Dell EMC Data Domain® Operating System

バージョン 6.2

管理ガイド

302-005-407
REV. 01

DELL EMC

2018 年 12 月発行

EMC ジャパン株式会社
〒 151-0053 東京都渋谷区代々木 2-1-1 新宿マインズタワー
www.DellEMC.com/ja-jp/index.htm
お問い合わせは
www.DellEMC.com/ja-jp/index.htm

目次

はじめに 17

第 1 章 **Data Domain システムの機能および統合** 21
改訂履歴 22
Data Domain システムの概要 22
Data Domain システムの機能 22
データの整合性 23
データ重複排除 23
リストア処理 24
Data Domain Replicator 24
マルチパスとロード バランシング 24
高可用性 24
ランダム I/O 処理 26
システム管理者のアクセス 26
ライセンス機能 27
ストレージ環境の統合 28

第 2 章 **はじめに** 31
Dell EMC Data Domain System Manager の概要 32
DD System Manager へのログインとログアウト 32
証明書を使用したログイン 35
DD System Manager インターフェイス 36
ページ要素 36
バナー 36
ナビゲーション パネル 36
情報パネル 37
フッター 37
［Help］ボタン 38
使用許諾契約書 38
構成ウィザードを使用したシステムの構成 38
［License］ページ 38
Network 39
File System 41
System Settings 46
DD Boost プロトコル 47
CIFS プロトコル 48
NFS プロトコル[NFS ぷろとこる] 49
DD VTL プロトコル 50
Data Domain のコマンド ライン インターフェイス 51
CLI へのログイン 52
CLI のオンライン ヘルプのガイドライン 52

第 3 章 **Data Domain システムの管理** 55
システム管理の概要 56
HA システム管理の概要 56

HA システムの計画的保守 57
システムの再起動 57
システム電源のオン/オフ 57
システムの電源オン 58
システム アップグレードの管理 59
アップグレード前のチェックリストと概要 60
システムでのアップグレード パッケージの表示 65
アップグレード パッケージの取得と確認 65
Data Domain システムのアップグレード 66
アップグレード パッケージの削除 68
電子ライセンスの管理 68
HA システムのライセンス管理 69
システム ストレージの管理 69
システム ストレージ情報の表示 70
エンクロージャの物理的配置 75
ディスクの物理的な場所の確認 75
ストレージの構成 75
DD3300 容量拡張 76
ディスクの障害と障害解除 77
ネットワーク接続の管理 78
HA システムのネットワーク接続管理 78
ネットワーク インターフェイスの管理 78
一般的なネットワーク設定の管理 94
ネットワーク ルートの管理 97
システム パスフレーズの管理 100
システム パスフレーズの設定 101
システム パスフレーズの変更 101
システム アクセスの管理 102
役割に基づいたアクセス制御 102
IP プロトコルのアクセス管理 104
ローカル ユーザー アカウントの管理 111
ディレクトリ ユーザーおよびグループの管理 119
認証に関する問題の診断 133
システムの認証方法の変更 134
メール サーバー設定の構成 135
日付と時刻の設定の管理 136
システム プロパティの管理 136
SNMP 管理 SNMP かんり 137
SNMP ステータスおよび構成の表示 137
SNMP の有効化/無効化 139
SNMP MIB のダウンロード 139
SNMP プロパティの構成 140
SNMP V3 ユーザーの管理 140
SNMP V2C Community の管理 142
SNMP トラップ ホストの管理 144
自動サポート レポートの管理 146
HA システムの自動サポートとサポート バンドルの管理性 146
Data Domain への自動サポート レポートの有効化および無効化 146
生成された自動サポート レポートの確認 147
自動サポート メーリング リストの構成 147
Data Domain が外部の受信者に ASUP とアラートのメールを送信できることを確認する 148

サポート バンドルの管理 149
サポート バンドルの生成 149
サポート バンドル リストの表示 150
コアダンプの管理 150
アラート通知の管理 151
HA システム アラート通知の管理 151
通知グループ リストの表示 152
通知グループの作成 153
グループのサブスクライバー リストの管理 154
通知グループの変更 155
通知グループの削除 155
通知グループ構成のリセット 156
日次サマリー スケジュールと配布リストの構成 156
Data Domain へのアラート通知の有効化および無効化 157
アラート メール機能のテスト 158
サポート デリバリの管理 158
Data Domain への標準メール デリバリの選択 159
セキュア リモート サービス デリバリの選択と設定 159
ConnectEMC の動作テスト 160
ログ ファイルの管理 160
DD System Manager でのログ ファイルの表示 161
CLI でのログ ファイルの表示 161
ログ メッセージの詳細について 162
ログ ファイルのコピーの保存 163
リモート システムへのログ メッセージの転送 164
IPMI によるリモート システムの電源管理 165
IPMI および SOL 制限 165
DD System Manager を使用した IPMI ユーザーの追加と削除 166
IPMI ユーザー パスワードの変更 167
IPMI ポートの構成 167
CLI を使用したリモート電源管理とコンソール モニタリングの準備 168
DD System Manager による電源の管理 170
CLI による電源の管理 170

第 4 章 Data Domain システムのモニタリング 173
個々のシステム ステータスおよび識別情報の表示 174
［Dashboard Alerts］領域 174
［Dashboard File System］領域 175
［Dashboard Services］領域 175
［Dashboard HA Readiness］領域 175
［Dashboard Hardware］領域 176
［Maintenance System］領域 176
［Health Alerts］パネル 176
現在のアラートの表示およびクリア 177
［Current Alerts］タブ 177
アラート ヒストリの表示 178
［Alerts History］タブ 178
ハードウェア コンポーネント ステータスの表示 179
ファン ステータス 180
温度ステータス 180
管理パネルのステータス 181

SSD ステータス（DD6300 のみ）.....181
電源ステータス.....181
PCI スロット ステータス.....181
NVRAM ステータス.....182
システム統計の表示.....182
パフォーマンス統計グラフ.....183
アクティブ ユーザーの表示.....184
ヒストリ レポートの管理.....184
レポートのタイプ.....185
タスク ログの表示.....188
システムの高可用性ステータスの表示.....189
高可用性のステータス.....189

第 5 章 ファイル システム 193
ファイル システムの概要.....194
ファイル システムによるデータの保存方法.....194
ファイル システムによるスペース使用率のレポート方法.....194
ファイル システムによる圧縮の使用.....194
ファイル システムによるデータの整合性の実装.....196
ファイル システムがファイル システム クリーニングによってストレージ領域を再利用する方法.....196
サポートされるインターフェイス.....197
対応しているバックアップ ソフトウェア.....197
新しい Data Domain システムに送信されるデータ ストリーム.....197
ファイル システムの制限.....200
ファイル システムの使用状況のモニタリング.....201
［File System］ビューへのアクセス.....201
ファイル システム操作の管理.....209
基本操作の実行.....209
クリーニングの実行.....211
浄化の実行.....214
基本設定の変更.....215
Fast Copy 操作.....217
Fast Copy 操作の実行.....218

第 6 章 MTree 219
MTree の概要.....220
MTree の制限.....220
クォータ.....220
［MTree］パネルについて.....221
［Summary］ビューについて.....221
［Space Usage］ビューについて（MTree）.....226
［Daily Written］ビューについて（MTree）.....226
MTree 使用状況のモニタリング.....227
物理容量の測定について.....227
MTree 操作の管理.....231
MTree の作成.....231
MTree クォータの構成と有効化/無効化.....232
MTree の削除.....233
MTree の復元.....233

MTree の名称変更....234

第 7 章 スナップショット 235
スナップショットの概要....236
スナップショットとそのスケジュールのモニタリング....237
［Snapshots］ビューについて....237
スナップショットの管理....238
スナップショットの作成....238
スナップショットの有効期限の変更....239
スナップショットの名称変更....239
スナップショットの期限切れ....239
スナップショット スケジュールの管理....240
スナップショット スケジュールの作成....240
スナップショット スケジュールの変更....241
スナップショット スケジュールの削除....242
スナップショットからのデータのリカバリ....242

第 8 章 CIFS 243
CIFS の概要....244
SMB 署名の構成....244
CIFS のセットアップの実行....245
HA システムと CIFS....245
Data Domain システムにアクセスするためのクライアントの準備....245
CIFS サービスの有効化....245
CIFS サーバーの命名....246
認証パラメーターの設定....246
CIFS サービスの無効化....247
共有の扱い....247
Data Domain システムでの共有の作成....247
Data Domain システムでの共有の変更....250
既存の共有からの共有の作成....250
Data Domain システムでの共有の無効化....251
Data Domain システムでの共有の有効化....251
Data Domain システムでの共有の削除....251
MMC 管理の実行....251
CIFS クライアントからの Data Domain システムへの接続....252
CIFS 情報の表示....253
アクセス制御の管理....253
Windows クライアントからの共有へのアクセス....254
ドメイン ユーザーへの管理アクセスの付与....254
Data Domain システムへのドメイン ユーザーによる管理アクセスの許可....254
Windows からの管理アクセスの制限....255
ファイル アクセス....255
CIFS 操作のモニタリング....258
CIFS ステータスの表示....258
CIFS 構成の表示....259
CIFS 統計の表示....261
CIFS のトラブルシューティングの実行....261
クライアントの現在のアクティビティの表示....261
接続上での最大オープン ファイル数の設定....262

Data Domain システム クロック..... 262
Windows ドメイン コントローラーからの同期.....263
NTP サーバーからの同期.....263

第 9 章 NFS 265
NFS の概要.....266
HA システムと NFS.....266
Data Domain システムへの NFS クライアント アクセスの管理..... 267
NFS サービスの有効化.....267
NFS サービスの無効化.....267
エクスポートの作成.....267
エクスポートの変更.....269
既存のエクスポートからのエクスポートの作成..... 270
エクスポートの削除.....270
NFS 情報の表示.....271
NFS ステータスの表示..... 271
NFS エクスポートの表示.....271
アクティブな NFS クライアントの表示.....271
Kerberos ドメインへの DDR の統合.....272
初期構成後の KDC サーバーの追加と削除..... 274

第 10 章 NFSv4 277
NFSv4 の概要..... 278
Data Domain システムでの NFSv3 と NFSv4 の比較.....278
NFSv4 ポート..... 279
ID マッピングの概要.....279
外部フォーマット.....279
標準の識別子フォーマット..... 279
ACE 識別子の拡張..... 280
代替フォーマット.....280
内部識別子のフォーマット.....280
ID マッピングが発生するタイミング..... 281
インプット マッピング..... 281
出力のマッピング.....281
資格情報のマッピング..... 282
NFSv4 と CIFS/SMB の相互運用性..... 282
CIFS/SMB Active Directory の統合.....283
NFSv4 のデフォルト DACL.....283
System Defaults SID.....283
NFSv4 ACL と SID の共通識別子.....283
NFS 参照.....283
参照のロケーション..... 284
参照のロケーション名.....284
参照とスケール アウト システム..... 284
NFSv4 と高可用性.....285
NFSv4 グローバル ネームスペース.....285
NFSv4 グローバル ネームスペースと NFSv3 サブマウント..... 285
NFSv4 構成..... 286
NFSv4 サーバの有効化.....286
NFSv4 を含めるデフォルト サーバ設定.....287

既存のエクスポートの更新....287
Kerberos と NFSv4....287
Linux ベースの KDC における Kerberos の構成....288
Kerberos 認証を使用する Data Domain システムの構成....289
クライアントの構成....290
Active Directory の有効化....290
Active Directory の構成....291
Active Directory のクライアントを構成します。....291

第 11 章 ストレージ移行 293
ストレージ移行の概要....294
移行計画に関する考慮事項....294
DS60 シェルフに関する考慮事項....296
移行ステータスの表示....296
移行準備の評価....296
DD System Manager を使用したストレージ移行....297
ストレージ移行のダイアログ説明....298
［Select a Task］ダイアログ....298
［Select Existing Enclosures］ダイアログ....298
［Selectct New Enclosures］ダイアログ....298
［Review Migration Plan］ダイアログ....299
［Verify Migration Preconditions］ダイアログ....299
［Migration progress］ダイアログ....300
CLI を使用したストレージ移行....300
CLI でのストレージ移行の例....302

第 12 章 Metadata on Flash 307
MDoF（Metadata on Flash）の概要....308
MDoF のライセンスと容量....309
SSD キャッシュ階層....310
MDoF SSD キャッシュ階層 - システム管理....310
SSD キャッシュ階層の管理....310
SSD のアラート....313

第 13 章 SCSI ターゲット 315
SCSI ターゲットの概要....316
［Fibre Channel］ビュー....317
NPIV の有効化....317
NPIV の無効化....320
［Resources］タブ....321
［Access Groups］タブ....328
DD OS バージョンでの FC リンク モニタリングの違い....328

第 14 章 DD Boost の扱い 329
Data Domain Boost....330
DD System Manager による DD Boost の管理....331
DD Boost ユーザー名の指定....331
DD Boost ユーザー パスワードの変更....332
DD Boost ユーザー名の削除....332

DD Boost の有効化....332
Kerberos の構成....332
DD Boost の無効化....333
DD Boost ストレージ ユニットの表示....333
ストレージ ユニットの作成....334
ストレージ ユニット情報の表示....336
ストレージ ユニットの変更....338
ストレージ ユニットの名称変更....339
ストレージ ユニットの削除....340
ストレージ ユニットの復元....340
DD Boost オプションの選択....341
DD Boost の証明書の管理....342
DD Boost クライアントのアクセスと暗号化の管理....344
インターフェイス グループについて....346
インタフェース....347
クライアント....348
インターフェイス グループの作成....348
インターフェイス グループの有効化/無効化....349
インターフェイス グループの名前とインターフェイスの変更....349
インターフェイス グループの削除....350
インターフェイス グループへのクライアントの追加....350
クライアントの名前またはインターフェイス グループの変更....351
インターフェイス グループからのクライアントの削除....351
MFR（管理ファイル レプリケーション）でのインターフェイス グループの使用352
DD Boost の破棄....353
DD Boost over Fibre Channel の構成....354
DD Boost ユーザーの有効化....354
DD Boost の構成....355
接続の検証とアクセス グループの作成....356
HA システムで DD Boost を使用....358
［DD Boost］タブについて....359
Settings....359
アクティブな接続....359
IP ネットワーク....361
ファイバー チャネル....361
Storage Units....361

第 15 章　DD 仮想テープ ライブラリ　363
DD 仮想テープ ライブラリの概要....364
DD VTL の計画....364
DD VTL の制限....365
DD VTL でサポートされるドライブ数....368
テープ バーコード....369
LTO テープ ドライブ互換性....370
DD VTL の設定....370
HA システムと DD VTL....371
DD VTL テープからクラウドへ....371
DD VTL の管理....371
DD VTL の有効化....373
DD VTL の無効化....373
DD VTL オプションのデフォルト....373

DD VTL デフォルト オプションの構成 374
ライブラリの扱い 375
ライブラリの作成 376
ライブラリの削除 378
テープの検索 378
選択されたライブラリの扱い 379
テープの作成 380
テープの削除 380
テープのインポート 381
テープのエクスポート 383
ライブラリ内のデバイス間のテープの移動 384
スロットの追加 385
スロットの削除 386
CAP の追加 386
CAP の削除 387
チェンジャー情報の表示 387
ドライブの扱い 388
ドライブの作成 389
ドライブの削除 389
選択されたドライブの扱い 390
テープの扱い 390
テープの書き込みまたは保存ロック状態の変更 391
ヴォールトの扱い 392
クラウド ベースのヴォールトの使用 392
データ移行のための VTL プールの準備 393
バックアップ アプリケーション インベントリからのテープの削除 395
データ移行するテープ ボリュームの選択 395
クラウド上のデータの復元 397
クラウド ストレージからのテープ ボリュームの手動リコール 397
アクセス グループの扱い 399
アクセス グループの作成 399
アクセス グループの削除 403
選択されたアクセス グループの扱い 403
デバイスのエンドポイントの選択 404
NDMP デバイス TapeServer グループの構成 404
リソースの処理 406
イニシエーターの扱い 407
エンドポイントの扱い 408
選択されたエンドポイントの扱い 409
プールの扱い 410
プールの作成 411
プールの削除 412
選択されたプールの扱い 413
ディレクトリ プールの MTree プールへの変換 415
プール間でのテープの移動 416
プール間でのテープのコピー 417
プールの名称変更 417

第 16 章 DD Replicator 419
DD Replicator の概要 420
レプリケーション構成の前提条件 421

レプリケーション バージョンの互換性 423
レプリケーション タイプ 428
管理ファイル レプリケーション 429
ディレクトリ レプリケーション 430
MTree レプリケーション 431
コレクション レプリケーション 433
DD Replicator と DD Encryption の使用 434
レプリケーション トポロジー 435
1 対 1 レプリケーション 436
双方向レプリケーション 436
1 対多レプリケーション 437
多対 1 レプリケーション 438
カスケード レプリケーション 438
レプリケーションの管理 439
レプリケーション ステータス 440
［Summary］ビュー 440
［DD Boost］ビュー 450
パフォーマンス ビュー 452
［Advanced Settings］ビュー 452
レプリケーションのモニタリング 455
バックアップ ジョブの推定完了時間の表示 455
レプリケーション コンテキストのパフォーマンスのチェック 456
レプリケーション進行状態のステータス追跡 456
レプリケーション ラグ 456
レプリケーションと HA 456
クォータのあるシステムからクォータのないシステムへのレプリケーション 457
レプリケーション スケーリング コンテキスト 457
ディレクトリから MTree へのレプリケーションの移行 458
ディレクトリ レプリケーションから MTree レプリケーションへの移行の実行 458
ディレクトリから MTree への移行の進行状況の表示 459
ディレクトリから MTree へのレプリケーションの移行ステータスの確認 460
D2M レプリケーションの中止 460
D2M のトラブルシューティング 461
D2M のトラブルシューティング（追加） 462
ディザスタリカバリ用コレクション レプリケーションおよび SMT の使用 462

第 17 章 DD Secure Multitenancy 465
Data Domain Secure Multitenancy の概要 466
SMT アーキテクチャの基本 466
SMT（Secure Multi-Tenancy）で使用される用語 466
制御パスとネットワークの分離 467
SMT の RBAC とは 468
テナント ユニットのプロビジョニング 469
テナント セルフサービス モードの有効化 473
プロトコルによるデータ アクセス 473
SMT における Multi-User DD Boost とストレージ ユニット 473
CIFS のアクセスの構成 474
NFS アクセスの構成 474
DD VTL のアクセスの構成 475
DD VTL NDMP TapeServer の使用 475
データ管理操作 475

パフォーマンス統計の収集 475
クォータの変更 476
SMT とレプリケーション 476
SMT テナント アラート 477
スナップショットの管理 478
ファイル システム Fast Copy の実行 478

第 18 章 DD Cloud Tier 479
DD Cloud Tier の概要 480
サポートするプラットフォーム 480
DD Cloud Tier のパフォーマンス 482
クラウド階層の構成 483
DD Cloud Tier のストレージの構成 483
クラウド ユニットの構成 485
ファイアウォールとプロキシの設定 485
CA 証明書のインポート 486
ECS（Elastic Cloud Storage）用のクラウド ユニットの追加 487
Virtustream 用のクラウド ユニットの追加 488
Alibaba 用のクラウド ユニットの追加 489
Amazon Web Services S3 用のクラウド ユニットの追加 491
Azure 用のクラウド ユニットの追加 492
Google Cloud Provider 向けのクラウド ユニットの追加 493
S3 フレキシブル プロバイダ クラウド ユニットの追加 495
クラウド ユニットまたはクラウド プロファイルの修正 496
クラウド ユニットの削除 497
データの移動 498
MTree へのデータ移動ポリシーの追加 498
手動データ移動 499
自動データ移動 499
Cloud Tier からのファイルのリコール 500
CLI を使用したクラウド階層からのファイルのリコール 501
クラウド階層からのダイレクト リストア 502
コマンド ライン インターフェイス（CLI）による DD Cloud Tier の構成 503
DD クラウド ユニットの暗号化の構成 506
システムが失われた場合に必要な情報 507
クラウド階層での DD Replicator の使用 508
クラウド階層での DD VTL（仮想テープ ライブラリ） の使用 508
DD Cloud Tier の容量消費グラフの表示 508
DD Cloud Tier のログ 509
CLI（コマンド ライン インターフェイス）による DD Cloud Tier の削除 509

第 19 章 DD Extended Retention 513
DD Extended Retention の概要 514
DD Extended Retention でサポートされルプロトコル 515
高可用性と Extended Retention 516
DD Extended Retention を使用した DD Replicator の使用 516
DD Extended Retention を使用したコレクション レプリケーション 516
DD Extended Retention を使用したディレクトリ レプリケーション 517
DD Extended Retention を使用した MTree レプリケーション 517
DD Extended Retention を使用した管理ファイル レプリケーション 517

DD Extended Retention のハードウェアとライセンス..... 518
DD Extended Retention の対応ハードウェア..... 518
DD Extended Retention のライセンス..... 521
DD Extended Retention 用のシェルフ容量ライセンスの追加..... 521
DD Extended Retention 用のストレージの構成..... 522
DD Extended Retention を使用するお客様提供のインフラストラクチャ. 522
DD Extended Retention の管理..... 522
DD Extended Retention 用の DD システムの有効化..... 523
DD Extended Retention 用の 2 階層型ファイル システムの作成..... 524
DD Extended Retention の［File System］パネル..... 525
DD Extended Retention の［File System］タブ..... 527
DD Extended Retention を使用したアップグレードおよびリカバリ..... 532
DD Extended Retention を使用した DD OS 5.7 へのアップグレード..... 532
DD Extended Retention を使用したハードウェアのアップグレード..... 533
DD Extended Retention が有効なシステムのリカバリ..... 533
アーカイブ階層から DD Cloud Tier へのデータの移行..... 534
キャパシティ プランニング..... 535
アーカイブ階層へのデータ移動の停止..... 537
ファイルの場所を確認する..... 538
Data Domain レプリケーション ライセンスの適用..... 538
ソース システムからターゲット システムへのレプリケーションの開始..... 539
レプリケーションの進行状況の監視..... 541
レプリケーションの初期化の完了または同期の確認..... 541
レプリケーション コンテキストを中断する..... 541
ソース システムのリパーパス..... 542
ターゲットシステムでの DD Cloud Tier の構成..... 543

第 20 章 DD Retention Lock 549
DD Retention Lock の概要..... 550
DD Retention Lock プロトコル..... 551
DD Retention Lock のフロー..... 551
対応するデータ アクセス プロトコル..... 552
MTree における DD Retention Lock の有効化..... 553
MTree における DD Retention Lock Governance の有効化..... 553
MTree における DD Retention Lock Compliance の有効化..... 554
クライアント側保存ロック ファイル コントロール..... 556
ファイルの保存ロックの設定..... 557
ファイルの保存ロックの延長..... 559
保存ロックされたファイルの識別..... 560
ディレクトリの指定とそのファイルのみのタッチ..... 560
ファイルのリストの読み取りとそのファイルのみのタッチ..... 560
ファイルの削除または失効..... 561
保存ロックされたファイルに対する ctime または mtime の使用..... 561
DD Retention Lock を使用したシステムの動作..... 561
DD Retention Lock Governance..... 562
DD Retention Lock Compliance..... 563

第 21 章 DD Encryption 575
DD 暗号化の概要..... 576
暗号化の構成..... 577
鍵管理について..... 577

紛失または破損したキーの修正 578
キー マネージャー サポート 578
RSA DPM Key Manager の処理 579
Embedded Key Manager の扱い 582
KeySecure Key Manager での作業 582
DD System Manager による KeySecure Key Manager のセット アップと管理 583
Data Domain CLI による KeySecure Key Manager の管理 585
クリーニング操作の機能 589
キー マネージャーのセットアップ 589
RSA DPM Key Manager の暗号化のセットアップ 589
KMIP キー マネージャの設定 592
セットアップ後のキー マネージャーの変更 594
RSA Key Manager の証明書の管理 595
静止データの暗号化設定のチェック 596
静止データの暗号化の有効化と無効化 596
静止データの暗号化の有効化 596
静止データの暗号化の無効化 596
ファイル システムのロックとロック解除 597
ファイル システムのロック 597
ファイル システムのロック解除 598
暗号化アルゴリズムの変更 598

はじめに

製品ラインを改善するための努力の一環として、Data Domain ではソフトウェアおよびハードウェアのリビジョンを定期的にリリースしています。そのため、このドキュメントで説明されている機能の中には、現在お使いのソフトウェアまたはハードウェアのバージョンによっては、サポートされていないものもあります。製品リリース ノートには、製品の機能、ソフトウェア アップデート、ソフトウェア互換性ガイドの最新情報、Data Domain の製品、ライセンス、サービスについて記載されています。

製品が正常に機能しない、またはこのマニュアルの説明どおりに動作しない場合には、テクニカル サポート プロフェッショナルにお問い合わせください。

注

このマニュアルには、発行時点で正確だった情報が記載されています。オンライン サポート（https://support.emc.com）にアクセスして、このマニュアルの最新バージョンを使用していることを確認してください。

目的

本ガイドでは、DD System Manager（Data Domain System Manager）、ブラウザ ベース GUI（グラフィカル ユーザー インターフェイス）を使用した手順に焦点を当て、Data Domain®システムの管理方法について説明します。重要な管理タスクが DD System Manager で対応していない場合、CLI（コマンド ライン インターフェイス）について説明します。

注

- DD System Manager は、以前は Enterprise Manager と呼ばれていました。
- CLI コマンドのオプションの方が、対応する DD System Manager 機能よりも多い場合があります。完全なコマンドとオプションの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

対象読者

本ガイドは、標準バックアップ パッケージと一般バックアップ管理に精通したシステム管理者向けです。

関連ドキュメント

詳細については、次の Data Domain システム ドキュメントを参照してください。

- 「Data Domain DD9300 System Installation Guide」など、お使いのシステムのインストールおよびセットアップ ガイド
- 「Data Domain ハードウェアの機能および仕様ガイド」
- 「 Data Domain Operating System USB Installation Guide」
- 「 Data Domain Operating System DVD Installation Guide」
- 「Data Domain オペレーティング システム リリース ノート」
- 「Data Domain Operating System 初期構成ガイド」
- 「Data Domain セキュリティ構成ガイド」
- 「Data Domain Operating System High Availability ホワイト ペーパー」
- 「Data Domain オペレーティング システム コマンド リファレンス ガイド」

- 「Data Domain Operating System MIB Quick Reference」
- 「Data Domain Operating System Offline Diagnostics Suite User's Guide」
- 「Field Replacement Guide, Data Domain DD4200, DD4500, and DD7200 Systems, IO Module and Management Module Replacement or Upgrade」など、お使いのシステム コンポーネントのフィールド交換ガイド
- 「 Data Domain、システム コントローラ アップグレード ガイド」
- 「Data Domain 拡張シェルフ ハードウェア ガイド」（シェルフ モデル ES30/FS15、DS60 用）
- 「Data Domain Boost for Partner Integration 管理ガイド」
- 「Data Domain Boost for OpenStorage 管理ガイド」
- 「Data Domain Boost for Oracle Recovery Manager 管理ガイド」
- 「Statement of Volatility for the Data Domain DD2500 System」
- 「Statement of Volatility for the Data Domain DD4200, DD4500, or DD7200 System」
- 「Statement of Volatility for the Data Domain DD6300, DD6800, or DD9300 System」
- 「Statement of Volatility for the Data Domain DD9500 or DD9800 System」

オプションの RSA Data Protection（DPM）Key Manager がある場合、RSA Key Manager 製品で使用可能な「RSA Data Protection Manager Server Administrator's Guide」の最新版を参照してください。

このマニュアルで使用される特記事項の表記規則
Data Domain では、特別な注意を要する事項に次の表記法を使用します。

通知

通知は、事業損失またはデータ消失を招く可能性のあるコンテンツを示します。

注

通知は、トピックに対して本質的ではなく偶発的な情報を示します。通知は、説明、コメント、テキストのポイントの補足、または単に関係するポイントだけを示す場合があります。

表記規則
本書では、以下の表記規則を使用します。

表 1 フォント

［太字］	ウィンドウ名、ダイアログ ボックス、ボタン、フィールド、タブ名、キー名、メニュー パスなど、インターフェイスの構成要素（ユーザーが明示的に選択またはクリックする対象）の名前を示します。
「斜体」	テキストにリストされた出版物のタイトルをハイライトします
`Monospace`	次のようなシステム情報を示します。 • システム コード • エラー メッセージやスクリプトなどのシステム出力 • パス名、ファイル名、プロンプト、構文 • コマンドおよびオプション
モノスペース斜体	変数値に置き換える必要があり変数名をハイライトします
モノスペース太字	テキストまたはユーザー入力を示します

表 1 フォント （続き）

[ ]	オプション値
|	縦棒は、他の選択を示す「or」を意味します
{ }	中括弧内は、ユーザーが指定する必要のある内容を示す（例：x、y、z）
...	省略記号は、例の中で省略した重要でない情報を示す

問い合わせ先

Data Domain のサポート情報、製品情報、ライセンス情報は、次の場所で入手できます。

製品情報

ドキュメント、リリース ノート、ソフトウェア アップデートや、Data Domain 製品の詳細については、オンライン サポート（https://support.emc.com）を参照してください。

テクニカル サポート

オンライン サポートにアクセスして、[サービス センター] をクリックします。テクニカル サポートへの問い合わせ方法がいくつか表示されます。サービス リクエストを開始するには、有効なサポート契約が必要です。有効なサポート契約を結ぶ方法の詳細や、アカウントに関する質問については、セールス担当者にお問い合わせください。

ご意見

マニュアルの精度、構成および品質を向上するため、お客様のご意見をお待ちしております。本書についてのご意見を以下のメール アドレスにお送りください。DPAD.Doc.Feedback@emc.com。

第 1 章

Data Domain システムの機能および統合

本章には、次のセクションが含まれます。

- 改訂履歴 22
- Data Domain システムの概要 22
- Data Domain システムの機能 22
- ストレージ環境の統合 28

改訂履歴

改訂履歴には、DD OS Release 6.2 に対応するために本書に加えられた大きな変更の一覧が記載されています。

表 2 ドキュメント改訂履歴

リビジョン	日付	説明
01 (6.2.0)	2018 年 12 月	このリビジョンには、次の新機能に関する情報が含まれています。 • DD SM 構成ウィザードの一部としてのメール サーバー資格情報の構成。 • DD300 の 8 TB から 16 TB への容量拡張。 • Secure LDAP 認証。 • Active Directory 接続診断ツール。 • コアダンプ ファイルを USB ドライブに保存。 • SMB Change Notify。 • トラステッド ドメインのオフライン アクセス。 • Alibaba と Google Cloud Platform クラウド プロバイダのための DD Cloud Tier のサポート。

Data Domain システムの概要

Data Domain システムは、エンタープライズ環境にデータ保護と DR（ディザスタリカバリ）を提供するディスク ベースの重複排除アプライアンスです。

すべてのシステムで DD OS（Data Domain オペレーティング システム）が実行されます。DD OS は、システム操作を実行する CLI（コマンド ライン インターフェイス）と、構成、管理、モニタリングを行う DD System Manager（Data Domain System Manager）GUI（グラフィカル ユーザー インターフェイス）の両方を備えています。

注

DD System Manager は、以前は Enterprise Manager と呼ばれていました。

システムは、ストレージ容量とデータ スループットが異なるアプライアンスで構成されています。システムは通常、ストレージ領域を追加する拡張エンクロージャで構成されています。

Data Domain システムの機能

Data Domain システムの機能を使用すると、データの整合性、信頼性の高いリストア、リソースの効率的な使用、管理のしやすさを実現できます。ライセンス機能では、それぞれのニーズと予算に合わせて、システム機能セットを拡張できます。

データの整合性

DD OS Data Invulnerability Architecture™は、ハードウェアやソフトウェアの障害によるデータ消失からデータを保護します。

- ディスクへの書き込み時、DD OS は、受信したすべてのデータに対し、チェックサムと自己記述メタデータを作成および保存します。データをディスクに書き込んだ後、DD OS はチェックサムとメタデータを再計算および確認します。
- 追加専用書き込みポリシーは、有効なデータの上書きからデータを保護します。
- バックアップ完了後、確認プロセスがディスクに書き込まれたデータを検証し、すべてのファイル セグメントがファイル システム内で論理的に正しいことおよびディスクへの書き込み前後でデータに変化がないことを確認します。
- バックグラウンドでは、オンライン検証操作は継続的に、そのディスク上のデータがただしく、前の検証処理から変更されていないことをチェックします。
- ほとんどの Data Domain システム内のストレージは、二重パリティ RAID 6 構成（2 パリティ ドライブ）でセットアップされます。また、8 台のディスクを使用する DD1xx シリーズ システムを除き、ほとんどの構成には、各エンクロージャに 1 つのホット スペアがあります。各パリティ ストライプでは、ブロック チェックサムを使用して、データが正しいことが確認されます。オンライン検証操作中および Data Domain システムからのデータ読み取り中は、チェックサムが継続的に使用されます。二重パリティがある場合、システムは、ディスク 2 つまでであれば、同時に発生したエラーを修正できます。
- ハードウェアまたは電源障害時にデータが同期されるようにするには、Data Domain システムが NVRAM（非揮発性 RAM）を使用して、未処理の I/O 操作を追跡します。バッテリが完全に充電された NVRAM カード（通常の状態）は、使用中のハードウェアによって決まる数時間の期間中、データを保持します。
- リストア作業でデータを読み取る際、DD OS は複数のレイヤーの整合性チェックを使用して、リストアされたデータが正しいことを確認します。
- SSD キャッシュに書き込むときに、DD OS は以下の操作を行います。
  - キャッシュに格納されるすべてのレコードに対する SL チェックサムを作成して、キャッシュ データの破損を検出します。このチェックサムは、すべてのキャッシュ読み取りで検証されます。
  - キャッシュ データの破損はキャッシュ ミスとして扱われ、データ消失は発生しません。そのためキャッシュ クライアントは、NVRAM や HDD などの他のバックアップ メカニズムなしでデータの最新のコピーを格納することはできません。
  - キャッシュ書き込みのインライン検証の必要性を排除します。これは、キャッシュ クライアントが誤った書き込みまたは消失した書き込みを検出して処理できるからです。これにより、I/O 帯域幅が節約されます。
  - ファイル システムの SSD データ抽出の必要性を排除します。これは、キャッシュ内のデータが頻繁に変更され、SAS BMS（バックグラウンド メディア スキャン）によってすでにデータ抽出されているからです。

データ重複排除

DD OS のデータの重複排除では、バックアップのたびに冗長データが特定され、固有データが一度だけ格納されます。

固有データの保存は、バックアップ ソフトウェアには認識されず、データ形式には依存しません。データは、データベースなどのように構造化されている場合と、テキスト ファイルなどのように構造化されていない場合があります。データは、ファイル システムまたは raw ボリュームから取得できます。

数週間の重複排除率は、通常は平均で 20 対 1 です。この比率から、週次フル バックアップと日次増分バックアップが行われていることが想定されます。最も重複排除の恩恵を受けるのは、重複

ファイルまたは類似ファイル（わずかな変更で何度かコピーされたファイル）を多く含むバックアップです。

バックアップのボリューム、サイズ、保存期間、変更率によって、重複排除の量は異なります。重複排除は、10 MiB（MiB は MB の 2 進数相当です）のバックアップ ボリューム サイズで行うのがベストです。

複数の Data Domain システムを最大限に活用するには、複数の Data Domain システムがあるサイトでは、同じクライアント システムまたはデータのセットを常に同じ Data Domain システムにバックアップする必要があります。たとえば、すべての販売データのフル バックアップを Data Domain システム A に保存する場合、販売データの増分バックアップと将来のフル バックアップも Data Domain システム A に保存すれば最大限の重複排除を実現できます。

リストア処理

ファイル リストア処理では、バックアップまたは他のリストア処理との競合はほとんど生じないか、まったく生じません。

Data Domain システムのディスクにバックアップすることで、増分バックアップを常に信頼でき、容易にアクセスすることができます。テープ バックアップの場合、リストア作業は増分バックアップを保持する複数のテープに依存する可能性があります。また、サイトで複数のテープに保存する増分バックアップが多いほど、リストア処理の所要時間とリスクが増えます。問題のあるテープが 1 つでもあると、リストアが中止されるおそれがあります。

Data Domain システムを使用すると、冗長データの保存ペナルティがない状態で、より頻繁にフル バックアップを実行できます。テープ・ドライブのバックアップとは異なり、複数のプロセスが同時に Data Domain システムにアクセスできます。Data Domain システムでは、サイトは安全かつユーザー主導の単一ファイル リストア作業を提供できます。

Data Domain Replicator

Data Domain Replicator は、2 つの Data Domain システム間のバックアップ データのレプリケーションを設定し、管理します。

DD Replicator のペアは、ソース システムとデスティネーション システムで構成され、ソース システムからデスティネーション システムに完全なデータセット、ディレクトリ、MTree がレプリケーションされます。個々の Data Domain システムが複数のレプリケーション ペアの一部になり、1 つ以上のペアのソースまたはデスティネーションとして機能します。レプリケーションが開始されると、ソース システムからデスティネーション システムに新しいバックアップ データが自動的に送信されます。

マルチパスとロード バランシング

ファイバー チャネルのマルチパス構成では、Data Domain システムとバックアップ サーバーまたはバックアップ デスティネーション アレイの間に 2 つ以上のパスが確立されます。複数のパスが存在する場合、システムによって自動的に、利用可能なパスの間でバックアップの負荷が分散されます。

マルチパス構成を作成するには、少なくとも 2 個の HBA ポートが必要です。バックアップ サーバーに接続している場合、マルチパス上の各 HBA ポートは、バックアップ サーバーの異なるポートに接続されます。

高可用性

HA（高可用性）機能を使用すれば、2 つの Data Domain システムをアクティブ/スタンバイのペアとして構成して、システム障害が発生した場合に冗長性を提供することができます。HA では、アクティブ システムとスタンバイ システムの同期を保つため、ハードウェアまたはソフトウェアの問題によりアクティブ ノードに障害が発生しても、スタンバイ ノードがサービスを引き継いで、障害が発生したノードが中断したところから続行することができます。

HA には次のような機能があります。

- 2 ノード システムで、バックアップ、リストア、レプリケーション、管理各サービスのフェイルオーバーをサポートします。自動フェイルオーバーには、ユーザー介入は不要です。
- システムが推奨に従って構成されている場合、そのシステム内では、単一障害点のない完全に冗長化された設計となります。
- フェイルオーバー時にパフォーマンスの損失がないアクティブ/スタンバイ システムを実現します。
- ほとんどの操作について、10 分以内にフェイルオーバーが可能です。CIFS、DD VTL、NDMP は、手動で再起動する必要があります。

  注

  DD Boost アプリケーションのリカバリには 10 分を超える時間がかかる場合があります。DD サーバーのフェイルオーバーが完了するまで Boost アプリケーションのリカバリを開始できないためです。さらに、Boost アプリケーションのリカバリは、アプリケーションが Boost ライブラリを呼び出すまで開始できません。同様に、NFS でもリカバリに余分な時間が必要になる場合があります。

- DD OS CLI によって、管理と構成が簡単になります。
- ハードウェアに障害が発生した場合にアラートを生成します。
- 通常モードと縮退モードの両方で、シングル ノードのパフォーマンスと拡張性を HA 構成内に保存します。
- スタンドアロンの DD システムと同じ機能セットをサポートしています。

  注

  DD Extended Retention と vDisk はサポートしていません。

- すべての SAS ドライブを備えたシステムをサポートしています。これには、すべての SAS ドライブを備えたシステムにアップグレードされたレガシー システムも含まれます。

  注

  Data Domain システムのハードウェアの概要と設置ガイドでは、新しい HA システムを設置する方法について説明します。「Data Domain シングル ノートから HA へのアップグレード」では、既存のシステムを HA ペアにアップグレードする方法について説明します。

- 製品の拡張機能には影響しません。
- 無停止でのソフトウェア アップデートをサポートしています。

HA は次の Data Domain システムでサポートされています。

- DD6800
- DD9300
- DD9500
- DD9800

HA アーキテクチャ

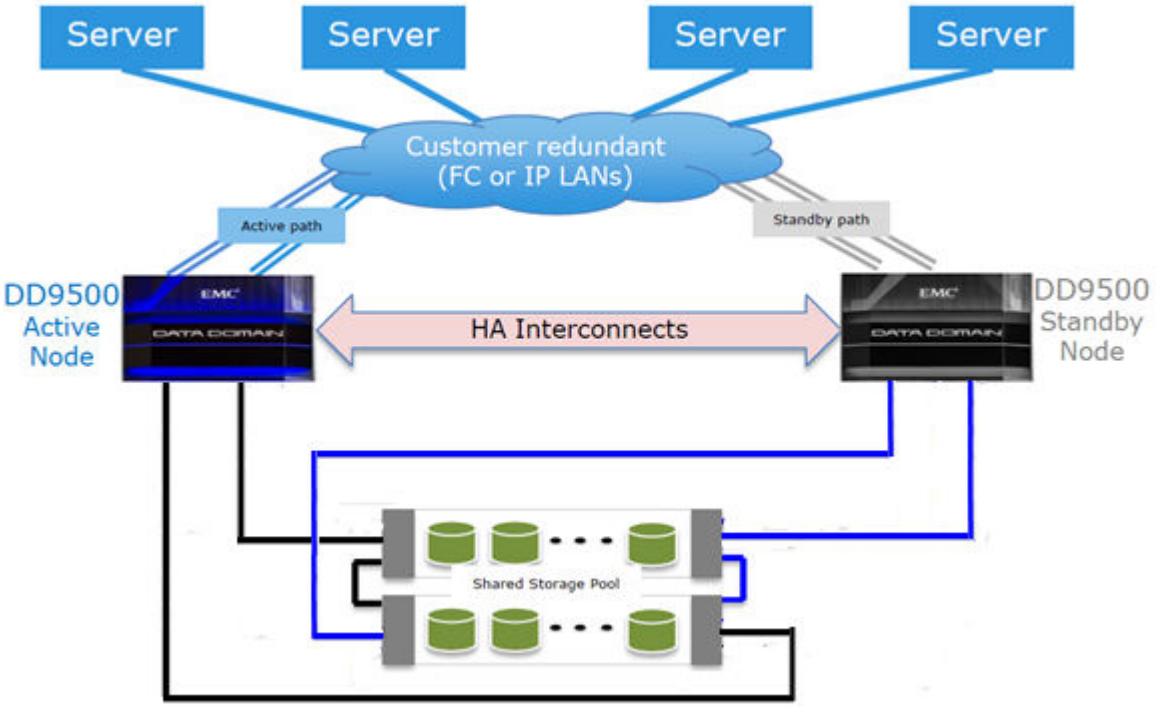
HA 機能は、IP 接続でも FC 接続でも利用できます。どちらのノードでも、環境の高可用性を実現するためには同じ IP ネットワーク、FC SAN、ホストにアクセスする必要があります。

IP ネットワークを介した HA は、どちらの物理ノードがアクティブ ノードであるかに関係なく、フローティング IP アドレスを使用して、Data Domain HA ペアへのデータ アクセスを提供します。

FC SAN の場合、HA は、NPIV を使用してノード間で FC WWN を移動し、FC イニシエーターがフェイルオーバー後に接続を再確立できるようにします。

図 1（26 ページ）に HA アーキテクチャを示します。

図 1 HA アーキテクチャ



ランダム I/O 処理

DD OS に含まれるランダム I/O 最適化は、シーケンシャルな読み取り/書き込み操作より大量のランダム読み取り/書き込み操作を生成するアプリケーションとユースケースのパフォーマンスを向上させます。

DD OS は、仮想マシンのインスタント アクセスやインスタント リストア、Avamar などのアプリケーションによって生成される永久増分バックアップなどのランダム読み取り/書き込み操作で構成されるワークロードを処理するように最適化されています。これらの最適化により、次のメリットが得られます。

- ランダム読み取り/書き込みのレイテンシが向上します。
- 読み取りサイズの削減によりユーザー IOPS が向上します。
- 単一ストリーム内でコンカレント I/O 操作をサポートします。
- より小さいストリームでピーク読み取り/書き込みスループットを実現します。

注

最大ランダム I/O ストリーム カウントは、Data Domain システムの最大リストア ストリーム カウントに制限されます。

ランダム I/O 処理の強化により、Data Domain システムは Avamar や Networker などのバックアップ アプリケーションのインスタント アクセス/インスタント リストア機能をサポートすることができます。

システム管理者のアクセス

システム管理者は、コマンド ライン インターフェイスまたはグラフィカル ユーザー インターフェイスを使用して、構成および管理のためにシステムにアクセスできます。

- DD OS CLI：コマンド ライン インターフェイスは、シリアル コンソールまたは SSH か Telnet を使用した Ethernet 接続を介して使用可能です。CLI コマンドでは、初期システムの構成、個別のシステム設定の変更、システム動作ステータスの表示を行うことができます。
- DD System Manager：Ethernet 接続を通して使用可能なブラウザー ベース グラフィカル ユーザー インターフェイス。DD System Manager を使用すると、初期システム構成を実行したり、初期構成の後の変更を行うとともに、システムとコンポーネントのステータスを示したり、レポートと表を生成することができます。

注

システムの一部は、システムに直接取り付けられたキーボードとモニターを使用したアクセスに対応しています。

ライセンス機能

機能のライセンス化により、使用する予定の機能のみ購入することができます。ライセンスが必要な機能の例としては、DD Extended Retention、DD Boost、ストレージ容量の増加などがあります。

ライセンス機能の購入に関する情報については、担当者にお問い合わせください。

表 3 ライセンスが必要な機能

機能名	ソフトウェア内のライセンス名	説明
Data Domain ArchiveStore	ARCHIVESTORE	ファイルとメールのアーカイブ、ファイルの階層化、コンテンツとデータベースのアーカイブなど、アーカイブを使用するための Data Domain システムにライセンスを適用します。
Data Domain Boost	DDBOOST	次のアプリケーションがある Data Domain システムを使用できるようにします。そのアプリケーションは、Avamar、NetWorker、Oracle RMAN、Quest vRanger、Symantec Veritas NetBackup（NBU）、Backup Exec です。DD Boost の管理対象ファイル レプリケーション機能には、DD Replicator のライセンスも必要です。
Data Domain Capacity on Demand	CONTROLLER-COD	4 TB DD2200 システムの容量を 7.5 TB または 13.18 TB までオン デマンドで増やすことができます。13.18 TB まで増やす場合は、EXPANDED-STORAGE ライセンスも必要になります。
Data Domain Cloud Tier	CLOUDTIER-CAPACITY	Data Domain システムを有効化して、アクティブ階層から、低コストで容量の大きいオブジェクト ストレージにデータを移動します。このストレージは、長期間の保存に備えたパブリック、プライベート、またはハイブリット クラウドに置かれます。
Data Domain Encryption	ENCRYPTION	システム ドライブまたは外部ストレージ上のデータを保存中に暗号化し、システムを別の場所に移動する場合ロックできるようにします。
Data Domain Expansion Storage	EXPANDED-STORAGE	Data Domain のシステム ストレージをベース システムで提供されているレベルを超えて拡張できます。

表 3 ライセンスが必要な機能 （続き）

機能名	ソフトウェア内のライセンス名	説明
Data Domain Extended Retention（旧 DD Archiver）	EXTENDED-RETENTION	DD Extended Retention ストレージ機能にライセンスを適用します。
Data Domain I/OS（IBM i オペレーティング環境）	I/OS	IBM i オペレーティング環境でシステムのバックアップに DD VTL が使用される場合、I/OS ライセンスが必要です。仮想テープ ドライブをライブラリに追加する前に、このライセンスを適用します。
Data Domain Replicator	REPLICATION	Data Domain システム間でのデータ レプリケーションのため、DD Replicator を追加します 各システムでライセンスが必要です。
Data Domain Retention Lock Compliance Edition	RETENTION-LOCK-COMPLIANCE	SEC17a-4 などの規制基準の厳格なデータ保存要件を満たします。
Data Domain Retention Lock Governance Edition	RETENTION-LOCK-GOVERNANCE	指定した保存期間の終了前に、選択したファイルが変更および削除されないようにします。
Data Domain Shelf Capacity-Active Tier	CAPACITY-ACTIVE	Data Domain システムのアクティブ階層ストレージの容量を追加エンクロージャまたはエンクロージャ内のディスク パックまで拡張可能にします。
Data Domain Shelf Capacity-Archive Tier	CAPACITY-ARCHIVE	Data Domain システムのアーカイブ階層ストレージの容量を追加エンクロージャまたはエンクロージャ内のディスク パックまで拡張可能にします。
Data Domain Storage Migration	STORAGE-MIGRATION-FOR-DATADOMAIN-SYSTEMS	古くて容量の少ないエンクロージャの交換をサポートするため、あるエンクロージャから別のエンクロージャへのデータ移行を可能にします。
DD VTL（Data Domain Virtual Tape Library）	VTL	Fibre Channel ネットワーク経由で仮想テープ ライブラリとして Data Domain システムを使用できるようにします。このライセンスにより、以前は個別のライセンスが必要だった NDMP Tape Server 機能も有効になります。
高可用性	HA-ACTIVE-PASSIVE	アクティブ/スタンバイ構成で高可用性機能を有効化します。購入する必要がある HA ライセンスは 1 つだけです。ライセンスはアクティブ ノードで実行され、スタンバイ ノードにミラーリングされます。

ストレージ環境の統合

Data Domain システムは、既存のデータセンターに簡単に統合できます。

- すべての Data Domain システムは、NFS、CIFS、DD Boost、または DD VTL プロトコルを使用した最先端のバックアップおよびアーカイブ アプリケーション用のストレージ デスティネーションとして構成できます。

- さまざまな構成を扱うアプリケーションの詳細については、https://support.emc.com で［互換性に関するドキュメント］を検索します。
- 複数のバックアップ サーバーで、1 つの Data Domain システムを共有できます。
- 1 つの Data Domain システムは、複数の同時バックアップとリストア作業を処理できます。
- 複数の Data Domain システムを 1 つ以上のバックアップ サーバーに接続できます。

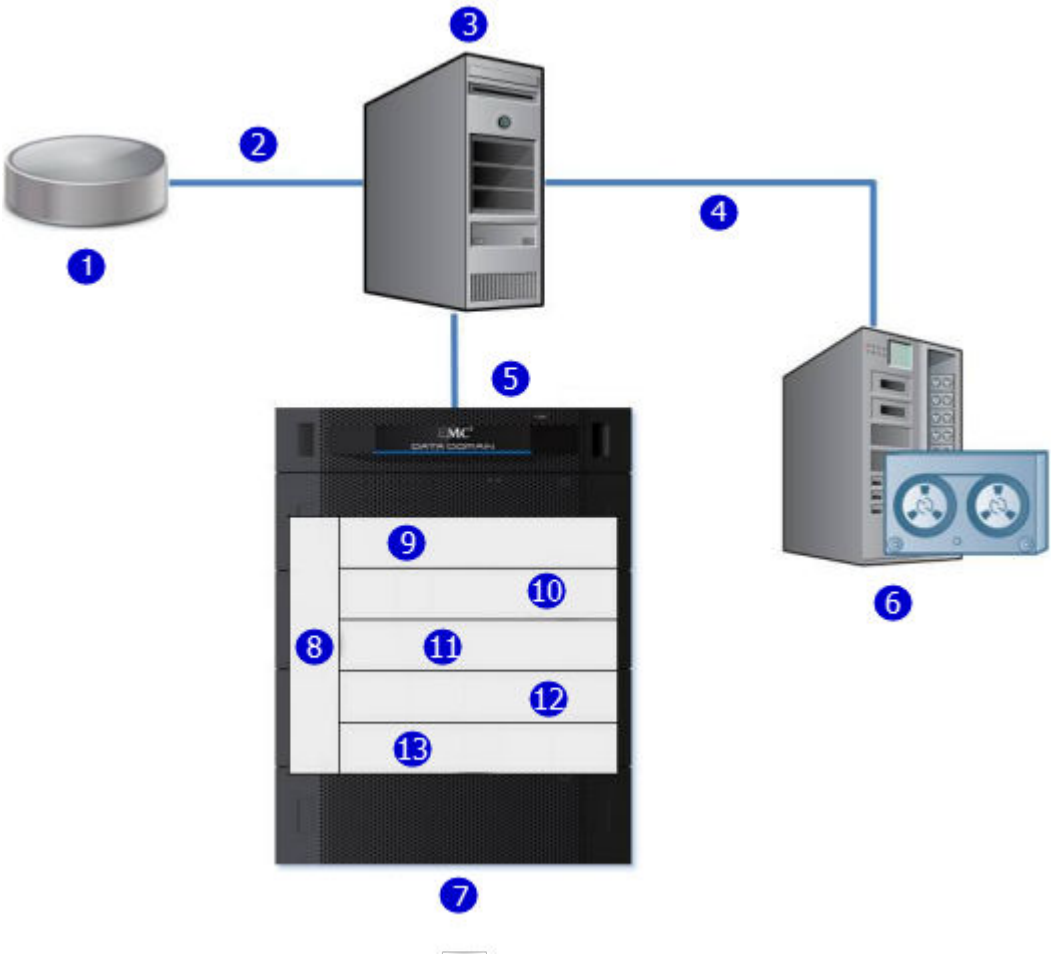
バックアップ デスティネーションとして使用するため、Data Domain システムは、Ethernet 接続でアクセスするファイル システムを含むディスク ストレージ ユニット、またはファイバーチャネル接続でアクセスする仮想テープ ライブラリとして構成できます。DD VTL 機能は、システム停止を最小限に抑えつつ、バックアップ ソフトウェアがすでにテープ バックアップ用に構成されている環境に Data Domain システムを統合できるようにします。

構成は、DD OS（本ガイドの関連セクションで説明しています）およびバックアップ アプリケーション（バックアップ アプリケーションの管理者ガイドと Data Domain アプリケーション関連ガイド/技術ノートで説明しています）の両方で実行されます。

バックアップ アプリケーションはすべて、Data Domain ディスク デバイス上の NFS または CIFS ファイル システムとして Data Domain システムにアクセスできます。

下図は、既存の基本バックアップ構成に統合された Data Domain システムを示しています。

図 2 ストレージ環境に統合された Data Domain システム



1. プライマリ ストレージ
2. Ethernet

図 2 ストレージ環境に統合された Data Domain システム （続き）

3. バックアップ サーバ
4. SCSI/Fibre Channel
5. ギガビット Ethernet または Fibre Channel
6. テープ システム
7. Data Domain システム
8. 管理
9. NFS/CIFS/DD VTL/DD Boost
10 データの検証
11. File system
12. グローバルな重複排除と圧縮
13. RAID

図 2（29 ページ）に示すとおり、データは Ethernet 接続またはファイバー チャネル接続を経由して Data Domain システムに流れます。すぐに、データ確認プロセスが始まり、それは Data Domain システム上にデータがある間は継続されます。ファイル システムでは、DD OS Global Compression™ アルゴリズムはストレージ用のデータを重複解除および圧縮します。その後、データはディスク RAID サブシステムに送信されます。リストア作業が必要な場合、データが Data Domain ストレージから取得され、解凍され、整合性が確認されて、Ethernet（NFS、CIFS、DD Boost の場合）またはファイバー チャネル（DD VTL と DD Boost の場合）を使用した Ethernet 経由でバックアップ サーバに転送されます。

DD OS は、バックアップ ソフトウェアから比較的大きいシーケンシャル データのストリームを収容し、高いスループット、継続的なデータ確認、高い圧縮率を実現するために最適化されます。それは、ニアライン ストレージ（DD ArchiveStore）に多くのより小さいファイルを収容します。

Data Domain システムが最高のパフォーマンスを発揮できるのは、次のように、特にバックアップ ソフトウェアではないアプリケーションからデータを格納するときです。

- データがシーケンシャル ライトとして Data Domain システムに送信される（上書きされない）場合。
- データは、Data Domain システムに送信される前に圧縮または暗号化されません。

第 2 章

はじめに

本章には、次のセクションが含まれます。

- Dell EMC Data Domain System Manager の概要 32
- DD System Manager へのログインとログアウト 32
- DD System Manager インターフェイス 36
- 構成ウィザードを使用したシステムの構成 38
- Data Domain のコマンド ライン インターフェイス 51
- CLI へのログイン 52
- CLI のオンライン ヘルプのガイドライン 52

Dell EMC Data Domain System Manager の概要

DD System Manager は、任意の場所にある単一システムを管理するために、Ethernet 接続を介して使用できるブラウザ ベースのユーザー インターフェイスです。DD System Manager は、数多くのシステム機能とシステム設定の構成と監視を実行できる、単一の統合管理インターフェイスを提供します。

注

Data Domain Management Center では、1 つのブラウザ ウィンドウから複数のシステムを管理することができます。

DD System Manager ではグラフやテーブルがリアルタイムで提供され、システム ハードウェア コンポーネントや構成された機能のステータスを監視することができます。

さらに、ユーザーはすべてのシステム機能を実行するコマンド セットを、CLI（コマンド ライン インターフェイス）から使用できます。コマンドを実行すると、システム設定の構成や、システム ハードウェア ステータス、機能構成、操作の表示を行うことができます。

コマンド ライン インターフェイスは、シリアル コンソールまたは SSH か Telnet を使用した Ethernet 接続を通して使用可能です。

注

システムの一部は、システムに直接取り付けられたキーボードとモニターを使用したアクセスに対応しています。

DD OS ソフトウェア バージョン

DD OS ソフトウェア リリースには、バージョンを実行しているインストール済みシステムの数を示す 3 つのパブリック ステータスがあります。

- ［一般販売］リリースは、Data Domain の内部 QA テストを完了し、本番環境でのインストールに使用できます。
- ［**Directed Availability - Controlled**（**Directed Availability**）］リリースは、少数のインストール向けの慎重にコントロールされるアクセス リリースです。お客様は、これらのリリースへのアクセス資格をリクエストできます。
- ［ターゲット コード］ - すべてのシステムは、できるだけ早く、リリース ファミリー内の Data Domain OS ターゲット コードにアップグレードすることをお勧めします。

  注

  所定のファミリーには、ターゲット コード リリースが 1 つしかありません。ターゲット コード リリースは、インストールおよび実行時の時間と品質のメトリックを満たしており、安定していて、大部分のお客様に影響を与えるような問題がないことを示しています。一部のファミリーでは、お客様の取り込みが限定的、品質の問題、またはその他の考慮事項が原因で、ターゲット コードが特定されない場合があります。

ファミリー間のアップグレードには製品の互換性に関する考慮事項があり、新しいリリース ファミリーへのアップグレードに先立って製品の互換性を注意深く確認する必要があります。

DD System Manager へのログインとログアウト

ブラウザを使用して、DD System Manager にログインします。

Web ブラウザから DD System Manager に接続すると、すべての HTTP 接続が自動的に HTTPS にリダイレクトされます。

手順

1. Web ブラウザを開いて、IP アドレスまたはホスト名を入力し、DD System Manager に接続します。これは次のいずれかである必要があります。
   - 完全修飾ドメイン名（例：`http://dd01.emc.com`）
   - ホスト名（`http://dd01`）
   - IP アドレス（`http://10.5.50.5`）

   注

   DD System Manager では、HTTP ポート 80 と HTTPS ポート 443 を使用します。Data Domain システムでファイアウォールが使われている場合、システムにアクセスするために、HTTP を使用している場合はポート 80 を、HTTPS を使用している場合はポート 443 を有効にしなければならない場合があります。セキュリティ要件で規定されている場合、ポート番号は簡単に変更できます。

注

Data Domain System Manager がどの Web ブラウザからも起動できない場合、表示されるエラー メッセージは「The GUI Service is temporarily unavailable. Please refresh your browser. If the problem persists, please contact Data Domain support for assistance.」です。SSH は、Data Domain システムにログインするために使用することができ、すべてのコマンドを実行することができます。
DD OS をアップグレードしていないにもかかわらず、この GUI エラーが発生する場合は、以下の手順を使用します。

a. 報告されたエラーがある Data Domain システム上の Web ブラウザ セッションを閉じます。
b. 次のコマンドを順番に実行します。
   - `adminaccess disable http`
   - `adminaccess disable https`
   - `adminaccess enable http`
   - `adminaccess enable https`
c. http および https サービスが完全に開始されるように、5 分間待ちます。
d. Web ブラウザを開き、Data Domain System Manager に接続します。

DD OS のアップグレード後にこの GUI の問題が発生した場合は、以下の手順を実行します。

a. レポートされたエラーがある Data Domain システム上の Web ブラウザ セッションを閉じます。
b. 次のコマンドを順番に実行します。
   - `adminaccess disable http`
   - `adminaccess disable https`
   - `adminaccess certificate generate self-signed-cert`
   - `adminaccess enable http`
   - `adminaccess enable https`
a. http および https サービスが完全に開始されるように、5 分間待ちます。
b. Web ブラウザを開き、Data Domain System Manager に接続します。

2. HTTPS セキュア ログインを行うには、［**Secure Login**］をクリックします。

   HTTPS を使用したセキュア ログインには、DD OS システムの ID を確認し、DD System Manager とブラウザ間の双方向的暗号化に対応するためのデジタル証明書が必要です。DD OS には自己署名証明書が含まれ、自分の証明書をインポートすることができます。
3. 割り当てられたユーザー名とパスワードを入力します。

注

初期のユーザー名は［sysadmin］、初期のパスワードはシステムのシリアル番号です。新しいシステムのセットアップの詳細については、「Data Domain Operating System 初期構成ガイド」を参照してください。

4. ［ログイン］をクリックします。

   これが初回ログインの場合、情報パネルに［Home］ビューが表示されます。

   注

   誤ったパスワードを 4 回連続で入力すると、指定したユーザー名はシステムによって 120 秒間ロックアウトされます。ログイン回数およびロックアウト期間は構成可能であり、お使いのシステムでは異なっていることがあります。

   注

   これが初回ログインであれば、パスワードの変更が必要になる場合があります。システム管理者がユーザー名の構成によってパスワード変更を必要とした場合、DD System Manager にアクセスする前に、パスワードを変更する必要があります。

5. ログアウトするには、［DD System Manager］バナーの［Log Out］ボタンをクリックします。

   ログアウトすると、ログアウトが完了したことを示すメッセージを表示したログイン ページが表示されます。

証明書を使用したログイン

ログイン ユーザー名とパスワードを使用する代わりに、CA（証明機関）の発行した証明書を使用して DD System Manager にログインできます。

証明書を使用してログインするには、Data Domain システムの承認権限が必要であり、かつ Data Domain システムが CA の証明書を信頼する必要があります。ユーザー名が、証明書の共通名フィールドに指定されている必要があります。

手順

1. Data Domain システム上のユーザー アカウントがあることを確認します。

   ローカル ユーザーとネーム サービス ユーザー（NIS/AD）のどちらでも構いません。ネーム サービス ユーザーの場合は、グループのロール マッピングを Data Domain システムで構成する必要があります。

2. 次の CLI コマンドを使用して、証明書を発行した CA の公開キーをインポートします。
   `adminaccess certificate import ca application login-auth`。

3. お使いのブラウザで PKCS12 形式の証明書をロードします。

   Data Domain システムが CA 証明書を信頼さると、［**Log in with certificate**］リンクが HTTPS のログイン画面に表示されます。

4. ［**Log in with certificate**］をクリックして、ブラウザが表示する証明書の一覧から証明書を選択します。

結果

Data Domain システムはトラスト ストアに対してユーザー証明書の確認を行います。アカウントに関連付けられた承認権限に基づいて、System Manager セッションが作成されます。

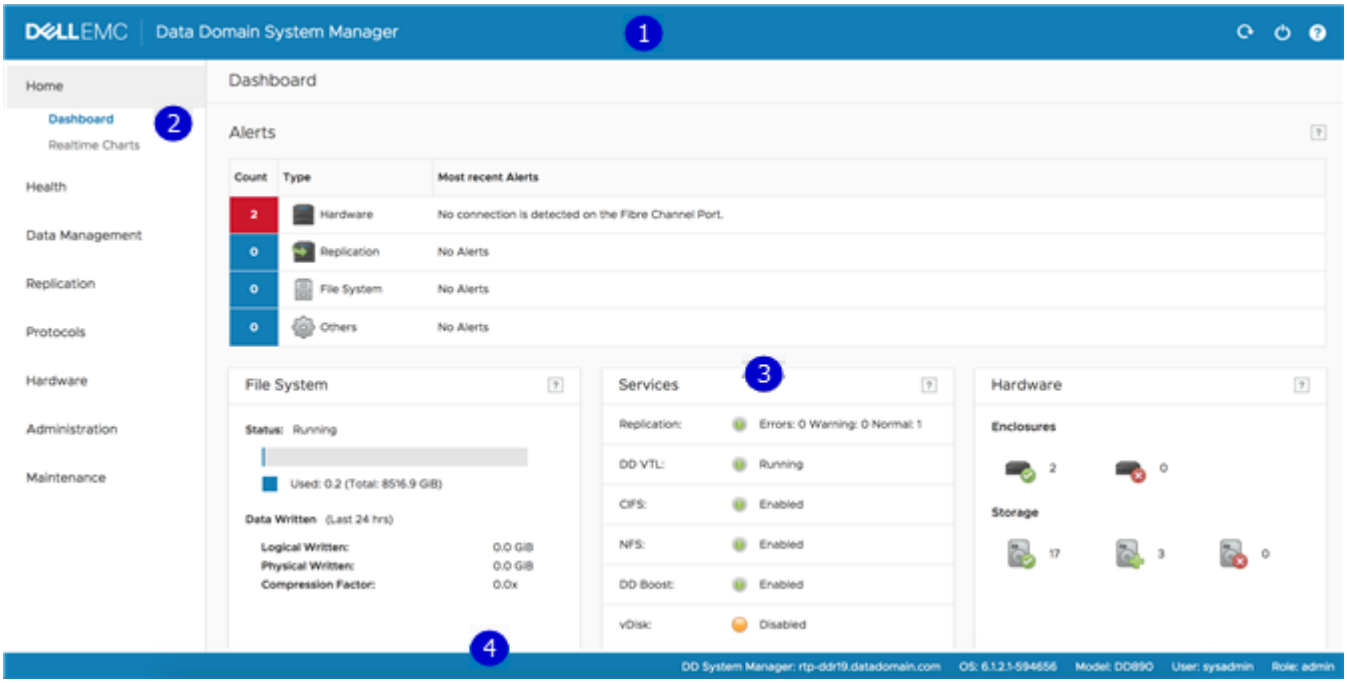
DD System Manager インターフェイス

DD System Manager インターフェイスはほとんどのページで共通する要素を提供します。これによって、構成と表示のオプション全体をナビゲートし、コンテキスト ヘルプを表示できるようになります。

ページ要素

主なページ要素は、バナー、ナビゲーション パネル、情報パネル、フッターです。

図 3 ［DD System Manager］ページのコンポーネント



1. バナー
2. ナビゲーション パネル
3. 情報パネル
4. フッター

バナー

DD System Manager のバナーには、プログラム名と、［**Refresh**］、［**Log Out**］、［**Help**］の各ボタンが表示されます。

ナビゲーション パネル

［Navigation］パネルには、最高レベルのメニューが表示され、選択できます。これを使用して、管理するシステム コンポーネントやタスクを指定できます。

［Navigation］パネルには、ナビゲーション システムの上位 2 レベルが表示されます。トップ レベルのタイトルいずれかをクリックすると、2 番目のレベルのタイトルが表示されます。［Information］パネル内のタブとメニューには、追加のナビゲーション コントロールが表示されます。

情報パネル

［Information］パネルには、［Navigation］パネルで選択した項目関連の情報とコントロールが表示されます。情報パネルでは、システム ステータス情報を確認し、システムを構成することができます。

［Navigation］パネルで選択した機能またはタスクに応じて、［Information］パネルにはタブ バー、トピック領域、テーブル ビューのコントロール、［More Tasks］メニューが表示されます。

Tab バー
タブでは、［Navigation］パネルで選択されたトピックの異なる面にアクセスできます。

トピック領域
トピック領域は［Information］パネルを、［Navigation］パネルまたは親タブで選択されたトピックの異なる面を表すセクションに分割されます。

HA（高可用性）システムの場合、System Manager ダッシュ ボードの［HA Readiness］タブは、HA システムがアクティブ ノードからスタンバイ ノードにフェールオーバーできる状態になっているかどうかを示します。［**HS Readiness**］をクリックすると、［**HEALTH**］の［**High Availability**］セクションに移動します。

テーブル ビュー オプションの扱い
項目のテーブルがあるビューの多くには、テーブル内の情報のフィルタリング、ナビゲーション、ソートのコントロールが含まれます。

共通テーブル コントトールを使用する方法：

- 列見出しのひし形のアイコンをクリックして、列内の項目のソート順を逆にします。
- ビュー右下の［**<**］および［**>**］矢印をクリックして、ページを進むまたは戻ります。先頭のページに戻るには、［**|<**］をクリックします。最後のページを追加するには、［**>|**］をクリックします。
- テーブルのすべての項目を表示するには、スクロール バーを使用します。
- ［**Filter By**］ボックスにテキストを入力して、それらの項目のリストを検索および優先化します。
- リストを更新するには［**Update**］をクリックします。
- ［**Reset**］をクリックして、デフォルト リストに戻ります。

［More Tasks］メニュー
一部のページでは、ビューの右上に、現在のビューに関係するコマンドが含まれている［More Tasks］メニューがあります。

フッター

DD System Manager のフッターには、管理セッションに関する重要な情報が表示されます。

バナーには、次の情報が一覧表示されます。

- システムのホスト名。
- DD OS バージョン
- 選択されたシステム モデル番号。
- 現在ログインしているユーザーのユーザー名と役割。

［Help］ボタン

［Help］ボタンは?として表示され、バナー、情報パネルの多くの領域のタイトル、多数のダイアログに表示されます。［Help］ボタンをクリックして、現在使用している機能に関するヘルプ ウィンドウを表示します。

ヘルプ ウィンドウには、ヘルプの上にコンテンツ ボタンとナビゲーション ボタンが表示されます。コンテンツ ボタンをクリックして、ガイド コンテンツとヘルプの検索に使用できる検索ボタンを表示します。方向矢印ボタンを使用して、シーケンシャルな順序でヘルプ トピックのページを切り替えます。

使用許諾契約書

EULA（使用許諾契約書）を表示するには、［**Maintenance**］ > ［**System**］ > ［**View EULA**］を選択します。

構成ウィザードを使用したシステムの構成

DD System Manager 構成ウィザードと CLI（コマンド ライン インターフェイス）構成ウィザードという 2 つのウィザードがあります。構成ウィザードに従うと、システム構成を簡素化でき、システムを迅速に運用状態にすることができます。

ウィザードを使用して基本構成を完了した後、DD System Manager と CLI で追加構成コントロールを使用して、さらにシステムを構成できます。

注

次の手順では、システムの初期構成後に DD System Manager 構成ウィザードを開始および実行する方法について説明します。システム起動時の構成ウィザードの実行手順については「Data Domain オペレーティング システム初期構成ガイド」を参照してください。

注

HA（高可用性）のシステムを構成する場合は、CLI 構成ウィザードを使用してこの操作を実行する必要があります。詳細は、「Data Domain DD9500/DD9800 ハードウェアの概要および設置ガイド」と「Data Domain オペレーティング システム初期構成ガイド」を参照してください。

手順

1. ［**Maintenance**］ > ［**System**］ > ［**Configure System**］を選択します。
2. ［Configuration Wizard］ダイアログの下部のコントロールを使用して、構成したい機能を選択し、ウィザードを進めます。機能のヘルプを表示するには、ダイアログの左下の角にあるヘルプ アイコン（疑問符）をクリックします。

［License］ページ

［License］ページには、インストールされているすべてのライセンスが表示されます。ライセンスを追加、変更、削除する場合は［**Yes**］、ライセンスのインストールをスキップするには［**No**］をクリックします。

License Configuration

［**Licenses Configuration**］セクションでは、ライセンス ファイルからライセンスを追加、変更、削除できます。Data Domain Operating System 6.0 以降では、複数の機能を単一のライセンス ファイル アップロードに組み込むことができる ELMS ライセンスをサポートしています。

ライセンスがまったく構成されていないシステム上で構成ウィザードを使用するときは、ドロップダウン リストからライセンスのタイプを選択し［**...**］ボタンをクリックします。ライセンス ファイルが存在するディレクトリを参照し、ファイルを選択してシステムにアップロードします。

表 4 ［License Configuration］ページの値

項目	説明
ライセンスの追加	ライセンス ファイルからライセンスを追加するには、このオプションを選択します。
Replace Licenses	ライセンスがすでに構成されている場合、［**Add Licenses**］選択項目は［**Replace Licenses**］に変わります。すでに追加されているライセンスを置き換えるには、このオプションを選択します。
Delete Licenses	システム上にすでに構成されているライセンスを削除するには、このオプションを選択します。

Network

［**Network**］セクションでは、ネットワーク設定を構成することができます。ネットワーク設定を構成するには［**Yes**］を、ネットワーク構成をスキップするには［**No**］をクリックします。

［Network General］ページ

［General］ページで、IP ネットワークにシステムが参加する方法を定義するネットワーク設定を構成できます。

構成ウィザード以外でそれらのネットワーク設定を構成するには、［**Hardware**］ > ［**Ethernet**］を選択します。

表 5 ［General］ページの設定

項目	説明
Obtain Settings using DHCP	システムが DHCP（Dynamic Host Control Protocol）サーバーからネットワーク設定を収集するように指定するには、このオプションを選択します。ネットワーク インターフェイスを構成する場合、1 つ以上のインターフェイスが DHCP を使用するよう構成する必要があります。
Manually Configure	このページの［Settings］領域で定義したネットワーク設定を使用するには、このオプションを選択します。
ホスト名	このシステムのネットワーク パラメーターを指定します。

表 5 ［General］ページの設定 （続き）

項目	説明
	注 DHCP を通してネットワーク設定を取得する場合、［**Hardware**］ > ［**Network**］ > ［**Settings**］または `net set hostname` コマンドでホスト名を手動で構成できます。IPv6 を介して DHCP を使用する場合、ホスト名を手動で構成する必要があります。
ドメイン名	このシステムが所属するネットワーク ドメインを指定します。
Default IPv4 Gateway	デスティネーション システムのルート エントリーがない場合に、システムがネットワーク要求を転送するゲートウェイの IPv4 アドレスを指定します。
Default IPv6 Gateway	デスティネーション システムのルート エントリーが存在しない場合に、システムがネットワーク要求を転送するゲートウェイの IPv6 アドレスを指定します。

［Network Interfaces］ページ

［Interfaces］ページで、IP ネットワークに各インターフェイスが参加する方法を定義するネットワーク設定を構成できます。

構成ウィザード以外でそれらのネットワーク設定を構成するには、［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。

表 6 ［Interfaces］ページの設定

項目	説明
インターフェイス	システム上で使用可能なインターフェイスをリストします。
Enabled	各インターフェイスが有効か（チェックボックスが選択されている）、無効か（選択されていない）を表示します。チェックボックスをクリックすると、インターフェイスの有効状態と無効状態が切り換わります。
DHCP	各インターフェイスの現在の DHCP（Dynamic Host Control Protocol）を表示します。IPv4 DHCP 接続の場合は［**v4**］、IPv6 接続の場合は［**v6**］、DHCP を無効化する場合は［**no**］を選択します。
IP アドレス	このシステムの IPv4 または IPv6 アドレスを指定します。IP アドレスを構成するには、DHCP を［**No**］に設定する必要があります。 注 DD140、DD160、DD610、DD620、および DD630 システムは、インターフェイス eth0a（レガシー ポート名を使用するシステムでは eth0）上、または同じインターフェイスで作成された VLAN 上の IPv6 には対応していません。
ネットマスク	このシステムのネットワーク マスクを指定します。ネットワーク マスクを構成するには、DHCP を［**No**］に設定する必要があります。

表 6 ［Interfaces］ページの設定 （続き）

項目	説明
リンク	Ethernet 接続がアクティブ’（Yes）かそうではない（No）かが表示されます。

［Network DNS］ページ

［DNS］ページでは、システムが DSN（ドメイン ネーム システム）で DNS サーバーの IP アドレスを取得する方法を構成できます。

構成ウィザード以外でそれらのネットワーク設定を構成するには、
［**Hardware**］ > ［**Ethernet**］ > ［**Settings**］を選択します。

表 7 ［DNS］ページの設定

項目	説明
DHCP を使用して DNS を取得します。	システムが DHCP（Dynamic Host Control Protocol）サーバーから DNS IP アドレスを収集するように指定するには、このオプションを選択します。ネットワーク インターフェイスを構成する場合、1 つ以上のインターフェイスが DHCP を使用するよう構成する必要があります。
Manually configure DNS list.	DNS サーバー IP アドレスを手動で入力したい場合、このオプションを選択します。
［Add］（[+]）ボタン	このボタンをクリックすると、DNS IP アドレスを［DNS IP Address］リストに追加できるダイアログが表示されます。DNS IP アドレスを追加または削除するには、［**Manually configure DNS list**］を選択する必要があります。
［Delete (X)］ボタン	このボタンをクリックすると、DNS IP アドレスが［DNS IP Address］リストから削除されます。このボタンを有効化するには、削除する IP アドレスを選択する必要もあります。DNS IP アドレスを追加または削除するには、［**Manually configure DNS list**］を選択する必要があります。
IP Address Checkboxes	削除したい DNS IP アドレスのチェックボックスを選択します。すべての IP アドレスを削除したい場合、［DNS IP Address］チェックボックスを選択します。DNS IP アドレスを追加または削除するには、［**Manually configure DNS list**］を選択する必要があります。

File System

［**File System**］セクションでは、アクティブ階層とクラウド階層のストレージを構成することができます。それぞれに、独立したウィザード ページがあります。このセクションでファイル システムを作成することもできます。ファイル システムがすでに作成されている場合、構成ページにはアクセスできません。

ファイル システムが作成されていないときに［**File System**］セクションを表示するといつでも、システムにエラー メッセージが表示されます。ファイル システムを作成する処理手順を続行します。

ストレージ階層の構成ページ

ストレージ階層の構成ページでは、アクティブ階層、アーカイブ階層、DD Cloud Tier という、システム上のライセンスされた各階層のストレージを構成できます。各階層には、独立したウィザード ペー

ジがあります。ファイル システムがすでに作成されている場合、ストレージ階層の構成ページにはアクセスできません。

アクティブ階層の構成

[Configure Active Tier] セクションでは、アクティブなストレージ階層のデバイスを構成することができます。アクティブ階層は、バックアップ データが存在する場所です。アクティブ階層にストレージを追加するには、1 台以上のデバイスを選択し、階層に追加します。インストールされている容量ライセンスまでストレージ デバイスを追加できます。

DD3300 システムでは、アクティブ階層用に 4 TB のデバイスが必要です。

表 8 追加可能ストレージ

項目	説明
ID (Device in DD VE)	ディスクの識別子は次のいずれかを指定できます。 • エンクロージャおよびディスク番号（エンクロージャ スロット形式、DS60 シェルフの場合はエンクロージャ パック形式）。 • DD VTL や vDisk などで使用される論理デバイスのデバイス番号 • LUN
ディスク	ディスク パックまたは LUN を構成するディスク。これは DD VE インスタンスには適用されません。
モデル	ディスク シェルフのタイプ。これは DD VE インスタンスには適用されません。
Disk Count	ディスク パックまたは LUN 内のディスクの数。これは DD VE インスタンスには適用されません。
Disk Size (Size in DD VE)	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]
License Needed	階層にストレージを追加するために必要なライセンスされた容量。
障害発生ディスク	ディスク パックまたは LAN 内の障害が発生したディスク。これは DD VE インスタンスには適用されません。
Type	SCSI。これは DD VE インスタンスにのみ適用されます。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

表 9 アクティブ階層の値

項目	説明
ID (Device in DD VE)	ディスクの識別子は次のいずれかを指定できます。 • エンクロージャおよびディスク番号（エンクロージャ スロット形式、DS60 シェルフの場合はエンクロージャ パック形式）。これは DD VE インスタンスには適用されません。 • DD VTL と vDisk などで使用される論理デバイスのデバイス番号 • LUN
ディスク	ディスク パックまたは LUN を構成するディスク。これは DD VE インスタンスには適用されません。

表 9 アクティブ階層の値 （続き）

項目	説明
モデル	ディスク シェルフのタイプ。これは DD VE インスタンスには適用されません。
Disk Count	ディスク パックまたは LUN 内のディスクの数。これは DD VE インスタンスには適用されません。
Disk Size (Size in DD VE)	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]
License Used	ストレージによって消費されたライセンスされた容量。
障害発生ディスク	ディスク パックまたは LAN 内の障害が発生したディスク。これは DD VE インスタンスには適用されません。
Configured	新規または既存のストレージ。これは DD VE インスタンスには適用されません。
Type	SCSI。これは DD VE インスタンスにのみ適用されます。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

アーカイブ階層の構成

［Configure Archive Tier］セクションでは、アーカイブ ストレージ階層のデバイスを構成することができます。アーカイブ階層は、DD Extended Retention 機能を使用してアーカイブされたデータが存在する場所です。アーカイブ階層にストレージを追加するには、1 台以上のデバイスを選択し、階層に追加します。インストールされている容量ライセンスまでストレージ デバイスを追加できます。

アーカイブ階層ストレージは、DD3300 システム上と、DD VE インスタンス上では使用できません。

表 10 追加可能ストレージ

項目	説明
ID	ディスクの識別子は次のいずれかを指定できます。 • エンクロージャおよびディスク番号（エンクロージャ スロット形式、DS60 シェルフの場合はエンクロージャ パック形式）。 • DD VTL や vDisk などで使用される論理デバイスのデバイス番号 • LUN
ディスク	ディスク パックまたは LUN を構成するディスク。
Model	ディスク シェルフのタイプ。
Disk Count	ディスク パックまたは LUN 内のディスクの数。
Disk Size (Size in DD VE)	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]
License Needed	階層にストレージを追加するために必要なライセンスされた容量。
障害発生ディスク	ディスク パックまたは LAN 内の障害が発生したディスク。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

表 11 アーカイブ階層の値

項目	説明
ID	ディスクの識別子は次のいずれかを指定できます。 • エンクロージャおよびディスク番号（エンクロージャ スロット形式、DS60 シェルフの場合はエンクロージャ パック形式）。これは DD VE インスタンスには適用されません。 • DD VTL と vDisk などで使用される論理デバイスのデバイス番号 • LUN
ディスク	ディスク パックまたは LUN を構成するディスク。
Model	ディスク シェルフのタイプ。
Disk Count	ディスク パックまたは LUN 内のディスクの数。
Disk Size (Size in DD VE)	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]
License Used	ストレージによって消費されたライセンスされた容量。
障害発生ディスク	ディスク パックまたは LAN 内の障害が発生したディスク。
Configured	新規または既存のストレージ。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

クラウド階層の構成

[Configure Cloud Tier] セクションでは、クラウド ストレージ階層のデバイスを構成することができます。クラウド階層にストレージを追加するには、1 台以上のデバイスを選択し、階層に追加します。インストールされている容量ライセンスまでストレージ デバイスを追加できます。

DD3300 システムでは、DD Cloud Tier 用に 1 TB のデバイスが必要です。

表 12 追加可能ストレージ

項目	説明
ID (Device in DD VE)	ディスクの識別子は次のいずれかを指定できます。 • エンクロージャおよびディスク番号（エンクロージャ スロット形式、DS60 シェルフの場合はエンクロージャ パック形式）。 • DD VTL や vDisk などで使用される論理デバイスのデバイス番号 • LUN
ディスク	ディスク パックまたは LUN を構成するディスク。これは DD VE インスタンスには適用されません。
モデル	ディスク シェルフのタイプ。これは DD VE インスタンスには適用されません。
Disk Count	ディスク パックまたは LUN 内のディスクの数。これは DD VE インスタンスには適用されません。
Disk Size (Size in DD VE)	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]

表 12 追加可能ストレージ （続き）

項目	説明
License Needed	階層にストレージを追加するために必要なライセンスされた容量。
障害発生ディスク	ディスク パックまたは LAN 内の障害が発生したディスク。これは DD VE インスタンスには適用されません。
Type	SCSI。これは DD VE インスタンスにのみ適用されます。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

表 13 クラウド階層の値

項目	説明
ID (Device in DD VE)	ディスクの識別子は次のいずれかを指定できます。 • エンクロージャおよびディスク番号（エンクロージャ スロット形式、DS60 シェルフの場合はエンクロージャ パック形式）。これは DD VE インスタンスには適用されません。 • DD VTL と vDisk などで使用される論理デバイスのデバイス番号 • LUN
ディスク	ディスク パックまたは LUN を構成するディスク。これは DD VE インスタンスには適用されません。
モデル	ディスク シェルフのタイプ。これは DD VE インスタンスには適用されません。
Disk Count	ディスク パックまたは LUN 内のディスクの数。これは DD VE インスタンスには適用されません。
Disk Size (Size in DD VE)	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]
License Used	ストレージによって消費されたライセンスされた容量。
障害発生ディスク	ディスク パックまたは LAN 内の障害が発生したディスク。これは DD VE インスタンスには適用されません。
Configured	新規または既存のストレージ。これは DD VE インスタンスには適用されません。
Type	SCSI。これは DD VE インスタンスにのみ適用されます。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

ファイル システムの作成ページ

［Create File System］ページでは、ファイル システム内の各ストレージ階層の許容サイズを確認し、作成後にファイル システムを自動的に有効化できます。

System Settings

［**System Settings**］セクションでは、システム パスワードおよびメール設定を構成できます。システム設定を構成するには［**Yes**］を、システム設定の構成をスキップするには［**No**］をクリックします。

［System Settings Administrator］ページ

［Administrator］ページには、管理者パスワードおよびシステムの管理者との通信方法を構成できます。

表 14 ［Administrator］ページの設定

項目	説明
ユーザー名	デフォルトの管理者名は［sysadmin］です。sysadmin ユーザーには、名称変更および削除は実行できません。
古いパスワード	sysadmin の古いパスワードを入力します。
新しいパスワード	sysadmin の新しいパスワードを入力します。
Verify New Password	sysadmin の新しいパスワードを再入力します。
Admin Email	DD System Manager がアラートと自動サポート メール メッセージを送信するメール アドレス指定します。
Send Alert Notification Emails to this address	チェックすると、アラート イベント発生時に、DD System Manager が管理者 E メール アドレスにアラート通知を送信するように構成されます。
Send Daily Alert Summary Emails to this address	チェックすると、毎日の終わりに、DD System Manager が管理者 E メール アドレスにアラート サマリーを送信するように構成されます。
Send Autosupport Emails to this address	チェックすると、DD System Manager が管理者ユーザー自動サポート E メール（システム アクティビティおよびステータスを記載した日次レポート）を送信するように構成されます。

［System Settings Email/Location］ページ

［Email/Location］ページでは、メール サーバー名の構成、Data Domain に送信されるシステム情報の管理、システムを識別する場所の名前を指定します。

表 15 ［Email/Location］ページの設定

項目	説明
メール サーバ	システムとやり取りするメールを管理するメール サーバーの名前を指定します。
認証情報	メール サーバーの資格情報を要求するかどうかを選択します。
User Name	資格情報が有効になっている場合は、メール サーバーのユーザー名を指定します。
Password	資格情報が有効になっている場合は、メール サーバーのパスワードを指定します。

表 15 ［Email/Location］ページの設定 （続き）

項目	説明
Send Alert Notification Emails to Data Domain	チェックすると、DD System Manager が Data Domain にアラート通知メールを送信するように構成されます。
Send Vendor Support Notification Emails to Data Domain	チェックすると、DD System Manager が Data Domain にベンダー サポート通知メールを送信するように構成されます。
Location	必要に応じて、このオプション属性を使用してシステムの場所を記録します。場所を指定した場合、この情報は SNMP システムの場所として保存されます。

DD Boost プロトコル

［**DD Boost**］設定セクションでは、DD Boost プロトコルの設定を構成することができます。DD Boost プロトコルの設定を構成するには［**Yes**］を、DD Boost 構成をスキップするには［**No**］をクリックします。

［DD Boost Protocol Storage Unit］ページ

［Storage Unit］ページでは、DD Boost ストレージ ユニットを構成できます。

構成ウィザード外でそれらの設定を構成するには、［**Protocols** ］>［**DD Boost** ］>［**Storage Units** ］ > ［**+**（プラス記号）］を選択してストレージ ユニットを追加するか、［**pencil**］をクリックしてストレージ ユニットを変更するか、［**X**］をクリックしてストレージ ユニットを削除します。

表 16 ［Storage Unit］ページの設定

項目	説明
Storage Unit	DD Boost ストレージ ユニットの名前。オプションで、この名前を変更できます。
ユーザー	デフォルト DD Boost ユーザーには、既存のユーザーを選択するか、［Create a new Local User］を選択し、［User name］、［Password］、［Management Role］を入力します。役割には次のいずれかを指定できます。 • ［Admin role］: Data Domain システム全体を構成および監視できます。 • ［User role］: Data Domain システムを監視し、自分のパスワードを変更できます。 • ［Security role］: user ロール権限に加えて、セキュリティ担当者の設定およびその他のセキュリティ担当オペレーターの管理が可能になります。 • ［Backup-operator role］: user ロール権限に加えて、スナップショットの作成、テープのインポートとエクスポート、DD VTL ライブラリ内のテープの移動が可能になります。 • ［None role］: DD Boost 認証での使用のみを目的としているため、Data Domain システムを監視または構成できません。None

表 16 ［Storage Unit］ページの設定 （続き）

項目	説明
	は、SMT tenant-admin と tenant-user の役割の親役割です。また None は、DD Boost ストレージ オーナーの優先ユーザー タイプでもあります。ここでローカル ユーザーを作成すると、そのユーザは none の役割のみを持ちます。

［DD Boost Protocol Fibre Channel］ページ

［Fibre Channel］ページでは、Fibre Channel 経由の DD Boost Access Group を構成できます。

構成ウィザード外でそれらの設定を構成するには、［**Protocols** ］ > ［**DD Boost** ］ > ［**Fibre Channel** ］ > ［**+**（プラス記号）］を選択してアクセス グループを追加するか、［**pencil**］をクリックしてアクセス グループを変更するか、［**X**］をクリックしてアクセス グループを削除します。

表 17 ［Fibre Channel］ページの設定

項目	説明
Configure DD Boost over Fibre Channel	Fibre Channel 経由で DD Boost を構成したい場合、このチェックボックスを選択します。
Group Name (1-128 Chars)	アクセス グループを作成します。一意の名前を入力します。重複アクセス グループには対応していません。
Initiators	1 つ以上のイニシエーターを選択します。オプションで、新しいものを入力して、イニシエーター名を変更します。イニシエーターは、FC（Fibre Channel）プロトコルを使用してデータの読み取りと書き込みを行うシステムに接続するバックアップ クライアントです。特定のイニシエータでは、FC 経由の DD Boost または DD VTL のいずれかをサポートできますが、両方はサポートできません。
デバイス	使用するデバイスがリストされます。これらのデバイスはすべてのエンドポイントで利用できます。エンドポイントは、Data Domain システム上の論理ターゲットで、イニシエーターの接続先です。

CIFS プロトコル

［**CIFS Protocol**］設定セクションでは、CIFS プロトコルの設定を構成することができます。CIFS プロトコルの設定を構成するには［**Yes**］を、CIFS 構成をスキップするには［**No**］をクリックします。

Data Domain システムでは、MTree という用語を使用してディレクトリを表します。ディレクトリ パスを構成するとき、DD OS は MTree を作成し、そこにデータが存在します。

［CIFS Protocol Authentication］ページ

［Authentication］ページでは、システムの Active Directory とワークグループを構成できます。

構成ウィザード以外でこれらの設定を構成するには、
［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

表 18 ［Authentication］ページの設定

項目	説明
Active Directory/Kerberos Authentication	Active Directory Kerberos 認証を有効化、無効化、および構成する場合、このパネルを展開します。
Workgroup Authentication	Workgroup authentication を構成する場合、このパネルを展開します。
LDAP 認証	LDAP 認証を構成する場合、このパネルを展開します。
NIS Authentication	NIS 認証を構成する場合、このパネルを展開します。

［CIFS Protocol Share］ページ

［Share］ページでは、システムの CIFS プロトコル共有名とディレクトリ パスを構成できます。

構成ウィザード以外でそれらの設定を構成するには、
［**Protocols**］ > ［**CIFS**］ > ［**Shares**］ > ［**Create**］を選択します。

表 19 ［Share］ページの設定

項目	説明
Share Name	システムの共有名を入力します。
Directory Path	システムへのディレクトリ パスを入力します。
［Add］（[+]）ボタン	［+］をクリックして、システム クライアント、ユーザー、またはグループを入力します。
鉛筆アイコンをクリックし、	クライアント、ユーザー、またはグループを変更します。
［Delete (X)］ボタン	［X］をクリックして、選択したクライアント、ユーザー、またはグループを削除します。

NFS プロトコル[NFS ぷろとこる]

［**NFS Protocol**］設定セクションでは、NFS プロトコルの設定を構成することができます。NFS プロトコルの設定を構成するには［**Yes**］を、NFS 構成をスキップするには［**No**］をクリックします。

Data Domain システムでは、MTree という用語を使用してディレクトリを表します。ディレクトリ パスを構成するとき、DD OS は MTree を作成し、そこにデータが存在します。

［NFS Protocol Export］ページ

［Export］ページでは、NFS プロトコルのエクスポート ディレクトリ パス、ネットワーク クライアント、および NFSv4 の参照を構成できます。

構成ウィザード以外でそれらの設定を構成するには、［**Protocols**］ > ［**NFS**］ > ［**Create**］を選択します。

表 20 ［Export］ページの設定

項目	説明
Directory Path	エクスポートのパス名を入力します。

表 20 ［Export］ページの設定 （続き）

項目	説明
［Add］（[+]）ボタン	［+］をクリックして、システム クライアントまたは NFSv4 の参照を開きます。
鉛筆アイコンをクリックし、	クライアントまたは NFSv4 の参照を変更します。
［Delete (X)］ボタン	［X］をクリックして、選択されたクライアントまたは NFSv4 の参照を削除します。

DD VTL プロトコル

［**DD VTL Protocol**］設定セクションでは、Data Domain 仮想テープ ライブラリの設定を構成することができます。DD VTL 設定を構成するには［**Yes**］を、DD VTL 構成をスキップするには［**No**］をクリックします。

［VTL Protocol Library］ページ

［Library］ページでは、ライブラリの DD VTL プロトコル設定を構成できます。

構成ウィザード外でこれらの設定を構成するには、［**PROTOCOLS**］ > ［**VTL**］ > ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > ［**More Tasks**］ > ［**Library**］ > ［**Create**］を選択します。

表 21 ［Library］ページの設定

項目	説明
Library Name	英数字 1～32 文字で名前を入力します。
ドライブ数	サポートされるテープ ドライブの数。
Drive Model	ドロップダウン リストから任意のモデルを選択します。 • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5（デフォルト） • HP-LTO-3 • HP-LTO-4
スロット数	ライブラリ 1 つあたりのスロットの数を入力します。 • 1 ライブラリあたり最大 32,000 個のスロット • 1 システムあたり最大 64,000 個のスロット • この値は、ドライブの数以上にする必要があります。
Number of CAPs	（オプション）CAP（カートリッジ アクセス ポート）の数を入力します。 • 1 ライブラリあたり最大 100 個の CAP • 1 システムあたり最大 1000 個の CAP

表 21 ［Library］ページの設定 （続き）

項目	説明
Changer Model Name	ドロップダウン リストから任意のモデルを選択します。 • L180（デフォルト） • RESTORER-L180 • TS3500 • i2000 • I6000 • DDVTL
Starting Barcode	A990000LA の形式で、最初のテープの所定のバーコードを入力します。
Tape Capacity	（オプションで）テープ容量を入力します。指定されなかった場合、容量はバーコードの最後の文字から取られます。

［VTL Protocol Access Group］ページ

［Access Group］ページでは、アクセス グループの DD VTL プロトコルの設定を構成できます。

構成ウィザード外でそれらの設定を構成するには、［**PROTOCOLS**］ > ［**VTL**］ > ［**Access Groups**］ > ［**Groups**］ > ［**More Tasks**］ > ［**Group**］ > ［**Create**］を選択します。

表 22 ［Access Group］ページの設定

項目	説明
グループ名	1～128 文字の一意の名前を入力します。重複アクセス グループには対応していません。
Initiators	1 つ以上のイニシエーターを選択します。オプションで、新しいものを入力して、イニシエーター名を変更します。イニシエータは、FC（ファイバ チャネル）プロトコルを使用してデータの読み取りと書き込みを行うシステムに接続するバックアップ クライアントです。特定のイニシエータでは、FC 経由の DD Boost または DD VTL のいずれかをサポートできますが、両方はサポートできません。
Devices	使用されるデバイス（ドライブとチェンジャー）がリストされます。これらのデバイスはすべてのエンドポイントで利用できます。エンドポイントは、Data Domain システム上の論理ターゲットで、イニシエーターの接続先です。

Data Domain のコマンド ライン インターフェイス

CLI（コマンド ライン インターフェイス）は、DD System Manager の代わりに、または DD System Manager に加えて使用できるテキスト方式のインターフェイスです。ほとんどの管理タスクは、DD System Manager で、または CLI を使用して実行できます。場合によっては、DD System Manager ではまだサポートされていない構成オプションとレポートが CLI によって提供されます。

IP アドレス一覧など、一覧を受け入れる Data Domain システム コマンドでは、コンマ、スペース、またはその両方によって区切られたエントリーを使用できます。

Tab キーを使用して、次のことを行うことができます。

- エントリーが一意の場合に、コマンド エントリーを記入する。Tab 補完機能は、すべてのキーワードでサポートされます。たとえば、`syst` Tab `sh`Tab `st` Tab と入力するとコマンド `system show stats` が表示されます。
- Tab キーを押す前に文字を入力しなかった場合、次の使用可能なオプションを表示する。
- Tab キーを押す前に文字を入力した場合、部分一致のトークンを表示するか、一意のエントリーを記入する。

各 CLI コマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。オンライン ヘルプが使用可能であり、各コマンドの完全な構文が表示されます。

CLI へのログイン

システムへの直接接続を使用するか、SSH または Telnet を介した Ethernet 接続を使用して、CLI にアクセスできます。

はじめに

CLI を使用するには、次のいずれかの方式を使用して、システムへのローカルまたはリモート接続を確立する必要があります。

- システムのシリアル コンソール ポートを介して接続している場合は、ターミナル コンソールをそのポートに接続して、通信設定 （9,600 ボー、8 データ ビット、パリティなし、1 ストップ ビット）を使用します。
- システムにキーボードとモニター用のポートがある場合は、キーボードとモニターをそれらのポートに接続します。
- Ethernet 経由で接続している場合は、SSH または Telnet クライアント ソフトウェアを使用して、システムと通信可能な Ethernet ネットワークにコンピューターを接続します。

手順

1. SSH または Telnet 接続を使用して CLI にアクセスする場合は、SSH または Telnet クライアントを起動して、システムの IP アドレスまたはホスト名を指定します。

   接続の開始方法については、クライアント ソフトウェアのマニュアルを参照してください。システムからユーザー名を要求するプロンプトが表示されます。
2. プロンプトが表示されたら、お使いのシステムのユーザー名を入力します。
3. プロンプトが表示されたら、お使いのシステムのパスワードを入力します。

次の例は、SSH クライアント ソフトウェアを使用した、[mysystem] という名前のシステムへの SSH ログインを示しています。

```
# ssh -l sysadmin mysystem.mydomain.com
Data Domain OS 5.6.0.0-19899
Password:
```

CLI のオンライン ヘルプのガイドライン

CLI では、コマンド構文を含む 2 つのタイプのヘルプ（syntax-only help と command-description help）が表示されます。どちらのタイプのヘルプにも、必要な情報の検索にかかる時間を短縮できる機能があります。

次のガイドラインでは、syntax-only help の使用方法について説明しています。

- 最上位 CLI コマンドを一覧表示するには、疑問符（**?**）を入力するか、プロンプトでコマンド `help` を入力します。
- 最上位コマンドのすべての形式を一覧表示するには、プロンプトでオプションなしでコマンドを入力するか、**command**`?`を入力します。
- 特定のキーワードを使用するすべてのコマンドを一覧表示するには、`help`**keyword** または`?` **keyword** を入力します。
  たとえば、`? password` は **password** 引数を使用するすべての **Data Domain** システム コマンドを表示します。

次のガイドラインでは、**command-description help** の使用方法について説明しています。

- 最上位 CLI コマンドを一覧表示するには、疑問符（**?**）を入力するか、プロンプトでコマンド `help` を入力します。
- 最上位コマンドのすべての形式を紹介とともに一覧表示するには、`help`**command** または`?` **command** を入力します。
- 各ヘルプの説明の末尾に、`END` とマークされます。**Enter** キーを押して、**CLI** プロンプトに戻ります。
- 完全なヘルプの説明が画面に納まらない場合、コロン プロンプト（**:**） が画面の下部に表示されます。次のガイドラインでは、このプロンプトが表示されたときの対応方法について説明しています。
  - ヘルプ画面内を移動するには、上下矢印を使用します。
  - 現在のヘルプ画面を終了し、**CLI** プロンプトに戻るには、**q** を押します。
  - ヘルプ画面の移動についてのヘルプを表示するには、**h** を押します。
  - ヘルプ画面でテキストを検索するには、スラッシュ（**/**）の後に、検索基準として使用するパターンを入力し、**Enter** キーを押します。一致がハイライトされます。

第 3 章

Data Domain システムの管理

本章には、次のセクションが含まれます。

- システム管理の概要 56
- システムの再起動 57
- システム電源のオン/オフ 57
- システム アップグレードの管理 59
- 電子ライセンスの管理 68
- システム ストレージの管理 69
- ネットワーク接続の管理 78
- システム パスフレーズの管理 100
- システム アクセスの管理 102
- メール サーバー設定の構成 135
- 日付と時刻の設定の管理 136
- システム プロパティの管理 136
- SNMP 管理 SNMP かんり 137
- 自動サポート レポートの管理 146
- サポート バンドルの管理 149
- コアダンプの管理 150
- アラート通知の管理 151
- サポート デリバリの管理 158
- ログ ファイルの管理 160
- IPMI によるリモート システムの電源管理 165

システム管理の概要

DD System Manager によって、DD System Manager がインストールされたシステムを管理できます。

- レプリケーションに対応するには、DD System Manager は、以前の 2 つのバージョン、現在のバージョン、次の 2 つのバージョン（公開されたとき）を実行しているシステムの追加に対応しています。Release 6.0 では、DD System Manager は、DD OS バージョン 5.6～5.7 および以降 2 リリースのレプリケーションについて、システムの追加に対応しています。

注

高い負荷を処理する際、システムは通常よりも反応が遅くなる場合があります。その場合、DD System Manager または CLI から発行された管理コマンドの所要時間が長くある場合があります。所要時間が許容限度を超えると、操作が完了した場合でも、タイムアウト エラーが返されます。

下表は、DD System Manager がサポートするユーザー セッションの最大数の推奨値を示しています。

表 23 DD System Manager がサポートするユーザーの最大数

システム モデル	最大アクティブ ユーザー数	最大ログイン ユーザー数
4 GB モデル [a]	5	10
8 GB モデル [b]	10	15
16 GB およびそれ以上のモデル [c]	10	20

a. DD140 と DD2200（4 TB）を含む
b. DD610 と DD630 を含む
c. DD670、DD860、DD890、DD990、DD2200（>7.5 TB）、DD4200、DD4500、DD6300、DD6800、DD7200、DD9300、DD9500、DD9800 を含む

注

HA システムの初期設定は、DD System Manager からは実行できませんが、構成済みの HA システムのステータスは DD System Manager から表示できます。

HA システム管理の概要

2 つのノード（アクティブ ノードとスタンバイ ノード）間の HA 関係は、DDSH CLI を通じて設定します。

初期設定は 2 つのノードのどちらででも実行できますが、一度に 1 つのノードでしか実行できません。システムの相互接続と同一ハードウェアが両方のノードで最初にセットアップされていることが、HA の前提条件です。

注

両方の DDR で、設定時およびシステム起動時に検証されるハードウェアが同一である必要があります。

システムの新規インストールで設定を行う場合、ライセンスがインストールされているノードで `ha create` コマンドを実行する必要があります。既存のシステムと、新しくインストールしたシステム（アップグレード）で設定を行う場合は、既存のシステムから実行する必要があります。

HA システムの計画的保守

HA アーキテクチャでは、ローリング アップグレードが利用できます。ローリング アップグレードにより、DD OS アップグレードのためのメンテナンス ダウンタイムが短縮されます。

ローリング アップグレードを行うと、自動的に HA ノードが 1 つずつ順にアップグレードされます。スタンバイ ノードが再起動され、最初にアップグレードされます。新しくアップグレードされたノードは、HA フェールオーバーによってアクティブなロールを引き継ぎます。フェールオーバーの後は 2 番目のノードが再起動され、アップグレードの後のスタンバイ ノードの役割を担います。

両方のシステムが同じレベルにアップグレードされ、HA の状態が完全にリストアされるまでは、データ変換が必要なシステム アップグレード操作は開始できません。

システムの再起動

タイム ゾーンの変更などの構成の変更時には、システムの再起動が必要になることがあります。

手順

1. ［**Maintenance**］ > ［**System**］ > ［**Reboot System**］を選択します。
2. ［**OK**］をクリックして確定します。

システム電源のオン/オフ

システム電源をオン/オフする際には、適切な手順に従い、ファイル システムと構成の整合性を保つ必要があります。

シャーシの電源スイッチを使用してシステムの電源をオフにしないでください。そうすることで、IPMI を使用したリモート電源制御ができなくなります。代わりに `system poweroff` コマンドを使用します。`system poweroff` コマンドは、システムをシャットダウンし、電源をオフにします。

IMPI Remote System Power Down 機能は、DD OS の計画的なシャットダウンを実行しません。`system poweroff` コマンドが失敗した場合のみ、この機能を使用します。

HA システムでは、両方のノードへの接続が必要です。

Data Domain システムの電源をオフにするには、次の手順を実行します。

手順

1. システム上の I/O が停止したことを確認します。

   次のコマンドを実行します。

   - `cifs show active`
   - `nfs show active`
   - `system show stats view sysstat interval 2`
   - `system show perf`

2. HA システムでは、HA 構成の稼働状態を確認します。

   次のコマンドを実行します。
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
-------------------------- --------- --------- --------
```

注

この出力例は、正常稼働しているシステムを示します。障害が発生したコンポーネントを交換するためにシステムがシャット ダウン中の場合、[HA System Status] は degraded になり、一方または両方のノードで [HA State] はオフラインと表示されます。

3. `alerts show current` コマンドを実行します。HA ペアでは、最初にアクティブ ノードでコマンドを実行してからスタンバイ ノードで実行します。
4. HA システムでは、システムが高可用性状態で、両方のノードがオンラインであれば、`ha offline` コマンドを実行します。HA ステータスが縮退の場合は、このステップをスキップします。
5. `system poweroff` コマンドを実行します。HA ペアでは、最初にアクティブ ノードでコマンドを実行してからスタンバイ ノードで実行します。

   ```
   # system poweroff

   Continue? (yes|no|?) [no]: yes
   ```

   このコマンドは、自動的に DD OS 処理の計画的なシャットダウンを実行し、管理ユーザーのみ使用できます。
6. 1 台以上のコントローラ上の PSU から電源コードを取り外します。
7. 1 台以上のコントローラ上の青い電源 LED がオフであるかどうか調べて、システムが電源オフになっていることを確認します。

   コントローラーの電源がオフになったら、外部拡張シェルフ（ES30、DS60、FS15）をすべて電源オフにします。

システムの電源オン

システムのダウンタイムが完了したら Data Domain システムに電源をリストアします。

手順

1. Data Domain コントローラーの電源をオンにする前に、拡張シェルフの電源をオンにします。すべての拡張シェルフの電源がオンになった後、約 3 分待機します。

   注

   コントローラーは、シャーシといずれかの内部ストレージです。[Data Domain システム]とは、コントローラーとオプションの外部ストレージを指します。
2. コントローラーの電源コードを接続し、コントローラーに電源ボタンがある場合は電源ボタンを押します（お使いの Data Domain システムについては、「Installation and Setup Guide」を参照してください）。HA システムでは、まずアクティブ ノードの電源をオンにし、次にスタンバイ ノードをオンにします。

注

一部の Data Domain アプライアンスには、従来の電源ボタンがなく、「常時オン」になるように設計されており、AC 電源が供給されるとすぐに電源が投入されます。

3. HA システムでは、HA 構成の稼働状態を確認します。

   次のコマンドを実行します。
   `ha status`

```
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com         0       active    online
apollo-ha3a-p1.emc.com         1       standby   offline
--------------------------- --------- --------- --------
```

4. HA システムでノードのいずれかがオフラインとして表示されている場合は、このノード上で `ha online` コマンドを実行して HA 構成をリストアします。
5. Data Domain が完全に起動し、オペレーティング システムが実行されていることを確認します。これは、システム コンソールまたは SSH セッションから Data Domain システムに対して行うことができます。システムにログインできれば、システムは起動しています。
6. `alerts show current` コマンドを実行します。HA ペアでは、最初にアクティブ ノードでコマンドを実行してからスタンバイ ノードで実行します。

システム アップグレードの管理

DD OS システムをアップグレードするには、ターゲット システム上に新しいソフトウェアをインストールするスペースが十分にあることを確認して、アップグレードされるシステムにソフトウェアを転送し、アップグレードを開始します。HA システムの場合、アクティブ ノードにソフトウェアを転送し、アクティブ ノードからアップグレードを開始します。

HA システムでソフトウェアのアップグレードを実行するには、フローティング IP アドレスを使用して DD System Manager にアクセスします。

⚠ 注意

DD OS 6.0 では、Secure Remote Support バージョン 3（ESRSv3）を使用します。DD OS 5.X を実行するシステムを DD OS 6.0 にアップグレードすると、既存の ConnectEMC 構成がシステムから削除されます。アップグレードが完了したら、ConnectEMC を手動で再構成します。

システムが、MD5 で署名された証明書を使用している場合は、アップグレード プロセス中に強力なハッシュ アルゴリズムを使って証明書を再生成します。

最小停止アップグレード
最小停止アップグレード（MDU）機能を使用すると、システムを再起動せずに特定のソフトウェア コンポーネントをアップグレードしたり、バグ修正を適用したりできます。MDU 機能を使用すると、アップグレードされるコンポーネントに依存するサービスのみが停止するため、特定のソフトウェア アップグレード中に大幅なダウンタイムを防ぐことができます。

すべてのソフトウェア コンポーネントが最小停止アップグレードの対象となるわけではありません。このようなコンポーネントは、通常の DD OS システム ソフトウェア アップグレードの一環としてアップグレードする必要があります。DD OS ソフトウェア アップグレードでは、大規模な RPM（アップグレード バンドル）を使用します。この RPM では、すべての DD OS コンポーネントのアップグレード アクションが

実行されます。MDU では、より小規模なコンポーネント バンドルを使用します。このバンドルでは、特定のソフトウェア コンポーネントが個別にアップグレードされます。

RPM 署名検証
RPM 署名検証では、アップグレード用にダウンロードした Data Domain RPM を検証します。RPM が改ざんされておらず、デジタル署名が有効である場合は、通常どおり RPM を使用できます。RPM が改ざんされており、デジタル署名が破損により無効である場合、RPM は DD OS によって拒否されます。適切なエラー メッセージが表示されます。

注

5.6.0.x から 6.0 にアップグレードする場合、最初に 5.6.0.x システムを 5.6.1.x（またはそれ以降）にアップグレードしてから 6.0 にアップグレードします。

サポート ソフトウェア
DD OS 6.1 では、サポート ソフトウェアと呼ばれるソフトウェア パッケージが導入されています。サポート ソフトウェアは、特定の問題に対処する目的で Data Domain Support Engineering より提供されています。デフォルトでは、Data Domain システムはサポート ソフトウェアをシステムにインストールできません。サポート ソフトウェアの詳細についてはサポートにお問い合わせください。

アップグレード前のチェックリストと概要

DD OS アップグレードを実行する前に、これらの事前チェックリストにあるアイテムを確認する必要があります。それによって、アップグレード プロセスを簡単にして、潜在的な問題を回避します。

アップグレード前の手動タスク

⚠ 注意

このセクションのタスクを実行しないと、アップグレードが失敗する可能性があります。

アップグレード前にこれらのタスクの実行を計画する必要があります。これらのタスクは、どのプロセスでも自動実行されません。

1. Data Domain システムを再起動します。HA システムの場合は、このセクションの残りのチェックを実行した後で、HA システムのアップグレードに関する考慮事項（62 ページ）で説明されている再起動手順に従います。
2. 現在のアラートを確認します。これによって、アップグレード前に解消する必要があるディスクとその他のハードウェアの障害を明らかにできます。

   ```
   # alert show current
   ```

3. `config.net.*`、`crontab`、ネットワークに関連するレジストリ設定が有効であることを確認します。

   たとえば、`reg show config.net` 操作を使用して、`noauto.enabled`、`noauto.speed`、`noauto.full_duplex` が適切に設定されているかどうかを確認します。これによって、ネットワークの速度をネゴシエートできるようになります。また、`.use_dhcp=true` がどうかを確認します。これによって、IP アドレスとネットマスクだけでなく、ゲートウェイも簡単に設定できるようになります。

   この確認が重要なのは、こうした要素の構成を誤ると、再起動が発生して、ネットワークが使用できなくなる可能性があるためです。
4. すべてのネットワーク インターフェイスが使用可能で、適切な IP アドレスが割り当てられているかどうかを確認します。また、次のコマンドで、Data Domain System Manager または他のクライアントを使用して Data Domain システムにアクセスできるかどうかを確認します。

```
# net show
```

5. ディスクの状態を確認して、Data Domain システムのスペアが深く設定されているか、存在しない、障害がある、または再構成状態のディスクがある場合、アップグレードは実行できません。

   ```
   # disk show state
   ```

   ```
   # disk show reliability-data
   ```

6. ディスクの信頼性を確認し、再割り当てセクタが 50 個を超えているディスクを交換します。

   ```
   # disk show reliability-data
   ```

7. エンクロージャのステータスを確認します。

   ```
   # enclosure show all
   ```

   すべてのデバイスが「OK」である必要があります。

8. エンクロージャのトポロジーが正しいことを確認します。

   ```
   # enclosure show topology
   ```

   [**enc.ctrl.port**] フィールドの隣にアスタリスクが着いたエラーがないかも確認します。[**Error Message**] フィールドに`"A possible problem was detected for this shelf controller or the cable connected to it."`のようなエラーがないことも確認します。

9. デバイスのポート マッピングが正しいことを確認します。

   ```
   # system show hardware
   ```

10. 接続したポートのリンク速度を確認します。

    ```
    # system show ports
    ```

11. ファイル システムのステータスを確認して、そのファイル システムが有効化されていて正常に動作していることを判別します。

    ```
    # filesys status
    ```

12. ファイル システムのクリーニングが実行されているかどうかを確認し、実行されている場合は停止します。

    ```
    # filesys clean status
    ```

    ```
    # filesys clean stop
    ```

13. レプリケーションが有効であればそのステータスを確認します。

    ```
    # replication status
    ```

14. システムがクラスタ構成の場合は、クラスタが使用可能で動作しているかどうかを確認します。

    ```
    # cluster show config
    ```

15. DD Cloud Tier 対応システムでは、データの移動がないことを確認します。

    ```
    # data-movement status
    ```

    ```
    # data-movement stop all
    ```

16. クラウドのクリーニングが実行されているかどうかを確認し、実行されている場合は停止します。

    ```
    # cloud clean status
    ```

    ```
    # cloud clean stop
    ```

17. バックアップとリストアのアクティビティが進行中かどうかを確認し、進行中の場合は停止します。

    ```
    # system show stats
    ```

18. `kern.info` のログを確認します。また、ハードウェアに障害が多発している場合は、Data Domain サポートに問い合わせて、アップグレードを実行する前にシステムを調査してください。

    `# log view debug/platform/kern.info`

19. Autosupport Report を、DD OS アップグレードを実行する直前に実行して、解消すべき問題が残っていないかを確認します。

    `# autosupport send <your_email_address>`

HA システムのアップグレードに関する考慮事項

HA システムでは、アップグレード操作を開始する前に複数の固有のステップと、アップグレードの完了後に 1 つの固有の事後チェックを必要とします。

⚠ 注意

HA システムを再起動する前にアップグレード前の手動タスク（60 ページ）で説明されている手動チェックを実行します。

HA システムをアップグレードするときに、アップグレード RPM パッケージをアクティブ ノードにアップロードします。

1. HA システムは、DD OS のアップグレードを実行する前に、両方のノードがオンラインである高可用性状態でなければなりません。`ha status` コマンドを実行して、HA システムの状態を確認します。

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com        0       active    online
apollo-ha3a-p1.emc.com        1       standby   online
--------------------------- --------- --------- --------
```

2. スタンバイ ノード（ノード 1）を再起動します。
3. `ha status` コマンドを実行して、スタンバイ ノードの再起動後に HA システムのステータスが `highly available` と表示されることを確認します。
4. `ha failover` コマンドを実行して、アクティブ ノードからスタンバイ ノードへのフェールオーバーを開始します。
5. `ha status` コマンドを実行して、ノード 1 がアクティブ ノードであり、ノード 0 がスタンバイ ノードであることを確認します。

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com        0       standby   online
apollo-ha3a-p1.emc.com        1       active    online
--------------------------- --------- --------- --------
```

6. スタンバイ ノード（ノード 0）を再起動します。
7. `ha status` コマンドを実行して、スタンバイ ノードの再起動後に HA システムのステータスが `highly available` と表示されることを確認します。
8. `ha failover` コマンドを実行して、アクティブ ノードからスタンバイ ノードへのフェールオーバーを開始します。
9. `ha status` コマンドを実行して、ノード 0 がアクティブ ノードであり、ノード 1 がスタンバイ ノードであることを確認します。

```
# ha status
HA System Name: apollo-ha3a.emc.com
HA System Status: highly available
Node Name                   Node ID   Role      HA State
--------------------------- --------- --------- --------
apollo-ha3a-p0.emc.com       0       active    online
apollo-ha3a-p1.emc.com       1       standby   online
--------------------------- --------- --------- --------
```

アクティブ ノードからアップグレードを開始します。DD OS は HA システムを自動的に認識し、両方のノードでアップグレード手順を実行します。HA アップグレードは、次の順序で実行されます。

1. スタンバイ ノードがまずアップグレードされ、次に再起動されます。
2. 再起動が完了すると、HA システムはフェールオーバーを開始し、スタンバイ ノードがアクティブ ノードとして引き継ぎます。
3. 元のアクティブ ノードがアップグレードされ、その後再起動して、スタンバイ ノードのままになります。

両方のノードがアップグレードされた後、システムはノードを元の構成に戻すために別のフェールオーバーを実行しません。

アップグレード手順が完了したら、`ha status` コマンドを再度実行して、システムが高可用性状態で、両方のノードがオンラインであることを確認します。

必要に応じて、`ha failover` コマンドを実行して、ノードをアップグレード前のロールに戻します。

アップグレード前に実行する自動タスク

DD OS アップグレードのこうした側面を理解することで、プロセスをスムーズに進められます。

アップグレード前に、Data Domain システムの DD OS バージョンで次のタスクを実行します。

1. レプリケーションの初期化が進行中かどうかを判断します。進行中の場合、アップグレードは進められません。
2. .rpm ファイルに含まれるすべてのダイジェストおよびシグネチャを調べて、パッケージの整合性と元を確認します。シグネチャが無効な場合、アップグレードは進められません。
3. 古いバージョンの DD OS のから新しいものにアップグレードすることが可能かどうかを判断します。DD OS 5.7.x または 6.0.x を実行している Data Domain システムは、直接 6.1 にアップグレードできます。この制限は、RPM 署名に起因します。通常、次の状態ではアップグレードできません。
   a. 6.0.0.1 から 6.0.0.4 など、同じバージョン間のアップグレード。（特別な状況下では上書き可能です。詳細は Data Domain サポート担当にお問い合わせください）。
   b. 6.0 から 5.7 など、アップグレードがダウングレード。
   c. 5.5 から 6.0 など、2 つ以上の機能ファミリーを飛び越えるアップグレード。
4. 未知の NFS マウント ポイントがないかどうかを判断します。未知の NFS マウント ポイントが存在する場合、アップグレードは進められません。
5. 実行されている場合、前のアップグレードが正常に完了しているかどうかを判断します。前のアップグレードが正常に終了していない場合または完了しなかった場合、現在のアップグレードは進められません。

アップグレード前に、アップグレード スクリプト（.rpm ファイル内）によって実行される自動タスク

これらのテストによって、Data Domain システム上で実際のアップグレード プロセスが進められます。

1. 異なる 2 種類の NVRAM カードが存在するかどうかを判断します。
2. スペースの使用効率のため、`/ddr` パーティションおよび/（root）パーティションのサイズを確認します。

3. OST のバージョンを確認します。
4. RAID メタグループをアセンブリしてるかどうかを判断します。アセンブリしていない場合、アップグレード プロセスは始まりません。
5. ファイル システムで使用可能なスペースを指定します。
6. アップグレードに十分なスペースを使用できるかどうかを判断します。
7. VTL が存在する場合は、VTL のバージョンを確認します。
8. ファイル システムが有効かどうかを判断し、有効でない場合は有効にします。
9. VTL が有効かどうかを判断します。
10. VTL プールを確認して、MTree への変換を確保します。
11. VTL スペースが十分に使用可能かどうかを判断します。
12. MTree と VTL プールの数が 100 を超えていないことを確認します （この確認は DD OS バージョン 5.0 以降に適用されます）。
13. すべての dg0 ディスクがヘッド ユニットに存在するかどうかを判断します。存在しない場合、アップグレード プロセスは進められないため、この問題を解決する必要があります。
14. ConnectEMC が構成されているかどうかを確認します。構成されている場合は、アップグレード後に ConnectEMC を再構成するようお客様に通知する警告メッセージが表示されます。

これらの確認に加えて、システムでは、ファイル システムを正常に、問題なくシャットダウンできるかどうかを判断します。ファイル システムを正常にシャットダウンできない場合、アップグレード プロセスは停止します。

アップグレード プロセスを妨げる条件

アップグレード プロセスが停止する条件はいくつか考えられます。

- Data Domain システムが動作する状態にない。例：
  - エンクロージャが見つからないなど、ストレージの動作に不具合がある。
  - ファイル システムを正常にシャットダウンできず、コア ダンプが発生する。
  - 以前のアップグレードが正常に終了していない。
- スペースの使用率に問題がある。例：
  - ログ ファイル、コア ダンプ、その他で / （ルート）または /ddr パーティションが一杯になっている。
  - データのアップグレードを実行できるストレージ スペースが足りない。
- Data Domain システムの構成が正しくない。たとえば、NFS マウント ポイントがルート以下に手動で作成されている。
- ストレージ ユニット名を MTree 名に変換できなかった。MTree 名に変換するため、ストレージ ユニット名は、大文字と小文字（a～z、A～Z）、数字（0～9）、アンダースコア（_）のみを使用し、50 文字を超えないようにする。

これらの条件をチェックする目標は、問題があるアップグレードまたはファイル システムの異常が発生したり、伝播したりしないようにすることです。また、この条件は、レプリケーション中のソースとデスティネーションのパートナー システムに関係するアップグレードに適用されます。レプリケーションのソースである Data Domain システム上でアップグレードが失敗したりファイル システムに異常が発生したことが原因で、レプリケーションのデスティネーションとして動作する Data Domain システム上のファイル システムが破損することはありません。

システムでのアップグレード パッケージの表示

DD System Manager を使用することで、システムで最大 5 個のアップグレード パッケージを表示および管理できます。システムをアップグレードするには、Online Support サイトからローカル コンピューターにアップグレード パッケージをダウンロードし、それをターゲット システムにアップロードする必要があります。

手順

1. ［**Maintenance**］ > ［**System**］を選択します。
2. 必要に応じて、アップグレード パッケージを選択し、［**View Checksum**］をクリックしてアップグレード パッケージの MD5 および SHA256 チェックサムを表示します。

結果

DD System Manager では、システムに格納されているすべてのパッケージのファイル名、ファイル サイズ、最終変更日が ［Upgrade Packages Available on Data Domain System］というタイトルのリストに表示されます。

アップグレード パッケージの取得と確認

DD System Manager を使用して、Data Domain Support Web サイトでアップグレード パッケージ ファイルを見つけ、それらのファイルのコピーをシステムにアップロードできます。

注

FTP または NFS を使用して、アップグレード パッケージをシステムにコピーできます。DD System Manager が管理できるシステム アップグレード パッケージの数は最大 5 つですが、`/ddvar/releases` ディレクトリで直接ファイルを管理する場合、スペースの制限以外には制限はありません。FTP はデフォルトで無効になっています。NFS を使用するには、`/ddvar` を外部ホストからエクスポートし、マウントする必要があります。

手順

1. ［**Maintenance**］ > ［**System**］を選択します。
2. アップグレード パッケージを取得するには、［**EMC Online Support**］リンクをクリックして、［Downloads］をクリックし、検索機能を使用してサポート担当者がお使いのシステムに推奨するパッケージを見つけます。アップグレード パッケージをローカル コンピューターに保存します。
3. ［Upgrade Packages Available on Data Domain System］リストにリストされているパッケージが 4 つ以下であることを確認します。

   DD System Manager は、最大 5 つのアップグレード パッケージを管理できます。5 つのパッケージがリストに表示されている場合、新しいパッケージをアップグレードする前に 1 つ以上のパッケージを削除します。
4. ［**Upload Upgrade Package**］をクリックして、アップグレード パッケージからシステムへの転送を開始します。
5. ［Upload Upgrade Package］ダイアログで、［**Browse**］をクリックして、［Choose File to Upload］ダイアログを開きます。ダウンロードしたファイルがあるフォルダーに移動して、ファイルを選択し、［**Open**］をクリックします。
6. ［**OK**］をクリックします。

アップロード進行状況ダイアログが表示されます。アップロードが正しく完了すると、ダウンロード ファイル（拡張子は.rpm）が ［Upgrade Packages Available on Data Domain System］というタイトルのリストに表示されます。

7. アップグレード パッケージの整合性を確認するには、［**View Checksum**］をクリックし、ダイアログに表示されている計算済みのチェックサムをオンライン サポート サイト上の正式なチェックサムと比較します。
8. 手動でアップグレード プレチェックを開始するには、アップグレード パッケージを選択して、［**Upgrade Precheck**］をクリックします。

Data Domain システムのアップグレード

システム上にアップグレード パッケージ ファイルが存在する場合、DD System Manager を使用して、そのアップグレード パッケージを使用したアップグレードを実行できます。

はじめに

アップグレードを完了する手順と、アップグレードに影響する可能性のあるすべての問題の対応については、DD OS のリリース ノートをお読みください。

次の手順では、DD System Manager を使用してアップグレードを開始する方法について説明します。DD System Manager を使用してシステムをアップグレードする前に、アップグレードを実行するシステムのすべてのデータ ドメインの CLI セッションからログアウトします。

注

アップグレード パッケージ ファイルは、ファイル拡張子に.rpm を使用します。このトピックは、DD OS のみを更新していると想定しています。スワッピングの追加、インターフェイス カードの移動など、ハードウェアに変更があった場合、ハードウェアの変更に対応するため、DD OS 構成を更新する必要があります。

手順

1. アップグレードを実行するシステムの DD System Manager にログインします。

   注

   ほとんどのリリースで、2 世代前のメジャー リリース バージョンからのアップグレードまで認められます。リリース 6.0 の場合、アップグレードはリリース 5.6 および 5.7 から認められます。

   注

   リリース ノートでお勧めしているとおり、アップグレード前に Data Domain システムを再起動して、ハードウェアが正常な状態にあることを確認してください。再起動中に問題が検出された場合、アップグレードを開始する前にこれらの問題を解決してください。MDU アップグレードの場合は、再起動する必要がない場合があります。

2. ［**Data Management**］ > ［**File System**］を選択し、ファイル システムが有効かつ実行中であることを確認します。
3. ［**Maintenance**］ > ［**System**］を選択します。
4. ［Upgrade Packages Available on this Data Domain System］リストで、アップグレードに使用するパッケージを選択します。

注

最新バージョンの DD OS のアップグレード パッケージを選択する必要があります。DD OS では、以前のバージョンへのダウングレードはサポートされていません。

5. ［**Perform System Upgrade**］をクリックします。

   ［System Upgrade］ダイアログが表示され、そのダイアログにはアップグレードについての情報とアップグレードされるシステムに現在ログイン中のユーザーのリストが表示されます。

6. アップグレード パッケージのバージョンを確認して、［**OK**］をクリック s 、アップグレードを続けます。

   ［System Upgrade］ダイアログには、アップグレード ステータスと残り時間が表示されます。

   システムのアップグレード中は、アップグレードが完了するまで、DD System Manager を使用してそのシステムを管理することはできません。システムがリスタートすると、リスタート後にアップグレードが続行され、ログイン後、DD System Manager にアップグレード ステータスが表示されます。アップグレードが完了するか、システムがシャットダウンするまで、［System Upgrade progress］ダイアログを開いたままにすることを推奨します。DD OS Release 5.5 以降から新しいバージョンにアップグレードしている場合、およびシステム アップグレードがシャットダウンを必要としない場合、アップグレード完了時に［Login］リンクが表示されます。

注

CLI を使用したアップグレードのステータスを表示するには、`system upgrade status` コマンドを入力します。アップグレードのログ メッセージは`/ddvar/log/debug/platform/upgrade-error.log` および`/ddvar/log/debug/platform/upgrade-info.log` に保存されます。

7. システムがシャットダウンした場合、システムから AC 電源を取り外し、以前の構成をクリアする必要があります。すべての電源ケーブルを 30 秒間抜いた状態にした後、差し直します。システムの電源がオンになり、再起動します。
8. システムの電源が自動的にオンにならず、前面パネルに電源ボタンがある場合は、そのボタンを押します。

必要条件

アップグレードの完了後に、次の要件が適用される場合があります。

- 自己署名 SHA-256 証明書を使用する環境では、アップグレード プロセスが完了した後に証明書を手動で再生し、Data Domain システムに接続する外部システムとの信頼を再確立する必要があります。
  1. 自己署名 CA およびホスト証明書を再生成するには、**`adminaccess certificate generate self-signed-cert regenerate-ca`** コマンドを実行します。証明書を再生成すると、外部システムとの既存の信頼関係が失われます。
  2. Data Domain システムと外部システム間の相互信頼を再確立するには、**`adminaccess trust add host hostname type mutual`** コマンドを実行します。
- WWPN または WWNN 情報が欠落している既存または構成済みの FC ポートを示しているか、FC HBA（ホスト バス アダプタ）ドライバがインストールされていないことをレポートしているシステムでは、`scsitarget endpoint enable all` コマンドを実行します。

レプリケーションの注意

コレクション レプリケーションでは、アップグレードの開始前にレプリケーションが終了しなかった場合、デスティネーション Data Domain システム上でファイルが表示されません。アップグレードの後、レプリケーションが完了するまで待って、宛先システムでファイルを確認してください。

ConnectEMC のメモ

このリリースでは、Secure Remote Services VE（Secure Remote Service Virtual Edition）ゲートウェイをサポートするように ConnectEMC が変更されました。この変更では、アップグレード後に ConnectEMC への Data Domain システムの再構成が必要です。

注

ConnectEMC は Service Remote Services VE（V3）でのみ機能し、古いバージョンの Service Remote Services でもそれ自体でも E メールを送信できません。以前のリリースの DD OS（5.7、5.6 など）で ConnectEMC を使用している場合、Service Remote Services VE サーバ構成はテクノロジー アップグレードを理由にアップグレード プロセス中に削除されるため再入力する必要があります。

注

以前の Service Remote Services ゲートウェイを使用している場合は、安全な通信を実現するように Service Remote Services VE ゲートウェイを実装する必要があります。

アップグレード中に ConnectEMC が構成されていることを検出した場合、既存の構成は削除されます。さらに、サポート通知方法として ConnectEMC がイベント メッセージを送信するように構成されている場合は、E メールに切り替えられます。アップグレード後は、新しい ConnectEMC コマンドを使用して ConnectEMC を再構成できます。`support connectemc device register`。

ConnectEMC が構成された後で、`support notification method set connectemc` を使用して ConnectEMC を有効化します。

アップグレード パッケージの削除

最大 5 つのアップグレード パッケージは、DD System Manager を使用してシステムにアップロードされます。アップグレード中のシステムに 5 つのアップグレード パッケージが含まれている場合、そのシステムをアップグレードする前に 1 つ以上のパッケージを削除する必要があります。

手順

1. ［**Maintenance**］ > ［**System**］を選択します。
2. ［Upgrade Packages Available on this Data Domain System］というリストで、削除するパッケージを選択します。一度に削除できるパッケージは 1 つのみです。
3. ［**Remove Upgrade Package**］をクリックします。

電子ライセンスの管理

Data Domain システムで電子ライセンスの追加と削除を行います。製品の機能、ソフトウェア アップデート、ソフトウェア互換性ガイドの最新情報、および製品、ライセンス、サービスについては、該当する「Data Domain Operating System リリース ノート」を参照してください。

HA システムのライセンス管理

HA はライセンスされた機能であり、システム ライセンス キーを登録する方法は、他のライセンスを DD システムに追加する方法と同じです。

システムはアクティブ/スタンバイとして構成され、ここでノードの 1 つが「スタンバイ」と指定されます。各ノードに個別のライセンスが必要なのではなく、1 組のライセンスだけが必要になります。フェイルオーバー時には、一方のノードのライセンスが他のノードにフェイルオーバーします。

システム ストレージの管理

システム ストレージ管理機能を使用すると、ストレージ領域のステータスと構成の確認、ディスクの識別を容易にするためのディスク LED の点滅、ストレージ構成の変更を行うことができます。

注

2 ノードのアクティブ/スタンバイ HA システムで接続または使用されているすべてのストレージを、単一システムとして表示できます。

CLI を使用した、使用可能なストレージ領域の計算

RAID オーバーヘッドを考慮した、Data Domain システムで使用可能なストレージを計算するには、以下の値が必要です。

- N=dg（ディスク グループ）で使用されているディスクの数。
- C=フォーマット後の各ディスクの容量。
- R=2（RAID 6 パリティに使用されるディスクの数）

キャッシュ階層ディスクは RAID で保護されていないため、この計算はキャッシュ階層ストレージでは機能しません。

`storage show all` コマンドを実行して N および C の値を取得します。

図 4 `storage show all` コマンドの例

```
sysadmin@ddbeta90# storage show all
Active tier details:
Disk       Disks       Count   Disk       Additional
Group                          Size       Information
-------    --------    -----   --------   -----------
dg2        2.1-2.14    14      2.7 TiB
(spare)    2.15        1       2.7 TiB
-------    --------    -----   --------   -----------

Current active tier size: 32.7 TiB
Active tier maximum capacity: 131.0 TiB
```

この例では、dg2 で使用されている 14 個のディスクがあり、各ディスクの容量は 2.7 TiB であるため、N=14、C=2.7 TiB です。

有効容量を得るには、式(N-R) x C を使います。この例では、方程式は(14-2) x 2.7 TiB です。

12 x 2.7 TiB = 32.4 TiB、つまり 35.6 TB です。

注

計算値は、表示のために容量値が丸められる方法により、`storage show all` コマンドの出力と正確に一致しない場合があります。`disk show hardware` コマンドは、小数点以下の桁数を追加してディスク容量を表示します。

システム ストレージ情報の表示

［Storage Status］領域には、［Operational］、［Non-operational］など、ストレージの現在のステータスとストレージの移行ステータスが表示されます。［Status］領域の下には、ストレージ インベントリーがどのように表示されるかを示すタブがあります。

手順

1. ストレージのステータスを表示するには、［**Hardware**］ > ［**Storage**］を選択します。
2. ストレージのステータスの後にアラートのリンクが表示される場合は、そのリンクをクリックするとストレージのアラートが表示されます。
3. ［Storage Migration Status］が［Not licensed］の場合、［**Add License**］をクリックしてこの機能のライセンスを追加できます。

［Overview］タブ

［Overview］タブには、Data Domain システム内の全ディスクの情報が、タイプ別にまとめて表示されます。表示されるカテゴリーは、使用中のストレージ構成のタイプによって異なります。

［Overview］タブには、以下の 1 つ以上のセクションで検出されたストレージがリストされます。

- アクティブ階層
  アクティブ階層のディスクは、現在ファイル システムによって利用可能とマークされています。ディスクは［Disks in Use］と［Disks Not in Use］の 2 つのタブにリストされます。
- 保存階層
  オプションの Data Domain Extended Retention（旧 DD Archiver）ライセンスがインストールされた場合、このセクションには DD Extended Retention ストレージ用に構成されたディスクが表示されます。ディスクは［Disks in Use］と［Disks Not in Use］の 2 つのタブにリストされます。
- キャッシュ階層
  キャッシュ階層の SSD は、メタデータのキャッシュに使用されます。SSD は、ファイル システムで使用できません。ディスクは［Disks in Use］と［Disks Not in Use］の 2 つのタブにリストされます。
- クラウド階層
  クラウド階層のディスクは、クラウド ストレージに存在するデータのメタデータを格納するために使用されます。ディスクは、ファイル システムで使用できません。ディスクは［Disks in Use］と［Disks Not in Use］の 2 つのタブにリストされます。
- 追加可能ストレージ
  オプションのエンクロージャがあるシステムの場合、このセクションには、システムに追加できるディスクとエンクロージャが表示されます。
- Failed/Foreign/Absent ディスク（システム ディスクを除く）
  失敗状態のディスクを表示します。これらは、システムの Active 階層や Retention 階層には追加できません。
- システム ディスク
  Data Domain コントローラにデータ ストレージ ディスクが含まれない場合、DD OS があるディスクが表示されます。

- 移行履歴
  移行の履歴を表示します。

各セクション見出しには、そのセクション用に構成されたストレージのサマリーが表示されます。サマリーには、ディスク、使用中のディスク、スペア ディスク、再構築中のスペア ディスク、使用可能なディスク、既知のディスクの総数の集計が表示されます。

セクションのプラス（+）ボタンをクリックして詳細情報を表示するか、マイナス（-）ボタンをクリックして詳細情報を非表示にします。

表 24 ［Disks In Use］列ラベルの説明

項目	説明
Disk Group	ファイル システム（dg1 など）によって作成されたディスク グループの名前。
State	ディスクのステータス（Normal、Warning など）。
Disks Reconstructing	再構成しているディスク（ディスク ID（1.11 など））。
Total Disks	使用可能なディスクの総数（14 など）。
Disks	使用可能なディスクのディスク ID（2.1～2.14 など）。
Size	ディスク グループのサイズ（25.47 TiB など）。

表 25 ［Disks Not In Use］列ラベルの説明

項目	説明
Disk	ディスクの識別子は次のいずれかを指定できます。 • エンクロージャおよびディスク番号（Enclosure.Slot 形式）。 • DD VTL と vDisk などで使用される論理デバイスのデバイス番号。 • LUN
スロット	ディスクが存在するエンクロージャ
パック	ディスクが存在するエンクロージャ内のディスク パック（1～4）。DS60 拡張シェルフの場合、この値は 2～4 のみです。
State	ディスクのステータス（In Use、Available、Spare など）。
Size	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]
Type	ディスクの接続およびタイプ（SAS など）。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

［Enclosure］タブ

［Enclosures］タブには、システムに接続されたエンクロージャの詳細をまとめたテーブルが表示されます。

［Enclosures］タブには、次の詳細が表示されます。

表 26 ［Enclosures］タブの列ラベルの説明

項目	説明
エンクロージャ	エンクロージャ番号。エンクロージャ 1 はヘッド ユニットです。
シリアル番号	エンクロージャ シリアル番号。
ディスク	エンクロージャに含まれるディスク。形式は<エンクロージャ番号>.1-<エンクロージャ番号>.<N>。
モデル	エンクロージャ モデル。エンクロージャ 1 の場合、モデルはヘッド ユニットです。
Disk Count	エンクロージャのディスクの数。
ディスク サイズ	Data Domain システムで使用する際のディスクのデータ ストレージ容量。[a]
障害発生ディスク	エンクロージャ内の障害が発生したディスク。
温度ステータス	エンクロージャの温度ステータス。

a. ディスク スペースの計算の Data Domain 規則は、メーカーの評価とは異なるディスク容量を与え、1 ギビバイトを 230 バイトとして定義します。

［Disks］タブ

［Disks］タブには、各システム ディスクに関する情報が表示されます。ディスクのビューをフィルターして、すべてのディスク、特定の階層のディスク、特定のグループのディスクを表示できます。

［Disk State］テーブルには、すべてのシステム ディスクの状態が表示されるサマリー ステータス テーブルが表示されます。

表 27 ［Disks State］テーブルの列ラベルの説明

項目	説明
Total	Data Domain システム内のインベントリされたディスクの総数。
使用中	ファイル システムによって現在使用中のディスクの数。
Spare	スペア ディスクの数（障害が発生したディスクの交換に使用可能）。
Spare (reconstructing)	データ再構築中のディスク（障害が発生したディスクの交換に使用されているスペア ディスク）の数。
Available	Active または DD Extended Retention ストレージ階層への割り当てに使用可能なディスクの数。
Known	既知の未割り当てディスクの数。
Unknown	未知の未割り当てディスクの数。
Failed	Failed ディスクの数。
Foreign	Foreign ディスクの数。
なし	Absent ディスクの数。
マイグレーション中	ストレージ移行のソースとして機能するディスクの数。
ターゲット	ストレージ移行のターゲットとして機能するディスクの数。
電源オフ	電源がオンになっていないディスクの数。

表 27 ［Disks State］テーブルの列ラベルの説明 （続き）

項目	説明
Not Installed	システムが検出できる空のディスク スロットの数。

［Disks］テーブルには、システムにインストールされている各ディスクに関する情報が表示されます。

表 28 ［Disks］テーブルの列ラベルの説明

項目	説明
Disk	ディスク識別子。次のいずれかです。 • エンクロージャおよびディスク番号（形式は［Enclosure.Slot］）。 • DD VTL や vDisk などで使用される論理デバイスのデバイス番号。 • LUN
Size	ディスクのサイズ。
Slot	ディスクが存在するエンクロージャ
パック	ディスクが存在するエンクロージャ内のディスク パック（1～4）。DS60 拡張シェルフの場合、この値は 2～4 のみです。
State	ディスクのステータス。次のいずれかです。 • Absent。示された場所にはディスクがインストールされていません。 • Available。利用可能なディスクがアクティブ階層または保存階層に割り当てられていますが、現在は使用されていません。 • Copy Recovery。ディスクはエラー率が高いですが、障害は発生していません。現在、RAID によりスペア ドライブにコンテンツがコピーされています。コピーの再構築が完了するとドライブ障害となります。 • Destination。ディスクは、ストレージ移行のターゲットとして使用されています。 • Error。ディスクはエラー率が高いですが、障害は発生していません。ディスクはコピーの再構築のためにキューに入っています。この状態は、コピーの再構築が始まると「Copy Recovery」に変わります。 • Foreign。ディスクは階層に割り当てられていますが、ディスクが他のシステムによって所有されている可能性がディスク データに示されています。 • In-Use。ディスクはバックアップ データ ストレージに使用されています。 • Known。ディスクは割り当ての準備ができているサポート対象ディスクです。 • Migrating。ディスクは、ストレージ移行のソースとして使用されています。 • Powered Off。ディスクの電源がサポートによって取り外されています。

表 28 ［Disks］テーブルの列ラベルの説明 （続き）

項目	説明
	• Reconstruction。ディスクは、`disk fail` コマンドに応じて、または RAID/SSM からの指示によって再構築されています。 • Spare。ディスクはスペアとして使用可能です。 • System。システム ディスクには、DD OS およびシステム データが格納されます。バックアップ データは、システム ディスクには格納されません。 • Unknown。不明ディスクは、アクティブ階層または保存階層には割り当てられません。管理者または RAID システムによって障害とされている可能性があります。
Manufacturer/Model	メーカー モデル指定。ストレージ アレイが送信するベンダー文字列によっては、モデル ID、RAID タイプなどの情報が表示されることもある。
Firmware	サード パーティ物理ディスク ストレージ コントローラーが使用するファームウェア レベル。
Serial Number	メーカーのディスクのシリアル番号。
Disk Life Used	SSD の定格寿命の消費率。
Type	ディスクの接続およびタイプ（SAS など）。

［Reconstruction］タブ

［Reconstruction］タブには、再構築中のディスクに関する追加情報を提供するテーブルが表示されます。

次の表では、［Reconstructing］テーブルのエントリーについて説明します。

表 29 ［Reconstruction］テーブルの列ラベルの説明

項目	説明
Disk	再構築中のディスクが識別されます。ディスクのラベルは、［enclosure.disk］の形式です。エンクロージャ 1 は Data Domain システム、外部シェルフはエンクロージャ 2 でナンバリングを開始します。たとえば、ラベル 3.4 は、2 番目のシェルフの 4 番目のディスクです。
Disk Group	再構築中のディスクの RAID グループ（dg#）が表示されます。
Tier	障害が発生したディスクが再構築中の階層の名前。
残り時間	再構築が完了するまでの時間。
進捗状況	完了した再構築の割合。

スペア ディスクが使用可能な場合、ファイル システムが自動的に障害が発生したディスクをスペアに交換し、スペアを RAID ディスク グループに統合する再構築プロセスを開始します。そのディスク使用は「`Spare`」と表示され、ステータスは「`Reconstructing`」になります。再構築は一度に 1 つのディスクに対してしか実行できません。

エンクロージャの物理的配置

DD System Manager に表示されているエンクロージャに対応している物理エンクロージャの特定が難しい場合は、CLI ビーコン機能を使用して、正常な動作を示すエンクロージャ IDENT LED とすべてのディスクの LED を点滅させることができます。

手順

1. システムで CLI セッションを確立します。
2. 「`enclosure beacon` **enclosure**」と入力します。
3. LED の点滅を停止するには、**ctrl+c** を押します。

ディスクの物理的な場所の確認

DD System Manager に表示されているディスクに対応している物理ディスクの特定に苦労している場合は、ビーコン機能を使用して物理ディスクの LED を点滅させることができます。

手順

1. ［**Hardware**］ > ［**Storage**］ > ［**Disks**］を選択します。
2. ［**Disks**］テーブルからディスクを選択し、［**Beacon**］をクリックします。

   注

   一度に選択できるディスクは 1 つのみです。

   ［Beaconing Disk］ダイアログ ウィンドウが表示され、ディスクの LED ライトが点滅し始めます。
3. ［**Stop**］をクリックすると、LED の点滅が停止します。

ストレージの構成

ストレージの構成機能を使用すると、アクティブ階層、保存階層、クラウド階層でストレージ拡張エンクロージャの追加および削除ができます。拡張エンクロージャにあるストレージ（拡張シェルフと呼ばれることもある）は、階層に追加されるまで使用できません。

注

ストレージを追加するには、1 つまたは複数の適切なライセンスおよび新しいストレージ容量をサポートするための十分なメモリが必要です。ライセンスまたはメモリがさらに必要な場合は、エラー メッセージが表示されます。

DD6300 システムでは、使用可能なライセンス容量が正確に 21.8 TiB の場合、アクティブ階層で ES30 エンクロージャの 4 TB ドライブ（43.6 TiB）を使用率 50%（21.8 TiB）で使用するオプションをサポートします。部分容量シェルフを使用する場合は、次のガイドラインが適用されます。

- 部分容量を使用するための他のエンクロージャ タイプまたはドライブ サイズはサポートされません。
- 部分容量シェルフは、アクティブ階層にのみ存在できます。
- 部分容量 ES30 は、アクティブ階層に 1 つのみ存在できます。
- 部分容量シェルフが階層に存在する場合、そのシェルフが全容量で追加されるまで別の ES30 を構成することはできません。

注

その場合、部分容量シェルフの残りの 21.8 TiB を使用するには、十分な追加容量のライセンスが必要です。

- 使用可能な容量が 21.8 TB を超えている場合は、部分容量シェルフを追加することはできません。
- 21 TiB ライセンスを削除しても、全容量シェルフは部分容量シェルフに自動的に変換されません。いったんシェルフを取り外してから部分容量シェルフとして追加する必要があります。

手順

1. ［**Hardware**］ > ［**Storage**］ > ［**Overview**］を選択します。
2. いずれかの使用可能ストレージ階層のダイアログ ボックスを展開します。
   - ［アクティブ階層］
   - ［長期保存階層］
   - ［キャッシュ階層］
   - ［クラウド階層］
3. ［**Configure**］をクリックします。
4. ［Configure Storage］ダイアログで、［**Available Storage**］リストから追加するストレージを選択します。
5. ［**Configure**］リストから、［**Active Tier**］または［**Retention Tier**］を選択します。

   アクティブ階層に追加できるストレージの最大容量は、使用される DD コントローラーによって異なります。

   注

   ライセンスされた容量のバーには、インストールされたエンクロージャにライセンスされた容量（使用済みと未使用）の割り当てが表示されます。
6. 追加するシェルフのチェックボックスを選択します。
7. ［**Add to Tier**］ボタンをクリックします。
8. ［**OK**］をクリックして、ストレージを追加します。

   注

   追加したシェルフを削除するには、それを［Tier Configuration］リストからクリックし、［**Remove from Configuration**］、［**OK**］を順にクリックします。

DD3300 容量拡張

DD3300 システムは 3 通りの異なる容量構成で利用可能です。ある構成から別の構成への容量拡張がサポートされています。

DD3300 システムは次の容量構成で利用可能です。

- 4 TB
- 8 TB
- 16 TB

- 32 TB

アップグレードに関して次の考慮事項があります。

- 4 TB のシステムは 16 TB までアップグレードできます。
- 8 TB は 16 TB にアップグレードでき、16 TB から 32 TB にアップグレードできます。
- 16 TB のシステムは 32 TB までアップグレードできます。
- 4 TB から 32 TB へのアップグレード パスはありません。

［**Maintenance**］ > ［**System**］を選択して容量拡張に関する情報にアクセスし、容量拡張プロセスを開始します。

容量拡張は、1 回限りのプロセスです。［**Capacity Expansion History**］パネルには、システムがすでに拡張されているかどうかが表示されます。システムがまだ拡張されていない場合は、［**Capacity Expand**］ボタンをクリックして容量の拡張を開始します。

すべての容量拡張では、システムに追加ディスクとメモリの取り付けが必要です。ハードウェア アップグレードが完了するまで容量を拡張しないでください。以下の表は、容量拡張のハードウェア アップグレード要件を示します。

表 30 容量拡張のための DD3300 アップグレード要件

容量拡張	追加のメモリ	追加の HDD	追加の SSD
4～16 TB	32 GB	6 x 4 TB HDD	1 x 480 GB SSD
8～16 TB	8 TB から 16 TB への拡張には、ライセンスと構成の変更のみが必要です。ハードウェア アップグレードは不要です。		
16～32 TB	16 GB	6 x 4 TB HDD	N/A

「Data Domain DD3300 Field Replacement and Upgrade Guide」に、システム容量を拡張するための詳細な手順が記載されています。

容量拡張

［**Select Capacity**］ドロップダウン リストからターゲット容量を選択します。容量拡張は、メモリの不足、物理容量（HDD）の不足、システムを拡張済み、または容量拡張のターゲットがサポートされていないために実施できないことがあります。容量の拡張を完了できない場合は、ここに理由が表示されます。

容量拡張履歴

［**Capactiy Expansion History**］表には、システムの容量に関する詳細が表示されます。この表には、ソフトウェアを初めてインストールしたときのシステムの容量、ソフトウェアを最初にインストールした日付が表示されます。容量が拡張された場合、この表には、拡張された容量と拡張が実施された日付も表示されます。

ディスクの障害と障害解除

ディスク障害機能を使用すると、ディスクを手動で障害状態に設定して、ディスクに格納されたデータを強制的に再構築できます。ディスク障害解除機能を使用すると、障害状態のディスクを稼動状態に戻すことができます。

ディスクの障害

ディスクおよび強制再構成が失敗します。［**Hardware**］ > ［**Storage**］ > ［**Disks**］ > ［**Fail**］を選択します。

テーブルからディスクを選択し、［**Fail**］をクリックします。

ディスクの障害解除

Failed または Foreign とマークされたディスクをシステムで使用可能にします。
［**Hardware**］ > ［**Storage**］ > ［**Disks**］ > ［**Unfail**］を選択します。

テーブルからディスクを選択し、［**Unfail**］をクリックします。

ネットワーク接続の管理

ネットワーク接続管理機能を使用すると、ネットワーク インターフェイス、全般的なネットワークの設定、ネットワーク ルートの表示および構成ができます。

HA システムのネットワーク接続管理

HA システムは、2 種類の IP アドレス（固定アドレスとフローティング アドレス）に依存します。各タイプには、特定の動作と制限事項があります。

HA システムでは、固定 IP アドレスには次のような特徴があります。

- CLI によるノード管理に使用する
- ノードに添付（「固定」）されている
- 静的アドレスにすることも、DHCP、IPv6 SLAAC にすることもできる
- オプションの `type fixed` 引数を設定すると、特定のノードで構成が実行される

注

ファイル システム アクセスはすべて、フローティング IP 経由で行う必要があります。

フローティング IP アドレスは、2 ノード HA システムにのみ存在します。フェイルオーバー時には、IP アドレスが新しいアクティブ ノードに「フロート」します。フローティング アドレスには次のような特徴があります。

- アクティブ ノードでのみ構成される
- ファイル システムへのアクセスと、ほとんどの構成に使用される
- 静的アドレスにのみすることができる
- 構成には `type floating` 引数が必要である

ネットワーク インターフェイスの管理

ネットワーク インターフェイス管理機能を使用すると、システムをネットワークに接続する物理インターフェイスを管理し、リンク統合、ロード バランシング、リンクまたはノードのフェイルオーバーをサポートする論理インターフェイスを作成できます。

インターフェイス情報の表示

［Interfaces］タブでは、物理インターフェイスと仮想インターフェイス、VLAN、DHCP、DDNS、IP アドレスとエイリアスを管理できます。

IPv6 インターフェイスを管理する際には、次のガイドラインを考慮してください。

- CLI（コマン ドラインインターフェイス）は、基本 Data Domain ネットワークおよびレプリケーションコマンドの IPv6 に対応していますが、バックアップおよび DD Extended Retention（`archive`）コマンドについては対応していません。CLI コマンドは IPv6 アドレスを管理します。DD System Manager を使用して IPv6 アドレスを表示できますが、DD System Manager で IPv6 は管理できません。
- コレクション、ディレクトリ、および Mtree レプリケーションは、IPv6 アドレス スペースを活用できる IPv6 ネットワークで対応しています。DD Boost を使用した Managed File Replication と同様に、IPv6 および IPv4 ネットワークを通した同時レプリケーションにも対応しています。
- IPv6 アドレスのインターフェイスにはいくつかの制限があります。たとえば、最小 MTU は 1280 です。IPv6 アドレスを使用したインターフェイスで 1280 未満の MTU を設定しようとすると、エラー メッセージが表示され、そのインターフェイスがサービスから削除されます。IPv6 アドレスはインターフェイスにアタッチされた VLAN に上にあり、直接インターフェイス上にあるわけではありませんが、インターフェイスに影響する可能性があります。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。

   次の表は、［Interfaces］タブ上の情報の説明を示しています。

   表 31 ［Interfaces］タブのラベルの説明

項目	説明
仮想マトリックス	選択したシステムに関連づけられた各インターフェイスの名前。
Enabled	そのインターフェイスが有効かどうか。 • インターフェイスを有効化してネットワークに接続するには、［**Yes**］選択します。 • インターフェイスを無効化してネットワークから切断するには、［**No**］を選択します。
DHCP	インターフェイスが手動（`no`）、DHCP（動的ホスト構成プロトコル）IPv4 サーバー（`v4`）、または DHCP IPv6 サーバー（`v6`）のどれで構成されているかを示します。
IP アドレス	インターフェイスに関連づけられた IP アドレス。インターフェイスを識別するためにネットワークによって使用されるアドレス。インターフェイスが DHCP を通じて構成されている場合、この値の後にアスタリスクが表示される。
ネットマスク	インターフェイスに関連づけられたネットマスク。標準的な IP ネットワーク マスク形式が使用される。インターフェイスが DHCP を通じて構成されている場合、この値の後にアスタリスクが表示される。
リンク	Ethernet 接続がアクティブかどうか（Yes/No）。
アドレス タイプ	HA システムでは、アドレス タイプには Fixed、Floating、Interconnect のいずれかが示されます。
Additional Info	インターフェイスの追加設定。結合モードなど。

表 31 ［Interfaces］タブのラベルの説明 （続き）

項目	説明
IPMI interfaces configured	［Yes］または［No］で表示され、IPMI 稼働状態モニタリングおよび電源管理がインターフェイスに対して構成されているかどうかが示されます。

2. インターフェイス リストをインターフェイス名でフィルタリングする場合は、［**Interface Name**］フィールドに値を入力して、［**Update**］をクリックします。

   フィルターは、eth*、veth*、eth0*などのワイルドカードに対応しています。

3. インターフェイス リストをインターフェイス タイプでフィルタリングする場合は、［**Interface Type**］メニューから値を選択して、［**Update**］をクリックします。

   HA システムには、IP アドレスのタイプ（Fixed、Floating、Interconnect） でフィルタ リングするフィルタ ドロップダウン メニューがあります。

4. インターフェイス テーブルをデフォルト リスティングに戻すには、［**Reset**］をクリックします。
5. ［Interface Details］領域に記入するテーブル内のインターフェイスを選択します。

表 32 ［Interface Details］のラベルの説明

項目	説明
Auto-generated Addresses	選択したインターフェイスの自動生成された IPv6 アドレスを表示します。
Auto Negotiate	この機能が `Enabled` と表示されている場合、インターフェイスは自動的に速度と重複設定をネゴシエートします。この機能が `Disabled` と表示されている場合、速度と重複値を手動で設定する必要があります。
ケーブル	インターフェイスが Copper と Fiber のどちらかを示します。 注 ケーブル ステータスを有効にするには、起動状態にする必要があるインターフェイスもあります。
二重モード	データ転送プロトコルを設定するため、Speed 値と合わせて使用されます。オプションは、Unknown、Full、Half です。
Hardware Address	選択したインターフェイスの MAC アドレス。00:02:b3:b0:8a:d2 など。
Interface Name	選択したインターフェイスの名前。
Latent Fault Detection (LFD) - HA systems only	［LFD］フィールドには `View Configuration` リンクがあり、LFD アドレスとインターフェイスをリストしたポップアップを表示します。
Maximum Transfer Unit (MTU)	インターフェイスに割り当てられる MTU（最大転送単位）の値。
Speed	データ転送率を設定するため、Duplex 値と合わせて使用されます。オプションは、Unknown、10 Mb/s、100 Mb/s、1000 Mb/s、10 Gb/s です。

表 32 ［Interface Details］のラベルの説明 （続き）

項目	説明
	注 速度、二重、対応速度を表示するには、自動ネゴシエートされたインターフェイスをセットアップする必要があります。
Supported Speeds	インターフェイスが使用できるすべての速度をリストします。

6. IPMI インターフェイスの構成および管理オプションを表示するには、［**View IPMI Interfaces**］をクリックします。

   このリンクには、［**Maintenance**］ > ［**IPMI**］の情報が表示されます。

物理インターフェイスの名前と制限

物理インターフェイス名の形式は、Data Domain システムおよびオプション カードによって異なり、一部のインターフェイスには制限が適用されます。

- 多くのシステムで、物理インターフェイス名形式は `eth`**xy** となり、**x** はオンボード ポートまたはオプション ポートのスロット番号であり、**y** は英数字の文字列です。たとえば、**eth0a** です。
- 多くのオンボード NIC 垂直インターフェイスで、上のインターフェイスの名前は **eth0a** であり、下のインターフェイスは **eth0b** です。
- 多くのオンボード NIC 水平インターフェイスで、後ろから見て左のインターフェイスの名前は **eth0a** であり、右のインターフェイスは **eth0b** です。
- DD990 システムには、上に 2 個、下に 2 個、計 4 個のオンボード インターフェイスがあります。左上インターフェイスは **eth0a**、右上は **eth0b**、左下は **eth0c**、右下は **eth0d** です。
- DD2200 システムには、4 個のオンボード 1G Base-T NIC ポート： ethMa（左上）、ethMb（右上）、ethMc（左下）、ethMd（右下）があります。
- DD2500 システムには、6 個のオンボード インターフェイスがあります。4 個のオンボード 1G Base-T NIC ポートは、ethMa（左上）、ethMb（右上）、ethMc（左下）、ethMd（右下）です。2 個のオンボード 10G Base-T NIC ポートは、ethMe（上）と ethMf（下）です。
- DD4200、DD4500、DD7200 システムには、1 個のオンボード Ethernet ポート（ethMa）があります。
- DD140 から DD990 の間のシステムの場合、I/O モジュールの物理インターフェイス名はモジュールの先頭または左側から始まります。最初のインターフェイスは **ethxa**、次は **ethxb**、次は **ethxc** となります。
- 水平 DD2500 I/O モジュールのポート番号は、モジュール ハンドル（左側）の反対の端から順にラベル付けされます。最初のポートのラベルは 0 で、物理インターフェイス名 **ethxa** に対応し、次は **1/ethxb**、次は **2/ethxc** となります。
- 垂直 DD4200、DD4500、DD7200 I/O モジュールのポート番号は、モジュール ハンドル（下）の反対の端から順にラベル付けされます。最初のポートのラベルは 0 で、物理インターフェイス名 **ethxa** に対応し、次は **1/ethxb**、次は **2/ethxc** となります。

一般インターフェイス構成ガイドライン

システム インターフェイスを構成する前に、一般インターフェイスの構成ガイドラインを確認します。

- バックアップおよびレプリケーション トラフィック両方に対応する場合は、どちらのトラフィック タイプも他方に影響しないようにするため、各トラフィック タイプに異なるインターフェイスを使用することを推奨します。
- 10 GbE インターフェイスは高速トラフィックに最適化されているため、レプリケーション タイプが 1 Gb/s 未満になると予想される場合は、レプリケーション トラフィックの 10 GbE インターフェイスを使用することは推奨されません。
- Data Domain サービスが標準以外のポートを使用しており、ユーザーが DD OS6.0 にアップグレードするか、またはユーザーが DD OS 6.0 システムで標準以外のポートを使用するためにサービスを変更する場合、そのサービスを使用するすべてのクライアントに対してネット フィルターを追加して、クライアント IP アドレスが新しいポートを使用するようにします。
- IPMI を使用する DD4200、DD4500、DD7200 システムでは、（HTTP、Telnet、SSH などのプロトコルを使用した）インターフェイス ethMa を IPMI トラフィックとシステム管理トラフィック用に確保することを推奨します。バックアップ データ トラフィックは、他のインターフェイスに送信する必要があります。

物理インターフェイスの構成

システムをネットワークに接続する前に、すくなくとも 1 つの物理インターフェイスを構成する必要があります。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. 構成するインターフェイスを選択します。

   注

   DD140、DD160、DD610、DD620、および DD630 システムは、インターフェイス eth0a（レガシー ポート名を使用するシステムでは eth0）上、または同じインターフェイスで作成された VLAN 上の IPv6 には対応していません。

3. ［**Configure**］をクリックします。
4. ［Configure Interface］ダイアログで、インターフェイス IP アドレスの設定方法が定義されます。

   注

   HA システムでは、［Configure Interface］ダイアログに、フローティング IP を指定するかどうか（Yes/No）のフィールドがあります。［**Yes**］を選択すると、`Manually Configure IP Address` ラジオ ボタンが自動で選択されます。フローティング IP インターフェイスは手動でのみ構成できます。

   - Use DHCP to assign the IP address：［IP Settings］領域で、［**Obtain IP Address using DHCP**］を選択し、IPv4 アクセスの場合［**DHCPv4**］、IPv6 アクセスの場合［**DHCPv6**］を選択します。
     物理インターフェイスが自動的に DHCP を使用するように設定すると、インターフェイスが有効化されます。

注

DHCP を通してネットワーク設定を取得する場合、［**Hardware**］ > ［**Ethernet**］ > ［**Settings**］または `net set hostname` コマンドでホスト名を手動で構成できます。IPv6 を介して DHCP を使用する場合、ホスト名を手動で構成する必要があります。

- Specify IP Settings manually：［IP Settings］領域で、［**Manually configure IP Address**］を選択します。
  ［**IP Address**］および［**Netmask**］フィールドがアクティブになります。

5. IP アドレスを手動で入力することを選択した場合は、IPv4 または IPv6 アドレスを入力します。IPv4 アドレスを入力した場合、ネットマスク アドレスを入力します。

注

この手順では、インターフェイスに割り当てることができる IP アドレスは 1 件のみです。他の IP アドレスを割り当てた場合、新しいアドレスが古いアドレスに取って代わります。追加 IP アドレスをインターフェイスにアタッチするには、IP エイリアスを作成します。

6. Speed/Duplex 設定を指定します。

   速度および二重通信モード設定の組み合わせにより、インターフェイスを介したデータ転送の速度が決定されます。次のいずれかのオプションを選択します。

   - ［**Autonegotiate Speed/Duplex**］：カードによるインターフェイスの回線速度と二重通信モードの設定の自動ネゴシエーションを可能にする場合、このオプションを選択します。自動ネゴシエーションは、次の DD2500、DD4200、DDD4500、DDD7200 I/O モジュールでは［サポートされていません］。
     - LC コネクタ付き Dual Port 10GbE SR Optical（SFP 使用）
     - Dual Port 10GbE Direct Attach Copper（SFP ＋ケーブル）
     - Quad port 2 port 1GbE Copper（RJ45）/2 port 1GbE SR Optical
   - ［**Manually configure Speed/Duplex**］：インターフェイス データ転送速度を手動で設定するには、このオプションを選択します。メニューから、速度および二重を選択します。
     - 二重通信モードのオプションは、半二重、全二重、不明です。
     - 表示される速度オプションは、ハードウェア デバイスの性能に制限されます。オプションは、10 Mb、100 Mb、1000 Mb（1 Gb）、10 Gb、不明です。10G Base-T ハードウェアは、100 Mb、1000 Mb、10 Gb 設定にのみ対応しています。
     - 半二重は、10 Mb と 100 Mb の速度のみで使用できます。
     - 1000 Mb および 10 Gb の回線速度では全二重が必要です。
     - DD2500、DD4200、DD4500、DD7200 10GbE I/O モジュールでは、銅線インターフェイスは 10 Gb 速度の設定にのみ対応しています。
     - 10G Base-T インターフェイスのデフォルト設定は、Autonegotiate Speed/Duplex です。手動で速度を 1000 Mb または 10 Gb に設定した場合、Duplex 設定を Full に設定する必要があります。

7. 物理（Ethernet）インターフェイスに対して、MTU（最大転送単位）のサイズを指定します。

   次の操作を実行します。

- 設定をデフォルト値に戻すには、［**Default**］ボタンをクリックします。
- 使用しているネットワーク コンポーネントのすべてが、このオプションを使用したサイズ セットをサポートしているか確認してください。

8. オプションで［**Dynamic DNS Registration**］を選択します。

   DDNS（動的 DNS）は、DNS（ドメイン ネーム システム）サーバーでローカル IP アドレスを登録するプロトコルです。このリリースでは、DD System Manager は Windows モード DDNS に対応しています。UNIX モード DDNS を使用するには、`net ddns` CLI コマンドを使用します。

   このオプションを有効にするには、DDNS を登録する必要があります。

   注

   このオプションを選択すると、このインターフェイスで DHCP が無効化されます。

9. ［次へ］をクリックします。

   ［Configure Interface Settings］サマリー ページが表示されます。表示される値には新しいシステムとインターフェイスの状態が反映され、［Finish］をクリックしたときに適用されます。

10. ［**Finish**］と［**OK**］をクリックします。

MTU サイズ値

MTU サイズは、ネットワーク接続のパフォーマンスを最適化するために正しく設定する必要があります。MTU サイズが正しくないとインターフェイスのパフォーマンスに悪影響を及ぼす可能性があります。

物理（Ethernet）インターフェイスに対して、MTU（最大転送単位）のサイズを指定します。サポートされる値は 350～9000 です。100 Base-T およびギガビット ネットワークの場合は、1500 が標準のデフォルト値です。

注

IPv6 インタ フェースの最小 MTU は 1280 です。1280 より小さい MTU を設定するとインターフェイスが終了します。

固定 IP アドレスの移動

各固定 IP アドレスは、システム上の 1 個のインターフェイスにのみ割り当てる必要があります。固定 IP アドレスは、インターフェイスから正しく削除してから、他のインターフェイスに構成する必要があります。

手順

1. 固定 IP アドレスをホストするインターフェイスが DD Boost インターフェイス グループの一部である場合、インターフェイスをそのグループを削除します。
2. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
3. 移動したい固定 IP アドレスを削除します。
   a. 移動したい IP アドレスを使用しているインターフェイスを選択します。
   b. ［Enabled］列で、［**No**］を選択して、インターフェイスを無効化します。
   c. ［**Configure**］をクリックします。

d. [IP Address] を 0 に設定します。

> 注
>
> インターフェイスに割り当てる別の IP アドレスがない場合は、IP アドレスを 0 に設定します。複数のインターフェイスに同じ IP アドレスを割り当てることはできません。

e. [**Next**] をクリックし、[**Finish**] をクリックします。

4. 削除された固定 IP アドレスを他のインターフェイスに追加します。

a. IP アドレスを移動したいインターフェイスを選択します。

b. [Enabled] 列で、[**No**] を選択して、インターフェイスを無効化します。

c. [**Configure**] をクリックします。

d. 削除した固定 IP アドレスに一致する IP Address を設定します。

e. [**Next**] をクリックし、[**Finish**] をクリックします。

f. [Enabled] 列で、[**Yes**] を選択して、更新されたインターフェイスを有効化します。

仮想インターフェイス構成ガイドライン

仮想インターフェイスの構成ガイドラインは、フェイルオーバー インターフェイスと統合仮想インターフェイスに適用されます。両方には適用されませんが、フェイルオーバーまたは統合インターフェイスのいずれかに適用される追加のガイドラインも存在します。

- virtual-name は、`veth`**x** の形式である必要があります（**x** は数字です）。名前サイズ制限があるため、推奨最大数は 99 です。
- 物理インターフェイスの数と同じ数まで仮想インターフェイスも作成できます。
- 仮想インターフェイスで使用される各インターフェイスは、まず無効化する必要があります。仮想インターフェイスの一部であるインターフェイスは、その他のネットワーク構成オプションに対しては無効なものとして認識されます。
- 仮想インターフェイスが破棄されると、そのインターフェイスに関連づけられた物理インターフェイスも無効のままになります。物理インターフェイスを手動で再有効化する必要があります。
- インストールされているカードの数とタイプによって、使用可能な Ethernet ポートの数が決まります。
- 各物理インターフェイスは 1 つの仮想インターフェイスに属すことができます。
- 1 つのシステムで、前述の制限の対象となるフェイルオーバーおよび統合仮想インターフェイスの組み合わせを複数サポートできます。
- 仮想インターフェイスは、同一の物理インターフェイスから作成する必要があります。たとえば、すべて銅線、光メディア、1 Gb、10 Gb とします。ただし、1 Gb インターフェイスは銅線と光メディアインターフェイスの組み合わせの結合に対応しています。これは、Chelsio カードを除く、同一の物理インターフェイスを持つ複数のカード間の仮想インターフェイスに適用されます。Chelsio カードの場合、フェイルオーバーにのみ対応しており、それは同じカード上のインターフェイス間のみとなります。
- フェールオーバーおよび統合リンクによって、複数のネットワーク インターフェイスを並列して使用することでネットワーク パフォーマンスとリカバリ性が改善し、統合リンクのリンク速度と単一インターフェイスのリンク速度に対する信頼性が上がります。
- [**Configure**] ボタンを使用することで、削除機能を使用できます。[Interfaces] タブのインターフェイスのリストで仮想インターフェイスをクリックした後、[**Configure**] をクリックします。ダイアログ ボックスのインターフェイスのリストから、インターフェイスのチェックボックスをクリアして結合からそれを削除し（フェイルオーバーまたは統合）、[**Next**] をクリックします。

- 結合インターフェイスの場合、スレーブ インターフェイス用のハードウェアに障害が発生した場合は、残りのスレーブを使用して結合インターフェイスが作成されます。スレーブがない場合は、スレーブなしで結合インターフェイスが作成されます。このスレーブ ハードウェアの障害により、障害が発生したスレーブごとに 1 つの管理対象アラートが生成されます。

  注

  障害が発生したスレーブがシステムから削除されると、そのアラートは表示されなくなります。新しいハードウェアが設置されるとアラートは表示されなくなり、結合インターフェイスは再起動後に新しいスレーブ インターフェイスを使用します。

- DD3300、DD4200、DD4500、DD7200 システムでは、ethMa インターフェイスはフェールオーバーにもリンク統合にも対応していません。

リンク統合用の仮想インターフェイスの構成のガイドライン

リンク統合によって、1 つ以上のネットワーク インターフェイスを並列して使用することでネットワーク パフォーマンスとリカバリ性が改善し、リンク速度と単一インターフェイスのリンク速度に対する信頼性が上がります。これらのガイドラインにより、リンク統合の使用を最適化できます。

- 無効化された Ethernet インターフェイスへの変更は、ルーティング テーブルをフラッシュします。スケジュール設定された保守ダウンタイム中にのみインターフェイスを変更することを推奨します。その後、ルーティング ルールおよびゲートウェイを再構成します。
- 物理インターフェイスおよびモードを指定し、IP アドレスを付与することで、既存の仮想インターフェイス上で統合を有効化します。
- 10 Gb 単一ポート光学 Ethernet カードは、リンク統合に対応していません。
- 1 GbE インターフェイスと 10 GbE インターフェイスを一緒に統合することはできません。
- 銅線インターフェイスと光インターフェイスを一緒に統合することはできません。
- DD4200、DD4500、および DD7200 システムでは、ethMA インターフェイスはリンク統合に対応していません。

フェイルオーバー用の仮想インターフェイス構成のガイドライン

リンク フェイルオーバーは、プライマリ インターフェイスが動作していない場合にネットワーク トラフィックをサポートできるバックアップ インターフェイスを特定することで、ネットワークの安定性とパフォーマンスを向上させます。 これらのガイドラインにより、リンク フェイルオーバーの使用を最適化できます。

- プライマリ インターフェイスは、フェイルオーバーの一部である必要があります。プライマリ インターフェイスをフェイルオーバーから削除しようとすると、エラー メッセージが表示されます。
- プライマリ インターフェイスがフェイルオーバー構成に使用されている場合、それは明示的に指定し、仮想インターフェイスへの結合インターフェイスである必要があります。プライマリ インターフェイスがダウンし、複数のインターフェイスがまだ使用可能である場合、次のインターフェイスが無作為に選択されます。
- 仮想インターフェイス内のすべてのインターフェイスが、同じ物理ネットワークにある必要があります。仮想インターフェイスが使用するネットワーク スイッチが、同じ物理ネットワークにある必要があります。
- フェイルオーバー用の物理インターフェイスの推奨数は、2 以上です。ただし、次のものを除き、1 個のプライマリ インターフェイスを 1 個以上のフェイルオーバー インターフェイスを構成できます。
  - 同じカードからの 1 個のプライマリ インターフェイスと 1 個のフェイルオーバー インターフェイスに制限される 10 Gb CX4 Ethernet カード。

- 使用できない 10 Gb 単一ポート光学 Ethernet カード。

- DD4200、DD4500、および DD7200 システムでは、ethMA インターフェイスはリンク フェイルオーバーに対応していません。

仮想インターフェイスの作成

仮想インターフェイスを作成して、リンク統合またはフェイルオーバーをサポートします。仮想インターフェイスは、フェイルオーバー用に統合または関連づけられるリンクのコンテナーとして機能します。

リンク統合用の仮想インターフェイスの作成

統合に加わるリンクを関連づけるためのコンテナーとして機能する、リンク統合用の仮想インターフェイスを作成します。

リンク統合インターフェイスでは、リンクの結合モードを指定する必要があり、ハッシュ選択が必要な場合があります。たとえば、LACP（Link Aggregation Control Protocol）モードおよびハッシュ XOR-L2L3 を使用して、仮想インターフェイス（veth1）から物理インターフェイス（eth1 および eth2）に対するリンク統合を有効化することができます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. ［**Interfaces**］テーブルでは、［Enabled］列で［**No**］をクリックして仮想インターフェイスが追加される物理インターフェイスを無効化します。
3. ［**Create**］メニューから、［**Virtual Interface**］を選択します。
4. ［Create Virtual Interface］ダイアログで、［**veth**］ボックスに仮想インターフェイス名を指定します。

   仮想インターフェイス名を vethx の形式で入力します。x は一意の ID です（通常、1 または 2 桁）。VLAN および IP エイリアスを持つ通常の完全仮想インターフェイスであれば、veth56.3999:199 といった名前になります。完全名の最大長は 15 文字です。特殊文字は使えません。数字は 0～4094 の間でなくてはなりません。

5. ［**Bonding Type**］リストでは［**Aggregate**］を選択します。

   注

   レジストリ設定は、ボンディング構成とは異なる場合があります。仮想インターフェイスにインターフェイスを追加する場合、仮想インターフェイスに IP アドレスが付与され、起動されるまでボンディング モジュールには情報が送信されません。それまでの間、レジストリとボンディング ドライバ構成は異なっています。

6. ［**Mode**］リストでは、ボンディング モードを選択します。

   インターフェイスが直接接続されているシステムの要件と互換性のあるモードを指定してください。

   - ラウンド・ロビン
     統合されたグループ内で最初に利用可能なリンクから最後まで、シーケンシャルな順序でパケットを転送します。
   - Balanced
     選択したハッシュ法で決定されたインターフェイスを介してデータを送信します。これには、スイッチ上の関連づけられたインターフェイスの Ether チャネル（トランク）へのグループ化と Load Balance パラメーターを介したハッシュの付与が必要です。

- LACP
  Link Aggregation Control Protocol は、他方と通信する制御プロトコルを使用し、使用できるボンド内のリンクを調整する点を除き、Balanced と同じです。LACP は、一種のハートビート フェイルオーバーを提供し、リンクの両側で構成する必要があります。

7. Balanced または LACP モードを選択している場合、［**Hash**］リストでボンディング ハッシュ タイプを指定します。

   オプション: XOR-L2、XOR-L2L3、または XOR-L3L4.

   XOR-L2 は、レイヤー 2（インバウンドおよびアウトバウンド MAC アドレス）の XOR ハッシュのある結合インターフェイスを介して転送します。

   XOR-L2L3 は、レイヤー 2（インバウンドおよびアウトバウンド MAC アドレス）とレイヤー 3（インバウンドおよびアウトバウンド IP アドレス）の XOR ハッシュのある結合インターフェイスを介して転送します。

   XOR-L3L4 は、レイヤー 3（インバウンドおよびアウトバウンド IP アドレス）とレイヤー 4（インバウンドおよびアウトバウンド ポート）の XOR ハッシュのある結合インターフェイスを介して転送します。

8. 統合構成に追加するインターフェイスを選択するには、インターフェイスに対応するチェックボックスを選択し、［**Next**］をクリックします。

   ［Create virtual interface veth_name］ダイアログが表示されます。

9. IP アドレスを入力します。IP アドレスを指定しない場合は、0 と入力します。
10. ネットマスク アドレスまたはプレフィックスを入力します。
11. Speed/Duplex オプションを指定します。

    速度および二重通信モード設定の組み合わせにより、インターフェイスを介したデータ転送の速度が決定されます。次のいずれかを選択します。

    - ［**Autonegotiate Speed/Duplex**］
      このオプションを選択すると、ネットワーク インターフェイス カードによりインターフェイスの回線速度と二重通信モードの設定が自動ネゴシエーションされます。
    - ［**Manually configure Speed/Duplex**］
      インターフェイスのデータ転送速度を手動で設定するにはこのオプションを選択します。
      - 二重通信モードのオプションは、半二重または全二重です。
      - 表示される速度オプションは、ハードウェア デバイスの性能に制限されます。オプションは、10 Mb、100 Mb、1000 Mb、10 Gb です。
      - 半二重は、10 Mb と 100 Mb の速度のみで使用できます。
      - 1000 Mb および 10 Gb の回線速度では全二重が必要です。
      - 光インターフェイスでは［Autonegotiate］オプションが必要です。
      - 10 GbE 銅線 NIC のデフォルトは 10 Gb です。銅線インターフェイスの回線速度が 1000 Mb または 10 Gb に設定されている場合、二重通信は全二重とする必要があります。

12. MTU 設定を指定します。
    - デフォルト値（1500）を選択するには、［**Default**］をクリックします。
    - 異なる設定を選択するには、［MTU］ボックスに設定を入力します。使用しているネットワーク コンポーネントのすべてが、このオプションを使用したサイズ セットをサポートしているか確認してください。

13. オプションで、［Dynamic DNS Registration］オプションを選択します。

    DDNS（動的 DNS）は、DNS（ドメイン ネーム システム）サーバーでローカル IP アドレスを登録するプロトコルです。このリリースでは、DD System Manager は Windows モード DDNS に対応しています。UNIX モード DDNS を使用するには、`net ddns` CLI コマンドを使用します。

    このオプションを有効にするには、DDNS を登録する必要があります。

14. ［**Next**］をクリックします。

    ［Configure Interface Settings］サマリー ページが表示されます。記載されている値は新しいシステムおよびインターフェイスの状態を反映しています。

15. ［**Finish**］と［**OK**］をクリックします。

リンク フェイルオーバー用の仮想インターフェイスの作成

フェイルオーバーに加わるリンクを関連づけるためのコンテナーとして機能する、リンク フェイルオーバー用の仮想インターフェイスを作成します。

フェイルオーバーが有効な仮想インターフェイスは、いずれかをプライマリとして指定できるセカンダリ インターフェイスのグループを表します。システムは、プライマリ インターフェイスが動作している場合、プライマリ インターフェイスをアクティブ インターフェイスにします。設定可能な Down Delay フェイルオーバー オプションによって、900 ミリ秒間隔でフェイルオーバー遅延を設定できます。フェイルオーバー遅延は、ネットワークが不安定な場合におけるフェイルオーバーの頻発を防止します。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. Interfaces テーブルでは、Enabled 列で No をクリックして仮想インターフェイスが追加される物理インターフェイスを無効化します。
3. ［**Create**］メニューから、［**Virtual Interface**］を選択します。
4. ［Create Virtual Interface］ダイアログで、［**veth**］ボックスに仮想インターフェイス名を指定します。

    仮想インターフェイス名を `veth`**x** の形式で入力します。**x** は一意の ID です（通常、1 または 2 桁）。VLAN および IP エイリアスを持つ通常の完全仮想インターフェイスであれば、**veth56.3999:199** といった名前になります。完全名の最大長は 15 文字です。特殊文字は使えません。数字は 0～4094 の間でなくてはなりません。

5. ［**Bonding Type**］リストでは［**Failover**］タイプを選択します。
6. フェイルオーバー構成に追加するインターフェイスを選択して、［**Next**］をクリックします。仮想統合インターフェイスはフェイルオーバーに使用できます。

    ［Create virtual interface veth_name］ダイアログが表示されます。

7. IP アドレスを入力します。IP アドレスを指定しない場合は、**0** と入力します。
8. ネットマスクまたはプレフィックスを入力します。
9. Speed/Duplex オプションを指定します。

    速度および二重通信モード設定の組み合わせにより、インターフェイスを介したデータ転送の速度が決定されます。

    - ［**Autonegotiate Speed/Duplex**］を選択すると、カードによるインターフェイスの回線速度と二重通信モードの設定の自動ネゴシエーションが可能になります。

- ［**Manually configure Speed/Duplex**］を選択すると、手動でインターフェイス データ転送レートを設定します。
  - ［Duplex］オプションは、半二重または全二重です。
  - 表示される速度オプションは、ハードウェア デバイスの性能に制限されます。オプションは、10 Mb、100 Mb、1000 Mb、10 Gb です。
  - 半二重は、10 Mb と 100 Mb の速度のみで使用できます。
  - 1000 Mb および 10 Gb の回線速度では全二重が必要です。
  - 光インターフェイスでは［Autonegotiate］オプションが必要です。
  - 銅線インターフェイスのデフォルトは 10 Gb です。銅線インターフェイスの回線速度が 1000 Gb または 10 Gb に設定されている場合、二重通信は全二重とする必要があります。

10. MTU 設定を指定します。
    - デフォルト値（1500）を選択するには、［**Default**］をクリックします。
    - 異なる設定を選択するには、［MTU］ボックスに設定を入力します。使用しているネットワーク パス コンポーネントのすべてが、このオプションを使用したサイズ セットをサポートしているか確認してください。
11. オプションで、［Dynamic DNS Registration］オプションを選択します。

    DDNS（動的 DNS）は、DNS（ドメイン ネーム システム）サーバーでローカル IP アドレスを登録するプロトコルです。このリリースでは、DD System Manager は Windows モード DDNS に対応しています。UNIX モード DDNS を使用するには、`net ddns` CLI コマンドを使用します。

    このオプションを有効にするには、DDNS を登録する必要があります。

    注

    このオプションを選択すると、このインターフェイスで DHCP が無効化されます。
12. ［次へ］をクリックします。

    ［Configure Interface Settings］サマリー ページが表示されます。記載されている値は新しいシステムおよびインターフェイスの状態を反映しています。
13. ［Interface］に記入し、［**Finish**］と［**OK**］をクリックします。

仮想インターフェイスの変更

仮想インターフェイスを作成後、ネットワークの変更への対応または問題解決のために設定を更新できます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. ［Interfaces］列では、インターフェイスを選択し、［**Enabled**］列で［**No**］をクリックして、仮想インターフェイスを無効化します。警告ダイアログ ボックスの［**OK**］をクリックします。
3. ［**Interfaces**］列で、インターフェイスを選択し、［**Configure**］をクリックします。
4. ［**Configure Virtual Interface**］ダイアログ ボックスで、設定を変更します。
5. ［**Next**］と［**Finish**］をクリックします。

VLAN の構成

新規 VLAN インターフェイスを、物理インターフェイスまたは仮想インターフェイスから作成します。

推奨される VLAN の合計数は 80 です。システムにより作成が禁止されるため、インターフェイスは最大で 100 個（ここからエイリアス、物理および仮想インターフェイスの数を引く）までしか作成できません。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. インターフェイス テーブルで、VLAN を追加したいインターフェイスを選択します。

   VLAN を追加するには、IP アドレスを指定して、選択するインターフェイスを構成する必要があります。
3. ［**Create**］をクリックして［**VLAN**］を選択します。
4. ［Create VLAN］ダイアログ ボックスで、［**VLAN Id**］ボックスに数字を入力して VLAN ID を指定します。

   VLAN ID の範囲は 1～4094 です。
5. IP アドレスを入力します。IP アドレスを指定しない場合は、0 と入力します。

   IP（インターネット プロトコル）アドレスは、インターフェイスに割り当てられる数字ラベルです。たとえば、192.168.10.23 のようになります。
6. ネットマスクまたはプレフィックスを入力します。
7. MTU 設定を指定します。

   VLAN MTU は、割り当てられた物理または仮想インターフェイスに定義された MTU 以上である必要があります。サポート物理または仮想インターフェイスに定義された MTU が設定された VLAN 値を下回ると、サポート インターフェイスに一致するように VLAN 値が自動的に削減されます。サポート インターフェイスの MTU 値が設定された VLAN 値を超えると、VLAN 値は変更されません。

   - デフォルト値（1500）を選択するには、［**Default**］をクリックします。
   - 異なる設定を選択するには、［MTU］ボックスに設定を入力します。DD System Manager は、VLAN が割り当てられた物理または仮想インターフェイスに定義された MTU サイズを超える MTU サイズは許可しません。
8. ［Dynamic DNS Registration］オプションを指定します。

   DDNS（動的 DNS）は、DNS（ドメイン ネーム システム）サーバーでローカル IP アドレスを登録するプロトコルです。このリリースでは、DD System Manager は Windows モード DDNS に対応しています。UNIX モード DDNS を使用するには、`net ddns` CLI コマンドを使用します。

   このオプションを有効にするには、DDNS を登録する必要があります。
9. ［**Next**］をクリックします。

   ［**Create VLAN**］サマリー ページが表示されます。
10. 構成の設定を確認して、［**Finish**］をクリックして、［**OK**］をクリックします。

VLAN インターフェイスの変更

VLAN インターフェイスを作成後、ネットワークの変更への対応または問題解決のために設定を更新できます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. ［**Interfaces**］列では、インターフェイスのチェックボックスを選択し、［**Enabled**］列で［**No**］をクリックして、VLAN インターフェイスを無効化します。［警告］ダイアログ ボックスの［**OK**］をクリックします。
3. Interfaces 列で、インターフェイスのチェックボックスを選択し、［**Configure**］をクリックします。
4. ［**Configure VLAN Interface**］ダイアログで、設定を変更します。
5. ［**Next**］と［**Finish**］をクリックします。

IP エイリアスの構成

IP エイリアスは、追加 IP アドレスを物理インターフェイス、仮想インターフェイス、VLAN に割り当てます。

システムに存在可能な IP エイリアス、VLAN、物理インターフェイス、仮想インターフェイスの推奨される合計数は 80 個です。サポートされるインターフェイスは最大 100 個ですが、最大数に近づくと表示が遅くなる場合があります。

注

Data Domain HA システムを使用する場合、作成されたユーザーが最初にアクティブ ノードにログインせずにスタンバイ ノードにログインすると、そのユーザーは、デフォルトのエイリアスを使用できません。つまり、スタンバイ ノードでエイリアスを使用するためには、ユーザーはまずアクティブ ノードにログインする必要があります。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. ［**Create**］をクリックして［**IP Alias**］を選択します。

   ［Create IP Alias］ダイアログが表示されます。

3. ［**IP ALIAS Id**］ボックスに数字を入力して、IP エイリアス ID を指定します。

   範囲は 1～4094 です。

4. IPv4 または IPv6 アドレスを入力します。
5. IPv4 アドレスを入力した場合、ネットマスク アドレスを入力します。
6. ［Dynamic DNS Registration］オプションを指定します。

   DDNS（動的 DNS）は、DNS（ドメイン ネーム システム）サーバーでローカル IP アドレスを登録するプロトコルです。このリリースでは、DD System Manager は Windows モード DDNS に対応しています。UNIX モード DDNS を使用するには、`net ddns` CLI コマンドを使用します。

   このオプションを有効にするには、DDNS を登録する必要があります。

7. ［次へ］をクリックします。

［Create IP Alias］サマリー ページが表示されます。

8. 構成の設定を確認して、［**Finish**］と［**OK**］をクリックします。

IP エイリアス インターフェイスの変更

IP エイリアスを作成後、ネットワークの変更への対応または問題解決のために設定を更新できます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. ［**Interfaces**］列では、インターフェイスのチェックボックスを選択し、［**Enabled**］列の［**No**］をクリックして、IP エイリアス インターフェイスを無効化します。［警告］ダイアログ ボックスの［**OK**］をクリックします。
3. ［**Interfaces**］列で、インターフェイスのチェックボックスを選択し、［**Configure**］をクリックします。
4. ［Configure IP Alias］ダイアログ ボックスで、IP Alias の作成手順に示すとおり、設定を変更します。
5. ［**Next**］と［**Finish**］をクリックします。

DDNS へのインターフェイスの登録

DDNS（動的 DNS）は、DNS（ドメイン ネーム システム）サーバーでローカル IP アドレスを登録するプロトコルです。

このリリースでは、DD System Manager は Windows モード DDNS に対応しています。UNIX モード DDNS を使用するには、`net ddns` CLI コマンドを使用します。次の操作を行えます。

- 構成されたインターフェイスを DDNS 登録リストに手動で登録（追加）する。
- インターフェイスを DDNS 登録リストから削除する。
- DNS 更新を有効化または無効化する。
- DDNS 登録が有効か無効かを表示する。
- DDNS 登録リストのインターフェイスを表示する。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］ > ［**DDNS Registration**］を選択します。
2. ［DDNS Windows Mode Registration］ダイアログで、［**Add**］をクリックして、DDNS にインターフェイスを追加します。

   ［Add Interface］ダイアログ ボックスが表示されます。

   a. ［**Interface**］フィールドに名前を入力します。

   b. ［**OK**］をクリックします。
3. オプションで、DDNS からインターフェイスを削除します。

   a. 削除するインターフェイスを選択し、［**Remove**］をクリックします。

   b. ［Confirm Remove］ダイアログ ボックスで、［**OK**］をクリックします。
4. DDNS Status を指定します。
   - ［**Enable**］を選択して、登録されているすべてのインターフェイスの更新を有効化します。

- ［**Default**］をクリックして、DDNS 更新のデフォルト設定を選択します。
- ［**Enable**］をクリアして、登録されているインターフェイスの DDNS 更新を無効化します。

5. DDNS 構成を完了するには、［**OK**］をクリックします。

インターフェイスの破棄

DD System Manager を使用して、仮想、VLAN、および IP エイリアス インターフェイスを破棄または削除します。

仮想インターフェイスが破棄されると、システムが仮想インターフェイスを削除して、結合物理インターフェイスをリリースし、仮想インターフェイスにアタッチされた VLAN またはエイリアスを削除します。VLAN インターフェイスを削除すると、OS は VLAN とその下で作成された IP エイリアス インターフェイスを削除します。IP エイリアスを破棄すると、OS はそのエイリアス インターフェイスのみ削除します。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］を選択します。
2. 破棄する各インターフェイス（Virtual、VLAN、または IP Alias）の隣にあるボックスをクリックします。
3. ［**Destroy**］をクリックします。
4. ［**OK**］をクリックして確定します。

ツリー ビューでのインターフェイス階層の表示

［Tree View］ダイアログには、物理インターフェイスと仮想インターフェイス間の関連づけが表示されます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］ > ［**Tree View**］を選択します。
2. ［Tree View］ダイアログ ボックスで、階層を表示するツリー ビューを展開する、または折りたたむには、プラスまたはマイナス ボックスをクリックします。
3. ［**Close**］をクリックしてこのビューを終了してください。

一般的なネットワーク設定の管理

ホスト名、ドメイン名、検索ドメイン、ホスト マッピング、DNS リストの構成の設定は、すべて［Settings］タブで管理されます。

ネットワーク設定情報の表示

［Settings］タブには、ホスト名、ドメイン名、検索ドメイン、ホスト マッピング、DNS の現在の構成が表示されます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Settings**］を選択します。

結果

［Settings］タブには、次の情報が表示されます。

ホスト設定

ホスト名
選択したシステムのホスト名。

ドメイン名
選択したシステムに関連づけられている完全修飾ドメイン名。

Search Domain List

Search Domain
選択されたシステムが使用する検索ドメインのリスト。システムは、検索ドメインをホスト名に対するサフィックスとして適用します。

Hosts Mapping

IP アドレス
解決するホストの IP アドレス。

ホスト名
IP アドレスに関連付けられているホスト名。

DNS List

DNS IP Address
選択したシステムに関連づけられている現在の DNS IP アドレス。アスタリスク（*）は、DHCP を通じて割り当てられた IP アドレスを示します。

DD System Manager ホスト名の設定

DD System Manager ホスト名およびドメイン名を手動で構成できます。また、DD OS が自動的にホストおよびドメイン名を DHCP（動的ホスト構成プロトコル）サーバーから受信するよう構成することもできます。

手動でホストおよびドメイン名を構成することの利点の 1 つが、DHCP サーバーとそれにつながるインターフェイスへの依存関係をなくせることです、サービス割り込みのリスクを軽減するには、ホストおよびドメイン名を手動で構成することを推奨します。

ホスト名とドメイン名を構成する場合、次のガイドラインを考慮してください。

- 一部のブラウザと互換性がないため、ホスト名には下線を使用しないでください。
- レプリケーションと CIFS 認証は、名称変更後に再構成する必要があります。
- システムが完全修飾名なし（ドメイン名なし）で追加されていた場合、ドメイン名を変更するには、影響を受けるシステムを削除してから追加しなおすか、Search Domain List を更新して新しいドメイン名を含める必要があります。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Settings**］を選択します。
2. ［**Host Settings**］領域で、［**Edit**］をクリックします。［Configure Host］ダイアログが表示されます。
3. 手動でホストおよびドメイン名を構成する手順：
   a. ［**Manually configure host**］を選択します。
   b. ［**Host Name**］ボックスにホスト名を入力します。
      例：`id##.yourcompany.com`
   c. ［**Domain Name**］ボックスにドメイン名を入力します。

これは、お使いの Data Domain システムに関連づけられたドメイン名であり、通常、貴社のドメイン名です。例：yourcompany.com

d. ［**OK**］をクリックします。

変更が適用されると、システムは進行状況メッセージを表示します。

4. DHCP サーバーからホストおよびドメイン名を取得するには、［**Obtain Settings using DHCP**］を選択し、［**OK**］をクリックします。

DHCP を使用するには、1 個以上のインターフェイスを構成する必要があります。

ドメイン検索リストの管理

ドメイン検索リストを使用して、システムが検索可能なドメインを定義します。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Settings**］を選択します。
2. ［Search Domain List］領域で［**Edit**］をクリックします。
3. ［Configure Search Domains］ダイアログを使用して検索ドメインを追加するには、次の手順を実行します。
   a. ［Add］（［**+**］）をクリックします。
   b. ［Add Search Domain］ダイアログの［**Search Domain**］ボックスに名前を入力します。

   例：`id##.yourcompany.com`

   c. ［**OK**］をクリックします。

   システムが、新しいドメインを検索可能なドメインのリストに追加します。
   d. ［**OK**］をクリックして変更を適用し、［Settings］ビューに戻ります。
4. ［Configure Search Domains］ダイアログを使用して検索ドメインを削除するには、次の手順を実行します。
   a. 削除する検索ドメインを選択します。
   b. ［Delete］（［**X**］）をクリックします。

   システムが、選択されたドメインを検索可能なドメインのリストから削除します。
   c. ［**OK**］をクリックして変更を適用し、［Settings］ビューに戻ります。

ホスト マップの追加と削除

ホスト マップにより、IP アドレスがホスト名にリンクされるため、IP アドレスまたはホスト名を使用してホストを指定できます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Settings**］を選択します。
2. ホスト マップを追加するには、次の手順を行います。
   a. ［Hosts Mapping］領域で、［**Add**］をクリックします。
   b. ［Add Hosts］ダイアログの［**IP Address**］ボックスにホストの IP アドレスを入力します。
   c. ［Add］（［**+**］）をクリックします。

d. ［Add Host］ダイアログで、リストされているシステムの［**Host Name**］ボックスに **id##.yourcompany.com** などのホスト名を入力します。

e. ［**OK**］をクリックして、［Host Name］リストに新しいホスト名を追加します。

f. ［**OK**］をクリックして、［Settings］タブに戻ります。

3. ホスト マップを削除するには、次の手順を行います。

a. ［Hosts Mapping］領域で、削除するホスト マッピングを選択します。

b. ［Delete］（［**X**］）をクリックします。

DNS IP アドレスの構成

DNS IP アドレスでは、ホスト マッピング テーブルに含まれていないホスト名の IP アドレスを取得するために、システムが使用できる DNS サーバーを指定します。

DNS IP アドレスを手動で構成できます。また、DD OS が自動的に DHCP サーバーから IP アドレスを受け取るように設定することも可能です。手動で DNS IP アドレスを構成することの利点の 1 つが、DHCP サーバーとそれにつながるインターフェイスへの依存関係をなくせることです、サービス割り込みのリスクを軽減するには、EMC が DNS IP アドレスを手動で構成することを推奨します。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Settings**］を選択します。
2. ［DNS List］領域で、［**Edit**］をクリックします。
3. DNS IP アドレスを手動で追加する手順：

a. ［**Manually configure DNS list**］を選択します。

DNS IP アドレス チェックボックスがアクティブになります。

b. ［Add］（［**+**］）をクリックします。

c. ［Add DNS］ダイアログ ボックスに、追加する DNS IP アドレスを入力します。

d. ［**OK**］をクリックします。

システムは、新しい IP アドレスを DNS IP アドレスのリストに追加します。

e. ［**OK**］をクリックして変更を適用します。

4. リストから DNS IP アドレスを削除する手順：

a. ［**Manually configure DNS list**］を選択します。

DNS IP アドレス チェックボックスがアクティブになります。

b. 削除する DNS IP アドレスを選択し、［Delete］（［**X**］）をクリックします。

システムは、IP アドレスを DNS IP アドレスのリストから削除します。

c. ［**OK**］をクリックして変更を適用します。

5. DHCP サーバーから DNS アドレスを取得するには、［**Obtain DNS using DHCP**］を選択し、［**OK**］をクリックします。

DHCP を使用するには、1 個以上のインターフェイスを構成する必要があります。

ネットワーク ルートの管理

ルートは、ローカル ホスト（Data Domain システム）と他のネットワークまたはホスト間でのデータの転送に使用されるパスを決定します。

Data Domain システムは、ネットワーク ルーティング管理プロトコル（RIP、EGRP/EIGRP、BGP）を生成しませんし、応答もしません。Data Domain システムに実装されているルーティングは IPv4 のポリシー ベースのルーティングのみです。これにより、ルーティング テーブルごとにデフォルト ゲートウェイへのルートが 1 つだけ許可されます。ルート テーブルもデフォルト ゲートウェイも複数使用できます。デフォルト ゲートウェイと同じサブネットを持つアドレスごとにルーティング テーブルが 1 つ作成されます。ルーティング ルールでは、テーブルを作成するために使用された IP アドレスと一致するソース IP アドレスを持つパケットをルーティング テーブルに送信します。ルーティング テーブルと一致しないソース IP アドレスを持つその他のすべてのパケットは、メイン ルーティング テーブルに送信されます。

各ルーティング テーブル内に静的ルートを追加することはできますが、ソース ルーティングを使用してテーブルへのパケットが取得されるため、機能する静的ルートは各テーブルのソース アドレスを持つインターフェイスを使用する静的ルートのみです。それ以外の場合は、メイン テーブルに入力する必要があります。

他のルーティング テーブルに対して行われるこれらの IPv4 ソース ルーティングを除き、Data Domain システムでは、IPv4 と IPv6 のメイン ルーティング テーブル用にソース ベースのルーティングを使用します。つまり、複数インターフェイスのサブネットに一致するアウトバウンド ネットワーク パケットは、パケットのソース IP アドレスと一致する IP アドレスを持つ物理インターフェイス、つまりパケットの発生元を介してのみルーティングされます。

IPv6 の場合は、複数のインターフェイスが同じ IPv6 サブネットを含む静的ルートを設定し、そのサブネットを持つ IPv6 アドレスに対して接続が確立されます。通常、静的ルートは、バックアップ用など、同じサブネットの IPv4 アドレスでは必要ありません。Data Domain システムからリモート システムへの接続など、接続を機能させるために静的アドレスが必要になる場合があります。

静的ルートは、ルート指定に対してテーブルの追加または削除を行うことにより、個々のルーティング テーブルに対して追加および削除できます。これにより、特定のソース アドレスを持つパケットを特定のルート テーブルを使用して送信するルールが実現されます。これらのソース アドレスを持つパケットのために静的ルートが必要な場合は、この IP アドレスがルーティングされる特定のテーブルにルートを追加する必要があります。

注

レプリケーション用などに Data Domain システムから開始された接続のルーティングは、同じサブネット上のインターフェイスに使用されるソース アドレスに依存します。特定のインターフェイスのトラフィックを特定の宛先に向けて強制するには（そのインターフェイスが他のインターフェイスと同じサブネットにある場合でも）、2 つのシステム間の静的ルーティング エントリーを構成します。この静的ルーティングによってソース ルーティングがオーバーライドされます。ソース アドレスが IPv4 であり、デフォルト ゲートウェイが関連づけられている場合、この対処は必要ありません。この場合、ソース ルーティングはすでに独自のルーティング テーブルを介して処理されています。

ルート情報の表示

［Routes］タブには、デフォルトのゲートウェイ、静的ルート、動的ルートが表示されます。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Routes**］を選択します。

結果

［Static Routes］領域には、各静的ルートの構成に使用されるルート仕様がリストされます。
［Dynamic Routes］テーブルには、動的に割り当てられた各ルートの情報がリストされます。

表 33 ［Dynamic Routes］列ラベルの説明

項目	説明
ターゲット	ネットワーク トラフィック（データ）が送信される宛先ホスト/ネットワーク。
Gateway	DD ネットワークにおけるルーターのアドレスまたは 0.0.0.0（ゲートウェイが設定されていない場合）
Genmask	宛先ネットのネットマスク。ホスト宛先の場合 255.255.255.255、デフォルト ルートの場合 0.0.0.0 に設定します。
フラグ	フラグには次のものが含まれます。U：ルートが起動中、H：ターゲットがホスト、G：ゲートウェイを使用、R：ダイナミック ルーティングのルートの復元、D：デーモンまたはリダイレクトによって動的インストール、M：ルーティング デーモンまたはリダイレクトから変更、A：addrconf によってインストール、C：キャッシュ エントリー、!：ルートを拒否。
メトリック	ターゲットまでの距離（通常、ホップ単位でカウント）。DD OS は使用せず、ルーティング デーモンが必要とする可能性があります。
MTU	物理（Ethernet）インターフェイスに対する MTU（最大転送単位）のサイズ。
ウィンドウ	このルートを介した TCP 接続のデフォルト ウィンドウ サイズ。
IRTT	遅い場合がある回答を待たずに最高の TCP プロトコル パラメーターを推定するため、カーネルが使用する初期 RTT（往復応答時間）
インターフェイス	ルーティング インターフェイスに関連づけられたインターフェイス名。

デフォルト ゲートウェイの設定

デフォルト ゲートウェイを手動で構成できます。また、DD OS が自動的に DHCP サーバーからデフォルト ゲートウェイ IP アドレスを受け取るように設定することも可能です。

手動でデフォルト ゲートウェイを構成することの利点の 1 つが、DHCP サーバーとそれにつながるインターフェイスへの依存関係をなくせることです、サービス割り込みのリスクを最小限に抑えるには、可能であれば、デフォルト ゲートウェイ IP アドレスを手動で構成します。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Routes**］を選択します。
2. 構成するデフォルトのゲートウェイ タイプ（IPv4 または IPv6）の隣にある［**Edit**］をクリックします。
3. デフォルト ゲートウェイ アドレスを手動で構成する手順：
   a. ［**Manually Configure**］を選択します。
   b. ［**Gateway**］ボックスにゲートウェイ アドレスを入力します。
   c. ［**OK**］をクリックします。
4. DHCP サーバーからデフォルト ゲートウェイ アドレスを取得するには、［**Use DHCP value**］を選択し、［**OK**］をクリックします。

   DHCP を使用するには、1 個以上のインターフェイスを構成する必要があります。

静的ルートの作成

静的ルートでは、システムが通信できるデスティネーション ホストまたはネットワークを定義します。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Routes**］を選択します。
2. ［Static Routes］エリアで［**Create**］をクリックします。
3. ［**Create Routes**］ダイアログで、静的ルートをホストするインターフェイスを選択し、［**Next**］をクリックします。
4. デスティネーションを指定します。
   - 宛先ネットワークを指定するには、［**Network**］を選択し、宛先ネットワークのネットワーク アドレスとネットマスクを入力します。
   - 宛先ホストを指定するには、［**Host**］を選択し、宛先ホストのホスト名と IP アドレスを入力します。
5. オプションで、宛先ネットワークまたはホストへの接続に使用するゲートウェイを指定します。
   a. ［**Specify a gateway for this route**］を選択します。
   b. ［**Gateway**］ボックスにゲートウェイ アドレスを入力します。
6. 構成を確認してから［**Next**］をクリックします。

   ［Create Routes］サマリー ページが表示されます。
7. ［**Finish**］をクリックします。
8. プロセスが完了したら、［**OK**］をクリックします。

   新しいルート仕様が［Route Spec list］に一覧表示されます。

静的ルートの削除

システムと宛先ホストまたはネットワーク間の通信が不要になった場合は、静的ルートを削除します。

手順

1. ［**Hardware**］ > ［**Ethernet**］ > ［**Routes**］を選択します。
2. 削除するルート仕様の Route Spec を選択します。
3. ［**Delete**］をクリックします。
4. ［**Delete**］をクリックして確認し、［**Close**］をクリックします。

   選択されたルート仕様が［Route Spec］リストから削除されます。

システム パスフレーズの管理

システム パスフレーズは、システムの暗号化キーとともに Data Domain システムを移植可能にするキーです。暗号化キーはデータを保護し、システム パスフレーズは暗号化キーを保護します。

システム パスフレーズは、マシン使用可能 AES 256 暗号化キーの生成に使用される判読可能な（理解可能な）キー（スマート カードなど）です。システムが輸送中に盗難に会った場合、攻撃者は容易にデータをリカバリできず、暗号化されたユーザー名と暗号化されたキーをリカバリするのが精一杯です。

パスフレーズは、Data Domain ストレージ サブシステムの隠された部分に内部で保存されます。それによって、Data Domain システムは起動し、管理者の介入なしでデータ アクセスを提供し続けることができます。

システム パスフレーズの設定

システム パスフレーズは、システムでデータの暗号化をサポートする前か、デジタル証明書を要求する前に設定する必要があります。

はじめに

システム パスフレーズの最小長は、DD OS のインストール時には構成されませんが、CLI には最小長を設定するためのコマンドがあります。パスフレーズの最小長が構成されているかどうか確認するには、`system passphrase option show` CLI コマンドを入力します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。

   システム パスフレーズが設定されていない場合、［Passphrase］領域に［**Set Passphrase**］ボタンが表示されます。システム パスフレーズが構成されている場合、［**Change Passphrase**］ボタンが表示されます。選択できるのは、パスフレーズを変更するオプションだけです。

2. ［**Set Passphrase**］ボタンをクリックします。

   ［Set Passphrase］ダイアログが表示されます。

3. ボックスにシステム パスフレーズを入力して、［**Next**］をクリックします。

   システム パスフレーズの最小長が構成されている場合、入力するパスフレーズには最小の文字数が含まれている必要があります。

結果

システム パスフレーズが設定され、［**Change Passphrase**］ボタンが［**Set Passphrase**］ボタンに置き換わります。

システム パスフレーズの変更

管理者は、実際の暗号化キーを操作せずにパスフレーズを変更できます。パスフレーズを間接的に変更すると、キーの暗号化が変更されますが、ユーザー データまたは基礎となっている暗号化キーは影響を受けません。

パスフレーズを変更するには、データの破壊を防ぐための 2 ユーザー認証が必要です。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. システム パスフレーズを変更するには、［**Change Passphrase**］をクリックします。

   ［Change Passphrase］ダイアログが表示されます。

   注

   ファイル システムでは、パスフレーズの変更を無効化する必要があります。ファイル システムが実行中の場合、無効にするように求められます。

3. テキスト フィールドに、次の項目を入力します。

   - セキュリティ担当者アカウント（Data Domain システムのセキュリティ担当者グループの許可されたユーザー）のユーザー名とパスワード。

- パスフレーズ変更時の現在のパスフレーズ。
- 新しいパスフレーズ（`system passphrase option set min-length` コマンドで構成した最小の文字数を含んでいる必要があります）。

4. ［**Enable file system now**］のチェックボックスをクリックします。
5. ［**OK**］をクリックします。

通知

パスフレーズは慎重に取り扱ってください。パスフレーズをなくした場合、ファイル システムのロック解除およびデータ アクセスができなくなり、結果的にデータが失われます。

システム アクセスの管理

システム アクセスの管理機能を使用すると、ローカル データベースまたはネットワーク ディレクトリでのユーザーへのシステム アクセスを制御できます。追加のコントロールで、異なるアクセス レベルを定義し、システムにアクセスできるプロトコルを制御します。

役割に基づいたアクセス制御

RBAC（役割に基づくアクセス制御）は、ユーザーがシステム上でアクセスできる DD System Manager のコントロールと CLI コマンドを制御する認証ポリシーです。

たとえば、［管理者］役割が割り当てられたユーザーはシステム全体を構成および監視でき、［ユーザー］役割を割り当てられたユーザーはシステムのモニタリングに限定されます。DD System Manager にログインすると、ユーザーは自分に割り当てられた役割に基づいて使用を許可されたプログラム機能のみ表示できます。DD OS の管理に使用可能な役割は次のとおりです。

admin

［admin］役割を持つユーザーは、Data Domain システムを構成および監視できます。ほとんどの構成機能とコマンドは、［admin］役割を持つユーザーのみ使用できます。ただし、一部の機能とコマンドは、タスクを完了させるために［security］役割を持つユーザーの承認を必要とします。

limited-admin

［limited-admin］役割を持つユーザーは、Data Domain システムを限定的に構成および監視できます。この役割が割り当てられているユーザーは、データの削除操作、レジストリの編集、bash または SE モードの使用ができません。

user

［user］役割を持つユーザーは、システムを監視し、自分のパスワードを変更できます。
［user］管理役割を割り当てられたユーザーは、システム ステータスを表示できますが、システム構成は変更できません。

security（セキュリティ担当者）

セキュリティ担当者とも呼ばれる、［security］役割を持つユーザーは、他のセキュリティ担当者の管理、セキュリティ担当者の承認が必要なプロシージャの承認、user 役割を持つユーザーに認められるすべてのタスクを実行できます。

［security］役割は、WORM（Write Once Read-Many）規制に対応するために与えられます。この規制は、電子情報開示などを目的に、電子保存された企業のデータを変更されていない元の状態で保管することを求めています。Data Domain は、この機能を強化するため、監査およびログ機能を追加しました。コンプライアンス規制の結果、DD Encryption、DD

Retention Lock Compliance、アーカイブなどの機密性の高い操作を管理するコマンド オプションのほとんどは、セキュリティ担当者の承認を必要とします。

典型的なシナリオでは、［admin］役割を持つユーザーがコマンドを発行し、セキュリティ担当者の承認が必要な場合、システムは承認のプロンプトを表示します。元のタスクを続行するには、セキュリティ担当者は、コマンドが実行されたものと同じコンソールで自身のユーザー名とパスワードを入力する必要があります。システムがセキュリティ担当者の認証情報を認識した場合、プロシージャは承認されます。認識されなかった場合、セキュリティ アラートが生成されます。

security 役割を持つユーザーに適用されるガイドラインは次のとおりです。

- 最初の security 役割を持つユーザーを作成できるのは、［sysadmin］ユーザー（DD OS インストール時に作成されたデフォルト ユーザー）のみです。作成後、［sysadmin］ユーザーがセキュリティ担当者を作成する権限は削除されます。
- 最初のセキュリティ担当者が作成された後は、セキュリティ担当者のみが、他のセキュリティ担当者を作成できます。
- セキュリティ担当者を作成しても、セキュリティ担当者許可ポリシーは有効化されません。許可ポリシーは有効化するには、セキュリティ担当者はログインして、許可ポリシーを有効化する必要があります。
- 権限と義務の分離が適用されます。［admin］役割を持つユーザーはセキュリティ担当者のタスクを実行できず、セキュリティ担当者はシステム構成タスクを実行できません。
- アップグレード時、システム構成にセキュリティ担当者が含まれる場合、現在のセキュリティ担当者全員のリストを含む sec-off-defaults 権限が作成されます。

backup-operator

［backup-operator］役割を持つユーザーは、［user］役割のユーザーに許可されたすべてのタスクの実行、MTree のスナップショットの作成、仮想テープ ライブラリ内の構成要素間でのテープのインポート、エクスポート、移動、プール間のテープのコピーを行うことができます。

［backup-operator］役割を持つユーザーは、パスワードを必要とするログイン用の SSH 公開キーの追加と削除も実行できます （この機能は、ほとんどの場合、自動スクリプト作成に使用されます）。このユーザーは、CLI コマンド エイリアスの追加、削除、リセット、表示、変更されたファイルの同期、レプリケーションがデスティネーション システムで完了するまでの待機を実行できます。

none

［none］役割は、DD Boost 認証とテナント ユニット ユーザーにのみ使用されます。［none］役割を持つユーザーは、Data Domain システムにログインし、自分のパスワードを変更できますが、プライマリ システムの監視、管理、または構成は実行できません。プライマリ システムがテナント ユニットにパーティション化されている場合、［tenant-admin］または［tenant-user］役割は、特定のテナント ユニットに関してユーザーの役割を定義するために使用されます。テナント ユーザーにはまず、プライマリ システムへのアクセスを最小限にするため［none］役割が割り当てられ、その後、［tenant-admin］または［tenant-user］役割が追加されます。

tenant-admin

SMT（Secure Multi-Tenancy）機能が有効になっている場合、［tenant-admin］役割を他の（tenant 以外の）役割に追加できます。［tenant-admin］ユーザーは、特定のテナント ユニットを構成および監視できます。

tenant-user

SMT 機能が有効になっている場合、［tenant-user］役割を他の（tenant 以外の）役割に追加できます。［tenant-user］役割を持つユーザーは、特定のテナント ユニットを監視し、

自分のパスワードを変更できます。[tenant-user] 管理役割を割り当てられたユーザーは、テナント ユニット ステータスを表示できますが、テナント システム構成は変更できません。

IP プロトコルのアクセス管理

この機能では、FTP、FTPS、HTTP、HTTPS、SSH、SCP、Telnet プロトコルのシステム アクセスを管理します。

IP サービス構成の表示

[Administrator Access] タブには、システムにアクセスするために使用できる IP プロトコルの構成ステータスが表示されます。FTP および FTPS プロトコルだけが、管理者に限定されています。

手順

1. [**Administration**] > [**Access**] > [**Administrator Access**] を選択します。

結果

[Access Management] ページには、[Administrator Access]、[Local Users]、[Authentication]、[Active Users] タブが表示されます。

表 34 [Administrator Access] タブの情報

項目	説明
Passphrase	パスフレーズが設定されていない場合、[**Set Passphrase**] ボタンが表示されます。パスフレーズが設定されている場合、[**Change Passphrase**] ボタンが表示されます。
サービス	システムにアクセスできるサービス/プロトコルの名前。
Enabled (Yes/No)	サービスのステータス。サービスが無効になっている場合、リストで選択し、[**Configure**] をクリックして有効化します。ダイアログ ボックスの [General] タブに入力します。サービスが有効になっている場合、リストで選択し、[**Configure**] をクリックして、その設定を変更します。ダイアログ ボックスの [General] タブで設定を編集します。
Allowed Hosts	サービスにアクセスできるホスト（複数の場合あり）。
Service Options	リストで選択されているサービスのポートまたはセッション タイムアウト値。
FTP/FTPS	セッション タイムアウトのみ設定できます。
HTTP port	HTTP プロトコル（デフォルトではポート 80）に開かれたポート番号。
HTTPS port	HTTPS プロトコル（デフォルトではポート 443）に開かれたポート番号。
SSH/SCP port	SSH/SCP プロトコル（デフォルトではポート 22）に開かれたポート番号。
Telnet	ポート番号は設定できません。
セッション タイムアウト	接続が閉じられるまでの許容非アクティブ時間の長さ。デフォルトは Infinite で、接続は閉じません。可能であれば、セッション タイムアウトの最大値を 5 分に設定します。タイムアウトを秒単位で設定する場合、ダイアログ ボックスの [**Advanced**] タブを使用します。

FTP アクセスの管理

FTP（File Transfer Protocol）を使用すると、管理者は Data Domain システム上のファイルにアクセスできます。

管理者管理役割を割り当てられたユーザーの FTP または FTPS アクセスを有効化します。FTP アクセスによって、FTP を非セキュア アクセス メソッドにして、管理ユーザー名とパスワードをクリアテキストでネットワーク間をまたいで使用できるようになります。FTPS は、安全なアクセス方法として推奨されています。FTP または FTPS アクセスを有効化すると、他方のアクセス方法は無効化されます。

注

管理者管理役割を割り当てられたユーザーのみが、FTP を使用してシステムにアクセスできます。

注

FTPS または FTP を介して Data Domain システムに接続する LFTP クライアントは、設定されたタイムアウトの上限に達すると切断されます。ただし、コマンド実行中にタイムアウト後、LFTP クライアントはキャッシュされたユーザー名とパスワードを使用して再接続します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. ［**FTP**］を選択し、［**Configure**］をクリックします。
3. FTP アクセスおよび接続できるホストを管理するには、［General］タブを選択し、次の手順を行います。
   a. FTP アクセスを有効化するには、［**Allow FTP Access**］を選択します。
   b. すべてのホストが接続できるようにするには、［**Allow all hosts to connect**］を選択します。
   c. ホストを選択するアクセスを制限するには、［**Limit Access to the following systems**］を選択し、［Allowed Hosts］リストを変更します。

      注

      完全修飾ホスト名、IPv4 アドレス、または IPv6 アドレスを使用して、ホストを識別できます。

      - ホストを追加するには、［Add］（［**+**］）をクリックします。ホスト ID を入力し、［**OK**］をクリックします。
      - ホスト ID を変更するには、［**Hosts**］リストでホスト名を選択し、［Edit］（鉛筆）をクリックします。ホスト ID を変更し、［**OK**］をクリックします。
      - ホスト ID を削除するには、［**Hosts**］リストでホスト名を選択し、［Delete］（［**X**］）をクリックします。
4. セッション タイムアウトを設定するには、［**Advanced**］タブを選択し、秒単位でタイムアウト値を入力します。

   注

   セッション タイムアウト デフォルトは Infinite で、接続は閉じません。

5. ［**OK**］をクリックします。

   FTPS が有効になっている場合、警告メッセージとともにプロンプトが表示されるので、［**OK**］をクリックして処理を進めます。

FTPS アクセスの管理

FTPS（FTP Secure）プロトコルを使用すると、管理者は Data Domain システム上のファイルにアクセスできます。

FTPS は、TLS（Transport Layer Security）および SSL（Secure Sockets Layer）暗号形式プロトコルへの対応など、FTP を使用した追加セキュリティを提供します。FTPS を使用する場合は、次のガイドラインを考慮してください。

- 管理者管理役割を割り当てられたユーザーのみ、FTPS を使用してシステムにアクセスできます。
- FTPS アクセスを有効にすると、FTP アクセスは無効になります。
- FTPS は、DD OS 5.3 以降を実行している DD システムから管理される、DD OS 5.2 を実行している DD システムのサービスとして表示されます。
- `get` コマンドの発行時に、一致するバージョンの SSL が Data Domain システムにインストールされておらず、LFTP クライアント上でコンパイルされている場合、致命的エラー メッセージ「`SSL_read: wrong version number lftp`」というメッセージが表示されます。回避策として、同じファイルで `get` コマンドの再発行を試します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. ［**FTPS**］を選択し、［**Configure**］をクリックします。
3. FTPS アクセスおよび接続できるホストを管理するには、［General］タブを選択し、次の手順を行います。
   a. FTPS アクセスを有効化するには、［**Allow FTPS Access**］を選択します。
   b. すべてのホストが接続できるようにするには、［**Allow all hosts to connect**］を選択します。
   c. ホストを選択するアクセスを制限するには、［**Limit Access to the following systems**］を選択し、ホストのリストを変更します。

   注

   完全修飾ホスト名、IPv4 アドレス、または IPv6 アドレスを使用して、ホストを識別できます。

   - ホストを追加するには、［Add］（［**+**］）をクリックします。ホスト ID を入力し、［**OK**］をクリックします。
   - ホスト ID を変更するには、［**Hosts**］リストでホスト名を選択し、［Edit］（鉛筆）をクリックします。ホスト ID を変更し、［**OK**］をクリックします。
   - ホスト ID を削除するには、［**Hosts**］リストでホスト名を選択し、［Delete］（［**X**］）をクリックします。
4. セッション タイムアウトを設定するには、［**Advanced**］タブを選択し、秒単位でタイムアウト値を入力します。

注

セッション タイムアウト デフォルトは Infinite で、接続は閉じません。

5. ［**OK**］をクリックします。FTP が有効になっている場合、警告メッセージが表示されるので、［**OK**］をクリックして処理を進めます。

HTTP と HTTPS アクセスの管理

HTTP または HTTPS アクセスは、DD System Manager へのブラウザ アクセスをサポートするために必要です。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. ［**HTTP**］または［**HTTPS**］を選択して、［**Configure**］をクリックします。

   ［Configure HTTP/HTTPS Access］ダイアログが表示され、そこに一般構成、高度な構成、証明書管理のタブが表示されます。
3. アクセス方法および接続できるホストを管理するには、［General］タブを選択し、次の手順を行います。
   a. 許可したいアクセス方法のチェックボックスを選択します。
   b. すべてのホストが接続できるようにするには、［**Allow all hosts to connect**］を選択します。
   c. ホストを選択するアクセスを制限するには、［**Limit Access to the following systems**］を選択し、ホストのリストを変更します。

      注

      完全修飾ホスト名、IPv4 アドレス、または IPv6 アドレスを使用して、ホストを識別できます。

      - ホストを追加するには、［Add］（［**+**］）をクリックします。ホスト ID を入力し、［**OK**］をクリックします。
      - ホスト ID を変更するには、［**Hosts**］リストでホスト名を選択し、［Edit］（鉛筆）をクリックします。ホスト ID を変更し、［**OK**］をクリックします。
      - ホスト ID を削除するには、［**Hosts**］リストでホスト名を選択し、［Delete］（［**X**］）をクリックします。
4. システム ポートとセッションのタイムアウト値を構成するには、［**Advanced**］タブを選択して、フォームの入力を完了します。
   - ［**HTTP Port**］ボックスに、ポート番号を入力します。ポート 80 がデフォルトで割り当てられます。
   - ［**HTTP Port**］ボックスに、番号を入力します。ポート 443 がデフォルトで割り当てられます。
   - ［**Session Timeout**］ボックスに、接続が終了するまでのインターバルを秒単位で入力します。最小は 60 秒、最大は 31536000 秒（1 年）です。

注

デフォルトのセッション タイムアウトは 10,800 秒です。

5. ［**OK**］をクリックします。

HTTP と HTTPS のホスト証明書の管理

ホスト証明書によって、ブラウザーは管理セッションの確立時にシステムのアイデンティティを検証できます。

HTTP と HTTPS のホスト証明書の要求

DD System Manager を使用して、ホスト証明書のリクエストを生成し、CA（認証機関）に転送することができます。

注

CSR を作成するには、システム パスフレーズ（システム パスフレーズ セット）を構成する必要があります。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. ［Services］領域で、［**HTTP**］または［**HTTPS**］を選択し、［**Configure**］をクリックします。
3. ［**Certificate**］タブを選択します。
4. ［追加］をクリックします。
   この手順で前に選択したプロトコル用のダイアログが表示されます。
5. ［**Generate the CSR for this Data Domain system**］をクリックします。
   ダイアログが展開し、CSR フォームが表示されます。

   注

   DD OS は、一度につき 1 個のアクティブ CSR に対応します。CSR が生成されると、［**Generate the CSR for this Data Domain system**］リンクが［**Download the CSR for this Data Domain system**］リンクに置き換わります。CSR を削除するには、`adminaccess certificate cert-signing-request delete` CLI コマンドを使用します。
6. CSR フォームに記入し、［**Generate and download a CSR**］をクリックします。
   CSR ファイルは次のパスに保存されます：`/ddvar/certificates/CertificateSigningRequest.csr`。SCP、FTP、FTPS を使用して、CSR ファイルをシステムから、CSR を CA に送信できるコンピューターに転送します。

HTTP と HTTPS のホスト証明書の追加

DD System Manager を使用して、システムにホスト証明書を追加できます。

手順

1. ホスト証明書をまだ要求していない場合、認証機関にホスト証明書を要求します。
2. ホスト証明書を受け取ったら、それをコピーし、DD Service Manager を実行するコンピューターにそれを移します。

3. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
4. ［Services］領域で、［**HTTP**］または［**HTTPS**］を選択し、［**Configure**］をクリックします。
5. ［**Certificate**］タブを選択します。
6. ［**Add**］をクリックします。

   この手順で前に選択したプロトコル用のダイアログが表示されます。

7. .p12 ファイルに組み込まれたホスト証明書を追加するには、次の手順を行います。
   a. ［**I want to upload the certificate as a .p12 file**］を選択します。
   b. ［**Password**］ボックスにパスワードを入力します。
   c. ［**Browse**］をクリックして、システムにアップロードするホスト証明書ファイルを選択します。
   d. ［**Add**］をクリックします。
8. .pem ファイルに組み込まれたホスト証明書を追加するには、次の手順を行います。
   a. ［**I want to upload the public key as a .pem file and use a generated private key**］を選択します。
   b. ［**Browse**］をクリックして、システムにアップロードするホスト証明書ファイルを選択します。
   c. ［**Add**］をクリックします。

HTTP と HTTPS のホスト証明書の削除

DD OS は、HTTP と HTTPS に対して 1 つのホスト証明書に対応しています。現在、システムでホスト証明書を使用していて、別のホスト証明書を使用する場合は、現在の証明書を削除してから新しい証明書を追加する必要があります。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. ［Services］領域で、［**HTTP**］または［**HTTPS**］を選択し、［**Configure**］をクリックします。
3. ［**Certificate**］タブを選択します。
4. 削除したいジョブを選択します。
5. ［**Delete**］、次に［**OK**］をクリックします。

SSH と SCP アクセスの管理

SSH は、SCP（セキュア コピー）の有無に関係なく、システム CLI へのネットワーク アクセスを可能にするセキュアなプロトコルです DD System Manager を使用して、SSH プロトコルを使用したシステム アクセスを有効にできます。SCP は SSH を必要とするため、SSH が無効化されると、SCP が自動的に無効化されます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. ［**SSH**］または［**SCP**］を選択して［**Configure**］をクリックします。
3. アクセス方法および接続できるホストを管理するには、［**General**］タブを選択します。
   a. 許可したいアクセス方法のチェックボックスを選択します。
   b. すべてのホストが接続できるようにするには、［**Allow all hosts to connect**］を選択します。

c. ホストを選択するアクセスを制限するには、［**Limit Access to the following systems**］を選択し、ホストのリストを変更します。

注

完全修飾ホスト名、IPv4 アドレス、または IPv6 アドレスを使用して、ホストを識別できます。

- ホストを追加するには、［Add］（［**+**］）をクリックします。ホスト ID を入力し、［**OK**］をクリックします。
- ホスト ID を変更するには、［**Hosts**］リストでホスト名を選択し、［Edit］（鉛筆）をクリックします。ホスト ID を変更し、［**OK**］をクリックします。
- ホスト ID を削除するには、［**Hosts**］リストでホスト名を選択し、［Delete］（［**X**］）をクリックします。

4. システム ポートとセッションのタイムアウト値を設定するには、［**Advanced**］タブをクリックします。
   - ［**SSH/SCP Port**］テキスト入力ボックスに、ポート番号を入力します。ポート 22 がデフォルトで割り当てられます。
   - ［**Session Timeout**］ボックスに、接続が終了するまでのインターバルを秒単位で入力します。

注

セッション タイムアウト デフォルトは Infinite で、接続は閉じません。

注

［**Default**］をクリックして、デフォルト値に戻します。

5. ［**OK**］をクリックします。

Telnet アクセスの管理

Telnet は、システム CLI へのネットワーク アクセスを可能にする非セキュアなプロトコルです。

注

Telnet アクセスによって、Telnet を非セキュアな アクセス メソッドにして、ユーザー名とパスワードをクリアテキストでネットワーク間をまたいで使用できるようになります。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Administrator Access**］を選択します。
2. ［**Telnet**］を選択し、［**Configure**］をクリックします。
3. Telnet アクセスと接続できるホストを管理するには、［**General**］タブを選択します。
   a. Telnet アクセスを有効化するには、［**Allow Telnet Access**］を選択します。
   b. すべてのホストが接続できるようにするには、［**Allow all hosts to connect**］を選択します。
   c. ホストを選択するアクセスを制限するには、［**Limit Access to the following systems**］を選択し、ホストのリストを変更します。

注

完全修飾ホスト名、IPv4 アドレス、または IPv6 アドレスを使用して、ホストを識別できます。

- ホストを追加するには、［Add］（［**+**］）をクリックします。ホスト ID を入力し、［**OK**］をクリックします。
- ホスト ID を変更するには、［**Hosts**］リストでホスト名を選択し、［Edit］（鉛筆）をクリックします。ホスト ID を変更し、［**OK**］をクリックします。
- ホスト ID を削除するには、［**Hosts**］リストでホスト名を選択し、［Delete］（［**X**］）をクリックします。

4. セッション タイムアウトを設定するには、［Advanced］タブを選択し、秒単位でタイムアウト値を入力します。

   注

   セッション タイムアウト デフォルトは Infinite で、接続は閉じません。

5. ［**OK**］をクリックします。

ローカル ユーザー アカウントの管理

ローカル ユーザーは、Windows Active Directory、Windows ワークグループ、NIS ディレクトリに定義される代わりに、Data Domain システムに構成されているユーザー アカウント（ユーザー名とパスワード）です。

トラステッド ドメインが設定されると、そのドメインに属しているユーザーは、そのトラステッド ドメインがオフラインの場合でも、Data Domain システムにログインできるようになります。

UID 競合： ローカル ユーザーと NIS ユーザー アカウント

NIS 環境で Data Domain システムをセットアップするときは、ローカル ユーザーと NIS ユーザーのアカウント間の UID 競合の可能性に注意してください。

Data Domain システム上のローカル ユーザー アカウントは、500 の UID から始まります。競合を避けるため、NIS ユーザーに許される UID 範囲を定義するときに、将来的なローカル アカウントのサイズを考慮します。

ローカル ユーザー情報の表示

ローカル ユーザーは、Active Directory、ワークグループ、UNIX ではなく、システムに定義されているユーザー アカウントです。ローカル ユーザーのユーザー名、管理役割、ログイン ステータス、ターゲットの無効化日付を表示できます。また、ユーザーのパスワード コントロール、ユーザーがアクセスできるテナント ユニットを表示できます。

注

ユーザー認証モジュールは、GMT（グリニッジ標準時）を使用します。ユーザー アカウントとパスワードが正しく期限切れになるように、ターゲットのローカル時間に対応した GMT を使用するように設定を構成します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Local Users**］を選択します。

［Local Users］ビューが表示され、そのビューには［Local Users］テーブルと［Detailed Information］領域が表示されます。

表 35 ローカル ユーザー リストの列ラベルの説明

項目	説明
NAME	システムに追加されるユーザー ID。
Management Role	表示される役割は、admin、user、security、backup-operator、または none です。この表では、テナント ユーザーの役割は［none］として表示されます。割り当てられたテナント役割を表示するには、ユーザーを選択し、［Detailed Information］領域に役割を表示します。
Status	• Active：アカウントへのユーザーのアクセスが許可されています。 • Disabled：アカウントが管理者によって無効にされたか、現在の日付がアカウントの有効期限を過ぎているか、ロックされたアカウントのパスワードを更新する必要があるため、アカウントへのユーザーのアクセスが拒否されています。 • Locked：パスワードが期限切れになったため、ユーザーのアクセスが拒否されています。
Disable Date	アカウントが無効化されるよう設定された日付。
Last Login From	ユーザーが最後にログインした場所。
Last Login Time	ユーザーが最後にログインした時間。

注

管理者またはセキュリティ担当者役割が構成されているユーザー アカウントは、すべてのユーザーを表示できます。他の役割のユーザーは、自分のユーザー アカウントしか表示できません。

2. ユーザーのリストから表示したいユーザーを選択します。

   選択されたユーザーについての情報が、［Detailed Information］領域に表示されます。

表 36 詳細なユーザー情報、行ラベルの説明

項目	説明
Password Last Changed	パスワードが最後に変更された日付。
Minimum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最小日数として、ユーザーに許可する値。デフォルトは 0 日です。
Maximum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最大日数として、ユーザーに許可する値。デフォルトは 90 です。
Warn Days Before Expire	パスワードが期限切れになる前にユーザーに警告する日数。デフォルトは 7 日前です。
Disable Days After Expire	パスワードが期限切れになった後にユーザー アカウントを無効にする日数。デフォルトは Never です。

注

デフォルト値は、初期デフォルト・パスワード ポリシーの値です。システム管理者（admin 役割）は、［**More Tasks**］ > ［**Change Login Options**］を選択することでこれらを変更できます。

ローカル ユーザーの作成

外部ディレクトリを介さずに、ローカル システムのアクセスを管理する場合は、ローカル ユーザーを作成します。Data Domain システムは、最大 500 個のローカル ユーザー アカウントに対応しています。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Local Users**］を選択します。

   ［Local Users］ビューが表示されます。

2. ［**Create**］をクリックして新規ユーザーを作成します。

   ［Create User］ダイアログが表示されます。

3. ［General］タブにユーザー情報を入力します。

   表 37 ［Create User］ダイアログ、一般設定

項目	説明
ユーザー	ユーザー ID またはユーザー名。
パスワード	ユーザーのパスワード。デフォルト パスワードを設定します。ユーザーは、後からパスワードを変更することができます。
Verify Password	ユーザーのパスワードをもう一度入力します。
Management Role	ユーザーに割り当てられた役割（管理者、セキュリティ、ユーザー、バックアップオペレーター、またはなし）。 注 最初のセキュリティ役割を持つユーザーを作成できるのは、sysadmin ユーザー（DD OS インストール時に作成されたデフォルト ユーザー）のみです。最初のセキュリティ役割を持つユーザーが作成されると、セキュリティ役割を持つユーザーは他のセキュリティ役割を持つユーザーを作成できます。
強制的なパスワードの変更	このチェックボックスを選択すると、SSH または Telenet を使用した DD System Manager または CLI への初回ログイン時にユーザーによるパスワード変更が必要になります。

   パスワードの最小長のデフォルト値は 6 文字です。ユーザー パスワードに必要な文字クラスの最小数のデフォルト値は 1 です。許容される文字クラスは次のとおりです。

   - 小文字の a～z
   - 大文字の A～Z
   - 数字の 0～9
   - 特殊文字（$、%、#、+など）

注

sysadmin はデフォルトの管理者ユーザーで、削除または変更はできません。

4. パスワードとアカウント有効期限を管理するには、［Advanced］タブを選択し、次の表に示すコントロールを使用します。

表 38 ［Create User］ダイアログ、高度な設定

項目	説明
Minimum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最小日数として、ユーザーに許可する値。デフォルトは 0 日です。
Maximum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最大日数として、ユーザーに許可する値。デフォルトは 90 です。
Warn Days Before Expire	パスワードが期限切れになる前にユーザーに警告する日数。デフォルトは 7 日前です。
Disable Days After Expire	パスワードが期限切れになった後にユーザー アカウントを無効にする日数。デフォルトは Never です。
Disable account on the following date	このボックスにチェックを入れ、このアカウントを無効にする日付を mm/dd/yyyy 形式で入力します。カレンダーをクリックして日付を選択することもできます。

5. ［**OK**］をクリックします。

注

注：デフォルトのパスワード ポリシーは、管理者の役割を持つユーザーが変更した場合に変更されます（［**More Tasks**］ > ［**Change Login Options**］）。デフォルト値は、初期デフォルト パスワード ポリシーの値です。

ローカル ユーザー プロファイルの変更

ユーザーを作成後、DD System Manager を使用して、ユーザーの構成を変更できます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Local Users**］を選択します。

   ［Local Users］ビューが表示されます。

2. リストのユーザー名をクリックします。
3. ［**Modify**］をクリックして、ユーザー アカウントを変更します。

   ［Modify User］ダイアログ ボックスが開きます。

4. ［General］タブで情報を入力します。

注

SMT が有効で、何もない状態から別の役割への役割変更がリクエストされていると、変更を受け入れられるのは、ユーザーが、管理ユーザーとしてテナント ユニットが割り当てられておらず、デフォルトのテナント ユニット セットを持つ DD Boost ユーザーではなく、テナント ユニットに割り当てられていないストレージ ユニットの所有者ではない場合のみです。

注

ストレージ ユニットをまったく所有していない DD Boost ユーザーの役割を変更するには、DD Boost ユーザーとしての割り当てを解除し、ユーザーの役割を変更してから、DD Boost ユーザーとして再度割り当てます。

表 39 ［Modify User］ダイアログ、一般設定

項目	説明
ユーザー	ユーザー ID またはユーザー名。
Role	リストから役割を選択してください。

5. ［Advanced］タブで情報を更新します。

表 40 ［Modify User］ダイアログ、高度な設定

項目	説明
Minimum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最小日数として、ユーザーに許可する値。デフォルトは 0 日です。
Maximum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最大日数として、ユーザーに許可する値。デフォルトは 90 です。
Warn Days Before Expire	パスワードが期限切れになる前にユーザーに警告する日数。デフォルトは 7 日前です。
Disable Days After Expire	パスワードが期限切れになった後にユーザー アカウントを無効にする日数。デフォルトは Never です。

6. ［**OK**］をクリックします。

ローカル ユーザーの削除

ユーザー役割に基づき、特定のユーザーを作成できます。選択したユーザーが 1 つでも削除できない場合は、［Delete］ボタンが無効になっています。

sysadmin ユーザーは削除できません。Admin ユーザーはセキュリティ担当者を削除できません。セキュリティ担当者は、他のセキュリティ担当者を削除、有効化、無効化できます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Local Users**］を選択します。
   ［Local Users］ビューが表示されます。
2. 一覧から 1 つまたは複数のユーザー名をクリックします。
3. ［**Delete**］をクリックして、ユーザー アカウントを削除します。
   ［Delete User］ダイアログ ボックスが開きます。

4. ［**OK**］と［**Close**］をクリックします。

ローカル ユーザーの有効化と無効化

管理者ユーザーは、sysadmin ユーザーおよび security の役割を持つユーザーを除くすべてのユーザーを有効化または無効化できます。sysadmin ユーザーは無効化できません。セキュリティ担当者のみが、他のセキュリティ担当者を有効化または無効化できます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Local Users**］を選択します。

   ［Local Users］ビューが表示されます。

2. 一覧から 1 つまたは複数のユーザー名をクリックします。
3. ［**Enable**］または［**Disable**］ボタンをクリックして、ユーザー アカウントの有効化または無効化を行います。

   ［Enable or Disable User］ダイアログ ボックスが表示されます。

4. ［**OK**］と［**Close**］をクリックします。

セキュリティ許可の有効化

Data Domain システム CLI（コマンド ライン インターフェイス）を使用して、セキュリティ許可ポリシーを有効化および無効化できます。

この手順で使用されるコマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

注

DD Retention Lock Compliance ライセンスをインストールする必要があります。DD Retention Lock Compliance システムで許可ポリシーを無効化することは認められません。

手順

1. セキュリティ担当者のユーザー名とパスワードを使用して、CLI にログインします。
2. セキュリティ担当者許可ポリシーを有効化するには、次のコマンドを実行します。`# authorization policy set security-officer enabled`

ユーザー パスワードの変更

ユーザーを作成後、DD System Manager を使用して、ユーザーのパスワードを変更できます。個々のユーザーが自身のパスワードを変更することもできます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Local Users**］をクリックします。

   ［Local Users］ビューが表示されます。

2. リストのユーザー名をクリックします。
3. ユーザー パスワードを変更するには、［**Change Password**］をクリックします。

   ［Change Password］ダイアログ ボックスが表示されます。

4. ［**Old Password**］ボックスに、古いパスワードを入力します。
5. ［**New Password**］ボックスに、新しいパスワードを入力します。

6. ［**Verify New Password**］ボックスに、新しいパスワードを再度入力します。
7. ［**OK**］をクリックします。

「admin」役割を持つユーザーのみ、他のユーザーのパスワードを変更できます。管理者は、`user change password [<user>]` コマンドを実行することによって、CLI から他のユーザーのパスワードを変更できます。

注

セキュリティ上の理由から、「admin」役割を持つユーザーは、他の「admin」ユーザーのパスワードを変更することはできません。別のユーザーとしてログインして「admin」ユーザー パスワードを変更する必要がある場合は、サポート リクエストまたはチャット リクエストを作成して、DELL-EMC サポートにお問い合わせください。

パスワード ポリシーとログイン コントロールの変更

パスワード ポリシーとログイン コントロールでは、すべてのユーザーのログイン要件を定義します。管理者は、パスワードの変更頻度、有効なパスワードを作成するための要件、無効なログインの試みに対するシステムの対応方法を指定できます。

手順

1. ［**Administration**］ > ［**Access**］を選択します。
2. ［**More Tasks**］ > ［**Change Login Options**］を選択します。

   ［Change Login Options］ダイアログが表示されます。

3. 各オプションのボックスで、新しい構成を指定します。デフォルト値を選択するには、該当オプションの隣にある［**Default**］をクリックします。
4. ［**OK**］をクリックして、パスワード設定を保存します。

［Change Login Options］ダイアログ

このダイアログを使用して、パスワード ポリシーを設定し、ログインの最大試行回数とロックアウト期間を指定します。

表 41 ［Change Login Options］ダイアログのコントロール

項目	説明
Minimum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最小日数として、ユーザーに許可する値。この値は、［**Maximum Days Between Change**］の値から［**Warn Days Before Expire**］の値を引いた値より小さい値である必要があります。デフォルト設定は 0 です。
Maximum Days Between Change	パスワードを変更してから次にパスワードを変更するまでの最大日数として、ユーザーに許可する値。最小値は 1 です。デフォルト値は 90 です。
Warn Days Before Expire	パスワードが期限切れになる前にユーザーに警告する日数。この値は、［**Maximum Days Between Change**］の値から［**Minimum Days Between Change**］の値を引いた値より小さい値である必要があります。デフォルト設定は 7 です。
Disable Days After Expire	このオプションで指定した日数に従い、パスワードの有効期限後にユーザー アカウントが無効にされます。有効なエントリーは、［never］または 0 以上の数値です。デフォルト設定は never です。

表 41 ［Change Login Options］ダイアログのコントロール （続き）

項目	説明
Minimum Length of Password	必要な最小パスワード長。デフォルトは 6。
Minimum Number of Character Classes	ユーザー パスワードに必要な文字クラスの最低数。デフォルトは 1。文字クラスには次のものが含まれる： • 小文字の a～z • 大文字の A～Z • 数字の 0～9 • 特殊文字（$、%、#、+など）
Lowercase Character Requirement	最低 1 文字の小文字を必要とする要件を有効または無効にします。デフォルト設定は disabled です。
Uppercase Character Requirement	最低 1 文字の大文字を必要とする要件を有効または無効にします。デフォルト設定は disabled です。
One Digit Requirement	最低 1 文字の数字を必要とする要件を有効または無効にします。デフォルト設定は disabled です。
Special Character Requirement	最低 1 文字の特殊文字を必要とする要件を有効または無効にします。デフォルト設定は disabled です。
Max Consecutive Character Requirement	最大 3 文字の繰り返し文字の要件を有効または無効にする。デフォルト設定は disabled です。
Number of Previous Passwords to Block	世代管理するパスワードの数を指定します。範囲は 0～24 で、デフォルト設定は 1 です。 注 この設定の数を減らしても、世代管理されているパスワード リストは、次回パスワードが変更されるまで変わりません。たとえば、この設定を 4 から 3 に変更した場合、最後の 4 つのパスワードは、次回パスワードが変更されるまで世代管理されています。
Maximum login attempts	ユーザー アカウントに強制ロックがかかるまでに試行可能なログインの最大回数を指定します。この制限は、sysadmin を含む、すべてのユーザー アカウントに適用される。ロックされたユーザーは、アカウントがロックされている間はログインできない。範囲は 4～10 で、デフォルト値は 4 です。
Unlock timeout (seconds)	ログインの試行が最大回数を超えた後、ユーザー アカウントがロックされる時間を指定します。構成されているアンロックのタイムアウトに達すると、ユーザーはログインを試みることができます。範囲は 120～600 秒で、デフォルトの期間は 120 秒です。
Maximum active logins	許可するアクティブなログインの最大数を指定します。デフォルト値は 100 です。

ディレクトリ ユーザーおよびグループの管理

DD System Manager を使用して、Windows Active Directory、Windows ワークグループ、NIS 内のユーザーとグループのシステムへのアクセスを管理できます。Kerberos 認証は、CIFS クライアントと NFS クライアントのオプションです。

Active Directory および Kerberos 情報の表示

Active Directory Kerberos 構成によって、CIFS および NFS クライアントが認証に使用する方法が決まります。［Active Directory/Kerberos Authentication］パネルにこの構成が表示されます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。
2. ［Active Directory/Kerberos Authentication］パネルを展開します。

表 42 Active Directory/Kerberos Authentication ラベルの説明

項目	説明
モード	認証モードのタイプ。Windows/Active Directory モードでは、CIFS クライアントは Active Directory および Kerberos 認証を使用し、NFS クライアントは Kerberos 認証を使用します。UNIX モードでは、CIFS クライアントは Workgroup 認証（Kerberos なし）を使用し、NFS クライアントは Kerberos 認証を使用します。Disabled モードでは、Kerberos 認証は無効で、CIFS クライアントは Workgroup 認証を使用します。
レルム	ワーク グループまたは Active Directory のレルム名。
DDNS	Dynamic Domain Name System が有効になっているかどうか。
Domain Controllers	ワーク グループまたは Active Directory のドメイン コントローラー名。
組織単位	ワーク グループまたは Active Directory の組織単位名。
*CIFS サーバー名	使用中の CIFS サーバーの名前（Windows モードのみ）。
WINS Server	使用中の WINS サーバーの名前（Windows モードのみ）。
Short Domain Name	ドメインの省略された名前
NTP	有効/無効（UNIX モードのみ）
NIS	有効/無効（UNIX モードのみ）
Key Distribution Centers	使用中の KDC のホスト名または IP（UNIX モードのみ）
Active Directory Administrative Access	Enabled/Disabled：クリックして、Active Directory（Windows）グループの管理アクセスを有効化または無効化します。

表 43 Active Directory 管理グループおよび役割

項目	説明
Windows Group	Windows グループの名前。
Management Role	グループの役割（管理者、ユーザーなど）。

Active Directory および Kerberos 認証の構成

Active Directory 認証を構成すると、Data Domain システムが Windows Active Directory レルムの一部になります。CIFS クライアントと NFS クライアントは Kerberos 認証を使用します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［Active Directory/Kerberos Authentication］パネルを展開します。
3. ［Mode］の隣にある［**Configure...**］をクリックして、構成ウィザードを開始します。

   ［Active Directory/Kerberos Authentication］ダイアログが表示されます。
4. ［**Windows/Active Directory**］を選択し、［**Next**］をクリックします。
5. システムの完全なレルム名（例：domain1.local）、Data Domain システムのユーザー名とパスワードを入力します。その後、［**Next**］をクリックします。

   注

   完全なレルム名を使用します。ユーザーにシステムをドメインに参加させるための権限が割り当てられていることを確認します。ユーザー名とパスワードは、Active Directory ドメインの Microsoft 要件に対応している必要があります。このユーザーは、このドメインにアカウントを作成する権限も割り当てられている必要があります。
6. デフォルトの CIFS サーバー名を選択するか、［**Manual**］を選択して CIFS サーバー名を入力します。
7. ドメイン コントローラーを選択するには、［**Automatically assign**］を選択するか、［**Manual**］を選択して最大 3 個のドメイン コントローラー名を入力します。

   完全修飾ドメイン名、ホスト名、または IP（IPv4 または IPv6）アドレスを入力することができます。
8. 組織単位を選択するには、［**Use default Computers**］を選択するか、［**Manual**］を選択して組織単位名を入力します。

   注

   アカウントは、新しい組織ユニットに移動されます。
9. ［次へ］をクリックします。

   構成の［Summary］ページが表示します。
10. ［**Finish**］をクリックします。

    システムが、［Authentication］ビューに構成情報が表示されます。
11. 管理アクセスを有効化するには、［**Active Directory Administrative Access**］の右側にある［**Enable**］をクリックします。

認証モードの選択

認証モードの選択によって、CIFS および NFS クライアントがサポートされている Active Directory、Workgroup、Kerberos 認証の組み合わせを使用して認証を行う方法が決まります。

DD OS は、次の認証オプションをサポートしています。

- Disabled： CIFS および NFS クライアントの Kerberos 認証は無効です。CIFS クライアントは Workgroup 認証を使用します。
- Windows/Active Directory： CIFS および NFS クライアントの Kerberos 認証は有効です。CIFS クライアントは、Active Directory 認証を使用します。
- UNIX： NFS クライアントのみ Kerberos 認証が有効です。CIFS クライアントは Workgroup 認証を使用します。

Active Directory の管理グループの管理

［Active Directory/Kerberos Authentication］パネルを使用して、Active Directory（Windows）グループを作成、変更、削除したり、作成したグループに管理役割（管理者、バックアップ オペレーターなど）を割り当てることができます。

グループの管理を準備するには、［**Administration** ］ > ［**Access**］ > ［**Authentication**］を選択し、［Active Directory/Kerberos Authentication］パネルを展開して、Active Directory Administrative Access の［**Enable**］ボタンをクリックします。

Active Directory の管理グループの作成

Active Directory グループで構成されたすべてのユーザーに管理役割を割り当てる場合は、管理グループを作成します。

はじめに

［**Administration**］ > ［**Access**］ > ［**Authentication**］ページの［Active Directory/Kerberos Authentication］パネルで、［Active Directory Administrative Access］を有効にします。

手順

1. ［**Create...**］をクリックします。
2. バックスラッシュで区切ったドメイン名とグループ名を入力します。例：domainname \groupname。
3. ドロップダウン メニューからグループの管理役割を選択します。
4. ［**OK**］をクリックします。

Active Directory の管理グループの変更

Active Directory グループ用に構成された管理グループ名または管理役割を変更する場合は、管理グループを変更します。

はじめに

［**Administration**］ > ［**Access**］ > ［**Authentication**］ページの［Active Directory/Kerberos Authentication］パネルで、［Active Directory Administrative Access］を有効にします。

手順

1. ［**Active Directory Administrative Access**］見出しで変更するグループを選択します。
2. ［**Modify...**］をクリックします。
3. ドメイン名とグループ名を変更します。名前は、バックスラッシュで区切られます。例：domainname\groupname。
4. ドロップダウン メニューから異なるロールを選択して、グループの管理役割を変更します。

Active Directory の管理グループの削除

Active Directory グループで構成されたすべてのユーザーのシステム アクセスを終了する場合は、管理グループを削除します。

はじめに

［**Administration**］ > ［**Access**］ > ［**Authentication**］ページの［Active Directory/Kerberos Authentication］パネルで、［Active Directory Administrative Access］を有効にします。

手順

1. ［**Active Directory Administrative Access**］見出しで削除するグループを選択します。
2. ［**Delete**］をクリックします。

UNIX Kerberos 認証の構成

UNIX Kerberos 認証を構成すると、NFS クライアントが Kerberos 認証を使用できるようになります。CIFS クライアントは Workgroup 認証を使用します。

はじめに

UNIX モード Kerberos 認証を機能させるには、NIS が実行中である必要があります。Kerberos の有効化の手順については、NIS サービスの有効化に関するセクションを参照してください。

UNIX 用の Kerberos を構成すると、NFS クライアントが Kerberos 認証を使用できるようになります。CIFS クライアントは Workgroup 認証を使用します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［Active Directory/Kerberos Authentication］パネルを展開します。
3. ［Mode］の隣にある［**Configure...**］をクリックして、構成ウィザードを開始します。

   ［Active Directory/Kerberos Authentication］ダイアログが表示されます。
4. ［**UNIX**］を選択し、［**Next**］をクリックします。
5. レルム名（domain1.local など）、KDC（キー配布センター）用の最大 3 個のホスト名または IP アドレス（IPv4 または IPv6）を入力します。
6. オプションで、［**Browse**］をクリックしてキータブ ファイルをアップロードし、［**Next**］をクリックします。

   構成の［Summary］ページが表示します。

   注

   キータブ ファイルは認証サーバー（KDC）で生成され、KDC サーバーと DDR 間の共有シークレットを含みます。

   通知

   Kerberos 認証が正常に動作するには、キータブ ファイルをアップロードおよびインポートする必要があります。

7. ［**Finish**］をクリックします。

   システムが、［Active Directory/Kerberos Authentication］パネルに構成情報を表示します。

Kerberos 認証の無効化

Kerberos 認証を無効化すると、CIFS および NFS クライアントが Kerberos 認証を使用できなくなります。CIFS クライアントは Workgroup 認証を使用します。

手順

1. ［**Administration**］ > ［**Access Management**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［Active Directory/Kerberos Authentication］パネルを展開します。
3. ［Mode］の隣にある［**Configure...**］をクリックして、構成ウィザードを開始します。

   ［Active Directory/Kerberos Authentication］ダイアログが表示されます。

4. ［**Disabled**］を選択し、［**Next**］をクリックします。

   システムが、変更箇所が太字で表示されるサマリー ページを表示します。

5. ［**Finish**］をクリックします。

   システムが、［Active Directory/Kerberos Authentication］パネルの［Mode］の隣に［Disabled］を表示します。

Workgroup 認証情報の表示

［Workgroup Authentication］パネルを使用して、ワーク グループ構成情報を表示します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。
2. ［Workgroup Authentication］パネルを展開します。

表 44 Workgroup 認証ラベルの説明

項目	説明
モード	認証モードのタイプ（Workgroup または Active Directory）。
ワークグループ名	指定されたワーク グループ
*CIFS サーバー名	使用中の CIFS サーバーの名前
WINS Server	使用中の WINS サーバーの名前

ワークグループ認証パラメーターの構成

ワークグループ認証パラメーターを使用すると、ワークグループ名と CIFS サーバー名を構成できます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［Workgroup Authentication］パネルを展開します。
3. ［**Configure**］をクリックします。

   ［Workgroup Authentication］ダイアログ ボックスが表示されます。

4. ［Workgroup Name］には、［**Manual**］を選択して、追加するワーク グループ名を入力するか、デフォルトを使用します。

   Workgroup モードは、Data Domain システムをワーク グループ ドメインに追加します。

5. ［CIFS Server Name］には、［**Manual**］を選択して、サーバー名（DDR）を入力するか、デフォルトを使用します。
6. ［**OK**］をクリックします。

LDAP 認証情報の表示

［LDAP Authentication］パネルには、LDAP 構成パラメーターおよび LDAP 認証の状態（有効/無効）が表示されます。

LDAP を有効化すれば、既存の OpenLDAP サーバーか Data Domain システムを備えた導入環境を、システムレベルのユーザー認証、NFSv4 ID マッピング、LDAP を使用する NFSv3 Kerberos、または LDAP を使用する NFSv4 Kerberos に使用できます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［LDAP Authentication］パネルを展開します。

結果

表 45 ［LDAP Authentication］パネル項目

項目	説明
LDAP Status	有効または無効。
Base Suffix	LDAP ベース サフィックス。
Bind DN	LDAP サーバーに関連付けられたアカウント名。
SSL	有効または無効。
Server	認証サーバー
LDAP Group	LDAP グループの名前。
Management Role	グループの役割（管理者、ユーザーなど）。

LDAP 認証の有効化と無効化

［LDAP authentication］パネルを使用して、LDAP 認証を有効化、無効化、リセットします。

手順

1. ［**Maintenance**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［LDAP authentication］パネルを展開します。
3. LDAP 認証を有効化するには［LDAP Status］の隣にある［**Enable**］、無効化するには［**Disable**］をクリックします。

   ［Enable or Disable LDAP authentication］ダイアログ ボックスが表示されます。

   注

   LDAP 認証を有効にする前に、LDAP サーバーが存在している必要があります。

4. ［**OK**］をクリックします。

LDAP 認証のリセット

［**Reset**］ボタンにより、LDAP 認証が無効化され、LDAP 構成情報がクリアされます。

LDAP 認証の設定

「LDAP 認証」パネルを使用して、LDAP 認証を構成します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［LDAP Authentication］パネルを展開します。
3. ［**Configure**］をクリックします。

   ［Configure LDAP Authentication］ダイアログ ボックスが表示されます。

4. ［**Base Suffix**］フィールドにベース サフィックスを指定します。
5. ［**Bind DN**］フィールドに、LDAP サーバーに関連付けるアカウント名を指定します。
6. ［**Bind Password**］フィールドで、バインド DN アカウントのパスワードを指定します。
7. 必要に応じて、［**Enable SSL**］を選択します。
8. 必要に応じて、［**Demand server certificate**］を選択して、Data Domain システムに LDAP サーバーから CA 証明書をインポートするよう要求します。
9. ［**OK**］をクリックします。
10. 後で、必要に応じて、［**Reset**］をクリックして LDAP 構成をデフォルト値に戻します。

LDAP 認証サーバーの指定

［LDAP authentication］パネルを使用して、LDAP 認証サーバーを指定します。

はじめに

LDAP サーバーを構成する前に、LDAP 認証を無効にする必要があります。

注

LDAP によるログイン時の DD SM のパフォーマンスは、Data Domain システムと LDAP サーバーの間のホップ数が増えるにつれて低下します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

［Authentication］ビューが表示されます。

2. ［LDAP authentication］パネルを展開します。
3. サーバーを追加するには、［**+**］ボタンをクリックします。
4. LDAP サーバを次の形式で指定します。
   - IPv4 アドレス：`10.26.16.250`
   - IPv6 アドレス：`[::ffff:9.53.96.21]`
   - ホスト名：`myldapserver`
5. ［**OK**］をクリックします。

LDAP グループの構成

［LDAP Authentication］パネルを使用して、LDAP グループを構成します。

LDAP グループ構成は、Data Domain システムでのユーザー認証に LDAP を使用する場合にのみ適用されます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。
2. ［LDAP Authentication］パネルを展開します。
3. ［LDAP Group］テーブルで LDAP グループを構成します。
   - LDAP グループを追加するには、［Add］（［**+**］）をクリックし、LDAP グループの名前と役割を入力して［**OK**］をクリックします。
   - LDAP グループを変更するには、LDAP グループ リストのグループ名のチェックボックスを選択し、［Edit］（鉛筆）をクリックします。LDAP グループ名を変更し、［**OK**］をクリックします。
   - LDAP グループ名を削除するには、リストで LDAP グループを選択し、［Delete］（［**X**］）をクリックします。

CLI（コマンド ライン インターフェイス）を使用して、LDAP 認証を構成します。

Data Domain コマンド ライン インターフェイスを使用して、システム レベルのユーザー認証、NFSv4 ID マッピング、LDAP を使用した NFSv3 Kerberos、または LDAP を使用した NFSv4 Kerberos のために、Data Domain システムを使用した既存の OpenLDAP サーバーまたは導入を構成できます。

LDAP サーバーの構成

同時に 1 台以上の LDAP サーバを構成できます。

注

構成を変更するときは、LDAP を無効にする必要があります。

LDAP サーバを次の形式で指定します。

- IPv4 アドレス：`10.<A>.<B>.<C>`

- IPv4 アドレスとポート番号：**10.<A>.<B>.<C>:400**
- IPv6 アドレス：**[::ffff:9.53.96.21]**
- IPv6 アドレスとポート番号：**[::ffff:9.53.96.21]:400**
- ホスト名：**myldapserver**
- ホスト名とポート番号：**myldapserver:400**

複数のサーバを構成する場合：

- スペースを使用して各サーバを区切ります。
- `authentication ldap servers add` コマンドを使用したときに表示される最初のサーバがプライマリ サーバになります。
- いずれかのサーバを構成できない場合、表示されたすべてのサーバに対するコマンドが失敗します。

手順

1. `authentication ldap servers add` コマンドを使用して 1 台以上の LDAP サーバを追加します。

```
# authentication ldap servers add 10.A.B.C 10.X.Y.Z:400
LDAP server(s) added
LDAP Server(s):        2
#     IP Address/Hostname
---   --------------------
1.    10.A.B.C (primary)
2.    10.X.Y.Z:400
---   --------------------
```

2. `authentication ldap servers del` コマンドを使用して 1 台以上の LDAP サーバを削除します。

```
# authentication ldap servers del 10.X.Y.Z:400
LDAP server(s) deleted.
LDAP Servers: 1
#   Server
-   ------------   ---------
1   10.A.B.C       (primary)
-   ------------   ---------
```

3. `authentication ldap servers reset` コマンドを使用してすべての LDAP サーバを削除します。

```
# authentication ldap servers reset
LDAP server list reset to empty.
```

LDAP ベース サフィックスの設定

ベース サフィックスは検索のベース DN であり、そこから LDAP ディレクトリの検索が開始されます。

手順

1. `authentication ldap base set` コマンドを使用して LDAP ベース サフィックスを設定します。

```
# authentication ldap base set "dc=anvil,dc=team"
LDAP base-suffix set to "dc=anvil,dc=team".
```

2. `authentication ldap base reset` コマンドを使用して LDAP ベース サフィックスをリセットします。

```
# authentication ldap base reset
LDAP base-suffix reset to empty.
```

LDAP クライアント認証の設定

LDAP サーバでの認証やクエリの作成に使用するアカウント（バインド DN）とパスワード（バインド PW）を設定します。

必ずバインド DN およびパスワードを設定する必要があります。通常、LDAP サーバではデフォルトで認証済みのバインドが必要です。`client-auth` が設定されていない場合、ユーザー名またはパスワードを指定しない匿名アクセスが求められます。`authentication ldap show` の出力は、次のようになります。

```
# authentication ldap show
LDAP configuration
        Enabled:          yes (*)
        Base-suffix:      dc=u2,dc=team
        Binddn:           (anonymous)
        Server(s):        1
#   Server
-   -------------   ---------
1   10.207.86.160   (primary)
-   -------------   ---------

Secure LDAP configuration
        SSL Enabled:      no
        SSL Method:       off
        tls_reqcert:      demand

(*) Requires a filesystem restart for the configuration to take
effect.
```

`client-auth` CLI を使用してバインド DN を設定し、バインド PW を指定していない場合は、未認証アクセスが求められます。

```
# authentication ldap client-auth set binddn
"cn=Manager,dc=u2,dc=team"
Enter bindpw:
** Bindpw is not provided. Unauthenticated access would be requested.
LDAP client authentication binddn set to "cn=Manager,dc=u2,dc=team".
```

手順

1. `authentication ldap client-auth set binddn` コマンドを使用してバインド DN およびパスワードを設定します。

   ```
   # authentication ldap client-auth set binddn
   "cn=Administrator,cn=Users,dc=anvil,dc=team"
       Enter bindpw:
       LDAP client authentication binddn set to
   "cn=Administrator,cn=Users,dc=anvil,dc=team".
   ```

2. `authentication ldap client-auth reset` コマンドを使用してバインド DN およびパスワードをリセットします。

   ```
   # authentication ldap client-auth reset
   LDAP client authentication configuration reset to empty.
   ```

LDAP の有効化

はじめに

LDAP を有効にする前に LDAP を設定しておく必要があります。さらに、NIS を無効にして LDAP サーバに到達できることを確認するとともに、LDAP サーバのルート DSE にクエリを行えるようにしておく必要があります。

手順

1. `authentication ldap enable` コマンドを使用して LDAP を有効にします。

```
# authentication ldap enable
```

操作を続行する前に確認できるよう、LDAP の設定の詳細が表示されます。続行するには **yes** と入力し、LDAP の設定を有効にするためにファイル システムを再起動します。

2. `authentication ldap show` コマンドを使用して現在の LDAP の設定を表示します。

```
# authentication ldap show
LDAP configuration
        Enabled:          no
        Base-suffix:      dc=anvil,dc=team
        Binddn:
cn=Administrator,cn=Users,dc=anvil,dc=team
        Server(s):        2
#   Server
-   ----------------    ---------
1   10.26.16.250        (primary)
2   10.26.16.251:400
-   ----------------    ---------

Secure LDAP configuration
        SSL Enabled:      no
        SSL Method:       off
        tls_reqcert:      demand
```

基本的な LDAP とセキュリティで保護された LDAP の設定の詳細が表示されます。

3. `authentication ldap status` コマンドを使用して現在の LDAP のステータスを表示します。

```
# authentication ldap status
```

LDAP のステータスが表示されます。LDAP のステータスが `good` でない場合は、出力に問題が示されます。たとえば、次のように表示されます。

```
# authentication ldap status
Status: invalid credentials
```

または

```
# authentication ldap status
Status: invalid DN syntax
```

4. `authentication ldap disable` コマンドを使用して LDAP を無効にします。

```
# authentication ldap disable
LDAP is disabled.
```

セキュリティで保護された LDAP の有効化

SSL を有効にすると、DDR を設定してセキュリティで保護された LDAP を使用できます。

はじめに

LDAP の CA 証明書がなく、`tls_reqcert` が `demand` に設定されていると、操作が失敗します。その場合は、LDAP の CA 証明書をインポートしてもう一度やり直します。

`tls_reqcert` が `never` に設定されている場合、LDAP の CA 証明書は必要ありません。詳細については、インポートした CA 証明書による LDAP サーバ証明書の検証の設定（130 ページ）を参照してください。

手順

1. `authentication ldap ssl enable` コマンドを使用して SSL を有効にします。

   ```
   # authentication ldap ssl enable
   Secure LDAP is enabled with 'ldaps' method.
   ```

   デフォルトの方法は、セキュリティで保護された LDAP か［ldaps］です。TLS などの別の方法を指定できます。

   ```
   # authentication ldap ssl enable method start_tls
   Secure LDAP is enabled with 'start_tls' method.
   ```

2. `authentication ldap ssl disable` コマンドを使用して SSL を無効にします。

   ```
   # authentication ldap ssl disable
   Secure LDAP is disabled.
   ```

インポートした CA 証明書による LDAP サーバ証明書の検証の設定

TLS リクエスト証明書の動作を変更できます。

手順

1. `authentication ldap ssl set tls_reqcert` コマンドを使用して、TLS リクエスト証明書の動作を変更します。

   証明書を検証しない場合：

   ```
   # authentication ldap ssl set tls_reqcert never
   "tls_reqcert" set to "never". LDAP server certificate will not
   be verified.
   ```

   証明書を検証する場合：

   ```
   # authentication ldap ssl set tls_reqcert demand
   "tls_reqcert" set to "demand". LDAP server certificate will be
   verified.
   ```

2. `authentication ldap ssl reset tls_reqcert` コマンドを使用して、TLS リクエスト証明書の動作をリセットします。デフォルトの動作は `demand` です。

   ```
   # authentication ldap ssl reset tls_reqcert
   tls_reqcert has been set to "demand". LDAP Server certificate
   will be verified with imported CA certificate.Use "adminaccess"
   CLI to import the CA certificate.
   ```

LDAP の CA 証明書の管理

証明書をインポートまたは削除して、現在の証明書の情報を表示できます。

手順

1. `adminaccess certificate import` コマンドを使用して、LDAP サーバ証明書を検証するための CA 証明書をインポートします。

   `ca application` の `ldap` を指定します。

   ```
   # adminaccess certificate import{host application {all | aws-
   federal | ddboost | https| keysecure | rkm | <application-
   list>}| ca application { LDAP }} [file <file-name>] Import host
   or ca certificate
   ```

2. `adminaccess certificate delete` コマンドを使用して、LDAP サーバ証明書を検証するための CA 証明書を削除します。

   `application` の `ldap` を指定します。

```
# adminaccess certificate delete
{ subject <subject-name> | fingerprint <fingerprint>}
[application { LDAP }]
```

`imported-ca application` の `ldap` を指定します。

```
# adminaccess certificate delete
{ imported-host application { all | aws-federal | ddboost |
https
| keysecure | rkm | <application-list>}
| imported-ca application { LDAP }}
```

3. `adminaccess certificate show` コマンドを使用して、LDAP サーバ証明書を検証するための現在の CA 証明書の情報を表示します。

```
# adminaccess certificate show imported-ca ldap
```

NIS 認証情報の表示

［NIS Authentication］パネルには、NIS 構成パラメーターおよび NIS 認証の状態（有効/無効）が表示されます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［NIS Authentication］パネルを展開します。

結果

表 46 ［NIS Authentication］パネル項目

項目	説明
NIS Status	有効または無効。
ドメイン名	このサービスのドメインの名前。
サーバー	認証サーバー
NIS Group	NIS グループの名前。
Management Role	グループの役割（管理者、ユーザーなど）。

NIS 認証の有効化と無効化

［NIS Authentication］パネルを使用して、NIS 認証を有効または無効にします。

手順

1. ［**Maintenance**］ > ［**Access**］ > ［**Authentication**］を選択します。

   ［Authentication］ビューが表示されます。

2. ［NIS Authentication］パネルを展開します。
3. NIS 認証を有効化するには［NIS Status］の隣にある［**Enable**］、無効化するには［**Disable**］をクリックします。

   ［Enable or Disable NIS］ダイアログ ボックスが表示されます。

4. ［**OK**］をクリックします。

NIS ドメイン名の構成

［NIS Authentication］パネルを使用して、NIS ドメイン名を構成します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。
   ［Authentication］ビューが表示されます。
2. ［NIS Authentication］パネルを展開します。
3. NIS ドメイン名を編集するには、［Domain Name］の隣にある［**Edit**］をクリックします。
   ［Configure NIS Domain Name］ダイアログ ボックスが表示されます。
4. ［**Domain Name**］ボックスにドメイン名を入力します。
5. ［**OK**］をクリックします。

NIS 認証サーバーの指定

［NIS Authentication］パネルを使用して、NIS 認証サーバーを指定します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。
   ［Authentication］ビューが表示されます。
2. ［NIS Authentication］パネルを展開します。
3. ドメイン名で、以下のいずれかを選択します。
   - ［**Obtain NIS Servers from DHCP**］：DHCP を使用して自動的に NIS サーバーが取得されます。
   - ［**Manually Configure**］：以下の手順に従い、手動で NIS サーバーを構成します。
   - 認証サーバーを追加するには、サーバー テーブルで［Add］（［**+**］）をクリックして、サーバー名を入力し、［**OK**］をクリックします。
   - 認証サーバーを変更するには、認証サーバー名を選択して、サーバー名を入力し、編集アイコン（鉛筆）をクリックします。サーバー名を変更し、［**OK**］をクリックします。
   - 認証サーバー名を削除するには、サーバーを選択して、［X］アイコンをクリックし、［**OK**］をクリックします。
4. ［**OK**］をクリックします。

NIS グループの構成

［NIS Authentication］パネルを使用して、NIS グループを構成します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。
   ［Authentication］ビューが表示されます。
2. ［NIS Authentication］パネルを展開します。
3. ［NIS Group］テーブルで NIS グループを構成します。
   - NIS グループを追加するには、［Add］（［**+**］）をクリックし、NIS グループの名前と役割を入力して［**Validate**］をクリックします。［**OK**］をクリックして、［add NIS group］ダ

イアログ ボックスを終了します。［**OK**］を再度クリックして、［**Configure Allowed NIS Groups**］ダイアログ ボックスを終了します。

- NIS グループを変更するには、NIS グループ リストの NIS グループ名のチェックボックスを選択し、［Edit］（鉛筆）をクリックします。NIS グループ名を変更し、［**OK**］をクリックします。
- NIS グループ名を削除するには、リストで NIS グループを選択し、［Delete］（［**X**］）をクリックします。

4. ［**OK**］をクリックします。

認証に関する問題の診断

Data Domain Operating System は、Data Domain System Manager のインターフェイス内から Active Directory の認証に関する問題を診断する機能を提供します。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Authentication**］を選択します。
2. ［Active Directory/Kerberos Authentication］パネルを展開します。
3. ［**Diagnose**］をクリックします。
4. 調査する問題を選択し、［**Diagnose**］をクリックします。
5. リクエストされた情報を入力します。

   Active Directory ユーザーとしてログインする問題を診断するには、以下を提供します。

   - Active Directory サーバーの IP アドレス
   - Active Directory サーバーの FQDN
   - Active Directory サービスの

   注

   ユーザー名ここで指定する Active Directory ユーザー アカウントには、次の特権が必要です。

   - ドメイン名によって識別されるベース DN への read-only アクセス。
   - ベース DN 内のすべてのユーザーのクエリ属性に対する read-only アクセス。
   - Data Domain システムのマシン アカウントのクエリ属性に対する read-only アクセス。

   - Active Directory サービス パスワード
   - ログイン障害が発生している Data Domain ユーザー名

   Data Domain システムを Active Directory ドメインに参加させる問題を診断するには、次の情報を提供します。

   - Active Directory サーバーの IP アドレス
   - Active Directory サーバーの FQDN
   - Active Directory サービスのユーザー名
   - Active Directory サービス パスワード

6. ［**Diagnose**］をクリックします。

7. レポートを表示します。
   - ［**View Report**］をクリックして、レポートをオンラインで表示します。［Action Items］表の各アイテムをクリックして、追加の詳細を確認できます。
   - ［**Download**］をクリックして、レポートのコピーをダウンロードします。
8. 問題に対する提案された修正案をレビューして実装し、操作を再試行します。

システムの認証方法の変更

Data Domain システムは、パスワード ベースの認証、または証明書ベースの認証をサポートしています。パスワード ベースの認証がデフォルトの方法となっています。

はじめに

証明書ベースの認証では SSH キーが必要となり、パスワード ベースの認証が無効になったときにユーザーがシステムで認証を行えるよう、CA 証明書がインポートされます。

システムの認証方法をパスワード ベースの認証から証明書ベースの認証に変更するには、次の手順を実行します。

手順

1. ［**Administration**］ > ［**Access**］を選択します。

   ［Access Management］ビューが表示されます。
2. ［**Manage CA Certificates**］をクリックします。
3. ［**Add**］をクリックして新しい証明書を作成します。
4. 証明書を追加します。
   - ［**I want to upload the certificate as a .pem file**］を選択して［**Choose File**］をクリックし、証明書ファイルを選択してシステムにアップロードします。
   - ［**I want to copy and paste the certificate text**］を選択し、証明書のテキストをコピーしてテキスト フィールドにペーストします。
5. ［**Add**］をクリックします。
6. ［**More Tasks**］ > ［**Change Login Options**］を選択します。
7. ［**Password Based Login**］ドロップ ダウン メニューで［**Disable**］を選択します。

   注

   システムで必要な SSH キーと CA 証明書が設定されていない場合は、ドロップ ダウン メニューが無効になっています。
8. ［**OK**］をクリックします。

   セキュリティ ポリシーが設定されている場合は、セキュリティ担当者の認証情報の入力を求められます。認証情報を入力し、［**OK**］をクリックします。

パスワード ベースの認証へのシステムの認証方法のリセット

システムの認証方法を証明書ベースの認証からパスワード ベースの認証に変更するには、次の手順を実行します。

手順

1. ［**Administration**］ > ［**Access**］を選択します。

   ［Access Management］ビューが表示されます。

2. ［**More Tasks**］ > ［**Change Login Options**］を選択します。
3. ［**Password Based Login**］ドロップ ダウン メニューで［**Enable**］を選択します。
4. ［**OK**］をクリックします。

   セキュリティ ポリシーが設定されている場合は、セキュリティ担当者の認証情報の入力を求められます。認証情報を入力し、［**OK**］をクリックします。

メール サーバー設定の構成

［Mail Server］タブでは、DD OS からメール レポートが送信されるメール サーバーを指定できます。

手順

1. ［**Administration**］ > ［**Settings**］ > ［**Mail Server**］を選択します。
2. ［**More Tasks**］ > ［**Set Mail Server**］を選択します。

   ［Set Mail Server］ダイアログ ボックスが表示されます。

3. ［**Mail Server**］フィールドでメール サーバーの名前を指定します。
4. ［**Credentials**］ボタンを使用して、メール サーバーの資格情報の使用を有効または無効にします。
5. 資格情報が有効になっている場合は、［**User Name**］フィールドにメール サーバーのユーザー名を指定します。
6. 資格情報が有効になっている場合は、［**Password**］フィールドにメール サーバーのパスワードを指定します。
7. ［**Set**］をクリックします。
8. 必要に応じて、CLI を使用してメール サーバーの設定を確認およびトラブルシューティングします。
   a. **config show mailserver** コマンドを実行して、メール サーバーが設定されていることを確認します。
   b. メール サーバーに ping するために **net ping <mailserver-hostname> count 4** コマンドを実行します。
   c. メール サーバーが正しく設定されていない場合は、**config set mailserver <mailserver-hostname>**コマンドを実行してメール サーバーを設定し、再度 ping を試行します。
   d. **net show dns** コマンドを実行して、DNS サーバーが構成されていることを確認します。
   e. net ping **の実行 <DNS-hostname> count 4** コマンドを実行して、DNS サーバーに対して ping を実行します。
   f. DNS サーバーが正しく設定されていない場合は、**config set dns <dns-IP>**コマンドを実行して DNS サーバーを設定し、再度 ping を試行します。
   g. 必要に応じて、**net hosts add <IP-address> <hostname>**コマンドを実行して、ローカルで解決するために、Data Domain の hosts ファイルにメール サーバーの IP アドレスとホスト名を追加します。
   h. メール サーバーに ping するために **net ping <mailserver-hostname> count 4** コマンドを実行します。

日付と時刻の設定の管理

［Time and Date Settings］タブでは、システムの日付と時刻を表示および構成したり、ネットワーク タイム プロトコルを構成して、日付と時刻を設定したりできます。

手順

1. 現在の時刻と日付の構成を表示するには、［**Administration**］>［**Settings**］>［**Time and Date Settings**］を選択します。

   ［Time and Date Settings］ページには、現在のシステムの日付と時刻、NTP の状態（有効/無効）が表示され、構成済み NTP サーバーの IP アドレスまたはホスト名がリストされます。

2. 構成を変更するには、［**More Tasks**］ > ［**Configure Time Settings**］を選択します。

   ［Configure Time Settings］ダイアログが表示されます。

3. ［**Time Zone**］ドロップダウン リストで、Data Domain システムが存在するタイム ゾーンを選択します。
4. 手動で日時を設定するには、［**None**］を選択して、［**Date**］ボックスに日付を入力し、［**Time**］ドロップダウン リストから時刻を選択します。
5. NTP を使用して時刻を同期させるには、［NTP］を選択して、NTP サーバーへのアクセス方法を設定します。
   - サーバーの自動選択に DHCP を使用するには、［**Obtain NTP Servers using DHCP**］を選択します。
   - NTP サーバー IP アドレスを構成するには、［**Manually Configure**］を選択して、サーバーの IP アドレスを追加し、［**OK**］をクリックします。

   注

   Active Directory ドメイン コントローラーから時間同期を使用すると、NTP とドメイン コントローラー両方が時間を変更している場合、システムの時間が過剰に変更される可能性があります。

6. ［**OK**］をクリックします。
7. タイム ゾーンを変更した場合、システムを再起動する必要があります。
   a. ［**Maintenance**］ > ［**System**］を選択します。
   b. ［More Tasks］メニューから、［Reboot System］を選択します。
   c. ［OK］をクリックして確定します。

システム プロパティの管理

［System Properties］タブでは、管理対象システムの場所、管理者のメール アドレス、ホスト名を特定するシステム プロパティの表示および構成ができます。

手順

1. 現在の構成を表示するには、［**Administration**］ > ［**Settings**］ > ［**System Properties**］を選択します。

   ［System Properties］タブには、システムの場所、管理者のメール アドレス、管理者のホスト名が表示されます。

2. 構成を変更するには、［**More Tasks**］ > ［**Set System Properties**］を選択します。

   ［Set System Properties］ダイアログ ボックスが表示されます。

3. ［**Location**］ボックスに、Data Domain システムの場所についての情報を入力します。
4. ［**Admin Email**］ボックスに、システム管理者のメール アドレスを入力します。
5. ［**Admin Host**］ボックスに、管理者サーバーの名前を入力します。
6. ［**OK**］をクリックします。

SNMP 管理 SNMP かんり

SNMP（Simple Network Management Protocol）は、ネットワーク管理情報を交換するためのスタンダード プロトコルであり、TCP/IP（Transmission Control Protocol/Internet Protocol）プロトコル スイートの一部です。SNMP には、ネットワーク管理者が Data Domain システムなどのネットワーク接続型デバイスで注意する必要のある状態を管理および監視するためのツールがあります。

SNMP を使用して Data Domain システムを監視するには、SNMP Management システムに Data Domain MIB をインストールする必要があります。DD OS は標準 MIB-II にも対応しているため、ネットワーク統計などの一般データの MIB-II 統計のクエリーにも対応しています。使用可能なデータを完全にカバーするには、Data Domain MIB と標準 MIB-II MIB を両方活用する必要があります。

Data Domain システムの SNMP エージェントは、SNMP v1、v2c、v3 を使用して、管理システムからの Data Domain 固有情報に関するクエリーを受け入れます。SNMP v3 は、クリアテキスト コミュニティ文字列（認証に使用）を、MD5 または SHA1 を使用したユーザー ベースの認証と置き換えることにより、v2c および v1 よりも高度なセキュリティを提供します。また、SNMP v3 のユーザー認証パケットは暗号化することができ、その整合性が DES または AES によって検証されます。

Data Domain システムは、SNMP v2c および SNMP v3 を使用して SNMP トラップ（アラート メッセージ）を送信することができます。SNMP v1 トラップがサポートされていないため、SNMP v2c または v3 の使用を推奨します。

SNMP を有効化すると開かれるデフォルトのポートは、ポート 161 です。トラップはポート 162 で送信されます。

- 「Data Domain オペレーティング システム初期構成ガイド」には、Data Domain システムで SNMP モニタリングを使用するためのセットアップ方法が説明されています。
- Data Domain MIB 分岐に含まれる完全な MIB パラメーターについては、「Data Domain Operating System MIB Quick Reference」を参照してください。

SNMP ステータスおよび構成の表示

［SNMP］タブには、現在の SNMP のステータスと構成が表示されます。

手順

1. ［**Administration**］ > ［**Settings**］ > ［**SNMP**］を選択します。

［SNMP］ビューには、SNMP ステータス、SNMP プロパティ、SNMP V3 構成、SNMP V2C 構成が表示されます。

［SNMP］タブのラベル

［SNMP］タブのラベルでは、SNMP の全体的なステータス、SNMP のプロパティの値、SNMPv3 と SNMPv2 の構成を識別できます。

Status
［Status］領域には、システム上の SNMP エージェントの動作ステータス（「Enabled」または「Disabled」）が表示されます。

SNMP のプロパティ

表 47 SNMP のプロパティの説明

項目	説明
SNMP System Location	監視中の Data Domain システムの場所。
SNMP System Contact	Data Domain システム管理の連絡担当者として指定された者。
SNMP System Notes	（オプション）追加の SNMP 構成データ。
SNMP Engine ID	Data Domain システムの一意の 16 進識別子。

SNMP V3 構成

表 48 SNMP Users 列の説明

項目	説明
Name	Data Domain システムのエージェントにアクセスできる SNMP マネージャー上のユーザーの名前。
Access	SNMP ユーザーのアクセス権限（Read-only または Read-write）。
Authentication Protocols	SNMP ユーザーの確認に使用される Authentication Protocol（MD5、SHA1、または None）。
Privacy Protocol	SNMP ユーザー認証時に使用される暗号化プロトコル（AES、DES、または None）。

表 49 Trap Hosts 列の説明

項目	説明
Host	SNMP 管理ホストの IP アドレスまたはドメイン名。
Port	ホストとの SNMP トラップ通信に使用するポート。たとえば、162 はデフォルトです。
User	Data Domain の SNMP 情報へのアクセスを許可されたトラップ ホスト上のユーザー。

SNMP V2C 構成

表 50 Communities 列の説明

項目	説明
Community	コミュニティ名。public、private、localCommunity などです。
Access	割り当てられたアクセス権限（Read-only または Read-write）。
Hosts	コミュニティ内のホスト。

表 51 Trap Hosts 列の説明

項目	説明
Host	Data Domain システムが生成した SNMP トラップを受信するよう指定されたシステム。このパラメーターが設定されていると、SNMP エージェントが無効になっていても、システムがアラート メッセージを受信します。
Port	ホストとの SNMP トラップ通信に使用するポート。たとえば、162 はデフォルトです。
Community	コミュニティ名。public、private、localCommunity などです。

SNMP の有効化/無効化

［SNMP］タブを使用して、SNMP を有効化または無効化します。

手順

1. ［**Administration** ］ > ［**Settings**］ > ［**SNMP**］を選択します。
2. ［Status］領域で、［**Enable**］または［**Disable**］をクリックします。

SNMP MIB のダウンロード

［SNMP］タブを使用して、SNMP MIB をダウンロードします。

手順

1. ［**Administration**］ > ［**Settings**］ > ［**SNMP**］を選択します。
2. ［**Download MIB file**］をクリックします。
3. ［Opening DATA_DOMAIN.mib］ダイアログ ボックスで、［**Open**］を選択します。
4. ブラウザー ウィンドウで MIB を表示するには、［**Browse**］をクリックし、ブラウザーを選択します。

   注

   Microsoft Internet Explorer ブラウザーを使用する場合、ファイル ダウンロードの自動プロンプトを有効化します。

5. MIB を保存するか、ブラウザーを閉じます。

SNMP プロパティの構成

［SNMP］タブを使用して、システムの場所およびシステムの担当者のテキスト エントリーを構成します。

手順

1. ［**Administration**］ > ［**Settings**］ > ［**SNMP**］を選択します。
2. ［SNMP Properties］領域で、［**Configure**］をクリックします。

   ［SNMP Configuration］ダイアログ ボックスが表示されます。

3. テキスト フィールドに次に示す情報を指定します。
   - ［SNMP System Location］: Data Domain システムの場所の説明。
   - ［SNMP System Contact］: Data Domain システムのシステム管理者のメール アドレス。
   - ［SNMP System Notes］:（オプション）追加の SNMP 構成情報。
   - ［SNMP Engine ID］: SNMP エンティティの一意の識別子。エンジン ID は、5～34 文字の 16 進文字である必要があります（SNMPv3 のみ）。

     注

     SNMP エンジン ID が長さの要件を満たさないか、無効な文字を使用するとエラーが表示されます。

4. ［**OK**］をクリックします。

SNMP V3 ユーザーの管理

［SNMP］タブを使用して、SNMPv3 ユーザーとトラップ ホストを作成、変更、削除します。

SNMP V3 ユーザーの作成

SNMPv3 ユーザーを作成する場合は、ユーザー名を定義し、読み取り専用または読み取り/書き込みアクセス権を指定して、認証プロトコルを選択します。

手順

1. ［**Administration**］ > ［**Settings**］ > ［**SNMP**］を選択します。
2. ［SNMP Users］領域で、［**Create**］をクリックします。

   ［Create SNMP User］ダイアログ ボックスが表示されます。

3. ［**Name**］テキスト フィールドに、Data Domain システム エージェントへのアクセス権を付与するユーザーの名前を入力します。名前は 8 文字以上の長さで指定します。
4. このユーザーの読み取り専用または読み取り/書き込みアクセスを選択します。
5. ユーザーを認証するには、［**Authentication**］を選択します。
   a. MD5 または SHA1 プロトコルを選択します。
   b. ［**Key**］テキストフィールドに認証キーを入力します。
   c. 認証セッションに暗号化を行うには、［**Privacy**］を選択します。

d. AES または DES プロトコルを選択します。

e. [**Key**] テキストフィールドに暗号化キーを入力します。

6. [**OK**] をクリックします。

新しく追加したユーザー アカウントが、[SNMP Users] テーブルに表示されます。

SNMP V3 ユーザーの変更

既存の SNMPv3 ユーザーのアクセス レベル（読み取り専用または読み取り/書き込み）および認証プロトコルを変更できます。

手順

1. [**Administration**] > [**Settings**] > [**SNMP**] を選択します。
2. [**SNMP Users**] 領域で、ユーザーのチェックボックスを選択し、[**Modify**] をクリックします。

[Modify SNMP User] ダイアログ ボックスが開きます。次の設定を追加または変更します。

3. このユーザーの読み取り専用または読み取り/書き込みアクセスを選択します。
4. ユーザーを認証するには、[**Authentication**] を選択します。

a. MD5 または SHA1 プロトコルを選択します。

b. [Key] テキスト フィールドに認証キーを入力します。

c. 認証セッションに暗号化を行うには、[**Privacy**] を選択します。

d. AES または DES プロトコルを選択します。

e. [**Key**] テキストフィールドに暗号化キーを入力します。

5. [**OK**] をクリックします。

このユーザー アカウントの新しい設定が、[SNMP Users] テーブルに表示されます。

SNMP V3 ユーザーの削除

[SNMP] タブを使用して、既存の SNMPv3 ユーザーを削除します。

手順

1. [**Administration**] > [**Settings**] > [**SNMP**] を選択します。
2. [SNMP Users] エリアで、当該ユーザーのチェック ボックスを選択して [**Delete**] をクリックします。

[Delete SNMP Group] ダイアログ ボックスが開きます。

注

[**Delete**] ボタンが無効になっている場合は、選択したユーザーが 1 つまたは複数のトラップ ホストで使用されています。そのトラップ ホストを削除してから、ユーザーを削除します。

---

3. 削除するユーザーの名前を確認して [**OK**] をクリックします。
4. [Delete SNMP User Status] ダイアログ ボックスで、[**Close**] をクリックします。

［SNMP Users］テーブルからユーザー アカウントが削除されます。

SNMP V2C Community の管理

SNMP V2C Community（パスワードとして機能）を定義して、Data Domain システムへの管理システムのアクセスを制御します。指定されたコミュニティを使用する特定のホストへのアクセスを制限するには、それらのホストを対象コミュニティに割り当てます。

注

SNMP V2C Community 文字列はクリアテキスト形式で送信され、インターセプトが非常に容易です。これが発生した場合、インターセプターがネットワーク上のデバイスから情報を取得して、構成を変更し、場合によってはシャットダウンできます。SNMP V3 は、インターセプトを防止する認証および暗号化機能を提供します。

注

SNMP コミュニティの定義では、管理ステーションへの SNMP トラップの転送は有効になりません。管理ステーションへのトラップの送信を有効にするには、トラップ ホストを定義する必要があります。

SNMP V2C Community の作成

コミュニティを作成して、DDR システムへのアクセス、またはトラップ ホストにトラップを送信する際に使用するアクセスを制限します。トラップ ホストとともに使用するコミュニティを選択する前に、コミュニティを作成してホストに割り当てる必要があります。

手順

1. ［**Administration**］ > ［**Settings**］ > ［**SNMP**］を選択します。
2. ［Communities］領域で、［**Create**］をクリックします。

   ［Create SNMP V2C Community］ダイアログ ボックスが開きます。
3. ［**Community**］ボックスで、Data Domain システム エージェントへのアクセスを許可するコミュニティの名前を入力します。
4. このコミュニティの読み取り専用または読み取り/書き込みアクセスを選択します。
5. コミュニティを 1 つ以上のホストに関連づける場合は、次のようにホストを追加します。
   a. ホストを追加するには、［**+**］をクリックします。

      ［Host］ダイアログ ボックスが表示されます。
   b. ［**Host**］テキスト フィールドで、ホストの IP アドレスまたはドメイン名を入力します。
   c. ［**OK**］をクリックします。

      ［Host］がホスト リストに追加されます。
6. ［**OK**］をクリックします。

   新しいコミュニティ エントリーが［**Communities**］テーブルに表示され、選択したホストが表示されます。

SNMP V2C Community の変更

手順

1. ［**Administration**］ > ［**Settings**］ > ［**SNMP**］を選択します。
2. ［Communities］領域で、コミュニティのチェックボックスを選択し、［**Modify**］をクリックします。

   ［Modify SNMP V2C Community］ダイアログ ボックスが開きます。

3. このコミュニティのアクセス モードを変更するには、［**read-only**］または［**read-write**］アクセスを選択します。

   注

   同じシステム上のトラップ ホストがそのコミュニティの一部として構成された場合、選択されたコミュニティの［Access］ボタンは無効になります。アクセス設定を変更するには、トラップ ホストを削除し、コミュニティの変更後に追加し直します。

4. 1 つまたは複数のホストをこのコミュニティに追加するには、次の手順を行います。
   a. ホストを追加するには、［**+**］をクリックします。

      ［Host］ダイアログ ボックスが表示されます。

   b. ［**Host**］テキスト フィールドで、ホストの IP アドレスまたはドメイン名を入力します。
   c. ［**OK**］をクリックします。

      ［Host］がホスト リストに追加されます。

5. 1 つまたは複数のホストをホスト リストから削除するには、次の手順を行います。

   注

   DD System Manager では、同一システム上のトラップ ホストが対象コミュニティの一部として構成されている場合、ホストを削除できません。コミュニティからトラップ ホストを削除するには、そのトラップ ホストを削除し、コミュニティの変更後に追加し直します。

   注

   トラップ ホストが IPv6 アドレスを使用しており、システムが IPv6 に対応していない以前の DD OS バージョンで管理されている場合、選択されたコミュニティの［Access］ボタンは無効になりません。管理対象システムと同じか、新しいバージョンの DD OS を使用している管理システムを常に選択することをお勧めします。

   a. 各ホストのチェックボックスを選択するか、テーブルの先頭にある［Host］チェックボックスをクリックして、リストされているすべてのホストを選択します。
   b. 削除ボタン（X）をクリックします。
6. ホスト名を編集するには、次の手順を行います。
   a. 対象ホストのチェックボックスを選択します。
   b. 編集ボタン（鉛筆アイコン）をクリックします。
   c. ホスト名を編集します。

d. [**OK**] をクリックします。

7. [**OK**] をクリックします。

   変更されたコミュニティ エントリーが、[Communities] テーブルに表示されます。

SNMP V2C Community の削除

[SNMP] タブを使用して、既存の SNMPv2 コミュニティを削除します。

手順

1. [**Administration**] > [**Settings**] > [**SNMP**] を選択します。
2. [**Communities**] 領域で、コミュニティのチェックボックスを選択し、[**Delete**] をクリックします。

   [Delete SNMP V2C Community] ダイアログ ボックスが表示されます。

   注

   [**Delete**] ボタンが無効になっている場合は、選択したコミュニティが 1 つまたは複数のトラップ ホストで使用されています。そのトラップ ホストを削除してから、コミュニティを削除します。

3. 削除するコミュニティの名前を確認して [**OK**] をクリックします。
4. [Delete SNMP V2C Communities Status] ダイアログ ボックスで、[**Close**] をクリックします。コミュニティのエントリーが [Communities] テーブルから削除されます。

SNMP トラップ ホストの管理

トラップ ホストの定義により、Data Domain システムから SNMP 管理ステーションに、SNMP トラップ メッセージ形式でアラート メッセージを送信可能になります。

SNMP V3 および V2C トラップ ホストの作成

トラップ ホストの定義により、システムから SNMP トラップ メッセージを受信するリモート ホストが特定されます。

はじめに

既存の SNMP V2C Community をトラップ ホストに割り当てる予定の場合は、まず [Communities] 領域を使用して、そのトラップ ホストをコミュニティに割り当てる必要があります。

手順

1. [**Administration**] > [**Settings**] > [**SNMP**] を選択します。
2. [SNMP V3 Trap Hosts] または [SNMP V2C Trap Hosts] 領域で、[**Create**] をクリックします。

   [Create SNMP [V3 or V2C] Trap Hosts] ダイアログが表示されます。

3. [**Host**] ボックスに、トラップを受信する SNMP ホストの IP アドレスまたはドメイン名を入力します。
4. [**Port**] ボックスに、トラップ送信用のポート番号を入力します（ポート 162 は共有ポートです）。
5. ドロップダウン メニューからユーザー（SNMP V3）またはコミュニティ（SNMP V2C）を選択します。

注

［Community］リストには、トラップ ホストがすでに割り当てられているコミュニティのみ表示されます。

6. 新しいコミュニティを作成するには、次の手順を行います。
   a. ［Community］ドロップダウン メニューで、［**Create New Community**］を選択します。
   b. ［**Community**］ボックスに、新しいコミュニティの名前を入力します。
   c. アクセス タイプを選択します。
   d. ［Add］（+）ボタンをクリックします。
   e. トラップ ホスト名を入力します。
   f. ［**OK**］をクリックします。
   g. ［**OK**］をクリックします。
7. ［**OK**］をクリックします。

SNMP V3 および V2C トラップ ホストの変更

既存のトラップ ホスト構成のポート番号とコミュニティの選択を変更できます。

手順

1. ［**Administration**］ > ［**Settings**］ > ［**SNMP**］を選択します。
2. ［**SNMP V3 Trap Hosts**］または［**SNMP V2C Trap Hosts**］領域で、Trap Host エントリーを選択し、［**Modify**］をクリックします。

   ［Modify SNMP [V3 or V2C] Trap Hosts］ダイアログ ボックスが表示されます。

3. ポート番号を変更するには、［**Port**］ボックスに新しいポート番号を入力します（ポート 162 は共有ポート）。
4. ドロップダウン メニューからユーザー（SNMP V3）またはコミュニティ（SNMP V2C）を選択します。

注

［Community］リストには、トラップ ホストがすでに割り当てられているコミュニティのみ表示されます。

5. 新しいコミュニティを作成するには、次の手順を行います。
   a. ［Community］ドロップダウン メニューで、［**Create New Community**］を選択します。
   b. ［**Community**］ボックスに、新しいコミュニティの名前を入力します。
   c. アクセス タイプを選択します。
   d. ［Add］（+）ボタンをクリックします。
   e. トラップ ホスト名を入力します。
   f. ［**OK**］をクリックします。

g. [**OK**] をクリックします。

6. [**OK**] をクリックします。

SNMP V3 および V2C トラップ ホストの削除

[SNMP] タブを使用して、既存のトラップ ホスト構成を削除します。

手順

1. [**Administration**] > [**Settings**] > [**SNMP**] を選択します。
2. (V3 または V2C の) [**Trap Hosts**] 領域で、トラップ ホストのチェックボックスを選択し、[**Delete**] をクリックします。

   [Delete SNMP [V3 or V2C] Trap Hosts] ダイアログ ボックスが表示されます。

3. 削除するホスト名を確認し、[**OK**] をクリックします。
4. [Delete SNMP [V3 or V2C] Trap Hosts Status] ダイアログ ボックスで、[**Close**] をクリックします。

   トラップ ホスト エントリーが、[**Trap Hosts**] テーブルから削除されます。

自動サポート レポートの管理

自動サポート機能では、ASUP というレポートが生成されます。ASUP には、システム識別情報、多くの Data Domain システム コマンドからの統合出力、さまざまなログ ファイルからのエントリーが表示されます。レポートの最後には、広範かつ詳細な内部統計が表示されます。このレポートは、システムの問題のデバッグ時に Data Domain Support をサポートするように設計されています。

ASUP は、ファイル システムの起動時 (通常は 1 日 1 回) に毎回生成されます。ただし、ファイル システムは日に複数回起動することができます。

日次の ASUP レポートを受け取るようにメール アドレスを構成し、Data Domain への ASUP レポートの送信を有効化または無効化できます。日次の ASUP のデフォルトの送信時刻は午前 6:00 ですが、構成可能です。ASUP を Data Domain に送信する場合、従来のセキュリティ保護のない方式か、転送前に情報が暗号化される ConnectEMC 方式を選択できます。

HA システムの自動サポートとサポート バンドルの管理性

構成はアクティブ ノードで実行され、スタンバイ ノードにミラーリングされます。そのため、両方のノードの構成は同じになりますが、統合 ASUP とサポート バンドルはありません。

アクティブ ノードでの自動サポートとサポート バンドルには、ファイル システム、レプリケーション、プロトコル、完全な HA 情報、ローカル ノード情報が含まれます。スタンバイ ノードでの自動サポートとサポート バンドルには、ローカル ノード情報と一部の HA 情報 (構成とステータス) が含まれますが、ファイル システム、レプリケーション、プロトコル情報は含まれません。HA システムのステータス (ファイル システム、レプリケーション、プロトコル、HA 構成) に関連する問題をデバッグするには、両方のノードの自動サポートおよびサポート バンドルが必要です。

Data Domain への自動サポート レポートの有効化および無効化

Data Domain への自動サポート レポートは、アラートが Data Domain に送信されるかどうかとは無関係に、有効化または無効化できます。

手順

1. 自動サポート レポートのステータスを表示するには、[**Maintenance**] > [**Support**] > [**Autosupport**] を選択します。

［Support］領域の［Scheduled auto support］ラベルの隣にある自動サポート レポートのステータスがハイライト表示されます。現在の構成に応じて、［**Enable**］または［**Disable**］ボタンが［Scheduled auto support］行に表示されます。

2. Data Domain への自動サポート レポートを有効化するには、［Scheduled auto support］行で［**Enable**］をクリックします。
3. Domain への自動サポート レポートを無効化するには、［Scheduled auto support］行で［**Disable**］をクリックします。

生成された自動サポート レポートの確認

自動サポート レポートを確認して、過去に収集されたシステム統計および構成情報を確認します。システムには、最大 14 個の自動サポート レポートが格納されます。

手順

1. ［**Maintenance**］ > ［**Support**］ > ［**Autosupport**］を選択します。

   ［Autosupport Reports］ページに、自動サポート レポート ファイル名およびファイル サイズ、レポートが生成された日付が表示されます。レポートは自動的に命名されます。最新のレポートは autosupport、前日のものは autosupport.1 となり、レポートが過去にさかのぼるにつれ数字が増えます。

   ［**CLI** 相当機能］

   ```
   # autosupport show history
   ```

2. テキスト エディターを使用してレポートを表示するには、ファイル名リンクをクリックします。ブラウザーでそれを行うことが必要である場合、まずファイルをダウンロードします。

自動サポート メーリング リストの構成

自動サポート メーリング リストのサブスクライバーは、メールを通じて自動サポート メッセージを受け取ります。［Autosupport］タブを使用して、サブスクライバーを追加、変更、削除します。

自動サポート メールは、自動サポート メール リストのすべてのサブスクライバーに構成されたメール サーバーを通して送信されます。メール サーバーと自動サポート メール リストを構成した後、自動サポート メッセージが意図した宛先に到達するようにするため、セットアップをテストすることを推奨します。

手順

1. ［**Maintenance**］ > ［**Support**］ > ［**Autosupport**］を選択します。
2. ［**Configure**］をクリックします。

   ［Configure Autosupport Subscribers］ダイアログ ボックスが表示されます。

3. サブスクライバーを追加するには、以下の手順に従います。
   a. ［Add］（［**+**］）をクリックします。

      ［Email］ダイアログ ボックスが表示されます。

   b. ［Email］ボックスに受信者メール アドレスを入力します。
   c. OK をクリックします。

   ［**CLI** 相当機能］

   ```
   # autosupport add asup-detailed emails djones@company.com # autosupport add alert-summary emails djones@company.com
   ```

4. サブスクライバーを削除するには、以下の手順に従います。
   a. [Configure Autosupport Subscribers] ダイアログ ボックスに、削除するサブスクライバーを選択します。
   b. [**Delete**] ([X]) をクリックします。

   [**CLI** 相当機能]

   ```
   # autosupport del asup-detailed emails djones@company.com # autosupport del alert-summary emails djones@company.com
   ```

5. サブスクライバー メール アドレスを変更するには、以下の手順に従います。
   a. [Configure Autosupport Subscribers] ダイアログ ボックスに、編集するサブスクライバー名を選択します。
   b. [Modify] (鉛筆アイコン) をクリックします。

      [Email] ダイアログ ボックスが表示されます。
   c. 必要に応じて、メール アドレスを変更します。
   d. OK をクリックします。
6. [**OK**] をクリックして、[Configure Autosupport Subscribers] ダイアログ ボックスを閉じます。

   変更された自動サポート メール リストが、[Autosupport Mailing List] 領域に表示されます。

Data Domain が外部の受信者に ASUP とアラートのメールを送信できることを確認する

外部のメール受信者が、Data Domain デバイスから送信した ASUP (autosupport) およびアラートのメールを受信できることを確認します。

ASUP (autosupport) が Exchange サーバーによってリレーされていることを確認します。

手順

1. ASUP をローカル メール アドレス、つまり同じメール サーバー上のメール アドレスに送信できることを確認します。

   ```
   # autosupport send [internal-email-addr]
   ```

2. ASUP をローカル メール サーバーの外部のメール アドレスに送信できることを確認します。

   ```
   # autosupport send [external email-addr]
   ```

3. メールがメール サーバーの外部メール アドレスに届かない場合は、次のようなエラーが表示されることがあります。

   ```
   **** Unable to send message: (errno 51: Unrecoverable errors from server--giving up)
   ```

   この場合、通常は、KB 資料「Configure Email Relay on MS Exchange」(https://support.emc.com/kb/181900) に記載されているステップを使用して、ローカル メール サーバー上で Data Domain システムに対して転送を有効にする必要があります。
4. ASUP が外部のメール アドレスに送信されても、Data Domain に届いていない場合は、ファイアウォール設定またはスパム フィルターに問題がある可能性があります。
5. ASUP アラートが Data Domain に届いているが、ケースが作成されていない場合は、アラート メールの件名または本文に無効な文字がある可能性があります。確認方法は次のとおりです。

a. 現在の autosupport で HOSTNAME、SYSTEM_ID、LOCATION を調べて、単一引用符、アポストロフィを確認します。これは無効な文字であり、DD OS バージョン 4.9.2.0 以前では削除する必要があります。

```
Example:


==========  GENERAL INFO  ==========
GENERATED_ON=Thu Apr 28 06:54:55 PDT 2011


VERSION=Data Domain OS 4.9.2.6-226914
SYSTEM_ID=7FP5105000


MODEL_NO=DD510
HOSTNAME=system.datadomain.com


LOCATION=123 O Malley Lane
```

b. システムの HOSTNAME または LOCATION または両方から無効な文字をすべて削除します。次のコマンドがあります。

```
net set hostname <host>

config set location "location"
```

c. アラートをシミュレートして、新しい設定をテストします。最も簡単な方法は、スペア ディスク ドライブを手動で障害状態にし、アラートが送信されたことを確認し、同じドライブをすぐに障害解除してスペアの状態に戻すことです。

サポート バンドルの管理

サポート バンドルは、システム構成と運用情報を含むファイルです。ソフトウェア アップグレードまたはシステム トポロジーの変更（コントローラー アップグレードなど）を行う前に、サポート バンドルを作成することを推奨します。

Data Domain Support は、多くの場合、サポートを提供する際にサポート バンドルを要求します。

KB 記事「How to collect/upload a support bundle (SUB) from a Data Domain Restorer (DDR)」（https://support.emc.com/kb/180563）で、サポート バンドルの操作に関する追加情報を提供しています。

サポート バンドルの生成

問題のトラブルシューティングの際、Data Domain カスタマー サポートは、オートサポート ヘッダーを特定する README ファイルとともに tar-g で圧縮したログ ファイルであるサポート バンドルを要求することがあります。

手順

1. ［**Maintenance**］ > ［**Support**］ > ［**Support Bundles**］を選択します。
2. ［**Generate Support Bundle**］をクリックします。

注

システムは、最大 5 個のサポート バンドルに対応しています。6 番目のサポート バンドルを生成しようとすると、自動的に最も古いサポート バンドルが削除されます。CLI コマンド `support bundle delete` を使用して、サポート バンドルを削除することもできます。

また、古い形式 `support-bundle.tar.gz` を使用して命名されたサポート バンドルを含む、アップグレード済みのシステムでサポート バンドルを生成する場合、そのファイルは新しい名前形式を使用するように名称変更されます。

3. ファイルをカスタマー サポート（support@emc.com）までメールで送付します。

注

バンドルが大きすぎてメールできない場合は、オンライン サポート サイトでバンドルをアップロードしてください。https://support.emc.com に移動します。

サポート バンドル リストの表示

［Support Bundles］タブを使用して、システム上のサポート バンドル ファイルを表示します。

手順

1. ［**Maintenance**］ > ［**Support**］ > ［**Support Bundles**］を選択します。

   サポート バンドル リストが表示されます。

   サポート バンドル ファイル名、ファイル サイズ、バンドルの作成日がリストされます。バンドルは、自動的に `hostname-support-bundle-datestamp.tar.gz` の形式で命名されます。たとえば、ファイル名が `localhost-support-bundle-1127103633.tar.gz` の場合、サポート バンドルが 11 月 27 日の 10:36:33 にローカル ホスト システム上に作成されたことを示しています。

2. ファイル名リンクをクリックし、gz/tar 解凍ツールを選択してバンドルの ASCII コンテンツを表示します。

コアダンプの管理

コアダンプが原因で DD OS がクラッシュすると、その問題について説明するコア ファイルが `/ddvar/core` ディレクトリに作成されます。このファイルは容量が大きく、Data Domain システムからコピーするのが難しい場合があります。

コア ファイルの容量が大きすぎて Data Domain システムからコピーできない場合は、**`support coredump split <filename> by <n> {MiB|GiB}`**コマンドを実行します。

- <filename>は`/ddvar/core` ディレクトリのコア ファイルの名前です
- <n>はコア ファイルを分割して生成する小さいチャンクの数です

注

1 つのコア ファイルは、最大 20 個のチャンクに分割できます。指定したサイズによってチャンクの数が 20 個を超えると、エラーが発生してコマンドが失敗します。

たとえば、`cpmdb.core.19297.1517443767` という名前の 42.1 MB のコア ファイルを 10 MB のチャンクに分割すると、5 個のチャンクが生成されます。

```
# support coredump split cpmdb.core.19297.1517443767 10 MiB
cpmdb.core.19297.1517443767 will be split into 5 chunks.
Splitting...

The md5 and split chunks of cpmdb.core.19297.1517443767:
File                                Size       Time Created
---------------------------------   --------   ------------------------
cpmdb.core.19297.1517443767_5_01    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_02    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_03    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_04    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_05    2.1 MiB    Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767.md5     0 MiB      Mon Feb  5 11:50:58 2018
---------------------------------   --------   ------------------------
Download the files as soon as possible. Otherwise they will be automatically delete in 48
hours.
```

support coredump save <file-list>コマンドを実行して、指定されたコアダンプ ファイルを USB ドライブに保存します。

アラート通知の管理

アラート機能は、構成可能なメール リストと Data Domain に配布できるイベント レポートおよびサマリー イベントを生成します。

イベント レポートはすぐに送信され、システム イベントに関する詳細情報を提示します。イベント アラートの配布リストは、［通知グループ］と呼ばれます。1 個以上のメール アドレスを含むように通知グループを構成できます。また、そのアドレスに送信されるイベント レポートのタイプと重大度レベルを構成できます。たとえば、クリティカル イベントについて知る必要があるユーザーの通知グループとクリティカルでないイベントを監視するユーザーの別のグループを構成できます。さまざまな技術のグループを構成することもできます。たとえば、すべてのネットワーク イベントについての E メール メッセージを受信する通知グループ 1 組とストレージの問題についてのメッセージを受信する他のグループ 1 組を構成できます。

サマリー レポートは毎日送信されます。このレポートには、過去 24 時間に発生したイベントのサマリーが記載されています。サマリー レポートには、イベント レポートで提供されるすべての情報は含まれません。日次レポートのデフォルト生成時間は午前 8:00 ですが、変更できます。サマリー レポートは、イベント通知グループとは異なる専用のメール リストを使用して送信されます。

Data Domain へのアラート配布を有効化または無効化することができます。レポートを Data Domain に送信する場合は、従来のセキュリティ保護されない方法、またはセキュア リモート サービスでセキュリティ保護される転送方法を選択できます。

HA システム アラート通知の管理

HA システムのアラート機能では、非 HA システムと同様のイベントおよびサマリー レポートが生成されますが、HA システムがこれらのアラートを管理する方法は、2 ノード システム設定のため異なります。

アラートの初期構成は、アクティブ ノードで完了し、スタンバイ ノードにミラーリングされます（つまり、両方のノードで同じ構成になります）。ローカル アラートおよび AM アラートは、通知設定に従って電子メールにより送信されます。メールには、HA システムからのアラートであることと、アラートを生成したのがどちらのノード（アクティブまたはスタンバイ）であるかを示す情報が含まれています。

フェイルオーバーが発生したときに、ファイル システム、レプリケーション、またはプロトコルに関するアクティブなアラートがある場合、そのアクティブ アラートは、アラートの条件がクリアされない限り、フェイルオーバー後の新しいアクティブ ノードにも引き続き表示されます。

ファイル システム、レプリケーション、およびプロトコルに関する過去のアラートは、フェイルオーバー時にファイル システムとともにフェイルオーバーするのではなく、発生元のノードにとどまります。つまり、ア

クティブ ノードの CLI には、ファイル システム、レプリケーション、プロトコルに関する過去のアラートを完全な形で継続的に表示する機能はありません。

フェイルオーバー時、過去のローカル アラートは発生元のノードにとどまりますが、ファイル システム、レプリケーション、およびプロトコル用の過去のアラート（いわゆる「論理アラート」）は、ファイル システムと一緒にフェイルオーバーします。

注

［**Health**］ > ［**High Availability**］パネルには、HA に関連するアラートのみが表示されます。これらのアラートは、HA Manager、Node、Interconnect、Storage、SAS 接続などの主要な HA コンポーネントによってフィルタリングできます。

通知グループ リストの表示

通知グループは、アラート タイプのセット（クラス）と、メール アドレスのグループ（サブスクライバー）を定義します。システムによって通知リストで選択されたアラート タイプが生成されると、毎回そのアラートがリストのサブスクライバーに送信されます。

手順

1. ［**Health**］ > ［**Alerts**］ > ［**Notification**］を選択します。

   ［**CLI** 相当機能］

   ```
   # alerts notify-list show
   ```

2. ［Group Name］リストのエントリーを制限（フィルタリング）するには、［Group Name］ボックスにグループ名を入力するか、［Alert Email］ボックスにサブスクライバー メールを入力し、［**Update**］をクリックします。

   注

   ［**Reset**］をクリックすると、すべての構成済みグループが表示されます。

3. グループの詳細を表示するには、［Group Name］リストのグループを選択します。

［Notification］タブ

［Notification］タブを使用すると、ユーザーが選択したアラート タイプと重大度レベルのシステム アラートを受信するメール アドレスのグループを構成できます。

表 52 グループ名リスト、列ラベルの説明

項目	説明
グループ名	グループの構成名。
クラス	グループに報告されるアラート クラスの数。
Subscribers	メールで通知を受信するように構成されているサブスクライバーの数。

表 53 詳細情報、ラベルの説明

項目	説明
Class	アラートを転送可能なサービスまたはサブシステム。リストされているクラスは、通知グループがアラートを受信するクラスです。

表 53 詳細情報、ラベルの説明 （続き）

項目	説明
重大度	通知グループへのメールをトリガーする重大度レベル。指定された重大度以上のレベルのアラートはすべて通知グループに送信されます。
Subscribers	サブスクライバー領域には、通知グループに対して構成されているすべてのメール アドレスのリストが表示されます。

表 54 ［Notification］タブのコントロール

Control	説明
［Add］ボタン	［**Add**］ ボタンをクリックして、通知グループの作成を開始します。
［Class Attributes Configure］ボタン	このボタンをクリックして、選択した通知グループに対して生成されるアラートのクラスと重大度レベルを変更します。
［Delete］ボタン	［**Delete**］ボタンをクリックして、選択した通知グループを削除します。
［Filter By: Alert Email］ボックス	このボックスにテキストを入力し、グループ名リストのエントリーを、指定したテキストが含まれているメール アドレスを含んでいるグループに制限します。
［Filter By: Group Name］ボックス	このボックスにテキストを入力し、グループ名リストのエントリーを指定したテキストが含まれているグループ名に制限します。
［Modify］ボタン	［**Modify**］ ボタンをクリックして、選択した通知グループの構成を変更します。
［Reset］ ボタン	このボタンをクリックして、各［Filter By］ボックスのエントリーをすべて削除して、すべてのグループ名を表示します。
［Subscribers Configure］ボタン	このボタンをクリックして、選択した通知グループのメール リストを変更します。
［Update］ボタン	フィルター ボックスにテキストを入力した後に、このボタンをクリックして、グループ名リストを更新します。

通知グループの作成

［Notification］タブを使用して、通知グループを追加し、各グループの重大度のレベルを選択します。

手順

1. ［**Health**］ > ［**Alerts**］ > ［**Notification**］を選択します。
2. ［**Add**］をクリックします。

   ［Add Group］ダイアログ ボックスが開きます。

3. ［**Group Name**］ボックスにグループ名を入力します。

4. 通知されるアラート クラスのチェックボックスを選択します。
5. クラスのデフォルト重大度レベル（Warning）を変更するには、関連づけられたリスト ボックスで他のレベルを選択します。

   重大度レベルは、重大度レベルの昇順で一覧表示されます。［Emergency］は最高の重大度レベルです。
6. ［**OK**］をクリックします。

   ［**CLI** 相当機能］

```
# alerts notify-list create eng_grp class hardwareFailure
```

グループのサブスクライバー リストの管理

［Notification］タブを使用して、通知グループ サブスクライバー リストからメール アドレスを追加、変更、削除します。

手順

1. ［**Health**］ > ［**Alerts**］ > ［**Notification**］を選択します。
2. ［Notifications］グループ リストでグループのチェックボックスを選択し、次のいずれかを行います。
   - ［**Modify**］をクリックし、［**Subscribers**］を選択します。
   - ［Subscribers］リストで、［**Configure**］をクリックします。
3. サブスクライバーをグループに追加するには、以下の手順に従います。
   a. ［**+**］アイコンをクリックします。

      ［Email Address］ダイアログ ボックスが表示されます。

   b. サブスクライバーのメール アドレスを入力します。

   c. ［**OK**］をクリックします。

      ［**CLI** 相当機能］

```
 # alerts notify-list add eng_lab emails
mlee@urcompany.com,bob@urcompany.com
```

4. メール アドレスを変更するには、次の操作を行います。
   a. ［**Subscriber Email**］リストでメール アドレスのチェックボックスをクリックします。

   b. 鉛筆アイコンをクリックします。

   c. ［Email Address］ボックスでメール アドレスを編集します。

   d. ［**OK**］をクリックします。
5. メール アドレスを削除するには、［**Subscriber Email**］リストでメール アドレスのチェックボックスをクリックし、［**X**］アイコンをクリックします。

   ［**CLI** 相当機能］

```
# alerts notify-list del eng_lab emails bob@urcompany.com
```

6. ［**Finish**］または［**OK**］をクリックします。

通知グループの変更

［Notification］テーブルを使用して、既存グループの属性クラスを変更します。

手順

1. ［**Health**］ > ［**Alerts**］ > ［**Notification**］を選択します。
2. グループ リストで変更するグループのチェックボックスを選択します。
3. グループのクラス属性を変更するには、次の操作を行います。
   a. ［Class Attributes］エリアで、［**Configure**］をクリックします。

      Edit Group ダイアログ ボックスが表示されます。

   b. 1 個以上のクラス属性のチェックボックスを選択（またはクリア）します。
   c. クラス属性の重大度レベルを変更するには、対応するリスト ボックスからレベルを選択します。
   d. ［**OK**］をクリックします。

      ［**CLI** 相当機能］

      ```
      # alerts notify-list add eng_lab class cloud severity warning
      # alerts notify-list del eng_lab class cloud severity notice
      ```

4. グループのサブスクライバー リストを変更するには、次の操作を行います。
   a. ［Subscribers］領域で、［**Configure**］をクリックします。

      ［Edit Subscribers］ダイアログ ボックスが開きます。

   b. グループ リストからサブスクライバーを削除するには、サブスクライバーのチェックボックスを選択し、［Delete］アイコン（［X］）をクリックします。
   c. サブスクライバーを追加するには、［Add］アイコン［+］をクリックして、サブスクライバーのメール アドレスを入力し、［OK］をクリックします。
   d. ［**OK**］をクリックします。

      ［**CLI** 相当機能］

      ```
      # alerts notify-list add eng_lab emails
      mlee@urcompany.com,bob@urcompany.com
      # alerts notify-list del eng_lab emails bob@urcompany.com
      ```

5. ［**OK**］をクリックします。

通知グループの削除

［Notification］タブを使用して、既存の 1 つ以上の通知グループを削除します。

手順

1. ［**Health**］ > ［**Alerts**］ > ［**Notification**］を選択します。
2. ［Notifications］グループ リストでグループのチェックボックスを 1 個以上選択し、［**Delete**］をクリックします。

   ［Delete Group］ダイアログ ボックスが開きます。

3. 削除を確認し、［**OK**］をクリックします。

   ［**CLI** 相当機能］

   ```
   # alerts notify-list destroy eng_grp
   ```

通知グループ構成のリセット

［Notification］タブを使用して、Default グループに追加されたすべての通知グループを削除し、Default グループに加えられたすべての変更を削除します。

手順

1. ［**Health**］ > ［**Alerts**］ > ［**Notification**］を選択します。
2. ［**More Tasks**］ > ［**Reset Notification Groups**］を選択します。
3. ［Reset Notification Groups］ダイアログ ボックスでは、検証ダイアログで［**Yes**］をクリックします。

   ［**CLI** 相当機能］

   ```
   # alerts notify-list reset
   ```

日次サマリー スケジュールと配布リストの構成

毎日、各管理対象システムが、alertssummary.list メール グループに構成された Daily Alert Summary メールをサブスクライバーに送信します。Daily Alert Summary メールには、すぐに対応するのが望ましい重要ではないハードウェアの状況とディスク領域の使用数に関するメッセージが表示される現在および過去のアラートが含まれています。

ファンの障害は、可能な限り早く対応するのが望ましい重要ではない問題の例です。サポートが故障通知を受け取ると、部品の交換の手配について連絡します。

手順

1. ［**Health**］ > ［**Alerts**］ > ［**Daily Alert Summary**］を選択します。
2. 8 AM のデフォルト配信時間で問題がある場合、次の手順を行います。

   a. ［**Schedule**］をクリックします。

      ［Schedule Alert Summary］ダイアログ ボックスが表示されます。

   b. リスト ボックスを使用して、サマリー レポートの時間、分、AM または PM を選択できます。

   c. ［**OK**］をクリックします。

      ［**CLI** 相当機能］

      ```
      # autosupport set schedule alert-summary daily 1400
      ```

3. 日次アラート サブスクライバー リストを構成するには、次の手順を行います。

   a. ［**Configure**］をクリックします。

      ［Daily Alert Summary Mailing］ダイアログ ボックスが表示されます。

   b. 日次アラート サブスクライバー リストの変更は、次のように行います。

      - サブスクライバーを追加するには、［**+**］アイコンをクリックして、メール アドレスを入力し、［**OK**］をクリックします。
        ［**CLI** 相当機能］

```
# autosupport add alert-summary emails djones@company.com
```

- メール アドレスを変更するには、サブスクライバーのチェックボックスを選択して、鉛筆アイコンをクリックし、メール アドレスを編集して、［**OK**］をクリックします。
- メール アドレスを削除するには、サブスクライバーのチェックボックスを選択し、［**X**］をクリックします。
  ［**CLI** 相当機能］

```
# autosupport del alert-summary emails djones@company.com
```

c. ［完了］をクリックします。

［Daily Alert Summary］タブ

［Daily Alert Summary］タブを使用して、日に一度、すべてのシステム アラートのサマリーの受信を希望するユーザーのメール リストを構成できます。このリストに含まれているユーザーは、通知グループにも追加されている場合を除き、個々のアラートは受信しません。

表 55 ［Daily Alert Summary］、ラベルの説明

項目	説明
Delivery Time	デリバリ時刻には、毎日のメールの構成時刻が表示されます。
Email List	このリストには、毎日のメールを受信するユーザーのメール アドレスが表示されます。

表 56 ［Daily Alert Summary］タブのコントロール

Control	説明
［Configure］ボタン	［**Configure**］ボタンをクリックして、サブスクライバーのメール リストを編集します。
［Schedule］ボタン	［**Schedule**］ボタンをクリックして、毎日のレポートの送信時刻を構成します。

Data Domain へのアラート通知の有効化および無効化

Data Domain へのアラート通知は、自動サポート レポートが Data Domain に送信されるかどうかとは無関係に、有効化または無効化できます。

手順

1. アラート レポートのステータスを表示するには、
   ［**Maintenance**］ > ［**Support**］ > ［**Autosupport**］を選択します。

   ［Support］領域の［Real-time alert］ラベルの隣にある、アラート通知ステータスが、緑でハイライト表示されます。現在の構成に応じて、［**Enable**］または［**Disable**］ボタンが［Real-time alert］行に表示されます。
2. Data Domain に報告するアラートを有効化するには、［Real-time alert］行の［**Enable**］をクリックします。
3. Data Domain に報告するアラートを無効化するには、［Real-time alert］行の［**Disable**］をクリックします。

アラート メール機能のテスト

［Notification］タブを使用して、選択した通知グループまたはメール アドレスにテスト メールを送信します。この機能によって、システムがアラート メッセージを送信すりょうに正しく構成されているかどうかを判断できます。

手順

1. テスト アラートが Data Domain に送信されるかどうかを制御するには、次の手順に従ってください。
   a. ［**Maintenance**］ > ［**Support**］ > ［**Autosupport**］を選択します。
   b. ［**Alert Support**］領域で、［**Enable**］または［**Disable**］をクリックして、テスト メールが送信されるかどうかを制御します。
      メール アドレスは変更できません。
2. ［**Health**］ > ［**Alerts**］ > ［**Notification**］を選択します。
3. ［**More Tasks**］ > ［**Send Test Alert**］を選択します。
   ［Send Test Alert］ダイアログ ボックスが開きます。
4. ［**Notification Groups**］リストで、テスト メールを受信するグループを選択し、［**Next**］をクリックします。
5. オプションで、メールを受信するメール アドレスを追加します。
6. ［**Send Now**］と［**OK**］をクリックします。
   ［**CLI** 相当機能］

   ```
   # alerts notify-list test jsmith@yourcompany.com
   ```

7. Data Domain へのテスト アラートの送信を無効化しており、この機能は有効化したい場合、次の手順を実行します。
   a. ［**Maintenance**］ > ［**Support**］ > ［**Autosupport**］を選択します。
   b. ［**Alert Support**］領域で、［**Enable**］をクリックします。

結果

メーラーの問題についての新たに追加されたアラート メールをテストするには、次のように入力します：**autosupport test email**email-addr

たとえば、メール アドレス djones@yourcompany.com をリストに追加した後、次のコマンドを入力します：**autosupport test email**djones@yourcompany.com

サポート デリバリの管理

デリバリの管理は、アラートおよび自動サポートのレポートを Data Domain に送信する方法を定義します。デフォルトでは、アラートおよび自動サポート レポートは、標準の（安全ではない）E メールを使用して Data Domain カスタマー サポートに送信されます。ConnectEMC 方式では、セキュア リモート サービス VE（Virtual Edition）ゲートウェイを経由してメッセージを安全な形式で送信します。

ConnectEMC 方式で使用する場合のセキュア リモート サービス ゲートウェイの利点の 1 つは、複数のシステムからのメッセージを 1 つのゲートウェイで転送できることです。このため、複数のシステムに対してではなく、セキュア リモート サービス ゲートウェイに対してのみネットワーク セキュリティを構成

すれば済みます。また、電子ライセンスを導入している場合は、使用状況インテリジェンス レポートが生成され、送信されます。

セキュア リモート サービス ゲートウェイを構成するにあたり、Data Domain システムでは、複数のゲートウェイを登録して冗長性を確保できます。

Data Domain への標準メール デリバリの選択

標準（安全ではない）のメール デリバリ方式を選択する場合、この方法はアラートと自動サポート レポートの両方に適用されます。

手順

1. ［**Maintenance**］ > ［**Support**］ > ［**Autosupport**］を選択します。
2. ［Support］領域の［Channel］行で［**Configure**］をクリックします。

   ［Configure EMC Support Delivery］ダイアログが表示されます。デリバリ方式は、［Support］領域の［Channel］ラベルの後に表示されます。
3. ［**Channel**］リスト ボックスで、［**Email to datadomain.com**］を選択します。
4. ［**OK**］をクリックします。

   ［**CLI** 相当機能］

   ```
   # support notification method set email
   ```

セキュア リモート サービス デリバリの選択と設定

Secure Remote Services VE（Virtual Edition）Gateway は、包括的なセキュリティ システムによって強化された IP ベースのソリューションを使用して、自動化された Connect Home およびリモート サポート アクティビティを提供します。

オンプレミスのセキュア リモート サービス バージョン 3 ゲートウェイを使用することで、オンプレミスの Data Domain システムと DD VE インスタンス、クラウド ベースの DD VE インスタンスを監視できます。

手順

1. ［**Maintenance**］ > ［**Support**］ > ［**Autosupport**］を選択します。
2. ［Support］領域の［Channel］行で［**Configure**］をクリックします。

   ［Configure Dell EMC Support Delivery］ダイアログ ボックスが表示されます。デリバリ方式は、［Support］領域の［Channel］ラベルの後に表示されます。
3. ［**Channel**］リスト ボックスで、［**Secure Remote Services**］を選択します。
4. ゲートウェイ ホスト名を入力し、Data Domain システムのローカル IP アドレスを選択します。
5. ［**OK**］をクリックします。
6. サービス リンク ユーザー名とパスワードを入力します。
7. ［**Register**］をクリックします。

   セキュア リモート サービスの詳細が［Autosupport］パネルに表示されます。

   ［**CLI** 相当機能］

```
# support connectemc device register ipaddr esrs-gateway [host-list] [ha-peer ipaddr]
```

⚠ 注意

Data Domain HA ペアでセキュア リモート サービスの提供を設定する場合：

- **`ha-peer` パラメーターは、Data Domain HA ペアでセキュア リモート サービスを設定して両方のノードを登録するときに必要です。**
- **HA ペアをユーザーとして登録しようとすると失敗して RSA キー トークンの同期がとれなくなるため、お客様は HA ペアで `support connectemc device register` コマンドを実行するためにサービス リンク資格情報を提供する必要があります。**

ConnectEMC の動作テスト

CLI コマンドにより、セキュア リモート サービス ゲートウェイ経由でサポートにテスト メッセージを送信し、ConnectEMC の動作をテストできます。

手順

1. ConnectEMC の操作をテストするには、CLI を使用します。

```
#support connectemc test
Sending test message through ConnectEMC...
Test message successfully sent through ConnectEMC.
```

ログ ファイルの管理

Data Domain システムは、発生する可能性があるシステムの問題のトラブルシューティングをサポートするため、バンドル化し、サポートに送信できるログ ファイルのセットを保持します。ログ ファイルは、DD System Manager で変更も削除もできませんが、ログ ディレクトリからコピーして、システムから管理することはできます。

注

HA システムでのログ メッセージはログ ファイルの生成元のノードに保存されます。

ログ ファイルは、毎週ローテーションされます。毎週日曜日午前 0:45 に、システムが自動的に既存のログ用に新しいログ ファイルを開き、番号を付与して前のファイルを名称変更します。たとえば、運用の最初の週が終わると、前週の `messages` ファイルの名前が `messages.1` に変更され、新しいメッセージが新しいメッセージ ファイルに保存されます。各番号付きファイルは、毎週、次の番号に繰り上げられます。たとえば、2 週目が終わると `messages.1` ファイルは `messages.2` に繰り上げられ、`messages.2` ファイルがすでに存在する場合は、`messages.3` に繰り上げられます。（下表に示されている）保存期間終了時、期限切れのログが削除されます。たとえば、`messages.8` が `messages.9` に繰り上げられると、既存の `messages.9` ファイルは削除されます。

`audit.log` では週 1 回のローテーションは行われません。代わりに、ファイルのサイズが 70 MB に達したときにローテーションされます。

このトピックに記載がある場合を除き、ログ ファイルは `/ddvar/log` に保存されます。

注

Linux ユーザーに/ddvar ディレクトリの［書き込み］権限が割り当てられている場合、そのディレクトリ内のファイルは Linux コマンドを使用して削除できます。

各システム上のログ ファイルのセットは、そのシステム上で構成された機能と発生するイベントによって決まります。次の表は、システムが生成できるログ ファイルを示します。

表 57 システム ログ ファイル

Log File（ログ ファイル）	説明	Retention Period
audit.log	ユーザー ログイン イベントについてのメッセージ。	15 週間
cifs.log	CIFS サブシステムからのログ メッセージは、debug/cifs/cifs.log にのみ記録されます。サイズ制限は 50 MiB。	10 週間
メッセージ	実行されたコマンドを含む一般システム イベントについてのメッセージ。	9 週間
secure.log	ログインの成功と失敗、ユーザーの追加と削除、パスワードの変更などのユーザー イベントに関するメッセージ。このファイルは、Admin 役割を持つユーザーのみ閲覧できます。	9 週間
space.log	システム コンポーネントによるディスク領域使用率についてのメッセージとクリーン処理からのメッセージ。領域使用メッセージは 1 時間ごとに生成されます。クリーン処理が実行されるたびに約 100 個のメッセージが作成されます。すべてのメッセージは、ディスク領域メッセージをクリーン処理メッセージから分離するために使用できるタグ付きのコンマ区切り値形式です。サード パーティのソフトウェアを使用して、いずれかのメッセージ セットを分析できます。ログ ファイルには、次のタグが使用されます。 • クリーン操作からのデータ行の CLEAN。 • クリーン操作データ行のヘッダーを含む行の CLEAN_HEADER。 • ディスク領域データ行の SPACE。 • ディスク領域データ行のヘッダーを含む行の SPACE_HEADER。	1 個のファイルは永続的に保持されます。このログのログ ファイル ローテーションはありません。

DD System Manager でのログ ファイルの表示

［Logs］タブを使用して、DD System Manager でシステム ログ ファイルを表示したり開いたりします。

手順

1. ［**Maintenance**］ > ［**Logs**］を選択します。

   ［Logs］リストには、ログ ファイル名、各ログ ファイルのサイズと作成日が表示されます。

2. ログ ファイル名をクリックすると、その内容が表示されます。Notepad.exe などのアプリケーションを選択して、ファイルを開くよう求められる場合があります。

CLI でのログ ファイルの表示

log view コマンドを使用して、CLI でログ ファイルを表示します。

手順

1. CLI でログ ファイルを表示するには、 `log view` コマンドを使用します。

   引数がない場合、このコマンドは現在のメッセージ ファイルを表示します。

2. ログを表示する場合、上下矢印を使用してファイルをスクロールし、終了するときは **q** キーを使用します。ファイル内を検索するには、スラッシュ文字（/）とパターンを入力します。

メッセージ ファイルの表示は、次と同様です。例の最後のメッセージは、Data Domain システムが自動的に生成する毎時システム ステータス メッセージです。メッセージは、システムのアップタイム、保存されているデータの量、NFS 操作、データ領域に使用されるディスク領域の量（%）をレポートします。毎時メッセージはシステム ログと（アタッチされている場合）シリアル コンソールに保存されます。

```
# log view
Jun 27 12:11:33 localhost rpc.mountd: authenticated unmount
request from perfsun-g.emc.com:668 for /ddr/col1/segfs (/ddr/
col1/segfs)

Jun 27 12:28:54 localhost sshd(pam_unix)[998]: session opened
for user jsmith10 by (uid=0)

Jun 27 13:00:00 localhost logger: at 1:00pm up 3 days, 3:42,
52324 NFS ops, 84763 GiB data col. (1%)
```

注

GiB = ギビバイト = ギガバイトのバイナリ相当。

ログ メッセージの詳細について

お使いの DD OS バージョンの Error Message Catalog でエラー メッセージを検索します。

ログ ファイル内のテキストは次のようになります。

```
Jan 31 10:28:11 syrah19 bootbin: NOTICE: MSG-SMTOOL-00006: No
replication throttle schedules found: setting throttle to
unlimited.
```

メッセージのコンポーネントは次のとおりです。

```
DateTime Host Process [PID]: Severity: MSG-Module-MessageID: メッセージ
```

重大度レベルは高い順から、Emergency、Alert、Critical、Error、Warning、Notice、Info、Debug です。

手順

1. オンライン サポートの Web サイト（https://support.emc.com）にアクセスし、検索ボックスに「[Error Message Catalog]」と入力して、検索ボタンをクリックします。
2. 結果のリストで、お使いのシステムのカタログを探して、リンクをクリックします。
3. ブラウザの検索ツールを使用して、メッセージ内の一意のテキスト文字列を検索します。

   エラー メッセージの説明は、次のようになります。

   ```
   ID: MSG-SMTOOL-00006 - Severity: NOTICE - Audience:
   customerMessage: No replication throttle schedules found:
   ```

```
setting throttle to unlimited. Description: The restorer
cannot find a replication throttle schedule. Replication
is running with throttle set to unlimited. Action: To set
a replication throttle schedule, run the replication
throttle add command.
```

4. 問題を解決するには、推奨アクションを行ってください。

   メッセージの説明の例に基づき、`replication throttle add` コマンドを実行して、スロットルを設定できます。

ログ ファイルのコピーの保存

ファイルをアーカイブしたい場合、ログ ファイル コピーを他のデバイスに保存します。

NFS、CIFS マウント、または FTP を使用して、ファイルを他のマシンにコピーします。CIFS または NFS を使用する場合、デスクトップに**/ddvar** をマウントし、ファイルをマウント ポイントからコピーします。次の手順では、FTP を使用してファイルを他のマシンに移動する方法について説明します。

手順

1. Data Domain システムで、`adminaccess show ftp` コマンドを使用して、FTP サービスが有効になっているかどうかを確認します。サービスが無効な場合、コマンド `adminaccess enable ftp` を使用します。
2. Data Domain システムで、 `adminaccess show ftp` コマンドを使用して、FTP アクセス リストに使用リモート マシンの IP アドレスが含まれていることを確認します。アドレスがリストにない場合は、 `adminaccess add ftp` **ipaddr** コマンドを使用します。
3. リモート マシンで、Web ブラウザーを開きます。
4. Web ブラウザー上部の［**Address**］ボックスで、次の例に示すように、FTP を使用して Data Domain システムにアクセスします。

   `ftp://Data Domain system_name.yourcompany.com/`

   注

   マシンが匿名ログインを許可していない場合、自動的にログインを求めない Web ブラウザーもあります。その場合、ユーザー名とパスワードを FTP 行に追加します。次に例を挙げます。**`ftp://sysadmin:your-pw@Data Domain system_name.yourcompany.com/`**

5. ログイン ポップアップで、ユーザー **`sysadmin`** として Data Domain システムにログインします。
6. Data Domain システムでは、ログ ディレクトリの 1 つ上の階層のディレクトリにいます。ログ ディレクトリを開き、メッセージ ファイルをリストします。
7. 保存するファイルをコピーします。ファイル アイコンを右クリックし、［**Copy To Folder**］を選択します。ファイル コピーの場所を選択します。
8. Data Domain システムで FTP サービスを無効化したい場合、ファイル コピー完了後に、SSH を使用して Data Domain システムに sysadmin としてログインし、コマンド `adminaccess disable ftp` を呼び出します。

リモート システムへのログ メッセージの転送

一部のログ メッセージは、Data Domain システムから他のシステムに送信できます。DD OS は、システムログを使用してログ メッセージをリモート システムに公開します。

Data Domain システムは、ログ ファイル用に次の facility.priority セレクターをエクスポートします。サード パーティ システムでのセレクターの管理とメッセージの受信については、受信システムに関するベンダー提供のドキュメントを参照してください。

- *.notice：通知優先度以上ですべてのメッセージを送信します。
- *.alert：アラート優先度以上ですべてのメッセージを送信します。アラートは*に含まれます。
- kern.*：すべてのカーネル メッセージを送信します（kern.info ログ ファイル）。

`log host` コマンドは、別のシステムへのログ メッセージ送信処理を管理します。

ログ ファイル転送の構成の表示

`log host show` CLI コマンドを使用して、ログ ファイルの転送の状態（有効/無効）およびログ ファイルを受信するホストを表示します。

手順

1. 構成を表示するには、`log host show` コマンドを入力します。

```
# log host show
Remote logging is enabled.
Remote logging hosts
     log-server
```

ログ メッセージ転送の有効化および無効化

CLI コマンドを使用して、ログ メッセージ転送を有効化または無効化する必要があります。

手順

1. ログ メッセージの他のシステムへの送信を有効化するには、`log host enable` コマンドを使用します。
2. ログ メッセージの他のシステムへの送信を無効化するには、`log host disable` コマンドを使用します。

受信ホストの追加または削除

CLI コマンドを使用して、受信ホストを追加または削除する必要があります。

手順

1. Data Domain システム ログ メッセージを受信するシステムをリストに追加するには、`log host add` コマンドを使用します。
2. システム ログ メッセージを受信するシステムをリストから削除するには、次のコマンドを使用します。`log host del`。

次のコマンドは、ログ メッセージを受信するホストに［log-server］という名前のシステムを追加します。

```
log host add log-server
```

次のコマンドは、ログ メッセージを受信するホストから［log-server］という名前のシステムを削除します。

```
log host del log-server
```

次のコマンドは、ログの送信を無効化し、デスティネーション ホスト名のリストをクリアします。

```
log host reset
```

IPMI によるリモート システムの電源管理

Select DD システムは、IPMI（インテリジェント プラットフォーム管理インターフェイス）を使用したリモート電源管理に対応し、また、SOL（Serial Over LAN）を使用したブート シーケンスのリモート モニタリングに対応しています。

IPMI 電源管理は、IPMI イニシエーターと IPMI リモート ホスト間で実行されます。IPMI イニシエーターは、リモート ホストの電源を制御するホストです。イニシエーターからのリモート電源管理をサポートするには、IPMI のユーザー名とパスワードを使用してリモート ホストを構成する必要があります。イニシエーターは、リモート ホストでの電源を管理する場合、このユーザー名とパスワードを提供する必要があります。

IPMI は、DD OS から独立して動作し、IPMI ユーザーはリモート システムが電源とネットワークに接続されている限りシステム電源を管理できます。イニシエーターとリモート システムの間に、IP ネットワーク接続が必要です。正しく構成および接続されると、IPMI 管理によって、リモート システムに物理的にアクセスして電源のオン/オフを切り換える必要がなくなります。

DD System Manager と CLI の両方を使用して、リモート システムの IPMI ユーザーを構成できます。リモート システムの IPMI を構成した後は、別のシステムで IPMI イニシエーター機能を使用してログインし、電源を管理できます。

注

ハードウェアまたはソフトウェアの制限により、システムで IPMI をサポートできない場合、構成ページに移動しようとすると、DD System Manager から通知メッセージが表示されます。

SOL は、リモート システムの電源の入れ直し後にブート シーケンスを表示するために使用されます。SOL によって、通常はシリアル ポートまたは直接接続されたコンソールに送信されるテキスト コンソール データが、LAN 経由で送信され、管理ホストで表示することができます。

DD OS CLI は SOL のリモート システムの構成と、リモート コンソール出力の表示を可能にします。この機能は、CLI でのみサポートされています。

通知

DD OS コマンドを使用した電源シャットダウンが失敗した緊急時用に、IPMI 電源遮断が用意されています。IPMI 電源遮断はシステムへの電源を遮断するのみで、DD OS ファイル システムの計画的なシャットダウンは実行しません。電源を遮断および復旧する適切な方法は、DD OS `system reboot` コマンドを使用することです。システム電源を遮断する適切な方法は、DD OS `system poweroff` コマンドを使用して、コマンドによってファイル システムが正しくシャットダウンされるのを待つことです。

IPMI および SOL 制限

一部の Data Domain システムでは、IPMI および SOL のサポートに制限があります。

- IPMI は、DD140、DD610、DD630 を除き、このリリースが対応しているすべてのシステムで対応しています。
- IPMI ユーザー サポートは、次の点で異なります。
  - Model DD990：最大ユーザー ID 数 = 15。デフォルト ユーザー 3 人（NULL、anonymous、root）。使用可能な最大ユーザー ID 数 = 12。
  - Model DD640、DD4200、DD4500、DD7200、DD9500：最大ユーザー ID 数 = 10。デフォルト ユーザー 2 人（NULL、root）。使用可能な最大ユーザー ID 数 = 8。
- SOL は、次のシステムで対応しています。それは、DD160、DD620、DD640、DD670、DD860、DD890、DD990、DD2200、DD2500（DD OS 5.4.0.6 以降が必要）、DD4200、DD4500、DD7200、DD9500 です。

注

ユーザー root は、DD160 システムでの IPMI 接続には対応していません。

DD System Manager を使用した IPMI ユーザーの追加と削除

各システムには構成済み IPMI ユーザーの独自リストが含まれ、これを使用してローカルの電源管理機能へのアクセスを制御します。IPMI イニシエーターとして動作している別のシステムでは、有効なユーザー名とパスワードを提供した後にのみ、リモート システムの電源を管理できます。

IPMI ユーザーに複数のリモート システムの電源を管理する権限を与えるには、そのユーザーを各リモート システムに追加する必要があります。

注

各リモート システムの IPMI ユーザー リストは、管理者アクセスとローカル ユーザーの DD System Manager リストからは独立しています。管理者とローカル ユーザーは、IPMI 電源管理の許可を継承しません。

手順

1. ［**Maintenance**］ > ［**IPMI**］を選択します。
2. Direct NFS を追加するには、次のステップを行います。
   a. ［IPMI Users］テーブルで、［**Add**］をクリックします。
   b. ［Add User］ダイアログ ボックスで、適切なテキスト ボックスにユーザー名（16 文字以下）とパスワードを入力します（［**Verify Password**］ボックスにパスワードを入力し直します）。
   c. ［**Create**］をクリックします。

      ユーザー エントリーが、［**IPMI Users**］テーブルに表示されます。
3. ユーザーを追加するには、次のステップを行います。
   a. ［IPMI Users］リストで、ユーザーを選択して［**Delete**］をクリックします。
   b. ［Delete User］ダイアログ ボックスで、［**OK**］をクリックして、ユーザーの削除を確認します。

IPMI ユーザー パスワードの変更

電源管理に古いパスワードを使用できないようにするため、IPMI ユーザー パスワードを変更します。

手順

1. ［**Maintenance**］ > ［**IPMI**］を選択します。
2. ［IPMI Users］テーブルで、ユーザーを選択し、［**Change Password**］をクリックします。
3. ［Change Password］ダイアログ ボックスで、適切なテキスト ボックスにパスワードを入力し、［**Verify Password**］ボックスにパスワードを入力し直します。
4. ［**Update**］をクリックします。

IPMI ポートの構成

システムのポートを構成する場合、ネットワーク ポート リストからポートを選択し、そのポートの IP 構成パラメーターを指定します。表示された IPMI ポートの選択は、Data Domain システムのモデルによって決定されます。

一部のシステムは、IPMI トラフィックにのみ使用できる 1 個以上の専用ポートに対応しています。その他のシステムは、IPMI トラフィックと［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］ビューの物理インターフェイスが対応しているすべての IP トラフィック両方に使用できるポートに対応します。共有ポートは、専用 IPMI ポートを提供するシステムでは提供できません。

［IPMI Network Ports］リストのポート名には、ベース ボード管理コントローラーを表す bmc をプレフィックスとして使用します。ポートが専用ポートか共有ポートかを判断するには、ネットワーク インターフェイス リストのポートとポート名の残りの部分を比較します。IPMI ポート名の残りの部分がネットワーク インターフェイス リストのインターフェイスに一致する場合、そのポートは共有ポートです。IPMI ポート名の残りの部分がネットワーク インターフェイス リストの名前とは異なる場合、そのポートは専用ポートです。

注

DD4200、DD4500、および DD7200 システムには、前掲の命名規則の例外です。これらのシステムでは、IPMI ポート bmc0a はネットワーク インターフェイス リストの共有ポート ethMa に対応しています。（HTTP、Telnet、SSH などのプロトコルを使用した）共有ポート ethMa を IPMI トラフィックとシステム管理トラフィック用に確保することを推奨します。バックアップ データ トラフィックは、他のポートに送信する必要があります。

IPMI および非 IPMI IP トラフィックが Ethernet ポートを共有する場合、リンク状態の変更が IPMI 接続に干渉する可能性があるため、共有インターフェイスでリンク統合機能を使用しないことを推奨します。

手順

1. ［**Maintenance**］ > ［**IPMI**］を選択します。

   ［IPMI Configuration］領域には、管理対象システムの IPMI 構成が表示されます。
   ［Network Ports］テーブルには、IPMI を有効化および構成できるポートがリストされます。
   ［IPMI Users］テーブルには、管理対象システムをアクセスできる IPMI ユーザーが表示されます。

表 58 Network Ports リスト列の説明

項目	説明
ポート	IPMI 通信に対応するポートの論理名。
Enabled	IPMI のポートが有効かどうか（Yes または No）。
DHCP	ポートが DHCP を使用して、その IP アドレスを設定するかどうか（Yes または No）。
MAC アドレス	ポートのハードウェア MAC アドレス。
IP アドレス	ポートの IP アドレス。
ネットマスク	ポートのサブネット マスク。
Gateway	ポートのゲートウェイ IP アドレス。

表 59 IPMI Users リスト列の説明

項目	説明
ユーザー名	リモート システムの電源を管理する権限を持つユーザーの名前。

2. ［**Network Ports**］テーブルで、構成するポートを選択します。

注

IPMI ポートが IP トラフィック（管理者アクセスまたはバックアップ トラフィック）にも対応している場合、IPMI を構成するには、インターフェイス ポートを有効化する必要があります。

3. ［**Network Ports**］テーブルで、［**Configure**］をクリックします。

［Configure Port］ダイアログ ボックスが表示されます。

4. ネットワーク アドレス情報を割り当てる方法を選択します。
   - DHCP サーバから IP アドレス、ネットマスク、ゲートウェイ構成を収集するには、［**Dynamic (DHCP)**］を選択します。
   - 手動でネットワーク構成を定義するには、［**Static (Manual)**］を選択し、IP アドレス、ネットマスク、ゲートウェイ アドレスを入力します。
5. ［**Network Ports**］テーブルでネットワーク ポートを選択して、［**Enable**］をクリックすることにより、無効な IPMI ネットワーク ポートを有効化します。
6. ［**Network Ports**］テーブルでネットワーク ポートを選択して、［**Disable**］をクリックすることにより、有効な IPMI ネットワーク ポートを無効化します。
7. ［**Apply**］をクリックします。

CLI を使用したリモート電源管理とコンソール モニタリングの準備

リモート コンソール モニタリングには、SOL（Serial Over Lan）機能を使用して、シリアル サーバーを使用せずにテキスト ベース コンソール出力の表示を可能にします。システムをリモート電源管理とコンソール モニタリング用にセットアップするには、CLI を使用する必要があります。

リモート コンソール モニタリングは通常、`ipmi remote power cycle` コマンドと組み合わせて使用して、システムのブート シーケンスを表示します。この手順は、ブート シーケンス中にコンソールをリモートで表示したいすべてのシステムで行う必要があります。

手順

1. コンソールをシステムに直接またはリモートで接続します。
   - 直接接続するには、次のコネクタを使用します。
     - PS/2 キーボード用の DIN タイプのコネクタ
     - USB キーボード用の USB-A レセプタクル ポート
     - VGA モニター用の DB15 メス コネクタ

     注

     システム DD4200、DD4500、および DD7200 は、KVM を含む直接接続には対応していません。

   - シリアル接続を行うには、標準 DB9 オスまたは Micro-DB9 メス コネクタを使用します。システム DD4200、DD4500、および DD7200 は、メス Micro-DB9 コネクタを提供します。通常のラップトップ接続用にオスのマイクロ DB9 コネクタと標準のメス DB9 コネクタがある Null モデム ケーブルが含まれます。
   - リモート IPMI/SOL 接続を行うには、次のように適切な RJ45 レセプタクルを使用します。
     - DD990 システムの場合、デフォルト ポート eth0d を使用します。
     - その他のシステムの場合、保守ポートまたはサービス ポートを使用します。ポートの場所については、ハードウェアの概要、インストールとセットアップ ガイドなどのシステム ドキュメントを参照してください。
2. リモート コンソール モニタリングに対応するには、デフォルトの BIOS 設定を使用します。
3. IPMI ポート名を表示するには、`ipmi show config` と入力します。
4. IPMI を有効化するには、「`ipmi enable {`**port** `| all}`」と入力します。
5. IPMI ポートを表示するには、「`ipmi config port { dhcp | ipaddress` **ipaddr**`netmask`**mask**`gateway`**ipaddr**`}`」と入力します。

   注

   IPMI ポートが IP トラフィック（管理者アクセスまたはバックアップ トラフィック）にも対応している場合、インターフェイス ポートは IPMI を構成する前に `net enable` コマンドで有効化する必要があります。

6. IPMI を使用するのが初めてである場合、`ipmi user reset` を実行して、2 つのポート間で同期されていない可能性がある IPMI ユーザーをクリアし、デフォルト ユーザーを無効化します。
7. 新しい IPMI ユーザーを追加するには、「`ipmi user add`**user**」と入力します。
8. SOL をセットアップするには、以下の手順に従ってください。
   a. 「`system option set console lan`」と入力します。
   b. 求められたら、**y** と入力して、システムを再起動します。

DD System Manager による電源の管理

IPMI がリモート システムで正しくセットアップされると、IPMI イニシエーターとして DD System Manager を使用してリモート システムにログインし、電源ステータスを表示および変更できます。

手順

1. ［**Maintenance**］ > ［**IPMI**］を選択します。
2. ［**Login to Remote System**］をクリックします。

   ［IPMI Power Management］ダイアログ ボックスが表示されます。

3. リモート システムの IPMI IP アドレスまたはホスト名、IPMI ユーザー名とパスワードを入力して、［**Connect**］をクリックします。
4. IPMI ステータスを表示します。

   ［IPMI Power Management］ダイアログ ボックスが表示され、そこにターゲット システム ID と現在の電源ステータスが表示されます。［Status］領域には、常に現在のステータスが表示されます。

   注

   ステータスの隣にある Refresh アイコン（青い矢印）を使用して、構成ステータスを更新できます（IPMI IP アドレスまたはユーザー構成が CLI コマンドを使用して過去 15 分以内に変更された場合など）。

5. IPMI 電源ステータスを変更するには、適切なボタンをクリックします。
   - ［**Power Up**］: リモート システムの電源がオフになると表示されます。リモート システムの電源をオンにするには、このボタンをクリックします。
   - ［**Power Down**］: リモート システムの電源がオンになると表示されます。リモート システムの電源をオフにするには、このボタンをクリックします。
   - ［**Power Cycle**］: リモート システムの電源がオンになると表示されます。リモート システムの電源を入れ直すには、このボタンをクリックします。
   - ［**Manage Another System**］: IPMI 電源管理用の他のリモート システムにログインするには、このボタンをクリックします。
   - ［**Done**］: クリックすると、［IPMI Power Management］ダイアログ ボックスが閉じます。

   通知

   IPMI Power Down 機能は、DD OS の計画的なシャットダウンを実行しません。このオプションは DD OS がハングした場合に使用でき、正常にシステムをシャットダウンする場合には使用できません。

CLI による電源の管理

CLI を使用して、リモート システムの電源を管理し、リモート コンソールの監視を開始することができます。

注

電源を管理する、またはシステムを監視するには、リモート システムを適切にセットアップする必要があります。

手順

1. リモート システムを監視したいシステムで CLI セッションを確立します。
2. リモート システムで電源を管理するには、`ipmi remote power {on | off | cycle | status} ipmi-target <ipaddr | hostname> user user` と入力します。
3. リモート コンソール モニタリングを開始するには、`ipmi remote console ipmi-target <ipaddr | hostname> user user` と入力します。

   注

   ユーザー名は、リモート システムで IPMI に定義された IPMI ユーザー名です。DD OS ユーザー名は、自動的には IPMI が対応しません。

4. リモート コンソール モニタリング セッションから切断し、コマンド ラインに戻るには、アットマーク（@）を入力します。
5. リモート コンソール モニタリングを終了するには、チルダ記号（~）を入力します。

第 4 章

Data Domain システムのモニタリング

本章には、次のセクションが含まれます。

- 個々のシステム ステータスおよび識別情報の表示 174
- ［Health Alerts］パネル 176
- 現在のアラートの表示およびクリア 177
- アラート ヒストリの表示 178
- ハードウェア コンポーネント ステータスの表示 179
- システム統計の表示 182
- アクティブ ユーザーの表示 184
- ヒストリ レポートの管理 184
- タスク ログの表示 188
- システムの高可用性ステータスの表示 189

個々のシステム ステータスおよび識別情報の表示

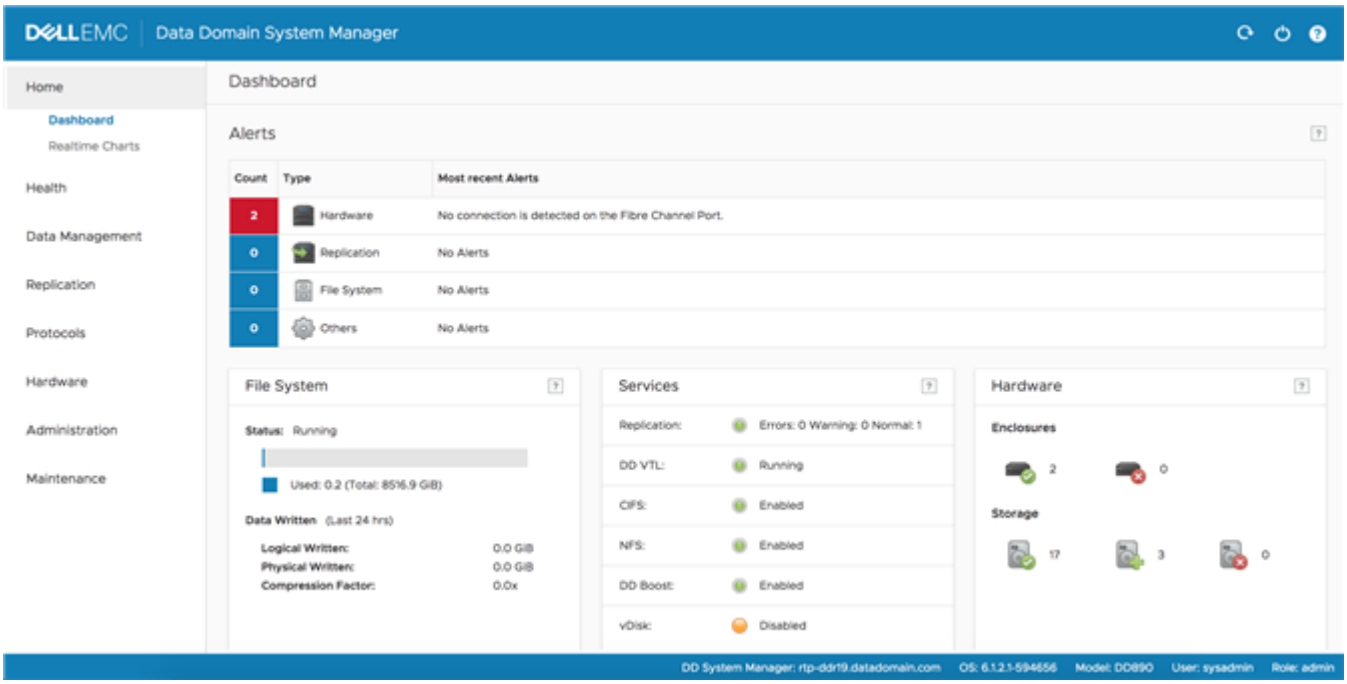
［**Dashboard**］領域には、アラート、ファイル システム、ライセンス サービス、ハードウェア エンクロージャのサマリー情報とステータスが表示されます。［**Maintenance**］領域には、システムのアップタイム、システムとシャーシのシリアル番号を含む、システムの詳細情報が表示されます。

システム名、ソフトウェア バージョン、ユーザー情報は、いつでもフッターに表示されます。

手順

1. システム ダッシュ ボードを表示するには、［**Home**］ > ［**Dashboard**］を選択します。

   図 5 システム ダッシュボード



2. システムのアップタイムと識別情報を表示するには、［**Maintenance**］ > ［**System**］を選択します。

   ［System］領域には、システムのアップタイムと ID 情報が表示されます。

［Dashboard Alerts］領域

［Dashboard Alerts］領域には、各サブシステム（ハードウェア、レプリケーション、ファイル システムなど）に関する、システム内の最新アラートのカウント、タイプ、テキストが表示されます。［Alerts］領域の任意の場所をクリックすると、現在のアラートの詳細情報が表示されます。

表 60 ［Dashboard Alerts］列の説明

列	説明
Count	隣接する列で指定されたサブシステム タイプの現在のアラートのカウント。背景色は、アラートの重大度を示します。
タイプ	アラートが発生したサブシステム。

表 60 ［Dashboard Alerts］列の説明 （続き）

列	説明
直近のアラート	隣接する列で指定されたサブシステム タイプの直近のアラートのテキスト。

［Dashboard File System］領域

［Dashboard File System］領域には、ファイル システム全体の統計が表示されます。［File System］領域の任意の場所をクリックすると、詳細情報が表示されます。

表 61 ［File System］領域のラベルの説明

列	説明
Status	ファイル システムの現在のステータス。
X.Xx	ファイル システムの平均圧縮率の減少係数。
Used	使用されている総ファイル システム スペース。
書き込まれたデータ：圧縮前	圧縮前にシステムが受信するデータ量。
書き込まれたデータ：圧縮後	圧縮後にシステムに格納されるデータ量。

［Dashboard Services］領域

［Dashboard Services］領域には、レプリケーション、DD VTL、CIFS、NFS、DD Boost、vDisk のサービス ステータスが表示されます。サービスをクリックして、そのサービスに関する詳細情報を表示します。

表 62 ［Services］領域の列の説明

列	説明
左の列	左の列には、システムで使用できるサービスが一覧表示されます。これらのサービスには、レプリケーション、DD VTL、CIFS、NFS、DD Boost、vDisk があります。
右の列	右の列には、サービスの動作ステータスが表示されます。ほとんどのサービスで、ステータスは［enabled］、［disabled］、［not licensed］になります。レプリケーション サービス行には、通常、警告、エラー状態になっているレプリケーション コンテキストの数が表示されます。色で区別されるボックスで、通常動作は緑、警告状態は黄、エラーがある場合は赤が表示されます。

［Dashboard HA Readiness］領域

HA（高可用性）システムでは、必要に応じてシステムをアクティブ ノードからスタンバイ ノードにフェイルオーバーできるかどうかが、HA パネルに示されます。

［**HS** パネル］をクリックすると、［**HEALTH**］の［**High Availability**］セクションに移動します。

［Dashboard Hardware］領域

［Dashboard Hardware］領域には、システム エンクロージャおよびドライブのステータスが表示されます。［Hardware］領域の任意の場所をクリックすると、コンポーネントの詳細が表示されます。

表 63 ［Hardware］領域のラベルの説明

ラベル	説明
Enclosures	エンクロージャ アイコンには、通常（緑のチェックマーク）および縮退（赤の X）の状態で動作するエンクロージャの数が表示されます。
ストレージ	ストレージ アイコンには、通常（緑のチェックマーク）、スペア（緑の+）、障害（赤の X）の状態で動作するディスク ドライブの数が表示されます。

［Maintenance System］領域

［Maintenance System］領域には、システムのモデル番号、DD OS バージョン、システム アップタイム、システムとシャーシのシリアル番号番号が表示されます。

表 64 ［System］領域のラベルの説明

ラベル	説明
モデル番号	モデル番号は、Data Domain システムに割り当てられる番号です。
バージョン	バージョンは、DD OS バージョンと、システムで実行されているソフトウェアのビルド番号です。
システム アップタイム	システム アップタイムには、システムが最後に起動されてから実行されている時間が表示されます。括弧内は、システム アップタイムが最後に更新された時間を示します。
システム シリアル番号	システム シリアル番号は、システムに割り当てられるシリアル番号です。DD4500、DD7200 などの新しいシステムでは、システム シリアル番号はシャーシ シリアル番号から独立しており、シャーシ交換など各種保守イベント中も変わりません。DD990 以前のレガシー システムでは、システム シリアル番号がシャーシ シリアル番号に設定されます。
シャーシ シリアル番号	シャーシ シリアル番号は、現在のシステム シャーシのシリアル番号です。

［Health Alerts］パネル

アラートは、システム サービスおよびサブシステムからのメッセージで、システム イベントをレポートします。［Health］＞［Alerts］パネルには、現在のアラートと現在のものでないアラート、事前に構成

されたアラート通知グループ、日次アラート サマリー レポートを受信するユーザーの構成を表示できるタブが表示されます。

アラートは SNMP トラップとしても送信されます。トラップの完全なリストについては、「MIB クイック リファレンス ガイド」または SNMP MIB を参照してください。

現在のアラートの表示およびクリア

［Current Alerts］タブには、現在の全アラートのリストと選択したアラートの詳細が表示されます。原因となっている状況が修正されるか、手動でクリアされると、アラートは自動的に［Current Alerts］リストから削除されます。

手順

1. 現在のアラートをすべて表示するには、［**Health**］ > ［**Alerts**］ > ［**Current Alerts**］を選択します。
2. 現在のアラート リストのエントリー数を制限するには、次の手順を実行します。
   a. ［Filter By］領域で、［**Severity**］と［**Class**］を選択して、その選択に対応するアラートのみを表示します。
   b. ［**Update**］をクリックします。

   ［Severity］と［Class］に一致しないすべてのアラートがリストから削除されます。
3. ［**Details**］領域に特定アラートの追加情報を表示するには、リストのアラートをクリックします。
4. アラートをクリアするには、リストのアラート チェックボックスを選択して［**Clear**］をクリックします。

   クリアされたアラートは現在のアラート リストに表示されなくなりますが、アラート ヒストリ リストで参照できます。
5. フィルタリングを削除し、再度、現在のアラートをすべて表示するには、［**Reset**］をクリックします。

［Current Alerts］タブ

［Current Alerts］タブには、アラート リストと選択したアラートの詳細が表示されます。

表 65 アラート リスト、列ラベルの説明

項目	説明
メッセージ	アラート メッセージ テキスト。
重大度	アラートの重大度のレベル。warning、critical、info、emergency など。
日付	アラートが発生した日時。
クラス	アラートが発生したサブシステム。
オブジェクト	アラートが発生した物理コンポーネント。

表 66 ［Details］領域、行ラベルの説明

項目	説明
Name	アラートのテキスト識別子
メッセージ	アラート メッセージ テキスト。
重大度	アラートの重大度のレベル。warning、critical、info、emergency など。
クラス	アラートが発生したサブシステムとデバイス。
日付	アラートが発生した日時。
Object ID	アラートが発生した物理コンポーネント。
イベント ID	イベント ID。
Tenant Units	影響を受けるテナント ユニットをリストします。
説明	アラートについての詳細。
アクション	アラートに対応する方法の提案。
Object Info	影響を受けるオブジェクトの補足情報。
SNMP OID	SNMP オブジェクト ID。

アラート ヒストリの表示

［Alerts History］タブには、クリアされたアラートすべてのリストと選択したアラートの詳細が表示されます。

手順

1. すべてのアラート履歴を表示するには、［**Health**］ > ［**Alerts**］ > ［**Alerts History**］を選択します。
2. 現在のアラート リストのエントリー数を制限するには、次の手順を実行します。
   a. ［Filter By］領域で、［**Severity**］と［**Class**］を選択して、その選択に対応するアラートのみを表示します。
   b. ［**Update**］をクリックします。
   ［Severity］と［Class］に一致しないすべてのアラートがリストから削除されます。
3. ［**Details**］領域に特定アラートの追加情報を表示するには、リストのアラートをクリックします。
4. フィルタリングを削除し、再度、クリアされたアラートをすべて表示するには、［**Reset**］をクリックします。

［Alerts History］タブ

［Alerts History］タブには、クリアされたアラートのリストと選択したアラートに関する詳細が表示されます。

表 67 アラート リスト、列ラベルの説明

項目	説明
メッセージ	アラート メッセージ テキスト。
重大度	アラートの重大度のレベル。warning、critical、info、emergency など。
日付	アラートが発生した日時。
クラス	アラートが発生したサブシステム。
オブジェクト	アラートが発生した物理コンポーネント。
Status	ステータスが posted と cleared のどちらであるか。posted のアラートはクリアされていません。

表 68 ［Details］領域、行ラベルの説明

項目	説明
Name	アラートのテキスト識別子
メッセージ	アラート メッセージ テキスト。
重大度	アラートの重大度のレベル。warning、critical、info、emergency など。
クラス	アラートが発生したサブシステムとデバイス。
日付	アラートが発生した日時。
Object ID	アラートが発生した物理コンポーネント。
イベント ID	イベント ID。
Tenant Units	影響を受けるテナント ユニットをリストします。
関連情報	アラートについての詳細。
Status	ステータスが posted と cleared のどちらであるか。posted のアラートはクリアされていません。
説明	アラートについての詳細。
アクション	アラートに対応する方法の提案。

ハードウェア コンポーネント ステータスの表示

［Hardware Chassis］パネルには、シャーシ シリアル番号とエンクロージャ ステータスを含むシステムの各エンクロージャのブロック描画が表示されます。各ブロック描画には、ディスク、ファン、電源、NVRAM、CPU、メモリなどのエンクロージャ コンポーネントがあります。表示されるコンポーネントは、システムのモデルによって異なります。

DD OS 5.5.1 以降を実行しているシステムでは、システム シリアル番号も表示されます。DD4500、DD7200 などの新しいシステムでは、システム シリアル番号はシャーシ シリアル番号から独立しており、シャーシ交換など各種保守イベント中も変わりません。DD990 以前のレガシー システムでは、システム シリアル番号がシャーシ シリアル番号に設定されます。

手順

1. ［**Hardware**］ > ［**Chassis**］を選択します。

［Chassis］ビューには、システム エンクロージャが表示されます。Enclosure 1 はシステム コントローラーであり、残りのエンクロージャは Enclosure 1 の下に表示されます。

問題のあるコンポーネントは、黄（警告）または赤（エラー）が表示されます。それ以外の場合、コンポーネントは OK と表示されます。

2. カーソルをコンポーネントに合わせると、詳細ステータスが表示されます。

ファン ステータス

ファンには番号が付けられ、シャーシ内の場所に対応しています。システム ファンの上にカーソルを移動するとデバイスのヒントが表示されます

表 69 ファン ツールチップ、列ラベルの説明

項目	説明
説明	ファンの名前。
Level	現在の動作速度範囲（Low、Medium、High）。動作速度は、シャーシ内の温度によって変わります。
Status	ファンの稼働状態。

温度ステータス

Data Domain システムといくつかのコンポーネントは、構成できない温度プロファイルで定義される特定の温度範囲内で動作するように構成されます。温度ツールチップを表示するには、［Temperature］ボックスにカーソルを合わせます。

表 70 温度ツールチップ、列ラベルの説明

項目	説明
説明	測定中のシャーシ内の場所。表示されるコンポーネントはモデルによって異なり、多くの場合は略語で表示されます。次にいくつかの例を示します。 • CPU 0 Temp（中央処理装置） • MLB Temp 1（メイン論理ボード） • BP middle temp（バックプレーン） • LP temp（I/O ライザー FRU の薄型） • FHFL temp（I/O ライザー FRU のフルハイト フルレングス） • FP temp（フロント パネル）
C/F	C/F 列には、セ氏温度および華氏温度が表示されます。CPU の説明で［relative］（CPU n Relative）が指定されている場合、この列に各 CPU が最大許容温度を下回った温度の数とシャーシ内部（シャーシ周囲）の実際の温度が表示されます。
Status	温度ステータスを表示します。 • OK：温度は許容範囲内です。 • Critical：温度がシャットダウン温度よりも高い状態です。

表 70 温度ツールチップ、列ラベルの説明 （続き）

項目	説明
	• Warning：温度が警告温度よりも高いが、シャットダウン温度よりは低い状態です。 • ダッシュ（-）：コンポーネントに温度閾値が構成されていないため、ステータスはレポートされません。

管理パネルのステータス

DD6300、DD6800、DD9300 システムには、シャーシの背面に管理ネットワーク用の Ethernet ポートが搭載された固定管理パネルがあります。Ethernet ポートにカーソルを合わせると、ツールチップが表示されます。

表 71 管理パネルのツールチップ、列ラベルの説明

項目	説明
説明	管理パネルに搭載されている NIC のタイプ。
Vendor	管理 NIC の製造元。
ポート	管理ネットワーク（Ma）の名前。

SSD ステータス（DD6300 のみ）

DD6300 は、シャーシ背面にあるスロットで、最大 2 台のソリッド ステート ドライブをサポートしています。SSD スロットには番号が付けられ、シャーシ内の場所に対応しています。SSD の上にカーソルを移動するとデバイスのヒントが表示されます

表 72 SSD ツールチップ、列ラベルの説明

項目	説明
説明	SSD の名前。
ステータス	SSD の状態。
使用期間	定格耐用年数で SSD が使用済みのパーセンテージ。

電源ステータス

ツールチップには、電源のステータス（電源がない、または故障している場合、それぞれ［OK］または［DEGRADED］）が表示されます。また、エンクロージャのバック パネルを見て、各電源の LED をチェックし、交換が必要なものを特定できます。

PCI スロット ステータス

シャーシ ビューに表示される PCI スロットは、PCI スロットの数と各スロットの番号を示します。ツールチップは、PCI スロット内の各カードのコンポーネント ステータスを示します。たとえば、ある NVRAM カード モデルのツールチップには、メモリ サイズ、温度データ、バッテリー レベルが表示されます。

NVRAM ステータス

Non-Volatile RAM、バッテリー、その他のコンポーネントについての情報を表示するには、NVRAM にカーソルを合わせます。

表 73 NVRAM ツールチップ、列ラベルの説明

項目	説明
コンポーネント	コンポーネント リストの項目は、システムにインストールされている NVRAM によって変わります。含まれる項目は次のとおりです。 • ファームウェアのバージョン • メモリ サイズ • エラー数 • フラッシュ コントローラーのエラー カウント • ボード温度 • CPU 温度 • バッテリー数（バッテリーの数はシステム タイプに依存します）。 • NVRAM の現在のスロット番号。
C/F	摂氏/華氏形式で選択されたコンポーネントの温度を表示します。
値	選択されたコンポーネントに値が与えられ、その値は次の項目を示します。 • ファームウェア バージョン番号 • 表示されたユニットのメモリ サイズ値 • メモリ、PCI、コントローラーのエラー カウント • 次のグループにソートされるフラッシュ コントローラーのエラー カウント：構成エラー（Cfg Err）、パニック状態（Panic）、バスの異常停止、不正ブロック警告（Bad Blk Warn）、バックアップ エラー（Bkup Err）、リストア エラー（Rstr Err） • 充電率、ステータスなどのバッテリー情報（有効または無効）

システム統計の表示

［Realtime Charts］パネルには、CPU 使用率、ディスク トラフィックなど、リアルタイム サブシステム パフォーマンス統計を示す最大 7 個のグラフが表示されます。

手順

1. ［**Home**］ > ［**Realtime Charts**］を選択します。

   ［Performance Graphs］領域には、現在選択されているグラフが表示されます。
2. 表示するグラフの選択を変更するには、リスト ボックスでグラフのチェックボックスを選択およびクリアします。
3. 特定のデータ ポイント情報を表示するには、グラフ ポイントにカーソルを合わせます。

4. グラフに複数のデータが含まれる場合、グラフ右上のチェックボックスを使用して、表示するものを選択します。たとえば、ディスク アクティビティ グラフの右上で Read が選択されると、書き込みデータのみがグラフに表示されます。

結果

各グラフには、過去 200 秒の使用率が表示されます。［**Pause**］をクリックして、表示を一時的に停止します。［**Resume**］をクリックすると再開され、一時停止中に表示しなかったポイントが表示されます。

パフォーマンス統計グラフ

パフォーマンス統計グラフには、主要なシステム コンポーネントおよび機能の統計が表示されます。

DD Boost Active Connections

［DD Boost Active Connections］グラフには、過去 200 秒間の各 DD Boost のアクティブな接続数が表示されます。グラフ内の別の行には、読み取り（リカバリ）接続と書き込み（バックアップ）接続の数が表示されます。

DD Boost Data Throughput

［DD Boost Data Throughput］グラフには、過去 200 秒間に転送されたバイト数/秒が表示されます。グラフ内の各線は、DD Boost クライアントがシステムから読み取ったデータと DD Boost クライアントがシステムに書き込んだデータの比率を示します。

Disk

［Disk］グラフには、システム内のすべてのディスク間を行き来するデータ量が、受け取ったデータに基づいて適切な測定単位（1 秒あたりの KiB または MiB）で表示されます。

File System Operations

File System Operations グラフには、過去 200 秒に実行された 1 秒あたりの操作数の推移が表示されます。グラフ内の各ラインは、1 秒あたりの NFS および CIFS 操作を示します。

ネットワーク

Network グラフには、各 Ethernet 接続を通ってデータ量が、受け取ったデータに基づいて適切な測定単位（1 秒あたりの KiB または MiB）で表示されます。Ethernet ポートごとに 1 本の線が表示されます。

Recent CPU Usage

Recent CPU Usage グラフには、過去 200 秒に転送された CPU 使用率のパーセンテージの推移が表示されます。

Replication（DD Replicator のライセンスが必要です）

Replication グラフには、過去 200 秒にネットワークを介してやり取りしたレプリケーション データの量が表示されます。各線は、In と Out のデータを示します。

- In：DD Replicator ペアの他方から受信測定単位の総数（1 秒あたりのキロバイト数など）。宛先では、この値にバックアップ データ、レプリケーション オーバーヘッド、ネットワーク オーバーヘッドが含まれます。ソースでは、この値にレプリケーション オーバーヘッドとネットワーク オーバーヘッドが含まれます。
- Out：DD Replicator ペアの他方に送信した測定単位の総数（1 秒あたりのキロバイト数など）。ソースでは、この値にバックアップ データ、レプリケーション オーバーヘッド、ネットワーク オーバーヘッドが含まれます。宛先では、この値にレプリケーション オーバーヘッドとネットワーク オーバーヘッドが含まれます。

アクティブ ユーザーの表示

［Active Users］タブには、システムにログインしているユーザーの名前、現在のユーザー セッションに関する統計が表示されます。

手順

1. ［**Administration**］ > ［**Access**］ > ［**Active Users**］を選択します。

   各ユーザーの情報を表示する Active Users リストが表示されます。

   表 74 アクティブ ユーザー リスト、列ラベルの説明

項目	説明
Name	ログイン ユーザーのユーザー名。
Idle	ユーザーの最後の活動以降の時間。
Last Login From	ユーザーがログインしたシステム。
Last Login Time	ユーザーがログインした時間の日付スタンプ。
TTY	ログインの端末表記。DD System Manager ユーザーに GUI が表示されます。

注

ローカル ユーザーを管理するには、［**Go to Local Users**］をクリックします。

ヒストリ レポートの管理

DD System Manager では、最長過去 2 年間の Data Domain システムでのスペース使用状況をトラッキングするレポートを生成できます。レプリケーションの進行状況を確認できるレポートを生成したり、ファイル システムで日単位のレポートや累積レポートを表示することもできます。

［Reports］ビューは 2 つのセクションに分かれています。上のセクションでは、各種レポートを作成できます。下のセクションでは、保存されているレポートを表示および管理できます。

レポートは、そのタイプによってテーブル形式またはグラフとして表示されます。特定の Data Domain システムのレポートを選択し、特定の期間を指定することができます。

レポートには、リアルタイム データではなく履歴データが表示されます。生成されたレポートのグラフは静的であり、更新されません。レポートから取得できる情報のタイプの例には、次のものが含まれます。

- システムにバックアップされたデータの量と完了した重複排除の量
- 週次使用率トレンドに基づく、Data Domain システムがフルになったタイミングの推定
- 選択された間隔に基づくバックアップおよび圧縮の活用
- クリーニング サイクルの時間、クリーンできるスペースの量、再利用されたスペースの量を含む過去のクリーニング パフォーマンス
- ソースとデスティネーションでレプリケーションに使用される WAN 帯域幅の量と帯域幅がレプリケーション要件を満たすかどうか
- システム パフォーマンスおよびリソース使用率

レポートのタイプ

［New Report］領域には、システムで生成できるレポートのタイプが一覧表示されます。

注

レプリケーション レポートは、システムにレプリケーション ライセンスがあり、有効なレプリケーション コンテキストが構成されている場合にのみ作成できます。

File System Cumulative Space Usage Report

File System Cumulative Space Usage Report には、指定された期間、システムのスペース使用率の詳細を示す 3 種類のチャートが表示されます。このレポートは、バックアップされたデータの量、実行された重複解除の量、使用されるスペースの量の分析に使用されます。

表 75 ファイル システム：使用率チャート ラベルの説明

項目	説明
Data Written（GiB）	圧縮前に書き込まれたデータの量。これは、レポートの紫で網掛けされた部分によって示されます。
時刻	書き込まれたデータのタイムライン。このレポートで表示される時間は、チャートが作成されると、Duration の選択に基づいて変更されます。
Total Compression Factor	総圧縮率は、圧縮率をレポートします。

表 76 ファイル システム：使用量チャート ラベルの説明

項目	説明
Used（GiB）	圧縮後に使用されたスペースの量。
時刻	データが書き込まれた日付。このレポートで表示される時間は、チャートが作成されると、Duration の選択に基づいて変更されます。
Used (Post Comp)	圧縮後に使用されたストレージの量。
Usage Trend	黒い点線は、ストレージ使用率トレンドを示します。線が上部の赤線に達すると、ストレージはほぼフルになっています。
容量	Data Domain システムの合計容量。
Cleaning	Cleaning は、Cleaning サイクル（各クリーニング サイクルの開始時間と終了時間）です。管理者はこの情報を使用して、スペース クリーニングを実行する最善の時間と最適なスロットル設定を選択できます。

表 77 ファイル システム週間累積容量チャート ラベルの説明

項目	説明
Date (or Time for 24 hour report)	レポートに設定された基準に基づく、各週の最後の日。レポートでは、24 時間の期間は正午から次の正午となります。
Data Written (Pre-Comp)	指定された期間に圧縮前に書き込まれた累積データ。
Used (Post-Comp)	指定された期間に圧縮後に書き込まれた累積データ。
圧縮率	総圧縮率。これは、レポートの黒線によって示されます。

File System Daily Space Usage Report

File System Daily Space Usage Report には、指定された期間、スペース使用率の詳細を示す 5 種類のチャートが表示されます。このレポートは、日次アクティビティの分析に使用されます。

表 78 ファイル システム日次スペース使用率チャート ラベルの説明

項目	説明
Space Used（GiB）	使用中のスペースの量。Post-comp は、赤で網掛けされた部分です。Pre-Comp は、紫で網掛けされた部分です。
Time	データが書き込まれた日付。
Compression Factor	総圧縮率。これは、レポートでは黒い枠によって示されます。

表 79 ファイル システム日次容量使用率チャート ラベルの説明

項目	説明
Date	データが書き込まれた日付。
Data Written (Pre-Comp)	圧縮前に書き込まれたデータの量。
Used (Post-Comp)	圧縮後に使用されたストレージの量。
Total Compression Factor	総圧縮率。

表 80 ファイル システム週次容量使用率チャート ラベルの説明

項目	説明
Start Date	このサマリーの、週の最初の日。
End Date	このサマリーの、週の最後の日。
Available	使用可能なストレージの総量。
Consumed	使用中のストレージの総量。
Data (Post -Comp)	指定された期間に圧縮前に書き込まれた累積データ。
Replication (Post-Comp)	指定された期間に圧縮後に書き込まれた累積データ。
Overhead	非データ ストレージに使用されている追加のスペース。
Reclaimed by Cleaning	クリーニング後に再利用されている総スペース。

表 81 ファイル システム圧縮サマリー チャート ラベルの説明

項目	説明
Time	このレポートのデータ コレクションの期間。
Data Written (Pre-Comp)	圧縮前に書き込まれたデータの量。
Used (Post-Comp)	圧縮後に使用されたストレージの量。
Total Compression Factor	総圧縮率。

表 82 ファイル システム クリーニング アクティビティ チャート ラベルの説明

項目	説明
Start Time	クリーニング アクティビティが開始された時刻。
End Time	クリーニング アクティビティが終了した時刻。
Duration（Hours）	クリーニングに必要な合計時間（時間単位）。
Space Reclaimed	再利用されているスペース（GiB（ギビバイト））。

レプリケーション ステータス レポート

[Replication Status] レポートには、システムで実行中の現在のレプリケーション ジョブのステータスを示す 3 種類のチャートが表示されます。このレポートは、すべてのレプリケーション コンテキストで発生していることのスナップショットを提供するために使用され、Data Domain システムでの全体的なレプリケーション ステータスの理解に役立ちます。

表 83 レプリケーション コンテキスト サマリー チャート ラベルの説明

項目	説明
ID	Replication Context ID。
Source	ソース システム名。
Destination	宛先システム名。
Type	レプリケーション コンテキストのタイプ： MTree、Directory、Collection、または Pool。
Status	レプリケーション ステータス タイプ： Error、Normal。
Sync as of Time	最後の同期の日時スタンプ。
Estimated Completion	レプリケーションが完了する推定時間。
Pre-Comp Remaining	レプリケーションされる圧縮前データの量。これは、Collection タイプにのみ適用されます。
Post-Comp Remaining	レプリケーションされる圧縮後データの量。これは、Directory および Pool タイプにのみ適用されます。

表 84 レプリケーション コンテキスト エラー ステータス チャート ラベルの説明

項目	説明
ID	Replication Context ID。
Source	ソース システム名。
Destination	宛先システム名。
Type	レプリケーション コンテキスト タイプ： Directory または Pool。
Status	レプリケーション ステータス タイプ： Error、Normal、Warning。
Description	エラーの説明。

表 85 レプリケーション宛先スペース可用性チャート ラベルの説明

項目	説明
Destination	宛先システム名。
Space Availability（GiB）	使用可能なストレージの総量。

レプリケーション サマリー レポート

レプリケーション サマリー レポートには、システムのネットワーク全体のレプリケーションのための入出力状況に関するパフォーマンス情報に加え、指定された期間のコンテキスト レベルごとのパフォーマンス情報が表示されます リストから分析されるコンテキストを選択します。

表 86 レプリケーション サマリー レポート ラベルの説明

項目	説明
Network In（MiB）	システムに入るデータの量。Network In は、細い緑の線で示されます。
Network Out（MiB）	システムから送信されたデータの量。Network Out は、太いオレンジ色の線で示されます。
Time	データが書き込まれた日付。
Pre-Comp Remaining（MiB）	レプリケーションされる圧縮前データの量。Pre-Comp Remaining は、青の線で示されます。

タスク ログの表示

タスク ログには、レプリケーション、システム アップグレードなどの現在実行中のジョブのリストが表示されます。DD System Manager は、複数のシステムを管理し、それらのシステムでタスクを開始できます。タスクがリモート システムで開始された場合、そのタスクの進行状況は、リモート システム タスク ログではなく管理ステーション タスク ログで追跡されます。

手順

1. ［**Health**］ > ［**Jobs**］を選択します。

   ［Tasks］ビューが表示されます。

2. ［Filter By］リスト ボックスから Task Log を表示するフィルターを選択します。［**All**］、［**In Progress**］、［**Failed**］、または［**Completed**］を選択できます。

   ［Tasks］ビューには、選択するフィルターに基づきすべてのタスクのステータスが表示され、60 秒ごとに更新されます。

3. 手動で［Tasks］リストを更新するには、次のいずれかを行います。

   - タスク ログを更新するには、［**Update**］をクリックします。
   - すべてのタスクを表示して、設定したフィルターを削除するには、［**Reset**］をクリックします。

4. タスクの詳細を表示するには、タスク リストでタスクを選択します。

表 87 詳細情報、ラベルの説明

項目	説明
System	ファイル名
Task Description	タスクの説明。
Status	タスクのステータス（completed、failed、または in progress）。
Start Time	タスクが開始された日時。
終了時刻	タスクが終了した日時。
Error Message	アプリケーション エラー メッセージ（もしあれば）。

システムの高可用性ステータスの表示

［**High Availability**］パネルを使用すると、システムの HA ステータスに関する詳細情報、および必要な場合にシステムがフェイルオーバーを実行できるかどうかを確認することができます。

手順

1. DD System Manager で、［**Health**］**>**［**High Availability**］を選択します。

   ［**Health High Availability**］画面が表示されます。
   緑色のチェック マークは、システムが正常に動作し、フェイルオーバーの準備が整っていることを示しています。

   画面には、アクティブ ノード（通常はノード 0）が表示されます。

2. ノードにカーソルを合わせてステータスを確認します。

   ノードがアクティブな場合は、青色でハイライト表示されます。

3. アクティブ ノードからスタンバイ ノード（通常はノード 1）にビューを変更する場合は、バナーのドロップダウン メニューをクリックします。

高可用性のステータス

［**Health High Availability**］（HA）ビューには、ノードと、ノードに接続されているストレージの図を使用して、システムのステータスに関する情報が表示されます。さらに、システムの詳細情報に加えて現在のアラートもすべて確認できます。

アクティブ ノードとストレージが動作しているかどうかは、カーソルを合わせるとわかります。それぞれが正常に動作している場合は、青色でハイライト表示されます。スタンバイ ノードはグレーで表示されます。

また、コンポーネントをクリックしてアラート テーブルをフィルタリングすることもできます。選択したコンポーネントに関連するアラートのみが表示されます。

図 6 稼働状態/高可用性インジケーター

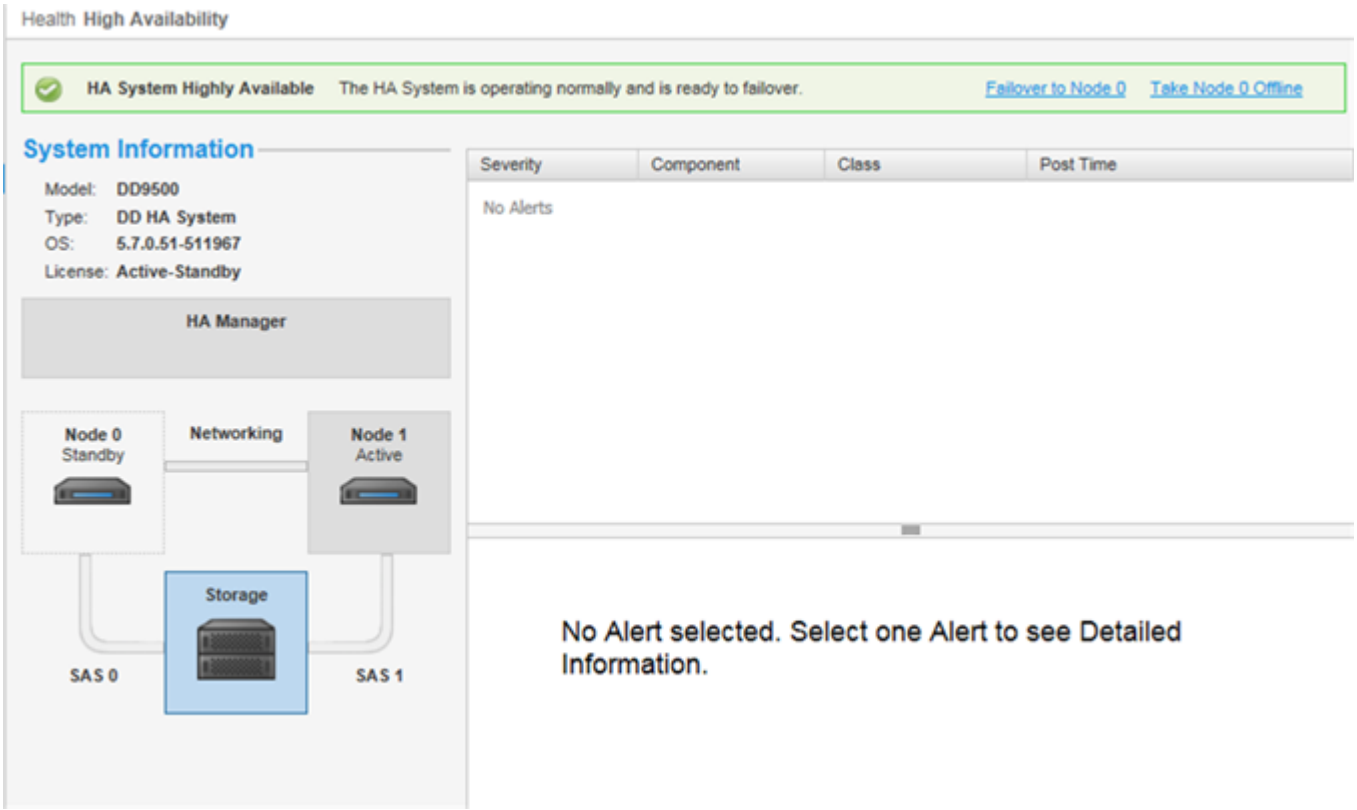


表 88 高可用性インジケーター

項目	説明
HA システム バー	システムが正常に動作し、フェイルオーバーの準備が整っている場合は、緑色のチェック マークが表示されます。
ノード 0 にフェイルオーバー	スタンバイ ノードに手動でフェイルオーバーすることができます。
ノード 1 をオフラインに	必要な場合、アクティブ ノードをオフラインにすることができます。
システム情報	Data Domain システムのモデル、システムのタイプ、使用中の Data Domain オペレーティング システムのバージョン、適用されている HA ライセンスを一覧表示します。
HA Manager	ノード、ノードに接続されているストレージ、HA 相互接続、ケーブル接続が表示されます。
重大度	システムの HA ステータスに影響を及ぼす可能性のあるすべてのアラートの重大度を示します。
コンポーネント	影響を受けるコンポーネントを示します。
クラス	ハードウェア、環境、その他など、受信アラートのクラスを示します。

表 88 高可用性インジケーター （続き）

項目	説明
投稿時刻	アラートが記録された日時を示します。

第 5 章

ファイル システム

本章には、次のセクションが含まれます。

- ファイル システムの概要 194
- ファイル システムの使用状況のモニタリング 201
- ファイル システム操作の管理 209
- Fast Copy 操作 217

ファイル システムの概要

ファイル システムの使用方法について説明します。

ファイル システムによるデータの保存方法

Data Domain ストレージ容量は、複数のバックアップを保存し、次のクリーニングまでバックアップの保存用として 20%の空きスペースを維持することで適切に管理されます。スペースの使用量は、主にデータのサイズと圧縮率、保存期間に影響します。

Data Domain システムは、バックアップおよびアーカイブ データ用の非常に信頼性の高いオンライン システムとして設計されています。新しいバックアップがシステムに追加されると、古いシステムは削除されます。この削除は通常、設定された保存期間に基づき、バックアップまたはアーカイブ ソフトウェアの制御の下で行われます。

バックアップ ソフトウェアが Data Domain システムから古いバックアップを期限切れにするか、削除した場合、その Data Domain システムのスペースは Data Domain システムがディスクから期限切れしたバックアップのデータをクリーニングした後にのみ使用可能になります。Data Domain システムのスペースを管理する優れた方法として、ある程度の空きスペース（使用可能なスペース全体の約 20%）を残しつつ、できる限り多くのオンライン バックアップを保持して、デフォルトで週 1 回実行される、次にスケジュール設定されたクリーニングまで快適にバックアップを格納することが挙げられます。

一部のストレージ容量は、Data Domain システムが内部インデックスとその他のメタ データに使用できます。メタ データ用に一定期間使用されるストレージの量は、保存されたデータのタイプと保存されたファイルのサイズによって異なります。それ以外の点では全く同じ 2 つのシステムの場合、各システムに異なるデータ セットが送信されると、時間が経つにつれ片方のシステムの方が他方より、実際のバックアップ データよりもメタデータに多くのスペースを確保するようになる可能性があります。

Data Domain システム上のスペース使用率は、主に次の要素によって影響を受けます。

- バックアップ データのサイズと圧縮率。
- バックアップ ソフトウェアで指定された保存期間。

重複が多いデータセットをバックアップし、長期間それらを保持する場合の圧縮結果の概要。

ファイル システムによるスペース使用率のレポート方法

すべての DD System Manager のウィンドウとシステム コマンドは、2 進数計算を使用してストレージ容量を表示します。たとえば、使用中のディスク領域の 1 GiB を表示するコマンドは、2^{30} バイト = 1,073,741,824 バイトをレポートします。

- 1 KiB = 2^{10} = 1024 バイト
- 1 MiB = 2^{20} = 1,048,576 バイト
- 1 GiB = 2^{30} = 1,073,741,824 バイト
- 1 TiB = 2^{40} = 1,099,511,627,776 バイト

ファイル システムによる圧縮の使用

ファイル システムは、データを格納するときに使用可能なディスク領域を最適化するために圧縮を使用するため、ディスク領域は物理と論理の 2 通りで計算されます （圧縮のタイプに関するセクションを参照してください）。物理スペースは、Data Domain システムで使用される実際のディスク領域です。論理スペースは、システムに書き込まれた未圧縮データの量です。

ファイル システム スペース レポート ツール（DD System Manager グラフと `filesys show space` コマンド、またはエイリアス `df`）は、物理スペースと論理スペースを両方表示します。これらのツールは、使用中のスペースと使用可能なスペースのサイズと量もレポートします。

Data Domain システムがマウントされると、ファイル システムによるスペースの物理的使用率を表示する通常のツールが使用できます。

ファイル システムが容量の 90%、95%、および 100%に達すると、Data Domain システムは警告メッセージを出します。次に示すデータ圧縮についての情報は、一定期間にわたるディスク利用のガイドラインです。

Data Domain システムが長時間使用するディスク領域の量は、次の要素によって異なります。

- 初期フル バックアップのサイズ。
- 一定期間内に保存された追加バックアップ（増分およびフル）の数。
- バックアップ データセットの増加率。
- データの変更率。

通常の変更率と増加率のデータ セットの場合、データ圧縮は通常、次のガイドラインに適合します。

- Data Domain システムの最初のフル バックアップの場合、圧縮率は通常 3:1 です。
- 初期フル バックアップの各増分バックアップの圧縮率は通常、6:1 の範囲内です。
- 次のフル バックアップの圧縮率は約 60:1 です。

週 1 回のフル バックアップおよび 1 日 1 回の増分バックアップのスケジュールで一定期間行う場合、すべてのデータの累積圧縮率は約 20:1 となります。増分のみのデータまたは重複データの少ないバックアップの場合、圧縮率は低くなります。すべてのバックアップがフル バックアップの場合、圧縮率は高くなります。

圧縮のタイプ

Data Domain は、2 つのレベル（グローバルとローカル）でデータを圧縮します。Global Compression は、すでにディスクに保存されているデータと受信済みデータを比較します。新しいデータはディスクに書き込み前にローカルで圧縮されますが、重複データは再度保存する必要はありません。

ローカル圧縮

Data Domain システムは、データがディスクに書き込まれるときのスループットを最大化するために開発されたローカル圧縮アルゴリズムを使用します。デフォルト アルゴリズム（lz）によって、バックアップ ジョブのバックアップ ウィンドウを短くできますが、より多くのスペースを使用します。他に 2 種類のローカル圧縮（gz、gzfast）を使用できます。いずれも lz と比べて圧縮率が向上しますが、CPU ロードが増えるという代償があります。ローカル圧縮オプションは、パフォーマンスの低下とスペース使用のトレードオフを伴います。ローカル圧縮を無効にすることもできます。圧縮を変更するには、ローカル圧縮の変更（215 ページ）を参照してください。

圧縮の変更後、すべての新しい書き込みで新しい圧縮タイプが使用されます。既存のデータは、クリーニング中に新しい圧縮タイプに変換されます。圧縮の変更前に存在していたすべてのデータを圧縮しなおすには、数ラウンドのクリーニングが必要です。

圧縮変更後の最初のクリーニングは、通常よりも時間がかかります。圧縮タイプを変更したかどうかにかかわらず、システムを 1 週間または 2 週間にわたり注意深く監視し、それが適切に動作していることを検証します。

ファイル システムによるデータの整合性の実装

データが Data Domain システム ディスクに正しく書き込まれたことを確認するため、バックアップ アプリケーションから受信したデータに対して複数のレイヤーのデータ検証が DD OS ファイル システムによって実行されます。それによって、エラーなくデータを取得できます。

DD OS は、データ保護目的で構築されており、データ非脆弱性を備えるアーキテクチャで設計されています。この後のセクションで示すとおり、4 つの重要な領域があります。

エンド・ツー・エンドの検証

エンド ツー エンド チェックは、すべてのファイル システム データとメタデータを保護します。データがシステムに書き込まれると、堅牢なチェックサムが計算されます。データは非重複化され、ファイル システム上に保存されます。すべてのデータは、ディスクにフラッシュされた後、読み取られ、再度チェックサムが行われます。データとファイル システム メタデータ両方が正しく保存されていることを検証するため、チェックサムが比較されます。

障害回避と抑制

Data Domain は、既存のデータを上書きまたは更新しないログ構造化ファイル システムを使用します。新しいデータが常に新しいコンテナーに書き込まれ、既存の古いコンテナーに追加されます。古いデータ コンテナは適切に保持され、ソフトウェア的な障害やデータ書き込み中に発生しうるハードウェア的な障害からも守られています。

継続的なエラー検出と修正

継続的な障害検知と復旧の機能がストレージ システム障害を未然に防ぎます。システムは定期的に RAID ストライプの整合性を検証し、RAID の冗長性を活用して障害点を復旧します。毎読み取り時に、データの整合性が確認され、エラーがオンザフライで補正されます。

ファイル・システムの復旧可能性

データは自己記述形式で書き込まれる 必要に応じて、ログをスキャンし、データ領域に埋め込まれたメタデータを再構築することでファイル システムを再生成することができます。

ファイル システムがファイル システム クリーニングによってストレージ領域を再利用する方法

バックアップ アプリケーション（NetWorker または NetBackup など）のデータが期限切れになると、データは Data Domain システムによって削除としてマークされます。ただし、このデータはすぐには削除されず、クリーニング操作中に削除されます。

- クリーニング操作中でも、ファイル システムは、バックアップ（書き込み）やリストア（読み取り）など通常のすべての処理に使用できます。
- クリーニングは大量のシステム リソースを使用しますが、クリーニングはセルフ スロットリングのため、ユーザー トラフィックの存在下でシステム リソースを引き渡します。
- Data Domain は、Data Domain システムの最初のフル バックアップ後にクリーニング操作を実行することを推奨します。フル バックアップでの初期のローカル圧縮は、通常 1.5～2.5 の圧縮比です。即時クリーニングの操作ではさらに 1.15～1.2 の圧縮比が追加され、対応する容量のディスク領域が再利用されます。
- クリーニング操作が終了すると、再利用されたストレージ領域の割合を示すメッセージがシステム ログに送信されます。

デフォルト スケジュールは、毎週火曜日午前 6 時（tue 0600）にクリーニング操作を実行します。スケジュールは変更でき、操作を手動で実行することもできます（クリーニング スケジュールの変更に関するセクションを参照してください）。

Data Domain は、週に 1 回クリーニング操作を実行することを推奨します。

ファイル システムを無効化する、またはクリーニング操作中 Data Domain システムをシャットダウンする操作（システム電源オフ、再起動など）は、クリーニング操作を中止します。システムの再起動時、クリーニング操作はすぐに再開されません。手動でクリーニング操作を再開するか、次にスケジュール設定されたクリーニング操作まで待ちます。

コレクション レプリケーションでは、レプリケートされていないソース システム上のレプリケーション コンテキストのデータをファイル システムのクリーニングのために処理することはできません。ソース システムとデスティネーション システムが同期していないことが原因でファイル システムのクリーニングを完了できない場合、システムではクリーニング操作のステータスが `partial` と報告され、クリーニング操作にはごく一部のシステム統計しか使用できません。コレクション レプリケーションが無効になっている場合、レプリケーションのソース システムとデスティネーション システムが同期しない状態が続くため、ファイル システムのクリーニングのために処理できないデータの量が増加します。オンライン サポート サイト（https://support.emc.com）にあるナレッジ ベース記事「Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases」に補足情報が記載されています。

MTree レプリケーションの場合、スナップショットのレプリケーション中にファイルが作成され、削除された場合、次のスナップショットにはこのファイルについての情報がなく、システムはこのファイルに関連づけられたコンテンツをレプリケーションしません。作成と削除は近い間隔で実行されますが、ディレクトリ レプリケーションは作成と削除両方をレプリケーションします。

ディレクトリ レプリケーションが使用するレプリケーション ログの場合、削除、名称変更などの操作はシングル ストリームとして実行されます。これによって、レプリケーション スループットが減ります。MTree レプリケーションによるスナップショットを使用することで、この問題を避けることができます。

サポートされるインターフェイス

ファイル システムでサポートされるインターフェイスは次のとおりです。

- NFS
- CIFS
- DD Boost
- DD VTL

対応しているバックアップ ソフトウェア

バックアップ ソフトウェアおよびバックアップ サーバーを Data Domain システムで使用できるように設定するためのガイダンスは、support.emc.com で取得できます。

新しい Data Domain システムに送信されるデータ ストリーム

パフォーマンスを最適にするため、Data Domain は Data Domain システムとバックアップ サーバー間の同時ストリームに対する制限を推奨します。

次のテーブルのコンテキストでは、データ ストリームが、バックアップ ファイルへの書き込みストリーム、リストア イメージからの読み取りストリームなどのシーケンシャル ファイル アクセスに伴うバイト数の大きいストリームを指します。レプリケーション ソースまたはデスティネーション ストリームは、ディレクトリ レプリケーション操作またはファイル レプリケーション操作に伴う DD Boost ファイル レプリケーション ストリームを指します。

表 89 新しい Data Domain システムに送信されるデータ ストリーム

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD140、DD160、DD610	4 GB または 6 GB / 0.5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620、DD630、DD640	8 GB / 0.5 GB または 1 GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640、DD670	16 GB または 20 GB / 1 GB	90	30	60%	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670、DD860	36 GB / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b]/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 または 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60%	16	30	60%	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 または 64 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 または 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256 / 512 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885

表 89 新しい Data Domain システムに送信されるデータ ストリーム （続き）

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD9800	256/768 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest+w<=1080; Total<=1885
DD6300	48/96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8 TB	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE 16 TB	16 GB / 512 MB または 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE 32 TB	24 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 48 TB	36 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 TB	48 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96 TB	64 GB / 2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 4 TB	12 GB（仮想メモリー） / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 TB	32 GB（仮想メモリー）/ 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16 TB	32 GB（仮想メモリー）/ 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 32 TB	46 GB（仮想メモリー）/ 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

表 89 新しい Data Domain システムに送信されるデータ ストリーム （続き）

a. DirRepl, OptDup, MTreeRepl streams
b. Data Domain Extended Retention ソフトウェア オプションは、（最大）メモリが拡張されたデバイスでのみ使用可能です。

ファイル システムの制限

ファイル システムの制限事項には、ファイル、バッテリーなどの数の制限が含まれます。

Data Domain システムにおけるファイル数の制限

10 億を超えるファイルの格納による影響および考慮事項。

Data Domain は、システム上に格納するファイルの数は 10 億個までとすることを推奨します。大量のファイルを格納すると、クリーニングのパフォーマンスと長さに悪影響が出る可能性があり、ファイル システム クリーニングなどの一部のプロセスは、大量のファイルがある場合、実行にかかる時間がかなり長くなる可能性があります。たとえば、クリーニングの列挙フェーズは、システムにおけるファイル数によって数分から数時間かかる場合があります。

注

システムが最大ファイル量に対応する必要があり、クライアント マシンからの作業負荷が注意深く制御されていない場合、Data Domain システムの全体的なパフォーマンスは許容範囲外のレベルまで落ちます。

ファイル システムが 10 億個のファイル数制限をクリアすると、複数のプロセスまたは操作が次のような悪影響を受ける可能性があります。

- クリーニング完了まで非常に長い時間かかる可能性があります （おそらく数日）。
- AutoSupport 操作には、さらに長い時間がかかる可能性があります。
- すべてのファイルの列挙に必要なプロセスまたはコマンド。

小さいファイルが多くある場合、他にも次のような懸念があります。

- サイズが非常に小さい場合でも、Data Domain システムに移動できる MB/s ではなく、1 秒あたりの作成可能な個別のファイル数が制限されます。サイズが大きい場合、ファイル作成速度は需要ではありませんが、ファイルが小さい場合、ファイル作成速度が支配的であり、要因の 1 つになる場合があります。ファイル作成速度は、MTree と CIFS 接続の数によって、1 秒あたり約 100～200 ファイルです。顧客環境が大量のファイルの一括取り込みを必要とする場合、この速度をシステムのサイズ設定時に考慮する必要があります。
- ファイル アクセス レーテンシーは、ディレクトリ内のファイル数に影響されます。可能な範囲で、ディレクトリ サイズは 250,000 未満にすることを推奨します。ディレクトリ サイズがそれより大きいと、ディレクトリ内のファイルのリスト、ファイルの開閉などのメタデータ操作に対する応答が遅くなる可能性があります。

バッテリーの制限

NVRAM を使用するシステムの場合、オペレーティング システムはバッテリーの充電が容量の 80% を下回ると低バッテリーアラートを出し、ファイル システムは無効になります。

通知

Data Domain DD2200 システムは NVRAM を使用しないため、ファームウェア計算によって、データを保存するために十分なバッテリーの充電があるかどうかを判断し、AC 電源が失われた場合にファイル システムを無効化します。

サポートされる inode の最大数

NFS または CIFS クライアント リクエストが発行されると、Data Domain システムは約 20 億個の inode（ファイルとディレクトリ）をレポートします。Data Domain システムはこの数字を超えることはできますが、クライアント上でのレポートが不正確になる場合があります。

最大パス名長

フル パス名の最大長（`/data/col1/backup` の文字を含む）は 61 文字です。シンボリック リンクの最大長も 61 文字です。

HA フェイルオーバー中のアクセス制限

高可用性システムでのフェイルオーバー時には、ファイルへのアクセスが最大で 10 分間中断される可能性があります （DD Boost および NFS ではさらに時間が必要です）。

ファイル システムの使用状況のモニタリング

リアルタイム データ ストレージ統計が表示されます。

［File System］ビューには、リアルタイムのデータ ストレージ統計情報、クラウド ユニット情報、暗号化情報、およびスペース使用量、消費係数、データ書き込みトレンドのグラフにアクセスするためのタブとコントロールが用意されています。また、ファイル システム クリーニング、拡張、コピー、破棄の管理に関するコントロールもあります。

［File System］ビューへのアクセス

このセクションでは、ファイル システムの機能について説明します。

手順

- ［**Data Management**］ > ［**File System**］を選択します。

［File System Status］パネルについて

ファイル システム サービスのステータスを表示します。

［File System Status］パネルにアクセスするには、［**Data Management**］ > ［**File System**］ > ［**Show Status of File System Services**］の順にクリックします。

ファイル システム

［**File System**］フィールドには、［**Enable**］/［**Disable**］リンクが含まれ、ファイル システムの作業状態が表示されます。

- Enabled and running：直近の連続した期間、ファイル システムが有効かつ実行中の状態でした。
- Disabled and shutdown。
- Enabling and disabling：有効化または無効化処理中。
- Destroyed：ファイル システムが削除された場合。

- Error：ファイル システムを初期化する問題などのエラー条件がある場合。

Cloud File Recall

［**Cloud File Recall**］フィールドには、Cloud Tier からファイルのリコールを開始する［**Recall**］リンクがあります。任意のアクティブなリコールが進行中であれば、［**Details**］リンクが利用可能です。詳細については、「クラウド階層からのファイルのリコール」を参照してください。

物理容量の測定

［**Physical Capacity Measurement**］フィールドには、物理容量の測定ステータスが無効な場合、［**Enable**］ボタンが表示されます。有効な場合は、システムに［**Disable**］ボタンおよび［**View**］ボタンが表示されます。［**View**］をクリックすると、MTree、優先度、送信時間、開始時間、期間など、現在実行されている物理容量の測定情報が表示されます。

データ移行

［**Data Movement**］フィールドには、［**Start**］/［**Stop**］ボタンが含まれ、最後のデータ移動操作が終了した日付、コピーされたファイルの数、コピーされたデータ量を表示します。システムには、データ移動操作が利用可能であれば［**Start**］ボタン、データ移動操作が実行中であれば［**Stop**］ボタンが表示されます。

アクティブ階層のクリーニング

［**Active Tier Cleaning**］フィールドには、［**Start**］/［**Stop**］ボタンが含まれ、最後にクリーニング操作が行われた日付または（クリーニング操作が現在実行中の場合）現在のクリーニング ステータスを表示します。例：

```
Cleaning finished at 2009/01/13 06:00:43
```

または（ファイル システムが無効化されている場合）

```
Unavailable
```

クラウド階層のクリーニング

［**Cloud Tier Cleaning**］フィールドには、［**Start**］/［**Stop**］ボタンが含まれ、最後にクリーニング操作が行われた日付または（クリーニング操作が現在実行中の場合）現在のクリーニング ステータスを表示します。例：

```
Cleaning finished at 2009/01/13 06:00:43
```

または（ファイル システムが無効化されている場合）

```
Unavailable
```

［Summary］タブについて

［Summary］タブをクリックすると、アクティブ階層とクラウド階層のスペース使用量統計が表示されます。また、ファイル システムのステータス表示、ファイル システムの設定、Fast Copy 操作の実行、容量の拡張、ファイル システムの破棄を行うコントロールにアクセスできます。

各階層では、スペース使用量統計に以下が含まれます。

- ［**Size**］：データに使用可能な物理ディスク スペースの総量。
- ［**Used**］：圧縮されたデータに使用されている実際の物理領域。使用量が 90%、95%、100%に達すると、警告メッセージがシステム ログに送られ、メール アラートが生成されます。100%になると、Data Domain システムはそれ以上バックアップ ホストからデータを受け取りません。
  使用量が常に高い場合、コマンド スケジュールをチェックして、クリーニング操作が自動的に実行される頻度を確認します。その後、「クリーニング スケジュールの変更」の手順に従い、操作を

行う回数を増やします。データ保存期間を短縮するか、他の Data Domain システムにバックアップ データの一部を分割することを検討します。

- ［**Available**］ (GiB)：データ ストレージに使用可能なスペースの総量。Data Domain システムがデータで満たされるのに伴って、内部インデックスが拡張することがあるため、この値は変化する場合があります。インデックスの拡張は、使用可能な GiB の量から領域を使用します。
- ［**Pre-Compression**］ (GiB)：圧縮前に書き込まれたデータ。
- ［**Total Compression Factor (Reduction %)**］：圧縮前/圧縮後。
- ［**Cleanable (GiB)**］：クリーニング操作が実行された場合に再利用できる領域の推定量。

Cloud Tier の場合、［**Cloud File Recall**］フィールドには、Cloud Tier からファイルのリコールを開始する［**Recall**］リンクがあります。任意のアクティブなリコールが進行中であれば、［**Details**］リンクが利用可能です。詳細については、「クラウド階層からのファイルのリコール」を参照してください。

別のパネルには、各階層の過去 24 時間にわたる次の統計情報が表示されます。

- ［**Pre-Compression** ］ (GiB)：圧縮前に書き込まれたデータ。
- ［**Post-Compression**］ (GiB)：圧縮後使用されたストレージ。
- ［**Global Compression Factor**］：（Pre-Compression/グローバル圧縮後のサイズ）。
- ［**Local Compression Factor**］：（グローバル圧縮後のサイズ） /Post-Compression）。
- ［**Total Compression Factor (Reduction %)**］：［（Pre-Comp - Post-Comp） /Pre-Comp］*100。

ファイル システムの設定について

システム オプションと現在のクリーニング スケジュールを表示および変更します。

［File System Settings］ダイアログにアクセスするには、［**Data Management**］ > ［**File System**］ > ［**Settings**］の順にクリックします。

表 90 全般的な設定

全般的な設定	説明
Local Compression Type	使用中のローカル圧縮のタイプ。 • 概要は、圧縮のタイプに関するセクションを参照してください。 • ローカル圧縮の変更に関するセクションを参照してください。
Cloud Tier Local Comp	クラウド階層の使用中の圧縮のタイプ。 • 概要は、圧縮のタイプに関するセクションを参照してください。 • ローカル圧縮の変更に関するセクションを参照してください。
Report Replica as Writable	アプリケーションによるレプリカの扱い。 • 読み取り専用設定の変更に関するセクションを参照してください。
Staging Reserve	ディスク ステージングを管理します。 • ディスク ステージングの処理に関するセクションを参照してください。 • ディスク ステージングの構成に関するセクションを参照してください。
Marker Type	データ ストリームのバックアップ ソフトウェア マーカー（テープ マーカー、タグ ヘッダー、またはその他の名前が使用されます）。テープ マーカー設定に関するセクションを参照してください。

表 90 全般的な設定 （続き）

全般的な設定	説明
スロットル	物理容量の測定スロットルの設定に関するセクションを参照してください。
キャッシュ	物理容量キャッシュの初期化によって、キャッシュをクリーンアップして、測定速度を向上させます。

ファイル システムのワークロードのバランスを調整することで、使用状況に基づいてパフォーマンスを向上させることができます。

表 91 ワークロード バランスの設定

ワークロード バランスの設定	説明
Random workloads (%)	ランダム ワークロードを使用すると、インスタント アクセスとリストアのパフォーマンスが向上します。
Sequential workloads (%)	ランダムなワークロードを使用すると、従来のバックアップとリストアのパフォーマンスが向上します。

表 92 データ移動の設定

データ移動ポリシーの設定	説明
File Age Threshold	データの移動が開始されると、指定された閾値の日数の間変更されていないファイルは、すべてアクティブ階層からアーカイブ階層に移動されます。
Schedule	データを移動する日時を指定します。
スロットル	システムがデータの移動に使用できるリソースの割合。100%のスロットル値はデフォルト値として、データ移動は制限されていないことを意味します。

表 93 クリーニングの設定

クリーニング スケジュールの設定	説明
時刻	日時クリーニング操作が実行されます。 • クリーニング スケジュールの変更に関するセクションを参照してください。
スロットル	システム リソース割り当て。 • クリーニング操作の変更に関するセクションを参照してください。

［Cloud Units］タブについて

クラウド ユニットに関するサマリー情報を表示し、クラウド ユニットを追加および変更し、証明書を管理します。

［File System］ページ上の［Cloud Units］タブは、オプション DD Cloud Tier ライセンスが有効な場合にのみ表示されます。このビューには、サマリー情報（ステータス、ネットワーク帯域幅、読み取りアクセス、ローカル圧縮、データ移動、データ ステータス）、クラウド プロバイダーの名前、使用済

み容量、および、ライセンスされた容量が表示されます。クラウド ユニットの編集、証明書の管理、新しいクラウド ユニットの追加を行うためのコントロールが用意されています。

［Retention Units］タブについて

保存ユニットとその状態、ステータス、サイズが表示されます。

［File System］ページ上の［Retention Units］タブは、オプション DD Extended Retention ライセンスが有効な場合にのみ表示されます。このビューには、保存ユニットがリストされ、その状態（new、sealed、または target）、ステータス（disabled または ready）、サイズが表示されます。ユニットが封印され、データが追加できない場合、封印された日付が表示されます。

列見出しの右のひし形記号を選択して、値の順序を逆にソートします。

［DD Encryption］タブについて

暗号化ステータス、進行状況、アルゴリズムなどが表示されます。

表 94 ［DD Encryption］の設定

設定	説明
DD System	ステータスは以下のいずれかになります。 • Not licensed：他の情報がありません。 • Not configured：暗号化がライセンスされているが、構成されていません。 • Enabled：暗号化が有効で実行中です。 • Disabled：暗号化が無効です。
アクティブ階層	アクティブ階層の暗号化ステータスを表示します。 • Enabled：暗号化が有効で実行中です。 • Disabled：暗号化が無効です。
Cloud Unit	クラウド ユニットごとの暗号化ステータスを表示します。 • Enabled：暗号化が有効で実行中です。 • Disabled：暗号化が無効です。
Encryption Progress	データの変更と再暗号化の適用に関するアクティブ階層の暗号化ステータスの詳細を表示します。ステータスは以下のいずれかになります。 • なし • Pending • Running • Done ［View Details］をクリックして、［Encryption Status Details］ダイアログを表示します。アクティブ階層に関する次の情報が表示されます。 • Type（例：暗号化がすでに開始されている場合は［Apply Changes］、暗号化が危害を受けたデータ（おそらく過去の破棄されたキーの結果である場合は［Re-encryption］）。 • Status（例：［Pending］）。

表 94 ［DD Encryption］の設定 （続き）

設定	説明
	• Details：（例：12 月 xx/xx/xx に要求され、次のシステム クリーニング後に取得）。
暗号化アルゴリズム	データの暗号化に使用されるアルゴリズム： • AES 256-bit（CBC）（デフォルト） • AES 256-bit（GCM）（より安全だが、速度が遅い） • AES 128-bit（CBC）（256-bit と同程度に安全） • AES 128-bit（GCM）（256-bit と同程度に安全） 詳細については「暗号化アルゴリズムの変更」を参照してください。
Encryption Passphrase（暗号化パスフレーズ）	構成されると、「*****」と表示されます。パスフレーズの変更方法については、「システム パスフレーズの管理」を参照してください。
File System Lock	
Status	File System Lock ステータスは、次のいずれかとなります。 • Unlocked：機能が無効です。 • Locked：機能が有効です。
Key Management	
Key Manager	内部 Data Domain Embedded Key Manager またはオプションの RSA Data Protection Manager（DPM）Key Manager のいずれかです。キーマネージャーを切り替える（両方構成されている場合）、または Key Manager オプションを変更するには、［**Configure**］をクリックします。
サーバー	RSA Key Manager Server の名前。
サーバー ステータス	オンライン、オフライン、RSA Key Manager Server が返すエラー メッセージ。
Key Class	暗号化キーと類似の文字列をグループ化する RSA DPM（RSA Data Protection Manager）Key Manager で使用される特殊なセキュリティ クラス。Data Domain システムは、キー クラスにより RSA サーバーからキーを取得します。キー クラスは現在のキーを返すか、あるいは毎回新しいキーを生成するか、どちらかを設定できます。 注 Data Domain システムがサポートするのは現在のキーを返すキー クラスだけです。
ポート	RSA サーバーのポート番号。
FIPS mode	インポートされたホスト証明書が FIPS 準拠かどうか。デフォルト モードが有効です。
Encryption Keys	ID 番号ごとにキーをリストします。キーが作成された日時、それが有効な期間、タイプ（RSA DPM Key Manager または Data Domain 内部キー）、状態（「RSA DPM Key Manager の処理」と「Data Domain が対応する DPM 暗号化キー状態」を参照してください）、キーで暗号化されたデータの量を表示します。システムが、右の列の上にキー情報の最終更新時間を表示します。リストの選択されたキーには次の操作が可能です。

表 94 ［DD Encryption］の設定 （続き）

設定	説明
	• 同期。リストに RSA サーバーに追加された新しいキーが表示されるようにする（ただし、ファイル システムを再起動するまでは使用できません）。 • 削除。 • 破棄。

スペース使用量ビューについて（ファイル システム）

ある時点でのファイル システムのデータ使用量を視覚的に（ただし静的に）表示します。

［**Data Management**］ > ［**File System**］ > ［**Charts**］の順にクリックします。［Chart］ドロップダウン リストから［**Space Usage**］を選択します。

グラフの線上のポイントにカーソルを合わせると、そのポイントのデータが表示されます。グラフの線は次の測定値を示しています。

- Pre-comp Written：バックアップ サーバーによって MTree に送信されたデータの総量です。MTree 上の圧縮前データは、グラフの［Space Used］（左）縦軸で示すとおり、バックアップ サーバーがストレージ ユニットとしての MTree が保持する総未圧縮データ量とみなすものです。
- Post-comp Used：グラフの［Space Used］（左）縦軸で示される MTree で使用中のディスク ストレージの総量。
- ［Comp Factor］：グラフの［Compression Factor］（右）縦軸で示される Data Domain システムが受信したデータに対して実行した圧縮量（圧縮率）です。

過去のストレージ使用量のチェック
［Space Usage］グラフで、グラフの上の日付範囲（1w、1m、3m、1y、All）をクリックすると、グラフに表示されるデータの日数を 1 週間からすべての間で変更できます。

［Consumption］ビューについて

時間の経過に沿って使用されているスペースが、システムの総容量に対する比率で表示されます。

［**Data Management**］ > ［**File System**］ > ［**Charts**］の順にクリックします。［Chart］ドロップダウン リストから［**Consumption**］を選択します。

グラフの線上のポイントにカーソルを合わせると、そのポイントのデータが表示されます。グラフの線は次の測定値を示しています。

- ［Capacity］：Data Domain システム上のデータに使用可能なディスク ストレージの総量です。この量は、グラフ左側の［Space Used］という縦軸で示されます。［Capacity］チェックボックスで、この線のオン/オフを切り換えることができます。
- ［Post-comp］：Data Domain システムで使用中のディスク ストレージの総量です。グラフ左側の［Space Used］という縦軸で示されます。
- ［Comp Factor］：Data Domain システムが受信したデータに対して実行した圧縮量（圧縮率）です。グラフ右側の［Compression Factor］という縦軸で示されます。
- ［Cleaning］：ファイル システム クリーニング操作が開始されるたびに灰色のひし形がグラフに表示されます。
- ［Data Movement］：アーカイブ ライセンスが有効になっている場合に、アーカイブ ストレージ エリアに移されたディスク領域の量です。

過去の使用量のチェック
［Consumption］グラフで、グラフの上の日付範囲（1w、1m、3m、1y、All）をクリックすると、グラフに表示されるデータの日数を「1 週間」から「すべて」の間で変更できます。

［Daily Written］ビューについて（ファイル システム）

一定期間にわたるデータのフローが表示されます。データ量は、圧縮前と圧縮後について時系列に表示されます。

［**Data Management**］ > ［**File System**］ > ［**Charts**］の順にクリックします。［Chart］ドロップダウン リストから［**Daily Written**］を選択します。

グラフの線上のポイントにカーソルを合わせると、そのポイントのデータを含むボックスが表示されます。グラフの線は次の測定値を示しています。

- Pre-Comp Written：バックアップ サーバーによってファイル システムに書き込まれたデータの総量です。ファイル システム上の圧縮前データは、バックアップ ホストでは、ファイル システムが保持する非圧縮データの合計と見なされます。
- Post-Comp Written：GiB 単位で示される、圧縮実行後にファイル システムに書き込まれたデータの総量で、GiB で示されます。
- Total Comp Factor：グラフの［Total Compression Factor］（右）縦軸で示される Data Domain システムが受信したデータに対して実行した総圧縮量（圧縮率）です。

過去の書き込まれたデータのチェック
［Daily Written］グラフで、グラフの上の日付範囲（1w、1m、3m、1y、All）をクリックすると、グラフに表示されるデータの日数を 1 週間からすべての間で変更できます。

ファイル システムがフルまたはフルに近い場合

Data Domain システムには、フルになるまで 3 つの進行レベルがあります。各レベルに達すると、禁止される操作が段階的に増えていきます。各レベルで、データを削除し、ファイル システム クリーニング操作を実行すると、ディスク領域が使用可能になります。

注

ファイルとスナップショットを削除するプロセスでは、ディスク領域はすぐに再利用されませんが、次のクリーニング操作でその領域が再利用されます。

- レベル 1：使用率の最初のレベルで、ファイル システムにそれ以上新しいデータを書き込みできません。参考容量不足アラートが生成されます。
  Remedy：不必要なデータセットを削除して、保存期間を短縮し、スナップショットを削除し、ファイル システム クリーニング操作を実行します。
- レベル 2：容量不足の第 2 レベルで、ファイルを削除できません。これは、ファイルの削除にも空きスペースが必要ですが、システムの空きスペースが少なすぎてファイルの削除も行えないためです。
  Remedy：スナップショットを期限切れにし、ファイル システム クリーニング操作を実行します。
- レベル 3：使用率の第 3 および最終レベルで、スナップショットを期限切れにするか、ファイルを削除するか、新しいデータの書き込みを失敗させます。
  Remedy：少なくとも一部のファイルを削除するか、一部のスナップショットを期限切れにし、クリーニングを再開するために必要なスペースを空けるため、ファイル システム クリーニング操作を実行します。

メール アラートを使用したスペース使用量の監視

ファイル システムが 90%、95%、100%使用されている場合、アラートは生成されます。これらのアラートを送信するには、ユーザーをアラート メーリング リストに追加します。

注

アラート メール リストに参加するには、「アラートのクリアと表示」を参照してください。

ファイル システム操作の管理

このセクションでは、ファイル システム クリーニング、浄化、基本操作の実行について説明します。

基本操作の実行

基本ファイル システム操作には、ファイル システムの有効化と無効化、ファイル システムの破棄（使用するのは稀）が含まれます。

ファイル システムの作成

［Data Management］>［File System］ページで、［Summary］タブを使用してファイル システムを作成します。

ファイル システムの作成する理由は、次の 3 つです。

- Data Domain システムの新規作成。
- クリーン インストール後のシステムの起動。
- ファイル システムの破棄。

ファイル システムを作成する手順：

手順

1. ストレージが設置され、構成されていることを確認します（詳細については、システム ストレージ情報の表示に関するセクションを参照してください）。ファイル システムがこの前提条件を満たしていない場合、警告メッセージが表示されます。ファイル システムを作成する前に、ストレージをインストールおよび構成します。
2. ［**Data Management**］>［**File System**］>［**Summary**］>［**Create**］を選択します。

   ファイル システムの作成ウィザードが起動します。表示される指示に従います。

ファイル システムの有効化または無効化

ファイル システムを有効化または無効化するオプションは、ファイル システムの現在の状態によって異なります。有効になっている場合は無効化でき、無効化している場合は有効化できます。

- ファイル システムを有効化すると、Data Domain システム操作が開始できます。この機能を使用できるのは管理ユーザーのみです。
- ファイル システムを無効化すると、クリーニングを含むすべての Data Domain システム操作が停止します。この機能を使用できるのは管理ユーザーのみです。

⚠ 注意

バックアップ アプリケーションがデータをシステムに送信しているときにファイル システムを無効化すると、バックアップ プロセスが失敗する可能性があります。バックアップ ソフトウェア アプリケーションの一部は、ファイルのコピーを再開できる場合、中止した場所から再開することでリカバリを実行できますが、それ以外のものは障害となり、バックアップが不完全になります。

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］を選択します。
2. ［**File System**］で、［**Enable**］または［**Disable**］をクリックします。
3. 確認ダイアログで［**Close**］をクリックします。

ファイル システムの拡張

「When the File System Is Full or Nearly Full」というメッセージで示される提案が通常の運用に十分なスペースをクリアしなかった場合、ファイル システムのサイズを拡張する必要があります。

ただし、次の理由により、ファイル システムは拡張不可能な場合があります。

- ファイル システムは有効になっていません。
- アクティブ、保存、クラウドの各階層には、未使用のディスクまたはエンクロージャがない。
- 拡張されたストレージ ライセンスはインストールされていない。
- 十分な容量ライセンスがインストールされていない。

DD6300 システムでは、使用可能なライセンス容量が正確に 21.8 TiB の場合、ES30 エンクロージャの 4 TB ドライブ（43.6 TiB）をアクティブ階層において使用率 50%（21.8 TiB）で使用するオプションをサポートします。部分容量シェルフを使用する場合は、次のガイドラインが適用されます。

- 部分容量を使用するための他のエンクロージャ タイプまたはドライブ サイズはサポートされません。
- 部分容量シェルフは、アクティブ階層にのみ存在できます。
- 部分容量 ES30 は、アクティブ階層に 1 台のみ存在できます。
- 部分容量シェルフが階層に存在する場合、そのシェルフが全容量で追加されるまで別の ES30 を構成することはできません。

  注

  その場合、部分容量シェルフの残りの 21.8 TiB を使用するには、十分な追加容量のライセンスが必要です。

- 使用可能な容量が 21.8 TB を超えている場合は、部分容量シェルフを追加することはできません。
- 21 TiB ライセンスを削除しても、全容量シェルフは部分容量シェルフに自動的に変換されません。いったんシェルフを取り外してから部分容量シェルフとして追加する必要があります。

ファイル システムを拡張する手順：

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Expand Capacity**］を選択します。

   ［Expand File System Capacity］ウィザードが起動します。［**Storage Tier**］ドロップダウン リストには、アクティブ階層が必ず含まれ、長期保存階層またはクラウド階層のいずれか

が 2 番目の選択肢として含まれる場合があります。ウィザードには、階層ごとのファイル システムの現在の容量と、使用可能な拡張用の追加ストレージ容量が表示されます。

注

ファイル システムの容量は、物理ディスクがシステムにインストールされていて、ファイル システムが有効な場合にのみ拡張できます。

2. ［**Storage Tier**］ドロップダウン リストから、階層を選択します。
3. ［**Addable Storage**］領域では、使用するストレージ デバイスを選択して［**Add to Tier**］をクリックします。
4. ウィザードの指示に従ってください。確認ページが表示されたら、［**Close**］をクリックします。

ファイル システムの破棄

ファイル システムの破棄は、カスタマー サポートの指示の下でのみ行ってください。このアクションは、仮想テープを含め、ファイル システム内のすべてのデータを削除します。削除されたデータは、リカバリ不可能です。この操作は、Replication 構成設定も削除します。

システムが操作から削除されているため、この操作は、既存のデータのクリーンアップ、新しいコレクション レプリケーション デスティネーションの作成、またはコレクション ソースが必要な場合、またはセキュリティ上の理由で使用されます。

⚠ 注意

オプションの［Write zeros to disk］操作は、効果的にすべてのデータのトレースを削除して、すべてのファイル システム ディスクに 0 を書き込みます。Data Domain システムに大量のデータが含まれる場合、この操作は完了までに何時間も（あるいは何日も）かかる可能性があります。

注

これは破壊的な手順ですので、この操作は管理ユーザーのみ使用できます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Summary**］ > ［**Destroy**］を選択します。
2. ［Destroy File System］ダイアログ ボックスでは、sysadmin のパスワードを入力します（それが唯一の許可されたパスワードです）。
3. オプションで、［**Write zeros to disk**］のチェックボックスをクリックして、データを完全に削除します。
4. ［**OK**］をクリックします。

クリーニングの実行

このセクションでは、クリーニングに関する情報を提供し、クリーニング スケジュールを開始、停止、変更する方法について説明します。

DD OS は、アクティブ階層用に「Cleanable GiB」というカウンターを維持しようとします。この数は、クリーニング/ガベージ コレクションを実行することによって、アクティブ階層でどのくらいの物理（postcomp）スペースが再利用される可能性があるかを推定したものです。このカウンターは、`filesys show space` と `df` のコマンドを使用して表示されます。

```
Active Tier:
Resource Size GiB Used GiB Avail GiB Use% Cleanable GiB*
```

```
---------------- -------- --------- --------- ----
--------------
/data: pre-comp - 7259347.5 - - -
/data: post-comp 304690.8 251252.4 53438.5 82% 51616.1 <=== NOTE
/ddvar 29.5 12.5 15.6 44% -
---------------- -------- --------- --------- ----
--------------
```

次のいずれかの場合、アクティブ階層のクリーニングを実行します。

- 「Cleanable GiB」の値が大きい
- DDFS が 100%フルになっている（したがって読み取り専用）

クリーニングの 1 回の実行ですべての潜在的なスペースを必ず再利用できるわけではありません。非常に大規模なデータセットが含まれている Data Domain システムでは、クリーニングは、不要なデータを最も含むファイル システムの部分に対して動作し、すべての潜在的なスペースが再利用されるまで複数回実行する必要があることがあります。

クリーニングの開始

クリーニング操作をすぐに開始するには、次の手順に従ってください。

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Settings**］ > ［**Cleaning**］を選択します。

   ［**File System Setting**］ダイアログ ボックスの［**Cleaning**］タブには、各階層の構成可能な設定が表示されます。

2. アクティブ階層の場合：
   a. ［Throttle %］テキスト ボックスに、システム スロットルの量を入力します。これは、クリーニング専用の CPU 使用率です。デフォルトは 50%。
   b. ［Frequency］ドロップダウン リストで、頻度として ［Never］、［Daily］、［Weekly］、［Biweekly］、［Monthly］のいずれかを選択します。デフォルトは［Weekly］です。
   c. ［At］で、時刻を設定します。
   d. ［On］で、曜日を選択します。
3. クラウド階層の場合：
   a. ［Throttle %］テキスト ボックスに、システム スロットルの量を入力します。これは、クリーニング専用の CPU 使用率です。デフォルトは 50%。
   b. ［Frequency］ドロップダウン リストで、頻度として［Never］、［After every 'N' Active Tier cleans］のいずれかを選択します。

   注

   クラウド階層のクリーニングを実行するときにクラウド ユニットにアクセスできない場合、そのクラウド ユニットはその実行ではスキップされます。クラウド ユニットが使用可能になった場合、そのクラウド ユニットのクリーニングは次回の実行で行われます。クリーニングスケジュールでは、2 つの実行間の期間を決定します。クラウド ユニットが使用可能になり、スケジュール設定された次回の実行まで待つことができない場合は、クリーニングを手動で開始できます。

4. ［**Save**（保存）］をクリックします。

注

CLI を使用してクリーニング操作を開始するには、`filesys clean start` コマンドを使用します。

```
# filesys clean start
Cleaning started. Use 'filesys clean watch' to monitor progress.
```

クリーニングが進行中であることを確認するには、`filesys status` コマンドを使用します。

```
# filesys status
The filesystem is enabled and running.
Cleaning started at 2017/05/19 18:05:58: phase 1 of 12 (pre-merge)
50.6% complete, 64942 GiB free; time: phase 0:01:05, total 0:01:05
```

既にクリーニングが実行されている場合は、起動を試みたときに次のメッセージが表示されます。

```
**** Cleaning already in progress. Use 'filesys clean watch' to monitor
progress.
```

注

クリーニングを開始できない場合は、ご契約のサポート プロバイダに問い合わせてください。この問題は、システムで `missing segment error` が発生し、クリーニングが無効になっていることを示している可能性があります。

クリーニングのスケジュール設定または停止

クリーニング操作をすぐに停止またはスケジュール設定するには、次の手順を実行します。

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Settings**］ > ［**Cleaning**］を選択します。

   File System Setting ダイアログ ボックスの Cleaning タブには、各階層の構成可能な設定が表示されます。

2. アクティブ階層の場合：

   a. ［Frequency］ドロップダウン リストで、必要な頻度を選択します。

3. クラウド階層の場合：

   a. ［Frequency］ドロップダウン リストで、必要な頻度を選択します。

4. ［**Save**（保存）］をクリックします。

注

CLI を使用して、クリーニングのスケジュールが設定されていることを確認できます。

```
# filesys clean show schedule
```

必要に応じて、アクティブ階層のクリーニング スケジュールを設定します。次の例では、毎週火曜日の午前 6 時にクリーニングを実行するように設定します。

```
# filesys clean set schedule Tue 0600
Filesystem cleaning is scheduled to run "Tue" at "0600".
```

ER（Extended Retention）を使用して構成されたシステムでは、データ移動の完了後にクリーニングを実行するように構成でき、独自のスケジュールを設定することはできません。

浄化の実行

政府のガイドラインを順守するには、分類されたデータまたは機密データがそのデータの保存を承認されていないシステムに書き込まれたときに、システム浄化（データ シュレッダとも呼ばれる）を実行する必要があります。

事故が発生すると、システム管理者は事故で書き込まれたデータを完全に消去する措置をすぐに実行する必要があります。目標は、ストレージ デバイスをそのイベントが発生しなかったかのような状態に効果的にリストアすることです。データ漏洩に機密データが含まれている場合、Data Domain Professional Services' Secure Data 消去手順を使用して、ストレージ全体を浄化する必要があります。

バックアップ セットか個別のファイルかにかかわらず、管理者が論理レベルでファイルを削除できるようにする Data Domain 浄化コマンドが存在します。ほとんどのファイル システムで、ファイルの削除に含まれるステップは、ファイルへのフラグ付けまたはディスク上のデータへの参照の削除、後で使用される物理スペースの解放のみです。ただし、この単純なアクションには、基礎となるデータの残留分をディスク上に物理的に残してしまうという問題があります。重複排除されたストレージ環境には、この問題に対する耐性がありません。

システムでデータ シュレッダを行うと、そのデータの残留分が消去されるため、シュレッダ実行後にファイルがアクセス可能になる可能性がなくなります。Data Domain の浄化アプローチでは、次の仕様の DoD（Department of Defense）5220.22 の 2007 年度版に準拠していることを確認します。

- 「US Department of Defense 5220.22-M Clearing and Sanitization Matrix」
- 「National Institute of Systems and Technology (NIST) Special Publication 800-88 Guidelines for Media Sanitization」

重複排除されたデータの浄化

Data Domain システムが、既存のデータをそのネイティブの重複排除されていない状態で浄化します。

重複排除ストレージ システムは、システムに送信されたファイルから共通データ パターンを抽出し、冗長なインスタンスをすべて参照して、これらのパターンに固有のコピーのみ保存します。これらのデータ パターンまたはセグメントがシステム内の多くのファイル間で共有されている可能性があるため、浄化処理ではまず、汚染されたファイルの各セグメントがクリーンなファイルを共有されているかどうかを判断し、汚染されたメタデータとともに、共有されていないセグメントのみ削除する必要があります。

削除されたファイルにのみ属するすべてのセグメントのすべてのコピーが削除されるよう、すべてのストレージ階層、キャッシュ、未使用の容量、空き領域がクリアされます。システムは、そのシステムに汚染されたファイルが存在しなかった場合の状態にストレージ デバイスを効果的にリストアするため、それらのセグメントが使用しているストレージをすべて再利用および上書きします。

浄化レベル 1：データ クリアまたはシュレッダ

削除する必要があるデータが未分類である場合、「US Department of Defense 5220.22-M Clearing and Sanitization Matrix」に示すとおり、レベル 1 浄化を使用して、影響を受けたストレージを上書きできます。これは、ほとんどのデータ シュレッダとシステム浄化のケースにおいて対応の基礎となります。

Data Domain システム浄化機能を使用すると、消去されたファイルにのみ属するすべてのセグメントのコピーがすべて、単一パス ゼロ化メカニズムを使用して上書きされます。浄化中のシステムのクリーンなデータは、オンラインとなり、ユーザーが使用できる状態になります。

手順

1. バックアップ ソフトウェアまたは対応するクライアントを通して、汚染されたファイルまたはバックアップを削除します。バックアップの場合、必ず適切にバックアップ ソフトウェアを管理して、そ

のイメージの関連ファイルが調整されている状態、必要に応じてカタログ レコードが管理されている状態などを保ちます。

2. 汚染された Data Domain システムで `system sanitize start` コマンドを実行すると、その中の以前に使用したスペースがすべて一度上書きされます（下図参照）。
3. 影響を受けたシステムが浄化されるまで待ちます。浄化は、`system sanitize watch` コマンドを使用して監視できます。

   影響を受けた Data Domain システムがレプリケーションを有効にしている場合、レプリカを含むすべてのシステムを同様に処理する必要があります。システムに存在するデータの量とその分散によって、`system sanitize` コマンドは時間がかかる場合があります。ただし、その間も、ユーザーはシステム内のクリーンなデータはすべて使用できます。

浄化レベル 2：フル システム浄化

削除する必要があるデータが分類済みである場合、「US Department of Defense 5220.22-M Clearing and Sanitization Matrix」に示すとおり、レベル 2 浄化（またはフル システム浄化）が必要です。

Data Domain は、Blancco には上書きパターンと証明書を使用したマルチ パス上書きを推奨します。これは、完全なシステム浄化が必要な総合国防総省要件への対応の基礎となります。詳細については、次のサイトを参照してください。

https://www.emc.com/auth/rcoll/servicekitdocument/cp_datadomaindataerase_psbasddde.pdf

基本設定の変更

このセクションの説明に従って、使用する圧縮のタイプ、マーカー タイプ、Replica 書き込みステータス、ステージング予約割合を変更します。

ローカル圧縮の変更

ローカル圧縮タイプを構成するには、［File System Settings］ダイアログ ボックスの［General］タブを使用します。

注

必要ない限り、ローカル圧縮のタイプは変更しないでください。

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Settings**］ > ［**General**］を選択します。
2. ［Local Compression Type］ドロップダウンリストで、新しい圧縮タイプを選択します。

表 95 圧縮タイプ

オプション	説明
NONE[NONE]	データを圧縮しません。
LZ	最高のスループットを実現するデフォルトのアルゴリズム。Data Domain の推奨オプション

表 95 圧縮タイプ （続き）

オプション	説明
GZFAST	圧縮データの使用領域を縮小できる zip 形式の圧縮。ただし、CPU サイクルは増大（lz の 2 倍）。パフォーマンスよりも容量の圧縮を優先するサイトでの代替方式として推奨されるオプション
GZ	データ ストレージの使用領域が最も少ない（平均で lz よりも 10～20%少ないが、一部のデータセットでは圧縮率が高くなる）zip 形式の圧縮。CPU サイクルの使用は最大（最大で lz の 5 倍）。一般的に、パフォーマンス要件が低いニアライン ストレージ アプリケーションで使用される

3. ［**Save**］をクリックします。

読み取り専用設定の変更

レプリカを書き込み可能に変更します。一部のバックアップ アプリケーションは、レプリカからリストアまたはヴォールト操作を行うためにレプリカを書き込み可能とみなす必要があります。

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Settings**］ > ［**General**］を選択します。
2. ［Report Replica as Writable］領域で、必要に応じて［**Disabled**］と［**Enabled**］を切り替えます。
3. ［**Save**］をクリックします。

ディスク ステージングの処理

ディスク ステージングによって、Data Domain システムは、CIFS 共有または NFS マウント ポイントを介して基本ディスクとみなされた場合、ステージング デバイスとして機能できます。

ディスク ステージングは NetWorker や Symantec の NBU（NetBackup）などのバックアップ ソフトウェアとともに使用できます。ライセンスは不要で、デフォルトでは無効になっています。

注

Data Domain システムが Disk Staging デバイスとして使用される場合、DD VTL 機能は必要なく、対応していません。

一部のバックアップ アプリケーションがディスク ステージング デバイスを使用する理由は、テープ ドライブが継続的にストリームできることです。データがテープにコピーされた後、それはスペースが許す限りディスクに保存されます。最近のバックアップからのリストアが必要な場合、高い確率でデータはまだディスクにあり、テープからよりもドライブからリストアする方が楽です。ディスクの空きスペースがなくなったら、古いバックアップを削除してスペースを確保できます。このオン デマンド削除ポリシーによって、ディスクを最大限活用できます。

通常の運用では、Data Domain システムはクリーニング操作が実行されるまで、削除されたファイルからスペースを再利用しません。これは、ファイル削除時にスペースが再利用されることを想定しているステージング モードで動作するバックアップ ソフトウェアには対応していません。ディスク ステージングを構成するときは、システムがスペースの即時解放をシミュレートできるよう、総スペースの一部（通常 20～30%）を確保します。

使用可能なスペースの量は、ステージング リザーブの分だけ減ります。保存されたデータの量によって使用可能なスペースがなくなった場合、システムがフルになります。ただし、ファイルが削除されると、クリーニングによって回復するスペース量をシステムが推定し、その量の分だけ使用可能なスペースを増やすためステージング リザーブから借ります。クリーニング操作が実行されると、スペースが実

際に回復し、リザーブが初期サイズに戻ります。ファイルを削除して使用可能になったスペースの量は推定に過ぎないため、クリーニングによって再利用される実際のスペースは推定と一致しない可能性があります。ディスク ステージングの目的は、クリーニングの実行がスケジュールされる前にスペースがなくならないように十分なリザーブを構成することです。

ディスク ステージングの構成

ディスク ステージングを有効化し、ステージング予約割合を指定します。

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Settings**］ > ［**General**］を選択します。
2. ［Staging Reserve］領域で、必要に応じて［**Disabled**］と［**Enabled**］を切り替えます。
3. ［Staging Reserve］を有効化した場合は、［% of Total Space］ボックスに値を入力します。

   この値は、ディスク ステージングのために予約される総ディスク領域の割合（通常、20～30%）を表します。
4. ［**Save**］をクリックします。

テープ マーカー設定

一部のベンダーのバックアップ ソフトウェアは、Data Domain システムに送信されたすべてのデータ ストリーム（ファイル システムと DD VTL バックアップ）でマーカー（テープ マーカー、タグ ヘッダー、またはその他の名前が使用されます）を挿入します。

マーカーは、Data Domain システムのデータ圧縮のパフォーマンスを大幅に下げます。そのため、デフォルト マーカー タイプは auto に設定され、ユーザーは変更できません。この設定がお使いのバックアップ ソフトウェアに対応していない場合、ご契約のサポート プロバイダーにお問い合わせください。

注

Data Domain 環境におけるアプリケーションの動作の詳細については、「EMC Data Domain システムをストレージ環境に統合する方法」を参照してください。ベンダー関連問題のトラブルシューティングには、これらのマトリックスと統合ガイドを使用できます。

SSD ランダム ワークロード共有

Data Domain システムでのランダム I/O を制限するための閾値を、要件と I/O パターンの変化に合わせてデフォルト値から調整することができます、

デフォルトでは、SSD ランダム ワークロード共有は Data Domain システムによって 40%に設定されています。この値は、必要に応じて上下に調整できます。［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Settings**］ > ［**Workload Balance**］を選択し、スライダーを調節します。

［**Save**］をクリックします。

Fast Copy 操作

fastcopy 操作は、ファイルとソース ディレクトリのディレクトリ ツリーを、Data Domain システムのターゲット ディレクトリにコピーします。

`force` オプションを使用すると、デスティネーション ディレクトリが存在する場合に、そのディレクトリに上書きできます。**fastcopy** 操作を実行すると、進行状況ステータスのダイアログ ボックスが表示されます。

注

Fast Copy 操作ではデスティネーションがソースと同じになりますが、特定の時間では同じになりません。この操作中にどちらかのフォルダーを変更した場合、2 つが同じである、または過去に同じであったことは保証されません。

Fast Copy 操作の実行

Data Domain システムのソース ディレクトリから Data Domain システム上の他の場所にファイルまたはディレクトリ ツリーをコピーします。

手順

1. ［**Data Managment**］ > ［**File System**］ > ［**Summary**］ > ［**Fast Copy**］を選択します。

   ［Fast Copy］ダイアログ ボックスが表示されます。

2. Source テキスト ボックスに、コピーされるデータがあるディレクトリのパス名を入力します。たとえば、`/data/col1/backup/.snapshot/`**snapshot-name**`/dir1` と入力します。

   注

   col1 は、小文字の l で始まり後ろに数字の 1 が付きます。

3. ［Destination］テキスト ボックスに、データがコピーされるディレクトリのパス名を入力します。たとえば、`/data/col1/backup/dir2` です。宛先ディレクトリが空でない場合、操作は失敗します。

   - ［Destination］ディレクトリがある場合、［**Overwrite existing destination if it exists**］チェックボックスをクリックします。

4. ［**OK**］をクリックします。
5. 表示される進行状況ダイアログ ボックスで、［**Close**］をクリックして終了します。

第 6 章

MTree

本章には、次のセクションが含まれます。

- MTree の概要 220
- MTree 使用状況のモニタリング 227
- MTree 操作の管理 231

MTree の概要

MTree は、ファイル システムの論理パーティションです。

MTree は、DD Boost ストレージ ユニット、DD VTL プール、NFS/CIFS 共有のいずれかの方法で使用できます。MTree は、スナップショット、クォータ、DD Retention Lock の細分性管理を可能にします。DD Extended Retention と Active Tier から Retention Tier へのデータ移行ポリシーの細分性管理を行うシステムの場合、MTree 操作はファイル システム全体ではなく、特定の MTree で実行できます。

注

MTree レプリケーション コンテキストには、構成可能な最大数まで MTree を指定できます。

MTree の最上位ディレクトリにはユーザー ファイルを配置しないでください。

MTree の制限

Data Domain システムの MTree 制限

表 96 サポートされている Mtree

Data Domain システム	DD OS バージョン	サポートされている構成可能 MTree	サポートされている同時アクティブ MTree
DD9800	6.0 以降	256	256
DD9500	5.7 以降	256	256
DD6800、DD9300	6.0 以降	128	128
DD6300	6.0 以降	100	32
DD990、DD4200、DD4500、DD7200	5.7 以降	128	128
その他のすべての DD システム	5.7 以降	100	モデルに応じて最大 32
DD9500	5.5.6	100	64
DD990、DD890	5.3 以降	100	モデルに応じて最大 32
DD7200、DD4500、DD4200	5.4 以降	100	モデルに応じて最大 32
その他のすべての DD システム	5.2 以降	100	モデルに応じて最大 14

クォータ

MTree クォータは、MTree に書き込まれた論理データにのみ割り当てられます。

管理者は、MTree、ストレージ ユニット、DD VTL プールのストレージ領域制限を設定し、余分な領域が消費されるのを防ぐことができます。クォータ制限には、ハード制限とソフト制限の 2 種類があります。ソフト制限かハード制限、またはソフト制限とハード制限の両方を設定できます。値は両方整数である必要があり、ソフト値はハード値よりも小さい必要があります。

ソフト制限が設定されている場合、MTree サイズが制限を超えるとアラートが送信されますが、データの書き込みは可能です。ハード制限が設定されている場合、ハード制限に達するとデータを MTree に書き込めません。そのため、データが MTree から削除されるまで、すべての書き込み操作が失敗します。

詳細については、MTree クォータの構成（232 ページ）を参照してください。

クォータ適用

クォータ適用を有効化または無効化します。

［MTree］パネルについて

システム上のアクティブな MTree がすべて表示され、リアルタイム データ ストレージ統計が表示されます。概要領域の情報は、スペース使用率トレンドを視覚化する場合に役立ちます。

［**Data Management**］ > ［**MTree**］を選択します。

- リスト内の MTree のチェックボックスを選択して、詳細を表示し、［Summary］ビューで構成を行います。
- ［Filter By MTree Name］フィールドにテキスト（ワイルドカード対応）を入力し、［**Update**］をクリックしてリスト内の特定の MTree 名を一覧表示します。
- フィルター テキストを削除し、［**Reset**］をクリックしてデフォルト リストに戻ります。

表 97 MTree 概要情報

項目	説明
MTree Name	MTree のパス名。
Quota Hard Limit	使用されたソフト制限の割合。
Last 24 Hr Pre-Comp (pre-compression)	過去 24 時間に書き込まれたバックアップ アプリケーションから取得した未フォーマットのデータの量。
Last 24 Hr Post-Comp (post-compression)	過去 24 時間の圧縮後に使用されたストレージの量。
Last 24 hr Comp Ratio	過去 24 時間の圧縮率。
Weekly Avg Post-Comp	過去 5 週間に使用された圧縮ストレージの平均量。
Last Week Post-Comp	過去 7 日間に使用された圧縮ストレージの平均量。
Weekly Avg Comp Ratio	過去 5 週間の平均圧縮率。
Last Week Comp Ratio	過去 7 日間の平均圧縮率。

［Summary］ビューについて

重要なファイル システム統計が表示されます。

詳細情報の表示

情報を表示する MTree を選択します。

表 98 選択された MTree の MTree 詳細情報

項目	説明
Full Path	MTree のパス名。
Pre-Comp Used	MTree に書き込まれたバックアップ アプリケーションから取得した未フォーマットのデータの現在の量。
Status	MTree のステータス（組み合わせに対応）。ステータスの種類： • D：削除済み • RO：読み取り専用 • RW：R/W • RD：Replication destination • RLCE：DD Retention Lock Compliance 有効 • RLCD：DD Retention Lock Compliance 無効 • RLGE：DD Retention Lock Governance 有効 • RLGD：DD Retention Lock Governance 無効
Quota	
Quota Enforcement	有効または無効。
Pre-Comp Soft Limit	現在の値。［Configure］をクリックしてクォータ制限を修正します。
Pre-Comp Hard Limit	現在の値。［Configure］をクリックしてクォータ制限を修正します。
Quota Summary	使用されたハード制限の割合。
プロトコル	
CIFS Shared	CIFS 共有のステータス：ステータスの種類： • Yes：MTree またはその親ディレクトリが共有されています。 • Partial：この MTree に属するサブディレクトリが共有されています。 • No：この MTree とその親またはサブディレクトリが共有されていません。 CIFS リンクをクリックして、CIFS ビューを表示します。
NFS Exported	NFS エクスポート ステータス。ステータスの種類： • Yes：MTree またはその親ディレクトリがエクスポートされています。 • Partial : この MTree に属するサブディレクトリがエクスポートされています。 • No：この MTree とその親またはサブディレクトリがエクスポートされていません。 NFS リンクをクリックして、NFS ビューを表示します。
DD Boost Storage Unit	DD Boost エクスポート ステータス。ステータスの種類： • Yes：MTree がエクスポートされています。 • Yes：MTree がエクスポートされていません。 • Unknown：情報がありません。

表 98 選択された MTree の MTree 詳細情報 （続き）

項目	説明
	DD Boost リンクをクリックして、DD Boost ビューを表示します。
DD VTL プール	VTL プール レポートのステータス。ステータスの種類： • Yes：MTree は、DD VTL MTree プールです。 • No：MTree は、DD VTL MTree プールではありません。 • Unknown：情報がありません。
vDisk Pool	vDisk レポートのステータス。ステータスの種類： • Unknown：vDisk サービスが有効ではありません。 • No：vDisk サービスは有効になっているが、MTree は vDisk プールではありません。 • Yes : vDisk サービスは有効になっていて、MTree は vDisk プールです。
Physical Capacity Measurements	
Used (Post-Comp)	圧縮データが取得された後に使用される MTree スペース。
Compression	Global Comp-factor。
Last Measurement Time	前回システムが MTree を測定した時間。

スケジュール	割り当てられているスケジュールの数。
	［**Assign**］をクリックすると、スケジュールが表示され、MTree に割り当てられます。
	• Name：スケジューラの名前。
	• Status：［Enabled］または［Disabled］
	• Priority：
	  ▪ Normal：測定タスクを処理キューに送信します。
	  ▪ Urgent：測定タスクを処理キューの最初に送信します。
	• Schedule：タスクの実行にかかる時間。
	• MTree Assignments：スケジュールが割り当てられた MTree の数。

Submitted Measurements	MTree の圧縮後のステータスを表示します。 ［**Measure Now**］をクリックして、MTree の手動の圧縮後ジョブを送信し、そのジョブの優先度を選択します。 • 0：測定ジョブを送信しません。 • 1：1 件の測定ジョブが実行中です。 • 2：2 件の測定ジョブが実行中です。
スナップショット	これらの統計を表示します。 • スナップショットの総数

表 98 選択された MTree の MTree 詳細情報 （続き）

項目	説明
	• 期限切れ • Unexpired • 最も古いスナップショット • Newest Snapshot • Next Scheduled • Assigned Snapshot Schedules ［**Total Snapshots**］をクリックすると、［**Data Management**］ > ［**Snapshots**］ビューに移動します。 ［**Assign Schedules**］をクリックして、スナップショットのスケジュールを設定します。

MTree レプリケーション情報の表示

MTree レプリケーション構成を表示します。

選択された MTree がレプリケーションのために構成された場合、構成についてのサマリー情報がこの領域に表示されます。それ以外の場合、この領域に「`No Record Found`」が表示されます。

- 構成を実行するか、詳細を確認するには、［Replication］リンクをクリックして、［Replication］ページに移動します。

表 99 MTree レプリケーション情報

項目	説明
ソース	ソース MTree パス名。
ターゲット	デスティネーション MTree パス名。
Status	MTree レプリケーション ペアのステータス。ステータスは Normal、Error、または Warning となります。
Sync As Of	レプリケーション ペアが同期された最後の日時。

MTree スナップショット情報の表示

選択された MTree がスナップショットに構成された場合、スナップショット構成についてのサマリー情報が表示されます。

- 構成を実行するか、詳細を確認するには、［**Snapshots**］リンクをクリックして、［Snapshots］ページに移動します。
- ［**Assign Schedules**］をクリックして、スナップショット スケジュールを選択された MTree に割り当てます。スケジュールのチェックボックスを選択し、［**OK**］と［**Close**］をクリックします。スナップショット スケジュールを作成するには、［**Create Snapshot Schedule**］をクリックします（手順については、スナップショット スケジュールの作成に関するセクションを参照してください）。

表 100 MTree スナップショット情報

項目	説明
スナップショットの総数	この MTree に作成されたスナップショットの総数。各 MTree に、計 750 個のスナップショットを作成できます。
期限切れ	作成対象としてマークされたが、まだクリーニング操作で削除されていない、この MTree 内のスナップショットの数。
Unexpired	保持対象としてマークされている、この MTree 内のスナップショットの数。
最も古いスナップショット	この MTree の最も古いスナップショットの日付。
Newest Snapshot	この MTree の最も新しいスナップショットの日付。
Next Scheduled	次にスケジュール設定されたスナップショットの日付。
Assigned Snapshot Schedules	この MTree に割り当てられたスナップショット スケジュールの名前。

MTree Retention Lock 情報の表示

選択された MTree が DD Retention Lock ソフトウェア オプションのいずれかに構成された場合、DD Retention Lock 構成についてのサマリー情報が表示されます。

注

MTree の DD Retention Lock 管理方法については、DD Retention Lock の扱いに関するセクションを参照してください。

表 101 DD Retention Lock 情報

項目	説明
Status	DD Retention Lock が有効か無効かを示します。
Mode	MTree が DD Retention Lock Compliance または DD Retention Lock Governance 用に構成されているかどうかを示します。
Use	MTree の使用を示します。
Retention period min	最短の DD Retention Lock 期間を示します。
Retention period max	最長の DD Retention Lock 期間を示します。

DD Retention Lock 設定の有効化と管理

GUI の［DD Retention Lock］領域を使用して、保存ロック期間を変更します。

手順

1. ［**Data Management**］ > ［**MTree**］ > ［**Summary**］を選択します。
2. Retention Lock 領域で、［**Edit**］をクリックします。
3. ［Modify Retention Lock］ダイアログ ボックスで、［**Enable**］を選択して、Data Domain システムで DD Retention Lock を有効化します。
4. ［Retention Period］パネルで、最短または最長保存期間を変更します（まず機能を有効化する必要があります）。

5. 間隔（分、時間、日、年）を選択します。［**Default**］をクリックして、デフォルト値を表示します。
6. ［**OK**］をクリックします。

結果

［Modify Retention Lock］ダイアログ ボックスを閉じた後、更新された MTree 情報が［DD Retention Lock］サマリー領域に表示されます。

［Space Usage］ビューについて（MTree）

特定の時点における MTree のデータ使用量を視覚的に表示します。

［**Data Management**］ > ［**MTree**］ > ［**Space Usage**］を選択します。

- グラフの線上のポイントにカーソルを合わせると、そのポイントのデータを含むボックスが表示されます。
- 標準の［**Print**］ダイアログ ボックスを開くには、グラフの下部にある［Print］をクリックします。
- 新しいブラウザ ウィンドウでグラフを表示するには、［**Show in new window**］をクリックします。

グラフの線は次の測定値を示しています。

- Pre-comp Written：バックアップ サーバーによって MTree に送信されたデータの総量です。MTree 上の圧縮前データは、グラフの［Space Used］（左）縦軸で示すとおり、バックアップ サーバーがストレージ ユニットとしての MTree が保持する総未圧縮データ量とみなすものです。
- Post-comp Used：グラフの［Space Used］（左）縦軸で示される MTree で使用中のディスク ストレージ領域の圧縮後の総量。
- Comp Factor：MTree に格納されているデータの圧縮率を、グラフの［Comp Factor］（右）縦軸で示します。

注

［MTrees Space Usage］ビューの場合、システムは未圧縮の情報のみ表示します。データは MTree 間で共有できるため、1 つの MTree 用の圧縮使用率を表示されます。

過去のストレージ使用量のチェック

［Space Usage］グラフで、グラフの上の［Duration］線上の間隔（1w、1m、3m、または 1y）をクリックすると、グラフに表示されるデータの日数（7～120 日）を変更できます。

120 日を超える間隔のスペース使用量を確認するには、次のコマンドを発行します。

```
# filesys show compression [summary | daily | daily-detailed] {[last n {hours | days | weeks | months}] | [start date [end date]]}
```

［Daily Written］ビューについて（MTree）

過去 24 時間のデータ フローが表示されます。データ量は、圧縮前と圧縮後について時系列に表示されます。

また、グローバル圧縮とローカル圧縮の量、圧縮前と圧縮後の量の合計も提供されます。

- グラフの線上のポイントにカーソルを合わせると、そのポイントのデータを含むボックスが表示されます。
- 標準の［**Print**］ダイアログ ボックスを開くには、グラフの下部にある［Print］をクリックします。
- 新しいブラウザー ウィンドウでグラフを表示するには、［**Show in new window**］をクリックします。

グラフの線は次の測定値を示しています。

- Pre-Comp Written：バックアップ サーバーによって MTree に書き込まれたデータの総量です。MTree 上の圧縮前のデータは、バックアップホストでは、ストレージユニットとしての MTree が保持する非圧縮データと見なされます。
- Post-Comp Written：GiB 単位で示される、圧縮実行後に MTree に書き込まれたデータの総量で、GiB で示されます。
- Total Comp Factor：グラフの［Total Compression Factor］（右）縦軸で示される Data Domain システムが受信したデータに対して実行した総圧縮量（圧縮率）です。

過去の書き込まれたデータのチェック

［Daily Written］グラフで、グラフの上の［Duration］線上の間隔（7d、30d、60d、または 120d）をクリックすると、グラフに表示されるデータの日数（7～120 日）を変更できます。

［Daily Written］グラフの下には、現在の期間値に対する次の合計値が表示されます。

- Pre-Comp Written
- Post-Comp Written
- Global-Comp Factor
- Local-Comp Factor
- Total-Comp Factor

MTree 使用状況のモニタリング

MTree のスペース使用量とデータ書き込みトレンドが表示されます。

手順

- ［**Data Management**］ > ［**MTree**］を選択します。

  ［MTree］ビューには、構成されている MTree のリストが表示され、リストで選択されている場合は［Summary］タブに MTree の詳細が表示されます。［Space Usage and Daily Written］タブには、選択された MTree のスペース使用量とデータ書き込みトレンドを視覚的に表示するグラフが表示されます。このビューには、CIFS、NFS、DD Boost 用の MTree 構成を可能にするオプションに加え、スナップショットと MTree に対する DD Retention Lock の管理のセクションも含まれます。

  ［MTree］ビューには、［MTree］概要パネルと 3 つのタブがあります。その詳細については、次に示すセクションを参照してください。

  - ［MTree］パネルについて（221 ページ）
  - ［Summary］ビューについて（221 ページ）
  - ［Space Usage］ビューについて（MTree）（226 ページ）
  - ［Daily Written］ビューについて（MTree）（226 ページ）

  注

  物理容量の測定（PCM）は、MTree のスペース使用状況に関する情報を提供します。PCM の詳細については、物理容量の測定に関するセクションを参照してください。

物理容量の測定について

PCM（物理容量の測定）は、ストレージ領域のサブ セットの使用状況の情報を提供します。DD System Manager から使用する場合、PCM は MTree のスペース使用に関する情報を提供しま

すが、コマンド ライン インターフェイスから使用する場合は MTree、テナント、テナント ユニット、パス セットのスペース使用情報を表示できます。

PCM のパスを選択すると、その下のすべてのパスが自動的に含められます。親パスを選択した後に子パスを選択しないでください。たとえば、`/data/col1/mtree3` を選択した場合は、**mtree3** の下のサブディレクトリを選択しないでください。

コマンド ラインからの PCM の使用の詳細については、「Data Domain Operating System コマンド リファレンス ガイド」を参照してください。

物理容量の測定の有効化、無効化、表示

物理容量の測定は、MTree のスペース使用状況に関する情報を提供します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Summary**］を選択します。

   ［File System］パネルに［Summary］タブが表示されます。

2. 右下隅にある［**^**］をクリックして、ステータス パネルを表示します。
3. ［**Physical Capacity Measurement Status**］の右にある［**Enable**］をクリックして、PCM を有効化します。
4. ［**Physical Capacity Measurement Status**］の右にある［**Details**］をクリックして、現在実行中の PCM ジョブを表示します。
   - ［**MTree**］：PCM が測定している MTree。
   - ［**Priority**］：タスクの優先度（［Normal］または［Urgent］）
   - ［**Submit Time**］：タスクがリクエストされた時刻。
   - ［**Duration**］：タスクを完了するまで PCM を実行した時間の長さ。
5. ［**Physical Capacity Measurement Status**］の右にある［**Disable**］をクリックして、PCM を無効化し、現在実行中の PCM ジョブをすべてキャンセルします。

物理容量の測定の初期化

物理容量の測定（PCM）の初期化は 1 回限りのアクションです。PCM が有効でキャッシュが初期化されていない場合のみ実行できます。キャッシュをクリーンアップし、測定速度を向上させます。PCM ジョブは初期化プロセス中も管理および実行できます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Configuration**］を選択します。
2. ［Cache］の右にある［Physical Capacity Measurement］の下で、［**Initialize**］をクリックします。
3. ［**Yes**］をクリックします。

物理容量の測定スケジュールの管理

物理容量の測定スケジュールを作成、編集、削除、表示します。このダイアログには、MTree 用に作成されたスケジュールと、現在割り当てられていないスケジュールのみが表示されます。

手順

1. ［**Data Management**］ > ［**MTree**］ > ［**Manage Schedules**］を選択します。
   - ［**Add**］（+）をクリックしてスケジュールを作成します。
   - スケジュールを選択し、［**Modify**］（鉛筆）をクリックしてスケジュールを編集します。

- スケジュールを選択し、［**Delete**］（X）をクリックしてスケジュールを削除します。

2. オプションとして、見出しの名前をクリックして、スケジュールの次の項目でソートします：［**Name**］、［**Status**］（Enabled または Disabled）、［**Priority**］（Urgent または Normal）、［**Schedule** ］（スケジュールのタイミング）、［**MTree Assignments**］（スケジュールを割り当てる MTree の数）。

物理容量の測定スケジュールの作成

物理容量の測定スケジュールを作成して、MTree に割り当てます。

手順

1. ［**Data Management**］ > ［**MTree**］ > ［**Manage Schedules**］を選択します。
2. ［**Add**］（+）をクリックしてスケジュールを作成します。
3. スケジュールの名前を入力します。
4. ステータスを選択します。
   - ［標準］：測定タスクを処理キューに送信します。
   - ［**Urgent**］：測定タスクを処理キューの最初に送信します。
5. スケジュールによって測定をトリガーする頻度を選択します：［**Day**］（毎日）、［**Week**］（毎週）、［**Month**］（毎月）。
   - ［**Day**］では時間を選択します。
   - ［**Week**］は、週の時間と曜日を選択します。
   - ［**Month**］は、その月の時間と曜日を選択します。
6. スケジュールの MTree 割り当てを選択します（MTree はスケジュールを割り当てる対象）。
7. ［**Create**］をクリックします。
8. オプションとして、見出しの名前をクリックして、スケジュールの次の項目でソートします：［**Name**］、［**Status**］（Enabled または Disabled）、［**Priority**］（Urgent または Normal）、［**Schedule** ］（スケジュールのタイミング）、［**MTree Assignments**］（スケジュールを割り当てる MTree の数）。

物理容量の測定スケジュールの編集

物理容量の測定スケジュールを編集します。

手順

1. ［**Data Management**］ > ［**MTree**］ > ［**Manage Schedules**］を選択します。
2. スケジュールを選択して、［**Modify**］（鉛筆）をクリックします。
3. スケジュールを変更して、［**Save**］をクリックします。

   スケジュールのオプションについては、「物理容量の測定スケジュールの作成」トピックで説明しています。
4. オプションとして、見出しの名前をクリックして、スケジュールの次の項目でソートします：［**Name**］、［**Status**］（Enabled または Disabled）、［**Priority**］（Urgent または Normal）、［**Schedule** ］（スケジュールのタイミング）、［**MTree Assignments**］（スケジュールを割り当てる MTree の数）。

物理容量の測定スケジュールの MTree への割り当て

スケジュールを MTree に割り当てます。

はじめに

PCM（物理容量の測定）スケジュールを作成する必要があります。

注

管理者は、MTree に最大 3 つの PCM スケジュールを割り当てることができます。

手順

1. ［**Data Management**］ > ［**MTree**］ > ［**Summary**］を選択します。
2. スケジュールを割り当てる MTree を選択します。
3. ［Physical Capacity Measurement］領域まで下にスクロールして、スケジュールの右にある［**Assign**］をクリックします。
4. MTree に割り当てるスケジュールを選択して、［**Assign**］をクリックしまします。

物理容量の測定の即時開始

できるだけ早く、測定プロセスを開始します。

手順

1. ［**Data Management**］ > ［**MTree**］ > ［**Summary**］を選択します。
2. ［Physical Capacity Measurement］領域まで下にスクロールして、［Submitted Measurements］の右にある［**Measure Now**］をクリックします。
3. ［**Normal**］（測定タスクを処理キューに送信）または［**Urgent**］（測定タスクを処理キューの先頭に送信）を選択します。
4. ［送信］をクリックします。

物理容量の測定スロットルの設定

物理容量の測定に使用される専用のシステム リソースの割合（%）を設定します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Settings**］を選択します。
2. ［Physical Capacity Measurement］領域で、スロットルの左にある［**Edit**］をクリックします。
3.

オプション	説明
Click Default	システム デフォルトの 20%を入力する。
Type throttle percent	物理容量の測定に使用される専用のシステム リソースの割合（%）。

4. ［**Save**］をクリックします。

MTree 操作の管理

このセクションでは、MTree の作成、構成、MTree クォータを有効化および無効化する方法などについて説明します。

MTree の作成

MTree は、ファイル システムの論理パーティションです。DD Boost ストレージ ユニット、DD VTL プール、NFS/CIFS 共有に MTrees を使用します。

MTree は、area/data/col1/mtree_name に作成されます。

手順

1. ［**Data Management**］ > ［**MTree**］を選択します。
2. MTree 概要領域で、［**Create**］をクリックします。
3. ［MTree Name］テキスト ボックスに MTree 名を入力します。MTree 名は 50 文字以下にする必要があります。次の文字が使用できます。
   - 大文字および小文字の英字：A～Z、a～z
   - 数字：0～9
   - 組み込みスペース
   - カンマ（,）
   - ピリオド（.）（名前の前には付けられません）。
   - 感嘆符（!）
   - シャープ記号（#）
   - ドル記号（$）
   - パーセンテージ記号（%）
   - プラス記号（+）
   - アットマーク（@）
   - 等号記号（=）
   - アンパサンド（&）
   - セミコロン（;）
   - 括弧（(と)）
   - 角括弧（[と]）
   - 中括弧（{と}）
   - キャレット（^）
   - チルダ（~）
   - アポストロフィ（傾斜していない一重引用符）
   - 傾斜した一重引用符（‘）
4. MTree が過剰に余分なスペースを使用することを防ぐため、ストレージ領域制限を設定します。ソフトまたはハード制限クォータ設定、またはその両方を入力します。ソフト制限がある場合、MTree サイズが上限を超えるとアラートが送信されますが、データはまだ MTree に書き込みできます。ハード制限に達すると、データを MTree に書き込めません。

注

クォータ制限は、圧縮前値です。
MTree にクォータ制限を設定するには、［**Set to Specific value**］を選択し、値を入力します。測定単位を MiB、GiB、TiB、PiB から選択します。

注

ソフト制限とハード制限両方を設定する場合、クォータのソフト制限はクォータのハード制限を超えることはできません。

5. ［**OK**］をクリックします。

   MTree テーブルで新しい MTree を表示します。

注

パス名全体を表示するには、［MTree Name］列の幅を拡張する必要がある場合があります。

MTree クォータの構成と有効化/無効化

MTree、ストレージ ユニット、DD VTL プールのストレージ領域制限を設定します。

［**Data Management**］ > ［**Quota**］ページは、管理者に対してソフトまたはハード クォータが設定されていない MTree の数を表示します。クォータが設定された MTree については、このページに、使用中の圧縮前ソフト リミットおよびハード リミットの割合が表示されます。

クォータを管理する場合は、次の情報を考慮してください。

- MTree クォータは、取り込み操作に適用されます。これらのクォータは、それがどの階層にあるかにかかわらず、DD Extended Retention ソフトウェアがあるシステムに加え、DD VTL、DD Boost、CIFS、NFS のデータに適用されます。
- スナップショットはカウントされません。
- クォータは、`/data/col1/backup` ディレクトリでは設定できません。
- 許可された最大クォータ値は 4096 PiB です。

MTree クォータの構成

［MTree］タブまたは［Quota］タブを使用して、MTree クォータを構成します。

手順

1. 次のメニュー パスのいずれかを選択します。
   - ［**Data Management**］ > ［**MTree**］を選択します。
   - ［**Data Management**］ > ［**Quota**］を選択します。
2. ［MTree］タブで MTree を 1 つだけ選択するか、［Quota］タブで 1 つ以上の MTree を選択します。

注

クォータは、`/data/col1/backup` ディレクトリでは設定できません。

3. ［MTree］タブで、［**Summary**］タブをクリックした後、［Quota］領域で［**Configure**］ボタンをクリックします。
4. ［Quota］タブで、［**Configure Quota**］ボタンをクリックします。

MTree クォータの構成

ハード クォータおよびソフト クォータの値を入力して、測定単位を選択します。

手順

1. ［Configure Quota for MTrees］ダイアログ ボックスで、ハード/ソフト クォータを入力し、単位を MiB、GiB、TiB、PiB から選択します。
2. ［OK］をクリックします。

MTree の削除

MTree テーブルから MTree を削除します。MTree データは次のクリーニングで削除されます。

注

MTree とその関連データはファイル クリーニングが実行されるまで削除されないため、削除された MTree がクリーニング操作によってファイル システムから完全に削除されるまで、削除された MTree と同じ名前の MTree を新規作成できません。

手順

1. ［**Data Management**］ > ［**MTree**］を選択します。
2. MTree を選択します。
3. MTree 概要領域で、［**Delete**］をクリックします。
4. ［**Warning**］ダイアログ ボックスの［OK］をクリックします。
5. 進行状況を確認した後、［Delete MTree Status］ダイアログ ボックスで［**Close**］をクリックします。

MTree の復元

復元すると、MTree とそのデータを取得し、それを MTree テーブルに戻すことができます。

MTree を復元すると、MTree とそのデータを取得し、それを MTree テーブルに戻すことができます。

復元は、MTree が削除対象としてマークされた後にファイル クリーニングが実行されていない場合にのみ実行可能です。

注

この手順を使用して、ストレージ ユニットを復元することもできます。

手順

1. ［**Data Management**］ > ［**MTree**］ > ［**More Tasks**］ > ［**Undelete**］を選択します。
2. 復元したい MTree のチェックボックスを選択し、［**OK**］をクリックします。
3. 進行状況を確認した後、［Undelete MTree Status］ダイアログ ボックスで［**Close**］をクリックします。

リカバリされた MTree が MTree テーブルに表示されます。

MTree の名称変更

Data Management MTree GUI を使用して、MTrees を名称変更します。

手順

1. ［**Data Management**］ > ［**MTree**］を選択します。
2. MTree テーブルで MTree を選択します。
3. ［Summary］タブを選択します。
4. ［Detailed Information］概要領域で、［**Rename**］をクリックします。
5. MTree の名前を［New MTree Name］テキスト ボックスに入力します。

   許可された文字リストについては、MTree の作成に関するセクションを参照してください。
6. ［**OK**］をクリックします。

   MTree テーブルに名称変更された MTree が表示されます。

第 7 章

スナップショット

本章には、次のセクションが含まれます。

- スナップショットの概要 236
- スナップショットとそのスケジュールのモニタリング 237
- スナップショットの管理 238
- スナップショット スケジュールの管理 240
- スナップショットからのデータのリカバリ 242

スナップショットの概要

本章では、MTree を使用したスナップショット機能の使用方法について説明します。

スナップショットは、特定の時点で指定された MTree の読み取り専用コピー（[スナップショット］を呼ばれます）を保存します。スナップショットをリストア ポイントとして使用できます。また、MTree スナップショットとスケジュールを管理し、既存のスナップショットのステータスに関する情報を表示できます。

注

ソース Data Domain システムで作成されたスナップショットは、コレクションおよび MTree レプリケーションの宛先にレプリケーションされます。コレクション レプリケーションのレプリカである Data Domain システムでスナップショットは作成できません。MTree レプリケーションのデスティネーション MTree でスナップショットを作成することもできません。ディレクトリ レプリケーションはスナップショットをレプリケーションせず、デスティネーション システムで別途スナップショットを作成する必要があります。

backup という名前の MTree のスナップショットは、システム ディレクトリ/data/col1/backup/.snapshot で作成されます。/data/col1/backup の下の各ディレクトリには、そのディレクトリを含む各スナップショットの名前を含む .snapshot ディレクトリも含まれます。各 MTree には同じタイプの構造があるため、SantaClara という名前の MTree には/data/col1/SantaClara/.snapshot というシステム ディレクトリがあり、/data/col1/SantaClara の各サブディレクトリにも同様に .snapshot ディレクトリがあります。

注

/data しかマウントされていない場合、.snapshot ディレクトリは表示されません。MTree 自体がマウントされている場合、.snapshot ディレクトリは表示されます。

期限切れのスナップショットは次のファイル システム クリーニング操作まで引き続き利用できます。

MTree あたりの許可されたスナップショットの最大数は 750 です。MTree あたりのスナップショットの数が最大許容数の 90%（675～749）に達すると警告が出されます。最大数に達するとアラートが出されます。警告をクリアするには、スナップショットを期限切れにし、ファイル システム クリーニング操作を実行します。

注

スナップショットの最大数に近付いている MTree を特定するには、MTree スナップショット情報の表示に関する［MTree］ページの［Snapshots］パネルをチェックします。

MTree のスナップショット保存にはスペースが必要ですが、スナップショットが存在し、元のファイルがすでに存在しない場合、そのスペースは再利用できません。

注

スナップショットおよび CIFS プロトコル：DD OS 5.0 では、Windows Explorer または DOS CMD シェルのディレクトリ リストで .snapshot ディレクトリは表示されなくなりました。Windows Explorer のアドレス バーまたは DOS CMD シェルに名前を入力して、.snapshot ディレクトリにアクセスできます。たとえば、 Z:が\\dd\backup としてマッピングされている場合は\\dd\backup\.snapshot または Z:\.snapshot です。

スナップショットとそのスケジュールのモニタリング

このセクションには、スナップショットとスナップショット スケジュールのステータスの詳細およびサマリー情報が表示されます。

［Snapshots］ビューについて

このセクションのトピックでは、［Snapshots］ビューについて説明します。

［Snapshots］概要パネル

スナップショットの合計数、期限切れスナップショットの数、有効期限前のスナップショット、次のクリーニングの時間が表示されます。

［**Data Management**］ > ［**Snapshots**］を選択します。

表 102 ［Snapshot］概要パネル情報

フィールド	説明
Total Snapshots (Across all MTrees)	システムのすべての MTree 上のアクティブまたは期限切れのスナップショットの総数。
期限切れ	作成対象としてマークされたが、まだクリーニング操作で削除されていないスナップショットの数。
Unexpired	保持対象としてマークされているスナップショットの数。
Next file system clean scheduled	次にスケジュール設定されたファイル システム クリーニング操作が実行される日付。

［Snapshots］ビュー

名前、MTree、作成時間、アクティブかどうか、有効期限ごとにスナップショット情報が表示されます。

［Snapshots］タブには、スナップショットのリストが表示され、次の情報がリストされます。

表 103 スナップショット情報

フィールド	説明
Selected Mtree	スナップショットが動作する MTree を選択するドロップダウン リスト。
Filter By	表示されるスナップショットのリストで検索するアイテム。オプション: • ［**Name**］: スナップショットの名前（ワイルドカード使用可）。 • ［**Year**］: 年を選択するドロップダウン リスト。
Name	スナップショット イメージの名前。
Creation Time	スナップショットが作成された日付。
Expires On	スナップショットの期限が切れる日付。
Status	スナップショットがアクティブな場合は Expired または空欄となるスナップショットのステータス。

［Schedules］ビュー

スナップショットが取得される日、時刻、保持される期間、命名規則が表示されます。

表 104 スナップショット スケジュール情報

フィールド	説明
Name	スナップショット スケジュールの名前。
Days	スナップショットが取られる日付。
Times	スナップショットが取られる時刻。
Retention Period	スナップショットが保存される期間。
Snapshot Name Pattern	スナップショット名を示す文字列と変数を入力します（たとえば、「scheduled-2010-04-12-17-33」を示す `scheduled-%Y-%m-%d-%H-%M` など）。

1. ［Schedules］タブでスケジュールを選択します。同じスケジュールを選択された MTree と共有する MTree がリストされる［Detailed Information］領域が表示されます。
2. スケジュール リストから MTree を追加または削除するには、［**Add/Remove**］ボタンをクリックします。

スナップショットの管理

このセクションでは、スナップショットを管理する方法について説明します。

スナップショットの作成

スケジュールされていないスナップショットが必要な場合にスナップショットを作成します。

手順

1. ［**Data Management**］ > ［**Snapshots**］を選択して、［Snapshots］ビューを表示します。
2. ［Snapshots］ビューで、［**Create**］をクリックします。
3. ［Name］テキスト フィールドに、スナップショットの名前を入力します。
4. ［MTree］領域の［Available MTrees］パネルで 1 つ以上の MTree のチェックボックスを選択し、［**Add**］をクリックします。
5. ［Expiration］領域で、次の有効期限のいずれかを選択します。
   a. ［**Never Expire**］。
   b. テキスト フィールドに、数字を入力し、ドロップダウン リストから［**Days**］、［**Weeks**］、［**Month**］、または［**Years**］を選択します。スナップショットは、それが作成された日の同じ時刻まで保存されます。
   c. ［On］テキスト フィールドに、日付（mm/dd/yyyy 形式を使用）を入力するか、［**Calendar**］をクリックし、日付をクリックします。スナップショットは、指定された日の深夜（00:00。日の最初の分）まで保存されます。
6. ［**OK**］と［**Close**］をクリックします。

スナップショットの有効期限の変更

スナップショットの有効期限を変更して、それらを削除したり、監査またはコンプライアンスのために期限を延長します。

手順

1. ［**Data Management**］ > ［**Snapshots**］を選択して、［Snapshots］ビューを表示します。
2. リストのスナップショット エントリーのチェックボックスをクリックし、［**Modify Expiration Date**］をクリックします。

   注

   さらにチェックボックスをクリックすることで、複数のスナップショットを選択できます。

3. ［Expiration］領域で、有効期限に次のいずれかを選択します。
   a. ［**Never Expire**］。
   b. ［In］テキスト フィールドに、数字を入力し、ドロップダウン リストから［**Days**］、［**Weeks**］、［**Month**］、または［**Years**］を選択します。スナップショットは、それが作成された日の同じ時刻まで保存されます。
   c. ［**On**］テキスト フィールドに、日付（mm/dd/yyyy 形式を使用）を入力するか、［**Calendar**］をクリックし、日付をクリックします。スナップショットは、指定された日の深夜（00:00。日の最初の分）まで保存されます。
4. ［**OK**］をクリックします。

スナップショットの名称変更

［Snapshot］タブを使用して、スナップショットを名称変更します。

手順

1. ［**Data Management**］ > ［**Snapshots**］を選択して、［Snapshots］ビューを表示します。
2. リストでスナップショット エントリーのチェックボックスを選択し、［**Rename**］をクリックします。
3. ［Name］テキスト フィールドに、新しい名前を入力します。
4. ［**OK**］をクリックします。

スナップショットの期限切れ

スナップショットは削除できません。ディスク領域を解放するには、スナップショットを期限切れにし、有効期限後の次のクリーニング サイクルで削除されるようにします。

手順

1. ［**Data Management**］ > ［**Snapshots**］を選択して、［Snapshots］ビューを表示します。
2. リストのスナップショット エントリーの隣にあるチェックボックスをクリックし、［**Expire**］をクリックします。

注

さらにチェックボックスを選択することで、複数のスナップショットを選択できます。
そのスナップショットは、［Status］列で Expired としてマークされ、次のクリーニング操作で削除されます。

スナップショット スケジュールの管理

一定間隔（スナップショット スケジュール）で自動的に取得される一連のスナップショットを設定して管理します。

複数のスナップショット スケジュールが同時にアクティブになる可能性があります。

注

複数のスナップショットが同時に実行されるようにスケジュール設定された場合、1 つのみ保存されます。どれを保存するかは定義されていないため、同じ時間に複数のスナップショットをスケジュールしないようにする必要があります。

スナップショット スケジュールの作成

データ管理 GUI を使用して、週次または月次のスナップショット スケジュールを作成します。

手順

1. ［**Data Management**］ > ［**Snapshots**］ > ［**Schedules**］を選択して、［Schedules］ビューを開きます。
2. ［**Create**］をクリックします。
3. ［**Name**］テキスト フィールドに、スケジュールの名前を入力します。
4. ［**Snapshot Name Pattern**］テキスト ボックスに、名前パターンを入力します。

   スナップショット名を示す文字列と変数を入力します（たとえば、**`scheduled-%Y-%m-%d-%H-%m`** は「scheduled-2012-04-12-17-33」を意味します）。現在の値を示す英字、数字、_、-、変数を使用します。

5. ［**Validate Pattern & Update Sample**］をクリックします。
6. ［次へ］をクリックします。
7. スケジュールを実行する日付を選択します。
   a. Weekly：曜日の隣のチェックボックスをクリックするか、［**Every Day**］を選択します。
   b. Monthly：［**Selected Days**］をクリックしてカレンダー上の日付をクリックするか、［**Last Day of the Month**］オプションを選択します。
   c. ［次へ］をクリックします。
8. スケジュールを実行する時刻を選択します。
   a. At Specific Times：［**Add**］をクリックすると表示される［Time］ダイアログに、hh:mm 形式で時刻を入力し、［**OK**］をクリックします。
   b. In Intervals：ドロップダウン矢印をクリックして、hh:mm 形式で開始時間と終了時間および午前または午後を選択します。［**Interval**］ドロップダウン矢印をクリックして、数字を選択した後、間隔の時間または分を選択します。

c. [次へ] をクリックします。

9. [Retention Period] テキスト エントリー フィールドで、数字を入力し、ドロップダウン矢印をクリックして、日数、月数、または年数を選択し、[**Next**] をクリックします。

   スケジュールには、保存時間を明示的に指定する必要があります。

10. スケジュール サマリーのパラメーターを確認し、[**Finish**] をクリックして、スケジュールを完了するか、[**Back**] をクリックしてエントリーを変更します。
11. MTree がスケジュールと関連づけられていない場合、警告ダイアログ ボックスに、MTree をスケジュールに追加するかどうかを確認するメッセージが表示されます。続けるには [**OK**] をクリックします（終了する場合、[**Cancel**] をクリックします）。
12. MTree をスケジュールに割り当てるには、[MTree] 領域の [Available MTrees] パネルで 1 つ以上の MTree のチェックボックスをクリックした後、[**Add**]、[**OK**] をクリックします。

スケジュールによって作成されたスナップショットの命名規則

スケジュール設定されたスナップショットの命名規則では、単語 scheduled の後ろにスナップショットが取られた日付を `scheduled-yyyy-mm-dd-hh-mm` 形式で付けます。たとえば、`scheduled-2009-04-27-13-30` のようにします。

「mon_thurs」は、スナップショット スケジュールの名前です。このスケジュールによって生成されたスナップショットの名前は、`scheduled-2008-03-24-20-00`、`scheduled-2008-03-25-20-00` などにできます。

スナップショット スケジュールの変更

スナップショット スケジュールの名前、日付、保存期間を変更します。

手順

1. スケジュール リストで、スケジュールを選択し、[**Modify**] をクリックします。
2. [Name] テキスト フィールドに、スケジュールの名前を入力し、[**Next**] をクリックします。

   英数字、_、-を使用できます。

3. スケジュールを実行する日付を次の中から選択します。
   a. Weekly：曜日の隣のチェックボックスをクリックするか、[**Every Day**] を選択します。
   b. Monthly：[**Selected Days**] をクリックしてカレンダー上の日付をクリックするか、[**Last Day of the Month**] オプションを選択します。
   c. [次へ] をクリックします。
4. スケジュールを実行する時刻を選択します。
   a. At Specific Times：[Times] リストでスケジュール設定された時刻のチェックボックスをクリックし、[**Edit**] をクリックします。表示される [Times] ダイアログに、hh:mm 形式で新しい時刻を入力し、[**OK**] をクリックします。または [**Delete**] をクリックして、スケジュール設定された時刻を削除します。
   b. In Intervals：ドロップダウン矢印をクリックして、hh:mm 形式で開始時間と終了時間および午前または午後を選択します。[Interval] ドロップダウン矢印をクリックして、数字を選択した後、間隔の時間または分を選択します。
   c. [次へ] をクリックします。
5. [Retention Period] テキスト エントリー フィールドで、数字を入力し、ドロップダウン矢印をクリックして、日数、月数、または年数を選択し、[**Next**] をクリックします。

6. スケジュール サマリーのパラメーターを確認し、［**Finish**］をクリックして、スケジュールを完了するか、［**Back**］をクリックしてエントリーを変更します。

スナップショット スケジュールの削除

スケジュール リストからスナップショット スケジュールを削除します。

手順

1. スケジュール リストで、チェックボックスをクリックしてスケジュールを選択し、［**Delete**］をクリックします。
2. 検証ダイアログ ボックスで、［**OK**］をクリックした後、［**Close**］をクリックします。

スナップショットからのデータのリカバリ

fastcopy 操作を使用して、スナップショットに保存されているデータを取得します。fastcopy 操作に関するセクションを参照してください。

第 8 章

CIFS

本章には、次のセクションが含まれます。

- CIFS の概要 244
- SMB 署名の構成 244
- CIFS のセットアップの実行 245
- 共有の扱い 247
- アクセス制御の管理 253
- CIFS 操作のモニタリング 258
- CIFS のトラブルシューティングの実行 261

CIFS の概要

CIFS（共通インターネット ファイル システム）クライアントは、Data Domain システムのシステム ディレクトリにアクセスできます。

- `/data/col1/backup` ディレクトリは、圧縮されたバックアップ サーバー データの宛先ディレクトリです。
- `/ddvar/core` ディレクトリには、Data Domain System コアとログ ファイルが含まれます（古いログとコア ファイルを削除して、この領域のスペースに空きを作ります）。

注

また、もしあれば、`/ddvar` ディレクトリまたは`/ddvar/ext` ディレクトリからコア ファイルを削除できます。

Data Domain システムでバックアップおよびリストア作業を実行するバックアップ サーバーのようなクライアントは、少なくとも、`/data/col1/backup` ディレクトリへのアクセス権が必要です。管理アクセス権を持つクライアントは、コアおよびログ ファイルを取得するために、`/ddvar/core` ディレクトリにアクセスできる必要があります。

初期 Data Domain システム構成の一環として、CIFS クライアントはこれらのディレクトリにアクセスするように構成されました。本章では、Data DD Manager と `cifs` コマンドを使用してこれらの設定を変更する方法およびデータ アクセスを管理する方法について説明します。

注

- DD System Manager の［**Protocols**］ > ［**CIFS**］ページでは、CIFS の有効化と無効化、認証の設定、共有の管理、構成および共有情報の表示などの、CIFS に関する主な操作を実行できます。
- `cifs` コマンドは、Windows クライアントと Data Domain システム間の CIFS バックアップとリストアを管理し、CIFS 統計およびステータスを表示するオプションが含まれます。`cifs` コマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。
- 初期システム構成の詳細については、「Data Domain オペレーティング システム初期構成ガイド」を参照してください。
- クライアントが Data Domain システムをサーバーとして使用するセットアップの詳細については、support.emc.com Web サイトで閲覧可能な「CIFS Tuning Guide」などの関連チューニング ガイドを参照してください。［検索］フィールドを使用して、ドキュメントの完全名を検索します。

SMB 署名の構成

対応する DD OS バージョンでは、サーバー署名と呼ばれる CIFS オプションを使用して SMB 署名機能を構成できます。

この機能を使用するとパフォーマンスが低下するため、デフォルトでは無効になっています。有効化されると、SMB 署名によってスループット パフォーマンスが 29%（読み取り）～50%（書き込み）低下する可能性がありますが、個別のシステム パフォーマンスは場合によって異なります。SMB 署名の設定値は、disabled、auto、mandatory の 3 つです。

- disabled に設定されると、SMB 署名は無効化されます。この設定がデフォルトです。
- required に設定されると、SMB 署名は必須となり、SMB 接続の両コンピューターは SMB 署名を有効化する必要があります。

SMB 署名 CLI コマンド

`cifs option set "server-signing" required`
サーバー署名を required に設定します。

`cifs option reset "server-signing"`
サーバー署名をデフォルト（disabled）にリセットします。

SMB 署名オプションを変更するたびに、次の CLI コマンドを使用して CIFS サービスを一旦無効化してから、有効化し直す（再起動する）ことをベスト プラクティスとして推奨します。

```
cifs disable
cifs enable
```

［DD System Manager］インターフェイスには、SMB 署名オプションが disabled であるか、auto または mandatory に設定されているかが表示されます。このインターフェイスにこの設定を表示するには、［**Protocols**］ > ［**CIFS**］ > ［**Configuration tab**］に移動します。［Options］領域で、SMB 署名オプションの値は、CLI コマンドを使用して値のセットを反映し、disabled、auto、または mandatory となります。

CIFS のセットアップの実行

このセクションでは、CIFS サービスを有効化する手順、CIFS サーバーを命名する手順などについて説明します。

HA システムと CIFS

HA システムは CIFS と互換性がありますが、フェイルオーバー時に進行中の CIFS ジョブがある場合は、そのジョブを再開する必要があります。

「/ddvar は ext3 ファイル システムであり、通常の MTree ベースの共有のように共有することはできません。2 つのノードでファイルハンドルが異なるため、アクティブ ノードがスタンバイ ノードにフェイルオーバーする際に、/ddvar の情報が古くなります。ログ ファイルにアクセスするため、またはシステムをアップグレードするために/ddvar をマウントしていて、前回/ddvar をマウントした後でフェイルオーバーが発生した場合は、/ddvar をアンマウントしてから再マウントしてください。」

Data Domain システムにアクセスするためのクライアントの準備

ドキュメントをオンラインで検索します。

手順

1. オンライン サポート（support.emc.com）Web サイトにログインします。
2. ［検索］フィールドで、探しているドキュメントの名前を入力します。
3. 「CIFS and Data Domain Systems Tech Note」などの適切なドキュメントを選択します。
4. ドキュメントの指示に従います。

CIFS サービスの有効化

CIFS プロトコルを使用して、クライアントがシステムにアクセスできるようにします。

クライアントが Data Domain システムにアクセスできるように構成した後、CIFS サービスを有効化します。これにより、クライアントは CIFS プロトコルを使用してシステムにアクセスできるようになります。

手順

1. ［DD System Manager Navigation］ツリーで選択されている Data Domain システムに対して、［**Protocols**］ > ［**CIFS**］をクリックします。
2. ［CIFS Status］領域で、［**Enable**］をクリックします。

CIFS サーバーの命名

CIFS サーバーとして機能している Data Domain システムのホスト名は、システムの初期構成中に設定されます。

CIFS サーバー名を変更するには、認証パラメーターの設定に関するセクションの手順を参照してください。

Data Domain システムのホスト名は、DNS テーブルの IP アドレスまたはアドレスに割り当てられた名前と一致する必要があります。そうでなければ、認証に加え、ドメインに参加する試行も失敗する可能性があります。Data Domain システムのホスト名の変更が必要な場合は、`net set hostname` コマンドを使用して、システムの DNS テーブル内のエントリーも変更してください。

Data Domain システムが CIFS サーバーとして機能する場合、システムのホスト名を使います。互換性を維持するために、NetBIOS 名も作成します。NetBIOS 名は、ホスト名の先頭の構成要素で、すべて大文字です。例えば、ホスト名 `jp9.oasis.local` は、NetBIOS 名 `JP9` にトランケートされます。CIFS サーバーはどちらの名前にも対応します。

NetBIOS のホスト名を変更することで、NetBIOS レベルで異なる名前に CIFS サーバーが応答するようにできます。

NetBIOS のホスト名の変更

CLI を使用して NetBIOS のホスト名を変更します。

手順

1. 次のコマンドを入力して、現在の NetBIOS 名を表示します。

   ```
   # cifs show config
   ```

2. `cifs set nb-hostname [nb-hostname]` コマンドを使用します。

認証パラメーターの設定

CIFS の処理のための Data Domain 認証パラメーターを設定します。

［Configuration］タブの［Authentication］ラベルの左側にある［Configure］リンクをクリックします。システムは、Active Directory、Kerberos、Workgroups、NIS の認証を構成できる［**Administration**］ > ［**Access**］ > ［**Authentication**］タブに移動します。

CIFS オプションの設定

CIFS 構成を表示し、匿名接続を制限します。

手順

1. ［**Protocols**］ > ［**CIFS**］ > ［**Configuration**］を選択します。
2. ［Options］領域で、［**Configure Options**］をクリックします。
3. 匿名接続を制限するには、［Restrict Anonymous Connections］領域の［**Enable**］オプションのチェックボックスをクリックします。
4. ［LogLevel］領域で、ドロップダウン リストをクリックして、レベル番号を選択します。

レベルは 1～5 の整数です。1 は最も詳細レベルの低い、CIFS 関連ログ メッセージを送信するデフォルト システム レベルです。5 に設定すると、最も詳細レベルが高くなります。ログ メッセージはファイル `/ddvar/log/debug/cifs/cifs.log` に保存されます。

注

ログ レベルが 5 の場合、システム パフォーマンスが低下します。問題のデバッグを行った後、［Log Level］領域で［**Default**］をクリックします。これによって、レベルが 1 に設定されます。

5. ［Server Signing］領域で、次のように選択します。
   - ［**Enabled**］：サーバー署名が有効
   - ［**Disabled**］：サーバー署名が無効
   - ［**Required**］：サーバー署名が必須

CIFS サービスの無効化

クライアントが Data Domain システムにアクセスしないようにします。

手順

1. ［**Protocols**］ > ［**CIFS**］を選択します。
2. ［Status］領域で、［**Disable**］をクリックします。
3. ［**OK**］をクリックします。

   CIFS アクセスを無効化した後でも、CIFS 認証サービスは Data Domain システムで動作を続けます。アクティブなディレクトリ ドメイン ユーザーの管理アクセスを認証するには、このサービスの継続が必要です。

共有の扱い

データを共有するには、Data Domain システムで共有を作成します。

共有は Data Domain システムと CIFS システムで管理されます。

Data Domain システムでの共有の作成

共有を作成する際は、各ディレクトリに個別にクライアント アクセスを割り当て、各ディレクトリから個別にアクセスを削除する必要があります。たとえば、`/ddvar` からクライアントを削除できますが、`/data/col1/backup` へのアクセスはまだ可能です。

Data Domain システムは、最大 3000 個の CIFS 共有に対応しています。[1] また、同時に 600 の接続が可能です。ただし、サポートされる接続の最大数はシステム メモリーに基づいています。1 回の接続で開かれるファイルの最大数を設定する詳細については、該当のセクションを参照してください。

1. ハードウェアの制限により影響を受けることがあります。

注

レプリケーションの実装が予定されている場合、Data Domain システムは、CIFS クライアントと NFS クライアントの両方からバックアップを受信することができますが、それぞれに別々のディレクトリが使用されます。同一のディレクトリに CIFS データと NFS データを混在させないでください。

手順

1. ［**Protocols**］ > ［**CIFS**］タブを選択して、［CIFS］ビューに移動します。
2. 認証パラメーターの設定に関するセクションの説明に従って、認証が構成されていることを確認します。
3. CIFS クライアントで、共有ディレクトリ権限またはセキュリティ オプションを設定します。
4. ［CIFS］ビューで、［Shares］タブをクリックします。
5. ［**Create**］をクリックします。
6. ［Create Shares］ダイアログ ボックスで、次の情報を入力します。

表 105 ［Shares］ダイアログ ボックス情報

項目	説明
Share Name	共有の記述名。
Directory Path	ターゲット ディレクトリへのパス（例：`/data/col1/backup/dir1`）。 注 col1 は小文字の L を使用し、後に数字 1 を使用します。
Comment	共有に関する説明用コメント。

注

共有名は、最大 80 文字までで、\ / : * ? " < > | + [ ] ; , =、拡張 ASCII 文字は使用できません。

7. ［Clients］領域で［Add］（［**+**］）をクリックして、クライアントを追加します。［Client］ダイアログ ボックスが表示されます。［Client］テキスト ボックスにクライアントの名前を入力して、［**OK**］をクリックします。

   クライアント名を入力する場合は、以下の点を考慮してください。

   - ブランクやタブ（空白）文字は有効化されません。
   - アスタリスク（*）と個別のクライアント名両方または特定の共有の IP アドレスを使用することは推奨されません。アスタリスク（*）がある場合、その共有のその他のクライアント エントリーは使用されません。
   - 特定の共有で同じクライアントのクライアント名とクライアント IP アドレス両方を使用する必要はありません。クライアント名が DNS テーブルで定義されている場合、クライアント名を使用します。
   - 共有がすべてのクライアントに使用できるようにするには、アスタリスク（*）をクライアントとして使用します。1 つ以上のユーザー名が指定されない限り（この場合、共有にアクセスできるのはリストされた名前のみです）、クライアント リストのすべてのユーザーは共有にアクセスできます。

   構成対象のクライアントごとにこのステップを繰り返します。

8. ［Max Connections］領域のテキスト ボックスを選択し、一度に有効化される共有への接続の最大数を入力します。デフォルト値（［Unlimited］ボタンでも設定可能）0 の場合、接続数は制限されません。
9. ［**OK**］をクリックします。

   新たに作成された共有が共有のリストの末尾に表示され、［Shares］パネルの中心に置かれます。

CLI 相当機能

手順

1. `cifs status` コマンドを実行して、CIFS が有効化されていることを確認します。
2. `filesys status` コマンドを実行して、ファイル システムが有効化されていることを確認します。
3. `hostname` コマンドを実行して、システムのホスト名を判別します。
4. CIFS 共有を作成します。

   ```
   cifs share create [<share>] path [<path>] {max-connections
   [<max connections>] | clients [<clients>] | users
   [<users>] | comment [<comment>]}
   ```

   ```
   # cifs share create backup path /backup
   ```

5. クライアントに共有へのアクセスを許可します。

   ```
   cifs share modify [<share>] {max-connections [<max
   connections>] | clients [<clients>] | browsing {enabled |
   disabled} | writeable {enabled | disabled} | users
   [<users>] | comment [<comment>]}
   ```

   ```
   # cifs share modify backup clients
   "srvr24.yourdomain.com,srvr24,10.24.160.116
   ```

6. 必要に応じて共有を可視にします。

   ```
   cifs share [<share>] browsing enabled
   ```

   ```
   # cifs share backup browsing enabled
   ```

7. 必要に応じて、共有を書き込み可能にします。

   ```
   cifs share [<share>] writeable enabled
   ```

   ```
   # cifs share backup writeable enabled
   ```

8. Windows システムから、［スタート］ > ［ファイル名を指定して実行］を選択し、CIFS 共有のホスト名とディレクトリを入力します。

   \\<DDhostname>.<DDdomain.com>\<sharename>

9. CIFS 共有への接続に問題がある場合は、`cifs share show` コマンドを実行して共有のステータスを確認します。

   警告 `WARNING: 共有パスが存在しません。`共有が存在しない場合、または作成時に綴りが誤っている場合に表示されます。

   ```
   # cifs share show
   --------------- share backup ---------------
   ```

```
enabled: yes
path: /backup
```

10. それでも CIFS 共有にアクセスできない場合は、すべてのクライアント情報がアクセス リストにあり、すべてのネットワーク接続が機能していることを確認します。

Data Domain システムでの共有の変更

共有情報と接続を変更します。

手順

1. [**Protocols**] > [**CIFS**] > [**Shares**] を選択して、[CIFS] ビューの [Shares] タブに移動します。
2. [Share Name] リストで、変更する共有の隣にあるチェックボックスをクリックします。
3. [変更] をクリックします。
4. 共有情報を変更します。
   a. コメントを変更するには、[Comment] テキスト フィールドに新しいテキストを入力します。
   b. User または Group 名を変更するには、[User/Group] リストで、ユーザーまたはグループのチェックボックスをクリックし、[**Edit**] (鉛筆アイコン) または [**Delete**] (X) をクリックします。ユーザーまたはグループを追加するには、([**+**]) をクリックし、[User/Group] ダイアログ ボックスで、User または Group の Type を選択して、ユーザーまたはグループ名を入力します。
   c. クライアント名を変更するには、[Client] リストで、クライアントのチェックボックスをクリックし、[**Edit**] (鉛筆アイコン) または [**Delete**] (X) をクリックします。クライアントを追加するには、[Add] ([**+**]) をクリックし、[Client] ダイアログ ボックスに名前を入力します。

   注

   共有がすべてのクライアントに使用できるようにするには、アスタリスク (*) をクライアントとして使用します。1 つ以上のユーザー名が指定されない限り (この場合、共有にアクセスできるのはリストされた名前のみです)、クライアント リストのすべてのユーザーは共有にアクセスできます。

   d. [**OK**] をクリックします。
5. [Max Connections] 領域のテキスト ボックスで、一度に許可される共有への接続の最大数を変更します。または、Unlimited を選択して、接続数の制限をなくします。
6. [**OK**] をクリックします。

既存の共有からの共有の作成

既存の共有から共有を作成し、必要に応じて新しい共有を変更します。

注

既存の共有のユーザー権限は、新しい共有に継承されます。

手順

1. [CIFS Shares] テーブルでは、ソースとして使用する共有のチェックボックスをクリックします。

2. ［**Create From**］をクリックします。
3. Data Domain システムでの共有の変更に関するセクションで示すとおり、共有情報を変更します。

Data Domain システムでの共有の無効化

1 つ以上の既存の共有を無効化します。

手順

1. ［Shares］タブでは、［Share Name］リストで無効化する共有のチェックボックスをクリックします。
2. ［無効化］をクリックします。
3. ［**Close**］をクリックします。

Data Domain システムでの共有の有効化

1 つ以上の既存の共有を有効化します。

手順

1. ［Shares］タブでは、［Share Name］リストで有効化する共有のチェックボックスをクリックします。
2. ［**Enable**］をクリックします。
3. ［**Close**］をクリックします。

Data Domain システムでの共有の削除

1 つ以上の既存の共有を削除します。

手順

1. ［Shares］タブでは、［Share Name］リストで削除する共有のチェックボックスをクリックします。
2. ［**Delete**］をクリックします。

   ［Warning］ダイアログ ボックスが表示されます。

3. ［OK］をクリックします。

   共有が削除されます。

MMC 管理の実行

管理には MMC（Microsoft 管理コンソール）を使用します。

DD OS は、次の MMC 機能に対応しています。

- 共有追加時のブラウズ、手動プロセスであるオフライン設定のデフォルトの変更を除く共有管理。
- セッション管理。
- ファイルの削除を除くファイル管理の開始。

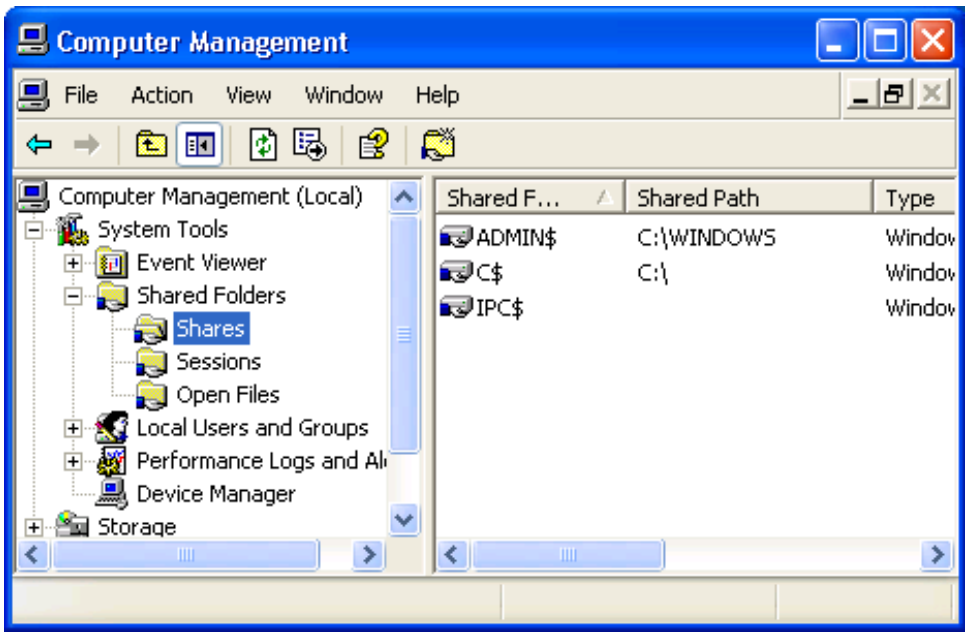
CIFS クライアントからの Data Domain システムへの接続

CIFS を使用して Data Domain システムに接続し、読み取り専用バックアップ サブフォルダーを作成します。

手順

1. ［Data Domain system CIFS］ページで、CIFS Status が、CIFS が有効かつ実行中であることを示していることを確認します。
2. ［Control Panel］で、［Administrative Tools］を開き、［**Computer Management**］を選択します。
3. ［Computer Management］ダイアログ ボックスで、［**Computer Management (Local)**］を右クリックし、メニューから［**Connect to another computer**］を選択します。
4. ［Select Computer］ダイアログ ボックスで、［**Another computer**］を選択し、Data Domain システムの名前または IP アドレスを入力します。
5. `\backup` サブフォルダーを読み取り専用として作成します。詳細については、読み取り専用としての/data/col1/backup サブフォルダーに関するセクションを参照してください。

図 7 ［Computer Management］ダイアログ ボックス



読み取り専用としての\data\col1\backup サブフォルダーの作成

パス、共有名を入力して、権限を選択します。

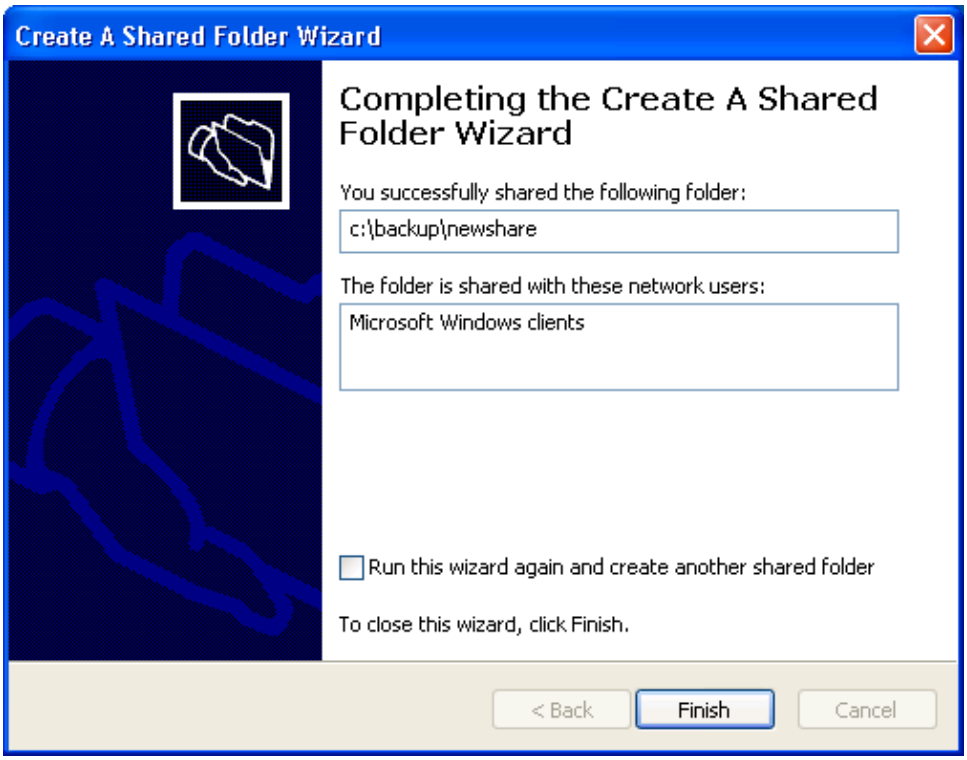
手順

1. ［Control Panel］で、［Administrative Tools］を開き、［**Computer Management**］を選択します。
2. Shared Folders ディレクトリで［**Shares**］を右クリックします。
3. メニューから［**New File Share**］を選択します。

   ［**Create a Shared Folder**］ウィザードが開きます。コンピューター名は、Data Domain システムの名前または IP アドレスである必要があります。

4. `C:\data\col1\backup\newshare` などの共有する Folder のパスを入力します。
5. **`newshare`** などの Share 名を入力します。［Next］をクリックします。
6. ［Share Folder Permissions］で選択された Administrator はフルアクセス権を持ちます。他のユーザーは読み取り専用アクセス権を持ちます。［Next］をクリックします。

図 8 ［Create a Shared Folder］ウィザードの完了



7. ［Completing］ダイアログは、ネットワーク上のすべての Microsoft Windows クライアントとフォルダーを正しく共有されたことを示します。［Finish］をクリックします。

   新たに作成された共有フォルダーは、［Computer Management］ダイアログ ボックスにリストされます。

CIFS 情報の表示

共有フォルダー、セッション、オープン ファイルの情報を表示します。

手順

1. ［Control Panel］で、［Administrative Tools］を開き、［**Computer Management**］を選択します。
2. ［System Tools］ディレクトリで［Shared Folders］（［**Shares**］、［**Sessions**］、または［**Open Files**］）のいずれかを選択します。

   共有フォルダー、セッション、オープン ファイルについての情報が、右のパネルに表示されます。

アクセス制御の管理

Windows クライアントから共有にアクセスし、管理アクセスを提供し、トラステッド ドメイン ユーザーからのアクセスを許可します。

Windows クライアントからの共有へのアクセス

コマンド ラインを使用して、共有をマッピングします。

手順

- Windows クライアントから、次の DOS コマンドを使用します：
  `net use [drive] : [backup-location]`

たとえば、次のように入力します。

```
# \\dd02\backup /USER:dd02\backup22
```

このコマンドは、Data Domain システム dd02 からバックアップ共有を Windows システムのドライブ H に割り当て、backup22 という名前のユーザーに`\\DD_sys\backup` ディレクトリのアクセス権を与えます。

DD OS は、SMB Change Notify 機能をサポートしています。これにより、CIFS サーバーが CIFS 共有の変更を Windows クライアントに自動的に通知できるようになり、クライアントが Data Domain システムをポーリングして共有に対する変更を検索する必要がなくなるため、Windows クライアント上の CIFS のパフォーマンスが向上します。

ドメイン ユーザーへの管理アクセスの付与

コマンド ラインを使用して、CIFS を追加し、SSH コマンドにドメイン名を含めます。

手順

- 次のコマンドを実行します。**adminaccess authentication add cifs**

  Data Domain システムにアクセスする SSH、Telnet、または FTP コマンドには、ドメイン名、バックスラッシュ、二重引用符で囲んだユーザー名を含める必要があります。次に例を挙げます。

  ```
  C:> ssh "domain2\djones" @dd22
  ```

Data Domain システムへのドメイン ユーザーによる管理アクセスの許可

コマンド ラインを使用して、DD システムのデフォルト グループ番号をマッピングし、CIFS 管理アクセスを有効化します。

手順

1. Data Domain System のデフォルト グループ番号を、デフォルト グループ名とは異なる Windows グループ名にマッピングするには、
   `cifs option set "dd admin group2" ["windows [grp-name] "]`
   コマンドを使用します。

   Windows グループ名は、Windows ドメイン コントローラーに存在するグループ（ユーザー役割（管理者、ユーザー、またはバックアップ オペレーター）のいずれかに基づく）です。また、最大 50 のグループ（dd admin group1 から dd admin group50）を指定できます。

   注

   DD OS ユーザー役割と Windows グループの詳細については、Data Domain システムの管理に関するセクションを参照してください。

2. 次のコマンドを入力して、CIFS 管理アクセスを有効化します。

   ```
   adminaccess authentication add cifs
   ```

- デフォルト Data Domain System グループ dd admin group1 は、Windows グループ Domain Admins にマッピングされます。
- デフォルト Data Domain System グループ dd admin group2 を、Windows ドメイン コントローラー上に作成する Data Domain という名前の Windows グループにマッピングします。
- SSH、Telnet、FTP、HTTP、HTTPS を通してアクセスできます。
- Windows グループ **Data Domain** から Data Domain システムへの管理アクセスをセットアップした後、`adminaccess` コマンドを使用して CIFS 管理アクセスを有効化する必要があります。

Windows からの管理アクセスの制限

コマンド ラインを使用して、DD アカウントを持たないユーザーへのアクセスを禁止します。

手順

- 次のコマンドを実行します。**adminaccess authentication del cifs**

  このコマンドは、Data Domain システム上にアカウントを持っていない場合の Data Domain システムへの Windows ユーザー アクセスを禁止します。

ファイル アクセス

このセクションには、ACL についての情報、Windows Explorer を使用した DACL および SACL 権限の設定についての情報などが含まれています。

NT アクセス コントロール リスト

Data Domain システム上では、ACL（アクセス コントロール リスト）がデフォルトで有効になっています。

⚠ 注意

Data Domain は、NTFS ACL が有効化されている場合はそれを無効化しないことを推奨します。NTFS ACL を無効化する前、Data Domain Support にお問い合わせください。

デフォルト ACL 権限

ACL が有効な場合に CIFS プロトコルを通して作成された新しいオブジェクトに割り当てられたデフォルト権限は、親ディレクトリのステータスに依存します。次の 3 つの可能性があります。

- 親ディレクトリが NFS プロトコルで作成されたため、ACL がない。
- 親ディレクトリが CIFS プロトコルで作成されたか、ACL が明示的に設定されたため、継承可能な ACL がある。継承可能な ACL が新しいオブジェクトで設定されている。
- 親ディレクトリが継承できないため、ACL がない。権限は次のとおりです。

表 106 権限

タイプ	Name	権限	適用先
許可する	SYSTEM	フル コントロール	このフォルダーのみ
許可する	CREATOR OWNER	フル コントロール	このフォルダーのみ

注

CREATOR OWNER は、通常のユーザーの場合は当該ファイル/フォルダーを作成したユーザー、管理ユーザーの場合は Administrator となります。

親ディレクトリに ACL がない場合の新しいオブジェクトの権限
権限は次のとおりです。

- BUILTIN\Administrators:(OI)(CI)F
- NT AUTHORITY\SYSTEM:(OI)(CI)F
- CREATOR OWNER:(OI)(CI)(IO)F
- BUILTIN\Users:(OI)(CI)R
- BUILTIN\Users:(CI)(special access:)FILE_APPEND_DATA
- BUILTIN\Users:(CI)(IO)(special access:)FILE_WRITE_DATA
- Everyone:(OI)(CI)R

これらの権限の詳細は次のとおりです。

表 107 権限の詳細

タイプ	Name	権限	適用先
許可する	管理者	フル コントロール	このフォルダー、サブフォルダー、ファイル
許可する	SYSTEM	フル コントロール	このフォルダー、サブフォルダー、ファイル
許可する	CREATOR OWNER	フル コントロール	サブフォルダーとファイルのみ
許可する	ユーザー	読み取りと実行	このフォルダー、サブフォルダー、ファイル
許可する	ユーザー	サブフォルダーの作成	このフォルダーとサブフォルダーのみ
許可する	ユーザー	ファイルの作成	サブフォルダーのみ
許可する	Everyone	読み取りと実行	このフォルダー、サブフォルダー、ファイル

ACL 権限とセキュリティの設定
NetBackup などの Windows ベース バックアップとリストア ツールは、DACL 保護ファイルと SACL 保護ファイルのバックアップ、Data Domain システムからのそれらのリストアに使用できます。

細分性の高い複雑な権限（DACL）
`cacls`、`xcacls`、`xcopy`、`scopy` などの Windows コマンドまたは Windows Explorer GUI を使用した CIFS プロトコルによって、ファイル システム内のファイルまたはフォルダー オブジェクトに対する細分性の高い複雑な権限（DACL）を設定できます。

監査 ACL（SACL）
コマンドまたは Windows Explorer GUI を使用した CIFS プロトコルを通して、ファイル システムのオブジェクトで監査 ACL（SACL）を設定できます。

Windows Explorer を使用した DACL 権限の設定

Explorer のプロパティ設定を使用して、DACL 権限を選択します。

手順

1. ファイルまたはフォルダーを右クリックし、［**Properties**］を選択します。
2. ［Properties］ダイアログ ボックスの［Security］タブをクリックします。
3. リストから、［**Administrators**］などのグループまたはユーザー名を選択します。この場合、`Administrators, Full Control` の権限が表示されます。
4. ［**Advanced**］ボタンをクリックすると、特殊権限を設定できます。
5. ［Advanced Security Settings for ACL］ダイアログ ボックスで、［Permissions］タブをクリックします。
6. リストで権限エントリーを選択します。
7. 権限エントリーの詳細を表示するには、エントリーを選択し、［**Edit**］をクリックします。
8. 親オプションから［Inherit］を選択して、親エントリーの権限を子オブジェクトに継承させ、［**OK**］をクリックします。

Windows Explorer を使用した SACL 権限の設定

Explorer のプロパティ設定を使用して、SACL 権限を選択します。

手順

1. ファイルまたはドライブを右クリックし、メニューから［**Properties**］を選択します。
2. ［Properties］ダイアログ ボックスの［Security］タブをクリックします。
3. リストから、［**Administrators**］などのグループまたはユーザー名を選択すると、その権限が表示されます（この場合は `Full Control`）。
4. ［**Advanced**］ボタンをクリックすると、特殊権限を設定できます。
5. ［Advanced Security Settings for ACL］ダイアログ ボックスで、［Auditing］タブをクリックします。
6. リストで監査エントリーを選択します。
7. 特殊な監査エントリーの詳細を表示するには、エントリーを選択し、［**Edit**］をクリックします。
8. 親オプションから［Inherit］を選択して、親エントリーの権限を子オブジェクトに継承させ、［**OK**］をクリックします。

現在の所有者のセキュリティ ID（所有者の SID）の表示または変更

［Advanced Security Settings for ACL］ダイアログ ボックスを使用します。

手順

1. ［Advanced Security Settings for ACL］ダイアログ ボックスで、［Owner］タブをクリックします。
2. 所有者を変更するには、［Change owner］リストから名前を選択し、［**OK**］をクリックします。

ID アカウント マッピングの制御

CIFS オプション idmap-type は、IP アカウント マッピング動作を制御します。

このオプションの値は、rid（デフォルト）と none の 2 つです。オプションが rid に設定されると、ID から ID へのマッピングが内部で実行されます。オプションが none に設定されると、すべての CIFS ユーザーが、ローカルな UNIX ユーザーのグループに属する「cifsuser」という名前のローカル UNIX ユーザーにマッピングされます。

このオプションを管理するときは、次の情報を考慮してください。

- このオプションを設定するには、CIFS を無効化する必要があります。CIFS が動作中の場合、CIFS サービスを無効化します。
- idmap-type は、ACL サポートが有効な場合にのみ none に設定できます。
- idmap タイプが変更されると、正しくファイルにアクセスするためにファイル システム メタデータが必要となる場合があります。ユーザーは、変換なしではデータにアクセスできない可能性があります。メタデータを変換するには、契約しているサポート プロバイダーに相談してください。

CIFS 操作のモニタリング

CIFS 操作の監視のトピック。

CIFS ステータスの表示

CIFS ステータスを表示し、有効化/無効化します。

手順

1. DD System Manager で、［**Protocols**］ > ［**CIFS**］を選択します。
   - ステータスは、有効で実行中である、または無効であるが CIFS 認証は実行中であることを示します。
     CIFS を有効化するには、CIFS サービスの有効化に関するセクションを参照してください。CIFS を無効化するには、CIFS サービスの無効化に関するセクションを参照してください。
   - ［**Connections**］には、開いた接続と開いたファイルの集計がリストされます。

   表 108 ［Connections Details］の情報

項目	説明
Open Connections	CIFS 接続を開く
Connection Limit	許可される最大接続数
開いているファイル	現在開いているファイル
Max Open Files	Data Domain システムで開くファイルの最大数

2. ［**Connection Details**］をクリックして詳細情報を確認します。

   表 109 ［Connections Details］の情報

項目	説明
セッション	アクティブな CIFS セッション
コンピューター	セッションの DDR と接続されている IP アドレスまたはコンピューター名
ユーザー	DDR に接続されているコンピューターを動かしているユーザー
開いているファイル	各セッションで開いているファイル数
Connection Time	接続の長さ（分単位）
ユーザー	コンピューターのドメイン名
モード	ファイルの権限

表 109 ［Connections Details］の情報 （続き）

項目	説明
ロック	ファイルのロック数
ファイル	ファイルの場所

CIFS 構成の表示

このセクションには、CIFS 構成が表示されます。

認証構成

［Authentication］パネルの情報は、構成される認証のタイプによって異なります。

［Configuration］タブの［Authentication］ラベルの左側にある［Configure］リンクをクリックします。［**Administration**］ > ［**Access**］ > ［**Authentication**］ページに移動し、Active Directory、Kerberos、ワークグループ、NIF の認証を構成できます。

Active Directory 構成

表 110 Active Directory 構成情報

項目	説明
モード	Active Directory モードが表示されます。
レルム	構成済みのレルムが表示されます。
DDNS	DDNS サーバーのステータス（有効または無効）が表示されます。
Domain Controllers	構成済みのドメイン コントローラーの名前が表示されます。すべてのコントローラーが許可されている場合は*が表示されます。
組織単位	構成済みの組織単位の名前が表示されます。
*CIFS サーバー名	構成済みの CIFS サーバーの名前が表示されます。
WINS Server Name	構成済みの WINS サーバーの名前が表示されます。
Short Domain Name	短縮ドメイン名が表示されます。

Workgroup Configuration

表 111 Workgroup Configuration Authentication Information

項目	説明
モード	Workgroup モードが表示されます。
Workgroup Name	構成済みのワーク グループ名が表示されます。
DDNS	DDNS サーバーのステータス（有効または無効）が表示されます。
*CIFS サーバー名	構成済みの CIFS サーバーの名前が表示されます。
WINS Server Name	構成済みの WINS サーバーの名前が表示されます。

共有情報の表示

このセクションには、共有情報が表示されます。

構成済みの共有の表示

構成済みの共有のリストの表示

表 112 構成済みの共有の情報

項目	説明
Share Name	共有の名前（share1 など）。
Share Status	共有のステータス： enabled または disabled。
Directory Path	共有へのディレクトリ パス（`/data/col1/backup/dir1` など）。 注 col1 には、小文字の L の後に数字の 1 を使います。
Directory Path Status	ディレクトリ パスのステータス。

- 特定の共有についての情報をリストするには、［Filter by Share Name］テキスト ボックスに共有名を入力し、［**Update**］をクリックします。
- ［**Update**］をクリックして、デフォルト値に戻ります。
- 共有のリストのページを変えるには、ビュー右下の［**<**］および［**>**］矢印をクリックして、前または後ろのページに移動します。リストの先頭に戻るには、［**|<**］をクリックします。末尾に進むには、［**>|**］をクリックします。
- ［**Items per Page**］ドロップダウン矢印をクリックして、ページにリストされた共有エントリーの数を変更します。選択肢は、15、30、または 45 エントリーです。

詳細な共有情報の表示

共有リストで共有名をクリックして、詳細な共有情報を表示します。

表 113 共有情報

項目	説明
Share Name	共有の名前（share1 など）。
Directory Path	共有へのへのディレクトリ パス（例： `/data/col1/backup/dir1`）。 注 col1 は小文字の L を使用し、後に数字 1 を使用します。
Directory Path Status	DDR に構成済みのディレクトリ パスが存在するかどうかを示す。使用可能な値は［Path Exists］または［Path Does Not Exist］。後者は不正または不完全な CIFS 構成を示す。
Max Connections	共有への最大同時接続数。デフォルト値は［Unlimited］。

表 113 共有情報 （続き）

項目	説明
Comment	共有が作成されたときに構成されたコメント。
Share Status	共有のステータス（有効または無効）。

- ［Clients］領域には、共有にアクセスするよう構成されたクライアントがリストされ、リストの下にクライアント集計が表示されます。
- ［User/Groups］領域には、共有にアクセスするよう構成されたユーザーまたはグループの名前とタイプがリストされ、リストの下にユーザーまたはグループ集計が表示されます。
- ［Options］領域には、構成されたオプションの名前と値がリストされます。

CIFS 統計の表示

コマンド ラインを使用して、CIFS 統計を表示します。

手順

- 次のコマンドを実行します。**`cifs show detailed-stats`**

  出力には、受信した各種 SMB 要求の数とその処理に要した時間が表示されます。

CIFS のトラブルシューティングの実行

このセクションでは、基本的なトラブルシューティング手順について説明します。

注

`cifs troubleshooting` コマンドを実行すると、CIFS ユーザーおよびグループの詳細が表示されます。

クライアントの現在のアクティビティの表示

コマンド ラインを使用して、CIFS セッションと開いているファイルの情報を表示します。

手順

- 次のように入力します：**`cifs show active`**

結果

表 114 セッション

コンピューター	ユーザー	開いているファイル	接続時間（秒）	アイドル時間（秒）
::ffff:10.25.132.84	ddve-25179109\sysadmin	1	92	0

表 115 開いているファイル

ユーザー	モード	ロック	ファイル
ddve-25179109\sysadmin	1	0	C:\data\col1\backup

接続上での最大オープン ファイル数の設定

コマンド ラインを使用して、同時にオープンできるファイルの最大数を設定します。

手順

- 次のとおり入力します：**`cifs option set max-global-open-files`**value。

  グローバル オープン ファイルの最大 value は、1 から、オープン ファイルの上限の間で指定できます。上限は DDR のシステム メモリに基づきます。12 GB を超えるシステムの場合、オープン ファイルの上限は 30,000 です。12 GB より小さいシステムの場合、オープン ファイルの上限は 10,000 です。

  表 116 接続とオープン ファイルの上限

DDR モデル	メモリ	接続の上限	オープン ファイルの上限
DD620、DD630、DD640	8 GB	300	10,000
DD640	16 GB	600	30,000
DD640	20 GB	600	30,000
DD860	36 GB	600	30,000
DD860、DD860ArT	72 GB	600	30,000
	96 GB	600	30,000
	128 GB	600	30,000
	256 GB	600	30,000

注

このシステムでは、CIFS 接続数は最大 600 件まで、オープン ファイル数は最大 250,000 個までに制限されています。ただし、システムのオープン ファイルが不足した場合、ファイルの数を増やすことができます。

注

ファイル アクセス レーテンシーは、ディレクトリ内のファイル数に影響されます。可能な範囲で、ディレクトリ サイズは 250,000 未満にすることを推奨します。ディレクトリ サイズがそれより大きいと、ディレクトリ内のファイルのリスト、ファイルの開閉などのメタデータ操作に対する応答が遅くなる可能性があります。

Data Domain システム クロック

CIFS アクセスのアクティブ ディレクトリ モードを使用する場合、Data Domain System クロック タイムは、ドメイン コントローラーの時間と最大 5 分まで差が出る場合があります。

DD System Manager では、［**Administration**］ > ［**Settings**］ > ［**Time and Date Settings**］タブでクロックとタイム サーバーを同期します。

Windows ドメイン コントローラーは外部ソースから時間を取得するため、NTP を構成する必要があります。Windows オペレーティング システム バージョンまたはドメイン コントローター上で実行中のサービス パック用の NTP を構成する方法については、Microsoft 社のドキュメントを参照してください。

アクティブ ディレクトリ認証モードでは、Data Domain システムが定期的にクロックを Windows Active Directory Domain Controller と同期します。

Windows ドメイン コントローラーからの同期

Windows ドメイン コントローラーでコマンド ラインを使用して、NTP サーバーと同期します。

注

これは、Windows 2003 SP1 の例です。NTP サーバーの名前（ntpservername）のドメイン サーバーの代替となります。

手順

1. Windows システムで、次のようなコマンドを入力します。

   ```
   C:\>w32tm /config /syncfromflags:manual /manualpeerlist: ntp-server-name C:\>w32tm /config /update C:\>w32tm /resync
   ```

2. NTP がドメイン コントローラーで構成された後、日時設定に関するセクションの説明に従って時間サーバー同期を構成します。

NTP サーバーからの同期

日時設定に関するセクションの説明に従って、時間サーバー同期を構成します。

第 9 章

NFS

本章には、次のセクションが含まれます。

- NFS の概要 266
- Data Domain システムへの NFS クライアント アクセスの管理 267
- NFS 情報の表示 271
- Kerberos ドメインへの DDR の統合 272
- 初期構成後の KDC サーバーの追加と削除 274

NFS の概要

NFS（ネットワーク ファイル システム）クライアントは、システム ディレクトリまたは Data Domain システムの MTree にアクセスすることがでます。

- /backup ディレクトリは、非 MTree 圧縮バックアップ サーバー データのデフォルトのデスティネーションです。
- 圧縮バックアップ サーバー データに MTree を使用する場合、/data/col1/backup パスが、デスティネーションのルート パスになります。
- /ddvar/core ディレクトリには、Data Domain System コアとログ ファイルが含まれます（古いログとコア ファイルを削除して、この領域のスペースに空きを作ります）。

注

Data Domain システムでは、/ddvar/core は別のパーティションに存在します。/ddvar だけをマウントする場合、/ddvar のマウント ポイントから/ddvar/core へのナビゲートはできません。

Data Domain システムでバックアップおよびリストア作業を実行するバックアップ サーバーのようなクライアントは、/backup または/data/col1/backup エリアへのアクセス権が必要です。管理アクセス権を持つクライアントは、コアおよびログ ファイルを取得するために、/ddvar/core ディレクトリにアクセスできる必要があります。

初期 Data Domain システム構成の一環として、NFS クライアントはこれらの領域にアクセスするように構成されました。本章では、これらの設定の変更方法とデータ アクセスの管理方法について説明します。

注

- 初期システム構成の詳細については、「Data Domain オペレーティング システム初期構成ガイド」を参照してください。
- nfs コマンドは、NFS クライアントと Data Domain システム間のバックアップとリストアを管理し、NFS 統計およびステータスを表示します。nfs コマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。
- サード パーティ クライアントが Data Domain システムをサーバーとして使用するセットアップの詳細については、Data Domain サポート Web サイトで閲覧可能な「Solaris System Tuning」などの関連チューニング ガイドを参照してください。［Documentation］ > ［Integration Documentation］ ページで、リストからベンダーを選択し、［**OK**］ をクリックします。リストからチューニング ガイドを選択します。

HA システムと NFS

HA システムは NFS と互換性があります。フェイルオーバー時に進行中の NFS ジョブがある場合でも、ジョブを再開する必要は**ありません**。

注

/ddvar は ext3 ファイル システムであり、通常の MTree ベースの共有のように共有することはできません。2 つのノードでファイルハンドルが異なるため、アクティブ ノードがスタンバイ ノードにフェイルオーバーする際に、/ddvar の情報が古くなります。ログ ファイルにアクセスするため、またはシステムをアップグレードするために/ddvar をマウントしていて、前回/ddvar をマウントした後でフェールオーバーが発生した場合は、/ddvar をアンマウントしてから再マウントしてください。

HA でフェールオーバーする有効な NFS エクスポートを作成するには、エクスポートをアクティブ HA ノードから作成し、フェールオーバー ネットワーク インターフェイス上で一般的に共有する必要があります。

Data Domain システムへの NFS クライアント アクセスの管理

このセクションのトピックでは、NFS クライアントの Data Domain System アクセスの管理方法について説明します。

KB 資料「NFS Best Practices for Data Domain and client OS」（https://support.emc.com/kb/180552）では、NFS のベスト プラクティスに関する追加情報を提供しています。

NFS サービスの有効化

クライアントがシステムにアクセスできるよう、NFS プロトコルを使用して NFS サービスを有効にします。

手順

1. ［**Protocols**］ > ［**NFS**］を選択します。

   ［NFS］ビューが開いて、［Exports］タブが表示されます。

2. ［**Enable**］をクリックします。

NFS サービスの無効化

クライアントがシステムにアクセスできないようにするために、NFS プロトコルを使用して NFS サービスを無効にします。

手順

1. ［**Protocols**］ > ［**NFS**］タブを選択します。

   ［NFS］ビューが開いて、［Exports］タブが表示されます。

2. ［**Disable**］をクリックします。

エクスポートの作成

［NFS］ビューで Data Domain System Manager の［Create］ボタンを使用して、または構成ウィザードを使用して、`/backup`、`/data/col1/backup`、`/ddvar`、`/ddvar/core` 領域、または`/ddvar/ext` 領域（存在する場合）にアクセスできる NFS クライアントを指定します。

Data Domain システムでは、最大 2048 エクスポートまでサポートし [2]、システム メモリに従ったコネクション数のスケーリングもサポートします。

2. ハードウェアの制限による影響を受ける可能性があります。

注

各エクスポートに個別にクライアント アクセスを割り当て、各エクスポートから個別にアクセスを削除する必要があります。例えば、`/ddvar` からクライアントを削除できますが、`/data/col1/backup` へのアクセスはまだ可能です。

⚠ 注意

レプリケーションの実装が予定されている場合、それぞれに別々のディレクトリまたは MTree が使用されている限り、1 つのデスティネーション Data Domain システムは、CIFS クライアントと NFS クライアントの両方からバックアップを受信することができます。同一の領域に CIFS データと NFS データを混在させないでください。

手順

1. ［**Protocols**］ > ［**NFS**］を選択します。

   ［NFS］ビューが開いて、［Exports］タブが表示されます。

2. ［**Create**］をクリックします。
3. ［Directory Path］テキスト ボックスのパス名（`/data/col1/backup/dir1` など）を入力します。

   注

   `col1` には、小文字の L の後に数字の 1 を使います。

4. ［Clients］領域で、他のクライアントを選択するか、プラス（［**+**］）アイコンをクリックしてクライアントを作成します。

   ［Client］ダイアログ ボックスが表示されます。

   a. テキスト ボックスにサーバー名を入力します。

      完全修飾ドメイン名、ホスト名、IP アドレスのいずれかを入力します。アスタリスク（*）1 文字はワイルドカードとして認識され、すべてのバックアップ サーバーがクライアントとして使用されることを示します。

      注

      `/data/col1/backup` ディレクトリへのアクセス権を持つクライアントは、全体ディレクトリにアクセスできます。`/data/col1/backup` のサブディレクトリへのアクセス権を持つクライアントは、そのサブディレクトリにのみアクセス権があります。

      - クライアントは、完全修飾ドメイン ホスト名、IPv4 または IPv6 IP アドレス、ネットマスクまたはプレフィックス長のいずれかを持つ IPv4 アドレス、プレフィックス長を持つ IPv6 アドレス、プレフィックス@または**`*.yourcompany.com`** のようなドメイン名のアスタリスク（**`*`**）ワイルド カードを持つ NIS ネットグループ名のいずれかです。
      - `/data/col1/backup` の下のサブディレクトリに追加されたクライアントは、そのサブディレクトリにのみアクセス権があります。
      - クライアント リストとしてアスタリスク（**`*`**）を入力すると、ネットワーク上のすべてのクライアントにアクセス権が与えられます。

b. クライアント用の NFS オプションのチェックボックスを選択します

全般：

- 読み取り専用権限（ro）。
- 1024 以下のポートからの接続を許可します（secure）（デフォルト）。

匿名 UID/GID：

- UID（ユーザー識別子）または GID（グループ識別子）0 から匿名 UID/GID（root _squash）へのリクエストをマッピングします。
- すべてのユーザー リクエストを匿名 UID/GID（all _squash）に割り当てる
- デフォルトの匿名 UID/GID を使用します。

許可された Kerberos 認証モード：

- 認証されている接続（sec=sys）。認証をしない場合に選択します。
- 認証されている接続（sec=krb5）。

注

整合性とプライバシーがサポートされますが、パフォーマンスが著しく遅くなる可能性があります。

c. [**OK**] をクリックします。

5. [**OK**] をクリックしてエクスポートを作成します。

エクスポートの変更

GUI を使用して、ディレクトリ パス、ドメイン名、その他のオプションを変更します。

手順

1. [**Protocols**] > [**NFS**] を選択します。

   [NFS] ビューが開いて、[Exports] タブが表示されます。

2. [NFS Exports] テーブルでエクスポートのチェックボックスをクリックします。
3. [変更] をクリックします。
4. [Directory Path] テキスト ボックスのパス名を変更します。
5. [Clients] 領域で、他のクライアントを選択するか、鉛筆アイコン（編集）をクリックするか、[**+**] アイコンをクリックして、クライアントを作成します。

   a. [Client] テキスト ボックスにサーバー名を入力します。

   完全修飾ドメイン名、ホスト名、IP アドレスのいずれかを入力します。アスタリスク（*）1 文字はワイルドカードとして認識され、すべてのバックアップ サーバーがクライアントとして使用されることを示します。

   注

   `/data/col1/backup` ディレクトリへのアクセス権を持つクライアントは、全体ディレクトリにアクセスできます。`/data/col1/backup` のサブディレクトリへのアクセス権を持つクライアントは、そのサブディレクトリにのみアクセス権があります。

- クライアントは、完全修飾ドメイン ホスト名、IPv4 または IPv6 IP アドレス、ネットマスクまたはプレフィックス長のいずれかを持つ IPv4 アドレス、プレフィックス長を持つ IPv6 アドレス、プレフィックス@または`*.yourcompany.com` のようなドメイン名のアスタリスク（*）ワイルド カードを持つ NIS ネットグループ名のいずれかです。`/data/col1/backup` の下のサブディレクトリに追加されたクライアントは、そのサブディレクトリにのみアクセス権があります。
- クライアント リストとしてアスタリスク（*）を入力すると、ネットワーク上のすべてのクライアントにアクセス権が与えられます。

b. クライアント用の NFS オプションのチェックボックスを選択します

全般：

- 読み取り専用権限（ro）。
- 1024 以下のポートからの接続を許可します（secure）（デフォルト）。

匿名 UID/GID：

- UID（ユーザー識別子）または GID（グループ識別子）0 から匿名 UID/GID（root _squash）へのリクエストをマッピングします。
- すべてのユーザー リクエストを匿名 UID/GID（all _squash）に割り当てる
- デフォルトの匿名 UID/GID を使用します。

許可された Kerberos 認証モード：

- 認証されている接続（sec=sys）。認証をしない場合に選択します。
- 認証されている接続（sec=krb5）。

注

Integrity と Privacy に対応していません。

c. [**OK**] をクリックします。

6. エクスポートを変更するには、[**OK**] をクリックします。

既存のエクスポートからのエクスポートの作成

既存のエクスポートからエクスポートを作成し、必要に応じて変更します。

手順

1. [NFS Exports] タブでは、ソースとして使用するエクスポートのチェックボックスをクリックします。
2. [**Create From**] をクリックします。
3. エクスポートの変更に関するセクションで示すとおり、エクスポート情報を変更します。

エクスポートの削除

[NFS Exports] タブからエクスポートを削除します。

手順

1. [NFS Exports] タブで、削除したいエクスポートのチェックボックスをクリックします。

2. ［**Delete**］をクリックします。
3. ［**OK**］と［**Close**］をクリックして、エクスポートを削除します。

NFS 情報の表示

このセクションのトピックでは、DD System Manager を使用して NFS クライアント ステータスと NFS 構成を監視する方法について説明します。

NFS ステータスの表示

NFS がアクティブかどうか、Kerberos が有効かどうかが表示されます。

手順

- ［**Protocols**］ > ［**NFS**］をクリックします。

  トップ パネルには、NFS の動作ステータス（NFS が現在アクティブで実行中かどうか、Kerberos モードが有効かどうか、など）が表示されます。

  注

  ［Configure］をクリックして、［**Administration**］ > ［**Access**］ > ［**Authentication**］タブを表示します。ここでは、Kerberos 認証を構成できます。

NFS エクスポートの表示

Data Domain システムへのアクセスを許可されたクライアントのリストが表示されます。

手順

1. ［**Protocols**］ > ［**NFS**］をクリックします。

   ［Exports］ビューに、Data Domain System 用に構成された NFS エクスポートのテーブルおよび各エクスポートのマウント パス、ステータス、NFS オプションが表示されます。

2. テーブルでエクスポートをクリックして、［Exports］テーブルの下の［Detailed Information］領域に記入します。

   システムは、そのエクスポートのディレクトリ パス、構成済みのオプション、ステータスに加え、クライアントのリストも表示します。

   ［Filter By］テキスト ボックスを使用して、マウント パスでソートします。

   ［**Update**］をクリックすると、システムがテーブルを更新し、提供されたフィルターを使用します。

   ［**Reset**］をクリックすると、システムが Path および Client フィルターをクリアします。

アクティブな NFS クライアントの表示

過去 15 分間に接続されたすべてのクライアントと各クライアントのマウント パスが表示されます。

手順

- ［**Protocols**］ > ［**NFS**］ > ［**Active Clients**］タブを選択します。

  過去 15 分に接続されたすべてのクライアントとそのマウント パスが表示される［Active Clients］ビューが表示されます。

［Filter By］テキスト ボックスを使用して、マウント パスとクライアント名でソートします。

［**Update**］をクリックすると、システムがテーブルを更新し、提供されたフィルターを使用します。

［**Reset**］をクリックすると、システムが Path および Client フィルターをクリアします。

Kerberos ドメインへの DDR の統合

DDR のドメイン名、ホスト名、DNS サーバーを設定します。

DDR は認証サーバーを Key Distribution Center（UNIX 用）および Distribution Center（Windows Active Directory 用）として使用できるようになります。

⚠ 注意

この説明で示す例は、この演習の作成に使用されたオペレーティング システム（OS）に固有のものです。OS 固有のコマンドを使用する必要があります。

注

UNIX Kerberos モードでは、キータブ ファイルをそれが生成された KDC（キー配布センター）から DDR に転送する必要があります。複数の DDR を使用している場合、各 DDR に別々のキータブ ファイルが必要です。キータブ ファイルには、KDC サーバと DDR 間の共有シークレットが含まれます。

注

UNIX KDC を使用している場合、DNS サーバーは KDC サーバーである必要はなく、別のサーバーでも構いません。

手順

1. DDR コマンドを使用して、DDR のホスト名とドメイン名を設定します。

   ```
   net set hostname <host>
   net set {domainname <local-domain-name>}
   ```

   注

   ホスト名は DDR の名前です。

2. KDC（キー配布センター）で DDR の NFS プリンシパル（ノード）を構成します。

   例：

   ```
   addprinc nfs/hostname@realm
   ```

   注

   ホスト名は DDR の名前です。

3. KDC でプリンシパルとして追加された nfs エントリーがあることを確認します。

   例：

   ```
   listprincs
   nfs/hostname@realm
   ```

4. DDR プリンシパルをキータブ ファイルに追加します。

   例：
   ktadd <keytab_file> nfs/hostname@realm

5. KDC で構成された nfs キータブ ファイルがあることを確認します。

   例：
   klist -k <keytab_file>

   注

   <keytab_file>は、前のステップでキーの構成に使用したキータブ ファイルです。

6. NFS DDR のキーが生成された場所から/ddvar/ディレクトリ内の DDR にキータブ ファイルをコピーします。

   表 117 キータブ デスティネーション

ファイルのコピー元	ファイルのコピー先
<keytab_file>（前のステップで構成されたキータブ ファイル）。	/ddvar/

7. 次の DDR コマンドを使用して、DDR 上のレルムを設定します。

   authentication kerberos set realm <home realm> kdc-type <unix, windows.> kdcs <IP address of server>

8. kdc-type が UNIX である場合、キータブ ファイルを/ddvar/から/ddr/etc/（Kerberos 構成ファイルで設定されている）にインポートします。次の DDR コマンドを使用して、ファイルをコピーします。

   authentication kerberos keytab import

   通知

   このステップは、kdc-type が UNIX である場合にのみ必要となります。

   Kerberos セットアップが完了しました。

9. NFS マウント ポイントを追加して Kerberos を使用するには、nfs add コマンドを使用します。

   詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

10. KDC（キー配布センター）で各 NFS クライアントのホスト、NFS、関連ユーザー プリンシパルを追加します。

    例：**listprincs**

    ```
    host/hostname@realm
    nfs/hostname@realm
    root/hostname@realm
    ```

11. 各 NFS クライアントで、そのプリンシパルをすべて、クライアント上のキータブ ファイルにインポートします。

    例：
    ktadd -k <keytab_file> host/hostname@realm

```
ktadd -k <keytab_file> nfs/hostname@realm
```

初期構成後の KDC サーバーの追加と削除

DDR を Kerberos ドメインに統合して、DDR が認証サーバーを Key Distribution Center（UNIX 用）および Distribution Center（Windows Active Directory 用）として使用できるようにすると、次の手順で KDC サーバーを追加または削除できます。

手順

1. DDR を Windows AD（Active Directory）サーバーまたは UNIX KDC（Key Distribution Center）に参加させます。

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   例： **authentication kerberos set realm krb5.test kdc-type unix kdcs nfskrb-kdc.krb5.test**

   このコマンドを実行すると、システムが krb5.test realm に参加し、NFS クライアントの Kerberos 認証が有効化されます。

   注

   Kerberos を使用して認証を行うには、この KDC で生成されたキー タブが DDR 上に存在している必要があります。

2. Kerberos 認証構成を確認します。

   authentication kerberos show config

   ```
   Home Realm:           krb5.test
   KDC List:             nfskrb-kdc.krb5.test
   KDC Type:             unix
   ```

3. 2 台目の KDC サーバーを追加します。

   authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}

   例： **authentication kerberos set realm krb5.test kdc-type unix kdcs ostqa-sparc2.krb5.test nfskrb-kdc.krb5.test**

   注

   Kerberos を使用して認証を行うには、この KDC で生成されたキー タブが DDR 上に存在している必要があります。

4. 2 台の KDC サーバーが存在していることを確認します。

   authentication kerberos show config

   ```
   Home Realm:           krb5.test
   KDC List:             ostqa-sparc2.krb5.test, nfskrb-
   kdc.krb5.test
   KDC Type:             unix
   ```

5. Kerberos 構成キーの値を表示します。

   reg show config.keberos

   ```
   config.kerberos.home_realm = krb5.test
   config.kerberos.home_realm.kdc1 = ostqa-sparc2.krb5.test
   ```

```
config.kerberos.home_realm.kdc2 = nfskrb-kdc.krb5.test
config.kerberos.kdc_count = 2
config.kerberos.kdc_type = unix
```

6. KDC サーバーを削除します。

   削除したい KDC サーバーをリストせずに、**authentication kerberos set realm <home-realm> kdc-type {windows [kdcs <kdc-list>] | unix kdcs <kdc-list>}**コマンドを使用して、KDC サーバーを削除します。たとえば、既存の KDC サーバーが kdc1、kdc2、kdc3 であり、kdc2 をレルムから削除したい場合、次のコマンドを実行します。

   authentication kerberos set realm <realm-name> kdc-type <kdc_type> kdcs kdc1,kdc3

第 10 章

NFSv4

本章には、次のセクションが含まれます。

- NFSv4 の概要 278
- ID マッピングの概要 279
- 外部フォーマット 279
- 内部識別子のフォーマット 280
- ID マッピングが発生するタイミング 281
- NFSv4 と CIFS/SMB の相互運用性 282
- NFS 参照 283
- NFSv4 と高可用性 285
- NFSv4 グローバル ネームスペース 285
- NFSv4 構成 286
- Kerberos と NFSv4 287
- Active Directory の有効化 290

NFSv4 の概要

NFS クライアントのデフォルト NFS プロトコル レベルに NFSv4.x が使われることが増えてきたため、Data Domain システムではクライアントに対して下位互換性モードでの動作を要求する代わりに、NFSv4 を採用できるようになりました。

Data Domain システムでは、NFSv4 と NFSv3 が同じ NFS エクスポートにアクセスできる必要のある混在環境でクライアントを動作させることが可能です。

Data Domain NFS サーバは、サイトの要件次第で NFSv4 および NFSv3 をサポートするように構成できます。各 NFS エクスポートに対して、NFSv3 クライアントでのみ利用可能、NFSv4 クライアントでのみ利用可能、または両方の環境で利用可能となるように設定できます。

NFSv4 と NFSv3 のどちらを選択するかには、いくつかの要因が影響します。

- NFS クライアントのサポート
  NFS クライアントのなかには、NFSv3 のみをサポートするもの、NFSv4 のみをサポートするもの、あるいはいずれか 1 つのバージョンにより最適化されたものがあります。
- 運用上の要件
  企業は、NFSv4 と NFSv3 のどちらを使用するかを厳密に標準化する場合があります。
- セキュリティ
  強固なセキュリティが必要な場合、NFSv4 は NFSv3 よりも高度なセキュリティ レベルを提供します。これには ACL や拡張オーナーおよびグループ構成が含まれます。
- 機能要件
  バイト範囲ロックまたは utf-8 ファイルが必要な場合は、NFSv4 を選択してください。
- NFSv3 サブマウント
  既存の構成で NFSv3 サブマウントを使用している場合、NFSv3 が適している可能性があります。

Data Domain システムでの NFSv3 と NFSv4 の比較

NFSv4 は、NFSv3 に比べて高度な機能や特徴を提供します。

次の表では、NFSv4 と NFSv3 の機能を比較します。

表 118 NFSv4 と NFSv3 の比較

機能	NFSv3	NFSv4
標準に基づくネットワーク ファイルシステム	可	可
Kerberos のサポート	可	可
Kerberos と LDAP	可	可
クォータのレポート作成	可	可
クライアント ベースのアクセス リストによる複数のエクスポート	可	可
ID マッピング	可	可
Utf-8 文字のサポート	×	可
ファイル/ディレクトリ ベースの ACL（アクセス制御リスト）	×	可
オーナー/グループの拡張（OWNER@）	×	可

表 118 NFSv4 と NFSv3 の比較 （続き）

機能	NFSv3	NFSv4
ファイルの共有ロック	×	可
バイト範囲ロック	×	可
DD CIFS 統合（ロック、ACL、AD）	×	可
ステートフルなファイルのオープンと復旧	×	可
グローバル ネームスペースと pseudoFS	×	可
参照によるマルチ システム ネームスペース	×	可

NFSv4 ポート

NFSv4 と NFSv3 は個別にの有効または無効にできます。さらに、NFS のバージョンを異なるポートに移動できます。両方のバージョンで同じポートを使用する必要はありません。

NFSv4 では、ポートを変更する場合の Data Domain ファイル システムの再起動は必要ありません。次の場合にのみ NFS の再起動が必要です。

NFSv3 同様、NFSv4 がデフォルトのポート番号 2049 で実行されており、かつ有効な場合。

NFSv4 でポートマッパー（ポート番号 111）または mountd（ポート番号 2052）を使用しない場合。

ID マッピングの概要

NFSv4 は、`joe@example.com` などの一般的な外部フォーマットによってオーナーとグループを識別します。これらの一般的なフォーマットは識別子、または ID と呼ばれます。

識別子は NFS サーバに格納され、ID 12345 や ID S-123-33-667-2 といった内部表現を使用します。内部識別子と外部識別子の間の変換は ID マッピングと呼ばれます。

識別子は、次のように関連づけられます。

- ファイルやディレクトリのオーナー
- ファイルやディレクトリのオーナー グループ
- ACL（アクセス制御リスト）のエントリー

Data Domain システムは NFS と CIFS/SMB プロトコルで共通の内部フォーマットを使用します。このため、ファイルとディレクトリを NFS と CIFS/SMB の間で共有できます。各プロトコルは、独自の ID マッピングを使用して内部フォーマットを外部フォーマットに変換します。

外部フォーマット

NFSv4 識別子の外部フォーマットは NFSv4 標準（たとえば、RFC-7530 for NFSv4.0）に従います。さらに、相互運用性のために補足的な形式もサポートされます。

標準の識別子フォーマット

NFSv4 の標準外部識別子は `identifier@domain` のようなフォーマットを持ちます。この識別子は NFSv4 のオーナー、オーナー グループ、および ACE（アクセス制御エントリ）に使用されま

す。ドメインは、nfs option のコマンドで使用するよう設定された構成済み NFSv4 ドメインと一致する必要があります。

次の CLI の例では Data Domain NFS サーバとして、NFSv4 ドメインを mycorp.com に設定しています。

```
nfs option set nfs4-domain mycorp.com
```

クライアントに NFS ドメインを設定するには、お手持ちのクライアント固有のドキュメントを参照してください。オペレーティング システムによっては、構成ファイルの更新（たとえば、/etc/idmapd.conf）や、クライアント管理ツールの使用が必要な場合があります。

注

既定値が設定されていない場合は、Data Domain システムの DNS 名に従います。

注

nfs4-domain の DNS ドメインが自動更新するよう変更したあとは、ファイル システムを再起動する必要があります。

ACE 識別子の拡張

ACL ACE エントリーでは、NFSv4 RFC で定義された次の標準的な NFSv4 ACE 拡張識別子を、Data Domain NFS サーバでもサポートします。

- OWNER@。ファイルまたはディレクトリの現在の所有者。
- GROUP@。ファイルまたはディレクトリの現在のオーナー グループ。
- INTERACTIVE@、NETWORK@、DIALUP@、BATCH@、ANONYMOUS@、AUTHENTICATED@、SERVICE@といった特殊識別子。

代替フォーマット

相互運用を可能にするために、Data Domain システムの NFSv4 サーバでは、入力と出力の代替の識別子フォーマットをいくつかサポートします。

- 数値識別子。たとえば、「12345」。
- 「S-NNN-NNN-...」の形式で表現される Windows 互換の SID（セキュリティ識別子）。

これらのフォーマットの制限に関する詳細については、入力マッピングおよび出力マッピングの章を参照してください。

内部識別子のフォーマット

Data Domain ファイルシステムは、ファイルシステムの各オブジェクト（ファイルまたはディレクトリ）と識別子を格納します。すべてのオブジェクトは、UID（ユーザ ID）と GID（グループ ID）を数値で持ちます。一連のモード ビットに加えてこれらの値を使用して、伝統的な UNIX/Linux の識別とアクセス制御を可能にします。

CIFS/SMB プロトコルまたは NFSv4 プロトコル（NFSv4 の ACL が有効な場合）で作成されたオブジェクトには、拡張 SD（セキュリティ記述子）も付与されます。各 SD には次の情報が含まれます。

- オーナー SID（セキュリティ識別子）
- オーナー グループ SID

- DACL（随意アクセス制御リスト）
- （省略可能）SACL（システム ACL）

各 SID には、Windows SID に同様の方法での、RID（相対 ID）と異なるドメインが含まれています。SID と SID のマップングの詳細については、NFSv4 と CIFS の相互運用性に関するセクションを参照してください。

ID マッピングが発生するタイミング

Data Domain NFSv4 サーバでは、次の状況でマッピングを実行します。

- 入力のマッピング
  データ ドメイン NFS サーバは、NFSv4 クライアントから識別子を受信します。インプット マッピング（281 ページ）を参照してください。
- 出力のマッピング
  Data Domain NFS サーバから NFSv4 クライアントに識別子が送信されます。出力のマッピング（281 ページ）を参照してください。
- 資格情報のマッピング
  RPC クライアントの資格情報は、アクセス制御とその他の操作の内部 ID にマップされます。資格情報のマッピング（282 ページ）を参照してください。

インプット マッピング

インプット マッピングは、NFSv4 クライアントが Data Domain NFSv4 サーバに対して識別子を送信する際に発生します。たとえば、ファイルのオーナーまたはオーナー グループを設定するときが該当します。インプット マッピングは資格情報マッピングとは異なります。資格情報マッピングの詳細については、xxxx を参照してください。

`joe@mycorp.com` などの標準フォーマットの識別子は、構成済みの変換ルールに基づいて内部 UID/GID に変換されます。NFSv4 ACL が有効な場合は、構成済みの変換ルールに基づいて SID も生成されます。

数値識別子（「12345」など）は、クライアントが Kerberos 認証を使用していない場合、対応する UID/GID に直接変換されます。Kerberos を使用している場合は、NFSv4 スタンダードの推奨に従ってエラーが生成されます。NFSv4 ACL が有効の場合は、変換規則に基づいて SID が生成されます。

Windows SID（たとえば、「S-NNN-NNN-...」）は検証され、対応する SID に直接変換されます。UID/GID は、変換規則に基づいて生成されます。

出力のマッピング

NFSv4 サーバが NFSv4 クライアントに識別子を送信するときは出力マッピングが発生します。たとえば、サーバがファイルのオーナーまたはオーナー グループを返す場合などです。

1. 設定によっては、出力は数値 ID になります。
   これは、ID マッピングの構成がなされていない NFSv4 クライアント（たとえば、いくつかの Linux クライアントなど）で有用です。
2. 構成済みのマッピング サービス（たとえば、NIS または Active Directory）を使用してマッピングを試行します。
3. マッピングが失敗し、かつ構成が許可されている場合、出力は ID の数値または SID の文字列になります。
4. それ以外の場合は、何も返されません。

`nfs option nfs4-idmap-out-numeric` で出力マッピングを構成します。

- **nfs option nfs4-idmap-out-numeric** が **map-first** に設定されていると、マッピングが試行されます。エラーの場合は、許可されていれば数の文字列が出力されます。これはデフォルト設定です。
- **nfs option nfs4-idmap-out-numeric** が **always** に設定されていると、出力は許可されている場合は常に数の文字列になります。
- **nfs option nfs4-idmap-out-numeric** が **never** に設定されていると、マッピングが試行されます。エラーの場合は、**nobody@nfs4-domain** が出力されます。
  RPC 接続で GSS/Kerberos を使用する場合は、数値形式の文字列は許可されないため **nobody@nfs4-domain** が出力されます。

次の例では、常に数の文字列の出力を試みるように Data Domain NFS サーバを構成します。Kerberos では nobody が返されます。

```
nfs option set nfs4-idmap-out-numeric always
```

資格情報のマッピング

NFSv4 サーバでは、NFSv4 クライアントの資格情報を提供します。

これらの資格情報は次の機能に影響します。

- 操作のアクセス ポリシーの決定。たとえば、ファイルを読み取る能力。
- 新しいファイルとディレクトリのデフォルト オーナーおよびオーナー グループの決定。

クライアントから送信される資格情報は `john_doe@mycorp.com` であるか、あるいは `UID=1000, GID=2000` のようなシステム資格情報であることがあります。システム資格情報は補助グループ ID のほか、UID/GID を指定します。

NFSv4 ACL を無効にした場合は、UID/GID と補助グループ ID が資格情報として使用されます。

NFSv4 の ACL を有効にすると、構成済みマッピングサービスを用いて資格情報の拡張セキュリティ記述子が構築されます。

- オーナー、オーナー グループ、補助グループの SID は、SD（セキュリティ記述子）にマップおよび追加されます。
- 資格情報の権限がある場合は SD に追加されます。

NFSv4 と CIFS/SMB の相互運用性

NFSv4 と CIFS で使用するセキュリティ記述子は違いがあるものの、ID マッピングの観点から似ています。

相互運用性を最適化するためには以下に注意する必要があります。

- Active Directory では CIFS と NFSv4 の両方に対して構成する必要があります。また、ID マッピングに Active Directory を使用するように NFS ID マッパーを構成する必要があります。
- CIFS ACL を広範囲にわたって使用している場合は、NFSv4 ACL を有効化すると相互運用性を向上できます。
  - NFSv4 ACL を有効化することで、DACL のアクセスを評価する際に、NFSv4 の資格情報が適切な SID にマップできます。
- CIFS サーバは、デフォルトの ACL とユーザー権限を含む資格情報を CIFS クライアントから受信します。

- 対照的に、NFSv4 サーバでは、資格情報の限られたセットを受信し、その ID マッパーを使用して実行時に資格情報を構築します。このため、ファイルシステムが別の資格情報を参照することがあります。

CIFS/SMB Active Directory の統合

Data Domain NFSv4 サーバは、Data Domain CIFS サーバで設定されている Windows Active Directory の構成を使用して構成できます。

Data Domain システムは、可能な場合は Active Directory を使用してマップされます。この機能はデフォルトで無効になっていますが、次のコマンドで有効化できます。

```
nfs option set nfs4-idmap-active-directory enabled
```

NFSv4 のデフォルト DACL

NFSv4 では、CIFS が提供するデフォルト DACL（discretionary access control list）とは異なるデフォルト DACL を設定します。

デフォルトの NFSv4 DACL では OWNER@、GROUP@、および EVERYONE@のみ定義されます。ACL 継承を使用すると、適切な場合は CIFS で重要な ACE をデフォルトで追加できます。

System Defaults SID

NFSv3、および ACL のない NFSv4 で作成されたファイルとディレクトリは、デフォルトのシステム ドメイン（デフォルトの UNIX ドメインと呼ばれることもあります）を使用します。

- システム ドメインのユーザー SID にはフォーマット `S-1-22-1-N` があります。ここで N は UID です。
- システム ドメインのグループ SID にはフォーマット `S-1-22-2-N` があります。ここで N は GID です。
  たとえば、`UID 1234` のユーザーの所有者 SID は `S-1-22-1-1234` です。

NFSv4 ACL と SID の共通識別子

NFSv4 ACL の EVERYONE@識別子、およびその他の特殊な識別子（たとえば、BATCH@など）と同等の CIFS SID を使用し、互換性があります。

OWNER@と GROUP@識別子に直接対応する識別子は CIFS にありません。これらはファイルまたはディレクトリの現在の現在の所有者およびオーナー グループとして表示されます。

NFS 参照

参照機能により、NFSv4 から 1 つまたは複数の場所に存在するエクスポート（またはファイルシステム）にアクセスできます。同一 NFS サーバまたは異なる NFS サーバを参照可能で、エクスポートの参照には同一パスまたは異なるパスが使用できます。

参照は NFSv4 の機能であるため、NFSv4 マウントにのみ適用されます。

参照は NFSv4 以降を使用する任意のサーバで作成可能であり、次のサーバでも作成可能です。

- NFSv4 を有効にした NFS を実行する Data Domain システム
- Linux サーバ、NAS アプライアンス、VNX システムなどの、NFSv4 をサポートするその他のサーバ。

参照では、Data Domain ファイルシステムのカレント パスを使用するか否かによらず、NFS のエクスポート ポイントを使用できます。

参照付きの NFS エクスポートは NSFv3 経由でもマウントできますが、参照は NFSv4 の機能であるため、NFSv3 のクライアントはリダイレクトされません。この特徴は、エクスポートのリダイレクト許可をスケール アウト システムのファイル管理レベルで行う際に有用です。

参照のロケーション

NFSv4 の参照は常に 1 つ以上のロケーションを持ちます。

これらのロケーションは、次の要素で構成されます。

- 参照先ファイルシステムへのリモート NFS サーバ上のパス。
- クライアントからリモートの NFS サーバに到達可能な 1 つ以上のサーバ ネットワーク アドレス。

通常、複数のサーバ アドレスが同じロケーションに関連づけられる場合、それらのアドレスは同じ NFS サーバ上にあります。

参照のロケーション名

NFS エクスポート内の各参照のロケーションに名前を付けることができます。名前を使用して、参照へのアクセス、変更または削除ができます。

参照名は次の文字セットから最大 80 文字まで含めることができます。

- a～z
- A～Z
- 0～9
- "."
- ","
- "_"
- "-"

注

名前に埋め込む形でスペースを含めることもできます。埋め込みスペースを使用する場合は、二重引用符で名前全体を囲む必要があります。

「.」で始まる名前は Data Domain システムが自動作成するために予約されています。これらの名前は削除できますが、CLI（コマンド ライン インタフェース）または SMS（システム管理サービス）を使用して作成や変更することはできません。

参照とスケール アウト システム

Data Domain システムをスケール アウトする際、NFSv4 の参照とロケーションによりアクセスが向上することがあります。

Data Domain システムにグローバル ネームスペースが含まれる場合と含まれない場合があるため、次の 2 つのシナリオを用いて NFSv4 の参照の使用法を説明します。

- Data Domain システムにはグローバル ネームスペースが含まれません。
  - NFSv4 の参照を使用して、グローバルな名前空間を構築します。システム管理者は、これらのグローバル ネームスペースを作成することも、SM（スマート システム マネージャ）を使用して参照を構築することもできます。
- Data Domain システムにはグローバル名前空間がすでに存在します。

- 特定ノードに配置された MTree を伴うグローバル ネームスペースがシステムに存在する場合、スケールアウト システムに追加されたノードに MTree へのアクセスをリダイレクトするような NFS 参照を作成できます。必要な SM または FM（ファイル マネージャ）情報が利用可能であれば、これらの参照を作成したり、あるいは NFS 内で自動的に参照されるようにすることが可能です。
  MTree の詳細については、「Data Domain Operating System 管理ガイド」を参照してください。

NFSv4 と高可用性

NFSv4 では、HA（高可用性）設定の場合、プロトコルのエクスポート（たとえば、/data/col1/<mtree>）はミラーリングされます。ただし、/ddvar のような構成のエクスポートはミラーリングされません。

/ddvar ファイルシステムは HA ペアの各ノードで一意です。その結果、 /ddvar のエクスポートおよび関連するクライアント アクセス リストは HA 環境のスタンバイ ノードにミラーリングされません。

アクティブ ノードがスタンバイ ノードにフェールオーバーすると、/ddvar の情報は古くなります。オリジナルのアクティブ ノードの/ddvar に付与されたクライアントのあらゆるアクセス許可は、フェールオーバー後の新しいアクティブ ノードで再作成する必要があります。

オリジアンルのアクティブ ノードで作成された追加の/ddvar エクスポートとそのクライアント（たとえば、/ddvar/core）も、フェールオーバー後の新しいアクティブ ノードでの追加が必要です

最後に、すべての/ddvar エクスポートはフェールオーバー後にクライアントからアンマウントし、再マウントする必要があります。

NFSv4 グローバル ネームスペース

NFSv4 サーバでは、NFS エクスポートを検索可能なパスのセットに接続するために、疑似ファイル システム（PseudoFS）として知られている仮想ディレクトリ ツリーを提供しています。

疑似ファイル システム（PseudoFS）を使用するという点で、NFSv4 は、補助的 mountd プロトコルを使用する NFSv3 とは異なっています。

ほとんどの構成では、NFSv3 mountd から NFSv4 グローバル ネームスペースへの変更は透過的で、NFSv4 クライアントおよびサーバによって自動的に処理されます。

NFSv4 グローバル ネームスペースと NFSv3 サブマウント

NFSv3 エクスポート サブマウントを使用すると、NFSv4 のグローバル ネームスペースの機能により、NFSv4 マウントからサブマウントが参照できなくなる可能性があります。

例 1 NFSv3 のメイン エクスポートとサブマウント エクスポート

NFSv3 にメイン エクスポートとサブマウント エクスポートがある場合、これらのエクスポートで同じ NFSv3 クライアントを異なるアクセス レベルで使用する可能性があります。

表 119 NFSv3 のメイン エクスポートとサブマウント エクスポート

エクスポート	パス	クライアント	オプション
Mt1	/data/col1/mt1	client1.example.com	ro

例 1 NFSv3 のメイン エクスポートとサブマウント エクスポート （続き）

表 119 NFSv3 のメイン エクスポートとサブマウント エクスポート （続き）

エクスポート	パス	クライアント	オプション
Mt1-sub	/data/col1/mt1/subdir	client1.example.com	rw

前の表では、次の要素が NFSv3 に適用されます。

- client1.example.com が/data/col1/mt1 をマウントする場合、クライアントは読み取り専用アクセスを取得します。
- client1.example.com が/data/col1/mt1/subdir をマウントする場合、クライアントは読み取り/書き込みアクセスを取得します。

NFSv4 は、最上位のエクスポート パスに関しては同様に動作します。NFSv4 では、最上位のエクスポート パス（/data/col1/mt1）に到達するまで、client1.example.com は NFSv4 PseudoFS をナビゲートし、読み取り専用アクセスを取得します。

ただし、エクスポートが選択されているため、サブマウント エクスポート（Mt1-sub）はクライアントの PseudoFS の一部にはならず、読み取り/書き込みアクセス権が与えられません。

ベスト プラクティス
システムで NFSv3 エクスポート サブマウントを使用して、マウント パスに基づいてクライアントに読み取り/書き込みアクセスを与えている場合、NFSv4 のサブマウント エクスポートを使用する前にこのことを考慮する必要があります。

NFSv4 では、個々のクライアントがそれぞれ異なる PseudoFS を持ちます。

表 120 NFSv3 サブマウント エクスポート

エクスポート	パス	クライアント	オプション
Mt1	/data/col1/mt1	client1.example.com	ro
Mt1-sub	/data/col1/mt1/subdir	client2.example.com	rw

NFSv4 構成

デフォルト Data Domain システム構成は NFSv3 のみ有効です。NFSv4 を使用するには、はじめに NFSv4 サーバを有効化する必要があります。

NFSv4 サーバの有効化

手順

1. nfs enable version 4 を入力して NFSv4 を有効にします。

```
# nfs enable version 4
NFS server version(s) 3:4 enabled.
```

2. （省略可能）NFSv3 を無効にする場合は、`nfs disable version 3` を入力します。

```
# nfs disable version 3
NFS server version(s) 3 disabled.
NFS server version(s) 4 enabled.
```

必要条件

NFSv4 サーバを有効にしたあとで、サイト用の追加の NFS 構成タスクを実行することが必要になる場合があります。これらのタスクには、Data Domain システムで行う次の操作を含めることができます。

- NFSv4 ドメインの設定
- NFSv4 ID マッピングの構成
- ACL（アクセス制御リスト）の構成

NFSv4 を含めるデフォルト サーバ設定

Data Domain NFS コマンドのオプションである **`default-server-version`** は、バージョンを指定せずに `nfs enable` コマンドを実行した際に有効化される NFS のバージョンを制御します。

手順

1. 次の `nfs option set default-server-version 3:4` コマンドを入力します。

```
# nfs option set default-server-version 3:4
NFS option 'default-server-version' set to '3:4'.
```

既存のエクスポートの更新

既存のエクスポートを更新して Data Domain システムで使用する NFS バージョンを変更することができます。

手順

1. 次のコマンドを入力します。`nfs export modify all`

```
# nfs export modify all clients all options version=ビルド番号
```

既存のすべてのクライアントがバージョン 3 か 4、またはその両方をサポートするよう、NFS のバージョンを適切な文字列に変更できます。次の例では、バージョン 3 と 4 を含むように NFS を変更します。

```
#nfs export modify all clients all options version=3:4
```

`nfs export` コマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

Kerberos と NFSv4

NFSv4 と NFSv3 はどちらも、ユーザー資格情報の保護に Kerberos 認証メカニズムを使用します。

Kerberos は NFS パケットからユーザー資格情報がスプーフィングされるのを防ぎ、データ ドメイン システムに向かう途中の改ざんから保護します。

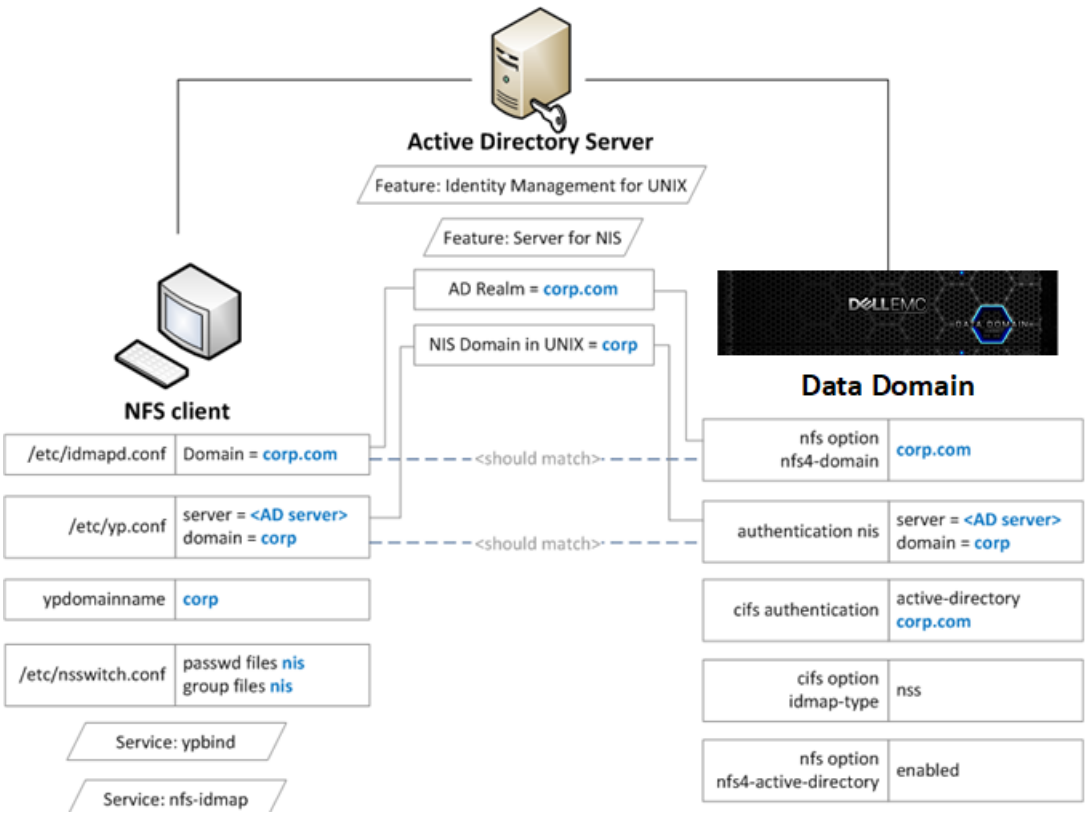
NFS の Kerberos には次の種類があります。

- Kerberos 5（`sec = krb5`）
  ユーザー資格情報に Kerberos を使用します。
- Kerberos 5 with integrity（`sec=krb5i`）
  Kerberos を使用するとともに、暗号化されたチェックサムを使用して NFS ペイロードの整合性をチェックします。
- Kerberos 5 with security（`sec=krb5p`）
  Kerberos 5 integrity を使用するとともに、NFS ペイロード全体を暗号化します。

注

NFS クライアントとデータ ドメイン システムの両方の処理で追加のオーバーヘッドが発生するため、`krb5i` と `krb5p` はどちらもパフォーマンスの低下を招く可能性があります。

図 9 Active Directory 構成



Kerberos を使用するようシステムを構成する際は、NFSv3 でも使用可能な既存のコマンドを使用します。詳細については「データ ドメイン コマンド リファレンス ガイド」の NFSv3 の項目を参照してください。

Linux ベースの KDC における Kerberos の構成

はじめに

すべてのシステムが KDC（キー配布センター）にアクセスできることを確認する必要があります。

システムで KDC に到達できない場合は、DNS（ドメイン ネーム システム）設定を確認してください。

クライアントと Data Domain システムのキータブ ファイルの作成は次の手順で行います。

- 手順 1～3 で Data Domain システムの keytab ファイルを作成します。
- 手順 4～5 でクライアントの keytab ファイルを作成します。

手順

1. **nfs/<ddr_dns_name>@<realm>**サービス プリンシパルを作成します。

```
kadmin.local: addprinc -randkey nfs/ddr12345.<domain-
name>@<domain-name>
```

2. **nfs/<ddr_dns_name>@<realm>**を keytab ファイルにエクスポートします。

```
kadmin.local: ktadd -k /tmp/ddr.keytab nfs/
ddr12345.corp.com@CORP.COM
```

3. キータブ ファイルを Data Domain システムの以下の場所にコピーします。

```
/ddr/var/krb5.keytab
```

4. 次のいずれかのプリンシパルをクライアント向けに作成して、そのプリンシパルを keytab ファイルにエクスポートします。

```
nfs/<client_dns_name>@<REALM>
root/<client_dns_name>@<REALM>
```

5. キータブ ファイルを次の場所からクライアントにコピーします。

```
/etc/krb5.keytab
```

注

すべてのエンティティの時間を同期させるために、NTP サーバを使用することをお勧めします。

Kerberos 認証を使用する Data Domain システムの構成

手順

1. コマンド `authentication` を使用して、Data DOmain システムの KDC と Kerberos レルムを構成します。

```
# authentication kerberos set realm <レルム> kdc-type unix kdcs
<kdc-server>
```

2. キータブ ファイルをインポートします。

```
# authentication kerberos keytab import
```

3. （省略可能）次のコマンドを入力して、NIS サーバを構成します。

```
# authentication nis servers add <server>
# authentication nis domain set <domain-name>
# authentication nis enable
# filesys restart
```

4. （省略可能）コマンド `nfs option` を使用して、**nfs4-domain** を Kerberos レルムと等しくします。

```
nfs option set nfs4-domain <kerberos-realm>
```

5. コマンド `nfs export add` に **sec = krb5** を追加して、既存のエクスポートにクライアントを追加します。

```
nfs export add <export-name> clients * options
version=4,sec=krb5
```

クライアントの構成

手順

1. DNS サーバを構成し、前方および逆引き参照が動作していることを確認します。
2. `/etc/krb5.conf` 構成ファイルを設定して KDC および Kerberos レルムを構成します。

   使用しているクライアント オペレーティング システムに基づいてこの手順を実行する必要があります。
3. NIS またはその他の外部ネーム マッピング サービスを構成します。
4. （省略可能）`/etc/idmapd.conf` ファイルを編集して、Kerberos レルムと等しくなることを確認します。

   使用しているクライアント オペレーティング システムに基づいてこの手順を実行する必要があります。
5. keytab ファイル **/etc/krb5.keytab** に **nfs/**サービス プリンシパルまたは **root/**プリンシパルのエントリーが含まれることを確認します。

```
[root@fc22 ~]# klist -k
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
----
-------------------------------------------------------------------
----------
3 nfs/fc22.domain-name@domain-name
```

6. **sec = krb5** オプションを使用してエクスポートをマウントします。

```
[root@fc22 ~]# mount ddr12345.<domain-name>:/data/col1/
mtree1 /mnt/nfs4 -o sec=krb5,vers=4
```

Active Directory の有効化

Active Directory 認証を構成すると、Data Domain システムが Windows Active Directory レルムの一部になります。CIFS クライアントと NFS クライアントは Kerberos 認証を使用します。

手順

1. コマンド `cifs set` を使用して、アクティブ ディレクトリの領域を結合します。

```
# cifs set authentication active-directory <レルム>
```

   Kerberos は、Data Domain システムに自動的に設定されます。必要な nfs/サービス プリンシパルが KDC 上に自動的に作成されます。
2. コマンド `authentication nis` を使用して NIS を構成します。

```
# authentication nis servers add <windows-ad-server>
# authentication nis domain set <ad-realm>
# authentication nis enable
```

3. コマンド `cifs` を使用して、ID マッピングに NSS を使用するよう CIFS を構成します。

```
# cifs disable
# cifs option set idmap-type nss
# cifs enable
# filesys restart
```

4. **`nfs4-domain`** を設定して、Active Directory レルムと設定を等しくします。

```
# nfs option set nfs4-domain <ad-realm>
```

5. コマンド `nfs` を使用して、NFSv4 の ID マッピングで Active Directory を有効にします。

```
# nfs option set nfs4-idmap-active-directory enabled
```

Active Directory の構成

手順

1. Windows サーバに AD DS（Active Directory Domain Service）のロールをインストールします。
2. UNIX コンポーネント用 ID Management をインストールします。

```
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:adminui /all
C:\Windows\system32>Dism.exe /online /enable-feature /
featurename:nis /all
```

3. NIS ドメインがサーバーに構成されていることを確認します。

```
C:\Windows\system32>nisadmin
The following are the settings on localhost

Push Interval : 1 days
Logging Mode  : Normal

NIS Domains
NIS Domain in AD  Master server  NIS Domain in UNIX
----------------  -------------  ----------------
corp              win-ad-server  corp
```

4. AD ユーザーとグループに NFSv4 サーバの UNIX UID/GID を割り当てます。
   a. [**Server Manager**] > [**Tools**] > [**Active Directory**] を選択します。
   b. AD ユーザーまたはグループの [**Properties**] を開きます。
   c. [UNIX Atributes] タブで、NIS ドメイン、UID、プライマリ GID フィールドを入力します。

Active Directory のクライアントを構成します。

手順

1. AD サーバに新しい AD ユーザーを作成して、NFS クライアントのサービス プリンシパルを定義します。
2. NFS クライアント用の NFS/サービス プリンシパルを作成します。

```
> ktpass -princ nfs/<client_dns_name>@<REALM> -mapuser nfsuser -
pass **** -out nfsclient.keytab
/crytp rc4-hmac-nt /ptype KRB5_NT_PRINCIPAL
```

3. （省略可能）キータブ ファイルをクライアントの `/etc/krb5.keytab` にコピーします。

この手順を実行する必要があるかどうかは、使用しているクライアント OS によって決まります。

第 11 章

ストレージ移行

本章には、次のセクションが含まれます。

- ストレージ移行の概要 294
- 移行計画に関する考慮事項 294
- 移行ステータスの表示 296
- 移行準備の評価 296
- DD System Manager を使用したストレージ移行 297
- ストレージ移行のダイアログ説明 298
- CLI を使用したストレージ移行 300
- CLI でのストレージ移行の例 302

ストレージ移行の概要

ストレージ移行では、既存ストレージ エンクロージャを新しいエンクロージャに交換して、パフォーマンスの向上、容量の増加、フットプリントの削減を実現できます。

新しいエンクロージャの設置が終了すると、システムで他のプロセス（データのアクセス、拡張、クリーニング、レプリケーションなど）のサポートを継続しながら、古いエンクロージャから新しいエンクロージャにデータを移行できます。ストレージ移行がシステム リソースを必要することは事実ですが、スロットル設定で移行の優先度を相対的に高くまたは低くすることにより、これを制御できます。また、移行を一時停止して他のプロセスで使用可能なリソースを増やし、リソース需要が低くなった時点で移行を再開することができます。

移行中、システムは、ソースおよびデスティネーション エンクロージャのデータを使用します。新しいデータは、新しいエンクロージャに書き込まれます。移行されないデータはソース エンクロージャで更新され、移行されたデータはデスティネーション エンクロージャで更新されます。移行が中断された場合、移行済みとマークされていないブロックの移行を再開できます。

移行中、各データ ブロックはコピーおよび検証されます。ソース ブロックが解放されて移行済みとマークされ、システムのインデックスが新しいロケーションを使用するように更新されます。ソース ブロック宛てに送られた新しいデータは、デスティネーション ブロックにリダイレクトされます。ソースから割り当てられるはずだったすべての新しいデータ ブロックの割り当ては、ターゲットから割り当てられます。

移行のコピー処理は、論理データ レベルではなくシェルフ レベルで行われるため、ソース シェルフ上のすべてのディスク セクターは、そこにデータがあるかどうかに関係なく、アクセスされコピーされます。したがって、ストレージの移行ユーティリティを論理データの設置面積縮小に使用することはできません。

注

データ セットは移行中にソースとデスティネーションのエンクロージャ間で分割されるため、移行を一時停止してソース エンクロージャのみの使用を再開することはできません。いったん開始した移行は完了させる必要があります。ディスク ドライブのエラーなどの障害が発生した場合は、移行が中断され、問題を解決してから再開されます。

移行するデータの量と選択したスロットル設定に応じて、ストレージ移行には数日から数週間かかる場合があります。すべてのデータを移行すると、`storage migration finalize` コマンドを使用して手動で開始する必要がある確定プロセスによって、ファイル システムが再起動されます。再起動中にソース エンクロージャはシステム構成から削除され、デスティネーション エンクロージャはファイル システムの一部になります。確定プロセスが完了したら、ソース エンクロージャをシステムから削除できます。

ストレージ移行後、DD OS によってレポートされるディスク シェルフの番号がシーケンシャルでない場合があります。これは、シェルフの番号は個別の各ディスク シェルフのシリアル番号に関連づけられているためです。ナレッジベース記事 499019、「Data Domain: Storage enclosure numbering is not sequential」（https://support.emc.com で入手可能）に追加の詳細があります。DD OS バージョン 5.7.3.0 以降では、ナレッジ ベース記事で説明されている `enclosure show persistent-id` コマンドには、SE アクセスではなく管理者アクセスが必要です。

移行計画に関する考慮事項

ストレージの移行を開始する前に、次のガイドラインを考慮します。

- ストレージ移行は、1 回のみ使用可能なライセンスを必要とし、DD OS バージョン 5.7 以降がサポートされたシステム モデルで実行します。

注

複数のストレージ移行操作には、複数のライセンスが必要です。ただし、1 回の操作で複数のソース エンクロージャを複数のデスティネーション エンクロージャに移行できます。

- ストレージの移行はエンクロージャの数ではなく容量に基づいています。そのため、次のような移行が可能です。
  - 1 つのソース エンクロージャを 1 つののデスティネーション エンクロージャに移行できます。
  - 1 つのソース エンクロージャを複数のデスティネーション エンクロージャに移行できます。
  - 複数のソース エンクロージャを 1 つのデスティネーション エンクロージャに移行できます。
  - 複数のソース エンクロージャを複数のデスティネーション エンクロージャに移行できます。
- デスティネーション エンクロージャの条件は次の通りです。
  - 新しい、未使用かつライセンス未登録のシェルフであること。
  - DD システム モデルでサポートされていること。
  - リプレースするエンクロージャと少なくとも同程度の有効容量があること。

    注

    ソース シェルフの使用率を決定することはできません。Data Domain システムは、シェルフの容量に基づいてすべての計算を実行します。
- DD システム モデルには、新しいエンクロージャのアクティブな階層のストレージ容量をサポートするための、十分なメモリが必要です。
- システム コントローラー内のディスクのデータ移行はサポートされていません。
- ⚠ 注意

  進行中のストレージ移行が完了するまでは、DD OS をアップグレードしないでください。
- ファイル システムが無効な場合、または DD OS アップグレードの進行中、別の移行の進行中、RAID 再構築の進行中は、ストレージ移行は開始できません。

注

ストレージ移行が進行中の場合、進行中の移行の完了後に新しいストレージ移行操作を開始するには新しいストレージ移行ライセンスが必要です。ストレージ移行ライセンスの有無は、アップグレード事前チェックの一部として報告されます。

- すべての指定されたソース エンクロージャは、同じ階層（アクティブまたはアーカイブ）内に存在する必要があります。
- 各ソース エンクロージャ内に存在できるディスク グループは 1 つのみで、そのディスク グループ内のすべてのディスクは同じエンクロージャ内に設置されている必要があります。
- 各デスティネーション エンクロージャ内のすべてのディスクは、同じタイプ（たとえば、すべて SATA またはすべて SAS）にする必要があります。
- 移行の開始後、デスティネーション エンクロージャは削除できません。
- ソース エンクロージャは、移行が終了して完了するまで削除できません。
- ストレージ移行にかかる時間は、システム リソース（システム モデルによって異なる）、システム リソースの可用性、移行するデータ量に応じて異なります。ストレージ移行には、完了まで数日から数週間かかる場合があります。

DS60 シェルフに関する考慮事項

DS60 高密度シェルフは 60 台のディスクを保持できるため、ラックのスペースを最大限に活用できます。キャビネットからシェルフを拡張することで、シェルフの上部からドライブにアクセスします。DS60 シェルフの重量はフル構成時で約 225 lb となるため、シェルフへのストレージ移行の前にこのセクションをお読みください。

DS60 シェルフを使用する場合は、次の事項に注意してください。

⚠ 注意

- **ラックの最上部にシェルフを設置すると、シェルフが倒れる恐れがあります。**
- **フロアが DS60 シェルフの合計重量に対応できることを確認してください。**
- **ラックが DS60 シェルフに十分な電力を供給できることを確認してください。**
- **最初のラックに 5 台を超える DS60、または 2 番目のラックに 6 台を超える DS60 を追加する場合、DS60 シェルフを保持するために固定用バーと踏み台が必要です。**

移行ステータスの表示

DD System Manager には、ストレージ移行のステータスを表示する方法が 2 つあります。

手順

1. ［**Hardware**］ > ［**Storage**］を選択します。

   ［Storage］領域で、［Storage Migration Status］行を確認します。ステータスが［Not Licensed］の場合、ストレージ移行機能を使用する前にライセンスを追加する必要があります。ストレージ移行ライセンスがインストールされている場合、ステータスは次のいずれかになります：［None］、［Starting］、［Migrating］、［Paused by User］、［Paused by System］、［Copy Completed - Pending Finalization］、［Finalizing］、［Failed during Copy］、［Failed during Finalize］。

2. ストレージ移行が進行中の場合、［**View Storage Migration**］をクリックすると、進行状況のダイアログが表示されます。

   注

   移行のステータスには、転送済みブロックの割合（%）が表示されます。多くの空きブロックがあるシステムでは、空きブロックは移行されませんが、進捗の指標には含まれています。このような状況でデータ移行を開始すると、進行状況のインジケーターが迅速に進行し、その後遅くなります。

3. ストレージ移行の進行中、ステータスは［**Health**］ > ［**Jobs**］を選択して表示することもできます。

移行準備の評価

システムを使用して、移行の開始をコミットしないでストレージ移行の準備を評価できます。

手順

1. 製品の設置ガイドの手順を使用して、ターゲット エンクロージャを設置します。
2. ［**Administration**］ > ［**Licenses**］を選択して、ストレージ移行のライセンスがインストールされていることを確認します。
3. ストレージ移行のライセンスがインストールされていない場合は、［**Add Licenses**］をクリックしてライセンスを追加します。
4. ［**Hardware**］ > ［**Storage**］を選択してから［**Migrate Data**］をクリックします。
5. ［Select a Task］ダイアログで［**Estimate**］を選択してから、［**Next**］をクリックします。
6. ［Select Existing Enclosures］ダイアログで、チェックボックスを使用してストレージ移行の各ソース エンクロージャを選択して、［**Next**］をクリックします。
7. ［Select New Enclosures］ダイアログで、チェックボックスを使用してストレージ移行の各ターゲット エンクロージャを選択して、［**Next**］をクリックします。

   ［Add Licenses］ボタンでは、現在のタスクを中断せずに、新しいエンクロージャのストレージライセンスを必要に応じて追加できます。
8. ［Review Migration Plan］ダイアログで、推定移行スケジュールを確認して、［**Next**］をクリックします。
9. ［Verify Migration Preconditions］ダイアログで事前チェックの結果を確認して、［Close］をクリックします。

結果

事前テストのいずれかで障害が発生した場合は、移行を開始する前に、問題を解決してください。

DD System Manager を使用したストレージ移行

ストレージ移行プロセスでは、システムの準備を評価し、移行を開始するかどうかを確認するプロンプトが表示されます。また、データを移行した後は、プロセスを確定するプロンプトが表示されます。

手順

1. 製品のインストール ガイドの手順を使用して、ターゲット エンクロージャをインストールします。
2. ［**Administration**］ > ［**Licenses**］を選択して、ストレージ移行のライセンスがインストールされていることを確認します。
3. ストレージ移行のライセンスがインストールされていない場合は、［**Add Licenses**］をクリックしてライセンスを追加します。
4. ［**Hardware**］ > ［**Storage**］を選択してから［**Migrate Data**］をクリックします。
5. ［Select a Task］ダイアログで［**Migrate**］を選択してから、［**Next**］をクリックします。
6. ［Select Existing Enclosures］ダイアログで、チェックボックスを使用してストレージ移行の各ソース エンクロージャを選択して、［**Next**］をクリックします。
7. ［Select New Enclosures］ダイアログで、チェックボックスを使用してストレージ移行の各ターゲット エンクロージャを選択して、［**Next**］をクリックします。

   ［Add Licenses］ボタンでは、現在のタスクを中断せずに、新しいエンクロージャのストレージライセンスを必要に応じて追加できます。
8. ［Review Migration Plan］ダイアログで、推定移行スケジュールを確認して、［**Start**］をクリックします。

9. ［Start Migration］ダイアログで［**Start**］をクリックします。

   ［Migrate］ダイアログが表示され、移行 3 フェーズ（ Starting Migration、Migration in Progress、Copy Complete）の間更新されます。

10. ［Migrate］ダイアログのタイトルに［Copy Complete］が表示され、ファイル システムの再起動が可能になったら、［**Finalize**］をクリックします。

    注

    このタスクはファイル システムを再起動し、通常は 10～15 分かかります。この間はシステムを利用できません。

結果

移行の確定タスクが完了すると、ターゲット エンクロージャとソース エンクロージャを使用するシステムを削除できます。

ストレージ移行のダイアログ説明

DD System Manager のダイアログ説明には、ストレージ移行に関する追加の詳細が示されます。この情報は、ダイアログのヘルプ アイコンをクリックしても利用できます。

［Select a Task］ダイアログ

このダイアログの構成では、システムがストレージ移行の準備を評価して停止するか、準備を評価してストレージ移行を開始するかを指定します。

［**Estimate**］を選択すると、システムの準備を評価して停止します。

［**Migrate**］を選択すると、システムの評価後に移行を開始します。システムの評価と移行の開始の間に、ダイアログからストレージ移行を確認/キャンセルするプロンプトが表示されます。

［Select Existing Enclosures］ダイアログ

このダイアログの構成では、アクティブまたは保存階層と、移行のソース エンクロージャのいずれかを選択します。

DD Extended Retention 機能がインストールされている場合は、リスト ボックスを使用して、［**Active Tier**］または［**Retention Tier**］を選択します。DD Extended Retention がインストールされていない場合は、リスト ボックスは表示されません。

［Existing Enclosures］リストには、ストレージ移行の候補になるエンクロージャが表示されます。移行するエンクロージャの各チェック ボックスをオンにします。続行する準備ができたら、［**Next**］をクリックします。

［Selectct New Enclosures］ダイアログ

このダイアログの構成では、移行のターゲット エンクロージャを選択します。また、このダイアログには、ストレージのライセンス ステータスと［**Add Licenses**］ボタンが表示されます。

［Available Enclosures］リストには、ストレージ移行のターゲット候補になるエンクロージャが表示されます。必要なターゲット エンクロージャそれぞれのチェックボックスを選択します。

ライセンスのステータス バーには、システムにインストールされているすべてのストレージ ライセンスが表示されます。緑色の部分には使用中のライセンスが表示され、クリアな部分にはターゲット エンクロージャに使用可能な、ライセンスされたストレージ容量が表示されます。追加ライセンスをインスト

ールして、選択したターゲット コントローラーをサポートする場合は、［**Add Licenses**］をクリックします。

続行する準備ができたら、［**Next**］をクリックします。

［Review Migration Plan］ダイアログ

このダイアログには、ストレージ移行期間の予想が 3 段階のストレージ移行に応じてまとめられ、表示されます。

ストレージ移行のステージ 1 では、一連のテストを実行し、システムが移行用に準備されていることを検証します。テスト結果は、［Verify Migration Preconditions］ダイアログに表示されます。

ステージ 2 では、データがソース エンクロージャからデスティネーション エンクロージャにコピーされます。システムがバックアップ クライアントへの対応を続行している一方で、コピーはバックグラウンドで実行されるため、大量のデータが存在する場合は、コピーが完了するまで数日から数週間かかることがあります。［Migration in Progress］ダイアログの設定では、移行の優先度を変更して、速度を上げたり下げたりすることができます。

［Copy Complete］ダイアログから手動で起動するステージ 3 では、デスティネーション エンクロージャを使用するようにシステム構成を更新し、ソース コントローラーの構成を削除できます。この段階では、ファイル システムが再起動され、バックアップ クライアントはシステムを使用できません。

［Verify Migration Preconditions］ダイアログ

このダイアログは、移行を開始する前に実行したテスト結果を表示します。

次のリストにテスト シーケンスと各テストの詳細を示します。

P1：システムのプラットフォームをサポートしている。

以前の DD システム モデルではストレージ移行をサポートしていません。

P2：ストレージ移行ライセンスが使用可能。

ストレージ移行のライセンスが必要です。

P3：現在実行中の移行は他にない。

前のストレージ移行は、別の移行を開始する前に完了する必要があります。

P4：現在の移行リクエストが中断された移行リクエストと同じ。

中断した移行を再開し、完了します。

P5：既存エンクロージャ上のディスク グループ レイアウトを確認する。

ストレージ移行では、各ソース エンクロージャに含まれるディスク グループは 1 つのみである必要があり、グループ内のすべてのディスクがそのエンクロージャ内にある必要があります。

P6：最終的なシステム容量を確認する。

移行およびソース エンクロージャの削除後の合計システム容量は、DD システム モデルがサポートしている容量を超えることはできません。

P7：交換用エンクロージャの容量を確認する。

デスティネーション エンクロージャの使用可能容量は、ソース エンクロージャの使用可能容量を上回る必要があります。

P8：ソース エンクロージャは同じアクティブ階層または保存ユニット内にある。

システムは、アクティブ階層または保存階層のいずれかからのストレージ移行をサポートします。両方の階層からの同時データ移行はサポートしていません。

P9：ソース エンクロージャはヘッド ユニットに含まれない。

システム コントローラーは CLI 内でエンクロージャとしてリストされていても、ストレージ移行はシステム コントローラーに設置されたディスクからの移行はサポートしていません。

P10：交換用エンクロージャはストレージに追加可能。

各デスティネーション エンクロージャ内のすべてのディスクは、同じタイプ（たとえば、すべて SATA またはすべて SAS）にする必要があります。

P11：ソース コントローラーでは RAID 再構築が発生していない。

RAID 再構築が進行中であれば、ストレージ移行は開始できません。

P12：ソース シェルフはサポートされている階層に属している。

ソース ディスク エンクロージャは、移行先でサポートされている階層の一部である必要があります。

［Migration progress］ダイアログ

この一連のダイアログには、ストレージ移行のステータスおよび各段階で適用するコントロールが表示されます。

移行：移行の開始
最初の段階では、進捗は進行状況バーに表示され、使用可能なコントロールはありません。

移行：移行が進行中
2 番目の段階では、データはソース エンクロージャからデスティネーション エンクロージャにコピーされ、進捗は進行状況バーに表示されます。データ コピーは完了まで数日または数週間かかることがあるため、表示されるコントロールにより、移行中に使用されるリソースを管理し、リソースが他のプロセスに必要な場合は移行を一時停止することが可能です。

［**Pause**］をクリックすると移行を一時停止でき、後で［**Resume**］をクリックすると移行を続行できます。

［**Low**］、［**Medium**］、［**High**］のボタンは、ストレージ移行のリソース需要に関するスロットル設定を定義します。［Low］スロットル設定は、ストレージ移行のリソース優先度を低くすることで、移行が低速になり、必要なシステム リソースが低減します。反対に、［High］スロットル設定は、ストレージ移行のリソース優先度を高くすることで、移行が高速になり、必要なシステム リソースが増大します。［Medium］設定では、中間の優先度を選択します。

移行中にこのダイアログ ボックスを開いたままにする必要はありません。このダイアログ ボックスを閉じた後で移行のステータスを確認するには、［**Hardware**］ > ［**Storage**］を選択して、移行ステータスを表示します。［Hardware/Storage］ページからこのダイアログ ボックスに戻るには、［**Manage Migration**］をクリックします。［**Health**］ > ［**Jobs**］を選択して、移行の進行状況を表示することもできます。

移行：コピー完了
コピーが完了すると、［**Finalize**］をクリックするまで、移行プロセスは待機します。この最終段階は 10～15 分かかりますが、その間、ファイル システムが再起動され、システムは使用できなくなります。この段階は、メンテナンス期間やシステムのアクティビティが低い期間に開始することをお勧めします。

CLI を使用したストレージ移行

移行で必要とされるのは、割り当てられたブロックすべてを、ソース DG 上でフォーマットされたブロックセット（例、ソース ブロックセット）から、ターゲット DG 上でフォーマットされたブロックセット（例、ターゲット ブロックセット）に移動することだけです。すべての割り当てられたブロックがソース ブロックセット

から移動されると、それらのブロックセットはファイル システムから削除できるようになり、それらのディスクはストレージ階層から削除できるようになります。また、物理ディスクとエンクロージャは DDR から削除できます。

注

ストレージ移行の新しいエンクロージャの準備は、ストレージ移行プロセスによって管理されます。ターゲット エンクロージャは、エンクロージャの追加で行うようには準備しないでください。たとえば、`filesys expand` コマンドの使用はエンクロージャ追加では適切ですが、このコマンドではエンクロージャをストレージ移行のターゲットとして使用できません。

DS60 ディスク シェルフには 4 個のディスク パックが含まれており、それぞれ 15 台のディスクで構成されています。DS60 シェルフが移行のソースまたはターゲットである場合、ディスク パックは**エンクロージャ:パック**として表されます。この例では、ソースはエンクロージャ 7、パック 2（7:2）、ターゲットはエンクロージャ 7、パック 4（7:4）となります。

手順

1. 製品のインストール ガイドの手順を使用して、ターゲット エンクロージャをインストールします。
2. ストレージ移行の機能のライセンスがインストールされていることを確認します。

   ```
   # elicense show
   ```

3. ライセンスがインストールされていない場合は、e ライセンスを更新してストレージ移行機能ライセンスを追加します。

   ```
   # elicense update
   ```

4. ソースおよびターゲット ディスクのディスク状態を表示します。

   ```
   # disk show state
   ```

   ソース ディスクを active 状態にする必要があり、ターゲット ディスクは unknown 状態にする必要があります。

5. ストレージ移行の事前チェックコマンドを実行して、システムで移行の準備ができているかどうかを判断します。

   ```
   # storage migration precheck source-enclosures 7:2 destination-enclosures 7:4
   ```

6. 移行のスロットル設定を表示します。

   ```
   storage migration option show throttle
   ```

7. システムの準備ができたら、ストレージ移行を開始します。

   ```
   # storage migration start source-enclosures 7:2 destination-enclosures 7:4
   ```

8. オプションで、移行中のソースおよびターゲット ディスクのディスク状態を表示します。

   ```
   # disk show state
   ```

   移行中、ソース ディスクは migrating 状態にする必要があり、ターゲット ディスクは destination 状態にする必要があります。

9. 必要に応じて、移行のステータスを確認します。

   ```
   # storage migration status
   ```

10. ソースおよびターゲット ディスクのディスク状態を表示します。

    ```
    # disk show state
    ```

移行中、ソース ディスクは migrating 状態にする必要があり、ターゲット ディスクは destination 状態にする必要があります。

11. 移行が完了したら、構成を更新してターゲット エンクロージャを使用します。

注

このタスクはファイル システムを再起動し、通常は 10～15 分かかります。この間はシステムを利用できません。

```
storage migration finalize
```

12. 各ソース エンクロージャからすべてのデータを削除する場合は、ここでデータを削除します。

```
storage sanitize start enclosure <enclosure-id>[:<pack-id>]
```

注

storage sanitize コマンドでは、認定データ消去は実行できません。Data Domain では認定データ消去をサービスとして提供しています。詳細については、Data Domain 担当営業までお問い合わせください。

13. ソースおよびターゲット ディスクのディスク状態を表示します。

```
# disk show state
```

移行の後、ソース ディスクを unknown 状態にする必要があり、ターゲット ディスクは active 状態にする必要があります。

結果

移行の確定タスクが完了すると、ターゲット ストレージとソース ストレージを使用するシステムを削除できます。

CLI でのストレージ移行の例

elicense show

```
# elicense show
Feature licenses:
## Feature     Count Mode            Expiration Date
-- ----------- ----- --------------- ---------------
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

elicense update

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature          Count   Mode             Expiration Date
-- -----------       -----  ---------------  ---------------
1  REPLICATION       1      permanent (int)  n/a
2  VTL               1      permanent (int)  n/a
3  Storage Migration 1      permanent (int)
-- -----------       -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above EMC ELMS
licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

disk show state

図 10 `disk show state`

```
# disk show state
Enclosure        Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------   ---------------------------------------------
1                .  .  .  .
2                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7               |--------|--------|--------|--------|
                | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)   |U  U  U |.  .  s |U  U  U |U  U  U |
     D(37-48)   |U  U  U |.  .  . |U  U  U |U  U  U |
     C(25-36)   |U  U  U |.  .  . |U  U  U |U  U  U |
     B(13-24)   |U  U  U |.  .  . |U  U  U |U  U  U |
     A( 1-12)   |U  U  U |.  .  . |U  U  U |U  U  U |
                |--------|--------|--------|--------|
--------------   ---------------------------------------------

Legend   State            Count
------   ---------------  -----
.        In Use Disks     18
s        Spare Disks      1
v        Available Disks  15
U        Unknown Disks    105
------   ---------------  -----
```

storage migration precheck

```
#storage migration precheck  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

      1 "Verifying platform support.....................................................PASS"
      2 "Verifying valid storage migration license exists...............................PASS"
      3 "Verifying no other migration is running........................................PASS"
      4 "Verifying request matches interrupted migration................................PASS"
      5 "Verifying data layout on the source shelves....................................PASS"
      6 "Verifying final system capacity................................................PASS"
      7 "Verifying destination capacity.................................................PASS"
      8 "Verifying source shelves belong to same tier...................................PASS"
      9 "Verifying enclosure 1 is not used as source....................................PASS"
     10 "Verifying destination shelves are addable to storage...........................PASS"
     11 "Verifying no RAID reconstruction is going on in source shelves.................PASS"
Migration pre-check PASSED

Expected time to migrate data: 8 hrs 33 min
```

storage migration show history

図 11 storage migration show history

```
# storage migration show history
Id   Source       Source Enclosure   Dest         Dest Enclosure    Status      Start Time                 End Time
     Enclosure*   Serial No.         Enclosure*   Serial No.
--   ----------   ----------------   ----------   ---------------   ---------   ------------------------   ------------------------
2    9:0          SHU952400106A23    7:0          SHU9524084G055B   Finalized   Sat Aug  8 11:59:37 2015   Mon Aug 10 11:10:11 2015
1    9:0          SHU952400106A23    7:0          SHU9524084G055B   Finalized   Thu Aug  6 16:39:55 2015   Fri Aug  7 10:28:07 2015
                                     8:0          SHU9524084G04LR
--   ----------   ----------------   ----------   ---------------   ---------   ------------------------   ------------------------
(*) Enclosure ids at migration start time.
```

storage migration start

```
#storage migration start  source-enclosures 2  destination-enclosures 11

  Source enclosures:
  Disks      Count   Disk    Disk         Enclosure   Enclosure
                     Group   Size         Model       Serial No.
  --------   -----   -----   ----------   ---------   --------------
  2.1-2.15   15      dg1     1.81 TiB     ES30        APM00111103820
  --------   -----   -----   ----------   ---------   --------------
  Total source disk size: 27.29 TiB

  Destination enclosures:
  Disks        Count   Disk      Disk       Enclosure   Enclosure
                       Group     Size       Model       Serial No.
  ----------   -----   -------   --------   ---------   --------------
  11.1-11.15   15      unknown   931.51 GiB ES30        APM00111103840
  ----------   -----   -------   --------   ---------   --------------
  Total destination disk size: 13.64 TiB

  Expected time to migrate data: 84 hrs 40 min

**   Storage migration once started cannot be aborted.
     Existing data on the destination shelves will be overwritten.
        Do you want to continue with the migration? (yes|no) [no]: yes

Performing migration pre-check:
      1 Verifying platform support.....................................................PASS
      2 Verifying valid storage migration license exists...............................PASS
      3 Verifying no other migration is running.......................................PASS
      4 Verifying request matches interrupted migration...............................PASS
      5 Verifying data layout on the source shelves...................................PASS
      6 Verifying final system capacity...............................................PASS
      7 Verifying destination capacity................................................PASS
      8 Verifying source shelves belong to same tier..................................PASS
      9 Verifying enclosure 1 is not used as source...................................PASS
     10 Verifying destination shelves are addable to storage..........................PASS
     11 Verifying no RAID reconstruction is going on in source shelves................PASS

Migration pre-check PASSED

Storage migration will reserve space in the filesystem to migrate data.
Space reservation may add up to an hour or more based on system resources.

Storage migration process initiated.
Check storage migration status to monitor progress.
```

storage migration status

図 12 storage migration status

```
# storage migration status
Id   Source        Destination   State       Percent   Estimated Time to Complete   Current Throttle
     Enclosure(s)  Enclosure(s)              Complete                               Setting
--   ------------  ------------  ---------   -------   --------------------------   ----------------
5    7:2           7:4           migrating   45%       30 hrs 18 mins               high
--   ------------  ------------  ---------   -------   --------------------------   ----------------
```

disk show state, migration in progress

図 13 `disk show state, migration in progress`

```
# disk show state
Enclosure        Disk
  Row(disk-id)    1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------   ----------------------------------------------
1                 .  .  .  .
2                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                 v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                 U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                |--------|--------|--------|--------|
                 | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)    |U  U  U |m  m  s |U  U  U |s  d  d |
     D(37-48)    |U  U  U |m  m  m |U  U  U |d  d  d |
     C(25-36)    |U  U  U |m  m  m |U  U  U |d  d  d |
     B(13-24)    |U  U  U |m  m  m |U  U  U |d  d  d |
     A( 1-12)    |U  U  U |m  m  m |U  U  U |d  d  d |
                 |--------|--------|--------|--------|
--------------   ----------------------------------------------

Legend   State               Count
------   -----------------   -----
.        In Use Disks        4
s        Spare Disks         2
v        Available Disks     15
U        Unknown Disks       90
m        Migrating Disks     14
d        Destination Disks   14
```

storage migration finalize

図 14 `storage migration finalize`

```
# storage migration finalize

Storage migration finalize restarts the filesystem.
This can take several minutes and the filesystem is unavailable until the operation completes.
        Do you want to continue? (yes|no) [no]: yes

Performing migration finalization pre-check:
(P1)    Verifying storage migration is ready for finalization....PASS
(P2)    Verifying there are no foreign disks.....................PASS
(P3)    Verifying data layout on the source shelves..............PASS

Migration finalization pre-check PASSED
Finalizing the storage migration with id 5:

Notifying filesystem to finalize migration...

Done.

Disabling the filesystem
Please wait..........
The filesystem is now disabled.
Removing source enclosures from filesystem...

Done.

Removing source enclosures from storage tier...

Done.

Enabling the filesystem
Please wait.....................
The filesystem is now enabled.
Storage migration with id 5 from enclosure(s) 7.2 to enclosure(s) 7.4 has been finalized.
```

disk show state, migration complete

図 15 `disk show state, migration complete`

```
# disk show state
Enclosure         Disk
  Row(disk-id)     1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
--------------    ---------------------------------------------
1                  .  .  .  .
2                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
4                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
5                  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6                  U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
7                 |--------|--------|--------|--------|
                  | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
     E(49-60)     |U  U  U |U  U  U |U  U  U |s  .  . |
     D(37-48)     |U  U  U |U  U  U |U  U  U |.  .  . |
     C(25-36)     |U  U  U |U  U  U |U  U  U |.  .  . |
     B(13-24)     |U  U  U |U  U  U |U  U  U |.  .  . |
     A( 1-12)     |U  U  U |U  U  U |U  U  U |.  .  . |
                  |--------|--------|--------|--------|
--------------    ---------------------------------------------

Legend   State             Count
------   ---------------   -----
.        In Use Disks      18
s        Spare Disks       1
v        Available Disks   15
U        Unknown Disks     105
------   ---------------   -----
```

注

現在、ストレージ移行はアクティブ ノードでのみサポートされています。HA クラスタのパッシブ ノードでは、ストレージ移行はサポートされていません。

第 12 章

Metadata on Flash

本章には、次のセクションが含まれます。

- MDoF（Metadata on Flash）の概要 308
- MDoF のライセンスと容量 309
- SSD キャッシュ階層 310
- MDoF SSD キャッシュ階層 - システム管理 310
- SSD のアラート 313

MDoF（Metadata on Flash）の概要

MDoF では、フラッシュ テクノロジーを使用してファイル システム メタデータのキャッシュを作成します。SSD キャッシュは、メタデータとデータへのアクセスを高速化する、低レイテンシ、高 IOPS（1 秒あたりの I/O 操作の回数）のキャッシュです。

注

必要なソフトウェアの最小バージョンは、DD OS 6.0 です。

SSD にファイル システム メタデータをキャッシュすることで、従来のワークロードとランダム ワークロードの両方の I/O パフォーマンスが向上します。

従来のワークロードの場合、メタデータへのランダム アクセスを HDD から SSD にオフロードすることで、ハード ドライブはストリーミング書き込みおよび読み取りリクエストに対応できます。

ランダム ワークロードの場合、SSD キャッシュは低レイテンシのメタデータ操作を実現するため、HDD はキャッシュ リクエストではなくデータ リクエストを処理できます。

SSD に読み取りキャッシュを配置すると、頻繁にアクセスされるデータをキャッシュすることでランダム読み取りのパフォーマンスが向上します。NVRAM へのデータの書き込みと NVRAM のドレインを高速化する低レイテンシのメタデータ操作を組み合わせることで、ランダム書き込みのレイテンシが向上します。キャッシュがない場合でも、ファイル システム操作は妨げられず、ファイル システムのパフォーマンスに影響するだけです。

キャッシュ層がはじめて作成された際は、ファイル システムの実行後にキャッシュ層が追加された場合、ファイル システムの再起動のみが必要です。キャッシュ層のディスクに付属している新しいシステムについては、ファイル システムを有効化する前にキャッシュ層がはじめて作成された場合、ファイル システムの再起動は必要ありません。ファイル システムを無効化および有効化せずにキャッシュをライブ システムに追加できます。

注

DD OS 5.7 から DD OS 6.0 にアップグレードした DD9500 システムでは、最初にキャッシュ階層を作成した後に一度だけファイル システムを再起動する必要があります。

SSD 固有の条件は、残りのスペア ブロック数がゼロに近づいた場合、SSD は読み取り専用状態に入ることです。読み取り専用状態の場合、DD OS はドライブを読み取り専用キャッシュとして扱い、アラートを送信します。

MDoF は、次の Data Domain システムでサポートされています。

- DD6300
- DD6800
- DD9300
- DD9500
- DD9800
- DD3300 システムを含む、容量構成 16 TB 以上の DD VE インスタンス（DD VE の SSD キャッシュ階層）

MDoF のライセンスと容量

ELMS 経由で有効化されたライセンスは、MDoF 機能を使用するために必要です。SSD キャッシュ ライセンスは、デフォルトでは有効化されません。

次の表に、さまざまな SSD 容量ライセンスと、特定のシステムの SSD 容量を示します。

表 121 システムあたりの SSD 容量ライセンス

モデル	メモリ	SSD の数	SSD の容量
DD6300	48 GB（基本）	1	800 GB
	96 GB（拡張）	2	1600 GB
DD6800	192 GB（基本）	2	1600 GB
	192 GB（拡張）	4	3200 GB
DD9300	192 GB（基本）	5	4000 GB
	384 GB（拡張）	8	6400 GB
DD9500	256 GB（基本）	8	6400 GB
	512 GB（拡張）	15	12000 GB
DD9800	256 GB（基本）	8	6400 GB
	768 GB（拡張）	15	12000 GB

DD VE の SSD キャッシュ階層

DD VE インスタンスと DD3300 システムでは、SSD キャッシュ階層のライセンスは必要ありません。サポートされる SSD の最大容量は、アクティブ階層の容量の 1%です。

次の表に、さまざまな SSD 容量ライセンスと、特定のシステムの SSD 容量を示します。

表 122 DD VE と DD3300 の SSD の容量

容量構成	SSD の最大容量
DD VE 16 TB	160 GB
DD VE 32 TB	320 GB
DD VE 48 TB	480 GB
DD VE 64 TB	640 GB
DD VE 96 TB	960 GB
DD3300 8 TB	160 GB
DD3300 16 TB	160 GB
DD3300 32 TB	320 GB

SSD キャッシュ階層

SSD キャッシュ階層は、ファイル システムの SSD キャッシュ ストレージを提供します。ファイル システムは、ユーザーによるアクティブな操作なしで SSD キャッシュ階層から必要なストレージを取得します。

MDoF SSD キャッシュ階層 - システム管理

SSD キャッシュについては、次の事項に注意してください。

- コントローラ内に導入された SSD は、内部ルート ドライブとして扱われます。これらは、`storage show all` コマンドの出力にエンクロージャ 1 として表示されます。
- 個々の SSD は、HDD と同じように `disk` コマンドで管理します。
- `storage add` コマンドを実行して、個々の SSD または SSD エンクロージャを SSD キャッシュ階層に追加します。
- SSD キャッシュ階層のスペースを管理する必要はありません。ファイル システムは SSD キャッシュ階層から必要なストレージを取得し、そのクライアント間で共有します。
- SSD がシステムで使用可能な場合、`filesys create` コマンドは SSD ボリュームを作成します。

  注

  SSD を後でシステムに追加する場合、システムは自動的に SSD ボリュームを作成し、ファイル システムに通知します。SSD Cache Manager は、その登録済みクライアントに通知して、クライアントがキャッシュ オブジェクトを作成できるようにします。

- SSD ボリュームにアクティブ ドライブが 1 つだけ含まれている場合、アクティブ ドライブがシステムから削除されると、最後にオフラインになったドライブがオンラインに復帰します。

次のセクションでは、Data Domain System Manager と DD OS CLI を使用して SSD キャッシュ階層を管理する方法について説明します。

SSD キャッシュ階層の管理

ストレージ構成機能を使用すると、SSD キャッシュ階層でストレージの追加と削除ができます。

手順

1. ［**Hardware**］ > ［**Storage**］ > ［**Overview**］を選択します。
2. ［**Cache Tier**］ダイアログを展開します。
3. ［**Configure**］をクリックします。

   アクティブ階層に追加できるストレージの最大容量は、使用される DD コントローラーによって異なります。

   注

   ライセンスされた容量のバーには、インストールされたエンクロージャにライセンスされた容量（使用済みと未使用）の割り当てが表示されます。

4. 追加するシェルフのチェックボックスを選択します。

5. ［**Add to Tier**］ボタンをクリックします。
6. ［**OK**］をクリックして、ストレージを追加します。

注

追加したシェルフを削除するには、それを［Tier Configuration］リストからクリックし、［**Remove from Configuration**］、［**OK**］を順にクリックします。

［**CLI** 相当］
キャッシュ階層 SSD がヘッド ユニットに搭載されている場合。

a. SSD をキャッシュ階層に追加します。

```
#  storage add disks 1.13,1.14 tier cache
Checking storage requirements...done
Adding disk 1.13 to the cache tier...done

Updating system information...done

Disk 1.13 successfully added to the cache tier.


Checking storage requirements...
done
Adding disk 1.14 to the cache tier...done

Updating system information...done

Disk 1.14 successfully added to the cache tier.
```

b. 新しく追加された SSD の状態を確認します。

```
# disk show state
Enclosure   Disk
             1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------   ------------------------------------------------
1            .  .  .  .  s  .  .  s  s  s  s  s  v  v
2            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
3            U  U  U  U  U  U  U  U  U  U  U  U  U  U  U
---------   ------------------------------------------------

Legend   State              Count
------   ---------------    -----
.        In Use Disks       6
s        Spare Disks        6
v        Available Disks    2
U        Unknown Disks      30
------   ---------------    -----
Total 44 disks
```

キャッシュ階層 SSD が外部シェルフに搭載されている場合。

a. SSD シェルフがシステムに認識されていることを確認します。次の例では、SSD シェルフはエンクロージャ 2 です。

```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    ------------------------------------------------
1            .  .  .  .
2            U  U  U  U  U  U  U  U  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
```

```
10           |--------|--------|--------|--------|
             | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60) |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48) |v  v  v |v  v  v |v  v  v |v  v  v |
   C(25-36) |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24) |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12) |v  v  v |v  v  v |v  v  v |v  v  v |
            |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------   -----------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

b. SSD シェルフのシェルフ ID を識別します。SSD は `Type` 列に `SAS-SSD` または `SATA-SSD` として表示されます。

```
#  disk show hardware
```

図 16

Disk (enc/disk)	Slot	Manufacturer/Model	Firmware	Serial No.	Capacity	Type
1.1	0	TG32C10400GA3EMC_____118000371	PRO6E344	FG009826	372.61 GiB	SATA-SSD
1.2	1	TG32C10400GA3EMC_____118000371	PRO6E344	FG0097VL	372.61 GiB	SATA-SSD
1.3	2	TG32C10400GA3EMC_____118000371	PRO6E344	FG009881	372.61 GiB	SATA-SSD
1.4	3	TG32C10400GA3EMC_____118000371	PRO6E344	FG00988X	372.61 GiB	SATA-SSD
2.1	0	HITACHI HUSMR148_CLAR800	C29C	07V4P2AA	745.22 GiB	SAS-SSD
2.2	1	HITACHI HUSMR148_CLAR800	C29C	07V4P3LA	745.22 GiB	SAS-SSD
2.3	2	HITACHI HUSMR148_CLAR800	C29C	07V4P2XA	745.22 GiB	SAS-SSD
2.4	3	HITACHI HUSMR148_CLAR800	C29C	07V4TW4A	745.22 GiB	SAS-SSD
2.5	4	HITACHI HUSMR148_CLAR800	C29C	07V4ULYA	745.22 GiB	SAS-SSD
2.6	5	HITACHI HUSMR148_CLAR800	C29C	07V4P0BA	745.22 GiB	SAS-SSD
2.7	6	HITACHI HUSMR148_CLAR800	C29C	07V4UVBA	745.22 GiB	SAS-SSD
2.8	7	HITACHI HUSMR148_CLAR800	C29C	07V4UTNA	745.22 GiB	SAS-SSD

c. SSD シェルフをキャッシュ階層に追加します。

```
#  storage add enclosure 2 tier cache

Checking storage requirements...done
Adding enclosure 2 to the cache tier...Enclosure 2
successfully added to the cache tier.

Updating system information...done

Successfully added: 2  done
```

d. 新しく追加された SSD の状態を確認します。

```
# disk show state
Enclosure   Disk
Row(disk-id) 1  2  3  4  5  6  7  8  9  10 11 12 13 14 15
---------    -----------------------------------------------
1            .  .  .  .
2            .  .  .  .  .  .  .  .  -  -  -  -  -  -  -
3            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
4            .  .  .  .  .  .  .  .  .  .  .  .  .  .  v
5            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
6            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
7            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
8            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
9            v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
10           |--------|--------|--------|--------|
             | Pack 1 | Pack 2 | Pack 3 | Pack 4 |
   E(49-60) |v  v  v |v  v  v |v  v  v |v  v  v |
   D(37-48) |v  v  v |v  v  v |v  v  v |v  v  v |
```

```
   C(25-36) |v  v  v |v  v  v |v  v  v |v  v  v |
   B(13-24) |v  v  v |v  v  v |v  v  v |v  v  v |
   A( 1-12) |v  v  v |v  v  v |v  v  v |v  v  v |
            |--------|--------|--------|--------|
11           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
12           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
13           v  v  v  v  v  v  v  v  v  v  v  v  v  v  v
---------   ---------------------------------------------

Legend   State               Count
------   ------------------  -----
.        In Use Disks        32
v        Available Disks     182
U        Unknown Disks       8
-        Not Installed Disks 7
------   ------------------ -----
Total 222 disks
```

コントローラ搭載の SSD をキャッシュ階層から削除するには、次のように入力します。

```
# storage remove disk 1.13

Removing disk 1.13...done

Updating system information...done

Disk 1.13 successfully removed.
```

SSD シェルフをシステムから削除するには、次のように入力します。

```
# storage remove enclosure 2

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done
```

SSD のアラート

SSD キャッシュ階層に固有のアラートは 3 つあります。

SSD キャッシュ階層のアラートは次のとおりです。

- ライセンス
  ファイル システムが有効化されており、構成されている物理キャッシュ容量がライセンスで許可されている容量より小さい場合、アラートが生成され、現在の SSD 容量と容量ライセンスが示されます。このアラートは、警告として分類されます。キャッシュがない場合でも、ファイル システム操作は妨げられず、ファイル システムのパフォーマンスに影響するだけです。ファイル システムを無効化および有効化せずにキャッシュをライブ システムに追加できます。
- 読み取り専用状態
  残りのスペア ブロック数がゼロに近づいた場合、SSD は読み取り専用状態に入ります。読み取り専用状態の場合、DD OS はドライブを読み取り専用キャッシュとして扱います。

  SSD が読み取り専用状態に入り、交換する必要がある場合、アラート `EVT-STORAGE-00001` が表示されます。
- SSD の寿命
  SSD がその寿命に達すると、ハードウェア障害アラートが生成され、SSD シェルフ内での SSD の位置が示されます。このアラートは、重大なアラートに分類されます。

EOL カウンターが 98 に達すると、アラート EVT-STORAGE-00016 が表示されます。EOL カウンターが 99 に達すると、ドライブが事前に障害状態に入ります。

第 13 章

SCSI ターゲット

本章には、次のセクションが含まれます。

- SCSI ターゲットの概要 316
- ［Fibre Channel］ビュー 317
- DD OS バージョンでの FC リンク モニタリングの違い 328

SCSI ターゲットの概要

SCSI（Small Computer System Interface）ターゲットは、すべての SCSI サービスとトランスポートに向けた統合管理デーモンです。SCSI ターゲットは、DD VTL（仮想テープ ライブラリ）、FC（ファイバー チャネル）経由の DD Boost、vDisk/ProtectPoint ブロック サービスと、DD システム上にターゲット LUN（論理ユニット番号）を持つものはすべてサポートします。

［**SCSI** ターゲット サービスおよびトランスポート］

SCSI ターゲット デーモンは、FC ポートが存在する場合、または DD VTL がライセンスされている場合に開始されます。すべての SCSI Target［サービス］と［トランスポート］に向けた統合管理が提供されます。

- ［サービス］とは、SCSI ターゲット コマンドを使用する DD システムにターゲット LUN を持つもの、たとえば DD VTL（テープ ドライブおよびチェンジャー）や FC 経由の DD Boost（プロセッサ デバイス）、vDisk（仮想ディスク デバイス）などを指します。
- ［トランスポート］により、［デバイス］が［イニシエーター］に認識されます。
- ［イニシエーター］は、FC プロトコルを使用してデータの読み取りと書き込みを行うシステムに接続するバックアップ クライアントです。特定のイニシエータでは、FC 経由の DD Boost、vDisk、DD VTL のいずれかをサポートできますが、3 つすべてはサポートできません。
- ［デバイス］は物理ポートを介して SAN（ストレージ エリア ネットワーク）で認識されます。ホスト イニシエーターは、SAN を介して DD システムと通信を行います。
- ［アクセス グループ］は、デバイスとイニシエーター間のアクセスを管理します。
- ［エンドポイント］は、DD システム上の論理ターゲットで、イニシエーターの接続先です。エンドポイントは、無効化、有効化、および名称変更できます。関連づけられたトランスポート ハードウェアが存在していては、エンドポイントを削除することはできません。新しいトランスポート接続が確立されると、エンドポイントは自動的に発見および作成されます。エンドポイントには、ポートトポロジー、FCP2-RETRY ステータス、WWPN、WWNN の属性があります。
- ［NPIV］（N_port ID Virtualization）は、複数のエンドポイントで 1 つの物理ポートを共有できる FC 機能です。NPIV は、ハードウェア要件を軽減し、フェイルオーバー機能を提供します。
- DD OS 6.0 では、ユーザーはフェールオーバー用のセカンダリ システム アドレスの順序を指定できます。たとえば、システムによって 0a、0b、1a、1b が指定され、ユーザーが 1b、1a、0a、0b を指定した場合、ユーザーが指定した順序がフェールオーバー用に使用されます。`scsitarget endpoint show detailed` コマンドは、ユーザーが指定したシーケンスを表示します。

次の例外に注意してください。

- DD Boost は、FC と IP クライアントの両方に同時に対処できますが、両方のトランスポートは同じイニシエーターを共有できません。
- アクセス グループ 1 つにつき存在できるイニシエーターは 1 つのみです。各アクセス グループには、タイプ（DD VTL、vDisk/ProtectPoint ブロック サービス、または FC 経由の DD Boost）が割り当てられます。

［**SCSI** ターゲット アーキテクチャ **-** サポートの有無］

SCSI ターゲットは、次のアーキテクチャをサポートします。

- ［異なるイニシエータの **DD VTL** と **FC** 経由の **DD Boost**：］（同一または異なるクライアント上にある）2 つの異なるイニシエータは、同一または異なる DD システム ターゲット エンドポイントを介して、DD VTL および FC 経由の DD Boost を使用する DD システムにアクセスできます。

- ［**1** つのイニシエータから **2** つの異なる **DD** システムに対する **DD VTL** と **FC** 経由の **DD Boost** : ］ シングル イニシエーターは、任意のサービスを使用する 2 つの異なる DD システムにアクセスできます。

SCSI ターゲットは、次のアーキテクチャをサポートしません。

- ［**1** つのイニシエータから同じ **DD** システムに対する **DD VTL** と **FC** 経由の **DD Boost** : ］ シングル イニシエーターは、異なるサービスを介して同じ DD システムにアクセスすることはできません。

［シン プロトコル］

シン プロトコルは、プライマリ プロトコルが応答できないときに SCSI コマンドに応答する、VDisk と DD VTL 用の軽量のデーモンです。複数のプロトコルを使用するファイバー チャネル環境の場合、シン プロトコルには次の利点があります。

- イニシエータのハングを防止します。
- イニシエータの不必要な終了を防止します。
- イニシエータ デバイスの消失を防止します。
- スタンバイ モードをサポートします。
- 高速かつ早期検出可能なデバイスをサポートします。
- プロトコルの HA 動作を強化します。
- 高速なレジストリ アクセスを不要にします。

［**DD Boost** と **scscitarget** コマンド（**CLI**）の詳細］

DD System Manager を介した DD Boost の使用の詳細については、本書の関連する章を参照してください。DD Boost のその他の情報については、「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。

この章は、DD System Manager を介した SCSI ターゲットの使用に焦点を当てています。基本タスクを理解したら、「Data Domain オペレーティング システム コマンド リファレンス ガイド」の `scscitarget` コマンドで、より高度な管理タスクについて参照してください。

過剰な DD VTL トラフィックがある場合は、`scsitarget group use` コマンドを実行して、グループ内の 1 つ以上の SCSI ターゲットまたは vdisk デバイスの使用中のエンドポイント リストをプライマリ エンドポイント リストとセカンダリ エンドポイント リストで切り替えることはしないでください。

［Fibre Channel］ビュー

［Fibre Channel］ビューには、ファイバー チャネルおよび/または NPIV が有効かどうかの現在のステータスが表示されます。また、2 つのタブ、［Resources］と［Access Groups］があります。［Resources］には、イニシエーターとエンドポイントが含まれます。アクセス グループは、イニシエーター WWPN（World Wide Name ポート名）またはエイリアス、およびアクセスを許可されるドライブとチェンジャーのコレクションを保持します。

NPIV の有効化

NPIV（N_Port ID Virtualization）は、複数のエンドポイントで 1 つの物理ポートを共有できるファイバー チャネル機能です。NPIV はハードウェア要件を軽減し、エンドポイントのフェイルオーバー/フェイルバック機能を提供します。NPIV はデフォルトでは構成されていないため、これを有効にする必要があります。

注

NPIV は、HA 構成ではデフォルトで有効化されています。

NPIV は、複数システムの統合を簡略化します。

- NPIV は ANSI T11 標準であり、1 個の HBA 物理ポートを複数の WWPN を使用するファイバー チャネル ファブリックに登録できます。
- 仮想ポートと物理ポートのポート プロパティは同じで、まったく同じ動作をします。
- 場合によってエンドポイントとポート間には m:1 の関係があり、複数のエンドポイントで同じ物理ポートを共有できます。

具体的には、NPIV を有効化すると次の機能が有効化されます。

- それぞれが仮想（NPIV）ポートを使用する物理ポートあたりで複数のエンドポイントを許可されます。ベース ポートは物理ポートのプレースホルダーであり、エンドポイントと関連づけられていません。
- NPIV を使用する場合、エンドポイントのフェイル オーバー/フェイルバックは自動的に有効化されます。

  注

  NPIV が有効化されたら、各エンドポイントで「セカンダリ システムのアドレス」を指定する必要があります。指定しない場合、エンドポイントのフェイルオーバーは発生しません。

- 複数の DD システムを 1 つの DD システムに統合できますが、HBA の数は 1 つの DD システムと同じで変わりません。
- ポートがオフラインからオンラインになったときを FC-SSM が検出すると、エンドポイントのフェイルオーバーがトリガーされます。Scsitarget が有効化される前に物理ポートがオフラインになっていて、scsitarget を有効化した後もオフラインのままである場合は、FC-SSM がポート オフライン イベントを生成しないため、エンドポイントのフェイルオーバーが可能になりません。ポートがオンラインに戻り、自動フェイルバックが有効化されると、そのポートをプライマリ ポートとして使用するフェイルオーバー済みのエンドポイントは、すべてプライマリ ポートにフェイルバックします。

Data Domain の HA 機能では、NPIV が、フェイルオーバー プロセス中に HA ペアのノード間で WWN を移動する必要があります。

注

NPIV を有効にするには、次の条件を満たす必要があります。

- DD システムは DD OS 5.7 が実行されている必要があります。
- すべてのポートが、4 Gb、8 Gb、16 Gb のファイバー チャネル HBA および SLIC に接続される必要があります。
- DD システムの ID が有効（0 ではない）である必要があります。

さらに、NPIV の有効化を妨げる可能性がある、ポートのトポロジーとポート名を確認します。

- ［すべて］のポートのトポロジーが loop-preferred の場合、NPIV が許可されます。
- ポートの［一部］のトポロジーが loop-preferred の場合、NPIV は許可されます。ただし、NPIV は、loop-only のポートを無効化する必要があります。または、適切に機能させるためにトポロジーを loop-preferred に再構成する必要があります。
- loop-preferred のトポロジーを持つポートが［ない］場合、NPIV は［許可されません］。
- ポート名がアクセス グループ内に存在する場合、そのポート名は関連するエンドポイント名と置き換えられます。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］を選択します。
2. ［NPIV: Disabled］の隣にある［**Enable**］を選択します。
3. ［Enable NPIV］ダイアログでは、NPIV を有効化する前に、すべてのファイバー チャネル ポートを無効化する必要があることを示すメッセージが表示されます。これを実行する場合は、［**Yes**］を選択します。

   ［**CLI** 相当］

   a. （グローバル）NPIV が有効になっていることを確認します。

   ```
   # scsitarget transport option show npiv
   SCSI Target Transport Options
   Option   Value
   ------   --------
   npiv     disabled
   ------   --------
   ```

   b. NPIV が無効になっている場合、有効化します。最初に、すべてのポートを無効にする必要があります。

   ```
   # scsitarget port disable all
   All ports successfully disabled.
   # scsitarget transport option set npiv enabled
   Enabling FiberChannel NPIV mode may require SAN zoning to
   be changed to configure both base port and NPIV WWPNs.
   Any FiberChannel port names used in the access groups will
   be converted to their corresponding endpoint names in order
   to prevent ambiguity.
       Do you want to continue? (yes|no) [no]:
   ```

   c. 無効なポートを再度有効化します。

   ```
   # scsitarget port enable all
   All ports successfully enabled.
   ```

   d. 物理ポートの NPIV 設定が「auto」になっていることを確認します。

   ```
   # scsitarget port show detailed 0a
   System Address:     0a
   ```

```
Enabled:             Yes
Status:              Online
Transport:           FibreChannel
Operational Status: Normal
FC NPIV:             Enabled (auto)
.
.
.
```

e. 選択したプライマリおよびセカンダリ ポートを使用して新しいエンドポイントを作成します。

```
# scsitarget endpoint add test0a0b system-address 0aprimary-
system-address 0a secondary-system-address 0b
```

エンドポイントはデフォルトで無効になっているため、有効化することに注意してください。

```
# scsitarget endpoint enable test0a0b
```

エンドポイント情報を表示します。

```
# scsitarget endpoint show detailed test0a0b
Endpoint:                  test0a0b
Current System Address:    0b
Primary System Address:    0a
Secondary System Address: 0b
Enabled:                   Yes
Status:                    Online
Transport:                 FibreChannel
FC WWNN:                   50:02:18:80:08:a0:00:91
FC WWPN:                   50:02:18:84:08:b6:00:91
```

f. 新しく作成したエンドポイントの自動生成 WWPN に、ホスト システムをゾーニングします。

g. DD VTL、vDisk、または DFC（DD Boost over Fibre Channel）デバイスを作成して、このデバイスをホスト システムで使用可能にします。

h. 選択した DD デバイスがホストにアクセス（読み取り/書き込み）できることを確認します。

i. 「secondary」オプションを使用してエンドポイント フェイルオーバーをテストし、エンドポイントを SSA（セカンダリ システム アドレス）に移動します。

```
# scsitarget endpoint use test0a0b secondary
```

j. 選択した DD デバイスが依然としてホストにアクセス（読み取り/書き込み）できることを確認します。「primary」オプションを使用してフェイルバックをテストし、エンドポイントを PSA（プライマリ システム アドレス）に移動します。

```
# scsitarget endpoint use test0a0b primary
```

k. 選択した DD デバイスが依然としてホストにアクセス（読み取り/書き込み）できることを確認します。

NPIV の無効化

NPIV を無効にする前に、複数のエンドポイントを使用しているポートをなくす必要があります。

注

NPIV は、HA 構成に必要です。デフォルトで有効化されていて、無効化することはできません。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］を選択します。
2. ［NPIV: Enabled］の隣にある［**Disable**］を選択します。

3. ［Disable NPIV］ダイアログで、構成を修正することについてのメッセージを確認し、準備ができたら、［**OK**］を選択します。

［Resources］タブ

［**Hardware**］ > ［**Fibre Channel**］ > ［**Resources**］タブには、ポート、エンドポイント、イニシエーターについての情報が表示されます。

表 123 ポート

項目	説明
システム アドレス	ポートのシステム アドレス
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
Enabled	ポート動作ステータス（［Enabled］または［Disabled］）。
NPIV	NPIV のステータス（［Enabled］または［Disabled］）。
リンク ステータス	リンクのステータス（［Online］または［Offline］）。これは、ポートが起動しており、トラフィックを処理できるかどうかを示します。
Operation Status	操作のステータス（［Normal］または［Marginal］）。
# of Endpoints	このポートに関連づけられたエンドポイントの数。

表 124 エンドポイント

項目	説明
Name	エンドポイントの名前。
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
システム アドレス	エンドポイントのシステム アドレス。
Enabled	ポート動作状態（［Enabled］または［Disabled］）。
リンク ステータス	Online または Offline。これは、ポートが起動しており、トラフィックを処理できるかどうかを示します。

表 125 Initiators

項目	説明
Name	イニシエーターの名前。

表 125 Initiators （続き）

項目	説明
サービス	イニシエーターによるサービス サポート（DD VTL、DD Boost、または vDisk）。
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
Vendor Name	イニシエーターのモデル。
Online Endpoints	このイニシエーターが認識しているエンドポイント。イニシエーターが使用できない場合、［none］または［offline］が表示されます。

ポートの構成

起動時にポートが検出され、ポートごとに 1 個のエンドポイントが自動作成されます。

ベース ポートのプロパティは、NPIV が有効になっているかどうかによって異なります。

- 非 NPIV モードでは、ポートはエンドポイントと同じプロパティを使用します。つまり、ベース ポートの WWPN とエンドポイントは同じです。
- NPIV モードでは、ベース ポートのプロパティは、デフォルト値から派生します。つまり、ベース ポートの WWPN が新たに生成され、NPIV モード間で一貫したスイッチングが可能になるように保存されます。また、NPIV モードは、ポートあたり複数のエンドポイントをサポートする機能を提供します。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［**Resources**］を選択します。
2. ［**Ports**］の下でポートを選択した後、［**Modify**］（鉛筆）を選択します。
3. ［Configure Port］ダイアログでは、このポートの NPIV を自動的に有効化または無効化するかを選択します。
4. ［Topology］では、［Loop Preferred］、［Loop Only］、［Point to Point］、または［Default］を選択します。
5. ［Speed］では、［1 Gbps］、［2 Gbps］、［4 Gbps］、［8 Gbps］、［16 Gbps］、［Auto］のいずれかを選択します。
6. ［**OK**］を選択します。

ポートの有効化

使用する前に、ポートを有効にする必要があります。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［**Resources**］を選択します。
2. ［**More Tasks**］ > ［**Ports**］ > ［**Enable**］を選択します。すべてのポートがすでに有効になっている場合、それを示すメッセージが表示されます。
3. ［Enable Ports］ダイアログで、リストから 1 つ以上のポートを選択した後、［**Next**］を選択します。

4. 確認した後、［**Next**］を選択して、タスクを完了します。

ポートの無効化

単純に 1 つ（または複数の）ポートを無効化するか、1 つ（または複数の）ポートのすべてのエンドポイントを別のポートにフェイルオーバーするかを選択できます。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［**More Tasks**］ > ［**Ports**］ > ［**Disable**］を選択します。
3. ［Disable Ports］ダイアログで、リストから 1 つ以上のポートを選択した後、［**Next**］を選択します。
4. 確認ダイアログで、続けて単純にポートを無効化するか、そのポートのすべてのエンドポイントを別のポートにフェイルオーバーするかを選択できます。

エンドポイントの追加

エンドポイントは、基礎となる仮想ポートに割り当てられた仮想オブジェクトです。非 NPIV モード（HA 構成では利用できないモード）では、物理ポート 1 個につき許可されるエンドポイントは 1 個のみであり、ベース ポートを使用してそのエンドポイントをファブリックに構成します。NPIV が有効な場合は、それぞれが仮想（NPIV）ポートを使用する複数のエンドポイントを物理ポートあたりで許可され、エンドポイントのフェイルオーバー/フェイルバックが有効です。

注

HA 構成では非 NPIV モードは利用できません。NPIV はデフォルトで有効化されていて、無効化することはできません。

注

NPIV モードでは、エンドポイントには次の特徴があります。

- プライマリ システムのアドレスがある。
- 0 個以上のセカンダリ システム アドレスが存在する場合がある。
- ポート障害時の代替システム アドレスへのフェイルオーバー候補のすべてとなる。ただし、周辺ポートへのフェイルオーバーはサポートされていない。
- ポートがオンラインでバックアップされると、フェイルバックされ、それらのプライマリ ポートを使用できる。

注

NPIV を使用する場合は、エンドポイントあたりで 1 つのプロトコルのみ（つまり、DD VTL Fibre Channel、DD Boost-over-Fibre Channel、vDisk Fibre Channel）を使用することをお勧めします。フェイルオーバー構成では、セカンダリ エンドポイントも構成して、プライマリと同じプロトコルを指定する必要があります。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［**Resources**］を選択します。
2. ［**Endpoints**］の下で、［**Add**］（+記号）を選択します。

3. ［Add Endpoint］ダイアログで、エンドポイントの名前を入力します（1～128 文字）。フィールドには空欄または「all」は指定できず、アスタリスク（*）、疑問符（?）、スラッシュまたはバック スラッシュ（/、\）、右または左括弧（(、)）は使用できません。
4. ［Endpoint Status］は、［Enabled］または［Disabled］を選択します。
5. プライマリ システム アドレスで NPIV が有効な場合は、ドロップダウン リストから選択します。プライマリ システムのアドレスは、任意のセカンダリ システム アドレスと異なる必要があります。
6. セカンダリ システム アドレスへのフェイルオーバーで NPIV が有効な場合は、セカンダリ システム アドレスの横にある適切なボックスをオンにします。
7. ［**OK**］を選択します。

エンドポイントの構成

追加したエンドポイントは、［Configure Endpoint］ダイアログを使用して変更できます。

注

NPIV を使用する場合は、エンドポイントあたりで 1 つのプロトコルのみ（つまり、DD VTL Fibre Channel、DD Boost-over-Fibre Channel、vDisk Fibre Channel）を使用することをお勧めします。フェイルオーバー構成では、セカンダリ エンドポイントも構成して、プライマリと同じプロトコルを指定する必要があります。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［**Resources**］を選択します。
2. ［**Endpoints**］の下でエンドポイントを選択した後、［**Modify**］（鉛筆）を選択します。
3. ［Configure Endpoint］ダイアログで、エンドポイントの名前を入力します（1～128 文字）。フィールドには空欄または「all」は指定できず、アスタリスク（*）、疑問符（?）、スラッシュまたはバック スラッシュ（/、\）、右または左括弧（(、)）は使用できません。
4. ［Endpoint Status］は、［Enabled］または［Disabled］を選択します。
5. プライマリ システム アドレスは、ドロップダウン リストから選択します。プライマリ システムのアドレスは、任意のセカンダリ システム アドレスと異なる必要があります。
6. セカンダリ システム アドレスへのフェイルオーバーでは、セカンダリ システム アドレスの横にある適切なボックスをオンにします。
7. ［**OK**］を選択します。

エンドポイントのシステム アドレスの変更

コマンド オプションを使用して、SCSI`scsitarget endpoint modify` ターゲット エンドポイントのアクティブ システム アドレスを変更できます。これは、コントローラーのアップグレード後、コントローラー HBA（ホスト バス アダプタ）の移動時など、すでに存在しないシステム アドレスにエンドポイントが関連づけられている場合に有効です。エンドポイントのシステム アドレスが変更されると、WWPN と WWNN（それぞれ worldwide port name と worldwide node name）を含むエンドポイントのすべてのプロパティ（もしあれば）が保存され、新しいシステム アドレスで使用されます。

次の例では、エンドポイント ep-1 がシステム アドレス 5a に割り当てられましたが、このシステム アドレスはすでに無効になっています。新しいコントローラー HBA がシステム アドレス 10a に追加されました。SCSI ターゲット サブシステムは自動的に、新たに検出されたシステム アドレス用の新しいエンドポイント（ep-new）を作成しました。特定のシステム アドレスに関連づけできるエンドポイントは 1 個のみであるため、ep-new は削除し、ep-1 をシステム アドレス 10a に割り当てる必要があります。

注

WWPN と WWNN は別のシステム アドレスに移動されているため、SAN 環境によっては変更されたエンドポイントがオンラインになるには時間がかかる場合があります。新しい構成を反映するには、SAN ゾーニングも更新する必要がある場合があります。

手順

1. 変更するエンドポイントを検証するため、すべてのエンドポイントを表示します。
   ```
   # scsitarget endpoint show list
   ```
2. すべてのエンドポイントを無効化します。
   ```
   # scsitarget endpoint disable all
   ```
3. 新しい不必要なエンドポイント（ep-new）を削除します。
   ```
   # scsitarget endpoint del ep-new
   ```
4. 新しいシステム アドレス 10a を割り当てて、使用したいエンドポイント（ep-1）を変更します。
   ```
   # scsitarget endpoint modify ep-1 system-address 10a
   ```
5. すべてのエンドポイントを有効化します。
   ```
   # scsitarget endpoint enable all
   ```

エンドポイントの有効化

現在無効化されている場合、つまり非 NPIV モードの場合のみ、エンドポイントの有効化によってポートが有効化されます。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［**More Tasks**］ > ［**Endpoints**］ > ［**Enable**］を選択します。すべてのエンドポイントがすでに有効になっている場合、それを示すメッセージが表示されます。
3. ［Enable Endpoints］ダイアログで、リストから 1 つ以上のエンドポイントを選択した後、［**Next**］を選択します。
4. 確認した後、［**Next**］を選択して、タスクを完了します。

エンドポイントの無効化

そのポートを使用しているすべてのエンドポイントが無効化されない限り、つまり非 NPIV モードでない限り、エンドポイントの無効化では関連ポートは無効化されません。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［**More Tasks**］ > ［**Endpoints**］ > ［**Disable**］を選択します。
3. ［Disable Endpoints］ダイアログで、リストから 1 つ以上のエンドポイントを選択した後、［**Next**］を選択します。エンドポイントが使用中の場合、それを無効化するとシステムが停止する可能性がある旨を示すメッセージが表示されます。
4. ［**Next**］を選択して、タスクを完了します。

エンドポイントの削除

基盤ハードウェアが使用できなくなっている場合、エンドポイントを削除できます。ただし、基板ハードウェアがまだ存在しているか、使用可能になった場合は、ハードウェアの新しいエンドポイントが自動的に検出され、デフォルト値に基づいて構成されます。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［**More Tasks**］ > ［**Endpoints**］ > ［**Delete**］を選択します。
3. ［Delete Endpoints］ダイアログで、リストから 1 つ以上のエンドポイントを選択して、［**Next**］を選択します。エンドポイントが使用中の場合、それを削除するとシステムが停止する可能性がある旨を示すメッセージが表示されます。
4. ［**Next**］を選択して、タスクを完了します。

イニシエーターの追加

イニシエーターを追加して、FC（ファイバー チャネル）プロトコルを使用してデータの読み取りと書き込みを行うシステムに接続するバックアップ クライアントを提供します。特定のイニシエータでは、FC 経由の DD Boost または DD VTL のいずれかをサポートできますが、両方はサポートできません。1 つの DD システムに対して最大 1024 のイニシエーターを構成できます。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［Initiators］の下の［Add］（+記号）を選択します。
3. ［Add Initiator］ダイアログに、指定された形式でポートの一意の WWPN を入力します。
4. イニシエーターの名前を入力します。
5. ［Address Method］を選択します。［**Auto**］は標準アドレス指定に使用されます。［**VSA**］（ボリューム セット アドレス指定）は、主に仮想バス、ターゲット、LUN のアドレス指定に使用されます。
6. ［**OK**］を選択します。

   ［**CLI** 相当］

   ```
   # scsitarget group add My_Group initiator My_Initiator
   ```

イニシエーターの変更または削除

イニシエーターを削除するには、オフラインにして、グループにはアタッチしないようにする必要があります。そうしなければ、エラー メッセージが表示され、イニシエーターは削除されません。アクセス グループを削除する前に、アクセス グループ内のすべてのイニシエーターを削除する必要があります。イニシエーターが認識可能のままである場合、それは自動的に再検出される可能性があります。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［Initiators］で、いずれかのイニシエーターを選択します。削除する場合は、［Delete］（X）を選択します。変更する場合は、［Modify］（鉛筆）を選択して、［Modify Initiator］ダイアログを表示します。
3. イニシエーターの名前/アドレス方法を変更します。［**Auto**］は標準アドレス指定に使用されます。［**VSA**］（ボリューム セット アドレス指定）は、主に仮想バス、ターゲット、LUN のアドレス指定に使用されます。

4. ［**OK**］を選択します。

［イニシエーター エイリアスの設定の推奨事項（**CLI** のみ）］
構成プロセス中に混乱やヒューマン エラーを軽減するために、イニシエーター エイリアスを設定することを強くお勧めします。

```
# vtl initiator set alias NewAliasName wwpn 21:00:00:e0:8b:9d:0b:e8
# vtl initiator show
Initiator  Group    Status   WWNN                     WWPN                     Port
---------  -------  -------  -----------------------  -----------------------  ---
NewVTL     aussie1  Online   20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6a
                    Offline  20:00:00:e0:8b:9d:0b:e8  21:00:00:e0:8b:9d:0b:e8  6b

Initiator  Symbolic Port Name  Address Method
---------  ------------------  --------------
NewVTL                              auto
---------  ------------------  --------------
```

ハード アドレス（ループ ID）の設定

一部のバックアップ ソフトウェアでは、すべてのプライベート ループ ターゲットが他のノードと競合しないハード アドレス（ループ ID）があることを必要とします。ループ ID の範囲は、0～125 です。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［**More Tasks**］ > ［**Set Loop ID**］を選択します。
3. ［Set Loop ID］ダイアログで、ループ ID（0～125）を入力し、［**OK**］を選択します。

フェイルオーバー オプションの設定

NPIV が有効な場合、自動フェイルオーバーおよびフェイルバックのオプションを設定できます。

アプリによるファイバー チャネル ポートのフェイルオーバーで予想される動作は次のとおりです。

- DDD Boost-over-Fibre Channel 操作では、ファイバー チャネルのエンドポイント フェイルオーバーに、ユーザーの介入は不要の状態が続くと予想されます。
- DD VTL Fibre Channel 操作は、DD VTL ファイバーチャネルのエンドポイント フェールオーバーで中断されることが予想されます。影響を受けるファイバーチャネル エンドポイントを使用して、イニシエータで、検出（オペレーティング システム検出と DD VTL デバイスの構成）の実行が必要になる場合があります。アクティブなバックアップを再度開始して、操作をリストアすることが予想されます。
- vDisk Fibre Channel 操作では、ファイバー チャネルのエンドポイント フェイルオーバーに、ユーザーの介入は不要の状態が続くと予想されます。

すべてのポートが無効化され、続いて有効化される場合（管理者によってトリガーされる可能性がある）、ポートを有効化する順番は指定されていないため、自動フェイルバックは保証されません。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［ **Resources**］を選択します。
2. ［**More Tasks**］ > ［**Set Failover Options**］を選択します。
3. ［Set Failover Options］ダイアログで、フェイルオーバーおよびフェイルバックの遅延を秒単位で入力し、自動フェイルバックを有効にするかどうかを指定して、［**OK**］を選択します。

［Access Groups］タブ

［**Hardware**］ > ［**Fibre Channel**］ > ［**Access Groups**］タブには、DD Boost および DD VTL アクセス グループに関する情報が表示されます。［View DD Boost Groups］または［View VTL Groups］へのリンクを選択すると、DD Boost または DD VTL のページが表示されます。

表 126 Access Groups

項目	説明
グループ名	アクセス グループの名前。
サービス	このアクセス グループのサービス：DD Boost または DD VTL のいずれか。
Endpoints	このアクセス グループと関連づけられているエンドポイント。
Initiators	このアクセス グループに関連づけられたイニシエーター。
デバイス数	このアクセス グループに関連づけられたデバイスの数。

DD OS バージョンでの FC リンク モニタリングの違い

さまざまな DD OS のリリースが、さまざまな方法で FC（ファイバー チャネル）リンク モニタリングを処理します。

DD OS 5.3 以降
ポート モニタリングは、システム起動時に FC ポートを検出し、ポートが有効であるがオフラインの場合にアラートを出します。アラートをクリアするには、`scsitarget port` コマンドを使用して未使用のポートを無効化します。

DD OS 5.1～5.3
ポートがオフラインの場合、アラートによってリンクがダウンしていることが通知されます。アラートは管理されているため、クリアされるまでアクティブなままとなります。DD VTL FC ポートがオンラインであるか、無効になっている場合に、アラートが出されます。ポートが使用中ではない場合は、監視する必要がないのであれば無効化します。

DD OS 5.0～5.1
ポートがオフラインの場合、アラートによってリンクがダウンしていることが通知されます。アラートが管理されていないため、アクティブにならず、現在のアラート リストには表示されません。ポートがオフラインの場合、アラートによってリンクが起動していることが通知されます。ポートが使用中ではない場合は、監視する必要がないのであれば無効化します。

DD OS 4.9～5.0
FC ポートは、監視される DD VTL グループに含まれている必要があります。

第 14 章

DD Boost の扱い

本章には、次のセクションが含まれます。

- Data Domain Boost 330
- DD System Manager による DD Boost の管理 331
- インターフェイス グループについて 346
- DD Boost の破棄 353
- DD Boost over Fibre Channel の構成 354
- HA システムで DD Boost を使用 358
- ［DD Boost］タブについて 359

Data Domain Boost

DD Boost（Data Domain Boost）は、バックアップ アプリケーションとエンタープライズ アプリケーションとの高度な統合を実現して、パフォーマンスと使いやすさを向上させます。DD Boost は、重複排除プロセスの一部をバックアップ サーバーまたはアプリケーション クライアントに分散させることで、クライアント側の重複排除を高速にし、バックアップとリカバリの効率を向上させます。

DD Boost はオプション製品であり、Data Domain システムで実行するには別途ライセンスが必要です。Data Domain システムの DD Boost ソフトウェア ライセンス キーは、Data Domain から直接購入できます。

注

特別なライセンス「BLOCK-SERVICES-PROTECTPOINT」によって、ProtectPoint ブロック サービスを使用するクライアントは、DD Boost のライセンスなしでも DD Boost 機能を使用できるようになります。DD Boost が ProtectPoint クライアントのみで有効な（つまり、BLOCK-SERVICES-PROTECTPOINT ライセンスのみがインストールされている）場合、DD Boost が ProtectPoint のみで有効であることはライセンスのステータスで分かります。

DD Boost には、バックアップ サーバー上で動作するコンポーネントと Data Domain システム上で動作するコンポーネントの 2 つのコンポーネントが存在します。

- NetWorker バックアップ アプリケーションのコンテキストでは、Avamar バックアップ アプリケーション、その他の DD Boost パートナー バックアップ アプリケーション、バックアップ サーバ（DD Boost ライブラリ）で動作するコンポーネントは、特定のバックアップ アプリケーションに統合されます。
- Symantec バックアップ アプリケーション（NetBackup と Backup Exec）と Oracle RMAN プラグインのコンテキストでは、各メディア サーバーにインストールされている DD Boost プラグインの適切なバージョンをダウンロードする必要があります。DD Boost プラグインには、Data Domain システムで動作する DD Boost サーバーとの統合用の DD Boost ライブラリーが含まれます。

バックアップ アプリケーション（Avamar、NetWorker、NetBackup、Backup Exec など）は、バックアップと複製が実行される時間を制御するポリシーを設定します。管理者は、単一のコンソールからバックアップ、複製、リストアを管理し、WAN 効率の良い Replicator ソフトウェアを含む、DD Boost のあらゆる機能を使用できます。アプリケーションは、カタログ内のすべてのファイル（データの集まり）を管理し、それらには Data Domain システムによって作成されたものも含まれます。

Data Domain システムでは、作成するストレージ ユニットは DD Boost プロトコルを使用するバックアップ アプリケーションに公開されます。Symantec アプリケーションの場合、ストレージ ユニットはディスク プールとして認識されます。NetWorker の場合、ストレージ ユニットは LSU（論理ストレージ ユニット）として認識されます。ストレージ ユニットは MTree であるため、MTree クォータ設定に対応しています （ストレージ ユニットの代わりに MTree を作成しないでください）。

本章には、インストール手順は含まれません。インストールしたい製品のドキュメントを参照してください。たとえば、Symantec バックアップ アプリケーション（NetBackup と Backup Exec）を使用した DD Boost のセットアップの情報については、「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。他のアプリケーションを使用した DD Boost のセットアップの情報については、アプリケーション固有のドキュメントを参照してください。

Data Domain システム上での DD Boost の構成と管理について、追加の詳細は、「Data Domain Boost for OpenStorage 管理ガイド」（NetBackup および Backup Exec）と「EMC Data Domain Boost for Partner Integration 管理ガイド」（その他のバックアップ アプリケーション）を参照してください。

DD System Manager による DD Boost の管理

DD System Manager の［DD Boost］ビューにアクセスします。

手順

1. ［**Data Management**］ > ［**File System**］を選択します。この状態をチェックして、ファイル システムが有効で実行されていることを確認します。
2. ［**Protocols**］ > ［**DD Boost**］を選択します。

   ライセンスなしで［DD Boost］ページを表示した場合、［Status］には DD Boost がライセンスされていない旨が表示されます。［**Add License**］をクリックし、［Add License Key］ダイアログ ボックスに有効なライセンスを入力します。

   注

   特別なライセンス「BLOCK-SERVICES-PROTECTPOINT」によって、ProtectPoint ブロック サービスを使用するクライアントは、DD Boost のライセンスなしでも DD Boost 機能を使用できるようになります。DD Boost が ProtectPoint クライアントのみで有効な場合、すなわち、BLOCK-SERVICES-PROTECTPOINT ライセンスのみがインストールされている場合は、ライセンスのステータスによって DD Boost が ProtectPoint のみで有効であることが分かります。

   ［DD Boost］タブ（［Settings］、［Active Connections］、［IP Network］、［Fibre Channel］、［Storage Units］）を使用して、DD Boost を管理します。

DD Boost ユーザー名の指定

DD Boost ユーザーは DD OS ユーザーでもあります。既存の DD OS ユーザー名を選択するか、新しい DD OS ユーザー名を作成し、その名前を DD Boost ユーザー名にして、DD Boost ユーザーを指定します。

バックアップ アプリケーションが、Data Domain システムに接続する DD Boost ユーザー名およびパスワードを使用します。このシステムに接続する各バックアップ サーバーに関する認証情報を構成する必要があります。Data Domain システムは、複数の DD Boost ユーザーに対応しています。Symantec NetBackup と Backup Exec による DD Boost のセットアップの詳細については、「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。他アプリケーションを使用した DD Boost の設定について、詳細は「Data Domain Boost for Partner Integration 管理ガイド」と、アプリケーション付属のドキュメントを参照してください。

手順

1. ［**Protocols**］ > ［**DD Boost**］を選択します。
2. DD Boost アクセス リストから、ユーザーの上の［**Add**］（［+］）を選択します。

   ［Add User］ダイアログが表示されます。

3. 既存のユーザーを選択するには、ドロップダウン リストでユーザー名を選択します。

   管理役割権限が［none］に設定されたユーザー名を選択することを推奨します。

4. 新しいユーザーを作成および選択するには、［**Create a new Local User**］を選択し、次の手順を行います。

   a. ［User］フィールドに新しいユーザー名を入力します。

ユーザーは、Data Domain システムに接続するバックアップ アプリケーションで構成する必要があります。

b. 適切なフィールドにパスワードを 2 回入力します。

5. ［**Add**］をクリックします。

DD Boost ユーザー パスワードの変更

DD Boost ユーザー・パスワードを変更します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］を選択します。
2. ［DD Boost Access］リストの［Users］からユーザーを選択します。
3. DD Boost ユーザー リストで［**Edit**］ボタン（鉛筆アイコン）をクリックします。

   ［Change Password］ダイアログが表示されます。

4. 適切なボックスにパスワードを 2 回入力します。
5. ［変更］をクリックします。

DD Boost ユーザー名の削除

DD Boost アクセス リストからユーザーを削除します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］を選択します。
2. ［DD Boost Access］リストの［Users］で、削除する必要があるユーザーを選択します。
3. DD Boost ユーザー リストで［**Remove**］（［X］）をクリックします。

   ［Remove User］ダイアログが表示されます。

4. ［**Remove**］をクリックします。

   削除後、ユーザーは DD OS アクセス リストに残ります。

DD Boost の有効化

［DD Boost Settings］タブを使用して、DD Boost を有効にし、DD Boost ユーザーを選択または追加します。

手順

1. ［**Protocols**］ > ［**DD Boost**］を選択します。
2. ［DD Boost Status］領域で、［**Enable**］をクリックします。

   ［Enable DD Boost］ダイアログ ボックスが表示されます。

3. メニューから既存のユーザー名を選択するか、名前、パスワード、役割を与えて新しいユーザーを追加します。

Kerberos の構成

Kerberos を構成するには、［DD Boost Settings］タブを使用します。

手順

1. ［**Protocols > DD Boost > Settings**］を選択します。
2. ［Kerberos Mode］ステータス領域で［**Configure**］をクリックします。

   ［**Administration > Access**］の下に［Authentication］タブが表示されます。

   注

   また、System Manager で［**Administration > Access**］の下の［Authentication］タブに直接移動して Kerberos を有効にすることもできます。
3. ［Active Directory/Kerberos Authentication］で、［**Configure**］をクリックします。

   ［Active Directory/Kerberos Authentication］ダイアログ ボックスが表示されます。
   使用する Kerberos KDC（キー配布センター）のタイプを選択します。

   - ［**Disabled**］

     注

     ［**Disabled**］を選択すると、NFS クライアントは Kerberos 認証を使用しません。CIFS クライアントは Workgroup 認証を使用します。
   - ［**Windows/Active Directory**］

     注

     Active Directory 認証用のレルム名、ユーザー名、パスワードを入力します。
   - ［**UNIX**］
     a. 1～3 台の KDC サーバのレルム名、IP アドレス/ホスト名を入力します。
     b. いずれかの KDC サーバからキータブ ファイルをアップロードします。

DD Boost の無効化

DD Boost を無効化すると、バックアップ サーバーへのアクティブな接続がすべてドロップします。DD Boost を無効化または破棄すると、DD Boost FC サービスも破棄されます。

はじめに

無効化する前に、バックアップ アプリケーションから実行されているジョブがないことを確認します。

注

2 つの Data Domain リストア間で DD Boost によって開始されたファイル レプリケーションはキャンセルされません。

手順

1. ［**Protocols**］ > ［**DD Boost**］を選択します。
2. ［DD Boost Status］領域で、［**Disable**］をクリックします。
3. ［Disable DD Boost］確認ダイアログ ボックスで、［**OK**］をクリックします。

DD Boost ストレージ ユニットの表示

［Storage Units］タブにアクセスして、DD Boost ストレージ ユニットの表示と管理を行います。

［DD Boost Storage Unit］タブ

- ストレージ ユニットをリストし、各ストレージ ユニットの次の情報を表示します。

表 127 ストレージ ユニットの情報

項目	説明
Storage Unit	ストレージ ユニットの名前。
ユーザー	ストレージ ユニットを所有する DD Boost ユーザー。
Quota Hard Limit	使用されたハード制限クォータの割合。
Last 24 hr Pre-Comp	過去 24 時間に書き込まれたバックアップアプリケーションから取得した未フォーマットのデータの量。
Last 24 hr Post-Comp	過去 24 時間の圧縮後に使用されたストレージの量。
Last 24 hr Comp Ratio	過去 24 時間の圧縮率。
Weekly Avg Post-Comp	過去 5 週間に使用された圧縮ストレージの平均量。
Last Week Post-Comp	過去 7 日間に使用された圧縮ストレージの平均量。
Weekly Avg Comp Ratio	過去 5 週間の平均圧縮率。
Last Week Comp Ratio	過去 7 日間の平均圧縮率。

- ストレージ ユニットの作成、変更、削除が可能。
- リストから選択されたストレージ ユニットの 4 つの関連タブ （Storage Unit、Space Usage、Daily Written、Data Movement）を表示します。

  注

  ［Data Movement］タブは、オプションの Data Domain Extended Retention（旧 DD Archiver）か DD Cloud Tier（Data Domain Cloud Tier）のライセンスがインストールされている場合のみ使用可能です。

- ［**View DD Boost Replications**］リンクをクリックすると、［**Replication**］ > ［**On-Demand**］ > ［**File Replication**］に移動します。

  注

  DD Replicator ライセンスは、DD Boost が［File Replication］タブ以外のタブを表示するために必要です。

ストレージ ユニットの作成

Data Domain システムで 1 つ以上のストレージ ユニットを作成する必要があります。DD Boost ユーザーは、そのストレージ ユニットに割り当てる必要があります。［Storage Units］タブを使用して、ストレージ ユニットを作成します。

各ストレージ ユニットは、`/data/col1` ディレクトリの最上位サブディレクトリであす。ストレージ ユニット間の階層はありません。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Storage Units**］を選択します。
2. ［**Create**］（+）をクリックします。

   ［Create Storage Unit］ダイアログが表示されます。

3. ［Name］ボックスにストレージ ユニット名を入力します。

   各ストレージ ユニット名は一意でなければなりません。ストレージ ユニット名には 50 文字まで指定できます。次の文字が使用できます。

   - 大文字および小文字の英字：A～Z、a～z
   - 数字：0～9
   - 組み込みスペース

     注

     名前に埋め込みスペースがある場合、ストレージ ユニット名は二重引用符（"）で囲む必要があります。

   - カンマ（,）
   - ピリオド（.）（名前の先頭には使用できません）
   - 感嘆符（!）
   - シャープ記号（#）
   - ドル記号（$）
   - パーセンテージ記号（%）
   - プラス記号（+）
   - アットマーク（@）
   - 等号記号（=）
   - アンパサンド（&）
   - セミコロン（;）
   - 括弧（(と)）
   - 角括弧（[と]）
   - 中括弧（{と}）
   - キャレット（^）
   - チルダ（~）
   - アポストロフィ（傾斜していない一重引用符）
   - 傾斜した一重引用符（‘）
   - マイナス記号（-）
   - アンダースコア（_）

4. このストレージ ユニットへのアクセス権を持つ既存のユーザー名を選択するには、ドロップダウン リストでユーザー名を選択します。

   管理役割権限が［none］に設定されたユーザー名を選択することを推奨します。

5. このストレージ ユニットへのアクセス権を持つ新しいユーザー名を作成および選択するには、［**Create a new Local User**］を選択し、

   a. ［User］ボックスに新しいユーザー名を入力します。

      ユーザーは、Data Domain システムに接続するバックアップ アプリケーションで構成する必要があります。

b. 適切なボックスにパスワードを 2 回入力します。

6. ストレージ ユニットが過剰なスペースを消費することを防ぐため、ストレージ領域制限を設定します。ソフト制限かハード制限のクォータ設定、またはハード制限とソフト制限の両方を設定します。ソフト制限の場合、ストレージ ユニット サイズが制限を超えるとアラートが送信されますが、データの書き込みは可能です。ハード制限に達すると、データをストレージ ユニットに書き込めません。

   注

   クォータ制限は圧縮前の値です。クォータ制限を設定するには、[**Set to Specific value**] を選択し、値を入力します。測定単位を MiB、GiB、TiB、PiB から選択します。

   注

   ソフト制限とハード制限両方を設定する場合、クォータのソフト制限はクォータのハード制限を超えることはできません。

7. [**Create**] をクリックします。
8. Data Domain Boost が有効なシステムそれぞれに前述のステップを繰り返します。

ストレージ ユニット情報の表示

[DD Boost Storage Units] タブから、ストレージ ユニットを選択し、選択したストレージ ユニットの [Storage Unit]、[Space Usage]、[Daily Written]、[Data Movement] タブにアクセスできます。

[Storage Unit] タブ

[Storage Unit] タブには、[Summary] および [Quota] パネルに選択されたストレージ ユニットの詳細が表示されます。[Snapshot] パネルにはスナップショットの詳細が表示され、新しいスナップショットとスケジュールを作成でき、[**Data Management**] > [**Snapshots**] タブへのリンクがあります。

- [Summary] パネルには、選択されたストレージ ユニットの要約情報が表示されます。

  表 128 [Summary] パネル

Summary 項目	説明
Total Files	ストレージ ユニット上のファイル イメージの総数。ログ ファイルにダウンロードできる圧縮の詳細については、[Download Compression Details] リンクをクリックします。生成には最大数分かかります。完了したら、[Download] をクリックします。
Full Path	`/data/col1/filename`
Status	R：読み取り、W：書き込み、Q：定義済みクォータ
Pre-Comp Used	使用済み圧縮前ストレージの量。

- [Quota] パネルには、選択されたストレージ ユニットのクォータ情報が表示されます。

表 129 ［Quota］パネル

Quota 項目	説明
Quota Enforcement	有効または無効。［Quota］をクリックすると、［**Data Management**］ > ［**Quota**］タブに移動し、そこでクォータを構成できます。
Pre-Comp Soft Limit	ストレージ ユニットに設定されたソフト クォータの現在の値。
Pre-Comp Hard Limit	ストレージ ユニットに設定されたハード クォータの現在の値。
Quota Summary	使用されたハード制限の割合。

タブに表示される圧縮前ソフトおよびハード制限を変更する手順：

1. ［Quota］パネルの［**Quota**］リンクをクリックします。
2. ［Configure Quota］ダイアログ ボックスで、ハード/ソフト クォータを入力し、単位を MiB、GiB、TiB、PiB から選択します。［**OK**］をクリックします。

- スナップショット
［Snapshots］パネルには、ストレージ ユニットのスナップショットの詳細が表示されます。

表 130 ［Snapshots］パネル

項目	説明
スナップショットの総数	この MTree に作成されたスナップショットの総数。各 MTree に、計 750 個のスナップショットを作成できます。
期限切れ	作成対象としてマークされたが、まだクリーニング操作で削除されていない、この MTree 内のスナップショットの数。
Unexpired	保持対象としてマークされている、この MTree 内のスナップショットの数。
最も古いスナップショット	この MTree の最も古いスナップショットの日付。
Newest Snapshot	この MTree の最も新しいスナップショットの日付。
Next Scheduled	次にスケジュール設定されたスナップショットの日付。
Assigned Snapshot Schedules	この MTree に割り当てられたスナップショット スケジュールの名前。

［Shapshots］パネルを使用すると、以下を実行できます。

- スナップショット スケジュールを選択されたストレージ ユニットに割り当てます。［**Assign Schedules**］をクリックします。スケジュールのチェックボックスを選択し、［**OK**］と［**Close**］をクリックします。
- 新しいスケジュールを作成する手順：［**Assign Snapshot Schedules**］ > ［**Create Snapshot Schedule**］をクリックします。新しいスケジュールの名前を入力してください

注

スナップショットの名前は、文字、数字、_、-、%d（日付を示す数字：01～31）、%a（曜日の略称）、%m（月を示す数字：01～12）、%b（月名の略称）、%y（2 桁の年）、%Y（4 桁の年）、%H（時間：00～23）、%M（分：00～59）から、ダイアログ ボックスに表示されるパターンに従って構成できます。新しいパターンを入力し、［**Validate Pattern & Update Sample**］をクリックします。［次へ］をクリックします。

- スケジュールを実行する日付を選択します。毎週、毎日（または選択された日）、カレンダーでクリックして選択した特定の日付で毎月、または月末から選択します。［次へ］をクリックします。
- スケジュールを実行する時刻を入力します。［At Specific Times］または［In Intervals］を選択します。特定の時刻を選択する場合、リストから時刻を選択します。［Add］（［**+**］）をクリックして新しい時刻（24 時間形式）を追加します。間隔の場合、［In Intervals］を選択し、開始時間と終了時間および 8 時間ごとなどの頻度（Every）を設定します。［次へ］をクリックします。
- スナップショットの保存期間を日、月、または年単位で入力します。［次へ］をクリックします。
- 構成の Summary を確認します。値を編集する場合は［**Back**］をクリックします。［**Finish**］をクリックしてスケジュールを作成します。

- ［Snapshots］リンクをクリックすると、［**Data Management**］ > ［**Snapshots**］タブに移動します。

［Space Usage］タブ

［Space Usage］タブには、ストレージ ユニットのデータ使用量の推移を視覚的に表示するグラフが含まれています。

- グラフの線上のポイントにカーソルを合わせると、そのポイントのデータを含むボックスが表示されます。
- 標準の［**Print**］ダイアログ ボックスを開くには、グラフの下部にある［Print］をクリックします。
- 新しいブラウザ ウィンドウでグラフを表示するには、［**Show in new window**］をクリックします。

表示されるグラフ データのタイプは、［Logical Space Used (Pre-Compression)］と［Physical Capacity Used (Post-Compression)］の 2 つです。

［Daily Written］タブ

［Daily Written］ビューには、7 日から 120 日の間で選択できる期間にわたって、システムに書き込まれたデータを日単位で視覚的に表示するグラフが含まれています。データ量は、圧縮前と圧縮後について時系列に表示されます。

［Data Movement］タブ

アーカイブ ライセンスが有効になっている場合に、DD Extended Retention ストレージ エリアに移されたディスク領域の量を表示する Daily Written グラフと同じ形式のグラフ（DD Extended Retention ライセンスが有効な場合）。

ストレージ ユニットの変更

［Modify Storage Unit］ダイアログを使用して、ストレージ ユニットの名称変更、異なる既存ユーザーの選択、新規ユーザーの作成と選択、クォータ設定の編集を行います。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Storage Units**］を選択します。
2. ［Storage Unit］リストで、変更するストレージ ユニットを選択します。
3. 鉛筆アイコンをクリックします。

   ［Modify Storage Unit］ダイアログが表示されます。

4. ストレージ ユニットの名称を変更するには、［**Name**］フィールドでテキストを編集します。
5. 別の既存のユーザーを選択するには、ドロップダウン リストでユーザー名を選択します。

   管理役割権限が［none］に設定されたユーザー名を選択することを推奨します。

6. 新しいユーザーを作成および選択するには、［**Create a new Local User**］を選択し、次の手順を行います。
   a. ［User］ボックスに新しいユーザー名を入力します。

      ユーザーは、Data Domain システムに接続するバックアップ アプリケーションで構成する必要があります。

   b. 適切なボックスにパスワードを 2 回入力します。
7. 必要に応じて Quota Settings を編集します。

   ストレージ ユニットが過剰なスペースを消費することを防ぐため、ストレージ領域制限を設定します。ソフト制限かハード制限のクォータ設定、またはハード制限とソフト制限の両方を設定します。ソフト制限の場合、ストレージ ユニット サイズが制限を超えるとアラートが送信されますが、データの書き込みは可能です。ハード制限に達すると、データをストレージ ユニットに書き込めません。

   注

   クォータ制限は圧縮前の値です。クォータ制限を設定するには、［**Set to Specific value**］を選択し、値を入力します。測定単位を MiB、GiB、TiB、PiB から選択します。

   注

   ソフト制限とハード制限両方を設定する場合、クォータのソフト制限はクォータのハード制限を超えることはできません。

8. ［変更］をクリックします。

ストレージ ユニットの名称変更

［Modify Storage Unit］ダイアログを使用して、ストレージ ユニットを名称変更します。

ストレージ ユニットを名称変更すると、そのストレージ ユニットの名称は変更されますが、以下の内容は保持されます。

- ユーザー名の所有権
- ストリーム リミットの構成
- 容量クォータの構成と報告された物理的なサイズ
- ローカル Data Domain システム上の AIR の関連づけ

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Storage Units**］に移動します。
2. ［Storage Unit］リストで、名称変更するストレージ ユニットを選択します。
3. 鉛筆アイコンをクリックします。

   ［Modify Storage Unit］ダイアログが表示されます。

4. ［**Name**］フィールドのテキストを編集します。
5. ［変更］をクリックします。

ストレージ ユニットの削除

［Storage Units］タブを使用して、Data Domain システムからストレージ ユニットを削除します。ストレージ ユニットを削除すると、ストレージ ユニットとそのストレージ ユニットに含まれているすべてのイメージが Data Domain システムから削除されます。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Storage Units**］を選択します。
2. リストから削除するストレージ ユニットを選択します。
3. ［Delete］（［**X**］）をクリックします。
4. ［**OK**］をクリックします。

結果

Data Domain システムからそのストレージ ユニットが削除されます。対応するバックアップ アプリケーション カタログ エントリーも削除する必要があります。

ストレージ ユニットの復元

［Storage Units］タブを使用して、ストレージ ユニットを復元します。

ストレージ ユニットを復元すると、以下の内容とともに、以前削除されたストレージ ユニットがリカバリされます。

- ユーザー名の所有権
- ストリーム リミットの構成
- 容量クォータの構成と報告された物理的なサイズ
- ローカル Data Domain システム上の AIR の関連づけ

注

削除されたストレージ ユニットは、`filesys clean` コマンドが次に実行されるまで使用できます。

手順

1. ［**Protocols**］>［**DD Boost**］>［**Storage Units**］>［**More Tasks**］>［**Undelete Storage Unit...**］を選択します。
2. ［Undelete Storage Units］ダイアログ ボックスで、復元するストレージ ユニット（複数可）を選択します。
3. ［**OK**］をクリックします。

DD Boost オプションの選択

［Set DD Boost Options］ダイアログを使用して、分散セグメント処理、仮想合成、ファイル レプリケーション用の低帯域幅の最適化、ファイル レプリケーション暗号化、ファイル レプリケーション ネットワーク環境設定（IPv4 または IPv6）の設定を指定します。

手順

1. DD Boost のオプション設定を表示するには、［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］ > ［**Advanced Options**］を選択します。
2. 設定を変更するには、［**More Tasks**］ > ［**Set Options**］を選択します。

   ［Set DD Boost Options］ダイアログが表示されます。
3. 有効化するオプションを選択します。
4. 無効化するオプションを選択解除します。

   File Replication Network Preference オプションを選択解除するには、他のオプションを選択します。
5. DD Boost のセキュリティ オプションを設定します。
   a. ［**Authentication Mode**］を選択します。
      - None
      - Two-way
      - Two-way Password
   b. ［**Encryption Strength**］を選択します。
      - None
      - Medium
      - High

   Data Domain システムは、グローバル認証モードおよび暗号化の強度を、クライアントごとの認証モードおよび暗号化の強度と比較して、有効な認証モードおよび認証の暗号化の強度を計算します。システムでは、あるエントリーによる最高の認証モードを使用しながら、別のエントリーによる最高の暗号化の設定を使用することはしません。有効な認証モードと暗号化の強度は、最高の認証モードを提供する単一のエントリーから採用されます。
6. ［**OK**］をクリックします。

注

`ddboost option` コマンドを介して、分散セグメント処理を管理することもできます。その詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

分散セグメント処理

分散セグメント処理を実行すると、メディア サーバーと Data Domain システム間の重複データ転送がなくなり、ほとんどの場合、バックアップ スループットが増えます。

`ddboost option` コマンドを介して、分散セグメント処理を管理することができます。その詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

注

分散セグメント処理は、デフォルトでは Data Domain Extended Retention（旧 Data Domain Archiver）構成によって有効になっており、無効化できません。

仮想合成

仮想合成フル バックアップは、最後に実施されたフル バックアップ（統合またはフル）とそれ以降のすべての増分バックアップの組み合わせです。仮想合成はデフォルトで有効になっています。

低帯域幅の最適化

WAN（低帯域幅ネットワーク）でファイル レプリケーションを使用している場合、低帯域幅の最適化を使用してレプリケーション速度を上げることができます。この機能によって、データ転送中に追加の圧縮ができます。低帯域幅の圧縮は、Replication ライセンスがインストールされた Data Domain システムで使用可能です。

低帯域幅の最適化は、デフォルトでは無効化されており、統合帯域幅が 6 Mbps 未満のネットワークで使用するよう設計されています。最大限のファイル システム ライト パフォーマンスが必要な場合は、このオプションを使用しないでください。

注

`ddboost file-replication` コマンドを介して、低帯域幅の最適化を管理することもできます。その詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

ファイル レプリケーション暗号化

DD Boost ファイル レプリケーション暗号化オプションを有効にして、データ レプリケーション ストリームを暗号化できます。

注

DD Boost ファイル レプリケーション暗号化は、Data at Rest オプションを指定せずにシステムで使用されている場合、ソースおよびデスティネーション システムの両方でオンに設定する必要があります。

管理ファイル レプリケーション TCP ポートの設定

DD Boost 管理ファイル レプリケーションの場合、ソースおよびターゲット Data Domain システムの両方で同じグローバル リスン ポートを使用します。リスン ポートを設定するには、「Data Domain オペレーティング システム コマンド リファレンス ガイド」の説明に従い、`replication option` コマンドを使用します。

ファイル レプリケーション ネットワーク環境設定

このオプションを使用して、DD Boost ファイル レプリケーションの優先ネットワーク タイプを IPv4 または IPv6 に設定します。

DD Boost の証明書の管理

ホスト証明書によって、接続の確立時に DD Boost クライアント プログラムによるシステム ID の検証が可能になります。CA 証明書によって、システムによって信頼される必要がある証明機関が識別されます。このセクションのトピックでは、DD Boost のホスト証明書と CA 証明書の管理方法について説明します。

DD Boost のホスト証明書の追加

システムにホスト証明書を追加します。DD OS は、DD Boost の 1 つのホスト証明書に対応しています。

手順

1. ホスト証明書をまだ要求していない場合、トラステッド CA にホスト証明書を要求します。
2. ホスト証明書を受け取ったら、DD Service Manager を実行するコンピューターにコピーまたは移動します。
3. ホスト証明書を追加したいシステムで DD System Manager を起動します。

   注

   DD System Manager は、管理システム（DD System Manager を実行しているシステム）でのみ証明書管理に対応しています。

4. ［**Protocols**］ > ［**DD Boost**］ > ［**More Tasks**］ > ［**Manage Certificates...**］を選択します。

   注

   管理対象システム上の証明書をリモートで管理しようとすると、DD System Manager は証明書管理ダイアログの上部に参考メッセージが表示されます。システムの証明書を管理するには、そのシステムで DD System Manager を起動する必要があります。

5. ［Host Certificate］領域で、［**Add**］をクリックします。
6. .p12 ファイルに組み込まれたホスト証明書を追加するには、次の手順を行います。
   a. ［**I want to upload the certificate as a .p12 file**］を選択します。
   b. ［**Password**］ボックスにパスワードを入力します。
   c. ［**Browse**］をクリックして、システムにアップロードするホスト証明書ファイルを選択します。
   d. ［**Add**］をクリックします。
7. .pem ファイルに組み込まれたホスト証明書を追加するには、次の手順を行います。
   a. ［**I want to upload the public key as a .pem file and use a generated private key**］を選択します。
   b. ［**Browse**］をクリックして、システムにアップロードするホスト証明書ファイルを選択します。
   c. ［**Add**］をクリックします。

DD Boost の CA 証明書の追加

トラステッド CA の証明書をシステムに追加します。DD OS は、トラステッド CA の複数の証明書に対応しています。

手順

1. トラステッド CA の証明書を取得します。
2. DD Service Manager を実行するコンピューターにトラステッド CA 証明書をコピーまたは移動します。
3. CA 証明書を追加するシステムで DD System Manager を起動します。

注

DD System Manager は、管理システム（DD System Manager を実行しているシステム）でのみ証明書管理に対応しています。

4. ［**Protocols**］ > ［**DD Boost**］ > ［**More Tasks**］ > ［**Manage Certificates...**］を選択します。

注

管理対象システム上の証明書をリモートで管理しようとすると、DD System Manager は証明書管理ダイアログの上部に参考メッセージが表示されます。システムの証明書を管理するには、そのシステムで DD System Manager を起動する必要があります。

5. ［CA Certificates］領域で、［**Add**］をクリックします。

   ［Add CA Certificate for DD Boost］ダイアログが表示されます。

6. .pem ファイルに組み込まれた CA 証明書を追加するには、次の手順を行います。
   a. ［**I want to upload the certificate as a .pem file**］を選択します。
   b. ［**Browse**］をクリックして、システムにアップロードするホスト証明書ファイルを選択し、［**Open**］をクリックします。
   c. ［**Add**］をクリックします。
7. コピー アンド ペーストを使用して CA 証明書を追加するには、次の手順を行います。
   a. オペレーティング システムのコントロールを使用して、証明書テキストをクリップボードにコピーします。
   b. ［**I want to copy and paste the certificate text**］を選択します。
   c. コピー アンド ペーストの選択の下にあるボックスに証明書テキストをペーストします。
   d. ［**Add**］をクリックします。

DD Boost クライアントのアクセスと暗号化の管理

［DD Boost Settings］タブを使用して、Data Domain システムとの DD Boost 接続を確立できる特定のクライアントまたは一連のクライアント、クライアントで暗号化が使用されるかどうかを構成します。デフォルトでは、すべてのクライアントが暗号化を使用しないでアクセスできるようにシステムが構成されます。

注

未了（in-flight）の暗号化を有効にすると、システム パフォーマンスに影響を及ぼします。

注

DD Boost では、MITM（中間者攻撃）からシステムを守るためのグローバル認証と暗号化オプションを利用できます。Data Domain システムで GUI を使用するか、CLI コマンドを使用して、認証と暗号化の設定を指定します。詳細については、「Data Domain Boost for OpenStorage 3.4 管理ガイド」、および DD Boost クライアントの追加（345 ページ）または「Data Domain 6.1 コマンド リファレンス ガイド」を参照してください。

DD Boost クライアントの追加

許可された DD Boost クライアントを作成して、そのクライアントで暗号化が使用されるかどうかを指定します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］を選択します。
2. ［Allowed Clients］セクションで、［**Create (+)**］をクリックします。

   ［Add Allowed Client］ダイアログが表示されます。

3. クライアントのホスト名を入力します。

   ホスト名には、完全修飾ドメイン名（host1.emc.com など）またはワイルドカード付きのホスト名（*.emc.com など）を指定できます。

4. ［Encryption Strength］を選択します。

   ［None］（暗号化なし）、［Medium］（AES128-SHA1）、［High］（AES256-SHA1）のオプションがあります。

5. 認証モードを選択します。

   ［One Way］、［Two Way］、［Two Way Password］、［Anonymous］のオプションがあります。

6. ［**OK**］をクリックします。

DD Boost クライアントの変更

許可された DD Boost クライアントの名前、暗号化の強度、認証モードを変更します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］を選択します。
2. ［Allowed Clients］リストで、変更するクライアントを選択します。
3. 鉛筆アイコンが表示されている［**Edit**］ボタンをクリックします。

   ［Modify Allowed Client］ダイアログが表示されます。

4. クライアントの名前を変更するには、クライアントのテキストを編集します。
5. 暗号化の強度を変更するには、オプションを選択します。

   ［None］（暗号化なし）、［Medium］（AES128-SHA1）、［High］（AES256-SHA1）のオプションがあります。

6. 認証モードを変更するには、オプションを選択します。

   ［One Way］、［Two Way］、［Anonymous］のオプションがあります。

7. ［**OK**］をクリックします。

DD Boost クライアントの削除

許可された DD Boost クライアントを削除します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］を選択します。
2. リストからクライアントを選択します。
3. ［**Delete**（**X**）］をクリックします。

   ［Delete Allowed Clients］ダイアログが表示されます。

4. クライアント名を確認して選択します。［**OK**］をクリックします。

インターフェイス グループについて

インターフェイス グループ機能を使用して、複数の Ethernet リンクをグループにまとめて、Data Domain システム上の 1 つのインターフェイスだけをバックアップ アプリケーションに登録することができます。DD Boost Library は Data Domain システムとネゴシエートして、データ送信に最適なインターフェイスを取得します。ロード バランシングにより、Data Domain システムへの物理スループットが向上します。

インターフェイス グループを構成することにより、グループとして示される IP アドレスで構成されるプライベート ネットワークが Data Domain システム内に作成されます。クライアントは単一のグループに割り当てられ、グループのインターフェイスはロード バランシングを使用して、データ転送のパフォーマンスを向上させ、信頼性を高めます。

たとえば、Symantec NetBackup 環境で、メディア サーバー クライアントは単一パブリック ネットワーク IP アドレスを使用して、Data Domain システムにアクセスします。Data Domain システムとの通信はすべて、NetBackup サーバーで構成されるこの管理 IP 接続を介して開始されます。

インターフェイス グループが構成された場合、Data Domain システムがメディア サーバー クライアントからデータを受信すると、データ転送がグループ内のすべてのインターフェイスで負荷分散されて配分されます。それによって、特に複数の 1 GigE 接続を使用する顧客の場合、入力/出力スループットが改善します。

データ転送は、インターフェイス上の未処理の接続数に基づいて負荷分散されます。バックアップおよびリストア ジョブの接続のみが負荷分散されます。グループ内のインターフェイス上の未処理の接続数の詳細については、Active Connections をチェックします。

万が一グループ内のインターフェイスで障害が発生した場合、そのインターフェイスへのすべての未了（in-flight）ジョブが自動的に正常な動作リンクで再開されます（バックアップ アプリケーションには認識されません）。障害発生後に開始されたすべてのジョブは、グループ内の正常なインターフェイスに経路指定されます。グループが無効化されるか、代替インターフェイスでリカバリする試行が失敗した場合、管理 IP がリカバリに使用されます。1 つのグループ内での障害は、他のグループからのインターフェイスを使用しません。

インターフェイス グループを管理する場合は、次の情報を考慮してください。

- IP アドレスを Data Domain システム上に構成し、インターフェイスを有効化する必要があります。インターフェイス構成をチェックするには、［**Hardware**］ > ［**Ethernet**］ > ［**Interfaces**］ページを選択して、空きポートをチェックします。インターフェイスの IP アドレスの構成の詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」または「Data Domain オペレーティング システム初期構成ガイド」の `net` に関する章を参照してください。
- `ifgroup` コマンドを使用して、インターフェイス グループを管理できます。これらのコマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。
- インターフェイス グループは、固定 IPv6 アドレスを完全サポートし、IPv4 同様に、IPv6 にも同じ機能を提供します。コンカレント IPv4 と IPv6 のクライアント接続が許可されます。IPv6 で接続したクライアントは IPv6 ifgroup インターフェイスのみを認識します。IPv4 で接続したクライア

ントは IPv4 ifgroup インターフェイスのみを認識します。個々の ifgroup は、すべての IPv4 アドレスまたはすべての IPv6 アドレスを含みます。詳細については、「Data Domain Boost for Partner Integration 管理ガイド」または「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。

- 構成されたインターフェイスは、［Activities］ページの下部の Active Connections にリストされます。

注

HA システムでインターフェイス グループを使用する場合の重要な情報については、HA システムで DD Boost を使用（358 ページ）を参照してください。

次のトピックでは、インターフェイス グループの管理方法について説明します。

インタフェース

IFGROUP は、物理インターフェイスと仮想インターフェイスに対応しています。

IFGROUP インターフェイスは単一の IFGROUP<group-name>のメンバーであり、以下で構成することができます。

- 物理インターフェイス。例：`eth0a`
- リンク フェールオーバーまたはリンク統合用に作成された仮想インターフェイス。例：`veth1`
- 仮想エイリアス インターフェイス。例：`eth0a:2` または `veth1:2`
- 仮想 VLAN インターフェイス。例：`eth0a.1` または `veth1.1`
- IFGROUP<group-name>では、ネットワーク エラーの発生時にフェイルオーバーが行えるように、すべてのインターフェイスが一意のインターフェイス（Ethernet、仮想 Ethernet）である必要があります。

IFGROUP は、固定 IPv6 アドレスを完全サポートし、IPv6 にも IPv4 と同様の機能を提供します。コンカレント IPv4 と IPv6 のクライアント接続が許可されます。IPv6 で接続したクライアントは IPv6 IFGROUP インターフェイスのみを認識します。IPv4 で接続したクライアントは IPv4 IFGROUP インターフェイスのみを認識します。個々の IFGROUP は、すべての IPv4 アドレスまたはすべての IPv6 アドレスを含みます。

詳細については、「DD Boost for OpenStorage 管理ガイド」または「DD Boost for Partner Integration 管理ガイド」を参照してください。

インターフェイスの適用

IFGROUP では、プライベート ネットワークの接続を強化して、ネットワーク エラー発生後に、失敗したジョブがパブリック ネットワークにリコネクトしないようにできます。

インターフェイス適用を有効化してある場合、失敗したジョブは代替プライベート ネットワーク IP アドレスでのみ再試行できます。インターフェイス適用は IFGROUP インターフェイスを使用するクライアントでのみ使用可能です。

インターフェイス適用はデフォルトでオフ（FALSE）です。インターフェイス適用を有効化するには、次の設定をシステム レジストリに追加する必要があります。

`system.ENFORCE_IFGROUP_RW=TRUE`

これをレジストリに入力したうえで、設定を有効化するために `filesys restart` を実行する必要があります。

詳細については、「DD Boost for OpenStorage 管理ガイド」または「EMC DD Boost for Partner Integration 管理ガイド」を参照してください。

クライアント

IFGROUP は、クライアントのさまざまな命名形式に対応しています。クライアントの選択は、指定された優先順序に基づき行われます。

IFGROUP クライアントは単一の ifgroup<group-name>のメンバーであり、以下で構成することができます。

- FQDN（完全修飾ドメイン名）。例：ddboost.datadomain.com
- 部分ホスト。ホスト名の最初の n 文字が検索できます。たとえば、n=3 の場合、有効なフォーマットは `rtp_.*emc.com` と `dur_.*emc.com` です。n には 5 つの異なる値（1～5）が設定できます。
- ワイルドカード。例：`*.datadomain.com` または「`*`」
- クライアントの短い名前。例：ddboost
- クライアントのパブリック IP 範囲。例：128.5.20.0/24

クライアントでは、書き込み処理または読み取り処理に先立って、サーバーからの IFGROUP IP アドレスを要求します。クライアントの IFGROUP の関連づけを選択するために、以下の優先順序に従い、クライアントの情報が評価されます。

1. 接続されている Data Domain システムの IP アドレス。クライアントと Data Domain システムの間にすでにアクティブ接続が存在しており、この接続が IFGROUP のインターフェイスに存在している場合は、IFGROUP インターフェイスをクライアントで利用できます。
2. 接続されたクライアントの IP 範囲。クライアント ソース IP に対する IP マスクのチェックが実行されます。クライアントのソース IP アドレスが IFGROUP クライアント リストにあるマスクと一致する場合、IFGROUP インターフェイスをクライアントで利用できます。
   - IPv4 では、ネットワークに基づいて 5 つの異なる範囲マスクを選択できます。
   - IPv6 の場合、固定マスク/64、/112、/128 を使用できます。

   このホスト範囲チェックは、一意の部分ホスト名（ドメイン）がない多数のクライアントを含む個別の VLAN の場合に有用です。
3. Client Name: `abc-11.d1.com`
4. Client Domain Name: `*.d1.com`
5. All Clients: `*`

詳細については、「Data Domain Boost for Partner Integration 管理ガイド」を参照してください。

インターフェイス グループの作成

［IP Network］タブを使用して、インターフェイス グループを作成し、そのグループにインターフェイスおよびクライアントを追加します。

複数のインターフェイス グループを使用することで、次のことが可能になり、DD Boost の効率が向上します。

- DD Boost がグループに構成された特定のインターフェイスを使用するよう構成する。
- インターフェイス グループのいずれかにクライアントを割り当てる。
- どのインターフェイスが DD Boost クライアントに対してアクティブになっているかを監視する。

まず、インターフェイス グループを作成し、次にクライアントを（使用可能になる新しいメディア サーバーとして）インターフェイス グループに追加します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Interface Groups］セクションで［Add］（[**+**]）をクリックします。
3. インターフェイス グループ名を入力します
4. 1 つ以上のインターフェイスを選択します。最大 32 個のインターフェイスを構成できます。

   注

   エイリアシング構成によっては、同じグループ内の他のインターフェイスと物理インターフェイスを共有している場合、一部のインターフェイスが選択不可能になる場合があります。これは、フェイルオーバー リカバリを行うため、グループ内の各インターフェイスは別々の物理インターフェイス上にある必要があるためです。

5. ［**OK**］をクリックします。
6. ［Configured Clients］セクションで［Add］（[**+**]）をクリックします。
7. 完全修飾クライアント名または`*.mydomain.com`を入力します。

   注

   *クライアントは、初めからデフォルト グループで使用可能です。*クライアントは、1 つの ifgroup のメンバーとしてのみ構成できます。

8. 構成済みのインターフェイス グループを選択し、［**OK**］をクリックします。

インターフェイス グループの有効化/無効化

［IP Network］タブを使用して、インターフェイス グループを有効化および無効化します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Interface Groups］セクションで、リストのインターフェイス グループを選択します。

   注

   インターフェイス グループにクライアントとインターフェイス両方が割り当てられている場合、グループを有効化できません。

3. ［**Edit**］（鉛筆）をクリックします。
4. インターフェイス グループを有効化するには、［**Enabled**］をクリックします。無効化するにはチェックボックスをオフにします。
5. ［**OK**］をクリックします。

インターフェイス グループの名前とインターフェイスの変更

［IP Network］タブを使用して、インターフェイス グループの名前とそのグループと関連づけられているインターフェイスを変更します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。

2. ［Interface Groups］セクションで、リストのインターフェイス グループを選択します。
3. ［**Edit**］（鉛筆）をクリックします。
4. 名前を入力し直して、名前を変更します。

   グループ名は、1～24 文字でなければならず、文字、数字、下線、ダッシュのみ使用できます。他のグループと同じ名前は使用できず、「**default**」、「**yes**」、「**no**」、「**all**」は指定できません。

5. ［Interfaces］リストでクライアント インターフェイスを選択または選択解除します。

   注

   グループからすべてのインターフェイスを削除した場合、自動的に無効化されます。

6. ［**OK**］をクリックします。

インターフェイス グループの削除

［IP Network］タブを使用して、インターフェイス グループを削除します。インターフェイス グループを削除すると、そのグループと関連づけられているすべてのインターフェイスとクライアントが削除されます。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Interface Groups］セクションで、リストのインターフェイス グループを選択します。デフォルト グループを削除できません。
3. ［Delete］（［**X**］）をクリックします。
4. 削除を確認します。

インターフェイス グループへのクライアントの追加

［IP Network］タブを使用して、クライアントをインターフェイス グループに追加します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Configured Clients］セクションで［Add］（［**+**］）をクリックします。
3. クライアントの名前を入力してください。

   クライアント名は一意であり、以下の内容で構成されている必要があります。

   - **`FQDN`**
   - **`*.domain`**
   - クライアントのパブリック IP の範囲
     - IPv4 の場合、`xx.xx.xx.0/24` により、接続している IP に対する 24 ビットのマスクが行われます。**/24** は、クライアントのソース IP アドレスを IFGROUP へのアクセス用に評価する場合に、マスクされるビットを表します。
     - IPv6 の場合、`xxxx::0/112` は、接続する IP に対する 112 ビット マスクを提供します。**/112** は、クライアントのソース IP アドレスを IFGROUP へのアクセス用に評価する場合に、マスクされるビットを表します。

   クライアント名は最長 128 文字です。

4. 構成済みのインターフェイス グループを選択し、［**OK**］をクリックします。

クライアントの名前またはインターフェイス グループの変更

［IP Network］タブを使用して、クライアントの名前またはインターフェイス グループを変更します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Configured Clients］セクションでは、クライアントを選択します。
3. ［**Edit**］（鉛筆）をクリックします。
4. 新しいクライアント名を入力します。

   クライアント名は一意であり、以下の内容で構成されている必要があります。

   - **FQDN**
   - ***.domain**
   - クライアントのパブリック IP の範囲
     - IPv4 の場合、`xx.xx.xx.0/24` により、接続している IP に対する 24 ビットのマスクが行われます。**/24** は、クライアントのソース IP アドレスを IFGROUP へのアクセス用に評価する場合に、マスクされるビットを表します。
     - IPv6 の場合、`xxxx::0/112` は、接続する IP に対する 112 ビット マスクを提供します。**/112** は、クライアントのソース IP アドレスを IFGROUP へのアクセス用に評価する場合に、マスクされるビットを表します。

   クライアント名は最長 128 文字です。
5. メニューから新しいインターフェイス グループを選択します。

   注

   クライアントがない場合、古いインターフェイス グループは無効化されます。
6. ［**OK**］をクリックします。

インターフェイス グループからのクライアントの削除

［IP Network］タブを使用して、インターフェイス グループからクライアントを削除します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Configured Clients］セクションでは、クライアントを選択します。
3. ［**Delete**］（［X］）をクリックします。

   注

   クライアントが属するインターフェイス グループに他のクライアントがなくなっている場合、インターフェイス グループは無効化されます。
4. 削除を確認します。

MFR（管理ファイル レプリケーション）でのインターフェイス グループの使用

インターフェイス グループを使用すると、DD Boost MFR に使用されるインターフェイスを制御すること、レプリケーション接続を特定のネットワークに導くこと、フェイルオーバー状態時に広帯域幅と信頼性を備えた複数のネットワーク インターフェイスを使用することができます。すべての Data Domain IP タイプ（IPv4 または IPv6、エイリアス IP/VLAN IP、LACP/フェイルオーバー統合）がサポートされています。

注

レプリケーションに使用されるインターフェイス グループは、以前に説明したインターフェイス グループとは異なり、DD Boost MFR（管理ファイル レプリケーション）の場合にのみサポートされています。MFR に対するインターフェイス グループの使用について、詳細は「Data Domain Boost for Partner Integration 管理ガイド」または「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。

インターフェイス グループを使用しないレプリケーションの構成では、複数のステップを実行する必要があります。

1. ソース Data Domain システムの`/etc/hosts` ファイルにターゲット Data Domain システムのエントリーを追加し、プライベート LAN ネットワーク インターフェイスの 1 つを宛先の IP アドレスとしてハード コーディングします。
2. ソース Data Domain システム上のルートをターゲット Data Domain システムに追加し、ソース Data Domain システムの物理または仮想ポートをリモートの宛先 IP アドレスに指定します。
3. ロード バランシングとフェイルオーバーを実行できるように、Data Domain システム間のすべてのスイッチにネットワーク経由の LACP を構成します。
4. `/etc/hosts` ファイルの名前の競合を回避するために、ターゲット Data Domain システムにはアプリケーションごとに異なる名前を使用する必要があります。

レプリケーションにインターフェイス グループを使用すると、DD OS System Manager または DD OS CLI コマンドを使用することで、この構成が簡素化されます。インターフェイス グループを使用してレプリケーション パスを構成すると、次のことが可能になります。

- 別のプライベート Data Domain システムの IP アドレスを使用して、ホスト名解決済みの IP アドレスをパブリック ネットワーク以外の宛先にリダイレクトする。
- 構成済みの選択基準に基づきインターフェイス グループを識別し、すべてのインターフェイスにターゲット Data Domain システムからアクセスできる単一のインターフェイス グループを提供する。
- グループに属しているインターフェイスのリストからプライベート ネットワーク インターフェイスを選択し、そのインターフェイスが正常であることを保証する。
- 同じプライベート ネットワーク内にある複数の Data Domain インターフェイス間でのロードバランシングを実行する。
- インターフェイス グループの各インターフェイスのために、リカバリ用のフェイルオーバー インターフェイスを提供する。
- ソース Data Domain システム上に構成されている場合に、ホスト フェイルオーバーを可能にする。
- NAT（ネットワーク アドレス変換）の使用

ファイル レプリケーションに一致するインターフェイス グループを判断するための選択順序は次のとおりです。

1. ローカル MTree（storage-unit）パスおよび特定のリモート Data Domain ホスト名

2. ローカル MTree（storage-unit）パスおよび任意のリモート Data Domain ホスト名
3. 任意の MTree（storage-unit）パスおよび特定のリモート Data Domain ホスト名

異なる Data Domain ホスト名が設定されている場合に限って、複数のインターフェイス グループに同じ MTree が表示される場合があります。異なる MTree が設定されている場合に限って、複数のインターフェイス グループに同じ Data Domain ホスト名が表示される場合があります。リモート ホスト名は、FQDN（dd890-1.emc.com など）になります。

インターフェイス グループの選択は、ソース Data Domain システムとターゲット Data Domain システムの両方でローカルに、互いに独立して実行されます。WAN レプリケーション ネットワークの場合は、ソース IP アドレスがリモート IP アドレスのゲートウェイに対応しているため、構成する必要があるのはリモート インターフェイス グループのみです。

インターフェイス グループへのレプリケーション パスの追加

［IP Network］タブを使用して、レプリケーション パスをインターフェイス グループに追加します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Configured Replication Paths］セクションで、［Add］（［**+**］）をクリックします。
3. ［**MTree**］および/または［**Remote Host**］の値を入力します。
4. 構成済みのインターフェイス グループを選択し、［**OK**］をクリックします。

インターフェイス グループのレプリケーション パスの変更

［IP Network］タブを使用して、インターフェイス グループのレプリケーション パスを変更します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Configured Replication Paths］セクションで、レプリケーション パスワードを選択します。
3. ［**Edit**］（鉛筆）をクリックします。
4. ［**MTree**］、［**Remote Host**］、［**Interface Group**］のいずれかまたはすべての値を変更します。
5. ［**OK**］をクリックします。

インターフェイス グループのレプリケーション パスの削除

［IP Network］タブを使用して、インターフェイス グループのレプリケーション パスを削除します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**IP Network**］を選択します。
2. ［Configured Replication Paths］セクションで、レプリケーション パスワードを選択します。
3. ［**Delete**］（［X］）をクリックします。
4. ［Delete Replication Path(s)］ダイアログで［**OK**］をクリックします。

DD Boost の破棄

このオプションを使用して、ストレージ ユニットに収容されているすべてのデータ（イメージ）を完全に削除します。DD Boost を無効化または破棄すると、DD Boost FC サービスも破棄されます。DD Boost を破棄できるのは、管理ユーザーのみです。

手順

1. 対応するバックアップ アプリケーション カタログ エントリーを手動で削除する（期限切れにする）必要があります。

   注

   複数のバックアップ アプリケーションが同じ Data Domain システムを使用している場合、アプリケーション カタログそれぞれからすべてのエントリーを削除します。

2. ［**Protocols**］ > ［**DD Boost**］ > ［**More Tasks**］ > ［**Destroy DD Boost...**］を選択します。
3. プロンプトが表示されたら、管理認証情報を入力します。
4. ［**OK**］をクリックします。

DD Boost over Fibre Channel の構成

前のバージョンの DD OS では、DD Boost Library と Data Domain システムとのすべての通信は、IP ネットワークを使用して行われていました。最新の DD OS では、DD Boost Library と Data Domain システム間の通信の代替転送メカニズムとしてファイバー チャネルが導入されています。

注

Windows、Linux、HP-UX（64 ビットの Itanium アーキテクチャ）、AIX、Solaris のクライアント環境がサポートされています。

DD Boost ユーザーの有効化

Data Domain システムに DD Boost-over-FC サービスを構成する前に、1 人以上の DD Boost ユーザーを追加して DD Boost を有効にする必要があります。

はじめに

- DD System Manager にログインします。手順については、「DD System Manager へのログインとログアウト」を参照してください。
  ［**CLI** 相当機能］

  ```
  login as: sysadmin
  Data Domain OS 5.7.x.x-12345
  Using keyboard-interactive authentication.
  Password:
  ```

- CLI を使用している場合は、SCSI ターゲット デーモンが有効になっていることを確認してください。

  ```
  # scsitarget enable
  Please wait ...
  SCSI Target subsystem is enabled.
  ```

  注

  DD System Manager を使用している場合、後続の手順で DD Boost-over-FC サービスを有効にすると、SCSI ターゲット デーモンが自動的に有効になります。

- DD Boost ライセンスがインストールされていることを確認します。DD System Manager で、［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］を選択します。［Status］に DD Boost のライセンスが存在しないと示されている場合は、［**Add License**］をクリックして、［Add License Key］ダイアログ ボックスに有効なライセンスを入力します。

［**CLI** 相当機能］

```
# license show
```

```
# license add license-code
```

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Settings**］を選択します。
2. ［DD Boost Access］セクションの［Users］で、1 つ以上の DD Boost ユーザー名を指定します。

   DD Boost ユーザーは DD OS ユーザーでもあります。DD Boost ユーザー名を指定するときは、既存の DD OS ユーザー名を選択するか、新しい DD OS ユーザー名を作成して、その名前を DD Boost ユーザー名にすることができます。このリリースは、複数の DD Boost ユーザーに対応しています。詳細な手順については、「DD Boost ユーザー名の指定」を参照してください。

   ［**CLI** 相当機能］

   ```
   # user add username [password password]
   ```

   ```
   # ddboost set user-name exampleuser
   ```

3. ［**Enable**］をクリックして、DD Boost を有効化します。

   ［**CLI** 相当機能］

   ```
   # ddboost enable
   Starting DDBOOST, please wait..............
   DDBOOST is enabled.
   ```

結果

これで、Data Domain システムに DD Boost-over-FC サービスを構成する準備ができました。

DD Boost の構成

ユーザーを追加して、DD Boost を有効にしたら、［Fibre Channel］オプションを有効にして、DD Boost ファイバー チャネル サーバー名を指定する必要があります。使用アプリケーションによっては、1 つ以上のストレージ ユニットを作成し、Data Domain システムにアクセスするメディア サーバーに DD Boost API/プラグ インをインストールする必要があります。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Fibre Channel**］を選択します。
2. ［**Enable**］をクリックして、ファイバー チャネル転送を有効にします。

   ［**CLI** 相当機能］

   ```
   # ddboost option set fc enabled
   Please wait...
   DD Boost option "FC" set to enabled.
   ```

3. DD Boost ファイバー チャネル サーバー名をデフォルト（ホスト名）から変更するには、［**Edit**］をクリックし、新しいサーバー名を入力して［**OK**］をクリックします。

   ［**CLI** 相当機能］

   ```
   # ddboost fc dfc-server-name set DFC-ddbeta2
   ```

```
DDBoost dfc-server-name is set to "DFC-ddbeta2" for DDBoost FC.
Configure clients to use "DFC-DFC-ddbeta2" for DDBoost FC.
```

4. ［**Protocols**］ > ［**DD Boost**］ > ［**Storage Units**］を選択して、ストレージ ユニットを作成します（アプリケーションによって作成済みでない場合）。

   Data Domain システムで 1 つ以上のストレージ ユニットを作成する必要があります。DD Boost ユーザーは、そのストレージ ユニットに割り当てる必要があります。詳細な手順については、「ストレージ ユニットの作成」を参照してください。

   ［**CLI** 相当機能］

   ```
   # ddboost storage-unit create storage_unit_name-su
   ```

5. DD Boost API/プラグ インをインストールします（使用アプリケーションで必要な場合）。

   DD Boost OpenStorage プラグ イン ソフトウェアは、Data Domain システムにアクセスする必要がある NetBackup メディア サーバーにインストールする必要があります。このプラグ インには、Data Domain システムと統合される必須の DD Boost ライブラリが含まれます。インストールおよび構成手順の詳細については、「Data Domain Boost for Partner Integration 管理ガイド」または「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。

結果

これで、接続を検証し、アクセス グループを作成する準備ができました。

接続の検証とアクセス グループの作成

［**Hardware**］ > ［**Fibre Channel**］ > ［**Resources**］に移動して、アクセス ポイントのイニシエーターとエンドポイントを管理します。［**Protocols**］ > ［**DD Boost**］ > ［**Fibre Channel**］に移動して、DD Boost-over-FC アクセス グループを作成および管理します。

注

アクティブなバックアップまたはリストア ジョブの実行中に Data Domain システムでアクセス グループを変更しないでください。変更すると、アクティブなジョブが失敗する場合があります。アクティブなジョブの実行中に行った変更の影響は、バックアップ ソフトウェアやホスト構成の組み合わせによって異なります。

手順

1. ［**Hardware**］ > ［**Fibre Channel**］ > ［**Resources**］ > ［**Initiators**］を選択して、イニシエーターが存在することを確認します。

   イニシエーターにエイリアスを割り当てて、構成処理中の混乱を軽減することをお勧めします。

   ［**CLI** 相当機能］

   ```
   # scsitarget initiator show list
   Initiator      System Address                Group   Service
   ------------   ----------------------   ----------   -------
   initiator-1    21:00:00:24:ff:31:b7:16         n/a       n/a
   initiator-2    21:00:00:24:ff:31:b8:32         n/a       n/a
   initiator-3    25:00:00:21:88:00:73:ee         n/a       n/a
   initiator-4    50:06:01:6d:3c:e0:68:14         n/a       n/a
   initiator-5    50:06:01:6a:46:e0:55:9a         n/a       n/a
   initiator-6    21:00:00:24:ff:31:b7:17         n/a       n/a
   initiator-7    21:00:00:24:ff:31:b8:33         n/a       n/a
   initiator-8    25:10:00:21:88:00:73:ee         n/a       n/a
   initiator-9    50:06:01:6c:3c:e0:68:14         n/a       n/a
   ```

```
initiator-10   50:06:01:6b:46:e0:55:9a          n/a       n/a
tsm6_p23       21:00:00:24:ff:31:ce:f8   SetUp_Test       VTL
------------   ----------------------   ----------   -------
```

2. イニシエーターにエイリアスを割り当てるには、いずれかのイニシエーターを選択して、鉛筆（編集）アイコンをクリックします。［Modify Initiator］ダイアログの［Name］フィールドにエイリアスを入力して、［**OK**］をクリックします。

   ［**CLI** 相当機能］

```
# scsitarget initiator rename initiator-1 initiator-renamed
Initiator 'initiator-1' successfully renamed.
```

```
# scsitarget initiator show list
Initiator           System Address                 Group
Service
-----------------   ----------------------   ----------
-------
initiator-2         21:00:00:24:ff:31:b8:32          n/a
n/a
initiator-renamed   21:00:00:24:ff:31:b7:16          n/a
n/a
-----------------   ----------------------   ----------
-------
```

3. ［Resources］タブで、エンドポイントが存在し、有効になっていることを確認します。

   ［**CLI** 相当機能］

```
# scsitarget endpoint show list
-------------   --------------   ------------   -------   ------
endpoint-fc-0   5a               FibreChannel   Yes       Online
endpoint-fc-1   5b               FibreChannel   Yes       Online
-------------   --------------   ------------   -------   ------
```

4. ［**Protocols**］ > ［**DD Boost**］ > ［**Fibre Channel**］に移動します。
5. ［DD Boost Access Groups］領域で［**+**］アイコンをクリックして、アクセス グループを追加します。
6. アクセス グループの一意の名前を入力します。重複名はサポートされていません。

   ［**CLI** 相当機能］

```
# ddboost fc group create test-dfc-group
DDBoost FC Group "test-dfc-group" successfully created.
```

7. 1 つ以上のイニシエーターを選択します。オプションで、新しいものを入力して、イニシエーター名を変更します。［**Next**］をクリックします。

   ［**CLI** 相当機能］

```
#ddboost fc group add test-dfc-group initiator initiator-5
Initiator(s) "initiator-5" added to group "test-dfc-group".
```

   イニシエーターは、ファイバー チャネル プロトコルを使用して、データの読み取りと書き込みを行うためにシステムに接続するバックアップ クライアントに接続されている HBA 上のポートです。WWPN は、メディア サーバーの Fibre Channel ポートの World-Wide Port Name です。

8. グループで使用される DD Boost デバイスの数を指定します。この数により、イニシエーターが検出できるデバイス数が決まり、その結果、Data Domain システムへの I/O パスの数が決まります。デフォルトは 1、最小値は 1、最大値は 64 です。

   ［**CLI** 相当機能］

```
# ddboost fc group modify Test device-set count 5
Added 3 devices.
```

クライアントごとの推奨値については、「Data Domain Boost for OpenStorage Administration Guide」を参照してください。

9. グループに含まれるエンドポイント（all、none）を示すか、エンドポイントのリストから選択します。［次へ］をクリックします。

［CLI 相当機能］

```
# scsitarget group add Test device ddboost-dev8 primary-endpoint allsecondary-endpoint all
Device 'ddboost-dev8' successfully added to group.
```

```
# scsitarget group add Test device ddboost-dev8 primary-endpointendpoint-fc-1 secondary-endpoint fc-port-0
Device 'ddboost-dev8' is already in group 'Test'.
```

HBA 上の接続された FC ポート経由で LUN を提示する場合、ポートは「primary」、「secondary」、「none」として指定できます。一連の LUN のプライマリ ポートは、現在それらの LUN をファブリックに公開しているポートです。セカンダリ ポートは、プライマリ パスの障害発生時に一連の LUN をブロードキャストするポートです（手動の操作が必要です）。なしの設定は、選択した LUN をアドバタイズしたくない場合に使用されます。LUN の提示方法は、SAN トポロジーによって異なります。

10. Summary を確認し、変更を行います。［**Finish**］をクリックして、［DD Boost Access Groups］リストに表示されるアクセス グループを作成します。

［CLI 相当機能］

```
# scsitarget group show detailed
```

注

既存のアクセス グループの設定を変更するには、リストから選択し、鉛筆アイコン［Modify］をクリックします。

アクセス グループの削除

［Fibre Channel］タブを使用して、アクセス グループを削除します。

手順

1. ［**Protocols**］ > ［**DD Boost**］ > ［**Fibre Channel**］を選択します。
2. ［DD Boost Access Groups］リストから削除されるグループを選択します。

注

イニシエーターが割り当てられているグループは削除できません。まず、イニシエーターを削除するグループを編集します。

3. ［**Delete**］（［X］）をクリックします。

HA システムで DD Boost を使用

HA は、DD Boost を使用して任意のアプリケーションのシームレスなフェイルオーバーを可能にします。つまり、手動で介入しなくても、続けてバックアップまたはリストア操作を実行します。他のすべての DD Boost ユーザー シナリオは、HA システムでもサポートされています。シナリオには、MFR（管

理ファイル レプリケーション）、DSP（分散セグメント処理）、ファイルコピー、DIG（ダイナミック インターフェイス グループ ） などがあります。

HA システムで DD Boost を使用する場合は、次の特別な考慮事項に注意してください。

- HA を有効化した Data Domain システムでは、10 分経過しないうちに DD サーバーのフェイルオーバーが発生します。ただし、DD Boost アプリケーションのリカバリにはこれより長い時間がかかる場合があります。DD サーバーのフェイルオーバーが完了するまで Boost アプリケーションのリカバリを開始できないためです。さらに、Boost アプリケーションのリカバリは、アプリケーションが Boost ライブラリを呼び出すまで開始できません。
- HA システム上の DD Boost では、Boost アプリケーションが Boost HA ライブラリを使用する必要があります。非 HA Boost ライブラリを使用するアプリケーションでは、シームレスなフェイルオーバーは表示されません。
- MFR は、ソースとデスティネーションの両方のシステムで HA が有効化されている場合にシームレスにフェイルオーバーします。MFR は、HA が有効化されたシステムで障害が発生した場合は、部分的な HA 構成（つまり、ソースまたはデスティネーションのいずれかのシステムは有効化されているが、両方は有効化されていない状態） でもサポートされます。詳細は、「DD Boost for OpenStorage 管理ガイド」または「EMC DD Boost for Partner Integration 管理ガイド」を参照してください。
- ダイナミック インターフェイス グループに、Data Domain のアクティブ システムとスタンバイ システム間の直接の相互接続に関連する IP アドレスを含めることはできません。
- DD Boost クライアントは、フローティング IP アドレスを使用するように構成する必要があります。

［DD Boost］タブについて

DD System Manager の［DD Boost］タブの使用方法について説明します。

Settings

［Settings］タブを使用して、DD Boost の有効化または無効化、クライアントとユーザーの選択、詳細オプションの指定を行います。

［Settings］タブには、DD Boost のステータス（Enabled または Disabled）が表示されます。［**Status**］ボタンを使用して［**Enabled**］または［**Disabled**］を切り換えます。

［**Allowed Clients**］の下で、システムへのアクセス権を持つクライアントを選択します。［**Add**］、［**Modify**］、［**Delete**］ボタンを使用して、クライアントのリストを管理します。

［**Users with DD Boost Access**］の下で、DD Boost アクセス権を持つユーザーを選択します。［**Add**］、［**Change Password**］、［**Remove**］ボタンを使用して、ユーザーのリストを管理します。

［**Advanced Options**］を展開して、有効になっている詳細オプションを確認します。［**More Tasks**］ > ［**Set Options**］を選択して、有効になっているオプションをリセットします。

アクティブな接続

［Active Connections］タブを使用して、クライアント、インターフェイス、アウトバウンド ファイルに関する情報を確認します。

表 131 接続されたクライアントの情報

項目	説明
クライアント	接続されたクライアントの名前。
Idle	クライアントがアイドルかどうか（Yes/No）。
Plug-In Version	インストールされている DD Boost プラグイン バージョン（2.2.1.1 など）。
OS Version	インストールされているオペレーティング システム バージョン（Linux 2.6.1 7-1.2142_FC4smp x86_64 など）。
Application Version	インストールされているバックアップ アプリケーション バージョン（NetBackup 6.5.6 など）。
暗号化	接続が暗号化されているかどうか（Yes/No）。
DSP	接続に DSP（分散セグメント処理）が使用されているかどうか。
Transport	使用中のトランスポートのタイプ（IPv4、IPv6、または FC（Fibre Channel））

表 132 構成されたインターフェイス接続の情報

項目	説明
インターフェイス	インターフェイスの IP アドレス。
Interface Group	次のいずれかを選択します。 • インターフェイス グループの名前。 • None（メンバーではない場合）。
バックアップ	アクティブなバックアップ接続数。
リストア	アクティブなリストア接続数。
レプリケーション	アクティブなレプリケーション接続数。
シンセティック	シンセティック バックアップの数。
Total	インターフェイス用の接続の総数。

表 133 アウトバウンド ファイル レプリケーションの情報

アウトバウンド ファイル項目	説明
File Name	発信イメージ ファイルの名前。
Target Host	ファイルを受信するホストの名前。
Logical Bytes to Transfer	転送される論理バイト数。
Logical Bytes Transferred	転送済みの論理バイト数。
Low Bandwidth Optimization	転送済みの低帯域幅バイト数。

IP ネットワーク

［IP Network］タブには、構成されたインターフェイス グループがリストされます。詳細には、グループの状態（有効/無効）、構成されたクライアントのインターフェイスが含まれます。管理者は、［Interface Group］メニューを使用して、インターフェイス グループに関連づけられたクライアントを表示することができます。

ファイバー チャネル

［Fibre Channel］タブには、構成済みの DD Boost アクセス グループが一覧表示されます。［Fibre Channel］タブを使用して、アクセス グループを作成および削除し、DD Boost アクセス グループのイニシエーター、デバイス、エンドポイントを構成します。

Storage Units

［**Storage Units**］タブを使用して、ストレージ ユニットを表示、作成、変更、削除します。

表 134 ［Storage Units］タブ

項目	説明
Storage Units	
View DD Boost Replications	DD Boost レプリケーション コンテキストを表示します。
Storage Unit	ストレージ ユニットの名前。
User	ストレージ ユニットに関連付けられたユーザー名。
Quota Hard Limit	ストレージ ユニットに設定されているハード クォータ。
Last 24hr Pre-Comp	過去 24 時間にストレージ ユニットに書き込まれたデータの量（圧縮前）。
Last 24hr Post-Comp	過去 24 時間にストレージ ユニットに書き込まれたデータの量（圧縮後）。
Last 24hr Comp Ratio	過去 24 時間にストレージ ユニットに書き込まれたデータの圧縮率。
Weekly Avg Post-Comp	ストレージ ユニットに書き込まれたデータの週あたり平均量（圧縮後）。
Last Week Post-Comp	先週ストレージ ユニットに書き込まれたデータの量（圧縮後）。
Weekly Avg Comp Ratio	ストレージ ユニットに書き込まれたデータの週あたり平均圧縮率。
Last Week Comp Ratio	先週ストレージ ユニットに書き込まれたデータの圧縮率。

詳細情報を確認するには、ストレージ ユニットを選択します。詳細情報は、次の 3 つのタブで提供されます。

- ［Storage Unit］タブ

  表 135 Storage unit details: ［Storage Unit］タブ

項目	説明
Total Files	ストレージ ユニット上のファイル イメージの総数。

表 135 Storage unit details: ［Storage Unit］タブ （続き）

項目	説明
Full Path	ストレージ ユニットのフル パス。
Status	ストレージ ユニットの現在のステータス（組み合わせに対応しています）。ステータスの種類： ■ D：削除済み ■ RO：読み取り専用 ■ RW：読み取り/書き込み ■ RD：レプリケーション デスティネーション ■ RLE：DD Retention Lock 有効 ■ RLD：DD Retention Lock 無効
Pre-Comp Used	使用済み圧縮前ストレージの量。
Used (Post-Comp)	ストレージ ユニット内のファイルの圧縮後合計サイズ。
Compression	ファイルで達成される圧縮率。
スケジュール	ストレージ ユニットに割り当てられている物理容量測定スケジュールの数。
Submitted Measurements	ストレージ ユニットの物理容量が測定された回数。
Quota Enforcement	［Quota］をクリックして、MTree によって使用されるハードおよびソフト クォータ値/割合が表示される［Data Management Quota］ページに移動します。
Pre-Comp Soft Limit	ストレージ ユニットに設定されたソフト クォータの現在の値。
Pre-Comp Hard Limit	ストレージ ユニットに設定されたハード クォータの現在の値。
Quota Summary	使用されたハード制限の割合。
スナップショットの総数	ストレージ ユニットのスナップショットの合計数。
期限切れ	ストレージ ユニットの期限切れスナップショットの数。
Unexpired	ストレージ ユニットの期限切れでないスナップショットの数。
最も古いスナップショット	ストレージ ユニットの最も古いスナップショット。
Newest Snapshot	ストレージ ユニットの最新のスナップショット。
Next Scheduled	ストレージ ユニットの次にスケジュール設定されたスナップショット。
Assigned Snapshot Schedules	ストレージ ユニットに割り当てられているスナップショット スケジュール。

- ［Space Usage］タブ：使用量の圧縮前のバイト数、圧縮後のバイト数、および圧縮率を示すグラフが表示されます。
- ［Daily Written］タブ：書き込み量の圧縮前のバイト数、圧縮後のバイト数、および総圧縮率を示すグラフが表示されます。

第 15 章

DD 仮想テープ ライブラリ

本章には、次のセクションが含まれます。

- DD 仮想テープ ライブラリの概要 364
- DD VTL の計画 364
- DD VTL の管理 371
- ライブラリの扱い 375
- 選択されたライブラリの扱い 379
- チェンジャー情報の表示 387
- ドライブの扱い 388
- 選択されたドライブの扱い 390
- テープの扱い 390
- ヴォールトの扱い 392
- クラウド ベースのヴォールトの使用 392
- アクセス グループの扱い 399
- 選択されたアクセス グループの扱い 403
- リソースの処理 406
- プールの扱い 410
- 選択されたプールの扱い 413

DD 仮想テープ ライブラリの概要

DD VTL（Data Domain 仮想テープ ライブラリ）は、物理テープの使用をエミュレートするディスク ベース バックアップ システムです。VTL を使用すると、物理テープ ライブラリとほぼ同一の機能を使用して、バックアップ アプリケーションを DD システム ストレージに接続し、DD システム ストレージを管理できます。

仮想テープ ドライブは、物理テープ ドライブの場合と同様に、バックアップ ソフトウェアにアクセスできます。DD VTL でこれらのドライブを作成すると、そのドライブが SCSI テープ ドライブとしてバックアップ ソフトウェアに認識されます。DD VTL 自体は、標準のドライバー インターフェイスを介してアクセスされる SCSI ロボット デバイスとしてバックアップ ソフトウェアに表示されます。ただし、メディア チェンジャーとバックアップ イメージの移動は、DD VTL として構成された DD システムではなく、バックアップ ソフトウェアによって管理されます。

次の用語は、DD VTL と使用された場合に特殊な意味を持ちます。

- ［Library］：ライブラリは、ドライブ、チェンジャー、CAP（カートリッジ アクセス ポート）、スロット（カートリッジ スロット）のある物理テープ ライブラリをエミュレートします。
- ［テープ］：テープはファイルとして表されます。テープは、ヴォールトからライブラリにインポートできます。テープは、ライブラリからヴォールトにエクスポートできます。テープは、ドライブ、スロット、CAP をまたいで、ライブラリ内で移動できます。
- ［プール］：プールは、ファイル システム上のディレクトリにマッピングされるテープのコレクションです。プールは、デスティネーションへのテープのレプリケーションに使用されます。デフォルトでは、プールは、作成時にディレクトリ プールとして指定しない限り、MTree プールとして作成されます。ディレクトリ ベース プールを MTree ベース プールに変換することで、MTree の機能をより有効に活用できます。
- ［ヴォールト］：ヴォールトには、どのライブラリでも使用されていないテープが保持されます。テープは、ライブラリまたはヴォールトに置けます。

DD VTL は、特定のバックアップ ソフトウェアとハードウェア構成によってテストされ、対応されています。詳細については、オンライン サポート サイトの適切な「Backup Compatibility Guide」を参照してください。

DD VTL は、テープ ライブラリとファイル システム（NFS/CIFS/DD Boost）インターフェイスの同時使用に対応しています。

DR（災害復旧）が必要な場合は、DD Replicator を使用して、プールとテープをリモートの DD システムにレプリケーションできます。

テープ上のデータを変更できないようにするには、DD Retention Lock Governance ソフトウェアを使用してテープをロックします。

注

現在、16 Gb/秒の場合は、ファブリック トポロジーとポイント ツー ポイント トポロジーがサポートされています。他のトポロジーの場合は問題が発生します。

KB 記事「Data Domain：VTL ベスト プラクティス ガイド」（https://support.emc.com/kb/180591 で入手可能）に、DD VTL のベスト プラクティスに関する追加情報が記載されています。

DD VTL の計画

DD VTL（仮想テープ ライブラリ）には、適切なライセンス、インターフェイス カード、ユーザー権限などの固有の要件があります。以下に、それらの要件の詳細および推奨事項を示します。

- 適切な DD VTL ライセンス。
  - DD VTL はライセンスが必要な機能であり、IP（インターネット プロトコル）を経由で NDMP（ネットワーク データ管理プロトコル）を使用するか、FC（ファイバー チャネル）経由で直接 DD VTL を使用する必要があります。
  - IBM i システムには、追加ライセンス（I/OS ライセンス）が必要です。
  - DD System Manager を使用して DD VTL ライセンスを追加すると、DD VTL 機能が自動的に無効化および有効化されます。
- インストールされた FC インターフェイス カードまたは NDMP を使用するよう構成された DD VTL。
  - バックアップ サーバーと DD システム間の DD VTL 通信で FC インターフェイスが使用されている場合、DD システムに FC インターフェイス カードを取り付ける必要があります。FC インターフェイス カードが DD システムから取り外された場合（またはシステム内で変更された場合）は常に、そのカードと関連づけられた DD VTL 構成を更新する必要があります。
  - バックアップ サーバーと DD システム間の DD VTL 通信で NDMP が使用されている場合、FC インターフェイス カードは必要ありません。ただし、TapeServer アクセス グループを構成する必要があります。また、NDMP を使用する場合、すべてのイニシエーターとポート機能は適用されません。
  - ネット フィルターは、NDMP クライアントが情報を DD システムに送信できるように構成する必要があります。**net filter add operation allow clients <client-IP-address>**コマンドを実行して、NDMP クライアントのアクセスを許可します。
    - セキュリティを強化するために、**net filter add operation allow clients <client-IP-address> interfaces コマンドを実行します。<DD-interface-IP-address>**コマンド。
    - **seq-id 1** オプションをコマンドに追加すると、他のネット フィルター ルールの前にこのルールを強制的に適用できます。
- バックアップ ソフトウェア最低レコード（ブロック）サイズ。
  - バックアップ ソフトウェアが 64 KiB 以上の最低レコード（ブロック）サイズを使用するように設定することを推奨します。通常、サイズが大きくなると、パフォーマンスは高くなり、データ圧縮率が高まります。
  - 初期構成後にサイズを変更した場合、バックアップ アプリケーションによっては、元のサイズで書き込まれたデータが読み取り不可能になる場合があります。
- システムへの適切なユーザー アクセス権。
  - 基本テープ操作およびモニタリングに必要なものはユーザー ログインのみです。
  - DD VTL サービスを有効化および構成し、その他の構成タスクを実行するには、sysadmin でログインする必要があります。

DD VTL の制限

DD VTL を設定または使用する前に、サイズ、スロットなどの制限を確認してください。

- I/O サイズ：DD VTL を使用する DD システムの最大対応 I/O サイズは 1 MB です。
- ライブラリ：DD VTL は、DD システムあたり最大 64 個のライブラリ（つまり、DD システムごとに 64 個の DD VTL インスタンス）に対応します。
- イニシエーター：DD VTL は、DD システムあたり最大 1024 個のイニシエーターまたは WWPN（ワールド ワイド ポート名）に対応します。

- テープ ドライブ：テープ ドライブに関する情報については、次のセクションを参照してください。
- データ ストリーム：データ ストリームに関する情報は、次の表に表示されます。

表 136 新しい Data Domain システムに送信されるデータ ストリーム

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD140、DD160、DD610	4 GB または 6 GB / 0.5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620、DD630、DD640	8 GB / 0.5 GB または 1 GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640、DD670	16 GB または 20 GB / 1 GB	90	30	60%	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670、DD860	36 GB / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b]/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 または 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60%	16	30	60%	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 または 64 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD4500	192 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 または 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540

表 136 新しい Data Domain システムに送信されるデータ ストリーム （続き）

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD9500	256 / 512 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8 TB	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE 16 TB	16 GB / 512 MB または 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE 32 TB	24 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 48 TB	36 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 TB	48 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96 TB	64 GB / 2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180
DD3300 4 TB	12 GB（仮想メモリー） / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 TB	32 GB（仮想メモリー） / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16 TB	32 GB（仮想メモリー） / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90

表 136 新しい Data Domain システムに送信されるデータ ストリーム （続き）

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD3300 32 TB	46 GB（仮想メモリー） / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl streams
b. Data Domain Extended Retention ソフトウェア オプションは、（最大）メモリが拡張されたデバイスでのみ使用可能です。

- スロット：DD VTL は最大で次の数のスロットに対応します。
  - 1 ライブラリあたり最大 32,000 スロット
  - DD システムあたり最大 64,000 スロット

  DD システムでは、スロット数をドライブ数以上に保つために自動的にスロットが追加されます。

  注

  一部のデバイス ドライバー（IBM AIX atape デバイス ドライバーなど）には、固有のドライブ/スロット制限に対するライブラリ構成の制限があり、DD システムのサポート数より少ないことがあります。そのようなアプリケーションによって使用されるバックアップ アプリケーションおよびドライブは、この制限の影響を受ける場合があります。
- CAP（カートリッジ アクセス ポート）：DD VTL は最大で次の数の CAN に対応します。
  - 1 ライブラリあたり最大 100 CAP
  - DD システムあたり最大 1000 CAP

DD VTL でサポートされるドライブ数

DD VTL でサポートされるドライブの最大数は、DD システムにインストールされている CPU コア数とメモリ（該当する場合は、RAM と NVRAM 両方）の量によって異なります。

注

次の表にはモデル番号は記載されていません。それはモデルごとに CPU コア数とメモリの組み合わせが多数あり、サポートされるドライブ数は特定のモデル自体ではなく、CPU コア数とメモリによって［のみ］決まるためです。

表 137 DD VTL でサポートされるドライブ数

CPU コアの数	RAM（GB 単位）	NVRAM（GB 単位）	サポートされるドライブの最大数
32 未満	4 以下	NA	64
	4 より多く 38 以下	NA	128
	38 より多く 128 以下	NA	256
	128 より多い	NA	540

表 137 DD VTL でサポートされるドライブ数 （続き）

CPU コアの数	RAM（GB 単位）	NVRAM（GB 単位）	サポートされるドライブの最大数
32～39	最大 128	4 未満	270
	最大 128	4 以上	540
	128 より多い	NA	540
40～59	NA	NA	540
60 以上	NA	NA	1080

テープ バーコード

テープを作成する場合、一意の識別子として［バーコード］を割り当てる必要があります（重複バーコードを使用すると、予測不能の動作が発生することがあるため、絶対に使用しないでください）。各バーコードは 8 文字で構成されます。最初の 6 文字は数字または大文字（0～9、A～Z）で、最後の 2 文字は、次の表に示されている、対応しているテープ タイプのテープ コードです。

注

DD VTL バーコードは 8 文字で構成されていますが、文字のタイプに応じて 6 または 8 文字がバックアップ アプリケーションに送信される場合があります。

表 138 テープ タイプごとのテープ コード

テープ タイプ	デフォルト容量（特に指定がない限り）	テープ コード
LTO-1	100 GiB	L1
LTO-1	50 GiB（非デフォルト）	LA[a]
LTO-1	30 GiB（非デフォルト）	LB
LTO-1	10 GiB（非デフォルト）	LC
LTO-2	200 GiB	L2
LTO-3	400 GiB	L3
LTO-4	800 GiB	L4
LTO-5（デフォルト）	1.5 TiB	L5

a. TSM には、LA コードが無視された場合、L2 テープ コードを使用します。

複数のテープ ライブラリがある場合、6 番目の文字（「L」の前）が数字であれば、バーコードが自動的にインクリメントされます。オーバーフローが発生した場合（9～0）、ナンバリングでは位置が 1 つ左に移動します。増分する次の文字が文字である場合、インクリメントは停止します。次に、サンプル バーコードおよびそれぞれがどのようにインクリメントされるかについて説明します。

- 000000L1 は、100 GiB 容量のテープを作成し、最大 100,000 テープ（000000～99999）までのカウントを許可できます。
- AA0000LA は、50 GiB 容量のテープを作成し、最大 10,000 テープ（0000～9999）までのカウントを許可できます。

- AAAA00LB は、30 GiB 容量のテープを作成し、最大 100 テープ（00～99）までのカウントを許可できます。
- AAAAAALC は、10 GiB 容量のテープを 1 つ作成します。この名前で作成できるテープは 1 つのみです。
- AAA350L1 は、100 GiB 容量のテープを作成し、最大 650 テープ（350～999）までのカウントを許可できます。
- 000AAALA は、50 GiB 容量のテープを 1 つ作成します。この名前で作成できるテープは 1 つのみです。
- 5M7Q3KLB は、30 GiB 容量のテープを 1 つ作成します。この名前で作成できるテープは 1 つのみです。

LTO テープ ドライブ互換性

セットアップ時に複数の世代の LTO（Linear Tape-Open）テクノロジーを設定することもできます。それらの世代間の互換性は、表形式で示されています。

テーブル内の略語について：

- RW = 読み取り/書き込み互換性あり
- R = 読み取り専用互換性あり
- — = 互換性なし

表 139 LTO テープ ドライブ互換性

テープ形式	LTO-5 ドライブ	LTO-4 ドライブ	LTO-3 ドライブ	LTO-2 ドライブ	LTO-1 ドライブ
LTO-5 テープ	RW	—	—	—	—
LTO-4 テープ	RW	RW	—	—	—
LTO-3 テープ	R	RW	RW	—	—
LTO-2 テープ	—	R	RW	RW	—
LTO-1 テープ	—	—	R	RW	RW

DD VTL の設定

シンプルな DD VTL を設定するには、［はじめに］の章で説明されている構成ウィザードを使用します。

同様の内容は、「Data Domain オペレーティング システム初期構成ガイド」にも記載されています。

その後、次のトピックに進み、DD VTL の有効化、ライブラリの作成、テープの作成とインポートを行います。

注

導入環境に DD VTL クライアントとして AS400 システムが含まれている場合は、Data Domain システムと AS400 クライアント システム間の DD VTL 関係を構成する前に、DD VTL デフォルト オプションの構成（374 ページ）を参照して、VTL チェンジャーおよびドライブ用のシリアル番号プレフィックスを構成してください。

HA システムと DD VTL

HA システムは、DD VTL と互換性があります。ただし、フェールオーバー時に DD VTL ジョブが進行中である場合は、フェールオーバーの完了後にそのジョブを手動で再開する必要があります。

「Data Domain Operating System Backup Compatibility Guide」には、HA 環境で DD VTL を使用する場合の HBA、スイッチ、ファームウェア、およびドライバの要件の詳細が記載されています。

DD VTL テープからクラウドへ

DD VTL は、DD Cloud Tier ストレージへの VTL ヴォールトの格納をサポートします。この機能を使用するには、Data Domain システムが Cloud Tier の構成をサポートする必要があり、さらに VTL ライセンスに加えて Cloud Tier ライセンスを保持する必要があります。

ヴォールトをクラウド ストレージに格納する場合は、DD VTL を構成する前に DD Clout Tier ストレージの構成とライセンス登録を行ってください。DD Cloud Tier の要件、および DD Cloud Tier の構成方法の詳細については、DD Cloud Tier（479 ページ）を参照してください。

FC とネットワーク インターフェイスについての VTL の要件は、クラウド ベースのヴォールト ストレージとローカルのヴォールト ストレージとで等しくなります。DD VTL では、ヴォールトのクラウド ストレージを使用するための特別な構成は必要ありません。DD VTL を構成するときは、ヴォールトの場所としてクラウド ストレージを選択します。ただし、クラウド ベースのヴォールトを使用する場合、クラウド ベース ヴォールト固有のデータ管理オプションがあります。詳細については、クラウド ベースのヴォールトの使用（392 ページ）を参照してください。

DD VTL の管理

DD System Manager（Data Domain System Manager）または DD OS（Data Domain オペレーティング システム）CLI（コマンド ライン インターフェイス）を使用して DD VTL を管理することができます。ログイン後、DD VTL プロセスのステータスのチェック、ライセンス情報のチェック、オプションの確認と構成ができます。

ログイン

DD VTL（DD 仮想テープ ライブラリ）を管理する GUI（グラフィカル ユーザー インターフェイス）を使用するには、DD System Manager にログインします。

CLI 相当

次の CLI を使用してログインすることもできます。

```
login as: sysadmin
Data Domain OS
Using keyboard-interactive authentication.
Password:
```

SCSI ターゲット デーモンの有効化（CLI のみ）

CLI からログインする場合、scsitarget デーモン（ファイバー チャネル サービス）を有効にできます。このデーモンは、DD System Manager で DD VTL または DD Boost-FC の有効化を選択している間、有効になります。CLI では、これらのプロセスは個別に有効にする必要があります。

```
# scsitarget enable
Please wait ...
SCSI Target subsystem is enabled.
```

DD VTL へのアクセス

DD System Manager の左側のメニューで、［**Protocols**］ > ［**VTL**］を選択します。

Status

［**Virtual Tape Libraries**］> ［**VTL Service**］領域では、DD VTL プロセスのステータスを確認できます。上部にたとえば、［**Enabled: Running**］のように表示されます。ステータスの最初の部分は、［**Enabled**］（オン）または［**Disabled**］（オフ）になります。2 番目の部分は、次のプロセス状態のいずれかになります。

表 140 DD VTL プロセスの状態

State	説明
実行中	DD VTL プロセスが有効かつアクティブな状態です（緑で表示）。
起動中	DD VTL プロセスが起動中です。
停止中	DD VTL プロセスがシャットダウン中です。
Stopped	DD VTL プロセスが無効です（赤で表示）。
Timing out	DD VTL プロセスがクラッシュし、自動再起動を試行しています。
Stuck	自動再起動が何度か失敗すると、DD VTL プロセスは正常にシャットダウンできなくなるため、それを解決するための試行を実行中です。

DD VTL ライセンス

［I/OS License］ラインが、DD VTL ライセンスが適用されたかどうかを伝えます。Unlicensed と表示された場合、［**Add License**］を選択します。［Add License Key］ダイアログ ボックスにライセンス キーを入力します。［**Next**］および［**OK**］を選択します。

注

すべてのライセンス情報は、出荷時の構成プロセスの一環として入力されている必要がありますが、DD VTL を後日購入した場合、その時点では DD VTL ライセンス キーが DD システムに入力されていないことがあります。

CLI 相当

次の CLI を使用して、DD VTL ライセンスがインストールされていることを確認することもできます。

```
# elicense show
## License Key                    Feature
--    --------------------       -----------
1     DEFA-EFCD-FCDE-CDEF        Replication
2     EFCD-FCDE-CDEF-DEFA        VTL
--    --------------------       -----------
```

ライセンスが存在しない場合、各ユニットに購入したライセンスを示すドキュメント（クイック インストール ガイド）が付属しています。次のいずれかのコマンドを入力して、ライセンス キーを設定します。

```
# license add <license-code>
```

```
# elicense update <license-file>
```

I/OS License（IBM i ユーザー用）

IBM i のお客様については、［I/OS License］ラインがお使いの I/OS ライセンスが適用されているかどうかを示します。Unlicensed と表示された場合、［**Add License**］を選択します。いずれかの形式で有効な I/OS ライセンスを入力する必要があります。**xxxx-xxxx-xxxx-xxxx** または **xxxx-xxxx-xxxx-xxxx-xxxz** の形式で有効な I/OS ライセンスを入力する必要があります。IBM i システムで使用されるライブラリとドライブを作成するには、お使いの I/OS ライセンスをインストールする必要があります。［**Next**］および［**OK**］を選択します。

DD VTL の有効化

DD VTL で Data Domain HBA の WWN をカスタマー ファブリックにブロードキャストできるようにし、すべてのライブラリとライブラリ ドライブを有効化します。変更制御プロセスの形式での転送プランが必要な場合は、ゾーニングを促進するためにこのプロセスを有効にする必要があります。

手順

1. DD VTL ライセンスがあり、ファイル システムが有効化されていることを確認してください。
2. ［**Virtual Tape Libraries**］ > ［**VTL Service**］を選択します。
3. ［Status］領域の右にある［**Enable**］を選択します。
4. ［Enable Service］ダイアログで、［**OK**］を選択します。
5. DD VTL が有効になると、［Status］が［**Enabled: Running**］（緑字）に変わります。構成された DD VTL オプションが［Option Defaults］領域に表示されていることも確認してください。

   ［**CLI** 相当］

   ```
   # vtl enable Starting VTL, please wait ... VTL is enabled.
   ```

DD VTL の無効化

DD VTL を無効にすると、すべてのライブラリが閉じ、DD VTL プロセスがシャットダウンします。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］を選択します。
2. ［Status］領域の右にある［**Disable**］を選択します。
3. ［Disable Service］ダイアログで、［**OK**］を選択します。
4. DD VTL が無効になると、［Status］が［**Disabled: Stopped**］（赤字）に変わります。

   ［**CLI** 相当］

   ```
   # vtl disable
   ```

DD VTL オプションのデフォルト

［VTL Service］ページの［Option Default］領域には、デフォルトの DD VTL オプション（auto-eject、auto-offline、barcode-length）の現在の設定が表示されます。この設定は構成できます。

［**Virtual Tape Libraries**］ > ［**VTL Service**］領域には、お使いの DD VTL の現在のデフォルト オプションが表示されます。［**Configure**］を選択すると、これらの値のいずれかを変更できます。

表 141 オプションのデフォルト

項目	説明
プロパティ	構成されたオプションをリストします。 • auto-eject • auto-offline

表 141 オプションのデフォルト （続き）

項目	説明
	• barcode-length
値	構成されたオプションそれぞれの値を与えます。 • auto-eject：default (disabled)、enabled、disabled • auto-offline：default (disabled)、enabled、disabled • barcode-length：default (8)、6、8

DD VTL デフォルト オプションの構成

DD VTL のデフォルト オプションは、ライセンスの追加時、ライブラリの作成時、その後の任意の時点で構成できます。

注

DD VTL は、デフォルトで割り当てられたグローバル オプションであり、これらのオプションは、この方法を使用して手動で変更しない限り、グローバル オプションの変更時に必ず更新されます。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］を選択します。
2. ［Option Defaults］領域で［**Configure**］を選択します。［Configure Default Options］ダイアログで、デフォルト オプションのいずれかまたはすべてを変更します。

表 142 DD VTL デフォルト オプション

オプション	値	注
auto-eject	default（disabled）、enable、disable	自動取り出しを有効にすると、CAP（カートリッジ アクセス ポート）に入れられたテープが自動的に仮想ヴォールトに移動するようになります。ただし、次の場合は除きます。 • テープがヴォールトから来たものである場合（そのテープは CAP に残ります）。 • 値が 0（false）の ALLOW_MEDIUM_REMOVAL コマンドがライブラリに発行され、CAP から外へのメディアの取り外しができなくなっている場合。
auto-offline	default（disabled）、enable、disable	自動オフラインを有効化すると、テープ移動操作が実行される前にド

表 142 DD VTL デフォルト オプション （続き）

オプション	値	注
		ライブが自動的にオフラインになります。
barcode-length	default（8）、6、8（L180、RESTORER-L180、DDVTL チェンジャー モデルでは自動で 6 に設定）	DD VTL バーコードは 8 文字で構成されていますが、文字のタイプに応じて 6 または 8 文字がバックアップ アプリケーションに送信される場合があります。

3. ［**OK**］を選択します。
4. または、これらのサービス オプションをすべて無効化するには、［**Reset to Factory**］を選択します。値はただちに工場出荷時のデフォルトにリセットされます。

必要条件

DD VTL 環境に、DD VTL クライアントとして AS400 が含まれている場合は、AS400 を DD VTL 環境に追加する前に、シリアル番号プレフィックス用の DD VTL オプションを手動で構成します。これは、DD VTL を使用する複数の Data Domain システムがある場合に、シリアル番号が重複しないようにするために必要です。シリアル番号プレフィックスの値は、以下を満たす必要があります。

- 環境内の Data Domain システム上の他の DD VTL が同じプレフィックス番号を持たないようにした固有の 6 桁の値であること
- ゼロで終わらないこと

この値は、Data Domain システムの導入および DD VTL の構成時に 1 回だけ構成してください。これは、システム上で将来実施するすべての DD OS アップグレードでも存続します。この値を設定しても、DD VTL サービスを再開する必要はありません。この値を設定した後に作成されたすべての DD VTL ライブラリでは、シリアル番号に新しいプレフィックスが使用されます。

CLI equivalent

```
# vtl option set serial-number-prefix value
# vtl option show serial-number-prefix
```

ライブラリの扱い

ライブラリは、ドライブ、チェンジャー、CAP（カートリッジ アクセス ポート）、スロット（カートリッジ スロット）のある物理テープ ライブラリをエミュレートします。［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］を選択すると、構成されたすべてのライブラリの詳細情報が表示されます。

表 143 ライブラリ情報

項目	説明
Name	構成されたライブラリの名前。
Drives	ライブラリで構成されたドライブの数。
Slots	ライブラリで構成されたスロットの数。
CAPs	ライブラリで構成された CAP（カートリッジ アクセス ポート）の数。

［More Tasks］メニューから、ライブラリの作成と削除、テープの検索が行えます。

ライブラリの作成

DD VTL は、システムあたり最大 64 個のライブラリに対応しています。つまり、DD システムごとに 64 個の仮想テープ ライブラリ インスタンスを同時にアクティブにできます。

はじめに

導入環境に DD VTL クライアントとして AS400 システムが含まれている場合は、DD VTL ライブラリを作成して Data Domain システムと AS400 クライアント システム間の DD VTL 関係を構成する前に、DD VTL デフォルト オプションの構成（374 ページ）を参照して、VTL チェンジャーおよびドライブ用のシリアル番号プレフィックスを構成してください。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］を選択します。
2. ［**More Tasks**］ > ［**Library**］ > ［**Create**］を選択します。
3. ［Create Library］ダイアログで、次の情報を入力します。

表 144 ［Create Library］ダイアログ

フィールド	ユーザー入力
Library Name	英数字 1～32 文字で名前を入力します。
ドライブ数	ドライブの数（1～98）を入力します（「注」を参照）。作成されるドライブ数は、ライブラリに書き込まれるデータ ストリーム数に対応します。 注 DD VTL でサポートされるドライブの最大数は、DD システムにインストールされている CPU コア数とメモリ（該当する場合は、RAM と NVRAM 両方）の量によって異なります。
Drive Model	ドロップダウン リストから任意のモデルを選択します。 • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5（デフォルト） • HP-LTO-3 • HP-LTO-4 同一ライブラリ内でドライブ タイプまたはメディア タイプを混在させないでください。混在させると、バックアップ処理で予期せぬ結果やエラーが発生することがあります。
スロット数	ライブラリ内のスロットの数を入力します。検討すべき内容をいくつか示します。 • スロット数は、ドライブ数以上にする必要があります。 • ライブラリごとに最大 32,000 のスロットを保持できます。 • システムごとに最大 64,000 のスロットを保持できます。

表 144 ［Create Library］ダイアログ （続き）

フィールド	ユーザー入力
	• DD VTL の再構成を回避し、管理オーバーヘッドを減らすために、テープが DD VTL 内に留まり、ヴォールトにエクスポートする必要が生じないように、十分な数のスロットを用意してください。 • スロットの数で、ライセンスされるアプリケーションを検討してください。 たとえば、DD580 の標準の 100 GB カートリッジの場合は、5000 スロット構成できます。これで、500 TB まで十分に保持できます（適度に圧縮可能なデータの場合）。
Number of CAPs	（オプション）CAP（カートリッジ アクセス ポート）の数を入力します。 • ライブラリごとに最大 100 の CAP を保持できます。 • システムごとに最大 1000 の CAP を保持できます。 ガイダンスについては、オンライン サポート サイトで、使用しているバックアップ ソフトウェア アプリケーションのマニュアルを参照してください。
Changer Model Name	ドロップダウン リストから任意のモデルを選択します。 • L180（デフォルト） • RESTORER-L180 • TS3500 • i2000 • I6000 • DDVTL ガイダンスについては、オンライン サポート サイトで、使用しているバックアップ ソフトウェア アプリケーションのマニュアルを参照してください。また、DD VTL サポート マトリックスを参照して、エミュレート ライブラリとサポートされているソフトウェアの互換性を確認してください。
［オプション］	
auto-eject	default（disabled）、enable、disable
auto-offline	default（disabled）、enable、disable
barcode-length	default（8）、6、8（L180、RESTORER-L180、DDVTL チェンジャー モデルでは自動で 6 に設定）

4. ［**OK**］を選択します。

［Create Library status］ダイアログに［**Completed**］と表示されたら、［**OK**］を選択します。

新しいライブラリが［VTL Service］ツリーの［Libraries］アイコンの下に表示され、構成したオプションがそのライブラリの下にアイコンとして表示されます。ライブラリを選択すると、情報パネルにライブラリについての詳細が表示されます。

VTL とドライブへのアクセスは Access Group で管理される点に留意してください。

［**CLI** 相当］

```
# vtl add NewVTL model L180 slots 50 caps 5
This adds the VTL library, NewVTL. Use 'vtl show config NewVTL'
```

```
to view it.

# vtl drive add NewVTL count 4 model IBM-LTO-3
This adds 4 IBM-LTO-3 drives to the VTL library, NewVTL.
```

ライブラリの削除

テープがライブラリ内のドライブにあり、そのライブラリが削除された場合、そのテープはヴォールトに移動されますが、テープのプールは変更されません。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］を選択します。
2. ［**More Tasks**］ > ［**Library**］ > ［**Delete**］を選択します。
3. ［Delete Libraries］ダイアログで、削除する項目のチェックボックスを選択するか、選択されていることを確認します。
   - 各ライブラリの名前。
   - Library Names（すべてのライブラリを削除する場合）
4. ［**Next**］を選択します。
5. 削除するライブラリを確認し、確認ダイアログで［**Submit**］を選択します。
6. ［Delete Libraries Status］ダイアログに `Completed` と表示されたら、［**Close**］を選択します。選択されたライブラリが DD VTL から削除されます。

［**CLI** 相当］

```
# vtl del OldVTL
```

テープの検索

さまざまな基準（場所、プール、バーコードなど）を使用して、テープを検索できます。

手順

1. ［**Virtual Tape Libraries**］または［**Pools**］を選択します。
2. 検索する領域（ライブラリ、ヴォールト、プール）を選択します。
3. ［**More Tasks**］ > ［**Tapes**］ > ［**Search**］を選択します。
4. ［Search Tapes］ダイアログで、検索するテープに関する情報を入力します。

表 145 ［Search Tapes］ダイアログ

フィールド	ユーザー入力
Location	場所を指定するか、デフォルト（All）のままにします。
Pool	テープを検索するプールの名前を選択します。プールが作成されていない場合、［Default］プールを使用します。
Barcode	一意のバーコードを指定するか、デフォルト（*）のままにして、テープのグループを戻します。バーコードには、ワイルドカード（?と*）を使用できます。?は任意の 1 文字、*は 0 文字以上に一致します。

表 145 ［Search Tapes］ダイアログ （続き）

フィールド	ユーザー入力
Count	戻されるテープの最大数を入力します。このフィールドを空欄にすると、バーコードのデフォルト（*）が使用されます。

5. ［**Search**］を選択します。

選択されたライブラリの扱い

［**Virtual Tape Libraries**］ > ［ **VTL Service**］ > ［ **Libraries**］ > library を選択すると、選択されたライブラリの詳細情報が表示されます。

表 146 デバイス

項目	説明
Device	ドライブ、スロット、CAP（カートリッジ アクセス ポート）などのライブラリ内の構成要素。
ロード	メディアがロードされたデバイスの数。
空	メディアがロードされていないデバイスの数。
Total	ロードされた空のデバイスの総数。

表 147 オプション

プロパティ	値
auto-eject	enabled または disabled
auto-offline	enabled または disabled
barcode-length	6 または 8

表 148 Tapes

項目	説明
プール	テープが配置されているプールの名前。
Tape Count	そのプール内のテープ数。
容量	そのプール内のテープの構成された合計データ容量（GiB（ギビバイト、GB-ギガバイトの 2 進数相当））。
Used	そのプール内の仮想テープ上で使用されている領域の量。
Average Compression	そのプール内のテープで実現された圧縮の平均量（MB）。

［More Tasks］メニューから、ライブラリのオプションを削除、名前変更、または設定できます。さらに、テープの作成、削除、インポート、エクスポート、移動と、スロットおよび CAP の追加または削除を実行できます。

テープの作成

テープは、ライブラリまたはプールに作成できます。プールから開始した場合、まずテープが作成されて、次にテープがライブラリにインポートされます。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library または ［**Vault**］ or ［**Pools**］ > ［**Pools**］ > pool を選択します。
2. ［**More Tasks**］ > ［**Tapes**］ > ［**Create**］を選択します。
3. ［Create Tapes］ダイアログで、テープに関する以下の情報を入力します。

表 149 ［Create Tapes］ダイアログ

フィールド	ユーザー入力
Library（ライブラリーから開始された場合）	ドロップダウン メニューが有効な場合、ライブラリーを選択するか、デフォルトの選択を残します。
プール名	ドロップダウン リストから、テープが存在するプールの名前を選択します。プールが作成されていない場合、デフォルトのプールを使用します。
テープ数	ライブラリの場合、1 から 20 まで選択します。プールの場合、1 から 100,000 までを選択するか、デフォルト（20）のままにします。（サポートされるテープの数は無制限ですが、一度に 100,000 個以上のテープを作成することはできません）。
Starting Barcode	（フォーマット A99000LA を使用して）初期バーコード番号を入力します。
Tape Capacity	（オプション）各テープルに、1～4000 から GiB の数を指定します（この設定は、バーコード容量設定をオーバーライドします）。ディスク領域を効率的に使用するには、100 GiB 以下に指定します。

4. ［**OK**］、［**Close**］を選択します。

［**CLI** 相当］

```
 # vtl tape add A00000L1 capacity 100 count 5 pool VTL_Pool ...
added 5 tape(s)...
```

注

自動増分テープのボリューム名は、base10 形式にする必要があります。

テープの削除

テープは、ライブラリまたはプールから削除できます。ライブラリーから開始された場合、システムはまずテープをエクスポートした後、それを削除します。テープはライブラリーではなくヴォールト内にある必要があります。Replication デスティネーション DD システムでは、テープの削除は許可されていません。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries >** ］ library または ［**Vault**］ or ［**Pools**］ > ［**Pools >** ］ pool を選択します。
2. ［**More Tasks**］ > ［**Tapes**］ > ［**Delete**］を選択します。

3. ［Delete Tapes］ダイアログで、削除するテープに関する検索情報を入力して、［**Search**］を選択します。

表 150 ［Delete Tapes］ダイアログ

フィールド	ユーザー入力
Location	ドロップダウン リストが表示されている場合は、ライブラリを選択するか、デフォルトの［**Vault**］選択を残します。
プール	テープを検索するプールの名前を選択します。プールが作成されていない場合、デフォルトのプールを使用します。
バーコード	一意のバーコードを指定するか、デフォルト（*）が選択されたままにして、テープのグループを検索します。バーコードには、ワイルドカード（?と*）を使用できます。?は任意の 1 文字、* は 0 文字以上に一致します。
Count	戻されるテープの最大数を入力します。このフィールドを空欄にすると、バーコードのデフォルト（*）が使用されます。
Tapes Per Page	表示されるテープのページあたりの最大数を選択します。選択できる値は 15、30、45 です。
Select all pages	［**Select All Pages**］チェックボックスを選択して、検索クエリーが返すすべてのテープを選択します。
Items Selected	複数のページにまたがって選択されたテープの数を示します。各テープの選択に対して、自動的に更新されます。

4. 削除するテープのチェックボックスまたはすべてのテープを削除する見出し列のチェックボックスを選択し、［**Next**］を選択します。
5. 確認ウィンドウで［**Submit**］を選択し、［**Close**］を選択します。

注

テープが削除されると、ファイル システム クリーニング操作が終わるまで、テープに使用される物理ディスク領域は再利用されません。

［**CLI** 相当］

```
# vtl tape del barcode [count count] [pool pool]
```

例：

```
# vtl tape del A00000L1
```

注

範囲に従いアクションを起こすことができますが、その範囲内に紛失しているテープがある場合、そのアクションは停止します。

テープのインポート

［テープをインポートすると］、既存のテープはヴォールトからライブラリ スロット、ドライブ、または CAP（カートリッジ アクセス ポート）に移動されます。

一度にインポートできるテープの数は、ライブラリ内の空きスロットの数によって制限されます。つまり、現在の空きスロットの数を超える数のテープはインポートできません。

ライブラリの使用可能なスロットを表示するには、スタック メニューからライブラリを選択します。ライブラリの情報パネルには、［Empty］列にカウントが表示されます。

- テープがドライブ内にあり、テープの元がスロットであることが分かっている場合、そのスロットが予約されます。
- テープがドライブ内にあり、テープの元が分からない（スロットまたは CAP）場合、そのスロットが予約されます。
- テープがドライブ内にあり、テープの元が CAP であることが分かっている場合、そのスロットが予約されます （そのテープは、ドライブから削除されると CAP に戻ります）。
- テープをドライブに移動するには、次のテープの移動に関するセクションを参照してください。

手順

1. 手順 a または手順 b を使用して、テープをインポートできます。

   a. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library を選択します。次に、［**More Tasks**］ > ［**Tapes**］ > ［**Import**］を選択します。［Import Tapes］ダイアログにインポートするテープに関する検索情報を入力して、［**Search**］を選択します。

   表 151 ［Import Tapes］ダイアログ

フィールド	ユーザー入力
Location	ドロップダウン リストがある場合は、テープの場所を選択するか、デフォルトの［**Vault**］のままにします。
プール	テープを検索するプールの名前を選択します。プールが作成されていない場合、デフォルトのプールを使用します。
バーコード	一意のバーコードを指定するか、デフォルト（*）のままにして、テープのグループを戻します。バーコードには、ワイルドカード（?と*）を使用できます。?は任意の 1 文字、*は 0 文字以上に一致します。
Count	戻されるテープの最大数を入力します。このフィールドを空欄にすると、バーコードのデフォルト（*）が使用されます。
［Select Destination］ > ［Device］	テープがインポートされる宛先デバイスを選択します。使用できる値は、Drive、CAP、Slot です。
Tapes Per Page	ページあたりの最大表示テープ数を選択します。取り得る値は 15、30、45 です。
Items Selected	複数のページにまたがって選択されたテープの数を示します。各テープの選択に対して、自動的に更新されます。

   前述の条件に基づき、インポートするテープを選択するため、テープのデフォルト セットが検索されます。プール、バーコード、またはカウントが変更された場合、［Search］を選択して、選択可能なテープのセットを更新します。

   b. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library > ［**Changer**］ > ［**Drives**］ > drive > ［**Tapes**］を選択します。次の項目の隣にあるチェックボックスを選択して、インポートするテープを選択します。

   - 個別のテープ ドライブ
   - ［**Barcode**］列（現在のページ上のすべてのテープを選択する場合）、または

- ［**Select all pages**］チェックボックス（検索クエリーが返すすべてのテープを選択する場合）。

［Location］に Vault が表示されているテープのみインポートできます。

［**Import from Vault**］を選択します。このボタンはデフォルトでは無効になっており、選択されたテープがすべてヴォールトからのものである場合のみ有効化されます。

2. ［Import Tapes: library］ビューから、サマリー情報とテープ リストを確認し、［**OK**］を選択します。
3. ステータス ウィンドウで［**Close**］を選択します。

［**CLI** 相当］

```
# vtl tape show pool VTL_Pool
Processing tapes....
Barcode  Pool     Location State    Size    Used (%)           Comp ModTime
-------- -------- -------- ----- ------- --------------- ---- -------------------
A00000L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00001L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00002L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00003L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
A00004L3 VTL_Pool vault    RW    100 GiB 0.0 GiB (0.00%) 0x   2010/07/16 09:50:41
-------- -------- -------- ----- ------- --------------- ---- -------------------
VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x

# vtl import NewVTL barcode A00000L3 count 5 pool VTL_Pool
... imported 5 tape(s)...

# vtl tape show pool VTL_Pool
Processing tapes....

VTL Tape Summary
----------------
Total number of tapes:     5
Total pools:               1
Total size of tapes:       500 GiB
Total space used by tapes: 0.0 GiB
Average Compression:       0.0x
```

テープのエクスポート

［テープをエクスポートする］と、スロット、ドライブ、CAP（カートリッジ アクセス ポート）からテープが削除され、テープがヴォールトに送信されます。

手順

1. テープは、次のステップ a.またはステップ b.を使用してエクスポートできます。
   a. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library を選択します。次に、［**More Tasks**］ > ［**Tapes**］ > ［**Export**］を選択します。［Export Tapes］ダイアログで、エクスポートするテープに関する検索情報を入力して、［**Search**］を選択します。

表 152 ［Export Tapes］ダイアログ

フィールド	ユーザー入力
Location	ドロップダウン リストが表示されている場合は、テープがあるライブラリの名前を選択するか、選択されているライブラリを残します。
プール	テープを検索するプールの名前を選択します。プールが作成されていない場合、デフォルトのプールを使用します。
バーコード	一意のバーコードを指定するか、デフォルト（*）のままにして、テープのグループを戻します。バーコードには、ワイルドカード（?と*）を使用できます。?は任意の 1 文字、*は 0 文字以上に一致します。
Count	戻されるテープの最大数を入力します。このフィールドを空欄にすると、バーコードのデフォルト（*）が使用されます。
Tapes Per Page	ページあたりの最大表示テープ数を選択します。取り得る値は 15、30、45 です。
Select all pages	［**Select All Pages**］チェックボックスを選択して、検索クエリーが返すすべてのテープを選択します。
Items Selected	複数のページにまたがって選択されたテープの数を示します。各テープの選択に対して、自動的に更新されます。

b. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library > ［**Changer**］ > ［**Drives**］ > drive > ［**Tapes**］を選択します。次の項目の隣にあるチェックボックスを選択して、エクスポートするテープを選択します。

- 個別のテープ ドライブ
- ［**Barcode**］列（現在のページ上のすべてのテープを選択する場合）、または
- ［**Select all pages**］チェックボックス（検索クエリーが返すすべてのテープを選択する場合）。

［Location］列のライブラリ名が付いているテープのみエクスポートできます。

［**Export from Library**］を選択します。このボタンはデフォルトでは無効になっており、選択したすべてのテープに、［Location］列のライブラリ名が付いている場合のみ有効になります。

2. ［Export Tapes: library］ビューから、サマリー情報とテープ リストを確認し、［**OK**］を選択します。
3. ステータス ウィンドウで［**Close**］を選択します。

［**CLI** 相当］

```
# vtl export NewVTL cap address 1 count 4
... exported 4 tape(s)...
```

ライブラリ内のデバイス間のテープの移動

テープをライブラリ内の物理デバイス間で移動して、物理テープ ライブラリのバックアップ ソフトウェア プロシージャを模倣できます（スロットからドライブ、スロットから CAP、CAP からドライブ、またはその逆にテープが移動します）。物理テープ ライブラリでは、バックアップ ソフトウェアはライブラリ外にテープを移動させません。そのため、宛先ライブラリは変更できず、明確化のためにのみ表示されます。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > ［**library**］を選択します。

   ライブラリから開始した場合、［Tapes］パネルでテープはデバイス間でしか移動できない点に留意してください。

2. ［**More Tasks**］ > ［**Tapes**］ > ［**Move**］を選択します。

   ライブラリから開始した場合、［Tapes］パネルでテープはデバイス間でしか移動できない点に留意してください。

3. ［Move Tape］ダイアログで、移動するテープに関する検索情報を入力して、［**Search**］を選択します。

   表 153 ［Move Tape］ダイアログ

フィールド	ユーザー入力
Location	場所は変更できません。
Pool	プールを選択します
バーコード	一意のバーコードを指定するか、デフォルト（*）のままにして、テープのグループを戻します。バーコードには、ワイルドカード（?と*）を使用できます。?は任意の 1 文字、*は 0 文字以上に一致します。
Count	戻されるテープの最大数を入力します。このフィールドを空欄にすると、バーコードのデフォルト（*）が使用されます。
Tapes Per Page	ページあたりの最大表示テープ数を選択します。取り得る値は 15、30、45 です。
Items Selected	複数のページにまたがって選択されたテープの数を示します。各テープの選択に対して、自動的に更新されます。

4. 検索結果リストから、移動するテープを選択します。
5. 次のいずれかを実行します。
   a. ［Device］リストからデバイス（スロット、ドライブ、CAP など）を選択し、2 番目以降のテープのシーケンシャル番号を使用して開始アドレスを入力します。各テープを移動するには、指定されたアドレスが使用されている場合、次の使用可能なアドレスを使用します。
   b. ドライブ内のテープが元々スロットから来ており、後でそのスロットに戻される場合、またはテープが次の使用可能なスロットに移動される場合、アドレスは空のままとします。
6. ［**Next**］を選択します。
7. ［Move Tape］ダイアログで、サマリー情報とテープ リストを確認し、［**Submit**］を選択します。
8. ステータス ウィンドウで ［**Close**］を選択します。

スロットの追加

構成されたライブラリからスロットを追加して、ストレージ エレメントの数を変更します。

注

一部のバックアップ アプリケーションは自動的には、スロットが DD VTL に追加されたことを認識しません。アプリケーションがこのタイプの変更を認識するように構成する方法の詳細については、アプリケーションのドキュメントを参照してください。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library を選択します。
2. ［**More Tasks**］ > ［**Slots**］ > ［**Add**］を選択します。
3. ［Add Slots］ダイアログで、追加するスロットの数を［Number of Slots］に入力します。システム上の 1 つのライブラリまたはすべてのライブラリ内のスロットの総数は、最大でライブラリ 1 つあたり 32,000、システム 1 つあたり 64,000 です。
4. ステータスに `Completed` と表示されたら、［**OK**］および［**Close**］を選択します。

スロットの削除

構成されたライブラリからスロットを削除して、ストレージ エレメントの数を変更できます。

注

一部のバックアップ アプリケーションは自動的には、スロットが DD VTL から削除されていることを認識しません。アプリケーションがこのタイプの変更を認識するように構成する方法の詳細については、アプリケーションのドキュメントを参照してください。

手順

1. 削除したいスロットにカートリッジが含まれる場合、そのカートリッジをヴォールトに移動します。システムは、空のコミットされていないスロットのみ削除します。
2. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > bibliothèque を選択します。
3. ［**More Tasks**］ > ［**Slots**］ > ［**Delete**］を選択します。
4. ［Delete Slots］ダイアログで、［Number of Slots］に削除するスロットの数を入力します。
5. ステータスに `Completed` と表示されたら、［**OK**］および［**Close**］を選択します。

CAP の追加

構成されたライブラリから CAP（カートリッジ アクセス ポート）を追加して、ストレージ エレメントを変更できます。

注

CAP を使用するバックアップ アプリケーションの数は制限されています。CAP に対応していることを確認するため、アプリケーションのドキュメントを参照してください。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries >**］ library を選択します。
2. ［**More Tasks**］ > ［**CAPs**］ > ［**Add**］を選択します。
3. ［Add CAPs］ダイアログで、［Number of CAPs］に追加する CAP の数を入力します。追加できる数は、1 ライブラリあたり 1～100 CAP、1 システムあたり 1～1,000 CAP です。

4. ステータスに Completed と表示されたら、［**OK**］および［**Close**］を選択します。

CAP の削除

構成されたライブラリーから CAP（カートリッジ アクセス ポート）を削除して、ストレージ エレメントを変更できます。

注

一部のバックアップ アプリケーションは自動的には、CAP が DD VTL から削除あれていることを認識しません。アプリケーションがこのタイプの変更を認識するように構成する方法の詳細については、アプリケーションのドキュメントを参照してください。

手順

1. 削除したい CAP にカートリッジが含まれる場合、そのカートリッジをヴォールトに移動します。自動的に移動される場合もあります。
2. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library を選択します。
3. ［**More Tasks**］ > ［**CAPs**］ > ［**Delete**］を選択します。
4. ［Delete CAPs］ダイアログで、削除する CAP の数を入力します。削除できるのは、1 ライブラリーあたり 100 CAP、1 システムあたり 1000 CAP です。
5. ステータスに Completed と表示されたら、［**OK**］および［**Close**］を選択します。

チェンジャー情報の表示

DD VTL ごとに 1 つのチェンジャーのみ使用できます。チェンジャー モデルの選択は、個別のユーザーの構成によって異なります。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］を選択します。
2. 特定のライブラリを選択します。
3. 展開されていない場合、左側のプラス記号（[**+**]）を選択してライブラリを開き、プラス記号構成要素を選択して、［Changer information］のパネルを表示します。次の情報が表示されます。

表 154 ［Changer information］パネル

項目	説明
Vendor	チェンジャーを製造したベンダーの名前
製品	モデル名
リビジョン	リビジョン レベル
シリアル番号	チェンジャーのシリアル番号

ドライブの扱い

［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library > ［**Drives**］を選択すると、選択したライブラリのすべてのドライブの詳細情報が表示されます。

表 155 ［Drives information］パネル

列	説明
Drive	名前ごとのドライブのリスト。名前は「Drive #」です。#は 1～n で、ドライブ リストにあるドライブの、アドレスまたは場所を表します。
Vendor	IBM などのドライブの製造業者またはベンダー。
Product	ULTRIUM-TD5 などのドライブの製品名。
リビジョン	ドライブ製品のリビジョン番号。
Serial Number	ドライブ製品のシリアル番号。
Status	ドライブのステータス（Empty、Open、Locked、または Loaded）。テープは、ロックまたはロードするドライブ用のものである必要があります。
Tape	ドライブ内のテープのバーコード（もしあれば）。
Pool	ドライブ内のテープのプール（もしあれば）。

［**Tape and library drivers**］：ドライブを扱う場合、IBM LTO-1、IBM LTO-2、IBM LTO-3、IBM LTO-4、IBM LTO-5（デフォルト）、HP-LTO-3、HP-LTO-4 ドライブおよび StorageTek L180（デフォルト）、RESTORER-L180、IBM TS3500、I2000、I6000、DDVTL ライブラリに対応するバックアップ ソフトウェア ベンダーが提供するテープおよびライブラリ ドライバーを使用する必要があります。詳細については、ベンダーの「Application Compatibility Matrices and Integration Guides」を参照してください。ドライブを構成する場合、使用中のプラットフォームによって決定されるバックアップ データ ストリームには制限がある点に留意してください。

［**LTO drive capacities**］：DD システムは LTO ドライブを仮想ドライブとして扱うため、各ドライブ タイプの最大容量を 4 TiB（4000 GiB）に設定できます。各 LTO ドライブ タイプのデフォルト容量は次のとおりです。

- LTO-1 ドライブ：100 GiB
- LTO-2 ドライブ：200 GiB
- LTO-3 ドライブ：400 GiB
- LTO-4 ドライブ：800 GiB
- LTO-5 ドライブ：1.5 TiB

［**Migrating LTO-1 tapes**］：既存の LTO-1 タイプ VTL から他の対応 LTO タイプのテープとドライブを含む VTL にテープを移行できます。移行オプションはバックアップ アプリケーションごとに異なるため、アプリケーションに固有の LTO テープ移行ガイドの指示に従います。適切なガイドを見つけるには、オンライン サポート サイトにアクセスし、検索テキスト ボックスの［**LTO Tape Migration for VTLs**］に入力します。

［**Tape full: Early warning**］：残りのテープ スペースがフルに近くなる（99.9%より大きく 100%より小さい）と警告が出されます。アプリケーションは、100%の容量に達するテープの終わりに来るまで、書き込みを続けることができます。ただし、最後の書き込みはリカバリ不可能です。

［More Tasks］メニューから、ドライブを作成または削除できます。

ドライブの作成

［DD VTL でサポートされるドライブ数］セクションを参照し、特定の DD VTL でサポートされるドライブの最大数を決定します。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library > ［**Changer**］ > ［**Drives**］を選択します。
2. ［**More Tasks**］ > ［**Drives**］ > ［**Create**］を選択します。
3. ［Create Drive］ダイアログ ボックスで、次の情報を入力します。

   表 156 ［Create Drive］ダイアログ

フィールド	ユーザー入力
Location	ライブラリ名を選択するか、名前が選択された状態のままにします。
ドライブ数	この章の［DD VTL でサポートされるドライブ数］セクションにある表を参照してください。
Model Name	ドロップダウン リストからモデルを選択します。すでに他のドライブが存在する場合、このオプションは非アクティブになり、既存のドライブ タイプを使用する必要があります。同じライブラリ内でドライブ タイプを混合することはできません。 • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5（デフォルト） • HP-LTO-3 • HP-LTO-4

4. ［**OK**］を選択し、ステータスに `Completed` が表示されたら、［**OK**］を選択します。

   追加されたドライブがドライブ リストに表示されます。

ドライブの削除

ドライブは削除する前に空にする必要があります。

手順

1. 削除したいドライブ内にテープがある場合、そのテープを削除します。
2. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries >** ］library［**> Changer**］ > ［**Drives**］を選択します。
3. ［**More Tasks**］ > ［**Drives**］ > ［**Delete**］を選択します。
4. ［Delete Drives］ダイアログで、削除するドライブのチェックボックスまたはすべての設定を削除する［**Drive**］チェックボックスを選択します。
5. ［**Next**］を選択し、正しい削除対象のドライブが選択されていることを確認した後、［**Submit**］を選択します。
6. ［Delete Drive Status］ダイアログに `Completed` と表示されたら、［**Close**］を選択します。

ドライブが［Drives］リストから削除されます。

選択されたドライブの扱い

［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > library > ［**Drives**］ >drive を選択すると、選択されたライブラリの情報が表示されます。

表 157 ［Drive］タブ

列	説明
Drive	名前ごとのドライブのリスト。名前は「Drive #」です。#は 1～n で、ドライブ リストにあるドライブの、アドレスまたは場所を表します。
Vendor	IBM などのドライブの製造業者またはベンダー。
Product	ULTRIUM-TD5 などのドライブの製品名。
Revision	ドライブ製品のリビジョン番号。
Serial Number	ドライブ製品のシリアル番号。
Status	ドライブのステータス（Empty、Open、Locked、または Loaded）。テープは、ロックまたはロードするドライブ用のものである必要があります。
Tape	ドライブ内のテープのバーコード（もしあれば）。
Pool	ドライブ内のテープのプール（もしあれば）。

表 158 ［Statistics］タブ

列	説明
Endpoint	エンドポイントの特定の名前。
Ops/s	1 秒あたりの操作数。
Read KiB/s	1 秒あたりの KiB 数単位の読み取り速度。
Write KiB/s	1 秒あたりの KiB 数単位の書き込み速度。

［More Tasks］メニューから、ドライブを削除するか、更新を実行できます。

テープの扱い

テープはファイルとして表されます。テープは、ヴォールトからライブラリにインポートできます。テープは、ライブラリからヴォールトにエクスポートできます。テープは、複数のドライブ、スロット（カートリッジ スロット）、CAP（カートリッジ アクセス ポート）間で、1 つのライブラリ内で移動できます。

テープを作成すると、ヴォールトに追加されます。テープは、ヴォールトに追加した後、インポート、エクスポート、移動、検索、削除が可能です。

［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］> library > ［**Tapes**］を選択すると、選択されたライブラリのすべてのテープの情報が表示されます。

表 159 テープの説明

項目	説明
バーコード	テープの一意のバーコード。
プール	テープを保持するプールの名前。Default プールは、ユーザーが作成したプールに割り当てられていないすべてのテープを保持します。
場所	テープの場所（ライブラリ（ドライブ、CAP、またはスロット番号）または仮想ヴォールト）。
State	テープの状態。 • RW：読み取り/書き込み可能 • RL：保存ロック • RO：読み取り専用 • WP：ライト プロテクト • RD：レプリケーション デスティネーション
容量	テープの合計容量。
使用済	テープ上で使用されているスペースの量。
Compression	テープ上のデータで実行される圧縮の量。
最終更新日	テープの情報の最終変更日。経過時間ベース ポリシーにシステムが使用する変更時間は、DD System Manager のテープ情報セクションに表示される最終変更時間とは異なる場合があります。
Locked Until	DD Retention Lock 期限が設定されている場合、設定された時間が表示されます。保存ロックが存在する場合、この値は `Not specified` です。

情報パネルで、ヴォールトからのテープのインポート、ライブラリへのテープのエクスポート、テープの状態の設定、テープの作成、またはテープの削除が可能です。

［More Tasks］メニューから、テープを移動できます。

テープの書き込みまたは保存ロック状態の変更

テープの書き込みまたは保存ロック状態を変更するには、テープが作成およびインポート済みである必要があります。DD VTL テープは、標準 Data Domain Retention Lock ポリシーに従います。テープの保存期間が満了すると、そのテープには書き込みできず、変更もできません（ただし、削除は可能です）。

手順

1. ［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Libraries**］ > ［**library**］ > ［**Tapes**］を選択します。
2. リストから変更するテープを選択し、［**Set State**］（リストの上）を選択します。
3. ［Set Tape State］ダイアログで、［**Read-Writeable**］、［**Write-Protected**］、または［**Retention-Lock**］を選択します。
4. 状態が Retention-Lock である場合、
   - 指定された日数、週数、月数、年数でテープの有効期限を入力します
   - または、カレンダー アイコンを選択し、そのカレンダーから日付を選択します。Retention-Lock は、選択された日付の正午に期限切れします。

5. ［**Next**］を選択し、［**Submit**］を選択して状態を変更します。

ヴォールトの扱い

ヴォールトには、どのライブラリでも使用されていないテープが保持されます。テープは、ライブラリまたはヴォールトに置けます。

［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Vault**］を選択すると、ヴォールト内の Default プールとその他の既存プールの詳細情報が表示されます。

DD Cloud Tier と DD VTL があるシステムでは、クラウド ストレージにヴォールトを保存するオプションを選択できます。

表 160 プール サマリー

項目	説明
Pool Count	VTL プールの数。
Tape Count	プール内のテープ数。
Size	プール内のスペースの総量。
Logical Used	プール内で使用されているスペースの量。
Compression	プール内の圧縮の平均量。

［**Protection Distribution**］ウィンドウには、次の情報が表示されます。

注

このテーブルは、Data Domain システムで DD Cloud Tier が有効になっている場合にのみ表示されます。

表 161 Protection Distribution

項目	説明
ストレージ タイプ	ヴォールトまたはクラウド。
クラウド プロバイダー	DD Cloud Tier にテープが配置されているシステムの場合、各クラウド プロバイダの列があります。
Logical Used	プール内で使用されているスペースの量。
Pool Count	VTL プールの数。
Tape Count	プール内のテープ数。

［More Tasks］メニューから、ヴォールトでテープを作成、削除、検索できます。

クラウド ベースのヴォールトの使用

DD VTL では、DD クラウド階層に格納されたヴォールトの構成に固有の、いくつかのパラメーターをサポートします。

クラウド ベースのヴォールト ストレージを使用する際は以下の操作が行えます。

- 指定された VTL プールの、データ移行ポリシーとクラウド ユニット情報を構成します。次のコマンドを実行します。**`vtl pool modify <pool-name> data-movement-policy {user-`**

managed | age-threshold <days> | none} to-tier {cloud} cloud-unit <cloud-unit-name>
利用可能なデータ移行ポリシーは次のとおりです。

- ユーザー管理：管理者はプールでこのポリシーを設定すると、プールからクラウド階層へと移行するテープを手動で選択できます。テープを選択した後の最初のデータ移行操作時に、テープはクラウド階層に移行します。
- 経過時間の閾値：管理者はプールでこのポリシーを設定すると、プールからクラウド階層へと移行するテープを、テープの経過時間に基づいて DD VTL が自動で選択できるよう許可できます。テープは閾値に達してから移行の対象として選択され、テープが選択されてから最初のデータの移動で移行されます。

- クラウド階層へ移行するテープを選択します。次のコマンドを実行します。**vtl tape select-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}**。
- クラウド階層へ移行するよう指定したテープを選択解除します。次のコマンドを実行します。**vtl tape deselect-for-move barcode <barcode> [count <count>] pool <pool> to-tier {cloud}**。
- クラウド階層からテープをリコールします。次のコマンドを実行します。**vtl tape recall start barcode <barcode> [count <count>] pool <pool>**
リコール後は、テープがローカルの DD VTL ヴォールトに存在し、かつアクセスできるようライブラリにインポートする必要があります。

注

テープの現在のロケーションを確認するには `vtl tape show` のコマンドを実行します。テープのロケーションは、クラウド階層へ、またはクラウド階層からテープを移動して 1 時間以内に更新されます。

データ移行のための VTL プールの準備

ローカル ヴォールトから DD Cloud Tier への VTL データの移行を管理するデータ移動ポリシーを VTL プール上に設定します。

VTL のデータ移行は、テープ ボリューム レベルで発生します。個々のテープ ボリュームまたはテープ ボリュームのコレクションをクラウド階層へ移行できますが、ヴォールトの場所からしか移行できません。VTL の他の要素のテープは移行できません。

注

VTL のデフォルト プールとヴォールト、`/data/col1/backup` ディレクトリおよびレガシー ライブラリ構成は、クラウドへのテープの移行には使用できません。

手順

1. ［**Protocols**］ > ［**DD VTL**］を選択します。
2. プールのリストを展開し、DD Cloud Tier への移行を有効にするプールを選択します。
3. ［**Cloud Data Movement**］ウィンドウで ［**Cloud Data Movement Policy**］の下の［**Create**］をクリックします。
4. ［**Policy**］ドロップダウン リストで、データ移動ポリシーを選択します。
   - ［テープの経過日数］
   - ［手動選択］

5. データ移動ポリシーの詳細を設定します。
   - ［**Age of tapes in days**］では、これを経過するとテープを DD Cloud Tier に移行する経過時間閾値を選択し、デスティネーションのクラウド ユニットを指定します。
   - ［**Manual selection**］では、デスティネーションのクラウド ユニットを指定します。
6. ［**Create**］をクリックします。

注

データ移動ポリシーを作成した後は、［**Edit**］ボタンと［**Clear**］ボタンを使用してデータ移動ポリシーを変更および削除することができます。

CLI 相当機能

手順

1. データ移行ポリシーをユーザー管理または経過時間のしきい値に設定します。

注

VTL プールとクラウド ユニット名は大文字と小文字を区別し、正しくない場合、コマンドは失敗します。

- ユーザー管理にデータ移行ポリシーを設定するには、次のコマンドを実行します。
  `vtl pool modify cloud-vtl-pool data-movement-policy user-managed to-tier cloud cloud-unit ecs-unit1`

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy is set to "user-managed" for VTL pool "cloud-vtl-pool".
```

- 経過時間のしきい値にデータ移行ポリシーを設定するには、次のコマンドを実行します。

注

最小値は 14 日で、最大値は 182,250 日です。

```
vtl pool modify cloud-vtl-pool data-movement-policy age-
threshold 14 to-tier cloud cloud-unit ecs-unit1
```

```
**   Any tapes that are already selected will be migrated on the next data-movement
run.
VTL data-movement policy "age-threshold" is set to 14 days for the VTL pool "cloud-
vtl-pool".
```

2. VTL プールのデータ移動ポリシーを確認します。

   次のコマンドを実行します。
   `vtl pool show all`

```
VTL Pools
Pool                    Status   Tapes   Size (GiB)   Used (GiB)   Comp   Cloud Unit
Cloud Policy
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
cloud-vtl-pool          RW          50          250           41    45x   ecs-unit1
user-managed
Default                 RW           0            0            0     0x   -
none
---------------------   ------   -----   ----------   ----------   ----   ----------
------------
8080 tapes in 5 pools
```

```
 RO  : Read Only
 RD  : Replication Destination
 BCM : Backwards-Compatibility
```

3. VTL プールの MTree のポリシーの確認は app-managed です。

   次のコマンドを実行します。
   data-movement policy show all

```
Mtree                        Target(Tier/Unit Name)    Policy        Value
-------------------------    ----------------------    -----------   -------
/data/col1/cloud-vtl-pool    Cloud/ecs-unit1           app-managed   enabled
-------------------------    ----------------------    -----------   -------
```

バックアップ アプリケーション インベントリからのテープの削除

バックアップ アプリケーションを使用して、クラウドへと移行するテープ ボリュームのマーキングとインベントリ登録がバックアップ アプリケーションの要件に従っているかを検証します。

データ移行するテープ ボリュームの選択

DD Cloud Tier に移行するテープ（すぐに移行するか、または次回のスケジュール設定されたデータ移行で移行するか）を手動で選択するか、移行スケジュールからテープを手動で削除します。

はじめに

バックアップ アプリケーションがクラウド ストレージに移動されたボリュームのステータス変化を認識することを確認します。最新のボリューム ステータスを反映するように、インベントリを更新するには、バックアップ アプリケーションのために必要な手順を実行します。

テープがヴォールト内にない場合は、DD Cloud Tier に移行することはできません。

手順

1. ［**Protocols**］ > ［**DD VTL**］を選択します。
2. プールのリストを展開し、DD Cloud Tier にテープを移行するように構成されたプールを選択します。
3. ［Pool］パネルで［**Tape**］タブをクリックします。
4. DD Cloud Tier への移行対象のテープを選択します。
5. 次回のスケジュール設定された移行でテープを移行するには［**Select for Cloud Move**］を、今すぐテープを移行するには［**Move to Cloud Now**］をクリックします。

   注

   データ移動ポリシーがテープの経過時間に基づいている場合、テープは Data Domain システムによって移行対象として自動的に選択されるため、［**Select for Cloud Move**］は使用できません。

6. 確認ダイアログで［**Yes**］をクリックします。

データ移行対象からのテープ ボリュームの選択解除

DD Cloud Tier への移行対象として選択されたテープを移行スケジュールから削除できます。

手順

1. ［**Protocols**］ > ［**DD VTL**］を選択します。
2. プールのリストを展開し、DD Cloud Tier にテープを移行するように構成されたプールを選択します。

3. ［Pool］パネルで［**Tape**］タブをクリックします。
4. DD Cloud Tier への移行対象のテープを選択します。
5. ［**Unselect Cloud Move**］をクリックして移行スケジュールからテープを削除します。
6. 確認ダイアログで［**Yes**］をクリックします。

CLI 相当機能

手順

1. 移動するテープ ボリュームのスロットの位置を識別します。

   次のコマンドを実行します。
   `vtl tape show cloud-vtl`

```
Processing tapes....
Barcode    Pool             Location            State    Size           Used (%)
Comp   Modification Time
--------   --------------   -----------------   -----   -----   -----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1    RW      5 GiB   5.0 GiB (99.07%)
205x   2017/05/05 10:43:43
T00002L3   cloud-vtl-pool   cloud-vtl slot 2    RW      5 GiB   5.0 GiB (99.07%)
36x   2017/05/05 10:45:10
T00003L3   cloud-vtl-pool   cloud-vtl slot 3    RW      5 GiB   5.0 GiB (99.07%)
73x   2017/05/05 10:45:26
```

2. DD VTL からエクスポートするテープのスロットを数値で指定します。

   次のコマンドを実行します。
   `vtl export cloud-vtl-pool slot 1 count 1`

3. テープがヴォールトにあることを確認します。

   次のコマンドを実行します。
   `vtl tape show vault`

4. データ移行するテープを選択します。

   次のコマンドを実行します。
   `vtl tape select-for-move barcode T00001L3 count 1 pool cloud-vtl-pool to-tier cloud`

   注

   データ移行ポリシーが経過時間のしきい値の場合、データ移動は 15～20 分後に自動的に開始します。

5. 次のデータ移行処理中にクラウド ストレージへの移行が予定されているテープの一覧を表示します。データ移行が予定されているテープの［場所］列には `(S)` と表示されます。

   次のコマンドを実行します。
   `vtl tape show vault`

```
Processing tapes.....
Barcode    Pool               Location    State      Size           Used (%)   Comp
Modification Time
--------   ----------------   ---------   ------   ------   ----------------   ----
-------------------
T00003L3   cloud-vtl-pool     vault (S)   RW        5 GiB   5.0 GiB (99.07%)    63x
2017/05/05 10:43:43
T00006L3   cloud-vtl-pool     ecs-unit1   n/a       5 GiB   5.0 GiB (99.07%)    62x
2017/05/05 10:45:49
--------   ----------------   ---------   ------   ------   ----------------   ----
-------------------
* RD : Replication Destination
```

```
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4024
Total pools:               3
Total size of tapes:       40175 GiB
Total space used by tapes: 39.6 GiB
Average Compression:       9.7x
```

6. データ移行ポリシーがユーザー管理の場合は、データ移行操作を開始します。

   次のコマンドを実行します。
   `data-movement start`

7. データ移行操作のステータスを確認します。

   次のコマンドを実行します。
   `data-movement watch`

8. テープ ボリュームがクラウド ストレージに正常に移行できたことを確認します。

   次のコマンドを実行します。
   `vtl tape show all cloud-unit ecs-unit1`

```
Processing tapes.....
Barcode  Pool           Location  State  Size         Used (%) Comp Modification Time
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
T00001L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  89x 2017/05/05 10:41:41
T00006L3 cloud-vtl-pool ecs-unit1 n/a   5 GiB 5.0 GiB (99.07%)  62x 2017/05/05 10:45:49
-------- -------------- --------- ----- ----- ---------------- ---- -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     4
Total pools:               2
Total size of tapes:       16 GiB
Total space used by tapes: 14.9 GiB
Average Compression:       59.5x
```

クラウド上のデータの復元

バックアップ アプリケーション サーバからのリストアのためにクライアントがデータを要求する際、バックアップ アプリケーションはクラウド ユニットから要求された必要なボリュームへのリクエストのメッセージまたは警告を生成する必要があります。

バックアップ アプリケーションがボリュームの存在を通知される前に、クラウドからボリュームをリコールして、Data Domain VTL ライブラリにチェックインする必要があります。

注

クラウド ストレージに移動されたボリュームのステータス変化をバックアップ アプリケーションが認識できることを確認します。バックアップ アプリケーションに対する次の手順を実行してインベントリを更新し、最新のボリュームの状態を反映するようにします。

クラウド ストレージからのテープ ボリュームの手動リコール

DD Cloud Tier からテープをローカルの VTL ヴォールトにリコールします。

手順

1. ［**Protocols**］ > ［**DD VTL**］を選択します。
2. プールのリストを展開し、DD Cloud Tier にテープを移行するように構成されたプールを選択します。
3. ［Pool］パネルで［**Tape**］タブをクリックします。
4. クラウド ユニットに配置されている 1 つまたは複数のテープを選択します。
5. ［**Recall Cloud Tapes**］をクリックして DD Cloud Tier からテープをリコールします。

結果

スケジュール設定された次回データ移行の後で、テープがクラウド ユニットからヴォールトにリコールされます。テープは、ヴォールトからライブラリに返却できます。

CLI 相当機能

手順

1. データを復元するために必要なボリュームを識別します。
2. ヴォールトからテープ ボリュームをリコールします。

   次のコマンドを実行します。
   ```
   vtl tape recall start barcode T00001L3 count 1 pool cloud-vtl-pool
   ```
3. リコール操作の開始を確認します。

   次のコマンドを実行します。
   ```
   data-movement status
   ```
4. リコール操作が正常に完了したことを確認します。

   次のコマンドを実行します。
   ```
   vtl tape show all barcode T00001L3
   ```

```
Processing tapes....
Barcode    Pool             Location           State    Size           Used (%)
Comp   Modification Time
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
T00001L3   cloud-vtl-pool   cloud-vtl slot 1   RW      5 GiB   5.0 GiB (99.07%)
239x   2017/05/05 10:41:41
--------   --------------   ----------------   -----   -----   ----------------
----   -------------------
(S) Tape selected for migration to cloud. Selected tapes will move to cloud on the next
data-movement run.
(R) Recall operation is in progress for the tape.

VTL Tape Summary
----------------
Total number of tapes:     1
Total pools:               1
Total size of tapes:       5 GiB
Total space used by tapes: 5.0 GiB
Average Compression:       239.1x
```

5. ファイルのロケーションを検証します。

   次のコマンドを実行します。
   ```
   filesys report generate file-location path /data/col1/cloud-vtl-pool
   ```

```
filesys report generate file-location path /data/col1/cloud-vtl-pool
-------------------------------      --------------------------
File Name                            Location(Unit Name)
```

```
--------------------------------      ---------------------------
/data/col1/cloud-vtl-pool/.vtl_pool     Active
/data/col1/cloud-vtl-pool/.vtc/T00001L3 Active
----------------------------------------------------------------
```

6. DD VTL にリコールされたテープをインポートします。

   次のコマンドを実行します。
   `vtl import cloud-vtl barcode T00001L3 count 1 pool cloud-vtl-pool element slot`

```
imported 1 tape(s)...sysadmin@ddbeta70# vtl tape show cloud-vtlProcessing tapes.....
```

7. バックアップ アプリケーション インベントリのボリュームを確認します。
8. バックアップ アプリケーションを使用してデータを復元します。
9. 復元が完了した後で、バックアップ アプリケーション インベントリのテープ ボリュームを確認します。
10. テープ ボリュームを Data Domain VTL から Data Domain Vault へエクスポートします。
11. クラウド ユニットへテープを戻します。

アクセス グループの扱い

[アクセス グループ] は、イニシエーター WWPN（World Wide Name ポート名）またはエイリアス、およびアクセスを許可されるドライブとチェンジャーのコレクションを保持します。[TapeServer] という名前の DD VTL デフォルト グループを使用して、NDMP（ネットワーク データ管理プロトコル）ベース バックアップ アプリケーションに対応するデバイスを追加できます。

アクセス グループ構成によって、イニシエーター（通常、バックアップ アプリケーション）は、同じアクセス グループに含まれているデバイスに対してデータの読み取り/書き込みを実行できます。

アクセス グループによって、クライアントはシステム上の選択された LUN（メディア チェンジャーまたは仮想テープ ドライブ）に対してのみアクセスできます。アクセス グループのクライアント セットアップは、そのアクセス グループ内のデバイスに対してのみアクセスできます。

アクティブなバックアップまたはリストア ジョブの実行中に DD システムでアクセス グループを変更しないでください。変更すると、アクティブなジョブが失敗する場合があります。アクティブなジョブの実行中に行った変更の影響は、バックアップ ソフトウェアやホスト構成の組み合わせによって異なります。

[**Access Groups**] > [**Groups**] を選択すると、すべてのアクセス グループについて次の情報が表示されます。

表 162 アクセス グループの情報

項目	説明
グループ名	グループの名前。
Initiators	グループ内のイニシエーターの数。
デバイス	グループ内のデバイスの数。

[**View All Access Groups**] を選択する場合、[Fibre Channel] ビューに移動します。

[More Tasks] メニューから、グループを作成または削除できます。

アクセス グループの作成

アクセス グループは、デバイスとイニシエーター間のアクセスを管理します。NDMP を使用しない場合は、デフォルトの TapeServer アクセス グループを使用しないでください。

手順

1. ［**Access Groups**］ > ［**Groups**］を選択します。
2. ［**More Tasks**］ > ［**Group**］ > ［**Create**］を選択します。
3. ［Create Access Group］ダイアログで、名前（1～128 文字）を入力して［**Next**］を選択します。
4. デバイスを追加して、［**Next**］を選択します。
5. サマリーをレビューして、必要に応じて［**Finish**］または［**Back**］を選択します。

   ［**CLI** 相当］

   ```
   # vtl group create My_Group
   ```

アクセス グループ デバイスの追加

アクセス グループ構成によって、イニシエーター（通常、バックアップ アプリケーション）は、同じアクセス グループに含まれているデバイスに対してデータの読み取り/書き込みを実行できます。

手順

1. ［**Access Groups**］ > ［**Groups**］を選択します。特定のグループを選択することもできます。
2. ［**More Tasks**］ > ［**Group**］ > ［**Create**］または［**Group**］ > ［**Configure**］を選択します。
3. ［Create or Modify Access Group］ダイアログに、任意で［**Group Name**］を入力するか、変更します （このフィールドは入力必須です）。
4. イニシエーターをアクセス グループに構成するには、イニシエーターの隣にあるボックスをチェックします。後でグループにイニシエーターを追加できます。
5. ［**Next**］を選択します。
6. ［Devices］表示で、［Add］（［**+**］）を選択して［Modify Devices］ダイアログを表示します。
   a. 正しいライブラリが［Library Name］ドロップダウン リストで選択されていることを確認するか、その他のライブラリを選択します。
   b. ［Device］領域では、グループに含めるデバイス（チェンジャーとドライブ）のチェックボックスを選択します。
   c. オプションで、［LUN Start Address］テキスト ボックスの開始 LUN を指定します。

      これは、DD システムがイニシエーターに返す LUN です。各デバイスは、ライブラリとデバイス名で一意に識別されます。（たとえば、Library 1 にドライブ 1、Library 2 にもドライブ 1 を設定できます）。そのため、LUN はライブラリとデバイス名で識別されるデバイスに関連づけられます。

      FC HBA/SLIC 上の接続された FC ポート経由で LUN を提示する場合、ポートは「primary」、「secondary」、「none」として指定できます。一連の LUN に対するプライマリ ポートは、ファブリックにそれらの LUN を現在アドバタイズしているポートです。セカンダリ ポートは、プライマリ パスの障害発生時に一連の LUN をブロードキャストするポートです（手動の操作が必要です）。なしの設定は、選択した LUN をアドバタイズしたくない場合に使用されます。LUN の存在は、当該の SAN トポロジーによって変わります。

      アクセス グループのイニシエーターは、グループに追加される LUN デバイスとやり取りします。

      アクセス グループの作成時に許容される最大 LUN は 16383 です。

LUN は、グループごとに 1 回のみ使用できます。同じ LUN を複数のグループに使用することができます。

一部のイニシエータ（クライアント）には、ターゲット LUN ナンバリングについての特定のルールがあります。たとえば、LUN 0 または連続 LUN が必要です。そのルールに従わなかった場合、イニシエータは DD VTL ターゲット ポートに割り当てられている LUN の一部またはすべてにアクセスできなくなる可能性があります。

特別ルールに関するイニシエータのドキュメントをチェックし、必要に応じて、DD VTL ターゲット ポート上のデバイス LUN を変更してルールに従います。たとえば、イニシエータが LUN 0 を DD VTL ターゲット ポートに割り当てることを要件としている場合、ポートに割り当てられたデバイスの LUN をチェックし、LUN 0 にデバイスが割り当てられていない場合、LUN 0 に割り当てられるようにデバイスの LUN を変更します。

d. ［Primary and Secondary Endpoints］領域で、選択されたデバイスが認識されるポートを決定するオプションを選択します。次の条件が、指定されたポートに適用されます。

- all：チェックされたデバイスは、すべてのポートから認識されます。
- none：チェックされたデバイスは、どのポートからも認識されません。
- select：チェックされたデバイスは、選択されたポートから認識されます。適切なポートのチェックボックスを選択します
  プライマリ ポートのみ選択された場合、チェックされたデバイスはプライマリ ポートからのみ認識されます。

  セカンダリ ポートのみ選択された場合、チェックされたデバイスはセカンダリ ポートからのみ認識されます。プライマリ ポートが使用不可能になった場合、セカンダリ ポートを使用できます。

セカンダリ ポートへのスイッチオーバーは自動操作ではありません。プライマリ ポートが使用不可能になった場合、DD VTL デバイスをセカンダリ ポートに手動で切り替える必要があります。

ポート リストは、物理ポート番号のリストです。ポート番号は PCI スロットを示し、文字は PCI カード上のポートを示します。たとえば、1a、1b、2a、2b のようになります。

ドライブは、構成したすべてのポート上の同じ LUN で表示されます。

e. ［**OK**］を選択します。

新しいグループがリストされている［Devices］ダイアログ ボックスに戻ります。デバイスを追加するには、次の 5 つのサブステップを繰り返します。

7. ［**Next**］を選択します。
8. 「Completed」ステータス メッセージが表示されたら、［**Close**］を選択します。

［**CLI** 相当］

```
# vtl group add VTL_Group vtl NewVTL changer lun 0 primary-port all secondary-port all#
vtl group add VTL_Group vtl NewVTL drive 1 lun 1 primary-port all secondary-port all#
vtl group add SetUp_Test vtl SetUp_Test drive 3 lun 3 primary-port endpoint-fc-0
secondary-port endpoint-fc-1

# vtl group show Setup_Test
Group: SetUp_Test

Initiators:
Initiator Alias   Initiator WWPN
---------------   ----------------------
tsm6_p23          21:00:00:24:ff:31:ce:f8
```

```
---------------   ------------------------

Devices:
Device Name          LUN   Primary Ports   Secondary Ports    In-use Ports
------------------   ---   -------------   ---------------   -------------
SetUp_Test changer     0             all               all             all
SetUp_Test drive 1     1             all               all             all
SetUp_Test drive 2     2              5a                5b              5a
SetUp_Test drive 3     3   endpoint-fc-0     endpoint-fc-1   endpoint-fc-0
------------------   ---   -------------   ---------------   -------------
```

アクセス グループ デバイスの変更または削除

アクセス グループのデバイスを変更または削除する必要がある場合があります。

手順

1. ［**Protocols**］ > ［**VTL**］ > ［**Access Groups**］ > ［**Groups**］> group を選択します。
2. ［**More Tasks**］ > ［**Group**］ > ［**Configure**］を選択します。
3. ［Modify Access Group］ダイアログで、［**Group Name**］を入力するか変更します。（このフィールドは入力必須です）。
4. イニシエーターをアクセス グループに構成するには、イニシエーターの隣にあるボックスをチェックします。後でグループにイニシエーターを追加できます。
5. ［**Next**］を選択します。
6. デバイスを選択し、編集（鉛筆）アイコンを選択して、［Modify Devices］ダイアログを表示します。その後、ステップ **a**～**e** を行います。ただデバイスを削除したいだけの場合、削除（X）アイコンを選択し、ステップ **e** にスキップします。

   a. 正しいライブラリが［Library］ドロップダウン リストで選択されていることを確認するか、その他のライブラリを選択します。

   b. ［Devices to Modify］領域では、変更するデバイス（Changer とドライブ）のチェックボックスを選択します。

   c. オプションで、［LUN Start Address］ボックスの開始 LUN（論理ユニット番号）を変更します。

      これは、DD システムがイニシエーターに返す LUN です。各デバイスは、ライブラリとデバイス名で一意に識別されます。（たとえば、Library 1 にドライブ 1、Library 2 にもドライブ 1 を設定できます）。そのため、LUN はライブラリとデバイス名で識別されるデバイスに関連づけられます。

      アクセス グループのイニシエーターは、グループに追加される LUN デバイスとやり取りします。

      アクセス グループの作成時に許容される最大 LUN は 16383 です。

      LUN は、グループごとに 1 回のみ使用できます。同じ LUN を複数のグループに使用することができます。

      一部のイニシエータ（クライアント）には、ターゲット LUN ナンバリングについての特定のルールがあります。たとえば、LUN 0 または連続 LUN が必要です。そのルールに従わなかった場合、イニシエータは DD VTL ターゲット ポートに割り当てられている LUN の一部またはすべてにアクセスできなくなる可能性があります。

      特別ルールに関するイニシエータのドキュメントをチェックし、必要に応じて、DD VTL ターゲット ポート上のデバイス LUN を変更してルールに従います。たとえば、イニシエータが LUN 0 を DD VTL ターゲット ポートに割り当てることを要件としている場合、ポートに割

り当てられたデバイスの LUN をチェックし、LUN 0 にデバイスが割り当てられていない場合、LUN 0 に割り当てられるようにデバイスの LUN を変更します。

d. ［Primary and Secondary Ports］ 領域で、選択されたデバイスが認識されるポートを決定するオプションを変更します。次の条件が、指定されたポートに適用されます。

- all：チェックされたデバイスは、すべてのポートから認識されます。
- none：チェックされたデバイスは、どのポートからも認識されません。
- select：チェックされたデバイスは、選択されたポートから認識されます。デバイスが認識されるポートのチェックボックスを選択します。
  プライマリ ポートのみ選択された場合、チェックされたデバイスはプライマリ ポートからのみ認識されます。

  セカンダリ ポートのみ選択された場合、チェックされたデバイスはセカンダリ ポートからのみ認識されます。プライマリ ポートが使用不可能になった場合、セカンダリ ポートを使用できます。

セカンダリ ポートへのスイッチオーバーは自動操作ではありません。プライマリ ポートが使用不可能になった場合、DD VTL デバイスをセカンダリ ポートに手動で切り替える必要があります。

ポート リストは、物理ポート番号のリストです。ポート番号は PCI スロットを示し、文字は PCI カード上のポートを示します。たとえば、1a、1b、2a、2b のようになります。

ドライブは、構成したすべてのポート上の同じ LUN で表示されます。

e. ［**OK**］ を選択します。

アクセス グループの削除

アクセス グループを削除する前に、すべてのイニシエーターと LUN を削除する必要があります。

手順

1. イニシエーターと LUN をすべてグループから削除します。
2. ［**Access Groups**］ > ［**Groups**］ を選択します。
3. ［**More Tasks**］ > ［**Group**］ > ［**Delete**］ を選択します。
4. ［Delete Group］ ダイアログで、削除するグループのチェックボックスを選択し、［**Next**］ を選択します。
5. グループ確認ダイアログで、削除を確認し、［**Submit**］ を選択します。
6. ［Delete Groups Status］ に `Completed` と表示されたら、［**Close**］ を選択します。

［**CLI** 相当］

```
# scsitarget group destroy My_Group
```

選択されたアクセス グループの扱い

［**Access Groups**］ > ［**Groups**］ >group を選択すると、選択されたアクセス グループについて次の情報が表示されます。

表 163 ［LUNs］タブ

項目	説明
LUN	デバイス アドレス：最大数は 16,383 です。LUN は 1 つのグループ内で 1 回しか使用できませんが、他のグループで再度使用できます。グループに追加された DD VTL デバイスは、連続した LUN を使用する必要があります。
ライブラリ	この LUN に関連づけられているライブラリの名前。
Device	チェンジャーとドライブ。
In-Use Endpoints	現在使用中のエンドポイントのセット（プライマリまたはセカンダリ）。
Primary Endpoints	バックアップ アプリケーションが使用する初期（またはデフォルト）エンドポイント。このエンドポイントでの障害発生時に、使用可能であれば、セカンダリ エンドポイントが使用できます。
Secondary Endpoints	プライマリ エンドポイントで障害が発生した場合に使用するフェイルオーバー エンドポイントのセット。

表 164 ［Initiators］タブ

項目	説明
Name	イニシエーターの名前（イニシエーターに割り当てられた WWPN またはエイリアス）。
WWPN	ファイバー チャネル ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。

［More Tasks］メニューから、選択したグループで、そのグループを構成するか、使用中のエンドポイントを設定できます。

デバイスのエンドポイントの選択

エンドポイントはデバイスをイニシエーターに接続するため、デバイスを接続する前にこのプロセスを使用してエンドポイントをセットアップします。

手順

1. ［**Access Groups**］ > ［**Groups**］> group を選択します。
2. ［**More Tasks**］ > ［**Endpoints**］ > ［**Set In-Use**］を選択します。
3. ［Set in-Use Endpoints］ダイアログで、特定のデバイスのみを選択するか、［**Devices**］を選択してリスト内のすべてのデバイスを選択します。
4. エンドポイントがプライマリかセカンダリかを示します。
5. ［**OK**］を選択します。

NDMP デバイス TapeServer グループの構成

DD VTL TapeServer グループには、NDMP（ネットワーク データ管理プロトコル）ベースのバックアップ アプリケーションとやり取りし、FC（ファイバー チャネル）ではなく IP（インターネット プロトコル）を通して管理情報とデータ ストリームを送信するテープ ドライブがあります。NDMP TapeServer で

使用されるデバイスは、DD VTL グループの TapeServer に存在する必要があり、NDMP TapeServer［にのみ］使用できます。

手順

1. テープ ドライブを新しいまたは既存のライブラリ（この例では、「dd990-16」という名前のもの）に追加します。
2. ライブラリ用のスロットと CAP を作成します。
3. ライブラリ（この例では、「dd990-16」）内の作成されたデバイスを、TapeServer アクセス グループに追加します。
4. 次のコマンド ラインに入力して、NDMP デーモンを有効化します。

```
# ndmpd enable
Starting NDMP daemon, please wait.............
NDMP daemon is enabled.
```

5. NDMP デーモンが TapeServer グループのデバイスを認識していることを確認します。

```
ndmpd show devicenames
NDMP Device          Virtual Name       Vendor   Product       Serial Number
-----------------    ----------------   ------   -----------   -------------
/dev/dd_ch_c0t0l0    dd990-16 changer   STK      L180          6290820000
/dev/dd_st_c0t1l0    dd990-16 drive 1   IBM      ULTRIUM-TD3   6290820001
/dev/dd_st_c0t2l0    dd990-16 drive 2   IBM      ULTRIUM-TD3   6290820002
/dev/dd_st_c0t3l0    dd990-16 drive 3   IBM      ULTRIUM-TD3   6290820003
/dev/dd_st_c0t4l0    dd990-16 drive 4   IBM      ULTRIUM-TD3   6290820004
-----------------    ----------------   ------   -----------   -------------
```

6. 次のコマンドを使用して、NDMP ユーザー（この例では ndmp）を追加します。

```
# ndmpd user add ndmp
Enter password:
Verify password:
```

7. ユーザー ndmp が正しく追加されていることを確認します。

```
# ndmpd user show
ndmp
```

8. NDMP 構成を表示します。

```
# ndmpd option show all
Name              Value
--------------    --------
authentication    text
debug             disabled
port              10000
preferred-ip
--------------    --------
```

9. セキュリティを強化するため、デフォルト ユーザー パスワード認証で MD5 暗号化を使用するように変更し、その変更を確認します（テキストから md5 に認証値が変更されていることを確認します）。

```
# ndmpd option set authentication md5# ndmpd option show all
Name              Value
--------------    --------
authentication    md5
debug             disabled
port              10000
preferred-ip
--------------    --------
```

結果

NDMP が構成され、TapeServer アクセス グループにはデバイス構成が表示されます。完全なコマンド セットとオプションについては、「Data Domain オペレーティング システム コマンド リファレンス ガイド」の ndmpd の章を参照してください。

リソースの処理

［**Resources**］ResourcesResourcesInitiators を選択すると、イニシエーターとエンドポイントに関する情報が表示されます。［イニシエーター］は、FC（ファイバー チャネル）プロトコルを使用してデータの読み取りと書き込みを行うシステムに接続するバックアップ クライアントです。特定のイニシエータでは、FC 経由の DD Boost または DD VTL のいずれかをサポートできますが、両方はサポートできません。［エンドポイント］は、DD システム上の論理ターゲットで、イニシエーターの接続先です。

表 165 ［Initiators］タブ

項目	説明
名前	イニシエーターの名前（イニシエーターに割り当てられた WWPN またはエイリアス）。
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
Online Endpoints	イニシエーターがポートを認識するグループの名前。イニシエーターが使用できない場合、`None` または `Offline` が表示されます。

表 166 ［Endpoints］タブ

項目	説明
名前	エンドポイントの特定の名前。
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
システム アドレス	エンドポイントのシステム アドレス。
Enabled	HBA（ホスト バス アダプタ）ポートの動作状態。`Yes`（有効）または `No`（無効）。
Status	DD VTL リンク ステータス。`Online`（トラフィック処理可能）または `Offline`。

Configure Resources

［**Configure Resources**］を選択すると、［Fibre Channel］領域に移動して、エンドポイントとイニシエーターを構成できます。

イニシエーターの扱い

［**Resources**］ > ［**Resources**］ > ［**Initiators**］を選択すると、イニシエーターに関する情報が表示されます。［イニシエーター］は、DD システムがインターフェイス接続するクライアント システム FC HBA（ファイバー チャネル ホスト バス アダプタ）WWPN（World Wide Name ポート名）です。便宜上、［イニシエーター名］はクライアントの WWPN のエイリアスとします。

クライアントがイニシエーターとしてマッピングされている（ただし、アクセス グループにはまだ追加されていない）場合、クライアントは DD システム上のデータにアクセスできません。

イニシエーターまたはクライアントのアクセス グループを追加すると、クライアントはそのアクセス グループのデバイスにのみアクセスできます。クライアントには、複数のデバイスのアクセス グループのみ設定できます。

アクセス グループには複数のイニシエーターを含めることができますが、1 つのイニシエーターは 1 つのアクセス グループにのみ存在できます。

注

1 つの DD システムに対して最大 1024 のイニシエーターを構成できます。

表 167 イニシエーター情報

項目	説明
名前	イニシエーターの名前。
Group	イニシエーターに関連づけられたグループ。
Online Endpoints	イニシエーターが認識しているエンドポイント。イニシエーターが使用できない場合、`none` または `offline` が表示されます。
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
Vendor Name	イニシエーターのベンダー名。

［**Configure Initiators**］を選択すると、［Fibre Channel］領域に移動して、エンドポイントとイニシエーターを構成できます。

CLI 相当

```
# vtl initiator show
Initiator  Group      Status  WWNN                    WWPN                    Port
---------  ---------  ------  ----------------------  ----------------------  ----
tsm6_p1    tsm3500_a  Online  20:00:00:24:ff:31:ce:f8  21:00:00:24:ff:31:ce:f8 10b
---------  ---------  ------  ----------------------  ----------------------  ----

Initiator  Symbolic Port Name                          Address Method
---------  ------------------------------------------  --------------
tsm6_p1    QLE2562 FW:v5.06.03 DVR:v8.03.07.15.05.09-k  auto
---------  ------------------------------------------  --------------
```

エンドポイントの扱い

［**Resources** ］ > ［**Resources**］ > ［**Endpoints**］を選択すると、エンドポイントのハードウェアと接続に関する情報が表示されます。

表 168 ［Hardware］タブ

項目	説明
システム アドレス	エンドポイントのシステム アドレス。
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
Enabled	HBA（ホスト バス アダプタ）ポートの動作状態。`Yes`（有効）または `No`（無効）。
NPIV	このエンドポイントの NPIV ステータス：［Enabled］または［Disabled］。
リンク ステータス	このエンドポイントのリンク ステータス：［Online］または［Offline］。
Operation Status	このエンドポイントの操作ステータス：［Normal］または［Marginal］。
# of Endpoints	このエンドポイントに関連するエンドポイントの数。

表 169 ［Endpoints］タブ

項目	説明
NAME	エンドポイントの特定の名前。
WWPN	FC（ファイバー チャネル）ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
システム アドレス	エンドポイントのシステム アドレス。
Enabled	HBA（ホスト バス アダプタ）ポートの動作状態。`Yes`（有効）または `No`（無効）。
リンク ステータス	このエンドポイントのリンク ステータス：［Online］または［Offline］。

エンドポイントの構成

［**Configure Endpoints**］を選択すると、［Fibre Channel］領域に移動して、エンドポイントに関する前述の情報を変更できます。

CLI 相当

```
# scsitarget endpoint show list
Endpoint       System Address  Transport     Enabled  Status
--------       --------------  ---------     -------  ------
endpoint-fc-0  5a              FibreChannel  Yes      Online
endpoint-fc-1  5b              FibreChannel  Yes      Online
```

選択されたエンドポイントの扱い

［**Resources** ］ > ［**Resources**］ > ［**Endpoints**］> endpoint を選択すると、エンドポイントのハードウェア、接続、統計に関する情報が表示されます。

表 170 ［Hardware］タブ

項目	説明
システム アドレス	エンドポイントのシステム アドレス。
WWPN	ファイバー チャネル ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
Enabled	HBA（ホスト バス アダプター）ポートの動作状態。Yes（有効）または No（無効）。
NPIV	このエンドポイントの NPIV ステータス：［Enabled］または［Disabled］。
LInk Status	このエンドポイントのリンク ステータス：［Online］または［Offline］。
Operation Status	このエンドポイントの操作ステータス：［Normal］または［Marginal］。
# of Endpoints	このエンドポイントに関連するエンドポイントの数。

表 171 ［Summary］タブ

項目	説明
Name	エンドポイントの特定の名前。
WWPN	ファイバー チャネル ポートの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide Name ポート名。
WWNN	FC ノードの 64 ビット識別子（60 ビット値の先頭に 4 ビットの［Network Address Authority］識別子を加えたもの）である一意の World Wide ノード名。
システム アドレス	エンドポイントのシステム アドレス。
Enabled	HBA（ホスト バス アダプター）ポートの動作状態。Yes（有効）または No（無効）。
LInk Status	このエンドポイントのリンク ステータス：［Online］または［Offline］。

表 172 ［Statistics］タブ

項目	説明
Endpoint	エンドポイントの特定の名前。
ライブラリ	エンドポイントを含むライブラリの名前。
Device	デバイスの数。
Ops/s	1 秒あたりのオペレーション数。
Read KiB/s	1 秒あたりの KiB 数単位の読み取り速度。
Write KiB/s	1 秒あたりの KiB 数単位の書き込み速度。

表 173 ［Detailed Statistics］タブ

項目	説明
Endpoint	エンドポイントの特定の名前。
# of Control Commands	制御コマンドの数。
# of Read Commands	読み取りコマンドの数。
# of Write Commands	書き込みコマンドの数。
In (MiB)	書き込まれた MiB 数（MB のバイナリ相当）。
Out (MiB)	読み取られた MiB 数。
# of Error Protocol	エラー プロトコルの数。
# of Link Fail	リンク障害の数。
# of Invalid Crc	無効な CRC（巡回冗長検査）の数。
# of Invalid TxWord	無効な tx（伝送）ワードの数。
# of Lip	LIP（loop initialization primitive）の数。
# of Loss Signal	失われた信号または接続の数。
# of Loss Sync	同期を失った信号または接続の数。

プールの扱い

［**Pools**］ > ［**Pools**］を選択すると、Default プールとその他の既存のプールの詳細情報が表示されます。［プール］は、ファイル システム上のディレクトリにマッピングされるテープのコレクションです。プールは、デスティネーションへのテープのレプリケーションに使用されます。ディレクトリ ベース プールを MTree ベース プールに変換することで、MTree の機能をより有効に活用できます。

プールについて、次の点に留意してください。

- プールのタイプは、MTree（推奨）または Directory（下位互換性あり）です。
- 個別のテープの配置場所を問わず、プールはレプリケーションできます。テープはヴォールトまたはライブラリ（スロット、キャップ、またはドライブ）内に置けます。
- あるプールから他のプールにテープをコピーおよび移動できます。
- プールは、バックアップ ソフトウェアからはアクセスできません。

- プールをレプリケーションする際、レプリケーション デスティネーションに DD VTL 構成またはライセンスは必要ありません。
- 一意のバーコードでテープを作成する必要があります。重複バーコードによって、バックアップ アプリケーションで予測不能の動作が発生し、ユーザーが混乱する可能性があります。
- DD システム上の異なる 2 つのプール内にある 2 つのテープの名前が同一の場合、どちらのテープも他方のテープのプールに移動できません。同様に、レプリケーション デスティネーションに送信されるプールの名前は、そのデスティネーション上でに一意である必要があります。

表 174 ［Pools］タブ

項目	説明
NAME	プールの名前。
Type	Directory プールと MTree プールのどちらか。
Status	プールのステータス。
Tape Count	プール内のテープ数。
Size	そのプール内のテープの構成された合計データ容量（GiB（ギビバイト、GB-ギガバイトの 2 進数相当））。
Physical Used	そのプール内の仮想テープ上で使用されている領域の量。
Compression	そのプール内のテープで実現された圧縮の平均量。
Cloud Unit	DD VTL プールがデータを移行するクラウド ユニットの名前。
Cloud Data Movement Policy	DD VTL データの DD Cloud Tier ストレージへの移行を制御するデータ移動ポリシー。

表 175 ［Replication］タブ

項目	説明
NAME	プールの名前。
Configured	そのプールにレプリケーションが構成されているかどうか。yes または no。
Remote Source	プールが他の DD システムからレプリケーションされている場合のみエントリーが含まれています。
Remote Destination	プールが他の DD システムにレプリケーションされている場合のみエントリーが含まれています。

［More Tasks］メニューから、プールの作成、削除、検索が行えます。

プールの作成

5.2 以前の DD OS システムとのレプリケーションなど、セットアップに必要な場合は、下位互換性のあるプールを作成できます。

手順

1. ［**Pools**］ > ［**Pools**］を選択します。
2. ［**More Tasks**］ > ［**Pool**］ > ［**Create**］を選択します。
3. ［Create Pool］ダイアログで、新しい Pool Name を入力します。次の点に留意してください。

- 「all」、「vault」、「summary」は使用できません。
- プール名の先頭または末尾にスペースまたはピリオドは使用できません。
- プール名では大文字と小文字が区別されます。

4. 以前のバージョンの DD System Manager と下位互換性があるディレクトリ プールを作成する場合は、「Create a directory backwards compatibility mode pool」オプションを選択します。ただし、MTree プールを使用することの利点は、次の操作ができるようになることである点に留意してください。
   - 個別のスナップショットを作成し、スナップショットをスケジュールする。
   - 保存ロックを適用する。
   - 個別の保存ポリシーを設定する。
   - 圧縮情報を取得する。
   - Retention Tier へのデータ移行ポリシーを取得する。
   - ハード制限とソフト制限を設定して、ストレージ領域使用ポリシー（クォータ サポート）を確立します。
5. ［**OK**］を選択して、［Create Pool Status］ダイアログを表示します。
6. ［Create Pool Status］ダイアログに `Completed` と表示されたら、［**Close**］を選択します。そのプールが［Pools］サブツリーに追加され、それに仮想テープを追加できるようになります。

［**CLI** 相当機能］

```
# vtl pool add VTL_Pool
A VTL pool named VTL_Pool is added.
```

プールの削除

プールを削除するには、それに含まれるテープをすべて削除する必要があります。プールに対してレプリケーションが構成されている場合、そのレプリケーション ペアも削除する必要があります。プールを削除すると、MTree が名称変更され、次のクリーニング プロセスで削除されます。

手順

1. ［**Pools**］ > ［**Pools**］ > ［**pool**］を選択します。
2. ［**More Tasks**］ > ［**Pool**］ > ［**Delete**］を選択します。
3. ［Delete Pools］ダイアログで、削除する項目のチェックボックスを選択します。
   - 各プールの名前、または
   - ［**Pool Names**］（すべてのプールを削除する場合）。
4. 確認ダイアログで［**Submit**］を選択します。
5. ［Delete Pool Status］ダイアログに `Completed` と表示されたら、［**Close**］を選択します。

   プールが、［Pools］サブツリーから削除されます。

選択されたプールの扱い

［**Virtual Tape Libraries**］ > ［**VTL Service**］ > ［**Vault**］ > pool と［**Pools**］ > ［**Pools**］ > pool の両方に、選択されたプールの詳細が表示されます。プール「Default」は常に存在しています。

［Pool］タブ

表 176 サマリー

項目	説明
Convert to MTree Pool	Directory プールを MTree プールに変換するには、このボタンを選択します。
タイプ	Directory プールと MTree プールのどちらか。
Tape Count	プール内のテープ数。
容量	そのプール内のテープの構成された合計データ容量（GiB（ギビバイト、GB-ギガバイトの 2 進数相当））。
Logical Used	そのプール内の仮想テープ上で使用されている領域の量。
Compression	そのプール内のテープで実現された圧縮の平均量。

表 177 ［Pool］タブ：Cloud Data Movement - Protection Distribution

項目	説明
Pool type (%)	VTL プールとクラウド（該当する場合）およびデータの現在の割合（括弧内）。
NAME	ローカル VTL プールまたはクラウド プロバイダの名前。
Logical Used	そのプール内の仮想テープ上で使用されている領域の量。
Tape Count	プール内のテープ数。

表 178 ［Pool］タブ：Cloud Data Movement - Cloud Data Movement Policy

項目	説明
Policy	テープの経過日数、または手動選択。
Older Than	経過時間ベースのデータ移動ポリシーの経過時間閾値。
Cloud Unit	デスティネーションのクラウド ユニット。

［Tape］タブ

表 179 テープ制御

項目	説明
［**Create**］	新しいテープの作成。
［**Delete**］	選択したテープの削除。

表 179 テープ制御 （続き）

項目	説明
［**Copy**］	テープのコピーを作成。
［**Move between Pool**］	選択したテープを別のプールに移動。
［**Select for Cloud Move**］[a]	DD Cloud Tier への移行対象として選択したテープをスケジュール設定。
［**Unselect from Cloud Move**］[a]	DD Cloud Tier への移行スケジュールから選択したテープを削除。
［**Recall Cloud Tapes**］	選択したテープを DD Cloud Tier からリコール。
［**Move to Cloud Now**］	スケジュール設定された次回の移行を待つことなく、選択したテープを DD Cloud Tier に移行。

a. このオプションは、データ移動ポリシーが手動選択用に構成されている場合にのみ使用できます。

表 180 テープ情報

項目	説明
バーコード	テープ バーコード。
Size	テープの最大サイズ。
Physical Used	テープによって使用されている物理ストレージ容量。
Compression	テープ上の圧縮率。
Location	テープの場所。
変更時間	テープの最終更新時刻。
Recall Time	テープの最終リコール時刻。

［Replication］タブ

表 181 レプリケーション

項目	説明
NAME	プールの名前。
Configured	そのプールにレプリケーションが構成されているかどうか。yes または no。
Remote Source	プールが他の DD システムからレプリケーションされている場合のみエントリーが含まれています。
Remote Destination	プールが他の DD システムにレプリケーションされている場合のみエントリーが含まれています。

右上の［**Replication Detail**］ボタンを選択して、選択されたプールの［Replication information］パネルに直接移動することもできます。

［Virtual Tape Libraries］または［Pools］領域いずれかの［More Tasks］メニューから、プール内のテープを作成、削除、移動、コピー、検索できます。

［Pools］領域の［More Tasks］メニューからは、プールを名前変更または削除できます。

ディレクトリ プールの MTree プールへの変換

MTree プールには、ディレクトリ プールに勝る利点が多数あります。詳細については、［Creating pools］セクションを参照してください。

手順

1. 次の前提条件が満たされていることを確認します。
   - テープの数と両側のデータが変化しないようにするため、ソースおよびデスティネーション プールを同期する必要があります。
   - ディレクトリ プールは、レプリケーションのソースまたはデスティネーションではない。
   - ファイル システムがいっぱいではない必要。
   - ファイル システムは、許可された MTree の最大数（100）に達していない。
   - 同じ名前の MTree が存在しない。
   - ディレクトリ プールが複数のシステムでレプリケーションされている場合、それらのレプリケーション中のシステムは管理システムに認識される必要があります。
   - ディレクトリ プールが古い DD OS にレプリケートされている場合（DD OS 5.5 から DD OS 5.4 など）、それは変換できません。次に回避策を説明します。
     - 第 2 DD システムにディレクトリ プールをレプリケーションします。
     - 第 2 DD システムから第 3 DD システムにディレクトリ プールをレプリケーションします。
     - 管理 DD システムの Data Domain ネットワークから第 2 および第 3 DD システムを削除します。
     - DD OS 5.5 を実行するシステムの［Pools］サブメニューで、［**Pools**］、ディレクトリ プールを選択します。［Pools］タブで、［**Convert to MTree Pool**］を選択します。
2. 変更したいディレクトリ プールがハイライトされている場合、［**Convert to MTree Pool**］を選択します。
3. ［Convert to MTree Pool］ダイアログで［**OK**］を選択します。
4. 変換は次のようにレプリケーションに影響する点に留意してください。
   - DD VTL は、変換中、レプリケーションされているシステムでは一時的に無効化されます。
   - 新しいレプリケーションが初期化および同期されるまでデータを保存するため、デスティネーション データがデスティネーション システム上の新しいプールにコピーされます。その後、この一時的にコピーされたプールを安全に削除できます。そのプールは、［**CONVERTED-**］［pool］という名前になっており、［pool］（長いプール名の場合は先頭 18 文字）はアップグレードされたプールの名前です。[これは、DD OS 5.4.1.0 以降にのみ適用されます。]
   - ターゲット レプリケーション ディレクトリは、MTree 形式に変換されます。[これは、DD OS 5.2 以降にのみ適用されます。]
   - レプリケーション ペアは、プール変換を行う前に破棄され、エラーが発生しなかった場合、後で再確立されます。
   - DD Retention Lock は、MTree プール変換に含まれるシステムでは有効化できません。

プール間でのテープの移動

ヴォールト内に存在するテープは、レプリケーション アクティビティを格納するためにプール間で移動できます。たとえば、すべてのテープが［Default］プールで作成された場合にプールが必要ですが、テープのグループをレプリケーションするには、後で独立したグループが必要となります。名前が付けられたプールを作成し、テープのグループを新しいプールに再編成します。

注

ディレクトリ レプリケーション ソースであるテープ プールからはテープを移動できません。次に回避策を説明します。

- テープを新しいプールにコピーし、そのテープを古いプールから削除します。
- MTree プールを使用して、ディレクトリ レプリケーション ソースであるテープ プールからはテープを移動できます。

手順

1. ハイライト表示されているプールでは、［**More Tasks**］ > ［**Tapes**］ > ［**Move**］を選択します。

   プールから開始した場合、Tapes Panel でテープはプール間でしか移動できない点に留意してください。

2. ［Move Tapes］ダイアログで、移動するテープの検索情報を入力し、［**Search**］を選択します。

   表 182 ［Move Tapes］ダイアログ

フィールド	ユーザー入力
Location	場所は変更できません。
プール	テープが配置されているプールの名前を選択します。プールが作成されていない場合、デフォルトのプールを使用します。
バーコード	一意のバーコードを指定するか、デフォルト（*）のままにして、テープのグループをインポートします。バーコードには、ワイルドカード（?と*）を使用できます。?は任意の 1 文字、*は 0 文字以上に一致します。
Count	戻されるテープの最大数を入力します。このフィールドを空欄にすると、バーコードのデフォルト（*）が使用されます。
Tapes Per Page	ページあたりの最大表示テープ数を選択します。取り得る値は 15、30、45 です。
Items Selected	複数のページにまたがって選択されたテープの数を示します。各テープの選択に対して、自動的に更新されます。

3. 検索結果リストから、移動するテープを選択します。
4. ［Select Destination: Pool］リストから テープを移動するプールの場所を選択します。（名前が付けられた）［Pool］ビューから開始した場合のみ、このオプションを使用できます。
5. ［**Next**］を選択します。
6. ［Move Tapes］ビューから、サマリー情報とテープ リストを確認し、［**Submit**］を選択します。

7. ステータス ウィンドウで［**Close**］を選択します。

プール間でのテープのコピー

テープは、レプリケーション アクティビティを格納するためにプール間またはヴォールトからプール間でに移動できます。（名前が付けられた）［Pool］ビューから開始した場合のみ、このオプションを使用できます。

手順

1. ハイライト表示されているプールでは、［**More Tasks**］ > ［**Tapes**］ > ［**Copy**］を選択します。
2. ［Copy Tapes Between Pools］ダイアログで、コピーするテープのチェックボックスを選択するか、コピーするテープを検索する情報を入力して、［**Search**］を選択します。

表 183 ［Copy Tapes Between Pools］ダイアログ

フィールド	ユーザー入力
Location	テープを検出するため、ライブラリまたは［**Vault**］を選択します。テープは常にプール（［Pools］メニュー）に表示されますが、それらは技術的には、ライブラリまたはヴォールトに存在しますが、両方には存在することはなく、同時に 2 つのライブラリに存在することはありません。インポート/エクスポート オプションを使用して、ヴォールトとライブラリ間でテープを移動します。
プール	プール間でテープをコピーするには、テープが現在置かれているプールの名前を選択します。プールが作成されていない場合、［**Default**］プールを使用します。
バーコード	一意のバーコードを指定するか、デフォルト（*）のままにして、テープのグループをインポートします。バーコードには、ワイルドカード（?と*）を使用できます。?は任意の 1 文字、*は 0 文字以上に一致します。
Count	インポートするテープの最大数を入力します。このフィールドを空欄にすると、バーコードのデフォルト（*）が使用されます。
Tapes Per Page	ページあたりの最大表示テープ数を選択します。取り得る値は 15、30、45 です。
Items Selected	複数のページにまたがって選択されたテープの数を示します。各テープの選択に対して、自動的に更新されます。

3. 検索結果リストから、コピーするテープを選択します。
4. ［Select Destination: Pool］リストから テープがコピーされるプールを選択します。バーコードが一致するテープがすでにデスティネーション プールにある場合、エラーが表示され、コピーが中止されます。
5. ［**Next**］を選択します。
6. ［Copy Tapes Between Pools］ダイアログから、サマリー情報とテープ リストを確認し、［**Submit**］を選択します。
7. ［Copy Tapes Between Pools Status］ウィンドウで［**Close**］を選択します。

プールの名称変更

ライブラリにテープがない場合のみ、プールを名称変更できます。

手順

1. ［**Pools**］ > ［**Pools**］ > ［**pool**］を選択します。
2. ［**More Tasks**］ > ［**Pool**］ > ［**Rename**］を選択します。
3. ［Rename Pool］ダイアログで、新しい Pool Name を入力します。次の点に留意してください。
   - 「all」、「vault」、「summary」は使用できません。
   - プール名の先頭または末尾にスペースまたはピリオドは使用できません。
   - プール名では大文字と小文字が区別されます。
4. ［**OK**］を選択して、［Rename Pool status］ダイアログを表示します。
5. ［Rename Pool status］ダイアログに `Completed` と表示されたら、［**OK**］を選択します。

   ［Pools］と［Virtual Tape Libraries］両方の領域の［Pools］サブツリーで、プールの名前が変更されます。

第 16 章

DD Replicator

本章には、次のセクションが含まれます。

- DD Replicator の概要 420
- レプリケーション構成の前提条件 421
- レプリケーション バージョンの互換性 423
- レプリケーション タイプ 428
- DD Replicator と DD Encryption の使用 434
- レプリケーション トポロジー 435
- レプリケーションの管理 439
- レプリケーションのモニタリング 455
- レプリケーションと HA 456
- クォータのあるシステムからクォータのないシステムへのレプリケーション 457
- レプリケーション スケーリング コンテキスト 457
- ディレクトリから MTree へのレプリケーションの移行 458
- ディザスタリカバリ用コレクション レプリケーションおよび SMT の使用 462

DD Replicator の概要

DD Replicator（[Data Domain Replicator]）は、DR（ディザスタリカバリ）や複数サイトのバックアップとアーカイブの統合に使用できる、ポリシー ベースで自動化されたネットワーク効率に優れた暗号化レプリケーションを提供します。DD Replicator は、WAN（ワイド エリア ネットワーク）を通して圧縮および重複排除されたファイルのみを非同期的にレプリケーションします。

DD Replicator は、帯域幅要件を大幅に削減するため、［ローカル］と［サイト間］という 2 つのレベルの重複排除を実行します。ローカル重複排除によって、WAN 経由でレプリケーションされた一意のセグメントが決定されます。複数のサイトが同じデスティネーション システムにレプリケートする場合は、サイト間の重複排除により帯域幅の要件をさらに低減できます。サイト間の重複排除を使用すると、他のサイトによって、あるいはローカル バックアップまたはアーカイブの結果として以前に転送された冗長セグメントが再びレプリケートされることはありません。これにより、すべてのサイトでネットワーク効率が向上し、日常のネットワーク帯域幅の要件が最大 99%低減されるため、高速でコスト パフォーマンスに優れた信頼できるネットワーク ベースのレプリケーションが実現されます。

DD Replicator は、さまざまな災害復旧要件に対応するために、フルシステム ミラーリング、双方向、多対 1、1 対多、カスケードなど柔軟なレプリケーション トポロジーを提供します。さらに、DD システム上の全データをレプリケーションするか、データのサブセットをレプリケーションするかを選択できます。最高レベルのセキュリティを実現するために、DD Replicator では、DD システム間でレプリケーションされているデータを標準的な SSL（Secure Socket Layer）プロトコルを使用して暗号化できます。

DD Replicator では、パフォーマンスとサポート可能なファン イン比率を高めて大規模な企業環境をサポートできます。

DD Replicator の使用を開始する前に、次の一般的な要件を確認してください。

- DD Replicator はライセンス製品です。ライセンスを購入するには、Data Domain 担当営業にお問い合わせください。
- 通常、2 つのリリース（例、5.6 から 6.0）内のマシン間でのみレプリケートが可能です。ただし、これには例外（変則的なリリース番号など）が存在する可能性もあるため、［レプリケーション バージョンの互換性］セクションの表を確認するか、Data Domain 担当営業までお問い合わせください。
- 現在のバージョンの DD System Manager から DD Replicator を管理および監視できない場合は、「Data Domain オペレーティング システム コマンド リファレンス ガイド」で説明されている `replication` コマンドを使用します。

レプリケーション構成の前提条件

レプリケーションを構成する前に、次の前提条件を確認し、初回のデータ転送時間の短縮、データの上書き防止などに役立てます。

- ［**Contexts**］：次の表でレプリケーション ストリーム数を確認して、DD システムのコンテキストの最大数を決定します。

  表 184 新しい Data Domain システムに送信されるデータ ストリーム

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD140、DD160、DD610	4 GB または 6 GB / 0.5 GB	16	4	15	20	w<= 16 ; r<= 4 ReplSrc<=15; ReplDest<=20; ReplDest+w<=16; w+r+ReplSrc <=16;Total<=20
DD620、DD630、DD640	8 GB / 0.5 GB または 1 GB	20	16	20	20	w<=20; r<=16; ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; Total<=30
DD640、DD670	16 GB または 20 GB / 1 GB	90	30	60%	90	w<=90; r<=30; ReplSrc<=60; ReplDest<=90; ReplDest+w<=90; Total<=90
DD670、DD860	36 GB / 1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD860	72 GB[b]/1 GB	90	50	90	90	w<=90; r<=50; ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; Total<=90
DD890	96 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD990	128 または 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD2200	8 GB	20	16	16	20	w<=20; r<=16; ReplSrc<=16; ReplDest<=20; ReplDest+w<=20; Total<=20
DD2200	16 GB	60%	16	30	60%	w<=60; r<=16; ReplSrc<=30; ReplDest<=60; ReplDest+w<=60; Total<=60
DD2500	32 または 64 GB / 2 GB	180	50	90	180	w<=180; r<=50; ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; Total<=180
DD4200	128 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270

表 184 新しい Data Domain システムに送信されるデータ ストリーム （続き）

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD4500	192 GB[b]/4 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD7200	128 または 256 GB[b]/4 GB	540	150	270	540	w<=540; r<=150; ReplSrc<=270; ReplDest<=540; ReplDest +w<=540; Total<=540
DD9500	256 / 512 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD9800	256/768 GB	1885	300	540	1080	w<=1885; r<=300; ReplSrc<=540; ReplDest<=1080; ReplDest +w<=1080; Total<=1885
DD6300	48/96 GB	270	75	150	270	w<=270; r<=75; ReplSrc<=150; ReplDest<=270; ReplDest +w<=270; Total<=270
DD6800	192 GB	400	110	220	400	w<=400; r<=110; ReplSrc<=220; ReplDest<=400; ReplDest +w<=400; Total<=400
DD9300	192/384 GB	800	220	440	800	w<=800; r<=220; ReplSrc<=440; ReplDest<=800; ReplDest +w<=800; Total<=800
DD VE 8 TB	8 GB / 512 MB	20	16	20	20	w<= 20 ; r<= 16 ReplSrc<=20; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=20;Total<=20
DD VE 16 TB	16 GB / 512 MB または 24 GB / 1 GB	45	30	45	45	w<= 45 ; r<= 30 ReplSrc<=45; ReplDest<=45; ReplDest+w<=45; w+r+ReplSrc <=45;Total<=45
DD VE 32 TB	24 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 48 TB	36 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 64 TB	48 GB / 1 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD VE 96 TB	64 GB / 2 GB	180	50	90	180	w<= 180 ; r<= 50 ReplSrc<=90; ReplDest<=180; ReplDest +w<=180; w+r+ReplSrc <=180;Total<=180

表 184 新しい Data Domain システムに送信されるデータ ストリーム （続き）

Model	RAM/ NVRAM	Backup write streams	Backup read streams	Repl[a] source streams	Repl[a] dest streams	Mixed
DD3300 4 TB	12 GB（仮想メモリー） / 512 MB	20	16	30	20	w<= 20 ; r<= 16 ReplSrc<=30; ReplDest<=20; ReplDest+w<=20; w+r+ReplSrc <=30;Total<=30
DD3300 8 TB	32 GB（仮想メモリー） / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 16 TB	32 GB（仮想メモリー） / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=90
DD3300 32 TB	46 GB（仮想メモリー） / 1.536 GB	90	50	90	90	w<= 90 ; r<= 50 ReplSrc<=90; ReplDest<=90; ReplDest+w<=90; w+r+ReplSrc <=90;Total<=140

a. DirRepl, OptDup, MTreeRepl streams
b. Data Domain Extended Retention ソフトウェア オプションは、（最大）メモリが拡張されたデバイスでのみ使用可能です。

- ［**Compatibility**］: 異なるバージョンの DD OS を実行している DD システムを使用している場合は、次のセクションの「レプリケーション バージョンの互換性」を参照してください。
- ［**Initial Replication**］: ソースに大量のデータがある場合、初回のレプリケーション処理に何時間もかかることがあります。レーテンシーの低い高速リンクを使用して、両方の DD システムを同じ場所に配置することを検討してください。最初のレプリケーション後は、新規データのみ送信されるため、各システムをそれぞれの予定していた場所に移動することができます。
- ［**Bandwidth Delay Settings**］: ソースとデスティネーションの両方の帯域幅遅延設定は同じである必要があります。これらのチューニング制御により、TCP（伝送制御プロトコル）のバッファー サイズを制御することで、高レーテンシー リンクを介してレプリケーション パフォーマンスを改善できます。その後、ソース システムは確認を待ちながら十分なデータをデスティネーションに送信できるようになります。
- ［**Only One Context for Directories/Subdirectories**］: ディレクトリ（およびそのサブディレクトリ）は一度に 1 つのコンテキストにのみ存在できます。そのため、ソース ディレクトリ配下のサブディレクトリが、別のディレクトリ レプリケーション コンテキストで使用されていないことを確認してください。
- ［**Adequate Storage**］: 少なくとも、デスティネーションにはソースと［同じ量のスペース］が必要です。
- ［**Destination Empty for Directory Replication**］: ディレクトリ レプリケーションの場合、内容は上書きされるため、デスティネーション ディレクトリは空であるか、必要のない内容だけである必要があります。
- ［**Security**］: DD OS では、Ethernet 接続経由で安全なレプリケーションを構成するためにポート 3009 を開ける必要があります。

レプリケーション バージョンの互換性

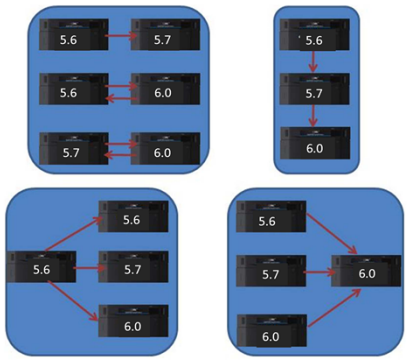
ソースとデスティネーションで異なるバージョンの DD OS を実行している DD システムを使用するには、後述の各表に記載されている単一ノード、DD Extended Retention、DD Retention Lock、

MTree、ディレクトリ、コレクション、デルタ（低帯域幅の最適化）、カスケード レプリケーションの互換性情報を参照してください。

一般なガイドラインは次のとおりです。

- DD Boost または OST の場合、サポートされている構成については「Data Domain Boost for Partner Integration 管理ガイド」の「Optimized Duplication Version Compatibility」または「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。
- 同一データのレプリケーションに、MTree およびディレクトリ レプリケーションを同時に使用することはできません。
- リカバリ手順は、すべてのサポートされているレプリケーション構成で有効です。
- ファイル移行は、コレクション レプリケーションがサポートされている場合は常にサポートされます。
- DD OS 5.2.x を実行しているソース DD システムと DD OS 5.4.x または DD OS 5.5.x を実行しているデスティネーション DD システム間の MTree レプリケーションは、ソース MTree 上で DD Retention Lock Governance が有効になっている場合はサポートされません。
- DD OS 6.0 を実行しているソース DD システムから旧バージョンの DD OS を実行しているターゲット DD システムへの MTree レプリケーションの場合、レプリケーション プロセスは、デスティネーション DD システム上の旧バージョンの DD OS に従って動作します。デスティネーション DD システムからリストア操作またはカスケード レプリケーションを実行すると、仮想合成は適用されません。
- カスケード構成の場合、ホップの最大数は 2、つまり、3 つの DD システムです。
  ディレクトリから MTree への移行では、2 つ前までのリリースとの下位互換性がサポートされます。ディレクトリから Mtree への移行の詳細については、ディレクトリから MTree へのレプリケーションの移行（458 ページ）を参照してください。
- 1 対多、多対 1、カスケード レプリケーションでは、後述の図に示されているように、最大 3 つの連続した DD OS リリース ファミリーがサポートされます。

図 17 有効なレプリケーション構成



各表の内容の説明

- 各 DD OS リリースには、そのファミリーのすべてのリリースが含まれます。たとえば、DD OS 5.7 には 5.7.1、5.7.x、6.0 などが含まれます。
- c = コレクション レプリケーション
- dir = ディレクトリ レプリケーショ
- m = MTree レプリケーション
- del = デルタ（低帯域幅最適化）レプリケーション

- dest = デスティネーション
- src = ソース
- NA = 該当せず

表 185 構成：シングル ノードからシングル ノード

src/dest	5.0（dest）	5.1（dest）	5.2（dest）	5.3（dest）	5.4（dest）	5.5（dest）	5.6（dest）	5.7（dest）	6.0（dest）	6.1（dest）	6.2（dest）
5.0（src）	c、dir、del	dir、del	dir、del	NA	NA	NA	NA	NA	NA	NA	NA
5.1（src）	dir、del	c、dir、del、m[a]	dir、del、m[a]	dir、del、m[a]	dir、del、m[a]	NA	NA	NA	NA	NA	NA
5.2（src）	dir、del	dir、del、m[a]	c、dir、del、m[b]	dir、del、m	dir、del、m	dir、del、m	NA	NA	NA	NA	NA
5.3（src）	NA	dir、del、m[a]	dir、del、m	c、dir、del、m	dir、del、m	dir、del、m	NA	NA	NA	NA	NA
5.4（src）	NA	dir、del、m[a]	dir、del、m	dir、del、m	c、dir、del、m	dir、del、m	dir、del、m	NA	NA	NA	NA
5.5（src）	NA	NA	dir、del、m	dir、del、m	dir、del、m	c、dir、del、m	dir、del、m	dir、del、m	NA	NA	NA
5.6（src）	NA	NA	NA	NA	dir、del、m	dir、del、m	c、dir、del、m	dir、del、m	dir、del、m	NA	NA
5.7（src）	NA	NA	NA	NA	NA	dir、del、m	dir、del、m	c、dir、del、m	dir、del、m	dir、del、m	NA
6.0（src）	NA	NA	NA	NA	NA	NA	dir、del、m	dir、del、m	c、dir、del、m	dir、del、m	dir、del、m
6.1（src）	NA	NA	NA	NA	NA	NA	NA	dir、del、m	dir、del、m	c、dir、del、m	dir、del、m
6.2（src）	NA	NA	NA	NA	NA	NA	NA	NA	dir、del、m	dir、del、m	c、dir、del、m

a. MTree レプリケーションは DD VTL には対応していません。
b. コレクション レプリケーションはコンプライアンス データにのみ対応しています。

表 186 構成: DD Extended Retention から DD Extended Retention

src/dest	5.0（dest）	5.1（dest）	5.2（dest）	5.3（dest）	5.4（dest）	5.5（dest）	5.6（dest）	5.7（dest）	6.0（dest）	6.1（dest）	6.2（dest）
5.0（src）	c	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.1(src)	NA	c	m[a]	m[b]	m[b]	NA	NA	NA	NA	NA	NA
5.2（src）	NA	m[a]	c、m[a]	m[a]	m[a]	m[a]	NA	NA	NA	NA	NA
5.3（src）	NA	m[c]	m[c]	c、m	m	m	NA	NA	NA		NA
5.4（src）	NA	m[c]	m[c]	m	c、m	m	m	NA	NA	NA	NA

表 186 構成: DD Extended Retention から DD Extended Retention （続き）

src/ dest	5.0 （dest）	5.1 （dest）	5.2 （dest）	5.3 （dest）	5.4 （dest）	5.5 （dest）	5.6 （dest）	5.7 （dest）	6.0 （dest）	6.1 （dest）	6.2 （dest）
5.5 （src）	NA	NA	m[c]	m	m	c、m	m	m	NA	NA	NA
5.6 （src）	NA	NA	NA	NA	m	m	c、m	m	m		NA
5.7 （src）	NA	NA	NA	NA	NA	m	m	c、m	m	m	NA
6.0 （src）	NA	NA	NA	NA	NA	NA	m	m	c、m	m	m
6.1（src）	NA	NA	NA	NA	NA	NA	NA	m	m	c、m	m
6.2 （src）	NA	NA	NA	NA	NA	NA	NA	NA	m	m	c、m

a. この構成では、ソースまたはデスティネーション上の MTree レプリケーションによるファイル移行はサポートされていません。
b. この構成では、ソース上の MTree レプリケーションによるファイル移行はサポートされていません。
c. この構成では、デスティネーション上の MTree レプリケーションによるファイル移行はサポートされていません。

表 187 構成：シングル ノードから DD Extended Retention

src/ dest	5.0（dest）	5.1（dest）	5.2（dest）	5.3（dest）	5.4（dest）	5.5（dest）	5.6（dest）	5.7（dest）	6.0（dest）	6.1（dest）	6.2（dest）
5.0（src）	dir	dir	NA	NA	NA	NA	NA	NA	NA	NA	NA
5.1(src)	dir	dir、m[a]	dir、m[a]	dir、m	dir、m	NA	NA	NA	NA	NA	NA
5.2（src）	dir	dir、m[a]	dir、m[a]	dir、m	dir、m	dir、m	NA	NA	NA	NA	NA
5.3（src）	NA	dir、m[a]	dir、m[a]	dir、m	dir、m	dir、m	NA	NA	NA	NA	NA
5.4（src）	NA	dir、m[a]	dir、m[a]	dir、m	dir、m	dir、m	dir、m	NA	NA	NA	NA
5.5（src）	NA	NA	dir、m[a]	dir、m	dir、m	dir、m	dir、m	dir、m	NA	NA	NA
5.6（src）	NA	NA	NA	NA	dir、m	dir、m	dir、m	dir、m	dir、m	NA	NA
5.7（src）	NA	NA	NA	NA	NA	dir、m	dir、m	dir、m	dir、m	dir、m	NA
6.0（src）	NA	NA	NA	NA	NA	NA	dir、m	dir、m	dir、m	dir、m	dir、m
6.1(src)	NA	NA	NA	NA	NA	NA	NA	dir、m	dir、m	dir、m	dir、m
6.2（src）	NA	NA	NA	NA	NA	NA	NA	NA	dir、m	dir、m	dir、m

a. この構成では、ファイル移行はサポートされていません。

レプリケーション タイプ

レプリケーションは、通常、バックアップ システムからデータを受け取る［ソース］DD システムと、1 つ以上の［デスティネーション］DD システムで構成されます。各 DD システムは、レプリケーション コンテキストのソースおよびデスティネーションになることができます。レプリケーション中、各 DD システムは通常のバックアップおよびリストア処理を実行できます。

レプリケーション タイプごとに、ソース上の既存ディレクトリまたは MTree と関連づけられた［コンテキスト］が設定されます。コンテキストが設定されると、レプリケーションされたコンテキストがデスティネーションに作成されます。コンテキストにより、常にアクティブであるレプリケーション ペアが設定されます。また、ソースに届くデータはすべて、できるだけ早い機会にデスティネーションにコピーされます。レプリケーション コンテキストに構成されるパスは絶対参照であり、構成されているシステムに基づき変更することはできません。

Data Domain システムは、ディレクトリ、コレクション、MTree レプリケーションに対してセットアップできます。

- ［ディレクトリ レプリケーション］では、個々のディレクトリ レベルでレプリケーションできます。
- ［コレクション レプリケーション］では、ソース上のデータ ストア全体が複製されて、デスティネーションに転送されます。レプリケーションされたボリュームは読み取り専用です。

- ［MTree レプリケーション］では、MTree（つまり、高度な管理を可能にする仮想ファイル構造）全体がレプリケーションされます。メディア プールもレプリケーション可能で、デフォルト（DD OS 5.3 の時点）では、MTree が作成されてレプリケーションされます （メディア プールは下位互換性モードでも作成でき、レプリケーションされると、ディレクトリ レプリケーション コンテキストになります）。

すべてのレプリケーション タイプにおいて、次の要件に注意してください。

- デスティネーション Data Domain システムには、少なくとも、ソース ディレクトリの予想される最大サイズ分の利用可能なストレージ容量を用意する必要があります。デスティネーション Data Domain システムに、レプリケーション ソースからのすべてのトラフィックを処理するのに十分なネットワーク帯域幅とディスク領域があることを確認してください。
- ファイル システムは有効になっているか、レプリケーション タイプに基づき、レプリケーション初期化の一環として有効になる必要があります。
- ソースは存在している必要があります。
- デスティネーションは存在していない必要があります。
- デスティネーションは、コンテキストが作成されて初期化されると作成されます。
- レプリケーションが初期化された後、デスティネーションの所有権と権限は常に、ソース MTree と同じになります。
- レプリケーション コマンドのオプションでは、特定のレプリケーション ペアは常にデスティネーションによって特定されます。
- 両方のシステムに、IP ネットワーク経由のアクティブな可視ルートが存在し、各システムがそれぞれのパートナーのホスト名を解決できる必要があります。

レプリケーション タイプの選択は、ニーズによって異なります。後続のセクションでは、3 つのレプリケーション タイプの説明と機能に加えて、DD Boost で使用される管理ファイル レプリケーションの概要について説明します。

管理ファイル レプリケーション

DD Boost によって使用される［管理ファイル レプリケーション］は、バックアップ ソフトウェアによって管理および制御されるレプリケーションのタイプです。

管理ファイル レプリケーションでは、バックアップ イメージは、バックアップ ソフトウェアからの要求に応じて 1 つずつ、1 つの DD システムから他のシステムに直接転送されます。

バックアップ ソフトウェアは、レプリケーション ステータスの監視と複数コピーからのリカバリを容易に実行できるように、すべてのコピーを履歴管理します。

管理ファイル レプリケーションでは、フル システム ミラーリング、双方向、多対 1、1 対多、カスケードを含め、柔軟なレプリケーション トポロジーが提供され、効率的なサイト間重複排除が可能です。

次に、管理ファイル レプリケーションに関するいくつかの追加の考慮事点を示します。

- レプリケーション コンテキストを構成する必要はありません。
- ライフサイクル ポリシーにより、ユーザーが介入しなくても、情報のレプリケーションが制御されます。
- DD Boost では、必要に応じてオンザフライでコンテキストの作成と分解が行われます。

詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」の `ddboost file-replication` コマンドを参照してください。

ディレクトリ レプリケーション

［ディレクトリ レプリケーション］では、レプリケーション ソースとして構成されている DD ファイル システム ディレクトリ内の重複排除されたデータが、別のシステム上のレプリケーション デスティネーションとして構成されているディレクトリに転送されます。

ディレクトリ レプリケーションを使用することで、DD システムは一部のレプリケーション コンテキストのソースとその他のコンテキストのデスティネーションを兼ねることができます。また、DD システムは、データのレプリケーションを行いながら、バックアップ アプリケーションとアーカイブ アプリケーションからデータを受信することもできます。

ディレクトリ レプリケーションには、管理対象ファイル レプリケーション（DD Boost によって使用されるタイプ）と同じ柔軟なネットワーク展開トポロジーとサイト間重複排除があります。

ディレクトリ レプリケーションを使用するタイミングを検討する際、次の点に留意してください。

- 同一のディレクトリに CIFS データと NFS データを混在させないでください。単一のデスティネーション DD システムは、CIFS と NFS で異なるディレクトリが使用されている限り、CIFS クライアントと NFS クライアントの両方からバックアップを受信することができます。
- ディレクトリは一度に 1 つのコンテキストにのみ存在できます。親ディレクトリは、その親の子ディレクトリがすでにレプリケーションされている場合、レプリケーション コンテキストで使用できないことがあります。
- ディレクトリ レプリケーション ソース ディレクトリ［に入る、またはそこから出る］ファイルまたはテープの名称変更（移動）は、［許可されていません］。ディレクトリ レプリケーション ソース ディレクトリ［内での］ファイルまたはテープの名称変更は、［許可されています］。
- デスティネーション DD システムには、少なくとも、ソース ディレクトリの予想される圧縮後の最大サイズのストレージ容量を用意する必要があります。
- レプリケーションが初期化されると、デスティネーション ディレクトリが自動的に作成されます。
- レプリケーションが初期化された後、デスティネーション ディレクトリのオーナーシップとアクセス許可はソース ディレクトリと常に同じです。コンテキストが存在する限り、デスティネーション ディレクトリは読み取り専用の状態に維持され、ソース ディレクトリからのみデータを受信可能です。
- グローバル圧縮には常に差があるため、ソースとデスティネーション ディレクトリはサイズが異なる場合があります。

フォルダー作成時の推奨事項

ディレクトリ レプリケーションは、`/data/col1/backup` にある個別のサブディレクトリのレベルでデータをレプリケーションします。

データを細かく分割するためには、ホスト システムから、**/backup Mtree** 内に他のディレクトリ（DirA、DirB など）を作成する必要があります。各ディレクトリは、使用環境およびそれらのディレクトリを別の場所にレプリケーションするための要件に基づいている必要があります。**/backup MTree** 全体のレプリケーションはできないため、**/data/col1/backup/**の下にある各サブディレクトリ（例、**/data/col1/backup/DirC**）にレプリケーション コンテキストをセットアップします。この目的は次のとおりです。

- デスティネーションの場所をコントロールし、DirA を 1 つのサイトにレプリケーションし、DirB を別のサイトにレプリケーションすることができます。
- このレベルの細分性があることで、管理、監視、障害の切り分けが可能になります。各レプリケーション コンテキストを一時停止、停止、破棄、報告することができます。
- パフォーマンスは単一のコンテキストに限定されます。複数コンテキストを作成することで、統合レプリケーションのパフォーマンスを向上できます。

- 一般的な推奨事項として、複数のレプリケーション ストリーム間でレプリケーションの負荷を分散させるには、約 5～10 のコンテキストが必要になります。この妥当性は、サイトの設計およびその場所のデータの量と構成に対して検証する必要があります。

注

推奨されるコンテキストの数は、設計に左右される問題であり、場合によっては、レプリケーションを最適化する目的で行われるデータの分離に関する選択に重大な意味をもたらすことがあります。データは通常、レプリケーション方式ではなく、格納方式のために最適化されます。バックアップ環境を変更する際には、この点に注意してください。

MTree レプリケーション

［MTree レプリケーション］は、DD システム間での MTree のレプリケーションに使用されます。定期的なスナップショットがソース上に作成され、それらの間の違いが、ディレクトリ レプリケーションに使用されるのと同じサイト間重複排除メカニズムを利用して宛先に転送されます。これによって、常にファイル整合性を保ちつつ、宛先上のデータをソースのポイント イン タイム コピーとすることができます。また、これによってデータ中のチャーンのレプリケーションを削減し、WAN をより効率的に活用します。

ディレクトリ レプリケーションでは、ソース ディレクトリのコンテンツに対するすべての変更を順番にレプリケートする必要がありますが、MTree レプリケーションでスナップショットを使用すると、ソースに対する一部の中間の変更をスキップすることができます。これらの変更をスキップすると、ネットワーク経由で送信されるデータの量がさらに減り、その結果、レプリケーションの遅延が減少します。

MTree レプリケーションを使用することで、DD システムは一部のレプリケーション コンテキストのソースとその他のコンテキストの宛先を兼ねることができます。また、DD システムは、データのレプリケーションを行いながら、バックアップ アプリケーションとアーカイブ アプリケーションからデータを受信することもできます。

MTree レプリケーションには、管理対象ファイル レプリケーション（DD Boost によって使用されるタイプ）と同じ柔軟なネットワーク展開トポロジーとサイト間重複排除があります。

MTree レプリケーションを使用するタイミングを検討する際、次の点に留意してください。

- レプリケーションが初期化されると、宛先に読み取り専用の MTree が自動的に作成されます。
- データは、レプリケーションのパフォーマンスを向上させるために、複数の MTree に論理的に分離されます。
- スナップショットは、ソース コンテキストに作成する必要があります。
- スナップショットは、レプリケーションの宛先には作成できません。
- スナップショットは、1 年間の固定の保存期間でレプリケーションされますが、保存期間は宛先上で調整可能であり、宛先で調整する必要があります。
- レプリケーション コンテキストは、ソースと宛先の両方に構成する必要があります。
- DD VTL テープ カートリッジ（またはプール）のレプリケーションは、単に DD VTL テープ カートリッジを含む MTree またはディレクトリのレプリケーションを意味します。メディア プールは、デフォルトで、MTree レプリケーションによってレプリケーションされます。メディア プールは下位互換性モードで作成し、その後、ディレクトリ ベースのレプリケーションでレプリケーションすることができます。コマンド ラインを使用してレプリケーション コンテキストを作成するために、pool://構文を使用することはできません。DD System Manager でプール ベースのレプリケーションを指定すると、メディア プールのタイプに基づき、ディレクトリまたは MTree レプリケーションが作成されます。
- MTree 下でのディレクトリのレプリケーションは禁止されています。
- 宛先の DD システムには、少なくとも、ソース MTree の予想される圧縮後の最大サイズのストレージ容量を用意する必要があります。

- レプリケーションが初期化された後、デスティネーション ディレクトリの所有権と権限は常に、ソース MTree と同じになります。コンテキストが存在する限り、デスティネーション MTree は読み取り専用の状態で保持され、ソース MTree からのみデータを受信できます。
- どの時点においても、グローバル圧縮での違いのため、ソース MTree とデスティネーション MTree のサイズが異なることがあります。
- DD Extended Retention システムから非 DD Extended Retention システムへの MTree レプリケーションは、両方が DD OS 5.5 以降を実行している場合にサポートされます。
- DD Retention Lock Compliance は、デフォルトで、MTree レプリケーションに対応しています。ソースに DD Retention Lock のライセンスがある場合、宛先にも DD Retention Lock のライセンスが必要です。ライセンスがない場合、レプリケーションは失敗します （この状況を回避するには、DD Retention Lock を無効にする必要があります）。レプリケーション コンテキストで DD Retention Lock が有効になっている場合、レプリケーションされた宛先のコンテキストには、常に Retention Lock 付きのデータが含まれることになります。

MTree レプリケーションの詳細

MTree レプリケーションには、次のステップが含まれます。

1. スナップショットは、ソース レプリケーション コンテキストで作成されます。
2. このスナップショットは、直前のスナップショットと比較されます。
3. 2 つのスナップショット間の相違が、デスティネーション レプリケーション コンテキストに送信されます。
4. デスティネーションでは、MTree は更新されますが、すべての変更がデスティネーション システムによって受信されるまで、ファイルはユーザーに公開されません。

これらのステップは、ソース MTree でスナップショットが作成されるたびに繰り返されます。以下の状況では、ソース システムでスナップショットの作成がトリガーされます。

- システムによって生成された定期的なスナップショット：レプリケーションの遅延が 15 分を超えており、現在レプリケートされているスナップショットがない場合。
- ユーザーが作成したスナップショット：バックアップ ジョブの完了後など、ユーザーが指定した時刻。

さまざまな種類のスナップショットの相互作用を示す例については、KB 資料「How MTree Replication Works」（https://support.emc.com/kb/180832）を参照してください。

スナップショットがレプリケートされると、デスティネーションへの接続は閉じられます。ソースとデスティネーションの間の新しい接続は、次のスナップショットがレプリケートされるときに確立されます。

AMS（自動マルチ ストリーミング）

AMS（自動マルチ ストリーミング）により MTree レプリケーションのパフォーマンスが向上します。AMS は、複数のストリームを使用して単一の大容量ファイル（32 GB 以上）をレプリケーションし、レプリケーション中のネットワーク帯域幅の使用率を向上させます。また、個々のファイルのレプリケーション速度を高めることにより、レプリケーション キューのパイプラインの効率とレプリケーションのスループットを向上させ、レプリケーション ラグを低減します。

ワークロードに複数の最適化オプションがある場合、AMS はワークロードに最適なオプションを自動的に選択します。たとえば、ワークロードが fastcopy 属性を持つ大容量ファイルの場合、レプリケーション操作では、fastcopy の最適化によってファイル スキャンのオーバーヘッドを回避し、レプリケーション ペア間の一意のセグメントを特定します。ワークロードが合成を使用している場合、レプリケーションは AMS 上のシンセティック レプリケーションを使用して、各レプリケーション ストリームでファイルが生成されるようにデスティネーション システムのローカル操作を活用します。

AMS は常に有効になっており、無効にすることはできません。

コレクション レプリケーション

［コレクション レプリケーション］は、1 対 1 のトポロジーでシステム全体のミラーリングを実行し、DD ファイル システムのすべての論理ディレクトリとファイルを含む、基盤となるコレクション内の変更を継続的に転送します。

コレクション レプリケーションには他のタイプの柔軟性がないが、スループットを改善し、より少ないオーバーヘッドでより多くのオブジェクトに対応できます。これは、規模の大きい企業の場合には有効です。

コレクション レプリケーションは、ソース DD システムの `/data/col1` 領域全体をデスティネーション DD システムにレプリケーションします。

注

コレクション レプリケーションは、クラウド階層対応システムではサポートされていません。

コレクション レプリケーションを使用するタイミングを検討する際、次の点に留意してください。

- レプリケーションの詳細な制御はできません。ソースの全データがデスティネーションにコピーされて、読み取り専用のコピーが作成されます。
- コレクション レプリケーションを行うには、デスティネーション システムのストレージ容量は、ソース システムのストレージ容量以上である必要があります。デスティネーションの容量がソースの容量よりも小さい場合、ソース上で使用可能な容量がデスティネーションと同じまで減らされます。
- コレクション レプリケーションのデスティネーションとして使用される DD システムは、レプリケーションを構成する前に空にする必要があります。レプリケーションを構成すると、このシステムはソース システムからのデータ受信専用になります。
- コレクション レプリケーションでは、すべてのユーザー アカウントおよびパスワードがソースからデスティネーションにレプリケーションされます。ただし、DD OS 5.5.1.0 時点では、DD システムの構成とユーザー設定の他の構成要素はデスティネーションにはレプリケーションされません。リカバリ後に明示的に再構成する必要があります。
- コレクション レプリケーションは、DD SMT（Secure Multitenancy）でサポートされます。テナントや UUID が一致するテナント ユニットの定義など、レジストリの名前空間に含まれるコア SMT の情報は、レプリケーション操作中に自動的に転送されます。ただし、次の SMT の情報はレプリケーションのために自動的に含められないため、デスティネーション システムで手動で構成する必要があります。
  - テナント ユニットごとのアラート通知リスト
  - SMT テナントが使用する、DD Boost プロトコルに割り当てられているすべてのユーザー（システムで DD Boost が構成されている場合）
  - 各 DD Boost ユーザーに関連づけられているデフォルトのテナント ユニット（システムで DD Boost が構成されており、関連づけられている場合）

  レプリケーション先でこれらのアイテムを手動で構成する方法については、「ディザスタリカバリ用コレクション レプリケーションおよび SMT の使用（462 ページ）」で説明します。
- DD Retention Lock Compliance はコレクション レプリケーションに対応しています。
- コレクション レプリケーションは、クラウド階層対応システムではサポートされていません。
- コレクション レプリケーションでは、ファイル システムのクリーニングのためにレプリケートされていないソース システム上のレプリケーション コンテキストのデータを処理することはできません。ソース システムとデスティネーション システムが同期していないことが原因でファイル システムのクリーニングを完了できない場合、システムではクリーニング操作のステータスが `partial` と報告され、

クリーニング操作にごく一部のシステム統計しか使用できません。コレクション レプリケーションが無効になっている場合、レプリケーションのソース システムとデスティネーション システムが同期しない状態が続くため、ファイル システムのクリーニングのために処理できないデータの量が増加します。オンライン サポート サイト （https://support.emc.com）にあるナレッジ ベース記事「Data Domain: An overview of Data Domain File System (DDFS) clean/garbage collection (GC) phases」に補足情報が記載されています。

- 広帯域幅環境でスループットを向上させるには、**`replication modify <destination> crepl-gc-gw-optim`** コマンドを実行し、コレクション レプリケーションの帯域幅最適化を無効にします。

DD Replicator と DD Encryption の使用

DD Replicator をオプションの［DD Encryption］機能とともに使用することで、コレクション、ディレクトリ、MTree レプリケーションのいずれかを使用して暗号化されたデータをレプリケーションできます。

レプリケーション コンテキストは、常に［共有シークレット］で認証されます。その共有シークレットは、Diffie-Hellman キー交換プロトコルを使用したセッション キーの確立に使用されます。そのセッション キーは、必要に応じて Data Domain システム暗号化キーの暗号化と復号化に使用されます。

レプリケーション タイプはそれぞれ、暗号化に対して独自に対応し、同じレベルのセキュリティを実現します。

- ［コレクション レプリケーション］の場合、デスティネーション データがソース データの正確なレプリカとなることが期待されているため、ソースとデスティネーションの暗号化の構成が同じである必要があります。特に、暗号化機能のオンまたはオフについてはソースとデスティネーションの両方で同じ設定にする必要があります。暗号化機能がオンになっている場合、暗号化アルゴリズムとシステムのパスフレーズも一致している必要があります。パラメーターはレプリケーション関連付け段階でチェックされます。
  コレクション レプリケーション中、ソースは暗号化された形式でデータを送信し、デスティネーションに暗号化キーも送信します。デスティネーションには同じパスフレーズと同じシステム暗号化キーがあるため、データはデスティネーションでリカバリできます。

  注

  コレクション レプリケーションは、クラウド階層対応システムではサポートされていません。

- ［MTree またはディレクトリ レプリケーション］の場合、ソースとデスティネーションの両方で暗号化の構成を同じにする必要はありません。その代わり、レプリケーション関連づけフェーズ中にソースとデスティネーションでデスティネーションの暗号化キーが安全に交換されます。データはデスティネーションの暗号化キーを使用してソースで再暗号化されてから、デスティネーションに送信されます。
  デスティネーションの暗号化構成が異なる場合、送信されたデータは適切に準備されます。たとえば、デスティネーションで機能がオフになっている場合、ソースはデータを復号化し、それを暗号化されていない状態でデスティネーションに送信します。
- ［カスケード レプリケーション］ トポロジーでは、レプリカは 3 つの Data Domain システム間でつながれています。チェーンの最後のシステムは、コレクション、MTree、またはディレクトリのいずれかとして構成できます。最後のシステムがコレクション レプリケーション デスティネーションである場合、それは同じ暗号化キーおよび暗号化されたデータをそのソースとして使用します。最後のシステムが MTree またはディレクトリ レプリケーション デスティネーションである場合、それは自身のキーを使用し、データはソースで暗号化されます。各リンクのデスティネーションの暗号化キーは、暗号化に使用されます。チェーンのシステムの暗号化は、レプリケーション ペアと同様に機能します。

レプリケーション トポロジー

DD Replicator は、5 つのレプリケーション トポロジー（1 対 1、1 対 1 の双方向、1 対多、多対 1、カスケード）に対応しています。このセクションの表には、（1）これらのトポロジーと 3 つのタイプのレプリケーション（MTree、ディレクトリ、コレクション）と 2 つのタイプの DD システム（SN（単一ノード）と DD Extended Retention）の対応、（2）カスケード レプリケーションでの混在トポロジーのサポートが示されています。

一般なガイドラインは次のとおりです。

- SN（単一ノード）システムは、すべてのレプリケーション トポロジーに対応しています。
- SN -> SN（単一ノード対単一ノード）は、すべてのレプリケーション タイプで使用できます。
- DD Extended Retention システムは、ディレクトリ レプリケーションのソースにはできません。
- コレクション レプリケーションは、SN（単一ノード）システムから DD Extended Retention 対応システムにも、DD Extended Retention 対応システムから SN システムにも構成できません。
- SN システムから DD 高可用性対応システムへも、DD 高可用性対応システムから SN システムへも、コレクション レプリケーションを構成することはできません。
- MTree およびディレクトリ レプリケーションでは、DD 高可用性システムは SN システムと同様に扱われます。
- 一方または両方のシステムが Cloud Tier に対応している場合は、コレクション レプリケーションを構成することはできません。

テーブル内の略語について：

- SN = 単一ノード DD システム（DD Extended Retention なし）
- ER = DD Extended Retention システム

表 188 レプリケーション タイプと DD システム タイプ別のトポロジーのサポート

トポロジー	MTree レプリケーション	ディレクトリ レプリケーション	コレクション レプリケーション
1 対 1	{SN | ER} -> {SN | ER} ER->SN（5.5 リリースからサポート開始、5.5 以前はリカバリのみ）	SN -> SN SN -> ER	SN -> SN ER -> ER
1 対 1 の双方向	{SN | ER} -> {SN | ER}	SN -> SN	サポートされていません
1 対多	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	サポートされていません
多対 1	{SN | ER} -> {SN | ER}	SN -> SN SN -> ER	サポートされていません
カスケード	{SN | ER } -> {SN | ER} -> {SN | ER}	SN -> SN -> SN SN -> SN -> ER	ER -> ER -> ER SN -> SN -> SN

カスケード レプリケーションは、カスケード接続の 2 番目のボリュームが、接続の最初のタイプとは異なっている混在トポロジーに対応しています（A -> B がディレクトリ レプリケーションで、B -> C がコレクション レプリケーションの場合など）。

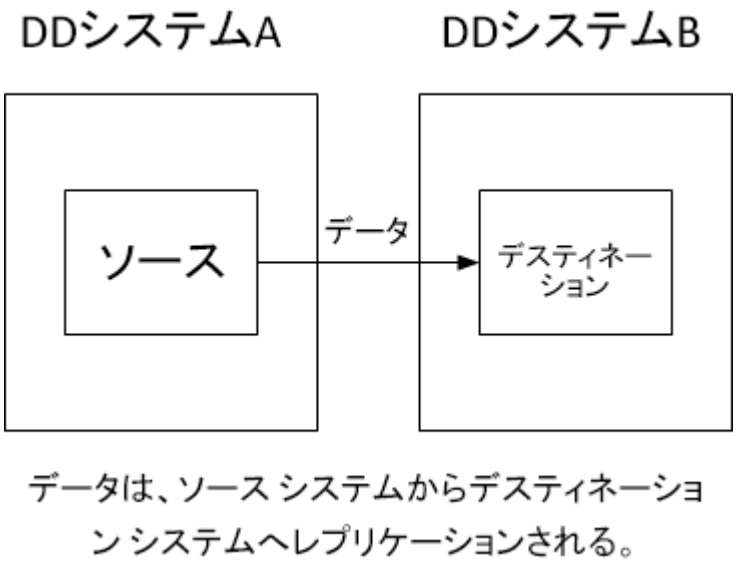
表 189 カスケード レプリケーションでサポートされている混在トポロジー

混在トポロジー	
SN – ディレクトリ レプリケーション -> ER – MTree レプリケーション -> ER – MTree レプリケーション	SN – ディレクトリ レプリケーション -> ER – コレクション レプリケーション -> ER – コレクション レプリケーション
SN – MTree レプリケーション -> SN – コレクション レプリケーション -> SN – コレクション レプリケーション	SN – MTree レプリケーション -> ER – コレクション レプリケーション -> ER – コレクション レプリケーション

1 対 1 レプリケーション

最もシンプルなタイプのレプリケーションは、DD ソース システムから DD デスティネーション システムへのレプリケーションです。これは［1 対 1］レプリケーション ペアとも呼ばれています。このレプリケーション トポロジーは、ディレクトリ、MTree、コレクションのレプリケーション タイプで構成できます。

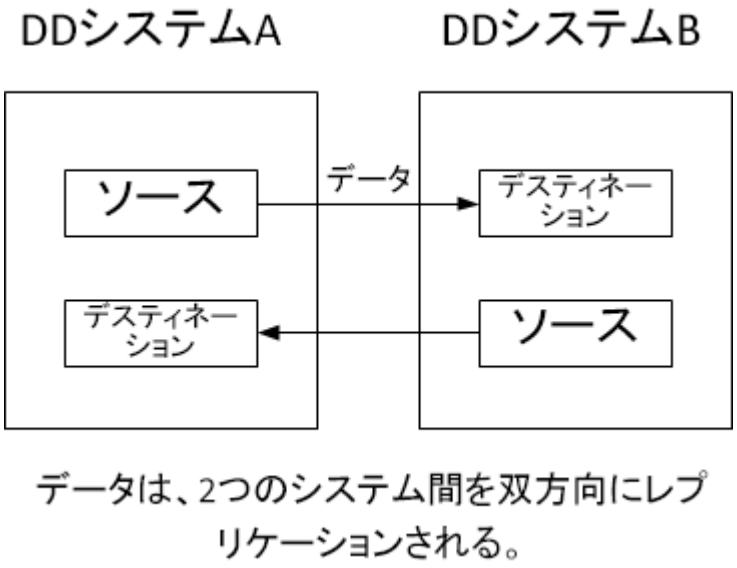
図 18 1 対 1 レプリケーション ペア



双方向レプリケーション

双方向レプリケーション ペアでは、DD システム A のディレクトリまたは MTree のデータが DD システム B にレプリケーションされ、DD システム B の別のディレクトリまたは MTree のデータが DD システム A にレプリケーションされます。

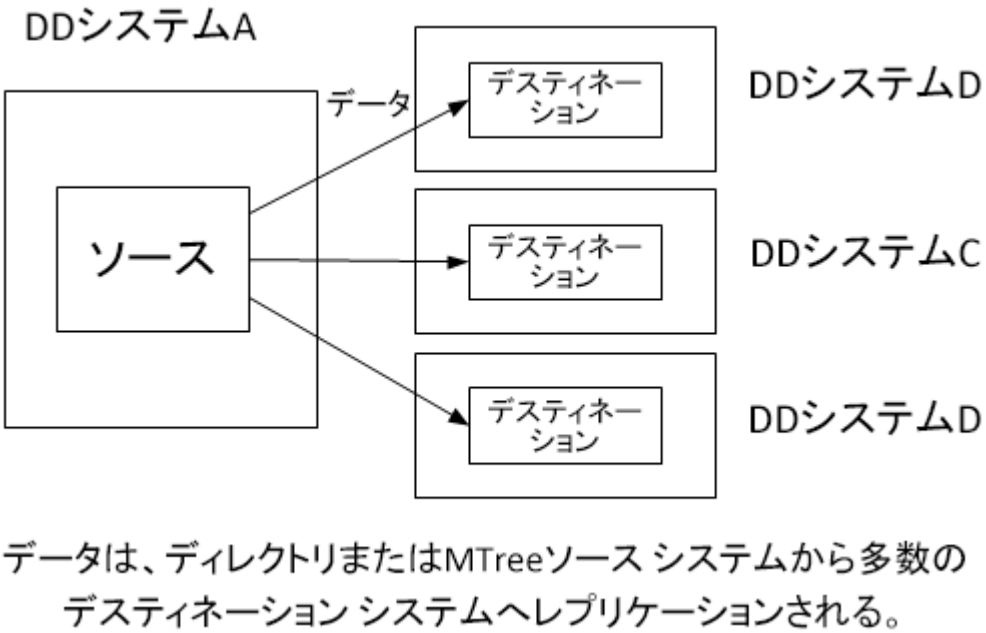
図 19 双方向レプリケーション



1 対多レプリケーション

1 対多レプリケーションでは、1 つの DD システムのソース ディレクトリまたは MTree のデータが、複数のデスティネーション DD システムにレプリケーションされます。このタイプのレプリケーションを使用すると、データ保護の強化のために複数のコピーを作成したり、複数サイトでの使用のためにデータを分散することが可能になります。

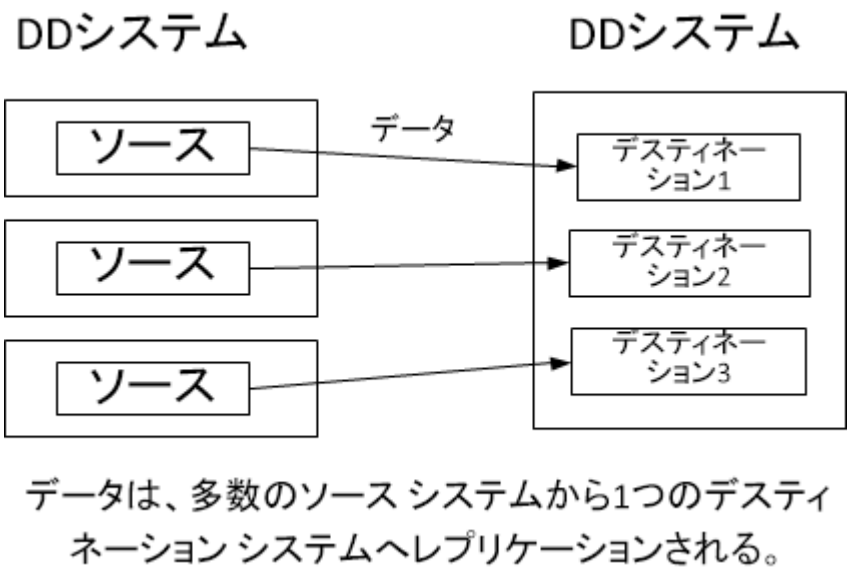
図 20 1 対多レプリケーション



多対 1 レプリケーション

多対 1 レプリケーションでは、MTree かディレクトリかを問わず、レプリケーション データは複数のソース DD システムから単一のデスティネーション DD システムにレプリケーションされます。このタイプのレプリケーションは、複数の支店から本社の IT システムにデータ リカバリ保護を提供する場合に使用できます。

図 21 多対 1 レプリケーション

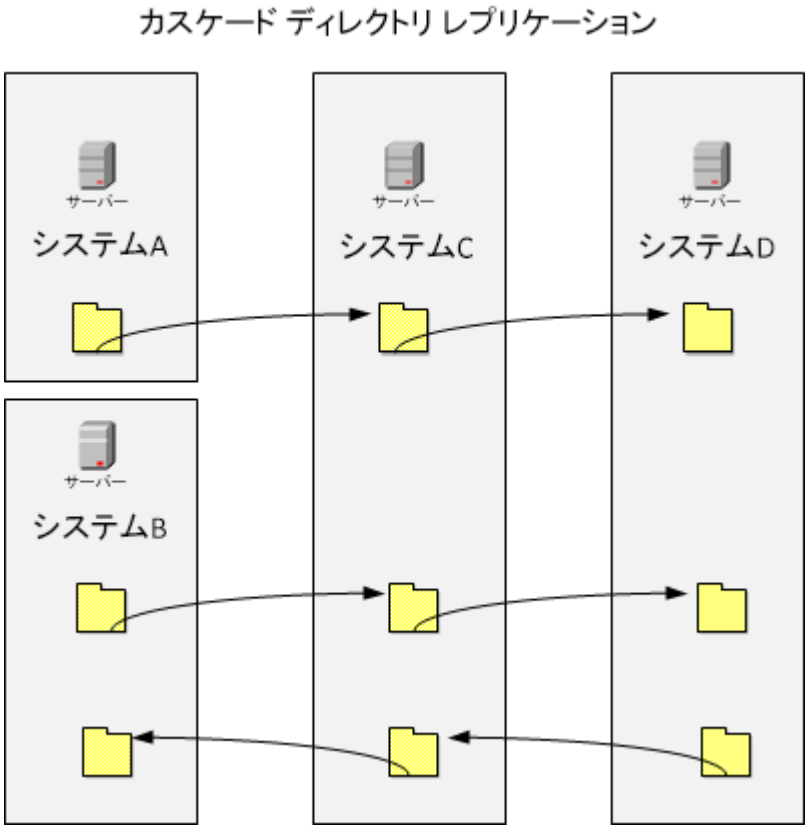


カスケード レプリケーション

カスケード レプリケーション トポロジーでは、ソース ディレクトリまたは MTree は 3 つの DD システム間でつながれています。チェーンの最後にあるホップは、ソースがディレクトリか MTree かに応じて、コレクション、MTree、ディレクトリのレプリケーションとして構成できます。

たとえば、DD システム A から DD システム B に 1 つ以上の Mtree がレプリケーションされ、次にそれらの MTree が DD システム C にレプリケーションされる場合、DD システム B 上の Mtree は（DD システム A からの）デスティネーションと（DD システム C への）とソースの両方を兼ねます。

図 22 カスケード ディレクトリ レプリケーション



非縮退レプリケーション ペア コンテキストからデータ リカバリを行うことができます。次に例を挙げます。

- DD システム A のリカバリが必要な場合、DD システム B からデータをリカバリできます。
- DD システム B のリカバリが必要な場合、最も単純な方法は、DD システム A から（交換用）DD システム B にレプリケーションの再同期を行う方法です。この場合、DD システム B から DD システム C へのレプリケーション コンテキストは最初に破棄する必要があります。DD システム A から DD システム B へのレプリケーション コンテキストの再同期が終了したら、新しい DD システム B から DD システム C へのコンテキストを構成して、再同期する必要があります。

レプリケーションの管理

DD System Manager（Data Domain System Manager）または DD OS（Data Domain オペレーティング システム）CLI（コマンド ライン インターフェイス）を使用してレプリケーションを管理することができます。

GUI（グラフィカル ユーザー インターフェイス）を使用してレプリケーションを管理するには、DD System Manager にログインします。

手順

1. DD System Manager の左側のメニューで、［**Replication**］を選択します。ライセンスが追加されていない場合は、［**Add License**］を選択します。
2. ［**Automatic**］または［**On-Demand**］を選択します（［On-Demand］には DD Boost ライセンスが必要）。

   ［**CLI** 相当］

次の CLI を使用してログインすることもできます。

```
login as: sysadmin
Data Domain OS 6.0.x.x-12345
Using keyboard-interactive authentication.
Password:
```

レプリケーション ステータス

［Replication Status］には、警告（黄色のテキスト）、エラー（赤色のテキスト）状態、または通常状態を表すレプリケーション コンテキストのシステム全体のカウントが表示されます。

［Summary］ビュー

［Summary］ビューには、DD システムの構成済みレプリケーション コンテキストがリストされ、選択した DD システムに関する集約情報（インバウンドおよびアウトバウンド レプリケーション ペアに関するサマリー情報）が表示されます。DD システム自体および DD システムの入出力に焦点が当てられます。

［Summary］テーブルは、Source または Destination 名を入力するか、State（Error、Warning、または Normal）を選択して、フィルタリングできます。

表 190 ［Replication Summary］ビュー

項目	説明
Source	ソース コンテキストのシステムおよびパス名。形式は system.path。たとえば、`system dd120-22` 上のディレクトリ `dir1` の場合、`dd120-22.chaos.local/data/col1/dir1` と表示されます。
Destination	デスティネーション コンテキストのシステムおよびパス名。形式は system.path。たとえば、`system dd120-44` 上の MTree `MTree1` の場合、`dd120-44.chaos.local/data/col1/MTree1` と表示されます。
Type	コンテキストのタイプ：MTree、ディレクトリ（Dir）、またはプール。
State	可能性があるレプリケーション ペア ステータスの状態は、次のとおりです。 • Normal：レプリカが Initializing、Replicating、Recovering、Resyncing、Migrating のいずれかである場合。 • Idle：MTree レプリケーションでは、レプリケーション プロセスが現在アクティブではない、またはネットワーク エラー（デスティネーション システムにアクセスできない、など）が発生した場合、この状態が表示されます。 • Warning：最初の 5 つの状態に異常な遅延がある場合、または Uninitialized 状態の場合 • Error：Disconnected などの可能なエラー状態
Synced As Of Time	ソースによって実行される最後の自動レプリケーション同期操作用のタイムスタンプ MTree レプリケーションでは、スナップショットがデスティネーションで公開されると、この値が更新されます。ディレクトリ レプリケーションでは、ソースによって挿入された同期ポイントが適用されると、この値が更新されます。レプリケーション初期化中に不明な値が表示されます。
Pre-Comp Remaining	レプリケーションされる残りの圧縮前データの量。

表 190 ［Replication Summary］ビュー （続き）

項目	説明
Completion Time (Est.)	値は `Completed`、または過去 24 時間の転送レートに基づくレプリケーション データ転送の完了に必要な推定期間です。

レプリケーション コンテキストの詳細情報

［Summary］ビューから 1 つのレプリケーション コンテキストを選択すると、そのコンテキストの情報が［Detailed Information］、［Performance Graph］、［Completion Stats］、［Completion Predictor］に入力されます。

表 191 Detailed Information

項目	説明
State Description	レプリカの状態についてのメッセージ。
Source	`system.path` 形式のソース コンテキストのシステムおよびパス名。たとえば、`dir1` システムのディレクトリ `dd120-22` の場合、`dd120-22.chaos.local/data/col1/dir1` と表示されます。
Destination	`system.path` 形式のデスティネーション コンテキストのシステムおよびパス名。たとえば、`MTree1` システムの MTree `dd120-44` の場合、`dd120-44.chaos.local/data/col1/MTree1` と表示されます。
Connection Port	レプリケーション接続に使用されるシステム名とリスン ポート。

表 192 Performance Graph

項目	説明
Pre-Comp Remaining	レプリケーションされる残りの圧縮前データの量。
Pre-Comp Written	ソースに書き込まれた圧縮前データ
Post-Comp Replicated	レプリケーションされた圧縮後データの量。

表 193 Completion Stats

項目	説明
Synced As Of Time	ソースによって実行される最後の自動レプリケーション同期操作用のタイムスタンプ MTree レプリケーションでは、スナップショットがデスティネーションで公開されると、この値が更新されます。ディレクトリ レプリケーションでは、ソースによって挿入された同期ポイントが適用されると、この値が更新されます。レプリケーション初期化中に不明な値が表示されます。
Completion Time (Est.)	値は `Completed`、または過去 24 時間の転送レートに基づくレプリケーション データ転送の完了に必要な推定期間です。
Pre-Comp Remaining	レプリケーションされる残りのデータの量。
Files Remaining	（Directory Replication のみ）レプリケーションされていないファイルの数。

表 193 Completion Stats （続き）

項目	説明
Status	ソースおよびデスティネーション エンドポイントについて、次のようなシステム上の主なコンポーネントのステータス（Enabled、Disabled、Not Licensed、など）が表示されます。 • Replication • File System • DD Retention Lock • DD Encryption at Rest • DD Encryption over Wire • Available Space • Low Bandwidth Optimization • Compression Ratio • Low Bandwidth Optimization Ratio

Completion Predictor

Completion Predictor は、選択されたコンテキストについての、バックアップ ジョブの進行状況の追跡およびレプリケーションが完了するタイミングの予測用のウィジェットです。

レプリケーション ペアの作成

レプリケーション ペアを作成する前に、デスティネーションが［存在］しないことを確認してください。存在する場合、エラーになります。

手順

1. ［**Replication**］［**Automatic**］［**Summary tab**］［**Create Pair**］を選択します。
2. 次のセクションの説明に従って、［Create Pair］ダイアログで情報を追加し、MTree、ディレクトリ、コレクション、プール レプリケーション ペアを作成します。

レプリケーション用 DD システムの追加

レプリケーション ペアを作成する前に、ホストまたはターゲットとして DD システムの追加が必要になる場合があります。

注

追加対象システムが、互換性のある DD OS バージョンを実行していることを確認してください。

手順

1. ［Create Pair］ダイアログでは、［Add System］を選択します。
2. ［System］には、追加するシステムのホスト名または IP アドレスを入力します。
3. ［User Name］と［Password］には、システム管理者のユーザー名とパスワードを入力します。
4. オプションで、［**More Options**］を選択して、直接到達できないシステムのプロキシ IP アドレス（またはシステム名）を入力します。構成されている場合、デフォルト ポート 3009 の代わりにカスタム ポートを入力します。

注

IPv6 アドレスに対応するのは、DD OS 5.5 以降のシステムを DD OS 5.5 以降を使用している管理システムに追加する場合のみです。

5. ［**OK**］を選択します。

注

DD System Manager にシステムを追加した後で、そのシステムにアクセスできない場合、管理システムから追加システムへのルートがあることを確認します。ホスト名（完全修飾ドメイン名（FQDN）または非 FQDN）を入力した場合、それが管理対象システムで解決可能であることを確認します。管理対象システムのドメイン名を構成するか、システムの DNS エントリーが存在することを確認するか、IP アドレスからホスト名へのマッピングが定義されていることを確認します。

6. システム証明書が確認されていない場合、［Verify Certificate］ダイアログに証明書に関する詳細が表示されます。システム認証情報を確認します。証明書を信頼する場合は［**OK**］を選択します。信頼しない場合は［**Cancel**］を選択します。

コレクション レプリケーション ペアの作成

このタイプのレプリケーションの一般情報については、［コレクション レプリケーション］を参照してください。

コレクション レプリケーション ペアを作成する前に、以下の点を確認してください。

- デスティネーション システムのストレージ容量は、ソース システムのストレージ容量以上である（デスティネーションの容量がソースの容量よりも少ない場合、ソース上で使用可能な容量がデスティネーションの容量まで減らされます）。
- デスティネーションは、破棄後に再作成されているが、有効にはなっていない。
- 各デスティネーションと各ソースは、一度に 1 つのコンテキストにのみ存在する。
- ソースの暗号化を構成し有効にしている間、レプリカ上のファイル システムが無効になっている。
- レプリカの暗号化を構成し有効にしている間、ソース上のファイル システムが無効になっている。

手順

1. ［Create Pair］ダイアログで、［**Replication Type**］メニューから［**Collection**］を選択します。
2. ［**Source System**］メニューからソース システムのホスト名を選択します。
3. ［**Destination System**］メニューからデスティネーション システムのホスト名を選択します。このリストには、［DD-Network］リストのホストのみが含まれます。
4. ホスト接続設定を変更したい場合、［**Advanced**］タブを選択します。
5. ［**OK**］を選択します。ソースからデスティネーションへのレプリケーションが開始されます。

結果

Data Domain からのテスト結果から、次に示すレプリケーション初期化のパフォーマンス ガイドラインが得られました。これは［あくまで］ガイドラインであり、本番環境で見られる実際のパフォーマンスは異なる可能性があります。

- ギビビット LAN の場合： ドライブ最大入力/出力に達するのに十分なシェル カウントと理想的な条件が揃えば、コレクション レプリケーションはプラットフォームによって、1GigE リンク（モジュロ

10%プロトコル オーバーヘッド）に加え、10gigE 上で 400～900 MB/秒を飽和させることができます。

- WAN を通して、パフォーマンスは WAN リンク ライン速度、帯域幅、レーテンシー、パケット損失率によって統制されます。

MTree、ディレクトリ、プール レプリケーション ペアの作成

これらのタイプのレプリケーションに関する一般的な情報については、［MTree レプリケーション］セクションおよび［ディレクトリ レプリケーション］セクションを参照してください。

MTree、ディレクトリ、プール レプリケーション ペアを作成する場合の注意事項

- レプリケーションが正しいインターフェイスを経由していること確認します。レプリケーション コンテキストを定義する場合、ソースとデスティネーションのホスト名は正引き参照および逆引き参照で解決できる必要があります。データがデフォルトのリゾルビング インターフェイスではなく、システム上の代替インターフェイスを通過するようにするには、レプリケーション コンテキストを作成後に変更する必要があります。場合によっては、コンテキストが非リゾルビング（クロス オーバー）インターフェイスに定義されるようにホスト ファイルをセットアップする必要があります。
- MTree レプリケーションのコンテキストを「逆にする」、つまり、デスティネーションとソースを切り替えることができます。
- MTree は全体としてレプリケートされるため、MTree 内のサブディレクトリはレプリケートできません。
- 両方が DD OS 5.5 以降を実行している場合、DD Extended Retention が有効なシステムから DD Extended Retention が有効ではないシステムへの MTree レプリケーションがサポートされます。
- デスティネーション DD システムには、少なくとも、ソース ディレクトリまたは MTree の予想される圧縮後の最大サイズのストレージ容量が必要です。
- レプリケーションが初期化されると、デスティネーション ディレクトリが自動的に作成されます。
- DD システムは、同時に 1 つのコンテキストのソースと他のコンテキストのデスティネーションになることができます。

手順

1. ［Create Pair］ダイアログで、［**Replication Type**］メニューから［**Directory**］、［**MTree**］（デフォルト）または［**Pool**］を選択します。
2. ［**Source System**］メニューからソース システムのホスト名を選択します。
3. ［**Destination System**］メニューからデスティネーション システムのホスト名を選択します。
4. ［**Source Path**］テキスト ボックスにソース パスを入力します（パスの最初の部分は、選択されたレプリケーションのタイプに基づき、変化する定数である点に留意してください）。
5. ［**Destination Path**］テキスト ボックスに宛先パスを入力します（パスの最初の部分は、選択されたレプリケーションのタイプに基づき、変化する定数である点に注意してください）。
6. ホスト接続設定を変更したい場合、［**Advanced**］タブを選択します。
7. ［**OK**］を選択します。

   ソースからデスティネーションへのレプリケーションが開始されます。

   Data Domain からのテスト結果から、次に示すレプリケーション初期化に必要な時間の推定に関するガイドラインが得られました。

   これは［あくまで］ガイドラインであり、特定の本番環境において正しいとは限りません。

   - T3 接続（100ms WAN）を使用した場合、パフォーマンスは圧縮前データで約 40 MiB/秒となります。その場合のデータ転送パフォーマンスは次のとおりです。

40 MiB/秒 = 25 秒/GiB = 3.456 TiB/日

- ギガビット LAN の 2 進数相当を使用した場合、パフォーマンスは圧縮前データで約 80 MiB/秒となります。その場合のデータ転送パフォーマンスは T3 WAN のレートの約 2 倍です。

例 2 CLI 相当

CLI を使用して、MTree レプリケーション ペアを作成する例を示します。この例では、ソース Data Domain システムは **dd640** であり、デスティネーション Data Domain システムは **dlh5** です。詳細については、「Data Domain Operating System コマンド リファレンス ガイド」を参照してください。

1. ソース Data Domain システムで MTree を作成します。

```
sysadmin@dd640# mtree create /data/col1/Oracle2
MTree "/data/col1/Oracle2" created successfully.
```

2. 完全なホスト名を使用して、デスティネーション Data Domain システムでレプリケーション コンテキストを作成します。

```
sysadmin@dlh5# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

3. 完全なホスト名を使用して、ソース Data Domain システムでレプリケーション コンテキストを作成します。

```
sysadmin@dd640# replication add source mtree://dd640.chaos.local/data/col1/Oracle2
destination mtree://dlh5.chaos.local/data/col1/Oracle2
```

4. MTree レプリケーション コンテキストが作成されたことを確認するには、`replication show config` コマンドを使用します。
この例では、出力は左右方向で切り捨てられています。

```
sysadmin@dlh5# replication show config
CTX  Source                                        Destination
---  --------------------------------------------
-----------------------------------------
1    dir://dd640.chaos.local/backup/Oracle2        dir://dlh5.chaos.local/backup/
Oracle2
2    mtree://dd640.chaos.local/data/col1/Oracle2   mtree://dlh5.chaos.local/data/col1/
Oracle2
---  --------------------------------------------
-----------------------------------------
 * Used for recovery only.
```

5. ソースとデスティネーション間のレプリケーションを開始するには、ソースで `replication initialize` コマンドを使用します。このコマンドにより、構成と接続が正しいことが確認され、問題がある場合はエラー メッセージが返されます。

```
sysadmin@dd640# replication initialize mtree://dlh5.chaos.local/data/col1/Oracle2
 (00:08) Waiting for initialize to start...
 (00:10) Intialize started.
 Use 'replication watch mtree://dlh5.chaos.local/data/col1/Oracle2' to monitor progress.
```

双方向レプリケーションの構成

双方向レプリケーション ペアを作成するには、ホスト A からホスト B へのディレクトリまたは MTree レプリケーション ペア手順（たとえば、mtree2 を使用）を使用します。同じ手順を使用して、ホスト B からホスト A へのレプリケーション ペア（たとえば、mtree1 を使用）を作成します。この構成の場合、デスティネーションのパス名は同一にできません。

1 対多レプリケーションの構成

1 対多レプリケーション ペアを作成するには、ホスト A 上でディレクトリまたは MTree レプリケーション ペア手順（mtree1 などを使用して）使用し、（1）ホスト B 上の mtree1、（2）ホスト C 上の mtree1、（3）ホスト D 上の mtree1 へのペアを作成します。パスが他のコンテキストのソース パスで

あるソース コンテキストには、レプリケーションのリカバリは実行できません。他のコンテキストを中断し、リカバリ後に再同期する必要があります。

多対 1 レプリケーションの構成
多対 1 レプリケーションを作成するには、ディレクトリまたは MTree レプリケーション ペア手順を使用します（たとえば、（1）ホスト A の mtree1 からホスト C の mtree1、（2）ホスト B の mtree2 からホスト C の mtree2）。

カスケード レプリケーションの構成
カスケード レプリケーション ペアを作成するには、次のようなディレクトリまたは MTree レプリケーション ペアの手順を使用します。（1）ホスト A 上の mtree1 からホスト B 上の mtree1、（2）ホスト B 上で、mtree1 からホスト C 上の mtree1 へのペアを作成します。最終宛先コンテキスト（この例ではホスト C 上ですが、4 つ以上のホップに対応しています）には、コレクション レプリカ、ディレクトリ レプリカ、MTree レプリカを指定できます。

レプリケーション ペアの無効化と有効化

一時的にレプリケーション ペアを無効化すると、ソースとデスティネーション間のデータのアクティブなレプリケーションが停止します。ソースはデスティネーションへのデータの送信を停止し、デスティネーションはソースへのアクティブな接続としての機能を停止します。

手順

1. ［Summary］テーブルで 1 つ以上のレプリケーション ペアを選択し、［**Disable Pair**］を選択します。
2. ［Display Pair］ダイアログで、［**Next**］、［**OK**］を選択します。
3. 無効化されたレプリケーション ペアの操作を再開するには、［Summary］テーブルでいに以上のレプリケーション ペアを選択し、［**Enable Pair**］を選択して［Enable Pair］ダイアログを表示します。
4. ［**Next**］を選択し、［**OK**］を選択します。データのレプリケーションが再開されます。

   ［**CLI** 相当機能］

```
# replication disable {destination | all}

# replication enable {destination | all}
```

レプリケーション ペアの削除

ディレクトリまたは MTree レプリケーション ペアが削除されると、デスティネーション ディレクトリまたは MTree がそれぞれ書き込み可能になります。コレクション レプリケーション ペアが削除されると、デスティネーション DD システムがスタンドアロンの読み取り/書き込みシステムになり、ファイル システムは無効になります。

手順

1. ［Summary］テーブルで 1 つ以上のレプリケーション ペアを選択し、［**Delete Pair**］を選択します。
2. ［Delete Pair］ダイアログで、［**Next**］、［**OK**］を選択します。レプリケーション プールが削除されます。

   ［**CLI** 相当］
   このコマンドを実行する前に、必ず `filesys disable` コマンドを実行します。その後、`filesys enable` コマンドを実行します。

```
# replication break {destination | all}
```

問題を解決するためにレプリケーションを再同期する必要がある状況が発生する場合があります。レプリケーションの中断と再同期の詳細については、KB 記事「Break and Resync Directory Replication」（https://support.emc.com/kb/180668）を参照してください。

ホスト接続設定の変更

特定のポートからトラフィックを外に出すには、代替システムにアドレスを指定するためにローカル ホスト ファイルに事前に定義したホスト名を使用して、接続ホストのパラメーターを変更し、現在のコンテキストを変更します。そのホスト名は、デスティネーションに対応し、ホスト エントリーは、該当ホストの代替デスティネーション アドレスを示します。この条件は、ソース システムとデスティネーション システムの両方で満たされる必要があります。

手順

1. ［Summary］テーブルでレプリケーション ペアを選択し、［**Modify Settings**］を選択します。［**Advanced**］タブを選択して、Create Pair、Start Resync、または Start Recover を実行しているときにも、これらの設定を変更できます。
2. ［Modify Connection Settings］ダイアログで、次の設定の一部またはすべてを変更します。
   a. ［**Use Low Bandwidth Optimization**］: データ セットが小さく、ネットワークの帯域幅が 6 Mb/s 以下の企業の場合、DD Replicator は［低帯域幅の最適化］を使用して送信されるデータの量をさらに減らすことができます。これによって、限定された帯域幅しかないリモート サイトでも、さらに低い帯域幅を使用するか、既存のネットワーク経由でより多くのデータをレプリケートして保護できます。低帯域幅の最適化は、ソースとデスティネーションの両方の DD システムで有効にする必要があります。ソースとターゲットに互換性のない低帯域幅の最適化が設定されている場合、低帯域幅の最適化はそのコンテキストに対して非アクティブになります。ソースとデスティネーションで低帯域幅の最適化を有効化した後、両システムはフル クリーニング サイクルを行って既存のデータを準備する必要があるため、`filesys clean start` を両システムで実行します。クリーニング サイクルの所要時間は DD システム上のデータ量によって異なりますが、通常のクリーニングよりは長くなります。`filesys` コマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

      ［重要：］ DD Extended Retention ソフトウェア オプションがどちらかの DD システムで有効化されている場合、低帯域幅の最適化はサポートされません。Collection Replication にも対応していません。

   b. ［**Enable Encryption Over Wire**］: DD Replicator は、ADH-AES256-GCM-SHA384 および DHE-RSA-AES256-GCM-SHA384 暗号スイートを使用して安全なレプリケーション接続を確立する標準 SSL（Secure Socket Layer）プロトコル バージョン 1.0.1 を使用した未了（in-flight）データの暗号化に対応しています。暗号化を進めるには、接続の両側でこの機能を有効化する必要があります。

   c. ［**Network Preference**］: IPv4 または IPv6 を選択できます。サービスに IPv4 を経由して到達可能な場合、IPv6 が有効なレプリケーション サービスでは、IPv4 レプリケーション クライアントからの接続を受入れることができます。サービスに IPv4 を経由して到達可能な場合、IPv6 が有効なレプリケーション クライアントは、IPv4 レプリケーション サービスと通信できます。

   d. ［**Use Non-default Connection Host**］: ソース システムは、デスティネーション システム リスン ポートにデータを送信します。1 つのソース システムに複数の（それぞれが異なるリスン ポートを使用する）デスティネーション システムに対するレプリケーションを構成できるため、ソースの各コンテキストでは、デスティネーションの対応するリスン ポートに対する接続ポートを構成できます。
3. ［**Next**］を選択し、［**Close**］を選択します。

レプリケーション ペア設定が更新され、レプリケーションが再開されます。

［**CLI** 相当］

```
#replication modify <destination> connection-host <new-host-
name> [port <port>]
```

レプリケーション システムの管理

レプリケーションに使用する Data Domain システムは、［Manage Systems］ダイアログを使用して追加または削除できます。

手順

1. ［**Manage Systems**］を選択します。
2. ［Manage Systems］ダイアログで、必要に応じて Data Domain システムを追加/削除します。
3. ［**Close**］を選択します。

レプリケーション ペアからのデータのリカバリ

ソース レプリケーション データがアクセスできなくなった場合、それはレプリケーション ペア デスティネーションから［リカバリ］できます。リカバリを進めるには、ソースが空になっている必要があります。リカバリは、MTree レプリケーションを除く、すべてのレプリケーション トポロジーに対して実行できます。

ディレクトリ プールからのデータのリカバリおよびディレクトリとコレクション レプリケーション ペアからのデータのリカバリについては、次のセクションを参照してください。

ディレクトリ プール データのリカバリ

ディレクトリ ベースのプールからはデータをリカバリできますが、MTree ベースのプールからはできません。

手順

1. ［**More**］ > ［**Start Recover**］を選択します。
2. ［Start Recover］ダイアログで、［**Replication Type**］メニューから［**Pool**］を選択します。
3. ［**System to recover to**］メニューからソース システムのホスト名を選択します。
4. ［**System to recover from**］メニューからデスティネーション システムのホスト名を選択します。
5. データをリカバリするデスティネーションのコンテキストを選択します。
6. ホスト接続設定を変更したい場合、［**Advanced**］タブを選択します。
7. ［**OK**］を選択してリカバリを開始します。

コレクション レプリケーション ペア データのリカバリ

コレクション レプリケーション ペア データを正常にリカバリするためには、ソース ファイル システムが初期状態にあり、デスティネーション コンテキストが完全に初期化されている必要があります。

手順

1. ［**More**］ > ［**Start Recover**］を選択して、［Start Recover］ダイアログを表示します。
2. ［**Replication Type**］メニューから、［**Collection**］を選択します。
3. ［**System to recover to**］メニューからソース システムのホスト名を選択します。

4. ［**System to recover from**］メニューからデスティネーション システムのホスト名を選択します。
5. データをリカバリするデスティネーションのコンテキストを選択します。デスティネーションにコレクションは 1 つしかありません。
6. ホスト接続の設定を変更するには、［**Advanced**］タブを選択します。
7. ［**OK**］を選択してリカバリを開始します。

ディレクトリ レプリケーション ペア データのリカバリ

ディレクトリ レプリケーション ペア データを正常にリカバリするためには、元のコンテキストで使用されていたのと同じディレクトリを作成し、空のままにしておく必要があります。

手順

1. ［**More**］ > ［**Start Recover**］を選択して、［Start Recover］ダイアログを表示します。
2. ［**Replication Type**］メニューから、［**Directory**］を選択します。
3. ［**System to recover to**］メニューから、［データをリストアする必要があるシステム］のホスト名を選択します。
4. ［**System to recover from**］メニューから、［データ ソースとなるシステム］のホスト名を選択します。
5. コンテキスト リストからリストアするコンテキストを選択します。
6. ホスト接続の設定を変更するには、［**Advanced**］タブを選択します。
7. ［**OK**］を選択してリカバリを開始します。

レプリケーション ペア リカバリの中止

レプリケーション ペア リカバリが失敗したか、終了する必要がある場合は、レプリケーション リカバリを停止できます。

手順

1. ［More］メニューを選択し、［**Abort Recover**］を選択して、現在リカバリを実行中のコンテキストが表示される［Abort Recover］ダイアログを表示します。
2. リストから中止する 1 つ以上のコンテキストのチェックボックスを選択します。
3. ［**OK**］を選択します。

必要条件

できるだけ早く、ソースのリカバリを再開する必要があります。

MTree、ディレクトリ、プール レプリケーション ペアの再同期

［再同期］とは、手動の中断後、ソースとデスティネーションのレプリケーション ペア間でデータをリカバリする（または同期状態に戻す）処理のことです。レプリケーション ペアは、両方のエンド ポイントに同じデータが含まれるように再同期されます。再同期は、MTree、ディレクトリ、プール レプリケーションには使用できますが、コレクション レプリケーションには使用できません。

レプリケーション再同期は、次の場合にも使用できます。

- 削除されているコンテキストの再作成する場合。
- デスティネーションでスペースが不足しているが、まだソース システムにレプリケートするデータがある場合。
- ディレクトリ レプリケーション ペアを MTree レプリケーション ペアに変換する場合。

手順

1. レプリケーション ソースとレプリケーション デスティネーション システムの両方でコンテキストを削除する必要があります。
2. レプリケーション ソースまたはレプリケーション デスティネーション システムのどちらかから、［**More**］ > ［**Start Resync**］を選択して、［Start Resync］ダイアログを表示します。
3. 再同期するレプリケーション タイプを ［**Directory**］、［**MTree**］、［**Pool**］の中から選択します。
4. ［**Source System**］メニューからレプリケーション ソース システムのホスト名を選択します。
5. ［**Destination System**］メニューからレプリケーション デスティネーション システムのホスト名を選択します。
6. ［**Source Path**］テキスト ボックスにレプリケーション ソース パスを入力します。
7. ［**Destination Path**］テキスト ボックスにレプリケーション宛先パスを入力します。
8. ホスト接続の設定を変更するには、［**Advanced**］タブを選択します。
9. ［**OK**］を選択します。

［**CLI** 相当］

```
# replication resync destination
```

レプリケーション ペアの再同期の中止

レプリケーション ペアの再同期が失敗したか、終了する必要がある場合は、再同期を停止できます。

手順

1. レプリケーション ソースまたはレプリケーション デスティネーション システムのどちらかから、［**More**］ > ［**Abort Resync**］を選択して［Abort Resync］ダイアログを表示します。このダイアログには、現在再同期を実行中のすべてのコンテキストがリストされます。
2. 再同期を中止する 1 つ以上のコンテキストのチェックボックスを選択します。
3. ［**OK**］を選択します。

［DD Boost］ビュー

［DD Boost］ビューは、DD Boost AIR（自動イメージ レプリケーション）、または管理対象ファイル レプリケーションを使用する DD Boost アプリケーションを使用するように DD システムを構成した NetBackup 管理者に、構成およびトラブルシューティングの情報を提供します。

DD Boost AIR の構成手順については、「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。

［**File Replication**］タブには、次の情報が表示されます。

- Currently Active File Replication：
  - 方向（Out-Going と In-Coming）とそれぞれのファイル数。
  - 残りのレプリケーション対象データ（GiB 単位の圧縮前値）とレプリケーション済みのデータの量（GiB 単位の圧縮前値）。
  - Total size：レプリケーション対象データとレプリケーション済みのデータの量の量（GiB 単位の圧縮前値）。
- Most Recent Status：合計ファイル レプリケーションと完了したかどうか

- 過去 1 時間
- 過去 24 時間

- Remote Systems：
  - リストからレプリケーションを選択します。
  - メニューからカバーする期間を選択します。
  - これらのリモート システム ファイルの詳細を確認するには、［**Show Details**］をクリックします。

［**Storage Unit Associations**］タブには、次の情報が表示されます。これは、監査目的またはストレージ ユニットのイメージ レプリケーションに使用される DD Boost AIR イベントのステータスのチェックに使用できます。

- システムが認識しているすべてのストレージ ユニットの［**Associations**］のリスト。ソースは左側、デスティネーションは右側にあります。この情報は、Data Domain システム上の AIR の構成を示します。
- ［**Event Queue**］は保留中のイベント リストです。ローカル ストレージ ユニット、イベント ID、イベントのステータスが表示されます。

ペアを形成するよう DD Boost パスの両側に一致させ、それを 1 つのペア/レコードとして提示します。何かしらの理由で一致させることが不可能な場合、そのリモート パスは［Unresolved］としてリストされます。

リモート システム ファイル

［Show Details］ボタンを押すと、選択したリモート ファイル レプリケーション システムの情報が表示されます。［File Replications］には、選択されたリモート ファイル レプリケーション システムの開始および終了情報に加え、サイズとデータ量が表示されます。［Performance Graph］には、選択されたリモート ファイル レプリケーション システムの一定期間中のパフォーマンスが表示されます。

表 194 ファイル レプリケーション

項目	説明
Start	期間の開始点。
End	期間の終了点。
File Name	特定のレプリケーション ファイルの名前。
Status	直近のステータス（Success、Failure）。
Pre-Comp Size (MiB)	ネットワーク スループットまたは圧縮後のデータと比較した圧縮前のアウトバウンドおよびインバウンド データの量（MiB 単位）。
Network Bytes (MiB)	ネットワーク スループット データの量（MiB 単位）。

表 195 Performance Graph

項目	説明
Duration	レプリケーションの所要時間（1d、7d、または 30d）。
Interval	レプリケーションの間隔（Daily または Weekly）。
Pre-Comp Replicated	圧縮前のアウトバウンドおよびインバウンド データの量（GiB 単位）。
Post-Comp Replicated	圧縮後のデータの量（GiB 単位）。

表 195 Performance Graph （続き）

項目	説明
Network Bytes	ネットワーク スループット データの量（GiB 単位）。
Files Succeeded	正常にレプリケーションされたファイルの数。
Files Failed	レプリケーションに失敗したファイルの数。
Show in new window	別のウィンドウを起動します。
Print	グラフを印刷します。

パフォーマンス ビュー

［Performance］ビューには、レプリケーション中のデータの変動を表すグラフが表示されます。それらは、DD システムの各レプリケーション ペアの集約された統計です。

- ［**Duration**］（x 軸）はデフォルトでは 30 日です。
- ［**Replication Performance**］（y 軸）は、ギビバイト数またはメビバイト数（ギガバイトとメガバイトのバイナリ相当）です。
- ［**Network In**］は、システムに入力されるレプリケーション ネットワークの総バイト数（全コンテキスト）です。
- ［**Network Out**］は、システムから出力されるレプリケーション ネットワークの総バイト数（全コンテキスト）です。
- 特定の時点を確認する場合は、カーソルをグラフ上の場所に移動します。
- 非アクティブ時間（転送されているデータがない時間）の間は、グラフの形状は、想定される急な下降線ではなく、緩やかな下降線で表示される場合があります。

［Advanced Settings］ビュー

［Advanced Settings］では、スロットルおよびネットワーク設定を管理できます。

［**Throttle Settings**］

- ［**Temporary Override**］：スロットル レート（構成されている場合）または 0（すべてのレプリケーション トラフィックが停止していることを示す）が表示されます。
- ［**Permanent Schedule**］：スケジュール設定されたスロットルが実行される曜日と時刻が表示されます。

［ネットワーク設定］

- ［**Bandwidth**］：帯域幅が構成されている場合は、構成されたデータ ストリーム レート、帯域幅が構成されていない場合は、Unlimited（デフォルト）が表示されます。レプリケーション デスティネーションへの平均データ ストリームは、最低 1 秒あたり 98,304 ビット（12 KiB）です。
- ［**Delay**］：ネットワーク遅延の設定が構成されている場合は、構成された設定（ミリ秒単位）、構成されていない場合は、None（デフォルト）が表示されます。
- ［**Listen Port**］：リスン ポートの値が構成されている場合は、構成された値、構成されていない場合は、2051（デフォルト）が表示されます。

スロットル設定の追加

レプリケーション用にネットワークが使用する帯域幅の量を変更するために、レプリケーション トラフィックの［レプリケーション スロットル］を設定できます。

レプリケーション スロットル設定には、次の 3 つのタイプがあります。

- ［**Scheduled throttle**］：事前定義された時間または期間のスロットル レートが設定されます。
- ［**Current throttle**］：次にスケジュール設定された変更時またはシステム再起動時までのスロットル レートが設定されます。
- ［**Override throttle**］：前述の 2 タイプのスロットルがオーバーライドされます。これは、［**Clear Throttle Override**］を選択するか、`replication throttle reset override` コマンドを発行するまで、（再起動後）も継続します。

次のように、デフォルト スロットルまたは特定の宛先のスロットルも設定できます。

- ［**Default throttle**］：これが設定されると、宛先スロットルによって指定された宛先を除き、すべてのレプリケーション コンテキストがこのスロットルに限定されます（次の項目を参照してください）。
- ［**Destination throttle**］：調整する必要がある宛先が数箇所しかない場合、または宛先がデフォルト スロットルとは異なるスロットル設定を必要としている場合、このスロットルが使用されます。デフォルト スロットルがすでに存在する場合、このスロットルが指定された宛先のスロットルよりも優先されます。たとえば、デフォルト レプリケーション スロットルを［10 kbps］に設定し、宛先スロットルを使用して、単一のコレクション レプリケーション コンテキストを［unlimited］に設定することができます。

注

現在は、宛先スロットルの設定と変更は、CLI（コマンドライン インターフェイス）でのみ可能です。この機能は、DD System Manager では使用できません。この機能の詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」の `replication throttle` コマンドを参照してください。DD System Manager が、1 つ以上の宛先スロットル セットがあることを検出した場合、警告が出され、進めるには CLI を使用する必要があります。

レプリケーション スロットリングに関する追加の注

- スロットルはソースにのみ設定されます。宛先に適用されるスロットルは、すべてのレプリケーション トラフィックを無効化する［**0 Bps (Disabled)**］オプションのみです。
- レプリケーション スロットルの最小値は、1 秒あたり 98,304 ビットです。

手順

1. ［**Replication**］ > ［**Advanced Settings**］ > ［**Add Throttle Setting**］を選択して、［Add Throttle Setting］ダイアログを表示します。
2. ［**Every Day**］または各日付の隣にあるチェックボックスを選択して、スロットリングがアクティブになる曜日を設定します。
3. スロットリングが［**Start Time**］ドロップダウン セレクターから開始される時間を hour:minute および AM/PM 形式で設定します。
4. ［**Throttle Rate**］の場合：
   - ［**Unlimited**］を選択して、制限がないように設定します。

- テキスト ボックスに数値（たとえば、20000）を入力し、メニューからレート（bps、Kbps、Bps、KBps）を選択します。
- ［**0 Bps (disabled)**］オプションを選択して、すべてのレプリケーション トラフィックを無効にします。

5. ［**OK**］を選択して、スケジュールを設定します。新しいスケジュールが、［**Permanent Schedule**］に表示されます。

結果

レプリケーションは、次のスケジュール設定された変更時または新しいスロットル設定による強制変更時まで、指定されたレートで実行されます。

スロットル設定の削除

単一のスロットル設定または同時にすべてのスロットル設定を削除できます。

手順

1. ［**Replication**］ > ［**Advanced Settings**］ > ［**Delete Throttle Setting**］を選択して、［Delete Throttle Setting］ダイアログを表示します。
2. 削除するスロットル設定のチェックボックスを選択するか、すべての設定を削除する見出しチェックボックスを選択します。このリストには、「disabled」状態の設定を含めることができます。
3. ［**OK**］を選択して、設定を削除します。
4. ［Delete Throttle Setting Status］ダイアログ ボックスで、［**Close**］を選択します。

スロットル設定の一時的なオーバーライド

スロットル オーバーライドは、一時的にスロットル設定を変更します。現在の設定は、ウィンドウの最上部にリストされます。

手順

1. ［**Replication**］ > ［**Advanced Settings**］ > ［**Set Throttle Override**］を選択して、［Throttle Override］ダイアログを表示します。
2. 新しいスロットル オーバーライドを設定するか、前のオーバーライドをクリアします。
   a. 新しいスロットル オーバーライドを設定する手順：
      - ［**Unlimited**］を選択して、システム設定スロットル レート（スロットルが実行されない）に戻す。または、
      - テキスト ボックスにスロットリング ビット（例えば、20000）およびレート（bps、Kbps、Bps、KBps）を選択します。
      - ［**0 Bps (Disabled)**］を選択して、スロットル レートを 0 に設定することで、効果的にすべてのレプリケーション ネットワーク トラフィックを停止できます。
      - 変更を一時的に適用するには、［**Clear at next scheduled throttle event**］を選択します。

   b. 前に設定したオーバーライドをクリアするには、［**Clear Throttle Override**］を選択します。
3. ［**OK**］を選択します。

ネットワーク設定の変更

帯域幅とネットワーク遅延設定を同時に使用して、レプリケーションはレプリケーションで使用するのに適切な TCP（Transmission Control Protocol）バッファー サイズを計算します。これらのネッ

トワーク設定は、DD システムに対してグローバルであり、システムごとに 1 回だけ設定する必要があります。

次の点に注意してください。

- `ping` コマンドを使用して、実際の帯域幅と実際のネットワーク遅延値を決定します。
- リストア作業におけるデフォルトのネットワーク パラメーターは、レーテンシー ラウンド トリップ時間（`ping` コマンドで測定）が通常 1 ミリ秒未満であるローカル 100Mbps または 1000Mbps Ethernet ネットワークなど、低レーテンシー構成でのレプリケーションに適しています。デフォルトは、レーテンシーが最高で 50～100 ミリ秒である低帯域幅から中帯域幅の WAN を介したレプリケーションにも適しています。ただし、高帯域幅高レーテンシー ネットワークの場合、ネットワーク パラメーターを多少調整する必要があります。
  調整すべき主な数字は、ネットワークの帯域幅とラウンドトリップ レーテンシーを掛けて計算される帯域幅遅延の数字です。この数字は、相手側から確認が返されるまでにネットワーク経由で送信できるデータ量の測定値です。レプリケーション ネットワークの帯域幅遅延の数字が 100,000 より大きい場合、両方のリストアを実行しているシステムのネットワーク パラメーターを設定すると、レプリケーション パフォーマンスが向上します。

手順

1. ［**Replication**］ > ［**Advanced Settings**］ > ［**Change Network Settings**］を選択して、［Network Settings］ダイアログを表示します。
2. ［Network Settings］領域で、［**Custom Values**］を選択します。
3. テキスト ボックスに［**Delay**］と［**Bandwidth**］の値を入力します。ネットワーク遅延設定はミリ秒単位、帯域幅は 1 秒あたりのバイト数単位です。
4. ［Listen Port］領域のテキスト ボックスに新しい値を入力します。レプリケーション ソースからデータ ストリームを受信するレプリケーション デスティネーションのデフォルトの IP リスン ポートは 2051 です。これは、DD システムのグローバル設定です。
5. ［**OK**］を選択します。新しい設定が、［Network Settings］テーブルに表示されます。

レプリケーションのモニタリング

DD System Manager には、レプリケーション ペアのステータスの確認から、バックアップ ジョブのトラッキング、パフォーマンスの確認、レプリケーション プロセスのトラッキングまで、レプリケーションのステータスをトラッキングする方法が複数あります。

バックアップ ジョブの推定完了時間の表示

Completion Predictor を使用して、バックアップ レプリケーション ジョブの推定完了時間を確認できます。

手順

1. ［**Replication**］ > ［**Summary**］を選択します。
2. ［Detailed Information］を表示する Replication コンテキストを選択します。
3. ［Completion Predictor］領域で、レプリケーション完了時刻の［**Source Time**］ドロップダウン リストからオプションを選択し、［**Track**］を選択します。

   ［Completion Time］領域に、特定のバックアップ ジョブによるデスティネーションへのレプリケーションが終了する推定時間が表示されます。レプリケーションが終了すると、この領域に `Completed` と表示されます。

レプリケーション コンテキストのパフォーマンスのチェック

一定期間中のレプリケーション コンテキストのパフォーマンスをチェックするには、［Summary］ビューで Replication コンテキストを選択し、［Detailed Information］領域で［**Performance Graph**］を選択します。

レプリケーション進行状態のステータス追跡

レプリケーション初期化、再同期、リカバリ操作の進行状況を表示するには、［**Replication**］ > ［**Summary**］ビューを使用して、現在の状態を確認します。

CLI 相当機能

```
# replication show config all
CTX  Source                                    Destination
Connection Host and Port     Enabled
---  ------------------------        ------------------------        ------------------------
-------
1       dir://host2/backup/dir2     dir://host3/backup/dir3
host3.company.com               Yes
2       dir://host3/backup/dir3     dir://host2/backup/dir2
host3.company.com               Yes
```

IP バージョンを指定する場合は、次のコマンドを使用して、その設定を確認します。

```
# replication show config rctx://2

CTX:                          2
Source:                       mtree://ddbeta1.dallasrdc.com/data/col1/EDM1
Destination:                  mtree://ddbeta2.dallasrdc.com/data/col1/EDM_ipv6
Connection Host:              ddbeta2-ipv6.dallasrdc.com
Connection Port:              (default)
Ipversion:                    ipv6
Low-bw-optim:                 disabled
Encryption:                   disabled
Enabled:                      yes
Propagate-retention-lock:     enabled
```

レプリケーション ラグ

データの 2 コピー間にある時間の長さは、レプリケーション ラグと呼ばれます。

replication status コマンドを使用して、2 つのコンテキスト間のレプリケーション ラグを測定できます。レプリケーション ラグの原因を特定し、その影響を軽減する方法については、KB 記事「Troubleshooting Replication Lag」（https://support.emc.com/kb/180482）を参照してください。

レプリケーションと HA

フローティング IP アドレスでは、HA システムで、HA ペアのどのノードがアクティブであるかに関係なく動作するレプリケーション構成用の単一の IP アドレスを指定できます。

IP ネットワークを介した HA システムは、どちらの物理ノードがアクティブ ノードであるかに関係なく、フローティング IP アドレスを使用して、Data Domain HA ペアへのデータ アクセスを提供します。net config コマンドには、フローティング IP アドレスを構成する **[type {fixed | floating}]** オプションがあります。詳細は、「Data Domain Operating System コマンド リファレンス ガイド」に記載されています。

フローティング IP アドレスにアクセスするためにドメイン名を必要とする場合は、ドメイン名として HA システム名を指定します。`ha status` コマンドを実行して HA システム名を見つけます。

注

`net show hostname type ha-system` コマンドを実行して、HA システム名を表示し、必要な場合は、`net set hostname ha-system command` を実行して HA システム名を変更します。

ファイル システム アクセスはすべて、フローティング IP アドレス経由で行う必要があります。HA ペアでのバックアップおよびレプリケーション オペレーションを構成するときは、Data Domain システムの IP アドレスとして常にフローティング IP アドレスを指定します。DD Boost、レプリケーションなどの Data Domain の機能では、非 HA システムのシステム IP アドレスを受け入れるときと同じように、HA ペアのフローティング IP アドレスを受け入れます。

HA システムと非 HA システム間のレプリケーション

HA（高可用性）システムと、DD OS 5.7.0.3 以前を実行しているシステムの間のレプリケーションを設定する場合、DD System Manager の GUI（グラフィカル ユーザー インターフェイス）を使用するには、そのレプリケーションを HA システム上に作成して管理する必要があります。

ただし、CLI を使用すれば、HA システムから非 HA システムへのレプリケーションも、非 HA システムから HA システムへのレプリケーションも実行できます。

HA システムと非 HA システム間のコレクション レプリケーションはサポートされません。HA システムと非 HA システム間でデータをレプリケートするには、ディレクトリまたは MTree レプリケーションが必要です。

クォータのあるシステムからクォータのないシステムへのレプリケーション

クォータに対応している DD OS のある Data Domain システムを、クォータがない DD OS のあるシステムにレプリケーションします。

- 逆再同期。クォータのないシステムからデータを取得し、クォータが有効化されているシステム上の MTree にそれを置く（クォータは有効化の状態が続く）
- クォータのないシステムからの逆初期化。クォータに対応しているシステムでデータを取得し、新しい MTree を作成するが、クォータのないシステムでデータから作成されたため、クォータは有効化されていない。

注

クォータは、DD OS 5.2 で導入されました。

レプリケーション スケーリング コンテキスト

レプリケーション スケーリング コンテキスト機能は、より柔軟なレプリケーション コンテキストの構成を可能にします。

ディレクトリと MTree 両方のレプリケーション コンテキストを含めて 299 を超えるレプリケーション コンテキストがある環境では、この機能によってどのような順番でもコンテキストを構成できます。これまでは、ディレクトリ レプリケーション コンテキストを先に、その後 MTree レプリケーション コンテキストを構成する必要がありました。

レプリケーション コンテキストの合計数は、540 を超えることはできません。

注

この機能は、DD OS バージョン 6.0 を実行している Data Domain システムでのみ表示されます。

ディレクトリから MTree へのレプリケーションの移行

ディレクトリから MTree（D2M）へのレプリケーション最適化機能を使用すると、ファイル システムの論理パーティションである Mtree に基づいて、既存のディレクトリ レプリケーション コンテキストを新しいレプリケーション コンテキストに移行できます。この機能を使用すると、このプロセスを監視し、正常に完了したことを確認することもできます。

D2M 機能は、Data Domain Operating System バージョン 6.0、5.6、5.7 と互換性があります。

この機能を使用するには、ソース Data Domain システムが DD OS 6.0 を実行している必要がありますが、デスティネーション システムは 6.0、5.6、5.7 を実行できます。ただし、パフォーマンス最適化のメリットは、ソースとデスティネーションの両方のシステムが 6.0 を実行している場合にのみ得られます。

注

この操作にはグラフィカル ユーザー インターフェイス（GUI）を使用できますが、最適なパフォーマンスを実現するためにコマンド ライン インターフェイス（CLI）を使用することをお勧めします。

ディレクトリ レプリケーションから MTree レプリケーションへの移行の実行

ディレクトリから MTree（D2M）への移行中は、システムをシャットダウンまたは再起動しないでください。

手順

1. ディレクトリ レプリケーションのソース ディレクトリへの取得操作をすべて停止します。
2. ソース DD システムで MTree を作成します。**`mtree create /data/col1/mtree-name`**

   注

   デスティネーション DD システムでは MTree を作成しないでください。

3. （オプション）MTree で DD Retention Lock を有効化します。

   注

   ソース システムに保存ロックされたファイルが含まれている場合、新しい MTree で DD Retention Lock を維持できます。

   MTree における DD Retention Lock Compliance の有効化を参照してください。
4. ソースとデスティネーションの両方の DD システムで、MTree レプリケーション コンテキストを作成します。**`replication add source mtree://source-system-name/source mtree replication add destination mtree://destination-system-name/destination mtree`**
5. D2M 移行を開始します。**`replication dir-to-mtree start from rctx://1 to rctx://2`**

   上記の例で、
   `rctx://1`
   は、ソース システムのディレクトリ `backup backup/dir1` をレプリケートするディレクトリ レプリケーション コンテキストを表します。
   `rctx://2`

は、ソース システムの MTree `/data/col1/mtree1` をレプリケートする MTree レプリケーション コンテキストを表します。

注

このコマンドは、完了するまで予想以上に時間がかかる場合があります。このプロセス中に Ctrl + C キーを押さないでください。押した場合は、D2M 移行がキャンセルされます。

```
Phase 1 of 4 (precheck):
    Marking source directory /backup/dir1 as read-only...Done.

Phase 2 of 4 (sync):
    Syncing directory replication context...0 files flushed.
current=45 sync_target=47 head=47
current=45 sync_target=47 head=47
Done. (00:09)

Phase 3 of 4 (fastcopy):
    Starting fastcopy from /backup/dir1 to /data/col1/
mtree1...
    Waiting for fastcopy to complete...(00:00)
    Fastcopy status: fastcopy /backup/dir1 to /data/col1/
mtree1: copied 24
files, 1 directory in 0.13 seconds
    Creating snapshot 'REPL-D2M-
mtree1-2015-12-07-14-54-02'...Done

Phase 4 of 4 (initialize):
    Initializing MTree replication context...
(00:08) Waiting for initialize to start...
(00:11) Initialize started.

Use 'replication dir-to-mtree watch rctx://2' to monitor
progress.
```

ディレクトリから MTree への移行の進行状況の表示

D2M（directory-to-MTree）レプリケーションで、現在進行中の移行のステージを表示できます。

手順

1. 進行状況を表示するには、「**`replication dir-to-mtree watch rctx://2`**」と入力します。

   「
   `rctx://2`
   」はレプリケーション コンテキストを指定します。

   次の出力が表示されます。

```
Use Control-C to stop monitoring.
Phase 4 of 4 (initialize).
(00:00) Replication initialize started...
(00:02) initializing:
(00:14)     100% complete, pre-comp: 0 KB/s, network: 0 KB/
s
(00:14) Replication initialize completed.
Migration for ctx 2 successfully completed.
```

ディレクトリから MTree へのレプリケーションの移行ステータスの確認

`replication dir-to-mtree status` コマンドを使用すると、ディレクトリから MTree への移行（D2M）が正常に完了したかどうかをチェックできます。

手順

1. 次のコマンドを入力します。ここで、
   `rctx://2`
   はソース システム上の MTree レプリケーション コンテキストを表します。**`replication dir-to-mtree status rctx://2`**

   出力は次のようになります。

   ```
   Directory Replication CTX:          1
   MTree Replication CTX:              2
   Directory Replication Source:       dir://127.0.0.2/backup/dir1
   MTree Replication Source:           mtree://127.0.0.2/data/
   col1/mtree1
   MTree Replication Destination:      mtree://127.0.0.3/data/
   col1/mtree1
   Migration Status:                   completed
   ```

   進行中の移行がない場合は、次のように表示されます。

   ```
   # replication dir-to-mtree status rctx://2
   No migration status for context 2.
   ```

2. 移行プロセスが完了すると、ソース DD システム上の MTree へのデータの取得を開始します。
3. （オプション）ソースおよびターゲット システム上のディレクトリ レプリケーション コンテキストを破棄します。

   `replication break` コマンドの詳細については、「Data Domain Operating System バージョン 6.0 コマンド リファレンス ガイド」を参照してください。

D2M レプリケーションの中止

必要な場合は、ディレクトリから MTree（D2M）への移行手順を中止することができます。

`replication dir-to-mtree abort` コマンドを使用すると、実行中の移行プロセスが中止され、ディレクトリが読み取り専用から読み取り/書き込み状態に戻ります。

手順

1. コマンド ライン インターフェイス（CLI）で、次のコマンドを入力します。
   `rctx://2`
   は MTree レプリケーション コンテキストです。**`replication dir-to-mtree abort rctx://2`**

   次のような出力が表示されます。

   ```
   Canceling directory to MTree migration for context dir-name.
   Marking source directory dir-name as read-write...Done.
   The migration is now aborted.
   Remove the MTree replication context and MTree on both source
   ```

```
and destination
host by running 'replication break' and 'mtree delete'
commands.
```

2. MTree レプリケーション コンテキストを破棄します。**replication break rctx://2**
3. ソース システム上の MTree を削除します。**mtree delete mtree-path**

D2M のトラブルシューティング

ディレクトリから MTree（D2M）へのレプリケーションの設定に問題が発生した場合は、次の処理手順を実行することでさまざまな問題に対応できます。

`dir-to-mtree abort` 処理手順を使用すると、D2M プロセスを正常に中止できます。この処理手順は、次の場合に実行する必要があります。

- D2M 移行のステータスが中止として表示されている。
- D2M 移行中に Data Domain システムが再起動した。
- `replication dir-to-mtree start` コマンドの実行中にエラーが発生した。
- 移行を開始する前に取得を停止しなかった。
- `replication dir-to-mtree start` コマンドを入力する前に MTree レプリケーション コンテキストが初期化された。

注

D2M プロセスが完了する前に MTree レプリケーション コンテキストで **replication break** を実行しないでください。
mrepl コンテキストで **replication break** コマンドを実行する前に、常に **replication dir-to-mtree abort** を実行してください。

replication break コマンドを誤って早期に実行すると、drepl ソース ディレクトリが永続的に読み取り専用に設定されます。

このような場合は、サポートに問い合わせてください。

手順

1. **replication dir-to-mtree abort** と入力してプロセスを中止します。
2. ソースとデスティネーションの両方の Data Domain システムで、新しく作成した MTree レプリケーション コンテキストを破棄します。

   次の例では、MTree レプリケーション コンテキストは `rctx://2` です。

   ```
   replication break rctx://2
   ```

3. ソースとデスティネーションの両方のシステムで、対応する Mtree を削除します。

   ```
   mtree delete mtree-path
   ```

注

削除対象としてマークされた MTree は、`filesys clean` コマンドが実行されるまで、ファイル システムに留まります。

詳細については、「Data Domain Operating System バージョン 6.0 コマンド リファレンス ガイド」を参照してください。

4. ソース システムとデスティネーション システムの両方で `filesys clean start` コマンドを実行します。

   `filesys clean` コマンドの詳細については、「Data Domain Operating System バージョン 6.0 コマンド リファレンス ガイド」を参照してください。

5. プロセスを再起動します。

   詳細については、ディレクトリ レプリケーションから MTree レプリケーションへの移行の実行を参照してください。

D2M のトラブルシューティング（追加）

新しい MTree に対して DD Retention Lock を有効化するのを忘れた場合、またはディレクトリから MTree への移行が初期化された後にエラーが発生した場合は、いくつかの解決策があります。

DD Retention Lock が有効化されていない

新しい MTree に対して DD Retention Lock を有効化するのを忘れ、ソース ディレクトリに保存ロックされたファイルまたはディレクトリが存在する場合は、次のオプションがあります。

- D2M 移行を続行します。ただし、移行後の MTree に DD Retention Lock 情報はありません。
- D2M レプリケーションの中止 （460 ページ）に従って現在の D2M プロセスを中止し、ソース MTree で DD Retention Lock を有効化してからプロセスを再実行します。

初期化後にエラーが発生する

`replication dir-to-mtree start` プロセスがエラーなしで完了する一方で、MTree レプリケーションの初期化中（D2M 移行プロセスのフェーズ 4）にエラーが発生した場合は、次の手順を実行できます。

1. ネットワークの問題がないことを確認します。
2. MTree レプリケーション コンテキストを初期化します。

ディザスタリカバリ用コレクション レプリケーションおよび SMT の使用

ディザスタリカバリのリプレース システムとして SMT で構成されているコレクション レプリケーション ペアのデスティネーション システムを使用するには、リプレース システムをオンラインにするために必要なその他の構成ステップに加えて、追加の SMT 構成手順を実行する必要があります。

はじめに

この方法でコレクション レプリケーションのデスティネーション システムを使用するには、オートサポート レポートが構成され、保存されている必要があります。KB 記事「Collection replica with smt enabled」（https://support.emc.com で利用可能）に追加情報が記載されています。

リプレース システムは、次の SMT の詳細を持たないようになります。

- テナント ユニットごとのアラート通知リスト

- SMT テナントが使用する、DD Boost プロトコルに割り当てられているすべてのユーザー（システムで DD Boost が構成されている場合）
- 各 DD Boost ユーザーに関連づけられているデフォルトのテナント ユニット（システムで DD Boost が構成されており、関連づけられている場合）

リプレース システム上で SMT を構成するには、次の手順を実行します。

手順

1. オートサポート レポートで、`smt tenant-unit show detailed` コマンドの出力を検索します。

```
Tenant-unit: "tu1"
Summary:
Name   Self-Service   Number of Mtrees   Types           Pre-Comp(GiB)
----   ------------   ----------------   --------        -------------
tu1    Enabled        2                  DD Boost        2.0
----   ------------   ----------------   --------        -------------

Management-User:
User     Role
------   ------------
tu1_ta   tenant-admin
tu1_tu   tenant-user
tum_ta   tenant-admin
------   ------------

Management-Group:
Group    Role
------   ------------
qatest   tenant-admin
------   ------------

DDBoost:
Name   Pre-Comp (GiB)   Status   User    Tenant-Unit
----   --------------   ------   -----   -----------
su1               2.0   RW/Q     ddbu1   tu1
----   --------------   ------   -----   -----------
Q    : Quota Defined
RO   : Read Only
RW   : Read Write

Getting users with default-tenant-unit tu1
DD Boost user   Default tenant-unit
-------------   -------------------
ddbu1           tu1
-------------   -------------------

Mtrees:
Name              Pre-Comp (GiB)   Status   Tenant-Unit
--------------    --------------   ------   -----------
/data/col1/m1                0.0   RW/Q     tu1
/data/col1/su1               2.0   RW/Q     tu1
--------------    --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

Quota:
Tenant-unit: tu1
Mtree             Pre-Comp (MiB)   Soft-Limit (MiB)   Hard-Limit(MiB)
--------------    --------------   ----------------   ----------------
/data/col1/m1                  0              71680             81920
/data/col1/su1              2048              30720             51200
--------------    --------------   ----------------   ----------------
```

```
Alerts:
Tenant-unit: "tu1"
Notification list "tu1_grp"
Members
------------------
tom.tenant@abc.com
------------------

No such active alerts.
```

2. リプレース システム上で、SMT がまだ有効になっていない場合は有効化します。
3. リプレース システム上で、DD Boost が必要でまだ有効になっていない場合は DD Boost をライセンス許可し、有効化します。
4. DD Boost が構成されている場合、「**smt tenant-unit show detailed**」出力の `DD Boost` セクションに記載されている各ユーザーを DD Boost ユーザーとして割り当てます。

   ```
   # ddboost user assign ddbu1
   ```

5. DD Boost が構成されている場合、デフォルト テナント ユニットが出力にあれば、`smt tenant-unit show detailed` 出力の `DD Boost` セクションに記載されている各ユーザーをデフォルト テナント ユニットに割り当てます。

   ```
   # ddboost user option set ddbu1 default-tenant-unit tu1
   ```

6. `smt tenant-unit show detailed` 出力の `Alerts` セクションにあるアラート通知グループと同じ名前で新しいアラート通知グループを作成します。

   ```
   # alert notify-list create tu1_grp tenant-unit tu1
   ```

7. `smt tenant-unit show detailed` 出力の `Alerts` セクションにあるアラート通知グループ内の各メール アドレスを新しいアラート通知グループに割り当てます。

   ```
   # alert notify-list add tu1_grp emails tom.tenant@abc.com
   ```

第 17 章

DD Secure Multitenancy

本章には、次のセクションが含まれます。

- Data Domain Secure Multitenancy の概要 466
- テナント ユニットのプロビジョニング 469
- テナント セルフサービス モードの有効化 473
- プロトコルによるデータ アクセス 473
- データ管理操作 475

Data Domain Secure Multitenancy の概要

Data Domain ［SMT（Secure Multitenancy）］とは、内部 IT 部門または外部プロバイダーが、複数の消費者やワークロード（ビジネスユニット/部門/テナント）向けの IT インフラストラクチャを同時にホスティングすることを指します。

SMT により共有インフラストラクチャ内の多くのユーザーと作業負荷を安全に分離できるため、あるテナントのアクティビティが別のテナントに表示されることがなくなります。

［テナント］は、ホストされる環境に永続的に存在する消費者（事業部/部門/顧客）です。

エンタープライズ内では、テナントは、IT スタッフが構成および管理する Data Domain システム上の 1 個以上の事業部または部門で構成されます。

- BU（事業部）の使用事例では、ある企業の財務部と人事部が同じ Data Domain システムを共有できましたが、それぞれの部門は相手方の存在は認識していませんでした。
- サービス プロバイダー（SP）の使用事例では、SP は 1 個以上の Data Domain システムを展開し、複数のエンド カスタマーに対するさまざまな Protection Storage サービスを収容できました。

両使用事例では、同じ物理 Data Domain システム上での異なる顧客データの区別を強調しています。

SMT アーキテクチャの基本

SMT（Secure Multitenancy）は、MTree を使用してテナントとテナント ユニットを構成する簡単なアプローチを提供します。SMT 構成は、DD Management Center や DD OS コマンド ライン インターフェイスを使用して実行されます。この管理ガイドでは、SMT といくつかの一般的なコマンド ラインの手順の原理を説明します。

SMT の基本アーキテクチャは次のとおりです。

- テナントは DD Management Center や DD システムで作成されます。
- テナント ユニットは、そのテナントの DD システムで作成されます。
- 1 つまたは複数の MTree を作成して、テナントのさまざまなタイプのバックアップに対するストレージ要件を満たします。
- 新規に作成された MTree がテナント ユニットに追加されます。
- バックアップ アプリケーションを構成して、構成済みのテナント ユニット MTree への各バックアップを送信します。

注

DD Management Center の詳細については、「DD Management Center ユーザー ガイド」を参照してください。DD OS コマンド ライン インターフェイスの詳細については、「DD OS コマンド リファレンス」を参照してください。

SMT（Secure Multi-Tenancy）で使用される用語

SMT で使用される用語を理解すると、この独自の環境をよりよく理解できるようになります。

MTree

［MTree］は、ファイル システムの論理パーティションであり、高い管理粒度を提供します。それによって、ユーザーはファイル システム全体に影響を与えることなく特定の MTree 上で操作を実行できます。MTree は、テナント ユニットに割り当てられ、SMT の管理と監視のテナント ユニット個別の設定を含みます。

マルチテナンシー
［マルチテナンシー］とは、同時に複数の消費者/作業負荷（ビジネスユニット/部門/テナント）をカバーする、内部 IT 部門または外部サービス プロバイダーによる IT インフラストラクチャのホスティングを指します。Data Domain SMT は、［サービスとしてのデータ保護］に対応しています。

RBAC（役割に基づいたアクセス制御）
［RBAC］は、マルチテナント Data Domain システムで管理分離を行うため、組み合わせて使用する、複数の権限レベルのある複数の役割を提供します（次のセクションでは、こうした役割を定義します）。

Storage Unit
［Storage Unit］は、DD Boost プロトコル用に構成された MTree です。データ分離は、ストレージ ユニットを作成し、それを DD Boost ユーザーに割り当てることで行われます。DD Boost プロトコルは、Data Domain システムに接続された DD Boost ユーザーに割り当てられたストレージ ユニットにのみアクセスを許可します。

テナント
［テナント］は、ホストされる環境に永続的に存在する消費者（事業部/部門/顧客）です。

Tenant Self-Service
［テナント セルフ サービス］は、テナントを Data Domain システムにログインさせて、一部の基本サービス（ローカル ユーザー、NIS グループ、AD グループの追加、編集、削除）を実行する方法です。これによって、こうした基本タスクの管理者が常に経験するボトルネックを削減します。テナントは、割り当てられたテナント ユニットにのみアクセスできます。当然、テナント ユーザーとテナント管理者が持つ権限は異なります。

Tenant Unit
［テナント ユニット］は、テナント間の管理分離の単位として機能する Data Domain システムのパーティションです。テナントに割り当てられているテナント ユニットは、同じ Data Domain システムにも、違うシステムにも配置でき、保護され、互いに論理的に分離されています。それによって、共有インフラストラクチャ上で同時に複数のテナントを実行するときに、制御パスのセキュリティと分離を確保しています。テナント ユニットは、マルチテナンシー構成に必要なすべての構成要素を含む 1 個以上の［MTree］を含むことができます。ユーザー、管理グループ、通知グループ、その他の構成要素は、テナント ユニットの一部です。

制御パスとネットワークの分離

［制御パスの分離］は、テナント ユニットに［tenant-admin］と［tenant-user］のユーザー役割を与えることで行われます。データ アクセスと管理アクセスの［ネットワーク分離］は、［データ アクセス IP アドレス］と［管理 IP アドレス］の固定セットをテナント ユニットに関連づけることで実現します。

［tenant-admin］と［tenant-user］の役割は、特定のテナント ユニットの範囲と機能に限定され、そのテナント ユニットで実行できる操作も制限されます。データ パスの論理的な安全性と分離を確保するため、システム管理者は SMT 環境の各プロトコルに 1 つ以上のテナント ユニット MTree を構成する必要があります。サポートされるプロトコルは、DD Boost、NFS、CIFS、DD VTL です。アクセスは、ネイティブ アクセス制御メカニズムによって厳格に調整されます。

［テナント セルフ サービス セッション］（ssh 経由）は、DD システムの［管理 IP アドレス］の固定セットに限定することができます。また、管理アクセス セッション（ssh/http/https 経由）も、DD システムの管理 IP アドレスの固定セットに制限することができます。ただし、デフォルトでは、テナント ユニットに関連づけられた管理 IP アドレスは存在しないため、標準の制限は［tenant-admin］と［tenant-user］の役割を使用することのみです。`smt tenant-unit management-ip` を使用して、テナント ユニットの管理 IP アドレスを追加し、維持する必要があります。

同様に、（テナント ユニットに対する）データ アクセスとデータ フローも、ローカルまたはリモートの［データ アクセス IP アドレス］の固定セットに制限できます。割り当てられているデータ アクセス IP アドレスの使用により、SMT 関連のセキュリティ チェックを追加することで、DD Boost および NFS プロトコルのセキュリティが強化されます。たとえば、DD Boost RPC で返されるストレージ ユニットのリストを、割り当てられているローカル データ アクセス IP アドレスを持つテナント ユニットに属するストレージ ユニットに制限できます。NFS の場合、エクスポートのアクセスと可視性を、構成されているローカル データ アクセス IP アドレスに基づてフィルターできます。たとえば、テナント ユニットのローカル データ アクセス IP アドレスから `showmount -e` を使用した場合は、そのテナント ユニットに属する NFS エクスポートのみが表示されます。

［sysadmin］は、`smt tenant-unit data-ip` を使用してテナント ユニットのデータ アクセス IP アドレスを追加および管理する必要があります。

注

SMT 以外の IP アドレスを使用して SMT で MTree をマウントしようとすると、操作は失敗します。

複数のテナント ユニットが同じテナントに属している場合、それらのテナント ユニットはデフォルト ゲートウェイを共有できます。ただし、異なるテナントに属する複数のテナント ユニットは、同じデフォルト ゲートウェイを使用できません。

同じテナントに属する複数のテナント ユニットは、デフォルト ゲートウェイを共有できます。異なるテナントに属するテナント ユニットには、同じデフォルト ゲートウェイを使用できません。

SMT の RBAC とは

SMT（Secure Multi-Tenancy）では、タスクを実行する権限はユーザーに割り当てられた役割に依存します。DD Management Center は RBAC（役割に基づいたアクセス制御）を使用してこれらの権限を制御します。

すべての DD Management Center ユーザーは、次の操作を実行できます。

- すべてのテナントの表示
- 任意のテナントに属するテナント ユニットの作成、読み取り、更新、削除（テナント ユニットをホストする Data Domain システムの管理者の場合）
- テナントへの/からのテナント ユニットの割り当ておよび割り当て解除（テナント ユニットをホストする Data Domain システムの管理者の場合）
- 任意のテナントに属するテナント ユニットの表示（テナント ユニットをホストする Data Domain システムで役割を割り当てられている場合）

より高度なタスクの実行は、次のユーザーの役割に依存します。

admin ロール

［admin］ロールを持つユーザーは、Data Domain システムですべての管理操作を実行できます。［admin］は、Data Domain システムで、SMT のセットアップ、SMT ユーザー役割の割り当て、テナント セルフ サービス モードの有効化、テナントの作成など、すべての SMT 管理操作を実行できます。SMT では、［admin］は通常、［ランドロード］と呼ばれます。DD OS では、［sysadmin］とも呼ばれます。

テナントを編集または削除する権限を持つには、そのテナントのテナント ユニットに関連づけられたすべての Data Domain システムで、DD Management Center の［admin］と DD OS の［sysadmin］の両方である必要があります。テナントにテナント ユニットがない場合、そのテナントを編集または削除するには DD Management Center の［admin］である必要があるだけです。

limited-admin ロール
［limited-admin］ロールを持つユーザーは、［admin］として Data Domain システムですべての管理操作を実行できます。ただし、［limited-admin］ロールのユーザーは MTree を削除/破棄できません。DD OS には、同等の［limited-admin］ロールがあります。

tenant-admin ロール
［tenant-admin］ロールを持つユーザーは、［tenant self-service］モードが特定のテナント ユニットで有効になっている場合のみ、特定のタスクを実行できます。責任には、そのテナントのバックアップ アプリケーションのスケジュール設定と実行、割り当てられたテナント ユニット内のリソースと統計の監視が含まれます。［tenant-admin］は監査ログを表示できますが、RBAC により、［tenant-admin］に属するテナント ユニットの監査ログへのアクセスのみが許可されます。さらに、［tenant-admins］は、テナント セルフサービス モードが有効な場合は管理分離を行います。SMT では、［tenant-admin］ロールは通常、［バックアップ管理者］と呼ばれます。

tenant-user ロール
［tenant-user］ロールを持つユーザーは、テナント セルフ サービスが有効な場合にのみ、自分に割り当てられたテナント ユニットでのみ SMT コンポーネントのパフォーマンスと使用率を監視できます。ただし、このロールを持つユーザーは、自分に割り当てられたテナント ユニットの監査ログを表示することはできません。さらに、［tenant-users］は `show` コマンドと `list` コマンドを実行できます。

none ロール
［none］のロールを持つユーザーは、DD Boost を使用したパスワードの変更とデータのアクセス以外の操作を Data Domain システムで実行できません。ただし、SMT が有効化されると、［admin］は Data Domain システムから［none］ロールを持つユーザーを選択し、そのユーザーに［tenant-admin］または［tenant-user］の SMT 固有のロールを割り当てることができます。さらに、ユーザーは SMT 管理オブジェクトに対して操作を実行できます。

管理グループ
BSP（バックアップ サービス プロバイダー）は、1 つの外部 AD（Active Directory）または NIS（Network Information Service）で定義された［management groups］を使用して、テナント ユニットのユーザー役割の管理を簡易化できます。各 BSP テナントは独立した外部企業であり、AD、NIS などの名前サービスを使用できます。

SMT 管理グループがある場合、AD および NIS サーバは SMT ローカル ユーザーと同様に、［admin］によってセットアップおよび構成されます。［admin］は、AD または NIS 管理者にグループの作成および構成を依頼できます。その後、［admin］は SMT のロールをグループ全体に割り当てます。Data Domain システムにログインするグループのユーザーは、グループに割り当てられた役割でログインします。

ユーザーがテナントの会社を退職するか、そこに入社すると、AD または NIS 管理者はそのユーザーをグループから削除またはグループに追加できます。グループのメンバーのユーザーが追加または削除されても、Data Domain システムで RBAC 構成を変更する必要はありません。

テナント ユニットのプロビジョニング

構成ウィザードを起動すると、SMT（Secure Multitenancy）の最初のプロビジョニング手順が開始されます。手順の間、ウィザードはテナント構成要件に基づき、新しいテナント ユニットを作成およびプロビジョニングします。情報は、要求時に管理者が入力します。手順の完了後、管理者はテナント セルフサービス モードの有効化から始まる次のタスクのセットに進みます。初期セットアップ後、手動の手順と構成変更は必要に応じて実行できます。

手順

1. SMT を開始します。

```
# smt enable SMT enabled.
```

2. SMT が有効であることを確認します。

```
# smt status SMT is enabled.
```

3. SMT 構成ウィザードを立ち上げます。

```
# smt tenant-unit setup No tenant-units.
```

4. 構成プロンプトに従います。

```
SMT TENANT-UNIT Configuration

  Configure SMT TENANT-UNIT at this time (yes|no) [no]: yes

  Do you want to create new tenant-unit (yes/no)? : yes

Tenant-unit Name
  Enter tenant-unit name to be created
  : SMT_5.7_tenant_unit
Invalid tenant-unit name.
  Enter tenant-unit name to be created
  : SMT_57_tenant_unit

Pending Tenant-unit Settings
Create Tenant-unit   SMT_57_tenant_unit

Do you want to save these settings (Save|Cancel|Retry): save
SMT Tenant-unit Name Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration

  Configure SMT TENANT-UNIT MANAGEMENT-IP at this time (yes|no) [no]: yes

  Do you want to add a local management ip to this tenant-unit? (yes|no) [no]: yes

port  enabled  state  DHCP        IP address                netmask     type additional
                                                          /prefix length        setting
----- ------- ------- ---- -------------------------- -------------- ---- ----------
ethMa   yes   running  no  192.168.10.57              255.255.255.0   n/a
                           fe80::260:16ff:fe49:f4b0** /64
eth3a   yes   running ipv4 192.168.10.236*            255.255.255.0*  n/a
                           fe80::260:48ff:fe1c:60fc** /64
eth3b   yes   running  no  192.168.50.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1c:60fd** /64
eth4b   yes   running  no  192.168.60.57              255.255.255.0   n/a
                           fe80::260:48ff:fe1f:5183** /64
----- ------- ------- ---- -------------------------- -------------- ---- ----------
* Value from DHCP
** auto_generated IPv6 address

Choose an ip from above table or enter a new ip address. New ip addresses will need
to be created manually.

Ip Address
  Enter the local management ip address to be added to this tenant-unit
  : 192.168.10.57

  Do you want to add a remote management ip to this tenant-unit? (yes|no) [no]:

Pending Management-ip Settings

Add Local Management-ip    192.168.10.57
  Do you want to save these settings (Save|Cancel|Retry): yes
  unrecognized input, expecting one of Save|Cancel|Retry

  Do you want to save these settings (Save|Cancel|Retry): save
  Local management access ip "192.168.10.57" added to tenant-unit "SMT_57_tenant_unit".

SMT Tenant-unit Management-IP Configurations saved.

SMT TENANT-UNIT MANAGEMENT-IP Configuration
```

```
  Do you want to add another local management ip to this tenant-unit? (yes|no) [no]:

  Do you want to add another remote management ip to this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT DDBOOST Configuration
  Configure SMT TENANT-UNIT DDBOOST at this time (yes|no) [no]:

SMT TENANT-UNIT MTREE Configuration
  Configure SMT TENANT-UNIT MTREE at this time (yes|no) [no]: yes

Name                        Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------   --------------   ------   -----------
/data/col1/laptop_backup           4846.2   RO/RD     -
/data/col1/random                 23469.9   RO/RD     -
/data/col1/software2               2003.7   RO/RD     -
/data/col1/tsm6                  763704.9   RO/RD     -
-------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create a mtree for this tenant-unit now? (yes|no) [no]: yes

MTree Name
  Enter MTree name
  :  SMT_57_tenant_unit
Invalid mtree path name.
  Enter MTree name
  :
SMT_57_tenant_unit


Invalid mtree path name.
  Enter MTree name
  : /data/col1/SMT_57_tenant_unit

MTree Soft-Quota
  Enter the quota soft-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

MTree Hard-Quota
  Enter the quota hard-limit to be set on this MTree (<n> {MiB|GiB|TiB|PiB}|none)
  :

Pending MTree Settings
Create MTree        /data/col1/SMT_57_tenant_unit
MTree Soft Limit    none
MTree Hard Limit    none

  Do you want to save these settings (Save|Cancel|Retry): save
  MTree "/data/col1/SMT_57_tenant_unit" created successfully.
  MTree "/data/col1/SMT_57_tenant_unit" assigned to tenant-unit  "SMT_57_tenant_unit".

SMT Tenant-unit MTree Configurations saved.

SMT TENANT-UNIT MTREE Configuration

Name                        Pre-Comp (GiB)   Status   Tenant-Unit
-------------------------   --------------   ------   -----------
/data/col1/laptop_backup           4846.2   RO/RD     -
/data/col1/random                 23469.9   RO/RD     -
/data/col1/software2               2003.7   RO/RD     -
/data/col1/tsm6                  763704.9   RO/RD     -
```

```
------------------------   --------------   ------   -----------
D    : Deleted
Q    : Quota Defined
RO   : Read Only
RW   : Read Write
RD   : Replication Destination
RLGE : Retention-Lock Governance Enabled
RLGD : Retention-Lock Governance Disabled
RLCE : Retention-Lock Compliance Enabled

  Do you want to assign another MTree to this tenant-unit? (yes|no) [no]: yes

  Do you want to assign an existing MTree to this tenant-unit? (yes|no) [no]:

  Do you want to create another mtree for this tenant-unit? (yes|no) [no]:

SMT TENANT-UNIT SELF-SERVICE Configuration

  Configure SMT TENANT-UNIT SELF-SERVICE at this time (yes|no) [no]: yes
  Self-service of this tenant-unit is disabled

  Do you want to enable self-service of this tenant-unit? (yes|no) [no]: yes

  Do you want to configure a management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure a management group for this tenant-unit (yes|no) [no]: yes

Management-Group Name
  Enter the group name to be assigned to this tenant-unit
  : SMT_57_tenant_unit_group

What role do you want to assign to this group  (tenant-user|tenant-admin) [tenant-user]:
tenant-admin

Management-Group Type
  What type do you want to assign to this group (nis|active-directory)?
  : nis

Pending Self-Service Settings
Enable Self-Service       SMT_57_tenant_unit
Assign Management-group   SMT_57_tenant_unit_group
Management-group role     tenant-admin
Management-group type     nis

  Do you want to save these settings (Save|Cancel|Retry): save
  Tenant self-service enabled for tenant-unit "SMT_57_tenant_unit"
  Management group "SMT_57_tenant_unit_group" with type "nis" is assigned to tenant-unit
  "SMT_57_tenant_unit" as "tenant-admin".

SMT Tenant-unit Self-Service Configurations saved.

SMT TENANT-UNIT SELF-SERVICE Configuration

  Do you want to configure another management user for this tenant-unit? (yes|no) [no]:

  Do you want to configure another management group for this tenant-unit? (yes|no)
[no]:

SMT TENANT-UNIT ALERT Configuration

  Configure SMT TENANT-UNIT ALERT at this time (yes|no) [no]: yes
  No notification lists.

Alert Configuration

Alert Group Name
  Specify alert notify-list group name to be created
  : SMT_57_tenant_unit_notify

Alert email addresses
```

```
  Enter email address to receive alert for this tenant-unit
  : dd_proserv@emc.com

  Do you want to add more emails (yes/no)?
  : no

Pending Alert Settings
Create Notify-list group   SMT_57_tenant_unit_notify
Add emails                 dd_proserv@emc.com

  Do you want to save these settings (Save|Cancel|Retry): save
  Created notification list "SMT_57_tenant_unit_notify" for tenant "SMT_57_tenant_unit".
  Added emails to notification list "SMT_57_tenant_unit_notify".

SMT Tenant-unit Alert Configurations saved.

Configuration complete.
```

テナント セルフサービス モードの有効化

制御パス分離に必要なテナントのセルフサービスを実装するため、管理義務の分離と管理タスクのデリゲーションを行うには、システム管理者はテナント ユニットでこのモードを有効化し、テナント管理者またはテナント ユーザーの役割でユニットを管理するユーザーを割り当てます。その役割によって、管理者以外のユーザーが、自分に割り当てられたテナント ユニットで特定の管理タスクを実行できます。管理の分離に加えて、テナント セルフサービス モードにより、社内の IT やサービス プロバイダー スタッフの管理作業を軽減することができます。

手順

1. 1 つまたはすべてのテナント ユニットのテナント セルフサービス モード ステータスを表示します。
   ```
   # smt tenant-unit option show { tenant-unit | all }
   ```
2. 選択されたテナント ユニットでテナント セルフサービス モードを有効化します。
   ```
   # smt tenant-unit option set tenant-unit self-service { enabled
   | disabled }
   ```

プロトコルによるデータ アクセス

プロトコル固有アクセス制御によるセキュア データ パスは、テナント ユニットのセキュリティと分離を可能にします。SMT（Secure Multitenancy）環境では、Data Access Protocol 管理コマンドは、テナント ユニット パラメーターで拡張して統合レポートも可能にします。

DD システムは DD Boost、NFS、CIFS、DD VTL を含む複数のデータ アクセス プロトコルに同時に対応します。DD システムは、それ自体を Ethernet を介した NFS または CIFS アクセスを提供するファイル サーバ、DD VTL デバイス、DD Boost デバイスなどのアプリケーション固有インターフェイスとして機能させます。

各対応プロトコルのネイティブ アクセス制御メカニズムにより、各テナントのデータ パスを分け、切り離した状態にします。そのメカニズムには、CIFS の ACL（アクセス制御リスト）、NFS のエクスポート、DD Boost 認証情報、Multi-User Boost 認証情報認識アクセス制御が含まれます。

SMT における Multi-User DD Boost とストレージ ユニット

SMT（Secure Multi-Tenancy）とともに Multi-User DD Boost を使用する場合、ユーザー権限はストレージ ユニットの所有権ごとに設定されます。

［Multi-User DD Boost］は、DD Boost アクセス制御での複数の DD Boost ユーザー資格情報の使用を意味します。各ユーザーが、異なるユーザー名とパスワードを持ちます。

［Storage Unit］は、DD Boost プロトコル用に構成された MTree です。ユーザーは、1 個以上の Storage Unit に関連づけ（「所有」）できます。あるユーザーが所有するストレージ ユニットは、他

のユーザーが所有することはできません。そのため、ストレージ ユニットにバックアップ/リストアなどのタイプのデータ アクセスができるのは、そのストレージ ユニットを所有するユーザーのみです。DD Boost ユーザー名の数は、MTree の最大数よりも少なくする必要があります。（ 各 DD モデルに対する MTree の現在の最大数については、本書の「MTree」の章を参照してください。） SMT に関連付けられているストレージ ユニットには［none］ロールを割り当てる必要があります。

各バックアップ アプリケーションは、その DD Boost ユーザー名とパスワードを使用して認証を行う必要があります。認証後、DD Boost は認証された認証情報を検証して、Storage Unit の所有権を確認します。バックアップ アプリケーションは、バックアップ アプリケーションから渡されたユーザー資格情報が Storage Unit に関連づけられたユーザー名に一致する場合にのみ、その Storage Unit へのアクセスが許可されます。ユーザー資格情報とユーザー名が一致しない場合、ジョブは権限エラーで失敗します。

CIFS のアクセスの構成

CIFS（共通インターネット ファイル システム）は、リモート ファイル アクセスのファイル共有プロトコルです。SMT（Secure Multitenancy）構成では、バックアップとリストアには、関連づけられたテナント ユニットの MTree に常駐する CIFS 共有へのクライアント アクセスが必要です。データ分離は、CIFS 共有と CIFS ACL を使用して実現されます。

手順

1. CIFS 用の MTree を作成し、テナント ユニットに MTree を割り当てます。

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. MTree の容量ソフトおよびハード制限を設定します。

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. MTree から pathname の CIFS 共有を作成します。

   ```
   # cifs share create share path pathname clients clients
   ```

NFS アクセスの構成

NFS は、リモート ファイル アクセスの UNIX ベース ファイル共有プロトコルです。SMT（Secure Multitenancy）環境では、バックアップとリストアには、関連づけられたテナント ユニットの MTree に常駐する NFS エクスポートへのクライアント アクセスが必要です。データ分離は、NFS エクスポートとネットワーク分離を使用して実現されます。NFS は、MTree がネットワーク分離テナント ユニットに関連づけられているかどうかを判定します。関連づけられている場合、NFS はテナント ユニットに関連づけられた接続プロパティを確認します。接続プロパティには、宛先 IP アドレスおよびインターフェイスまたはクライアント ホスト名が含まれます。

手順

1. NFS 用の MTree を作成し、テナント ユニットに MTree を割り当てます。

   ```
   # mtree create mtree-path tenant-unit tenant-unit
   ```

2. MTree の容量ソフトおよびハード制限を設定します。

   ```
   # mtree create mtree-path tenant-unit tenant-unit] [quota-soft-
   limit n{MiB|GiB|TiB|PiB} ] [quota-hard-limit n {MiB|GiB|TiB|PiB}
   ```

3. 1 個以上のクライアントを MTree に追加して NFS エクスポートを作成します。

   ```
   # nfs add path client-list
   ```

DD VTL のアクセスの構成

DD VTL テナント データ分離は、ホスト システムと DD VTL 間の仮想アクセス パスを作成する DD VTL アクセス グループを使用して実現されます。（ホスト システムと DD VTL 間の物理ファイバー チャネル接続が存在している必要があります）。

DD VTL にテープを置くことで、ホスト システムのバックアップ アプリケーションでそれを書き込むまたは読み取ることができます。DD VTL テープは、MTree である DD VTL プールで作成されます。DD VTL プールは MTree であるため、プールはテナント ユニットに割り当てることができます。この関連づけによって、SMT 監視/レポート作成を有効化します。

たとえば、テナント管理者に DD VTL プールを含むテナント ユニットが割り当てられた場合、テナント管理者は MTree コマンドを実行して、読み取り専用情報を表示できます。コマンドは、テナント ユニットに割り当てられた DD VTL プールでのみ実行できます。

次のコマンドが含まれます。

- `mtree list`：テナント ユニットの MTrees リストを表示します。
- `mtree show compression` ：MTree 圧縮の統計情報を表示します。
- `mtree show performance` ：パフォーマンスの統計情報を表示します。

ほとんどの `list` および `show` コマンドからの出力には、サービス プロバイダーによるスペース使用率とチャージ バック料金の計算を可能にする統計が含まれます。

DD VTL 操作は影響を受けず、正常に動作し続けます。

DD VTL NDMP TapeServer の使用

DD VTL テナント データ分離には、NDMP を使用する方法もあります。DD OS は、NDMP（ネットワーク データ管理プロトコル）対応システムが 3way NDMP バックアップを介してバックアップ データを DD システムに送信できるようにする NDMP テープ サーバーを実装します。

バックアップ データは、特殊 DD VTL グループ［TapeServer］に割り当てられた DD VTL によって（プール内の）仮想テープに書き込まれます。

バックアップ データはプール内のテープに書き込まれるため、MTree に関する DD VTL トピックの情報は Data Domain NDMP TapeServer にも適用されます。

データ管理操作

SMT（Secure Multitenancy）管理操作には、ストレージ ユニット、MTree などのテナント ユニットとその他のオブジェクトのモニタリングが含まれます。一部の SMT オブジェクトでは、追加構成または変更も必要な場合があります。

パフォーマンス統計の収集

各 MTree のパフォーマンス（または「使用率」）、統計、その他のリアルタイム情報を測定できます。DD Boost ストレージ ユニットについては、過去の消費率を確認できます。コマンド出力によって、テナント管理者はテナント ユニットに関連づけられた MTree、またはすべての MTree と関連づけられたテナント ユニットの使用率統計と圧縮率を収集できます。出力は、分から月の間隔で使用率を表示するようフィルタリングできます。結果は、統計をチャージバック メトリックとして使用する管理者に渡されます。ストレージ ユニットの使用率統計と圧縮率の収集にも、同様の方法が使用されます。

手順

1. MTree パフォーマンスの統計情報を表示します。

   ```
   # mtree show stats
   ```

2. テナント ユニットに関連づけられた MTree のパフォーマンス統計を収集します。

   ```
   # mtree show performance
   ```

3. テナント ユニットに関連づけられた MTree の圧縮統計を収集します。

   ```
   # mtree show compression
   ```

クォータの変更

QoS 基準を満たすには、システム管理者は DD OS「ノブ」を使用して、テナント構成が必要とする設定を調整します。たとえば、管理者は、DD Boost ストレージ ユニットに「ソフト」および「ハード」クォータ制限を設定できます。ストリーム「ソフト」および「ハード」クォータ制限は、テナント ユニットに割り当てられた DD Boost ストレージ ユニットにのみ割り当てることができます。管理者がクォータを設定すると、テナント管理者は、各オブジェクトがそれに割り当てられたクォータを超えず、システム リソースの他のものを奪わないようにするため、1 個またはすべてのテナント ユニットを監視できます。

クォータは、構成ウィザードで要求されたときに最初に設定されますが、後で調整または変更できます。次に、DD Boost のクォータを変更する方法の例を示します。（`quota capacity` と `quota streams` を使用して、容量およびストリーム クォータおよび制限を扱うことができます）。

手順

1. DD Boost ストレージ ユニット「su33」でソフトおよびハード クォータ制限を変更する場合：

   ```
   ddboost storage-unit modify su33 quota-soft-limit 10 Gib quota-hard-limit 20 Gib
   ```

2. DD Boost ストレージ ユニット「su33」でソフトおよびハード ストリーム制限を変更する場合：

   ```
   ddboost storage-unit modify su33 write-stream-soft-limit 20 read-stream-soft-limit 6 repl -stream-soft-limit 20 combined-stream-soft-limit 20
   ```

3. DD Boost ストレージ ユニット「su33」の物理サイズを報告する場合：

   ```
   ddboost storage-unit modify su33 report-physical-size 8 GiB
   ```

SMT とレプリケーション

災害発生時、ユーザー役割によって、データ リカバリ操作でユーザーが行えるサポートの方法が決まります。SMT 構成では、さまざまなレプリケーション タイプを使用できます。（レプリケーションの実行方法の詳細については、［DD Replicator］の章を参照してください）。

ユーザー役割に関する考慮事項は次のとおりです。

- 管理者は、レプリケーションされたコピーから MTree をリカバリできます。
- テナント管理者は、DD Boost 管理ファイル レプリケーションを使用して MTree をシステム間でレプリケーションできます。
- テナント管理者は、DD Boost 管理ファイル レプリケーションを使用して、レプリケーションされたコピーから MTree をリカバリすることもできます。

コレクション レプリケーション
コレクション レプリケーションは、コア テナント ユニット構成情報をレプリケーションします。

パブリック インターネットを介した安全なレプリケーション
パブリック インターネット接続経由でレプリケーションするときに中間者（MITM）攻撃から保護するために、認証には、レプリケーションのソースとデスティネーションでの SSL 証明書に関連する情報の妥当性検査が含まれます。

DD Boost 管理ファイル レプリケーションを使用する MTree レプリケーション（NFS/CIFS）
MTree レプリケーションは、DD Boost 管理ファイル レプリケーションを使用して、テナント ユニットに割り当てられた MTree で対応しています。MTree レプリケーション中、1 つのシステムでテナント ユニットに割り当てられた MTree は、他のシステムのテナント ユニットに割り当てられた MTree にレプリケーションできます。MTree レプリケーションは、2 つの DD システム上の 2 つの異なるテナント間では許可されません。セキュリティ モードが［厳格］に設定されていると、MTree レプリケーションは、MTree が同じテナントに属している場合のみ許可されます。

下位互換性については、テナント ユニットに割り当てられた MTree から割り当てられていない MTree への MTree レプリケーションには対応していますが、手動で構成する必要があります。手動構成によって、デスティネーション MTree のテナント ユニットの設定が正しくなるようにします。割り当てられていない MTree からテナント ユニットに割り当てられた MTree への MTree レプリケーションにも対応しています。

SMT に対応した MTree レプリケーションを設定する場合、［セキュリティ モード］は、テナントのチェックをどの程度実行するかを定義します。［デフォルト］ モードは、ソースおよびターゲットが異なるテナントに属していないことをチェックします。［厳格］モードは、ソースとターゲットが同じテナントに属していることを確認します。そのため、厳格モードを使用する場合、レプリケートする MTree と関連づけられたソース マシン上のテナント UUID と同じ UUID を使用して、ターゲット マシンでテナントを作成する必要があります。

DD Boost 管理ファイル レプリケーション（DD Boost AIR も使用）
テナント ユニットに割り当てられているのが片方か両方かにかかわらず、ストレージ ユニット間の DD Boost 管理ファイル レプリケーションに対応しています。

DD Boost 管理ファイル レプリケーションの間、ストレージ ユニットは全体的にレプリケーションされません。その代わり、レプリケーション用のバックアップ アプリケーションによってストレージ ユニット内の特定のファイルが選択されます。ストレージ ユニットで選択され、1 つのシステムでテナント ユニットに割り当てられたファイルは、他のシステムでテナント ユニットに割り当てられたストレージ ユニットにレプリケーションできます。

下位互換性については、テナント ユニットに割り当てられたストレージ ユニット内の選択されたファイルは、割り当てられていないストレージ ユニットにレプリケーションできます。割り当てられていないストレージ ユニット内の選択されたファイルは、テナント ユニットに割り当てられたストレージ ユニットにレプリケーションできます。

DD Boost 管理ファイル レプリケーションは、DD Boost AIR 展開でも使用できます。

QoS のためのレプリケーション制御
MTree に対して、レプリケーション スループットの上限値（`repl-in`）を指定できます。各テナントの Mtree はテナント ユニットに割り当てられるため、この上限値を設定することで、各テナントのレプリケーション リソースの使用量を制限できます。この機能と SMT との関係により、MTree レプリケーションはこのスループット制限に従います。

SMT テナント アラート

DD システムは、ソフトウェアまたはハードウェアに問題がある可能性がある場合、［イベント］を生成します。イベントが生成されると、［アラート］通知がすぐに、通知リストで指定されたメンバーと Data Domain 管理者にメールで送信されます。

SMT アラートは、各テナント ユニットに固有であり、DD システム アラートとは異なります。テナント セルフサービス モードが有効になっている場合、テナント管理者は、自分が関連づけられている各

種システム オブジェクト、および予期せぬシステム シャットダウンなどのクリティカルなイベントに関するアラートを受け取ることができます。テナント管理者は、自分が関連づけられた通知リストのみ表示または変更できます。

次の例は、サンプル アラートを示します。通知の下部にある 2 個のイベント メッセージは、「Tenant」という語で示されるマルチ テナント環境に固有である点に留意してください。DD OS と SMT アラートの全体リストについては、［Data Domain MIB クイック リファレンス ガイド］または SNMP MIB を参照してください。

```
EVT-ENVIRONMENT-00021 - Description: The system has been shutdown by
abnormal method; for example, not by one of the following: 1) Via
IPMI chassis control command 2) Via power button 3) Via OS shutdown.
Action: This alert is expected after loss of AC (main power) event.
If this shutdown is not expected and persists, contact your
contracted support provider or visit us online at https://
my.datadomain.com. Tenant description: The system has experienced an
unexpected power loss and has restarted. Tenant action: This alert is
generated when the system restarts after a power loss. If this alert
repeats, contact your System Administrator.
```

スナップショットの管理

［スナップショット］は、ポイント イン タイムでキャプチャーされた MTree の読み取り専用コピーです。スナップショットは、システムの異常発生時のリストア ポイントなど、多くの用途に使用できます。`snapshot` の使用に必要な役割は、admin または tenant-admin です。

MTree またはテナント ユニットのスナップショット情報を表示する場合：

```
# snapshot list mtree mtree-path | tenant-unit tenant-unit
```

MTree またはテナント ユニットのスナップショット スケジュールを表示する場合：

```
# snapshot schedule show [name | mtrees mtree-listmtree-list | tenant-
unit tenant-unit]
```

ファイル システム Fast Copy の実行

Fast Copy 操作は、ファイルとソース ディレクトリのディレクトリ ツリーを、DD システムのターゲット ディレクトリにコピーします。SMT（Secure Multitenancy）による Fast Copy に関しては、特別な事情があります。

テナント セルフサービス モードを有効にした状態でファイル システム Fast Copy を実行する際の考慮事項をいくつか示します。

- テナント管理者は、テナント管理者が両方のテナント ユニットのテナント管理者であり、その 2 個のテナント ユニットが同じテナントに属している場合、1 個のテナント ユニットから他のテナント ユニットへファイルを Fast Copy できます。
- テナント管理者は、同じテナント ユニット内でファイルを Fast Copy できます。
- テナント管理者は、ソースと宛先のテナント ユニット内でファイルを Fast Copy できます。

ファイル システム Fast Copy を実行する場合：

```
# filesys fastcopy source <src> destination <dest>
```

第 18 章

DD Cloud Tier

本章には、次のセクションが含まれます。

- DD Cloud Tier の概要 480
- クラウド階層の構成 483
- クラウド ユニットの構成 485
- データの移動 498
- コマンド ライン インターフェイス（CLI）による DD Cloud Tier の構成 503
- DD クラウド ユニットの暗号化の構成 506
- システムが失われた場合に必要な情報 507
- クラウド階層での DD Replicator の使用 508
- クラウド階層での DD VTL（仮想テープ ライブラリ） の使用 508
- DD Cloud Tier の容量消費グラフの表示 508
- DD Cloud Tier のログ 509
- CLI（コマンド ライン インターフェイス）による DD Cloud Tier の削除 509

DD Cloud Tier の概要

DD Cloud Tier は、DD OS 6.0（以降）のネイティブ機能であり、データをアクティブ階層から長期保存用のパブリック クラウド、プライベート クラウド、ハイブリッド クラウド内の低コスト、大容量オブジェクト ストレージに移動するために使用します。DD Cloud Tier は、コンプライアンス、規制、ガバナンス上の理由により保持しているアクセス頻度の低いデータの長期保存用として最適です。DD Cloud Tier に最適なデータは、通常のリカバリ ウィンドウを経過したデータです。

DD Cloud Tier は、単一の Data Domain ネームスペースを使用して管理されます。クラウド ゲートウェイまたは仮想アプライアンスを別途用意する必要はありません。データ移動は、ネイティブな Data Domain ポリシー管理フレームワークによりサポートされます。概念上、クラウド ストレージは Data Domain システムに接続されている追加のストレージ階層（DD Cloud Tier）として扱われ、データは必要に応じて階層間で移動します。クラウドに格納されているデータに関連づけられたファイル システム メタデータは、ローカル ストレージで保持される上、クラウドにもミラーリングされます。ローカル ストレージに置かれたメタデータにより、重複排除、クリーニング、Fast Copy、レプリケーションなどの操作が容易になります。このローカル ストレージは、管理を容易にするためにクラウド ユニットと呼ばれる自己完結型のバケットに分割されます。

サポートするプラットフォーム

クラウド階層は、別のストレージ階層に対応するために必要なメモリ、CPU、ストレージ接続を持つ物理プラットフォームでサポートされます。

DD Cloud Tier は、これらのシステムでサポートされます。

表 196 DDCloud Tier をサポートする構成

モデル	メモリ	クラウド容量	SAS I/O モジュールの必要数	サポートするメタデータ ストレージのシェルフ ディスク タイプ	ES30 シェルフまたは DS60 ディスク パックの必要数	メタデータ ストレージに必要な容量
DD990	256 GB	1140 TB	4	ES30	4	180 TB（60 台の 3 TB HDD）
DD3300 4 TB	16 GB	8 TB	N/A	N/A	N/A	1 TB（1 台の 1 TB 仮想ディスク）
DD3300 8 TB	48 GB	16 TB	N/A	N/A	N/A	2 TB（2 台の 1 TB 仮想ディスク）
DD3300 16 TB	48 GB	32 TB	N/A	N/A	N/A	2 TB（2 台の 1 TB 仮想ディスク）
DD3300 32 TB	64 GB	64 TB	N/A	N/A	N/A	4 TB（4 台の 1 TB 仮想ディスク）
DD4200	128 GB	378 TB	3	DS60 または ES30	2	90 TB（30 台の 3 TB HDD）
DD4500	192 GB	570 TB	3	DS60 または ES30	2	120 TB（30 台の 4 TB HDD）
DD6800	192 GB	576 TB	2	DS60 または ES30	2	120 TB（30 台の 4 TB HDD）

表 196 DDCloud Tier をサポートする構成 （続き）

モデル	メモリ	クラウド容量	SAS I/O モジュールの必要数	サポートするメタデータ ストレージのシェルフ ディスク タイプ	ES30 シェルフまたは DS60 ディスク パックの必要数	メタデータ ストレージに必要な容量
DD7200	256 GB	856 TB	4	DS60 または ES30	4	240 TB（60 台の 4 TB HDD）
DD9300	384 GB	1400 TB	2	DS60 または ES30	4	240 TB（60 台の 4 TB HDD）
DD9500	512 GB	1728 TB	4	DS60 または ES30	5	300 TB（75 台の 4 TB HDD）
DD9800	768 GB	2016 TB	4	DS60 または ES30	5	300 TB（75 台の 4 TB HDD）
DD VE 16 TB	32 GB	32 TB	N/A	N/A	N/A	500 GB（1 台の 500 GB 仮想ディスク）[a]
DD VE 64 TB	60 GB	128 TB	N/A	N/A	N/A	500 GB（1 台の 500 GB 仮想ディスク）[a]
DD VE 96 TB	80 GB	192 TB	N/A	N/A	N/A	500 GB（1 台の 500 GB 仮想ディスク）[a]

a. メタデータの最小サイズはハード リミットです。Data Domain では、メタデータ ストレージ用の 1 TB から開始し、1 TB 単位で拡張することをユーザーに推奨しています。「Data Domain Virtual Edition インストールおよび管理ガイド」に、DD Cloud Tier と DD VE を使用する詳細が記されています。

注

DD Cloud Tier では、Data Domain HA（高可用性）の使用がサポートされています。両方のノードが DD OS 6.0 以降を実行しており、HA に対応している必要があります。

注

DD Cloud Tier は、リストされていないいずれのシステムでもサポートされておらず、Extended Retention 機能を有効化してあるか Collection Replication を構成してあるいずれのシステムでもサポートされていません。

注

クラウド階層機能は、特に低帯域幅構成（1 Gbps）の場合に、共有 WAN リンクで使用可能なすべての帯域幅を消費することがあり、このことが WAN リンクを共有する他のアプリケーションに影響することがあります。WAN 上に共有アプリケーションがある場合は、輻輳を回避し、長期的に安定したパフォーマンスを確保するために QoS やその他のネットワーク制限の使用をお勧めします。帯域幅が限られている場合は、データ移動速度は低速になり、クラウドに移動できるデータの量が限られます。Cloud Tier に移動するデータ専用のリンクを使用することをお勧めします。

注

オンボードの管理ネットワーク インターフェイス コントローラ（ethMx インターフェイス）を介してトラフィックを送信しないでください。

DD Cloud Tier のパフォーマンス

Data Domain システムは、内部最適化によって DD Cloud Tier のパフォーマンスを最大限まで高めます。

クラウド シーディング

クラウドへの現在の移行エンジンはファイル ベースであり、効率的な重複排除最適化エンジンが一意のセグメントのみを特定してクラウドに移行するために使用されます。このファイル ベースの移行エンジンの効率は、より高い世代のデータをクラウド階層に移行する際に高くなります。クラウド階層には重複排除の対象となるいくらかのデータがすでにあります。ただし、クラウド階層が空またはほぼ空の場合、重複排除の対象となるデータはありません。重複排除に費やされるコンピューティング サイクルのオーバーヘッドがあります。シーディング ベースの移行では、重複排除フィルタリングはアクティブ階層自体で維持され、一意のデータのみが一括でクラウド階層に移行されます。クラウド シーディングでは、エンジンで重複排除のための処理を行うことなく、ローカル ストレージからクラウド ストレージにコンテンツが移行されます。クラウド シーディングがアクティブな場合、シーディングによって識別されたすべてのファイルの移行が完了するまで、アクティブ階層ファイル システムのクリーニングの一環として、クラウド ストレージへの移行用にマークされたファイルはクリーンアップされません（つまり、スペースは解放されません）。アクティブ階層のストレージは、大量のデータがクラウド ストレージに移行される環境でこれを考慮してサイズ設定する必要があります。DD Cloud Tier ストレージの容量が 5%を下回り、show space コマンドで示される圧縮後のデータ使用量が 30 TiB 以上になると、Data Domain システムでは、データをクラウド ストレージに移行するときに自動的にクラウド シーディングを使用します。

DD Cloud Tier の容量の 5%が消費されると、クラウド シーディングが自動的に非アクティブになり、クラウド ストレージへの移行の前にデータの重複排除処理が行われます。

シーディング移行を使用する場合に考慮すべきその他のポイントを次に示します。

- 移行は、次の場合にのみシーディング モードでサポートされます。
  - アクティブ階層の圧縮後使用サイズが、filesys show space の出力で 30 TiB 以上であるとレポートされていること。
  - filesys show space の出力で、移行の開始時にアクティブ階層の使用率が 70%未満であると報告されていること。

    注

    シーディング モードで進行中の移行サイクルの間にアクティブ階層の使用率が 90%を超えた場合、移行は中止され、通常のファイルコピー モードで移行が再開されます。
- シーディング モードでの移行は、アクティブ階層でのクリーニングの期間全体にわたって、アクティブ階層でのクリーニングによって自動的に中断されます。クリーニングが完了すると、シーディングが自動的に再開され、クラウドへの移行が再開されます。
- シーディング モードでの移行は、移行先のクラウドの UNAVAIL イベントがクラウド ユニットで受信された場合に自動中断し（クラウド ユニットは「切断」としてレポートされます）、クラウド ユニットが利用可能になり、アクティブであることがレポートされてのみ再開されます。
- シーディング モードで進行中の移行操作の宛先であるクラウド ユニットでは、クリーニングを開始できません。

注

クラウド ユニット 2 つのシステムで、シードされていない 2 番目のクラウド ユニットのクリーニングを強制的に開始するには、data-movement suspend CLI を使用してシーディング モードでの移行を中断し、2 番目のクラウド ユニットで cloud clean start CLI を実行します。

- クラウドでの確率的ファイル検証は、デフォルト ポリシーに従ってスケジュール設定されている場合でも、スキップされ、移行がシーディング モードで進行中のクラウド ユニットでは行われません。
- クラウド階層またはアクティブ階層でクリーニングが既に進行中で、スケジュール設定されたデータ移動がシーディング モードで開始される場合は、クリーニング アクティビティの間、データ移動は自動で中断されます。
- シーディング モードでの移行では、ファイルが移行に適格であっても、レプリケーション先である MTree からのファイルの移行はスキップされます。レプリケーション先 MTree（RO/RD）であるこれらの MTree からのファイルは、すべての適格な MTree からのシーディング モードでの移行が完了すると、ファイルコピー エンジンを使用して移行されます。
- 物理容量レポート機能が有効になっていてスケジュール設定されている場合、シーディング モードでの移行は、シード ベースの移行の間、容量レポート機能を中断します。
- シーディング モードでの移行は、80 Gb を超える RAM を搭載したすべてのクラウド対応 Data Domain システムおよび構成でのみサポートされます。シーディング ベースの移行は、DD VE ではデフォルトで無効になっています。

サイズの大きいオブジェクト
DD Cloud Tier では、メタデータのオーバーヘッドを削減し、クラウド ストレージに移行するオブジェクトの数を減らすために、（クラウド ストレージ プロバイダーに応じて）1 MB か 4 MB のサイズのオブジェクトを使用します。

クラウド階層の構成

クラウド階層を構成するには、ライセンスとエンクロージャを追加し、システムのパスフレーズを設定して、クラウドへのデータ移動をサポートするファイル システムを作成します。

- クラウド階層を使用するには、クラウド容量ライセンスが必要です。
- クラウド階層のライセンスを取得するには、製品の機能、ソフトウェア アップデート、ソフトウェア互換性ガイドの最新情報、および EMC の製品、ライセンス、サービスに関する情報が記載されている、該当する「Data Domain オペレーティング システム リリース ノート」を参照してください。
- システムのパスフレーズを設定するには、［**Administration**］ > ［**Access**］ > ［**Administrator Access**］タブを使用します。システム パスフレーズが設定されていない場合、［Passphrase］領域に［**Set Passphrase**］ボタンが表示されます。システム パスフレーズが構成されている場合、［**Change Passphrase**］ボタンが表示されます。選択できるのは、パスフレーズを変更するオプションだけです。
- ストレージを構成するには、［**Hardware**］ > ［**Storage**］タブを使用します。
- ファイル システムを作成するには、ファイル システムの作成ウィザードを使用します。

DD Cloud Tier のストレージの構成

クラウド ユニットでは、DD システム上のクラウド階層ストレージが必要なです。このストレージは、クラウドに保存されているファイルのメタデータを保持します。

手順

1. ［**Hardware**］ > ［**Storage**］を選択します。
2. ［Overview］タブで、［**Cloud Tier**］を拡張します。
3. ［**Configure**］をクリックします。

   ［Configure Cloud Tier］ダイアログ ボックスが表示されます。
4. ［Addable Storage］セクションから、追加するシェルフのチェック ボックスを選択します。

   ⚠ 注意

   DD3300 システムでは、DD Cloud Tier のメタデータ ストレージ用に 1 TB ストレージ デバイスを使用する必要があります。
5. ［**Add to Tier**］ボタンをクリックします。
6. ［**Save**］をクリックして、ストレージを追加します。
7. ［**Data Management**］ > ［**File System**］を選択し、クラウド階層機能を有効化します。
8. ［**Disable**］（画面の最下部）をクリックしてファイル システムを無効化します。
9. ［**OK**］をクリックします。
10. ファイル システムを無効化したら、［**Enable Cloud Tier**］を選択します。

    クラウド階層を有効化するには、ライセンス容量のストレージ要件を満たす必要があります。
    ファイル システムのクラウド階層を構成します。［**Next**］をクリックします。
    クラウド ファイル システムでは、クラウド メタデータのローカル コピー用のローカル ストアが必要です。
11. ［**Enable file system**］を選択します。

    クラウド階層が指定されたストレージで有効になります。
12. ［**OK**］をクリックします。

    ファイル システムを作成したら、クラウド ユニットを別個に作成する必要があります。

クリーニング可能なスペースの推定

クリーニング可能なスペースの推定ツールは、`data-movement` で適格なファイルをクラウドに移動し、GC でファイル システムをクリーンアップする場合に、アクティブ階層で解放できる領域の量を評価します。

このツールは、クラウド/アーカイブ ライセンスが存在するかどうかにかかわらず動作します。

クラウド/アクティブ ライセンスがない場合は、アクティブ階層のクリーニング可能なスペースの総量を評価するのに使用される経過時間閾値を指定して下さい。MTree 上に設定されたポリシーと経過時間閾値の両方がある場合は、ユーザーが指定した経過時間閾値が優先されます。

3 つのワークフローがあります。

- クラウド移行ポリシーが設定されたシステム：ファイルは、それぞれの MTree に設定されたポリシーに基づいて「適格」として識別され、クリーニング可能なスペースが計算されます。
- クラウド移行ポリシーが設定されている一方で、ユーザーが指定した経過時間閾値があるシステム：ファイルは、ユーザーが指定した経過時間閾値に基づいて識別され、システム ポリシーは上書きされます。

- クラウドのないシステム：クリーニング可能なスペースの総量を判別するために使用される経過時間閾値をユーザーが指定する必須要件。

考慮すべきいくつかの追加ポイント：

- データ移動は、データ移動の適格性チェックと並列で実行することはできません。逆も同じです。
- 適格性チェックが実行中の場合は、アクティブ階層でのクリーニングを開始できません。逆も同じです。
- 適格性チェックが実行中の場合は、クラウド階層でのクリーニングを開始できません。逆も同じです。
- UNAVAIL イベントを受信したことで、適格性チェック操作に影響を与えることはありません。
- ファイルシステムが停止するかクラッシュした場合、適格性チェックは停止し、ファイルシステムが再び動作するようになったとき、自動で再開されません。

注

Data Domain System Manager GUI から適格性チェックを開始する用意はありません。

クラウド ユニットの構成

クラウド階層は最大 2 つのクラウド ユニットで構成され、各クラウド ユニットは 1 つのクラウド プロバイダにマッピングされます。このため、Data Domain システムごとに複数のクラウド プロバイダを有効化できます。Data Domain システムはクラウドに接続されている必要があり、サポートされているクラウド プロバイダのアカウントを持っている必要があります。

クラウド ユニットの構成には、次のステップが含まれます。

- ファイアウォールやプロキシの設定を含むネットワークの構成
- CA 証明書のインポート
- クラウド ユニットの追加

ファイアウォールとプロキシの設定

ネットワーク ファイアウォール ポート

- ポート 443（HTTPS）とポート 80（HTTP）は、双方向トラフィックを許可するために、クラウド プロバイダー ネットワークのエンドポイント IP とプロバイダー認証 IP の両方に対して開放する必要があります。
  たとえば、Amazon S3 の場合は、s3-ap-southeast-1.amazonaws.com と s3.amazonaws.com の両方に対してポート 80 とポート 443 をブロック解除し、双方向 IP トラフィックを許可する必要があります。

  注

  一部のパブリック クラウド プロバイダーは、エンドポイント アドレスと認証アドレスに IP 範囲を使用します。この場合、IP の変更に対応するために、プロバイダー側で使用される IP 範囲に対するブロックを解除する必要があります。

- リモートのクラウド プロバイダー デスティネーション IP とアクセス認証 IP のアドレス範囲は、ファイアウォールを介して許可する必要があります。
- ECS プライベート クラウドの場合は、ローカル ECS 認証と Web ストレージ（S3）アクセスの IP 範囲とポート 9020（HTTP）および 9021（HTTPS）は、ローカルのファイアウォールを介して許可する必要があります。

注

ECS プライベート クラウドのロード バランサー IP アクセスとポート ルールも構成する必要があります。

プロキシ設定

特定のサイズを超えるデータを拒否する既存のプロキシ設定がある場合は、最大 4.5 MB のオブジェクト サイズを許可するようにそれらの設定を変更する必要があります。

顧客のトラフィックがプロキシを介してルーティングされる場合、自己署名と CA 署名のプロキシ証明書をインポートする必要があります。詳細については「CA 証明書のインポート」を参照してください。

OpenSSL 暗号スイート

- 暗号 - ECDHE-RSA-AES256-SHA384、AES256-GCM-SHA384
- TLS バージョン：1.2

注

すべてのクラウド プロバイダとのデフォルトの通信は、強力な暗号を使用して開始されます。

サポートされるプロトコル

- HTTP
- HTTPS

注

すべてのパブリック クラウド プロバイダとデフォルトの通信は、セキュアな HTTP（HTTPS）で行われますが、デフォルトの設定を上書きして HTTP を使用することができます。

CA 証明書のインポート

ECS（Elastic Cloud Storage）、Virtustream Storage Cloud、Alibaba Cloud、AWS（Amazon Web Services）S3、Azure クラウド用のクラウド ユニットを追加する前に、CA 証明書をインポートする必要があります。

はじめに

AWS、Virtustream、Azure パブリック クラウド プロバイダの場合は、ルート CA 証明書を https://www.digicert.com/digicert-root-certificates.htm からダウンロードできます。

- AWS クラウド プロバイダの場合は、Baltimore CyberTrust ルート証明書をダウンロードします。
- Virtustream クラウド プロバイダの場合は、DigiCert High Assurance EV Root CA 証明書をダウンロードします。
- ECS の場合、ルート証明機関はお客様によって異なります。
  ECS のクラウド ストレージを実装するには、ロード バランサーが必要です。HTTPS エンドポイントを構成内でエンドポイントとして使用する場合は、ルート CA 証明書を必ずインポートしてください。詳細については、ロード バランサーのプロバイダーにお問い合わせください。
- Azure クラウド プロバイダの場合は、Baltimore CyberTrust ルート証明書をダウンロードします。
- S3 フレキシブル プロバイダーの場合は、ルート CA 証明書をインポートします。詳細については、S3 フレキシブル プロバイダーにお問い合わせください。

ダウンロードした証明書の拡張子が.crt である場合は、PEM でエンコードされた証明書への変換が必要な場合があります。その場合は、OpenSSL を使用して.crt 形式から.pem に変換します

（例：`openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out BaltimoreCyberTrustRoot.pem`）。

Alibaba の場合：

1. GlobalSign ルート R1 証明書を https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates からダウンロードします。
2. ダウンロードした証明書を PEM エンコード形式に変換します。この変換のための OpenSSL コマンドは次のとおりです。`openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`。
3. Data Domain システムに証明書をインポートします。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ツール バーで、［**Manage Certificates**］をクリックします。

   ［Manage Certificates for Cloud］ダイアログ ボックスが表示されます。
3. ［**Add**］をクリックします。
4. 次のいずれかのオプションを選択します。
   - ［**I want to upload the certificate as a .pem file.**］
     証明書を参照して選択します。
   - ［**I want to copy and paste the certificate text.**］
     - .pem ファイルの内容をコピー バッファにコピーします。
     - ダイアログ ボックスにバッファをペーストします。
5. ［**Add**］をクリックします。

ECS（Elastic Cloud Storage）用のクラウド ユニットの追加

Data Domain システムまたは DD VE インスタンスでは、Data Domain クラウド ユニットを構成するのに、ECS システムとの厳密な時刻同期を必要とします。Data Domain システムまたは DD VE インスタンス上と、ECS システム上で NTP を構成することでこの問題が解消されます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ［追加］をクリックします。

   ［Add Cloud Unit］ダイアログ ボックスが表示されます。
3. このクラウド ユニットの名前を入力します。入力できるのは英数字だけです。

   ［Add Cloud Unit］ダイアログの残りのフィールドは、クラウド プロバイダのアカウントに関連するものです。
4. ［**Cloud provider**］では、ドロップダウン リストから［**EMC Elastic Cloud Storage (ECS)**］を選択します。
5. パスワード テキストとしてプロバイダの［**Access key**］を入力します。
6. パスワード テキストとしてプロバイダの［**Secret key**］を入力します。
7. プロバイダの［**Endpoint**］を **`http://<ip/hostname>:<port>`**の形式で入力します。保護されたエンドポイントを使用している場合は、代わりに **`https`** を使用します。

注

ECS のクラウド ストレージを実装するには、ロード バランサーが必要です。

ECS では、デフォルトでは、HTTP の場合ポート 9020、HTTPS の場合 9021 で、S3 プロトコルを実行します。ロード バランサーを使用するとき、これらのポートは、HTTP の場合 80 に、HTTPS の場合 443 に、それぞれ再マップされることがあります。ネットワーク管理者に問い合わせて適切なポートを確認してください。

8. このプロバイダのファイアウォールを回避するために HTTP プロキシ サーバが必要な場合は、［**HTTP Proxy Server**］の［**Configure**］をクリックします。

   プロキシのホスト名、ポート、ユーザー名、パスワードを入力します。

   注

   クラウド ユニットを追加する前に、クラウド プロバイダ検証ツールを実行するオプションの手順があります。このツールは、事前チェック テストを実行して、実際のクラウド ユニットを追加する前に、すべての要件が満たされていることを確認します。

9. ［**Add**］をクリックします。

   ［File System］メイン ウィンドウに、新しいクラウド ユニットのサマリー情報と、クラウド ユニットを有効化および無効化するためのコントロールが表示されます。

Virtustream 用のクラウド ユニットの追加

Virtustream は、さまざまなストレージ クラスを提供します。「クラウド プロバイダの互換性マトリックス」は、http://compatibilityguide.emc.com:8080/CompGuideApp/にあり、サポートされているストレージ クラスに関する最新情報を提供します。

ストレージ クラスとリージョンに応じて、次のエンドポイントが Virtustream クラウド プロバイダによって使用されます。クラウド ユニットを構成する前に、DNS でこれらのホスト名を解決できることを確認します。

- s-us.objectstorage.io
- s-eu.objectstorage.io
- s-eu-west-1.objectstorage.io
- s-eu-west-2.objectstorage.io
- s-us-central-1.objectstorage.io

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ［追加］をクリックします。

   ［Add Cloud Unit］ダイアログ ボックスが表示されます。

3. このクラウド ユニットの名前を入力します。入力できるのは英数字だけです。

   ［Add Cloud Unit］ダイアログ ボックスの残りのフィールドは、クラウド プロバイダのアカウントに関連するものです。

4. ［**Cloud provider**］として、ドロップダウン リストから［**Virtustream Storage Cloud**］を選択します。
5. ドロップダウン リストからストレージ クラスを選択します。

6. ドロップダウン リストから、アカウントのタイプに対応する適切な地域を選択します。
7. パスワード テキストとしてプロバイダの［**Access key**］を入力します。
8. パスワード テキストとしてプロバイダの［**Secret key**］を入力します。
9. このプロバイダのファイアウォールを回避するために HTTP プロキシ サーバが必要な場合は、［**Configure**］の［**HTTP Proxy Server**］をクリックします。

   プロキシのホスト名、ポート、ユーザー名、パスワードを入力します。

   注

   クラウド ユニットを追加する前に、クラウド プロバイダ検証ツールを実行するオプションの手順があります。このツールは、事前チェック テストを実行して、実際のクラウド ユニットを追加する前に、すべての要件が満たされていることを確認します。

10. ［**Save**（保存）］をクリックします。

    ［File System］メイン ウィンドウに、新しいクラウド ユニットのサマリー情報と、クラウド ユニットを有効化および無効化するためのコントロールが表示されます。

Alibaba 用のクラウド ユニットの追加

リージョンは、オブジェクト レベルではなくバケット レベルで設定されます。したがって、バケットに含まれるすべてのオブジェクトは、同じリージョンに格納されます。リージョンは、バケットの作成時に指定され、作成後に変更することはできません。

表 197 Alibaba のリージョン

リージョン	ロケーション	リージョン名
中国本土のリージョン	中国東部 1（杭州）	oss-cn-hangzhou
	中国東部 2（上海）	oss-cn-shanghai
	中国北部 1（青島）	oss-cn-qingdao
	中国北部 2（北京）	oss-cn-beijing
	中国北部 3（張家口）	oss-cn-zhangjiakou
	中国北部 5（フフホト）	oss-cn-huhehaote
	中国南部 1（深圳）	oss-cn-shenzhen
国際リージョン	香港	oss-cn-hongkong
	米国西部 1（シリコンバレー）	oss-us-west-1
	米国東部 1（バージニア）	oss-us-east-1
	アジアパシフィック SE 1（シンガポール）	oss-ap-southeast-1
	アジア パシフィック SE 2（シドニー）	oss-ap-southeast-2
	アジアパシフィック SE 3（クアラルンプール）	oss-ap-southeast-3
	アジアパシフィック SE 5（ジャカルタ）	oss-ap-southeast-5

表 197 Alibaba のリージョン （続き）

リージョン	ロケーション	リージョン名
	アジア パシフィック NE 1（東京）	oss-ap-northeast-1
	アジア パシフィック SOU 1（ムンバイ）	oss-ap-south-1
	EU 中央 1（フランクフルト）	oss-eu-central-1
	中東 1（ドバイ）	oss-me-east-1

Alibaba Cloud ユーザー資格情報には、バケットの作成と削除、および作成したバケット内のファイルの追加、変更、削除を実行する権限が必要です。AliyunOSSFullAccess が推奨されますが、これらは最小要件です。

- ListBuckets
- GetBucket
- PutBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ［追加］をクリックします。

   ［Add Cloud Unit］ダイアログ ボックスが表示されます。
3. このクラウド ユニットの名前を入力します。入力できるのは英数字だけです。

   ［**Add Cloud Unit**］ダイアログ ボックスの残りのフィールドは、クラウド プロバイダのアカウントに関連するものです。
4. ［**Cloud provider**］ドロップダウン リストから、［**Alibaba Cloud**］を選択します。
5. ［**Storage class**］ドロップダウン リストから［**Standard**］または［**IA**］を選択します。
6. ［**Storage region**］ドロップダウン リストからリージョンを選択します。
7. パスワード テキストとしてプロバイダの［**Access key**］を入力します。
8. パスワード テキストとしてプロバイダの［**Secret key**］を入力します。
9. ファイアウォールでポート 443（HTTPS）がブロックされていないことを確認します。Alibaba クラウド プロバイダとの通信は、ポート 443 で行われます。
10. このプロバイダのファイアウォールを回避するために HTTP プロキシ サーバーが必要な場合は、［**Configure**］の［**HTTP Proxy Server**］をクリックします。

    プロキシのホスト名、ポート、ユーザー名、パスワードを入力します。

    注

    クラウド ユニットを追加する前に、クラウド プロバイダ検証ツールを実行するオプションの手順があります。このツールは、事前チェック テストを実行して、実際のクラウド ユニットを追加する前に、すべての要件が満たされていることを確認します。

11. ［**Add**］をクリックします。

    ［File System］メイン ウィンドウに、新しいクラウド ユニットのサマリー情報と、クラウド ユニットを有効化および無効化するためのコントロールが表示されます。

Amazon Web Services S3 用のクラウド ユニットの追加

AWS は、さまざまなストレージ クラスを提供します。「クラウド プロバイダの互換性マトリックス」は、http://compatibilityguide.emc.com:8080/CompGuideApp/にあり、サポートされているストレージ クラスに関する最新情報を提供します。

セキュリティを強化するために、Cloud Tier 機能では、AWS のすべてのリクエストにシグネチャ バージョン 4 を使用します。シグネチャ バージョン 4 の署名はデフォルトで有効化されています。

ストレージ クラスとリージョンに応じて、次のエンドポイントが AWS クラウド プロバイダによって使用されます。クラウド ユニットを構成する前に、DNS でこれらのホスト名を解決できることを確認します。

- s3.amazonaws.com
- s3-us-west-1.amazonaws.com
- s3-us-west-2.amazonaws.com
- s3-eu-west-1.amazonaws.com
- s3-ap-northeast-1.amazonaws.com
- s3-ap-southeast-1.amazonaws.com
- s3-ap-southeast-2.amazonaws.com
- s3-sa-east-1.amazonaws.com
- ap-south-1
- ap-northeast-2
- eu-central-1

注

中国地域はサポートされていません。

注

AWS ユーザー資格情報には、バケットの作成と削除、およびバケット内のファイルの追加、変更、削除を実行する権限が必要です。S3FullAccess が推奨されますが、これらは最小要件です。

- CreateBucket
- ListBucket
- DeleteBucket
- ListAllMyBuckets
- GetObject
- PutObject
- DeleteObject

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ［追加］をクリックします。

［Add Cloud Unit］ダイアログ ボックスが表示されます。

3. このクラウド ユニットの名前を入力します。入力できるのは英数字だけです。

   ［Add Cloud Unit］ダイアログ ボックスの残りのフィールドは、クラウド プロバイダのアカウントに関連するものです。

4. ［**Cloud provider**］ドロップダウン リストから、［**Amazon Web Services S3**］を選択します。
5. ドロップダウン リストからストレージ クラスを選択します。
6. ドロップダウン リストから適切な［**Storage region**］を選択します。
7. パスワード テキストとしてプロバイダの［**Access key**］を入力します。
8. パスワード テキストとしてプロバイダの［**Secret key**］を入力します。
9. ファイアウォールでポート 443（HTTPS）がブロックされていないことを確認します。AWS クラウド プロバイダとの通信は、ポート 443 で行われます。
10. このプロバイダーのファイアウォールを回避するために HTTP プロキシ サーバが必要な場合は、［**Configure**］の［**HTTP Proxy Server**］をクリックします。

    プロキシのホスト名、ポート、ユーザー名、パスワードを入力します。

    注

    クラウド ユニットを追加する前に、クラウド プロバイダ検証ツールを実行するオプションの手順があります。このツールは、事前チェック テストを実行して、実際のクラウド ユニットを追加する前に、すべての要件が満たされていることを確認します。

11. ［**Add**］をクリックします。

    ［File System］メイン ウィンドウに、新しいクラウド ユニットのサマリー情報と、クラウド ユニットを有効化および無効化するためのコントロールが表示されます。

Azure 用のクラウド ユニットの追加

Microsoft Azure は、さまざまなストレージ アカウント タイプを提供しています。「クラウド プロバイダの互換性マトリックス」は、http://compatibilityguide.emc.com:8080/CompGuideApp/にあり、サポートされているストレージ クラスに関する最新情報を提供します。

ストレージ クラスと地域に応じて、次のエンドポイントが Azure クラウド プロバイダによって使用されます。クラウド ユニットを構成する前に、DNS でこれらのホスト名を解決できることを確認します。

- Account name.blob.core.windows.net

アカウント名は、Azure クラウド プロバイダ コンソールから取得します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ［追加］をクリックします。

   ［Add Cloud Unit］ダイアログ ボックスが表示されます。

3. このクラウド ユニットの名前を入力します。入力できるのは英数字だけです。

   ［Add Cloud Unit］ダイアログ ボックスの残りのフィールドは、クラウド プロバイダのアカウントに関連するものです。

4. ［**Cloud provider**］ドロップダウン リストから、［**Microsoft Azure Storage**］を選択します。

5. ［**Account type**］では、［**Government**］または［**Public**］を選択します。
6. ドロップダウン リストからストレージ クラスを選択します。
7. ［**Account name**］にプロバイダのアカウント名を入力します。
8. パスワード テキストとしてプロバイダの［**Primary key**］を入力します。
9. パスワード テキストとしてプロバイダの［**Secondary key**］を入力します。
10. ファイアウォールでポート 443（HTTPS）がブロックされていないことを確認します。Azure クラウド プロバイダとの通信は、ポート 443 で行われます。
11. このプロバイダのファイアウォールを回避するために HTTP プロキシ サーバが必要な場合は、［**Configure**］の［**HTTP Proxy Server**］をクリックします。

    プロキシのホスト名、ポート、ユーザー名、パスワードを入力します。

    注

    クラウド ユニットを追加する前に、クラウド プロバイダ検証ツールを実行するオプションの手順があります。このツールは、事前チェック テストを実行して、実際のクラウド ユニットを追加する前に、すべての要件が満たされていることを確認します。

12. ［**Add**］をクリックします。

    ［File System］メイン ウィンドウに、新しいクラウド ユニットのサマリー情報と、クラウド ユニットを有効化および無効化するためのコントロールが表示されます。

Google Cloud Provider 向けのクラウド ユニットの追加

次の表に、データの格納に使用できるクラウド ストレージのロケーションを示します。

表 198 マルチリージョンのロケーション

マルチリージョン名	マルチリージョンの説明
アジア	アジアのデータ センター
US	米国のデータ センター
EU	欧州連合のデータ センター

表 199 リージョンのロケーション

リージョンのロケーション	ロケーション	リージョン名
北米	northamerica-northeast1	モントリオール
	us-central1	アイオワ
	us-east1	サウスカロライナ
	us-east4	北バージニア
	us-west1	オレゴン
	us-west2	ロサンゼルス
南米	southamerica-east1	サンパウロ
ヨーロッパ	europe-north1	フィンランド

表 199 リージョンのロケーション （続き）

リージョンのロケーション	ロケーション	リージョン名
	europe-west1	ベルギー
	europe-west2	London
	europe-west3	フランクフルト
	europe-west4	オランダ
アジア	asia-east1	台湾
	asia-northeast1	東京
	asia-south1	ムンバイ
	asia-southeast1	シンガポール
オーストラリア	australia-southeast1	シドニー

Google Cloud Provider ユーザー資格情報には、バケットの作成と削除、および作成したバケット内のファイルの追加、変更、削除を実行する権限が必要です。以下は最小要件です。

- ListBucket
- PutBucket
- GetBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

注

DD Cloud Tier はニアラインのみをサポートし、セットアップ時に自動的に選択されます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ［追加］をクリックします。

   ［Add Cloud Unit］ダイアログ ボックスが表示されます。
3. このクラウド ユニットの名前を入力します。入力できるのは英数字だけです。

   ［**Add Cloud Unit**］ダイアログ ボックスの残りのフィールドは、クラウド プロバイダのアカウントに関連するものです。
4. ［**Cloud provider**］として、ドロップダウン リストから［**Google Cloud Storage**］を選択します。
5. パスワード テキストとしてプロバイダの［**Access key**］を入力します。
6. パスワード テキストとしてプロバイダの［**Secret key**］を入力します。
7. ［**Storage class**］はデフォルトで［**Nearline**］として設定されます。

   マルチリージョンのロケーションが選択されている場合（アジア、EU、または米国）、ストレージ クラスとロケーション制約はニアライン マルチリージョンになります。他のすべてのリージョン ロケーションには、ニアライン リージョンとしてストレージ クラスが設定されています。

8. ［**Region**］を選択します。
9. ファイアウォールでポート 443（HTTPS）がブロックされていないことを確認します。Google Cloud Provider との通信は、ポート 443 で行われます。
10. このプロバイダのファイアウォールを回避するために HTTP プロキシ サーバーが必要な場合は、［**Configure**］の［**HTTP Proxy Server**］をクリックします。

    プロキシのホスト名、ポート、ユーザー名、パスワードを入力します。

    注

    クラウド ユニットを追加する前に、クラウド プロバイダ検証ツールを実行するオプションの手順があります。このツールは、事前チェック テストを実行して、実際のクラウド ユニットを追加する前に、すべての要件が満たされていることを確認します。

11. ［**Add**］をクリックします。

    ［File System］メイン ウィンドウに、新しいクラウド ユニットのサマリー情報と、クラウド ユニットを有効化および無効化するためのコントロールが表示されます。

S3 フレキシブル プロバイダ クラウド ユニットの追加

クラウド階層機能では、S3 フレキシブル プロバイダーの構成オプションで追加の認定 S3 クラウド プロバイダーがサポートされます。

S3 フレキシブル プロバイダ オプションは、標準および標準低頻度アクセス ストレージ クラスをサポートします。エンドポイントは、クラウド プロバイダ、ストレージ クラス、リージョンに応じて異なります。クラウド ユニットを構成する前に、DNS でこれらのホスト名を解決できることを確認します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. ［追加］をクリックします。

   ［Add Cloud Unit］ダイアログ ボックスが表示されます。
3. このクラウド ユニットの名前を入力します。入力できるのは英数字だけです。

   ［Add Cloud Unit］ダイアログ ボックスの残りのフィールドは、クラウド プロバイダのアカウントに関連するものです。
4. ［**Cloud provider**］では、ドロップダウン リストから［**Flexible Cloud Tier Provider Framework for S3**］を選択します。
5. パスワード テキストとしてプロバイダの［**Access key**］を入力します。
6. パスワード テキストとしてプロバイダの［**Secret key**］を入力します。
7. 適切な［**Storage region**］を指定します。
8. プロバイダの［**Endpoint**］を `http://<ip/hostname>:<port>`の形式で入力します。保護されたエンドポイントを使用している場合は、代わりに `https` を使用します。
9. ［**Storage class**］では、ドロップダウン リストから適切なストレージ クラスを選択します。
10. ファイアウォールでポート 443（HTTPS）がブロックされていないことを確認します。S3 クラウド プロバイダとの通信は、ポート 443 で行われます。
11. このプロバイダのファイアウォールを回避するために HTTP プロキシ サーバが必要な場合は、［**Configure**］の［**HTTP Proxy Server**］をクリックします。

    プロキシのホスト名、ポート、ユーザー名、パスワードを入力します。

注

クラウド ユニットを追加する前に、クラウド プロバイダ検証ツールを実行するオプションの手順があります。このツールは、事前チェック テストを実行して、実際のクラウド ユニットを追加する前に、すべての要件が満たされていることを確認します。

12. ［**Add**］をクリックします。

［File System］メイン ウィンドウに、新しいクラウド ユニットのサマリー情報と、クラウド ユニットを有効化および無効化するためのコントロールが表示されます。

クラウド ユニットまたはクラウド プロファイルの修正

クラウド ユニットの資格情報、S3 フレキシブル プロバイダ名、またはクラウドのプロファイルの詳細を変更します。

クラウド ユニットの認証情報の変更

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. 変更する認証情報を持つクラウド ユニットの鉛筆アイコンをクリックします。

   ［Modify Cloud Unit］ダイアログ ボックスが表示されます。
3. ［**Account name**］に新しいアカウント名を入力します。
4. ［**Access key**］に、新しいプロバイダー アクセス キーをパスワード テキストとして入力します。

   注

   ECS 環境では、アクセス キーを変更することはできません。
5. ［**Secret key**］に、新しいプロバイダー秘密キーをパスワード テキストとして入力します。
6. ［**Primary key**］に、新しいプロバイダー プライマリ キーをパスワード テキストとして入力します。

   注

   プライマリ キーの変更は、Azure 環境でのみ行うことができます。
7. このプロバイダーのファイアウォールを回避するために HTTP プロキシ サーバが必要な場合は、［**Configure**］の［**HTTP Proxy Server**］をクリックします。
8. ［**OK**］をクリックします。

S3 フレキシブル プロバイダ名を変更します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Cloud Units**］を選択します。
2. 変更する名前を持つ S3 フレキシブル クラウド ユニットの鉛筆アイコンをクリックします。

   ［Modify Cloud Unit］ダイアログ ボックスが表示されます。
3. ［**S3 Provider Name**］に新しいプロバイダ名を入力します。

4. ［**OK**］をクリックします。

CLI によるクラウド プロファイルの変更

手順

1. コマンド `cloud profile modify` を実行してクラウド プロファイルの詳細を変更します。システムで、クラウド プロファイルの個々の詳細を変更するよう求められます。

   Virtustream、AWS S3、または Azure プロファイルの場合は、このコマンドを実行して既存のクラウド プロファイルにストレージ クラスを追加します。

   次に示すように、変更可能なプロファイルの詳細はクラウド プロバイダーによって異なります。

   - Alibaba Cloud は、アクセス キーと秘密キーの変更をサポートしています。
   - AWS S3 は、アクセス キーと秘密キーの変更をサポートしています。
   - Azure は、アクセス キー、秘密キー、プライマリ キーの変更をサポートしています。
   - ECS は、秘密キーの変更をサポートしています。
   - Virtustream は、アクセス キーと秘密キーの変更をサポートしています。
   - S3 フレキシブルは、アクセス キー、秘密キー、プロバイダ名の変更をサポートしています。

クラウド ユニットの削除

この操作の結果、削除することを選択したクラウド ユニットにあるすべてのデータが失われます。クラウド ユニットを削除する前に必ずすべてのファイルを削除してください。

はじめに

- クラウドへのデータ移動が実行されているかどうかをチェックします（CLI コマンド：data-movement status）。実行されている場合は、「data-movement stop」CLI コマンドを使用してデータ移動を停止します。
- このクラウド ユニットのクラウドのクリーニングが実行されているかどうかをチェックします（CLI コマンド：cloud clean status）。実行されている場合は、「cloud clean」CLI コマンドを使用してクラウドのクリーニングを停止します。
- このクラウド ユニットのデータ移動ポリシーが構成されているかどうかをチェックします（CLI コマンド：data-movement policy show）。構成されている場合は、「data-movement policy reset」CLI コマンドを使用してこのポリシーを削除します。

手順

1. 次の CLI コマンドを使用してクラウド ユニット内のファイルを識別します。

   ```
   # filesys report generate file-location
   ```

2. 削除するクラウド ユニットにあるファイルを削除します。
3. 次の CLI コマンドを使用してクラウドのクリーニングを実行します。

   ```
   # cloud clean start unit-name
   ```

   クリーニングが完了するまで待機します。クラウド ユニットに存在するデータの量によってはクリーニングに時間がかかる場合があります。
4. ファイル システムを無効化します。
5. 次の CLI コマンドを使用してクラウド ユニットを削除します。

```
# cloud unit del unit-name
```

内部的には、これによってクラウド ユニットは DELETE_PENDING としてマークされます。

6. 次の CLI コマンドを使用してクラウド ユニットが DELETE_PENDING 状態であることを確認します。

```
# cloud unit list
```

7. ファイル システムを有効にします。

ファイル システムでは、このクラウド ユニットのクラウドにあるバケットから残りのすべてのオブジェクトを削除してからバケットを削除する処理手順をバックグラウンドで開始します。これらのバケットに残っているオブジェクトの数によっては、このプロセスに時間がかかることがあります。バケットのクリーンアップが完了するまで、このクラウド ユニットは Data Domain システム上のスロットを使用し続けます。このため両方のスロットが占有されている場合に新しいクラウド ユニットの作成が妨げられる可能性があります。

8. 次の CLI コマンドを使用して、状態を定期的に確認します。

```
# cloud unit list
```

バックグラウンドでクリーンアップが実行されている間、状態は DELETE_PENDING のままです。

9. すべての対応するバケットが削除され、関連付けられているスペースが解放されたことをクラウド プロバイダの S3 ポータルから確認します。
10. 必要な場合は、影響を受ける MTree のデータ移動ポリシーを再構成し、データ移動を再開します。

結果

この処理手順を完了することが難しい場合は、サポートにお問い合わせください。

データの移動

データは、個々のデータ移動ポリシーの設定に従ってアクティブ階層からクラウド階層に移動します。ポリシーは、MTree 単位で設定します。データ移動は、手動で開始することも、スケジュールを使用して自動的に開始することもできます。

MTree へのデータ移動ポリシーの追加

ファイルは、最終変更日に基づいてアクティブ階層からクラウド階層に移されます。データの整合性を保つため、このとき、ファイル全体が移されます。［データ移動ポリシー］では、ファイルの経過期間の閾値、経過期間の範囲、デスティネーションを設定します。

注

/backup MTree に対するデータ移動ポリシーは構成できません。

手順

1. ［**Data Management**］ > ［**MTree**］を選択します。
2. 上部のパネルで、データ移動ポリシーの追加先となる MTree を選択します。
3. ［**Summary**］タブをクリックします。
4. ［**Data Movement Policy**］で、［**Add**］をクリックします。

5. ［**File Age in Days**］で、ファイルの経過期間の閾値（［**Older than**］）を設定し、必要に応じて経過期間の範囲（［**Younger than**］）を設定します。

   注

   ［**Older than**］の最小日数は 14 です。非統合型バックアップ アプリケーションの場合、クラウド階層に移動されるファイルには直接アクセスできません。アクセスするには、アクティブ階層にリコールする必要があります。したがって、クラウド階層に移動したファイルにアクセスする必要性を排除できるように、または最小限に抑えることができるように経過時間の閾値を選択します。

6. ［**Destination**］で、デスティネーション クラウド ユニットを指定します。
7. ［追加］をクリックします。

手動データ移動

データ移動を手動で停止および開始できます。有効なデータ移動ポリシーが適用されている MTree には、移動対象ファイルが存在します。

手順

1. ［**Data Management**］ > ［**File System**］を選択します。
2. ページの下部で、［**Show Status of File System Services**］をクリックします。

   次のステータス アイテムが表示されます。

   - ファイル システム
   - 物理容量の測定
   - データの移動
   - アクティブ階層のクリーニング

3. ［**Data Movement**］で、［**Start**］をクリックします。

自動データ移動

スケジュールとスロットルを使用すると、データを自動的に移動できます。スケジュールは日単位、週単位、月単位のいずれかです。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Settings**］を選択します。
2. ［**Data Movement**］タブをクリックします。
3. スロットルとスケジュールを設定します。

   注

   スロットルは、Data Domain の内部プロセス用のリソースを調整するためのものであり、ネットワーク帯域幅には影響しません。

注

クラウド階層のデータ移動を実行するときにクラウド ユニットにアクセスできない場合、そのクラウド ユニットはその実行ではスキップされます。クラウド ユニットが使用可能になった場合、そのクラウド ユニットのデータ移動は次回の実行で行われます。データ移動のスケジュールでは、2 つの実行間の期間を決定します。クラウド ユニットが使用可能になり、スケジュール設定された次回の実行まで待つことができない場合は、データ移動を手動で開始できます。

Cloud Tier からのファイルのリコール

非統合型バックアップ アプリケーションの場合は、データをリストアする前に、アクティブ階層にデータをリコールする必要があります。クラウド ベースのバックアップをリストアする前に、バックアップ管理者がリコールをトリガーするか、バックアップ アプリケーションがリコールを実行する必要があります。ファイルがリコールされたら、経過時間がリセットされて再び 0 から開始され、ファイルは経過時間ポリシー セットに基づいて使用可能になります。ファイルは、同じ MTree にのみリコールできます。統合されたアプリケーションは、ファイルを直接リストアできます。

注

MTree レプリケーション コンテキストでは、ファイルはデスティネーション MTree では読み取り専用です。

注

ファイルがスナップショットにのみ存在する場合は、直接リコールできません。スナップショット内のファイルをリコールするには、fastcopy を使用してスナップショットからアクティブな MTree にファイルをコピーして戻したうえで、クラウドからファイルをリコールします。ファイルはクラウドからアクティブな MTree にのみリコールできます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Summary**］を選択します。
2. 次のいずれかを実行します。
   - ［Space Usage］パネルの［Cloud Tier］セクションで［**Recall**］をクリックします。
   - 画面の下部にある［File System status］パネルを展開し［**Recall**］をクリックします。

   注

   ［**Recall**］リンクは、クラウド ユニットが作成されており、データがある場合にのみ使用できます。
3. ［Recall File from Cloud］ダイアログで、次のように、リコールするファイルの正確なファイル名（ワイルドカードを使用しない）およびフル パスを入力します。`/data/col1/mt11/file1.txt`。［**Recall**］をクリックします。
4. リコールのステータスを確認するには、次のいずれかを実行します。
   - ［Space Usage］パネルの［Cloud Tier］セクションで［**Details**］をクリックします。
   - 画面の下部にある［File System status］パネルを展開し［**Details**］をクリックします。

   ［Cloud File Recall Details］ダイアログが表示され、ファイル パス、クラウド プロバイダ、リコールの進行状況、および転送されたデータの量が表示されます。リコール中にリカバリ不可

能なエラーがあった場合は、エラー メッセージが表示されます。詳細と可能な対応処置を含むツールのヒントを表示するにはエラー メッセージにカーソルを合わせます。

結果

ファイルがアクティブ階層にリコールされたら、データをリストアできます。

注

非統合型アプリケーションの場合は、クラウド階層からアクティブ階層にファイルがリコールされたら、最低 14 日間が経過しなければそのファイルをデータ移動の対象にすることはできません。14 日間が経過すると、通常のデータ移動処理がファイルに対して発生します。このファイルは、今度は mtime ではなく ptime が検査されるので、クラウドに再度移動するために経過時間閾値または経過時間範囲を待たなければならなくなりました。この制限は、統合されたアプリケーションには適用されません。

注

データ移動の場合、非統合型アプリケーションは、クラウド階層に移行するファイルを指定する経過時間ベースのデータ移動ポリシーを Data Domain システムに構成します。このポリシーは、MTree 内のすべてのファイルに同様に適用されます。統合されたアプリケーションは、アプリケーションで管理されるデータ移動ポリシーを使用します。このポリシーでは、クラウド階層に移行するファイルを個別に指定できます。

CLI を使用したクラウド階層からのファイルのリコール

非統合型バックアップ アプリケーションの場合は、データをリストアする前に、アクティブ階層にデータをリコールする必要があります。クラウド ベースのバックアップをリストアする前に、バックアップ管理者がリコールをトリガーするか、バックアップ アプリケーションがリコールを実行する必要があります。ファイルがリコールされたら、経過時間がリセットされて再び 0 から開始され、ファイルは経過時間ポリシー セットに基づいて使用可能になります。ファイルは、ソース MTree にのみリコールできます。統合されたアプリケーションは、ファイルを直接リコールできます。

注

ファイルがスナップショットにのみ存在する場合は、直接リコールできません。スナップショット内のファイルをリコールするには、fastcopy を使用してスナップショットからアクティブな MTree にファイルをコピーして戻したうえで、クラウドからファイルをリコールします。ファイルはクラウドからアクティブな MTree にのみリコールできます。

手順

1. 次のコマンドを使用してファイルの場所を確認します。
   ```
   filesys report generate file-location [path {<path-name> | all}] [output-file <filename>]
   ```
   パス名はファイルまたはディレクトリです。ディレクトリの場合、ディレクトリ内のすべてのファイルが表示されます。
   ```
   Filename                    Location
   --------                    --------
   /data/col1/mt11/file1.txt   Cloud Unit 1
   ```

2. 次のコマンドを使用してファイルをリコールします。
   ```
   data-movement recall path <path-name>
   ```
   このコマンドは非同期であり、リコールを開始します。
   ```
   data-movement recall path /data/col1/mt11/file1.txt
   Recall started for "/data/col1/mt11/file1.txt".
   ```

3. リコールのステータスを監視するには次のコマンドを使用します。
   ```
   data-movement status [path {[pathname]  | all | [queued]
   [running] [completed] [failed]} | to-tier cloud | all]
   ```

   ```
   data-movement status path /data/col1/mt11/file1.txt
   Data-movement recall:
   ---------------------
   Data-movement for "/data/col1/mt11/file1.txt": phase 2 of 3
   (Verifying)
   80% complete; time: phase  XX:XX:XX total  XX:XX:XX
   Copied (post-comp): XX XX, (pre-comp) XX XX
   ```

   ステータスでリコールが特定のパスに対して実行されていないことが示された場合は、リコールが完了しているか、または失敗した可能性があります。

4. 次のコマンドを使用してファイルの場所を確認します。
   ```
   filesys report generate file-location [path {<path-name> |
   all}] [output-file <filename>]
   ```

   ```
   Filename                    Location
   --------                    --------
   /data/col1/mt11/file1.txt   Active
   ```

結果

ファイルがアクティブ階層にリコールされたら、データをリストアできます。

注

非統合型アプリケーションの場合は、クラウド階層からアクティブ階層にファイルがリコールされたら、最低 14 日間が経過しなければそのファイルをデータ移動の対象にすることはできません。14 日間が経過すると、通常のデータ移動処理がファイルに対して発生します。この制限は、統合されたアプリケーションには適用されません。

注

データ移動の場合、非統合型アプリケーションは、クラウド階層に移行するファイルを指定する経過時間ベースのデータ移動ポリシーを Data Domain システムに構成します。このポリシーは、MTree 内のすべてのファイルに同様に適用されます。統合されたアプリケーションは、アプリケーションで管理されるデータ移動ポリシーを使用します。このポリシーでは、クラウド階層に移行するファイルを個別に指定できます。

クラウド階層からのダイレクト リストア

ダイレクト リストアにより、統合されていないアプリケーションでもアクティブ階層を経由せず、クラウド階層からファイルを直接読み込めるようになります。

ダイレクト リストアを使用する際に考慮すべき重要な点は次のとおりです。

- ダイレクト リストアは統合アプリケーションを必要とせず、非統合アプリケーションに対して透過的です。
- クラウド階層からの読み取りの際は、アクティブ階層への最初のコピーは必要ありません。
- クラウド階層からの直接読み取りの追跡にヒストグラムや統計量を使用できます。
- ダイレクト リストアは ECS クラウド プロバイダでのみサポートされます。
- アプリケーションがクラウド階層の遅延の影響を受けます。
- クラウド階層からの直接読み取りは、帯域幅の最適化がなされていません。
- ダイレクト リストアでは、少ないジョブ数しかサポートしません。

クラウド階層についての情報が不要であり、かつクラウド上のファイルの頻繁なリストアが不要な非統合アプリケーションにおいて、ダイレクト リストアは有用です。

コマンド ライン インターフェイス（CLI）による DD Cloud Tier の構成

Data Domain コマンド ライン インターフェイスを使用して DD Cloud Tier を構成できます。

手順

1. アクティブ階層とクラウド階層の両方のストレージを構成します。動作条件として、アクティブ階層およびクラウド階層の両方で適切な容量のライセンスがインストールされている必要があります。

   a. CLOUDTIER-CAPACITY および CAPACITY-ACTIVE の機能のライセンスがインストールされていることを確認します。ELMS ライセンスを確認するには、次のように入力します。

   ```
   # elicense show
   ```

   ライセンスがインストールされていない場合は、`elicense update` コマンドを使用してライセンスをインストールします。コマンドを入力し、次のプロンプトの後で、ライセンス ファイルの内容をペーストします。ペースト後に、キャリッジ リターンがあることを確認し、**Ctrl+D** を押して保存します。ライセンスを置き換えるようプロンプトが表示されたら、［yes］と答えます。ライセンスが適用され、表示されます。

   ```
   # elicense update
   Enter the content of license file and then press Control-D,
   or press Control-C to cancel.
   ```

   b. 使用可能なストレージを表示します。

   ```
   # storage show all# disk show state
   ```

   c. アクティブ階層にストレージを追加します。

   ```
   # storage add enclosures <enclosure no> tier active
   ```

   d. クラウド階層にストレージを追加します。

   ```
   # storage add enclosures <enclosure no> tier cloud
   ```

2. 証明書をインストールします。

   クラウド プロファイルを作成する前に、関連づけられた証明書をインストールする必要があります。詳細については、証明書のインポート（590 ページ）を参照してください。

   AWS、Virtustream、Azure パブリック クラウド プロバイダーの場合は、ルート CA 証明書を https://www.digicert.com/digicert-root-certificates.htm からダウンロードできます。

   - AWS または Azure クラウド プロバイダの場合は、Baltimore CyberTrust ルート証明書をダウンロードします。
   - Alibaba の場合は、Alibaba が https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates から GlobalSign ルート R1 証明書をダウンロードします。
   - Virtustream クラウド プロバイダの場合は、DigiCert High Assurance EV Root CA 証明書をダウンロードします。
   - ECS の場合、ルート証明機関はお客様によって異なります。詳細については、ロード バランサーのプロバイダにお問い合わせください。

ダウンロードした証明書ファイルには、拡張子.crt が付いています。openssl がインストールされている任意の Linux または Unix システム上で openssl を使用して、ファイルを.crt 形式から.pem に変換します。

```
$openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
-out DigiCertHighAssuranceEVRootCA.pem
```

```
$openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
BaltimoreCyberTrustRoot.pem
```

```
# adminaccess certificate import ca application cloud
Enter the certificate and then press Control-D, or press
Control-C to cancel.
```

3. クラウドへのデータ移動のために Data Domain システムを構成するには、まず、「クラウド」機能を有効化し、まだ設定されていない場合は、システム パスフレーズを設定する必要があります。

```
# cloud enable
Cloud feature requires that passphrase be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
Encryption is recommended on the cloud tier.
    Do you want to enable encryption? (yes|no) [yes]:
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
```

4. クラウド プロバイダの認証情報を使用して、クラウド プロファイルを構成します。プロンプトおよび変数は、プロバイダによって異なります。

```
# cloud profile add <profilename>
```

注

セキュリティ上の理由から、このコマンドでは、入力するアクセス キー/シークレット キーは表示されません。

プロバイダを選択します。

```
Enter provider name (alibabacloud|aws|azure|ecs|google|
s3_flexible|virtustream)
```

- Alibaba Cloud では、アクセス キー、シークレット キー、ストレージ クラス、リージョンが必要です。
- AWS S3 では、アクセス キー、シークレット キー、ストレージ クラス、リージョンが必要です。
- Azure では、アカウント名（アカウントが Azure Government アカウントであるかどうかを問わない）、プライマリ キー、セカンダリ キー、ストレージ クラスが必要です。
- ECS では、アクセス キー、シークレット キー、エンドポイントを入力する必要があります。
- Google Cloud Platform には、アクセス キー、シークレット キー、およびリージョンが必要です。（ストレージ クラスはニアラインです）。
- S3 フレキシブル プロバイダでは、プロバイダ名、アクセス キー、シークレット キー、リージョン、エンドポイント、ストレージ クラスが必要です。
- Virtustream では、アクセス キー、シークレット キー、ストレージ クラス、リージョンが必要です。

各プロファイルの追加の最後に、プロキシを設定するかどうか質問されます。設定する場合は、次の値が必要です。proxy hostname、proxy port、proxy username、proxy password。

5. クラウド プロファイル構成を確認します。

```
# cloud profile show
```

6. まだ作成されていない場合は、アクティブ階層のファイル システムを作成します。

```
# filesys create
```

7. ファイル システムを有効化します。

```
# filesys enable
```

8. クラウド ユニットを構成します。

```
# cloud unit add unitname profile profilename
```

`cloud unit list` コマンドを使用して、クラウド ユニットをリストします。

9. 必要に応じて、クラウド ユニットの暗号化を構成します。

   a. ENCRYPTION ライセンスがインストールされていることを確認します。

   ```
   # elicense show
   ```

   b. クラウド ユニットの暗号化を有効化します。

   ```
   # filesys encryption enable cloud-unit unitname
   ```

   c. 暗号化ステータスを確認します。

   ```
   # filesys encryption status
   ```

10. 1 つ以上の MTree を作成します。

```
# mtree create /data/col1/mt11
```

11. DD Cloud Tier の設定を確認します。

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED
```

```
S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. この MTree のファイル移行ポリシーを構成します。このコマンドでは、複数の MTree を指定できます。ポリシーは、経過時間の閾値または範囲に基づいて作成できます。

    a. 経過時間の閾値（指定した時間経過より古いファイルをクラウドに移行）を構成するには、次のようにします。

    ```
    # data-movement policy set age-threshold age_in_days to-tier
    cloud cloud-unit unitname mtrees mtreename
    ```

    b. 時間範囲（指定した経過時間の範囲に含まれるファイルのみの移行）を構成するには、次のようにします。

    ```
    # data-movement policy set age-range min-age age_in_days max-
    age age_in_days to-tier cloud cloud-unit unitname mtrees
    mtreename
    ```

13. ファイル システムをエクスポートし、クライアントからファイル システムをマウントし、アクティブ階層にデータを取得します。データ移行の対象となるように、取得したファイルの変更日を変更します。（データ移動ポリシーを構成するときに指定した経過時間の閾値の値よりも前の日付を設定）。
14. 経過時間に達したファイルのファイル移行を開始します。このコマンドでも、複数の MTree を指定できます。

    ```
    # data-movement start mtrees mtreename
    ```

    データ移動のステータスを確認するには、次のようにします。

    ```
    # data-movement status
    ```

    また、データ移動の進行状況を監視することもできます。

    ```
    # data-movement watch
    ```

15. ファイル移行が機能してファイルがクラウド階層に格納されたことを確認します。

    ```
    # filesys report generate file-location path all
    ```

16. ファイルをクラウド階層に移行した後で、ファイルを直接読み取ることはできません（実行しようとするとエラーが発生します）。ファイルは、アクティブ階層にリコールすることのみ可能です。アクティブ階層にファイルをリコールするには、次のようにします。

    ```
    # data-movement recall path pathname
    ```

DD クラウド ユニットの暗号化の構成

暗号化は、Data Domain システム、アクティブ階層、クラウド ユニットの 3 つのレベルで有効化できます。アクティブ階層の暗号化は、Data Domain システムに対する暗号化が有効化されている場

合にのみ適用できます。クラウド ユニットには、暗号化を有効にするための別個のコントロールがあります。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**DD Encryption**］を選択します。

   注

   暗号化ライセンスがシステムに存在しない場合は、［Add Licenses］ページが表示されます。

2. ［DD Encryption］パネルで、次のいずれかを実行します。
   - ［クラウド ユニット **x**］の暗号化を有効化するには、［**Enable**］をクリックします。
   - ［クラウド ユニット **x**］の暗号化を無効化するには、［**Disable**］をクリックします。

   注

   暗号化を有効にするために、セキュリティ担当者の認証情報の入力を求められます。

3. セキュリティ担当者の［**Username**］と［**Password**］を入力します。必要に応じて、［**Restart file system now**］をオンにします。
4. 必要に応じて、［**Enable**］または［**Disable**］をクリックします。
5. ［File System Lock］パネルで、ファイル システムをロックまたはロック解除します。
6. ［Key Management］パネルで、［**Configure**］をクリックします。
7. ［Change Key Manager］ダイアログ ボックスで、セキュリティ担当者の認証情報キー マネージャを構成します。

   注

   クラウド暗号化は、Data Domain Embedded Key Manager を通してのみ許可できます。外部キー マネージャはサポートされません。

8. ［**OK**］をクリックします。
9. ［DD Encryption Keys］パネルを使用して、暗号化キーを構成できます。

システムが失われた場合に必要な情報

Cloud Tier を Data Domain システム上で構成したら、システムに関する次の情報を記録し、Data Domain システムとは別の安全な場所に保存します。この情報は、Data Domain システムが失われた場合に、Cloud Tier データをリカバリするために必要になります。

注

このプロセスは緊急の場合のみを対象としており、Data Domain のエンジニアリング スタッフの多大な時間と労力を必要とします。

- 元の Data Domain システムのシリアル番号
- 元の Data Domain システムのシステム パスフレーズ

- 元の Data Domain システムの DD OS バージョン番号
- Cloud Tier のプロファイルと構成情報

クラウド階層での DD Replicator の使用

コレクション レプリケーションは、クラウド階層対応 Data Domain システムではサポートされていません。

ディレクトリ レプリケーションは/backup MTree でのみ機能し、この MTree はクラウド階層に割り当てることはできません。そのため、ディレクトリ レプリケーションはクラウド階層の影響を受けません。

管理ファイル レプリケーションと MTree レプリケーションは、クラウド階層対応 Data Domain システムでサポートされています。クラウド階層対応システムは一方でも両方でもかまいません。ソース システムがクラウド階層対応である場合、ファイルがすでにクラウド階層に移行されていれば、データはクラウドから読み取る必要があります。クラウド階層が有効になっている場合でも、レプリケートされるファイルは最初にデスティネーション システムのアクティブ階層に配置されます。ファイルは、クラウド階層からソース MTree のアクティブ階層にのみリコールできます。デスティネーション MTree へのファイルのリコールは許可されません。

注

DD OS 5.6 または 5.7 を実行しているソース システムから MTree レプリケーションを使用してクラウド階層対応システムにレプリケートする場合は、クラウド階層対応システムにレプリケート可能なリリースにソース システムをアップグレードする必要があります。詳細については、「DD OS リリース ノート」のシステム要件を参照してください。

注

クラウド階層内のファイルは、仮想合成操作のベース ファイルとして使用することはできません。増分永続または合成フル バックアップでは、ファイルが新しいバックアップの仮想合成で使用される場合、それらのファイルがアクティブ階層に存在することを確認する必要があります。

クラウド階層での DD VTL（仮想テープ ライブラリ） の使用

クラウド階層と DD VTL で構成されたシステムでは、VTL ヴォールトとしてのクラウド ストレージの使用をサポートします。DD VTL テープをクラウドで使用するには、まずクラウド ストレージのライセンス登録と構成をした後で、VTL のヴォールト ロケーションとしてクラウド ストレージを選択します。

クラウド階層での VTL の使用に関する詳細は、DD VTL テープからクラウドへ（371 ページ）を参照してください。

DD Cloud Tier の容量消費グラフの表示

クラウド階層の消費量に関する統計情報を表示するために、Space Usage、Consumption、Daily Written の 3 種類のグラフが用意されています。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Charts**］を選択します。
2. ［**Chart**］で、次のいずれかを選択します。
   - 領域の使用状況
   - Consumption

- Daily Written

3. ［**Scope**］で、［**Cloud Tier**］を選択します。
   - ［Space Usage］タブに、一定期間の使用容量が MiB 単位で表示されます。期間は、1 週間、1 か月、3 か月、1 年間、またはすべて）から選択できます。データは、圧縮前使用（青）、圧縮後使用（赤）、圧縮率（緑）として色分け表示されます。
   - ［Consumption］タブには、圧縮後の使用済みストレージ容量と一定期間にわたる圧縮率が表示されます。この情報を利用することで消費トレンドを分析できます。期間は、1 週間、1 か月、3 か月、1 年間、またはすべて）から選択できます。データは、容量（青）、圧縮後使用（赤）、圧縮率（緑）、クリーニング（オレンジ）、データ移動（紫）として色分け表示されます。
   - ［Daily Written］タブには、1 日あたりの書き込み量が表示されます。期間は、1 週間、1 か月、3 か月、1 年間、またはすべて）から選択できます。データは、圧縮前書き込み（青）、圧縮後使用（赤）、合計圧縮率（緑）として色分け表示されます。

DD Cloud Tier のログ

DD Cloud Tier の構成や操作で、何らかの種類の障害が発生した場合、システムは自動的に、障害の発生時に関連付けられたタイムスタンプ付きのフォルダを作成します。

ログにアクセスするための `/ddvar/log/debug` ディレクトリをマウントします。

注

`log list view` コマンドの出力では、DD Cloud Tier の障害に対して作成された詳細ログ ファイルの一部は一覧表示されません。

CLI（コマンド ライン インターフェイス）による DD Cloud Tier の削除

Data Domain コマンド ライン インターフェイスを使用して DD Cloud Tier 構成を削除できます。

はじめに

システムから DD Cloud Tier 構成を削除する前に、クラウド ユニット内のすべてのファイルを削除してください。`filesys report generate file-location path all output-file file_loc` コマンドを実行してクラウド ユニット内のファイルを特定し、MTree の NFS マウント ポイントからそれらを削除します。

注

前述のコマンドは、`/ddr/var/`ディレクトリにレポート `file_loc` を作成します。

手順

1. ファイル システムを無効化します。

```
# filesys disable

This action will disable the file system.
Applications may experience interruptions
while the file system is disabled.
    Are you sure? (yes|no) [no]: yes

ok, proceeding.
```

```
Please wait.............
The filesystem is now disabled.
```

2. システム上のクラウド ユニットをリストします。

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Active
cloud_unit-2   cloudProfile2  Active
------------   ------------   ------
```

3. クラウド ユニットを個別に削除します。

```
# cloud unit del cloud_unit-1

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-1".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-1"
Cloud unit 'cloud_unit-1' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.

# cloud unit del cloud_unit-2

This command irrevocably destroys all data
 in the cloud unit "cloud_unit-2".
    Are you sure? (yes|no) [no]: yes

ok, proceeding.

Enter sysadmin password to confirm:

Destroying cloud unit "cloud_unit-2"
Cloud unit 'cloud_unit-2' deleted. The data in the cloud will be deleted asynchronously
on the filesystem startup.
```

4. 削除操作が進行中であることを確認します。

```
# cloud unit list
Name           Profile        Status
------------   ------------   ------
cloud_unit-1   cloudProfile   Delete-Pending
cloud_unit-2   cloudProfile2  Delete-Pending
------------   ------------   ------
```

5. ファイル システムを再起動します。

```
# filesys enable
Please wait.....................................
The filesystem is now enabled.
```

6. `cloud unit list` コマンドを実行して、どちらのクラウド ユニットも表示されないことを確認します。

   1 つまたは両方のクラウド ユニットがまだステータス `Delete-Pending` で表示される場合はサポートに問い合わせます。

7. DD Cloud Tier に割り当てられているディスク エンクロージャを特定します。

```
# storage show tier cloud

Cloud tier details:
```

```
Disk   Disks               Count   Disk     Additional
Group                              Size     Information
------ ------------------- ------  -------- ------------
dgX    2.1-2.15, 3.1-3.15  30      3.6 TiB
------ ------------------- ------  -------- ------------
Current cloud tier size: 0.0 TiB
Cloud tier maximum capacity: 108.0 TiB
```

8. DD Cloud Tier から、ディスク エンクロージャを削除します。

```
# storage remove enclosures 2, 3

Removing enclosure 2...Enclosure 2 successfully removed.

Updating system information...done

Successfuly removed: 2 done

Removing enclosure 3...Enclosure 3 successfully removed.

Updating system information...done

Successfuly removed: 3 done
```

第 19 章

DD Extended Retention

本章には、次のセクションが含まれます。

- DD Extended Retention の概要 514
- DD Extended Retention でサポートされルプロトコル 515
- 高可用性と Extended Retention 516
- DD Extended Retention を使用した DD Replicator の使用 516
- DD Extended Retention のハードウェアとライセンス 518
- DD Extended Retention の管理 522
- DD Extended Retention を使用したアップグレードおよびリカバリ 532
- アーカイブ階層から DD Cloud Tier へのデータの移行 534

DD Extended Retention の概要

DD Extended Retention（Data Domain Extended Retention）は、DD システムにおいてバックアップ データをコスト パフォーマンスに優れた方法で長期保存するための内部階層方式を提供します。DD Extended Retention は、バックアップの長期保存用として DD システムを活用し、テープへの依存を最小限に抑えることができます。

注

DD Extended Retention は以前は、［Data Domain Archiver］と呼ばれていました。

2 階層型ファイル システム

DD Extended Retention が有効な DD システムの内部 2 階層型ファイル システムは、［アクティブ階層］と［保存階層］で構成されます。ただし、ファイル システムは、1 つのエンティティとして表示されます。着信データは、まずファイル システムのアクティブ階層に配置されます。データ（完全なファイルの形）は、個別の［Data Movement Policy］で指定したように、その後ファイル システムの保存階層に移行されます。たとえば、アクティブ階層は 90 日間、毎週のフル バックアップと毎日の増分バックアップを継続し、保存階層は 7 年間、毎月のフル バックアップを継続できます。

保存階層は、1 個以上の保存ユニットで構成されており、それぞれのユニットが 1 個以上のシェルフからストレージを取得します。

注

DD OS 5.5.1 の時点では、保存階層あたり 1 個しか保存ユニットは認められません。ただし、DD OS 5.5.1 以前にセットアップされたシステムは複数の保存ユニットを持ち続けることができますが、それ以上、保存ユニットを追加することはできません。

動作の透過性

DD Extended Retention が有効な DD システムは、オープン システム用の DD VTL と IBMi による、または DD Boost などのアプリケーション固有インターフェイスを使用するディスク ベース ターゲットとして、Ethernet を介した NFS および CIFS ファイル サービス プロトコルを通した同時データ アクセス方法を使用する既存のバックアップ アプリケーションに対応しています（Avamar®、NetWorker®、GreenPlum、Symantec OpenStorage、Oracle RMAN とともに使用するため）。

DD Extended Retention は、アクティブ階層から保存階層への自動透過的データ移動によって DD アーキテクチャを拡張します。2 階層のすべてのデータにアクセスできますが、保存階層のデータに初めてアクセスするときは若干の遅延がある可能性があります。システムの名前空間はグローバルであり、データ移動の影響は受けません。2 階層型ファイル システムを活用するには、ファイル システムのパーティション化が必要です。

データ移動ポリシー

カスタマイズできる［Data Movement Policy］は、ファイルがアクティブ階層から保存階層に移動されるポリシーです。ファイルが最後に変更された時間に基づきます。MTree ごとにポリシーを設定できるため、各データのサブセットに対して異なるポリシーを設定できます。更新できるファイルには、変化しないものとは異なるポリシーが必要です。

保存ユニット内での重複解除

障害分離のため、重複解除は完全に DD Extended Retention が有効な DD システム用の保存ユニット内で行われます。アクティブ階層と保存階層間または複数の保存ユニット間のクロス重複解除は行われません。

各階層から取得したストレージ
階層化の概念は、DD Extended Retention が有効な DD システムのストレージ レベルまで拡張しています。ファイル システムのアクティブ階層は、ストレージのアクティブ階層からストレージを取得します。ファイル システムの保存階層は、ストレージの保存階層からストレージを取得します。

注

アクティブ階層と保存階層の両方で、DD OS 5.2 以降のリリースは ES20 および ES30 シェルフに、DD OS 5.7 以降のリリースは DS60 シェルフに対応しています。異なる Data Domain シェルフを同じシェルフ セットで組み合わせることはできず、シェルフ セットは「ES30 拡張シェルフ ハードウェア ガイド」または「DS60 拡張シェルフ ハードウェア ガイド」で指定された構成ルールに従ってバランスを取る必要があります。DD Extended Retention では、同一コントローラに対して接続可能なストレージが大幅に増加します。たとえば、DD Extended Retention では DD990 上に最大で 56 個の ES30 シェルフを付けることができます。アクティブ階層は、1 個以上のシェルフで構成されるストレージがなければなりません。Data Domain コントローラ モデルの最小と最大のシェルフ構成については、ES30 および DS60 の拡張シェルフ ハードウェア ガイドを参照してください。

データ保護
DD Extended Retention が有効な DD システムでは、データは組み込み型障害分離機能、災害復旧機能、DIA（データ非脆弱性アーキテクチャ）で保護されます。ファイルがアクティブ階層から保存階層に移動されると、DIA がそのファイルをチェックします。データが保存階層にコピーされると、コンテナとファイル システム構造が読み取られ、確認されます。ファイルの場所が更新され、ファイルが保存階層に正しく書き込まれたことが確認されたらアクティブ階層のスペースが再利用されます。

保存ユニットがフルになると、名前空間の情報とシステム ファイルがそれにコピーされるため、システムの他の部分が消失しても保存ユニットのデータを復元できます。

注

DD Extended Retention が有効な DD システムでは、浄化といくつかの形式のレプリケーションには対応していません。

領域回収
保存階層に移動されたデータによって空いたスペースを再利用するには、低優先度のアクティビティとしてバックグラウンドで動作する［Space Reclamation］（DD OS 5.3 時点）を使用できます。データ移動、クリーニングなどのより優先度の高いアクティビティがある場合、それは自動的に中断されます。

保存用データの暗号化
DD OS 5.5.1 では、暗号化ライセンスがあれば、DD Extended Retention が有効な DD システムに対して［静止データの暗号化］機能を使用できます。暗号化は、デフォルトでは有効になっていません。

これは、DD Extended Retention を使用していないシステムで、DD OS 5.5.1 以前からすでに使用可能な暗号化機能の拡張機能です。

暗号化機能のセットアップおよび利用の詳細な手順については、本ガイドの「[格納データの暗号化の管理]」の章を参照してください。

DD Extended Retention でサポートされルプロトコル

DD Extended Retention が有効な DD システムがサポートするプロトコルは、NFS、CIFS、DD Boost です。DD VTL は DD OS 5.2 から、NDMP は DD OS 5.3 から対応しています。

注

DD Boost に対応するアプリケーションのリストについては、オンライン サポートサイトの［DD Boost Compatibility List］を参照してください。

DD Extended Retention を使用している場合、まずデータがアクティブ階層に入ります。Data Movement Policy に規定されたとおり、ファイル全体が保存階層の保存ユニットに移動されます。すべてのファイルは同じ名前空間にあります。データをパーティション化する必要はなく、任意でファイル システムを拡張できます。

すべてのデータはユーザーから見え、すべてのファイル システム メタデータはアクティブ階層にあります。

データをアクティブ階層から保存階層に移動させると、（アクティブ階層の）容量を増やせますが、アクセスされるユニットのアクセス準備ができていない場合には、（保存階層側のデータへの）アクセス時間がかかります。

高可用性と Extended Retention

HA（高可用性）が有効化されている Data Domain システムでは、DD Extended Retention はサポートされていません。DD OS は、現時点では Extended Retention with HA をサポートできません。

DD Extended Retention を使用した DD Replicator の使用

いくつかの形式のレプリケーションが、DD Extended Retention が有効な DD システムでサポートされます。

サポートされるレプリケーション タイプは、保護対象のデータによって異なります。

- ［ソース］となっているシステムでデータを保護する場合、DD Extended Retention が有効な DD システムは、コレクション レプリケーション、MTree レプリケーション、DD Boost 管理ファイル レプリケーションに対応します。
- ［デスティネーション］となっている他のシステムでデータを保護する場合、DD Extended Retention が有効な DD システムは、ディレクトリ レプリケーション、コレクション レプリケーション、MTree レプリケーション、DD Boost 管理ファイル レプリケーションに対応します。

注

デルタ（低帯域幅の最適化）レプリケーションは、DD Extended Retention ではサポートされません。DD システムで DD Extended Retention を有効化する前に、すべてのコンテキストでデルタ レプリケーションを無効化する必要があります。

DD Extended Retention を使用したコレクション レプリケーション

コレクション レプリケーションは、DD Extended Retention が有効な 2 つの DD システムの対応するアクティブ階層と保存ユニット間で行われます。ソースのアクティブ階層または保存ユニットに障害が発生すると、リモート サイトの対応するユニットから新しいユニットにデータがコピーされ、交換ユニットとしてお客様のサイトに送られます。

コレクション レプリケーションのセットアップの前提条件：

- ソースとデスティネーションの両方のシステムが、DD Extended Retention が有効な DD システムとして構成されている必要があります。

- 保存ユニットが追加され、レプリケーションが構成されるまで、デスティネーションではファイル システムを有効化しないでください。

DD Extended Retention を使用したディレクトリ レプリケーション

ディレクトリ レプリケーションでは、DD Extended Retention が有効な DD システムがレプリケーションのターゲットとして使用され、任意の対応 DD システムからの 1 対 1 および多対 1 のトポロジーがサポートされます。ただし、DD Extended Retention が有効な DD システムは、双方向ディレクトリ レプリケーションには対応しておらず、ディレクトリ レプリケーションの［ソース］にはなれません。

注

ディレクトリ レプリケーションを使用してデータを DD Extended Retention が有効な DD システムにコピーするには、ソースが DD OS 5.0 以降を実行している必要があります。そのため、DD OS 5.0 以前を実行するシステムでは、まず DD OS 5.0 以降を実行している中間システムにデータをインポートする必要があります。たとえば、DD OS 4.9 Extended Retention が有効なシステムから DD OS 5.2 Extended Retention が有効ではないシステムにレプリケーションできます。その後、DD OS 5.2 システムから DD OS 4.9 システムにレプリケーションできます。

DD Extended Retention を使用した MTree レプリケーション

2 つの DD Extended Retention が有効な DD システム間の MTree レプリケーションをセットアップできます。レプリケートされたデータは、まずデスティネーション システムのアクティブ階層に配置されます。デスティネーション システムの Data Movement Policy によって、レプリケートされたデータを保存階層に移行するタイミングが決まります。

次のように、MTree レプリケーション制限およびポリシーは DD OS リリースによって異なる点に留意してください。

- DD OS 5.1 では、MTree を使用して、データを DD Extended Retention が有効ではないシステムから DD Extended Retention が有効なシステムにレプリケーションできます。
- DD OS 5.2 では、データを DD Extended Retention が有効なシステムのアクティブ階層にレプリケーションすることで、そのデータをアクティブ階層内で保護できます。
- DD OS 5.5 では、両方 DD OS 5.5 以降で動作している場合、データを DD Extended Retention が有効ではないシステムから DD Extended Retention が有効なシステムへの MTree レプリケーションに対応しています。
- DD OS 5.3 および 5.4 では、DD Extended Retention を有効にしたい場合、ソース マシンで /backup MTree のレプリケーションをセットアップしないでください （DD OS 5.5 以降にはこの制限はありません）。

DD Extended Retention を使用した管理ファイル レプリケーション

DD Extended Retention が有効な DD システムで対応している DD Boost 管理ファイル レプリケーションのトポロジーは、1 対 1、多対 1、双方向、1 対多、カスケードです。

注

DD Boost 2.3 以降では、バックアップ アプリケーション内で複数のコピーを作成および管理する方法が指定できます。

DD Extended Retention のハードウェアとライセンス

DD Extended Retention が有効な DD システムには、特定のハードウェア構成が必要です。ライセンス（特に個別のシェルフ容量ライセンス）もこの機能に特有です。

DD Extended Retention の対応ハードウェア

DD Extended Retention が有効な DD システムのハードウェア要件には、メモリ要件、シェルフ、NIC/FC カードなどがあります。DD Extended Retention に必要なハードウェア構成の詳細については、お使いの DD システムのインストールおよび設定ガイド、およびお使いの拡張シェルフの拡張シェルフ ハードウェア ガイドを参照してください。

次の DD システムが DD Extended Retention に対応しています。

DD860

- 72 GB の RAM
- 1 - NVRAM IO モジュール（1 GB）
- 3 - クワッド ポート SAS IO モジュール
- 2 - マザーボードの 1 GbE ポート
- 0～2 - 外部接続の 1/10 GbE NIC IO カード
- 0～2 - 外部接続の Dual-Port FC HBA IO カード
- 0～2 - 結合 NIC/FC カード
- 1～24 - 142 TB のシステム最大有効容量を超えない ES20 または ES30 シェルフ（1 TB または 2 TB ディスク）

DD860 で DD Extended Retention が有効になっている場合、アクティブ階層の最大有効容量は 142 TB です。保存階層の最大有効容量は 142 TB です。アクティブ階層と保存階層の総有効ストレージ容量は 284 TB です。

DD990

- 256 GB の RAM
- 1 - NVRAM IO モジュール（2 GB）
- 4 - クワッド ポート SAS IO モジュール
- 2 - マザーボードの 1 GbE ポート
- 0～4 - 外部接続の 1 GbE NIC IO カード
- 0～3 - 外部接続の 10 GbE NIC カード
- 0～3 - 外部接続の Dual-Port FC HBA カード
- 0～3 - 結合 NIC/FC カード、任意の 1 つの特定の IO モジュールに対し 3 個を超えないこと。
- 1～56 - 570 TB のシステム最大有効容量を超える ES20 または ES30 シェルフ（1、2、または 3 TB ディスク）

DD990 で DD Extended Retention が有効になっている場合、アクティブ階層の最大有効容量は 570 TB です。保存階層の最大有効容量は 570 TB です。アクティブ階層と保存階層の総有効ストレージ容量は 1140 TB です。

DD4200

- 128 GB の RAM
- 1 - NVRAM IO モジュール（4 GB）
- 4 - クワッド ポート SAS IO モジュール
- 1 - マザーボードの 1 GbE ポート
- 0～6 - 外部接続の 1/10 GbE NIC カード
- 0～6 - 外部接続の Dual-Port FC HBA カード
- 0～6 - 特定の IO モジュール 4 個分を超えない結合 NIC/FC カード。
- 1～16 - 192 TB のシステム最大有効容量を超えない ES30 SAS シェルフ（2 TB または 3 TB ディスク） ES30 SATA シェルフ（1、2、または 3 TB ディスク）は、システム コントローラー アップグレードに対応しています。

DD4200 で DD Extended Retention が有効になっている場合、アクティブ階層の最大有効容量は 192 TB です。保存階層の最大有効容量は 192 TB です。アクティブ階層と保存階層の総有効ストレージ容量は 384 TB です。外部接続は、最大 16 シェルフの DD Extended Retention 構成に対応しています。

DD4500

- 192 GB の RAM
- 1 - NVRAM IO モジュール（4 GB）
- 4 - クワッド ポート SAS IO モジュール
- 1 - マザーボードの 1 GbE ポート
- 0～6 - 外部接続の 1/10 GbE NIC IO カード
- 0～6 - 外部接続の Dual-Port FC HBA カード
- 0～5 - 特定の IO モジュール 4 個分を超えない結合 NIC/FC カード。
- 1～20 - 285 TB のシステム最大有効容量を超えない ES30 SAS シェルフ（2 または 3 TB ディスク）。ES30 SATA シェルフ（1、2、または 3 TB）は、システム コントローラー アップグレードに対応しています。

DD4500 で DD Extended Retention が有効になっている場合、アクティブ階層の最大有効容量は 285 TB です。保存階層の最大有効容量は 285 TB です。アクティブ階層と保存階層の総有効ストレージ容量は 570 TB です。外部接続は、最大 24 シェルフの DD Extended Retention 構成に対応しています。

DD6800

- 192 GB の RAM
- 1 - NVRAM IO モジュール（8 GB）
- 3 - クワッド ポート SAS IO モジュール
- 1 - マザーボードの 1 GbE ポート
- 0～4 - 外部接続の 1/10 GbE NIC カード
- 0～4 - 外部接続の Dual-Port FC HBA カード
- 0～4 - 結合 NIC/FC カード
- シェルフの組み合わせについては、お使いの DD システムのインストールおよびセットアップ ガイド、およびお使いの拡張シェルフの拡張シェルフ ハードウェア ガイドを参照してください。

DD6800 で DD Extended Retention が有効になっている場合、アクティブ階層の最大有効容量は 288 TB です。保存階層の最大有効容量は 288 TB です。アクティブ階層と保存階層の総

有効ストレージ容量は 0.6 PB です。外部接続は、最大 28 シェルフの DD Extended Retention 構成に対応しています。

DD7200

- 256 GB の RAM
- 1 - NVRAM IO モジュール（4 GB）
- 4 - クワッド ポート SAS IO モジュール
- 1 - マザーボードの 1 GbE ポート
- 0～6 - 外部接続の 1/10 GbE NIC カード
- 0～6 - 外部接続の Dual-Port FC HBA カード
- 0～5 - 特定の IO モジュール 4 個分を超えない結合 NIC/FC カード。
- 1～20 - 432 TB のシステム最大有効容量を超えない ES30 SAS シェルフ（2 または 3 TB ディスク）。ES30 SATA シェルフ（1、2、または 3 TB）は、システム コントローラー アップグレードに対応しています。

DD7200 で DD Extended Retention が有効であれば、アクティブ階層ストレージの最大有効容量は 432 TB です。保存階層の最大有効容量は 432 TB です。アクティブ階層と保存階層の総有効ストレージ容量は 864 TB です。外部接続は、最大 32 シェルフの DD Extended Retention 構成に対応しています。

DD9300

- 384 GB の RAM
- 1 - NVRAM IO モジュール（8 GB）
- 3 - クワッド ポート SAS IO モジュール
- 1 - マザーボードの 1 GbE ポート
- 0～4 - 外部接続の 1/10 GbE NIC カード
- 0～4 - 外部接続の Dual-Port FC HBA カード
- 0～4 - 結合 NIC/FC カード
- シェルフの組み合わせについては、お使いの DD システムのインストールおよびセットアップ ガイド、およびお使いの拡張シェルフの拡張シェルフ ハードウェア ガイドを参照してください。

DD9300 で DD Extended Retention が有効になっている場合、アクティブ階層の最大有効容量は 720 TB です。保存階層の最大有効容量は 720 TB です。アクティブ階層と保存階層の総有効ストレージ容量は 1.4 PB です。外部接続は、最大 28 シェルフの DD Extended Retention 構成に対応しています。

DD9500

- 512 GB の RAM
- 1 - NVRAM IO モジュール（8 GB）
- 4 - クワッド ポート SAS IO モジュール
- 1 - マザーボードのクワッド 1 GbE ポート
- 0～4 - 外部接続の 10 GbE NIC カード
- 0～4 - 外部接続の Dual-Port 16 Gbe FC HBA カード
- シェルフの組み合わせについては、お使いの DD システムのインストールおよびセットアップ ガイド、およびお使いの拡張シェルフの拡張シェルフ ハードウェア ガイドを参照してください。

DD9500 で DD Extended Retention が有効であれば、アクティブ階層ストレージの最大有効容量は 864 TB です。保存階層の最大有効容量は 864 TB です。アクティブ階層と保存階層の総

有効ストレージ容量は 1.7 PB です。外部接続は、最大 56 シェルフの DD Extended Retention 構成に対応しています。

DD9800

- 768 GB の RAM
- 1 - NVRAM IO モジュール（8 GB）
- 4 - クワッド ポート SAS IO モジュール
- 1 - マザーボードのクワッド 1 GbE ポート
- 0～4 - 外部接続の 10 GbE NIC カード
- 0～4 - 外部接続の Dual-Port 16 Gbe FC HBA カード
- シェルフの組み合わせについては、お使いの DD システムのインストールおよびセットアップ ガイド、およびお使いの拡張シェルフの拡張シェルフ ハードウェア ガイドを参照してください。

DD9800 で DD Extended Retention が有効になっている場合、アクティブ階層の最大有効容量は 1008 TB です。保存階層の最大有効容量は 1008 TB です。アクティブ階層と保存階層の総有効ストレージ容量は 2.0 PB です。外部接続は、最大 56 シェルフの DD Extended Retention 構成に対応しています。

DD Extended Retention のライセンス

DD Extended Retention は、サポート対象の DD システムでインストールされた、ライセンスされたソフトウェア オプションです。

アクティブ階層と保存階層両方にインストールされたシェルフについては、各ストレージ シェルフに別々のシェルフ容量が必要です。シェルフ容量ライセンスは、アクティブ階層シェルフまたは保存階層シェルフのいずれかに固有です。

Data Domain モデルに応じて、エントリー容量を超えてアクティブ階層ストレージ容量を拡張する場合に、Expanded-Storage ライセンスが必要です。追加ストレージを使用するには、先に適切なライセンスを適用する必要があります。

DD Extended Retention 用のシェルフ容量ライセンスの追加

DD Extended Retention が有効な DD システムのすべてのシェルフには、個別のライセンスが必要です。

手順

1. ［**Administration**］ > ［**Licenses**］を選択します。
2. ［**Add Licenses**］をクリックします。
3. それぞれの後に Enter キーを押して、1 個以上のライセンス（1 行あたりの 1 つ）を入力します。終了したら、［**Add**］をクリックします。エラーがある場合は、追加されたライセンスのサマリーとエラーのため追加されなかったものがリストされます。エラーがあるライセンス キーを選択して修正します。

結果

DD システムのライセンスは、2 つのグループで表示されます。

- ソフトウェア オプションのライセンス。DD Extended Retention や DD Boost などのオプションに必要です。
- シェルフ容量ライセンス。シェルフの容量（TiB 単位）、シェルフのモデル（ES30 など）、シェルフのストレージ階層（アクティブまたは保存）を表示します。

ライセンスを削除するには、［Licenses］リストでライセンスを選択し、［**Delete Selected Licenses**］をクリックします。確認を求めるプロンプトが表示されたら、警告を読み、［**OK**］をクリックして続行します。

DD Extended Retention 用のストレージの構成

DD Extended Retention 用の追加ストレージには適切なライセンスが必要です。また、追加ストレージのサポートには、DD システムに十分なメモリがインストールされている必要があります。ライセンスまたはメモリがさらに必要な場合は、エラー メッセージが表示されます。

手順

1. ［**Hardware**］ > ［**Storage**］タブを選択します。
2. ［Overview］タブで［**Configure Storage**］を選択します。
3. ［Configure Storage］タブで、［Addable Storage］リストから追加するストレージを選択します。
4. メニューから適切な Tier Configuration（［**Active**］または［**Retention**］）を選択します。アクティブ階層は、標準の DD システムと同様にし、同じようなサイズにする必要があります。アクティブ階層に追加できるストレージの最大容量は、使用される DD コントローラーによって異なります。
5. 追加するシェルフのチェックボックスを選択します。
6. ［**Add to Tier**］ボタンをクリックします。
7. ［**OK**］をクリックして、ストレージを追加します。
8. 追加したシェルフを削除するには、それを［Tier Configuration］リストから選択し、［**Remove from Tier**］、［**OK**］を順に選択します。

DD Extended Retention を使用するお客様提供のインフラストラクチャ

DD Extended Retention を有効化する前に、環境とセットアップが特定要件を満たしている必要があります。

- ［仕様、設置場所の要件、ラック スペース、相互ケーブル接続］：DD システム モデルについては、「Data Domain のインストールとセットアップ ガイド」を参照してください。
- ［ラックへの設置とケーブル接続］：将来の拡張を考慮してシステムをラックに設置することをお勧めします。すべてのシェルフは、1 つの DD システムに取り付けられます。

  注

  - お使いのシェルフ モデル（ES20、ES30、DS60）の「Data Domain 拡張シェルフ ハードウェア ガイド」を参照してください。

DD Extended Retention の管理

DD システムで DD Extended Retention をセットアップして使用するには、DD System Manager や DD CLI を使用します。

- DD System Manager（以前は Enterprise Manager と呼ばれていた）は、GUI（グラフィカル ユーザー インターフェイス）です。この GUI については、本書を参照してください。
- DD CLI（コマンド ライン インターフェイス）で入力される `archive` コマンドについては、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

DD System Manager を使用する場合に使用できないコマンドは、`archive report` だけです。

DD Extended Retention 用の DD システムの有効化

DD Extended Retention 用の DD システムを使用する前に、正しいライセンスとファイル システムをセットアップする必要があります。

手順

1. 正しいライセンスが適用されていることを確認。［**Administration**］ > ［**Licenses**］、を選択して、Extended Retention の［Feature Licenses］リストを確認します。
2. ［**Data Management**］ > ［**File System**］ > ［**More Tasks**］ > ［**Enable DD Extended Retention**］を選択します。

   このオプションが利用できるのは、Data Domain システムが DD Extended Retention をサポートしており、ファイル システムが DD Extended Retention 用に構成されていない場合だけです。DD Extended Retention が有効化された後は、ファイル システムを破棄するまで無効化できない点に留意してください。

   a. ファイル システムが（非 DD Extended Retention システムとして）すでに有効化されている場合は、それを無効化するよう促すプロンプトが表示されます。［**Disable**］をクリックして無効化します。

   b. DD Extended Retention で使用するためにファイル システムを変換することを確認するプロンプトが表示された場合は、［**OK**］をクリックします。

      ファイル システムが DD Extended Retention ファイル システムに変換されると、ファイル システムのページは両方の階層の情報を含むように更新され、［**Retention Units**］というラベルの新しいタブが表示されます。

      ［**CLI** 相当］

      次の CLI を使用して、Extended Retention ライセンスがインストールされていることを確認することもできます。

      従来のライセンス方法を使用します。

```
# license show
## License Key                    Feature
--    --------------------        -----------
1     AAAA-BBBB-CCCC-DDDD         Replication
2     EEEE-FFFF-GGGG-HHHH         VTL
--    --------------------        -----------
```

      ライセンスが存在しない場合、各ユニットに購入したライセンスを示すドキュメント（クイック インストール ガイド）が含まれています。次のコマンドを入力して、ライセンス キーを入力します。

```
# license add license-code
```

      次のコマンドを入力して、Extended Retention を有効化します。

```
# archive enable
```

      電子ライセンスを使用します。

```
# elicense show
Feature licenses:
## Feature     Count Mode            Expiration Date
-- ----------- ----- --------------- ---------------
1  REPLICATION 1     permanent (int) n/a
2  VTL         1     permanent (int) n/a
-- ----------- ----- --------------- ---------------
```

ライセンスが存在しない場合は、新しいフィーチャー ライセンスのライセンス ファイルを更新します。

```
# elicense update mylicense.lic
New licenses: Storage Migration
Feature licenses:
## Feature            Count   Mode             Expiration Date
-- -----------------  -----  ---------------  ---------------
1  REPLICATION        1      permanent (int)  n/a
2  VTL                1      permanent (int)  n/a
3  EXTENDED RETENTION 1      permanent (int)  n/a
-- -----------------  -----  ---------------  ---------------
** This will replace all existing Data Domain licenses on the system with the above
EMC ELMS licenses.
Do you want to proceed? (yes|no) [yes]: yes
eLicense(s) updated.
```

次のコマンドを入力して、Extended Retention を有効化します。

```
# archive enable
```

DD Extended Retention 用の 2 階層型ファイル システムの作成

DD Extended Retention には、アクティブ階層と保存階層の 2 階層型ファイル システムがあります。DD システムはこのスペシャル ファイル システムを有効化する前に、DD Extended Retention に対して有効化されている必要があります。

手順

1. ［**Data Management**］ > ［**File System**］を選択します。
2. ファイル システムが存在する場合は、それを破棄します。
3. ［**More Tasks**］ > ［**Create file system**］を選択します。
4. 保存可能なファイル システムを選択して、［**Next**］をクリックします。
5. ［File System Create］ダイアログ ボックスで［**Configure**］をクリックします。

   ファイル システムを作成する前に、ストレージを構成する必要があります。
6. ［Configure Storage］ダイアログ ボックスを使用して、アクティブ階層および保存階層から使用可能なストレージを追加および削除します。終了したら、［**OK**］をクリックします。

   アクティブ階層のストレージを使用してアクティブなファイル システム階層を作成し、保存階層のストレージを使用して保存ユニットを作成します。

   注

   DD OS 5.5.1 の時点では、保存階層あたり 1 個しか保存ユニットは認められません。ただし、DD OS 5.5.1 以前にセットアップされたシステムは複数の保存ユニットを持ち続けることができますが、それ以上の保存ユニットを追加することはできません。
7. ［File System Create］ダイアログ ボックスを使用して以下を実行します。
   a. ドロップダウン リストから保存ユニットのサイズを選択します。
   b. ［**Enable file system after creation**］オプションを選択します。
   c. ［次へ］をクリックします。

   ［Summary］ページには、新しいファイル システムのアクティブ階層と保存階層のサイズが表示されます。

8. ［**Finish**］をクリックして、ファイル システムを作成します。
   各作成ステップの進行状況が表示され、進捗バーで全体のステータスが監視されます。
9. ファイル システムの実行が完了したら、［**OK**］をクリックします。
   ［**CLI** 相当］
   追加シェルフを追加するには、各エンクロージャにこのコマンドを 1 回使用します。

```
# storage add tier archive enclosure 5
```

   アーカイブ・ユニットを作成し、ファイル・システムに追加します。アーカイブ ユニット内のエンクロージャ数を指定するように求められます。

```
# filesys archive unit add
```

   作成したアーカイブ・ユニットがファイル・システムに追加されたことを確認します。

```
# filesys archive unit list all
```

   システムによって認識されたファイル システムを確認します。

```
# filesys show space
```

DD Extended Retention の［File System］パネル

DD Extended Retention 用の DD システムを有効化した後、［**Data Management**］ > ［**File System**］パネルの表示が次のように少し変わります（DD Extended Retention が有効ではないシステムと少し異なります）。

- ［**State**］は、ファイル システムが有効か無効かを示します。すぐに右にある［Disable/Enable］ボタンを使用して、状態を変更できます。
- ［**Clean Status**］は、最後にクリーニング操作が完了した時間または（クリーニング操作が現在実行中の場合）現在のクリーニング ステータスを表示します。クリーニングを実行できる場合、［**Start Cleaning**］ボタンが表示されます。クリーニングを実行する際、［**Start Cleaning**］ボタンは［**Stop Cleaning**］ボタンに代わります。
- ［**Data Movement Status**］は、最後のデータ移動が終了した時間を示します。データ移動を実行できる場合、［**Start**］ボタンが表示されます。データ移動を実行する際、［**Start**］ボタンは［**Stop**］ボタンに代わります。
- ［**Space Reclamation Status**］は、保存階層でデータを削除した後に再利用されるスペースの量を示します。スペース再利用を実行できる場合、［**Start**］ボタンが表示されます。それがすでに実行中の場合、［**Stop**］および［**Suspend**］ボタンが表示されます。それがすでに実行されて、中断状態になっている場合、［**Stop**］および［**Resume**］ボタンが表示されます。開始時間、終了時間、完了率、再利用されているユニット、空きスペースなどの詳細情報を表示する［**More Information**］ボタンもあります。
- ［**More Tasks**］ > ［**Destroy**］を選択すると、仮想テープを含むファイル システムのすべてのデータを削除できます。これは、システム管理者が管理できます。
- ［**More Tasks**］ > ［**Fast Copy**］を選択すると、ソース ディレクトリのファイルと MTree を宛先ディレクトリにコピーできます。DD Extended Retention が有効なシステムについては、ファスト コピーはアクティブ階層と保存階層間でデータを移動しない点に留意してください。
- ［**More Tasks**］ > ［**Expand Capacity**］を選択すると、アクティブ階層または保存階層を拡張できます。

アクティブ階層または保存階層の拡張

ファイル システムが有効な場合、アクティブ階層または保存階層を拡張できます。

［**Active**］階層を拡張するには、次の手順を実行します。

手順

1. ［**Data Management > File System > More Tasks > Expand Capacity**］を選択します。
2. ［Expand File System Capacity］ダイアログで、［**Active Tier**］を選択してから［**Next**］をクリックします。
3. ［**Configure**］をクリックします。
4. ［Configure Storage］ダイアログで、Active Tier が Configure 選択として表示されていることを確認し、［**OK**］をクリックします。
5. 構成終了後、［Expand File System Capacity］ダイアログに戻ります。［**Finish**］を選択して、アクティブ階層拡張を完了します。

［保存］階層を拡張するには、次の手順を実行します。

手順

1. ［**Data Management > File System > More Tasks > Expand Capacity**］を選択します。
2. ［Expand File System Capacity］ダイアログで、［**Retention Tier**］を選択してから［**Next**］を選択します。
3. 保存ユニットを使用できる場合は、［**Select Retention Unit**］ダイアログが表示されます。拡張したい保存ユニットを選択して、［**Next**］を選択します。保存ユニットを使用できない場合は［**Create Retention Unit**］ダイアログが表示され、次に進む前に保存ユニットを作成する必要があります。

   注

   DD Extended Retention が有効な DD システムのパフォーマンスを最適にするには、最低でも 2 シェルフ単位で保存階層を拡張する必要があります。保存ユニットを拡張するには、それがフルに近くなるまで待つ必要はありません。

4. 保存ユニットを拡張するサイズを選択した後、［**Configure**］をクリックします。
5. 構成終了後、［Expand File System Capacity］ダイアログに戻ります。［**Finish**］をクリックして、保存階層の拡張を完了します。

保存階層のスペースの再利用

スペース再利用（DD OS 5.3 から実装）を実行することで保存階層の削除されたデータからスペースを再利用できます。スペース再利用は、ファイル システム クリーニング時にも行われます。

手順

1. ［**Data Management**］ > ［**File System**］を選択します。タブのすぐ上の［**Space Reclamation Status**］には、保存階層でデータを削除した後に再利用されるスペースの量が表示されます。
2. スペース再利用を実行できる場合、［**Start**］ボタンが表示されます。それがすでに実行中の場合、［**Stop**］および［**Suspend**］ボタンが表示されます。それがすでに実行されて、中断状態になっている場合、［**Stop**］および［**Resume**］ボタンが表示されます。
3. サイクル名、開始時間、終了時間、有効実行時間、完了率（進行中の場合）、再利用されているユニット、ターゲット ユニットの空きスペース、総空きスペースの詳細を表示するには、［**More Information**］をクリックします。

注

`archive space-reclamation` コマンドを使用すると、1 回限りのサイクルのオプションを使用していない場合は、システムは手動で停止されるまで、バックグラウンドでスペースの再利用を実行します。`archive space-reclamation schedule set` コマンドを使用して、スペースの再利用の開始時間を設定することもできます。

［**CLI** 相当］
スペースの再利用を有効化する場合：

```
# archive space-reclamation start
```

スペースの再利用を無効化する場合：

```
# archive space-reclamation stop
```

スペースの再利用のステータスを表示する場合：

```
archive space-reclamation status-detailed
Space-reclamation will start when 'archive data-movement'
completes.

Previous Cycle:
---------------
Start time                 : Feb 21 2014 14:17
End time                   : Feb 21 2014 14:49
Effective run time         : 0   days, 00:32.
Percent completed          : 00 % (was stopped by user)
Units reclaimed            : None
Space freed on target unit : None
Total space freed          : None
```

DD Extended Retention の［File System］タブ

DD Extended Retention 用の DD システムを有効化した後、［**Data Management**］ > ［**File System**］タブの表示が少し変わり（DD Extended Retention が有効ではないシステムと少し異なり）、次のタブが 1 つ追加されます。［**Retention Units**］

［Summary］タブ

［Summary］タブには、ディスク領域使用率およびアクティブ階層と保存階層両方の圧縮についての情報が表示されます。

［**Space Usage**］: 合計サイズ、使用中のスペースの量、アクティブ階層と保存階層の使用可能なスペースの量と総計を表示します。アクティブ階層のクリーニング可能なスペースの量が表示されます。

［**Active Tier and Retention Tier**］: 現在使用中の圧縮前および圧縮後の値と過去 24 時間に書き込まれた値が表示されます。グローバル、ローカル、および総圧縮（削減率）率も表示されます。

［Retention Units］タブ

［Retention Units］タブには、保存ユニットが表示されます。DD OS 5.5.1.4 の時点では、保存階層あたり 1 個しか保存ユニットは認められません。ただし、DD OS 5.5.1.4 以前にセットアップされたシステムは複数の保存ユニットを持ち続けることができますが、それ以上、保存ユニットを追加することはできません。

次の情報が表示されます：ユニットの State（New、Empty、Sealed、Target、または Cleaning）、Status（Disabled、Ready、または Stand-by）、その Start Date（保存階層に移動された場合）、Unit Size。スペース再利用が実行中の場合、ユニットはクリーニング状態です。ユニットが封印され、データが追加できない場合、Sealed Date が表示されます。保存ユニットのチェ

ックボックスを選択すると、［Detailed Information］パネルに関連情報（Size、Used、Available、Cleanable）が表示されます。

2 つのボタン、［**Delete**］（ユニットの削除用）と［**Expand**］（ユニットへのストレージの追加用）があります。このユニットは、拡張される新しい状態またはターゲット状態である必要があります。

［Configuration］タブ

［Configuration］タブでは、システムを構成できます。

Options の［**Edit**］ボタンを選択すると、［Modify Settings］ダイアログが表示されます。そこでは、Local Compression Type（オプションは none、lz（デフォルト）、gz、gzfast）と Retention Tier Local Comp（ression）（オプションは none、lz、gz（デフォルト）、gzfast）を変更できます。

Clean Schedule の［**Edit**］ボタンを選択すると、クリーニング スケジュールとスロットル パーセンテージを変更できる［Modify Schedule］ダイアログが表示されます。

Data Movement Policy の［**Edit**］ボタンを選択すると、いくつかのパラメーターを設定できる［Data Movement Policy］ダイアログが表示されます。File Age Threshold は、カスタム デフォルトを設定していないすべての MTree に適用されるシステム全体おデフォルトです。最低値は 14 日です。Data Movement Schedule によって、データ移動が行われる頻度を確立できます。推奨スケジュールは 2 週間ごとです。File System Cleaning によって、データ移動後にシステム クリーニングを行わないように設定できますが、このオプションは選択されたままにすることを強く推奨します。

File Age Threshold per MTree Link

［**File Age Threshold per MTree**］リンクを選択すると、［File System］から［MTree］領域に（［**Data Management**］ > ［**MTree**］を選択してアクセスすることもできます）移動します。そこでは、各 MTree にカスタマイズされた File Age Threshold を設定できます。

MTree を選択した後、Data Movement Policy の隣の［**Edit**］を選択します。［Modify Age Threshold］ダイアログで、File Age Threshold の新しい値を入力し、［**OK**］を選択します。DD OS 5.5.1 の場合、最低値は 14 日以上である必要があります。

［Encryption］タブ

［Encryption］タブによって、格納データの暗号化を有効化または無効化できます。これは、保存ユニットが 1 個だけのシステムのみ対応しています。5.5.1 では、DD Extended Retention は 1 個の保存ユニットしか対応していないため、5.5.1 以降にセットアップされたシステムにはこの制限への対応に関して問題はありません。ただし、5.5.1 以前にセットアップされたシステムには複数の保存ユニットがある場合がありますが、保存ユニットを 1 個残して削除するまで格納データの暗号化は使用しないか、データが 1 個の保存ユニットに移動または移行されています。

［Space Usage］タブ

［Space Usage］タブでは、MiB 単位でスペース使用率の推移を表示する 3 種類のチャート タイプ（（全体）File System、Active（階層）、Archive（階層））の中からいずれかを選択します。右上で期間値（7、30、60、または 120 日）を選択することもできます。データは、圧縮前書き込み（青）、圧縮後使用（赤）、圧縮率（黒）として表示されます（色分け）。

［Consumption］タブ

［Consumption］タブでは、使用中の圧縮後ストレージの量と圧縮率の推移を表示する 3 種類のチャート タイプ（（全体）File System、Active（階層）、Archive（階層））の中からいずれかを選択できます。それによって、消費トレンドを表示できます。右上で期間値（7、30、60、または 120 日）を選択することもできます。［Capacity］チェックボックスで、総システム容量に対する圧縮後ストレージを表示するかどうかを選択できます。

［Daily Written］タブ

［Daily Written］タブでは、1 日あたりの書き込まれたデータの量を確認する期間（7、30、60、または 120 日）を選択できます。データは、グラフと表形式両方で圧縮前書き込み（青）、圧縮後使用（赤）、圧縮率（黒）として表示されます（色分け）。

保存ユニットの拡張

最適なパフォーマンスを得るには、保存ユニットがフルに近くなる前に 1 シェルフ単位で拡張するようにします。ファイル システム作成後に、ストレージをアクティブ階層から保存階層に移動させることはできません。保存階層には未使用のエンクロージャのみ追加することができます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Retention Units**］を選択します。
2. 保存ユニットを選択します。

   クリーニングが実行されている場合、保存ユニットは拡張できないことに注意してください。
3. ［**Expand**］をクリックします

   システムには、現在の保存階層のサイズ、予想される拡張サイズ、拡張された容量の合計が表示されます。追加のストレージが使用可能な場合は、［Configure］リンクをクリックできます。
4. ［次へ］をクリックします。

   システムには、この操作の後はファイル システムを元のサイズに戻すことができなくなることを示すメッセージが表示されます。
5. ［**Expand**］をクリックしてファイル システムを拡張します。

保存ユニットの削除

保存ユニットのすべてのファイルが不要になった場合は、それらを削除すると、ユニットが再使用可能になります。ファイル ロケーション レポートを生成して、保存ユニットが実際に空であることを確認したら、保存ユニットを削除して、新しいアーカイブ ユニットとして追加することができます。

手順

1. ファイル システムが実行中の場合は、［**Data Management**］ > ［ **File System**］を選択して［**Disable**］をクリックし、無効化します。
2. ［**Data Management**］ > ［**File System**］ > ［**Retention Units**］を選択します。
3. 保存ユニットを選択します。
4. ［**Delete**］をクリックします。

保存階層ローカル圧縮の変更

保存階層への以降のデータ移動のため、ローカル圧縮アルゴリズムを変更できます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Configuration**］を選択します。
2. ［**Options**］の右にある［**Edit**］をクリックします。
3. ［Retention Tier Local Comp］メニューから圧縮オプションを 1 つ選択し、［**OK**］をクリックします。

デフォルトは gz です。これは zip 形式の圧縮で、データ ストレージに使用するスペースが最も少なくなります（平均で lz よりも 10～20%少なくなりますが、データセットによっては圧縮率ははるかに高くなります）。

データ移動ポリシーの理解

ファイルは、最終変更日に基づきアクティブ階層から保存階層に移されます。データの整合性を保つため、このとき、ファイル全体が移されます。［Data Movement Policy］によって、［File Age Threshold］と［Data Movement Schedule］が実現できます。File Age Threshold で設定された期間、データが変更されなかった場合、Data Movement Schedule によって確立された日付にデータがアクティブ階層から保存階層に移されます。

注

DD OS 5.5.1 の場合、File Age Threshold は 14 日以上である必要があります。

定義された MTree それぞれに対して異なる File Age Threshold を指定できます。MTree は、管理目的でデータの論理セットとなる名前空間内のサブツリーです。たとえば、別の MTree に財務データ、メール、エンジニアリング データを置くことができます。

DD OS 5.3 で導入された［スペース再利用］機能を活用するには、隔週（14 日ごと）でデータ移動とファイル システム クリーニングをスケジュール設定することを推奨します。デフォルトでは、クリーニングは必ずデータ移動完了後に実行されます。デフォルトを変更しないことを強く推奨します。

次のような、一般的なサイズ設定エラーを回避します。

- データの移動頻度が高すぎる、過度に積極的な Data Movement Policy の設定。
- 控えめすぎる Data Movement Policy の設定。アクティブ階層の空きスペースがなくなると、システムにデータを書き込みできなくなります。
- アクティブ階層が小さすぎる場合における、それを補うための過度に積極的な Data Movement Policy の設定。

スナップショットおよびファイル システム クリーニングに関係する次の注意事項に注意してください。

- スナップショットのファイルは、保存階層に移動後もクリーニングされません。スペースは、スナップショットが削除されるまで再利用できません。
- スナップショットの File Age Threshold を 14 日以上に設定することを推奨します。

次に示すのは、Data Movement Policy のセットアップ方法の 2 つの例です。

- 変更の程度が異なるデータを 2 個の異なる MTree に分け、データが安定したらすぐにデータを移動するように File Age Threshold を設定します。毎日の増分バックアップ用に MTree A を、毎週のフル バックアップ用に MTree B を作成します。データが［移動されない］ようにするため MTree A の File Age Threshold を設定しますが、MTree B の File A は 14 日（最低閾値）に設定します。
- 別々の MTree に分けられないデータについては、次の操作を行います。毎日の増分バックアップの保存期間が 8 週間、毎週のフル バックアップの保存期間が 3 年であるとします。この場合、File Age Threshold は 9 週間に設定するのが最適です。それ以上低く設定すると、すぐに削除する毎日の増分データを移動することになります。

Data Movement Policy の変更

各 MTree に異なる Data Movement Policy を設定できます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Configuration**］を選択します。

2. ［**Data Movement Policy**］の右にある［**Edit**］をクリックします。
3. ［Data Movement Policy］ダイアログで、システム全体のデフォルト File Age Threshold 値を日数で指定します。DD OS 5.5.1 の場合、この値は 14 日以上である必要があります。この値は、［**File Age Threshold per MTree**］リンクを使用して MTree の経過時間ごとの閾値を割り当てていない、新たに作成された MTree に適用されます（ステップ 7 を参照してください）。データの移動が開始されると、指定された閾値の日数の間変更されていないファイルは、すべてアクティブ階層からアーカイブ階層に移動されます。
4. データ移動が行われる Data Movement Schedule を、毎日、毎週、隔週（14 日ごと）、毎月、毎月末などに指定します。特定の日および時間（時間と分）も選択できます。DD OS 5.3 で導入されたスペース再利用機能を活用するには、隔週（14 日ごと）でデータ移動とファイル システム クリーニングをスケジュール設定することを強く推奨します。
5. Data Movement Throttle、システムがデータの移動に使用できるリソースの割合を指定します。100%の値は、データ移動が制限されていないことを意味します。
6. デフォルトでは、ファイル システム クリーニングは必ずデータ移動完了後に実行されます。［**Start file system clean after Data Movement**］が選択された状態にしておくことを強く推奨します。
7. OK を選択します。
8. ［Configuration］タブに戻り、右下の［**File Age Threshold per MTree**］リンクを使用して、個別の MTree の経過時間閾値を指定できます。

［**CLI** 相当］
経過時間を設定する場合：

```
# archive data-movement policy set age-threshold {days|none}
mtrees mtree-list
```

必要に応じて、［デフォルト］の経過時間を設定する場合：

```
# archive data-movement policy set default-age-threshold days
```

経過時間の設定を確認する場合：

```
# archive data-movement policy show [mtree mtree-list]
```

移行スケジュールを指定する場合：

```
# archive data-movement schedule set days days time time [no-
clean]
```

スケジュールの許容値は、次のとおりです。

- days sun time 00:00
- days mon,tue time 00:00
- days 2 time 10:00
- days 2,15 time 10:00
- days last time 10:00（月の最終日）

移行スケジュールを確認する場合：

```
# archive data-movement schedule show
```

ファイル クリーニング スケジュールを無効化する場合：

注

クリーニング スケジュールを無効化する理由は、クリーニングとデータ移動でスケジュールの競合をなくすためです。データ移動が完了すると、クリーニングが自動的に開始されます。データ移動を無効化する場合は、ファイル システム クリーニングを再度有効化する必要があります。

```
# filesys clean set schedule never
```

オン デマンドでのデータ移動の開始または停止

通常の Data Movement Policy がある場合でも、［オンデマンドで］データ移動を開始または停止することもできます。

手順

1. ［**Data Management**］ > ［**File System**］を選択します。
2. ［**Data Movement Status**］の右にある［**Start**］をクリックします。
3. ［Start Data Movement］ダイアログは、ファイル システム クリーニングの前に Data Movement Policy での定義に従い、データがアクティブ階層から保存階層に移動されることを警告します。［**Start**］を選択し、データ移動を開始します。

   ファイル システム クリーニングがすでに進行中の場合、データ移動はクリーニング完了後に行われます。ただし、このオン デマンド データ移動が完了すると、もう一度クリーニングが自動的に開始されます。
4. ［**Start**］ボタンは［**Stop**］ボタンに変わります。
5. データ移動を停止するには、いつでも［**Stop**］をクリックして、［Stop Data Movement］ダイアログで［**OK**］を選択して確定します。

データ移動パッキングの使用

データは、ファイル移行ごとにターゲット パーティションで圧縮されます（DD OS 5.2 時点）。［データ移動パッキング］と呼ばれるこの機能は、デフォルトではオンに設定されています。

この機能が有効化されている場合、保存階層の圧縮は全体的に向上しますが、移行時間はわずかに増加します。

この機能が有効かどうかを判断するには、［**Data Management**］ > ［**File System**］ > ［**Configuration**］を選択します。

［**Packing data during Retention Tier data movement**］の現在の値は、Enabled または Disabled です。この設定を変更する場合、システム エンジニアと相談します。

DD Extended Retention を使用したアップグレードおよびリカバリ

次のセクションでは、DD Extended Retention が有効な DD システムでの、ソフトウェアおよびハードウェア アップグレードの実行方法、データのリカバリ方法について説明します。

DD Extended Retention を使用した DD OS 5.7 へのアップグレード

DD Extended Retention が有効な DD システムのアップグレード ポリシーは、標準 DD システムと同じです。

最大 2 リリース前の主要なリリースからのアップグレードがサポートされています。DD OS をアップグレードする方法の指示については、ターゲット DD OS バージョンの「リリース ノート」で、アップグレード手順のセクションを参照してください。

DD Extended Retention が有効な DD システムを DD OS 5.7 にアップグレードする場合、スペース再利用機能を活用するため、必ず既存のデータ移動スケジュールを隔週（14 日）に更新してください。

DD Extended Retention が有効な DD システムは、データ移動完了後、自動的にクリーニングを実行するため、DD System Manager または CLI（コマンド ライン インターフェイス）を使用して別途クリーニングをスケジュールしないでください。

アクティブ階層が使用可能な場合、プロセスはアクティブ階層と保存ユニットをアップグレードし、システムを前のアップグレードの完了が確認される前の状態に戻します。この状態は、ファイル システムが有効化され、ファイル システムに属する保存ユニットすべてがアップグレードされたことを確認した後に、ファイル システムによってクリアされます。この状態がクリアされるまで、それ以降のアップグレードは許可されません。

アクティブ階層が使用不可能な場合、アップグレード プロセスはシステム シャーシをアップグレードし、それをファイル システムの作成または許可が可能になる状態にします。

アップグレード プロセス終了後、保存ユニットが使用可能になると、ユニットがシステムに接続されたとき、または次のシステム起動時に、そのユニットは自動的にアップグレードされます。

DD Extended Retention を使用したハードウェアのアップグレード

DD Extended Retention が有効な DD システムをより新しいまたはパフォーマンスの高いものにアップグレードできます。たとえば、DD Extended Retention が有効な DD860 を DD Extended Retention が有効な DD990 にアップグレードできます。

注

契約サービス プロバイダーに相談し、適切な「システム コントローラー アップグレード ガイド」の指示を参照してください。

このタイプのアップグレードは、次のように DD Extended Retention に影響します。

- 新しいシステムにアクティブ階層と保存階層よりも新しいバージョンの DD OS がある場合、アクティブ階層と保存階層は新しいシステムのバージョンにアップグレードされます。それ以外の場合、新しいシステムはアクティブ階層と保存階層のバージョンにアップグレードされます。
- 新しいシステムに接続されたアクティブ階層と保存階層は、新しいシステムに所有されます。
- アクティブ階層がある場合、アクティブ階層のレジストリが新しいシステムにインストールされます。それ以外の場合、最近更新されたレジストリがある保存階層のレジストリが新しいシステムにインストールされます。

DD Extended Retention が有効なシステムのリカバリ

DD Extended Retention が有効なシステムでアクティブ階層と保存ユニットのサブセットが失われ、利用できるレプリカがない場合は、サポートにより、残りの封印された保存ユニットを新しい DD システムに再構成できる場合があります。

DD Extended Retention が有効な DD システムは、1 つ以上の保存ユニットが失われた場合に読み取り/書き込み要求サービスを引き続き利用できるように設計されています。ファイル システムをリスタートするまで、または保存ユニットに保管されたアクセス データへのアクセスを試みるまで、保存ユニットが失われたことがファイル システムで検出されない場合があります。後者の状況で、ファイル システムがリスタートする可能性があります。保存ユニットが失われたことをファイル システムが検出した後、そのユニットに保存されているデータへの要求に応答して、エラーが返されます。

消失したデータをレプリカからリカバリすることができない場合は、サポートにより、失われた保存ユニットと、そのユニットにすべてまたは一部が存在するファイルを削除して、システムをクリーンアップできる可能性があります。

レプリケーション リカバリの使用

DD Extended Retention が有効な DD システムのレプリケーション リカバリ手順は、レプリケーション タイプによって異なります。

- コレクション レプリケーション—新しいソースを、デスティネーションと同じ数（またはそれ以上）の保存ユニットを持つ DD Extended Retention が有効な DD システムとして構成する必要があります。保存ユニットが追加され、レプリケーション リカバリが開始されるまでは、新しいソースでファイル システムを有効化することはできません。

  注

  1 つの保存ユニットなど、システムの一部のみをコレクション レプリカからリカバリする必要がある場合は、サポートに連絡してください。

- MTree レプリケーション：「[DD Replicator の扱い]」の章の「[MTree レプリケーション]」のセクションを参照してください。
- DD Boost 管理ファイル レプリケーション：「Data Domain Boost for OpenStorage 管理ガイド」を参照してください。

システム障害からのリカバリ

DD Extended Retention が有効な DD システムには、システムのさまざまな部分での障害に対処するためのツールが装備されています。

手順

1. システム コントローラーとストレージ間の接続をリストアします。システム コントローラーが損失した場合は、新しいシステム コントローラーと交換する。
2. データは消失したがレプリカが使用できる場合は、レプリカからデータのリストアを試みる。レプリカが利用できない場合は、サポートを通じて DD Extended Retention の障害分離機能を活用し、データの消失を制限します。

アーカイブ階層から DD Cloud Tier へのデータの移行

この手順では、MTree レプリケーションを使用して、Extended Retention のある Data Domain システムのアーカイブ階層から、シングル ノードの Data Domain システムまたは DD Cloud Tier を持つ DD VE インスタンスにデータを移行します。

はじめに

- レプリケーションおよび DD Cloud Tier のライセンスが必要です。
- ターゲット システムは、DD Cloud Tier をサポートするために、Data Domain Operating System バージョン 6.0 以降を実行している必要があります。
- データは少なくとも 14 日間はターゲット システム上の DD Cloud Tier ストレージに移動されないため、ターゲット システムには、ソース システム上のアクティブ階層とアーカイブ階層の両方からのデータを保持するのに十分なアクティブ階層容量が必要です。
- Data Domain では、少なくとも 14 日間のレプリケートされたデータ向けに、十分なアクティブ階層容量をキャパシティ プランニングに含めることをお勧めします。
- ソース システム上のすべてのバックアップ ジョブおよびその他のライト アクティビティは、ターゲット システムにリダイレクトする必要があります。
- ターゲット システムは、ソース システムによって満たされたものと同じコンプライアンス要件をすべて満たしている必要があります。

- お客様は、ターゲットおよびソースの Data Domain システムに対するすべての適切なアカウントと資格情報を提供する必要があります。

その他の考慮事項：

- DD Cloud Tier ストレージへの即時のデータ移行が必要な場合は、Dell EMC サポートにお問い合わせください。
- お客様のバックアップ アプリケーションは、このデータ移行をトラッキングできません。
- この手順では、MFR（管理ファイル レプリケーション）については説明しません。
- Data Domain システムで使用できるライセンス：
  - レガシー ライセンス：`license show` コマンドを使用
  - ELMS ライセンス：`elicense show` コマンドを使用

レガシー ライセンスを使用する Data Domain システムでは、ライセンスを段階的に追加できます。レガシー ライセンスでは、新しい機能の一部がサポートされないことに注意してください。

DD OS 6.0 以降でインストールされた Data Domain システムでは、ELMS ライセンスを必要とする機能に変換またはアップグレードした場合は、ライセンスを適用および表示するときに `elicense` コマンドを使用します。新しいライセンスキー ファイルを適用すると、新しいキー一式によって古いキーが完全に置き換えられます。

⚠ 注意

ELMS ライセンスを更新する場合は、既存の容量または機能を削除しないようにしてください。

この手順では、次の使用法について説明します。

- お客様は、アーカイブ階層ストレージからターゲット システム上の DD Cloud Tier ストレージにデータを移動したいと考えています。
- お客様は、ソース システム上のアクティブおよびアーカイブ階層ストレージからターゲット システム上のアクティブ階層ストレージにデータを移動したいと考えています。
- お客様は、複数のソース システム上のアーカイブ階層ストレージからターゲット システム上のアクティブまたは DD Cloud Tier ストレージにデータを移動したいと考えています。
- 移行操作の完了後に、ソース システムまたはそのディスク エンクロージャをリパーパスすることをお客様が望んでいます。

キャパシティ プランニング

はじめに

ターゲット システムには、ソース システムのアクティブ階層とアーカイブ階層を組み合わせて格納するための十分なアクティブ階層容量が必要です。

さらに、ソース システムのアクティブ階層には、アーカイブ階層へのデータ移動が停止された時点から、ソース システムからターゲット システムへの移行が完了するまでの期間に、スケジュール設定されたバックアップからのすべてのデータを保持するための十分なスペースが必要です。

この手順は、2 つの DD9800 システムと 10 GbE LAN 接続を使用して開発およびテストされました。

手順

1. お客様が指定した sysadmin アカウント ログイン資格情報を使用して、ソース Data Domain システムにログインし、過去 7 日間にソース システムのアクティブ階層に取得されたデータ量を特定します。

注

この情報は、アプライアンスによって生成された最後の Autosupport からも抽出できます。この情報に Autosupport を使用する場合は、最新のものであることを確認してください。

```
# filesys show compression
From: 2018-08-29 17:00 To: 2018-09-05 17:00

Active Tier:
                Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                   (GiB)       (GiB)        Factor       Factor          Factor
                                                                   (Reduction %)
-------------   --------   ---------   -----------   ----------   -------------
Written:
  Last 7 days    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
  Last 24 hrs    80730.2     37440.7          1.0x         2.2x     2.2x
(53.6)
-------------   --------   ---------   -----------   ----------   -------------

Archive Tier:
                Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                   (GiB)       (GiB)        Factor       Factor          Factor
…
…
Currently Used:*
               Pre-Comp   Post-Comp   Global-Comp   Local-Comp      Total-Comp
                  (GiB)       (GiB)        Factor       Factor          Factor

…
…
       Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100
```

この例では、週単位の取得は 1 週間あたり約 37 TB で、1 日あたり 5.28 TB に相当します。

2. ソース システムで、 `filesys show space` コマンドを実行して、アクティブ階層の空き容量を判別します。

```
# filesys show space
Active Tier:
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB*
----------------   --------   --------   ---------   ----   --------------
/data: pre-comp           -    69480.4           -      -                -
/data: post-comp    30352.2       35.5     30316.7     0%              0.0
/ddvar                 47.2        9.2        35.6    21%                -
/ddvar/core           984.3        2.0       932.3     0%                -
----------------   --------   --------   ---------   ----   --------------

Cloud Tier
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -        0.0           -      -               -
/data: post-comp        0.0        0.0         0.0     0%             0.0
----------------   --------   --------   ---------   ----   -------------

Total:
Resource           Size GiB   Used GiB   Avail GiB   Use%   Cleanable GiB
----------------   --------   --------   ---------   ----   -------------
/data: pre-comp           -    69480.4           -      -               -
/data: post-comp    30352.2       35.5     30316.7     0%             0.0
/ddvar                 47.2        9.2        35.6    21%               -
/ddvar/core           984.3        2.0       932.3     0%               -
----------------   --------   --------   ---------   ----   -------------
 * Estimated based on last cleaning of 2018/09/04 06:03:57.
```

3. 前の月に消費されたスペースの量と、ターゲット システムへの移行が完了するまでに必要な追加スペースを見積もります。

4. ソース システムのアクティブ階層の使用可能なスペースが必要な容量より少ない場合は、移行を続行する前に、アクティブ階層にストレージを追加します。

   ⚠ 注意

   これには、この手順を停止し、ストレージの追加後に再開する必要があります。

5. ソース システムのアクティブ階層で十分な容量が使用可能になった後、残りの移行ステップを続行します。

アーカイブ階層へのデータ移動の停止

手順

1. ソース システムに設定されているアーカイブ スケジュールを表示します。

```
# archive data-movement schedule show
Archive data movement is scheduled to run on day(s) "tue" at
"06:00" hrs
```

2. アーカイブ スケジュールを［never］に設定してデータ移動を停止します。

```
# archive data-movement schedule set never
The archive data-movement schedule will be deleted.
        Are you sure? (yes|no|?) [no]: yes
Ok, proceeding.
The archive data-movement is not scheduled.
```

3. データ移動スケジュールが［never］に設定されていることを確認します。

```
# archive data-movement schedule show
There is no archive data movement schedule.
```

4. ソース システムでアーカイブ階層スペース再利用スケジュールが構成されているかどうかを判別します。

```
# archive space-reclamation schedule show
Archive space-reclamation is scheduled to run on day(s) "mon"
at "10:10" hrs
```

5. スペース再利用スケジュールを［never］に設定してデータ移動を停止します。

```
# archive space-reclamation schedule set never
The archive space-reclamation schedule will be reset to "never".
        Are you sure? (yes|no|?) [no]: yes
 ok, proceeding.
 The archive space-reclamation schedule is reset to "never".
```

6. スペース再利用スケジュールが［never］に設定されていることを確認します。

```
# archive space-reclamation schedule show
Archive space-reclamation does not have any schedule.
```

7. ソース システムでデータ移動が進行中でないことを確認します。

```
# archive data-movement status
Data-movement was started on Jun 12 2018 06:00 and completed on
Jun 12 2018 06:01
```

8. ソース システムでスペース再利用が進行中でないことを確認します。

```
# archive space-reclamation status
Space-reclamation has never been started.
```

9. データ移動またはスペース再利用操作が進行中の場合は、終了するまで待ってから続行してください。

ファイルの場所を確認する

必要に応じて、ソース システム MTree を表示して、各 MTree 上のファイルがアクティブ階層またはアーカイブ階層のどちらにあるかを判別します。このタスクは情報提供を目的としており、ソース システムからターゲット システムへのデータ転送を完了するために必要なタスクではありません。

手順

1. データ移動ポリシーが設定されているソース システム上の MTree を表示します。ターゲット システムへのレプリケーションを構成するときに使用するためにこの情報を記録します。

```
# archive data-movement policy show
The default age-threshold value is "none".
Mtree-name                    Age-threshold
----------------------------  --------------
/data/col1/backup             none (default)
/data/col1/large_files_100gb  1
----------------------------  --------------
```

2. 特定の MTree のファイルの場所を表示します。

```
# archive report generate file-location path /data/col1/large_files_100gb
-------------------------------                 ----------------------------
File Name                                       Location(Tier/Archive Unit)
-------------------------------                 ----------------------------
/data/col1/large_files_100gb/File_50g.0002.0000  Active
/data/col1/large_files_100gb/File_50g.0001.0000  Active
/data/col1/large_files_100gb/File_50g.0003.0000  archive-unit-2
/data/col1/large_files_100gb/File_50g.0006.0000  archive-unit-2
```

3. 必要に応じて、`archive report generate file-location path all` コマンドを実行して、システム上に存在するすべてのファイルのリストを表示します。

注

ソース システムに保管されているファイルの数によっては、このコマンドが完了するまで長い時間がかかります。

Data Domain レプリケーション ライセンスの適用

手順

1. レガシー ライセンスを使用するソース システムのライセンスを表示します。

```
# license show
Feature licenses:
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
--   -------------------   ------------------
```

2. レプリケーション ライセンスを追加します。

```
# license add <license-key>
```

3. レプリケーション ライセンスがソース システムに追加されていることを確認します。

```
# license show
Feature licenses:
##   License Key           Feature
--   -------------------   ------------------
1    SSRF-VRVZ-ZHYB-WDRF   EXTENDED-RETENTION
2    WTXV-TSWX-HWDR-RHDX   DDBOOST
```

```
3    EZXW-SZZF-BGCS-VRZX   REPLICATION
--   -------------------   -----------------
```

4. ELMS ライセンスを使用するターゲット システムのライセンスを表示します。

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                        Count   Mode              Expiration Date
--   ----------------------------   -----   ---------------   ---------------
1    DDBOOST                            1   permanent         n/a
--   ----------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

5. ライセンス ポータルから取得したライセンス キーを更新して、レプリケーション ライセンスを追加します。テキスト エディタでライセンス ファイルを開き、それをコピーして更新プロンプトに貼り付け、次に **Ctrl + D** キーを押します。

```
# elicense update
Enter the content of license file and then press Control-D, or
press Control-C to cancel.
```

6. レプリケーション ライセンスがソース システムに追加されていることを確認します。

```
# elicense show
System locking-id: APM00000000001

Licensing scheme: EMC Electronic License Management System (ELMS) node-locked mode

Capacity licenses:
##   Feature              Shelf Model   Capacity     Mode        Expiration Date
--   ------------------   -----------   ----------   ---------   ---------------
1    CAPACITY-ACTIVE      ES30          32.74 TiB    permanent   n/a
2    SSD-CAPACITY         n/a           1.45 TiB     permanent   n/a
3    CLOUDTIER-CAPACITY   n/a           218.27 TiB   permanent   n/a
--   ------------------   -----------   ----------   ---------   ---------------
Licensed Active Tier capacity: 32.74 TiB*
* Depending on the hardware platform, usable filesystem capacities may vary.

Feature licenses:
##   Feature                        Count   Mode              Expiration Date
--   ----------------------------   -----   ---------------   ---------------
1    REPLICATION                        1   permanent         n/a
2    DDBOOST                            1   permanent         n/a
--   ----------------------------   -----   ---------------   ---------------
License file last modified at : 2018/06/28 06:29:03.
```

ソース システムからターゲット システムへのレプリケーションの開始

Data Domain システムが保持できる MTree およびレプリケーション コンテキストの最適な最大数に注意してください。ソース システムに、同時に許可される最大レプリケーション コンテキスト数を超える数の MTree がある場合、ターゲット システムにデータを転送するために、複数のシリアル レプリケーション コンテキストが必要になることがあります。たとえば、DD860 は 90 個の MTree レプリケーション コンテキストをサポートし、DD990 は最大 270 個の MTree レプリケーション コンテキストをサポートします。

手順

1. ソース システムのホスト名を判別します。

```
# hostname
The Hostname is: Source.ER.FQDN
```

2. ターゲット システムのホスト名を判別します。

```
# hostname
The Hostname is: Target.DD.FQDN
```

3. ソース システムで、ターゲット システムへの MTree レプリケーション コンテキストを設定します。

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

4. ターゲット システムで、ソース システムへの MTree レプリケーション コンテキストを設定します。

```
# replication add source mtree://Source.ER.FQDN/data/col1/large_files_100gb destination
mtree://Target.DD.FQDN/data/col1/large_files_100gb encryption enabled
Encryption enabled for replication context mtree://Target.DD.FQDN/data/col1/
large_files_100gb
Please verify that replication encryption is also enabled for this context on the
remote host.
```

5. ソース システムで、レプリケーション操作を開始します。このコマンドは、ターゲット システムで実行する必要はありません。

注

レプリケーション コンテキストを初期化するために必要な時間は、最初にレプリケートされるソース MTree に存在するデータの量によって異なります。

```
# replication initialize mtree://Target.ER.FQDN/data/col1/
large_files_100gb
(00:08) Waiting for initialize to start...
(00:10) Initialize started.
Use 'replication watch mtree://Target.DDR.FQDN/data/col1/one'
to monitor progress.
```

6. ソース システムで、レプリケーション構成にエラーがないことを確認します。

注

レプリケーション コンテキストを初期化するために必要な時間は、最初にレプリケートされるソース MTree に存在するデータの量によって異なります。

```
#  replication status mtree://target.ER.FQDN/data/col1/
large_files_100gb
CTX:                                    1
Mode:                                   source
Destination:                            mtree://Target.DD.FQDN/
data/col1/one
Enabled:                                yes
Low bandwidth optimization:             disabled
Replication encryption:                 enabled
Replication propagate-retention-lock:   enabled
Local filesystem status:                enabled
Connection:                             connected since Tue Jun
12 17:46:14
State:                                  initializing 3/3 0%
```

```
Error:                                  no error
Sync'ed-as-of time:                     -
Current throttle:                       unlimited
```

7. ソース システムで、レプリケーションが進行中であることを確認します。

```
#  replication watch mtree://Source.ER.FQDN/data/col1/large_files_100gb
Use Control-C to stop monitoring.

(00:00) Replication initialize started...
(00:02) initializing:
(00:18)       0% complete, pre-comp: 213183 KB/s, network: 120855 KB/s
(00:22)       0% complete, pre-comp: 246130 KB/s, network: 120719 KB/s
```

レプリケーションの進行状況の監視

手順

1. ソース システム上のすべての MTree レプリケーション コンテキストについて構成の詳細を表示します。

```
# replication show config
```

2. 進行中のすべてのレプリケーション操作の全体的な進行状況を表示します。

```
# replication show detailed-stats
```

3. 特定のレプリケーション操作の進行状況を表示します。

```
# replication show detailed-stats mtree://Target.ER.FQDN/data/col1/large_files_100gb
```

4. すべてのレプリケーション コンテキストのパフォーマンスを表示します。

```
# replication show performance all
06/12 17:58:14
       rctx://1               rctx://2               rctx://3
 Pre-comp    Network     Pre-comp    Network     Pre-comp    Network
  (KB/s)     (KB/s)       (KB/s)     (KB/s)       (KB/s)     (KB/s)
 ---------  ---------    ---------  ---------    ---------  ---------
     29459      37607        36374      38071     13089559      39043
    113832      45061        38138      37327     13012122      38812
     29298      42153        33231      36388     12869385      38387
```

レプリケーションの初期化の完了または同期の確認

手順

1. ソース システムから、レプリケーション統計を表示します。

```
# replication show detailed-stats
```

レプリケーション操作が完了すると、出力の `Post-comp Bytes Remaining` 列に値ゼロが表示されます。この `Sync'ed-as-of` 列の値には、ソース システムとターゲット システムが同期している直近の時刻が表示されます。

2. レプリケーションがまだ進行中の場合は、操作が完了するまで待機します。
3. ソースとターゲットのシステムの MTree サイズが一致していることを確認します。両方のシステムで次のコマンドを実行します。

```
# mtree list
Name                          Pre-Comp (GiB)   Status
----------------------------  --------------   ------
/data/col1/large_files_100gb          2500.0   RW
----------------------------  --------------   ------
```

レプリケーション コンテキストを中断する

はじめに

ソース システム上の MTree がデータを取得しなくなったことを確認します。

手順

1. ソース システム上のレプリケーション コンテキストを中断します。

```
# replication break mtree://Target.DD.FQDN /data/col1/
large_files_100gb
```

2. ターゲット システム上のレプリケーション コンテキストを中断します。

```
# replication break mtree://Target.DD.FQDN /data/col1/
large_files_100gb
```

3. ソース システム上のレプリケーション コンテキストが中断されていることを確認します。

```
# replication show config
```

4. ターゲット システム上のレプリケーション コンテキストが中断されていることを確認します。

```
# replication show config
```

5. ターゲット システムの MTree が読み取り/書き込みに設定されていることを確認します

```
# mtree list
Name                            Pre-Comp (GiB)   Status
------------------------------  --------------   ------
/data/col1/large_files_100gb    2500.0           RW
------------------------------  --------------   ------
```

ソース システムのリパーパス

はじめに

⚠ 注意

ソース システムをリパーパスする前に、次の項目を完了する必要があります。すべての要件が完了するまで、このタスクを続行しないでください。

- **ソース システムからのすべてのデータがターゲット システムにレプリケートされていること。**
- **すべてのバックアップ ジョブがターゲット システムをポイントするようになったこと。**
- **古いバックアップのすべての読み取りとリストアが、ターゲット システムによって実行されていること。**
- **すべてのコンプライアンス要件がターゲット システムによって満たされていること。**

手順

1. ソース システム上のファイル システムが破棄されて占有領域の解放処理が行われていること。

```
# filesys destroy and-zero
```

注

アーカイブ階層を無効化することはできません。削除する唯一の方法は、ファイル システムを破棄することです。

2. アーカイブ階層に接続されたディスク エンクロージャを識別します。

```
# storage show tier archive
Archive tier details:
Disk       Disks      Count   Disk       Additional
```

```
Group                          Size       Information
-------   --------   -----    --------   -----------
dg2       4.1-4.15   15       1.8 TiB
dg3       3.1-3.15   15       1.8 TiB
```

3. システムからアーカイブ階層ストレージ エンクロージャを除去します。

```
# storage remove enclosures 3
Removing enclosure 3...Enclosure 3 successfully removed.

Updating system information...done

Successfully removed: 3  done

# storage remove enclosures 4
Removing enclosure 4...Enclosure 4 successfully removed.

Updating system information...done

Successfully removed: 4  done
```

4. システムからアーカイブ階層エンクロージャが除去されていることを確認します。

```
# storage show all
Active tier details:
Disk      Disks      Count   Disk       Additional
Group                        Size       Information
-------   --------   -----   --------   -----------
dg1       2.1-2.14   14      1.8 TiB
(spare)   2.15       1       1.8 TiB
-------   --------   -----   --------   -----------
Current active tier size: 21.8 TiB
Active tier maximum capacity: 43.7 TiB
Storage addable disks:
Disk        Disks      Count   Disk       Enclosure   Shelf
Capacity   Additional
Type                           Size       Model       License
Needed   Information
---------   --------   -----   --------   ---------
--------------   ----------
(unknown)   3.1-3.15   15      1.8 TiB    ES30        21.8 TiB
(unknown)   4.1-4.15   15      1.8 TiB    ES30        21.8 TiB
---------   --------   -----   --------   ---------
--------------   ----------
```

5. ラックからアーカイブ階層ストレージ エンクロージャを除去します。

ターゲットシステムでの DD Cloud Tier の構成

DD Cloud Tier には、DD OS 6.0.X 以降が必要で、特定の Data Domain システム モデルでのみサポートされています。サポートするプラットフォーム（480 ページ）に、DD Cloud Tier をサポートするモデルのリストがあります。DD Cloud Tier とアーカイブ階層のストレージは、同じ Data Domain システム上で同時に構成することはできません。

手順

1. アクティブ階層とクラウド階層の両方のストレージを構成します。動作条件として、アクティブ階層およびクラウド階層の両方で適切な容量のライセンスがインストールされている必要があります。

   a. CLOUDTIER-CAPACITY および CAPACITY-ACTIVE の機能のライセンスがインストールされていることを確認します。ELMS ライセンスを確認するには、次のように入力します。

   ```
   # elicense show
   ```

   ライセンスがインストールされていない場合は、`elicense update` コマンドを使用してライセンスをインストールします。コマンドを入力し、次のプロンプトの後で、ライセンス ファイルの内容をペーストします。ペースト後に、キャリッジ リターンがあることを確認し、

Ctrl+D を押して保存します。ライセンスを置き換えるようプロンプトが表示されたら、[yes] と答えます。ライセンスが適用され、表示されます。

```
# elicense update
Enter the content of license file and then press Control-D,
or press Control-C to cancel.
```

b. 使用可能なストレージを表示します。

```
# storage show all# disk show state
```

c. アクティブ階層にストレージを追加します。

```
# storage add enclosures <enclosure no> tier active
```

d. クラウド階層にストレージを追加します。

```
# storage add enclosures <enclosure no> tier cloud
```

2. 証明書をインストールします。

クラウド プロファイルを作成する前に、関連づけられた証明書をインストールする必要があります。詳細については、証明書のインポート（590 ページ）を参照してください。

AWS、Virtustream、Azure パブリック クラウド プロバイダーの場合は、ルート CA 証明書を https://www.digicert.com/digicert-root-certificates.htm からダウンロードできます。

- AWS または Azure クラウド プロバイダの場合は、Baltimore CyberTrust ルート証明書をダウンロードします。
- Alibaba の場合は、Alibaba が https://support.globalsign.com/customer/portal/articles/1426602-globalsign-rootcertificates から GlobalSign ルート R1 証明書をダウンロードします。
- Virtustream クラウド プロバイダの場合は、DigiCert High Assurance EV Root CA 証明書をダウンロードします。
- ECS の場合、ルート証明機関はお客様によって異なります。詳細については、ロード バランサーのプロバイダにお問い合わせください。

ダウンロードした証明書ファイルには、拡張子.crt が付いています。openssl がインストールされている任意の Linux または Unix システム上で openssl を使用して、ファイルを.crt 形式から.pem に変換します。

```
$openssl x509 -inform der -in DigiCertHighAssuranceEVRootCA.crt
-out DigiCertHighAssuranceEVRootCA.pem
```

```
$openssl x509 -inform der -in BaltimoreCyberTrustRoot.crt -out
BaltimoreCyberTrustRoot.pem
```

```
# adminaccess certificate import ca application cloud
Enter the certificate and then press Control-D, or press
Control-C to cancel.
```

3. クラウドへのデータ移動のために Data Domain システムを構成するには、まず、「クラウド」機能を有効化し、まだ設定されていない場合は、システム パスフレーズを設定する必要があります。

```
# cloud enable
Cloud feature requires that passphrase be set on the system.
Enter new passphrase:
Re-enter new passphrase:
Passphrases matched.
The passphrase is set.
Encryption is recommended on the cloud tier.
```

```
    Do you want to enable encryption? (yes|no) [yes]:
Encryption feature is enabled on the cloud tier.
Cloud feature is enabled.
```

4. クラウド プロバイダの認証情報を使用して、クラウド プロファイルを構成します。プロンプトおよび変数は、プロバイダによって異なります。

```
# cloud profile add <profilename>
```

注

セキュリティ上の理由から、このコマンドでは、入力するアクセス キー/シークレット キーは表示されません。

プロバイダを選択します。

```
Enter provider name (alibabacloud|aws|azure|ecs|google|
s3_flexible|virtustream)
```

- Alibaba Cloud では、アクセス キー、シークレット キー、ストレージ クラス、リージョンが必要です。
- AWS S3 では、アクセス キー、シークレット キー、ストレージ クラス、リージョンが必要です。
- Azure では、アカウント名（アカウントが Azure Government アカウントであるかどうかを問わない）、プライマリ キー、セカンダリ キー、ストレージ クラスが必要です。
- ECS では、アクセス キー、シークレット キー、エンドポイントを入力する必要があります。
- Google Cloud Platform には、アクセス キー、シークレット キー、およびリージョンが必要です。（ストレージ クラスはニアラインです）。
- S3 フレキシブル プロバイダでは、プロバイダ名、アクセス キー、シークレット キー、リージョン、エンドポイント、ストレージ クラスが必要です。
- Virtustream では、アクセス キー、シークレット キー、ストレージ クラス、リージョンが必要です。

各プロファイルの追加の最後に、プロキシを設定するかどうか質問されます。設定する場合は、次の値が必要です。proxy hostname、proxy port、proxy username、proxy password。

5. クラウド プロファイル構成を確認します。

```
# cloud profile show
```

6. まだ作成されていない場合は、アクティブ階層のファイル システムを作成します。

```
# filesys create
```

7. ファイル システムを有効化します。

```
# filesys enable
```

8. クラウド ユニットを構成します。

```
# cloud unit add unitname profile profilename
```

`cloud unit list` コマンドを使用して、クラウド ユニットをリストします。

9. 必要に応じて、クラウド ユニットの暗号化を構成します。

   a. ENCRYPTION ライセンスがインストールされていることを確認します。

```
# elicense show
```

b. クラウド ユニットの暗号化を有効化します。

```
# filesys encryption enable cloud-unit unitname
```

c. 暗号化ステータスを確認します。

```
# filesys encryption status
```

10. 1 つ以上の MTree を作成します。

```
# mtree create /data/col1/mt11
```

11. DD Cloud Tier の設定を確認します。

```
# cloud provider verify
This operation will perform test data movement after creating a temporary profile and
bucket.
Do you want to continue? (yes|no) [yes]:
Enter provider name (aws|azure|virtustream|ecs|s3_generic): aws
Enter the access key:
Enter the secret key:
Enter the region (us-east-1|us-west-1|us-west-2|eu-west-1|apnortheast-1|ap-southeast-1|
ap-southeast-2|
sa-east-1|ap-south-1|ap-northeast-2|eu-central-1):

Verifying cloud provider …
This process may take a few minutes.
Cloud Enablement Check:
 Checking Cloud feature enabled: PASSED
 Checking Cloud volume: PASSED

Connectivity Check:
 Checking firewall access: PASSED
 Validating certificate PASSED

Account Validation:
 Creating temporary profile: PASSED
 Creating temporary bucket: PASSED

S3 API Validation:
 Validating Put Bucket: PASSED
 Validating List Bucket: PASSED
 Validating Put Object: PASSED
 Validating Get Object: PASSED
 Validating List Object: PASSED
 Validating Delete Object: PASSED
 Validating Bulk Delete: PASSED

Cleaning Up:
 Deleting temporary bucket: PASSED
 Deleting temporary profile: PASSED

Provider verification passed.
```

12. この MTree のファイル移行ポリシーを構成します。このコマンドでは、複数の MTree を指定できます。ポリシーは、経過時間の閾値または範囲に基づいて作成できます。

a. 経過時間の閾値（指定した時間経過より古いファイルをクラウドに移行）を構成するには、次のようにします。

```
# data-movement policy set age-threshold age_in_days to-tier
cloud cloud-unit unitname mtrees mtreename
```

b. 時間範囲（指定した経過時間の範囲に含まれるファイルのみの移行）を構成するには、次のようにします。

```
# data-movement policy set age-range min-age age_in_days max-
age age_in_days to-tier cloud cloud-unit unitname mtrees
mtreename
```

13. ファイル システムをエクスポートし、クライアントからファイル システムをマウントし、アクティブ階層にデータを取得します。データ移行の対象となるように、取得したファイルの変更日を変更します。（データ移動ポリシーを構成するときに指定した経過時間の閾値の値よりも前の日付を設定）。
14. 経過時間に達したファイルのファイル移行を開始します。このコマンドでも、複数の MTree を指定できます。

    ```
    # data-movement start mtrees mtreename
    ```

    データ移動のステータスを確認するには、次のようにします。

    ```
    # data-movement status
    ```

    また、データ移動の進行状況を監視することもできます。

    ```
    # data-movement watch
    ```

15. ファイル移行が機能してファイルがクラウド階層に格納されたことを確認します。

    ```
    # filesys report generate file-location path all
    ```

16. ファイルをクラウド階層に移行した後で、ファイルを直接読み取ることはできません（実行しようとするとエラーが発生します）。ファイルは、アクティブ階層にリコールすることのみ可能です。アクティブ階層にファイルをリコールするには、次のようにします。

    ```
    # data-movement recall path pathname
    ```

第 20 章

DD Retention Lock

本章には、次のセクションが含まれます。

- DD Retention Lock の概要 550
- 対応するデータ アクセス プロトコル 552
- MTree における DD Retention Lock の有効化 553
- クライアント側保存ロック ファイル コントロール 556
- DD Retention Lock を使用したシステムの動作 561

DD Retention Lock の概要

DD Retention Lock で有効化された MTree 上でデータがロックされると、DD Retention Lock によってデータの整合性が保たれます。ロックされたデータは、ユーザー定義保存期間（最長 70 年間）は上書き、変更、削除はできません。

2 つの DD Retention Lock のエディションがあります。

- ［Data Domain Retention Lock Governance Edition］は、DD OS 5.2 以前の Data Domain Retention Lock の機能を保持しています。システム管理者によって実装された内部 IT ガバナンス ポリシーに準拠するため、Data Domain Retention Lock Governance を使用して、特定の期間中保存されるデータの保存ポリシーを定義できます。
- ［Data Domain Retention Lock Compliance Edition］によって、SEC 17a-4(f)など、最も厳格な規制基準のデータ永続性要件を満たすことができます。規制基準には、次のものが含まれます。
  - CFTC Rule 1.31b
  - FDA 21 CFR Part 11
  - Sarbanes-Oxley Act
  - IRS 98025 および 97-22
  - ISO Standard 15489-1
  - MoREQ2010

  証明書の情報については、次のリンクの「[Compliance Assessments - Summary and Conclusions – EMC Data Domain Retention Lock Compliance Edition]」を参照してください

  https://www.emc.com/collateral/analyst-reports/cohasset-dd-retention-lock-assoc-comp-assess-summ-ar.pdf

  （ログインが必要です）。

  これらの標準を遵守することで、Data Domain Retention Lock Compliance Edition ソフトウェアを使用して Data Domain システムでロックされたファイルは保存期間が終わるまで変更または破棄できなくなります。Data Domain Retention Lock Compliance Edition には、ポリシーの実装のセキュリティ担当者が必要です。監査ログ ファイルは、管理者またはセキュリティ担当者がアクセスできます。

各エディションには、別途アドオン ライセンスが必要であり、いずれかまたは両方を 1 つの Data Domain システム上で使用できます。

DD Retention Lock Governance Edition と Compliance Edition の保存ロック プロトコルは同じです。使用中の差異は、コンプライアンス要件を満たす上での DD Retention Lock Compliance Edition のシステム動作のより厳格な制限によるものです。概要については、次のリンクの「[EMC Data Domain Retention Lock Software – A Detailed Review]」（ホワイト ペーパー）を参照してください

https://www.emc.com/collateral/hardware/white-papers/h10666-data-domain-retention-lock-wp.pdf

（ログインが必要です）。

DD Retention Lock Governance Edition は、セキュリティ担当者を必要とせず、Data Domain システム上のアーカイブ データ保存の高い柔軟性を実現します。

アーカイブ コンプライアンス ストレージ要件については、SEC ルールは、保存ロックされたデータの別のコピーをオリジナルと同じ保存要件で保存することを規定しています。保存ロックされたファイルは、DD Replicator を使用して、他の Data Domain システムにレプリケーションできます。保存ロックさ

れたファイルがレプリケーションされた場合、ソース ファイルと同じ保護レベルでデスティネーション システム上で保存ロックされたままとなります。

DD Retention Lock Governance Edition は、オン プレミス、クラウド ベース、DD3300 DD VE インスタンスでサポートされます。DD Retention Lock Compliance Edition は、オン プレミス、クラウド ベース、または DD3300 DD VE インスタンスでサポートされます。

次のトピックでは、DD Retention Lock の詳細について説明します。

DD Retention Lock プロトコル

保存ロックされたファイルに明示的にコミットされたファイルのみ、Data Domain システム上で保存ロックされます。DD Retention Lock Governance または Compliance がファイルを含む MTree 上で有効な状態で発行されたクライアント側ファイル コマンドを通して、ファイルが保存ロックされたファイルになるようコミットされます。

注

Linux、UNIX、および Windows クライアント環境に対応しています。

（DD Retention Lock Governance または Compliance がファイルを含む MTree 上で有効化された場合）保存対象としてコミットされていない共有またはエクスポートに書き込まれたファイルは、いつでも変更または削除できます。

保存ロックは、クライアント側の atime 更新コマンドで指定された保存期間中、保存中のファイルの変更または削除が CIFS 共有または NFS エクスポートから直接行われることを防ぎます。アーカイブ アプリケーションとバックアップ アプリケーションは、適切な構成されるとこのコマンドを発行できます。このコマンドを発行しないアプリケーションまたはユーティリティは、DD Retention Lock を使用してファイルをロックできません。

保存ロックが後で無効化された場合、または保存ロックライセンスがすでに無効な場合でも、保存ロックされたファイルは、常に変更と予定より早い削除から保護されます。

保存ロックが有効な MTree 内で空ではないフォルダーまたはディレクトリは名称変更または削除できません。ただし、空のフォルダーまたはディレクトリを名称変更または削除し、新規作成します。

ファイルの atime を更新することで、保存ロックされたファイルの保存期間を延長することはできますが、短縮することはできません。

DD Retention Lock Governance および Compliance 両方で、ファイルの保存期間が終了したら、ファイルはクライアント側コマンド、スクリプト、またはアプリケーションを使用して削除できます。ただし、ファイルの保存期間が終了した後でも、そのファイルは変更できません。Data Domain システムは、自動的には保存期間終了時にファイルを削除しません。

DD Retention Lock のフロー

DD Retention Lock を使用したアクティビティの一般的なフロー。

1. DD System Manager またはシステム コンソールから発行された DD OS コマンドを使用して、MTree の DD Retention Lock Governance または Compliance 保存ロックを有効にします。
2. 手動またはスクリプトの使用により適切に構成されたアーカイブ/バックアップ アプリケーションから発行されたクライアント側コマンドを使用して、Data Domain システムでファイルの保存ロックをコミットします。

注

Windows クライアントは、DD OS 互換性を保つためにユーティリティ プログラムをダウンロードする必要がある場合があります。

3. オプションで、クライアント側コマンドを使用してファイル保存時間を延長します。
4. オプションで、クライアント側コマンドを使用して、保存期間の切れたファイルを削除します。

対応するデータ アクセス プロトコル

DD Retention Lock は、業界標準 NAS ベース WORM（Write-Once-Read-Many）プロトコルと互換性があります。Symantec Enterprise Vault、SourceOne、Cloud Tiering Appliance、DiskXtender などのアーカイブ アプリケーションとの統合が可能です。CommVault などのバックアップ アプリケーションを使用しているお客様は、カスタム スクリプトを開発して、Data Domain Retention Lock を使用することもできます。

DD Retention Lock のプロトコル サポートは、次のとおりです。

- NFS は、DD Retention Lock Governance および Compliance 両方に対応しています。
- CIFS は、DD Retention Lock Governance および Compliance 両方に対応しています。
- DD VTL は、DD Retention Lock Governance に対応していますが、DD Retention Lock Compliance には対応していません。
  ここでは [テープ] と呼んでいる仮想テープは、ファイル システム上ではファイルとして表されます。
  - ストレージ プール（ファイル システム上のディレクトリにマッピングされたテープのコレクション）を作成すると、（下位互換性のために）古いスタイルのディレクトリ プールを選択していない限り、MTree が作成されます。DD OS 5.3 以前で作成されたストレージ プールを MTree に変換することもできます。これらの MTree は、保存ロックおよびレプリケーションできます。
  - `vtl tape modify` コマンドを使用して、1 つ以上のテープを保存ロックできます。詳細は、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。`mtree retention-lock revert`**path** コマンドは、`vtl tape modify` コマンドでロックされたテープの保存ロック状態を戻すために使用できます。テープがロック解除されると、それを更新できます。DD VTL サービスが一旦無効化されて、再度有効化されるまで、ロック解除状態は DD System Manager または CLI を介して表示されません。ただし、更新はロック解除されたテープに適用されます。この機能は、DD Retention Lock Governance Edition でのみ使用できます。
  - テープの保存時間は、`time-display retention` 引数で `vtl tape show` コマンドを使用して表示されます。
  - DD System Manager を使用して個別のテープを保存ロックできます。
- DD Boost は、DD Retention Lock Governance および Compliance 両方に対応しています。
  クライアント側スクリプトを使用してバックアップ ファイルまたはバックアップ イメージを保存ロックした場合に、バックアップ アプリケーション（Veritas NetBackup など）が DD Boost を介してシステムでも使用された場合、バックアップ アプリケーションはクライアント側スクリプトのコンテキストを共有しない場合があります。そのため、クライアント側スクリプトを介して保存ロックされたファイルをバックアップ アプリケーションが期限切れにさせるか、削除しようとすると、Data Domain システムでスペースは解放されません。

  Data Domain は、管理者が保存ロック時間に合わせて保存期間ポリシーを変更することを推奨します。これは Veritas NetBackup、Veritas Backup Exec、NetWorker などの、DD Boost と統合されたバックアップ アプリケーションの多くに適用されます。

DSP モードの DD Boost ファイルに取り込み中のデータに対しては、保存ロックを設定できません。保存ロックが設定されているクライアントはエラーを受け取ります。保存ロックはデータの取り込みが完了してから設定してください。

OST モードの DD Boost ファイル、または NFS ファイルに取り込み中のデータに対しては、保存ロックを設定できません。保存ロックが設定されると、データを書き込み中のクライアントはエラーを受け取ります。保存ロックの前に書き込まれた部分ファイルは、ワーム ファイルとしてディスクに設定およびコミットされます。

MTree における DD Retention Lock の有効化

DD Retention Lock Governance または Compliance が有効な MTree 内のファイルのみ、保存ロックできます。

DD Retention Lock Compliance が有効な MTree は、DD Retention Lock Governance MTree には変換できず、その逆の変換もできません。

次の手順では、MTree で DD Retention Lock Governance または DD Retention Lock Compliance を有効化する方法について説明します。

MTree における DD Retention Lock Governance の有効化

DD Retention Lock Governance ライセンスをシステムに追加して、1 つ以上の MTree で DD Retention Lock Governance を有効化します。

手順

1. ［Feature Licenses］に表示されていない場合は、DD Retention Lock Governance ライセンスを追加します。
   a. ［**Administration**］ > ［**Licenses**］を選択します。
   b. ［Licenses］領域で［**Add Licenses**］をクリックします。
   c. ［License Key］テキスト ボックスで、ライセンス キーを入力します。

      注

      ライセンス キーでは大文字と小文字が区別されません。キーを入力する際、ハイフンを含めます。

   d. ［**Add**］をクリックします。
2. 保存ロック用の MTree を選択します。
   a. ［**Data Management**］ > ［**MTree**］を選択します。
   b. 保存ロックに使用する MTree を選択します。空の MTree を作成して、後でそれにファイルを追加することもできます。
3. 選択された MTree の情報を表示するには、［MTree Summary］タブをクリックします。
4. ［Retention Lock］領域まで下にスクロールし、［Retention Lock］の右にある［**Edit**］をクリックします。
5. MTree で DD Retention Lock Governance を有効化し、必要に応じてその MTree のデフォルトの最短および最長保存期間を変更します。

   ［Modify Retention Lock］ダイアログ ボックスで次のアクションを実行します。

a. [**Enable**] を選択して、MTree で DD Retention Lock Governance を有効化します。

b. MTree の最短または最長保存期間を変更するには、最短または最長期間を変更します。

テキスト ボックスに間隔の数字を入力します（`5`、`14` など）。

ドロップダウン リストから、間隔（分、時間、日、年）を選択します。

注

12 時間未満の最短保存期間または 70 年より長い最長保存期間を指定すると、エラーが発生します。

c. [**OK**] をクリックして、設定を保存します。

[Modify Retention Lock] ダイアログ ボックスを閉じた後、更新された MTree 情報が [Retention Lock] 領域に表示されます。

6. MTree の保存ロック情報をチェックします。

次の保存ロック フィールドに留意してください。

- 上部：
  - [Status] フィールドは、MTree の read/write アクセス、MTree 上の保存ロックのタイプ、保存ロックが有効か無効かを示します。
- 下部：
  - [Status] フィールドは、MTree で保存ロックが有効かどうかを示します。
  - [Retention Period] フィールドは、MTree の最短および最長保存期間を示します。MTree でファイルに指定された保存期間は、最短保存期間以上、最長保存期間以下である必要があります。
  - [UUID] フィールドは、MTree に生成された一意の識別番号です。

注

MTree の保存ロック構成設定をチェックするには、ナビゲーション パネルで [MTree] を選択した後、[Summary] タブをクリックします。

必要条件

保存ロックが有効な MTree でファイルを保存ロックします。

MTree における DD Retention Lock Compliance の有効化

DD Retention Lock Compliance ライセンスのシステムへの追加、システム管理者と 1 人以上のセキュリティ担当者のセットアップ、システムでの DD Retention Lock Compliance ソフトウェアの使用の構成と有効化を行い、最終的に 1 つ以上の MTree で DD Retention Lock Compliance を有効化します。

手順

1. もしなければ、DD Retention Lock Compliance ライセンスをシステムに追加します。

a. まず、ライセンスがすでにインストール済みかどうかをチェックします。

```
license show
```

b. RETENTION-LOCK-COMPLIANCE 機能が表示されていない場合、ライセンスをインストールします。

```
license addlicense-key
```

注

ライセンス キーでは大文字と小文字が区別されません。キーを入力する際、ハイフンを含めます。

2. RBAC（役割に基づいたアクセス制御）ルールに従って、1 つ以上のセキュリティ担当者ユーザー アカウントをセットアップします。

a. システム管理者の役割で、セキュリティ担当者アカウントを追加します。

```
user adduserrole security
```

b. セキュリティ担当者許可を有効化します。

```
authorization policy set security-officer enabled
```

3. システムによる DD Retention Lock Compliance の使用を構成および有効化します。

注

DD Retention Lock Compliance を有効化すると、トラブルシューティング時に使用されるシステム機能への低レベル アクセスに多くの制限が適用されます。その制限が適用されると、システムを初期化してからリロードする（システムの上のすべてのデータが失われます）以外に、DD Retention Lock Compliance を無効化する方法はありません。

a. システムによる DD Retention Lock Compliance の使用を構成します。

```
system retention-lock compliance configure
```

システムが自動的に再起動されます。

b. 再起動プロセスが完了した後、システムで DD Retention Lock Compliance を有効化します。

```
system retention-lock compliance enable
```

4. 保存ロックされたファイルを含む MTree 上でコンプライアンスを有効化します。

```
mtree retention-lock enable mode compliance mtreemtree-path
```

注

コンプライアンスは、/backup、またはプール MTree では有効化できません。

5. コンプライアンスが有効な MTree のデフォルトの最短および最長保存ロック期間を変更するには、セキュリティ担当者許可で次のコマンドを使用します。

```
mtree retention-lock set min-retention-
periodperiodmtreemtree-path
mtree retention-lock set max-retention-
periodperiodmtreemtree-path
```

注

保存期間は、[number] [unit]の形式で指定されます。例：1 min、1 hr、1 day、1 mo、1 year。12 時間未満の最短保存期間または 70 年より長い最長保存期間を指定すると、エラーが発生します。

追加 MTree を有効化するには、ステップ 4 および 5 を繰り返します。

必要条件

保存ロック ファイルは保存ロックが有効な MTree に存在します。

クライアント側保存ロック ファイル コントロール

このセクションでは、Data Domain システムに保存されたファイルをロックするための DD Retention Lock クライアント コマンド インターフェイスについて説明します。クライアント コマンドは、DD Retention Lock Governance および Compliance のどちらに対しても同じです。Linux、UNIX、および Windows クライアント環境に対応していますが、Windows クライアントはファイルをロックするために、コマンドを含むユーティリティ プログラムをダウンロードする必要がある場合があります。

注

アプリケーションがすでに業界標準の WORM に対応している場合、WORM ファイルを DD Retention Lock Governance または Compliance が有効な MTree に書き込むと、Data Domain システム上のファイルがロックされます。アプリケーション内での保存時間は、DD Retention Lock 設定に準拠する必要があります。このセクションで説明するコマンドを使用する必要はありません。アプリケーションがテストされ、DD Retention Lock の認定を受けているかどうかをチェックするには、「Data Domain Archive Application Compatibility Guide」を参照してください。

注

NFS を使用するがレガシー OS を実行しているクライアント マシンには、保存期限を 2038 年以降に設定できないものがあります。NFS プロトコルは、2038 年の上限は設けられず、2106 年までの時間を指定することができます。さらに、DD OS では、2038 年の上限は設けられません。

クライアント側コマンドは、個別のファイルの保存ロックの管理に使用されます。これらのコマンドは、すべての保存ロック対応 Data Domain システムに適用され、Data Domain システム上の DD Retention Lock のセットアップと構成と合わせて発行する必要があります。

Windows クライアントに必要なツール

Windows ベース クライアントから保存ロックを実行するには、`touch.exe` コマンドが必要です。

このコマンドを取得するには、Windows のバージョンに応じた Linux/UNIX ベース アプリケーションのユーティリティをダウンロードおよびインストールしてください。これらのユーティリティは Data Domain が最も強く推奨するものであり、顧客環境に合わせて使用する必要があります。

- Windows 8、Windows 7、Windows Server 2008、Windows Vista、Windows Server 2003、Windows XP の場合：
  http://sourceforge.net/projects/unxutils/files/latest
- Windows Server 2008、Windows Vista Enterprise、Windows Vista Enterprise 64-bit 版、Windows Vista SP1、Windows Vista Ultimate、Windows Vista Ultimate 64-bit 版の場合：
  http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23754

- Windows Server 2003 SP1 および Windows Server 2003 R2 の場合
  http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=20983

注

Windows 用の `touch` コマンドは、本章の Linux の例とは形式が異なる可能性があります。

規定されたインストール手順に従い、クライアント マシン上で必要に応じて検索パスを設定します。

Data Domain システム ファイルへのクライアント アクセス

MTree で DD Retention Lock Governance または Compliance を有効化すると、次の操作を実行できます。

- MTree に基づき CIFS 共有を作成します。この CIFS 共有はクライアント マシンで使用できます。
- MTree 用の NFS マウントを作成し、クライアント マシンで NFS マウント ポイントからそのファイルにアクセスします。

注

このセクションで挙げたコマンドは、そのクライアント上でのみ使用するものです。DD System Manager または CLI から実行することはできません。コマンド構文は、使用中のユーティリティによってわずかに異なる可能性があります。

次のトピックでは、クライアント側保存ロック ファイル コントロールの管理方法について説明します。

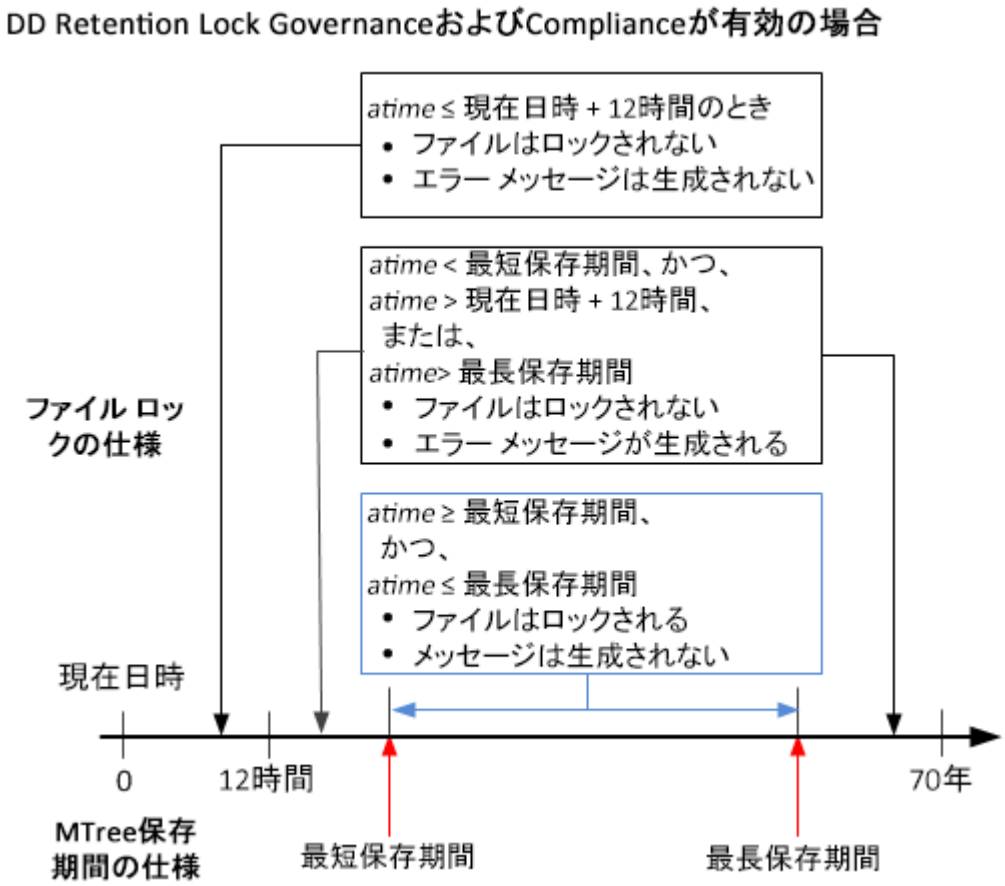
ファイルの保存ロックの設定

ファイルの保存ロックを実行するには、そのファイルの最終アクセス時間（atime）をそのファイルの任意の保存時間（ファイルを削除できるようになる時間）に変更します。

このアクションは通常、アーカイブ アプリケーションによって実行され、Data Domain システムで現在認定されているすべてのアーカイブ アプリケーション（「Data Domain Archive Application Compatibility Guide」を参照）は、ここで説明する基本ロック プロトコルに従います。

指定した将来の atime は、次の図に示すとおり、（現在の時間からのオフセットとして）そのファイルの MTree の最短および最長保存期間に準拠する必要があります。

図 23 ファイルの保存ロック ファイルに対して有効/無効な atimes



注

NFS を使用するがレガシー OS を実行しているクライアント マシンには、保存期限を 2038 年以降に設定できないものがあります。NFS プロトコルは、2038 年の上限は設けられず、2106 年までの時間を指定することができます。さらに、DD OS では、2038 年の上限は設けられません。

エラーは、権限拒否エラーです（EACCESS（標準 POSIX エラー）とも呼ばれます）。そのエラーは、atime を設定したスクリプトまたはアーカイブ アプリケーションに返されます。

注

ファイルは、保存ロックされたファイルとしてコミットされる前に、Data Domain システムへの書き込みを完了している必要があります。

次のコマンドは、atime を設定するため、クライアントで使用できます。

```
touch -a -t [[atime]] [[filename]]
```

atime の形式は次のとおりです。

```
[[[YY]] [YY]]  [MMDDhhmm] [. [ss]]
```

例として、現在の日時が 2012 年 1 月 18 日午後 1 時（201201181300）であり、最短保存期間が 12 時間であると仮定します。最短保存期間の 12 時間をその日付に加えると、時間の結果値は 201201190100 になります。そのため、ファイルの atime が 201201190100 よりも大きい値に設定されている場合、そのファイルは保存ロックされます。

次のコマンドを実行します。

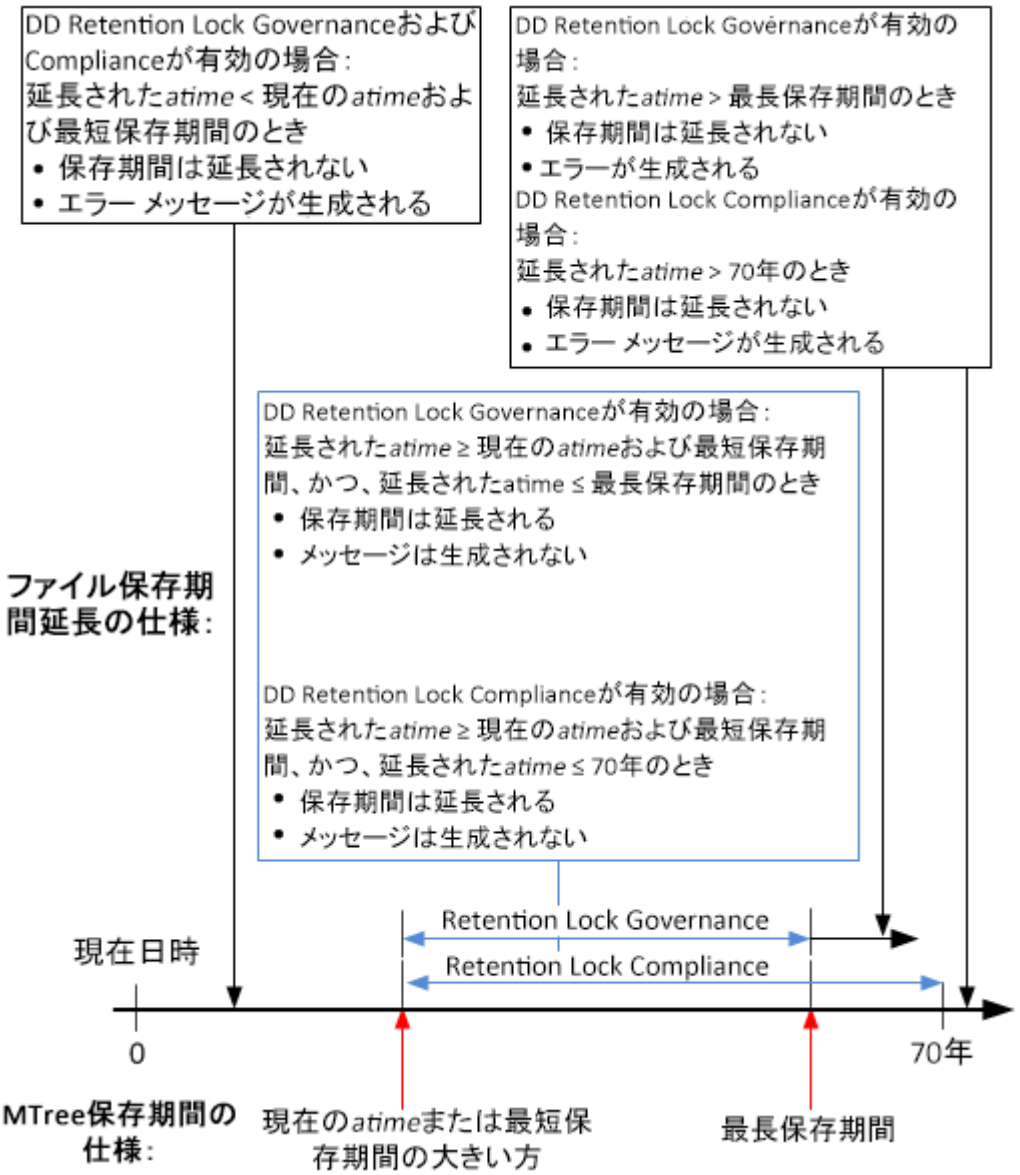
```
ClientOS# touch -a -t 201412312230 SavedData.dat
```

これは、ファイル `SavedData.dat` を 2014 年 12 月 31 日午後 10 時 30 分までロックします。

ファイルの保存ロックの延長

保存ロックされたファイルの保存時間を延長するには、下図に示すとおり、ファイルの **atime** にそのファイルの現在の **atime** よりも大きく、そのファイル **MTree** の最長保存期間よりも小さい値を設定します（現在の時間からのオフセットとして）。

図 24 ファイルの保存ロックの延長に有効/無効な atimes



たとえば、次のコマンドを使用して **atime** を `201412312230` から `202012121230` に変更します。

```
ClientOS# touch -a -t 202012121230 SavedData.dat
```

この場合、2020 年 12 月 12 日 午後 12:30 までファイルがロックされます。

注

NFS を使用するがきわめて古い OS を実行しているクライアント マシンには、保存期限を 2038 年以降に設定できないものがあります。NFS プロトコルは、2038 年の上限は設けられず、2106 年までの時間を指定することができます。さらに、DD OS では、2038 年の上限は設けられません。

エラーは、権限拒否エラーです（EACCESS（標準 POSIX エラー）とも呼ばれます）。そのエラーは、atime を設定したスクリプトまたはアーカイブ アプリケーションに返されます。

保存ロックされたファイルの識別

保存ロックされたファイルの atime は、その保存時間です。ファイルが保存ロックされているかどうかを判断するには、ファイルの atime をその現在の atime よりも早い値に設定します。このアクションは、ファイルが保存ロックされている場合にのみ、権限拒否エラーが出て失敗します。

まず、現在の atime 値をリストし、次のコマンドを使用してそれより早い atime で `touch` コマンドを実行します。

```
ls -l --time=atime [[filename]]
touch -a -t [atime] [[filename]]
```

次の例は、コマンド シーケンスを示しています。

```
ClientOS# ls -l --time=atime SavedData.dat
202012121230
ClientOS# touch -a -t 202012111230 SavedData.dat
```

`SavedData.dat` の atime が 202012121230（2020 年 12 月 12 日午後 12:30）であり、`touch` コマンドがそれより早い atime である 202012111230（2020 年 12 月 11 日午後 12:30）を指定した場合、`touch` コマンドは失敗します。これは、`SavedData.dat` が保存ロックされていることを示します。

注

`--time=atime` オプションは、UNIX のすべてのバージョンで対応しているわけではありません。

ディレクトリの指定とそのファイルのみのタッチ

コマンド ラインを使用して、アクセス時間を変更するファイルが含まれるルート ディレクトリを作成します。

このルーチンでは、root directory to start from には、このクライアント システム コマンドを使用してアクセス時間を変更したいファイルが含まれます。

```
find [[root directory to start from]] -exec touch -a -t
[[expiration time]] {} \;
```

次に例を挙げます。

```
ClientOS# find [/backup/data1/] -exec touch -a -t 202012121230 {} \;
```

ファイルのリストの読み取りとそのファイルのみのタッチ

このルーチンでは、name of file list は、アクセス時間を変更したいファイルの名前を含むテキスト ファイルの名前でしす。各行には、1 つのファイルの名前が含まれます。

次に示すのは、クライアント システム コマンド構文です。

```
touch -a -t [[expiration time]] 'cat [[name of file list]]'
```

次に例を挙げます。

```
ClientOS# touch -a -t 202012121230 'cat /backup/data1/filelist.txt'
```

ファイルの削除または失効

クライアント アプリケーションを使用して期限切れした保存ロックのあるファイルを削除または期限切れにするか、標準 file-delete コマンドを使用してファイルを削除します。

アプリケーションを使用してファイルを期限切れにすると、そのファイルにアプリケーションでアクセスできるようになります。期限切れ操作によって Data Domain システムからファイルを実際に削除するかどうかは任意です。ファイルが削除されなかった場合、アプリケーションは別途削除操作を行います。DD Retention Lock から独立して、ファイルを削除するには適切なアクセス権が必要です。

注

保存ロックされたファイルの保存期間が終了している場合、削除操作を行うと権限拒否エラーが発生します。

Privileged delete

DD Retention Lock Governance（のみ）では、この 2 ステップのプロセスを使用して、保存ロック ファイルを削除できます。

手順

1. `mtree retention-lock revert`path コマンドを使用して、保存ロック ファイルを復元します。
2. `rm`filename コマンドを使用して、クライアント システムのファイルを削除します。

保存ロックされたファイルに対する ctime または mtime の使用

［ctime］は、ファイルの最終メタデータ変更時間です。

ctime

［ctime］は、次のイベントのいずれかが発生すると現在の時間に設定されます。

- 保存ロックされていないファイルが保存ロックされた。
- 保存ロックされたファイルの保存時間が延長された。
- 保存ロックされたファイルの設定が元に戻された。

注

保存ロックされたファイルのユーザー アクセス パーミッションは、Linux コマンド ライン ツール `chmod` を使用して更新されます。

mtime

［mtime］は、ファイルの最終変更時間です。ファイルの内容が変更された場合にのみ変更されます。そのため、保存ロックされたファイルの mtime は変更できません。

DD Retention Lock を使用したシステムの動作

システムの動作については、以降のセクションで、DD Retention Lock Governance と DD Retention Lock Compliance についてそれぞれ説明します。

DD Retention Lock Governance

DD Retention Lock Governance を使用する場合、特定の DD OS コマンドの動作が異なります。以降のセクションでは、それぞれの違いについて説明します。

レプリケーション

コレクション レプリケーション、MTree レプリケーション、ディレクトリ レプリケーションは、ロックされている状態またはロックされていない状態のファイルをレプリケーションします。

ソースでガバナンス保存ロックされたファイルは、デスティネーションでもガバナンス保存ロックされ、保護レベルも同じになります。レプリケーションを実行するには、ソース システムに DD Retention Lock Governance ライセンスがインストールされている必要があります（デスティネーション システムではライセンスは不要です）。

次に示すシステム間でのレプリケーションに対応しています。

- 同じメジャー DD OS バージョンを実行しているシステム（両方のシステムが DD OS 5.5.x.x を実行している場合など）。
- 実行している DD OS のメジャー リリース バージョンの違いが 2 世代上または下の範囲内であるシステム（5.3.x.x と 5.5.x.x、5.5.x.x と 5.3.x.x など）。Cross-release replication is supported only for directory and MTree replication.

注

MTree レプリケーションは、DD OS 5.0 以前では対応していません。

注：

- コレクション レプリケーションと MTree レプリケーションは、MTree で構成された最短および最長保存期間をデスティネーション システムにレプリケーションします。
- ディレクトリ レプリケーションは、最短および最長保存期間をデスティネーション システムにレプリケーションしません。

コレクション、MTree、およびディレクトリ レプリケーションを構成および使用する手順は、DD Retention Lock Governance ライセンスがない Data Domain システムを同じです。

レプリケーション再同期
デスティネーション システムとソース システム間で MTree またはディレクトリ レプリケーション コンテキストが破棄されると、`replication resync`**destination** コマンドはデスティネーションをソースに同期させようとします。このコマンドはコレクション レプリケーションには使用できません。次の点を確認してください。

- コンテキストが破棄される前にファイルをクラウド階層に移行する場合、MTree レプリケーション再同期によってデスティネーション上のすべてのデータが上書きされます。そのため、ファイルをもう一度クラウド階層に移行する必要があります。
- デスティネーション ディレクトリで DD Retention Lock が有効化されており、ソース ディレクトリで DD Retention Lock が有効化されていない場合、ディレクトリ レプリケーションの再同期は失敗します。
- Mtree レプリケーションでは、ソースの MTree で保存ロックが有効化されておらず、デスティネーションの MTree で保存ロックが有効化されている場合、再同期は失敗します。
- Mtree レプリケーションでは、ソースとデスティネーションの Mtree で保存ロックが有効化されていても、伝播保存ロック オプションが FALSE に設定されていると、再同期は失敗します。

Fast Copy

`filesys fastcopy [retention-lock] source`**src**`destination`**dest** コマンドを DD Retention Lock Governance が有効な MTree があるシステムで実行する場合、**fastcopy** の操作中はコマンドにより Retention Lock ファイル属性が維持されます。

注

デスティネーション MTree で保存ロックが有効でない場合、Retention Lock ファイル属性は維持されません。

filesys destroy

DD Retention Lock Governance が有効な MTree のあるシステムで実行された場合の `filesys destroy` コマンドの影響。

- 保存ロックされたデータを含め、すべてのデータが破棄されます。
- すべての `filesys` オプションがデフォルトに戻ります。つまり、保存ロックは無効化され、最短および最長保存期間は新たに作成されたファイル システムのデフォルト値に戻るということです。

注

このコマンドは、DD Retention Lock Compliance がシステムで有効になっている場合は使用できません。

MTree の削除

現在データを含んでいる、`mtree delete` **mtree-path** コマンドが、DD Retention Lock Governance が有効な（または過去に有効であった）MTree を削除しようとすると、コマンドはエラーを返します。

注

`mtree delete` の動作は、ディレクトリを削除するコマンドと同様です。MTree が空の場合のみ、保存ロックが有効な（または過去に有効であった） MTree を削除できます。

DD Retention Lock Compliance

DD Retention Lock Compliance を使用する場合、特定の DD OS コマンドの動作が異なります。以降のセクションでは、それぞれの違いについて説明します。

レプリケーション

DD Retention Lock Compliance が有効な MTree は、MTree とコレクション レプリケーションのみを介してレプリケーションできます。ディレクトリ レプリケーションはサポートされていません。

MTree レプリケーションとコレクション レプリケーションは、ロックされている状態またはロックされていない状態のファイルをレプリケーションします。ソースでコンプライアンス保存ロックされたファイルは、デスティネーションでもコンプライアンス保存ロックされ、保護レベルも同じになります。MTree 上で構成された最短および最大保存期間は、デスティネーション システムにレプリケーションされます。

コレクション レプリケーションを実行するには、デスティネーション システムへのレプリケーションを開始する前、および以降のソース/レプリカ ペアの有効期間中、同じセキュリティ担当者ユーザーがソース システムとデスティネーションシステム両方に存在している必要があります。

レプリケーション再同期

`replication resync`**destination** コマンドは、MTree レプリケーションで使用できますが、コレクション レプリケーションでは使用できません。

- デスティネーション MTree に、ソースに存在しない、保存ロックされたファイルが含まれる場合、再同期は失敗します。
- ソースと宛先両方の MTree で DD Retention Lock Compliance が有効になっていなければ、再同期は失敗します。

レプリケーション プロシージャ

このセクションのトピックでは、DD Retention Lock Compliance に対応している MTree およびコレクション レプリケーション プロシージャについて説明します。

注

次のトピックで言及するコマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

MTree のレプリケーション 1 対 1 トポロジー

ソース システムからデスティネーション システムに、DD Retention Lock Compliance が有効な MTree をレプリケーションします。

はじめに

MTree 上で DD Retention Lock を有効化し、レプリケーションの前にクライアント側保存ロック ファイル制御を構成します。

手順

1. 別途指示がある場合を除き、デスティネーション システムでのみで次の手順を行います。
2. もしなければ、DD Retention Lock Compliance ライセンスをシステムに追加します。
   a. まず、ライセンスがすでにインストール済みかどうかをチェックします。
      `license show`
   b. RETENTION-LOCK-COMPLIANCE 機能が表示されていない場合、ライセンスをインストールします。
      `license add`**license-key**

      注

      ライセンス キーでは大文字と小文字が区別されません。キーを入力する際、ハイフンを含めます。
3. RBAC（役割に基づいたアクセス制御）ルールに従って、1 つ以上のセキュリティ担当者ユーザー アカウントをセットアップします。
   a. システム管理者の役割で、セキュリティ担当者アカウントを追加します。
      `user add`**user**`role security`
   b. セキュリティ担当者許可を有効化します。
      `authorization policy set security-officer enabled`
4. システムによる DD Retention Lock Compliance の使用を構成および有効化します。

注

DD Retention Lock Compliance を有効化すると、トラブルシューティング時に使用されるシステム機能への低レベル アクセスに多くの制限が適用されます。その制限が適用されると、システムを初期化してからリロードする（システムの上のすべてのデータが失われます）以外に、DD Retention Lock Compliance を無効化する方法はありません。

a. システムによる DD Retention Lock Compliance の使用を構成します。

```
system retention-lock compliance configure
```

システムが自動的に再起動されます。

b. 再起動プロセスが完了した後、システムで DD Retention Lock Compliance を有効化します。

```
system retention-lock compliance enable
```

5. レプリケーション コンテキストを作成します。

```
replication add source mtree:// [source-system-name] /data/col1/ [mtree-name] destination mtree:// [destination-system-name] /data/col1/ [mtree-name]
```

6. ソース システムでのみ次の手順を行います。
7. レプリケーション コンテキストを作成します。

```
replication add source mtree:// [source-system-name] /data/col1/ [mtree-name] destination mtree:// [destination-system-name] /data/col1/ [mtree-name]
```

8. レプリケーション コンテキストを初期化します。

```
replication initialize mtree:// [destination-system-name] /data/col1/ [mtree-name]
```

9. レプリケーションが完了していることを確認します。

```
replication status mtree://[destination-system-name] /data/col1/ [mtree-name] detailed
```

このコマンドは、レプリケーション終了時に残っている 0 圧縮前バイトをレポートします。

MTree のレプリケーション 1 対多トポロジー

ソース システムから複数のデスティネーション システムに DD Retention Lock Compliance が有効な MTree をレプリケーションします。

はじめに

MTree 上で DD Retention Lock コンプライアンスを有効化し、レプリケーションの前にクライアント側保存ロック ファイル制御を構成します。

手順

1. 別途指示がある場合を除き、デスティネーション システムでのみで次の手順を行います。
2. もしなければ、DD Retention Lock Compliance ライセンスをシステムに追加します。

a. まず、ライセンスがすでにインストール済みかどうかをチェックします。

```
license show
```

b. RETENTION-LOCK-COMPLIANCE 機能が表示されていない場合、ライセンスをインストールします。

```
license addlicense-key
```

注

ライセンス キーでは大文字と小文字が区別されません。キーを入力する際、ハイフンを含めます。

3. RBAC（役割に基づいたアクセス制御）ルールに従って、1 つ以上のセキュリティ担当者ユーザー アカウントをセットアップします。

a. システム管理者の役割で、セキュリティ担当者アカウントを追加します。

```
user adduserrole security
```

b. セキュリティ担当者許可を有効化します。

```
authorization policy set security-officer enabled
```

4. システムによる DD Retention Lock Compliance の使用を構成および有効化します。

注

DD Retention Lock Compliance を有効化すると、トラブルシューティング時に使用されるシステム機能への低レベル アクセスに多くの制限が適用されます。その制限が適用されると、システムを初期化してからリロードする（システムの上のすべてのデータが失われます）以外に、DD Retention Lock Compliance を無効化する方法はありません。

a. システムによる DD Retention Lock Compliance の使用を構成します。

```
system retention-lock compliance configure
```

システムが自動的に再起動されます。

b. 再起動プロセスが完了した後、システムで DD Retention Lock Compliance を有効化します。

```
system retention-lock compliance enable
```

5. レプリケーション コンテキストを作成します。

```
replication add source mtree:// [source-system-name] /data/
col1/ [mtree-name] destination mtree:// [destination-system-
name] /data/col1/ [mtree-name]
```

6. ソース システムでのみ次の手順を行います。
7. 各デスティネーション システム用のレプリケーション コンテキストを作成します。

```
replication add source mtree:// [source-system-name] /data/
col1/ [mtree-name] destination mtree:// [destination-system-
name] /data/col1/ [mtree-name]
```

8. 各デスティネーション システム MTree 用のレプリケーション コンテキストを初期化します。

```
replication initialize mtree:// [destination-system-name] /
data/col1/ [mtree-name]
```

9. 各デスティネーション システムのレプリケーションが完了していることを確認します。

`replication status mtree://[destination-system-name]/data/col1/[mtree-name] detailed`
このコマンドは、レプリケーション終了時に残っている 0 圧縮前バイトをレポートします。

既存の MTree レプリケーション ペアへの DD Retention Lock Compliance 保護の追加

保存ロックが有効化されていない既存の MTree レプリケーション ペアに DD Retention Lock Compliance 保護を追加します。

手順

1. 別途指示がある場合を除き、ソース システムとデスティネーション システム両方で次の手順を行います。
2. DD System Manager にログインします。

   ナビゲーション パネルの［DD System Manager］ウィンドウに［**DD Network**］と表示されます。
3. Data Domain システムを選択します。

   ナビゲーション パネルで、［**DD Network**］を展開し、システムを選択します。
4. ［Feature Licenses］に表示されていない場合は、DD Retention Lock Governance ライセンスを追加します。
   a. ［**Administration**］ > ［**Licenses**］を選択します。
   b. ［Licenses］領域で［**Add Licenses**］をクリックします。
   c. ［License Key］テキスト ボックスで、ライセンス キーを入力します。

   注

   ライセンス キーでは大文字と小文字が区別されません。キーを入力する際、ハイフンを含めます。

   d. ［**Add**］をクリックします。
5. レプリケーション ペアで現在の MTree コンテキストを破棄します。

   `replication break mtree://[destination-system-name]/data/col1/[mtree-name]`
6. 新しいレプリケーション コンテキストを作成します。

   `replication add source mtree://[source-system-name]/data/col1/[mtree-name] destination mtree://[destination-system-name]/data/col1/[mtree-name]`
7. ソース システムでのみ次の手順を行います。
8. 保存ロック用の MTree を選択します。

   ［**Data Management**］ > ［**MTree** ］タブをクリックした後、保存ロックに使用する MTree のチェックボックスをクリックします（空の MTree を作成して、後でそれにファイルを追加することもできます）。
9. 選択された MTree の情報を表示するには、［MTree Summary］タブをクリックします。
10. コンプライアンスが有効な MTree でファイルをロックします。

11. ソース MTree と宛先（レプリカ）MTree 両方が同じであることを確認します。

    ```
    replication resync mtree://[destination-system-name]/data/col1/[mtree-name]
    ```

12. 再同期の進行状況をチェックします。

    ```
    replication watch mtree://[destination-system-name] /data/col1/[mtree-name]
    ```

13. レプリケーションが完了していることを確認します。

    ```
    replication status mtree://[destination-system-name]/data/col1/[mtree-name] detailed
    ```
    このコマンドは、レプリケーション終了時に残っている 0 圧縮前バイトをレポートします。

コレクション レプリケーション ペアの MTree レプリケーション ペアへの変換

DD OS 5.2 の DD Retention Lock Compliance でコレクション レプリケーションを使用し、コレクション レプリケーション ペアのコンプライアンスが有効な MTree から MTree レプリケーション ペアに変換したいと考えている顧客向けの手順です。

手順

1. ソース システムのみ：

    a. DD Retention Lock Compliance が有効な各 MTree 用のスナップショットを作成します。

    ```
    snapshot create [snapshot-name]  /data/col1/[mtree-name]
    ```

    b. コレクション レプリケーション ペアを同期します。

    ```
    replication sync col://[destination-system-name]
    ```

    c. レプリケーションが完了していることを確認します。

    ```
    replication status col://[destination-system-name] detailed
    ```
    このコマンドは、レプリケーション終了時に残っている 0 圧縮前バイトをレポートします。

    d. DD Retention Lock Compliance が有効な各 MTree 用のスナップショット情報を表示します。

    ```
    snapshot list mtree /data/col1/[mtree-name]
    ```
    後で使用するスナップショット名に注意してください。

2. デスティネーション システムのみ：

    a. レプリケーションが完了していることを確認します。

    ```
    replication status mtree://[destination-system-name]/data/col1/[mtree-name] detailed
    ```
    このコマンドは、レプリケーション終了時に残っている 0 圧縮前バイトをレポートします。

    b. デスティネーション システムにレプリケーションされた各 MTree スナップショットを表示します。

    ```
    snapshot list mtree /data/col1/[mtree-name]
    ```

    c. ここで作成されたスナップショット名をソース システム上で生成されたものと比較して、すべての DD Retention Lock Compliance MTree スナップショットがレプリケーションされたことを確認します。

    ```
    snapshot list mtree /data/col1/[mtree-name]
    ```

3. ソース システムとデスティネーション システム両方：

   a. ファイル システムを無効化します。

   ```
   filesys disable
   ```

   b. コレクション レプリケーション コンテキストを破棄します。

   ```
   replication break col:// [destination-system-name]
   ```

   c. ファイル システムを有効にします。（セキュリティ担当者の許可が必要な場合があります）。

   ```
   filesys enable
   ```

   d. DD Retention Lock Compliance が有効な各 MTree 用のレプリケーション コンテキストを追加します。

   ```
   replication add source mtree:// [source-system-name] /
   data/col1/ [mtree-name] destination mtree:// [destination-
   system-name] /data/col1/ [mtree-name]
   ```

   注

   ソースおよびデスティネーション MTree 名は同じである必要があります。

4. ソース システムのみ：

   a. ソース MTree とデスティネーション MTree 両方が同じであることを確認します。

   ```
   replication resync mtree:// [destination-system-name]
   ```

   b. 再同期の進行状況をチェックします。

   ```
   replication watch [destination]
   ```

   c. レプリケーションが完了していることを確認します。

   ```
   replication status mtree:// [destination-system-name] /
   data/col1/ [mtree-name] detailed
   ```

   このコマンドは、レプリケーション終了時に残っている 0 圧縮前バイトをレポートします。

コレクション レプリケーションの実行

コンプライアンスが有効なソース システムからコンプライアンスが有効なデスティネーション システムに/data/col1 をレプリケーションします。

注

コレクション レプリケーションの場合、ソースおよびデスティネーション システム両方で同じセキュリティ担当者アカウントを使用する必要があります。

手順

1. 別途指示がある場合を除き、ソース システムでのみで次の手順を行います。
2. DD System Manager にログインします。

   ナビゲーション パネルの［DD System Manager］ウィンドウに［**DD Network**］と表示されます。

3. Data Domain システムを選択します。

   ナビゲーション パネルで、［**DD Network**］を展開し、システムを選択します。

4. ［Feature Licenses］に表示されていない場合は、DD Retention Lock Governance ライセンスを追加します。
   a. ［**Administration**］ > ［**Licenses**］を選択します。
   b. ［Licenses］領域で［**Add Licenses**］をクリックします。
   c. ［License Key］テキスト ボックスで、ライセンス キーを入力します。

      注

      ライセンス キーでは大文字と小文字が区別されません。キーを入力する際、ハイフンを含めます。

   d. ［**Add**］をクリックします。
5. レプリケーション コンテキストを作成します。

   ```
   replication add source col:// [source-system-name]
   destination col:// [destination-system-name]
   ```
6. 別途指示がある場合を除き、デスティネーション システムでのみで次の手順を行います。
7. ファイル システムを破棄します。

   ```
   filesys destroy
   ```
8. DD System Manager にログインします。

   ナビゲーション パネルの［DD System Manager］ウィンドウに［**DD Network**］と表示されます。
9. Data Domain システムを選択します。

   ナビゲーション パネルで、［**DD Network**］を展開し、システムを選択します。
10. ファイル システムを作成しますが、有効化はしません。

    ```
    filesys create
    ```
11. レプリケーション コンテキストを作成します。

    ```
    replication add source col:// [source-system-name]
    destination col:// [destination-system-name]
    ```
12. システムによる DD Retention Lock Compliance の使用を構成および有効化します。

    ```
    system retention-lock compliance configure
    ```

    （システムは、自動的に再起動し、コマンド `system retention-lock compliance enable` を実行します。）
13. ソース システムでのみ次の手順を行います。
14. レプリケーション コンテキストを初期化します。

    ```
    replication initialize source col:// [source-system-name]
    destination col:// [destination-system-name]
    ```
15. レプリケーションが完了していることを確認します。

    ```
    replication status col://[destination-system-name] detailed
    ```
    このコマンドは、レプリケーション終了時に残っている 0 圧縮前バイトをレポートします。

既存のコレクション レプリケーション ペアへの DD Retention Lock Compliance 保護の追加

ソースおよびデスティネーション システムで DD Retention Lock Compliance を有効化せずに作成されたコレクション レプリケーション ペアに DD Retention Lock Compliance 保護を追加します。

手順

1. 別途指示がある場合を除き、ソース システムとデスティネーション システム両方で次の手順を行います。
2. レプリケーションを無効化します。

   ```
   replication disable col:// [destination-system-name]
   ```

3. DD System Manager にログインします。

   ナビゲーション パネルの［DD System Manager］ウィンドウに［**DD Network**］と表示されます。

4. Data Domain システムを選択します。

   ナビゲーション パネルで、［**DD Network**］を展開し、システムを選択します。

5. 別途指示がある場合を除き、ソース システムで次の手順を行います。
6. システムによる DD Retention Lock Compliance の使用を構成および有効化します。

   ```
   system retention-lock compliance configure
   ```

   （システムは、`system retention-lock compliance enable` コマンドを実行して自動的に再起動します。）
7. レプリケーション コンテキストを有効化します。

   ```
   replication enable col:// [destination-system-name]
   ```

8. 別途指示がある場合を除き、デスティネーション システムで次の手順を行います。
9. システムによる DD Retention Lock Compliance の使用を構成および有効化します。

   ```
   system retention-lock compliance configure
   ```

   （システムは、`system retention-lock compliance enable` コマンドを実行して自動的に再起動します。）
10. レプリケーション コンテキストを有効化します。

    ```
    replication enable col:// [destination-system-name]
    ```

Fast Copy

`filesys fastcopy [retention-lock] source`**src**`destination`**dest** コマンドを DD Retention Lock Compliance が有効な MTree があるシステムで実行する場合、fastcopy の操作中はコマンドにより Retention Lock ファイル属性が維持されます。

注

デスティネーション MTree で保存ロックが有効でない場合、Retention Lock ファイル属性は維持されません。

CLI 使用量

DD Retention Lock Compliance を使用した Data Domain システムに関する考慮事項。

- コンプライアンスに違反するコマンドは実行できません。次のコマンドは禁止されています。
  - `filesys archive unit del [archive-unit]`
  - `filesys destroy`
  - `mtree delete [mtree-path]`
  - `mtree retention-lock reset {min-retention-period [period] | max-retention-period [period]} mtree [mtree-path]`
  - `mtree retention-lock disable mtree [mtree-path]`
  - `mtree retention-lock revert`
  - `user reset`
- 次のコマンドは、DD Retention Lock Compliance に対して削除中のライセンスが有効である場合は、セキュリティ担当者の許可が必要です。
  - `license del license-feature [[license-feature] ...] | license-code [[license-code] ...]`
- 次のコマンドは、DD Retention Lock Compliance が、コマンドで指定された MTree で有効になっている場合は、セキュリティ担当者の許可が必要です。
  - `mtree retention-lock set {min-retention-period [period] | max-retention-period [period]} mtree [mtree-path]`
  - `mtree rename [mtree-path new-mtree-path]`
- 次のコマンドは、DD Retention Lock Compliance が、システムで有効になっている場合は、セキュリティ担当者の許可が必要です。

  注

  これらのコマンドは、対話形式モードで実行する必要があります。

  - `alerts notify-list reset`
  - `config set timezone [zonename]`
  - `config reset timezone`
  - `cifs set authentication active-directory realm { [[dc1] [[dc2] ...]]`
  - `license reset`
  - `ntp add timeserver [time server list]`
  - `ntp del timeserver [time server list]`
  - `ntp disable`
  - `ntp enable`
  - `ntp reset`
  - `ntp reset timeservers`
  - `replication break {[destination] | all}`

- `replication disable {[destination] | all}`
- `system set date [MMDDhhmm] [[[CC]] [YY]]`

システム クロック

DD Retention Lock Compliance は、システム ロックの悪意のある改ざんを防止するため、内部セキュリティ クロックを実装しています。

セキュリティ クロックは、システム クロックを厳重に監視および記録します。セキュリティ クロックとシステム クロックの間に 1 年以内に累計で 2 週間のスキューがある場合、ファイル システムが無効化され、セキュリティ担当者のみ再開できます。

システム クロック スキューの検出

DD OS コマンド `system retention-lock compliance status`（セキュリティ担当者認証が必要です）を実行して、最後に記録されたセキュリティ クロック値を含むシステムおよびセキュリティ クロック情報および累計システム クロック誤差を取得できます。この値は、10 分ごとに更新されます。

システム クロック スキューの削除

クロック スキューは、セキュリティ ロックがシステム クロックの新しい値を記録するたびに更新されます。1 年後、0 にリセットされます。

いつでも、DD OS コマンド `system set date`MMDDhhmm[[CC]YY]を実行して、システム クロックの時間を設定できます（セキュリティ担当者の許可が必要です）。クロック スキューが現在の値（2 週間）よりも大きくなると、ファイル システムは無効化されます。次の手順に従って、ファイル システムを再起動し、セキュリティとシステム クロック間のスキューをなくします。

手順

1. システム コンソールで、ファイル システムを有効化します。

   ```
   filesys enable
   ```

2. プロンプトで、`filesys enable` コマンドを終了しようとしていることを確認し、システムの日付が正しいかどうかチェックします。
3. システムの日付を表示します。

   ```
   system show date
   ```

4. システムの日付が正しくない場合、正しい日付を設定し（セキュリティ担当者の許可が必要です）、それを確認します。

   ```
   system set date [MMDDhhmm] [[[CC]] [YY]]
   system show date
   ```

5. ファイル システムを再度有効化します。

   ```
   filesys enable
   ```

6. プロンプトで、有効化プロシージャを続けます。
7. セキュリティ担当者プロンプトが表示されます。セキュリティ担当者の許可を完了し、ファイル システムを開始します。セキュリティ ロックは、自動的に現在のシステムの日付に更新されます。

第 21 章

DD Encryption

本章には、次のセクションが含まれます。

- DD 暗号化の概要 576
- 暗号化の構成 577
- 鍵管理について 577
- キー マネージャーのセットアップ 589
- セットアップ後のキー マネージャーの変更 594
- 静止データの暗号化設定のチェック 596
- 静止データの暗号化の有効化と無効化 596
- ファイル システムのロックとロック解除 597

DD 暗号化の概要

データの暗号化を使用すると、Data Domain システムが盗まれたり、輸送中に物理ストレージ したドライブを交換した場合でも、過失によるデータ漏洩が起こりません。

データが対応しているプロトコル（NFS、CIFS、DD VTL、DD Boost、NDMP Tape Server）を使用して Data Domain システムを入力すると、そのストリームに対してセグメント化、フィンガープリント作成、重複排除（グローバル圧縮）が行われます。その後、ディスクに保存される前にマルチ セグメント圧縮領域へのグループ化、ローカル圧縮、暗号化が行われます。

格納データの暗号化機能を有効化すると、Data Domain システムに入ってくるすべてのデータが暗号化される。これよりも詳細なレベルで暗号化を有効化することはできません。

⚠ 注意

DD Encryption 機能を有効化する前に保存されたデータは、自動的には暗号化されません。システム上のすべてのデータを保護するため、必ず暗号化を構成するときに既存のデータを暗号化するオプションを有効化します。

追加の注意事項：
DD OS 5.5.1.0 では、1 個の保存ユニットのある DD Extended Retention が有効なシステムに対する格納データの暗号化に対応しています。5.5.1.0 では、DD Extended Retention は 1 個の保存ユニットしか対応していないため、5.5.1.0 以降にセットアップされたシステムにはこの制限への対応に関して問題はありません。ただし、5.5.1.0 以前にセットアップされたシステムには複数の保存ユニットがある場合がありますが、保存ユニットを 1 個残して削除するまで格納データの暗号化は使用しないか、データが 1 個の保存ユニットに移動または移行されています。

`filesys encryption apply-changes` コマンドは、次のクリーニング サイクルに暗号化構成の変更をファイル システムにあるすべてのデータに適用します。このコマンドの詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

静止データの暗号化は、オンライン サポート（http://support.emc.com）で閲覧可能な Backup Compatibility Guide に記載された、現在対応しているバックアップ アプリケーションのすべてに対応しています。

Data Domain Replicator は、暗号化オプションとともに使用でき、さまざまなトポロジーのコレクション、ディレクトリ、MTree、またはアプリケーション固有の管理されたファイル レプリケーションを使用した暗号化されたデータのレプリケーションを可能にします。レプリケーション形式はそれぞれ、暗号化に対して独自に対応し、同じレベルのセキュリティを実現します。詳細については、レプリケーションを併用した格納データの暗号化の使用に関するセクションを参照してください。

Data Domain Retention Lock を使用してロックされたファイルは、保存、暗号化、およびレプリケーションできます。

自動サポート機能には、次のような Data Domain システムでの暗号化の状態についての情報が含まれます。

- 暗号化が有効かどうか
- 有効な Key Manager と使用されるキー
- 構成されている暗号化アルゴリズム
- ファイル システムの状態

暗号化の構成

この手順には、キー マネージャの構成が含まれます。

［**Data Management**］ > ［**File System**］ > ［**Encryption**］タブの［Encryption Status］に［Not Configured］と表示されている場合、［**Configure**］をクリックして、Data Domain システムで暗号化をセットアップします。

注

システム パスフレーズは暗号化を有効にするために設定する必要があります。

次の情報を入力します。

- アルゴリズム
  - ドロップダウン リストから暗号化アルゴリズムを選択するか、デフォルト AES 256-bit（CBC）を許可します。
    AES 256-bit Galois/Counter Mode（GCM）は最も安全なアルゴリズムですが、CBC（Cipher Block Chaining）モードよりも速度はかなり低いです。
  - 暗号化するデータ（既存データと新規データの両方、または新規データのみ）を確認します。ファイル システムの再起動後、最初のクリーニング サイクルで既存のデータが暗号化される。既存のデータの暗号化には、標準ファイル システム クリーニング操作よりも長くかかる可能性があります。
- Key Manager（3 つのうちいずれかを選択します）。
  - Embedded Key Manager
    デフォルトでは、RSA DPM Key Manager を構成しない限り、ファイル システムを再起動した後、Data Domain Embedded Key Manager が有効になります。

    キー ローテーションを有効化または無効化できます。有効化された場合、1～12 か月のローテーション インターバルを入力します。
  - RSA DPM Key Manager
  - SafeNet KeySecure Key Manager

  注

  Embedded Key Manager、RSA DPM Key Manager、SafeNet KeySecure Key Manager の動作例については、鍵管理に関するセクションを参照してください。

［Summary］には、選択された設定可能な値が表示されます。それが正しい値かどうかを検討します。値を変更するには、［**Back**］をクリックして、その値が入力されたページに移動し、それを変更します。

暗号化を有効化するには、システムを再起動する必要があります。新しい構成を適用するには、ファイル システムを再起動するオプションを選択します。

注

ファイル システムの再起動中、アプリケーションが中断される可能性があります。

鍵管理について

暗号化キーによって、暗号化アルゴリズムの出力が決定されます。暗号化キーはパスフレーズによりさらに保護されます。パスフレーズは、ディスクの複数の場所に暗号化キーを保存する前に、暗号化

キーを暗号化する際に使用します。パスフレーズはユーザーが生成します。パスフレーズの変更には管理者およびセキュリティ担当者の両方が必要です。

キー マネージャは、複数の暗号化キーの生成、配布、ライフサイクル管理を行います。Data Domain システムは、Embedded Key Manager または RSA DPM（Data Protection Manager）または SafeNet KeySecure Key Manager のいずれかを使用できます。KMIP（Key Management Interoperability Protocol）が DD OS 6.1 からサポートされています。

一度に 1 つのみ有効化できます。暗号化が Data Domain システムで有効化されると、Embedded Key Manager がデフォルトに有効になります。RSA DPM または SafeNet KeySecure Key Manager を構成した場合、それが Embedded Key Manager に取って代わり、無効化されると Embedded Key Manager に戻ります。新しいキー マネージャを動作させるには、ファイル システムの再起動が必要です。

システムは Data Domain システムに入力されたデータの暗号化に一度に 1 つのキーしか使用しませんが、埋め込みと DPM 両方のキー マネージャが複数のキーを提供します。外部のキー マネージャが構成済みで、有効化されている場合、Data Domain システムは、RSA DPM キー マネージャ サーバから提供されるキーを使用します。同じ DPM キー マネージャが複数の Data Domain システムを管理する場合、各システムが同期済みで、Data Domain ファイル システムが再起動されると、すべてのシステムが同じアクティブ キー（同じキー クラスを使用している場合）を持ちます。Embedded Key Manager は、内部でキーを生成します。

両方のキー マネージャは、キーをローテーションし、最大 254 個のキーに対応します。Embedded Key Manager によって、（ファイル システム再起動後）キーが交換されるまで何か月有効になるかを指定できます。RSA DPM Key Manager は、キー クラスに応じて定期的にキーをローテーションします。Embedded Key Manager キー ローテーションは、Data Domain システムで管理されます。Key Manager キー ローテーションは、外部の Key Manager サーバーで管理されます。

KeySecure

KeySecure 8.5 および 8.9 がサポートされています。これは Safenet Inc/Gemalto KeySecure の、KMIP 準拠のキー マネージャ製品です。KMIP キー マネージャを使用するには、キー マネージャと Data Domain システム/DD VE の両方を設定して、お互いを信頼するようにする必要があります。ユーザーはキー マネージャのキーを事前に作成する必要があります。データ ドメイン システムは、セキュリティで保護された TLS 接続が確立された後で、これらのキーとその状態を KeySecure から取得します。キーの作成、および Data Domain システムでキーを使用する方法の詳細については、「Data Domain オペレーティング システムと Gemalto KeySecure 統合ガイド」を参照してください。

紛失または破損したキーの修正

システムの現在の暗号化キーをすべて含むファイルを作成します。万が一キーを紛失または破損した場合、サポート プロバイダーは、このファイルを使用してそのキーをシステムにインポートし直せます。定期的にエクスポート ファイルを作成することを推奨します。

キーをエクスポートするため、セキュリティ担当者の認証情報を入力するように求められます。追加キー ファイル保護を適用するには、Data Domain システムで使用されるものとは異なるパスフレーズを使用します。エクスポートの後、許可されたユーザーのみアクセスできるセキュア ファイル サーバーでキー ファイルを保存することを推奨します。キー ファイルに使用されるパスフレーズはメモしておいてください。パスフレーズを紛失または失念した場合、Data Domain システムはキーのインポートとリストアを行えません。次のコマンドを実行します。

```
# filesys encryption keys export
```

キー マネージャー サポート

すべての Key Manager がすべての DD OS ファイル システム プロトコルに対応しています。

レプリケーション
ディレクトリ MTree レプリケーション用の Data Domain システムを構成する場合、各 Data Domain システムを個別に構成します。2 つのシステムは、同じまたは異なるキー クラスおよび同じまたは異なるキー マネージャーを使用できます。

コレクション レプリケーション構成の場合、Data Domain システムはソースで構成する必要があります。レプリケーション破棄後、元のレプリカ Data Domain システムを Key Manager 用に構成する必要があります。構成されなかった場合、Data Domain システムは直近の既知のキーを使用し続けます。

RSA DPM Key Manager の処理

RSA DPM キー マネージャーが構成済みで、有効化されている場合、Data Domain システムは、RSA DPM キー マネージャー・サーバーから提供されるキーを使用します。同じ DPM キー マネージャが複数の Data Domain システムを管理する場合、各システムが同期済みで、Data Domain ファイル システムが再起動されると、すべてのシステムが同じアクティブ キー（同じキー クラスを使用している場合）を持つことになります。キー ローテーションは、RSA DPM Key Manager サーバーで管理されます。

RSA DPM キー マネージャーが構成済みで、有効化されている場合、Data Domain システムは、RSA DPM キー マネージャー・サーバーから提供されるキーを使用します。同じ DPM キー マネージャが複数の Data Domain システムを管理する場合、各システムが同期済みで、Data Domain ファイル システムが再起動されると、すべてのシステムが同じアクティブ キー（同じキー クラスを使用している場合）を持つことになります。キー ローテーションは、RSA DPM Key Manager サーバーで管理されます。

Encryption Key States
1 個の Activated-RW キーが常に有効です。アクティブ キーが漏洩すると、RSA DPM Key Manager は新しいキーを与えます。Data Domain システムが新しいキーを検出すると、管理者のアラートを発行して、ファイル システムを再起動します。

期限切れのキーは、Data Domain システム上の既存のデータに対して読み取り専用となり、新しいアクティブ キーは取り込まれるすべての新しいデータに適用されます。キーが漏洩すると、既存のデータはファイル システム クリーニング実行後に新しい暗号化キーを使用して再暗号化されます。キーの最大数に達すると、新しいキー用のスペースを確保するため、未使用のキーを削除する必要があります。

Data Domain システムにある暗号化キーについての情報を表示するには、DD System Manager を開き、［**Data Management**］ > ［**File System**］ > ［**Encryption**］タブを開きます。キーは、［Encryption］タブの［**Encryption Keys**］セクションに ID 番号ごとにリストされます。キーごとに、キーが作成された日時、それが有効な期間、タイプ（RSA DPM または Data Domain）、状態（「Data Domain が対応する DPM 暗号化キー状態」を参照してください）、圧縮後のサイズが表示されます。システムに Extended Retention のライセンスがある場合、次のフィールドも表示されます。

Active Size (post comp)
キーで暗号化されたアクティブ階層上の物理スペースの量。

Retention Size (post comp)
キーで暗号化された保存階層上の物理スペースの量。

Key MUID をクリックすると、システムが［Key Details］ダイアログに次に示すキーの情報を表示します。階層/ユニット（Active、Retention-unit-2 など）、作成日、有効期限、状態（「Data Domain が対応する DPM 暗号化キー状態」を参照してください）、圧縮後のサイズが表示されます。［Close］をクリックしてダイアログを閉じます。

表 200 Data Domain がサポートする DPM 暗号化キー状態

状態	定義
Pending-Activated	キーは作成されたばかりです。ファイル システム再起動後、キーは Activated-RW になります。
Activated-RW および Activated-RO	Activated-RW と Activated-RO は両方、それぞれのキーで暗号化されたデータを読み込みます。Activated-RW は、最後にアクティブ化されたキーです。
De-Activated	現在の時間が有効期間を超えると、キーが無効になります。キーは読み取りに使用されます。
Compromised	キーは復号化のみ可能です。漏洩したキーで暗号化されたすべてのデータが暗号化された後、状態が Destroyed Compromised に変わります。ファイル システム クリーニングが実行されると、キーは再暗号化されます。必要に応じて、Destroyed Compromised キーを削除できます。
Marked-For-Destroy	データを再暗号化するために破棄するキーがマークされています。
Destroyed	このキーで暗号化されたすべてのデータを再暗号化した後、DD OS はそれを Marked-For-Destroy から Destroyed に変更します。また、破棄されたキーが漏洩すると、それは Compromised-Destroyed になります。Destroyed のキーと Compromised-Destroyed のキーは削除できます。 注 クリーニング操作が実行され、完了するまで、Data Domain システムでキーは破棄されません。

RSA DPM Key Manager と同期したキーの管理

自動キー同期は、毎日深夜に実行されます。手動キー同期は、スケジュール設定された同期を待てない場合にのみ必要です。新しいキーが Data Domain システム上で同期されると、アラートが出されます。このアラートは、ファイル システムの再起動後にクリアされます。

RSA DPM Key Manager Server が新しいキーを作成したら、［**Sync**］ボタンをクリックして、［Data Domain System Manager's Encryption］タブの［Encryption Key］リストにそのキーを表示します。

注

最後の同期以降にキーが変更された場合、ファイル システム再起動が必要になります。

手順

1. DD System Manager を使用して、ナビゲーション パネルで使用する Data Domain システムを選択します。

注

ナビゲーション パネルで選択したシステムでは、必ず DD System Manager 機能を実行します。

2. ［**Data Management**］ > ［**File System**］ > ［**Encryption**］を選択します。
3. ［Encryption Keys］セクションで、［**RSA DPM**］キーを選択し、［**Sync**］をクリックします。

キーの破棄（RSA DPM key manager）

データの暗号化に使用したくないキーを破棄します。この手順にはセキュリティ担当者の認証情報が必要です。

注

セキュリティ担当者の詳細については、ローカル ユーザーの作成とセキュリティ許可に関するセクションを参照してください。

RSA DPM キーを破棄できる状態に変更する手順：

手順

1. RSA DPM Server でキーを非アクティブ化します。
2. Data Domain システムで非アクティブ化されるキーのファイル システムを再起動します。
3. DD System Manager を使用して、［**Data Management**］ > ［**File System**］ > ［**Encryption**］を選択します。
4. ［Encryption Keys］セクションで、リストで破棄するキーを選択します。
5. ［**Destroy...**］をクリックします。

   システムは、キーの階層と状態が含まれる［Destroy］ダイアログを表示します。
6. セキュリティ担当者のユーザー名とパスワードを入力します。
7. ［**Destroy**］をクリックしてキーを破棄する意思があることを確認します。

   注

   ファイル システム クリーニング実行後、キーの状態が Destroyed に変わります。

キーの削除

Destroyed または Compromised-Destroyed 状態の Key Manager キーは削除できます。ただし、キーの数が 254 個の上限に達した場合のみ、キーを削除する必要があります。この手順にはセキュリティ担当者の認証情報が必要です。

注

Destroyed 状態にするには、Destroying a Key 手順（Embedded Key Manager または RSA DPM Key Manager）をそのキーに実行し、システム クリーニングを実行する必要があります。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Encryption**］を選択します。
2. ［Encryption Keys］セクションで、リストから削除するキー（複数も可）を選択します。

3. ［**Delete...**］をクリックします。

   システムは、削除するキーおよびそのキーの階層と状態を表示します。

4. セキュリティ担当者のユーザー名とパスワードを入力します。
5. ［**Delete**］をクリックして、キーを削除する意思があることを確認します。

Embedded Key Manager の扱い

Embedded Key Manager を選択すると、Data Domain System は独自のキーを作成します。

キー ローテーション ポリシーが構成されている場合、新しいキーが自動的に次のローテーションで作成されます。新しいキーが生成されると、アラートが出されます。新しいキーをアクティブ化し、古いキーを非アクティブ化するには、ファイル システムを再起動する必要があります。Embedded Key Manager Key のローテーション状態に関連づけられた無効化ボタンをクリックして、キー ローテーション ポリシーを無効化できます。

キーの作成（Embedded Key Manager）

Embedded Key Manager の暗号化キーを作成します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**DD Encryption**］を選択します。
2. ［Encryption Keys］セクションで、［**Create...**］をクリックします。
3. セキュリティ担当者のユーザー名とパスワードを入力します。
4. ファイル システムを再起動する場合、［**Restart the filesystem now**］をクリックします。

   新しい Data Domain キーが作成されます。ファイル システムの再起動後、以前のキーは非アクティブ化され、新しいキーがアクティブ化されます。

5. ［**Create**］をクリックします。

キーの破棄（Embedded Key Manager）

Embedded Key Manager の暗号化キーを破棄します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Encryption**］を選択します。
2. ［Encryption Keys］セクションで、リストで破棄するキーを選択します。
3. ［**Destroy...**］をクリックします。

   システムは、キーの階層と状態が含まれる［Destroy］ダイアログを表示します。

4. セキュリティ担当者のユーザー名とパスワードを入力します。
5. ［**Destroy**］をクリックしてキーを破棄する意思があることを確認します。

   注

   ファイル システム クリーニング実行後、キーの状態が Destroyed に変わります。

KeySecure Key Manager での作業

KeySecure Key Manager では、KMIP（Key Management Interoperability Protocol）による外部キー マネージャをサポートし、単一の一元化されたプラットフォームで暗号化キーを一元管理します。

- キーは Key Manager で事前に作成されます。
- 暗号化が有効になった 1 つ以上のクラウド ユニットがシステムに存在する場合、KMIP Key Manager を有効にできません。

DD System Manager による KeySecure Key Manager のセット アップと管理

このセクションでは、DD SM（Data Domain System Manager）を使用して KeySecure Key Manager を管理する方法について説明します。

KeySecure Key Manager のキーの作成

KMIP（KeySecure Key Manager）の暗号化キーを作成します。

手順

1. ［**Key Manager Encryption Keys**］表が表示されるまで下にスクロールします。
2. ［**Add**］をクリックして新しい Key Manager の暗号化キーを作成します。
   a. セキュリティ担当者のユーザー名とパスワードを入力します。
   b. ［**Restart the file system now**］をクリックします。
   c. ［**Create**］をクリックします。
3. ［**Restart the file system now**］をクリックして変更を有効にします。

   新しい KIMP キーが作成されます。ファイル システムの再起動後に以前のキーが非アクティブになり、新しいキーがアクティブ化されます。

KeySecure Key Manager の既存キーの状態の変更

DD SM を使用して、既存の KMIP 暗号化キーの状態を変更します。

はじめに

キーの状態を変更するための条件を確認します。

- キーがすでに存在する（アクティブな）状態で新しいキーが作成されると、ユーザーがファイル システムを再起動するまで新しいキーが `Pending-Activated` 状態に変わります。
- ユーザーは、代わりになる `Pending-Activated` キーがある場合にのみ `Activated-RW` 状態のキーを非アクティブ化できます。
- `Pending-Activated` 状態のキーは、代わりになる別の `Pending-Activated` キーがある場合にのみ非アクティブ化されます。
- `Activated-RO` キーのキーは必要な条件がないため、いつでも非アクティブ化できます。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**DD Encryption**］を選択します。
2. 下にスクロールして［**Key Manager Encryption Keys**］表を表示させます。
3. ［**Key Manager Encryption Keys**］表から適切なキーを選択します。
4. キーを非アクティブ化します。
   a. `Activated` 状態の任意のキーをクリックします。
   b. セキュリティ担当者のユーザー名とパスワードを入力します。
   c. ［**DEACTIVATE**］をクリックします。

   図 25 KMIP キーを非アクティブ化状態に変更

5. ［**Restart the filesystem now**］をクリックします。

結果

既存キーの状態が変更されます。

KeySecure Key Manager の設定

DD SM を使用して、Data Domain システムからキー ローテーション ポリシーを設定します。

はじめに

望ましいキー ローテーションの期間（週または月単位）、キー ローテーションの開始日、次のキー ローテーションの日を確認します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**DD Encryption**］を選択します。
2. ［**Key Management**］セクションの［**Configure**］をクリックします。［**Change Key Manager**］ダイアログ ボックスが開きます。
3. セキュリティ担当者のユーザー名とパスワードを入力します。
4. ［**Key Manager Type**］ドロップダウン メニューの［**KeySecure Key Manager**］を選択します。［Change Key Manager］情報が表示されます。
5. キー ローテーション ポリシーを設定します。

   注

   ローテーション ポリシーは、数週間および数か月単位で指定されます。キー ローテーション ポリシーの最小増分は 1 週間、最大増分は 52 週間（12 か月）です。

   a. キー ローテーション ポリシーを有効にします。［**Enable Key rotation policy**］ボタンを設定して有効にします。
   b. キー ローテーション スケジュール フィールドに適切な日付を入力します。
   c. ［**Weeks**］または［**Months**］ドロップダウン メニューから適切な週数か月数を選択します。
   d. ［**OK**］をクリックします。
   e. ファイル システムを再起動してすぐに変更を有効にしたい場合は、［**Restart the filesystem now**］をクリックします（図 3 を参照）。

結果

キー ローテーション ポリシーが設定または変更されます。

Data Domain CLI による KeySecure Key Manager の管理

このセクションでは、CLI を使用して KeySecure Key Manager を管理する方法について説明します。

KeySecure Key Manager での新しいアクティブ キーの作成

Data Domain CLI を使用して新しいアクティブ キーを作成します。

はじめに

適切なユーザー資格情報を持っていることを確認します。これらのコマンドを実行するには、セキュリティ ロールが必要です。

手順

1. セキュリティ ロールを使用して Data Domain システムにログインします。

   ユーザー名：`<security office user>`

   パスワード：`<security officer password>`

2. 新しいアクティブ キーを作成します。

```
# filesys encryption key-manager keys create
```

3. 次のようなメッセージが表示されます。

```
New encryption key was successfully created.
The filesystem must be restarted to activate the new key.
```

結果

新しいアクティブ キーが作成されます。

KeySecure Key Manager の既存キーの状態の変更

Data Domain CLI を使用して既存キーの状態を非アクティブ化状態に変更します。

はじめに

適切なユーザー資格情報を持っていることを確認します。これらのコマンドを実行するには、セキュリティ ロールが必要です。

手順

1. セキュリティ ロールを使用して Data Domain システムにログインします。

   ユーザー名：`<security officer user>`

   パスワード：`<security officer password>`

2. 既存キーの状態を変更します。

   ```
   # filesys encryption key-manager keys modify{<key-id> | muid
   <key-muid>}state deactivated
   ```

   次に例を挙げます。

   ```
   # filesys encryption key-manager keys modify muid
   740D711374A8C964A62817B4AD193C8DC44374A6ED534C85642782014F2E9D
   41 state deactivated
   ```

3. 次のようなメッセージが表示されます。

   ```
   Key state modified.
   ```

結果

既存キーの状態が変更されます。

KeySecure Key Manager でのキー ローテーション ポリシーの設定または再設定

Data Domain CLI を使用して、Data Domain システムで定期的にキーをローテーションするためのキー ローテーション ポリシーを設定します。数週間および数か月単位でローテーション ポリシーが指定されることに注意してください。キー ローテーション ポリシーの最小増分は 1 週間、最大増分は 52 週間（12 か月）です。

はじめに

適切なユーザー資格情報を持っていることを確認します。これらのコマンドを実行するには、セキュリティ ロールが必要です。

手順

1. セキュリティ ロールを使用して Data Domain システムにログインします。

   ユーザー名：`sec`

   パスワード：`<security officer password>`

2. 初めてのキー ローテーション ポリシーを設定します。この例では、ローテーション ポリシーを［**3** 週間］に設定します。

```
# filesys encryption key-manager set key-rotation-policy
                  {every <n> {weeks | months} | none}
```

例：

```
# filesys encryption key-manager set key-rotation-policy
every 3 weeks
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 3 weeks.
```

3. その後、既存のキー ローテーション ポリシーの変更を選択する場合は、このコマンドを実行します。この例では、ローテーション ポリシーを［**3** 週間］から［**4** か月］に変更します。

注

セキュリティ ロールを使用して Data Domain システムにログインします（ユーザー名は sec、パスワードは<security officer password>）。

```
# filesys encryption key-manager reset [key-rotation-policy]
```

たとえば、次のように表示されます。

```
filesys encryption key-manager set key-rotation-policy every
4 months
```

Output that is similar to the following appears:

```
Key-rotation-policy is set. Encryption key will be rotated
every 4 months.
```

4. 現在のキー ローテーション ポリシーを表示するか、ポリシーが正しく設定されていることを確認します。

```
# filesys encryption key-manager show
```

Output that is similar to the following appears:

```
The current key-manager configuration is:
Key Manager:                                Enabled
Server Type:                                KeySecure
Server:                                     <IP address of
KMIP server>
Port:                                       5696
Fips-mode:                                  enabled
Status:                                     Online
Key-class:                                  <key-class>
KMIP-user:                                  <KMIP username>
Key rotation period:                        2 months
Last key rotation date:                     03:14:17 03/19
2018
Next key rotation date:                     01:01:00 05/17
2018
```

結果

キー ローテーション ポリシーが設定または変更されます。

クリーニング操作の機能

暗号化は、Compromised または Marked-For-Destroyed キーで暗号化されたデータは Activated-RW キーを使用して再暗号化されたときのクリーニング操作のパフォーマンスに影響します。

クリーニング操作の終了時に、Compromised または Marked-For-Destroyed キーで暗号化されたデータはありません。また、クリーニング操作によって書き込まれるデータは Activated-RW キーで暗号化されます。

キー マネージャーのセットアップ

使用しているキー マネージャーのタイプについての指示に従います。

SafeNet KeySecure Key Manager のセットアップの詳細については、「Data Domain Operating System および Gemalto KeySecure 統合ガイド」を参照してください。

RSA DPM Key Manager の暗号化のセットアップ

RSA DPM Key Manager は、RSA DPM サーバーと Data Domain システム両方でセットアップする必要があります。

RSA DPM Server でのこのセットアップの実行

（グラフィカル ユーザー インターフェイスを使用して） RSA DPM Server をセットアップする主な手順です。

注

この手順の各ステップの詳細については、「RSA Data Protection Manager Server Administrator's Guide」の最新版を参照してください。

RSA DPM Key Manager Server で設定されたアルゴリズムおよび暗号モードは、Data Domain システムでは無視されます。Data Domain システムで、これらの設定を構成します。

手順

1. X509 証明書を使用して、Data Domain システムの ID を作成します。この証明書をベースに、安全なチャネルが作成されます。
2. 適切な属性を持つキー クラスを作成します。
   - キーの長さ： 256 ビット。
   - Duration： 6 か月、ポリシーに一致する期間など。
   - 自動キー生成： 選択すると、キーが自動的に生成されるようになります。

   注

   Multiple Data Domain システムは、同じキー クラスを共有できます。キー クラスの詳細については、RSA DPM キー クラスに関するセクションを参照してください。
3. Data Domain システムのホスト証明書を ID 証明書として使用して、ID を作成します。ID とキー クラスは、同じ ID グループに含まれている必要があります。
4. 証明書をインポートします。詳細については、証明書のインポートに関するセクションを参照してください。

RSA DPM Key クラスについて

Data Domain システムは、キー クラスごとに RSA DPM Key Manager からキーを取得します。キー クラスは、同様の特徴を持つ暗号キーをグループ化する RSA DPM Key Manager によって使用されるセキュリティ クラスの専用タイプです。

RSA DPM Key Manager Server によって、キー クラスが現在のキーに戻るか、新しいキーを毎回生成するかをセットアップできます。Data Domain システムは、現在のキーを返すように構成されたキー クラスにのみ対応しています。新しいキーを毎回生成するように構成されたキー クラスは使用できません。

注

キーの長さが 256 ビットではない場合、DPM 構成が失敗します。

証明書のインポート

証明書を取得した後、それを Data Domain システムにインポートします。

はじめに

- Host 証明書は、PKCS12 形式である必要があります。
- CA 証明書は、PEM 形式である必要があります。
- RSA DPM Key Manager と互換性のある CA および Host 証明書を取得する必要があります。それらの証明書は第三者証明機関に依頼するか、適切な SSL ユーティリティ ツールを使用して作成できます。
- システム パスフレーズが設定されていない場合、ホスト証明書をインポートできません。暗号化を有効化すると、パスフレーズが設定されます。それを変更する場合、「Data Domain システムの管理」の章のシステム パスフレーズに関するセクションを参照してください。

DD OS は、Data DD Manager と RSA DPM Key Manager 両方について、一切拡張のない証明書およびサーバーとクライアントの拡張のない証明書に対応しています。クライアントの拡張のある証明書に対応しているのは RSA DPM Key Manager のみであり、サーバーの拡張のある証明書に対応しているのは DD System Manager のみです。

DD OS は、自動登録された証明書の直接アップロードや複数の証明書のインポートを行う RSA DPM Key Manager Server の Auto Registration Certificate 機能には対応していません。そのため、Data Domain システムの CA および Host 証明書をインポートする必要があります。

次に、証明書の管理中に発生することがあるいくつかのアラートへの対応方法を示します。

- インポートされた証明書の破損によって HTTPS が再起動に失敗した場合、自己署名証明書が使用されます。この状態になると、管理されているアラート（UnusableHostCertificate）が発行されます。アラートをクリアするには、破損した証明書を削除し、新しい証明書を再インポートします。
- システム ヘッドスワップ時などにインポートされた証明書が削除され、インポートされた証明書のコピーが失敗した場合、管理されているアラート（MissingHostCertificate）が発行されます。証明書を再インポートして、アラートをクリアします。

証明書を取得した後、次のようにそれを Data Domain システムにインポートします。

手順

1. RSA DPM Key Manager Server で CA および Host 証明書が使用されるよう構成します。操作手順については、「RSA DPM Key Manager Server 管理ガイド」を参照してください。
2. `ssh` コマンド構文で証明書ファイルをリダイレクトして、証明書をインポートします。詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

   ssh sysadmin@<Data-Domain-system> adminaccess certificate import {host password password **|ca } <** path_to_the_certificate
   たとえば、`ssh` を使用して、自分のパーソナル コンピューターのデスクトップからホスト証明書 host.p12 を Data Domain システム DD1 にインポートする場合、次のコマンドを入力します。

   # ssh sysadmin@DD1 adminaccess certificate import host password abc123 < C:\host.p12

3. 次のコマンドを入力して、デスクトップから DD1 に、SSH 経由で CA 証明書（ca.pem など）をインポートします。

   # `ssh sysadmin@DD1`**adminaccess certificate import ca < C:\ca.pem**

Data Domain システムでのこのセットアップの実行

DPM Key Manager を使用して、Data Domain System Manager で暗号化を構成します。

手順

1. RSA DPM Server で DPM Key Manager セットアップを完了します。
2. Data Domain システムは、そのホスト名を使用してその IP アドレスを解決する必要があります。このマッピングが DNS サーバーに追加されていない場合、このコマンド ラインを使用してエントリーを`/etc/hosts` ファイルに追加します。

   # `net hosts add`ipaddrhost-list
   ipaddr は Data Domain システムの IP アドレスで、host-list は Data Domain システのホスト名です。

   デュアル スタック環境で作業している場合、次のエラー メッセージが表示されます：「RKM is not configured correctly」。`net hosts add`ipaddrhost-list コマンドを使用して、Data Domain System の IPv4 アドレスを/etc/hosts ファイルに追加します。

注

IPv6 アドレスのみを使用する環境では、DPM サーバーは有効化できません。

注

デフォルトでは、FIPS モードは有効になっています。PKCS #12 クライアント認証情報が FIPS 140-2 承認アルゴリズム（RC2 など）で暗号化されていない場合、FIPS モードを無効化する必要があります。FIPS モードの無効化の詳細については、「Data Domain オペレーティング システム コマンド リファレンス ガイド」を参照してください。

3. DD System Manager をログインし、ナビゲーション パネルで使用する Data Domain システムを選択します。

注

ナビゲーション パネルで選択したシステムでは、必ず DD System Manager 機能を実行します。

4. ［**Data Management**］ > ［**File System**］ > ［**Encryption**］タブをクリックします。
5. 暗号化の構成に関するセクションの手順に従い、［**DPM Key Manager**］を選択します。暗号化がすでにセットアップされている場合、セットアップ後のキー マネージャの変更に関するセクションの手順に従います。

KMIP キー マネージャの設定

KMIP サポートにより、KMIP キー マネージャの静止データ暗号化に使用する対称キー オブジェクトを、Data Domain アプライアンスが取得できるようになりました。

手順

1. IP アドレスが<IP1>の KeySecure インスタンスを設定します。
2. KeySecure で SSL サーバ証明書の作成とインストールを実行します。
3. ［**Device**］ > ［**Key Server**］に移動して KMIP を有効にします。

   使用している IP アドレスが<IP1>、ポートが<Port1>であり、かつステップ 2 のサーバ証明書が使われていることを確認します。
4. Data Domain システム/DD VE または Linux コンピューターのシステムで使用する CSR（証明書署名要求）を作成します。
   a. Data Domain システムにログインします。
   b. コマンド `adminaccess certificate cert-signing-request generate` を実行します。

      コマンドが成功すると、ファイル `CertificateSigningRequest.csr` が `/ddvar/certificates/` に生成されます。

デフォルトでは、NFS エクスポートは証明書フォルダへのアクセス権限を持ちません。これは root ユーザーも同様です。

```
# mount 16tbddve:/ddvar /mnt/DDVE
# cd /mnt/DDVE/certificates/
bash: cd: /mnt/DDVE/certificates/: Permission denied
# ls -al /mnt/DDVE/
total 800292
```

```
drwxr-xr-x 25 root staff      4096 Apr 10 08:32 .
drwxr-xr-x 26 root root       4096 Oct 24 12:11 ..
-rwxr-xr-x  1 root staff       180 Apr 10 08:36 .bashrc
drwxrwsr-x  2 root staff      4096 Aug 18  2016 benchmark
drwxr-sr-x  3 root staff      4096 Apr  4 15:49 cacerts
drwxrwsr-x  2 root staff      4096 Apr  4 12:50 cdes
drwxrws---  2 root staff      4096 Apr 11  2017 certificates
drwxrwsr-x  3 root staff      4096 Jul  1  2016 core
```

5. この CSR を取得し、KeySecure の CA で発行/署名する必要があります。

   コマンドが成功すると、ファイル `CertificateSigningRequest.csr` が`/ddvar/certificates/`に生成されます。

6. 署名済み証明書（x.509 pem ファイル）を Data Domain システムにダウンロードして、CSR のプライベート キーを用いて pkcs #12 ファイルを作成します。

   ファイル名の `csr` を `pem` に変更します。

7. KeySecure の CA から root CA 証明書をダウンロードします（［**Security**］ > ［**Local CAs**］）。

8. Data Domain システム/DD VE では、`adminaccess`CLI で pkcs #12 クライアント証明書と CA 証明書をインストールします。アプリケーションの種類には［**keysecure**］を使用します。

9. KeySecure では、アルゴリズムとキーの長さを AES-256 にして対称キーを作成します。

   a. Data Domain システム/DD VE 上で KMIP として使用するユーザーを所有者に設定します。

   b. `Exportable` オプションを選択します。

   c. キーに関するオプションは［**Security**］ > ［**Keys**］ > ［**Attributes**］にあります。［**Application Namespace**］に［**DD_DARE_KEYS**］と設定します。設定することを確認［**Application Data**］に Data Domain システム/DD VE で使用する予定の key-class を設定します。

10. コマンド `filesys encryption key-manager set` を使用して keysecure キー マネージャにアクセスするすべてのパラメーターを設定します。

11. コマンド `filesys encryption key-manager enable` を使用して外部キー マネージャを有効にします。

12. コマンド `filesys encryption enable` と `filesys restart` を使用して暗号化を有効にします。

    この操作を行うとファイル システムは再起動します。

13. ローカル キー テーブルに表示される keysecure キー マネージャからキーを自動的に取得する必要があります。

    `filesys encryption keys show` のローカル キー テーブルの出力サンプルは次のようになります。

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                          post-comp

---   ---------------------------------------------------------------  -------------  ---------

0.1   e56                                                              Deactivated       0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Activated-RW      0
---   ---------------------------------------------------------------  -------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:02:02 2017.
```

    カレント アクティブ キーは取得したすべてのデータの暗号化に使用されます。

14. キーの状態を同期します。
    a. keysecure Web インターフェイスで、前述したように、新しいアクティブ キーを作成します。
    b. keysecure Web インターフェイスでは、キーをクリックして［**Life Cycle**］タブへ移動すると古いキーを無効化できます。［**Edit State**］をクリックします。［**Cryptographic State**］に［**Deactivated**］を設定します。［**Save**］をクリックします。
15. Data Domain システム上で、コマンド `filesys encryption keys sync` を実行してローカル キー テーブルを同期します。

    `filesys encryption keys show` のローカル キー テーブルの出力例は次のようになります。

```
Active Tier:

Key   Key                                                              State          Size
Id    MUID                                                                           post-comp

---   ---------------------------------------------------------------  -------------  ---------

0.1   e56                                                              Deactivated        0
0.2   953C694E2128F977FC8B18D7F8A51E44F8847A8D171D0BBDC8C01576FF5DE1D5  Deactivated        0
0.3   851631E574D6F02886CAEF2795896D4C401EBC57A0997EFE04A146E584E9A99A  Activated-RW       0
---   ---------------------------------------------------------------  -------------  ---------

   * Post-comp size is based on last cleaning of Tue Feb 14 10:12:05 2017.
```

注

キーは、バージョン管理キーとしてマークできます。特定のキーの第 2 版、第 3 版が生成された場合、現在の KMIP クエリーはこれらのキーをピックアップせず、Data Domain システムまたは DD VE でそのキーを使用している場合は不具合が発生することがあります。

セットアップ後のキー マネージャーの変更

Embedded Key Manager または RSA DPM Key Manager から選択します。

はじめに

システムの証明書を管理するには、そのシステムで DD System Manager を起動する必要があります。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Encryption**］を選択します。
2. ［Key Management］で、［**Configure**］をクリックします。
3. セキュリティ担当者のユーザー名とパスワードを入力します。
4. 使用する Key Manager を選択します。
    - Embedded Key Manager : キー ローテーションを有効化または無効化します。有効化された場合、1～12 か月のローテーション間隔を入力します。［**Restart the file system now**］を選択し、［**OK**］をクリックします。
    - RSA DPM Key Manager：サーバー名、キー クラス、ポート（デフォルトでは 443）、インポートされたホスト証明書が FIPS 対応であるかどうかを入力します。デフォルト モードが有効です。［**Restart the file system now**］を選択し、［**OK**］をクリックします。
5. 証明書を追加するには、［**Manage Certificates**］をクリックします。

RSA Key Manager の証明書の管理

RSA Key Manager でホスト証明書と CA 証明書両方使用する必要があります。

注

証明書は、RSA Key Manager にのみ必要です。Embedded Key Manager には、証明書は必要ありません。

RSA Key Manager の CA 証明書の追加

CA 証明書をアップロードするかコピーしてペーストします。

手順

1. 以下のいずれかを選択します。
   - CA 証明書を.pem ファイルとしてアップロードするオプションを選択し、［**Browse**］をクリックしてファイルを見つけます。
   - CA 証明書をコピー アンド ペーストするオプションを選択し、表示されたフィールドに証明書の内容をペーストします。
2. ［**Add**］をクリックして証明書を追加します。

RSA Key Manager 用のホスト証明書の追加

証明書を.p12 ファイルとしてアップロードするか、パブリック キーを.pem ファイルとしてアップロードして生成されたプライベート キーを使用します。

開始するには、次の手順の 1 つ目または 2 つ目を選択します。

手順

1. 証明書を.p12 ファイルとしてアップロードするオプションを選択します。
   a. パスワードを入力します。
   b. ［**Browse**］をクリックし、.p12 ファイルを検出します。
2. パブリック キーを.pem ファイルとしてアップロードするオプションを選択し、生成されたプライベート キーを使用します。
   a. ［**Browse**］をクリックし、.pem ファイルを検出します。
3. ［**Add**］をクリックします。

証明書の削除

正しいフィンガープリントがある証明書を選択します。

手順

1. 削除する証明書を選択します。
2. ［削除］をクリックします。

   システムは、削除する証明書のフィンガープリントがある［Delete Certificate］ダイアログが表示されます。
3. ［OK］をクリックします。

静止データの暗号化設定のチェック

DD Encryption 機能のステータスをチェックします。

［**Data Management**］ > ［**File System**］ > ［**Encryption**］タブをクリックします。現在使用中の Key Manager は Enabled と表示されます。DD Encryption 設定の詳細については、暗号化ビューに関するセクションを参照してください。

静止データの暗号化の有効化と無効化

DD Encryption を構成すると、ステータスは有効化され、［Disabled］ボタンがアクティブになります。DD Encryption が無効化されると、［Enabled］ボタンがアクティブになります。

静止データの暗号化の有効化

DD System Manager を使用して、DD Encryption 機能を有効化します。

手順

1. DD System Manager を使用して、ナビゲーション パネルで使用する Data Domain システムを選択します。
2. ［Encryption］ビューで、［**Enable**］ボタンをクリックします。
3. 次のオプションが両方使用可能です。
   - ［**Apply to existing data**］を選択し、［**OK**］をクリックします。ファイル システムの再起動後、最初のクリーニング サイクルで既存のデータが暗号化されます。
   - ［**Restart the file system now**］を選択し、［**OK**］をクリックします。ファイル システムの再起動後、DD Encryption が有効になります。

必要条件

注

ファイル システムの再起動中、アプリケーションが中断される可能性があります。

静止データの暗号化の無効化

DD System Manager を使用して、DD Encryption 機能を無効化します。

手順

1. DD System Manager を使用して、ナビゲーション パネルで使用する Data Domain システムを選択します。
2. ［Encryption］ビューで、［**Disable**］ボタンをクリックします。

   ［Disable Encryption］ダイアログ ボックスが表示されます。

3. ［Security Officer Credentials］領域に、セキュリティ担当者のユーザー名とパスワードを入力します。
4. 次のいずれか 1 つを選択します。
   - ［**Apply to existing data**］を選択し、［**OK**］をクリックします。ファイル システムの再起動後、最初のクリーニング サイクルで既存のデータが復号化されます。

- ［**Restart the file system now**］を選択し、［**OK**］をクリックします。ファイル システムの再起動後、DD Encryption が無効化されます。

必要条件

注

ファイル システムの再起動中、アプリケーションが中断される可能性があります。

ファイル システムのロックとロック解除

DD Encryption が有効な Data Domain システム（およびその外部ストレージ デバイス）が転送されているとき、または交換中のディスクをロックしたい場合、この手順を使用します。この手順には、アカウントが 2 つ必要です。Security Officer および System Administration 役割です。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Encryption**］を選択します。

   ［File System Lock］領域の［Status］には、そのファイル システムが［Locked］か［Unlocked］かが表示されます。

2. ［File System status］領域で［**Disabled**］をクリックして、ファイル システムを無効化します。
3. この手順を使用して、ファイル システムをロックまたはロック解除します。

ファイル システムのロック

ファイル システムをロックするには、DD Encryption を有効化し、ファイル システムを無効化する必要があります。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Encryption** ］を選択し、［**Lock File System**］をクリックします。
2. ［Lock File System］ダイアログ ボックスのテキスト フィールドに、次の項目を入力します。
   - セキュリティ担当者アカウント（Data Domain システムのセキュリティ担当者グループの許可されたユーザー）のユーザー名とパスワード。
   - 現在のパスフレーズと新しいパスフレーズ。
3. ［**OK**］をクリックします。

   この手順で、新しいパスフレーズで暗号化キーが再暗号化されます。このプロセスでは、現在のパスフレーズのキャッシュされたコピー（インメモリとオンディスクの両方）は破棄されます。

   注

   パスフレーズを変更するには、危険な従業員によるデータの破壊の可能性から保護するための 2 ユーザー認証が必要です。

⚠ 注意

パスフレーズは慎重に取り扱ってください。パスフレーズを紛失すると、ファイル システムのロックを解除できず、データに一切アクセスできなくなります。データは失われ、リカバリできません。

4. システムをシャットダウンする手順：

   ⚠ 注意

   シャーシの電源スイッチを使用してシステムの電源をオフにしないでください。代わりに、コマンド プロンプトで次のコマンドを入力します。

   ```
   # system poweroff The 'system poweroff' command shuts down
   the system and turns off the power. Continue? (yes|no|?)
   [no]:
   ```

5. システムをトランスポートするか、交換中のディスクを削除します。
6. システムをオンにし、ファイル システムをロック解除する手順を使用します。

ファイル システムのロック解除

この手順では、宛先に到着した後に使用する暗号化されたファイル システムを準備します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Encryption** ］を選択し、［**Unlock File System**］をクリックします。
2. テキスト フィールドに、ファイル システムのロックに使用されたパスフレーズを入力します。
3. ［**OK**］をクリックします。
4. ［**Close**］をクリックして終了します。

   パスフレーズが不正である場合、ファイル システムは起動せず、システムがエラーをレポートします。前のステップの指示に従って、正しいパスフレーズを入力します。

暗号化アルゴリズムの変更

必要に応じて暗号化アルゴリズムをリセットするか、新規データと既存データまたは新規データのみを暗号化するオプションを選択します。

手順

1. ［**Data Management**］ > ［**File System**］ > ［**Encryption**］を選択します。
2. Data Domain システムの暗号化に使用される Encryption Algorithm を変更するには、［**Change Algorithm**］をクリックします。

   ［Change Algorithm］ダイアログ ボックスが表示されます。対応している暗号化アルゴリズムは次のとおりです。

   - AES-128 CBC
   - AES-256 CBC
   - AES-128 GCM
   - AES-256 GCM

3. ドロップダウン リストから暗号化アルゴリズムを選択するか、デフォルト AES 256-bit（CBC）を許可します。

   AES 256-bit Galois/Counter Mode（GCM）は最も安全なアルゴリズムですが、CBC（Cipher Block Chaining）モードよりも速度はかなり低いです。

   注

   アルゴリズムをデフォルト AES 256-bit（CBC）にリセットするには、［Reset］をクリックしてデフォルトに戻します。

4. 暗号化されるデータを決定する手順：

   - システムの既存および新規データを暗号化するには、［**Apply to Existing data, Restart file system now**］のチェックボックスをクリックし、［**OK**］をクリックする。ファイル システムの再起動後、最初のクリーニング サイクルで既存のデータが暗号化される。

   注

   既存のデータの暗号化には、標準ファイル システム クリーニング操作よりも長くかかる可能性があります。

   - 新規データのみ暗号化するには、［**Restart file system now**］を選択し［**OK**］をクリックする。

5. ステータスが表示されます。プロセスが完了したら、［**Close**］ボタンをクリックします。

   注

   ファイル システムの再起動中、アプリケーションが中断される可能性があります。