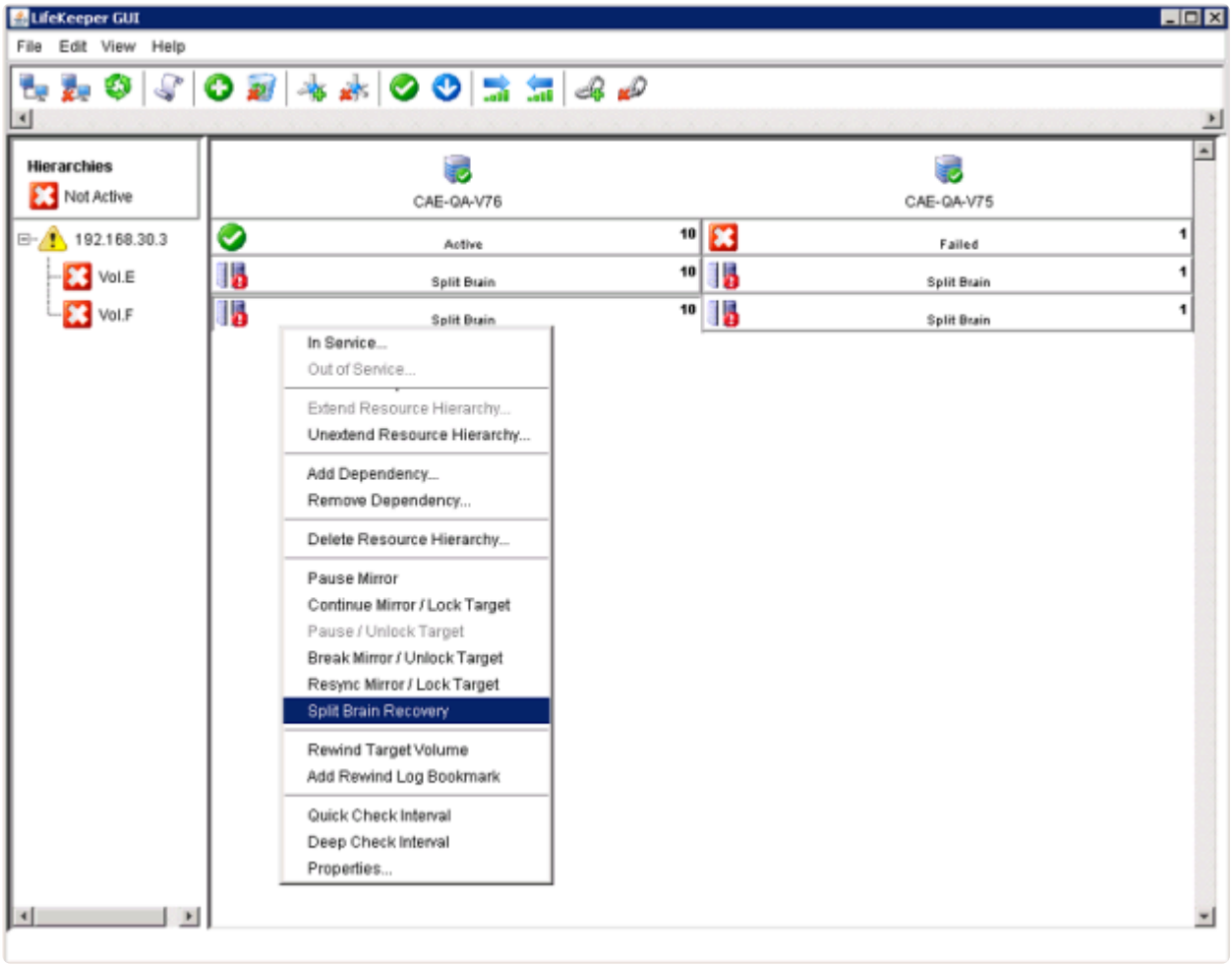
8.4.6.5. スプリットブレインリカバリ

システムのコミュニケーションパスが復旧した後にボリュームがスプリットブレイン状態にあることが検出された場合、以下の **スプリットブレインリカバリ** 手順を実行する必要があります。

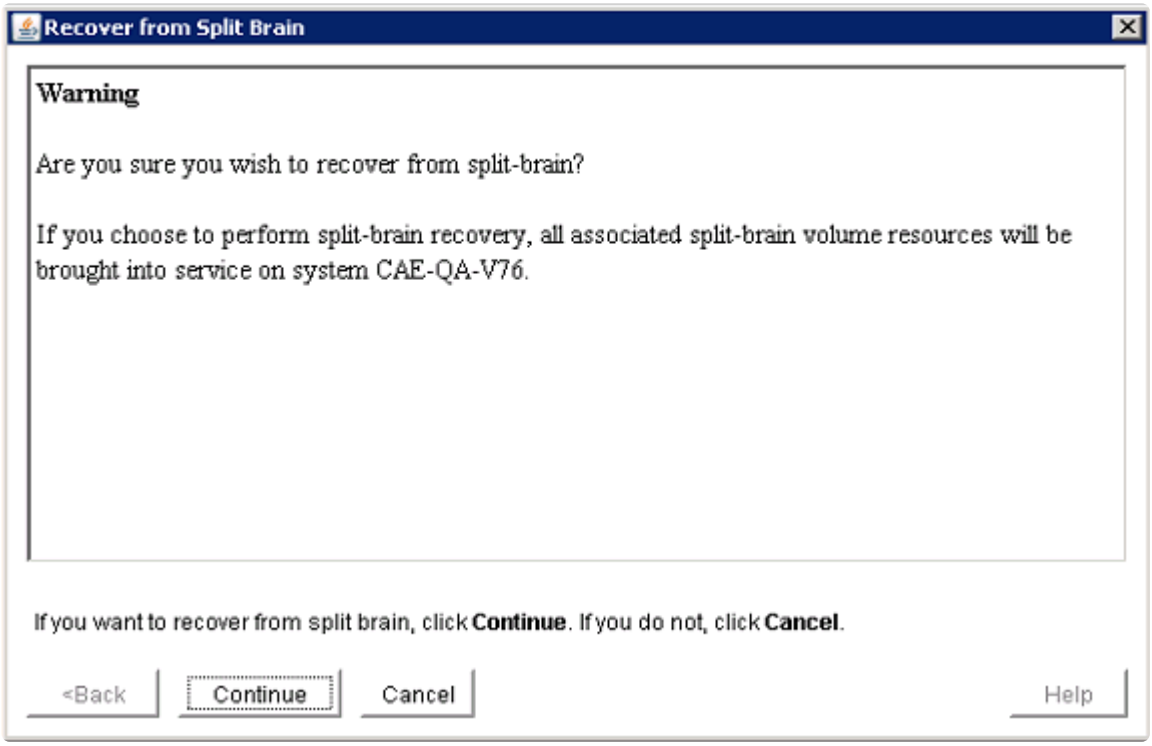
注記: 複数のボリュームが異なるリソース階層で検出された場合は、それぞれのボリュームでスプリットブレインリカバリ手順を実行する必要があります。スプリットブレイン状態のボリュームが同じ階層にある場合は、リカバリが同時に実行されます。

1. ソースにするシステムの下のボリュームインスタンスアイコンを右クリックします。**リソースコンテキスト** メニューが表示されます。一番左のパネルの **リソース階層** リストのボリュームインスタンスアイコンを右クリックすることもできます。メニューから **[スプリットブレインリカバリ]** を選択すると、ミラーソースとするサーバを選択するよう求められます。

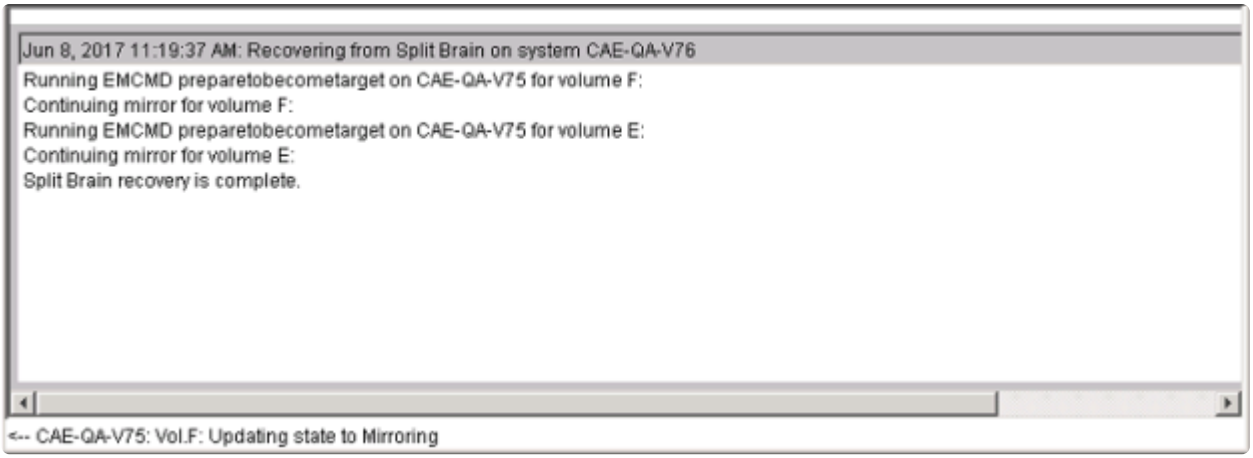
2. メニューから **[スプリットブレインリカバリ]** を選択します。



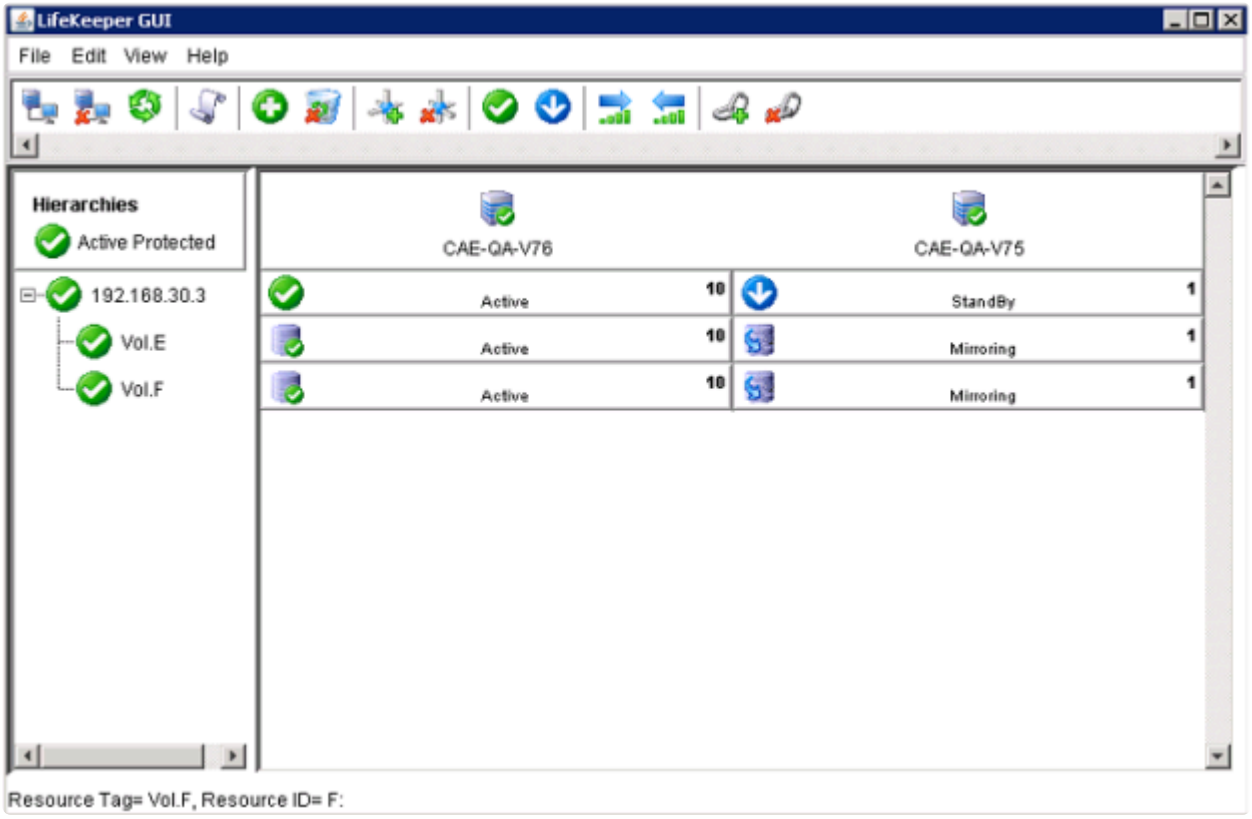
3. 以下の警告メッセージが表示されます。**[続行]** ボタンをクリックすると、スプリットブレインリカバリプロセスが完了します。



4. **[完了]** をクリックします。



5. リカバリが完了すると、復旧したリソースは GUI に以下のように表示されます。ミラーが再同期すると、スプリットブレインリカバリプロセスは完了します。


LifeKeeper GUI
File Edit View Help
Hierarchies
Active Protected
192.168.30.3
Vol.E
Vol.F
CAE-QA-V76
CAE-QA-V75
Active 10
StandBy 1
Active 10
Mirroring 1
Active 10
Mirroring 1
Resource Tag= Vol.F, Resource ID= F:

8.5. DataKeeper

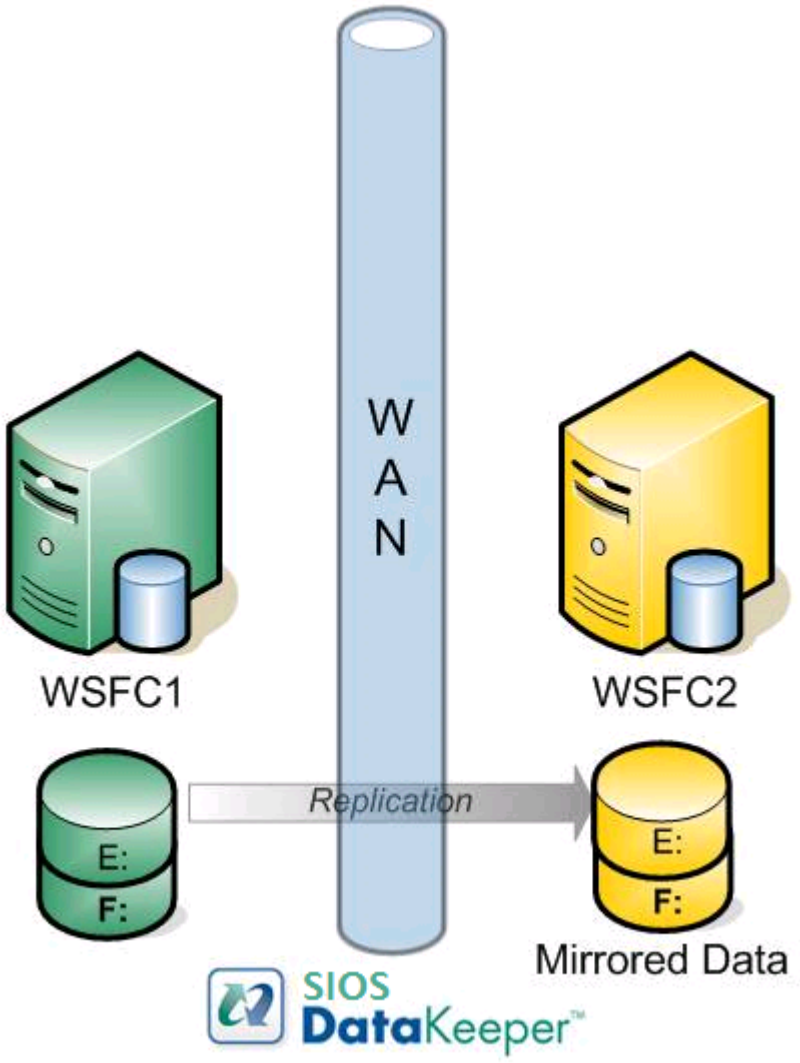
SIOS DataKeeper Cluster Edition の情報リソース

SIOS Technology Corp. は、SIOS DataKeeper Cluster Edition のサポートされているすべてのバージョンのドキュメントを維持・管理しています。
私たちは、お客様からの提案やフィードバックを継続的なドキュメントの改善に役立てたいと考えています。ぜひ簡単なドキュメントフィードバック調査にご協力ください。

8.5.1. はじめに

SIOS DataKeeper の概要

SIOS DataKeeper は、最適化されたホストベースのレプリケーションソリューションとして、ソースサーバから 1 台以上のターゲットサーバにネットワーク経由で可能な限り高速かつ効率的にデータを複製します。



機能

機能のいくつかを以下に示します。

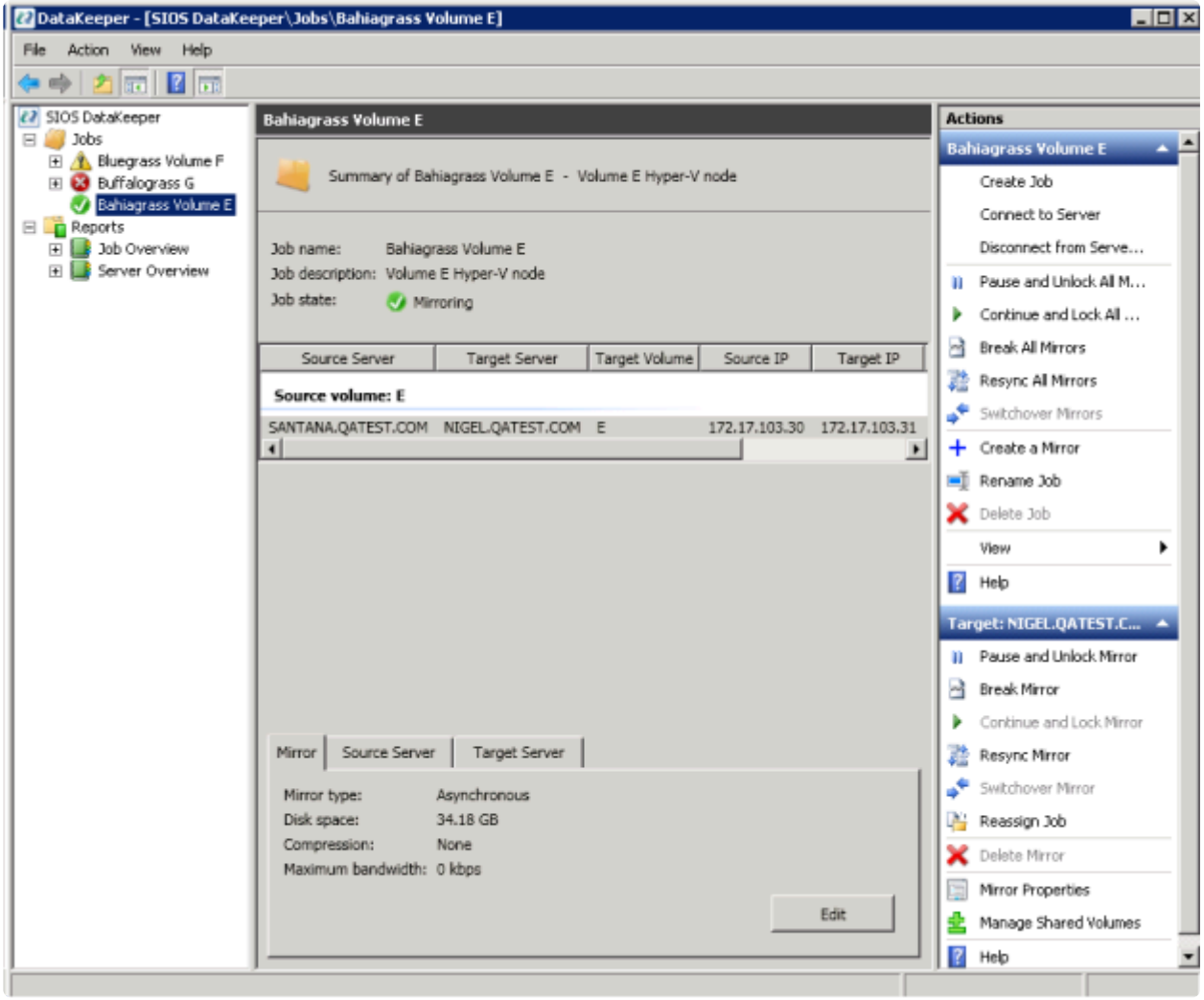
- ブロックレベルでの同期または非同期のボリュームレプリケーション。
- 組み込みの WAN 最適化機能により、WAN アクセラレータを使用せずに、高速ネットワークと待機時間の長いネットワークの接続をフルに活用できます。
- 圧縮アルゴリズムで帯域を有効活用することができます。

- 直感的な MMC 3.0 の GUI を使用することができます。

8.5.1.1. ユーザインターフェース

SIOS DataKeeper ユーザインターフェース

SIOS DataKeeper のユーザインターフェースは標準の MMC スナップインを使用しています。



- 左側のペインには、コンソールツリーが表示されます。ここには **[ジョブ]** および **[レポート]** が表示されます。現在、2 つのレポート (**[ジョブ概要]** および **[サーバ概要]**) が使用できます。*ジョブ概要*レポートは、接続しているサーバ上のすべてのジョブの概要を示しています。**サーバ概要** レポートは、接続しているサーバ上のすべてのミラーの概要を示しています。

- 中間のペインは **[概要]** ビューです。ここには、選択した項目についての情報が表示されます。

- 右側の列は **[操作]** ビューです。このペインは **[表示]** メニューから起動した場合に表示されます。このペインから使用可能なオプションは **[操作]** メニューからも同じく使用可能です。このペインは 2 つのセクションに分かれています。上部セクションの **[操作]** は、ジョブおよびジョブ内の各ミラーに適用されます。下部セクションの **[操作]** は、選択したミラーにのみ適用されます。

- メインウィンドウの下部に 3 つのタブが表示されます。、**[ソースサーバ]** 、および **[ターゲットサーバ]** です。これらのタブには、選択されたミラーの情報が表示されます。

- アイコンがミラーの状態を示します。Failover Cluster UI のアイコンや状態よりも多くの情報が得られます。

8.5.1.2. DataKeeper コンポーネント

SIOS DataKeeper for Windows は以下のコンポーネントから構成されています。

- **DataKeeper ドライバ (ExtMirr.sys)** - DataKeeper ドライバはカーネルモードドライバであり、ミラーエンドポイント間のすべてのミラー処理を行います。

- **DataKeeper サービス (ExtMirrSvc.exe)** - DataKeeper サービスは、DataKeeper GUI とコマンドラインインターフェースを DataKeeper ドライバとリンクします。ミラーを操作するコマンドはすべて、DataKeeper サービスを通して DataKeeper ドライバに中継されます。

> **重要:** DataKeeper サービスを停止してもミラーリングは停止しません。ミラーリングを中断するには、ミラーの一時停止、中断、または削除のコマンドをドライバに送信するしかありません。

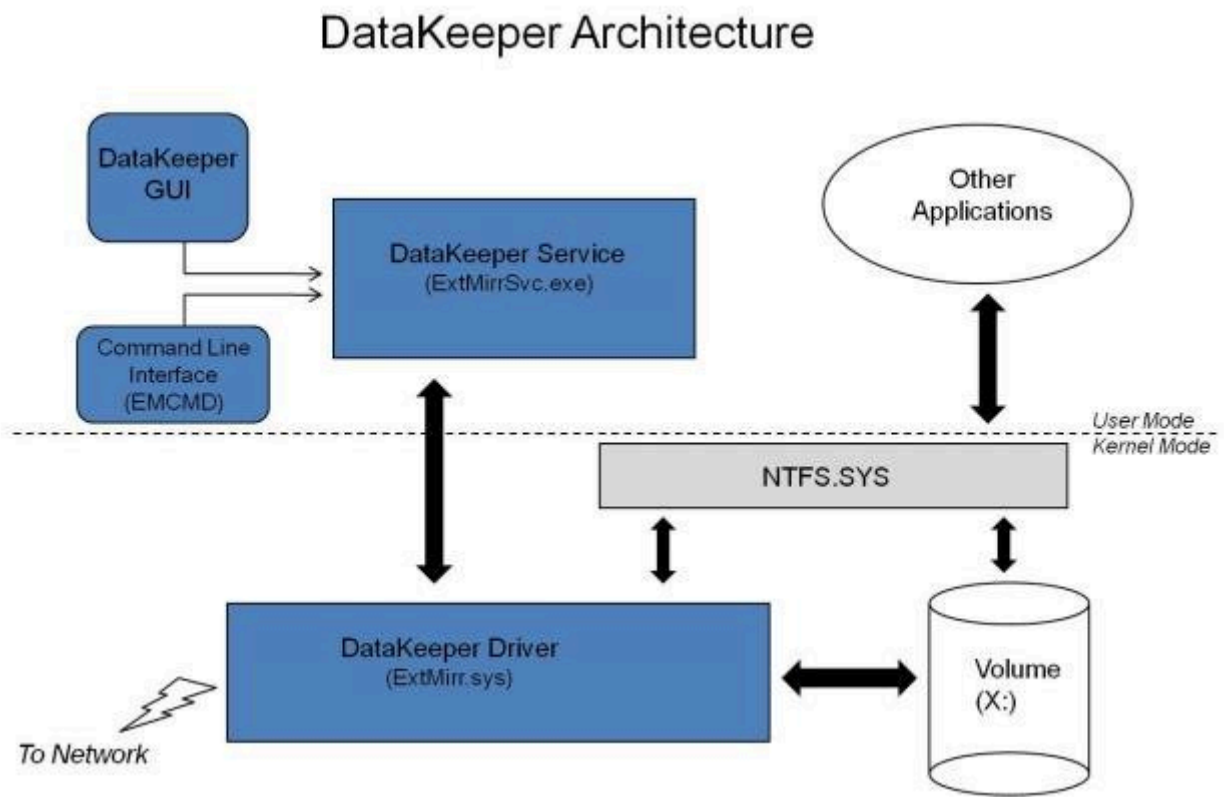
- **DataKeeper サービスログオン ID とパスワードの選択 -** DataKeeper サービスログオン ID とパスワードを選択すると、サービスの起動に使用するアカウントの種類を選択できます。管理者権限を持つドメインアカウント ID またはサーバアカウント ID を使用すると、ネットワーク障害が発生した場合の障害回復を強化することができます。

- **コマンドラインインターフェース (EMCMD.exe)** - DataKeeper の操作に使用できる EMCMD コマンドオプションが揃っています。

- **DataKeeper GUI (Datakeeper.msc)** - DataKeeper GUIは MMC 3.0 (Microsoft 管理コンソール) ベースのユーザインターフェースであり、ミラー処理をコントロールしたり、ミラーの状態を取得したりすることができます。

- **パッケージファイル、SIOS Protection Suite のスクリプト、ヘルプファイルなど**

次の図は、DataKeeper コンポーネントが NTFS ファイルシステムや各コンポーネント間のインターフェースとなり、データレプリケーションを実行する仕組みを示したものです。


DataKeeper Architecture
DataKeeper GUI
Command Line Interface (EMCMD)
DataKeeper Service (ExtMirrSvc.exe)
Other Applications
User Mode
Kernel Mode
NTFS.SYS
DataKeeper Driver (ExtMirr.sys)
Volume (X:)
To Network

8.5.1.2.1. DataKeeper サービスログオン ID とパスワードの選択

新規の DataKeeper インストール設定時に、ユーザは DataKeeper サービスログオン ID とパスワードの入力を求められます。

DataKeeper サービスは、認証された接続を使用してボリュームのスイッチオーバを実行し、複数のサーバ間でミラーロールを変更します。DataKeeper サービスを実行するために選択されたログオン ID アカウントに応じて、サーバ間の接続を確立してボリュームスイッチオーバを実行するために使用できる権限が決まります (特に、サーバまたはネットワークの障害が発生した場合)。

以下のように、数種類のサービスログオン ID アカウントを使用できます。

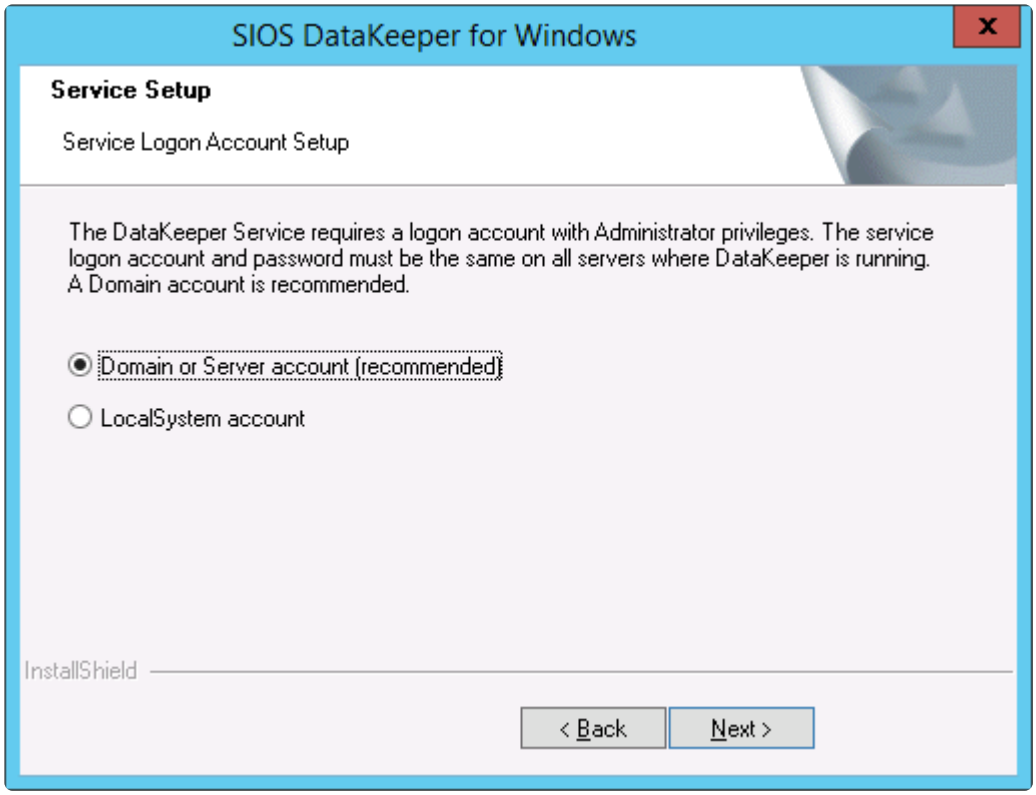
- ドメイン内の接続されたすべてのサーバで有効な、管理者権限を持つ **ドメインアカウント** (*推奨*)
- 接続されたすべてのサーバで有効な、管理者権限を持つ **サーバアカウント**
- **ローカルシステムアカウント** (*推奨しない*)

  注記: ワークグループの場合は、各システム上で DataKeeper の サービスアカウントとして*サーバアカウント*オプションおよびサーバ名 /
  管理者を使用してください。**すべてのサーバに同一の ログオン ID および パスワードを使用する必要があります** (関連する既知の問題 を参照)。

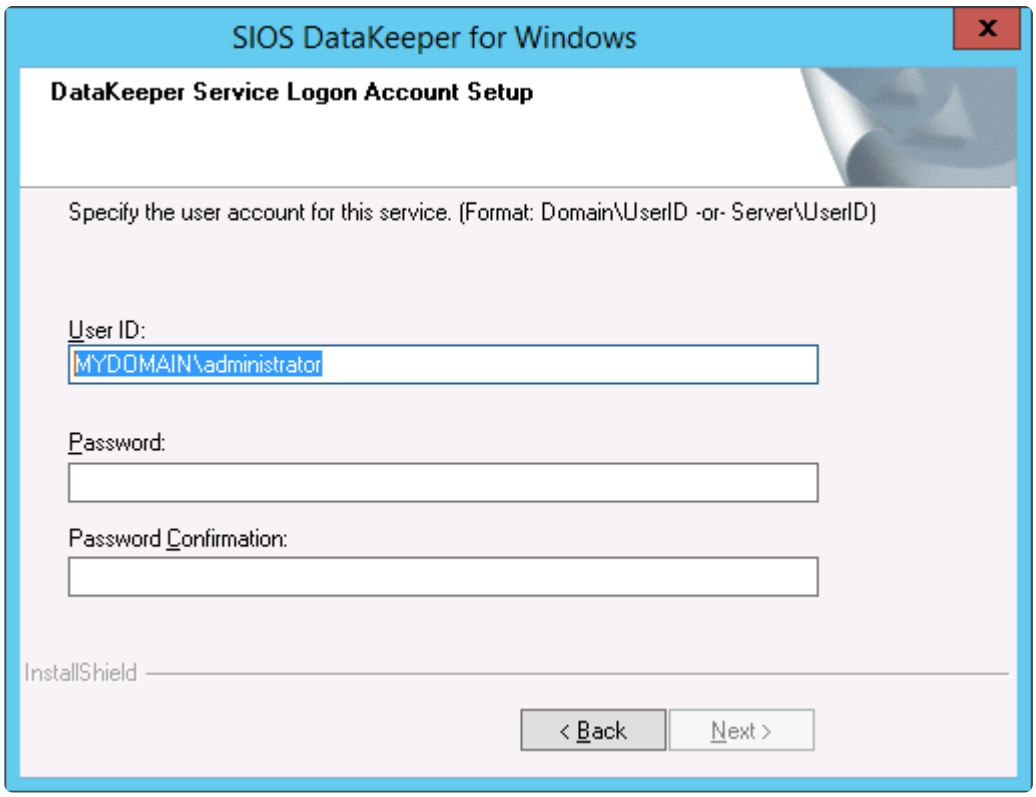
注記: 使用するドメインアカウントまたはサーバアカウントは、ローカルシステム管理者グループに追加する必要があります。アカウントには、DataKeeper がインストールされているサーバの管理者権限が備わっている必要があります。

Active Directory によるネットワーク接続が失われた場合、ローカルシステムアカウントはドメイン内で正常に認証できないことに注意してください。その場合、ローカルシステムアカウントではサーバ間の接続を確立できず、ネットワーク経由の DataKeeper ボリュームのスイッチオーバコマンドは拒否されます。ネットワーク障害などの障害回復時にフォールトトレランスを要求される IT 部門では、ローカルシステムアカウントを使用しないでください。

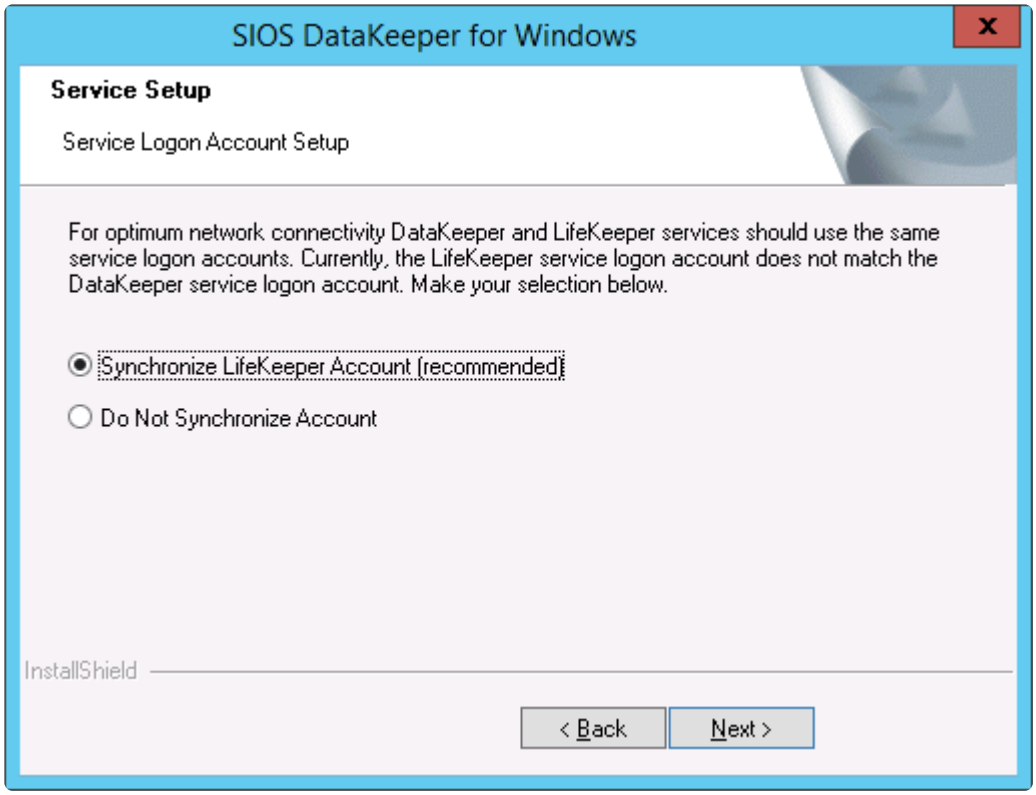
DataKeeper のインストール – サービスログオン ID タイプの選択



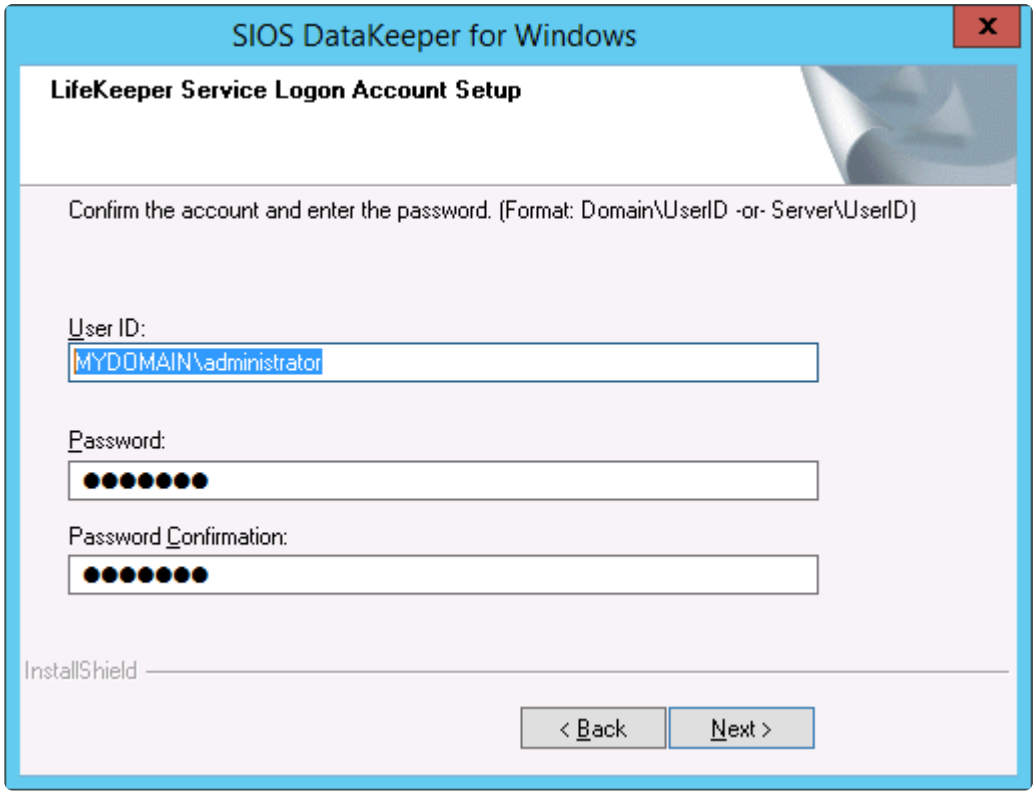
上の画面でドメインアカウントまたはサーバアカウントを選択した場合は、DataKeeper サービスログオン ID とパスワードの入力フォームが表示され、情報を入力できます。



より信頼性の高いスイッチオーバーとフェールオーバーのための、LifeKeeperとDataKeeperのサービスアカウント同期機能の提供をします。

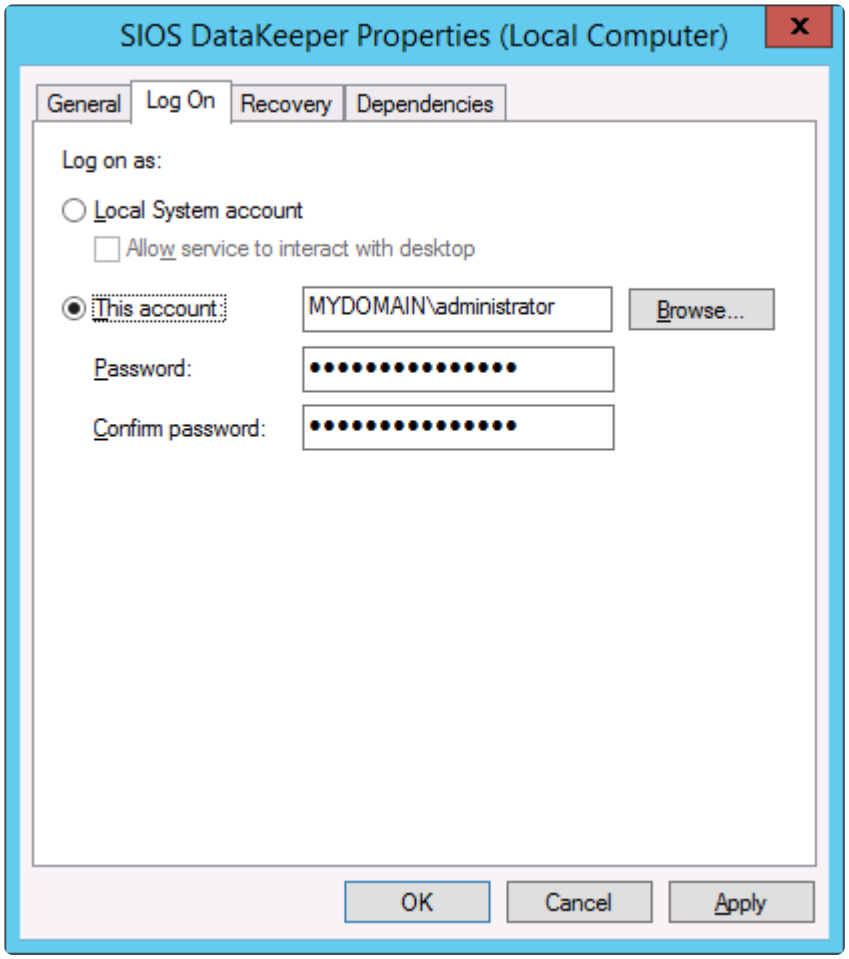


LifeKeeper Serviceのログオン



すでにサービスログオン ID とパスワードを使用して DataKeeper サービスを設定している場合、サービス ID とパスワードの選択ダイアログは表示されません。ただし、管理者は、Windows サービスアプレットを使用して、DataKeeper サービスログオン ID とパスワードをいつでも変更できます。ログオン ID やパスワードを変更した後

は、必ず DataKeeper サービスを再起動してください。



次の表はそれらの要件について概説しています。

環境	DataKeeper サービスの要件	DataKeeper UI の要件
同じドメイン または 信頼されたドメイン環境	• 同じアカウントを持つすべてのシステムで、同じ認証情報を使用して DK サービスを起動してください。 • default = Local System Account を使用することが許可されています。	• ドメイン管理者でログインし、DK GUI を起動してください。 • 「run as」管理オプションを使用して DK GUI を起動してください。
ドメインサーバとワークグループサーバが混在した環境 または 個々のドメインサー	• 各システムで同じアカウント名およびパスワードにてローカルアカウントを作成してください。 • このローカルアカウントを Administrator グループに追加してください。 • すべてのシステムで、ローカルアカウントを使用して DK サービスを起動してください。	• DK サービスを起動するために作成したローカルアカウントを使用してログインしてください。 • DK GUI を起動してください。 **すべてのサーバに同一の ログオン ID および パスワードを使用する必要があります** (関連する 既知の問題 を参照)。

バ		

8.5.1.3. レプリケーションについて

SIOS DataKeeper の動作について

DataKeeper は、あるシステム (ソース) 上のボリュームを別のシステム (ターゲット) 上の別のボリュームにネットワーク経由でミラーリングする機能を提供します。ミラーを作成すると、最初にソースボリューム上のすべてのデータがターゲットボリュームに複製され、上書きされます。このボリュームの初期同期 (データの完全再同期とも呼ばれる) が完了すると、ターゲットボリュームはサイズとデータの中身に関してソースボリュームの厳密な複製となります。ミラーが確立されると、ソースボリュームに対するすべての書き込みが DataKeeper によって割り込まれ、そのデータがネットワーク経由でターゲットボリュームに複製されます。

レプリケーションは、以下のどちらかの方法によってブロックレベルで実行されます。

- 同期レプリケーション
- 非同期レプリケーション

通常、WANでは非同期ミラーリング、LANでは同期ミラーリングを推奨します。

8.5.1.3.1. SIOS DataKeeper インテントログ

SIOS DataKeeper は、インテントログ (ビットマップファイルとも呼ばれる) を使用して、ソースボリュームに対する変更や、ターゲットがロック解除中に行われたターゲットボリュームに対する変更を追跡します。インテントログには、両サーバにコミットされる前の書き込み要求が永続的に記録されます。

インテントログを使用することで、SIOS DataKeeper は、システム復旧後にミラーの完全再同期をすることなく、ソースまたはターゲットシステムの障害または再起動から復旧することが可能です。

ボリュームへの書き込みはインテントログファイルにも反映される必要があるため、多少のパフォーマンスオーバーヘッドが発生します。この影響を最小限に抑えるために、大量の読み取りまたは書き込み処理に使用されていない物理ディスクにインテントログを格納することをお勧めします。詳細については インテントログの再配置 を参照してください。

DataKeeper ビットマップのファイルサイズの計算

- ブロックごとに1ビット（各ブロックは 64KB）
- 1ビットは64KBのボリュームスペースを表します

    例： ボリュームが 640GB の場合、ビットマップは1,310,720バイトです。

    640 × 1073741824 / 65536 / 8

    計算すると、ビットマップは1,310,720バイトになります。

非共有ボリューム

デフォルトでは、インテントログの機能は有効になっており、インテントログファイルは、SIOS DataKeeper がインストールされるディレクトリ下の「Bitmaps」というサブディレクトリに保存されます。

デフォルト以外のディレクトリにインテントログを作成する場合は、BitmapBaseDir レジストリエントリを SIOS DataKeeper がファイルを作成するディレクトリに設定してください。詳細については「 インテントログの再配置 」を参照してください。

インテントログの機能を無効にする場合は、現時点での全てのおよび潜在的にミラーのエンドポイントとなるサーバ上で BitmapBaseDir レジストリエントリをクリア (空欄に設定) してください。**インテントログの機能を無効にするには、それらの各システムで設定が反映されるように再起動する必要があります。**この機能が無効になっている場合は、ソースシステムの障害時に完全再同期が必要になります。

共有ボリューム

共有ボリュームを複製しているとき、インテントログは、複製されたボリューム上の「ReplicationBitmaps」というサブディレクトリに保存されます。この設定はデータの完全再同期を実行することなく、共有ボリュームを使用する他のソースサーバへのスイッチオーバを可能にするために必要です。

SIOS は、インテントログをデフォルトの場所から移動させることを推奨していません。

設定に関する注意点

BitmapBaseDir のレジストリエントリを設定する場合、指定したフォルダとドライブレターが存在していることを確認してください。ドライブレターが存在しないまま設定すると、システム起動時に以下のエラーメッセージが表示されます。

> グローバルビットマップボリューム {ドライブレター}: はまだ検出されていません。このボリュームが存在しない場合、ミラーソーススレッドがハングすることがあります。BitmapBaseDir レジストリエントリが、ビットマップ格納用の正しいボリュームを指定していることを確認してください。

8.5.1.3.2. インテントログの再配置

インテントログ (ビットマップファイル) を再配置するには、関連するすべてのサーバ上で以下を実施してください。

> **注記:** ミラーはミラーリングの状態のままにしてください。一時停止し、ビットマップファイルを移動させないでください。

1. DataKeeper ミラーが複数ある場合、単一システムにすべてのミラーを移動し、すべてのミラーのソースにしてください。

> **注記:** これは、すべてのクラスター構成（2、3、4またはそれ以上のノード構成）に適用されます。

2. すべてのシステムで、ビットマップファイル (*R:\Bitmaps*)の新しい場所のディレクトリを作成してください。**重要:** ビットマップファイルをデフォルトの場所 (*%EXTMIRRBASE%\Bitmaps*) から移動する場合は、新しいディレクトリを作成してからレジストリで位置を変更し、システムを再起動する必要があります。

3. ミラーのソースシステム以外のすべてのシステムで、新しい場所を表すようにレジストリ値 BitmapBaseDir を修正してください。ターゲットおよびミラーのソースとボリュームを共有しているシステムもしくはターゲットとボリュームを共有しているシステムが含まれます。

   regedit でレジストリを編集してください。

   ```
   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\
   Parameters
   ```

   「BitmapBaseDir」パラメータを修正し、(新しい場所_R:\Bitmaps_)に変更してください。

4. ターゲット側の各システムを再起動してください。ボリュームが Windows クラスタの一部の場合は、同時に多数のノードをシャットダウンしないでください。クラスタクォーラムを失い、残りのクラスタ上のノードがシャットダウンすることがあります。

5. ソースシステム上のボリュームを別のシステム (ターゲットもしくは共有ソース) へスイッチオーバしてください。以前ソースであったシステムで手順 2 ～ 3 を繰り返し実行してください。

6. 旧ソースシステムを再起動した後、すべてのボリュームリソースはシステムにスイッチバックすることが可能です。

8.5.1.3.3. SIOS DataKeeper の再同期

SIOS DataKeeper は、ビットマップファイル (インテントログ) を使用して再同期を行います。割り当てたメモリを使用して、「ダーティ」または「クリーン」をブロックで把握しています。完全再同期が開始するときに、ファイルシステムが使用している各ブロックのビットが SIOS DataKeeper によって 1 (「ダーティ」) に初期化されます。これで、ターゲットシステムに送信する必要があることが示されます。完全再同期はミラーの初期作成時、またはミラーが中断された後の再同期中に発生します。続いて、ビットマップの先頭から処理を開始し、ビットが 1 (ダーティ) に設定されている最初のブロックを検出し、ローカルハードディスクから対応するブロックを読み取って、リモートシステムへ送信します。この処理が完了すると、ブロックを 0 (「クリーン」) に設定します。その後、SIOS DataKeeper は、次のダーティビットを検知し、このプロセスを繰り返します。

再同期中に新しい書き込みが発生すると、対応するブロックは 1 (ダーティ) に設定されます。

再同期処理が最後のビットマップに達すると、ダーティビットが残っていないかどうかを確認します。この確認は、ダーティになると 1 加算され、クリーンになると 1 減算されるカウンタを使用して行われます。ダーティブロックが残っている場合、ポインタをビットマップの先頭にリセットして処理を再開し、ダーティブロックだけをリモートシステムに送信します。

このプロセスは、すべてのブロックがクリーンになるまで複数のパスで実行されます。このプロセスが完了するとミラーの状態が **再同期** から **ミラーリング** に変わり、この時点ですべての書き込みがミラーリングされたことになります (この時点でビットマップも不要になります)。

再同期処理の進行状況は、パフォーマンスモニタで再同期制御カウンタを表示して確認できます。

この再同期処理と同じ仕組みが、ミラーの再開および一時停止処理にも使用されています。

> ! ミラーが一時停止およびロック解除されたときにDK GUI を介してターゲットシステムをリブート / シャットダウンする場合は、完全再同期が発生します。このケースにおいて完全再同期を回避するには、ターゲットシステムの再起動またはシャットダウンの前に「ミラーの再開およびロック 」を実行してください。

ミラーの初期作成

ミラーが作成されると、DataKeeper はソースボリュームからターゲットボリュームに対してデータの 初期同期 を実行する必要があります。これは完全再同期とも呼ばれます。ただし、データの初期同期が開始される前に DataKeeper はまず、ソースボリューム上で現在使用されていない領域のすべてのブロックを初期同期から除外する「 **空き領域の除外** 」と呼ばれる処理を実行します。除外したブロックは、ターゲットボリュームで複製する必要がありません。

例: 空き領域の除外

ソースボリュームの容量	80 GB
ソースボリュームの空き容量	35 GB
ミラーの初期作成時にソースボリュームからターゲットボリュームへ再同期されるデータ量	55 GB

8.5.1.3.4. 同期および非同期ミラーリング

SIOS DataKeeper は、非同期および同期ミラーリング両方の方式を採用しています。SIOS DataKeeper を正しく動作させるためには同期および非同期ミラーリングの長所と短所を理解することが必要です。

同期ミラーリング

同期ミラーリングでは、書き込みごとに割り込んでソースシステム上のストレージに書き込まれると同時にターゲットボリュームへの書き込みのために、ターゲットシステムへ転送します。ローカルおよびターゲットの書き込みが完了すると、書き込み要求が完了したと認識され、制御が書き込みを開始したアプリケーションへと戻されます。ソースシステム上の永続的なビットマップファイルが更新されます。

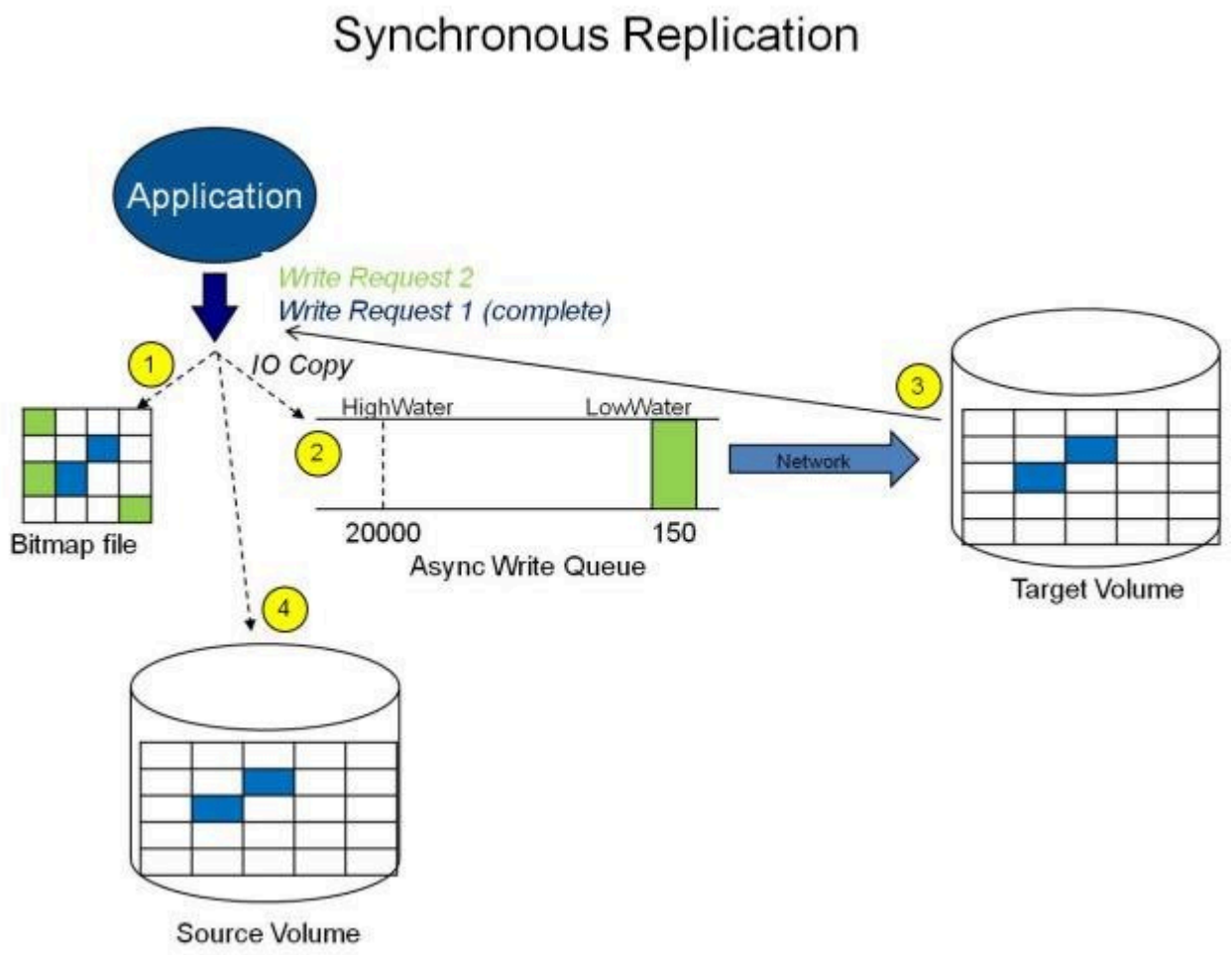
同期ミラーのソースボリュームに対して書き込み要求が行われた場合の処理を、以下の一連のイベントで説明します。

1. 以下の処理が並列で発生します。

   a.書き込みのコピーがミラー書き込みキューに置かれます。
   b.書き込みがローカルボリュームに送られて完了します。

2. 上記の両方の処理が完了すると、書き込みは完了の状態を呼び出し元に返します。

   a.ターゲットで書き込みが完了できない状態（ネットワーク伝送エラー、またはターゲットシステムでの書き込みエラー）が発生した場合、ミラー状態は [一時停止] に変更されます。ただし、呼び出し元に返されるボリューム書き込みの状態は影響を受けません。
   b.ローカルボリュームの書き込み状況が呼び出し元に返されます。



この図では、書き込み要求 1 はすでに完了しています。ターゲットボリュームとソースボリュームの両方が更新されています。

書き込み要求 2 はアプリケーションから送信され、書き込みがターゲットボリュームに書き込まれようとしています。ターゲットボリュームに書き込まれると、DataKeeper はターゲットボリュームで書き込みが成功したという確認応答を送信し、並行して、書き込みがソースボリュームに対してコミットされます。

この時点で、書き込み要求が完了し、書き込みを開始したアプリケーションに制御が戻されます。

同期ミラーリングは、ソースシステムの障害時にデータの損失が発生しないことを保証しますが、アプリケーションのパフォーマンスに影響をもたらします。ソースへの書き込みとネットワーク経由でのターゲットへの書き込みが完了するまでアプリケーションが待機する必要があるので、特に WAN または低速なネットワーク構成においてはパフォーマンスが低下します。

非同期ミラーリング

非同期ミラーリングでは、書き込みごとに割り込んで、データのコピーを作成します。このコピーはネットワークが送信可能な状態になるまでキューに入れられます。一方、元の書き込み要求はストレージデバイスへコミットされ、制御が書き込みを開始したアプリケーションへと即時に返されます。

複数のボリュームにまたがるデータ（データベースログおよびデータファイルなど）の一貫性を維持するために、いくつかのアプリケーションはそのボリュームにフラッシュリクエストを送信します。DataKeeper は、キュー内のすべての

書き込みがターゲットシステムに送信され、認識されるのを待つことによって、ミラーリング状態のミラーを持つボリューム上のフラッシュリクエストを受け取ります。このような場合にパフォーマンスが影響を受けるのを防ぐには、レジストリエントリ「 DontFlushAsyncQueue 」を設定するか、すべてのファイルを同じボリューム上に配置することを検討してください。

つまり、どの時点をとってもソースマシンからターゲットマシンへの送信を待っている書き込みトランザクションが存在することになります。しかし、ターゲットボリュームへの書き込み順序が正確なので、データの整合性は常に保たれます。万が一ソースシステムに障害が発生した場合、ターゲットシステムはキューにたまっていたすべての書き込みを受け取らないようにすることは可能ですが、ターゲットボリュームに対して送信されるデータは、有効なものとなります。

非同期ミラーのソースボリュームに対して書き込み要求が行われた場合の処理を、以下の一連のイベントで説明します。

1. ソースシステム上の永続的なビットマップファイルが更新されます。

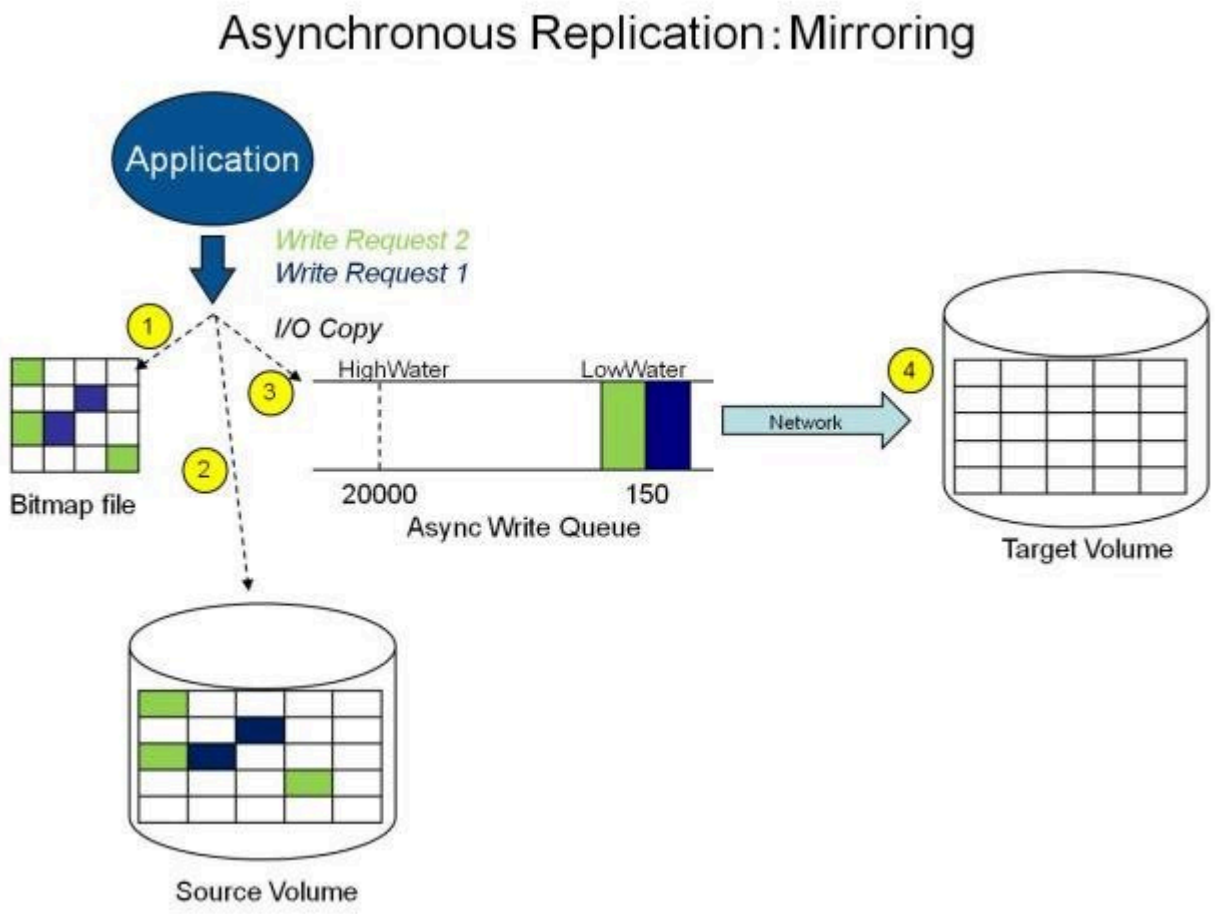
2. ソースシステムは書き込みのコピーをミラー書き込みキューに追加します。

3. ソースシステムでソースボリュームへの書き込み要求が実行され、呼び出し元に制御が返されます。

4. キュー内の書き込みはターゲットシステムに送られます。ターゲットシステムでターゲットボリュームに対する書き込み要求が実行されて、書き込みの状況がプライマリ側に返されます。

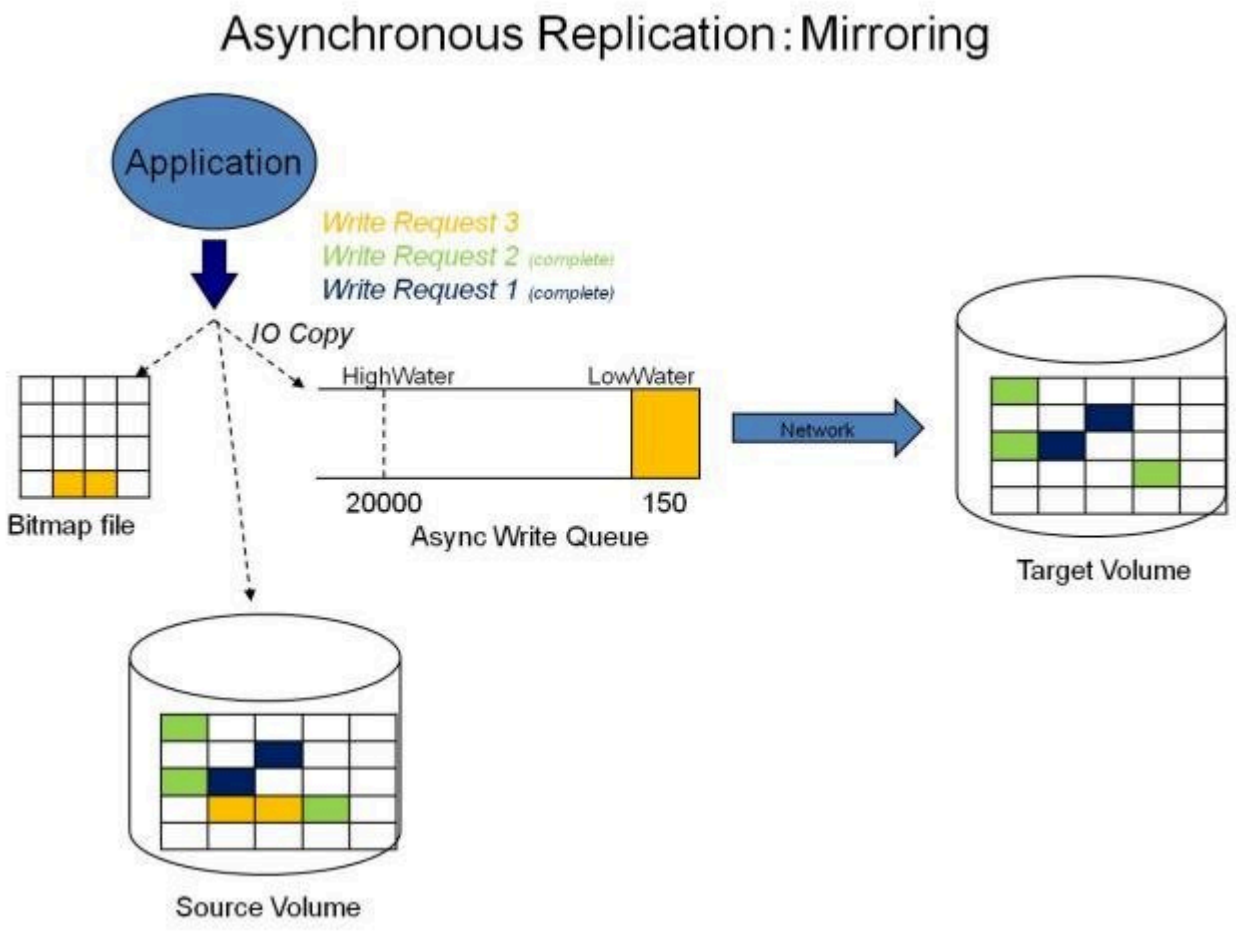
5. ミラーの書き込みキューが設定された制限に達すると（WriteQueueHighWater または WriteQueueByteLimit に達した場合）、動作を決定するためにミラーの「BlockWritesOnLimitReached」の設定が使用されます。BlockWritesOnLimitReached が「0」の場合、ミラーは一時停止され、少し後に部分再同期が開始されます。BlockWritesOnLimitReached が「1」の場合、書き込みキューに空きができるまで、書き込みは遅延します。ミラーはミラーリング状態のままですが、ネットワークの速度とリモートノードのボリュームに応じてアプリケーションのスループットが低下します。

6. ネットワーク転送時またはターゲットシステムでのターゲットボリューム書き込み実行時にエラーが発生した場合、セカンダリ側での書き込み処理は中断されます。ここで、ミラーの状態が **ミラーリング** から **一時停止** に変更されます。



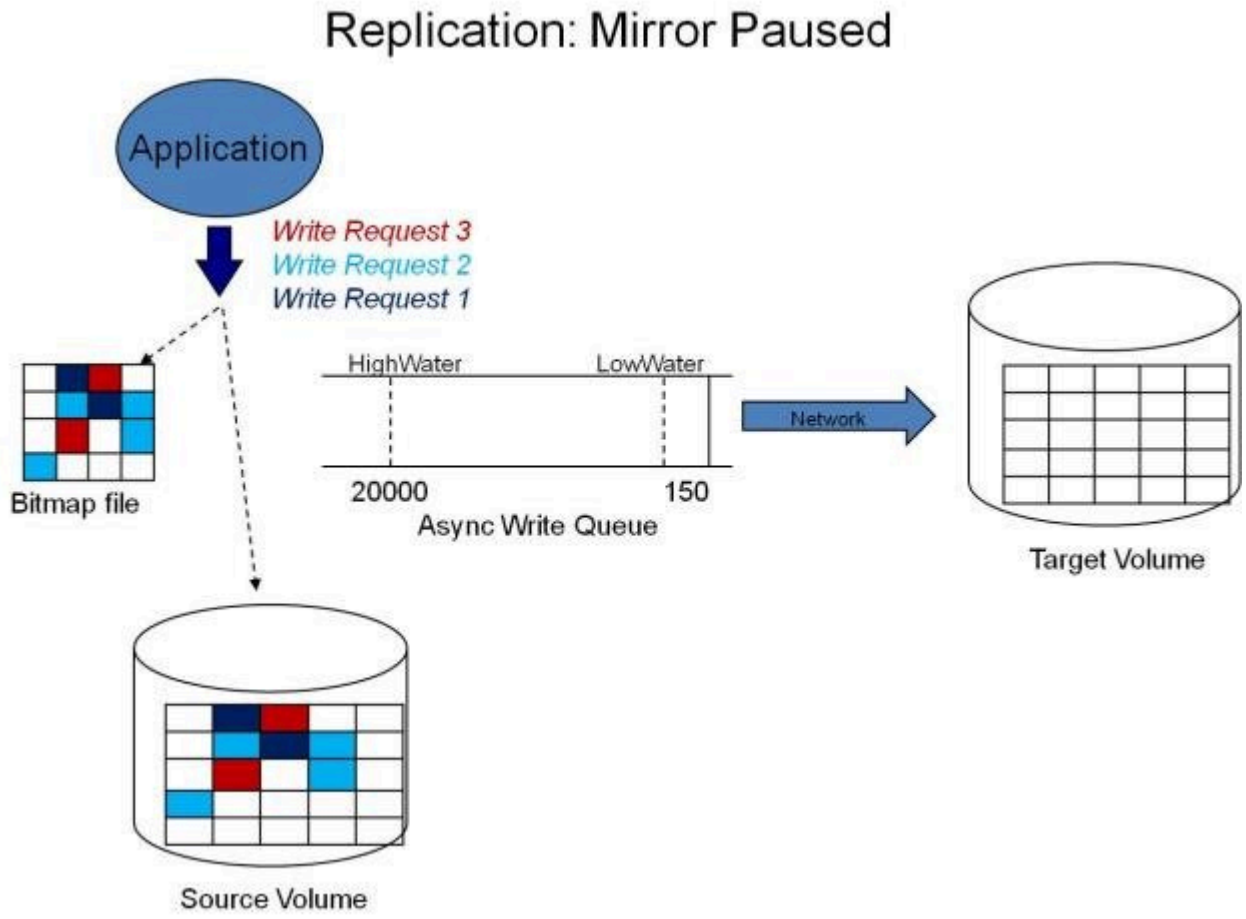
上の図では、2 つの書き込み要求がソースボリュームに書き込まれ、ターゲットシステムに送信するためにキューに入っています。ただし、制御はすでに書き込みを開始したアプリケーションに戻っています。

下の図では、最初の 2 つの書き込みがソースボリュームとターゲットボリュームの両方に正常に書き込まれている間に、3 つ目の書き込み要求が開始されています。ミラーリング中は、書き込み要求が時間の順にターゲットボリュームに送信されます。したがって、ターゲットボリュームはある時点で必ずソースボリュームの完全な複製となります。



ミラー一時停止

上記の通常のミラーリングプロセスが中断された場合は、ミラーの状態が **ミラーリング** から **一時停止** に変更されます。ソースボリュームに対するすべての変更が永続的なビットマップファイルだけでトラックされ、ターゲットシステムへは何も送信されません。



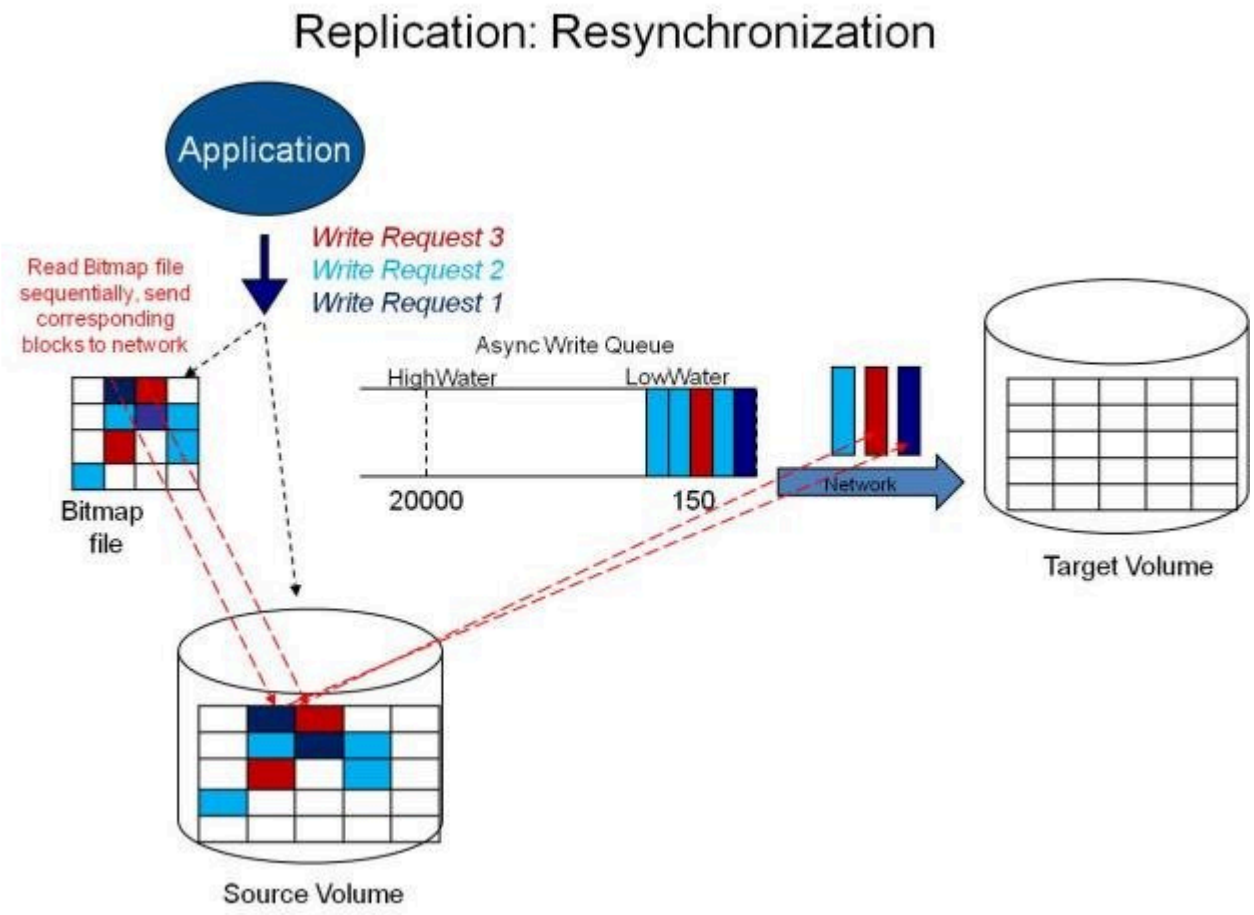
ミラー再同期

非同期または同期ミラーの中断が解決された場合は、ソースおよびターゲットの再同期が必要になり、ミラーは **再同期** 状態になります。

DataKeeper は、永続的なビットマップファイルを順次読み取ってミラーが **一時停止** 中にソースボリュームで変更されたブロックを判断し、それらのブロックのみをターゲットボリュームと再同期します。この手順は、データの部分再同期と呼ばれます。

GUI では **再同期 (ペンディング)** 状態と表示される場合がありますが、これは一時的な状態であり、**再同期** 状態に変更されます。

再同期中、ミラーが同期ミラーであったとしてもすべての書き込みが非同期として扱われます。ビットマップ内のダーティーとしてマークされた特定のビットが上記で説明されている部分同期の処理中にターゲットに送信されます。


Replication: Resynchronization
Application
Write Request 3
Write Request 2
Write Request 1
Read Bitmap file sequentially, send corresponding blocks to network
Async Write Queue
HighWater
LowWater
20000
150
Network
Bitmap file
Target Volume
Source Volume

8.5.1.3.5. 読み込みおよび書き込み操作

ボリュームミラーが作成され、プライマリサーバとセカンダリサーバの 2 つのドライブが同期されると、次のイベントが発生します。

- システムがすべてのユーザのターゲットボリュームへのアクセスをロックします。ターゲットボリュームへの読み込みおよび書き込みは拒否されます。ソースボリュームは書き込みおよび読み込み可能です。

- プライマリサーバのドライバへのミラーボリュームおよび非ミラーボリュームの読み込み操作は、割り込みせずに通過し通常通りに完了します。セカンダリシステム上のミラーボリュームの読み込み操作は許可されません。すなわち、セカンダリは障害の発生したプライマリの役割を引き継ぎません。

- プライマリサーバが書き込み要求を受けると、まず最初にシステムがミラーボリュームに対するものかどうかを判断します。ミラーボリュームに対するものでない場合、書き込みはそれ以上割り込みされず、通常通りに完了します。書き込み要求がミラーリングされたボリュームに対するものである場合は、書き込み要求はミラーリングの種類に応じて処理されます。

- ミラーリングの種類が 同期 の場合、書き込み要求はターゲットに送信するためにミラーの書き込みキューに置かれ、同時にローカルのソースボリュームに送られます。ソースディスクの書き込みが完了し、**かつ** ターゲットから（成功または失敗の）通知を受けるまで、書き込みを発行したプロセスに対して書き込み処理は完了したと認識されません。ネットワーク転送時またはターゲットシステムの書き込み実行時にエラーが発生した場合、ターゲット側での書き込み処理は中断し、ミラーの状態は **一時停止** に変更されます。ターゲットの書き込みの状態に関係なく、ソースボリュームは書き込みを完了します。

- ミラーリングの種類が 非同期 の場合、プライマリ側のソースボリュームに対する書き込み要求が実行され、書き込みのコピーが非同期書き込みキューに格納されて、呼び出し元に制御が返されます。キュー内の書き込みはターゲットボリュームに送られます。セカンダリ側のターゲットボリュームに対する書き込み要求が実行されて、書き込みの状況がプライマリ側に返されます。ネットワーク転送時またはセカンダリ側でのミラーボリューム書き込み時にエラーが発生した場合、セカンダリ側の書き込み処理は中断します。ここで、ミラーの状態が **ミラーリング** から **一時停止** に変更されます。

システム運用を確実にするために、SIOS DataKeeper は次のような場合にミラーの一時停止と自動再開 (すなわち、部分的な再同期) を行います。

- 短期間でのボリュームへの大量の書き込み（例：データベースの作成時など）によりミラーの BlockWritesOnLimitReached 設定が 0 で、ミラー書き込みキューの長さが WriteQueueHighWater の上限値に達するか、キューのバイト数が WriteQueueByteLimitMB の上限値に達した場合。ユーザは SIOS DataKeeper パフォーマンスモニタカウンタを使用してミラーリング処理を監視し、必要に応じて WriteQueueHighWater を調整することができます。詳細は、レジストリエントリ を参照してください。

- ターゲットシステムへの書き込みの転送がタイムアウトした場合や、リソース不足のために失敗したとき (例えば、短時間の大量書き込みや、ネットワーク転送により、ソースシステムがリソース不足になった場合)。

8.5.1.3.6. ボリュームの考慮事項

SIOS DataKeeper のプライマリおよびセカンダリシステムには、システム、非ミラー、ミラーの 3 種類のボリュームが備わっています。ミラーリング処理の間、システムおよび非ミラーボリュームは影響を受けず、ユーザはボリューム上のすべてのアプリケーションおよびデータに完全にアクセスすることが可能です。

ミラーリングできないボリューム

SIOS DataKeeper サービスは次の種類のディスクパーティションを処理対象から除外します。

- Windows システムボリューム
- Windows ページファイルを含むボリューム
- NTFS 形式以外のボリューム (FAT、FAT32、Raw FS、ReFSなど)
- 固定ドライブ以外 (CD-ROM、フロッピーディスクなど)
- ソースボリュームよりサイズの小さいターゲットボリューム

ボリュームサイズの考慮事項

ソースシステムとターゲットシステムのドライブは、物理サイズが同じでなくてもかまいません。ミラーを確立するとき、ターゲットボリュームはソースボリュームと同じサイズ、またはそれ以上のサイズでなければなりません。

SIOS DataKeeper ミラーに加えることができるボリュームのサイズに制限はありません。しかしながらミラーの初期作成時に、ボリューム上のファイルシステムが使用するデータはすべて、ターゲットに送信する必要があります。例えば、20 GB ボリューム上で、2 GB が使用済みで 18 GB が空きである場合は、2 GB のデータをターゲットと同期する必要があります。両システム間のネットワーク接続の速度は、同期するデータの量とともに、最初のミラーの作成にかかる時間を決定づけます。

注記：バージョン8.3 以前では、LifeKeeperとWSFCの組み合わせで許容される最少のボリュームサイズは500MB（536,870,912 bytes）

8.5.1.3.7. ミラーリング用ネットワークカードの指定

SIOS DataKeeper では、ミラーエンドポイントとして使用する IP アドレスを管理者が指定することができます。この処理により、必要に応じてクライアントネットワークと複製データを送信するためのミラーリング用のトラフィックを分離することが可能になります。

レプリケーション専用の LAN

必須ではありませんが、2 つのサーバ間を専用 (プライベート) ネットワークでつなぐと、パフォーマンスが向上し、クライアントネットワークに悪影響を及ぼしません。

8.5.1.3.8. パフォーマンスモニタカウンタ

SIOS DataKeeper は、ボリュームのミラーリングステータスに関する統計機能でパフォーマンスモニタを拡張したカウンタを装備しています。このカウンタは、SIOS DataKeeper ソフトウェアのフルインストールでインストールされます。

このカウンタにアクセスするには、次の操作を行ってください。

1. **Microsoft Windows 2008** システムでは、**[スタート]** メニューの **[信頼性とパフォーマンス]** グループから **Windows の [パフォーマンス モニター]** を開始してください。

   Microsoft Windows 2012 システムでは、**[管理ツール]** の **[パフォーマンス モニター]** オプションから **Windows の [パフォーマンス モニター]** を開始してください。
   Windows のすべてのバージョンで、コマンドラインに `perfmon.msc` コマンドを入力してパフォーマンスモニタを開始できます。

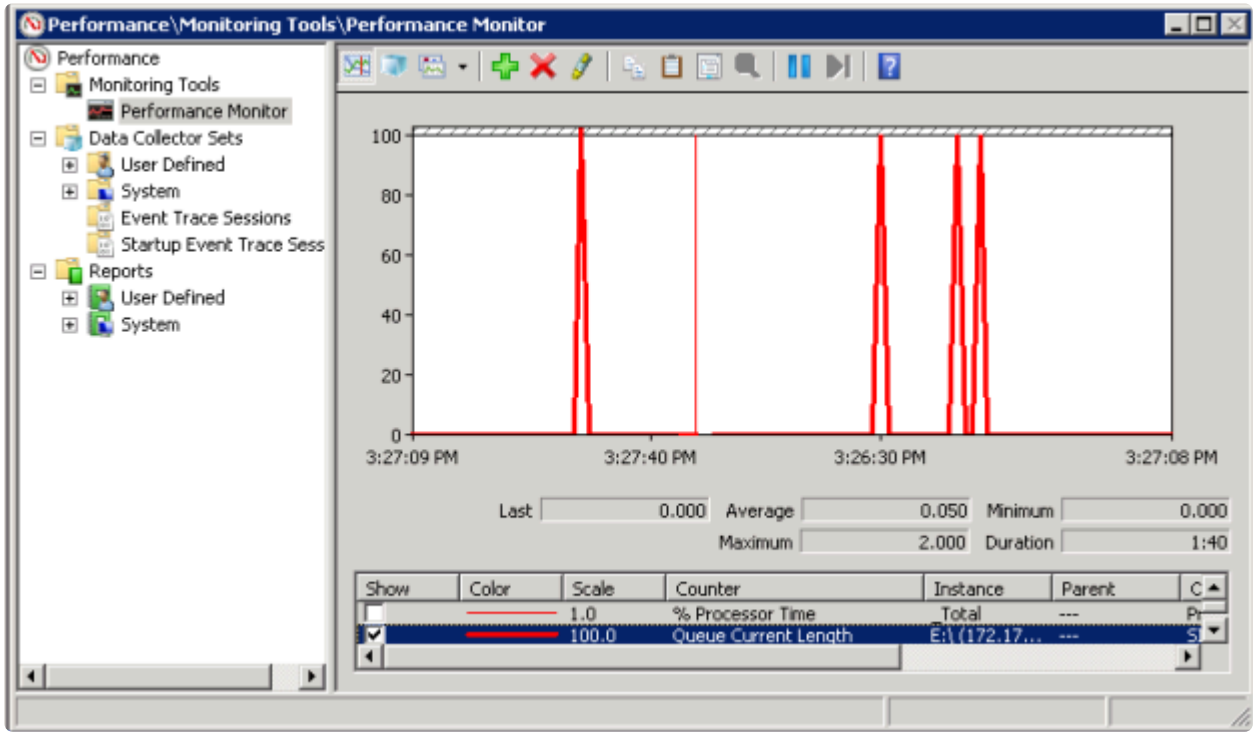
2. **[モニタリングツール]** ペインから **[パフォーマンスモニター]** を選択してください。

3. チャートペインの **[+]** ボタンをクリックして、**[カウンタの追加]** ダイアログボックスを開いてください。

4. **SIOS Data Replication** オブジェクトを選択してください。

> DataKeeper（DK）およびDataKeeper Cluster Edition（DKCE）のパフォーマンスモニタカウンタは、ミラーの ソース ロールにあるシステムでのみ利用できます。ソースの役割にミラーがあるシステムでは、そのミラーの各ターゲットで使用可能な指定されたカウンタのインスタンスが1つ存在します。SIOS DataKeeperパフォーマンスカウンタは、ミラーがターゲットロールにあるシステムでは使用できません。

SIOS DataKeeper には、製品に関する各種の動作を監視できるカウンタが 17 個あります。これらのカウンタを使用すると、それらの動作をステータス、キューの統計値、および一般的なミラーステータスとして監視できます。



ミラー状態カウンタ

Mirror Elapsed Time（ミラー経過時間）

デフォルト値:　0

範囲:　0 ～ MAX_ULONG

この値は、ボリュームがミラー状態である時間 (単位: 秒) を表します。この値が 0 のボリュームは、現在ミラーに関係していないボリューム、現在ミラーを作成中 (および同期中) のボリューム、およびミラーが破損したか削除されたボリュームです。

Mirror State（ミラーの状態）

デフォルト値:　0

範囲:　0 ～ 5

この値は、ボリュームの現在のミラー状態を表します。定義されている値は以下のとおりです。

0 (なし): ボリュームは現在、ミラーに関与していません。

1 (ミラーリング): ボリュームは現在、ターゲットをミラーリングしています。

2 (再同期): ボリュームは現在、ターゲットと同期中です。

3 (破損): ミラーが存在しますが、ソースとターゲットのボリュームが非同期です。このボリュームへの新規書き込みは追跡されません。

4 (一時停止): ミラーが存在しますが、ソースとターゲットのボリュームが非同期です。ソースサーバは、すべての新規書き込みを追跡します。

5 (再同期保留): ソースボリュームが再同期を待っています。

Mirror Type（ミラーの種類）

デフォルト値: 0

範囲: 0 ～ 2

この値は、このボリュームが関与するミラーリングの種類を表します。このリリースでは、以下の値が定義されています。

0 (なし): ボリュームは現在、ミラーに関与していません。

1 (同期): データはターゲットにへの送信のために書き込みキューに置かれ、ローカルボリュームに同時に書き込まれます。両方の処理が完了するまで、書き込み処理は完了したとは認識されません。

2 (非同期): データはターゲットへの送信のために書き込みキューに置かれ、ローカルボリュームに同時に書き込まれます。ローカルボリュームの書き込み処理が完了すると、書き込み処理が認識されます。

Network Number of Reconnects（ネットワーク再接続回数）

デフォルト値: 0

範囲: 0 ～ MAX_ULONG

この値は、ボリュームがミラーリングされていた間に実行されたネットワークの再接続回数です。ネットワーク再接続は、ターゲットとの通信が切断された場合に発生します。

書き込みキューカウンタ

Queue Byte Limit（キューの最大バイト数）

デフォルト値: 0

この値は、WriteQueueByteLimitMB レジストリ値で設定されている書き込みキューバイトの最大値を表します。この値はバイトで表示されるため、レジストリで設定された値の 1048576 倍です。

Queue Current Age（キューの現在の待ち時間）

デフォルト値: 0

範囲: 0 -

この値は書き込みキューの最も古い書き込み要求の経過時間（ミリ秒）です。

Queue Current Bytes（キューの現在のバイト数）

範囲： 0 ～ <ミラーの書き込みキューに割り当てられたバイト数>

この値は、指定されたミラーの書き込みキューに割り当てられたバイト数を表します。

Queue Current Length（キューの現在の長さ）

デフォルト値: 0

範囲: 0 ～ <ミラー書き込みキューの書き込み回数>

この値は、選択されたミラーに対する書き込みキューの現在の長さを書き込み回数で表しています。

Queue High Water（キューの最大値）

デフォルト値: 20000

このカウンタは WriteQueueHighWater のレジストリ値で設定されている書き込みキューの上限を表します。

Queue Low Water（キューの最小値）

デフォルト値: 150

この値は非推奨であり、現在使用されていません。ただし、パフォーマンスモニタによって追跡することができます。

再同期制御カウンタ

Resync Reads（再同期読み込み数）

デフォルト値: 20

この値は、ミラー再同期の間、読み込んでターゲットシステムに送信するために処理中にできる最大ディスクブロック数を表します。

Resync Current Block（現在再同期中のブロック）

デフォルト値: 0

範囲: 0 ～ <再同期ブロック総数>

同期中の場合、この値はターゲットに送信されている現在のブロックを表示します。同期中でない場合 (すなわちミラーの状態が EmMirrorStateResync でない場合)、この値は 0 です。

同期中にボリュームへの書き込みが継続している場合、指定されたブロックは複数回にわたってターゲットへ送信されます。これは必要な再同期の回数に基づきます。

Resync Dirty Blocks（再同期するダーティブロック数）

デフォルト値:　0

範囲:　0 ～ <再同期ブロック総数>

この値はミラーの再同期中にダーティとされたブロックの合計数です。「ダーティ」ブロックとは、同期が完了する前にターゲットマシンに送信する必要があるブロックです。この値は、EmMirrorStateResync 以外の状態で 0 です。

ミラーの同期が開始されると、この値は当初、再同期ブロック数の値と等しくなります。ミラーの同期中にボリュームに対する大量の書き込みが発生すると、再同期ダーティブロック数が増加することに注意してください。

注記: このカウンターを使用して、再同期するために残っているデータ量を確認できます。残りのデータ量は “Resync Dirty Blocks” X 65536 です（65536 はブロック内のバイト数です）。

Resync Elapsed Time（再同期経過時間）

デフォルト値:　0

範囲:　0 ～ MAX_ULONG

ミラーが再同期されている間、この値は再同期処理が発生してからの経過時間 (単位: 秒)を表します。ミラーが再同期処理に成功すると、最後にシステムが起動してから前回の再同期処理までにかかった再同期の総時間を表します。再同期されていないボリューム、または最後の起動時に同期されなかったボリュームの値は 0 になります。

Resync New Writes（再同期する新規書き込み数）

デフォルト値:　0

範囲:　0 ～ MAX_ULONG

この値は、再同期処理が開始されてからボリューム上で発生した書き込み数を表します。この値はダーティブロックの数、ミラーの同期に必要なパスの回数、および再同期の完了に要した時間に直接影響します。

Resync Pass（再同期パス）

デフォルト値:　10

範囲:　0 ～ MaxResyncPasses (レジストリ)

この値は、ターゲットを更新するための再同期処理中に現在ボリュームを介して実行されるパスの数です。再同期処理の完了に必要なパスの数は、再同期中に実行される書き込みの量に従って増加します。再同期中はソースボリュームへの書き込みが許可されているので、大量の書き込みにより再同期処理の完了に要する時間が長くなります。

Resync Total Blocks（再同期ブロック総数）

デフォルト値:　0

範囲:　0 ～ MAX_ULONG

この値は、ミラーボリュームの再同期に対して使用された 64k ブロックの数を表します。この値は、ボリュームのファイルシステムを 64k で除算した商とほぼ等しくなります。ファイルシステムのサイズは、Windows のディスクの管理プログラムで表示されるディスクパーティションのサイズより小さいことに注意してください。ファイルシステムのサイズを確認するには、CHKDSK X: (X はドライブレター) を実行してください。

Resync Phase（再同期フェーズ）

デフォルト値:　0

範囲:　0 ～ 3

この値は非推奨であり、現在使用されていません。

8.5.2. 構成

要件/考慮事項

このセクションでは、DataKeeper の設定を行う前に知っておくべき前提条件を確認します。

- セクタサイズ
- ネットワーク帯域
- ネットワークアダプタ設定
- DataKeeper サービスログオン ID とパスワードの選択
- ファイアウォール設定
- 高速ストレージのベストプラクティス
- クラスタノードから外部DRサイトへのデータレプリケーション構成
- パフォーマンスチューニング
- 「すべてのドライブのページングファイルサイズを自動で管理する」を無効にする
- WAN の考慮事項
  - LAN / WAN 間のデータの初期同期
  - 圧縮
  - ネットワーク帯域制限

8.5.2.1. セクタサイズ

DataKeeper バージョン 7.2.1 以降では、セクタサイズが 512 バイト以外のディスクがサポートされます。ただし、DataKeeper では、ミラーターゲットが構成されたディスクと同じセクタサイズのディスク上にミラーソースボリュームを構成する必要があります。NTFS メタデータにはディスクのセクタサイズが含まれます。DataKeeper はソースからターゲットに NTFS ファイルシステム全体を複製するので、セクタサイズが一致する必要があります。

注記: DataKeeper バージョン 7.2 以前では、セクタサイズが標準の 512 バイトであるディスクデバイスのみがサポートされます。

8.5.2.2. ネットワーク帯域

DataKeeper は使用可能な任意のネットワークを経由してデータを複製できるので、「1 日中ソースボリュームを更新しながらボリュームを正常に複製し、ミラーの **ミラーリング** 状態を維持するのに十分な帯域はあるか」という問題を特に考慮する必要があります。

ボリュームのスイッチオーバはミラーが **ミラーリング** 状態でなければ実行できないので、ミラーの **ミラーリング** 状態を維持することは重要です。

ネットワーク帯域要件の特定

SIOS DataKeeper をインストールする前に、データを複製するためのネットワーク帯域要件を特定する必要があります。レプリケーションする予定のデータの変更の割合を測定するには、以下の方法を使用してください。この値は、そのデータを複製するために必要なネットワーク帯域の量を示します。

ネットワーク帯域要件を特定した後、パフォーマンスが最大になるようにネットワークを設定してください。ネットワーク帯域要件が現在使用できるネットワークの性能を上回っている場合には、以下の点を考慮する必要があります。

- DataKeeper で (または、可能であればネットワークハードウェアで) 圧縮を有効にする
- Hyper-V 仮想マシンを複製する場合は、一時データとスワップファイル用に、ローカルに複製されないストレージリポジトリを作成する
- 複製対象のデータの量を減らす
- ネットワーク性能を強化する

ディスク上で発生する変更の割合に対応するにはネットワーク性能が不十分である場合、DataKeeper ミラーは長時間、再同期状態のままになります。再同期中はターゲットボリュームのデータの一貫性は保証されません。

変更の割合の測定

パフォーマンスモニタ (perfmon) を使用して、複製対象のボリュームで発生する変更の割合を測定してください。このためには、一定期間 (例えば 1 日) のディスク書き込み処理のログを作成して、ディスク書き込みのピーク期間を確認するのが最善の方法です。

ディスク書き込み処理を追跡するには、以下の操作を行ってください。

- perfmon を使用して、Windows 2008 または Windows 2012　のユーザ定義データコレクタセットを作成します。
- ボリュームごとにカウンタ [Disk Write Bytes/sec] を追加します。ボリュームカウンタは論理ディスクグループにあります。
- ログを開始し、事前に決めておいた期間実行してから停止し、ログを開きます。

ディスク書き込みのログを作成する代わりに、パフォーマンスモニタツールの perfmon を使用して対話形式でディスク書き込みバイト数/秒を追跡し、最大値および平均値を確認することもできます。

SIOS DataKeeper は、短時間の爆発的な量の書き込み処理に対処するために、そのデータを非同期キューに追加します。ただし、長期的には、すべての複製対象ボリュームを合わせたディスク書き込み処理の平均が、DataKeeper およびネットワークで転送できる変更量を下回っていることを確認してください。

SIOS DataKeeper は、概算の平均で、以下の変更の割合を処理できます。

ネットワーク帯域	変更の割合
1.5 Mbps (T1)	182,000 バイト/秒 (1.45 Mbps)
10 Mbps	1,175,000 バイト/秒 (9.4 Mbps)
45 Mbps (T3)	5,250,000 バイト/秒 (41.75 Mbps)
100 Mbps	12,000,000 バイト/秒 (96 Mbps)
1000 Mbps (ギガビット)	65,000,000 バイト/秒 (520 Mbps)

8.5.2.3. ネットワークアダプタ設定

DataKeeper では、名前付きパイプ接続を行うためにネットワークインターフェース上で「 **Microsoft ネットワーク用ファイルとプリンタ共有** 」を有効にして、DataKeeper のコマンドラインツール (EMCMD) を実行できるようにする必要があります。

名前付きパイプ接続を実行できるかどうかをテストするには、ターゲットシステム上でネットワークドライブのマッピングを試してください。これに失敗する場合は、名前付きパイプに問題があります。

また、DataKeeper では、**NetBIOS over TCP/IP** および **SMB** のプロトコルも有効にする必要があります。GUI が正常に動作しない場合は、以下のネットワーク設定が有効になっていることを確認してください。

- 以下の例のように、**NetBIOS over TCP/IP** および **SMB** のプロトコルを有効にしてください。

  ［マイ コンピュータ］ -> ［管理］ -> ［システム ツール］ -> ［デバイス マネージャ］ -> ［表示］ -> ［非表示のデバイスの表示］ -> ［プラグ アンド プレイではないドライバ］ -> ［NetBIOS over Tcpip］ (有効)

- 以下の例のように、ミラートラフィックを転送する各ネットワークアダプタで **NetBIOS over TCP/IP** を有効にしてください。

  ［スタート］ -> ［設定］ -> ［ネットワークとダイアルアップ接続］ -> <ネットワークアダプタ> -> ［プロパティ］ -> ［インターネット プロトコル (TCP/IP)］ -> ［プロパティ］ -> ［詳細...］ ボタン -> ［WINS］ タブ -> ［NetBIOS over TCP/IP を有効にする］ ラジオボタン (有効)

- DataKeeper Administrator GUI を使用する各システムで、Microsoft の「 **Microsoft ネットワーク用クライアント** 」コンポーネントを有効にしてください。これは、前述の **NetBIOS over TCP/IP** を有効にしたネットワークアダプタで実行する必要があります。以下に例を示します。

  ［スタート］ -> ［設定］ -> ［ネットワークとダイアルアップ接続］ -> <ネットワークアダプタ> -> ［プロパティ］ -> ［Microsoft ネットワーク クライアント］ (有効)

- DataKeeper Administrator GUI がローカルおよびリモートで接続する各システムで、Microsoft の「 **Microsoft ネットワーク用ファイルとプリンタ共有** 」コンポーネントを有効にしてください。これは、**NetBIOS over TCP/IP** を有効にしたのと同じアダプタ (上記) で実行する必要があります。以下に例を示します。

  ［スタート］ -> ［設定］ -> ［ネットワークとダイアルアップ接続］ -> <ネットワークアダプタ> -> ［プロパティ］ -> ［Microsoft ネットワーク用ファイルとプリンタ共有］

8.5.2.4. DataKeeper サービスログオン ID とパスワードの選択

新規の DataKeeper インストール設定時に、ユーザは DataKeeper サービスログオン ID とパスワードの入力を求められます。

DataKeeper サービスは、認証された接続を使用してボリュームのスイッチオーバを実行し、複数のサーバ間でミラーロールを変更します。DataKeeper サービスを実行するために選択されたログオン ID アカウントに応じて、サーバ間の接続を確立してボリュームスイッチオーバを実行するために使用できる権限が決まります (特に、サーバまたはネットワークの障害が発生した場合)。

以下のように、数種類のサービスログオン ID アカウントを使用できます。

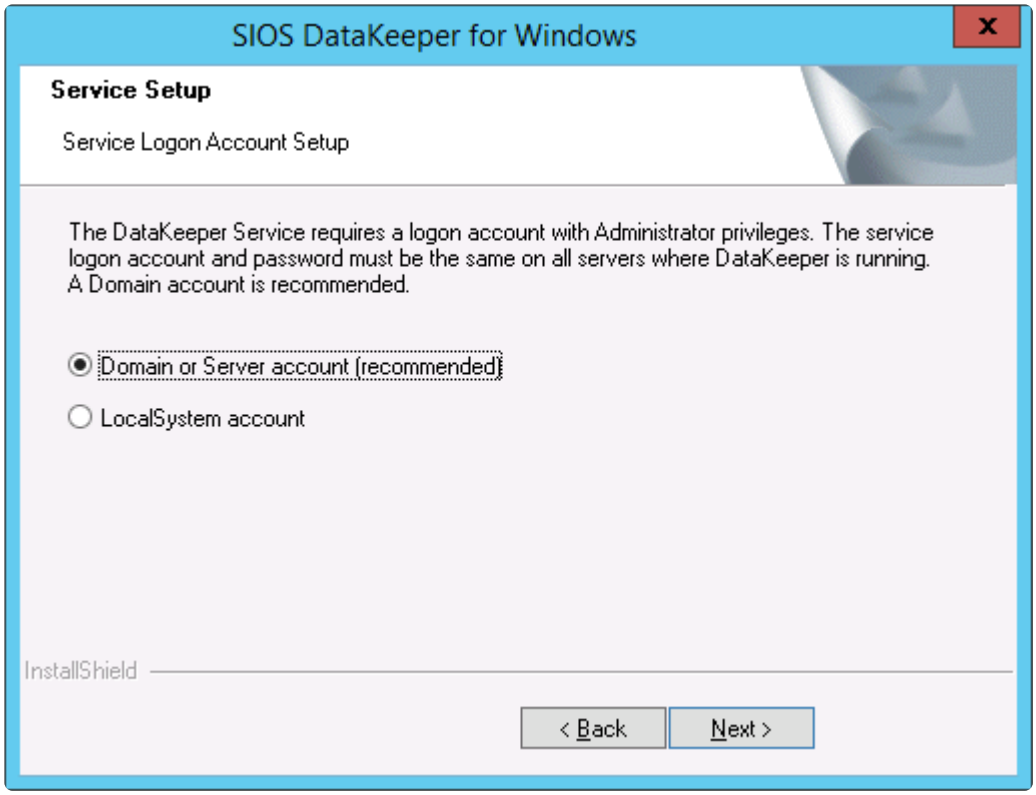
- ドメイン内の接続されたすべてのサーバで有効な、管理者権限を持つ **ドメインアカウント** (*推奨*)
- 接続されたすべてのサーバで有効な、管理者権限を持つ **サーバアカウント**
- **ローカルシステムアカウント** (*推奨しない*)

  注記: ワークグループの場合は、各システム上で DataKeeper の サービスアカウントとして **サーバアカウント** オプションおよびサーバ名 / 管理者を使用してください。**すべてのサーバに同一の ログオン ID および パスワードを使用する必要があります** (関連する 既知の問題 を参照)。

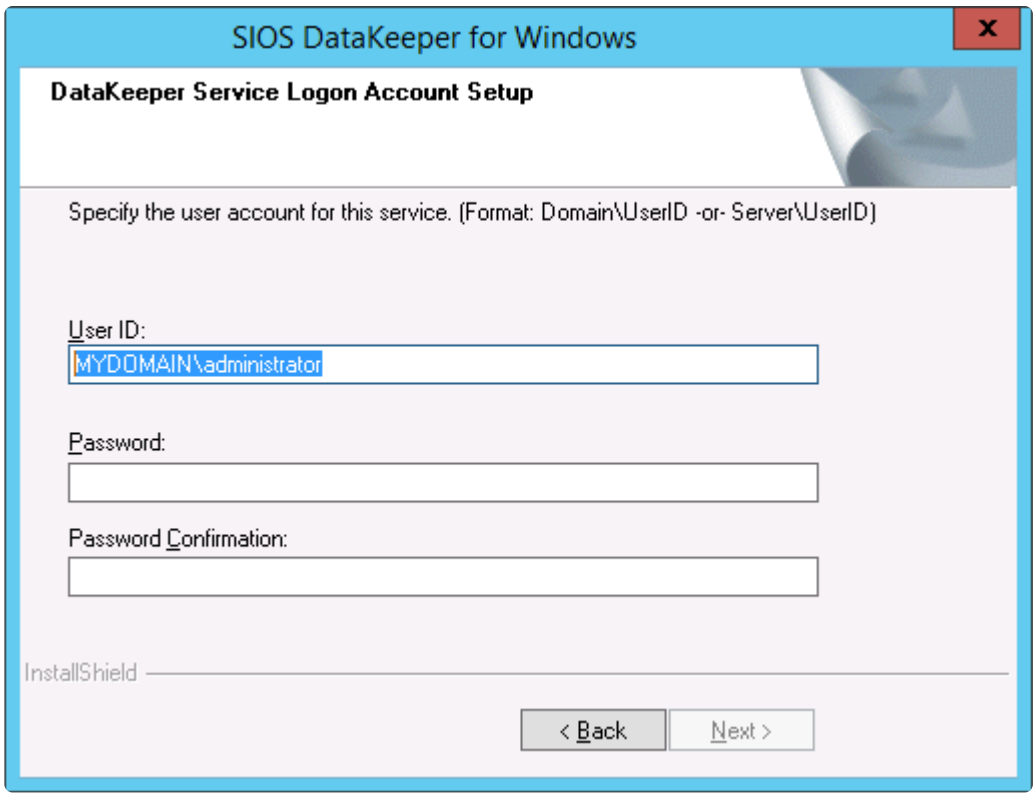
注記: 使用するドメインアカウントまたはサーバアカウントは、ローカルシステム管理者グループに追加する必要があります。アカウントには、DataKeeper がインストールされているサーバの管理者権限が備わっている必要があります。

Active Directory によるネットワーク接続が失われた場合、ローカルシステムアカウントはドメイン内で正常に認証できないことに注意してください。その場合、ローカルシステムアカウントではサーバ間の接続を確立できず、ネットワーク経由の DataKeeper ボリュームのスイッチオーバコマンドは拒否されます。ネットワーク障害などの障害回復時にフォールトトレランスを要求される IT 部門では、ローカルシステムアカウントを使用しないでください。

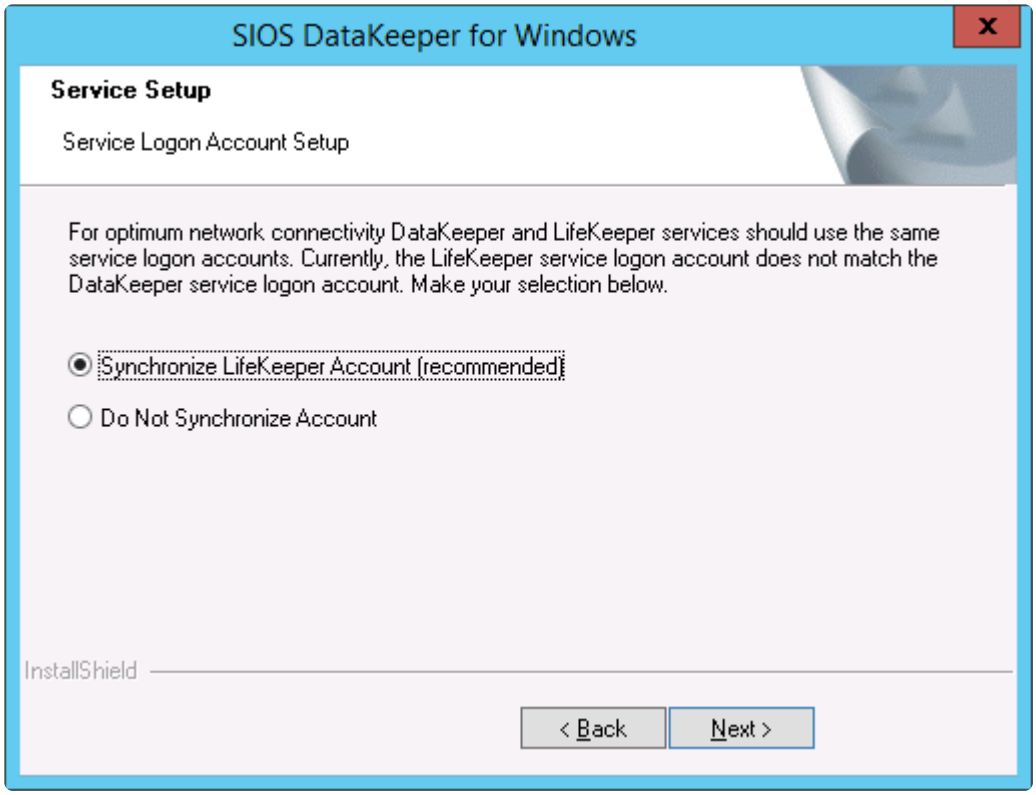
DataKeeper のインストール – サービスログオン ID タイプの選択



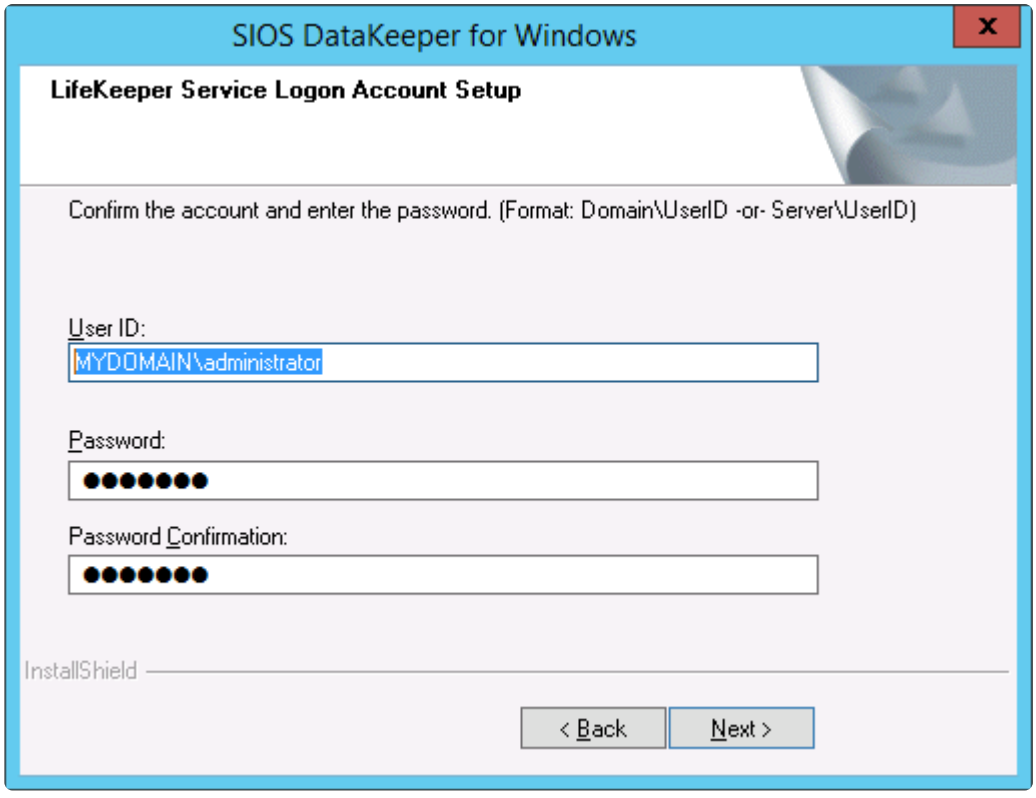
上の画面でドメインアカウントまたはサーバアカウントを選択した場合は、DataKeeper サービスログオン ID とパスワードの入力フォームが表示され、情報を入力できます。



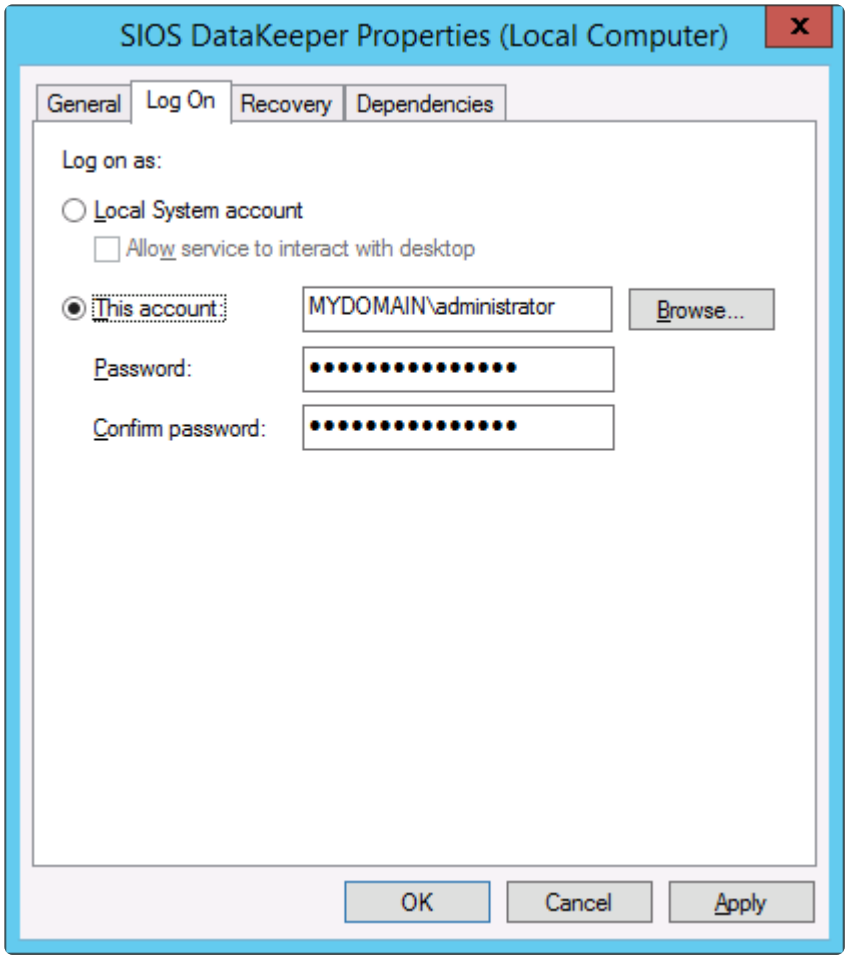
より信頼性の高いスイッチオーバーとフェールオーバーのための、LifeKeeperとDataKeeperのサービスアカウント同期機能の提供をします。



LifeKeeper Serviceのログオン



すでにサービスログオン ID とパスワードを使用して DataKeeper サービスを設定している場合、サービス ID とパスワードの選択ダイアログは表示されません。ただし、管理者は、Windows サービスアプレットを使用して、DataKeeper サービスログオン ID とパスワードをいつでも変更できます。ログオン ID やパスワードを変更した後は、必ず DataKeeper サービスを再起動してください。



次の表はそれらの要件について概説しています。

環境	DataKeeper サービスの要件	DataKeeper UI の要件
同じドメイン または 信頼されたドメイン環境	• 同じアカウントを持つすべてのシステムで、同じ認証情報を使用して DK サービスを起動してください。 • default = Local System Account を使用することが許可されています。	• ドメイン管理者でログインし、DK GUI を起動してください。 • 「run as」管理オプションを使用して DK GUI を起動してください。
ドメインサーバとワークグループサーバが混在した環境 または 個々のドメインサーバ	• 各システムで同じアカウント名およびパスワードにてローカルアカウントを作成してください。 • このローカルアカウントを Administrator グループに追加してください。	DK サービスを起動するために作成したローカルアカウントを使用してログインしてください。 DK GUI を起動してください。 **すべてのサーバに同一の ログオン ID およびパスワードを使用する必要があります** (関連

	• すべてのシステムで、ローカルアカウントを使用して DK サービスを起動してください。	する 既知の問題 を参照)。

8.5.2.5. ファイアウォール設定

ソースマシンとターゲットマシンでファイアウォールが正しく設定されていない場合、SIOS DataKeeper は正常に動作しません。つまり、レプリケーショントラフィックを転送するネットワークのファイアウォールに加えて、SIOS DataKeeper を実行する各サーバの送受信接続に関する規則も設定する必要があります。

SIOS DataKeeper のインストール時に、DataKeeper に必要なファイアウォール規則の設定に加えて、Windows 2008 および 2012 上での DataKeeper に必要なその他のシステム設定をインストーラに許可するかどうかの確認を求められます。インストーラによる変更を許可した場合は、手動でファイアウォールを設定する必要はありません。インストーラによる変更を許可しなかった場合は、このセクションの説明に従って、手動でシステムを設定する必要があります。

レプリケーションのために開けておく必要があるポートは、137、138、139、445、9999 です。また、レプリケーションに使用する予定のボリュームレターに応じて 10000 ～ 10025 の範囲内のポートを開けておく必要があります。以下の表に、レプリケーションに使用する予定のドライブレターに応じて追加で開く必要があるポートを示します。

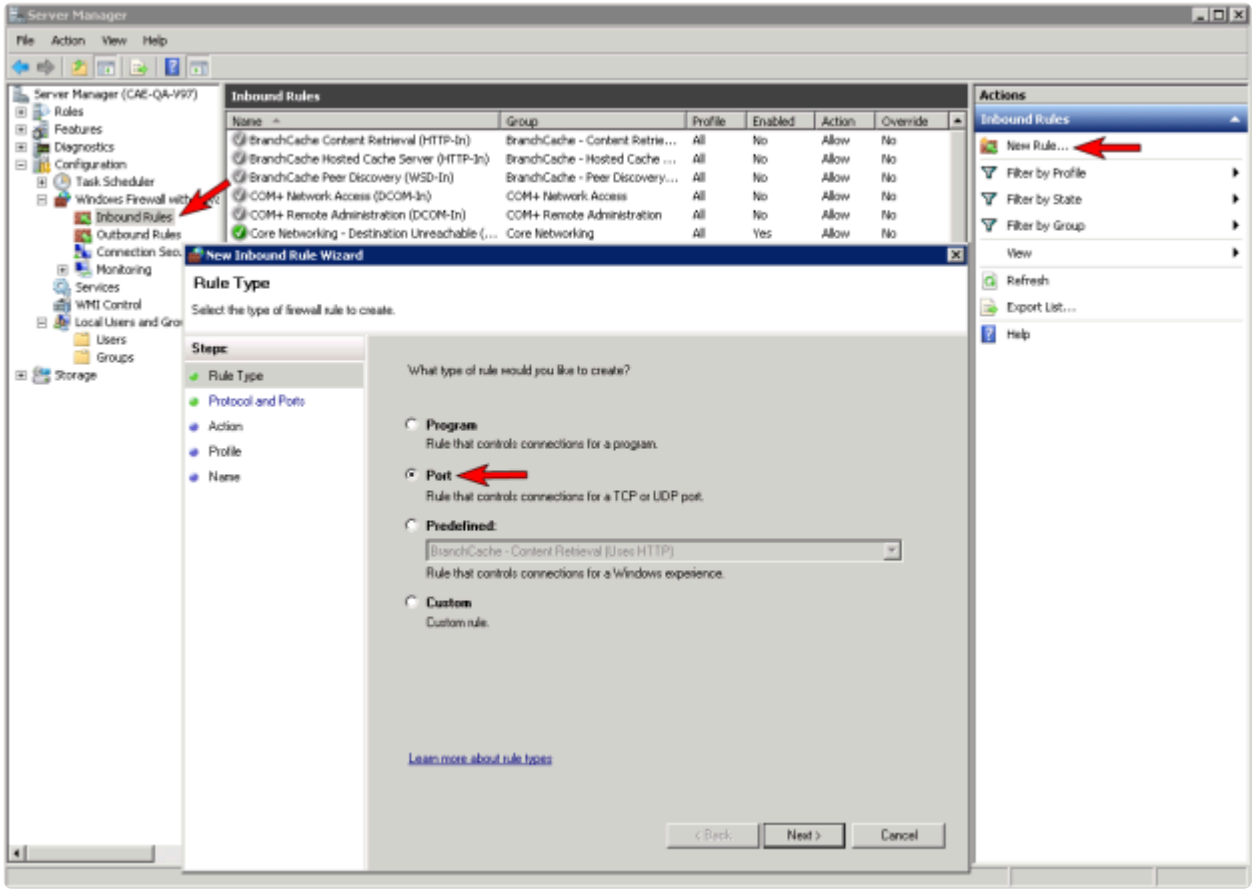
ポート番号:	ボリュームレター	ポート番号:	ボリュームレター
10000	A	10013	N
10001	B	10014	O
10002	C	10015	P
10003	D	10016	Q
10004	E	10017	R
10005	F	10018	S
10006	G	10019	T
10007	H	10020	U
10008	I	10021	V
10009	J	10022	W
10010	K	10023	X
10011	L	10024	Y
10012	M	10025	Z

セキュリティが強化された Microsoft の Windows ファイアウォールの設定例

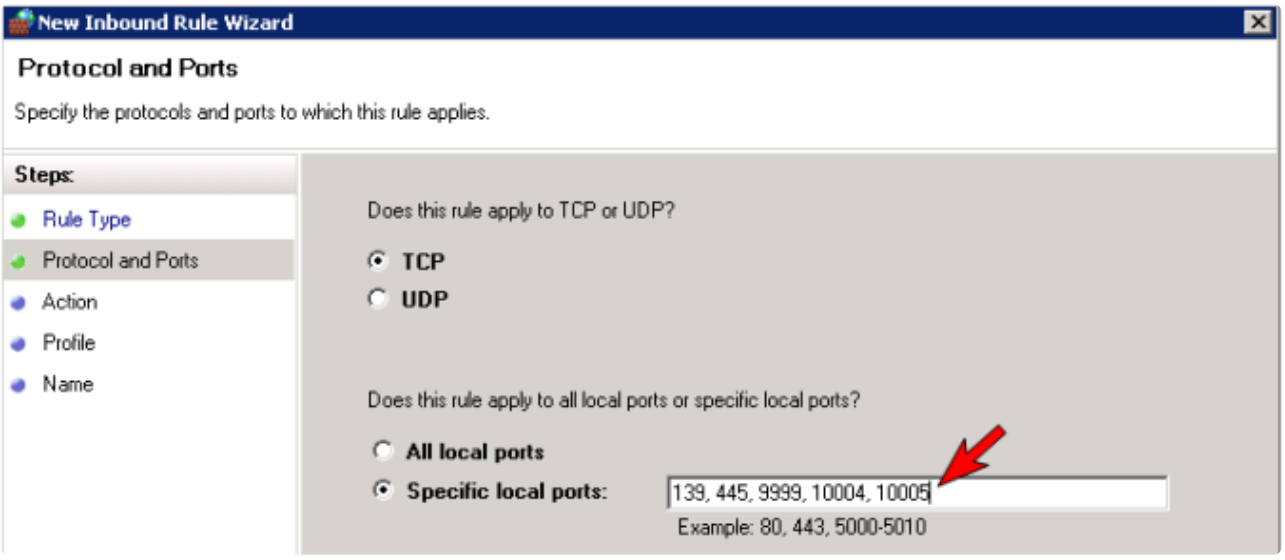
各クラスタのファイアウォールの設定に必要な正確な手順は、クラスタごとの設定に応じて異なります。以下の手順およびスクリーンショットは、SIOS DataKeeper を使用して E: および F: のボリュームを複製する場合の例です。前のセクションにあるポート番号とボリュームレターの表を参照してください。

1. Microsoft の **Windows サーバー マネージャー** を開き、**[受信の規則]** を選択して、TCP プロトコルと UDP プロトコルの規則を作成してください。

2. ウィンドウの右側にある **[操作]** パネルから **[新規の規則]** を選択してください。作成する規則の種類として **[ポート]** を選択してください。**[次へ]** を選択してください。

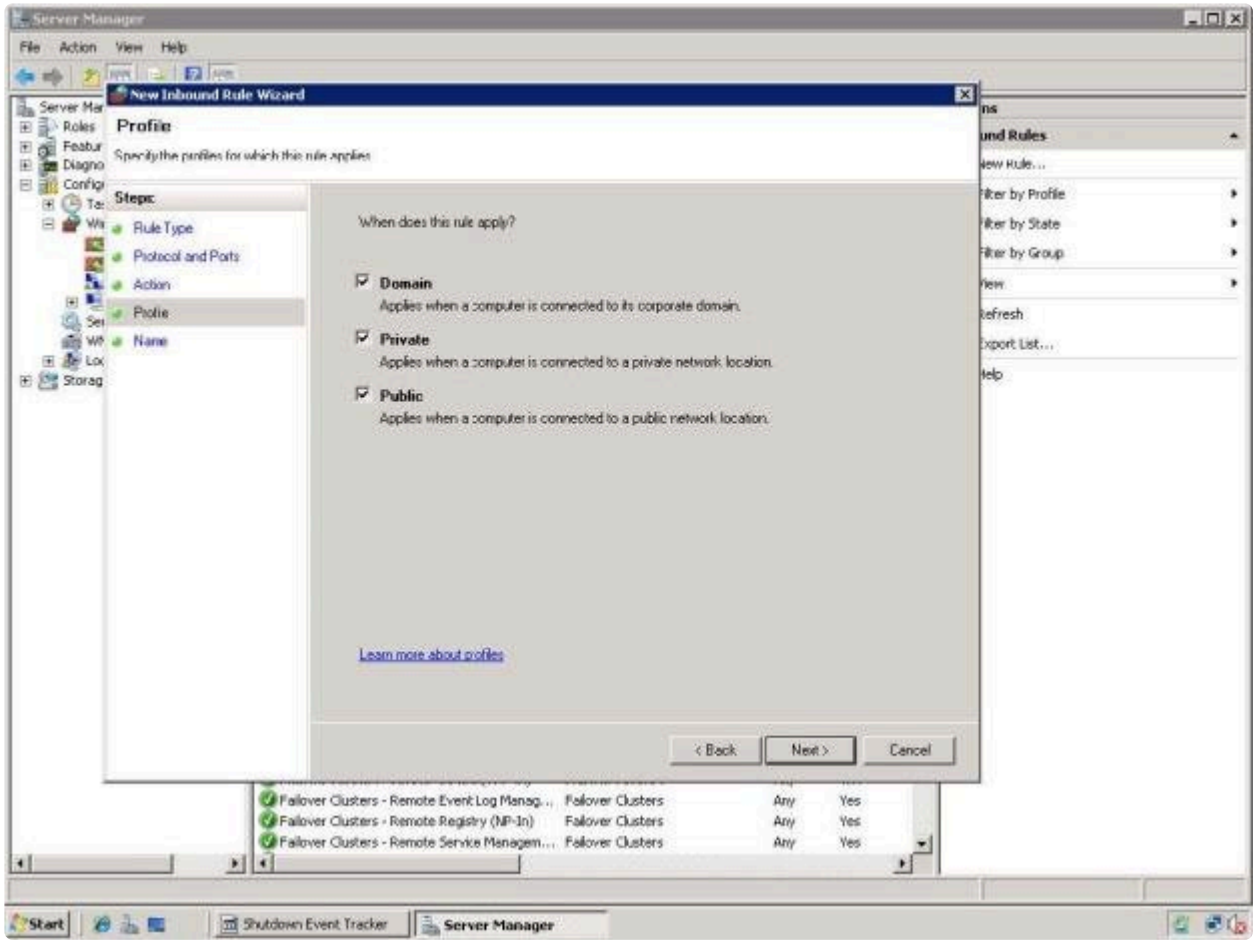


3. この規則の対象となるプロトコルの種類として、**[TCP]** を選択してください。*[特定のローカル ポート]* ボタンを選択し、**139** 、**445** 、**9999** 、**10004** (E ドライブ用)、および **10005** (F ドライブ用) の各ポートを入力してください。**[次へ]** を選択してください。

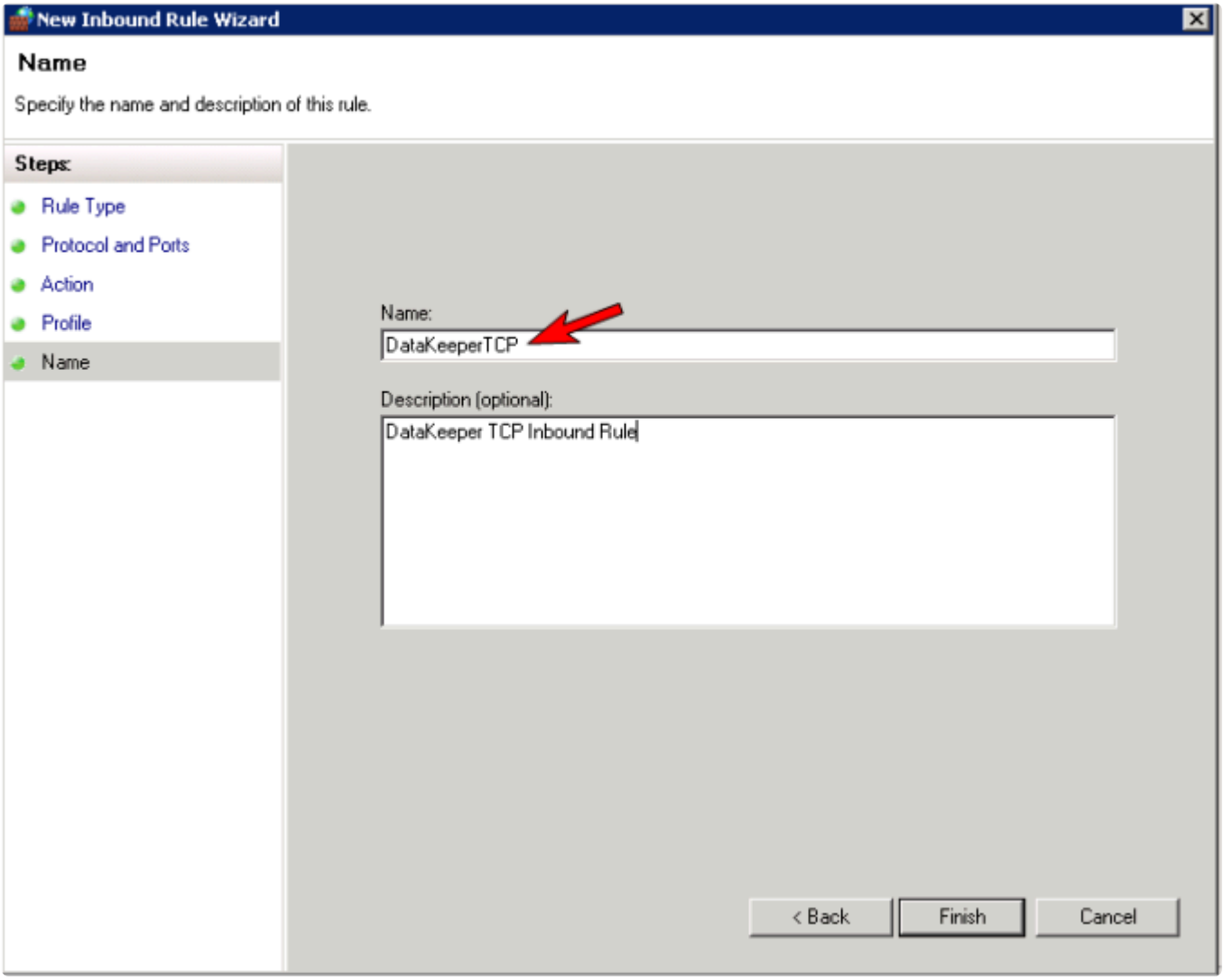


4. 操作として **[接続を許可する]** を選択してください。**[次へ]** を選択してください。

5. プロファイルには、この規則を適用する条件として **[ドメイン]** 、**[プライベート]** 、および **[パブリック]** を選択してください。**[次へ]** を選択してください。



6. 新規の **[受信の規則]** の **[名前]** および **[説明]** を入力し、**[完了]** をクリックしてください。



7. **[新規の規則]** を再び選択し、**UDP プロトコル** の規則を作成してください。作成する規則の種類として **[ポート]** を選択してください。*[次へ] *を選択してください。

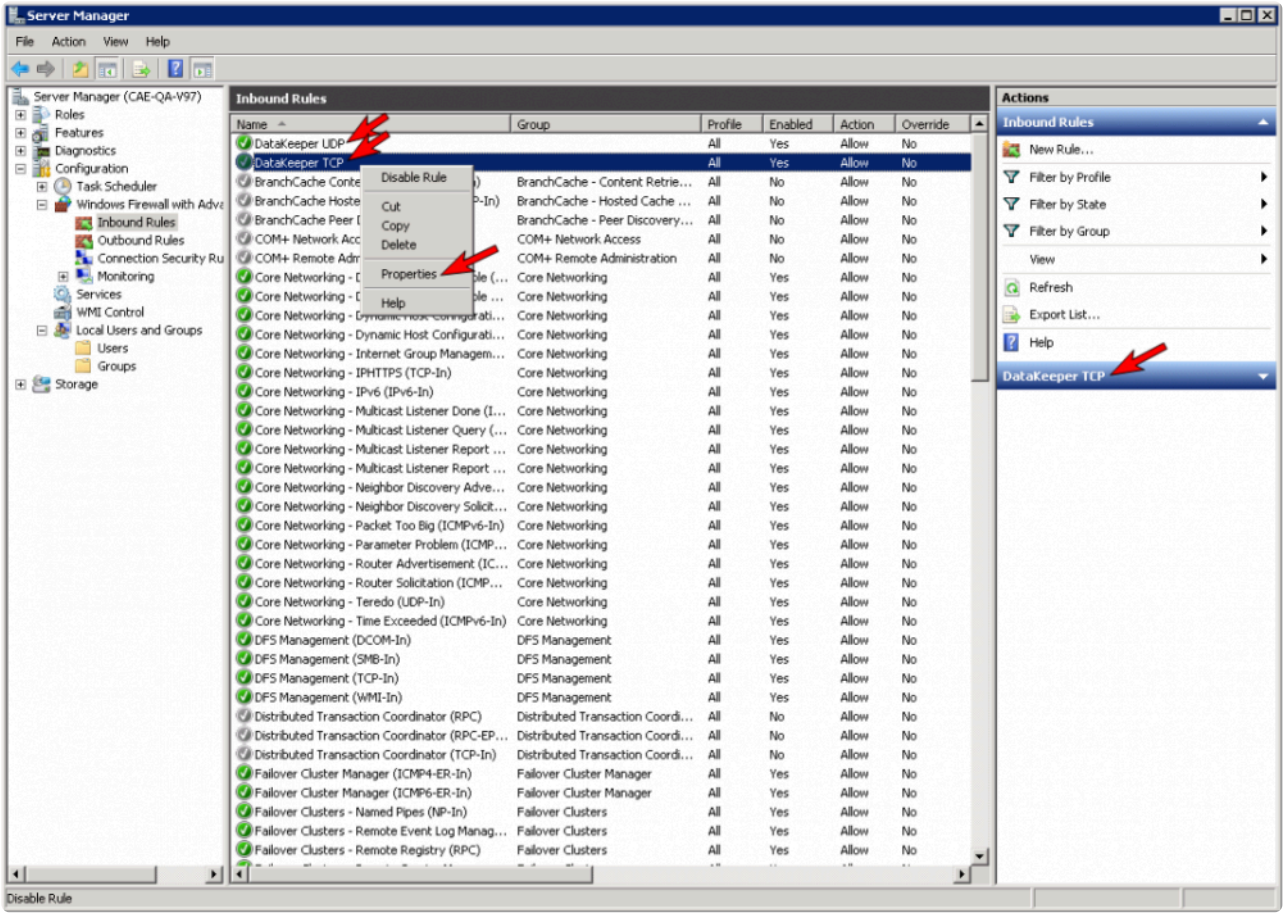
8. この規則の対象となるプロトコルの種類として、**[UDP]** を選択してください。**[特定のローカル ポート]** ボタンを選択し、[特定のローカル ポート] フィールドに **137** 、**138** を入力してください。**[次へ]** を選択してください。

9. 操作として **[接続を許可する]** を選択してください。**[次へ]** を選択してください。

10. プロファイルには、この規則を適用する条件として **[ドメイン]** 、**[プライベート]** 、および **[パブリック]** を選択してください。**[次へ]** を選択してください。

11. 新規の **[受信の規則]** の **[名前]** および **[説明]** を入力し、**[完了]** をクリックしてください。

12. **[受信の規則] リスト*およびパネルの *[操作]** 列に、新しい DataKeeper の規則が表示されます。中央のパネルで DataKeeper の規則 を選択して右クリックすると、規則の **[プロパティ]** を参照できます。


Server Manager
File Action View Help
Server Manager (CAE-QA-V97)
Roles
Features
Diagnostics
Configuration
Task Scheduler
Windows Firewall with Adva
Inbound Rules
Outbound Rules
Connection Security Ru
Monitoring
Services
WMI Control
Local Users and Groups
Users
Groups
Storage
Inbound Rules
Name
Group
Profile
Enabled
Action
Override
DataKeeper UDP
DataKeeper TCP
Disable Rule
Cut
Copy
Delete
Properties
Help
Actions
Inbound Rules
New Rule...
Filter by Profile
Filter by State
Filter by Group
View
Refresh
Export List...
Help
DataKeeper TCP
Disable Rule

8.5.2.6. 高速ストレージのベストプラクティス

ビットマップの設定

DataKeeper のデフォルトのビットマップの場所 (`(%ExtMirrBase%\Bitmaps)`) が高速ストレージ上にない場合は、ビットマップアクセスの I/O ボトルネックを解消するためにビットマップを高速ストレージデバイスに移動する必要があります。このために、ビットマップファイルを配置する高速ストレージドライブに小さいディスクパーティションを割り当ててください。ビットマップを配置する場所にフォルダを作成し、次にこの場所にビットマップ (インテントログ) を再配置 してください。

ディスクパーティションのサイズ

ディスクパーティションのサイズは、システムに存在する各ミラーのすべてのビットマップファイル格納できるだけの十分な大きさである必要があります。DataKeeper ビットマップの各ビットはボリューム上の 64 KB の領域を表すので、ビットマップファイルのサイズを決定するには、以下の式を使用してください。

<volume size in bytes> / 65536 / 8

例:

765 GB のボリュームの場合、765 GB をバイトに換算します。

```
765 * 1,073,741,824 = 821,412,495,360 バイト
```

この結果を 64K (65,536 バイト) で除算すると、ブロック数/バイト数が得られます。

```
821,412,495,360 / 65,536 = 12,533,760 ブロック/バイト
```

このブロック数/バイト数を 8 で除算すると、ビットマップファイルのサイズ (単位: バイト) が得られます。

```
12,533,760 / 8 = 1,566,720
```

したがって、765 GB のボリュームのビットマップファイルには、1,566,720 バイト、つまり約 1.5 MB が必要です。

簡略化した概算では、ディスク容量 1 GB あたり 2 KB のビットマップファイル容量が必要です。

すべてのミラーターゲット用の容量を忘れずに確保してください (マルチターゲットシステムでは、各ターゲットにビットマップファイルが必要です)。また、ミラーリングされるすべてのボリューム用の容量も確保してください。

管理されていないシャットダウン処理の問題

電力喪失やその他の状況により管理されていないシャットダウンが発生すると、再起動時に整合性チェックが強制的に実行されます。このチェックには数分以上かかることがあり、一部のベンダーのドライブが再接続されず、ミラーが未解決になることがあります。ドライブが再接続しない場合は、デバイスの管理者コンソールを使用してドライブを

再接続するか、システムを再起動して、チェックが実行されていることを確認してください。詳細については、ユーザーガイドまたはお使いのデバイスのベンダーガイドを参照してください。

そのほかの推奨および提案

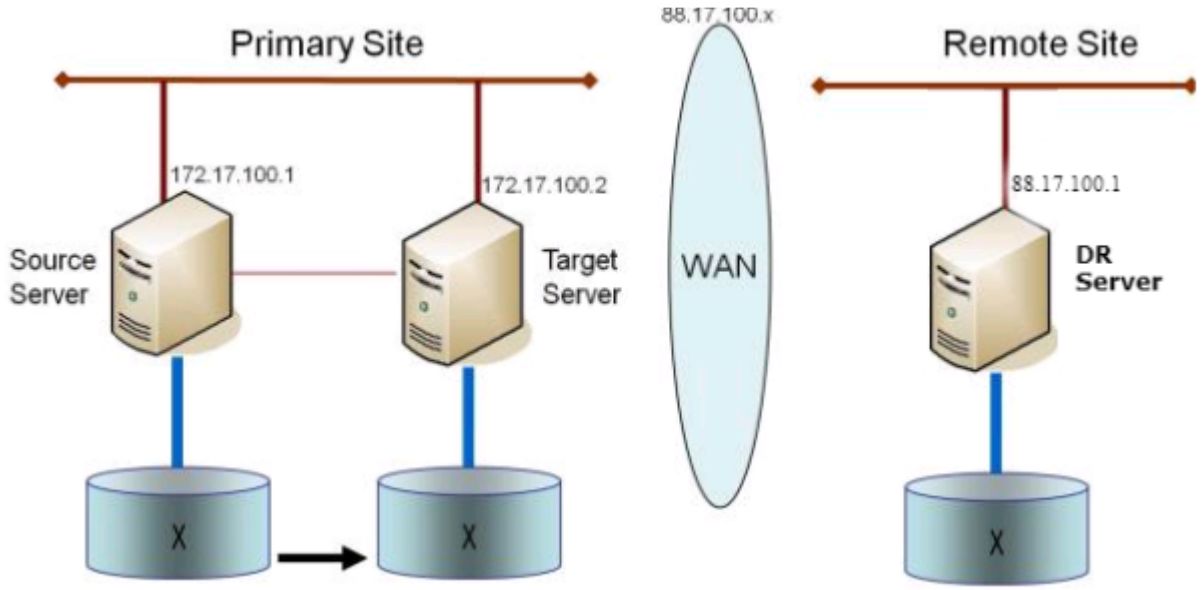
- ネットワークインターフェース構成の設定をチェックしてください。インターフェース上の受信バッファと送信バッファを増加すると、多くの場合レプリケーションのパフォーマンスが向上します。パフォーマンスに影響を与える可能性のある、その他の設定として以下のものがあります。フロー制御、ジャンボフレーム、および TCP オフロード。場合によっては、フロー制御と TCP オフロードを無効にするとレプリケーションのパフォーマンスが向上することがあります。大規模イーサーネット環境ではスループットが向上します。

- バス上の NIC の場所 (NIC が物理的に取り付けられているスロット) を確認してください。これもまたスピードに影響を与えることがあります。

- インターネット上にある無償提供の I/O サブシステム測定/特性分析ツール Iometer を使用して、ネットワークするープットをテストしてください。Iometer はクライアント/サーバ構成で設定可能で、ネットワークスループットを直接テストできます。別の方法では、複製したIP アドレスを使用してファイル共有を設定し、大量のデータをそこにコピーして、`Perfmon` (Network Interface / Bytes Sent Per Second)、またはタスクマネージャの [ネットワーク] タブを使用してネットワークスループットを監視してください。

- ネットワークアダプタに最新のドライバおよびファームウェアを使用しているかを確認してください。

8.5.2.7. クラスタノードから外部DRサイトへのデータレプリケーション構成



8.5.2.8. パフォーマンスチューニング

SIOS DataKeeperのパフォーマンスを向上させる方法については、以下のトピックを参照してください。

SIOS DataKeeper インテントログ – SIOS DataKeeperは、インテントログ（ビットマップファイルとも呼ばれます）を使用して、ソースに加えられた変更、またはターゲットのロックが解除されたときにターゲットボリュームに加えられた変更を追跡します。このログは、まだ両方のサーバーにコミットされていない書き込み要求の永続的な記録です。インテントログにより、SIOS DataKeeperは、システムの回復後に完全なミラー再同期をしなくとも、ソースまたはターゲットシステムの障害や再起動に耐えることができます。インテントログに関連するパフォーマンスオーバーヘッドが発生しますが、これはボリュームへの書き込みはインテントログファイルにも反映される必要があるためです。この影響を最小限に抑えるためには、インテントログを大量の読み取りまたは書き込みに関与しない物理ディスクに格納することをお勧めします。詳細については、インテントログの再配置 を参照してください。

高速ストレージのベストプラクティス – DataKeeper のデフォルトのビットマップの場所 `((%ExtMirrBase%\Bitmaps))` が高速ストレージ上にない場合は、ビットマップアクセスの I/O ボトルネックを解消するためにビットマップを高速ストレージデバイスに移動する必要があります。このためには、ビットマップファイルを配置する高速ストレージドライブに小さなディスクパーティションを割り当ててください。ビットマップを配置する場所にフォルダを作成し、次にこの場所にビットマップ (インテントログ) を再配置 してください。

> 注記:システムが Azure または AWS にある場合は、揮発性ストレージを推奨します。

8.5.2.9. 「すべてのドライブのページングファイルサイズを自動で管理する」を無効にする

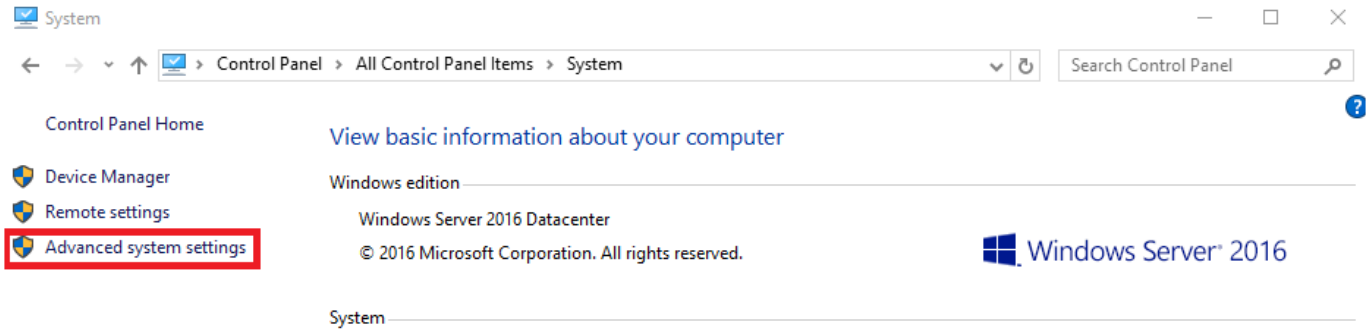
デフォルトではオペレーティングシステムが最適であると判断したページファイルが自動的にボリューム上に作成されるように、Windows は仮想メモリを構成します。この仮想メモリの設定は「すべてのドライブのページングファイルサイズを自動で管理する」と呼ばれます。

この設定を有効にすると、DataKeeper ミラーの一部であるボリューム上のオペレーティングシステムによってページファイルが作成されることがあります。ページファイルが作成されると、DataKeeper は完全な保護に必要なボリューム上で操作を実行できません。この設定は、DataKeeper ミラーを持つすべてのシステムで無効にする必要があります。

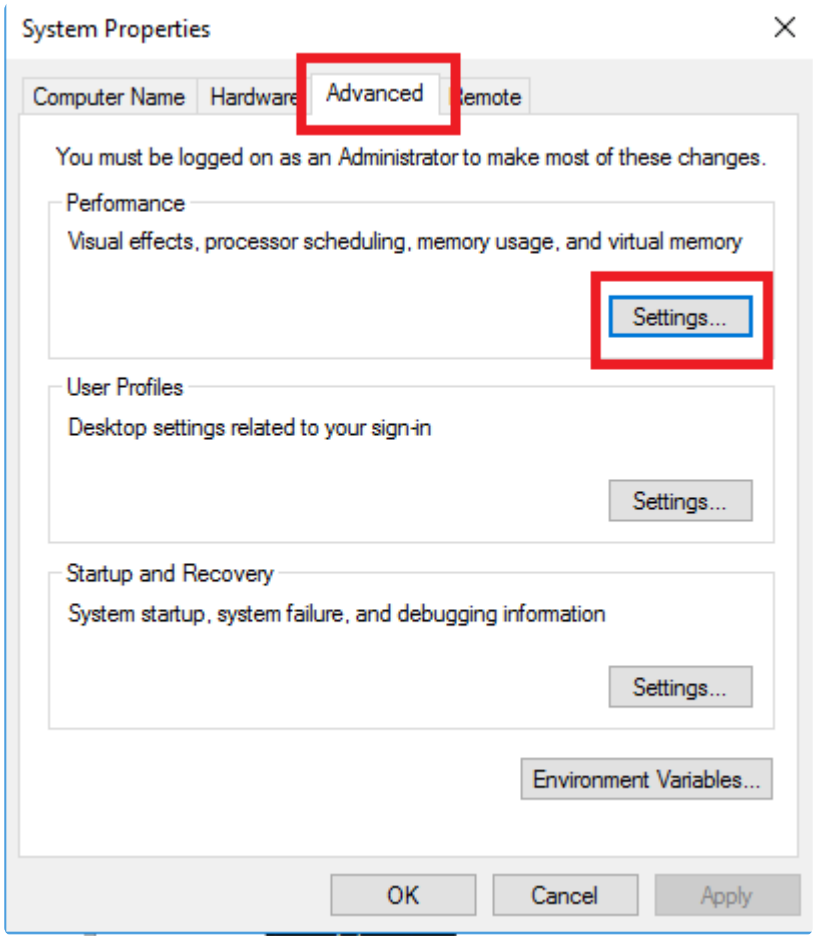
「すべてのドライブのページングファイルサイズを自動で管理する」を無効にする方法

この設定は、コントロールパネルの「システム」ダイアログにあります。

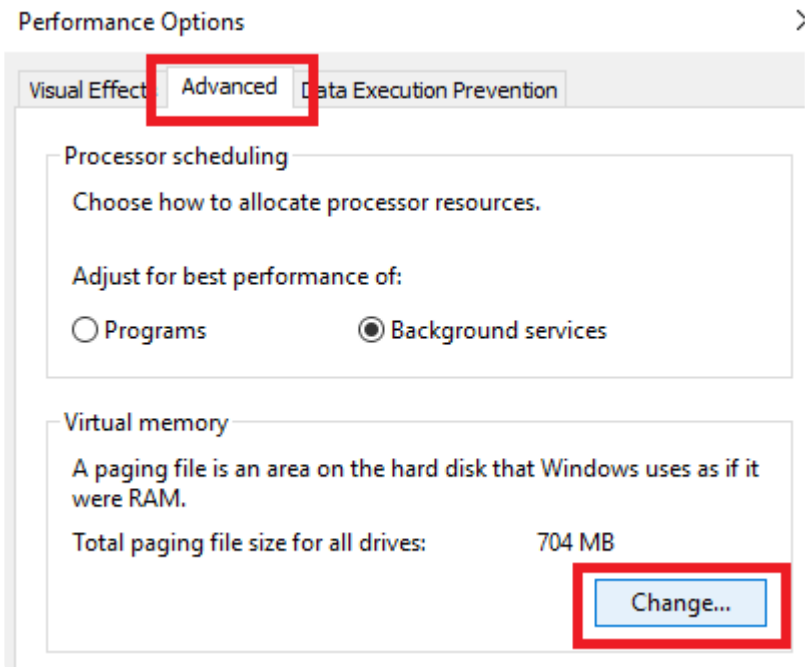
まず、**[詳細システム設定]** オプションをクリックします。



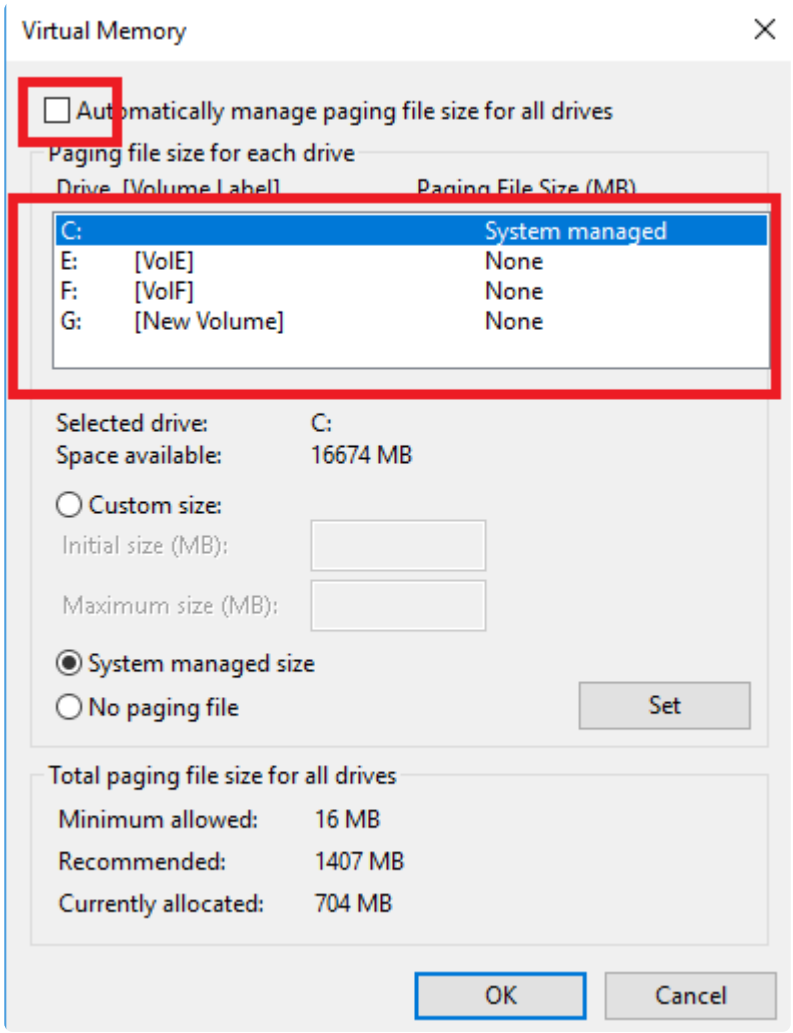
[システムのプロパティ] ダイアログで **[詳細設定]** タブを選択し、**[パフォーマンス]** セクションの **[設定]** ボタンをクリックします。



[パフォーマンスオプション] ダイアログボックスの **[詳細設定]** タブを選択し、[仮想メモリ] セクションの **[変更する...]** ボタンをクリックします。



[仮想メモリ] ダイアログで、「すべてのドライブのページングファイルサイズを自動で管理する」を **オフ** にします。その後、DataKeeper の保護下にあるボリュームにページファイルが設定されないようにページファイルを設定します。



注記: Windows 仮想メモリの構成を変更すると、システムのパフォーマンスに影響する可能性があります。これらの変更に関する推奨事項については、Microsoft のマニュアルを参照してください。

8.5.2.10. WAN に関する考慮事項

ソースサーバから遠く離れた場所にあるリモートサーバに対してネットワーク経由でデータを複製するのは、DataKeeper の最も一般的な使用方法です。一般的に、この構成は DataKeeper でデータをレプリケーションするためのネットワークとして提供される WAN の種類に依存します。WAN の帯域が制限されている場合は、以下のような考慮すべき事項がいくつかあります。

- LAN/WAN 間のデータの初期同期
- 圧縮
- ネットワーク帯域制限

8.5.2.10.1. LAN/WAN 間のデータの初期同期

WAN 接続で大量のデータを複製する場合は、ネットワーク帯域 と時間を大量に消費してしまう完全再同期を避けることを推奨します。DataKeeper はビットマップを使用して、ほぼすべての完全再同期を回避します。ただし、ミラーを最初に作成するときに行われるデータの初期同期を回避することはできません。

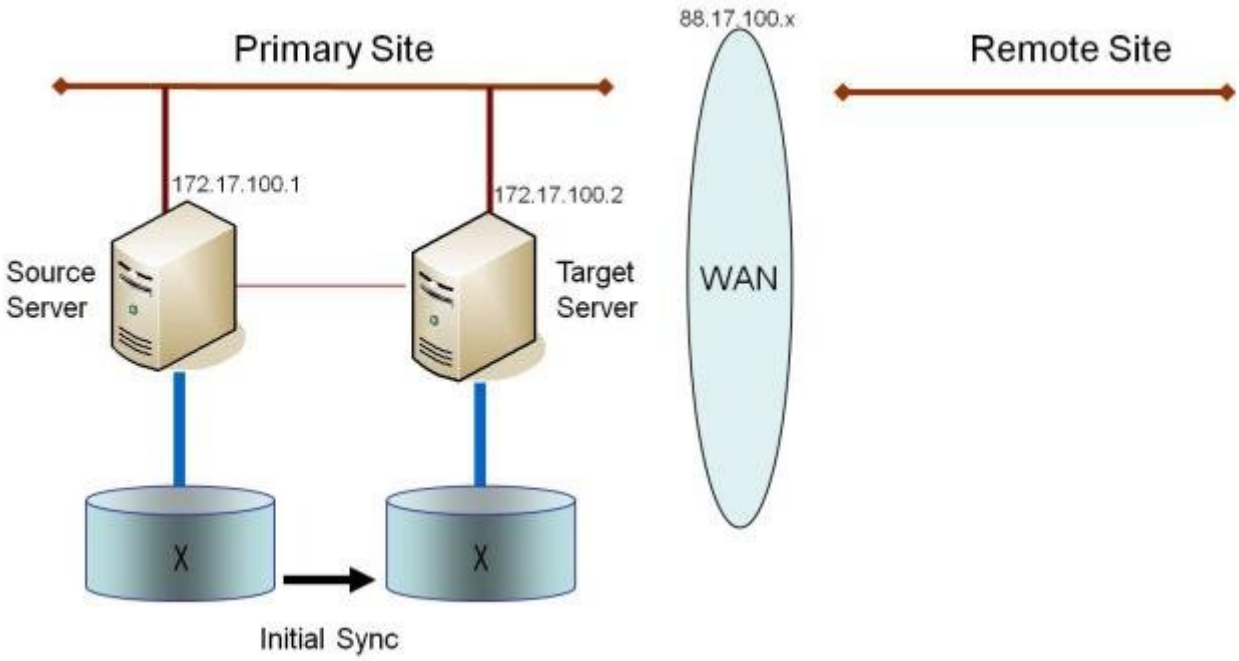
WAN 構成において WAN 間のデータの完全な初期同期を回避する方法の 1 つとして、両方のシステムを LAN 上に構成してミラーを作成し、完全な初期同期が LAN 上で実行されるようにする方法があります。初期同期が完了したら、ソースおよびターゲットの IP アドレスを更新してください。これによって、ミラーは*一時停止*状態になります。ターゲットシステムを新しい位置に移動してください。ターゲットシステムを本来の位置に移動したら、電源を入れて、更新された IP アドレスなどすべてのネットワーク設定を確認してください。ソースシステムで **CHANGEMIRRORENDPOINTS** コマンドを実行してください。ミラーが **再開** され、データの 部分再同期 (ミラーが **一時停止** されてからソースボリュームで生じた変更) を行うだけでターゲットボリュームをソースと同期させることができます。

> このコマンドは 3 ノード以下で構成されるミラーボリュームのエンドポイントの変更をサポートします。4 ノード以上の構成では、ローカルサイトで最終的なエンドポイントのミラーを作成し、route add を使用してミラーの作成と再同期を行ってから、サーバを最終的な位置 / アドレス /DR サイトに移動します。

例

以下の例では、プライマリサイトでローカルにミラーを作成してから、ターゲットをリモートサイトに移動します。ソースサーバには IP アドレス 172.17.100.1 が、ターゲットサーバには IP アドレス 172.17.100.2 が割り当てられています。WAN ネットワーク IP は 88.17.100.x です。

- DataKeeper UI を使用してボリューム X 上で 172.17.100.1 から 172.17.100.2 にミラーを作成します。*注記:* 後で新しい IP アドレスに変更したときに DNS の名前解決をさせるため、「名前」指定でターゲットに接続することを推奨します。



データの初期同期が完了したら、以下の操作を実行します。

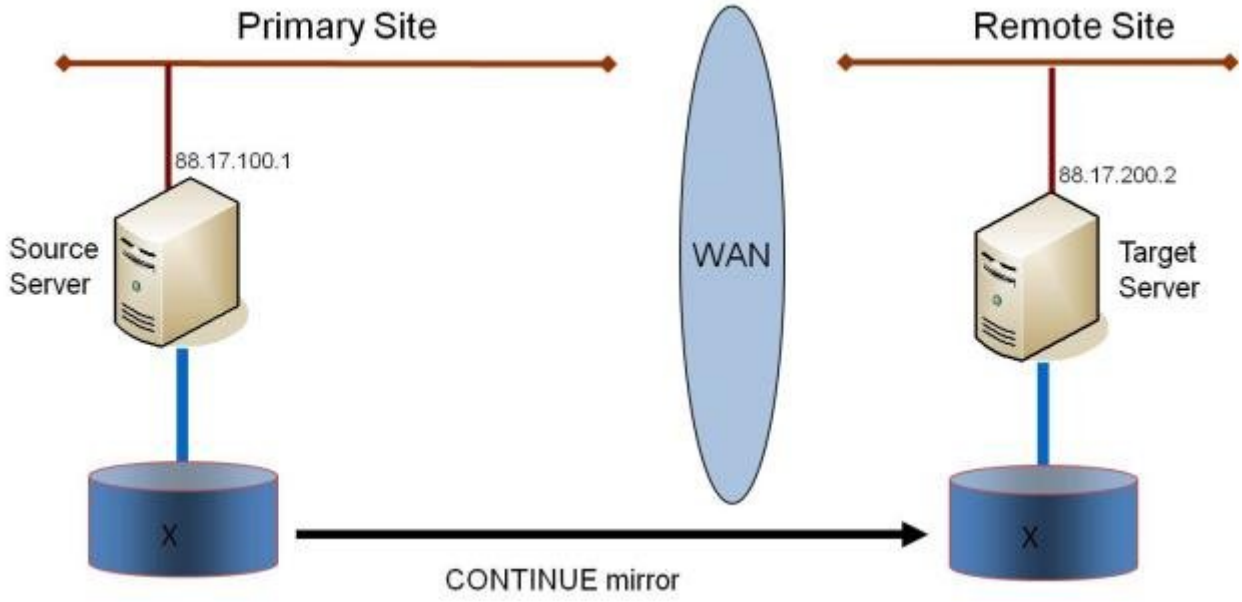
- ソースのネットワークアダプタの IP アドレスを 88.17.100.1 に更新し、ターゲットのネットワークアダプタの IP アドレスを 88.17.200.2 に更新します。これによって、ソース側のミラーが一時停止状態になります。
- ターゲットマシンを新しい位置に移動します。
- ターゲットマシンを起動し、上記で更新した IP アドレスを含むネットワーク設定を確認します。
- ソースシステムで DOS コマンドウィンドウを開き、以下のコマンドを実行してディレクトリを DataKeeper ディレクトリに変更します。

```
cd EXTMIRRBASE
```

- 以下のコマンドを実行して、既存のミラーエンドポイントを新しい IP アドレスに更新します。

```
EMCMD 172.17.100.1 CHANGEMIRRORENDPOINTS X 172.17.100.2 88.17.100.1
88.17.200.2
```

- DataKeeper によって、ターゲットサーバが接続されていないときにソースサーバで生じた変更の再同期が行われます。
- この部分再同期が完了すると、ミラーは*ミラーリング*状態になります。



ターゲットボリュームのデータの確認

設計上、DataKeeper はターゲットボリュームをロックします。これによって、複製中にターゲットボリュームに対する書き込みを防止します。ただし、DataKeeper では、ターゲットボリュームのロックを解除し、ミラーリング中の読み取り / 書き込み処理を可能にする機構が用意されています。これを行う方法は 2 通りあります。

1. DataKeeper UI でミラーの一時停止 / ロック解除 オプションを使用して、ミラーの一時停止とターゲットボリュームのロック解除を行ってください。

2. DataKeeper コマンドラインインターフェース (EMCMD) を使用して、ミラーの一時停止 (PAUSEMIRROR) およびターゲットボリュームのロック解除 (UNLOCKVOLUME) を行ってください。

ロック解除されると、ターゲットボリュームは完全にアクセス可能になります。ターゲットボリュームの検査が終了したら、必ずミラーを再開してターゲットボリュームを再度ロックし、ミラーを一時停止していた間にソースボリュームで生じた変更の再同期が行われるようにしてください。ロック解除中に行われたターゲットボリュームへの書き込みは、ミラーの再開時に失われます。

> ! ターゲットボリュームがロック解除されている間にターゲットシステム上で再起動が実行された場合、ターゲットシステムの復帰時に完全再同期が行われます。

8.5.2.10.2. 圧縮

DataKeeper では、ミラーごとに関連付けられる圧縮レベルをユーザが選択できます。圧縮を有効にすると、特に低速なネットワークにおいて、レプリケーションパフォーマンスを向上させることができます。システム、ネットワーク、および作業負荷に応じて、3 ～ 5 の圧縮レベルに設定することで CPU 利用率とネットワーク効率のバランスの改善が見込めます。

注記: ミラーの圧縮レベルはミラーを作成した後で変更できます。既存のミラーの圧縮レベルの変更 を参照してください。

8.5.2.10.3. ネットワーク帯域制限

DataKeeper は、使用可能なネットワーク帯域をすべて利用しようとします。DataKeeper が他のアプリケーションと帯域を共有している場合には、DataKeeper が使用できる帯域幅を制限することもできます。DataKeeper には、このための **ネットワーク帯域制限** という機能が搭載されています。この機能はレジストリ設定を用いて有効にします。

注記: **圧縮** および **ネットワーク帯域制限** の詳細については、以下のトピックを参照してください。

- レジストリエントリ
- 既存のミラーの圧縮レベルの変更

8.5.3. 管理

このセクションでは、DataKeeper の管理作業を行うための詳細な手順について説明します。

DataKeeper イベントログ通知

プライマリサーバのシャットダウン

セカンダリサーバの障害

大量書き込みの考慮事項

CHKDSK の考慮事項

DKHEALTHCHECK

DKSUPPORT

イベントログの考慮事項

ディスク管理の使用

レジストリエントリ

SIOS DataKeeper で EMCMD を使用する

SIOS DataKeeperでDKPwrShellを使用する

8.5.3.1. DataKeeper のイベントログ通知

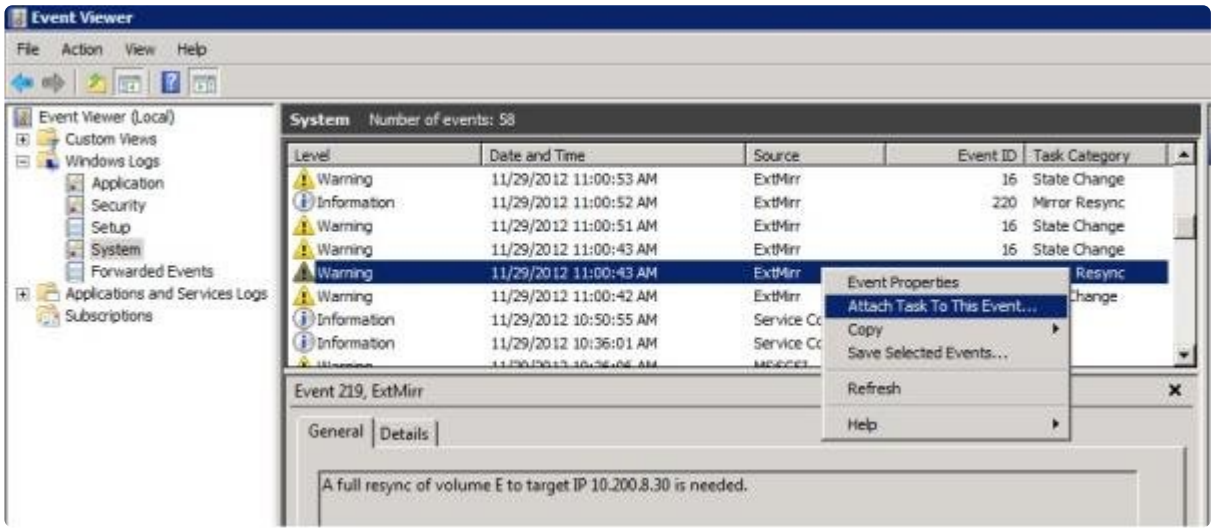
イベントログ通知 とは、特定のイベントが発生したときに 1 人以上のユーザが E メールを受信できる仕組みです。記録された特定の DataKeeper イベントを通知するように、**Windows のイベントログ** を設定できます。

> このオプションは、**Windows Server 2008 R2** でのみ使用できます。

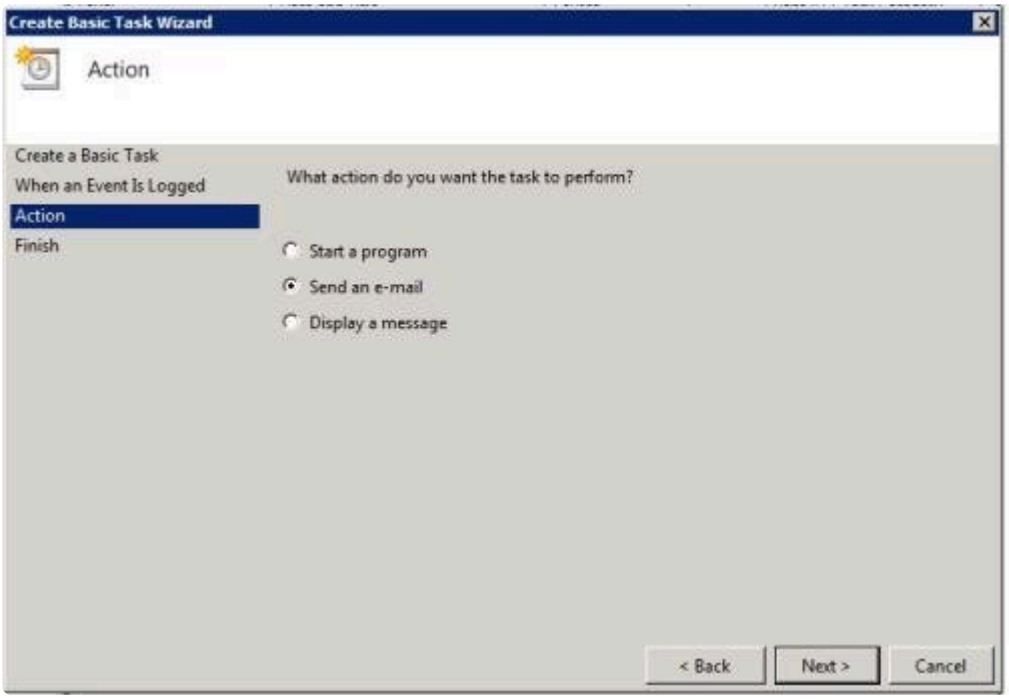
DataKeeper のイベントについて **Windows のイベントログの E メール送信タスク** を設定するには、以下の手順を実行してください。

1. **[イベント ビューアー]** を開き、**[システム]** または **[アプリケーション]** のログに移動して、通知するイベントを選択してください。

2. イベントを右クリックし、**[タスクをこのイベントに添付]** を選択してください。



3. **タスク ウィザード** の指示に従い、プロンプトが表示されたら **[電子メールを送信する]** オプションを選択し、必要な情報を入力します。



4. **タスク ウィザード** の最後に **[完了]** をクリックすると、新規タスクが作成され、Windows のスケジュールに追加されます。

これらの E メールは、E メール通知を生成する各ノードについて設定する必要があります。

8.5.3.2. プライマリサーバのシャットダウン

ソースサーバが正常にシャットダウンすると、ターゲットへの保留中のすべての書き込みが完了します。これにより、ターゲットシステムにデータが存在していることが保証されます。

ソースサーバに予期しない障害が発生した場合でも、インテントログ の機能により、ソースサーバの復旧後に完全再同期を行わなくてすみます。インテントログ機能が無効になっている場合、またはボリュームのインテントログファイルへのアクセス障害が SIOS DataKeeper によって検出された場合には、ソースサーバがサービスを開始できるようになった後に完全再同期が実行されます。

8.5.3.3. セカンダリサーバの障害

セカンダリ (ターゲット) システムに影響を及ぼす障害が発生した場合は、影響を受けたミラーの状態は **一時停止** になります。セカンダリサーバの障害の原因となった状況を解消して、ボリュームを再同期する必要があります。セカンダリサーバに障害が発生した後は、ターゲットに対する書き込みは一切行われません。

障害発生後、セカンダリサーバがオンライン状態に戻ると、ミラーのソース側が自動的にターゲット側に再接続します。続いて、部分再同期が実行されます。

8.5.3.4. 大量書き込みに対する考慮事項

SIOS DataKeeper では、同期中のボリュームにアクセスして書き込むことができます。再同期中、DataKeeper はビットマップを複数回パスし、検出された各ダーティビットに対応するデータを同期します。これが行われている間、ボリューム上で発生する書き込みは、すでに同期されているブロックをダーティにする可能性があります。特定の条件下では、ソースボリュームに対する書き込み処理が頻繁に行われるため、再同期が完了しないことがあります。

ソースボリュームで書き込みが行われている間に再同期を完了させるために、DataKeeper は最後のダーティブロックが同期できるよう書き込みを一時的に遅らせる場合があります。ResyncLowWater レジストリの値は、DataKeeper が書き込みを遅らせるためにビットマップに存在できるダーティブロックの最大数を指定します。ResyncBlockWritesTimeoutMs レジストリの値は、書き込みが遅れる最大時間（単位：ミリ秒）を指定します。

DataKeeper は、再同期が複数の再同期パスを試行するまで（具体的には、MaxResyncPasses レジストリの値で指定された値の10%）、書き込みを遅らせません。たとえば、MaxResyncPasses がデフォルトの200に設定されている場合、21番目がビットマップをパスするまで DataKeeper は書き込みを遅らせず、ダーティブロックの数が ResyncLowWater 以下の場合にのみ書き込みを遅らせます。

書き込みが遅延しても ResyncBlockWritesTimeoutMs で指定された時間内に再同期が完了しない場合、再同期は失敗し、書き込みが完了できるようになります。また、ミラーは一時停止状態になります。

書き込みの遅延を完全に無効にするには、ResyncLowWater を 0 に設定してください。

8.5.3.5. CHKDSK に関する考慮事項

SIOS DataKeeper でミラーするボリュームで CHKDSK を実行しなければならない場合は、最初にミラーを **一時停止** することをお勧めします。**CHKDSK** を実行した後、ミラーを **再開** してください。部分再同期が実行され (CHKDSK による書き込みがアップデートされます)、ミラーが再開します。

一時停止 に失敗した場合、ミラーは自動的に **一時停止** 状態になり、CHKDSK の実行時に **再同期** が実行される場合があります。これによって明らかな問題が発生しない場合でも、CHKDSK が遅延し、SIOS DataKeeper に不必要な状態の変化が生じてしまいます。

SIOS DataKeeper では、ミラーを構成するボリューム (ソース、ターゲットのどちらであっても) がシステム起動時に自動的にチェックされないように自動的に確認されます。この機能によって、ミラーボリューム上のデータは常に一貫した状態に保たれます。

注記: ビットマップファイル (非共有ボリューム用) は、BitmapBaseDir により定義されるデフォルトの保存場所の C ドライブに配置されます。**ソース** システムの C ドライブ　で CHKDSK を実行するとアクティブなビットマップファイルが原因でエラーが発生します。スイッチオーバを実行してソースをターゲットにし、ビットマップファイルをインアクティブにしてください。その後、そのシステムを新しいターゲット(旧ソース)として CHKDSK を実行することが可能です。

8.5.3.6. CLEANUPMIRROR

C:\Program Files (x86)\SIOS\DataKeeper\Support>cleanupmirror <volume_letter>

このコマンドはノード上でローカルでのみ実行でき、残っているすべてのミラーを削除します。

用途：

- WSFCまたはDataKeeper GUIから削除されなかったミラーを削除する
- ミラーが再作成された際に（emcmd、createmirrorコマンド）、WSFCに影響を与えずに残りのミラーの残りを削除する

パラメーターは以下の通りです。

<root>\Program Files (x86)\SIOS\DataKeeper\Support>	The location of the \DataKeeper\Support Directory
<volume_letter>	Mirror volume letter. Valid values: A – Z

- Administrator コマンドプロンプトを起動します。
- `cd %extmirrbase%` と入力します。
- DataKeeper ディレクトリまたは c:\Program Files (x86) \SIOS\DataKeeper に移動しました。
- 移動したディレクトリで、`cd support` と入力します。
- サポートディレクトリ内から、以下のコマンドを実行します。
  `cleanupmirror <volume_letter>`
- DataKeeper ミラーリングの対象になっているすべてのシステムで、このコマンドを実行します。

8.5.3.7. DKSUPPORT

DKSUPPORT .cmd は *<DataKeeper Installation Path>\SUPPORT* ディレクトリにあり、重要な設定情報ファイルとイベントログファイルを収集して zip ファイルに圧縮するために使用されます。サポートプロセスの一環として、SIOS のサポートエンジニアが通常、この zip ファイルを必要とします。このユーティリティを実行するには、エクスプローラのウィンドウに表示された DKSUPPORT ファイルをダブルクリックするか、DataKeeper Notification アイコン を右クリックして Gather Support Logs をクリックします。

このユーティリティは、以下の手順を使用したコマンドプロンプトからも実行できます。

- コマンドプロンプトを開きます。
- 「 *cd %extmirrbase%* 」と入力します。
- DataKeeper のディレクトリ (または c:\Program Files (x86) \SIOS\DataKeeper) に移動します。
- 移動先のディレクトリで、「 *cd support* 」と入力します。
- support ディレクトリで、「 *dksupport.cmd* 」コマンドを実行します。
- DataKeeper のミラーリングに使用されているすべてのシステムでこのコマンドを実行します。

support ディレクトリに zip ファイルが作成されます。この zip ファイルは、電子メールで support@us.sios.com に送付することも、ファイル転送 (FTP) でサポートエンジニアリングに送信することもできます。

注記: このコマンドの実行が完了するまで時間がかかることがあります。

8.5.3.8. DKHEALTHCHECK

DKHealthCheck.exe は <DataKeeper のインストールパス>\DKTools ディレクトリにあり、基本的なミラーの状態を表示し、ミラーの問題検出を行うツールです。SIOS のサポートでは、サポートプロセスの一環として、このツールを実行するよう要求する場合があります。

注記: DKHEALTHCHECK の出力はDKSupport で自動的にキャプチャされるため、DKSupport をすでに実行している場合は、個別に実行する必要はありません。

このツールは、DataKeeper Notification Icon を右クリックし、[Launch Health Check] をクリックするか、下記の手順を実行します。

コマンドプロンプトを開きます。

「`cd %extmirrbase%`」と入力します。

DataKeeper のディレクトリ (または c:\Program Files (x86) \SIOS\DataKeeper) に移動します。

上述のディレクトリで「`cd DKTools`」と入力します。

DKTools ディレクトリ内で、以下の「`DKHealthCheck.exe`」コマンドを実行します。

ツールの結果をコマンドプロンプトからコピーおよび貼り付けて、電子メールで **support@us.sios.com** に送付することができます。

または、DKTools ディレクトリ内で下記のコマンドを実行して、ファイルに出力するように指定することもできます。

- `DKHealthCheck.exe > HealthCheck.txt`

このファイルを電子メールに添付して送付することができます。

注記: このコマンドの実行が完了するまで時間がかかることがあります。

8.5.3.9. イベントログの考慮事項

SIOS DataKeeper の動作ログはイベントログに対して書き込みが可能な状態であることが重要です。イベントログがいっぱいにならないように注意する必要があります。次の手順に従って、必要に応じてイベントを上書きするようにイベントログを設定するのも 1 つの方法です。

1. **[イベントログ]** を開きます。
2. **[システムログ]** の上で右クリックし、**[プロパティ]** を選択します。
3. **[最大ログサイズ]** の下にある **[必要に応じてイベントを上書きする]** を選択します。

8.5.3.10. ディスク管理の使用

Windows のディスクの管理ユーティリティを使用して SIOS DataKeeper ボリュームにアクセスする場合は、次の点に注意してください。

- ディスクの管理を使用してミラー中のパーティションを削除することはサポートされていません。SIOS DataKeeper のミラーに使用されているパーティションを削除すると、予期せぬ事態を招くことがあります。
- SIOS DataKeeper のミラーに使用されているパーティションに割り当てられたドライブレターをディスクの管理ユーティリティを使用して変更する方法はサポートされておらず、使用すれば予期せぬ事態を招くことがあります。
- Windows のディスクの管理ユーティリティは、ドライブ数に応じてターゲットノードでの起動時に時間がかかります。Windows オペレーティングシステムにはエラー条件時の再試行が組み込まれているので、ボリュームがロックされている場合、「ロックされている」ターゲットノードで起動するときの処理速度が影響を受けます。

8.5.3.11. レジストリエントリ

以下のレジストリは SIOS DataKeeper サービスまたはドライバに関連があり、Regedt32 を使用して参照および編集することができます。

ここに記載されているもの以外、DataKeeper のレジストリキーの値を変更しないでください。

修正可能なレジストリエントリ

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters

SIOS DataKeeper ドライバは以下のパラメータキーを使用します。パラメータキー内 (* で示す) の値はシステムのすべてのボリュームに対してグローバルな値です。各ターゲット IP のレジストリキー († で示す) の下の値はミラーのみに特有です。* および † で示される値は両方のキーの下に表示されます。(この場合、ターゲット特有の値が優先されます)

BandwidthThrottle †

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\BandwidthThrottle***		
名前	タイプ	デフォルトデータ
BandwidthThrottle	REG_DWORD	0
ミラーに使用するネットワーク帯域幅の最大値 (単位 Kb/s)を指定してください。0 は [制限なし] という意味です。		

BitmapBaseDir *

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\BitmapBaseDir***		
名前	タイプ	デフォルトデータ
BitmapBaseDir	REG_SZ	*C:\%EXTMIRRBASE%\Bitmaps* (通常は *C:|Program Files\SIOS\DataKeeper\Bitmaps* ですが、システムをアップグレードした場合、または SIOS DataKeeper を別のパスにインストールした場合は異なります)。
SIOS DataKeeper がインテントログを保存するディレクトリを指定してください。(注記: ドライブレターは大文字である必要があります。) 空の文字列のディレクトリ設定はインテントログを無効にします。**インテントログの機能を無効にするには、それらの各システムで設定が反映されるように再起動する必要があります。**		

BitmapBytesPerBlock * †

場所: 新しいミラーに対して:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\BitmapBytesPerBlock

既存のミラーに対して:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\BitmapBytesPerBlock

注:Parametersでこの編集する場合、すべての新規作成のミラーはこの値を引き継ぎますが、{Target IP}でこの編集を行った場合には、値はそのTargetのみに反映されます。また、**{Target IP}において設定された値は、Parameter で設定された値に優先します。**

名前	タイプ	デフォルトデータ
BitmapBytesPerBlock	REG_DWORD	65536 (0×10000)

書き込み要求が発生した際に DataKeeper Intent Log のビットマップにダーティーとして表されるバイト数を指定します。ビットマップ内の単一のビットは65536バイトを表し、BitmapBytesPerBlock は、複数のビットとして表される有効なブロックサイズを表します。この値を増やすことで、シーケンシャル書き込みや比較的レイテンシの大きなBitmapストレージでの動作など、特定の状況においてレプリケーションのパフォーマンスを改善することが可能です。65,536バイト以下ブロックのシーケンシャル書き込みでは、より大きなブロックサイズはビットマップファイルへの書き込み回数の減少を意味します。より大きなブロックサイズを指定することは、もっぱらランダムな書き込みが行われる環境や、低レイテンシの高速なシステム上では顕著なパフォーマンスの改善にはつながりません。また、より大きなブロックサイズはシステム障害時における再同期時にデータ量の増大につながる場合もあります。

注: BitmapBytesPerBlockの最低値は65,536であり、これより低い数値は65,536として扱われます。最大値には制限はありません。

注: BitmapBytesPerBlock はミラー再同期の速度には影響しません。

BlockWritesOnLimitReached * †

場所:

新しいミラーに対して:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\BlockWritesOnLimitReached

既存のミラーに対して:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters

Volumes\{Volume GUID}\Targets\{Target IP}\BlockWritesOnLimitReached

注: **Parameters** の下のこのエントリを編集する場合、作成されたすべての新しいミラーはこの値を継承します。**{Target IP}** の下のこのエントリを編集する場合、値はそのターゲットにのみ関係します。**すべての {Target IP} の値は、グローバルパラメータ値を上書きします。**

名前	タイプ	デフォルトデータ
BlockWritesOnLimitReached	REG_DWORD	0

この値は、ミラーの書き込みキューが定義された上限値に達した場合（WriteQueueHighWater または WriteQueueByteLimit に達した場合）のミラーの動作を決定します。BlockWritesOnLimitReached が「0」の場合、ミラーは一時停止され、少し後に部分再同期が開始されます。BlockWritesOnLimitReached が「1」の場合、書き込みキューに空きができるまで、書き込みは遅延します。ミラーはミラーリング状態のままですが、ネットワークの速度とリモートノードのボリュームに応じてアプリケーションのスループットが低下します。このレジストリ値を更新した後、DataKeeper が直ちに新しい値の使用を開始できるように、READREGISTRY コマンドを実行してください。

BlockWritesOnNDLGTimeoutReached *

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\BlockWritesOnNDLGTimeoutReached***

名前	タイプ	デフォルトデータ
BlockWritesOnNDLGTimeoutReached	REG_DWORD	1

この値は、同期ミラーのクラスター TargetState 値を設定するときに DataKeeper がタイムアウトを処理する方法を決定します。データの損失を回避するために、DataKeeper は通常、そのようなタイムアウトを検出するとボリュームをロックし、未処理の書き込みを失敗させます。これは、この値が「1」に設定されている場合のデフォルトの動作です。

ボリュームがロックされ、書き込みが失敗するのを防ぐには、この値を「0」に設定します。変更した設定を有効にするには、ノードを再起動する必要があります。

注記: この値を「0」に設定するとアプリケーションデータが失われる可能性があるため、これは推奨しません。

CompressionLevel †

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\CompressionLevel***

名前	タイプ	デフォルトデータ

CompressionLevel	REG_DWORD	0
指定したミラーに対する圧縮レベルを指定してください。有効値は 0 ～ 9 です。レベル 0 は「圧縮なし」です。1 ～ 9 の値は、圧縮の CPU の集中レベルを増分的に指定します。圧縮レベル 1 は高速圧縮です。データを圧縮する CPU 時間は最短ですが、パケットサイズが最大になります。レベル 9 は圧縮時間が最長ですが、圧縮率は最大になります。つまり、CPU 時間は長くなりますが、パケットサイズは最小になります。お使いのシステム、ネットワーク、および作業負荷に応じて、CPU 利用率とネットワーク効率の均衡を取るように適切なレベルに調節することができます。		

DontFlushAsyncQueue *

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\DontFlushAsyncQueue***		
名前	タイプ	デフォルトデータ
DontFlushAsyncQueue	REG_SZ	空 <drive letter> [<drive letter>]
ドライバがフラッシュ要求を受けた場合に、非同期キューをフラッシュしないボリュームを指定することができます。この値は適用されるボリュームのドライブレターを含みます。ドライブレターは続けて入力するか (XY) またはスペースで区切って (X Y) 入力してください。コロンは不要です。このレジストリ値を更新した後、DataKeeper が新しい値を使用してすぐに起動できるように READREGISTRY コマンドを実行してください。**(注記: DontFlushAsyncQueue を設定する場合は、データとデータベースログを同じパーティションに配置してください)**		

MaxResyncPasses *

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\MaxResyncPasses***		
名前	タイプ	デフォルトデータ
MaxResyncPasses	REG_DWORD	200 (0xc8)
SIOS DataKeeperが再同期プロセスを一時的に中断する前に、ソースボリュームに一定の書き込み処理がある間に再同期の最大パス数を指定してください。この中断後、通常は60秒後に再同期が自動的に再開されます。すべてのパスで、SIOS DataKeeperはパスの途中で書き込まれたボリュームブロックをマークします。次のパスでは、マークされたブロックのみをターゲットに送信します。 注：設定されたすべての変更の反映には、システムの再起動が必要となります。		

NotificationIconUpdateStatus *

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\NotificationIconUpdateStatus***		
名前	タイプ	デフォルトデータ
NotificationIconUpdateStatus	REG_SZ	**true**
マシン上の DataKeeper 通知アイコンのすべてのインスタンスによって実行されるステータス更新チェックを無効にすることができます。この値には、**True** または **False** のいずれかを設定する必要があります。コンテキストメニューから通知アイコンを無効にすると、このエントリーは **False** に設定されます。		

PingInterval *

場所: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\PingInterval*		
名前	タイプ	デフォルトデータ
PingInterval	REG_DWORD	3000 (0xBB8)
ping 間の発行間隔をミリ秒で指定してください。WAN 接続または信頼性の低いネットワークに対しては、高い値を設定してください。**MaxPingMisses** の値とともに発行間隔をカスタマイズすることでミラーリングのパフォーマンスを調整することが可能です。		

ResyncBlockWritesTimeoutMs * †

場所:

新しいミラーの場合:

および

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\ResyncBlockWritesTimeoutMs

既存のミラーの場合:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\ResyncBlockWritesTimeoutMs

注記 : パラメータ の下にあるこのエントリを編集する場合、作成されたすべての新しいミラーはこの値を継承します。**{Target IP}** の下にあるこのエントリを編集する場合、値はそのターゲットにのみ関連します。**すべての {Target IP}の値は、グローバルパラメータの値を上書きします。**

名前	タイプ	デフォルトデータ
ResyncBlockWritesTimeoutMs	REG_DWORD	15000 (0×3a98)
再同期中に DataKeeper が書き込みを遅らせる最大時間を指定します。詳細については、大量書き込みに対する考慮事項 のトピックを参照してください。		

ResyncLowWater * †

場所:

新しいミラーの場合:

および

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\ResyncLowWater

既存のミラーの場合：

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\ResyncLowWater

注記：パラメータ の下にあるこのエントリを編集する場合、作成されたすべての新しいミラーはこの値を継承します。**{Target IP}** の下にあるこのエントリを編集する場合、値はそのターゲットにのみ関連します。**すべての {Target IP}の値は、グローバルパラメータの値を上書きします。**

名前	タイプ	デフォルトデータ
ResyncLowWater	REG_DWORD	150 (0×96)

再同期中に DataKeeper が書き込みを遅らせるダーティーブロックの最大数を指定します。詳細については、大量書き込みに対する考慮事項 のトピックを参照してください。

ResyncReads *

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\ResyncReads***

名前	タイプ	デフォルトデータ
Resync Reads	REG_DWORD	20 (0×14)

この値は、ミラー再同期の間、読み込んでターゲットシステムに送信するために処理中にできる最大ディスクブロック数を表します。この値を変更するとミラーの再同期速度が変更されます。

注記: この値の調整は、同期および非同期のミラーに適用することができます。

SnapshotLocation †

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\SnapshotLocation***

名前	タイプ	デフォルトデータ
SnapshotLocation	REG_SZ	<drive letter>

このボリュームのターゲットスナップショットファイルを格納するフォルダを指定します。

TargetDispatchPort *

場所

ターゲットシステム:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\TargetDispatchPort

上記ターゲットにミラーを作成するソースシステム:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Targets{Target IP}（つまり、ターゲットシステムのIPアドレスを名前とするキーを作成するか、すでに存在する場合はそのキーの**TargetDispatchPort**の値を更新します。）

名前	タイプ	デフォルトデータ
TargetDispatchPort	REG_DWORD	9999

ディスパッチポートを 9999 から変更する場合は、TargetDispatchPort を設定すべき箇所が 2 か所あります。ターゲットシステムでは、*ExtMirr\Parameters* キー内に配置してください。新しい設定は、サーバのすべての既存および新規ターゲットに対して適用されます。**変更したパラメータキーの設定を反映させるには、ターゲットの再起動が必要です。**このターゲットへのミラーを作成するソースシステムで、ミラーがすでに存在する場合は、*ExtMirr\Parameters\Targets\{Target IP}* キーに配置します。そのキーがまだ存在しない場合は作成してください。

注記: ソースとターゲットの両方で、ポートを同じにしてください。

新しいディスパッチポートを動作させるためにはすべてのソースおよびターゲットサーバ上でファイアウォールを開放する必要があります。

TargetPortBase *

場所: ***HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\TargetPortBase***

名前	タイプ	デフォルトデータ
TargetPortBase	REG_DWORD	10000

ターゲットボリュームへの接続に対するベースの TCP ポート番号を指定してください。この番号はデフォルトのポートが他のサービスで使用されている場合、またはファイアウォールでブロックされている場合に調整する必要があることもあります。ターゲットが使用する実際のポートは次のように計算されます。

ポート = **TargetPortBase** + (ボリュームレター - A:)

以下に例を示します。

TargetPortBase = 10000

ボリュームレター = H

ポート = 10000 + (H:-A:)= 10007

TargetPortIncr *

場所: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\TargetPortIncr*		
名前	タイプ	デフォルトデータ
TargetPortIncr	REG_DWORD	256
ベースの TCP ポート番号の増分を指定してください。これは、TCP ポートが使用されている場合にのみ使用されます。例えば、ターゲットがポート 10005 を使用しようとしたがこのポートが使用中だった場合、ポート 10005 + **TargetPortIncr** を使用して処理が再試行されます。		

TargetSnapshotBlocksize *

場所: *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\TargetSnapshotBlocksize*		
名前	タイプ	デフォルトデータ
TargetSnapshotBlocksize	REG_DWORD	なし

DataKeeper のターゲットスナップショットは、スナップショットファイルに書き込むすべてのエントリについて、デフォルトのブロックサイズ 64KB を使用します。このブロックサイズを変更するには、TargetSnapshotBlocksize レジストリキーを作成します。

この値は必ず、ディスクセクタサイズ (通常は 512 バイト) の倍数にする必要があります。特定の作業負荷と書き込みパターンについて、ブロックサイズ変更のメリットがあります。たとえば、データの順次ストリームで書き込むボリューム (SQL Server のログファイルなど) では、大きいブロックサイズが効果的です。ブロックサイズを大きくすると、連続するブロックを書き込むときにターゲットの読み取り回数が少なくなります。ただし、ランダムなパターンで書き込まれるボリュームでは、小さい値、またはデフォルトの 64KB が効果的です。ブロックサイズを小さくすると、ランダム書き込み要求でのスナップショットファイルの使用量が少なくなります。

VssQuiesceWaitTimeoutMs *

場所

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\VssQuiesceWaitTimeoutMs

名前	タイプ	デフォルトデータ
VssQuiesceWaitTimeoutMs	REG_DWORD	60000
DataKeeper のサービスが VSS スナップショットソースの開始要求を完了するまでの待機時間（ミリ秒単位）を指定します。VSS スナップショットソースの開始要求は、VSS を使用してスナップショットボリュームのデータを静止させます。		

WriteQueueByteLimitMB †

場所

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\WriteQueueByteLimitMB

名前	タイプ	デフォルトデータ
WriteQueueByteLimitMB	REG_DWORD	0

このミラーの書き込みキューに割り当てることができる最大バイト数を指定します（メガバイト単位 - 1048576バイトの倍数）。値「0」は「制限なし」を意味します。大量のディスク書き込み処理の間、このミラーの書き込みキューが WriteQueueByteLimitMB に達するレベルまで増加すると、SIOS DataKeeper ドライバーはミラーを一時停止してキューを排出し、自動的に部分再同期を開始します。このレジストリ値を更新した後、DataKeeper が新しい値を使用してすぐに起動できるように READREGISTRY コマンドを実行してください。

この値は、ミラーが再同期状態にある場合だけでなくミラーがミラーリング状態にある場合にも、ボリュームデータをターゲットに送信する間使用されます。再同期中に書き込みキューに置くことのできる64KB（65536バイト）ブロックの数を指定する ResyncReads の値（下記参照）が、WriteQueueByteLimitMB で指定した上限を超えないようにする必要があります。WriteQueueByteLimitMB が0に設定されていない場合、ResyncReads に65536を乗じて1048576で割った値はWriteQueueByteLimitMB を超えてはなりません。

この値は、WriteQueueHighWater（下記参照）と組み合わせて使用できます。両方の値の上限が0以外の値に設定されている場合、いずれかの上限に達するとミラーは一時停止されます。一方が0に設定されて他方が0以外の値に設定されている場合、0ではないほうの値が優先されます（書き込みキューによる非ページメモリの使用は推奨しません）。

注記：この調整パラメーターは、同期ミラーと非同期ミラーに適用されます。SIOS DataKeeper パフォーマンスモニタカウンタ、特に [キューの現在のバイト数] を使用してミラーリングの動作を監視し、それに応じてこの制限を設定できます。

WriteQueueHighWater * †

場所

新規ミラーの場合:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\WriteQueueHighWater

および

既存ミラーの場合:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ExtMirr\Parameters\Volumes\{Volume GUID}\Targets\{Target IP}\WriteQueueHighWater

注記 : このエントリの **Parameters** を編集した場合、新規に作成されたミラーは全てこの値を継承します。このエントリの **Target** を編集した場合、その値は作成された 1 つのターゲットにのみ適用されます。**Target の値は Parameter の値よりも優先されます。**

名前	タイプ	デフォルトデータ
WriteQueueHighWater	REG_DWORD	20000 (0×4e20)

このミラーの書き込みキューに格納できる書き込み要求の最大数（バイト数ではありません）を指定してください。値「0」は「制限なし」を意味します。大量のディスク書き込み処理の間にこのミラーの書き込みキューの長さがこの値に達した場合、SIOS DataKeeper ドライバーは一時的にミラーを停止して、キューを排出し、自動的に部分再同期を開始します。この値は、バイト数ではなく、キュー内の書き込み要求の数を表します。このレジストリ値を更新した後、DataKeeper が新しい値を使用してすぐに起動できるように READREGISTRY コマンドを実行してください。

この値は、ミラーが再同期状態にある場合だけでなくミラーがミラーリング状態にある場合にも、ボリュームデータをターゲットに送信する間使用されます。ResyncReads の値（下記参照）は再同期中に書き込みキューに置くことができるブロック数を指定し、WriteQueueHighWater が0に設定されていない場合、WriteQueueHighWater で指定された上限を超えないようにする必要があります。

この値は、WriteQueueByteLimitMB と組み合わせて使用できます。両方の上限が0以外の値に設定されている場合、いずれかの上限に達するとミラーは一時停止されます。一方が0に設定されて他方が0以外の値に設定されている場合、0ではないほうの値が優先されます。両方とも0に設定されている場合、ミラーの書き込みキューは一切制限されません（この設定は推奨しません。WriteQueue は Nonpaged メモリを使用します）。

注記: この値の調整は、同期および非同期のミラーに適用されます。この値はシステムで使用可能なメモリに依存します。SIOS DataKeeper パフォーマンスモニタカウンタを使用してミラーリング処理を監視すると、この値を適切に設定することができます。

8.5.3.12. SIOS DataKeeper で EMCMD を使用する

SIOS DataKeeper に付属の EMCMD ユーティリティは、コマンドラインでのミラー操作方法を提供します。スクリプトは「通常の」確認ルールが適用できない状況で実行されるため、EMCMD は SIOS DataKeeper ユーザインターフェースを使用して実行されるものと同種の正常チェックを実行しません。EMCMD は、SIOS DataKeeper レプリケーションサービスにコマンドを渡すだけで、サービスは任意の決定を下すことができます。DataKeeper ユーザインターフェースを使用した場合に行われるようなチェックがないことによって、EMCMD は便利な診断およびサポートツールになります。ただし、SIOS DataKeeper の内部構造に詳しくないユーザにとっては、潜在的に危険です。

以下のセクションでは、EMCMD SIOS DataKeeper コマンドラインの操作について詳しく説明します。

- Administrator コマンドプロンプトを起動します。
- `cd %extmirrbase%` と入力します。
- DataKeeper ディレクトリまたは c:\Program Files (x86) \SIOS\DataKeeper に移動しました。

注記: 以下の表現規則を使用します。

<system>	システムの NetBIOS 名、IP アドレス、または完全修飾ドメイン名を使用して、指定のシステムに接続してください。emcmd を実行しているローカルシステムは、ピリオド (.) で表すこともできます。
<drive>	参照されているドライブレターを指します。EMCMD は 1 文字目の後はすべて解析するので、「:」(コロン) は無効です。

場合によっては、一連の EMCMD コマンドを実行して機能を実行する必要があります。

例: 削除されたミラーをクリーンアップするには、各クラスタノードで次の3つのコマンドを実行する必要があります。

- emcmd . `deletelocalmirroronly` <クリーンアップするミラーのボリュームレター>
- emcmd . `clearswitchover` <クリーンアップするミラーのボリュームレター>
- emcmd . `updatevolumeinfo` <クリーンアップするミラーのボリュームレター>

次に、emcmd createmirror コマンドを使用してミラーを再作成します (例: emcmd <ミラーのソースのアドレス> createmirror <ボリュームレター> <ミラーのターゲットのアドレス> <ミラーのタイプ（同期の場合はS、非同期の場合はA）>。このコマンドでミラーを再作成し、既存のDataKeeperジョブに接続します。

注記: これらのコマンドは注意して実行してください。ご質問がある場合は、弊社サポート support@us.sios.com までお問い合わせください。

ミラー状態の定義

BREAKMIRROR

CHANGEMIRRORENDPOINTS

CHANGEMIRRORTYPE

CLEARBLOCKTARGET

CLEARSNAPSHOTLOCATION

CLEARSWITCHOVER

CONTINUEMIRROR

CREATEJOB

CREATEMIRROR

DELETEJOB

DELETELOCALMIRRORONLY

DELETEMIRROR

DROPSNAPSHOT

GETBLOCKTARGET

GETCOMPLETEVOLUMELIST

GETCONFIGURATION

GETEXTENDEDVOLUMEINFO

GETJOBINFO

GETJOBINFOFORVOL

GETMIRRORTYPE

GETMIRRORVOLINFO

GETREMOTEBITMAP

GETRESYNCSTATUS

GETSERVICEINFO

GETSNAPSHOTLOCATION

GETSOURCEMIRROREDVOLUMES

GETTARGETMIRROREDVOLUMES

GETVOLUMEDRVSTATE

GETVOLUMEINFO

ISBREAKUSERREQUESTED

ISPOTENTIALMIRRORVOL

LOCKVOLUME

MERGETARGETBITMAP

PAUSEMIRROR

PREPARETOBECOMETARGET

READREGISTRY

REGISTERCLUSTERVOLUME

RESTARTVOLUMEPIPE

RESYNCMIRROR

SETBLOCKTARGET

SETCONFIGURATION

SETSNAPSHOTLOCATION

STOPSERVICE

SWITCHOVERVOLUME

TAKESNAPSHOT

UNLOCKVOLUME

UPDATEJOB

UPDATEVOLUMEINFO

8.5.3.12.1. ミラー状態の定義

さまざまな状態の記述のため、内部的に次の数字が使用されます。この数字は EMCMD によって使用されますが、イベントログのエントリにある状態番号でもあります。

-1: 無効な状態

0: ミラーなし

1: ミラーリング

2: ミラーは再同期中

3: ミラーは中断

4: ミラーは一時停止

5: 再同期は待ち状態

8.5.3.12.2. BREAKMIRROR

EMCMD <system> BREAKMIRROR <volume letter> [<targetsystem>]

このコマンドはミラーを **中断** 状態にします。ミラーを中断すると、ミラーの再開時または再同期時に完全再同期が実行されます。パラメータは次のとおりです。

<system>	中断するミラーのソースシステムです。ターゲットシステムでの BREAKMIRROR コマンドは無効です。
<volume letter>	中断するミラーのボリュームレターです。
<target system>	中断するミラーのターゲットシステムの IP アドレスです。ミラーに複数のターゲットが関連している場合は、オプションパラメータを使用することもできます。このオプションパラメータを指定しない場合、ミラーはすべてのターゲットに対して中断されます。

8.5.3.12.3. CHANGEMIRRORENDPOINTS

EMCMD <NEW source IP> CHANGEMIRRORENDPOINTS <volume letter> <ORIGINAL target IP> <NEW source IP> <NEW target IP>

このコマンドは DataKeeper が保護するボリュームをネットワーク上の別の場所に移動します。

注記: このコマンドは 3 ノード以下で構成されるミラーボリュームのエンドポイントの変更をサポートします。4 つ以上のノードで構成される場合は、ミラーを削除してから再作成する必要があります。

以下の例を参照してください。

「 設定 」セクションの「 WAN に関する考慮事項 」および「 LAN/WAN 間のデータの初期同期 」を参照してください。

<new source IP> または <system name>	ミラーに使用できる新しいソース IP アドレスがあるシステムです。
<volume letter>	変更するミラーのドライブレターです。
<old target IP>	ターゲットシステムの以前の IP アドレスです。
<new source IP>	ソースシステムの新しい IP アドレスです。
<new target IP>	ターゲットシステムの新しい IP アドレスです。

注記:

- ジョブには複数のボリュームおよび複数のミラーが含まれる場合があります。CHANGEMIRRORENDPOINTS コマンドを使用するたびに、1 つのミラーのエンドポイントが変更されます。1×1 ミラー (1 つのソース、1 つのターゲット) の場合、コマンドを 1 回実行する必要があります。2×1 ミラー (1 つのターゲットノードで共有ボリュームを持つノード 2 つ) または 1×1×1 (1 つのソース、2 つのターゲットノード) の場合、必要なミラーエンドポイントを変更するには、コマンドを 2 回実行する必要があります。

- エンドポイントを変更する既存のミラーが現在アクティブなミラーである場合は、エンドポイントを変更する前に、一時停止 、中断 、または **再同期 (ペンディング)** の状態にする必要があります。

> **注意:** 中断 のコマンドを使用すると、**完全再同期** が実行されます。中断ではなく、ミラーを 一時停止 してください。|

- 変更前にボリュームの **ジョブ情報** を表示すると参考になります。例: emcmd . getJobInfoForVol D .

- エンドポイントを変更する間、DataKeeper GUI の **[ジョブ]** アイコンが赤くなる場合がありますが、ContinueMirror コマンドを実行すると緑に戻ります。

以下の例では、172.17.103 サブネットから 192.168.1 サブネットにミラーを移動します。基本的な手順は以下のとおりです。

1. ボリュームの **ジョブ情報を表示** します。
2. EMCMD コマンドラインを使用して **ミラーを一時停止** します。
3. システムの **IP アドレスを変更** します (必要な場合)。

> **重要:** ソースとターゲットの **IP アドレスを更新** していない場合は、**CHANGEMIRRORENDPOINTS** コマンドを実行する前に更新してください。このコマンドは、自動的にミラーを **一時停止** の状態にします。

4. **EMCMD CHANGEMIRRORENDPOINTS を実行** して、新しい IP アドレスに変更します。
5. **EMCMD CONTINUEMIRRORを実行** してミラーリングを再開します。

> **注意:** ミラーが継続される前にソースシステムが再起動されると、ミラーリングされたボリューム上で完全な再同期が実行されます。|

1×1 ミラーの CHANGEMIRRORENDPOINTS コマンドの例

1×1 ミラー (ソースとターゲットのみ) の場合、コマンドを 1 回実行する必要があります。

```
emcmd SYS1.MYDOM.LOCAL getJobInfoForVol D

       ID = caa97f9f-ac6a-4b56-8f25-20db9e2808a8

       Name = Mirr Vol D

       Description = Mirror Volume D

       MirrorEndPoints =
SYS3.MYDOM.LOCAL;D;172.17.103.223;SYS1.MYDOM.LOCAL;E;172.17.103.221;A

emcmd SYS1.MYDOM.LOCAL PauseMirror D

emcmd SYS1.MYDOM.LOCAL ChangeMirrorEndPoints D 172.17.103.223 192.168.1.221
192.168.1.223

emcmd SYS1.MYDOM.LOCAL getJobInfoForVol D
```

```
…

       MirrorEndPoints =
SYS3.MYDOM.LOCAL;D;192.168.1.223;SYS1.MYDOM.LOCAL;D;192.168.1.221;A

emcmd SYS1.MYDOM.LOCAL ContinueMirror D
```

2×1 ミラーの CHANGEMIRRORENDPOINTS コマンドの例

共有ソースボリュームとターゲットボリュームを含む 2×1 ミラーの場合は、コマンドを 2 回実行する必要があります。

```
emcmd SYS1.MYDOM.LOCAL getJobInfoForVol E

       ID = caa97f93e-ac6a-4b56-8f25-20db9e2808a8

       Name = Mirr Vol E

       Description = Mirror Volume E

       MirrorEndPoints = SYS1.MYDOM.LOCAL;E;0.0.0.0;SYS2.MYDOM.LOCAL;E
;0.0.0.0;D

       MirrorEndPoints =
SYS3.MYDOM.LOCAL;E;172.17.103.223;SYS2.MYDOM.LOCAL;E;172.17.103.222;A

       MirrorEndPoints =
SYS3.MYDOM.LOCAL;E;172.17.103.223;SYS1.MYDOM.LOCAL;E;172.17.103.221;A

emcmd SYS1.MYDOM.LOCAL PauseMirror E

emcmd SYS1.MYDOM.LOCAL ChangeMirrorEndPoints E 172.17.103.223 192.168.1.221
192.168.1.223

emcmd SYS2.MYDOM.LOCAL ChangeMirrorEndPoints E 172.17.103.223 192.168.1.222
192.168.1.223

emcmd SYS1.MYDOM.LOCAL getJobInfoForVol E

…

       MirrorEndPoints =
SYS1.MYDOM.LOCAL;E;0.0.0.0;SYS2.MYDOM.LOCAL;E;0.0.0.0;D

       MirrorEndPoints =
SYS3.MYDOM.LOCAL;E;192.168.1.223;SYS2.MYDOM.LOCAL;E;192.168.1.222;A
```

```
        MirrorEndPoints =
SYS3.MYDOM.LOCAL;E;192.168.1.223;SYS1.MYDOM.LOCAL;E;192.168.1.221;A

emcmd SYS1.MYDOM.LOCAL ContinueMirror E
```

1×1×1 ミラーの CHANGEMIRRORENDPOINTS コマンドの例

2 つのターゲットボリュームを含む 1×1×1 ミラーの場合は、コマンドを 2 回実行する必要があります。

```
emcmd SYS1.MYDOM.LOCAL getJobInfoForVol J

        ID = caa97f93j-ac6a-4b56-8f25-20db9j2808a8

        Name = Mirr Vol J

        Description = Mirror Volume J

        MirrorEndPoints =
SYS1.MYDOM.LOCAL;J;172.17.103.221;SYS3.MYDOM.LOCAL;J;172.17.103.223;A

        MirrorEndPoints =
SYS3.MYDOM.LOCAL;J;172.17.103.223;SYS2.MYDOM.LOCAL;J;172.17.103.222;A

        MirrorEndPoints =
SYS1.MYDOM.LOCAL;J;172.17.103.221;SYS2.MYDOM.LOCAL;J;172.17.103.222;A
```

この例では、システム「SYS3.MYDOM.LOCAL」が別のサイトに移動されます。

SYS1 と SYS2 は、新しいサブネット (192.168.1.*) を使用して SYS3 と通信するようになります。

ただし、SYS1 と SYS2 は、相互の通信に 172.17.103.* を使用し続けます。

```
emcmd SYS1.MYDOM.LOCAL PauseMirror J

emcmd SYS1.MYDOM.LOCAL ChangeMirrorEndPoints J 172.17.103.223 192.168.1.221
192.168.1.223

emcmd SYS2.MYDOM.LOCAL ChangeMirrorEndPoints J 172.17.103.223 192.168.1.222
192.168.1.223

emcmd SYS1.MYDOM.LOCAL getJobInfoForVol J

…

        MirrorEndPoints =
SYS1.MYDOM.LOCAL;J;192.168.1.221;SYS3.MYDOM.LOCAL;J;192.168.1.223;A
```

```
      MirrorEndPoints =
SYS3.MYDOM.LOCAL;J;192.168.1.223;SYS2.MYDOM.LOCAL;J;192.168.1.222;A

      MirrorEndPoints =
SYS1.MYDOM.LOCAL;J;172.17.103.221;SYS2.MYDOM.LOCAL;J;172.17.103.222;A

emcmd SYS1.MYDOM.LOCAL ContinueMirror J
```

8.5.3.12.4. CHANGEMIRRORTYPE

EMCMD <system> CHANGEMIRRORTYPE <volume letter> <remote ip> <A/S>

このコマンドは、DataKeeper ジョブの一部であるミラーのミラータイプを変更するために使用します。

注記: ボリュームがオンラインになっている必要があります。

以下の例を参照してください。

サポートされている DataKeeper のミラータイプについては、「 同期および非同期ミラーリング 」を参照してください。

<system>	ミラータイプの変更を開始するソースまたはターゲットシステムです。
<volume letter>	変更するミラーのドライブレターです。
<old target IP>	リモートシステムの IP アドレスです。
<A/S>	新規ミラータイプ（非同期または同期）です。

注記:

- ジョブには複数のボリュームおよび複数のミラーが含まれる場合があります。CHANGEMIRRORTYPE コマンドを使用するたびに、1 つのミラーのエンドポイントが変更されます。
- 既存のミラーのミラータイプを変更するには、ミラー内の各システムでボリュームがオンラインになっている必要があります。
- 既存のミラーのミラータイプは、ミラーがアクティブなミラーリング状態のときに変更できます。タイプの変更は直ちに有効になります。
- 存在しないミラーのミラータイプを変更することができます。以下の1×1×1の例を参照してください。
- スプリットブレイン状態にあるミラーのミラータイプは変更できません。スプリットブレインを最初に解決する必要があります。
- ジョブに複数のミラーが含まれている場合は、個々のミラータイプを変更できます。1 つのジョブ内、およびジョブ内の個々のボリュームのミラー内で、ミラータイプを混在させることができます。

1×1 ミラーの CHANGEMIRRORTYPE コマンドの例

```
emcmd SYS1.MYDOM.LOCAL getJobInfoForVol D

   ID = caa97f9f-ac6a-4b56-8f25-20db9e2808a8

   Name = Mirr Vol D
```

```
    Description = Mirror Volume D

    MirrorEndPoints  =  SYS3.MYDOM.LOCAL;D;172.17.103.223;SYS1.MYDOM.LOCAL;E;172.17

emcmd SYS1.MYDOM.LOCAL ChangeMirrorType D 172.17.103.223 S
```

この例では、SYS1 とSYS3 の間のD: のミラーを同期に変更しています。

1×1×1 ミラーの CHANGEMIRRORTYPE コマンドの例

```
emcmd SYS1.MYDOM.LOCAL getJobInfoForVol J

    ID caa97f93j-ac6a-4b56-8f25-20db9j2808a8

    Name = Mirr Vol J

    Description = Mirror Volume J

    MirrorEndPoints =
    SYS1.MYDOM.LOCAL;J;172.17.103.221;SYS2.MYDOM.LOCAL;J;172.17.103.222;A

    MirrorEndPoints =
    SYS1.MYDOM.LOCAL;J;172.17.103.221;SYS3.MYDOM.LOCAL;J;172.17.103.223;A

    MirrorEndPoints =
    SYS3.MYDOM.LOCAL;J;172.17.103.223;SYS2.MYDOM.LOCAL;J;172.17.103.222;A

emcmd SYS1.MYDOM.LOCAL GetMirrorVolInfo J

    J: 1 SYS1.MYDOM.LOCAL 172.17.103.222 1

    J: 1 SYS1.MYDOM.LOCAL 172.17.103.223 1

emcmd SYS1.MYDOM.LOCAL ChangeMirrorType J 172.17.103.222 S

emcmd SYS1.MYDOM.LOCAL ChangeMirrorType J 172.17.103.223 S

emcmd SYS2.MYDOM.LOCAL ChangeMirrorType J 172.17.103.223 S
```

この例では、すべてのミラータイプを同期に変更しています。3つ目のコマンドで、SYS2 と SYS3 間の存在しないミラーのミラータイプを変更しています。

8.5.3.12.5. CLEARBLOCKTARGET

EMCMD <システム> CLEARBLOCKTARGET <ボリュームレター>

このコマンドは、ブロックターゲットフラグの状態を FALSE に設定します。ブロックターゲットフラグがFALSE に設定されると、システムは選択されたボリュームのターゲットになることができます。このコマンドは、内部での使用のみを目的としています。このコマンドを実行しても出力は生成されません。

パラメータは次のとおりです。

<system>	ソースまたは、ターゲットシステムのどちらかです。
<volume letter>	ブロックターゲットフラグの状態を　FALSEに設定するボリュームのドライブレターです。

8.5.3.12.6. CLEARSNAPSHOTLOCATION

EMCMD <system> CLEARSNAPSHOTLOCATION <volume letter>

このコマンドは、指定システムの指定ボリュームについて、スナップショットの場所 (ディレクトリのパス) をクリアします。このコマンドが正常に実行されると、指定ボリュームのスナップショットが無効になります。

パラメータは次のとおりです。

<system>	スナップショットの場所のシステム名 / IP アドレスです。
<volume letter>	スナップショットを作成する対象のボリュームのドライブレターです。

出力例

```
Status = 0
```

このコマンドが正常に実行されると、ステータス 0 が返されます。コマンドが失敗した場合は、0 以外のステータスが返されます。

8.5.3.12.7. CLEARSWITCHOVER

EMCMD <system> CLEARSWITCHOVER <volume letter>

このコマンドは前回、ミラーが DELETELOCALMIRRORONLY コマンドで削除され、再構成を必要とするターゲットシステムで実行する必要があります。このコマンドは DELETELOCALMIRRORONLY を使用してターゲットから削除されたボリュームに対して設定された SIOS DataKeeper スイッチオーバフラグをクリアします。DELETELOCALMIRRORONLY を使用して削除したターゲットに CLEARSWITCHOVER を実行しない場合、システムを再起動しない限り、ミラーターゲットを再構成できません。

<system>	DELETELOCALMIRRORONLY を実行したターゲットシステムです。
<volume letter>	ミラーのドライブレターです。

8.5.3.12.8. CONTINUEMIRROR

EMCMD <system> CONTINUEMIRROR <volume letter> [<target system>]

このコマンドは一時停止、または中断したミラーを再開します。再同期 (完全再同期または部分再同期) が正常に完了すると、ミラーの状態は **ミラーリング** に変更されます。このコマンドは、ターゲットシステムがロック解除されている場合は自動的に再ロックしません。

注記: ターゲットボリュームがロック解除されている場合、このコマンドを実行する前に 再ロック する必要があります。

パラメータは次のとおりです。

<system>	ミラーを再開するミラーのソースシステムです。
<volume letter>	ミラーを再開するミラーのボリュームレターです。
<target system>	再同期を行うミラーのターゲットシステムの IP アドレスです。ミラーに複数のターゲットが関連している場合は、オプションパラメータを使用することもできます。このオプションパラメータを指定しない場合、再同期がすべてのターゲットに対して実行されます。

8.5.3.12.9. CREATEJOB

EMCMD . CREATEJOB <JobName> <Description> <FQDN Source> <DrvLetter1> <IP SourceReplication> <FQDN Target> <DrvLetter2> <IP Target for Replication><MirrorType> …

このコマンドは、内部での使用のみを目的としています。

8.5.3.12.10. CREATEMIRROR

EMCMD <system> CREATEMIRROR <volume letter> <target system> <type> [options]

このコマンドは、それぞれ同じドライブレターを使用して 2 つのマシン間にミラーを作成します。パラメータは次のとおりです。

<system>	ソースシステムの IP アドレスです (以下の 注記 を参照)。
<volume letter>	ミラーされるドライブレターです。これは、ソースおよびターゲットのドライブレターになります。
<target system>	ターゲットシステムの IP アドレスです (以下の 注記 を参照)。
<type>	ミラーの種類で、1 文字で表します。 A - 非同期ミラーを作成します。 S - 同期ミラーを作成します。
[options]	標準ではない処理を指定するオプションの引数。複数のオプションをまとめて指定できます (*10 進数の加算 - 例えばオプション 1 と オプション 4 を指定するには、5 (1 + 4) をコマンドに指定*)。それらは以下になります。 1: 完全な再同期処理を実行しないでミラーを作成します。 2: ターゲット側のミラー作成の完了を待ちません。 4: 起動時の制限を使用して作成します。基本的に、起動プロセスの一部としてミラーを再構成します。このオプションでは、リモートシステムが既にソースであるかどうかを調べて、ソースである場合には作成が失敗します。

注記: ディスクセクタサイズは、ソースボリュームとターゲットボリュームの両方で一致している必要があります。詳細はセクタサイズ を参照してください。

注記: ソースとターゲットの IP アドレスは同じプロトコルのものである必要があります。2 つの IPV4 アドレス、または 2 つの IPV6 の アドレスの組み合わせでのみ、ミラーを作成できます。DataKeeper は現在、異なるプロトコルを使用するミラーエンドポイントをサポートしていません。

IPv4 の例

```
EMCMD 192.168.1.1 CREATEMIRROR E 192.168.1.2 A 5
```

IPv6 の例

```
EMCMD 2001:5c0:110e:3304:a6ba:dbff:feb2:f7fd CREATEMIRROR F
2001:5c0:110e:3304:a6ba:dbff:feb2:afd7 A 5
```

8.5.3.12.11. DELETEJOB

EMCMD <system> DELETEJOB [<JobId>]

このコマンドは、内部での使用のみを目的としています。

8.5.3.12.12. DELETELOCALMIRRORONLY

EMCMD <system> DELETELOCALMIRRORONLY <volume letter>[<target system>]

このコマンドは、発行対象の <system> のミラーのみを削除します。ミラーリングを構成しているサーバのうち、ターゲットサーバが存在しソースサーバが存在しない状態、またはその逆の状態で終わるケースを処理します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	削除するミラーのドライブレターです。
<target system>	削除するミラーのターゲットシステムの IP アドレスです。ミラーに複数のターゲットが関連している場合は、オプションパラメータを使用することもできます。

8.5.3.12.13. DELETEMIRROR

EMCMD <system> DELETEMIRROR <volume letter> [<target system>]

このコマンドは、<system> がソースである場合にソースおよびターゲットの両方からミラーを削除します。<system> がターゲットの場合はソースシステムがダウンしている場合に限って、ターゲット側のミラーを削除します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	削除するミラーのドライブレターです。
<target system>	削除するミラーのターゲットシステムの IP アドレスです。ミラーに複数のターゲットが関連している場合は、オプションパラメータを使用することもできます。このオプションパラメータを指定しない場合、ミラーはすべてのターゲットに対して削除されます。

8.5.3.12.14. DROPSNAPSHOT

EMCMD <system> DROPSNAPSHOT <volume letter> [<volume letter> …]

このコマンドは、DataKeeper にボリュームをロックして作成済みのスナップショットファイルをクリーンアップするように指示します。パラメータは次のとおりです。

<system>	スナップショットを含むシステムの IP アドレスです。
<volume letter>	ターゲットサーバ上にある、スナップショットを作成したボリュームのドライブレターです。複数のスナップショットをクリーンアップする場合は、ドライブレターをスペースで区切って入力してください。

8.5.3.12.15. GETBLOCKTARGET

EMCMD <システム> GETBLOCKTARGET <ボリュームレター>

このコマンドは、ブロックターゲットフラグの現在の状態を TRUE または FALSE のどちらかで返します。ブロックターゲットフラグが TRUE に設定されている場合は、システムは選択されたボリュームのターゲットになることはできません。このコマンドは、内部での使用のみを目的としています。

パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	ブロックターゲットフラグの状態を取得するボリュームのドライブレターです。

出力例:

c:> EMCMD . GETBLOCKTARGET E

FALSE

8.5.3.12.16. GETCOMPLETEVOLUMELIST

EMCMD <system> GETCOMPLETEVOLUMELIST

このコマンドは、ミラーリングに適している、またはすでにミラー状態にあるすべてのボリュームの情報を表示します。
出力例:

ボリューム 1 の情報

Volume Root	= F:
Volume Label	= New Volume
Volume File System	= NTFS
Volume Total Space	= 2151608320
Mirror Role	= 01
Number of targets	= 2
Target 0 information:	
Volume State	= 0001
Target System	= 10.1.1.133
Target Drive Letter	= F
Target 1 information:	
Volume State	= 0002
Target System	= 10.1.1.134
Target Drive Letter	= F

8.5.3.12.17. GETCONFIGURATION

EMCMD <system> GETCONFIGURATION <volume letter>

このコマンドは、ボリュームのネットアラート設定 (別名、「ボリューム属性」) を取得して表示します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	情報収集対象のボリュームのドライブレターです。

出力例:

p(. ** Calling GetConfiguration [Volume F] **

All Net Alert bit	IS NOT enabled
Net Alert	IS NOT enabled
Broken State Alert	IS NOT enabled
Resync Done Alert	IS NOT enabled
Failover Alert	IS NOT enabled
Net Failure Alert	IS NOT enabled
LK Config	IS NOT enabled
Auto Resync	IS NOT enabled
MS Failover Cluster Config	IS NOT enabled
Shared Volume	IS NOT enabled

8.5.3.12.18. GETEXTENDEDVOLUMEINFO

EMCMD <system> GETEXTENDEDVOLUMEINFO <volume letter>

このコマンドは、選択したボリュームについて、ディスクシグネチャ、物理ディスクオフセット、内部ディスク ID などの拡張ボリューム情報を返します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	情報収集対象のボリュームのドライブレターです。

出力例

----------EXTENDED INFO ---

Physical Disk Signature = {217abb5a-0000-0000-0000-000000000000}

Physical Disk Offset = 32256

Internal Disk ID = 0xf2fa

8.5.3.12.19. GETJOBINFO

EMCMD <system> GETJOBINFO [<JobId>]

このコマンドは、特定のジョブ ID またはすべての定義されたジョブに対するジョブ情報を表示します。

8.5.3.12.20. GETJOBINFOFORVOL

EMCMD <system> GETJOBINFOFORVOL <DrvLetter>[<FullSysname>|<IP>]

このコマンドは、特定のシステム上の特定のボリュームに関連するジョブ情報を表示します。

8.5.3.12.21. GETMIRRORTYPE

EMCMD <system> GETMIRRORTYPE <volume letter>

このコマンドは、ミラータイプを数値で出力します。

パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	情報収集対象のボリュームのドライブレターです。

出力フォーマット

c:>EMCMD .GETMIRRORTYPE F

Target system 10.1.1.133, Type 2

Target system 10.1.1.134, Type 2

ミラータイプ

-1: 無効なタイプ (EMCMD は要求された情報を取得できない)

0: ミラーなし

1: 同期ミラー

2: 非同期ミラー

8.5.3.12.22. GETMIRRORVOLINFO

EMCMD <system> GETMIRRORVOLINFO <volume letter>

このコマンドはミラー状態をきわめて簡潔な出力で表示します。GETMIRRORVOLINFO コマンドは複数の出力行を返すことが可能です (1 つのターゲットにつき 1 行)。表示される情報は、実質的に GETVOLUMEINFO コマンドのものと同じです。

パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	情報収集対象のボリュームのドライブレターです。

出力例

c:>EMCMD .GETMIRRORVOLINFO F

F: 1 CARDINAL10.1.1.133 1

F: 1 CARDINAL10.1.1.134 1

出力フォーマット

[ボリュームレター} {ミラーの役割} [ソースシステム] [ターゲットシステム] [ミラーの状態]

ミラーの役割: 1 = ソース、2 = ターゲット

ミラー状態

-1: 無効な状態

0: ミラーなし

1: ミラーリング

2: ミラーは再同期中

3: ミラーは中断

4: ミラーは一時停止

5: 再同期は待ち状態

8.5.3.12.23. GETREMOTEBITMAP

EMCMD <system> GETREMOTEBITMAP <volume letter> <targetsystem> <local file>

このコマンドは、内部での使用のみを目的としていま

8.5.3.12.24. GETRESYNCSTATUS

EMCMD <system> GETRESYNCSTATUS <volume letter>

このコマンドは再同期処理の全体的な状況を示す情報を返します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	構成を設定するボリュームのドライブレターです。

出力例

Resync Status for Volume F:

Target 0 (Target System 10.1.1.133)

ResyncPhase : 3

BitmapPass : 1

NumberOfBlocks : 32831

DirtyBlocks : 0

CurrentBlock : 0

NewWrites : 1803

ResyncStartTime : Fri Nov 05 13.57.51 2008

LastResyncTime : Fri Nov 05 13.57.51 2008

Target 1 (Target System 10.1.1.134)

ResyncPhase : 2

BitmapPass : 0

NumberofBlocks : 32831

DirtyBlocks : 2124

CurrentBlock 29556

NewWrites : 0

ResyncStartTime : Fri Nov 05 15:09:47 2008

LastResyncTime : Fri Nov 05 15:09:47 2008

ResyncPhase は内部で使用され、開発環境外ではあまり重要ではありません。値は 0 (不明)、1 (初期)、2 (更新)、3 (完了) です。

BitmapPass はダーティブロックの数を示すビットマップを通過した回数です。カウントは 0 から行います。1 つのパスで再同期処理を実行すると、この値は増分しません。

NumberOfBlocks は、ボリューム上の 64K データブロックの数です。

DirtyBlocks パラメータは、更新が必要である (そしてまだ実行されていない) ことをビットマップが示すブロックの数です。

CurrentBlock パラメータは、ビットマップでの現在の位置を示します。

NewWrites パラメータは、再同期処理を実行してから行われたボリュームでの書き込みの数です。

ResyncStartTime と **LastResyncTime** のパラメータは、再同期処理が開始された時間、ネットワークで再同期の書き込み処理が最後に送信された時間を示します。

8.5.3.12.25. GETSERVICEINFO

EMCMD <system> GETSERVICEINFO

このコマンドは、指定のマシンで実行されている SIOS DataKeeper サービスとドライバのバージョンおよびその他の情報を取得します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。

出力例

Service Description:= SIOS DataKeeper Service

Service Build Type: = Release

Service Version = 7.0

Service Build = 1

Driver Version = 7.0

Driver Build = 1

Volume Bit Map = 1000070h

Service Start Time = Fri Oct 06 11:20:45 2008

Last Modified Time = Fri Oct 06 15:11:53 2008

8.5.3.12.26. GETSNAPSHOTLOCATION

EMCMD <system> GETSNAPSHOTLOCATION <volume letter>

このコマンドは、指定システムの指定ボリュームについて、現在設定されているスナップショットの場所 (ディレクトリのパス) を取得します。指定ボリュームにスナップショットの場所が設定されていない場合は、空の結果が返されます。

パラメータは次のとおりです。

<system>	スナップショットを作成する対象のボリュームを含むシステムのシステム名 / IP アドレスです。
<volume letter>	スナップショットを作成する対象のボリュームのドライブレターです。

出力例

> C:\Temp

コマンドが正常に実行された場合、stdout にスナップショットのディレクトリパスを報告します。スナップショットの場所が設定されていない場合は空の値が返されます。

8.5.3.12.27. GETSOURCEMIRROREDVOLUMES

EMCMD <system> GETSOURCEMIRROREDVOLUMES

このコマンドは、ソースが現在ミラー状態のシステムのボリュームに関する情報を表示します。

出力例

Status = 0

Source Volume = F:

Source Label = New Volume

Source #Targs = 2

Target 0

Target System = 10.1.1.133

Mirror State = 0001

Target 1

Target System = 10.1.1.134

Mirror State = 0001

8.5.3.12.28. GETTARGETMIRROREDVOLUMES

EMCMD <system> GETTARGETMIRROREDVOLUMES

このコマンドは、ターゲットが現在ミラー状態のシステムのボリュームに関する情報を表示します。

出力例

** Calling GetTargetMirroredVolumes **

Returned 1 Target Volumes

Target Volume 1 information:

Volume Root = F:

Volume State = 1

Source = 10.1.1.132

Target = BLUEJAY

8.5.3.12.29. GETVOLUMEDRVSTATE

EMCMD <system> GETVOLUMEDRVSTATE <volume letter>

このコマンドは、SIOS DataKeeper のデバイスドライバの現在の状態を取得します。

パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	構成を取得するボリュームのドライブレターです。

出力は状態を示す数字となっています。この出力が意図的に簡素化されているのは DataKeeper のリカバリスクリプトで解析できるように設計されているからです。出力は次のミラー状態のいずれかです。

-1: 無効な状態

0: ミラーなし

1: ミラーリング

2: ミラーは再同期中

3: ミラーは中断

4: ミラーは一時停止

5: 再同期は待ち状態

出力にはミラーエンドポイント (ソースまたはターゲット) のアドレスも表示されます。

8.5.3.12.30. GETVOLUMEINFO

EMCMD <system> GETVOLUMEINFO <volume letter> <level>

このコマンドは、選択したボリュームの情報を取得します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	情報収集対象のボリュームのドライブレターです。
<level>	1 ～ 3 の数字で、必要とする詳細の度合いを示します。

出力例

----------LEVEL 1 INFO----------

Volume Root = F:

Last Modified = Fri Nov 05 15:24:14 2008

Mirror Role = SOURCE

Label = New Volume

FileSystem = NTFS

Total Space = 2151608320

Num Targets = 2

Attributes : 20h

---------- -------LEVEL 2 INFO----------

>> Remote [0] = 10.1.1.133, F:

Mirror State = MIRROR

Mirror Type = ASYNCHRONOUSLY

>> Remote [1] = 10.1.1.133, F:

Mirror State = MIRROR

Mirror Type = ASYNCHRONOUSLY

----------LEVEL 3 INFO----------

>> Remote [0} = 10.1.1.133, F:

No Resync or CompVol Statistics to report

>> Remote [1] = 10.1.1.134, F:

No Resync or CompVol Statistics to report

8.5.3.12.31. ISBREAKUSERREQUESTED

EMCMD <system> ISBREAKUSERREQUESTED <volume letter>

中断したミラーがユーザの要求の結果かどうかを調べます。このコマンドはローカルシステム上でのみ実行できます。パラメータは次のとおりです。

<system>	ローカルシステムです。
<volume letter>	調査するボリュームのドライブレターです。

出力

TRUE	ミラーはユーザの要求により中断されました。
FALSE	ミラーは SIOS DataKeeper によって中断されました。(例: ネットワーク障害やターゲット側のデータ書き込みの失敗など) ボリュームは中断 (3) 状態ではありません。

8.5.3.12.32. ISPOTENTIALMIRRORVOL

EMCMD <system> ISPOTENTIALMIRRORVOL <volume letter>

このコマンドは、ボリュームがミラーリングに適しているかどうかを調べます。このコマンドはローカルシステム上でのみ実行できます。パラメータは次のとおりです。

<system>	ローカルシステムです。
<volume letter>	調査するボリュームのドライブレターです。

出力

TRUE - ボリュームはミラーリングに使用できます。

それ以外の場合、出力は以下の組み合わせとなります。

System Drive

RAW filesystem

FAT filesystem

ACTIVE partition

Contains PageFile

GetDriveType not DRIVE_FIXED

Contains DataKeeper bitmap files

ドライブレターが新規作成ボリューム (未接続の SIOS DataKeeper ドライバなど) やディスクではないもの (ネットワーク共有、CD-ROM) を指している場合、出力は以下のようになります。

Unable to open - SIOS DataKeeper driver might not be attached (you may need to reboot) or this might not be a valid hard disk volume.

ボリューム情報を取得中に内部エラーがあった場合は、以下のメッセージが表示されます。

Unable to retrieve the volume information for use in determining the potential use as a mirrored volume. The volume may be locked by another process or may not be formatted as NTFS.

8.5.3.12.33. LOCKVOLUME

EMCMD <system> LOCKVOLUME <volume letter>

このコマンドは、指定されたボリュームに排他的ロックを強制的に実行します。この呼び出しは、プロセスが開いたハンドルをボリュームに所有している場合は失敗します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	ロックするボリュームのドライブレターです。

8.5.3.12.34. MERGETARGETBITMAP

EMCMD <system> MERGETARGETBITMAP <volume letter> <target system>

このコマンドは、内部での使用のみを目的としています。

8.5.3.12.35. PAUSEMIRROR

EMCMD <system> PAUSEMIRROR <volume letter> [<target system>]

このコマンドはミラーを **一時停止** の状態にします。パラメータは次のとおりです。

<system>	一時停止するミラーのソースシステムです。PAUSEMIRROR コマンドをターゲットで実行しても影響はありません。
<volume letter>	ミラーのドライブレターです。
<target system>	一時停止するミラーのターゲットシステムの IP アドレスです。ミラーに複数のターゲットが関連している場合は、オプションパラメータを使用することもできます。このオプションパラメータを指定しない場合、ミラーはすべてのターゲットに対して一時停止します。

8.5.3.12.36. PREPARETOBECOMETARGET

EMCMD <system> PREPARETOBECOMETARGET <volume letter>

このコマンドは、スプリットブレイン 状態から復旧する場合にのみ使用してください。ターゲットになるべきミラーとミラーソースとして有効であるシステム上で実行する必要があります。このコマンドは、ミラーを削除し、ボリュームをロックします。

スプリットブレイン状態から復旧するには、ミラーソースとして残っているシステムで “:#continuemirror を実行してください。

シナリオ例

ボリューム F ドライブが SYSA および SYSB の両方でミラーソースである場合、emcmd を使用してスプリットブレインの状態を解消することができます。ソースとして残すシステムの 1 つを選択します (例: SYSA)。SYSB に保存しておく必要のあるファイルまたは変更がないことを確認してください。それらが SYSB にある場合は、手動で SYSA へコピーしてください。ミラーを再構成する場合は、以下の手順を実行してください。

```
EMCMD SYSB PREPARETOBECOMETARGET F
```

SYSB の F ドライブのミラーが削除され、F ドライブがロックされます。

```
EMCMD SYSA CONTINUEMIRROR F
```

SYSA から SYSB への F ドライブへのミラーリングが構成され、部分再同期が発生し (それまでの SYSB の変更はすべて上書きされる) 、ミラーが **ミラーリング** 状態になります。

8.5.3.12.37. READREGISTRY

EMCMD <system>READREGISTRY <volume letter>

このコマンドは、SIOS DataKeeper のドライバにレジストリ設定を再読み込みさせます。パラメータは次のとおりです。

<system>	ソースシステムまたはターゲットシステムのどちらかです。
<volume letter>	設定の再読み込みを行うミラーのドライブレターです。

このコマンドによって次のレジストリ設定の再読み込みが行われ、変更が有効になります。

ソースシステム (次のパラメータの変更はただちに有効になります)

BandwidthThrottle

BitmapBytesPerBlock

BlockWritesOnLimitReached

CompressionLevel

ResyncReads

WriteQueueByteLimitMB

WriteQueueHighWater

WriteQueueLowWater (この値は非推奨であり、現在使用されていません。)

DontFlushAsyncQueue

ターゲットシステム (次のパラメータの変更はソースおよびターゲットシステムの次回の再接続時に有効になります)

TargetPortBase

TargetPortIncr

8.5.3.12.38. REGISTERCLUSTERVOLUME

EMCMD <system> REGISTERCLUSTERVOLUME <volume letter>

このコマンドは、DataKeeper が保護するボリュームを WSFC Windows 2008 クラスタに登録します。

<system>	ミラーのソースシステムです。
<volume letter>	登録するミラーのドライブレターです。

8.5.3.12.39. RESTARTVOLUMEPIPE

EMCMD <system> RESTARTVOLUMEPIPE <volume letter>

このコマンドは、内部での使用のみを目的としています。

8.5.3.12.40. RESYNCMIRROR

EMCMD <system> RESYNCMIRROR <volume letter> [<target system>]

このコマンドはミラーに対して完全再同期を実行します。パラメータは次のとおりです。

<system>	ソースシステム名です。
<volume letter>	再同期を行うミラーのドライブレターです。
<target system>	再同期を行うミラーのターゲットシステムの IP アドレスです。ミラーに複数のターゲットが関連している場合は、オプションパラメータを使用することもできます。オプションパラメータを指定しない場合は、すべてのターゲットに対して再同期が実行されます。

8.5.3.12.41. SETBLOCKTARGET

EMCMD <システム> SETBLOCKTARGET <ボリュームレター>

このコマンドは、ブロックターゲットフラグの状態を TRUE に設定します。ブロックターゲットフラグがTRUE に設定されると、システムは選択されたボリュームのターゲットになることができません。このコマンドは、内部での使用のみを目的としています。このコマンドを実行しても出力は生成されません。

パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	ブロックターゲットフラグの状態を TRUE に設定するボリュームのドライブレターです。

8.5.3.12.42. SETCONFIGURATION

EMCMD <system> SETCONFIGURATION <volume letter><configuration mask>

このコマンドは、ボリュームにネットアラート設定 (別名「ボリューム属性」) を設定します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	構成を設定するボリュームのドライブレターです。
<configuration mask>	ネットアラートを設定するビットマスクです。次のビットマスクが定義されています。 1 -- 0×01: すべてのネットアラートが有効 2 -- 0×02: 中断状態のアラートが有効 4 -- 0×04: 再同期処理完了アラートが有効 8 -- 0×08: フェイルオーバアラートが有効 16 -- 0×10: ネット障害アラートが有効 32 -- 0×20: LifeKeeper 設定が有効 64 -- 0×40: 自動再同期が有効 128 -- 0×80: MS フェイルオーバクラスタ構成が有効 256 -- 0×100: 共有ボリュームが有効

すべてのフラグをクリアする場合の例

EMCMD .SETCONFIGURATION E 0

共有ボリュームと MS フェイルオーバクラスタの構成を有効にする複数構成の例 (*10 進数値 256 と 128 を加算*):

EMCMD .SETCONFIGURATION E 384

8.5.3.12.43. SETSNAPSHOTLOCATION

EMCMD <system> SETSNAPSHOTLOCATION <volume letter> "<directory path>"

このコマンドは、指定システムの指定ボリュームについて、スナップショットの場所 (ディレクトリのパス) を設定します。このディレクトリは、該当システムで有効である必要があり、ローカルドライブ / パスを表す絶対パスにする必要があります。また、空白にしておくことはできません (CLEARSNAPSHOTLOCATION を参照)。スナップショットの場所が現在設定されていない場合、このコマンドを実行すると、指定ボリュームのターゲットのスナップショットが可能になります。

パラメータは次のとおりです。

<system>	スナップショットを作成する対象のボリュームを含むシステム名 / IP アドレスです。
<volume letter>	スナップショットを作成する対象のボリュームのドライブレターです。
<directory path>	<system> のローカルにあるディレクトリの絶対パスであり、スナップショットファイルの場所を示します。パスにスペース文字が含まれる場合は、この値を引用符で囲む必要があります。

出力例

```
Status = 0
```

このコマンドが正常に実行されると、ステータス 0 が返されます。コマンドが失敗した場合は、0 以外のステータスが返されます。

8.5.3.12.44. STOPSERVICE

EMCMD <system> STOPSERVICE

このコマンドは DataKeeper サービスを停止します。

8.5.3.12.45. SWITCHOVERVOLUME

EMCMD <system> SWITCHOVERVOLUME <volume letter> [-f]

このコマンドは、指定したシステムをソースにします。**このコマンドは、内部での使用のみを目的としています。**

<system>	ソースになるシステムの IP アドレスです。**注記:** システムの NetBIOS 名、IP アドレス、または完全修飾ドメイン名を使用して、指定のシステムに接続してください。emcmd を実行しているローカルシステムは、ピリオド (.) で表すこともできます。
<volume letter>	要求されたボリュームのドライブレターです。
[-f]	このオプションは、**高速** (*安全ではない*) スイッチオーバに使用できます。このオプションは、現在のソースのステータスが既知の場合にのみ使用してください。このコマンドを正しく使用しない場合、スプリットブレイン 状態が発生することがあります。

8.5.3.12.46. TAKESNAPSHOT

EMCMD <target system> TAKESNAPSHOT <volume letter> [<volume letter> …]

このコマンドはターゲットシステム上で実行し、指定システム上にある指定ボリュームのスナップショットを作成するように DataKeeper に通知します。スナップショットの場所を設定しない場合、コマンドは失敗します。

パラメータは次のとおりです。

<target system>	スナップショットを作成する対象のボリュームを含むターゲットシステム名 / IP アドレスです。
<volume letter>	ターゲットサーバ上にある、スナップショットを作成する対象のボリュームのドライブレターです。複数のボリュームのスナップショットを作成する場合、ドライブレターをスペースで区切ってください。

注記: すべてのターゲットボリュームのソースシステムが同じである必要があります。

8.5.3.12.47. UNLOCKVOLUME

EMCMD <system> UNLOCKVOLUME <volume letter>

このコマンドは指定したボリュームをロック解除します。パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	ロック解除するボリュームのドライブレターです。

8.5.3.12.48. UPDATEJOB

EMCMD <system> UPDATEJOB <JobId> <Name> <Descr>[<SysName1> <DrvLetter1> <IP1> <SysName2><DrvLetter2> <IP2> <MirrorType>]…

このコマンドは、内部での使用のみを目的としています。

8.5.3.12.49. UPDATEVOLUMEINFO

EMCMD <system> UPDATEVOLUMEINFO <volume letter>

このコマンドを実行すると、SIOS DataKeeper サービスはドライバをクエリ処理して正しいミラー状態を取得します。DataKeeper GUI に表示されている情報が正しくないか、最新の情報でない場合、このコマンドを使用すると便利です。

注記: SIOS DataKeeper サービスはシステムイベントログ 内の新しい情報に基づいて、ボリューム情報を自動的にアップデートします。

パラメータは次のとおりです。

<system>	ソースまたはターゲットシステムのどちらかです。
<volume letter>	情報を更新したいボリュームのドライブレターです。

もし、ボリューム情報のアップデートに内部エラーが起きた場合には、次のメッセージが表示されることがあります。

Unable to update the volume information. The volume may be locked by another process or may not be formatted as NTFS.

EMCMD コマンドの Proxy オプションを使用する

全ての EMCMD リクエストは "Proxy" DataKeeper サービスを経由することができます。Proxy を経由して実行する場合には、実行する EMCMD コマンドの最後に以下のオプションを追加してください。

-proxy <proxy_system> -

<proxy_system>には<system>オプションと同じフォーマットを使用してください。EMCMDコマンドは最初に <proxy_system> とのコネクションを開き、そのリクエストを <system> へとフォワードします。<proxy_system> 上の DataKeeper サービスは <system> とのコネクションを開き、<system> へEMCMDコマンドのリクエストを送り、そのレスポンスをユーザーへ返します。

-proxy <proxy_system> オプションは DataKeeper ノード同士の通信が可能な状態かを確認することができます。

使用例

```
EMCMD DK_NODE_2 GETSERVICEINFO -proxy DK_NODE_1
```

DK_NODE_1 で動作している DataKeeper サービスへのコネクションをオープンし、次に DK_NODE_2 への接続をオープンします。そして、`GETSERVICEINFO` リクエストをフォワードし、DK_NODE_2 から GETSERVICEINFO の結果としてサービス情報を返します。このコマンドは、DK_NODE_1 上の DataKeeper サービスが DK_NODE_2 上で DataKeeper サービスと通信することができることを確認するために利用できます。

8.5.3.13. SIOS DataKeeperでDKPwrShellを使用する

SIOS DataKeeperには、ユーザがMicrosoft Powershellを使用して、DataKeeperのミラーを操作できるPowershellモジュール（DKPwrShell）が含まれています。コマンドは、SIOS DataKeeperサービスに渡され、サービスが実行中でない場合は失敗します。

Microsoft Powershell v3.0以降では、SIOS DataKeeperのPowershellモジュールは、Powershell開始時に自動的にロードされます。Microsoft Powershell v3.0 より前の SIOS DataKeeperのPowershellモジュールは、以下の構文を使用してimport-moduleコマンドでロードする必要があります。

```
import-module "<DK InstallPath>\DKPwrShell"
```

> **注記:** 初期値では、`<DK InstallPath>`は `C:\Program Files (x86)\SIOS\DataKeeper` に設定されています。

New-DataKeeperMirror

New-DataKeeperJob

Remove-DataKeeperMirror

Remove-DataKeeperJob

Add-DataKeeperJobPair

Get-DataKeeperVolumeInfo

8.5.3.13.1. New-DataKeeperMirror

このコマンドは、新しいDataKeeperのミラーを作成するのに使用します。

パラメータ

パラメータ	タイプ	必須	注記
SourceIP	String	Yes	DataKeeperのミラーデータに使用されるソース上のIPアドレス。
SourceVolume	String	Yes	ミラーのためのソースボリューム。
TargetIP	String	Yes	DataKeeperのミラーデータに使用されるターゲット上のIPアドレス。
TargetVolume	String	No	ミラーターゲットになるためのターゲットボリューム。特定されない場合は、ソースボリュームパラメータによって、同じボリュームが表示されます。
SyncType	String	Yes	有効なオプション: Sync - 同期ミラー。 Async - 非同期ミラー。
CreateFlags	uint	No	標準から逸脱した動作を特定するオプションの引数。オプションのセットを作成するために、複数の引数を使用することができます。(小数値を追加してください。例: option 1 + option 2には、コマンドで3を設定。) 1. 全同期操作をしないで、ミラーを作成してください。 2. 戻す前に作成されるミラーのターゲット側を待たないでください。

入力

なし

出力

コマンドのステータスを表す整数値。0は、成功したコマンドです。他の値は、Windowsのエラーコードとなります。

> ✻ 注記: ソースとターゲットIPアドレスは、同じプロトコルである必要があります。ミラーは、2つのIPV4、あるいは2つのIPV6アドレスを使用することによってのみ、作成することができます。現在DataKeeperは、異なるプロトコルにおけるミラーのエンドポイントをサポートしていません。

例:

New-DataKeeperMirror -SourceIP 10.200.8.55 -TargetIP 10.200.8.56 -SourceVolume e -SyncType Async

New-DataKeeperMirror 10.200.8.55 E 10.200.8.56 E Async

> ✻ 注記: ディスクセクタのサイズは、ソースボリュームとターゲットボリュームの両方で一致する必要があります。詳細は セクタサイズ を参照してください。

8.5.3.13.2. New-DataKeeperJob

このコマンドは、2つのノードから成るDataKeeperのジョブを作成するのに使用します。

Parameters

パラメータ	タイプ	必須	注記
JobName	String	Yes	ジョブの名前。
JobDescription	String	No	ジョブの簡単な説明。
Node1Name	String	Yes	第1ノードのFQDN。
Node1IP	String	Yes	DataKeeper のレプリケーションに使用される第1ノードのIPアドレス。
Node1Volume	String	Yes	レプリケーションに関する第1ノードのボリューム。
Node2Name	String	Yes	第2ノードのFQDN。
Node2IP	String	Yes	DataKeeper のレプリケーションに使用される第2ノードのIPアドレス。
Node2Volume	String	Yes	レプリケーションに関する第2ノードのボリューム。
SyncType	String	Yes	有効なオプション: Sync - 同期ミラー。 Async - 非同期ミラー。 Disk - これら2つのボリュームが、1つの共有ディスク。

入力

なし

出力

成功時は、生成されたジョブを表すオブジェクト。失敗時は、Windowsエラーコードを含む例外。

> **注記:** IPアドレスは同じプロトコルである必要があります（IPv4、またはIPv6）。現在DataKeeperは、異なるプロトコルにおけるミラーのエンドポイントをサポートしていません。

例:

New-DataKeeperJob -Node1Name example1.domain.com -Node1IP 10.200.8.55 Node1Volume e -Node2Name example2.domain.com -Node1IP 10.200.8.56 Node1Volume f -SyncType Async

8.5.3.13.3. Remove-DataKeeperMirror

このコマンドは、DataKeeperのミラーを削除し、このミラーをすべてのノードから削除しようとします。そして、ダウン、あるいはネットワークアクセスできないノードからはミラーを削除しません。

パラメータ

パラメータ	タイプ	必須	注記
Source	String	Yes	ミラーのソースノード。
Volume	String	Yes	削除したいソースノード上にあるミラーボリュームのレター。
Target	String	No	ミラーのターゲットシステムに対するIPアドレス。このパラメータの左が空欄の場合は、ソースボリュームのすべてのターゲットが削除されます。

入力

なし

出力

コマンドのステータスを表す整数値。0は、成功したコマンドです。他の値は、Windowsのエラーコードとなり

8.5.3.13.4. Remove-DataKeeperJob

このコマンドは、指定したIDのDataKeeperジョブを削除します。このジョブは、ジョブに含まれる全てのシステムから削除されます。

パラメータ

パラメータ	タイプ	必須	注記
JobID	String	Yes	ジョブが作成された時割り当てられた唯一無二のジョブGUID。
Node	String	Yes	FQDN、またはジョブIDによって特定されたジョブを含むノードのIPアドレス。

入力

なし

出力

コマンドのステータスを表す整数値。0は、成功したコマンドです。他の値は、Windowsのエラーコードとなります。

8.5.3.13.5. Add-DataKeeperJobPair

このコマンドは、既存のDataKeeperジョブにノードペアを追加します。

既存のジョブに含まれるノードとボリュームを拡張するのに使用します。例えば、ジョブがノードAとノードBの間のボリュームにあり、ノードCを追加したい場合はAddDataKeeperJobPairを2回実行します。1回目は、ノードAとノードCの間の新しい関係定義のため、2回目は、ノードBとノードCの新しい関係定義のためとなります。

パラメータ

パラメータ	タイプ	必須	注記
JobID	String	Yes	ジョブが作成された時割り当てられた一意のジョブGUID。
Node1Name	String	Yes	第1ノードのFQDN。
Node1IP	String	Yes	DataKeeper レプリケーションに使用される第1ノードのIPアドレス。
Node1Volume	String	Yes	レプリケーションに関係する第1ノードのボリューム。
Node2Name	String	Yes	第2ノードのFQDN。
Node2IP	String	Yes	DataKeeper レプリケーションに使用される第2ノードのIPアドレス。
Node2Volume	String	Yes	レプリケーションに関係する第2ノードのボリューム。
SyncType	String	Yes	有効なオプション: Sync - 同期ミラー。 Async - 非同期ミラー。 Disk - これら2つのボリュームが、1つの共有ディスク。

入力

なし

出力

コマンドのステータスを表す整数値。0は、成功したコマンドです。他の値は、Windowsのエラーコードとなります。

例:

Add-DataKeeperJobPair -JobID a1f1ecc6-649e-476b-bbff-286b815fdd30 -Node1Name example1.domain.com -Node1IP 10.200.8.55 Node1Volume e -Node2Name example2.domain.com -Node1IP 10.200.8.56 Node1Volume f -SyncType Async

8.5.3.13.6. Get-DataKeeperVolumeInfo

この cmdlet は、DataKeeper で使用中のボリュームについての情報のフェッチに使用され、DataKeeper のボリューム情報をレポートします。

パラメータ	タイプ	必須	位置	注記
ノード	文字列	はい	0	ノードパラメータを使用して、複製するボリュームを含むシステムを指定します。このパラメータは IPv4 アドレス、FQDN、またはローカルシステムの場合、単に「.」のいずれかです。
ボリューム	文字列	はい	1	(システムノード上の) ミラーボリュームレターです。

入力

なし

出力

VolumeInfo オブジェクト

例:

Get-DataKeeperVolumeInfo -Node example.domain.com -Volume E

Get-DataKeeperVolumeInfo 10.200.8.55 E

Get-DataKeeperVolumeInfo . E

Get-DataKeeperVolumeInfo

8.5.4. ユーザガイド

このセクションは、SIOS DataKeeper を初めて使用する際のリファレンスとなるように作成されています。実装する構成の種類を決定するための参考となる情報を提供し、SIOS DataKeeper のソフトウェアを効果的に使用するための詳細な手順を説明します。

入門

セットアップ

ミラーの構成

ジョブに関連する作業

ミラーに関連する作業

共有ボリュームに関連する作業

Windows 2012 上の DK で iSCSI ターゲットを使用する

DataKeeper Notification Icon

ターゲットスナップショッ

DKSE を使用して Hyper-V 仮想マシンのディザスタリカバリを行う

8.5.4.1. 入門

構成の選択

DataKeeper は、多様な構成で、以下のようなさまざまな機能を利用することができます。

- データの 2 つ目の物理コピーを提供する。
- 既存の MSCS/WSFC クラスタをリモート DR サイトに拡張する。
- 従来の MSCS/WSFC クラスタに関連する単一障害点を除去する。

以下のレプリケーション構成および例示されたユースケースを確認して、DataKeeper の機能を理解してください。その後、関心がある構成に関連するトピックを参照して、その構成の詳細を確認してください。

ディスクからディスク

1 対 1

1 対多

多対 1

1 つに複製される N 共有ディスク

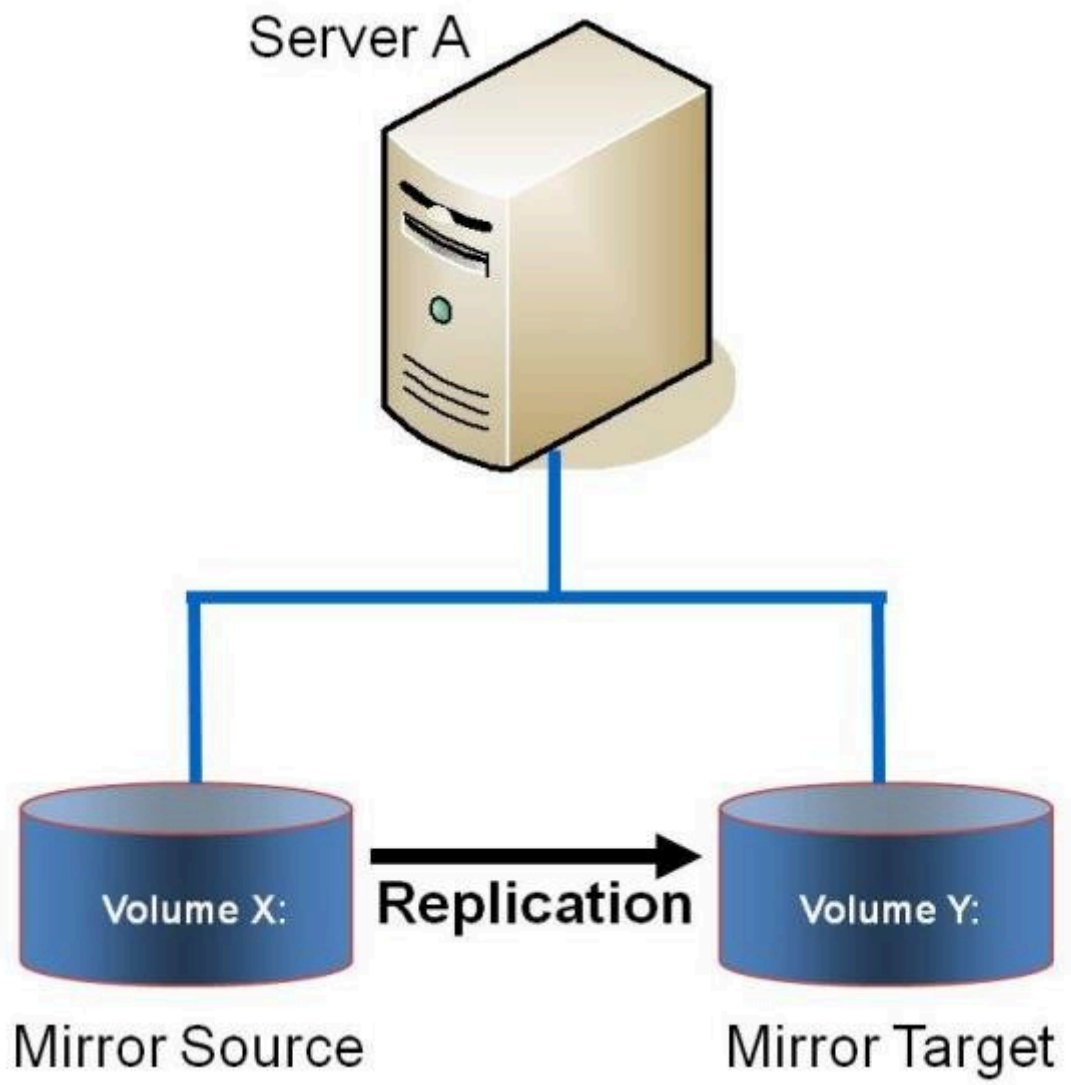
N 共有ディスクに複製される N 共有ディスク

複数の N 共有ディスクターゲットに複製される N 共有ディスク

8.5.4.1.1. ディスクからディスク

これは、1 台のサーバ、2 つのディスク構成で、サーバ A 上のボリューム X をサーバ A 上のボリューム Y にミラーリングする簡単なケースです。このDisk to Disk構成に使用されたボリュームは他のシステムとのレプリケーションを構成できません。

注意 :このDisk to Diskの構成では複数のターゲットを使用したミラーリングはサポートしていません。



例:ユースケース
あるサーバ上のボリュームから同一サーバ上の別のボリュームにデータを複製します。これらのディスクは異なるストレージアレイとすることもでき、プライマリ SAN に障害が発生した場合にデータを損失から保護します。

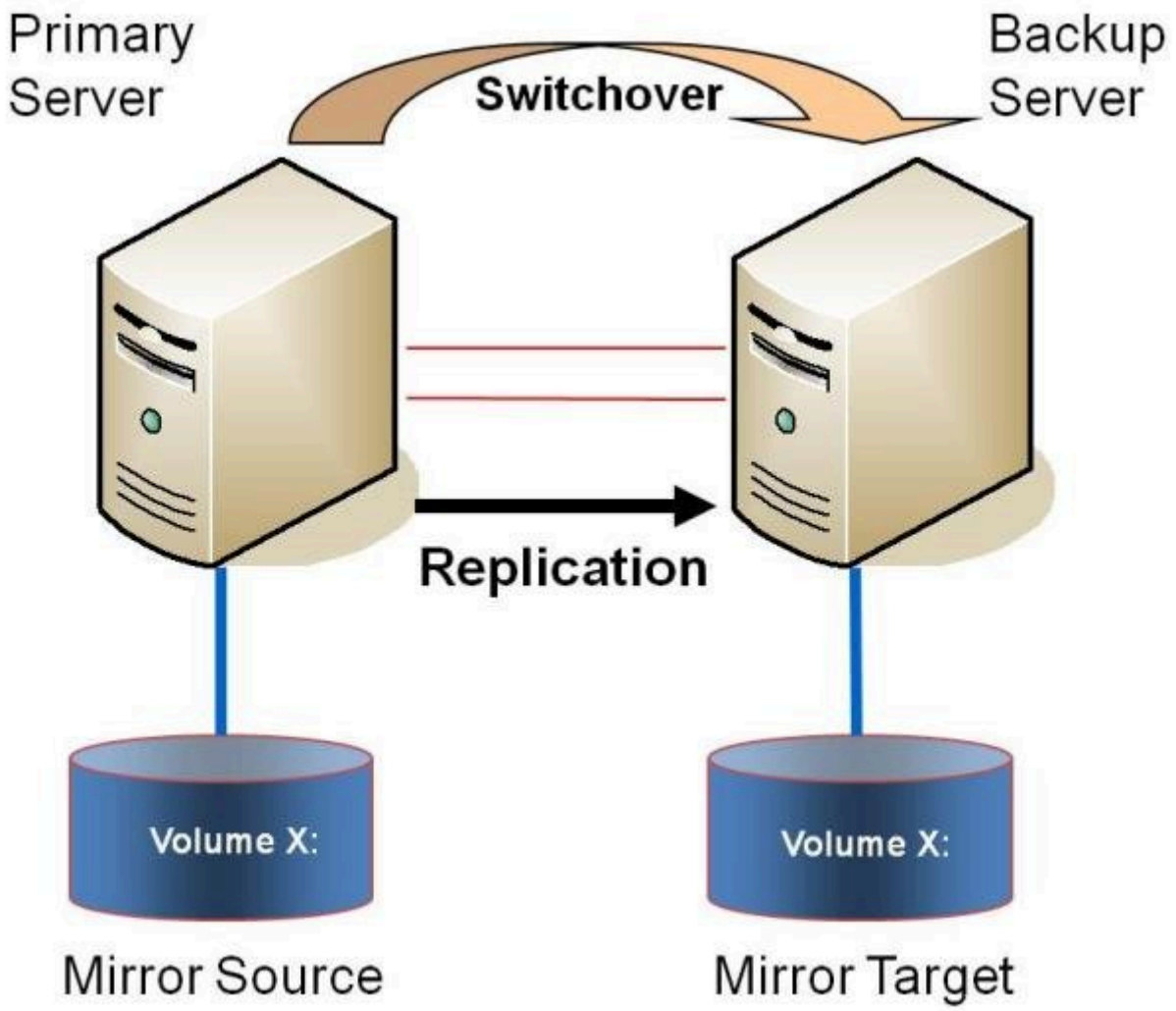
関連項目

- ミラーの作成
- ミラーの管理
- 大量書き込みに対する考慮事項

- よくある質問

8.5.4.1.2. 1 対 1

これはソース 1 つ、ターゲット 1 つの簡単な構成で、ネットワーク経由でボリューム X: のミラーリングを行います。データの 2 つ目の物理コピーを提供するのに加えて、DataKeeper ではミラーのスイッチオーバ機能も提供しており、バックアップサーバのデータをアクティブにすることができます。



例:
1 つまたは複数のボリュームのデータを、ある都市のサーバから別の都市にある別のサーバに複製します。

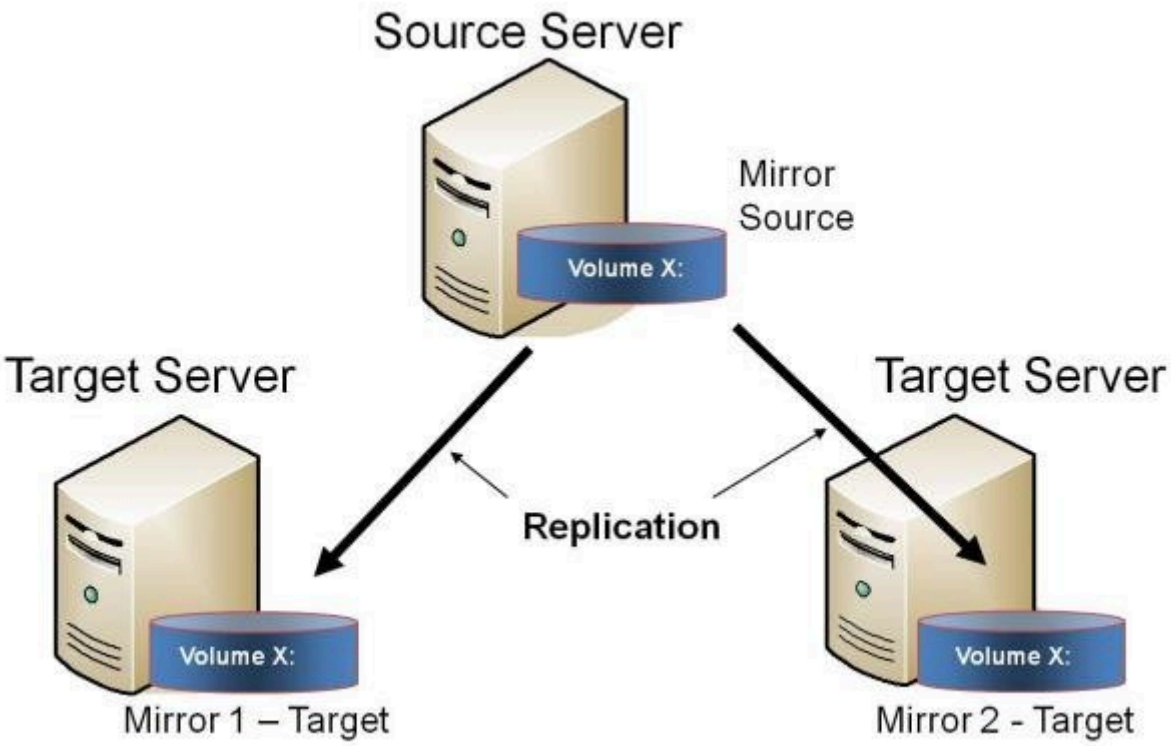
関連項目

- プライマリサーバのシャットダウン
- セカンダリサーバの障害

- DataKeeper Standard Edition を使用して Hyper-V 仮想マシンのディザスタリカバリを行う
- よくある質問

8.5.4.1.3. 1 対多 (マルチターゲット)

この構成には、ネットワーク経由で 2 つの異なるターゲットシステムに対して 1 つ (または複数) のボリュームを複製する 1 つのプライマリ (ソース) システムが含まれます。これはマルチターゲット構成と呼ばれます。



互いに完全に独立したミラーが 2 つあることに注意してください。ミラーは異なるネットワークを使用している場合があります。圧縮またはネットワーク帯域制限の設定が異なる場合や、状態がまったく異なる場合 (例: ミラー 1 -- ミラーリング、ミラー 2 -- 再同期) もあります。

例:ユースケース	プライマリサーバと同じサイトにある 1 台のターゲットサーバにデータを複製し、プライマリサイトに障害が発生した場合の障害回復のために、リモートサイトにもデータを複製します。
例:ユースケース	単一のソースシステムから複数のターゲットシステムに定期的にデータを複製 (「プッシュ」) します。

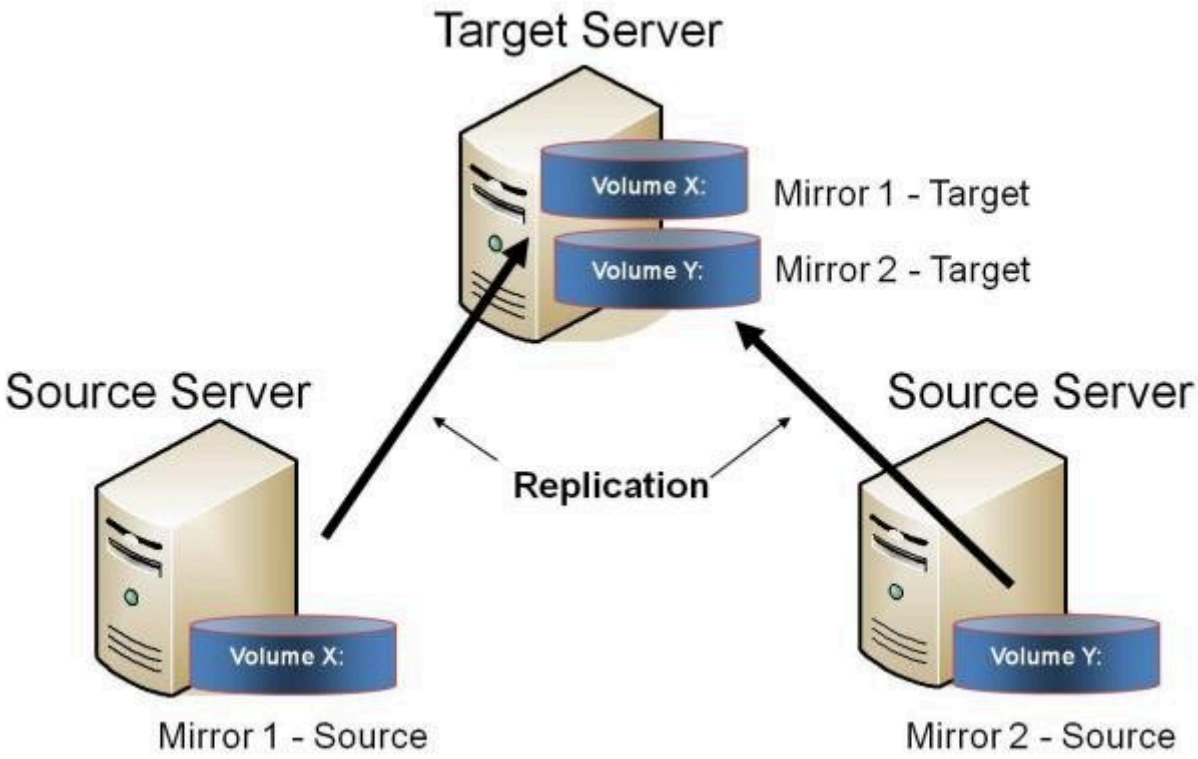
関連項目

- プライマリサーバのシャットダウン
- セカンダリサーバの障害
- 複数ターゲットとのミラーの作成
- 複数ターゲットのスイッチオーバおよびフェイルオーバ
- DataKeeper Standard Edition を使用して Hyper-V 仮想マシンのディザスタリカバリを行う

- よくある質問

8.5.4.1.4. 多対 1

この構成には、同一のターゲットシステムに対して 1 つ (または複数) のボリュームを複製する、複数のソースサーバが含まれます。この構成では、ターゲットサーバに複製される各ボリュームは一意のドライブレターを持つ必要があります。



注記: これは実際には 2 つの 1 対 1 ミラーです。

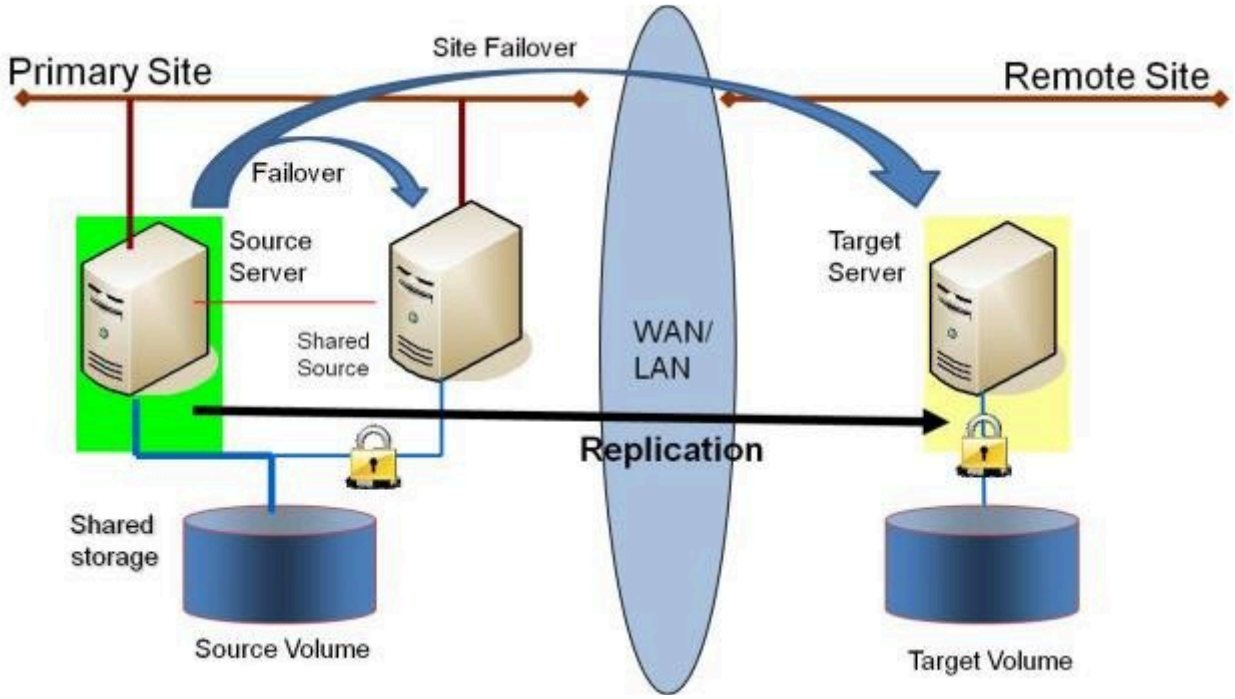
例:ユースケース	バックアップの統合や障害回復のために、複数の分岐を単一のデータセンタに戻すこともできます。

関連項目

- プライマリサーバのシャットダウン
- セカンダリサーバの障害
- DataKeeper Standard Edition を使用して Hyper-V 仮想マシンのディザスタリカバリを行う
- よくある質問

8.5.4.1.5. 共有ディスクを単体のディスクにレプリケーションする構成

この構成では、プライマリサイトの共有ボリュームをネットワーク経由でリモートシステムにレプリケーションできます。



この構成は、プライマリサイト内のローカルフェイルオーバと、プライマリサイト全体がダウンした場合のディザスタリカバリを提供するのに最適です。

例:ユースケース	共有ボリュームをリモートターゲットに複製して、WSFC クラスタを DR サイトに拡張します。プライマリサイトが停止した場合には、リモートサーバがアクティブサーバになります。

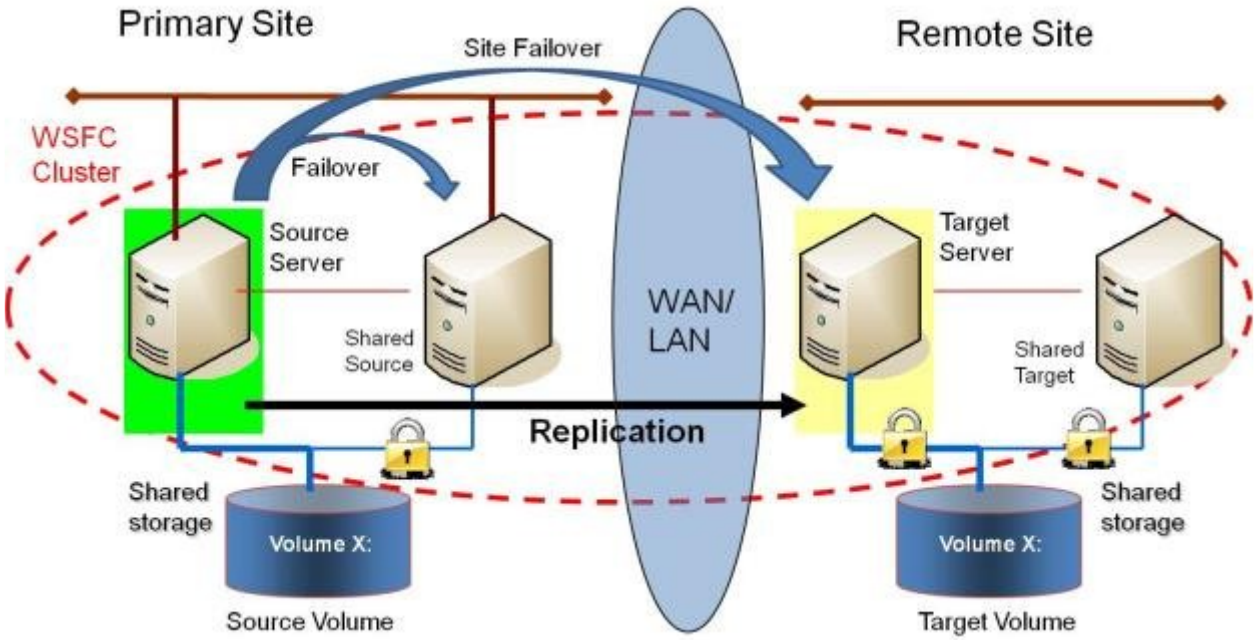
関連項目

DataKeeper スタンドアロン

- 共有ボリュームとのミラーの作成
- 共有ボリュームの管理
- 共有システムの追加
- 共有システムの削除
- よくある質問

8.5.4.1.6. 共有ディスク同士でレプリケーションする構成

この構成では、共有ストレージを利用しているサイト間でデータを複製します。



プライマリサイト内のシステムの数は、リモートサイト内のシステムの数と同じでなくてもかまいません。

また、ソースサーバのみがソースボリュームにアクセスできることにも注意してください。共有ソースシステムおよびターゲット側のすべてのシステムはボリュームにアクセスできず、ファイルシステムからはロックされています。

例:ユースケース	DR サイトで同じレベルの可用性を提供するには、この構成を展開して、どのサイトがサービス中であるかにかかわらず可用性レベルが一定になるようにします。
例:ユースケース	Hyper-V クラスタが多数のクラスタノード間に分散した仮想マシンで構成されている場合は、障害回復時に同程度の数のクラスタノードを使用できるようにして、障害発生時にすべての仮想マシンを実行できるリソースを確保することが重要です。

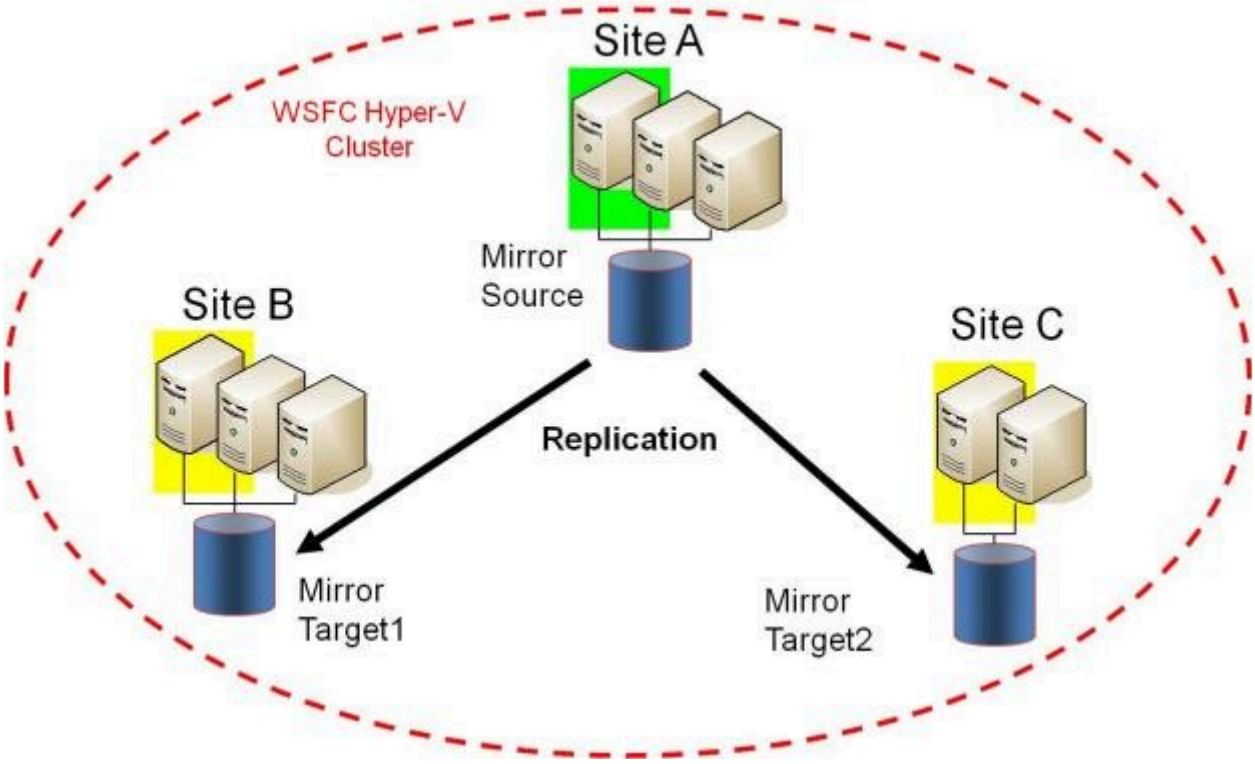
関連項目

- 共有ボリュームとのミラーの作成
- 共有ボリュームの管理
- 共有システムの追加
- 共有システムの削除

- よくある質問

8.5.4.1.7. N 個の共有ディスクターゲットへレプリケーションされる N 個の共有ディスク構成

これは、複数の共有ターゲットに対して共有ストレージ環境をレプリケーションしている複雑な構成です。



プライマリサイトのシステムの数は、リモートサイトのシステムの数と同じである必要はありません。

また、ソースボリュームにアクセスできるのはソースサーバーのみであることに注意してください。共有ソースシステムとターゲット側のすべてのシステムはボリュームにアクセスできず、ファイルシステムの観点ではロックされています。

例: ユースケース	DR サイトでも同じレベルの可用性を提供したいユーザーは、この構成を展開して、どのサイトが In Service であっても可用性レベルが変わらないようにします。
例: ユースケース	Hyper-V クラスターが多数のクラスターノードに分散している仮想マシンで構成されている場合、災害時にリソースを利用してすべての仮想マシンを実行できるように、災害復旧サイトでも同じ数のクラスターノードが利用可能になっているようにすることが重要です。

その他の参考トピックは以下の通りです。

- 共有ボリュームとのミラーの作成
- 共有ボリュームの管理

- 共有システムの追加
- 共有システムの削除
- よくある質問

8.5.4.2. SIOS DataKeeper の設定方法

以下の手順に従って SIOS DataKeeper の使用をスタートしてください。

1. レプリケーションに使用する サーバへ接続 します。左側のペインに表示されているジョブフォルダの上で右クリックし **[サーバへ接続]** を選択するか、**[操作]** パネルから **[サーバへ接続]** を選択します。

2. ジョブを作成 します。この操作は **[操作]** パネルから、**[ジョブの作成]** を選択するか、左側のペインに表示されているジョブフォルダの上で右クリックし **[ジョブの作成]** を選択することで実行できます。

3. 新しいジョブの ミラーを作成 します。

8.5.4.2.1. SIOS DataKeeper の設定方法

SIOS DataKeeper の設定方法

以下の手順に従って SIOS DataKeeper の使用をスタートしてください。

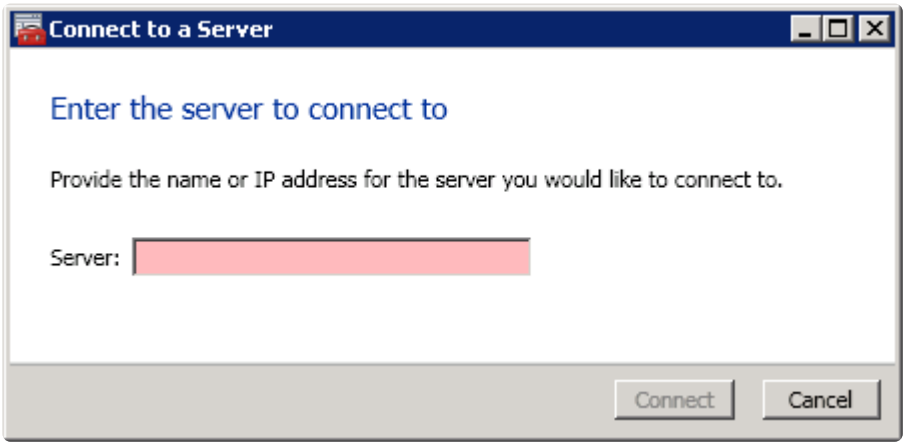
1. レプリケーションに使用する サーバへ接続 します。左側のペインに表示されているジョブフォルダの上で右クリックし **[サーバへ接続]** を選択するか、**[操作]** パネルから **[サーバへ接続]** を選択します。

2. ジョブを作成 します。この操作は **[操作]** パネルから、**[ジョブの作成]** を選択するか、左側のペインに表示されているジョブフォルダの上で右クリックし **[ジョブの作成]** を選択することで実行できます。

3. 新しいジョブの ミラーを作成 します。

8.5.4.2.2. サーバへ接続

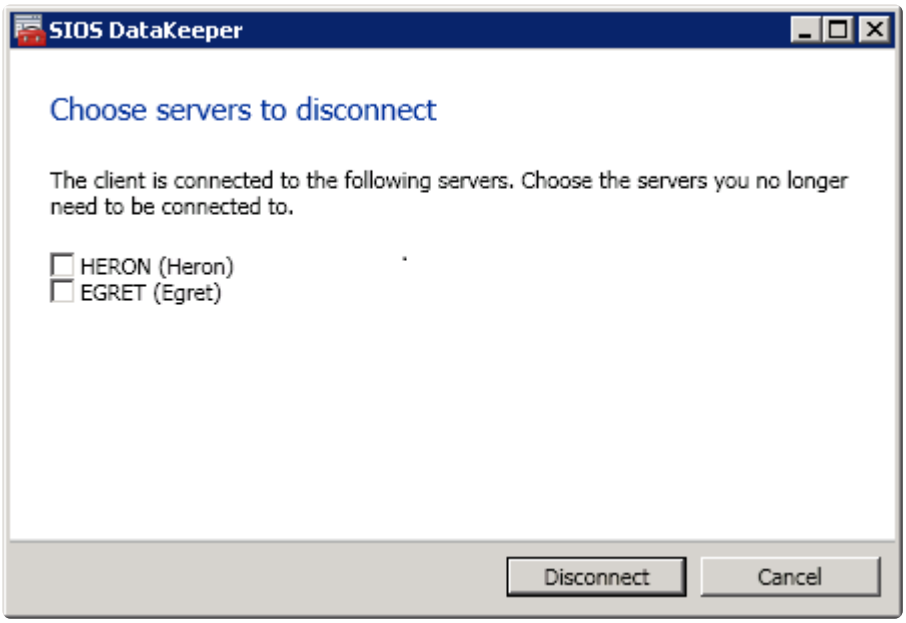
選択したサーバに接続するには、このダイアログを使用してください。サーバの IP アドレス、システム NetBIOS 名、または完全システムドメイン名を入力できます。選択するには **[接続]** をクリックしてください。



8.5.4.2.3. サーバからの切断

サーバから切断するには、このダイアログを使用します。このオプションは、管理ウィンドウにサーバを表示する必要がなくなった場合に使用できます。

サーバのリストから切断するサーバを選択して、**[切断]** をクリックしてください。



8.5.4.2.4. ジョブの作成

1. 現在接続していない場合は、ジョブ を作成したい サーバへ接続 します。

2. 右側の **[操作]** パネルから、**[ジョブの作成]** を選択します。**ジョブの作成ウィザード** が表示され、**[ジョブ名]** およびジョブの **[説明]** を入力するように求められます。

3. 適切な情報を入力して **[ジョブの作成]** を選択すると、ジョブの作成が完了します。

4. 次に新しいジョブに対する ミラーの作成 を行

8.5.4.3. ミラーの設定

ミラーの作成

共有ボリュームとのミラーの作成

共有ストレージボリュームリソースの安全な作成

複数ターゲットとのミラーの作成

複数ターゲットのスイッチオーバとフェイルオーバ

8.5.4.3.1. ミラーの作成

ミラーを作成する前に、必ず以下のことを確認してください。

- ミラーを行う ジョブを作成 している。
- ソースおよびターゲットの両方のボリュームのファイルシステムのタイプが **NTFS** である。
- ターゲットボリュームはソースボリュームより大きいまたは同等である。
- ボリュームを **ダイナミックディスク** 上に構成する場合は、ダイナミックボリュームを作成しシステムを再起動してから、ミラーの作成を続行してください (詳細については、ダイナミックディスクのミラーリング の既知の問題を参照)。
- ミラーできないボリュームを含む詳細は ボリュームの考慮事項 を参照してください。
- ミラーを作成する前にソースおよびターゲットの両方に接続している。**[操作]** ペイン内または **[ミラーを作成]** ダイアログ内の [サーバへ接続] のリンクを使用してください。

ミラーの作成

1. 右側の列の **[操作]** ペインから **[ミラーを作成]** を選択します。**[ソースの選択]** ダイアログが表示されます。
2. ソースボリュームの **[サーバ名]** を入力または選択します。この時点で、このフィールドの下にある **[サーバへ接続]** のリンクを選択し、サーバへ接続することができます。
3. レプリケーショントラフィックに使用するサブネットの **[IP アドレス]** を選択します。
4. 選択したサーバで使用する **[ボリューム]** を選択します。**[次へ]** を選択します。**[ターゲットの選択]** ダイアログが表示されます。
5. **[ターゲットボリューム]** のサーバを入力または選択します。この時点で必要に応じて、**[サーバへ接続]** を選択することができます。
6. レプリケーショントラフィックに使用するサブネットの **[IP アドレス]** を選択します。
7. 選択したサーバで使用する **[ボリューム]** を選択します。**[次へ]** をクリックします。**[詳細の設定]** ダイアログが表示されます。
8. スライドバーを使用してソースシステムからターゲットシステムにデータを送信する際の **圧縮レベル** を設定します。**注記:** 圧縮は、WAN を介したレプリケーションでの使用を推奨します。
9. ソースボリューム / ターゲットボリューム間の転送モードを選択します (非同期または同期) 。
10. レプリケーションに使用する帯域幅を制限したい場合は、転送に対する **最大帯域幅** を入力します。帯域幅を制限する必要がない場合は、デフォルト設定のままにします。**[完了]** を選択します。新しいミラーとジョブが左のツリーとメイン画面に表示されます。

注記: ミラーを作成した後、初期の状態は **[概要]** ペインで「 **再同期を保留しています** 」と表示されます。ミラーの初期の再同期が完了すると、自動的に **ミラー** の状態に変更されます。

8.5.4.3.2. 共有ボリュームとのミラーの作成

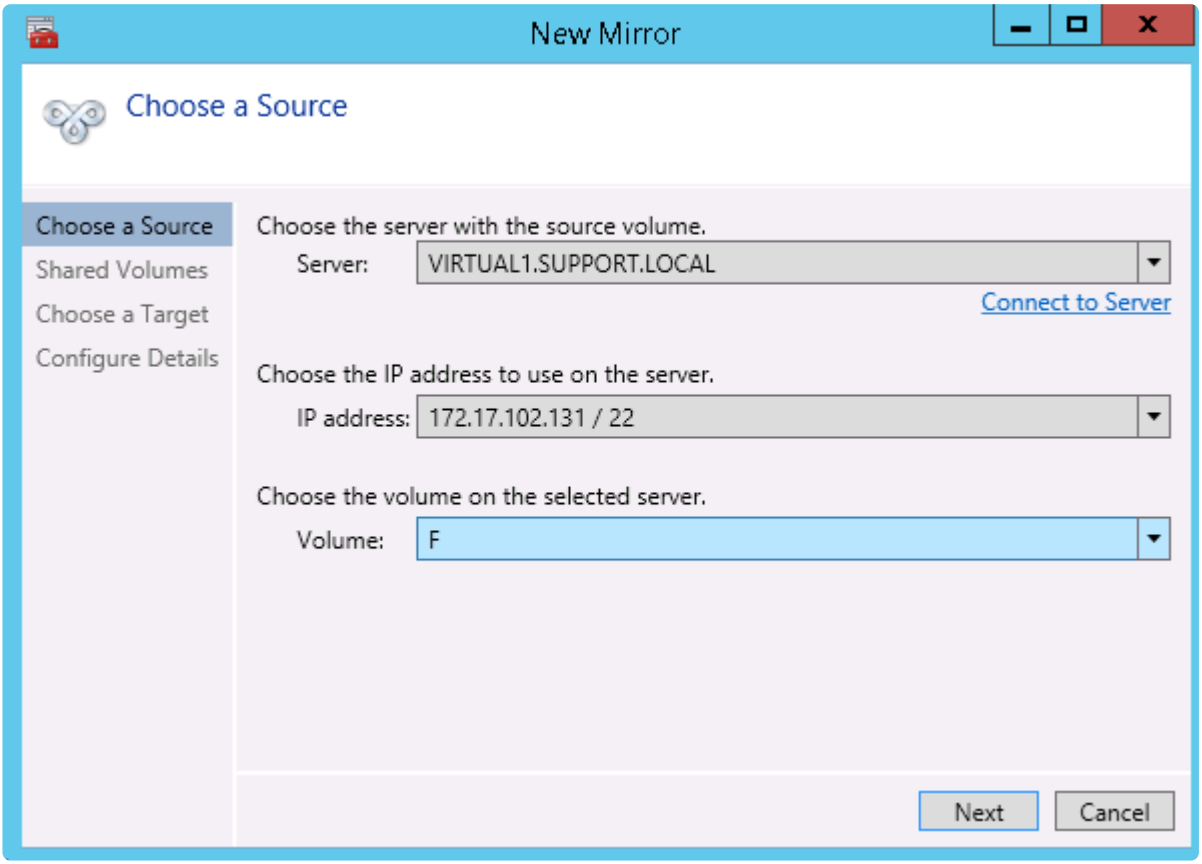
共有ボリューム構成にて DataKeeper を正しく構成するために、**DataKeeper GUI** を使用して共有ボリュームが構成されているすべてのシステムに接続する必要があります。接続されると、DataKeeper GUI は ハードウェアシグネチャを使用して、どのボリュームが共有されていて、どのボリュームが共有されていないかを自動的に検知します。

重要: GUI がシステムに接続していない場合は、システム上の共有ボリュームを検知することができません。

注記 : ダイナミックディスクは共有ストレージではサポート対象外です。ダイナミックディスク構成は各システム上のどこかに (文書化されていません) 保存されますが、ディスク自体には保存されないためです。現在 2 つのシステム間で構成を複製する方法が存在しません。

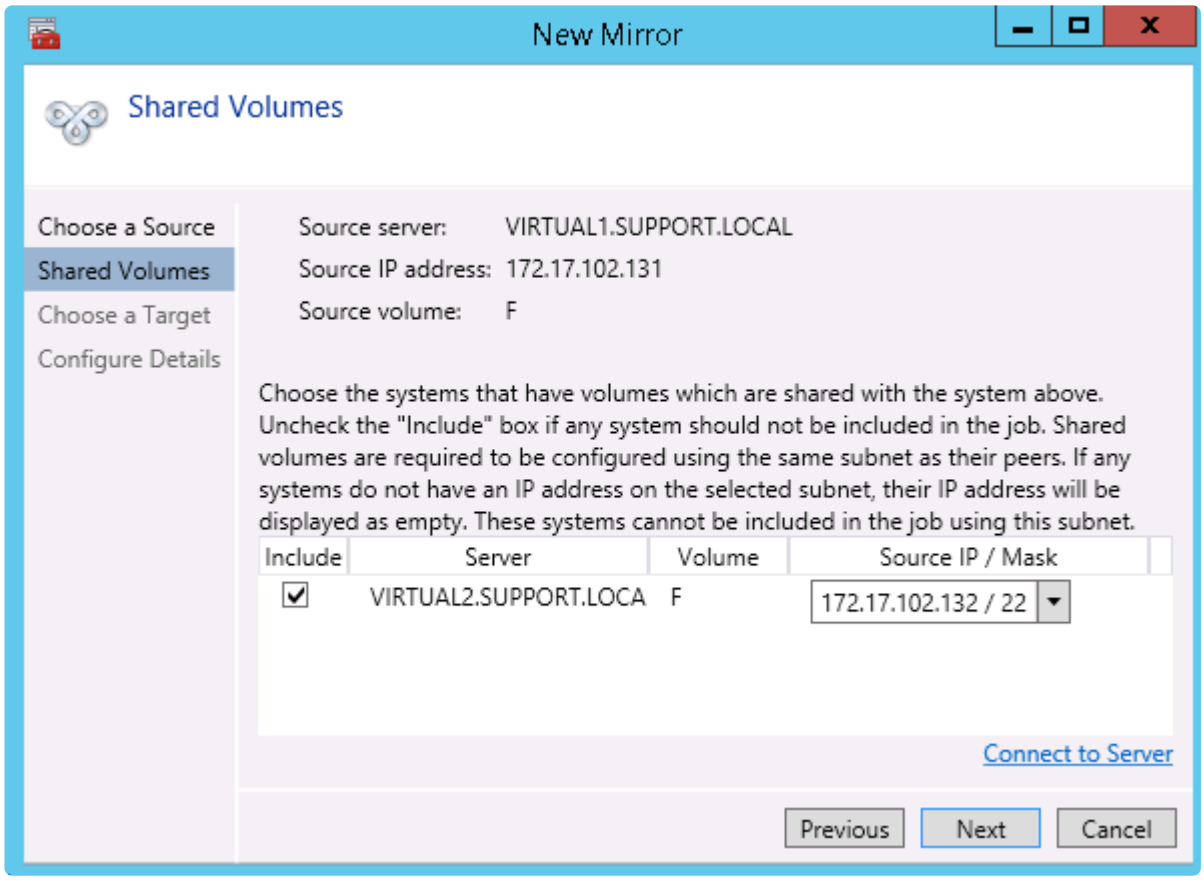
注記: DataKeeper では、複数のシステムが同じ物理ストレージにアクセスしている共有ボリューム上にミラーを作成することができます。同時アクセスを防ぐには、以下の手順を実行する前に、共有ストレージボリュームリソースの安全な作成 を参照してください。

1. **DataKeeper GUI** を介してすべてのシステムに接続します。
2. [ジョブの作成] を選択します。
3. ジョブ名とジョブの説明を定義し、**[ジョブの作成]** をクリックします。**[ソースを選択してください]** ダイアログが表示されます。



4. **[ソースシステム]** 、**[IP アドレス]** 、**[ボリューム]** を選択します。

5. **[次へ]** を選択します。**[共有ボリューム]** ダイアログが表示されます。



6. ソースシステムと共有するボリュームを持つシステムを選択します。

   注記: 共有ボリュームに接続されるすべてのシステムは同じサブネット上の IP アドレスで構成されている必要があります。該当のすべてのシステムが有効な IP アドレスを設定されるまで、**[次へ]** ボタンは有効になりません。

   該当のシステムの **[含む]** のチェックボックスのチェックをはずすことは可能なため、表示されるボリュームが本当に共有されるボリュームでないことを確認してチェックをはずしてください。(まれにしかありませんが) 2 つのボリュームが共有されていない場合であっても、それらのハードウェアシグネチャが一致することがあります。この場合は、**[含む]** チェックボックスのチェックをはずしてください。

7. **[次へ]** を選択します。**[ターゲットの選択]** ダイアログが表示されます。

8. **[ターゲットシステム]** 、**[IP アドレス]** 、**[ボリューム]** を選択します。

9. **[次へ]** を選択します。

   注記: ターゲットボリュームと共有している他のシステムにボリュームがある場合は、**[共有ボリューム]** ダイアログは次に表示されます。上記で共有するソースボリュームを構成したときのように共有するターゲットボリュームの構成を行ってください。

10. **[次へ]** を選択して続行します。**[詳細の設定]** ダイアログが表示されます。

11. スライドバーを使用してソースシステムからターゲットシステムにデータを送信する際の **圧縮レベル** を設定します。

    注記: 圧縮は、WAN を介したレプリケーションでの使用を推奨します。

12. ソースボリューム/ターゲットボリューム間の転送モードを選択します (非同期または同期) 。

13. レプリケーションに使用する帯域幅を制限したい場合は、転送に対する 最大帯域幅 を入力します。帯域幅を制限する必要がない場合は、デフォルト設定のままにします。

14. **[完了]** を選択します。新しいミラーとジョブが左のツリーとメイン画面に表示されます。

8.5.4.3.3. 共有ストレージボリュームリソースの安全な作成

DataKeeper では、複数のシステムが同じ物理ストレージにアクセスしている共有ボリューム上にミラーを作成することができます。共有ボリュームは、ミラーのソース側に作成することも、ターゲット側に作成することもできます。

注記：ダイナミックディスクは共有ストレージではサポート対象外です。ダイナミックディスク構成は各システム上のどこかに (文書化されていません) 保存されますが、ディスク自体には保存されないためです。現在 2 つのシステム間で構成を複製する方法が存在しません。

共有ストレージボリュームリソースを安全に作成するには、ボリュームに対する書き込みアクセスを持つのが、どの時点においても、1 つのシステムだけになるようにする必要があります。これには DataKeeper ミラーを作成する前も含まれます。DataKeeper はミラーを作成する前にボリュームが共有されていることを認識しないので、ボリュームが同時に 2 つ以上のシステムで書き込み可能になることがないように、手動での手順が必要になります。

ボリュームの同時書き込みアクセスを防ぐには、以下の手順を使用してください。この例では、2 つのシステム (*SYSA* および *SYSB*) が共有ストレージに接続され、3 つ目のターゲットシステム (*SYSC*) に複製されています。このストレージは 2 つのボリュームで構成されており、3 つすべてのシステムでドライブレター *E:* および *F:* を割り当てます。

1. *SYSB* の電源はオフにしたまま、*SYSA* の電源をオンにします。
2. もしインストールされていない場合は、DataKeeper をインストールします。
3. ボリュームにドライブレター *E:* および *F:* を割り当て、まだフォーマットしていない場合は NTFS でフォーマットします。
4. *SYSA* の電源をオフにします。
5. *SYSB* の電源をオンにします。
6. DataKeeper をまだインストールしていない場合はインストールして、インストール後にシステムを再起動します。
7. 共有ボリュームにドライブレター *E:* および *F:* を割り当てます。
8. コマンドプロンプトで以下のコマンドを実行して、「共有」構成フラグを設定します。

```
"%ExtMirrBase%\emcmd" . setconfiguration E 256

"%ExtMirrBase%\emcmd" . setconfiguration F 256
```

9. *SYSB* を再起動します。*E:* および *F:* ドライブがロックされて再起動します。
10. *SYSA* の電源をオンにします。*E:* および *F:* ドライブが書き込み可能になって再起動します。

11. DataKeeper GUI を使用して、*SYSA E:* (ソース) から *SYSC E:* (ターゲット) へ、また *SYSA F:* (ソース) から *SYSC F:* (ターゲット) へ、ジョブとミラーを作成 します。DataKeeper によって、*SYSB* が共有ソースシステムであることが検出されます。

    注記: WSFC を使用している場合は、WSFC で DataKeeper ボリュームリソースを作成する を参照してください。

システムの電源をオフにする代わりに、**ディスク管理** を使用して、共有物理ディスクをオフラインにすることもできます。

この手順を使用して共有ターゲットボリュームに安全にミラーを作成することもできます。上記の例では、*SYSC* から *SYSA* にミラーを作成できます。その場合、ボリューム *SYSB* は共有ターゲットになります。

3 つ以上の共有ディスクを持つサイトの場合は、同様の手順で 1 つ目のミラーボリュームに含まれていないすべての領域についてロックすることができます。

8.5.4.3.4. 複数ターゲットとのミラーの作成

SIOS DataKeeper では、シングルソースボリュームから 1 つまたは複数のターゲットボリュームへデータのレプリケーションを行うことが可能です。さらに、DataKeeper はスイッチオーバ操作を行い、任意のターゲットボリュームをソースにすることが可能です。すでに、ミラーの作成 手順でミラーを含むジョブを作成していると仮定して、以下の手順を使用して同じソースボリュームから異なるターゲットボリュームへ 2 つ目のミラーを作成してください。

1. 既存のジョブの上で右クリックします。
2. **[ミラーを作成]** を選択します。
3. 既存のミラーの **ソース** を選択します (新しいミラーのソースにもなります)。
4. 新しいミラーの **ターゲット** を選択します。
5. **[完了]** を選択します。

   次に表示されるダイアログで、DataKeeper がソースボリュームをターゲットボリュームのうちの 1 つへ正常にスイッチオーバするために必要な追加の情報について設定することになります。1 つ目のミラーを作成したとき、ソースシステムと 1 つ目のターゲットシステムとの間のネットワークのエンドポイントを指定しているはずです。また、2 つ目のミラーを作成したときソースシステムと 2 つ目のターゲットシステムとの間のネットワークエンドポイントを指定しているはずです。

   最後の設定で必要になるのは 1 つ目のターゲットシステムと 2 つ目のターゲットシステム間のネットワークのエンドポイントです。それを指定することにより、どのシステムがソースになっても問題はなく、ミラーがすべてのシステム間で正常に確立されます。

6. **[追加情報]** ダイアログで、1 つ目のターゲットシステムと 2 つ目のターゲットシステム間のミラーの作成に必要となる **ネットワークエンドポイント** を選択します。

   注記 : **この時点でミラーは作成されていません** 。DataKeeper は、ミラー作成時に使用するエンドポイントの保存のみ実行しています。

7. **[OK]** を選択します。

   注記: シングルソースボリュームを 2 つ以上のターゲットボリュームへレプリケーションしている場合は、関連するすべてのシステム間で、ミラーに対するネットワークエンドポイントを提供する必要があります。

例

3 ノード (A、B、C) - ミラーエンドポイントの定義	
作成されたミラー	**追加のミラー関係**
A → B	B → C
A → C	

4 ノード (A、B、C、D) - ミラーエンドポイントの定義	
作成されたミラー	**追加のミラー関係**
A → B	B → C B → D C → D
A → C	
A → D	

8.5.4.3.5. 複数ターゲットのスイッチオーバおよびフェイルオーバ

複数のターゲットがある構成において、以下のシナリオにおける DataKeeper の動作について理解しておくことが重要です。

- ターゲットサーバへの手動スイッチオーバ
- ソースサーバ障害によるターゲットサーバへの手動スイッチオーバ

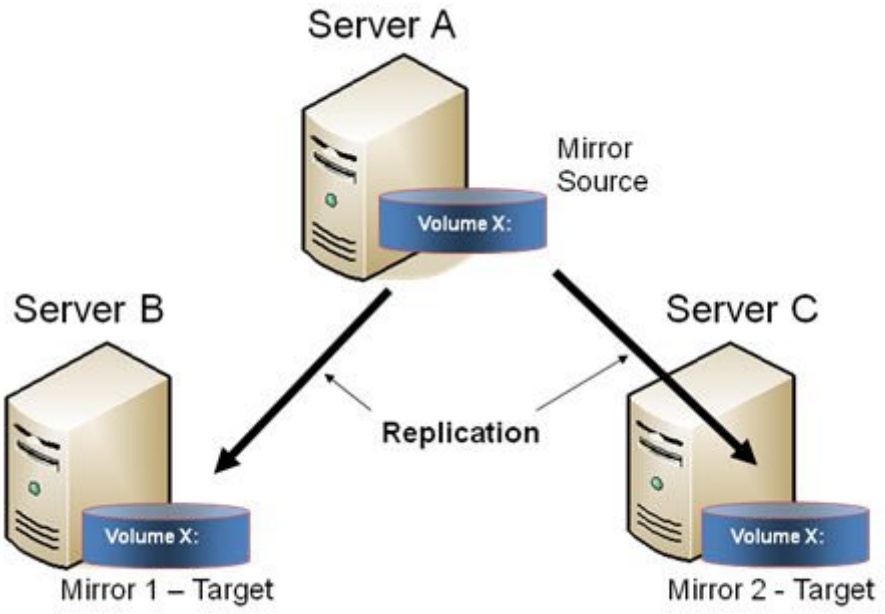
例:

以下のシナリオにおいて、3 つのサーバがあります。

- サーバ A (ソース)
- サーバ B (ターゲット 1)
- サーバ C (ターゲット 2)

2 つの独立したミラーがあり、サーバ A は 2 つの異なるターゲットボリュームをミラーリングしているので注意してください。

- ミラー 1: サーバ A → B
- ミラー 2: サーバ A → C



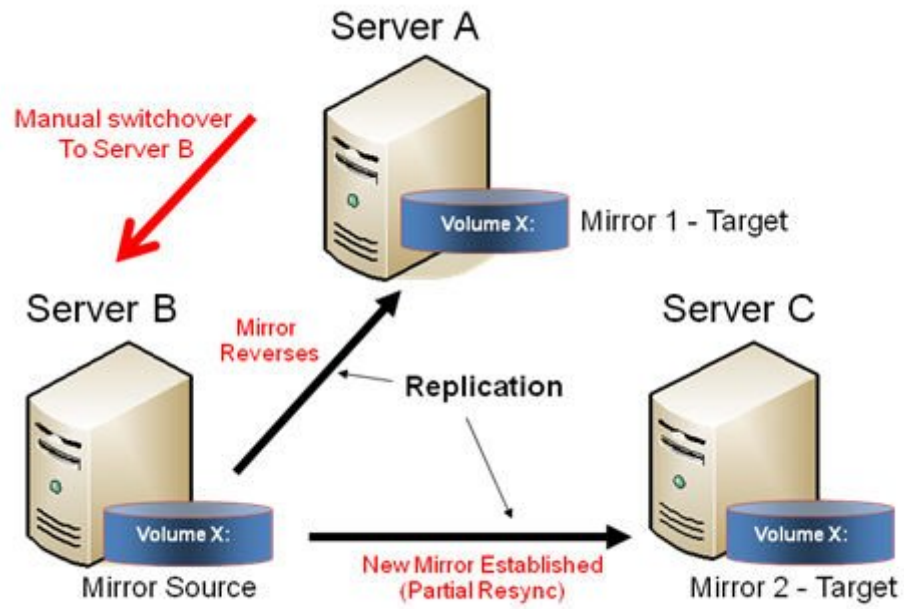
ターゲットサーバへの手動スイッチオーバ

サーバ B をアクティブ (ソース) サーバにする場合は、以下の処理が行われます。

1. 管理者は、DataKeeper UI を使用して **ミラーのスイッチオーバ** を行うことにより、サーバ B へのスイッチオーバを開始します。
2. サーバ A はソースボリューム宛のデータをすべて書き出します。
3. ミラー 1 は、いったん削除され、サーバ B からサーバ A へ再作成されます。
4. サーバ A とサーバ C 間のミラーも同様に自動的に削除されます (注記: DataKeeper GUI ではほんの数秒遅れを感じることがあります。この遅れは ネットワーク帯域 およびサーバのパフォーマンスに基づいて発生します)。
5. サーバ B とサーバ C 間に新しいミラーが確立されます。サーバ A からの インテントログ がサーバ B にコピーされます。これによりサーバ B およびサーバ C 間のデータ同期は部分再同期が要求されます。(部分再同期は新しいエンドポイントを確立するのに必要なデータのみの再同期であり、完全再同期に比べ格別に早くなります)。

結果

- ミラー 1: サーバ B → A (部分再同期)
- ミラー 2: サーバ B → C (サーバ A からのインテントログ、部分再同期)



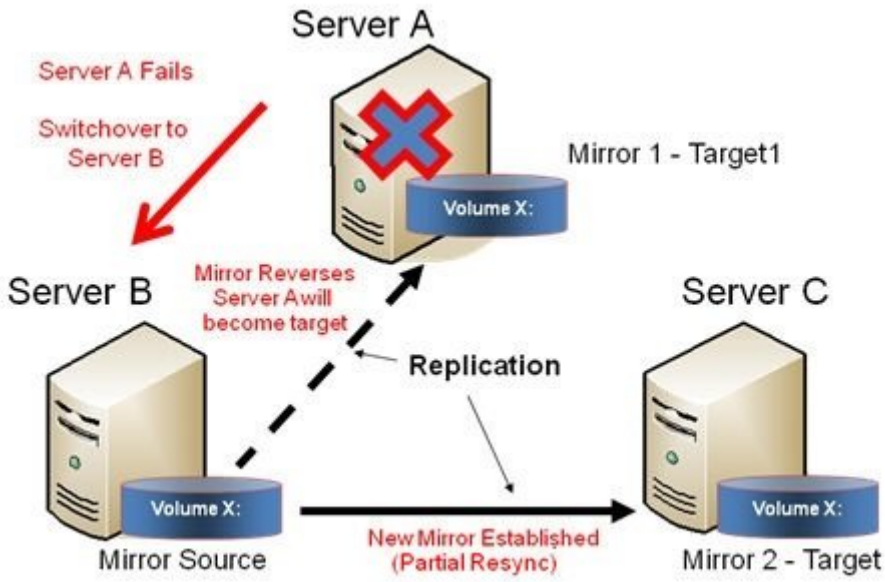
ソースサーバ障害 - ターゲットサーバへの手動スイッチオーバ

アクティブ (ソース) サーバに障害が発生した場合、DataKeeper ではサーバ B をアクティブ (ソース) サーバにすることが可能です。以下の処理が行われます。

1. サーバ A に障害が発生します。
2. 管理者は、DataKeeper UI を使用して「ミラーのスイッチオーバ」を行うことにより、サーバ B へのスイッチオーバを開始します。
3. サーバ B はローカル側のミラーを削除し、サーバ B からサーバ A へ新しいミラーを作成します。
4. サーバ A とサーバ C 間のミラーは削除されます。
5. サーバ B とサーバ C 間に新しいミラーが確立されます。
6. サーバ A が復旧したとき、サーバ A は、サーバ A がダウンしている間にサーバ B がソースとなり、自分自身が自動的にターゲットとなったことを検知します。

結果

- ミラー 1: サーバ B → A (サーバ A が復旧した場合は部分再同期)
- ミラー 2: サーバ B → C (部分再同期)



8.5.4.4. ジョブ操作

ジョブ

ジョブの名前変更

ジョブの削除

ジョブの再割り当て

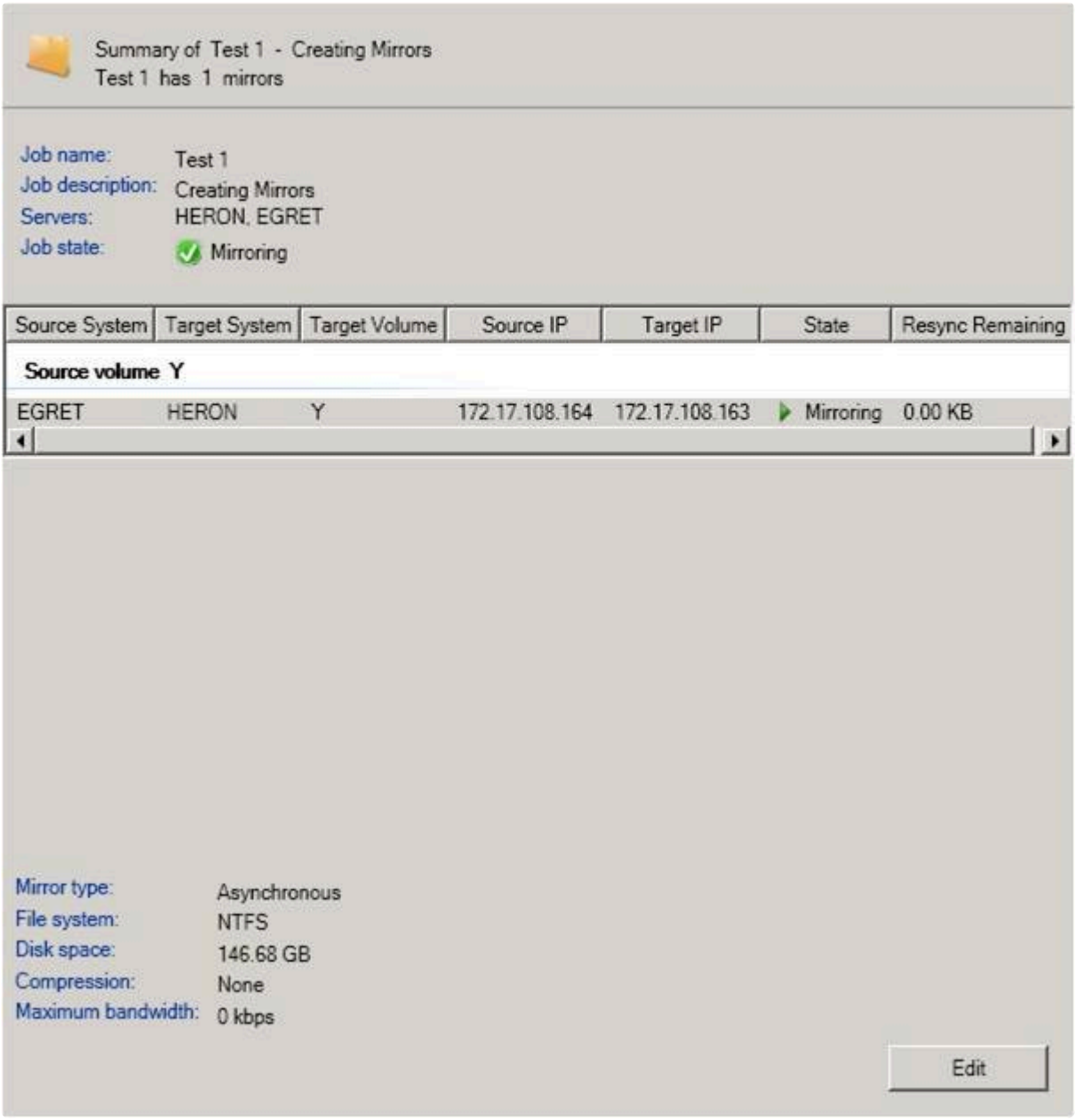
ミラーのスイッチオーバ

8.5.4.4.1. ジョブ

SIOS DataKeeper は、ジョブと呼ばれるものを使ってミラーの管理を行います。ジョブは関連するミラーおよびサーバの論理的な集合となります。このため SIOS DataKeeper のユーザインターフェースを使うことで、ジョブを作成するための複雑で反復的な作業をすばやく実行することができます。

関連するミラーは 1 つのジョブに配置する必要があります。例えば、複数のミラーで SQL Server のようなアプリケーションを保護する場合はそれぞれを同じジョブに配置する必要があります。関連しないミラーは別々のジョブに配置する必要があります。

注記: 前回のバージョンの SIOS Data Replication で作成したミラーは、個々のジョブとしてインポートされます。管理者はミラーが論理グループに集約されるよう注意してください。



8.5.4.4.2. ジョブ名の変更

1. DataKeeper のウィンドウの左側にある **コンソールツリー** のジョブを選択します。

2. **[操作]** ペインから **[ジョブ名を変更]** を選択するか、選択したジョブの上で右クリックし、表示されるメニューから **[ジョブ名を変更]** を選択します。

3. 新しい **[ジョブ名]** および **[ジョブの説明]** を入力します。

8.5.4.4.3. ジョブの削除

1. DataKeeper のウィンドウの左側の **コンソールツリー** ペインのジョブを選択します。

2. **[操作]** ペインから **[ジョブを削除]** を選択するか、選択したジョブの上で右クリックし、表示されるメニューから **[ジョブを削除]** を選択します。

3. **[はい]** を選択します。選択したジョブおよび関連するミラーが削除されます。

8.5.4.4.4. ジョブの再アサイン

ジョブの再アサイン 機能を使用すると、ミラーを削除せずにあるジョブから別のジョブへ既存のミラーを移動させることができます。

1. 中央の **[概要]** パネルからジョブを選択します。
2. 右クリックして、**[ジョブの再アサイン]** を選択するか、**[操作]** パネルから **[ジョブの再アサイン]** を選択します。
3. **[既存のジョブ]** ドロップダウンリストから既存のジョブを選択し、**[ジョブにアサイン]** ボタンを押します。中央の **[概要]** パネルに、新規にアサインされたジョブが表示されます。

注記: 既存のジョブを使用したくない場合は、このダイアログで **[新しいジョブの作成]** を選択することも可能です。

8.5.4.4.5. ミラーのスイッチオーバ

ミラーのスイッチオーバ機能では、ジョブ内のすべてのミラーまたはジョブ内のミラーのうち 1 つだけをスイッチオーバすることが可能です。「ミラー」は、標準的な単一ターゲットのレプリケーションや、複雑なジオメトリ、例えば複数ターゲットのレプリケーションや共有のノードのソースやターゲットなどを含んでいます。これらの複雑なミラー構成およびジオメトリは、実際は単一のユニットとして動作するミラーの集まりとして実装されています。

注記: ミラーは、現在のターゲットシステムにスイッチオーバする前には、**ミラーリング** の状態である必要があります。複数のターゲットが存在している構成や共有のソース / ターゲットが存在する構成におけるスイッチオーバ時の要件については、以下の **スイッチオーバ時の要件** をご参照ください。ミラーの状態を表示するには、DataKeeper GUI を使用してください。WSFC GUI では、DataKeeper GUI のような詳細な情報は提供されず、ミラーがミラーリング状態ではない場合でもリソースがオンライン (緑色) として表示されます。

1. 左側のパネルのジョブを選択します。
2. そのジョブの上で右クリックし、**[ミラーのスイッチオーバ]** を選択します。
3. ダイアログが表示され、選択したジョブまたはミラーにおいてどのノード / ホストをミラーのソースにするかを指定することになります。

   複雑なミラーの場合は、現在のミラーソースの共有グループまたは現在ミラーリング状態の有効なターゲットのうちの 1 つ、のどちらかを選択することが有効です。有効なターゲット側の共有ピアーまたは現在ミラーリング状態ではないターゲットを選択すると、エラーにより現在のミラーの状態のままになり、設定は変更されません。
4. 砂時計のアイコンが左側のパネル上に表示されます。
5. **[概要]** パネルでミラーの状態を確認することでスイッチオーバが完了したかどうかを確認することができます。

注記: **スイッチオーバ** オプションがグレイアウト (有効ではない) されている場合は、ボリュームがクラスタの保護下にあることを意味します。(Microsoft クラスタもしくは SIOS Protection Suite クラスタ)。

スイッチオーバ時の要件

設定の種類	設定例	スイッチオーバ操作	スイッチオーバ時の要件
単一ターゲット	A → B	Bへスイッチオーバ	ミラーがミラーリング状態の場合のみ可能です。
複数ターゲット	A → B (ミラーリング) A → C (一時停止)	Bへスイッチオーバ	A → B へのミラーがミラーリングの状態なので可能です。
		Cへスイッチオーバ	不可能

共有ソース / ターゲット	*S1、S2、S3 → *T1、T2 (S1 は現在のソース) (T1 は現在のターゲット)	共有ソースへスイッチオーバ (S2 または S3)	常時可能
		現在のターゲットにスイッチオーバ (T1)	ミラーがミラーリング状態の場合のみ可能です。
		共有ターゲットにスイッチオーバ (T2)	不可能 - スイッチオーバが失敗します。

8.5.4.5. ミラーの操作

ミラーの管理

一時停止およびロック解除

再開/ロック

部分再同期

中断

再同期

ミラーの削除

ターゲットの置き換え

DataKeeper ボリュームのサイズ変更

ミラープロパティ

既存のミラーの圧縮レベルの変更

8.5.4.5.1. ミラーの管理

[操作] ペインからジョブを選択し、ジョブにあるすべてのミラーの管理、またはジョブにある単一のミラーの操作を行うことができます。

ジョブを選択した後、以下の操作を実行できます。

- 全ミラーの一時停止 / ロック解除
- 全ミラーの再開 / ロック
- 全ミラーの中断
- 全ミラーの再同期
- 全ミラーのスイッチオーバ

ターゲット単位の操作 (**[操作]** ペインの下) では個々のミラーに対して実行します。例えば、2 つのミラーのジョブを持っていて、そのうちの 1 つを選択しターゲットで **[ミラーの一時停止 / ロック解除]** を選択した場合は、選択したミラーのみが一時停止します。

8.5.4.5.2. 一時停止 / ロック解除

この操作ではミラーを一時停止し、ターゲットシステム側のボリュームのロックを解除します。ボリュームのバックアップを作成する場合は、ターゲットボリュームのロックを解除します。

警告: ロック解除中のターゲットボリュームへのどの書き込みも、ミラーの再開時に失われます。

注記: ターゲットボリュームを *再配置* する場合は、新しいターゲットボリュームが作成された際にソースボリュームからターゲットボリュームへのデータの全同期を実行するために ミラーの中断 または ミラーの削除 を実行する必要があります。詳細な情報は ターゲットの再配置 を参照してください。

再開およびロック のコマンドでは、ターゲットボリュームを再ロックし、部分再同期(**またはターゲットがロック解除中に再起動かシャットダウンされた場合に完全再同期を実行します**)およびミラーリングの再開を実行します。

1. ロックを解除したいミラーを含むジョブを選択します。

2. ジョブの上で右クリックし、**[全ミラーの一時停止 / ロック解除]** を選択するか、または **[操作]** ペインから **[全ミラーの一時停止 / ロック解除]** を選択します。

3. **[はい]** を選択し、選択したジョブですべてのミラーを一時停止しロック解除を実行します。

8.5.4.5.3. 再開 / ロック

この操作によってターゲットシステム上のボリュームがロックされ、ミラーリングプロセスが再開されます。

ミラーの一時停止中、ソースシステムに対する書き込みは SIOS DataKeeper インテントログ に記録されます。**再開 / ロック** 処理を実行すると、これらの変更されたブロックは、ターゲットボリュームで変更されたブロックとともにソースからターゲットに送信され、ミラーは部分再同期 と呼ばれる方法で再同期されます。

警告: ロック解除中にターゲットボリュームに書き込んだ内容はミラーを再開すると失われてしまいます。また、一時停止およびロック解除中にターゲットシステムで再起動またはシャットダウンを実行すると、再開 / ロックが実行された場合に完全再同期が行われます。

注記: ターゲットボリュームを *再配置* する場合は、ミラーの 中断 または ミラーの削除 のいずれかが、つまりミラーの再開およびロックの代わりに **再同期** または **再作成** が必要です。詳細は ターゲットの再配置 を参照してください。

1. 再開したいミラーを含むジョブを選択します。
2. ジョブの上で右クリックし、**[全ミラーの再開 / ロック]** を選択するか、または **[操作]** パネルから **[全ミラーの再開 / ロック]** を選択します。
3. **[はい]** を選択し、選択したジョブですべてのミラーの再開とロックを実行します。
4. **[ミラー概要]** ウィンドウで、ミラーの状態が **[ミラーリング]** に変わります。

8.5.4.5.4. 部分再同期

新しいエンドポイントを確立するためだけに必要となるデータのみの再同期は、完全再同期に比べ格別に早くなります。

8.5.4.5.5. 中断

ミラーの中断は一時停止およびロック解除機能に似ています。これによってミラー処理が停止し、読み書きアクセスのターゲットボリュームがロック解除されます。違いは、**中断** 処理では DataKeeper インテントログ のすべてのビットがダーティとマークされ、ミラーを再同期してミラーリングを再開するときに、強制的に完全再同期が実行されるということです。

警告: ミラーリングの中断中には、ターゲットボリュームにデータを書き込まないでください。中断時に書き込んだデータは、ミラーの再同期時に失われます。

1. 中断したいミラーを含むジョブを選択します。
2. ジョブの上で右クリックし、**[全ミラーの中断]** を選択するか、または **[操作]** ペインから **[全ミラーの中断]** を選択します。
3. **[はい]** を選択し、選択したジョブですべてのミラーを中断します。
4. **[ミラー概要]** ウィンドウで、ミラーの状態が **[中断]** に変わります。

注記: **Resync** コマンドはターゲットボリュームを再度ロックし、**完全再同期** を実行してミラーリングの処理を再開します。

8.5.4.5.6. 再同期

このコマンドは、中断したミラーを再確立します。完全な再同期が実行されます。

1. 再同期したいミラーを含むジョブを選択します。
2. ジョブの上で右クリックし、**[全ミラーの再同期]** を選択するか、または **[操作]** タスクペインから **[全ミラーの再同期]** を選択します。
3. **[はい]** を選択し、選択したジョブですべてのミラーを再同期します。
4. **[ミラー概要]** ウィンドウで、ミラーの状態が **[ミラーリング]** に変わります。

8.5.4.5.7. ミラーの削除

この操作によってレプリケーションが終了し、関連するジョブからミラーが削除されます。ターゲットボリュームはロック解除され、完全にアクセス可能になります。

1. 削除したいミラーを含むジョブを選択します。
2. ミラーの上で右クリックし、**[ミラー削除]** を選択するか、**[操作]** ペインから **[ミラー削除]** を選択します。
3. **[はい]** を選択してミラーを削除します。
4. ミラーが削除され、関連するジョブから取り除かれます。

注記: **ミラーの削除** オプションがグレイアウト (有効ではない) されている場合は、ボリュームがクラスタの保護下にあることを意味します。(Microsoft クラスタもしくは SPS クラスタ)。

8.5.4.5.8. ターゲットの再配置

ターゲットボリュームを再配置する場合は、ターゲットボリュームが再配置された際にソースボリュームからターゲットボリュームへのデータの完全再同期を実行するために ミラーの削除 を実行する必要があります。ミラーを削除すると、レプリケーションが終了してジョブからミラーが削除されるので、新しいターゲットを使用してミラーを再作成すると、完全再同期が実行されます。

削除コマンドを使用する

1. 再配置するターゲットを含むミラーを選択します。
2. ミラーの上で右クリックし、**[ミラー削除]** を選択するか、または **[操作]** タスクペインから **[ミラー削除]** を選択します。
3. **[はい]** を選択してミラーを削除します。
4. 新しいターゲットが配置されたら、ミラーを再作成 します。

8.5.4.5.9. DataKeeper ボリュームのサイズ変更

DataKeeper では、ミラーの設定を行う際、動的にDataKeeper ボリュームを拡張および縮小することが可能です。一旦サイズ変更が完了すると、部分同期が実行されます。

注記: サイズ変更は、一度に 1 つのボリュームでのみ実施する必要があります。

> **警告:** DataKeeper for Windows v7.4以前のバージョンでサイズ変更をしないでください。

制限

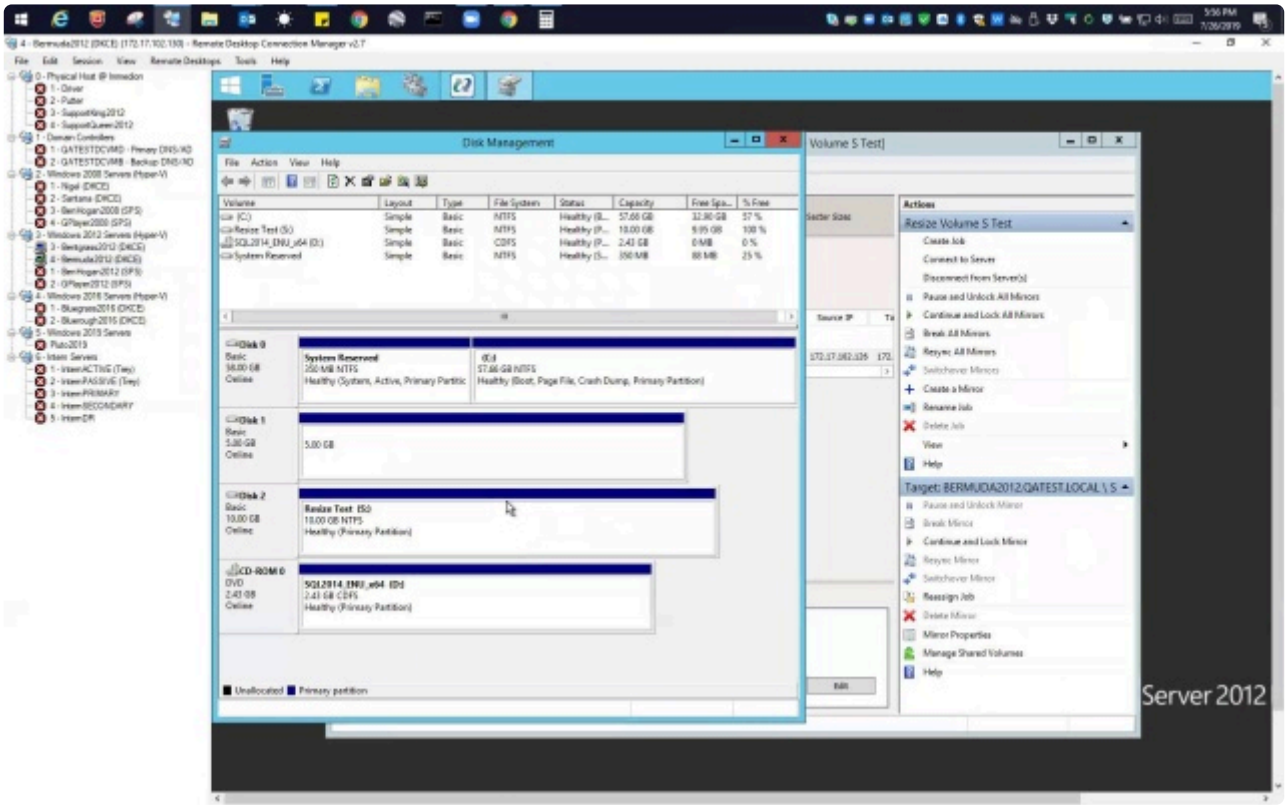
- DataKeeper はミラー対象のボリュームが存在する物理ディスクのディスクの種類を変更することはサポートされていません (たとえば **ベーシックディスク** から **ダイナミックディスク** — ダイナミックディスクを作成する前にミラーを削除する必要があります)。
- DataKeeper はパーティションのサイズ変更を行うサードパーティ製品をサポートしていません。
- DataKeeper は、**ダイナミックディスク** 上に構成される共有ボリューム上のボリュームのサイズ変更をサポートしません。Windows での共有ダイナミックディスクの使用には信頼性において問題があります。

非共有ボリュームの場合

以下の手順を使用するためのサンプル構成には、次のものが含まれます。

- ディスクからディスク
- 1 対 1
- 1 対多
- 多対 1

非共有ボリューム構成で DataKeeper ボリュームをサイズ変更するには、以下の手順を実行します。



参考動画（英語）

v8.7.2 より、DataKeeper はサイズ変更されるミラーを手動で一時停止しない場合、自動的にミラーを一時停止します。

1. DataKeeper UIの ミラーの一時停止 / ロック解除 オプションを使用して全ミラーを一時停止し、全ターゲットボリュームのロックを解除してください。

2. **Windows ディスクの管理** ユーティリティを使用して **サイズ変更ウィザード** で **[ボリュームの拡張]** もしくは **[ボリュームの縮小]** を選択して、ソースシステムでボリュームサイズを拡大 (オペレーティングシステムにおいて可能な場合は縮小) します。**サイズ変更が完了して確認されたら、ターゲットシステムをサイズ変更します。各ターゲットの未処理ボリュームサイズがソースボリュームのサイズ以上であることを確認してください。**

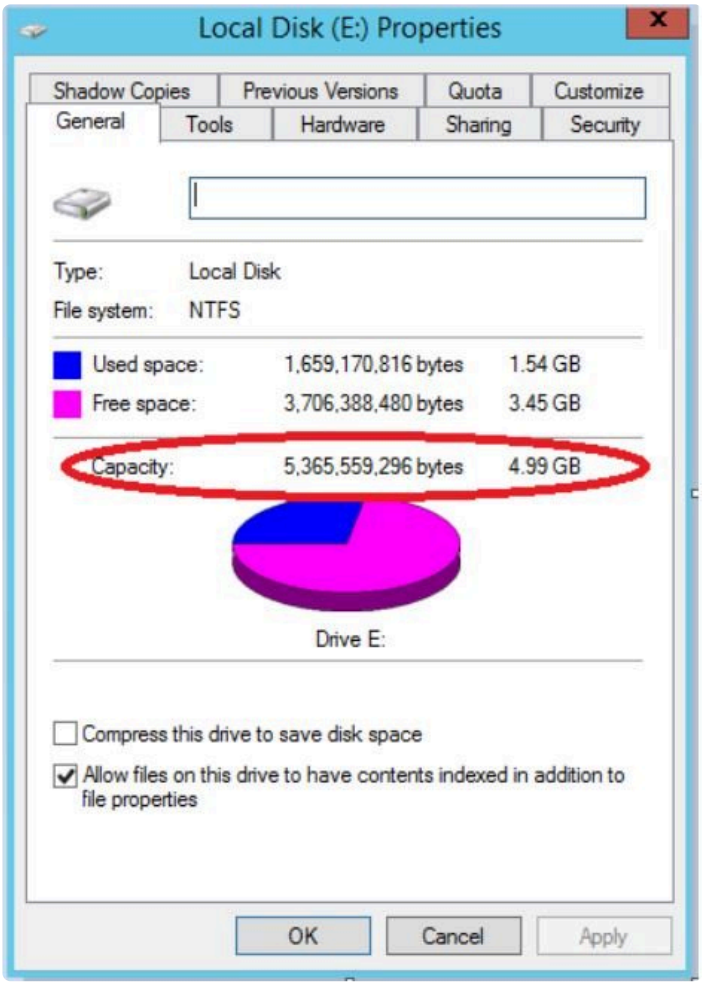
   注記: Windows ディスクの管理ユーティリティは、ドライブ数に基づいてターゲットノードで開始する場合、より長い時間がかかります。ボリュームがロックされている場合、Windows オペレーティングシステムには、エラー条件の再試行が組み込まれているため、「ロックされた」ターゲットノードで開始する際の速度が影響を受けます。

   注記: ソースとターゲットのサイズを変更した後、ディスク管理で再スキャンを実行してください。次にクラスタ内の各システムで以下のコマンドを実行し、DataKeeper が新しいボリュームサイズを認識するようにします。

   - コマンドプロンプトを起動します（管理者として実行）
   - cd extmirrbase

- emcmd . updatevolumeinfo <enter-volume-letter>

3. ディスクの管理で「ロック解除された」ドライブを表示して、サイズを確認してください。合計容量（単位：バイト）は、ソースとターゲットで等しいか、ターゲットがソースよりも大きくなければなりません。



4. ボリュームのサイズ変更後、ミラーの 再開 / ロック を行ってください。ミラーリング処理が再開され、部分同期が発生します。

共有ボリュームの場合 – ベーシックディスク

このサイズ変更手順は、**ベーシックディスク** 上に “共有ボリューム” が構成されている場合に適用できます。以下の手順を使用するためのサンプル構成には、次のものが含まれます。

> 共有ボリューム – 複数のシステムが同じ物理ストレージにアクセスできます。この共有ボリュームは、ミラーのソース側、ターゲット側のどちらにあっても構いません。

- 共有ディスクを単体のディスクにレプリケーションする構成
- 共有ディスク同士でレプリケーションする構成
- N 個の共有ディスクターゲットへレプリケーションされる N 個の共有ディスク構成

ディスク上のフリーディスクがある場合は、ボリュームを別のスペースで使用するために拡張することが可能です。

1. DataKeeper UIの ミラーの一時停止 / ロック解除 オプションを使用して全ミラーを一時停止し、全ターゲットボリュームのロックを解除してください。

2. すべての共有ソースまたは共有ターゲットシステムをシャットダウン (電源オフに) します。(**注記:** 現在のソースと現在のターゲットシステムはシャットダウンしないでください。)

3. 上記の非共有ボリュームの場合の手順にしたがってボリュームサイズを変更してください。

4. サイズ変更後、ミラーの 再開 / ロック を行ってください。

5. 共有システムの電源をオンにします。新しいボリューム構成が自動的に認識されます。

エラー処理

1. ミラーの **再開とロック** を実施後、GUIが長時間「 **一時停止** 」状態のままの場合は、ソースとターゲットノードの両方でシステムログを確認してください。

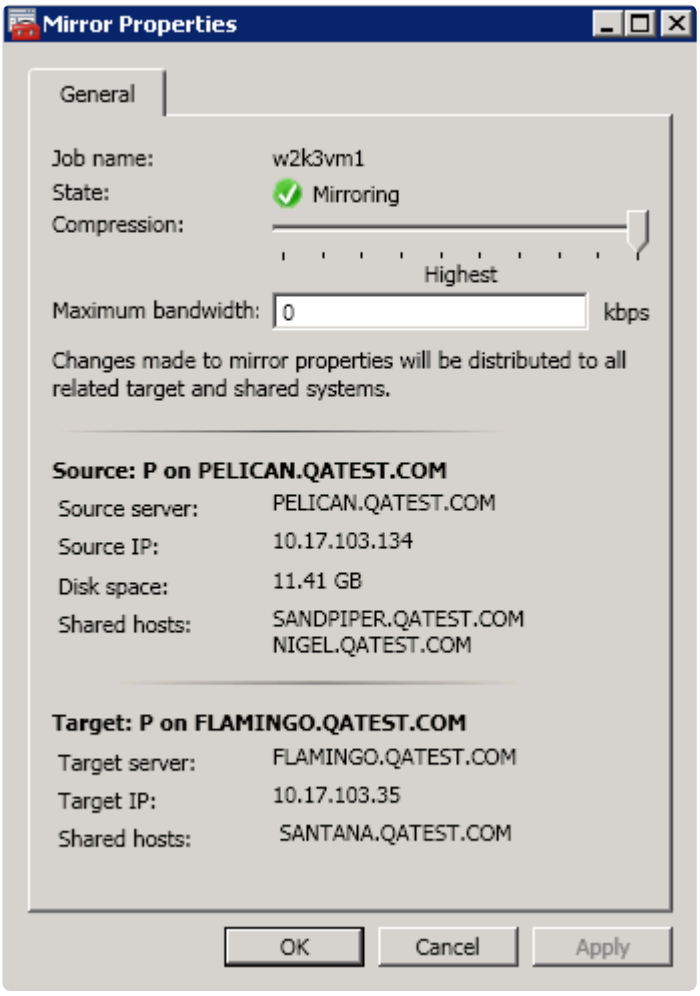
2. DataKeeper は、ターゲットボリュームがソースボリュームよりも小さい場合にミラーの同期が開始されるのを防ぎます。UNLOCKVOLUME コマンドを介して、システムログがそのようなエラーを表示した場合、ターゲットのボリュームサイズがソースボリュームのサイズ以上であることを確認し、ボリュームを再びサイズ変更する必要があります。その上で、上記の再開 / ロック手順に進みます。

3. ミラーを継続している DataKeeper は、新しいボリュームサイズを使用してビットマップファイルおよびインメモリビットマップバッファの割り当てをしなおします。ソースもしくはターゲットに十分なメモリリソースがないため DataKeeper がビットマップバッファの割り当てに失敗した場合、ミラーは、全同期を必要とする‘ **中断** ‘状態となります。

4. 一旦ボリュームのサイズ変更が開始されると、サイズの変更機能を元にもどす手段はなく、DataKeeper に関連するエラー処理は、ビットマップファイルおよびインメモリビットマップバッファの配置しなおしが必要となります。配置のしなおしに失敗するとミラーが中断され、強制的に全同期が発生します。

8.5.4.5.10. ミラープロパティ

[ジョブの概要] ペインのジョブを選択し、右クリックして **[ミラープロパティ]** を選択してください。



このダイアログはジョブ、ソースシステム、ターゲットシステムに関する以下の情報を表示します。

- **ジョブ名**
- **ステータス** (ジョブの現在の状態、例: アクティブ)
- **ソースシステム**
  - サーバ - ソースサーバの名前
  - ソース IP - ソースサーバの IP アドレス
  - ディスク空き容量 - ソースボリュームの容量
  - 共有ホスト - 共有ストレージを介してこのボリュームへアクセスする別のシステム
- **ターゲットシステム**
  - サーバ - ターゲットサーバの名前
  - ターゲット IP - ターゲットサーバの IP アドレス

[ミラープロパティ] ダイアログでは、次の設定を修正することができます。

- 圧縮レベル - 特定のミラーに対して圧縮レベルを指定します。圧縮レベルは、[Lowest] から [Highest] まで設定できます。**[Medium low]** に設定することを推奨していますが、テストを行いネットワーク環境に適した

設定を行ってください。なお、転送速度が 100 Mbps より大きい場合、圧縮を行う必要はありません。

注記: 圧縮レベルの設定変更を行った場合は、**[ミラープロパティ]** 画面に表示されているすべてのシステムに対して自動的に反映されます。

- 最大帯域 - 特定のミラーに使用するネットワークの帯域幅の最大値を指定します (キロビット/秒)。0 は「制限なし」という意味です。

注記: A がソース、B および C がターゲットのマルチターゲット構成においては、B または C がソースとなるまで B-C 間のミラーのプロパティを構成できません。

8.5.4.5.11. 既存のミラーの圧縮レベルの変更

ミラーの圧縮レベルは、ミラー作成時に設定され、そのミラーだけに適用されます。

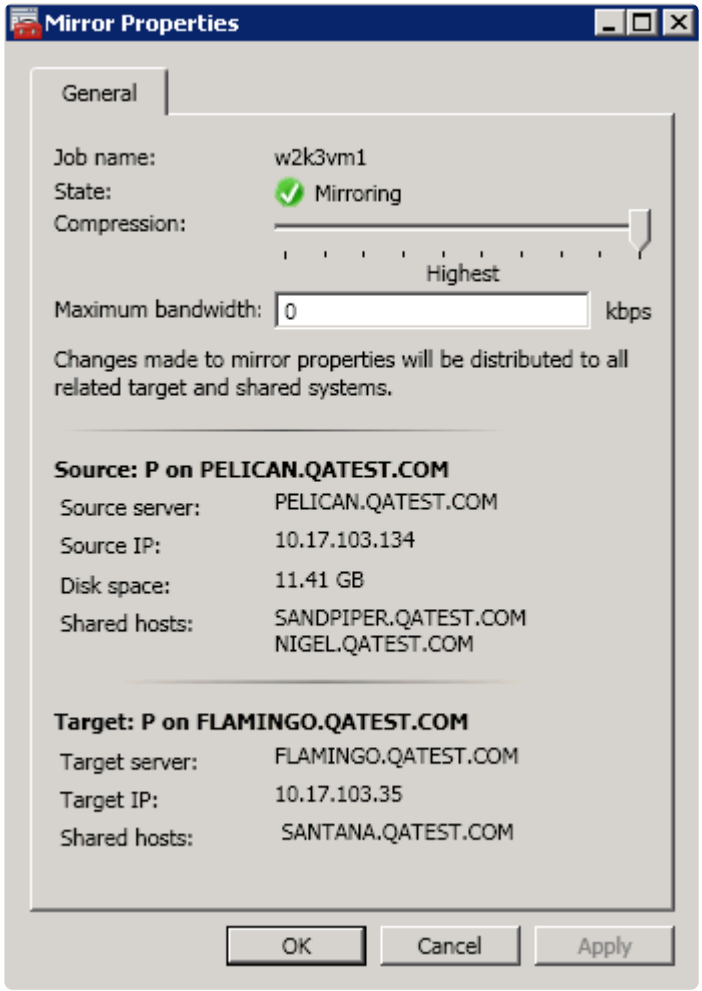
既存のミラーの圧縮レベルを変更するには、DataKeeper GUI 内からミラーのプロパティを編集してください。

1. ミラーを選択して **[編集]** をクリックします。

2. スライダボタンをドラッグして、圧縮レベルを変更します。

値は [Lowest] から [Highest] まで変更できます。[Medium low] に設定することを推奨していますが、テストを行いネットワーク環境に適した設定を行ってください。

また、ダイアログのコメントのとおりにパラメータを変更すると、[ミラープロパティ] 画面にリストされるすべてのシステムに圧縮プロパティが反映されることにも注意してください。



8.5.4.6. 共有ボリュームの操作

共有ボリュームの管理

共有システムの追加

共有システムの削除

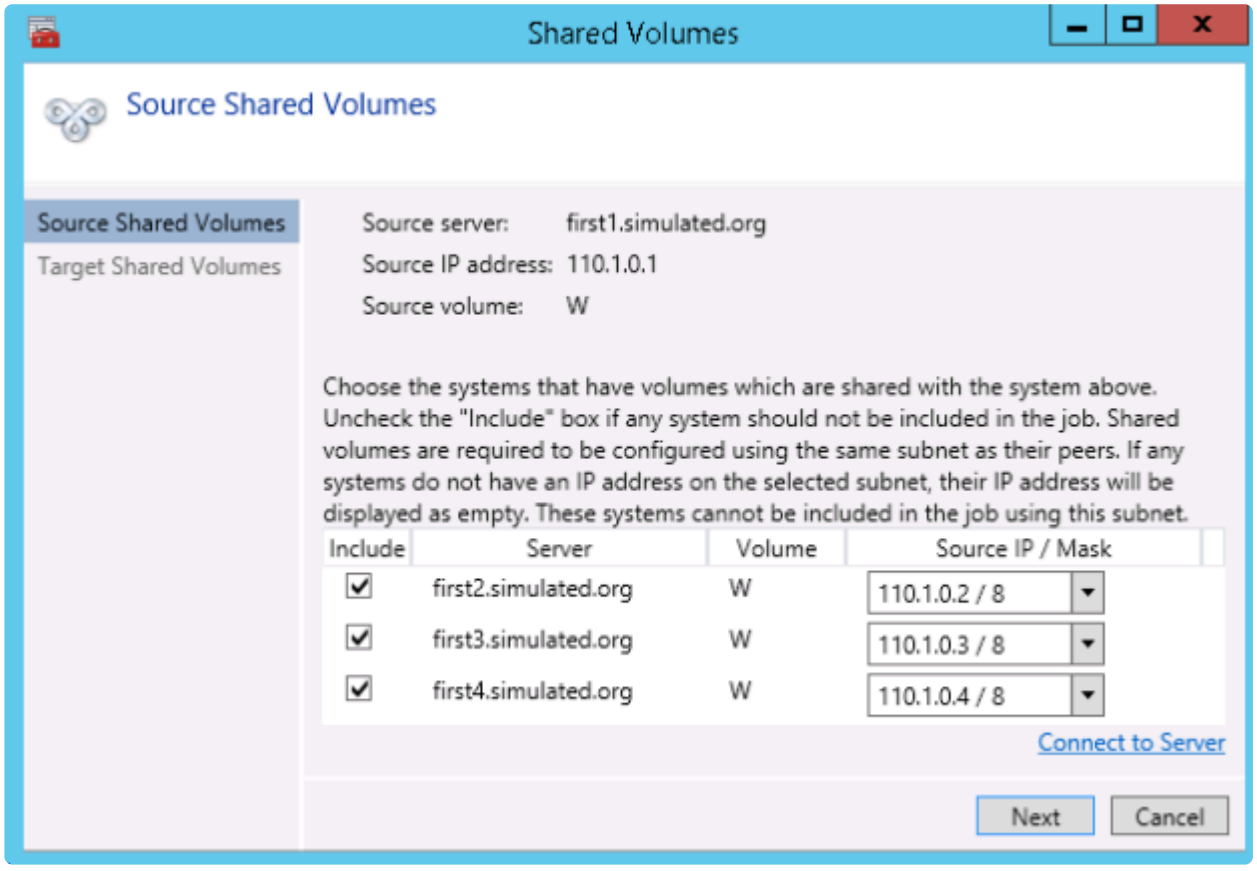
8.5.4.6.1. 共有ボリュームの管理

ミラーの作成後から、DataKeeper では共有ボリュームの管理を行うことができます。DataKeeper GUI の **[共有ボリュームの管理]** を選択することにより、ミラーされているボリュームを共有している 別のシステムをジョブに追加する ことができます。また、ジョブから 共有システムを削除する ことも可能です。これらのシステムはミラーのソースまたはターゲットのどちらかに存在することができます。

ミラーのソースまたはターゲット側でミラーされているボリュームを共有しているシステムを追加または削除したい場合は、管理したいジョブを選択し、編集対象のボリュームを含むミラーをハイライトしてください。

ボリュームが 1 つまたは複数のターゲットに対してミラーされていてミラーのソース側の共有システムを追加または削除したい場合、それらすべてが同じソースボリュームを参照しているため、どのミラーでも選択可能です。そのミラーに対して **[共有ボリュームの管理]** を選択すると、**[共有ボリューム]** のダイアログが表示されます。

ミラーのターゲット側の共有システムを追加または削除したい場合は、特定のミラーを指定する必要があります。



8.5.4.6.2. 共有システムの追加

ミラーのソースまたはターゲットのどちらかに共有システムを追加する場合は、そのシステムに接続している必要があります。**[共有ボリュームの管理]** ダイアログを開始する前にシステムに接続するか、そのダイアログ内の **[サーバへ接続]** をクリックすることでシステムへの接続が可能です。このどちらかの場合において、ソースまたはターゲットボリュームのどちらかに一致するシステムに存在する共有ボリュームがある場合は、ダイアログの中でそのシステムとそのシステムに一致する IP アドレスが表示されます。このジョブの設定においてそのシステムを含む場合は **[含む]** チェックボックスはチェックしたままで、そのシステムで使用する正しい IP アドレスを選択してください。

共有システムで既存のミラーシステムと IP アドレスのサブネットが一致しない場合、[IP アドレス] の欄が空欄になり、**[含む]** チェックボックスのチェックがはずれた状態になります。そのサブネット上に IP アドレスを設定するためにシステムの再設定が必要になります。再度共有ボリュームの追加を行ってください。

新しい共有システムを追加した後 **[完了]** をクリックすると、ジョブに追加されます。複数のミラーが存在している場合は、新規に追加されたシステムとその他すべてのターゲット間で使用するネットワークアドレスを設定することになります。

8.5.4.6.3. 共有システムの削除

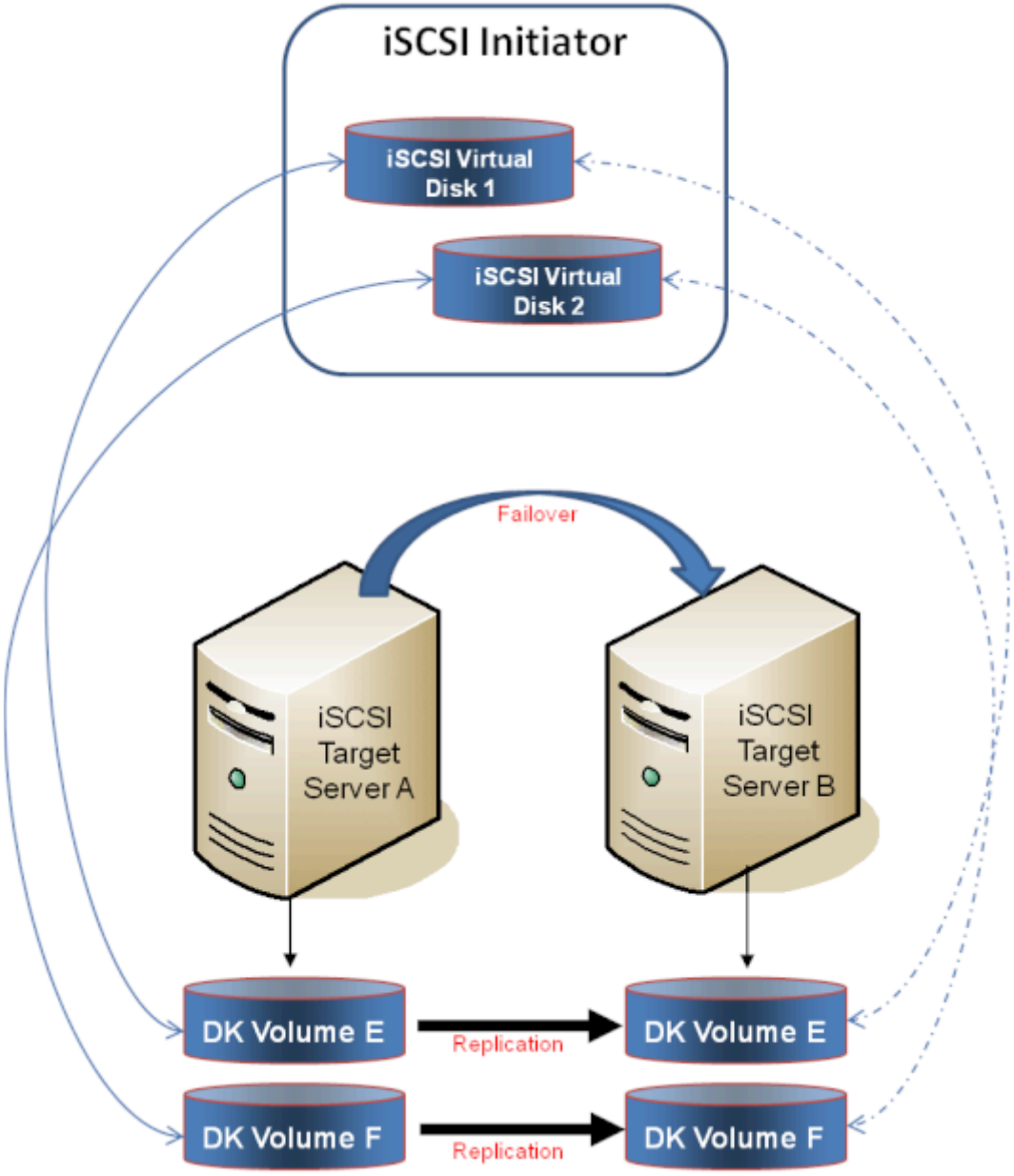
共有システムからミラーの片側を削除する場合は、**[共有ボリュームの管理]** ダイアログを起動し、削除したいシステムの **[含む]** チェックボックスからチェックをはずしてください。**[完了]** をクリックすると、ジョブが更新され、そのシステムがジョブから削除されます。

警告: 共有システムをミラーのソース側から削除した場合、その時点でソースボリュームは複数のシステムでアクセス可能となります。ソースボリュームは同時アクセスが可能となるため、同時アクセスによるデータ破壊をまねく恐れがあります。

8.5.4.7. Windows Server 2012 上での Microsoft iSCSI ターゲットと DataKeeper の使用

以下のトピックでは、ユーザインターフェースを使用してMicrosoft iSCSI ターゲットと DataKeeper を設定する手順を説明します。

> **注記:** この設定は、VMware ESX 環境ではサポートされません。



---

iSCSI ターゲットのインストール

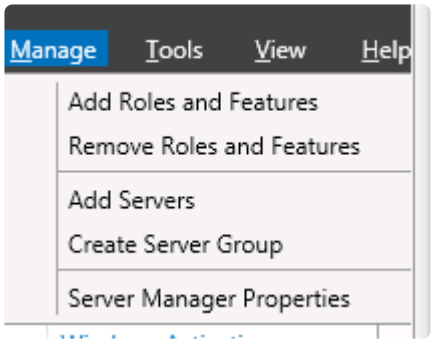
ミラー作成とクラスタ構成

iSCSI 仮想ディスクの作成

iSCSI Initiator のセットアップ

8.5.4.7.1. iSCSI ターゲットのインストール

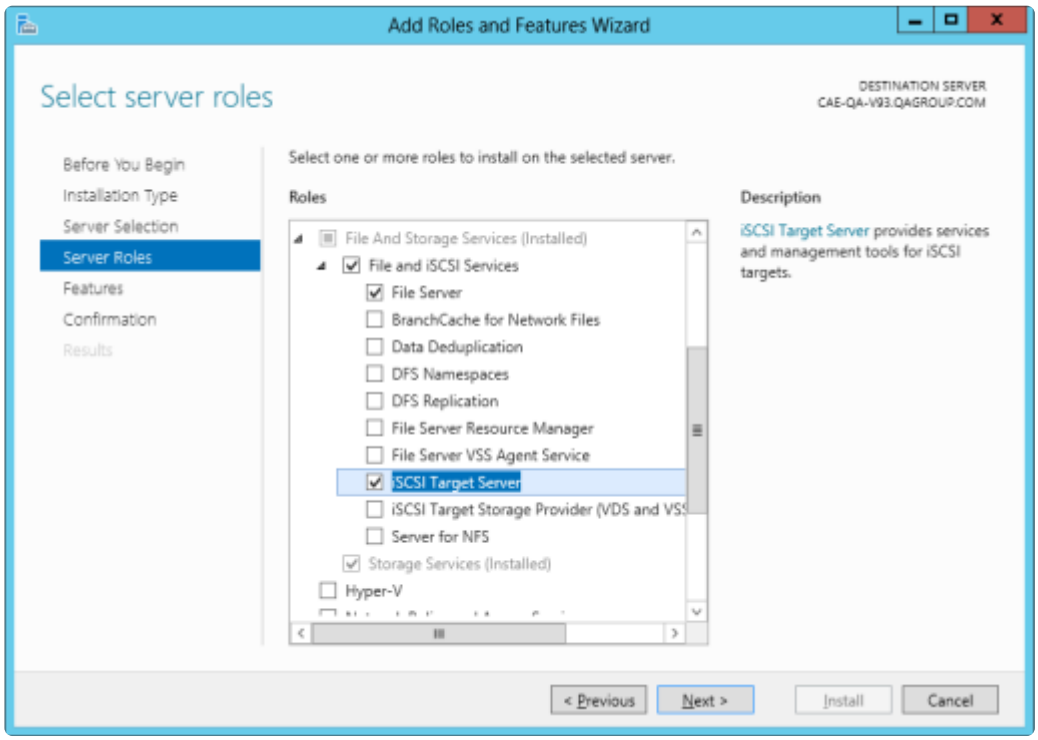
1. **Server Manager** のメニューの **[管理]** ドロップダウンから **[役割と機能の追加]** を選択してください。



2. **[役割ベースまたは機能ベースのインストール]** オプションを選択してください。

3. 表示されたサーバのリストから、適切なサーバを選択してください。

4. **[サーバの役割の選択]** 画面の **[サーバの役割]** で、**[ファイルサービスおよび iSCSI サービス]** / **[iSCSI ターゲットサーバ]** を選択してください。**注記: [ファイルサービスおよび iSCSI サービス]** はツリー階層にあり、通常はグレー表示で見つけにくい **[ファイルおよびストレージサービス]** の下にあります。



5. **[次へ]** を 2 回クリックし、表示された **[インストール]** ボタンをクリックして役割をインストールしてください。

6. インストールが開始され、進行状況が表示されます。

7. インストールが完了すると、メッセージ「 **インストールが正常に完了しました** 」が表示されます。

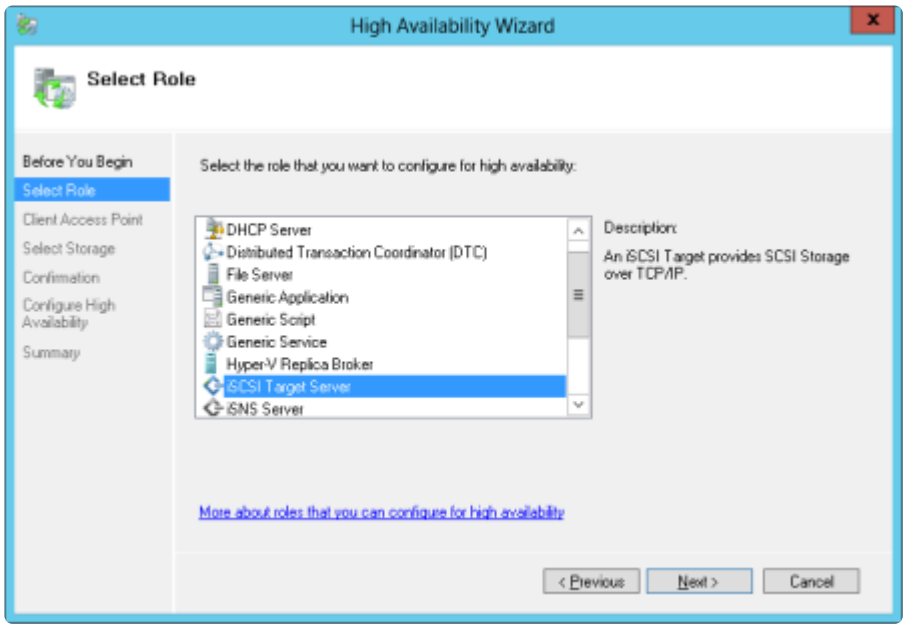
8. クラスタ内のすべてのサーバについて、上記の手順を繰り返してください。

8.5.4.7.2. ミラーの作成とクラスタの構成

1. **DataKeeper ボリューム** と **クラスタ** を作成してください。参考として、WSFC で DataKeeper ボリュームリソースを作成する を参照してください。

> **重要:** iSCSI ターゲットの役割は、**ベーシックディスク** 上に配置した **シンプルボリューム** のミラーである DataKeeper ボリュームのみをサポートします。いずれかのミラーが、ソースシステムまたはターゲットシステムのダイナミックディスク上にあるストライプボリュームまたはスパンボリュームを使用している場合、これらの DataKeeper ボリュームをストレージ用に使用する iSCSI ターゲットの役割を作成することはできません。

2. **Windows Failover Cluster Manager UI** (cluadmin.msc) から **[役割の構成]** を選択し、画面に移動して **iSCSI ターゲットの役割** を選択してください。

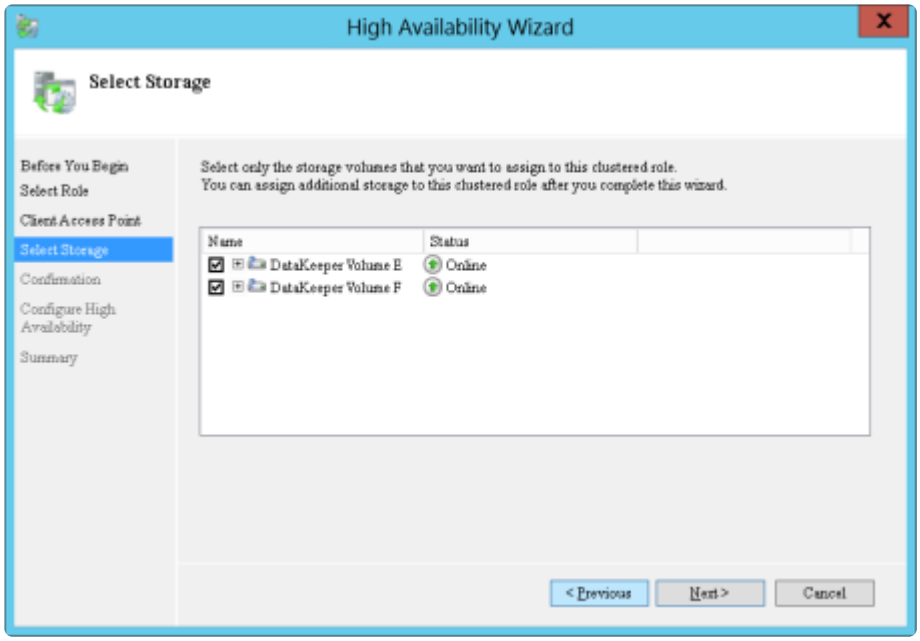


3. **iSCSI ターゲットサーバ** の役割を選択し、**[次へ]** を選択してください。

4. **[クライアントアクセスポイント]** ページが表示されます。iSCSI ターゲットサーバインスタンスの **クライアントアクセスポイントの名前** と **IP アドレス** を入力してください。

> **重要:** この名前と IP アドレスは、後でクライアントがサーバのアドレスにアクセスするために使用するので、DNS に記録する必要があります。これは、サーバがこれらの名前を解決できるようになるために非常に重要です。

5. **[ストレージの選択]** ダイアログで、**DataKeeper ボリューム** を選択してください。



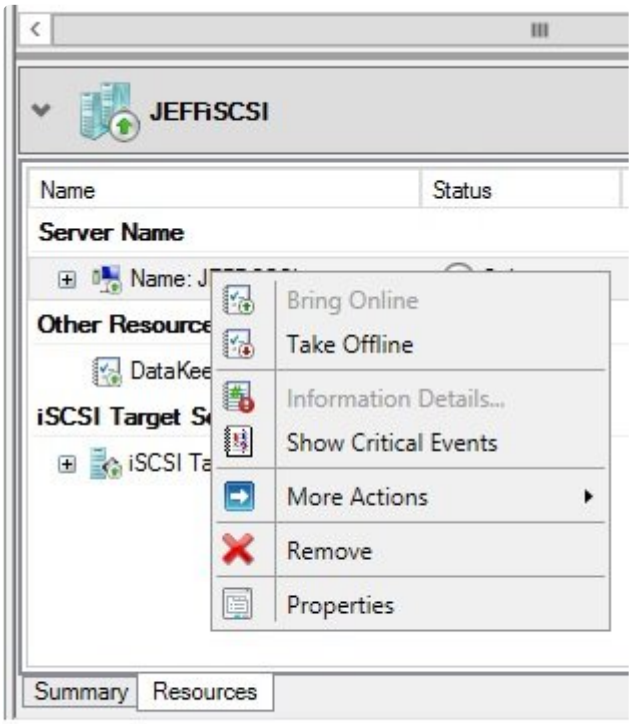
6. 以降の画面で、構成を完了できます。

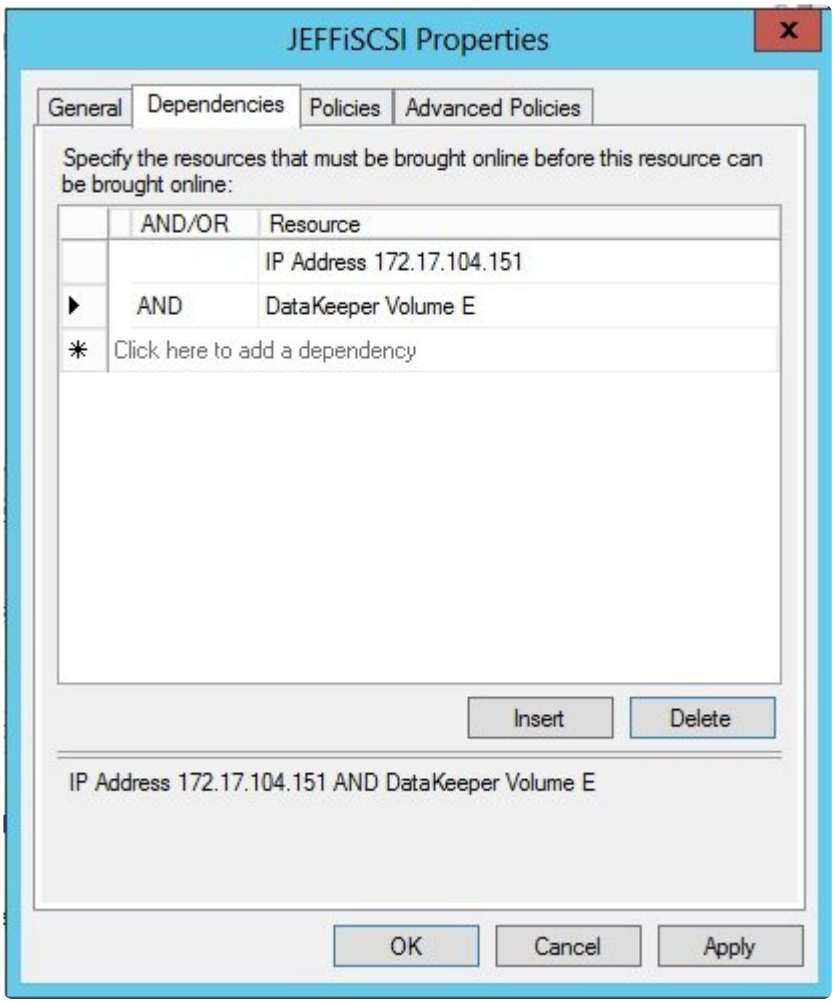
7. 設定後、**Failover Cluster UI** から、DataKeeper ボリュームの依存関係を追加します。

   a. 左側のペインにある **[役割]** をクリックし、次に上部中央のペインにある **iSCSI ターゲットサーバ** のリソースをクリックします。

   b. 下部中央のペインにある **[リソース]** タブをクリックし、次に **[サーバ名]** 見出しの下にある **[名前: <クライアントアクセスポイント名>]** を右クリックして **[プロパティ]** を選択します。

   c. **[依存関係]** タブをクリックし、依存関係として適切な DataKeeper ボリュームを追加します。



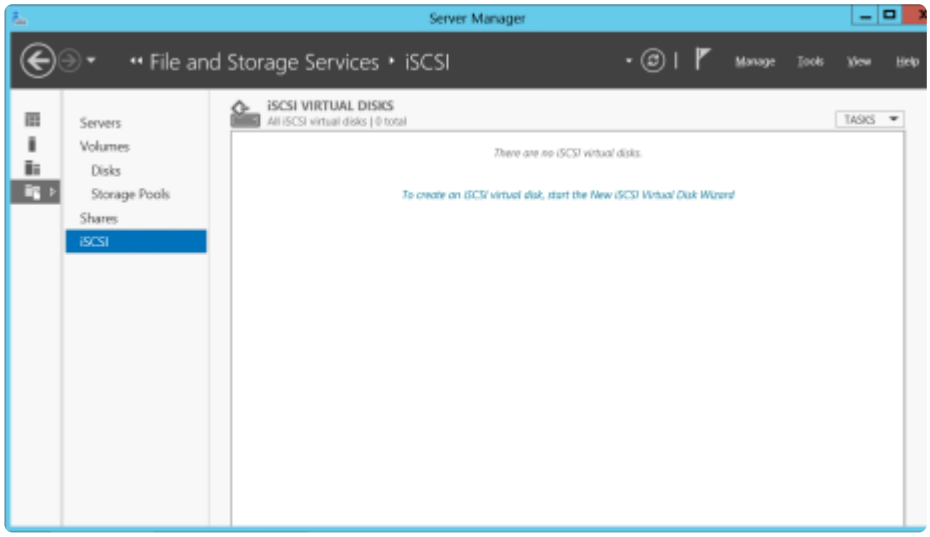


8. 設定は完了です。[iSCSI 仮想ディスク] の設定に進んでください。

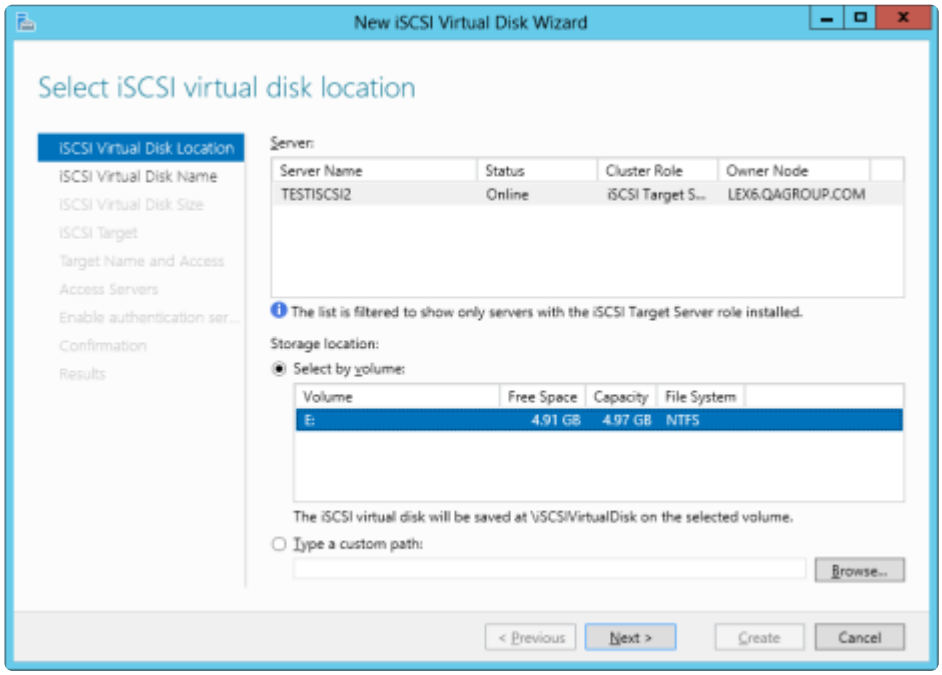
8.5.4.7.3. iSCSI 仮想ディスクの作成

その時点で iSCSI ターゲットサーバがオンラインであるプライマリサーバ で、以下の操作を行ってください。

1. **Server Manager** の **[ファイルおよびストレージサービス]** に移動し、**[iSCSI]** を選択してください。**[iSCSI 仮想ディスクを作成するには、*新しい iSCSI 仮想ディスクウィザード* を起動してください]** のリンクをクリックしてください (または、画面の右上にある **[タスク]** ドロップダウンメニューから **[新しい iSCSI 仮想ディスク]** を選択)。**注記:** Windows Server 2012 **Server Manager** は、ユーザへの情報の表示や更新に時間がかかります。



2. **新しい iSCSI 仮想ディスクウィザード** に、サーバとボリュームが表示されます。**DataKeeper ボリューム** を選択し、**[次へ]** をクリックします(注記: サーバ名は 前の手順 で作成した名前であり、ボリュームは認識された DataKeeper ボリュームです)。



3. 次のパネルに従って、**iSCSI 仮想ディスク** を構成してください。

a. **[iSCSI 仮想ディスク名]** を指定します。

b. **[iSCSI 仮想ディスクのサイズ]** を指定します (**注記:** 複数のファイルを作成できます。ファイルサイズがディスク全体になる場合、作成する VHD ファイルによりディスク全体が使用されるので、OS によりディスク容量が少ないと警告されることがあります)。

c. **[iSCSI ターゲットの割り当て]** 画面で、iSCSI 仮想ディスクを **既存の iSCSI ターゲット** に割り当てるか、**新しい iSCSI ターゲット** に割り当てるかを指定します (**既存の iSCSI ターゲット** を選択する場合の説明については、以下の説明 を参照してください)。

d. **[iSCSI ターゲット名]** を指定します。

e. **[アクセスサーバ]** 画面で **[追加]** を選択します。この **iSCSI 仮想ディスク** にアクセスする **iSCSI イニシエータ** を追加します。**注記:** iSCSI イニシエータは一度に 1 つずつ追加してください。

4. すべての情報を指定したら、iSCSI 仮想ディスク / ターゲットの作成は完了です。iSCSI イニシエータ の設定に進んでください。

同一のターゲット名に複数の仮想ディスクを設定する

同一の iSCSI ターゲット名に、複数の iSCSI 仮想ディスクを設定することもできます。iSCSI イニシエータがそのようなターゲットに接続する場合は常に、その名前が割り当てられたすべての仮想ディスクに接続します。

あらかじめ、どのファイルを作成するか、またそれらのファイルに同時にアクセスするか、個別にアクセスする必要があるかを計画する必要があります。

ユースケースの例

同一仮想マシンのシステムディスク、およびデータディスクになる 2 つの仮想ディスクを設定します。ターゲットに「server-1-disks 」の名前を付けます。iSCSI イニシエータがターゲット名「 server-1-disks 」に接続すると、両方のディスクがイニシエータシステムに接続します。また、クラスタ (および CSV) の一部を構成する仮想ディスクを持つ iSCSI ターゲットを設定する場合、これらのすべてのディスクを同一のターゲットにすることができます。

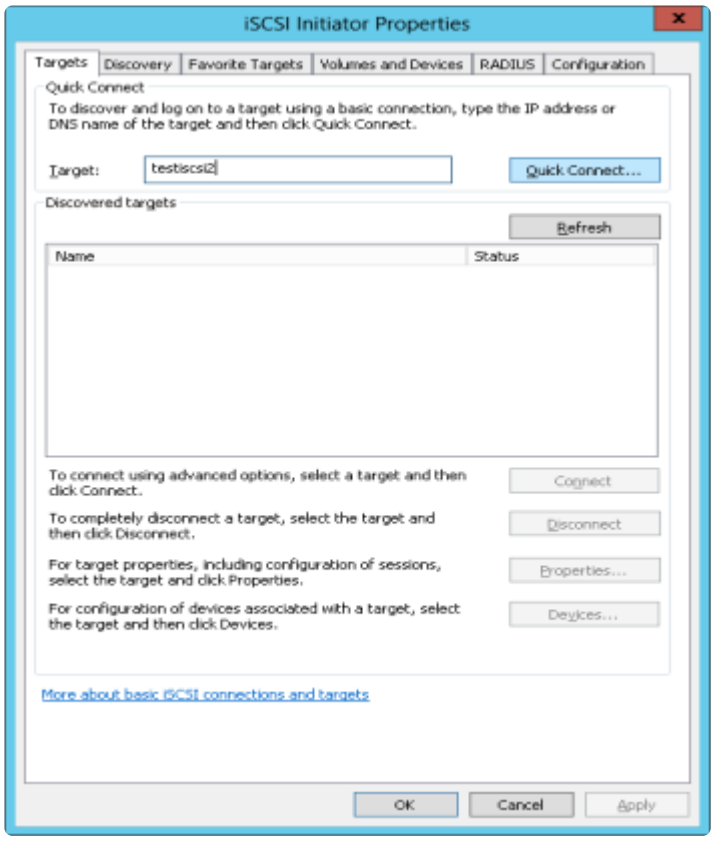
同一ターゲット名に複数の仮想ディスクを設定するには、手順 3c で、**[iSCSI ターゲットの割り当て]** 画面で **新規 iSCSI ターゲット** を選択せずに、**既存のiSCSI ターゲット** を選択し、前の手順で作成した iSCSI ターゲット名を指定します。このターゲット名は、iSCSI イニシエータが iSCSI ターゲットサーバに接続すると [ターゲット] リストに表示されます。ターゲットに複数の仮想ディスクが関連付けられている場合、イニシエータはそれらの各ディスクと接続します (ディスクは [ディスク管理] に新規ディスクとして表示される)。

8.5.4.7.4. Windows 2012 での iSCSI イニシエータの設定

仮想ディスク / ターゲットを作成した後、Microsoft の iSCSI イニシエータ経由で、個々のクラスタサーバの接続を開始する必要があります。

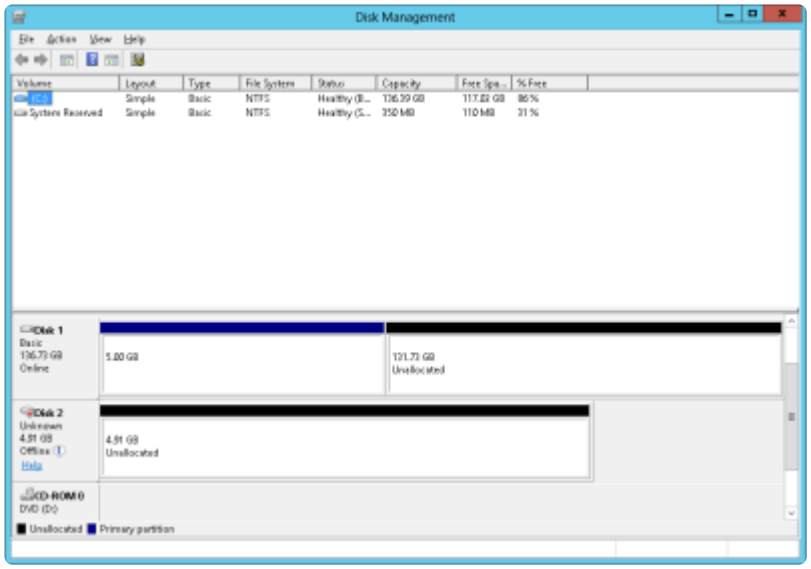
1. **[サーバマネージャ]** の **[管理ツール]** から **[iSCSI イニシエータ]** を開始してください。

2. **[ターゲット]** タブを選択し、前の手順 で作成した **クラスタ化 iSCSI ターゲット** の **ネットワーク名** または **IP アドレス** を入力してください。**[クイック接続]** を選択します。



3. 新しいパネルに、「 **正常にログイン** 」したことが示されます。**[OK]** をクリックしてパネルの表示を消します。

4. 「 **Disk Manager** 」を開始してください。新しい iSCSI 仮想ディスクが表示され、初期化可能になります。



5. ディスクを右クリックし、オンラインにしてください。

6. ディスクを初期化してください。

7. 新しいボリュームを作成し、ドライブレターを割り当ててください。

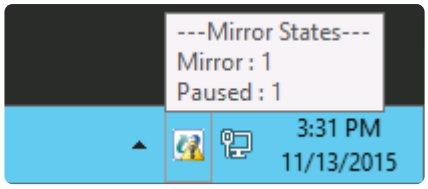
8. 設定が完了しました。

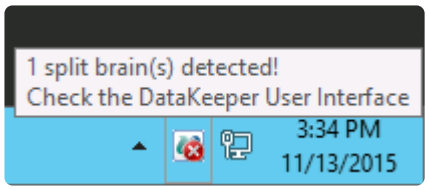
8.5.4.8. DataKeeper Notification Icon

DataKeeper Notification Icon は、Windows の通知領域に DataKeeper ミラーについての概要を表示するアプリケーションです。表示されるアイコンは、検出された状態を以下の優先度順に示します。

- Error: スプリットブレインなどのエラー状態が検出されました。
- Warning: ミラーの一時停止または中断など、管理者の介入が必要になる場合がある状態を示します。
- Resync: ミラーが再同期または再同期のペンディング状態であることを示します。
- Mirroring: すべてのミラーがミラーリング状態であることを示します。
- Disabled: ステータスの更新をもう実行していないことを示します。この状態の間は他のステータス条件は表示されません。

DataKeeper Notification Icon 上にマウスのポインタを置くと、各状態のミラー数、検出されたエラー状態の特性など、詳細な条件が表示されます。下記に例をいくつか示します。





注記: DataKeeper Notification Icon は、DataKeeper のジョブを使用して、情報を検査するリモートシステムを決定します。レポートされるのは、DataKeeper Notification Icon が実行中のノードを含むジョブのミラーの状態のみです。

表示機能に加えて、DataKeeper Notification Icon は、DataKeeper ミラーを管理するショートカットとしても機能します。DataKeeper Notification Icon をダブルクリックすると、DataKeeper GUI が起動します。

右クリックすると、以下のオプションを持つメニューが表示されます。

- Launch DataKeeper GUI - DataKeeper GUI を起動します。
- Launch License Manager - SIOS ライセンスマネージャを起動します。
- Launch Health Check – コマンドプロンプトを開いて DKHealthCheck を実行します。
- Gather Support Logs - DKSupport を実行し、新規アーカイブを含む場所のエクスプローラのウィンドウを

開きます。

- Set Refresh Rate – アイコンが状態の情報を更新する頻度を設定できます。
- Disable/Enable Status Updates – 状態の更新を無効化または有効化します。EmTray を管理者権限で実行します。
- Exit - DataKeeper Notification Icon を停止して閉じます。

ログイン時の自動起動

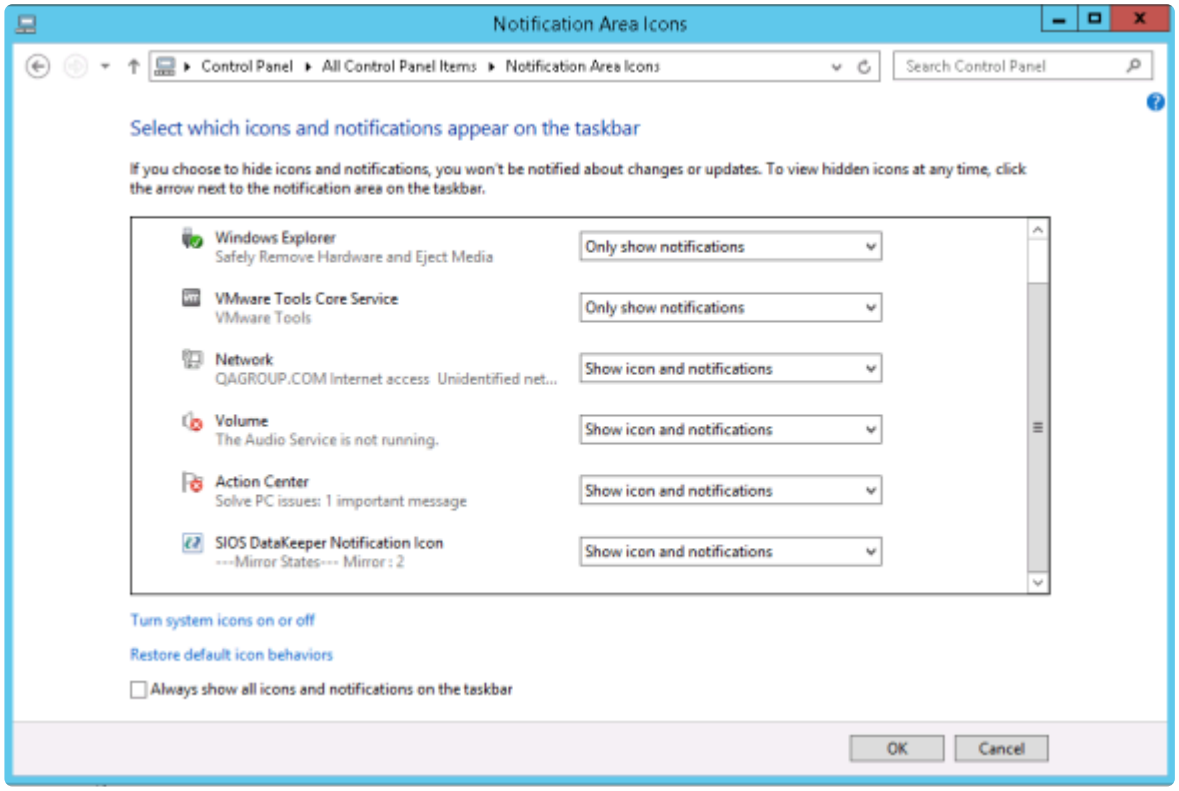
ノードにログインすると、Windowsの通知領域に Notification Icon が自動的に表示されます。

この機能を無効にするには、以下の場所から EmTray.exe へのショートカットを削除します。

• C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

この機能を再有効にするには、<DataKeeper のインストールパス>\DKTools にある EmTray.exe から上記の場所へのショートカットを作成するだけです。

注記: デフォルトでは、Microsoft Windows の通知領域はNotification Tray Icons を表示しません。[コントロールパネル] の [通知領域アイコン] のオプションで、[SIOS DataKeeperNotification Icon] の設定を [Show icon and notifications] に変更することによって表示することができます。



8.5.4.9. DataKeeper ターゲットスナップショット

概要

DataKeeper と DataKeeper Cluster Edition の両方に統合されている DataKeeper のターゲットスナップショット機能は、特定時点の複製ボリュームのコピーを作成するプロセスであり、ソースシステムからのデータレプリケーション動作を妨げることなく、スタンバイクラスタノード上のデータにアクセスすることができます。どの時点でも、データ保護は失われません。ターゲットスナップショットを有効にすると、ソースのパフォーマンスに悪影響を与えずに、アイドル状態になっていたターゲットノード上のデータを使用できます。

ターゲットスナップショットを使用しない場合、DataKeeper と DataKeeper Cluster Edition は、ターゲットシステム上にソースシステムのデータのリアルタイムレプリカを維持できます。ただし、ミラーを一時停止し、ターゲットシステムをロック解除しない限り、このレプリカにアクセスすることはできません。この一時停止とロック解除の状態では、ミラーのフェイルオーバとスイッチオーバが実行されることはないので、保護されているアプリケーションの可用性が低下します。アプリケーションと整合性のあるターゲットスナップショットを使用すると、ソースシステム上で動作しているアプリケーションの可用性を高く維持したまま、ターゲットシステムのデータにアクセスできます。ミラーは **ミラーリング** の状態に維持され、ソースからのすべての書き込みを使用してターゲットボリュームの更新を継続します。ターゲットスナップショットはボリュームシャドウコピーサービス (VSS) と統合されており、ターゲットシステム上に現れるデータを確実にアプリケーションと整合性がある状態にします。

ターゲットスナップショットの活用

DataKeeperのターゲットスナップショットは、ターゲットシステム上のデータへアクセスするための “Pause and Unlock“ コマンドの使用に代わるものですが、ターゲットスナップショットにはPause and Unlock にはない以下のようなメリットがあります。

- ミラーリング状態のまま、ソースシステムからのデータのレプリケーション継続を妨げません。
- 複数のボリュームのスナップショットを同時に実行できます。
- ターゲットシステムで対象となるデータがアプリケーションに適合した状態であることを確実にするため、ソースシステムで稼働しているVSS対応のアプリケーション（MS SQL Server など）は、VSS により一旦停止されます。

ターゲットスナップショットの使い方

ターゲットシステム上でスナップショットの場所を定義する

ターゲットスナップショットを使用するには、アクセスする予定のボリュームごとにターゲットシステム上でスナップショットの場所を定義する必要があります。スナップショットの場所は、DataKeeper GUIの [ミラープロパティ] ダイアログで定義できます。ターゲットシステムで EMCMD SETSNAPSHOTLOCATION を実行して定義することもできます。

```
EMCMD <system> SETSNAPSHOTLOCATION <volume letter> "<directory path>"
```

ソースシステムでSIOS VSSプロバイダーを有効にする

DataKeeper ターゲットスナップショットは VSS を使用して、ミラーソースシステム上のデータを静止します。DataKeeper には、この実行に使用される VSS プロバイダーコンポーネントがあります。しかし、SIOS VSS Providerといくつかのバックアップ製品の干渉が報告されたため、これは無効の状態で出荷されます。スナップショットを作成するには、ミラーソースシステム上の VSS Provider を有効にする必要があります。

SIOS VSS Provider を有効にするには、"%ExtMirrBase%\ VSSProvider" にあるスクリプト "install-siosprovider.cmd" を実行します。

ターゲットスナップショットを作成した後、同じフォルダ内のコマンド "uninstall-siosprovider.cmd" を実行することにより、ミラーソースシステム上でそのスナップショットを無効にすることができます。SIOS VSS Provider と互換性のないバックアップ製品を使用している場合は、このコマンドを使用して無効にする必要があります（互換性のない製品については、「 既知の問題 」を参照）。ただし、互換性のない製品を使用していない場合は、VSS Provider を有効のままにしておくことができます。
注記： すべての DataKeeper アップデートでプロバイダーが無効になるため、この後にターゲットスナップショットを取得するには再度有効にする必要があります。

SIOS VSS Provider は、スナップショット取得時のみ必要です。プロバイダーが無効化された後、ターゲットシステム上にスナップショットを残しておき、プロバイダーが無効になっている間はスナップショットを削除することができます。

TAKESNAPSHOT コマンドの実行

ミラーボリュームごとにスナップショットロケーションが定義され、ソースシステム上でSIOS VSS Providerが有効化された後、EMCMD TAKESHAPSHOT コマンドを実行すると、ターゲットシステム上でボリュームにアクセスできるようになります。

```
EMCMD <target_system> TAKESNAPSHOT <volume letter> [<volume letter>…]
```

<target_system> がターゲットシステムの名称またはIPアドレスの場合、<volume letter> はスナップショットの対象となる一方のボリュームのドライブレターであり、[<volume letter>…] は同時にスナップショットの対象となるもう一方のドライブのドライブレター（オプション）です。

ターゲットスナップショットの仕組み

DataKeeper のターゲットスナップショットは「書き込み時にコピー」方針を使用し、特定時点におけるボリュームの表示を維持して提示します。ボリューム情報の格納にはスナップショットファイルが使用されます。このスナップショットファイルの場所を設定することが、ターゲットスナップショットを有効にするための最初の手順です。

EMCMD コマンド `TAKESNAPSHOT` を実行すると、DataKeeper によりスナップショットファイルが作成され、設定したスナップショットフォルダにマウントされます。次に、VSS を使用して特定のボリューム上の VSS 書き込みを休止すること、およびディスクへのすべての書き込み動作が停止してそのボリュームが正しく定義された状態になったときにターゲットに通知することを指示するリクエストがソースシステムに送信されます。

データベース/アプリケーションの休止

このアプリケーションとの整合性維持機能はボリュームシャドウコピーサービス (VSS) と統合されており、ターゲットシステム上に現れるデータを確実にアプリケーションと整合性がある状態にします。スナップショットが要求されると、VSS サービスはシステムを一時停止し、ディスク上のデータを変更するすべてのアプリケーションのすべてのアプリケーションファイルを確実に整合性がある状態にしてから、スナップショットを作成します。これを、「データベース/アプリケーションの休止」と呼びます。データベースをシャットダウンして制限付きモードで再度開くこととは異なり、一時的な休止では、スナップショットの作成に必要な短期間のみ、アプリケーションの書き込み I/O リクエストを凍結します (読み取り I/O リクエストは継続して可能)。休止状態になると、スナップショットメッセージをドライバのミラー書き込みキューに追加することにより、各ボリュームのスナップショットが開始されます。VSS は次にアプリケーションを凍結解除してボリュームをロック解除するので、アプリケーションが休止している時間が最短に抑えられます。このとき、ユーザはターゲットシステムで動作を実行できる一方、ミラーは **ミラーリング** 状態であり、ソースシステム上のアプリケーションの可用性は高く維持されています。

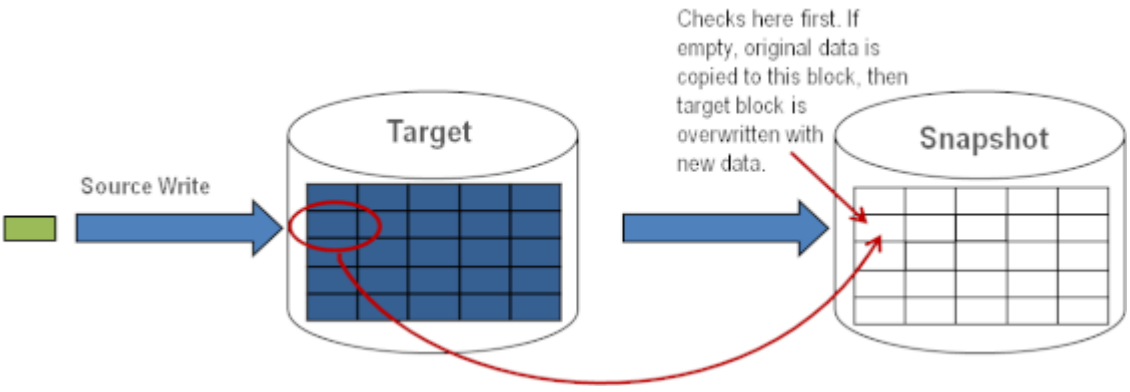
読み取りと書き込みの I/O リクエスト

スナップショットは、バックアップ対象ボリュームのライブコピーと並行して存在するので、スナップショットの準備と作成が実行される短期間を除いて、アプリケーションは継続して動作できます。ただし、ターゲットがこの状態である期間、ターゲットへの書き込みは別の方法で処理されます。

ソースシステムからのデータのミラーリングは引き続き中断されませんが、スナップショットを実行した後にソースから受信される新規データは、スナップショットがドロップされるまでターゲットでは表示されなくなります。これにより、ターゲットシステム上のアプリケーションは、スナップショットの実行時点のソースシステムのデータを表すデータを使用 (および更新) して動作することができます。

ソースへの書き込み

ソースへの書き込みを実行するには、ソースから新規データが到達したときに、DataKeeper はまず、特定データブロックがすでにスナップショットファイルに書き込まれているかどうかを調べます。



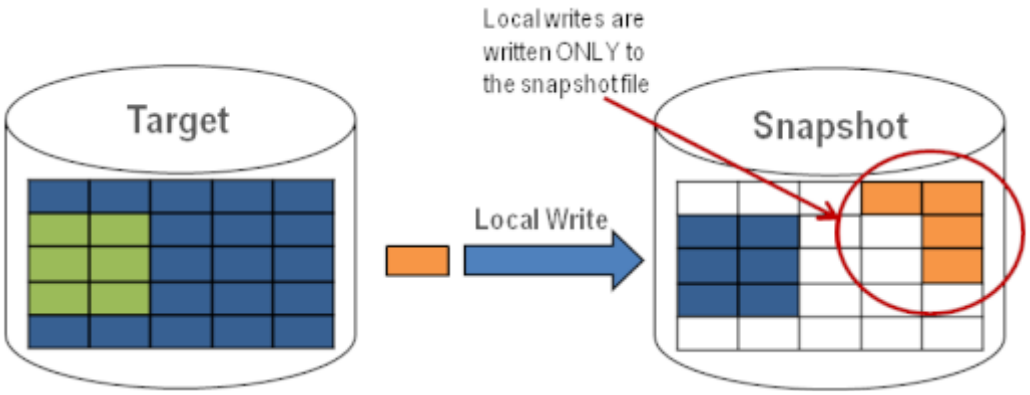
> 上の図に示すように、そのブロックがまだ書き込まれていない場合、スナップショットデータを保持するために **元の** ブロックがスナップショットファイルに書き込まれ、次に新規データがターゲットに書き込まれます。結果を以下に示します。



> このブロックがすでにスナップショットファイルに書き込まれていると DataKeeper が判断した場合、この手順は省略され、ブロックは単にターゲットに書き込まれます。頻繁に上書きされるソースボリューム上のブロックの場合、スナップショットファイルは 1 回のみ更新する必要があり、スナップショットの実行後の初回にそのブロックが書き込まれます。

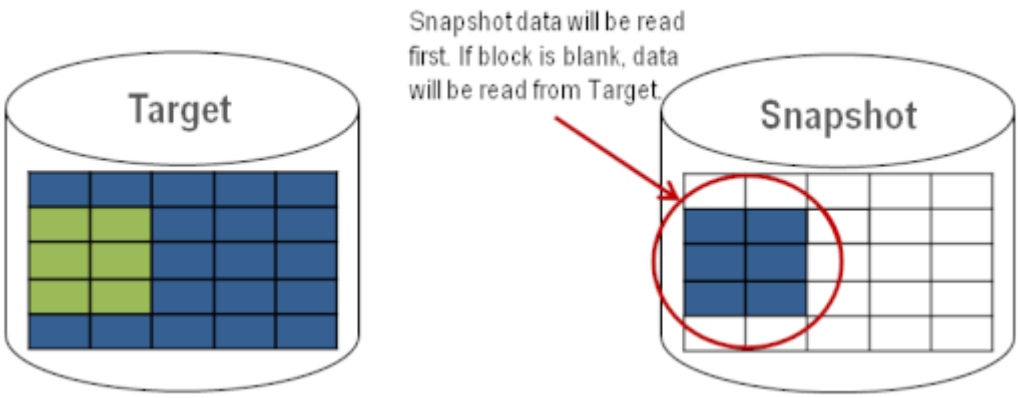
ローカル書き込み

ターゲットでローカル書き込みが (ターゲットシステムのアプリケーションから) 実行される場合、これらの書き込みはスナップショットファイルに格納され、複製ボリューム上のブロックを上書きすることはしません。(**注記**: スナップショットファイルに格納されたローカル書き込みは、スナップショットのドロップ時に失われます。)



ターゲット読み取りリクエスト

ターゲットボリューム上の読み取りリクエストは、スナップショットデータを返します。この動作は、はじめにスナップショットファイルに書き込まれたデータを読み取ることにより実行されます。スナップショットファイルに保存されていないブロックは、ターゲットボリュームから読み取られます。



ターゲットスナップショットを使用する

ターゲットスナップショットを使用するときには、以下の 3 つのタスクを実行する必要があります。スナップショットの場所の設定 、および スナップショットの開始 を実行する必要があります。ターゲットのレポート動作が完了したら、スナップショットのドロップ を実行する必要があります。

スナップショットの場所を設定する

ターゲットスナップショットを開始すると、DataKeeper はスナップショットデータを保持するファイルを作成し、スナップショットの場所にマウントします。スナップショットを開始する前に、この場所を設定する必要があります。マウントするスナップショットディスクの詳細については、以下の ファイル/ディスクデバイス/レジストリエントリ を参照してください。

スナップショットの場所は、以下の条件を満たすように設定してください。

- スナップショットが要求されたときにのみ使用される。
- DataKeeper のミラーボリューム上には保存できない。
- 異なるボリュームのスナップショットファイルを複数保存することはできない。
- ソースのミラーボリュームのサイズおよびスナップショット使用時の書き込みに従って、増大するファイルを作成して保存できるだけの十分な空き容量がある。

注記: スナップショットの実行中にスナップショットの場所を変更しないでください。

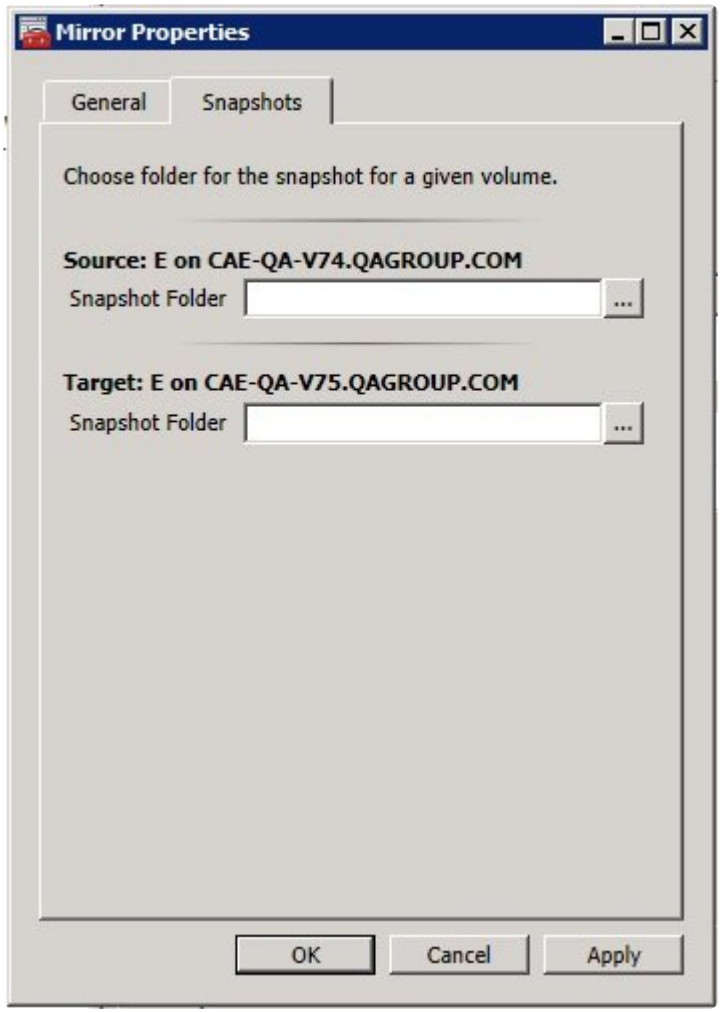
スナップショットの場所のサイズ

スナップショットの場所のサイズは、複数の条件に基づいて、個別に決定する必要があります。実際、スナップショットファイルに必要なサイズは、スナップショットを作成するボリュームのサイズよりも非常に小さくなっています。必要なストレージは、スナップショットの使用中にソースシステム上で変更されるデータを格納できるように十分に大きい必要があります。スナップショットを開始するたびに、すべてのスナップショットファイルがゼロに設定され、使用中にサイズが徐々に増加します。スナップショットがドロップされると、これらのファイルは削除されます。書き込み時のコピープロセスは「変更された」ブロックのみをスナップショットファイルに書き込むので、スナップショットの継続時間、およびミラーボリュームの変更の割合を考慮する必要があります。過去のアクティビティのスナップショットについて履歴を表示すると、サイズを再評価できます。

ベストプラクティス: 控え目に推定して、空き容量を余分に確保してください。十分な空き容量が割り当てられていない場合、上限に達するとスナップショットがドロップされます。

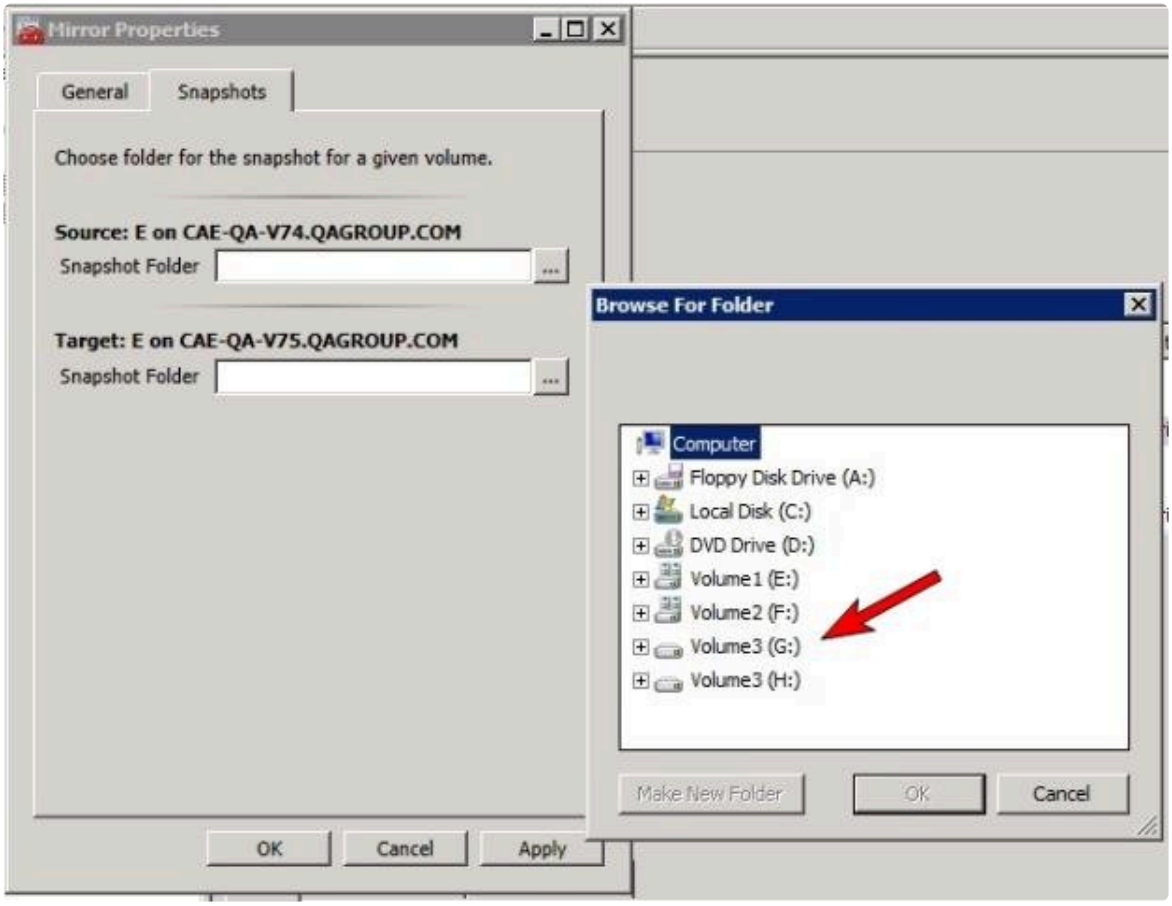
スナップショットの場所の選択

1. 適切なミラーを右クリックし、**[ミラープロパティ]** を選択してください。
2. **[ミラープロパティ]** ダイアログの **[スナップショット]** タブを選択してください。



> **注記:** DataKeeper は、ターゲットノード上に設定したスナップショットの場所を使用します。ただし、ミラーのいずれのノードもターゲットになることが可能なので、スナップショットの場所をソースとターゲットの両方に設定できます。

3. **[参照]** ... ボタンを使用してスナップショットの場所を選択するか、テキストボックスに **パス** を入力してください。



> GUI が動作しているシステムに対応する **[参照]** ボタンをクリックすると、**[フォルダの参照]** ダイアログが表示されます。GUI が動作しているシステム以外のシステムに対応する **[参照]** ボタンをクリックすると、**[リモートフォルダの参照]** ダイアログが表示されます。

4. ソースとターゲットの **スナップショット** の場所を選択します。このボリュームに、このスナップショットの動作が正常に実行できるだけの十分な空き容量があることを確認してください。スナップショットのボリュームサイズを推定するときの詳細については、スナップショットの場所のサイズ を参照してください。**[適用]** をクリックしてください。

> **注記:** 指定したシステムの各ボリュームについて、同じ場所を使用することも、別の場所を選択することもできます。

	GUI をバイパスする場合 、コマンドラインから SETSNAPSHOTLOCATION コマンドを使用して、スナップショットファイルの場所を設定できます。指定したボリュームの現在のスナップショットの場所を表示するには、GETSNAPSHOTLOCATION コマンドを使用します。

スナップショットを実行する

ターゲットシステムで **スナップショットの場所** を設定した後、スナップショットを実行できます。ターゲットノードから、EMCMD コマンド TAKESNAPSHOT を実行してください。

スナップショットをドロップする

スナップショットが不要になったときには、通常の処理に戻すためにボリュームのスナップショットをドロップする必要があります。EMCMD コマンド DROPSNAPSHOT を実行してください。このコマンドは、ボリュームをロックし、作成したスナップショットファイルをクリーンアップします。その後、ボリュームが通常のターゲットに戻り、ソースからの書き込みは、書き込み時のコピー保存を実行せずに直接ボリュームに書き込まれます。

注記: Windows 2012 R2では、「ディスク # が突然取り外されました。」という警告メッセージが表示されます。

特定のボリュームのターゲットスナップショットを無効にする

特定のボリュームのターゲットスナップショットを無効にするには、スナップショットの場所をクリアする必要があります。この操作は、GUI から実行できます。

1. 該当するミラーを右クリックし、**[ミラープロパティ]** を選択してください。
2. **[ミラープロパティ]** ダイアログの **[スナップショット]** タブを選択してください。
3. ターゲットスナップショットを無効にするボリュームのスナップショットフォルダを削除してください。
4. **[適用]** をクリックしてください。

	**スナップショットファイルの場所は、コマンドラインから CLEARSNAPSHOTLOCATION コマンドを実行しても削除できます。**

コマンドが正常に実行された場合、そのボリュームのスナップショットを再び開始するには、スナップショットの場所を再設定する必要があります。

ターゲットスナップショットの注記

サポートする設定

DataKeeper のターゲットスナップショットは SPS でサポートされているすべての Windows OS バージョンで、非共有（1×1 および 1×1×1）環境でサポートされています。

Out of Service のソース

ソースが out of service の場合、DataKeeper のターゲットスナップショットを開始することはできません。ただし、スナップショットの開始後にソースが out of service になった場合、スナップショットは意図どおりに動作を継続します。ソースが out of service である期間、スナップショットを継続して使用でき、不要になったときにはドロップできます。

スイッチオーバとフェイルオーバ

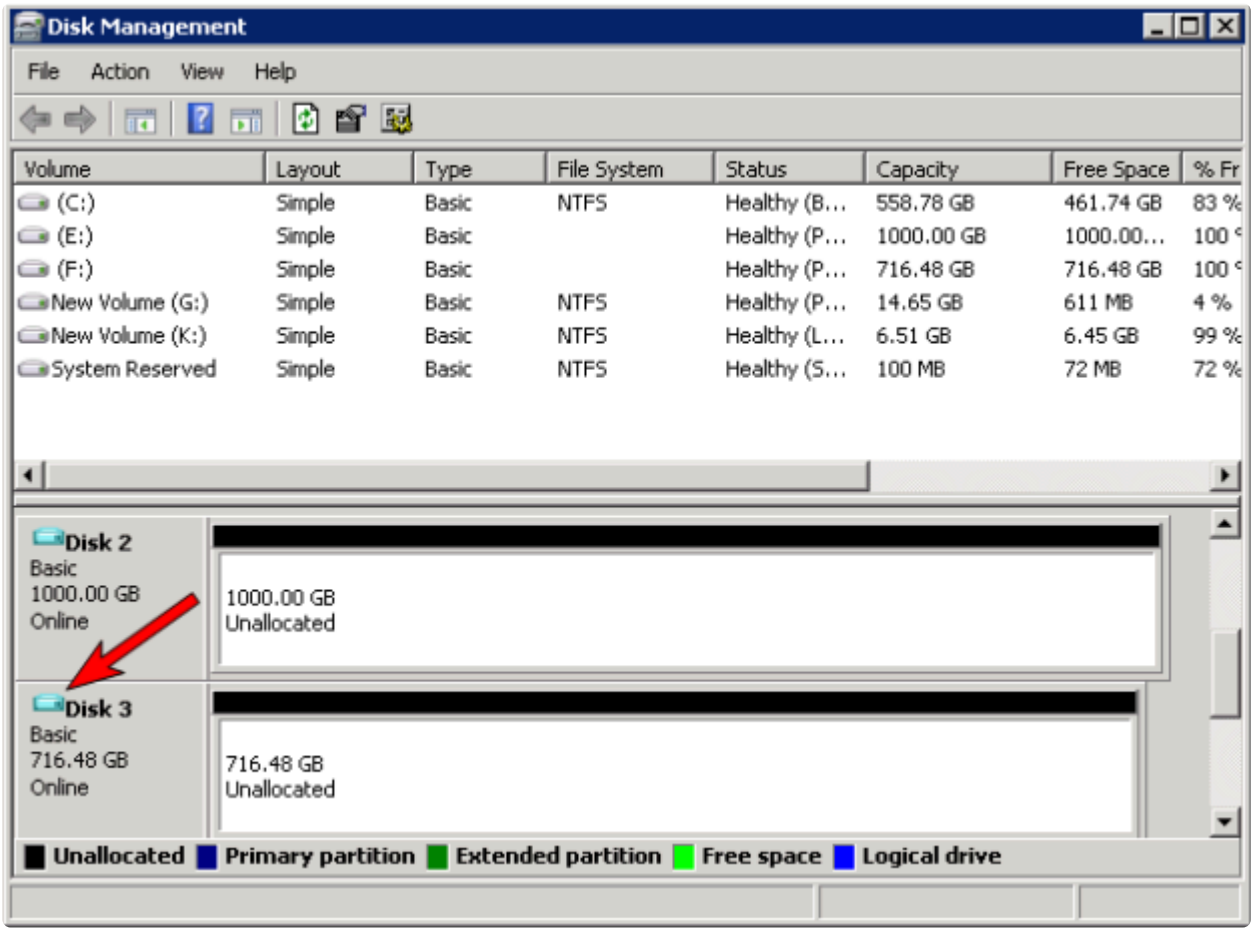
スナップショットを使用中の場合、スナップショットがドロップされるまで、スナップショットされているボリュームはミラーソースになることができません。ローカルノードへのボリュームのスイッチオーバやフェイルオーバを可能にするには、DROPSNAPSHOT を実行する必要があります。スナップショットを実行したボリューム上に存在するデータにアクセスするプロセスはすべて、スナップショットのドロップ時にハンドルが無効になります。ただし、ボリュームがその後ロック解除される場合、これらのプロセスがそのハンドルを再び開かないようにする必要があります。この時点で、データが「 **ライブ** 」のアプリケーションデータになります。スナップショットされたデータではありません。

注記: SQL Server のリカバリ時に保護するには、ターゲットノード上にある SQL インスタンスのレポートを停止する弊社提供の汎用スクリプトを追加する必要があります。手順は、"<DataKeeper のインストールパス>\support" の restore_snapshot.vbs スクリプトにあります。LifeKeeper 階層に追加する方法については、スクリプトコードを参照してください。

ファイル/ディスクデバイス/レジストリエントリ

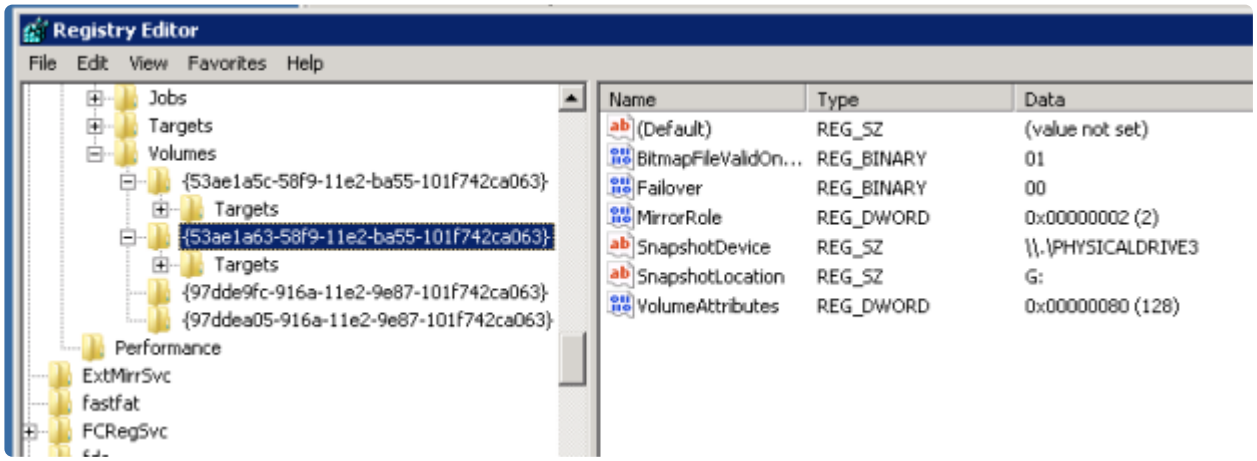
スナップショットを実行すると、実行対象の各ボリュームについて、スナップショットファイルがそのボリュームのスナップショットの場所に作成されます。作成されるファイルの名前は datakeeper_snapshot_vol<X>.vhd で、<x> はドライブレターです。この VHD ファイルは、Windows のディスク管理で表示できる仮想ディスクとして接続されます。

> **注記:** ディスク番号の横にある色付きアイコンは、このディスクが VHD であることを表します。



> **注意:** 作成された仮想ディスクデバイスは、パーティションが作成されていないベーシックディスクとして表示されます。この仮想ディスクデバイスは **スナップショットデータ専用** であり、スナップショットの使用中には切断やパーティションの作成を行うことはできません。これらの動作を実行すると、スナップショットデータが破損することがあります。**パーティションの作成やフォーマットを実行できる仮想ディスクデバイスと混同しないようにしてください。**

これらの仮想ディスクデバイスを接続すると、ボリュームのキーに SnapshotDevice というレジストリエントリが作成されます。値が \\.\PHYSICALDRIVE<x> に設定され、<x> は以下に示すディスク番号です。



`TargetSnapshotBlocksize` レジストリ値

DataKeeper のターゲットスナップショットは、ターゲットファイルに書き込むすべてのエントリについて、デフォルトのブロックサイズ 64KB を使用します。このブロックサイズを変更するには、ボリュームのレジストリキーに TargetSnapshotBlocksize という名前の REG_DWORD 値を作成します。

この値は常に、ディスクセクターサイズ (通常は 512 バイト) の倍数に設定する必要があります。特定のワークロードと書き込みパターンでは、ブロックサイズを変更すると効果がある場合があります。例えば、データのシーケンシャルストリーム (*SQL Server のログファイルなど*) に書き込まれるボリュームでは、ブロックサイズが大きいほうが効果的です。ブロックサイズを大きくすると、連続するブロックの書き込み時にターゲットボリュームからの読み取り回数が少なくなります。ただし、ランダムパターンに書き込まれるボリュームでは、小さいサイズ、またはデフォルトの 64KB が効果的です。ブロックサイズを小さくすると、ランダム書き込みリクエストでのターゲットファイルの使用量が少なくなります。

SQL Server の注記

DataKeeper のターゲットスナップショットを SIOS Protection Suite 環境で SQL Server とともに使用する場合、データベースをスナップショットに接続するために個別の SQL Server インスタンスを使用することを推奨します。

クラスタ化された SQL Server 環境では、データベースをスナップショットに接続するために個別の SQL Server インスタンスを使用する必要があります。

既知の問題

SIOS VSS Provider と互換性のないバックアップ製品

SIOS VSS Provider のコンポーネントでは、以下のバックアップ製品を使用するとバックアップが失敗することが報告されています。

- IBM Tivoli Storage Manager
- Microsoft Data Protection Manager

Microsoft .NET Framework 4.5.2の要件

ターゲットスナップショット機能を使用するには、Microsoft .NET Framework 4.5.2をインストールする必要があります。次のサイトからダウンロードしてください http://www.microsoft.com/net

NTFS ファイルシステムのメッセージ

ターゲットスナップショットの開始後にスナップショットの内部エラーが発生した場合 (スナップショットファイルの容量不足、ユーザによる接続の切断など)、スナップショットが無効になり、ボリュームがロックされます。また、失敗したボリュームのスナップショットファイルが削除されます。スナップショットエラーの処理中は、NTFS ファイルシステムのエラーが表示されることがあります。このメッセージは通常のものであり、無視できます。

スナップショットを使用するアプリケーションデータ

ターゲットスナップショットデータをアプリケーションとともに使用している場合、ターゲットスナップショットが更新された後、データを更新するには、アプリケーションを閉じてから開き直す必要があることがあります。

ボリュームシャドウコピーサービス (VSS) のディスクの空き容量の要件

ターゲットスナップショットボリュームの空き容量が不足した場合、そのボリュームが関係する VSS の動作が「予期しないエラー」で失敗することがあります。これを防ぐには、スナップショットボリュームが Microsoft の記事article Windows サーバー バックアップ (WBADMIN) では、Windows Server 2008 と Windows Server 2008 R2 を実行する VSS の問題をトラブルシューティングします。 のガイドラインに従う必要があります。

この記事には、ディスクの空き容量について以下の要件が記載されています。

500 MB 未満のボリュームの場合、空き容量の最小値は 50 MB です。500 MB を超えるボリュームの場合、空き容量の最小値は 320 MB です。ボリュームサイズが 1 GB を超える場合、各ボリューム上に 1 GB 以上のディスクの空き容量を確保することを推奨します。

8.5.4.10. SIOS DataKeeper Standard Edition を使用して Hyper-V 仮想マシンのディザスタリカバリを行う

考慮事項

異なるサブネット間で Hyper-V 環境を準備する場合は、仮想マシン内で実行されるアプリケーションのサブネットについても考慮する必要があります。構成に IP アドレスを「ハードコード」しているアプリケーションもあります。このようなアプリケーションが、異なるサブネット上のターゲットサーバに (DataKeeper によって複製されるボリュームを介して) 複製される仮想マシンに読み込まれた場合、ネットワーク設定の違いのために予想通りの動作をしないことがあります。

環境の準備

1. 少なくとも 2 つのパーティションを持つ 2 台のサーバに Windows をインストールします。パーティションの 1 つは OS 用、もう 1 つは Hyper-V 仮想マシン (VM) のファイル用です。ターゲットサーバ上のファイル用パーティションは、ソースサーバの「データ」パーティションと同じか、それよりも大きいサイズでなければなりません。Microsoft の *Hyper-V Planning and Deployment Guide* および *Hyper-V Getting Started Guide* の説明に従って、各サーバ上で Hyper-V の役割のインストールと構成を行ってください。ただし、DataKeeper によって複製されるボリュームを作成するまでは仮想マシンを作成しないでください。

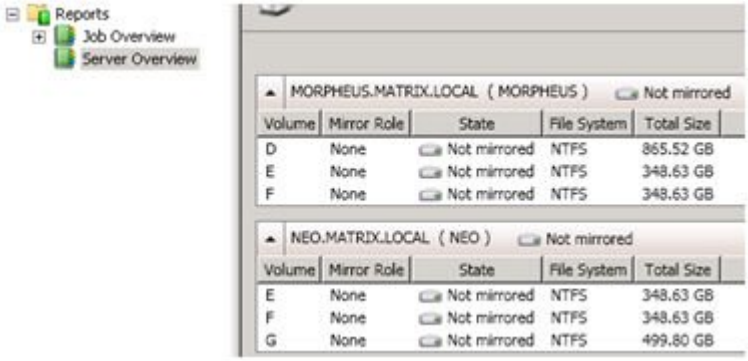
2. SIOS DataKeeper ソフトウェアのインストール要件を満たす環境にします。

3. サーバに接続 します。

接続すると、新しいオプションが中央のペインに表示されます。

サーバ概要 を表示して、ボリュームのステータスを確認することもできます。

DataKeeper をインストールしてライセンスを設定した複数のサーバに接続する場合は、ここに複数のサーバとボリュームが表示されます。



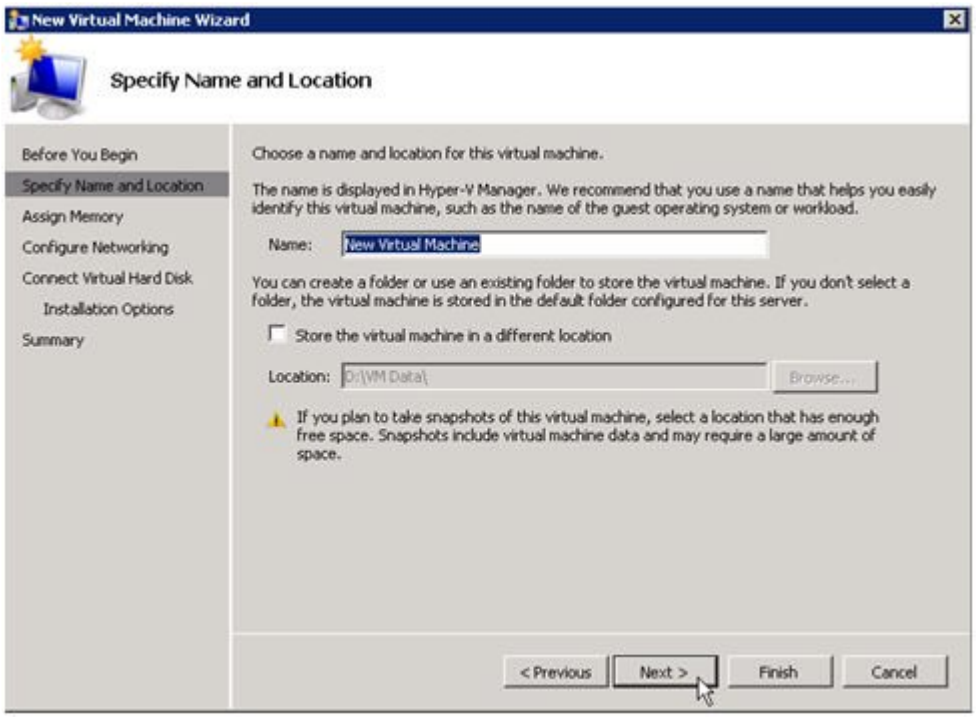
4. ジョブ と ミラーボリュームを作成 します。

> **注記**: ソースサーバを選択する場合は、必ず複製元にするボリュームがあるサーバを選択してください。これらの手順でソースとターゲットを逆にすると、ソースボリュームはターゲットサーバのボリュームの内容によって (それが空であったとしても) すべて上書きされ、ソースボリュームに保存されていたデータはすべて失われます。

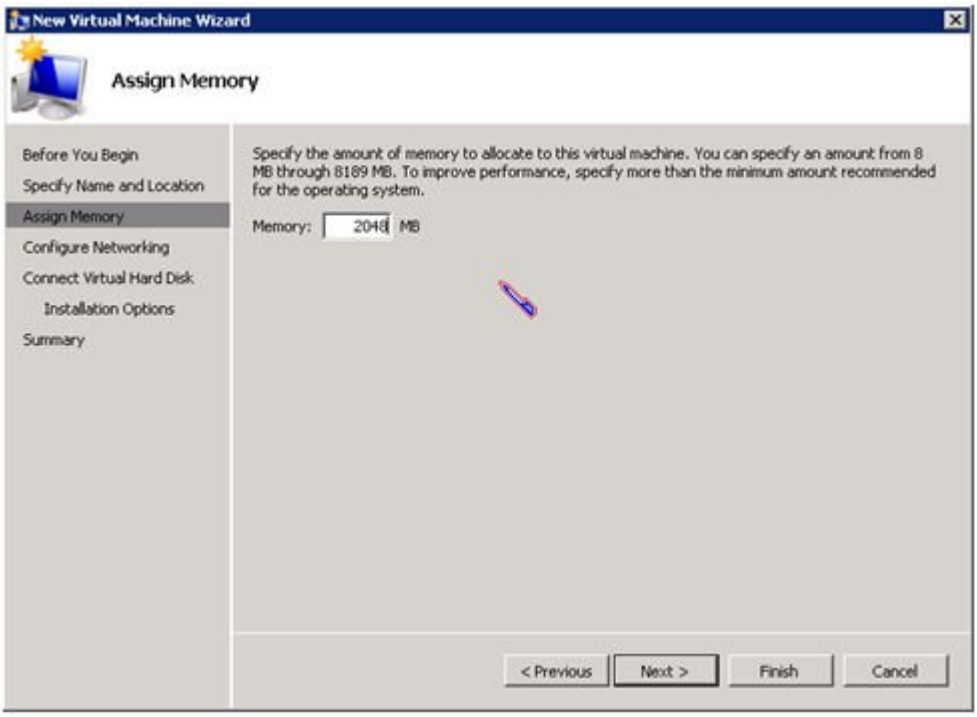
Hyper-V 仮想マシンの作成と構成

1. **[スタート]** - **[管理ツール]** - **[Hyper-V マネージャ]** から、**Hyper-V コンソール** を起動します。

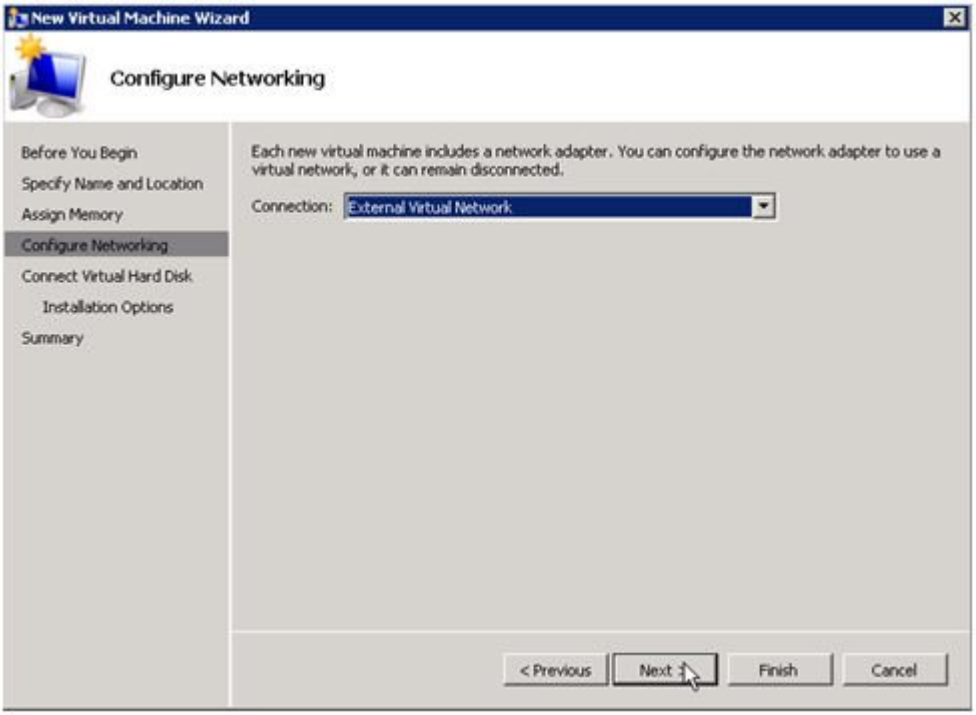
2. **新しい仮想マシンウィザード** を起動します。



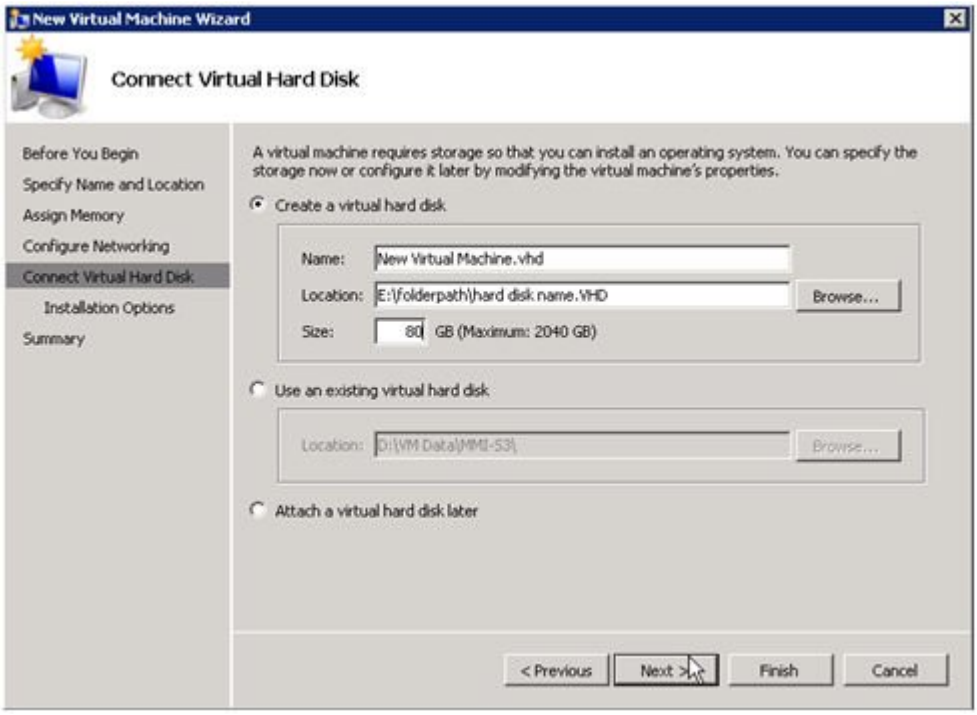
3. 使用する **RAM** の量を指定します。



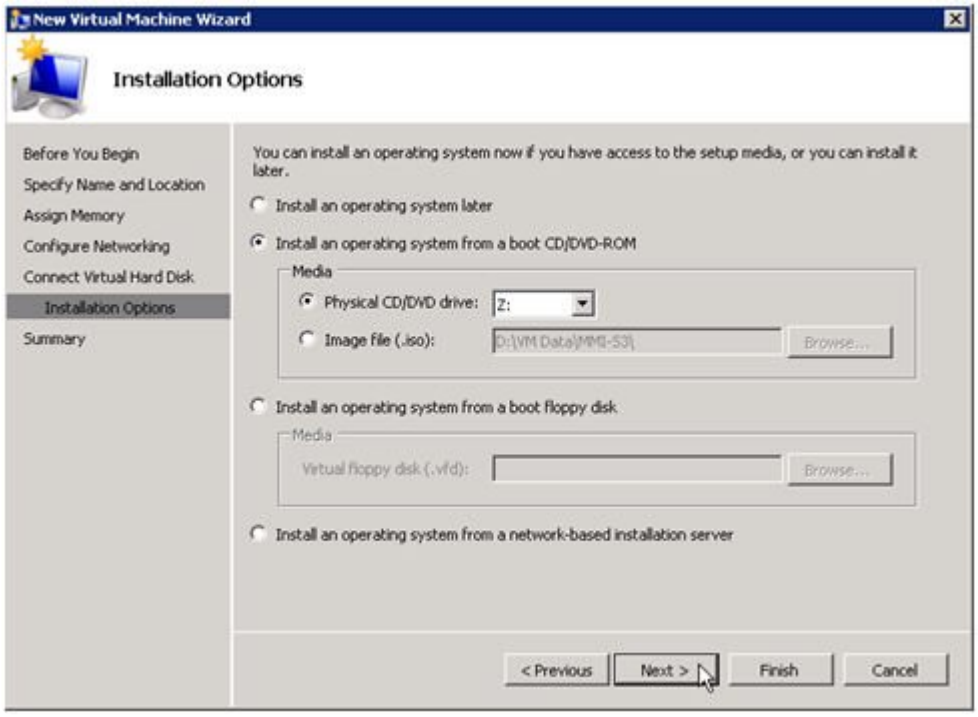
4. 使用する **ネットワークアダプタ** を選択します。



5. 複製されるボリュームに新しい **仮想ハードディスク** を作成します (または既存の VHD を複製されるソースボリュームにコピーし、作成ウィザードで仮想ディスクとして使用するよう指定します)。



6. オペレーティングシステムのインストールオプション を指定します。



7. ウィザードを 終了 して、仮想マシン を起動します。

オペレーティングシステムおよび仮想マシンに必要なアプリケーションのインストール

1. メーカーまたはベンダの指定する、ベストプラクティスとして要求されるオペレーティングシステムを仮想マシンに読み込みます。

2. DHCP アドレスを使用するように、仮想マシン内のネットワークを構成します。クライアント接続のアドレスの整合性に必要な場合は、同様に DHCP 予約および DNS または WINS による名前解決を行ってください。

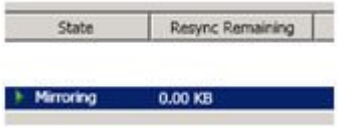
3. 必要なアプリケーションを仮想マシンにインストールします。

仮想マシンを実行するターゲットサーバの構成

1. ソース Hyper-V ホストサーバで **Hyper-V マネージャ** を開き、仮想マシンに接続して、仮想マシンのシャットダウンを実行します。この操作によってディスク上のデータが休止状態になり、ターゲットサーバのデータの整合性が保たれます。

2. 上記のように、**DataKeeper コンソール** を起動します。

3. ミラーの状態をチェックして、ボリュームが完全にミラーリングされていることを確認します。ステータスは **ミラーリング** で、**同期残容量 0 KB** でなければなりません。



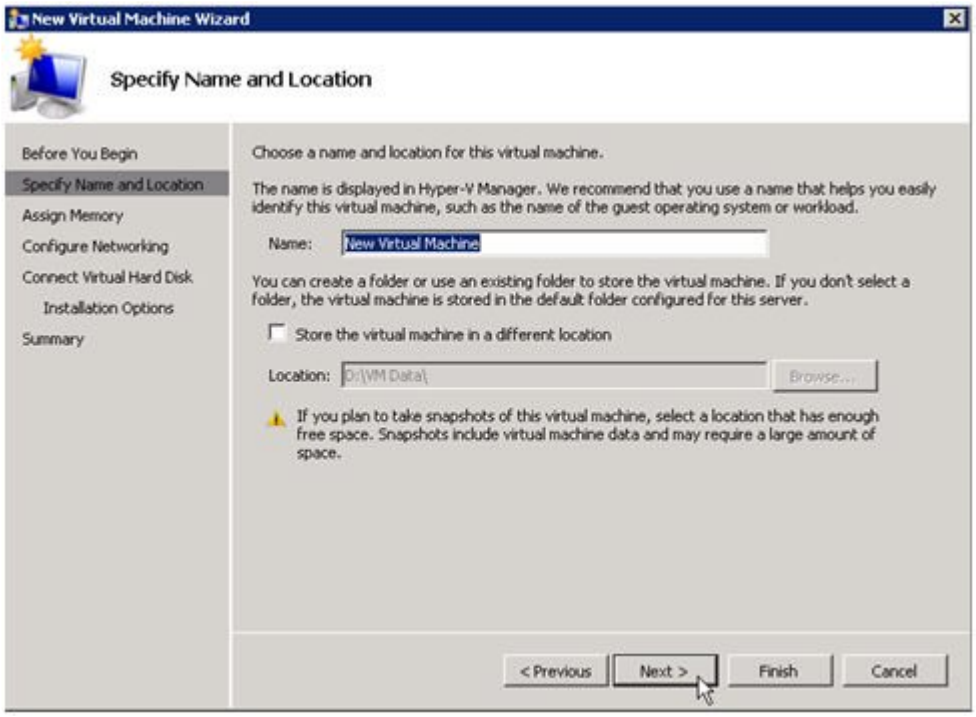
4. **[操作]** ペインでミラーを選択し、**[スイッチオーバ]** をクリックします。



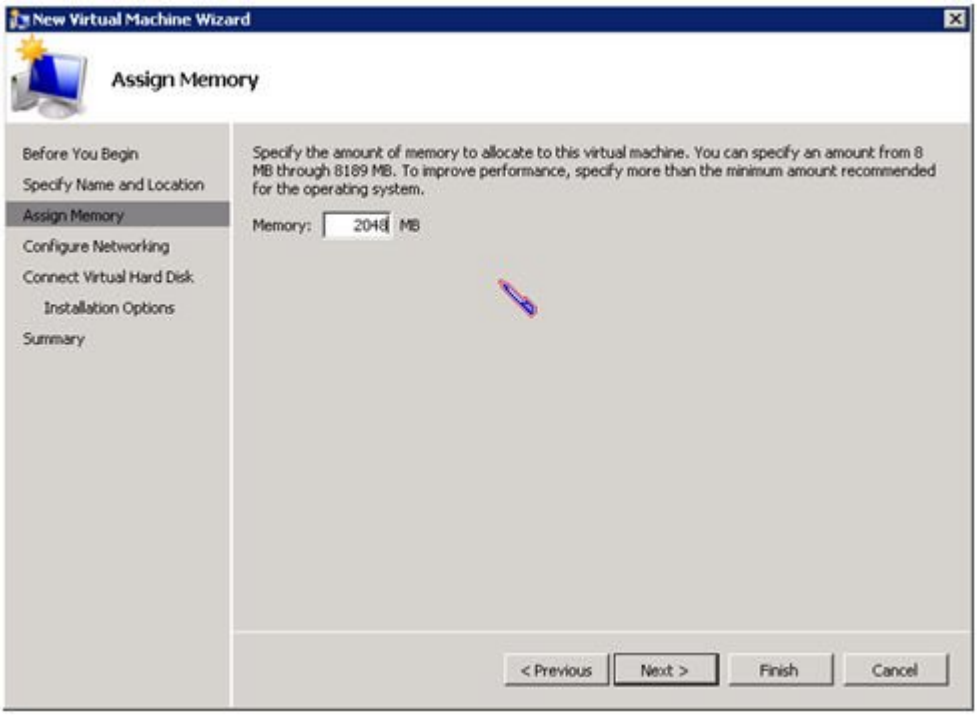
これによってソースとターゲットが入れ替わり、ターゲットサーバ上の仮想マシンを準備することができます。

5. ターゲットサーバで **Hyper-V マネージャ** を起動します。

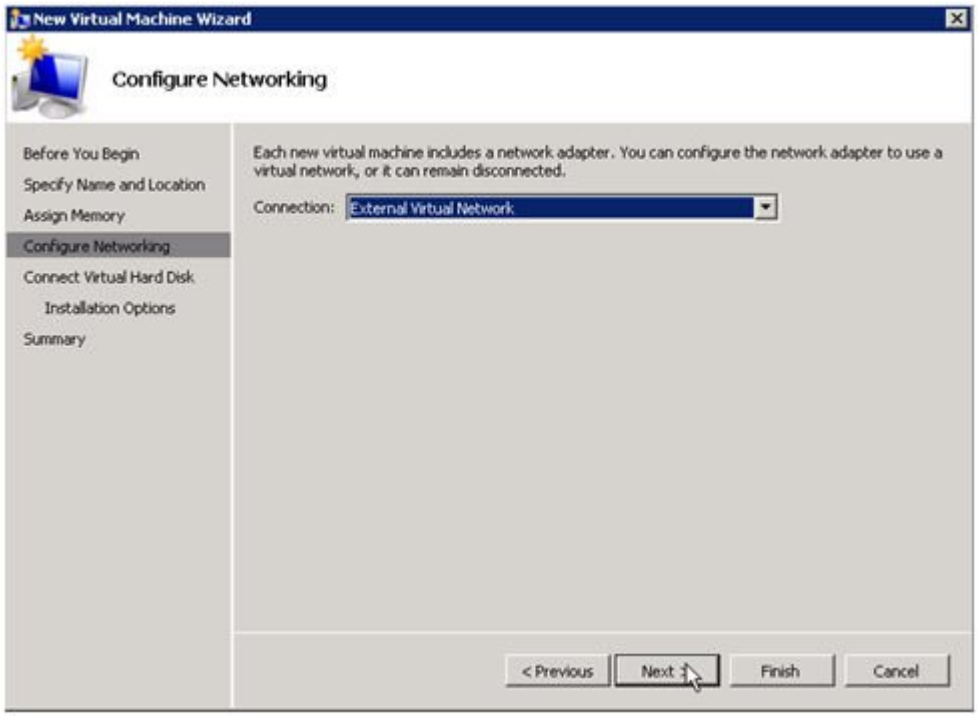
6. **新しい仮想マシンウィザード** を起動します。



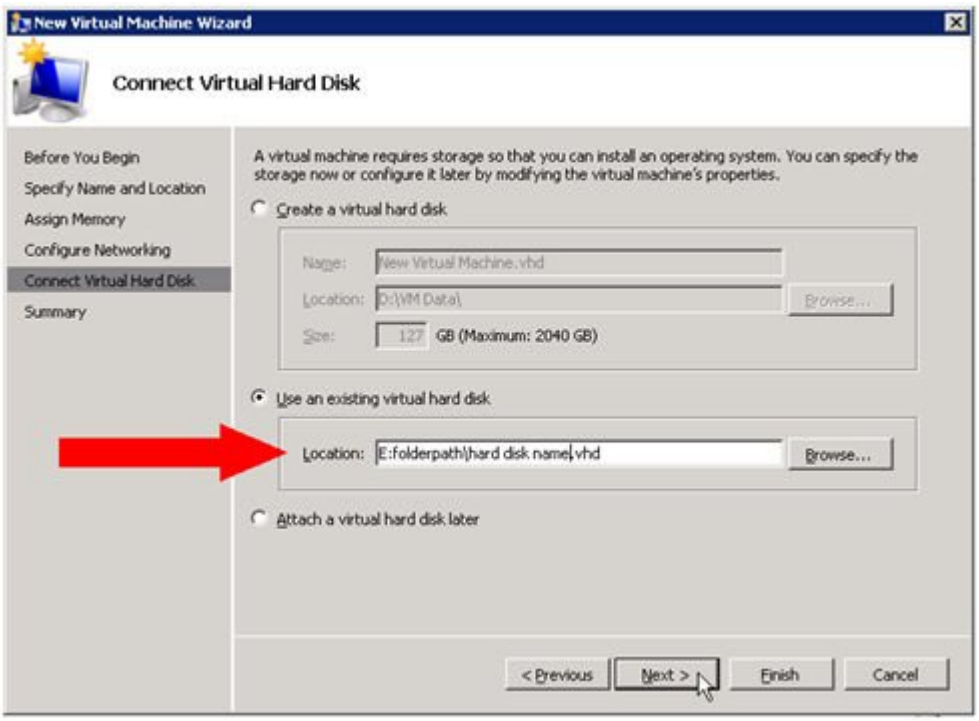
7. 使用する **RAM** の量を指定します。



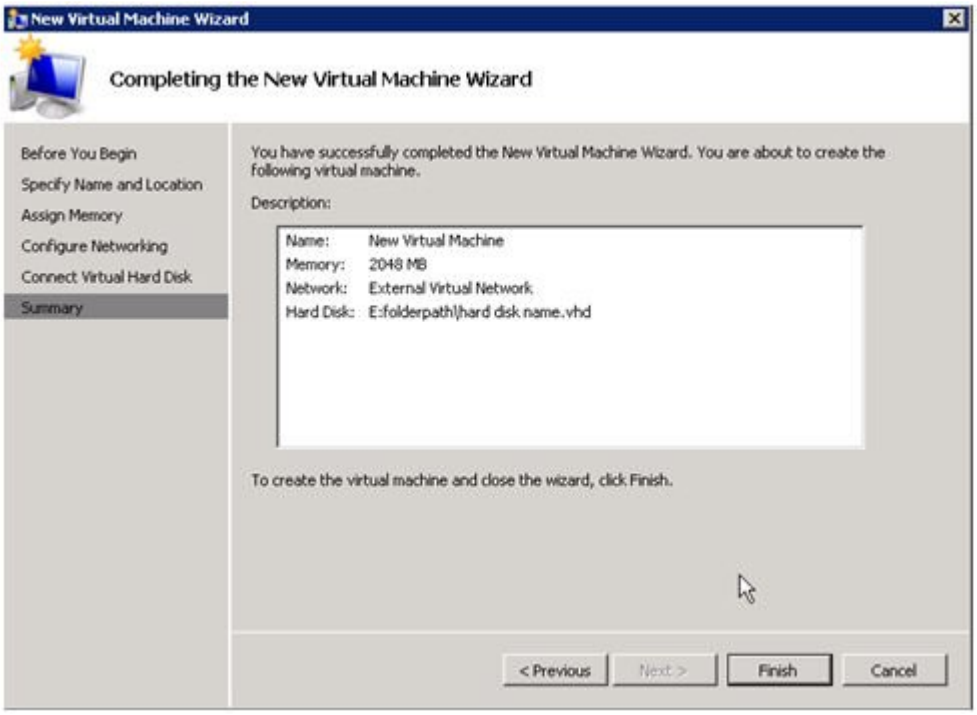
8. 使用する **ネットワークアダプタ** を選択します。



重要: 複製されたボリュームで既存の仮想ハードディスクを使用してください。



9. **[完了]** をクリックして、仮想マシン作成プロセスを終了させます。



仮想マシンを起動して、予想通りに動作することを確認してください。

計画済 / 計画外スイッチオーバ

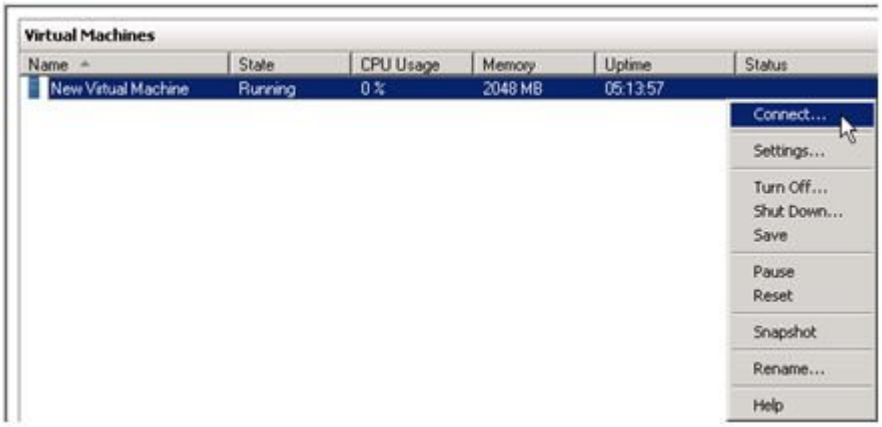
仮想マシンをソースサーバに戻すには、**計画済スイッチオーバ** を開始します。

テストまたはプライマリサーバでの実際の停電のためにスイッチオーバを開始したい場合は、**計画的スイッチオーバ** の実行をお勧めします。スイッチオーバには、**計画済** と **計画外** の 2 種類があります。

計画済スイッチオーバ

計画済スイッチオーバは、通常、ユーザコミュニティが計画されたダウンタイムの通知を受けることができる場合に、メンテナンスウィンドウで実行されます。

1. 上記のように、仮想マシンを実行しているサーバで **Hyper-V マネージャ** を起動し、**仮想マシン** に接続します。



2. 仮想マシンの内部から、仮想マシンを **シャットダウン** します。





3. 同じサーバで、上記のように **DataKeeper コンソール** を起動します。

ミラーの状態 をチェックして、ボリュームが **ミラーリング** 状態であることを確認します。スイッチオーバを実行するには、ステータスが **ミラーリング** で、**同期残容量 0 KB** でなければなりません。



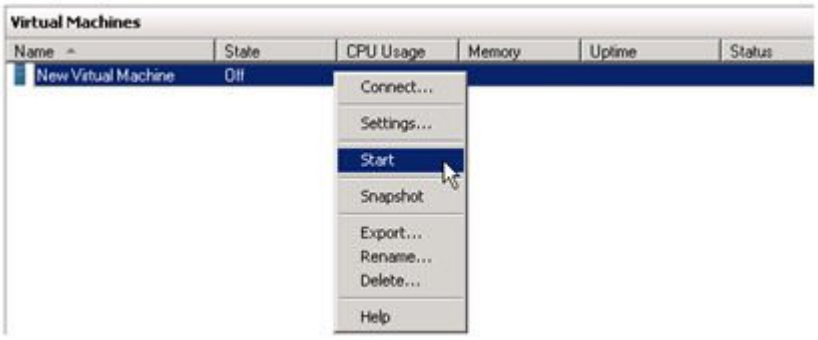
4. **[操作]** パネルでミラーを選択し、**[スイッチオーバ]** をクリックします。



ミラーのスイッチオーバが完了し、DataKeeper ユーザインターフェース (UI) にロールが正常に逆転したことが表示

されるまで待機してください。

5. DataKeeper インターフェースで、ソースサーバになったばかりの **Hyper-V ホストサーバ** にログインします。
6. 上記のように、**Hyper-V マネージャ** を起動します。
7. 仮想マシンを起動します。



計画外スイッチオーバ

計画外スイッチオーバが必要になるのは、何らかの障害が発生して、ソースシステムが使用できなくなるか、システム間の接続が切断され、ターゲットサーバ上で仮想マシンをオンラインにしなければならない場合です。

このケース、つまり何らかの理由でソースサーバが利用できず、ソースサーバ上のデータを静止できないような場合でも、ターゲットサーバ上で仮想マシンをオンラインにするために必要となるのは、以下の手順だけです。

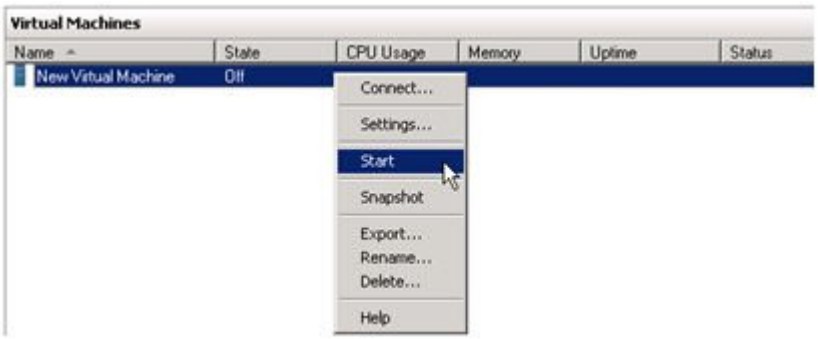
1. ターゲットサーバで、上記のように **DataKeeper コンソール** を起動します。
2. **[操作]** パネルでミラーを選択し、**[スイッチオーバ]** をクリックします。



サーバでミラーが完全に起動し、ソースサーバが有効になっていることが DataKeeper ユーザインターフェース (UI) に表示されるまで待機してください。

3. 同じサーバで、上記のように **Hyper-V マネージャ** を起動します。

仮想マシンを起動します。



スイッチバックタイプ

スイッチバックは、仮想マシンをターゲットサーバからソースサーバに戻すという計画されたイベントであり、プロセスは計画済スイッチオーバプロセスとまったく同じです。スイッチバックの影響については、上記の **計画済スイッチオーバ** の手順を参照してください。

8.5.5. よくある質問

SIOS DataKeeper に関してよくある質問の回答については、このセクションを参照してください。

Windows ファイル名とディレクトリ名の認識

ミラーのエンドポイントの変更

ミラータイプの変更

ミラー作成、ジョブの名前変更、およびジョブの削除の各操作がグレイアウトされる

データ転送ネットワークプロトコル

および [スイッチオーバ] 操作がグレイアウトされる

ミラーの削除

エラーメッセージロ

ミラーを作成できない

ネットワーク切断

ターゲットドライブの全容量の回収

Windows Server フェールオーバークラスターロールから DataKeeper ストレージを削除する

ミラー対象ボリュームのサイズ変更または拡張

スプリットブレインに関するよくある質問

ソースとターゲットの間のレプリケーションの停止

ボリュームシャドウコピーの使用

ミラーリングに使用できないボリューム

8.5.5.1. Windows のファイル名およびディレクトリ名の認識

質問

SIOS DataKeeper は Windows のファイル名とディレクトリ名を認識しますか。

回答

SIOS DataKeeper は、物理ディスクドライバの上かつファイルシステムの下に位置する Windows カーネルモードフィルタドライバを使用して実装されています。そのため、SIOS DataKeeper ドライバは、個々のファイルまたはファイルシステム自体については何も認識しません。認識するのは、ディスクに対するそのままの書き込みのみです。

8.5.5.2. AWSに関する問題と回避策

質問

AWSでクラスター化されたVMをシャットダウンするベストプラクティスは何ですか？

回答

プライマリソースノードをシャットダウンする場合、SIOS DataKeeperボリュームリソースに依存するすべてのクラスターロールをオフライン状態にする必要があります。また、VMをシャットダウンする前に、すべてのミラーがミラーリング状態になっていることを確認してください。前の手順を実行していれば、ノードのシャットダウン順序は重要ではありません。

8.5.5.3. ミラーエンドポイントの変更

質問

既存のミラーに現在関連付けられているシステムのミラーエンドポイント (IP アドレス) を変更することはできますか。

回答

はい。CHANGEMIRRORENDPOINTS という EMCMD を使用すると、3 ノード以下で構成されるミラーボリュームのエンドポイントを変更できます (4 つ以上のノードで構成される場合は、ミラーを削除してから再作成する必要があります)。

8.5.5.4. ミラータイプの変更

質問

既存のミラーのミラータイプを、同期から非同期 (またはその逆) に変更することはできますか。

回答

はい。EMCMD CHANGEMIRRORTYPE コマンドを使用してミラータイプを変更できます。

8.5.5.5. [ミラーを作成]、[ジョブ名を変更]、[ジョブを削除] 操作がグレイアウトされる

質問

[ミラーを作成]、[ジョブ名を変更]、[ジョブを削除] 操作がグレイアウトされているのはなぜですか。

回答

ジョブの一部が停止しているノードでは、これらの操作は無効になります。

8.5.5.6. データ転送ネットワークプロトコル

質問

SIOS DataKeeper のデータ転送で使用されているネットワークプロトコルは何ですか。

回答

SIOS DataKeeper では名前付きパイプ通信および TCP ソケットを使用します。

8.5.5.7. [削除] および [スイッチオーバ] 操作がグレイアウトされる

質問

DataKeeper のユーザインターフェースの [削除] および [スイッチオーバ] 操作がグレイアウトされているのはなぜですか。

回答

ボリュームがクラスタの保護下 (マイクロソフトのクラスタまたは SIOS LifeKeeper のクラスタ) にある場合、これらの操作は無効になります。

8.5.5.8. ミラーの削除に関する FAQ

質問

ミラーを削除すると、実際にはどのような処理が実行されますか。

回答

両方の側のデータが残りますが、ターゲットとソースのデータは同期されなくなります。ターゲットボリュームはロック解除され、完全にアクセス可能になります。

8.5.5.9. サーバーに適用されているGPOの確認

問題:

サーバーの再起動後にグループポリシーオブジェクト（GPO）がデプロイまたは再デプロイされることがあり、LifeKeeper（GUI）またはDataKeeperの動作に影響を与える場合があります。

ソリューション:

以下の2つの方法があります。

- [スタート] > [ファイル名を指定して実行] を選択し、**rsop.msc** と入力する
  - コンソールに、サーバーに適用されているポリシーの一覧が表示されます。
- または、管理者特権のコマンドプロンプトで、**gpresult /Scope Computer /v** と入力する
  - サーバーに適用されているポリシーの一覧が出力されます。

注記: ユーザーごとに適用されているGPOを確認するには、**gpresult /Scope user /v** と入力してください。

8.5.5.10. エラーメッセージログ

質問

DataKeeper のエラーメッセージはどこに記録されますか。

回答

DataKeeper のイベントは、**Windows アプリケーションイベントログ** および **Windows システムイベントログ** に記録されます。検索用にメッセージの分類を以下に示します。

アプリケーションイベントログ

- Source = ExtMirrSvc – DataKeeper サービスに関連するイベント。
- Source = DataKeeperVolume – Windows Failover Clustering (WSFC) で定義された DataKeeper ボリュームリソースに関連するイベント。
- Source = SIOS.SDRSnapIn – DataKeeper システムに接続している DataKeeper GUI に関連するイベント。

システムイベントログ

- Source = ExtMirr – ミラーの作成、ミラーの操作、およびレプリケーションに直接関連するイベント。

注記: システムイベントログ は必ず **[必要に応じてイベントを上書きする]** に設定してください。システムイベントログがいっぱいになったり破損したりすると、DataKeeper はミラーの状態変化を正常に認識できなくなります。

8.5.5.11. ミラーを作成できない

質問

ミラーを作成できないのは、なぜですか。

回答

- よくある原因は、ソースまたはターゲットのボリュームが別のプロセスで使用中であることです。ボリュームにアクセスしているプロセスを停止して、再試行してください。ミラーの作成中は、SIOS DataKeeper がターゲットボリュームに排他的にアクセスできるようにする必要があります。

- ターゲットボリュームのサイズはソースボリューム以上でなければなりません。ディスクの管理ユーティリティを使用して、ターゲットボリュームとソースボリュームのサイズを比較することを推奨します。サイズが同じでない場合は、ターゲットパーティションを少しだけ大きくして再作成してください。詳細については、ボリュームの考慮事項 を参照してください。
- ミラーの作成 時に発生したエラーは、ターゲットボリュームが壊れていることを示している場合があります。この場合、ターゲットボリュームをフォーマットし、ミラーを作成しなおしてください。

警告: Windows Server Failover Clustering を使用する場合は、ターゲットおよびソースのドライブレターを必ず一致させる必要があります。

8.5.5.12. ネットワーク切断

シナリオ #1

WAN経由のソースサーバおよびターゲットサーバ間で 100TB のボリュームを複製している 2 ノードの非クラスタ構成 (1×1) では、ネットワークが 20 分間切断されます。

質問

このシナリオにおいて、DataKeeper Standard Edition では **ミラーの状態** がどのようになりますか。

回答

数分後にソースサーバがネットワークの切断を検知し、ミラーの状態は **ミラーリング** から **一時停止** になります。

質問

DataKeeper はソースサーバ上の変更をトラックし続けますか。

回答

はい。ミラーが **一時停止** の間、ビットマップ (ダーティセクタ数) がソースサーバで更新され続けます。

質問

ネットワークが復旧すると、ターゲットサーバへの部分同期が発生しますか?

回答

はい。ミラーが **同期中** になり、すべてのダーティセクタがターゲットサーバへ書き込まれるまでそのままになります。その後、部分同期になります。

シナリオ #2

WAN経由のソースサーバおよびターゲットサーバ間で 100TB のボリュームを複製している 2 ノードの非クラスタ構成 (1×1) では、ネットワークが 12 時間切断されます。ネットワーク切断中にソースサーバが再起動されます。

質問

このシナリオにおいて、DataKeeper Standard Edition のソースサーバのステータスはどのようになりますか。

回答

(ディスク上で) ソースサーバのビットマップは存在し続けているので、ソースの再起動による影響は受けません。ソースサーバの再起動時には部分同期のみが必要になります。ターゲットサーバは、ソースサーバに再接続されるまで

ミラーリング 状態になります。同期が開始されると、**同期中** 状態になります。

8.5.5.13. ターゲットドライブの全容量を再利用する

質問

ターゲットドライブをミラーリングで使用する必要がなくなったときに、ドライブをフル容量で利用できるようにする方法はありますか。

回答

ターゲットドライブは、ファイルシステムに SIOS DataKeeper の処理が加わっているため、実際のパーティションサイズより容量が小さくなっています。ディスクの管理ユーティリティでは完全なパーティションサイズが表示されますが、SIOS DataKeeper と Windows エクスプローラでは容量の小さいミラーサイズが表示されます。ドライブをフル容量で利用できるようにするには、パーティションを再フォーマットするか、または GParted (gparted.sourceforge.net/) のようなパーティション再構成ユーティリティを使用してください。

8.5.5.14. Windows Server フェールオーバークラスターロールから DataKeeper ストレージを削除する

Windows Serverフェールオーバー クラスタリングから既存のDataKeeperリソース/ミラーを削除します。この手順は、

- WSFCの既存の役割（ファイル共有、SAP、Oracle、SQLなど）に影響を与えません。
- deletelocalmirroronly や cleanupmirror などの様々な emcmd コマンドを実行する必要がありません。

注記: DataKeeper UIでは、「スイッチオーバー」、「ジョブを削除」、「ミラー削除」は、アクションパネルでグレーアウトされています。

理由: DataKeeperミラーがクラスター/WSFCの一部である場合、またはクラスター/WSFCの一部になった場合、すべての管理はWSFCレベルで行われるためです。

削除手順

フェールオーバークラスターマネージャーで、次の手順を実行します。

1. **[Roles]** パネルから、**[Storage]** と関連する **DataKeeper Volume** を選択します。
2. 右クリックして、**[Remove from the role you've created]** を選択し、**[Yes]** を選択します。
3. WFSC から、**Storage\Disk** を選択します。

   DataKeeper ボリュームが /Assigned To、Available Storage としてリストされます。
4. **[Remove]** を選択し、次に **[Yes]** を選択します。

   DataKeeper ストレージは、クラスター/WSFC のリソースではなくなりました。
5. DataKeeper UI > Action Panel で、**[Delete Job]** を選択します。「Are you sure you want to delete the 'Volume (drive)' and its mirror?」というメッセージが表示されたら、**[Yes]** を選択します。

   複数のミラー/ターゲットがある場合、**[Delete Mirror]** を選択するとジョブも削除されます。

8.5.5.15. ミラーボリュームのサイズ変更または拡張

質問

ミラーボリュームのサイズを変更したり、増やしたりすることはできますか。

回答

はいできます。バージョン 7.4 以降、ユーザはミラー設定を維持したまま、DataKeeper ボリュームを動的に拡張したり縮小したりすることができます。詳細については、DataKeeper ボリュームのサイズ変更 を参照してください。

8.5.5.16. スプリットブレインに関するFAQ

シナリオ

DataKeeper を非クラスタ環境で使用しています。あるサイトの　Server1 から、2つ目のサイトの Server2 にミラーリングしています。サイト間の VPN 通信が切れ、Server1 から Server2 にフェイルオーバする必要があります。どこからも Server1 にアクセスできません。実際 Server1 は 起動していますが、内部または外部からアクセスすることはできず、まだいくつかのプロセスはバックエンドで動作中です。

質問

どうすれば Server1 から Server2 にフェイルオーバすることができますか。

回答

SWITCHOVERVOLUME コマンドまたは DataKeeper UIの **[ミラーのスイッチオーバ]** オプションを使用して、Server2 にミラーのソースを切り替えてください。ターゲットがソースへの接続を行っている間、遅延が発生しますが、30 ～ 40秒程度で完了します。

質問

スイッチオーバ中に　Server1 と Server2 の両方がディスク (Server1 と Server2 の両方の F ボリューム) に新しいデータを書き込んでいます。接続がオンラインに戻ったときに、Server1 は自動的にターゲットになりますか。

回答

いいえ。このシナリオでは、スプリットブレイン 状態が発生します。以下のいずれかを実行して現象を解決してください。

- DataKeeper ユーザインターフェースを使用して、スプリットブレインのリカバリ手順 を実行してください。

> または

- ターゲットになるシステムで EMCMD PREPARETOBECOMETARGET コマンドを実行し、ソースになるシステムで CONTINUEMIRROR コマンドを実行してください。

質問

スプリットブレインを解決するための上記 2 つの方法のうち、どちらが推奨されますか。

回答

どちらの方法も同じ機能を実行するので、どちらでも希望される方を実行してください。

質問

ターゲットサーバに対するコマンドはソースサーバから実行可能ですか。

回答

はい。ターゲットサーバに対するコマンドはソースサーバから実行可能です。

質問

どのようにして DataKeeper は変更のあったブロックと変更のなかったブロックを同期しますか。

回答

スプリットブレイン状態を解消する際、ターゲットになっているシステム上のどの変更も上書きされ失われます。状態を保っておきたいしたいシステム上に変更がある場合は手動でそれらの変更をソースになるシステムへコピーしてください。

質問

スプリットブレイン状態を解消するために PREPARETOBECOMETARGET コマンドを実行する際、ソースから発生するのは全同期ですか、部分同期ですか。

回答

Preparetobecometarget コマンドはシステム上のミラーを削除しますが、ボリュームをロックしたままにします。ビットマップはそのままの状態なので、次のステップ (CONTINUEMIRROR) で部分同期を実行できます。

質問

どのようにすれば、スプリットブレイン状態をシミュレーションすることができますか。

回答

スプリットブレイン状態をシミュレーションするには、2 つのシステムが通信できないように、システム間のネットワークを切断してください。ターゲットで SWITCHOVERVOLUME コマンドを実行 (または DataKeeper UIの **[ミラーのスイッチオーバ]** オプションを選択) すると、両方ともソースになり、ネットワークに再接続します。この時点でスプリットブレイン状態となります。

質問

ソースで continuemirror を実行する前に、**PREPARETOBECOMETARGET** コマンドの完了を待たなければなりませんか。

回答

PREPARETOBECOMETARGET コマンドは即時に完了します。

8.5.5.17. ソースとターゲットの間のレプリケーションの停止

質問

ソースとターゲットボリュームの間のレプリケーションはどのように停止するのですか。

回答

レプリケーションはドライバレベルで実行されます。停止または中断するには、DataKeeper GUI または DataKeeper コマンドライン (EMCMD) から DataKeeper ドライバに対して、以下のいずれかを実行するコマンドを送信するしかありません。

- ミラーの一時停止 – ミラーエンドポイントは存在したままですが、すべてのレプリケーションが停止されます。ソースシステムに対する書き込みはトラックされるので、ミラーを再開したときにデータの部分再同期を行うだけでターゲットボリュームを同期状態に戻すことができます。

- ミラーの中断 – ミラーエンドポイントは存在したままですが、すべてのレプリケーションが停止されます。ソースシステムに対する書き込みはトラックされません。ミラーを再同期すると、ターゲットボリュームをソースと同期させるために必要なデータの完全再同期が開始されます。

- ミラーの削除 – ミラーエンドポイントを削除し、レプリケーションを停止します。

注記: DataKeeper サービスを停止してもレプリケーションは停止しません。

8.5.5.18. ボリュームシャドウコピーを使用する

質問

DataKeeper ボリュームではボリュームシャドウコピー (VSS) を使用できますか。

回答

DataKeeper ボリュームで VSS シャドウコピーを有効にすることができます。ただし、以下のガイドラインが適用されます。

- DataKeeper ボリュームには VSS スナップショットイメージを保存できません。DataKeeper ボリュームに VSS スナップショットを保存すると、DataKeeper はボリュームをロックして別のノードにスイッチオーバすることができません。
- DataKeeper ボリュームがスイッチオーバまたはフェイルオーバした場合、DataKeeper ボリュームから取得された以前のスナップショットは破棄され、再利用することができません。
- VSS スナップショットスケジュールは DataKeeper サーバ間でコピーされません。プライマリサーバで 1 日 2 回スナップショットを取得するように予定されているときにスイッチオーバが発生した場合、このスケジュールはバックアップサーバには渡されず、バックアップサーバで再定義する必要があります。
- スナップショットが以前有効になっていたサーバに切り替えられた場合、VSS スナップショットは自動的に再度有効になります。ただし、以前に作成したDataKeeper ボリュームのスナップショットは削除され再利用することはできません。

8.5.5.19. ミラーリングに使用できないボリューム

質問

ボリュームの中にミラーリングに使用できないものがあるのは、なぜですか。

回答

SIOS DataKeeper サービスは次の種類のディスクパーティションを処理対象から除外します。

- Windows システムボリューム
- Windows ページファイルを含むボリューム
- NTFS 形式以外のボリューム (FAT、Raw FS など)
- 固定ドライブ以外 (CD-ROM、フロッピーディスクなど)
- ソースボリュームよりサイズの小さいターゲットボリューム

8.5.6. トラブルシューティング

以下は、DataKeeper および DataKeeper Edition の既知の問題です。回避策や解決策についても記載しています。

- 指定したボリュームへのアクセス拒否
- クラスタリソースタイプとして使用できない DataKeeper ボリューム
- ミラーの作成に失敗する
- Hyper-V ホストクラスタエラー
- MaxResyncPasses 値
- ダイナミックディスクのミラーリング
- 新しいリソースがオフラインだがロック解除されている
- サーバログインアカウントおよびパスワードはクラスタの各サーバで同一である必要がある
- システムイベントログ - GUI でミラー作成に失敗する
- 以前のインストールパスを判定できない
- ユーザインターフェース - ミラーの作成に失敗する
- ユーザインターフェース - ミラーの片側しか表示されない
- Windows Server 2012 固有の問題
  - Windows Server 2012 DataKeeper MMC スナップインクラッシュ
  - Windows Server 2012 iSCSI ターゲットの役割がダイナミックディスクをサポートしない
  - Windows Server 2012 NIC チーミングの問題
- Windows Server 2016 に固有の問題
  - 偶発的なジョブ作成の失敗
  - ファイルサーバーの役割を作成するとサーバー マネージャーまたはフェールオーバー クラスター マネージャーを使用してWSFC 2016ファイル共有を作成できない

8.5.6.1. 既知の問題と回避策

以下は、DataKeeper および DataKeeper Edition の既知の問題です。回避策や解決策についても記載しています。

- 指定したボリュームへのアクセス拒否
- DataKeeper ボリュームをクラスタリソースタイプとして使用できない
- ミラーの作成に失敗する
- Hyper-V ホストクラスタエラー
- MaxResyncPasses 値
- ダイナミックディスクのミラーリング
- 新しいリソースがオフラインだがロック解除されている
- サーバログインアカウントおよびパスワードはクラスタの各サーバで同一である必要がある
- システムイベントログ - GUI でミラー作成に失敗する
- 以前のインストールパスを確認できない
- ユーザインターフェース - ミラーの作成に失敗する
- ユーザインターフェース - ミラーの片側しか表示されない
- Windows Server 2012 固有の問題
  - Windows Server 2012 DataKeeper MMC スナップインのクラッシュ
  - Windows Server 2012 iSCSI Target の役割はダイナミックディスクをサポートしていない
  - ミラー作成中に Windows Server 2012 のデフォルト情報が表示されない
  - Windows Server 2012 NIC チーミングの問題
- Windows Server 2016 固有の問題
  - 偶発的なジョブ作成の失敗
  - ファイルサーバーの役割を作成するとサーバー マネージャーまたはフェールオーバー クラスター マネージ

ャーを使用して WSFC 2016 ファイル共有を作成できない

8.5.6.1.1. 指定したボリュームへのアクセス拒否

指定したボリュームへのアクセスが拒否された場合は、ミラーを作成しようとしているボリュームに他のアプリケーションがアクセスしていないか確認してください。SIOS DataKeeper では、ミラーの作成中はターゲットシステム上でボリュームをロックして他からのアクセスを排除する必要があります。

特に、Distributed Tracking Client service は、Windows ではデフォルトで実行されるように設定されており、ボリュームごとにファイルハンドルを 2 つ開いたままにします。ボリュームに SIOS DataKeeper のターゲットを格納している場合は、SIOS DataKeeper のドライバはボリュームをロックできません。したがって、Distributed Tracking Client service を停止し、スタートアップの種類を [手動] に設定してください。

8.5.6.1.2. LifeKeeper および DataKeeper for Windows のアンチウイルスソフトウェアの除外リスト

説明

ウイルス対策ソフトウェアにより、LifeKeeper は LifeKeeper レジストリキーを更新できなくなります。
ウイルス対策ソフトウェアは LifeKeeper と DataKeeper の実行可能ファイルも隔離するため、LifeKeeper と DataKeeper が正常に実行されなくなります。

推奨される対応

LifeKeeper および DataKeeper に関し、ウイルス対策ソフトウェアで除外するものは以下の通りです。

- SPS:

  *C:\LK** フォルダ（または LifeKeeper がインストールされているフォルダ）

- DataKeeper:

  C:\Program Files (x86)\SIOS\DataKeeper フォルダ（またはDataKeeperがインストールされているフォルダ）

- ビットマップファイルの場所（デフォルトでは c: ドライブにありますが、再配置される場合があります *C:\Program Files (x86)\SIOS\DataKeeper\Bitmaps* ）

これらの場所にはすべての実行可能ファイルが含まれていますが、ウイルス対策ソフトウェアによってこれらのファイルが隔離され、LifeKeeper または DataKeeper が動作不能になることがあります。

LifeKeeper と DataKeeper が使用するレジストリキーのリストについては、レジストリエントリ を参照してください。

また、

UpperFilters レジストリキーは以下の場所にあります。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}

8.5.6.1.3. DataKeeper ボリュームをクラスタリソースタイプとして使用できない

WSFC サーバ - Microsoft WSFC 環境に DataKeeper をインストールした後、DataKeeper ボリュームをクラスタリソースタイプとして使用できない

エラー / メッセージ

Microsoft WSFC 環境に DataKeeper をインストールした後、DataKeeper ボリュームをクラスタリソースタイプとして使用することはできません。

イベントログには次のメッセージが記録されます。「 **Failed to register the 'DataKeeper Volume' Resource DLL (DataKeeperVolume.dll).Error: 70** 」

説明

リソース DLL を登録するには、すべてのクラスタノードが起動し、オンラインである必要があります。既存のクラスタのいずれかのノードが現在使用できない場合 (オフライン、クラスタサービスの停止など)、自動 DataKeeper リソース DLL 登録はインストール時や更新時に失敗する可能性があります。

推奨される処置

この問題は通常、他のクラスタノードがオンラインになると自動的に修正されます。DataKeeper サービスが起動されるとすぐに、リソース DLL 登録がそのノードから試行され、クラスタ全体で登録が実行されます。自動リソース DLL 登録が実行されない場合には、すべてのクラスタノードが起動しオンラインになった後、いずれかのノードで DataKeeper サービスを再起動してください。登録プロセスは、DataKeeper サービスが起動してから 60 秒後に開始されます。

8.5.6.1.4. ミラーの作成に失敗する

ユーザインターフェース - ミラーを作成できない - アプリケーションイベントログ

エラー / メッセージ

アプリケーションイベントログ に以下のように記録されます。

File:.\GuiThread.cpp Line:3099 Attempt to connect to remote system REMOTESERVER failed with error 5. Please ensure that the local security policy for "**Network Access: Let Everyone permissions apply to anonymous users** " is enabled on all the servers running DataKeeper.

確認: 指定されたシステムのローカルセキュリティポリシー設定。

説明

ミラーの作成に失敗しました。ミラーは作成されましたが、ジョブに格納されていません。

推奨される処置

ローカルセキュリティポリシーを変更してコマンドプロンプトを開き、「`%EXTMIRRBASE %\emcmd . deletemirror <volume>`」を実行してから、ミラー作成処理を再度実行してください。

8.5.6.1.5. Hyper-V ホストクラスタエラー

VMがクラスタ化されている状態での仮想マシンの設定変更後に、フェイルオーバクラスタエラーが発生する

説明

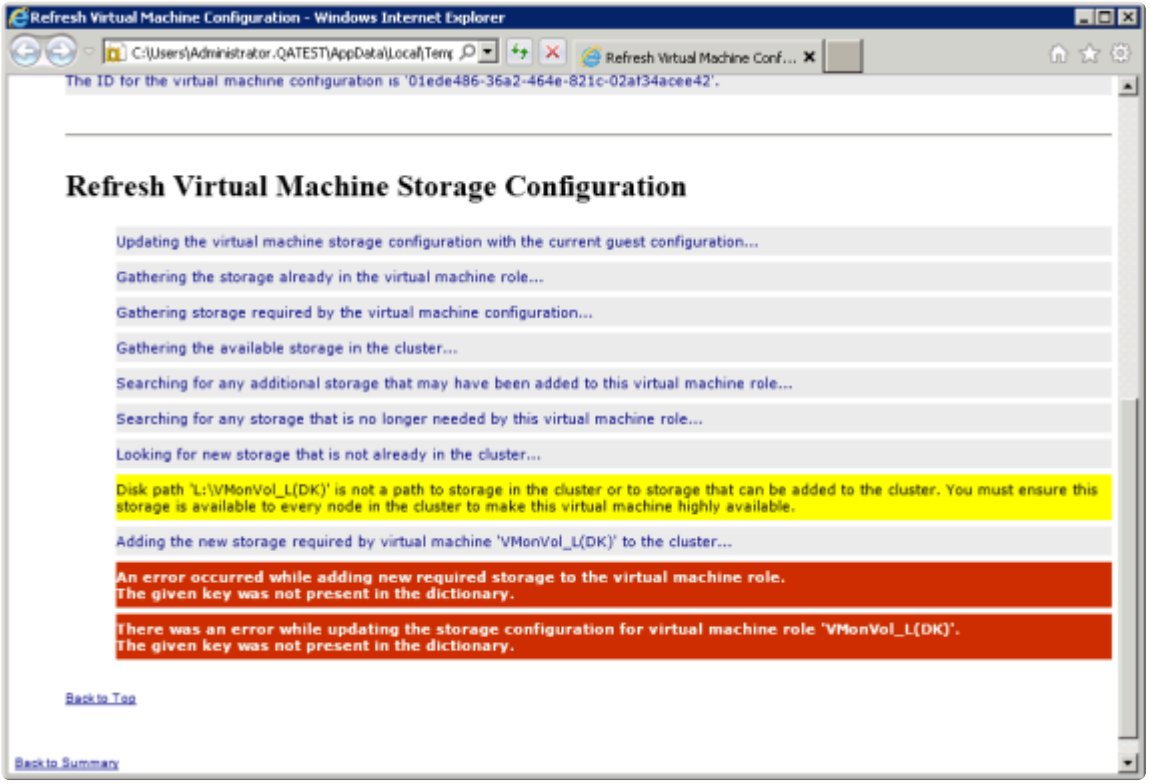
VMをクラスタ化している状態でフェイルオーバクラスタマネージャを使ってVM 設定の変更を行う際にVMに対してネットワークインターフェースの追加などを行うと、「 **Refresh Virtual Machine Storage Configuration** 」エラーが表示され、VM の別のクラスタノードへの Quick Migration や Live Migration に失敗します。

この問題は以下の状態にあてはまる場合に発生します。

1. VM がクラスタ化されている。
2. VM ネットワーク設定を変更するためにフェイルオーバクラスタマネージャが使用されている。
3. クラスタ共有ディスク以外のストレージが DataKeeper ボリューム複製ストレージなどの VM ストレージに使用されている。

3 つすべての状態にあてはまる場合にこのエラーが発生します。このエラーは、VM がクラスタ外に存在し、VM ネットワーク設定の変更に Hyper-V マネージャが使用されていれば発生しません。

以下がその際に表示される画面です。

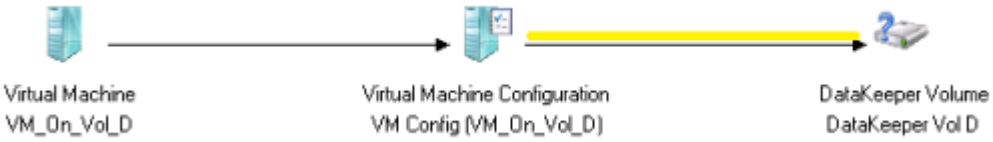


推奨される処置

ソリューションの詳細については、Microsoft にお問い合わせください。

Microsoft Hotfix をインストールせずに仮想マシンのネットワークアダプタを変更する場合は、以下の手順を実行してください。

1. VM をクラスタ外へ移動させる。
2. NIC 接続の仮想ネットワーク名がすべてのクラスタノードで一意であることを確認する。
3. Hyper-V マネージャを使用して仮想マシンのネットワーク設定を変更する。
4. VM をクラスタへ戻し、DataKeeper ボリュームリソースを VM リソース階層に移動させる。
5. 仮想マシン設定リソースを Datakeeper ボリュームリソース階層に再作成する。(下記の黄線部分)



8.5.6.1.6. Live Migration の失敗

仮想ネットワーク名が異なる場合、Live Migration に失敗する

説明

NIC 接続の **仮想ネットワーク名** がクラスタノードによって異なる場合、**フェイルオーバクラスタマネージャ** で別のノードへの仮想マシンの Live Migration を実行しようとすると、マイグレーションで「失敗」ステータスが発行されます。

推奨される対策

NIC 接続の **仮想ネットワーク名** がすべてのクラスタノードで一意であることを確認してください。

8.5.6.1.7. MaxResyncPasses 値

ボリュームの再同期中にインテントログに記録されるパスが **MaxResyncPasses** レジストリ値 (デフォルトは 200) を超えると、SIOS DataKeeper は **イベントログ** に、再同期プロセスのパス数が大量なので、再同期されているドライブに書き込みを行っているその他のプロセスを停止するよう管理者に対して要求するメッセージを記録します。その後ミラーは **一時停止** の状態になります。再同期処理の時間を長くしたい場合には、レジストリの **MaxResyncPasses** の値を増加させてください。

8.5.6.1.8. ダイナミックディスクのミラーリング

ベーシックディスク から **ダイナミックディスク** に変更すると、基盤となるボリューム GUID は再起動時に OS によって変更される場合があります。これによって、DataKeeper ミラーは中断されます。

推奨される処置

ダイナミックディスクのミラーリングを行う場合は、ミラーを作成する前に **ダイナミック** ボリュームを作成し、再起動を実行してください。ミラーがすでに作成されている場合は、ダイナミックボリュームの作成前に削除する必要があります。

8.5.6.1.9. 新しいリソースはオフラインだがロック解除されている

WSFC サーバ - 新しく作成されたリソースはオフラインに見えるが、ロック解除されている

エラー / メッセージ

新しく作成されたリソースはオフラインに見えますが、ロック解除されています。

説明

新しいリソースは、使用前は常にオフラインであり、ロック解除されています。

推奨される処置

リソースをオンラインに切り替えてください。

8.5.6.1.10. サーバログインアカウントおよびパスワードはクラスタの各サーバで同一である必要がある

サーバの **ログインアカウント** と **パスワード** が各サーバで異なる場合、DataKeeper GUI からクラスタ内のターゲットサーバに接続することができません。

エラーメッセージ

エラーコード 1326 がアプリケーションログに表示されます (**注記**: イベント ID が 0 で、エラーコードが 2 であることもあります)。

```
SteelEye.Dialogs.AddServerWindow: Failed to connect to server:
172.17.105.112 System.ApplicationException: Failed to open a connection
to 172.17.105.112 (error_code = 1326) at
SteelEye.DAO.Impl.DataReplication.ClientLibrarySDRService.throwIfNonZero(UInt32
errorCode, String message) at
SteelEye.DAO.Impl.DataReplication.ClientLibrarySDRService.getServiceInfo(String
serverName) at
SteelEye.DAO.Impl.DataReplication.CachingSDRService.<>c__DisplayClass2.b__0()
at SteelEye.DAO.Impl.DataReplication.Cacher`1.fetch(String typekey,
String datakey, Fetcher fetcher) at
SteelEye.DAO.Impl.DataReplication.CachingSDRService.getServiceInfo(String
serverName) at
SteelEye.DataKeeper.SDR.SDRDataKeeperService.ConnectToServer(String
serverName) at
SteelEye.Dialogs.AddServerWindow.<>c__DisplayClass4.b__0(Object s,
DoWorkEventArgs e) at
System.ComponentModel.BackgroundWorker.WorkerThreadStart(Object argument)

net helpmsg 1326 shows:

Logon failure: unknown user name or bad password
```

説明 / 原因

DataKeeper の起動に使用されているサービスアカウントのユーザ名とパスワードが両方のサーバで同じであり、ファイアウォールがサーバで無効になっていますが、サーバ自体へのログインに使用するパスワードが異なっています。

推奨される処置

DataKeeper GUI では、サーバのログイン ID とパスワードを使用します。そのため、サーバ自体へのログインに使用するユーザ名とパスワードは各サーバで同じである必要があり、管理者権限を持っている必要があります。

8.5.6.1.11. システムイベントログ – GUI でのミラー作成の失敗

エラー / メッセージ

GUI でのミラー作成に失敗します。

説明

これは、vmms.exe プログラムがボリュームを保持し、SIOS DataKeeper がロックするのを防いでいる場合に発生することがあります。

8.5.6.1.12. 以前のインストールパスを確認できない

インストール - 致命的なエラー: 以前のインストールパスを確認できない

エラー / メッセージ

致命的なエラー: 以前のインストールパスを確認できません。DataKeeper をアンインストールまたは再インストールすることができません。

説明

DataKeeper の「 **修復** 」または「 **アンインストール** 」を実行する場合、***HKLM\System\CurrentControlSet\Control\Session Manager\Environment*** では、レジストリ内の DataKeeper のインストールパスで「 **ExtMirrBase** 」値を見つけることはできません。

推奨される処置

以下のいずれかを実行してください。

・**Environment** キーに「 **ExtMirrBase** 」を REG_SZ として作成し、値に DataKeeper のインストールパス (***C:\Program Files(x86)\SIOS\DataKeeper***) を設定してください。

・InstallShield で DataKeeper の新規インストールを強制的に実行する場合は、以下のレジストリキーを削除してください。

```
HKLM\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\
Uninstall\
{B00365F8-E4E0-11D5-8323-0050DA240D61}.
```

これは DataKeeper v7.1.0 製品のために InstallShield によって作成されるインストールキーです。

8.5.6.1.13. ユーザインターフェース – ミラーを作成できない

ユーザインターフェース - ミラーを作成できない、イベント ID 137

エラー / メッセージ

ミラーの作成に失敗しました。
イベント ID: 137
システムイベントログ

ターゲットマシンでミラーを初期化できません。

ボリュームデバイス:
ソースボリューム: E
ターゲットマシン: 10.17.103.135
ターゲットボリューム: E
失敗した操作: ターゲット報告エラー
エラーコード: 0xC0000055

説明

DataKeeper はミラー作成時にターゲットボリュームをロックできません。

推奨される処置

1. いずれかのシステムで Distributed Link Tracking Client サービスが実行されていないことを確認してください。

2. DataKeeper がターゲットボリュームをロックするのを妨げている可能性があるその他のプロセス (アンチウイルスソフトウェアなど) を停止してください。

3. ミラーを再作成してください。

8.5.6.1.14. ユーザインターフェース – ミラーの片側しか表示されない

SIOS DataKeeper UI でボリュームが 1 つだけソースとして表示され、対応するターゲットも使用できる状態で表示される場合、あるいは逆にボリュームが 1 つだけターゲットとして表示され、対応するソースボリュームも使用できる状態で表示される場合は、コマンドラインユーティリティを使用して SIOS DataKeeper GUI を強制的に更新するか、その片側状態のミラーを削除することができます。コマンドプロンプトから予期しないミラー状態が表示されているサーバ上の SIOS DataKeeper ディレクトリに移動し、以下の手順を実行してください。

1. ミラーがソース上で **一時停止** 状態または **中断** 状態にないことを確認してください。その場合は、ソース上でミラーを再開してください。これによって、ターゲットに対してミラーが再構築されます。

2. 次のコマンドを実行してください。EMCMD <system name> UpdateVolumeInfo <volume letter>

   意味は以下のとおりです。

   <system name> はシステムの名前です。

   <volume letter> はボリュームレターです。

3. 手順 1 で問題が解決されない場合は、SIOS DataKeeper を停止してから再起動してください。

8.5.6.1.15. Windows Server 2012 固有の問題

Windows Server 2012 に関する問題については、以下のトピックを参照してください。

Windows Server 2012 DataKeeper MMC スナップインクラッシュ

Windows Server 2012 iSCSI ターゲットの役割がダイナミックディスクをサポートしない

ミラー作成中に Windows Server 2012 のデフォルト情報が表示されない

Windows Server 2012 NIC チーミングの問題

8.5.6.1.15.1. Windows Server 2012 MMC スナップインのクラッシュ

Windows Server 2012 MMC スナップインのクラッシュ

説明

Windows Server 2012 上で DataKeeper のユーザインターフェース (MMC スナップイン) を使用している場合、内部の .NET または Windows Presentation Foundation (WPF) の問題により、mmc.exe プロセスが予期せずクラッシュすることがあります。エラーは、画面やイベントビューアに表示されることがあります。

推奨される処置

このクラッシュは、スナップインの接続先であったサーバにも、クラッシュ時に確立された DataKeeper ミラーにも影響しません。MMC スナップインを問題なく再起動できることがあります。単に UI を閉じ、再起動してください。

このエラー時にログに記録されることがある **アプリケーションイベントログのメッセージ** 例を以下に示します。

```
Log Name: Application
Source: Desktop Window Manager
Date: 11/28/2012 8:34:00 AM
Event ID: 9009
Task Category: None
Level: Information
Keywords: Classic
User: N/A
Computer: CAE-QA-V96.QAGROUP.COM
Description:
The Desktop Window Manager has exited with code (0xd00002fe)
```

```
Log Name: Application
Source: .NET Runtime
Date: 11/28/2012 8:34:00 AM
Event ID: 1026
Task Category: None
Level: Error
Keywords: Classic
User: N/A
```

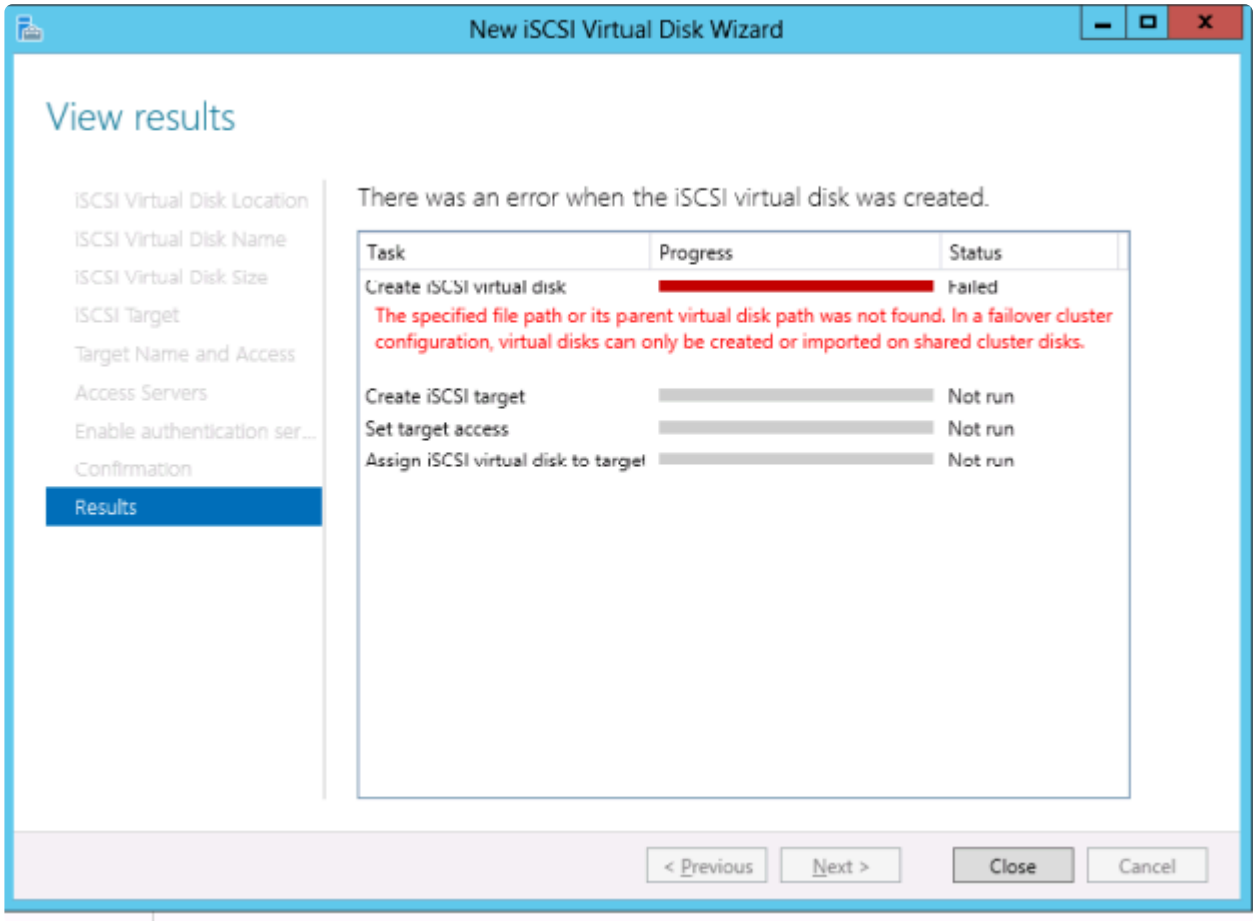
Computer: CAE-QA-V96.QAGROUP.COM
Description:
Application: mmc.exe
Framework Version: v4.0.30319
Description:The process was terminated due to an unhandled exception.

Log Name: Application
Source: Application Error
Date: 11/28/2012 8:34:00 AM
Event ID: 1000
Task Category: (100)
Level: Error
Keywords: Classic
User: N/A
Computer: CAE-QA-V96.QAGROUP.COM
Description:
Faulting application name: mmc.exe, version: 6.2.9200.16384, time stamp: 0×50109efd
Faulting module name: KERNELBASE.dll, version: 6.2.9200.16384, time stamp: 0×5010ab2d
Exception code: 0xe0434352
Fault offset: 0×00000000000189cc
Faulting process id: 0xdc4
Faulting application start time: 0×01cdccd27c68a1c6
Faulting application path: C:\Windows\system32\mmc.exe
Faulting module path: C:\Windows\system32\KERNELBASE.dll
Report Id: 443c3ed3-3960-11e2-9400-0050569b131b
Faulting package full name:
Faulting package-relative application ID:

8.5.6.1.15.2. Windows Server 2012 iSCSI Target の役割はダイナミックディスクをサポートしていない

説明

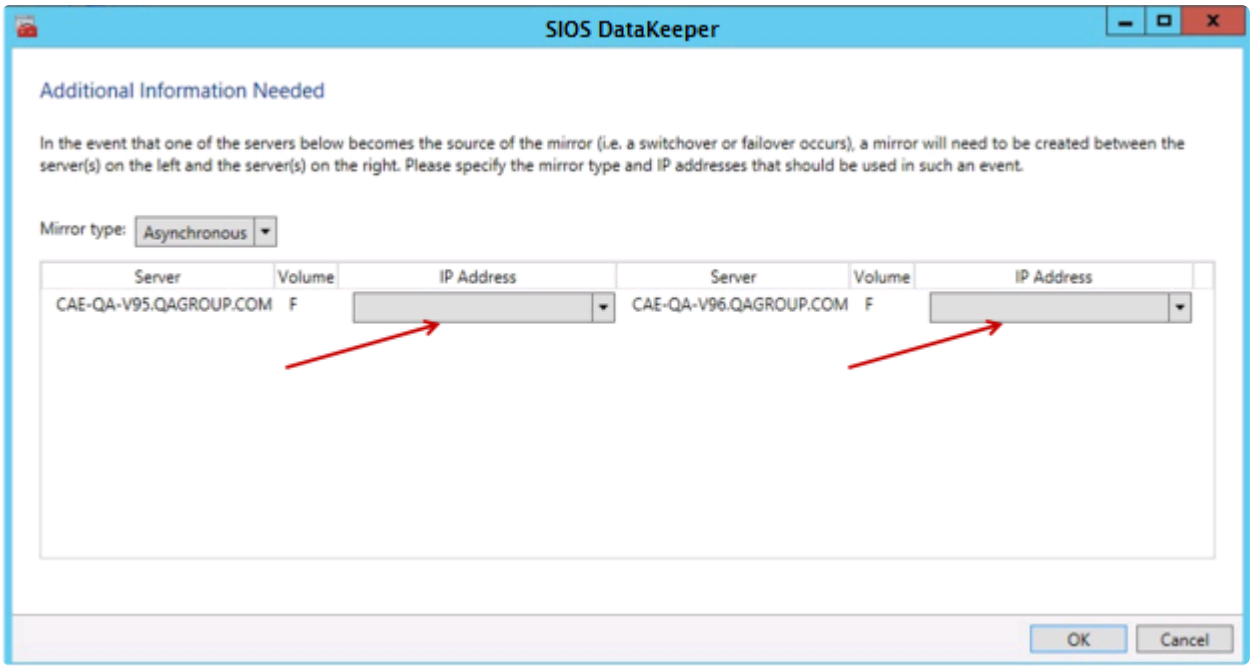
iSCSI Target の役割は、**ベーシックディスク** 上に配置された **シンプルボリューム** のミラーである DataKeeper ボリュームしかサポートしていません。いずれかのミラーが、ソースシステムまたはターゲットシステムでダイナミックディスク上のストライプボリュームやスパンボリュームなどのボリュームを使用している場合、それらの DataKeeper ボリュームリソースをストレージに使用する iSCSI Target の役割は作成できません。



8.5.6.1.15.3. ミラー作成中にWindows Server 2012のデフォルト情報が表示されない

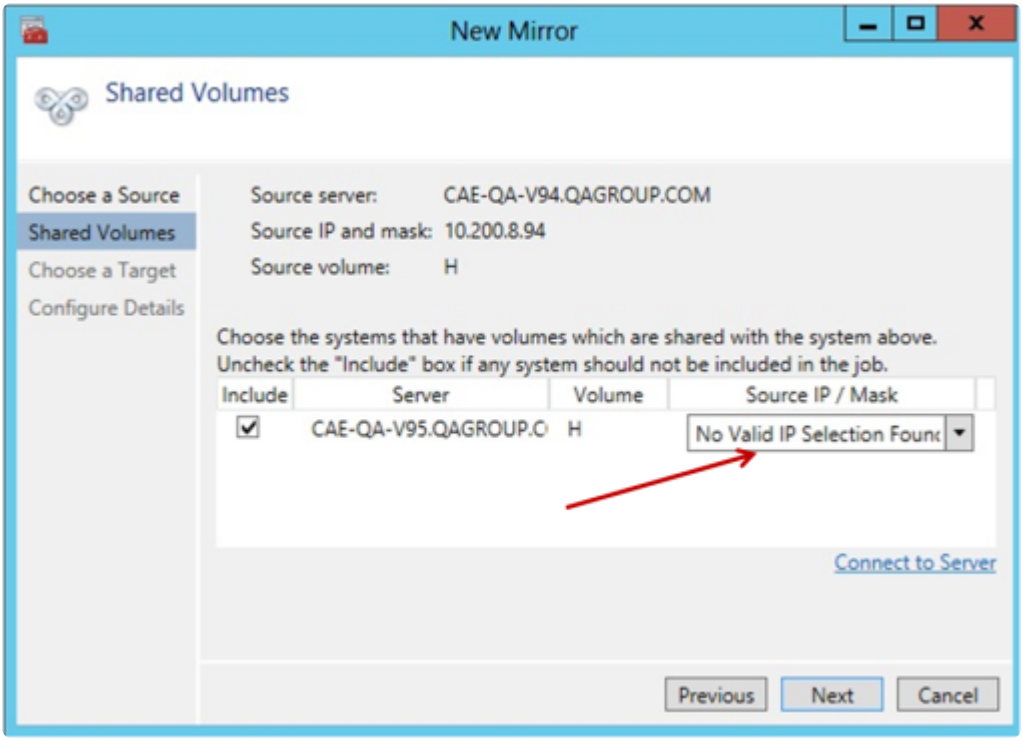
マルチターゲットでのミラーの作成

最初の問題は、マルチターゲット構成でのミラー作成中に生じるものです。最後のステップで、ユーザーは2次関係情報の入力を求められます。以前のバージョンのOSでは、デフォルトの送信元IPが **[Additional Information Needed]** ダイアログで提供されていました。しかしWindows Server 2012では、このデフォルトのIPが提供されていないにもかかわらず、正しいIPアドレスを選択する必要があります。IPアドレスを選択せずに **[OK]** をクリックした場合もミラーは作成されますが、重要な関係情報は表示されません。



共有ボリュームを使用したミラーの作成

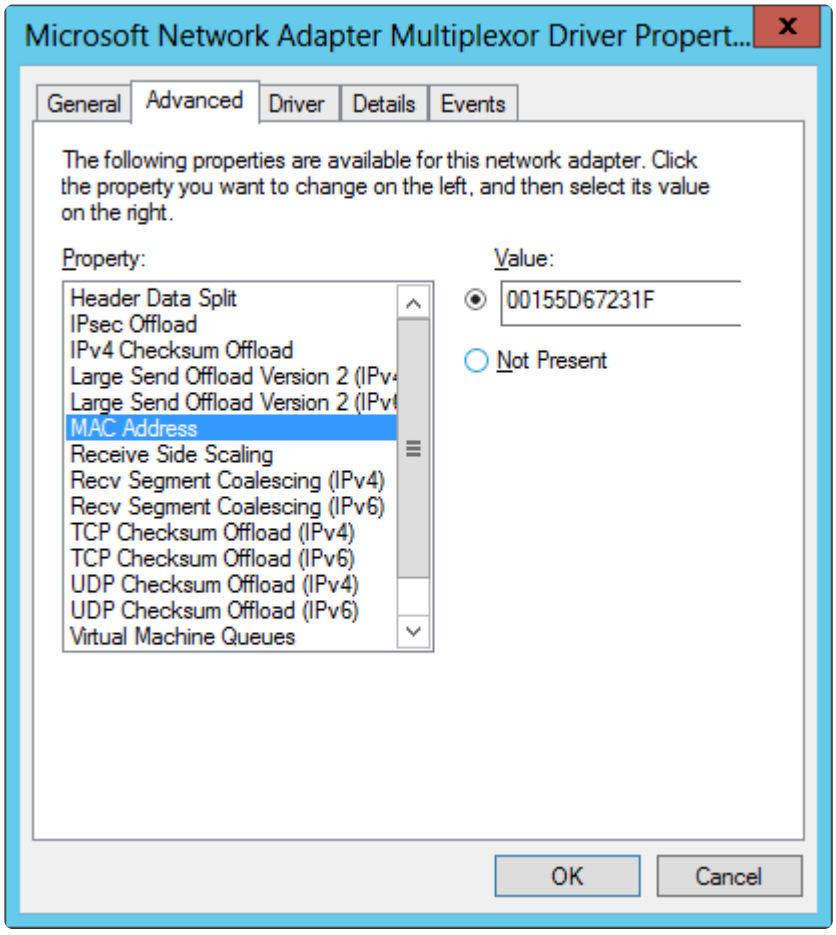
もう1つの問題は、共有ボリュームでミラーを作成する際の **[Shared Volumes]** ダイアログボックスです。以前のOSバージョンではデフォルトの送信元IPがこの画面に表示されていました。しかしWindows Server 2012では、このダイアログには **[No Valid IP Selection Found]** と表示されるにもかかわらず、正しい送信元IPを選択する必要があります。


New Mirror
Shared Volumes
Choose a Source
Shared Volumes
Choose a Target
Configure Details
Source server: CAE-QA-V94.QAGROUP.COM
Source IP and mask: 10.200.8.94
Source volume: H
Choose the systems that have volumes which are shared with the system above.
Uncheck the "Include" box if any system should not be included in the job.
Include
Server
Volume
Source IP / Mask
CAE-QA-V95.QAGROUP.C
H
No Valid IP Selection Found
Connect to Server
Previous
Next
Cancel

8.5.6.1.15.4. Windows Server 2012 NIC チーミングの問題

Windows Server 2012 の **NIC チーミング** 機能を使用している場合、Windows 2012 では、1 つのアダプタの MAC アドレスしかライセンスの対象として報告されません。基となるアダプタが多数ある場合、MAC アドレスは任意に変わるため、Windows で、許可されていないアダプタのいずれかが選択されることがあります。

この問題を解決するには、仮想チームアダプタの **MAC アドレス** プロパティを設定します。このプロパティは、**アダプタのプロパティ** の **[詳細設定]** タブを使用して変更できます (下図を参照)。



WSFC 2008 R2 SP1 手順の変更

説明

WSFC 2008 R2 SP1 を使用する場合、従来の 1×1 2 ノード WSFC クラスタを共有複製 3 ノードクラスタに拡張するための手順が変更されています。DataKeeper 共有ボリュームをホストしているノードを追加するために WSFC mmc GUI を使用することはできません。

推奨される処置

WSFC 2008 R2 SP1 を使用している場合、共有 DataKeeper ボリュームを持つノードを既存のクラスタに安全に追加するには、WSFC コマンドラインツール「 *cluster /add /node:* 」を使用するしかありません。**非常に重要:** 詳細については、従来の 2 ノードクラスタを Shared-Replicated 設定に拡張する を参照してください。

8.5.6.1.16. Windows Server 2016 固有の問題

Windows Server 2016 に関する問題については、以下のトピックを参照してください。

偶発的なジョブ作成の失敗

ファイルサーバーの役割を作成するとサーバー マネージャーまたはフェールオーバー クラスター マネージャーを使用して WSFC 2016 ファイル共有を作成できない

8.5.6.1.16.1. 偶発的なジョブ作成の失敗

説明

Windows 2016 システムでは、新規ジョブの作成が時折失敗することがあります。失敗した場合は再度作成しなおしてください。

8.5.6.1.16.2. ファイルサーバーの役割を作成するとサーバー マネージャーまたはフェールオーバー クラスター マネージャーを使用して WSFC 2016 ファイル共有を作成できない

説明

クラスターのファイルサーバーの役割が作成されると、**サーバー マネージャー** も **フェールオーバー クラスター マネージャー** も最初に共有を作成する際に使用できなくなります。

推奨される処置

Microsoft の記事 2804526 では、この問題を含むいくつかのWSFC Server 2016 の問題に関する概要を説明しています。この記事では、Windows Server 2012 のいくつかの修正プログラムを紹介しています。

Windows Server 2016 でフェールオーバー クラスター マネージャーを使用している場合、[ファイル共有の追加] ショートカットを右クリックしても（サードパーティ製のストレージを使用している場合は右側のパネルの [ファイル共有の追加] ボタンを使用しても）ファイル共有ウィザードは起動しません。Microsoft Hotfix 2795993 をインストールするとこの問題は解決します。

または、次のWindows Update モジュールを Windows Server 2012 にインストールしてもこの問題は解決します。

KB2815769 KB2803676 KB2785094 KB2779768 KB2771744 KB2761094

KB2812829 KB2800088 KB2784160 KB2779562 KB2771431 KB2758246

KB2812822 KB2795944 KB2783251 KB2778171 KB2770917 KB2756872

KB2811660 KB2790920 KB2782419 KB2777166 KB2769165 KB2751352

KB2803748 KB2788350 KB2780342 KB2771821 KB2764870

上記の **Windows Server 2012 用の Windows Update** リストは、2013年4月2日時点の累計です。また当社のラボテストで Hotfix 2795993 はすべての Windows Server 2012 システムにはインストールされていないことが判明しました。このため、最低でも上記の Windows Update モジュールをインストールすることをお勧めします。

Windows Server 2012 では、サードパーティ製のストレージを使用している場合、サーバー マネージャーツールを使用してクラスター化されたボリューム上に共有を作成することはできません。
Microsoft Hotfix 2796000 をインストールするとこの問題を解決できます。また、上記の Windows Update モジュールをインストールしてもこの問題を解決できます。

上記をインストールしない場合の回避策は、**Windows エクスプローラー** を使用して共有を作成することです。Windows エクスプローラーで共有を作成したら、**サーバー マネージャー** または **フェールオーバー クラスターコンソール** を使用してアクセス許可やファイル共有のその他の設定を調整できます。

8.5.6.2. 制限事項

以下は DataKeeper および DataKeeper Edition に関連する制限事項です。回避策や解決策についても記載しています。

Bitlocker は DataKeeper をサポートしない

CHANGEMIRRORENDPOINTS

CHKDSK

DataKeeper ボリュームのサイズ変更の制限

ビットマップ用ディレクトリは再配置の前に作成する必要がある

同一ジョブ内で IP アドレスの重複は認められない

同期レプリケーションによる集中 I-O

リソースタグ名の制限

8.5.6.2.1. Bitlocker は DataKeeper をサポートしていない

Microsoft によると、BitLocker のソフトウェア RAID 設定での動作はサポートされていません。DataKeeper は本質的にソフトウェア RAID 1 であるため、Bitlocker を DataKeeper とともに使用することはできません。

注記: EFS (Encrypting File System)とTDE (Transparent Disk Encryption)は、DataKeeperと互換性があるので、暗号化されたデータに使用することができます。これに加えて、両方ともDataKeeperによってネットワークに送られるデータの暗号化も行います。

次の記事およびセクションで具体的な説明を参照できます。

https://technet.microsoft.com/en-us/library/ee449438#BKMK_R2disks

8.5.6.2.2. CHANGEMIRRORENDPOINTS

説明

このコマンドを使用すると DataKeeper によって保護されているボリュームをネットワーク上の別の場所に移動することができますが、3 ノード以下で設定されたミラーボリュームのエンドポイントの変更しかサポートしません。

回避策

4 ノード以上の設定では、ローカルサイトで最終的なエンドポイントのミラーを削除して再作成し、route add を使用してミラーの作成と再同期を行ってから、サーバを最終的な位置/アドレス/DR サイトに移動する必要があります。

8.5.6.2.3. CHKDSK

説明

SIOS DataKeeper で複製したボリュームで CHKDSK を実行する必要がある場合は、ミラーを **一時停止** してから CHKDSK を起動してください。CHKDSK を実行後、ミラーを **再開** してください。部分再同期 が実行され (CHKDSK による書き込みがアップデートされます)、レプリケーションが再開します。

注記: ビットマップファイル (非共有ボリューム用) は BitmapBaseDir により定義されるデフォルトの保存場所の C ドライブに配置されます。**ソース** システムの C ドライブで CHKDSK を実行すると、アクティブなビットマップファイルが原因でエラーが発生します。スイッチオーバを実行してソースをターゲットにし、ビットマップファイルを非アクティブ化してください。その後、そのシステムを新しいターゲット (元ソース) として、CHKDSK を実行できるようになります。

8.5.6.2.4. DataKeeper ボリュームのサイズ変更の制限事項

DataKeeper ボリュームのサイズ変更手順を実行するのは、1 度に 1 つのボリュームだけにしてください。

8.5.6.2.5. 再配置の前にビットマップ用ディレクトリを作成する必要がある

説明

ビットマップファイルをデフォルトの場所 (***%EXTMIRRBASE%\Bitmaps***) から移動する場合は、新しいディレクトリを作成してからレジストリで位置を変更し、システムを再起動する必要があります。

8.5.6.2.6. 同一ジョブ内で IP アドレスの重複は認められない

DataKeeper のジョブには、ジョブの一部としてすべてのミラーのエンドポイント情報が含まれます。この情報には各ミラーエンドポイントのホスト名、IP アドレス、ドライブ文字が含まれます。

1 つのジョブの中で、1 つの IP アドレスを複数のノード上に重複させることはできません。1 つのジョブに 4 つのノードがある場合の例では、ノード「A」および「B」をプライベートネットワーク接続で構成し、ノード「C」および「D」を別のプライベートネットワーク接続で構成することができます。しかし、それらのプライベートネットワーク上の IP アドレスは各ノードごとに必ずユニークでなければなりません。仮にノード A と B のレプリケーションで 192.168.0.1 と 192.168.0.2 を使用するとした場合、ノード C と D のレプリケーションにも 192.168.0.1 と 192.168.0.2 を使用することはできません。

8.5.6.2.7. 同期レプリケーションによる大量の I/O

説明

同期レプリケーションの性質 (ターゲットシステムからの応答を待機する間、ボリュームの書き込みをブロックする) のため、ミラーボリュームに書き込みを行うアプリケーションの動作が停滞する場合があります。この現象の頻度は、「システムリソース」に対する「ボリューム I/O トラフィック」の比率に大きく依存しています。ボリュームに対して継続的かつ大量の I/O トラフィックが予想される場合や SIOS DataKeeper を低帯域ネットワークで使用する場合には、非同期レプリケーションを使用してください。

8.5.6.2.8. リソースタグ名の制限

タグ名の長さ

SIOS Protection Suite DataKeeper 内のすべてのタグは、256 文字以内にする必要があります。

有効な「特殊」文字

-	_	.	/						

タグの最初の文字に「.」および「/」を使用することはできません。

無効な文字

+	;	:	!	@	#	$	*	=	「スペース」

8.6. トラブルシューティング

このセクションでは、既知の問題および制限事項に関する重要な情報とそれらに対するワークアラウンドおよび/また解決方法について説明します。

LifeKeeper および DataKeeper for Windows のアンチウイルスソフトウェアの除外リスト

アプレットのトラブルシューティング

LifeKeeper で OpenJDK をデプロイする

コマンドプロンプトから LifeKeeper コマンドを実行しようとしたときにエラーが発生する

GUI エラーメッセージ

GUI ネットワーク関連 - サーバへの初期接続の失敗

GUI ネットワーク関連 - Windows プラットフォームにおける長期の接続遅延

GUI ネットワーク関連 - 接続試行時に生成される NoRouteToHostException メッセージ

GUI ネットワーク関連 - 接続試行時に生成される不明なホスト例外メッセージ

GUI サーバのトラブルシューティング

エラーが出力されずに LifeKeeper GUI アプリケーションの起動に失敗する

Java 1.8.xのLifeKeeper GUI問題

ヘルスチェックタイムアウト

不完全なリソース作成

インストール - アクセス拒否

IP リソース作成の問題

Java の署名付き / 署名なし混在コードの警告

参照リストに LANMAN 名が 2 回表示される場合がある

ライセンス - ライセンスされたリカバリキットリソースが起動しない

ライセンス - ライセンスキーが見つからない

SPS Web クライアントがロックされる場合がある

SPS Web クライアントがロックされる場合がある - 既存の階層が複数変更された

新しい評価ライセンスキーのエラー

SPS のサーバ障害からの復旧

サービス休止中の階層のリカバリ

LifeKeeper から DataKeeper ストレージを削除する

リカバリキットのアンインストール時に Remove がハングする

複製ボリュームのスイッチオーバの失敗

リソースタグ名の制限

リストアおよびヘルスチェックアカウントの障害

SQL 2008

SQL Server Reporting Services

2 サーバクラスタの問題

不明なユーザ名または誤ったパスワード

Web クライアントのトラブルシューティング

Win2008 - IIS リソース階層作成エラー

8.6.1. LifeKeeper および DataKeeper for Windows のアンチウイルスソフトウェアの除外リスト

説明

ウイルス対策ソフトウェアにより、LifeKeeper は LifeKeeper レジストリキーを更新できなくなります。
ウイルス対策ソフトウェアは LifeKeeper と DataKeeper の実行可能ファイルも隔離するため、LifeKeeper と DataKeeper が正常に実行されなくなります。

推奨される対応

LifeKeeper および DataKeeper に関し、ウイルス対策ソフトウェアで除外するものは以下の通りです。

- SPS:

  *C:\LK** フォルダ（または LifeKeeper がインストールされているフォルダ）

- DataKeeper:

  C:\Program Files (x86)\SIOS\DataKeeper フォルダ（またはDataKeeperがインストールされているフォルダ）

- ビットマップファイルの場所（デフォルトでは c: ドライブにありますが、再配置される場合があります *C:\Program Files (x86)\SIOS\DataKeeper\Bitmaps* ）

これらの場所にはすべての実行可能ファイルが含まれていますが、ウイルス対策ソフトウェアによってこれらのファイルが隔離され、LifeKeeper または DataKeeper が動作不能になることがあります。

LifeKeeper と DataKeeper が使用するレジストリキーのリストについては、レジストリエントリ を参照してください。

また、

UpperFilters レジストリキーは以下の場所にあります。

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Class\{71A27CDD-812A-11D0-BEC7-08002BE2092F}

8.6.2. アプレットのトラブルシューティング

説明

Web クライアントに ダイアログボックス が表示されない場合は、以下を実行してください。

1. アプレットが起動に失敗したか確認してください。通常は、ブラウザのウィンドウ内にアプレットの状態を示すメッセージが表示されます。Internet Explorer では、状態を表すメッセージのほかに、アプレットの代わりのアイコンが表示されることがあります。このアイコンをクリックすると、失敗に関する説明が表示されます。

2. Java コンソールを開いてください。

   ・FireFox および旧バージョンの Internet Explorer を使用している場合は、**コントロールパネル** を開き、**[Java プラグイン]** アイコンをクリックしてください。コンソール表示を有効にした後、Web ブラウザを再起動してください。

   ・新しいバージョンの Internet Explorer を使用している場合は、**[ツール] メニューの [Sun の Java コンソール]** をオンにしてください。[Sun の Java コンソール] メニューが表示されない場合は、**[ツール] メニューの [アドオンの管理]** をクリックし、コンソール表示を有効にしてから、ブラウザを再起動すると、Java コンソールが表示されます。

   ・Mozilla を使用している場合は、**[ツール] メニューの [Web 開発] をクリックし、[Sun の Java コンソール]** をクリックしてください。

3. Web クライアントが開かない場合は、URL (*http://<server name>:81*) を指定して、ブラウザを再起動してください。

4. コンソールのメッセージを確認してください。エラーメッセージが表示された場合は、それを参考にして問題を解決してください。問題がネットワークに関係している場合は、「ネットワーク関連のトラブルシューティング」を参照してください。

8.6.3. LifeKeeper で OpenJDK をデプロイする

- https://openjdk.java.net/ から、Windows x64 インストーラーの OpenJDK をダウンロードします。
- 最初に、ターゲットノードにソフトウェアをデプロイします。
- LifeKeeper で、スイッチオーバー/サービス開始 を実行します。
- スイッチオーバーが完了した後、他のターゲットで上記の手順を繰り返します。

> **注記:** ソースノード/アクティブノードにソフトウェアをインストールすることはないため、これは可用性の高いデプロイメントです。

コマンドプロンプトで以下を実行します

`javac -version` と入力します。

以下のように出力されます。

"C:\Windows\system32>javac -version javac 14.0.1"

上記のように出力されない場合は、システム変数 PATH/environment に以下を追加する必要がある場合があります。

- コントロールパネル\システムとセキュリティ\システム\システムのプロパティ（システムの詳細設定）\
- **[詳細設定タブ]** を選択します。
- **[起動と回復]** を選択します。
- **[環境変数...]** を選択します。
- **[Path]** を選択し、次に **[編集]** を選択します。

以下の例のように、文字列に *C:\Program Files\Java\jdk-14.0.1\bin* を追加します。

C:\Program Files (x86)\Common Files\Oracle\Java\javapath;SystemRoot%\system32;%SystemRoot;%SystemRoot%\System32\Wbem;%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\;C:\Program Files\Microsoft SQL Server\Client SDK\ODBC\110\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL Server\120\Tools\Binn\;C:\Program Files\Microsoft SQL Server\120\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\120\Tools\Binn\ManagementStudio\;C:\Program Files (x86)\Microsoft SQL Server\120\DTS\Binn\;**C:\Program Files\Java\jdk-14.0.1\bin**

クラスタ内のすべてのノードで上記の手順を実行します。

8.6.4. コマンドプロンプトから SIOS Protection Suite コマンドを実行しようとしたときにエラーが発生する

現象

コマンドプロンプトから SIOS Protection Suite コマンドを実行しようとしたときに、以下のエラーが発生します。

```
[File:lock.CLine:1610] Win32 Error: 2
CRITICAL (No. 472) Can't run this application without LCD Daemon running.
```

解決策

SIOS Protection Suite コマンドを実行するには、「コンソール」権限が必要です。Server 2008 以降で SIOS Protection Suite Core を実行している場合は、「/admin」スイッチを付けてリモートデスクトップ接続を起動してください。

例: %SystemRoot%\system32\mstsc.exe/console

SIOS Protection Suite システム自体のコマンドプロンプトから SIOS Protection Suite コマンドを実行することもできます。

8.6.5. GUI エラーメッセージ

説明

エラー 101: 不正な引数が渡されました。

エラー 102: このプログラムを正しく実行するには、バージョン 1.5 以上の Java 仮想マシンが必要です。LifeKeeper GUI のドキュメントを参照し、ブラウザの設定を確認してください。

エラー 103: LifeKeeper GUI のルックアンドフィールを設定できませんでした。

エラー 104: <filename> イメージをロードできませんでした。

エラー 106: RMI 経由でデータを取得しようとしたときにエラーが発生しました。処理を完了できませんでした。

エラー 107: グローバルリソースインスタンスの作成に失敗しました。

エラー 108: グローバルリソースの作成に失敗しました。

エラー 109: ダイアログでサーバを選択する必要があります。

エラー 112: リソースインスタンスをグローバルイクイバレンシに一致させられませんでした。

エラー 114: <server name> セキュリティ例外が発生したため、このサーバへの接続に失敗しました。そのため、クラスタリソースのレンダリングが縮退することがあります。Java ポリシーファイルが正しくインストールされていることを確認してください。SIOS Protection Suite Web クライアントの実行 を参照してください。

エラー 115: <server name> このサーバの名前を解決できなかったため、このサーバーへの接続に失敗しました。そのため、クラスタリソースのレンダリングが縮退することがあります。LifeKeeper GUI のドキュメントを参照し、ネットワーク命名規則を確認してください。不明なホスト例外 を参照してください。

エラー 116: <server name> このサーバがこのクライアントホストの名前を解決できなかったため、このサーバーへの接続に失敗しました。そのため、クラスタリソースのレンダリングが縮退することがあります。l":#lifekeeper-gui のドキュメントを参照し、ネットワーク命名規則を確認してください。不明なホスト例外 を参照してください。

エラー 117: サーバとの初期接続に失敗しました。LifeKeeper GUI は接続を再試行します。LifeKeeper GUI のドキュメントを参照し、SIOS Protection Suite と LifeKeeper GUI サーバがこのシステムで稼働していることを確認してください。Java RMI のバインドに関する問題 を参照してください。

エラー 118: クライアントパッケージとサーバパッケージに互換性がないため、接続に失敗しました。ターゲットサーバとクライアント起動元サーバのバージョンを調べて、互換性があることを確認してください。

エラー 119: リモートオブジェクトをエクスポートできませんでした。

エラー 120: リモートメソッドの呼び出しで例外が発生しました。

エラー 121: 管理 JavaBean を初期化できませんでした。

エラー 122: 管理 JavaBean にロードできるダイアログクラスがありません。管理 JavaBean を記述したプロパティファイルに「list」プロパティがありません。

エラー 123: 管理 JavaBean を記述したプロパティファイルに次のプロパティがありません。

エラー 124: プロパティバンドルが見つかりませんでした。

エラー 125: URLClassLoader を作成しようとしたときにセキュリティ例外が発生しました。java.policy ファイルで正しいパーミッションが付与されていることを確認してください。通常は .java.policy ファイルをホームディレクトリに作成します。java.policy ファイルの内容には大文字と小文字の区別があります。そのため、LifeKeeper GUI パッケージ付属のサンプルファイルをコピーするのが最善の方法です。

Java のブラウザプラグインを使用している場合は、Java コンソールを有効にして表示される最初の数行を調べれば、Java 環境用に使用されているユーザホームディレクトリをチェックできます。GUI クライアントの設定の詳細については、LifeKeeper GUI の設定 を参照してください。

エラー 126: サーバにリソースが見つかりませんでした。

エラー 127: このキットの拡張プロパティファイルが見つかりませんでした。

エラー 128: 内部プロパティファイルエラーです。

エラー 129: サーバへの RMI 接続を確立できません。サーバ上で LifeKeeper GUI サーバが稼働していることを確認してください。

エラー 130: 入力したタグは別のリソースで使用されています。別のタグを入力してください。

エラー 131: ユーザインターフェースの更新のために invokeAndWait メソッドを呼び出しているときに例外が発生しました。

エラー 132: 管理 JavaBean の呼び出し中に例外が発生しました。

エラー 133: イクイバレンシの優先順位として入力した値が無効です。優先順位の値は 1 から 999 の範囲になければなりません。

エラー 134: イクイバレンシの優先順位の値がテーブル内の別の優先順位と競合しています。イクイバレンシの優先順位の値はそれぞれテーブル内で一意でなければなりません。

8.6.6. GUI ネットワーク関連 – サーバへの初期接続の失敗 (エラー 117)

現象

サーバとの初期接続に失敗しました (エラー 117)。

複数のネットワークインターフェースカード (NIC) を持つサーバに接続する場合、最初の NIC の IP アドレスが到達不能な場合、Java RMI のバインドに関する問題が発生します。最初の NIC とは、ipconfig ユーティリティが出力する最初の IP アドレスを指します。

解決策

SIOS Protection Suite サーバのネットワークサービスが使用するプロトコルバインディングの順序を変更してください。SIOS Protection Suite サーバ上で [ネットワークとダイヤルアップ接続] を開き、**[詳細設定]** メニューの **[詳細設定]** をクリックしてください。ダイアログボックス上部の **リストボックス** に NIC が表示されます。これが現在の順番です。**矢印ボタン** を使用して、到達可能な NIC をリストの最上位に移動してください。このように NIC の順番を変更すると、Java RMI は、クライアントによるサーバへの接続を許可します。サーバをリブートして設定を反映してください。

8.6.7. GUI ネットワーク関連 – Windows プラットフォーム上の長期接続遅延

この問題への対処方法は2つあります。1つは「解決策 1 – IPV4 インターフェースメトリック」、もう1つは「解決策 2 – ローカルホストファイル」です。

現象

Windows プラットフォーム上で、接続が長時間遅延します。

解決策 1 – IPV4 インターフェースメトリック

これは、異なるサブネットに複数の NIC が接続されている LifeKeeper システムに適用されます。Java RMI ホストルックアップは、各インターフェースの IPV4 インターフェースメトリックを使用してホストの IPアドレスを決定します。RMI が両方向の接続で同じネットワーク上で通信するようにするには、ホストのパブリック NIC が最小のインターフェースメトリックを持つように IPV4 インターフェースメトリックを指定する必要があります。これにより、ホストのパブリック IPアドレスが確実に報告されます。

デフォルトでは、Windows ネットワークインターフェースは「自動」インターフェースメトリックで構成されています。これにより、LK GUI クライアントと LK ホスト間の RMI 通信に誤ったネットワークが使用される場合もあります。よって自動メトリックを無効にし、適切なメトリックを指定する必要があります。パブリック NIC の場合は、メトリック「1」を指定し、追加の NIC ごとに、増加するメトリック値（2、3、4…）を指定します。

解決策 2 – ローカルホストファイル

サンマイクロシステムズ社の FAQ より

「通常の場合、ホストのネットワーク設定が不適切なことが原因です。RMI は JavaAPI のネットワークのクラス (java.net.InetAddress) を使用して、両方のホストの TCP/IP ホスト名を参照し、IP アドレスとホスト名をマッピングします。Windows プラットフォームでは、この参照はネイティブの Windows ソケットライブラリが実行するため、遅延は RMI ではなく、Windows ライブラリで発生します。ホストで DNS を使用する場合、DNS サーバは通信に参加するホストを認識しないため、DNS 参照がタイムアウトになることが問題となります。その場合は、ホスト名/アドレスをローカルの *local file\winnt\system32\drivers\etc\hosts* ファイルまたは *\windows\hosts* ファイルに記述します。ホストファイルは次の書式で記述します。

```
IPAddress Server Name

e.g.: 208.2.84.61 homer.somecompany.com
```

以上のように記述すると、最初の参照時間を短縮できます。」

また、サブネットマスクとゲートウェイアドレスの設定を間違うと、接続遅延や障害の原因となります。DNS の設定が正しいことをネットワーク管理者に確認してください。

8.6.8. GUI ネットワーク関連 – 接続試行時に生成される NoRouteToHostException メッセージ

現象

接続試行時に NoRouteToHostException というメッセージが生成されます。

ホストとの接続を確立できないため、ソケットをリモートホストに接続できません。

解決策

ローカルサーバとリモートサーバを結ぶネットワークの一部のリンクが停止しているか、リモートサーバがファイアウォールで保護されています。

8.6.9. GUI ネットワーク関連 – 接続試行時に生成される不明なホスト例外メッセージ

現象

接続試行時に不明なホスト例外メッセージが生成されます。

LifeKeeper GUI のクライアントとサーバは、Java RMI (Remote Method Invocation) 技術を使用して通信します。RMI が適切に動作するには、クライアントとサーバは、解決可能なホスト名または IP アドレスを使用する必要があります。解決不能な名前 (WINS 名) または不適切な DHCP 名を使用すると、Java は UnknownHostException をスローします。

このエラーメッセージは、次の場合にも表示されます。

- サーバ名が見つからない。サーバ名のスペルを確認してください。
- DHCP サーバの設定が不適切な場合、RMI サーバの完全修飾ドメイン名が、RMI サーバの実際に存在するドメインではなく、リゾルバドメインのドメイン名に設定されることがあります。その場合、ドメイン名が不正なため、サーバの DHCP ドメインの外側にある RMI クライアントはサーバに接続できません。
- サーバが Windows Internet Naming Service (WINS) を使用するネットワーク上にある。WINS に登録されたホストは、DNS だけを使用するホストから接続できないことがあります。
- RMI クライアントとサーバがファイアウォールを挟んだ両側にある。RMI クライアントがファイアウォールの外側にあり、サーバがその内側にある場合、クライアントはリモートコールをサーバに送信できません。

解決策

LifeKeeper GUI を使用するときは、クライアントが使用するホスト名は、サーバが解決できなければなりません。また、クライアントはサーバのホスト名を解決できなければなりません。LifeKeeper GUI はこの例外を捕捉してユーザに警告します。クライアントがサーバのホスト名を解決できない場合は、この例外がスローされて、エラーメッセージ 115 が表示されます。サーバがクライアントのホスト名を解決できない場合は、この例外がスローされて、エラーメッセージ 116 が表示されます。2 つのメッセージは、ホストが見つからないことを通知する Java の例外です。

ホスト名が適切に解決されていることをテストして確認するには、以降に示す手順に従ってください。

Windows の場合

1. SIOS Protection Suite サーバとの通信が確立していることを確認します。プロンプトから、ホスト名を指定して ping を打ってください。

   ```
   ping<TARGET_NAME>
   ```

   以下に例を示します。

```
ping homer
```

ターゲットのホスト名と IP アドレスが返ります。

2. 設定が適切なことを確認します。

   a.DNS の設定を確認するか、DNS サーバをネットワークにインストールしてください。

   b.DNS の設定を確認するには、**[コントロール パネル] -> [ネットワーク] -> [プロトコル] -> [TCP/IP]** の順に選択してください。DNS の設定が正しいことをネットワーク管理者に確認してください。[DNS] タブのホスト名がローカルのネームサーバと同じであることを確認してください。また、この名前が GUI エラーメッセージに表示されたホスト名であることを確認してください。

   c.ローカルホストと接続先の SIOS Protection Suite サーバを hosts ファイルに記述してください。

Windows 2008 R2 および 2012　の hosts ファイルは、次の場所にあります。

```
%SystemRoot%\system32\drivers\etc\HOSTS (例: C:\windows\system32\
drivers\etc\HOSTS)
```

注記: Windows 2008 R2　および　2012　では、hosts ファイルの最終エントリの後に改行記号 (CR/LF) がないと、hosts ファイルは参照されません。

例えば、ユーザのシステムが HOSTCLIENT.MYDOMAIN.COM であり、IP アドレスが 153.66.140.1 である場合、hosts ファイルに次のエントリを追加します。

```
153.66.140.1 HOSTCLIENT.MYDOMAIN.COM
```

3. GUI クライアントが使用するホスト名のプロパティを設定します。ホスト名のプロパティを設定するには、Java Plug-in をインストールした Web ブラウザを開き、**Java プラグインコントロールパネル** を表示して、次の 1 行を [Java Run Time Parameters] に追加してください。

```
-Djava.rmi.server.hostname=<MY_HOST>
```

4. www.microsoft.com にアクセスして、Microsoft が提供するネットワーク関連のパッチを確認します。

Linux の場合

1. ホスト名または IP アドレスを指定して ping を打ち、ターゲットサーバとの接続が確立していることを確認します。

```
ping -s<TARGET_NAME>
```

以下に例を示します。

```
ping -s homer
```

ターゲットのホスト名が返ります。

2. ホスト名または IP アドレスを指定して ping を打ち、クラスタサーバが *localhost* 名を解決していることを確認します。DNS が実装されていなければ、*/etc/hosts* ファイルを編集し、*localhost* 名を追加してください。ローカルサーバの IP アドレス、またはデフォルトエントリ (127.0.0.1) を指定できます。

3. DNS が NIS の前に記述されていることを確認します。DNS は、*/etc/nsswitch.conf* のホスト行で NIS の前に記述します。また、*/etc/resolv.conf* には適切に設定された DNS サーバを指定します。

4. DNS が実装されていないか、他の名前解決プロトコルが機能していない場合は、ホスト名を */etc/hosts* ファイルに記述します。

5. GUI クライアントが使用するホスト名のプロパティを設定します。これは、管理者ごとに変更する必要があります。

   ホスト名のプロパティを設定するには、Java Plug-in をインストールした Web ブラウザを開き、**Java プラグインコントロールパネル** を表示して、次の 1 行を **[Java RunTime Parameters]** に追加してください。

   ```
   -Djava.rmi.server.hostname=<MY_HOST>
   ```

   この作業を HotJava ブラウザから実行するには、次の 1 行を hotjava コマンドラインに追加してください。

   ```
   -Djava.rmi.server.hostname=<MY_HOST>
   ```

   例

   ```
   -Djava.rmi.server.hostname=153.66.140.1

   -Djava.rmi.server.hostname= homer.somecompany.com
   ```

8.6.10. GUI サーバのトラブルシューティング

現象

LifeKeeper GUI は、管理 Web サーバと Java リモートオブジェクトレジストリに、各サーバのポート 81 および 82 を使用します。別のアプリケーションが同じポートを使用している場合、LifeKeeper GUI は正常に機能しません。

解決策

値を変更するには、以下のレジストリエントリを編集してください。

```
GUI_WEB_PORT=81

GUI_RMI_PORT=82
```

これらのエントリは、以下のレジストリキーにあります。

```
HKEY_LOCAL_MACHINE\SOFTWARE\SIOS\LifeKeeper\JavaGUI\Server
```

注記: ポートの値は GUI サーバの起動時に初期化されます。変更した場合は、GUI サーバを停止して再起動する必要があります。これらの値は、接続するクラスタすべてで同じでなければなりません。

8.6.11. エラーが出力されずに LifeKeeper GUI アプリケーションの起動に失敗する

現象

LifeKeeper（管理者専用）アプリケーションを使用して管理者として実行すると、LifeKeeper GUI が起動しない。

LK GUI アプリケーションを起動するウィンドウはまったく表示されない。

ログにはエラーメッセージは何も出力されていない。

IP メトリック設定（各システムの各イーサネットカードの下）を見ると、プライマリイーサネットカードで IP メトリックが 1（バインド順序で 1番目のものは LifeKeeper GUI が使用するイーサネットカード）に設定されなくなり、自動（Automatic）に戻る。また、ネットワークカードで IPv6 が再有効化されている。

解決策

クラスター内の各システムのネットワークカードで IPv6 を無効にします。

クラスター内の各システムで、プライマリカードの IP メトリック設定（バインド順序で1番目、`ipconfig/all` リストで 1番目）を Automatic から 1 に変更します。詳細については、以下の「 **特定の NIC に対してインターフェイスメトリックを使用する必要がある場合** 」を参照してください。

問題：

特定の NIC に対してインターフェイスメトリックを使用する必要がある場合

対応方法：

LifeKeeper GUI の動作が遅くなっている（またはリソースの状態に「?」マークが表示されている）場合、次を実行します。

- クラスター内のすべてのノードで LifeKeeper を閉じます。
- 両方のサーバーで、ネットワークインターフェイスのバインド順序をパブリックが 1番目、プライベートが 2番目になるようにします。
  - これは、**[コントロールパネル]** ＞ **[ネットワークとインターネット]** ＞ **[ネットワークと共有センター]** ＞ **[アダプターの設定の変更]** ＞ **[詳細]** ＞ **[詳細設定]** で設定できます。
- TCP/IP の詳細設定で、インターネットプロトコルバージョン4（TCP/IPv4）を使用しているすべてのネットワークインターフェイスについて、**[自動メトリック]** チェック ボックスをオフにしてから、インターフェイスメトリックを選択します。

  例：

`Public = 10`

`Private = 20`

`NIC 3 = 30` など

クラスター内の他のノードにも同じ値を適用します。

注記:これは、無効になっていてもまだ TCP/IP が NIC にバインドされている NIC にも適用されます。

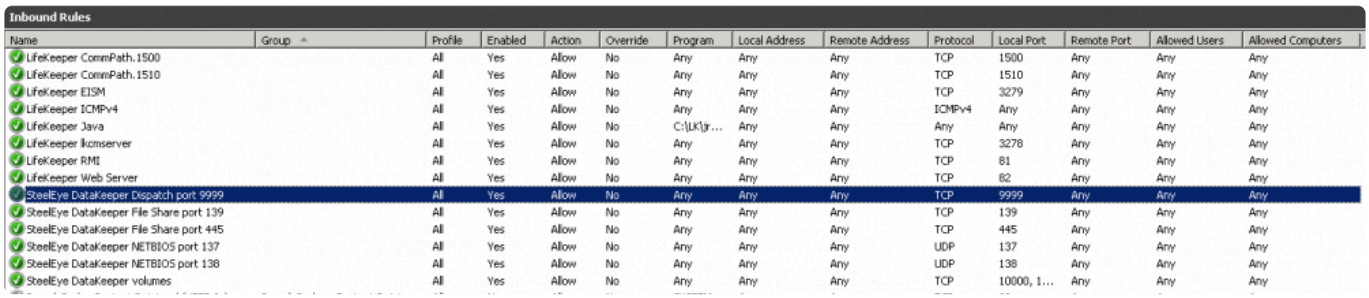
インターフェイスメトリックを変更した後、lkGUIserver.exe プロセスを強制終了してください。その後、これは新しいメトリック設定を使用して再起動します。このタスクを行うには、次のコマンドを実行してください。

- 管理者特権のコマンドプロンプトから
- `cd c:\lk\bin`
- `tasklist |findstr lkGUIs` と入力して lkGUIserver.exe を見つけます
  - 見つかったら、プロセス ID が表示されるので、これを終了する必要があります
- `kill {process ID}` と入力します
- `tasklist | findstr lkGUIs` を再実行して新しいプロセスIDを反映させ、新しいプロセスが起動されたことを確認します

その後、LifeKeeper GUI アプリを再起動すると、パフォーマンスが向上しています。

インバウンドルールに、LifeKeeper GUI が適切に機能するために必要なポートの開放が含まれていることを確認します。インバウンドルールには、LifeKeeper RMI エントリと以下にリストされている他の LifeKeeper エントリが含まれている必要があります。

Windows ファイアウォールがオンになっている場合、DataKeeper のデフォルトを受け入れると、インバウンドルールはどうなりますか？



LK GUIアプリケーションは、各システムで正常に起動します。

8.6.12. Java 1.8.xのLifeKeeper GUI問題

現象

JRE v7 と JRE v8を使用するクライアントシステム上で、ウェブブラウザを介してLifeKeeper GUIをロードすることができない

解決策

クライアントシステム上のJavaコントロールパネルで、セキュリティ設定を編集し、例外サイト・リストの定義にクラスタノードを入力してください。

8.6.13. ヘルスチェックタイムアウト

現象: 時として SIOS Protection Suite は正常に動作しないシステムにインストールされることがあります。そこには SIOS Protection Suite が検知することが可能な、ヘルスチェックが正常に起動または終了しないといったような前兆現象があります。チェック処理のタイムアウトを引き起こすもっとも一般的な問題は、データベースまたはメールサーバに対するシステムメモリの最適化が適切でない場合です。常時ヘルスチェックプロセスを起動し、フェールオーバを実施するためには十分なメモリが必要です。

解決策: SIOS Protection Suite リリースノートは、SIOS Protection Suite のシステムメモリ要件を定義するためのガイドラインを記載しています。また、使用するシステムにおいて、SIOS Protection Suite のようなアプリケーションが動作するのに十分なメモリがあるかを確認するための Windows Performance Monitors の使用方法についても説明しています。この状態を確認する手助けとして、チェック処理のタイムアウトが発生した際に、異常なふるまいを記録する 2 つのリソース監視オプションと、是正操作を行う 3 つのオプションがあります。5 つのオプションはすべて SIOS Protection Suite のレジストリ設定で有効または無効にし、ユーザにあった要件やパフォーマンスを満たすことができます。

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\STEELEYE\LifeKeeper\General\
ResMon_RecordTimeout

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\STEELEYE\LifeKeeper\General\
ResMon_RecordMemory

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\STEELEYE\LifeKeeper\General\
ResMon_ResFail

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\STEELEYE\LifeKeeper\General\
ResMon_RebootWaitInSec

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\STEELEYE\LifeKeeper\General\
ResMon_ResFailMaxWaitInMin
```

最初の 4　つのオプション (RecordTimeout, RecordMemory, ResFail, RebootWaitInSec) は、期待される時間内に完了しない保護対象のリソースを監視している SIOS Protection Suite のクイックチェックもしくはディープチェックプロセスによって引き起こされます。

ResMon_RecordTimeout - このオプションはタイムアウトするクイックチェックもしくはディープチェック処理を記録します。この情報は *<LifeKeeper Root Folder>\Out\ResMonTimeout.log file* ファイルに記録されます。このオプションはデフォルトで有効 (=1) になっています。無効にする場合は値を 0 に設定してください。

ResMon_RecordMemory - このオプションは、クイックチェックもしくはディープチェックがタイムアウトするとアクティブなプロセスに対するシステムメモリの使用量とプロセスメモリの使用量を記録します。メモリの使用率は *<LifeKeeper Root Folder>\Out\ResMonTimeout.log file* に記録されます。このオプションはデフォルトで有効 (=1) になっています。無効にする場合は値を 0 に設定してください。

ResMon_ResFail - このオプションはクイックチェックもしくはディープチェックがタイムアウトしたときリソース階層

のフェールオーバを発生させます。影響を受ける階層の従属リソースがフェールオーバします。このオプションはデフォルトで無効 (=0) になっています。有効にする場合は値を 1 にしてください。

ResMon_RebootWaitInSec - このオプションはクイックチェックもしくはディープチェックがタイムアウトしたときシステムの再起動を発生させます。このオプションはデフォルトで無効 (=0) になっています。有効にする場合はレジストリ設定で 0 以外を入力してください。この数は、システムがこの機能により再起動されるときにシステムコンソール上に表示されるカウントダウンになります。再起動のシーケンスは自動およびシステム操作を必要としないデザインになっています。一旦カウントダウンが開始されると、再起動は停止することができません。

ResMon_ResFailMaxWaitInMin - このオプションは、フェールオーバ発生時に SIOS Protection Suite のフェールオーバ処理を監視します。レジストリ設定の値は、SIOS Protection Suite がリソースのフェールオーバ完了までに待つ時間 (分) になります。フェールオーバ処理が開始されない場合、もしくはフェールオーバ処理が指定された時間内に完了しない場合は、SIOS Protection Suite はシステムの再起動を試みます。リソースがフェールオーバされなかった場合は、再起動されたサーバと同じ場所で in service されます。このオプションはデフォルトで無効 (=0) になっています。

リソース監視オプション はすべての保護対象のリソースに対して適用され、いつでもそれらを変更することが可能です。変更された設定は、次回クイックチェックもしくはディープチェックプロセスが開始されたときに反映されます。

8.6.14. 不完全なリソースの作成

説明

リソースの設定プロセスが途中で中断し、インスタンスが不完全な状態で作成された場合は、リソースを再作成する前にクリーンアップを手動で実行してください。部分的に作成されたリソースは、LifeKeeper の GUI を使用して削除します。詳細については、全サーバのリソース階層の削除 を参照してください。不完全なリソースが階層の一覧に表示されない場合は、`ins_remove` と `dep_remove` コマンドでクリーンアップしてください。

8.6.15. インストール – アクセス拒否

現象

SIOS Protection Suite のアップグレード時または再インストール時に、「Access is denied」というエラーメッセージが表示されます。

解決策

SIOS Protection Suite サービスが完全に停止していません。これは、セットアッププログラムが SIOS Protection Suite サービスを停止することができなかった場合に発生する可能性があります。コマンドウィンドウを開いて `$LKROOT\bin\lkstop` と入力して、すべての SIOS Protection Suite サービスを停止してください。その後、「LIFEKEEPER NOW STOPPED 」と表示されるまで待機してからセットアップを実行してください。

8.6.16. IP リソース作成問題

現象

新しい IP アドレスが既存の IP　アドレスと部分的に一致した場合IP リソースの ***Pre-Extend Wizard*** に失敗します。

ワークアラウンド

現在有効なワークアラウンドはありません。この問題については将来のリリースにおいて対応されます。

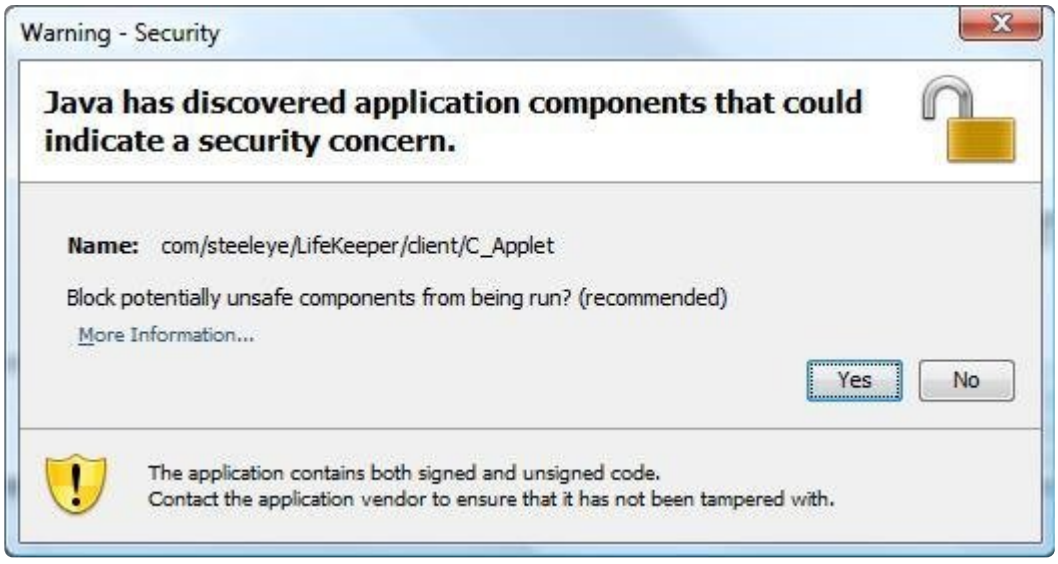
8.6.17. Java の署名があるコードとないコードの混在の警告

現象

リモートシステムから LifeKeeper Java GUI クライアントアプレットを読み込むとき、以下のセキュリティ警告が表示される場合があります。



[実行] を選択すると、以下のダイアログが表示されます。



ブロックについては **[いいえ]** を選択すると、LifeKeeper GUI の実行が許可されます。

解決策

以下の 2 つの方法でセキュリティ警告の数を減らすことができます。

1. **この発行者からのコンテンツを常に信頼します** チェックボックスをオンにして、**実行** を選択してください。次に LifeKeeper GUI Java クライアントを読み込むときは警告メッセージが表示されません。

   または

2. ブロックに関する 2 つ目のダイアログが表示されないようにするには、Java の「 **deployment.properties** 」ファイルに以下のエントリを追加してください。Java クライアントを読み込むときにセキュリティ警告は表示されますが、アプレットはブロックされず、ブロックの確認ダイアログは表示されません。この設定はすべての Java アプレットに適用されることに注意してください。

   deployment.security.mixcode=HIDE_RUN

両方のメッセージを回避するには、1 および 2 を実行してください。

8.6.18. 参照リストに LANMAN 名が 2 回表示される場合がある

現象

LANMAN リソースを作成した後、参照リストに LANMAN 名が 2 回表示される場合があります。

解決策

エントリの 1 つは使用できないワークステーションレコードです。このエントリを無視し、もう 1 つの LANMAN サーバ名を使用してください。

8.6.19. ライセンス – ライセンスされたリカバリキットリソースが起動しない

現象

ライセンスされたリカバリキットをアップグレードした後、リソースが起動せず、SIOS Protection Suite によって以下のエラーが **アプリケーションイベントログ** に記録されます。

```
“Process: lcdmachfail(3176) *ERROR* (No. 1001) resource <tag name>
requires a license (for Kit <recovery kit type>) but none is installed.”
```

解決策

SIOS Protection Suite ライセンスユーティリティを使用して、リカバリキットのライセンスキーをインストールしてください。ライセンスのインストールについては ライセンスの取得とインストール を参照してください。

8.6.20. ライセンス – ライセンスキーが見つからない

現象

ライセンスされたリカバリキットをインストールした後、SIOS Protection Suite によって以下のエラーが **アプリケーションイベントログ** に記録されます。

```
“Process: Lkinit:(1832) *ERROR* (No. 20042) SPS Recovery Kit <licensed recovery kit> license key NOT FOUND”.
```

解決策

SIOS Protection Suite ライセンスユーティリティを使用して、リカバリキットのライセンスをインストールしてください。ライセンスのインストールについては ライセンスの取得とインストール を参照してください。

8.6.21. SIOS Protection Suite Web クライアントがロックされる場合がある

現象

サーバマシンから使用しているとき、そのサーバについての SIOS Protection Suite リソースの初期描画時に「-」(リソースの高さを減らす) または「+」(リソースの高さを増やす) アクセラレータキーを押した場合、SIOS Protection Suite Web クライアントがロックされることがあります。

解決策

復旧するには、Windows タスクマネージャを開き、**LifeKeeper - <web browser (例: Microsoft Internet Explorer)>** アプリケーションに対して **[タスクの終了]** を選択してください。プロセスを終了するのに最大で 1 分かかる場合があります。**[スタート]** -> **[プログラム]** -> **SIOS** ショートカットから SIOS Protection Suite Web クライアントを再起動し、初期画面の描画が完了するまで待機してからアクセラレータキーを使用してください。

8.6.22. SIOS Protection Suite Web クライアントがロックされる場合がある – 既存の階層が複数変更された

現象

サーバマシンから使用しているとき、既存の階層に対して複数の変更 (つまり、依存関係の作成/削除) が行われ、その変更の間に SIOS Protection Suite クライアントを閉じてから開き直した場合、SIOS Protection Suite Web クライアントがロックされることがあります。

解決策

復旧するには、**Windows タスクマネージャ** を開き、**LifeKeeper - <web browser (例: Microsoft Internet Explorer)>** アプリケーションに対して **[タスクの終了]** を選択してください。プロセスを終了するのに最大で 1 分かかる場合があります。サーバの階層管理には LifeKeeper GUI を使用してください。ショートカットは、**スタート** -> **プログラム** -> **SIOS** -> **LifeKeeper** -> **LifeKeeper GUI** です。(管理者のみ)

8.6.23. 新しい評価ライセンスキーのエラー

現象

SIOS Protection Suite for Windows の評価時、新しい評価ライセンスキーを使用していないとエラーが発生する場合があります。古い評価用ライセンスはこのリリースでは機能しません。

解決策

新しい評価ライセンスキーを取得する必要があります。**ライセンスキーマネージャ** を再起動して、新しいライセンスキーを適切な形式で入力してください。

8.6.24. 1 × 1 構成における SIOS Protection Suite のサーバ障害からの復旧

SIOS Protection Suite クラスタにおいてサーバにオペレーティングシステムの再インストール (SIOS Protection Suite も同じく) が必要となるような障害が発生した場合、クラスタの各サーバからリソース階層を再拡張することが必要となります。クラスタのサーバが再インストールされるサーバとイクイバレンシ関係を共有している場合でも SIOS Protection Suite では、再インストールされるサーバへ既存のリソース階層を拡張することができません。実際には階層が再インストールされたサーバ上に存在しないため再インストールされるサーバから階層を拡張解除することもできません。

推奨される処置

オペレーティングシステムおよび SIOS Protection Suite と同様にすべての関連するパッチを再インストールした後、以下の手順に従って復旧を行ってください。(**注意**: 下記で説明する推奨されるアクションの例において "BENHOGAN" および "GPLAYER" というテストシステム名を使用します。)

1. リソース階層が構成されている各サーバで、eqv_list コマンドを使用して、すべての共有イクイバレンシの一覧を取得してください。

   ```
   eqv_list [-d destsys] [-s sys] [-t tag] [-e SHARED] [-fC]
   ```

   この機能は、リソースインスタンス間のイクイバレンシ関係を記述している一般的なアウトプットを表示します。

   例:

   ```
   c:\LK\Bin>eqv_list

   BENHOGAN2008 LK1-BENHOGAN2K8 GPLAYER2008 LK1-BENHOGAN2K8 SHARED 1 10

   BENHOGAN2008 Vol.E GPLAYER2008 Vol.E SHARED 1 10
   ```

   See LifeKeeper GUI below of hierarchies, resources, etc.

   下記の LifeKeeper GUI の階層やリソースなどを参照してください。



2. リソース階層が構成されているサーバで eqv_remove を使用して手動で階層の各リソースのイクイバレンシ関係を削除してください。

   システム sys と othersys それぞれに存在するリソースタグ名とその他タグ間で、 -e オプションを指定し、イクイバレンシタイプのシステム destsys (指定されない場合はローカル) 上のコンフィギュレーションデータベースからイクイバレンシを削除します。

   ```
   eqv_remove [-d destsys] [-s sys] -t tag [-S othersys]-o othertag [-e SHARED]

   eqv_remove -s {this system} -t {TAGNAME} -S {othersys that has gone away} [-e SHARED]
   ```

   例:

   ```
   c:\LK\Bin>eqv_remove -s BENHOGAN2008 -t LK1-BENHOGAN2K8 -S GPLAYER2008 -e SHARED

   c:\LK\Bin>
   ```

3. eqv_list コマンドを再度実行してください。共有イクイバレンシの一覧は表示されません。

   ターゲットリソースがどのように削除されているかを下記の LifeKeeper GUI で確認してください。



4. クラスタにおいて Datakeeper でミラーされているボリュームが構成されている場合は、そのボリュームに対する LKDRInfo ファイルをクリーンアップしてください。

   SIOS Protection Suite は、各ミラー対象のボリュームリソースに対して %LKROOT%\subsys\filesys\resources\volume フォルダに LKDRInfo. を作成します。このファイルは削除されます。

   ```
   C:\LK\BIN> cd %LKROOT%\subsys\filesys\resources\volume

   C:\LK\subsys\filesys\resources\volume> dir LKDRInfo.E

   05/23/2012 01:02 PM 39 LKDRInfo.E

   C:\LK\subsys\filesys\resources\volume> del LKDRInfo.E
   ```

5. クラスタにおいて Datakeeper でミラーされているボリュームが構成されている場合は、ミラーをクリーンアップし、ミラーを含む DataKeeper ジョブを削除してください。

   クラスタが再インストールされるサーバに再拡張する際に DataKeeper のミラーとジョブを再作成する必要があります。そのため、構成されるミラーのローカルエンドを削除し、それらのミラーとともに構成されるジョブを削除する必要があります。

   ```
   C:\LK\subsys\filesys\resources\volume> cd %ExtMirrBase%

   C:\Program Files\SIOS\DataKeeper> emcmd . getjobinfoforvol E

   ID = e829700c-27b0-447f-b852-1a3135da31a7

   Name = E Vol

   Description =

   MirrorEndPoints = BENHOGAN2008;E;10.200.8.25;GPLAYER2008;E

   ;10.200.8.26;A

   C:\Program Files\SIOS\DataKeeper> reg /delete HKLM\System\
   CurrentControlSet\Services\ExtMirr\Parameters\Jobs\
   e829700c-27b0-447f-b852-1a3135da31a7

   Permanently delete the registry key HKEY_LOCAL_MACHINE\System\
   CurrentControlSet\Services\ExtMirr\Parameters\Jobs\
   1b5e8715-a488-4030-8166-45c9232bc04e (Yes/No)? y

   The operation completed successfully.

   C:\Program Files\SIOS\DataKeeper> emcmd . getjobinfoforvol E
   ```

```
C:\Program Files\ SIOS\DataKeeper> emcmd . deletelocalmirroronly E

Status = 0

C:\Program Files\ SIOS\DataKeeper> emcmd . clearswitchover E

Status = 0
```

これらの手順をすべてのミラー対象のボリュームに対して繰り返してください。**このジョブはレジストリディレクトリからの削除が必要です。emcmd . deletejob を使用して削除しようとすると DataKeeper が全ノードでのジョブの削除を試みるので操作に失敗します。これらのノードのひとつがもう存在しておらず、ジョブがそのまま残るからです。**

6. 古いシステムを削除する準備が整いました。

   a. .SIOS Protection Suite クラスタのすべてのシステムを表示させます。

   ```
   sys_list [-d destsys]
   ```

   例:

   ```
   c:\LK\Bin>sys_list

   BENHOGAN2008

   GPLAYER2008
   ```

   b. すべての古いターゲット/システムを削除します。

   ```
   sys_remove [-d destsys] -s sys
   ```

   例:

   ```
   c:\LK\Bin>sys_remove -s GPLAYER2008
   ```

   Do this for all systems participating in the SIOS Protection Suite cluster

   Note: If attempting to execute this command for the local/source system, the following error will be received:

   ```
   c:\LK\Bin>sys_remove -s BENHOGAN2008

   (null)Process: sys_remove(2728)

   [File:sys.C Line:81]
   ```

```
*ERROR* (No. 424) can't remove entry for local system
"BENHOGAN2008"
```

7. コミュニケーションパスを削除してください。

   a. コミュニケーションパスが存在することを確認してください。

   ```
   net_list
   ```

   b. これらのコミュニケーションパスを削除してください。

   ```
   net_remove
   ```

8. 変更を加えてください。

   lcdsync [-d destname]

   例:

   ```
   c:\LK\Bin>lcdsync
   ```

   この機能は共有メモリに保存されている SIOS Protection Suite リソース階層の構成とコミュニケーションパスの状態が修正されているかどうかをチェックします。もし相違があったら、データはディスクに対して "同期" 書き込みを行います。これによって、このプログラムが終了すると、正しいデータがディスク上で保障されます。

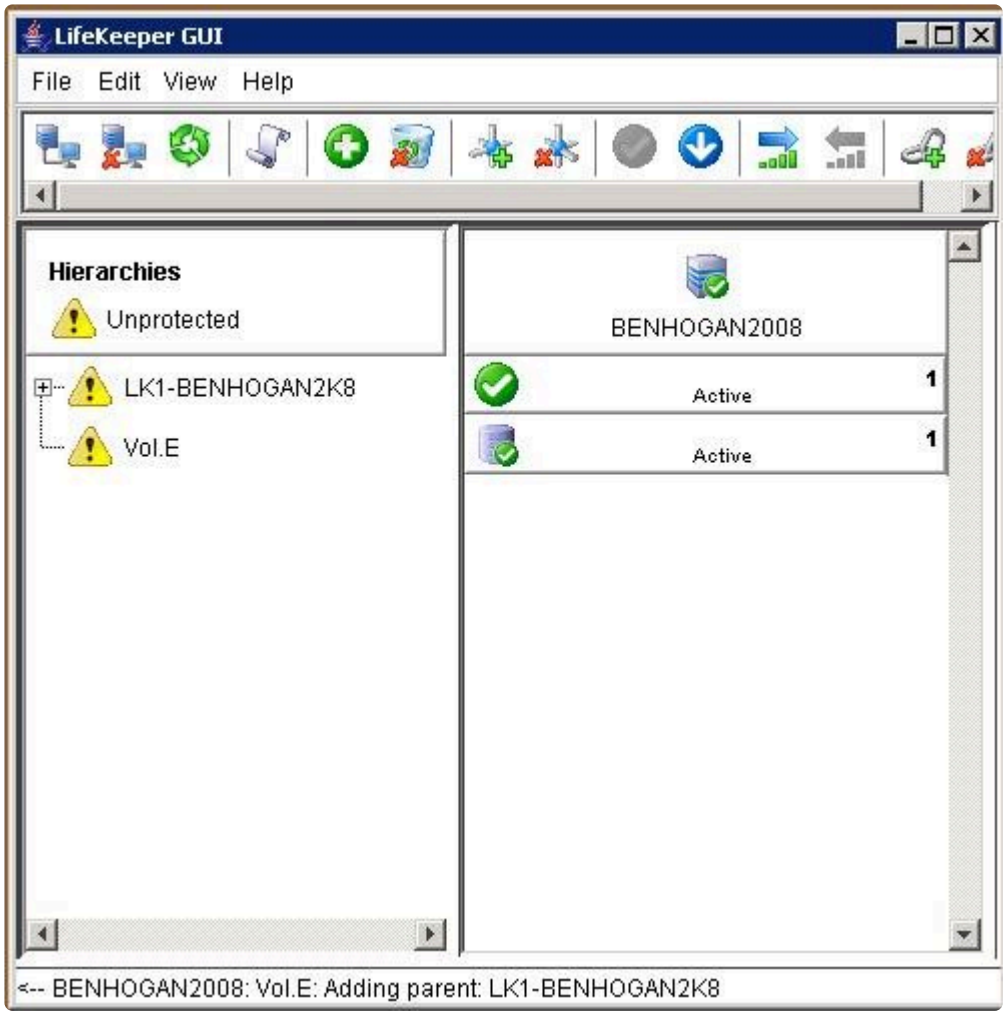
   追加情報: すべてのリソースを完全に削除する場合は、まずはじめにすべてのリソースインスタンスの一覧を生成してください。

   ins_list [-d destsys] [-fC] [-R top] [-a appname] [-r typ][-t tag] [-i id]

   その後すべてのインスタンスを削除してください。

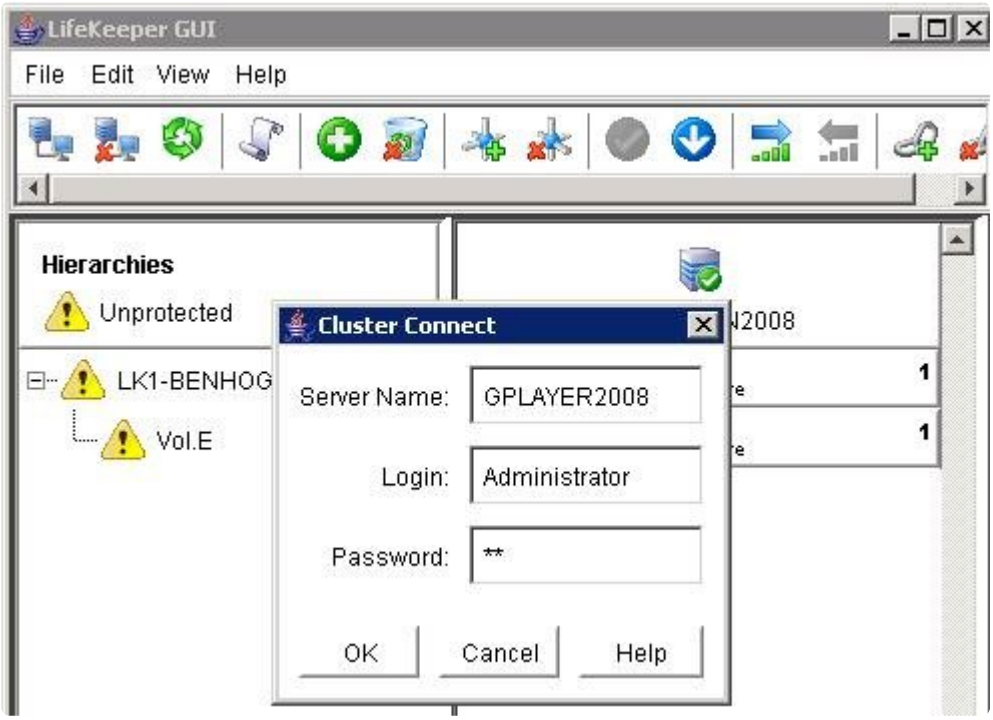
   ins_remove [-d destsys] [-R roottag] [-a appname] [-r restyp][-t tag] [-i id] [-v] [-I] [-N] [-G]

9. LifeKeeper GUI を閉じて、再度起動してください。

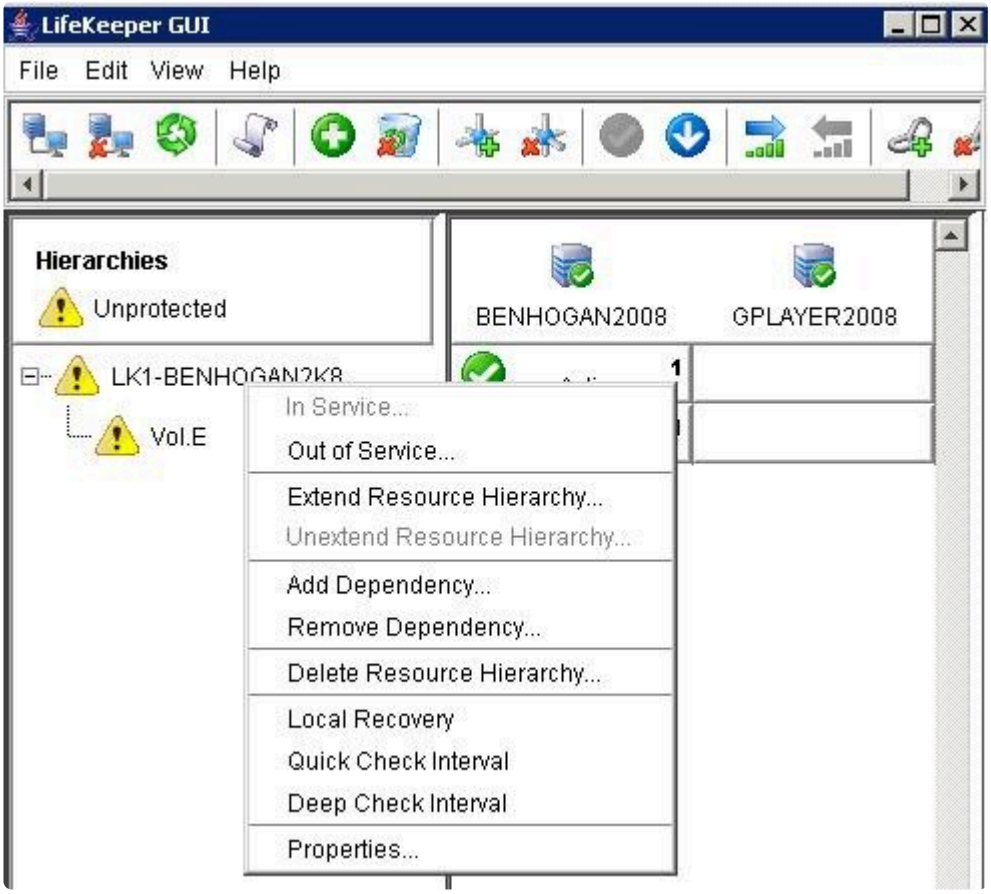


10. GUI を使用して、各リソース階層をリソース階層が　in service になっているサーバから再インストールされたサーバへ拡張してください。

    a. 再インストールされたサーバ/ターゲットに接続してください。**注記:** コミュニケーションパスの再作成もまた必要になります。



b. リソース階層を拡張してください。



c. ミラーリソースを追加/拡張してください。



完了 -- すべての保護対象のリソースが復旧し、再度保護対象となります。

8.6.25. サービス休止中の階層のリカバリ

説明

障害が発生した SIOS Protection Suite サーバ上のリソース階層は、障害発生時に他のサーバ上で起動されていなくても、リカバリ処理の一環として、障害発生時に優先度が最高のサーバにリカバリされます。このリカバリ操作は、サービスを休止しているサーバが最後にサービスを稼働していたサーバ (障害が発生したサーバ)、バックアップサーバ、他のクラスタサーバでも、同様に処理されます。

8.6.26. LifeKeeper から DataKeeper ストレージを削除する

LifeKeeper/SPS から既存の DataKeeper リソース/ミラーを削除します。この手順は、

- LifeKeeper/SPS の既存の役割（ファイル共有、SAP、Oracle、SQL、DNS など）に影響を与えません。
- deletelocalmirroronly、cleanupmirror などの様々な emcmd コマンドを実行する必要がありません。

注記: DataKeeper UI では、「スイッチオーバー」、「ジョブを削除」、「ミラー削除」は、アクションパネルでグレーアウトされています。

理由: DataKeeper ミラーが LifeKeeper/SPS の一部である場合、または LifeKeeper/SPS の一部になった場合、すべての管理は LifeKeeper/SPS レベルで行われるためです。

削除手順

LifeKeeper/SPS で、次の手順を実行します。

LifeKeeper GUI コンソールで、ボリュームが関連付けられている依存関係を削除します。

1. **親レベルのリソース** を右クリックして、**[Remove Dependency...]** を選択します。
2. 適切な **ソースサーバー** を選択し、**[Next]** をクリックします
3. **[Child Resource]** で、ドロップダウンリストから対象の **ボリューム** を選択し、**[Next]** をクリックします。
4. 親/子の依存関係に関連するダイアログが表示されたら、**[Remove Dependency]** を選択し、**[Done]** を選択します。

   これで、ボリュームリソースがスタンドアロン階層としてリストされました。削除するには、次の手順を実行します。
5. **[Volume/Volume Hierarchy]** を右クリックし、**[Delete Resource Hierarchy...]** を選択します。
6. **[Target Server]** を選択し、**[Next]** を選択します。
7. ボリューム階層とターゲットサーバーの削除に関するダイアログが表示されたら、**[Delete]** を選択し、**[Done]** を選択します。

   これで、DataKeeper ストレージは LifeKeeper/SPS のリソースではなくなりました。
8. DataKeeper UI > Action Panel で、**[Delete Job]** を選択します。
9. 「Are you sure you want to delete the 'Volume (drive)' and its mirror?」というメッセージが表示された

ら、**[Yes]** を選択します。

複数のミラー/ターゲットがある場合、**[Delete Mirror]** を選択するとジョブも削除されます。

8.6.27. リカバリキットのアンインストール時に Remove がハングする

現象

サービス中のリカバリキットのリソース階層が存在するときにそのリカバリキットをアンインストールした場合、**Remove** がハングします。

これを回避するために、必ずリカバリキットのリソース階層のサービスを停止し、削除してから、リカバリキットソフトウェアをアンインストールすることを推奨します。

解決策

この状況では多数の関連プロセスがハングしており、すべてをクリアするのは難しいので、ほとんどの場合はシステムを再起動する必要があります。

8.6.28. 複製ボリュームのスイッチオーバの失敗

説明

複製ボリュームがスイッチオーバする際、DELETEMIRROR コマンドが失敗すると、以下のエラーメッセージがアウトプットパネルに表示されます。

> *WARNING* (No. 12104) Delete mirror action for volume R: failed with status 51 (command=C:/SDR/EMCmd10.10.1.2 DELETEMIRROR R: 10.10.1.1)

エラーステータス番号、説明、および推奨される処置に関する以下の表を参照してください。また、以下のコマンドを使用することでも、エラーステータスについての情報を得ることができます。

> コマンド: net helpmsg {status}
>
> 例: net helpmsg 51

エラーステータス	説明	推奨される処置
5	現在のソース上で、ミラーが削除されることを許可していません。	>両システムでミラーボリュームのアクセスからローカルシステムアカウントを除外しているかチェックしてください。
46	システム間でユーザ/パスワードが適合していません。コマンドプロンプトからの DELETEMIRROR が作動している場合にのみ発生します。	ドメインアカウントを使用するか、あなたが登録したローカルユーザアカウントと同じパスワードを使用してください。
51	Windows はネットワークパスを見つけることができません。	両システムで、すべてのネットワークカードが、Microsoft ネットワーク用ファイルとプリンタ共有にチェックされていることを確認してください。
53	指定された IP アドレスにアクセスできません。	ネットワーク設定を確認してください (HOSTS ファイルや DNS は一貫して IP アドレスを決定します)。
207	ring 2 stack が使用中です。	両システムで、すべてのネットワークカードが Microsoft ネットワーク用クライアントにチェックされていることを確認してください。

8.6.29. リソースタグ名の制限

タグ名の長さ

SIOS Protection Suite DataKeeper 内のすべてのタグは、256 文字以内にする必要があります。

有効な「特殊」文字

-	_	.	/					

タグの最初の文字に「.」および「/」を使用することはできません。

無効な文字

+	;	:	!	@	#	$	*	=	「スペース」

8.6.30. リストアおよびヘルスチェックアカウントの障害

現象

一部のリカバリキットは、ユーザやクライアントの動作をシミュレートするクエリ操作を実行することで、保護対象リソースを監視しています。これによって、SIOS Protection Suite は保護対象のアプリケーションやサービスに関する正確なステータス情報を得ることができます。また、リソースオブジェクト作成時には、ログイン権限を持った有効なユーザアカウント ID およびパスワードが必要になります。ユーザアカウントが特定のシステム上でログイン権限を持っていない場合、**Windows アプリケーションイベントログ** に以下のエラーメッセージが記録されます。

```
Error Number 1385 – "Logon failure: the user has not been granted the
requested logon type at this computer.
```

解決策

ドメイン管理者からユーザアカウントにログイン権限を付与してもらってください。また、ID とパスワードが必要なリカバリキットのほとんどにリソースプロパティまたは構成タブがあり、管理者はリソースに対するアカウント情報を変更できます。リソースオブジェクトを右クリックし、該当するプロパティまたは構成タブを選択してください。リソースにアカウント更新機能がない場合は、リソースオブジェクトを削除してから、アカウント情報を更新して新しく作成する必要があります。

8.6.31. SQL 2008

現象

SQL 2008 を使用する場合、スイッチオーバまたはフェイルオーバの後も変数 @@servername がプライマリシステムを参照しています。

解決策

変数 @@servernameを使用する代わりに、select SERVERPROPERTY('ServerName') を使用してください。このクエリは、スイッチオーバまたはフェイルオーバの後も正しいマシン名を返します。
または

1. 新しいバックアップサーバで以下のコマンドを実行してください。

   sp_dropserver @server='sys-A'

   sp_addserver @server='sys-B', local='LOCAL'

2. サービスを再起動してください。

8.6.32. SQL Server Reporting Services (MSSQLSERVER)

現象

SQL Server 2008 R2 サービスを保護する場合、オプションの保護対象サービスとして、「SQL Server Reporting Services (MSSQLSERVER)」が選択されることがあります。しかしながら、このサービスの起動に必要な時間が、デフォルトの Windows サービスタイムアウトを超える場合、エラー 1053 が発生してサービスの起動に失敗することがあります。SIOS Protection Suite リソースのサービス中処理は失敗します。

解決策

この問題は、システムのパフォーマンスおよび構成の問題に関連している場合があります。このサービスは保護しないことを推奨します。しかしながら、このサービスを保護する必要がある場合は、次のレジストリ設定によって、サービスが起動するまでの時間を延長することができます。HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control レジストリキーに DWORD の ServicesPipeTimeout 値を追加し、値に 60000 (十進数、= 60 秒) を設定してください。

8.6.33. 2 サーバクラスタの問題

現象

2 サーバクラスタでは、プライマリサーバに障害が発生したか、シャットダウンされて、バックアップサーバへのリソース階層のフェイルオーバが行われたとき、バックアップサーバへの階層のフェイルオーバが完全に実行される前に、バックアップサーバにも障害が発生したかシャットダウンされた場合、以下の動作が検出されます。

両方のサーバを再起動したとき、階層内の一部のリソースは一方のサーバで起動し、一部はもう一方のサーバで起動します。上位の親リソースがいずれのサーバでも起動していない場合があります。

解決策

両方のサーバを再起動し、SIOS Protection Suite の初期化が完了した後、階層管理インターフェースから起動しなかった階層内の親リソースを選択し、手動で起動してください。すべての階層が起動するまで、この作業を繰り返してください。

8.6.34. 不明なユーザ名または誤ったパスワード

アクセス拒否:不明なユーザ名または誤ったパスワード

現象

SIOS Protection Suite クライアントがシャットダウン中のサーバと通信しようとした場合、サーバはクライアントのログオンを拒否して、認証プロセスを中止することがあります。その場合、クライアントには次のメッセージが表示されます。「Access Denied: unknown user name or bad password.Only members of the SIOS Protection Suite-authorized security groups can use SIOS Protection Suite.Would you like to re-enter the authentication data?」

解決策

新しい証明書を入力するために **[はい]** をクリックしてから、**[キャンセル]** をクリックするか、証明書を再入力して **[OK]** をクリックしてください。

注記: 最初に **[いいえ]** をクリックした場合、LifeKeeper GUI はそのサーバから切断され、自動再接続は行われません。

8.6.35. Web クライアントのトラブルシューティング

背景

Web クライアントに ダイアログボックス が表示されません。

回答

Web クライアントに ダイアログボックス が表示されない場合は、以下を実行してください。

1. アプレットが起動に失敗したか確認してください。通常は、ブラウザのウィンドウ内にアプレットの状態を示すメッセージが表示されます。Internet Explorer では、状態を表すメッセージのほかに、アプレットの代わりのアイコンが表示されることがあります。このアイコンをクリックすると、失敗に関する説明が表示されます。
2. **Java コンソール** を開いてください。

   ・**FireFox** および 旧バージョンの **Internet Explorer** を使用している場合は、コントロールパネルを開き、[Java プラグイン] アイコンをクリックして、コンソール表示を有効にしてください。ブラウザを再起動してください。

   ・**新しいバージョンの Internet Explorer** を使用している場合は、**[ツール] メニューの [Sun の Java コンソール]** をオンにしてください。[Sun の Java コンソール] メニューが表示されない場合は、**[ツール] メニューの [アドオンの管理]** をクリックし、コンソール表示を有効にしてから、ブラウザを再起動すると、Java コンソールが表示されます。

   ・**Mozilla** を使用している場合は、**[ツール] メニューの [Web 開発] をクリックし、[Sun の Java コンソール]** をクリックしてください。

Web クライアントが開かない場合は、URL (**http://<server name>:81**) を指定して、ブラウザを再起動してください。

コンソールのメッセージを確認してください。エラーメッセージが表示された場合は、それを参考にして問題を解決してください。問題がネットワークに関係している場合は、「 ネットワーク関連のトラブルシューティング 」を参照してください。

8.6.36. Win2008 – IIS リソース階層作成エラー

現象

Win2008 システムでは、IIS リソース階層を作成するときに以下のメッセージが表示されます。

No qualified sites were found…

作成は失敗します。

背景/トラブルシューティング:

以下のコマンドを実行してください。

C:\LK\Admin\kit\webapp\bin>enumiis query all

以下のエラーメッセージを探してください。

ERROR: CoCreateInstance Failed! Error: -2147221164 (80040154)

ERROR: W3Service Com Object Failed to initialize

解決策

Win2008 では、SIOS Protection Suite IIS キットに IIS 6 Management Compatibility (役割サービス) が必要です。すべてのオプション (Metabase Compatibility、WMI Compatibility、Scripting Tools、Management Console) をインストールしてください。

9. アプリケーションリカバリーキット

SIOS Protection Suite for Windows Application Recovery Kits (ARKs) は特定のアプリケーションをSPS上で管理、制御するためのツールとユーティリティを含んでいます。今バージョンのSPSで利用できるARKは以下の通りです。

SIOS Protection Suite Microsoft SQL Server リカバリーキット

SIOS Protection Suite PostgreSQL Server リカバリーキット

SIOS Protection Suite Oracle リカバリーキット

SIOS Protection Suite Microsoft Internet Information Services リカバリーキット

9.1. はじめに SIOS Protection Suite Microsoft SQL Server

SIOS Protection Suite Microsoft SQL Server

SIOS Protection Suite Microsoft SQL Server Recovery Kit ソフトウェアを使用すると、Microsoft SQL を使用したデータベースのデータの完全性と、SIOS Protection Suite for Windows による可用性の向上に結び付けることができます。

LifeKeeper GUI によって、SQL リソース階層を簡単に作成できるようになります。SIOS Protection Suite は、SQL Server インスタンスが使用するすべてのディスクリソースはもちろん、データベースアクセスに使用される IP ソケットリソースも保護します。

重要: 本キットでは、SQL Serverの次の機能を利用できません：SQLレプリケーション（スナップショット、マージ、トランザクション）、SQLのログ配布、SQLデータベースのミラーリング、SQL Server AlwaysOn 可用性グループ

Microsoft によると、SQL Server failover cluster インスタンス (FCI) では、クラスターノードをドメイン参加させる必要があります。この制約により、SIOS Protection Suite for Windows は、ワークグループ環境でMicrosoft SQL Server Failover Cluster インスタンスを保護するために使用することができません。

9.1.1. SQL Server サービス

SIOS Protection Suite Microsoft SQL Server Recovery Kit は次のサービスを監視および保護します。

SQL2008(R2), 2012, 2014, 2016 or 2017:

コアサービス	オプションサービス
SQL Server (MSSQLSERVER)	SQL Server Agent
	SQL Server Reporting Services
	Distributed Transaction Coordinator
	SQL Server Browser
	SQL Server VSS Writer
	SQL Server Integration Services
	SQL Full-text Filter Daemon Launcher（SQL Server 2014 より利用可能）
	SQL Server Launchpad（SQL Server 2016 より利用可能）
	SQL Server PolyBase Data Movement（SQL Server 2016 より利用可能）
	SQL Server PolyBase Engine（SQL Server 2016 より利用可能）
	SQL Server CEIP service（SQL Server 2016 より利用可能）

注記：「SQL Server Integration Services」は、SQL Server のオプションとしてのその機能をインストールする際に、保護するオプションサービスのリストに表示されます。

データファイルは共有ボリュームまたは複製ボリュームに格納されます。SIOS Protection Suite は障害を検出すると、データベースとともに、関連するボリュームと IP ソケットリソースをバックアップサーバに切り替えます。SIOS Protection Suite は、すべての依存リソースをバックアップサーバに切り替えると、SQL サービスおよび保護対象のオプションサービスを起動します。

9.1.2. リカバリキットの要件

SIOS Protection Suite Microsoft IIS Recovery Kit をインストールして設定する前に、構成が以下の要件を満たしていることを確認してください。

- SIOS Protection Suite は、SIOS Protection Suite for Windows リリースノートの オペレーティングシステム に記載されている Windows オペレーティングシステムをサポートします。
- **SIOS Protection Suite ソフトウェア** 。クラスタ内のすべてのサーバに同じバージョンの SIOS Protection Suite for Windows をインストールする必要があります。共有ストレージではなく複製ボリュームで Microsoft SQL Server を使用する計画を立てている場合は、SIOS DataKeeper for Windows ソフトウェアを各サーバ上にインストールする必要があります。
- **Microsoft SQL Server RDBMS ソフトウェア** 。このキットは Microsoft SQL2008(R2)、2012 または 2014 の全バージョンに対して互換性があります。ただし、クラスタ内のすべてのシステム上に同じバージョンの Microsoft SQL Server がインストールされている必要があります。
- **通信プロトコル** 。Microsoft はクラスタ環境では TCP/IP を使用するように強く推奨しています。SIOS Protection Suite は LAN Manager をサポートしますが、このドキュメントはユーザが TCP/IP を使用していることを前提とし、設定の説明では LAN Manager リソースではなく切り替え可能 IP リソースについて説明しています。

リリースおよびご注文につきましては、弊社の SIOS Protection Suite 営業担当者にお問い合わせください。

9.1.3. SQL Server のインストール

SIOS Protection Suite Microsoft SQL Server Recovery Kit を適切に操作するには、ハードウェアとソフトウェアを正しくセットアップする必要があります。

最初に、このガイドの「 階層の管理 」セクションを参照してください。このセクションでは、SIOS Protection Suite 環境における Microsoft SQL Server の管理に役立つ一般的なガイドライン、設定の詳細、トラブルシューティングのヒントを提供します。

9.1.3.1. リカバリキットのインストール

SIOS Protection Suite Microsoft SQL Server Recovery Kit は FTP ダウンロードで配布されます。インストールは、標準のインストールインターフェースを提供する InstallShield を使用して、簡単にすばやく実行できます。

SIOS Protection Suite Microsoft SQL Server Recovery Kit ソフトウェアをインストールする前に、製品の前提条件 をよく理解していることを確認してください。SIOS Protection Suite で SQL リソースを保護するには、SIOS Protection Suite Microsoft SQL Server Recovery Kit ライセンスキットをインストールする必要があります。

9.1.3.2. キットの削除

SIOS Protection Suite Microsoft SQL Server Recovery Kit ソフトウェアを削除するには、コントロールパネルの **[プログラムの追加と削除]** または **[プログラムと機能]** アプレットにある **Microsoft SQL Server Recovery Kit** を選択してください。

注意: キットを削除するときには、サービス中の SQL インスタンスおよびリソースが存在しないことを確認してください。キットが削除されると、これらのリソースは使用できなくなります。また、キットを削除する前にすべての SQL 階層を削除してください。

9.1.3.3. SIOS Protection Suite とともに SQL Server をインストールおよび設定する

SIOS Protection Suite Microsoft SQL Server Recovery Kit を適切に操作するには、ハードウェアとソフトウェアを正しくセットアップする必要があります。

このセクションでは、SIOS Protection Suite 環境における Microsoft SQL Server の管理に役立つ一般的なガイドライン、設定の詳細、トラブルシューティングのヒントを提供します。階層の管理 作業についての再確認を忘れないでください。

SQL Server をインストールする前に

SQL Server ソフトウェアをインストールする前に、サーバとストレージが設定され、SIOS Protection Suite がクラスタ内の各サーバにインストールされている必要があります。

9.1.3.4. インストール – 共有ストレージシステム

プライマリサーバ上

1. バックアップサーバの電源を落とします。これは、共有ストレージへの同時アクセスが発生しないようにするためです。

2. **Windows ディスク管理** ツールを使用して、ディスクリソースを設定し、使用したい共有ボリュームを定義します。(ボリュームは適切なサイズにしてください。)

3. **Windows エクスプローラ** を使用して、SQL Server インスタンスによって使用されるすべてのボリュームをネットワークから共有解除します。

4. ネットワークを、SIOS Protection Suite TCP/IP コミュニケーションパスと切り替え可能な IP アドレス (該当する場合) をサポートするように設定します。

5. SIOS Protection Suite Core ソフトウェア、SIOS Protection Suite SQL Server Recovery Kit の順にローカルディスクにインストールします。

バックアップサーバ上

1. バックアップサーバを起動し、**ディスク管理** ユーティリティを使用して、プライマリサーバに割り当てたものと同じドライブレターを共有ボリュームに割り当てます。

2. SIOS Protection Suite Core ソフトウェア、SIOS Protection Suite SQL Server Recovery Kit の順にローカルディスクにインストールします。

プライマリサーバ上

これで両方のサーバに SIOS Protection Suite がインストールされました。プライマリサーバに戻って、以下を実行してください。

1. SIOS Protection Suite で、プライマリサーバとバックアップサーバの間のコミュニケーションパスを作成します。

2. SIOS Protection Suite でボリュームリソースと IP コミュニケーションパスを作成し、それらをバックアップサーバに拡張します。その後、SQL Server リソース階層を作成するときに、SIOS Protection Suite は依存関係に従ってこれらのリソースを自動で階層内に移動します。

SQL Server ソフトウェアのインストール

1. 共有ボリュームを使用している場合は、LifeKeeper GUI を使用してバックアップサーバ上でボリュームリソース階層を [サービス開始] にします。

2. 以下のガイドラインに従って、バックアップサーバに Microsoft SQL Server をインストールします。

・追加の機能と共に、データベースエンジンをインストールします。インスタンスデータとログファイルを、SIOS Protection Suite によって保護されているボリュームに格納されるように設定します。

・「 **混合モード** 」のデータベース認証を選択し、SA アカウント用の空白でないパスワードを入力します。パスワードは、クラスター内のすべてのサーバーで同一にする必要があります。

インストールが完了したら **Microsoft SQL Server Configuration Manager** を使用して、バックアップサーバ上で SQL Server が正しく起動されるかどうかを確認します。バックアップサーバ上の Microsoft SQL サービスをすべて停止してください。

共有ボリュームに対して、以下の手順を実行してください。

1. プライマリサーバ上で、ボリュームリソース階層を [サービス開始] にします。
2. プライマリサーバ上で **エクスプローラ** を開き、共有ボリュームに関連付けられたドライブにアクセスします。
3. 以前に SQL データファイルをインストールしたディレクトリを削除します。(これらのディレクトリは次の手順で再インストールします。)
4. Microsoft SQL Server を、バックアップサーバとまったく同じ方法でプライマリサーバにインストールします (プログラムファイルをローカルディスク、データファイルを共有ボリュームにインストール)。

インストールが完了したら、**Microsoft SQL Server Configuration Manager** を使用して、プライマリサーバ上で SQL Server が正しく起動されるかどうかを確認します。

9.1.3.5. ターゲットシステムで管理者ではないローカルシステムアカウントを使用する

特定の状況で、SQL Server サービスアカウント (sql_svc) をローカル管理者グループまたはドメイン管理者グループに追加することができない場合があります。このような場合、そのサービスアカウントでファイルの権限の問題が発生します。ユーザには、以下のようなメッセージで「アクセス拒否」エラーが通知されます。

”Open failed: Could not open file E:\SQL1\MSSQL10_50.SQL1\MSSQL\DATA\master.mdf for file number 1. OS error: 5 (Access is denied). ”

解決策: 以下を実行してください。

1. ファイル (例: c:\file.ksh) に以下のスクリプトコードをコピーします。

```
$LKROOT/bin/find . > $LKROOT/out/file
while read filename
do
icacls "${filename}" /grant $1:F
done < $LKROOT/out/file
$LKDROOT/bin/rm $LKROOT/out/file
```

2. 各ドライブ (E、F) で以下のコマンドを実行して、ボリュームで起動します。このコマンドは管理者 (ローカルまたはドメイン) として実行してください。これによって、当該ユーザのみにファイル権限が付与されます。SQL Server サービスユーザはファイルにアクセスできるようになり、管理者アカウントとして追加する必要はありません。

```
E:\>c:\lk\bin\sh c:\file.ksh domain\sql_svc
```

注記: この例では、SteelEye Protection Suite は c:\lk にインストールされており、domain\sql_svc は SQL Server サービスユーザ ID の名前です。

9.1.3.6. インストール – 複製ストレージシステム

プライマリサーバ上

1. **[Windows ディスク管理]** ツールを使用して、ディスクリソースを設定し、使用したい複製ボリュームを定義します。(ボリュームは適切なサイズにしてください。)

2. **Windows エクスプローラ** を使用して、SQL Server によって使用されるすべてのボリュームをネットワークから共有解除します。

3. ネットワークを、SIOS Protection Suite TCP/IP コミュニケーションパスと切り替え可能な IP アドレス (該当する場合) をサポートするように設定します。

4. SIOS Protection Suite Core ソフトウェア、SIOS Protection Suite SQL Server Recovery Kit の順にローカルディスクにインストールします。

5. SIOS DataKeeper ソフトウェアをローカルディスクにインストールします。詳細については、SIOS Protection Suite for Windows インストレーションガイド を参照してください。

6. LifeKeeper GUI を使用して、プライマリサーバとバックアップサーバの間のコミュニケーションパスを作成します。

7. SIOS Protection Suite で IP コミュニケーションパスを作成し、それらをバックアップサーバに拡張します。その後、SQL Server リソース階層を作成するときに、SIOS Protection Suite は依存関係に従ってこれらのリソースを自動で階層内に移動します。

注記: SQL Server 階層が作成されるとき、SIOS DataKeeper リソースは自動的に作成され、依存関係に従って SQL Server リソース階層に移動されます。

バックアップサーバ上

1. **LifeKeeper GUI** を使用して、ボリュームリソース階層をサービス開始の状態にします。

2. 以下のガイドラインに従って、Microsoft SQL Server をインストールします。

   ・追加の機能と共に、データベースエンジンをインストールします。インスタンスデータとログファイルを、SIOS Protection Suite によって保護されているボリュームに格納されるように設定します。

   ・「 **混合モード** 」のデータベース認証を選択し、SA アカウント用の空白でないパスワードを入力します。パスワードは、クラスター内のすべてのサーバーで同一にする必要があります。

3. インストールが完了したら **Microsoft SQL Server Configuration Manager** を使用して、バックアップサーバ上で SQL Server が正しく起動されるかどうかを確認します。バックアップサーバ上の Microsoft SQL サービスをすべて停止してください。

注記: 複製ボリュームの場合、*SQL tempdb* データベースを SIOS Protection Suite で保護されていないボリュームに移動してパフォーマンスを改善することもできます。

4. Microsoft SQL Server を、バックアップサーバとまったく同じ方法でプライマリサーバにインストールします (プログラムファイルをローカルディスク、データファイルを複製ボリュームにインストール)。

5. インストールが完了したら **Microsoft SQL Server Configuration Manager** を使用して、プライマリサーバ上で SQL Server が正しく起動されるかどうかを確認します。

   注記: データファイルが複製ボリュームにインストールされた場合、_SQL tempdb_ データベースを SIOS Protection Suite で保護されていないボリュームに移動してパフォーマンスを改善することもできます。

プライマリサーバ上

1. プライマリサーバ上で、**通信リソース** をサービス中にします。

2. プライマリサーバ上で **SQL Server サービス** を開始します。

3. プライマリサーバ上に **SQL Server 階層** を作成して、バックアップサーバに拡張します。**ボリュームリソースの拡張** 処理中に、**作成された複製のミラー** を選択し、**[次へ]** を選択してウィザードを終了します。設定はこれで完了です。詳細については、SQL 階層の作成 を参照してください。

   手動でフェイルオーバを実行し、新しい **SQL Server 階層** をテストしてください。

9.1.3.7. 拡張構成の追加のセットアップ作業

ご利用の設定で共有のストレージデバイスを使用している場合、または SIOS DataKeeper を使用している場合は、3 番目 (またはそれ以上) のサーバに拡張する設定を選択することができます。

1. SIOS Protection Suite による SQL Server のインストールおよび設定 に示されている手順で 2 つのシステムを設定します。

2. 保護対象ボリュームを 3 番目のサーバに切り替えます。

3. Microsoft SQL Server ソフトウェアをローカルドライブにインストールし、マスターデータベースを他のサーバが使用しているものと同じ共有ボリューム / 複製ボリューム上にインストールします。こうすることで、階層を拡張して SIOS Protection Suite のカスケーディング機能を使用できるようになります。

9.1.3.8. SQL 階層の作成

SIOS Protection Suite for Windows インストレーションガイド に記述されている必要なセットアップ作業が完了したら、以下の手順に従ってデータベースを保護する SQL Server 階層を定義してください。

重要	既存の SQL データベースがインストールされている場合、この手順を完了する前に SQL データベースにアクセスしているすべてのクライアントアプリケーション (ローカル、リモートにかかわらず) を閉じる必要があります。オペレーションは自動化されており、その間にデータベースの起動と再起動が複数回行われ、実行中アプリケーションは各サービス動作のコマンドの影響を受ける可能性があります。そのため、この手順が完了した後にアプリケーションを再起動してください。

1. LifeKeeper GUI メニューから **[編集]** を選択し、次に **[サーバ]** を選択します。メニューから **[リソース階層の作成]** を選択します。

2. **[保護するアプリケーションの作成]** ダイアログボックスが表示されます。プルダウンリストから **プライマリ** および **バックアップ** サーバを選択します。**[次へ]** を選択して続行します。

3. ダイアログボックスはクラスタ内にインストールされたすべての認証済みのリカバリキットが表示されたドロップダウンリストボックスとともに表示されます。**[MS SQL Server]** を選択し、**[次へ]** をクリックします。

4. 次の表に示す情報を入力するように求められます。ダイアログボックス内で **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは、前に入力した情報を修正する必要があるエラーが発生した場合に便利です。いつでも **[キャンセル]** をクリックして、作成処理全体を取り消すことができます。

フィールド	説明
Microsoft SQL Server のインスタンスの選択	SIOS Protection Suite で保護する Microsoft SQL Server のインスタンスを選択します。 SIOS Protection Suite は、このインスタンスの設定データを読み込み、関連ボリュームを階層に組み込みます。
Microsoft SQL 管理ユーザ名の入力	このサーバで Microsoft SQL の管理権限を持つユーザの名前を入力してください。管理ユーザアカウントはマスタデータベースに対する SA 権限を持っている必要があります。
パスワードの入力	入力したユーザアカウントの管理パスワードを入力してください。
設定の確認	データベースファイルの現在の位置を示します。SIOS Protection Suite を使用して保護するインスタンスに関連するファイルがシステムドライブ (C:) に配置されていた場合、その場所をハイライトで示します。
以下のフィールドはデータベースの再配置が必要な場合にのみ表示されます。	
データベースを再配置するボリュームの選択	データベースのマイグレーションが必要な場合に、影響を受けるデータベースを保存するボリュームを選択してください。
MOVE オペレーションの確認	選択したデータベースの配置場所と内容について確認してください。

データベースの再配置	MOVE オペレーション時に、データベースを再配置する処理の経過を操作ウィンドウに表示します。
保護対象のオプショナルサービスの選択	この階層で保護されるオプションの SQL サービスを選択してください。このリストには LifeKeeper の保護に適したサービスのみが表示されます。
保護する IP アドレス	インスタンスで保護する IP アドレスを選択してください。名前付きパイプだけを使用する場合、IP アドレスは不要です。ただし、名前付きパイプだけの使用は避けてください。
名前付きパイプの別名	名前付きパイプの別名
Microsoft SQL Server のリソース名	固有のタグ名を入力します。自動で表示されるデフォルトのタグ名をそのまま使用することもできます。 **注意：**タグ名に使用できる文字はASCII印字可能文字のみです。

5. **[作成]** をクリックすると、**ウィザード** により SQL リソースが作成されます。SIOS Protection Suite によって入力データが検査されます。SIOS Protection Suite が問題を検出すると、情報ボックスにエラーメッセージが表示されます。

6. 別の情報ボックスが表示され、SQL リソース階層の作成に成功したこと、およびフェイルオーバによって保護するには、クラスタ内の別のサーバにリソース階層を **拡張** する必要があることを示すメッセージが表示されます。**[次へ]** をクリックします。

7. **[続行]** をクリックすると SIOS Protection Suite の **拡張前処理ウィザード** が起動されます。

9.1.3.9. SQL 階層の拡張

この操作は **[編集]** メニューから開始できますが、**[リソース階層の作成]** オプションの処理を完了すると自動的に開始されます。その場合は、下記の手順 2 を参照してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の拡張]** を選択します。**[拡張前処理ウィザード]** が表示されます。**拡張** 操作に慣れていない場合は、**[次へ]** をクリックしてください。

2. **[拡張前処理ウィザード]** では引き続き情報の入力を求めるメッセージが表示されます。**注記**: 最初の 2 つのフィールドは、**[編集]** メニューから **拡張** を開始した場合のみ表示されます。

3. 拡張前のチェックが正常に終了したというメッセージが表示されたら、**[次へ]** をクリックします。

フィールド	説明
バックアップの優先順位	1～999 の数値を入力して、このリソースのカスケーディングフェイルオーバシーケンスにおけるテンプレートサーバの優先順位を指定してください。小さい数値ほど優先順位が高くなります。SIOS Protection Suite は、階層が作成されたサーバに「1」を割り当てます。特定のリソースに関して 2 台のサーバが同じ優先順位を持つことはできません。

4. **[拡張]** をクリックします。

重要	データベースを移動させた後に、SQL アプリケーションとデータベースファイルにアクセスできることを確認する必要があります。すべてのファイルは、システムコピーユーティリティを使用して再配置されます。この手順が正常に完了していることを確認した後、関連するデータとログファイルを削除することができます。

9.1.3.10. SQL 階層の拡張解除

SIOS Protection Suite クラスタの 1 つのサーバからリソース階層を削除する場合は、次の手順を実行してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の拡張解除]** を選択します。

2. SQL リソースの拡張解除の対象となる **ターゲットサーバ** を選択します。SQL リソースが現在 In Service のサーバは選択できません。(右側のペインにあるリソースインスタンスを右クリックして **拡張解除** 作業を選択した場合、このダイアログボックスは表示されません。) **[次へ]** をクリックします。

3. 拡張解除する SQL 階層を選択し、**[次へ]** をクリックします。(左右どちらかのペインのリソースインスタンスを右クリックして **拡張解除** 作業を選択した場合、このダイアログボックスは表示されません。)

4. 拡張解除するために選択したターゲットサーバと SQL リソース階層を確認する情報ボックスが表示されます。**[拡張解除]** をクリックします。

5. SQL リソースの拡張解除に成功したことを通知する情報ボックスが表示されます。**[完了]** をクリックして、**[リソース階層の拡張解除]** メニューを終了します。

9.1.3.11. SQL 階層の削除

SQL 階層または SQL インスタンスを削除する前に、プライマリサーバでその階層がアクティブ (緑色) になっていることを確認してください。階層を削除する前に依存関係を解除することもできます。依存関係を解除しないと、それも削除されます。

SIOS Protection Suite 環境のすべてのサーバからリソース階層を削除するには、次の手順を実行してください。

1. **[編集]** メニューの **[リソース]** を選択し、次に **[リソース階層の削除]** を選択します。

2. SQL リソース階層を削除する **ターゲットサーバ** の名前を選択し、**[次へ]** をクリックします。(左右どちらかのペインのリソースインスタンスを右クリックして **リソース削除** 作業を選択した場合、このダイアログボックスは表示されません。)

3. **削除する階層** を選択します。(左右どちらかのペインのリソースインスタンスを右クリックして **リソース削除** 作業を選択した場合は、このダイアログボックスは表示されません。) **[次へ]** をクリックします。

4. 選択したターゲットサーバと削除対象として選択した階層を確認する情報ボックスが表示されます。**[次へ]** をクリックします。

5. SQL リソースの削除に成功したことを通知する情報ボックスが表示されます。

6. **[完了]** をクリックして終了します。

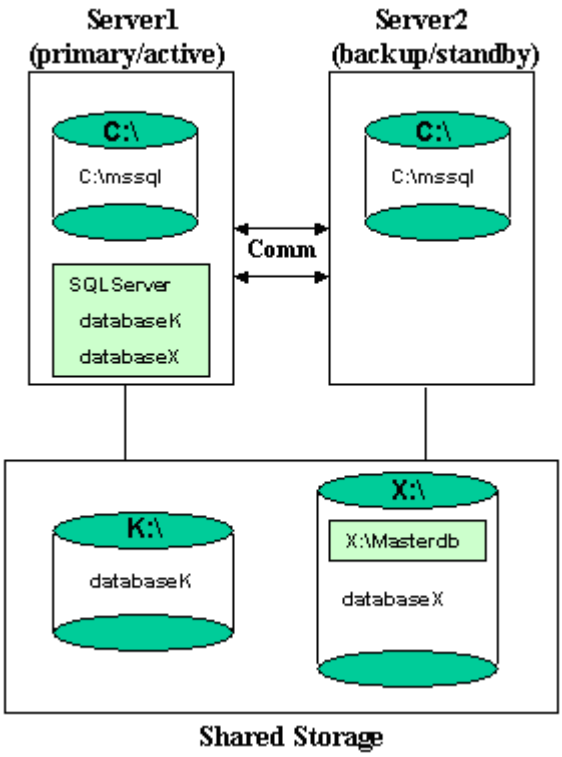
9.1.4. SQL Server 設定上の考慮事項

クラスタをインストールして設定する前に、アクティブ/スタンバイ構成の概念と、複数のインスタンスを SQL 構成で設定する方法を理解することが重要です。

SQL 構成

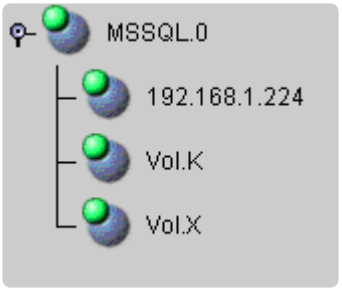
各 SQL Server にマスタデータベースが 1 つしかなく、それを共有ボリュームまたは複製ボリュームに配置した場合、クラスタはアクティブ/スタンバイ構成になります。サービスは一度に 1 つのシステムだけで実行されます。サーバには、SIOS Protection Suite 内部で優先順位が割り当てられ、特定の階層をフェイルオーバする順序が決定されます。

1 組のサーバに 1 つの SQL インスタンスをインストールした状態を次図に示します。インスタンスには 2 つのデータベース (databaseK と databaseX) があり、各データベースは個別のボリュームに格納されています。マスタデータベースは 1 つであり、共有ボリューム X に格納されていることに注意してください。



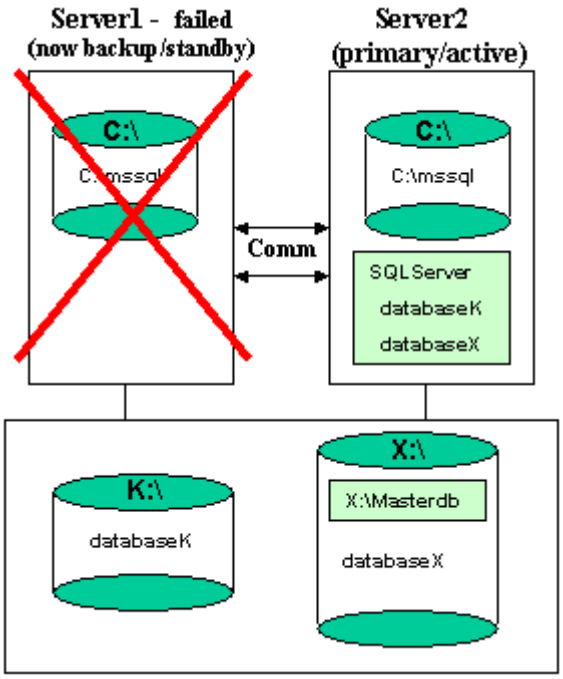
SIOS Protection Suite 内に SQL 階層を作成すると、保護する SQL インスタンス、およびデータベース接続に使用する IP リソースを指定するように求められます。SIOS Protection Suite は、そのインスタンスの設定データを読み込み、指定されたボリュームを階層に組み込みます。

作成した階層は、LifeKeeper GUI に次のように表示されます。



フェイルオーバ

SIOS Protection Suite は、障害が発生すると、バックアップサーバの SQL Server 階層をサービス中にします。バックアップサーバの SQL Server が起動して、定義済みデータベースの保護を引き継ぎます (次図参照)。

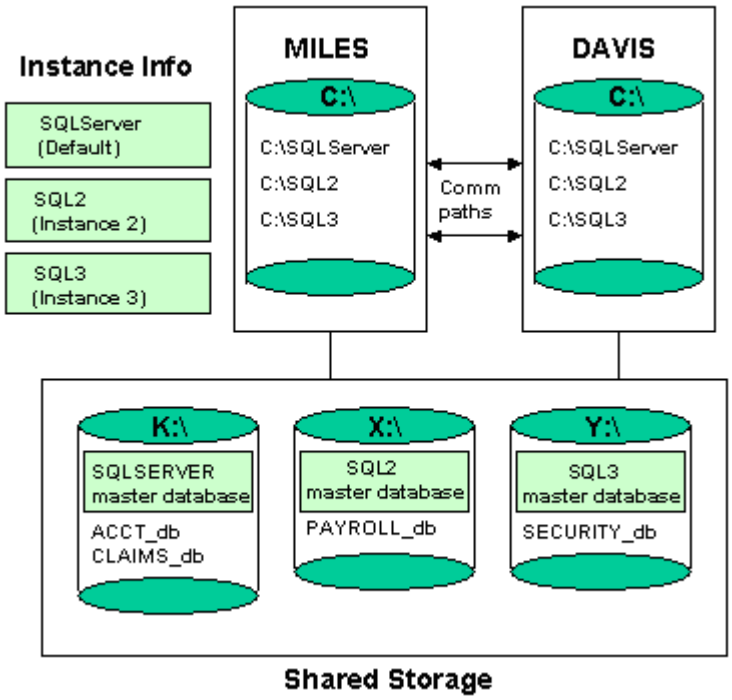


複数の SQL インスタンス

SQL Server を複数回インストールして、複数の SQL インスタンスを作成できます。SIOS Protection Suite は SQL Server の複数のインスタンスを保護できます。SIOS Protection Suite は、SQL のインストール時に指定された固有の名前でインスタンスを識別します。

1 つの SQL インスタンスには複数の SQL データベースを登録できます。各インスタンスは単一の SIOS Protection Suite 階層で保護されます。したがって、SQL インスタンスに 2 つのデータベースがある場合、対応する SIOS Protection Suite 階層は 2 つのデータベースと関連する IP とボリュームリソースを保護します。

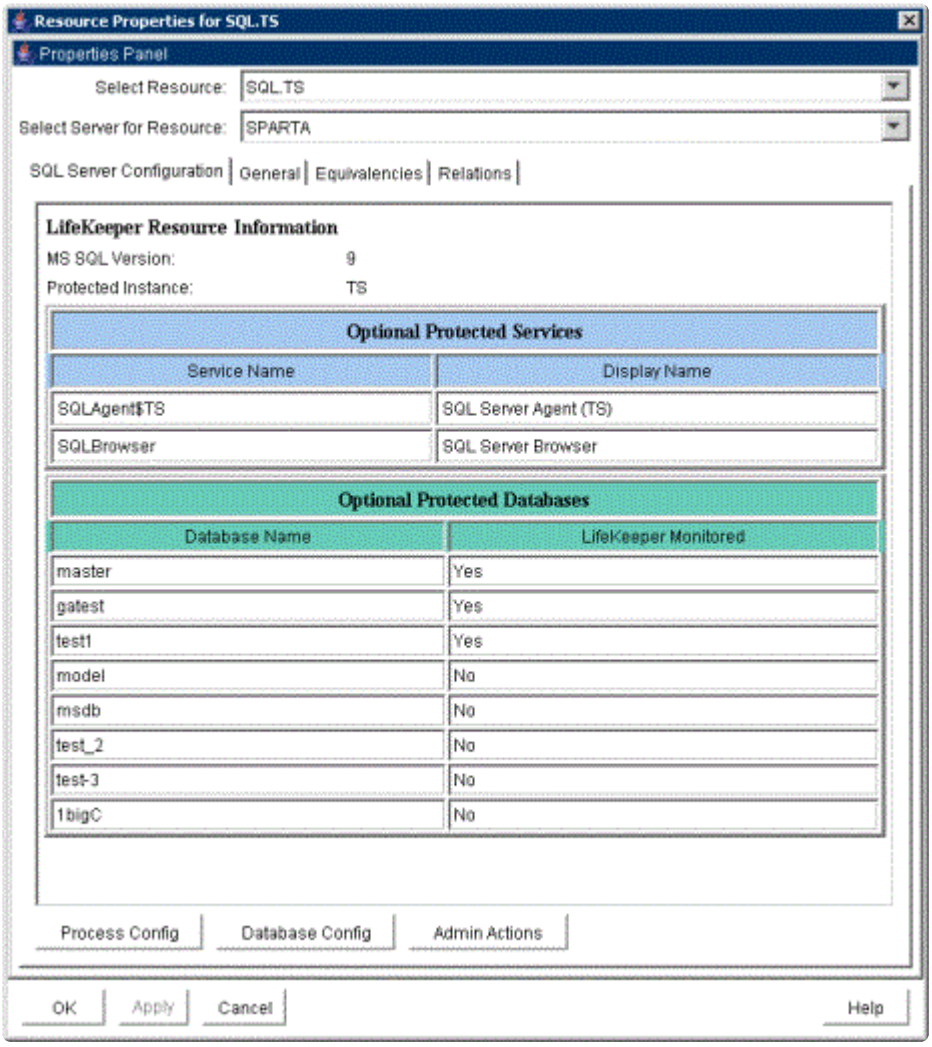
下の図は、SQLServer (デフォルトのインスタンス)、SQL2、SQL3 の 3 つの SQL インスタンスです。これらのインスタンスは 1 組のサーバ (MILES と DAVIS) にインストールされています。



注記	• データベースは 3 つの異なる共有ストレージボリューム (K、X、Y) に格納されています。デフォルトのインスタンスには 2 つのデータベース、残り 2 つのインスタンスにはそれぞれ 1 つのデータベースが格納されていることに注意してください。 • 各サーバは複数のインスタンスのプライマリサーバとバックアップサーバとして動作します。 • MILES がデフォルトインスタンスのプライマリサーバになり、DAVIS が SQL2 と SQL3 インスタンスのプライマリサーバになることも可能です。

9.1.4.1. SQL Server の設定管理

LifeKeeper GUI を使用して保護対象の SQL Server リソースを管理するには、LifeKeeper GUI の右側のペインで SQL Server リソースを右クリックし、**[プロパティ]** 、**[SQL Server 設定]** タブの順にクリックします。**[SQL Server 設定]** ページでは、SQL リソースの情報を参照または変更できます。



9.1.4.2. プロセス設定メニュー

このメニューでは、リソース階層で保護されているオプションの SQL プロセス一覧を変更できます。SIOS Protection Suite は保護されているすべてのオプションサービスを監視します (SQL 階層の監視 を参照してください)。

操作 の選択

- *プロセスの追加* - 保護対象の構成にプロセスを追加します。SIOS Protection Suite は新しい SQL サービスの監視を開始します。
- *プロセスの削除* - 保護対象の構成からプロセスを削除します。

フィールド	説明
サービス名	保護対象の構成に **追加** または **削除** するサービス名を入力してください。
すべてのシステムを更新	該当のクラスタ内のすべてのシステムを更新する場合は、**[はい]** を選択してください。それ以外の場合は、**[いいえ]** を選択して現在のシステムだけを更新します。**[いいえ]** を選択した場合は、プロセスを手動でバックアップサーバに追加する必要があります。

9.1.4.3. データベース設定メニュー

このメニューでは、リソース階層で保護するオプションの SQL データベースを変更します。SIOS Protection Suite は SQL クエリを発行してデータベースとの接続をテストし、保護対象の SQL データベース (オプション) を監視します (SQL 階層の監視 を参照してください)。

操作 の選択:

- *データベースの追加* - 保護対象の設定にデータベースを追加します。**注記** : このオプションは、SQL リソースがアクティブ (サービス中) になっているサーバだけに使用できます。

- *データベースの削除* - 保護対象の設定からデータベースを削除します。

フィールド	説明
データベース名の入力	保護対象の設定に **追加** または **削除** するデータベースの名前を入力してください。
すべてのシステムを更新	該当のクラスタ内のすべてのシステムを更新する場合は、**[はい]** を選択してください。それ以外の場合は、**[いいえ]** を選択して現在のシステムだけを更新します。**[いいえ]** を選択した場合は、プロセスを手動でバックアップサーバに追加する必要があります。

9.1.4.4. 管理操作メニュー

このメニューでは、SIOS Protection Suite を操作する SQL 管理ユーザを管理します。または階層を拡張する際、プライマリサーバとバックアップサーバとの間で発生した ID 競合も解決します。

[管理操作] の選択

- *ユーザ管理* - 保護対象のリソース階層が使用する現在のユーザ名を表示または更新します。

9.1.4.5. 管理ユーザメニュー

管理作業 の選択

- *現在のユーザを表示* - 保護対象のリソース階層で使用される現在のユーザ名を表示します。
- *パスワードの変更* - 保護対象のリソース階層に関連付けた現在のユーザのパスワードを変更します。
- *ユーザおよびパスワードの変更* - SIOS Protection Suite の操作の際に SQL インスタンスを管理監視するユーザとパスワードの両方を更新します。ユーザは、保護下にあるすべてのデータベースに対して sqladmin 権限を持つ必要があります。

注記: ユーザおよびパスワードを変更するには、SQL インスタンスが実行されている必要があります。

フィールド	説明
ユーザ名の入力	管理ユーザ名を入力してください。管理ユーザのアカウントには、SIOS Protection Suite で保護する全データベースに対する SA パーミッションを付与する必要があります。
パスワードの入力	更新するユーザアカウントの管理パスワードを入力してください。

ID 不一致の解決 (SQL 2005 のみ)

フィールド	説明
サービスの種類の選択	レジストリを修復して、SIOS Protection Suite による保護を許可するサービスを選択してください。 プライマリサーバとバックアップサーバの SQL Server サービス ID だけが異なる場合は、**[Sql]** を選択してください。 プライマリサーバとバックアップサーバの SQL OLAP Service ID だけが異なる場合は、**[Olap]** を選択してください。 プライマリサーバとバックアップサーバの SQL Reporting Service ID だけが異なる場合は、**[Rs]** を選択してください。 **Sql** 、**Rs** 、**Olap** サービスを同時に更新する場合は、**[All]** を選択してください。
テンプレートサーバの選択	修復するリソースのテンプレートサーバ (プライマリ) を選択します。テンプレートサーバは、サービス中 (ISP) のリソースを保持する必要があります。
ターゲットサーバの選択	修復するリソースのターゲット (バックアップ) サーバを選択します。ターゲットサーバは、サービス中 (ISP) のリソースを保持していてはなりません。
確認	上記で入力した情報が正確かどうかを確認します。処理を実行するには **[続行]** 、情報を変更するには **[戻る]** 、キャンセルする場合は **[キャンセル]** を選択してください。

9.1.4.6. SQL リソース階層のテスト

手動スイッチオーバを開始すると、SQL リソース階層をテストできます。これにより、リソースインスタンスのプライマリサーバからバックアップサーバへのフェイルオーバがシミュレートされます。

[編集] 、**[リソース]** 、**[サービス開始]** の順に選択。例えば、バックアップサーバでサービス開始要求を実行すると、アプリケーション階層はプライマリサーバでサービス停止になり、バックアップサーバではサービス開始となります。この時点で、元のバックアップサーバがプライマリサーバとなり、元のプライマリサーバがバックアップサーバとなります。

[サービス停止] の要求を実行した場合、このアプリケーションはサービス停止になり、別のサーバのアプリケーションはサービス開始になりません。

9.1.5. SQL Server 階層の管理

SQL Server の管理は、以下のガイドラインどおりに行ってください。

保護されたコミュニケーションパス経由でアクセスする

リモートアクセスにリソース名を使用する

ボリュームを SQL 専用にする

SQL Server 環境での手動スイッチオーバの制限について

Microsoft SQL Management ツールの実行

SQL Server の起動と停止は SIOS Protection Suite 上で実行する

Microsoft SQL Server ボリュームの追加

スイッチオーバ後にデータベースの「Suspect」状態から回復

Microsoft SQL Server (MSSQLServer) の一時停止

切り替え可能な IP アドレスで接続するように SQL Server を設定

SQL Server のログインおよびパスワードの管理

SQL 階層の監視

9.1.5.1. 保護されたコミュニケーションパス経由でアクセスする

サービスへのリモートアクセスは、リソース階層によって保護されている IP アドレスで行う必要があります。これにより、どのサーバが現在実行中かにかかわらず、ユーザは SQL サービスに確実にアクセスできます。

9.1.5.2. リモートアクセスにリソース名を使用する

アプリケーションがクラスタに対応していない場合、**Microsoft SQL Enterprise Manager** を使用してサービスを管理するときは、切り替え可能なリソース名 (TCP/IP アドレスを使用してユーザがサーバにアクセスできる名前) によってサービスを登録する必要があります。これにより、この処理のバイアビリティを継続的に監視できます。

SQL Server をシステム名で登録すると、システムも監視できます。

9.1.5.3. ボリュームを SQL 専用にする

保護対象の SQL ファイルを含むボリュームは、SQL 専用にする必要があります。

SIOS Protection Suite の保護対象のボリュームにアプリケーション、プロセス、またはリモートユーザがアクセスすると、スイッチオーバに失敗する可能性があります。

9.1.5.4. SQL Server 環境での手動スイッチオーバの制限について

手動操作を実行する場合は、すべてのユーザが SQL Server リソースからログオフしている必要があります。

ボリュームに読み取り専用アクセスをしているローカルプロセスがあっても、サービスからリソースを削除できますが、スイッチバックしようとすると復元に失敗することがあります。例えば、パフォーマンスモニタは定期的に各ボリュームをポーリングし、共有ボリュームや複製ボリュームにインストールされた実行中のプロセスをチェックしています。この種の復元が失敗する可能性は、Microsoft SQL Server をローカルドライブにインストールして、データベースだけを共有ボリュームまたは複製ボリュームに置くことで、最小限に抑えることができます。

9.1.5.5. Microsoft SQL Management ツールの実行

Microsoft SQL Server Configuration Manager (SQL 2005) は、必要なときだけ実行してください。

Microsoft SQL Server Configuration Manager (SQL 2005) がオープンしていて、データベースレベルでアクティブな場合、SQL 階層が正しくサービス中の状態になるのが妨げられて、フェイルオーバが正常に完了しないことがあります。このような問題が発生した場合は、Microsoft SQL Server Configuration Manager (SQL 2005) を閉じて、SQL リソースを手動でサービス中にしてください。

9.1.5.6. SQL Server の起動と停止は SIOS Protection Suite 上で実行する

Microsoft SQL Server の管理の多くは Microsoft SQL Enterprise Manager を使用して行われますが、SIOS Protection Suite 管理オプションを使用して Microsoft SQL Server をサービス開始およびサービス停止にすることによって、2 つの明確なメリットが得られます。

1. **一貫した表示** 。SIOS Protection Suite が Microsoft SQL Server を停止して起動しても、設定内のすべてのノードについて、サーバの表示の一貫性が保たれます。

2. **詳細設定の保存** 。Microsoft SQL Server 設定を変更した場合、SIOS Protection Suite によってサーバを停止および開始するか、または手動でのスイッチオーバを行うことができます。ペアノード上での設定変更は SIOS Protection Suite によって自動的に複製されます。

   注記: これらのオプションを使用してペアサーバ上の新しい設定情報を複製しないと、フェイルオーバの状況では、バックアップサーバによって古い設定情報が使用されます。

3. **コントロールパネルの「サービス」** ツールで、**保護対象の Microsoft SQL サービス** の起動モードを **手動** に設定する必要があります。

9.1.5.7. Microsoft SQL Server ボリュームの追加

環境の規模が拡大するにつれて、新しい Microsoft SQL Server データベースを新しい共有ボリュームまたは複製ボリュームに追加することが必要になります。その場合は、Microsoft SQL Server 内で新しいデータベースを管理する前に、次の作業を実行して、新しいボリュームを SIOS Protection Suite 階層に追加する必要があります。

新しいボリュームリソースを既存の SQL Server 階層に追加するには、次の作業を実行します。

1. **リソースの作成** 。SQL Server 階層がサービス中のサーバ上で SQL 階層と優先順位が同じボリュームリソースを作成して拡張します。

2. **依存関係の作成** 。SQL Server リソースを右クリックし、ポップアップメニューの [依存関係の作成] をクリックします。**[子リソース]** タグで新しいボリュームリソースを選択します。

この SIOS Protection Suite 作業を完了すると、管理作業を実行して、SQL Server データベースを追加できます。すでにリソース階層の一部であるボリュームに新しいデータベースを追加する場合は、SIOS Protection Suite 固有の管理は必要ありません。

9.1.5.8. スイッチオーバ後にデータベースの「Suspect」状態から回復

データベースを格納したボリュームがシステムで利用できない場合、Microsoft SQL Server を起動すると、データベースが suspect 状態になることがあります。SIOS Protection Suite を使用して SQL データベースを保護しているときは、SQL の起動と停止は、階層をサービス中またはサービス停止にする機能としてだけ実行する必要があります。データベースが suspect 状態になり、データベースに問題がないことがわかっている状況では、次の手順を実行してこの問題を解決してください。

プライマリまたはセカンダリサーバで suspect となったデータベースの場合

1. データベースが格納されているボリュームがアクティブ (緑) で、このサーバによって保護されていることを確認します。

2. sp_resetstatus を使用してデータベースの状態を変更します。次のコマンドをクエリウィンドウで実行し、suspect 状態のデータベースをリセットしてください。

```
While in master database, execute sp_configure ‘allow updates’, 1

Reconfigure with override

Sp_resetstatus ‘dbname’

Sp_configure ‘allow updates’, 0

Reconfigure with override
```

3. Microsoft SQL Server を **停止** します。

4. Microsoft SQL Server を **開始** します。

9.1.5.9. Microsoft SQL Server (MSSQLServer) の一時停止

SQL 管理者は Microsoft SQL Server を手動で一時停止状態にできます。その場合、Microsoft SQL Server に対する既存の接続は処理を続行できますが、新しい接続は許可されません。この場合、SIOS Protection Suite は MSSQLServer サービスが実行中状態でないことを検出しますが、サービスをローカルで再起動したり、SQL 階層をバックアップサーバにフェイルオーバしたりすることはありません。どちらも適切な動作ではないため、Microsoft SQL Server が一時停止状態のときは、SQL リソースの監視は実質的に無効になります。

Microsoft SQL Server をこの状態にするには手動操作が必要であったため、SQL 管理者は SQL Server をこの状態から手動で変更する必要があります。一時停止状態でなくなると、SIOS Protection Suite は先に説明したように SQL リソースの監視を再開できます。

9.1.5.10. 切り替え可能な IP アドレスで接続するように SQL Server を設定

SQL がインストールされている場合は、初期設定で TCP/IP ソケットがデフォルトのネットワークプロトコルとして設定されます。この設定を変更する場合は、**SQL Server Configuration Manager** ツールを使用し　TCP/IP ネットワーク設定を再び有効にしてください。

9.1.5.11. SQL Server のログインおよびパスワードの管理

ユーザは SIOS Protection Suite SQL リソースを作成する際、Microsoft SQL Server のインスタンスにアクセスする SQL 管理ユーザ名とパスワードを入力する必要があります。管理ユーザ名とパスワードを変更した場合、SQL リソースは、クラスタ内のすべてのシステムで新しいパスワードを使用して更新する必要があります。新しいパスワードで更新しない場合は、これらのシステム上の SQL サーバに対して SIOS Protection Suite が十分な監視を行えなくなります。警告メッセージがアプリケーションイベントログに登録されますが、SQL リソースは障害とみなされません。

SIOS Protection Suite SQL リソースに関連付けた SQL 管理ユーザ名とパスワードは、LifeKeeper GUI の **[SQL Server 設定]** タブで変更できます。LifeKeeper GUI を使用して、保護対象の SQL Server リソースを管理するには、LifeKeeper GUI の右側のペインで SQL Server リソースを右クリックし、**[プロパティ]** 、**[SQL Server 設定]** タブの順にクリックします。**[管理操作]** をクリックし、**[SQL Server 設定]** ページの [ユーザの管理] をクリックして、SQL リソース情報を参照または変更します。

[SQL Server 設定] ページの詳細については、SQL Server の設定管理 を参照してください。

9.1.5.12. SQL 階層の監視

SIOS Protection Suite は、すべての SQL リソースに対しても、MS SQL Server サービス、および SQL 階層作成時とそれ以降に選択されたオプションサービスを監視します。いずれかのサービスが停止した場合、SQL リソースに関連付けられた監視プロセスがそれを検出して、ローカルリカバリが有効な場合は、ローカルサーバ上でサービスの再起動が試みられます。ローカルリカバリが無効に設定されている場合、リソースをバックアップサーバにフェイルオーバします。

SIOS Protection Suite は SQL クエリを発行して、保護対象の SQL データベースとの接続を確認します。SQL クエリがマスタデータベースとの接続に失敗すると、SQL リソースに関連付けられた監視プロセスは、問題を検出して、ローカルリカバリが有効に設定されていれば、サービスを再起動します。ローカルリカバリが無効に設定されている場合、リソースをバックアップサーバにフェイルオーバします。保護対象のデータベースを SQL 階層の作成後に追加した場合、エラーは **Application Event ログ** に記録されます。

9.1.6. トラブルシューティング

このセクションでは、SIOS Protection Suite ソフトウェアには特別な関係がない、全体的な環境に関連する現象についての解決案と考えられる原因を提示します。

マスタ、あるいはユーザデータベースがシステムドライブにある場合リソースの作成や拡張に失敗する

SQL リソースの拡張に失敗する

名前付きインスタンスで SQLAgent サービスを開始できない

SQL Server の名前付きインスタンスへの ODBC クライアントの接続

9.1.6.1. マスタ、あるいはユーザデータベースがシステムドライブにある場合リソースの作成や拡張に失敗する

現象

マスタデータベースやユーザデータベースが SIOS Protection Suite　で保護できないシステムドライブやボリュームに配置されている場合、Microsoft SQL Server リソースの **作成** および **拡張** に失敗します。SIOS Protection Suite は *tempdb* データベースを SIOS Protection Suite で保護されたボリュームに配置することを必須としておらず、このデータベースは SQL Server が起動されるたびに再構成されます。

推奨される処置

以下のサイトにマスタデータベースやユーザデータベースの保存先をボリュームへ移動させる方法が掲載されています。SIOS Protection Suite はそのボリュームを保護します。

support.microsoft.com/kb/224071/en-us

www.databasejournal.com/features/mssql/article.php/3379901

9.1.6.2. SQL リソースの拡張に失敗する

現象

プライマリサーバとバックアップサーバの設定が一致しない場合 (例: Microsoft SQL ID の不一致)、Microsoft SQL リソースの拡張は失敗します。拡張時に LifeKeeper GUI に表示されるエラーメッセージの例を次に示します。

```
Process: canextend.ksh(1292)

*ERROR* (No. 14003) The target value for Database file location does not
match the template value (target=- DQ:\SQLDEFAULT\MSSQL.1\MSSQL\DATA\
MASTER.MDF,template=DQ:\SQLDEFAULT\MSSQL.4\MSSQL\DATA\MASTER.MDF)

Process: canextend.ksh(1572)

*ERROR* (No. 14003) The target value for Temp DB location does not match
the template value (target=-EQ:\SQLDEFAULT\MSSQL.1\MSSQL\LOG\
ERRORLOG,template=-EQ:\SQLDEFAULT\MSSQL.4\MSSQL\LOG\ERRORLOG)

Process: canextend.ksh(1156)

*ERROR* (No. 14003) The target value for Log file location does not match
the template value (target=-LQ:\SQLDEFAULT\MSSQL.1\MSSQL\DATA\
MASTLOG.LDF,template=-LQ:\SQLDEFAULT\MSSQL.4\MSSQL\DATA\MASTLOG.LDF)

Error - extmgr (HAWK, MSSQL.0, MSSQL.0, OSPREY) - canextend failed
```

推奨される処置

ID Conflict Resolution オプションを使用して、プライマリサーバとバックアップサーバの Microsoft SQL ID が一致しないトラブルを解決してください。LifeKeeper GUI の右ペインに移動し、**[SQL Server リソース]** を右クリックしてください。続いて、**[プロパティ]** をクリックし、**[SQL Server 設定]** タブをクリックしてください。**[管理操作]** をクリックし、**[SQL Server 設定]** ページの **[ID Conflict Resolution]** を選択してください。

[SQL Server 設定] ページの詳細については、SQL Server の設定管理 を参照してください。

9.1.6.3. 名前付きインスタンスで SQLAgent サービスを開始できない

現象

SIOS Protection Suite が SQLAgent サービスを保護している Microsoft SQL Server の名前付きインスタンスでは、リソースが最初にサービス中になると、このサービスの起動を SQL 問題によって妨げられ、この SQL が SQLAgent サービス開始の試みを放棄するまでに MAXWAIT 状況 (300 秒の遅延) が強制されます。

このメッセージは、SQL リソースの INFO フィールドが壊れていることを示しています。SQL リソースを削除して再作成する必要があります。リソースを削除する前に、すべての IP およびボリュームの依存関係を削除する必要があります。依存関係は新しい SQL リソースを作成した時点で SIOS Protection Suite によって再作成されます。

SQLAgent サービスが開始しようとしているシステム上で Microsoft SQL Server サービスがすでに開始している場合は、このシナリオに遭遇することがあります。

SQL 階層の作成時に SQLAgent サービスと Microsoft SQL Server サービスが両方とも開始している場合は、この問題は発生しません。

推奨される処置

Microsoft SQL Server サービスの停止と開始を行うと、通常この問題は解決し、続いて SQLAgent サービスが開始されます。ただし、SQL Server サービスの停止は適切な選択とはいえません。

デフォルトのインスタンスまたは名前付きインスタンスで、MSSQLServer サービスおよび SQLServerAgent サービスはいずれも、ローカルシステムアカウントを使用して正しく起動する必要があります。各システム上でローカル管理者グループにドメイン管理者アカウントを追加した場合、この 2 つのサービスはともにドメイン管理者アカウントを使用して起動します。

9.1.6.4. SQL Server の名前付きインスタンスへの ODBC クライアントの接続

現象

保護された IP アドレスを介して SIOS Protection Suite クラスタに ODBC 接続を作成した後で、SQL リソースをバックアップサーバに切り替えると、接続に失敗します。

推奨される処置

1. プライマリ上で各インスタンスをサービス休止中にしてから、In Service 状態に戻します。アプリケーションイベントログを調べて、その特定の SQL Server のインスタンスがどの IP:PORT で listen しているのか確認します。

2. セカンダリサーバで各階層の In Service を行い、各 SQL のインスタンスが listen している IP:PORT を記録します。

3. クライアントが ODBC を介していずれかのサーバに接続可能であることを確実にするには、各インスタンスが listen しているポートがプライマリサーバおよびセカンダリサーバのいずれでも同一であることを確認します。

4. この確認を行うには、Microsoft SQL Server ネットワークユーティリティを使用します。SQL インスタンスを選択し (当該マシン上で動作している必要があります)、TCP/IP プロトコルを強調表示し、プロパティを確認して SQL インスタンスが listen しているデフォルトのポートを特定します。

5. このインスタンスについてデフォルトのポートが両方のシステムで同一になるようにこの値を変更します。

6. 手順 5 で設定した、保護された IP:PORT を使用して、各インスタンスの ODBC 接続を作成します。

9.2. はじめに SIOS Protection Suite PostgreSQL サーバー

SIOS Protection Suite PostgreSQL サーバー

SIOS Protection Suite PostgreSQL Server Recovery Kit を使用すると、PostgreSQL ベースのデータベースのデータの整合性を、SIOS Protection Suite for Windows が提供する高い可用性と統合することができます。

LifeKeeper GUI を使用すると、PostgreSQL のリソース階層を簡単に作成できます。SIOS Protection Suite は、クライアントがデータベースへのアクセスに使用する LifeKeeper ネットワークリソースに加えて、PostgreSQL サーバーインスタンスが使用するすべてのディスクリソースを保護することができます。

9.2.1. PostgreSQL サーバーのインストール

SIOS Protection Suite PostgreSQL Server Recovery Kit を正しく操作できるかどうかは、ハードウェアとソフトウェアが正しく設定されているかどうかによって決まります。

先に進む前に、このガイドの 階層の管理 セクションを事前に確認してください。このセクションには、SIOS Protection Suite 環境での PostgreSQL サーバーの管理に役立つ一般的なガイドライン、設定の詳細およびトラブルシューティングのヒントを記載しています。

9.2.1.1. インストールと設定の詳細 – 既存の PostgreSQL の構成に LifeKeeper を追加する

このセクションでは、LifeKeeper を既存のPostgreSQLの構成に追加する際の SIOS Protection Suite および PostgreSQL ソフトウェアのインストールと設定について説明します。プライマリーサーバーは、保護対象のアクティブな PostgreSQL データベースクラスターの場所にあると想定します。これらのステップでは、保護対象のデータベースクラスターが PostgreSQL のデフォルトインストールで作成されたバージョンであることを前提としています（例：PostgreSQL v9.6 の postgresql-x64-9.6 など）。以下のステップは、記載されている順序で実施してください。

1. プライマリーサーバーおよびバックアップサーバーにSIOS Protection Suiteソフトウェアをインストールします。

2. プライマリーサーバーで LifeKeeper GUI を使用して、プライマリーサーバーとバックアップサーバーの間にコミュニケーションパスを作成します。

3. プライマリーサーバーで、以下の作業を実施します。

    a. **Disk Management** ユーティリティを使用してディスクリソースを構成し、使用する共有ボリュームまたは複製ボリュームを定義します。ボリュームのサイズが適切であることを確認してください。共有ボリュームを構成する場合は、構成中にバックアップサーバーの電源を切り、ストレージに同時にアクセスしないようにします。

    b. **Windows エクスプローラー** を使用して、ネットワークから PostgreSQL サーバーインスタンスが使用するすべてのボリュームの共有を解除することを推奨します。

    c. 必要な場合は、SIOS Protection Suite の TCP/IP コミュニケーションパスと切り替え可能な IP アドレスをサポートするようにネットワークを設定します。

4. バックアップサーバーで、以下の作業を実施します。

    a. ステップ3で、共用ボリュームを構成するためにバックアップサーバーを停止した場合は起動します。

    b. **Disk Management** ユーティリティを使用してディスクリソースを構成し、使用する共有ボリュームまたは複製ボリュームを定義します。共有ストレージを使用している場合は、プライマリーサーバーに割り当てられているものと同じドライブ文字を共有ボリュームに割り当てます。複製されたストレージの場合、ボリュームサイズが適切であることを確認してください。

5. プライマリーサーバーで、以下の作業を実施します。

    a. SIOS Protection Suite で、共有ボリュームリソースまたは複製されたボリュームリソース（PostgreSQL データベースクラスターが存在するボリュームリソース）を作成し、バックアップサーバーに拡張します。後で PostgreSQL サーバーリソース階層を作成すると、SIOS Protection Suite は自動的にリソースを依存関係として階層に追加します。

6. バックアップサーバーで、以下の作業を実施します。

    a. **LifeKeeper GUI** を使用して、ボリュームリソース階層を In Service にします。

    b. 以下のガイドラインに従って、プライマリーサーバーにインストールされているものと同じプログラムフォルダに PostgreSQL をインストールします。

        i. PostgreSQL インストーラーへの引数 —extract-only は、PostgreSQL Recovery Kit に必要なすべての情報を設定しないため、この引数の使用は推奨しません。

        ii. デフォルトでは、PostgreSQL ソフトウェアをインストールすると、単一のデータベースクラスターが作成されます（データベースクラスターは、実行中の PostgreSQL データベースサーバーの単一のインスタンスが管理するデータベースの集合です）。インストール時に、データベースディレクトリのプロンプトがデータベースクラスターの作成場所を決定します。デフォルトインスタンスはステップ 6d で削除されるので、任意の場所にインストールできます。

    c. インストール時に作成されるデフォルトのデータベースクラスターインスタンスは不要なので、削除できます。

        i. インストール中に作成されたデータベースクラスターインスタンスを停止します。

        ii. **エクスプローラー** を開き、複製されたボリュームに関連付けられたドライブにアクセスします。

        iii. インストール中に作成された PostgreSQL データベースクラスターディレクトリを削除します。

        iv. インストール時に作成された PostgreSQL サービスを削除します。削除するには、Windows の “sc delete <servicename>” コマンドを使用します。

7. プライマリーサーバーで、以下の作業を実施します。

    a. **LifeKeeper GUI** を使用して、ボリュームリソース階層を In Service にします。

    b. PostgreSQL Recovery Kit で保護される PostgreSQL データベースクラスターインスタンスを停止します。

    c. **オプション** - 上記で作成した保護対象のボリュームに移動する前に、PostgreSQL データベースクラスターのデータディレクトリのバックアップを実行します。

    d. データベースクラスターのデータディレクトリを、上記で作成した保護対象のボリュームに移動します。

    e. データベースクラスターのデータディレクトリへのアクセス権を設定します。このインスタンスに対する Windows Service を制御するために作成したユーザーアカウントには、データディレクトリ上のファイルへのフルコントロールのアクセス許可が必要です。

    f. プライマリーサーバーで、Postmaster のポート引数設定 に記載されている手順を実施します。設定には、データディレクトリの場所を指定する -D 引数の変更も含める必要があります。これは、保護対象のボリューム上のパスに変更します。

g.プライマリーサーバーで、自動接続設定 で説明しているステップを実施します。

h.インストールと設定が完了したら、Windows PostgreSQL サービスを起動して、Postmaster のポート引数および保護対象のボリューム上にあるデータディレクトリと共に、PostgreSQL サーバーがプライマリーサーバー上で正しく起動することを確認してください。

i.プライマリーサーバー上に PostgreSQL サーバー階層を作成し、それをバックアップサーバーに拡張します。詳細については、PostgreSQL 階層の作成 を参照してください。また、手動のスイッチオーバーを実行して新しい PostgreSQL サーバー階層をテストしてください。

9.2.1.2. インストールと設定 – 既存の LifeKeeper 構成に PostgreSQL を追加する

このセクションでは、PostgreSQL を既存の LifeKeeper クラスターに追加する際の SIOS Protection Suite および PostgreSQL ソフトウェアのインストールと設定について説明します。このステップは、ここに記載している順番で実施する必要があります。

1. プライマリーサーバーで、以下の作業を実施します。

    a. **Windows Disk Management** ツールを使用してディスクリソースを構成し、使用する共有ボリュームまたは複製ボリュームを定義します。ボリュームのサイズが適切であることを確認してください。共有ボリュームを構成する場合は、構成中にバックアップサーバーの電源を切り、ストレージに同時にアクセスしないようにします。

    b. **Windows エクスプローラー** を使用して、ネットワークから PostgreSQL サーバーインスタンスが使用するすべてのボリュームの共有を解除することを推奨します。

    c. 必要な場合は、SIOS Protection Suite の TCP/IP コミュニケーションパスと切り替え可能な IP アドレスをサポートするようにネットワークを設定します。

2. バックアップサーバーで、以下の作業を実施します。

    a. ステップ1 で、共用ボリュームを構成するためにバックアップサーバーを停止した場合は起動します。

    b. **Disk Management** ユーティリティを使用してディスクリソースを構成し、使用する共有ボリュームまたは複製ボリュームを定義します。共有ストレージを使用している場合は、プライマリーサーバーに割り当てられているものと同じドライブ文字を共有ボリュームに割り当てます。複製されたストレージの場合、ボリュームサイズが適切であることを確認してください。

3. プライマリーサーバーで、以下の作業を実施します。

    a. SIOS Protection Suite で、共有ボリュームリソースまたは複製されたボリュームリソース（PostgreSQL データベースクラスターが存在するボリュームリソース）を作成し、バックアップサーバーに拡張します。後で PostgreSQL サーバーリソース階層を作成すると、SIOS Protection Suite は自動的にリソースを依存関係として階層に追加します。

4. バックアップサーバーで、以下の作業を実施します。

    a. **LifeKeeper GUI** を使用して、ボリュームリソース階層を In Service にします。

    b. 以下のガイドラインに従って、PostgreSQL サーバーソフトウェアをインストールしてください。

        i. PostgreSQL インストーラーへの引数 —extract-only は、PostgreSQL Recovery Kit に必要なすべての情報を設定しないため、この引数の使用は推奨しません。

        ii. デフォルトでは、PostgreSQL ソフトウェアをインストールすると、単一のデータベースクラスター

が作成されます（データベースクラスターは、実行中の PostgreSQL データベースサーバーの単一のインスタンスが管理するデータベースの集合です）。インストール時に、データベースディレクトリのプロンプトがデータベースクラスターの作成場所を決定します。デフォルトインスタンスはステップ6dで削除されるので、任意の場所にインストールできます。指定した場所は、ステップ3a で作成した保護対象のボリューム上である必要があります。

iii. インストール中に作成されたデータベースサービスは、SIOS Protection Suite PostgreSQL Server Recovery Kit がインスタンスを適切に管理するために必要なポート引数（-p port）で始まるように postmaster プロセスを設定しません。デフォルトのデータベースクラスター用に作成された Windows サービス（例：PostgreSQL v9.6 の postgresql-x64-9.6）を SIOS Protection Suite で保護する場合は、このオプションを含めるように変更する必要があります。詳細については、Postmaster のポート引数設定 を参照してください。

c. pgpass.conf を認証に使用する場合は、自動接続設定 に記載されている手順に従ってください（pg_hba.conf ファイルを使用して信頼関係を設定する場合は、プライマリーサーバーの設定の一部として実施されるため、この手順をスキップできます）。

d. （Postmaster のポート引数と自動接続に対する）インストールと設定が完了したら、Windows PostgreSQL データベースクラスターが起動することを確認します。確認するためには、PostgreSQL 用のデフォルトの Windows サービスを停止して再起動する必要があります。検証が完了したら、PostgreSQL サービスを停止します。

5. プライマリーサーバーで、以下の作業を実施します。

a. **LifeKeeper GUI** を使用して、ボリュームリソース階層を In Service にします。

b. **エクスプローラー** を開き、複製されたボリュームに関連付けられたドライブにアクセスします。

c. バックアップサーバーでのインストール中に作成された PostgreSQL データベースクラスターディレクトリを削除します。（これは次のステップで再作成します。）

d. バックアップサーバーで実施したのと同じように、PostgreSQL サーバーソフトウェアを正確にインストールしてください（ローカルディスク上の同じディレクトリにあるプログラムファイルと、保護対象のボリューム上の同じ場所にあるデータファイル）。

e. プライマリーサーバーで、Postmaster のポート引数設定 に記載されているステップを実施します。

f. プライマリーサーバーで、自動接続設定 に記載されているステップを実施します。

g. インストールが完了したら、Windows PostgreSQL サービスを開始して、PostgreSQL サーバーがプライマリーサーバー上で正常に起動できることを確認します。

h. プライマリーサーバー上に PostgreSQL サーバー階層を作成し、それをバックアップサーバーに拡張します。詳細については、PostgreSQL 階層の作成 を参照してください。手動のフェールオーバーを実行して、新しい PostgreSQL サーバー階層をテストしてください。

9.2.1.3. 拡張設定のための追加のセットアップ作業

共有ストレージデバイスを使用する構成の場合、または SIOS DataKeeper を使用している場合は、3台目（またはそれ以上）のサーバーに拡張する構成を選択できます。

1. まだ実施していない場合は、SIOS Protection Suite を使用した PostgreSQL サーバーのインストールと設定 の手順に従って、2つのシステムを設定します。

2. **Disk Management** ユーティリティを使用してディスクリソースを構成し、使用する共有ボリュームまたは複製ボリュームを定義します。共有ストレージを使用している場合は、プライマリーサーバーに割り当てられているものと同じドライブ文字を共有ボリュームに割り当てます。複製されたストレージの場合、ボリュームサイズが適切であることを確認してください。

3. プライマリーサーバーで実行したのと同じように（ローカルディスクの同じディレクトリにあるプログラムファイルと保護対象のボリューム上の同じ場所にあるデータファイル）、PostgreSQL サーバーソフトウェアを以下のガイドラインに従ってインストールします。

    a. PostgreSQL インストーラーへの引数 —extract-only は、PostgreSQL Recovery Kit に必要なすべての情報を設定しないため、この引数の使用は推奨しません。

    b. デフォルトでは、PostgreSQLソフトウェアをインストールすると単一のデータベースクラスターが作成されます（データベースクラスターは、実行中の PostgreSQL データベースサーバーの単一のインスタンスが管理するデータベースの集合です）。インストール時に、データベースディレクトリのプロンプトでデータベースクラスターの作成場所を決定します。デフォルトインスタンスは後のステップで削除されるので、任意の場所を選択してください。複製したストレージを使用している場合は、ステップ2 で作成したボリュームにすることができます。共有ストレージを使用している場合は、現在の PostgreSQL データベースクラスターを上書きしないように、上記のボリュームは使用しないでください。

    c. インストール中に作成されたデータベースサービスは、SIOS Protection Suite PostgreSQL Server Recovery Kit によるインスタンスの適切な管理に必要なポート引数（ -p port ）で始まるようには postmaster プロセスを設定しません。デフォルトのデータベースクラスター用に作成された Windows サービス（例: PostgreSQL v9.6 の postgresql-x64-9.6）は、SIOS Protection Suite によって保護される場合は、このオプションを含めるように更新する必要があります。詳細については、Postmaster のポート引数設定 を参照してください。Postmaster のポート引数を更新する際に、プライマリーサーバー上のインストール場所に合わせてデータディレクトリパス（-D 引数値）を更新する必要があります。

4. pgpass.conf を認証に使用する場合は、自動接続設定 に記載されている手順に従います（pg_hba.conf ファイルを使用して信頼関係を設定する場合は、プライマリーサーバー上の設定の一部として既に実施しているので、この手順は省略できます）。

5. インストール中に作成されるデフォルトのデータベースクラスターインスタンスは不要なので、削除できます。

    a. インストール中に作成されたデータベースクラスターインスタンスを停止します。

b. **エクスプローラー** を開き、PostgreSQL ソフトウェアのインストール中に入力したデータディレクトリの場所に移動します。

c. PostgreSQL データベースクラスターディレクトリを削除します。

d. インストール時に作成された PostgreSQL サービスを削除します。これを行うには、Windows の “sc delete <servicename>” コマンドを使用します。

6. LifeKeeper の新しいクラスターノードにコミュニケーションパスがない場合は、プライマリーサーバー上で LifeKeeper GUI を使用して、プライマリークラスターと新しい LifeKeeper クラスターノード間、バックアップサーバーと新しい LifeKeeper クラスターノード間にコミュニケーションパスを作成します。

7. PostgreSQL 階層を新しい LifeKeeper クラスターノードに拡張します。詳細については、PostgreSQL 階層の作成 を参照してください。その後、新しい LifeKeeper クラスターノードへの手動スイッチオーバーを実行して、新しい PostgreSQL サーバー階層をテストしてください。

9.2.2. PostgreSQL サーバーの設定に関する考慮事項

PostgreSQL データベースクラスターをインストールして設定する前に、設定する方法を理解しておくことが重要です。また、アクティブ/スタンバイとアクティブ/アクティブ構成の概念、およびそれらを PostgreSQL 構成で設定する方法を理解することも重要です。

PostgreSQL データベースクラスターの設定に関する考慮事項

SIOS Protection Suite for PostgreSQL は、PostgreSQL データベースクラスターの管理に Windows サービスを使用します。PostgreSQL データベースクラスター用の Windows サービスがない場合は、PostgreSQL 階層の作成時にセットアップされます。

SIOS Protection SuiteでPostgreSQL データベースクラスターを保護するには、次の条件が必要です。

- PostgreSQL サーバーが稼働している
- PostgreSQL の postmaster プロセスを、port オプション -p port を指定して実行している
- PostgreSQL データベースのクラスターデータディレクトリは、保護対象のボリューム上に存在する
- PostgreSQL データベースのクラスターデータディレクトリ、サブディレクトリ、およびすべてのファイルは、すべてのサーバー上の Windows サービスアカウントからアクセス可能である

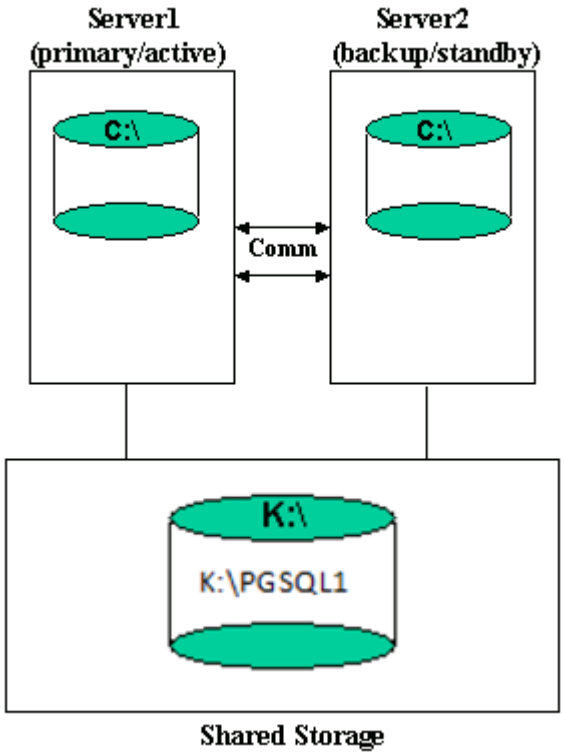
現在、この Recovery Kit には次の構成上の制限事項があります。

- IP リソースインスタンスを階層の一部として自動的に追加しません。ユーザーがリモートで接続する場合は、IP リソースを作成し、PostgreSQL 階層に子リソースとして追加する必要があります。
- どのボリュームリソースをリソース階層の一部として含める必要があるかを判断するときは、データベースクラスターのデータディレクトリの場所のみを考慮に入れてください。データベーステーブルスペースがデータディレクトリと同じ保護ボリューム上にない場合は、テーブルスペースを含むボリュームを保護し、PostgreSQL 階層内の子リソースとして追加する必要があります。

PostgreSQL のアクティブ/スタンバイ構成

共有ボリュームまたは複製されたボリューム上に PostgreSQL データベースクラスターが1つしかない場合、構成はアクティブ/スタンバイになります。PostgreSQL データベースのクラスターサービスは、一度に1つのシステム上でのみ実行されます。サーバーには、特定の階層のフェールオーバーの順序を決定する SIOS Protection Suite 内の優先順位が割り当てられます。

以下の図は、1つの PostgreSQL インスタンスが 1組のサーバーにインストールされている様子を示しています。このインスタンスには、1つのボリューム上に存在する1つのデータベースクラスター PGSQL1 が含まれています。



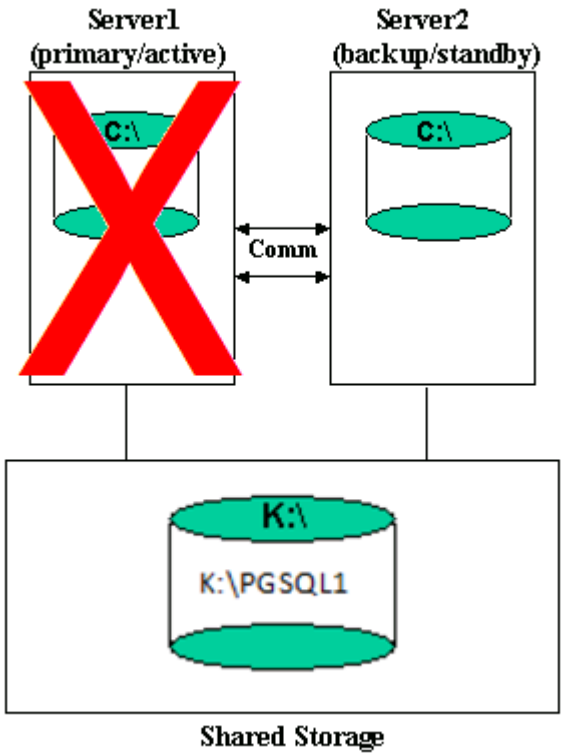
SIOS Protection Suite 内で PostgreSQL 階層を作成する場合は、PostgreSQL のデータディレクトリ（データベースクラスターの場所）を指定するように求められます。データベースクラスターへのリモート接続を行う場合、保護された IP リソースを設定し、リソース階層に追加する必要があります。その後、SIOS Protection Suite はそのインスタンスの構成データを読み取り、関連付けられたボリュームを階層にプルします。

階層が作成されると、LifeKeeper GUI に次のように表示されます。



アクティブ/スタンバイフェールオーバー

障害が発生した場合、SIOS Protection Suiteは、PostgreSQL サーバーの階層をバックアップサーバーで In Service にします。PostgreSQL サーバーはバックアップサーバーで起動され、以下の図に示すように、データベースクラスターの保護を引き継ぎます。

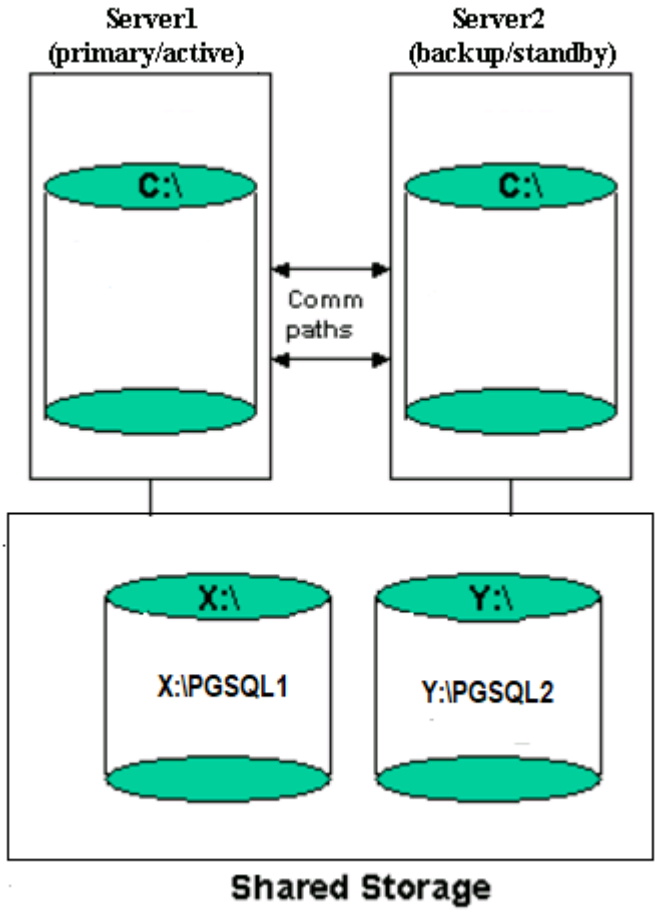


PostgreSQL のアクティブ/アクティブ構成

initdb を使用して、複数の PostgreSQL サーバーのデータベースクラスターを任意のサーバー上で設定できます。SIOS Protection Suite は、アクティブ/アクティブ構成と呼ばれる複数の PostgreSQL データベースクラスターを保護することができます。SIOS Protection Suite は、接続に使用されるポートによって各インスタンスを識別します。

各データベースクラスターは、単一の SIOS Protection Suite 階層で保護されています。

以下の図は、2つの PostgreSQL データベースクラスター、PGSQL1 と PGSQL2 を示しています。



注記:

- この構成では、Server1 が PGSQL1 データベースクラスターのプライマリーサーバー、Server2 が PGSQL2 データベースクラスターのプライマリーサーバーです。
- 各サーバーは、複数のインスタンスのプライマリーサーバーおよびバックアップサーバーとなることができます。
- Server1 または Server2 が両方のデータベースクラスターのプライマリーサーバーになる可能性があります。

9.2.2.1. PostgreSQL 階層の作成

SIOS Protection Suite for Windows インストールガイド に記載されている必要な設定作業を完了したら、以下の手順に従ってデータベースクラスターを保護する PostgreSQL サーバー階層を作成します。

重要	既存の PosgreSQL データベースクラスターがインストールされている場合は、この手順を実行する前に、PostgreSQL データベースクラスターにアクセスしているクライアントアプリケーション（ローカルまたはリモート）を閉じる必要があります。また、次のいずれかの条件が存在する場合も、すべてのクライアント接続を閉じる必要があります。 • PostgreSQL データベースクラスターのデータディレクトリが保護対象のボリューム上にない場合。高い可用性を実現するには、PostgreSQL のデータディレクトリが、LifeKeeper クラスター内のノード間で切り替え可能な保護対象のボリューム上に存在する必要があります。これには、リソース階層を作成する前に手動でデータディレクトリを移動する必要があります。移動が完了したら、PostgreSQL データベースクラスターサービスを再起動します。 • 既存の Windows サービスは、PostgreSQL Server インスタンスを制御しません。保護された PostgreSQL サーバーの管理を容易にするために、Windows サービスが存在しない場合は階層の作成によって Windows サービスが作成されます。これには、PostgreSQL データベースのクラスターサービスの停止と再起動が必要です。 • postmaster プロセスが “-p port” オプションで実行されていない場合。postmaster のポート引数を指定して PostgreSQL の確認と起動を実行する方法の詳細については、Postmaster のポート引数設定 を参照してください。

1. LifeKeeper GUI **[Edit]** > **[Server]** を選択します。次にメニューから、**[Create Resource Hierarchy]** を選択します。

2. **[Create Protected Application]** ダイアログボックスが表示されます。プルダウンリストから **プライマリーサーバー** と **バックアップサーバー** を選択します。**[Next]** を選択して続行します。

3. ダイアログボックスが表示され、クラスター内にインストールされ、認識されている Recovery Kit がすべてドロップダウンリストボックスに表示されます。**[PostgreSQL Server]** を選択し、**[Next]** をクリックします。

4. 以下の情報の入力を求められます。いずれかのダイアログボックスで **[Back]** ボタンが有効になっている場合は前のダイアログボックスに戻ることができるので、前に入力した情報を修正する必要があるエラーが発生した場合に戻ることができます。また、いつでも **[Cancel]** をクリックして、作成プロセス全体をキャンセルすることができます。

フィールド	ヒント
PostgreSQL Service Name	このインスタンスのWindowsサービス名を入力してください。 入力した名前が既存のPostgreSQLサービスである場合、PostgreSQLリカバリーキットはサービ

	ス情報を使用してリソース作成のための情報を取得します。 入力された名前が既存のPostgreSQLサービスではない場合、作成プロセスでは、入力された名前を使用してWindowsサービスを作成するために追加の入力が必要になります。 **注記:** PostgreSQL リソースの作成中に Windows サービスが作成された場合、PostgreSQL リソースを削除すると PostgreSQL サービスは削除されます。PostgreSQL サービスが作成時に既に存在する場合は、PostgreSQL リソースを削除しても、サービスは削除されません。
PostgreSQL Executable Location	PostgreSQL の実行ファイル（pg_ctl.exe とpsql.exe が存在するディレクトリ）の場所を選択します。システムに複数のバージョンの PostgreSQL がインストールされている場合、選択されたパスは、保護対象のデータベースクラスターを作成するために使用した PostgreSQL のバージョンと一致する必要があります。 例: バージョン10 の intidb を使用してデータベースクラスターを作成した場合、pg_ctl.exe と psql.exe に対して選択されたパスはバージョン10 のパスでなければなりません。
PostgreSQL Data Directory	保護対象の PostgreSQL データベースクラスターのデータディレクトリへのパスを入力します。入力した PostgreSQL サービス名が存在する場合、そのサービスで定義されているデータディレクトリがデフォルト値になります。
PostgreSQL Port	PostgreSQL データベースクラスターで使用するポートを選択します。このフィールドは、postmaster デーモンがクライアントアプリケーションからの接続を Listen する TCP/IP ポート番号を指定するために使用されます。デフォルトの選択は実行中の PostgreSQL サーバーから取得されます。
Enter Database Administrator User	PostgreSQLデータベースクラスターの管理ユーザーの名前を入力します。このユーザーには、接続権限と管理権限が必要です。
PostgreSQL Database Tag	固有のタグ名を入力します。自動で表示されるデフォルトのタグ名をそのまま使用することもできます。 **注意：**タグ名に使用できる文字はASCII印字可能文字のみです。
以下のフィールドは、入力した PostgreSQL サービス名が Windows サービスとして存在しない場合にのみ表示されます	
PostgreSQL Service Logon Account	新しい PostgreSQL Windows サービスのログオン資格情報に使用するユーザーアカウントを入力します。このアカウントには、保護対象の PostgreSQL サーバーインスタンスを起動および停止する権限が必要です。このユーザーアカウントには、PostgreSQL データディレクトリ内のすべてのファイルに対するフルコントロールのファイルアクセス権も必要です。
PostgreSQL Service Logon Password	新しい PostgreSQL Windows サービスのログオン資格情報で使用するユーザーパスワードを入力します。 **注記:** ビルトインのシステムアカウント（「Local System」や「Network Service」など）を使用する場合は、このフィールドに空白以外の値を入力します（空白にはできません）。ビルトインアカウントの場合、パスワードは無視されます。

5. **[Create]** をクリックすると、**ウィザード** によって PostgreSQL リソースが作成されます。SIOS Protection

Suite は、入力されたデータを検証します。SIOS Protection Suite が問題を検出すると、情報ボックスにエラーメッセージが表示されます。

6. PostgreSQL リソース階層を正常に作成したことを示す別の情報ボックスが表示されます。フェールオーバー保護を実施するためには、その階層をクラスター内の別のサーバーに拡張する必要があります。**[Next]** をクリックします。

7. **[Next]** をクリックすると、SIOS Protection Suite が **Pre-Extend Wizard** を起動します。

9.2.2.2. PostgreSQL 階層の拡張

この操作は、**[Edit]** メニューから開始することも、**[Create Resource Hierarchy]** オプションの完了時に自動的に開始することもできます。その場合は、以下の手順2を参照してください。

1. **[Edit]** メニューから **[Resource]** を選択し、**[Extend Resource Hierarchy]** を選択します。Pre-Extend Wizard が表示されます。拡張操作に精通していない場合は、**[Next]** をクリックします。

2. Pre-Extend Wizard では、次の情報を入力するよう求められます。
   注記：これらの最初の 2つのフィールドは、**[Edit]** メニューから **[Extend]** を開始した場合にのみ表示されます。

フィールド	ヒント
Primary Server	拡張するリソース階層を現在定義し、使用しているサーバーを選択します。
Resource Hierarchy to Extend	拡張するリソース階層を選択します。
Backup Server	リソース階層のバックアップサーバーとなるサーバーを選択します。

3. 事前の拡張チェックが成功したというメッセージを受信したら、**[Next]** をクリックします。

4. 拡張ウィザードでは、以下の情報を入力するよう求められます。注記：最初の2つのフィールドは、PostgreSQL サーバー用の Windows サービスがバックアップサーバーに存在しない場合にのみ表示されます（作成時にプライマリーサーバーに入力されたサービス名がバックアップサーバーのチェックに使用されます）。

フィールド	ヒント
PostgreSQL Service Logon Account	バックアップサーバー上の PostgreSQL Windows サービスのログオン資格情報に使用するユーザーアカウントを入力します。このアカウントには、保護対象の PostgreSQL サーバーインスタンスを起動および停止する権限が必要です。
PostgreSQL Service Logon Password	新しい PostgreSQL Windows サービスのログオン資格情報に使用するユーザーパスワードを入力します。
PostgreSQL Executable Location	PostgreSQL の実行ファイル（pg_ctl.exe と psql.exe が存在するディレクトリ）の場所を選択します。システムに複数のバージョンの PostgreSQL がインストールされている場合、選択されたパスは、保護対象のデータベースクラスターを作成するために使用したPostgreSQL のバージョンと一致する必要があります。 例：バージョン10 の intidb を使用してデータベースクラスターを作成した場合、pg_ctl.exe と psql.exe に対して選択されたパスはバージョン10 のパスでなければなりません。
Backup Priority	1～999 の数値を入力して、このリソースのカスケードフェールオーバーシーケンスでのテンプレートサーバーの優先順位を指定します。数値が小さいほど優先度が高くなります。SIOS Protection Suite では、階層が作成されたサーバーに番号 "1"が割り当てられます。特定のリソースに対して2つのサーバーが同じ優先度を持つことはできません。

5. **[Extend]** をクリックします。

9.2.2.3. PostgreSQL 階層の拡張解除

SIOS Protection Suite クラスター内の単一サーバーからリソース階層を削除するには、次の手順を実行してください。

1. **[Edit]** メニューで、**[Resource]** > **[Unextend Resource Hierarchy]** の順に選択します。

2. SQL リソースの拡張を解除するターゲットサーバーを選択します。PostgreSQL リソースが現在稼動しているサーバーにすることはできません。(このダイアログボックスは、右ペインのリソースインスタンスを右クリックして **[Unextend]** タスクを選択した場合は表示されません。) **[Next]** をクリックします。

3. 拡張を解除する PostgreSQL 階層を選択し、**[Next]** をクリックします。(いずれかのペインでリソースインスタンスを右クリックして **[Unextend]** タスクを選択した場合、このダイアログは表示されません)。

4. 拡張の解除を選択したターゲットサーバーと SQL リソース階層を確認する情報ボックスが表示されます。**[Unextend]** をクリックします。

5. PostgreSQL リソースの拡張解除が正常に実行されたことを確認する別の情報ボックスが表示されます。**[Unextend Resource Hierarchy]** メニューを終了するには、**[Done]** をクリックします。

9.2.2.4. PostgreSQL 階層の削除

PostgreSQLの 階層またはインスタンスを削除する前に、プライマリーサーバーで階層がアクティブ（緑色）になっていることを確認してください。階層を削除する前に依存関係を削除することもできますが、階層の削除後は依存関係も削除されます。

SIOS Protection Suite 環境のすべてのサーバーからリソース階層を削除するには、次の手順を実行してください。

1. **[Edit]** メニューで 、**[Resource]** > **[Delete Resource Hierarchy]** の順に選択します。

2. PostgreSQL リソース階層を削除する **ターゲットサーバー** を選択し、**[Next]** をクリックします。（このダイアログは、いずれかのペインでリソースインスタンスを右クリックして **[Delete Resource]** タスクを選択した場合は表示されません。）

3. **削除する階層** を選択します。（このダイアログは、左側または右側のペインでリソースインスタンスを右クリックして **[Delete Resource]** タスクを選択した場合は表示されません。）**[Next]** をクリックします。

4. 削除するように選択したターゲットサーバーと階層の選択を確認する情報ボックスが表示されます。**[Delete]** をクリックします。

5. PostgreSQL リソースが正常に削除されたことを確認する情報ボックスが表示されます。

6. **[Done]** をクリックして終了します。

9.2.2.5. PostgreSQL リソース階層のテスト

手動スイッチオーバーを開始することにより、PostgreSQL リソース階層をテストできます。このテストでは、プライマリーサーバーからバックアップサーバーへのリソースインスタンスのフェールオーバーをシミュレートします。

[Edit] → **[Resource]** → **[In Service]** を選択します。たとえば、バックアップサーバー上で実行される In Service 要求によって、アプリケーション階層がプライマリーサーバー上のサービスで停止され、バックアップサーバー上のサービスに配置されます。この時点で、元のバックアップサーバーがプライマリーサーバーになり、元のプライマリーサーバーがバックアップサーバーになります。

Out of Service 要求を実行すると、アプリケーションは他のサーバー上でサービスを開始せずにサービス停止状態になります。

9.2.3. PostgreSQL サーバー階層の管理

PostgreSQL サーバーを管理する際は、以下のガイドラインに従ってください。

保護されたコミュニケーションパス経由でのアクセス

PostgreSQL を排他的に使用するためのボリュームの予約

SIOS Protection Suite 経由のみでの PostgreSQL サーバーの起動と停止

追加の PostgreSQL データベースクラスターの作成と保護

PostgreSQL 管理ログイン

自動接続設定

Postmaster のポート引数設定

PostgreSQL 階層の監視

9.2.3.1. 保護されたコミュニケーションパス経由でのアクセス

サービスのリモートアクセスはすべて、階層の LifeKeeper ネットワークリソース経由で実行する必要があります。これにより、現在実行中のサーバーがどのサーバーであっても、ユーザーは PostgreSQL データベースクラスターにアクセスできるようになります。

注記: 現時点では、PostgreSQL Recovery Kit では、IP 通信リソースを階層内の依存リソースとして自動的には含んでいません。どのサーバーで現在 PostgreSQL データベースクラスターを実行していてもリモートアクセスを保証するためには、IP リソースを作成し、PostgreSQL リソースの子リソースとして追加する必要があります。さらに、このアドレスで Listen するように PostgreSQL データベースクラスターを設定する必要があります。

9.2.3.2. PostgreSQL を排他的に使用するためのボリュームの予約

保護された PostgreSQL ファイルを含むボリュームは、PostgreSQL が排他的に使用するために予約する必要があります。

SIOS Protection Suite で保護対象のボリュームは、別のアプリケーション、プロセスまたはリモートユーザーによってアクセスされた場合、スイッチオーバーに失敗することがあります。

9.2.3.3. SIOS Protection Suite 経由のみでの PostgreSQL サーバーの起動と停止

PostgreSQL サーバーの管理タスクの多く はPostgreSQL ツールを使用して実施しますが、PostgreSQL サーバーの起動と停止は PostgreSQL ツールではなく、以下の方法で実施してください。

1. **一貫した状態** - SIOS Protection SuiteがPostgreSQL サーバーの停止と起動を実行すると、保護された Microsoft サービスの一貫した状態を維持します。pg_ctl.exe などの PostgreSQL ツールを使用してコマンドラインから開始および停止要求を実行すると、実行中の状態または停止している状態を検出できないため、Microsoft サービスの状態が矛盾します。その結果、PostgreSQL サーバーの問題の検出と修正ができなくなります。

2. **保護対象の PostgreSQL サービス** は、**コントロールパネル** の「**サービス**」ツールを使用して、**手動** のスタートアップモードに設定する必要があります。**注記:** PostgreSQL のリソース階層を作成する場合、保護されたサービスは自動的に **手動** のスタートアップモードに設定されます。

9.2.3.4. 追加の PostgreSQL データベースクラスターの作成と保護

環境が拡大するにつれて、既存または新規の共有ボリュームや複製ボリュームに、新しい PostgreSQL サーバーのデータベースクラスターを追加する必要が生じる場合があります。

新しいデータベースクラスターおよび関連するボリュームを追加・保護するには、次の手順に従ってください。

1. **ボリュームリソースを作成します。** PostgreSQL データベースクラスターが配置されているサーバー上で、ボリュームリソースを作成して拡張します。

2. **データベースクラスターを作成します。** initdb を実行して新しいデータベースクラスターを作成します。上記で作成したボリュームリソース上にデータディレクトリを配置してください。

3. **アクセス許可を設定します。** PostgreSQL データベースクラスターの起動および停止を実行するには、データディレクトリおよびすべてのファイルとサブディレクトリに、クラスター内のすべてのノードが認識するアクセス権が必要です。デフォルトでは、データディレクトリとすべてのファイルおよびサブディレクトリには、initdb を実行しているユーザーに基づいたアクセス権が設定されます。ユーザーがローカル管理者の場合、他のサーバーでデータベースクラスターを開始しようとすると、そのサーバーに対するアクセス権がないため失敗します。ドメインユーザーとしてログオンしているときにinitdb を実行するか、NT AUTHORITY\NetworkService に対するアクセス権限を追加することを推奨します。このアカウントはすべてのサーバーへのアクセスのために使用し、PostgreSQL リソースを作成する際に Windows サービスログオン資格情報に使用されるものと同じアカウントである必要があります。

4. **自動接続を設定します。** データベースクラスターは、パスワードを必要とせずに接続できるように構成する必要があります。詳細については、自動接続設定 を参照してください。

5. **データベースクラスターを起動します。** PostgreSQL リソースを作成するには、データベースクラスターを実行している必要があります。pg_ctl.exe で -o “-p port” 引数を指定してデータベースクラスターを起動します。Postmaster のポート引数を指定して PostgreSQL の確認と起動を実行する方法の詳細については、Postmaster のポート引数設定 を参照してください。

6. **PostgreSQL リソースを作成します。** 新しいデータベースクラスターが作成されたサーバー上で、PostgreSQL リソースを作成して拡張します。リソースの作成中に、ログオン資格情報（ユーザーアカウントおよびパスワード）とともに、Windows サービス名の入力を求められます。Windows サービス名は何でもかまいません。これは、データベースクラスターの管理（開始、停止など）のためのサービスアカウントの作成に使用されます。使用されるログオン資格情報は、すべてのサーバーに対するアクセス権を確保するために、手順 3 で設定した資格情報でなければなりません。

9.2.3.5. PostgreSQL 管理ログイン

SIOS Protection Suite PostgreSQL リソースの作成中に、ユーザーはそのデータベースクラスターの PostgreSQL 管理ユーザー名を入力する必要があります。この管理ユーザー名は、psql ユーティリティによるクライアント接続に使用されます。

ユーザー名は、以下の要件を満たす必要があります。

1. データベース（template1）への接続に加え、インスタンス用に定義されたデータベースのリストの取得が可能

2. システムテーブルの表示、一般的な照会の実行が可能

3. 自動（非ターミナルまたはスクリプト）接続を許可する。詳細については、自動接続設定 を参照してください。

9.2.3.6. 自動接続設定

SIOS Protection Suite PostgreSQL リソースの作成中に、ユーザーはそのデータベースクラスターの PostgreSQL 管理ユーザー名を入力する必要があります。PostgreSQL Recovery Kit では、このユーザー名に対してパスワードは要求されません。したがって、ヘルスチェック中に正常に実行された接続テストでは、次の 2つの設定方法のいずれかを使用する必要があります。

- 信頼構成（パスワードなし）
- pgpass.conf で提供される資格情報

信頼構成

PostgreSQL データベースクラスターの信頼できる接続を設定するには、pg_hba.conf ファイルの変更が必要です。データベースクラスターの管理ユーザーの認証方式は、「trust」に設定する必要があります。以下に、管理ユーザー pgsql のエントリーの例を示します。

#タイプ	データベース	ユーザー	アドレス	方式
# IPv4ローカル接続				
host	all	pgsql	127.0.0.1/32	trust
# IPv6ローカル接続				
host	all	pgsql	::1/128	trust

pgpass.conf による証明書

PostgreSQL データベースクラスターの管理ユーザーおよびパスワードの資格情報を提供するには、LifeKeeper のサービス用に指定されたログオンアカウント用の pgpass.conf ファイルを作成する必要があります。このファイルは、ユーザーの APPDATA フォルダに作成する必要があります。LifeKeeper の起動に使用したユーザーアカウントでログインし、次の手順を実行してください。

- ディレクトリを appdata に変更する
- ディレクトリ postgresql が存在しない場合は作成する
- ディレクトリを postgresql に変更する
- 次の形式で pgpass.conf ファイルを作成する

```
hostname:port:database:user:password
```

PostgreSQL データベースクラスターの管理ユーザーのパスワードが変更された場合、pgpass.conf ファイルをパスワード設定で更新する必要があります。

非ログインユーザーアカウント（例：ビルトインアカウント「Network Service」や「Local System」など）を使用してノードで LifeKeeper を開始する場合、%APPDATA% フォルダは、LifeKeeper クラスター内の別のノードで以下の LifeKeeper コマンドを実行することによって判別できます。

```
lcdremexec -d <node> – echo $APPDATA
```

pgpass.conf ファイルは、そのフォルダのシステム管理者が作成できます。作成された pgpass.conf ファイルには、LifeKeeper ログインアカウントユーザーの読み取り権限を必ず追加してください。

9.2.3.7. Postmaster のポート引数設定

PostgreSQL データベースクラスターを適切に管理するために、PostgreSQL Recovery Kit では postmaster プロセスをポートの引数 “-p port” で実行する必要があります。このポートは、PostgreSQL リソース階層を作成し、作成された階層を監視するために必要です。postmaster プロセスの現在の引数一覧を表示するには、PostgreSQL データベースクラスターのデータディレクトリにある postmaster.opts ファイルを参照してください。このファイルの内容の例を以下に示します。

```
C:/Program Files/PostgreSQL/9.6/bin/postgres.exe "-D" "E:\PGSQL1" "-p" "5432"
```

この例では、ポートの引数を指定して postmaster プロセスを実行しています。postmaster プロセスがポートの引数で実行されていない場合は、以下の 2つの方法のいずれかを使用して追加する必要があります。

- 既存の Windows サービスインスタンスにポートの引数を追加する
- Windows 以外のサービスインスタンスにポートの引数を追加する

既存の Windows サービスインスタンスにポートの引数を追加する

PostgreSQL Recovery Kit によって保護される PostgreSQL データベースクラスターが、PostgreSQL ソフトウェア v9.6 の初期インストールで作成された postgresql-x64-9.6 サービスなどの Windows サービスを介して実行されている場合、サービスのスタートアップコマンドラインを変更する必要があります。これは、以下の手順で実施できます。

1. 既存の PostgreSQL データベースクラスターインスタンスを停止します。これは、以下のいずれかの方法で実施します。
    a. Windows サービスインターフェース（services.msc）を使用して、サービスの停止を選択する
    b. コマンドラインユーティリティ "sc" を使用する（例：sc stop service_name）
    c. コマンド "net" を使用する（例：net stop service_name）
2. サービスのスタートアップコマンドラインを変更します。これは、"sc" ユーティリティを使用するコマンドラインまたはレジストリのスタートアップコマンドラインを編集することで実行できます。**注記：** PostgreSQL サービスのスタートアップコマンドラインは、pg_ctl.exe ユーティリティを使用します。pg_ctl ユーティリティから postmaster プロセスに引数を渡すには、"-o" 引数を使用する必要があります。"-o" 引数には、以下に示す変更で使用される "-p port" のような postmaster スタートアップオプションの引用符付きリストがあります。"sc" コマンドラインユーティリティを使用してスタートアップコマンドラインを編集するには、以下の手順に従ってください。この例では、postgresql-x64-9.6 サービスを使用しています。
    a. サービスの binPath（スタートアップコマンドライン）を取得します。例えば、"sc qc postgresql-x64-9.6" は次のようになります（この例では、スタートアップコマンドラインの出力行のみが表示されます）。
    BINARY_PATH_NAME : “C:\Program Files\PostgreSQL\9.6\bin\pg_ctl.exe” runservice -N “postgresql-x64-9.6” -D “E:\PGSQL1” –w

3. binPath を更新してください。**注記:** binPath 引数では "="の後ろには 1つのスペースがあり、値は二重引用符で囲まなければなりません。したがって、埋め込みの二重引用符をエスケープする必要があります。
sc config postgresql-x64-9.6 binPath= “\“C:\Program Files\PostgreSQL\9.6\bin\pg_ctl.exe\” runservice -N \“postgresql-x64-9.6\” -D \“E:\PGSQL1\” –w –o \”-p 5432\” “

   レジストリ内のスタートアップコマンドラインを編集するには、regedit などのレジストリ編集ツールを使用する必要があります。

   a. regedit を使用して、サービス ImagePath のレジストリ値を見つけます。

      HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\postgresql-x86-9.6\ImagePath

   b. 既存のコマンドラインの最後にポートの引数を追加して、ImagePath の値を変更します。

      -o “-p 5432”

3. 既存の PostgreSQL データベースクラスターのインスタンスを再起動します。これは、以下のいずれかの方法で実施できます。

   a. Windows サービスインターフェース（services.msc）を使用して、サービスの開始を選択する

   b. コマンドラインユーティリティ "sc" を使用する（例：sc start service_name）

   c. コマンド “net” を使用する（例：net start service_name）

4. postmaster.opts ファイルをチェックして、postmaster プロセスがポートの引数で実行されていることを確認します。

Windows 以外のサービスインスタンスにポートの引数を追加する

PostgreSQL データベースクラスター用の Windows サービスが存在しない場合は、PostgreSQL ユーティリティ pg_ctl.exe を使用して、PostgreSQL データベースクラスターの停止と再起動を実行する必要があります。これは、以下の手順で行うことができます。

1. PostgreSQL データベースクラスターを停止する

   pg_ctl stop –D F:\PGSQL2

2. PostgreSQL データベースクラスターを起動する

   pg_ctl start –D F:\PGSQL2 –w –o “-p 5433”

3. 先述のように postmaster.opts ファイルをチェックして、postmaster プロセスがポートの引数で実行されていることを確認します。

9.2.3.8. PostgreSQL 階層の監視

SIOS Protection Suite は、すべての PostgreSQL リソースの PostgreSQL データベースクラスターサービスを監視します。サービスが停止した場合、PostgreSQL リソースに関連付けられた監視プロセスはこれを検出し、ローカルリカバリーが有効になっている場合はローカルサーバー上のサービスの再起動を試みます。ローカルリカバリーが無効になっている場合は、リソースはバックアップサーバーにフェールオーバーされます。

SIOS Protection Suite は、保護された PostgreSQL データベースクラスターへの接続をテストするクエリも実行します。クエリが失敗した場合、PostgreSQL リソースに関連付けられた監視プロセスはこれを検出し、ローカルリカバリーが有効になっている場合はローカルサーバー上のサービスの再起動を試みます。ローカルリカバリーが無効になっている場合は、リソースはバックアップサーバーにフェールオーバーされます。

9.2.4. トラブルシューティング

このセクションでは、具体的に SIOS Protection Suite ソフトウェアに関連するわけではありませんが、環境全体に関連する事象についての提案とインサイトを提供します。

作成の失敗

リストアの失敗

9.2.4.1. 作成の失敗

現象:

データベースクラスターのデータディレクトリがあるボリューム上にあり、そのボリュームが SIOS Protection Suite によって保護されていないボリューム上にある場合、PostgreSQL サーバーリソースの作成は失敗します。

推奨する対応:

データディレクトリのボリュームリソースを作成します。

現象:

PostgreSQL データベースクラスターの postmaster プロセスが "-p port" オプションで実行されていない場合、PostgreSQL サーバーリソースの作成は失敗します。

推奨する対応:

正しい PostgreSQL データベースクラスターにアクセスするには、postmaster プロセスが "-p port"引数で実行されている必要があります。postmaster のポート引数を指定してPostgreSQLの確認と起動を実行する方法の詳細は、Postmaster のポート引数設定 を参照してください。

現象:

自動接続設定が間違っているか存在しない場合、管理ユーザーでログイン後に PostgreSQL サーバーリソースの作成がハングします。

推奨する対応:

自動接続を正しく設定下さい。詳細は 自動接続設定 を参照してください。

9.2.4.2. リストアの失敗

この状態を修正するには、データベースクラスターを **pg_ctl stop** で停止する必要があります。停止が完了したら、LifeKeeper の In Service アクションは成功します。

現象:

PostgreSQL サーバーリソースのリストアは、サーバークラッシュのためにデータベースクラスターが正常にシャットダウンしなかった場合、またはシャットダウン時に PostgreSQL サービスがハングアップした場合（ハングアップのシミュレーションに windbg を使用した場合）に失敗する可能性があります。正常にシャットダウンできないと、次回の起動時にデータベースクラスターの復旧処理が強制されます。この復旧処理により、Windows サービスの開始アクションが失敗し、サービスがデータベースクラスターの状態と矛盾した状態になる可能性があります。

不完全なシャットダウン後の起動時に、PostgreSQLは 次のメッセージを（他の多くのログと共に）記録する場合があります。

> Waiting for server start up
>
> LOG: database system was interrupted; last known up at 2017-07-25 16:12:10 EDT
>
> FATAL: the database system is starting up
>
> LOG: database system was not properly shut down; automatic recovery in progress

リカバリーが完了すると、PostgreSQL データベースのクラスタープロセスは実行中になりますが、Windows サービスの状態は「停止」になり、LifeKeeper PostgreSQL リソースは失敗した状態になります。LifeKeeper のリストア処理がデータベースクラスターの稼働中に試行されると、PostgreSQL は次のメッセージを記録します。

> FATAL: lock file “postmaster.pid” already exists
>
> HINT: Is another postmaster (PID 3488) running in data directory “E:/PGSQL1”?

推奨する対応:

この状態を修正するには、リカバリーの完了後にデータベースクラスターを **pg_ctl stop** で停止する必要があります。停止が完了したら、LifeKeeper の In Service アクションは成功します。

9.2.5. PostgreSQL Recovery Kit の変更可能な設定

PostgreSQL Recovery Kit は、特定のシナリオでリソースの保護をカスタマイズするのに役立つ変更可能な環境変数を提供しています。これらの変数の値を変更するには “%LKROOT%\etc\default\LifeKeeper” ファイルを編集します。新しい設定を有効にするためにプロセスを再起動する必要はありません。PostgreSQL Recovery Kit がインストールされるほとんどの環境において、デフォルト値で動作します。

- LKPGSQL_START_RETRIES

  このパラメーターは、失敗した状態であきらめるまでに、PostgreSQL Recovery Kit がデータベースクラスターの起動を待ってループする回数を制御します。各再試行の間には 5秒の待機時間があります。デフォルトでは Recovery Kit は 12回再試行され、データベースクラスターが起動するまで 60秒待機します。この値の最小値は 12です。

- LKPGSQL_STOP_RETRIES

  このパラメーターは、失敗した状態であきらめるまでに、PostgreSQL Recovery Kitがデータベースクラスターの停止を待ってループする回数を制御します。各再試行の間には5秒の待機時間があります。デフォルトではRecovery Kitは12回再試行され、データベースクラスターが起動するまで60秒待機します。この値の最小値は12です。

- LKPGSQL_RESTORE_CONNECT_RETRIES

  このパラメーターは、データベースクラスターが接続要求に応答するのを待ってリストアアクションを実行している間にPostgreSQL Recovery Kitがループする回数を制御します。再試行が指定された回数に達すると、リストア操作は失敗します。各再試行の間には5秒の待機時間があります。デフォルトではRecovery Kitは2回再試行され、データベースクラスターが接続要求に応答するまで10秒間待機します。この値の最小値は2です。

PostgreSQL データベースクラスターの変更可能な設定

Recovery Kit の deepchk スクリプトは、PostgreSQL データベースクラスターの稼働状態をチェックするために、データベースクラスターの template1 db への接続を試行します。利用可能な接続がすべて使用されている場合、この接続操作は失敗する可能性があります。これは、PostgreSQL のスーパーユーザー接続のパラメーターを変更することによって回避できます。

- superuser_reserved_connections

  データベースクラスター postgresql.conf ファイル内のこのパラメーターは、許可されるスーパーユーザー接続の数を制御します。デフォルトではこの設定はコメントアウトされているので、コメントアウトを解除する必要があります。変更を有効にするには、PostgreSQL データベースクラスターを停止して再起動する必

要があります。

9.3. はじめに SIOS Protection Suite Oracle

LifeKeeper Oracle

LifeKeeper Oracle Recovery Kit を使用すれば、Oracle データベースインスタンス (バージョン11g、12c、18c、19c) を障害の発生したサーバからバックアップサーバに復旧させることができます。また、データベースインスタンスの保護を他のサーバに拡張することもできます。LifeKeeper GUI を使用して、完全なリソース階層を簡単に作成し、データベースアクセスに使用される名前付きパイプまたは IP ソケットリソース (あるいはその両方) だけでなく、Oracle System Identifier (SID) が使用するすべてのディスクリソースをリカバリ操作に含めることができます。

9.3.1. Oracle の概要

LifeKeeper Oracle Recovery Kit では、他のサーバで Oracle データベースインスタンスを同時に実行したり、任意でそれらのインスタンスを LifeKeeper の保護下に置くこともできます。この設定はアクティブ / アクティブと呼ばれ、通常の稼働状態で LifeKeeper サーバを十分に活用できます。

LifeKeeper Oracle Recovery Kit には、データベースインスタンスをスタンバイサーバにフェイルオーバする前に、ローカルで回復させる機能 (ローカルリカバリ) があります。

LifeKeeper Oracle Recovery Kit は、以下の Core / 標準の Oracle サービスを保護します。

- Oracle Service
- Oracle TNS Listener

LifeKeeper Oracle Recovery Kit は、各リリースにおいて以下のオプションサービスを保護します。

オプション 11g サービス	オプション 12c サービス	オプション 18c サービス	オプション 19c サービス
Oracle DB Console	Oracle DB Console	Oracle DB Console	Oracle DB Console
Oracle Job Scheduler	Oracle Job Scheduler	Oracle Job Scheduler	Oracle Job Scheduler
Oracle Cluster Service の注記: このサービスの対象は Automatic Storage Management (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。	Oracle Cluster Service の注記: このサービスの対象は Automatic Storage Management (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。	Oracle Cluster Service の注記: このサービスの対象は Automatic Storage Management (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。	Oracle Cluster Service の注記: このサービスの対象は Automatic Storage Management (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。

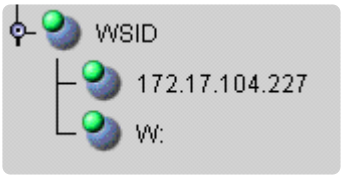
標準の Oracle リソース階層は、以下のリソースで構成されます。

- Oracle
- 共有通信リソース (IP または LAN Manager の別名)
- ボリューム

保護対象の SID のすべての Oracle データ、ログ、トレース (コアデータデース) ファイルは、共有または複製ボリュームに格納されます。障害検出時に、LifeKeeper は関連するデータボリュームと通信リソースとともにコアデータベースファイルをバックアップサーバに切り替えます。リカバリ作業がデータベースユーザに意識されることはまったくありません。LifeKeeper はすべての依存リソースをバックアップサーバに切り替えると、バックアップサーバで Oracle サービスを起動します。

次に示す LifeKeeper GUI 表示は、標準のリソース階層を表します。Oracle リソースは、階層ツリーの最上位のリソースです。Oracle リソースは、依存リソース (通信リソースおよびボリュームリソース) を正しい順序で起動および停止します。

この Oracle 階層では、通信 /Listener リソースとして IP のみが使用されます。



9.3.2. Oracle サービス

LifeKeeper Oracle Recovery Kit は、以下のコア / 標準の Oracle サービスを保護します。

- Oracle Service
- Oracle TNS Listener

LifeKeeper Oracle Recovery Kit は、各リリースにおいて以下のオプションサービスを保護します。

オプション 11g サービス	オプション 12c サービス	オプション 18c サービス	オプション 19c サービス
Oracle DB Console	Oracle DB Console	Oracle DB Console	Oracle DB Console
Oracle Job Scheduler	Oracle Job Scheduler	Oracle Job Scheduler	Oracle Job Scheduler
Oracle Cluster Service 注記: このサービスの対象は **Automatic Storage Management** (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。	Oracle Cluster Service 注記: このサービスの対象は **Automatic Storage Management** (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。	Oracle Cluster Service 注記: このサービスの対象は **Automatic Storage Management** (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。	Oracle Cluster Service 注記: このサービスの対象は **Automatic Storage Management** (ASM) です。LifeKeeper では現在 ASM をサポートしないため、LifeKeeper 下での保護には無効です。

9.3.3. Oracle リソース階層

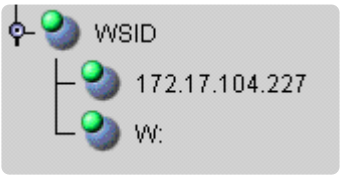
標準の Oracle リソース階層は、以下のリソースで構成されます。

- Oracle
- 共有通信リソース (IP または LAN Manager の別名)
- ボリューム

保護対象の SID のすべての Oracle データ、ログ、トレース (コアデータデース) ファイルは、共有または複製ボリュームに格納されます。障害検出時に、LifeKeeper は関連するデータボリュームと通信リソースとともにコアデータベースファイルをバックアップサーバに切り替えます。リカバリ作業がデータベースユーザに意識されることはまったくありません。LifeKeeper はすべての依存リソースをバックアップサーバに切り替えてから、Oracle サービスを起動します。

次に示す LifeKeeper GUI 表示は、標準のリソース階層を表します。Oracle リソースが最上位のリソースであり、依存リソース (通信リソースおよびボリュームリソース) を正しい順序で、開始と停止を行います。

この Oracle 階層では、通信/Listener リソースとして IP のみが使用されます。



制限事項: 複数の Oracle インスタンスを設定している場合、一意の仮想 IP アドレス上で各リスナーがリスンするように設定する必要があります。

LifeKeeper では、ポートが異なる同じ仮想 IP アドレスで、複数のリスナーがリスンすることを許可していません。

9.3.4. リカバリキットの要件

LifeKeeper Oracle Recovery Kit をインストールして設定する前に、構成が以下の要件を満たしていることを確認してください。

オペレーティングシステムソフトウェア。 LifeKeeper がサポートしている Windows オペレーティングシステムのバージョンの一覧は、SIOS Protection Suite for Windows サポートマトリックス を参照してください。

注記 : LifeKeeper ソフトウェア。各サーバに同じバージョンの LifeKeeper ソフトウェアとすべてのパッチをインストールする必要があります。具体的な LifeKeeper の要件については、リリースノート を参照してください。

SIOS DataKeeper ソフトウェア (オプション)。 共有ストレージではなく複製ボリュームでの Oracle の使用を予定してる場合は、SIOS DataKeeper for Windows ソフトウェアを各サーバ上にインストールする必要があります。

Oracle データベース。 Oracle Recovery kit がサポートする Oracle のバージョンは SIOS Protection Suite for Windows サポートマトリックス を参照してください。

9.3.5. Oracle のインストール

LifeKeeper Oracle Recovery Kit は FTP でダウンロードすることができます。標準のインストールインターフェースを提供する InstallShield を使用して簡単にインストールできます。

9.3.5.1. リカバリキットのインストール

LifeKeeper Oracle Recovery Kit をインストールする前に、前述した製品の要件と、Oracle とともに LifeKeeper をインストールおよび設定する で説明されているインストールおよび設定手順をよく理解してください。

Recovery Kit の旧バージョンからのアップグレード

LifeKeeper Oracle Recovery Kit ソフトウェアの旧バージョンから、リソース階層を維持したままアップグレードすることができます。

注記: LifeKeeper Oracle Recovery Kit をアップグレードした後、LifeKeeper GUI を終了して再起動する必要があります。

キットの削除

LifeKeeper Oracle Recovery Kit ソフトウェアを削除するには、コントロールパネルの **[プログラムと機能] アプレット** で「**LifeKeeper Oracle Recovery Kit vX.X**」を選択してください。

9.3.5.2. Oracle とともに LifeKeeper をインストールおよび設定する

Oracle とともに LifeKeeper をインストールおよび設定する手順は、複製ストレージと共有ストアシステムとでやや異なります。このドキュメントでは、インストールと設定のプロセスを明確にするために、それぞれのタイプのストレージ構成について、個別のセクションを設けてあります。

最も効率的にセットアップを行うためには、以下の作業を実行して、最初にプライマリサーバ上、次にセカンダリサーバ上に Oracle データベースインスタンスを作成してください。

重要事項

- 特定のサーバ上で作業しているときは、通信リソースを該当のサーバに切り替えてください。例えば、バックアップサーバ上で作業しているときは、通信リソースをバックアップサーバに切り替えてください。
- アップグレード時に、リソース階層は保持されます。
- Oracle Home ディレクトリごとに 1 つの SID のみがサポートされます。
- Oracle Home がデータベース (SID) と同じ LifeKeeper 保護対象ボリュームにインストールされていない場合は、特別な配慮が必要です。Oracle Home が異なる共有ボリュームまたはレプリケーションボリュームにインストールされている場合、そのボリュームは LifeKeeper の保護対象でなければならず、Oracle リソース階層に依存リソースとして手動で追加する必要があります。Oracle Home が LifeKeeper 保護対象ボリュームにインストールされていない場合は、変更は不要です。
- Windows ディスク管理ツールを使用して、ディスクリソースとボリュームを設定してください。Net Manager などの Oracle ツールを使用して、ネットワークプロトコルを設定してください。

9.3.5.3. Oracle をインストールする前に

Oracle ソフトウェアをインストールする前に、サーバとストレージが設定され、LifeKeeper がクラスタ内の各サーバにインストールされている必要があります。こうすることで、LifeKeeper によってすでに保護されているボリュームに Oracle をインストールできるようになります。

レプリケーションストレージシステム

プライマリサーバ上

1. **Windows ディスク管理** ツールを使用して、ディスクリソースを設定し、使用したい複製ボリュームを定義します。(ボリュームは適切なサイズにしてください。)

2. **Windows エクスプローラ** を使用して、Oracle SID によって使用されるすべてのボリュームのネットワークから共有解除します。

3. ネットワークを、LifeKeeper TCP/IP コミュニケーションパスと切り替え可能な IP アドレス (該当する場合) をサポートするように設定します。

4. LifeKeeper Core ソフトウェア、LifeKeeper Oracle Recovery Kit の順にローカルディスクにインストールします。

5. 使用している Oracle データベースが非常に大きい場合は、MAXWAIT 値を確認して、増やすことを検討します。

6. SIOS DataKeeper ソフトウェアをローカルディスクにインストールします。詳細については、SIOS Protection Suite インストレーションガイド を参照してください。

バックアップサーバ上

1. バックアップサーバを起動し、**ディスクの管理** ユーティリティを使用して、プライマリサーバに割り当てたものと同じドライブレターを複製ボリュームに割り当てます。
2. LifeKeeper Core ソフトウェア、LifeKeeper Oracle Recovery Kit の順にローカルディスクにインストールしてください。
3. 使用している Oracle データベースが非常に大きい場合は、MAXWAIT 値を確認して、増やすことを検討します。
4. SIOS DataKeeper ソフトウェアをインストールします。

プライマリサーバ上

これで両方のサーバに LifeKeeper がインストールされました。プライマリサーバに戻って、以下を実行してください。

1. LifeKeeper GUI を使用して、プライマリサーバとバックアップサーバの間のコミュニケーションパスを作成します。

2. LifeKeeper で通信リソースを作成し (IP、LAN Manager のいずれか、または両方)、これらをバックアップサーバに拡張してください。その後、Oracle リソース階層を作成するときに、LifeKeeper は依存関係に従ってこれらのリソースを自動で階層内に移動します。

注記: Oracle 階層が作成されるときに、SIOS DataKeeper リソースが自動的に作成され、依存関係に従って Oracle リソース階層に移動されます。

9.3.5.4. Oracle のインストール

LifeKeeper をインストールしてボリュームと通信リソースを設定すると、Oracle を保護対象ボリュームにインストールする準備が整います。

Oracle 12c のインストール: Oracle12cには、いくつかの新しいインストールオプションがあります。ソフトウェアとサンプルデータベースのインストールには、以下のオプションを推奨します。

- Oracle Services Account - "Windows Built-In Account" を選択してください。これは、ローカルシステムアカウントを参照します。
- Container Database - "Container Database"のチェックを選択してください。これは、サンプルデータベースのチェックボックスオプションです。

  Oracle 12c R2 をインストールする場合 SYS と SYSTEM のユーザ名を変更するために **拡張インストール** に進みます。
- Password Management - サンプルデータベースがインストールされると、"Password Management" ボタンが表示されます。 ボタンを押下して、SYSとSYSTEM管理者アカウントにパスワードを設定してください。選択したこれらのアカウントのうち、どちらかがOracleリソース階層を作成するのに必要となります。

プライマリサーバ上

1. Oracle ソフトウェアを保護対象の共有ボリュームにインストールします。これで Oracle SID が作成されます。この Oracle SID に関連するすべてのファイル (ログ、トレース、コントロール、データファイルなど) は保護対象ボリューム上に置かれている必要があります。
2. デフォルトの TNSListener サービスである Oracle<OraHome>TNSListener を停止して、起動モードを **[手動]** に設定します。(この後の手順で、保護対象となる SID の新しい Listener を作成します。)
3. Oracle Net Manager を使用して、以下の手順に従って、Oracle が LifeKeeper で保護する通信リソースを使用するように設定します。
   a. SID 名を使用して、新しい **TNSListener サービス** を作成します。**リスニング位置** を設定して、LifeKeeper で保護する IP アドレスおよび名前付きパイプ (LAN Manager 別名) を指定します。次に、データベースサービスを設定して、**Oracle ホームディレクトリ** と SID を指定します。
   b. SID の **Oracle サービス** を変更します。TCP/IP については、ホスト名を保護される IP アドレスに変更してください。**名前付きパイプ** については、マシン名を LAN Manager の別名に変更してください。
4. LifeKeeper で保護される SID の **TNSListener サービス** インスタンスを個別に作成します。このサービスは、`lsnrctl Start <SID>` コマンドを使用して作成する必要があります。これにより、*`Oracle<OraHome>TNSListener<SID>`* という名前をもつサービスが作成されます。
5. **[サービス]** ツールを使用して、以下の手順で Oracle サービスをテストします。

a. 新規の **TNSListener** サービスを正常に停止および起動できるかどうかを確認します。

b. `OracleService<SID>` サービスが Oracle によって作成されたことを確認します。

c. すべての Oracle サービスを停止します。

バックアップサーバ上

1. LifeKeeper で、バックアップサーバ上の保護対象ボリュームをサービス中にします。
2. Oracle インベントリディレクトリを削除して、Oracle データファイルを含むディレクトリの名前を変更します。新規インストールの場合は、データファイルを削除することができます。
3. Oracle ソフトウェアを保護対象のボリュームにインストールします。使用するインストールオプションは、プライマリサーバと完全に一致させてください (Oracle Home、SID 名およびパスを同じにする)。プロンプトが表示されたら、既存の Oracle 設定の上書きを選択します。**注記**: *.bak へのファイルの移動に関するエラーは無視してください。
4. デフォルトの TNSListener サービスである *Oracle<OraHome>TNSListener* を停止して、起動モードを **[手動]** に設定します。
5. 必要に応じて以下の手順に従って、**Oracle Net Manager** を使用して、Oracle が LifeKeeper で保護する通信リソースを使用するように設定します。

   a. SID 名を使用して、新しい **TNSListener** サービスを作成します。**リスニング位置** を設定して、LifeKeeper で保護する IP アドレスおよび名前付きパイプ (LAN Manager 別名) を指定します。次に、**データベースサービス** を設定して、Oracle Home ディレクトリと SID を指定します。

   b. SID の **Oracle サービス** を変更します。TCP/IP については、ホスト名を保護される IP アドレスに変更してください。**名前付きパイプ** については、マシン名を LAN Manager の別名に変更してください。

6. LifeKeeper で保護される SID の **TNSListener サービス** インスタンスを個別に作成します。このサービスは、lsnrctl Start <SID> コマンドを使用して作成する必要があります。これにより、*Oracle<OraHome>TNSListener<SID>* という名前をもつサービスが作成されます。
7. **[サービス]** ツールを使用して、以下のように Oracle サービスをテストします。

   a. 新規の TNSListener サービスを正常に停止および起動できるかどうかを確認します。

   b. *OracleService<SID>* サービスが Oracle によって作成されたことを確認します。

   c. バックアップサーバ上の Oracle サービスをすべて停止します。

プライマリサーバ上

1. プライマリサーバ上で、ボリュームリソースをサービス中に戻します。

2. プライマリサーバ上で *OracleService<SID>* サービスを開始します。

3. プライマリサーバ上に Oracle 階層を作成して、バックアップサーバに拡張します。詳細については、Oracle 階層の作成 を参照してください。

4. 手動フェイルオーバを実行し、新しい Oracle 階層をテストします。

9.3.6. Oracle 設定タスク

前のセクションで説明したようにセットアップ作業を完了すると、Oracle リソース階層の作成と拡張を行う準備ができます。

このガイドでは以下の 4 つの作業について説明します。これらは Oracle リソースインスタンス特有のものであり、各 Recovery Kit で異なっています。

- リソース階層の作成 - アプリケーションリソース階層を LifeKeeper クラスタに作成します。
- リソース階層の拡張 - プライマリサーバからバックアップサーバにリソース階層を拡張します。
- リソース階層の拡張解除 - リソース階層を LifeKeeper クラスタ内の 1 つのサーバから拡張解除 (削除) します。
- リソース階層の削除 - リソース階層を LifeKeeper クラスタ内のすべてのサーバから削除します。

以下の作業の手順はすべての Recovery Kit に共通しているため、LifeKeeper オンライン製品マニュアルの「GUI による管理作業」のセクションで説明しています。

- リソース依存関係の作成。既存のリソースと別のリソースインスタンスとの間に親子依存関係を作成し、クラスタ内のすべての対象サーバに依存関係の変化を通知します。
- リソース依存関係の削除。リソース依存関係を削除して、その依存依存関係の変更をクラスタ内の適用可能なすべてのサーバに反映させます。
- サービス開始: 特定のサーバのリソース階層を In Service にします。
- サービス停止: 特定のサーバのリソース階層を Out of Service にします。
- プロパティの表示と編集。特定のサーバのリソース階層のプロパティを表示または編集します。

注記: このセクションの残りの部分では、設定作業はすべて [編集] メニューから実行されます。また設定作業の大半は次の方法でも実行できます。

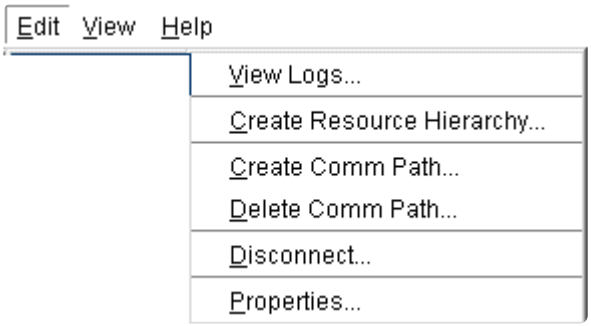
- ツールバーから
- 状態表示の左ペインにあるグローバルリソースを右クリック
- 状態表示の右ペインにあるリソースインスタンスを右クリック

右クリックの方法では、[編集] メニューを使用するときに必要な情報を入力しないですみます。

9.3.6.1. Oracle 階層の作成

必要な設定作業終了後、以下の手順に従って、データベースを保護する Oracle Server 階層を定義してください。

1. LifeKeeper GUI メニューから **[編集]** を選択し、次に **[サーバ]** を選択します。メニューから **[リソース階層の作成]** を選択します。



2. **[保護するアプリケーションの作成]** ダイアログボックスが表示されます。プルダウンリストから適切な **[プライマリサーバ]** と **[バックアップサーバ]** を選択します。**[次へ]** を選択して続行してください。クラスタ内にインストールされ、認識されているすべての Recovery Kit が表示されます。

3. **[Oracle]** を選択し、**[次へ]** をクリックします。

4. 次の表に示す情報を入力するように求められます。ダイアログボックスで **[戻る]** ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは、前に入力した情報を修正する必要があるエラーが発生した場合に便利です。いつでも **[キャンセル]** をクリックして、作成処理全体を取り消すことができます。

フィールド	説明
Oracle ホームディレクトリの選択	この階層に適した Oracle Home ディレクトリを選択してください。
Oracle SID の選択	LifeKeeper の保護下に置く Oracle SID を選択してください。
Oracle ユーザ名の入力	Oracle の管理ユーザ名を入力してください。このユーザアカウントには、データベースへのシステム許可を持たせる必要があります。
パスワードの入力	Oracle 管理ユーザのシステムパスワードを入力してください。
オプションサービス	この階層とともに保護するオプションのサービスを選択してください。リストには LifeKeeper 保護に適したサービスだけが記載されています。
Oracle タグ名	固有のタグ名を入力します。自動で表示されるデフォルトのタグ名をそのまま使用することもできます。 **注意：**タグ名に使用できる文字はASCII印字可能文字のみです。

5. **[次へ]** をクリックすると、**リソース作成ウィザード** によって Oracle リソースが作成されます。LifeKeeper によ

って入力データが検査されます。LifeKeeper が問題を検出すると、情報ボックスにエラーメッセージが表示されます。

6. 別の情報ボックスが表示され、Oracle リソース階層が正常に作成されたこと、フェイルオーバによって保護するには、その階層をクラスタ内の別のサーバに拡張する必要があることを示すメッセージが表示されます。**[次へ]** をクリックします。

7. **[次へ]** をクリックすると、LifeKeeper の **拡張前処理ウィザード** が起動します。リソース階層を別のサーバに拡張する方法の詳細については、Oracle 階層の拡張 を参照してください。

9.3.6.2. Oracle 階層の拡張

この操作は **[編集]** メニューから開始できますが、**[リソース階層の作成]** オプションの処理を完了すると自動的に開始されます。その場合は、以下の手順 2 を参照してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の拡張]** を選択します。**拡張前処理ウィザード** が表示されます。**拡張** 操作に慣れていない場合は、**[次へ]** をクリックしてください。
2. **拡張前処理ウィザード** に以下の情報を入力してください。

フィールド	説明
バックアップの優先順位	1～999 の数値を入力して、このリソースのカスケーディングフェイルオーバシーケンスにおけるターゲットサーバの優先順位を指定してください。小さい数値ほど優先順位が高くなります。階層の拡張が行われる最初のサーバには、デフォルトで 10 が指定されます。

3. 拡張前のチェックが正常に終了したというメッセージが表示されたら、**[次へ]** をクリックします。

4. 拡張する階層に応じて、拡張する **リソースタグ** を表示する情報ボックスが表示されます。リソースタグは編集できません。**[拡張]** をクリックします。

9.3.6.3. Oracle 階層の拡張解除

LifeKeeper クラスタの 1 つのサーバからリソース階層を削除する場合は、次の手順を実行してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の拡張解除]** を選択します。
2. Oracle リソースを拡張解除したい **ターゲットサーバ** を選択します。Oracle リソースが現在 In Service のサーバは選択できません。(右側のペインにあるリソースインスタンスを右クリックして **拡張解除** 作業を選択した場合、このダイアログボックスは表示されません。) **[次へ]** をクリックします。
3. 拡張解除する Oracle 階層を選択して、**[次へ]** をクリックします。(左右どちらかのペインのリソースインスタンスを右クリックして **拡張解除** 作業を選択した場合、このダイアログボックスは表示されません。)
4. 拡張解除のために選択したターゲットサーバと Oracle リソース階層を確認する情報ボックスが表示されます。**[拡張解除]** をクリックします。
5. Oracle リソースが正常に拡張解除されたことを示す別の情報ボックスが表示されます。**[完了]** をクリックして、**[リソース階層の拡張解除]** メニューを終了します。

9.3.6.4. Oracle 階層の削除

Oracle 階層または Oracle インスタンスを削除する前に、その階層がプライマリサーバでアクティブ (緑色) になっていることを確認してください。階層を削除する前に依存関係を削除することもできます。その操作を行わない場合、依存関係も削除されます。

Oracle 階層を削除するには、以下の手順を実行してください。

- Oracle サービスを停止してください。
- Oracle 階層とすべての依存関係を削除してください。

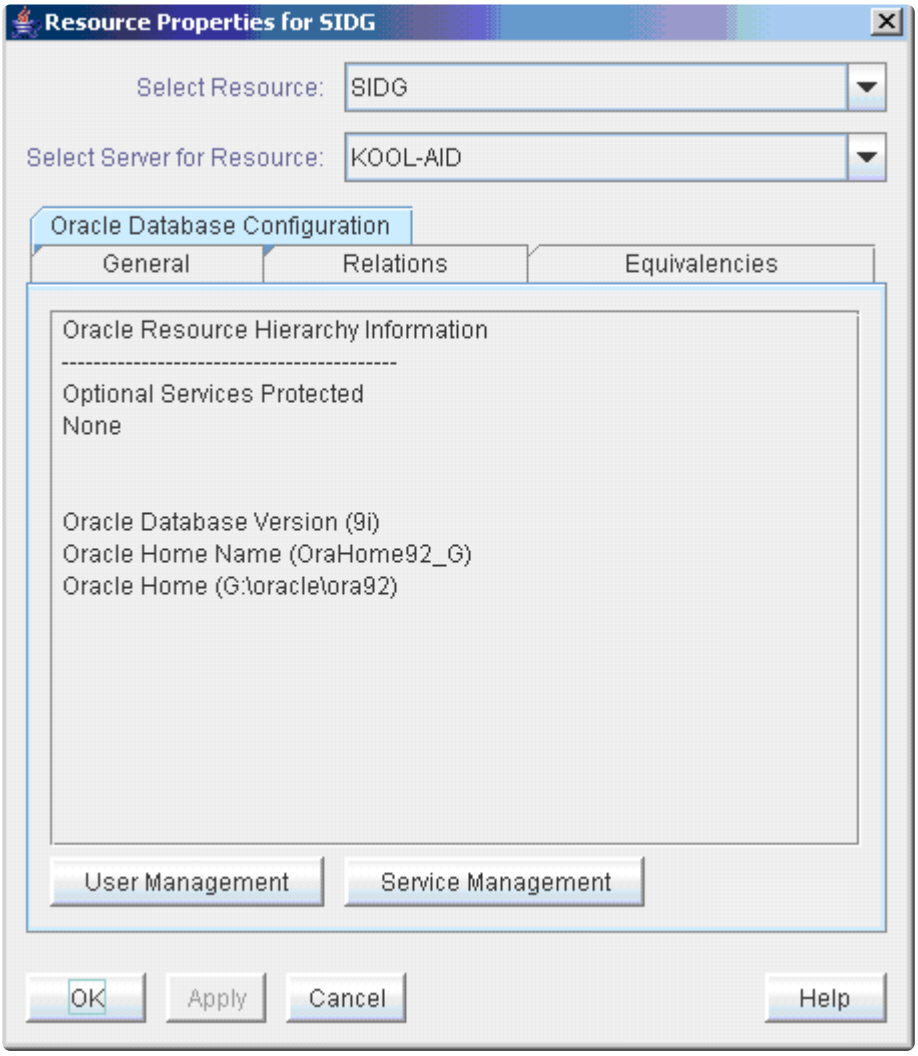
注記:
• LifeKeeper に対して削除を開始するときは、データベースをバックアップサーバから正しく退避させるために、両方のサーバがアクティブであることを確認してください。
• IP アドレスとボリュームを LifeKeeper の保護下にとどめる場合は、Oracle 階層を削除する前にボリュームと TCP/IP の依存関係を削除しておく必要があります。

LifeKeeper 環境のすべてのサーバからリソース階層を削除するには、次の手順を実行してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の削除]** を選択します。
2. Oracle リソース階層を削除する **ターゲットサーバ** を選択し、**[次へ]** をクリックします。(左右どちらかのペインのリソースインスタンスを右クリックしてリソースの削除作業を選択した場合、このダイアログボックスは表示されません。)
3. **削除する階層** を選択します。(右側のペインでリソースインスタンスを右クリックしてリソースの削除作業を選択した場合は、このダイアログボックスは表示されません。) **[次へ]** をクリックします。
4. 選択したターゲットサーバと削除対象として選択した階層を確認する情報ボックスが表示されます。**[次へ]** をクリックします。
5. Oracle リソースが正常に削除されたことを示す別の情報ボックスが表示されます。
6. **[完了]** をクリックして終了します。

9.3.6.5. Oracle データベースの設定管理

LifeKeeper GUI を使用して保護対象の Oracle リソースを管理するには、右側のペインに移動して、Oracle リソースを右クリックし、**[プロパティ]** 、**[Oracle データベース設定]** タブを順にクリックしてください。**[Oracle データベース設定]** ページでは、Oracle リソース情報を表示して変更できます。



ユーザ管理:

[ユーザ管理] メニューでは、LifeKeeper を操作する Oracle DBA ユーザを管理します。

管理作業の選択:

- **現在のユーザを表示** - 保護対象のリソース階層で使用される現在のユーザ名を表示します。
- **パスワードの変更** - 保護対象のリソース階層に関連付けた現在のユーザのパスワードを変更します。
- **ユーザとパスワードの変更** - Oracle インスタンスを管理監視する Oracle DBA ユーザとパスワードの両方を変更します。ユーザには、保護対象のすべてのデータベースに対する DBA 権限を付与する必要があります。

フィールド	説明
ユーザ名の入力	管理ユーザ名を入力します。管理ユーザのアカウントには、LifeKeeper が保護する全データベースに対する DBA 権限を与える必要があります。
パスワードの入力	更新するユーザアカウントの管理パスワードを入力してください。

サービス管理

このメニューでは、リソース階層で保護するオプションの Oracle サービスの一覧を変更します。LifeKeeper は保護対象のオプションサービスを監視します。

サービス作業の選択:

- **サービスの追加** - 保護設定にサービスを追加します。LifeKeeper は、オプションとして追加した Oracle サービスの監視を開始します。
- **サービスの削除** - 保護設定からサービスを削除します。LifeKeeper はオプションの Oracle サービス監視を停止します。

フィールド	説明
サービス名	保護設定に **追加** するか、そこから **削除** するサービスの名前を入力してください。サービスを追加する場合は、サービス名を入力してください。サービスを削除する場合は、削除するサービスを一覧から選択してください。
クラスタ更新	該当クラスタ内のすべてのシステムを更新する場合は、**[はい]** を選択してください。それ以外の場合は、**[いいえ]** を選択して現在のシステムだけを更新します。**[いいえ]** を選択した場合は、サービスを手動でバックアップサーバに追加する必要があります。

9.3.6.6. Oracle Multitenant 構成による Pluggable Database の設定

Oracle データベースが Oracle Multitenant アーキテクチャに対応し、Oracle データベースがコンテナ・データベース（以下、CDB と呼ぶ）を保護する場合、Oracle データベースサーバに加えて、プラガブル・データベース（以下、PDB と呼ぶ）を保護することができます。

CDB と PDB の確認

1. PDB を保護するためには Oracle リソースが作成されている必要があります。また、保護しているOracle リソースが CDB である必要があります。CDB であるかの確認はデータベースへ接続後に以下のコマンドを使って確認することができます。

   ```
   SQL> select CDB from V$DATABASE;
   ```

2. PDB を保護するにあたって、CDB の中に PDB がマウントされている必要があります。PDB がマウントされているかの確認はデータベース接続後に以下のコマンドで確認することができます。

   ```
   SQL> show pdbs;
   ```

Oracle PDB リソース階層の作成

1. LifeKeeper GUI メニューから **[Edit]** を選択し、次に **[Server]** を選択してください。ドロップダウンメニューから、**[Create Resource Hierarchy]** を選択してください。

   重要: リソースを作成するときは、Oracle リソースが作成されており、In Serviceである必要があります。

   ダイアログボックスが表示され、クラスタ内にインストール済みの認識されているすべての Recovery Kit がドロップダウンリストボックスに表示されます。ドロップダウンリストから **[Oracle Pluggable Database]** を選択してください。**[Next]** をクリックして次のダイアログボックスに進んでください。

   注記: ダイアログボックスで **[Back]** ボタンが有効な場合は、前のダイアログボックスに戻ることができます。これは、エラーが発生して、以前に入力した情報を訂正する必要がある場合に特に役立ちます。

   階層作成手順のどの段階でも、**[Cancel]** をクリックすると、作成プロセス全体がキャンセルされます。

2. 以下の情報を入力するように要求されます。ダイアログボックスで **[Back]** ボタンが有効な場合は、前のダイアログボックスに戻ることができます。これは、エラーが発生して、前に入力した情報を修正する必要がある場合に便利な機能です。いつでも **[Cancel]** をクリックして、作成処理全体を取り消すことができます。

フィールド	ヒント
Server	Oracle PDB リソースを作成する LifeKeeper サーバを選択します。
ORACLE_SID	保護しているOracleデータベースのSIDを指定します。

Oracle PDBs	保護したいPDBを指定します。このフィールドでは複数選択が可能です。
PDB Tag	プライマリサーバ上の新しい Oracle PDB リソースに対する固有のタグ名です。デフォルトのタグ名は「pdb-<ORACLE_SID>」となっています.。別の固有のタグ名を入力することもできます。タグ名に対する有効な文字は、アルファベット、数字および以下の特別な記号になります。- _ ./

3. **[Next]** をクリックしてください。**[Create Resource Wizard]** が表示され、Oracle PDB リソース階層が作成されます。LifeKeeper によって入力データが検査されます。問題が検出された場合、情報ボックスにエラーメッセージが表示されます。

4. Oracle PDB リソース階層が正常に作成されたこと、フェイルオーバによる保護を実現するにはその階層をクラスタ内の別のサーバに拡張する必要があることを示すメッセージが表示されます。**[Next]** をクリックします。

5. **[Continue]** をクリックします。**[Pre-extend Wizard]** が起動されます。リソース階層を別のサーバに拡張する方法の詳細については、「Oracle PDB リソース階層の拡張」の **手順 2** を参照してください。

Oracle PDB リソース階層の拡張

この操作は **[Edit]** メニューから開始できます。または、**[Create Resource Hierarchy]** オプションが完了すると自動的に開始されます。その場合は下の手順 2 を参照してください。

1. **[Edit]** メニューの **[Resource]** から **[Extend Resource Hierarchy]** を選択します。**[Pre-Extend Wizard]** が表示されます。拡張操作に慣れていない場合は、**[Next]** をクリックします。LifeKeeper のリソース階層の拡張作業のデフォルト値が分かっていて、入力と確認を省略する場合は、**[Accept Defaults]** をクリックします。

2. **[Pre-Extend Wizard]** で以下の情報を入力します。

   注記: 最初の 2 つのフィールドは **[Edit]** メニューの **[Extend]** から操作を開始した場合にだけ表示されます。

フィールド	ヒント
Template Server	Oracle PDB リソースが現在 In Service のサーバを選択します。
Tag to Extend	拡張する Oracle PDB リソースを選択します。
Target Server	拡張先のサーバを入力または選択します。
Template Priority	**テンプレートの優先順位** を選択または入力します。これはサーバで現在 In Service の Oracle PDB 階層の優先順位です。優先順位は、1 ～ 999 の範囲で未使用の値が有効で、小さい数字ほど優先順位が高くなります (数字 1 が最高の優先順位に相当)。拡張処理時に、別のシステムですでに使用中の優先順位をこの階層に対して指定することはできません。デフォルト値を推奨します。 **注記:** このフィールドは階層を最初に拡張するときだけ表示されます。

Target Priority	これは、新しく拡張する Oracle PDB 階層が、他のサーバに存在する同等の階層に対して持つ相対的な優先順位です。1 ～ 999 の範囲で、まだ優先順位として使用されていない値が有効で、リソースのカスケーディングフェイルオーバシーケンスにおけるサーバの優先順位を示します。LifeKeeper のデフォルトでは、階層が作成されたサーバに「1」が割り当てられることに注意してください。優先順位は連続している必要はありませんが、特定のリソースについて 2 つのサーバに同じ優先順位を割り当てることはできません。

3. 拡張前のチェックが正常に終了したというメッセージが表示されたら、**[Next]** をクリックします。

4. 拡張する階層に応じて、拡張されるリソースタグ (一部編集不可) を示す一連の情報ボックスが表示されます。

5. **[Extend Wizard]** でTag名が正しいかを確認し **[Extend]** をクリックします。

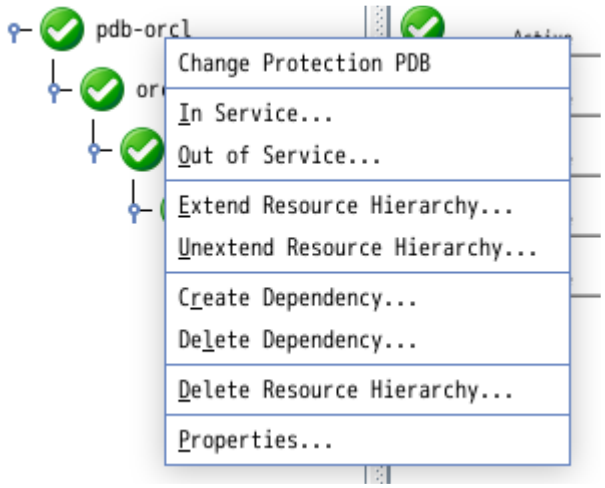
6. 「Hierarchy extend operations completed (階層の拡張操作が完了しました)」というメッセージが表示されたら、階層を別のサーバに拡張する場合は、**[Next Server]** をクリックし、拡張作業が必要ない場合は、**[Finish]** をクリックします。

7. 「Hierarchy Verification Finished (階層の検査が完了しました)」というメッセージが表示されたら、**[Done]** をクリックします。

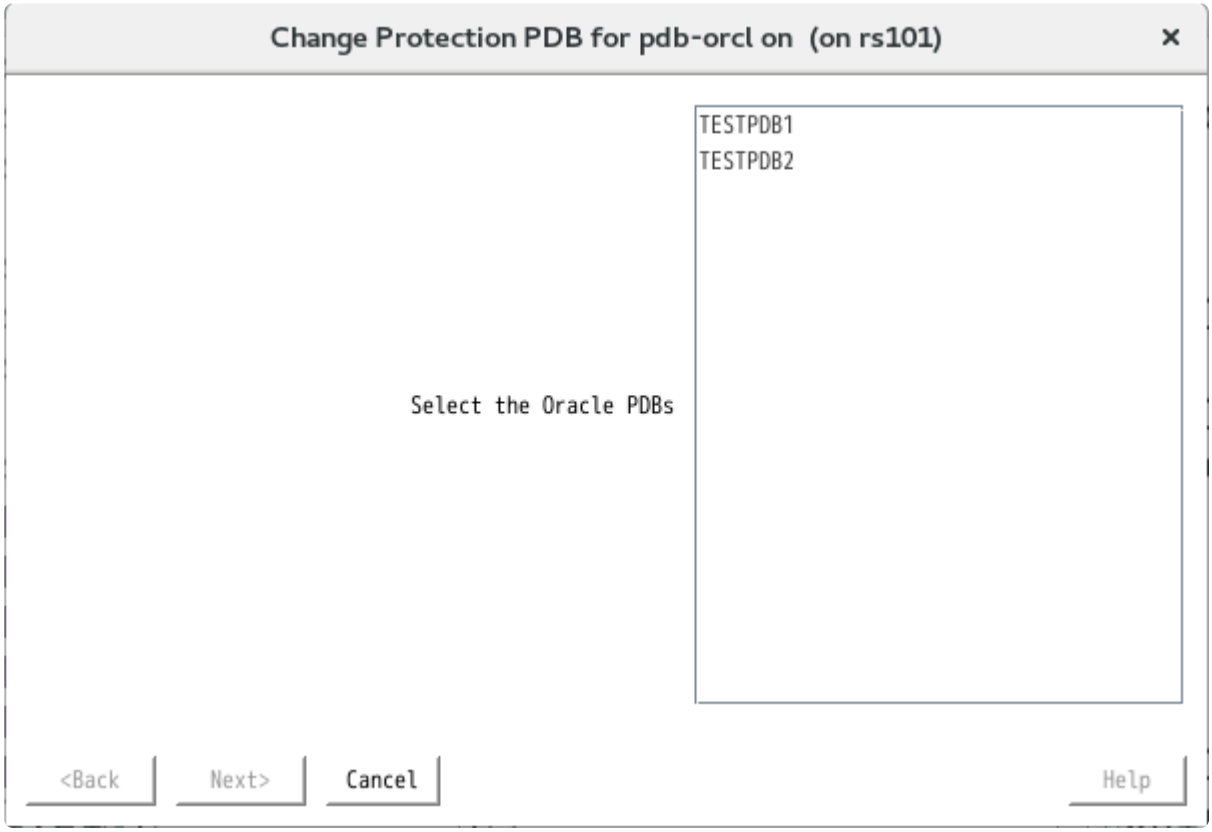
保護する PDB の変更

階層作成後、以下の手順で保護する PDB を変更してください。

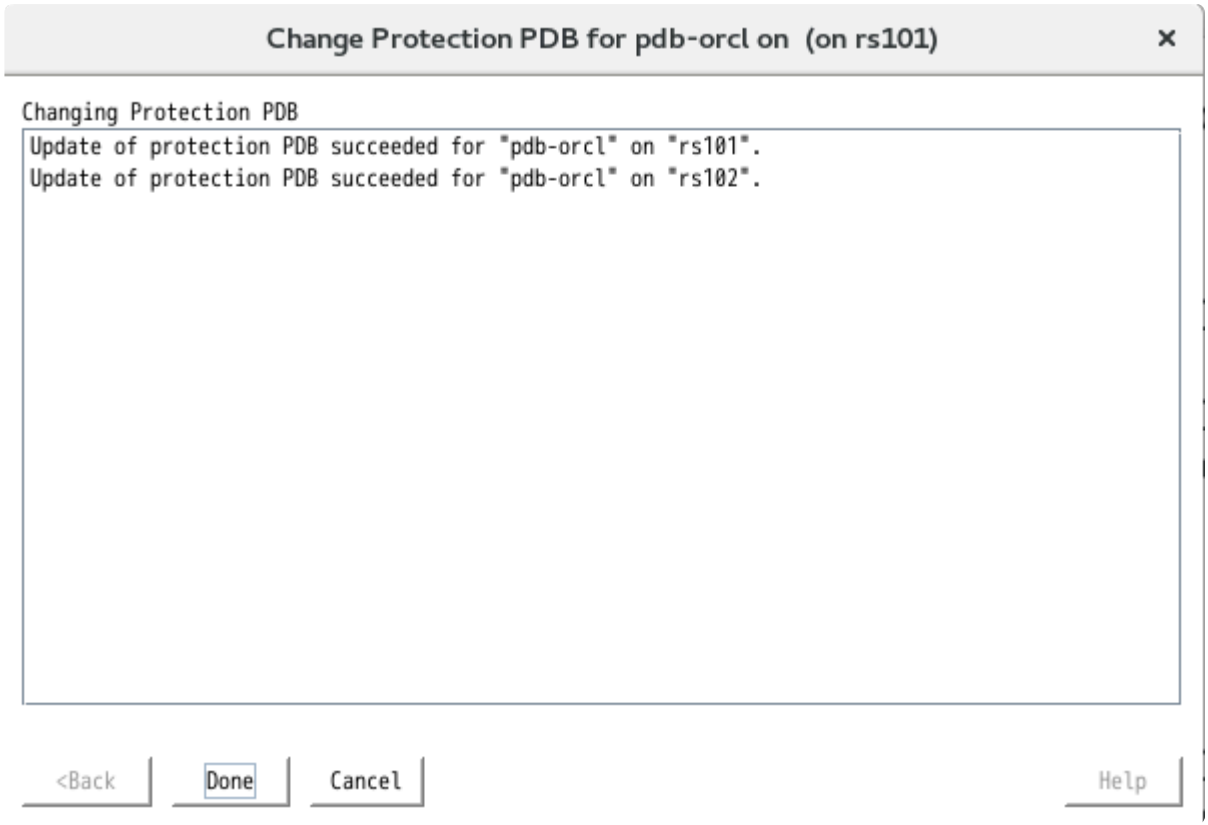
1. LifeKeeper GUI から Oracle PDB リソース階層を右クリックし、**[Change Protection PDB]** を選択してください。



2. 保護したい PDB を選択してください。(複数選択可能です)



3. **[Next]** をクリックすると設定が変更されます。



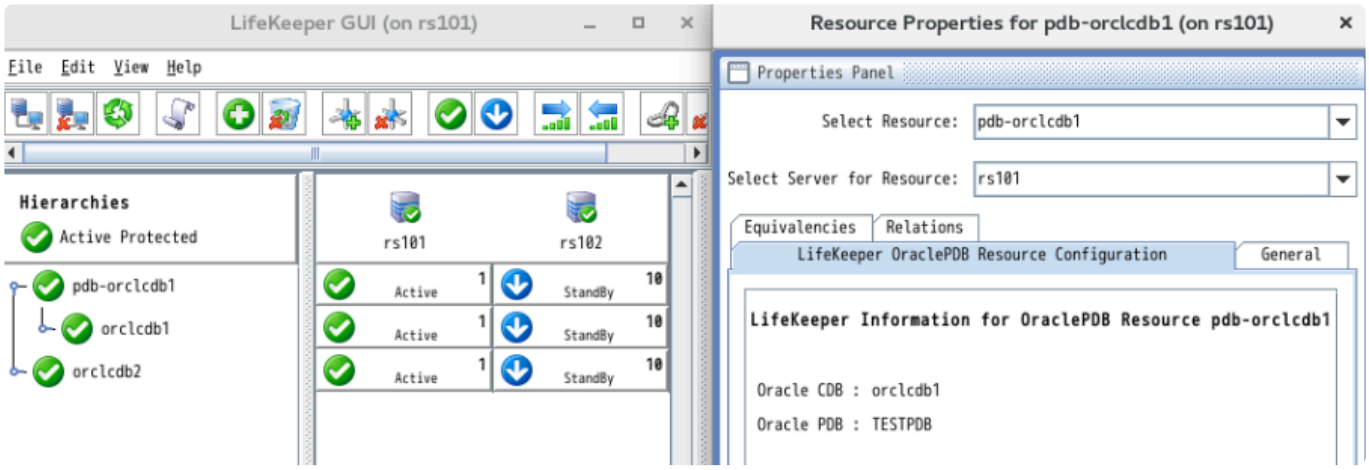
4. **[Done]** をクリックして設定変更を完了してください。

9.3.6.7. Pluggable Database の移行

LifeKeeper で保護されている、コンテナ・データベース（以下、CDB）間でプラガブル・データベース（以下、PDB）を移行する手順を紹介します。事前にデータベースのバックアップを取得しておくことをおすすめします。

移行手順

本手順では、PDB のプラグ/アンプラグを使用した方法による PDB の移行を示します。
下図の構成の場合を例に、ソース CDB（ORCLCDB1）から ターゲット CDB（ORCLCDB2）へ PDB（TESTPDB）を移行する手順です。



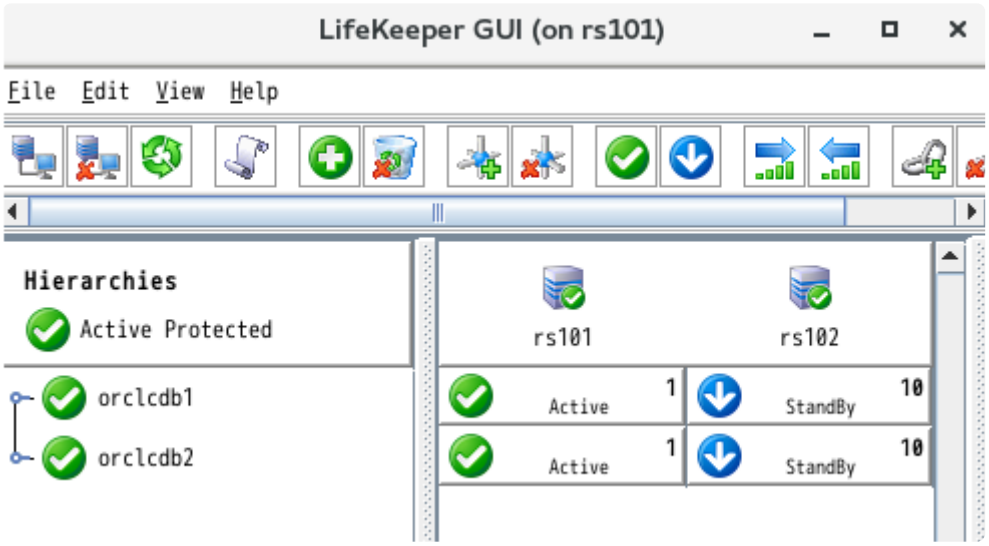
1. 移行前にソース CDB に接続し、対象の PDB の情報を確認します。

```
SQL> COLUMN NAME FORMAT A8

     SELECT NAME, DBID, GUID FROM V$CONTAINERS WHERE NAME='<PDB>';
```

2. PDB リソースから Oracle リソース階層を削除します。

3. Oracle PDB リソースを Out of Service にし、リソースを削除します。
   複数の PDB を保護している Oracle PDB リソースがある場合は、リソース設定 [Change Protection PDB]（保護するPDBの変更 を参照）で対象の PDB を保護対象から削除します。



4. ソース CDB に接続し対象の PDB をアンプラグします。(PDB が停止していない場合、PDB を停止します。)

```
SQL> ALTER PLUGGABLE DATABASE <PDB> UNPLUG INTO '/home/
oracle/<PDB>.xml';

SQL> DROP PLUGGABLE DATABASE <PDB>;
```

5. ターゲット CDB に接続し対象の PDB をプラグし、PDB を起動します。

```
SQL> CREATE PLUGGABLE DATABASE <PDB> USING '/home/oracle/.xml'
<COPY|NOCOPY>;

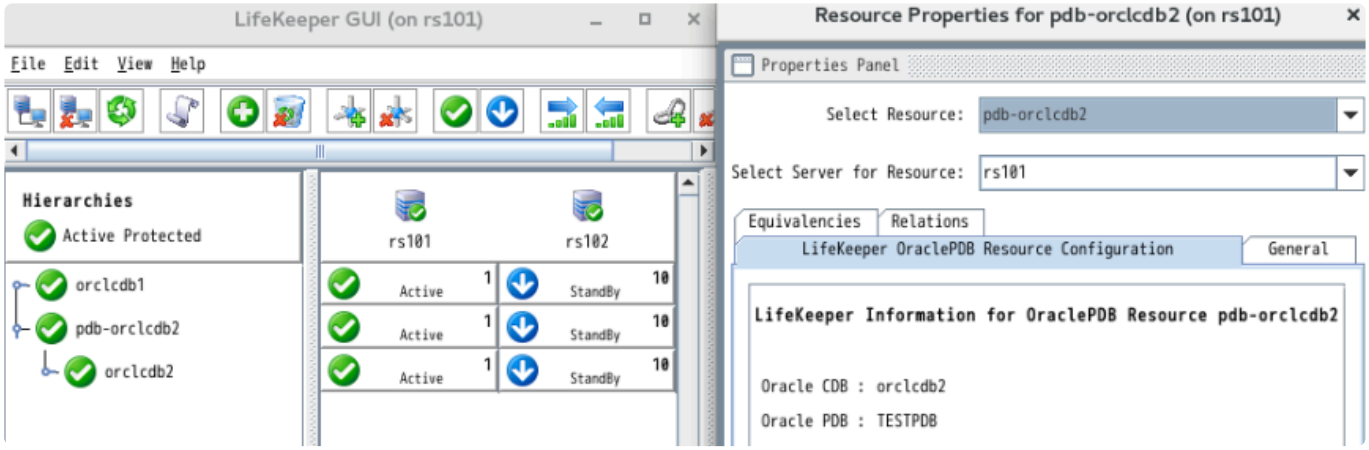
SQL> ALTER PLUGGABLE DATABASE <PDB> OPEN;
```

6. 移行後の PDB の情報が移行前と一致することを確認します。

```
SQL> COLUMN NAME FORMAT A8

     SELECT NAME, DBID, GUID FROM V$CONTAINERS WHERE NAME='<PDB>';
```

7. ターゲット CDB を指定して Oracle PDB リソースを作成します。
   既に PDB を保護している Oracle PDB リソースがある場合は、リソース設定 [Change Protection PDB] (保護するPDBの変更 を参照)で対象の PDB を保護対象に追加して一つのリソースで管理することも可能です。


LifeKeeper GUI (on rs101)
File Edit View Help
Hierarchies
Active Protected
orclcdb1
pdb-orclcdb2
orclcdb2
rs101
rs102
Active 1
StandBy 10
Active 1
StandBy 10
Active 1
StandBy 10
Resource Properties for pdb-orclcdb2 (on rs101)
Properties Panel
Select Resource: pdb-orclcdb2
Select Server for Resource: rs101
Equivalencies
Relations
LifeKeeper OraclePDB Resource Configuration
General
LifeKeeper Information for OraclePDB Resource pdb-orclcdb2
Oracle CDB : orclcdb2
Oracle PDB : TESTPDB

9.3.6.8. Oracle リソース階層のテスト

手動スイッチオーバを開始することによって、Oracle リソース階層をテストできます。これにより、リソースインスタンスのプライマリサーバからバックアップサーバへのフェイルオーバがシミュレートされます。

[編集]、**[リソース]**、**[サービス開始]** の順に選択してください。例えば、バックアップサーバで In Service 要求を実行すると、アプリケーション階層がプライマリサーバ側で out of service になり、バックアップサーバ側では in service になります。この時点で、元のバックアップサーバがプライマリサーバとなり、元のプライマリサーバがバックアップサーバとなります。

Out of Service 要求を実行すると、アプリケーションは他のサーバで in service になることなく out of service になり、Oracle サービスは停止されます。

9.3.7. Oracle 階層の管理

このセクションでは、Oracle 階層の管理について説明します。

9.3.7.1. Oracle 階層の管理に関するガイドライン

Oracle 階層の管理は、以下のガイドラインどおりに行ってください。

- **保護されたコミュニケーションパス経由でアクセスしてください。**ユーザが実行中の物理システムに関わらず確実に Oracle SID にアクセスできるように、データベースのリモートアクセスは、すべて Oracle 階層の一部である保護された名前付きパイプ (LAN Managerの別名) または IP アドレス経由で行う必要があります。スイッチオーバの発生時には、LifeKeeper ではバックアップシステムで利用可能な保護されたコミュニケーションパスを自動的に利用可能にします。

- **Oracle 専用のボリュームを確保してください。**Oracle データベースファイルを含む Oracle 専用のボリュームを確保してください。これらのボリュームは、LAN Manager 経由でアクセスするユーザと共有することはできません。また、他のローカルアプリケーションからアクセスできないように設定する必要があります。これは、リモートユーザがネットワーク経由でボリュームの 1 つにアクセスしている場合や、ローカルのプロセスがボリュームへの書き込みアクセスのためにオープンを行った場合に、例えばフェイルオーバ時にサービスからボリュームリソースを削除する LifeKeeper の動作が失敗することがあるためです。

  ボリュームへの読み取り専用アクセスを行うローカルのプロセスはサービスから実行されるリソースの削除を妨げることはありませんが、読み取り専用アクセスは、リソースの切り替え復帰時に回復失敗の原因となることがあります。読み取り専用アクセスの例としては、各ボリュームを定期的に検査する Performance Monitor や、共有ボリュームにインストールされた稼働中のプロセスがあります。

- **Oracle の起動および停止は、LifeKeeper 経由で実行してください。**Oracle データベースの管理の多くは Oracle ツールを使用して行えますが、Oracle SID の停止には LifeKeeper の [サービス停止] 機能を、Oracle SID の起動には [サービス開始] 機能を使用します。LifeKeeper が SID を停止または起動しても、設定内のすべてのノードのサーバは表示された状態に維持されます。

- **ボリュームリソースを保護してから Oracle SID に追加してください。**環境の規模が大きくなり、すでに LifeKeeper の保護下にある Oracle SID に新しいボリュームを追加する必要が生じた場合は、以下の手順を実行してください。

1. 初めに、ボリュームを保護してください (ボリュームリソースを作成します)。

2. そのボリュームを SID に追加します。

3. Oracle リソースとボリュームリソース間の依存関係を手動で作成します。

9.3.7.2. LifeKeeper Oracle Recovery Kit の変数

LifeKeeper Oracle Recovery Kit のインストールでは、3 つのレジストリエントリ変数が作成され、次のレジストリキーに格納されます。

```
HKEY_LOCAL_MACHINE\SOFTWARE\SIOS\LifeKeeper\RK\ORAapp
```

MAXWAIT は、1 つの Oracle サービスが起動または停止するときに Recovery Kit が待機する秒数を指定する 10 進数の整数です。指定した秒数以内にサービスが開始または停止しない場合、LifeKeeper では Failed(失敗) ステータスとなります。_MAXWAIT_ のデフォルト値は **300** ですが、非常に大きなデータベースの場合、データベースサービスが_開始_または_停止_状態に達するのに 300 秒では十分でないことがあります。その場合、レジストリエントリを適切な値に変更してください。

RESTORE_DEEPCHK_MAX_RETRY は、リストアまたはリカバリ操作中に Oracle サービスの状態の確認を複数回試行するのに使われる 10 進数の整数です。予想外にロードが重いサーバー上では、保護された Oracle サービスが実行中状態であることを確認するのに、サービスの状態を確認するデフォルトの回数は必ずしも十分ではない場合があります。この変数のデフォルト値は 0 で通常各サービスに対して Oracle サービス状態の確認は 1 回のみ行われます。この回数を増やす必要がある場合は値を変更することができます。

RESTORE_DEEPCHK_SLEEP は、リストアまたはローカルリカバリ操作中に Oracle サービス状態確認の追加試行にスリープ間隔を挿入します。10 進数の整数で、秒数で計測されます。このオプションは上記の RESTORE_DEEPCHK_MAX_RETRY オプションが使用されている場合に有効です。この変数のデフォルト値は 0 で通常 Oracle サービス状態の追加確認試行にスリープ時間は設定されません。
RESTORE_DEEPCHK_MAX_RETRY 変数を設定した場合は、RESTORE_DEEPCHK_SLEEP 変数も同様に設定し、Oracle サービス状態確認の信頼性とパフォーマンスを強化することを強くお勧めします。

9.3.7.3. LifeKeeper で使用する Oracle ユーザ名とパスワードの更新

LifeKeeper Oracle リソースの作成中、Oracle ユーザ名とパスワードをその Oracle のインスタンスに入力する必要があります。将来入力したユーザ名のパスワードを変更する場合は、クラスタ内のすべてのシステムの LifeKeeper Oracle リソースを新しいパスワードで更新する必要があります。更新しない場合、Oracle リソースは同期外となり、サービス開始、停止を正しく行うことができなくなります。LifeKeeper は、その後のフェイルオーバまたは手動スイッチオーバ時にリソースの削除または復元ができなくなることを示すエラーメッセージを、**アプリケーションイベントログ** に記録します。

LifeKeeper GUI には、Oracle リソースに関連付けたユーザアカウントを管理するインターフェースがあります。詳細については、Oracle データベースの設定管理 を参照してください。

9.3.7.4. 手動による Oracle 11g DB Console の設定

サービスがクラスタ内のすべてのシステムで正常に開始するように、保護された仮想 IP アドレスまたは LAN Manager の別名を使用するには、Oracle 11g DB Console を手動で設定する必要があります。

プライマリサーバ上で、**<ORACLE_HOME>\<SYSTEM_NAME>_<ORACLE_SID>\sysman\config\emoms.properties** を編集してください。

プロパティの **oracle.sysman.emSDK.svlt.ConsoleServerHost** =<仮想 IP アドレス> または <LAN Manager の別名> を設定してください。

9.3.8. Oracle のトラブルシューティングのヒント

このセクションでは、LifeKeeper ソフトウェアには特別な関係がない、全体的な環境に関連する現象についての解決策と考えられる原因を提示します。

9.3.8.1. 階層の作成に失敗した

解決策

以下を確認してください。

- SID に関連付けられているすべてのボリュームリソースおよび通信リソース (IP または LAN Managerあるいはその両方) がすでに LifeKeeper の保護下に置かれている。
- すべての共有ボリュームまたは複製ボリュームがプライマリサーバで使用可能で、すべてのボリュームが各サーバ上で同じドライブレターにマップされている。

9.3.8.2. サービス開始に失敗した

解決策

サービス開始を行おうとしたシステムで他の Oracle リソースがサービス中になっているかどうか、またはそのシステムから共有ボリュームにアクセスできること (あるいはその両方) を確認します。

Oracle サービスの状態が実行中か追加で確認する必要がある場合、レジストリの LifeKeeper Oracle Recovery Kit 変数を使ってサービス開始の回数を増やすことを検討してください。LifeKeeper Oracle Recovery Kit の変数

9.3.8.3. Oracle TNSListener Service が必要に応じて起動または停止しない

解決策

以下を実行してください。

- 少なくとも 1 つの TCP/IP または LAN Manager リソースが Oracle 階層に含まれているかどうかを確認します。
- 階層をサービス停止にしてからサービス中に戻し、*Oracle<OraHome>TNSListener<SID>* を開始します。

9.3.8.4. サーバが応答しない

LifeKeeper によるスイッチオーバが正常に完了した後に TCP/IP クライアントからサーバにアクセスできない (サーバが応答しない)

考えられる原因

クライアントシステムのアドレス解決プロトコル (arp) が使用する物理 IP アドレス変換テーブルに古い情報が残っている。

解決策

サーバへのアクセスに使用する IP アドレスを再設定する必要があります。アドレスを再設定するには、arp -d server_ip_address コマンドを実行してください。この操作によって、変換テーブルからアドレスが削除されます。その IP アドレスの次の要求に応じて、テーブル記入項目が記入されます。

9.3.8.5. リモートユーザが ORA 12504、ORA 12514、ORA 12541 の理由でログインできない

考えられる原因

Oracle の接続の問題は、LifeKeeper によって発生するわけではなく Oracle TNS セットアップの問題です。

解決策

以下を実行してください。

- Oracle のエラーおよびメッセージを確認確認します。
- **Oracle Net Manager** を使用して、リスナ名と TNS 名が正しく設定されていることを確認します。
- サービスが IP または LAN Manager の別名を使用して正しく設定されていることを確認します。
- TNSPING を使用してサービスにアクセスします。

9.4. はじめに SIOS Protection Suite Microsoft Internet Information Services

SIOS Protection Suite Microsoft Internet Information Services

SIOS Protection Suite Microsoft IIS Recovery Kit は、インターネットサーバに特定の保護機能を追加することで、SIOS Protection Suite 製品を拡張します。SIOS Protection Suite Microsoft IIS Recovery Kit は、インターネットサーバの状態を継続的に監視し、問題が発生した場合には、問題の影響を受けたサイトをスタンバイシステムに自動的にフェイルオーバします。Microsoft IIS Recovery Kit は、Web、FTP および SMTP サイトを保護します。複数の IIS リソースが設定されている場合は、Web、FTP、または SMTP サイトを個々に停止 / 開始できます。

9.4.1. IIS の概要

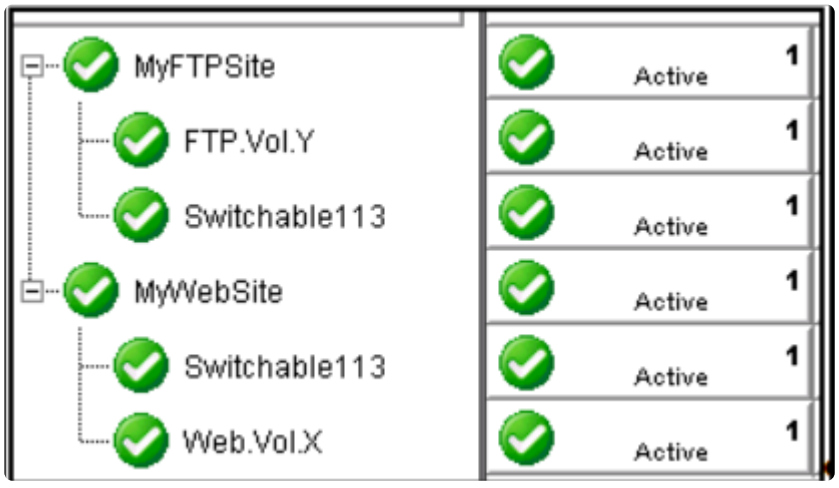
SIOS Protection Suite Microsoft IIS Recovery Kit は、次の問題が発生しないようにインターネットサーバを保護します。

- システム障害またはサーバ停止
- ネットワークインターフェースカード (NIC) 障害
- 通信障害 (Web サーバは稼働するが、応答しない)
- スタートアップ障害 (スタートアップ時に Web サーバが停止状態になる)

SIOS Protection Suite Microsoft IIS Recovery Kit には 2 つのリカバリ手順があります。システム障害または NIC 障害の場合は、Recovery Kit が問題の Web サーバの IP アドレスをスタンバイシステムに転送して、スタンバイ Web サーバを起動します。通信障害またはスタートアップ障害が発生し、ローカルのリカバリが有効な場合、SIOS Protection Suite Microsoft IIS Recovery Kit は、問題の影響を受けた Web サーバを最初に停止させ、再起動して、問題が解決するかどうかを調べます。Recovery Kit は再起動に失敗すると、サービスをバックアップ Web サーバにフェイルオーバします。

SIOS Protection Suite Microsoft IIS Recovery Kit は、IIS アプリケーション、IP、ボリュームリソース間の依存関係を管理します。最初に、Web サーバで使用する IP リソースとボリュームリソースを作成します。次に IIS リソースを作成すると、SIOS Protection Suite Microsoft IIS Recovery Kit が Microsoft IIS 設定を読み取って、IIS リソースと IP/ ボリュームリソース間に必要な依存関係を自動的に作成します。

次に示すのは LifeKeeper の GUI に表示される IIS 階層の例です。Web サイトには、「Switchable113」という IP アドレスと「WEB.Vol.X」というボリュームの両方に依存関係があり、ここの Web サイトのコンテンツを含んだホームディレクトリが常駐しています。IP リソースとボリュームリソースはいずれも、この Web サイトを作成する前に作成されたものです。



9.4.2. IIS のインストール

このセクションでは、LifeKeeper Microsoft IIS Recovery Kit のインストールについて説明します。

ハードウェアとソフトウェアの要件

キットのインストール

キットの削除

構成の定義と制限

IIS 構成の考慮事項

LifeKeeper とともに IIS をインストールおよび設定する

SIOS Protection Suite およびリカバリキットのインストールと設定

全サーバでの Microsoft IIS のインストールと設

SMTP 仮想サーバのインストールと設定

9.4.2.1. ハードウェアとソフトウェアの要件

SIOS Protection Suite Microsoft IIS Recovery Kit のインストールまたは削除を試みる前に、設定が以下の要件を満たしていることを確認してください。

- **オペレーティングシステムソフトウェア。** サポートされるオペレーティングシステムについては SIOS Protection Suite for Windows サポートマトリックス を参照してください。
- **SIOS Protection Suite ソフトウェア。** 各サーバに同じバージョンの SIOS Protection Suite ソフトウェアとすべてのパッチをインストールする必要があります。具体的な要件については、*リリースノート* を参照してください。
- **SIOS DataKeeper ソフトウェア (オプション)。** 共有ストレージではなく複製ボリュームで IIS を使用する計画を立てている場合は、SIOS DataKeeper for Windows ソフトウェアを各サーバ上にインストールする必要があります。
- **SIOS Protection Suite IP Recovery Kit。** 各サーバ上に SIOS Protection Suite IP Recovery Kit をインストールしておく必要があります。その IP Recovery Kit のすべての TCP/IP 設定要件は、SIOS Protection Suite Microsoft IIS Recovery Kit にも該当します。
- **IP ネットワークインターフェース。** 各サーバに、最低 1 つの TCP/IP 対応ネットワークインターフェースが必要です。IP 切り替えを正しく機能させるためには、ローカルネットワークに接続されたユーザシステムが標準の TCP/IP 仕様に準拠している必要があります。

注記: 各サーバに必要なネットワークインターフェースは 1 つのみですが、スループット要件、単一障害点の排除、ネットワークセグメンテーションなどのいくつかの理由で複数のインターフェースを使用する必要があります。

- **TCP/IP プロトコル。** サーバごとに TCP/IP をインストールし、正しく設定する必要があります。
    - 2 つのサーバが、同一の LAN セグメント上に存在する (つまり、2 つのシステムの間にルータがない) 必要があります。
    - SIOS Protection Suite 階層を作成するための空きの IP アドレスが必要です。
        - アクティブな Microsoft IIS サイトごとに、アクティブ IIS サイトとスタンバイ IIS サイトの間で共有する切り替え可能な IP アドレスが 1 つ必要です。
        - 複数の Microsoft IIS サイトを保護する場合は、保護対象の IIS リソースごとに追加の IP アドレスが必要です。
- **IIS ソフトウェア。** IISリカバリーキットはサポートされている Microsoft Windows のすべてのバージョンで、IIS のネイティブバージョンをサポートしています。

    SIOS Protection Suite および SIOS Protection Suite Microsoft IIS Recovery Kit を設定する前に、Microsoft IIS ソフトウェア、IIS サーバーロール、FTP 機能、または SMTP 機能をインストールして構成す

る必要があります。同じバージョンを各サーバーにインストールする必要があります。各サーバーにインストールする必要がある要件については、IIS の必要な役割、役割サービス、および機能 を参照してください。

9.4.2.2. キットのインストール

SIOS Protection Suite Microsoft IIS Recovery Kit は CD-ROM または FTP ダウンロードで提供される SIOS Protection Suite for Windows コア製品に含まれています。

9.4.2.3. キットの削除

注意: Recovery Kit を削除する前に、必ずすべての SIOS Protection Suite IIS リソースをサービスから削除してください。キットが削除されると、これらのリソースは使用できなくなります。

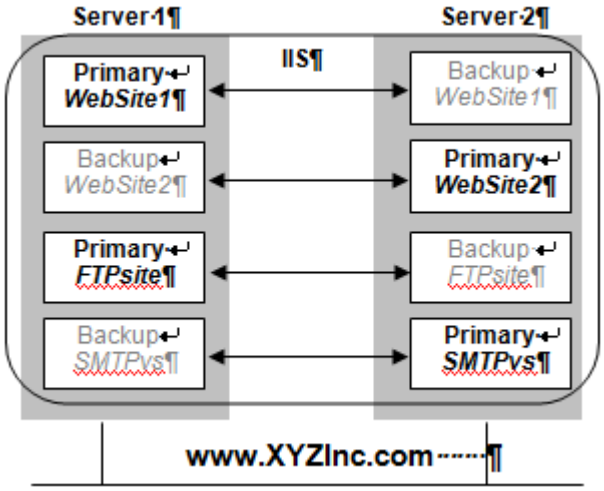
SIOS Protection Suite Microsoft IIS Recovery Kit は SIOS Protection Suite for Windows コア製品に含まれており、このコア製品を削除するとアンインストールされます。

9.4.2.4. 構成の定義と制限

アクティブ/アクティブ構成

IIS では、1 つのクラスタ内の各サーバで複数の Web/FTP サイトと SMTP 仮想サーバを動作させることができます。1 つのシステムで許可される (または必要とされる) IIS ソフトウェアのインスタンスは 1 つのみです。LifeKeeper では、Web サイト、FTP サイト、SMTP 仮想サーバを個々に保護し、管理できます。これ以降の説明では、Web サイト、FTP サイト、SMTP 仮想サーバを意味する一般用語として「サイト」を使用します。

次の図は、Web サーバの標準構成を図示したものです。



この構成では、各サーバに 2 つの Web サイト、すなわち、1 つのプライマリ Web サイトと 1 つのバックアップ Web サイトがあります。サーバ1 には *WebSite1* のプライマリインスタンスと *WebSite2* のバックアップインスタンスがあります。サーバ2 は逆の構成、つまり *WebSite2* のプライマリインスタンスと *WebSite1* のバックアップインスタンスの構成になっています。ある特定のサーバでユーザ要求のサービスを実際に行うのは Web サイトのプライマリインスタンスのみです。

また、サーバ 1 には、_FTPsite_ という名前の FTP サイトのプライマリインスタンスと *SMTPvs* という名前の SMTP 仮想サーバのバックアップインスタンスがありますが、サーバ 2 には FTP サイトのバックアップインスタンスと SMTP 仮想サーバのプライマリインスタンスがあります。

プライマリの Web サイトがユーザ要求のサービスを中止すると、LifeKeeper は、バックアップサーバ上のバックアップインスタンスをアクティブにして、サービスを引き継がせます。そのため、サーバ1 の *WebSite1* に障害が発生すると、LifeKeeper はサーバ 2 にある *WebSite1* バックアップインスタンスをアクティブにします。このスイッチオーバの後に、サーバ2 で 2 つのアクティブインスタンスが動作します。障害が発生した Web サーバの問題が解決したら、サービスをサーバ 1 に戻すことができます。LifeKeeper Microsoft IIS Recovery Kit では、サービスを手動でスイッチバックできるほか、LifeKeeper の自動スイッチバック機能を使用できます。

9.4.2.5. IIS 構成の考慮事項

LifeKeeper では、インターネットサーバ設定に関して一定の制限を設けています。これらの制限によって、スタンバイ Web サーバ/サイトが正しく完全にアクティブ Web サーバ/サイトと切り替わります。

デフォルト Web サイトおよび新規 Web サイト

IIS のインストール処理によって作成されたデフォルト Web サイトを LifeKeeper で保護するには、小さな設定変更を 1 つ行います。デフォルト Web サイトを再設定して、サイトに LifeKeeper で保護された IP アドレスを使用する必要があります。

また、サイトに LifeKeeper で保護された IP アドレスを使用するように設定されている新規の Web サイトも、LifeKeeper で保護することができます。

プライマリとバックアップの指定

アクティブサイトの作成先のサーバがこの Web サイト用のプライマリ LifeKeeper サーバになります。スタンバイサイトの作成先のサーバがこのサイト用のバックアップサーバになります。「プライマリ」サーバと「バックアップ」サーバの指定が設定対象のサイトごとに異なることを念頭に置いてください

命名規約

LifeKeeper 保護を可能にするには、次のサイト名規則を使用する必要があります (名前は IIS コンソールの [説明] フィールドに入力する)。

- 英数文字およびダッシュのみを使用してください (スペースは使用できない)。
- 保護対象の Web サイトの名前 (説明) を変更する必要がある場合は、最初に、LifeKeeper IIS リソースを削除してから、説明を変更し、リソースを作り直してしてください。

同一のプライマリ/バックアップ Web サイト

プライマリ IIS サイトごとに、他方のサーバに同じバックアップ IIS サイトを作成する必要があります。これらの 2 台のサーバを LifeKeeper ハートビートで接続する必要があります。プライマリサイトとバックアップサイトを同じにするには、次の基準を満たす必要があります。

- [プロパティ] フォームの *[説明]* フィールドに、大文字、小文字の区別も含めて同じサイト名を入力する必要があります。
- プロパティフォームのサイトに割り当てられている切り替え可能な IP アドレス、ポート、ヘッダは同じにしてください。
- Web または FTP コンテンツ用に共有または複製ボリュームを使用する場合には、*[ホームディレクトリのパス]* フィールドに割り当てるボリュームのドライブレターとフォルダを同じにする必要があります。

- 特定の Web サイトに対して、複数のバックアップサイトを設定する場合は、他の Web サイトにも同じ ID を設定する必要があります。すなわち、プライマリおよびバックアップの Web サイトは同一の IP アドレス、ポートおよびヘッダを含んでいる必要があります。

- 一方の Web サイトを安全な Web サイトとして設定する場合には、他方の Web サイトも安全な Web サイトとして設定する必要があります。安全な Web サイトには、別の制限が適用されます。詳細については、以下のセクションを参照してください。

安全なサーバの構成

安全なサーバとは、通信で SSL (Secure Socket Layers) を使用する Web サーバです。送受信されるデータが暗号化され、また、Web クライアントと Web サーバが互いに相手を識別できるため、セキュリティが向上します。安全なサーバでは、URL に *http:* ではなく *https:* を使用します。安全なサーバのデフォルトのポート番号は 443 です。

LifeKeeper Microsoft IIS Recovery Kit と LifeKeeper は、安全な IIS Web サイトを稼働させる方法に違いはありません。実際、IIS では、同じ Web サイトに TCP ポートと SSL ポートの両方を設定できます。スタートアップ手順や操作手順は変わりません。そのため、キーが生成され、該当のデジタル署名が IIS にインストールされたら、SSL ポートを設定して、動作させることができます。

IIS 設定

LifeKeeper 保護を確実にするためには、次の構成規則を守る必要があります。

- IP アドレスが [プロパティ] フォームまたは [バインディング] フォームの [IP アドレス] のフィールドに指定されていない IIS サイトを保護することはできません。
- Web コンテンツで共有または複製ボリュームを使用している場合には、「このコンピュータ上のディレクトリ」として、ホームディレクトリを指定する必要があります。次のいずれかとして指定している場合、LifeKeeper はホームディレクトリを保護できません。
    - 別のコンピュータ上での共有
    - URL へのリダイレクト
    - LifeKeeper で保護されていないボリューム

ドキュメントコンテンツの場所

共有および複製コンテンツストレージ

コンテンツボリュームが共有または複製ボリューム上にある場合は、両方の Web サイトが同じ共有または複製ボリュームおよびフォルダを指定する必要があります。アクティブとスタンバイの Web サーバ / サイトを同じにするには、プライマリサーバとバックアップサーバに同じコンテンツファイルを含める必要があります。ただし、コンテンツボリュームの共有または複製を行わない場合は、コンテンツはいずれかのシステムの任意の場所に配置できます。

フェイルオーバ時にデータを確実に使用できるようにするには、プライマリサーバ上の共有ディスクまたは複製されたディスク上のフォルダとしてホームディレクトリを設定し、プライマリサーバと同じホームディレクトリをバックアップサーバ上に設定してください。これにより、コンテンツファイルの 1 つのコピーのみをメンテナンスできます。

非共有ストレージ

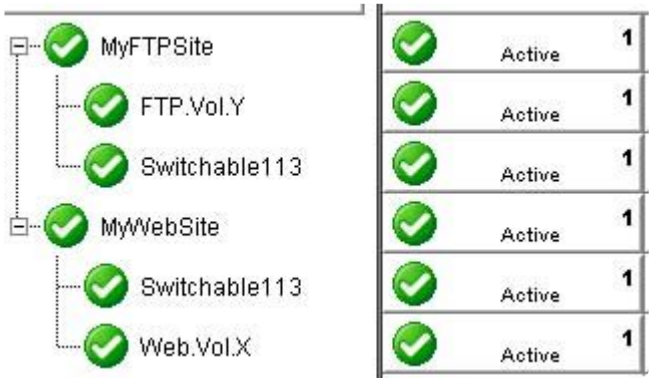
設定で共有ストレージを使用しない場合には、それぞれのサーバ上のローカルボリューム間でコンテンツを同期する必要があります。LifeKeeper Microsoft IIS Recovery Kit には、2 つのサーバ間でコンテンツを同期する機能はありませんが、以下のように、いくつかの推奨事項があります。

- SIOS DataKeeper を使用すると、自動的に各アクティブサーバ上のデータボリュームをスタンバイサーバにコピーします。
- Microsoft Site Server 3.0 などのコンテンツコピーツールを使用してください。コンテンツコピーツールとして、*Robocopy* ユーティリティも使用できます。Microsoft Site Server のほうが推奨されます。
- テープバックアップシステムを使用している場合にはプライマリサーバにファイルのテープバックアップを作成してから、それらを必要に応じてバックアップサーバ上に復元します。

複数の IIS サイトで異なるボリュームを使用する

LifeKeeper Microsoft IIS Recovery Kit は、IIS リソース階層を作成するときに、IIS の構成として指定された IP アドレスとホームディレクトリのパスを使用してコンテンツボリュームに関連する依存関係を作成します。複数のサイトを保護する場合は、サイトごとに異なる IP アドレスおよびボリュームを指定してください。

例として、次の階層に、同じ IP アドレスおよび異なるボリュームリソースを使用する *MyFTPSite* および *MyWebSite* を示します。一方のサイトで行うメンテナンスは、もう一方のサイトに影響します。これは、両サイトに共通の IP リソース依存関係があるためです。



バックアップサーバ上で *MyFTPSite* をサービス開始にすると、その依存関係もバックアップサーバに移動します。これにより、_MyWebSite_ はプライマリサーバ上でサービス停止になります。その場合、バックアップサーバ上で *MyWebSite* をサービス状態に手動で戻す必要があります。

保護された IIS サイトごとに異なる IP アドレスとボリュームを割り当てると、個別管理が可能になるため、リソースを柔軟に管理できます。ただし、上記の図のようにそれらをグループとして管理するほうが適している場合もあります。

9.4.2.6. LifeKeeper とともに IIS をインストールおよび設定する

次に進む前に、このガイドの前の章での推奨事項に従ってストレージとネットワークの設定を済ませておく必要があります。

インストールのチェックリスト

インストールおよびセットアップのシーケンスは、以下の順序で実行される必要があります (各手順の詳細については、他のトピックを参照してください)。

1. 複製ボリュームを使用している場合は、各サーバに SIOS DataKeeper をインストールして、ミラーを作成します。

2. LifeKeeper IP Recovery Kit および LifeKeeper Microsoft IIS Recovery Kit を含む LifeKeeper Core を各サーバにインストールして、設定します。

3. すべてのサーバで Microsoft IIS をインストールして、設定します。

SIOS DataKeeper のインストールとミラーの作成

複製ボリュームを使用する場合は、ここで Windows ソフトウェア用の SIOS DataKeeper をインストールしてミラーを作成する必要があります。詳細については、SIOS Protection Suite インストレーションガイド を参照してください。

9.4.2.7. SIOS Protection Suite およびリカバリキットのインストールと設定

次の手順では、IP Recovery Kit および Microsoft IIS Recovery Kit を含む SIOS Protection Suite をすべてのサーバにインストールします。SIOS Protection Suite のインストールの詳細については、SIOS Protection Suite のインストール のトピックを参照してください。すべてのサーバに、同じバージョンの SIOS Protection Suite をインストールする必要があります。

LifeKeeper をインストールした後で、すべてのサーバを再起動する必要があります。再起動したら、すべてのサーバ上で LifeKeeper が稼働していることを確認してください。

これで、LifeKeeper を設定できるようになりました。以下に、LifeKeeper のセットアップ作業の正しい順番を示します。LifeKeeper の設定作業の詳しい説明については、**[ヘルプ]** ボタンをクリックするか、LifeKeeper の設定 を参照してください。

> DataKeeper を使用している場合、シャットダウンとともにリソースを切り替える設定はサポートしていません。詳細は サーバのシャットダウン方法の設定 を参照してください。

1. LifeKeeper コミュニケーションパスを設定してください。最大の信頼性が得られるようにコミュニケーションパスを設定するには、2 つの別々のコミュニケーションパス (可能であれば 3 つ) を作成してください。TCP/IP コミュニケーションパスの場合、2 つのサーバ間でプライベートネットワークを使用した際に最も良い結果が得られます。

2. 必要に応じて、各 Web サーバ / サイトのペアに切り替え可能な IP アドレスを作成します。**[編集]** メニューの **[サーバ]** から **[リソース階層の作成]** を選択します。ドロップダウンリストから **IP アドレス** を選択して、**保護対象アプリケーションウィザード** に必要な情報を入力します。必要に応じて、それぞれの切り替え可能 IP アドレスについて繰り返してください。

   LifeKeeper 切り替え可能 IP アドレスを作成するときは、以下の点を考慮してください。

   a. プライマリサーバとは、通常はアクティブな Web サーバ / サイトを実行するサーバです。これは優先順位を 1 に設定して、IP リソースが後で作成される IIS リソースと一致するようにする必要があります。

   b.必要に応じて、スイッチバックストラテジーを *[インテリジェント]* (デフォルト) から *[自動]* に変更します。

   c.同じサブネット上に 2 つの NIC がある場合は、IP ローカルリカバリ* オプションを設定して、LifeKeeper に 2 つのカード間で切り替え可能な IP アドレスのサービスを移動させるようにすると、可用性を高めることができます。

   スイッチバックストラテジー および IP ローカルリカバリ の詳細については、関連のトピックを参照してください。

4. 切り替え可能な IP アドレスの切り替えと応答をテストします。

    a. 切り替えのテストを行うには、LifeKeeper GUI を起動してください。切り替え可能な IP アドレスは、プライマリサーバでは緑 (アクティブ)、バックアップサーバでは青 (スタンバイ) で表示されます。階層ツリー内の IP インスタンスを右クリックし、ポップアップメニューから [サービス開始] を選択して、リストボックスからバックアップサーバを選択してください。この切り替え可能 IP リソースは、バックアップサーバ上で青から緑に変わります。残りのすべての切り替え可能 IP アドレスに対して、このテストを繰り返してください。すべての切り替え可能 IP アドレスのテストが完了したら、プライマリサーバ上でこれらをサービス中に戻してください。

    b. 応答のテストを行うには、MS-DOS ウィンドウを開いて、各切り替え可能 IP アドレスに対して ping コマンドを実行してください。切り替え可能 IP アドレスからは、ping に対して応答時間とパケットロス値が返されます。

    c. 切り替え可能 IP アドレスが切り替えと ping のテストに合格するまで、先に進まないでください。

5. Web/FTP/SMTP サービスのためのホームディレクトリを含むボリュームリソースを作成します。ボリュームリソース切り替えを実行して、ボリュームがプライマリサーバとバックアップサーバ上でサービス中の状態になることを確認してください。また、保護対象の IP およびボリュームリソースに割り当てた優先順位が、各サーバ上で一致していることを確認してください。

9.4.2.8. 全サーバでの Microsoft IIS のインストールと設定

次の手順では、クラスタ内のすべてのサーバ上に Microsoft IIS を設定します。

Microsoft IIS Web または FTP サイトのインストールおよび設定

Web サイトまたは FTP サイトのペアを作成するには、各サーバ上に新規のサイトを追加して、ペアが同じになるように設定する必要があります。または、デフォルトの Web または FTP サイトの保護を選択することもできます。

1. LifeKeeper GUI を使用して、プライマリサーバ上で切り替え可能な IP アドレスと保護対象ボリューム (存在する場合) をサービス中の状態にします。

2. [プログラム] メニューの [管理ツール] から、Internet Information Services (IIS) Manager を起動します。このインターフェースを使用して、プライマリおよびバックアップサイトを作成します。

3. [新しい Web サイト] ウィザードを起動して、「サイト名」または「説明」を入力します。プライマリおよびバックアップサーバの両方を同じ名前にする必要があることに留意してください。

4. **Web サイトのみ:** [TCP ポート] と [ホストヘッダ] のフィールドに入力してください。プライマリサーバとバックアップサーバで、これらが同じになるようにしてください。

5. Web サイトの切り替え可能 IP アドレスを選択するか、または入力します。サービス停止の状態の場合は、保護対象の切り替え可能 IP アドレスはドロップダウンリストに表示されないことがありますが、入力することは可能です。プライマリサーバとバックアップサーバでは、Web サイトの IP アドレスは同じである必要があります。

#6Web サイトのみ: 複数の ID を持つ Web サイトを設定する場合は、すべての ID の [IP アドレス] フィールドに切り替え可能 IP アドレスを入力してください。

7. サイトのホームディレクトリや物理パスをローカル (LifeKeeper によって保護されない) にすることができます。または、LifeKeeper の共有ストレージや複製ストレージを使用することができます。共有ストレージまたは複製ストレージを使用する場合は、ボリュームがサービス中の状態で、このディレクトリがすでに存在している必要があります。

8. **Web サイトのみ:** Web サイトのアクセス権を選択します。

9. Microsoft IIS サイトが起動されていることを確認し、バックアップサーバ上での Web サイト設定に進む前に、テストを行ってサイトがアクセス可能で正しく機能しているかどうかを確認します。

10. LifeKeeper GUI を使用して、バックアップサーバ上で切り替え可能な IP アドレスと保護対象ボリューム (存在する場合) をサービス中の状態にします。

11. 手順 2 から 10 を繰り返して、バックアップサーバ上にサイトを作成します。プライマリサーバとバックアップサ

ーバでは、Web または FTP サイトペアは同じでなければならないことに留意してください。

すべての IIS サイトを作成して設定したら、次の操作を行ってください。

1. LifeKeeper GUI を使用して、プライマリサーバ上で切り替え可能な IP アドレスと保護対象ボリューム (存在する場合) をサービス中の状態にします。

2. Internet Information Services (IIS) Manager を使用して、プライマリサーバ上のプライマリサイトを開始し、バックアップサーバ上のバックアップサイトを停止します。

注記: LifeKeeper で保護される IP アドレスが該当のサーバ上でサービス中でない場合でも、Microsoft の IIS 管理コンソールの画面には、サイトで使用可能なすべての IP アドレスが表示されることがあります。これは Microsoft 管理コンソールスナップインのバグです。ただし、運用上の影響はありません。

保護対象の FTP サイトで匿名ログインを許可していない場合は、LifeKeeper のディープチェックプロセスを、匿名ではないログインを実行するように設定する必要があります。詳細については、匿名接続を使用できない FTP サイトを保護する場合 を参照してください。

SMTP 仮想サーバを作成する場合は、SMTP 仮想サーバのインストールと設定 に進んでください。それ以外の場合は、すでに 1 つまたは複数の IIS リソース階層を設定することによってインターネットサーバに LifeKeeper の保護を追加する準備ができています。

9.4.2.9. SMTP 仮想サーバのインストールと設定

SMTP 仮想サーバを作成するには、以下の手順を実行してください。それぞれのシステムに新しい仮想サーバを追加して、ペアが同じになるように設定する必要があります。

1. LifeKeeper GUI を使用して、プライマリサーバ上で切り替え可能な IP アドレスと保護対象ボリューム (存在する場合) をサービス中の状態にします。

2. SMTP サイトのために、[プログラム] メニューの [管理ツール] から、Internet Information Services (IIS) Manager を起動します。このインターフェースを使用して、プライマリおよびバックアップの SMTP 仮想サーバを作成します。

3. サーバ名を選択して [新しい Web サイト] ウィザードを起動し、[操作] メニューで [新規]、[SMTP 仮想サーバ] の順に選択します。

4. サイトの説明を入力します。このとき、プライマリサーバとバックアップサーバの両方の説明が同じでなければならないことに留意してください。

5. 「この Web サイトに使用する IP アドレスを選択してください」というプロンプトが表示されたら、SMTP 仮想サーバ用の切り替え可能 IP アドレスを選択します。これは、プライマリサーバとバックアップサーバで同じにしてください。

6. ホームディレクトリのパスのプロンプトが表示されたら、ファイル共有を選択するか、共有または複製ストレージデバイス上のボリュームを選択します。

7. この仮想サーバのデフォルトドメインを入力します。

8. SMTP 仮想サーバが起動されていることを確認し、バックアップサーバ上での設定に進む前に、テストを行ってサイトがアクセス可能で正しく機能しているか確認します。

9. LifeKeeper GUI を使用して、バックアップサーバ上で切り替え可能な IP アドレスと保護対象ボリューム (存在する場合) をサービス中の状態にします。

10. 手順 2 から 9 を繰り返して、バックアップサーバ上にサイトを作成します。プライマリサーバとバックアップサーバで、サイトペアが同じでなければならないことに留意してください。

すべての SMTP 仮想サーバを作成して設定したら、以下のようにプライマリサイトを開始し、バックアップ Web サイトを停止してください。

1. LifeKeeper GUI を使用して、プライマリサーバ上で切り替え可能な IP アドレスと保護対象ボリューム (存在する場合) をサービス中の状態にします。

2. Internet Information Services (IIS) Manager を使用して、プライマリサーバ上のプライマリ SMTP サイトを開始します。

これで、1 つまたは複数の IIS リソース階層を作成してインターネットサーバに LifeKeeper の保護を追加する準備

ができました。

9.4.3. IIS の構成の定義と制限

このセクションでは、SIOS Protection Suite Microsoft Internet Information Services Recovery Kit の構成方法について説明します。

IIS の必要な役割、役割サービス、および機能

IIS アクティブ / アクティブ設定

プライマリとバックアップの指定

命名規約

同一のプライマリ/バックアップ Web サイト

安全なサーバの構成

IIS 設定

ドキュメントコンテンツの場所

複数の IIS サイトで異なるボリュームを使用する

9.4.3.1. IIS の必要な役割、役割サービス、および機能

IIS に対するLifeKeeper インターフェースは、サーバにインストールする以下の役割、役割サービス、および機能を必要とします。

役割

- Web Server (IIS)

役割サービス

- IIS Management Console
- FTP Server (FTP サイトを保護する場合)
- FTP Service

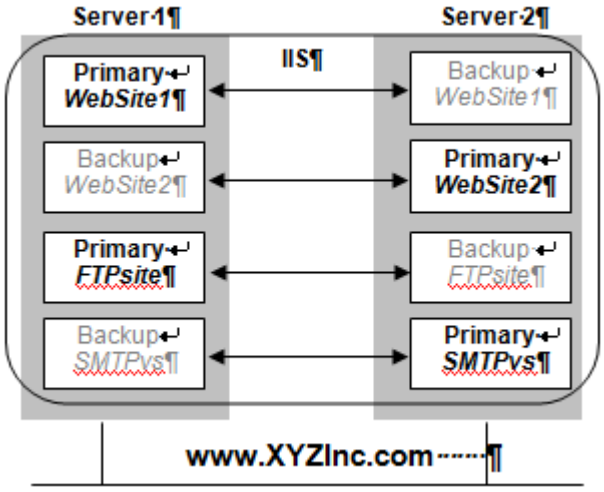
機能

- SMTP Server (SMTP サイトを保護する場合)

9.4.3.2. IIS アクティブ / アクティブ設定

IIS では、1 つのクラスタ内の各サーバで複数の Web/FTP サイトと SMTP 仮想サーバを動作させることができます。1 つのシステムで許可される (または必要とされる) IIS ソフトウェアのインスタンスは 1 つのみです。Web サイト、FTP サイト、および SMTP 仮想サーバは、LifeKeeper によって個別に保護し、管理することができます。以下の説明では「サイト」という用語で Web サイト、FTP サイト、および SMTP 仮想サーバを総称的に示します。

次の図は、Web サーバの標準構成を図示したものです。



この構成では、各サーバに 2 つの Web サイト、すなわち、1 つのプライマリ Web サイトと 1 つのバックアップ Web サイトがあります。サーバ1 には *WebSite1* のプライマリインスタンスと *WebSite2* のバックアップインスタンスがあります。サーバ2 は逆の構成、つまり *WebSite2* のプライマリインスタンスと *WebSite1* のバックアップインスタンスの構成になっています。ある特定のサーバでユーザ要求のサービスを実際に行うのは Web サイトのプライマリインスタンスのみです。

また、サーバ 1 には、FTP サイトという名前を持つ FTP サイトのプライマリインスタンスと *SMTPvs* という名前を持つ SMTP 仮想サーバのバックアップインスタンスがありますが、サーバ 2 には FTP サイトのバックアップインスタンスと SMTP 仮想サーバのプライマリインスタンスがあります。

プライマリの Web サイトがユーザ要求のサービスを中止すると、LifeKeeper は、バックアップサーバ上のバックアップインスタンスをアクティブにして、サービスを引き継がせます。そのため、サーバ1 の *WebSite1* に障害が発生すると、LifeKeeper はサーバ 2 にある *WebSite1* バックアップインスタンスをアクティブにします。このスイッチオーバの後に、サーバ2 で 2 つのアクティブインスタンスが動作します。障害が発生した Web サーバの問題を解決した後、サービスをサーバ 1 に戻すことができます。LifeKeeper Microsoft IIS Recovery Kit では、サービスを手動でスイッチバックできるほか、LifeKeeper の自動スイッチバック機能を使用できます。

9.4.3.3. プライマリとバックアップの指定

アクティブサイトの作成先のサーバがこの Web サイト用のプライマリ LifeKeeper サーバになります。スタンバイサイトの作成先のサーバがこのサイト用のバックアップサーバになります。「プライマリ」サーバと「バックアップ」サーバの指定が設定対象のサイトごとに異なることに留意してください。

9.4.3.4. 命名規約

LifeKeeper 保護を可能にするには、次のサイト名規則を使用する必要があります (名前は IIS コンソールの [説明] フィールドに入力する)。

- 英数字とダッシュのみを使用します。
- 保護対象の Web サイトの名前 (説明) を変更する必要がある場合は、最初に、LifeKeeper IIS リソースを削除してから、説明を変更し、リソースを作り直してしてください。

9.4.3.5. 同一のプライマリ/バックアップ Web サイト

プライマリ IIS サイトごとに、他方のサーバに同じバックアップ IIS サイトを作成する必要があります。これらの 2 台のサーバを LifeKeeper ハートビートで接続する必要があります。プライマリサイトとバックアップサイトを同じにするには、次の基準を満たす必要があります。

- **[プロパティ]** フォームの **[説明]** フィールドに、大文字、小文字の区別も含めて同じサイト名を入力する必要があります。
- **[プロパティ]** フォームでサイトに割り当てる切り替え可能な IP アドレス、ポート、ヘッダ は同じでなければなりません。
- Web または FTP コンテンツ用に共有または複製ボリュームを使用する場合には、**[ホームディレクトリのパス]** フィールドに割り当てるボリュームのドライブレターとフォルダを同じにする必要があります。
- 特定の Web サイトに対して、複数のバックアップサイトを設定する場合は、他の Web サイトにも同じ ID を設定する必要があります。すなわち、プライマリおよびバックアップの Web サイトは同一の IP アドレス、ポートおよびヘッダを含んでいる必要があります。
- 一方の Web サイトを安全な Web サイトとして設定する場合には、他方の Web サイトも安全な Web サイトとして設定する必要があります。安全な Web サイトには、別の制限が適用されます。詳細については、安全なサーバの構成 を参照してください。

9.4.3.6. 安全なサーバの構成

安全なサーバとは、通信で SSL (Secure Socket Layers) を使用する Web サーバです。送受信されるデータが暗号化され、また、Web クライアントと Web サーバが互いに相手を識別できるため、セキュリティが向上します。安全なサーバでは、URL として http: ではなく https: を使用します。安全なサーバのデフォルトのポート番号は 443 です。

LifeKeeper Microsoft IIS Recovery Kit と LifeKeeper は、安全な IIS Web サイトを稼働させる方法に違いはありません。実際、IIS では、同じ Web サイトに TCP ポートと SSL ポートの両方を設定できます。スタートアップ手順や操作手順は変わりません。そのため、キーが生成され、該当のデジタル署名が IIS にインストールされたら、SSL ポートを設定して、動作させることができます。

9.4.3.7. IIS 設定

LifeKeeper 保護を確実にするためには、次の設定規則を守る必要があります。

- IP アドレスが **[プロパティ]** フォームまたは **[バインディング]** フォームの [IP アドレス] のフィールドに指定されていない IIS サイトを保護することはできません。
- Web コンテンツで共有または複製ボリュームを使用している場合には、「 **このコンピュータ上のディレクトリ** 」として、**ホームディレクトリ** を指定する必要があります。LifeKeeper は、次のいずれかとして指定している **ホームディレクトリ** を保護できません。
  - 別のコンピュータ上での共有
  - URL へのリダイレクト
  - LifeKeeper で保護されていないボリューム

9.4.3.8. ドキュメントコンテンツの場所

共有および複製コンテンツストレージ

コンテンツボリュームが共有または複製ボリューム上にある場合は、両方の Web サイトが同じ共有または複製ボリュームおよびフォルダを指定する必要があります。アクティブとスタンバイの Web サーバ/サイトを同じにするには、プライマリサーバとバックアップサーバに同じコンテンツファイルを含める必要があります。ただし、コンテンツボリュームの共有または複製を行わない場合は、コンテンツはいずれかのシステムの任意の場所に配置できます。

フェイルオーバ時にデータを確実に使用できるようにするには、プライマリサーバ上の共有ディスクまたは複製されたディスク上のフォルダとして **ホームディレクトリ** を設定し、プライマリサーバと同じ **ホームディレクトリ** をバックアップサーバ上に設定します。これにより、コンテンツファイルの 1 つのコピーのみをメンテナンスできます。

非共有ストレージ

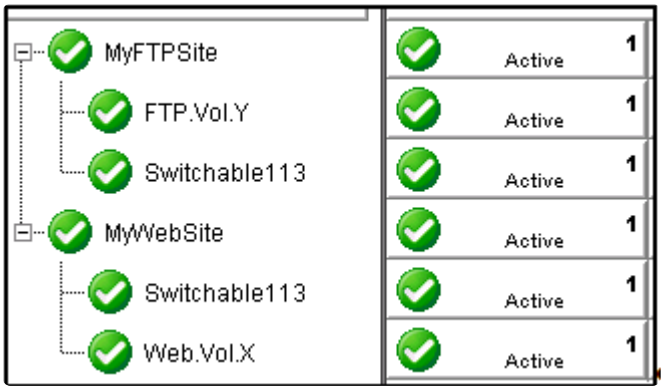
設定では共有ストレージまたは複製されたストレージを使用する必要があります。設定で共有ストレージまたは複製されたストレージを使用しない場合は、各サーバーのローカルボリューム間でコンテンツを同期する必要があります。LifeKeeper Microsoft IIS Recovery Kit には、2台のサーバー間でコンテンツを同期させる機能はありませんが、以下のようにいくつかの推奨があります。

- SIOS DataKeeper を使用してください。自動的に各アクティブサーバ上のデータボリュームをスタンバイサーバにコピーします。
- Microsoft Site Server 3.0 などのコンテンツコピーツールを使用してください。コンテンツコピーツールとして、Robocopy ユーティリティも使用できます。Microsoft Site Server のほうが推奨されます。
- テープバックアップシステムを使用している場合にはプライマリサーバにファイルのテープバックアップを作成してから、それらを必要に応じてバックアップサーバ上に復元します。

9.4.3.9. 複数の IIS サイトで異なるボリュームを使用する

LifeKeeper Microsoft IIS Recovery Kit は、IIS リソース階層を作成するときに、IIS の設定に指定されたホームディレクトリのパスを使用して、IP アドレスとコンテンツボリュームに関連する依存関係を作成します。複数のサイトを保護する場合は、サイトごとに異なる IP アドレスおよびボリュームを指定してください。

下記の階層は同じ IP アドレスと異なるボリュームリソースを使用する MyFTPSite および MyWebSite です。一方のサイトで行うメンテナンスは、もう一方のサイトに影響します。これは、両サイトに共通の IP リソース依存関係があるためです。



バックアップサーバ上で *MyFTPSite* をサービス開始にすると、その依存関係もバックアップサーバに移動します。これにより、*MyWebSite* はプライマリサーバ上でサービス停止になります。その場合、バックアップサーバ上で *MyWebSite* をサービス状態に手動で戻す必要があります。

保護された IIS サイトごとに異なる IP アドレスとボリュームを割り当てると、個別管理が可能になるため、リソースを柔軟に管理できます。ただし、上記の図のようにそれらをグループとして管理するほうが適している場合もあります。

9.4.4. IIS リソースの設定タスク

このセクションのトピックでは、リソースの設定に関するタスクについて説明します。

IIS リソース階層の作成

IIS リソース階層の拡張

IIS リソース階層の削除

IIS リソース階層の拡張解除

10. IIS リソース階層の作成

IIS 階層を作成する前に、関連のボリュームと IP リソース階層 (必要であれば) を最初に作成したか確認しておく必要があります。

プライマリサーバからリソースインスタンスを作成するには、次の手順を実行する必要があります。

1. LifeKeeper GUI メニューから **[編集]** を選択し、次に **[サーバ]** を選択します。ドロップダウンメニューの **[リソース階層の作成]** をクリックします。保護するアプリケーションに対するサーバを選択した後、**[次へ]** をクリックします。

   ダイアログボックスが表示され、クラスタ内で保護することが可能なアプリケーションがドロップダウンリストボックスに表示されます。

   注記: ダイアログボックス内で [戻る] ボタンがアクティブになっているときは、直前のダイアログボックスに戻ることができます。これは特に、前に入力した情報の訂正が必要なエラーが発生した場合に役立ちます。階層の作成手順の途中で [キャンセル] をクリックすると、作成プロセス全体が取り消されます。

2. **[保護するアプリケーションの作成]** ウィンドウが表示されます。**[保護するアプリケーション]** ドロップダウンリストから **[IIS]** を選択し、**[次へ]** をクリックします。

3. サービスの種類 (**WEB** 、**FTP** 、または **SMTP**) を選択し、**[次へ]** をクリックします。

4. 表示されたサイト名を使用するか、複数のサイト名がある場合はドロップダウンリストから選択し、**[次へ]** をクリックします。LifeKeeper は、IIS 設定情報からこのリストを生成します。

5. サイト名と同様に、表示されたサイトタグを使用するか、または新規に **サイトタグ** を入力し、**[次へ]** をクリックして IIS リソースを作成します。

   注意：タグ名に使用できる文字はASCII印字可能文字のみです。

LifeKeeper は、リソース階層作成用の有効なデータを指定したかどうかを検証します。LifeKeeper が問題を検出すると、情報ボックスにエラーメッセージが表示されます。検証に成功すると、リソースが作成されます。

11. IIS リソース階層の拡張

この操作は **[編集]** メニューから開始できますが、**[IIS リソース階層の作成]** オプションの処理を完了すると自動的に開始されます。その場合は、以下の手順 2 を参照してください。

1. **[編集]** メニューの **[リソース]** から **[リソース階層の拡張]** を選択してください。**拡張前処理ウィザード** が表示されます。

2. **拡張前処理ウィザード** で以下の情報を入力してください。

   注記: 最初の 2 つのフィールドは **[編集]** メニューから **拡張** 操作を開始した場合にだけ表示されます。

フィールド	説明
プライマリサーバ	IIS リソースが In Service になっているサーバを入力してください。
拡張するリソース階層	拡張する IIS リソース階層を選択してください。
バックアップサーバ	管理権限をもっているサーバのリストから IIS リソースのバックアップサーバになるサーバを選択してください。

3. 拡張前のチェックが正常に終了したというメッセージが表示されたら、**[次へ]** をクリックします。

4. 拡張する階層に応じて、拡張する **リソースタグ** を示す情報ボックスが表示されます。リソースタグは編集できません。[次へ] をクリックし、依存関係を拡張します。

5. バックアップサーバ上の IIS リソースに対する優先順位を選択します。**[拡張]** をクリックし、IIS リソースをバックアップサーバへ拡張します。

6. **[完了]** をクリックして、拡張処理を完了します。

12. IIS リソース階層の削除

LifeKeeper 環境のすべてのサーバからリソース階層を削除するには、次の手順を実行してください。

1. LifeKeeper GUI メニューから **[編集]** を選択し、次に **[リソース]** を選択します。ドロップダウンメニューの **[リソース階層の削除]** をクリックします。

2. IIS リソース階層の削除対象となる **ターゲットサーバ** を選択します。**[次へ]** をクリックして、次のダイアログボックスに進みます。**注記**: 右側のペイン内の個々のリソースインスタンスを右クリックするか、1 台のサーバにのみリソースがあるような左側のペイン内のグローバルリソースを右クリックして、**リソースの削除** 作業を選択した場合には、このダイアログは表示されません。

3. 削除する階層を選択します。リストボックスには、ターゲットサーバ上のすべて (すなわち、サービス中およびサービス休止状態) の階層が表示されることを覚えておいてください。IIS インスタンスを停止して、LifeKeeper 保護からリソース階層を削除する場合には、必ず階層を サービス停止にしてから削除する必要があります。**注記**: 左側のペイン内のグローバルリソースを右クリックするか、右側のペイン内の個々のリソースインスタンスを右クリックして、**リソースの削除** 作業を選択した場合、このダイアログは表示されません。

4. **[次へ]** をクリックして、次のダイアログボックスに進みます。

5. 選択したターゲットサーバと削除対象として選択した階層を確認する情報ボックスが表示されます。**[削除]** をクリックし、LifeKeeper の保護から IIS リソースを削除します。IIS リソースとその依存関係が LifeKeeper の保護から削除されます。IIS リソースの削除に成功したことを知らせる別の情報ボックスが表示されます。

6. **[完了]** をクリックして **[リソース階層の削除]** メニュー選択を終了します。

13. IIS リソース階層の拡張解除

システムから IIS 階層を拡張解除するには

1. LifeKeeper GUI メニューから **[編集]** を選択し、次に **[リソース]** を選択します。ドロップダウンメニューから **[リソース階層の拡張解除]** を選択します。

2. IIS リソースの拡張解除の対象となるターゲットサーバを選択します。IIS リソースが In Service であるサーバは選択できません。

   注記: 右側のペインにある個々のリソースインスタンスを右クリックして **拡張解除** 作業を選択した場合には、ターゲットサーバを選択するダイアログボックスは表示されません。

2. **[次へ]** をクリックして、次のダイアログボックスに進みます。

3. 拡張解除する IIS リソース階層を選択してください。**[次へ]** をクリックして、次のダイアログボックスに進みます。

   注記: 左側のペイン内のグローバルリソースを右クリックするか、右側のペイン内の個々のリソースインスタンスを右クリックして、**拡張解除** 作業を選択した場合は、このダイアログは表示されません。

4. 拡張解除するために選択したターゲットサーバと IIS リソース階層を確認する情報ボックスが表示されます。**[拡張解除]** をクリックします。

5. IIS リソースの拡張解除に成功したことを確認する別の情報ボックスが表示されます。**[完了]** をクリックして終了します。

14. IIS リソース階層のテスト

このセクションでは、IIS リソース階層のテストについて説明します。

GUI からの手動スイッチオーバの実行

リカバリ操作

14.1. GUI からの手動スイッチオーバの実行

手動スイッチオーバを開始するには、LifeKeeper の GUI メニューから **[編集]** 、**[リソース]** 、**[サービス開始]** の順に選択してください。例えば、バックアップサーバでサービス開始要求を実行すると、アプリケーション階層はバックアップサーバ側でサービス中となり、プライマリサーバのサービスは停止されます。この時点で、元のバックアップサーバがプライマリサーバとなり、元のプライマリサーバがバックアップサーバとなります。

[サービス停止] の要求を実行した場合、このアプリケーションはサービス停止になり、別のサーバのアプリケーションはサービス中になりません。

14.2. リカバリ操作

プライマリサーバに障害が発生すると、LifeKeeper Microsoft IIS Recovery Kit ソフトウェアが次の処理を実行します。

- バックアップサーバのいずれかの物理ネットワークインターフェース上の IP アドレス (複数) を [サービス開始] にして、そのサーバで IIS リソース階層を In Service にします。
- バックアップサーバ側の共有または複製ボリューム (使用している場合) をアンロックし、プライマリサーバ側でそれをロックします。
- バックアップサーバで IIS Web サイトを開始します。

リカバリの完了後、Web サーバのユーザは、ブラウザの **[リロード/リフレッシュ]** ボタンをクリックして再接続できます。

15. IIS 階層の管理

このセクションでは、IIS 階層の管理について説明します。

クイックチェック間隔、ディープチェック間隔、ローカルリカバリの設定変更

手動スイッチオーバ

IIS のフェイルオーバ

匿名接続を使用できない FTP サイトを保護する場合

FTP ログインスクリプトを使用する

FTP のディープチェックを無効にする

LifeKeeper Microsoft IIS Recovery Kit 構成の変更

Microsoft IIS の削除

ネットワークインターフェースカード (NIC) の変更

15.1. クイックチェック間隔、ディープチェック間隔、ローカルリカバリの設定変更

クイックチェック間隔、ディープチェック間隔、ローカルリカバリのデフォルト値は、リソースが LifeKeeper の保護対象となった後、LifeKeeperGUI を使用して変更可能です。デフォルト値を変更する場合は、リソース上で右クリックし、変更したいエントリをメニューリストから選択してください。値を変更後、**[変更]** ボタンをクリックしてください。修正の操作結果がダイアログボックスに表示されます。**[完了]** ボタンをクリックして終了してください。

デフォルト値は以下のようになっています。

- クイックチェック間隔は **180秒** (3分)
- ディープチェック間隔は **300秒** (5分)
- ローカルリカバリは「**有効**」

15.2. 手動スイッチオーバ

手動スイッチオーバは、LifeKeeper GUI の **[サービス開始]** オプションを使用して実行できます。LifeKeeper は、切り替え可能な IP アドレス、ボリューム、IIS Web/FTP/SMTP サイトを他方のサーバに移します。例えば、フェイルオーバの後にプライマリを修復してから、プライマリを再び使用したい場合などは、この操作を行うとよいでしょう。

15.3. IIS のフェイルオーバ

フェイルオーバは次の 2 つの状況で発生します。

- 最初の状況は、ハードウェアまたはオペレーティングシステムで重大な障害が発生し、サーバが稼働しなくなったときです。バックアップサーバ上の LifeKeeper Core は、ハートビートメッセージ送信の失敗時にこれを検出します。この時点で、LifeKeeper Core がキットのリカバリスクリプトを呼び出します。このリカバリスクリプトにより、インターネットサーバ (複数) がバックアップサーバでサービス中になることが保証されます。

- 2 番目の状況は、リカバリキットの **ディープチェック** / **クイックチェック** スクリプトがアプリケーションの障害を検出したときです。これらのスクリプトは LifeKeeper Core に障害を示すコードを応答します。LifeKeeper Core は、フェイルオーバプロセスを開始して、キットのリカバリスクリプトを呼び出します。LifeKeeper Core は最初にローカルサーバを停止させて (まだ停止していない場合)、切り替え可能 IP アドレスと LifeKeeper ボリュームを非アクティブにします。次にバックアップサーバへのフェイルオーバを続行します。

プライマリサーバを修復すると、スイッチバックタイプが **[自動]** の場合、インターネットサーバがプライマリサーバに自動的に戻ります。スイッチバックタイプが **[インテリジェント]** の場合には、手動スイッチオーバを行う必要があります。

Web クライアントが比較的少ない場合には、切り替えまたはフェイルオーバが発生すると常に問題が起こります。第一に、IP アドレスとボリュームをバックアップシステムに移動して、バックアップサーバを開始するプロセスには約 45 秒かかり (IP アドレスとボリュームの数により異なる)、ユーザはその間、サーバに接続できません。第二に、スイッチオーバ中にアクティブサーバが停止して、アクティブサーバとユーザとの接続が切れます。いずれの場合も、IIS クライアントが要求を再試行すれば、その要求は正しく処理されます。切り替え可能 IP アドレスとボリュームをバックアップシステムに移して、バックアップサイトが稼働状態になると、サービスは正常な状態に戻ります。

15.4. 匿名接続を使用できない FTP サイトを保護する場合

保護された FTP サイトを監視するため、デフォルトでは匿名ユーザを使用して接続し、ログインします。この機能は各 FTP サイトの監視に割り当てられているディープチェックプロセスにより実行されます。サイトが匿名接続を許可していない場合、デフォルトのディープチェックは失敗します。匿名接続が許可されていない場合は、LifeKeeper を使って簡単なログインのためのスクリプトを使用するか、ディープチェックの間隔を 0 秒に設定して、LifeKeeper リソースのディープチェックプロセスを無効にしてください。

15.5. FTP ログインスクリプトを使用する

Microsoft FTP コマンドはスクリプト化された FTP ログインを使用する機能を提供します。LifeKeeperは保護された各 FTP サイトの空のログインスクリプトファイルを作成します。そのファイルは FTP サイト名と一致します。LifeKeeper は FTP コマンドが実行されるまで、空のスクリプトを使用することはありません。それらは以下のフォルダで作成されます。

```
<LifeKeeper のルートインストールフォルダ>\admin\kit\webapp
```

「既定の FTP サイト」の空のログインスクリプトが置かれている場所の例は次のとおりです。

```
<LifeKeeper のルートインストールフォルダ>\admin\kit\webapp\Default FTPSite.txt/
font>
```

ファイル名にスペースを使用できるので、.txt 拡張子を持つ FTP サイト名 と確実にマッチさせることができます。スクリプトのコンテンツは、4 列のみ持つことができ、FTP オープンコマンド、ログイン ID、ログインパスワード、および FTP bye コマンドを含んでいます。例えば、ログインスクリプトは以下の 4 行で構成される場合があります。

```
open 192.168.1.10
mytestloginID
mytestloginPW
bye
```

LifeKeeper はFTP クライアントユーティリティからの各応答に対して検索システムを使用します。「230」で始まるレスポンスはログインに成功したことを示します。ログイン障害が発生するとディープチェックに失敗します。そのほかのコマンドも、このスクリプトに追加はできますが LifeKeeper は、それを無視します。

15.6. FTP のディープチェックを無効にする

保護された FTP サイトが、匿名ユーザのログインを許可しない場合や、ログインスクリプトを使用したくない場合は、LifeKeeper の保護対象である特定のリソースに対するディープチェックを無効にすることが可能です。LifeKeeper の「bin」フォルダのディレクトリへ Change directory を行い、以下の LifeKeeper コマンドを使用してリソースに対するディープチェックを無効にしてください。

```
cd <LifeKeeper Root Install Folder>\bin
ins_setchkint - t <LifeKeeper リソースのタグ名> -c d - v 0
```

15.7. LifeKeeper Microsoft IIS Recovery Kit 構成の変更

ポート番号、IP アドレス、ハードウェア仮想サーバ、または安全/非安全設定に影響を与える構成変更は、LifeKeeper の構成にも影響を与えます。サーバとキット間にダイレクトなリンクがないため、次の手順で構成を同期する必要があります。

1. 階層をサービス休止状態にしてから、階層を削除することによって、IIS リソースの保護を削除します。
2. プライマリサーバ側で、IIS Console を正しく実行して、変更をこのサーバに適用します。
3. バックアップサーバ側で、IIS Console を実行して、変更をこのサーバに適用します。
4. IIS リソース階層を作成し、それをバックアップサーバに拡張することによって、IIS リソースに LifeKeeper 保護を追加します。

15.8. Microsoft IIS の削除

サイト自体またはソフトウェアパッケージのいずれかを削除する前に、IIS Web/FTP/SMTP サイトの LifeKeeper 保護を削除してください。存在していないものの保護を LifeKeeper が試行しないようにするため、この操作は重要です。

注記: キットのこのリリースは、Microsoft IIS 5.0 と Microsoft IIS 6.0 でテストされています。このリリースが最新のリリースと必ずしも互換性が維持されるとは限りません。その理由は、主として個々のレジストリキーと設定ファイルの位置と内容の依存関係です。

15.9. ネットワークインターフェースカード (NIC) の変更

ネットワークインターフェースカード (NIC) の変更手順により、Web サービスが中断されます。この根本的な理由は、LifeKeeper の IP 階層データに NIC のモデル番号が含まれているからです。このデータは簡単には変更できないので、以下の手順で切り替え可能 IP アドレスを削除してから再インストールしてください。

1. LifeKeeper GUI を使用して、IIS リソースのサービスを停止状態にしてから各階層を削除し、すべての IIS リソースから保護を削除します。
2. バックアップサーバ上のものも含めて、すべての IIS サービスを停止します。これで、すべての IIS サービスがサービス停止になりました。
3. すべての IP 階層を削除します (設定データを必ずメモしてください)。
4. サーバを停止させ、NIC を交換してからサーバを再起動します。
5. すべての IP 階層を再び作成します。
6. 各 Web サイトのプライマリサーバで IP 階層をサービス中にします。
7. プライマリサーバで、IIS サービスを再起動してください。Web サイトが再びサービス中になります。
8. 各 Web サーバのプライマリサーバで、LifeKeeper GUI を使用して、IIS リソース階層を再作成します。

注記 1: 現在搭載している NIC のタイプを素早く確認するには、DOS プロンプトから ipconfig コマンドを実行します。NIC のタイプが出力に表示されます (例えば、「Ethernet adapter: DC21×41」は、DC21×41 という名称の Ethernet NIC を表します)。

注記 2: プライマリ NIC を変更すると、LifeKeeper のライセンスに影響を与える可能性があります。ライセンスの詳細については、「プランニングおよびインストールの手引き」を参照してください。

16. IIS のトラブルシューティング

このセクションでは、LifeKeeper ソフトウェアには特別な関係がない、全体的な環境に関連する現象についての解決策と考えられる原因を提示します。

16.1. 現象と解決策

現象: プライマリとセカンダリの両サーバに同じサイトが作成されるが、それぞれのサイトが **リソース作成ウィザード** の **サイト名リスト** に表示されない。

解決策:

- 同じオプションパラメータを指定しているか、また、それらの値が両システムで同じになっているかチェックしてください (値は大文字小文字が区別される)。
- すべてのサイトに LifeKeeper の有効な説明が含まれているか確認してください (説明には英数字とダッシュのみが使用可能)。保護対象の Web サイトの名前 (説明) を変更する必要がある場合は、最初に IIS を削除してから、説明を変更し、リソースを作り直してしてください。

現象: FTP サイトにアクセスしようとすると、以下のエラーメッセージが表示される。

```
"User x cannot login, home directory inaccessible".
```

解決策: *ANONYMOUS* として FTP にユーザがログインするのを許可するには、インターネットゲストアカウントユーザ `IUSR_{machine name}` にローカルのログイン権限を付与する必要があります。

現象: Internet Information Services (IIS) Manager で IIS Web/FTP/SMTP を設定しているときに、ドロップダウンリストから IP アドレスを選択しようとすると、切り替え可能 IP アドレスが表示されない。

解決策: 切り替え可能な IP アドレスを手動で入力してください。

17. SIOS Protection Suite for Windows サポートマトリックス

サーバー コンポーネント

サポート対象のオペレーティングシステム	v8.0.0	v8.0.1	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0	v8.6.1	v8.6.2	v8.6.3	v8.6.4
Microsoft Windows Server 2008 R2 Standard、Enterprise、および DataCenter Edition	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Microsoft Windows Server 2012 Standard および DataCenter Edition	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Microsoft Windows Server 2012 R2 Standard および DataCenter Edition			64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Microsoft Windows Server 2016 Standard および DataCenter									64 ビット	64 ビット	64 ビット	64 ビット	64 ビット

注記 : すべてのバージョンで Microsoft .NET Framework 4.5.2 が必要です。次のサイトからダウンロードしてください
http://www.microsoft.com/net

注記 : 上記一覧のオペレーティングシステムバージョンは以下の仮想プラットフォームで実行するゲスト用にサポートされます

- Amazon EC2 (AWS)
- VMware vSphere 5.5, 6.0, 6.5, 6.7, 7.0
- Microsoft Hyper-V Server 2008 R2 以降

サポート対象のオペレーティングシステム	v8.0.0	v8.0.1	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0	v8.6.1	v8.6.2	v8.6.3	v8.6.4
Editions													
Microsoft Windows Server 2019 Standard および DataCenter Editions													64 ビット

注記 : すべてのバージョンで Microsoft .NET Framework 4.5.2 が必要です。次のサイトからダウンロードしてください
http://www.microsoft.com/net

注記 : 上記一覧のオペレーティングシステムバージョンは以下の仮想プラットフォームで実行するゲスト用にサポートされます

- Amazon EC2 (AWS)
- VMware vSphere 5.5, 6.0, 6.5, 6.7, 7.0
- Microsoft Hyper-V Server 2008 R2 以降

ユーザーインターフェイス コンポーネント

サポート対象のオペレーティングシステム	v8.0.0	v8.0.1	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0	v8.6.1	v8.6.2	v8.6.3	v8.6.4	v8
Microsoft Windows Server 2008	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Microsoft Windows Server	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット

注記 : すべてのバージョンで Microsoft .NET Framework 4.5.2 が必要です。次のサイトからダウンロードしてください
http://www.microsoft.com/net

注記 : 上記一覧のオペレーティングシステムバージョンは以下の仮想プラットフォームで実行するゲスト用にサポートされます

- Amazon EC2 (AWS)
- VMware vSphere 5.5, 6.0, 6.5, 6.7, 7.0
- Microsoft Hyper-V Server 2008 R2 以降

サポート対象のオペレーティングシステム	v8.0.0	v8.0.1	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0	v8.6.1	v8.6.2	v8.6.3	v8.6.4	v8
2008 R2														
Microsoft Windows Server 2012	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Microsoft Windows Server 2012 R2			64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Microsoft Windows Server 2016									64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Microsoft Windows Server 2019													64 ビット	64 ビット
Windows XP														
Windows Vista														
Windows 7	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Windows 8	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット	64 ビット
Windows 10														

注記：すべてのバージョンで Microsoft .NET Framework 4.5.2 が必要です。次のサイトからダウンロードしてください
http://www.microsoft.com/net

注記：上記一覧のオペレーティングシステムバージョンは以下の仮想プラットフォームで実行するゲスト用にサポートされます

- Amazon EC2 (AWS)
- VMware vSphere 5.5, 6.0, 6.5, 6.7, 7.0
- Microsoft Hyper-V Server 2008 R2 以降

SQL Server Recovery Kit

サポート対象のアプリケーション	v8.0.0	v8.0.1	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0	v8.6.1	v8.6.2	v8.6.3	v8.
Microsoft SQL Server 2000													
Microsoft SQL Server 2005													
Microsoft SQL Server 2008 R1	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Ed
Microsoft SQL Server 2008 R2	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Ed
Microsoft SQL Server 2012	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Ed
Microsoft SQL Server 2014				すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Ed
Microsoft SQL Server 2016									すべての Edition	すべての Edition	すべての Edition	すべての Edition	すべての Ed
Microsoft SQL Server 2017										すべての Edition	すべての Edition	すべての Edition	すべての Ed
Microsoft SQL Server 2019													

PostgreSQL Server Recovery Kit

サポート対象のアプリケーション	v8.0.0	v8.0.1	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0	v8.6.1	v8.6.2	v8.6.3	v8.6.4
PostgreSQL									9.6.x	9.6.x	9.6.x	9.6.x, 10.x	9.6.x, 10.x, 11.x
EnterpriseDB Postgres Plus Advanced Server/EDB Postgres Advanced Server													

Oracle Recovery K

サポート対象のアプリケーション	v8.0.0*	v8.0.1*	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0
Oracle 11g									
Oracle 11g Release 2	Standard Edition, Standard Edition One, Enterprise Edition	Standard Edition, Standard Edition One, Enterprise Edition	Standard Edition, Standard Edition One, Enterprise Edition	Standard Edition, Standard Edition One, Enterprise Edition	Standard Edition, Standard Edition One, Enterprise Edition	Standard Edition, Standard Edition One, Enterprise Edition	Standard Edition, Standard Edition One, Enterprise Edition	Standard Edition, Standard Edition One, Enterprise Edition	Standa Edition Standa Edition One, Enterpr Edition
Oracle 12c						Enterprise Edition	Standard Edition Two,	Standard Edition Two,	Standa Edition Two,

* それぞれのバージョンに対する Oracle Recovery Kit のバージョンは 7.2.1 です。

サポート対象のアプリケーション	v8.0.0*	v8.0.1*	v8.1.0	v8.2.0	v8.2.1	v8.3.0	v8.4.0	v8.5.0	v8.6.0
							Enterprise Edition	Enterprise Edition	Enterpr Edition
Oracle 12c Release 2									
Oracle 18c									
Oracle 19c									

* それぞれのバージョンに対する Oracle Recovery Kit のバージョンは 7.2.1 です。

18. プロダクトライフサイクル

LifeKeeper/DataKeeper の各バージョンにおけるプロダクトライフサイクルについては、こちら を参照してください

19. LifeKeeper Single Server Protection for Windows

はじめに

LifeKeeper Single Server Protection（SSP）を使用すると、単一ノード構成でのアプリケーション監視が可能になります（クラスタの要件や制約はありません）。物理または仮想（vSphere、KVM、Amazon EC2）いずれの単一ノード環境でも使用できます。LifeKeeper SSPは、実績のある安定したSIOS LifeKeeperのアーキテクチャ上に構築されており、優れたアプリケーション監視を提供し、障害が発生したアプリケーションおよびシステムインフラ要素（IPアドレス、ファイル共有リストなど）のリカバリを実行できます。何らかの理由でアプリケーションを回復できない場合、LifeKeeper SSPは、システムの再起動またはVMおよびアプリケーション監視用に構成されたVMware仮想マシンのVMware HAの再起動機能により、ノードの再起動を開始します。

> 注記: LifeKeeper SSPはSIOS LifeKeeperのテクノロジを使用して構築されているため、本ドキュメントではLifeKeeperのマニュアルを参照しています。SIOS Protection Suite for Windowsと共通のトピックについてはSIOS Protection Suite for Windowsのドキュメントにある情報を参照しています。これらの共通のトピックを参照する場合、次の項目に関してはLifeKeeper SSPには適用されません。

- クラスタリング
- コミュニケーションパス
- 共有ストレージ（要件、構成など）
- リソース階層の拡張/拡張解除
- リソース/マシンのフェイルオーバ（デフォルトでは、LifeKeeper SSPではノードが再起動します）
- リソースのスイッチオーバ
- 切り替え可能なIPアドレス（LifeKeeper SSPでは、一部の保護対象のアプリケーションには切り替え可能なIPアドレスが必要ですが、ノードが1つしかないため、実際には切り替えは行われません）

> 注記: Amazon EC2で実行している場合、IPリソースを作成する前に、Amazon EC2マネジメントコンソールを使用して、NICにセカンダリプライベートIPアドレスを割り当てます。次に、LifeKeeper GUIクライアントを使用しているNICでプライベートIPアドレスとしてIPリソースを作成します。Elastic IPをIPリソースに関連付けることができます。

LifeKeeper SSPの基盤であるSIOS LifeKeeper製品の詳細については、SIOS Protection Suite for Windowsの共通リリース番号のドキュメントを参照してください。このドキュメントには、リソース階層の作成、リソースタイプ、状態と関係、グラフィカルユーザインターフェイス（GUI）、および一般的なタスクと高度なタスクに関する詳細情報を記載しています。

LifeKeeper Single Server Protection for Windows リリースノート

LifeKeeper Single Server Protection for Windows インストレーションガイド

19.1. LifeKeeper Single Server Protection for Windows リリースノート

バージョン8.7.2

リリース日:2020/11/20

重要!!

本製品をインストールまたは使用する前に、必ずこのドキュメントをお読みください。
このドキュメントには、インストール時とその前後に留意すべき重要な項目に関する情報が記載されています。

はじめに

このドキュメントは LifeKeeper Single Server Protection for Windows (LKSSP) 製品のインストールや設定、管理を行う担当者向けのものであり、このドキュメントには、LifeKeeper Single Server Protection のマニュアルには記載されていない重要な情報が含まれています。LifeKeeper Single Server Protectionソフトウェアをインストールして設定する前に、必ずこのドキュメントの内容を確認してください。

LifeKeeper Single Server Protection 製品の説明

LifeKeeper Single Server Protectionを使用すると、物理および仮想のいずれでも、単一ノード構成でのアプリケーション監視を実施できます（つまり、クラスタの要件や制約はありません）。LifeKeeper Single Server Protectionは、実績のある安定したSIOS LifeKeeperのアーキテクチャに基づいて構築されています。LifeKeeper Single Server Protection for Windowsは、優れたアプリケーション監視を提供し、障害が発生したアプリケーションおよびシステムインフラストラクチャの要素（IPアドレス、ファイル共有リストなど）のリカバリを実行できます。何らかの理由でアプリケーションを回復できない場合、LifeKeeper Single Server Protectionは、システムの再起動またはVMおよびアプリケーション監視用に設定されたVMware仮想マシンのVMware HA再起動によって、ノードを再起動します。

LifeKeeper Single Server Protection for Windows Version 8 の新機能

機能	説明
本バージョンでの新機能	
OpenJDK 15	LifeKeeper Single Server Protection for Windows は、OpenJDK15 をサポート

	し、同梱するようになりました
Oracle Pluggable Database Recovery Kit	Oracle プラガブルデータベースをサポートするようになりました
全体的なメンテナンス	下記の バグ修正 を参照してください。
バージョン 8.7.1 の新機能	
全体的なメンテナンス	バグ修正

バグの修正

以下に、最新のバグの修正および機能強化のリストを示します。

	説明
PW-932	リソースのフェールオーバー中に削除の失敗を無視する問題を修正しました
PW-1280	LK SQL Optional Servicesは、SQL 2017 および SQL 2019 Reporting Services をサポートするようになりました
PW-1464	ソースのサイズ変更後、ターゲット上のファイルシステムの状態が RAW になる問題を修正しました

コンポーネント

LifeKeeper Single Server Protection Softwareはバンドルされており、64ビットシステム（x86_64）で実行されます。

製品	オペレーティングシステム
LifeKeeper Single Server Protection for Windows (サーバコンポーネント)	SPS サポートマトリックス を参照
LifeKeeper Single Server Protection for Windows (ユーザインターフェース)	SPS サポートマトリックス を参照

仮想環境	上記のオペレーティングシステムは以下の仮想プラットフォーム上で動作するゲストとしてサポートされています。仮想プラットフォームOSバージョンの詳細等につきましては こちら にお問い合わせください。 • Amazon EC2 (AWS) • VMware vSphere • Microsoft Hyper-V • Citrix XenServer • KVM with Kernel
上記の OS プラットフォームすべての 64 ビットバージョン (Itanium を除くx64) がサポートされます。	

オプションのリカバリーキット

LifeKeeper Single Server Protection for Windows とオプションの LifeKeeper Single Server Protection for Windows リカバリーキットを連携させるには、ソフトウェアライセンスキーが必要です。

Kit Name	Versions/Requirement(s)
Microsoft SQL Server リカバリーキット	SPS サポートマトリックス を参照
Oracle リカバリーキット	SPS サポートマトリックス を参照

要件

LifeKeeper Single Server Protection を Windows 2008 にインストールするとき、以下に説明するようにシステム設定を変更するかどうかを確認するダイアログボックスが表示されます。インストーラで変更できない場合は、インストールが終了してから手動で変更する必要があります。

- Windows ファイアウォール
- **Distributed Link Tracking Client** を 無効 にする

LifeKeeper Single Server Protection for Windows および Microsoft FTP Service 7.5 for IIS 7.0 を実行するシステムの場合は、Windows 2008 R2 以降が必要です。

さらに、Windows サーバがドメイン内にない場合は、ローカルセキュリティポリシー設定 "***ネットワークアクセス: Everyone アクセス許可を匿名ユーザに適用する***" を有効にする必要があります。サーバがドメイン内にある場合、この設定は必要ありません。

LifeKeeper Single Server Protection for Windows の要件

以下の表に、LifeKeeper Single Server Protection for Windows およびリカバリーキットに該当する要件を示します。

Core	要件
LifeKeeper Single Server Protection for Windows のライセンス	LifeKeeper Single Server Protection for Windowsを実行するサーバごとに 1 つのライセンスが必要です。これは物理サーバおよび仮想サーバの両方に適用されます。
LAN Manager リカバリーキット	**“Microsoft ネットワーク用ファイルとプリンタ共有”** コンポーネント (lanmanserver) を Windows サーバにインストールする必要があります。NetBIOS も有効にする必要があります。そうしないと、LAN Manager リソースは起動しません。
メモリ要件	LifeKeeper Single Server Protection for Windows をサポートするシステムに必要な最小メモリ容量は、使用している オペレーティングシステム のメモリ要件に基づいて決まります。ユーザアプリケーションを実行するには SIOS Protection Suite に必要なメモリ以外に追加のメモリが必要です。
GUI	**ポート:** LifeKeeper Single Server Protection for Windows は、GUI サーバと GUI クライアントの間の Remote Method Invocation (RMI) 通信にポート 82 を使用します。 LifeKeeper GUI は管理 Web サーバにポート 81 を使用します。管理 Web サーバはパブリック Web サーバとは別のものにする必要があります。これはリモートクライアント上で Java アプレットとして実行する場合に GUI で使用されます。 既存のアプリケーションと競合する場合、これらのポートを変更するには、SIOS\LIFEKEEPER\JAVAGUI\SERVER レジストリキーの RMI_PORT または WEB_PORT エントリを編集します。

クライアントプラットフォームおよびブラウザ

LifeKeeper Single Server Protection Web クライアントは、Java Runtime Environment JRE8 アップデート 51 をサポートしている任意のプラットフォームで実行できます。現在サポートされている構成は、Firefox（Firefox 51以前）および Windows 上の Internet Explorer、Windows Server 2008 R2、Windows Server 2012 R2、Windows Server 2016、Windows 7、Windows 8 または Windows 10（JRE8アップデート51）です。その他の最近のプラットフォームおよびブラウザもSPS Webクライアントで動作する可能性はありますが、SIOS Technology Corpではテストを行っていません。さらに、各ブラウザの特定の機能もテストしていません。

LifeKeeper Single Server Protection コンポーネント（例：VMware 構成にインストールされている場合の SteelEye Management Console および vCenter）および保護対象の Windows ゲストの IP アドレスは、DNS またはローカルホストファイル (通常は /etc/hosts または C:\windows\system32\drivers\etc\hosts) を介して解決できる必要があります。ローカルホストファイルを使用すると、クライアント接続時間が最小限に抑えられ、クライアン

トはドメインネームサーバ（DNS）に障害が発生した場合でも接続できます。

既知の問題

SIOS AppKeeper

SIOS LifeKeeperは、AWS EC2のクラスター環境でOSおよびアプリケーションサービスを監視・修復します。このため、これらの環境でSIOS LifeKeeperに加えてSIOS AppKeeperを使用することは、推奨もサポートもされていません。

テクニカルサポート

サポート契約を結んでいるSIOS Technology Corp.のお客様は、新しい SIOS Technology Corp. Support Self-Service Portal にアクセスできます。

SIOS Technology Corp. Support Self-Service Portal では、以下のことができます。

- **ソリューションナレッジベース** を検索して、問題の解決策と質問への回答を探すことができます。

- SIOS Technology Corp.のサポートチームによる24時間年中無休のサポートサービス経由で、以下のことができます。
  - **ケースを記録して** 新しいインシデントを報告する
  - **ケースを表示して** 、未解決および解決済のインシデントをすべて表示する
  - **Review Top Solutions** で、お客様によく見られている最も一般的な問題解決に関する情報を提供する

セルフサービスポータルアカウントのセットアップと有効化は、SIOS Technology Corp.サポート support@us.sios.com までご連絡ください。

SIOS Technology Corp.サポートへのお問い合わせは、以下の連絡先もご利用いただけます。

1-877-457-5113 (通話料無料)

1-803-808-4270 (海外からのお問い合わせ)

メールアドレス: support@us.sios.com

19.2. LifeKeeper Single Server Protection for Windowsインストレーションガイド

LifeKeeper Single Server Protection for Windowsについて

LifeKeeper Single Server Protection（SSP）を使用すると、単一ノード構成でのアプリケーション監視が可能になります（クラスタの要件や制約はありません）。物理または仮想（vSphere、KVM、Amazon EC2）いずれの単一ノード環境でも使用できます。LifeKeeper SSPは、実績のある安定したSIOS LifeKeeperのアーキテクチャ上に構築されており、優れたアプリケーション監視を提供し、障害が発生したアプリケーションおよびシステムインフラ要素（IPアドレス、ファイル共有リストなど）のリカバリを実行できます。何らかの理由でアプリケーションを回復できない場合、LifeKeeper SSPは、システムの再起動またはVMおよびアプリケーション監視用に構成されたVMware仮想マシンのVMware HAの再起動機能により、ノードの再起動を開始します。

> 注記: LifeKeeper SSPはSIOS LifeKeeperのテクノロジを使用して構築されているため、本ドキュメントではLifeKeeperのマニュアルを参照しています。SIOS Protection Suite for Windowsと共通のトピックについてはSIOS Protection Suite for Windowsのドキュメントにある情報を参照しています。これらの共通のトピックを参照する場合、次の項目に関してはLifeKeeper SSPには適用されません。

- クラスタリング
- コミュニケーションパス
- 共有ストレージ（要件、構成など）
- リソース階層の拡張/拡張解除
- リソース/マシンのフェイルオーバ（デフォルトでは、LifeKeeper SSPではノードが再起動します）
- リソースのスイッチオーバ
- 切り替え可能なIPアドレス（LifeKeeper SSPでは、一部の保護対象のアプリケーションには切り替え可能なIPアドレスが必要ですが、ノードが1つしかないため、実際には切り替えは行われません）

> 注記: Amazon EC2で実行している場合、IPリソースを作成する前に、Amazon EC2マネジメントコンソールを使用して、NICにセカンダリプライベートIPアドレスを割り当てます。次に、LifeKeeper GUIクライアントを使用しているNICでプライベートIPアドレスとしてIPリソースを作成します。Elastic IPをIPリソースに関連付けることができます。

LifeKeeper SSPの基盤であるSIOS LifeKeeper製品の詳細については、共通するリリース番号の SIOS Protection Suite for Windows ドキュメンテーション を参照してください。このドキュメントには、リソース階層の作成、リソースタイプ、状態と関係、グラフィカルユーザインターフェイス（GUI）、および一般的なタスクと高度なタスクに関する詳細情報を記載しています。

20. LifeKeeper Single Server Protection for Windows テクニカルドキュメンテーション

LifeKeeper Single Server Protection for Windowsについて

LifeKeeper Single Server Protection（SSP）を使用すると、単一ノード構成でのアプリケーション監視が可能になります（クラスタの要件や制約はありません）。物理または仮想（vSphere、KVM、Amazon EC2）いずれの単一ノード環境でも使用できます。LifeKeeper SSPは、実績のある安定したSIOS LifeKeeperのアーキテクチャ上に構築されており、優れたアプリケーション監視を提供し、障害が発生したアプリケーションおよびシステムインフラ要素（IPアドレス、ファイル共有リストなど）のリカバリを実行できます。何らかの理由でアプリケーションを回復できない場合、LifeKeeper SSPは、システムの再起動またはVMおよびアプリケーション監視用に構成されたVMware仮想マシンのVMware HAの再起動機能により、ノードの再起動を開始します。

注記: LifeKeeper SSPはSIOS LifeKeeperのテクノロジを使用して構築されているため、本ドキュメントではLifeKeeperのマニュアルを参照しています。SIOS Protection Suite for Windowsと共通のトピックについてはSIOS Protection Suite for Windowsのドキュメントにある情報を参照しています。これらの共通のトピックを参照する場合、次の項目に関してはLifeKeeper SSPには適用されません。

- クラスタリング
- コミュニケーションパス
- 共有ストレージ（要件、構成など）
- リソース階層の拡張/拡張解除
- ストレージキット（DR、DMMP、HDLM、LVM、MD、PPATHおよびNEC SPS）

  注記: LifeKeeper SSPでストレージキットを使用していない場合、保護されているファイルシステムをマウントするために必要なデバイスがシステムブート中にアクティブになるように手順を実行する必要があります（たとえば、ファイルシステムが論理ボリュームにマウントされている場合、LifeKeeper SSPが起動する前にボリュームがアクティブ状態になっている必要があります）。

- リソース/マシンのフェイルオーバ（デフォルトでは、LifeKeeper SSPではノードが再起動します）
- リソースのスイッチオーバ
- 切り替え可能なIPアドレス（LifeKeeper SSPでは、一部の保護対象のアプリケーションには切り替え可能なIPアドレスが必要ですが、ノードが1つしかないため、実際には切り替えは行われません）

  注記: Amazon EC2で実行している場合、IPリソースを作成する前に、Amazon EC2マネジメントコンソールを使用して、NICにセカンダリプライベートIPアドレスを割り当てます。次に、LifeKeeper GUIクライアントを使用しているNICでプライベートIPアドレスとしてIPリソースを作成します。Elastic IPをIPリソースに関連付けることができます。

LifeKeeper SSPの基盤であるSIOS LifeKeeper製品の詳細については、共通するリリース番号の SIOS Protection Suite for Windows ドキュメンテーション を参照してください。このドキュメントには、リソース階層の作成、リソースタイプ、状態と関係、グラフィカルユーザインターフェイス（GUI）、および一般的なタスクと高度なタスクに関する詳細情報を記載しています。

20.1. ドキュメンテーションとトレーニング

SIOS LifeKeeper Single Server Protection for Windowsのインストール、設定、管理、トラブルシューティングの手順は、すべて LifeKeeper Single Server Protectionのドキュメント に記載されています。以下のセクションで、SIOS LifeKeeper Single Server Protection for Windowsのあらゆる側面を説明しています。

セクション	説明
はじめに	LifeKeeper Single Server Protection環境のプランニングと設定に役立つ情報を提供します。
管理	サーバーのプロパティの編集やリソースの作成などのサーバーレベルのタスク、リソースの編集や削除などのリソースレベルのタスクについて説明します。
ユーザーガイド	LifeKeeper GUI内で実行できる多くのタスクなど、LifeKeeper GUIの詳細情報を記載しています。
リカバリーキット	LifeKeeper Single Server Protectionで特定のアプリケーションの管理および制御をできるようにするために使用する、オプションのリカバリーキットの計画、インストール手順、管理、構成、およびユーザー情報を記載しています。

トレーニング

LifeKeeper Single Server Protectionのトレーニングは、SIOS Technology Corp.またはLifeKeeper Single Server Protectionプロバイダを通じて受講いただけます。詳細については、営業担当者にお問い合わせください。

テクニカルサポート

サポート契約を結んでいるSIOS Technology Corp.のお客様は、新しい SIOS Technology Corp. Support Self-Service Portal にアクセスできます。

The SIOS Technology Corp. Support Self-Service Portal では、以下のことができます。

- ソリューションナレッジベースを検索して、問題の解決策と質問への回答を探すことができます。
- SIOS Technology Corp.のサポートチームによる24時間年中無休のサポートサービスに、以下をご依頼いただけます。
- **ケースを記録して** 新しいインシデントを報告する
- **ケースを表示して** 、未解決および解決済のインシデントをすべて表示する
- **Review Top Solutions** で、お客様によく見られている最も一般的な問題解決に関する情報を提供する

セルフサービスポータルアカウントのセットアップと有効化は、SIOS Technology Corp.サポート support@us.sios.com までご連絡ください。

SIOS Technology Corp.サポートへのお問い合わせは、以下の連絡先もご利用いただけます。

1-877-457-5113 (通話料無料)

1-803-808-4270 (海外からのお問い合わせ)

メールアドレス: support@us.sios.com

20.2. VMware HA との統合

LifeKeeper Single Server Protection は、物理環境と仮想環境の両方で使用できるように設計されています。LifeKeeper SSP を VMware VM にインストールすると、VMware の HA 機能を LifeKeeper SSP と組み合わせることにより、保護されたリソースまたはノードの障害を監視および回復できます。これらの機能を有効にするには、LifeKeeper Single Server Protection と VMware HA 統合を有効にする を参照してください。

20.3. 管理

LifeKeeper Single Server Protection の管理

LifeKeeper Single Server Protectionでは、運用中の管理は不要です。LifeKeeper Single Server Protectionは自動的に動作して、保護対象のリソースを監視し、障害が発生した場合には指定されたリカバリーアクションを実行します。次の場合には、LifeKeeper Single Server Protection GUIを使用してください。

- **リソースおよび階層の定義** 。LifeKeeper Single Server Protectionは、次のインターフェースオプションを提供します。
    - ◦
        - º LifeKeeper Single Server Protection GUI。
        º LifeKeeper Single Server Protection コマンドラインインターフェース。

- **リソースの監視。** LifeKeeper Single Server Protection GUIから、リソースのステータス情報およびLifeKeeper Single Server Protectionログにアクセスできます。

- **手動による介入。** メンテナンスまたはその他の管理作業のために、サーバーまたは特定のリソースを停止する必要がある場合があります。LifeKeeper Single Server Protection GUIには、特定のリソースをIn ServiceまたはOut of Serviceにできるメニュー機能があります。アプリケーションがLifeKeeper Single Server Protectionの下に配置されると、これらのアプリケーションはLifeKeeper Single Server Protectionインターフェースを介してのみ起動および停止することができます。LifeKeeper Single Server Protectionの起動と停止は、コマンドラインからのみ実行できます。

リソース階層の作成など、管理、設定および保守操作の詳しい手順については、SPS for Windowsドキュメントのメンテナンス作業 を参照してください。

20.3.1. LifeKeeper Single Server ProtectionとVMware HAの統合を有効にする

LifeKeeper Single Server ProtectionがVMware VMにインストールされている場合、LifeKeeper Single Server ProtectiとVMware HAの統合はデフォルトでは無効になっています。統合を有効にするには、次の手順を実施する必要があります。

1. LifeKeeper Single Server Protection VMに、VMwareツールをインストールします。

2. *%LKROOT%\etc\default\LifeKeeper* を編集し、VMware HA統合の `HA_DISABLE` の値を1から0に変更します。

3. LifeKeeper Single Server Protectionを再起動します。LifeKeeper Single Server Protectionを実行中の場合は、上の手順で実施した *%LKROOT%\etc\default\LifeKeeper* の変更を有効にするために、停止して再起動する必要があります。

20.3.2. VMware HAの障害検出の有効化とリカバリシナリオ

アプリケーション内の問題の検出および警告機能は、最高の完全な耐障害性ソリューションを構築するためには必要不可欠です。特定のアプリケーションはすべてメカニズムと障害の形式が異なるため、一連の汎用メカニズムを使用することができません。

ただし、一般的には、多くのアプリケーション構成は、LifeKeeper Single Server Protectionで提供されているCoreシステムのエラー検出を使用できます。このトピックでは、LifeKeeper Single Server ProtectionのCore機能を説明します。

以下は、アプリケーションに障害が発生した場合にLifeKeeper Single Server Protectionが障害検出とリカバリを実施する方法を示すリカバリシナリオです。

1. LifeKeeper Single Server Protectionは、まずアプリケーションの再起動によるリカバリを試みます。

2. リカバリに成功した場合、アプリケーションは引き続き正常に実行されます。

3. リカバリに失敗した場合、以下のシナリオとなります。

    a. LifeKeeper Single Server Protectionのリカバリが失敗し、LifeKeeper Single Server ProtectionがHAが有効なVMwareゲストOSにインストールされている場合（%LKROOT%\etc\default\LifeKeeperでHA_DISABLE=0）、LifeKeeper Single Server Protectionは、アプリケーション監視インターフェースに送信するハートビートを保留することにより、VMware HAをトリガします。その後、VMware HAはサーバーを再起動して応答します。

    b. LifeKeeper Single Server Protectionのリカバリが失敗し、LifeKeeper Single Server ProtectionがVMwareゲストOSにインストールされていないか、VMwareゲストOSにインストールされているがHAが無効になっている場合（%LKROOT%\etc\default\LifeKeeperでHA_DISABLE=1）、システムは強制的に再起動されます。

オプションで、LifeKeeper Single Server Protectionを **通知専用** モードにすることができます。このモードでは、システムの再起動の自動トリガが無効になります（以下の「VMware HAと **通知専用** モード」セクションを参照）。**通知専用** モードでは、システムにログインして、障害の原因となった問題を修正する必要があります。

VMware HAと通知専用モード

1. **通知専用** モードを有効にするには、ファイル %LKROOT%\etc\default\LifeKeeper を編集し、値SSP_NOTIFICATION_ONLY=1を設定します。デフォルトでは、この値は0（無効）です。次に、ノードでLifeKeeper Single Server Protectionを再起動します。

2. **通知専用** のみモードで障害が検出されると、LifeKeeper Single Server Protectionはアプリケーションの再起動を試行しません。代わりに、リソースは **障害** としてマークされます。

3. CLIから **LifeKeeper管理コンソール** を開きます。

4. アプリケーションをIn Serviceに戻します。

20.3.3. VMware HAを使用したLifeKeeper Single Server Protectionハートビート

LifeKeeper Single Server ProtectionハートビートはVMware HAに送信される信号で（VMwareゲストOSで実行され、HAが有効になっている場合は10秒ごと）、保護対象のアプリケーションが正常であることを示します。アプリケーションで障害が発生すると、LifeKeeper Single Server Protectionは最初にアプリケーションのリカバリーを試みます。リカバリーに失敗した場合、LifeKeeper Single Server Protectionはハートビートを保留し、VMware HAはVMを再起動するよう指示されます。

20.3.4. LifeKeeper Single Server Protection で保護されているシステムのメンテナンス

LifeKeeper Single Server Protection で保護されているサーバでシステムまたはアプリケーションのメンテナンスを実施する場合は、LifeKeeper Single Server Protection の監視を停止するか、保護されたリソースをメンテナンスモードにする必要があります。これにより、アプリケーションのリカバリと VMware HA 障害イベントのトリガの両方が無効になり、LifeKeeper Single Server Protection はシステムおよびアプリケーションのメンテナンスタスクに干渉しなくなります。

LifeKeeper Single Server Protectionを停止して再起動するには、以下の手順を実行してください。

1. **LifeKeeper Single Server Protectionを停止する** 。***%LKROOT%\bin\lkstop.exe -f*** コマンドを使用して、LifeKeeper Single Server Protectionを停止します。リソースは実行中のままになりますが、LifeKeeper Single Server Protection による監視は停止されます。障害には手動で対応する必要があります。

2. **メンテナンスを実施する** 。必要なメンテナンスを実施してください。

3. **LifeKeeper Single Server Protectionを起動する** 。***%LKROOT%\bin\lkstart.exe*** コマンドを使用して、LifeKeeper Single Server Protection を起動します。リソースは保護されている状態になります。

20.4. アプリケーションリカバリーキット

LifeKeeper Single Server Protection Application Recovery Kits (ARKs) は特定のアプリケーションをLKSSP上で管理、制御するためのツールとユーティリティを含んでいます。今バージョンのLKSSPで利用できるARKは以下の通りです。

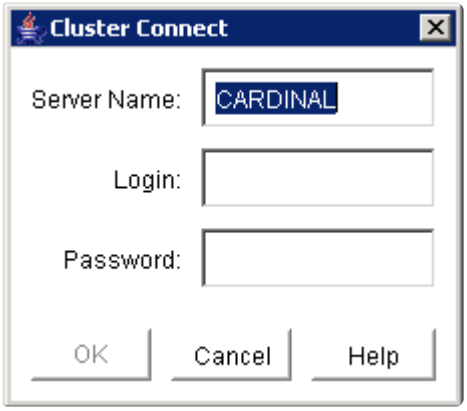
SIOS Protection Suite Microsoft SQL Server リカバリーキット

SIOS Protection Suite PostgreSQL Server リカバリーキット

SIOS Protection Suite Oracle リカバリーキット

SIOS Protection Suite Microsoft Internet Information Services リカバリーキット

[クラスタへの接続] ダイアログボックス



サーバ名 接続先サーバの名前を指定します。

ログイン 接続先サーバにある LifeKeeper を管理するユーザのログイン名を指定します。

パスワード 接続先サーバにログインするパスワードを指定します。

DataKeeper クイックスタートガイド

このトピックでは、DataKeeper Standard Edition のインストールと設定の手順を段階的に説明します。一連の手順には、各手順を詳細に説明したドキュメントへのリンクが含まれます。

前提条件とインストール

1. 最新情報については、SIOS Protection Suite for Windows リリースノート を参照してください。
2. ファイアウォール設定 : ファイアウォールで開く必要があるポートを確認してください。
3. ネットワーク帯域 : WAN 間で複製する場合は、十分な帯域を確保して変更の割合 分析を行うことが重要です。
4. DataKeeper はブロックレベルのボリュームレプリケーションソリューションであり、各サーバは、(システムドライブ以外に) サイズが同じ追加ボリュームを持つ必要があります。ストレージ要件の詳細については、ボリュームの考慮事項 を参照してください。
5. DataKeeper の仕組みと、同期レプリケーションと非同期レプリケーションの違いについては、レプリケーションについて セクションを参照してください。
6. インストール/アップグレード時に、DataKeeper サービスの起動に使用するユーザアカウントの選択と設定を求められます。各サーバでドメインアカウントを使用することをお勧めします (同じパスワードを持つ同一アカウント)。このアカウントは、各サーバのローカル管理者グループに追加する必要があります。**各サーバ** で以下の操作を実行します。

   a. **[ローカルユーザとグループの編集]** を選択します。

   b. **[グループ]** 、**[管理者]** の順に選択します。

   c. 使用する **DK サービスアカウント** をこの管理者グループに追加します。

これらのアカウントの詳細については、以下のトピックを参照してください。

DataKeeper サービスログオン ID とパスワードの選択

サーバログインアカウントおよびパスワードはクラスタの各サーバで同一である必要がある

7. ネットワークアダプタを設定 します。
8. セクタサイズ と GUI の要件、プラットフォーム、およびブラウザ を参照してください。
9. ブラウザのセキュリティ設定 を低くします。
10. イベントログを必要に応じて上書きするように 設定します。
11. **Distributed Link Tracking Client サービス** を無効にし、起動ポリシーを **手動** に設定します。
12. 高速ストレージを使用する場合は、高速ストレージのベストプラクティス を参照してください。

構成

1. データ保護の要件に適合するレプリケーション方式を選択します。可能な構成オプションを以下のリンクに示します。
   ディスクからディスク

1 対 1
1 対多 (マルチターゲット)
多対 1

2. DataKeeper UI を使用してジョブを作成します 。ジョブ作成プロセスでは、1 つ目のミラーも追加します。

3. 追加のミラーが必要な場合は、ジョブにミラーを追加する ことができます。

4. 1 対多 のレプリケーション方式を作成する場合は、複数ターゲットとのミラーの作成 を参照してください。

注記: 「ミラー」は、ソースボリューム、ターゲットボリューム、ソース IP、およびターゲット IP から構成されます。「ジョブ 」は、1 つ以上の関連する「ミラー」から構成されます。例えば、データ用の E:\ ボリュームとログファイル用の F:\ ボリュームで構成されるデータベースを複製する場合、E:\ ボリュームと F:\ ボリュームを同じ「ジョブ」に配置します。ただし、G:\、H:\、I:\ の各ボリュームに 1 つずつ、3 つの VM がある場合は、VM 自体は互いに関連していないので、個別のジョブを 3 つ作成します。一般的に、ミラーをグループとして移動する必要がある場合には、常に同じジョブにまとめます。

管理

一般的な管理機能を以下に示します。

ミラーのスイッチオーバ

ミラーの管理

一時停止およびロック解除

再開/ロック

中断

再同期

ミラーの削除

ミラープロパティ

既存のミラーの圧縮レベルの変更

DataKeeper ボリュームのサイズ変更

よくある質問. も参照してください。

詳細については、DataKeeper for Windows テクニカルドキュメンテーション. セクションを参照してください。

Hyper-V 仮想マシンの複製

DataKeeper を使用して非クラスタ環境で Hyper-V VHD ファイルを複製する場合、これらの複製 VHD ファイルに基づいた仮想マシンにアクセスし、準備する方法を理解する必要があります。Hyper-V 仮想マシンのディザスタリカバリを行う の手順に従ってください。

トラブルシューティング

以下のリソースはトラブルシューティングに役立ちます。

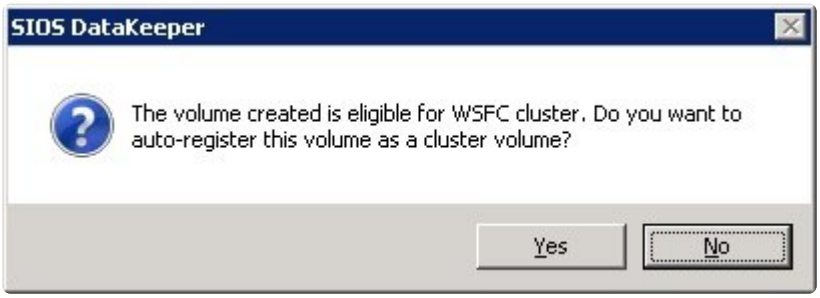
- トラブルシューティング セクション
- サポート契約を結んだお客様向け: support.us.sios.com/aspx/SupportHome
- 評価版を使用しているお客様のみ - Pre-sales support

WSFC で DataKeeper ボリュームリソースを作成する

WSFCでミラーを自動的に作成する

1. SIOS DataKeeper GUI を使用してミラーを設定します。

2. ミラーの作成処理の最後に、WSFC にミラーを DataKeeper ボリュームリソースとして自動的に追加するかどうかを確認する以下のダイアログボックスが表示されます。



[はい] を選択すると、DataKeeper ミラーが **DataKeeper ボリュームリソース** として WSFC の「 **使用可能記憶域** 」に追加されます。**[いいえ]** を選択した場合またはエラーになってしまった場合は、「WSFC でミラーを手動で作成する 」を参照し、手動でミラーを作成してください。

> ✻ 注記: DataKeeper ボリュームが使用可能記憶域としてリストされている場合、DataKeeper は高可用性には **なりません** 。DataKeeper ボリュームリソースは、Windows サーバーフェールオーバー クラスターの役割（SQL、Oracle、SAP、ファイルサーバー、Hyper-V、または汎用サービス）に割り当てられた後にのみ高可用性になります。
>
> 使用可能記憶域のスイッチオーバーを（役割に追加される前に）実行する必要がある場合、WSFC から使用可能記憶域を削除します。DataKeeper GUI では、アクションパネルの [Switchover Mirrors] オプションが太字になり、スイッチオーバーに使用できるようになります。

ミラーが自動的または手動で作成されたかに関係なく、DataKeeper ボリュームリソースは「 **使用可能記憶域** 」に保存されます。DataKeeper ボリュームリソースは、物理ディスクリソースのように使用されます。アプリケーション (例えば SQL) のクラスタリングを行う場合、DataKeeper ボリュームリソースは、物理ディスクリソースそのものとして認識され、同じように扱われます。これは、クラスタの作成を行っている間、DataKeeper ボリュームリソースがクラスタリソースへ自動的に組み込まれ、自動的に依存関係が作成されるということを意味しています。その他のアプリケーション、特に Hyper-V「バーチャルマシン」リソースでは、物理ディスクリソースを探すことがコード化されており、自動的に DataKeeper のリソースをクラスタ構成に組み込むことができません。このように、WSFC の GUI を使用して簡単に DataKeeper ボリュームリソースをクラスタリソースに追加し、手動で依存関係を作成することが可能です。

ミラーリング状態を監視するには、DataKeeper GUI を使用してください。この GUI には、フェイルオーバクラスタマネージャ UI よりも詳細な情報が表示されます。

WSFC でミラーを手動で作成する

1. ミラーが **ミラーリング** の状態になるまで待ちます。

2. **空のアプリケーション** を作成します。

   - **Microsoft Windows Failover Cluster GUI** を開きます。
   - **[サービスとアプリケーション]** の上で右クリックします (***Windows 2012*** では、***[役割]*** の上で右クリック)。
   - **[その他のアクションを展開]** へ。(***Windows 2012*** では不要)。
   - **[空のサービスまたはアプリケーションを作成]** を選択します (***Windows 2012*** *では、**[空の役割の作成]** を選択*)。
   - 新しく作成されたサービスの上で右クリックし、**[プロパティ]** を選択します。
   - 空のアプリケーションを **DataKeeper サービス** に名前を変更します。

3. 空のアプリケーションにリソースを追加します。

   - **[DataKeeper サービス]** の上で右クリックします。
   - **[リソースの追加]** を選択します。
   - **[その他のリソース]** から **[DataKeeper Volume の追加]** を選択します。

4. 新しく追加されたリソースの **[プロパティ]** を開き、**[リソース名]** を「 **DataKeeper Volume E** 」(E ドライブを示す) のような別のわかりやすい名前に変更します。**[DataKeeper Volume パラメータ]** タブを選択し、リソースとドライブレター (上記の例の E) を関連付けます。すべてのミラーボリュームのリストが表示されます。このリソースで管理するボリュームを選択します。

5. リソースの上で右クリックし、**[オンラインにする]** を選択します。DataKeeper Volume リソースがオンラインになったことを必ず確認してください。**注記:** オンラインの状態になったリソースはロック解除されます。オフライン状態になったリソースはロックされます　。

6. WSFC で保護する他のすべての DataKeeper Volume に対して、**手順 3 および 4** の操作を繰り返します。

7. 次の手順でリソースを使用可能記憶域に移動させます。

   - **[サービスとアプリケーション]** タブを展開します。
   - 先ほど作成した DataKeeper サービスを選択し、リソースをメモします
   - メイン画面からリソース (すなわち DataKeeper ボリューム E) を選択します。
   - 右クリックして **[DataKeeper サービスから削除]** を選択します。この操作で、リソースが **使用可能記憶域** に移動します。
   - 他のすべてのボリュームに対してこの操作を繰り返します。

8. 手順 2 で作成した空のアプリケーションを削除します。

従来の 2 ノード構成のクラスタを共有複製構成に拡張する

Windows Server 2008 R2、または 2012 を使用して共有ノードを追加する

Windows Server 2008 R2、または 2012 で、DataKeeper ボリュームを使用する 1×1 2 ノードレプリケーションクラスタを 2×1 共有ディスクとレプリケーションの 3 ノードクラスタに拡張するには、以下のいずれかの方法を使用してください。

- WSFC GUI
- WSFC コマンドラインツール : "cluster /add /node:<スタンバイノード名>"
- powershell コマンド : "Add-ClusterNode -Name <ホスト名>"

Windows Server 2008 R2、2012 では、共有ディスクを持つノードが追加された場合、DataKeeper 共有ディスクは、クラスタ内の DataKeeper ボリュームリソースのまま残ります。これは、共有ディスクはクラスタ内のすべてのノードでアクセス可能になることはなく、3 ノードクラスタ内の 2 つのシステムでのみアクセス可能になるためです。DataKeeper ボリュームリソースが WSFC 物理ディスクリソースに変換されないことは非常に重要です。

Windows Server 2008 R2「SP1」を使用して共有ノードを追加する

警告: Windows Server 2008 R2「SP1」における WSFC mmc GUI の動作は変更されました。

WSFC 2008 R2 SP1 以降、Microsoft はクラスタにノードを追加したときの WSFC mmc GUI の動作を変更しました。新しいノードがクラスタ内ですでに 1 つ以上の他のシステムによって共有されているディスクをホストしている場合、新しいノード上の共有ディスクおよび既存の DataKeeper ボリュームリソースは、クラスタにノードを追加したときに自動的に WSFC 物理ディスクリソースに変換されます。変換プロセスでボリュームレターが変更され、これによって DataKeeper ボリュームリソースおよび関連付けられたレプリケーションミラーが切断されます。クラスタ化されたアプリケーションは影響を受ける可能性があります。

Windows Server 2008 R2 SP1 を使用している場合、新しいノードが DataKeeper 共有ディスクをホストしているときには、WSFC GUI を使用してクラスタにノードを追加しないでください。

Windows Server 2008 R2 SP1 を使用している場合、DataKeeper 共有ボリュームを持つ追加ノードを WSFC クラスタに安全に追加するには、以下のように WSFC コマンドラインツールを使用する必要があります。

- WSFC コマンドラインツール: “cluster /add /node:<standby node name>”