

目次

[第 1 章] CloudFormation の基本要素と機能	8
1-1 CloudFormation を構成する要素	8
① テンプレートファイル	8
② スタック	8
③ リソース	8
1-2 CloudFormation の主な機能	9
① スタックの作成・更新・削除	9
② 変更セット	10
③ ドリフト	10
④ ネスト	11
⑤ スタックセット	11
1-3 テンプレートファイルの概要	12
1-3-1 YAML 形式と JSON 形式	12
1-3-2 テンプレートファイルのセクション	13
リソース (Resources) セクション	13
パラメータ (Parameters) セクション	13
その他セクション	14
1-3-3 リソースセクションの概要	14
論理 ID：リソースを作成する単位	15
リソースタイプ (Type) 属性	15
リソースのプロパティ (Properties) 属性	15
リソースのその他属性	16
疑似パラメータと組み込み関数	16
EC2 の AMI イメージ番号	16
○AMI ID はリージョン毎に異なる	17
○定期的にイメージは更新される	17
1-3-4 デフォルト設定に注意	20
1-3-5 おまけ 1：EC2「接続」のネットワーク構成	22
1-3-6 おまけ 2：①EC2 Instance Connect で 1) インスタンスにパブリック IP(IPv4)を利用して接続するとき	23
1-3-7 おまけ 3：EC2「接続」を利用する費用の試算	25
1-3-8 VPC エンドポイント作成のテンプレート例	26
1-3-9 予算超過時の通知設定のテンプレート例	27
[第 2 章] CloudFormation の主要な操作と Web コンソール画面	30
2-1 スタックの作成	30
2-1-1 <利用するテンプレートファイル> 2-1-s3min.yaml	30
2-1-2 <画面>スタックの作成	30
2-1-3 ステップ 1：スタックの作成	31
2-1-4 ステップ 2：スタックの詳細を指定	32
2-1-5 ステップ 3：スタックオプションの設定	32
2-1-6 ステップ 4：レビュー (スタック名)	33
2-1-7 スタック作成開始	35
エラー時の画面	35
2-1-8 スタックの詳細画面	36

2-1-9 スタックの詳細画面：スタックの情報.....	37
2-1-10 スタックの詳細画面：イベント.....	37
2-1-11 スタックの詳細画面：リソース	38
物理 ID とは.....	39
S3 バケット名を重複させない工夫.....	40
2-1-12 スタックの詳細画面：変更セット タブ.....	42
2-1-13 スタックの詳細画面：出力.....	43
2-1-14 スタックの詳細画面：パラメータ	44
2-1-15 スタックの詳細画面：テンプレート.....	44
2-1-16 CloudFormation が自動で登録するタグ.....	45
2-1-17 スタックの作成の補足.....	46
2-1-18 （補足）ステップ1：スタックの作成 その他選択肢	46
サンプルテンプレートを使用.....	46
デザイナーでテンプレートを作成.....	47
テンプレートの準備完了：テンプレートソース Amazon S3 URL.....	48
2-1-19 スタックの一覧画面と削除済みスタック	48
2-2 スタックの更新.....	49
2-2-1 <利用するテンプレートファイル> 2-2-s3notblock.yaml	49
2-2-2 <画面>スタックの更新.....	50
2-2-3 ステップ1：スタックの更新 タブ.....	50
2-2-4 ステップ2：スタックの詳細を指定 タブ.....	50
2-2-5 ステップ3：スタックオプションの設定 タブ.....	51
2-2-6 ステップ4：レビュー (スタック名) タブ	52
2-2-7 実行と結果確認	52
2-3 スタック更新の留意点.....	53
2-3-1 スタックから論理 ID がなくなると削除.....	53
2-3-2 更新はテンプレートの差分箇所のみ.....	54
2-4 ドリフト	55
2-4-1 <画面>ドリフトの検出.....	55
2-4-2 ドリフト結果を表示	55
2-4-3 ドリフトの結果を表示 その2	56
2-4-4 ドリフトの詳細を表示.....	57
2-4-5 特定のリソースのみドリフトを検出する	59
2-4-6 ドリフトの注意点	59
ドリフト検知はテンプレートに記載した内容のみ	59
ドリフト検知の差分を修正する機能はありません	59
ドリフトの結果はドリフト対応リソースのみ信用できます	60
アジアパシフィック (大阪)はドリフト未対応	62
2-5 置換(Replacement).....	63
2-5-1 置換で削除しない設定(UpdateReplacePolicy: Retain)	64
テンプレートファイル 2-5-S3updateReplacePolicy.yaml.....	64
2-5-2 置換のリソース削除タイミング.....	65
2-5-3 置換が発生する設定項目か確認する	66
2-5-4 置換が発生する時は「ロールバック無効」が利用できない	67
2-6 変更セットの作成・実行.....	69
2-6-1 <画面>変更セット	69

変更セット：変更 タブ	69
変更セット：入力 タブ	70
変更セット：テンプレート タブ	71
変更セット：JSON の変更 タブ	72
変更セット：フックの呼び出し タブ	72
変更セットを実行 ボタン	72
2-6-2 変更セットの作成方法 3 つ	73
作成方法 1. 「スタックアクション」 ボタンで作成	73
作成方法 2. スタックの詳細の「変更セット」タブ画面より作成	74
作成方法 3. 新規スタック作成、またはスタックの更新の途中で作成	74
2-6-3 <画面>スタックの詳細の「変更セット」タブ	75
2-6-4 <画面>変更セットのプレビュー	76
2-6-5 変更セットのプレビュー	76
2-6-6 変更セット補足	76
2-7 スタックの削除	77
2-7-1 <画面>スタックを削除	77
2-7-2 削除したスタックの表示	78
2-7-3 リソースを削除しない設定	79
2-7-4 テンプレートファイル 1.7-S3DeletionPolicy.yaml	79
2-7-5 スタック削除のエラー	80
2-8 ロールバックの一時停止 (正常にプロビジョニングされたリソースの保持)	81
2-8-1 <画面>スタックのロールバックが一時停止されました	81
2-8-2 <テンプレート>エラーを起こすテンプレート例	82
2-8-3 <画面>設定：ステップ 3 スタックの失敗オプション	82
2-8-4 <画面>設定：変更セットを実行	83
2-8-5 「ロールバック中に新しく作成されたリソースを削除する」オプション	83
2-8-6 「正常にプロビジョニングされたリソースの保持」の表記ゆれ	84
ロールバックの一時停止時 エラーメッセージ例 1	85
ロールバックの一時停止時 エラーメッセージ例 2	86
ロールバックの一時停止後にロールバック エラーメッセージ例	89
2-8-7 「スタックのロールバックが一時停止されました」メッセージ意識	89
2-8-8 「スタックの失敗オプション」選択時の注意点	90
ロールバックだと失敗する。ロールバック無効で一度失敗した後に再試行すると成功 する	90
ロールバック無効だと更新できない。ロールバック有効だと更新できる。	91
2-9 リソースをインポート	93
2-9-1 新規スタックにインポート (Web 管理コンソール)	93
ステップ 1：リソースを識別	94
ステップ 2 テンプレートの指定	94
ステップ 3 リソースを識別	94
ステップ 4 スタックの詳細を指定	95
ステップ 5 レビュー	95
インポートのイベント例	96
2-9-2 既存スタックにインポート (Web 管理コンソール)	96
2-9-3 コマンドでインポート(create-change-set --change-set-type IMPORT)	97
--resources-to-import オプションのフォーマット	97
--resources-to-import で指定する JSON ファイルの作成	98
--resources-to-import で指定する JSON ファイルで複数の ResourceIdentifier	100

インポートできないリソースタイプ	100
--resources-to-import で指定する JSON ファイルの例	101
create-change-set --change-set-type IMPORT で Parameters 設定	102
create-change-set --change-set-type IMPORT で --capabilities 要不要判断	102
コマンド実行：インポート用変更セットの作成	102
2-9-4 （参考）テンプレートのサマリーを作成 (get-template-summary)	106
2-9-5 リソースがインポート可能か確認する	107
2-9-6 リソースのインポートエラー	108
エラー 1：インポートするリソースに値が指定されていない	108
エラー 2：リソースに DeletionPolicy がない	108
エラー 3：インポートで指定した識別子が存在しない。	109
エラー 4：同じリソースを指定した	109
エラー 5：すでに他のスタックの管理下	109
エラー 6：インポートがサポートされていないリソースタイプ	110
エラー 7：このテンプレートにはインポートするリソースは含まれていません	110
2-9-7 インポートの注意点など	111
インポートは対象リソースを選べません	111
テンプレートファイルのリソースで DeletionPolicy を記載しておく必要があります	111
インポートと同時に他の操作はできません	111
インポートと同時に Outputs セクションへの追加変更削除は行えません	111
他のスタックのリソースはインポートできません	111
ネストのインポート制限	111
インポート時にインポート対象の設定変更は行われません	112
インポート実行後にドリフトの検出を推奨します	112
2-9-8 参考ツール：Former2	112
2-9-9 インポートの機能拡張について（2023 年 11 月）	113
2-10 スタック作成・更新のその他オプション	113
2-10-1 ステップ 3：タグ	113
2-10-2 ステップ 3：アクセス許可	114
IAM ロールの表示権限がない時のエラー	114
2-10-3 ステップ 3：詳細オプション スタックポリシー	115
2-10-4 ステップ 3：詳細オプション ロールバック設定	115
2-10-5 ステップ 3：詳細オプション 通知オプション	117
2-10-6 ステップ 3：スタックの作成オプション（タイムアウトと削除保護）	118
タイムアウト	118
削除保護	118
2-10-7 ステップ 4：クイック作成リンク	119
2-10-8 ステップ 4：変更セットの作成	120
2-10-9 AppliCation Manager で表示	121
2-10-10 テンプレートファイルの一時保存用 S3 バケット	122
2-11 スタックの作成・更新 エラーメッセージ例	123
2-11-1 ウィザード中 ステップ 1 でのエラー	123
2-11-2 ウィザード中 ステップ 3 でのエラー	124
2-11-3 ウィザード中 ステップ 4 でのエラー	124
2-12 ネスト	126
2-12-1 ネストの基本	126
2-12-2 ネストの階層	128
2-12-3 ネストされたスタックの Outputs 値を親スタックから参照する	128

Outputs 利用の注意事項	130
2-12-4 <画面> ネストされたスタックの Web コンソール表示	131
2-12-5 ネストとタグの伝播	131
2-12-6 スタックのインポート（既存スタックをネストに取り込む）	133
インポートの注意点	133
2-12-7 ネストの更新	134
2-12-8 ネストの変更セット	134
2-12-9 ネスト親だけの変更セット	135
2-12-10 ネストとドリフト検知	136
2-12-11 ネストの削除	136
2-12-12 ネストの活用例	137
複数のテンプレートの結合	137
ネストに閉じた情報共有	137
複数のテンプレートの一括実行	137
既存のスタックをインポートしてリソースを共有	137
テンプレートファイル分割	137
参考：1 ファイルあたりのテンプレートファイルの主な上限	138
2-12-13 ネストの考慮点など	138
ネストされたスタックで直接操作は非推奨	138
複雑化しやすい	138
S3 バケット上テンプレートファイルの管理	138
コマンド実行時の必要オプション	138
2-13 スタックセット(StackSets)	139
2-13-1 スタックセットのアクセス許可は 2 種類から選択	139
2-13-2 ①「セルフサービスのアクセス許可」：管理ロールと実行ロール	140
事前準備：管理ロールを作成するテンプレートの例	141
事前準備：実行ロールを作成するテンプレート例	142
2-13-3 StackSets の操作画面（①セルフサービスのアクセス許可）	145
<画面> StackSets の作成	145
ステップ 1 テンプレートの選択	146
ステップ 2 StackSet の詳細を指定	146
ステップ 3 StackSet オプションの設定	147
ステップ 4 デプロイオプションの設定	147
ステップ 5 レビュー	150
2-13-4 <画面> StackSet の詳細	151
StackSet の詳細 - スタックセットの情報 タブ	151
StackSet の詳細 - スタックインスタンス タブ	152
StackSet の詳細 - パラメータタブ	152
StackSet の詳細 - オペレーション タブ	152
StackSet の詳細 - テンプレートタブ	153
2-13-5 スタックセットの更新操作 「アクション」 ボタン	154
2-13-6 <画面> (1) StackSet にスタックを追加	155
ステップ 1 デプロイオプションの設定	155
ステップ 3 レビュー	155
2-13-7 <画面> (2) StackSet の詳細を編集	156
2-13-8 <画面> (3) StackSet のパラメータを上書き	157
ステップ 1 デプロイオプションの設定	157
ステップ 2 上書きの指定	158
ステップ 3 レビュー	159
補足：「StackSet のパラメータを上書き」の設定をコマンドで確認する	160

2-13-9 (4)StackSet からスタックを削除	162
(4)ステップ 1 デプロイオプションの設定	162
2-13-10 (5)自動デプロイを編集	163
2-13-11 (6)ドリフトの検出	163
2-13-12 (7)StackSet の削除	164
2-13-13 スタックをスタックセットにインポート	165
インポートの主な制約	165
2-13-14 ②「サービスマネージドアクセス許可」と事前準備	166
②-3 組織にメンバーアカウントを登録する	167
2-13-15 StackSet トップ画面 (②サービスマネージドアクセス許可)	167
管理者アカウント	167
メンバーアカウント・ターゲットアカウント	167
2-13-16 StackSets の操作画面 (②サービスマネージドアクセス許可)	167
2-13-17 <画面>StackSets を作成 (②サービスマネージドアクセス許可)	168
ステップ 1 テンプレートの選択	168
ステップ 4 デプロイオプションの設定 (新しいスタックのデプロイ)	168
ステップ 4 デプロイオプションの設定 (インポート)	170
2-13-18 委任された管理者	171
委任された管理者の委任範囲	171
<画面>委任された管理者アカウント トップ	171
必要な権限	172
コマンドオプション	172
対応リージョン	173
<画面>委任された管理者を登録	173
2-13-19 <画面>スタックセット作成・更新の停止 (キャンセル)	174
2-13-20 <画面>スタックセットのデプロイに失敗したとき	175
「StackSet の詳細を編集」または「StackSet のパラメータを上書き」で失敗したスタックを再実行する	176
「スタックを追加」で失敗したスタックを再実行する	177
2-14 デザイナー	177
2-15 スタックポリシー	178
2-15-1 スタックポリシーの注意点	179
スタック更新時のポリシー指定は一時的	179
変更セット	180
スタック削除時のスタックポリシー	180
2-15-2 アカウントゲート	180
2-16 出力(Outputs)セクションとエクスポート	183
2-16-1 出力とエクスポートの例 2-16-1-output-export.yaml	183
2-16-2 クロススタックの参照 (Export と Fn::ImportValue)	184
2-16-3 クロススタック利用時の注意点	185
利用中の Export は変更不可	185
Export の名前(Name)は重複できない	186
Export の名前(Name)の制限	186
2-16-4 ネストとクロススタック、SSM パラメータの比較	188
補足：SSM パラメータでのスタック間の値の授受例	189
2-17 Mappings セクション	190
2-17-1 ①Mappings セクション	190
2-17-2 ②Resources セクションで Fn::FindInMap を利用	191

2-17-3 Mapping の制限など	191
2-17-4 AWS::LanguageExtensions 拡張機能で Fn::FindInMap 対応	192
AWS::LanguageExtensions 拡張機能を利用したサンプルテンプレート	193
2-18 変換：Transform	194
変換したテンプレートを表示	194
「変換」の CAPABILITY_AUTO_EXPAND 許可	195
スタックの更新は「既存テンプレートを置き換える」が必要	195
「変換」一覧	196
2-19 循環参照（circular dependencies）問題	197
[第3章] JSON で理解する YAML フォーマット	199
3-1 JSON の概要	199
3-1-1 ペアとオブジェクト	199
3-1-2 Key と Value	199
3-1-3 インデントなど	200
3-1-4 エスケープシーケンス	200
3-1-5 JSON とシングルクォート	201
3-2 YAML：2種のスタイル：ブロックスタイルとフロースタイル	201
3-2-1 YAML ブロックスタイル 概要	201
3-2-2 YAML フロースタイル 概要	202
3-2-3 スタイルの混在	202
3-2-4 空のオブジェクト	203
3-2-5 YAML の Key と Value	203
3-2-6 ブロックスタイル詳細：インデント	203
3-2-7 配列	204
3-2-8 コメント記号	206
3-3 リテラル・折りたたみ：文字列中の改行	206
3-3-1 ブロックスタイルの値の途中の改行（プレーン）	207
3-3-2 リテラル(literal)	208
3-3-3 折りたたみ（Folded）	208
3-3-4 +と-	209
3-4 CloudFormation の YAML 短縮形	211
3-5 セパレーターなど	212
3-6 YAML でのダブルクォートとシングルクォート、クォートなしの扱い	213
3-6-1 ①シングルクォート(')で囲む場合	213
3-6-2 ②ダブルクォート(")で囲む場合：	213
3-6-3 ③クォートで囲まない場合	214
3-6-4 ④クォートで囲まず > または で次の行に記載する場合	214
[第4章] チートシート集	215
4-1 正規表現 (Regular expression ,regex pattern)	215
4-2 組み込み関数 (Intrinsic Functions)	217
4-3 テンプレート セクション一覧	221
4-3-1 セクションサンプル	221
4-4 リソースの属性	224

4-5 Rules セクション	224
4-6 ルール関数	226
4-6-1 true/false を返すルール関数	226
4-6-2 値や値の配列が利用できるルール関数	226
4-6-3 Fn::ValueOf と Fn::ValueOfAll でサポートする属性	227
4-7 条件関数 (Condition functions)	227
4-8 疑似パラメータ (Pseudo parameters)	228
4-9 パラメータ (Parameters) セクションで利用できるプロパティ	228
4-10 Parameters セクションの Type パラメータ値	229
4-11 AWS 固有のパラメータタイプ (AWS-specific parameter types)	230
4-12 SSM パラメータタイプ: Parameters セクションでサポートされているタイプ	231
4-13 SSM パブリックパラメータ 主な AMI ID	232
4-14 スタック操作コマンド一覧 (stackset 除く)	233
4-14-1 aws cloudformation コマンド	233
4-14-2 cloudformation スタック操作コマンドの共通オプション *	233
4-14-3 スタック作成 create-stack のみのオプション	234
4-14-4 変更セット create-change-set のみのオプション	234
4-14-5 wait コマンドの引数	234
4-14-6 deploy コマンドのオプション	234
4-15 スタックセット操作コマンド一覧 (stackset)	235