
MarkLogic サーバー

『Administrator's Guide』

MarkLogic 9
2017 年 5 月

最終更新 : 9.0-1, 2017 年 5 月

目次

『Administrator's Guide』

1.0	はじめに	16
1.1	目的	16
1.2	対象読者	16
1.3	範囲および要件	16
1.4	アーキテクチャの概要	17
2.0	管理画面	19
2.1	管理画面の概要	19
2.2	管理画面へのアクセス	20
2.3	管理画面からのログオフ	20
2.4	管理者の作成および管理	20
3.0	一般的な管理手順	21
3.1	MarkLogic サーバーのインストールおよびアップグレード	21
3.2	MarkLogic サーバーの開始および停止	21
3.3	フォレストおよびデータベースの作成および設定	22
3.4	アプリケーションサーバーの作成および設定	22
3.5	ユーザー、ロール、権限、およびパーミッションのセットアップ	23
3.6	データベースへのコンテンツの読み込み	23
3.7	XQuery ユースケースの実行およびシンプルなアプリケーションの構築	23
3.8	データのバックアップおよびリストア	24
3.9	パフォーマンスのモニタリングおよびチューニング	24
3.10	管理タスクのスク립ティングおよびスケジュール	25
3.11	クラスタ、グループ、およびフェイルオーバーの設定	26
4.0	MarkLogic サーバーの開始および停止	27
4.1	サーバーの開始	27
4.2	サーバーの停止	27
4.2.1	システムコマンドを使用した MarkLogic サーバーの停止	28
4.2.2	管理画面を使用した MarkLogic サーバーの停止	28
4.3	サーバーの再起動	29
4.4	XQuery スクリプトの例	29
4.4.1	MarkLogic サーバーを再起動するスクリプト	29
4.4.2	MarkLogic サーバーを停止するスクリプト	29

5.0	クラスタ	30
5.1	クラスタ設定の概要	30
5.2	OpenSSL FIPS 140-2 モード	30
5.3	クラスタを設定する手順	30
5.3.1	OpenSSL FIPS 140-2 モードの設定	31
5.3.2	クラスタ暗号化オプション	32
5.3.3	クラスタのカップリング	35
5.4	MarkLogic アプリケーションのメッセージおよびバナーの設定	35
5.4.1	設定の例	36
5.4.2	設定リファレンス	37
5.4.3	例：新しい設定ドキュメントの作成	37
5.4.4	例：設定のアクティブ化 / 非アクティブ化	38
5.4.5	例：通知ダイアログのテキストの修正	39
5.4.6	例：バナーテキストの修正	39
6.0	グループ	40
6.1	グループの概要	40
6.2	例	41
6.3	グループを設定および管理する手順	42
6.3.1	新しいグループの作成	42
6.3.2	グループ設定の表示	43
6.3.3	グループの削除	44
6.3.4	XDQP 上の SSL 通信の有効化	44
6.3.5	SMTP サーバーの設定	45
6.3.6	グループ内のすべてのホストの再起動	46
7.0	HTTP サーバー	47
7.1	HTTP サーバーの概要	47
7.2	HTTP サーバーを作成および管理する手順	48
7.2.1	新しい HTTP サーバーの作成	48
7.2.2	HTTP サーバーの出力オプションの設定	53
7.2.3	HTTP サーバー設定の表示	53
7.2.4	HTTP サーバーの削除	54
7.2.5	リクエストのキャンセル	55
8.0	XDBC サーバー	56
8.1	XDBC サーバーの概要	56
8.2	XDBC サーバーを作成および管理する手順	57
8.2.1	新しい XDBC サーバーの作成	57
8.2.2	XDBC サーバーの出力オプションの設定	62
8.2.3	XDBC サーバー設定の表示	62
8.2.4	XDBC サーバーの削除	63

9.0	WebDAV サーバー	64
9.1	WebDAV サーバーの概要	64
9.1.1	XQuery を実行しないデータベースへの読み取り / 書き込みアクセス	65
9.1.2	WebDAV サーバーのセキュリティ	65
9.1.3	ディレクトリ	66
9.1.3.1	データベース設定でのディレクトリの自動作成	67
9.1.3.2	ディレクトリのプロパティおよび URI	67
9.1.4	サーバーのルートディレクトリ	68
9.1.5	WebDAV サーバー内のドキュメント	69
9.2	WebDAV サーバーを作成および管理する手順	69
9.2.1	新しい WebDAV サーバーの作成	70
9.2.2	WebDAV サーバーの出力オプションの設定	73
9.2.3	WebDAV サーバー設定の表示	74
9.2.4	WebDAV サーバーの削除	75
9.3	WebDAV クライアント	75
9.3.1	テスト済みの WebDAV クライアント	76
9.3.2	サーバーに接続する一般的な手順	77
9.3.3	Windows エクスプローラーで Web フォルダに接続する手順	78
9.4	例：別のサーバーで使用されるドキュメントを追加 / 修正するために WebDAV サーバーをセットアップする	79
10.0	ODBC サーバー	80
10.1	ODBC サーバーの概要	80
10.2	ODBC サーバーを作成および管理する手順	81
10.2.1	新しい ODBC サーバーの作成	82
10.2.2	ODBC サーバーの出力オプションの設定	87
10.2.3	ODBC サーバー設定の表示	87
10.2.4	ODBC サーバーの削除	88
10.2.5	リクエストのキャンセル	89
11.0	イベントの監査	91
11.1	監査の概要	91
11.1.1	監査ログファイル	91
11.1.2	監査イベントの制限	92
11.1.3	成功、失敗、または両方の種類のイベントの監査	93
11.1.4	グループレベルでオン	93
11.2	監査可能イベント	93
11.2.1	監査ログのコンテンツ	97
11.2.2	監査ログの例	99
11.3	グループの監査の設定	99
11.3.1	グループの監査をオンにする	100
11.3.2	グループの監査をオフにする	100
11.3.3	特定イベントを監査する監査設定および特定の制限のセット アップ	100

12.0	ユーザーセッションの管理およびログイン試行のモニタリング	101
12.1	同時ユーザーセッション数の管理	101
12.1.1	ユーザーセッション制限による同時リクエスト数の制限	101
12.1.2	ユーザー同時セッション制御の設定	102
12.2	アプリケーションサーバーのリクエストブラックアウトの設定	102
12.2.1	リクエストブラックアウトの設定	102
12.2.2	リクエストブラックアウトの削除	103
12.3	最終ユーザーログイン試行の格納およびモニタリング	103
12.3.1	最終ログインデータベースへの最終ユーザーログイン情報の格納	104
12.3.2	ユーザーログインのモニタリング設定	104
12.3.3	アプリケーションサーバーまたは管理画面の最終ログイン情報の表示	105
13.0	データベース	106
13.1	データベースについて	106
13.1.1	Schemas および Security データベース	107
13.1.2	Modules データベース	107
13.1.3	Triggers データベース	108
13.1.4	データベース設定	108
13.1.4.1	基本的な管理設定	109
13.1.4.2	ドキュメントに影響を与えるインデックス設定	109
13.1.4.3	リバランサー設定	113
13.1.4.4	再インデックス付け設定	113
13.1.4.5	ドキュメントおよびディレクトリ設定	115
13.1.4.6	メモリおよびジャーナル設定	117
13.1.4.7	その他の設定	120
13.1.4.8	マージ制御設定	121
13.1.5	MarkLogic サーバーのデータベースの例	121
13.2	新しいデータベースの作成	123
13.3	データベースに対するフォレストのアタッチ / デタッチ	124
13.4	データベース設定の表示	125
13.5	ドキュメントをデータベースに読み込む	126
13.6	データベースのマージ	127
13.7	データベースの再インデックス付け	127
13.8	データベースのクリア	128
13.9	データベースの無効化	129
13.10	データベースの削除	130
13.11	データベース内にあるドキュメントのパーミッションの確認および設定	131
14.0	ワードクエリデータベースの設定	132
14.1	ワードクエリ設定について	132
14.1.1	設定オプションの概要	132
14.1.2	含有および除外される要素について	133
14.1.3	含まれる要素の関連度を増減するための重みの追加	135

14.1.4	含まれる要素の属性値の指定	135
14.1.5	インデックスオプション設定について	136
14.2	カスタマイズされたワードクエリ設定	136
15.0	データベースのフィールド設定	140
15.1	フィールドの概要	140
15.2	フィールド設定について	141
15.2.1	フィールド設定オプションの概要	141
15.2.2	ルートフィールドおよびパスフィールド	142
15.2.2.1	ルートフィールド	143
15.2.2.2	パスフィールド	143
15.2.2.3	含有および除外される要素をフィールド設定で決定する方法	144
15.2.2.4	含まれる要素またはプロパティの関連度を増減するための重みの追加	146
15.2.2.5	含まれる要素または除外される要素の属性値の指定	147
15.2.3	メタデータフィールド	148
15.2.4	インデックスオプション設定について	149
15.3	フィールドワードレキシコンとフィールド値レキシコン	149
15.4	フィールドの設定	150
15.4.1	新しいパスフィールドまたはルートフィールドの設定	150
15.4.2	新しいメタデータフィールドの設定	158
15.4.3	既存フィールドの修正	160
15.4.4	フィールドのレンジインデックスの作成	161
16.0	データベースのマージの概要と制御	162
16.1	マージの概要：マージの優れた機能について	162
16.1.1	ダイナミックな自己チューニング	162
16.1.2	マージ時の処理	163
16.1.3	マージをオフにするものの危険性	163
16.1.4	マージによってスコアが変更される	164
16.2	マージポリシーの設定	164
16.2.1	マージポリシーコントロールの概要	165
16.2.2	マージパラメータの説明	166
16.3	マージのブラックアウト期間	168
16.3.1	マージブラックアウトについて	169
16.3.2	マージブラックアウト期間の設定	169
16.3.3	マージブラックアウト期間の削除	170
16.4	マージとポイントインタイムクエリ	170
16.5	負のマージタイムスタンプを設定して、経過時間ウィンドウの期間にフラグメントを保持する	170
16.6	マージのモニタリング	171
16.6.1	ErrorLog.txt ファイル内のメッセージ	171
16.6.2	[Database Status] ページ	172

16.7	明示的なマージコマンド	172
16.7.1	マージの手動開始	172
16.7.2	マージのキャンセル	173
16.8	マージポリシーールールの設定	174
16.8.1	マージのベースラインの決定	174
16.8.2	大規模なマージの数を減らしたい場合	175
16.8.3	その他のソリューション	177
17.0	データベースのリバランス	178
17.1	データベースリバランスの概要	178
17.2	リバランストリガーイベント	179
17.3	リバランスのドキュメント割り当てポリシー	180
17.3.1	バケット割り当てポリシー	180
17.3.2	統計的割り当てポリシー	181
17.3.3	レンジ割り当てポリシー	182
17.3.4	クエリ割り当てポリシー	184
17.3.5	レガシー割り当てポリシー	186
17.3.6	割り当てポリシーのまとめ	187
17.4	リバランスがドキュメントを移動する方法	187
17.4.1	フォレストがデータベースにアタッチされるとき のデータ移動方法	188
17.4.2	フォレストがデータベースからリタイアする ときのデータ移動方法	188
17.5	データベースでのリバランスの設定	189
17.6	フォレストでのリバランスの設定	190
17.7	データベースからフォレストのリタイア	191
17.8	リバランスのステータスの確認	192
17.9	リバランスと他のデータベース設定や フォレスト設定との相互作用	193
17.9.1	データベースのレプリケーション	194
17.9.2	バックアップからデータベースの リストア	194
17.9.3	階層型ストレージ	194
17.9.4	高速ロック	194
17.9.5	dlete-only および read-only の フォレスト	195
17.10	以前のリリースからアップグレードした 後のリバランス設定	195
18.0	階層型ストレージ	196
18.1	この章で使われる用語	197
18.2	階層型ストレージの概要	198
18.3	レンジパーティション	200
18.4	クエリパーティション	202
18.5	パーティションの移行	203
18.6	データベースのレンジパーティション 設定	205
18.6.1	レンジパーティションキーの定義	205

18.6.2	レンジパーティションの作成	207
18.6.2.1	新しいフォレストによるレンジパーティションの作成	207
18.6.2.2	既存フォレストによるレンジパーティションの作成	208
18.7	データベースのクエリパーティション設定	209
18.7.1	クエリパーティションの作成	210
18.7.2	クエリパーティションのクエリ割り当てポリシーの設定	211
18.7.3	クエリパーティションの分離	213
18.8	階層型ストレージ REST API の概要	214
18.8.1	非同期操作	215
18.8.2	権限	215
18.8.3	/manage/v2/databases/{id name}/partitions	215
18.8.4	/manage/v2/databases/{id name}/partitions/{name}	216
18.8.5	/manage/v2/databases/{id name}/partitions/{name}/properties	217
18.8.6	/manage/v2/databases/{id name}/partition-queries	217
18.8.7	/manage/v2/databases/{id name}/partition-queries/{partition-number}	218
18.8.8	/manage/v2/databases/{id name}/partition-queries/{partition-number}/properties	218
18.8.9	/manage/v2/forests	219
18.8.10	/manage/v2/forests/{id name}	220
18.8.11	/manage/v2/forests/{id name}/properties	221
18.9	一般的なフォレストおよびパーティションの操作	222
18.9.1	パーティションの表示	222
18.9.2	フォレストおよびパーティションの移行	223
18.9.3	パーティションのサイズ変更	225
18.9.4	データベース間のパーティション移動	225
18.9.5	フォレストの結合	226
18.9.6	フォレストのリタイア	227
18.9.7	フォレストおよびパーティションのオフライン/オンライン化	227
18.9.8	パーティションの更新許可状態の設定	228
18.9.9	パーティションの削除	228
18.10	フォレストレベルのフェイルオーバーが設定されたパーティション	229
19.0	スーパーデータベースおよびクラスタ	231
19.1	概要	231
19.2	スーパーデータベースの作成	233
19.3	スーパーデータベースおよびサブデータベースの表示	234
20.0	データベースのバックアップおよびリストア	235
20.1	バックアップおよびリストアの概要	236
20.1.1	データベースレベルの一貫性のあるバックアップ	236
20.1.2	管理画面	237
20.1.3	バックアップおよびリストアのトランザクション	237
20.1.4	バックアップディレクトリの構造	237
20.1.5	バックアップおよびリストア操作のフェーズ	240

20.1.5.1	検証フェーズ	240
20.1.5.2	コピーフェーズ	240
20.1.5.3	同期フェーズ	240
20.1.6	バックアップおよびリストア操作に関する注意事項	241
20.2	ジャーナルアーカイブがオンのデータベースバックアップ	242
20.3	増分バックアップ	243
20.3.1	新規フォレストの増分バックアップ	244
20.4	増分バックアップとジャーナルアーカイブの同時使用	245
20.5	データベースのバックアップ	245
20.5.1	データベースの即時バックアップ	245
20.5.2	データベースバックアップのスケジュール	249
20.6	ジャーナルアーカイブがオフのデータベースリストア	252
20.7	ジャーナルアーカイブがオンのデータベースリストア	255
20.7.1	安全なタイムスタンプへのリストア	256
20.7.2	特定タイムスタンプへのリストア	258
20.7.3	サンプルドキュメントに基づいたリストア	258
20.8	ジャーナルアーカイブがオンの増分バックアップからのリストア	259
20.9	ローカルディスクフェイルオーバー後のデータベースのバックアップとリストア	262
21.0	ローリングアップグレード	266
21.1	ローリングアップグレードについて	266
21.1.1	有効バージョンとソフトウェアバージョン	267
21.2	例：ローリングアップグレード	268
21.3	ローリングアップグレードの実行	270
21.3.1	REST 管理 API を使用したローリングアップグレード	270
21.3.2	EC2 インスタンスのアップグレード	272
21.3.3	XQuery を使用したローリングアップグレード	276
21.3.4	本番クラスタと災害対策クラスタの両方のローリングアップグレード	277
21.4	部分アップグレードのロールバック	278
21.5	ローリングアップグレードの API	278
21.5.1	Admin API	278
21.5.2	REST 管理 API	279
21.6	他の MarkLogic 機能との関係	279
21.6.1	SQL	280
21.6.2	サーバーサイド JavaScript	280
21.6.3	カスタム UDF	281
21.6.4	円を含むリバースクエリ	281
21.7	その他のアップグレードオプション	281
22.0	ホスト	282
22.1	クラスタへのホストの追加	282
22.2	ホストのグループ変更	283
22.3	ホストのシャットダウンまたは再起動	284

22.4	ホスト上のフォレストのクリア	284
22.5	ホスト上のフォレストの削除	285
22.6	クラスタからの切り離し	285
22.7	ホストのライセンスキーの変更	287
22.8	トランザクションのロールバック	287
23.0	フォレスト	289
23.1	フォレストについて	290
23.2	フォレストの作成	292
23.3	フォレストを delete-only にする	295
23.4	フォレストを read-only にする	296
23.5	[Forest Summary] ページを使用したフォレストのアタッチおよび デタッチ	298
23.6	フォレストのバックアップ	299
23.6.1	フォレストのバックアップ	299
23.6.2	フォレストバックアップのスケジュール設定	301
23.7	フォレストのリストア	302
23.8	特定時刻へのフォレストのロールバック	303
23.9	フォレストのマージ	303
23.10	フォレストのクリア	304
23.11	フォレストの無効化	304
23.12	ホストからのフォレストの削除	305
23.13	準備された XA トランザクションブランチのロールバック	306
24.0	セキュリティ管理	308
24.1	セキュリティエンティティ	308
24.2	ユーザー	311
24.2.1	ユーザーの作成	311
24.2.2	ユーザー設定の表示	313
24.2.3	ユーザー設定の修正	314
24.2.4	ユーザーの削除	315
24.3	ロール	315
24.3.1	ロールの作成	316
24.3.2	ロールの表示	318
24.3.3	ロール設定の修正	320
24.3.4	ロールの削除	320
24.4	実行権限	321
24.4.1	実行権限の作成	321
24.4.2	実行権限の表示	323
24.4.3	実行権限の修正	323
24.4.4	実行権限の削除	324
24.5	URI 権限	325
24.5.1	URI 権限の作成	325
24.5.2	URI 権限の表示	326
24.5.3	URI 権限の修正	326
24.5.4	URI 権限の削除	327

24.6	Amp	327
24.6.1	Amp の作成	328
24.6.2	Amp の表示	329
24.6.3	Amp の修正	330
24.6.4	Amp の削除	330
24.7	保護されているコレクション	331
24.7.1	保護されているコレクションの作成	332
24.7.2	保護されているコレクションの表示	333
24.7.3	保護されているコレクションからのパーミッションの削除	333
24.7.4	保護されているコレクションの削除	334
24.8	証明書テンプレート	335
24.9	レルム	335
24.9.1	レルムの設定	335
24.9.2	レルムの変更	336
25.0	テキストインデックス	337
25.1	テキストインデックス	337
25.1.1	テキストインデックス設定について	338
25.1.2	テキストインデックス設定の表示	345
25.1.3	テキストインデックスの設定	347
25.2	フレージングおよび element-word-query 境界制御	347
25.2.1	フレージング制御	348
25.2.2	element word query through	349
25.2.3	手順	350
25.2.3.1	フレージングと element-word-query 設定の表示	350
25.2.3.2	フレージングと element-word-query の設定	351
25.2.3.3	フレージングまたは element-word-query 設定の削除	352
25.3	再インデックス付け設定をオンおよびオフにしたクエリ動作	353
25.3.1	reindexer enable 設定について	353
25.3.2	最小限共通項目に従ったクエリ評価	354
25.3.3	再インデックス付けはポイントインタイムバージョンのフラグメントに適用されない	354
25.3.4	シナリオ例	355
26.0	レンジインデックスおよびレキシコン	356
26.1	レンジインデックスについて	357
26.2	値レキシコンにレンジインデックスを使用する	361
26.3	ワードレキシコンについて	361
26.4	パスレンジインデックスについて	362
26.4.1	インデックスパス式の例	362
26.4.2	インデックスパス式の制約	363
26.4.3	インデックスパス式の有効性のテスト	364
26.4.4	インデックスパス式での名前空間プレフィックスの使用	364
26.4.5	インデックスパス式の文法	365
26.5	要素レンジインデックス設定の表示	366

26.6	要素レンジインデックスの定義	366
26.7	属性レンジインデックス設定の表示	368
26.8	属性レンジインデックスの定義	369
26.9	パスレンジインデックス設定の表示	371
26.10	パスレンジインデックスおよびフィールドで使用される名前空間プレフィックスの定義	372
26.11	パスレンジインデックスの定義	373
26.12	要素ワードレキシコン設定の表示	375
26.13	要素ワードレキシコンの定義	376
26.14	属性ワードレキシコン設定の表示	377
26.15	属性ワードレキシコンの定義	378
26.16	値レキシコンの定義	380
26.17	レンジインデックスまたはレキシコンの削除	380
26.18	フィールドレンジインデックスの定義	380
27.0	フラグメント	381
27.1	フラグメンテーション方針の選択	382
27.1.1	フラグメントルート	383
27.1.2	フラグメントの親	383
27.2	フラグメントルートの定義	384
27.3	フラグメントの親の定義	385
27.4	フラグメントルールの表示	387
27.5	フラグメントルールの削除	387
28.0	名前空間	389
28.1	グループの名前空間の定義	390
28.2	HTTP、ODBC、または XDBC サーバーの名前空間の定義	391
28.3	グループの名前空間設定の表示	392
28.4	HTTP、ODBC、または XDBC サーバーの名前空間設定の表示	392
28.5	グループの名前空間の削除	393
28.6	HTTP、ODBC、または XDBC サーバーの名前空間の削除	394
29.0	スキーマの理解と定義	395
29.1	スキーマについて	395
29.2	スキーマの定義の手順	396
29.2.1	グループのスキーマ定義の追加	397
29.2.2	HTTP、ODBC、または XDBC サーバーのスキーマ定義の追加	398
29.2.3	グループのスキーマ定義の表示	399
29.2.4	HTTP、ODBC、または XDBC サーバーのスキーマ定義の表示	400
29.2.5	グループのスキーマ定義の削除	401
29.2.6	HTTP、ODBC、または XDBC サーバーのスキーマ定義の削除	401
30.0	ログファイル	403
30.1	アプリケーションおよびシステムログファイル	403
30.2	ログレベルについて	403

30.3	システムログファイルの設定	404
30.4	アプリケーションログファイルの設定	406
30.5	システムログの表示	407
30.6	アプリケーションログとシステムファイルログの表示	407
30.7	アクセスログファイル	408
31.0	タスクのスケジュール設定	409
31.1	スケジュール設定されたタスクについて	409
31.2	モジュール呼び出しのスケジュール設定	410
31.3	タスクタイプの選択	412
31.3.1	分単位のスケジュール	412
31.3.2	時間単位のスケジュール	413
31.3.3	日と時間単位のスケジュール	414
31.3.4	週、日、および時間単位のスケジュール	414
31.3.5	月、日、および時間単位のスケジュール	415
31.3.6	カレンダーの日および時刻に 1 回の呼び出しのスケジュール	415
32.0	コンフィギュレーションマネージャの使用	416
32.1	コンフィギュレーションマネージャの概要	416
32.2	セキュリティの考慮事項	417
32.3	コンフィギュレーションマネージャへのアクセス	417
32.4	設定の表示	418
32.4.1	リソース設定の参照	418
32.4.2	リソースの検索	421
32.5	設定の検索	421
32.6	設定の編集	422
32.7	設定のエクスポートとインポート	424
32.7.1	設定のエクスポート	425
32.7.2	設定のインポート	427
32.7.3	インポートした設定と現在の設定との比較	428
32.8	インポートした設定の適用	432
33.0	付録 A : 管理タスクの「ホット」と「コールド」	433
33.1	グループ	434
33.2	HTTP、ODBC、XDBC、および WebDAV サーバー	435
33.3	データベース	435
33.4	ホスト	436
33.5	フォレスト	436
33.6	mimetype	436
33.7	セキュリティ	436
34.0	付録 B : 事前定義された実行権限	437

35.0	付録 C : 事前定義されたロール	460
35.1	admin	462
35.2	admin-builtins	462
35.3	admin-module-internal	463
35.4	alert-admin	464
35.5	alert-execution	464
35.6	alert-internal	464
35.7	alert-user	464
35.8	app-builder	464
35.9	app-builder-internal	464
35.10	app-user	464
35.11	application-plugin-registrar	465
35.12	appservices-internal	465
35.13	cpf-restart	465
35.14	custom-dictionary-admin	465
35.15	custom-dictionary-user	465
35.16	custom-language-admin-read	465
35.17	custom-language-admin-write	466
35.18	dls-admin	466
35.19	dls-internal	466
35.20	dls-user	466
35.21	domain-management	467
35.22	filesystem-access	467
35.23	flexrep-admin	467
35.24	flexrep-internal	467
35.25	flexrep-user	467
35.26	hadoop-internal	468
35.27	hadoop-user-all	468
35.28	hadoop-user-read	468
35.29	hadoop-user-write	468
35.30	infostudio-admin-internal	469
35.31	infostudio-internal	469
35.32	infostudio-user	469
35.33	manage-admin	470
35.34	manage-admin-internal	470
35.35	manage-internal	470
35.36	manage-user	471
35.37	merge	471
35.38	network-access	471
35.39	pipeline-execution	471
35.40	pipeline-management	472
35.41	pki	472
35.42	plugin-internal	472
35.43	qconsole-internal	472
35.44	qconsole-user	472
35.45	rest-admin	472

35.46	rest-admin-internal	473
35.47	rest-extension-user	473
35.48	rest-internal	473
35.49	rest-reader	473
35.50	rest-writer-internal	473
35.51	rest-writer	473
35.52	rest-reader-internal	473
35.53	search-internal	473
35.54	security	474
35.55	trigger-management	476
35.56	xa	476
35.57	xa-admin	476
35.58	welcome-internal	477
35.59	xinclude	477
36.0	テクニカルサポート	478

1.0 はじめに

MarkLogic サーバーは、デジタルコンテンツを活用するための強力な NoSQL データベースであり、現実の業務におけるミッションクリティカルなアプリケーションに必要なエンタープライズ機能が装備されています。MarkLogic を使って、XML、SGML、HTML、JSON などの一般的な形式の大量データを活用する複雑なアプリケーションを構築できます。MarkLogic のユニークなアーキテクチャは、アプリケーションの拡張性と高性能を両立しています。対象となるコンテンツリポジトリに対してトランザクションの整合性を保持しながら、検索結果を検索エンジン並みの速度で返します。MarkLogic は分散環境で利用できます。ハードウェアを追加することでインフラストラクチャを拡張できます。

1.1 目的

このドキュメントでは、システム上の MarkLogic の管理に必要なタスクについて説明します。

1.2 対象読者

このドキュメントは、技術系の読者、特に MarkLogic のシステム管理者を対象としています。

1.3 範囲および要件

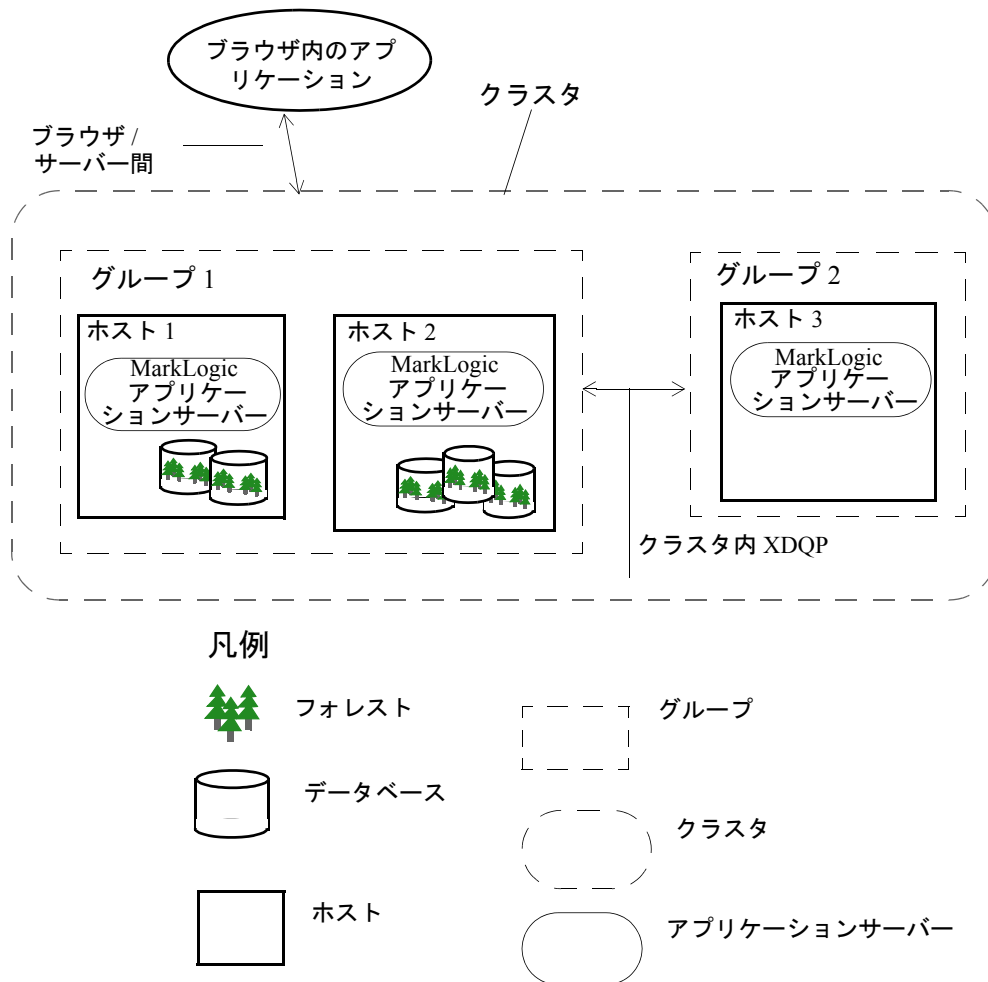
このガイドでは、すべてのプラットフォームで実行している MarkLogic の管理タスクについて説明します。サポートされているプラットフォームの詳細については、『*Installation Guide*』および『*Release Notes*』を参照してください。

このドキュメントでは、ソフトウェアの管理タスクについてのみ説明します。本ソフトウェアの使用法の概要やインストール方法については、次のドキュメントを適宜参照してください。

- 『*Getting Started With MarkLogic Server*』
- 『*MarkLogic Server Installation Guide*』

このドキュメントでは、『*Getting Started with MarkLogic Server*』で説明するすべてのタスクを完了していることを前提としています。そうでない場合、MarkLogic サーバーの管理作業を実行する前に、これらの基本タスクを完了してください。このリリースの機能のリスト、以前のリリースとの既知の非互換性のリスト、およびすべての MarkLogic ドキュメントのリストについては、『*Release Notes*』を参照してください。

1.4 アーキテクチャの概要



この図は、シンプルな MarkLogic サーバー実装の概念図です。各ホストは MarkLogic サーバーのインスタンスと設定済みのアプリケーションサーバーを実行しています。ホストにはあるデータベースに所属する 1 つまたは複数のフォレストが存在可能です。フォレストを持たないホストは、E ノードとして機能しています。1 つあるいは複数のホストが、グループに属することができます。1 つあるいは複数のグループがクラスタを構成します。

アプリケーションはネットワークを介して MarkLogic と通信します。クラスタ内のグループは、XDQP を使用して通信します。クラスタはクラスタ間 XDQP を使用して他のクラスタと通信できます。3 つの通信経路は、それぞれ TLS または SSL を使用するように設定できます。TLS および SSL プロトコルは、FIPS 140-2 承認済み暗号化関数を使用するように設定できます。FIPS モードがデフォルトです。詳細については、「OpenSSL FIPS 140-2 モード」(30 ページ) を参照してください。

詳細については、次を参照してください。

- [ホスト](#)
- アプリケーションサーバー。それぞれのサーバータイプを参照してください。
 - [HTTP サーバー](#)
 - [XDBC サーバー](#)
 - [WebDAV サーバー](#)
 - [ODBC サーバー](#)
- [グループ](#)
- [クラスタ](#)
- [データベース](#)
- [フォレスト](#)

2.0 管理画面

MarkLogic サーバー管理画面は、システム上の MarkLogic サーバーソフトウェアを設定するために使用されます。この章では、管理画面の概要について説明します。この章は、次のセクションで構成されます。

- [管理画面の概要](#)
- [管理画面へのアクセス](#)
- [管理画面からのログオフ](#)
- [管理者の作成および管理](#)

2.1 管理画面の概要

管理画面では、次のタスクを実行できます。

- 基本的なソフトウェア設定の管理
- グループの作成および設定
- データベースの作成および管理
- 新しいフォレストの作成および管理
- フォレストコンテンツのバックアップおよびリストア
- 新しい Web サーバーおよび Java 言語アクセスパスの作成および管理
- セキュリティ設定の作成および管理
- システムパフォーマンスのチューニング
- 名前空間およびスキーマの設定
- システム上のリソースのステータスの確認

管理画面は、MarkLogic サーバーの Web アプリケーションとして実装されています。デフォルトでは、ホストのポート 8001 で実行されます。『*Getting Started with MarkLogic Server*』マニュアルの基本タスクを完了すると、管理画面にアクセスするにはユーザー名およびパスワードの入力が必要となります。認証後は、現在のセッション中にこのガイドで説明する他のタスクを実行するために、ユーザー名およびパスワードを再入力する必要はありません。

設定を変更したら、変更を反映するためにサーバーの再起動が必要となる場合があります。変更の反映にサーバーの再起動が必要でない設定変更を、「ホット」と呼びます。クラスタ型実装の場合、「コールド」タスクでは、変更を反映するためにクラスタ内のすべてのホストで MarkLogic インスタンスを再起動する必要があります。シングルサーバー実装の場合、「コールド」タスクでは、変更を反映するために MarkLogic が再起動されます。「ホット」タスクと「コールド」タスクのリストについては、「付録 A：管理タスクの「ホット」と「コールド」」（433 ページ）を参照してください。

2.2 管理画面へのアクセス

承認済みの管理者のみが管理画面にログインできます。承認済みの管理者とは、`admin` ロールを持つユーザーのことです。承認済みの管理者は、MarkLogic サーバーのすべての管理タスクにアクセスできます。したがって、承認済みの管理者は信頼できる担当者であり、悪意を持っておらず、適切なトレーニングを受けており、正しい管理手順に従うことが要求されます。

管理画面にアクセスするには、次の手順を実行します。

1. ブラウザで、次の URL を開きます。

<http://localhost:8001/>

注： MarkLogic サーバーを実行しているシステム自体から管理画面にアクセスしていない場合は、`localhost` の代わりに MarkLogic サーバーの IP アドレスまたはドメイン名を使用する必要があります。

2. 管理ユーザー名およびパスワードでログインします。管理画面の概要画面が表示されます。

注： このセッション中にすでに管理ユーザーとしてログオンしている場合は、再度ログインする必要はありません。

[Summary] タブでは、MarkLogic サーバーで構成された多くの項目を表示およびクリックできます。[Summary] タブには、すべてのデータベース、アプリケーションサーバー、グループ、フォレスト、セキュリティオブジェクトが表示され、システムに設定されたホストも表示されます。任意のオブジェクトまたはカテゴリをクリックすると、そのオブジェクトまたはカテゴリの詳細ページに移動します。

2.3 管理画面からのログオフ

管理画面からログオフするには、管理画面へのアクセスに使用したブラウザウィンドウを閉じます。これだけで、現在のセッションが終了されます。別のセッションの開始時にはユーザーの再認証が必要となります。

2.4 管理者の作成および管理

MarkLogic サーバー管理者は、`admin` ロールを持つユーザーを定義することで管理されます。`admin` ロールを持つユーザーは、承認済み管理者とも呼ばれる信頼できる担当者であり、悪意を持っておらず、適切なトレーニングを受けており、正しい管理手順に従うことが要求されます。管理者を作成、管理、および削除する手順については、「セキュリティ管理」(308 ページ)を参照してください。

3.0 一般的な管理手順

この章では、MarkLogic サーバーの一般的な管理手順と、各手順の詳細情報の入手先について説明します。

一般的な管理手順には次のものがあります。

- [MarkLogic サーバーのインストールおよびアップグレード](#)
- [MarkLogic サーバーの開始および停止](#)
- [フォレストおよびデータベースの作成および設定](#)
- [アプリケーションサーバーの作成および設定](#)
- [ユーザー、ロール、権限、およびパーミッションのセットアップ](#)
- [データベースへのコンテンツの読み込み](#)
- [XQuery ユースケースの実行およびシンプルなアプリケーションの構築](#)
- [データのバックアップおよびリストア](#)
- [パフォーマンスのモニタリングおよびチューニング](#)
- [管理タスクのスク립ティングおよびスケジュール](#)
- [クラスタ、グループ、およびフェイルオーバーの設定](#)

3.1 MarkLogic サーバーのインストールおよびアップグレード

MarkLogic サーバーは、さまざまなプラットフォームで実行されます。サポートされているプラットフォームのリストとインストール手順については、『*Installation Guide*』を参照してください。

MarkLogic サーバーのアップグレードに関する問題と手順については、以下を参照してください。

- 『*Installation Guide*』の「[Upgrading from Previous Releases](#)」および「[Upgrades and Database Compatibility](#)」
- 『*Scalability, Availability, and Failover Guide*』の「[Upgrading a Cluster to a New Maintenance Release of MarkLogic Server](#)」

注： RedHat OS を使用している場合、オペレーションシステムを Redhat 6 から Redhat 7 にアップグレードする必要があります。MarkLogic 9 は RedHat 6 では実行できません。

3.2 MarkLogic サーバーの開始および停止

MarkLogic サーバーの開始、停止、および再起動操作については、「MarkLogic サーバーの開始および停止」（27 ページ）を参照してください。

3.3 フォレストおよびデータベースの作成および設定

MarkLogic サーバーでは、XML、JSON、XQuery、および JavaScript データが [forest](#) に格納されます。アプリケーションサーバーは [database](#) に接続し、データベースは 1 つあるいは複数のフォレストにアクセスします。

MarkLogic サーバーをインストールすると、複数の種類の [auxiliary databases](#) が作成されます。この詳細については「データベースについて」（106 ページ）を参照してください。このセクションでは、ドキュメントを格納するためのデータベースを作成する一般的な手順の概要を説明しています。

ドキュメントを格納するためのデータベースを作成するには、次の手順を実行します。

1. 1 つあるいは複数のフォレストを作成します。詳細については「フォレストの作成」（292 ページ）を参照してください。ストレージ、パフォーマンス、および可用性のニーズに応じて、複数のフォレストをそれぞれ別のホストに作成できます。詳細については、『*Scalability, Availability, and Failover Guide*』を参照してください。
2. 「新しいデータベースの作成」（123 ページ）で説明する手順に従って、データベースを作成します。すべてのデータベース設定を理解するまでは、[Database Name] フィールドにデータベースの名前を入力するだけにしてください。[Database Specification] のその他のフィールドは、すべてデフォルトの状態の問題ありません。
3. フォレストをデータベースにアタッチします。詳細については「データベースに対するフォレストのアタッチ / デタッチ」（124 ページ）を参照してください。

3.4 アプリケーションサーバーの作成および設定

アプリケーションは、アプリケーションサーバー上で実行されます。アプリケーションサーバーには、特定のデータベース、ポート番号などが設定されます。データベースを作成した後でアプリケーションサーバーを作成できます。MarkLogic サーバーでは、さまざまな種類のアプリケーションをサポートするために、4 種類のアプリケーションサーバーを作成できます。

- HTTP アプリケーションサーバー : XQuery または JavaScript を実行したり、Web サーバーなどのクライアントからの HTTP リクエストを処理したりするために使用します。HTTP アプリケーションサーバーの作成および設定の詳細については、「HTTP サーバーを作成および管理する手順」（48 ページ）を参照してください。
- XDBC アプリケーションサーバー : Java XCC ライブラリを使用するコンテンツベースコネクタ (XCC) アプリケーションに使用します。XDBC アプリケーションサーバーの作成および設定の詳細については、「XDBC サーバーを作成および管理する手順」（57 ページ）を参照してください。

- WebDAV アプリケーションサーバー : WebDAV クライアント経由で MarkLogic サーバーデータベースにアクセスするために使用します。WebDAV アプリケーションサーバーの作成および設定の詳細については、「WebDAV サーバーを作成および管理する手順」(69 ページ) を参照してください。
- ODBC アプリケーションサーバー : SQL クライアント経由で MarkLogic サーバーデータベースにアクセスするために使用します。ODBC アプリケーションサーバーの作成および設定の詳細については、「ODBC サーバーを作成および管理する手順」(81 ページ) を参照してください。

SSL を使用してアプリケーションサーバーの安全性を高めるには、「[XDQP 上の SSL 通信の有効化](#)」を参照してください。

3.5 ユーザー、ロール、権限、およびパーミッションのセットアップ

MarkLogic サーバーには、ドキュメントやアプリケーションへのユーザーアクセスを制御できるセキュリティオブジェクトのセットが豊富に用意されています。詳細については『*Security Guide*』およびこのガイドの「セキュリティ管理」(308 ページ) を参照してください。

管理画面の [Security] ページだけでなく、スクリプト内で XQuery、JavaScript、および REST 関数を使用しても、セキュリティオブジェクトをセットアップおよび管理できます。

3.6 データベースへのコンテンツの読み込み

ドキュメント読み込み関数を使用して、データベースにドキュメントを読み込むことができます。詳細については『*Loading Content Into MarkLogic Server Guide*』を参照してください。

ドキュメントを読み込むように WebDAV サーバーおよびクライアント (Windows エクスプローラーなど) をセットアップすることもできます。Windows エクスプローラーと連携するように WebDAV サーバーを設定する方法の詳細については、『*Content Processing Framework Guide*』の「[Simple Drag-and-Drop Conversion](#)」を参照してください。

ドキュメントは、XCC アプリケーションによってデータベースに読み込むこともできます。詳細については『*XCC Developer's Guide*』の「[Using the Sample Applications](#)」を参照してください。

3.7 XQuery ユースケースの実行およびシンプルなアプリケーションの構築

MarkLogic サーバー設定をテストするには、『*Getting Started with MarkLogic Server*』の「[Exploring the Use Cases](#)」の手順に従ってください。この手順では、クエリコンソールを使用して W3C XQuery ユースケースを評価します。

シンプルな XQuery アプリケーションを構築する手順については、『*Getting Started with MarkLogic Server*』の「[Sample XQuery Application that Runs Directly Against an App Server](#)」を参照してください。詳細については、『*Application Developer's Guide*』を参照してください。XCC API を介して MarkLogic サーバーと通信する Java アプリケーションを記述している場合は、『*XCC Developer's Guide*』を参照してください。

3.8 データのバックアップおよびリストア

データベースのバックアップを作成できます。詳細については「データベースのバックアップ」(245 ページ)を参照してください。このバックアップでは、データベース内のすべてのフォレストをバックアップします。また、データベースで使用される個別のフォレストのバックアップも作成できます。詳細については「フォレストのバックアップ」(299 ページ)を参照してください。

データベースレベルのバックアップとフォレストレベルのバックアップには重要な点で多くの違いがあります。データベースレベルのバックアップの場合、デフォルトでは指定されたディレクトリにデータベース内の全フォレストがバックアップされます。データベースバックアップが開始されるたびに、そのディレクトリに新しいセットのバックアップデータが作成されます。フォレストレベルのバックアップの場合、各フォレストが別々のディレクトリにバックアップされる必要があります。また、フォレストの増分バックアップは前回のバックアップデータに追加されます。フォレストバックアップでは、既存のスタンドバックアップを上書きする前に、前回以降のスタンドの変更の有無を確認することもできます。変更されたスタンドのみが上書きされます。

フルバックアップとともに、増分バックアップおよびジャーナルアーカイブを使用することで、データベースを特定時点 (ポイントインタイム) に復旧できるバックアップを作成できます。詳細については、「データベースのバックアップおよびリストア」(235 ページ)を参照してください。

データベースバックアップからデータベース全体をリストアできます。詳細については「ジャーナルアーカイブがオフのデータベースリストア」(252 ページ)を参照してください。個別のフォレストを、データベースバックアップからリストアできます (「ジャーナルアーカイブがオフのデータベースリストア」(252 ページ)を参照)。または個別のフォレストバックアップからリストアできます (「フォレストのリストア」(302 ページ)を参照)。

3.9 パフォーマンスのモニタリングおよびチューニング

MarkLogic サーバーのパフォーマンスのモニタリングの方法については、『*Query Performance and Tuning Guide*』の「[Monitoring MarkLogic Server Performance](#)」を参照してください。

システムパフォーマンスに影響を与える要因には次のものがあります。

- MarkLogic サーバーの設定。『*Scalability, Availability, and Failover Guide*』の「[Scalability Considerations in MarkLogic Server](#)」を参照してください。

- マージ。「マージの概要：マージの優れた機能について」（162 ページ）を参照してください。
- フラグメントのサイズ。「フラグメント」（381 ページ）を参照してください。
- インデックスの設定。「テキストインデックス」（337 ページ）を参照してください。
- レンジインデックス。「レンジインデックスおよびレキシコン」（356 ページ）を参照してください。
- データベースの再インデックス付け。「データベースの再インデックス付け」（127 ページ）を参照してください。
- データベースのメモリおよびジャーナル設定。「メモリおよびジャーナル設定」（117 ページ）を参照してください。
- データベースフィールドの設定。「データベースのフィールド設定」（140 ページ）を参照してください。
- ログのレベル。「ログレベルについて」（403 ページ）を参照してください。
- トレースイベント。左側のツリーメニューの [Diagnostics] ページのグループ名の下で設定します。

最大限のパフォーマンスが得られるようにアプリケーションをチューニングする方法の詳細については、『*Query Performance and Tuning Guide*』を参照してください。

3.10 管理タスクのスキプティングおよびスケジュール

MarkLogic サーバーには、MarkLogic サーバーの管理タスクを実行する XQuery、JavaScript、および REST スクリプトを記述できるビルトインモジュールおよびライブラリモジュールが用意されています。これらのモジュールで提供される関数を使用して、大半の管理手順をスクリプト化できます。

例えば、Admin Library Module (`admin.xqy`) では、データベース、フォレスト、アプリケーションサーバーを作成または変更したり、SSL セキュリティをセットアップしたりするスクリプトを記述できます。Security Library Module (`security.xqy`) は、セキュリティエンティティをセットアップするスクリプトを作成できる一連の関数を提供します。`xdmp` ビルトイン関数は、フォレストおよびデータベースのバックアップ / リストア操作を実行したり、その他のデータベースおよびフォレストの管理操作を実行したりできます。

管理タスクのスクリプト化の概要については、『*Scripting Administrative Tasks Guide*』の「[Scripting Administrative Tasks in MarkLogic Server](#)」を参照してください。使用可能なすべての管理関数については、『*XQuery and XSLT Reference Guide*』および『*MarkLogic REST API Reference*』を参照してください。

特定の間隔や時刻で管理スクリプトを呼び出すようにスケジュールできます。詳細については「タスクのスケジュール設定」（409 ページ）を参照してください。

3.11 クラスタ、グループ、およびフェイルオーバーの設定

シングルマシン上で実行されている MarkLogic サーバーのシングルインスタンスは、[host](#) と呼ばれます。複数のホストをまとめて 1 つの [cluster](#) として設定できます (『*Scalability, Availability, and Failover Guide*』を参照)。クラスタ内では、同様に設定されたホストをまとめた [groups](#) を作成できます (「グループ」(40 ページ)を参照)。ホストのグループごとに異なるタスクを実行したり、異なるシステム機能を持たせる場合には、設定をホストのグループごとに個別にできるため便利です。

あるホストがダウンした場合、クラスタ内の別のホストがその処理を引き継ぎます。MarkLogic は、フェイルオーバーに対応しています。このため、フォレストのプライマリホストがオフラインになった場合に、フォレストを別のホストに自動的にマウントできます。フェイルオーバーに対応するようにフォレストを設定する詳細については、『*Scalability, Availability, and Failover Guide*』の「[High Availability of Data Nodes With Failover](#)」および「[Configuring Shared-Disk Failover for a Forest](#)」を参照してください。

4.0 MarkLogic サーバーの開始および停止

MarkLogic サーバーを開始および停止するには、次の手順を実行します。

- [サーバーの開始](#)
- [サーバーの停止](#)
- [サーバーの再起動](#)
- [XQuery スクリプトの例](#)

4.1 サーバーの開始

MarkLogic サーバーを開始するには、プラットフォームに応じたコマンドを使用します。

プラットフォーム	コマンド
Microsoft Windows	<p>[スタート] > [すべてのプログラム] > [MarkLogic Server] > [Start MarkLogic Server] を選択します。</p> <p>注： [スタート] メニューから MarkLogic サーバーを起動すると、MarkLogic Server 用の Windows サービス設定が自動的に開始されるように設定されています。また、Windows Vista または Windows 7 を使用している場合、サービスを開始するには、[スタート] メニューの [Start MarkLogic Server] を右クリックし、[管理者として実行] を選択する必要があります。</p>
Red Hat Linux	<code>/sbin/service MarkLogic start</code>
Mac OS X	<code>~/Library/StartupItems/MarkLogic start</code>

4.2 サーバーの停止

MarkLogic サーバーのクリーンシャットダウンを実行する方法は 2 つあります。

- [システムコマンドを使用した MarkLogic サーバーの停止](#)
- [管理画面を使用した MarkLogic サーバーの停止](#)

4.2.1 システムコマンドを使用した MarkLogic サーバーの停止

プラットフォームに適用されるコマンドを使用して、MarkLogic サーバーを停止します。

プラットフォーム	コマンド
Microsoft Windows	[スタート] > [すべてのプログラム] > [MarkLogic Server] > [Stop MarkLogic Server] を選択します。 注： Windows Vista または Windows 7 を使用している場合、サービスを停止するには、[スタート] メニューの [Stop MarkLogic Server] を右クリックし、[管理者として実行] を選択して、操作を許可する必要があります。
Red Hat Linux	<code>/sbin/service MarkLogic stop</code>
Mac OS X	<code>~/Library/StartupItems/MarkLogic stop</code>

4.2.2 管理画面を使用した MarkLogic サーバーの停止

管理画面からサーバーを停止するには、次の手順を実行します。

1. 左側のツリーメニューで [Hosts] アイコンをクリックします。
2. シャットダウンするホストの名前をクリックします。
3. 右上の [Status] タブをクリックします。
4. [shutdown] をクリックします。
5. シャットダウン中に確認メッセージが表示されます。[ok] をクリックしてサーバーをシャットダウンします。

注： 管理画面を使用するには、MarkLogic サーバーが実行中である必要があります。サーバーを停止すると、MarkLogic サーバーを再度起動するまで管理画面にアクセスできなくなります。サーバーを再起動するには、該当プラットフォーム用のシステムコマンドを実行します。詳細については「サーバーの開始」(27 ページ) を参照してください。

4.3 サーバーの再起動

管理画面からサーバーを再起動するには、次の手順を実行します。

1. 左側のツリーメニューで [Hosts] アイコンをクリックします。
2. 右上の [Status] タブをクリックします。
3. [restart] をクリックします。
4. 再起動中に確認メッセージが表示されます。[ok] をクリックして MarkLogic サーバーを再起動します。

前述のようにサーバーを手動で停止してから開始することもできます。

注： 再起動操作は、通常は数秒以内に完了します。ただし、状況によっては時間がかかることがあります（例えば、セキュリティデータベースで復旧を実行する必要がある場合や、クラスタ内のホスト間接続が遅い場合）。MarkLogic サーバーの再起動に数秒以上かかる場合は、管理画面に「503: Service Unavailable」メッセージが表示されることがあります。このような状況が発生した場合は、数秒待ってから管理画面を再読み込みしてください。

4.4 XQuery スクリプトの例

このセクションでは、次の XQuery スクリプトを提供します。

- [MarkLogic サーバーを再起動するスクリプト](#)
- [MarkLogic サーバーを停止するスクリプト](#)

4.4.1 MarkLogic サーバーを再起動するスクリプト

次のスクリプトは、MarkLogic サーバーを再起動します。

```
xquery version "1.0-ml";
xdmp:restart((), "MarkLogic サーバーを再起動します ")
```

4.4.2 MarkLogic サーバーを停止するスクリプト

次のスクリプトは、MarkLogic サーバーを停止します。

```
xquery version "1.0-ml";
xdmp:shutdown((), "MarkLogic サーバーを停止します ")
```

5.0 クラスタ

この章では、管理画面を使用したクラスタの設定について説明します。「クラスタ」は、連携するホストの集合です。この章は、次のセクションで構成されています。

- [クラスタ設定の概要](#)
- [OpenSSL FIPS 140-2 モード](#)
- [クラスタを設定する手順](#)
- [MarkLogic アプリケーションのメッセージおよびバナーの設定](#)

5.1 クラスタ設定の概要

MarkLogic クラスタの一般的な設定では、「エバリュエータ」ノード（E ノード：クエリリクエストを処理するホスト）用に定義されたグループと、「データ」ノード（D ノード：フォレストがアタッチされたホスト）用に定義された別のグループが存在します。

管理画面のクラスタ設定ページでは、クラスタに FIPS 140-2 モードを設定したり、ローカルクラスタと外部クラスタのカップリングができます。各設定オプションについては、管理画面のグループ設定ページの Help タブを参照してください。MarkLogic サーバーのクラスタリングの動作については、『*Scalability, Availability, and Failover Guide*』の「[Clustering in MarkLogic Server](#)」を参照してください。

5.2 OpenSSL FIPS 140-2 モード

MarkLogic サーバーでは、FIPS 対応の OpenSSL を使って、Secure Sockets Layer (SSL v3) と Transport Layer Security (TLS v1) プロトコルを実装します。MarkLogic サーバーをインストールすると、FIPS モードがデフォルトでオンになり、セキュアな FIPS 140-2 暗号化を使用して SSL RSA キーが生成されます。この実装では、弱い暗号化を許可せず、FIPS 140-2 承認済み暗号化関数のみを使用します。アプリケーションを SSL FIPS モードで実行するのに問題がある場合は、後述するように管理画面を使用して FIPS モードをオフにできます。

OpenSSL FIPS 140-2 暗号化機能の詳細については、OpenSSL プロジェクトが提供する次のドキュメントを参照してください。<http://www.openssl.org/docs/fips/fipsvalidation.html>

5.3 クラスタを設定する手順

以下の手順では、MarkLogic サーバーでクラスタを設定する方法を説明します。

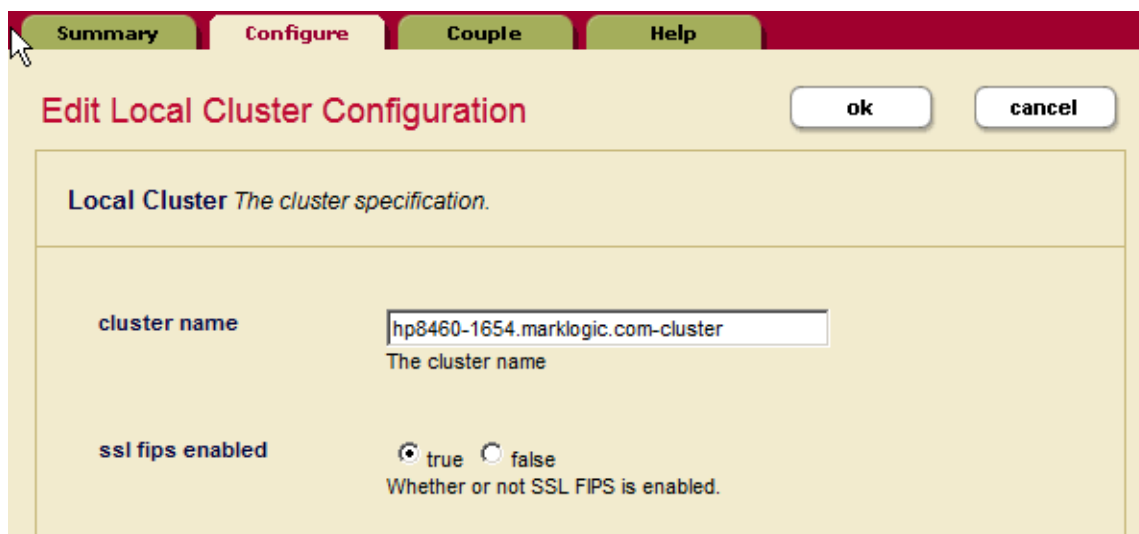
- [OpenSSL FIPS 140-2 モードの設定](#)
- [クラスタ暗号化オプション](#)
- [クラスタのカップリング](#)

5.3.1 OpenSSL FIPS 140-2 モードの設定

FIPS 140-2 モードがオンの場合、システムの起動時に OpenSSL ライブラリが FIPS 140-2 モードで初期化されます。これは MarkLogic サーバーのデフォルトの動作です。実行中のシステムで FIPS モードがオンまたはオフになると、サーバーの再起動を必要とせずに、OpenSSL ライブラリが適切に再設定されます。FIPS モード設定が変更され、セキュアな XDQP が設定されると、すべての XDQP 接続が切断され、再確立されます。

FIPS 140-2 モードで実行するようにクラスタを設定するには、次の手順を実行します。

1. 管理画面にログインします。
2. 左側のツリーメニューで [Clusters] アイコンをクリックします。
3. ローカルクラスタを選択します。[Edit Local Cluster Configuration] ページが表示されます。



4. FIPS 140-2 モードを設定するには、必要に応じて `true` または `false` を選択します。SSL FIPS をオンにするには、`true` を選択します。
5. [ok] をクリックして変更を保存します。

5.3.2 クラスタ暗号化オプション

Key Management Service (KMS) は、データを暗号化するために使用される暗号化キーを安全な場所に格納するキーストアを管理します。このキーストアは、MarkLogic の組み込み PKCS #11 保護ウォレット、または KMIP 標準インターフェイスに準拠する外部のサードパーティ KMS のいずれかです。組み込みのキーストアは、MarkLogic 9.0-x 以降をインストールすると、デフォルトでインストールされます。

このセクションでは、グループに暗号化を設定する方法について説明します。メディア上のデータを保護するように暗号化を設定する詳細については、『*Security Guide*』の「[Encryption at Rest](#)」を参照してください。

注： 暗号化情報を追加または変更するには、クラスタ内のすべてのホストを再起動する必要があります。

管理画面で組み込みのキーストアを使用して暗号化を設定するには、次の手順を実行します。

1. 左側のナビゲーションツリーで [Clusters] をクリックし、設定するクラスタの名前をクリックします。
2. ページが開いたら、[Configure] タブをクリックして [Edit Local Cluster Configuration] ページに移動します。

The screenshot shows a configuration window with the following settings:

- data encryption***: default-off (dropdown), Enable encryption at rest for user data
- config encryption***: off (dropdown), Enable encryption at rest for configuration files
- logs encryption***: off (dropdown), Enable encryption at rest for new log files, log files created from this point on.
- Key Management Service (KMS)**: internal external

* -- requires restart of all the hosts in the cluster

Buttons: ok, cancel

3. ドロップダウンメニューを使用して、データ、設定ファイル、ログファイルの暗号化を設定します。

設定	説明
data encryption	<p>ユーザーデータの暗号化をオンにするかどうかを指定します。 [force] オプションは、クラスタ内のすべてのデータを強制的に暗号化します。データベース設定ではこの設定を上書きできません。 [default-on] オプションは、暗号化をデフォルトでオンにします。データベース設定でこの設定を上書きできます。[default-off] オプションは、暗号化をオフにします。データベース設定でこの設定を上書きできます。</p>
config encryption	<p>設定ファイルの暗号化をオンにするかどうかを指定します。</p>
logs encryption	<p>ログファイルの暗号化をオンにするかどうかを指定します。</p>
Key Management Service (KMS)	<p>KMS のタイプを指定します。</p> <p>キーストアとは、データを暗号化するために使用される実際の暗号化キーが格納される安全な場所です。暗号化用キーストアとして安全なのは、キー管理システム (KMS) です。このキーストアは、MarkLogic の組み込み PKCS #11 保護ウォレット、または外部のサードパーティ KMS のいずれかです。</p>

4. 完了したら [ok] をクリックします。

外部の KMS を設定するには、次の手順を実行します。

1. [Key Management Service (KMS)] フィールドで、[external] を選択します。

Key Management Service (KMS)

internal external

host name
The host name of the Key Management Server

port
The Key Management Server's client socket port number

data encryption key id
An string identifying the encryption key at the KMS that should be use to encrypt user data

config encryption key id
An string identifying the encryption key at the KMS that should be use to encrypt configuration files

logs encryption key id
An string identifying the encryption key at the KMS that should be use to encrypt log files

* -- requires restart of all the hosts in the cluster

2. 外部の KMS および必要な暗号化キーを特定する次の情報を入力します。

設定	説明
host name	Key Management Server (KMS) のホスト名。
port	KMS クライアントのソケットポート番号。
data encryption key id	KMS に存在する、ユーザーデータを暗号化するための暗号化キー。
config encryption key id	KMS に存在する、設定ファイルを暗号化するための暗号化キー。
logs encryption key id	KMS に存在する、ログファイルを暗号化するための暗号化キー。

暗号化キーは、Network Working Group Request for Comments: 4122 で定める UUID の URN 表現にする必要があります。

<http://www.ietf.org/rfc/rfc4122.txt>

例えば次のようになります。

```
06ea22c9-b972-4652-8d0f-9e58c62e0f7f
```

3. 完了したら [ok] をクリックします。

5.3.3 クラスタのカップリング

管理画面を使用して、ローカルクラスタと外部クラスタをカップリング（連結）してクラスタ間のコミュニケーションをオンにできます。あるクラスタのデータベースを別のクラスタのデータベースにレプリケートするには、2つのクラスタをカップリングする必要があります。クラスタ間コミュニケーションとデータベースレプリケーションの関係の詳細については、『*Database Replication Guide*』を参照してください。具体的なクラスタのカップリングの詳細については、『*Database Replication Guide*』の「[Coupling the Local and Foreign Clusters](#)」を参照してください。

5.4 MarkLogic アプリケーションのメッセージおよびバナーの設定

このトピックでは、ユーザーがビルトインの MarkLogic アプリケーションのページ（クエリコンソールやモニタリングダッシュボードなど）に移動したときに通知ダイアログとアプリケーションバナーを表示するようにクラスタを設定する方法について説明します。

管理者は、次のような状況のときに、この機能を使用できます。

- ユーザーに重要なシステムステータス変更（計画された停止など）を通知する。
- ユーザーが MarkLogic クラスタを区別しやすくする（テスト環境と本番環境など）。

通知ダイアログは、ユーザーが MarkLogic アプリケーションに接続するホストごとに各ユーザーに 1 回のみ表示されます。通知メッセージが変更されると、影響を受けるいずれかのアプリケーションにユーザーが次回アクセスしたときに、ダイアログが再度表示されます。

URI `/cluster-ui-settings.xml` を使用して、App-Services データベース内の設定ドキュメントで UI 設定を指定します。MarkLogic では、カスタマイズの基礎として使用できるデフォルト設定が非アクティブな状態でインストールされています。

詳細については、次のトピックを参照してください。

- [設定の例](#)
- [設定リファレンス](#)
- [例：新しい設定ドキュメントの作成](#)
- [例：設定のアクティブ化 / 非アクティブ化](#)
- [例：通知ダイアログのテキストの修正](#)
- [例：バナーテキストの修正](#)

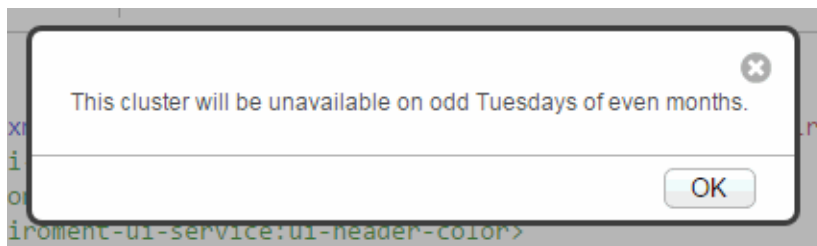
5.4.1 設定の例

この例は、次の設定に基づいています。(可読性を高めるため、スペースが追加されています。) 要素の構造および意味の詳細については、「設定リファレンス」(37 ページ)を参照してください。

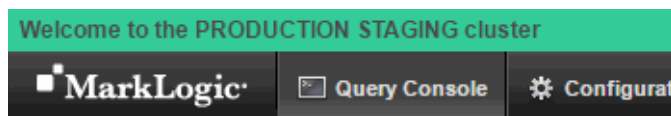
```
<env-ui:environment-ui xml:lang="zxx"
  xmlns:env-ui="http://marklogic.com/environment-ui">
  <env-ui:ui-active>true</env-ui:ui-active>
  <env-ui:ui-label>Welcome to the PRODUCTION STAGING cluster</env-ui:ui-label>
  <env-ui:ui-header-color>#33CC99</env-ui:ui-header-color>
  <env-ui:ui-header-text-color>#000000</env-ui:ui-header-text-color>
  <env-ui:ui-message>
    This cluster will be unavailable on odd Tuesdays of even months.
  </env-ui:ui-message>
</env-ui:environment-ui>
```

この設定は、クエリコンソールやモニタリングダッシュボードなどのアプリケーションの UI に次のような影響があります。

1. ユーザーがいずれかのビルトインの MarkLogic アプリケーションに初めて移動したときに、MarkLogic は次のダイアログを表示します。このテキストは、`ui-message` 設定要素で指定しています。



2. ユーザーがダイアログを閉じると、設定済みのバナーがアプリケーションページの上部に表示されます。このテキストは、`ui-label` 設定要素で指定しています。バナーの色は、`ui-header-color` および `ui-header-text-color` 要素で指定しています。



UI のカスタマイズがアクティブでない場合、バナーは表示されません。

5.4.2 設定リファレンス

App-Services データベースの `/cluster-ui-settings.xml` ドキュメントは、次の構造になっている必要があります。すべての要素が必須です。

```
<env-ui:environment-ui xml:lang="zxx"
  xmlns:env-ui="http://marklogic.com/environment-ui">
  <env-ui:ui-active>boolean</env-ui:ui-active>
  <env-ui:ui-label>banner_text</env-ui:ui-label>
  <env-ui:ui-header-color>color_code</env-ui:ui-header-color>
  <env-ui:ui-header-text-color>color_code</env-ui:ui-header-text-color>
  <env-ui:ui-message>notification_dialog_text</env-ui:ui-message>
</env-ui:environment-ui>
```

子要素の詳細について、次の表で説明します。

要素のローカル名	説明
ui-active	true に設定すると、設定が有効になります。false に設定すると、デフォルトの動作に戻ります（通知ダイアログやバナーを表示しない）。
ui-label	バナーに表示されるテキスト。
ui-header-color	バナーの背景色。
ui-header-text-color	バナーのメッセージテキストの色。
ui-message	通知ダイアログボックスに表示されるメッセージ。このメッセージは、新しいメッセージで設定を更新しない限り、ユーザーに（ユーザーがクラスタに接続するために使用するホストごとに）1 回のみ表示されます。

5.4.3 例：新しい設定ドキュメントの作成

まったく新しい設定ドキュメントを作成するときは、既存の設定の一部を置き換えるのではなく、この例を使用してください。変更を追加する場合は、残りの例を参照してください。

MarkLogic と同時にインストールされるテンプレート設定を使用して新しい設定を作成するには、この手順に従います。テンプレート設定はデフォルトでアクティブではないことに注意してください。

1. App-Services データベースからテンプレート設定を読み取り、これに変更を加えていきます。デフォルト設定を読み取るには、次のように入力します。

```
xquery version "1.0-ml";
fn:doc('/cluster-ui-settings.xml')
```

- 要件を満たすように設定を修正します。
- 新しい設定を App-Services データベースに挿入します。例えば次のようになります。

```
xquery version "1.0-m1";
let $new-config := (: YOUR CONFIG ELEM HERE :)
return xdm:document-insert('/cluster-ui-settings.xml', $new-config)
```

- いずれかのビルトイン MarkLogic アプリケーションに移動して、変更を確認します。例えば、クエリコンソール (<http://host:8000/qconsole>) に移動します。いずれかのアプリケーションをブラウザですでに開いている場合は、ページを再読み込みします。

ダイアログやバナーが表示されない場合は、設定にエラーがある可能性があります。MarkLogic は、設定を `INSTALL_DIR/Config/environment-ui.xsd` 内のスキーマに対して検証します。

5.4.4 例：設定のアクティブ化 / 非アクティブ化

次のスクリプトを使用して、設定をアクティブ化または非アクティブ化します。スクリプトはクエリコンソールで App-Services データベースに対して実行します。

```
xquery version "1.0-m1";
declare namespace env-ui = "http://marklogic.com/environment-ui";

(: Set this var to false to deactivate, true to activate :)
let $state := fn:false()
let $env-ui-node :=
  fn:doc('/cluster-ui-settings.xml')/env-ui:environment-ui
return
  if (exists($env-ui-node)) then
    xdm:node-replace(
      $env-ui-node/env-ui:ui-active,
      <env-ui:ui-active>{$state}</env-ui:ui-active>)
  else ()

(: Reload Query Console to see your changes :)
```

5.4.5 例：通知ダイアログのテキストの修正

次のスクリプトを使用して、通知ダイアログボックスに表示されるテキストを変更します。テキストを変更すると、ユーザーがいずれかのビルトインの MarkLogic アプリケーションに次回移動したときに、ダイアログが表示されます。

このスクリプトはクエリコンソールで App-Services データベースに対して実行します。

```
xquery version "1.0-ml";
declare namespace env-ui = "http://marklogic.com/environment-ui";

(: Set this variable to your new notification :)
let $new-message := "This is your new message."
let $env-ui-node :=
  fn:doc('/cluster-ui-settings.xml')/env-ui:environment-ui
return
  if (exists($env-ui-node)) then
    xdmp:node-replace(
      $env-ui-node/env-ui:ui-message,
      <env-ui:ui-message>{$new-message}</env-ui:ui-message>)
    else ()

(: Reload Query Console to see your changes.:)
```

クエリコンソールを再読み込みすると、通知ダイアログボックスが表示されます。新しいメッセージが含まれていることを確認してください。

5.4.6 例：バナーテキストの修正

次のスクリプトを使用して、ビルトイン MarkLogic アプリケーションの各ページ上部に表示されるバナーのテキストを変更します。スクリプトはクエリコンソールで App-Services データベースに対して実行します。

```
xquery version "1.0-ml";
declare namespace env-ui = "http://marklogic.com/environment-ui";

(: Set this variable to your new banner label :)
let $new-label := "This is your new banner text."
let $env-ui-node :=
  fn:doc('/cluster-ui-settings.xml')/env-ui:environment-ui
return
  if (exists($env-ui-node)) then
    xdmp:node-replace(
      $env-ui-node/env-ui:ui-label,
      <env-ui:ui-label>{$new-label}</env-ui:ui-label>)
    else ()

(: Reload Query Console to see your changes.:)
```

6.0 グループ

この章では、MarkLogic サーバーのグループについて説明します。次のセクションで構成されています。

- [グループの概要](#)
- [例](#)
- [グループを設定および管理する手順](#)

この章では、管理画面を使用してグループを作成および設定する方法について説明します。グループをプログラムによって作成および設定する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring Groups](#)」を参照してください。

6.1 グループの概要

グループ、ホスト、およびクラスタの基本的な定義は次のとおりです。

- 「グループ」とは、クラスタ内において同様に設定されたホストの集まりです。
- 「ホスト」とは、シングルマシン上で実行されている MarkLogic サーバーのインスタンスです。
- 「クラスタ」は、連携するホストの集合です。

シングルノード構成では、一度に1つのグループのみを使用できます（ホストが1つしかないため）。複数のホストによるクラスタ構成では、該当する環境に適切な数のグループ構成を使用できます。

グループを使用することで複数の構成を使用でき、それぞれの構成は別々のホストの集合に適用されます。ホストによって実行するタスクが異なる場合や、ホストによってシステム機能（ディスク容量、メモリなど）が異なる場合は、異なる構成が必要になることもよくあります。一般的なクラスタ構成では、「エバリュエータ」ノード（クエリリクエストを処理するホスト）用に定義されたグループと、「データ」ノード（フォレストがアタッチされたホスト）用に定義された別のグループが存在します。

HTTP、ODBC、XDBC、および WebDAV サーバーはグループレベルで定義され、グループ内のすべてのホストに適用されます。スキーマおよび名前空間もグループレベルで定義して、グループ全体に適用できます。

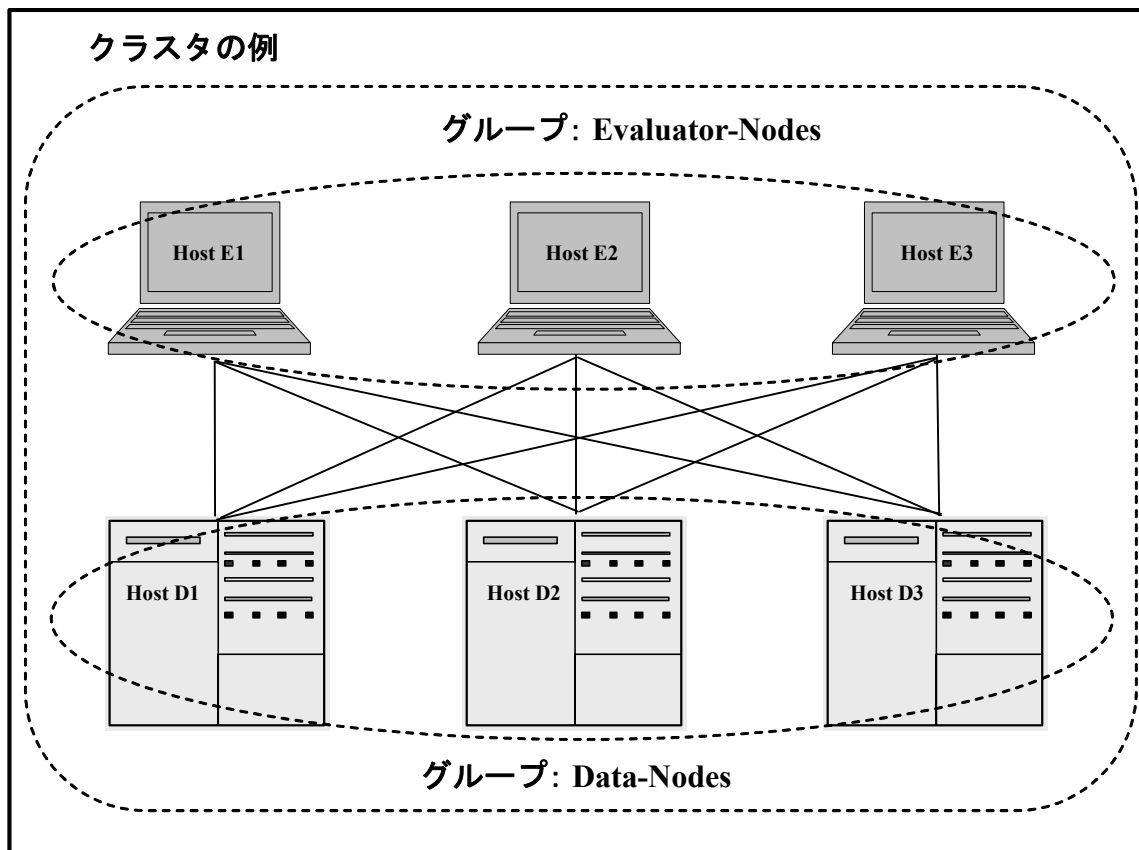
管理画面の [Group Administration] セクションの [Configure] タブでは、メモリ設定、SMTP サーバー設定、およびその他の設定について、設定情報を定義できます。設定の値は、インストール時のシステムメモリ構成に基づいて、インストール時に設定されません。各設定オプションについては、管理画面の [Group Administration] セクションの [Help] タブを参照してください。

6.2 例

MarkLogic サーバーにおけるクラスタ、グループ、およびホストの関係は、例で説明したほうがわかりやすいでしょう。

この例では、各マシンがサンプルクラスタ内でホストとして設定されています。具体的には、ホスト E1、E2、および E3 は、Evaluator-Nodes グループに属しています。これらのホストには、ユーザーアプリケーションを実行するための HTTP サーバーおよび XDBC サーバーが設定されています。Evaluator-Nodes グループ内のホストはすべて、MarkLogic サーバーの設定が全く同じになっています。

ホスト D1、D2、および D3 は、Data-Nodes グループに属しています。Data-Nodes グループ内のホストには、データフォレストが設定され、データリクエストを処理するために Evaluator-Nodes グループ内のノードとやり取りします。データフォレストの設定の詳細については、データベース、フォレスト、およびホストに関するセクションを参照してください。



クラスタの詳細については、『*Scalability, Availability, and Failover Guide*』を参照してください。

注： シングルホスト MarkLogic 環境を管理している場合、ホストはインストールプロセス時に Default グループに自動的に追加されます。グループにはホストが 1 つしかなく、他のホストをグループに追加できません。

6.3 グループを設定および管理する手順

以下の手順では、MarkLogic サーバーでグループを作成および管理する方法について説明します。

- [新しいグループの作成](#)
- [グループ設定の表示](#)
- [グループの削除](#)
- [XDQP 上の SSL 通信の有効化](#)
- [SMTP サーバーの設定](#)
- [グループ内のすべてのホストの再起動](#)

6.3.1 新しいグループの作成

新しいグループを作成するには、次の手順を実行します。

1. 管理画面にログインします。
2. 左側のツリーメニューで [Groups] 下にあるアイコンをクリックします。
3. [Group Summary] ページの [Create] タブをクリックします。[Create Group] ページが表示されます。



4. [group name] フィールドに移動し、グループの短い名前を入力します。

MarkLogic サーバーは、グループを参照するためにこの名前を使用します。

5. [list cache size]、[compressed tree cache size]、および [expanded tree cache size] の値は変更することもデフォルトのままにすることもできます。これらの設定では、タームリスト、圧縮形式のツリーデータ、および展開形式のツリーデータをキャッシュする専用のメモリ量を指定します。

6. [System Log Level] は、オペレーティングシステムに送信される最小ログレベルメッセージを指定します。ログレベルは、詳細なほうから降順にリスト表示されています。システムログレベルは変更することもデフォルトレベルのままにすることもできます。
7. [File Log Level] は、ログファイルに送信される最小ログレベルメッセージを指定します。ログレベルは、詳細なほうから降順にリスト表示されています。ファイルログレベルは変更することもデフォルトレベルのままにすることもできます。
8. [Rotate Log Files] フィールドは、新しいログファイルを開始する頻度を指定します。このフィールドは変更することも指定されているデフォルト値のままにすることもできます。
9. [Keep Log Files] フィールドは、保持するログファイルの数を指定します。このフィールドは変更することも指定されているデフォルト値のままにすることもできます。
10. [Failover Enable] は、グループ内のホストでフェイルオーバーをオンにする場合は [true] に設定します。フェイルオーバーを使用するには、個々のフォレストのフェイルオーバーをオンにする必要もあります。[Failover Enable] を [false] に設定すると、グループ内の他のフォレストの設定に関係なく、グループ内のすべてのホストでフェイルオーバーがオフになります。
11. [SSL Enabled] オプションおよび [XDQP SSL Ciphers] フィールドは XDQP で SSL をオンにするためのものです。
12. [ok] をクリックします。

注： 監査イベントを設定する方法など監査の詳細については、「イベントの監査」(91 ページ) を参照してください。

グループの追加は「ホット」管理タスクなので変更は再起動しなくてもすぐに反映されます。

6.3.2 グループ設定の表示

特定グループの設定を表示するには、次の手順を実行します。

1. 管理画面にログインします。
2. 左側のツリーメニューで [Groups] 下にあるアイコンをクリックします。
3. 右上の [Configure] タブをクリックします。
4. 設定を表示するグループを特定します。
5. このグループのアイコンをクリックします。
6. 設定を表示します。

6.3.3 グループの削除

グループを削除する前に、そのグループに割り当てられているすべてのホストをドロップする必要があります。グループを削除するには、次の手順を実行します。

1. 管理画面にログインします。
2. 左側のツリーメニューで [Groups] 下にあるアイコンをクリックします。
3. 右上の [Configure] タブをクリックします。
4. 削除するグループを特定します。
5. [Hosts] をクリックして、グループに割り当てられているホストがないことを確認します。グループを削除する前に、グループに割り当てられているすべてのホストがドロップされて（切り離されて）いる必要があります。グループからホストをドロップしても、クラスタからはドロップされません。
6. このグループのアイコンを再度クリックします。
7. [delete] をクリックします。グループを削除すると、そのグループがシステムから削除されます。
8. 確認メッセージが表示されます。[ok] をクリックすると、グループは恒久的に削除されます。

グループの削除はホット操作です。変更を反映するために、サーバーを再起動する必要はありません。

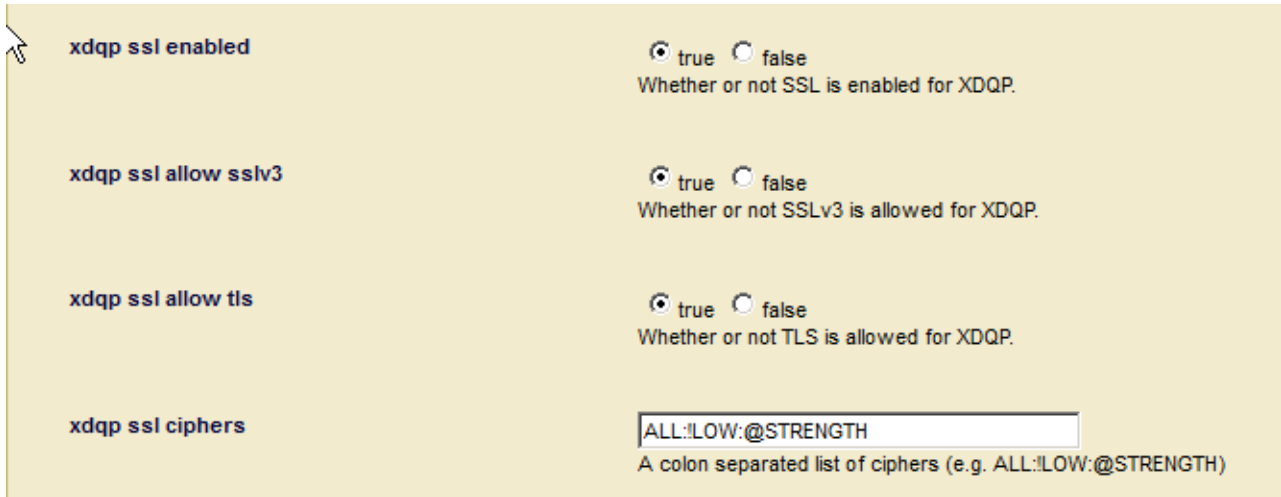
6.3.4 XDQP 上の SSL 通信の有効化

グループ内のホスト間で暗号化された SSL 通信を有効にするには、[xdqp ssl enabled] を [true] に設定します。ソケットの他端が SSL がオンでないグループ内であっても、グループ内のホスト間のすべての通信は保護されます。

ホストが使用する SSL キーおよび証明書は、MarkLogic サーバーをインストールまたはアップグレードするときに、自動的に生成されます。クラスタ内のサーバー間での内部 XDQP 接続では、外部の認証局による認証の証明は行われません。ここでの証明書は自己署名であり、クラスタ内の各サーバーによって信頼されます。

Web ブラウザとアプリケーションサーバーの間の SSL 通信を設定する方法の詳細については、『[Security Guide](#)』の「[Configuring SSL on App Servers](#)」を参照してください。SSL 通信の FIPS 140-2 モードを設定する方法の詳細については、「OpenSSL FIPS 140-2 モード」(30 ページ)を参照してください。

次の画面は、クラスタ内 XDQP 通信の SSL 設定に関連するオプションを示しています。



xdqp ssl enabled true false
Whether or not SSL is enabled for XDQP.

xdqp ssl allow sslv3 true false
Whether or not SSLv3 is allowed for XDQP.

xdqp ssl allow tls true false
Whether or not TLS is allowed for XDQP.

xdqp ssl ciphers
A colon separated list of ciphers (e.g. ALL:!LOW:@STRENGTH)

6.3.5 SMTP サーバーの設定

インストールプロセスでは、インストール時の環境に基づいて SMTP サーバーが設定されます。グループ内のすべてのホストに対して、SMTP サーバーが 1 つ設定されます。SMTP 設定は、アプリケーションで `xcmp:email` 関数を使用するときに使用されます。

システムの SMTP サーバーまたは SMTP タイムアウト（SMTP リクエストが失敗してエラーとなるまでの時間）を変更するには、次の手順を実行します。

1. 管理画面にログインします。
2. 左側のツリーメニューで [Groups] 下にあるアイコンをクリックします。
3. 右上の [Configure] タブをクリックします。
4. [SMTP Relay] フィールドで、SMTP サーバーのホスト名を入力します。
5. [SMTP Timeout] フィールドで、リクエストがタイムアウトするまでの時間（秒数）を入力します。
6. [ok] をクリックします。

SMTP 設定の変更はホット操作です。変更を反映するために、サーバーを再起動する必要はありません。

6.3.6 グループ内のすべてのホストの再起動

管理画面からグループ内のすべてのホストを再起動するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] 下にあるアイコンをクリックします。
2. メニューツリーまたは [Group Summary] ページで、再起動するグループの名前をクリックします。
3. 右上の [Status] タブをクリックします。
4. [restart] をクリックします。
5. 再起動中に確認メッセージが表示されます。[ok] をクリックして、MarkLogic サーバーグループ内のすべてのホストを再起動します。

注： 再起動操作は、通常は数秒以内に完了します。ただし、状況によっては時間がかかることがあります（例えば、セキュリティデータベースで復旧を実行する必要がある場合や、クラスタ内のホスト間接続が遅い場合）。MarkLogic サーバーの再起動に数秒以上かかる場合は、管理画面に「503: Service Unavailable」メッセージが表示されることがあります。このような状況が発生した場合は、数秒待ってから管理画面を再読み込みしてください。

7.0 HTTP サーバー

この章では、HTTP サーバーについて、および HTTP サーバーの設定手順について説明します。次のセクションで構成されています。

- [HTTP サーバーの概要](#)
- [HTTP サーバーを作成および管理する手順](#)

この章では、管理画面を使用して HTTP サーバーを作成および設定する方法について説明します。HTTP サーバーをプログラムによって作成および設定する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring App Servers](#)」を参照してください。

7.1 HTTP サーバーの概要

MarkLogic サーバーでは、サーバーサイド XQuery、JavaScript、および REST プログラムにアクセスできる HTTP サーバーに対して一連の XML または JSON コンテンツを提供する Web アプリケーションを開発できます。これらのアプリケーションは、ブラウザなどの HTTP 対応クライアントアプリケーションに対して XHTML、XML、または JSON コンテンツを返すことができます。

HTTP サーバーはグループレベルで定義され、グループ内のすべてのホストからアクセスできます。各 HTTP サーバーは、指定されたディレクトリ構造内にある一連の XQuery プログラムへのアクセスを提供します。グループ内の各ホストは、このディレクトリ構造にアクセスできるか、プログラムファイルとディレクトリ構造をミラーリングする必要があります。HTTP サーバーは、接続先のデータベースに対してサーバーサイドプログラムを実行します。

HTTP サーバーは、WebDAV、ODBC、および XDBC サーバーと同様に、MarkLogic サーバーセキュリティモデルに従います。サーバーは、これらのプログラムへのアクセスを認証するために、その HTTP サーバー用のセキュリティデータベースに格納されているユーザー ID およびパスワードを使用します（各 HTTP サーバーはデータベースに接続され、各データベースはユーザーなどのセキュリティオブジェクトが格納されているセキュリティデータベースに接続されています）。

HTTP サーバーは、指定されたファイルシステム内の場所や Modules データベースからコードを実行します。

システムやデータへのきめ細かなアクセス制御は、権限およびパーミッションを使用して実現されます。MarkLogic サーバーのセキュリティオブジェクトを設定する方法の詳細については、「セキュリティ管理」（308 ページ）を参照してください。MarkLogic サーバーセキュリティモデルの概念については、『*Security Guide*』を参照してください。

7.2 HTTP サーバーを作成および管理する手順

HTTP サーバーを作成および管理するには、次の手順を実行します。

- [新しい HTTP サーバーの作成](#)
- [HTTP サーバーの出力オプションの設定](#)
- [HTTP サーバー設定の表示](#)
- [HTTP サーバーの削除](#)
- [リクエストのキャンセル](#)

7.2.1 新しい HTTP サーバーの作成

新しいサーバーを作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. HTTP サーバーを定義するグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 右上の [Create HTTP] タブをクリックします。[Create HTTP Server] ページが表示されます。

The screenshot shows the 'Create HTTP Server' dialog box. The left sidebar shows a tree view with 'Configure' > 'Groups' > 'Default' > 'App Servers' > 'NewServer'. The main area has three input fields: 'server name', 'root', and 'port'. Each field has a description and a red error message: 'Required. You must supply a value for http-server-name.', 'Required. You must supply a value for root.', and 'Required. You must supply a value for port.' respectively. 'ok' and 'cancel' buttons are at the top right.

5. [Server Name] フィールドで、この HTTP サーバーの短い名前を入力します。MarkLogic サーバーでは、管理画面でこのサーバーを参照する際にこの名前を使用します。

6. [root] ディレクトリフィールドで、プログラムを格納するディレクトリの名前を入力します。[modules] フィールドでデータベースを指定している場合、ルートは指定された Modules データベース内のディレクトリ URI である必要があります。

[modules] フィールドでファイルシステムを指定している場合、ルートディレクトリは完全修飾パス名であるか、MarkLogic サーバーがインストールされているディレクトリからの相対パスとなります。プラットフォーム別のデフォルトのインストールディレクトリを次の表に示します。

プラットフォーム	プログラムディレクトリ
Microsoft Windows	C:\Program Files\MarkLogic
Red Hat Linux	/opt/MarkLogic
Mac OS X	~/Library/MarkLogic

注： 共有ドライブを指定する場合を除き、グループ内のすべてのホストにおいて、上記の指定ディレクトリ内にプログラムのコピーを保持する必要があります。

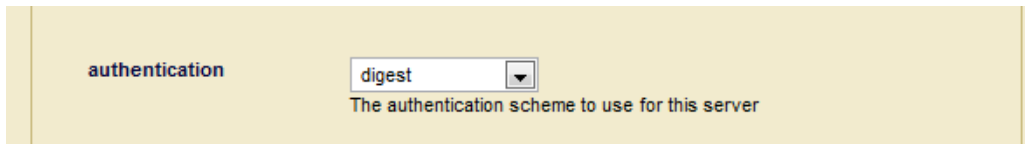
警告 Docs、Data、または Admin という名前の HTTP サーバールートディレクトリを作成しないでください。これらのディレクトリは、他の目的で MarkLogic サーバーによって予約されています。これらの名前で HTTP サーバールートディレクトリを作成すると、予期しないサーバー動作になる可能性があります。また、ソフトウェアのアップグレードが複雑になることもあります。

7. [Port] フィールドで、この HTTP サーバーを使用するためのポート番号を入力します。

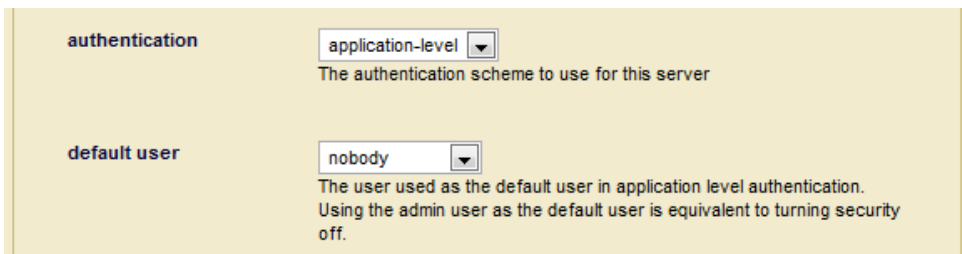
このポート番号は他の HTTP、ODBC、XDBC、WebDAV サーバーと重複しないようにしてください。

8. [Modules] フィールドで、ドキュメントの Modules データベースとして使用するデータベースを選択します。ファイルシステム上にモジュールを格納する場合はデフォルトのままにします。Modules データベースの詳細については、「Modules データベース」（107 ページ）を参照してください。
9. [Database] フィールドで、この HTTP サーバーがアクセスするデータベースを選択します。1 つのデータベースに対して、複数の HTTP、ODBC、XDBC、WebDAV サーバーがアクセスできます。

10. [Authentication] フィールドまでスクロールします。認証スキームとして `digest`、`basic`、`digestbasic`、または `application-level` を選択します。デフォルトは `digest` で、暗号化されたパスワードを使用します。



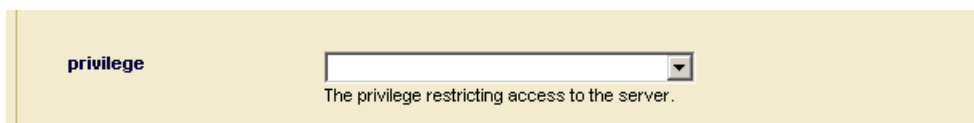
`application-level` 認証を選択した場合は、デフォルトユーザーも設定する必要があります。この場合、HTTP サーバーにログインすると自動的にこのデフォルトユーザーとなります（明示的に他のユーザーとしてログインした場合を除く）。



警告 管理者ユーザー（`admin`）をデフォルトユーザー（`admin` ロールを持つ承認済み管理者）として使用する場合、このアプリケーションサーバーを使用する全員が自動的に `admin` ロールを持つユーザーになり、このアプリケーションサーバーのセキュリティが実質的にオフになります。

11. 画面下部近くの [Privilege] フィールドまでスクロールします。このフィールドは、サーバーにアクセス（ログイン）するために必要な権限を表します。このフィールドは空白のままにしてもかまいません。

HTTP サーバーにアクセスするユーザーは、HTTP サーバーにアクセスするための実行権限が選択されている必要があります。前述の `application-level` 認証を選択した場合は、デフォルトユーザーが選択された権限を持っていることを確認する必要があります。



12. このアプリケーションサーバーの他のプロパティをニーズに合わせて設定します。

- [Last Login] および [Display Last Login] については、「最終ユーザーログイン試行の格納およびモニタリング」(103 ページ) を参照してください。
- [Address] は、アプリケーションサーバーの IP アドレスを指定します。
- [Backlog] は、HTTP サーバーソケットで許可される保留状態の接続の最大数を指定します。
- [Threads] は、アプリケーションサーバースレッドの最大数を指定します。
- [Request Timeout] は、ソケットが最初のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。
- [Keep Alive timeout] は、ソケットが同一接続上で後続のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。
- [Session Timeout] は、非アクティブなセッションがタイムアウトするまでの最大秒数を指定します。
- [Max Time Limit] は、リクエストの時間制限の上限を指定します。どのリクエストにも、この数値より大きな時間制限を（例えば `xdmp:set-request-time-limit` を使用して）設定できません。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
- [Default Time Limit] は、リクエストの制限時間が指定されていないときのデフォルト値を指定します。リクエストは、`xdmp:set-request-time-limit` を使用して時間制限を変更できます。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
- [Static Expires] は、静的コンテンツが指定された秒数後に期限切れになる「expires」HTTP ヘッダを追加します。
- [Pre-commit Trigger Limit] は、このアプリケーションサーバーに対するシングルステートメントが呼び出せるプリコミットトリガーの最大数を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。
- [Pre-commit Trigger Depth] は、このアプリケーションサーバーに対して実行されるプリコミットトリガーの最大深度（他のトリガーを発行できるようになるまでのトリガー数）を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。
- [Collation] は、このアプリケーションサーバーで実行されるクエリのデフォルトのコレーションを指定します。このコレーションは、クエリで指定されていない場合に文字列の比較およびソートに使用されます。詳細については、『*Search Developer's Guide*』の「[Encodings and Collations](#)」を参照してください。

- [Concurrent Request Limit] は、特定時点で任意のユーザーが実行している可能性のあるリクエストの最大数を指定します。0 は、最大数なしを表します。詳細については、「同時ユーザーセッション数の管理」(101 ページ)を参照してください。
- [Log Errors] は、このアプリケーションサーバーのキャッチされなかったエラーを ErrorLog.txt ファイルに記録するかどうかを指定します。アプリケーションサーバーで発生することのある例外を記録して後でデバッグに使用するとき便利です。
- [Debug Allow] は、このアプリケーションサーバーに対するリクエストをデバッグ (MarkLogic サーバーのデバッグ API を使用) のために停止できるようにするかどうかを指定します。
- [Profile Allow] は、このアプリケーションサーバーに対するリクエストをプロファイリング (MarkLogic サーバーのプロファイリング API を使用) のために停止できるようにするかどうかを指定します。詳細については、『*Query Performance and Tuning Guide*』の「[Profiling Requests to Evaluate Performance](#)」を参照してください。
- [Default XQuery Version] は、XQuery モジュールがこの言語バージョンを明示的に宣言する場合に、このアプリケーションサーバーのデフォルト XQuery 言語を指定します。
- [Multi Version Concurrency Control] は、最新のタイムスタンプの取得に関するクエリ動作の厳密度を指定します。これは、更新ステートメントではなくクエリステートメントのみに影響します。MarkLogic サーバーにおけるクエリおよびトランザクションの詳細については、『*Application Developer's Guide*』の「[Understanding Transactions in MarkLogic Server](#)」を参照してください。
- [Error Handler] および [URL Rewriter] フィールドについては、『*Application Developer's Guide*』の「[Controlling App Server Access, Output, and Errors](#)」を参照してください。
- SSL サポートに関連するプロパティについては、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

13. 上部または下部までスクロールして [ok] をクリックします。

これで HTTP サーバーが作成されます。HTTP サーバーの作成は「ホット」管理タスクなので変更はすぐに有効になります。ユーザーセッションの管理やログイン試行のトラッキングの詳細やセットアップ手順については、「ユーザーセッションの管理およびログイン試行のモニタリング」(101 ページ)を参照してください。

7.2.2 HTTP サーバーの出力オプションの設定

HTTP サーバーごとに、さまざまなデフォルト出力オプションを設定できます。出力オプションは、アプリケーションサーバーから返されるデータのシリアライズ方法に影響します。また、オプションをクエリレベルで設定することで、デフォルトオプションよりも優先させることができます。XQuery では `declare option XQuery` プロローグを使用し、XSLT では `<xsl:output>` 命令を使用して、アプリケーションサーバーのデフォルトよりも優先させるようなシリアライゼーションオプションを設定できます。XQuery でシリアライゼーションオプションを設定する方法の詳細については、『*XQuery and XSLT Reference Guide*』の「[Declaring Options](#)」を参照してください。XSLT 出力の詳細については、XSLT 仕様 (<http://www.w3.org/TR/xslt20#serialization>) を参照してください。

アプリケーションサーバーのデフォルトを指定するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 表示する HTTP サーバーが含まれるグループをクリックします (例えば Default)。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 編集するアプリケーションサーバーを選択します。
5. 左側のツリーメニューで [Output Options] を選択します。[Output Options Configuration] ページが表示されます。
6. このアプリケーションサーバーに関して制御するオプションを設定します。
7. [ok] をクリックして変更を保存します。

アプリケーションサーバーの出力の詳細については、『*Application Developer's Guide*』の「[Controlling App Server Access, Output, and Errors](#)」を参照してください。

7.2.3 HTTP サーバー設定の表示

特定の HTTP サーバーの設定を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 表示する HTTP サーバーが含まれるグループをクリックします (例えば Default)。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [Summary] タブで、設定を表示する HTTP サーバーを見つけます。
5. HTTP サーバーのアイコンをクリックします。
6. 設定を表示します。

7.2.4 HTTP サーバーの削除

HTTP サーバーの設定を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 削除する HTTP サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [Summary] タブで、削除する HTTP サーバーを見つけます。
5. HTTP サーバーのアイコンをクリックします。
6. [delete] をクリックします。
7. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

HTTP サーバーの削除は「コールド」管理タスクです。変更を反映するために、サーバーが再起動します。

7.2.5 リクエストのキャンセル

管理画面のアプリケーションサーバーの [Status] ページでリクエストをキャンセルできます（[Groups] > [グループ名] > [App Servers] > [アプリケーションサーバー名] > [Status] タブ）。

App Server Status

Summary Configure **Status** Create HTTP Create WebDAV Create XDBC Help

App Server: myAppServer[HTTP] [show less](#)

appserver status -- A detailed view of this appserver's activity.

App Server myAppServer [HTTP]
Database apidoc
Hosts raymond.marklogic.com

Host	Threads	Requests	Updates	Average Time	Request Rate	Oldest Request	Expanded Tree Cache		
							Hits	Misses	Ratio
raymond.marklogic.com	2	1	0	2.8 s	0.1	2.8 s	460224	34389	93%
	2	1	0	2.8 s	0.1	n/a	460224	34389	93%

Query	#	Average Time	Oldest Time	Expanded Tree Cache		Ratio
				Hits	Misses	
/cq-eval.xqy	1	2.8 s	2.8 s	0	0	n/a
Total	1	2.8 s	2.8 s	0	0	n/a

Host	Query	User	Client IP	Time	Expanded Tree Cache			
					Hits	Misses	Ratio	
raymond.marklogic.com	/cq-eval.xqy	admin	182.16.1.131	2.8 s	0	0	n/a	[cancel]
	Total				0	0	n/a	

実行時間が長いリクエスト（例えば実行時間が長いクエリステートメントや更新ステートメント）をキャンセルするには、次の手順を実行します。

1. 管理画面で、[Group] メニュー項目をクリックします。
2. ツリーメニューまたは [Summary] タブから、リクエストが発行されたアプリケーションサーバーに移動します。
3. [Status] タブをクリックします。
4. [show more] ボタンをクリックします。
5. アプリケーションサーバーの [Status] ページの右下で、キャンセルするクエリの行にある [cancel] ボタンをクリックします。
6. [Cancel Request] 確認ページで、[ok] をクリックします。確認ページが表示されたときにリクエストがすでに完了している場合は、リクエストが見つからないというメッセージがページに表示されます。

リクエストがキャンセルされ、アプリケーションサーバーの [Status] ページが再度表示されます。

8.0 XDBC サーバー

この章では、XDBC サーバーについて、および XDBC サーバーの設定手順について説明します。次のセクションで構成されています。

- [XDBC サーバーの概要](#)
- [XDBC サーバーを作成および管理する手順](#)

この章では、管理画面を使用して XDBC サーバーを作成および設定する方法について説明します。XDBC サーバーをプログラムによって作成および設定する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring App Servers](#)」を参照してください。

8.1 XDBC サーバーの概要

XDBC (XML Database Connector) サーバーはグループレベルで定義され、グループ内のすべてのホストからアクセスできます。各 XDBC サーバーは、特定のフォレスト、および指定されたディレクトリ構造内にある XQuery プログラムのライブラリ (ルート) へのアクセスを提供します。アプリケーションは、デフォルトでは XDBC サーバーに接続されているデータベースに対して実行されます。

XDBC サーバーを使うと、XCC (XML Contentbase Connector) アプリケーションと MarkLogic サーバー間の通信が可能になります。XCC は、Java ミドルウェアアプリケーションから MarkLogic サーバーへの通信に使用する API です。XDBC サーバーを使うと、旧式の XDBC アプリケーションと MarkLogic サーバー間の通信も可能ですが、XDBC アプリケーションは 3.1 以降のいくつかの機能 (ポイントインタイムクエリなど) を使用できません。XCC アプリケーションと XDBC アプリケーションの両方が同一のワイヤプロトコルを使用します。

XCC 経由でサブミットされる XQuery リクエストは、XQuery コードで指定されたとおりに結果を返します。これらの結果には、XML やその他のさまざまなデータ型を含めることができます。XCC アプリケーションは、提供されるさまざまなデータ型に適した方法で結果を解析、処理、および解釈します。このタスクを支援するために公開されているライブラリが多数ありますが、独自のコードを記述することも可能です。XCC 対応アプリケーションからの接続を受け入れるためには、XDBC サーバーが専用ポートでリスンする (接続を待ち受ける) ように MarkLogic サーバーを設定する必要があります。各 XDBC サーバーは、デフォルトで MarkLogic サーバー内の特定データベースに接続します。一方、XCC はアプリケーションが接続する (およびユーザーが必要なパーミッションや権限を持っている) MarkLogic サーバークラスタ内の任意のデータベースと通信できます。

XDBC サーバーは、HTTP および WebDAV サーバーと同様に、MarkLogic サーバーのセキュリティモデルに従います。サーバーは、これらのプログラムへのアクセスを認証するために、その XDBC サーバー用のセキュリティデータベースに格納されているユーザー ID およびパスワードを使用します（各 XDBC サーバーはデータベースに接続され、各データベースはユーザーなどのセキュリティオブジェクトが格納されているセキュリティデータベースに接続されています）。

システムやデータへのきめ細かなアクセス制御は、権限およびパーミッションを使用して実現されます。MarkLogic サーバーのセキュリティオブジェクトを設定する方法の詳細については、「セキュリティ管理」（308 ページ）を参照してください。MarkLogic サーバーセキュリティモデルの概念については、『*Security Guide*』を参照してください。

8.2 XDBC サーバーを作成および管理する手順

XDBC サーバーを作成および管理するには、次の手順を実行します。

- [新しい XDBC サーバーの作成](#)
- [XDBC サーバーの出力オプションの設定](#)
- [XDBC サーバー設定の表示](#)
- [XDBC サーバーの削除](#)

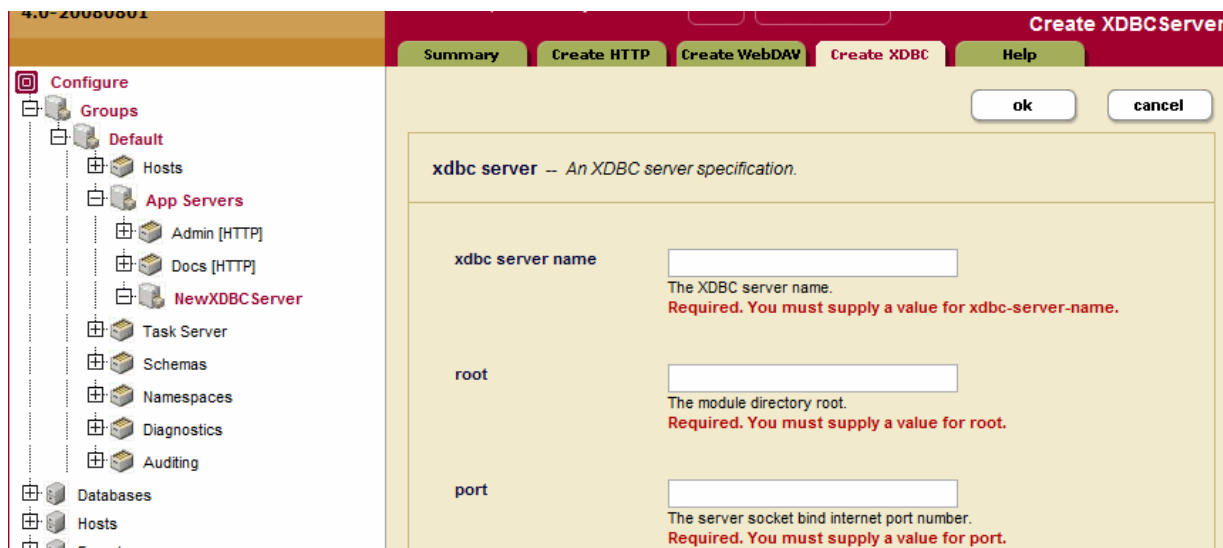
XDBC サーバーで実行中のリクエストをキャンセルする手順については、「リクエストのキャンセル」（55 ページ）を参照してください。

8.2.1 新しい XDBC サーバーの作成

新しいサーバーを作成するには、次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. XDBC サーバーを定義するグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。

4. 右上の [Create XDBC] タブをクリックします。[Create XDBC Server] ページが表示されます。



5. [XDBC Server Name] フィールドで、この XDBC サーバーの短い名前を入力します。MarkLogic サーバーでは、管理画面でこのサーバーを参照する際にこの名前を使用します。
6. [root] ディレクトリフィールドで、XQuery プログラムを格納するディレクトリの名前を入力します。[modules] フィールドでデータベースを指定している場合、ルートは指定された Modules データベース内のディレクトリ URI である必要があります。

[modules] フィールドでファイルシステムを指定している場合、ルートディレクトリは完全修飾パス名であるか、MarkLogic サーバーがインストールされているディレクトリからの相対パスとなります。プラットフォーム別のデフォルトのインストールディレクトリを次の表に示します。

プラットフォーム	プログラムディレクトリ
Microsoft Windows	C:\Program Files\MarkLogic
Red Hat Linux	/opt/MarkLogic
Mac OS X	~/Library/MarkLogic

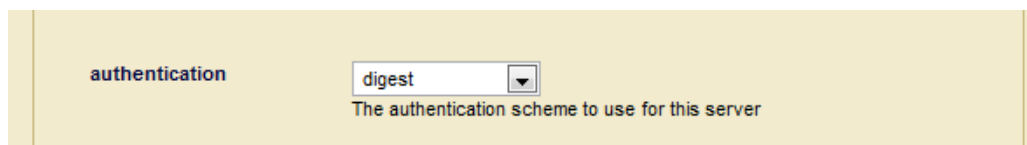
注： 共有ドライブを指定する場合を除き、グループ内のすべてのホストにおいて、上記の指定ディレクトリ内に XQuery プログラムのコピーを保持する必要があります。

警告 Docs、Data、または Admin という名前の XDBC サーバールートディレクトリを作成しないでください。これらのディレクトリは、他の目的で MarkLogic サーバーによって予約されています。これらの名前で XDBC サーバールートディレクトリを作成すると、予期しないサーバー動作になる可能性があります。また、ソフトウェアのアップグレードが複雑になることもあります。

7. [Port] フィールドで、この XDBC サーバーを使用するためのポート番号を入力します。

このポート番号は他の XDBC、HTTP、WebDAV サーバーと重複しないようにしてください。

8. [Modules] フィールドで、XQuery ドキュメントの Modules データベースとして使用するデータベースを選択します。ファイルシステム上に XQuery モジュールを格納する場合はデフォルトのままにします。Modules データベースの詳細については、「Modules データベース」(107 ページ) を参照してください。
9. [Database] フィールドで、この XDBC サーバーがアクセスするデータベースを選択します。1 つのデータベースに対して、複数の HTTP、XDBC、WebDAV サーバーがアクセスできます。
10. [Authentication] フィールドまでスクロールします。認証スキームとして digest、basic、または digestbasic を選択します。デフォルトは digest で、暗号化されたパスワードを使用します。



11. 画面下部近くの [Privilege] フィールドまでスクロールします。このフィールドは、サーバーにアクセス（ログイン）するために必要な権限を表します。このフィールドは空白のままにしてもかまいません。

XDBC サーバーにアクセスするユーザーは、XDBC サーバーにアクセスするための実行権限が選択されている（または `admin` ロールを持つメンバーである）必要があります。



12. このアプリケーションサーバーの他のプロパティをニーズに合わせて設定します。

- [Last Login] および [Display Last Login] については、「最終ユーザーログイン試行の格納およびモニタリング」(103 ページ) を参照してください。
- [Address] は、アプリケーションサーバーの IP アドレスを指定します。
- [Backlog] は、HTTP サーバーソケットで許可される保留状態の接続の最大数を指定します。
- [Threads] は、アプリケーションサーバースレッドの最大数を指定します。
- [Request Timeout] は、ソケットが最初のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。
- [Keep Alive Timeout] は、ソケットが同一接続上で後続のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。
- [Session Timeout] は、非アクティブなセッションがタイムアウトするまでの最大秒数を指定します。
- [Max Time Limit] は、リクエストの時間制限の上限を指定します。どのリクエストにも、この数値より大きな時間制限を（例えば `xdmp:set-request-time-limit` を使用して）設定できません。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
- [Default Time Limit] は、リクエストの制限時間が指定されていないときのデフォルト値を指定します。リクエストは、`xdmp:set-request-time-limit` を使用して時間制限を変更できます。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
- [Pre-commit Trigger Limit] は、このアプリケーションサーバーに対するシングルステートメントが呼び出せるプリコミットトリガーの最大数を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。
- [Pre-commit Trigger Depth] は、このアプリケーションサーバーに対して実行されるプリコミットトリガーの最大深度（他のトリガーを発行できるようになるまでのトリガー数）を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。
- [Collation] は、このアプリケーションサーバーで実行されるクエリのデフォルトのコレーションを指定します。このコレーションは、クエリで指定されていない場合に文字列の比較およびソートに使用されます。詳細については、『*Search Developer's Guide*』の「[Encodings and Collations](#)」を参照してください。

- [Concurrent Request Limit] は、特定時点で任意のユーザーが実行している可能性のあるリクエストの最大数を指定します。0 は、最大数なしを表します。詳細については、「同時ユーザーセッション数の管理」(101 ページ) を参照してください。
- [Log Errors] は、このアプリケーションサーバーのキャッチされなかったエラーを ErrorLog.txt ファイルに記録するかどうかを指定します。アプリケーションサーバーで発生することのある例外を記録して後でデバッグに使用するとき便利です。
- [Debug Allow] は、このアプリケーションサーバーに対するリクエストをデバッグ (MarkLogic サーバーのデバッグ API を使用) のために停止できるようにするかどうかを指定します。
- [Profile Allow] は、このアプリケーションサーバーに対するリクエストをプロファイリング (MarkLogic サーバーのプロファイリング API を使用) のために停止できるようにするかどうかを指定します。詳細については、『*Query Performance and Tuning Guide*』の「[Profiling Requests to Evaluate Performance](#)」を参照してください。
- [Default XQuery Version] は、XQuery モジュールがこの言語バージョンを明示的に宣言する場合に、このアプリケーションサーバーのデフォルト XQuery 言語を指定します。
- [Multi Version Concurrency Control] は、最新のタイムスタンプの取得に関するクエリ動作の厳密度を指定します。これは、更新ステートメントではなくクエリステートメントのみに影響します。MarkLogic サーバーにおけるクエリおよびトランザクションの詳細については、『*Application Developer's Guide*』の「[Understanding Transactions in MarkLogic Server](#)」を参照してください。
- SSL サポートに関連するプロパティについては、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

13. 上部または下部までスクロールして [ok] をクリックします。

新しい XDBC サーバーが作成されます。XDBC サーバーの作成は「ホット」管理タスクなので変更はすぐに有効になります。ユーザーセッションの管理やログイン試行のトラッキングの詳細やセットアップ手順については、「ユーザーセッションの管理およびログイン試行のモニタリング」(101 ページ) を参照してください。

8.2.2 XDBC サーバーの出力オプションの設定

XDBC サーバーごとに、さまざまなデフォルト出力オプションを設定できます。出力オプションは、アプリケーションサーバーから返されるデータのシリアライズ方法に影響します。また、オプションをクエリレベルで設定することで、デフォルトオプションよりも優先させることができます。XQuery では `declare option XQuery` プロローグを使用し、XSLT では `<xsl:output>` 命令を使用して、アプリケーションサーバーのデフォルトよりも優先させるようなシリアライゼーションオプションを設定できます。XQuery でシリアライゼーションオプションを設定する方法の詳細については、『*XQuery and XSLT Reference Guide*』の「[Declaring Options](#)」を参照してください。XSLT 出力の詳細については、XSLT 仕様 (<http://www.w3.org/TR/xslt20#serialization>) を参照してください。

アプリケーションサーバーのデフォルトを指定するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 表示する XDBC サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 編集するアプリケーションサーバーを選択します。
5. 左側のツリーメニューで [Output Options] を選択します。[Output Options Configuration] ページが表示されます。
6. このアプリケーションサーバーに関して制御するオプションを設定します。
7. [ok] をクリックして変更を保存します。

アプリケーションサーバーの出力の詳細については、『*Application Developer's Guide*』の「[Controlling App Server Access, Output, and Errors](#)」を参照してください。

8.2.3 XDBC サーバー設定の表示

XDBC サーバーの設定を表示するには、次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. 表示する XDBC サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [Summary] タブで、設定を表示する XDBC サーバーを見つけます。
5. XDBC サーバーのアイコンをクリックします。
6. 設定を表示します。

8.2.4 XDBC サーバーの削除

XDBC サーバーの設定を削除するには、次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. 削除する XDBC サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [Summary] タブで、削除する XDBC サーバーを見つけます。
5. この XDBC サーバーのアイコンをクリックします。
6. [Drop] をクリックします。
7. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

XDBC サーバーの削除は「コールド」管理タスクです。変更を反映するために、サーバーが再起動します。

9.0 WebDAV サーバー

MarkLogic サーバーにおける WebDAV サーバーは、HTTP サーバーに似ていますが、次のような重要な相違点があります。

- WebDAV サーバーは、XQuery コードを実行できません。
- WebDAV サーバーは、セキュリティ設定に応じて WebDAV クライアントがデータベースへの読み取りおよび書き込みアクセスを許可する WebDAV プロトコルをサポートします。
- WebDAV サーバーは、データベース内のドキュメントやディレクトリにのみアクセスします。ファイルシステムには直接アクセスしません。

この章では、次の各セクションで MarkLogic サーバーの WebDAV サーバーについて説明します。

- [WebDAV サーバーの概要](#)
- [WebDAV サーバーを作成および管理する手順](#)
- [WebDAV クライアント](#)
- [例：別のサーバーで使用されるドキュメントを追加 / 修正するために WebDAV サーバーをセットアップする](#)

この章では、管理画面を使用して WebDAV サーバーを作成および設定する方法について説明します。WebDAV サーバーをプログラムによって作成および設定する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring App Servers](#)」を参照してください。

9.1 WebDAV サーバーの概要

WebDAV (Web-based Distributed Authoring and Versioning) は、HTTP プロトコルを拡張したプロトコルであり、HTTP 拡張機能によるドキュメントの書き込みを可能にします。ドキュメントの書き込みには WebDAV クライアントが必要ですが、読み取りは Web ブラウザなどを使用して HTTP を介して行うことができます。MarkLogic サーバーでサポートされている WebDAV クライアントについては、「WebDAV クライアント」(75 ページ) を参照してください。WebDAV および WebDAV プロトコルの概要については、次の Web サイトを参照してください。

<http://webdav.org>

このセクションでは、MarkLogic サーバーの WebDAV サーバーの概要について説明します。この章は、次のトピックで構成されています。

- [XQuery を実行しないデータベースへの読み取り / 書き込みアクセス](#)
- [WebDAV サーバーのセキュリティ](#)
- [ディレクトリ](#)
- [サーバーのルートディレクトリ](#)
- [WebDAV サーバー内のドキュメント](#)

9.1.1 XQuery を実行しないデータベースへの読み取り / 書き込みアクセス

MarkLogic サーバーでは、WebDAV サーバーはグループレベルで定義され、グループ内のすべてのホストに適用されます。各 WebDAV サーバーは、必要なセキュリティパーミッションに応じて、単一のデータベースへの読み取り / 書き込みアクセスを提供します。ドキュメントが WebDAV 経由で読み取りまたは書き込みされると、その関連データ（プロパティ、メタデータ、コレクションなど）もすべてドキュメントとともに移動します。

管理画面で、データベースにアクセスするように WebDAV サーバーを設定します。そのデータベースに格納されているドキュメントは、HTTP 経由で読み取りアクセスが可能です。また、WebDAV クライアント経由でデータベースにアクセスして、ドキュメントを読み取り、修正、削除、および追加することもできます。ドラッグアンドドロップなどにより WebDAV クライアント経由でドキュメントを追加すると、実際にはデータベースにドキュメントを直接読み込むこととなります。

WebDAV サーバー経由でデータベースにアクセスしたときは、XQuery コードを実行できません。HTTP サーバーとは異なり、WebDAV サーバー用の Modules データベースはありません。ただし、データベースを HTTP、ODBC、または XDBC サーバーの Modules データベースとして設定でき、そのデータベースを WebDAV サーバーからのアクセス用に設定できます。その後、HTTP、ODBC、または XDBC サーバーから実行するコードを WebDAV サーバーから編集できます。この設定の例については、「例：別のサーバーで使用されるドキュメントを追加 / 修正するために WebDAV サーバーをセットアップする」（79 ページ）を参照してください。

9.1.2 WebDAV サーバーのセキュリティ

WebDAV サーバーは、HTTP、ODBC、および XDBC サーバーと同様に、MarkLogic サーバーのセキュリティモデルに従います。WebDAV サーバーは、そのサーバー用のセキュリティデータベースに格納されているユーザー ID およびパスワードを使用してユーザーを認証します。また、WebDAV サーバーは、権限およびロールを使用して、データベース内のオブジェクトへのアクセスを制御します（各 WebDAV サーバーはデータベースに接続され、各データベースはユーザーなどのセキュリティオブジェクトが格納されているセキュリティデータベースに接続されています）。

WebDAV サーバーにアクセスする全員がパスワードなしで同じユーザーとしてログインできるようにする場合は、application-level セキュリティを設定できます。例えば全員が読み取りと書き込みの両方の権限を持ち、事前に定義されたデフォルトの権限セットを持つ「ゲスト」としてログインできるようにしたいとします。この場合、この認証スキームを application-level に設定し、デフォルトユーザーを「guest」に設定します。

注： WebDAV サーバーにおいてデータベースへの書き込みパーミッションを持つユーザーは WebDAV クライアント経由でデータベースにドキュメントを読み込むことができます。このためこのユーザーが WebDAV フォルダにファイルをドラッグアンドドロップするなどして読み込んだドキュメントに、他のユーザーが読み取り / 書き込みを行えるパーミッションがあるように、そのようなユーザーには適切なデフォルトパーミッションを設定してください（セキュリティポリシーに基づいて設定します）。システムやデータへのそのようなきめ細かなアクセス制御は、権限およびパーミッションを使用して実現できます。MarkLogic サーバーでセキュリティ機能を使用する方法についての詳細は、「セキュリティ管理」（308 ページ）、および『*Application Developer's Guide*』のセキュリティ関連の章を参照してください。

9.1.3 ディレクトリ

WebDAV ディレクトリは、ファイルシステムディレクトリに該当します。ディレクトリは、そのディレクトリ内のドキュメントを WebDAV クライアント経由で表示するために必要です（ファイルシステムの場合と同様に、ディレクトリ内のファイルにアクセスするためには、そのディレクトリに移動する必要があります）。ディレクトリ内の各ドキュメントには、ディレクトリ URI をプレフィックスとして含む URI があります。また、WebDAV サーバーで認識される各ディレクトリにはプレフィックスとして WebDAV ルートが必要であり、データベースには WebDAV ルートを持つディレクトリが存在する必要があります。

例えば `http://marklogic.com/` という WebDAV ルートがあるとします。この場合、ドキュメントやディレクトリが WebDAV クライアントで認識されるためには、必ず URI がそのルートで始まる必要があります。また、URI が `http://marklogic.com/` のディレクトリがデータベース内に存在する必要があります。このため、URI が `http://marklogic.com/file.xml` のドキュメントはこの WebDAV サーバーで認識されます。また、URI が `http://marklogic.com/dir/` のディレクトリも認識されます。一方、URI が `/dir/` のディレクトリ、および URI が `/dir/file.xml` のドキュメントは、このサーバーで認識されません。これは URI が WebDAV ルートで始まらないためです。

以下のセクションでは、ディレクトリの詳細について説明します。

- [データベース設定でのディレクトリの自動作成](#)
- [ディレクトリのプロパティおよび URI](#)

ディレクトリおよびプロパティの詳細については、『*Application Developer's Guide*』の「プロパティドキュメントとディレクトリ」の章を参照してください。

9.1.3.1 データベース設定でのディレクトリの自動作成

管理画面のデータベース設定部分には、ディレクトリ作成の設定があります。ディレクトリ作成の設定では、ドキュメントを作成するときにディレクトリが自動的に作成されるかどうかを指定します。

WebDAV サーバーを使用してドキュメントをデータベースに読み込む場合は、管理画面を使用して、データベースのディレクトリ作成設定を `automatic` に設定することをお勧めします。ディレクトリ作成が `automatic` に設定されているデータベースにアクセスする WebDAV サーバーを作成すると、WebDAV クライアント経由でデータベースにアクセスするために必要なルートディレクトリが自動的に作成されます。自動的なディレクトリ作成は、データベース内に存在しないディレクトリ階層が URI に含まれるドキュメントを手動で（例えば `xdmp:document-load` 関数を使用して）読み込む場合にも便利です。ディレクトリ作成が `automatic` に設定されている場合は、URI で示されるディレクトリが自動的に作成されます。

また、XQuery の `xdmp:directory-create` および `xdmp:directory-delete` ビルトイン関数を使用して、ディレクトリを手動で作成および削除することもできます。

すべてのディレクトリ作成設定の詳細については、「基本的な管理設定」（109 ページ）を参照してください。

9.1.3.2 ディレクトリのプロパティおよび URI

ディレクトリは、プロパティドキュメントとして MarkLogic サーバーデータベースに格納されます。ドキュメントと同様に、ディレクトリには URI があります。ただし、URI の末尾はスラッシュ (/) である必要があります。 `xdmp:document-properties("uri_name")` 関数を使用してある URI のプロパティドキュメントを取得したり、 `xdmp:document-properties()` 関数を使用してデータベース内のすべてのプロパティドキュメントを取得できます。

プロパティは、`http://marklogic.com/xdmp/property` 名前空間内にあります。自動、手動いずれの場合でも、ディレクトリを作成するときは、データベース内に子要素 `directory` を持つプロパティドキュメントが作成されます。例えばデータベース内に `URI /myCompany/marketing/` を持つディレクトリがある場合、次のクエリによって次の結果が返されます。

```
xdmp:document-properties("/myServer/Marketing/")
=>
<prop:properties xmlns:prop="http://marklogic.com/xdmp/property">
  <prop:directory/>
</prop:properties>
```

返されるプロパティドキュメントには、ディレクトリの URI が含まれず、ディレクトリの存在を示す空要素 (`prop:directory`) だけが含まれます。

`xdmp:document-properties()` 関数は、データベース内にあるすべてのドキュメントのプロパティドキュメントを返します。プロパティドキュメント内にディレクトリ要素が存在する場合、データベース内にディレクトリが存在し、その要素で XQuery `xdmp:node-uri` ビルトイン関数を呼び出すと、そのディレクトリの URI が返されます。例えば次のクエリは、データベース内にあるすべてのディレクトリの URI を返します。

```
declare namespace prop="http://marklogic.com/xdmp/property"

for $x in xdmp:document-properties()/prop:properties/prop:directory
return <directory-uri>{xdmp:node-uri($x)}</directory-uri>
```

注： 末尾がスラッシュ (/) である URI を持つドキュメントを作成することは可能ですが、この場合、ディレクトリの URI と区別できなくなります。このため URI の末尾がスラッシュであるドキュメントは作成しないことをお勧めします。

9.1.4 サーバーのルートディレクトリ

各 WebDAV サーバーには、「ルート」という概念があります。ルートはサーバーからアクセスできる最上位のディレクトリです。ユーザーは、データベース内にあるこのルートの子であるあらゆるドキュメントやディレクトリにアクセスできます。そのため、ルートは WebDAV サーバーからアクセスできるすべてのドキュメントおよびディレクトリの URI のプレフィックスとして機能します。WebDAV のルートは管理画面から入力できます。ルートとしては、有効な URI であれば任意のものを指定できますが、常に末尾がスラッシュ (/) である必要があります。スラッシュがない場合は、入力した文字列にスラッシュが追加されます。

ルートは、ディレクトリ構造の最上位として機能できる一意の文字列にする必要があります。`http://<会社のドメイン名>/` という形式の WebDAV ルートを使用することが一般的ですが、必須ではありません。WebDAV ルートの例を次に示します。

```
http://myCompany/marketing/

/myCompany/marketing/
```

注： ディレクトリの末尾を 2 つのスラッシュ (//) にすることはできません。そのため、URI が `http://` であるディレクトリは作成できません。WebDAV サーバーにルート `http://myCompany` を指定し、データベースで `directory creation` が `automatic` に設定されている場合、URI `http://myCompany/` のディレクトリがデータベース内に自動的に作成されます。

ドキュメントを WebDAV サーバー経由でアクセス可能にするためには、ドキュメントに何らかのルートで始まる URI を付ける必要があります。また、WebDAV クライアント経由で作成されたドキュメント (Web フォルダにドラッグアンドドロップするなどして) には、読み込み時に WebDAV ルートで始まる URI が付けられます。

例えば URI が `/myCompany/marketing/strategy.doc` のドキュメントにはルートの `/myCompany/marketing/` があるので、WebDAV サーバー経由でアクセスできます（必要なセキュリティパーミッションがある場合）。またドキュメント `strategy.doc` を前述のように WebDAV サーバーへのアクセスが設定された Web フォルダへドラッグすると、このドキュメントが作成されます。

注： WebDAV クライアントが WebDAV サーバーにアクセスした際にデータベース内に WebDAV ルートディレクトリが存在しない場合、データベースの `directory creation` が `automatic` に設定されていればルートディレクトリが自動作成されます。ディレクトリはパーミッションなしで作成されるため、`admin` ロールを持つユーザーのみが読み取り可能です。他のユーザーが WebDAV サーバーを使用できるようにするには、`xdmp:document-add-permissions` などを使用してそのディレクトリに適切な読み取りパーミッションを追加する必要があります。ドキュメントおよびディレクトリのパーミッションの詳細については、『*Security Guide*』を参照してください。

9.1.5 WebDAV サーバー内のドキュメント

WebDAV サーバーの主な目的は、ユーザーがデータベースでドキュメントを簡単に格納、取得、および修正できるようにすることです。ドキュメントの種類は問いません。テキストドキュメント（`.txt` ファイルやソースコードなど）、バイナリドキュメント（画像ファイルなど）、Microsoft Word ファイル、XML ドキュメントでもかまいません。これらのドキュメントがデータベースに格納されているため、ドキュメントのコンテンツを使用するアプリケーションをあらゆる必要に応じて作成できます。また、データベースのバックアップおよびリストア機能を使用して、データベースのコンテンツを簡単にバックアップできます。

9.2 WebDAV サーバーを作成および管理する手順

このセクションでは、次の操作を実行する手順について説明します。

- [新しい WebDAV サーバーの作成](#)
- [WebDAV サーバーの出力オプションの設定](#)
- [WebDAV サーバー設定の表示](#)
- [WebDAV サーバーの削除](#)

WebDAV サーバーで実行中のリクエストをキャンセルする手順については、「リクエストのキャンセル」（55 ページ）を参照してください。

9.2.1 新しい WebDAV サーバーの作成

新しいサーバーを作成するには、次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. WebDAV サーバーを定義するグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 右上の [Create WebDAV] タブをクリックします。

[WebDAV Server Create] ページが表示されます。

5. [WebDAV Server Name] フィールドで、この WebDAV サーバーの短い名前を入力します。

MarkLogic サーバーは、管理画面やユーザーインターフェイスでこのサーバーを参照する際にこの名前を使用します。

6. [root] フィールドに、WebDAV ルートの名前を入力します。このルートは、WebDAV URI 階層の最上位を表す文字列です。この WebDAV サーバー経由でアクセスできるすべてのドキュメントは、URI がこのルート文字列で始まる必要があります。ルートの詳細については、「サーバーのルートディレクトリ」（68 ページ）を参照してください。

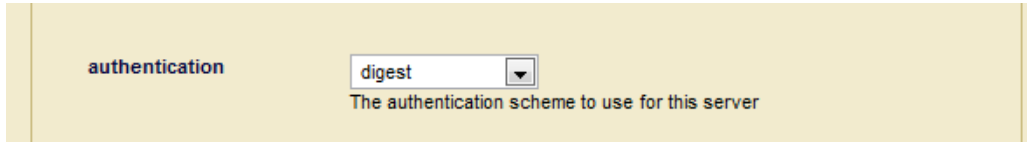
ルートディレクトリにスラッシュが含まれない場合は、スラッシュが自動的に追加されます。

7. [Port] フィールドで、この WebDAV サーバーを使用するためのポート番号を入力します。このポート番号は他のサーバーと重複しないようにしてください。
8. [database] フィールドで、この WebDAV サーバーがアクセスするデータベースを選択します。

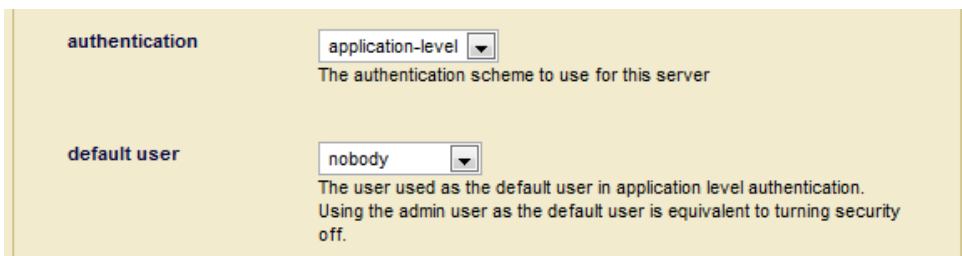
1 つのデータベースに対して、複数の HTTP、ODBC、XDBC、WebDAV サーバーを接続できます。

注： WebDAV サーバーでデータベースを使用する場合は、そのデータベースの directory creation 設定を `automatic` に設定してください。これによりデータベースにドキュメントが追加された際に、ルートディレクトリやその他のディレクトリが自動的に作成されます（ディレクトリが存在しない場合）。ディレクトリの詳細については、「ディレクトリ」（66 ページ）を参照してください。

9. [Authentication] フィールドまでスクロールします。認証スキームとして `digest`、`basic`、`digestbasic`、または `application-level` を選択します。デフォルトは `digest` で、暗号化されたパスワードを使用します。



`application-level` 認証を選択した場合は、デフォルトユーザーも設定する必要があります。この場合、アプリケーションサーバーにログインすると自動的にこのデフォルトユーザーとなります（明示的に他のユーザーとしてログインした場合を除く）。



警告 管理者ユーザー（`admin`）をデフォルトユーザー（`admin` ロールを持つ承認済み管理者）として使用する場合、このアプリケーションサーバーを使用する全員が自動的に `admin` ロールを持つユーザーになり、このアプリケーションサーバーのセキュリティが実質的にオフになります。

10. 画面下部近くの [Privilege] フィールドまでスクロールします。このフィールドは、サーバーにアクセス（ログイン）するために必要な権限を表します。このフィールドは空白のままにしてもかまいません。
11. このアプリケーションサーバーの他のプロパティをニーズに合わせて設定します。
- [Last Login] および [Display Last Login] については、「最終ユーザーログイン試行の格納およびモニタリング」（103 ページ）を参照してください。
 - [Address] は、アプリケーションサーバーの IP アドレスを指定します。
 - [Backlog] は、HTTP サーバーソケットで許可される保留状態の接続の最大数を指定します。
 - [Threads] は、アプリケーションサーバースレッドの最大数を指定します。
 - [Request Timeout] は、ソケットが最初のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。

- [Keep Alive timeout] は、ソケットが同一接続上で後続のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。
- [Session Timeout] は、非アクティブなセッションがタイムアウトするまでの最大秒数を指定します。
- [Max Time Limit] は、リクエストの時間制限の上限を指定します。どのリクエストにも、この数値より大きな時間制限を（例えば `xdmp:set-request-time-limit` を使用して）設定できません。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
- [Default Time Limit] は、リクエストの制限時間が指定されていないときのデフォルト値を指定します。リクエストは、`xdmp:set-request-time-limit` を使用して時間制限を変更できます。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
- [Static Expires] は、静的コンテンツが指定された秒数後に期限切れになる「expires」HTTP ヘッダを追加します。
- [Pre-commit Trigger Limit] は、このアプリケーションサーバーに対するシングルステートメントが呼び出せるプリコミットトリガーの最大数を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。
- [Pre-commit Trigger Depth] は、このアプリケーションサーバーに対して実行されるプリコミットトリガーの最大深度（他のトリガーを発行できるようになるまでのトリガー数）を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。
- [Collation] は、このアプリケーションサーバーで実行されるクエリのデフォルトのコレーションを指定します。このコレーションは、クエリで指定されていない場合に文字列の比較およびソートに使用されます。詳細については、『*Search Developer's Guide*』の「[Encodings and Collations](#)」を参照してください。
- [Concurrent Request Limit] は、特定時点で任意のユーザーが実行している可能性のあるリクエストの最大数を指定します。0 は、最大数なしを表します。詳細については、「同時ユーザーセッション数の管理」（101 ページ）を参照してください。
- [Log Errors] は、このアプリケーションサーバーのキャッチされなかったエラーを `ErrorLog.txt` ファイルに記録するかどうかを指定します。アプリケーションサーバーで発生することのある例外を記録して後でデバッグに使用するとき便利です。

- [Debug Allow] は、このアプリケーションサーバーに対するリクエストをデバッグ（MarkLogic サーバーのデバッグ API を使用）のために停止できるようにするかどうかを指定します。
- [Profile Allow] は、このアプリケーションサーバーに対するリクエストをプロファイリング（MarkLogic サーバーのプロファイリング API を使用）のために停止できるようにするかどうかを指定します。詳細については、『*Query Performance and Tuning Guide*』の「[Profiling Requests to Evaluate Performance](#)」を参照してください。
- [Default XQuery Version] は、XQuery モジュールがこの言語バージョンを明示的に宣言する場合に、このアプリケーションサーバーのデフォルト XQuery 言語を指定します。
- [Multi Version Concurrency Control] は、最新のタイムスタンプの取得に関するクエリ動作の厳密度を指定します。これは、更新ステートメントではなくクエリステートメントのみに影響します。MarkLogic サーバーにおけるクエリおよびトランザクションの詳細については、『*Application Developer's Guide*』の「[Understanding Transactions in MarkLogic Server](#)」を参照してください。
- SSL サポートに関連するプロパティについては、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

12. 上部または下部までスクロールして [ok] をクリックします。

新しい WebDAV サーバーが追加されます。WebDAV サーバーの追加は「ホット」管理タスクです。

9.2.2 WebDAV サーバーの出力オプションの設定

WebDAV サーバーごとに、さまざまなデフォルト出力オプションを設定できます。出力オプションは、アプリケーションサーバーから返されるデータのシリアル化方法に影響します。また、オプションをクエリレベルで設定することで、デフォルトオプションよりも優先させることができます。XQuery では `declare option XQuery` プロローグを使用し、XSLT では `<xsl:output>` 命令を使用して、アプリケーションサーバーのデフォルトよりも優先させるようなシリアル化オプションを設定できます。XQuery でシリアル化オプションを設定する方法の詳細については、『*XQuery and XSLT Reference Guide*』の「[Declaring Options](#)」を参照してください。XSLT 出力の詳細については、XSLT 仕様（<http://www.w3.org/TR/xslt20#serialization>）を参照してください。

アプリケーションサーバーのデフォルトを指定するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 表示する WebDAV サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 編集するアプリケーションサーバーを選択します。
5. 左側のツリーメニューで [Output Options] を選択します。[Output Options Configuration] ページが表示されます。
6. このアプリケーションサーバーに関して制御するオプションを設定します。
7. [ok] をクリックして変更を保存します。

アプリケーションサーバーの出力の詳細については、『*Application Developer's Guide*』の「[Controlling App Server Access, Output, and Errors](#)」を参照してください。

9.2.3 WebDAV サーバー設定の表示

WebDAV サーバーの設定を表示するには、次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. 表示する WebDAV サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [Summary] タブで、設定を表示する WebDAV サーバーを見つけます。
5. この WebDAV サーバーのアイコンをクリックします。
6. 設定を表示します。

9.2.4 WebDAV サーバーの削除

WebDAV サーバーの設定を削除するには、次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. 削除する WebDAV サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [WebDAVServers] アイコンをクリックします。
4. 右上の [Configure] タブをクリックします。
5. ツリーメニューまたは [Summary] タブで、削除する WebDAV サーバーを見つけます。
6. この WebDAV サーバーのアイコンをクリックします。
7. [delete] をクリックします。
8. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

WebDAV サーバーの削除は「コールド」管理タスクです。変更を反映するために、サーバーが再起動します。

9.3 WebDAV クライアント

WebDAV クライアントを使用すると、WebDAV サーバーにログインして、ドキュメントを読み取り、修正、挿入、追加、削除できます。このセクションでは、MarkLogic サーバーでサポートされている WebDAV クライアントを示し、一般のおよび特定の手順をいくつか説明します。次のトピックから構成されています。

- [テスト済みの WebDAV クライアント](#)
- [サーバーに接続する一般的な手順](#)
- [Windows エクスプローラーで Web フォルダに接続する手順](#)

9.3.1 テスト済みの WebDAV クライアント

MarkLogic サーバーでテスト済みの WebDAV クライアントを次の表に示します。

WebDAV クライアント	入手先	注
Windows エクスプローラー	Windows XP、Windows Vista、Windows 7 の一部であり、構成の種類は多数存在	Windows からのドラッグアンドドロップが可能です。セットアップの手順については、「Windows エクスプローラーで Web フォルダに接続する手順」(78 ページ)を参照してください。一部の Windows クライアント (例えば大半の構成の Windows Vista および Windows 7 クライアント) では、Digest 認証が必要です。
PerlDAV	http://www.webdav.org/perl原因/	perl ベースのコマンドライン WebDAV クライアント。スクリプトを作成できるように、また個々の WebDAV 呼び出しを送信できるように設計されています。
XML Spy	Altova Software (http://www.altova.com/)	XML Spy で XML ファイルを開いたり、編集や保存ができます。XML Spy の [File] > [Open URL] メニュー項目を使用します。
jEdit DAV プラグイン	developer.marklogic.com から入手可能	jEdit 4.2 でデータベースドキュメントを表示および編集できます。このバージョンは developer.marklogic.com から入手できます。

これらのクライアントの詳細については、各製品に付属のドキュメントを参照してください。

注： WebDAV 内 (および MarkLogic サーバーデータベース内) のディレクトリおよびドキュメントの名前では大文字と小文字が区別されますが、一部の WebDAV クライアント (Windows エクスプローラーなど) では大文字と小文字が区別されません。Windows 自体は大文字と小文字を識別しますが、NewFolder という名前のディレクトリは newFolder という名前のディレクトリと同一ディレクトリとして扱われます。そのため、大文字と小文字だけが異なるディレクトリ名やドキュメント名は、Windows エクスプローラーなどの大文字と小文字が区別されない WebDAV クライアントを使用するときに混乱を招くおそれがあります。可能な場合は、大文字と小文字だけが異なる名前 (NewFolder と newFolder など) をディレクトリやドキュメントに割り当てないでください。

注： Windows Vista および Windows 7 WebDAV クライアントでは、最初のドキュメント作成時に2つのトランザクションが生じます。1つ目はゼロ長の WebDAV PUT であり、新しいゼロ長ドキュメントが作成されます。2つ目はこのゼロ長ドキュメントに対する更新です。CPF（またはトリガーを使用するその他のアプリケーション）を使用する場合、これによって作成トリガー（最初のゼロ長ドキュメントが作成される時）と更新トリガー（ドキュメントがコンテンツで更新される時）の両方が発行されます。Vista または Windows 7 WebDAV クライアントと CPF アプリケーションを使用する場合は、このような動作に対して作成および更新の CPF アクションが適切に機能することを確認してください。ほとんどの場合、作成と更新に同じアクションを使用すれば十分ですが、ゼロ長ドキュメントをチェックするアクションを記述して特殊な処理を実行する必要がある場合もあります。

9.3.2 サーバーに接続する一般的な手順

WebDAV サーバーへの接続方法は各 WebDAV クライアントで異なりますが、一般的な手順は次のとおりです。

1. WebDAV クライアントを開始します。
2. WebDAV サーバーの接続情報を入力します。これには、WebDAV サーバーのサーバー名およびポート番号が含まれます。例えばマシン `marklogic.myCompany.com` のポート 9001 で実行する WebDAV サーバーがある場合、WebDAV クライアントの適切な場所に次の URL を入力します。

`http://marklogic.myCompany.com:9001/`

3. 必要があれば、WebDAV サーバーのユーザー名およびパスワードを入力します。application-level セキュリティが設定されている場合を除き、ユーザー名およびパスワードを求められます。

注： WebDAV サーバーにログインするユーザーは、WebDAV ルートディレクトリ下のドキュメントおよびディレクトリにアクセスするために必要な権限（ロールにより付与）を持つ必要があります。また、WebDAV ユーザーが WebDAV ルート下でドキュメントを作成できるようにする場合は、そのユーザーがルート下でドキュメントを作成するために必要な URI 権限（ロールにより付与）を持つ必要があります。必要な権限やパーミッションがないと、WebDAV ログインやその他の WebDAV 操作が失敗する可能性があります。URI 権限およびドキュメントパーミッションの詳細については、『*Security Guide*』を参照してください。

4. 各クライアントで利用できるブラウズ方法で、ドキュメントおよびディレクトリを追加、削除、修正します。例えば Windows エクスプローラーでは、フォルダをダブルクリックして展開したり、ドキュメントをフォルダにドラッグアンドドロップしたり、ドキュメントやディレクトリの名前を変更したりできます。

9.3.3 Windows エクスプローラーで Web フォルダに接続する手順

Windows では、次の手順を実行して Windows エクスプローラーの WebDAV クライアントを使用できます。

1. デスクトップの [マイ ネットワーク] アイコンをダブルクリックします。
2. [マイ ネットワーク] で、[ネットワークプレースの追加] アイコンをダブルクリックします。
3. [ネットワークプレースの追加] ウィザードで、WebDAV サーバーのアドレスおよびポート番号を入力します。例えばマシン `marklogic.myCompany.com` のポート 9001 で実行する WebDAV サーバーがある場合、次の URL を入力します。

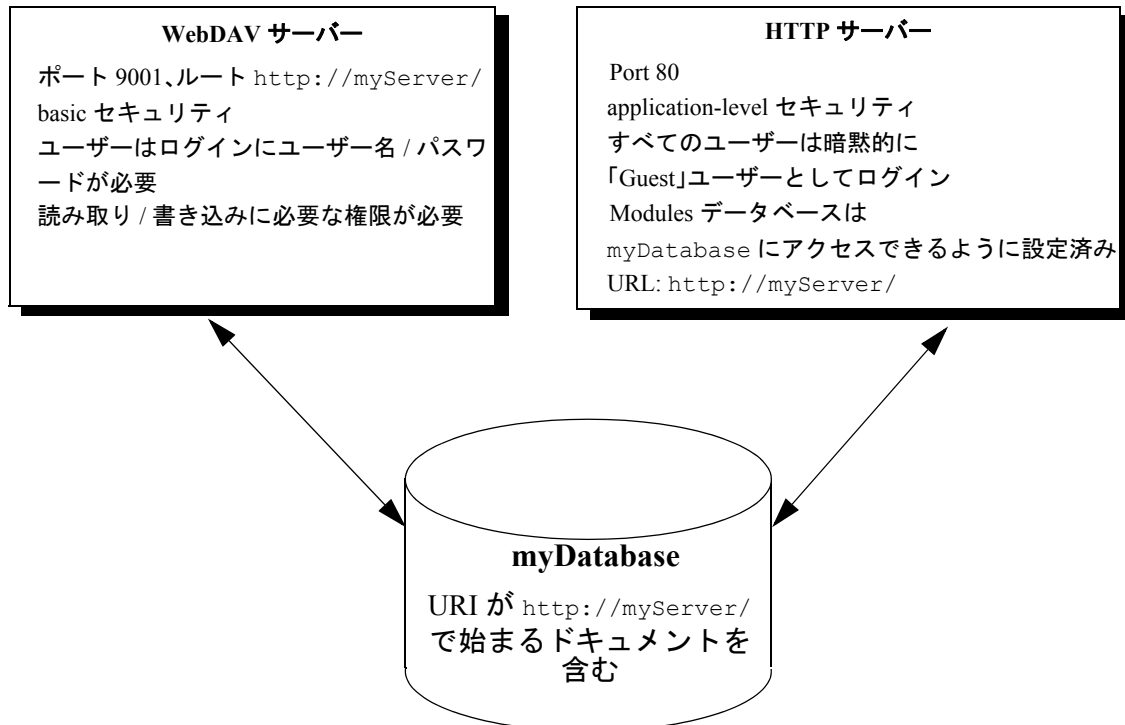
```
http://marklogic.myCompany.com:9001/
```

4. [次へ] をクリックします。
5. 必要があれば、WebDAV サーバーのユーザー名およびパスワードを入力します。
6. ネットワークの名前を入力し、[完了] をクリックします。

このフォルダは Windows の他のフォルダと同様に使用できます（ドキュメントのドラッグアンドドロップ、ドキュメント名の変更など）。MarkLogic サーバーの WebDAV サーバーに接続されている WebDAV フォルダにファイルをドラッグアンドドロップすると、実際にはデータベースにドキュメントを読み込むこととなります。

9.4 例：別のサーバーで使用されるドキュメントを追加 / 修正するために WebDAV サーバーをセットアップする

WebDAV サーバーを使うと、権限があるユーザーはデータベースへの書き込みができます (WebDAV クライアント経由)。そのデータベースは、1 つあるいは複数のサーバー (HTTP、ODBC、WebDAV、XDBC) に読み取りおよび実行アクセスを提供する Modules データベースとしても使用されている可能性があります。次の図に示すシナリオを考えてみましょう。



このシナリオでは、すべてのユーザーは Web ブラウザで URL `http://myServer/` にアクセスすることでコンテンツを表示できます。application-level セキュリティが設定されており、デフォルトユーザーの「Guest」でアクセスしているため、このサーバーにアクセスする際にパスワードは必要ありません。「Guest」ユーザーは読み取りパーミッションのみを持ちます。「Guest」ユーザーにアクセスさせたくないコンテンツがある場合は、「Guest」ユーザーが持たない権限でそのコンテンツを読み込みます。

一方で、適切な権限を持つユーザーは、WebDAV クライアント経由でログインし、ポート 9001 で WebDAV サーバーにアクセスできます。WebDAV サーバーは basic セキュリティが設定されているため、ユーザーは、WebDAV クライアント経由で (またはポート 9001 に接続された Web ブラウザ経由で) アクセスするときにユーザー名およびパスワードが要求されます。ユーザーは、データベースセキュリティポリシーに基づいて、WebDAV クライアントからドキュメントの追加、編集、読み取りが可能です。

Modules データベースについては、「Modules データベース」(107 ページ) を参照してください。

10.0 ODBC サーバー

ODBC サーバーは、MarkLogic サーバーに対する SQL クエリをサポートするコンポーネントの 1 つです。この章では、ODBC サーバーの概要および設定手順について説明します。次のセクションから構成されています。

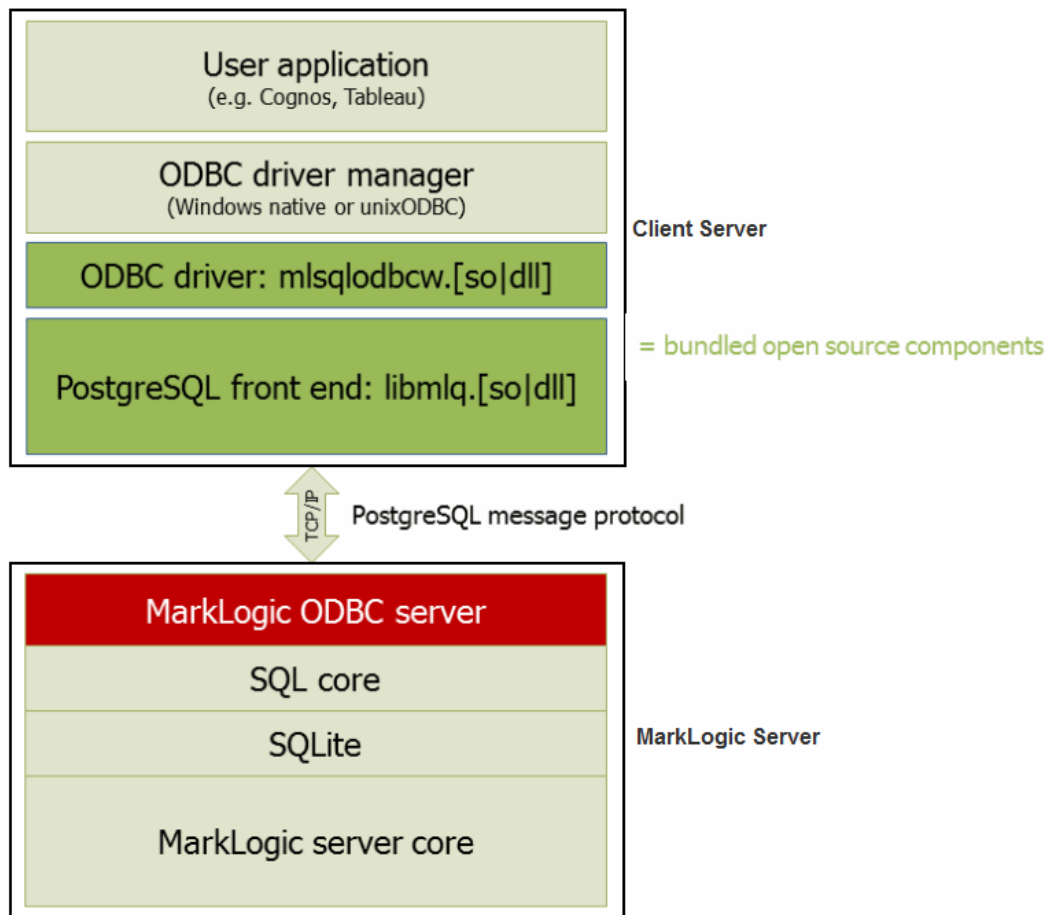
- [ODBC サーバーの概要](#)
- [ODBC サーバーを作成および管理する手順](#)

この章では、管理画面を使用して ODBC サーバーを作成および設定する方法について説明します。ODBC サーバーをプログラムによって作成および設定する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring App Servers](#)」を参照してください。

10.1 ODBC サーバーの概要

ODBC サーバーの基本的な目的は、SQL クエリに応答して、MarkLogic サーバー内にあるリレーショナル形式のデータを返すことです。ODBC サーバーは、BI（ビジネスインテリジェンス）ツールからの SQL および ODBC ステートメントのサブセットに答えて、タプル形式でデータを返し、サーバー状態を管理します。

下図の例では、ODBC サーバーは PostgreSQL メッセージプロトコルを使用してクライアント上の PostgreSQL フロントエンドと接続しています。ODBC サーバーは PostgreSQL フロントエンドからの SQL クエリを受け入れ、BI アプリケーションでレポートを作成するために必要となるリレーショナル形式のデータを返します。



10.2 ODBC サーバーを作成および管理する手順

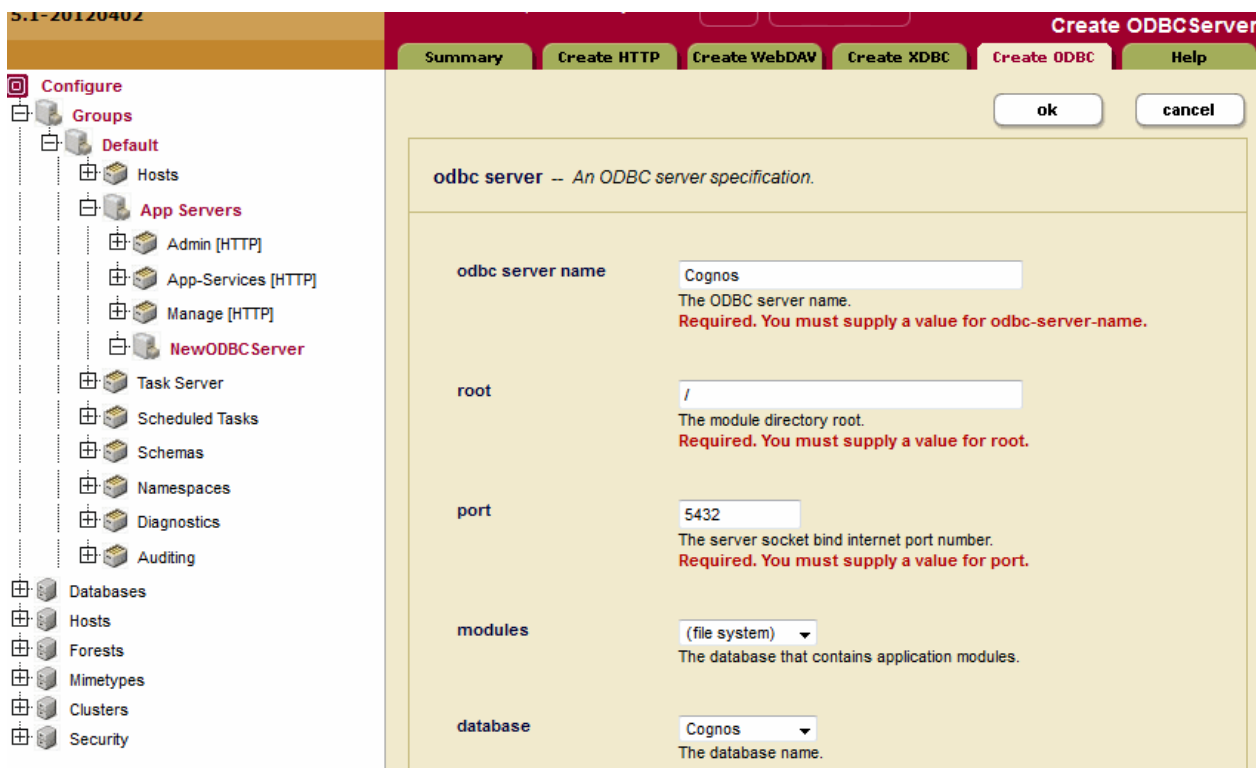
ODBC サーバーを作成および管理するには、次の手順を実行します。

- [新しい ODBC サーバーの作成](#)
- [ODBC サーバーの出力オプションの設定](#)
- [ODBC サーバー設定の表示](#)
- [ODBC サーバーの削除](#)
- [リクエストのキャンセル](#)

10.2.1 新しい ODBC サーバーの作成

新しいサーバーを作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. ODBC サーバーを定義するグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 右上の [Create ODBC] タブをクリックします。[Create ODBC Server] ページが表示されます。



5. [Server Name] フィールドで、この ODBC サーバーの短い名前を入力します。MarkLogic サーバーでは、管理画面でこのサーバーを参照する際にこの名前を使用します。

6. [root] ディレクトリフィールドで、データを格納するディレクトリの名前を入力します。[modules] フィールドでデータベースを指定している場合、ルートは指定された Modules データベース内のディレクトリ URI である必要があります。

[modules] フィールドでファイルシステムを指定している場合、ルートディレクトリは完全修飾パス名であるか、MarkLogic サーバーがインストールされているディレクトリからの相対パスとなります。プラットフォーム別のデフォルトのインストールディレクトリを次の表に示します。

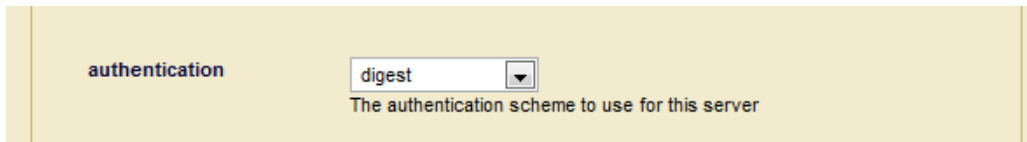
プラットフォーム	プログラムディレクトリ
Microsoft Windows	C:\Program Files\MarkLogic
Red Hat Linux	/opt/MarkLogic
Mac OS X	~/Library/MarkLogic

注： 共有ドライブを指定する場合を除き、グループ内のすべてのホストにおいて、上記の指定ディレクトリ内にアプリケーションモジュールのコピーを保持する必要があります。

警告 Docs、Data、または Admin という名前の ODBC サーバールートディレクトリを作成しないでください。これらのディレクトリは、他の目的で MarkLogic サーバーによって予約されています。これらの名前で ODBC サーバールートディレクトリを作成すると、予期しないサーバー動作になる可能性があります。また、ソフトウェアのアップグレードが複雑になることもあります。

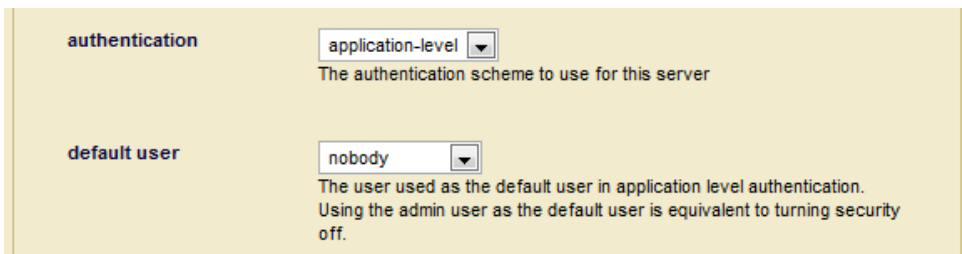
7. [Port] フィールドで、この ODBC サーバーを使用するためのポート番号を入力します。デフォルトの PostgreSQL リスンソケットポートは 5432 です。このポート番号はこの ODBC サーバーに一意である必要があります。他の ODBC、HTTP、XDBC、WebDAV サーバーと重複しないようにしてください。
8. [Modules] フィールドで、XQuery ドキュメントの Modules データベースとして使用するデータベースを選択します。ファイルシステム上に XQuery モジュールを格納する場合はデフォルトのままにします。Modules データベースの詳細については、「Modules データベース」(107 ページ) を参照してください。
9. [Database] フィールドで、この ODBC サーバーがアクセスするデータベースを選択します。SQL アプリケーションをサポートするために、このデータベースにはレンジインデックスおよびスキーマビューが必要です。SQL アプリケーションをサポートするようにデータベースをセットアップする方法の詳細については、『*SQL Data Modeling Guide*』を参照してください。1つのデータベースに対して、複数の ODBC、HTTP、XDBC、WebDAV サーバーがアクセスできます。

10. [Authentication] フィールドまでスクロールします。認証スキームとして `digest`、`basic`、`digestbasic`、または `application-level` を選択します。デフォルトは `digest` で、暗号化されたパスワードを使用します。



The screenshot shows a configuration panel with a label 'authentication' on the left. To its right is a dropdown menu with 'digest' selected. Below the dropdown is the text: 'The authentication scheme to use for this server'.

`application-level` 認証を選択した場合は、デフォルトユーザーも設定する必要があります。この場合、ODBC サーバーにログインすると自動的にこのデフォルトユーザーとなります（明示的に他のユーザーとしてログインした場合を除く）。

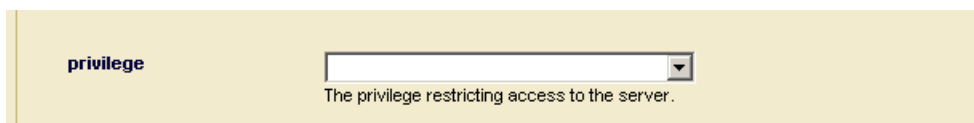


The screenshot shows two configuration panels. The top panel is labeled 'authentication' and has a dropdown menu with 'application-level' selected. Below it is the text: 'The authentication scheme to use for this server'. The bottom panel is labeled 'default user' and has a dropdown menu with 'nobody' selected. Below it is the text: 'The user used as the default user in application level authentication. Using the admin user as the default user is equivalent to turning security off.'

警告 管理者ユーザー (`admin`) をデフォルトユーザー (`admin` ロールを持つ承認済み管理者) として使用する場合、このアプリケーションサーバーを使用する全員が自動的に `admin` ロールを持つユーザーになり、このアプリケーションサーバーのセキュリティが実質的にオフになります。

11. 画面下部近くの [Privilege] フィールドまでスクロールします。このフィールドは、サーバーにアクセス（ログイン）するために必要な権限を表します。このフィールドは空白のままにしてもかまいません。

ODBC サーバーにアクセスするユーザーは、ODBC サーバーにアクセスするための実行権限が選択されている必要があります。前述の `application-level` 認証を選択した場合は、デフォルトユーザーが選択された権限を持っていることを確認する必要があります。



The screenshot shows a configuration panel with a label 'privilege' on the left. To its right is a dropdown menu that is currently empty. Below the dropdown is the text: 'The privilege restricting access to the server.'

12. このアプリケーションサーバーの他のプロパティをニーズに合わせて設定します。
- [Last Login] および [Display Last Login] については、「最終ユーザーログイン試行の格納およびモニタリング」(103 ページ) を参照してください。
 - [Address] は、アプリケーションサーバーの IP アドレスを指定します。
 - [Backlog] は、ODBC サーバーソケットで許可される保留状態の接続の最大数を指定します。
 - [Threads] は、アプリケーションサーバースレッドの最大数を指定します。
 - [Request Timeout] は、ソケットが最初のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。
 - [Keep Alive timeout] は、ソケットが同一接続上で後続のリクエストのタイムアウトを受け取るまでの最大秒数を指定します。
 - [Session Timeout] は、非アクティブなセッションがタイムアウトするまでの最大秒数を指定します。
 - [Max Time Limit] は、リクエストの時間制限の上限を指定します。どのリクエストにも、この数値より大きな時間制限を（例えば `xdmp:set-request-time-limit` を使用して）設定できません。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
 - [Default Time Limit] は、リクエストの制限時間が指定されていないときのデフォルト値を指定します。リクエストは、`xdmp:set-request-time-limit` を使用して時間制限を変更できます。このリクエストの時間制限は、クエリリクエストの処理を許可する最大秒数です。アプリケーションサーバーは、時間のかかるクエリの処理を中止して、エラーを返します。
 - [Static Expires] は、静的コンテンツが指定された秒数後に期限切れになる「expires」ODBC ヘッダを追加します。
 - [Pre-commit Trigger Limit] は、このアプリケーションサーバーに対するシングルステートメントが呼び出せるプリコミットトリガーの最大数を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。
 - [Pre-commit Trigger Depth] は、このアプリケーションサーバーに対して実行されるプリコミットトリガーの最大深度（他のトリガーを発行できるようになるまでのトリガー数）を指定します。トリガーの詳細については、『*Application Developer's Guide*』の「[Using Triggers to Spawn Actions](#)」を参照してください。

- [Collation] は、このアプリケーションサーバーで実行されるクエリのデフォルトのコレクションを指定します。このコレクションは、クエリで指定されていない場合に文字列の比較およびソートに使用されます。詳細については、『*Search Developer's Guide*』の「[Encodings and Collations](#)」を参照してください。
- [Concurrent Request Limit] は、特定時点で任意のユーザーが実行している可能性のあるリクエストの最大数を指定します。0 は、最大数なしを表します。詳細については、「同時ユーザーセッション数の管理」（101 ページ）を参照してください。
- [Log Errors] は、このアプリケーションサーバーのキャッチされなかったエラーを ErrorLog.txt ファイルに記録するかどうかを指定します。アプリケーションサーバーで発生することのある例外を記録して後でデバッグに使用するとき便利です。
- [Debug Allow] は、このアプリケーションサーバーに対するリクエストをデバッグ（MarkLogic サーバーのデバッグ API を使用）のために停止できるようにするかどうかを指定します。
- [Profile Allow] は、このアプリケーションサーバーに対するリクエストをプロファイリング（MarkLogic サーバーのプロファイリング API を使用）のために停止できるようにするかどうかを指定します。詳細については、『*Query Performance and Tuning Guide*』の「[Profiling Requests to Evaluate Performance](#)」を参照してください。
- [Default XQuery Version] は、XQuery モジュールがこの言語バージョンを明示的に宣言する場合に、このアプリケーションサーバーのデフォルト XQuery 言語を指定します。
- [Multi Version Concurrency Control] は、最新のタイムスタンプの取得に関するクエリ動作の厳密度を指定します。これは、更新ステートメントではなくクエリステートメントのみに影響します。MarkLogic サーバーにおけるクエリおよびトランザクションの詳細については、『*Application Developer's Guide*』の「[Understanding Transactions in MarkLogic Server](#)」を参照してください。
- [Error Handler] および [URL Rewriter] フィールドについては、『*Application Developer's Guide*』の「[Controlling App Server Access, Output, and Errors](#)」を参照してください。
- SSL サポートに関連するプロパティについては、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

13. 上部または下部までスクロールして [ok] をクリックします。

これで ODBC サーバーが作成されます。ODBC サーバーの作成は「ホット」管理タスクなので変更はすぐに有効になります。ユーザーセッションの管理やログイン試行のトラッキングの詳細やセットアップ手順については、「ユーザーセッションの管理およびログイン試行のモニタリング」（101 ページ）を参照してください。

10.2.2 ODBC サーバーの出力オプションの設定

ODBC サーバーごとに、さまざまなデフォルト出力オプションを設定できます。出力オプションは、アプリケーションサーバーから返されるデータのシリアル化方法に影響します。また、オプションをクエリレベルで設定することで、デフォルトオプションよりも優先させることができます。XQuery では `declare option XQuery` プロローグを使用し、XSLT では `<xsl:output>` 命令を使用して、アプリケーションサーバーのデフォルトよりも優先させるようなシリアル化オプションを設定できます。XQuery でシリアル化オプションを設定する方法の詳細については、『*XQuery and XSLT Reference Guide*』の「[Declaring Options](#)」を参照してください。XSLT 出力の詳細については、XSLT 仕様 (<http://www.w3.org/TR/xslt20#serialization>) を参照してください。

アプリケーションサーバーのデフォルトを指定するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 表示する ODBC サーバーが含まれるグループをクリックします (例えば Default)。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 編集するアプリケーションサーバーを選択します。
5. 左側のツリーメニューで [Output Options] を選択します。[Output Options Configuration] ページが表示されます。
6. このアプリケーションサーバーに関して制御するオプションを設定します。
7. [ok] をクリックして変更を保存します。

アプリケーションサーバーの出力の詳細については、『*Application Developer's Guide*』の「[Controlling App Server Access, Output, and Errors](#)」を参照してください。

10.2.3 ODBC サーバー設定の表示

特定 ODBC サーバーの設定を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 表示する ODBC サーバーが含まれるグループをクリックします (例えば Default)。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [Summary] タブで、設定を表示する ODBC サーバーを見つけます。
5. ODBC サーバーのアイコンをクリックします。
6. 設定を表示します。

10.2.4 ODBC サーバーの削除

ODBC サーバーの設定を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 削除する ODBC サーバーが含まれるグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [Summary] タブで、削除する ODBC サーバーを見つけます。
5. ODBC サーバーのアイコンをクリックします。
6. [delete] をクリックします。
7. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

ODBC サーバーの削除は「コールド」管理タスクです。変更を反映するために、サーバーが再起動します。

10.2.5 リクエストのキャンセル

管理画面のアプリケーションサーバーの [Status] ページでリクエストをキャンセルできます（[Groups] > [グループ名] > [App Servers] > [アプリケーションサーバー名] > [Status] タブ）。

App Server Status

Summary | Configure | **Status** | Create HTTP | Create WebDAV | Create XDBC | Help

App Server: myAppServer[HTTP] show less

appserver status -- A detailed view of this appserver's activity.

App Server: myAppServer [HTTP]
 Database: apidoc
 Hosts: raymond.marklogic.com

Host	Threads	Requests	Updates	Average Time	Request Rate	Oldest Request	Expanded Tree Cache Hits	Misses	Ratio
raymond.marklogic.com	2	1	0	2.8 s	0.1	2.8 s	460224	34389	93%
	2	1	0	2.8 s	0.1	n/a	460224	34389	93%

Query	#	Average Time	Oldest Time	Expanded Tree Cache Hits	Misses	Ratio
/cq-eval.xqy	1	2.8 s	2.8 s	0	0	n/a
Total	1	2.8 s	2.8 s	0	0	n/a

Host	Query	User	Client IP	Time	Expanded Tree Cache Hits	Misses	Ratio
raymond.marklogic.com	/cq-eval.xqy	admin	182.16.1.131	2.8 s	0	0	n/a [cancel]
	Total			0	0	n/a	

実行時間が長いリクエスト（例えば実行時間が長いクエリステートメントや更新ステートメント）をキャンセルするには、次の手順を実行します。

1. 管理画面で、[Group] メニュー項目をクリックします。
2. ツリーメニューまたは [Summary] タブから、リクエストが発行されたアプリケーションサーバーに移動します。
3. [Status] タブをクリックします。
4. [show more] ボタンをクリックします。

5. アプリケーションサーバーの [Status] ページの右下で、キャンセルするクエリの行にある [cancel] ボタンをクリックします。
6. [Cancel Request] 確認ページで、[ok] をクリックします。確認ページが表示されたときにリクエストがすでに完了している場合は、リクエストが見つからないというメッセージがページに表示されます。

リクエストがキャンセルされ、アプリケーションサーバーの [Status] ページが再度表示されます。

11.0 イベントの監査

MarkLogic サーバーには監査機能があり、ドキュメントの読み取りアクセス、サーバーの起動、サーバーのシャットダウン、ドキュメントのパーミッション変更など、さまざまなイベントを監査できます。これらの監査イベントのレコードは監査ファイルに記録されます。監査ファイルは MarkLogic サーバーのインスタンスごとに MarkLogic サーバーのデータディレクトリに格納されます。この章では、監査機能について説明します。以下のように構成されています。

- [監査の概要](#)
- [監査可能イベント](#)
- [監査ログのコンテンツ](#)

11.1 監査の概要

MarkLogic サーバーを監査する際に、どのイベントに対して監査イベントレコードを生成するのかを指定できます。大量のイベントのリストから監査対象を選択して、いくつかの識別子（ユーザー、ロール、ドキュメント URI など）に関するイベントだけを監査するように制限できます。このセクションでは、MarkLogic サーバーのログ記録機能について説明します。以下のように構成されています。

- [監査ログファイル](#)
- [監査イベントの制限](#)
- [成功、失敗、または両方の種類のイベントの監査](#)
- [グループレベルでオン](#)

11.1.1 監査ログファイル

監査がオンの場合、MarkLogic サーバーは監査イベントを `AuditLog.txt` ファイルに書き込みます。クラスタ内の各ホストが独自の監査ログファイルを維持します。アクションによっては複数の監査イベントをトリガーします。このようなイベントは、そのイベントが発生したホストで監査されるため、複数のホストでログに記録される可能性があります。監査イベントの詳細については、「監査可能イベント」（93 ページ）を参照してください。監査イベントログファイルについては、次の点に注意してください。

- さまざまなイベントについて、メッセージが `AuditLog.txt` ファイルに書き込まれます。
- それぞれのイベントごとにタイムスタンプ、イベントの種類、ユーザー、ロール、その他のイベント関連情報（`document-read` イベントのドキュメント URI など）があります。ログエントリの例については、「監査ログの例」（99 ページ）を参照してください。

- 監査ファイルをローテーションする頻度を設定できます（「ログファイル」（403 ページ）で説明しているログファイルと同様）。
- 監査ログファイルは、アクセスログファイル（`port_AccessLog.txt`）やエラーログファイル（`ErrorLog.txt`）と同じディレクトリに格納されます。これは `<marklogic-data-dir>/Logs` ディレクトリ内にあります。これらのファイルは監査イベントが発生したホスト独自のものです。
- 現在のファイルログやアーカイブ済みのファイルログは、標準的なテキストファイル表示ツールを使用していつでも表示できます。また、管理画面のメインページにある [Log] タブからログファイルにアクセスできます。

さまざまなプラットフォームにおける `AuditLog.txt` ファイルの場所を次の表に示します。

プラットフォーム	監査ファイル
Microsoft Windows	<code>C:\Program Files\MarkLogic\Data\Logs\AuditLog.txt</code>
Red Hat Linux	<code>/var/opt/MarkLogic/Logs/AuditLog.txt</code>
Mac OS X	<code>~Library/Application Support/MARKlogic/Data/Logs/AuditLog.txt</code>

11.1.2 監査イベントの制限

次の基準に基づいて監査対象イベントを制限するように監査機能を設定できます。

- 監査対象イベントを選択できます。
- ユーザー名に基づいて、イベントを含めたり除外したりできます。含めるユーザーの場合、指定されたユーザーによって開始されたイベントのみが監査されます。除外するユーザーの場合、指定されたユーザー以外のユーザーによって開始されたイベントのみが監査されます。
- ロールに基づいて、イベントを含めたり除外したりできます。含めるロールの場合、含めるロールを持つユーザーによって開始されたイベントのみが監査されます。除外するロールの場合、除外するロールを持たないユーザーによって開始されたイベントのみが監査されます。
- イベントの結果（成功 / 失敗 / 両方）に基づいて、イベントを含めたり除外したりできます。
- ドキュメント URI に基づいて、イベントを含めたり除外したりできます。ドキュメント URI はそのドキュメントのなんらかのフラグメントがメモリに読み込まれる場合に監査されます。その監査イベントは、ドキュメントが含まれるフォレストが存在するホスト上の監査ログに書き込まれます。

監査機能をセットアップする手順については、「特定イベントを監査する監査設定および特定の制限のセットアップ」（100 ページ）を参照してください。

11.1.3 成功、失敗、または両方の種類のイベントの監査

失敗のみ、成功のみ、または両方の種類のイベントを監査するように選択できます。多くのイベントを監査する場合や、成功と失敗の両方のイベントを監査する場合、最終的に多量のイベントを監査することになる可能性があります。多くのイベントを監査することは問題ではありませんが、監査ログが急激に巨大になる可能性があります。監査機能をセットアップする手順については、「特定イベントを監査する監査設定および特定の制限のセットアップ」(100 ページ) を参照してください。

11.1.4 グループレベルでオン

監査はグループごとにオンまたはオフにできます。グループの監査をオンにした場合、そのグループで設定済みの監査可能イベントが監査されます。監査をオンにする手順の詳細については、「グループの監査をオンにする」(100 ページ) を参照してください。

11.2 監査可能イベント

MarkLogic サーバーには多くの監査可能イベントがあります。監査がオンのときは、オンになっている監査可能イベントの記録がすべて `AuditLog.txt` ファイルに書き込まれます。クラスタ環境の場合、監査イベントはイベントが発生したホスト上の監査ファイルに書き込まれます。イベントはそのイベントが発生したホストで監査されるため、操作によっては監査イベントが複数のホストに分散して発生します。例えば、対象ドキュメントを含むフォレストが存在するデータノードに対してドキュメントアクセス監査イベントが監査されているとします。ここでドキュメント更新のクエリが実行された場合、クエリを評価するノード (エバリュエータノード) と、影響を受けるドキュメントが存在する 1 つあるいは複数のデータノードで、監査イベントが発生する可能性があります (監査設定およびクラスタ設定によって異なる)。

MarkLogic サーバーでオンにできる監査可能イベントを次の表に示します。

イベント	説明	URI 制限	ロール / ユーザーによる制限	成功または失敗による制限
amp-usage	Amp が評価されたときに Amp の URI を監査します。	可能 (Amp の URI に基づく)	可能	成功のみ
audit-configuration-change	監査設定の変更に対する成功または失敗を監査します。	該当なし	可能	可能
audit-shutdown	監査システムがオフになったときに監査します。	該当なし	可能	可能

イベント	説明	URI 制限	ロール/ ユーザーによる制限	成功または失敗による制限
audit-startup	監査システムがオンになったときに監査します。MarkLogic サーバーが起動したときはこのイベントが発生しないことに注意してください。監査システムがオンになったときのみが対象です。	該当なし	可能	可能
authentication-failure	失敗した認証試行を監査します。	該当なし	可能	失敗のみ
concurrent-request-denial	アプリケーションサーバーの同時リクエスト制限に達したためにリクエストが拒否されたときに監査します。	該当なし	可能	失敗のみ
configuration-change	設定ファイルへの変更に対する成功または失敗を監査します。変更された設定ファイルのパスが含まれます。	該当なし	可能	可能
document-execute	データベース内のドキュメント（XQuery ドキュメントなど）が実行されたときに監査します。監査レコードにはドキュメント URI が含まれます。	可能	可能	成功のみ
document-insert	新しいドキュメントが作成されたときに監査します。監査レコードにはドキュメントの URI が含まれます。	可能	可能	成功のみ

イベント	説明	URI 制限	ロール / ユーザーによる制限	成功または失敗による制限
document-read	ドキュメントが読み取られたときに監査します。監査レコードにはドキュメントの URI が含まれます。	可能	可能	成功のみ
document-update	ドキュメントが更新されたときに監査します。監査レコードにはドキュメントの URI が含まれます。	可能	可能	成功のみ
estimate	<code>xdmp:estimate</code> 式が評価されたときに監査します。	該当なし	可能	成功のみ
eval	データベースにアクセスするパス式が評価されたときに監査します。	該当なし	可能	成功のみ
exists	<code>xdmp:exists</code> 式が評価されたときに監査します。	該当なし	可能	成功のみ
FIPS-Disabled	FIPS モードがオフになったときに監査します。	該当なし	該当なし	成功のみ
FIPS-Enabled	FIPS モードがオンになったときに監査します。	該当なし	該当なし	成功のみ
lexicon-read	値レキシコン (例: <code>cts:element-values</code> など) の呼び出しが使用されたときに監査します。	該当なし	可能	成功のみ
mlcp-copy-export-start	mlcp の copy または export ジョブが開始したときに監査します。	該当なし	該当なし	成功のみ
mlcp-copy-export-finish	mlcp の copy または export ジョブが成功または失敗して完了したときに監査します。	該当なし	該当なし	不可

イベント	説明	URI 制限	ロール / ユーザーによる制限	成功または失敗による制限
no-permission	SEC-PERMDENIED 例外のために操作が失敗したときに監査します。この例外は、必要なパーミッションなしにドキュメントの操作（挿入、更新、または実行）が試行されるときに発生します。	可能	可能	失敗のみ
no-privilege	ユーザーが特定機能を実行するための十分な権限を持たない場合に監査します。	可能	可能	失敗のみ
permissions-change	ドキュメントのパーミッションが修正されたときに監査します。	可能	可能	可能
request-blackout-denial	リクエストブラックアウト期間のためにリクエストが拒否されたときに監査します。	該当なし	可能	失敗のみ (拒否されたとき)
role-change-failure	ユーザーのロールの追加または削除試行が失敗したときに監査します。	該当なし	可能	失敗のみ
search	cts:search 式が評価されたときに監査します。	該当なし	可能	成功のみ
security-access	次のセキュリティ関連関数のいずれかが呼び出されたときに監査します。 xdmp:can-grant-roles、 xdmp:has-privilege、 xdmp:user-roles、 xdmp:role-roles、 xdmp:privilege-roles、 xdmp:amp-roles、 xdmp:get-current-role、 xdmp:user、xdmp:role、 xdmp:amp。	該当なし	可能	可能

イベント	説明	URI 制限	ロール / ユーザーによる制限	成功または失敗による制限
server-restart	MarkLogic サーバーがクリーン再起動で（例えば管理画面から）再起動したときに監査します。	該当なし	可能	成功のみ
server-shutdown	MarkLogic サーバーがクリーンシャットダウンで（例えばシャットダウンスクリプトや管理画面から）シャットダウンしたときに監査します。	該当なし	可能	成功のみ
server-startup	MarkLogic サーバーが起動したときに監査します。	該当なし	該当なし	成功のみ
TLS-Failure	TLS または SSL リクエストが失敗したときに監査します。IP アドレスが含まれます。	該当なし	該当なし	失敗のみ
user-configuration-change	ユーザー設定で変更が発生したときに監査します。	該当なし	可能	可能
user-role-addition	ユーザーにロールが追加されたときに監査します。	該当なし	可能	可能
user-role-removal	ユーザーからロールが削除されたときに監査します。	該当なし	可能	可能

11.2.1 監査ログのコンテンツ

監査ログに含まれる情報は、イベントの種類によって異なります。すべての監査ログエントリには、イベントの種類、ユーザー、成功、ユーザーに割り当てられたロールなど、基本的な情報が含まれます。監査ログエントリには、次のフィールドがスペース区切りで含まれることがあります。

ログエントリのフィールド	説明	例
タイムスタンプ	監査可能アクションが発生した日時が含まれます。	2012-03-26 10:55:53.735
イベント	ログエントリをトリガーしたイベントの名前。可能性のある監査可能イベントは、「監査可能イベント」(93 ページ) に示しています。	event=amp-usage
関数	イベント中に実行されていた関数。	function=http://marklogic.com/xdmp/admin:read-config-file
式	この監査イベントをトリガーしたクエリ式。	expr=cts:element-value-query(xs:QName("info:status"),("active", "unloading"),("unstemmed","lang=en"), 1)
種類	特定イベントを生成した、MarkLogic サーバー内のタスクの種類。	type=node-update
URI	イベントに関係のあるドキュメント URI。	uri=/queries/5523898374388210414.txt
データベース	イベント中にアクセスされたデータベース。	database=Security
結果	監査イベントをトリガーしたアクションの成功または失敗を示します。	success=true
ユーザー	アクションを実行したユーザー。	user=infostudio-admin
ロール	アクションを実行したユーザーに割り当てられているロール。	roles=cpf-restart,infostudio-user

11.2.2 監査ログの例

次に、AuditLog.txt エントリの例を示します。ユーザー固有の情報は難読化されています。

```
2012-03-26 10:55:53.735 event=amp-usage;
function=http://marklogic.com/xdmp/admin:read-config-file;
uri=/MarkLogic/admin.xqy; database=filesystem;
success=true; user=admin; roles=admin;
```

```
2012-03-23 15:04:32.141 event=security-access; user(admin-xxx);
success=true;
user=admin-xxx; roles=admin;
```

```
2012-03-23 15:04:32.176 event=document-read;
uri=http://marklogic.com/xdmp/privileges/7768816571421711260;
database=Security; success=true; user=admin-xxx; roles=admin;
```

```
2012-03-23 15:05:26.957 event=lexicon-read;
expr=cts:element-value-query(xs:QName("info:status"),
("active", "unloading"), ("unstemmed", "lang=en"), 1);
database=App-Services; success=true; user=infostudio-admin;
roles=cpf-restart,infostudio-user;
```

```
2012-03-23 15:07:05.164 event=document-update; type=node-update;
uri=/workspaces/14061174091930893017.xml; database=App-Services;
success=true; user=admin-xxx; roles=admin;
```

```
2012-03-23 15:07:05.674 event=document-insert; type=insert;
uri=/queries/5523898374388210414.txt; database=App-Services;
success=true; user=admin-xxx; roles=admin;
```

11.3 グループの監査の設定

監査は、管理画面の [Auditing] ページを使用して、グループレベルで設定されます。グループの詳細については、「グループ」(40 ページ) を参照してください。このセクションでは、次の監査設定手順について説明します。

- [グループの監査をオンにする](#)
- [グループの監査をオフにする](#)
- [特定イベントを監査する監査設定および特定の制限のセットアップ](#)

11.3.1 グループの監査をオンにする

グループの監査をオンにするには、次の手順を実行します。

1. ブラウザで管理画面にアクセスします。
2. [Audit Configuration] 画面を開きます ([Groups] > [グループ名] > [Auditing])。
3. [audit enabled] ラジオボタンで [true] を選択します。
4. 監査イベントや監査制限を適宜設定します。
5. [ok] をクリックします。

11.3.2 グループの監査をオフにする

グループの監査をオフにするには、次の手順を実行します。

1. ブラウザで管理画面にアクセスします。
2. [Audit Configuration] 画面を開きます ([Groups] > [グループ名] > [Auditing])。
3. [audit enabled] ラジオボタンで [false] を選択します。
4. [ok] をクリックします。

グループの監査がすぐにオフになります。設定した内容は保存されますが、監査を再度オンにするまで有効になりません。

11.3.3 特定イベントを監査する監査設定および特定の制限のセットアップ

監査イベントおよび監査制限を設定する一般的な手順は次のとおりです。実際の手順は、設定するイベントや制限によって異なります。

1. ブラウザで管理画面にアクセスします。
2. [Audit Configuration] 画面を開きます ([Groups] > [グループ名] > [Auditing])。
3. [audit events] で、監査するイベントを選択します。各イベントの説明については、「監査可能イベント」(93 ページ)を参照してください。
4. [audit restrictions] で、制限を適宜入力します。監査制限の詳細については、「監査イベントの制限」(92 ページ)を参照してください。
5. [ok] をクリックして変更を保存します。

12.0 ユーザーセッションの管理およびログイン試行のモニタリング

MarkLogic サーバーでは、ユーザーセッションの制御や管理、およびログイン試行のモニタリングの機能を用意しています。この章では、これらの機能を使用および管理する方法について説明します。以下のように構成されています。

- [同時ユーザーセッション数の管理](#)
- [アプリケーションサーバーのリクエストブラックアウトの設定](#)
- [最終ユーザーログイン試行の格納およびモニタリング](#)

12.1 同時ユーザーセッション数の管理

MarkLogic サーバーでは、あるアプリケーションサーバーに対する同時ユーザーセッションの最大数を制限できます。このセクションでは、この機能について、および同時リクエスト制限の設定について説明します。以下のように構成されています。

- [ユーザーセッション制限による同時リクエスト数の制限](#)
- [ユーザー同時セッション制御の設定](#)

12.1.1 ユーザーセッション制限による同時リクエスト数の制限

各アプリケーションサーバー（HTTP、ODBC、XDBC、および WebDAV サーバー）の設定には、1人のユーザーがアプリケーションサーバーに対して実行できる「同時リクエスト」数を制限するオプションがあります。同時リクエストとは、あるユーザーからのアプリケーションサーバーへのリクエストが依然としてアクティブである間に、この同一ユーザーが要求した他のリクエストのことです。各アプリケーションサーバーには `concurrent request limit` 設定パラメータがあります。デフォルトは 0 で、同時リクエスト数の制限がないことを意味します。値は 0 以上の整数にする必要があります。

`concurrent request limit` 設定パラメータを 0 以外の値に設定すると、そのアプリケーションサーバーに対して任意のユーザーが実行できる同時リクエスト数が、指定された値に制限されます。例えば値を 3 に設定した場合、ユーザー `raymond` によるリクエストが 3 つ実行中のときに、`raymond` からさらに発行されたリクエストは例外で失敗します。

制限に達すると、アプリケーションは `XDMP-REQUESTLIMIT` 例外で 403 (forbidden) エラーをスローします。

12.1.2 ユーザー同時セッション制御の設定

ユーザー同時セッション制限を設定するには、管理画面で次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. 設定するアプリケーションサーバーが存在するグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 同時セッション制限を設定するアプリケーションサーバーを選択します。[App Server Configuration] ページが表示されます。
5. [concurrent request limit] フィールドで、許可する同時ユーザーセッションの最大数に相当する値を入力します。例えば、同時セッション数を 3 つだけにする場合は、3 と入力します。値 0 は、同時リクエスト制限がない（無制限である）ことを意味します。
6. [ok] をクリックして設定の変更を保存します。

新しいリクエストからこの新しい `concurrent request limit` に従います。

12.2 アプリケーションサーバーのリクエストブラックアウトの設定

MarkLogic サーバーでは、ユーザーまたはユーザーグループがアプリケーションサーバーに対してリクエストを実行できない期間を管理できます。このようなブラックアウト期間は、アプリケーションサーバーに 1 つあるいは複数のリクエストブラックアウトをセットアップすることで、アプリケーションサーバーごとに管理できます。リクエストブラックアウトでは、ブラックアウト対象のユーザー、ロール、および期間を指定できるほか、ブラックアウトが 1 回限りなのか繰り返しなのかを指定できます。

- [リクエストブラックアウトの設定](#)
- [リクエストブラックアウトの削除](#)

12.2.1 リクエストブラックアウトの設定

リクエストブラックアウト期間を設定するには、次の手順を実行します。

1. 管理画面のツリーメニューで、[Groups] > [group_name] > [App Servers] > [app_server_name] リンクをクリックします。ここで「group_name」はグループ名、「app_server_name」はリクエストブラックアウト期間を指定するアプリケーションサーバーの名前です。
2. アプリケーションサーバーの [Request Blackout] メニュー項目をクリックします。[Request Blackout Policy Configuration] ページが表示されます。

3. [Create] タブをクリックします。[Add Request Blackout] ページが表示されます。
4. 作成するブラックアウト期間に合わせてフォームを適宜設定します。ラジオボタンをクリックすると、設定するフォームがさらに表示されます。
5. [ok] をクリックしてブラックアウト期間を作成します。

新しいブラックアウト期間はすぐに有効になります。

12.2.2 リクエストブラックアウトの削除

リクエストブラックアウト期間を削除するには、次の手順を実行します。

1. 管理画面のツリーメニューで、[Groups] > [group_name] > [App Servers] > [app_server_name] リンクをクリックします。ここで「group_name」はグループ名、「app_server_name」はリクエストブラックアウト期間を指定するアプリケーションサーバーの名前です。
2. アプリケーションサーバーの [Request Blackout] メニュー項目をクリックします。[Request Blackout Policy Configuration] ページが表示されます。
3. 削除するブラックアウト期間に対応した領域で、[delete] ボタンをクリックします。
4. 確認ページで [ok] をクリックして、ブラックアウト期間を削除します。

ブラックアウト期間はすぐに削除されます。

12.3 最終ユーザーログイン試行の格納およびモニタリング

MarkLogic サーバーでは、ユーザーの最終ログイン試行時の結果を格納できます。このセクションでは、この機能について、およびこの機能の使用方法について説明します。以下のように構成されています。

- [最終ログインデータベースへの最終ユーザーログイン情報の格納](#)
- [ユーザーログインのモニタリング設定](#)
- [アプリケーションサーバーまたは管理画面の最終ログイン情報の表示](#)

12.3.1 最終ログインデータベースへの最終ユーザーログイン情報の格納

MarkLogic サーバーのインストール時（または 3.2 からのアップグレード時）に、Last-Login という名前のデータベースが作成されます。このデータベースは、1 つあるいは複数のアプリケーションサーバーの最終ログインデータベースとして使用できます。アプリケーションサーバー経由でログインが成功または失敗するたびに、その情報で最終ログインデータベースが更新されます。最終ログイン試行の情報のみが保持されます。このデータベースはログイン試行のたびに更新され続けるため（各リクエストが認証を受けるため、各リクエストによって最終ログインデータベースが更新されます）、コンテンツデータベースとは別のデータベースを最終ログインデータベースに使用することをお勧めします。一般に、この機能を使用するすべてのアプリケーションサーバーで共有される最終ログインデータベース 1 つを保持すれば問題ありません。ただしその場合は、情報がすべてのアプリケーションサーバーで共有されるという点に留意してください。つまり、最終ログイン時刻やその他の統計情報は、その最終ログインデータベースを使用するすべてのアプリケーションサーバーを対象にしているということです。

注： 成功したログイン試行の履歴は保持されません。成功した最終ログインの時刻のみがデータベースに格納されます。

12.3.2 ユーザーログインのモニタリング設定

あるアプリケーションサーバーのユーザーログインのモニタリングをセットアップするには、次の手順を実行します。

1. [Groups] アイコンをクリックします。
2. 設定するアプリケーションサーバーが存在するグループをクリックします（例えば Default）。
3. 左側のツリーメニューで [App Servers] アイコンをクリックします。
4. 最終ログインデータベースを設定するアプリケーションサーバーを選択します。[App Server Configuration] ページが表示されます。
5. 最終ログインデータベース用のデータベースを選択します。この目的用に Last-Login データベースが作成されますが、それ以外のデータベースを選択することもできます。最終ログインデータベースが選択されない場合、最終ログイン機能はオフになります。
6. 必要に応じて、[display last login] ラジオボタンで [true] を選択します。
7. [ok] をクリックして変更を保存します。

12.3.3 アプリケーションサーバーまたは管理画面の最終ログイン情報の表示

各アプリケーションサーバーの設定ページには `[display last login]` 設定があります。この設定の値は、`xdmp:user-last-login` API の XML 出力に含めて返されます。この情報をアプリケーションのロジックとして使用して、最終ログイン情報をアプリケーションに表示するかどうか決定できます。

管理画面では `[display last login]` 設定を使用して、最終ログイン試行に関する情報を表示します。最終ログインデータベースが設定されていて、`[display last login]` 設定が `true` の場合、次のようなメッセージが管理画面の各ページ下部に表示されます。

```
last successful login: September 2, 2008 7:54:16 PM
                        last unsuccessful login: none
unsuccessful login attempts since last login: 0
```

13.0 データベース

このセクションでは、データベースの基本的な管理手順について紹介します。このガイドの後半のセクションでは、データベースパフォーマンスのチューニングに関するコンセプトを紹介しています。データベースのバックアップおよびリストア操作については、「データベースのバックアップおよびリストア」(235 ページ)を参照してください。次のトピックから構成されています。

- [データベースについて](#)
 - [Schemas および Security データベース](#)
 - [Modules データベース](#)
 - [Triggers データベース](#)
 - [データベース設定](#)
 - [MarkLogic サーバーのデータベースの例](#)
- [新しいデータベースの作成](#)
- [データベースに対するフォレストのアタッチ/デタッチ](#)
- [データベース設定の表示](#)
- [ドキュメントをデータベースに読み込む](#)
- [データベースのマージ](#)
- [データベースの再インデックス付け](#)
- [データベースのクリア](#)
- [データベースの無効化](#)
- [データベースの削除](#)
- [データベース内にあるドキュメントのパーミッションの確認および設定](#)

この章では、管理画面を使用してデータベースを作成および設定する方法について説明します。データベースをプログラムによって作成および設定する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring Forests and Databases](#)」を参照してください。

13.1 データベースについて

MarkLogic サーバーの「データベース」は、フォレストと HTTP、WebDAV、XDBC サーバーとの間の抽象化レイヤーとして機能します。データベースは、同じクラスタ内のホストに設定されたデータ「フォレスト」で構成されます。ただし、同じグループ内にある必要はありません。クエリ目的で、1つあるいは複数のフォレストの集合を1つのまとまったコンテンツとして表すことができます。フォレストの詳細については、「フォレストについて」(290 ページ)を参照してください。

複数の HTTP、WebDAV、XDBC サーバーを 1 つのデータベースに接続できます。つまり 1 つの共通コンテンツベースを使って複数のアプリケーションを実行できます。データベースでは、複数のフォレストを複数のホストに分散できます。これによりハードウェアを増やしてデータを拡張できます。データベースの一貫性を保つために、同一データベースにアタッチされているフォレストはすべて利用可能になっている必要があります。

13.1.1 Schemas および Security データベース

インストールプロセスでは、デフォルトで「Documents」、「Last-Login」、「Schemas」、「Security」、「Modules」、「Triggers」という 5 つの「補助的な」データベースが作成されます。各データベースは、Security データベースと Schemas データベースをポイントします。セキュリティ設定情報は Security データベースに格納され、スキーマは Schemas データベースに格納されます。ドキュメントと同じリポジトリにセキュリティ情報およびスキーマが格納されている場合、データベースは、自身をセキュリティ用データベースならびにスキーマ用データベースとしてポイントできます。ただし、管理画面を使用して作成されたセキュリティオブジェクトは、デフォルトで「Security」データベースに格納されます。データベースのセキュリティ用データベースは、そのまま「Security」にしておくことをお勧めします。

13.1.2 Modules データベース

「Modules」データベースは、実行可能な XQuery、JavaScript、REST コードを格納するために使用される補助的なデータベースです。インストール時に「Modules」というデータベースが作成されますが、HTTP または XDBC サーバーで設定して、任意のデータベースをモジュール用データベースとして使用できます。また、実行可能なモジュール、クエリ可能なドキュメント、トリガーを格納するために同じデータベースを使用できます。

Modules データベースを使用する場合、このデータベース内の実行可能な各ドキュメントは、URI のプレフィックスとしてルート（HTTP または XDBC サーバーで指定）を持つ必要があります。また、WebDAV 経由でデータベース内のドキュメントにアクセスするには、automatic ディレクトリ作成がオンになっている必要があります。これは、WebDAV では automatic ディレクトリ作成が必須であるためです。ディレクトリおよびルートについては、「ディレクトリ」（66 ページ）および「サーバーのルートディレクトリ」（68 ページ）を参照してください。

例えば Modules データベースを使用していて、HTTP または XDBC サーバーのルートが `http://marklogic.com/` であると指定した場合は、そのサーバーから次のドキュメントが実行可能です。

```
http://marklogic.com/default.xqy
http://marklogic.com/myXQueryFiles/search_db.xqy
```

ただし、次のファイルは実行可能ではありません（URI がルートで始まらないため）。

```
http://mycompany.com/default.xqy  
/myXQueryFiles/search_db.xqy
```

Modules データベース内の任意のドキュメントを実行するには、ドキュメントが実行パーミッション付きで読み込まれている必要があります。このようにするには、実行パーミッションが含まれるデフォルト権限を持つユーザーとしてドキュメントを読み込むか、読み込み後のドキュメントにそのようなパーミッションを設定します。MarkLogic サーバーでパーミッション、権限、およびその他のセキュリティ機能を使用する方法については、「セキュリティ管理」（308 ページ）、および『*Application Developer's Guide*』のセキュリティ関連の章を参照してください。

13.1.3 Triggers データベース

「Triggers」データベースは、トリガーを格納するために使用される補助的なデータベースです。インストール時に、「Triggers」というデータベースが作成されますが、任意のデータベースをトリガー用データベースとして使用できます。また、実行可能なモジュール、クエリ可能なドキュメント、トリガーを格納するために同じデータベースを使用できます。Content Processing Framework を使用している場合、トリガー用データベースは必須です。Content Processing Framework の詳細については、『*Content Processing Framework Guide*』を参照してください。

13.1.4 データベース設定

各データベースには、メモリ割り当てやインデックス付けオプションなど、データベースのさまざまな側面を制御する設定があります。このような設定は、管理画面で行います。データベースごとに次のような基本的な設定を行えます。

- [基本的な管理設定](#)
- [ドキュメントに影響を与えるインデックス設定](#)
- [リバランサー設定](#)
- [再インデックス付け設定](#)
- [ドキュメントおよびディレクトリ設定](#)
- [メモリおよびジャーナル設定](#)
- [その他の設定](#)
- [マージ制御設定](#)

13.1.4.1 基本的な管理設定

管理設定では、データベース名やデータベースで使用するセキュリティデータベースおよびスキーマデータベースなどのプロパティを設定します。これらの設定は、管理画面で変更を加えるとすぐに有効になります。

データベース設定	説明
database name	データベースの名前。
security database	このデータベースがアクセスするセキュリティデータベースの名前。
schema database	このデータベースがアクセスするスキーマデータベースの名前。
triggers database	このデータベースがアクセスするトリガーデータベースの名前。
data encryption	このデータベースで保存データの暗号化をオンまたはオフにします。詳細については、『 <i>Security Guide</i> 』の「 Encryption at Rest 」を参照してください。
encryption key id	データ暗号化キー ID。詳細については、『 <i>Security Guide</i> 』の「 Encryption at Rest 」を参照してください。

13.1.4.2 ドキュメントに影響を与えるインデックス設定

データベースのいずれかのインデックス設定を変更すると、新しい設定は再インデックス付けがオンであるかどうか（`reindexer enable` が `true` に設定されているかどうか）に基づいて有効になります。テキストインデックスの詳細については、「テキストインデックス」（337 ページ）を参照してください。

一般に、インデックス付けオプションを追加すると、ドキュメントの読み込みが低速化し、データベースファイルのサイズが増加します。

データベース設定	説明
language	このデータベース内のコンテンツのデフォルト言語を指定します。 <code>xml:lang</code> 属性を持たないコンテンツは、ここで指定される言語でインデックス付けされます。英語以外の言語を指定する場合は、ライセンスキーが必要です。英語以外の言語を指定するときに、その言語のライセンスがないと、一般的なステミングおよびトークン化が適用されます。
stemmed searches	ワード検索に適用されるステミングのレベルを制御します。ステミング検索は、検索ワードの完全一致だけでなく、語幹と意味が同じワードもマッチします（例えば <code>be</code> の検索は、 <code>is</code> もマッチします）。ステミング検索の詳細については、『 <i>Search Developer's Guide</i> 』の「 Understanding and Using Stemmed Searches 」を参照してください。
word searches	ステミングなしのワード検索をオンにするかどうかを指定します。ワードの完全一致検索がオンになります。
word positions	フレーズ検索および <code>cts:near-query</code> 検索を高速にするために、ワードの位置をインデックス付けします。
fast phrase searches	いくつかの false positive の結果を除外することで、フレーズ検索をスピードアップします。
fast reverse searches	保存されたクエリをインデックス付けすることで、リバースクエリ検索をスピードアップします。
triple index	RDF トリプルインデックスをオンにして、RDF トリプルを使用した SPARQL 実行をサポートします。このパラメータが <code>true</code> の場合、 <code>sem:sparql</code> を使用できますが、ドキュメントの読み込みが低速化し、データベースファイルのサイズが大きくなります。 注： この機能には、有効なセマンティックライセンスキーが必要です。
triple positions	<code>cts:triple-range-query</code> 関数を使用する近接クエリのパフォーマンスをスピードアップするために、位置データをインデックス付けするかどうかを指定します。
fast case sensitive searches	いくつかの false positive の結果を除外することで、大文字 / 小文字を区別する検索をスピードアップします。
fast diacritic sensitive searches	一部の false-positive を除外することで、発音記号を区別する検索をスピードアップします。

データベース設定	説明
fast element word searches	いくつかの false positive の結果を除外することで、要素ワード検索をスピードアップします。
element word positions	要素ベースのフレーズ検索および <code>cts:near-query</code> 検索を高速にするために、要素ワード位置をインデックス付けします。
fast element phrase searches	いくつかの false positive の結果を除外することで、要素フレーズ検索をスピードアップします。
element value positions	<code>cts:element-value-query</code> を使用する要素ベースのフレーズ検索および <code>cts:near-query</code> 検索を高速にするために、要素ワード位置をインデックス付けします。
attribute value positions	<code>cts:element-value-query</code> を使用する属性ベースのフレーズ検索および <code>cts:near-query</code> 検索、および <code>cts:element-attribute-*-query</code> を使用する <code>cts:element-query</code> 検索を高速にするために、属性ワード位置をインデックス付けします。
field value searches	<code>cts:field-value-query</code> を使用する検索をオンにします。
field value positions	<code>cts:field-value-query</code> を使用する検索用に位置をオンにします。
three character searches	3 文字以上の連続する非ワイルドカード文字（例えば <code>abc*x</code> 、 <code>*abc</code> 、 <code>a?bcd</code> ）を含んでいる検索パターンで、ワイルドカード検索をオンにします。コードポイントワードレキシコンと組み合わせられると、（連続する非ワイルドカード文字が 3 文字よりも少ない検索も含めて）あらゆるワイルドカード検索のパフォーマンスを高速化します。MarkLogic では、three character search インデックスをコードポイントコレクションのワードレキシコンと組み合わせることを推奨しています。ワイルドカード検索の詳細については、『 <i>Search Developer's Guide</i> 』の「 Understanding and Using Wildcard Searches 」を参照してください。
three character word positions	3 文字のワイルドカードクエリ用にワード位置をインデックス付けします。
fast element character searches	ワイルドカード検索をオンにして、要素ベースのワイルドカード検索をスピードアップします。ワイルドカード検索の詳細については、『 <i>Search Developer's Guide</i> 』の「 Understanding and Using Wildcard Searches 」を参照してください。
trailing wildcard searches	検索パターンの末尾にワイルドカードがある（例えば <code>abc*</code> ）ワイルドカード検索を高速化します。ワイルドカード検索の詳細については、『 <i>Search Developer's Guide</i> 』の「 Understanding and Using Wildcard Searches 」を参照してください。

データベース設定	説明
trailing wildcard word positions	末尾ワイルドカード検索用にワード位置をインデックス付けします。
fast element trailing wildcard searches	特定要素内で検索パターンの末尾にワイルドカードがあるワイルドカード検索を高速化します。ただし、ドキュメントの読み込みが低速化し、データベースファイルのサイズが大きくなります。
word lexicon	データベース内のすべてのワードのレキシコンを保持します。一意性は、指定されたコレクションで決定されます。また、 <code>three character search</code> インデックスと連携してワイルドカード検索をスピードアップします。ワイルドカード検索の詳細については、『 <i>Search Developer's Guide</i> 』の「 Understanding and Using Wildcard Searches 」を参照してください。
two character searches	2文字以上の連続する非ワイルドカード文字（例えば、 <code>ab*</code> など）を含んでいる検索パターンで、ワイルドカード検索をオンにします。 <code>three character searches</code> とワードレキシコンがある場合、このインデックスは必要ありません。ワイルドカード検索の詳細については、『 <i>Search Developer's Guide</i> 』の「 Understanding and Using Wildcard Searches 」を参照してください。
one character searches	1文字の非ワイルドカード文字（例えば、 <code>a*</code> など）を含んでいる検索パターンで、ワイルドカード検索をオンにします。 <code>three character searches</code> とワードレキシコンがある場合、このインデックスは必要ありません。ワイルドカード検索の詳細については、『 <i>Search Developer's Guide</i> 』の「 Understanding and Using Wildcard Searches 」を参照してください。
uri lexicon	データベース内で使用されるすべての URI のレキシコンを保持します。URI レキシコンは、URI で制約するクエリを高速化します。これはデータベース内のすべての URI に対するレンジインデックスのようなものです。URI レキシコンから値にアクセスするには、 <code>cts:uris</code> または <code>cts:uri-match</code> API を使用します。
collection lexicon	データベース内で使用されるすべてのコレクション URI のレキシコンを保持します。コレクションレキシコンにより、コレクションに制約するクエリを高速化します。これはデータベース内のすべてのコレクション URI のレンジインデックスに似ています。コレクションレキシコンの値にアクセスするには、 <code>cts:collections</code> または <code>cts:collection-match</code> API を使用します。

13.1.4.3 リバランサー設定

データベースリバランサーをオンにして、データベース内のフォレスト間で自動的にコンテンツを均等に分散させることができます。データベースリバランスの詳細については、「データベースのリバランス」(178 ページ) を参照してください。

データベース設定	説明
assignment policy	データベースフォレスト間でドキュメントを分散する方法を指定します。リバランスプロセスおよびドキュメント読み込み / 挿入プロセスの両方がこのポリシーに従います。ドキュメント割り当てポリシーの詳細については、「リバランサーのドキュメント割り当てポリシー」(180 ページ) を参照してください。
rebalancer enable	true に設定すると、データベースリバランサーは、データベースフォレスト間でコンテンツを自動的に再分散します。false に設定すると、リバランスがオフになります。
rebalancer throttle	リバランス専用使用するシステムリソースのプライオリティを設定します。数字が大きいほどリバランスのプライオリティが高くなります。

13.1.4.4 再インデックス付け設定

再インデックス付け設定では、再インデックス付けをオンまたはオフにしたり、古いフラグメントを強制的に再インデックス付けしたりできます。

データベース設定	説明
reindexer enable	true に設定した場合、インデックス設定が変更されると、データベース全体のバックグラウンド再インデックス付け操作が自動的に開始されます。false に設定した場合、新しいインデックス設定はこれからデータベースに読み込まれるドキュメントで有効になり、既存のドキュメントは再読み込みされるか reindexer enable が true に設定されるまで古い設定のままになります。リインデクサーがクエリに与える影響については、「再インデックス付け設定をオンおよびオフにしたクエリ動作」(353 ページ) を参照してください。

データベース設定	説明
reindexer throttle	再インデックス付け専用を使用するシステムリソースのプライオリティを設定します。数字が大きいほど再インデックス付けのプライオリティが高くなります。
reindexer timestamp	フラグメントのタイムスタンプを指定し、再インデックス付け / 再フラグメント操作を強制的に実行します。[get current timestamp] ボタンをクリックすると、現在のシステムタイムスタンプが入力されます。このパラメータをタイムスタンプに設定し、reindex enable を true に設定した場合、指定されたタイムスタンプ以前のタイムスタンプを持つデータベース内のすべてのフラグメントで、再インデックス付けおよび再フラグメント操作が発生します。タイムスタンプが設定されているデータベースをリストアする場合、リストアされたコンテンツにフラグメントが存在し、指定されたコンテンツよりもそれらが古い場合、リストアされるとすぐに再インデックス付けが開始します。

13.1.4.5 ドキュメントおよびディレクトリ設定

ドキュメントおよびディレクトリの設定は、データベース内でドキュメントおよびディレクトリが作成される方法のデフォルト設定に影響を与えます。

データベース設定	説明
directory creation	<p>ドキュメントを作成した時点でディレクトリも自動的に作成されるかどうかを指定します。WebDAV サーバーや Modules データベースからアクセス可能なドキュメントを格納しているデータベースがある場合、これを <code>automatic</code> に設定する必要があります。以下の設定があります。</p> <ul style="list-style-type: none"> • <code>automatic</code> : ディレクトリはドキュメントの URI に基づいて自動作成されます。 • <code>manual-enforced</code> : URI に対応するディレクトリ階層がドキュメント作成前に存在している必要があります。ドキュメント作成時にそれに対応するディレクトリ階層が存在していない場合、エラーが発生します。例えば、次の URI のドキュメントを作成しようとした場合 : <code>http://marklogic.com/file.xml</code> URI が <code>http://marklogic.com/</code> であるディレクトリが存在する必要があります。存在しない場合は、エラーが発生します。この設定により、動作がファイルシステムと同じになります。 • <code>manual</code> : ディレクトリは自動作成されませんが、対応するディレクトリが存在しない状態でドキュメントが作成されます。 <p>ディレクトリの詳細については、「ディレクトリ」(66 ページ)を参照してください。Modules データベースの詳細については、「Modules データベース」(107 ページ)を参照してください。</p>
maintain last modified	<p>ドキュメントが作成または更新されるたびに、last-modified プロパティを作成および更新します。デフォルトは <code>true</code> です。</p>

データベース設定	説明
maintain directory last modified	ディレクトリが作成または更新されるたびに、ディレクトリの last-modified プロパティを作成および更新します。これが <code>true</code> の場合、ディレクトリ内のドキュメントを更新すると、このディレクトリの last-modified タイプスタンプも更新されます。この場合、ディレクトリ内で複数のドキュメントを更新しようとすると、競合（コンテンション）が発生する可能性があります。アプリケーションにおいて更新によるこのような競合が発生する場合（エラーログにデッドロック検知のメッセージが表示された場合など）、このプロパティを <code>false</code> に設定します。デフォルトは <code>false</code> です。
inherit permissions	<code>true</code> に設定した場合、ドキュメントおよびディレクトリは親ディレクトリからパーミッションを自動的に継承します（ドキュメントまたはディレクトリを作成したときにパーミッションが明示的に設定されていない場合）。ドキュメントまたはディレクトリを作成しているユーザーにデフォルトパーミッションが設定されている場合、そのパーミッションが継承されたパーミッションと組み合わせられます。
inherit collections	<code>true</code> に設定した場合、ドキュメントおよびディレクトリは親ディレクトリからコレクション設定を自動的に継承します（ドキュメントまたはディレクトリを作成したときにコレクションが明示的に設定されていない場合）。ドキュメントまたはディレクトリを作成しているユーザーにデフォルトコレクションが設定されている場合、そのコレクションが継承されたコレクションと組み合わせられます。
inherit quality	<code>true</code> に設定した場合、ドキュメントおよびディレクトリは親ディレクトリからクオリティ設定を自動的に継承します（ドキュメントまたはディレクトリを作成したときにクオリティが明示的に設定されていない場合）。

13.1.4.6 メモリおよびジャーナル設定

メモリおよびジャーナル設定は、インストール時に自動的に設定されます。メモリ設定はシステムのメモリ制限を設定し、ジャーナル設定はトランザクションジャーナル（データベーストランザクションが失敗した場合の復旧に使用）を制御します。ほとんどのシステムでは、デフォルト設定で十分です。システムの作業負荷によっては、メモリ設定がパフォーマンスに悪影響を与えることがあります。設定を変更する場合は、MarkLogic サポートにお問い合わせください。

データベース設定	説明
in memory limit	インメモリスタンド内のフラグメントの最大数。インメモリスタンドには、新しいまたは変更されたフラグメントの最新バージョンが含まれます。インメモリスタンドはフォレスト内の新しいスタンドとして定期的にディスクに書き込まれます。また、スタンドに累積するフラグメント数がこの制限を超える場合、スタンドはバックグラウンドスレッドによってディスクに自動的に保存されます。
in memory list size	インメモリリストストレージのサイズ（メガバイト）。
in memory tree size	インメモリツリーストレージのサイズ（メガバイト）。 in memory tree size は、データベースに読み込む予定の最大のテキストまたはスモールバイナリドキュメントよりも 1～2 メガバイト大きくする必要があります。スモールバイナリファイルの最大サイズは、常に large size threshold データベース設定による制約を受けます。
in memory range index size	インメモリレンジインデックスストレージのサイズ（メガバイト）。
in memory reverse index size	インメモリリバースインデックスストレージのサイズ（メガバイト）。
in memory triple index size	インメモリトリプルインデックスストレージのサイズ（メガバイト）。
large size threshold	ラージバイナリドキュメントをスタンドに直接格納するのではなく、ラージデータディレクトリに格納するためのしきい値となるサイズ（キロバイト）を指定します。このしきい値以下のバイナリはスモールバイナリファイルであるとみなされ、スタンドに格納されます。このしきい値より大きいバイナリはラージバイナリファイルであるとみなされ、ラージデータディレクトリに格納されます。

データベース設定	説明
locking	<p>トランザクションロックの堅牢度を指定します。<code>strict</code> に設定した場合、既存のドキュメントと新しいドキュメントで相互排他を適用します。<code>fast</code> に設定した場合、既存のドキュメントと新しいドキュメントで相互排他を適用しますが、新しいドキュメントに対してすべてのフォレストをロックするのではなく、ハッシュ関数を使用してロックするフォレストを1つ選択します。一般に、<code>strict</code> よりも高速になります。ただし、新しいフォレストが追加された後の短時間は、トランザクションによっては内部的に再試行が必要になることがあります。<code>off</code> に設定した場合、既存のドキュメントにも新しいドキュメントにも相互排他を適用しません。読み込んでいるすべてのドキュメントが新規（新規一括読み込みなど）であることが確かである場合のみ、この設定を使用してください。そうしないと、データベース内で重複した URI が作成されることがあります。</p>
journaling	<p>トランザクションジャーナリングの堅牢度を指定します。<code>strict</code> に設定した場合、ジャーナルによって MarkLogic サーバープロセス障害、ホストオペレーティングシステムカーネル障害、ホストハードウェア障害から保護されます。<code>fast</code> に設定した場合、ジャーナルによって MarkLogic サーバープロセス障害から保護されますが、ホストオペレーティングシステムカーネル障害やホストハードウェア障害からは保護されません。<code>off</code> に設定した場合、ジャーナルによって MarkLogic サーバープロセス障害、ホストオペレーティングシステムカーネル障害、ホストハードウェア障害から保護されません。</p>

データベース設定	説明
journal size	<p>各ジャーナルファイルのサイズ（メガバイト）。トランザクションが正常に完了しなかった場合、復旧操作にジャーナルファイルが使用されます。ほとんどのシステムでは、デフォルト値で十分です。デフォルト値は、システムのサイズに基づいてデータベース設定時に計算されます。ただし、その他のメモリ設定を変更する場合、ジャーナルサイズは <code>in memory list size</code> および <code>in memory tree size</code> の和と等しくする必要があります。さらに、レンジインデックスデータがジャーナルスペースを占めることがあるため、レンジインデックスを使用する場合は（特に、大量のレンジインデックスを使用する場合や、レンジインデックスのサイズが非常に大きい場合）、ジャーナルサイズに余裕を持たせる必要があります。また、ジャーナルが存在するフォレスト内にあるドキュメントだけでなくトランザクション内にあるすべてのドキュメントのロック情報を各ジャーナルが保持する必要があるため、トランザクションが複数のフォレストに渡る場合もジャーナルサイズを追加する必要があります。</p> <p>ジャーナルサイズを変更した場合は、次回新しいジャーナルが作成されるときに新しいサイズ制限が使用されます。既存のジャーナルは、新しいジャーナルと交換されるとき（例えばジャーナルがいっぱいになったとき、フォレストがクリアされたとき、システムがクリーンシャットダウンして再起動したとき）まで古いサイズ制限を使用し続けます。</p>
preallocate journals	8.0-4 の時点で、この設定は無効です。
preload mapped data	<p>フォレストがデータベースにマウントされるときに、メモリにマッピングされたデータ（例えばレンジインデックスやワードレキシコン）をメモリに読み込むかどうかを指定します。メモリにマッピングされたデータを事前読み込みすると、クエリのパフォーマンスが向上しますが、使用するメモリ量が増加します（特に多くのレンジインデックスやレキシコンがある場合）。また、データベース起動時に大量のディスク I/O が発生するため、マッピングされたデータがメモリに読み取られるときにシステムパフォーマンスが低下します。マッピングされたデータを事前読み込みしない場合、ページングが必要なデータをクエリでリクエストするとメモリに動的にページングされるため、クエリの応答時間が長くなります。</p>
range index optimize	<p>レンジインデックスを最適化する方法を指定します。<code>facet-time</code> に設定した場合、レンジインデックスは CPU の使用時間を最小化するように最適化されます。<code>memory-size</code> に設定した場合、メモリの使用量を最小化するように最適化されます。</p>

13.1.4.7 その他の設定

残りのデータベース設定オプションは次のとおりです。

データベース設定	説明
<code>position list max size</code>	<p>任意のタームに関するインデックスの位置リスト部分の最大サイズ（メガバイト）。タームの位置リストサイズが指定された制限より大きくなると、そのタームの位置情報が破棄されます。デフォルト値は 128、最小値は 1、最大値は 512 です。例えば、頻繁に出現するワード（「a」、「an」、「the」など）がこの制限に達すると、その位置クエリ（<code>cts:near-query</code>）はインデックスを使用せずに解決されます。このような種類のワードはインデックスを使用せずに解決されますが、この制限によって、データベースに実際に読み込まれるコンテンツに関してインデックスのサイズが小さくなり効率が良くなるため、パフォーマンスが向上します。</p>
<code>format compatibility</code>	<p>リクエストの検証中にこのデータベースのインデックスに MarkLogic サーバーが適用するバージョン互換性を指定します。この値を <code>automatic</code> 以外に設定すると、すべてのフォレストデータが指定されたオンディスク形式になり、インデックス互換性情報の自動確認がオフになります。自動検出は、データベース起動時とデータベース設定変更後に発生し、フォレストのサイズが非常に大きい場合やクラスタの規模が非常に大きい場合は、時間やシステムリソースを消費することがあります。ほとんどのインストールでは、デフォルト値 <code>automatic</code> が推奨されます。</p>
<code>index detection</code>	<p>コンテンツと現在のデータベース設定の間のインデックス互換性を自動検出するかどうかを指定します。この検出は、データベース起動時とデータベース設定変更後に発生し、フォレストのサイズが非常に大きい場合やクラスタの規模が非常に大きい場合は、時間やシステムリソースを消費することがあります。<code>none</code> に設定した場合は、一部の設定で再インデックス付けが完了していな場合でも、クエリで現在のデータベースインデックス設定を使用します。ほとんどのインストールでは、デフォルト値 <code>automatic</code> が推奨されます。</p>

データベース設定	説明
expunge locks	指定されたタイムアウトで、 <code>xdmp:lock-acquire</code> を使用して作成されたロックフラグメントを MarkLogic サーバーが自動抹消するかどうかを指定します。 <code>none</code> に設定した場合、ロックフラグメントは <code>xdmp:lock-release</code> を使用して明示的に削除するまでロックが期限切れになった後も（ドキュメントをロックしなくなっても）データベースに残ります。非常に大規模なクラスタでクラスタの起動時間をスピードアップする場合に限り、 <code>none</code> に設定することが推奨されます。ほとんどのインストールでは、デフォルト設定の <code>automatic</code> （ロックが期限切れになったときにロックをクリーンアップする）が推奨されます。
tf normalization	ドキュメントのサイズに基づいてターム頻度をスケールリングするデフォルトの TF (term-frequency) 正規化 (<code>scaled-log</code>) を使用するのか、ドキュメントサイズに関係なく、実際のターム頻度の関数としてターム頻度をドキュメントで使用する <code>unscaled-log</code> を使用するのか、デフォルトのドキュメントサイズベースのスケールリングよりも影響が小さい中間レベルのスケールリングを選択するのかを指定します。

13.1.4.8 マージ制御設定

マージ制御設定では、マージの発生タイミングを制御したり、マージパラメータを設定したり、マージを発生させないブラックアウト期間をセットアップしたりできます。マージ制御設定にアクセスするには、管理画面メニュー項目で [Database] > [データベース名] > [Merge Controls] をクリックします。マージを行わないと最適なデータベースパフォーマンスが実現されないため、マージパラメータの調整やマージブラックアウトの使用は慎重に行ってください。マージ制御設定について、およびマージ制御の詳細については、「データベースのマージの概要と制御」（162 ページ）を参照してください。

13.1.5 MarkLogic サーバーのデータベースの例

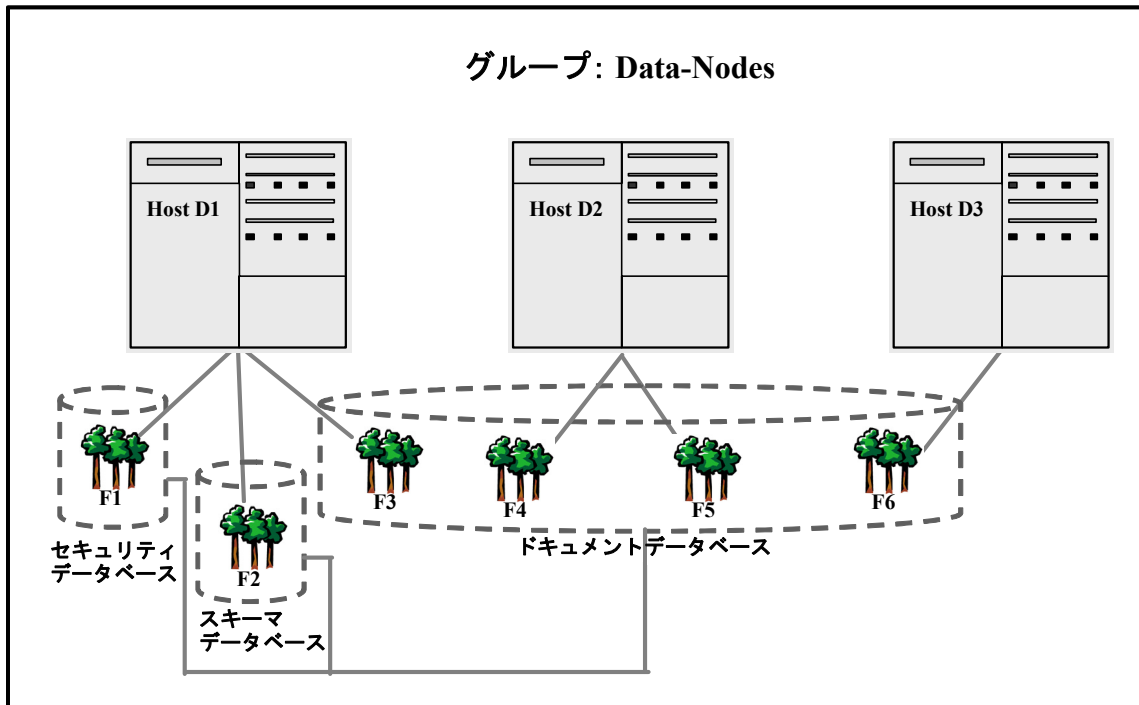
このセクションでは、データベースの概念と、MarkLogic サーバーのデータベース、ホスト、およびフォレストの間の関係を、例を挙げて説明します。

以下の図で、Host D1、D2、D3 は Data-Nodes グループに属しています。

D1 は、MarkLogic サーバーが読み込まれている Data-Nodes グループの最初のホストです。デフォルトで 3 つのデータベースが作成されます。セキュリティデータベース、スキーマデータベース、ドキュメントデータベースです。以下の図で、Host D1 上に 3 つのフォレスト F1、F2、F3 が構成され、それぞれセキュリティデータベース、スキーマデータベース、ドキュメントデータベースに割り当てられています。

D2 は、Data-Nodes グループに参加する 2 つめのホストです。D2 上にフォレスト F4 と F5 が構成され、ドキュメントデータベースにアタッチされています。

D3 は、Data-Nodes グループに参加する 3 つめのホストです。これにはフォレスト F6 が構成されています。F6 もドキュメントデータベースに割り当てられています。



13.2 新しいデータベースの作成

新しいデータベースを作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. 右上の [Create] タブをクリックします。[Create Databases] ページが表示されます。

database – The database specification.

database name
The database name.
Required. You must supply a value for database-name.

security database
The security database.

schema database
The database that contains schemas.

triggers database
The database that contains triggers.

3. データベースの名前を入力します。このデータベースを参照する際、システムはこの名前を使用します。
4. このデータベースに関連付けるセキュリティデータベースを選択します。セキュリティデータベースには「*Security*」を選択することをお勧めします。
5. このデータベースに関連付けるスキーマデータベースを選択します。
6. 残りのパラメータは変更しなくても問題ありません。必要に応じて設定してください。
7. [ok] をクリックします。

データベースが作成されます。これでフォレストをデータベースにアタッチできます。データベースの作成は「ホット」管理タスクです。

13.3 データベースに対するフォレストのアタッチ/デタッチ

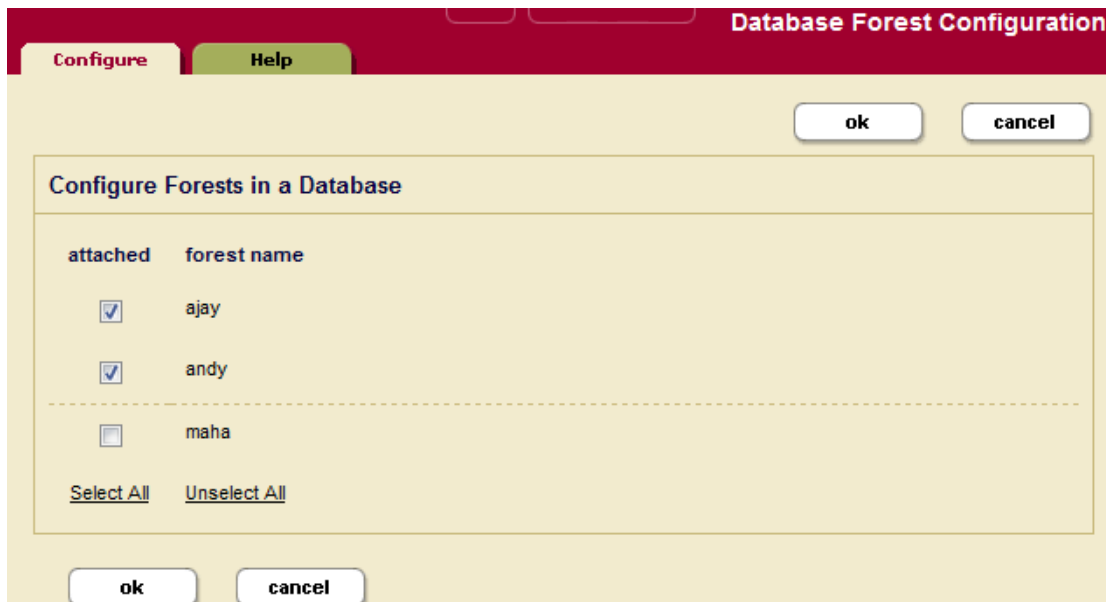
フォレスト内のコンテンツに対してクエリを実行するには、フォレストがデータベースにアタッチされている必要があります。フォレストは、あるデータベースからデタッチして別のデータベースにアタッチすることで、データベース間を移動できます。フォレストをデータベースからデタッチしても、そのフォレストは削除されません。フォレストは作成されたホスト上に残り、データは変更されません。フォレストは、あるデータベースからデタッチして別のデータベースにアタッチすることで、データベース間を移動できます。ただし、フォレストを別のデータベースにアタッチする前に、新しいデータベースが古いデータベースと同じ設定であることを確認してください。新しいデータベースの設定が異なっていて、新しいデータベースで `reindex enable` 設定が `true` に設定されている場合、フォレストは新しいデータベース設定と一致するように、アタッチされるとすぐに再インデックス付けを開始します。

注： ジャーナルアーカイブ機能（「ジャーナルアーカイブがオンのデータベースバックアップ」(242 ページ) を参照) を利用するデータベースに新しいフォレストをアタッチすると、フォレストは次回のデータベースバックアップまでジャーナルアーカイブに参加しません。データベースの即時バックアップを実行する方法の詳細については、「データベースの即時バックアップ」(245 ページ) を参照してください。

また、[Forest Summary] ページを使用して、データベースに対してフォレストをアタッチおよびデタッチすることもできます。詳細については、「[Forest Summary] ページを使用したフォレストのアタッチおよびデタッチ」(298 ページ) を参照してください。

管理画面を使用してデータベースに対して1つあるいは複数のフォレストをアタッチまたはデタッチするには、次の手順を実行します。

1. フォレストをアタッチするデータベースをクリックします。
2. データベースの [Forests] アイコンをクリックします。[Database Forest Configuration] ページが表示されます。



3. データベースにアタッチするフォレストに対応するチェックボックスをオンにします。データベースからデタッチするフォレストは、チェックボックスをオフにします。
4. [ok] をクリックします。

アタッチまたはデタッチしたフォレストがデータベース設定に反映されます。データベースに対するフォレストのアタッチおよびデタッチは「ホット」管理タスクです。

13.4 データベース設定の表示

特定データベースの設定を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、設定を表示するデータベースを見つけます。
3. 設定を表示するデータベースの名前をクリックします。

4. 設定を表示します。
5. [Forests]、[Triggers]、[Content Processing]、[Fragment Roots]、[Fragment Parents]、[Element-Word-Query-Throughs]、[Phrase-Throughs]、[Phrase-Arounds]、[Element Indexes]、[Attribute Indexes] をクリックして、データベースのこれらの設定を表示します。

13.5 ドキュメントをデータベースに読み込む

管理画面を使用して、ドキュメントをデータベースに読み込むことができます。ドキュメントはデフォルトのパーミッションで読み込まれ、管理画面にログインしたユーザーのデフォルトコレクションに追加されます。

複数のドキュメントを同時にデータベースに読み込むには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ドキュメントを読み込むデータベースをクリックします。
3. 右上近くにある [Load] タブをクリックします。



4. ドキュメントを含むディレクトリの名前を入力します。このディレクトリは、管理画面を現在実行しているホストからアクセスする必要があります。
5. 読み込むドキュメントの名前のフィルタを入力します (xml 拡張子を持つすべてのファイルを読み込む場合は *.xml)。完全一致の場合は、ドキュメントの完全な名前を入力します。
6. [ok] をクリックして続行します。
7. 読み込み確認画面に、指定されたフィルタに一致する、指定されたディレクトリ内のすべてのドキュメントがリストされます。[ok] をクリックして読み込みを完了させます。

ドキュメントがデータベースに読み込まれます。ドキュメントの URI パスはファイルシステムのパスと同じです。

13.6 データベースのマージ

管理画面を使用して、データベース内にあるすべてのフォレストデータをマージできます。「データベースのマージの概要と制御」(162 ページ) で説明するように、データベース内のフォレストをマージすると、パフォーマンスが向上します。これは MarkLogic サーバーによってバックグラウンドで定期的に自動実行されます。[merge] ボタンを使用すると、このデータベースのフォレストデータを明示的にマージできます。

データベースを明示的にマージするには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. マージするデータベースを決定します。
3. ツリーメニューまたは [Summary] タブで、データベース名をクリックします。
[Database Configuration] ページが表示されます。
4. [Database Configuration] ページで、[merge] ボタンをクリックします。
確認メッセージが表示されます。
5. このデータベース内にあるフォレストデータをマージすることを確認し、[ok] をクリックします。

データベース内のデータのマージは「ホット」管理タスクなので変更はすぐに有効になります。

13.7 データベースの再インデックス付け

管理画面を使用して、データベース内にあるすべてのドキュメントデータを再インデックス付けできます。「テキストインデックス」(337 ページ) で説明するように、テキストをインデックス付けすると、特定のクエリのパフォーマンスが向上します。これは MarkLogic サーバーによってバックグラウンドで定期的に自動実行されます。再インデックス付け操作では、[reindexer.timestamp](#) が現在のシステムタイムスタンプに設定されます。これにより、このタイムスタンプ以前であるデータベース内のすべてのフラグメントで、再インデックス付けおよび再フラグメント操作が発生します ([reindexer.enable](#) が true の場合)。[reindex] ボタンを使用すると、データベースで完全な再インデックス付け / 再フラグメント操作が実行されます。

データベースを再インデックス付けするには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. 再インデックス付けするデータベースを決定します。

3. ツリーメニューまたは [Summary] タブで、データベース名をクリックします。
[Database Configuration] ページが表示されます。
4. [Database Configuration] ページで、[reindex] ボタンをクリックします。
確認メッセージが表示されます。
5. このデータベースを再インデックス付けすることを確認し、[ok] をクリックします。

データベース内のデータの再インデックス付けは「ホット」管理タスクなので変更はすぐに有効になります。

13.8 データベースのクリア

管理画面を使用して、データベースからすべてのフォレストコンテンツをクリアできません。データベースをクリアすると、データベース内にあるすべてのフォレストからすべてのコンテンツが削除されますが、データベース設定は変更されません。

データベースからすべてのデータをクリアするには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. クリアするデータベースを決定します。
3. ツリーメニューまたは [Summary] タブで、データベース名をクリックします。
[Database Configuration] ページが表示されます。
4. [Database Configuration] ページで、[clear] ボタンをクリックします。
確認メッセージが表示されます。
5. このデータベースからフォレストデータをクリアすることを確認し、[ok] をクリックします。

データベースのクリアは「ホット」管理タスクなので変更はすぐに有効になります。

13.9 データベースの無効化

管理画面を使用して、データベースを無効にできます。データベースのみを無効にすることも、データベースとそのすべてのフォレストを無効にすることもできます。データベースのみを無効にすると、データベースが無効としてマークされ、すべてのフォレストがデータベースから切り離されます。ただし、データベースのフォレストは有効なままです。データベースとそのフォレストを無効にすると、データベースと各フォレストが無効としてマークされ、すべてのフォレストがデータベースから切り離され、データベースのすべてのフォレストのすべてのメモリキャッシュがクリアされます。データベースが無効の間は、どのようなクエリ操作にも使用できません。

データベースを無効にしても、設定やドキュメントのデータは削除されません。
[enable] をクリックすると、データベースやフォレストを後で再度オンにできます。

データベースを無効にするには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. 無効にするデータベースを決定します。
3. ツリーメニューまたは [Summary] タブで、データベース名をクリックします。

[Database Configuration] ページが表示されます。

4. [Database Configuration] ページで、[Disable] ボタンをクリックします。

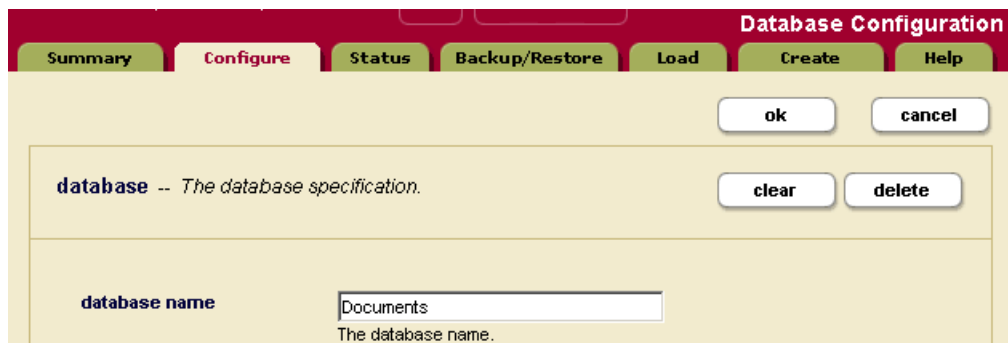
確認メッセージが表示されます。

5. [disable database] をクリックしてデータベースのみを無効にするか、[disable database and forests] をクリックしてデータベースとそのフォレストを無効にします。

13.10 データベースの削除

データベースを参照している HTTP、WebDAV、または XDBC サーバーが存在する場合、そのデータベースは削除できません。データベースを削除すると、アタッチされているフォレストはデタッチされますが、削除はされません。フォレストは作成されたホスト上に残り、データは変更されません。データベースを削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、削除するデータベースを見つけます。
3. 削除するデータベースの名前をクリックします。



4. 右上近くにある [delete] ボタンをクリックします。

注： [clear] ボタンをクリックすると、このデータベースにアタッチされているすべてのフォレストがクリアされ、そのフォレストからすべてのデータが削除されます。[delete] ボタンをクリックすると、データベース設定は削除されますが、フォレストに格納されているデータは削除されません。

5. そのデータベースを参照している HTTP、WebDAV、または XDBC サーバーが存在しない場合は、削除確認画面が表示されます。[ok] をクリックします。
6. データベースで使用されているフォレストを削除するには、各フォレストについて「ホストからのフォレストの削除」(305 ページ) で説明する手順を実行します。

これでデータベースが恒久的に削除されます。データベースの削除は「ホット」管理タスクです。

13.11 データベース内にあるドキュメントのパーミッションの確認および設定

管理画面を使用して、データベース内のドキュメントまたはディレクトリのパーミッションを確認できます。また、`xdmp:document-get-permissions` および

`xdmp:document-set-permissions` API を使用して、パーミッションを取得および設定できます。ドキュメントパーミッションの詳細については、『*Security Guide*』を参照してください。

管理画面を使用してデータベース内のドキュメントまたはディレクトリのパーミッションを確認または設定するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、パーミッションを確認または設定するデータベースを見つけます。
3. パーミッションを確認または設定するドキュメントが格納されているデータベースの名前をクリックします。[Database Configuration] ページが表示されます。
4. 左側のツリーメニューで選択されたデータベースの [Permissions] リンクをクリックします。[Permissions Admin] ページが表示されます。
5. ドキュメントまたはディレクトリの URI を入力し、[ok] をクリックします。
6. パーMISSIONを変更する場合は、ドロップダウンリストからロールおよび機能を選択します。さらにパーMISSIONを追加する場合は、[more permissions] ボタンをクリックします。
7. 変更をコミットするには、[ok] をクリックします。操作をキャンセルするには、[cancel] を押します。

14.0 ワードクエリデータベースの設定

この章では、`cts:word-query` 操作に対して、要素を含めたり除外したりするようにデータベースを設定する方法、インデックス設定を追加する方法、その他の設定変更を実行する方法について説明します。次のトピックから構成されています。

- [ワードクエリ設定について](#)
- [カスタマイズされたワードクエリ設定](#)

14.1 ワードクエリ設定について

MarkLogic サーバーにおけるワードおよびフレーズの基本検索は、クエリコンストラクタ `cts:word-query` に基づきます。ワードクエリのデータベース設定を変更することで、基本検索の動作を制御できます。ワードクエリで要素を除外したり含めたり、データベース設定で設定されたオプションと比較して、さらにインデックス付けオプションを追加したりできます。このセクションでは、ワードクエリ設定で使用可能なオプションについて説明します。以下のように構成されています。

- [設定オプションの概要](#)
- [含有および除外される要素について](#)
- [含まれる要素の関連度を増減するための重みの追加](#)
- [含まれる要素の属性値の指定](#)
- [インデックスオプション設定について](#)

14.1.1 設定オプションの概要

ワードクエリをデータベースで解決する方法を制御するためにワードクエリ設定で設定できる主なオプションを次に示します。

- デフォルトでは、すべての要素がワードクエリ設定に含まれ、インデックス付けオプションはデータベースのインデックス付けオプションと同じです。
- すべてのワードクエリ設定は、データベース単位で設定されます。
- ワードクエリ設定は、`cts:word-query`、`cts:words`、および `cts:word-match` API の動作を制御します。インデックス付けされるワードの制御や、クエリ評価のフィルタ（エバリュエータ）部分から返されるワードの制御などがあります。
- ワードクエリは、そのインデックス設定の基礎として、データベースのインデックス設定を継承します。
- ワードクエリ用にインデックスオプションを追加できます。追加されるインデックスオプションは、他のクエリ（例えば `cts:element-word-query`、`cts:element-attribute-word-query`）に影響を及ぼしません。
- データベース設定でオンになっているインデックス付けオプションはオフにできません。

- データベースでオンになっているインデックスオプションをワードクエリでオンにしても、動作は変更されません。ただしその後、ワードクエリ設定でオンになっているインデックス設定をデータベースでオフにすると、ワードクエリではオンのまま維持されます。
- ワードクエリでは名前付きの要素を含めたり除外したりできます。
- またオプションとして、含める要素に制約を課すことができます（指定した属性の値を使用します）。
- 含める要素の場合、重みを指定することもできます。この重みは関連度スコアの計算に使われます。要素内のマッチにおいて、重みが 1.0 より大きい場合はスコアがブーストされ、1.0 より小さい場合にはスコアが低くなります。

14.1.2 含有および除外される要素について

ワードクエリでは要素を含めたり除外したりできます。一部の要素コンテンツを検索しないようにする場合に便利です。このセクションでは、ワードクエリ設定で要素を含めたり除外したりしたときに、ワードクエリに含める、または除外するコンテンツを MarkLogic サーバーが決定する方法について説明します。

注： ワードクエリ内のすべてを検索できるようにしながら、一部の要素を含めたり除外したりするコンテンツの特殊なビューを必要とする場合は、ワードクエリ設定を修正するのではなく、フィールドを作成することを検討してください。フィールドの詳細については、「データベースのフィールド設定」（140 ページ）を参照してください。

デフォルトでは、すべての要素コンテンツ（要素のすべての子テキストノード）がワードクエリに含まれます。ワードクエリで任意の要素を含めたり除外したりする場合は、未指定の要素のどれがインデックス付けされ、どれがインデックス付けされないのかが規定するルールがあります。このルールは、親要素からの含有状態（含める / 除外する）の継承に基づきます。例えば、親要素が含まれる要素としてマークされている（したがって、ワードクエリに対してインデックス付けされ、評価される）場合、その子は、除外リストに出現しない限り、親と同様に含まれます。

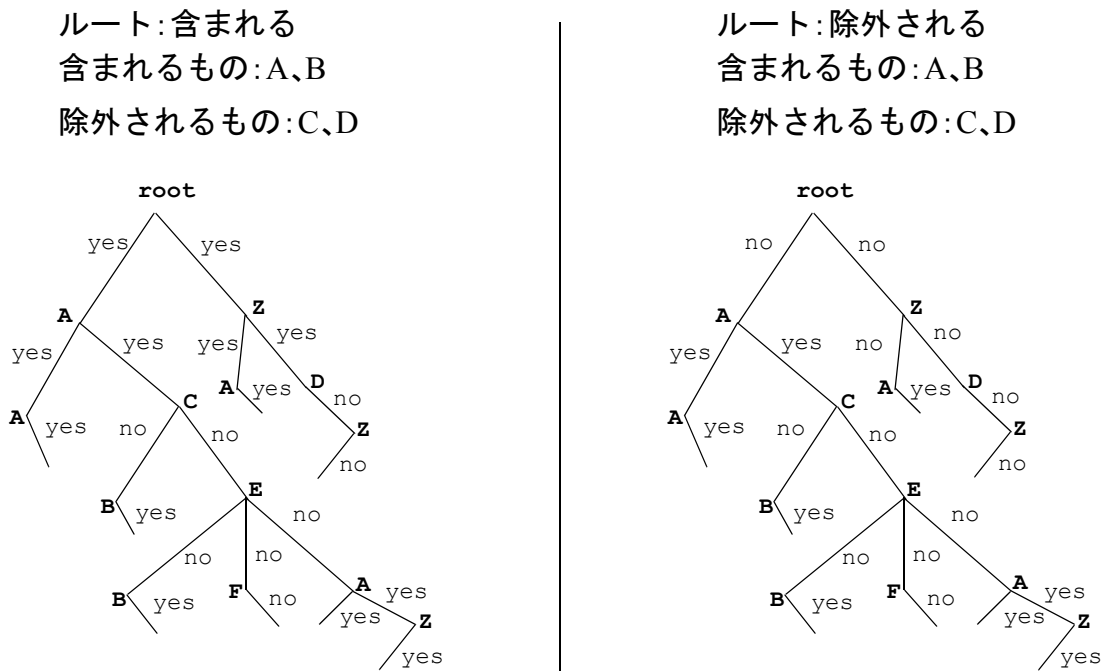
含めたり除外したりする要素を MarkLogic サーバーが決定するときに、次のルールを使用して XML ツリーを移動します。

1. ドキュメントのルートノードから開始します。
2. ルートノードが含まれる場合（明示的に含まれているため、または `include document root` が `true` に設定されているため）、MarkLogic サーバーはドキュメントルート要素の直接の子テキストノードを含めてから、その子要素に移動します。ルートノードが除外される場合、テキストノードを含めずに、MarkLogic サーバーはその子要素へと XML ツリーを下に移動します。
3. 親要素（この場合はルート要素）が含まれていた場合、MarkLogic サーバーはツリーを下に移動し続け、明示的に除外される要素が出現するまで子テキストノードを含め続けます。

4. 親要素（この場合はルート要素）が含まれていなかった場合、MarkLogic サーバーはツリーを下に移動し続け、明示的に含まれる要素が出現するまで子テキストノードを除外し続けます。
5. MarkLogic サーバーはツリーを下に移動し続け、親要素から継承した状態に従って含め続けるか除外し続けます。含まれる要素（継承が「除外」状態の場合）または除外される要素（継承が「含める」状態の場合）が次に出現するまで、状態が継承され続けます。
6. このプロセス中に、含まれず除外もされない要素が出現した場合は、親要素の含有状態（「除外」または「含める」）を継承します。
7. MarkLogic サーバーは、このロジックを使用してドキュメントの末尾に達するまで XML ツリーを下に移動し続け、含有状態を決定します。

要素の子テキストノードが確実に含まれるようにする唯一の方法は（含まれたり除外されたりする要素がある場合）、その要素を含有リストに追加することであり、要素が確実に含まれないようにする唯一の方法は、その要素を除外リストに追加することです。

2つの設定で含まれるものを次の図に示します。一方はルートノードが含まれる場合、もう一方はルートノードが含まれない場合です。含まれるものならびに除外されるものが、どちらの場合でも同じであることに注意してください。要素名の下に線はテキストノードを表し、「yes/no」はテキストノード内のコンテンツがワードクエリに含まれるかどうかを示しています。root は XML 構造のルートノードを表し、要素 A および B が含まれ、要素 C および D が除外されます。明示的に含めたり除外したりしていない要素（例えば E、F、Z）は、親から継承します。



線はテキストノード、「yes」は含まれること、「no」は除外されることを示す

Z ノード（明示的に含めたり除外したりしない）は、親要素の含有状態に応じて含まれる場合も除外される場合もあることに注意してください。

14.1.3 含まれる要素の関連度を増減するための重みの追加

要素を含める場合、含まれる要素の指定に重み (weight) を追加できます。重みを追加すると、この要素内のすべてのテキスト (要素のすべての子孫テキストノード内のあらゆるテキストを含む) が指定された値で重み付けされ、クエリ時に関連度が変更されません。要素内のマッチにおいて、指定する重みが 1.0 より大きい場合はスコアがブーストされ、1.0 より小さい場合にはスコアが低くなります。

重みを指定すると、その値と要素内のトークン (子孫テキストノード内のトークンを含む) のターム頻度が乗算されます。この処理は、ドキュメントの読み込み、更新、または再インデックス付けで発生します。例えば、重み 2.0 を指定した場合、各タームのターム頻度は 2.0 になり、各タームが 2 回出現した場合と同等になります (スコア計算目的の場合)。同様に、重み 0.5 を指定した場合、各タームのターム頻度は 0.5 になります。

注： 重みの増加はターム頻度に影響するため、ターム頻度が含まれるスコア計算アルゴリズムの関連度順のみに影響し (例えば `logtf/idf` や `logtf`)、重みを考慮しないスコア計算アルゴリズムは重みの影響を受けません (例えば `score-simple`)。

重みを追加すると、ある要素でマッチが発生するような検索のスコアを増減するのに便利です。例えば、`TITLE` 要素内のマッチが、その他の要素内のマッチよりも大きく関連度スコアに影響するようにする場合は、重み 2.0 を `TITLE` 要素に指定できます。逆に、`TITLE` 要素内のマッチが、その他の要素内のマッチよりも小さく関連度スコアに影響するようにする場合は、重み 0.5 を `TITLE` 要素に指定できます。関連度の計算方法の詳細については、『*Search Developer's Guide*』の章「[Composing cts:query Expressions](#)」を参照してください。

14.1.4 含まれる要素の属性値の指定

要素を含める場合、属性値を指定できます。これにより、特定の属性 / 値ペアを持つ要素のみを含めることができます。属性 / 値ペアは、コンテンツを制約するための条件として機能します。例えば、次の XML スニペットについて考えてみましょう。

```
<chapter class="history">some text here</chapter>
<chapter class="mathematics">some more text here</chapter>
<chapter class="english">some other text here</chapter>
<chapter class="history">some different text here</chapter>
<chapter class="french">other text here</chapter>
<chapter class="linguistics">still other text here</chapter>
```

要素 `chapter` について、`class` および `history` の属性 / 値ペアを指定した場合は、次の要素のみが含まれます。

```
<chapter class="history">some text here</chapter>
<chapter class="history">some different text here</chapter>
```

属性値は含まれる要素については指定できますが、除外される要素については指定できません。

14.1.5 インデックスオプション設定について

ワードクエリ設定では、データベース設定で現在設定されているインデックス付けオプションの他に、インデックス付けオプションを追加できます。ワードクエリ設定にインデックスオプションを追加しても、要素ベースのインデックスオプションには追加されません。

特定のインデックスオプションをワードクエリに追加するには、インデックスオプションに対応するチェックボックスをオンにします。データベース設定でオンになっていないインデックスオプションを追加すると、新しいドキュメントや更新されたドキュメントはワードクエリで新しいインデックス付けを使用し、データベース設定で `reindex enable` が true に設定されている場合は再インデックス操作がトリガーされます。

データベース設定でオンになっているオプションは、ワードクエリ設定では太字で表示されます。太字のオプションの横にあるチェックボックスをオンにした場合、設定は変更されません。ただしその後、そのインデックスオプションをデータベース設定でオフにすると、ワードクエリでそのチェックボックスがオンになっている限り、ワードクエリではオンの状態が維持されます。

14.2 カスタマイズされたワードクエリ設定

このセクションでは、ワードクエリ設定をカスタマイズする手順について説明します。フィールドのさまざまな設定オプションの意味の詳細については、「ワードクエリ設定について」(132 ページ)を参照してください。データベースのワードクエリ設定を修正する手順は次のとおりです。

注： ワードクエリ設定を修正すると、その修正は `cts:word-query` コンストラクタ (`cts:search` のデフォルトコンストラクタ) を使用するすべてのクエリに適用されます。ワードクエリ内のすべてを検索できるようにしながら、一部の要素を含めたり除外したりするコンテンツの特殊なビューを必要とする場合は、ワードクエリ設定を修正するのではなく、フィールドを作成することを検討してください。フィールドの詳細については、「データベースのフィールド設定」(140 ページ)を参照してください。

管理画面を使用して新しいフィールド設定をデータベースに追加するには、次の手順を実行します。

1. ブラウザで管理画面にアクセスします。
2. ツリーメニューまたは [Summary] タブで、ワードクエリ設定を変更するデータベースに移動してクリックします。
3. フィールドを作成するデータベースで、[Word Query] リンクをクリックします。[Word Query Configuration] ページが表示されます。

4. データベースのインデックスオプションの他にインデックスオプションをワードクエリに含める場合は、そのインデックス設定のチェックボックスをオンにします。太字で表示されているインデックス設定は、その設定がデータベース設定から継承されていることを示します。詳細については、「インデックスオプション設定について」(136 ページ) を参照してください。
5. ワードクエリにドキュメントのルート要素を含める場合、それを明示的に含めない場合でも、include root (ドキュメントルートを含める) ボタンをデフォルトの `true` のままにします。 `false` に設定した場合、ワードクエリから結果を得るためには、ワードクエリ設定で要素を含める必要があります。通常、この設定は `true` のままにしておき、明示的に除外あるいは含める要素を選択します (スコア付けの重みや属性値の制約を追加することもできます)。
6. [ok] をクリックして変更を保存します。変更が MarkLogic サーバー設定に加えられた後、設定ページが更新されます。
7. ワードクエリから要素を除外する場合は、[Excludes] タブをクリックします。
8. 名前空間 URI を適宜入力し、除外される要素のローカル名を入力します。

Add Word Query Exclude

Configure Includes **Excludes** Help

ok cancel

excluded element -- *The element included in word query.*

namespace uri
A namespace URI.

localname
The localname of the excluded element.
Required. You must supply a value for localname.

ok cancel

9. [ok] をクリックします。
10. 除外する各要素について、手順 [7](#) ~ [9](#) を繰り返します。

11. [Includes] タブをクリックし、ワードクエリに含める要素を指定します。

included element -- *The element included in word query.*

namespace uri
A namespace URI.

localname
The localname of the included element.
Required. You must supply a value for localname.

weight
The weight, used to boost or lower relevance scores, of the included element.

attribute namespace uri
Namespace of the child attribute.

attribute localname
Localname of the child attribute.

attribute value
Include only elements with the specified attribute having this value.

12. [Included Element] ページで、含める要素のローカル名を指定します。要素が名前空間内にある場合は、含める要素の名前空間 URI を指定します。
13. (オプション) この要素内のマッチの関連度への影響を増減する場合は、重みにデフォルトの 1.0 以外を指定します。重みが 1.0 より大きいと関連度への影響が増加し、1.0 より小さいと影響が減少します。
14. (オプション) 指定された値の属性を持つ要素のみを含める場合は、属性の名前空間 URI (適宜)、属性のローカル名、および属性の値を入力します。指定された値の属性が含まれる要素のみが含まれます。値を完全に指定してください (ワイルドカード文字は使用しないでください)。
15. この要素についてすべての項目を指定したら、[ok] をクリックします。
16. 含める各要素について、手順 [11](#) ~ [15](#) を繰り返します。

17. 含めたり除外したりするフィールドは、フィールド設定ページの下部にあるテーブルから削除できます。

The screenshot shows a dialog box with a light beige background. At the top, it is titled "Included Elements". Below this title is a table with the following columns: "Localname", "Namespace", "Attribute", "Attribute Namespace", "Value", and "Weight". A single row is present in the table with the following values: "ABSTRACT", an empty field, an empty field, an empty field, "2.0", and "[delete]". Below the "Included Elements" section is another section titled "Excluded Elements". This section has a table with two columns: "Localname" and "Namespace". A single row is present with the following values: "script", "http://www.w3.org/1999/xhtml", and "[delete]". At the bottom of the dialog box, there are two buttons: "ok" and "cancel".

Localname	Namespace	Attribute	Attribute Namespace	Value	Weight
ABSTRACT				2.0	[delete]

Localname	Namespace	
script	http://www.w3.org/1999/xhtml	[delete]

ok cancel

15.0 データベースのフィールド設定

この章では、データベース設定でフィールドを設定する方法について説明します。フィールドは、`cts:field-word-query`、`cts:field-words`、`cts:field-word-match` の各 API、およびフィールドレキシコン API で使用し、検索できる複数の要素で構成される名前付きフィールドを定義できます。次のトピックで構成されています。

- [フィールドの概要](#)
- [フィールド設定について](#)
- [フィールドワードレキシコンとフィールド値レキシコン](#)
- [フィールドの設定](#)

この章では、管理画面を使用してフィールドを作成および設定する方法について説明します。フィールドをプログラムによって作成および設定する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Adding a Database Field and Included Element](#)」を参照してください。フィールド上のレキシコンの詳細については、『*Search Developer's Guide*』の「[Browsing With Lexicons](#)」を参照してください。

15.1 フィールドの概要

フィールドを使用すると、XML 要素の QName または JSON プロパティ名に基づいて、データベースの一部を簡単にクエリできます。コレクションやディレクトリでは、ドキュメント URI に基づいてデータベースの一部にだけクエリを実行することができました。一方フィールドでは、XML 要素および JSON プロパティ名に基づいてデータベースの一部にだけクエリを実行できます。これはアプリケーション開発者にとって便利です。またデータベースの一部に対してクエリを実行する際に、他の方法よりもパフォーマンスに優れています。1 つあるいは複数の要素や JSON プロパティにひとまとまりで簡単かつ効率的にクエリしたいコンテンツがあるときに、フィールドを使用すると便利です。

フィールドクエリはワードクエリに似ています（デフォルト設定で、すべてが含まれる場合）が、フィールドクエリではデータベース内のすべてを対象にクエリするのではなく、指定されたフィールドに設定された内容のみを対象にクエリします。フィールドには独自のインデックスの集合があり、これはデータベースインデックスとは関係ありません。フィールドは通常、データベース全体の小さなサブセットであり、また独自のインデックスがあるため、フィールドのクエリは、同じ XML 要素や JSON プロパティを（例えば `cts:word-query` を使用して）直接クエリするよりも、多くの場合効率がよくなります。

また、フィールドの関連度は、フィールド独自のインデックスによりフィールド内のコンテンツに基づいて計算されます（データベース内のすべてのコンテンツではなく）。このため、フィールド検索の関連度は、その他の検索の場合と比べてきめ細かく設定できます。

フィールドを使用すると、ひとまとまりとしてクエリするコンテンツの部分を作成できます。さらに、データベースで設定されたインデックス付けオプションの上位に、インデックス付けオプションをフィールドに設定できます。例えば、多くの技術記事が含まれるデータベースを考えてみましょう。各記事には、短い概要が含まれています。記事の他の部分から検索する機能よりも概要から検索する機能が優れたアプリケーションを構築できます。ここで本文にはワイルドカードインデックスがないが、概要に対してワイルドカード検索を行いたい場合を考えてみます。この場合、概要に関するフィールドを作成し、そのフィールドにワイルドカードインデックスを追加します。フィールドはコンテンツ全体のごく一部なので、追加のインデックス付けにかかる相対コストは小さくなります。

JSON コンテンツと XML コンテンツのインデックス付けは若干異なります。このため、この 2 種類のコンテンツでフィールド値クエリおよびフィールドレンジクエリの動作に相違点があります。詳細については、『*Application Developer's Guide*』の「[How Field Queries Differ Between JSON and XML](#)」を参照してください。

15.2 フィールド設定について

MarkLogic サーバーにおけるワードおよびフレーズのフィールド検索は、クエリコンストラクタ `cts:field-word-query` に基づきます。クエリするフィールドのデータベース設定を変更することで、フィールド検索の動作を制御できます。パスフィールドおよびルートフィールドで要素を除外したり含めたりできるほか、一部の要素にインデックス付けオプションを追加できます。このセクションでは、設定で使用可能なオプションについて説明します。以下のように構成されています。

- [フィールド設定オプションの概要](#)
- [ルートフィールドおよびパスフィールド](#)
- [メタデータフィールド](#)
- [インデックスオプション設定について](#)

15.2.1 フィールド設定オプションの概要

指定フィールドに対するフィールドクエリに設定できる主なオプションを次に示します。

- デフォルトでは、フィールドクエリ設定には XML 要素や JSON プロパティは含まれておらず、インデックス付けオプションはデータベースのインデックス付けオプションと同じです。フィールドに何か含めるためには、含める 1 つ以上の要素またはプロパティを指定する必要があります。
- すべてのフィールド設定は、データベース単位で設定されます。
- フィールド設定は、`cts:field-word-query`、`cts:field-value-query`、`cts:field-range-query`、`cts:field-words`、および `cts:field-word-match` API の動作を制御します。インデックス付けされるタームの制御や、クエリ検証のフィルタ（エバリュエータ）部分から返されるタームの制御などがあります。

- フィールドは、そのインデックス設定の基礎として、データベースのインデックス設定を継承します。
- 各フィールド用にインデックスオプションを追加できます。追加されるインデックスオプションは、他のクエリに影響を及ぼしません（例えば `cts:word-query`、`cts:element-word-query`、`cts:element-attribute-word-query`、`cts:json-property-word-query`）。
- データベースでオンになっているインデックスオプションにワードクエリでオンにしても、動作は変更されません。ただしその後、フィールド設定でオンになっているインデックス設定をデータベースでオフにすると、フィールドではオンのまま維持されます。
- パスフィールドおよびルートフィールドで名前付きの XML 要素や JSON プロパティを含めたり除外したりできます。
- またオプションとして、含める XML 要素に制約を課すことができます（指定した XML 要素属性の値を使用します）。
- パスフィールドまたはルートフィールドに含める XML 要素や JSON プロパティの場合、重みを指定することもできます。この重みは関連度スコアの計算に使われます。要素またはプロパティ内のマッチにおいて、重みが 1.0 より大きい場合はスコアがブーストされ、1.0 より小さい場合にはスコアが低くなります。
- 各フィールドには独自のインデックスの集合があります。これらのインデックスはワードクエリインデックスとは共有されません。そのため、フィールドの要素がワードクエリよりも少ない場合、インデックス付けするコンテンツの量は少なくなり、インデックスからクエリを解決する（クエリ処理のインデックス解決フェーズ）ために必要な I/O 操作は少なくなります。

フィールドには 3 種類あります。

- [ルートフィールド](#)
- [パスフィールド](#)
- [メタデータフィールド](#)

ルートフィールドおよびパスフィールドについては、「ルートフィールドおよびパスフィールド」（142 ページ）を参照してください。メタデータフィールドについては、「メタデータフィールド」（148 ページ）を参照してください。

15.2.2 ルートフィールドおよびパスフィールド

ルートフィールドまたはパスフィールドでは要素を含めたり除外したりできます。一部の要素コンテンツを検索しないようにする場合に便利です。このセクションでは、フィールド設定で要素を含めたり除外したりするときに、フィールドに含める、または除外するコンテンツを MarkLogic サーバーが決定する方法について説明します。

このセクションでは、設定で使用可能なオプションについて説明します。以下のように構成されています。

- [ルートフィールド](#)
- [パスフィールド](#)
- [含有および除外される要素をフィールド設定で決定する方法](#)
- [含まれる要素またはプロパティの関連度を増減するための重みの追加](#)
- [含まれる要素または除外される要素の属性値の指定](#)

15.2.2.1 ルートフィールド

ルートフィールドは、ドキュメント内における相対位置に関係なく、ドキュメント要素を含めたり除外したりします。ルートフィールドではドキュメントルートから開始して要素を含めるのか除外するのかを選択できます。デフォルトでは、すべての要素コンテンツ（要素のすべての子テキストノード）がフィールドに含まれません。

15.2.2.2 パスフィールド

パスフィールドでは、含まれる要素および除外される要素はパスで識別されるサブツリーに制約されます。例えば、フィールドのパスが `/A/B/C` である場合は、ノード `C` 内の要素（`A/B/C/D`、`A/B/C/D/E`、`/A/B/C/Z` など）がフィールドで含まれたり除外されたりします。

パスフィールドには 1 つあるいは複数のパスを含めることができます。複数のパスは、パスの和集合として扱われます。したがって、それぞれのパスは、あるドキュメントにおけるフィールドインスタンスのルートを識別します。

パスで一部の要素に名前空間プレフィックスが含まれる場合、名前空間はパスレンジインデックスの場合と同じ方法で定義される必要があります。詳細については「パスレンジインデックスおよびフィールドで使用される名前空間プレフィックスの定義」（372 ページ）を参照してください。

フィールドのパスが単一のノードまたは属性で終了している場合、含有 / 除外定義は効果がありません。

各パスには重みを設定できます。重みは、パスの影響を受けるテキストの関連度を増減するために使用されます。

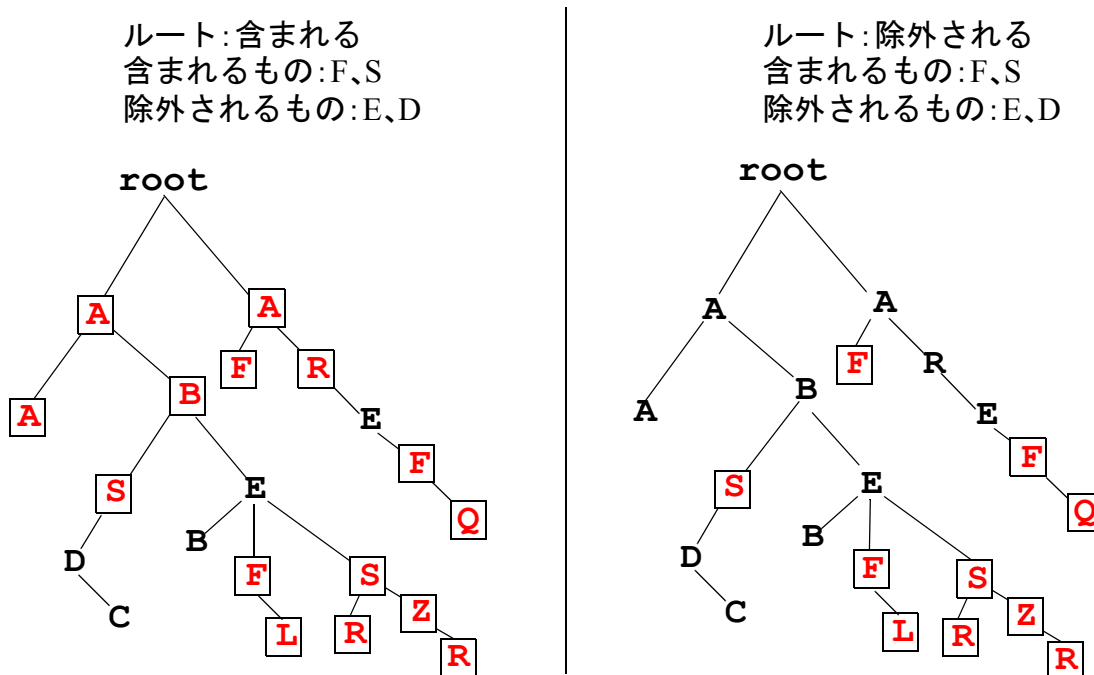
15.2.2.3 含有および除外される要素をフィールド設定で決定する方法

パスフィールドやルートフィールドを定義したら、含めたり除外したりするドキュメント要素を選択できます。含めたり除外したりする要素を MarkLogic サーバーが決定するときに、次のルールを使用して XML ツリーを移動します（これらはワードクエリ設定で要素を含めたり除外したりする場合に使用されるルールと同じです）。

1. ドキュメントのルートノードから開始します。
2. フィールドの種類がパスの場合、明示的に含まれる要素および除外される要素はパスで識別されるサブツリーに制約されます。その他のすべての要素が除外されます。
3. フィールドの種類がルートで、ルート要素が含まれる場合（明示的に含まれている、または `include document root` が `true` に設定されているため）、MarkLogic サーバーはドキュメントルート要素の直接の子テキストノードを含めてから、その子要素に移動します。ルート要素が除外される場合、テキストノードを含めずに、MarkLogic サーバーはその子要素へと XML ツリーを下に移動します。
4. 親要素が含まれていた場合、MarkLogic サーバーはツリーを下に移動し続け、明示的に除外される要素が出現するまで子テキストノードを含め続けます。
5. 親要素が含まれていなかった場合、MarkLogic サーバーはツリーを下に移動し続け、明示的に含まれる要素が出現するまで子テキストノードを除外し続けます。
6. このプロセス中に、含まれず除外もされない要素が出現した場合は、親要素の含有状態（「除外」または「含める」）を継承します。MarkLogic サーバーはツリーを下に移動し続け、親要素から継承した状態に従って含め続けるか除外し続けます。含まれる要素（親が「除外される」場合）または除外される要素（親が「含まれる」場合）が次に出現するまで、状態が継承され続けます。
7. MarkLogic サーバーは、このロジックを使用してドキュメントの末尾に達するまで XML ツリーを下に移動し続け、各要素の含有状態を決定します。

要素の子テキストノードが確実に含まれるようにする唯一の方法は（含まれたり除外されたりする要素がある場合）、その要素を含有リストに追加することであり、要素が確実に含まれないようにする唯一の方法は、その要素を除外リストに追加することです。

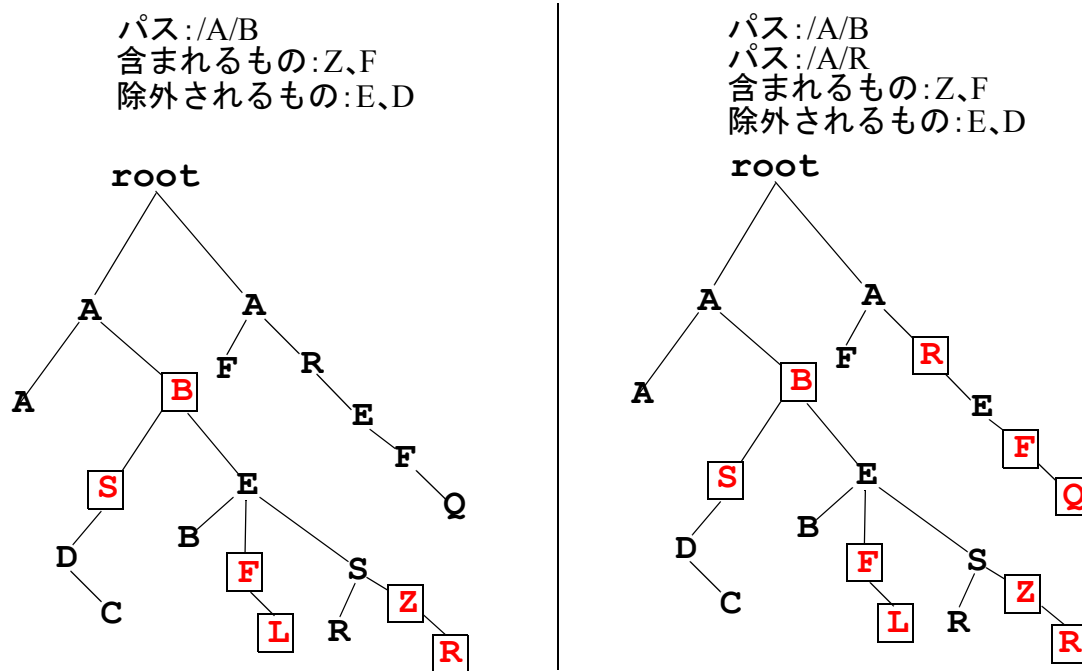
考えられる 2 つのルートフィールド設定で含まれるものを次の図に示します。一方はルートノードが含まれる場合、もう一方はルートノードが含まれない場合です。含まれるものならびに除外されるものが、どちらの場合でも同じであることを注意してください。要素名の下線はテキストノードを表し、四角で囲まれた赤字はテキストノード内のコンテンツがワードクエリに含まれることを示しています。root は XML 構造のルートノードを表し、要素 F および S が含まれ、要素 E および D が除外されます。明示的に含めたり除外したりしていない要素（例えば A、B、C）は、親から継承します。



線はテキストノード、四角で囲まれた赤字は含まれること、黒字は除外されることを示す

A、B、および R ノード（明示的に含めたり除外したりしない）は、親要素の含有状態に応じて含まれる場合も除外される場合もあることに注意してください。

考えられる 2 つのパスフィールド設定で含まれるものを次の図に示します。一方はシングルパスの場合、もう一方は 2 つのパスの場合です。ルートフィールド設定について示した前出の図と同様に、含まれるものならびに除外されるものが、どちらの場合でも同じです。



線はテキストノード、四角で囲まれた赤字は含まれること、黒字は除外されることを示す

15.2.2.4 含まれる要素またはプロパティの関連度を増減するための重みの追加

XML 要素または JSON プロパティを含める場合、含まれる要素またはプロパティの指定に重み (weight) を追加できます。重みを追加すると、この要素内のすべてのテキスト (要素のすべての子孫テキストノード内のあらゆるテキストを含む) が指定された値で重み付けされ、クエリ時に関連度を変更されます。要素内のマッチにおいて、指定する重みが 1.0 より大きい場合はスコアがブーストされ、1.0 より小さい場合にはスコアが低くなります。

重みを指定すると、その値と要素内のトークン (子孫テキストノード内のトークンを含む) のターム頻度が乗算されます。この処理は、ドキュメントの読み込み、更新、または再インデックス付けで発生します。例えば、重み 2.0 を指定した場合、各タームのターム頻度は 2.0 になり、各タームが 2 回出現した場合と同等になります (スコア計算目的の場合)。同様に、重み 0.5 を指定した場合、各タームのターム頻度は 0.5 になります。

注: 重みの増加はターム頻度に影響するため、ターム頻度が含まれるスコア計算アルゴリズムの関連度順のみに影響し (例えば `logtf/idf` や `logtf`)、重みを考慮しないスコア計算アルゴリズムは重みの影響を受けません (例えば `score-simple`)。

重みを追加すると、ある要素でマッチが発生するような検索のスコアを増減するのに便利です。例えば、`TITLE` 要素内のマッチが、その他の要素内のマッチよりも大きく関連度スコアに影響するようにする場合は、重み `2.0` を `TITLE` 要素に指定できます。逆に、`TITLE` 要素内のマッチが、その他の要素内のマッチよりも小さく関連度スコアに影響するようにする場合は、重み `0.5` を `TITLE` 要素に指定できます。関連度の計算方法の詳細については、『*Search Developer's Guide*』の章「[Composing cts:query Expressions](#)」を参照してください。

フィールドに重みの異なる 2 つ以上の要素があり、その 1 つが別の要素の子である場合、親要素の重みが使用され、子要素の重みは無視されます。例えば `test` という名前のフィールドがあり、要素 `A` および `B` を含むとします。`A` の重みは `10`、`B` の重みは `2` です。`cts:field-value-query("test", ("Foo")), "unfiltered")` が含まれる検索クエリで返される結果は、次のドキュメントの場合、重み `10` に基づいて計算されます。

```
<A>
  <B>Foo</B>
</A>
```

15.2.2.5 含まれる要素または除外される要素の属性値の指定

要素を含める場合、属性値を指定できます。これにより、特定の属性 / 値ペアを持つ要素のみを含めたり除外したりできます。属性 / 値ペアは、コンテンツを制約するための条件として機能します。例えば、次の XML スニペットについて考えてみましょう。

```
<chapter class="history">some text here</chapter>
<chapter class="mathematics">some more text here</chapter>
<chapter class="english">some other text here</chapter>
<chapter class="history">some different text here</chapter>
<chapter class="french">other text here</chapter>
<chapter class="linguistics">still other text here</chapter>
```

要素 `chapter` について、`class` および `history` の属性 / 値ペアを指定した場合は、次の要素のみが含まれます。

```
<chapter class="history">some text here</chapter>
<chapter class="history">some different text here</chapter>
```

同様に、除外される要素を設定するときには、除外される要素の属性値を指定できます。

15.2.3 メタデータフィールド

メタデータは、有効なシステムタイムスタンプやアーカイブ情報を格納するためにテンポラルドキュメントで使用されます。詳細については『*Temporal Developer's Guide*』を参照してください。ドキュメントのメタデータは、非テンポラルドキュメントで管理することもできます。

ルートフィールドやパスフィールドとは異なり、メタデータフィールドでは検索に含めたり除外したりする要素を定義しません。その代わりに、ドキュメントに関連したキー/値の組み合わせを定義して、そのドキュメントの外部に格納します。

メタデータフィールドは、フィールドを取る API 関数を使用して操作できます。例えば、メタデータフィールドでは次のすべての操作を実行できます。

- `cts:field-word-query` および `cts:field-value-query` 関数を使用してクエリを実行する。
- メタデータフィールドでワードレキシコンを作成し、`cts:field-words` および `cts:field-word-match` 関数で使用する。
- メタデータフィールドでレンジインデックスを作成し、`cts:field-range-query`、`cts:field-values`、`cts:field-value-match`、および `cts:field-value-ranges` 関数で使用する。
- メタデータフィールドレンジインデックスのレンジインデックスリファレンスを作成し、`cts:values`、`cts:value-match`、`cts:value-ranges`、`cts:value-co-occurrences`、`cts:value-tuples`、および `cts:ordering` 関数で使用する。
- トークナイザーオーバーライドを設定する。
- ステミング検索を設定する。
- ワード検索を設定する。
- フィールド値検索を設定する。
- 高速フレーズ検索を設定する。
- 高速大文字 / 小文字区別検索を設定する。
- 高速発音記号区別検索を設定する。
- 末尾ワイルドカード検索を設定する。
- 3 文字検索を設定する。
- 2 文字検索を設定する。
- 1 文字検索を設定する。

テンポラルドキュメントのメタデータは、テンポラル API によって管理されます。詳細については『*Temporal Developer's Guide*』の「[Managing Temporal Documents](#)」を参照してください。非テンポラルドキュメントの場合、メタデータをドキュメントとともに挿入するには、`xdmp.documentInsert` または `xdmp.documentLoad` 関数を使用します。ドキュメントのメタデータを追加または修正するには、`xdmp.documentPutMetadata` および `xdmp.documentSetMetadata` 関数を使用します。ドキュメントのメタデータを返すには、`xdmp.documentGetMetadata` および `xdmp.documentGetMetadataValue` 関数を使用します。

メタデータは、ドキュメントノードと関連付けることもできます。ノードのメタデータは、`xdmp.nodeMetadata` および `xdmp.nodeMetadataValue` 関数を使用して管理されます。

15.2.4 インデックスオプション設定について

フィールド設定では、データベース設定で現在設定されているインデックス付けオプションの他に、インデックス付けオプションを追加できます。フィールド設定にインデックスオプションを追加しても、データベースレベルでは要素ベースのインデックスオプションには追加されません。

特定のインデックスオプションをフィールドに追加または削除するには、インデックスオプションに対応するチェックボックスをオンまたはオフにします。データベース設定でオンになっていないインデックスオプションを追加すると、新しいドキュメントや更新されたドキュメントはフィールドで新しいインデックス付けを使用し、データベース設定で `reindex enable` が `true` に設定されている場合は再インデックス操作がトリガーされます。

データベース設定でオンになっているオプションは、フィールド設定では太字で表示されます。データベース設定におけるフィールド設定とデータベースフィールド設定におけるフィールド設定は、合わせて論理和集合を形成します。例えば、フィールド設定で太字のオプションの横にあるポッチェックボックスをオフにしても、データベース設定の同等のオプションは変更されません。データベースのフィールド設定をオフにするには、そのオプションのデータベース設定とフィールド設定を一致させる必要があります。

15.3 フィールドワードレキシコンとフィールド値レキシコン

ワードレキシコンと同様に、各フィールドにワードレキシコンを作成できます。「フィールドワードレキシコン」は、フィールドに出現するデータベース内にある一意のワードの、すべてのリストです。このリストは、指定されたコレクションで順に並んでいます。同じフィールド上に、異なるコレクションで複数のフィールドレキシコンを作成できます。フィールドワードレキシコンにアクセスするには、`cts:field-words` および `cts:field-word-match` API を使用します。

要素または属性レキシコンと同様に、フィールドに値レキシコンを作成できます。「フィールド値レキシコン」は、フィールドに出現するデータベース内にある一意の値の、すべてのリストです。フィールド値レキシコンを作成するには、フィールドレンジインデックスを定義します。

レキシコンの詳細については、『*Search Developer's Guide*』の「[Browsing With Lexicons](#)」を参照してください。

15.4 フィールドの設定

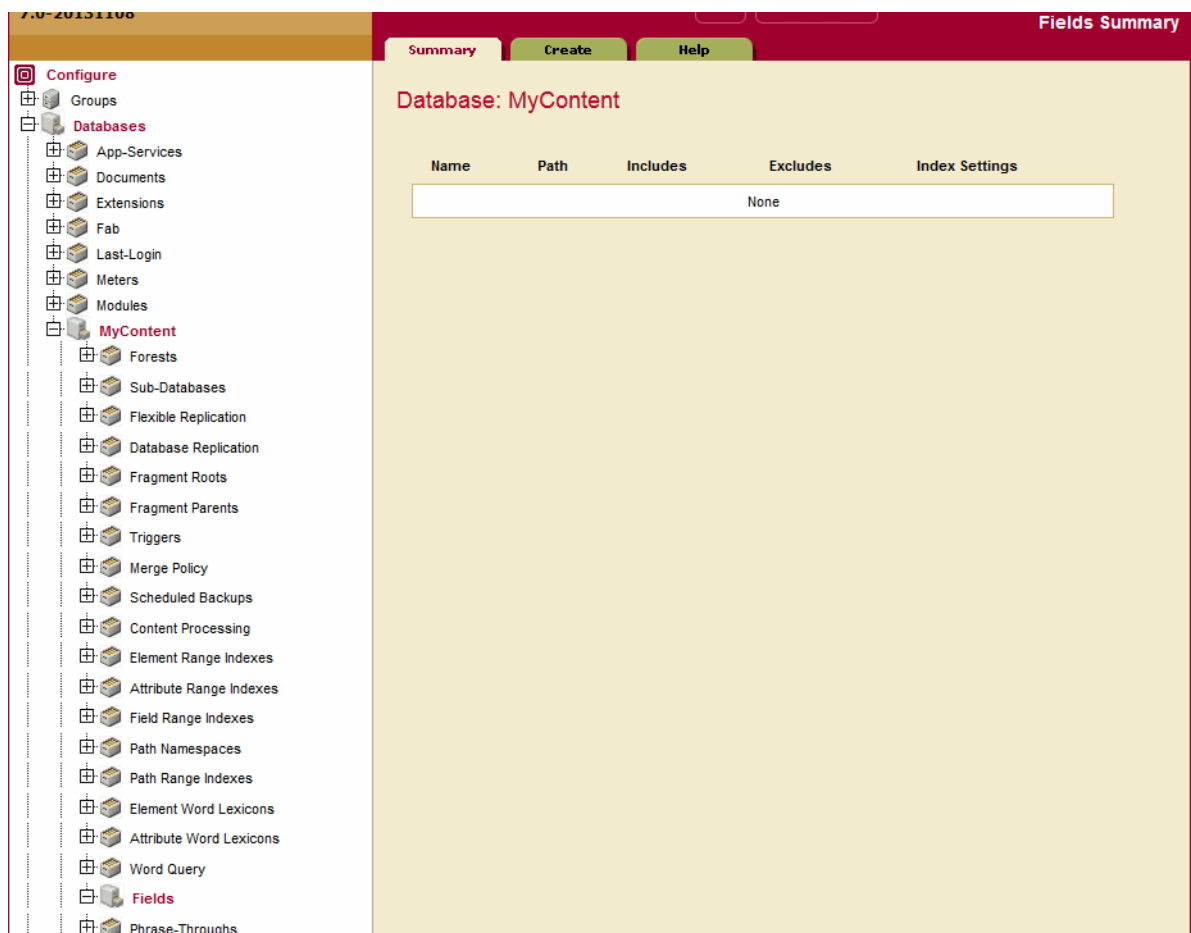
このセクションでは、データベースのフィールド設定を作成および修正する手順について説明します。フィールドのさまざまな設定オプションの意味の詳細については、「フィールド設定について」(141 ページ)を参照してください。このセクションでは、次の手順について説明します。

- [新しいパスフィールドまたはルートフィールドの設定](#)
- [新しいメタデータフィールドの設定](#)
- [既存フィールドの修正](#)
- [フィールドのレンジインデックスの作成](#)

15.4.1 新しいパスフィールドまたはルートフィールドの設定

管理画面を使用して新しいフィールド設定をデータベースに追加するには、次の手順を実行します。

1. ツリーメニューまたは [Summary] タブで、フィールドを作成するデータベースに移動してクリックします。
2. フィールドを作成するデータベースで、[Fields] リンクをクリックします。[Field Summary] ページが表示されます。



3. [Create] タブをクリックします。[Create Field in Database] ページが表示されます。
4. フィールドの名前を入力します。
5. デフォルトでは、フィールドの種類はパスです。パスフィールドを作成する場合は、パス式を入力します。このパス内のマッチの関連度への影響を増減する場合は、重みにデフォルトの 1.0 以外を指定します。重みが 1.0 より大きいと関連度への影響が増加し、1.0 より小さいと影響が減少します。複数のパスを定義する場合は、[more field paths] をクリックします。

Software pre-release expires in 69 days

Summary Create Help

ok cancel

Create Field in Database

field name
MyPathField
The field name.
Required. You must supply a value for field-name.

field type
 paths root metadata

field path

path
/A/B
The path expression. For example:/prefix1:locname1 /prefix2:locname2...

weight
1.0
The weight, used to boost or lower relevance scores.

more field paths

6. 必要な数のパスを入力します。

The screenshot shows the 'Create Field in Database' dialog box. It has three tabs: 'Summary', 'Create', and 'Help'. The 'Create' tab is active. At the top right, there are 'ok' and 'cancel' buttons. The main content area is titled 'Create Field in Database' and contains the following fields:

- field name:** A text input field containing 'MyPathField'. Below it, the text reads: 'The field name. Required. You must supply a value for field-name.'
- field type:** Three radio buttons: 'paths' (selected), 'root', and 'metadata'.
- field path:** A container for multiple path entries. Each entry consists of a 'path' text input field and a 'weight' text input field. The first entry has a path of '/A/B' and a weight of '1.0'. The second entry has a path of '/B/A' and a weight of '1.0'. Below the second entry is a 'more field paths' button.

7. (オプション) フィールドレンジインデックスまたはトークナイザーオーバーライドを作成します。後で戻って追加することもできます。

8. データベースのインデックスオプションの他にインデックスオプションをフィールドに含める場合、またはフィールドから何らかのインデックスオプションを削除する場合は、該当するインデックス設定のチェックボックスをオンまたはオフにします。太字で表示されているインデックス設定は、その設定がデータベース設定から継承されていることを示します。データベースレベルの設定から設定を継承しない場合は、継承されているインデックス設定のチェックボックスをオフにします。詳細については、「インデックスオプション設定について」（149 ページ）を参照してください。

index settings

- stemmed searches:** basic
- word searches
- field value searches
- field value positions
- fast phrase searches**
- fast case sensitive searches**
- fast diacritic sensitive searches**
- trailing wildcard searches**
- trailing wildcard word positions
- three character searches
- three character word positions
- two character searches
- one character searches

Options in bold inherited from database config

9. ルートフィールドを作成する場合は、フィールドの種類をルートに設定します。ほとんどの場合、パスフィールドで必要な設定が得られるため、ルートフィールドの作成が必要になることはあまりありません。

Summary Create Help

ok cancel

Create Field in Database

field name: MyRootField
The field name.
Required. You must supply a value for field-name.

field type: paths root metadata

10. ルートフィールドにドキュメントのルート要素を含めたい場合は、(ルート要素が明示的に含まれていない場合でも) include root で [true] ボタンをクリックし、ドキュメントのルートを含めるようにしてください。フィールドにデータベース内の要素の大部分を含める場合を除き、通常はデフォルトの false のままにします。

The screenshot shows a dialog box titled "Create Field in Database" with tabs for "Summary", "Create", and "Help". There are "ok" and "cancel" buttons at the top right. The dialog contains the following fields:

- field name:** A text input field containing "MyRootField". Below it, the text reads: "The field name. Required. You must supply a value for field-name."
- field type:** Three radio buttons: "paths", "root" (which is selected), and "metadata".
- include root:** Two radio buttons: "true" and "false" (which is selected). Below it, the text reads: "Includes XML elements or JSON properties starting at the document root."

11. [ok] をクリックします。設定ページにフィールドが表示され、以下の部分が設定ページの下部に追加されます。

The screenshot shows the "word lexicons" section of the MarkLogic interface. It includes a text input field with "[add]" next to it, a "collation builder" button, and a "Root Collation" dropdown menu. Below this is a "more word lexicons" button. There are two tables:

Included Elements					
Localname(s)	Namespace	Attribute	Attribute Namespace	Value	Weight
None					

Excluded Elements				
Localname(s)	Namespace	Attribute	Attribute Namespace	Value
None				

12. フィールドのワードレキシコンを追加する場合は、[add] テキストボックスの横にコレーション URI を入力します。UCA Default Collation の URI <http://marklogic.com/collation/> は、多くのアプリケーションで役立ちます。コレーションの詳細については、『*Search Developer's Guide*』の章「[Language Support in MarkLogic Server](#)」を参照してください。[ok] ボタンをクリックし、フィールドワードレキシコンを追加します (1 つ作成する場合)。コレーションの異なる他のフィールドワードレキシコンを作成する場合は、この手順を繰り返して、新しいレキシコンに別のコレーション URI を指定します。

13. [Includes] タブをクリックし、フィールドに含める要素を指定します。

The screenshot shows the 'Add Field Include' dialog box for the field 'myRootField'. The 'Includes' tab is selected. The dialog contains the following fields and descriptions:

- namespace uri**: A namespace URI.
- localname**: One or more localnames.
- weight**: The weight, used to boost or lower relevance scores, of the included element. (Current value: 1.0)
- attribute namespace uri**: Namespace of the child attribute.
- attribute localname**: Localname of the child attribute.
- attribute value**: Include only elements with the specified attribute having this value.

14. [Included Element] ページで、含める要素のローカル名を指定します。要素が名前空間内にある場合は、含める要素の名前空間 URI を指定します。
15. (オプション) この要素内のマッチの関連度への影響を増減する場合は、重みにデフォルトの 1.0 以外を指定します。重みが 1.0 より大きいと関連度への影響が増加し、1.0 より小さいと影響が減少します。
16. (オプション) 指定された値の属性を持つ要素のみを含める場合は、属性の名前空間 URI (適宜)、属性のローカル名、および属性の値を入力します。指定された値の属性が含まれる要素のみが含まれます。値を完全に指定してください (ワイルドカード文字は使用しないでください)。
17. この要素についてすべての項目を指定したら、[ok] をクリックします。
18. 含める各要素について、手順 [13](#) ~ [17](#) を繰り返します。

19. フィールドから要素を除外する場合は、[Excludes] タブをクリックします。
20. 名前空間 URI を適宜入力し、除外される要素のローカル名を入力します。

Field: myRootField

ok cancel

excluded element -- The element excluded from the field.

namespace uri
A namespace URI.

localname
One or more localnames.

attribute namespace uri
Namespace of the child attribute.

attribute localname
Localname of the child attribute.

attribute value
Include only elements with the specified attribute having this value.

ok cancel

21. (オプション) 指定された値の属性を持つ要素のみを除外する場合は、属性の名前空間 URI (適宜)、属性のローカル名、および属性の値を入力します。指定された値の属性が含まれる要素のみが除外されます。値を完全に指定してください (ワイルドカード文字は使用しないでください)。
22. [ok] をクリックします。
23. 除外する各要素について、手順 [19](#) ~ [22](#) を繰り返します。

24. 含めたり除外したりするフィールドは、フィールド設定ページの下部にあるテーブルから削除できます。

The screenshot shows a web interface for field settings. It features two tables: 'Included Elements' and 'Excluded Elements'. The 'Included Elements' table has columns for Localname(s), Namespace, Attribute, Attribute Namespace, Value, and Weight. It contains one row with 'ABSTRACT' in the Localname(s) column, a weight of '1.0', and a '[delete]' link. The 'Excluded Elements' table has columns for Localname(s), Namespace, Attribute, Attribute Namespace, and Value. It contains one row with 'script' in the Localname(s) column, 'http://www.w3.org/1999/xhtml' in the Namespace column, and a '[delete]' link. At the bottom of the interface are 'ok' and 'cancel' buttons.

Included Elements					
Localname(s)	Namespace	Attribute	Attribute Namespace	Value	Weight
ABSTRACT					1.0 [delete]

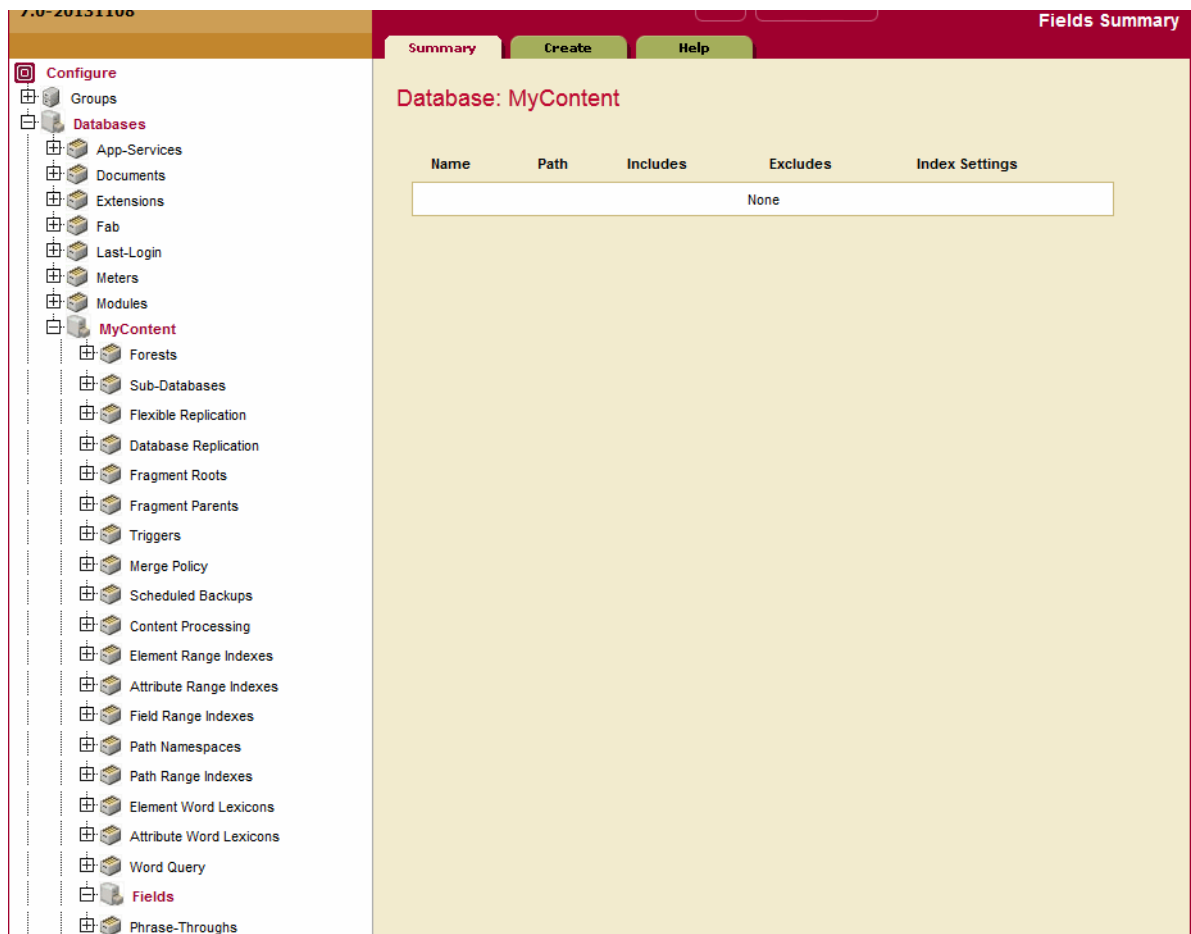
Excluded Elements				
Localname(s)	Namespace	Attribute	Attribute Namespace	Value
script	http://www.w3.org/1999/xhtml			[delete]

ok cancel

15.4.2 新しいメタデータフィールドの設定

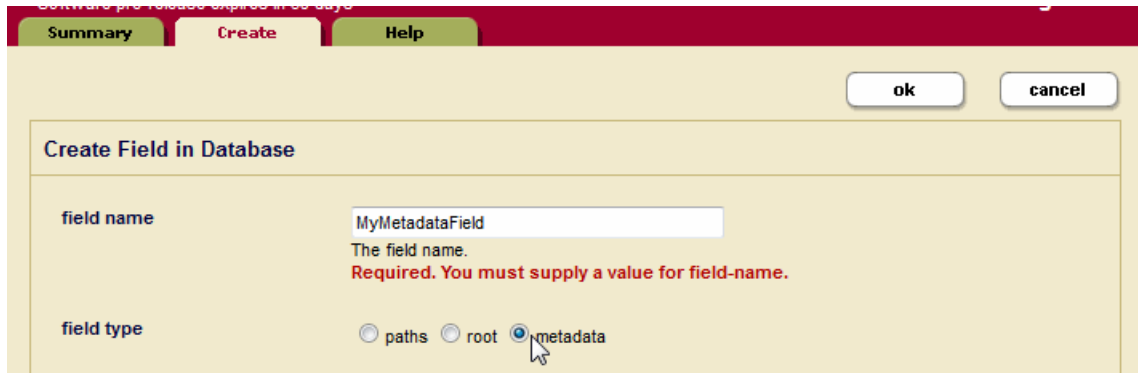
管理画面を使用して新しいメタデータフィールド設定をデータベースに追加するには、次の手順を実行します。

1. ツリーメニューまたは [Summary] タブで、フィールドを作成するデータベースに移動してクリックします。
2. フィールドを作成するデータベースで、[Fields] リンクをクリックします。[Field Summary] ページが表示されます。



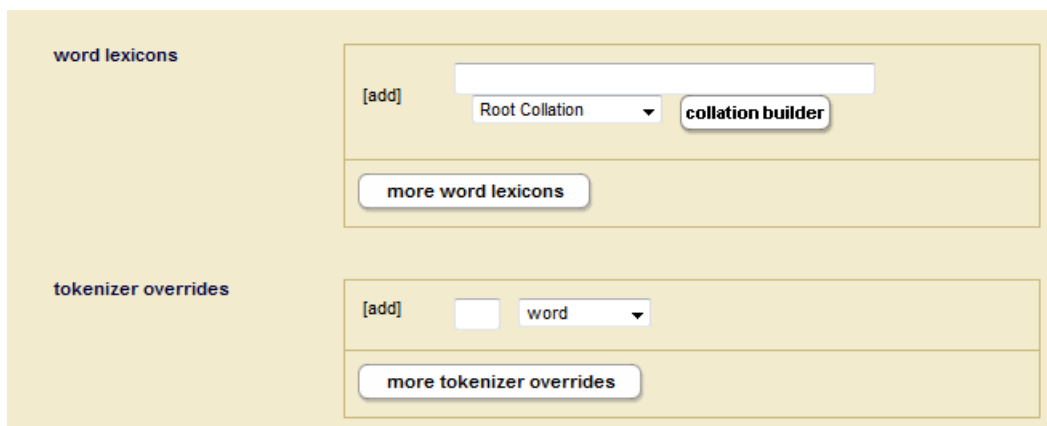
3. [Create] タブをクリックします。[Create Field in Database] ページが表示されます。
4. フィールドの名前を入力します。

5. フィールドの種類で、メタデータを選択します。



The screenshot shows a dialog box titled "Create Field in Database". At the top, there are tabs for "Summary", "Create", and "Help", and buttons for "ok" and "cancel". The main area contains two fields: "field name" with the value "MyMetadataField" and a red error message "Required. You must supply a value for field-name." below it, and "field type" with three radio buttons: "paths", "root", and "metadata", where "metadata" is selected.

6. フィールドのワードレキシコンを追加する場合は、[add] テキストボックスの横にコレーション URI を入力します。UCA Default Collation の URI <http://marklogic.com/collation/> は、多くのアプリケーションで役立ちます。コレーションの詳細については、『*Search Developer's Guide*』の章「[Language Support in MarkLogic Server](#)」を参照してください。[ok] ボタンをクリックし、フィールドワードレキシコンを追加します（1 つ作成する場合）。コレーションの異なる他のフィールドワードレキシコンを作成する場合は、この手順を繰り返して、新しいレキシコンに別のコレーション URI を指定します。
7. (オプション) フィールドレンジインデックスまたはトークナイザーオーバーライドを作成します。後で戻って追加することもできます。



The screenshot shows two sections: "word lexicons" and "tokenizer overrides". The "word lexicons" section has an "[add]" button, a text input field, a dropdown menu with "Root Collation" selected, and a "collation builder" button. Below it is a "more word lexicons" button. The "tokenizer overrides" section has an "[add]" button, a text input field, and a dropdown menu with "word" selected. Below it is a "more tokenizer overrides" button.

8. データベースのインデックスオプションの他にインデックスオプションをフィールドに含める場合、またはフィールドから何らかのインデックスオプションを削除する場合は、該当するインデックス設定のチェックボックスをオンまたはオフにします。太字で表示されているインデックス設定は、その設定がデータベース設定から継承されていることを示します。データベースレベルの設定から設定を継承しない場合は、継承されているインデックス設定のチェックボックスをオフにします。詳細については、「インデックスオプション設定について」（149 ページ）を参照してください。

注： field value positions、trailing wildcard word positions、および three character word positions オプションは、設定できますが、クエリに影響を及ぼしません。

15.4.3 既存フィールドの修正

既存のフィールドを修正するには、次の手順を実行します。

1. 既存のフィールドを修正するには、左側のツリーメニューで [Fields] リンクをクリックします。[Fields Summary] ページが表示されます。

Name	Includes	Excludes	Index Settings
myPathField			+stemmed (basic) +fast phrase +fast case sensitive +fast diacritic sensitive +trailing wildcard
myRootField	ABSTRACT	script	+stemmed (basic) +fast phrase +fast case sensitive +fast diacritic sensitive +trailing wildcard

2. 編集するフィールドの名前をクリックします。[Field Configuration] ページが表示されます。
3. 設定を変更する場合は、必要な修正を加えて [ok] をクリックします。
4. 残りの手順は、前に説明したフィールドを作成する手順と同じです。手順 12 から開始してフィールドワードレキシコンを作成し、パスフィールドおよびルートフィールドの場合は含めたり除外したりする要素の追加 / 削除に進みます。

15.4.4 フィールドのレンジインデックスの作成

フィールドに関するレンジインデックスを作成して、フィールドデータの検索を高速化できます。フィールドのレンジインデックスを作成する前に、フィールドを作成しておく必要があります。クエリスピード、読み込みスピード、サーバーリソース間の一般的なトレードオフ（「レンジインデックスについて」（357 ページ）を参照）が、フィールドレンジインデックスに適用されます。

フィールドに関するレンジインデックスを作成するには、次の手順を実行します。

1. ツリーメニューまたは [Summary] タブで、フィールドレンジインデックスを作成するデータベースに移動してクリックします。
2. 左側のツリーメニューで [Field Range Index] をクリックします。
3. [Add] タブをクリックします。[Add Field Range Indexes] ページが表示されます。
4. レンジインデックスの種類を選択します。
5. 既存フィールドの名前を入力します。
6. 必要に応じて、インデックスに位置データを格納するかどうかを指定します（メタデータフィールドは位置がないため、位置設定による影響はありません）。
7. [invalid values] で、レンジインデックスに指定されたタイプとマッチングしないフィールドのあるドキュメントを読み込まない場合は、[reject] を選択します。マッチングしないドキュメントの読み込みを許可する場合は、[ignore] を選択します。
8. [ok] をクリックします。

インデックスが作成されます。そのデータベースの [reindexer enable] 設定が [true] である場合、再インデックス付けがすぐに開始します。再インデックス付け操作が完了するまで、レンジおよびレキシコンクエリで新しいインデックスを使用できません。

16.0 データベースのマージの概要と制御

この章では、データベースのマージについて、およびデータベースのマージを制御する方法について説明します。以下のセクションで構成されています。

- [マージの概要：マージの優れた機能について](#)
- [マージポリシーの設定](#)
- [マージのブラックアウト期間](#)
- [マージとポイントインタイムクエリ](#)
- [負のマージタイムスタンプを設定して、経過時間ウィンドウの期間にフラグメントを保持する](#)
- [マージのモニタリング](#)
- [明示的なマージコマンド](#)
- [マージポリシーールールの設定](#)

16.1 マージの概要：マージの優れた機能について

このセクションでは、マージの概要について説明します。以下のように構成されます。

- [ダイナミックな自己チューニング](#)
- [マージ時の処理](#)
- [マージをオフにすることの危険性](#)
- [マージによってスコアが変更される](#)

16.1.1 ダイナミックな自己チューニング

マージは、システムのパフォーマンスを自己チューニングするための 1 つの方法です。MarkLogic サーバーでは、マージによる自己チューニングの効果を確認するために、各データベースの状態を継続的に評価します。デフォルトのマージ設定およびマージが本来持つダイナミックであるという性質により、ほとんどの場合でデータベースは常に最適な状態にチューニングされます。ただし、マージはリソース（ディスク I/O と CPU の両方）を過剰に消費する可能性があるため、状況によっては、マージを発生させる、または発生させないタイミングを DBA が制御する必要がある場合もあります。その際には、環境に合わせて適切なマージポリシーを設定します。詳細については「マージポリシーの設定」（164 ページ）を参照してください。

ダイナミックであり、自己チューニングが行われるマージは優れた機能です。ディスク領域を回復するだけでなく、システムのクエリや検索のパフォーマンスを向上します。データベースは 1 つあるいは複数のフォレストで構成され、フォレストは 1 つまたは複数のスタンドで構成されます。フォレスト内のスタンドが多くなるほど、クエリの解決にかかる時間が長くなります。マージによってデータベースの各フォレストにあるスタンド数が減少するため、クエリにかかる時間が短縮されます。

16.1.2 マージ時の処理

データベースは1つあるいは複数のフォレストで構成され、各フォレストは1つまたは複数のスタンドで構成されます。各スタンドは1つまたは複数のフラグメントで構成されます。ドキュメントが更新されると、ドキュメントの更新に関連するすべてのフラグメントの新しいバージョンが新しいスタンドに作成されます。フラグメントの古いバージョンはすべてシステムタイムスタンプ付きの古いスタンドに残され、MarkLogic サーバーではそのタイムスタンプによりフラグメントが古いバージョンであることが識別されます。同様に、ドキュメントが削除されると、そのフラグメントはシステムタイムスタンプ付きの古いスタンドに残され、MarkLogic サーバーではそのタイムスタンプによりフラグメントが古いバージョンであることが識別されます。

マージが行われると、未変更のフラグメントが古いスタンドから新しいスタンドに移動し、フラグメントの古いバージョン（削除されたフラグメントを含む）が削除されません。したがって、ディスク領域が解放され、使用可能なフラグメントはディスク上に小さくまとめられます。また、マージではスタンド内のすべてのフラグメントのインデックスデータが結合され、インデックスが最適化されます。マージはデータベースの標準的な挙動の1つであり、更新や削除が発生したときにシステムが最適な状態で実行され続けることを保証するものです。

つまり、マージの一環として、次の処理が実行されます。

- パフォーマンスを向上させるために、複数のスタンドが1つに結合されます。
- ディスク領域が回復されます。
- インデックスとレキシコンは結合され、新しいサイズに基づいて再度最適化されます。

その結果、マージ前と比べてデータベースはサイズが小さくなり、クエリの解決が大幅に高速化します。

16.1.3 マージをオフにすることの危険性

MarkLogic サーバーは、定期的にマージを行うように設計されています。システムに何らかの更新があるときにデータベースでマージがオフになっていると危険です。マージをオフにした場合、システムでマージと他のリクエストが同時に発生しているときにリソースの競合を回避できることもありますが、データベースに変更（挿入、更新、削除）が加えられたときにマージを処理できないと、MarkLogic サーバーのパフォーマンスは次第に低下します。

それだけでなく、マージをオフにしたり回避したりすると、最終的にはサーバーがデータベースに変更を加えられない状態になる可能性があります。例えば、インメモリスタンドがいっぱいになると、オンディスクスタンドに書き込まれます。MarkLogic サーバーの最大スタンド数は上限（64）が固定されているため、この上限に達してしまい、システムを更新できなくなってしまいます。そのため、マージをオフにするためのコントロールはありません。マージのオフが必要な場合は、MarkLogic カスタマーサポートまでお問い合わせください。

マージがシステム中断の原因となっている場合の大半では、マージポリシーパラメータを環境に適した設定に調整できるはずですが、マージのオフが必要である場合は、MarkLogic カスタマーサポートまでお問い合わせください。その際は、システムをモニタリングして、フォレストあたりのスタンド数が大きくなりすぎないようにしてください。マージコントロールの設定の詳細については、「マージパラメータの説明」(166 ページ) および「マージポリシールールの設定」(174 ページ) を参照してください。

場合によっては（特に多くのフォレストがあり、そのフォレストの多くにまたがるコンテンツを変更し続けているような環境では）、マージをオフにする代わりに、1 つあるいは複数のフォレストを `delete-only` に設定します。詳細については、「フォレストを `delete-only` にする」(295 ページ) を参照してください。

16.1.4 マージによってスコアが変更される

データベースをマージすると、データベース内に存在する古いフラグメントが削除されるため、データベース内のフラグメントの総数が変化します（少なくなります）。データベース内のフラグメント数は `cts:search` 操作のスコア決定に使用されるため、マージは検索スコアに影響を与えます。最終的には検索結果の順序に影響を及ぼす可能性があります（順序は関連度スコアに基づくため）。

マージがスコアに及ぼす影響の程度は、マージ処理待ちのフラグメントの古いバージョン数、古いフラグメントのコンテンツ、およびデータベース全体のサイズに依存します。変更が比較的少ない大規模データベースでは、スコアの差はかなり小さくなります。変更が大量に発生する小規模データベースでは、スコアがマージの前後で大きく異なる可能性があります。

16.2 マージポリシーの設定

このセクションでは、マージを制御するために使用できるツールについて説明します。以下のように構成されています。

- [マージポリシーコントロールの概要](#)
- [マージパラメータの説明](#)

場合によっては（特に多くのフォレストがあり、そのフォレストの多くにまたがるコンテンツを変更し続けているような環境では）、マージポリシーを設定する別の方法として、1 つあるいは複数のフォレストを `delete-only` に設定します（`updates allowed` を `false` に設定します）。詳細については、「フォレストを `delete-only` にする」(295 ページ) を参照してください。

16.2.1 マージポリシーコントロールの概要

マージの管理が必要であると判断した場合に、マージの発生条件を管理できるコントロールが数種類あります。

- MarkLogic サーバーが、マージが望ましいと判断する条件を決定するのは次のコントロールです。
 - `merge min size`
 - `merge min ratio`
- マージが可能であると判断する条件を決定するのは次のコントロールです。
 - `merge max size`
 - `merge blackout periods`
- マージの実行時にフラグメントの複数のバージョンを保持するかどうかを決定するのは次のコントロールです。
 - `merge timestamp`
- マージを明示的に開始するのは次のコントロールです（「マージの手動開始」（172 ページ）を参照）。
 - `xdmp:merge()`
 - 管理画面の [merge] ボタン
- 管理画面には、マージをキャンセルするためのコントロールがあります（「マージのキャンセル」（173 ページ）を参照）。

マージをより高度に制御できるようにシステムをセットアップする方法の詳細については、「マージポリシーールールの設定」（174 ページ）を参照してください。

16.2.2 マージパラメータの説明

次の表では、管理画面の [Databases] > [データベース名] > [Merge Policy] ページで利用可能な設定について説明します。これらのパラメータは、データベースで自動マージが発生するタイミングやその他の管理機能を決定します。

データベース 設定	説明
merge priority	<p>マージを実行する際の CPU スケジューラのプライオリティを指定します。設定は次のとおりです。</p> <ul style="list-style-type: none"> • normal は、リクエストの場合と同じ CPU スケジューラプライオリティを指定します。 • lower は、リクエストよりも低い CPU スケジューラプライオリティを指定します。 <p>17 個以上のスタンドが含まれるフォレストの場合、マージは常に normal プライオリティで実行されます。</p>
merge max size	<p>マージの結果得られるスタンドの最大サイズ（メガバイト）。スタンドが指定サイズを超える場合は、マージされません。2つのスタンドをマージすると指定サイズより大きくなる場合、それらのスタンドは相互にマージされません。この値を小さいサイズに設定すると、大規模なマージ（多くのディスクや CPU リソースが必要になることがある）が防止されます。デフォルトは 48GB（49152MB）です。スタンド数を少なく抑えながら非常に大きなマージが大量のディスク領域を使用しないようにするというバランスよい処理が実現できるため、この値が推奨されます。0 に設定すると、サイズに関係なくスタンドをマージできます。0 以外でデフォルト値より低い値に設定するときは注意してください。システムがパフォーマンスレベルを維持したりシステムに対する更新を最適化したりするために最終的に必要になるマージができなくなる可能性があります。</p>
merge min size	<p>1 つのスタンドに含めることができるフラグメントの最大数。内部のフラグメントがこの数より少ない複数のスタンドは自動的にマージされます。</p>

データベース 設定	説明
merge min ratio	<p>あるスタンド内にあるフラグメント数と、フォレスト内でそのスタンドより小さなすべてのスタンド（フラグメント数が少ないスタンド）内にあるフラグメント数の最小比を示す正の整数。あるスタンドのフラグメント数と、そのスタンドより小さなすべてのスタンドのフラグメント数がこの比を下回る場合、そのスタンドは小さなスタンドと自動的にマージされます。例については、「大規模なマージの数を減らしたい場合」（175 ページ）を参照してください。</p>
merge timestamp	<p>マージされたスタンドに格納されるタイムスタンプ。ポイントインタイムクエリで使用され、削除済みのフラグメントやフラグメントの古いバージョンによって占有されている領域をデータベースが回復できるタイミングを決定します。フラグメントがマージのタイムスタンプ以降に削除または更新された場合、ポイントインタイムクエリを使用するためにフラグメントの古いバージョンが維持されます。0（デフォルト）に設定すると、システムはマージ処理中にディスク領域を最大限に回復できます。0 に設定すると、マージの発生時に、削除済みおよび更新済みのフラグメントがすべて削除されます。コンテンツの読み込みまたは更新前に 1 に設定すると、データベースに対する変更の完全な時系列アーカイブが作成されます。現在のタイムスタンプに設定すると、この時点からのコンテンツのすべてのバージョンが保持されます。負数を設定すると、最後のマージから相対的なタイムスタンプ値のウィンドウ（1 秒は 1000 万チック）が設定されます。タイムスタンプは、MarkLogic サーバーが管理する数値で、システム内のいずれかのデータベースにおいて変更（クラスタ内のホストからの設定変更を含む）が発生するたびに 1 つずつ増えていきます。現在のタイムスタンプを設定するには、[current timestamp] ボタンをクリックします。[ok] を押して今後のマージ用にタイムスタンプをアクティブ化するまでタイムスタンプが赤で表示されます。ポイントインタイムクエリの詳細については、『<i>Application Developer's Guide</i>』を参照してください。</p>

データベース 設定	説明
retain until backup	<p>前回のフルバックアップまたは増分バックアップ以降の削除済みフラグメントを保持するかどうか指定します。オンにすると、retain until backup が merge timestamp より優先します。merge timestamp 設定に関係なく、削除済みフラグメントはバックアップが完了するまでマージされません。retain until backup をオンにすることは、merge timestamp を前回のバックアップのタイムスタンプに設定することと同じです。詳細については、「増分バックアップとジャーナルアーカイブの同時使用」(245 ページ) を参照してください。</p>
merge blackout periods	<p>マージがオフになるタイミングを指定します。マージブラックアウト期間を指定するには、[Create] タブをクリックし、ブラックアウトが発生する期間を指定します。繰り返しのブラックアウト期間にすることも、1 回限りのブラックアウト期間を指定することも可能です。システムで大幅な更新が発生する時間帯に大規模なブラックアウト期間を設定するときは注意してください。マージはデータベースの自己チューニングメカニズムの標準的な処理の 1 つであり、完全または長時間オフにするとパフォーマンスの低下が発生する可能性があります。</p>

16.3 マージのブラックアウト期間

マージは標準的なシステム挙動の 1 つであり、マージを開始するには不適切な時間もあります。マージブラックアウト期間を使用すると、マージを開始してはいけない時間帯を指定できます。このセクションでは、マージブラックアウトについて説明します。以下のように構成されています。

- [マージブラックアウトについて](#)
- [マージブラックアウト期間の設定](#)
- [マージブラックアウト期間の削除](#)

16.3.1 マージブラックアウトについて

マージブラックアウトは、自動マージがオフになる事前定義された時間帯です。マージブラックアウト期間の前に開始したマージは、マージが続行したままブラックアウト期間に入っても、完了するかキャンセルされるまで続行されます。ブラックアウト期間の開始時にマージを停止するには、手動でキャンセルする必要があります（「マージのキャンセル」（173 ページ）を参照）。ブラックアウト期間の直前に開始したマージはブラックアウト期間に入っても続行するため、期間中は確実にマージが発生しないようにするには、ブラックアウト期間の開始を早めてください。これは特に、長時間実行される可能性のあるマージの場合に当てはまります。

システムでマージが必要であると判断され、それがブラックアウト期間中である場合、ブラックアウト期間が経過するまでマージは開始しません。

16.3.2 マージブラックアウト期間の設定

マージブラックアウト期間を設定するには、次の手順を実行します。

1. 管理画面のツリーメニューで、[Databases] > [db_name] リンクをクリックします。ここで「db_name」はマージブラックアウト期間を指定するデータベースの名前です。
2. データベースの下で、[Merge Policy] メニュー項目をクリックします。[Merge Policy Configuration] ページが表示されます。
3. [Create] タブをクリックします。[Add Merge Blackout] ページが表示されます。

Add Merge Blackout Periods to a Database

merge blackout type recurring one time

this blackout will disable merges completely limit merges to: MBs

days Monday Tuesday Wednesday Thursday Friday Saturday Sunday
The days this blackout is active.

this blackout will last all day
 for a time period

4. 作成するブラックアウト期間に合わせてフォームを適宜設定します。ラジオボタンをクリックすると、設定するフォームがさらに表示されます。
5. [ok] をクリックしてブラックアウト期間を作成します。

新しいブラックアウト期間はすぐに有効になります。

16.3.3 マージブラックアウト期間の削除

マージブラックアウト期間を削除するには、次の手順を実行します。

1. 管理画面のツリーメニューで、[Databases] > [db_name] リンクをクリックします。ここで「db_name」はマージブラックアウト期間を削除するデータベースの名前です。
2. データベースの下で、[Merge Policy] メニュー項目をクリックします。[Merge Policy Configuration] ページが表示されます。
3. 削除するブラックアウト期間に対応した領域で、[delete] ボタンをクリックします。
4. 確認ページで [ok] をクリックして、ブラックアウト期間を削除します。

ブラックアウト期間はすぐに削除されます。

16.4 マージとポイントインタイムクエリ

マージが発生すると、設定されたマージタイムスタンプよりシステムタイムスタンプが古いマージ対象スタンドからすべてのフラグメントが削除されます (`merge timestamp` 設定が 0 の場合を除く。0 に設定されている場合は、現在のタイムスタンプよりも古いすべてのフラグメントが削除されます)。マージでは、データベースに同じフラグメントの複数のバージョンを保持できます。また、ポイントインタイムクエリを使用して古いフラグメントをクエリできます。詳細については、『*Application Developer's Guide*』でポイントインタイムクエリに関する章を参照してください。

16.5 負のマージタイムスタンプを設定して、経過時間ウィンドウの期間にフラグメントを保持する

更新操作を実行していて、開始時点までロールバックする機能が必要な場合は、`merge timestamp` を負の数値に設定して、指定されたチック数の間フラグメントを保持できます。チックは、1 秒あたり 10,000,000 チックとして計算されます。

例えば削除済みフラグメントを（前回のマージから相対的に）24 時間保持するには、マージタイムスタンプを -864,000,000,000 (10,000,000 チック / 秒 × 60 秒 / 分 × 60 分 / 時間 × 24 時間 / 日) に設定します。その後、データベース内のすべてのフォレストで `xdmp:forest-rollback` を使用して、最大で 1 日（または負のマージタイムスタンプを設定した時間帯の分だけ）ロールバックできます。

`merge timestamp` パラメータに負の値を設定する場合は、その期間は削除済みフラグメントが保持され、その分だけ期間中のデータベースのサイズが大きくなることに注意してください。特に、その期間に最終的に複数回の再読み込みが発生する場合、データベースの増大が顕著になります。

特定期間の負の `merge timestamp` を次の表に示します。

フラグメントを保持する期間	計算	<code>merge timestamp</code> 値
5 分	$10000000 * 60 * 5$	-30000000000
1 時間	$10000000 * 60 * 60$	-360000000000
24 時間	$10000000 * 60 * 60 * 24$	-8640000000000

16.6 マージのモニタリング

マージのモニタリング情報は主に 2 か所で確認できます。

- [ErrorLog.txt ファイル内のメッセージ](#)
- [\[Database Status\] ページ](#)

16.6.1 ErrorLog.txt ファイル内のメッセージ

マージの開始、完了、またはキャンセル時に、MarkLogic サーバーは INFO レベルのメッセージを `ErrorLog.txt` ファイルに記録します。他にも、マージ中に詳細なログ記録レベルで記録されるログメッセージがあります。一般的なマージのログメッセージ例を次に示します。

```
2006-04-20 13:43:11.151 Info: Merging /var/opt/MarkLogic/Forests/bill/00000004 and /var/opt/MarkLogic/Forests/bill/00000005 to /var/opt/MarkLogic/Forests/bill/00000006
2006-04-20 13:43:15.726 Debug: OnDiskStand /var/opt/MarkLogic/Forests/bill/00000006, disk=47MB, memory=20MB
2006-04-20 13:43:15.726 Info: Merged 81 MB in 4 s at 20 MB/s to /var/opt/MarkLogic/Forests/bill/00000006
2006-04-20 13:43:15.806 Debug: ~OnDiskStand /var/opt/MarkLogic/Forests/bill/00000004
2006-04-20 13:43:15.806 Debug: ~OnDiskStand /var/opt/MarkLogic/Forests/bill/00000005
2006-04-20 13:43:15.859 Info: Deleted /var/opt/MarkLogic/Forests/bill/00000004
2006-04-20 13:43:15.894 Info: Deleted /var/opt/MarkLogic/Forests/bill/00000005
```

マージをキャンセルした場合、`ErrorLog.txt` ファイルには次のようなメッセージが記録されます。

```
2006-05-08 17:45:44.027 Error: PooledThread::run: XDMP-CANCELED:
Canceled merge of stands: 13419435601900621379, 6182944041533805976 to:
C:\Program Files\MarkLogic\Data\Forests\bill\0000009a
```

`ErrorLog.txt` ファイルを調べることで、マージの開始時刻やキャンセル時刻、相互にマージされたスタンド、マージ先のスタンド、マージのサイズ、その他有用な情報を取得できます。

注： マージが正常に完了するためには、フォレストデータが格納されるファイルシステムに十分なディスク領域が必要です。マージによってディスク領域が不足すると、失敗してエラーメッセージが生成されます。また、システムのあらゆる処理を記録するには、ログファイルが存在するファイルシステムに十分なディスク領域が必要です。ログファイルのあるデバイスの残り領域がなくなると、MarkLogic サーバーが停止されます。また、ログファイルにメッセージを追加するために使用可能なディスク領域がない場合、MarkLogic サーバーは起動に失敗します。

16.6.2 [Database Status] ページ

[Database Status] ページにアクセスするには、ツリーメニューで [Databases] > [データベース名] リンクをクリックし、次に管理画面で [Status] タブをクリックします。[Database Status] にはマージが実行中であるかどうかを示すマージ状態、マージのサイズ、マージが完了するまでの推定所要時間が表示されます。また、現在のマージをキャンセルするためのリンクもあります（詳細については、「マージのキャンセル」(173 ページ) を参照)。

16.7 明示的なマージコマンド

このセクションでは、次の操作を手動で実行する方法について説明します。

- [マージの手動開始](#)
- [マージのキャンセル](#)

16.7.1 マージの手動開始

マージを手動で開始するには、`xdmp:merge` コマンドを明示的に発行するか (『*Scripting Administrative Tasks Guide*』の「[Merging the Forests in a Database](#)」を参照)、管理画面のデータベース設定ページにある [merge] ボタンをクリックします。いずれかの操作によって、データベース (`xdmp:merge` を使用する場合はリクエストに応答するアプリケーションサーバーが接続しているデータベース、管理画面を使用する場合は設定対象のデータベース) でマージがすぐに開始します。データベースでマージがオフになっていても、手動で開始したマージは続行します。

`xmdp:merge` コマンドを発行するか [merge] ボタンをクリックすると、自動的に発生するタイミングでなくてもマージが開始されます。`xmdp:merge` のオプションを指定しない場合は、デフォルト値が使用されます（データベースに設定された値ではなく）。

注： マージの処理中にシステムで更新が発生すると、アクティブなマージ操作中に新しいフラグメントはマージされません。その後のマージ操作でマージされます。

マージの手動開始は、非常に大規模なマージが発生しないようにマージコントロールを設定しておいて（例えば `merge min ratio` を 1 に設定）、そのような大規模マージをシステムの活動が低い期間に実行させる場合に便利です。また、自動マージのしきい値にまだ達していない削除済みフラグメントを抹消する場合にも便利です。データベースで `merge timestamp` が設定されている場合は、強制マージでもマージのタイムスタンプまでは削除済みフラグメントがマージされないことに注意してください。通常は、削除済みフラグメントは直近の 1 時間分が保持されます。そのような削除済みフラグメントを強制マージするには、`xmdp:merge` 呼び出しで `merge-timestamp` オプションを現在のタイムスタンプに明示的に設定する必要があります。

`xmdp:merge` API を使用すると、マージの最大サイズ、マージ対象のフォレスト、単一のスタンドにマージするかどうかなどのオプションをマージに指定することもできます。詳細については、『MarkLogic XQuery and XSLT Function Reference』で `xmdp:merge` を参照してください。

16.7.2 マージのキャンセル

管理画面の [Database Status] ページでマージをキャンセルできます（[Database] > [データベース名] > [Status] タブ）。マージ中にデータベースのステータスページにアクセスすると、マージされているスタンドのステータスページにキャンセル用のボタンがあります（通常はステータスページの右下）。

Forest	Stand	Merging	Stands	Size	Rate	Estimated Completion	
bill	00000063	00000062	1	52 MB	2.58MB/s	00:00:17	[cancel]
Total			1	52 MB	n/a	n/a	

マージをキャンセルすると、マージが完了していない新しいスタンドは破棄され、未マージのスタンドはマージの開始前の状態になります。自動マージをキャンセルする場合は、キャンセルするとすぐに新しいマージが開始することがあります（マージがトリガーされるようにマージコントロールが設定されている場合）。このような状況を避けるため、自動マージをキャンセルする前に、一部のマージコントロールパラメータを変更できます。

マージをキャンセルするには、次の手順を実行します。

1. 管理画面で、[Database] メニュー項目をクリックします。
2. ツリーメニューまたは [Summary] タブで、データベースの名前をクリックします。
3. [Status] タブをクリックします。
4. [Database Status] ページの右下で、マージされているスタンドの行にある [cancel] ボタンをクリックします。
5. [Cancel Merge] 確認ページで、[ok] をクリックします。

マージがキャンセルされ、[Database Status] ページが再度表示されます。

16.8 マージポリシールールの設定

一部のマージポリシーパラメータを変更することで、マージの特定の側面を効果的に制御できます。「マージパラメータの説明」(166 ページ) では、各パラメータの作用について説明しています。このセクションでは、条件を満たすようにマージコントロールパラメータをチューニングする方法について、シナリオとともにヒントを示します。次のセクションから構成されています。

- [マージのベースラインの決定](#)
- [大規模なマージの数を減らしたい場合](#)
- [その他のソリューション](#)

16.8.1 マージのベースラインの決定

システムのマージ特性は、フォレストのサイズ、システムの更新処理の量、データのフラグメント化方法など、多くの要因に依存します。マージの設定変更が必要な場合は、まず、データベースのマージ特性を特定します。これには、システムを通常の負荷で実行し、ログファイルを解析して、マージに関する次の点を判断します。

- マージの平均サイズ
- マージの平均頻度
- マージ完了までの平均時間

マージが完了するまでに数分しかかからないことが明らかになった場合、おそらく設定を変更する必要はありません。

16.8.2 大規模なマージの数を減らしたい場合

ほとんどの場合、MarkLogic サーバーはシステムが適切に最適化された状態を持続できる頻度で、比較的小さなマージを実行しています。通常、小さなマージは他への大きな影響がなく、十分速いです。しかし時には、マージが大規模すぎて時間がかかりすぎると感じられることもあります。どの程度大きければ「大規模」なマージになるのかを正確に計測することは困難ですが、マージが大規模すぎると判断した場合は、実際に大規模なマージが回避されるように設定を試してみます。

大規模なマージを回避する方法の1つが、`merge max size` 値を設定することです。ただし、データベースで大規模なマージを実行する必要があるのに実行できない状態が生じる可能性があるため、この値を設定する場合は最大マージサイズを一時的に制御する方法としてのみ設定してください。結果として、システムがあまり最適化されないことがあります。大規模なマージを考えるために、人の睡眠と比較してみましょう。人は、短期間（1-2日、人によっては3日）であればあまり睡眠をとらなくても行動できますが、最終的には睡眠をとる必要があります。そうしないと、その人の行動は極端に非常に悪くなり始めます。同様に、データベースのサイズが大きくなると、最終的には大規模なマージを実行する必要性が生じます。また、`merge max size` には、大量のスタンドが生じるような小さな値を設定しないように気を付けてください。`merge max size` 値を設定するときはデータベースで大量のスタンドが生じる可能性があるため、常に注意してください。これはパフォーマンスの低下を招く可能性があり、スタンドの最大数（64）に達すると、オフラインになります。

大規模なマージの数を減らすという目標を達成するには、`merge min ratio` の値を1まで下げる方法もあります。`merge min ratio` の値を1にすると、大規模なマージの発生を止めることはできませんが、最大スタンド内のフラグメント数がその他すべてのスタンドのフラグメント数を合計した値と等しくなったときのみ、大規模なマージが発生します。そのため、マージがフォレストサイズの半分より大きくなるのは、最大スタンドを除くすべてのスタンドのフラグメント数の合計が最大スタンドのフラグメント数以上になったときに限られます。これを図示するため、次のようなシナリオのフォレストを考えてみましょう。

スタンド 1	スタンド 2	スタンド 3	スタンド 4
10,000 フラグメント	5,000 フラグメント	1,000 フラグメント	500 フラグメント

`merge min ratio` が 1 に設定されている場合、次の比が 1 を下回るとスタンドがマージされます。

あるスタンド内のフラグメント数

フォレスト内のそれ以外の小さなスタンドすべてのフラグメント数の合計

スタンド 1 の場合、以下のような値になります。

$$10000 / (5000 + 1000 + 500) = 10000 / 6500 = 1.54$$

これは 1 を上回ります。そのため、スタンド 1 はマージされません。次にスタンド 2 の場合、以下のような値になります。

$$5000 / (1000 + 500) = 5000 / 1500 = 3.33$$

これは 1 を上回ります。そのため、スタンド 2 はマージされません。次にスタンド 3 の場合、以下のような値になります。

$$1000 / 500 = 2.0$$

これは 1 を上回ります。そのため、スタンド 3 はマージされません。つまり、フォレストがこのままの状態である（つまり新しいコンテンツが追加されない）場合、`merge min ratio` が 1 であればこのフォレストはマージされません。

次に、この期間に読み込みが発生し、フラグメントが 501 あるスタンドがフォレストに保存されたとします。次のようにスタンドが 5 つになります。

スタンド 1	スタンド 2	スタンド 3	スタンド 4	スタンド 5
10,000 フラグメント	5,000 フラグメント	1,000 フラグメント	500 フラグメント	501 フラグメント

次にスタンド 3 の場合、以下のような値になります。

$$1000 / (500 + 501) = 1000 / 1001 = 0.99$$

これは 1 を下回ります。そのため、スタンド 3 はマージされます。スタンド 4 および 5 はスタンド 3 よりも小さいために、これらのスタンドのフラグメントの合計が `merge min ratio` の分母に現れることに注意してください。そのため、スタンド 3、4、5 がマージされます。つまり、`merge min ratio` が 1 であれば、このフォレストは 3 つのスタンドにマージされます。スタンド 1 および 2 はマージされないままであり、スタンド 3、4、および 5 はマージされて新しいスタンドになります。これで、スタンドは次のようになります。

スタンド 1	スタンド 2	スタンド 3
10,000 フラグメント	5,000 フラグメント	2,001 フラグメント

実際に比較的大規模なフォレストが存在する場合、このシナリオ（小さなスタンドのフラグメント数の合計が最大スタンドのフラグメント数と同数になる）は頻繁に発生するものではありませんが、まれに発生することがあります。例えば、このフォレストで別の 3000 フラグメントがさらに累積すると、スタンド 1 は他のスタンドとマージされます。

16.8.3 その他のソリューション

場合によっては、マージパラメータの変更がシステムにとって最適なソリューションにならないこともあります。例えば、マージに非常に時間がかかる原因が低速なディスクドライブやその他のシステム競合にある場合は、多くのチューニングを施すよりもこのような問題に対処するほうが、マージ時間の短縮に大きな効果がある可能性があります。また、マージが巨大である場合は、フォレストが最適なサイズよりも大きい可能性があります。フォレストの最大サイズに固定値はありませんが、現場での経験から、フォレストが 256GB を超えるところからクエリパフォーマンスの低下とマージ時間の増加が始まることがわかっています。フォレストが 256GB を超える場合は、複数のフォレストへの分割を検討してください。

17.0 データベースのリバランス

データベース内のデータのニーズが拡大や縮小する場合、コンテンツをデータベースのフォレスト間でより均等に分散したほうが、パフォーマンスが向上し、ストレージリソースが効率的に使用されるようになります。この章では、MarkLogic サーバーがデータベースのフォレスト間でコンテンツを均等に分散できるようにするデータベースのリバランスのメカニズムについて説明します。

この章は、次の内容から構成されています。

- [データベースリ balancer の概要](#)
- [リ balancer トリガー イベント](#)
- [リ balancer のドキュメント割り当てポリシー](#)
- [リ balancer がドキュメントを移動する方法](#)
- [データベースでのリ balancer の設定](#)
- [フォレストでのリ balancer の設定](#)
- [データベースからフォレストのリタイア](#)
- [リ balancer のステータスの確認](#)
- [リ balancer と他のデータベース設定やフォレスト設定との相互作用](#)
- [以前のリリースからアップグレードした後のリ balancer 設定](#)

17.1 データベースリ balancer の概要

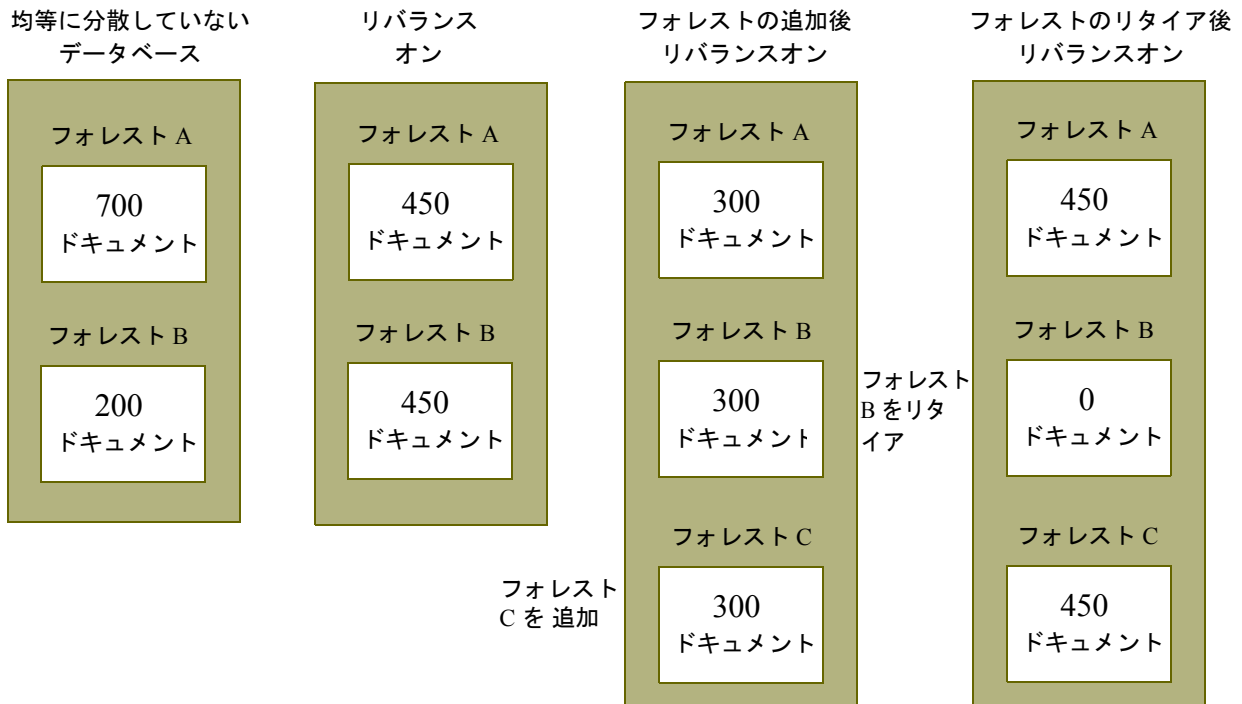
データベースリ balancer は、データ挿入およびリバランスのための「割り当てポリシー」と、データ移動のための「リ balancer」の 2 つから構成されます。リ balancer は、複数ある割り当てポリシーの 1 つを使用して設定できます。割り当てポリシーは、データベースの「バランスの取れた状態」を定義します。データベースに適切なポリシーを選択してください。リ balancer は、各フォレストで実行され、データベースの割り当てポリシーを照会してこのフォレストに「所属」しないドキュメントを判断し、そのドキュメントを適切なフォレストにプッシュします。

注： ドキュメントの読み込みおよびデータベースへの挿入は、リ balancer で使用されるドキュメント割り当てポリシーと同じものに従います。リ balancer がオンであるかオフであるかは関係ありません。

リ balancer が設定されたデータベースに新しいフォレストを追加すると、データベースでは新しいフォレストと既存のフォレストの間で自動的にドキュメントが再分散されます。データベース内にあるフォレストを「リタイア」して、そのフォレストからすべてのドキュメントを取り除いて、データベース内にある残りのフォレストの間で再分散することもできます。

リバランサーはデータベースレベルでオン/オフできるだけでなく、フォレストレベルでもオン/オフできます。リバランサーをフォレストで実行するには、データベースとフォレストの両方でオンにする必要があります。

次の図に、900 個のドキュメントが、リバランス前、リバランス後、データベースへの新しいフォレストの追加後、およびデータベースからのフォレストのリタイア後に、どのように分散されているのかを示します。



17.2 リバランサートリガーイベント

リバランサーがデータベースを定期的にもリバランスするのに加え、次のイベントもリバランサープロセスをトリガーします。

- データベースの設定変更（新しいフォレストの追加や既存フォレストのリタイアなど）。
- データベースでのリストア操作の完了時。
- データベースでのバックアップ操作の完了時。

17.3 リバランサーのドキュメント割り当てポリシー

データベースには、「割り当てポリシー」が設定されます。割り当てポリシーは、リバランサープロセスに参与する他のフォレストにドキュメントを再割り当てするときに、フォレストによって使用されるロジックを定義します。リバランサープロセスとドキュメント読み込み / 挿入プロセスは別のスレッドで実行されますが、両方ともリバランサーに対してデータベースで設定された同じ割り当てポリシーに従います。

よく使用される割り当てポリシーには、次の 5 つがあります。

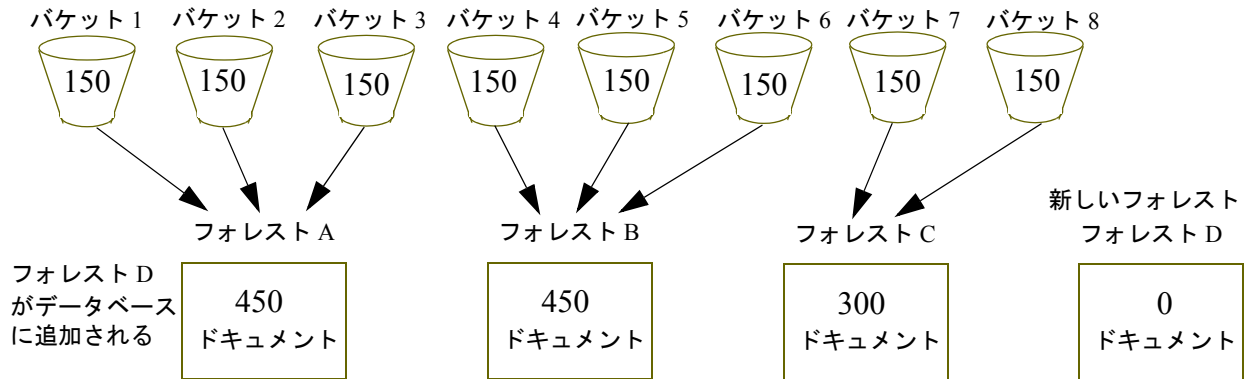
- [バケット割り当てポリシー](#)
- [統計的割り当てポリシー](#)
- [レンジ割り当てポリシー](#)
- [クエリ割り当てポリシー](#)
- [レガシー割り当てポリシー](#)

17.3.1 バケット割り当てポリシー

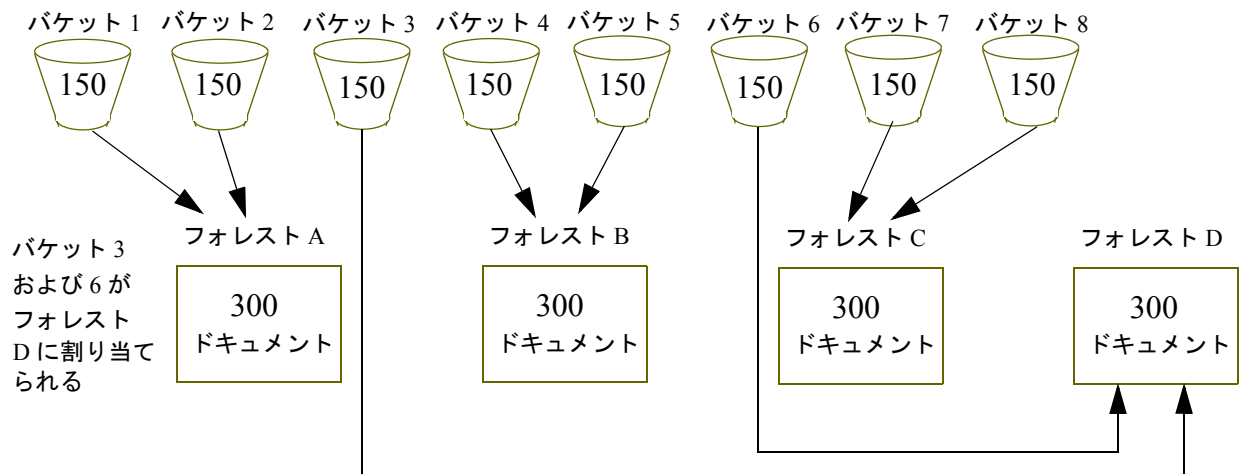
バケットポリシーでは、ドキュメントの URI に基づき、ドキュメントの割当先となるフォレストを決定します。最初に URI がバケットにマッピングされ、次にバケットがフォレストにマッピングされます。バケットからフォレストへのマッピングは、アクセスの高速化のためにメモリ上に保持されます。バケットの数は、データベース内にあるフォレストの数に関係なく、常に 16000 です。

注： ドキュメント URI がバケットにマッピングされる方法、およびバケットがフォレストにマッピングされる方法の設定は変更できません。

バケット割り当てポリシーで使用されるバケットは 16000 ありますが、以下の例では 8 つのバケットがあり、1200 個のドキュメントがフォレスト A、フォレスト B、フォレスト C という 3 つのフォレストに分散しているとします。また、バケット間で均等に分散されるようなドキュメント URI になっているとします。ここでフォレスト D がデータベースに追加されると、リバランサーはバケット 3 をフォレスト A からフォレスト D に、バケット 6 をフォレスト B からフォレスト D に再割り当てることにより、フォレスト A および B からドキュメントの 1/3 をフォレスト D に移動します。



リバランサープロセスが開始

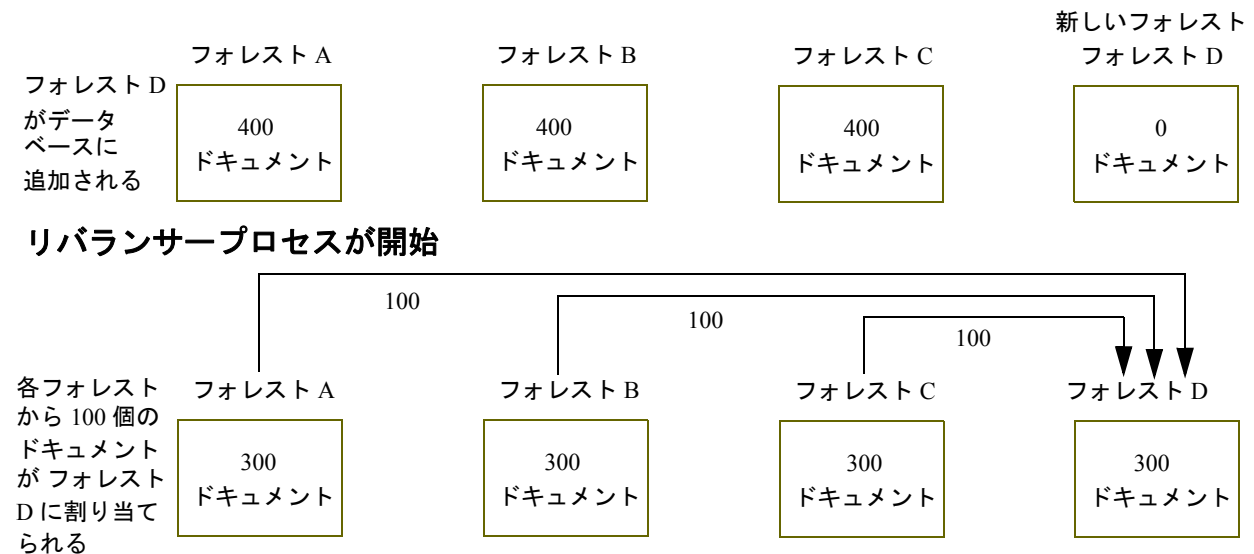


バケット割り当てポリシーは、ほとんどの場合で最も効率的なドキュメント割り当てポリシーです。バケットポリシーは決定論的であり、決定論的な割り当てポリシーの中ではデータの移動量が最も少なくなります。

17.3.2 統計的割り当てポリシー

統計的割り当てポリシーでは、URI をフォレストにマッピングしません。その代わりに、各フォレストは自身に存在するドキュメントの数を把握し、ハートビートを介してその情報を他のフォレストにブロードキャストします。それを受けて、リバランサーはドキュメント数が最も多いフォレストからドキュメント数が最も少ないフォレストへドキュメントを移動します。統計的割り当てポリシーでは、新しいフォレストが追加されると、バランスがとれた状態にするために必要な最小限の個数のドキュメントを移動します。「バランスのとれた状態」であるとみなされるために、データベース内のすべてのフォレストでドキュメントの個数が同じになる必要はありません。

例えば以下の図に示すように新しいフォレスト（フォレスト D）が、それぞれ 400 のドキュメントが存在するフォレスト A、フォレスト B、フォレスト C という 3 つのフォレストがすでに存在するデータベースに追加されるとします。既存の各フォレストから 100 個のドキュメントが新しいフォレスト（フォレスト D）に移動します。



注： 上記の例に示したドキュメント数は、統計的ポリシーが設定されたときのリ balancer の動作を示すために使用されています。実際には、このようなわずかな数のドキュメントをフォレスト間で移動しても効率的ではありません。一般に、フォレスト間のドキュメントの大幅なリバランスは、データベース内にあるドキュメントの数が 100,000 を超えると効果があります。

注： データベースのバランスがとれた状態（各フォレストのドキュメント数がほぼ同じ）では、統計的割り当てポリシーを適用してもすぐに大規模なデータ移動はトリガーされません。その後、新しく挿入が発生すると、フォレスト間で自動的にバランスがとられます。

17.3.3 レンジ割り当てポリシー

レンジポリシーは、「レンジパーティション」（200 ページ）で説明する階層型ストレージレンジパーティションで使用するために設計されました。ドキュメントの割り当て先フォレストを決定するために、レンジインデックス値を使用します。レンジポリシーを設定するときは、「パーティションキー」として使用するレンジインデックスを指定し、データベースにアタッチされた各フォレストに対し、下限と上限を定義する「レンジ」を設定します。

同じレンジを複数のフォレストがカバーすることは可能ですが、2つのフォレストが部分的に重複するレンジを持つことはできません。例えば、フォレスト A とフォレスト B の両方が「1～10」をカバーすることは有効ですが、フォレスト A が「1～6」をカバーしてフォレスト B が「4～10」をカバーすることは無効です。また、フォレスト A が「1～10」をカバーしてフォレスト B が「4～9」をカバーすることも無効です。統計的ポリシー（「統計的割り当てポリシー」（181 ページ）を参照）と同様なマッピングプロセスに従い、同じレンジをカバーするフォレスト間で各フォレストのドキュメント数に基づいてドキュメントが割り当てられます。

注： レンジの「ギャップ」や、パーティションキーとして使用される要素が含まれないドキュメントに対応するために、常に「デフォルトフォレスト」を設定する必要があります（後述）。

ドキュメントが Content Processing Framework（CPF）によって処理されると、そのドキュメントに関連付けられたプロパティドキュメントには、そのドキュメント内のパーティションキーとは別のパーティションキーが設定されることがあります。レンジポリシーを使用するときは、プロパティドキュメントが元のドキュメントと同じフォレストに移動されるように、`xdmp:document-add-properties` または `xdmp:document-set-properties` 関数を使用してドキュメント内で指定されるパーティションキーと同じキーをプロパティドキュメントに設定できます。例えばパーティションキーが `creation-date` であり、`example.xml` ドキュメントの `creation-date` が `2010-01-02` であるにもかかわらず、その関連するプロパティドキュメントには `creation-date` 要素がないとします。この場合は `xdmp:document-add-properties` 関数を次のように使用して、一致する `creation-date` 要素を `example.xml` プロパティドキュメントに追加できます。

```
xdmp:document-add-properties (  
  "example.xml",  
  (<creation-date>2010-01-02</creation-date>))
```

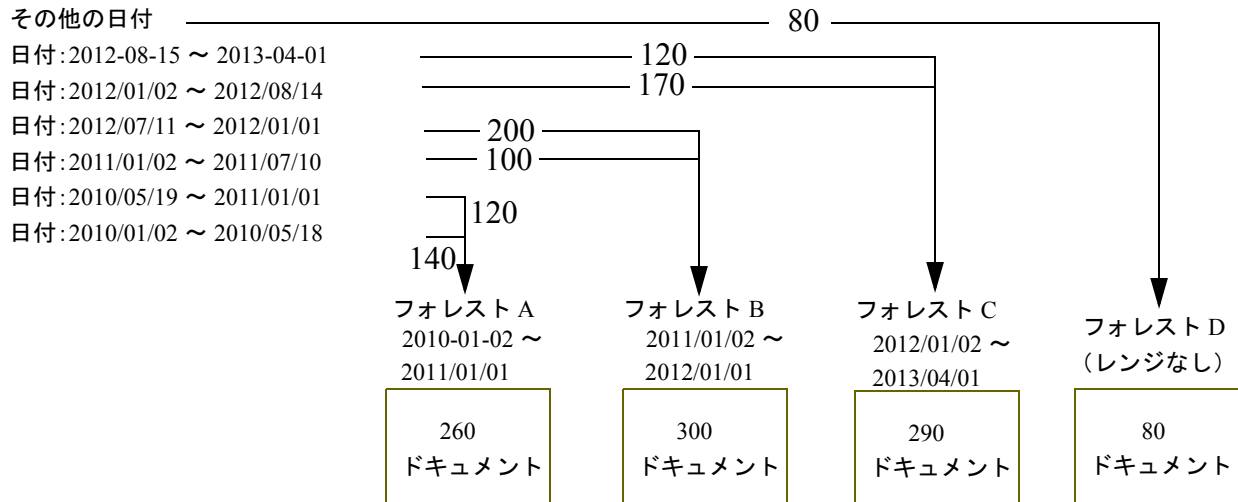
レンジ値のないフォレストは、デフォルトフォレストとして動作します。つまり、他のフォレストで設定されたいずれのレンジにも収まらないドキュメントは、デフォルトフォレストに移動します。ドキュメントの移動先となる別のフォレストが出現するまで、フォレストはリタイアできません。つまり、リタイアするフォレストと同じレンジの別のフォレストが存在するか、デフォルトフォレスト（レンジが設定されていない）がデータベースにアタッチされている必要があります。データベースにデフォルトフォレストが存在しない場合、パーティションキーが他のフォレストのレンジと一致しないドキュメントを含むフォレストをリタイアしようとしても、成功しません。

注： レンジ割り当てポリシーを設定するときは、デフォルトフォレストを必ず定義してください。

例えば以下の図に示すように、ドキュメントが6つの部分にまとめられていて、各ドキュメントにはドキュメントの作成日を示す `<creation-date>` 要素が含まれているとします。ここで、`creation-date` という名前の要素レンジインデックスを `date` 型で作成し、レンジポリシー用のパーティションキーとして指定します。フォレストが4つある場

合、フォレスト A のレンジの下限を 2010-01-02、上限を 2011-01-01 に設定し、フォレスト B の下限を 2011-01-02、上限を 2012-01-01 に、フォレスト C の下限を 2012-01-02、上限を 2013-04-01 に設定できます。4 つ目のフォレストであるフォレスト D はレンジを指定せずに、デフォルトフォレストとして指定します。日付が他のフォレストに設定された日付レンジ外にあるドキュメントは、デフォルトフォレストに移動します。

ドキュメントの日付レンジ



17.3.4 クエリ割り当てポリシー

クエリ割り当てポリシーは、レンジ割り当てポリシーと同様に、「クエリパーティション」(202 ページ) で説明する階層型ストレージクエリパーティションで使用するために設計されました。クエリ割り当てポリシーの動作は、レンジ割り当てポリシーに似ています。しかし、パーティション内にあるドキュメントを決定するために下限と上限の値を使用するのではなく、クエリを使用してパーティション内にあるドキュメントを決定します。複数のキーを使用したり、ドキュメントの種類に応じて異なる条件を使用したりといった柔軟性があります。

レンジ割り当てポリシーでは境界が固定されています。しかし、入力時刻と現在の時刻との差に基づいてリバランスしたい場合もあります。レンジクエリで `dateTime` を期間と比較すると、経過時間のクエリになります。

例えば次のクエリは、「LastModified」が過去 1 年以内であるドキュメントにマッチします。

```
cts:element-range-query(
  xs:QName("LastModified"),
  ">=",
  xs:yearMonthDuration("P1Y"))
```


クエリパーティションを作成するときは、パーティション番号を割り当てます。レンジパーティションとは異なり、クエリ割り当てポリシーを使用してパーティションに対して設定されたクエリは「重複」できます。ただし重複時は、番号が大きいパーティションより前に、番号が小さいパーティションが選択されます。

注： レンジ割り当てポリシーの場合と同様に、クエリ割り当てポリシーを設定するときは、デフォルトパーティションを必ず定義してください。

クエリ割り当てポリシーのセットアップ例を次に示します。MD および AD は、ドキュメント内の要素です。

パーティション名	Tier1	Tier2	Tier3	Tier4
パーティション番号	1	2	3	4
クエリ	(Termination が yes に等しい) または (Source が「Hiring」に等しいかつ MD > 30 日) または (Source が「CFO」に等しいかつ MD > 30 日)	(Source が「Hiring」に等しいかつ MD ≤ 30 日) かつ MD > 1 年) または (Source が「CFO」に等しいかつ MD ≤ 30 日) かつ MD > 60 日) または (Source が「Benefits」に等しいかつ AD > 1 年)	(Source が「Hiring」に等しいかつ MD ≤ 1 年) かつ MD > 3 年) または (Source が「CFO」に等しいかつ MD ≤ 60 日) または (Source が「Benefits」に等しいかつ AD ≤ 1 年)	(Source が「Hiring」に等しいかつ MD ≤ 3 年)
デフォルト	はい	いいえ	いいえ	いいえ

パーティションごとに `cts:query` は 1 つだけ存在します。

クエリ割り当てポリシーが使用されるときは、ドキュメント挿入で次のルールが使用されます。

- パーティション番号はプライオリティに使用されます。ドキュメントにマッチするクエリが複数ある場合、パーティション番号の小さいパーティションが使用されます。
- ドキュメントにマッチするクエリがない場合、デフォルトパーティションが使用されます。

- デフォルトパーティションがない場合、パーティション番号の設定されていないフォレストが使用されます。
- それ以外の場合、エラーになります。

パーティション内にあるフォレストの間では、ドキュメントをフォレストに割り当てるために統計的割り当てポリシーが使用されます。

クエリを使用するには、データベースで適切なインデックスが設定されている必要があります。クエリの複雑さが、挿入やリバランスのパフォーマンスに影響を与えます。そのため、ワイルドカードマッチングを使用するクエリなど、低速なクエリは推奨されません。

クエリ割り当てポリシーを設定する方法の詳細については、「クエリパーティションのクエリ割り当てポリシーの設定」(211 ページ)を参照してください。

17.3.5 レガシー割り当てポリシー

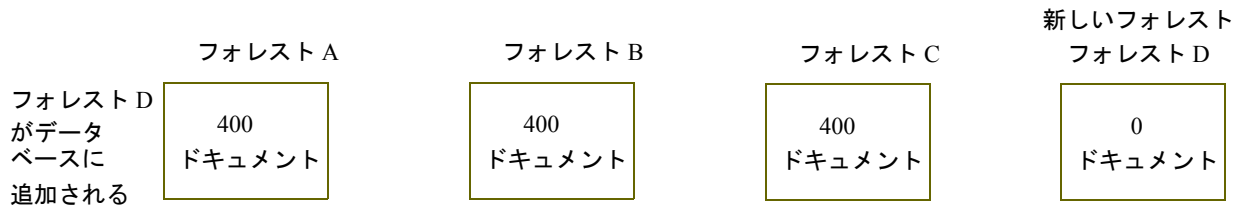
MarkLogic 7.0 へアップグレードすると、既存のデータベースはリバランサーがオフに設定され、レガシー割り当てポリシーが設定されます。これは、新しいドキュメントがデータベースに読み込まれるときに、想定される動作を保証するためです。

注： ほとんどの場合、データベースリバランサーがオンのときはレガシーポリシーを使用しません。

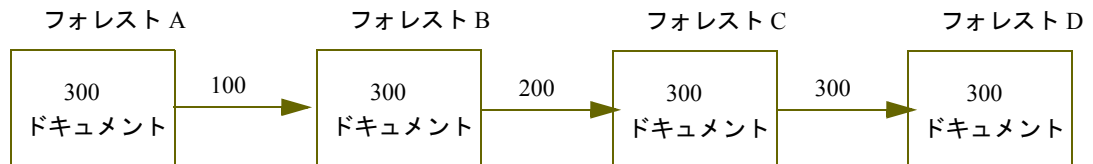
レガシーポリシーでは、ドキュメントの URI に基づき、ドキュメントの割り当て先となるフォレストを決定します。URI からフォレストへのマッピングでは、以前のリリースの MarkLogic サーバーで使用されていたものと同じアルゴリズムを使用します。

例えば以下の図に示すように新しいフォレスト（フォレスト D）が、それぞれ 400 のドキュメントが存在する（フォレスト間で均等に分散されるようなドキュメント URI になっているため）フォレスト A、フォレスト B、フォレスト C という 3 つのフォレストをすでに含むデータベースに追加されるとします。データは次のようにリバランスされます。

- フォレスト A は 100 個のドキュメントをフォレスト B に移動する
- フォレスト B は 200 個のドキュメントをフォレスト C に移動する
- フォレスト C は 300 個のドキュメントをフォレスト D に移動する



リバランサープロセスが開始



レガシーポリシーは、フォレスト間でリバランスするためのドキュメントの移動量が最も多くなるため、リバランサーポリシーとしては効率が最も悪いです。このため、レガシーポリシーはリバランサーがオフになっているレガシーデータベースでのみ使用してください。

17.3.6 割り当てポリシーのまとめ

リバランサー割り当てポリシーの特長を次の表にまとめます。

ポリシー	データの移動	決定論的である	後方互換性がある
バケット	少ない	はい (URI ベース)	いいえ
統計的	最少	いいえ	いいえ
レンジ	少ない	はい (パーティションキーベース)	いいえ
クエリ	少ない	はい (パーティションキーベース)	いいえ
レガシー	最多	はい (URI ベース)	はい

17.4 リバランサーがドキュメントを移動する方法

リバランスプロセスと再インデックス付けプロセスの間には多くの類似点があります。リバランスはデータベースレベルで設定し、フォレストごとに個別のリバランスプロセスが別々に実行されます。

リバランサーの主なタスクは、データベースに関連付けられた割り当てポリシーを調べて、このフォレストに本来所属すべきでないドキュメント（URI）のリストを取得し、適切なフォレストにプッシュすることです。リバランス対象フォレストからのドキュメント削除と適切なフォレストへの挿入は、同一のトランザクションで発生します。URI が同じフラグメントはすべて、同一トランザクションで処理されます。それぞれのトランザクションで 1 まとまりのドキュメントを移動させます。

リバランスがオンの場合は、データベースのリバランサーズロットルを設定できます。リバランサーズロットルはリインデクサーズロットルと同じ働きをして、リバランス専用のシステムリソースのプライオリティを確立します。リバランサーズロットルを 5（デフォルト）に設定すると、リバランサーは積極的に動作して、前のリバランスバッチが終了するとすぐに次のバッチを開始します。4 に設定した場合はバッチ間の待機時間が長くなり、3 に設定するとさらに長くなります。1 に設定したときの待機時間が最長です。数字が大きいほどリバランスのプライオリティが高くなり、使用するシステムリソースが多くなります。

次のセクションでは、データベースでフォレストが再設定されるときに、ドキュメントがどのように移動するのかについて説明します。

- [フォレストがデータベースにアタッチされるときのデータ移動方法](#)
- [フォレストがデータベースからリタイアするときのデータ移動方法](#)

17.4.1 フォレストがデータベースにアタッチされるときのデータ移動方法

空のフォレストをデータベースにアタッチすることは、新しいフォレストを追加することと同じです。アタッチするフォレストに既存のドキュメントが含まれている場合、そのドキュメントは、データベースにすでにアタッチされている他のフォレストにあるドキュメントとのリバランスに関与します。

17.4.2 フォレストがデータベースからリタイアするときのデータ移動方法

リバランサーがオンになっているフォレストをリタイアする場合、リバランサーはデータベースにアタッチされている他のフォレストへすべてのドキュメントを分散してフォレストを空にします。他のフォレストのリバランサーは、リタイアしたフォレストが存在しなくなったものとしてドキュメントのルーティングを再計算します。新しい挿入の場合、リタイアしたフォレストはドキュメント割り当てポリシーによる考慮対象から除外されます。

注： リタイアはデタッチや削除とは独立した操作です。読み取り専用のフォレストはリタイアできません。データベース内のすべてのドキュメントを維持するには、フォレストをデタッチするより前にそのフォレストをリタイアして、データベース内の残りのフォレストでドキュメントをリバランスする必要があります。

17.5 データベースでのリバランサーの設定

管理画面または Admin API を使用して、リバランスプロセスを設定およびモニタリングできます。

データベースでリバランサーを設定するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. リバランサーを設定するデータベースを決定します。
3. ツリーメニューまたは [Summary] タブで、データベース名をクリックします。
[Database Configuration] ページが表示されます。
4. [Database Configuration] ページを割り当てポリシーまで下にスクロールし、[Rebalancer Enable] を [true] に設定します。
5. [assignment policy] プルダウンメニューで、割り当てポリシーを選択します。選択可能なリバランサー割り当てポリシーの詳細については、「リバランサーのドキュメント割り当てポリシー」（180 ページ）を参照してください。

The screenshot shows a configuration panel with three sections:

- rebalancer enable**: Radio buttons for true and false. Below the text: "Enable automatic rebalancing after configuration changes."
- rebalancer throttle**: A dropdown menu showing the value "5". Below the text: "Larger numbers mean work harder at rebalancing."
- assignment policy**: A dropdown menu with options: bucket, bucket, statistical, range, legacy, query. The "statistical" option is highlighted. Below the text: "use for assignment and rebalancing."

At the bottom of the panel are two buttons: "ok" and "cancel".

6. [rebalancer throttle] プルダウンメニューで、リバランサーズロットル設定を選択します。リバランサーズロットルの詳細については、「リバランサーがドキュメントを移動する方法」（187 ページ）を参照してください。
7. [ok] をクリックします。

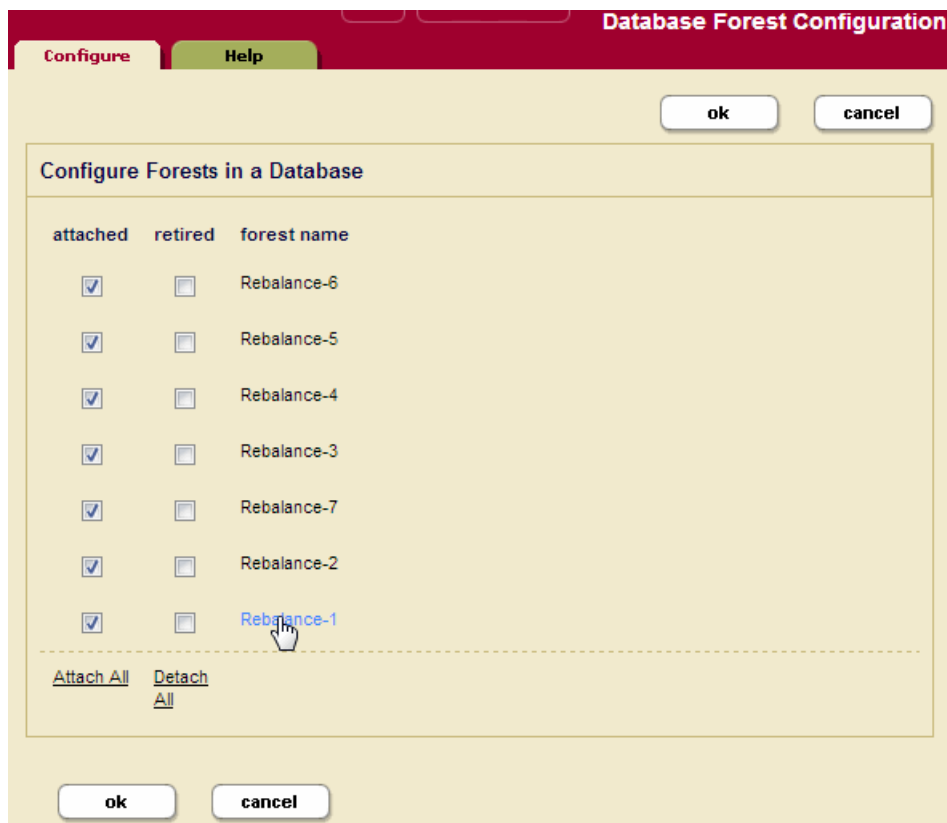
17.6 フォレストでのリバランサーの設定

リバランサーはデータベースレベルでオン/オフできるだけでなく（「データベースでのリバランサーの設定」（189 ページ）を参照）、個別のフォレストでもオン/オフできます。リバランサーをフォレストで実行するには、データベースとフォレストの両方でオンにする必要があります。

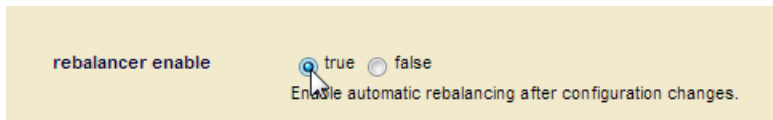
注： デフォルトでは、各新規フォレストでリバランサーがオンになっています。

フォレストでリバランサーを設定するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. フォレストを設定するデータベースを選択します。
3. ツリーメニューまたは [Summary] タブで、データベース名をクリックします。
4. 左側のツリーメニューで、データベース名の下にある [Forests] を選択します。
5. [Database Forest Configuration] ページで、リバランサーをオンまたはオフにするフォレストを選択します。



6. [Forest Configuration] ページで、[Rebalancer Enable] まで下にスクロールします。リ balancer をオンにするには [true]、オフにするには [false] に設定します。



7. フォレストのデータベースにレンジ割り当てポリシーを設定した場合は、下限と上限のフィールドにこのフォレスト用のレンジを設定できます。このフォレストをデフォルトフォレストとして機能させる場合は、レンジを設定しないでください。

8. [ok] をクリックします。

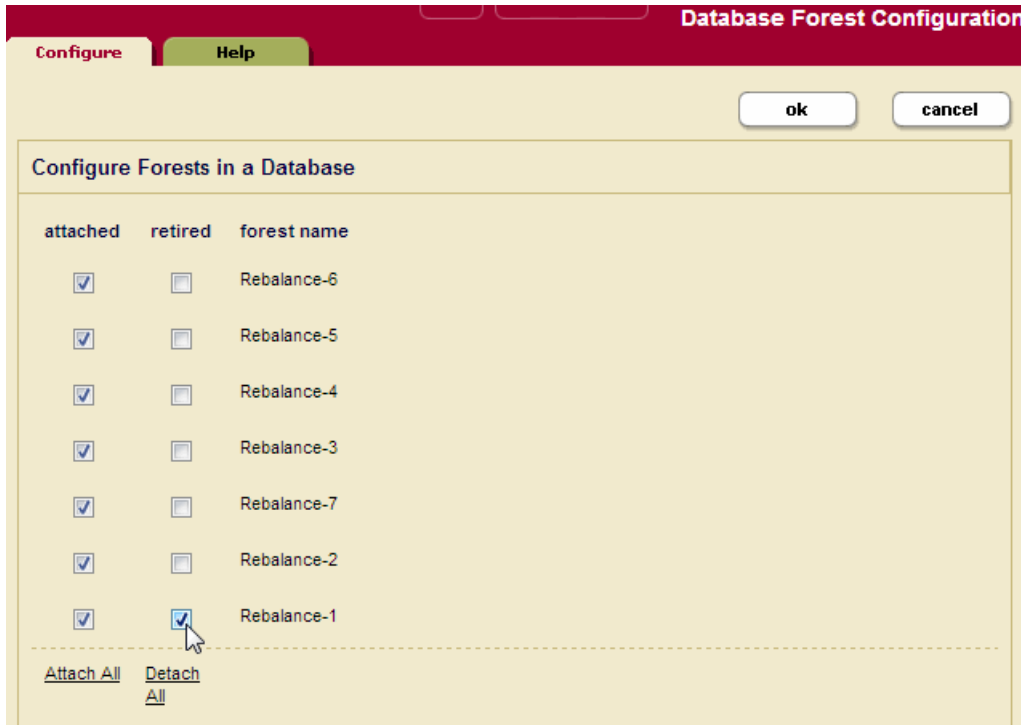
17.7 データベースからフォレストのリタイア

フォレストをデータベースから「リタイア」することで、フォレスト内のすべてのドキュメントを残りのフォレストに移動して、これらのフォレスト間でリバランスを実行できます。（「フォレストがデータベースからリタイアするときのデータ移動方法」（188 ページ）を参照）。データベースにフォレストのドキュメントを保持するには、フォレストをデータベースからデタッチする前にリタイアする必要があります。

データベースからフォレストをリタイアするには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. フォレストをリタイアするデータベースを決定します。
3. ツリーメニューまたは [Summary] タブで、データベース名をクリックします。
4. 左側のツリーメニューで、データベース名の下にある [Forests] を選択します。

5. [Database Forest Configuration] ページで、データベースからリタイアするフォレストの [retired] ボックスにチェックを付けます。データベースにフォレストのドキュメントを保持するには、フォレストの [attached] ボックスにチェックが付いたままにします。

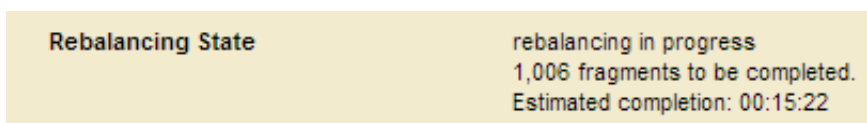


6. [ok] をクリックします。リタイアしたフォレスト内のドキュメントは、データベース内の他のフォレストに均等に再分散されます。
7. リタイアしたフォレストがリバランサーによって空になった後、そのフォレストが不要な場合は、フォレストをデータベースからデタッチできます。詳細については「データベースに対するフォレストのアタッチ / デタッチ」(124 ページ) を参照してください。

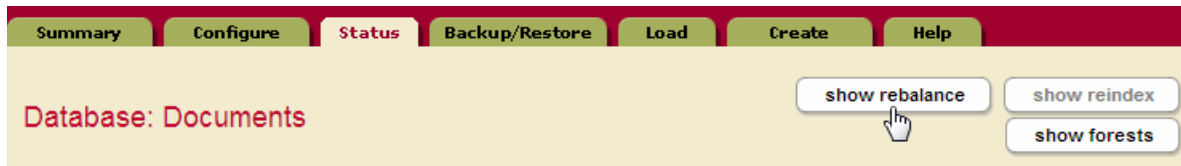
17.8 リバランサーのステータスの確認

データベースでリバランサーがオンのときは、リバランサーのステータスおよび完了推定時間を [Database Status] ページで確認できます。

例えば、データベースがドキュメントをリバランスしている場合は、次のようなステータスが表示されます。



データベースでリバランサーがオフのときは、[Database Status] ページの上部にある [show rebalance] ボタンをクリックすると、リバランスが保留中であるフラグメントの数を確認できます。



[Database Status] ページの中間部に、次のような表が表示されます。

Rebalancing	
Destination	Fragments Remaining
1 -- 10	0
11 -- 20	0
21 -- 30	0
31 -- 40	0
41 -- 100	0
101 -- 200	0
201 -- 300	0
301 -- 400	16
DEFAULT	1,227
401 -- 500	99

17.9 リバランサーと他のデータベース設定やフォレスト設定との相互作用

このセクションでは、データベースリバランサーが他のデータベース設定やフォレスト設定とどのように関係するのかについて説明します。次の内容を取り上げます。

- [データベースのレプリケーション](#)
- [バックアップからデータベースのリストア](#)
- [階層型ストレージ](#)
- [高速ロック](#)
- [delete-only および read-only のフォレスト](#)

17.9.1 データベースのレプリケーション

データベースがデータベースのレプリケーション向けに設定済みであり、そのデータベースでバケットポリシーまたはレガシーポリシーによるリバランスをオンにしてある場合は、データベース設定におけるフォレストの順序が重要になります。マスターデータベースとレプリカデータベースで順序が同一であることが必要です。マスターとレプリカでフォレストの順序が異なると、ログに次のようなメッセージが記録されます。

```
Warning: forest order mismatch: local forest XXX is at position A
while foreign master forest YYY (cluster=ZZZ) is at position B.
```

このエラーが出現した場合は、レプリカデータベースで `admin:database-reorder-forests` 関数を実行して、マスター側と同じ順序になるようにフォレストを並び替えることができます。マスターとレプリカが一致するようにフォレストを並べ替えないと、レプリケーションの設定が解除された際にリバランスが発生します。

17.9.2 バックアップからデータベースのリストア

データベースでバケットポリシーまたはレガシーポリシーによるデータベースのリバランスをオンにしてある場合に、データベースにおけるフォレストの順序が、データベースバックアップ時のフォレストの順序と異なることがあります。

`xdmp:database-restore-validate` 関数を実行して、バックアップ実行時のフォレストの順序を示す `database` 要素が含まれるバックアッププランを返すことができます。フォレストの順序がマッチしない場合は、バックアップからリストアする前に

`admin:database-reorder-forests` 関数を実行して、データベースでフォレストを並べ替える必要があります。

注： バケットポリシーまたはレガシーポリシーを使用していて、リストアされているデータベースにおけるフォレストの順序がデータベースバックアップ時のフォレストの順序と異なる場合は、リストア操作によって、リストアされたデータベース上のフォレストの間で大規模なデータ移動がトリガーされる可能性があります。

17.9.3 階層型ストレージ

「レンジ割り当てポリシー」(182 ページ) で説明するレンジ割り当てポリシーは、階層型ストレージをサポートするように設計されています。階層型ストレージの詳細については、「階層型ストレージ」(196 ページ) を参照してください。

17.9.4 高速ロック

高速ロックは、レガシーポリシーとバケットポリシーの両方で使用できます。ただし、統計的ポリシーおよびレンジポリシーは高速ロックと併用できません。統計的ポリシーで同一の URI を挿入する 2 つのトランザクションがある場合、一方のトランザクションは他方がどのフォレストを選択するのかを認識しないため、サーバーで厳密なロックを使用する必要があります。レンジポリシーでは、同一の URI を挿入する 2 つのトランザクションでレンジインデックスの値が異なる可能性があるため、サーバーで厳密なロックを使用する必要があります。

17.9.5 delete-only および read-only のフォレスト

delete-only (DO) および read-only (RO) のフォレストは、ドキュメントの割り当て方法に影響を与えます。割り当て機能と DO/RO フォレストの関係について、次の表にまとめます。

ポリシー	新しい挿入	RW -> DO/RO	DO/RO -> RW
レガシー	DO/RO は割り当てから除外されます。	URI ごとにルーティングを再計算します。大量の移動が発生します。	URI ごとにルーティングを再計算します。大量の移動が発生します。
バケット	DO/RO はルーティングテーブルの計算に含まれますが、DO/RO に属する URI は決定的な方法で再割り当てされます。	移動なし。	挿入時に (DO/RO 以外に) 再割り当てされたドキュメントのみ移動します。
統計的	DO/RO は割り当てから除外されます。RW はバランスが取れた読み込みとなります。	すべての RW のバランスが取れているため、移動なし。	すべての RW のバランスが取れるまで、若干の移動が発生。
レンジおよびクエリ	DO/RO は割り当てから除外されます。パーティション内で、RW はバランスが取れた読み込みとなります。	RW のバランスが取れているため、パーティション内で移動なし。	すべての RW のバランスが取れるまで、パーティション内で若干の移動が発生。

2 番目および 3 番目の列は、フォレストが RW から DO/RO へ、または DO/RO から RW へ変更されるときに RW でリバランサーが実行する処理について説明しています。

RO フォレストのリバランサーは常にオフです。DO フォレストのリバランサーは、「リタイア」するまでオフです。

フラッシュバックアップフォレストは、一般に RO フォレストとして処理されます (新しい挿入の場合を除く)。割り当てロジックでドキュメント挿入先フォレストが見つからない場合は、(例外ではなく) 再試行がスローされます。

17.10 以前のリリースからアップグレードした後のリバランサー設定

新しく作成されるデータベースの場合、リバランサーはデフォルトでオンであり、割り当てポリシーはバケットです。バケットポリシーは、フォレストの追加や削除の際に移動するデータはレガシーポリシーよりも少なくなり、決定論的です。

MarkLogic サーバーの以前のリリースからアップグレードすると、既存のデータベースのリバランサーはオフで、ポリシーはレガシーに設定されます。

フォレストレベルではどちらの場合もリバランサーがデフォルトでオンになっています。

18.0 階層型ストレージ

MarkLogic サーバーでは、ストレージおよび計算処理の環境が異なる複数の「階層」でデータを管理できます。最上位の階層では重要性の最も高いデータへの最速なアクセスが可能であり、最下位の階層では重要性の最も低いデータへの最遅なアクセスを提供します。Hadoop やパブリッククラウドなどのインフラストラクチャを利用することにより、膨大な量のデータを最下層に收容して、ストレージを経済的に拡張できます。データをさまざまなストレージ階層へと分離することで、コスト、パフォーマンス、可用性、柔軟性の間にあるトレードオフを最適化できます。

階層型ストレージは、XQuery、JavaScript、および REST API でサポートされます。この章では、REST API を使用した階層型ストレージの操作について説明します。REST API は、ストレージ管理スクリプトに統合できるすべての操作をサポートしています。

注： この機能を実環境で使用するには、階層型ストレージのライセンスが必要です。

この章は、次のセクションで構成されています。

- [この章で使われる用語](#)
- [階層型ストレージの概要](#)
- [レンジパーティション](#)
- [クエリパーティション](#)
- [パーティションの移行](#)
- [データベースのレンジパーティション設定](#)
- [データベースのクエリパーティション設定](#)
- [階層型ストレージ REST API の概要](#)
- [一般的なフォレストおよびパーティションの操作](#)
- [フォレストレベルのフェイルオーバーが設定されたパーティション](#)

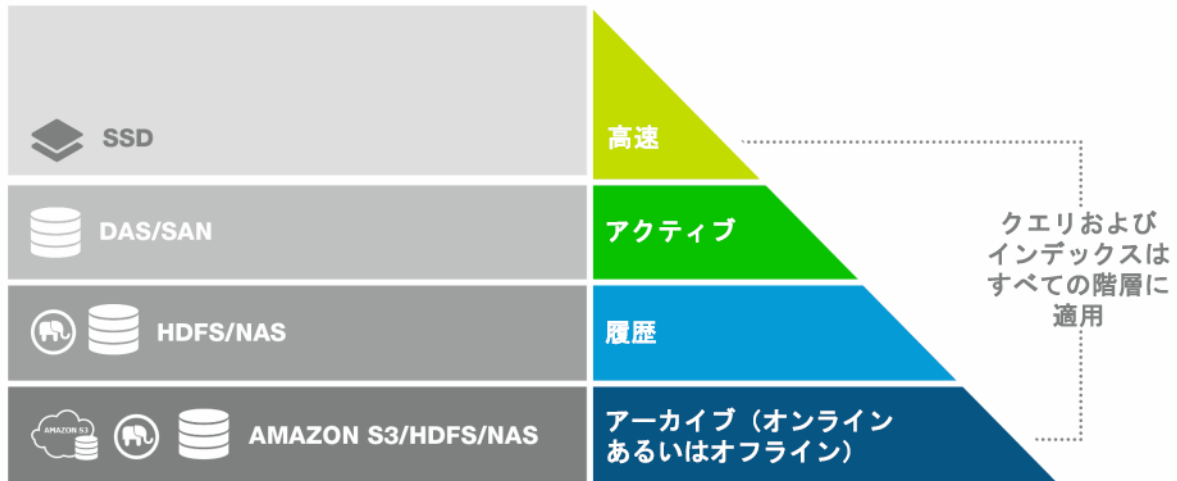
注： MarkLogic データを Amazon Elastic Compute Cloud (EC2) S3 バケットに格納している場合、us-east-1 リージョンの S3 バケットに存在するフォレストでは階層型ストレージ操作がサポートされません。

18.1 この章で使われる用語

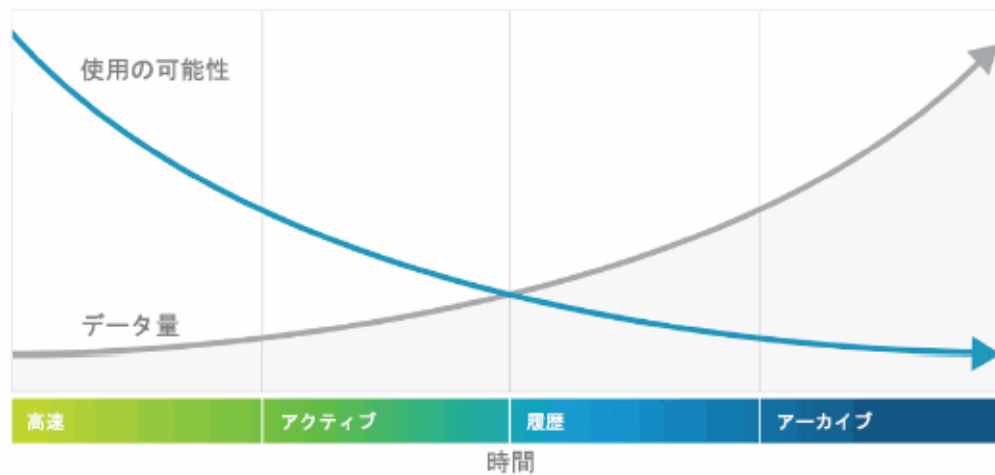
- 「パーティション」とは、同じ名前プレフィックスと同じパーティション定義を共有するフォレストの集まりです。一般に、パーティション内のフォレストは、同じ種類のストレージおよび設定（実行可能な更新、可用性、オンとなっているステータスなど）を共有します。パーティションは、フォレストの命名規則に基づきます。フォレストのパーティション名プレフィックスとフォレスト名の残りの部分は、ダッシュ (-) で区切られます。例えば、2011-0001 という名前のフォレストは、2011 パーティションに属します。
- 「レンジパーティション」とは、値のレンジが関連付けられているパーティションです。ドキュメントのパーティションキーがパーティションに指定されたレンジ内にある場合、そのドキュメントはそのレンジパーティションに格納されます。
- 「クエリパーティション」とは、クエリが関連付けられているパーティションです。クエリパーティションに指定されたクエリによって返されるドキュメントは、該当するクエリパーティションに格納されます。
- 「パーティションキー」は、レンジインデックス、コレクションレキシコン、またはフィールドが設定されている要素または属性を定義し、データベース内のレンジパーティションで設定されたレンジのコンテキストを定義します。パーティションキーはデータベースレベルの設定です。
- 「デフォルトパーティション」とは、レンジまたはクエリが定義されていないパーティションです。パーティションキーを持たないドキュメント、またはパーティションキーがパーティションのレンジやクエリに該当しないドキュメントは、デフォルトパーティションに格納されます。
- 「スーパーデータベース」とは、他のデータベース（サブデータベース）を含むデータベースであり、単一の論理データベースであるかのようにクエリの対象にできます。
- 「サブデータベース」とは、スーパーデータベースに含まれるデータベースです。
- 「アクティブデータ」とは、低レイテンシのクエリや更新が要求されるデータです。特定ドキュメントが「アクティブ」かどうかは、一般にドキュメントのリーゼンシー（経過時間）によって決まります。このためこれは時間の経過により変化します。
- 「履歴データ」は、最低レイテンシのクエリの対象としては「アクティブ」データほど重要ではありませんが、クエリするためにオンラインアクセスが必要です。通常、履歴データが更新されることはありません。
- 「アーカイブデータ」とは、オンラインストレージ階層における有用期間を超えて古くなったデータのことです。通常はオフラインになっています。
- 「オンライン」パーティションまたはフォレストは、クエリや更新が可能です。
- 「オフライン」パーティションまたはフォレストは、クエリに使用できませんが、クラストによって把握されます。データをオフラインにすると、RAM、CPU、およびネットワークリソースをオンラインデータ用に確保できるという利点があります。
- パーティションまたはフォレストの「可用性」とは、パーティションまたはフォレストのオンライン/オフラインのステータスを指します。

18.2 階層型ストレージの概要

MarkLogic の階層型ストレージ API により、データを、さまざまな階層にあるストレージ間で積極的かつ容易に移動させることが可能になります。例として、下図のように、データがさまざまなストレージデバイスでピラミッド形式に階層化される仕組みを視覚的に示します。

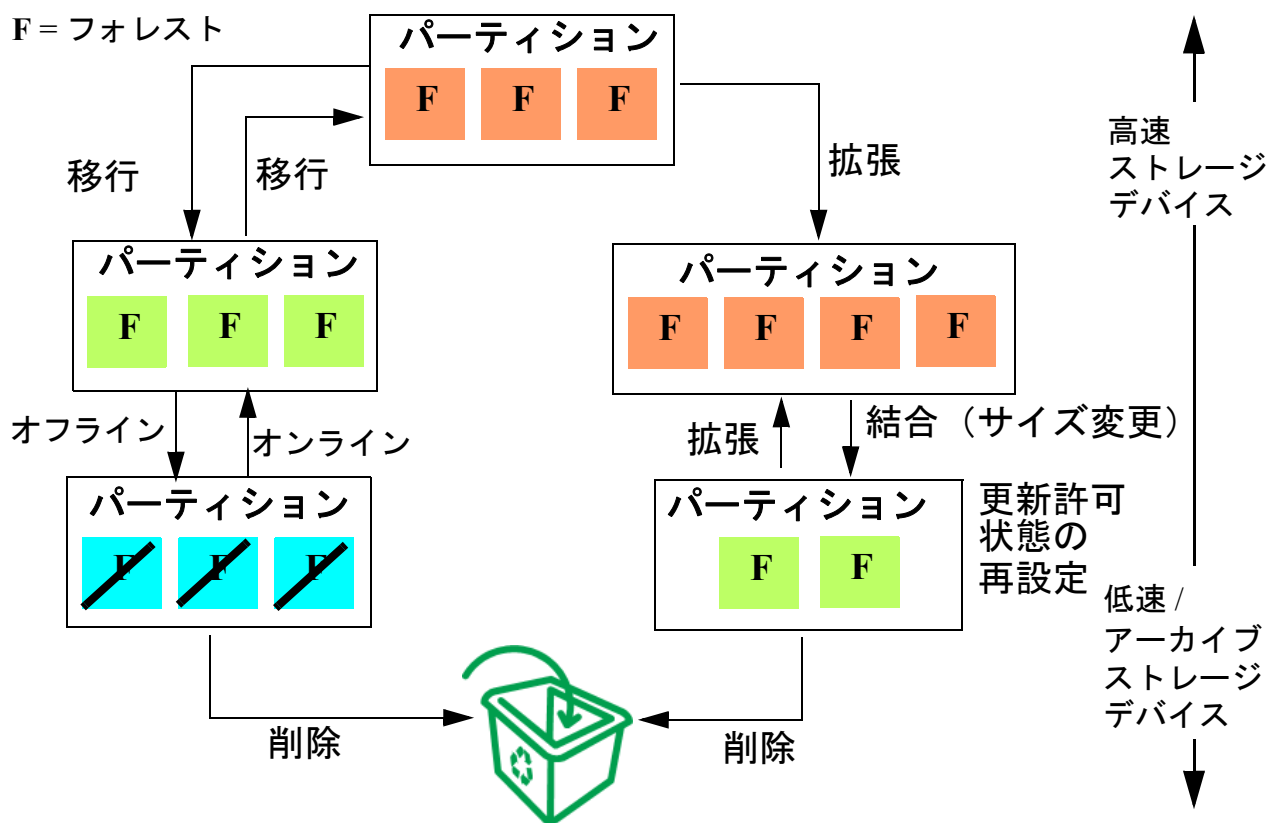


データが古くなり、更新やクエリでの利用の頻度が減った場合、これをより廉価かつ高密度なストレージデバイスに移行できます。これにより、より新しく、アクセスや更新の頻度が高いデータのために容量を空けることができます（下のグラフを参照）。



基本的な階層型ストレージの操作を下図に示します。

- パーティションを別のデータベース、ホスト、ディレクトリ（別のストレージデバイスへマウントされている場合もある）に移行する。
- パーティションのサイズを変更して、含まれるフォレストの数を拡張または縮小する。
- 多数のフォレストをシングルフォレストへ結合する。
- パーティションの更新許可状態を再設定する。例えば、パーティションを読み取り専用にして、フォレストのマージ用領域の予約が不要なデバイスにパーティションをよりコンパクトに格納できるようにします。
- パーティションをオフラインにしてアーカイブ化する。このパーティションデータはクエリ、更新、バックアップ、リストア、レプリケート操作に使用できません。
- パーティションをオンラインにして、再びパーティションデータを使用可能にする。
- 格納されているデータが有用期間を超えているパーティションを削除する。



警告 XA トランザクションの実行中にフォレストの移行、フォレストの結合、パーティションの移行、パーティションのサイズ変更を使用すると、データ消失のおそれがあります。

パーティションには次の 2 種類があります。

- [レンジパーティション](#)
- [クエリパーティション](#)

18.3 レンジパーティション

レンジパーティションは、同じ名前プレフィックスと同じ「レンジ割り当てポリシー」（「レンジ割り当てポリシー」（182 ページ）を参照）を共有するデータベースフォレストのグループで構成されます。

注： クラスタにフォレストを導入する際は、並列化および高可用性を得るために、ホスト間でフォレストとフォレストのレプリカを整合させる必要があります（『*Scalability, Availability, and Failover Guide*』を参照）。

パーティションのレンジは、そのパーティションに格納されるドキュメントの要素または属性の値の範囲を定義します。この要素または属性は、「パーティションキー」と呼ばれます。パーティションキーは、データベースに設定されたレンジインデックス、コレクションレキシコン、またはフィールドに基づきます。パーティションキーはデータベースに設定され、パーティションレンジはパーティションに設定されます。そのため、データベースにはレンジの異なる複数のパーティションを設定できます。

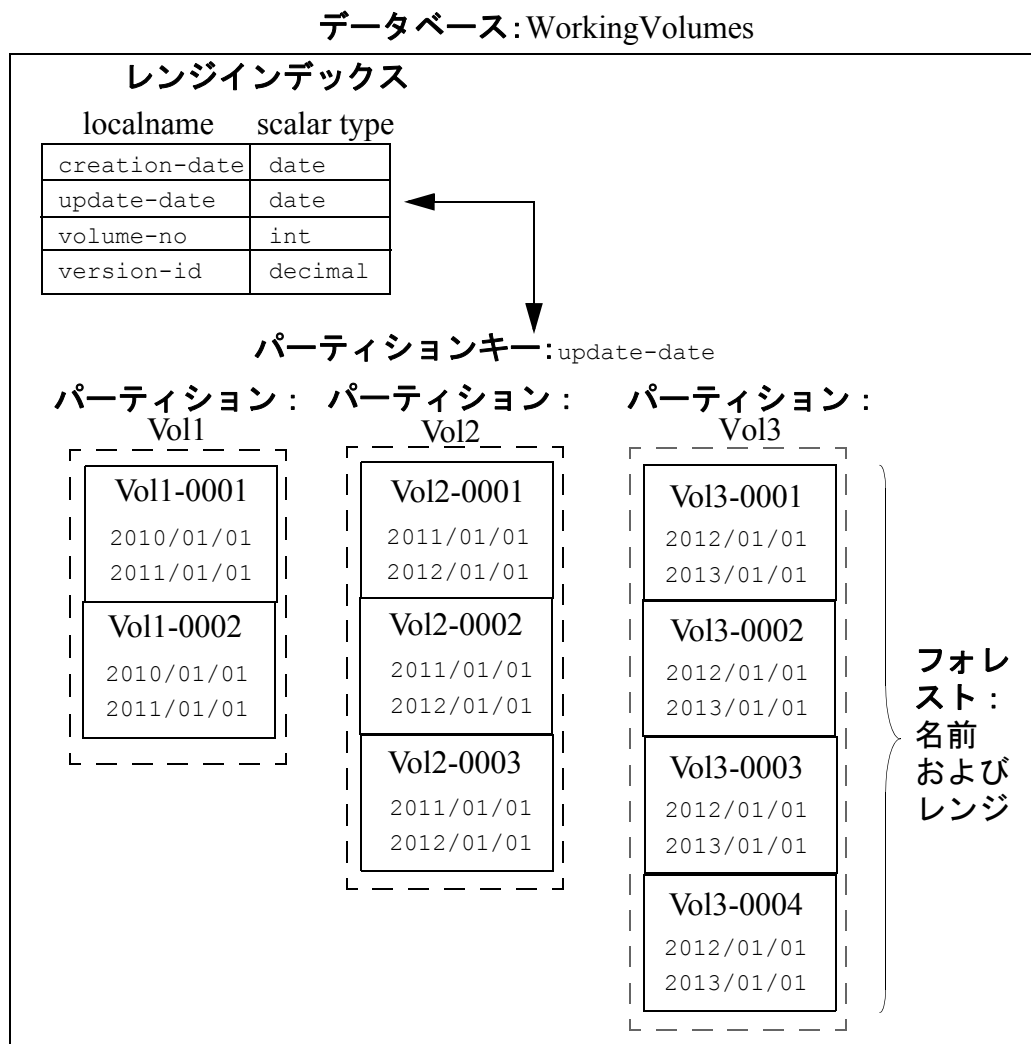
例えば、3 つのパーティションにグループ化された 9 つのフォレストが含まれるデータベース `WorkingVolumes` があるとします。`WorkingVolumes` データベースのレンジインデックスの中には、`update-date` 要素の要素レンジインデックスがあり、その型は `date` です。`WorkingVolumes` データベースでは、パーティションキーが `update-date` レンジインデックスで設定されています。`WorkingVolumes` データベースの各フォレストには、`date` 型の下限および上限のレンジ値が含まれています。次の表に示すように、このレンジ値はどのドキュメントがどのフォレストに格納されるのかを定義します。

パーティション名	フォレスト名 (プレフィックス - 名前)	パーティション レンジ 下限	パーティション レンジ 上限	下限を含む
Vol1	Vol1-0001 Vol1-0002	2010/01/01	2011/01/01	false
Vol2	Vol2-0001 Vol2-0002 Vol2-0003	2011/01/01	2012/01/01	false
Vol3	Vol3-0001 Vol3-0002 Vol3-0003 Vol3-0004	2012/01/01	2013/01/01	false

注： データベースで `Lower Bound Included`（下限を含む）が `false` に設定されている場合、パーティションレンジの下限は無視されます。この設定では、パーティションキー値が下限値にマッチするドキュメントはパーティションから除外され、上限値にマッチするドキュメントは含まれます。

この例では、update-date 要素値が 2011-05-22 であるドキュメントは、Vol2 パーティション内のいずれかのフォレストに格納されます。ドキュメントの update-date 要素値が 2012-01-02 以降に更新されると、ドキュメントは Vol3 パーティションへ自動的に移動します。パーティション間でドキュメントを再分散する方法は、データベーススリバランサーによって決定されます。詳細については「レンジ割り当てポリシー」(182 ページ)を参照してください。

次の図は、WorkingVolumes データベースです。レンジインデックス、パーティションキー、および含まれるパーティションとフォレストを示しています。



18.4 クエリパーティション

クエリパーティションは、同じ名前プレフィックスと同じ「クエリ割り当てポリシー」（「クエリ割り当てポリシー」（184 ページ）を参照）を共有するデータベースフォレストのグループで構成されます。

注： クエリパーティションは、ドキュメントをフィルタリングなしでクエリします。フィルタリングなしクエリの詳細については、『*Query Performance and Tuning Guide*』の章「[Fast Pagination and Unfiltered Searches](#)」を参照してください。

各クエリパーティションは、そのパーティションに格納されるドキュメントを決定するクエリに関連付けられています。クエリパーティションを作成するときは、パーティション番号を割り当てます。レンジパーティションとは異なり、クエリ割り当てポリシーを使用するパーティションに設定されるクエリは「重複」が可能です。つまり、1つのドキュメントが複数のパーティションに設定されたクエリにマッチする可能性があります。重複時は、番号の小さなパーティションが番号の大きなパーティションよりも優先して選択されます。

注： レンジ割り当てポリシーの場合と同様に、クエリ割り当てポリシーを設定するときは、デフォルトパーティションを定義してください。デフォルトパーティションが定義されていない場合、クエリパーティションに関連付けられていないデータベースフォレストが使用されます。

例えば、3つのクエリパーティションがあるとします。1つはデフォルトパーティションで、2つは次の種類のクエリに関連付けられたパーティションです。

クエリパーティション 1：（デフォルト -- クエリなし）

クエリパーティション 2：

要件	クエリタイプ
作者に「twain」が含まれる	ワード
ペーパーバック版がある	値
ペーパーバック版の価格が 9.00 ドル未満である	レンジ

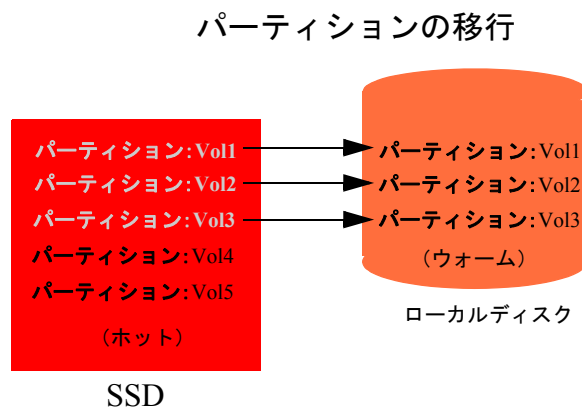
クエリパーティション 3：

要件	クエリタイプ
タイトルに「Adventures」が含まれる	ワード
登場人物に「Huck」が含まれる	ワード
分類が「フィクション」である	ワード

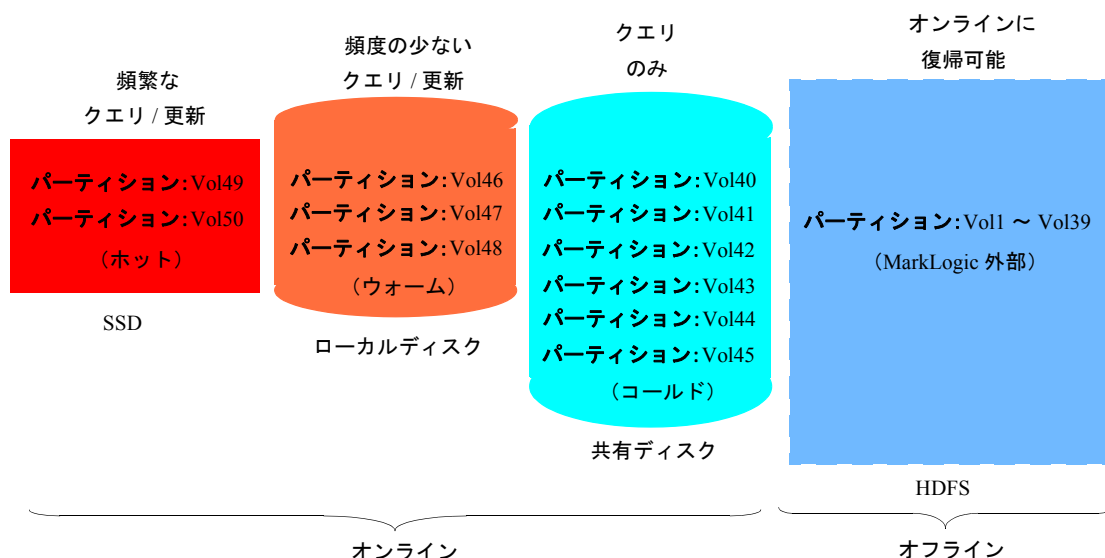
この例で、ドキュメント「Adventures of Huckleberry Finn」（「ハックルベリーフィンの冒険」）は両方のクエリにマッチしますが、クエリパーティション 2 に格納されます。こちらのほうが番号の小さいパーティションであるためです。一方、ドキュメント「Moby Dick」（「白鯨」）はどちらのクエリにもマッチしません。そのため、デフォルトのクエリパーティションであるパーティション 1 に格納されます。

18.5 パーティションの移行

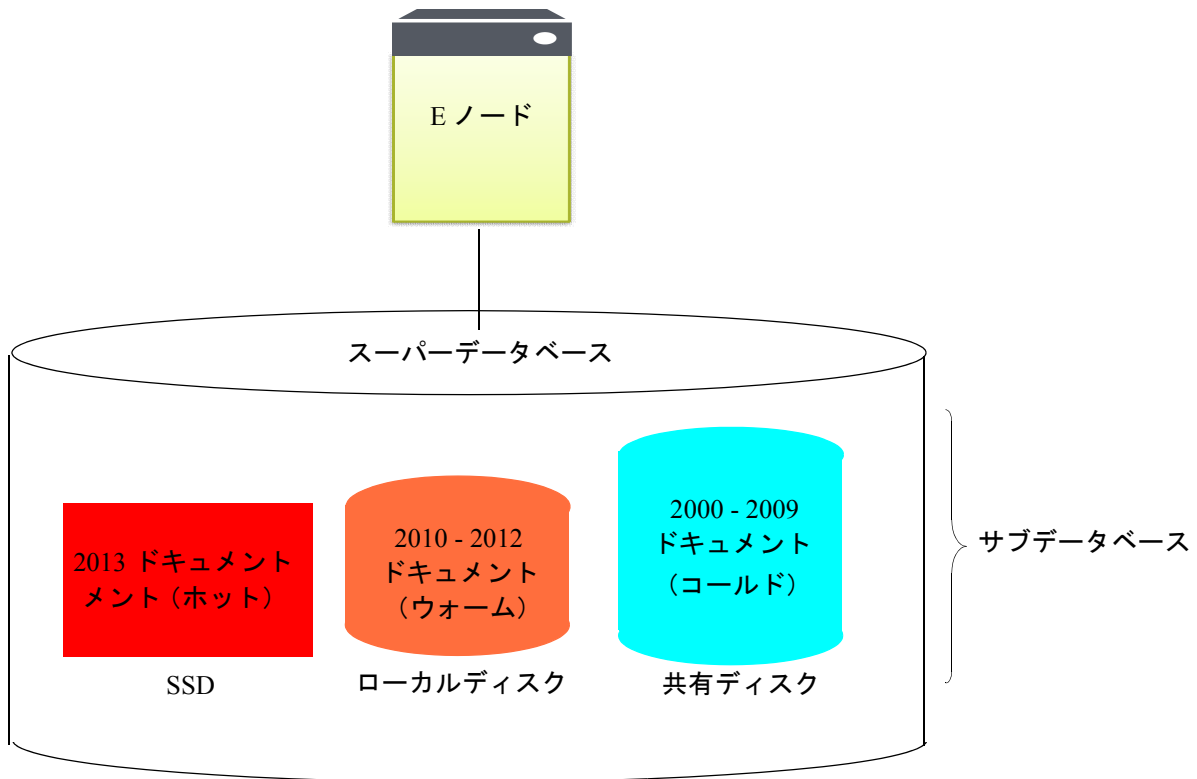
レンジパーティションとクエリパーティションは、どちらも異なる種類のストレージ間で移行できます。例えば、「レンジパーティション」（200 ページ）で作成したレンジパーティションで、数か月後にドキュメントの部数が 5 つに増加し、高速 SSD デバイス上にすべてを保持するには十分な領域がなくなったとします。そこで、最も古く最もクエリ数が少ない部分（Vol1 ~ Vol3）がローカルディスクドライブ（低速なストレージ階層）へ移行されます。



何年かのデータ増加後、ドキュメントの部数が 50 に増えました。ストレージ階層間で移行した後、パーティションは最終的に下図のようにストレージ階層間で分散されました。



複数のデータベースは、異なるストレージ階層で処理を実行していても、1つのクエリを複数のデータ階層にまたがって実行できるように「スーパーデータベース」へグループ化できます。スーパーデータベースに属するデータベースは「サブデータベース」と呼ばれます。1つのサブデータベースは複数のスーパーデータベースに属することができます。スーパーデータベースおよびサブデータベースの詳細については、「スーパーデータベースおよびクラスタ」(231 ページ) を参照してください。



18.6 データベースのレンジパーティション設定

レンジパーティションを使用する階層型ストレージスキームにデータベースを参加させる場合は、そのデータベースに次の設定が必要です。

- rebalancer enable が `true`
- リバランサーの assignment policy が `range`
- locking が `strict`
- パーティションキー用に設定されたレンジインデックス（「レンジインデックスおよびレキシコン」(356 ページ) を参照）
- パーティションキー（「レンジパーティションキーの定義」(205 ページ) を参照）
- レンジパーティション（「レンジパーティションの作成」(207 ページ) を参照）

警告 レンジパーティションを使用する階層型ストレージ向けに設定されたデータベース内のすべてのフォレストは、なんらかのパーティションに属している必要があります。

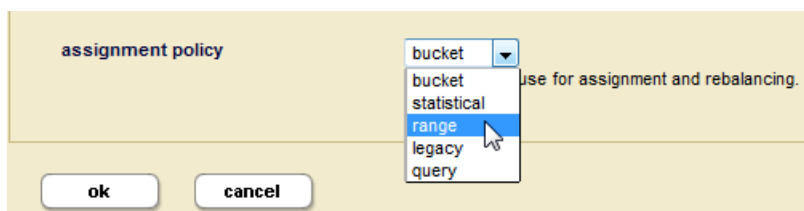
レンジ割り当てポリシーによるデータベースリバランサーの設定方法の詳細については、「レンジ割り当てポリシー」(182 ページ)、「データベースでのリバランサーの設定」(189 ページ)、および「フォレストでのリバランサーの設定」(190 ページ) を参照してください。

18.6.1 レンジパーティションキーの定義

パーティションキーは、格納されているドキュメントに共通する要素または属性のことです。ドキュメントのこの要素または属性の値によって、ドキュメントの格納先パーティションが決まります。パーティションキーは、データベースに設定されたレンジインデックス、コレクションレキシコン、または同名のフィールドに基づきます。パーティションキーで使用されるレンジインデックス、コレクションレキシコン、またはフィールドは、パーティションキーの作成前に作成する必要があります。

例えば、すべてのドキュメントに日付値の `update-date` 要素があるとします。次の手順では、`update-date` 要素のパーティションキーを作成する方法について説明します。

1. データベースに `date` 型の要素レンジインデックス `update-date` を作成します。要素レンジインデックスを作成する方法の詳細については、「要素レンジインデックスの定義」(366 ページ) を参照してください。
2. 管理画面でデータベースの設定ページを開き、[assignment policy] を [range] に設定します。[assignment policy] の下にその他の設定が表示されます。



- パーティションキーの値が下限値にマッチするドキュメントを含めて、上限値にマッチするドキュメントを除外する場合は [Lower Bound Included] を [true] に設定します。パーティションキーの値が下限値にマッチするドキュメントを除外して、上限値にマッチするドキュメントを含める場合は [Lower Bound Included] を [false] に設定します。例えばレンジが 2011-01-01 (下限) から 2012-01-01 (上限) であり、[Lower Bound Included] が [false] に設定されている場合、update-date 値が 2011-01-01 であるドキュメントはこのパーティションに含まれませんが、update-date 値が 2011-01-02 および 2012-01-01 であるドキュメントは含まれます。
- パーティションキーとして使用するレンジインデックス、フィールド、またはコレクションレキシコンの型およびスカラー型に注意してください。この例では、スカラー型が date である要素レンジインデックスを使用します。ドロップダウンメニューでインデックスおよびスカラー型を設定すると、データベースに設定された一致するレンジインデックス、フィールド、またはコレクションレキシコンがリスト表示されます。

assignment policy

range

What policy to use for assignment and rebalancing.

true false

Lower Bound Included.

Element

int

An atomic type specification.

Available range indexes by scalar type

- パーティションキーとして使用するレンジインデックス、フィールド、またはコレクションレキシコンを選択します。この例では update-date です。

assignment policy

range

What policy to use for assignment and rebalancing.

true false

Lower Bound Included.

Element

date

Range indexes type. An atomic type specification.

Name

update-date

creation-date

Available range indexes by scalar type

18.6.2 レンジパーティションの作成

レンジパーティションは、フォレストの命名規則に基づきます。フォレストのパーティション名プレフィックスとフォレスト名の残りの部分は、ダッシュ (-) で区切られます。例えば、June-0001 という名前のフォレストは、June パーティションに属します。

注： レンジが設定されたパーティションを作成する前に、デフォルトパーティション（レンジなしのパーティション）を作成することをお勧めします。そうすると、その他のパーティションの作成が完了する前に、デフォルトパーティションにドキュメントを読み込むことができます。レンジを使用する新しいパーティションが作成されると、ドキュメントはデフォルトパーティションからマッチするレンジのパーティションへ自動的に移動します。

警告 階層型ストレージ用に設定されたデータベース内にあるすべてのフォレストは、なんらかのパーティションに属している必要があります。

レンジパーティションは、次の 2 種類の方法で作成できます。

- [新しいフォレストによるレンジパーティションの作成](#)
- [既存フォレストによるレンジパーティションの作成](#)

18.6.2.1 新しいフォレストによるレンジパーティションの作成

POST:/manage/v2/databases/{id|name}/partitions REST リソースアドレスを使用すると、空のフォレストを含む新しいレンジパーティションを作成できます。レンジパーティションを作成するときは、パーティションレンジ、およびパーティションに作成するフォレストの数を指定します。クラスタ内の複数のホストに対してレンジパーティションを作成するように指定することもできます。この場合は、指定された数のフォレストが各ホストに作成されます。

例えば、以下はレンジパーティション 2011 をホスト MyHost1 および MyHost2 の Documents データベースに作成します。レンジは 2011-01-01 ~ 2012-01-01 であり、MyHost1 には 4 つの空のフォレスト 2011-0001、2011-0002、2011-0003、2011-0004、および MyHost2 には 4 つの空のフォレスト 2011-0005、2011-0006、2011-0007、2011-0008 が作成されます。

```
$ cat create-partition.xml
<partition xmlns="http://marklogic.com/manage">
  <partition-name>2011</partition-name>
  <upper-bound>2012-01-01</upper-bound>
  <lower-bound>2011-01-01</lower-bound>
  <forests-per-host>4</forests-per-host>
  <hosts>
    <host>MyHost1</host>
    <host>MyHost2</host>
  </hosts>
</partition>

$ curl --anyauth --user user:password -X POST \
-d @create-partition.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/Documents/partitions
```

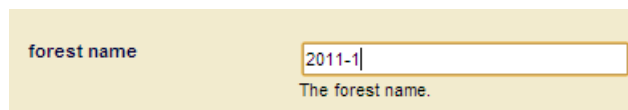
共有ディスクまたはローカルディスクのフェイルオーバー用にレプリカフォレストを作成する options 要素を含めることもできます。詳細については、「フォレストレベルのフェイルオーバーが設定されたパーティション」(229 ページ) を参照してください。

18.6.2.2 既存フォレストによるレンジパーティションの作成

フォレストの名前をレンジパーティションの命名規約に準拠して変更するだけで、既存のフォレストからレンジパーティションを作成できます。例えば 4 つのフォレスト 1-2011、2-2011、3-2011、4-2011 があるとします。1-2011 を 2011-1 に変更するなどして、これら 4 つのフォレストからレンジパーティション 2011 を作成できます。また、名前を変更した各フォレストで共通のレンジを指定するか、またはレンジフィールドを空にしてフォレストがデフォルトレンジパーティションに属するように指定する必要があります。デフォルトレンジパーティションは、パーティションキーの値が他のレンジパーティションに設定されたレンジのいずれにも収まらないドキュメントを格納します。

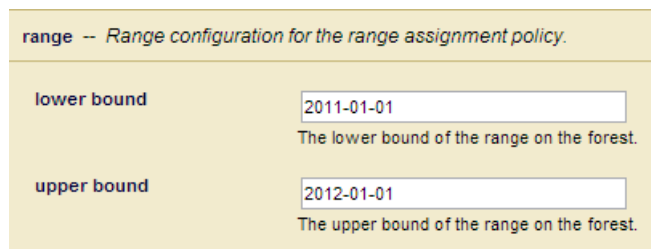
例えばフォレスト名を 1-2011 から 2011-1 に変更し、レンジを 2011-01-01 ~ 2012-01-01 に設定するには、次の手順を実行します。

1. 管理画面の [Forest Configuration] ページを開きます（「フォレストの作成」(292 ページ) を参照）。
2. [forest name] フィールドで、名前を 1-2011 から 2011-1 に変更します。



forest name
The forest name.

3. [Forest Configuration] ページの [range] ページで、[lower bound] 値を 2011-01-01、[upper bound] 値を 2012-01-01 に設定します。



range -- Range configuration for the range assignment policy.

lower bound
The lower bound of the range on the forest.

upper bound
The upper bound of the range on the forest.

4. [ok] をクリックします。

注： この操作は、XQuery、JavaScript、および REST API を使用して実行することもできます。例えば XQuery では `admin:forest-rename` 関数および `admin:forest-set-range-policy-range` 関数を使用します。

18.7 データベースのクエリパーティション設定

クエリパーティションを使用する階層型ストレージにデータベースを参加させる場合は、次の設定が必要です。

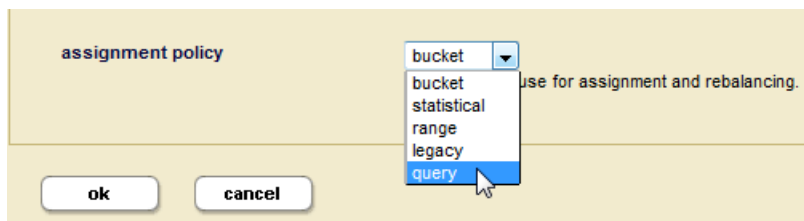
- rebalancer enable が `true`
- リバランサーの assignment policy が `query`
- locking が `strict`
- クエリ対象の要素またはプロパティにインデックスが付けられている
- クエリパーティション（「クエリパーティションの作成」（210 ページ）を参照）

注： レンジパーティションとは異なり、階層型ストレージ用に設定されたデータベース内にあるすべてのフォレストがクエリパーティションに属している必要はありません。

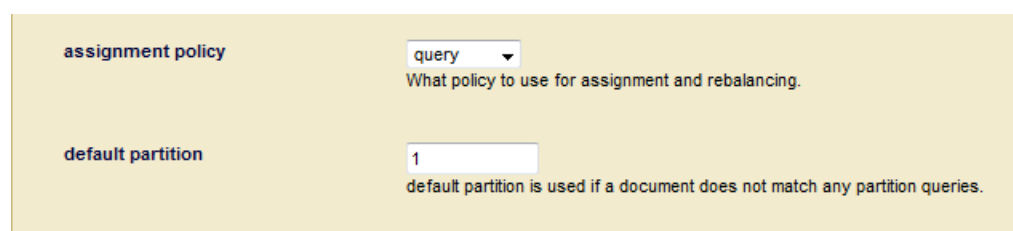
クエリ割り当てポリシーによるデータベースリバランサーの詳細については、「クエリ割り当てポリシー」（184 ページ）、「データベースでのリバランサーの設定」（189 ページ）、および「フォレストでのリバランサーの設定」（190 ページ）を参照してください。

次の手順では、クエリ割り当てポリシーを使用するようにデータベースを設定する方法について説明します。

1. 管理画面でデータベースの設定ページを開き、[assignment policy] を [query] に設定します。[assignment policy] の下に [default partition] 設定が表示されます。



2. 必要に応じて、[default partition] フィールドで、デフォルトクエリパーティションのパーティション番号を入力できます。デフォルトクエリパーティションを定義しない場合、データベースにはクエリパーティションに属さないフォレストが必要です。そのフォレストは、デフォルトパーティションと同じ役割を担います。



18.7.1 クエリパーティションの作成

クエリパーティションを作成するときは、クエリパーティション名、番号、およびクエリパーティションに作成するフォレストの数を指定します。クラスタ内の複数のホストに対してクエリパーティションを作成するように指定することもできます。この場合は、指定された数のフォレストが各ホストに作成されます。

クエリパーティションは、フォレストの命名規則に基づきます。フォレストのパーティション名プレフィックスとフォレスト名の残りの部分は、ダッシュ (-) で区切られます。例えば、`tier1-0001` という名前のフォレストは、`tier1` パーティションに属します。レンジパーティションとは異なり、階層型ストレージ用に設定されたデータベース内にあるすべてのフォレストがクエリパーティションに属している必要はありません。

注： デフォルトクエリパーティション（クエリなしのパーティション）を作成することをお勧めします。そうすると、その他のパーティションの作成が完了する前に、デフォルトパーティションにドキュメントを読み込むことができます。クエリを使用する新しいパーティションが作成されると、ドキュメントはデフォルトパーティションからマッチするクエリのクエリパーティションへ自動的に移動します。

クエリ割り当てポリシーによるデータベースリバランサーの設定方法の詳細については、「クエリ割り当てポリシー」（184 ページ）、「データベースでのリバランサーの設定」（189 ページ）、および「フォレストでのリバランサーの設定」（190 ページ）を参照してください。

クエリパーティションはフィルタリングなしクエリを実行します。つまり、結果は検証用にフィルタリングされません。フィルタリングなしクエリの詳細については、『*Query Performance and Tuning Guide*』の章「[Fast Pagination and Unfiltered Searches](#)」を参照してください。

例えば、以下は 2 つのフォレストがあるクエリパーティションを `MyHost1` の `Documents` データベースに、番号 `1`、名前 `tier1` で作成します。

```
curl -X POST --anyauth --user admin:admin \
-H "Content-type: application/json" \
-d '{
  "partition-name": "tier1",
  "partition-number": "1",
  "forests-per-host": 2,
  "host": [ "MyHost1" ],
  "option": [ "failover=none" ]
}' \
http://MyHost1:8002/manage/v2/databases/Documents/partitions
```

18.7.2 クエリパーティションのクエリ割り当てポリシーの設定

クエリパーティションを作成したら、`POST:/manage/v2/databases/{id|name}/partition-queries` REST リソースアドレスを使用して、そのクエリパーティションをクエリ割り当てポリシーに割り当てることができます（「クエリ割り当てポリシー」（184 ページ）を参照）。

注： クエリパーティションを作成する前に、クエリに必要なインデックスを作成する必要があります。

XML 形式のクエリ割り当てポリシーは次のようになります。

```
<partition-query-properties
xmlns="http://marklogic.com/manage/partition-query/properties">
  <partition-number>1</partition-number>
  <query>
    ....cts:query.....
  </query>
</partition-query-properties>
```

JSON 形式のクエリ割り当てポリシーは次のようになります。

```
{
  "partition-number": "1",
  "query": {
    ....cts:query.....
  }
}
```

検索部分は `cts:query` 式です（『*Search Developer's Guide*』の章「[Composing cts:query Expressions](#)」を参照）。パーティションごとに `cts:query` は 1 つだけ使用できます。

クエリでは、データベースで適切なインデックスが設定されている必要があります。クエリの複雑さが、挿入やリバランスのパフォーマンスに影響を与えます。そのため、ワイルドカードマッチングなどの低速なクエリは推奨されません。

例えば、先ほど作成した `tier1` クエリパーティションヘワード「Manager」または「Engineer」が含まれるすべてのドキュメントを移動するには、次のように実行します。

```
$ cat query1.xml
<partition-query-properties
xmlns="http://marklogic.com/manage/partition-query/properties">
  <partition-number>1</partition-number>
  <query>
    <cts:or-query xmlns:cts="http://marklogic.com/cts">
      <cts:word-query>
        <cts:text xml:lang="en">Manager</cts:text>
      </cts:word-query>
      <cts:word-query>
        <cts:text xml:lang="en">Engineer</cts:text>
      </cts:word-query>
    </cts:or-query>
  </query>
</partition-query-properties>

curl -X POST --anyauth -u admin:admin \
-H "Content-Type:application/xml" -d @query1.xml \
http://gordon-1:8002/manage/v2/databases/Schemas/partition-queries
```

次のクエリ割り当てポリシーは、「LastModified」が過去 1 年以内であるドキュメントにマッチします。

```
<partition-query-properties>
  <partition-number>1</partition-number>
  <query>
    <element-range-query operator=">=">
      <element>LastModified</element>
      <value type="xs:yearMonthDuration">P1Y</value>
    </element-range-query>
  </query>
</partition-query-properties>
```

同じクエリ割り当てポリシーは、JSON では次のようになります。

```
{
  "partition-number": 1,
  "query": {
    "element-range-query": {
      "operator": ">=",
      "element": "LastModified",
      "value": {
        "type": "xs:yearMonthDuration",
        "_value": "P1Y"
      }
    }
  }
}
```

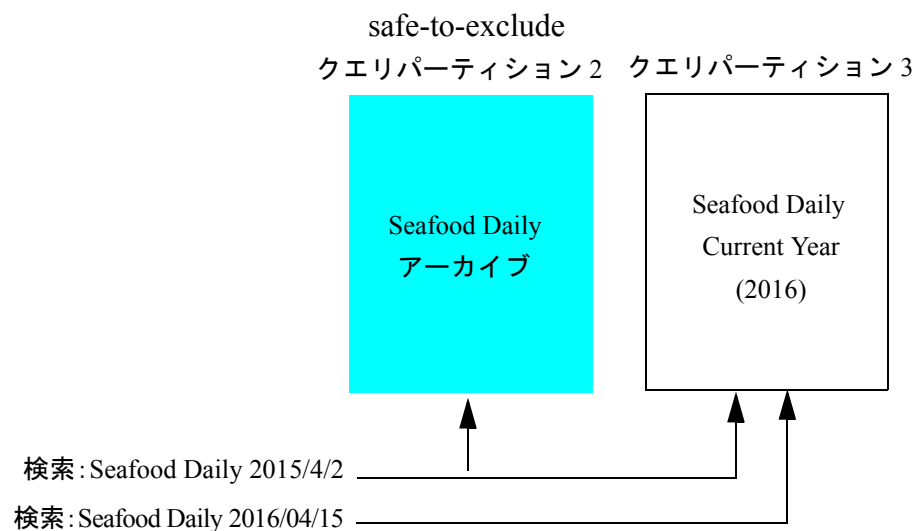
18.7.3 クエリパーティションの分離

デフォルトでは、検索クエリが MarkLogic に渡されると、パーティションに設定されたクエリ割り当てポリシーに関係なく、すべてのクエリパーティションが検索されます。このようなオーバーヘッドを避けるため、`tieredstorage:partition-set-exclusion-enabled` 関数を使用して、クエリパーティションで `safe-to-exclude` を設定できます。これにより、検索クエリがそのパーティションに設定されたクエリ割り当てポリシーにマッチしない場合は、そのパーティションが検索対象になりません。

日時に基づいてドキュメントがクエリパーティション間で分散されるときには、常に特定の階層（通常は最新のドキュメントを保持する階層）を検索するオプションが必要な場合があります。これは、その階層内の一部のドキュメントが別の階層に移行されようとしているがまだ移動していない可能性があるためです。そのため、検索で「下位」の階層に設定されたクエリのみにもマッチする場合、マッチしない「上位」の階層も検索して、まだ下層に移動していないドキュメントからマッチするものを探します。

例えば、以下のようにドキュメント「Seafood Daily」を保持する 2 つのクエリパーティションがあります。それぞれのクエリ割り当てポリシーは、ドキュメントの日付を現在の日付と比較し、ドキュメントをソートします。一方のパーティションには今年の発行物が含まれ、他方は昨年以前の発行物がアーカイブされます。アーカイブとして機能するクエリパーティションには `safe-to-exclude` が設定され、今年の発行物が含まれるクエリパーティションにはこのオプションが設定されません。

この例では今年（2016 年）であり、検索クエリが Archive パーティションのクエリにマッチする場合、Current Year パーティションも検索されます。ただし、Current Year パーティションにマッチする検索クエリは、Archive パーティションを除外します。



18.8 階層型ストレージ REST API の概要

階層型ストレージは、XQuery、JavaScript、および REST API でサポートされます。繰り返し実行されるストレージ管理操作を自動化するためにストレージ管理スクリプトに統合するすべての操作は、REST API で提供されます。ただし、初回 1 度限りのセットアップ操作の一部（データベースでのレンジポリシーやパーティションキーの設定に関連する操作など）は、管理画面および XQuery API でのみサポートされます。

注： 階層型ストレージ REST API は、JSON 形式と XML 形式の両方をサポートします。この章の例では、すべて XML 形式を使用します。

このセクションで取り上げるトピックは次のとおりです。

- [非同期操作](#)
- [権限](#)
- </manage/v2/databases/{id|name}/partitions>
- </manage/v2/databases/{id|name}/partitions/{name}>
- </manage/v2/databases/{id|name}/partitions/{name}/properties>
- </manage/v2/databases/{id|name}/partition-queries>
- </manage/v2/databases/{id|name}/partition-queries>
- </manage/v2/databases/{id|name}/partition-queries/{partition-number}>
- </manage/v2/databases/{id|name}/partition-queries/{partition-number}/properties>
- </manage/v2/forests>
- </manage/v2/forests/{id|name}>
- </manage/v2/forests/{id|name}/properties>

18.8.1 非同期操作

パーティションのサイズ変更や移行、フォレストの移行や結合などの操作は、非同期に処理されます。これは、このような操作では大量のデータを移動するために、制御がスクリプトに復帰するまでに通常妥当と考えられるよりも多くの時間がかかるためです。そのような非同期操作は、チケットエンドポイントを再使用してトラッキングされません。この非同期プロセスは、次の手順で説明するように、`GET:/manage/v2/tickets/{tid}?view=process-status` によって開始されます。

生成されたチケットは、次の形式で返されます。

```
/manage/v2/tickets/{id}?view=process-status.
```

操作のステータスを表示するには、URL にアクセスします。例えば、返されたチケットが次のようになっているとします。

```
/manage/v2/tickets/8681809991198462214?view=process-status
```

そしてホストが `MyHost` である場合は、操作のステータスを表示するために次の URL を使用します。

```
http://MyHost:8002/manage/v2/tickets/8681809991198462214?view=process-status
```

注： 過去のチケット情報は、チケットのデフォルトビューを表示してアクセスできます。

18.8.2 権限

このセクションで説明するリソースアドレスには次の権限が必要です。

- GET 操作には `manage-user` 権限が必要です。
- PUT、POST、および DELETE 操作には `manage-admin` 権限が必要です。

18.8.3 /manage/v2/databases/{id|name}/partitions

メソッド	説明	パラメータ	等価な XQuery
GET	データベース上のパーティションのリストを取得します。	format? (json xml)	tieredstorage:database-partitions
POST	データベースにレンジパーティションまたはクエリパーティションを追加します。	format? (json xml)	tieredstorage:range-partition-create tieredstorage:query-partition-create

例については、次を参照してください。

- [パーティションの表示](#)
- [レンジパーティションの作成](#)
- [クエリパーティションの作成](#)

18.8.4 /manage/v2/databases/{id|name}/partitions/{name}

メソッド	説明	パラメータ	等価な XQuery
GET	パーティションの概要を取得します。パーティションを含んでいるデータベースへのリンク、メンバーフォレストへのリンク、設定へのリンクなどが含まれます。	format? (json xml)	tieredstorage:partition-forests
DELETE	パーティションを削除します。	delete-data? (true false)	tieredstorage:partition-delete
PUT	パーティションで次のいずれかの操作を呼び出します。 <ul style="list-style-type: none"> • サイズ変更（非同期） • 転送（同期） • 移行（非同期） 	format? (json xml)	tieredstorage:partition-resize tieredstorage:partition-transfer tieredstorage:partition-migrate

例については、次を参照してください。

- [パーティションの削除](#)
- [パーティションのサイズ変更](#)
- [データベース間のパーティション移動](#)
- [フォレストおよびパーティションの移行](#)

18.8.5 /manage/v2/databases/{id|name}/partitions/{name}/properties

メソッド	説明	パラメータ	等価な XQuery
GET	パーティションプロパティを取得します (オン、更新許可)。	format? (json xml)	
PUT	パーティションプロパティを変更します (更新許可、オンライン/オフライン)。	format? (json xml)	tieredstorage:partition-set-availability tieredstorage:partition-set-updates-allowed

例については、次を参照してください。

- [フォレストおよびパーティションのオフライン/オンライン化](#)
- [パーティションの更新許可状態の設定](#)

18.8.6 /manage/v2/databases/{id|name}/partition-queries

メソッド	説明	パラメータ	等価な XQuery
GET	指定されたデータベースに設定されているクエリパーティションのクエリ割り当てポリシーを取得します。	format? (json xml)	tieredstorage:partition-queries
POST	クエリパーティションのクエリ割り当てポリシーを設定します。		tieredstorage:partition-set-query

例については、次を参照してください。

- [クエリパーティションのクエリ割り当てポリシーの設定](#)

18.8.7 /manage/v2/databases/{id|name}/partition-queries/{partition-number}

メソッド	説明	パラメータ	等価な XQuery
GET	指定された番号のクエリパーティションのクエリ割り当てポリシーを取得します。	format? (json xml)	tieredstorage:partition-get-query
DELETE	指定された番号のクエリパーティションのクエリ割り当てポリシーを削除します。		tieredstorage:partition-delete-query

18.8.8 /manage/v2/databases/{id|name}/partition-queries/{partition-number}/properties

メソッド	説明	パラメータ	等価な XQuery
GET	指定された番号のクエリパーティションの、クエリのプロパティを取得します。	format? (json xml)	tieredstorage:partition-get-query
PUT	指定された番号のクエリパーティション内のクエリ割り当てポリシーを更新します。	format? (json xml)	tieredstorage:partition-set-query

18.8.9 /manage/v2/forests

メソッド	説明	パラメータ	等価な XQuery
GET	フォレストの概要およびリストを取得します。	format? (json xml) view database-id group-id host-id fullrefs	admin:get-forest-ids xdmp:forests
POST	新しいフォレストを作成します。	format? (json xml)	admin:forest-create
PUT	フォレストで次のいずれかの操作を呼び出します。 <ul style="list-style-type: none"> • forest-combine • forest-migrate これらの操作は非同期です。	format? (json xml)	tieredstorage:forest-combine tieredstorage:forest-migrate

例については、次を参照してください。

- [フォレストおよびパーティションの移行](#)
- [フォレストの結合](#)

18.8.10 /manage/v2/forests/{id|name}

メソッド	説明	パラメータ	等価な XQuery
GET	フォレストの概要を取得します。	format? (json xml) view	admin:forest-get-*
POST	フォレストの状態変更を開始します。	state (clear merge restart attach detach retire employ)	xdmp:forest-clear xdmp:merge xdmp:forest-restart admin:database-attach-forest admin:database-detach-forest admin:database-retire-forest admin:database-employ-forest
DELETE	フォレストを削除します。	level (config-only full)	admin:forest-delete

例については、次を参照してください。

- [フォレストのリタイア](#)

18.8.11 /manage/v2/forests/{id|name}/properties

メソッド	説明	パラメータ	等価な XQuery
GET	フォレストのプロパティを取得します。	format? (json xml)	admin:forest-get-enabled admin:forest-get-rebalancer-enable admin:forest-get-updates-allowed admin:database-get-attached-forests admin:forest-get-failover-enable admin:forest-get-availability
PUT	フォレストのプロパティ変更を開始します。プロパティは次のとおりです。 フォレストのオン / オフ リバランサーのオン / オフ 更新許可の変更 フェイルオーバーホストまたはレプリカフォレストの指定 可用性	format? (json xml)	admin:forest-set-enabled admin:forest-set-rebalancer-enable admin:forest-set-updates-allowed admin:database-attach-forest admin:database-detach-forest admin:forest-set-failover-enable admin:forest-set-availability

18.9 一般的なフォレストおよびパーティションの操作

このセクションでは、次のパーティション操作について説明します。

- [パーティションの表示](#)
- [フォレストおよびパーティションの移行](#)
- [パーティションのサイズ変更](#)
- [データベース間のパーティション移動](#)
- [フォレストの結合](#)
- [フォレストのリタイア](#)
- [フォレストおよびパーティションのオフライン/オンライン化](#)
- [パーティションの更新許可状態の設定](#)
- [パーティションの削除](#)

一部の操作は非同期で実行され、操作のステータスを確認するために使用できるチケット番号をすぐに返します。例えば、次が返されるとします。

```
<link><kindref>process-status</kindref><uriref>/manage/v2/tickets/4678516920057381194?view=process-status</uriref></link>
```

この場合は、次のようなリソースアドレスを入力することで操作のステータスを確認できます。

```
http://MyHost:8002/manage/v2/tickets/4678516920057381194?view=process-status
```

非同期プロセスの詳細については、「非同期操作」（215 ページ）を参照してください。

18.9.1 パーティションの表示

パーティションの情報すべてを返すことができます。

例えば、Documents データベースの 2011 レンジパーティションの詳細を返すには、次を実行します。

```
curl -X GET --anyauth --user admin:admin --header \
"Content-Type:application/xml" \
http://MyHost:8002/manage/v2/databases/Documents/partitions/2011
```

18.9.2 フォレストおよびパーティションの移行

フォレストおよびパーティションは、ストレージデバイス間を移行できます。例えば、SSD 上のレンジパーティションが古くなってクエリの頻度が減少したら、低速で低コストのストレージデバイスに移動して、クエリ頻度の多いレンジパーティション用に領域を空けることができます。

例えば、`Documents` データベースの `2011` レンジパーティションがホスト `MyHost` のローカルディスクにマウントされているとします。`2011` レンジパーティションをホスト `OurHost` の共有ディスクにマウントされている `/warm-storage` データディレクトリに移行するには、次を実行します。

```
$ cat migrate-partition.xml
<migrate xmlns="http://marklogic.com/manage">
  <hosts>
    <host>OurHost</host>
  </hosts>
  <data-directory>/warm-storage</data-directory>
  <options>
    <option>failover=none</option>
    <option>local-to-shared</option>
  </options>
</migrate>

$ curl --anyauth --user user:password -X PUT \
-d @migrate-partition.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/Documents/partitions/2011
```

注： `data-directory` を指定しない場合、デフォルトのデータディレクトリが使用されます。

階層型ストレージの移行操作では、種類の異なるストレージの間でフォレストまたはパーティションを移行できます。4つの移行オプションを次の表に示します。選択する移行オプションによって、移行操作中に階層型ストレージによって実行される手順が決まります。

移行オプション	説明
local-to-local (デフォルト)	この移行によってデータをローカルストレージからローカルストレージへ移動することを示します。これは移行オプションが指定されない場合のデフォルトであり、ストレージの種類はデータディレクトリパスから取得できません。
local-to-shared	この移行によってデータをローカルストレージから共有ストレージへ移動することを示します。この種類の移行は、ホストの変更をサポートします。
shared-to-local	この移行によってデータを共有ストレージからローカルストレージへ移動することを示します。この種類の移行は、ホストの変更をサポートします。
shared-to-shared	この移行によってデータを共有ストレージから共有ストレージへ移動することを示します。この種類の移行は、ホストの変更をサポートします。

PUT: /manage/v2/forests リソースアドレスを使用して、個々のフォレストを移行できます。例えばフォレスト 2011-0001 および 2011-0002 がホスト MyHost のローカルディスクにマウントされているとします。これらのフォレストをホスト OurHost の共有ディスクにマウントされている /warm-storage データディレクトリに移行するには、次を実行します。

```
$ cat migrate-forests.xml
<forest-migrate xmlns="http://marklogic.com/manage">
  <forests>
    <forest>2011-0001</forest>
    <forest>2011-0002</forest>
  </forests>
  <host>MyHost</host>
  <data-directory>/warm-storage</data-directory>
  <options>
    <option>local-to-shared</option>
  </options>
</forest-migrate>

$ curl --anyauth --user user:password -X PUT \
-d @migrate-forests.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/forests
```

注： フォレストでフェイルオーバーが設定されている場合は、フォレストまたはパーティションの移行操作を実行した後でデータベースのフルバックアップを実行し、不具合があったときにデータをリカバリーできるようにしてください。また、フェイルオーバーが設定されている場合は移行操作に時間がかかるため、移行操作のタイムアウト設定の時間を延ばさなければならないことがあります。

18.9.3 パーティションのサイズ変更

パーティション内のフォレスト数を増減できます。サイズ変更操作が完了すると、パーティションフォレスト内のドキュメントは均等に分散するようにリバランスされます。

例えば、2011 レンジパーティションのサイズを 5 フォレストに変更するには、次を実行します。

```
$ cat resize-partition.xml
<resize xmlns="http://marklogic.com/manage">
  <forests-per-host>5</forests-per-host>
  <hosts>
    <host>MyHost</host>
  </hosts>
</resize>

$ curl --anyauth --user user:password -X PUT \
-d @resize-partition.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/Documents/partitions/2011
```

パーティションのサイズ変更だけでなく、ペイロードで異なるホストを指定しても別のホストにパーティションを移行できます。さらに、いずれかの移行オプションを指定して（「フォレストおよびパーティションの移行」（223 ページ）を参照）、パーティションを別のストレージ階層に移動することもできます（local-to-shared など）。

注： データベースのレプリケーションが設定されたデータベースのパーティションのサイズを変更する場合は、先にレプリカパーティションのサイズを変更してから、マスターパーティションのサイズを変更してください。

18.9.4 データベース間のパーティション移動

パーティションをデータベース間で移動できます。例えば、2011 レンジパーティションを DB1 データベースから DB2 データベースに移動するには、次を実行します。

```
$ cat transfer-partition.xml
<transfer xmlns="http://marklogic.com/manage">
  <destination-database>DB2</destination-database>
</transfer>

$ curl --anyauth --user user:password -X PUT \
-d @transfer-partition.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/DB1/range-partitions/2011
```

18.9.5 フォレストの結合

複数のフォレストを1つのフォレストへと結合する場合は、PUT:/manage/v2/forests リソースアドレスを使用できます。例えば、フォレスト 2011-0001 と 2011-0002 を1つのフォレスト 2011 へ結合するには、次を実行します。

```
$ cat combine-forests.xml
<forest-combine xmlns="http://marklogic.com/manage">
  <forests>
    <forest>2011-0001</forest>
    <forest>2011-0002</forest>
  </forests>
  <forest-name>2011</forest-name>
  <hosts>
    <host>MyHost</host>
  </hosts>
</forest-combine>

$ curl --anyauth --user user:password -X PUT \
-d @combine-forests.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/forests
```

ホストに異なる値を指定すれば、フォレストを結合する処理と結合後のフォレストを別のホストへ移行する処理を1回の操作で実行できます。いずれかの移行オプションを指定して（「フォレストおよびパーティションの移行」（223 ページ）を参照）、フォレストを別のストレージ階層に移動することもできます（local-to-shared など）。

注： データベースのレプリケーションが設定されたデータベースにアタッチされているフォレストを結合する場合は、`snapshot` オプションを指定して外部のレプリカフォレストを結合してから、マスターフォレストを結合してください。

注： フォレストでフェイルオーバーが設定されている場合は、フォレストの結合操作を実行した後でデータベースのフルバックアップを実行し、不具合があったときにデータをリカバリーできるようにしてください。また、フェイルオーバーが設定されている場合は結合操作に時間がかかるため、結合操作のタイムアウト設定の時間を延ばさなければならないことがあります。

18.9.6 フォレストのリタイア

フォレストをデータベースから「リタイア」することで、フォレスト内のすべてのドキュメントを残りのフォレストに移動して、これらのフォレスト間でリバランスを実行できます。（「フォレストがデータベースからリタイアするときのデータ移動方法」（188 ページ）を参照）。

例えば、フォレスト 2011 を Documents データベースからリタイアするには、次を実行します。

```
curl -i -X POST --digest --user user:password -H \
"Content-Type:application/x-www-form-urlencoded" \
--data "state=retire&database=Documents" \
http://MyHost:8002/manage/v2/forests/2011
```

18.9.7 フォレストおよびパーティションのオフライン/オンライン化

フォレストまたはパーティションをオフラインにしてアーカイブに格納し、必要に応じて後でオンラインに戻すことができます。データをオフラインにすると、RAM、CPU、およびネットワークリソースをオンラインデータ用に確保できるという利点があります。

オフラインのフォレスト/パーティションは、データベースが行うクエリ、更新、バックアップ、リストア、レプリケーションの対象外となります。オフラインのフォレストまたはパーティションは、アタッチ、デタッチ、または削除が可能です。名前変更、フォレストレベルのバックアップとリストア、移行、結合などの操作は、オフラインのフォレストまたはパーティションでサポートされません。フォレストでフェイルオーバーが設定されている場合、レプリカフォレストはマスターフォレストのオンライン/オフライン設定を継承するため、オフラインのマスターフォレストを無効にしても、フェイルオーバーはトリガーされません。

例えば、DB2 データベースの 2011 レンジパーティションをオフラインにするには、次を実行します。

```
$ cat partition-offline.xml
<partition-properties xmlns="http://marklogic.com/manage">
  <availability>offline</availability>
</partition-properties>

$ curl --anyauth --user user:password -X PUT \
-d @partition-offline.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/DB2/range-partitions/2011/properties
```

18.9.8 パーティションの更新許可状態の設定

パーティションの更新許可状態を変更してフォレストを作成できます。可能な状態を以下の表に示します。

状態	説明
all	読み取り、挿入、更新、および削除操作がパーティションで許可されます。
delete-only	読み取りおよび削除操作がパーティションで許可されますが、挿入および更新操作は許可されません。
read-only	読み取り操作がパーティションで許可されますが、挿入、更新、および削除操作は許可されません。このパーティション内のフラグメントに変更を加えようとするトランザクションは、例外をスローします。 注： 読み取り専用パーティションをサイズ変更してフォレスト数を減らしても、元のフォレストは維持されます。
flash-backup	パーティションを読み取り専用モードにしますが、挿入、更新、または削除トランザクションで例外をスローせず、トランザクションの再試行を許可します。

例えば、Documents データベースの 2011 レンジパーティションの更新許可状態を read-only に設定するには、次を実行します。

```
$ cat read-only-partition.xml
<partition-properties xmlns="http://marklogic.com/manage">
  <updates-allowed>read-only</updates-allowed>
</partition-properties>

$ curl --anyauth --user user:password -X PUT \
-d @read-only-partition.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/Documents/partitions/2011/properties
```

18.9.9 パーティションの削除

パーティションとそのすべてのフォレストを削除できます。例えば、Documents データベースの 2011 レンジパーティションを削除するには、次を実行します。

```
$ curl --anyauth --user user:password -X DELETE \
-H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/Documents/partitions/2011
```

18.10 フォレストレベルのフェイルオーバーが設定されたパーティション

パーティションの作成、移行、およびサイズ変更操作では、共有ディスクまたはローカルディスクのフェイルオーバー用のレプリカフォレストを作成するように `options` 要素を指定できます。詳細については『*Scalability, Availability, and Failover Guide*』の「[Configuring Local-Disk Failover for a Forest](#)」および「[Configuring Shared-Disk Failover for a Forest](#)」の章を参照してください。

フォレストレベルのフェイルオーバー用のレプリカフォレストを作成するには、2 つ以上のホストでパーティションを作成する必要があります。一方のホストで作成されたそれぞれのマスターフォレストに対して、もう一方のホストでレプリカフォレストが作成されます。例えば、2011 レンジパーティションの各フォレストについて 1 つのレプリカフォレストを作成し、フォレストに `MyHost1`、`MyHost2`、および `MyHost3` の間のローカルディスクフェイルオーバーを設定するには、次を実行します。

```
$ cat create-partition.xml
<partition xmlns="http://marklogic.com/manage">
  <partition-name>2011</partition-name>
  <upper-bound>2012-01-01</upper-bound>
  <lower-bound>2011-01-01</lower-bound>
  <forests-per-host>4</forests-per-host>
  <data-directory>/forests</data-directory>
  <hosts>
    <host>MyHost1</host>
    <host>MyHost2</host>
    <host>MyHost3</host>
  </hosts>
  <data-directory></data-directory>
  <large-data-directory></large-data-directory>
  <fast-data-directory></fast-data-directory>
  <options>
    <option>replicas=1</option>
    <option>failover=local</option>
  </options>
</partition>

$ curl --anyauth --user user:password -X POST \
-d @create-partition.xml -H 'Content-type: application/xml' \
http://MyHost:8002/manage/v2/databases/Documents/partitions
```

フォレストレベルのフェイルオーバー構成でパーティションまたはフォレストを設定するときは、次の点に注意してください。

- フォレストでフェイルオーバーが設定されている場合は、パーティションまたはフォレストの移行やフォレストの結合を実行した後でデータベースのフルバックアップを実行し、不具合があったときにデータをリカバリーできるようにしてください。また、フェイルオーバーが設定されている場合は移行または結合操作に時間がかかるため、これらの操作のタイムアウト設定の時間を延ばさなければなりません。
- ジャーナリングが off に設定されたデータベースにアタッチされているフォレストに対し、ローカルディスクフェイルオーバーを設定することはお勧めしません。
- 高速データディレクトリ (<fast-data-directory> で指定) が S3 上に存在しない場合を除き、Amazon Simple Storage Service (S3) 上で共有ディスクまたはローカルディスクフェイルオーバー構成のパーティションを設定できません。
- MarkLogic を Amazon Elastic Compute Cloud (EC2) 上に実装している場合、または複数のデータセンター間に分散している場合、フォレストレベルのフェイルオーバー構成のパーティションを作成、移行、またはサイズ変更するときに、異なるゾーンのホストの数を等しく指定する必要があります。例えば、us-east-1a に 2 つのホスト、us-east-1b に 2 つのホスト、us-east-1c に 2 つのホストがあるようにします。この例では、階層型ストレージによりマスターおよびレプリカフォレストが必ずゾーンが異なるホスト上に作成されるようになります。これにより、フォレスト、ホスト、またはゾーン全体がダウンした場合でも、パーティションはアクセス可能なままになります。

19.0 スーパーデータベースおよびクラスタ

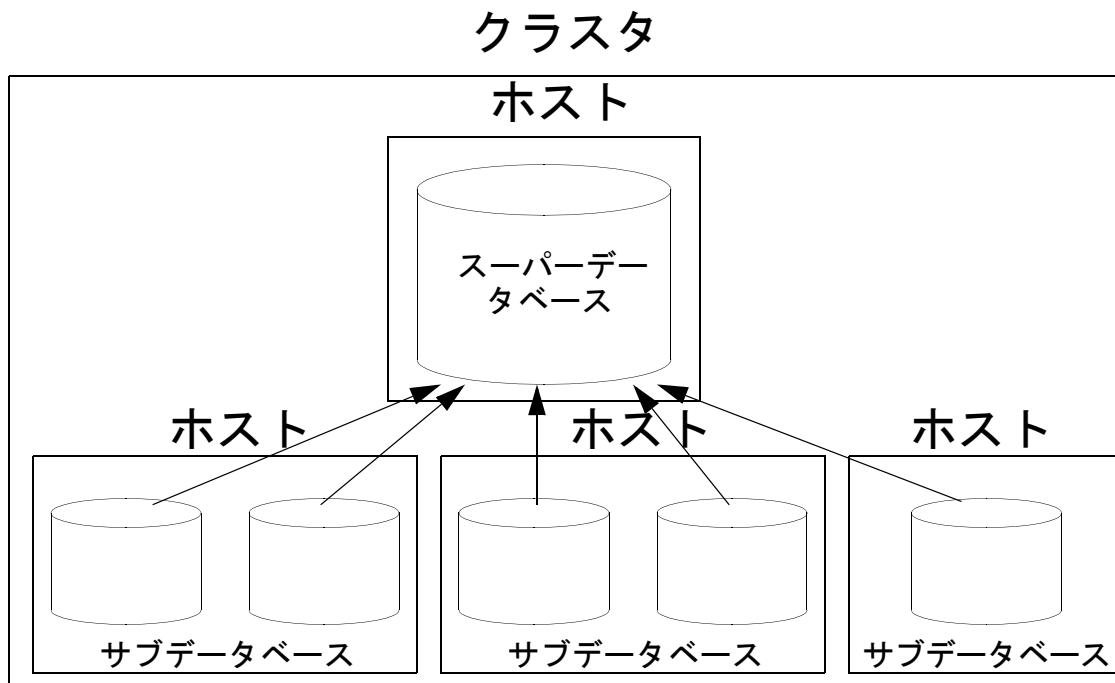
MarkLogic サーバーでは、複数のデータベースを「スーパーデータベース」にグループ化して、1つのクエリを複数のデータベースにわたって実行することができます。スーパーデータベースに含まれるデータベースは「サブデータベース」と呼ばれます。サブデータベースは、異なるストレージ階層や異なるクラスタ（「スーパークラスタ」）に分散できます。サブデータベースは、`kind` 要素で `active`（オンライン）または `archive`（オフライン）に指定できます。

この章は、次のセクションで構成されています。

- [概要](#)
- [スーパーデータベースの作成](#)
- [スーパーデータベースおよびサブデータベースの表示](#)

19.1 概要

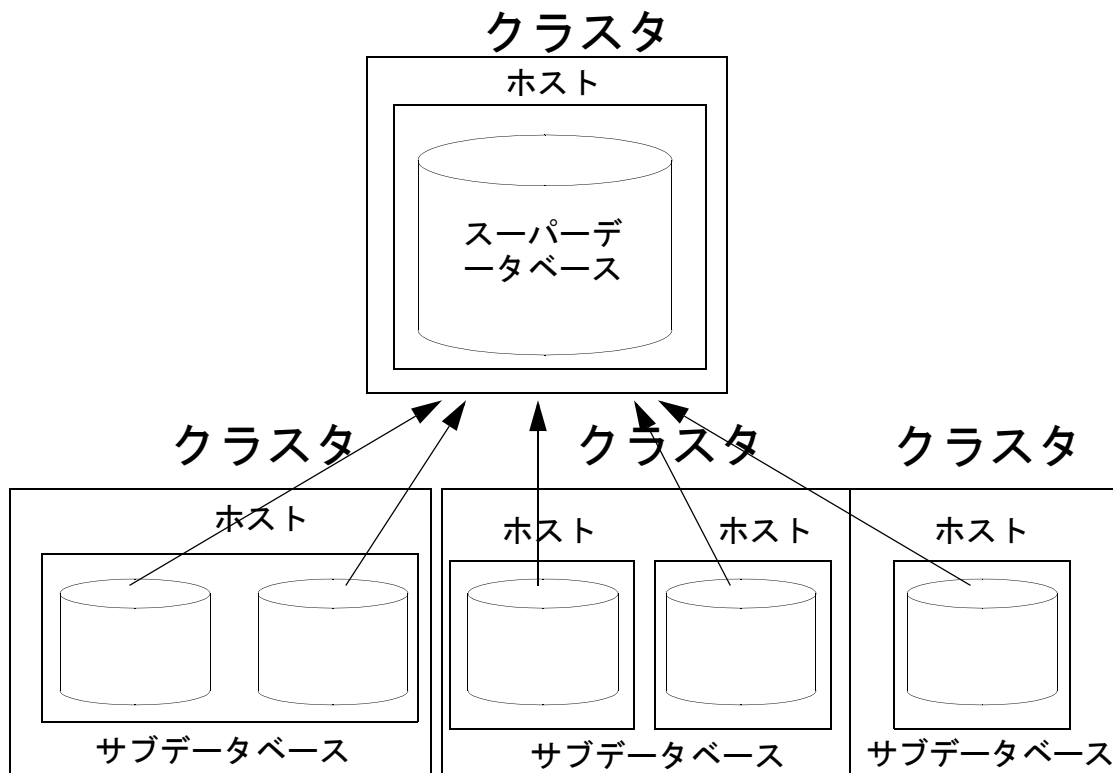
更新はサブデータベースで実行され、スーパーデータベースで認識されて読み取られません。単一クラスタに設定されたスーパーデータベースとサブデータベースの例を以下に示します。



別の外部クラスタ上にサブデータベースが設定されたスーパーデータベースを以下に示します。スーパーデータベースをホスティングするクラスタが、サブデータベースをホスティングする外部クラスタと結合する必要があります。クラスタを結合する方法の詳細については、『*Database Replication Guide*』の「[Coupling the Local and Foreign Clusters](#)」を参照してください。

注： 各外部クラスタには複数のブートストラップホストが必要です。こうしておけば、1つのブートストラップホストがダウンしても、スーパーデータベースは別のブートストラップホストを使用して、そのクラスタ上のサブデータベースをクエリできます。

スーパークラスタ



スーパーデータベースとサブデータベースの特長は次のとおりです。

- スーパーデータベースでサポートされるサブデータベースのレベルは1つのみです。つまり、あるサブデータベースをスーパーデータベースとして設定し、かつ自分自身をサブデータベースとすることはできません。
- サブデータベースに対する更新が、スーパーデータベースで認識されます。スーパーデータベースに書き込んで更新をサブデータベースに伝播することはできません。スーパーデータベース自体を更新するには、ローカルフォレストが必要です。ただし、スーパーデータベースにローカルフォレストを設定することは推奨されません。

- サブデータベースとそのスーパーデータベースはインデックス設定が同一である必要があります。それ以外の場合、クエリが動作しません。
- スーパーデータベースとそのサブデータベースは実質的に単一のデータベースであるため、URI が同一のドキュメントをスーパーデータベースとサブデータベースに同時に格納できません。ディレクトリを使用してドキュメント URI が一意になるようにすることをお勧めします。
- スーパーデータベースではフレキシブルレプリケーションを実行できません。
- サブデータベースが外部クラスタ間で分散している場合、各クラスタ上のデータベースにアクセスするには、セキュリティデータベースおよびスキーマデータベースも同様に分散している必要があります。これを確実に行うには、データベースのレプリケーションを使用してセキュリティデータベースおよびスキーマデータベースを各クラスタにレプリケートしてください。
- データを外部クラスタ上のサブデータベースに挿入すると、`request-timestamp` が挿入のコミットタイムスタンプより後になった時点で、挿入したドキュメントはスーパーデータベースで読み取られます。通常、これには数秒かかります。

19.2 スーパーデータベースの作成

`POST: /manage/v2/databases` リソースアドレスを呼び出して、スーパーデータベースを作成できます。サブデータベースにするデータベースを指定するだけで、スーパーデータベースを作成できます。

例えば、`mySuperDatabase` データベースをスーパーデータベースとして定義し、そこに同一クラスタ上の `subDB1`、`subDB2`、および `subDB3` サブデータベースを含めるには、次を実行します。

```
$ curl --anyauth --user user:password -X POST \
-d '{"database-name": "mySuperDatabase",
  "subdatabases": [
    "subdatabase":{"cluster-name":"localhost", "database-name":"subDB1"},
    "subdatabase":{"cluster-name":"localhost", "database-name":"subDB2"},
    "subdatabase":{"cluster-name":"localhost", "database-name":"subDB3"}
  ]}'
-H 'Content-type: application/json' \
http://MyHost:8002/manage/v2/databases
```

例えば、`mySuperCluster` データベースをスーパークラスタとして定義し、そこに別クラスタ上の `subDB1`、`subDB2`、および `subDB3` サブデータベースを含めるには、次を実行します。

```
$ curl --anyauth --user user:password -X POST \
-d '{"database-name": "mySuperCluster",
  "subdatabases": [
    "subdatabase":{"cluster-name":"foreign1", "database-name":"subDB1"},
    "subdatabase":{"cluster-name":"foreign2", "database-name":"subDB2"},
    "subdatabase":{"cluster-name":"foreign3", "database-name":"subDB3"}
  ]}'
-H 'Content-type: application/json' \
http://MyHost:8002/manage/v2/databases
```

注： スーパークラスタには、最大 32 個のクラスタを指定できます。

19.3 スーパーデータベースおよびサブデータベースの表示

GET:/manage/v2/databases/{id|name}/super-databases リソースアドレスを呼び出して、サブデータベースに関連付けられているスーパーデータベースのリストを返すことができます。例えば、subdb1 データベースのスーパーデータベースを表示するには、次を実行します。

```
$ curl --anyauth --user user:password -X GET \  
-H 'Content-type: application/xml' \  
http://MyHost:8002/manage/v2/databases/subdb1/super-databases
```

GET:/manage/v2/databases/{id|name}/sub-databases リソースアドレスを呼び出して、スーパーデータベースに関連付けられているサブデータベースのリストを返すことができます。例えば、superdb1 データベースのサブデータベースを表示するには、次を実行します。

```
$ curl --anyauth --user user:password -X GET \  
-H 'Content-type: application/xml' \  
http://MyHost:8002/manage/v2/databases/superdb1/sub-databases
```

注： 更新はスーパーデータベースとサブデータベースの両方のレベルで発生する可能性があるため、重複した URI がスーパーデータベースに生じやすくなります。自動的に生成される URI の一部は、スーパーデータベースレベルで重複が生じることがあります。この問題は、グラフドキュメントの自動生成 URI だけでなく、バイテンポラル LSQT ドキュメント、および自動ディレクトリ作成で作成されたディレクトリプロパティフラグメントにも当てはまります。重複した URI により、DUPURI 例外が生成されます。

20.0 データベースのバックアップおよびリストア

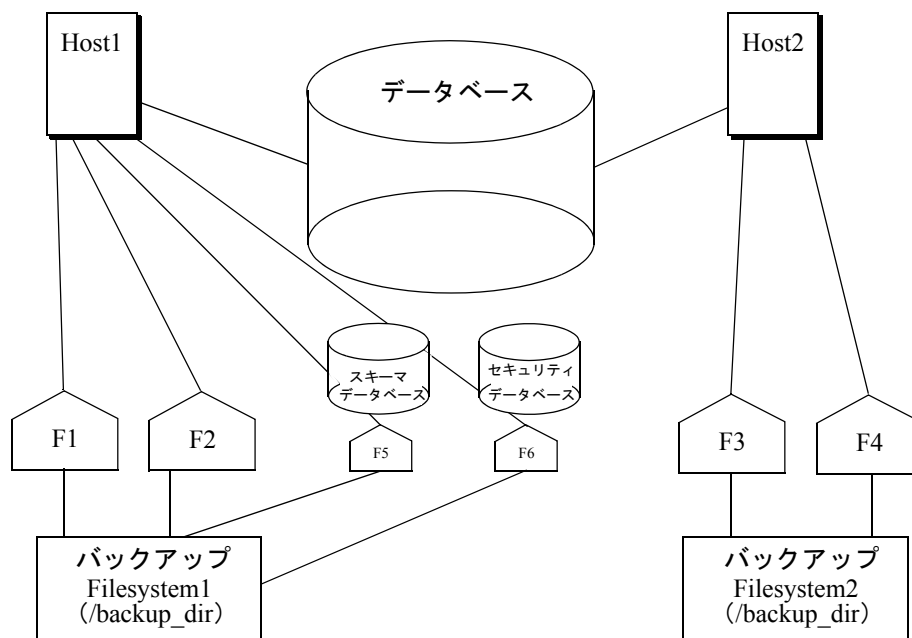
MarkLogic サーバーには、データベースの一貫性のあるバックアップを作成する機能が用意されています。このセクションでは、バックアップとリストアのアーキテクチャについて、およびデータベースのバックアップ手順およびリストア手順について説明します。次のトピックから構成されています。

- [バックアップおよびリストアの概要](#)
- [ジャーナルアーカイブがオンのデータベースバックアップ](#)
- [増分バックアップ](#)
- [データベースのバックアップ](#)
- [ジャーナルアーカイブがオフのデータベースリストア](#)
- [ジャーナルアーカイブがオンのデータベースリストア](#)
- [ジャーナルアーカイブがオンの増分バックアップからのリストア](#)
- [ローカルディスクフェイルオーバー後のデータベースのバックアップとリストア](#)

20.1 バックアップおよびリストアの概要

MarkLogic サーバーにおけるデータベースのバックアップとリストアはクラスタ内の全データノード（つまりフォレストを含む全てのノード）が対象となります。これにより一貫性のあるデータベースレベルのバックアップとリストアを実現します。

バックアップやリストア用に指定するディレクトリは、データベースに関連付けられた各データノード上に存在する必要があります（共有あるいは非共有ディレクトリ）。例えば、データノードとして Host1（フォレスト F1 と F2 が含まれる）と Host2（フォレスト F3 と F4 が含まれる）がある場合、指定するバックアップディレクトリは Host1 と Host2 の両方に存在する必要があります。以下の図は、このような構成を示しています。スキーマデータベースとセキュリティデータベースにはそれぞれ F5 と F6 があり、これらも Host1 にアタッチされています。



20.1.1 データベースレベルの一貫性のあるバックアップ

デフォルトでは、データベースをバックアップすると、以下の項目を含む、それに関連するものすべてがバックアップされます。

- 設定ファイル
- セキュリティデータベース（そのすべてのフォレストを含む）
- スキーマデータベース（そのすべてのフォレストを含む）
- バックアップ対象のデータベースのすべてのフォレスト

すべてのフォレストをバックアップする場合は、バックアップでファイルのコピーが開始した時点と全く同じ状態にリストアできるバックアップが作成されます。

また必要なフォレストだけをバックアップすることも可能です。この「フォレストレベルのバックアップ」では、このバックアップに含まれているフォレスト内のデータの一貫性は保たれますが、バックアップに含まれていないフォレスト内の変更とは一貫性がなくなる可能性があります。

セキュリティデータベースとスキーマデータベースをバックアップしないことも可能です。データベースのバックアップと同期されているこれらのデータベースをバックアップすることは、バックアップの開始時と正確に同一なシステムのビューを得るために重要です。適切な一貫性の保持を確保するこれらのデータベースのバックアップに、別のプロセスを使用することもできます。例えば、これらのデータベースがあまり頻繁に変更されない場合、変更時にのみバックアップするだけでも十分です。

MarkLogic サーバーにおけるデータベースレベルのバックアップとリストアでは、どのくらい多く / 少なくバックアップ / リストアするのかを決められる柔軟性があります。この選択は、システム内の変更の量や、バックアップとリストアに関する個別の要件に応じて変わります。

20.1.2 管理画面

バックアップおよびリストア操作を開始するには、管理画面を使用します。システムに設定された各データベースの [Backup/Restore] タブを使用して、バックアップおよびリストア操作を開始します。バックアップおよびリストア操作の具体的な手順については、「データベースのバックアップ」(245 ページ) および「ジャーナルアーカイブがオフのデータベースリストア」(252 ページ) を参照してください。

20.1.3 バックアップおよびリストアのトランザクション

バックアップおよびリストア操作はトランザクショナルであるため、一貫性のあるデータビューが保証されます。ただし、データベースをロックしません。そのため、バックアップまたはリストア操作を開始してから完了するまでの間にデータベース内のデータが変更された場合、その変更はバックアップおよびリストア操作に反映されません。同様に、バックアップまたはリストア操作中のセキュリティデータベースおよびスキーマデータベースに対する変更は、許可されますがバックアップまたはリストアに反映されません。

データベースおよびフォレストの管理タスク（ドロップ、クリア、削除など）はバックアップ中に実行できません。そのような操作はキューに格納され、バックアップトランザクションが完了した後で開始されます。

20.1.4 バックアップディレクトリの構造

データベースをバックアップするときは、バックアップディレクトリを指定します。バックアップディレクトリは構成内の各ホスト上に存在する必要があり、MarkLogic サーバーを実行するユーザー（デフォルトでは、UNIX で `daemon`、Windows でローカルの System ユーザー）によって読み取り / 書き込みが可能になっている必要があります。データベースバックアップの整合性は重要であるため、信頼性の高いファイルシステムへバックアップすることをお勧めします。各ホストのバックアップディレクトリの構造は同一ですが、フォレストはそのフォレストが提供されているホスト上にのみバックアップされる点が異なります。

指定バックアップディレクトリの下には、バックアップ開始日に基づいた名前でサブディレクトリが作成されます。サブディレクトリごとにバックアップが1つ含まれます。基本的なバックアップディレクトリ構造を次に示します。

```
<specified_backup_dir>/
  <date_1>-1/
    *.xml
    BackupTag.txt
    Forests/
      <security_forest_1>/
        <forest_files_and_directories>
      <security_forest_n>/
        <forest_files_and_directories>
      <schemas_forest_1>/
        <forest_files_and_directories>
      <schemas_forest_n>/
        <forest_files_and_directories>
      <database_forest_1>/
        <forest_files_and_directories>
      <database_forest_n>/
        <forest_files_and_directories>
      <triggers_forest_1>/
        <forest_files_and_directories>
      <triggers_forest_n>/
        <forest_files_and_directories>
  <date_1>-n/
    <backup_directory_structure>
  <date_n>-1/
    <backup_directory_structure>
  <date_n>-n/
    <backup_directory_structure>
```

例えば、データベースを 2004 年 9 月 1 日に /space/backups ディレクトリにバックアップする場合、次のようなディレクトリ構造が作成されます。

```
/space/backups
  20040901-1/
    *.xml
    BackupTag.txt
    Forests/
      Documents/
        Label
        000001e1/
        Journals/
      Schemas/
        Label
        000001e1/
        Journals/
      Security/
        Label
        000001e1/
        Journals/
      Triggers/
        Label
        000001e1/
        Journals/
```

増分バックアップは、フルバックアップの下のディレクトリに格納されます。この1つ目の例では、バックアップディレクトリ (backup-dir) は /space/backup で、増分バックアップディレクトリ (incremental-dir) は使用されていません。

```
/space/backups
  20140801-1223942093224  (full backup on 8/1)
    20140802
      331006226070  (incremental backup on 8/2)
    20130803
      1341007528950  (incremental backup on 8/3)
```

1 つ目の部分 20140801 はバックアップの年月日です。2 つ目の部分 1223942093224 はバックアップの時分秒およびナノ秒です。

次の例では、バックアップディレクトリ (backup-dir) は /space/backup で、増分バックアップディレクトリ (incremental-dir) は /space/incremental です。

```
/space/backups
  20140801-1223942093224  (full backup on 8/1)

/space/incremental
  20140801-1223942093224
    20140802
      331006226070  (incremental backup on 8/2)
    20140803
      341007528950  (incremental backup on 8/3)
```

ディレクトリ 20130801-1223942093224 は /space/incremental に作成されるため、バックアップ 20130801-1223942093224 がページされるときにその増分バックアップも簡単にページできます。

増分バックアップディレクトリが指定された場合、1 つ目の増分バックアップが終了すると、フルバックアップは別の場所にアーカイブできます。それ以降の増分バックアップでは、フルバックアップの検証は必要ありません。

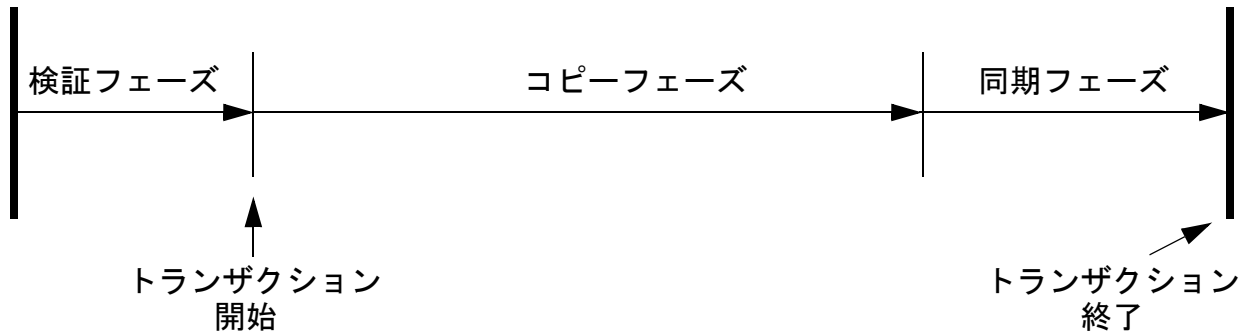
注： 増分バックアップからリストアすると、以前のフルバックアップの場所を現行の増分バックアップに使用できません。リストア後は新規にフルバックアップを作成し、そのフルバックアップディレクトリを現行の増分バックアップに使用する必要があります。つまり、増分バックアップのリストア後は、新規のフルバックアップの場所を使用するように定期バックアップを更新する必要があります。

20.1.5 バックアップおよびリストア操作のフェーズ

バックアップおよびリストア操作は、次のフェーズに分かれています。

- 検証
- コピー
- 同期

バックアップまたはリストア操作のフェーズを次の図に示します。



20.1.5.1 検証フェーズ

検証フェーズでは、バックアップディレクトリがチェックされて、必要なすべてのファイルが存在すること、および必要なすべてのバックアップディレクトリが存在して書き込み可能であることを確認します。バックアップ操作の場合は、十分なディスク領域があることが確認されます。リストア操作の場合は、設定ファイルが読み取られ、その他のバックアップファイルの有効性がチェックされます。検証フェーズでは、データを実際に書き込むことはなく、完全に非同期で実行されます。

20.1.5.2 コピーフェーズ

コピーフェーズでは、実際にファイルがバックアップディレクトリにコピーされたり、バックアップディレクトリからコピーされたりします。設定ファイルはバックアップ操作の開始時にコピーされ、この時点のタイムスタンプが `BackupTag.txt` ファイルに書き込まれます。データベースのサイズによっては、コピーフェーズに膨大な時間を要することがあります。コピーフェーズの開始によってトランザクションが開始します。リストア操作中にトランザクションが失敗すると、データベースは元の状態から変更されません。

20.1.5.3 同期フェーズ

バックアップまたはリストア操作の同期フェーズでは、一時ファイルの削除などのクリーンアップタスクが実行され、データベースは一貫性のある状態が維持されます。また、リストア操作の同期フェーズでは、データベースの古いバージョンがオフラインになり、新しくリストアされたバージョンで置き換えられます。

注： 「コールド」管理タスク（サーバー再起動が必要なタスク）は、バックアップまたはリストア操作が失敗する原因となります。バックアップまたはリストア操作時には、「コールド」管理タスクを実行しないでください。「ホット」および「コールド」操作のリストについては、「付録 A：管理タスクの「ホット」と「コールド」」（433 ページ）を参照してください。

20.1.6 バックアップおよびリストア操作に関する注意事項

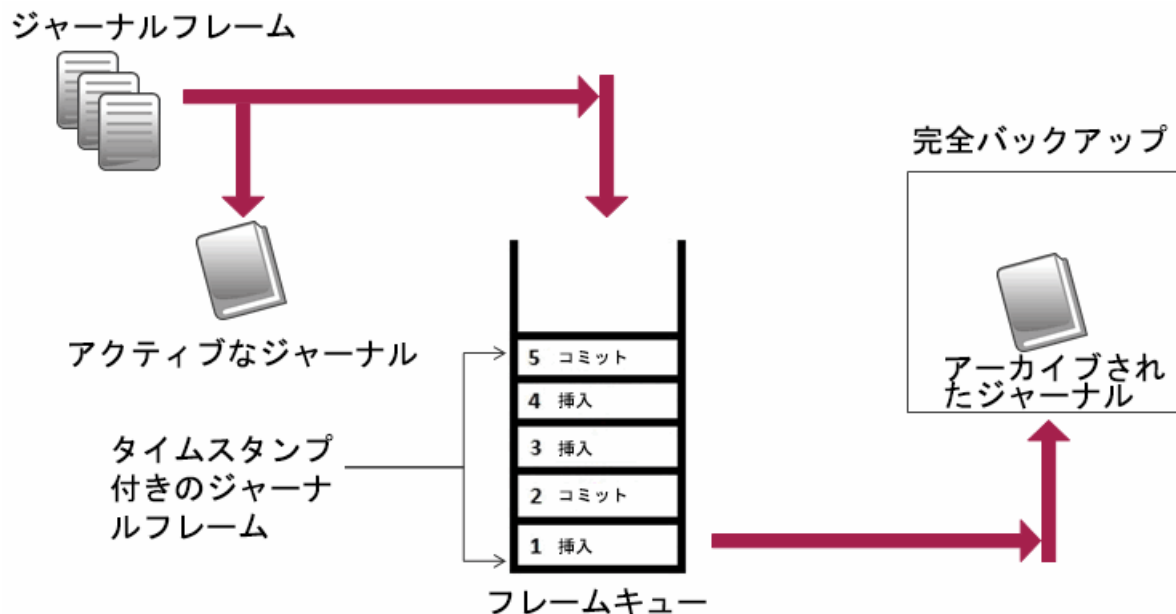
このセクションでは、MarkLogic サーバーデータベースのバックアップおよびリストアに関する注意および制限について説明します。

- バックアップファイルはプラットフォーム固有です。所定のプラットフォームでのバックアップは同一プラットフォームへのみリストアしてください。これは、データベースバックアップとフォレストバックアップの両方に当てはまります。
- データベースバックアップを使用して個別のフォレストをリストアするには、[Confirm Restore] 画面でリストアするフォレストを除くすべてのフォレストのチェックボックスをオフにします（「ジャーナルアーカイブがオフのデータベースリストア」（252 ページ）の手順 [10](#) を参照）。
- フォレストレベルのバックアップ / リストアではなく、データベースレベルのバックアップ / リストアを使用することをお勧めします。フォレストレベルのバックアップ / リストアを使用する場合は、フォレストレベルのバックアップで作成したバックアップをデータベースレベルのリストア操作でリストアできないことに注意してください。フォレストバックアップ / リストアユーティリティで作成したフォレストレベルのバックアップは、フォレストリストアユーティリティからリストアする必要があります。詳細については、「フォレストのリストア」（302 ページ）を参照してください。
- リストア操作は、バックアップ時と設定が同一であるデータベースにリストアするように設計されています。設定が同一であることは必須ではなく、チェックもありません。リストア操作は、設定が定義されたデータベースで実行してください。また、リストア操作ではデータベース設定ファイルを変更しません。設定ファイルはすべてのデータベース設定情報（インデックスオプション、フラグメンテーション、レンジインデックスなど）を保持するため、リストア後のデータベースはリストア先データベースの設定情報を引き継ぎます。この設定情報がバックアップ元データベースと異なる場合、かつ再インデックス付けがオンの場合、データベースはリストア完了後に新しい設定に対して再インデックス付けを行います。
- データベースのバックアップがキャンセルされると、実行中のバックアップは削除されます。データベースバックアップがキャンセルされるのは、管理画面のホストステータスページでバックアップのキャンセルボタンをクリックしたとき、ホストまたはクラスタが（管理画面または `xdmp:restart` コマンドから）再起動するとき、またはバックアップのエラー（ディスク領域不足エラーなど）が発生したときです。クリーン再起動時に実行中のバックアップの削除に時間がかかり、MarkLogic サーバーの再起動にかかる時間が長くなる場合があります。起動スクリプト（UNIX システムでは `/sbin/service MarkLogic`、Windows システムではコントロールパネル）を使用して再起動する場合、スクリプトでは 20 秒間に削除できるだけのバックアップを削除します。このような種類のシステムシャットダウンまたは再起動操作時に何らかのバックアップが実行中である場合は、操作後にそのバックアップを手動で削除してください。
- 増分バックアップからリストアすると、以前のフルバックアップの場所を現行の増分バックアップに使用できません。リストア後に新規にフルバックアップを作成し、そのフルバックアップディレクトリを現行の増分バックアップに使用する必要があります。つまり、増分バックアップのリストア後は、新規のフルバックアップの場所を使用するようにすべての定期バックアップを更新する必要があります。

20.2 ジャーナルアーカイブがオンのデータベースバックアップ

ジャーナルアーカイブがオンになっているバックアップ/リストア操作では、ポイントインタイムリカバリオプションが提供されます。ポイントインタイムリカバリオプションでは、ローカル時間を入力として、データベースの変更をフルバックアップ間の特定ポイントにリストアできます。ジャーナルアーカイブがオンの場合、各フォレストの現在のアクティブジャーナルからフレームを同期に近い状態でストリーミングすることにより、ジャーナルフレームがバックアップディレクトリに書き込まれます。

ジャーナルアーカイブがオンの場合、ジャーナルフレームのストリーミングにより、リストア時間が長くなり、システム負荷が若干増加します。



注： ジャーナルアーカイブは、フルバックアップ時のみオンにできます。バックアップをリストアして、ジャーナルアーカイブを再度オンにする場合は、その時点でフルバックアップを実行する必要があります。

ジャーナルアーカイブがオンの場合、フレームがフォレストのジャーナルに書き込まれてからバックアップジャーナルにストリーミングされるまでのタイムラグ（遅れ）の許容値（秒数）を設定できます。例えばタイムラグの上限が 30 秒に設定されると、アーカイブされるジャーナルはアクティブジャーナルと比べてトランザクションが最大で 30 秒遅れる可能性があります。タイムラグの上限を超過すると、バックアップジャーナルの処理が追いつくまでトランザクションは停止します。

アクティブジャーナルとバックアップジャーナルは少なくとも 30 秒間隔で同期されます。タイムラグの上限が 30 秒より小さい場合、同期はその期間内に少なくとも 1 回実行されます。タイムラグの上限が 30 秒より大きい場合、同期は 30 秒ごとに少なくとも 1 回実行されます。デフォルトのタイムラグの上限は 15 秒です。

タイムラグの上限時間の設定は、Recovery Point Objective (RPO) によって決まります。RPO は、災害発生時に喪失が許容されるデータ量です。RPO が小さいと、ほとんどのデータをリストアできますがパフォーマンスが犠牲になります。一方、RPO が大きいと、リストアできるデータ量が少なくなる可能性があります。パフォーマンスへの影響を小さくできます。一般に、タイムラグの上限は次の要因を考慮して選択します。

タイムラグの上限を小さくする場合：

- アクティブジャーナルとバックアップジャーナルの同期が正確になりますが、システムパフォーマンスが犠牲になる可能性があります。
- アーカイブの場所の I/O 帯域幅が広く、RPO 目標が低いときに使用します。

タイムラグの上限を大きくする場合：

- アクティブジャーナルとバックアップジャーナルの同期が遅延しますが、システムパフォーマンスへの影響は小さくなります。
- 保留状態のフレームがメモリに保持されるため、サーバーのメモリ使用率が高くなります。
- アーカイブの場所の I/O 帯域幅が狭く、RPO 目標が高いときに使用します。

20.3 増分バックアップ

増分バックアップでは、前回の増分およびフルバックアップ以降に変更されたデータだけを格納します。通常はフルバックアップと次のフルバックアップの間に、複数回行います。増分バックアップは、アーカイブ化されたジャーナルよりもコンパクトで、またより短時間でリストアできます。これを頻繁に行うようにスケジュール設定することもできます（数時間あるいは数分単位など）。これは増分バックアップでは、フルバックアップほど時間がかからないためです。

増分バックアップを行うには、バックアップを開始またはスケジュールするときに [Incremental backup] を [true] に設定します。詳細については、「データベースのバックアップ」（245 ページ）を参照してください。フルバックアップと増分バックアップは別々にスケジュールを設定する必要があります。例えば次のような構成が考えられます。

- フルバックアップは月 1 回
- 増分バックアップは毎日

フルバックアップと複数回の増分バックアップにより、データベース喪失の際でも回復できます。増分バックアップは、ジャーナルアーカイブと一緒に利用することもできます。増分バックアップとジャーナルアーカイブの両方を使用する場合、最後の増分バックアップのタイムスタンプに基づいてジャーナルをリプレイできます。ジャーナルアーカイブの詳細については、「ジャーナルアーカイブがオンのデータベースバックアップ」（242 ページ）を参照してください。

注： 増分バックアップからリストアした場合、再び増分バックアップを行う前に、一度フルバックアップを行う必要があります。

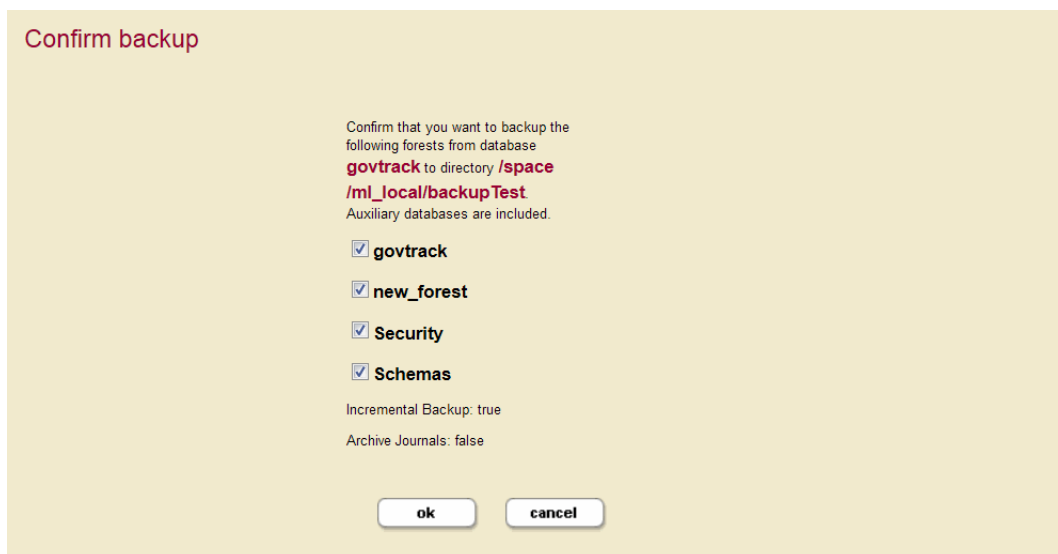
増分バックアップとジャーナルアーカイブの両方を利用することで、災害対策（DR）が実現されます。増分バックアップが使用するディスク容量は、ジャーナルアーカイブよりも小さいです。また増分バックアップのほうがジャーナルアーカイブよりも時間がかかりません。

リカバリ（復旧）に関しては、リカバリ開始のタイムスタンプを指定するだけです。これによりサーバーが、どのフルバックアップや増分バックアップを使用するのかを判断します。増分バックアップのスケジュールを設定するだけで、サーバーが一連の増分バックアップを自動的に関連付ける（まとめる）ことができます。詳細については、「ジャーナルアーカイブがオンの増分バックアップからのリストア」（259 ページ）を参照してください。

20.3.1 新規フォレストの増分バックアップ

増分バックアップでは、最後のフルバックアップ以降追加されたフォレストのバックアップができます。データベースのフルバックアップの後に新しいフォレストを追加した場合、この新規フォレストを、次回の増分バックアップに含めることができます。

データベースに新しく追加されたフォレストは、[Confirm backup] 画面のバックアップ対象フォレストのリストに含まれます（「データベースの即時バックアップ」（245 ページ）の手順 [11](#)）。



バックアップに含めるフォレストを選択して、[ok] をクリックします。詳細については、「データベースのバックアップ」（245 ページ）を参照してください。

20.4 増分バックアップとジャーナルアーカイブの同時使用

増分バックアップは、ジャーナルアーカイブにおけるリストアの時間と容量の両方の要件を改善しますが、これらは二者択一ではありません。両方を適宜使用でき、また適宜使用する必要があります。任意のポイントへリストアしながらデータ損失を最低限に抑えることが目標の場合は、次のようにすることをお勧めします。

1. 定期フルバックアップの頻度を少なくして（例えば毎週）、ジャーナルアーカイブをオンにします。
2. 定期増分バックアップの頻度を多くして（例えば毎時）、`purge-journal-archiving=true` を指定します。
3. データベースのマージポリシーで `[retain until backup]` を設定して、削除済みフラグメントが増分バックアップに含まれるまで保持されるようにします。詳細については、「マージポリシーの設定」（164 ページ）または `admin:database-set-retain-until-backup` を参照してください。

この設定により、ジャーナルアーカイブは最近の 1 時間分のみ必要になり、古いものはその時間をカバーする増分バックアップが発生するとパージされます。`[retain until backup]` をオンにすると、増分バックアップは前回の増分バックアップ以降の任意のポイントへデータベースをリストアするのに十分な状態になります。

リストアでは、フルおよび増分バックアップは、最新のバックアップより前の任意の時点へ戻すために使用できません。ジャーナルアーカイブは、リストアポイントが最後の増分バックアップよりも新しい場合のみ使用されます。

20.5 データベースのバックアップ

以下の手順を使用して、データベースバックアップをすぐに開始することも、将来実行されるようにバックアップのスケジュールを設定することもできます。

- [データベースの即時バックアップ](#)
- [データベースバックアップのスケジュール](#)

バックアップ手順には、ジャーナルアーカイブや増分バックアップを指定するオプションもあります。フルバックアップと増分バックアップのどちらを実行するのか、ジャーナルアーカイブをオンにするのかしないのかを選択できます。

20.5.1 データベースの即時バックアップ

データベースバックアップを開始するには、次の手順を実行します。

1. `admin` ロールを持つユーザーとして管理画面にログインします。
2. 管理画面の左側メニューで、`[Databases]` リンクをクリックします。
3. ツリーメニューまたは `[Summary]` タブで、バックアップするデータベースのデータベース名をクリックします。

4. [Backup/Restore] タブをクリックします。[Backup/Restore] 画面が表示されます。
5. [Backup to directory] フィールドに、データベースのバックアップ先ディレクトリを入力します。

注： バックアップディレクトリパスは、データベース内の任意のフォレストを提供するすべてのホストに存在する必要があります。指定したディレクトリは、オペレーティングシステムにマウントされたディレクトリパスでも、HDFS パスでも、S3 パスでもかまいません。MarkLogic で HDFS および S3 ストレージを使用する場合の詳細については、『*Query Performance and Tuning Guide*』の [Disk Storage Considerations](#) を参照してください。また、Windows を使用してリモートの Windows パスにバックアップする場合は、『*Windows Shared Disk Registry Settings and Permissions*』の説明に従ってレジストリおよびパーミッションを設定する必要があります。

6. フォレストにローカルディスクフェイルオーバーを設定した場合、必要に応じて [Include Replica Forests] を [true] に設定して、バックアップにレプリカフォレストを含めることができます。フォレストにローカルディスクフェイルオーバーを設定する方法の詳細については、『*Scalability, Availability, and Failover Guide*』の [Configuring Local-Disk Failover for a Forest](#) を参照してください。
7. [Incremental backup] を [true] に設定すると、増分バックアップが作成されます。デフォルトはフルバックアップ (false) です。
8. ポイントインタイムリカバリをオンにする場合は、[Archive Journals] を [true] に設定して、[Journal Archiving Lag Limit] を設定します。[Journal Archiving Lag Limit] については、『*ジャーナルアーカイブがオンのデータベースバックアップ*』(242 ページ) を参照してください。

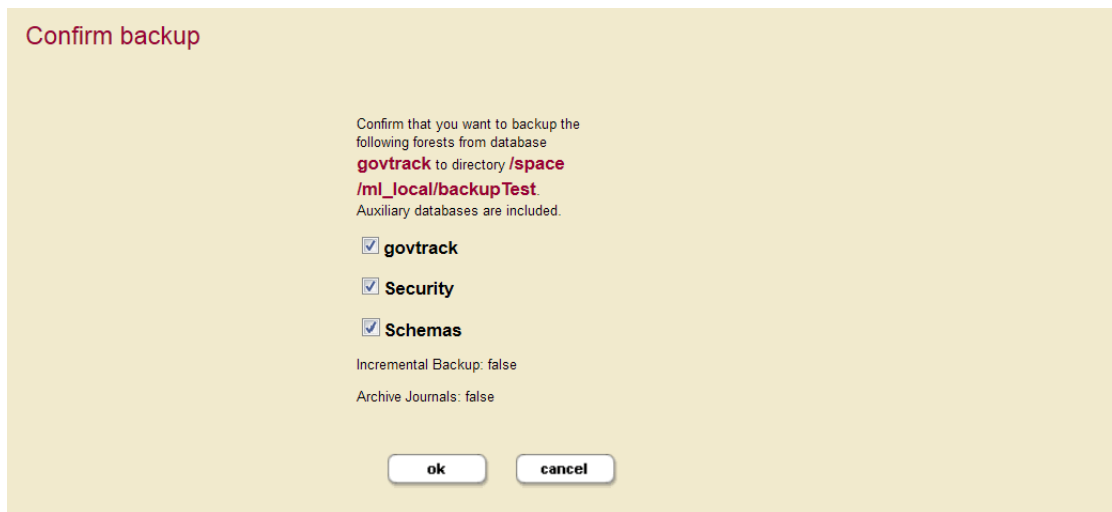
注： ジャーナルアーカイブがオンの場合は補助フォレストを含めることができません。補助フォレストには専用のバックアップが別途必要です。

The screenshot shows a dialog box titled "Backup the govtrack database." with the following settings:

- Backup to directory: /space/ml_local/backupTest (The backup directory pathname. Required.)
- Include replica forests: true false
- Incremental backup: true false
- Archive journals: true false

Buttons for "ok" and "cancel" are at the bottom.

9. [ok] をクリックします。
10. ディレクトリ作成エラーが表示された場合、ディレクトリは書き込み可能になっていません。既存のディレクトリのパーミッションを変更するか、または適切なパーミッション（MarkLogic サーバーを実行するユーザー（UNIX では `daemon`、Windows ではローカル System ユーザー）によって読み書き可能）で新しいディレクトリを作成し、もう一度 [ok] をクリックします。
11. [Confirm backup] 画面が表示され、バックアップ用に選択したすべてのフォレストがリストされます。



12. [ok] をクリックしてバックアップをすぐに開始するか、バックアップに含めないフォレストの選択を解除します。

注： バックアップするフォレストのいずれかを選択解除すると、リストアするデータベースの完全な一貫性のあるビューを得られないことがあります。バックアップ内容の意味を十分理解している場合に限り、フォレストを選択解除してください。データベースのまったく同一のビューを保証するため、データベースに関連しているすべてのフォレストをバックアップしてください（スキーマデータベースおよびセキュリティデータベースのフォレストを含む）。

13. バックアップの処理が開始されたら、管理画面は [Database Status] ページにリダイレクトされます。

Database: govtrack show rebalance show reindex show forests

database status -- A detailed view of this database's status.

Database	govtrack
Mount State	available (backing up) since July 14, 2014 3:34:25 PM
Size	300 MB
Large Data Size	0 MB
Forests	1
Merge State	0 merges in progress
Rebalancing State	Not rebalancing
Reindexing/Refragmenting State	Not reindexing/refragmenting
Backup/Recovery State	Backup in progress (see below for details)
Last Backup	2014-07-14T14:51:54.433-07:00
Last Restore	2014-07-14T14:41:16.031-07:00
Content Processing State	Not installed
Non-Blocking Timestamp	2014-07-14T15:43:01.042
Configured for Database Replication	No

Forest	Host	State	Documents	Fragments	Deleted Fragments	Stands	Size	Free Space	Large Free Space	Fast Free Space
govtrack	hp8470-2361.marklogic.com	open (backing up)	17,378	17,378	0	2	300 MB	397,498 MB	n/a	n/a
Total			17,378	17,378	0	2	300 MB			

Offline Forest	Host	State	Fragments	Size	Minimum Data Value	Maximum Data Value
None						
Total						

Forest	List Cache Hits	Misses	Ratio	Hit Rate	Miss Rate	Ratio
govtrack	282	620	31%	0	0	n/a
Total	282	620	31%	0	0	n/a

Forest	Compressed Tree Cache Hits	Misses	Ratio	Hit Rate	Miss Rate	Ratio
govtrack	0	0	n/a	0	0	n/a

14. [Database Status] 画面をリフレッシュすると、バックアップの進行状況を表示できます。[Backups] テーブルには、バックアップが開始した日時、推定残り時間、およびバックアップ操作に関するその他のステータス情報がリスト表示されます。

Backups											
Forest	Path	Start Time	Estimated Completion In	Current Size	Final Size						
govtrack	/space/ml_local/backupTest /20140714-1542588550000/Forests/govtrack	3:42 PM July 14, 2014	00:00:21	33 MB	300 MB						

Rates (Megabytes per Second)											
Forest	Query Reads	Journal Writes	Save Writes	Merge Reads	Merge Writes	Backup Reads	Backup Writes	Restore Reads	Restore Writes	Large Reads	Large Writes
govtrack	0	0	0	0	0	1.995201	1.974032	0	0	0	0

Loads (Seconds per Second)											
Forest	Query Reads	Journal Writes	Save Writes	Merge Reads	Merge Writes	Backup Reads	Backup Writes	Restore Reads	Restore Writes	Large Reads	Large Writes
govtrack	0	0	0	0	0	0.04247266	0.03109375	0	0	0	0

バックアップが完了すると、バックアップテーブル内のエントリは表示されなくなります。

いずれかのフォレストのステータスに「completed」以外の情報が表示されている場合、バックアップ操作時にエラーが発生しています。`Mark_Logic_Data/Logs/ErrorLog.txt` ファイルでエラーを確認して修正し、バックアップ操作をやり直してください。

20.5.2 データベースバックアップのスケジュール

データベースを定期的にバックアップするように、データベースバックアップをスケジュールできます。バックアップを毎日、毎週、毎月実行するようにスケジュールすることも、1回限りのバックアップをスケジュールすることもできます。必要な数の定期バックアップを作成できます。定期バックアップを作成するには、管理画面で次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] ページで、バックアップをスケジュールするデータベースを選択します。[Database Configuration] ページが表示されます。
3. データベースのツリーメニューで、[Scheduled Backup] リンクをクリックします。[Scheduled Backup Configuration] ページが表示されます。
4. [Scheduled Backup Configuration] ページで、既存の定期バックアップが不要になった場合は削除できます。

5. [Create] タブをクリックします。[Schedule a Database Backup] ページが表示されます。

6. バックアップディレクトリの絶対パスを入力します。バックアップディレクトリのパーミッションは、MarkLogic サーバープロセスがそのディレクトリを読み取り / 書き込みできるようになっている必要があります。

注： バックアップディレクトリパスは、データベース内の任意のフォレストを提供するすべてのホストに存在する必要があります。指定したディレクトリは、オペレーティングシステムにマウントされたディレクトリパスでも、HDFS パスでも、S3 パスでもかまいません。MarkLogic で HDFS および S3 ストレージを使用する場合の詳細については、『*Query Performance and Tuning Guide*』の [Disk Storage Considerations](#) を参照してください。

7. バックアップの種類として、定期的か 1 回限りかを選択します。
 - [minutely] の場合は、バックアップ間隔の分数を入力します。
 - [hourly] の場合は、バックアップ間隔の時間数を入力します。[Backup Minute] 設定は、正時から何分後にバックアップが開始するのかを指定します。[Backup Minute] 設定によって、間隔の時間が伸びることはありません。
 - [daily] の場合は、バックアップの間隔の日数と時刻を入力します。
 - [weekly] の場合は、バックアップ間の週数を入力し、1 つあるいは複数の曜日のチェックボックスをオンにして、バックアップが開始する時刻を入力します。
 - [monthly] の場合は、バックアップ間の月数を入力し、日 (1 ~ 31) を選択し、バックアップが開始する時刻を入力します。
 - [one-time] の場合は、バックアップの開始日を MM/DD/YYYY 表記 (例えば、2009 年 7 月 29 であれば 07/28/2009) で入力し、時刻を 24 時間表記で入力します。
8. バックアップを開始する時刻を入力します。
9. 保持するバックアップの最大数を入力します。指定された最大バックアップ数に達すると、次のバックアップ時に最も古いバックアップが削除されます。保持するバックアップ数を無制限にする場合は 0 を指定します。
10. この定期バックアップで、バックアップにセキュリティデータベース、スキーマデータベース、トリガーデータベースを含めるかどうかを選択します。
11. バックアップにレプリカフォレストやマスターフォレストを含めるかどうかを選択します。
12. 増分バックアップとフルバックアップのどちらをスケジュールするのか選択します。
13. バックアップでポイントインタイムリカバリ用にジャーナルアーカイブをオンにするかどうかを選択します。ジャーナルアーカイブの詳細については、「ジャーナルアーカイブがオンのデータベースバックアップ」(242 ページ) を参照してください。

注: ジャーナルアーカイブがオンの場合は補助フォレストを含めることができません。補助フォレストには専用のバックアップが別途必要です。
14. ジャーナルアーカイブをオンにした場合は、タイムラグの上限を変更して、バックアップしているジャーナルと現在アクティブなジャーナルの許容される時間差(秒数)を制御できます。
15. [ok] をクリックして定期バックアップを作成します。

バックアップは、指定されたスケジュールに従って自動的に開始します。

20.6 ジャーナルアーカイブがオフのデータベースリストア

このセクションでは、最後のバックアップでジャーナルアーカイブがオンではなかった場合にデータベースをリストアする方法について説明します。

注： 最後のバックアップでジャーナルアーカイブがオンであった場合は、先に進まず、「ジャーナルアーカイブがオンのデータベースリストア」(255 ページ) で説明する手順に従ってください。

バックアップからデータベース全体をリストアするには、次の手順を実行します。

1. `admin` ロールを持つユーザーとして管理画面にログインします。
2. 管理画面の左側メニューで、[Databases] リンクをクリックします。
3. ツリーメニューまたは [Summary] タブで、リストアするデータベースのデータベース名をクリックします。このデータベースは、バックアップしたデータベースと同じ設定（インデックスオプション、フラグメンテーション、レンジインデックス）になっている必要があります。
4. [Backup/Restore] タブをクリックします。[Backup/Restore] 画面が表示されます。
5. [Restore from directory] フィールドで、バックアップが存在するディレクトリを入力します。

注： 入力したディレクトリに同じデータベースの複数のバックアップが含まれる場合は、最新のバックアップが使用されます。リストア対象として特定のバックアップを選択する場合は、リストアするバックアップに対応する「`date_stamp`」サブディレクトリを入力します。ディレクトリ構造の詳細については、「バックアップディレクトリの構造」(237 ページ) を参照してください。

6. フォレストにローカルディスクフェイルオーバーを設定した場合、必要に応じて [Include Replica Forests] を [true] に設定して、バックアップからレプリカフォレストをリストアできます。このオプションを使用するには、バックアップ時にレプリカフォレストを含めるオプションをオンにしておく必要があります。フォレストにローカルディスクフェイルオーバーを設定する方法の詳細については、『*Scalability, Availability, and Failover Guide*』の [Configuring Local-Disk Failover for a Forest](#) を参照してください。
7. 増分バックアップを復元する場合は、[Use incremental backup] を [true] に設定します。

注： 増分バックアップからリストアすると、以前のフルバックアップの場所を現行の増分バックアップに使用できません。リストア後に新規にフルバックアップを作成し、そのフルバックアップディレクトリを現行の増分バックアップに使用する必要があります。増分バックアップのリストア後は、新規のフルバックアップの場所を使用するようにすべての定期バックアップを更新する必要があります。

8. [Journal Archiving] は [false] にします。

Restore the *govtrack* database.

Restore from directory: /space/ml_local/backupTest
The backup directory pathname.
Required.

Include replica forests: true false

Use incremental backup: true false

Use journal archive: true false

Restore to time:
Leave blank for latest restore time or use xs:DateTime-Format like 2014-07-14T15:50:14-07:00

ok cancel

9. [ok] をクリックします。
10. [Confirm restore] 画面が表示され、リストア対象に選択したすべてのフォレストがリストされます。

Confirm restore

Confirm that you want to restore the following forests to database **govtrack** from directory **/space/ml_local /backupTest**

govtrack

Schemas

Security

Use Incremental Backup: false

Use Journal Archive: false

RestoreToTime:

Backup was completed: 2014-07-14T15:43:10

Server version used: 8.0-20140714

ok cancel

[Confirm restore] 画面には、バックアップが実行された日付、および選択したバックアップで使用されたサーバーバージョンも表示されます。

11. デフォルトでは、データベースに関連するすべてのフォレストがリストア対象として選択されています。リストアしないフォレストがある場合は、リストアしないフォレストを選択解除します。

注： リストアするフォレスト（1つまたは複数）を選択解除すると、データベースの完全な一貫性のあるビューがリストアされない場合があります。リストア内容の意味を十分理解している場合に限り、フォレストを選択解除してください。データベースのまったく同一のビューを保証するため、データベースに関連しているすべてのフォレストをリストアしてください（スキーマデータベースおよびセキュリティデータベースのフォレストを含む）。

12. [ok] をクリックして、リストア操作を開始します。

[Restores] テーブルには、リストアが開始した日時、推定残り時間、およびリストア操作に関するその他のステータス情報がリストされます。

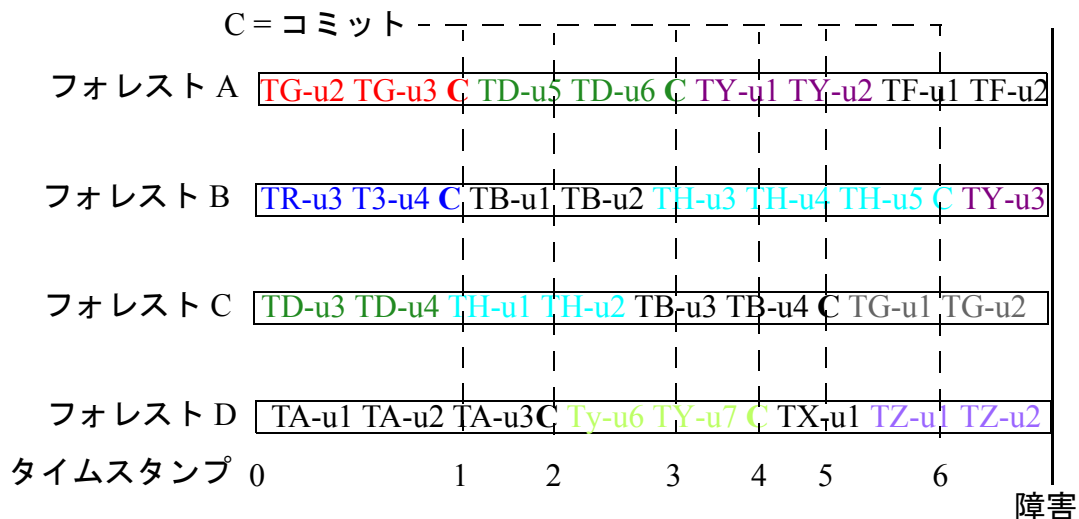
Restores												
Forest	Path	State	Start Time	Estimated Completion	Current Size	Final Size						
govtrack	/space/ml_local/backupTest /20140714-1438327200000/Forests/govtrack	copying	2:41 PM July 14, 2014	00:00:03	143 MB	300 MB						
Rates (Megabytes per Second)												
Forest	Query Reads	Journal Writes	Save Writes	Merge Reads	Merge Writes	Backup Reads	Backup Writes	Restore Reads	Restore Writes	Large Reads	Large Writes	
govtrack	0	0	0	0	0	0	0	7.23478	7.240455	0	0	
Loads (Seconds per Second)												
Forest	Query Reads	Journal Writes	Save Writes	Merge Reads	Merge Writes	Backup Reads	Backup Writes	Restore Reads	Restore Writes	Large Reads	Large Writes	
govtrack	0	0	0	0	0	0	0	0	0.1784313	0	0	

リストアが完了すると、バックアップテーブル内のエントリは表示されなくなります。いずれかのフォレストのステータスで「completed」以外の情報が表示されている場合、リストア操作時にエラーが発生しています。*Mark_Logic_Data/Logs/ErrorLog.txt* ファイルでエラーを確認して修正し、リストア操作をやり直してください。

20.7 ジャーナルアーカイブがオンのデータベースリストア

ジャーナルアーカイブがオンになっているデータベースをリストアすると、各フォレストは最後のトランザクションが異なるタイムスタンプでコミットされていることがあります。

例えば、以下の図は4つのフォレストとそれぞれのコミットされたトランザクションを示しています。各トランザクションの更新は表記規則「T#-u#」で識別され、コミットは「C」で識別されます。フォレストが最後のコミットを完了した時点はそれぞれ異なります。この例では、タイムスタンプ0～6をリストアしています。フォレストAはタイムスタンプ3までのトランザクションしかコミットしていませんが、フォレストBはタイムスタンプ6までのトランザクションをコミットしています。つまり、データベースをトランザクショナルに一貫性のある状態へ戻すには、すべてのフォレストをタイムスタンプ3以前までロールバックする必要があります。



データをリカバリしてデータベースをトランザクショナルに一貫性のある状態へ戻すには、次のオプションがあります。

- 可能な限り多くのデータをリストアする。「安全なタイムスタンプへのリストア」(256 ページ) の手順に従ってください。
- 特定のタイムスタンプ時点でデータをリストアする。「特定タイムスタンプへのリストア」(258 ページ) の手順に従ってください。
- 一部のサンプルドキュメントの状態に基づいて、特定タイムスタンプ時点のデータをリストアする。「サンプルドキュメントに基づいたリストア」(258 ページ) の手順に従ってください。

以降のセクションでは、XQuery API を使用してデータベースをリストアする方法について説明します。一部のタスクでは、管理画面も使用できます。

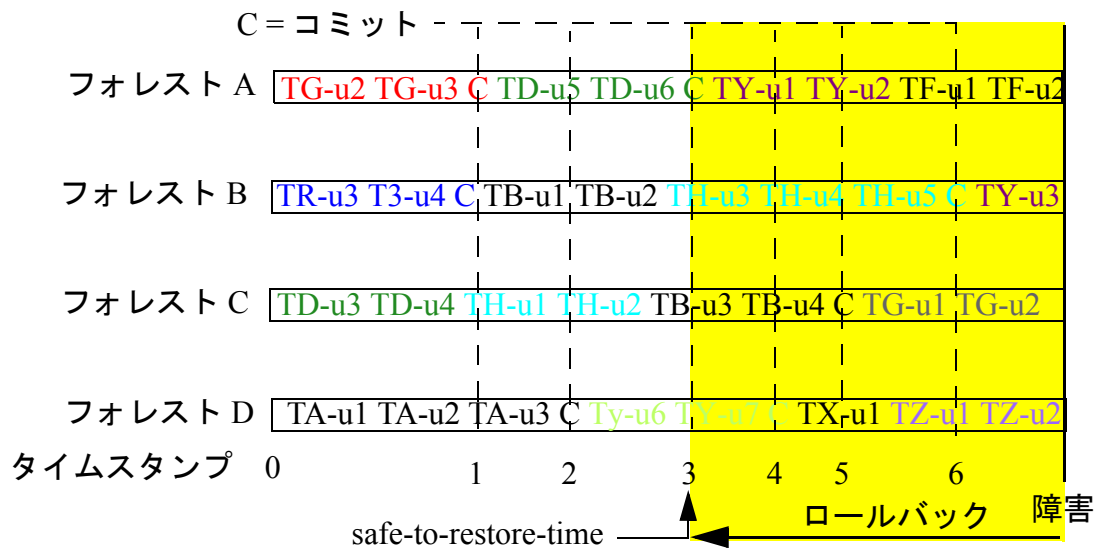
注： XA 分散トランザクション処理を使用している場合は、ある時点へのリストアによって、ターゲットのリストア時刻より前に準備され、その時刻より後にコミット / アボートされた XA トランザクションが復活することがあります。XA トランザクションを識別する方法の詳細については、『*XCC Developer's Guide*』の「[Heuristically Completing a MarkLogic Server Transaction](#)」を参照してください。

注： データベースクリア操作をまたいだロールバックはできません。そのため、クリア操作が発生した時点のサーバーログを確認する必要があります。

20.7.1 安全なタイムスタンプへのリストア

可能な限り多くのデータをリストアする場合は、最低限安全なタイムスタンプヘデータをリストアできます。

例えば、リストアするデータベースに以下のように 4 つのフォレストがあるとします。xdmp:host-status 関数を使用すると、safe-restore-to-time 値を見つけることができます。この値は、4 つの last-commit タイムスタンプのうち最も早いものです。この例では、safe-restore-to-time はフォレスト A で最後にコミットされたトランザクションのタイムスタンプです。



次の手順では、XQuery API を使用して最低限のタイムスタンプへリストアする方法について説明します。

1. `admin:database-get-merge-timestamp` 関数を使用して、現在のマージのタイムスタンプを取得します。この値は、ロールバック操作が完了するとリセットされる可能性があるため、保存しておきます。
2. `admin:database-set-merge-timestamp` 関数を使用して、マージのタイムスタンプを最低限安全なタイムスタンプより前の任意の時刻に設定します。これにより、フォレストデータをロールバックするまで、このタイムスタンプ後のマージでフラグメントが維持されます。
3. `xdmp:database-restore` 関数を使用し、`$journal-archiving` を `fn:true()`、`$restoreToTime` を `null()` に設定して、データベースを最新のタイムスタンプへリストアします。
4. リストア操作が完了したら、`xdmp:forest-rollback` 関数を使用して、フォレストを `xdmp:host-status` 関数によって返された `safe-restore-to-time` タイムスタンプへロールバックします。

例えば Documents データベースをリストアする場合は、次のクエリを使用してフォレストデータをロールバックできます。

```
xquery version "1.0-ml";
declare namespace host = "http://marklogic.com/xdmp/status/host";

let $timestamp :=
  xdmp:wallclock-to-timestamp(
    xs:dateTime(xdmp:host-status(xdmp:host("your-host.com"))
      /host:restore-jobs/host:restore-job/host:safe-restore-to-time
      /fn:data(.)))

return
  xdmp:forest-rollback(
    xdmp:database-forests(xdmp:database("Documents")),
    $timestamp)
```

5. `admin:database-set-merge-timestamp` 関数を使用して、マージのタイムスタンプを手順 1 で保存した値に戻します。

20.7.2 特定タイムスタンプへのリストア

次の手順では、XQuery API を使用して特定のタイムスタンプへデータベースをリストアする方法について説明します。

1. `admin:database-get-merge-timestamp` 関数を使用して、現在のマージのタイムスタンプを取得します。この値は、ロールバック操作が完了するとリセットされる可能性があるため、保存しておきます。
2. `admin:database-set-merge-timestamp` 関数を使用して、マージのタイムスタンプをリストアのタイムスタンプより前の任意の時刻に設定します。これにより、フォレストデータをロールバックするまで、このタイムスタンプ後のマージでフラグメントが維持されます。
3. `xdmp:database-restore` 関数を使用し、`$journal-archiving` を `fn:true()`、`$restoreToTime` をリストアのタイムスタンプに設定して、データベースをリストアします。
4. リストア操作が完了したら、`xdmp:forest-rollback` 関数を使用して、フォレストをリストアのタイムスタンプへロールバックします。例えば Documents データベースをリストアしていて、リストアのタイムスタンプが `2011-09-13T10:50:21.201832-07:00` である場合、`xdmp:forest-rollback` 関数の呼び出しは次のようになります。

```
xdmp:forest-rollback(  
  xdmp:database-forests(xdmp:database("Documents")),  
  xdmp:wallclock-to-timestamp(  
    xs:dateTime("2011-09-13T10:50:21.201832-07:00")))
```

5. `admin:database-set-merge-timestamp` 関数を使用して、マージのタイムスタンプを手順 1 で保存した値に戻します。

20.7.3 サンプルドキュメントに基づいたリストア

一部のサンプルドキュメントの状態を使用して、データベースをリストアする時刻を決定できます。

次の手順では、XQuery API を使用して一部のドキュメントの状態へリストアする方法について説明します。

1. `admin:database-get-merge-timestamp` 関数を使用して、現在のマージのタイムスタンプを取得します。この値は、ロールバック操作が完了するとリセットされる可能性があるため、保存しておきます。
2. `admin:database-set-merge-timestamp` 関数を使用して、マージのタイムスタンプをバックアップが作成された時点より前の任意の時刻に設定します。これにより、フォレストデータをロールバックするまで、このタイムスタンプ後のマージでフラグメントが維持されます。

3. `xdmp:database-restore` 関数を使用し、`$journal-archiving` を `true`、`$restoreToTime` を `null ()` に設定して、データベースを最新のタイムスタンプへリストアします。
4. リストア操作が完了したら、ポイントインタイムクエリを使用して (『*Application Developer's Guide*』の「[Point-In-Time Queries](#)」の章を参照)、サンプルドキュメントが最後に正しい状態であったと考えられる時刻を特定します。
5. `xdmp:forest-rollback` 関数を使用して、成功したポイントインタイムクエリで使ったタイムスタンプへのフォレストをロールバックします。例えば Documents データベースをリストアしていて、タイムスタンプが `2011-09-13T10:57:25.201832-07:00` であるドキュメントが正しい状態であると考えられる場合、`xdmp:forest-rollback` 関数の呼び出しは次のようになります。

```
xdmp:forest-rollback (
  xdmp:database-forests (xdmp:database ("Documents")),
  xdmp:wallclock-to-timestamp (
    xs:dateTime ("2011-09-13T10:50:21.201832-07:00")))
```
6. `admin:database-set-merge-timestamp` 関数を使用して、マージのタイムスタンプを手順 1 で保存した値に戻します。

20.8 ジャーナルアーカイブがオンの増分バックアップからのリストア

増分バックアップからリストアでは、サーバーはバックアップタグのベースバックアップを使用して、フルバックアップまでの一連の増分バックアップを取得します。フルバックアップを使用してリストアが開始します。次に、増分バックアップを逆順に使用してリストアします。フルバックアップのディレクトリと、必要に応じて増分バックアップのディレクトリを指定する必要があります。リストアタイムスタンプが指定されていない場合、サーバーはリストア対象となる最新のバックアップを見つけます。このプロセスが完了したら、ジャーナルアーカイブを使用してデータベースを現在の時刻へリストアできます。

リストアタイムスタンプが指定されている場合、サーバーはリストアタイムスタンプが最低限のクエリタイムスタンプとバックアップタイムスタンプの間にあるバックアップを見つけます。この要件を満たすバックアップがなく、ジャーナルアーカイブが存在する場合、サーバーはバックアップタイムスタンプがリストア対象タイムスタンプよりも小さな最新のバックアップを見つけます。そのバックアップへリストアし、ジャーナルをリストア対象タイムスタンプまでリプレイします。

ジャーナルアーカイブが存在する場合、サーバーは最新の増分バックアップのバックアップタイムスタンプを見つけ、そのタイムスタンプからジャーナルをリプレイします。

注： 増分バックアップからリストアすると、以前のフルバックアップの場所を現行の増分バックアップに使用できません。リストア後は新規にフルバックアップを作成し、そのフルバックアップの場所を現行の増分バックアップに使用する必要があります。つまり、増分バックアップからのリストア後は、新規のフルバックアップの場所を使用するようにすべての定期バックアップを更新する必要があります。リストア後に古いフルバックアップの場所を増分バックアップに使用すると、エラーが発生します。

次の手順では、フルバックアップ、1つあるいは複数の増分バックアップ、およびジャーナルアーカイブを使用して、データベースを現在の時点へリストアする方法について説明します。ジャーナルアーカイブを使用したフルバックアップと、ジャーナルアーカイブを使用した1つあるいは複数の増分バックアップが必要です。

1. `admin` ロールを持つユーザーとして管理画面にログインします。管理画面の左側メニューで、[Databases] リンクをクリックします。
2. ツリーメニューまたは [Summary] タブで、リストアするデータベースのデータベース名をクリックします。このデータベースは、バックアップしたデータベースと同じ設定（インデックスオプション、フラグメンテーション、レンジインデックス）になっている必要があります。

注： ジャーナルアーカイブには、リストアターゲットのタイムスタンプまたは現在のタイムスタンプが必要です。この例では、リストアターゲットに空のフィールド（最新のリストア時刻 / 現在のタイムスタンプ）を使用します。

3. [Backup/Restore] タブをクリックします。[Backup/Restore] 画面が表示されます。[Restore from directory] フィールドで、バックアップが存在するディレクトリを入力します。

注： 入力したディレクトリに同じデータベースの複数のバックアップが含まれる場合は、最新のバックアップが使用されます。リストア対象として特定のバックアップを選択する場合は、リストアするバックアップに対応する「date_stamp」サブディレクトリを入力します。ディレクトリ構造の詳細については、「バックアップディレクトリの構造」（237 ページ）を参照してください。

4. フォレストにローカルディスクフェイルオーバーを設定した場合、必要に応じて [Include Replica Forests] を [true] に設定して、バックアップからレプリカフォレストをリストアできます。このオプションを使用するには、バックアップ時にレプリカフォレストを含めるオプションをオンにしておく必要があります。フォレストにローカルディスクフェイルオーバーを設定する方法の詳細については、『*Scalability, Availability, and Failover Guide*』の [Configuring Local-Disk Failover for a Forest](#) を参照してください。

The screenshot shows a dialog box titled "Restore the govtrack database." with the following fields and options:

- Restore from directory:** A text input field containing "/backups". Below it, the text "The backup directory pathname. Required." is displayed.
- Include replica forests:** Radio buttons for "true" (selected) and "false".
- Use incremental backup:** Radio buttons for "true" (selected) and "false".
- Use journal archive:** Radio buttons for "true" (selected) and "false".
- Restore to time:** A text input field. Below it, the text "Leave blank for latest restore time or use xs.DateTime-Format like 2015-09-04T12:11:49-07:00" is displayed.

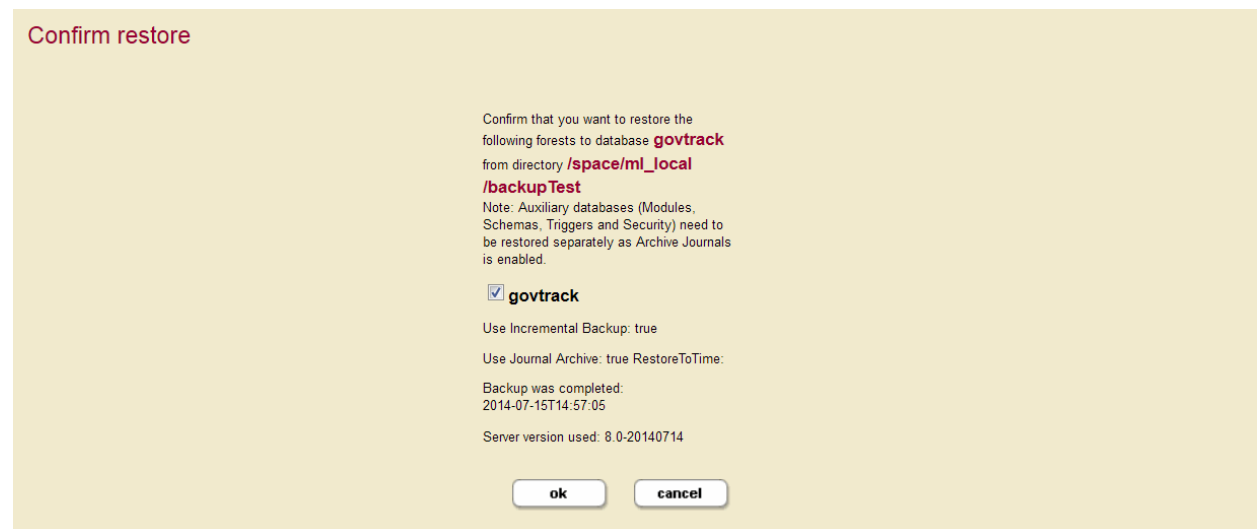
At the bottom of the dialog are "ok" and "cancel" buttons.

5. [Use incremental backup] を [true] に設定します。[Use journal archive] を [true] に設定します。[Restore to time] を空白のままにするか、`xs:DateTime-Format` で時刻を入力します。

注： ジャーナルアーカイブが動作するためには、[Restore to time] が必要です。これが存在しない場合、指定場所で見つかった最新の増分バックアップを使用してリストアが処理されます。また、[Merge Timestamp] は [Restore Time] より前に指定してください。

ジャーナルアーカイブがオンであるバックアップをリストアするときは、マージのタイムスタンプを 0 から 0 以外の値に変更してください。マージのタイムスタンプに 0 を使用した場合、ジャーナルアーカイブを使用して restore-to-time が 0 に指定されたリストアでエラーが発生します。マージのタイムスタンプは 0 以外の値に設定されている必要があります。

6. [ok] をクリックして、リストアプロセスを開始します。
7. [Confirm restore] 画面に、リストアに選択したすべてのオプションがリストされます。[ok] をクリックします。



[Restores] テーブルには、リストアが開始した日時、推定残り時間、およびリストア操作に関するその他のステータス情報がリストされます。

Restores												
Forest	Path	State	Start Time	Estimated Completion	Current Size	Final Size						
govtrack	/space/ml_local/backupTest /20140715-1456511200000/Forests/govtrack	copying	2:30 PM July 16, 2014	unknown	0 MB	300 MB						

Rates (Megabytes per Second)												
Forest	Query Reads	Journal Writes	Save Writes	Merge Reads	Merge Writes	Backup Reads	Backup Writes	Restore Reads	Restore Writes	Large Reads	Large Writes	
govtrack	0	0	0	1.15625	0	0	0	5.849562	7.285945	0	0	

Loads (Seconds per Second)												
Forest	Query Reads	Journal Writes	Save Writes	Merge Reads	Merge Writes	Backup Reads	Backup Writes	Restore Reads	Restore Writes	Large Reads	Large Writes	
govtrack	0	0	0	0.007625	0	0	0	0.003810196	0.1271666	0	0	

このプロセスが完了すると、[Restores] テーブル内のエントリは表示されなくなります。

20.9 ローカルディスクフェイルオーバー後のデータベースのバックアップとリストア

ローカルディスクフェイルオーバー用に設定されたマスターフォレストを含むホストで障害が発生すると、マスターフォレストにアタッチされたデータベースはレプリカフォレストへフェイルオーバーします。このセクションでは、残ったレプリカフォレストデータをバックアップし、そのデータを、マスターフォレストを含むホストがリストアされた後でリストアする方法について説明します。このセクションで説明する手順例では、Documents データベースが一方のホスト上の Documents-master フォレストにアタッチされていて、別のホスト上の Documents-rep フォレストへローカルディスクフェイルオーバーするように設定されています。

ローカルディスクフェイルオーバーを設定する方法の詳細については、『*Scalability, Availability, and Failover Guide*』の [Configuring Local-Disk Failover for a Forest](#) を参照してください。

1. 障害が発生する前、Documents-master フォレストは open 状態、Documents-rep フォレストは sync replicating 状態です。

Forest	Host	State	Documents
Documents-master	gordon-3.marklogic.com	open	290,001
Documents-rep	gordon-2.marklogic.com	sync replicating	290,001
Total			290,001

2. Documents-master フォレストを含むホストで障害が発生すると、Documents データベースは Documents-rep フォレストへ自動的にフェイルオーバーします。これで Documents-rep フォレストは open 状態になり、Documents データベースの代わりに更新に対応します。

注： Documents データベースの設定はフェイルオーバー前から変更されません。

Forest	Host	State	Documents
Documents-master - This forest has an error, is disabled, or is ca			
Documents-rep	gordon-2.marklogic.com	open	290,001
Total			290,001

Documents-rep フォレストをバックアップするには、次の手順を実行します。

注： バックアップ手順とリストア手順の両方を Documents-rep フォレストを含むホストで実行する必要があります。

1. Documents-rep フォレストを含むホストマシンで、Documents データベースをバックアップします。[Include Replica Forests] は [true] に設定します。

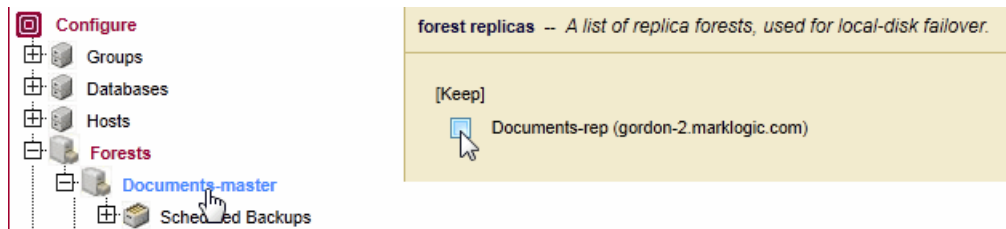
2. バックアップ対象として [Documents-rep] フォレストのみを選択します。

3. Documents-master フォレストを含むホストがリストアされると、Documents-master フォレストはレプリカフォレストになり、レプリケートされた更新を Documents-rep フォレストから受け取ります。

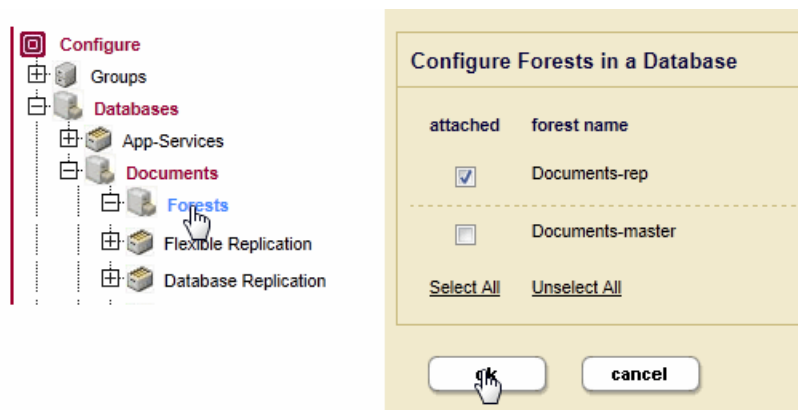
Forest	Host	State	Documents
Documents-master	gordon-3.marklogic.com	sync replicating	286,001
Documents-rep	gordon-2.marklogic.com	open	286,001
Total			286,001

フェイルオーバー後にバックアップした Documents-rep フォレストからデータをリストアする前に、Documents-master フォレストが新しいレプリカフォレストになるように Documents-rep フォレストから Documents-master フォレストへのローカルディスクフェイルオーバーを再設定します。

1. Documents-master フォレストの設定ページで、Documents-rep フォレストへのレプリケーションをオフにします。



2. Documents データベースの [Forests] 設定ページに移動します。Documents-master フォレストをアタッチ解除し、Documents-rep フォレストをアタッチします。



3. Documents-rep フォレストの設定ページに移動し、ローカルディスクフェイルオーバー用に Documents-master フォレストを選択します。



4. Documents-rep フォレストを含むホストで、このフォレストが open 状態であることを確認し、フェイルオーバー後に作成されたバックアップから Documents データベースをリストアします。

Restore the **Documents** database.

Restore from directory: /tmp
The backup directory pathname.
Required.

Include replica forests: true false

Use journal archive: true false

Restore to time: Leave blank for latest restore time or use xs:DateTime-Format like 2011-12-08T15:13:28-08:00

5. リストア対象として Documents-rep フォレストのみが選択されていることを確認します。

Confirm that you want to restore the following forests to database **Documents** from directory /tmp

Documents-rep Documents-master

Use Journal Archive: false RestoreToTime:

6. Documents-rep フォレストがリストアされると、更新は Documents-master フォレストにレプリケートされます。

Forest	Host	State	Documents
Documents-master	gordon-3.marklogic.com	sync replicating	290,001
Documents-rep	gordon-2.marklogic.com	open	290,001
Total			290,001

21.0 ローリングアップグレード

トランザクション負荷の高い環境で高可用性クラスタを使用するユーザーは、MarkLogic の新バージョンへシームレスにアップグレードする必要があります。クラスタ内のホストが1つずつアップグレードされるローリングアップグレードは、このニーズに対応するアプローチの1つです。ローリングアップグレードは、可用性のダウンタイムやトランザクションの中断を生じさせずに、多数のホストで構成される大規模なクラスタを MarkLogic サーバーの新バージョンにアップグレードするときに使用されます。パッチを複数のホストに適用するときにも、ローリングアップグレードが使用されます。

ローリングアップグレードを実行する目的は、サーバーの可用性やトランザクショナルデータのダウンタイムをゼロにすることです。これは、大量のトランザクションが進行中である大規模な高可用性 (HA) クラスタで最も有用です。ローリングアップグレードは、プライマリクラスタと災害対策 (DR) クラスタの両方で実行できます。

ローリングアップグレードを実行するには、MarkLogic 8.0-6 以降がインストールされている必要があります。ローリングアップグレード機能は、サポートされるすべてのプラットフォームで動作します。

注： ローリングアップグレードは MarkLogic 8.0-6 以降から MarkLogic 9.0-x 以降へアップグレードするときのみ機能します。

この章では、ローリングアップグレードについて説明します。以下のセクションで構成されています。

- [ローリングアップグレードについて](#)
- [例：ローリングアップグレード](#)
- [ローリングアップグレードの実行](#)
- [部分アップグレードのロールバック](#)
- [ローリングアップグレードの API](#)
- [他の MarkLogic 機能との関係](#)
- [その他のアップグレードオプション](#)

21.1 ローリングアップグレードについて

ローリングアップグレードでは、MarkLogic サーバーの新しいバージョンを順次 (ホストごとに) インストールします。新しいバージョンをインストールするためにクラスタ全体をダウンさせる必要はありません。ローリングアップグレードを実行すると、アップグレードプロセスの一定期間、クラスタは混在状態 (MarkLogic サーバーの複数バージョンが実行している状態) になることがあります。このプロセス中、MarkLogic の新バージョンの機能は、クラスタ全体が新しいバージョンにコミットされるまで使用できません。このため、アプリケーションコードが混在環境で動作するように、ローリングアップグレードを開始する前にコードの一部を変更または修正しなければならないことがあります。例えば、アップグレードのコミット前に JavaScript コードは修正が必要になることがあります (サーバーサイド JavaScript が V8 の新しいバージョンになるため)。

注： クラスタ内のすべてのノードが 9.0-1 にアップグレードされるまで、9.0-1 の機能を利用するようにアプリケーションを変更しないでください。

セキュリティデータベースとスキーマデータベースは、同じホスト上に存在する必要があります。またそのホストを、クラスタをアップグレードするときに最初にアップグレードする必要があります。

注： 混在ノードクラスタでは、アップグレードのコミット前に、MarkLogic 9.0-1 へアップグレードされたノードは読み取り専用になります。これは、9.0-1 ノードから設定が変更されないようにするためです。クラスタ全体のアップグレードが完了するまでは、設定の変更を加えないようにすることを強くお勧めします。

ローリングアップグレード機能を使用しなくても、トランザクションのダウンタイムを最小限に抑えて（5～10分未満）クラスタをアップグレードできます。通常のアップグレードプロセスの代わりに、複雑さが増すローリングアップグレードを使用することが正当かどうかを検討してください。通常のアップグレードプロセスについては、『*Installation Guide*』の「[Upgrading from Previous Releases](#)」を参照してください。

ローリングアップグレードプロセスの手順は次のとおりです。

- **バックアップ：** アップグレード対象となるホストをバックアップします。詳細については、「データベースのバックアップおよびリストア」（235 ページ）を参照してください。
- **準備：** アップグレード前に必要になる可能性のあるコードやアプリケーションを準備します（詳細については、「他の MarkLogic 機能との関係」（279 ページ）を参照）。
- **アップグレード：** 実際にアップグレードを実行します。
- **クリーンアップ**

アップグレードを開始する前に、アップグレード対象となるホストのバックアップが必要です。その後、考えられる準備に応じて、アップグレード前に必要なコードやアプリケーションを用意します（「他の MarkLogic 機能との関係」（279 ページ）を参照）。

アップグレードが完了したら、クリーンアップの実行が必要になることがあります。

21.1.1 有効バージョンとソフトウェアバージョン

アップグレードをコミットするまで、クラスタ内のホストで「有効なバージョン」は、新しいバージョンではなく以前のバージョンです（例えば 9.0-1 ではなく 8.0-6）。有効バージョンとは、クラスタが全体として実行しているバージョンです。「ソフトウェアバージョン」とは、各ホストにインストールされている MarkLogic サーバーのバージョンです。管理画面にログインするときにセキュリティデータベースをアップグレードすることを求められます。

注： ローリングアップグレードをコミットした後でリストアできるのは、以前のバージョン（例えば 8.0-6）ではなく新しいバージョン（例えば 9.0-1）のみです。未コミット状態のクラスタの実行は、MarkLogic のこれまでの（以前の）バージョンでの実行と同等です。アップグレードがコミットされるまでは、9.0-1 の機能を利用できません。

MarkLogic の新バージョンをコミットした後は、セキュリティデータベースのアップグレードが必要です。アップグレードのコミットによりすべてのホストが新しい（9.0-1）コードレベルになりますが、セキュリティデータベースがアップグレードされるまでクラスタは使用できません。

21.2 例：ローリングアップグレード

ローリングアップグレードをホスト 3 台の小規模なクラスタで実行する場合の単純化した手順を次に示します。大まかな流れは、初めにすべてのホストをバックアップし、ソフトウェアアプリケーションに変更を加え、各ノードのフェイルオーバーとアップグレードでローリングアップグレードを進めます。クラスタ内のすべてのノードがアップグレードされたら、アップグレードをコミットしてクラスタの有効バージョンを新バージョンに変更できることを確認します。最後に、必要なクリーンアップを実行します。

また、アップグレードを開始する前に、バージョンが混在するクラスタで実行できるように既存ソフトウェアの修正が必要になることがあります。詳細については、「他の MarkLogic 機能との関係」（279 ページ）を参照してください。

1. 既存クラスタのすべてのホストをバックアップします。ホストをバックアップする方法の詳細については、「データベースのバックアップおよびリストア」（235 ページ）を参照してください。
2. 修正が必要なコードがあれば修正を加えます。考えられるソフトウェアの問題の一覧については、「他の MarkLogic 機能との関係」（279 ページ）を参照してください。
3. ホストのモードを `maintenance` に切り替えて、このノードが保守のために一時ダウンすることを指定します。

a. `admin:host-set-mode($config,xdmp:host("hostname"),"maintenance","Upgrading host")`

4. 1 つ目のホストをダウンさせ、アップグレードを開始します。コマンドラインから以下のコマンドを使用します。

- a. MarkLogic を停止します。

```
sudo /sbin/service MarkLogic stop
```

- b. 既存の RPM をアンインストールします。

```
rpm uninstall MarkLogic-8.0-1.x86_64.rpm
```

- c. 新しい RPM をインストールします。

```
rpm install MarkLogic-9.0-1.x86_64.rpm
```

- d. ホストを復帰させ、MarkLogic を起動します。

```
sudo /sbin/service MarkLogic start
```

5. ホストのモードを `normal` に設定します。

- a. `admin:host-set-mode($config,xdmp:host("hostname"),"normal","Done Upgrading")`

6. クラスタ内の各ホストについて、手順 3 ~ 5 を繰り返します（ノードごとにアップグレードプロセスを実行する必要があります）。

7. すべてのホストのアップグレードが完了したら、ソフトウェアバージョン、およびクラスタの有効バージョンを確認し、アップグレードをコミットします。

クラスタの有効バージョンを確認するには、次の XQuery コマンドを使用します。

```
xquery version "1.0-ml";
import module namespace admin = "http://marklogic.com/xdmp/admin"
  at "/MarkLogic/admin.xqy";

let $config := admin:get-configuration()
return
  admin:cluster-get-effective-version($config)

=>
(: returns the effective software version of this cluster :)
```

クラスタがアップグレードをコミットできる状態であるかどうかを確認するには、次のクエリを使用します。

```
xquery version "1.0-ml";
import module namespace admin = "http://marklogic.com/xdmp/admin"
  at "/MarkLogic/admin.xqy";

return
  admin:can-commit-upgrade()

=>
(: returns true if the cluster is ready to commit the upgrade :)
```

アップグレードをコミットするには、クラスタのバージョンが 9000100 以降になっている必要があります。

アップグレードをコミットしたら、次のクエリを使用してアップグレードを検証します。

```
xquery version "1.0-m1";
import module namespace admin = "http://marklogic.com/xdmp/admin"
  at "/MarkLogic/admin.xqy";

let $config := admin:get-configuration()
return
  admin:cluster-get-effective-version($config)

=>
(: returns the effective software version of the cluster :)
```

ローリングアップグレード用のこのシンプルな手順例は、スクリプト化も可能です。スクリプトのモデル例については、「REST 管理 API を使用したローリングアップグレード」(270 ページ) を参照してください。

21.3 ローリングアップグレードの実行

REST 管理 API または XQuery API を使用してスクリプトを作成して、ローリングアップグレードを実行できます。ローリングアップグレードは、AWS クラスタ上でも実行できます。このセクションでは、ローリングアップグレードの設定および実行のさまざまなオプションについて説明します。

- [REST 管理 API を使用したローリングアップグレード](#)
- [EC2 インスタンスのアップグレード](#)
- [XQuery を使用したローリングアップグレード](#)
- [本番クラスタと災害対策クラスタの両方のローリングアップグレード](#)

21.3.1 REST 管理 API を使用したローリングアップグレード

ホストをバックアップし、アプリケーションを準備したら、REST 管理 API を使用してローリングアップグレードを実行できます。次の例では、8.0-6 がインストールされている 3 ノードクラスタを 9.0-x にアップグレードすること想定しています。

1 つの 3 ノードクラスタのアップグレードをスクリプト化するモデルとして、以下のコードサンプルを使用できます。

```
(: This is an end-to-end scenario to orchestrate a rolling upgrade on a
3-node 8.0 cluster to a 9.0 build.:)

(: Iterate over each host in the cluster :)
```

GET:/manage/v2/hosts

```
(: Remove host from load-balancer rotation if necessary :)
```

```
(: Place the host into maintenance mode :)
```

PUT:/manage/v2/hosts/{id|name}/properties

```
(: Disable any local-disk forests on the host to force a failover :)
PUT:/manage/v2/forests/{id|name}/properties

(: Change primary host for any shared-disk forests :)
PUT:/manage/v2/forests/{id|name}/properties

(: Restart any failover forests that are open on the host :)
PUT:/manage/v2/forests/{id|name}?state=restart

$ curl --anyauth --user user:password -i -X POST --data
"state=restart" \
  http://localhost:8002/manage/v2

(: Wait for task-server and app servers to become idle :)
GET:/manage/v2/servers, GET:/manage/v2/servers/{id|name}?view=status

(: Stop the host :)

$ curl -v -X POST --anyauth --user admin:admin
-H "Content-Type:application/x-www-form-urlencoded"
-d"state=stop" "http://localhost:8002/manage/v2"

(: Upgrade the software :)

curl -v -X POST --anyauth --user $MANAGEADMIN:$MANAGEPASS
--header "Content-Type:application/x-www-form-urlencoded"
-d"state=commit-upgrade" "http://localhost:8002/manage/v2"
(: Start the host :)

$ curl -v -X POST --anyauth --user admin:admin
-H "Content-Type:application/x-www-form-urlencoded"
-d"state=restart" "http://localhost:8002/manage/v2"

(: Enable any local-disk failover forest on the host :)
PUT:/manage/v2/forests/{id|name}/properties

(: Restore primary host for any shared-disk forests :)
PUT:/manage/v2/forests/{id|name}/properties

(: Restart any failover forests that should fail back. :)
PUT:/manage/v2/forests/{id|name}?state=restart

(: Take the host out of maintenance mode :)
PUT:/manage/v2/forests/{id|name}/properties

(: upgrade security db :)
curl -v -X POST --anyauth --user admin:admin
--header "Content-Type:application/x-www-form-urlencoded"
```

```
-d"state=security-database-upgrade"
"http://localhost:8002/manage/v2"

(: verify cluster version :)
curl -v -X GET --anyauth --user admin:admin
--header "Content-Type:application/json"
http://localhost:8002/manage/v2?format=json | tools/jq/jq '.
["local-clusterlocalhost-default"]["effective-version"]'
```

注： JSON プロパティを解析するために jq ツールを使用しています。
<https://stedolan.github.io/jq/> から無償でダウンロードできます。

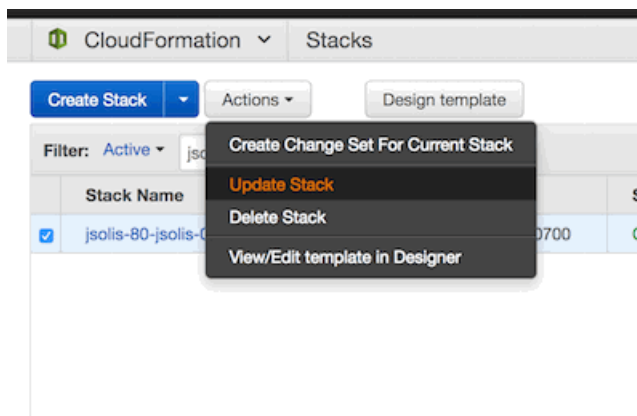
21.3.2 EC2 インスタンスのアップグレード

EC2 (AWS) でのローリングアップグレードプロセスは非常にシンプルです。CloudFormation テンプレートの通常の更新とよく似ています。通常の更新の詳細については、『*MarkLogic Server on Amazon EC2 Guide*』の「[Upgrading the MarkLogic AMI](#)」を参照してください。

この例では、CloudFormation テンプレートから MarkLogic 8.0 を実行している既存の 3 ノードクラスタがあると想定します。インスタンスをアップグレードする前に、新しい AMI (9.0 CF テンプレート) を参照するように CloudFormation テンプレートをアップグレードする必要があります。テンプレートをアップグレードする方法の詳細については、<http://developer.marklogic.com/products/aws> を参照してください。

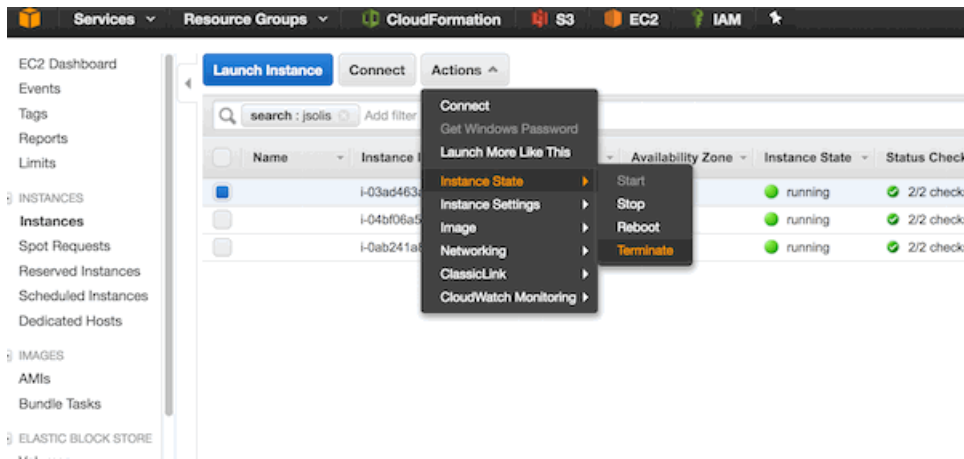
追加の手順は次のとおりです。

1. アップグレードの前に、重要なデータをすべてバックアップしておきます。
2. 更新後の CloudFormation テンプレートを使用してスタックを更新します。スタックの更新が完了していることを確認します。



注： CloudFormation テンプレートの自動置き換えは推奨されません。代わりに、既存のテンプレートをコピーし (AMI ID が含まれる場合)、AMI ID を編集し、そのテンプレートを更新に使用してください (AMI ID がパラメータやその他の方法で渡される場合は、その方法を使用してください)。

- EC2 ダッシュボードでインスタンスを1つずつ終了し、新しいインスタンスに置き換えられるまで待ちます。セキュリティデータベースが含まれる「マスター」インスタンスまたはノードから開始します。管理対象クラスタ機能によって、ホストは自動的に再起動します。

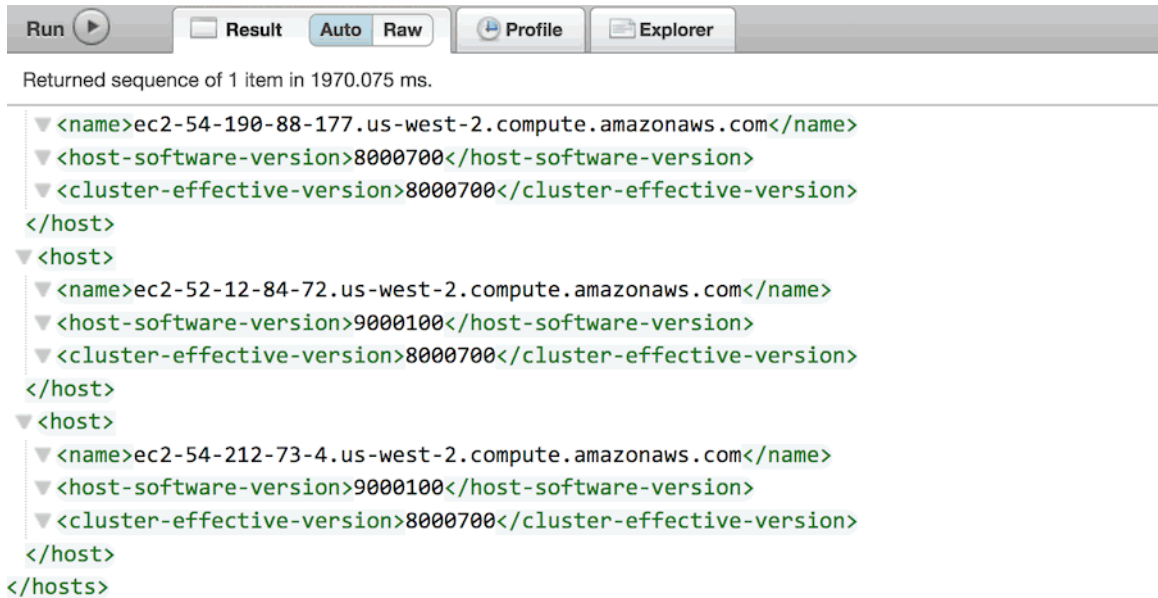


ホストが（新しいホスト名で）復帰するまで待ちます。

- EC2 ダッシュボードで、このプロセスを繰り返してノード2を停止します。
- すべてのノードが更新されたら、次のクエリを使用してクエリコンソールからクラスタの状態を確認します。

```
xquery version "1.0-m1";

<hosts>{
  for $i in xdmp:host-name(xdmp:hosts())
  return (
    let $response :=
      xdmp:http-get(concat("http://localhost:8002/manage/v2/hosts/",
        $i,"?view=status&format=json"),
        <options xmlns="xdmp:http">
          <authentication method="digest">
            <username>admin</username>
            <password>admin</password>
          </authentication>
          <headers>
            <content-type>application/json</content-type>
          </headers>
        </options>)
    return (
      <host>
        <name>{$response[2]//*:name/data()}</name>
        <host-software-version>{$response[2]//*:software-version/
          value/data()}</host-software-version>
        <cluster-effective-version>{$response[2]//*:
          effective-version/value/data()}</cluster-effective-versio
n>
      </host>
    ) )</hosts>
```



```

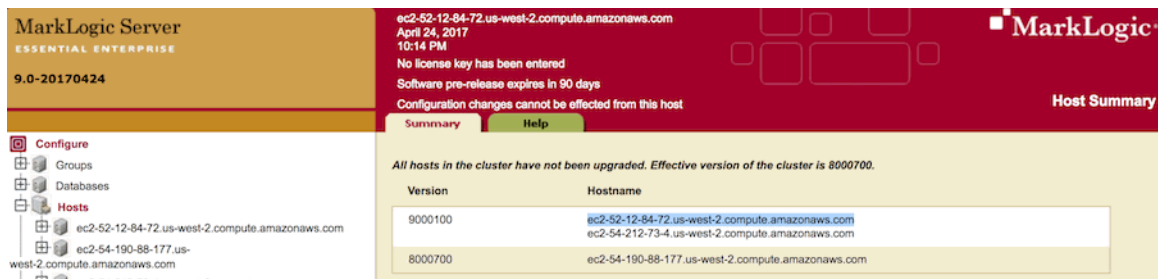
Returned sequence of 1 item in 1970.075 ms.

<▼ <name>ec2-54-190-88-177.us-west-2.compute.amazonaws.com</name>
  <▼ <host-software-version>8000700</host-software-version>
  <▼ <cluster-effective-version>8000700</cluster-effective-version>
</host>
<▼ <host>
  <▼ <name>ec2-52-12-84-72.us-west-2.compute.amazonaws.com</name>
  <▼ <host-software-version>9000100</host-software-version>
  <▼ <cluster-effective-version>8000700</cluster-effective-version>
</host>
<▼ <host>
  <▼ <name>ec2-54-212-73-4.us-west-2.compute.amazonaws.com</name>
  <▼ <host-software-version>9000100</host-software-version>
  <▼ <cluster-effective-version>8000700</cluster-effective-version>
</host>
</hosts>

```

この内容で問題ありません。

- ホストのステータスを確認するには、8001 から呼び出します。確認するための正確な URL は <http://hostname:8001/host-summary.xqy?section=host> です。



MarkLogic Server
ESSENTIAL ENTERPRISE
9.0-20170424

ec2-52-12-84-72.us-west-2.compute.amazonaws.com
April 24, 2017
10:14 PM
No license key has been entered
Software pre-release expires in 90 days
Configuration changes cannot be effected from this host

MarkLogic
Host Summary

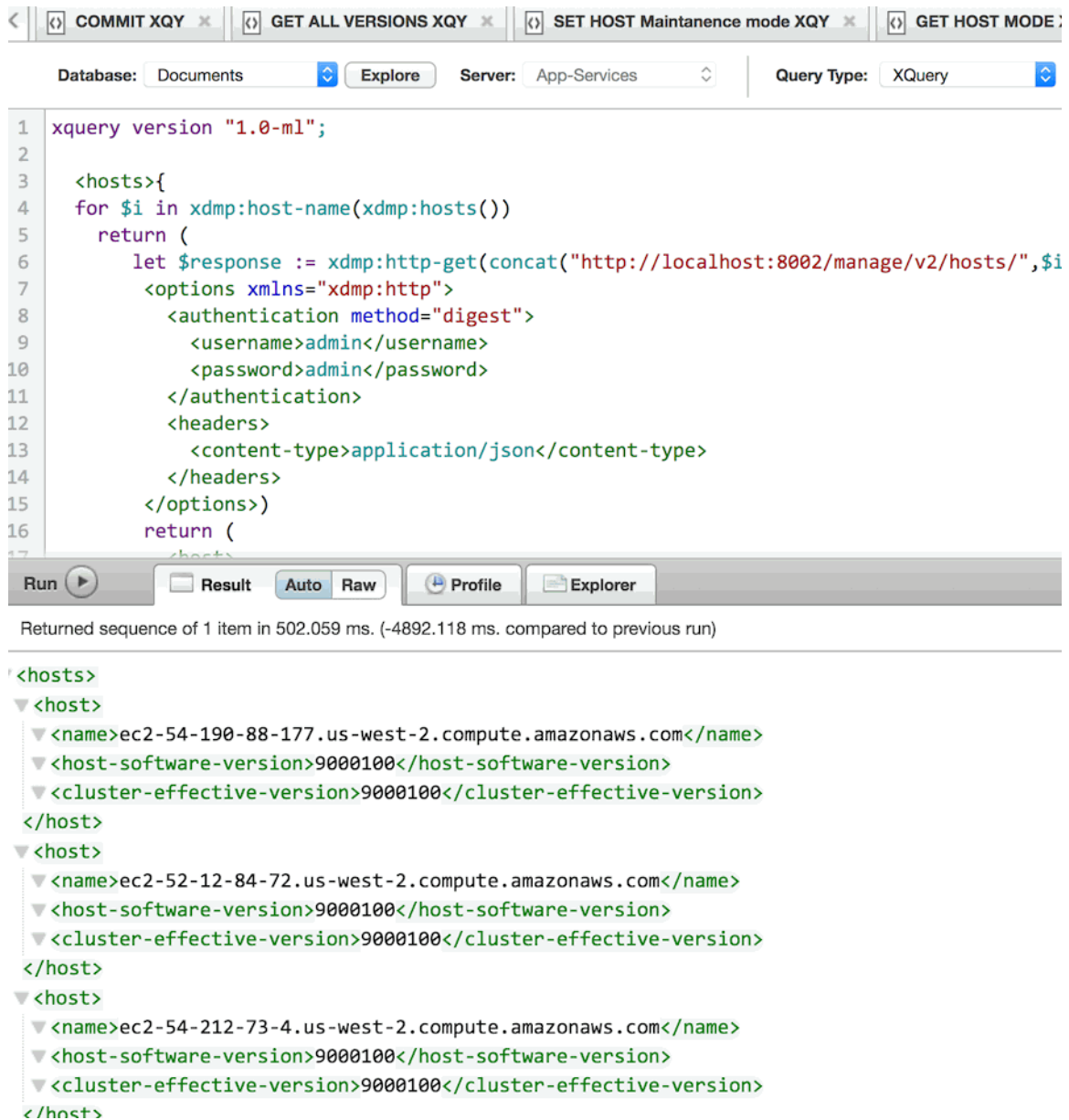
Summary Help

All hosts in the cluster have not been upgraded. Effective version of the cluster is 8000700.

Version	Hostname
9000100	ec2-52-12-84-72.us-west-2.compute.amazonaws.com ec2-54-212-73-4.us-west-2.compute.amazonaws.com
8000700	ec2-54-190-88-177.us-west-2.compute.amazonaws.com

- ノード3についてこの手順を繰り返します。

8. ノード 3 の更新が完了したら、クラスタの有効バージョンを確認して、アップグレードが完了したことを検証します。



The screenshot shows the MarkLogic Query Console interface. At the top, there are tabs for 'COMMIT XQY', 'GET ALL VERSIONS XQY', 'SET HOST Maintenance mode XQY', and 'GET HOST MODE'. Below the tabs, the 'Database' is set to 'Documents', the 'Server' is 'App-Services', and the 'Query Type' is 'XQuery'. The main area contains the following XQuery code:

```

1 xquery version "1.0-m1";
2
3 <hosts>{
4   for $i in xdm:host-name(xdm:hosts())
5     return (
6       let $response := xdm:http-get(concat("http://localhost:8002/manage/v2/hosts/", $i
7         <options xmlns="xdmp:http">
8           <authentication method="digest">
9             <username>admin</username>
10            <password>admin</password>
11          </authentication>
12          <headers>
13            <content-type>application/json</content-type>
14          </headers>
15        </options>)
16        return (
17          <host>{
18            <name>{ $response["name"] }
19            <host-software-version>{ $response["host-software-version"] }
20            <cluster-effective-version>{ $response["cluster-effective-version"] }
21          }
22        )
23      )
24   }
25 </hosts>

```

Below the code, there are buttons for 'Run', 'Result', 'Auto', 'Raw', 'Profile', and 'Explorer'. The 'Run' button is highlighted. Below the buttons, the text reads: 'Returned sequence of 1 item in 502.059 ms. (-4892.118 ms. compared to previous run)'. The output is shown as a JSON document:

```

<hosts>
  <host>
    <name>ec2-54-190-88-177.us-west-2.compute.amazonaws.com</name>
    <host-software-version>9000100</host-software-version>
    <cluster-effective-version>9000100</cluster-effective-version>
  </host>
  <host>
    <name>ec2-52-12-84-72.us-west-2.compute.amazonaws.com</name>
    <host-software-version>9000100</host-software-version>
    <cluster-effective-version>9000100</cluster-effective-version>
  </host>
  <host>
    <name>ec2-54-212-73-4.us-west-2.compute.amazonaws.com</name>
    <host-software-version>9000100</host-software-version>
    <cluster-effective-version>9000100</cluster-effective-version>
  </host>
</hosts>

```

9. ポート 8001 で任意の場所に移動すると、管理画面でセキュリティデータベースをアップグレードするように求められます。セキュリティデータベースをアップグレードするには、<http://ec2-52-12-84-72.us-west-2.compute.amazonaws.com:8001/security-upgrade.xqy> に移動します。これが終了すると、アップグレードが完了です。

21.3.3 XQuery を使用したローリングアップグレード

XQuery Admin API を使用して、クエリコンソールからローリングアップグレードをセットアップおよび実行できます。このセクションでは、クエリコンソールから使用できるサンプルコードを説明します。

REST 経由でホストバージョンを取得するには、次を実行します。

```
xquery version "1.0-m1";

<hosts>{
  for $i in xdmp:host-name(xdmp:hosts())
  return (
    let $response :=
      xdmp:http-get(concat("http://localhost:8002/manage/v2/hosts/", $i, "?view=status&format=json"),
        <options xmlns="xdmp:http">
          <authentication method="digest">
            <username>admin</username>
            <password>admin</password>
          </authentication>
          <headers>
            <content-type>application/json</content-type>
          </headers>
        </options>)
    return (
      <host>
        <name>{$response[2]//*:name/data()}</name>
        <host-software-version>{$response[2]//*:software-version/value/data()}</host-software-version>
        <cluster-effective-version>{$response[2]//*:effective-version/value/data()}</cluster-effective-version>
      </host>
    )
  )
}</hosts>
```

ホスト管理モードを maintenance に設定してホストをダウンさせるには、次を実行します。

```
xquery version "1.0-m1";
import module namespace admin = "http://marklogic.com/xdmp/admin"
  at "/MarkLogic/admin.xqy";

let $config := admin:get-configuration()
let $id := xdmp:host()
let $c := admin:host-set-mode($config, $id, "maintenance", "Bringing
down host to upgrade RPM")
return admin:save-configuration($c)
```

ホスト管理モードを normal に設定してホストを復帰させるには、次を実行します。

```
xquery version "1.0-m1";
import module namespace admin = "http://marklogic.com/xdmp/admin"
  at "/MarkLogic/admin.xqy";

let $config := admin:get-configuration()
let $id := xdmp:host()
let $c := admin:host-set-mode($config,$id,"normal", "Done upgrading
RPM")
return admin:save-configuration($c)
```

ホスト管理モードを取得するには、次を実行します。

```
xquery version "1.0-m1";
import module namespace admin = "http://marklogic.com/xdmp/admin"
  at "/MarkLogic/admin.xqy";

let $config := admin:get-configuration()
let $id := xdmp:host()
return (
  admin:host-get-mode($config,$id)
  ,admin:host-get-mode-description($config,$id)
)
```

アップグレードを完了するには、管理画面にログオンしてセキュリティデータベースをアップグレードします。

注： アップグレードをコミットすると、更新された設定が保存されます。このとき、5 秒の再読み取り遅延があり、XDQP 接続がドロップし始める前にすべてのオンラインホストが新しいファイルを受信できます。

「EC2 インスタンスのアップグレード」(272 ページ) の手順 10 を参照してください。サーバーが適切なバージョンではない場合、maintenance モードになっているホストがある可能性があります。admin:commit-upgrade 関数を使用すると、すべてのサーバーでソフトウェアバージョンが適切であるか検証できます。使用可能な XQuery 管理 API の詳細については、「Admin API」(278 ページ) を参照してください。

21.3.4 本番クラスタと災害対策クラスタの両方のローリングアップグレード

災害対策クラスタを先にアップグレードしてください。ソフトウェアの新しいバージョンではマスタークラスタでエンコードされたフラグメントやジャーナルフレームを受信できるようになるため、災害対策クラスタを先にアップグレードすることが重要です。

災害対策クラスタのアップグレードが完了してから、本番クラスタをアップグレードしてください。

21.4 部分アップグレードのロールバック

MarkLogic 9 以降へのアップグレードをコミット (`admin:commit-upgrade`) していない場合に限り、各ノードにサーバーの以前のバージョン (MarkLogic 8.0-6) を再インストールできます。

まだ完了およびコミットしていないアップグレードをロールバックする必要がある場合は、アップグレードしたマシンで MarkLogic の以前のバージョン (例えば 8.0-6) を再インストールすることで、部分アップグレードをロールバックできます。

21.5 ローリングアップグレードの API

MarkLogic クラスタでローリングアップグレードを管理するために使用できる API を次に示します。

21.5.1 Admin API

以下の Admin API 関数をローリングアップグレードに使用できます。

- `admin:cluster-get-effective-version`
クラスタの有効 MarkLogic バージョン (例えば 8.0-6 の場合は 8000700) を返します。
- `admin:can-commit-upgrade`
クラスタがアップグレードをコミットできる状態であれば `true` を返し、それ以外の場合は `false` を返します。
- `admin:host-get-mode`
ホストの現在のモードを取得します。モードは `normal` または `maintenance` です。
- `admin:host-get-mode-description`
ホストのホストモード説明を取得します (例えば `maintenance`)。
- `admin:host-set-mode`
ホストのモード (`normal` または `maintenance`) を設定します。
- `admin:commit-upgrade`
アップグレードをコミットし、クラスタの有効バージョンを新しいソフトウェアバージョンに設定します。

21.5.2 REST 管理 API

ローリングアップグレード操作を実行するときに、以下の REST 管理 API エンドポイントは有用な情報および機能を提供します。

- `GET:/manage/v2/properties` : 有効バージョンが含まれます
- `GET:/manage/v2/hosts?view=status` : `version`、`effective-version`、`maintenance-mode`、および `maintenance-mode-reason` が含まれます
- `GET:/manage/v2/hosts/{id|name}?view=status` : `version`、`effective-version`、`maintenance-mode`、および `maintenance-mode-reason` が含まれます
- `GET:/manage/v2/hosts/{id|name}/properties` : ホストの `maintenance` モードフラグおよび理由が含まれます
- `PUT:/manage/v2/hosts/{id|name}/properties` : ホストの `maintenance` モードフラグおよび理由を設定できます
- `POST:/manage/v2?state=commit-upgrade` : アップグレードを適用します

21.6 他の MarkLogic 機能との関係

MarkLogic 9 で想定どおりに動作する既存機能に対しては、ローリングアップグレードの影響はありません。一部の既存機能は、ローリングアップグレードが完了してクラスタが新しいバージョンへコミットされるまで、想定どおりに動作しない可能性があります。

一例として、セマンティックトリプルが挙げられます。ローリングアップグレードで混在モード中に同じデータが 2 回挿入されると、トリプルの件数が増える可能性があります。ローリングアップグレード中、MarkLogic 9 のトリプルインデックスは、MarkLogic 8 セマンティックの適切な順序でトリプルを返すことができません。そのため、このような状況が発生する値の種類を除き、同一のトリプルが複数必要になります。

MarkLogic 9 で導入された機能は、混在クラスタ（MarkLogic 9 への完全なアップグレードが完了していないため有効バージョンが 8.0-x であるクラスタ）で動作することも動作しないこともあります。ローリングアップグレードを実行する際に、確認が必要な可能性のある機能を次に示します。

- [SQL](#)
- [サーバーサイド JavaScript](#)
- [カスタム UDF](#)
- [円を含むリバースクエリ](#)

21.6.1 SQL

MarkLogic 9 では、トリプルインデックスを使用する新しいバージョンの SQL が導入されています。既存バージョン（MarkLogic 9 より前）は混在クラスタでも 9.0-x にアップグレードした後も引き続き動作します。新しいバージョンの SQL は混在クラスタでは動作しません。これらの機能を使用する前に、MarkLogic の新しいバージョンへアップグレードしてアップグレードをコミットする必要があります。

レンジインデックスに基づく以前の SQL バージョンは混在クラスタで動作し（アップグレードのコミット前）、MarkLogic 9 でも動作します。

21.6.2 サーバーサイド JavaScript

サーバーサイド JavaScript の新しいバージョンでは、`ValueIterator` が `Sequence` に置き換えられました。MarkLogic 8 で値のシーケンスを表現するために使用されていた `ValueIterator` インターフェイスは、新しい `Sequence` インターフェイスに置き換えられました。`Sequence` は JavaScript 反復可能オブジェクトです。これまで `ValueIterator` で動作していた、またはこれを返していたすべての関数は、代わりに `Sequence` を使用するようになりました。

多くの場合、この変更はコードに対して透過的です。ただし、次の `ValueIterator` のプロパティおよびメソッドに依存するコードは変更が必要です。

- `ValueIterator.next` : `for..of` ループを使用して、`Sequence` で反復します。`Sequence` の最初または 1 つの値を選択する場合は `fn.head` を使用します。
- `ValueIterator.count` : 代わりに `fn.count` を使用してください。
- `ValueIterator.clone` : 不要になりました。同一の `Sequence` で複数回反復できます。

可能性のある混在環境用にコードを準備するために、以下のように安全なコーディングパターンを使用できます。

```
var list = xdm.arrayValues(...);
if (list instanceof Sequence) {
  ...ML9 idiom ...
} else {
  ...ML8 idiom ...
}
```

詳細については、『*JavaScript Reference Guide*』の「[Sequence](#)」および『*MarkLogic Server-Side JavaScript Function Reference*』の「[Sequence](#)」を参照してください。

21.6.3 カスタム UDF

UDF のインターフェイスが変更されたため、プラグインは混在クラスタで動作しません。異なる 2 つのリリースの異なる 2 つの定義セットに対して同一のコードをコンパイルできません。UDF ライブラリを MarkLogic 9 向けに再コンパイルおよび再導入する必要があります。

21.6.4 円を含むリバースクエリ

MarkLogic 9 では、円の半径を格納する単位がマイルからキロメートルに変更されています。9.0-1 と 9.0-2 のノードから構成される混合クラスタで動作させる場合、円を含むリバースクエリで予期しない結果が生じる可能性があります。MarkLogic 8.0-x からアップグレードすると、そうした問題は起こりません。

21.7 その他のアップグレードオプション

パッチの適用やホストのアップグレードの場合は、ローリングアップグレードの代替策があります。クラスタ内のホストに対するアップグレードを極めて最低限のダウンタイムで実行できます。詳細については、『*Installation Guide*』の「[Upgrading from Previous Releases](#)」を参照してください。

22.0 ホスト

ホストとは、MarkLogic サーバーのインスタンスです。ホストは個別に設定できず、グループのメンバーとして設定します。インストール時に何らかのグループに参加しない場合、ホストは「デフォルト」グループに追加されます。例えば、MarkLogic がシングルホスト環境で実行されている場合、ホストは「デフォルト」グループに追加されます。

フォレストはホスト上に作成されてデータベースに追加され、同じまたは異なるホスト上で実行している HTTP、ODBC、および XDBC サーバーとやり取りします。

ホストとグループおよびデータベースとの関係性の詳細については、「グループ」(40 ページ) および「データベース」(106 ページ) を参照してください。

ホストは、[Group] および [Hosts] 設定画面から管理します。ホストを管理するには、以下の手順を実行します。

- [クラスタへのホストの追加](#)
- [ホストのグループ変更](#)
- [ホストのシャットダウンまたは再起動](#)
- [ホスト上のフォレストのクリア](#)
- [ホスト上のフォレストの削除](#)
- [クラスタからの切り離し](#)
- [ホストのライセンスキーの変更](#)
- [トランザクションのロールバック](#)

この章では、管理画面を使用してホストを管理する方法について説明します。ホストをプログラムによって管理する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Host Maintenance Operations](#)」を参照してください。

22.1 クラスタへのホストの追加

これは、マルチホストクラスタにのみ適用されます。MarkLogic をインストールする方法、およびクラスタへの参加手順の詳細については、『*Installation Guide*』を参照してください。

ホストをクラスタに追加するには、管理画面で次の手順を実行します。

1. MarkLogic サーバーがインストールされていない場合は、ホストにインストールします。
2. MarkLogic サーバーを起動します。
3. クラスタに追加するホストで管理画面にアクセスし、使用許諾書に同意します。

4. サーバーが再起動すると、クラスタに参加するように要求するプロンプトが表示されます。

Join a Cluster

Now that MarkLogic Server is installed on this host, you can join an existing cluster. In order to do so, enter the host name of one of the cluster's hosts and provide the port number of that host's administration interface.

Press skip if you do not wish to join a cluster.

Host Name
One of the target cluster's hosts
Required.

Admin Port
Port for admin interface on server
Required.

5. クラスタ内のいずれかのマシンの DNS 名または IP アドレスを入力します。例えば、これがインストールする 2 番目のホストである場合、インストールされている最初のホストの DNS 名を入力します。
6. 管理者のユーザー名とパスワードを入力するように要求されます。クラスタで使用されるセキュリティデータベースの管理者ユーザー名およびパスワードを入力します。[ok] をクリックします。
7. このホストを割り当てるグループを選択します。[ok] をクリックします。
8. [ok] をクリックして、このクラスタへの参加を確定します。
9. クラスタに参加したことを示す確認メッセージで [ok] をクリックします。

22.2 ホストのグループ変更

ホストが属するグループを変更するには、管理画面を使用して次の手順を実行します。

1. 左側のツリーメニューで [Hosts] アイコンをクリックします。
2. ツリーメニューまたは [Summary] タブで、変更するホストの名前をクリックします。
3. [Group] ドロップダウンメニューで、使用可能なグループから選択します。
4. [ok] をクリックして変更を確定します。

ホストが属するグループの変更は「コールド」タスクです。変更を反映するために、サーバーが再起動します。

22.3 ホストのシャットダウンまたは再起動

ホストをシャットダウンまたは再起動するには、次の手順を実行します。

1. 左側のツリーメニューで [Hosts] アイコンをクリックします。
2. ツリーメニューまたは [Summary] タブで、シャットダウンまたは再起動するホストの名前をクリックします。
3. 右上の [Status] タブをクリックします。
4. [shutdown] または [restart] ボタンを適宜クリックします。
5. [ok to confirm] をクリックして、シャットダウンまたは再起動操作を確定します。

注： 再起動操作は、通常は数秒以内に完了します。ただし、状況によっては時間がかかることがあります（例えば、セキュリティデータベースで復旧を実行する必要がある場合や、クラスタ内のホスト間接続が遅い場合）。MarkLogic サーバーの再起動に数秒以上かかる場合は、管理画面に「503: Service Unavailable」メッセージが表示されることがあります。このような状況が発生した場合は、数秒待ってから管理画面を再読み込みしてください。

22.4 ホスト上のフォレストのクリア

ホスト上のフォレストをクリアすると、そのフォレスト内のデータが恒久的に削除されます。フォレストの設定情報は保持されます。例えば、新しいデータを同じ設定に読み込む場合にフォレストのクリアが必要になることがあります。

フォレストからデータをクリアするには、管理画面で次の手順を実行します。

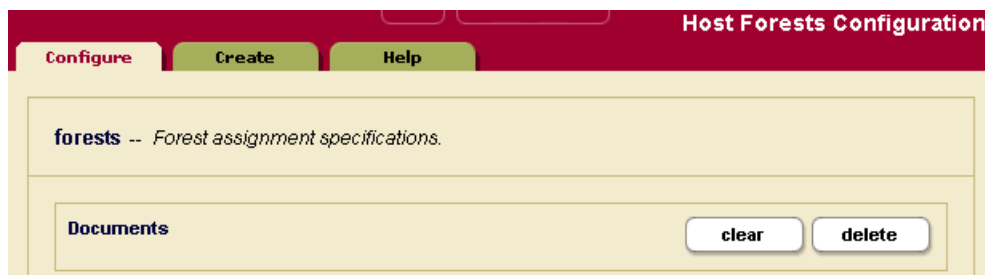
1. 左側のツリーメニューで [Hosts] アイコンをクリックします。
2. ツリーメニューまたは [Summary] タブで、クリアするフォレストが含まれているホストの名前をクリックします。
3. 選択したホストの [Forests] アイコンをクリックします。
4. クリアするフォレストに対応する [clear] ボタンをクリックします。
5. [ok] をクリックして、フォレストからデータのクリアを確定します。

22.5 ホスト上のフォレストの削除

ホスト上のフォレストを削除すると、そのフォレスト内のデータと設定情報が恒久的に削除されます。データベースにアタッチされているフォレストは削除できません。フォレストをホストから削除する前に、データベースからデタッチする必要があります。

フォレストがいずれのデータベースにもアタッチされていない場合は、次の手順を実行してフォレストをホストから削除します。

1. 左側のツリーメニューで [Hosts] アイコンをクリックします。
2. ツリーメニューまたは [Summary] タブで、削除するフォレストが含まれているホストの名前をクリックします。
3. 選択したホストの [Forests] アイコンをクリックします。
4. 削除するフォレストに対応する [delete] ボタンをクリックします。
5. [ok] をクリックして、ホストからのフォレストの削除を確定します。



6. [delete] ボタンをクリックします。
7. [ok] をクリックして、ホストからドロップすることを確定します。

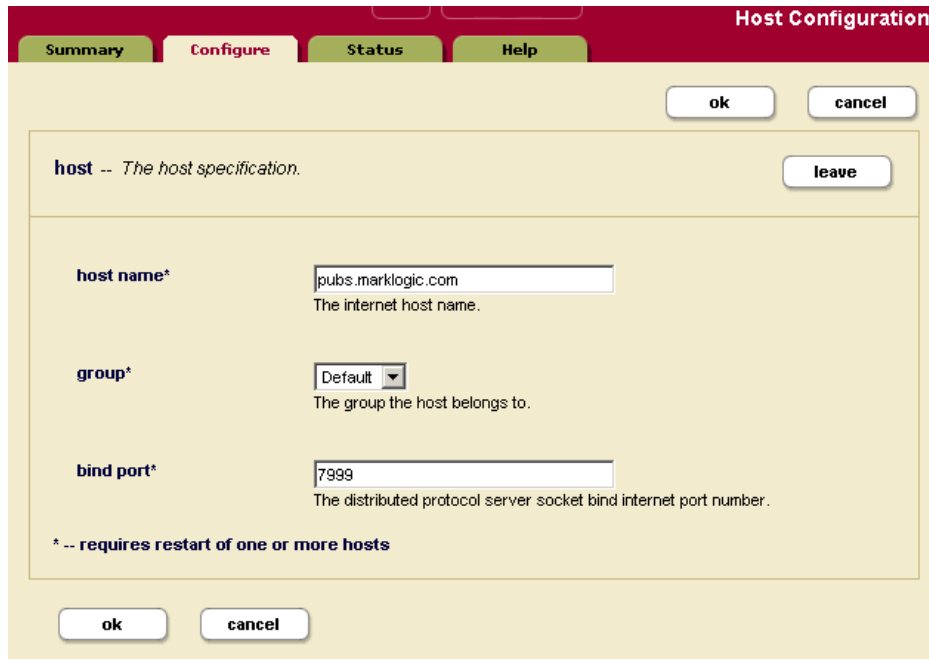
ホストの削除は、グループ内の他のホストに対する「ホット」管理タスクです。

22.6 クラスタからの切り離し

ホストを別のクラスタに移動するには、先にクラスタから切り離す必要があります。クラスタから切り離すことで、シングルホスト環境とマルチホスト環境の間でホストを切り替えることも可能です。ホストにフォレストがまだ割り当てられている場合や、何らかの外部クラスタが関連付けられている場合は、このホストをクラスタから切り離すことはできません。ホストをクラスタから切り離すには、ホストに割り当てられているすべてのフォレストを削除して、このホストに関連付けられているあらゆるクラスタから切り離しておく必要があります。シングルホスト環境では、フォレストが常にホストに割り当てられている状態になるため、ホストを切り離すことはできません。

ホストをクラスタから切り離すには、次の手順を実行します。

1. クラスタ内のいずれかのホストから管理画面にアクセスします。
2. 左側のツリーメニューで [Hosts] アイコンをクリックします。
3. クラスタから切り離すホストの名前をクリックします。ホスト設定画面が表示されます。



The image shows a 'Host Configuration' dialog box with a red header and four tabs: 'Summary', 'Configure', 'Status', and 'Help'. The 'Configure' tab is active. The dialog contains the following fields and controls:

- Buttons: 'ok' and 'cancel' at the top right, and 'leave' on the right side of the main content area.
- Text: 'host -- The host specification.'
- Field 'host name*': Contains 'pubs.marklogic.com'. Below it is the text 'The internet host name.'
- Field 'group*': A dropdown menu showing 'Default'. Below it is the text 'The group the host belongs to.'
- Field 'bind port*': Contains '7999'. Below it is the text 'The distributed protocol server socket bind internet port number.'
- Footnote: '* -- requires restart of one or more hosts'
- Buttons: 'ok' and 'cancel' at the bottom left.

4. [leave] ボタンをクリックします。
5. [ok] をクリックして、クラスタから切り離すことを確認します。
6. ホストが再起動し、新しい設定が読み込まれます。
7. [ok] をクリックして、初期状態のデータベースおよびアプリケーションサーバーをセルフインストールします。
8. クラスタへの参加が求められます。
9. 別のクラスタに参加するには、そのクラスタ内にあるいずれかのホストの名前を入力し、[ok] をクリックします。それ以外の場合は、[skip] をクリックします。
10. 必要に応じて、管理者のユーザー名およびパスワードをセットアップします。
11. 必要に応じて、管理ユーザー名およびパスワードでログインします。

管理画面が表示されます。

22.7 ホストのライセンスキーの変更

ホストのライセンスキーは、いつでも [Host Status] ページから変更できます。ライセンスキーの変更が必要なのは、以下の場合です。ライセンスキーが期限切れになった場合、既存ライセンスで使用できない機能が必要な場合、より多くの CPU やコアを搭載するハードウェアにアップグレードする場合、より大きなデータベースを使用できるライセンスが必要な場合、別の言語が必要な場合などです。ライセンスキーを変更すると、MarkLogic が自動的に再起動される場合があります（例えば、新しい言語が有効になる場合）。

ホストのライセンスキーを変更するには、管理画面を使用して次の手順を実行します。

1. 左側のツリーメニューで [Hosts] アイコンをクリックします。
2. ツリーメニューまたは [Summary] タブで、ライセンスキーを変更するホストの名前をクリックします。[Host Configuration] ページが表示されます。
3. [Status] タブをクリックします。[Host Status] ページが表示されます。
4. [license key] ボタンをクリックします。[License Key Entry] ページが表示されます。
5. 新しいライセンスキーの情報を入力します。MarkLogic サーバーのライセンスについては、MarkLogic の営業担当者にお問い合わせください。
6. [Licensee] および [License Key] フィールドに入力したら、[ok] をクリックします。必要に応じて MarkLogic が自動的に再起動し、新しいライセンスキーが有効になります。

22.8 トランザクションのロールバック

停止したトランザクションや長時間実行しているトランザクションをロールバックして、そのトランザクションで加えられた更新をすべて破棄するには、管理画面の [Host Status] ページを使用します。[Host Status] ページには、開始して未完了であるトランザクションのリストが表示されます。

注： 準備済みの XA トランザクションの MarkLogic サーバー部分をロールバックするには、「準備された XA トランザクションブランチのロールバック」(306 ページ) を参照してください。

管理画面を使用してトランザクションをロールバックするには、次の手順を実行します。

1. ブラウザで <http://yourhost:8001> に移動して、管理画面を開きます。
2. 左側のツリーメニューで [Hosts] をクリックします。ツリーが展開して、使用可能なホストが表示されます。

3. 左側のツリーメニューで対象となるホストの名前をクリックします。ホストの設定ビューが表示されます。
4. ページ上部にある [Status] タブをクリックします。ホストのステータスビューが表示されます。
5. トランザクションリストで、対象となるトランザクションを見つけます。ステータスページにトランザクションリストが表示されない場合は、このホストに未完了のトランザクションがありません。
6. トランザクションの横にある [rollback] をクリックして、トランザクションのロールバックを開始します。例えば次のようになります。

Transaction ID	Decision State (Coordinator)	Coordinator	Other Forests
5670604965531323769	prepare	samples-1	[rollback]

確認ダイアログが表示されます。

7. [ok] をクリックしてロールバックを確定します。[Host Status] ページが表示されます。

ロールバックが開始するタイミングとトランザクションが終了するタイミングには、若干の遅延が生じることがあります。この間トランザクションは [Host Status] ページに表示され続けますが、トランザクションステータスは「awaiting rollback」になります。

23.0 フォレスト

ここでは、MarkLogic サーバーのフォレストについて説明します。以下のセクションから構成されています。

- [フォレストについて](#)
- [フォレストの作成](#)
- [フォレストを delete-only にする](#)
- [フォレストを read-only にする](#)
- [\[Forest Summary\] ページを使用したフォレストのアタッチおよびデタッチ](#)
- [フォレストのバックアップ](#)
- [フォレストのリストア](#)
- [特定時刻へのフォレストのロールバック](#)
- [フォレストのマージ](#)
- [フォレストのクリア](#)
- [フォレストの無効化](#)
- [ホストからのフォレストの削除](#)
- [準備された XA トランザクションブランチのロールバック](#)

この章では、管理画面を使用してフォレストを管理する方法について説明します。フォレストをプログラムによって管理する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring Forests and Databases](#)」と「[Database Maintenance Operations](#)」を参照してください。

23.1 フォレストについて

フォレストは、XML、JSON、テキスト、またはバイナリのドキュメントの集合です。フォレストはホスト上で作成され、データベースにアタッチされ、クエリ対象の一体化されたコンテンツセットとして見なされます。フォレストは同時に1つのデータベースにのみアタッチできます。データベースにアタッチされていないフォレストには、データを読み込めません。

フォレストには、「スタンド」と呼ばれるインメモリおよびオンディスク構造が含まれます。各スタンドは XML、JSON、バイナリ、テキストのフラグメントで構成されます。また各フラグメントに関連するインデックス情報も含まれます。フラグメンテーションルールが適用されている場合、XML ドキュメントは、複数のスタンドにまたがる場合があります。MarkLogic サーバーは定期的に、複数のスタンドを単一のスタンドに「マージ」してパフォーマンスを最適化しています。マージの詳細については、「データベースのマージの概要と制御」（162 ページ）を参照してください。

フォレストには、ラージバイナリドキュメントなどの大型オブジェクトを格納するための個別のオンディスクラージデータディレクトリも含まれます。MarkLogic サーバーは、ラージオブジェクトを別途格納して、メモリ使用量、ディスク使用量、およびマージ時間を最適化します。スモールオブジェクトは、フラグメントとして直接スタンドに格納されます。ラージオブジェクトは、小さなリファレンスフラグメントがスタンドに格納され、完全なコンテンツはラージデータディレクトリに格納されます。ラージオブジェクトストア内にオブジェクトを格納するためのサイズしきい値と、ラージオブジェクトストアの場所は、管理画面と Admin API から設定できます。詳細については、『*Application Developer's Guide*』の「[Working With Binary Documents](#)」を参照してください。

フォレスト上でデフォルトで許可されている操作は、読み取り、挿入、更新、および削除です。次の更新タイプを設定することにより、フォレスト上で許可される操作を制御できます。

更新タイプ	説明
All	読み取り、挿入、更新、および削除の操作がフォレストで許可されます。
delete-only	読み取りと削除の操作がフォレストで許可されますが、挿入と更新の操作はフォレスト ID が指定されない限り許可されません。この場合、ドキュメントは別のフォレストに移動されます。フォレスト ID を指定しない場合、delete-only フォレストでドキュメントを更新すると、例外がスローされます。この更新タイプは、マージ操作で生じたオーバーヘッドを解消しながら、トランザクションでフォレストからデータを削除できるようにする場合に役立ちます。詳細については、「フォレストを delete-only にする」(295 ページ) を参照してください。
read-only ([Configure] でのみ設定可能)	フォレストで読み取り操作は許可されますが、挿入、更新、および削除の操作は許可されません。トランザクションでフォレスト内のフラグメントに変更を加えようとする、例外がスローされます。フォレストを読み取り専用メディアに置いてクエリ対象にする場合に、この更新タイプが役立ちます。詳細については、「フォレストを read-only にする」(296 ページ) を参照してください。
flash-backup ([Configure] で のみ設定可能)	このタイプはフォレストを read-only モードにしますが、挿入、更新、または削除のトランザクションで例外はスローされず、トランザクションを再試行できるようにします。この更新タイプは、フォレストのフラッシュバックアップを行うときに、一時的にフォレストを停止させたり、フォレストデータへの変更を無効にしたりする場合に役立ちます。詳細については、「フォレストを read-only にする」(296 ページ) を参照してください。

注： データベース全体を読み取り専用にするには、データベース内のすべてのフォレストを read-only にします。

23.2 フォレストの作成

新しいフォレストを作成するには、次の手順に従います。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. 右上の [Create] タブをクリックします。[Create Forest] ページが表示されます。

Summary Create Help

ok cancel

Create New Forests

forest -- The forest assignment specification.

forest name
The forest name.
Required. You must supply a value for forest-name.

host
The primary host to which the forest is assigned.

data directory
The optional public directory for forests.

large data directory
The optional directory for large objects in a forest.

fast data directory
The optional smaller but faster directory for forests.

updates allowed
The kinds of updates that should be allowed for this forest.

availability
Availability of the forest data.

rebalancer enable true false
Enable automatic rebalancing after configuration changes.

failover enable true false
Enable assignment to a failover host if the primary host is down.

failover hosts -- A list of failover hosts for shared-disk failover.

Failover Host Name

[add]

forest replicas -- A list of replica forests, used for local-disk failover.

database replication -- Database replication configuration.

3. [forest name] テキストボックスにフォレストの名前を入力します。フォレスト名は一意的である必要があります。
4. フォレストを作成するホストを選択します。

5. データディレクトリのパスを入力します。この場所にフォレストのデータが格納されます。このディレクトリはホストのファイルシステム上に存在し、使用するデータの格納に十分な容量が必要です。

フォレスト名はシステムによってディレクトリ名として扱われます。このため、フォレスト名はディレクトリ名として適切である必要があります。`* ? / : < > | "` の記号は使用できません。また、名前の最初にピリオド (.) や空白を使うことはできません。データディレクトリを指定する場合は、絶対パスを使用することをお勧めします。このようにデータディレクトリの絶対パスを指定しなかった場合、フォレストはデフォルトのデータディレクトリ内に作成されます。

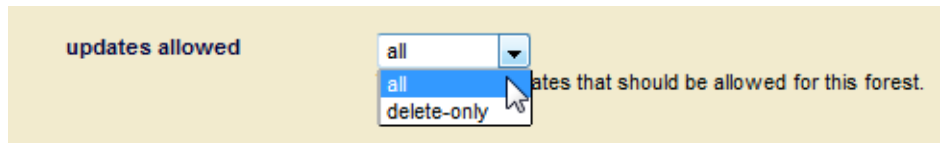
指定したディレクトリは、オペレーティングシステムにマウントされたディレクトリパスでも、HDFS パスでも、S3 パスでもかまいません。MarkLogic での HDFS および S3 ストレージの使用の詳細については、『*Query Performance and Tuning Guide*』の「[Disk Storage Considerations](#)」を参照してください。

フォレストディレクトリは完全修飾パス名（絶対パス名）、または MarkLogic サーバーがインストールされているディレクトリに基づいてインストール時に設定された Forests ディレクトリへの相対パスのいずれかです。次の表は、プラットフォームごとにデフォルトのフォレストディレクトリの場所を示したものです。

プラットフォーム	プログラムディレクトリ
Microsoft Windows	C:\Program Files\MarkLogic\Data\Forests
Red Hat Linux	/var/opt/MarkLogic/Forests
Mac OS X	~/Library/Application Support/MarkLogic/Data/Forests または ~/Library/"Application Support"/MarkLogic/Data/Forests または "~/Library/Application Support/MarkLogic/Data/Forests"

6. ラージオブジェクト（ラージバイナリドキュメントなど）の格納先に別のディレクトリを指定する場合は、ラージデータディレクトリを指定してください。ラージデータディレクトリを指定しない場合は、データディレクトリが使用されます。バイナリファイルのサポートの詳細については、『*Application Developer's Guide*』の「[Working With Binary Documents](#)」を参照してください。
7. 高パフォーマンスディレクトリを指定して、ジャーナルと、この高パフォーマンスディレクトリに収まるだけのフォレストデータを格納する場合は、高速データディレクトリを指定してください。ディスクと高速データディレクトリの詳細については、『*Query Performance and Tuning Guide*』の「[Disk Storage Considerations](#)」を参照してください。

8. フィールドで許可される更新のタイプを制限する場合は、このフォレストに許可する更新の種類を [updates allowed] フィールドで選択します。詳細については、「フォレストを delete-only にする」(295 ページ) を参照してください。



注： 「フォレストを read-only にする」(296 ページ) で説明している Read-Only 更新タイプは、既存のフォレストの [Configure] ページで設定できます。

9. [availability] フィールドで、[online] を選択してフォレストデータを階層型ストレージで使用可能にするか、[offline] を選択してデータを使用できないようにします。階層型ストレージの詳細については、「階層型ストレージ」(196 ページ) を参照してください。
10. [rebalancer enable] フィールドで、このフォレストのアタッチ先のデータベースのリバランサープロセスにこのフォレストを参加させるかどうかを指定します。データベースリバランサーの詳細については、「データベースのリバランス」(178 ページ) を参照してください。
11. ドキュメント割り当てポリシーをレンジにしてデータベースリバランサーを有効にしている場合は、このフォレストのレンジを [range] フィールドで指定してください。レンジポリシーの詳細については、「レンジ割り当てポリシー」(182 ページ) を参照してください。
12. [failover enable] フィールドで、プライマリホストが停止したときにこのフォレストを別のホストにフェイルオーバーするかどうかを指定します。フォレストでのフェイルオーバーの設定の詳細については、『*Scalability, Availability, and Failover Guide*』の「[Configuring Shared-Disk Failover for a Forest](#)」を参照してください。
13. [Failover Host Name] ドロップダウンメニューでフェイルオーバーホストを選択します。

14. [ok] をクリックします。

フォレストの作成は「ホット」管理タスクなので変更はすぐに有効になります。ただし、更新タイプを切り替えるとフォレストは再起動します。

23.3 フォレストを delete-only にする

フォレストは、読み取りおよび削除操作だけを許可するように設定できます。この場合、フォレストに格納されたすべてのドキュメントに対する挿入および更新は許可されません。delete-only フォレストは、データベース内に複数のフォレストがあり、変更されるフォレストを管理する場合に役立ちます。削除操作だけを許可する（挿入と更新を許可しない）ようにフォレストを設定するには、フォレストの設定ページに移動して [updates allowed] フィールドを [delete-only] に設定します。

フォレストを delete-only に設定した場合、フォレスト ID を指定しないで delete-only フォレスト内のドキュメントを更新すると、例外がスローされます。データベース内の他のフォレストの 1 つあるいは複数のフォレスト ID を指定して delete-only フォレスト内のドキュメントを更新すると、ドキュメントはそれらの他のフォレストのいずれかに移動します。ドキュメントがフォレストを移動すると、古いバージョンのドキュメントには削除マークが付けられ、次のマージ中にフォレストから削除されます。

delete-only フォレスト内のドキュメントが更新可能なフォレストに移動するように更新を指定するには、更新が許可されている少なくとも 1 つのフォレストのフォレスト ID を指定する必要があります。これを行うテクニックの 1 つが、次の `xdmp:document-insert` の例のように、常にすべてのフォレスト ID を指定するというものです。この場合、`$forest-ids` パラメータに対して、データベース内のすべてのフォレストがリストされます。

```
xdmp:document-insert($uri, $node, (), (), 0,
  xdmp:database-forests(xdmp:database()) )
```

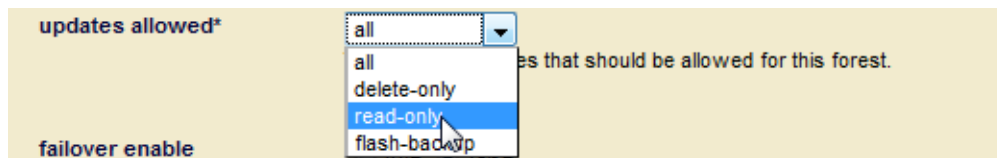
注： delete-only フォレストから更新を許可しているフォレストヘドキュメントを移動するには、複数のフォレスト ID を取る API を使用して、更新を許可するフォレストが 1 つ以上含まれるようにこれらのフォレスト ID を明示的に設定する必要があります。ノードレベルの更新ビルトイン関数（`xdmp:node-replace`、`xdmp:node-insert-child` など）にはフォレスト ID パラメータがないため、ドキュメントの移動はサポートされません。

通常の運用環境では、フォレストを delete-only に設定する必要はほとんどありません。また、データベースレベルで再インデックス付けがオンになっていても、delete-only に設定されたフォレストのドキュメントは再インデックス付けされません。

ただし、delete-only フォレストが役立つ場合があります。delete-only フォレストの使用例として、複数のフォレストがあり、いくつかのフォレストをマージするタイミングを制御する場合があります。フォレスト内でマージを制御する最善の方法は、フォレストに新しいコンテンツを挿入しないことです。このシナリオでは、一部のフォレストを delete-only に設定できます。この場合、設定している間はこれらのフォレストはマージしません (xdmp:merge API を使用するか、管理画面で [merge] ボタンをクリックして手動でマージを指定しない限り)。しばらくしてから、delete-only であるフォレストを入れ替えられます。例えば、4つのフォレストがある場合、1日の間それらのうちの2つを delete-only にして、次の日に残りの2つを delete-only にし、最初の2つのフォレストを更新可能に戻すことができます。このアプローチは、一度に更新される（および定期的にマージする）フォレストが2つだけになり、マージに必要なディスク領域を抑えられます。マージの詳細については、「データベースのマージの概要と制御」（162 ページ）を参照してください。

23.4 フォレストを read-only にする

既存のフォレストを、そこに格納されたすべてのドキュメントに対する読み取りだけを許可し、挿入、更新、および削除を許可しないように設定できます。



MarkLogic サーバーでは、次の2つの read-only フォレスト設定がサポートされています。

- `read-only` : この更新タイプを設定した場合、フォレストでの更新トランザクションが即座に停止します。
- `flash-backup` : この更新タイプを設定した場合、フォレストでの更新トランザクションは、更新タイプが再設定されるか、アプリケーションサーバーに設定されたデフォルトの時間制限に達するまで、再試行されます。

注 : `read-only` または `flash-backup` に設定できるのは既存のフォレストだけです。これらの設定で新しいフォレストは作成できません。

フォレストを読み取り専用メディアに置いてクエリ対象にする場合に、read-only フォレストは役立ちます。その他に `read-only` はディスク領域の制御に使用されます。例えば、マルチフォレストデータベースで、1つあるいは複数のフォレストがディスク容量の上限に達した場合、これらのフォレストに `read-only` のマークを付けると役立ちます。

`flash-backup` は、一部のファイルシステムで実行可能な非常に高速なバックアップである「フラッシュバックアップ」の操作中に、フォレストが更新されないようにする場合などに使用します。フラッシュバックアップの期間にフォレストを一時的に `read-only` モードにし、バックアップの完了時に更新タイプを再設定するように、`flash-backup` 更新タイプを設定できます。バックアップ期間中にフォレストに変更を加えようとするトランザクションは、再試行されます。

注： `read-only` または `flash-backup` と他のフォレスト更新タイプを切り替えると、フォレストの再起動がトリガーされます。このアクティビティはログファイルで確認できます。

`read-only` または `flash-backup` 更新タイプが設定されると、フォレストは以下の特徴を持つようになります。

- データベースに更新可能なフォレストが少なくとも 1 つあり、場所キーのない挿入、更新、または削除が要求された場合、データベースは更新可能なフォレストのいずれかを選択して操作を実行します。
- フォレストでのマージは許可されません。このようなフォレストを明示的にマージしようとしても何も起こりません。
- フォレストでは再インデックス付け / 再フラグメント化は許可されません。
- フォレストをアップグレードできません。アップグレードしようとするとエラーが返されます。
- フォレストを `read-only` または `flash-backup` に設定した場合、挿入、更新、または削除トランザクションは、例外を生成するか (`read-only` の場合)、後から再試行します (`flash-backup` の場合)。
- フォレストのクリア、リストア、完全な削除は行えません。ただし、「ホストからのフォレストの削除」(305 ページ) の説明に従って、フォレストの設定を削除できます。
- フォレストでのバックアップは許可されています。ただし、フォレストラベルにおける最終バックアップ時間は修正されません。結果として、フォレストの最終バックアップ時間は、フォレストが `read-only` または `flash-backup` ではなかったときにバックアップされた最後の時間が示されます。
- データベースインデックス設定が変更され、インデックス検出が「automatic」に設定されている場合、フォレストは機能しますが、インデックスは選択されません。インデックス検出を「none」に設定した場合、正しくない結果が得られません。
- `read-only` および `flash-backup` フォレストではフェイルオーバーをオンにできます。

23.5 [Forest Summary] ページを使用したフォレストのアタッチおよびデタッチ

[Forest Summary] ページには、クラスタ内のすべてのフォレストが一覧表示され、同時に各フォレストのステータス、プライマリホストであるホスト、空き容量などのさまざまな情報が表示されます。また、各フォレストがアタッチされているデータベースも示され、フォレストをデータベースにアタッチしたり、データベースからデタッチしたりできます。または、[Database Forest Configuration] ページを使用してフォレストをアタッチおよびデタッチできます（「データベースに対するフォレストのアタッチ/デタッチ」（124 ページ）を参照）。

1 つあるいは複数のフォレストをデータベースに対してアタッチまたはデタッチするには、管理画面を使用して次の手順を実行します。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。[Forest Summary] ページが表示されます。

Forest	Status	Database	Primary Host	Free Space	Data Dir
Documents	open	Documents	raymond.marklogic.com	13,703 MB	
elaine	open	elaine	raymond.marklogic.com	13,702 MB	
geo	open	geo	raymond.marklogic.com	13,702 MB	
maha	open		raymond.marklogic.com	13,702 MB	
Modules	open	Modules	raymond.marklogic.com	13,703 MB	
Schemas	open	Schemas	raymond.marklogic.com	13,702 MB	
Security	open	Security	raymond.marklogic.com	13,703 MB	
Triggers	open	Triggers	raymond.marklogic.com	13,702 MB	

2. データベース割り当てを変更する各フォレストに対して、新しいデータベース割り当ての名前を選択します。

注： あるデータベースから別のデータベースにデータベース割り当てを変更した場合、以前の設定からフォレストをデタッチし、新しい設定にアタッチすることになります。これが意図した操作であることを確認してください。また、あるデータベースからデタッチし、インデックス設定が異なる別のデータベースにアタッチする場合、[reindexer enable] が [true] に設定されていれば、フォレストは再インデックス付けを開始します。

3. 選択を行った後、[ok] をクリックして、フォレスト割り当ての変更を保存します。

アタッチまたはデタッチしたフォレストがデータベース設定に反映されます。データベースに対するフォレストのアタッチおよびデタッチは「ホット」管理タスクです。

23.6 フォレストのバックアップ

MarkLogic サーバーでは、指定したフォレストのイメージコピーをトランザクションで作成することにより、フォレストデータをバックアップします。フォレスト単位またはデータベース単位でデータをバックアップできます。フォレストのバックアップには管理画面を使用します。

フォレストレベルのバックアップでは、1つのフォレストのデータだけをバックアップするため、一貫性のあるデータベースの状態を保ったリストアは保証されません。1つのフォレスト内のデータは一貫していますが、データベースの他の部分（他のフォレスト、スキーマデータベースなど）はデータをリストアしたときに異なっている場合があります。バックアップの一貫性を保証するには、データベースのフルバックアップを実行してください。データベースのバックアップの詳細については、「データベースのバックアップおよびリストア」（235 ページ）を参照してください。

注： フォレストのバックアップにはジャーナルアーカイブ機能は備わっていません（「データベースのバックアップおよびリストア」（235 ページ）のデータベースバックアップの説明を参照）。ただし、フォレストバックアップ中に `xdmp:start-journal-archiving` 関数を手動で呼び出して、フォレストバックアップでジャーナルアーカイブを利用できます。

このセクションでは、フォレストバックアップ手順について説明します。以下のように構成されています。

- [フォレストのバックアップ](#)
- [フォレストバックアップのスケジュール設定](#)

23.6.1 フォレストのバックアップ

管理画面を使用してフォレストバックアップを開始するには、次の手順に従います。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. バックアップするフォレストを決定します。
3. バックアップするフォレストの名前のアイコンをクリックします。

4. 右上の [Backup/Restore] タブをクリックします。[Forest Backup] 画面が表示されます。



5. フォレストのバックアップコピーを保存するディレクトリの名前を入力します。絶対パスを指定する必要があります。各ディレクトリは、フォレストごとに一意である必要があります。

警告 新しいバックアップを書き込む前に、このディレクトリ内のすべてのファイルが削除されます。複数世代のバックアップを保持するには、バックアップごとに異なるバックアップディレクトリを指定します。

6. [Backup] を選択します。
7. [ok] をクリックします。
8. 確認メッセージが表示されます。もう一度 [ok] をクリックしてバックアップを確定します。

これで、選択したフォレスト内のデータが指定したディレクトリにバックアップされます。データのバックアップは「ホット」管理タスクなので変更はすぐに有効になります。

警告 Windows プラットフォームでバックアップを実行する場合、バックアップが行われている間、フォレストまたはデータディレクトリ（またはそれらの中のサブディレクトリ）を開いているユーザーがいないことを確認してください。

23.6.2 フォレストバックアップのスケジュール設定

フォレストを定期的にバックアップするように、フォレストバックアップのスケジュールを設定できます。バックアップを毎日、毎週、または毎月行うようにスケジュールを設定することも、1 回限りのバックアップスケジュールを設定することも可能です。スケジュールを設定したバックアップは、必要な数だけ作成できます。スケジュール設定したバックアップを作成するには、管理画面を使用して次の手順を実行します。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. ツリーメニューまたは [Forest Summary] ページで、バックアップのスケジュールを設定するフォレストを選択します。[Forest Configuration] ページが表示されます。
3. フォレストのツリーメニューで [Scheduled Backup] リンクをクリックします。[Scheduled Backup Configuration] ページが表示されます。
4. [Scheduled Backup Configuration] ページでは、スケジュールが設定された既存のバックアップが不要になった場合、それらを削除できます。
5. [Create] タブをクリックします。[Create Scheduled Backups] ページが表示されます。

Schedule a Forest Backup

backup directory
The backup directory pathname.
Required. You must supply a value for backup-directory.

backup type minutely hourly daily weekly monthly once

backup period
How often this backup should run (every n months, weeks, days, hours or minutes).

days Monday Tuesday Wednesday Thursday Friday Saturday Sunday
The days on which this backup occurs.

backup start time
The starting time (in 24:00 notation).
Required. You must supply a value for backup-start-time.

6. バックアップディレクトリの絶対パスを入力します。バックアップディレクトリは、MarkLogic サーバープロセスの読み取り / 書き込みを可能にするパーミッションが必要です。

7. [backup type] で定期的か 1 回限りを選択します。
 - 分単位の場合、バックアップ間の分数を入力します。
 - 時間単位の場合、バックアップ間の時間数を入力します。[Backup Minute] 設定では、バックアップが開始する正時からの分数を設定します。[Backup Minute] 設定によって、間隔の時間が伸びることはありません。
 - 日単位の場合、バックアップ間の日数と時刻を入力します。
 - 週単位の場合、バックアップ間の週数を入力し、1 つあるいは複数の曜日のチェックボックスをオンにして、バックアップを開始する時刻を入力します。
 - [monthly] の場合は、バックアップ間の月数を入力し、日 (1 ~ 31) を選択し、バックアップが開始する時刻を入力します。
 - 1 回限りの場合、MM/DD/YYYY の表記でバックアップ開始日 (例えば、2009 年 7 月 29 日は 07/29/2009) を入力し、24:00 表記で時刻を入力します。
8. バックアップを開始する時刻を入力します。
9. [ok] をクリックしてスケジュールを設定したバックアップを作成します。

バックアップは、指定されたスケジュールに従って自動的に開始します。

23.7 フォレストのリストア

管理画面を使用して以前に作成したバックアップからフォレストをリストアできます。バックアップは、フォレストのレベルでのみリストアされます。

注： 以前のバックアップが正しく完了している限り、以前のバージョンで作成されたバックアップからバージョン 4.1 にフォレストをリストアできません。バックアップが正しく完了しなかった場合 (ジャーナルファイルが存在する)、以前のバージョンでフォレストをリストアしてから、バージョン 4.1 にアップグレードする必要があります。

以前に作成したバックアップからフォレストをリストアするには、次の手順に従います。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. リストアするフォレストを決定します。
3. バックアップするフォレストの名前のアイコンをクリックします。
4. 右上の [Backup/Restore] タブをクリックします。
5. フォレストのバックアップコピーを含むディレクトリの名前を入力します。
6. [Restore] を選択します。

7. [ok] をクリックします。

確認メッセージが表示されます。

8. このバックアップディレクトリからデータをリストアすることを確認し、[ok] をクリックします。

バックアップからのデータのリストアは「ホット」管理タスクなので変更はすぐに有効になります。

警告 Windows プラットフォームでリストアを実行する場合、リストアプロセスが実行している間、フォレストまたはデータディレクトリ（またはそれらの中のサブディレクトリ）を開いているユーザーがいないことを確認してください。

23.8 特定時刻へのフォレストのロールバック

`xdmp:forest-rollback` 関数を使用して、1つまたは複数のフォレストの状態を、指定したシステムタイムスタンプにロールバックできます。過去のタイムスタンプにフォレストをロールバックするには、まず、削除したフラグメントが指定したタイムスタンプ以降保持されるようにマージタイムスタンプを設定する必要があります。ロールバックを実行する手順など、フォレストのロールバックの詳細については、『*Application Developer's Guide*』の「[Rolling Back a Forest to a Particular Timestamp](#)」および『*MarkLogic XQuery and XSLT Function Reference*』の `xdmp:forest-rollback` API のドキュメントを参照してください。

23.9 フォレストのマージ

管理画面を使用してフォレストデータをマージできます。「データベースのマージの概要と制御」（162 ページ）で説明しているように、フォレストのマージはパフォーマンスを高め、MarkLogic サーバーにより定期的にバックグラウンドで自動的に行われます。[merge] ボタンを使用すると、このフォレストのデータを明示的にマージできます。

フォレストを明示的にマージするには、次の手順に従います。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. マージするフォレストを決定します。
3. ツリーメニューまたは [Summary] タブで、フォレスト名をクリックします。

[Forest Configuration] ページが表示されます。

4. [Forest Configuration] ページの [merge] ボタンをクリックします。

確認メッセージが表示されます。

5. フォレストデータをマージすることを確認し、[ok] をクリックします。

フォレスト内のデータのマージは「ホット」管理タスクなので変更はすぐに有効になります。

23.10 フォレストのクリア

管理画面を使用して、フォレストからドキュメントデータをクリアできます。フォレストをクリアすると、フォレストからすべてのフラグメントが削除されますが、その設定情報は削除されません。

フォレストからすべてのデータをクリアするには、次の手順に従います。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. クリアするフォレストを決定します。
3. ツリーメニューまたは [Summary] タブで、フォレスト名をクリックします。

[Forest Configuration] ページが表示されます。

4. [Forest Configuration] ページの [clear] ボタンをクリックします。

確認メッセージが表示されます。

5. このフォレストからドキュメントデータをクリアすることを確認し、[ok] をクリックします。

フォレスト内のデータのクリアは「ホット」管理タスクなので変更はすぐに有効になります。

23.11 フォレストの無効化

管理画面を使用してフォレストを無効にできます。フォレストを無効にすると、データベースからフォレストがマウント解除され、データベース内のすべてのフォレストに対するすべてのメモリキャッシュがクリアされます。データベースは、そのフォレストのいずれかが無効になっている間、どのクエリ操作にも利用できません。

フォレストを無効にしても、設定やドキュメントデータは削除されません。後から [enable] をクリックしてフォレストを再度有効にできます。

フォレストを無効するには、次の手順に従います。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. 無効にするフォレストを決定します。
3. ツリーメニューまたは [Summary] タブで、フォレスト名をクリックします。
[Forest Configuration] ページが表示されます。
4. [Forest Configuration] ページの [disable] ボタンをクリックします。
確認メッセージが表示されます。
5. フォレストを無効にすることを確認し、[disable] をクリックします。

23.12 ホストからのフォレストの削除

管理画面を使用してフォレストを削除できます。フォレストの削除には次の2つのレベルがあります。

- 設定のみ削除。これはフォレストの設定情報を削除しますが、ドキュメントデータは保持します。
- 完全削除。これは、フォレストのドキュメントデータと設定情報を完全に削除します。

注： データベースにアタッチされている場合は、フォレストは削除できません。また、read-only または flash-backup フォレストでは設定情報を削除できませんが、このようなフォレストに対して完全削除は実行できません。

フォレストを削除するには、次の手順に従います。

1. 左側のツリーメニューで [Forests] アイコンをクリックします。
2. 削除するフォレストを特定します。
3. ツリーメニューまたは [Summary] タブで、フォレスト名をクリックします。
[Forest Configuration] ページが表示されます。
4. [Forest Configuration] ページの [delete] ボタンをクリックします。
確認メッセージが表示されます。
5. [Configuration Only] を選択して設定情報だけを削除するか、[Full Delete] を選択して設定情報とドキュメントデータを削除します。

6. [ok] をクリックします。

フォレストの削除は「ホット」タスクなので変更はすぐに有効になります。

23.13 準備された XA トランザクションブランチのロールバック

MarkLogic サーバートランザクションは、グローバルな分散 XA トランザクションに参加できます。XA トランザクションマネージャは通常、MarkLogic サーバーから独立して、XA トランザクションに参加しているトランザクションのライフサイクルを管理します。ただし、長期間トランザクションマネージャにアクセスできない場合、グローバルトランザクションの MarkLogic サーバー部分（「ブランチ」と呼ばれます）を手動でロールバックする必要があります。詳細については、『*XCC Developer's Guide*』の「[Heuristically Completing a Stalled Transaction](#)」を参照してください。

注： ヒューリスティックな完了は、トランザクションマネージャと 2 フェーズコミットプロセスをバイパスするので、データ整合性の問題を招く可能性があります。ヒューリスティックな完了は最終手段としてのみ使用してください。

XA トランザクションの MarkLogic サーバートランザクションを準備する前に、トランザクションを評価するホストのホストステータスページからトランザクションをロールバックすることも可能です。「トランザクションのロールバック」（287 ページ）を参照してください。

XA トランザクションの MarkLogic サーバートランザクションが準備完了状態になると、トランザクションは、連携フォレストのフォレストステータスページにのみ表示されます。連携フォレストを見つけるには、参加しているデータベースに所属する各フォレストの [Forest Status] ページを調べます。トランザクションは、連携フォレストのステータスページにのみ表示されます。

管理画面を使用して、XA トランザクションの MarkLogic サーバー部分をヒューリスティックにロールバックするには、次の手順に従います。

1. ブラウザで <http://yourhost:8001> に移動して、管理画面を開きます。
2. 左側のツリーメニューで、[Forests] をクリックします。[Forest Summary] ページが表示されます。
3. 連携フォレストの名前をクリックします。[Forest Status] ページが表示されます。
4. トランザクションリストで目的のトランザクションを見つけます。ステータスページにトランザクションリストが表示されない場合は、このフォレストは準備完了トランザクションの連携フォレストではありません。

5. 目的のトランザクションのステータスの右側の `[rollback]` をクリックして、ロールバックを開始します。ロールバックの確認ダイアログが表示されます。例えば次のようになります。

Transaction ID	Name	State	Mode	Timestamp	Run Time	Limit	Source	User	
8169053886267504764		active	query	13183478465171180	740.8 ms	600 s	Security	admin	<code>[rollback]</code>
1189889101125869537		idle	update	0	2.7 s	600 s	samples	admin	<code>[rollback]</code>

6. `[ok]` をクリックしてロールバックを確定します。ロールバック完了ページが表示されます。
7. `[ok]` をクリックして、`[Forest Status]` ページに戻ります。

ロールバックしたトランザクションは、「remember abort」状態になります。この状態は、トランザクションマネージャがグローバルトランザクションを再同期するまで、ローカルトランザクションが中止されていたという情報を MarkLogic サーバーが保持していることを示しています。再同期が行われると、トランザクションはこれ以降、フォレストステータスに表示されません。詳細については、『*XCC Developer's Guide*』の「[Heuristically Completing a MarkLogic Server Transaction](#)」を参照してください。

`[Forest Status]` ページを使用して、MarkLogic サーバーがトランザクションマネージャを待機せずにロールバック情報を消去するように強制できます。これはエラーを招き、トランザクションマネージャがグローバルトランザクションを再同期しようとしたときにデータ整合性の損失が生じる可能性があるためにお勧めしません。ロールバック情報を消去する必要がある場合は、`[Forest Status]` のトランザクションリストの `[forget]` リンクを使用してください。

Transaction ID	Decision State (Coordinator)	Coordinator	Other Forests
5670604965531323769	<code>remember abort</code>	samples-1	<code>[forget]</code>

24.0 セキュリティ管理

MarkLogic サーバーでは、ロールベースのセキュリティモデルを使用します。ユーザーの権限とパーミッションは、ユーザーに割り当てられたロールに基づきます。MarkLogic サーバーにおけるセキュリティモデルを理解するためのバックグラウンド情報については、『*Security Guide*』を参照してください。ここでは、セキュリティに関連する管理について説明します。次のセクションで構成されます。

- [セキュリティエンティティ](#)
- [ユーザー](#)
- [ロール](#)
- [実行権限](#)
- [URI 権限](#)
- [Amp](#)
- [保護されているコレクション](#)
- [レルム](#)

この章では、管理画面を使用してセキュリティオブジェクトを管理する方法について説明します。セキュリティオブジェクトをプログラムによって管理する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Creating and Configuring Roles and Users](#)」と「[User Maintenance Operations](#)」を参照してください。

24.1 セキュリティエンティティ

MarkLogic サーバーのセキュリティモデルの主要エンティティは次のとおりです。

- ユーザー
モデル内の「ユーザー」は一連のロールを保有します。ユーザーは、与えられたロールに基づいて、システム内での権限とパーミッションを保持します。
- ロール
「ロール」はユーザーに権限とパーミッションを与えます。ロールは複数のロールから継承できます。ロールの継承は「is-a」関係です。したがって、継承されたロールは、その親の権限とパーミッションも保有します。
- 実行権限
「実行権限」は、保護されたアクションを実行する認可を付与します。実行権限で指定されたロール（およびその継承ロール）だけが、そのアクションを実行できます。
- URI 権限
「URI 権限」は、保護されたベース URI 内にドキュメントを作成する認可を付与します。URI 権限で指定されたロール（およびその継承ロール）だけが、保護されたベース URI 内でドキュメントを作成できます。

- パーミッション

「パーミッション」は、ドキュメントまたはコレクションを保護します。各パーミッションは、単一のロールを機能（読み取り、更新、挿入）に関連付けます。保護されたドキュメントまたはコレクションには、一連の関連付けられたパーミッションがあります。

- コレクション

「コレクション」は、関連した一連のドキュメントをグループ化したものです。1つのドキュメントは、任意の数のコレクションに所属できます。コレクションは、システム内のドキュメントが「そのコレクションの一部である」と明示した場合にシステムに存在することになります。ただし、関連付けられたコレクションオブジェクトは、保護されていない限り、「セキュリティ」データベースでは作成も格納もされません。

コレクションレベルで作成されたパーミッションは、コレクションに適用されますが、コレクション内のドキュメントには適用されません。ドキュメントをコレクションに追加したり、コレクションから削除したりするには、ユーザーはコレクションとドキュメントの両方のレベルでパーミッションを保有する必要があります。

- Amp

「Amp」は、ユーザーが特定のタスクを実行（関数を実行）しているときに、一時的にユーザーに追加ロールを与えます。

- 認証局

「認証局」(CA) は、ユーザー、データベース、管理者、クライアント、サーバーなどのエンティティのアイデンティティを認証する信頼済みサードパーティです。CA は、ブラウザとアプリケーションサーバー間で暗号化された保護を実現するために、SSL (Secure Sockets Layer) セキュリティ標準で使用されます。CA は、エンティティから認証が要求されると、そのエンティティのアイデンティティを検証し、CA のプライベートキーで署名された証明書を付与します。CA が信頼できる場合は、無効にならない限り、その CA が発行するすべての証明書が信頼されます。MarkLogic サーバーにおける SSL のサポートの詳細については、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

- 証明書テンプレート

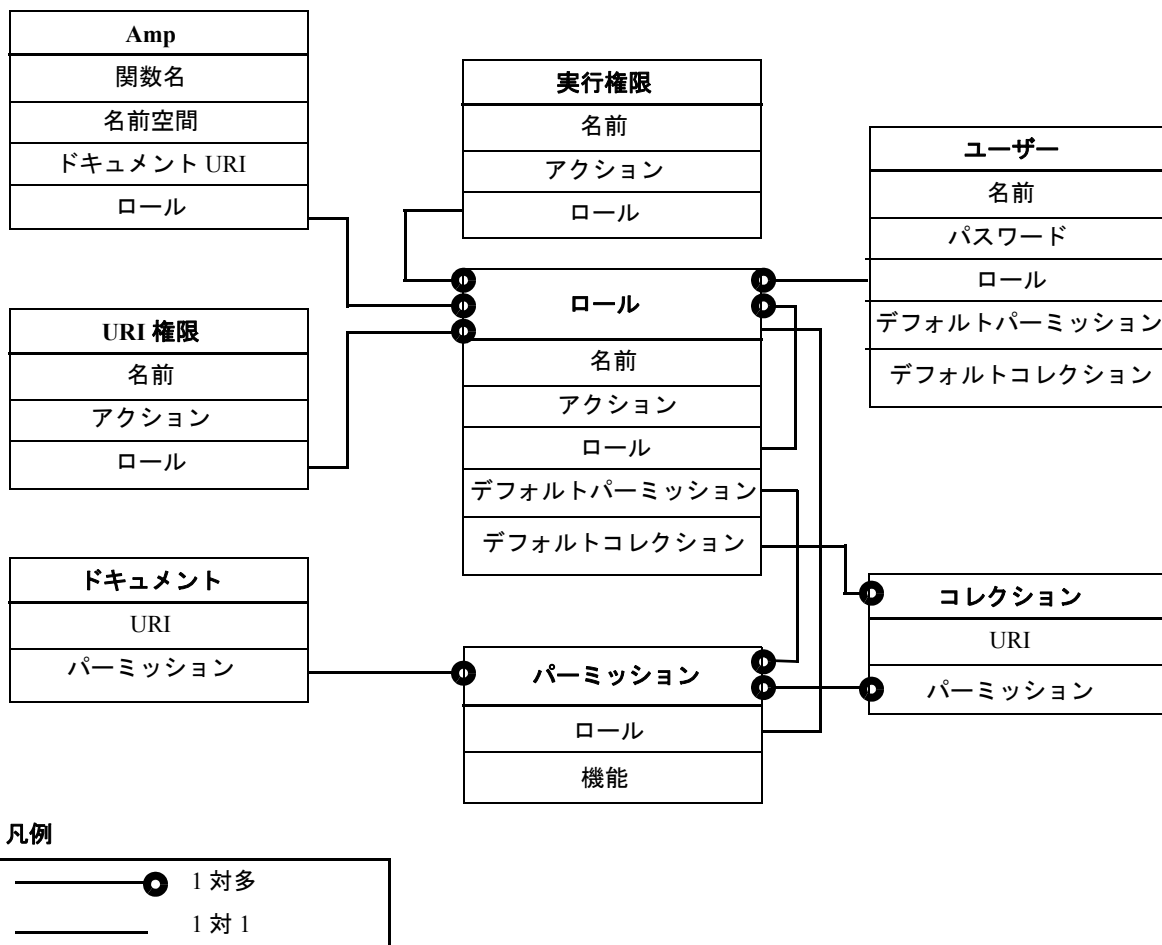
「証明書テンプレート」は、クラスタ内のさまざまなホストの証明書要求を生成するために使用される MarkLogic 構成物です。証明書テンプレートは、ブラウザとアプリケーションサーバー間で暗号化された保護を実現するために、SSL (Secure Sockets Layer) セキュリティ標準で使用されます。テンプレートは、証明書の名前、説明、証明書の所有者に関するアイデンティティ情報を定義します。MarkLogic サーバーにおける SSL のサポートの詳細については、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

- 外部認証

「外部認証設定オブジェクト」は、LDAP や Kerberos による外部認証に対して MarkLogic サーバーを設定するために使用されます。外部認証設定オブジェクトは、使用する認証プロトコルと認可スキーマの他、LDAP 認証に必要なその他のパラメータを指定します。MarkLogic サーバーにおける外部認証の詳細については、『*Security Guide*』の「[External Security](#)」の章を参照してください。

- セキュリティエンティティの関係性

次の図は、MarkLogic サーバーセキュリティモデル内のさまざまなエンティティ間の関係性を示したものです。



この章の以降のセクションでは、MarkLogic サーバーセキュリティエンティティを管理する手順について詳しく説明します。セキュリティ管理タスクはすべて「ホット」なので変更はサーバーを再起動せずにすぐに適用されます。

パーミッションは管理画面からは管理されないため、このドキュメントでは詳しく説明しません。MarkLogic サーバーにおけるパーミッションの使用の詳細については、『*MarkLogic XQuery and XSLT Function Reference*』を参照してください。

24.2 ユーザー

ユーザーには一連のロールが与えられます。ユーザーは、与えられたロールに基づいて、システム内での権限とパーミッションを保持します。ユーザーは、自身の権限に基づいてタスクを実行（関数を実行）し、自身のパーミッションに基づいてデータにアクセスできます。

それぞれのユーザーにはユーザー名とパスワードが関連付けられています。ユーザーはまた、デフォルトのコレクションも保有します。ユーザーがドキュメントを作成してもドキュメントを一連のコレクションに明示的に関連付けない場合は、そのドキュメントは自動的に、ユーザーのデフォルトのコレクションに追加されます。またユーザーのデフォルトのパーミッションを作成できます。ユーザーがドキュメントを作成してもドキュメントのパーミッションを明示的に設定しない場合は、ユーザーのデフォルトのパーミッションがそのドキュメントに与えられます。

HTTP、ODBC、または XDBC サーバーのセキュリティをオンにした場合、セキュリティデータベース内のすべてのユーザーがそのサーバーにアクセスできます。HTTP、ODBC、または XDBC サーバー上で実行している XQuery プログラム内の関数に対するよりきめ細かなセキュリティ制御は、`xdmp:security-assert()` をコード内で使用することにより実現されます。ドキュメントに対するきめ細かくセキュリティ制御されたアクセスは、保護されたそれぞれのドキュメントに関連付けられたパーミッションを使用することにより実現されます。

ユーザーの作成、管理、保守を行うには、次の手順を実行します。

- [ユーザーの作成](#)
- [ユーザー設定の表示](#)
- [ユーザー設定の修正](#)
- [ユーザーの削除](#)

24.2.1 ユーザーの作成

ユーザーを作成するには、次の手順に従います。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Users] アイコンをクリックします。

3. [Create] タブをクリックします。[User Configuration] ページが表示されます。

New User

user -- *A database user.*

user name
User/login name (unique)
Required. You must supply a value for user-name.

description
An object's description.

password
Encrypted Password.
Required.

confirm password
Encrypted Password.
Required.

external names -- *The external names specifications.*

external name

password extra -- *For storing extra information for password checking.*

roles -- *The roles assigned.*

Role	Compartment
<input type="checkbox"/> admin	
<input type="checkbox"/> admin-builtins	

4. [user name] フィールドにユーザーの名前を入力します。
5. ユーザーの説明を入力します（オプション）。
6. ユーザーのパスワードを入力します。

7. パスワードを再入力して確認します。
8. ユーザーが LDAP または Kerberos により外部で認証される場合、[external names] セクションで 1 つあるいは複数の識別名 (LDAP) かユーザープリンシパル (Kerberos) を入力する必要があります。外部認証の詳細については、『*Security Guide*』の「[External Security](#)」の章を参照してください。
9. [roles] セクションで、ユーザーに割り当てるロールのチェックボックスをオンにします。
10. このユーザーのデフォルトのパーミッションを作成します (オプション)。ロールを選択し、そのロールに適切な機能 (読み取り、挿入、更新) を組み合わせます。このユーザーに対してデフォルトのパーミッションを 4 つ以上追加する場合は、[ok] をクリックした後に次の画面で追加できます。
11. このユーザーのデフォルトのコレクションを作成します (オプション)。ユーザーのデフォルトのコレクションに追加するコレクションごとに、コレクション URI を入力します。このユーザーに対してデフォルトのコレクションを 4 つ以上追加する場合は、[ok] をクリックした後に次の画面で追加できます。
12. [ok] をクリックします。

これでユーザーがシステムに追加され、ユーザー設定ページが表示されます。デフォルトのパーミッションやコレクションをさらにユーザーに追加する場合は、デフォルトのパーミッションまたはコレクションのセクションまで下にスクロールします。

24.2.2 ユーザー設定の表示

ユーザーの設定を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Users] アイコンをクリックします。
3. ツリーメニューまたは [Summary] タブで、表示する設定を持つユーザーの名前を探します。

- 名前をクリックします。ユーザー設定ページが表示されます。ここでユーザーの設定を確認できます。

The screenshot shows a web interface for editing a user. The title is "User: testuser" with "ok" and "cancel" buttons. Below the title, it says "user -- A database user." with a "delete" button. The form contains four fields: "user name" with the value "testuser" and the label "User/login name (unique)"; "description" with the value "This is a test user" and the label "An object's description."; "password" with a masked value and the label "Encrypted Password."; and "confirm password" with a masked value and the label "Encrypted Password.".

24.2.3 ユーザー設定の修正

ユーザーの設定を修正するには、次の手順を実行します。

- 「ユーザー設定の表示」(313 ページ)の説明に従って、修正するユーザーの設定を表示します。
- ユーザーの設定に対して必要な修正を行います。修正では、ユーザーの資格情報(パスワードを含む)の変更、ロール割り当ての追加や削除、デフォルトのパーミッション設定の追加や削除、デフォルトのコレクション設定の追加や削除などを行います。

警告 ユーザー設定に変更を加えると、そのユーザーのアクセス制御ポリシーが影響を受けます。このためユーザーに認可される操作が増減する可能性があります。セキュリティシステムが機能する仕組みの詳細については、『*Security Guide*』を参照してください。

- [ok] をクリックして変更を保存します。

新しい変更内容は、ユーザーの変更がコミットされた後に開始するすべてのトランザクションで有効になります。

24.2.4 ユーザーの削除

セキュリティデータベースからユーザーを削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Users] アイコンをクリックします。
3. ツリーメニューまたは [Summary] タブで、削除するユーザーを探します。
4. ユーザー名をクリックします。
5. [delete] ボタンをクリックします。
6. [ok] をクリックして、ユーザーの削除を確定します。

ユーザーは、セキュリティデータベースから恒久的に削除されます。

24.3 ロール

MarkLogic サーバーはロールベースのセキュリティモデルを実装しています。したがって、ロールは、MarkLogic サーバーにおけるセキュリティの中心的概念になります。ロールは、システムで特定のアクションを実行するための権限（実行権限と URI 権限の両方）をユーザーに与えます。実行権限は、保護されたアクションの実行をユーザーに許可します。URI 権限は、保護された URI 下でのドキュメントの作成をユーザーに許可します。ロールはまた、保護されたドキュメントにアクセスするパーミッションもユーザーに与えます。

ロールは複数のロールから継承できます。ロールの継承関係は「is-a」関係です。したがって、ロールは、継承元のロールの権限とパーミッションを取得します。

MarkLogic サーバーのインストール時に、次のロールが事前定義されています。

ロール	説明
admin	このロールには、管理タスクの実行に必要な権限とパーミッションが含まれます。このロールのアクセス権は、システムで最高レベルのアクセス権です。
admin-builtins	このロールには、admin-builtins 関数の呼び出しに必要な権限が含まれます。
filesystem-access	このロールには、ファイルシステムにアクセスする権限が含まれます。
merge	このロールには、システムでマージを強制実行するために必要な権限が含まれます。
security	このロールには、セキュリティ関連のすべての管理機能を実行する権限が含まれます。

これらの事前定義されたロールは、その設定を変更したり（`admin` ロールは除く）、任意に削除したりできますが、慎重に進めることを強くお勧めします。

ロールにはデフォルトのコレクションが含まれます。あるロールのユーザーがドキュメントを作成してもドキュメントを一連のコレクションに明示的に関連付けない場合は、そのドキュメントは自動的に、一連のデフォルトのコレクションに追加されます。このデフォルトのコレクションセットは、ユーザーに対して定義されたデフォルトのコレクション、ユーザーに与えられているロール、およびユーザーが継承したロールの継承元のロールの和集合です。

ロールにはデフォルトのパーミッションが含まれます。あるロールのユーザーがドキュメントを作成してもドキュメントのパーミッションを明示的に設定しない場合は、そのドキュメントには一連のデフォルトのパーミッションが与えられます。このデフォルトのパーミッションセットは、ユーザーに対して定義されたデフォルトのパーミッション、ユーザーに与えられているロール、およびユーザーの直接割り当てられているロールの継承元のロールの集合です。

MarkLogic サーバーにおけるロールベースのセキュリティモデルの詳細については、『*Security Guide*』を参照してください。

ロールの作成、管理、保守を行うには、次の手順を実行します。

- [ロールの作成](#)
- [ロールの表示](#)
- [ロール設定の修正](#)
- [ロールの削除](#)

24.3.1 ロールの作成

ロールを作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Roles] アイコンをクリックします。

3. [Create] タブをクリックします。[Role Configuration] ページが表示されます。

Summary **Create** **Help**

New Role

ok cancel

role -- *A security role.*

role name
The Role name (unique)
Required. You must supply a value for role-name.

description
An object's description.

compartment
The compartment that this role is part of.

external names -- *The external names specifications.*

external name

more external names

roles -- *The roles assigned.*

Role	Compartment
<input type="checkbox"/> admin	
<input type="checkbox"/> admin-builtins	

4. [role name] フィールドにロールの名前を入力します。
5. ロールの説明を入力します（オプション）。
6. 名前付きコンパートメントにロールを配置する場合、[compartment] フィールドにコンパートメントの名前を入力します。ドキュメントに、コンパートメントを持つロールによるパーミッション（ロール / 機能の組み合わせ）が設定されている場合、ユーザーはいずれかの機能を実行するために、それぞれのコンパートメントでこれらのロールを保有する必要があります（どのパーミッションに含まれるかには関係ありません）。

7. ロールが LDAP グループにマッピングされる場合、[external names] セクションに 1 つあるいは複数のグループ名を入力します。外部認証の詳細については、『*Security Guide*』の「[External Security](#)」の章を参照してください。
8. [roles] セクションで、このロールが継承する元のロールを選択します。
9. [execute privileges] セクションで、ロールに関連付ける実行権限を選択します。
10. [URI privileges] セクションで、ロールに関連付ける URI 権限を選択します。
11. このロールのデフォルトのパーミッションを作成します（オプション）。ロールを選択し、そのロールに適切な機能（読み取り、挿入、更新）を組み合わせます。このロールに対してデフォルトのパーミッションを 4 つ以上追加する場合は、[ok] をクリックした後に次の画面で追加できます。
12. このロールのデフォルトのコレクションを作成します（オプション）。ロールのデフォルトのコレクションに追加するコレクションごとに、コレクション URI を入力します。このユーザーに対してデフォルトのパーミッションを 4 つ以上追加する場合は、[ok] をクリックした後に次の画面で追加できます。
13. [ok] をクリックします。

これでロールがシステムに追加され、[Role Configuration] ページが表示されます。デフォルトのパーミッションやコレクションをさらにロールに追加する場合は、デフォルトのパーミッションまたはコレクションのセクションまで下にスクロールします。

24.3.2 ロールの表示

ロールを作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Roles] アイコンをクリックします。

3. ツリーメニューまたは [Summary] タブで、表示するロールの名前をクリックします。[Role Configuration] ページが表示されます。

The screenshot shows the 'Role Configuration' page for a role named 'security'. The page has a navigation bar with tabs: Summary, Configure (selected), Describe, Create, and Help. Below the navigation bar, there is an 'Error:' message and a 'Role: security' header with 'ok' and 'cancel' buttons. The main content area is divided into several sections:

- role** -- A security role. (with a 'delete' button)
- role name**: security (The Role name (unique))
- description**: security role (An object's description.)
- compartment**: (The compartment that this role is part of.)
- external names** -- The external names specifications.
 - external name**: No Current External Name
 - [add] (with an input field)
 - more external names (button)
- roles** -- The roles assigned. (inherited roles in **Bold**)

Role	Compartment
<input type="checkbox"/> admin	
<input type="checkbox"/> admin-builtins	

ロールの設定を表示します。

24.3.3 ロール設定の修正

ロール設定を修正するには、次の手順を実行します。

1. 「ロールの表示」(318 ページ) の説明に従って、修正するロールの設定を表示します。
2. ロール設定に対して必要な修正を実行します。修正では、ロール割り当ての追加や削除、デフォルトのパーミッション設定の追加や削除、デフォルトのコレクション設定の追加や削除などを行います。

警告 ロール設定に変更を加えると、そのロールのアクセス制御ポリシーが影響を受けます。このためそのロールを（直接または間接的に）保有するすべてのユーザーに認可される操作が増減する可能性があります。セキュリティシステムが機能する仕組みの詳細については、『*Security Guide*』を参照してください。

3. [ok] をクリックして変更を保存します。

新しい変更内容は、ユーザーの変更がコミットされた後に開始するすべてのトランザクションで有効になります。

24.3.4 ロールの削除

セキュリティデータベースからロールを削除できます。システムでは、ロールを削除する前にそのロールを持つユーザーが存在するかどうかを確認されません。削除したロールは、そのロールに割り当てられているすべてのユーザーから自動的に削除されます。削除したロールに割り当てられていたユーザーは、そのロールにより付与されたパーミッションおよび権限を失います。

ロールを削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Roles] アイコンをクリックします。
3. ツリーメニューまたは [Summary] タブで、削除するロールの名前をクリックします。
4. [delete] ボタンをクリックします。
5. [ok] をクリックして、ロールの削除を確定します。

これでロールはセキュリティデータベースから削除されました。

24.4 実行権限

実行権限は、保護されたアクションを実行する認可を付与します。実行権限は、保護されたアクションと、そのアクションを実行できるロールを指定します。指定されたロールから継承したロールも、保護されたアクションを実行できます。保護されたアクションは、URI として表されます。

実行権限が作成されると、コード内で `xdmp:security-assert(<protected-action-uri>, "execute")` を使用することにより、XQuery プログラムで強制実行されます。つまり、`xdmp:security-assert(<protected-action-uri>, "execute")` は関数の開始箇所、または保護されているコードのセクションで追加できます。システムが、実行権限で指定された適切なロールを保有しないユーザーとして実行している場合、例外がスローされます。それ以外の場合、システムは `security-assert` 条件を満たし、保護されたコードの実行に進みます。

実行権限の作成、管理、保守を行うには、次の手順を実行します。

- [実行権限の作成](#)
- [実行権限の表示](#)
- [実行権限の修正](#)
- [実行権限の削除](#)

24.4.1 実行権限の作成

実行権限を作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Execute Privileges] アイコンをクリックします。

3. [Create] タブをクリックします。[Execute Privilege Configuration] ページが表示されます。

Execute Privilege Configuration

Summary Create Help

New Execute Privilege ok cancel

execute privilege -- Privilege representation.

privilege name
Privilege name (unique)
Required. You must supply a value for privilege-name.

action
A protected "action" (or object).
Required. You must supply a value for action.

roles -- The roles assigned.

admin

admin-builtins

4. 実行権限の名前を入力します。この実行権限で保護されるアクションを説明する名前を使用してください。例えば、`create-user` は、ロールにユーザー作成の認可を与える実行権限の名前です。
5. URI として表された、保護されたアクションを入力します。どのような URI でも使用できますが、組織内の命名規則に従うことをお勧めします。例えば、`create-user` 実行権限の URI は、`http://marklogic.com/xdmp/privileges/create-user` です。
6. [roles] セクションで、保護されたアクションの実行を許可されたロールを選択します。
7. [ok] をクリックします。

実行権限がセキュリティデータベースに追加されました。これで、コード内で `xdmp:security-assert()` 関数を使用して、保護された操作にこの権限を関連付けられます。

24.4.2 実行権限の表示

実行権限を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Execute Privileges] アイコンをクリックします。[Execute Privileges Summary] ページが表示されます。

Privilege	Action	Roles
amp-add-roles	http://marklogic.com/xdmp/privileges/amp-add-roles	security
amp-get-roles	http://marklogic.com/xdmp/privileges/amp-get-roles	security
amp-remove-roles	http://marklogic.com/xdmp/privileges/amp-remove-roles	security
amp-set-roles	http://marklogic.com/xdmp/privileges/amp-set-roles	security
any-collection	http://marklogic.com/xdmp/privileges/any-collection	security
any-uri	http://marklogic.com/xdmp/privileges/any-uri	security
collection-add-permissions	http://marklogic.com/xdmp/privileges/collection-add-permissions	security

3. 表示する実行権限の名前をクリックします。
4. 実行権限の設定が表示されます。

24.4.3 実行権限の修正

実行権限を修正するには、次の手順を実行します。

1. 「実行権限の表示」(323 ページ) の説明に従って、修正する権限の設定を表示します。
2. 権限に対して必要な修正を実行します (ロール割り当ての追加や削除など)。

警告 実行権限設定に変更を加えると、その権限のアクセス制御ポリシーが影響を受けます。このため割り当てられたいずれかのロールを (直接または間接的に) 保有するすべてのユーザーに認可される操作が増減する可能性があります。セキュリティシステムが機能する仕組みの詳細については、『*Security Guide*』を参照してください。

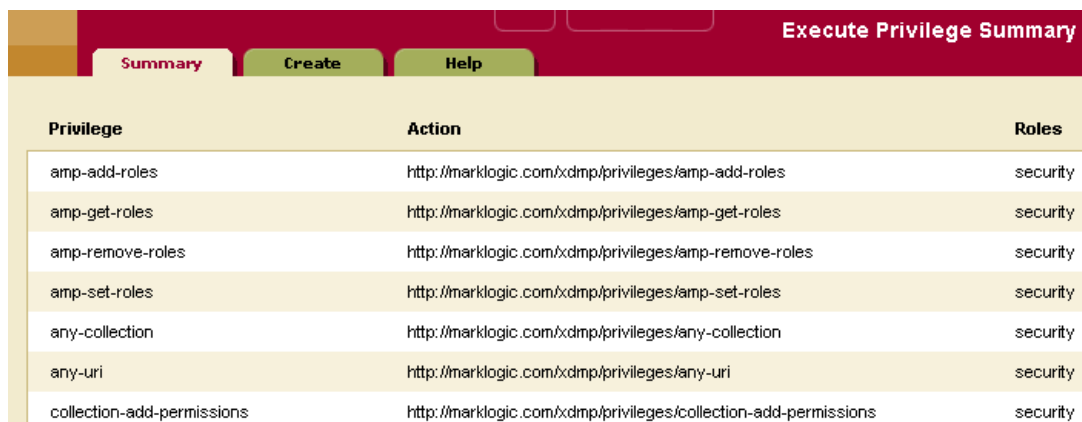
3. [ok] をクリックして変更を保存します。

新しい変更内容は、ユーザーの変更がコミットされた後に開始するすべてのトランザクションで有効になります。

24.4.4 実行権限の削除

セキュリティデータベースから実行権限を削除できます。ただし、削除した実行権限で指定された、保護されたアクションに対して `security-assert()` が行われた場合、例外がスローされます。つまり、削除した実行権限は、保護されたアクションへのアクセス権がロールに与えられていない実行権限と同様に動作します。実行権限を削除するには、次の手順に従います。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Execute Privileges] アイコンをクリックします。[Execute Privileges Summary] ページが表示されます。



Privilege	Action	Roles
amp-add-roles	http://marklogic.com/xdmp/privileges/amp-add-roles	security
amp-get-roles	http://marklogic.com/xdmp/privileges/amp-get-roles	security
amp-remove-roles	http://marklogic.com/xdmp/privileges/amp-remove-roles	security
amp-set-roles	http://marklogic.com/xdmp/privileges/amp-set-roles	security
any-collection	http://marklogic.com/xdmp/privileges/any-collection	security
any-uri	http://marklogic.com/xdmp/privileges/any-uri	security
collection-add-permissions	http://marklogic.com/xdmp/privileges/collection-add-permissions	security

3. 削除する実行権限の名前をクリックします。
4. 選択した権限の [Execute Privileges] ページで、[delete] ボタンをクリックします。
5. [ok] をクリックして、実行権限の削除を確定します。

これで実行権限はセキュリティデータベースから削除されました。

24.5 URI 権限

URI 権限は、保護された URI 下にドキュメントを作成する認可を付与します。つまり、URI 権限は、ドキュメント URI 内のベース URI（プレフィックス）を保護された URI として使用して、ドキュメントを作成できるロールを指定します。指定したロールから継承したロールでも、保護された URI 下にドキュメントを作成できます。

関数を保護するために `xdmp:security-assert()` を明示的に呼び出す必要がある実行権限とは異なり、URI 権限は自動的に強制されます。`xdmp:document-insert()` が呼び出されると、システムは指定されたドキュメント URI のベース URI（プレフィックス）を調べて、URI 権限で保護されているかどうかを確認します。ベース URI に URI 権限が関連付けられている場合、ユーザーのロールがチェックされ、いずれかのユーザーのロールにより、保護されたベース URI 内でドキュメントを作成する認可がユーザーに与えられているかどうかを確認されます。必要な認可がユーザーに与えられている場合、ドキュメントはデータベースに挿入されます。それ以外の場合は、例外がスローされます。

URI 権限の作成、管理、保守を行うには、次の手順を実行します。

- [URI 権限の作成](#)
- [URI 権限の表示](#)
- [URI 権限の修正](#)
- [URI 権限の削除](#)

24.5.1 URI 権限の作成

URI 権限を作成するには、次の手順を実行します。

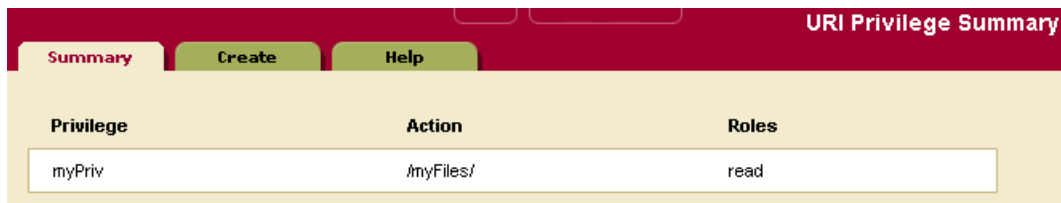
1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [URI Privileges] アイコンをクリックします。
3. [Create] タブをクリックします。[URI Privilege Configuration] ページが表示されます。
4. URI 権限の名前を入力します。保護されるベース URI を説明する名前を使用してください。例えば、会計グループ用に確保されているベース URI 下にドキュメントの作成を制限するには、「accounting_files」という名前を使用できます。
5. [action] フィールドに保護するベース URI を入力します。ベース URI は実際のディレクトリにマッピングしている必要はありませんが、ディレクトリ構造規則（例えば `/myfiles/accounting_files`）に従う必要があります。この例では、この URI 権限を持つユーザーだけが、URI が `/myfiles/accounting_files/account1.xml` のファイルを作成できます。
6. [roles] セクションで、ベース URI 下にドキュメントを作成することを許可されたロールを選択します。
7. [ok] をクリックします。

URI 権限が作成され、セキュリティベースに追加されます。

24.5.2 URI 権限の表示

URI 権限を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [URI Privileges] アイコンをクリックします。[URI Privileges Summary] ページが表示されます。



Privilege	Action	Roles
myPriv	/myFiles/	read

3. 表示する URI 権限の名前をクリックします。
4. URI 権限が表示されます。

24.5.3 URI 権限の修正

実行権限を修正するには、次の手順を実行します。

1. 「URI 権限の表示」(326 ページ) の説明に従って、修正する権限の設定を表示します。
2. 権限に対して必要な修正を実行します (ロール割り当ての追加や削除など)。

警告 URI 権限設定に変更を加えると、その権限のアクセス制御ポリシーが影響を受けます。このため割り当てられたいずれかのロールを (直接または間接的に) 保有するすべてのユーザーに認可される操作が増減する可能性があります。セキュリティシステムが機能する仕組みの詳細については、『*Security Guide*』を参照してください。

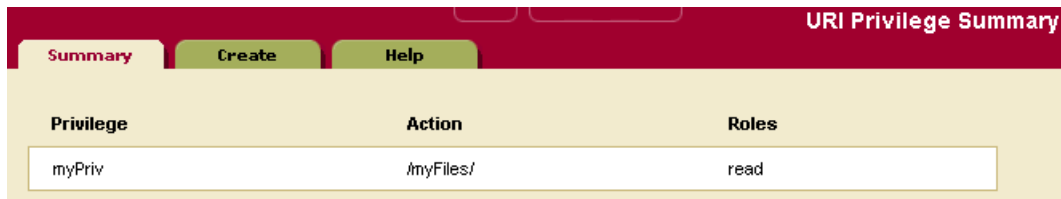
3. [ok] をクリックして変更を保存します。

新しい変更内容は、ユーザーの変更がコミットされた後に開始するすべてのトランザクションで有効になります。

24.5.4 URI 権限の削除

セキュリティデータベースから URI 権限を削除できます。URI 権限を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [URI Privileges] アイコンをクリックします。[URI Privileges Summary] ページが表示されます。



Privilege	Action	Roles
myPriv	/myFiles/	read

3. 指定した権限の [URI Privileges] ページで、[delete] ボタンをクリックします。
4. [ok] をクリックして、URI 権限の削除を確定します。

これで URI 権限はセキュリティデータベースから削除されました。

24.6 Amp

Amp は、ユーザーが特定のタスクを実行（関数を実行）しているときに、一時的にユーザーに追加ロールを与えます。ユーザーは、「amp-ed」関数を実行しているときに、追加ロールにより与えられる追加の権限とパーミッションが付与されます。Amp は、ユーザーが特定の関数を実行している間だけ追加の権限とパーミッションを必要とする場合に役立ちます。

ユーザーに永久的に追加ロールを与えると、システムのセキュリティを損ねる可能性があります。それに対して、Amp は、追加ロールの効力（権限とパーミッション）を特定の関数だけに制限することで、きめ細かなセキュリティ制御を実現します。例えば、ユーザーがレポートを作成しているときに、データベース内の全ドキュメントの数が必要になることがあります。ただし、ユーザーは、データベース内のすべてのドキュメントの読み取りパーミッションを持っているわけではないので、データベース内のすべてのドキュメントの存在はわかりません。ユーザーが関数を実行してシステム内のドキュメントをカウントしている間は、`document-count()` 関数がユーザーを一時的に `admin` ロールに昇格させるように Amp を作成できます。

Amp は、関数のローカル名、名前空間、およびドキュメント URI で定義されます。ドキュメント URI は、スラッシュ「/」で始める必要があり、インストールパスの「Modules」ディレクトリをルートとしてそこから相対的に扱われます。Amp を解決するときに、MarkLogic サーバーは、インストールパスの「Modules」ディレクトリをルートとしてそこからの相対パスを使用してファイルを検索します。指定されたパスを使用してローカル名と名前空間に一致する関数が見つかったら、Amp をこの関数に適用します。

Amp の詳細については、『*Security Guide*』を参照してください。Amp の例については、インストール中に作成されたいずれかの Amp を参照してください。Amp を表示するには、「Amp の表示」(329 ページ)のセクションの手順に従ってください。

Amp の作成、管理、保守を行うには、次の手順を実行します。

- [Amp の作成](#)
- [Amp の表示](#)
- [Amp の修正](#)
- [Amp の削除](#)

24.6.1 Amp の作成

Amp を作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Amps] アイコンをクリックします。
3. [Create] タブをクリックします。[Amp Configuration] ページが表示されます。

The screenshot shows the 'New Amp' configuration page. The page has a red header with 'Amp Configuration' and three tabs: 'Summary', 'Create', and 'Help'. The 'Create' tab is selected. The main content area is titled 'New Amp' and contains several input fields and a dropdown menu. The 'local name' field is empty and has a red error message: 'Required. You must supply a value for local-name.' The 'namespace' field is empty and has a red error message: 'Required. You must supply a value for namespace.' The 'document uri' field is empty and has a red error message: 'Required. You must supply a value for document-uri.' The 'database' field is a dropdown menu with '(filesystem)' selected. Below these fields is a section for 'roles' with checkboxes for 'admin' and 'admin-builtins'. The 'ok' and 'cancel' buttons are located at the top right of the form area.

4. 関数が格納されているデータベースを入力します。関数がファイルシステムの「Modules」ディレクトリに格納されている場合、データベースを `filesystem`（デフォルト値）に設定します。
5. Amp が適用される関数のローカル名を入力します（丸括弧は付けません）。例えば次のようになります。`my-function`。
6. 関数が定義されている名前空間を入力します。
7. 関数が定義されているドキュメントのドキュメント URI を入力します。このドキュメント URI は、スラッシュで始める必要があります（例えば、`/amped-functions.xqy`）。指定したドキュメントは、インストールパス内の「Modules」ディレクトリに配置されている必要があります。例えば、ドキュメント URI で `/mydir/my-amps.xqy` が指定されている場合、`my-amps.xqy` は `<installation-directory>/Modules/mydir` 内に配置されている必要があります。
8. [roles] セクションで、ユーザーが関数を実行している間にユーザーに与えられる追加ロールを選択します。
9. [ok] をクリックします。

これで Amp はセキュリティデータベースに追加されました。

24.6.2 Amp の表示

Amp を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Amps] アイコンをクリックします。[Amp Summary] ページが表示されます。

Local Name	Namespace	Database	Document URI
amp-add-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
amp-get-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
amp-remove-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
amp-set-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
check-admin	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy

3. 表示する Amp の名前をクリックします。
4. Amp が表示されます。

24.6.3 Amp の修正

Amp を修正するには、次の手順を実行します。

1. 「Amp の表示」(329 ページ) の説明に従って、修正する Amp の設定を表示します。
2. Amp に対して必要な修正を実行します (例えば、ロール割り当ての追加や削除)。

警告 Amp 設定に変更を加えると、その Amp のアクセス制御ポリシーが影響を受けます。このため割り当てられたいずれかのロールを (直接または間接的に) 保有するすべてのユーザーに認可される操作が増減する可能性があります。セキュリティシステムが機能する仕組みの詳細については、『*Security Guide*』を参照してください。

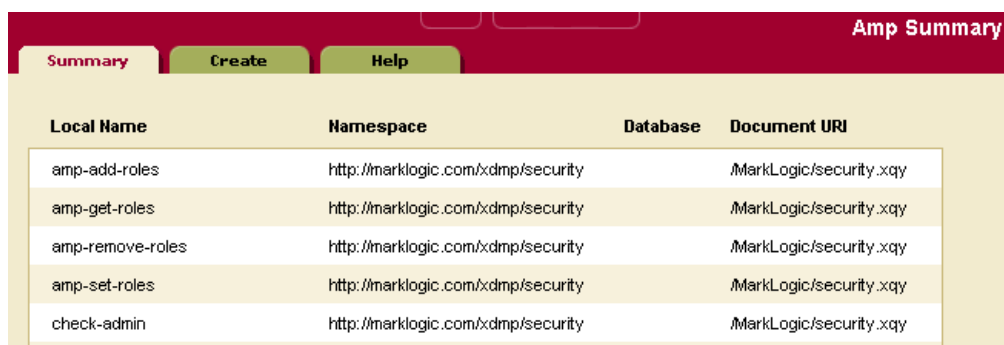
3. [ok] をクリックして変更を保存します。

新しい変更内容は、ユーザーの変更がコミットされた後に開始するすべてのトランザクションで有効になります。

24.6.4 Amp の削除

セキュリティデータベースから Amp を削除できます。Amp を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Amps] アイコンをクリックします。[Amp Summary] ページが表示されます。



Local Name	Namespace	Database	Document URI
amp-add-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
amp-get-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
amp-remove-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
amp-set-roles	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy
check-admin	http://marklogic.com/xdmp/security		/MarkLogic/security.xqy

3. 削除する Amp の名前をクリックします。
4. 指定した Amp の [Amp] ページで、[delete] ボタンをクリックします。
5. [ok] をクリックして、Amp の削除を確定します。

これで Amp はセキュリティデータベースから削除されました。

24.7 保護されているコレクション

コレクションは、関連した一連のドキュメントをグループ化し、データベース内のドキュメントのサブセットを効率的にクエリの対象にできるようにするものです。1つのドキュメントは、任意の数のコレクションに同時に所属できます。コレクションは、システム内のドキュメントが「そのコレクションの一部である」と明示した場合にシステムに存在することになります。ただし、関連付けられたコレクションオブジェクトは、保護されていない限り、セキュリティデータベースでは作成も格納もされません。管理画面を通じて作成されたコレクションは、保護されているコレクションであり、セキュリティデータベース内に格納されます。

読み取り、挿入、更新、および実行の機能は、コレクションに対するパーミッションを必要とします。コレクション別にコレクション内のドキュメントを確認するには、コレクションとドキュメントの両方の読み取りパーミッションがユーザーに必要です。コレクションにドキュメントを追加したりコレクションからドキュメントを削除したりするには、コレクションとドキュメントの両方の更新パーミッションがユーザーに必要です。

コレクションを作成し、管理し、保守するには、次の手順を実行します。

- [保護されているコレクションの作成](#)
- [保護されているコレクションの表示](#)
- [保護されているコレクションからのパーミッションの削除](#)
- [保護されているコレクションの削除](#)

24.7.1 保護されているコレクションの作成

保護されているコレクションを作成するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Collections] アイコンをクリックします。
3. [Create] タブをクリックし、[Collection Configuration] ページを表示します。

The screenshot shows the 'New Collection' dialog box in the MarkLogic Collection Configuration interface. The dialog has tabs for Summary, Configure, Create, and Help. The 'Create' tab is active. The title is 'New Collection'. There are 'ok' and 'cancel' buttons at the top right. The main content area is divided into sections: 'collection -- A collection object.' with a 'uri' input field and a red error message 'Required. You must supply a value for uri.'; and 'permissions -- Permissions to the collection' with three rows of 'Role Name + Capability' dropdown menus, each currently showing 'read'. There are 'ok' and 'cancel' buttons at the bottom.

4. コレクションの URI を入力します。
5. [permissions] セクションで、パーミッション（ロールと機能の組み合わせ）をコレクションに追加します。利用可能なロールから選択し、そのロールに対する読み取り、挿入、更新、または実行の機能を選択します。4 つ以上のパーミッションをロールに追加する場合は、[ok] をクリックした後に次の画面で追加できます。
6. [ok] をクリックします。

保護されているコレクションがデータベースに追加されます。

24.7.2 保護されているコレクションの表示

保護されているコレクションを表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Collections] アイコンをクリックします。[Collection Summary] ページが表示されます。
3. ツリーメニューまたは [Summary] タブで、表示するコレクションの名前をクリックします。[Collection Configuration] ページが表示されます。
4. コレクションが表示されます。

24.7.3 保護されているコレクションからのパーミッションの削除

保護されているコレクションからパーミッションを削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Collections] アイコンをクリックします。[Collection Summary] ページが表示されます。
3. ツリーメニューまたは [Summary] タブで、パーミッションを削除するコレクションの名前をクリックします。[Collection Configuration] ページが表示されます。

The screenshot shows the 'Collection Configuration' page for a collection named 'test'. The page has a dark red header with the title 'Collection Configuration' and several tabs: 'Summary', 'Configure', 'Describe', 'Create', and 'Help'. The 'Configure' tab is active. Below the header, the collection name 'test' is displayed, along with 'ok' and 'cancel' buttons. The main content area is divided into sections: 'collection -- A collection object.' with a 'delete' button; 'uri' with a text input field containing 'test' and the label 'The collection uri.'; and 'permissions -- Permissions to the collection'. The permissions section contains a table with columns for '[Keep]', 'Role Name (capability)', and an '[add]' row. The 'read (read)' permission is checked. At the bottom, there is an '[add]' row with a dropdown menu and a 'read' dropdown menu.

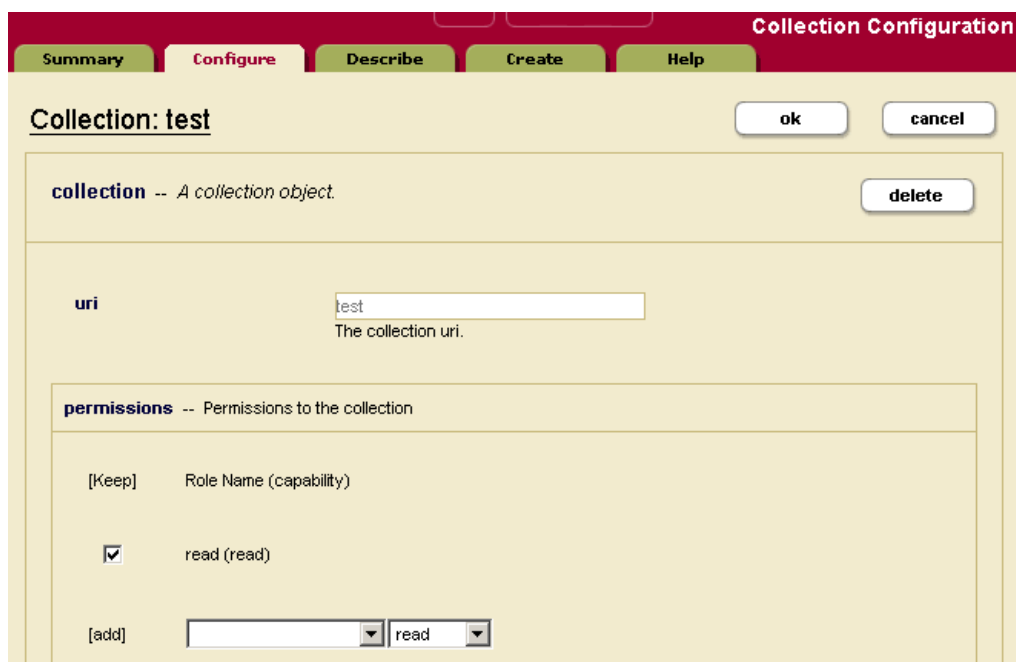
4. [permissions] セクションで、削除するパーミッションの横のチェックボックスをオフにします。
5. [ok] をクリックします。

パーミッションはコレクションから削除されます。

24.7.4 保護されているコレクションの削除

保護されているコレクションを削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Security] アイコンをクリックします。
2. [Collections] アイコンをクリックします。
3. ツリーメニューまたは [Summary] タブで、削除するコレクションの名前をクリックします。[Collection Configuration] ページが表示されます。



4. 右上近くにある [delete] ボタンをクリックします。
5. [ok] をクリックして、コレクションの削除を確定します。

保護されているコレクションがセキュリティデータベースから削除されます。

24.8 証明書テンプレート

証明書テンプレートには、SSL 証明書に関連付けられた識別情報が含まれます。詳細については、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

24.9 レルム

MarkLogic サーバーには、セキュリティデータベースにアプリケーションサーバー用のレルムが格納されています。各アプリケーションサーバーは、接続されているセキュリティデータベースのアプリケーションサーバー用レルムを利用します。レルムは、ダイジェストパスワードの計算で使用されます。

24.9.1 レルムの設定

レルムは、管理画面が接続しているセキュリティデータベースに格納され、インストール時に設定されます。

Security Setup

MarkLogic Server has detected that Administration has not been secured. Please supply a user name and password for the Administrative user to set up security.

You also need to specify a realm for this security database. This is the realm that will be displayed to clients authenticating against this database. Since this value is used in password hashes it is recommended that you not change this value once it is set. Please read the further documentation about realms.

Admin	<input type="text" value="admin"/> User/Login name (unique) Required. You must supply a value for user-name.
Password	<input type="password" value="*****"/> Encrypted Password. Required.
Confirm Password	<input type="password" value="*****"/> Encrypted Password. Required.
Realm	<input type="text" value="public"/> The authentication realm.

24.9.2 レルムの変更

セキュリティデータベース内のレルムを変更すると、すべてのユーザーの digest パスワードが無効になります。これは、[authentication] 設定が digest または digestbasic モードであるアプリケーションサーバーにのみ影響します。

digest モードでは、すべてのユーザーパスワードをセキュリティデータベースに再入力する必要があります。セキュリティデータベース内のパスワードを変更すると、サーバーは digest パスワードを再計算します。digestbasic モードでは、レルムの変更後に初めてユーザーがサーバーにログインしたときに、ユーザーはシステムにログインする前に、パスワードを複数回入力するように求められます。ただし、サーバーはその時点で新しいレルムを使用して digest パスワードを自動的に再計算し、今後のアクセスでは通常のログインプロセスが使用されます。

警告 レルムを変更した場合、digest 認証を使用するすべてのアプリケーションサーバーでは既存のパスワードが利用できなくなります。これには管理画面が含まれ、admin ロールのユーザーのパスワードが含まれます。したがって、レルムを変更すると、それ以降管理画面にログインできなくなります。

インストール後にレルムを変更することが確実な場合は、次の手順を実行してください（ただし上記の警告には注意してください）。

1. 左側のツリーメニューで、[Security] をクリックします。
2. [Configure] タブをクリックします。[Security Configuration] ページが表示されます。



3. レルムを必要な値に変更します。
4. [ok] をクリックします。
5. 確認ページでもう一度 [ok] をクリックします。これにより、すべての digest パスワードが無効になります。管理画面のアプリケーションサーバーが digest 認証に設定されている場合（デフォルト設定）は、管理画面を実行している現在のユーザーのパスワードが無効になります。

25.0 テキストインデックス

データベースにドキュメントを読み込む前に、これらのドキュメントのテキストコンポーネントの扱い方に影響する多数のパラメータを指定するオプションがあります。この章では、これらのパラメータについて説明します。次のセクションで構成されています。

- [テキストインデックス](#)
- [フレージングおよび element-word-query 境界制御](#)
- [再インデックス付け設定をオンおよびオフにしたクエリ動作](#)

テキストインデックスとフレージングパラメータは、データベースごとに設定されます。

25.1 テキストインデックス

MarkLogic サーバーでは、ドキュメントの読み込みおよび更新中にどのタイプのテキストインデックスを構築し保持するかを、データベースレベルで設定できます。各タイプのインデックスは、特定のタイプのクエリのパフォーマンスを高速化します。所定のデータベースについて、異なるタイプの各インデックスを保持するかどうかを指定できます。

注： インデックス設定は、データベース全体に適用されるように指定されます。ドキュメントがすでに読み込まれているデータベースでインデックス設定を変更した場合、そのデータベースの `[reindexer enable]` 設定を `[true]` に設定するか、データを再度読み込むことによって、既存データの再インデックス付けを行う必要があります。

使用する可能性のあるクエリセットについて理解しておく、どのインデックスタイプを利用するか判断する際に役立ちます。インデックスを追加した場合、ディスク容量とドキュメントの読み込み時間が増大するというデメリットがあります。利用するインデックスの数が増えるほど、ドキュメントの読み込みが遅くなります。MarkLogic サーバーでは、一般的な使用シナリオでクエリパフォーマンスが高速になるように設計されている一連のインデックスをデフォルトで構築します。

テキストインデックスタイプは、データベースごとに設定されます。この設定は、指定データベースにドキュメントを読み込む前に完了しておく必要があります。ただし後から変更することも可能です。ドキュメントをすでに読み込んだデータベースでインデックス設定を変更した場合、そのデータベースの `[reindexer enable]` 設定を `[true]` に設定するか、データを再度読み込むことによって、既存データの再インデックス付けを行う必要があります。

標準のインデックス以外に、データベース内の個々の要素および属性にインデックスを設定できます。データベース内の個々の要素または属性に対してレンジインデックスまたはレキシコン、あるいはその両方を作成できます。このようなインデックスの詳細については、「レンジインデックスおよびレキシコン」(356 ページ) を参照してください。指定の要素を明示的に含めたり、除いたりできる名前付きフィールドも作成できます。フィールドの詳細については、「データベースのフィールド設定」(140 ページ) を参照してください。

このセクションでは、MarkLogic サーバーでのテキストインデックスについて説明します。以下のサブセクションがあります。

- [テキストインデックス設定について](#)
- [テキストインデックス設定の表示](#)
- [テキストインデックスの設定](#)

25.1.1 テキストインデックス設定について

以下の表は、利用可能なさまざまなタイプのインデックスについて説明したものです。インデックスは相互に独立していません。ワード検索とステミング検索の両方のインデックスが無効な場合、ワード検索またはステミング検索インデックスが前提となっている残りのインデックスの設定はすべて、無効になります。

インデックス	デフォルト設定	説明
language	en	このデータベース内のコンテンツのデフォルト言語を指定します。 <code>xml:lang</code> 属性を持たないコンテンツは、ここで指定される言語でインデックス付けされます。英語以外の言語を指定する場合は、ライセンスキーが必要です。英語以外の言語を指定するときに、その言語のライセンスがないと、一般的なステミングおよびトークン化が適用されます。
stemmed searches	オフ (インデックスは構築されない)	<p>検索で、語幹をマッチさせることにより関連度でランク付けされた結果を返すかどうかを制御します。「語幹」とは、語形変化 (活用など) したバリエーションすべてに共通している語の部分です。例えば、英語では「run」は「run」、「runs」、「ran」、および「running」の語幹になります。</p> <p>ステミング検索は、クエリで指定した語の完全一致よりも多くのマッチ結果を返します。語のステミング検索では、ステミングなし検索と同じターム以外に、検索タームと同じ意味、同じ品詞から派生するタームも検索されます。例えば、<code>run</code> に対するステミング検索は、<code>run</code>、<code>running</code>、<code>runs</code>、および <code>ran</code> を含む結果を返します。ステミングの詳細については、『<i>Search Developer's Guide</i>』の「Understanding and Using Stemmed Searches」の章を参照してください。</p> <p>ステミングには、<code>basic</code> (1 語につき 1 語幹)、<code>advanced</code> (1 語につき 1 つあるいは複数の語幹)、<code>decompounding</code> (<code>advanced</code> に加え、大きな複合語の小さなコンポーネント語) の 3 つのタイプがあります。</p> <p>このインデックスもワード検索インデックスもない場合、MarkLogic サーバーは、関連度ランク付けを実行できず、<code>cts:word-query()</code> 関連のビルトイン関数の実行を拒否します。ステミング検索とワード検索インデックスの両方が有効な場合、MarkLogic サーバーは、(ステミングなし検索が明示的に指定されていない限り) デフォルトでステミング検索を実行します。</p> <p>ステミング検索を無効にする場合は、このインデックスをオフにしてください。ワード検索およびステミング検索がどちらもオフの場合、全文検索は実質的に無効になります。</p>

インデックス	デフォルト設定	説明
word searches (ステミングなし)	オン (インデックスが構築される)	<p>MarkLogic サーバーは、テキスト要素の語に完全に一致する結果を関連度順に返します。MarkLogic サーバーが <code>cts:word-query()</code> 関連の関数を実行するには、このインデックスまたはステミング検索インデックスのどちらかが必要です。</p> <p>多くのアプリケーションでは、必要なクエリの結果を返すには、このワード検索インデックスをオフのままにし、ステミング検索インデックスをオンのままにしておけば十分です。</p> <p>語の完全一致を行う場合は、このインデックスをオンにしてください。ワード検索およびステミング検索がどちらもオフの場合、全文検索は実質的に無効になります。</p>
word positions	オフ (インデックスは構築されない)	<p><code>cts:near-query</code> 関数を使用する近接クエリと、複数語フレーズ検索のパフォーマンスを高速化します。</p> <p>近接クエリまたはフレーズ検索を扱わない場合や、ディスク容量を節約して読み込み時間を短縮する場合は、このインデックスをオフにしてください。このオプションをオンにした場合、一部の機能が重複しているため <code>fast phrase searches</code> は不要になることもあります。</p>
fast phrase searches	オン (インデックスが構築される)	<p>読み込み (または再インデックス付け) 時に、語のシーケンス (並び順) を記述する追加インデックスを構築することによって、フレーズ検索を高速化します。このインデックスがなくても、MarkLogic サーバーではフレーズ検索を実行できますが、速度が低下します。</p> <p>クエリにおけるフレーズ検索の割合が低い場合や、ディスク容量の節約と読み込み速度の向上がクエリのパフォーマンスよりも重要な場合は、このインデックスをオフにしてください。</p>
fast case sensitive searches	オン (インデックスが構築される)	<p>読み込み時に大文字 / 小文字を区別したインデックスと大文字 / 小文字を区別しないインデックスの両方を構築することにより、大文字 / 小文字を区別した検索を高速化します。このインデックスがなくても、MarkLogic サーバーでは大文字 / 小文字を区別した検索を実行できますが、速度が低下します。</p> <p>テキスト検索における大文字 / 小文字を区別する検索の割合が低い場合や、ディスク容量の節約と読み込み速度の向上がクエリのパフォーマンスよりも重要な場合は、このインデックスをオフにしてください。</p>

インデックス	デフォルト設定	説明
fast reverse searches	オフ (インデックスは構築されない)	格納されているクエリにインデックスを付けることによって、リバースクエリ検索を高速化します。 <code>cts:reverse-query</code> を使用する検索を高速化する場合は、このオプションをオンにしてください。
fast diacritic sensitive searches	オン (インデックスが構築される)	一部の false-positive を除外することで、発音記号を区別する検索をスピードアップします。発音記号を区別する検索を行わない場合は、このオプションをオフにしてください。
fast element word searches	オン (インデックスが構築される)	読み込み時に追加インデックスを作成することによって、特定の要素内で語を探す検索を高速化します。このインデックスがなくても、MarkLogic サーバーではこれらの検索を実行できますが、速度が低下します。特定のドキュメント要素内での語の検索に依存するクエリの割合が低い場合や、ディスク容量の節約と読み込み速度の向上がクエリのパフォーマンスよりも重要な場合は、このインデックスをオフにしてください。
element word positions	オフ (インデックスは構築されない)	要素内で <code>cts:near-query</code> 関数を使用する近接クエリと、複数語要素フレーズ検索のパフォーマンスを高速化します。近接クエリを扱わない場合や、ディスク容量を節約して読み込み時間を短縮する場合は、このインデックスをオフにしてください。
fast element phrase searches	オン (インデックスが構築される)	読み込み (または再インデックス付け) 時に、要素内の語のシーケンスを記述する追加インデックスを作成することによって、要素でのフレーズ検索を高速化します。このインデックスがなくても、MarkLogic サーバーではフレーズ検索を実行できますが、速度が低下します。要素レベルでのフレーズ検索が含まれるクエリの割合が低い場合や、ディスク容量の節約と読み込み速度の向上がクエリのパフォーマンスよりも重要な場合には、このインデックスをオフにしてください。
element value positions	オフ (インデックスは構築されない)	<code>cts:element-value-query</code> 関数を使用する近接クエリのパフォーマンスを高速化します。近接クエリを扱わない場合や、ディスク容量を節約して読み込み時間を短縮する場合は、このインデックスをオフにしてください。

インデックス	デフォルト設定	説明
attribute value positions	オフ (インデックスは構築されない)	<code>cts:element-attribute-value-query</code> 関数を使用する近接クエリのパフォーマンスを高速化し、属性クエリコンストラクタを使用する <code>cts:element-query</code> 検索を高速化します。近接クエリを扱わない場合や、ディスク容量を節約して読み込み時間を短縮する場合は、このインデックスをオフにしてください。
field value searches	オフ (インデックスは構築されない)	<code>cts:field-value-query</code> 関数を使用するフィールド値検索のパフォーマンスを高速化します。このインデックスがない場合や、フィールド定義上に対応するインデックスがない場合、 <code>cts:field-value-query</code> を使用するクエリは例外をスローします。フィールド値クエリを扱わない場合や、ディスク容量を節約して読み込み時間を短縮する場合は、このインデックスをオフにしてください。
field value positions	オフ (インデックスは構築されない)	<code>cts:field-value-query</code> 関数を使用する近接クエリのパフォーマンスを高速化します。近接クエリを扱わない場合や、ディスク容量を節約して読み込み時間を短縮する場合は、このインデックスをオフにしてください。
trailing wildcard searches	オフ (インデックスは構築されない)	末尾にワイルドカード文字を含んでいる検索パターン (例えば、 <code>abc*</code> など) で、ワイルドカード検索を高速化します。末尾ワイルドカードとマッチするワイルドカード検索を高速化するには、このインデックスをオンにしてください。 <code>trailing wildcard search</code> インデックスは、 <code>three character search</code> インデックスとほぼ同じ容量のスペースを使用しますが、末尾ワイルドカードクエリの効率が向上します。ワイルドカード文字がタームの先頭にあるクエリは高速化しません。
trailing wildcard word positions	オフ (インデックスは構築されない)	<code>cts:near-query</code> 関数を使用するワイルドカードクエリや、1つあるいは複数のワイルドカードタームを含む複数語フレーズ検索などの末尾ワイルドカードワード検索を使用する近接クエリのパフォーマンスを高速化します。同じ検索内で、末尾ワイルドカード検索と近接クエリを同時に使用している場合は、このインデックスをオンにしてください。
fast element trailing wildcard searches	オフ (インデックスは構築されない)	特定要素内で検索パターンの末尾にワイルドカードがあるワイルドカード検索を高速化します。ただし、ドキュメントの読み込みが低速化し、データベースファイルのサイズが大きくなります。

インデックス	デフォルト設定	説明
three character searches	オフ（インデックスは構築されない）	<p>3 文字以上の連続する非ワイルドカード文字を含んでいる検索パターン（<code>abc*x</code>、<code>*abc</code>、<code>a?bcd</code> など）で、ワイルドカード検索を高速化します。コードポイントワードレキシコンと組み合わせられると、（連続する非ワイルドカード文字が 3 文字よりも少ない検索も含めて）あらゆるワイルドカード検索のパフォーマンスを高速化します。MarkLogic では、<code>three character search</code> インデックスをコードポイントコレクションのワードレキシコンと組み合わせることを推奨しています。ワイルドカード文字の詳細については、『<i>Application Developer's Guide</i>』の「Understanding and Using Wildcard Searches」を参照してください。</p> <p>文字のインデックス付けをオンにした場合、ほとんどのクエリ式で <code>fn:contains()</code>、<code>fn:matches()</code>、<code>fn:starts-with()</code>、および <code>fn:ends-with()</code> のパフォーマンスも改善されます。3 文字以上とマッチするワイルドカード検索を有効にする場合は、このインデックスをオンにしてください。ワイルドカード検索で、2 文字または 1 文字だけにマッチさせる必要がある場合は、2 文字検索または 1 文字検索、またはその両方を有効にする必要があります。</p>
three character word positions	オフ（インデックスは構築されない）	<p><code>cts:near-query</code> 関数を使用するクエリや、1 つあるいは複数のワイルドカードタームを含む複数語フレーズ検索などの 3 文字ワード検索を使用する近接クエリのパフォーマンスを高速化します。</p> <p>同じ検索内で、ワイルドカード検索と近接クエリを同時に使用している場合に、このインデックスをオンにします。</p>
two character searches	オフ（インデックスは構築されない）	<p>2 文字以上の連続する非ワイルドカード文字を含んでいる検索パターンで、ワイルドカード検索を有効にします。ワイルドカード文字の詳細については、『<i>Application Developer's Guide</i>』の「Understanding and Using Wildcard Searches」を参照してください。</p> <p>文字インデックス付けがデータベースでオンになっているとき、システムでは、ほとんどのクエリ式で <code>fn:contains()</code>、<code>fn:matches()</code>、<code>fn:starts-with()</code>、および <code>fn:ends-with()</code> のパフォーマンスも高くなります。</p> <p>2 文字以上とマッチするワイルドカード検索（例えば、<code>ab*</code> など）を高速化するには、このインデックスをオンにしてください。<code>three character searches</code> とワードレキシコンがある場合、このインデックスは必要ありません。</p>

インデックス	デフォルト設定	説明
one character searches	オフ (インデックスは構築されない)	<p>非ワイルドカード文字 1 文字のみを含む検索パターンで、ワイルドカード検索を高速化します。ワイルドカード文字の詳細については、『<i>Application Developer's Guide</i>』の「Understanding and Using Wildcard Searches」を参照してください。</p> <p>文字インデックス付けがデータベースでオンになっているとき、システムでは、ほとんどのクエリ式で <code>fn:contains()</code>、<code>fn:matches()</code>、<code>fn:starts-with()</code>、および <code>fn:ends-with()</code> のパフォーマンスも高くなります。</p> <p>1 つあるいは複数の文字とマッチするワイルドカード検索 (例えば、<code>a*</code> など) を有効にする場合は、このインデックスをオンにしてください。three character searches とワードレキシコンがある場合、このインデックスは必要ありません。</p>
fast element character searches	オフ (インデックスは構築されない)	<p>特定の XML 要素または JSON プロパティに対してクエリを実行するワイルドカード検索のパフォーマンスを向上させる場合は、このインデックスをオンにしてください。また、要素ベースのワイルドカード検索も高速化します。特定の要素に対してクエリを実行するワイルドカード検索のパフォーマンスを向上させる場合は、このインデックスをオンにしてください。ワイルドカード文字の詳細については、『<i>Application Developer's Guide</i>』の「Understanding and Using Wildcard Searches」を参照してください。</p>

インデックス	デフォルト設定	説明
word lexicons	オフ (インデックスは構築されない)	<p>データベース内のすべてのワードのレキシコンを保持します。一意性は、指定されたコレクションで決定されます。レキシコンの詳細については、「レンジインデックスおよびレキシコン」(356 ページ) および『<i>Application Developer's Guide</i>』のレキシコンに関する章を参照してください。コレクションの詳細については、『<i>Search Developer's Guide</i>』の章「Language Support in MarkLogic Server」を参照してください。</p> <p>ワイルドカード検索を高速化します。検索のインデックス解決とパフォーマンスの向上のために、他に利用可能なワイルドカードインデックスと組み合わせて機能します。</p> <p><code>three character search</code> インデックスと組み合わせて使用した場合、ワイルドカードのインデックス解決を向上させ、ワイルドカード検索を高速化します。データベースに対して <code>three character search</code> およびワードレキシコンをオンにした場合、<code>one character</code> インデックスまたは <code>two character search</code> インデックスのいずれも必要ありません。最適なパフォーマンスを得るには、ワードレキシコンがコードポイントコレクション (http://marklogic.com/collation/codepoint) 内にあることが必要です。ワイルドカード検索の詳細については、『<i>Application Developer's Guide</i>』のワイルドカード検索に関する章を参照してください。</p>
uri lexicon	オフ (インデックスは構築されない)	<p>データベース内で使用されるすべての URI のレキシコンを保持します。URI レキシコンは、URI で制約するクエリを高速化します。これはデータベース内のすべての URI に対するレンジインデックスのようなものです。URI レキシコンの値にアクセスするには、<code>cts:uris</code> または <code>cts:uri-match</code> API を使用します。</p>
collection lexicon	オン (インデックスが構築される)	<p>データベース内で使用されるすべてのコレクション URI のレキシコンを保持します。コレクションレキシコンにより、コレクションに制約するクエリを高速化します。これはデータベース内のすべてのコレクション URI のレンジインデックスに似ています。コレクションレキシコンの値にアクセスするには、<code>cts:collections</code> または <code>cts:collection-match</code> API を使用します。</p>

25.1.2 テキストインデックス設定の表示

特定のデータベースのテキストインデックス設定を表示するには、次の手順に従います。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、テキストインデックス設定を表示するデータベースを特定します。
3. 設定を表示するデータベースの名前をクリックします。
4. テキストインデックス設定が表示されるまで下にスクロールします。次のスクリーンショットは、データベースのテキストインデックス付けのデフォルト設定を示しています。

language
The default language assumed for content (if xml:lang encoding is absent)

stemmed searches
Enable stemmed word searches (slower document loads and larger database files).

word searches true false
Enable unstemmed word searches (slower document loads and larger database files).

word positions true false
Index word positions for faster phrase and near searches (slower document loads and larger database files).

fast phrase searches true false
Enable faster phrase searches (slower document loads and larger database files).

fast case sensitive searches true false
Enable faster case sensitive searches (slower document loads and larger database files).

fast reverse searches true false
Enable faster reverse searches (slower document loads and larger database files).

fast diacritic sensitive searches true false
Enable faster diacritic sensitive searches (slower document loads and larger database files).

fast element word searches true false
 Enable faster element-word searches (slower document loads and larger database files).

element word positions true false
 Index element word positions for faster element-based phrase and near searches (slower document loads and larger database files).

fast element phrase searches true false
 Enable faster element phrase searches (slower document loads and larger database files).

element value positions true false
 Index element value positions for faster near searches involving element-value-query (slower document loads and larger database files).

attribute value positions true false
 Index attribute value positions for faster near searches involving element-attribute-value-query (slower document loads and larger database files).

field value searches true false
 Index field values for faster searches involving field-value-query (slower document loads and larger database files).

field value positions true false
 Index field value positions for faster near searches involving field-value-query (slower document loads and larger database files).

three character searches true false
 Enable wildcard searches and faster character-based XQuery predicates using three or more characters (slower document loads and larger database files).

three character word positions true false
 Index word positions for three-character searches only when three-character-searches are enabled (slower document loads and larger database files).

fast element character searches true false
 Enable element wildcard searches and element-character-based XQuery predicates (slower document loads and larger database files).

trailing wildcard searches true false
 Enable trailing wildcard searches (slower document loads and larger database files).

trailing wildcard word positions true false
 Index word positions for trailing-wildcard searches only when trailing-wildcard-searches are enabled (slower document loads and larger database files).

fast element trailing wildcard searches true false
 Enable element trailing wildcard searches (slower document loads and larger database files).

word lexicons

[add]

collation builder

more word lexicons

two character searches true false
 Enable wildcard searches and faster character-based XQuery predicates using two character (slower document loads and larger database files).

25.1.3 テキストインデックスの設定

特定のデータベースのテキストインデックスを設定するには、次の手順に従います。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、テキストインデックス設定を表示するデータベースを特定します。
3. 設定を表示するデータベースの名前をクリックします。
4. テキストインデックス付けのコントロールが表示されるまで下にスクロールします。
5. 各インデックスタイプに対応する適切なラジオボタンを選択して、このデータベースのテキストインデックスを設定します。

特定のインデックスを利用する場合、そのテキストインデックスタイプの [true] ラジオボタンをクリックします。特定のインデックスを利用しない場合、そのテキストインデックスタイプの [false] ラジオボタンをクリックします。

注： ワード検索とステミング検索が無効な場合（つまり、[word searches] に対して [false] ラジオボタンが選択されており、[stemmed searches] に対して [off] が選択されている場合）、上述のように、他のテキストインデックスのテキストは無視されます。

6. 残りのパラメータはそのままにしておきます。
7. 右側のフレームの一番上または下までスクロールして、[ok] をクリックします。

これでデータベースに、新しいテキストインデックス付けが設定されます。

25.2 フレージングおよび element-word-query 境界制御

MarkLogic サーバーでは、XML 要素コンストラクタが、検索のテキストフレージングおよび element-word-query 境界に与える影響について指定できます。このセクションでは、以下の内容を取り上げます。

- [フレージング制御](#)
- [element word query through](#)
- [手順](#)

25.2.1 フレージング制御

MarkLogic サーバーでは、デフォルトですべての XML 要素コンストラクタがフレーズ境界として機能することを想定しています。したがって、フレーズ検索（タームのシーケンスの検索など）は、1つあるいは複数の XML 要素コンストラクタを含むタームのシーケンスをマッチしません。フレージング制御を使用すると、フレーズ境界に対して透過的にする必要がある XML 要素（太字や斜体要素など）と、フレーズの意味的に無視すべき XML 要素（脚注やグラフィックキャプションなど）を指定できます。

例として、次のサンプルの XML フラグメントについて考えます。

```
<paragraph>
  These two words <italic>are italicized</italic>.The italic element
  <footnote>Elements are defined in the W3C XML standard.</footnote>
  is a standard part of this document's schema.
</paragraph>
```

デフォルトでは、MarkLogic サーバーは、フレーズマッチングの目的で次の 5 つのテキストのシーケンスを抽出します（簡略化のため句読点と大文字 / 小文字を無視）。

- 「these two words」
- 「are italicized」
- 「the italic element」
- 「elements are defined in the w3c xml standard」
- 「is a standard part of this document's schema」

この XML フラグメントに対して「words are italicized」や「element is a standard part」のフレーズをマッチさせようとした場合、埋め込まれた XML 要素コンストラクタのためにマッチする結果は見つかりません。

実際、この XML フラグメントを見た人は、フレーズの意味に関して `italic` 要素には意味がないこと、また `footnote` 要素は完全に独立したテキストコンテナであることは理解できます。この観点から見ると、上記の XML フラグメントには、2 つのテキストシーケンスのみ含まれます（この場合も、簡略化のため句読点と大文字 / 小文字を無視）。

- 「these two words are italicized the italic element is a standard part of this document's schema」
- 「elements are defined in the w3c xml standard」

この場合、「words are italicized」と「element is a standard part」はそれぞれ、マッチ結果を正しく生成します。ただし「the w3c xml standard is a standard」の検索はマッチしません。

MarkLogic サーバーでは、特定の XML 要素名を、`phrase-through`、`phrase-around`、および `element-word-query-through` の要素として指定することにより、このタイプのフレーズ制御を実現できます。

タイプ	定義
Phrase-through	フレーズ境界を作成しない要素（上記の例では、 <code>italic</code> を <code>phrase-through</code> 要素として指定する必要があります）。
Phrase-around	現在のフレーズのコンテキストで完全に無視されるコンテンツを含む要素（上記の例では、 <code>footnote</code> を <code>phrase-around</code> 要素として指定する必要があります）。

フレーズ制御は、データベースごとに設定されます。この設定は、指定データベースにドキュメントを読み込む前に完了しておく必要があります。完了していない場合、既存のコンテンツに対して変更内容を有効にするために、設定の変更後、コンテンツを再度読み込むか、データベースの再インデックス付けを実行する必要があります。

25.2.2 element word query through

`element-word-query-through` を使用すると、親要素で `cts:element-word-query` を使用するときテキスト検索に含める必要のある要素を指定できます。例として、次の XML フラグメントについて考えます。

```
<a>
  <b>hello</b>
  <c>goodbye</c>
</a>
```

`<a>` で `cts:element-word-query` を実行し `hello` の語を検索している場合、検索で、このフラグメントでマッチする結果は見つかりません。次のクエリはこのパターンを示しています。

```
cts:search(fn:doc(), cts:element-word-query(xs:QName("a"), "hello"))
```

このクエリでは、`cts:element-word-query` は、要素 `<a>` の直接の子であるテキストノードだけを検索し、`<a>` の子ノードの子であるテキストノードは検索しないため、マッチする結果は見つかりません。`hello` は、`` の子であるテキストノードにあるため、`cts:element-word-query` を満たしません。

ただし、要素 `` に対して `element-word-query-through` を追加した場合、`hello` の語を検索している `<a>` での `cts:element-word-query` は、マッチする結果を返します。`` における `element-word-query-through` により、`` の子テキストノードは、その親（この場合は `<a>`）の子テキストノードのように機能します。

注： 要素が `phrase-through` として指定された場合、`element-word-query-through` としても機能するため、`element-word-query-through` として指定する必要はありません。

25.2.3 手順

次の手順を使用して、特定のデータベースに対しフレーズ制御を設定します。

- [フレーズと element-word-query 設定の表示](#)
- [フレーズと element-word-query の設定](#)
- [フレーズまたは element-word-query 設定の削除](#)

25.2.3.1 フレーズと element-word-query 設定の表示

特定のデータベースに対する element-word-query-through、phrase-through、および phrase-around 設定を表示するには、管理画面で次の手順に従います。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、element-word-query-through、phrase-through、または phrase-around 設定を表示するデータベースを探します。
3. 設定を表示するデータベースの名前をクリックします。
4. 表示する設定に応じて、[Element-Word-Query-Throughs]、[Phrase-Throughs]、または [Phrase-Arounds icon] のアイコンをクリックします。
5. 設定ページが表示されます。

次の例は、XHTML 名前空間の <abbr>、<acronym>、、<big>、
、および <center> 要素などの多数の phrase-through 要素でドキュメントデータベースが設定されていることを示します。

Phrase-Throughs Configuration

Configure Create Help

Database: Documents ok cancel

phrase throughs -- The phrase-through specifications.

phrase through -- Phrases may cross these markup boundaries. delete

namespace uri http://www.w3.org/1999/xhtml
A namespace URI.

localname a,abbr,acronym,b,big,br,center,cite,code,
One or more localnames.

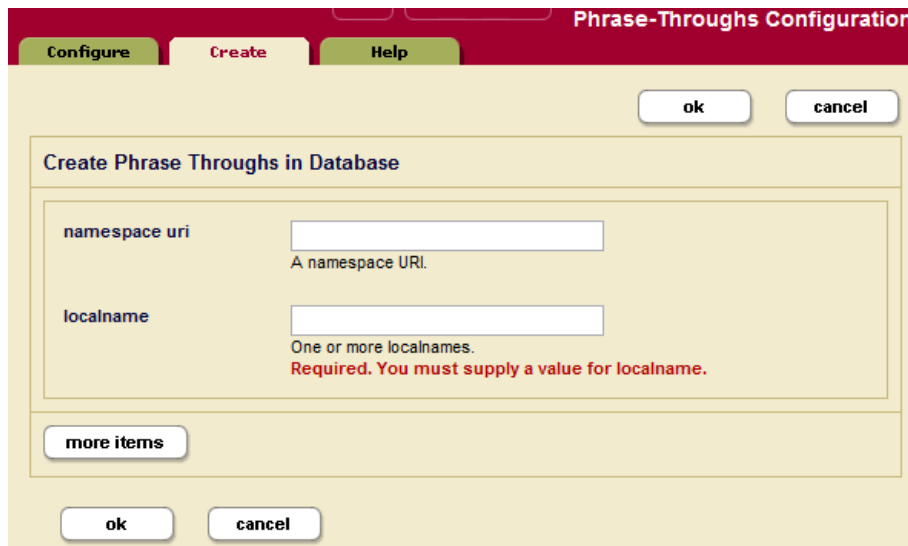
25.2.3.2 フレージングと element-word-query の設定

特定のデータベースに対して element-word-query-through、phrase-through、および phrase-around を設定するには、管理画面で次の手順に従います。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、element-word-query-through、phrase-through、または phrase-around を設定するデータベースを特定します。
3. 設定するデータベースの名前をクリックします。
4. 設定に応じて、[Element-Word-Query-Throughs]、[Phrase-Throughs]、または [Phrase-Arounds icon] のアイコンをクリックします。

注： この手順の残りでは、phrase-through を設定すると想定しています。phrase-around または element-word-query-through を設定する場合、対応するアイコンをクリックした後の手順は完全に同一です。

5. 右上の [Create] タブをクリックします。[Phrase-Throughs Configuration] ページが表示されます。



6. phrase-through 要素として指定する XML 要素の名前空間 URI を入力します。

XML 要素はすべて、名前空間と関連付けられます。phrase-through 設定が正確になるように、XML 要素に名前空間を指定する必要があります。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

または、[namespace uri] フィールドにアスタリスク (*) を入力することで、要素が名前空間に無関係であることを指定できます。

7. [localname] フィールドに要素名を入力します。
ローカル名は、phrase-through 要素として指定する XML 要素の名前です。指定した名前空間に関連付けられた要素を複数指定する場合、要素名をカンマ区切りで入力します。
8. さらに phrase-through を追加するには、[more items] ボタンをクリックして、必要に応じて phrase-through 要素ごとにステップ 6 からステップ 7 を繰り返します。
9. 上部または下部までスクロールして [ok] をクリックします。

新しい phrase-through が追加されます。

注： ドキュメントがすでに読み込まれた後で特定のデータベースの element-word-query-through、phrase-through、または phrase-around 設定を変更する場合、そのデータベースの [reindexer enable] 設定を [true] に指定するか、データを再度読み込むことによって、既存データの再インデックス付けを行う必要があります。

25.2.3.3 フレージングまたは element-word-query 設定の削除

特定のデータベースに対して element-word-query-through、phrase-through、または phrase-around 設定を削除するには、管理画面で次の手順に従います。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、element-word-query-through、phrase-through、または phrase-around 設定を削除するデータベースを特定します。
3. 設定を削除するデータベースの名前をクリックします。
4. 削除する設定に応じて、[Element-Word-Query-Throughs]、[Phrase-Throughs]、または [Phrase-Arounds icon] のアイコンをクリックします。

適切な設定ページが表示されます。

5. 削除する要素まで下にスクロールします。
6. 削除する要素の横にある [drop] ボタンをクリックします。

確認メッセージが表示されます。

7. 削除操作を確認し、[ok] をクリックします。

Phrase-Through または Phrase-Around 要素がデータベースから削除されます。

注： ドキュメントがすでに読み込まれた後で特定のデータベースの element-word-query-through、phrase-through、または phrase-around 設定を変更する場合、そのデータベースの [reindexer enable] 設定を [true] に指定するか、データを再度読み込むことによって、既存データの再インデックス付けを行う必要があります。

25.3 再インデックス付け設定をオンおよびオフにしたクエリ動作

ドキュメントはデータベースに読み込まれると、読み込み時のインデックス設定に基づいてインデックスが付けられます。データベースに対してクエリを実行すると、インデックス設定の一貫したビューに基づいて評価されます。この一貫したビューには、データベースでオンにされたインデックス機能が一部含まれていないことがあります。このセクションでは、データベースのさまざまなインデックス設定状態でのクエリの動作について説明します。以下のように構成されています。

- [reindexer.enable 設定について](#)
- [最小限共通項目に従ったクエリ評価](#)
- [再インデックス付けはポイントインタイムバージョンのフラグメントに適用されない](#)
- [シナリオ例](#)

25.3.1 reindexer.enable 設定について

データベースレベルでは、そのデータベースに対して `[reindexer.enable]` 設定を `[true]` または `[false]` に指定することによって、自動再インデックス付けをオンまたはオフにできます。リインデクサーをオンにすると、データベース設定に対するインデックスまたはフラグメントの変更により、その設定に応じてインデックス付け/フラグメント化されていないデータベース内のすべてのドキュメントに対して、再インデックス付け操作が開始されます。データベース設定と再インデックス付け操作について、以下の内容に注意してください。

- 再インデックス付けをオンにすると、再インデックス操作は、バックグラウンドタスクとして実行します。`[reindexer.throttle]` の設定を増減することによって、再インデックス付けタスクのプライオリティを増減できます。
- データベースで追加または更新された新しいドキュメントは、新しいデータベース設定を取得します。これは、再インデックス付けをオンにした場合にもオフにした場合にも当てはまります。
- データベースでインデックスまたはフラグメンテーション設定を変更した後、新しいドキュメントや修正したドキュメントは新しい設定を取得するため、データベース内の一部のドキュメントが、他のドキュメントとは異なったインデックス付け/フラグメント化になっている状態が発生します。
- 再インデックス付けがオンになっているデータベースでインデックスまたはフラグメンテーション設定を変更した後、古いドキュメントは新しい設定に従って再度インデックスが付けられますが、再インデックス付け操作が完了し、すべてのドキュメントにインデックスが付けられデータベース設定にマッチした状態になるまで、新しい設定はクエリに反映されません。
- 再インデックス付けがオフになっているデータベースでインデックスまたはフラグメンテーション設定を変更した後、新規または変更されたドキュメントは現在の設定を取得しますが、データベース内のすべてのドキュメントがデータベース設定にマッチするまで、クエリは新しい設定を利用しません。
- 再インデックス付けがオフになっている場合でも、トークナイザーオーバーライドをフィールドに追加すると、これらのトークン化の変更は即座に有効になるので、(以前のトークン化でインデックスが付けられている場合でも) そのフィールドに対するすべての新しいクエリは新しいトークン化を使用します。

25.3.2 最小限共通項目に従ったクエリ評価

クエリが評価される際は、所定の時点でデータベースに対して計算されたインデックス設定を使用します。クエリの現在のインデックス設定はクエリ評価の時点で決定され、以下の最小限共通項目（つまり、最低限のインデックス / フラグメンテーション設定）に基づきます。

- データベース設定で定義されたインデックス / フラグメンテーション設定
- データベースのドキュメント / フラグメントの実際のインデックス / フラグメンテーション

現在の最小限共通項目は、以下のイベントの発生時にいつでも無効化されます。

- システムの起動
- データベース設定の変更
- 再インデックス付け操作の完了時

最小限共通項目が無効化された場合、次回データベースに対してクエリが実行されたときに再計算されます。

最終的な影響は、次のようになります。データの読み込み後にデータベースでインデックス / フラグメンテーション設定が変更された場合、新しい設定が最小限共通項目の条件を満たすまで、クエリは新しい設定を利用できません。この結果、行ったインデックス設定の変更のタイプに応じて、インデックス設定の変更前にある方法で動作していたクエリが、変更後には別の動作を行うようになる可能性があります。次のセクションでは、この動作を表すサンプルシナリオを示します。

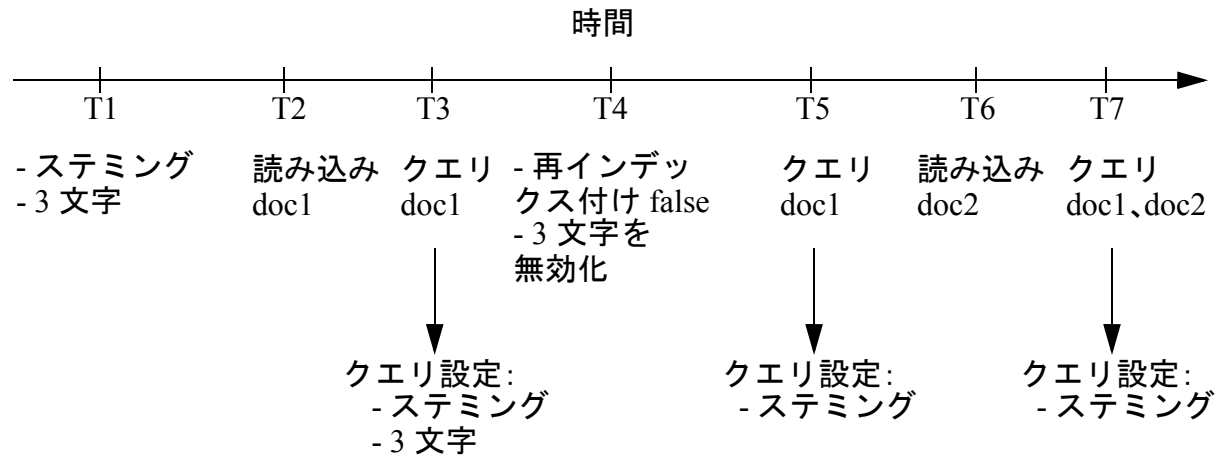
25.3.3 再インデックス付けはポイントインタイムバージョンのフラグメントに適用されない

ポイントインタイムクエリ用に古いバージョンのフラグメントを保持するように、データベースで `merge timestamp` を設定している場合、古いバージョンのフラグメントは、それらが更新された時点のデータベースのインデックス付けプロパティを保持します。このため、ポイントインタイムクエリを使用するデータベースの再インデックス付けにより、予測不能なクエリ結果が生じることがあります。`merge timestamp` パラメータが 0 以外の値に設定されているデータベースは、再インデックス付けしないことをお勧めします。ポイントインタイムクエリの詳細については、『*Application Developer's Guide*』のポイントインタイムクエリに関する章を参照してください。`merge timestamp` パラメータの設定の詳細については、「マージとポイントインタイムクエリ」(170 ページ) を参照してください。

25.3.4 シナリオ例

このセクションでは、クエリ動作におけるインデックス設定の変更の影響を時系列的に示す単純なシナリオについて説明します。

次の図は、インデックス設定の変更が行われた後に開始したクエリに、インデックス設定の変更がどのような影響を与える可能性があるかを示しています。



このシナリオでは、T3 時に実行されたクエリは、ステミングおよび 3 文字のワイルドカードインデックスを有効にして doc1 ドキュメントを参照します。abc* などのワイルドカードクエリは成功します。ただし、T5 時の同じワイルドカードクエリは、3 文字インデックス (abc* クエリに必要) が T4 時に無効になったので成功しません。ドキュメント doc1 には実際に 3 文字およびステミングのインデックスが付けられていますが、T5 時のクエリはステミングインデックスしか使用できません。T7 時には、データベースの doc1 にはステミングと 3 文字の両方のインデックスが付けられていますが、doc2 はステミングインデックスしか付けられていません。再インデックス付けが無効になっているので、T7 時のクエリは、最小共通項目 (この場合はステミング) を使用します。

26.0 レンジインデックスおよびレキシコン

MarkLogic サーバーでは、データベースレベルで、要素と属性に対し、その QName に従ってインデックスとレキシコンを作成できます。この章では、このレンジインデックスとレキシコンについて説明します。次のセクションで構成されています。

- [レンジインデックスについて](#)
- [値レキシコンにレンジインデックスを使用する](#)
- [ワードレキシコンについて](#)
- [パスレンジインデックスについて](#)
- [要素レンジインデックス設定の表示](#)
- [要素レンジインデックスの定義](#)
- [属性レンジインデックス設定の表示](#)
- [属性レンジインデックスの定義](#)
- [パスレンジインデックス設定の表示](#)
- [パスレンジインデックスおよびフィールドで使用される名前空間プレフィックスの定義](#)
- [パスレンジインデックスの定義](#)
- [要素ワードレキシコン設定の表示](#)
- [要素ワードレキシコンの定義](#)
- [属性ワードレキシコン設定の表示](#)
- [属性ワードレキシコンの定義](#)
- [値レキシコンの定義](#)
- [レンジインデックスまたはレキシコンの削除](#)
- [フィールドレンジインデックスの定義](#)

さらに、「フィールドのレンジインデックスの作成」（161 ページ）の説明に従って、フィールドのレンジインデックスを作成できます。

この章では、管理画面を使用してレンジインデックスとレキシコンを作成する方法について説明します。レンジインデックスをプログラムによって作成する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Adding Indexes to a Database](#)」を参照してください。

26.1 レンジインデックスについて

この章では、下の表に示されたレンジインデックスのタイプについて説明します。「フィールドのレンジインデックスの作成」(161 ページ) で説明しているように、フィールドレンジインデックスもあります。

タイプ	説明
要素レンジインデックス	XML 要素または JSON プロパティのレンジインデックス。
属性レンジインデックス	XML 要素内の属性のレンジインデックス。
パスレンジインデックス	XPath 式で定義された XML 要素、XML 属性、または JSON プロパティのレンジインデックス。
フィールドレンジインデックス	フィールドのレンジインデックス。詳細については、「データベースのフィールド設定」(140 ページ) を参照してください。

MarkLogic サーバーでは、XML および JSON ドキュメントのコレクション内にあるテキスト、構造、およびテキストと構造の組み合わせをすばやく検索するために、すべてのデータベースにおいてユニバーサルインデックスを使用します。

一方、XML および JSON ドキュメントには、数値または日付情報が含まれている場合があります。これらのドキュメントに対するクエリには、不等式に基づいた検索条件を含めることができます (`price < 100.00` や `date ≥ thisQtr` など)。これらの要素、属性、または JSON プロパティに対してレンジインデックスを指定すると、これらのクエリの評価が大幅に高速化されます。

レンジインデックスを定義しても、`cts:search` 操作でレンジクエリコンストラクタ (`cts:element-range-query` および `cts:element-attribute-range-query`) を使用でき、検索で使用する複雑なレンジクエリ式を簡単に構成できます。詳細については、『*Search Developer's Guide*』の「[Using Range Queries in cts:query Expressions](#)」の章を参照してください。

同様に、`xs:string` 型のレンジインデックスも作成できます。これらのインデックスは、文字列値でソートするクエリのパフォーマンスを高速化でき、レキシコンクエリにも使用されます(「ワードレキシコンについて」(361 ページ) を参照)。

ある要素でレンジインデックスを指定して、複雑なコンテンツ(子要素を伴う要素など)を持つその名前の要素がある場合、コンテンツは、指定されたタイプのレンジインデックスへの要素のキャストに基づいて、インデックスが付けられます。例えば、`h1` という名前の要素に `xs:string` 型のレンジインデックスを指定する場合、次の要素

```
<h1>This is a <b>bold</b> title.</h1>
```

に、`This is a bold title` の値でインデックスが付けられます。これは `h1` 要素を `xs:string` にキャストして返された値です。同じタイプのキャストは、XML 属性、JSON プロパティ、およびフィールドに関するレンジインデックスに適用されます。この動作により、コンテンツを事前処理せずに、複雑なコンテンツにインデックスを付けられます。

また、レンジインデックスは、`order by` 句を使用して結果をソートし、データのサブセット（例えば最初の 10 項目）を返すクエリのパフォーマンスを改善できます。レンジインデックスを使用したこの `order by` 最適化の詳細については、『*Query Performance and Tuning Guide*』の「[Sorting Searches Using Range Indexes](#)」を参照してください。

MarkLogic サーバーでは、広範な XML データ型にわたり、要素と属性の両方のレンジインデックスをサポートしています。このリストの大部分は、XML の全順序データ型に適合しています。

型	説明
<code>int</code>	正および負の整数
<code>unsignedInt</code>	正の整数（0 を含む）
<code>long</code>	大きな正および負の整数
<code>unsignedLong</code>	大きな正の整数（0 を含む）
<code>float</code>	32 ビットの浮動小数点数
<code>double</code>	64 ビットの浮動小数点数
<code>decimal</code>	大きな浮動小数点数
<code>dateTime</code>	日付と時刻の組み合わせ
<code>time</code>	時間（タイムゾーンを含む）
<code>date</code>	完全な日付（年、月、日）
<code>gYearMonth</code>	年と月のみ
<code>gYear</code>	年のみ
<code>gMonth</code>	月のみ
<code>gDay</code>	日のみ
<code>yearMonthDuration</code>	年数および月数による期間
<code>dayTimeDuration</code>	日数および時間数による期間
<code>string</code>	文字列データ
<code>anyURI</code>	URI 文字列

上記の日付と時刻の型は、日付と時刻に関する XML 規格に従っていることに注意してください。現在、他の形式の日付と時刻は、MarkLogic サーバーレンジインデックスでサポートしていません。これらのデータ型の定義の詳細については、W3C XML スキーマドキュメントを参照してください。

レンジインデックスは、管理画面、XQuery または JavaScript Admin API、あるいは REST 管理 API を使用して明示的に作成する必要があります。JSON プロパティでレンジインデックスを作成するには、要素レンジインデックスインターフェイスまたは関数を使用します。次の表は、各種インデックスを定義するために必要な基本情報を示したものです。

インデックスタイプ	必要な情報
XML 要素	要素名、要素の名前空間、その要素内で見つかった値のデータ型。
XML 属性	属性名、属性の親要素の名前、その要素の名前空間、その属性で見つかった値のデータ型。
JSON プロパティ	プロパティ名と、そのプロパティで見つかった値のデータ型。
パス	XPath 式と、XPath で表された要素、属性、または JSON プロパティで見つかった値のデータ型。
フィールド	フィールド名と、フィールドの値のデータ型。フィールド定義を設定する必要もあります。詳細については、「フィールドの設定」(150 ページ)を参照してください。

レンジインデックスは、ドキュメント読み込みプロセス中に生成され、インデックス付けされたデータへのその後の更新を通じて、自動的に同期状態が保たれます。したがって、レンジインデックスは、インデックス付けされるコンテンツを含む XML または JSON ドキュメントがデータベースに読み込まれる前に、そのデータベースに対して指定する必要があります。そうしない場合、新しいレンジインデックスを利用するために、コンテンツを再インデックス付けするか、コンテンツを再読み込みする必要があります。

JSON ドキュメントのインデックスを作成するには、要素レンジインデックスインターフェイスおよび API を使用します。一部の制限が適用されます。詳細については、『*Application Developer's Guide*』の「[Creating Indexes and Lexicons Over JSON Documents](#)」を参照してください。

要素または属性レンジインデックスで作成したものと同一タイプのインデックスをパスレンジインデックスで作成できます。パスレンジインデックスは、要素または属性レンジインデックスが機能しない環境で役立ちます。例えば、異なる親要素の下に同じ要素名が現れるドキュメントがあるときに、いずれかの親要素の下に現れる要素にだけインデックスを付けようとする場合があります。この場合、その要素に正しくインデックスを付けるには、パスレンジインデックスが必要になります。

スカラータイプの文字列 (`xs:string`) でレンジインデックスを作成するときに、要素 / 属性の QName または JSON プロパティ名に加えてコレーションを指定します。コレーションは、文字列値の一意の順序を指定します。同じ要素、属性、または JSON プロパティに関して複数のレンジインデックスを異なるコレーションで設定できます。つまり、コレーションは、文字列レンジインデックスの一意の識別子の一部になります。コレーションの詳細については、『*Search Developer's Guide*』の「[Encodings and Collations](#)」の章を参照してください。

レンジインデックスは型指定されたデータを格納するので、読み込んだデータがその型に従っていない場合、または指定した型に強制的に適合させられない場合は、ドキュメントに読み込めません。レンジインデックスごとに、無効な値を拒否 (`reject`) してドキュメントの読み込みで例外をスローして失敗させるか、無視 (`ignore`) して

`ErrorLog.txt` ファイルにエラーをログ記録するかを指定できます。デフォルトは、無効なデータの拒否 (`reject`) です。

レンジインデックスはディスク容量を使用し、メモリを消費します。これは、パフォーマンスの向上とのトレードオフです。さらに、大量のレンジインデックスデータがある場合、およびシステムが定期的に更新される場合は、ジャーナルのサイズを増やす必要があります。データベースジャーナル設定の詳細については、「メモリおよびジャーナル設定」(117 ページ) を参照してください。

26.2 値レキシコンにレンジインデックスを使用する

ソートおよび比較クエリの速度を上げる以外に、MarkLogic サーバーは、レンジインデックスを使用して、XML 要素、XML 属性、JSON プロパティ、およびフィールド値レキシコンクエリを解決します。これらのクエリは、次の search API を使用します。

- `cts:values`
- `cts:value-match`
- `cts:element-attribute-values`
- `cts:element-attribute-value-match`
- `cts:element-values`
- `cts:element-value-match`
- `cts:field-values`
- `cts:field-value-match`

`cts:values` および `cts:value-match` 関数は、あらゆる種類のレンジインデックスで機能し、インデックスを参照して呼び出されたときは、対応する同じタイプのインデックス固有関数に相当します。例えば、次の 2 つの関数呼び出しは同等です。

```
cts:values(cts:element-reference(xs:QName("some-element")))
cts:element-values(xs:QName("some-element"))
```

これらの API のいずれかを使用するには、クエリで指定される要素、属性、JSON プロパティ、またはフィールドのレンジインデックスを作成する必要があります。レンジインデックスのタイプは、レキシコン API で指定したタイプと一致している必要があります。

レキシコンの詳細については、『*Search Developer's Guide*』の「[Browsing With Lexicons](#)」の章を参照してください。レキシコン API の詳細については、『*MarkLogic XQuery and XSLT Function Reference*』を参照してください。

26.3 ワードレキシコンについて

MarkLogic サーバーでは、特定の XML 要素、XML 属性、JSON プロパティ、またはフィールドに制限されたワードレキシコンを作成できます。ワードレキシコンは、指定された要素、属性、または JSON プロパティに格納されている一意の語をすべて格納します。語は、大文字と小文字を区別し、発音記号を区別して格納されるので、レキシコンでは `Ford` と `ford` の語が異なるエントリーになります。ワードレキシコンを使用するには、次の search API を使用します。

- `cts:element-attribute-words`
- `cts:element-attribute-word-match`
- `cts:element-words`
- `cts:element-word-match`
- `cts:field-words`
- `cts:field-word-match`
- `cts:json-property-words`
- `cts:json-property-word-match`

26.4 パスレンジインデックスについて

パスレンジインデックスでは、XPath 式を使用して、XML 要素、XML 属性、または JSON プロパティのレンジインデックスを定義できます。パスレンジインデックスは、インデックス付け対象の細かな制御を可能にします。例えば、複数レベルで同じ名前の要素がコンテンツに含まれており、それらの 1 つにだけインデックスを付ける場合は、パスレンジインデックスを使用してその 1 つだけを対象にできます。

このセクションでは、パスレンジインデックスを定義するために使用できる XPath 式について説明します。パフォーマンス上の理由のため、パスレンジインデックスの定義には XPath のサブセットしか使えません。

- [インデックスパス式の例](#)
- [インデックスパス式の制約](#)
- [インデックスパス式の有効性のテスト](#)
- [インデックスパス式での名前空間プレフィックスの使用](#)
- [インデックスパス式の文法](#)

26.4.1 インデックスパス式の例

次の表は、パスレンジインデックスの定義に有効および無効である XPath 式の例を示したものです。

注： 同じ要素 / 属性で終わるパスインデックスを複数作成することは避けてください。共通の要素 / 属性で終わるパスインデックスが多いほど、読み込みパフォーマンスが低下します。

有効	無効
//a	./a
/a/b/c	/a/b[c=/p/q]
/a/b[c]	/a/b[c=5+3]
/a/b[c=5 and b=3]	
/a/b[1]	
//a/b[c<5]	
//a/b[c="test"]	/a/b/concat(c,d) 関数呼び出しは許可されません。
/a/*/c	

有効	無効
a/b	
/a[./b]/c	/a[/b]/c
a	
/a/(b c)	/a/(/b /c)
	(/a/b/c) [2]
author[first-name="John"][last-name="Smith"]	
author[first-name="John" and last-name="Smith"]	
author[first-name="John" or first-name="Sam"]	
/a/b[./c]	/a/b/[./c]
/a/b[c]	/a/b[//c]
	/a/b[/a/b/c]
/a/(./b c)/d	/a(/a/b /a/c)/d
/a/child::*/*b	/a/parent::*/*b
/a[fn:matches(@expr, 'is')]	/a[fn:matches(fn:name(.), "Joe")]
/a[fn:contains("this")]	/a[fn:contains(fn:name(.), "Bob")]

名前空間プレフィックスは、有効なすべてのパス式で使用できます。パス式の一部として `fn:matches` と `fn:contains` も使用できますが、他の関数はパス式では使用できないことに注意してください。パス式がインデックスパスに有効かどうかをテストするには、`cts:valid-index-path` を使用します。

26.4.2 インデックスパス式の制約

XPath 機能によっては、パスレンジインデックスでサポートされないものもあります。この制約についてこのセクションで説明します。XPath 式は、『*XQuery and XSLT Reference Guide*』の「[XPath Quick Reference](#)」で概要が説明されています。XPath の詳細については、W3C XPath 2.0 言語リファレンス (<http://www.w3.org/TR/xpath20/>) を参照してください。

注： 同じ要素 / 属性で終わるパスインデックスを複数作成することは避けてください。共通の要素 / 属性で終わるパスインデックスが多いほど、読み込みパフォーマンスが低下します。

パスレンジインデックスを定義するために使用されるパス式は、次のルールに従う必要があります。

- 述語式で使用できる唯一の演算子は、比較演算子です (=、!=、<、<=、>=、>、eq、ne、lt、le、ge、gt)。
- 述語での比較の右オペランドには、文字列リテラル、数値リテラル、または文字列リテラルや数値リテラルのシーケンスだけを指定できます。
- パスステップでは前方軸だけを使用できます。つまり、self::、child::、descendant:: などの軸は使用できますが、parent::、ancestor::、preceding:: などの逆行軸は使用できません。詳細は、<http://www.w3.org/TR/xpath/#predicates> を参照してください。
- フラグメントルートをもたぐことはできません。パスは、フラグメントルート内に範囲を定める必要があります。
- パスステップでは、名前なしノードを使用できません。例えば、JSON を扱うときには、node() や array-node() などのパスステップを含められません。node('a') などの名前付きノードを使用できます。

その他の制約が適用されることがあります。cts:valid-index-path を使用して、パスレンジインデックスの定義に XPath 式を使用できるかどうかをテストできます。詳細については、「インデックスパス式の有効性のテスト」(364 ページ) を参照してください。

JSON ドキュメントの場合、数値、ブール値、およびヌル値に個別にインデックスが付けられ、すべてテキストとしては扱われないことに注意してください。JSON ドキュメントでの XPath 式の構成の詳細については、『*Application Developer's Guide*』の「[Traversing JSON Documents Using XPath](#)」を参照してください。

26.4.3 インデックスパス式の有効性のテスト

XQuery 関数 cts:valid-index-path を使用して、パスレンジインデックスの定義に XPath 式を使用できるかどうかをテストできます。有効性をテストするには、クエリコンソールに次のクエリをコピーし、自分のパス式に修正して実行します。

```
xquery version "1.0-ml";
cts:valid-index-path("/a/b", fn:true())
```

2 番目のパラメータを使用して、その名前空間バインド定義が、パス式で使用される名前空間プレフィックスに対して設定されていることを検証するかどうかを制御します。

26.4.4 インデックスパス式での名前空間プレフィックスの使用

XML 名前空間プレフィックスは、すべての有効なパスレンジインデックス式で使用できますが、データベース設定で名前空間バインドを定義する必要があります。例えば、パス式が /ns:a/ns:b である場合、プレフィックス ns の名前空間バインドを設定する必要があります。

名前空間バインドを事前定義するには、管理画面でデータベースの [Path Namespaces configuration] ページを使用するか、XQuery 関数 `admin:database-add-path-namespace` を使用します。

詳細については、「パスレンジインデックスの定義」(373 ページ) を参照してください。

26.4.5 インデックスパス式の文法

大部分のユーザーは、「インデックスパス式の例」(362 ページ) の例と

`cts:valid-index-path` に基づいて、有効なパスレンジインデックス式を作成する必要があります。

このセクションには、上級ユーザー向けに、パスレンジインデックス定義で使用可能な XPath のサブセットの文法が BNF 形式で含まれています。文法は、W3C XML パス言語規格に基づいています。詳細については、<http://www.w3.org/TR/xpath/> を参照してください。

```

IndexPathExpr ::= (PathExpr)* (( "/" | "//" ) LeafExpr Predicates)
LeafExpr ::= "(" UnionExpr ")" | LeafStep
PathExpr ::= ("/" RelativePathExpr?) | ("//" RelativePathExpr) |
RelativePathExpr
RelativePathExpr ::= UnionExpr | "(" UnionExpr ")"
UnionExpr ::= GeneralStepExpr ("|" GeneralStepExpr)*
GeneralStepExpr ::= ("/" | "//")? StepExpr (( "/" | "//")? StepExpr)*
StepExpr ::= ForwardStep Predicates
ForwardStep ::= (ForwardAxis AbbreviatedForwardStep) |
AbbreviatedForwardStep
AbbreviatedForwardStep ::= "." | ("@" NameTest) | NameTest
LeafStep ::= ("@" QName) | QName
NameTest ::= QName | Wildcard
Wildcard ::= "*" | "<" NCName ":" "*" ">" | "<" "*" ":" NCName ">"
QName ::= PrefixedName | UnprefixedName
PrefixedName ::= Prefix ":" LocalPart
UnprefixedName ::= LocalPart
Prefix ::= NCName
LocalPart ::= NCName
NCName ::= Name - (Char* ":" Char*) /* An XML Name, minus the ":" */
Name ::= NameStartChar (NameChar)*
Predicates ::= Predicate*
Predicate ::= PredicateExpr | "[" Digit+ "]"
Digit ::= [0-9]
PredicateExpr ::= "[" PredicateExpr "and" PredicateExpr "]" | "["
PredicateExpr "or" PredicateExpr "]" | "[" ComparisonExpr "]"
ComparisonExpr ::= RelativePathExpr GeneralComp SequenceExpr |
RelativePathExpr ValueComp Literal | PathExpr
GeneralComp ::= "=" | "!=" | "<" | "<=" | ">" | ">="
ValueComp ::= "eq" | "ne" | "lt" | "le" | "gt" | "ge"
SequenceExpr ::= Literal+
Literal ::= NumericLiteral | StringLiteral

```

図で文法を確認したほうが簡単と思われる場合、上記の BNF を、BNF から「ルールロードダイアグラム」を生成する多くのツール (<http://bottlecaps.de/rr/ui> など) で問題なく使用できます。

26.5 要素レンジインデックス設定の表示

読み込まれるか再インデックス付けされたときにドキュメントに適用される要素レンジインデックスを表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、表示するレンジインデックスを持つデータベースを特定します。
3. レンジインデックスを表示するデータベースの名前をクリックします。
4. [Element Range Indexes] アイコンをクリックします。

[Element Index Configuration] ページが表示されます。

26.6 要素レンジインデックスの定義

XML 要素または JSON プロパティのレンジインデックスを定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、レンジインデックスを作成するデータベースを特定します。
3. レンジインデックスを作成するデータベースの名前をクリックします。
4. 選択したデータベースの下で、ツリーメニューの [Element Range Indexes] アイコンをクリックします。

5. [Add] タブをクリックします。[Add Element Range Indexes] ページが表示されます。

The screenshot shows the 'Add Element Range Indexes' dialog box. The 'Add' tab is selected. The dialog contains the following fields and options:

- scalar type:** A dropdown menu with 'int' selected. Below it is the text 'An atomic type specification.'
- namespace uri:** An empty text input field. Below it is the text 'A namespace URI.'
- localname:** An empty text input field. Below it is the text 'One or more localnames.'
- range value positions:** Two radio buttons, 'true' and 'false'. The 'false' radio button is selected. Below it is the text 'Index range value positions for faster near searches involving range queries (slower document loads and larger database files).'
- invalid values:** A dropdown menu with 'reject' selected. Below it is the text 'Allow ingestion of documents that do not have matching type of data.'

At the bottom of the dialog, there is a 'more items' button and 'ok' and 'cancel' buttons.

6. レンジインデックスを構築する XML 要素または JSON プロパティのタイプを選択します。
7. インデックスが `xs:string` 型である場合、コレーションボックスがデフォルトのコレーションとともに表示されます。デフォルト以外のコレーションをインデックスで使用する場合、コレーション URI を入力します。入力した言語とその他のパラメータに基づいてユーザーの代わりにコレーション URI を構築するウィザードの [Collation Builder] ボタンをクリックできます。コレーションの詳細については、『*Search Developer's Guide*』の「[Language Support in MarkLogic Server](#)」の章を参照してください。
8. XML 要素の名前空間 URI を入力します。JSON プロパティインデックスについてはこの手順をスキップします。

XML 要素はすべて、名前空間と関連付けられます。要素を厳密に区別するために、XML 要素に名前空間を指定します。名前空間の独立性を表すために、アスタリスク (*) を使用することはできません。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

9. 要素または JSON プロパティ名を [localname] フィールドに入力します。

ローカル名は、インデックスを付ける XML 要素の名前です。インデックスを付ける同じタイプの要素が同じ名前空間に複数存在する場合、要素名をカンマ区切りで入力します。
10. このインデックスのレンジ値の位置にインデックスを付けるかどうかを選択します。[range value positions] を [true] に設定すると、このインデックスとともに `cts:near-query` と `cts:element-query` を使用した検索のパフォーマンスは高速化しますが、位置をオフのままにした場合 ([range value positions] を [false] に設定) よりも多くのディスク容量を使用します。
11. [invalid values] フィールドで、レンジインデックスが設定される要素または JSON プロパティを含んでいるが、これらの要素の値をインデックスのデータ型に強制的に設定できないドキュメントの挿入を許可するかどうかを選択します。これは [ignore] または [reject] のどちらかに設定できます。デフォルトでは、サーバーはこのようなドキュメントの挿入を拒否します。ただし、無効な値を [ignore] に設定した場合、無効な要素または JSON プロパティ値を含むドキュメントを挿入できますが、無効な値にはインデックスが付けられません。主にレンジインデックスを利用して動作するレンジクエリとレキシコン関数は、データベース内のこのようなドキュメントの存在を無視します。
12. さらにインデックスを追加するには、[more items] ボタンをクリックして、必要に応じてそれぞれのインデックスに対してステップ 6 からステップ 11 を繰り返します。
13. 上部または下部までスクロールして [ok] をクリックします。

新しい要素レンジインデックスまたは要素ワードレキシコンが、データベースに追加されます。これらのルールは、この時点以降、指定のデータベースに読み込まれた XML および JSON ドキュメントに適用されます。

注： データベースに対して再インデックス付けを有効にしており、ドキュメントに存在する要素を指定した場合、再インデックス付けがバックグラウンドで実行されます。再インデックス付けが完了すると、新しいインデックスがクエリで使用できるようになります。

26.7 属性レンジインデックス設定の表示

読み込まれるか再インデックス付けされたときにドキュメントに適用される属性レンジインデックスを表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、レンジインデックスを表示するデータベースを特定します。
3. レンジインデックスを表示するデータベースの名前をクリックします。
4. 選択したデータベースの下で、ツリーメニューの [Attribute Range Indexes] アイコンをクリックします。

[Attribute Range Index Configuration] ページが表示されます。

26.8 属性レンジインデックスの定義

特定の要素の属性に対してレンジインデックスを定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、インデックスを作成するデータベースを特定します。
3. インデックスを作成するデータベースの名前をクリックします。
4. 選択したデータベースの下で、属性レンジインデックスのツリーメニューの [Attribute Range Indexes] アイコンをクリックします。
5. [Add] タブをクリックします。[Add Attribute Range Indexes] ページが表示されます。

The screenshot shows the 'Add Attribute Range Indexes' dialog box. The title bar includes 'Add Attribute Range Indexes' and tabs for 'Configure', 'Add', and 'Help'. The 'Add' tab is active. The dialog contains the following fields and options:

- scalar type:** A dropdown menu set to 'int'. Below it is the text: 'An atomic type specification.'
- parent namespace uri:** A text input field. Below it is the text: 'A parent element namespace URI.'
- parent localname:** A text input field. Below it is the text: 'One or more parent element localnames.'
- namespace uri:** A text input field. Below it is the text: 'A namespace URI.'
- localname:** A text input field. Below it is the text: 'One or more localnames.'
- range value positions:** Radio buttons for 'true' and 'false'. 'false' is selected. Below it is the text: 'Index range value positions for faster near searches involving range queries (slower document loads and larger database files).'
- invalid values:** A dropdown menu set to 'reject'. Below it is the text: 'Allow ingestion of documents that do not have matching type of data.'

At the bottom of the dialog, there is a 'more items' button and 'ok' and 'cancel' buttons.

6. 属性レンジインデックスを構築する XML 属性のタイプを選択します。

7. インデックスが `xs:string` 型である場合、コレーションボックスがデフォルトのコレーションとともに表示されます。デフォルト以外のコレーションをインデックスで使用する場合、コレーション URI を入力します。入力した言語とその他のパラメータに基づいてユーザーの代わりにコレーション URI を構築するウィザードの [Collation Builder] ボタンをクリックできます。コレーションの詳細については、『*Search Developer's Guide*』の「[Language Support in MarkLogic Server](#)」の章を参照してください。
8. [parent namespace uri] フィールドに、インデックスを付ける属性を含んだ XML 要素の名前空間 URI を入力します。

XML 要素はすべて、名前空間と関連付けられます。要素を厳密に区別するために、XML 要素に名前空間を指定します。名前空間の独立性を表すために、アスタリスク (*) を使用することはできません。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

9. [parent localname] フィールドに要素名を入力します。

ローカル名は、インデックスを付ける属性を含んだ XML 要素の名前です。インデックスを付ける属性を含んだ要素が同じ名前空間に複数存在する場合、要素名をカンマ区切りで入力します。

10. [namespace uri] フィールドに、インデックスを付ける属性の名前空間 URI を入力します。

すべての XML 属性は名前空間と関連付けられています。属性を厳密に区別するために、XML 属性の名前空間を指定します。名前空間の独立性を表すために、アスタリスク (*) を使用することはできません。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

11. [localname] フィールドに属性名を入力します。

ローカル名は、インデックスを付ける XML 属性の名前です。インデックスを付ける属性が指定された親要素内の同一の名前空間に複数存在する場合、属性名をカンマ区切りで入力します。

12. このインデックスのレンジ値の位置にインデックスを付けるかどうかを選択します。この値を [true] に設定すると、このインデックスとともに `cts:near-query` と `cts:element-query` を使用した検索のパフォーマンスは高速化しますが、位置をオフのままにした場合 ([range value positions] を [false] に設定) よりも多くのディスク容量を使用します。

13. [invalid values] フィールドで、レンジインデックスが設定される属性を含んでいるが、これらの要素の値をインデックスのデータ型に強制的に設定できないドキュメントの挿入を許可するかどうかを選択します。これは [ignore] または [reject] のどちらかに設定できます。デフォルトでは、サーバーはこのようなドキュメントの挿入を拒否します。ただし、無効な値を [ignore] に設定した場合、無効な属性を含むドキュメントを挿入できますが、無効な属性値にはインデックスが付けられません。主にレンジインデックスを利用して動作するレンジクエリとレキシコン関数は、データベース内のこのようなドキュメントの存在を無視します。
14. さらにインデックスを追加するには、[more items] ボタンをクリックして、必要に応じてそれぞれの属性インデックスに対してステップ 6 からステップ 13 を繰り返します。
15. 上部または下部までスクロールして [ok] をクリックします。

新しい属性インデックスがデータベースに追加されます。これらのルールは、この時点で降に指定のデータベースに読み込まれた XML ドキュメントに適用されます。

注： データベースに対して再インデックス付けを有効にしており、ドキュメントに存在する要素と属性のペアを指定した場合、再インデックス付けがバックグラウンドで実行されます。再インデックス付けが完了すると、新しいインデックスがクエリで使用できるようになります。

26.9 パスレンジインデックス設定の表示

読み込まれるか再インデックス付けされたときにドキュメントに適用されるパスレンジインデックスを表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、レンジインデックスを表示するデータベースを特定します。
3. レンジインデックスを表示するデータベースの名前をクリックします。
4. 選択したデータベースの下で、ツリーメニューの [Path Range Indexes] アイコンをクリックします。

[Path Range Index Configuration] ページが表示されます。

26.10 パスレンジインデックスおよびフィールドで使用される名前空間プレフィックスの定義

XML ドキュメントに対してパスレンジインデックスを定義し、パスで名前空間プレフィックスを使用する場合は、パス式で使用される名前空間バインドを事前に定義しておく必要があります。これらの名前空間バインドは、複数のパスレンジインデックスで使用できます。

名前空間バインドを定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、名前空間プレフィックスバインドを作成するデータベースを特定します。
3. 名前空間バインドを作成するデータベースの名前をクリックします。
4. 選択したデータベースの下で、ツリーメニューの [Path Namespaces] アイコンをクリックします。
5. [Add] タブをクリックします。[Path Namespaces Configuration] ページが表示されます。

The screenshot shows a web-based configuration interface titled "Path Namespaces Configuration". It features three tabs: "Configure", "Add", and "Help". The "Add" tab is selected. Below the tabs are "ok" and "cancel" buttons. The main content area is titled "Add Namespaces" and contains two input fields. The first field is labeled "prefix" and contains the text "my". Below this field is a red error message: "Required. You must supply a value for prefix." The second field is labeled "namespace uri" and contains the text "http://aaa.com". Below the "Add Namespaces" section is a "more items" button. At the bottom of the dialog are "ok" and "cancel" buttons.

6. [prefix] フィールドに、パスレンジインデックスの XPath 式で要素または属性に使用する予定の名前空間プレフィックスを入力します。
7. [namespace uri] フィールドに、XPath 式の XML 要素または属性の名前空間 URI を入力します。
8. [ok] をクリックします。

26.11 パスレンジインデックスの定義

XPath 式で表されるレンジインデックスを定義するには、次の手順を実行します。

1. XML データに対してパスレンジインデックスを作成する場合、インデックス XPath 式で使用するすべての名前空間プレフィックスのバインドを作成します。詳細については、「パスレンジインデックスおよびフィールドで使用される名前空間プレフィックスの定義」(372 ページ) を参照してください。
2. 左側のツリーメニューで [Databases] アイコンをクリックします。
3. ツリーメニューまたは [Database Summary] テーブルで、レンジインデックスを作成するデータベースを特定します。
4. レンジインデックスを作成するデータベースの名前をクリックします。
5. 選択したデータベースの下で、ツリーメニューの [Path Range Indexes] アイコンをクリックします。
6. [Add] タブをクリックします。[Path Range Index Configuration] ページが表示されます。

The screenshot shows the 'Add Path Range Indexes' configuration dialog. The 'Add' tab is selected. The dialog contains the following fields and options:

- scalar type:** A dropdown menu set to 'string'. Below it is the text: 'An atomic type specification.'
- path expression:** A text input field containing '/my:a[his:b="B1"]/my:c'. Below it is the text: 'The path expression. For example:./prefix1:locname1/prefix2:locname2...'
- collation:** A text input field containing 'http://marklogic.com/collation/' and a dropdown menu set to 'Root Collation'. Below the input field is a button labeled 'collation builder' and the text: 'A collation URI for string comparisons.'
- range value positions:** Two radio buttons, 'true' and 'false'. The 'false' radio button is selected. Below it is the text: 'Index range value positions for faster near searches involving range queries (slower document loads and larger database files).'
- invalid values:** A dropdown menu set to 'reject'. Below it is the text: 'Allow ingestion of documents that do not have matching type of data.'

At the top right of the dialog are 'ok' and 'cancel' buttons. At the bottom left is a 'more items' button. At the bottom center are 'ok' and 'cancel' buttons.

7. レンジインデックスを構築する XML 要素、XML 属性、または JSON プロパティのタイプを選択します。
8. インデックスが `xs:string` 型である場合、コレクションボックスがデフォルトのコレクションとともに表示されます。デフォルト以外のコレクションをインデックスで使用する場合、コレクション URI を入力します。入力した言語とその他のパラメータに基づいてユーザーの代わりにコレクション URI を構築するウィザードの [Collation Builder] ボタンをクリックできます。コレクションの詳細については、『*Search Developer's Guide*』の「[Language Support in MarkLogic Server](#)」の章を参照してください。
9. [path expression] フィールドに XPath 式を入力します。XML の場合、ステップ 1 で作成した任意の名前空間プレフィックスを使用できます。XPath 式については、『*XQuery and XSLT Reference Guide*』の「[XPath Quick Reference](#)」で概要が説明されています。XPath 機能によっては、パスレンジインデックスでサポートされないものもあります。詳細については、「パスレンジインデックスについて」(362 ページ) を参照してください。

注： `cts:valid-index-path` 関数を使用して、パスのシンタックスが正しく、パスレンジインデックスで使用できるかどうかをテストできます。

注： パスは、フラグメントルートをもたぐことはできません。パスは、フラグメントルート内に範囲を定める必要があります。
10. このインデックスのレンジ値の位置にインデックスを付けるかどうかを選択します。[range value positions] を [true] に設定すると、このインデックスとともに `cts:near-query`、`cts:element-query`、および `cts:json-property-scope-query` を使用する検索のパフォーマンスが高速化しますが、位置をオフのままにした場合 ([range value positions] を [false] に設定) よりも多くのディスク容量を使用します。
11. [invalid values] フィールドで、レンジインデックスが設定される XML 要素、XML 属性または JSON プロパティを含んでいるが、これらの要素、属性またはプロパティの値をインデックスのデータ型に強制的に設定できないドキュメントの挿入を許可するかどうかを選択します。これは [ignore] または [reject] のどちらかに設定できます。デフォルトでは、サーバーはこのようなドキュメントの挿入を拒否します。ただし、無効な値を `ignore` に設定した場合、このような無効な属性を含むドキュメントを挿入できますが、無効な値にはインデックスが付けられません。主にレンジインデックスを利用して動作するレンジクエリとレキシコン関数は、データベース内のこのようなドキュメントの存在を無視します。
12. さらにインデックスを追加するには、[more items] ボタンをクリックして、必要に応じてそれぞれのインデックスに対してステップ 7 からステップ 11 を繰り返します。

13. 上部または下部までスクロールして [ok] をクリックします。

新しいパスレンジインデックスがデータベースに追加されます。これらのルールは、この時点以降、指定のデータベースに読み込まれた XML または JSON ドキュメントに適用されます。

注： データベースに対して再インデックス付けを有効にしており、ドキュメントに存在する XML 要素、XML 属性、または JSON プロパティを指定した場合、再インデックス付けがバックグラウンドで実行されます。再インデックス付けが完了すると、新しいインデックスがクエリで使用できるようになります。

注： パスレンジインデックスを作成した後では、パス式は変更できません。変更する場合は、既存のパスレンジインデックスを削除して、更新したパス式で新しいパスレンジインデックスを作成する必要があります。

26.12 要素ワードレキシコン設定の表示

読み込まれるか再インデックス付けされたときにドキュメントに適用されるレキシコンを表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、表示するレンジインデックスまたはレキシコンを持つデータベースを特定します。
3. レキシコンを表示するデータベースの名前をクリックします。
4. [Element Word Lexicons] アイコンをクリックします。

[Element Word Lexicon Configuration] ページが表示されます。

26.13 要素ワードレキシコンの定義

XML 要素または JSON プロパティのレキシコンを定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、レキシコンを作成するデータベースを特定します。
3. レキシコンを作成するデータベースの名前をクリックします。
4. 選択したデータベースの下で、ツリーメニューの [Element Word Lexicons] アイコンをクリックします。
5. [Add] タブをクリックします。[Element Word Lexicon Configuration] ページが表示されます。

The screenshot shows the 'Element Word Lexicon Configuration' dialog box. The 'Add' tab is selected. The dialog is titled 'Add Element Word Lexicons to Database'. It contains three input fields: 'namespace uri' with a text box and the description 'A namespace URI.'; 'localname' with a text box and the description 'One or more localnames. Required. You must supply a value for localname.'; and 'collation' with a text box containing 'http://marklogic.com/collation/' and a dropdown menu set to 'Root Collation'. Below the 'collation' text box is a 'collation builder' button and the description 'A collation URI for string comparisons.' At the bottom of the main area is a 'more items' button. At the bottom of the dialog are 'ok' and 'cancel' buttons.

6. XML 要素に関するレキシコンを定義する場合は、XML 要素の名前空間 URI を入力します。

XML 要素はすべて、名前空間と関連付けられます。要素を厳密に区別するために、XML 要素に名前空間を指定します。名前空間の独立性を表すために、アスタリスク (*) を使用することはできません。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

7. XML 要素または JSON プロパティ名を [localname] フィールドに入力します。

ローカル名は、インデックスを付ける XML 要素または JSON プロパティの名前です。インデックスを付ける同じタイプの要素が同じ名前空間に複数存在しているか、複数のプロパティ名が存在している場合、名前をカンマ区切りで入力します。
8. コレクションボックスがデフォルトのコレクションとともに表示されます。デフォルト以外のコレクションをレキシコンで使用する場合は、コレクション URI を入力します。入力した言語とその他のパラメータに基づいてユーザーの代わりにコレクション URI を構築するウィザードの [Collation Builder] ボタンをクリックできます。コレクションの詳細については、『*Search Developer's Guide*』の「[Language Support in MarkLogic Server](#)」の章を参照してください。
9. さらにワードレキシコンを追加するには、[more items] ボタンをクリックして、必要に応じてそれぞれのレキシコンに対してステップ 6 からステップ 8 を繰り返します。
10. 上部または下部までスクロールして [ok] をクリックします。

新しいレンジインデックスまたはワードレキシコンが、データベースに追加されます。これらのルールは、この時点以降、指定のデータベースに読み込まれた XML または JSON ドキュメントに適用されます。

注： データベースに対して再インデックス付けを有効にしており、ドキュメントに存在する要素を指定した場合、再インデックス付けがバックグラウンドで実行されます。再インデックス付けが完了すると、新しいインデックスがクエリで使用できるようになります。

26.14 属性ワードレキシコン設定の表示

読み込まれるか再インデックス付けされたときにドキュメントに適用されるレキシコンを表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、レキシコンを表示するデータベースを特定します。
3. レキシコンを表示するデータベースの名前をクリックします。
4. 選択したデータベースの下で、ツリーメニューの [Attribute Word Lexicons] アイコンをクリックします。

[Element-Attribute Word Lexicon] ページが表示されます。

26.15 属性ワードレキシコンの定義

特定の要素の属性に対してレキシコンを定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、レキシコンを作成するデータベースを特定します。
3. レキシコンを作成するデータベースの名前をクリックします。
4. 選択したデータベースの下で、[Attribute Word Lexicon] アイコンをクリックします。
5. [Add] タブをクリックします。[Element-Attribute Word Lexicon Configuration] ページが表示されます。

The screenshot shows the 'Element-Attribute Word Lexicon Configuration' dialog box. The 'Add' tab is selected. The dialog is titled 'Add Element Attribute Word Lexicons to Database'. It contains the following fields and controls:

- parent namespace uri**: Text input field. Description: A parent element namespace URI.
- parent localname**: Text input field. Description: One or more parent element localnames. Error message: Required. You must supply a value for parent-localname.
- namespace uri**: Text input field. Description: A namespace URI.
- localname**: Text input field. Description: One or more localnames. Error message: Required. You must supply a value for localname.
- collation**: Text input field containing 'http://marklogic.com/collation/' and a dropdown menu set to 'Root Collation'. Below it is a 'collation builder' button. Description: A collation URI for string comparisons.

At the bottom of the dialog, there is a 'more items' button and 'ok' and 'cancel' buttons.

6. [parent namespace uri] フィールドに、インデックスを付ける属性を含んだ XML 要素の名前空間 URI を入力します。

XML 要素はすべて、名前空間と関連付けられます。要素を厳密に区別するために、XML 要素に名前空間を指定します。名前空間の独立性を表すために、アスタリスク (*) を使用することはできません。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

7. [parent localname] フィールドに要素名を入力します。

ローカル名は、インデックスを付ける属性を含んだ XML 要素の名前です。インデックスを付ける属性を含んだ要素が同じ名前空間に複数存在する場合、要素名をカンマ区切りで入力します。

8. [namespace uri] フィールドに、インデックスを付ける属性の名前空間 URI を入力します。

すべての XML 属性は名前空間と関連付けられています。属性を厳密に区別するために、XML 属性の名前空間を指定します。名前空間の独立性を表すために、アスタリスク (*) を使用することはできません。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

9. [localname] フィールドに属性名を入力します。

ローカル名は、インデックスを付ける XML 属性の名前です。インデックスを付ける属性が指定された親要素内の同一の名前空間に複数存在する場合、属性名をカンマ区切りで入力します。

10. コレクションボックスがデフォルトのコレクションとともに表示されます。デフォルト以外のコレクションをレキシコンで使用する場合は、コレクション URI を入力します。入力した言語とその他のパラメータに基づいてユーザーの代わりにコレクション URI を構築するウィザードの [Collation Builder] ボタンをクリックできます。コレクションの詳細については、『*Search Developer's Guide*』の「[Language Support in MarkLogic Server](#)」の章を参照してください。

11. さらに要素 - 属性ワードレキシコンを追加するには、[more items] ボタンをクリックして、必要に応じてそれぞれの属性インデックスに対してステップ 6 からステップ 10 を繰り返します。

12. 上部または下部までスクロールして [ok] をクリックします。

新しい属性インデックスまたは属性ワードレキシコンが、データベースに追加されます。これらのルールは、この時点以降に指定のデータベースに読み込まれた XML ドキュメントに適用されます。

注： データベースに対して再インデックス付けを有効にしておき、ドキュメントに存在する要素と属性のペアを指定した場合、再インデックス付けがバックグラウンドで実行されます。再インデックス付けが完了すると、新しいインデックスがクエリで使用できるようになります。

26.16 値レキシコンの定義

値レキシコンは、クエリ内で指定された要素、属性、JSON プロパティ、またはフィールドに関する `xs:string` 型のレンジインデックスを使用して実装されます。したがって、値レキシコンを作成するには、指定の要素、属性、JSON プロパティ、またはフィールドに対して `xs:string` 型のレンジインデックスを作成します。JSON プロパティ値レキシコンには要素レンジインデックスを使用します。

26.17 レンジインデックスまたはレキシコンの削除

特定のデータベースの要素または属性インデックス、あるいはレキシコンを削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] テーブルで、レンジインデックスまたはレキシコンを削除するデータベースを特定します。
3. レンジインデックスまたはレキシコンを削除するデータベースの名前をクリックします。
4. 要素レンジインデックス、属性レンジインデックス、要素ワードレキシコン、属性ワードレキシコンのどれを削除する必要があるのかを決定します。
5. [Element Range Index] アイコン、[Attribute Range Index] アイコン、[Path Range Index] アイコン、[Element Word Lexicon] アイコン、または [Attribute Word Lexicon] をクリックします。該当するインデックスの設定ページが表示されます。
6. 削除するインデックスを特定して、[delete] をクリックします。
7. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

インデックスまたはレキシコンがデータベースから削除されます。

26.18 フィールドレンジインデックスの定義

フィールドを使用すると、XML 要素の QName または JSON プロパティ名に基づいて、データベースの一部を簡単にクエリできます。フィールドを定義してから、それに対するレンジインデックスあるいはワードまたは値レキシコンを作成できます。詳細については、「データベースのフィールド設定」(140 ページ) を参照してください。

27.0 フラグメント

データベースにデータを読み込むときに、XML ドキュメントをフラグメントと呼ばれる小さな情報ブロックにパーティション化して（分割して）格納する方法を指定できます。大きな XML ドキュメントの場合、サイズが問題になることがあり、フラグメントの使用がシステムのパフォーマンスの管理に役立ちます。一般に、XML ドキュメントのフラグメントのサイズは 10K から 100K の間であることが望ましいです。フラグメントのサイズを非常に小さくまたは非常に大きく設定するとパフォーマンスが低下することがあるため、フラグメントのサイズを適切に設定することが重要です。

XML ドキュメントの実際のフラグメンテーションは、アプリケーション開発者に完全に透過的です。アプリケーションレベルでは、ドキュメントはディスク上でフラグメントとしてどのように格納および管理されているかには関係なく単一の一体構造として扱われます。フラグメンテーションは、アプリケーションに透過的なチューニングメカニズムです。

ただし、フラグメンテーションは関連度順に影響を与えます。関連度順アルゴリズムは、コンテンツの対象部分でのタームの出現頻度と、データベース全体でのタームの出現頻度の両方を考慮して、結果を関連度に応じてランク付けします。ランキングを行うために MarkLogic サーバーは XML ドキュメント全体でのタームの出現頻度を考慮するのではなく、ランク付けの対象の個々のフラグメント（およびその子孫）内でのタームの出現頻度を考慮します。その結果、フラグメンテーション方法が異なると関連度順に影響が及ぶ可能性があります。特に単一のフラグメントに、関連度に応じて区別しようとしている複数の XML 構造が含まれる場合に影響します。

MarkLogic サーバーでは、XML ドキュメントのパーティション化に使用されるフラグメンテーション「ルール」を指定します。これらのルールは一度に 1 つのドキュメントに適用されます。ただし、フラグメンテーションルールはデータベースレベルで指定されます。ここではデータベースに含まれる多数のドキュメントが同様の構造を持ち、同じフラグメンテーションルールが適用されると想定されています。

フラグメンテーションルールは、ドキュメントの読み込み、更新、およびデータベースの再インデックス付けの間にドキュメントに適用されます。ドキュメントが読み込まれた後に追加のフラグメンテーションルールを指定した場合、これらのドキュメントのそれ以降の更新や再インデックス付けでは新しいフラグメンテーションルールが使用されますが、既存のドキュメントのフラグメンテーションは変更されません（ただし、`[reindex enable]` が `[true]` に設定されている場合は、ドキュメントは最終的に再インデックス付けされ、新しいフラグメンテーションポリシーが適用されます）。結果として、すでに読み込まれているコンテンツのフラグメンテーションルールを変更する場合、新しいフラグメンテーションルールが有効になるように、ドキュメントを再度読み込むか、データベースを再インデックス付けする必要があります。

フラグメンテーションルールの管理には次の手順を使用します。

- [フラグメンテーション方針の選択](#)
- [フラグメントルートの定義](#)
- [フラグメントの親の定義](#)
- [フラグメントルールの表示](#)
- [フラグメントルールの削除](#)

27.1 フラグメンテーション方針の選択

適切なフラグメンテーションがパフォーマンスにとって重要です。読み込まれる XML データをフラグメント化する方法を指定する前に、フラグメンテーション方針を計画する必要があります。次のガイドラインが適用されます。

- フラグメントは、通常 XML 要素名を使用して記述されます。
- XML ドキュメントのフラグメントのサイズは、10K から 100K の間であることが望ましいです（これらは一般的なガイドラインに過ぎません。状況によっては、より大きなまたは小さなフラグメントサイズが相応しい場合あり、所定のフラグメントサイズのパフォーマンスに影響する要因は多数存在します。例えば、ディスクブロック、データベースに含まれるフラグメントの数、フラグメントへのアクセス頻度、アプリケーションで使用されるクエリのタイプなどが影響します）。
- フラグメントは階層的に入れ子構造にできます（多くの場合、その必要があります）。
- フラグメントサイズを小さくするほど、データベースでの要素レベルの更新を効率的に行えますが、フラグメントを過度に小さくすると、読み込み速度とクエリパフォーマンスの両方が低下する可能性があります。
- フラグメントを大きくした場合も、クエリの解決でディスクからデータの過度の読み込みが必要になるので、クエリパフォーマンスが低下することがあります。
- 一般に、上記のサイズ範囲であれば、フラグメントサイズが大きいほど、フラグメントサイズが小さい場合よりも全体的にパフォーマンスが高くなります。
- テキストとスモールバイナリドキュメントは、単一のフラグメントに収める必要があります。したがって、データベースの `in memory tree size` パラメータを、最もサイズの大きなテキストまたはスモールバイナリファイルよりも 1 から 2 MB 大きく設定してください。スモールバイナリファイルの最大サイズは、常に `large size threshold` データベース設定による制約を受けます。

データをフラグメント化する方法を決定したら、次のいずれかの方法を使用できます。

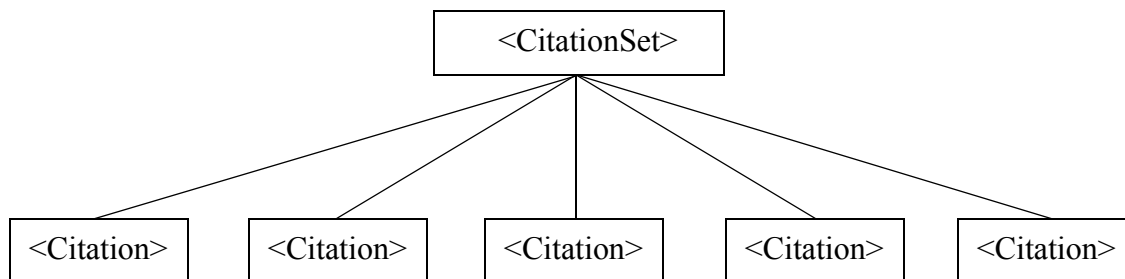
- [フラグメントルート](#)
- [フラグメントの親](#)

どちらの方法も、フラグメンテーション方針をシステムの具体的なルールに変換します。

27.1.1 フラグメントルート

共通の要素名を共有する XML 構造のインスタンスが多数ドキュメントに含まれている場合、これらの構造により適切なフラグメントが作成されます。MarkLogic サーバーでは、この共通の要素名をフラグメントルートとして使用できます。

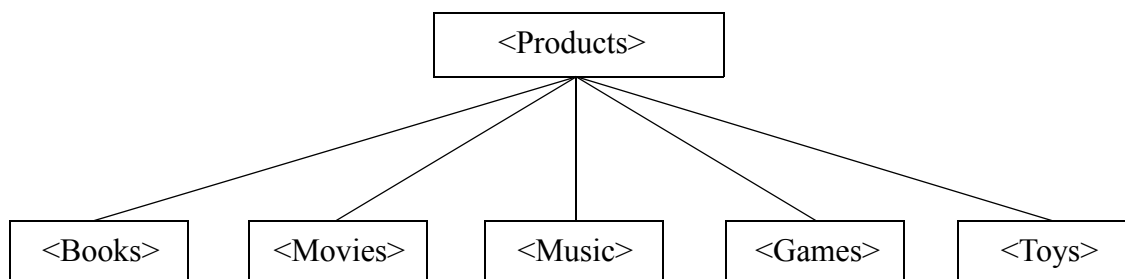
次の図は、<Citation> ノードの多くのインスタンスを含む <CitationSet> をルートとした XML ドキュメントを示したものです。それぞれの <Citation> ノードにはさらなる XML が含まれ、平均のサイズは 15K から 20K です。この情報に基づくと、<Citation> が、フラグメントルートとして使用する適切な要素になります。



27.1.2 フラグメントの親

ドキュメントにさまざまな XML 下位構造が多数含まれ、そのそれぞれがフラグメントの候補に適している場合、それぞれの下位構造をフラグメントルートに指定していると時間がかかります。その代わりに、名前とは無関係に、親の配下の下位構造すべてが個別のフラグメントになるように、これらの下位構造の親をフラグメントの親に設定することでフラグメントを指定できます。

次の図は、異なる名前の下位構造を持つドキュメントを示したものです。



この場合、<Products> 要素をフラグメントの親として使用でき、<Books>、<Movies>、<Music>、<Games>、および <Toys> という子が自動的にフラグメントになります。

27.2 フラグメントルートの定義

フラグメントルートのルールを定義するには、次の手順に従います。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. 新しいフラグメントルールを指定するデータベースを特定します。
3. ツリーメニューまたは [Database Summary] ページで、このデータベースのアイコンをクリックします。
4. [Fragment Roots] アイコンをクリックします。
5. [Create] タブをクリックします。[Fragment Roots Configuration] ページが表示されます。

The screenshot shows a dialog box titled "Create Fragment Roots" with three tabs: "Configure", "Create", and "Help". The "Create" tab is selected. The main content area is titled "Create Fragment Roots in Database" and contains two input fields: "namespace uri" and "localname". The "namespace uri" field has a placeholder text "A namespace URI." The "localname" field has a placeholder text "One or more localnames." and a red error message below it: "Required. You must supply a value for localname." There are "ok" and "cancel" buttons at the top right and bottom left of the dialog. A "more items" button is located below the input fields.

6. フラグメントルートのルールとして使用する XML 要素の名前空間 URI を入力します。

XML 要素はすべて、名前空間と関連付けられます。フラグメントルールが正確になるように、XML 要素の名前空間を指定する必要があります。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

または、[namespace uri] フィールドにアスタリスク (*) を入力することで、フラグメントルートのルールが名前空間に無関係であることを指定できます。

7. [localname] フィールドに要素名を入力します。

ローカル名は、フラグメントのルートとして使用される XML 要素の名前です。指定した名前空間に関連付けられたフラグメントルートルールが複数ある場合、要素名をカンマ区切りで入力します。

8. さらにフラグメントルートを追加するには、[more items] ボタンをクリックして、必要に応じてフラグメントルートごとにステップ 6 からステップ 7 を繰り返します。
9. 上部または下部までスクロールして [ok] をクリックします。

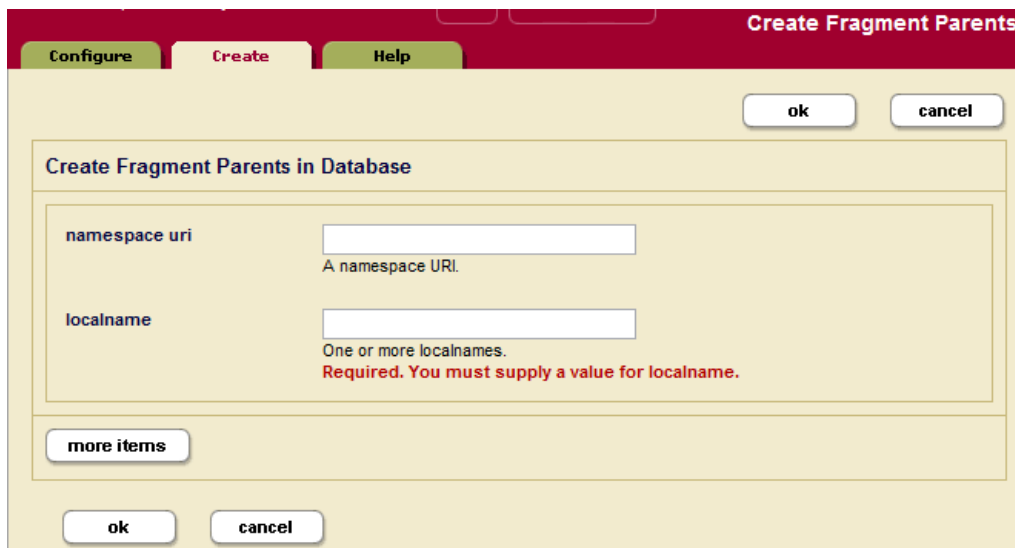
新しいフラグメントルートルールがデータベースに追加されます。これらのルールは、この時点以降に指定のデータベースに読み込まれた XML ドキュメントに適用されます。

27.3 フラグメントの親の定義

フラグメントの親のルールを定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. 新しいフラグメントの親を指定するデータベースを特定します。
3. ツリーメニューまたは [Database Summary] ページで、このデータベースのアイコンをクリックします。
4. [Fragment Parents] アイコンをクリックします。

5. [Create] タブをクリックします。[Create Fragment Parents] ページが表示されます。



6. フラグメントの親のルールとして使用する XML 要素の名前空間 URI を入力します。

XML 要素はすべて、名前空間と関連付けられます。フラグメントルールが正確になるように、XML 要素の名前空間を指定する必要があります。名前空間 URI のフィールドが空白の場合、ユニバーサルな無名の名前空間が割り当てられます。

または、[namespace uri] フィールドにアスタリスク (*) を入力することで、フラグメントルートのルールが名前空間に無関係であることを指定できます。

7. [localname] フィールドに要素名を入力します。

ローカル名は、子がフラグメントルートになる親の XML 要素の名前です。指定した名前空間に関連付けられたフラグメントの親のルールが複数ある場合、要素名をカンマ区切りで入力します。

8. さらにフラグメントの親を追加するには、[more items] ボタンをクリックして、必要に応じてフラグメントの親ごとにステップ 6 からステップ 7 を繰り返します。
9. 上部または下部までスクロールして [ok] をクリックします。

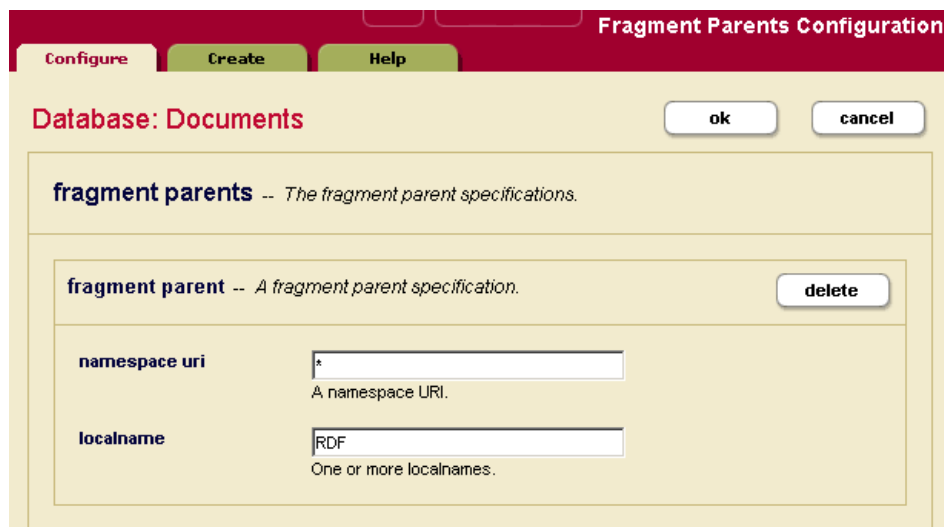
新しいフラグメントルールがデータベースに追加されます。これらのルールは、この時点以降に指定のデータベースに読み込まれた XML ドキュメントに適用されます。

27.4 フラグメントルールの表示

有効になっているフラグメントルールを表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] ページで、表示するフラグメントルールを含むデータベースを特定します。
3. このデータベースのアイコンをクリックします。
4. フラグメントルールのルールを表示するか、フラグメントの親のルールを表示するかを決定します。
5. 指定したデータベースの下で、[Fragment Roots] または [Fragment Parents] アイコンをクリックします。

次の例は、ドキュメントデータベースでフラグメントの親のルールが 1 つだけ定義されていることを示します。このルールは、<RDF> 要素の名前空間には関係なく、<RDF> 要素の直接の子がフラグメントのルートを形成することを示します。



27.5 フラグメントルールの削除

指定したデータベースのフラグメントルールを削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Databases] アイコンをクリックします。
2. ツリーメニューまたは [Database Summary] ページで、削除するフラグメントルールを含むデータベースを特定します。

3. このデータベースのアイコンをクリックします。
4. フラグメントルートのルールとフラグメントの親のルールのどちらを削除する必要があるかを決定します。
5. 指定したデータベースの下で、[Fragment Roots] または [Fragment Parents] アイコンをクリックします。
6. 削除するフラグメントルールを特定して、[delete] をクリックします。
7. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

フラグメントルールがグループから削除されます。

注： フラグメントルールを削除しても、データベースの再インデックス付けが有効になっていない限り、データベースに読み込まれたドキュメントにすでに適用されているフラグメンテーションには影響しません。

28.0 名前空間

名前空間は、複数の意味を持つ可能性がある XML 要素を区別するために使用される強力なメカニズムです。名前空間は、個々の XQuery プログラム内で定義できます。また、管理画面を使用して定義することもできます。

名前空間は、グループ内のすべての HTTP、ODBC、XDBC、および WebDAV サーバーに適用するように定義することも、特定の HTTP、ODBC、XDBC、または WebDAV サーバーに適用するように定義することもできます。ただし、名前空間は、特定のフォレスト、データベース、または XQuery プログラムに適用するには定義できません

名前空間の詳細については、『*XQuery and XSLT Reference Guide*』の名前空間に関する章を参照してください。ここでは XML 名前空間の詳細な説明とその使用法が記されています。管理画面を使用して名前空間を管理する前に、この情報を必ず確認してください。

管理画面で名前空間を管理するには、次の手順を使用してください。

- [グループの名前空間の定義](#)
- [HTTP、ODBC、または XDBC サーバーの名前空間の定義](#)
- [グループの名前空間設定の表示](#)
- [HTTP、ODBC、または XDBC サーバーの名前空間設定の表示](#)
- [グループの名前空間の削除](#)
- [HTTP、ODBC、または XDBC サーバーの名前空間の削除](#)

この章では、管理画面を使用して名前空間を管理する方法について説明します。名前空間をプログラムによって管理する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Group Maintenance Operations](#)」を参照してください。

28.1 グループの名前空間の定義

管理画面を使用してグループの名前空間を定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. ツリーメニューまたは [Groups Summary] ページで、名前空間を定義するグループをクリックします。
3. 左側のツリーメニューで、グループ名の下に [Namespaces] アイコンをクリックします。
4. [Add] タブをクリックします。[Namespaces Configuration] ページが表示されます。

The screenshot shows the 'Namespace Configuration' dialog box. It has a title bar with 'Namespace Configuration' and three tabs: 'Configure', 'Add', and 'Help'. The 'Add' tab is selected. Below the tabs are 'ok' and 'cancel' buttons. The main area is titled 'Add Namespaces' and contains two input fields: 'prefix' and 'namespace uri'. The 'prefix' field has a red error message: 'Required. You must supply a value for prefix.' Below the input fields is a 'more items' button. At the bottom of the dialog are 'ok' and 'cancel' buttons.

5. 名前空間のプレフィックスを入力します。
6. 名前空間の URI を入力します。

ユニバーサルな無名の名前空間のプレフィックスを定義している場合、URI は空白のままにしておきます。

7. さらに名前空間の定義を追加するには、[more items] ボタンをクリックして、必要に応じてそれぞれの名前空間に対してステップ 5 からステップ 6 を繰り返します。
8. 上部または下部までスクロールして [ok] をクリックします。

これでグループの名前空間が定義されました。

28.2 HTTP、ODBC、または XDBC サーバーの名前空間の定義

管理画面を使用して HTTP、ODBC、または XDBC サーバーの名前空間を定義するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. ツリーメニューまたは [Groups Summary] ページで、名前空間を定義する HTTP、ODBC、または XDBC サーバーを含むグループをクリックします。
3. 必要に応じて [App Servers] アイコンをクリックします。
4. 名前空間を定義するアプリケーションサーバーの名前をクリックします。
5. 左側のツリーメニューで、指定したアプリケーションサーバーの下の [Namespaces] アイコンをクリックします。
6. 右上の [Add] タブをクリックします。[Namespaces Configuration] ページが表示されます。

The screenshot shows a web-based dialog box titled "Namespace Configuration". It has three tabs: "Configure", "Add", and "Help". The "Add" tab is active. The main content area is titled "Add Namespaces" and contains two input fields. The first field is labeled "prefix" and has a red error message below it: "Required. You must supply a value for prefix." The second field is labeled "namespace uri" and has a description below it: "A namespace URI." Below the input fields is a button labeled "more items". At the bottom of the dialog are two buttons: "ok" and "cancel".

7. 名前空間のプレフィックスを入力します。
8. 名前空間の URI を入力します。

ユニバーサルな無名の名前空間のプレフィックスを定義している場合、URI は空白のままにしておきます。

- さらに名前空間の定義を追加するには、[more items] ボタンをクリックして、必要に応じてそれぞれの名前空間に対してステップ 7 からステップ 8 を繰り返します。
- 上部または下部までスクロールして [ok] をクリックします。

これでアプリケーションサーバーの名前空間が定義されました。

28.3 グループの名前空間設定の表示

管理画面で定義した名前空間を表示するには、次の手順を実行します。

- 左側のツリーメニューで [Groups] アイコンをクリックします。
- ツリーメニューまたは [Groups Summary] ページで、表示する名前空間を含むグループをクリックします。
- 左側のツリーメニューで、指定したグループの下の [Namespaces] アイコンをクリックします。[Namespace Configuration] ページが表示されます。

The screenshot shows a 'Namespace Configuration' dialog box. At the top, there are three tabs: 'Configure', 'Add', and 'Help'. Below the tabs are 'ok' and 'cancel' buttons. The main content area is titled 'namespaces -- The namespace binding specifications.' and contains a list of 'namespace -- A namespace binding specification.' with a 'delete' button. The 'prefix' field contains 'ml' and the 'namespace uri' field contains 'http://marklogic.com/ml'. Below the list are 'ok' and 'cancel' buttons.

28.4 HTTP、ODBC、または XDBC サーバーの名前空間設定の表示

管理画面で定義した名前空間を表示するには、次の手順を実行します。

- 左側のメニューツリーで [Groups] アイコンをクリックします。
- ツリーメニューまたは [Groups Summary] ページで、名前空間を表示する HTTP、ODBC、または XDBC サーバーを含むグループをクリックします。

3. 必要に応じて [App Servers] アイコンをクリックします。
4. 名前空間を表示するアプリケーションサーバーの名前をクリックします。
5. 左側のツリーメニューで、指定したアプリケーションサーバーの下の [Namespaces] アイコンをクリックします。[Namespace Configuration] ページが表示されます。

The screenshot shows the 'Namespace Configuration' dialog box. It features a title bar with 'Configure', 'Add', and 'Help' buttons. Below the title bar are 'ok' and 'cancel' buttons. The main content area displays a list of namespaces. The first entry is 'namespaces -- The namespace binding specifications.' Below it is a single entry 'namespace -- A namespace binding specification.' with a 'delete' button. The 'namespace' entry has two fields: 'prefix' with the value 'ml' and a description 'A QName prefix.', and 'namespace uri' with the value 'http://marklogic.com/ml' and a description 'A namespace URI.' At the bottom of the dialog are 'ok' and 'cancel' buttons.

28.5 グループの名前空間の削除

管理画面で定義した名前空間を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. ツリーメニューまたは [Groups Summary] ページで、名前空間を削除するグループをクリックします。
3. 左側のツリーメニューで、指定したグループの下の [Namespaces] アイコンをクリックします。
4. 削除する名前空間を特定して、[delete] をクリックします。
5. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

名前空間がグループから削除されます。

28.6 HTTP、ODBC、または XDBC サーバーの名前空間の削除

HTTP、ODBC、または XDBC サーバーに対して管理画面で定義した名前空間を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. ツリーメニューまたは [Groups Summary] ページで、名前空間を削除するアプリケーションサーバーを含むグループをクリックします。
3. [App Servers] アイコンをクリックします。
4. ツリーメニューまたは [App Server Summary] ページで、名前空間を削除するアプリケーションサーバーの名前をクリックします。
5. 左側のツリーメニューで、指定したアプリケーションサーバーの下の [Namespaces] アイコンをクリックします。[Namespace Configuration] 画面が表示されます。
6. 削除する名前空間を特定して、[delete] をクリックします。
7. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

名前空間がアプリケーションサーバーから削除されます。

29.0 スキーマの理解と定義

この章では、スキーマについて説明し、それを定義する手順を示します。次のトピックから構成されています。

- [スキーマについて](#)
- [スキーマの定義の手順](#)

スキーマデータベース、MarkLogic サーバーへのスキーマの読み込み、およびアプリケーションでのスキーマの使用の詳細については、『*Application Developer's Guide*』のスキーマの読み込みに関する章を参照してください。

29.1 スキーマについて

スキーマは、XML コンテンツのデータ辞書です。スキーマを指定するには、スキーマが適用される名前空間とスキーマファイルの場所を定義する必要があります。

スキーマは、XML ドキュメント内の要素のタイプを定義します。XML 要素のタイプを知ることが XQuery プログラムの評価に役立つ場合、MarkLogic サーバーは次の方法を使用して、(その要素の名前空間に基づいて) 関連するスキーマドキュメントを検索します。

1. XQuery プログラムが、対象の名前空間のスキーマを明示的に参照する場合、MarkLogic サーバーはこのリファレンスを使用します。
2. それ以外の場合、MarkLogic サーバーは、MarkLogic サーバーがタイプを特定しようとしている要素の名前空間とターゲット名前空間が同じ XML スキーマドキュメントをスキーマデータベースで検索します。
3. データベースでマッチするスキーマドキュメントが見つからない場合、MarkLogic サーバーはその `config` ディレクトリでマッチするスキーマドキュメントを検索します。
4. マッチするスキーマドキュメントが `config` ディレクトリに見つからない場合、スキーマは見つかりません。

MarkLogic サーバーがタイプを特定しようとしている要素の名前空間にターゲット名前空間がマッチするスキーマドキュメントがスキーマデータベースに複数ある場合は、上記のステップ 2 で問題が発生することがあります。この場合、管理画面を使用してデフォルトのマッピングを指定できると便利です。

スキーママッピングは、HTTP、ODBC、または XDBC サーバーに対して個別に指定することも、グループに対して指定して、そのグループ内のすべての HTTP、ODBC、または XDBC サーバーに適用することもできます。HTTP、ODBC、または XDBC サーバーに対して定義されているスキーママッピングが、グループに対して定義されているスキーママッピングと競合した場合、前者のマッピングが使用されます。

管理画面でスキーママッピングを指定した場合、MarkLogic サーバーは次の方法を使用してスキーマを特定します。

1. 初めに、MarkLogic サーバーは、スキーママッピングで指定した URI そのものを使用してドキュメントをスキーマデータベースで検索します。

注： HTTP、ODBC、または XDBC サーバーのスキーママッピングが、グループのスキーママッピングと競合した場合、前者のマッピングが使用されません。

2. マッチするスキーマドキュメントがスキーマデータベースに見つからない場合、MarkLogic サーバーは、指定した URI のファイル名部分にファイル名がマッチするスキーマドキュメントをその `config` ディレクトリで検索します。
3. マッチするスキーマドキュメントが `config` ディレクトリに見つからない場合、スキーマは見つかりません。

名前空間が、特定のデータベースに格納された 1 つあるいは複数のデータ要素によって呼び出され、その名前空間のスキーマがグループに対して、あるいは HTTP、ODBC、または XDBC サーバーに対して定義されている場合、MarkLogic サーバーはそのデータの格納、インデックス付け、および取得にそのスキーマを適用します。

注： この場合のスキーマデータベースは、データが存在するデータベースのスキーマデータベースです。

29.2 スキーマの定義の手順

スキーマの定義には次の手順を使用します。

- [グループのスキーマ定義の追加](#)
- [HTTP、ODBC、または XDBC サーバーのスキーマ定義の追加](#)
- [グループのスキーマ定義の表示](#)
- [HTTP、ODBC、または XDBC サーバーのスキーマ定義の表示](#)
- [グループのスキーマ定義の削除](#)
- [HTTP、ODBC、または XDBC サーバーのスキーマ定義の削除](#)

29.2.1 グループのスキーマ定義の追加

スキーマをグループ内のすべての HTTP、ODBC、または XDBC サーバーで利用できるようにするには、次の手順に従います。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. スキーマを定義するグループをクリックします。
3. 左側のツリーメニューで、指定したグループの下の [Schemas] アイコンをクリックします。
4. [Add] タブをクリックします。[Schema Configuration] ページが表示されます。

5. 名前空間 URI および対応するスキーマの場所を入力します。

`Config` ディレクトリにスキーマを格納する予定の場合は、次の表に、各プラットフォームでの `Config` ディレクトリのデフォルトの場所が示されています。

プラットフォーム	スキーマディレクトリ
Microsoft Windows	C:\Program Files\MarkLogic\Config
Red Hat Linux	/opt/MarkLogic/Config
Mac OS X	~/Library/MarkLogic/Config/

6. スキーマ定義を追加するには、[more items] ボタンをクリックし、必要に応じて他のスキーマについてステップ 5 を繰り返します。
7. 上部または下部までスクロールして [ok] をクリックします。

スキーマがグループに追加されます。

29.2.2 HTTP、ODBC、または XDBC サーバーのスキーマ定義の追加

スキーマを特定の HTTP、ODBC、または XDBC サーバーで利用できるようにするには、次の手順を行います。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. スキーマを追加する HTTP、ODBC、または XDBC サーバーを含んだグループの名前をクリックします。
3. [App Servers] アイコンをクリックします。
4. スキーマを追加するアプリケーションサーバーの名前をクリックします。
5. 左側のツリーメニューで、指定したアプリケーションサーバーの下で [Schemas] アイコンをクリックします。
6. [Add] タブをクリックします。[Schema Configuration] ページが表示されます。

The screenshot shows the 'Schema Configuration' dialog box with the 'Add' tab selected. The dialog contains two input fields: 'namespace uri' and 'schema location'. Below these fields is a 'more items' button. At the bottom of the dialog are 'ok' and 'cancel' buttons.

- 名前空間 URI および対応するスキーマの場所を入力します。

Config ディレクトリにスキーマを格納する予定の場合は、使用するプラットフォームでの Config ディレクトリのデフォルトの場所について次の表を参照してください。

プラットフォーム	スキーマディレクトリ
Microsoft Windows	C:\Program Files\MarkLogic\Config
Red Hat Linux	/opt/MarkLogic/Config
Mac OS X	~/Library/MarkLogic/Config/

- スキーマ定義を追加するには、[more items] ボタンをクリックし、必要に応じて他のスキーマについてステップ 7 を繰り返します。
- 上部または下部までスクロールして [ok] をクリックします。

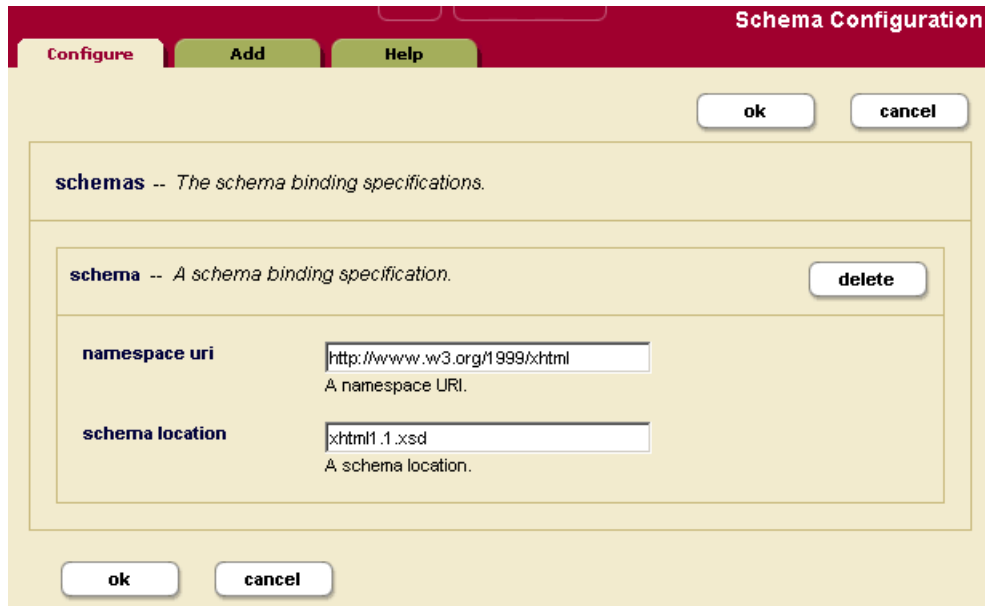
スキーマは HTTP、ODBC、または XDBC サーバーに追加されます。

29.2.3 グループのスキーマ定義の表示

グループのスキーマ定義を表示するには、次の手順に従います。

- 左側のツリーメニューで [Groups] アイコンをクリックします。
- 表示するスキーマを含んだグループをクリックします。
- 左側のツリーメニューで、指定したグループの下の [Schemas] アイコンをクリックします。

次の例は、1つのスキーマだけを表示します。これは、名前空間 <http://www.w3.org/1999/xhtml> のスキーマがファイル `xhtml.1.xsd` にあることを指定します。このファイルは MarkLogic サーバープログラムディレクトリの Config ディレクトリにあります。

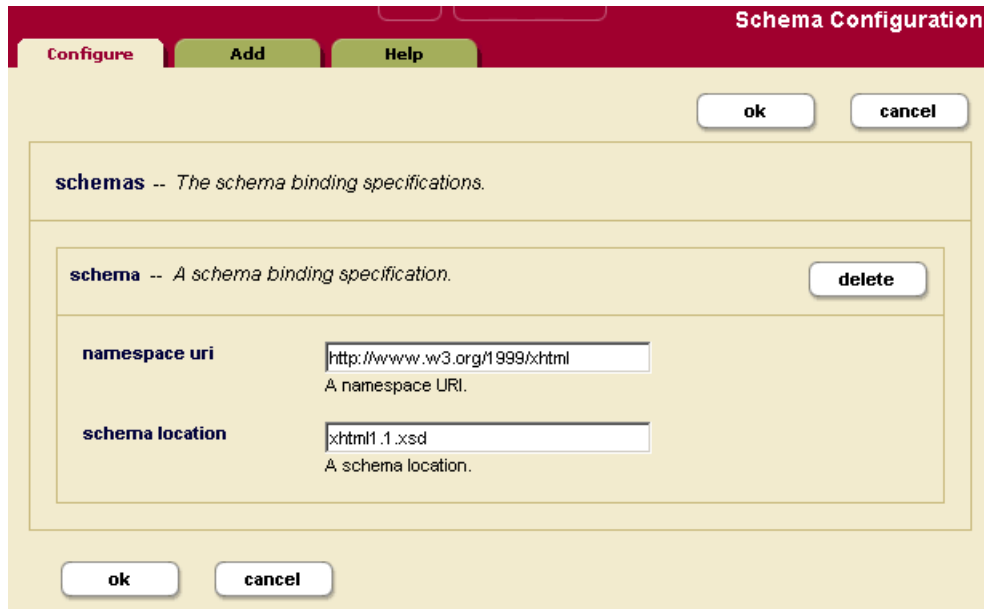


29.2.4 HTTP、ODBC、または XDBC サーバーのスキーマ定義の表示

HTTP、ODBC、または XDBC サーバーのスキーマ定義を表示するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 表示するスキーマを持つ HTTP、ODBC、または XDBC サーバーを含んだグループの名前をクリックします。
3. [App Servers] アイコンをクリックします。
4. 表示するスキーマを持つアプリケーションサーバーの名前をクリックします。
5. 左側のツリーメニューで、指定したアプリケーションサーバーの下の [Schemas] アイコンをクリックします。

次の例は、1つのスキーマだけを表示します。これは、名前空間 `http://www.w3.org/1999/xhtml` のスキーマがファイル `xhtml1.1.xsd` にあることを指定します。このファイルは MarkLogic サーバープログラムディレクトリの Config ディレクトリにあります。



29.2.5 グループのスキーマ定義の削除

グループのスキーマ定義を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. スキーマを削除するグループをクリックします。
3. 左側のツリーメニューで、指定したグループの下の [Schemas] アイコンをクリックします。
4. システムから削除するスキーマ定義を特定して、[delete] をクリックします。
5. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

スキーマがグループから削除されます。

29.2.6 HTTP、ODBC、または XDBC サーバーのスキーマ定義の削除

HTTP、ODBC、または XDBC サーバーのスキーマ定義を削除するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. 削除するスキーマを持つ HTTP、ODBC、または XDBC サーバーを含んだグループの名前をクリックします。
3. [App Servers] アイコンをクリックします。

4. 削除するスキーマを持つアプリケーションサーバーの名前をクリックします。
5. 左側のツリーメニューで、指定したアプリケーションサーバーの下の [Schemas] アイコンをクリックします。
6. 左側のツリーメニューで、指定したアプリケーションサーバーの下の [Schemas] アイコンをクリックします。
7. システムから削除するスキーマ定義を特定して、[delete] をクリックします。
8. 確認メッセージが表示されます。削除を確認して [ok] をクリックします。

スキーマがアプリケーションサーバーから削除されます。

30.0 ログファイル

この章では、ログファイルについて説明します。次のセクションで構成されます。

- [アプリケーションおよびシステムログファイル](#)
- [ログレベルについて](#)
- [システムログファイルの設定](#)
- [アプリケーションログファイルの設定](#)
- [システムログの表示](#)
- [アプリケーションログとシステムファイルログの表示](#)
- [アクセスログファイル](#)

監査ログファイルの詳細については、「イベントの監査」(91 ページ) を参照してください。

30.1 アプリケーションおよびシステムログファイル

アプリケーションで生成されるメッセージ用と、システムで生成されるメッセージ用に個別のログファイルがあります。これにより、個人を識別できる情報（ソーシャルセキュリティ番号など）と、システムメッセージ（マージ通知やその他のシステムアクティビティなど）を分離できます。アプリケーションログファイルはアプリケーションサーバーごとに設定され、システムログファイルはグループレベルで設定されます。各ホストには、独自のログファイルセット（アプリケーションログファイルとシステムログファイルの両方）があります。キャッチされなかったアプリケーションエラーなどの情報は、アプリケーションからのデータを含む可能性があるため、アプリケーションログに送信されます。MarkLogic サーバーのシステムアクティビティなどは、システムログファイルに送信されます。

30.2 ログレベルについて

MarkLogic サーバーは、オペレーティングシステムログと MarkLogic サーバーシステムファイルログの両方にログメッセージを送信します。さらに、アプリケーションログメッセージ（アプリケーションコードから生成されたメッセージ）はアプリケーションログに送信されます。ログ記録機能の設定に応じて、オペレーティングシステムログとファイルログの両方が、同数のメッセージを受信することも、受信しないこともあります。パフォーマンスを高めるため、システムログが受信するメッセージは、MarkLogic サーバーファイルログより少なくする必要があります。

MarkLogic サーバーは次のログ設定を使用します。ここでは [Finest] は情報が最も多く、[Emergency] は方法が最も少なくなります。

ログレベル	説明
Finest	極めて詳細なデバッグレベルのメッセージ。
Finer	非常に詳細なデバッグレベルのメッセージ。
Fine	詳細なデバッグレベルのメッセージ。
Debug	デバッグレベルのメッセージ。
Config	設定メッセージ。
Info	情報メッセージ。これがデフォルト設定です。
Notice	正常だが、注意が必要な状態。
Warning	警告状態。
Error	エラー状態。
Critical	致命的な状態。
Alert	即座の措置が必要。
Emergency	システムを使用できない。

ログファイル設定は、グループごとに適用されます。

デフォルトでは、グループのシステムログは [Notice] に設定されていますが、ファイルログは [Info] に設定されています。したがって、システムログが受信するログメッセージはファイルログより少なくなります。各自のニーズに合わせてこれらの設定を変更できます。例えば、システムの問題をデバッグしている場合、さらに情報を得るためにレベルを [Debug] に設定できます。[Debug] 以上のログレベルはシステムパフォーマンスを大幅に低下させるため、通常は使用しないでください。

30.3 システムログファイルの設定

ログ情報を生成する方法を設定するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. ログファイル設定を構成するグループをクリックします。

3. ページの下部に向かってログ設定を下にスクロールします。

次の例は、デフォルトのログ設定を示しています。

The screenshot shows a configuration panel with the following settings:

- system log level:** A dropdown menu set to "notice". Below it, the text reads: "The minimum log level for log messages sent to the operating system."
- file log level:** A dropdown menu set to "info". Below it, the text reads: "The minimum log level for log messages in the log file."
- rotate log files:** A dropdown menu set to "daily". Below it, the text reads: "When to start a new log file."
- keep log files:** A text input field containing the number "7". Below it, the text reads: "How many log files to keep."

4. [system log level] に移動し、必要に応じてレベルを変更します。
5. [file log level] に移動し、MarkLogic サーバーのプライベートログファイル (ErrorLog.txt) のログ記録レベルを変更します。
6. [rotate log files] に移動し、MarkLogic サーバーがこのグループの新しいプライベートログファイルを開始するタイミングを選択します。

次の表は、各時間枠について説明したものです。

時間枠	説明
Never	ログファイルは無制限に増大します。
Daily	新しいログファイルが毎日午前 12:00 に開始されます。
Sunday	新しいログファイルが毎週日曜日の午前 12:00 に開始されます。
Saturday	新しいログファイルが毎週土曜日の午前 12:00 に開始されます。
Friday	新しいログファイルが毎週金曜日の午前 12:00 に開始されます。
Thursday	新しいログファイルが毎週木曜日の午前 12:00 に開始されます。

時間枠	説明
Wednesdays	新しいログファイルが毎週水曜日の午前 12:00 に開始されます。
Tuesday	新しいログファイルが毎週火曜日の午前 12:00 に開始されます。
Monday	新しいログファイルが毎週月曜日の午前 12:00 に開始されます。
Monthly	新しいログファイルが毎月最初の日の午前 12:00 に開始されます。

7. [keep log files] で、保持するプライベートログファイルの数を入力します。

プライベートログファイルは、エイジングアーカイブに保持されます。ログファイル数が [keep log files] 設定で指定した値まで増えると、新しいログファイルが開始されたときに、最も古いログファイルアーカイブから自動的に削除されます。

8. 上部または下部までスクロールして [ok] をクリックします。

30.4 アプリケーションログファイルの設定

アプリケーションサーバーのログ情報を生成する方法を設定するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. アプリケーションログファイル設定を構成するアプリケーションサーバーを含むアプリケーションサーバーグループの下で、目的のアプリケーションサーバーをクリックします。
3. ページの下部に向かってログ設定を下にスクロールします。
4. [file log level] に移動し、必要に応じてアプリケーションログファイル（例えばポート 8543 のアプリケーションサーバーには `8543_ErrorLog.txt`）のログ記録レベルを変更します。
5. [Log Errors] に移動し、キャッチされていないアプリケーションエラーをログファイルに送信する場合は [true] をクリックし、それ以外の場合は [false] をクリックします。
6. 上部または下部までスクロールして [ok] をクリックします。

注： アプリケーションログファイルのログローテーションは、「システムログファイルの設定」（404 ページ）の手順で説明しているそのグループのシステムログファイルのルールと同じルールに従います。

30.5 システムログの表示

MarkLogic サーバーが生成するシステムログメッセージは、使用しているプラットフォームで利用可能な標準のシステムログ表示ツールを使用して表示できます。Windows プラットフォームでは、ログ記録メッセージの 7 つのレベルが 3 つの広いカテゴリにまとめられ、システムログメッセージは MarkLogic として登録されます。UNIX プラットフォームでは、システムログは LOG_DAEMON 機能を使用します。これは一般に、システムログメッセージを /var/log/messages などのファイルに送信しますが、システムの設定に応じて異なる可能性があります。

30.6 アプリケーションログとシステムファイルログの表示

プライベートシステムファイルログは、シンプルなテキストファイルとして保持され、アプリケーションログもシンプルなテキストファイルとして維持されます。現在のファイルログやアーカイブ済みのファイルログは、標準的なテキストファイル表示ツールを使用していつでも表示できます。また、管理画面のメインページにある [Log] タブからログファイルにアクセスできます。

ファイルは、お使いのプラットフォームに応じた MarkLogic サーバーデータディレクトリの下に Logs ディレクトリに格納されます。インストール時に、このディレクトリのデフォルトの場所をオーバーライドしている可能性があります。次の表は、プラットフォームでのファイルログのデフォルトの場所を示したものです。

プラットフォーム	プライベートログファイル
Microsoft Windows	C:\Program Files\MarkLogic\Data\Logs\ErrorLog.txt C:\Program Files\MarkLogic\Data\Logs\ <port>_ErrorLog.txt</port>
Red Hat Enterprise Linux	/var/opt/MarkLogic/Logs/ErrorLog.txt /var/opt/MarkLogic/Logs/<port>_ErrorLog.txt
Mac OS X	~/Library/Application Support/MarkLogic/Data/Logs/ErrorLog.txt ~/Library/Application Support/MarkLogic/Data/Logs/<port>_ErrorLog.txt

アプリケーションログファイルには、ログファイルに対応したアプリケーションサーバーのポート番号が前に付けられます。これらのファイルには、経時的に並べられた一連のログメッセージが含まれます。メッセージの数は、システムアクティビティと、設定したログレベルに応じて異なります。例えば、[Debug] に設定されたファイルログには多数の行のメッセージが含まれますが、[Emergency] に設定されたファイルログには最低限のメッセージセットが含まれます。

トレースイベントは、MarkLogic サーバー ErrorLog.txt ファイルにも書き込まれます。トレースイベントはアプリケーションのデバッグに使用されます。管理画面のグループの [Diagnostics] ページで、トレースイベントを有効化および設定できます。xdmp:trace 関数で、独自のトレースイベントも生成できます。

注： ログファイルが存在するファイルシステムには、十分なディスク容量が必要です。ログファイルのあるデバイスの残り領域がなくなると、MarkLogic サーバーが停止されます。また、ログファイルに使用できるディスク領域がない場合、MarkLogic サーバーは起動に失敗します。

30.7 アクセスログファイル

MarkLogic サーバーは、アプリケーションサーバーごとにアクセスログファイルも生成します。アクセスログは、NCSA 共通ログ形式で記録され、各アプリケーションサーバーに対して行われたリクエストを示します。アクセスログファイルは、`ErrorLog.txt` ログと同じディレクトリに置かれ、ポート番号がその名前に付加されます。例えば、管理画面のアクセスログファイルには、`8001_AccessLog.txt` という名前が付けられます。現在のファイルログやアーカイブ済みのファイルログは、標準的なテキストファイル表示ツールを使用していつでも表示できます。また、管理画面のメインページにある [Log] タブからログファイルにアクセスできます。以前のバージョンのアクセスログは、「システムログファイルの設定」(404 ページ) で説明しているように、グループレベルで構成された設定に従ってシステムから古い順に削除されます。

31.0 タスクのスケジュール設定

この章では、事前定義された日付 / 時刻または間隔で XQuery メインモジュールを実行するタスクのスケジュールを設定する方法について説明します。次のトピックから構成されています。

- [スケジュール設定されたタスクについて](#)
- [モジュール呼び出しのスケジュール設定](#)
- [タスクタイプの選択](#)

この章では、スケジュール設定されたタスクを管理画面を使用して管理する方法について説明します。スケジュール設定されたタスクをプログラムによって管理する方法の詳細については、『*Scripting Administrative Tasks Guide*』の「[Group Maintenance Operations](#)」を参照してください。

31.1 スケジュール設定されたタスクについて

MarkLogic サーバーでは、XQuery メインモジュールの実行スケジュールを設定できません。モジュールの実行スケジュールを設定する機能は次の場合に役立ちます。

- コンテンツの読み込み。例えば、web サイトや web サービスなどの外部データソースからの新しいコンテンツを定期的にチェックする場合です。
- コンテンツの同期化。例えば、MarkLogic がメタデータリポジトリとして使用される場合、変更のあったデータを定期的にチェックできます。
- コンテンツの一括提供。例えば、RSS フィードを時間単位または日単位で開始します。
- 時間単位または日単位での集約されたアラートの提供。
- 日単位、週単位、または月単位でのレポートの提供。
- PDF ファイルの作成などの非同期プロセスの完了に対するポーリング。

タスクは、特定の日付の特定の時間か、指定した間隔で実行するようにスケジュールを設定できます。MarkLogic サーバーは、指定された時刻にタスクサーバーのキューにタスクを入れようとはしますが、タスクの実際の実行は、この時刻には開始しないことがあります。キューがいっぱいの場合、タスクは失敗し、スケジュールされた次の間隔になるまで、再試行されません。

31.2 モジュール呼び出しのスケジュール設定

特定の日付 / 時刻または間隔でモジュールの呼び出しのスケジュールを設定するには、次の手順を実行します。

1. 左側のツリーメニューで [Groups] アイコンをクリックします。
2. タスクのスケジュールを設定するグループをクリックします（例えば [Default]）。
3. 左側のツリーメニューで [Scheduled Tasks] アイコンをクリックします。
4. [Create] タブをクリックして、[Schedule a Task] ページを表示します。
5. [task path] フィールドに、呼び出すモジュールの URI を指定します。このタスクパスは、スラッシュ (/) で始める必要があり、疑問符「?」、コロン「:」、またはシャープ「#」文字を含められません。
6. [task root] フィールドで、モジュールを含むルートディレクトリ（ファイルシステム）または URI ルート（データベース）を指定します。例えば、モジュールが `MarkLogic/Docs` の下のファイルシステムに置かれている場合、[Docs] を指定します。
7. [task type] フィールドで、「タスクタイプの選択」（412 ページ）で説明しているタスクタイプのいずれかを選択します。
8. [database] フィールドで、モジュールを呼び出すデータベースを選択します。
9. [task modules] フィールドで、[task path] フィールドで指定したモジュールを含んだファイルシステムまたはデータベースを選択します。

[task modules] を [(file system)] に設定した場合、[task root] で指定したディレクトリにモジュールを配置します。例えば、下記の設定では、`MarkLogic/Docs` ディレクトリに `Scheduler_test.xqy` ファイルを配置します。

[task modules] をデータベースに設定した場合、[task root] で指定された URI ルート下にある、該当データベースにモジュールを読み込みます。例えば、下記の設定で、[task modules] フィールドに [Documents] を指定した場合、`xdmp:document-load` 関数を使用して、次の URI オプションでモジュールを読み込みます。

```
<uri>Docs/Scheduler_test.xqy</uri>
```

10. [task user] フィールドと [task host] フィールドで、タスクを呼び出すパーミッションを持つユーザーと、タスクが呼び出されるホストコンピュータを指定します。ホストが指定されない場合、タスクはすべてのホスト上で実行されます。

注： [task user] フィールドで指定したユーザーは、モジュールで使用される関数の実行に必要な権限を持っている必要があります。実行権限の全リストについては、「付録 B：事前定義された実行権限」（437 ページ）を参照してください。

スケジュール設定されたタスク設定の例：

Schedule a Task

task path	<input type="text" value="/Scheduler_test.xqy"/> The module to invoke. Required. You must supply a value for task-path.
task root	<input type="text" value="Docs"/> The path to the module directory root. Required. You must supply a value for task-root.
task type	<input checked="" type="radio"/> minutely <input type="radio"/> hourly <input type="radio"/> daily <input type="radio"/> weekly <input type="radio"/> monthly <input type="radio"/> once
task period	<input type="text" value="45"/> How often this task should run (every n months, weeks, days, hours or minutes).
task database	<input type="text" value="Documents"/> <input type="button" value="v"/> The database name.
task modules	<input type="text" value="(file system)"/> <input type="button" value="v"/> The database that contains application modules.
task user	<input type="text" value="Jim"/> <input type="button" value="v"/> The user to run this task as.
task host	<input type="text" value=""/> <input type="button" value="v"/> The host to run this task on.

31.3 タスクタイプの選択

このセクションで説明する日付 / 時刻または間隔のスケジュールオプションのいずれかをタスクタイプとして選択できます。

経過時間で動作する間隔スケジュールオプションは次のとおりです。

- [分単位のスケジュール](#)
- [時間単位のスケジュール](#)

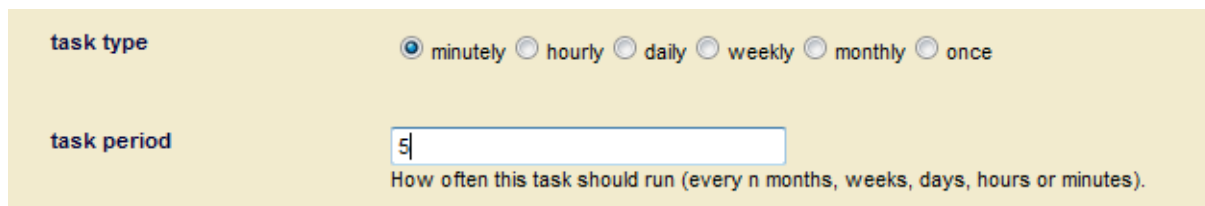
カレンダー時間で動作する日付 / 時刻スケジュールオプションは次のとおりです。

- [日と時間単位のスケジュール](#)
- [週、日、および時間単位のスケジュール](#)
- [月、日、および時間単位のスケジュール](#)
- [カレンダーの日および時刻に 1 回の呼び出しのスケジュール](#)

注： 日付 / 時刻オプションは、サーバーの時計で指定されたローカル時間によってスケジュール設定されます。したがって、夏時間が設定されている地域では、24 時間のスケジュール間隔と、特定の時刻で 1 日に 1 回というスケジュール間隔が同じにならない場合があります。

31.3.1 分単位のスケジュール

[minutely] (分単位) のタスクタイプを選択した場合、モジュールの各呼び出し間の経過分数を指定します。例えば、5 分ごとに (またはサーバーに過負荷がかかった場合はその後できるだけすぐに) モジュールを呼び出すには、次のように入力します。



The screenshot shows a configuration panel with a light yellow background. At the top, the label "task type" is followed by a row of radio buttons for "minutely", "hourly", "daily", "weekly", "monthly", and "once". The "minutely" radio button is selected. Below this, the label "task period" is followed by a text input field containing the number "5". Underneath the input field is the text "How often this task should run (every n months, weeks, days, hours or minutes)."

31.3.2 時間単位のスケジュール

[hourly]（時間単位）のタスクタイプを選択した場合、モジュールの各呼び出し間の経過時間数を指定します。[task minute] 設定は、その時間の何分にモジュールが呼び出されるかを指定します。[task minute] 設定は間隔には追加されないことに注意してください。

例えば、2 時間ごとにその時間の 30 分に（またはサーバーに過負荷がかかった場合はその後できるだけすぐに）モジュールを呼び出すには、次のように入力します。

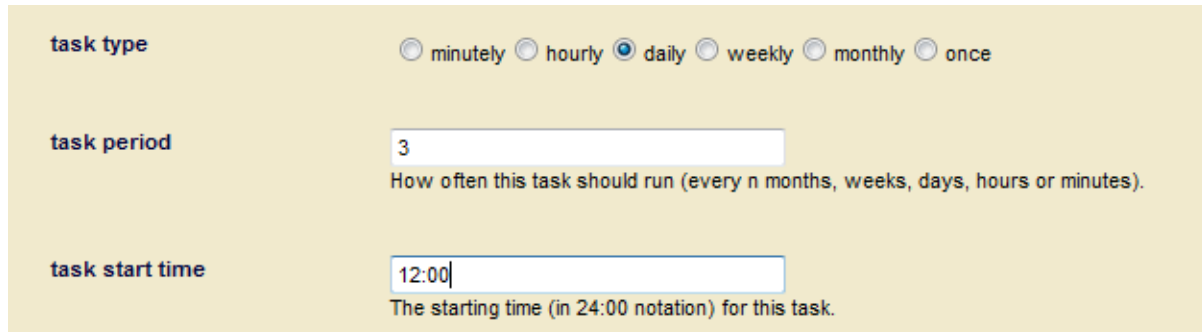
The screenshot shows a configuration form for a task. The 'task type' is set to 'hourly'. The 'task period' is set to '2'. The 'task minute' dropdown menu is open, showing a list of values from 0 to 44 in increments of 1. The value '30' is selected and highlighted. Other fields include 'task database', 'task modules', 'task user', and 'task host', each with a dropdown menu.

現在の時刻が午後 2:15 の場合、タスクは午後 2:30、午後 4:30、午後 6:30、午後 8:30 のように実行されます。

31.3.3 日と時間単位のスケジュール

[daily]（日単位）のタスクタイプを選択した場合、モジュールの各呼び出し間の経過日数と、呼び出しの時刻（24:00 表記）を指定します。

例えば、3 日ごとの午後 12:00 にモジュールを呼び出すには、次のように入力します。

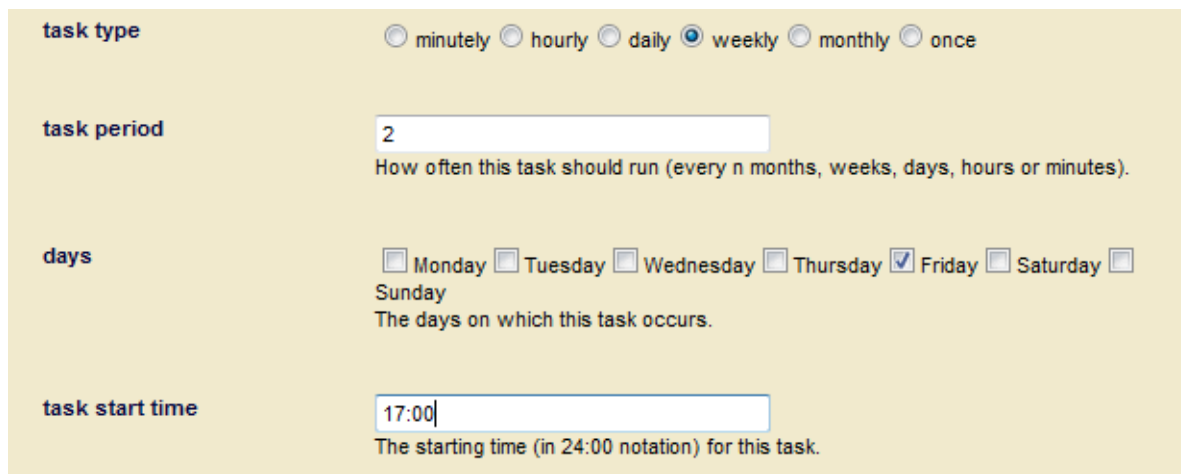


The screenshot shows a configuration form for a task. It has three main sections: 'task type', 'task period', and 'task start time'. 'task type' has radio buttons for 'minutely', 'hourly', 'daily' (selected), 'weekly', 'monthly', and 'once'. 'task period' has a text input field containing '3' and a label 'How often this task should run (every n months, weeks, days, hours or minutes)'. 'task start time' has a text input field containing '12:00' and a label 'The starting time (in 24:00 notation) for this task'.

31.3.4 週、日、および時間単位のスケジュール

[weekly]（週単位）のタスクタイプを選択した場合、モジュールの各呼び出し間の経過週数の他、呼び出しの 1 つあるいは複数の曜日と時刻（24:00 表記）を指定します。

例えば、隔週の金曜日の午後 5:00 にモジュールを呼び出すには、次のように入力します。

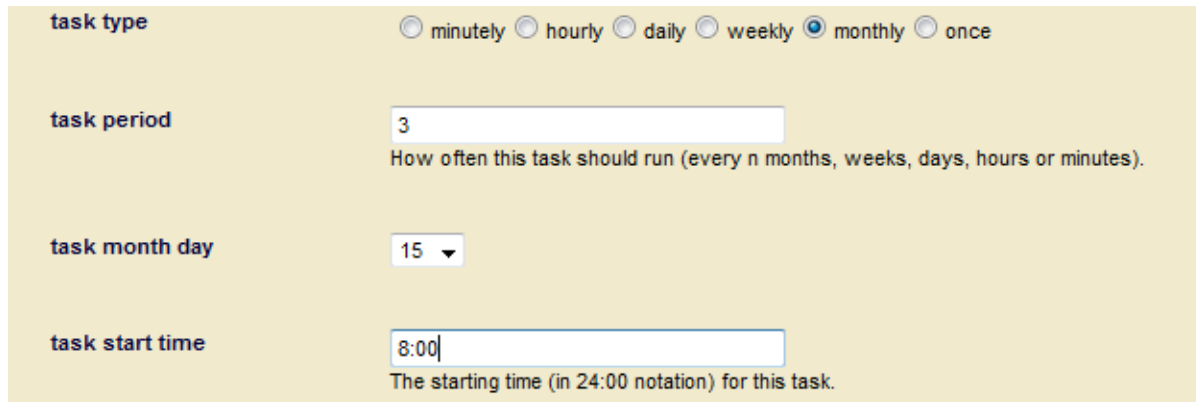


The screenshot shows a configuration form for a task. It has four main sections: 'task type', 'task period', 'days', and 'task start time'. 'task type' has radio buttons for 'minutely', 'hourly', 'daily', 'weekly' (selected), 'monthly', and 'once'. 'task period' has a text input field containing '2' and a label 'How often this task should run (every n months, weeks, days, hours or minutes)'. 'days' has checkboxes for 'Monday', 'Tuesday', 'Wednesday', 'Thursday', 'Friday' (checked), 'Saturday', and 'Sunday', with a label 'The days on which this task occurs'. 'task start time' has a text input field containing '17:00' and a label 'The starting time (in 24:00 notation) for this task'.

31.3.5 月、日、および時間単位のスケジュール

[monthly] 月単位のタスクタイプを選択した場合、モジュールの各呼び出し間の経過月数の他、呼び出しの日と時刻（24:00 表記）を指定します。

例えば、3 か月ごとの 15 日の午前 8:00 にモジュールを呼び出すには、次のように入力します。

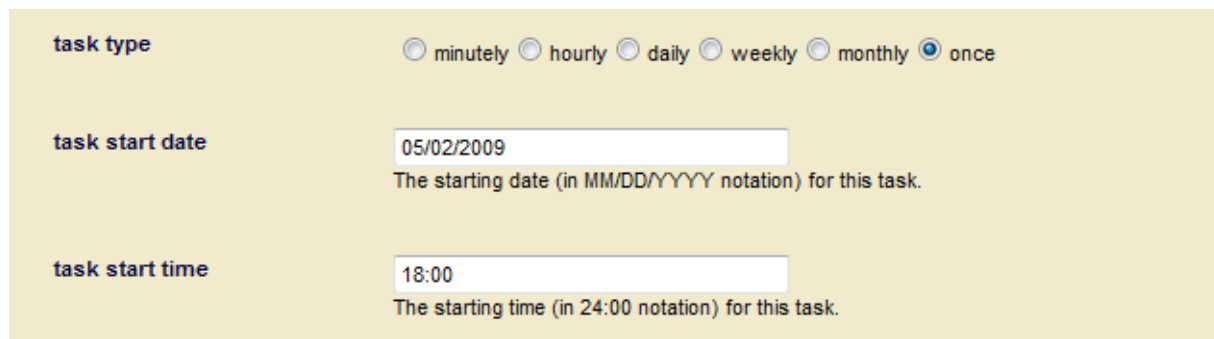


The screenshot shows a configuration form for a task. The 'task type' section has radio buttons for 'minutely', 'hourly', 'daily', 'weekly', 'monthly', and 'once', with 'monthly' selected. The 'task period' is a text input field containing '3', with a note below it: 'How often this task should run (every n months, weeks, days, hours or minutes)'. The 'task month day' is a dropdown menu showing '15'. The 'task start time' is a text input field containing '8:00', with a note below it: 'The starting time (in 24:00 notation) for this task.'

31.3.6 カレンダーの日および時刻に 1 回の呼び出しのスケジュール

[once] (1 回のみ) タスクタイプを選択した場合、呼び出しのカレンダー日（月 / 日 / 年）と時刻（24:00 表記）を指定します。

例えば、2009 年 5 月 2 日午後 6:00 にモジュールを呼び出すには、次のように入力します。



The screenshot shows a configuration form for a task. The 'task type' section has radio buttons for 'minutely', 'hourly', 'daily', 'weekly', 'monthly', and 'once', with 'once' selected. The 'task start date' is a text input field containing '05/02/2009', with a note below it: 'The starting date (in MM/DD/YYYY notation) for this task'. The 'task start time' is a text input field containing '18:00', with a note below it: 'The starting time (in 24:00 notation) for this task.'

32.0 コンフィギュレーションマネージャの使用

MarkLogic サーバーコンフィギュレーションマネージャには、管理画面用の読み取り専用インターフェイスと、設定を保存およびリストアするためのツールが用意されています。この章は、次のセクションで構成されています。

- [コンフィギュレーションマネージャの概要](#)
- [セキュリティの考慮事項](#)
- [コンフィギュレーションマネージャへのアクセス](#)
- [設定の表示](#)
- [設定の検索](#)
- [設定の編集](#)
- [設定のエクスポートとインポート](#)
- [インポートした設定の適用](#)

32.1 コンフィギュレーションマネージャの概要

コンフィギュレーションマネージャでは、MarkLogic サーバーリソースの設定を表示できます。「リソース」とは、データベース、フォレスト、アプリケーションサーバー、ホストなどの MarkLogic サーバーオブジェクトのことです。

コンフィギュレーションマネージャを使用して次の操作を実行できます。

- データベース、フォレスト、グループ、ホスト、およびアプリケーションサーバーの設定への読み取り専用アクセスを、管理者以外のユーザーに許可する。
- リソースと設定を簡単に検索する。
- 読み取り専用モードで設定を安全に確認してから、管理画面でリソースに直接ジャンプして設定を修正する（設定の修正には管理権限が必要です）。
- zip フォルダ内に XML としてリソース設定を保存する。
- 以前に保存したリソース設定をインポートする。設定をインポートすると、バージョンを比較して設定を更新できます。
- 管理 REST API を通じて使用可能なデータを表示する。

管理 REST API の詳細については、『*Monitoring MarkLogic Guide*』の「[Using the Management API](#)」を参照してください。

注： パッケージング REST API は MarkLogic 7 用に変更されています。MarkLogic 6 パッケージング REST API (v1) を使用して作成されたアプリケーションは、MarkLogic 7 パッケージング REST API (v2) で動作するように作成し直す必要があります。

32.2 セキュリティの考慮事項

[Configuration Manager] ページにアクセスするには、ユーザーに `manage-user` のロールが必要です。このロールでは、設定を修正する権限は付与されません。`manage-user` のロールを持つユーザーは、次の操作を実行できます。

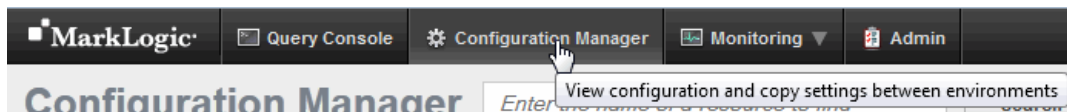
- コンフィギュレーションマネージャのページにアクセスして、リソースおよび設定を表示する。
- 設定を ZIP ファイルにエクスポートする (Modules データベースは除く)。
- 以前に保存した設定をコンフィギュレーションマネージャにインポートして、これらを表示または比較する。

`manage-user` ロールでは、設定の編集、インポートした設定からの設定変更の適用、または Modules データベースのエクスポートの権限は付与されません。Modules データベースのコンテンツをエクスポートするには、`manage-admin` ロールが必要です。ただし、アクセスパーミッションを持っていないモジュールは表示できません。パッケージをインストール (インポートしたパッケージを適用) するには、`admin` 権限が必要です。

`manage-internal` ロールは、MarkLogic サーバー内部での使用に限られます。このロールはユーザーには割り当てないでください。これをユーザーに割り当ててしまうと、通常は望ましくないシステムに関する権限を付与してしまうこととなります。

32.3 コンフィギュレーションマネージャへのアクセス

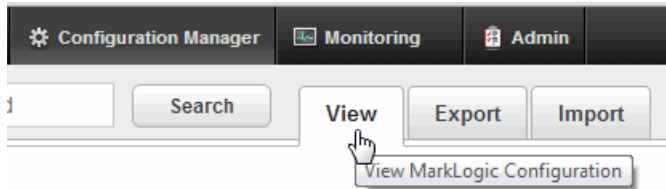
コンフィギュレーションマネージャにアクセスするには、<http://yourhostname:8002/nav/> の URL に移動するか、いずれかのアプリケーションサービスページから [Configuration Manager] タブをクリックします。



- 注：** アプリケーションが表示されない場合は、権限が十分でない可能性があります。コンフィギュレーションマネージャを十分に活用するには、`manage-admin` セキュリティロールが必要です。「セキュリティの考慮事項」(417 ページ) を参照してください。

32.4 設定の表示

MarkLogic サーバーリソースの設定を表示するには、[View] タブをクリックします。



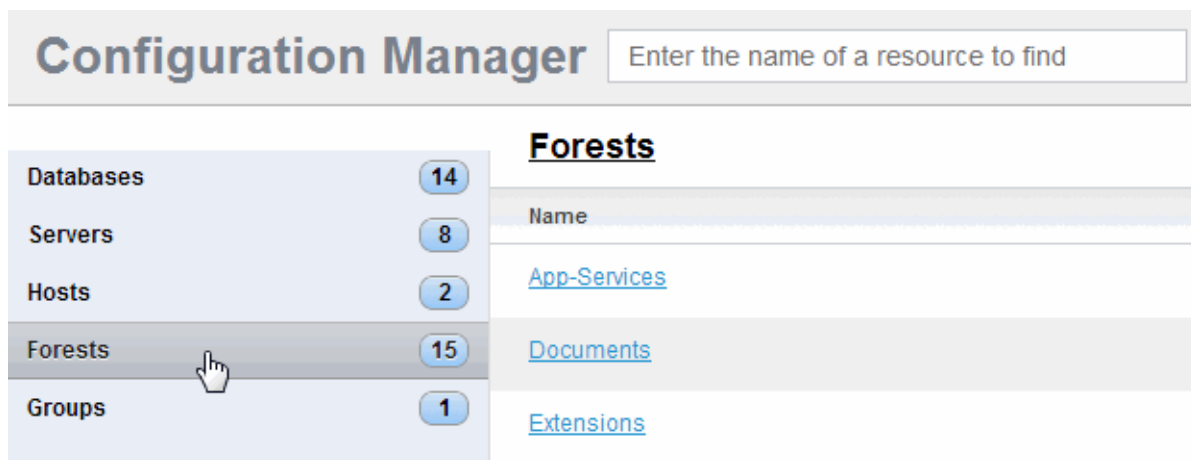
コンフィギュレーションマネージャには、特定のリソースの設定を検索するための手法が2つ用意されています。

- [リソース設定の参照](#)
- [リソースの検索](#)

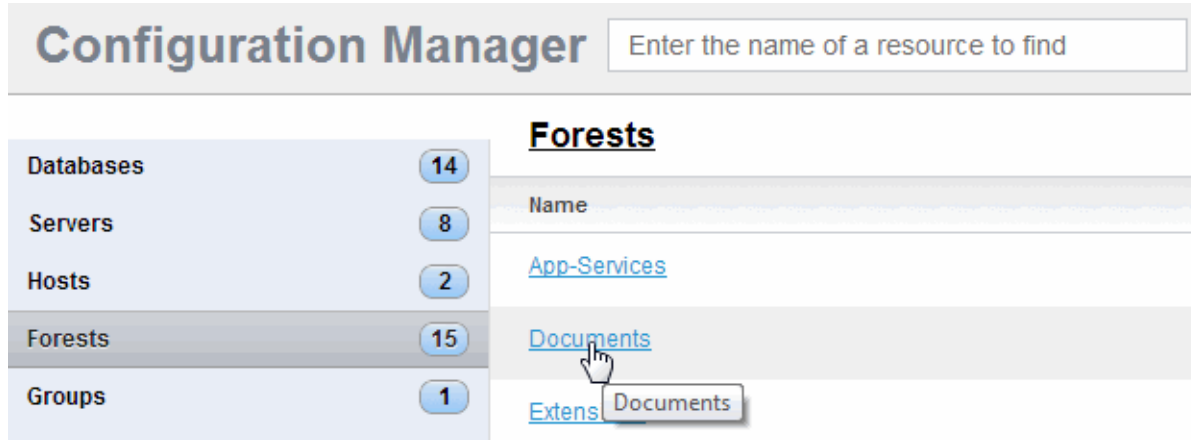
32.4.1 リソース設定の参照

リソースを見つけ、参照によってその設定を表示するには、次の手順に従います。

1. コンフィギュレーションマネージャの左側にあるリソースリストからリソースカテゴリをクリックします。選択したカテゴリのリソースのリストが表示されます。リソースカテゴリ名の右側にある数字は、そのリソースで存在している数を示します。

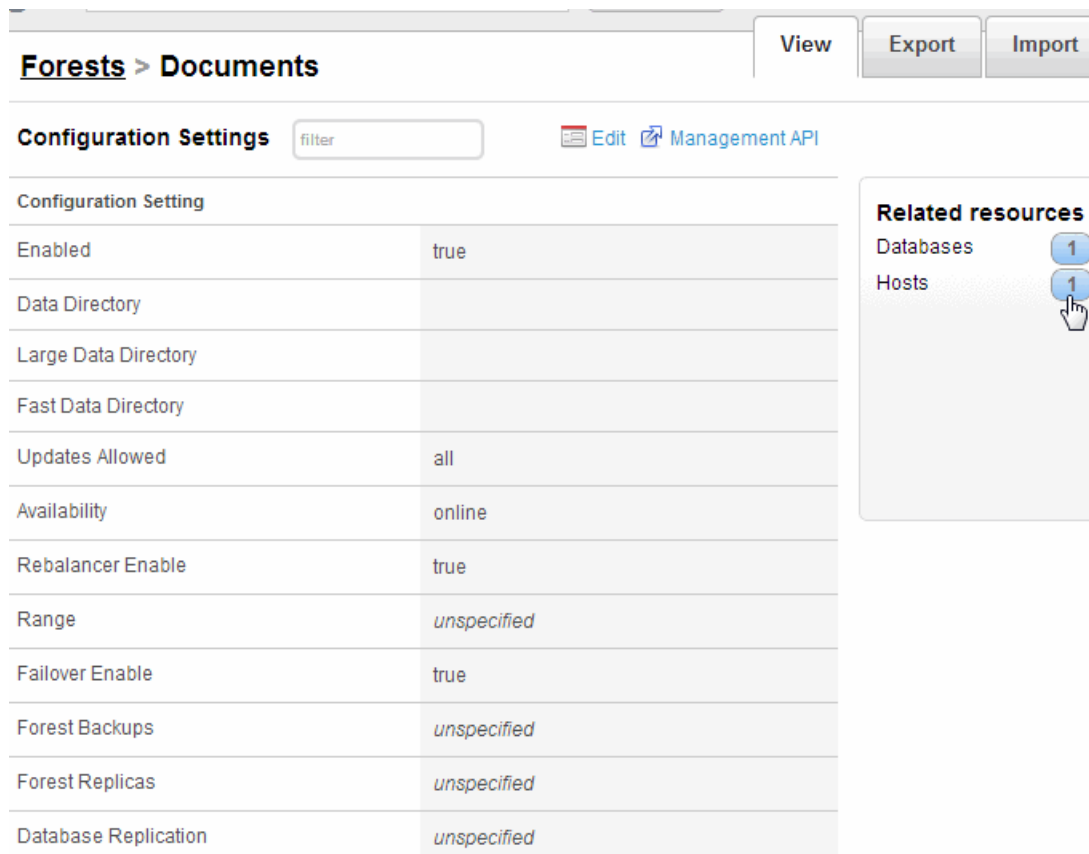


- 設定を表示するリソースの名前をクリックします。



- [Configuration Settings] ページに、選択したリソースの設定が表示されます。そのリソースに関連したリソースも右側のフレームに表示されます。関連したリソースをクリックすると、その設定を表示できます。



注： パーティションのあるフォレストの場合、関連リソースの下にパーティションリンクが含まれます。




4. 設定のいくつかは、コンテナに収納されています。これらは、コンテナ名の前に記された矢印で識別されます。矢印をクリックして、コンテナを展開して詳細を表示できます。例えば、フォレストレンジ設定を表示するには、下記のように [Range] コンテナの横の矢印をクリックします。

Forests > 10-0002

Configuration Settings

 [Edit](#)
 [Management API](#)

Configuration Setting	
Enabled	true
Data Directory	/tmp
Large Data Directory	
Fast Data Directory	
Updates Allowed	all
Availability	online
Rebalancer Enable	true
 Range	
Lower Bound	1
Upper Bound	10
Failover Enable	true
Forest Backups	<i>unspecified</i>
Forest Replicas	<i>unspecified</i>
Database Replication	<i>unspecified</i>

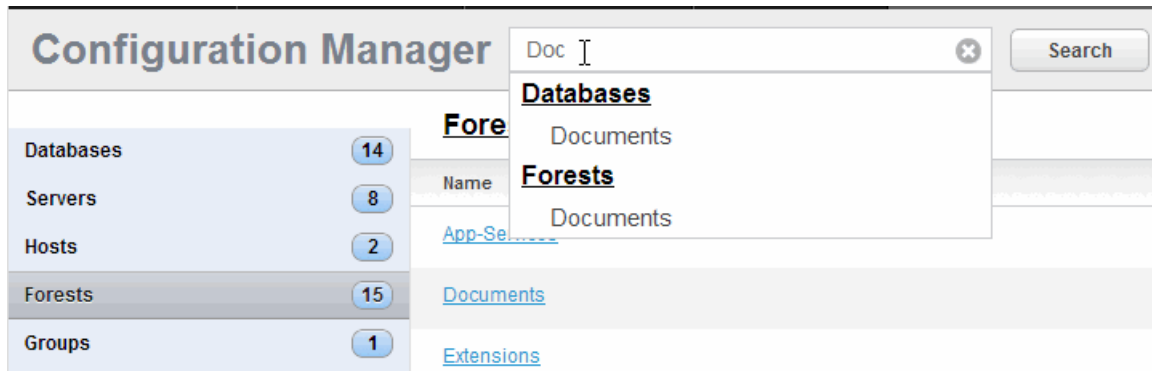
Related resources

Hosts 1

32.4.2 リソースの検索

名前で見つけたいリソースを検索するには、ページ最上部の検索ボックスを使用します。入力すると、コンフィギュレーションマネージャによりマッチするリソースが提示されます。

1. 検索ボックスをクリックして、リソースの名前の入力を開始します。検索にマッチした候補のドロップダウンが表示されます。

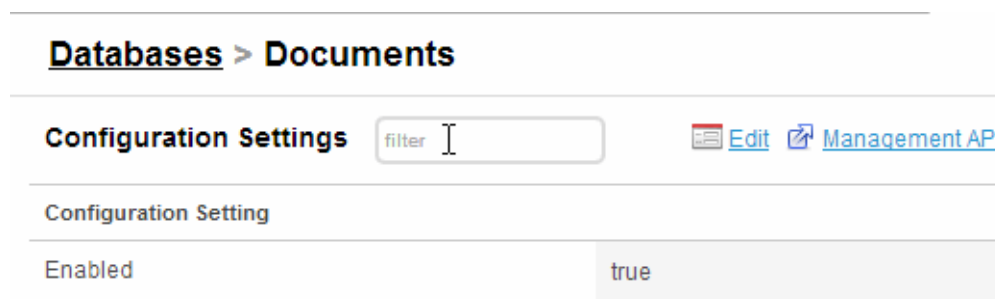


2. ドロップダウンリストの検索候補をクリックして、その設定を表示するか、[Search] ボタンをクリックしてマッチングリソースのページを表示し、ここから選択できます。

32.5 設定の検索

リソース設定内で設定名または値を検索できます。

1. 検索するリソースに移動します。「設定の表示」(418 ページ) を参照してください。
2. 設定のすぐ上の [filter] ボックスをクリックします。



3. 設定の名前または値の一部を入力し始めます。設定は入力に従ってフィルタリングされます。各設定においてマッチしているテキストが強調表示されます。

Databases > Documents

Configuration Settings [Edit](#) [Management API](#)

Triple Index	false
Re index er Enable	true
Re index er Throttle	5
Re index er Timestamp	0
In Memory Range Index Size	2
In Memory Reverse Index Size	2
In Memory Triple Index Size	2
Range Index Optimize	facet-time
Index Detection	automatic

32.6 設定の編集

編集機能を使用して、特定のリソースで管理画面を開き、設定を修正します。リソースカテゴリリストページまたはリソースの設定ページから、リソース設定を編集できます。

注： 設定を編集するには、管理権限が必要です。

リソースの設定を編集するには次の手順に従います。

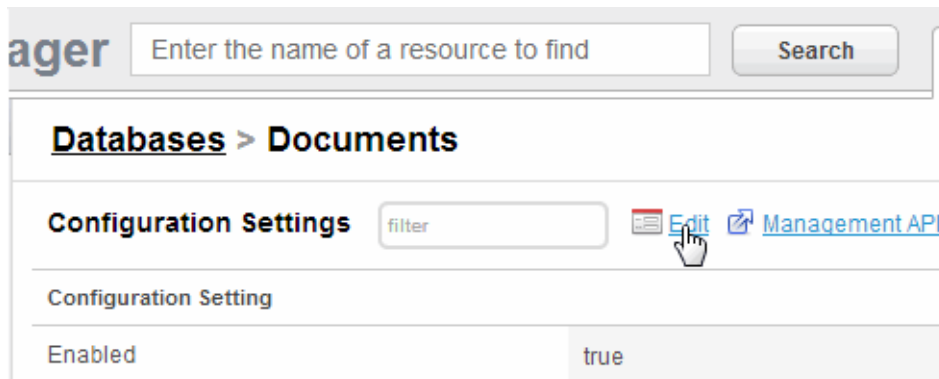
1. リソースカテゴリリストから、リソース名の右側にある編集アイコンをクリックします。そのリソースに対して管理画面が開きます。



2. 『*Monitoring MarkLogic Guide*』の「[Using the Management API](#)」の章で説明しているように、MarkLogic サーバーには、リソースのモニタリングデータおよび管理データを収集するための REST 管理 API が含まれています。コンフィギュレーションマネージャを使用して、リソースから取得されるデータを、REST 管理 API を通じて HTML、XML、または JSON として簡単に表示できます。コンフィギュレーションマネージャで得られる情報は、管理 API を通じて得られるデータと重複していますが、管理 API はステータス情報などのその他のデータを明らかにします。[Management API] アイコンをクリックして、管理 API でリソース設定を表示できます。



3. 管理画面と管理 API へのリンクは、リソースの [Configuration Settings] ページでも使用できます。例えば、データベースの [Configuration Settings] ページの最上部にある [Edit] アイコンをクリックすると、そのデータベースの設定ページが管理画面で開きます。



32.7 設定のエクスポートとインポート

コンフィギュレーションマネージャを使用すると、設定を zip ファイルに保存し、後からそれらをインポートして設定を比較し更新を適用できます。

コンフィギュレーションマネージャには、次の機能が備わっています。

- [設定のエクスポート](#)
- [設定のインポート](#)
- [インポートした設定と現在の設定との比較](#)

注： SSL や外部セキュリティ（LDAP や Kerberos）設定などのセキュリティ設定は、エクスポートした設定ファイルからインポートできません。エクスポートした設定に、SSL や外部セキュリティで構成されたサーバーが含まれる場合、それを新しいホストにインポートした後、サーバー上でこれらのセキュリティ設定を再構成する必要があります。

注： MarkLogic 6 に保存された設定を MarkLogic 7 にインポートできます。ただし、MarkLogic 7 に保存された設定は MarkLogic 6 にインポートできません。

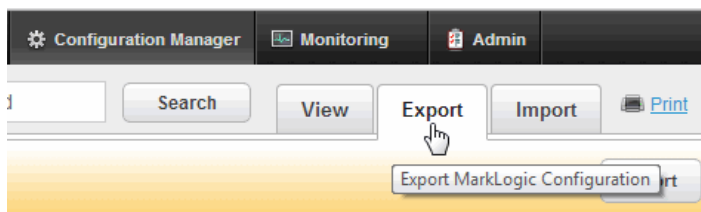
32.7.1 設定のエクスポート

リソース設定をエクスポートすると、それらの設定は zip ファイルに保存されます。これらの設定を再びインポートして、更新を比較、確認、および適用できます。

注： アプリケーションサーバーとデータベースの設定のみをエクスポートできます。ホスト、フォレスト、またはグループの設定はエクスポートできません。さらに、名前が 200 文字を超えるアプリケーションサーバーまたはデータベースはエクスポートできません。

次の手順では、設定をエクスポートする方法について説明します。

1. コンフィギュレーションマネージャに移動して、[Export] タブを選択します。



2. 設定をエクスポートするアプリケーションサーバーまたはデータベースを選択します。左側のフレームでカテゴリ名のチェックボックスをオンにして、データベースまたはサーバーのすべてを選択できます。例えば、すべてのデータベースを選択するには、次の手順を実行します。



注： 色付きのチェックボックスは、そのカテゴリ内のリソースの一部（ただしすべてではない）が選択されていることを示します。空白になるまでチェックボックスをクリックすると、選択したリソースをすべて選択解除できます。

3. アプリケーションサーバーが Modules データベースを利用する場合、追加のチェックボックスが [Modules] カラムに表示されます。アプリケーションサーバー設定とともに、Modules データベースをエクスポートするには、このボックスをオンにします。

注： 「セキュリティの考慮事項」(417 ページ) で説明しているように、Modules データベースのエクスポートおよびインポートには、適切なロールが必要です。

Servers			
Name	Include:	Modules	Settings
Admin [Default]			<input type="checkbox"/>
App-Services [Default]			<input checked="" type="checkbox"/>
HealthCheck [Default]			<input checked="" type="checkbox"/>
Manage [Default]			<input type="checkbox"/>
Oscars [Default]		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

4. エクスポートする設定すべてを選択したら、[Export] をクリックします。

The screenshot shows the Configuration Manager interface. At the top, there are buttons for Search, View, Export, Import, and Print. Below this is a yellow banner for 'Package Export' with the text 'Select the Resources to Export as a Package' and '16 resource(s) selected'. An 'Export' button is visible on the right. On the left, a sidebar shows 'Databases' with 13 items and 'Servers' with 5 items. The main area displays a table of servers with columns for Name, Include, Modules, and Settings. The 'Oscars [Default]' server is highlighted, and its 'Modules' checkbox is checked.

package{id}.zip の名前形式の zip ファイルが、ブラウザのダウンロードディレクトリにダウンロードされます。一意の ID が生成され、エクスポートされた各 zip ファイルの名前に追加されます。

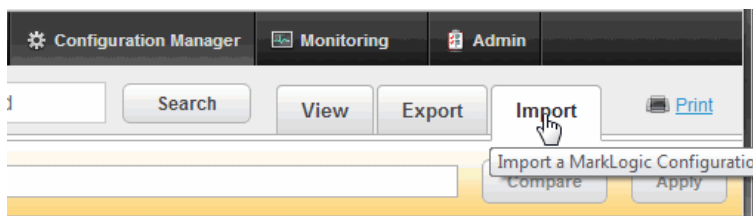
32.7.2 設定のインポート

コンフィギュレーションマネージャのインポート機能を使用して、以前にエクスポートした設定パッケージをアップロードして適用します。

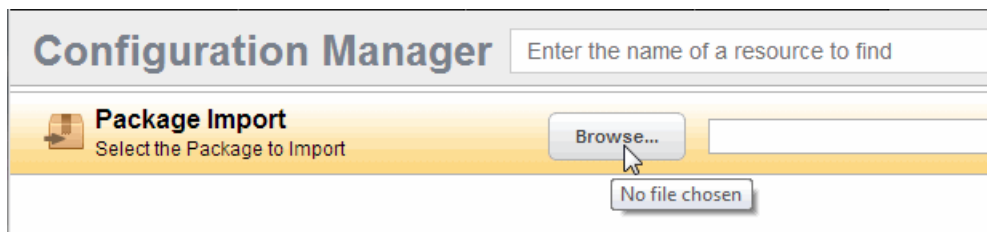
設定をインポートすると、保存した設定がコンフィギュレーションマネージャに読み込まれます。設定変更は自動的には行われません。設定（または設定の集まり）をインポートしたら、「インポートした設定と現在の設定との比較」（428 ページ）の説明に従って、設定を既存の設定と比較し、オプションとして設定変更を適用できます。

次の手順では、設定をインポートする方法について説明します。

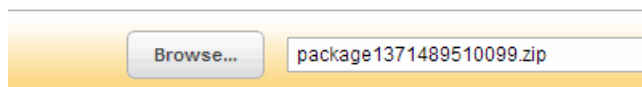
1. コンフィギュレーションマネージャに移動して、[Import] タブを選択します。



2. [Browse] をクリックし、エクスポートした zip ファイルの場所に移動します。



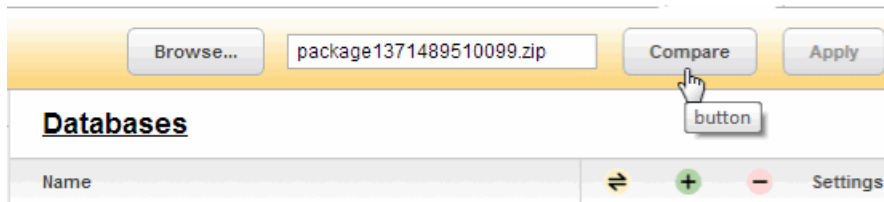
3. ポップアップディレクトリウィンドウが表示されます。パッケージ名をダブルクリックすると、[Browse] ボタンの横のフィールドにパッケージが表示されます。



32.7.3 インポートした設定と現在の設定との比較

このセクションでは、インポートした設定パッケージを現在の設定と比較する方法を説明し、また、インポートした設定を現在の設定にどのように適用するのかを特定する方法を説明します。

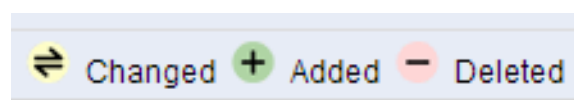
1. 設定をインポートした後、[Compare] ボタンをクリックして、インポートした設定を現在の設定と比較できます。



2. 現在の設定とインポートした設定との相違の要約が表示されます。リソースの相違の詳細を表示するには、下記の Documents データベースの例のようにリソースをクリックします。

Name	↔	+	-	Settings
Oscars-modules	0	0	0	<input checked="" type="checkbox"/>
Documents	6	1	0	<input checked="" type="checkbox"/>
Oscars	0	0	0	<input checked="" type="checkbox"/>

[Settings] の記号の意味は、ページ最下部の左側部分にある凡例に示されています。



3. リソースの [Configuration Settings] ページには、[Current] と [Package] の両方の設定が表示され、差異やエラーがあればこれらが強調表示されます。差異とエラーだけを表示するには、プルダウンメニューの [Show Differences & Errors] を選択します。エラーだけを表示するには、[Show Errors Only] を選択します。

Databases > Documents

Configuration Settings

Configuration Setting	Current	Package	
Enabled	true	true	<input type="checkbox"/>
Retired Forest Count	0	0	<input checked="" type="checkbox"/>
Language	en	en	<input checked="" type="checkbox"/>
Stemmed Searches	basic	basic	<input checked="" type="checkbox"/>
Word Searches	false	false	<input checked="" type="checkbox"/>
Word Positions	false	false	<input checked="" type="checkbox"/>
Fast Phrase Searches	false	true	<input checked="" type="checkbox"/>

4. デフォルトでは、パッケージングされた設定のすべてが現在の設定にインポートされます。パッケージングされた設定と競合する現在の設定を保持する場合は、その設定の [Import] チェックボックスをオフにして選択解除します。

Databases > Documents

Configuration Settings Show Differences & Errors

Configuration Setting	Current	Package	Import
Fast Phrase Searches	false	true	<input type="checkbox"/>
Element Word Positions	true	false	<input checked="" type="checkbox"/>
Field Value Positions	true	false	<input checked="" type="checkbox"/>
Uri Lexicon	false	true	<input type="checkbox"/>
Collection Lexicon	true	false	<input checked="" type="checkbox"/>
Maintain Last Modified	true	false	<input checked="" type="checkbox"/>

► Range Element Indexes + 1 - 0 Policy: Merge Import items:

5. 設定のいくつかは、コンテナに収納されています。これらは、コンテナ名の前に記された矢印で識別されます。矢印をクリックして、コンテナを展開して詳細を表示できます。例えば、レンジ要素インデックス設定間の差異を表示するには、下記のように [Range Element Indexes] コンテナの横の矢印をクリックします。

Browse... package1371573013943.zip Compare Apply

Databases > Documents

Configuration Settings filter Show Differences & Errors

Configuration Setting	Current	Package	Import
Fast Phrase Searches	false	true	<input checked="" type="checkbox"/>
Element Word Positions	true	false	<input checked="" type="checkbox"/>
Field Value Positions	true	false	<input checked="" type="checkbox"/>
Uri Lexicon	false	true	<input checked="" type="checkbox"/>
Collection Lexicon	true	false	<input checked="" type="checkbox"/>
Maintain Last Modified	true	false	<input checked="" type="checkbox"/>

Range Element Indexes + 1 - 0 Policy: Merge Import items:

6. コンテナ設定を現在の設定にどのようにインポートするかを設定できます。追加設定だけをインポートする場合は、[Merge] ポリシーを選択します。このポリシーでは、新しい設定だけがインポートされ、どの設定も現在の設定から削除されません。

▼ Range Element Indexes + 1 - 0 Policy: Merge Import items:

Scalar Type	<setting not defined>	unsig
Namespace Uri	<setting not defined>	http://marklogic.com/xdmp/dls
Localname	<setting not defined>	version-id
Collation	<setting not defined>	<setting not defined>
Range Value Positions	<setting not defined>	<setting not defined>
Invalid Values	<setting not defined>	reject

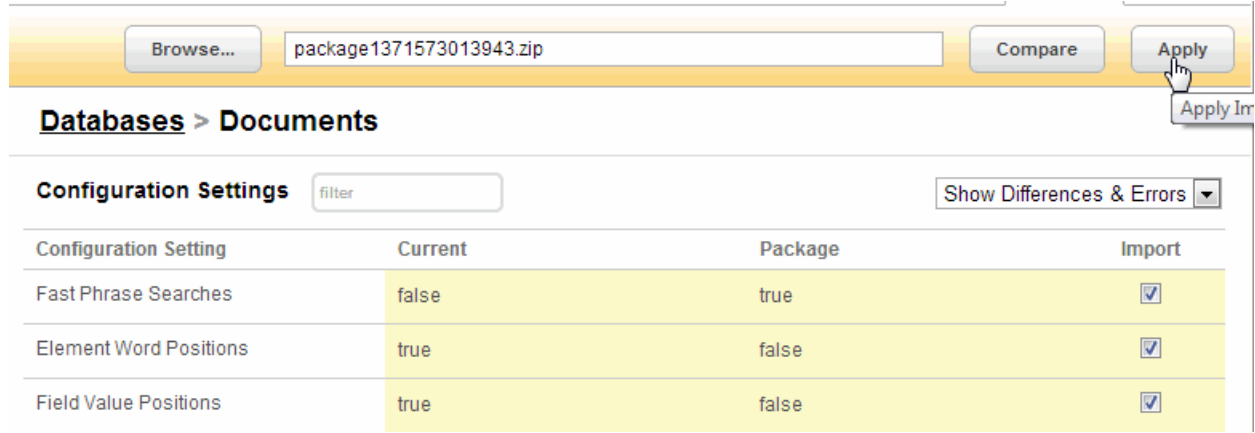
Select the policy for this setting container

7. インポートした設定に存在していない設定が現在の設定にある場合、[Replace] ポリシーを選択するとこれらの設定が表示されます。[Replace] ポリシーは現在の設定からこれらの設定を削除します。

▼ Range Element Indexes		+ 1	- 2	Policy: Replace	Import items: <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Scalar Type	<setting not defined>	unsig		Replace	<input checked="" type="checkbox"/>	
Namespace Uri	<setting not defined>	http://marklogic.com/xdmp/dls				
Localname	<setting not defined>	version-id				
Collation	<setting not defined>	<setting not defined>				
Range Value Positions	<setting not defined>	<setting not defined>				
Invalid Values	<setting not defined>	reject				
Scalar Type	date	<setting not defined>				
Namespace Uri	<setting not defined>	<setting not defined>				
Localname	update-date	<setting not defined>				
Collation	<setting not defined>	<setting not defined>				
Range Value Positions	<setting not defined>	<setting not defined>				
Invalid Values	reject	<setting not defined>				
Scalar Type	int	<setting not defined>				
Namespace Uri	<setting not defined>	<setting not defined>				
Localname	seconds	<setting not defined>				
Collation	<setting not defined>	<setting not defined>				
Range Value Positions	<setting not defined>	<setting not defined>				
Invalid Values	reject	<setting not defined>				

32.8 インポートした設定の適用

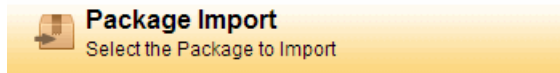
現在の設定の修正に使用する設定を選択し終わったら、[Apply] ボタンをクリックします。



The screenshot shows the MarkLogic configuration interface. At the top, there is a 'Browse...' button, a text input field containing 'package1371573013943.zip', a 'Compare' button, and an 'Apply' button. A mouse cursor is clicking on the 'Apply' button. Below this is a breadcrumb 'Databases > Documents'. Underneath is a 'Configuration Settings' section with a 'filter' input field and a 'Show Differences & Errors' dropdown menu. A table displays the configuration settings for 'Fast Phrase Searches', 'Element Word Positions', and 'Field Value Positions'. The 'Import' column for each row has a checked checkbox.

Configuration Setting	Current	Package	Import
Fast Phrase Searches	false	true	<input checked="" type="checkbox"/>
Element Word Positions	true	false	<input checked="" type="checkbox"/>
Field Value Positions	true	false	<input checked="" type="checkbox"/>

インポートの適用操作が成功したら、インポートした設定数の概要が表示されます。インポート操作により、インポートしたリソースの詳細を提示するチケットが生成されています。[link to details ticket] をクリックすることでこのチケットを表示できます。インポート操作をロールバックして、以前の設定をリストアする場合は、[link to rollback] をクリックします。



Package Import
Select the Package to Import

Imported package applied successfully

Imported: package_2013-9-16_12-28-43.zip

- 0 settings changed
- 63 settings added
- 0 settings deleted

Details ticket: [link to details ticket](#)

Rollback: [link to rollback](#)

注： インポート操作をロールバックしても、インポートしたフォレストは削除されません。

33.0 付録 A : 管理タスクの「ホット」と「コールド」

「ホット」管理タスクは、即座に有効になり、サーバーを再起動する必要がないタスクとして定義されます。「コールド」管理タスクは、変更を反映するために、サーバーの 1 つあるいは複数のインスタンスを再起動する必要があるタスクとして定義されます。コールドタスクは、管理画面で設定の横にアスタリスク (*) が付いています。

クラスタ型の実装では、「コールド」タスクは変更を反映するために、クラスタ内の 1 つあるいは複数のホストで MarkLogic のインスタンスを再起動する必要があります。単一サーバー実装では、「コールド」タスクは変更を反映するために、MarkLogic を再起動させます。

以降の表は、以下のオブジェクトタイプについて、オブジェクトの追加、設定パラメータの変更、およびオブジェクトの削除に対して「ホット」ステータスか「コールド」ステータスかを示したものです。

- [グループ](#)
- [HTTP、ODBC、XDBC、および WebDAV サーバー](#)
- [データベース](#)
- [ホスト](#)
- [フォレスト](#)
- [mimetype](#)
- [セキュリティ](#)

33.1 グループ

オブジェクトの追加	設定パラメータの変更	オブジェクトの削除
ホット	<p>次のグループパラメータはホットです。</p> <ul style="list-style-type: none"> > group name > system log level > file log level > rotate log files > keep log files > namespaces > schemas <p>次のグループパラメータは、グループ内のホストに対してコールドです。</p> <ul style="list-style-type: none"> > list cache size > compressed tree cache size > expanded tree cache size <p>グループに対するホストの追加と削除は、そのホストに対してコールドです。</p>	ホット

33.2 HTTP、ODBC、XDBC、および WebDAV サーバー

オブジェクトの追加	設定パラメータの変更	オブジェクトの削除
ホット	<p>次のアプリケーションサーバーパラメータはホットです。</p> <ul style="list-style-type: none"> > server name > root > database > request timeout > keep alive timeout > session timeout > time limit > realm > security mode > namespaces > schemas > ssl certificate template > ssl hostname > ssl ciphers <p>次のアプリケーションサーバーパラメータは、HTTP、ODBC、XDBC、または WebDAV サーバーを定義しているグループ内のすべてのホストに対してコールドです。</p> <ul style="list-style-type: none"> > port > address > backlog > threads > ssl enabled 	コールド

33.3 データベース

オブジェクトの追加	設定パラメータの変更	オブジェクトの削除
ホット	パラメータの変更はホットです。	ホット

33.4 ホスト

オブジェクトの追加	設定パラメータの変更	オブジェクトの削除
追加されたホストだけが再起動する必要があります。	パラメータを変更したホストだけが再起動する必要があります。 残りのホストはホットのままです。	残っているホストに対してホットです。

33.5 フォレスト

オブジェクトの追加	設定パラメータの変更	オブジェクトの削除
ホット	パラメータの変更はホットです。 バックアップはホットです。 リストア、クリア、および削除はホットです。	ホット

33.6 mimetype

オブジェクトの追加	設定パラメータの変更	オブジェクトの削除
コールド	パラメータの変更はコールドです。	コールド

33.7 セキュリティ

オブジェクトの追加	設定パラメータの変更	オブジェクトの削除
ホット	パラメータの変更はホットです。	ホット

34.0 付録 B : 事前定義された実行権限

次に示す事前定義された実行権限は、MarkLogic サーバーのすべてのインストールに含まれています。

名前	アクション URI	説明	保護する関数
admin-module-read	http://marklogic.com/xdmp/privileges/admin-module-read	設定情報を読み取るための Admin API を使用する権限	admin ビルトイン
admin-module-write	http://marklogic.com/xdmp/privileges/admin-module-write	設定情報を書き込むための Admin API を使用する権限	admin ビルトイン
admin-ui	http://marklogic.com/xdmp/privileges/admin-ui	管理画面を使用する権限	admin ビルトイン
amp-add-roles	http://marklogic.com/xdmp/privileges/amp-add-roles	Amp に追加ロールを割り当てる権限	sec:amp-add-roles
amp-change-database	http://marklogic.com/xdmp/privileges/amp-change-database	Amp に追加ロールを割り当てる権限	sec:amps-change-modules-database
amp-get-roles	http://marklogic.com/xdmp/privileges/amp-get-roles	Amp に関連付けられたロールを取得する権限	sec:amp-get-roles
amp-remove-roles	http://marklogic.com/xdmp/privileges/amp-remove-roles	Amp に割り当てられたロールを削除する権限	sec:amp-remove-roles
amp-set-roles	http://marklogic.com/xdmp/privileges/amp-set-roles	Amp に関連付けられたロールを設定する権限	sec-amp-set-roles
any-collection	http://marklogic.com/xdmp/privileges/any-collection	保護されているかどうかに関係なく任意のコレクションに追加したり、任意のコレクションから削除する権限	xdmp:document-add-collections、 xdmp:document-remove-collections、 xdmp:document-set-collections
any-uri	http://marklogic.com/xdmp/privileges/any-uri	URI が保護されているかどうかに関係なく任意の URI でドキュメントを作成する権限	xdmp:document-insert、 xdmp:document-load、 xdmp:load
app-builder	http://marklogic.com/xdmp/privileges/app-builder	Application Builder UI を使用する権限	
cancel-any-requests	http://marklogic.com/xdmp/privileges/cancel-any-requests	リクエストのキャンセルを試みているすべてのユーザーが実行したリクエストをキャンセルする権限	admin ビルトイン
cancel-my-requests	http://marklogic.com/xdmp/privileges/cancel-my-requests	リクエストのキャンセルを試みているユーザーが実行したリクエストをキャンセルする権限	admin ビルトイン

名前	アクション URI	説明	保護する関数
collection-add-permissions	http://marklogic.com/xdmp/privileges/collection-add-permissions	パーミッションをコレクションに追加する権限	sec:get-collections、 sec:collection-add-permissions
collection-get-permissions	http://marklogic.com/xdmp/privileges/collection-get-permissions	コレクションに対するパーミッションを取得する権限	sec:collection-get-permissions
collection-remove-permissions	http://marklogic.com/xdmp/privileges/collection-remove-permissions	コレクションからパーミッションを削除する権限	sec:get-collections、 sec:collection-remove-permissions
collection-set-permissions	http://marklogic.com/xdmp/privileges/collection-set-permissions	コレクションに対するパーミッションを設定する権限	sec:get-collections、 sec:collection-set-permissions
compartment-get-roles	http://marklogic.com/xdmp/privileges/compartment-get-roles	コンパートメントに対するロールを取得する権限	sec:compartment-get-roles
complete-any-transactions	http://marklogic.com/xdmp/privileges/complete-any-transactions	任意のトランザクションにトランザクションビルトインを使用する権限	xdmp:transaction-commit、 xdmp:xa-complete
complete-my-transactions	http://marklogic.com/xdmp/privileges/complete-my-transactions	現在のユーザーが開始したトランザクションにトランザクションビルトインを使用する権限	xdmp:transaction-commit、 xdmp:xa-complete
count-builtins	http://marklogic.com/xdmp/privileges/counts	xdmp:forest-counts を実行する権限	xdmp:forest-counts
create-amp	http://marklogic.com/xdmp/privileges/create-amp	Amp を作成する権限	sec:create-amp
create-domain	http://marklogic.com/xdmp/privileges/create-domain	ドメインを作成する権限	dom:create
create-pipeline	http://marklogic.com/xdmp/privileges/create-pipeline	パイプラインを作成する権限	p:insert p:create
create-privilege	http://marklogic.com/xdmp/privileges/create-privilege	権限を作成する権限	sec:create-role
create-role	http://marklogic.com/xdmp/privileges/create-role	ロールを作成する権限	sec:create-role
create-trigger	http://marklogic.com/xdmp/privileges/create-trigger	トリガーを作成する権限	trgr:create-trigger
create-user	http://marklogic.com/xdmp/privileges/create-user	ユーザーを作成する権限	sec:create-user
debug-any-requests	http://marklogic.com/xdmp/privileges/debug-any-requests	任意のユーザーからのすべてのリクエストをデバッグする権限	debug ビルトイン

名前	アクション URI	説明	保護する関数
debug-my-requests	http://marklogic.com/xdmp/privileges/debug-my-requests	自身のリクエストをデバッグする権限	debug ビルトイン
dls-admin	http://marklogic.com/xdmp/privileges/dls-admin	ライブラリサービスを設定する権限	dls:break-checkout、 dls:retention-rule、 dls:retention-rule-insert、 dls:retention-rule-remove

名前	アクション URI	説明	保護する関数
dls-user	http://marklogic.com/xdmp/privileges/dls-user	ライブラリサービスを使用する権限	dls:as-of-query dls:author-query dls:document-add-collections dls:document-add-permissions dls:document-add-properties dls:document-checkin dls:document-checkout dls:document-checkout-status dls:document-delete dls:document-extract-part dls:document-get-permissions dls:document-history dls:document-include-query dls:document-insert-and-manage dls:document-is-managed dls:document-manage dls:document-purge dls:document-remove-collections dls:document-remove-permissions dls:document-remove-properties dls:document-retention-rules dls:document-set-collections dls:document-set-permissions dls:document-set-properties dls:document-set-property dls:document-set-quality dls:document-unmanage dls:document-update dls:document-version dls:document-version-as-of dls:document-version-delete dls:document-version-query dls:document-version-uri dls:document-versions-query dls:documents-query dls:link-expand dls:link-references dls:node-expand dls:purge dls:retention-rules

名前	アクション URI	説明	保護する関数
flexrep-admin	http://marklogic.com/xdmp/privileges/flexrep-admin	フレキシブルレプリケーションを管理する権限	フレキシブルレプリケーションの関数
flexrep-internal	http://marklogic.com/xdmp/privileges/flexrep-internal	フレキシブルレプリケーション関数の Amp 化に使用	flexible-internal
flexrep-user	http://marklogic.com/xdmp/privileges/flexrep-user	フレキシブルレプリケーションを使用する権限	フレキシブルレプリケーションのユーザー関数
forget-any-xa-transactions	http://marklogic.com/xdmp/privileges/forget-any-xa-transactions	任意のトランザクションの XA トランザクションを消去するためのビルトインを実行する権限	xdmp:xa-forget、 xdmp:xq-forget-xid
forget-my-xa-transactions	http://marklogic.com/xdmp/privileges/forget-my-xa-transactions	ユーザーのトランザクションの XA トランザクションを消去するためのビルトインを実行する権限	xdmp:xa-forget、 xdmp:xq-forget-xid
get-amp	http://marklogic.com/xdmp/privileges/get-amp	Amp を取得する権限	sec:get-amp
get-compartments	http://marklogic.com/xdmp/privileges/get-compartments	コンパートメントを取得する権限	sec:get-compartments
get-privilege	http://marklogic.com/xdmp/privileges/get-privilege	アクション URI およびタイプから権限を取得する権限	sec:get-privilege
get-role-ids	http://marklogic.com/xdmp/privileges/get-role-ids	ロール ID を取得する権限	内部関数
get-role-names	http://marklogic.com/xdmp/privileges/get-role-names	ロール名を取得する権限	内部関数
get-user-names	http://marklogic.com/xdmp/privileges/get-user-names	ユーザー名を取得する権限	sec:get-user-names

名前	アクション URI	説明	保護する関数
grant-all-roles	http://marklogic.com/xdmp/privileges/grant-all-roles	ユーザーにすべてのロールを付与する権限 grant-all-roles または grant-my-roles のどちらかが、ロールを割り当てる関数で必要になります。	sec:create-user、 sec:user-set-roles、 sec:user-add-roles、 sec:user-remove-roles、 sec:create-role、 sec:role-set-roles、 sec:role-add-roles、 sec:role-remove-roles、 sec:remove-role-from-roles、 sec:remove-role-from-privileges、 sec:remove-role-from-amps、 sec:create-role、 sec:privilege-set-roles、 sec:privilege-add-roles、 sec:privilege-remove-roles、 sec:create-amp、 sec:amp-set-roles、 sec:amp-add-roles、 sec:amp-remove-roles

名前	アクション URI	説明	保護する関数
grant-my-roles	http://marklogic.com/xdmp/privileges/grant-my-roles	ユーザーに自分のロールを付与する権限 grant-all-roles または grant-my-roles のどちらかが、ロールを割り当てる関数で必要になります。	sec:create-user、 sec:user-set-roles、 sec:user-add-roles、 sec:user-remove-roles、 sec:create-role、 sec:role-set-roles、 sec:role-add-roles、 sec:role-remove-roles、 sec:remove-role-from-roles、 sec:remove-role-from-privileges、 sec:remove-role-from-amps、 sec:create-role、 sec:privilege-set-roles、 sec:privilege-add-roles、 sec:privilege-remove-roles、 sec:create-amp、 sec:amp-set-roles、 sec:amp-add-roles、 sec:amp-remove-roles
hadoop-user-read	http://marklogic.com/xdmp/privileges/hadoop-user-read	MarkLogic サーバーからデータを読み取る Hadoop MapReduce ジョブの入力として MarkLogic サーバーを使用する権限	Hadoop パッケージ内の Java API
hadoop-user-write	http://marklogic.com/xdmp/privileges/hadoop-user-write	MarkLogic サーバーからデータを書き込む Hadoop MapReduce ジョブの入力として MarkLogic サーバーを使用する権限	Hadoop パッケージ内の Java API
infostudio	http://marklogic.com/xdmp/privileges/infostudio	Information Studio を使用する権限	Information Studio の関数
管理	http://marklogic.com/xdmp/privileges/manage	管理 API を実行する権限	package:add-database、 package:add-appserver、 管理 API 内のすべてのリソースアドレス
odbc:eval	http://marklogic.com/xdmp/privileges/odbc-eval	ODBC から eval ステートメントを実行する権限	xdmp:eval

名前	アクション URI	説明	保護する関数
odbc:eval-in	http://marklogic.com/xdmp/privileges/odbc-eval-in	ODBC から eval-in ステートメントを実行する権限	xdmp:eval-in
odbc:eval-modules-change	http://marklogic.com/xdmp/privileges/ odbc-eval-modules-change	ODBC から Modules データベースを変更する eval ステートメントを実行する権限	xdmp:eval
odbc:eval-modules-change-file	http://marklogic.com/xdmp/privileges/ odbc-eval-modules-change-file	ODBC からファイルシステムルートを変更する eval ステートメントを実行する権限	xdmp:eval
odbc:insert	http://marklogic.com/xdmp/privileges/odbc-insert	ODBC から insert ステートメントを実行する権限	odbc insert
odbc:insert-in	http://marklogic.com/xdmp/privileges/odbc-insert-in	ODBC から insert ステートメントを実行する権限	別のデータベースへの odbc insert
odbc:invoke	http://marklogic.com/xdmp/privileges/odbc-invoke	ODBC から invoke ステートメントを実行する権限	odbc invoke
odbc:invoke-in	http://marklogic.com/xdmp/privileges/odbc-invoke-in	ODBC から invoke ステートメントを実行する権限	別のデータベースへの odbc invoke
odbc:invoke-modules-change	http://marklogic.com/xdmp/privileges/ odbc-invoke-modules-change	ODBC から Modules データベースを変更する invoke ステートメントを実行する権限	Modules データベースを変更する odbc invoke
odbc:invoke-modules-change-file	http://marklogic.com/xdmp/privileges/ odbc-invoke-modules-change-file	ODBC からファイルシステムルートを変更する invoke ステートメントを実行する権限	ファイルシステムルートを変更する odbc invoke
odbc:spawn	http://marklogic.com/xdmp/privileges/odbc-spawn	ODBC から spawn ステートメントを実行する権限	odbc spawn
odbc:spawn-in	http://marklogic.com/xdmp/privileges/odbc-spawn-in	ODBC から spawn ステートメントを実行する権限	別のデータベースへの odbc spawn
odbc:spawn-modules-change	http://marklogic.com/xdmp/privileges/ odbc-spawn-modules-change	ODBC から Modules データベースを変更する spawn ステートメントを実行する権限	Modules データベースを変更する odbc spawn
odbc:spawn-modules-change-file	http://marklogic.com/xdmp/privileges/ odbc-spawn-modules-change-file	ODBC からファイルシステムルートを変更する spawn ステートメントを実行する権限	ファイルシステムルートを変更する odbc spawn

名前	アクション URI	説明	保護する関数
pki	http://marklogic.com/xdmp/privileges/pki	PKI 関数を使用する権限	pki:create-template、 pki:delete-certificate、 pki:delete-template、 pki:generate-certificate-request、 pki:generate-template-certificate-authority、 pki:generate-temporary-certificate、 pki:generate-temporary-certificate-if-necessary、 pki:get-certificate、 pki:get-certificate-pem、 pki:get-certificate-xml、 pki:get-certificates、 pki:get-certificates-for-template、 pki:get-certificates-for-template-xml、 pki:get-pending-certificate-request、 pki:get-pending-certificate-requests-pem、 pki:get-pending-certificate-requests-xml、 pki:get-template、 pki:get-template-by-name、 pki:get-template-certificate-authority、 pki:get-template-ids、 pki:get-trusted-certificate-ids、 pki:insert-certificate-revocation-list、 pki:insert-signed-certificates、 pki:insert-template、 pki:insert-trusted-certificates、 pki:is-temporary、 pki:need-certificate、 pki:template-get-description、 pki:template-get-id、 pki:template-get-key-options、 pki:template-get-key-type、 pki:template-get-name、 pki:template-get-request、 pki:template-get-version、 pki:template-in-use、 pki:template-set-description、 pki:template-set-key-options、 pki:template-set-key-type、 pki:template-set-name、 pki:template-set-request

名前	アクション URI	説明	保護する関数
plugin-register	http://marklogic.com/xdmp/privileges/plugin-register	プラグイン API を使用する権限	plugin:register
plugin-server-fields	http://marklogic.com/xdmp/privileges/plugin-server-fields	プラグイン API を使用する権限	プラグイン API で使用
prepare-any-xa-transactions	http://marklogic.com/xdmp/privileges/prepare-any-xa-transactions	任意のトランザクションの XA トランザクションを準備するためのビルトインを実行する権限	xdmp:xa-prepare
prepare-my-xa-transactions	http://marklogic.com/xdmp/privileges/prepare-my-xa-transactions	ユーザーのトランザクションの XA トランザクションを準備するためのビルトインを実行する権限	xdmp:xa-prepare
privilege-add-roles	http://marklogic.com/xdmp/privileges/privilege-add-roles	追加ロールに権限を割り当てる権限	sec:privilege-add-roles
privilege-get-roles	http://marklogic.com/xdmp/privileges/privilege-get-roles	権限に関連付けられたすべてのロールを取得する権限	sec:privilege-get-roles
privilege-remove-roles	http://marklogic.com/xdmp/privileges/privilege-remove-roles	割り当てられているロールから権限を削除する権限	sec:privilege-remove-roles
privilege-set-name	http://marklogic.com/xdmp/privileges/privilege-set-name	権限の名前を設定する権限	sec:privilege-set-name
privilege-set-roles	http://marklogic.com/xdmp/privileges/privilege-set-roles	権限に関連付けられたロールを設定する権限	sec:privilege-set-roles
profile-any-requests	http://marklogic.com/xdmp/privileges/profile-any-requests	任意のユーザーが開始したリクエストをプロファイリングする権限	prof:enable および他のプロファイル API
profile-my-requests	http://marklogic.com/xdmp/privileges/profile-my-requests	プロファイリングの呼び出し元のリクエストを実行しているユーザーによって開始されたリクエストをプロファイリングする権限	prof:enable および他のプロファイル API
protect-collection	http://marklogic.com/xdmp/privileges/protect-collection	新しいまたは既存のコレクションを保護する権限	sec:protect-collection
qconsole	http://marklogic.com/xdmp/privileges/qconsole	クエリコンソールを実行する権限	
remove-amp	http://marklogic.com/xdmp/privileges/remove-amp	セキュリティデータベースから Amp を削除する権限	sec:remove-amp
remove-privilege	http://marklogic.com/xdmp/privileges/remove-privilege	セキュリティデータベースから権限を削除する権限	sec:remove-privilege
remove-role	http://marklogic.com/xdmp/privileges/remove-role	セキュリティデータベースからロールを削除する権限	sec:remove-role
remove-role-from-amps	http://marklogic.com/xdmp/privileges/remove-role-from-amps	セキュリティデータベースのすべての Amp からロールを削除する権限	sec:remove-role-from-amps

名前	アクション URI	説明	保護する関数
remove-role-from-privileges	http://marklogic.com/xdmp/privileges/remove-role-from-privileges	セキュリティデータベースのすべての権限からロールを削除する権限	sec:remove-role-from-privileges
remove-role-from-roles	http://marklogic.com/xdmp/privileges/remove-role-from-roles	セキュリティデータベースのすべてのロールからロールを削除する権限	sec:remove-role-from-roles
remove-role-from-users	http://marklogic.com/xdmp/privileges/remove-role-from-users	セキュリティデータベースのすべてのユーザーからロールを削除する権限	sec:remove-role-from-users
remove-user	http://marklogic.com/xdmp/privileges/remove-user	セキュリティデータベースからユーザーを削除する権限	sec:remove-user
rest-admin	http://marklogic.com/xdmp/privileges/rest-admin	REST API を使用して管理タスクを実行する権限	REST API
rest-reader	http://marklogic.com/xdmp/privileges/rest-reader	REST API を使用して読み取り操作を実行する権限	REST API
rest-writer	http://marklogic.com/xdmp/privileges/rest-writer	REST API を使用して更新タスクを実行する権限	REST API
role-add-roles	http://marklogic.com/xdmp/privileges/role-add-roles	指定されたロールに含まれるロールにロールを追加する権限	sec:role-add-roles
role-get-compartment	http://marklogic.com/xdmp/privileges/role-get-compartment	ロールのコンパートメントを取得する権限	sec:role-get-compartment
role-get-default-collections	http://marklogic.com/xdmp/privileges/role-get-default-collections	ロールのデフォルトのコレクションを取得する権限	sec:role-get-default-collections
role-get-default-permissions	http://marklogic.com/xdmp/privileges/role-get-default-permissions	ロールのデフォルトのパーミッションを取得する権限	sec:role-get-default-permissions
role-get-description	http://marklogic.com/xdmp/privileges/role-get-description	ロールの説明を取得する権限	sec:role-get-description
role-get-roles	http://marklogic.com/xdmp/privileges/role-get-roles	指定したロールに含まれているすべてのロールを取得する権限	sec:role-get-roles
role-privileges	http://marklogic.com/xdmp/privileges/role-privileges	所定のロールのすべての権限を取得する権限	sec:role-privileges
role-remove-roles	http://marklogic.com/xdmp/privileges/role-remove-roles	指定のロールに含まれるロールからロールを削除する権限	sec:role-remove-roles
role-set-default-collections	http://marklogic.com/xdmp/privileges/role-set-default-collections	ロールのデフォルトのコレクションを設定する権限	sec:role-set-default-collections

名前	アクション URI	説明	保護する関数
role-set-default-permissions	http://marklogic.com/xdmp/privileges/role-set-default-permissions	ロールのデフォルトのパーミッションを設定する権限	sec:role-set-default-permissions
role-set-description	http://marklogic.com/xdmp/privileges/role-set-description	ロールの名前を設定する権限	sec:role-set-description
role-set-name	http://marklogic.com/xdmp/privileges/role-set-name	ロールの名前を変更する権限	sec:role-set-name
role-set-roles	http://marklogic.com/xdmp/privileges/role-set-roles	指定のロール内のすべてのロールを変更する権限	sec:role-set-roles
sem:sparql	http://marklogic.com/xdmp/privileges/sem-sparql	SPARQL のクエリを実行する権限	sem:sparql
sem:sparql-update	http://marklogic.com/xdmp/privileges/sem-sparql-update	SPARQL の更新を実行する権限	sem:sparql-update
set-any-time-limit	http://marklogic.com/xdmp/privileges/xdmp-set-request-time-limit-any	リクエスト時間制限を変更する権限	xdmp:set-request-time-limit
set-any-transaction-name	http://marklogic.com/xdmp/privileges/xdmp-set-transaction-name-any	任意のトランザクションの名前を設定する権限	xdmp:set-transaction-name
set-any-transaction-time-limit	http://marklogic.com/xdmp/privileges/xdmp-set-transaction-time-limit-any	任意のトランザクションの時間制限を設定する権限	xdmp:set-transaction-time-limit
set-my-time-limit	http://marklogic.com/xdmp/privileges/xdmp-set-request-time-limit-my	リクエスト時間制限を変更する権限	xdmp:set-request-time-limit
set-my-transaction-name	http://marklogic.com/xdmp/privileges/xdmp-set-transaction-name-my	ユーザーのトランザクションの名前を設定する権限	xdmp:set-transaction-name
set-my-transaction-time-limit	http://marklogic.com/xdmp/privileges/xdmp-set-transaction-time-limit-my	ユーザーのトランザクションの時間制限を設定する権限	xdmp:set-transaction-time-limit
status-builtins	http://marklogic.com/xdmp/privileges/status-builtins	status ビルトインにアクセスする権限	status ビルトイン
unprotect-collection	http://marklogic.com/xdmp/privileges/unprotect-collection	コレクションのロールを変更する権限	xdmp:document-add-collections、 xdmp:document-remove-collections、 xdmp:document-set-collections
unprotected-collections	http://marklogic.com/xdmp/privileges/unprotected-collections	保護されていないコレクションに対して追加または削除する権限	xdmp:document-add-collections、 xdmp:document-remove-collections、 xdmp:document-set-collections

名前	アクション URI	説明	保護する関数
unprotected-uri	http://marklogic.com/xdmp/privileges/unprotected-uri	保護されていない URI でドキュメントを作成する権限	xdmp:document-insert、 xdmp:load
user-add-roles	http://marklogic.com/xdmp/privileges/user-add-roles	ユーザーにロールを追加する権限	sec:user-add-roles
user-get-default-collections	http://marklogic.com/xdmp/privileges/ user-gt-default-collections	ユーザーのデフォルトのコレクションを取得する権限	sec:user-get-default-collections
user-get-default-permissions	http://marklogic.com/xdmp/privileges/ user-get-default-permissions	ユーザーのデフォルトのパーミッションを取得する権限	sec:user-get-default-permissions
user-get-description	http://marklogic.com/xdmp/privileges/user-get-description	ユーザーの説明を取得する権限	sec:user-get-description (ユーザーとしてログインしていない場合)
user-get-password-extra	http://marklogic.com/xdmp/privileges/ user-get-password-extra	ユーザードキュメントから password-extra 要素を取得する権限	sec:user-get-password-extra
user-get-roles	http://marklogic.com/xdmp/privileges/user-get-roles	ユーザーのロールを取得する権限	sec:user-get-roles (ユーザーとしてログインしていない場合)
user-privileges	http://marklogic.com/xdmp/privileges/user-privileges	ユーザーの完全な権限を取得する権限	sec:user-privileges (ユーザーとしてログインしていない場合)
user-remove-roles	http://marklogic.com/xdmp/privileges/user-remove-roles	ユーザーからロールを削除する権限	sec:user-remove-roles
user-set-default-collections	http://marklogic.com/xdmp/privileges/ user-set-default-collections	ユーザーのデフォルトのコレクションを設定する権限	sec:user-set-default-collections
user-set-default-permissions	http://marklogic.com/xdmp/privileges/ user-set-default-permissions	ユーザーのデフォルトのパーミッションを設定する権限	sec:user-set-default-permissions
user-set-description	http://marklogic.com/xdmp/privileges/user-set-description	ユーザーの説明を設定する権限	sec:user-set-description (ユーザーとしてログインしていない場合)
user-set-name	http://marklogic.com/xdmp/privileges/user-set-name	ユーザーの名前を設定する権限	sec:user-set-name (ユーザーとしてログインしていない場合)
user-set-password	http://marklogic.com/xdmp/privileges/user-set-password	ユーザーのパスワードを設定する権限	sec:user-set-password (ユーザーとしてログインしていない場合)

名前	アクション URI	説明	保護する関数
user-set-password-extra	http://marklogic.com/xdmp/privileges/ user-set-password-extra	ユーザー ドキュメントで password-extra 要素を設定する権限	sec:user-set-password-extra
user-set-roles	http://marklogic.com/xdmp/privileges/user-set-roles	ユーザーのロールを設定する権限	sec:user-set-roles
xdbc:eval	http://marklogic.com/xdmp/privileges/xdbc-eval	XCC または XDBC から eval ステートメントを実行する権限	xdmp:eval
xdbc:eval-in	http://marklogic.com/xdmp/privileges/xdbc-eval-in	XCC または XDBC から eval-in ステートメントを実行する権限	xdmp:eval-in
xdbc:eval-modules-change	http://marklogic.com/xdmp/privileges/ xdbc-eval-modules-change	XCC または XDBC から Modules データベースを変更する eval ステートメントを実行する権限	xdmp:eval
xdbc:eval-modules-change-file	http://marklogic.com/xdmp/privileges/ xdbc-eval-modules-change-file	XCC または XDBC からファイルシステムルートを変更する eval ステートメントを実行する権限	xdmp:eval
xdbc:insert	http://marklogic.com/xdmp/privileges/xdbc-insert-in	XCC または XDBC から insert ステートメントを実行する権限	xcc または xdbc insert
xdbc:insert-in	http://marklogic.com/xdmp/privileges/xdbc-insert-in	XCC または XDBC から insert ステートメントを実行する権限	別のデータベースへの xdbc または xcc insert
xdbc:invoke	http://marklogic.com/xdmp/privileges/xdbc-invoke	XCC または XDBC から invoke ステートメントを実行する権限	xdbc または xcc invoke
xdbc:invoke-in	http://marklogic.com/xdmp/privileges/xdbc-invoke-in	XCC または XDBC から invoke ステートメントを実行する権限	別のデータベースへの xdbc または xcc invoke
xdbc:invoke-modules-change	http://marklogic.com/xdmp/privileges/ xdbc-invoke-modules-change	XCC または XDBC から Modules データベースを変更する invoke ステートメントを実行する権限	Modules データベースを変更する xdbc または xcc invoke
xdbc:invoke-modules-change-file	http://marklogic.com/xdmp/privileges/ xdbc-invoke-modules-change-file	XCC または XDBC からファイルシステムルートを変更する invoke ステートメントを実行する権限	ファイルシステムルートを変更する xdbc または xcc invoke
xdbc:spawn	http://marklogic.com/xdmp/privileges/xdbc-spawn	XCC または XDBC から spawn ステートメントを実行する権限	xdbc または xcc spawn
xdbc:spawn-in	http://marklogic.com/xdmp/privileges/xdbc-spawn-in	XCC または XDBC から spawn ステートメントを実行する権限	別のデータベースへの xdbc または xcc spawn

名前	アクション URI	説明	保護する関数
xdbc:spawn-modules-change	http://marklogic.com/xdmp/privileges/ xdbc-spawn-modules-change	XCC または XDBC から Modules データベースを変更する spawn ステートメントを実行する権限	Modules データベースを変更する xdbc または xcc spawn
xdbc:spawn-modules-change-file	http://marklogic.com/xdmp/privileges/ xdbc-spawn-modules-change-file	XCC または XDBC からファイルシステムルートを変更する spawn ステートメントを実行する権限	ファイルシステムルートを変更する xdbc または xcc spawn
xdmp:add-response-header	http://marklogic.com/xdmp/privileges/ xdmp-add-response-header	リクエスト関数にレスポンスヘッダを追加する関数を使用する権限	admin ビルトイン、alert-user
xdmp:address-bindable	http://marklogic.com/xdmp/privileges/ xdmp-address-bindable	admin 関数を実行する権限	admin ビルトイン
xdmp:alert-admin	http://marklogic.com/xdmp/privileges/xdmp-alert-admin	アラート admin 関数を実行する権限	alert-admin
xdmp:alert-internal	http://marklogic.com/xdmp/privileges/xdmp-alert-internal	アラート API 関数で使用される権限	alert-internal
xdmp:alert-user	http://marklogic.com/xdmp/privileges/xdmp-alert-user	ユーザーレベルのアラート関数を実行する権限	alert-user、alert-admin
xdmp:amp-roles	http://marklogic.com/xdmp/privileges/xdmp-amp-roles	Amp のロールを取得する権限	xdmp:amp-roles
xdmp:binary-join	http://marklogic.com/xdmp/privileges/xdmp-binary-join	binary-join ビルトインを実行する権限	xdmp:binary-join
xdmp:compressed-tree-cache-partitions	http://marklogic.com/xdmp/privileges/ xdmp-compressed-tree-cache-partitions	admin 関数を実行する権限	admin ビルトイン
xdmp:compressed-tree-cache-size	http://marklogic.com/xdmp/privileges/ xdmp-compressed-tree-cache-size	admin 関数を実行する権限	admin ビルトイン
xdmp:data-directory	http://marklogic.com/xdmp/privileges/xdmp-data-directory	データディレクトリにアクセスする権限	admin ビルトイン
xdmp:database-backup	http://marklogic.com/xdmp/privileges/ xdmp-database-backup	データベースバックアップを実行する権限	admin ビルトイン
xdmp:database-backup-cancel	http://marklogic.com/xdmp/privileges/ xdmp-database-backup-cancel	データベースバックアップをキャンセルする権限	admin ビルトイン
xdmp:database-backup-purge	http://marklogic.com/xdmp/privileges/ xdmp-database-backup-purge	データベースバックアップをバージする権限	admin ビルトイン
xdmp:database-backup-status	http://marklogic.com/xdmp/privileges/ xdmp-database-backup-status	データベースバックアップのステータスを取得する権限	admin ビルトイン

名前	アクション URI	説明	保護する関数
xdmp:database-backup-validate	http://marklogic.com/xdmp/privileges/xdmp-database-backup-validate	データベースバックアップを検証する権限	admin ビルトイン
xdmp:database-restore	http://marklogic.com/xdmp/privileges/xdmp-database-restore	データベースリストアを実行する権限	admin ビルトイン
xdmp:database-restore-cancel	http://marklogic.com/xdmp/privileges/xdmp-database-backup	データベースリストアをキャンセルする権限	admin ビルトイン
xdmp:database-restore-status	http://marklogic.com/xdmp/privileges/xdmp-database-restore-status	データベースリストアのステータスを取得する権限	admin ビルトイン
xdmp:database-restore-validate	http://marklogic.com/xdmp/privileges/xdmp-database-restore-validate	データベースリストアを検証する権限	admin ビルトイン
xdmp:default-in-memory-limit	http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-limit	admin 関数を実行する権限	admin ビルトイン
xdmp:default-in-memory-list-size	http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-list-size	admin 関数を実行する権限	admin ビルトイン
xdmp:default-in-memory-range-index-size	http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-range-index-size	admin 関数を実行する権限	admin ビルトイン
xdmp:default-in-memory-reverse-index-size	http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-reverse-index-size	admin 関数を実行する権限	admin ビルトイン
xdmp:default-in-memory-tree-size	http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-tree-size	admin 関数を実行する権限	admin ビルトイン
xdmp:default-journal-count	http://marklogic.com/xdmp/privileges/xdmp-default-journal-count	admin 関数を実行する権限	admin ビルトイン
xdmp:default-journal-size	http://marklogic.com/xdmp/privileges/xdmp-default-journal-size	admin 関数を実行する権限	admin ビルトイン
xdmp:default-preallocate-journals	http://marklogic.com/xdmp/privileges/xdmp-default-preallocate-journals	admin 関数を実行する権限	admin ビルトイン
xdmp:delete-cluster-config-file	http://marklogic.com/xdmp/privileges/xdmp-delete-cluster-config-file	admin 関数を実行する権限	admin ビルトイン

名前	アクション URI	説明	保護する関数
xdmp:delete-host-config-file	http://marklogic.com/xdmp/privileges/ xdmp-delete-host-config-file	admin 関数を実行する権限	admin ビルトイン
xdmp:disable-event	http://marklogic.com/xdmp/privileges/xdmp-disable-event	admin 関数を実行する権限	admin ビルトイン
xdmp:document-get	http://marklogic.com/xdmp/privileges/xdmp-document-get	関数を実行する権限	xdmp:document-get
xdmp:document-load	http://marklogic.com/xdmp/privileges/xdmp-document-load	関数を実行する権限	xdmp:document-load
xdmp:email	http://marklogic.com/xdmp/privileges/xdmp-email	メールする権限	xdmp:email
xdmp:email-address	http://marklogic.com/xdmp/privileges/xdmp-email-address	admin 関数を実行する権限	admin ビルトイン
xdmp:enable-event	http://marklogic.com/xdmp/privileges/xdmp-enable-event	admin 関数を実行する権限	admin ビルトイン
xdmp:eval	http://marklogic.com/xdmp/privileges/xdmp-eval	eval 関数を実行する権限	xdmp:eval
xdmp:eval-in	http://marklogic.com/xdmp/privileges/xdmp-eval-in	eval-in 関数を実行する権限	xdmp:eval-in
xdmp:eval-modules-change	http://marklogic.com/xdmp/privileges/ xdmp-eval-modules-change	Modules データベースを変更する eval ステートメント を実行する権限	Modules データベースを変更する xdmp:eval ステートメント
xdmp:eval-modules-change-file	http://marklogic.com/xdmp/privileges/ xdmp-eval-modules-change-file	ファイルシステムルートを変更する eval ステートメント を実行する権限	ファイルシステムルートを変更する xdmp:eval ステートメント
xdmp:eval-transaction	http://marklogic.com/xdmp/privileges/ xdmp-eval-transaction	トランザクションオプションとともに eval ステートメント を実行する権限	新しいトランザクションを開始する xdmp:eval ステートメント
xdmp:expanded-tree-cache-partitions	http://marklogic.com/xdmp/privileges/ xdmp-expanded-tree-cache-partitions	admin 関数を実行する権限	admin ビルトイン
xdmp:expanded-tree-cache-size	http://marklogic.com/xdmp/privileges/ xdmp-expanded-tree-cache-size	admin 関数を実行する権限	admin ビルトイン
xdmp:external-binary	http://marklogic.com/xdmp/privileges/xdmp-external-binary	外部バイナリ関数にアクセスする権限	xdmp:external-binary
xdmp:filesystem-directory	http://marklogic.com/xdmp/privileges/ xdmp-filesystem-directory	ビルトインを実行する権限	xdmp:filesystem-directory
xdmp:filesystem-directory-create	http://marklogic.com/xdmp/privileges/ xdmp-filesystem-directory-create	admin 関数を実行する権限	admin ビルトイン

名前	アクション URI	説明	保護する関数
xdmp:filesystem-file	http://marklogic.com/xdmp/privileges/xdmp-filesystem-file	admin 関数を実行する権限	admin ビルトイン
xdmp:filesystem-file-exists	http://marklogic.com/xdmp/privileges/ xdmp-filesystem-file-exists	ビルトインを実行する権限	xdmp:filesystem-file-exists
xdmp:filesystem-file-length	http://marklogic.com/xdmp/privileges/ xdmp-filesystem-file-length	ビルトインを実行する権限	xdmp:filesystem-file-length
xdmp:forest-backup	http://marklogic.com/xdmp/privileges/xdmp-forest-backup	admin 関数を実行する権限	admin ビルトイン
xdmp:forest-clear	http://marklogic.com/xdmp/privileges/xdmp-forest-clear	admin 関数を実行する権限	admin ビルトイン
xdmp:forest-delete	http://marklogic.com/xdmp/privileges/xdmp-forest-delete	admin 関数を実行する権限	admin ビルトイン
xdmp:forest-restart	http://marklogic.com/xdmp/privileges/xdmp-forest-restart	admin 関数を実行する権限	admin ビルトイン
xdmp:forest-restore	http://marklogic.com/xdmp/privileges/xdmp-forest-restore	admin 関数を実行する権限	admin ビルトイン
xdmp:forest-rollback	http://marklogic.com/xdmp/privileges/xdmp-forest-rollback	admin 関数を実行する権限	admin ビルトイン
xdmp:get	http://marklogic.com/xdmp/privileges/xdmp-get	メモリにドキュメントを取得する権限	xdmp:get
xdmp:get-forest-keys	http://marklogic.com/xdmp/privileges/xdmp-get-forest-keys	admin 関数を実行する権限	admin ビルトイン
xdmp:get-hot-updates	http://marklogic.com/xdmp/privileges/ xdmp-get-hot-updates	admin 関数を実行する権限	admin ビルトイン
xdmp:get-orphaned-binaries	http://marklogic.com/xdmp/privileges/ xdmp-get-orphaned-binaries	ビルトインを実行する権限	xdmp:get-orphaned-binaries
xdmp:get-server-field	http://marklogic.com/xdmp/privileges/ xdmp-get-server-field	サーバーフィールドを取得する権限	xdmp:get-server-field
xdmp:get-server-field-names	http://marklogic.com/xdmp/privileges/ xdmp-get-server-field-names	サーバーフィールド名を取得する権限	xdmp:get-server-field-names
xdmp:get-session-field	http://marklogic.com/xdmp/privileges/ xdmp-get-session-field	セッションフィールドを取得する権利	xdmp:get-session-field
xdmp:get-session-field-name	http://marklogic.com/xdmp/privileges/ xdmp-get-session-field-name	セッションフィールド名を取得する権利	xdmp:get-session-field-names

名前	アクション URI	説明	保護する関数
xdmp:host-cores	http://marklogic.com/xdmp/privileges/xdmp-host-cores	admin 関数を実行する権限	admin ビルトイン
xdmp:host-cpus	http://marklogic.com/xdmp/privileges/xdmp-host-cpus	admin 関数を実行する権限	admin ビルトイン
xdmp:host-size	http://marklogic.com/xdmp/privileges/xdmp-host-size	admin 関数を実行する権限	admin ビルトイン
xdmp:hostname	http://marklogic.com/xdmp/privileges/xdmp-hostname	admin 関数を実行する権限	admin ビルトイン
xdmp:http-get	http://marklogic.com/xdmp/privileges/xdmp-http-get	http 関数を実行する権限	xdmp:http-get
xdmp:http-head	http://marklogic.com/xdmp/privileges/xdmp-http-head	http 関数を実行する権限	xdmp:http-head
xdmp:http-options	http://marklogic.com/xdmp/privileges/xdmp-http-options	http 関数を実行する権限	xdmp:http-options
xdmp:http-delete	http://marklogic.com/xdmp/privileges/xdmp-http-delete	http 関数を実行する権限	xdmp:http-delete
xdmp:http-post	http://marklogic.com/xdmp/privileges/xdmp-http-post	http 関数を実行する権限	xdmp:http-post
xdmp:http-put	http://marklogic.com/xdmp/privileges/xdmp-http-put	http 関数を実行する権限	xdmp:http-put
xdmp:install-directory	http://marklogic.com/xdmp/privileges/ xdmp-install-directory	インストールディレクトリにアクセスする権限	admin ビルトイン
xdmp:invoke	http://marklogic.com/xdmp/privileges/xdmp:invoke	invoke 関数を実行する権限	xdmp:invoke
xdmp:invoke-in	http://marklogic.com/xdmp/privileges/xdmp:invoke-in	invoke-in 関数を実行する権限	xdmp:invoke-in
xdmp:invoke-modules-change	http://marklogic.com/xdmp/privileges/ xdmp:invoke-modules-change	Modules データベースを変更する invoke ステートメントを実行する権限	Modules データベースを変更する xdmp:invoke ステートメント
xdmp:invoke-modules-change-file	http://marklogic.com/xdmp/privileges/ xdmp:invoke-modules-change-file	ファイルシステムルートを変更する invoke ステートメントを実行する権限	ファイルシステムルートを変更する xdmp:invoke ステートメント
xdmp:invoke-transaction	http://marklogic.com/xdmp/privileges/ xdmp:invoke-transaction	<transaction-id> オプションを伴う invoke ステートメントを実行する権限	xdmp:invoke
xdmp:license-accepted	http://marklogic.com/xdmp/privileges/ xdmp-license-accepted	admin 関数を実行する権限	admin ビルトイン
xdmp:license-fee	http://marklogic.com/xdmp/privileges/xdmp-license-fee	admin 関数を実行する権限	admin ビルトイン

名前	アクション URI	説明	保護する関数
xdmp:license-key	http://marklogic.com/xdmp/privileges/xdmp-license-key	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-agreement	http://marklogic.com/xdmp/privileges/xdmp-license-key-agreement	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-cores	http://marklogic.com/xdmp/privileges/xdmp-license-key-cores	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-cpus	http://marklogic.com/xdmp/privileges/xdmp-license-key-cpus	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-decode	http://marklogic.com/xdmp/privileges/xdmp-license-key-decode	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-encode	http://marklogic.com/xdmp/privileges/xdmp-license-key-encode	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-expires	http://marklogic.com/xdmp/privileges/xdmp-key-expires	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-options	http://marklogic.com/xdmp/privileges/xdmp-license-key-options	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-size	http://marklogic.com/xdmp/privileges/xdmp-license-key-size	admin 関数を実行する権限	admin ビルトイン
xdmp:license-key-valid	http://marklogic.com/xdmp/privileges/xdmp-license-key-valid	admin 関数を実行する権限	admin ビルトイン
xdmp:licensee	http://marklogic.com/xdmp/privileges/xdmp-licensee	admin 関数を実行する権限	admin ビルトイン
xdmp:list-cache-partitions	http://marklogic.com/xdmp/privileges/xdmp-list-cache-partitions	admin 関数を実行する権限	admin ビルトイン
xdmp:list-cache-size	http://marklogic.com/xdmp/privileges/xdmp-list-cache-size	admin 関数を実行する権限	admin ビルトイン
xdmp:load	http://marklogic.com/xdmp/privileges/xdmp-load	ファイルシステムからドキュメントを読み込むために必要な権限	xdmp:load
xdmp:login	http://marklogic.com/xdmp/privileges/xdmp-login	対応するパスワードなしにユーザーをログインさせる権限	xdmp-login
xdmp:merge	http://marklogic.com/xdmp/privileges/xdmp-merge	フォレストのマージを開始する権限	xdmp-merge

名前	アクション URI	説明	保護する関数
xdmp:merging	http://marklogic.com/xdmp/privileges/xdmp-merging	現在マージしているフォレストのフォレスト ID を取得する権限	xdmp:merging
xdmp:missing-directories	http://marklogic.com/xdmp/privileges/xdmp-missing-directories	admin 関数を実行する権限	admin ビルトイン
xdmp:pre-release-expires	http://marklogic.com/xdmp/privileges/xdmp-pre-release-expires	admin 関数を実行する権限	admin ビルトイン
xdmp:privilege-roles	http://marklogic.com/xdmp/privileges/xdmp-privilege-roles	ロールの権限を取得するために必要な権限	xdmp:privilege-roles
xdmp:read-cluster-config-file	http://marklogic.com/xdmp/privileges/xdmp-read-cluster-config-file	admin 関数を実行する権限	admin ビルトイン
xdmp:read-host-config-file	http://marklogic.com/xdmp/privileges/xdmp-read-host-config-file	admin 関数を実行する権限	admin ビルトイン
xdmp:remove-orphaned-binary	http://marklogic.com/xdmp/privileges/xdmp-remove-orphaned-binary	ビルトインを実行する権限	xdmp:remove-orphaned-binary
xdmp:restart	http://marklogic.com/xdmp/privileges/xdmp-restart	admin 関数を実行する権限	admin ビルトイン
xdmp:role-roles	http://marklogic.com/xdmp/privileges/xdmp-role-roles	ロールに含まれているロールを取得する権限	xdmp:role-roles
xdmp:save	http://marklogic.com/xdmp/privileges/xdmp-save	ファイルシステムにドキュメントを保存するために必要な権限	xdmp:save
xdmp:server-backup	http://marklogic.com/xdmp/privileges/xdmp-server-backup	admin 関数を実行する権限	admin ビルトイン
xdmp:server-import-qualities	http://marklogic.com/xdmp/privileges/xdmp-server-import-qualities	admin 関数を実行する権限	admin ビルトイン
xdmp:server-restore	http://marklogic.com/xdmp/privileges/xdmp-server-restore	admin 関数を実行する権限	admin ビルトイン
xdmp:set-current-transaction	http://marklogic.com/xdmp/privileges/set-current-transaction	マルチステートメントトランザクション関数を実行する権限	xdmp:set-current-transaction
xdmp:set-hot-updates	http://marklogic.com/xdmp/privileges/xdmp-set-hot-updates	admin 関数を実行する権限	admin ビルトイン
xdmp:set-request-time-limit	http://marklogic.com/xdmp/privileges/xdmp-set-request-time-limit	リクエストの時間制限を設定する権限	xdmp:set-request-time-limit

名前	アクション URI	説明	保護する関数
xdmp:set-server-field	http://marklogic.com/xdmp/privileges/xdmp-set-server-field	サーバーフィールドを設定する権限	xdmp:set-server-field
xdmp:set-server-field-privilege	http://marklogic.com/xdmp/privileges/xdmp-set-server-field-privilege	サーバーフィールドの特定の権限を設定する権限	xdmp:set-server-field-privilege
xdmp:set-session-field	http://marklogic.com/xdmp/privileges/xdmp-set-session-field	ビルトインを実行する権限	xdmp:set-session-field
xdmp:shutdown	http://marklogic.com/xdmp/privileges/xdmp-shutdown	admin 関数を実行する権限	admin ビルトイン
xdmp:sleep	http://marklogic.com/xdmp/privileges/xdmp-sleep	admin 関数を実行する権限	admin ビルトイン
xdmp:smtp-relay	http://marklogic.com/xdmp/privileges/xdmp-smtp-relay	admin 関数を実行する権限	admin ビルトイン
xdmp:spawn	http://marklogic.com/xdmp/privileges/xdmp-spawn	spawn 関数を実行する権限	xdmp:spawn
xdmp:spawn-in	http://marklogic.com/xdmp/privileges/xdmp-spawn-in	spawn-in 関数を実行する権限	xdmp:spawn-in
xdmp:spawn-modules-change	http://marklogic.com/xdmp/privileges/xdmp-spawn-modules-change	Modules データベースを変更する spawn ステートメントを実行する権限	Modules データベースを変更する xdmp:spawn ステートメント
xdmp:spawn-modules-change-file	http://marklogic.com/xdmp/privileges/xdmp-spawn-modules-change-file	ファイルシステムルートを変更する spawn ステートメントを実行する権限	ファイルシステムルートを変更する xdmp:spawn ステートメント
xdmp:spawn-transaction	http://marklogic.com/xdmp/privileges/xdmp-spawn-transaction	<transaction-id> オプションを伴う spawn ステートメントを実行する権限	xsmp:spawn
xdmp:timestamp	http://marklogic.com/xdmp/privileges/xdmp-timestamp	ポイントインタイムクエリを実行する権限	xdmp:eval, xdmp:invoke (タイムスタンプオプション)
xdmp:transaction-create	http://marklogic.com/xdmp/privileges/xdmp-transaction-create	ビルトインを実行する権限	xdmp:transaction-create
xdmp:transaction-create-xid	http://marklogic.com/xdmp/privileges/xdmp-transaction-create-xid	ビルトインを実行する権限	xdmp:transaction-create-xid
xdmp:user-last-login	http://marklogic.com/xdmp/privileges/xdmp-user-last-login	ビルトインを実行する権限	xdmp:user-last-login
xdmp:user-roles	http://marklogic.com/xdmp/privileges/xdmp-user-roles	ユーザーのロールを取得する権限	xdmp:user-roles
xdmp:username	http://marklogic.com/xdmp/privileges/xdmp-username	admin 関数を実行する権限	admin ビルトイン
xdmp:value	http://marklogic.com/xdmp/privileges/xdmp-value	「式の評価」関数を使用する権限	xdmp:value

名前	アクション URI	説明	保護する関数
xdmp:with-namespace	http://marklogic.com/xdmp/privileges/ xdmp-with-namespace	「名前空間を保持している式の評価」関数を使用する権限	xdmp:with-namespace
xdmp:write-cluster-config-file	http://marklogic.com/xdmp/privileges/ xdmp-write-cluster-config-file	admin 関数を実行する権限	admin ビルトイン
xdmp:write-host-config-file	http://marklogic.com/xdmp/privileges/ xdmp-write-host-config-file	admin 関数を実行する権限	admin ビルトイン
xdmp:xslt-eval	http://marklogic.com/xdmp/privileges/xslt-eval	xdmp:xslt-eval を使用する権限	xdmp:xslt-eval
xdmp:xslt-eval-in	http://marklogic.com/xdmp/privileges/xslt-eval-in	xdmp:xslt-eval-in を使用する権限	xdmp:xslt-eval-in
xdmp:xslt-eval-modules-change	http://marklogic.com/xdmp/privileges/ xslt-eval-modules-change	xdmp:xslt-eval の Modules データベースを変更する権限	xdmp:xslt-eval
xdmp:xslt-eval-modules-change-file	http://marklogic.com/xdmp/privileges/ xslt-eval-modules-change-file	xdmp:xslt-eval のファイルシステムルートを変更する権限	<xdmp:xslt-eval
xdmp:xslt-eval-transaction	http://marklogic.com/xdmp/privileges/xslt-eval-transaction	<transaction-id> オプションを伴う xdmp:xslt-eval ステートメントを実行する権限	xdmp:xslt-eval
xdmp:xslt-invoke	http://marklogic.com/xdmp/privileges/xslt-invoke	xdmp:xslt-invoke を使用する権限	xdmp:xslt-invoke
xdmp:xslt-invoke-in	http://marklogic.com/xdmp/privileges/xslt-invoke-in	xdmp:xslt-invoke-in を使用する権限	xdmp:xslt-invoke-in
xdmp:xslt-invoke-modules-change	http://marklogic.com/xdmp/privileges/ xslt-invoke-modules-change	xdmp:xslt-invoke を使用し、Modules データベースを変更する権限	xdmp:xslt-invoke
xdmp:xslt-invoke-modules-change-file	http://marklogic.com/xdmp/privileges/ xslt-invoke-modules-change-file	xdmp:xslt-invoke を使用し、アプリケーションサーバールートを変更する権限	xdmp:xslt-invoke
xdmp:xslt-invoke-transaction	http://marklogic.com/xdmp/privileges/xslt-invoke-transaction	<transaction-id> オプションを伴う xdmp:xslt-invoke ステートメントを実行する権限	xdmp:xslt-invoke

35.0 付録 C : 事前定義されたロール

次のロールは、MarkLogic サーバーのすべてのインストールで事前定義されています。事前定義ロールごとに示された実行権限をユーザーに与えるには、ユーザーの既存のロールに実行権限を個別に追加するか、ユーザーの一連のロールに事前定義されたロールを追加します。

MarkLogic サーバーには、以下の事前に組み込まれたロールがあります。

- [admin](#)
- [admin-builtins](#)
- [admin-module-internal](#)
- [alert-admin](#)
- [alert-execution](#)
- [alert-internal](#)
- [alert-user](#)
- [app-builder](#)
- [app-builder-internal](#)
- [app-user](#)
- [application-plugin-registrar](#)
- [appservices-internal](#)
- [cpf-restart](#)
- [custom-dictionary-admin](#)
- [custom-dictionary-user](#)
- [custom-language-admin-read](#)
- [custom-language-admin-write](#)
- [dls-admin](#)
- [dls-internal](#)
- [dls-user](#)
- [domain-management](#)
- [filesystem-access](#)
- [flexrep-admin](#)
- [flexrep-internal](#)

- [flexrep-user](#)
- [hadoop-internal](#)
- [hadoop-user-all](#)
- [hadoop-user-read](#)
- [hadoop-user-write](#)
- [infostudio-admin-internal](#)
- [infostudio-internal](#)
- [infostudio-user](#)
- [manage-admin](#)
- [manage-admin-internal](#)
- [manage-internal](#)
- [manage-user](#)
- [merge](#)
- [network-access](#)
- [pipeline-execution](#)
- [pipeline-management](#)
- [pki](#)
- [plugin-internal](#)
- [qconsole-internal](#)
- [qconsole-user](#)
- [rest-admin](#)
- [rest-admin-internal](#)
- [rest-extension-user](#)
- [rest-internal](#)
- [rest-reader](#)
- [rest-writer-internal](#)
- [rest-writer](#)
- [rest-reader-internal](#)
- [search-internal](#)

- [security](#)
- [trigger-management](#)
- [welcome-internal](#)
- [xa](#)
- [xa-admin](#)
- [xinclude](#)

35.1 admin

`admin` ロールには、システム内におけるあらゆるアクションに必要な権限とパーミッションが与えられています。`admin` ロールに関連付けられたデフォルトのパーミッションはありません。`admin` ロールを持つユーザーは、認可された管理者と見なされます。これらのユーザーは信頼できる人物であり、悪意がなく、適切なトレーニングを受けており、正しい管理手順に従うことが要求されます。

35.2 admin-builtins

`admin-builtins` ロールは、`admin` ビルトイン関数を呼び出す実行権限を持っています。`admin-builtins` ロールに与えられている実行権限は次のとおりです。

名前	アクション URI
<code>cancel-any-request</code>	<code>http://marklogic.com/xdmp/privileges/cancel-any-request</code>
<code>cancel-my-request</code>	<code>http://marklogic.com/xdmp/privileges/cancel-my-request</code>
<code>count-builtins</code>	<code>http://marklogic.com/xdmp/privileges/counts</code>
<code>xdmp:address-bindable</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-address-bindable</code>
<code>xdmp:amp-roles</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-amp-roles</code>
<code>xdmp:castable-as</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-castable-as</code>
<code>xdmp:compressed-tree-cache-size</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-compressed-tree-cache-size</code>
<code>xdmp:compressed-tree-cache-partitions</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-compressed-tree-cache-partitions</code>
<code>xdmp:default-in-memory-limit</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-limit</code>
<code>xdmp:default-in-memory-list-size</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-list-size</code>
<code>xdmp:default-in-memory-range-index-size</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-default-in-memory-range-index-size</code>
<code>xdmp:in-memory-tree-size</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-in-memory-tree-size</code>
<code>xdmp:delete-cluster-config-file</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-delete-cluster-config-file</code>
<code>xdmp:delete-host-config-file</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-delete-host-config-file</code>
<code>xdmp:directory</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-directory</code>
<code>xdmp:disable-event</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-disable-event</code>
<code>xdmp:email</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-email</code>
<code>xdmp:email-address</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-email-address</code>

名前	アクション URI
xdmp:enable-event	http://marklogic.com/xdmp/privileges/xdmp-enable-event
xdmp:expanded-tree-cache-size	http://marklogic.com/xdmp/privileges/xdmp-expanded-tree-cache-size
xdmp:expanded-tree-cache-partitions	http://marklogic.com/xdmp/privileges/xdmp-expanded-tree-cache-partitions
xdmp:forest-backup	http://marklogic.com/xdmp/privileges/xdmp-forest-backup
xdmp:forest-clear	http://marklogic.com/xdmp/privileges/xdmp-forest-clear
xdmp:forest-delete	http://marklogic.com/xdmp/privileges/xdmp-forest-delete
xdmp:forest-restore	http://marklogic.com/xdmp/privileges/xdmp-forest-restore
xdmp:forest-status	http://marklogic.com/xdmp/privileges/xdmp-forest-status
xdmp:forest-keys	http://marklogic.com/xdmp/privileges/xdmp-forest-keys
xdmp:get-hot-updates	http://marklogic.com/xdmp/privileges/xdmp-get-hot-updates
xdmp:host-name	http://marklogic.com/xdmp/privileges/xdmp-hostname
xdmp:license-accepted	http://marklogic.com/xdmp/privileges/xdmp-license-accepted
xdmp:list-cache-size	http://marklogic.com/xdmp/privileges/xdmp-list-cache-size
xdmp:list-cache-partitions	http://marklogic.com/xdmp/privileges/xdmp-list-cache-partitions
xdmp:pre-release-expires	http://marklogic.com/xdmp/privileges/xdmp-pre-release-expires
xdmp:read-cluster-config-file	http://marklogic.com/xdmp/privileges/xdmp-read-cluster-config-file
xdmp:read-host-config-file	http://marklogic.com/xdmp/privileges/xdmp-read-host-config-file
xdmp:restart	http://marklogic.com/xdmp/privileges/xdmp-restart
xdmp:server-backup	http://marklogic.com/xdmp/privileges/xdmp-server-backup
xdmp:server-import-qualities	http://marklogic.com/xdmp/privileges/xdmp-server-import-qualities
xdmp:server-restore	http://marklogic.com/xdmp/privileges/xdmp-server-restore
xdmp:set-hot-updates	http://marklogic.com/xdmp/privileges/xdmp-set-hot-updates
xdmp:shutdown	http://marklogic.com/xdmp/privileges/xdmp-shutdown
xdmp:smtp-relay	http://marklogic.com/xdmp/privileges/xdmp-smtp-relay
xdmp:user-last-login	http://marklogic.com/xdmp/privileges/xdmp-user-last-login
xdmp:username	http://marklogic.com/xdmp/privileges/xdmp-username
xdmp:write-cluster-config-file	http://marklogic.com/xdmp/privileges/xdmp-write-cluster-config-file
xdmp:write-host-config-file	http://marklogic.com/xdmp/privileges/xdmp-write-host-config-file

`admin-builtins` ロールに関連付けられたデフォルトのパーミッションはありません。

35.3 admin-module-internal

`admin-module-internal` ロールは、管理ライブラリモジュールにより内部で使用されるため、ユーザーには一切割り当てないでください。詳細については、『*Scripting Administrative Tasks Guide*』の「[Scripting Administrative Tasks in MarkLogic Server](#)」を参照してください。

35.4 alert-admin

`alert-admin` ロールは、アラートアプリケーションの管理者に使用されます。詳細については、『*Search Developer's Guide*』の「[Creating Alerting Applications](#)」を参照してください。

35.5 alert-execution

`alert-execution` ロールは、アラート API によって内部で使用され、権限を保護して強化します。個々のユーザーにはこのロールを一切与えないでください。詳細については、『*Search Developer's Guide*』の「[Creating Alerting Applications](#)」を参照してください。

35.6 alert-internal

`alert-internal` ロールは、アラート API によって内部で使用され、権限を保護して強化します。個々のユーザーにはこのロールを一切与えないでください。詳細については、『*Search Developer's Guide*』の「[Creating Alerting Applications](#)」を参照してください。

35.7 alert-user

`alert-user` ロールは、アラートアプリケーションのユーザーにより使用されます。詳細については、『*Search Developer's Guide*』の「[Creating Alerting Applications](#)」を参照してください。

35.8 app-builder

`app-builder` ロールは、Application Builder を実行するために必要な権限を与えます。現在、Application Builder は MarkLogic には含まれていません。このロールは、後方互換性のためにのみ用意されています。

35.9 app-builder-internal

現在、Application Builder は MarkLogic には含まれていません。このロールは、後方互換性のためにのみ用意されています。

35.10 app-user

`app-user` ロールは、Application Builder が生成するあらゆるアプリケーションを実行するために必要な最低限の権限を持つロールです。現在、Application Builder は MarkLogic には含まれていません。このロールは、後方互換性のためにのみ用意されています。

35.11 application-plugin-registrar

`application-plugin-registrar` ロールはプラグイン API で使用され、次の実行権限があります。

名前	アクション URI
<code>plugin-server-fields</code>	<code>http://marklogic.com/xdmp/privileges/plugin-server-fields</code>
<code>plugin-register</code>	<code>http://marklogic.com/xdmp/privileges/plugin-register</code>
<code>xdmp:filesystem-directory</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-filesystem-directory</code>
<code>xdmp:get-server-field</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-get-server-field</code>
<code>xdmp:get-server-field-names</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-get-server-field-names</code>
<code>xdmp:invoke-modules-change-file</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-invoke-modules-change-file</code>
<code>xdmp:set-server-field</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-set-server-field</code>
<code>xdmp:set-server-field-privilege</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-set-server-field-privilege</code>

35.12 appservices-internal

`appservices-internal` ロールは、アプリケーションサービスが実行する特定の関数を強化するために、アプリケーションサービスによって使用されます。`appservices-internal` ロールはユーザーには明示的に付与しないでください。アプリケーションサービス内部での使用に限られます。

35.13 cpf-restart

`cpf-restart` ロールは、CPF 再起動トリガーへのアクセスを制御するために、CPF によって使用されます。CPF 再起動ユーザーは、通常のユーザーがドキュメントに関して持っているすべてのパーミッションおよび権限に加えて、`cpf-restart` ロールが必要です。

35.14 custom-dictionary-admin

`custom-dictionary-admin` ロールは、カスタム辞書 API で管理関数（構成における辞書の書き込み用）を実行するためのものです。

35.15 custom-dictionary-user

`custom-dictionary-user` ロールは、カスタム辞書 API でユーザー関数（構成における辞書の読み取り用）を実行するためのものです。

35.16 custom-language-admin-read

`custom-language-admin-read` ロールは、ユーザーによるカスタム言語設定の読み取りを可能にします。つまり、`clang:language-config-read` などの関数を使用できるようにします。

35.17 custom-language-admin-write

`custom-language-admin-write` ロールは、ユーザーによるカスタム言語設定の修正を可能にします。つまり、`clang:language-config-write` や `clang-language-config-delete` などの関数を使用できるようにします。これらの操作によりクラスタ設定ファイルが変更され、使用時にクラスタ全体が再起動します。

35.18 dls-admin

`dls-admin` ロールは、ライブラリサービスアプリケーションの管理者に対して、ライブラリサービス API を使用するために必要なすべての権限を付与するように用意されています。このロールには、保持ポリシーの挿入やチェックアウトのブレイクなどの操作を実行するために必要な権限が含まれます。そのため、`dls-admin` ロールは、信頼できるユーザー（悪意を持っておらず、適切なトレーニングを受けており、正しい管理手続きに従うことが想定されるユーザー）だけに付与してください。ライブラリサービスアプリケーションのすべての管理者に `dls-admin` ロールを割り当ててください。

詳細については、『*Application Developer's Guide*』の「[Library Services Applications](#)」の章を参照してください。

35.19 dls-internal

`dls-internal` ロールは、ライブラリサービス API が内部で使用するロールです。このロールは、ユーザーまたはロールに明示的に付与しないでください。このロールは、ライブラリサービスの特定の関数のコンテキストにおいて特別な権限を強化するために使用されません。これをユーザーに割り当ててしまうと、通常はシステム上の望ましくない権限を与えてしまうこととなります。このロールは、ユーザーに一切割り当てないでください。

詳細については、『*Application Developer's Guide*』の「[Library Services Applications](#)」の章を参照してください。

35.20 dls-user

`dls-user` ロールは、最低限の権限を持つロールです。このロールはライブラリサービス API で使用され、ライブラリサービスアプリケーションの通常のユーザー（`dls-admin` ユーザーではなく）が、ライブラリサービス API でコードを実行できるようにします。ユーザーは、ドキュメント更新パーミッションがあれば、管理対象ドキュメントの管理、チェックアウト、およびチェックインが可能です。

`dls-user` ロールには、ライブラリサービス API を実行するために必要な権限だけが含まれます。ライブラリサービス API の対象範囲外の関数に対する実行権限はありません。ライブラリサービス API では、上位の権限が必要とされる操作の管理を強化するメカニズムとして、`alert-user` ロールを使用します。そのため、ライブラリサービスアプリケーションを使用してもかまわないと考えられるユーザーに、このロールを割り当ててもそれほど危険ではありません。ライブラリサービスアプリケーションのすべてのユーザーに `dls-user` ロールを割り当ててください。

詳細については、『*Application Developer's Guide*』の「[Library Services Applications](#)」の章を参照してください。

35.21 domain-management

`domain-management` ロールには、コンテンツ処理ドメインを作成および修正する権限が含まれます。ドメイン管理ロールには、関連付けられた実行権限がありませんが、次のデフォルトのパーミッションが含まれます。

ロール	機能
<code>domain-management</code>	読み取り
<code>domain-management</code>	更新

35.22 filesystem-access

`filesystem-access` ロールは、ファイルシステムにアクセスする権限を持ちます。

`filesystem-access` ロールに付与された実行権限は次のとおりです。

名前	アクション URI
<code>xdmp:document-get</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-document-get</code>
<code>xdmp:document-load</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-document-load</code>
<code>xdmp:get</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-get</code>
<code>xdmp:load</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-load</code>
<code>xdmp:save</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-save</code>

`filesystem-access` ロールに関連付けられたデフォルトのパーミッションはありません。

35.23 flexrep-admin

`flexrep-admin` ロールは、レプリケーションの設定に必要です。

35.24 flexrep-internal

`flexrep-internal` ロールは、フレキシブルレプリケーションで実行される特定の関数を強化するために、フレキシブルレプリケーションで使用されます。`flexrep-internal` ロールは、ユーザーには明示的に付与しないでください。フレキシブルレプリケーション内部での使用に限られます。

35.25 flexrep-user

`flexrep-user` ロールのユーザーは、プッシュレプリケーションが設定されている場合はレプリカアプリケーションサーバーに、プルレプリケーションが設定されている場合はマスターアプリケーションサーバーに、アクセスする必要があります。レプリケーションユーザーは、`flexrep-user` ロールが与えられている必要があります。ドメインコンテンツを更新するために必要な権限を持っている必要があります。

35.26 hadoop-internal

`hadoop-internal` ロールは、内部での使用に限られます。このロールはユーザーには割り当てないでください。このロールは、Hadoop MapReduce Connector の特定の関数のコンテキストにおいて特別な権限を強化するために使用されます。これをユーザーに割り当ててしまうと、通常はシステム上の望ましくない権限を与えてしまうことになります。

35.27 hadoop-user-all

`hadoop-user-all` ロールは、`hadoop-user-read` と `hadoop-user-write` の権限を組み合わせます。

35.28 hadoop-user-read

`hadoop-user-read` ロールは、MapReduce ジョブの入力ソースとしての MarkLogic サーバーの使用を許可します。このロールではその他の権限は付与されないため、`mapreduce.marklogic.input.user` は、ターゲットデータベースからコンテンツを読み取るために追加の権限が必要になることもあります。`hadoop-user-read` ロールには次の実行権限があります。

名前	アクション URI
<code>hadoop-user-read</code>	<code>http://marklogic.com/xdmp/privileges/hadoop-user-read</code>
<code>xdbc:eval</code>	<code>http://marklogic.com/xdmp/privileges/xdbc-eval</code>
<code>xdbc:eval-in</code>	<code>http://marklogic.com/xdmp/privileges/xdbc-eval-in</code>
<code>xdmp:value</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-value</code>
<code>xdmp:with-namespaces</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-with-namespace</code>

35.29 hadoop-user-write

`hadoop-user-write` ロールは、MapReduce ジョブの出力先としての MarkLogic サーバーの使用を許可します。このロールではその他の権限が付与されないため、`mapreduce.marklogic.output.user` は、ターゲットデータベースのコンテンツを挿入または更新するために追加の権限が必要になることもあります。`hadoop-user-write` ロールには次の実行権限があります。

名前	アクション URI
<code>any-uri</code>	<code>http://marklogic.com/xdmp/privileges/any-uri</code>
<code>hadoop-user-write</code>	<code>http://marklogic.com/xdmp/privileges/hadoop-user-write</code>
<code>unprotected-collections</code>	<code>http://marklogic.com/xdmp/privileges/unprotected-collections</code>
<code>xdbc:eval</code>	<code>http://marklogic.com/xdmp/privileges/xdbc-eval</code>
<code>xdbc:insert-in</code>	<code>http://marklogic.com/xdmp/privileges/xdbc-insert-in</code>
<code>xdmp:with-namespaces</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-with-namespace</code>

35.30 infostudio-admin-internal

現在、Information Studio は MarkLogic には含まれていません。このロールは、後方互換性のためにのみ用意されています。

`infostudio-admin-user` ロールは、MarkLogic サーバーの予想外のシャットダウンと再起動の場合に、CPF の再起動の処理と、未完了の Information Studio タスクの再開に必要な権限を提供します。MarkLogic サーバーが再起動すると、長時間実行されているコレクタが、データベースでのドキュメントの読み込みを再開します。この状況では、コレクタを開始した元のユーザーが不明です。そのため、`infostudio-admin user` の目的は、コレクタの制御を再開することになります。

35.31 infostudio-internal

現在、Information Studio は MarkLogic には含まれていません。このロールは、後方互換性のためにのみ用意されています。

`infostudio-user` ロールは、Information Studio が実行する特定の関数を強化するために、Information Studio により使用されます。`infostudio-internal` ロールはユーザーには明示的に付与しないでください。Information Studio 内部での使用に限られます。

35.32 infostudio-user

現在、Information Studio は MarkLogic には含まれていません。このロールは、後方互換性のためにのみ用意されています。

`infostudio-user` ロールは、Information Studio を使用するために必要な、最低限の権限を持つロールです。Information Studio へのアクセスを許可されているすべてのユーザーにこのロールを付与する必要があります。

`infostudio-user` ロールには次の実行権限があります。

- `infostudio` (<http://marklogic.com/xdmp/privileges/infostudio>)
- `unprotected-collections`

35.33 manage-admin

`manage-admin` ロールには、設定を変更する操作に対して、管理 API および階層型ストレージ API へのアクセスに関連した権限があります。`manage-admin` ロールに付与された実行権限は次のとおりです。

名前	アクション URI
管理	http://marklogic.com/xdmp/privileges/manage
<code>manage-admin</code>	http://marklogic.com/xdmp/privileges/manage-admin
<code>ts:database-create-sub-database</code>	http://marklogic.com/xdmp/privileges/database-create-sub-database
<code>ts:database-create-super-database</code>	http://marklogic.com/xdmp/privileges/database-create-super-database
<code>ts:database-delete-sub-database</code>	http://marklogic.com/xdmp/privileges/database-delete-sub-database
<code>ts:database-delete-super-database</code>	http://marklogic.com/xdmp/privileges/database-delete-super-database
<code>ts:database-partitions</code>	http://marklogic.com/xdmp/privileges/database-partitions
<code>ts:forest-combine</code>	http://marklogic.com/xdmp/privileges/forest-combine
<code>ts:forest-migrate</code>	http://marklogic.com/xdmp/privileges/forest-migrate
<code>ts:partition-create</code>	http://marklogic.com/xdmp/privileges/partition-create
<code>ts:partition-delete</code>	http://marklogic.com/xdmp/privileges/partition-delete
<code>ts:partition-forests</code>	http://marklogic.com/xdmp/privileges/partition-forests
<code>ts:partition-migrate</code>	http://marklogic.com/xdmp/privileges/partition-migrate
<code>ts:partition-resize</code>	http://marklogic.com/xdmp/privileges/partition-resize
<code>ts:partition-set-availability</code>	http://marklogic.com/xdmp/privileges/partition-set-availability
<code>ts:partition-set-updates-allowed</code>	http://marklogic.com/xdmp/privileges/partition-set-updates-allowed
<code>ts:partition-transfer</code>	http://marklogic.com/xdmp/privileges/partition-transfer

`manage-admin` ロールに関連付けられたデフォルトのパーミッションはありません。

35.34 manage-admin-internal

`manage-admin-internal` ロールは、コンフィギュレーションマネージャと管理 API で使用される特定の関数の強化に使用されます。`manage-admin-internal` ロールはユーザーには明示的に付与しないでください。内部での使用に限られます。

35.35 manage-internal

`manage-internal` ロールは、コンフィギュレーションマネージャで使用される特定の関数の強化に使用されます。`manage-internal` ロールはユーザーには明示的に付与しないでください。内部での使用に限られます。

35.36 manage-user

`manage-user` ロールには、コンフィギュレーションマネージャへのアクセスに関連した権限が含まれます。`manage-user` ロールに付与された実行権限は次のとおりです。

名前	アクション URI
管理	http://marklogic.com/xdmp/privileges/manage

`manage-user` ロールに関連付けられたデフォルトのパーミッションはありません。

35.37 merge

`merge` ロールには、フォレストのマージに関連した権限が含まれます。`merge` ロールに付与された実行権限は次のとおりです。

名前	アクション URI
<code>xdmp:merge</code>	http://marklogic.com/xdmp/privileges/xdmp-merge
<code>xdmp:merging</code>	http://marklogic.com/xdmp/privileges/xdmp-merging

`merge` ロールに関連付けられたデフォルトのパーミッションはありません。

35.38 network-access

`network-access` ロールには、`xdmp:http-*` 関数 (`xdmp:http-get`、`xdmp:http-post` など) を実行する権限が含まれます。`network-access` ロールに付与された実行権限は次のとおりです。

名前	アクション URI
<code>xdmp:http-get</code>	http://marklogic.com/xdmp/privileges/xdmp-http-get
<code>xdmp:http-head</code>	http://marklogic.com/xdmp/privileges/xdmp-http-head
<code>xdmp:http-options</code>	http://marklogic.com/xdmp/privileges/xdmp-http-options
<code>xdmp:http-delete</code>	http://marklogic.com/xdmp/privileges/xdmp-http-delete
<code>xdmp:http-post</code>	http://marklogic.com/xdmp/privileges/xdmp-http-post
<code>xdmp:http-put</code>	http://marklogic.com/xdmp/privileges/xdmp-http-put

35.39 pipeline-execution

`pipeline-execution` ロールは、ドキュメントをドメインに書き込めるすべてのユーザーがパイプラインでコードを実行できるようにするために、XQuery コードで使用されます。

詳細については、『*Content Processing Framework Guide*』を参照してください。

35.40 pipeline-management

`pipeline-management` ロールには、コンテンツ処理パイプラインを作成および修正する権限が含まれます。`pipeline-management` ロールには、関連付けられた実行権限がありませんが、次のデフォルトのパーミッションが含まれます。

ロール	機能
<code>pipeline-management</code>	読み取り
<code>pipeline-management</code>	更新

35.41 pki

`pki` ロールには、PKI ライブラリ関数を使用するための権限が含まれます。詳細については、『*Security Guide*』の「[Configuring SSL on App Servers](#)」を参照してください。

35.42 plugin-internal

`plugin-user` ロールは、プラグインに関連付けられた特定の関数を強化するために使用されます。`plugin-internal` ロールはユーザーには明示的に付与しないでください。プラグイン API 内部での使用に限られます。

35.43 qconsole-internal

`qconsole-internal` ロールは、クエリコンソールが実行する特定の関数を強化するために、クエリコンソールで使用されます。`qconsole-internal` ロールはユーザーには明示的に付与しないでください。Information Studio 内部での使用に限られます。

35.44 qconsole-user

`qconsole-user` ロールは、クエリコンソールを使用するために必要な、最低限の権限を持つロールです。クエリコンソールの使用を許可されているすべてのユーザーにこのロールを付与する必要があります。

`qconsole-user` ロールには次の実行権限があります。

- `qconsole` (<http://marklogic.com/xdmp/privileges/qconsole>)

35.45 rest-admin

`rest-admin` ロールには、`rest-writer` と `manage-user` のロールが含まれ、REST API を介して読み書きするための完全なアクセス権を、そのロールが付与されたユーザーに付与します。

35.46 rest-admin-internal

`rest-admin-internal` ロールは、REST ライブラリ内部で使用されます。ユーザーやロールには、明示的にこのロールを付与しないでください。

35.47 rest-extension-user

`rest-extension-user` ロールは、リソースサービス拡張メソッドへのアクセスを可能にします。

35.48 rest-internal

`rest-internal` ロールは、REST ライブラリ内部で使用されます。ユーザーやロールには、明示的にこのロールを付与しないでください。

35.49 rest-reader

`rest-reader` ロールは、ドキュメントやメタデータの取得など、MarkLogic の REST API を通じた読み取り操作を可能にします。

35.50 rest-writer-internal

`rest-writer-internal` ロールは、REST ライブラリ内部で使用されます。ユーザーやロールには、明示的にこのロールを付与しないでください。

35.51 rest-writer

`rest-writer` ロールは、ドキュメント、メタデータ、設定情報の作成など、MarkLogic の REST API を通じた書き込み操作を可能にします。

35.52 rest-reader-internal

`rest-reader-internal` ロールは、REST ライブラリ内部で使用されます。ユーザーやロールには、明示的にこのロールを付与しないでください。

35.53 search-internal

`search-internal` ロールは、search API 内部で使用されるロールです。ユーザーやロールには、明示的にこのロールを付与しないでください。

35.54 security

`security` ロールには、セキュリティ関数を実行するために必要な権限が含まれます。
`security` ロールに付与された実行権限は次のとおりです。

名前	アクション URI
<code>amp-add-roles</code>	<code>http://marklogic.com/xdmp/privileges/amp-add-roles</code>
<code>amp-get-roles</code>	<code>http://marklogic.com/xdmp/privileges/amp-get-roles</code>
<code>amp-remove-roles</code>	<code>http://marklogic.com/xdmp/privileges/amp-remove-roles</code>
<code>amp-set-roles</code>	<code>http://marklogic.com/xdmp/privileges/amp-set-roles</code>
<code>any-collection</code>	<code>http://marklogic.com/xdmp/privileges/any-collection</code>
<code>any-uri</code>	<code>http://marklogic.com/xdmp/privileges/any-uri</code>
<code>collection-add-permissions</code>	<code>http://marklogic.com/xdmp/privileges/collection-add-permissions</code>
<code>collection-get-permissions</code>	<code>http://marklogic.com/xdmp/privileges/collection-get-permissions</code>
<code>collection-remove-permissions</code>	<code>http://marklogic.com/xdmp/privileges/collection-remove-permissions</code>
<code>collection-set-permissions</code>	<code>http://marklogic.com/xdmp/privileges/collection-set-permissions</code>
<code>create-amp</code>	<code>http://marklogic.com/xdmp/privileges/create-amp</code>
<code>create-privilege</code>	<code>http://marklogic.com/xdmp/privileges/create-privilege</code>
<code>create-role</code>	<code>http://marklogic.com/xdmp/privileges/create-role</code>
<code>create-user</code>	<code>http://marklogic.com/xdmp/privileges/create-user</code>
<code>get-amp</code>	<code>http://marklogic.com/xdmp/privileges/get-amp</code>
<code>get-privilege</code>	<code>http://marklogic.com/xdmp/privileges/get-privilege</code>
<code>get-role-ids</code>	<code>http://marklogic.com/xdmp/privileges/get-role-ids</code>
<code>grant-all-roles</code>	<code>http://marklogic.com/xdmp/privileges/grant-all-roles</code>
<code>grant-my-roles</code>	<code>http://marklogic.com/xdmp/privileges/grant-my-roles</code>
<code>permission</code>	<code>http://marklogic.com/xdmp/privileges/permission</code>
<code>privilege-add-roles</code>	<code>http://marklogic.com/xdmp/privileges/privilege-add-roles</code>
<code>privilege-get-roles</code>	<code>http://marklogic.com/xdmp/privileges/privilege-get-roles</code>
<code>privilege-remove-roles</code>	<code>http://marklogic.com/xdmp/privileges/privilege-remove-roles</code>
<code>privilege-set-name</code>	<code>http://marklogic.com/xdmp/privileges/privilege-set-name</code>
<code>privilege-set-roles</code>	<code>http://marklogic.com/xdmp/privileges/privilege-set-roles</code>
<code>protect-collection</code>	<code>http://marklogic.com/xdmp/privileges/protect-collection</code>
<code>remove-amp</code>	<code>http://marklogic.com/xdmp/privileges/remove-amp</code>
<code>remove-privilege</code>	<code>http://marklogic.com/xdmp/privileges/remove-privilege</code>
<code>remove-role</code>	<code>http://marklogic.com/xdmp/privileges/remove-role</code>
<code>remove-role-from-amps</code>	<code>http://marklogic.com/xdmp/privileges/remove-role-from-amps</code>
<code>remove-role-from-privileges</code>	<code>http://marklogic.com/xdmp/privileges/remove-role-from-privileges</code>
<code>remove-role-from-roles</code>	<code>http://marklogic.com/xdmp/privileges/remove-role-from-roles</code>
<code>remove-role-from-users</code>	<code>http://marklogic.com/xdmp/privileges/remove-role-from-users</code>
<code>remove-user</code>	<code>http://marklogic.com/xdmp/privileges/remove-user</code>

名前	アクション URI
role-add-roles	http://marklogic.com/xdmp/privileges/role-add-roles
role-get-default-collections	http://marklogic.com/xdmp/privileges/role-get-default-collections
role-get-default-permissions	http://marklogic.com/xdmp/privileges/role-get-default-permissions
role-get-roles	http://marklogic.com/xdmp/privileges/role-get-roles
role-privileges	http://marklogic.com/xdmp/privileges/role-privileges
role-remove-roles	http://marklogic.com/xdmp/privileges/role-remove-roles
role-set-default-collections	http://marklogic.com/xdmp/privileges/role-set-default-collections
role-set-default-permissions	http://marklogic.com/xdmp/privileges/role-set-default-permissions
role-set-description	http://marklogic.com/xdmp/privileges/role-set-description
role-set-name	http://marklogic.com/xdmp/privileges/role-set-name
role-set-roles	http://marklogic.com/xdmp/privileges/role-set-roles
unprotect-collection	http://marklogic.com/xdmp/privileges/unprotect-collection
user-add-roles	http://marklogic.com/xdmp/privileges/user-add-roles
user-get-default-collections	http://marklogic.com/xdmp/privileges/user-gt-default-collections
user-get-default-permissions	http://marklogic.com/xdmp/privileges/user-get-default-permissions
user-get-description	http://marklogic.com/xdmp/privileges/user-get-description
user-get-roles	http://marklogic.com/xdmp/privileges/user-get-roles
user-privileges	http://marklogic.com/xdmp/privileges/user-privileges
user-remove-roles	http://marklogic.com/xdmp/privileges/user-remove-roles
user-set-default-collections	http://marklogic.com/xdmp/privileges/user-set-default-collections
user-set-default-permissions	http://marklogic.com/xdmp/privileges/user-set-default-permissions
user-set-description	http://marklogic.com/xdmp/privileges/user-set-description
user-set-name	http://marklogic.com/xdmp/privileges/user-set-name
user-set-password	http://marklogic.com/xdmp/privileges/user-set-password
user-set-roles	http://marklogic.com/xdmp/privileges/user-set-roles
xdmp:amp-roles	http://marklogic.com/xdmp/privileges/xdmp:amp-roles
xdmp:privilege-roles	http://marklogic.com/xdmp/privileges/xdmp:privilege-roles
xdmp:role-roles	http://marklogic.com/xdmp/privileges/xdmp:role-roles
xdmp:user-roles	http://marklogic.com/xdmp/privileges/xdmp:user-roles

security ロールのデフォルトのパーミッションは次のとおりです。

ロール	機能
security	読み取り
security	挿入
security	更新

35.55 trigger-management

`trigger-management` ロールには、トリガーを作成および修正する権限が含まれます。
`trigger-management` ロールには、関連付けられた実行権限はありません。このロールには次のデフォルトのパーミッションがあります。

ロール	機能
<code>trigger-management</code>	読み取り
<code>trigger-management</code>	更新

35.56 xa

`xa` ユーザーロールは、MarkLogic サーバーでのそのユーザーの XA トランザクションブランチの作成と管理を許可します。`xa` ロールは、XA トランザクションに参加するために必要です。詳細については、『*XCC Developer's Guide*』の「[Participating in XA Transactions](#)」を参照してください。`xa` ロールには次の実行権限があります。

名前	アクション URI
<code>complete-my-transaction</code>	<code>http://marklogic.com/xdmp/privileges/complete-my-transactions</code>
<code>forget-my-xa-transactions</code>	<code>http://marklogic.com/xdmp/privileges/forget-my-xa-transactions</code>
<code>prepare-my-xa-transactions</code>	<code>http://marklogic.com/xdmp/privileges/prepare-my-xa-transactions</code>
<code>status-builtins</code>	<code>http://marklogic.com/xdmp/privileges/status-builtins</code>
<code>xdmp:set-current-transaction</code>	<code>http://marklogic.com/xdmp/privileges/set-current-transaction</code>
<code>xdmp:transaction-create</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-transaction-create</code>
<code>xdmp:transaction-create-xid</code>	<code>http://marklogic.com/xdmp/privileges/xdmp-transaction-create-xid</code>

35.57 xa-admin

`xa-admin` ロールは、MarkLogic サーバーでの任意のユーザーの XA トランザクションブランチの作成と管理を許可します。`xa-admin` ロールは主に、XA トランザクションを完了または無視する必要のある管理者向けです。`xa-admin` ロールには次の実行権限があります。

名前	アクション URI
<code>complete-any-transactions</code>	<code>http://marklogic.com/xdmp/privileges/complete-any-transactions</code>
<code>complete-my-transaction</code>	<code>http://marklogic.com/xdmp/privileges/complete-my-transactions</code>
<code>forget-any-xa-transactions</code>	<code>http://marklogic.com/xdmp/privileges/forget-any-xa-transactions</code>
<code>forget-my-xa-transactions</code>	<code>http://marklogic.com/xdmp/privileges/forget-my-xa-transactions</code>
<code>prepare-any-xa-transactions</code>	<code>http://marklogic.com/xdmp/privileges/prepare-any-xa-transactions</code>
<code>prepare-my-xa-transactions</code>	<code>http://marklogic.com/xdmp/privileges/prepare-my-xa-transactions</code>

名前	アクション URI
status-builtins	http://marklogic.com/xdmp/privileges/status-builtins
xdmp:set-current-transaction	http://marklogic.com/xdmp/privileges/set-current-transaction
xdmp:transaction-create	http://marklogic.com/xdmp/privileges/xdmp-transaction-create
xdmp:transaction-create-xid	http://marklogic.com/xdmp/privileges/xdmp-transaction-create-xid

35.58 welcome-internal

`welcome-internal` ロールは、MarkLogic サーバー Welcome ページ（現在削除されています）内部で使用されるロールです。ユーザーやロールには、明示的にこのロールを付与しないでください。

35.59 xinclude

`xinclude` ロールは、XInclude CPF アプリケーションで使用される XInclude コードを実行する権限を提供します。詳細については、『*Application Developer's Guide*』の「[Reusing Content With Modular Document Applications](#)」を参照してください。

36.0 テクニカルサポート

MarkLogic は、ソフトウェア使用許諾書またはエンドユーザー使用許諾書に詳述されている条件に従って、テクニカルサポートを提供します。

<http://help.marklogic.com> のサポート web サイトにアクセスして、既知および修正済みの問題に関する情報、ナレッジベースの記事などを確認してください。有効な保守契約のライセンスをお持ちのお客様の場合、サポート契約の登録と、MarkLogic テクニカルサポートチームとの連携の手順について『[Support Handbook](#)』を参照してください。

すべての開発者を対象とした完全な製品ドキュメント、最新の製品リリースのダウンロード、およびその他の有用な情報は、<http://developer.marklogic.com> で入手できます。一般的な質問については、[一般的な議論に関するメーリングリスト](#)に参加して、すべての MarkLogic 開発者に公開してください。