AWS 大規模な移行のためのプロジェクトガバナンスプレイブック

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS 大規模な移行のためのプロジェクトガバナンスプレイブック

Table of Contents

AWS 大規模な移行のためのプロジェクトガバナンスプレイブック

Amazon Web Services (寄稿者)

2022 年 2 月 (ドキュメント履歴)

> **Note**
>
> このガイドで参照されるプロジェクトチーム、ロール、ワークストリームについては、AWS 大規模な移行のための Foundation プレイブックで説明されています。このガイドのプロジェクトガバナンスタスクを開始する前に、基盤プレイブックを完了することをお勧めします。

への大規模な移行を成功させるには、効果的なプロジェクトガバナンスが不可欠です AWS クラウド。プロジェクトガバナンスは、移行を完了するためのルール、境界、計画を定義します。一般的なプロジェクトガバナンスツールには、コミュニケーション計画、利益追跡オフィス、エスカレーション計画、移行とカットオーバーの品質ゲートなどがあります。このプレイブックを完了すると、移行プロジェクトの実行方法を定義するガバナンスを作成およびカスタマイズできます。

大規模な移行、移行、モダナイズの第 3 フェーズでは、プロジェクトガバナンスモデルを改良し、移行中に使用するツールとテンプレートの多くを作成します。このプロセスを開始する前に、評価フェーズと準備フェーズを完了する必要があります。大規模な移行のフェーズの詳細については、「大規模な移行用ガイド」の「大規模な移行のフェーズ AWS 」を参照してください。

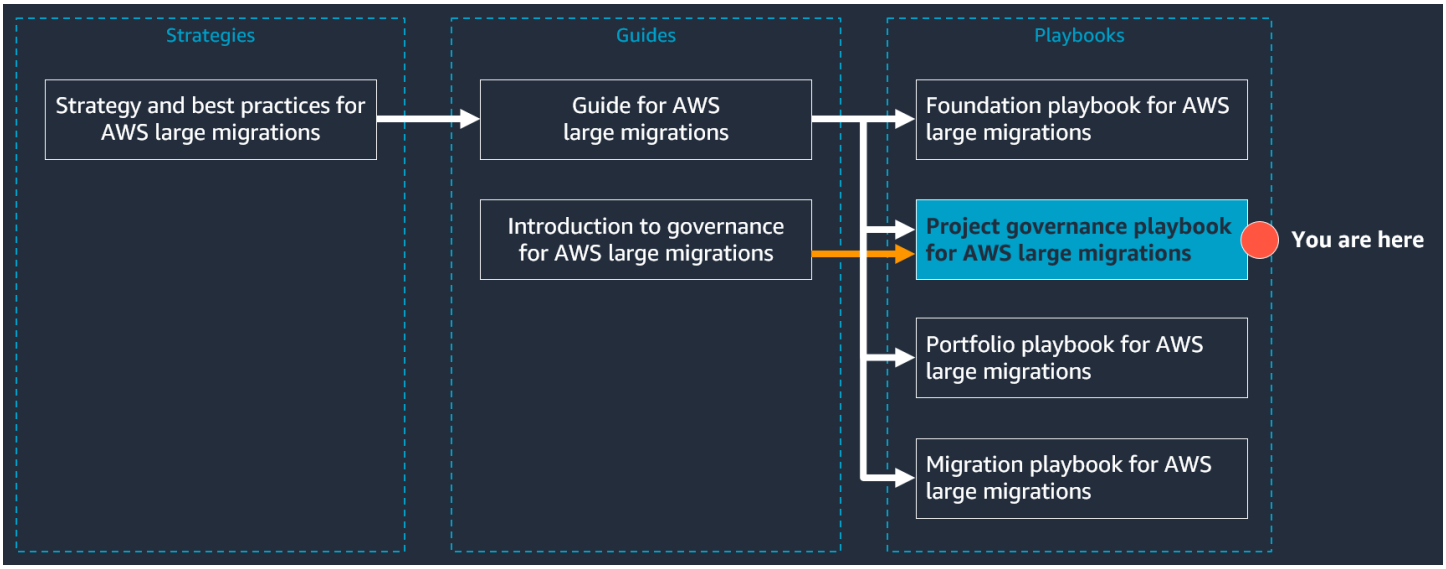
このプレイブックは、大規模な移行プロジェクトのための効果的なガバナンスモデルを迅速に開発するためのstep-by-stepアプローチを提供します。ここでは、移行フェーズ、初期化、実装の両方の段階にまたがる大規模な移行のプロジェクトガバナンスについて説明します。

- ステージ 1 では、チームの準備状況を評価し、ガバナンスモデルを立ち上げます。大規模な移行プロジェクトを管理するプロセスとツールを定義します。ステージ 1 の最後に、独自のユースケースに合わせてカスタマイズされたプロジェクトガバナンスツールがあります。
- ステージ 2 では、プロジェクトガバナンスプランに準拠するために、前のステージで作成したツールを使用します。

大規模な移行に関するガイダンス

300 台以上のサーバを移行することは「大規模な移行」と見なされます。大規模な移行プロジェクトの人材、プロセス、テクノロジーの課題は、通常、ほとんどの企業にとって新しいものです。このドキュメントは、 への大規模な移行に関する AWS 規範的ガイダンスシリーズの一部です AWS クラウド。このシリーズは、クラウドへの移行を合理化するために、最初から正しい戦略とベストプラクティスを適用するのに役立つように設計されています。

次の図は、このシリーズの他のドキュメントを示しています。最初に戦略を確認し、次にガイドを確認し、プレイブックに進みます。シリーズ全体にアクセスするには、「 への大規模な移行 AWS クラウド」を参照してください。



ツールとテンプレートについて

このプレイブックでは、以下のツールを作成します。これらのツールを使用して、移行チーム、アプリケーションオーナー、プロジェクトスポンサー、経営幹部など、プロジェクトのステークホルダーとコミュニケーションをとります。以下のツールの目的は、すべてのプロジェクトアクティビティの透明性を最大化し、大規模な移行を加速させることです。

- キックオフプレゼンテーション
- タイプと頻度を含む会議計画
- エスカレーション計画
- 週次プロジェクトステータスレポート
- ウェーブワークショップ

- カットオーバー準備状況評価プレゼンテーション
- メンバーシップステータスレポート
- 利点追跡オフィス
- プロジェクト概要ダッシュボード
- 財務レポートプロセス
- リソースプラン
- 決定ログ
- リスク、アクション、問題、依存関係 (RAID) ログ
- ゲート通信やリマインダーなどのコミュニケーションプランとテンプレート

このプレイブックに含まれているプロジェクトガバナンスプレイブックテンプレートを使用し、ポートフォリオ、プロセス、環境に合わせてカスタマイズすることをお勧めします。テンプレートは、効果的なコミュニケーションを促進し、明確な期待値を設定し、経営陣、アプリケーションオーナー、移行プロジェクトのステークホルダーを一致させるように設計されています。このプレイブックの手順では、チームがカスタマイズできる各テンプレートの目的に関するコンテキストを提供します。このプレイブックには、次のテンプレートが含まれています。

- カットオーバー準備状況評価テンプレート – このテンプレートは、品質ゲートと主要なプロジェクト管理マイルストーンを通じて各ウェーブの進行状況を追跡するのに役立ちます。
- 財務管理パステンプレート – このテンプレートは、プロジェクトスポンサーと定期的に財務状況を確認するために使用されます。
- キックオフプレゼンテーションテンプレート – このプレゼンテーションテンプレートは、ステージ 1 の早い段階でのキックオフミーティングで使用します。
- 会議計画テンプレート – このテンプレートを使用して、定期的な会議のタイプを定義し、その頻度を確立し、主要な参加者を特定します。
- ステータスレポートテンプレート – このテンプレートを使用して、プロジェクトステータスレビューミーティングの標準プレゼンテーション形式を作成します。
- ステアリング会議テンプレート – このテンプレートを使用して、ステアリングステアリング会議用の標準プレゼンテーション形式を作成します。
- ゲートコミュニケーションテンプレート – これらの E メールコミュニケーションテンプレートを使用して、ウェーブのステータスをプロジェクトのステークホルダーと共有し、最近の変更や今後のアクティビティについて知らせます。このプレイブックには、次のテンプレートが含まれています。

- カットオーバー完了のコミュニケーションテンプレート
- ハイパーケア完了のコミュニケーションテンプレート
- T-0 の通信テンプレート
- T-1 の通信テンプレート
- T-7 の通信テンプレート
- T-14 の通信テンプレート
- T-21 の通信テンプレート
- T-28 の通信テンプレート

大規模な移行の管理について

大規模な移行プロジェクトを管理および効果的に管理するには、プロジェクトマネージャーはポートフォリオ、大規模な移行のフェーズ、各ワークストリームの責任について高レベルに理解する必要があります。

このセクションは、以下のトピックで構成されます。

- 大規模な移行のワークストリーム
- 移行パイプラインへのフィード
- ハイパーケア期間
- アジャイルアプローチの確立

大規模な移行のワークストリーム

移行フェーズでは、いつでも、基盤、プロジェクトガバナンス、ポートフォリオ、移行ワークストリームの少なくとも 4 つのワークストリームが同時に運用されています。これらは大規模な移行プロジェクトの中核的なワークストリームであり、プロジェクトには追加のサポートワークストリームがある場合があります。詳細については、「大規模な移行のための Foundation プレイブック」の「大規模な移行のワークストリーム AWS 」を参照してください。

移行パイプラインへのフィード

移行ファクトリーでは、ウェーブプランニングと移行が同時に行われ、継続的に運用されます。ポートフォリオチームはウェーブを計画して移行パイプラインをフィードし、移行チームは移行とワークロードのカットオーバーを実行してパイプラインを完了します。ポートフォリオチームは初期化段階の最後に 5 つのウェーブを準備し、実装段階は移行チームが準備したウェーブの 1 つ以上を移行し始めたときに開始されます。

ウェーブごとに、ポートフォリオのワークストリームは 1～2 週間、移行ワークストリームは通常 3～4 週間実行されます。ポートフォリオワークストリームは移行ワークストリームより 5 ウェーブ先にあるため、ポートフォリオと移行ワークストリームの間には常に 5 ウェーブバッファがあります。実装段階では、ポートフォリオチームと移行チームの両方が引き続きウェーブを処理し、バッファによって移行ワークストリームのサーバーが不足して移行できなくなります。ウェーブスケジュールの例については、「大規模移行ガイド」の「ステージ 2: 大規模移行の実装 AWS 」を参照してください。

ポートフォリオチームはアプリケーションを優先し、論理移動グループのウェーブに割り当てます。ウェーブを計画するとき、ポートフォリオチームは移行の複雑さ、アプリケーションの類似点、アプリケーションとインフラストラクチャの依存関係を考慮します。これにより、アプリケーションとその依存関係全体が確実に移行されます。ウェーブプランニングの詳細については、AWS 「大規模な移行のためのポートフォリオプレイブック」を参照してください。プロジェクトガバナンスでは、アプリケーション、サーバー、アプリケーション所有者など、ウェーブとスプリントに関する情報を管理および追跡します。Confluence サイトのダッシュボード、Microsoft Excel のリスト、またはツールの組み合わせを使用できます。

ハイパーケア期間

カットオーバーが完了すると、移行されたアプリケーションとサーバーはハイパーケア期間に入ります。ハイパーケア期間中、移行チームは、問題に対処するためにクラウド内の移行されたアプリケーションを管理およびモニタリングします。通常、この期間は 1～4 日です。ハイパーケア期間の終了時に、移行チームはアプリケーションの責任をクラウド運用 (Cloud Ops) チームに移します。現時点では、ウェーブは完了したと見なされます。

アジャイルアプローチの確立

アジャイルなアプローチを確立することで、プロジェクトチームは移行中の変化に柔軟に対応し、迅速に適応できます。大規模な移行には、スクラムフレームワークを採用することをお勧めします。AWS 大規模な移行の移行プレイブックでは、スプリントにウェーブを割り当てます。スプリントは、移行チームがそのスプリント内のすべてのウェーブに作業する一定期間です。各スプリントの期間が 2 週間の場合、各ウェーブは少なくとも 2 つのスプリントにまたがります。スプリントは、スプリントの計画や毎日のスタンドアップミーティングの実施、レビュー、遡及などの標準イベントで構成されます。

スプリントの現在のタスクと保留中のタスクで構成されるスプリントバックログを使用して、アクティビティを管理します。このプレイブックでは、進行状況を追跡するためのプロジェクト管理ツールを選択します。Jira や Confluence などのプロジェクトや問題追跡アプリケーションを選択し、カンバンボードやガントチャートなどのタスクを表す視覚的なアプローチを選択することもできます。これらのツールの 1 つ以上でスプリントバックログを追跡することで、プロジェクトの透明性を提供し、各タスクに所有者を割り当て、明確な期限を設定します。

ステージ 1: 大規模な移行を初期化する

アプリケーションの移行を開始する前に、ガバナンスモデルをプロジェクトチーム全体と共有できるように、移行フェーズの早い段階でガバナンスモデルを定義し、キックオフミーティングを開催することが重要です。ガバナンスモデルが既に設定されている場合は、ステージ 2: 大規模な移行の実装「」に進んでください。ステージ 1 で確立されたプロジェクトガバナンスツールとモデルを使用します。適切な参加者、コミュニケーション形式、会議コンテンツを最初から確立することで、移行の加速に集中できます。プロジェクト会議やコミュニケーションの計画が効果的でないと、チームは移行に取り組むのではなく、会議に時間を費やしたり、ステータスの更新情報を提供したりしすぎる可能性があります。

> **Note**
>
> この章のタスクは、同時に実行することを目的としています。そのタスクの手順に記載されているように、タスクの多くは相互に依存しています。

ステージ 1 は、以下のセクション、タスク、ステップで構成されます。

- [開始する前に]
- タスク: 移行フェーズの開始
  - ステップ 1: キックオフプレゼンテーションを構築する
  - ステップ 2: キックオフミーティングを実施する
- タスク: コミュニケーションプランの作成
  - ステップ 1: コミュニケーションチームを作成する
  - ステップ 2: エスカレーション計画を立てる
  - ステップ 3: 会議とその頻度を定義する
  - ステップ 4: 会議のプレゼンテーションを準備する
  - ステップ 5: ステージ 1 の定期的な会議をスケジュールする
  - ステップ 6: 変更管理プロセスを理解する
- タスク: コミュニケーションゲートとスケジュールの定義
  - ステップ 1: 通信ゲートを定義する
  - ステップ 2: T-minus スケジュールテンプレートを作成する
  - ステップ 3: ゲートごとに標準の E メールテンプレートを作成する

[開始する前に]

次のように、大規模な移行のプロジェクトガバナンスの定義に進む準備ができていることを確認します。

- 前のフェーズの完了 – プロジェクトガバナンスの定義は、大規模な移行の第 3 フェーズと最終フェーズで行われます。まだ行っていない場合は、評価フェーズと準備フェーズを完了することをお勧めします。詳細については、AWS 「大規模な移行用ガイド」を参照してください。
- 利用可能な専門知識 – 大規模な移行プロジェクトを初めて使用する場合、利用可能なドキュメントを確認し、サポートが必要な場合は、社内または外部の対象分野のエキスパートと協力してチームの準備を検討してください。
- 移行チームの準備済み – アプリケーションのビジネスとユーザーへの影響を最小限に抑えるため、カットオーバーは通常の勤務時間後に発生する可能性があります。プロジェクトでその場合は、移行チームとアプリケーション所有者が作業スケジュールを認識し、準備していることを確認します。

タスク: 移行フェーズの開始

プロジェクトの移行フェーズを開始するには、キックオフミーティングをスケジュールします。この会議は、大規模な移行プロジェクト中に 1 回行われます。通常、ステージ 1 ではできるだけ早くこの会議を行い、大規模な移行を初期化します。プロジェクトチームメンバーを調整し、期待を早期に設定することで、ワークストリームは各自の責任を理解し、ランブックを構築できます。その目的は、プロジェクトの範囲、指針、コミュニケーション計画、チームメンバーの責任に関して、ステークホルダーとワークストリームを連携させることです。

このタスクでは、以下を実行します。

- ステップ 1: キックオフプレゼンテーションを構築する
- ステップ 2: キックオフミーティングを実施する

ステップ 1: キックオフプレゼンテーションを構築する

このステップでは、キックオフミーティングのプレゼンテーションを作成します。次のステップで説明したように、このプレゼンテーションを作成するには、このプレイブックの他のタスクで定義した計画とプロセスの一部が必要です。

すべてのプロジェクトには違いがありますが、プロジェクトガバナンスプレイブックテンプレートで使用できる Kickoff プレゼンテーションテンプレート (Microsoft PowerPoint 形式) から始めることをお勧めします。このテンプレートにはコアコンポーネントが含まれており、プロジェクトに合わせてカスタマイズできます。テンプレート全体を確認してカスタマイズする必要がありますが、少なくとも次のスライドを更新してください。

1. スライド 4 では、プロジェクトの範囲、指針、成功に不可欠な要素、成功を測定する基準を定義します。プロジェクト管理オフィス、利害関係者、移行チームと協力して、このスライドを組織に合わせてカスタマイズできます。
2. スライド 5 では、プロジェクトの大まかなスケジュールのロードマップを作成します。
3. スライド 6 では、移行に関係するチームと主要な個人を文書化します。ネットワークなど、組織内の他のチームからサポートを提供している個人を特定します。名前とロールで個人を特定し、内部リソースと外部リソースを区別します。大規模な移行プロジェクトの一般的なロールのリストについては、大規模な移行の Foundation プレイブックの「ロール」を参照してください。AWS
4. スライド 10 で、 から T-マイナススケジュールを追加しますステップ 2: T-minus スケジュールテンプレートを作成する。必要に応じて新しいスライドを追加して、リプラットフォームやリファクタリングなど、移行戦略ごとに T-マイナススケジュールを含めます。
5. スライド 13 で、 に従って会議計画を更新しますステップ 3: 会議とその頻度を定義する。
6. スライド 16 で、 に従ってエスカレーション計画を追加しますステップ 2: エスカレーション計画を立てる。
7. スライド 20 で、共有リポジトリとプロジェクト管理リソースへのリンクを追加します。

ステップ 2: キックオフミーティングを実施する

このステップでは、キックオフミーティングをスケジュールして実施します。以下の操作を実行します。

1. 移行フェーズのできるだけ早い段階でキックオフミーティングをスケジュールします。一般的な会議参加者には、プロジェクトのステークホルダー、経営幹部、ワークストリームリーダーが含まれます。
2. キックオフミーティングを実施し、前のステップで作成したプレゼンテーション を使用しますステップ 1: キックオフプレゼンテーションを構築する。
3. 会議で提示された計画とプロセスに変更がある場合は、会議後に、それに応じて計画を更新します。
4. 大規模な移行プロジェクトのすべてのメンバーが必要に応じてプレゼンテーションにアクセスできるように、キックオフプレゼンテーションを共有リポジトリに保存します。

タスク終了基準

このタスクは、以下を実行すると完了します。

- プロジェクトの Kickoff プレゼンテーションテンプレートをカスタマイズしました。
- キックオフミーティングを実施しました。
- キックオフプレゼンテーションを共有リポジトリに保存しました。

タスク: コミュニケーションプランの作成

ガバナンスモデルの重要な要素は、アプリケーション所有者との通信を担当するユーザーと、アプリケーション所有者が応答しない場合にエスカレーションする方法を特定することです。このタスクでは、コミュニケーションの責任者を定義し、定期的なコミュニケーションとミーティングの内容を決定し、標準コミュニケーションテンプレートを作成し、問題をエスカレーションする必要がある場合にどうなるかを決定します。

このタスクでは、以下を実行します。

- ステップ 1: コミュニケーションチームを作成する
- ステップ 2: エスカレーション計画を立てる

ステップ 1: コミュニケーションチームを作成する

コミュニケーションチームは、プロジェクトガバナンスワークストリームの一部です。このチームは、主要な移行マイルストーン、会議のスケジュール、フィードバックの調整、必要な会議の参加者の出席の確認において、プロジェクトのステークホルダーとコミュニケーションを取る責任があります。コミュニケーションチームのアクティビティは通常、 で定義したコミュニケーションゲートによって管理されますタスク: コミュニケーションゲートとスケジュールの定義。

以下の操作を実行します。

1. このチームの適切なメンバーを特定します。
2. コミュニケーションリードを指定します。この個人は、ゲートミーティングのスケジューリング、他のワークストリームからの質問とフィードバックの調整、必要な参加者との会議の出席の確認のために、移行全体で単一の連絡窓口として機能します。

ステップ 2: エスカレーション計画を立てる

移行で問題が発生した場合は、迅速に解決できる必要があります。移行の開始前にエスカレーション計画を定義することで、チームに明確なアクションプランを事前に提供できるため、遅延、不満、予期しない事態を防ぐことができます。ビジネスユニットごとにシングルスレッドリーダーを指定することをお勧めします。アプリケーション所有者が関与または応答していない場合は、その個人にエスカレーションできます。

このステップは通常、プロジェクトマネージャーとプロジェクトスポンサーによって完了されます。エスカレーション計画を確立するときは、問題のタイプ、問題をエスカレーションする状況 (トリガーと呼ばれる) を定義し、エスカレーションの階層を定義する必要があります。階層は 3 つ以下にすることをお勧めします。階層ごとに、対象者または応答所有者、および対象者が応答する時間を特定する必要があります。例えば、最初のエスカレーション対象者が 24 時間以内に問題を解決しない場合は、問題を別の対象者である 2 番目の階層にエスカレーションします。エスカレーションごとに、以前の階層の対象者を CC します。

以下の操作を実行します。

1. エスカレーション計画を作成します。Jira や Confluence などの専用のプロジェクト管理ツールを使用するか、Microsoft Excel でリストを作成できます。以下を文書化することをお勧めします。
   - 予想される、または経験した問題の簡単な説明
   - トリガー
   - エスカレーションと対象者の階層
   - 各階層が問題に応答する必要がある時間
2. ワークストリームリードとプロジェクトスポンサーとミーティングを行い、エスカレーション計画を確認します。
3. エスカレーション計画をプロジェクトチーム全体と共有し、すべてのメンバーがエスカレーションプロセスに精通していることを確認します。
4. エスカレーション計画を共有リポジトリに保存し、すべてのプロジェクトチームメンバーがアクセスできることを確認します。

#	問題	[Trigger] (トリガー)	階層 1		階層 2		階層 3
			対象者	の後にエスカレーションする	対象者	の後にエスカレーションする	対象者
1	ワークロードをに移行するには、ファイアウォールポートを開く必要がありますAWS	T-28 コミット会議でファイアウォールが開かれていない	ネットワークチーム、移行リーダー	24 時間	ネットワークチームマネージャー	24 時間	エグゼクティブチーム、影響を受けるビジネスユニットのリーダー

ステップ 3: 会議とその頻度を定義する

このステップでは、移行プロジェクトの定期的な会議を特定し、会議の頻度または頻度を設定します。会議とその頻度を文書化すると、プロジェクトの透明性が向上します。問題が発生した場合、チームメンバーは適切な会議をすばやく特定して対処できます。会議の名前、頻度、主要目標、所有者と参加者を特定する必要があります。移行が進むにつれてこのドキュメントを更新し、新しい会議参加者を特定する必要がある場合があります。

大規模な移行プロジェクトでは、次の定期的な会議が一般的です。

1. 会議の運営 – これらの会議は通常、月に 2 回開催され、プロジェクトのステータスを共有し、経営幹部の関与を必要とする問題を解決することが目的です。この会議の参加者には、通常、プロジェクトスポンサー、経営幹部、プロジェクト管理オフィスの担当者が含まれます。
2. プロジェクトステータスレビュー会議 – これらの会議は通常、週に 1 回開催されます。目的は、ワークストリームレベルでプロジェクトのステータスを確認し、リソースまたは対象分野の工キスパートの必要性を評価することです。この会議の参加者には、プロジェクトマネージャー、プロジェクトステークホルダー、ワークストリーム所有者、移行リーダーが含まれます。
3. 毎日のスタンドアップ – 1 日に 1 回開催される非常に短い会議です。会議は参加者が椅子を必要としないほど短くする必要があるため、スタンドアップと呼ばれます。目的は、計画されたタスクと最近完了したタスクを確認し、問題を明らかにすることです。毎日のスタンドアップでは、通常、「」で決定したカンバンボードやガントチャートなどの視覚的なタスク管理ツールを使用しますステップ 1: プロジェクト管理ツールを選択する。
4. インフラストラクチャと運用のチェックポイントミーティング – これらのミーティングは通常、週に 2 回開催されます。目的は、移行の進行状況の確認、アクティブな問題の確認、エスカレーションが必要かどうかの判断、ワークストリーム間のコラボレーション、次のスプリントのためのリソースの計画です。この会議の参加者には、RACI が定義した移行アクティビティを所有する技術チームのメンバーが含まれます。
5. 移行営業時間 – この時間は、アプリケーション所有者がサポートやガイダンスを求めるためのオープンミーティングとして予約されています。週 3 回営業時間を設定することをお勧めします。

プロジェクトガバナンスプレイブックテンプレートで利用可能な会議計画テンプレート (Microsoft Excel 形式) から始めることをお勧めします。このテンプレートにはデフォルトの例が含まれており、プロジェクトに合わせてカスタマイズできます。

ステップ 4: 会議のプレゼンテーションを準備する

「」で定義されているようにステップ 3: 会議とその頻度を定義する、大規模な移行では、ワークストリームを調整し、問題に対処し、移行がスケジュールどおりであることを確認するために、頻繁に会議を行う必要があります。これらの会議の標準形式とプレゼンテーションを定義すると、参加者は会議に対する一貫した期待値を確立できます。また、各会議の準備に必要な時間を短縮するのに役立ちます。このステップでは、定期的に予定されている会議用のプレゼンテーションテンプレートを作成します。

プロジェクトガバナンスプレイブックテンプレートに含まれている次のテンプレートから始めることをお勧めします。

- ステータスレポートテンプレート (Microsoft PowerPoint 形式)
- 会議用会議テンプレート (Microsoft PowerPoint 形式)
- ウェーブワークショップテンプレート (Microsoft PowerPoint 形式)
- カットオーバー準備状況評価テンプレート (Microsoft Excel 形式)

以下の操作を実行します。

1. プロジェクト用の会議テンプレートをカスタマイズします。
2. プロジェクトのステータスレポートテンプレートをカスタマイズします。このプレゼンテーションはプロジェクトステータスレビュー会議で使用され、通常は毎週行われます。このテンプレートは、前のステップで作成したエグゼクティブレベルの概要のより堅牢なバージョンです。
3. プロジェクトの Wave ワークショップテンプレートをカスタマイズします。このプレゼンテーションは、T-28 および T-14 コミット会議で使用されます。T-28 コミット会議では、アプリケーション所有者がウェーブにコミットし、T-14 コミット会議ではカットオーバー日に再コミットします。
4. プロジェクトのカットオーバー準備状況評価テンプレートをカスタマイズします。このプレゼンテーションは、インフラストラクチャと運用のチェックポイントミーティングで、移行アクティビティの現在の進行状況を確認するために使用されます。プレゼンテーションの目的は、進行状況ゲートが満たされ、アプリケーションがカットオーバーの準備が整っていることをチームが確認できるようにすることです。
5. これらのプレゼンテーションテンプレートは、会議の所有者がアクセスできる共有リポジトリに保存します。
6. 会議の種類ごとに、会議の所有者がプレゼンテーションを保存できる共有リポジトリを定義します。各会議の後、会議の所有者は、会議の参加者とプロジェクトチームがこの情報を参照できる

ように、プレゼンテーションのバージョンとその他の会議アーティファクトをこのリポジトリに保存する必要があります。例えば、プロジェクトステータスレビュー会議のリポジトリには、各会議で提示されたステータスレポートのコピーが含まれます。

ステップ 5: ステージ 1 の定期的な会議をスケジュールする

準備フェーズを完了した場合は、このステップでいくつかの会議を既に確立している可能性があります。まだスケジュールしていない会議については、このステップを完了します。で作成した会議計画に従ってステップ 3: 会議とその頻度を定義する、会議の所有者は、次の定期的な会議をスケジュールする必要があります。

- 各ワークストリームの日次スタンドアップ
- 財務レポート会議
- 会議を主催する
- プロジェクトのステータスレビュー
- インフラストラクチャと運用のチェックポイントミーティング

これらの会議は、移行が完了するまで続行されます。

ステップ 6: 変更管理プロセスを理解する

大規模な移行プロジェクトを成功させるには、組織の変更管理プロセスを理解することが不可欠です。変更管理プロセスは、移行のスケジュールと期限に影響します。各ワークロードに必要な情報と承認を理解する必要があります。以下を理解していることを確認してください。

- ウェーブプラン内のアプリケーションとサーバーのリストを送信するための期限
- 計画された日付にワークロードを移動するための承認を取得するために必要な基準と情報
- 完了する必要がある正式なプロセスドキュメント
- ファイアウォールまたはドメインの変更を送信するプロセス

すべての移行リードは、検出アクティビティの前に変更管理プロセスを理解する必要があります。一部の移行関連のタスクでは承認が必要であり、チームメンバーは変更管理プロセスにおける各自の責任を理解する必要があります。トレーニングの詳細については、「大規模な移行のための Foundation プレイブック」の「大規模な移行に必要なトレーニングとスキル」を参照してください。 AWS

タスク終了条件

このタスクは、以下を実行すると完了です。

- コミュニケーションチームを作成しました。
- すべての会議に参加者を定義しました。
- エスカレーション計画を確立し、承認した。
- 会議計画で定義されているように、ステージ 1 で始まる定期的な会議をスケジュールしている。
- 各会議で使用する標準的なプレゼンテーションを定義しました。
- 会議ごとに、すべてのプレゼンテーション、アクティビティ、アーティファクトをキャプチャするための共有リポジトリを定義しました。
- すべての変更管理プロセスを理解し、文書化します。

タスク: コミュニケーションゲートとスケジュールの定義

大規模な移行プロジェクトのステージ 2 では、ポートフォリオワークストリームがウェーブを積極的に計画し、移行ワークストリームがウェーブを移行しています。プロジェクトガバナンスのワークストリームは、これらのアクティビティを監督し、コミュニケーションゲートを通じて波をガイドするのに役立ちます。コミュニケーションゲートは、進行中のウェーブアクティビティとステータスをステークホルダーに正式に伝えるときのタッチポイントです。各ゲートで、指定されたゲート所有者が指定された対象者にウェーブステータスについて通知し、今後のアクティビティや会議についてアプリケーション所有者にリマインドします。ゲートは通常、移行のマイルストーンに対応し、コミュニケーションゲートを定義すると、すべてのプロジェクトの利害関係者の透明性が最大化されます。波はゲートを個別に移動するか、波をグループ化できます。

このタスクでは、以下を実行します。

- ステップ 1: 通信ゲートを定義する
- ステップ 2: T-minus スケジュールテンプレートを作成する
- ステップ 3: ゲートごとに標準の E メールテンプレートを作成する

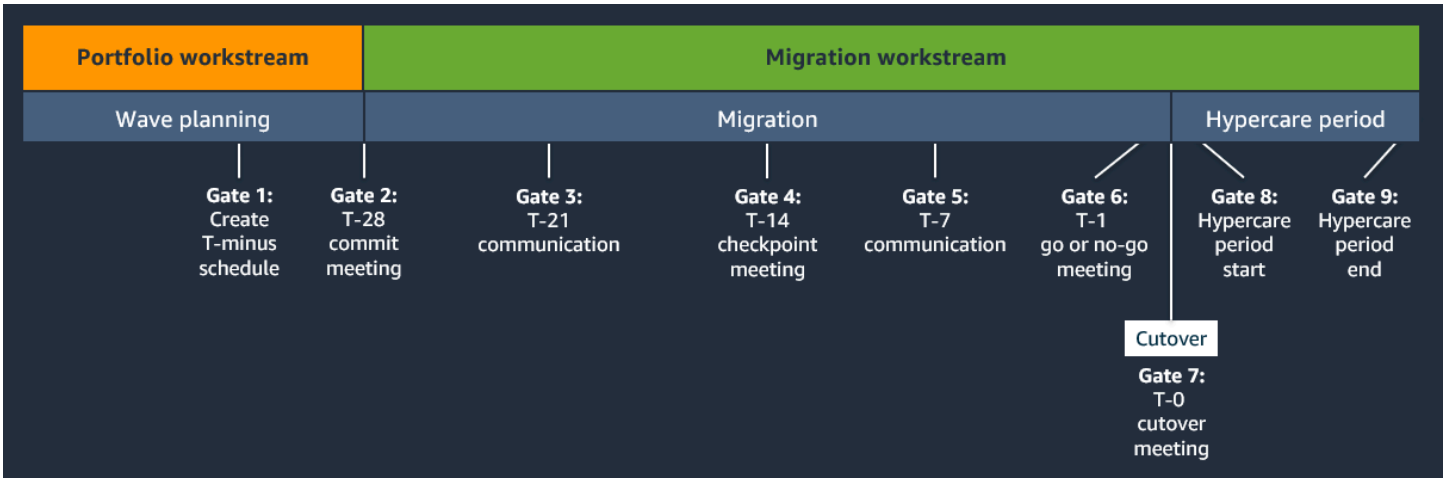
ステップ 1: 通信ゲートを定義する

移行中、すべてのワークロードを移行し、プロジェクトが完了するまで、各ウェーブまたはウェーブのグループの通信ゲートを繰り返します。少なくとも、次の通信ゲートをお勧めします。プロジェクトに応じて、プロジェクトにゲートを追加することもできます。

ゲート	おおよそのタイムライン	目的	ゲート所有者	対象者
ゲート 1: T マイナススケジュールを作成する	ウェーブプランが完了する前に	各ゲートのスケジュール日	プロジェクトマネージャーまたはコミュニケーションチーム	アプリケーションオーナー、コミュニケーションリーダー、移行リーダー
ゲート 2: T-28 コミットミーティング	カットオーバーの 4 週間前	アプリケーション所有者とのウェーブの開始	プロジェクトマネージャーまたはコミュニケーションチーム	アプリケーションオーナー、コミュニケーションリーダー、移行リーダー
ゲート 3: T-21 通信	カットオーバーの 3 週間前	カットオーバーは 21 日後に行われる予定であることに注意	プロジェクトマネージャーまたはコミュニケーションチーム	アプリケーション所有者、コミュニケーションリーダー
ゲート 4: T-14 チェックポイントミーティング	カットオーバーの 2 週間前	スケジュールを確認し、準備状況タスクの進捗状況を評価する	プロジェクトマネージャーと移行リーダー	アプリケーションオーナー、コミュニケーションリーダー、移行リーダー
ゲート 5: T-7 通信	カットオーバーの 1 週間前	カットオーバーは 7 日後に行われる予定であることにご注意ください	コミュニケーションチーム	アプリケーション所有者、運用チーム
ゲート 6: T-1 go または no-go ミーティング	カットオーバーの 24 ~ 48 時間前	移行カットオーバーの準備状況を確認する	プロジェクトマネージャーまたはコミュニケーションチーム	クラウド運用チーム、アプリケーションオーナー、インフラ

ゲート	おおよそのタイムライン	目的	ゲート所有者	対象者
				ストラクチャチーム
ゲート 7: T-0 カットオーバーミーティング	カットオーバー日	アプリケーションのカットオーバーとテスト	プロジェクトマネージャーと移行リーダー	クラウド運用チーム
ゲート 8: ハイパーケア期間の開始	カットオーバーから 1 営業日後	カットオーバーが完了し、ハイパーケア期間が開始したことの通知	プロジェクトマネージャーまたはコミュニケーションチーム	アプリケーション所有者
ゲート 9: ハイパーケア期間の終了	カットオーバーから 4 営業日後	ハイパーケア期間が完了したことの通知	プロジェクトマネージャー、コミュニケーションチーム、またはクラウド運用チーム	ウェーブのアプリケーションオーナー、コミュニケーションリーダー、クラウド運用チーム

次の図は、ポートフォリオと移行ワークストリームにおけるこれらの通信ゲートのシーケンスを示しています。ゲート 1 はウェーブプランニング中に、ゲート 2～6 は移行中に、ゲート 7 はカットオーバーミーティング、ゲート 8～9 はハイパーケア期間中に発生します。ゲート 2 ～ 6 には、 という形式で名前が付けられますT-#。は残り時間Tを参照し、 #は予定されたカットオーバー日までの残り日数です。



大規模な移行プロジェクトの通信ゲートを次のように定義します。

1. プロジェクトに追加の通信ゲートが必要かどうかを判断します。例えば、プロジェクトに、アプリケーション所有者との移行準備の円滑化を担当するシングルスレッドリーダーがいない場合は、今後のアクティビティと期日をアプリケーション所有者に知らせるための追加のコミュニケーションゲートを含めることができます。
2. Jira や Confluence などの共有リポジトリまたはプロジェクト追跡アプリケーションに、大規模な移行プロジェクトの通信ゲートを記録します。各ゲートに次の属性を必ず記録してください (例えば、通信ゲートの表を参照してください)。
   - ゲート番号と名前
   - ワークストリームのマイルストーンまたはカットオーバーに関連してゲートが発生する場合の概算タイムライン
   - ゲートの目的
   - ゲートの所有者と呼ばれる、ゲートを担当する個人またはチーム
   - 対象者と呼ばれる、コミュニケーションを受け取ったりゲート会議に参加したりする個人またはチーム
   - (オプション) ゲート所有者が使用する通信テンプレートまたはプレゼンテーションテンプレート

ステップ 2: T-minus スケジュールテンプレートを作成する

T マイナススケジュールは、ウェーブごとに完了する必要があるすべての高レベルの移行アクティビティを表す視覚的な方法です。ウェーブプランニングの終了からハイパーケア期間の終了までの時間をカバーします。高レベルの移行アクティビティは移行戦略によって異なるため、移行戦略ごと

に T-マイナススケジュールテンプレートが必要です。T-minus スケジュールは、キックオフ会議と T-28 および T-14 コミット会議で共有します。

通常、カットオーバー日からさかのぼって T-マイナススケジュールを作成します。アクティビティを移行マイルストーンに整理し、プロジェクト管理ツール内で詳細なタスクを個別に追跡します。T-minus スケジュールでは、 で定義した通信ゲートも強調表示されますステップ 1: 通信ゲートを定義する。

プロジェクトガバナンスプレイブックテンプレートで利用可能な T-minus スケジュールテンプレート (Microsoft PowerPoint 形式) から始めることをお勧めします。以下の操作を実行します。

1. T-minus スケジュールテンプレートを開きます。このテンプレートには、リホスト移行戦略のデフォルトの T-マイナススケジュールが含まれています。
2. ユースケースに基づいてデフォルトのリホスト移行アクティビティを変更します。各移行戦略のアクティビティのリストについては、AWS 「大規模な移行のための Foundation プレイブック」で作成した責任、説明責任、相談、情報 (RACI) マトリックスを参照してください。
3. で行った決定に基づいて、デフォルトの通信ゲートを変更しますステップ 1: 通信ゲートを定義する。
4. リホスト T マイナススケジュールを開始点として使用して、リプラットフォームやリファクタリングなどの移行戦略ごとに T マイナススケジュールを作成します。
5. T-minus スケジュールをコミュニケーションチーム、移行チーム、クラウド運用チームと共有します。すべてのチームが連携していて、調整の必要がないことを確認します。
6. 完成した T-minus スケジュールテンプレートをキックオフプレゼンテーションとウェーブワークショッププレゼンテーションに追加します。

ステップ 3: ゲートごとに標準の E メールテンプレートを作成する

各通信ゲートでアプリケーション所有者に送信する E メール通信のテンプレートを作成します。これらの E メールには、ウェーブ内のアプリケーションに関する基本情報が含まれ、ウェーブステータスをアプリケーションの所有者に通知し、今後の期日や会議について利害関係者に知らせます。

プロジェクトガバナンスプレイブックテンプレートに含まれている次のテンプレートから始めることをお勧めします。

- T-28 の通信テンプレート (Microsoft Word 形式)
- T-21 の通信テンプレート (Microsoft Word 形式)
- T-14 の通信テンプレート (Microsoft Word 形式)

- T-7 の通信テンプレート (Microsoft Word 形式)
- T-1 の通信テンプレート (Microsoft Word 形式)
- T-0 の通信テンプレート (Microsoft Word 形式)
- カットオーバー完了のコミュニケーションテンプレート (Microsoft Word 形式)
- ハイパーケア完了のコミュニケーションテンプレート (Microsoft Word 形式)

タスク終了基準

このタスクは、以下を実行すると完了します。

- 大規模な移行プロジェクトのコミュニケーションゲートを定義しました。
- T-minus スケジュールテンプレートを作成しました。
- T-minus スケジュールテンプレートをプロジェクトのステークホルダーと共有しました。
- T-minus スケジュールテンプレートをキックオフプレゼンテーションとウェーブワークショッププレゼンテーションに統合しました。
- ゲート E メール通信用の標準テンプレートを作成しました。

タスク: プロジェクト管理プロセスとツールの定義

大規模な移行プロジェクトでは、十分に確立された管理プロセスとツールが必要です。大規模な移行では、情報の共有、パフォーマンスメトリクスの追跡、正しい会議参加者の特定、所有者へのタスクの割り当てに違いがあります。このタスクでは、主要な移行タスクと所有者を文書化し、移行の主要な業績評価指標 (KPIs) を決定し、それらを測定する方法、予算を追跡する方法、リスクを管理し、決定を追跡するためのツールを開発する方法を決定します。

特に明記されていない限り、このタスクのステップの多くは同時に実行されます。通常、キックオフミーティングの前または直後にこれらのステップを完了します。

このタスクでは、以下を実行します。

- ステップ 1: プロジェクト管理ツールを選択する
- ステップ 2: すべての移行アクティビティの役割と責任を検証する
- ステップ 3: 利点追跡オフィスを設立する
- ステップ 4: プロジェクト概要ダッシュボードを作成する

ステップ 1: プロジェクト管理ツールを選択する

このステップでは、進行状況の追跡に使用するツールを確立します。Jira や Confluence などのソフトウェアソリューションを使用するか、Microsoft Excel で独自のダッシュボードを構築するか、これらのツールの組み合わせを使用するかを選択できます。プロジェクト管理ツールを選択または構築するときは、次のベストプラクティスを考慮してください。

- タスクの追跡と進行状況の追跡には、プロジェクト管理アプリケーションで一般的に利用できる、カンバンボードやガントチャートなどのビジュアル管理ツールをお勧めします。ビジュアル管理ツールは、現在のタスクとウェーブの進行状況を確認するための毎日のスタンドアップミーティングで特に効果的です。
- プロジェクト管理アプリケーションを選択する場合は、プロジェクト管理ツールに計画とプロセス (エスカレーション計画、決定ログ、RAID ログなど) を入力するかどうかを検討し、必要な機能があることを確認してください。
- プロジェクトスポンサー、エグゼクティブリーダー、プロジェクトマネージャー、および外部の利害関係者 (存在する場合) が、選択したツールに沿っていることが重要です。

これらのツールの使用方法の詳細については、「」を参照してくださいアジャイルアプローチの確立。

ステップ 2: すべての移行アクティビティの役割と責任を検証する

AWS 大規模な移行のための Foundation プレイブックでは、大規模な移行プロジェクトの移行戦略と高レベルのタスクごとに詳細な RACI マトリックスを作成しました。RACI マトリックスは責任割り当てツールであり、名前はマトリックスで定義されている 4 つの責任タイプ、責任 (R)、説明責任 (A)、相談先 (C)、情報 (I) から算出されます。このマトリックス形式は、すべての移行アクティビティで役割と責任を調整するために推奨されます。このマトリックスは、オンサイトのチームをリモートチームまたは外部パートナーと連携させることができます。このステップでは、マトリックスが正しいことを確認し、プロジェクトチームで確認します。

組織の RACI タスクを調整するには、次の点を考慮することをお勧めします。

- 変更管理プロセス、それらのプロセスに必要なリードタイム、変更の承認に関連するロールを理解します。詳細については、「ステップ 6: 変更管理プロセスを理解する」を参照してください。
- 移行を開始する前に、バックアップとディザスタリカバリ戦略を検証し、この戦略を移行チームと共有してください。戦略のギャップを特定する場合は、 や CloudEndure Disaster Recovery などの AWS Backup 統合クラウドサービスを使用することをお勧めします。

以下の操作を実行します。

1. まだ行っていない場合は、AWS 「大規模な移行のための Foundation プレイブック」の指示に従って、高レベルタスクごとに RACI マトリックスを作成します。
2. 各マトリックスの各チームとマトリックスを確認します。すべての詳細なタスクが示され、チームが各自の責任に精通していることを確認します。
3. 新しい移行戦略やサポートタスクを特定する際、移行全体で新しいマトリックスを更新して作成します。

ステップ 3: 利点追跡オフィスを設立する

このチームは、主要業績評価指標 (KPIs。このチームは、移行がスケジュールに従って進行しているかどうかを評価し、進行を妨げる遅延や問題に対応できます。このチームは、毎週または隔週のプロジェクトステータスミーティングの外で会議を行います。

通常、このチームは各会議で以下の質問を確認して回答します。

- 移行の現在のステータスは何ですか？
- 目標成果を達成するための軌道をたどっていますか？
- パフォーマンスを正確に測定していますか？
- 移行を高速化するために調整する必要がありますか？

利点追跡オフィスが移行が望ましい速度に達していないと判断した場合、このチームはプロセス、リソース、またはコミュニケーション計画の調整を推奨する必要があります。

大規模な移行のための利点追跡オフィスを設立するには、以下を実行します。

1. 適切な参加者を特定します。このチームの一般的なメンバーには、プロジェクトスポンサー、プロジェクトマネージャー、移行リーダー、およびワークロードが対象範囲内にある各ビジネスユニットの権限のある担当者が含まれます。

2. 利点追跡オフィスの定期的な会議の頻度を設定します。このチームは 2 週間に 1 回開催することをお勧めします。
3. プロジェクトスポンサーとの大規模な移行のための定性的および量的 KPIs を定義し、経営幹部から情報を収集します。メリット追跡オフィスは、KPI に照らして移行の進行状況を評価します KPIs 。KPIs の例は次のとおりです。
   - (量的) 計画と比較した実際の移行サーバー数
   - (量的) 計画と比較して廃止されたサーバーの数
   - (定性) アンケートフィードバックとアクションプランのレビュー
   - (定性) アンケートのフィードバックに応じて行われる是正措置

ステップ 4: プロジェクト概要ダッシュボードを作成する

プロジェクトチームは、主要なプロジェクトの利害関係者と共同で作業し、移行の進行状況を明確に伝えるダッシュボードを作成する必要があります。プロジェクト概要ダッシュボードは、1 ページで次のことを行う必要があります。

- プロジェクト全体の完了済みおよび残りのワークロードを定量化します。
- 最後に完了したウェーブ (計画と実績) のパフォーマンスを反映します。
- 今後のウェーブで予想されるワークロードを表示する (計画的)

プロジェクトガバナンスプレイブックテンプレートで利用可能なプロジェクト概要ダッシュボードテンプレート (Microsoft PowerPoint 形式) から始めることをお勧めします。以下の操作を実行します。

1. プロジェクトに必要なテンプレートを変更します。各移行戦略へのサーバーの割り当てを表すことをお勧めします。提供されているテンプレートには、リホストとリプラットフォームの移行戦略が含まれています。
2. 経営幹部を含むプロジェクトステークホルダーとプロジェクト概要ダッシュボードを確認し、すべてのステークホルダーが連携し、ダッシュボードの使用方法とアクセス方法を理解していることを確認します。
3. ダッシュボードを共有リポジトリに保存します。すべての利害関係者は、必要に応じてこの情報に自身でアクセスできる必要があります。

ステップ 5: 財務レポートプロセスを作成する

通常、より限られた対象者に提供する必要があるため、プロジェクトステータスレポートとは別に財務レポートを追跡します。財務レポートには、現在までに発生したコストである実際のコストと、プロジェクトの残りの期間に予想されるコストである予測コストを含める必要があります。内部リソースコストと外部リソースコストを個別に追跡します。実際の内部リソースコストと予測された内部リソースコストを評価するには、社内時間レポートとリソースプランを使用できます。外部リソースの場合は、パートナーまたはコンサルタントに実際のコストと予測コストを提供するように依頼する必要があります。

プロジェクトガバナンスプレイブックテンプレートで利用可能な Financial glide path テンプレート (Microsoft PowerPoint 形式) から始めることをお勧めします。以下の操作を実行します。

1. この財務レポートを受け取るステークホルダーを決定します。
2. この財務レポートを会議で共有するか、E メールで共有するかを決定します。
3. プロジェクトに必要なテンプレートを変更します。
4. エグゼクティブリーダーシップチームまたはプロジェクトスポンサーと財務レポートを確認し、形式と内容の整合性を確認します。
5. ステークホルダーとともに、このレポートを更新してレビューする頻度を決定します。
6. この財務レポートを保存する場所を決定します。機密性の高い財務情報が含まれているため、このテンプレートを共有リポジトリにプロジェクトドキュメントの残りの部分と一緒に保存することはお勧めしません。

ステップ 6: リソースを管理およびスケーリングする方法を決定する

プロジェクトの進行に合わせてリソースを効果的に管理することは、大規模な移行作業に不可欠です。プロジェクトが初期化段階から実装段階に移行するにつれて、移行チームは移行ウェーブをサポートするためにスケールアップする必要があります。同時に、残りの検出アクティビティによっては、検出チームがスケールダウンを開始できる場合があります。このステップでは、リソース管理とスケーリング計画を効率化のためにマッピングします。このステップは通常、プロジェクトマネージャーとワークストリームリードによって実行されます。計画が定義されたら、プロジェクト全体で継続的に監査し、計画内のすべてのリソースが必要かどうかを判断します。例えば、移行パイプラインの構築の遅延やlarger-than-anticipatedウェーブは、リソースプランに影響する可能性があります。

リソースプランは大規模な移行ごとに異なり、通常はプロジェクト固有の要因によって決まります。一般的な要因には、プロジェクト予算、プロジェクトチームの編成方法、検出アクティビティをどれ

だけ早く完了できるか、ポートフォリオを各移行戦略に分散させる方法 (リファクタリング、リホスト、リプラットフォームなど) 、組織内の変更管理プロセスに必要な時間などがあります。

リソースを計画するときは、ポートフォリオの移行戦略と、これらが移行チームとポートフォリオチームにどのように影響するかを検討してください。例えば、リホストは複雑さが低いため、大規模な移行の一般的な戦略です。ほとんどの大規模な移行プロジェクトには、4～5 人のリホスト移行ポッドが少なくとも 1 つあります。リプラットフォームやリファクタリングなど、複雑な移行戦略を含める場合は、これらの戦略用の移行チームポッドを作成し、リソースプランに追加の移行チームとポートフォリオチームリソースを含める必要があります。ワークストリーム、チーム構造、各ポッドに必要な人数の詳細については、大規模な移行のための Foundation プレイブックの「チームの編成と構成」を参照してください。 AWS

さらに、SAP などの特殊なワークロードが存在する場合は、それらのワークロードの経験を持つ個別の専門チームも必要です。特殊なワークロードの詳細については、AWS 「Migration Acceleration Program」の「MAP specialized workloads」を参照してください。

以下の操作を実行します。

1. プロジェクトガバナンスをサポートするために必要なリソースを定義します。一般的なリソースには、デリバリーガバナンスと監視のためのプログラムマネージャー、プロジェクトマネージャー、サポートプロジェクトマネージャーが含まれます。
2. 移行ツールをサポートするために必要なリソースを定義します。一般的なリソースには、クラウドアーキテクトや外部コンサルタントが含まれます。
3. プロジェクトに ERP システムなどの特殊なワークロードの移行が含まれている場合は、そのワークロードをサポートするために必要なリソースを定義します。特殊なワークロードの一般的なリソースは次のとおりです。
   - プロジェクトマネージャー
   - アーキテクチャリード
   - アーキテクチャエンジニア
   - DevOps エンジニア
   - 以下を含む特殊な移行ポッド：
     - 機能対象分野のエキスパート (SME)
     - テストスペシャリスト
4. リホストなど、各移行戦略をサポートするために必要なリソースを定義します。一般的なリソースは次のとおりです。
   - プロジェクトリード

- コンピューティング、ストレージ、ネットワーキングのアーキテクトとエンジニア
- テストスペシャリスト

5. 検出、初期化、実装など、プロジェクトのさまざまな段階でこれらのチームをサポートするために必要なリソースの数を割り当てます。プロセスを調整する際には移行の加速を検討し、ステージやプロジェクトの終了時にリソースをスケールダウンする方法を検討してください。

ステップ 7: 決定ログを作成する

大規模な移行を通じて、 リードは発生した問題を解決するための意思決定を行います。大規模な移行プロジェクトのサイズと範囲のため、すべての決定が下されたときにプロジェクトマネージャーが存在することはできません。ワークストリームリードは、ワークストリームに影響する決定を記録する責任があります。プロジェクトマネージャーは、決定事項を確認し、プロジェクトステータスレビューミーティングで最近の決定事項を提示する責任があります。

このステップは通常、プロジェクトマネージャーによって実行されます。このステップでは、共有リポジトリに決定ログを作成し、ワークストリームリードが決定のログ記録に関する各自の責任を理解していることを確認します。必要に応じて、エスカレーション計画を使用してタイムリーな意思決定を容易にします。詳細については、「ステップ 2: エスカレーション計画を立てる」を参照してください。すべてのチームメンバーが、各レベルで実行できる意思決定のタイプを理解していることを確認します。

以下の操作を実行します。

1. 決定ログを作成します。Jira や Confluence などの専用のプロジェクト管理ツールを使用することも、Microsoft Excel でリストを作成することもできます。以下を文書化することをお勧めします。
   - 決定の簡単な説明
   - ステータス
   - 決定がプロジェクトに与える影響
   - 考慮される代替オプション
   - 決定者
   - 決定が行われた日付
2. ワークストリームリードと会議を行い、決定ログを確認し、その使用方法をトレーニングします。決定を記録する文化を確立することが重要です。

3. 決定ログを共有リポジトリに保存し、すべてのワークストリームリードがアクセスできることを確認します。
4. 各プロジェクトステータスレビュー会議の前に、前回の会議以降に行われた決定についてログを確認し、プロジェクトステータスレポートプレゼンテーションにこれらの決定を含めます。これにより、プロジェクトの過程で行われたすべての決定について、プロジェクトレベルの透明性が確保されます。

ステップ 8: RAID ログを作成する

決定ログと同様に、リスク、アクション、問題、依存関係 (RAID) ログと呼ばれるプロジェクト管理ツールでリスクと問題を追跡する必要があります。大規模な移行をどれだけ徹底的に計画しても、問題が発生し、プロジェクトにいくつかのリスクを特定します。リスクと問題を特定して記録することで、プロジェクトに透明性を提供し、潜在的な問題を制御およびモニタリングするプロセスを確立し、プロジェクトへの影響を最小限に抑えます。

以下の操作を実行します。

1. RAID ログを作成します。Jira や Confluence などの専用のプロジェクト管理ツールを使用することも、Microsoft Excel でリストを作成することもできます。以下を文書化することをお勧めします。
   - タイプ (リスク、アクション、問題、または依存関係)
   - 項目の簡単な説明
   - オープン日
   - 見込み
   - Impact
   - 重要度スコア。確率と影響を乗算して計算されます。
   - 所有者
2. ワークストリームリードと会議を行い、RAID ログを確認し、その使用方法をトレーニングします。リスクと問題を記録する文化を確立することが重要です。
3. RAID ログを共有リポジトリに保存し、すべてのワークストリームリードがアクセスできることを確認します。
4. 各プロジェクトステータスレビューミーティングの前に、前回のミーティング以降に特定されたリスクと問題がないかログを確認し、プロジェクトステータスレポートプレゼンテーションに含めます。これにより、すべてのリスクと問題に対してプロジェクトレベルの透明性が確保されます。

タスク終了基準

このタスクは、以下を実行すると完了します。

- Microsoft Excel で Jira、Confluence、ダッシュボードやリストなどのプロジェクト管理ツールを 1 つ以上選択した。
- 移行戦略 (リホストなど) ごと、および大規模な移行プロジェクトの高レベルタスクごとに、詳細な RACI マトリックスを作成して検証しました。
- 利点追跡オフィスを作成し、会議の定期的な頻度を設定し、会議の所有権とレポートテンプレートを作成しました。
- 内部ステークホルダーは、財務レポートの処理方法に整合しています。財務レポートをレビューする正式な頻度を確立し、受取人を特定し、誰が財務レポートにアクセスできるかを決定しました。
- プロジェクトのリソースプランを作成しました。
- 共有リポジトリに決定ログを確立し、すべてのチームリーダーが更新を行うことができます。
- RAID ログの場所とテンプレートを定義しました。ログを維持し、問題に優先順位を付けるプロセスを確立しました。RAID ログのWeek-to-weekの変更は、ステータスレポートにまとめられています。
- すべてのプロジェクト関係者は、プロジェクト概要ダッシュボードでプロジェクトのステータスの概要をどのように伝えるかに調整されています。

ステージ 2: 大規模な移行の実装

前のステージでは、移行を管理するために必要なすべてのツール、テンプレート、計画、プロセスを確立しました。この段階では、これらのアセットを使用して、移行を効果的に管理および監督します。このステージは、移行チームがウェーブの への移行を開始したときに開始されます AWS クラウド。このステージのゲートは、各波またはシーケンシャル波のグループに対して繰り返します。

ステージ 2 は、次のタスクで構成されます。

- タスク: ステージ 2 の定期的な会議をスケジュールする
- タスク: 通信ゲートの完了
  - ゲート 1: ウェーブの T マイナススケジュールを作成する
  - ゲート 2: T-28 コミットミーティング
  - ゲート 3: T-21 通信
  - ゲート 4: T-14 チェックポイントミーティング
  - ゲート 5: T-7 通信
  - ゲート 6: T-1 go または no-go ミーティング
  - ゲート 7: T-0 カットオーバー会議
  - ゲート 8: ハイパーケア期間の開始
  - ゲート 9: ハイパーケア期間の終了

タスク: ステージ 2 の定期的な会議をスケジュールする

で作成した会議計画に従ってステップ 3: 会議とその頻度を定義する、会議の所有者は、次の定期的な会議をスケジュールする必要があります。これらの会議は、最初の T-28 コミット会議の後のステージ 2 の開始時に開始され、移行が完了するまで続行されます。

- 移行営業時間
- 利点追跡オフィス会議

> **Important**
>
> で設定した定期的な会議を引き続き開催しますステップ 5: ステージ 1 の定期的な会議をスケジュールする。これらの会議は、プロジェクトの最後まで継続されます。

タスク: 通信ゲートの完了

このタスクでは、 で定義した通信ゲートと T-マイナススケジュールを使用してタスク: コミュニケーションゲートとスケジュールの定義、移行とポートフォリオのワークストリームを通過する各ウェーブのステータスを伝えます。

これらのゲートを個別に移動したり、複数のウェーブが同じスケジュールにある場合は、グループ内のゲートを移動したりできます。移行ワークストリームのウェーブオーバーラップのため、移行のどの時点でも、異なるゲートに複数のウェーブまたはウェーブのグループがあるのが一般的です。次の表は、移行ワークストリームで波がどのように重複し、各波が 1 週間間隔でスケジュールされているかを示しています。この例では、移行ワークストリームでいつでも 6～7 個のウェーブがアクティブになり、各ウェーブは異なるゲートに配置されます。

ゲート	ウェーブ 1	ウェーブ 2	ウェーブ 3	ウェーブ 4	ウェーブ 5
ゲート 1: T-マイナススケジュール	3 月 13 日	3 月 20 日	3 月 27 日	4 月 3 日	4 月 10 日
ゲート 2: T-28 ミーティング	3 月 20 日	3 月 27 日	4 月 3 日	4 月 10 日	4 月 17 日
ゲート 3: T-21 通信	3 月 27 日	4 月 3 日	4 月 10 日	4 月 17 日	4 月 24 日
ゲート 4: T-14 ミーティング	4 月 3 日	4 月 10 日	4 月 17 日	4 月 24 日	5 月 1 日
ゲート 5: T-7 通信	4 月 10 日	4 月 17 日	4 月 24 日	5 月 1 日	5 月 8 日

ゲート	ウェーブ 1	ウェーブ 2	ウェーブ 3	ウェーブ 4	ウェーブ 5
ゲート 6: T-1 go または no-go ミーティング	4 月 16 日	4 月 23 日	4 月 30 日	5 月 7 日	5 月 14 日
ゲート 7: カットオーバー会議	4 月 17 日	4 月 24 日	5 月 1 日	5 月 8 日	5 月 15 日
ゲート 8: ハイパーケア期間の開始	4 月 18 日	4 月 25 日	5 月 2 日	5 月 9 日	5 月 16 日
ゲート 9: ハイパーケア期間の終了	4 月 22 日	4 月 29 日	5 月 6 日	5 月 13 日	5 月 20 日

このタスクは、次の通信ゲートで構成されます。

- ゲート 1: ウェーブの T マイナススケジュールを作成する
- ゲート 2: T-28 コミットミーティング
- ゲート 3: T-21 通信
- ゲート 4: T-14 チェックポイントミーティング
- ゲート 5: T-7 通信
- ゲート 6: T-1 go または no-go ミーティング
- ゲート 7: T-0 カットオーバー会議
- ゲート 8: ハイパーケア期間の開始
- ゲート 9: ハイパーケア期間の終了

ゲート 1: ウェーブの T マイナススケジュールを作成する

この通信ゲートで次の操作を行います。

1. このウェーブのドキュメントを保存する単一の共有リポジトリを作成します。

2. で作成した T-minus スケジュールテンプレートを使用してステップ 2: T-minus スケジュールテンプレートを作成する、このウェーブに固有の日付を入力し、T-minus スケジュールを共有リポジトリに保存します。
3. AWS 「大規模な移行用の移行プレイブック」で作成した移行タスクリストのコピーを作成し、共有リポジトリに保存します。このタスクリストは、ゲートを進める際のチェックリストとして使用します。
4. 適切な参加者との T-28 コミット会議をスケジュールします。この会議の詳細については、「」を参照してくださいステップ 3: 会議とその頻度を定義する。

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- ウェーブの共有リポジトリを確立しました。
- ウェーブの T マイナススケジュールを作成しました。
- ウェーブの移行タスクリストを作成しました。
- T-28 コミット会議をスケジュールしました。

次の移行アクティビティと、移行ランブックで定義されているその他のタスクが完了したら、次のゲートに進みます。

- ポートフォリオチームがウェーブプランを完了しました。
- ポートフォリオチームはウェーブの移行メタデータを収集しました。

ゲート 2: T-28 コミットミーティング

このゲートでは、移行チームがアプリケーション所有者とウェーブプランを確認し、ウェーブプランとカットオーバー日をコミットするようアプリケーション所有者に依頼します。この通信ゲートで次の操作を行います。

1. 「」で作成したウェーブワークショッププレゼンテーションを使用してステップ 4: 会議のプレゼンテーションを準備する、ウェーブに合わせてこのプレゼンテーションをカスタマイズし、共有リポジトリにプレゼンテーションを保存します。このプレゼンテーションは、このゲートと で使用しますゲート 4: T-14 チェックポイントミーティング。
2. T-28 コミットミーティングを実施し、プレゼンテーションを使用して以下を確認します。

- ウェーブプランと移行プロセスの概要を提供します。
- アプリケーション所有者の今後のアクション項目の詳細を提供します。
- アプリケーション所有者がこのウェーブの各アプリケーションを移行する準備ができていることを確認します。
- アプリケーション所有者が、アプリケーションのテストプランを提供する必要があることを理解していることを確認します。テストプランでは、カットオーバーが成功したことを検証する方法について説明します。テストはカットオーバーの直後に行われるため、問題が発生した場合、移行チームはビジネスユーザーやアプリケーションユーザーへの影響を最小限に抑えながらアプリケーションを元の環境にロールバックできます。
- ステークホルダーが波全体でどのように協力し、コミュニケーションを取ることが期待されているかを確認します。利害関係者がこのウェーブに関連するドキュメントを見つけることができる共有リポジトリの場所を指定します。
- で作成したエスカレーション計画を確認しますステップ 2: エスカレーション計画を立てる。
- 質問と回答の機会を提供します。

3. T-28 コミットミーティングの後、「」で作成した T-28 通信 E メールを送信しますステップ 3: ゲートごとに標準の E メールテンプレートを作成する。ウェーブ情報と受信者の E メールをカスタマイズし、このウェーブにすべてのアプリケーションとサーバーを追加します。
4. T-28 コミットミーティングの後、適切な参加者と次のミーティングをスケジュールします。
   - T-14 チェックポイント会議
   - T-1 go または no-go 会議
   - T-0 カットオーバー会議

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- T-28 コミットミーティングを実施しました。
- 共有リポジトリについてすべての主要な利害関係者に Wave ドキュメントへのアクセスを知らせ、すべての利害関係者がアクセスできます。
- に従って、移行営業時間の保持を開始しましたタスク: ステージ 2 の定期的な会議をスケジュールする。
- アプリケーション所有者は、ウェーブプラン内のアプリケーションを移行できることを確認しました。

- すべての利害関係者はコミュニケーションのアプローチを理解し、参加する必要がある会議を把握しています。
- アプリケーション所有者は、自分が担当する特定のアクション項目を理解します。
- T-28 通信 E メールをすべての利害関係者に送信しました。
- 会議のプレゼンテーションと会議のメモを共有リポジトリに保存し、すべての利害関係者がアクセスできるようにしました。
- T-14 コミット会議をスケジュールしました。
- T-1 go または no-go 会議をスケジュールしました。
- T-0 カットオーバー会議を予定しました。

次の移行アクティビティと、移行ランブックで定義されているその他のタスクが完了したら、次のゲートに進みます。

- T-28 コミット会議中に行われた変更でウェーブプランを更新しました。
- ウェーブ内のアプリケーションとサーバーの変更リクエスト (RFC) を送信し、変更ウィンドウがスケジュールされています。
- 変更管理プロセスを理解して特定します。
- 転送、ルーティング、プロキシサービスなどの新しいインフラストラクチャ要件について RFCs を送信済みである。
- 移行タスクリストを更新しました。

ゲート 3: T-21 通信

コミュニケーションチームは、アプリケーション所有者やビジネスユニットの担当者との連絡を継続します。これらの利害関係者は、質問の機会を提供するために、移行営業時間に招待されます。

1. で作成した T-21 通信 E メールを送信しますステップ 3: ゲートごとに標準の E メールテンプレートを作成する。ウェーブ情報と受信者の E メールをカスタマイズし、このウェーブにすべてのアプリケーションとサーバーを追加します。
2. 正しいアプリケーション所有者で、スケジュールされた T-14 チェックポイント会議を更新します。必要な参加者が参加できない場合は、エスカレーション計画に従って代替担当者が参加できることを確認します。

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- T-21 通信 E メールをすべての利害関係者に送信しました。

次の移行アクティビティと、移行ランブックで定義されているその他のタスクが完了したら、次のゲートに進みます。

- ソースサーバーがレプリケーションの最小要件を満たしていることを確認しました。
- ウェーブでアプリケーションとサーバーのレプリケーションを開始しました。
- 移行タスクリストを更新しました。

ゲート 4: T-14 チェックポイントミーティング

このゲートでは、アプリケーション所有者と T-14 チェックポイントミーティングを行い、チームがスケジュールどおりにカットオーバーする予定があるかどうかを評価します。この通信ゲートで次の操作を行います。

1. 「」で準備したウェーブワークショッププレゼンテーションを使用してゲート 2: T-28 コミットミーティング、T-14 チェックポイントミーティングのプレゼンテーションを更新します。
2. T-14 チェックポイントミーティングを実施し、以下を確認します。
   - このウェーブで移行されるアプリケーションとサーバーを確認します。
   - 残りのタスクとスケジュールを確認して、参加者がプロセスの残りのステップを理解していることを確認します。
   - カットオーバーミーティングですべてのアプリケーション所有者 (またはその代理人) が対応できることを確認します。
   - カットオーバーが完了すると、テストプランの準備が整っていることを確認します。
3. T-14 チェックポイントミーティングの後、「」で作成した T-14 通信 E メールを送信しますステップ 3: ゲートごとに標準の E メールテンプレートを作成する。ウェーブ情報と受信者の E メールをカスタマイズし、このウェーブにすべてのアプリケーションとサーバーを追加します。
4. アプリケーション所有者が指定した代替担当者など、参加者に変更があった場合は、T-1 go または no-go 会議と T-0 カットオーバー会議への招待を更新します。
5. 移行タスクリストを更新します。

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- T-14 チェックポイントミーティングを実施しました。すべてのアプリケーション所有者または指定された担当者が出席します。アプリケーション所有者が出席せず、応答しない場合は、エスカレーション計画に従って出席なしをエスカレーションします。
- その週の移行営業時間を設定しました。
- T-14 通信 E メールをすべての利害関係者に送信しました。
- 会議のプレゼンテーションと会議のメモを共有リポジトリに保存し、すべての利害関係者がアクセスできるようにしました。
- 移行前、移行中、移行後のすべてのタスクのチェックリストを作成し、完了したタスクをすべて閉じ、チェックリストを共有リポジトリに保存しました。

次の移行アクティビティと、移行ランブックで定義されているその他のタスクが完了したら、次のゲートに進みます。

- レプリケートされたアプリケーションとサーバーのヘルスとステータスを検証しました。問題をトラブルシューティング中であるか、トラブルシューティングを完了している。
- アプリケーション所有者は、移行チームにテストプランを提供しています。
- 移行タスクリストを更新しました。

ゲート 5: T-7 通信

このゲートでは、コミュニケーションチームはアプリケーション所有者やビジネスユニットの担当者との連絡を継続します。また、カットオーバーアクティビティと会議の準備も行います。

1. で作成した T-7 通信 E メールを送信しますステップ 3: ゲートごとに標準の E メールテンプレートを作成する。ウェーブ情報と受信者の E メールをカスタマイズし、このウェーブにすべてのアプリケーションとサーバーを追加します。
2. 必要な参加者が T-1 go または no-go 会議と T-0 カットオーバー会議に参加できることを確認します。必要に応じて会議の招待状を更新し、代替代理人を含めます。

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- T-7 通信 E メールをすべての利害関係者に送信しました。
- T-1 go または no-go 会議と T-0 カットオーバー会議への出席が確認されました。すべての参加者が会議を承諾したか、代替代理人が特定されました。

次の移行アクティビティと、移行ランブックで定義されているその他のタスクが完了したら、次のゲートに進みます。

- このウェーブに対するすべての変更リクエストが承認されました。
- ターゲットインフラストラクチャがカットオーバーの準備が整っていることを検証しました。
- インフラストラクチャを検証するために作成したテストインスタンスをシャットダウンしました。
- カットオーバータスクリストを検証しました。
- 移行タスクリストを更新しました。

ゲート 6: T-1 go または no-go ミーティング

このゲートでは、RACI マトリックスのすべてのチームメンバーと移行前アクティビティのチェックリストを確認して、ウェーブ内のアプリケーションとサーバーがカットオーバーの準備が整っていることを検証します。このゲートは、予定されたカットオーバーの 24～48 時間前に発生します。

1. T-1 go または no-go ミーティングで、RACI マトリックスのすべてのチームメンバーとチェックリストを確認して、ウェーブ内のアプリケーションとサーバーがカットオーバーの準備が整っていることを確認します。
2. 必要なすべての参加者が T-0 カットオーバー会議に参加できることを確認します。
3. ウェーブの移行 (go) に進む場合は、「」で作成した T-1 通信 E メールを送信しますステップ 3: ゲートごとに標準の E メールテンプレートを作成する。ウェーブ情報と受信者の E メールをカスタマイズし、このウェーブにすべてのアプリケーションとサーバーを追加します。
4. ウェーブまたは特定のアプリケーションとサーバーの移行 (no-go) を続行しない場合は、すべての利害関係者に決定を知らせる E メールを送信し、次のステップまたはスケジュールの変更に関する利用可能な情報を提供します。

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- T-0 カットオーバー会議でリソースが利用可能であること、および必要なすべての参加者が参加できることを確認しました。
- 会議のプレゼンテーションと会議のメモを共有リポジトリに保存し、すべての利害関係者がアクセスできるようにしました。
- T-1 通信 E メールをすべての利害関係者に送信しました。

次の移行アクティビティと、移行ランブックで定義されているその他のタスクが完了したら、次のゲートに進みます。

- 移行タスクリストで、すべての移行タスクが完了したことを確認しました。

ゲート 7: T-0 カットオーバー会議

このゲートでは、カットオーバー会議中にウェーブ内のすべてのサーバーとアプリケーションを移行し、すぐにアプリケーション所有者が移行したアプリケーションをテストして、期待どおりに動作していることを確認します。アプリケーション所有者は、会議全体に参加するか、アプリケーションに必要な場合にのみ参加できます。

1. カットオーバー会議の前に、「」で作成した T-0 通信 E メールを送信しますステップ 3: ゲートごとに標準の E メールテンプレートを作成する。ウェーブ情報と受信者の E メールをカスタマイズし、このウェーブにすべてのアプリケーションとサーバーを追加します。
2. T-0 カットオーバーミーティングでは、移行ランブックの指示に従ってウェーブ内のサーバーとアプリケーションを移行します。このランブックは、AWS 「大規模な移行のための移行プレイブック」の指示に従って開発しました。
3. アプリケーションまたはサーバーが移行されたら、アプリケーション所有者が作成したテストプランを使用して、アプリケーションが次のように機能していることを確認します。
   - アプリケーションまたはサーバーが想定どおりに機能している場合、または軽微な問題しかない場合は、 AWS 環境内に残して問題を修正します。
   - アプリケーションまたはサーバーが機能していない場合、または重大な問題がある場合は、ロールバックします。
4. 移行タスクリストのカットオーバーアクティビティを完了したら、タスクリストを更新します。
5. 「」で作成したカットオーバー完了通信 E メールを送信しますステップ 3: ゲートごとに標準の E メールテンプレートを作成する。ウェーブ情報と受信者の E メールをカスタマイズし、このウェーブにすべてのアプリケーションとサーバーを追加します。

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- ウェーブ内のすべてのアプリケーションまたはサーバーが正常に移行されたことを検証したか、ロールバックしました。
- ロールバックされたアプリケーションまたはサーバーを書き留めました。これらのアプリケーションまたはサーバーでは、移行パターンを更新するか、カットオーバー中に発生した問題に対処するためにターゲット状態を再定義する必要があります。これらのアプリケーションまたはサーバーは、将来のウェーブプランに含めます。
- カットオーバー完了のコミュニケーション E メールをすべての利害関係者に送信しました。

次のカットオーバーアクティビティが完了したら、次のゲートに進みます。

- 移行タスクリストのカットオーバータスクセクションのすべてのステップが完了しました。

ゲート 8: ハイパーケア期間の開始

このゲートでは、次の操作を行います。

1. プロジェクトの関係者に、クラウド内の移行されたアプリケーションとサーバーを確認するよう依頼します。問題が特定された場合は、移行チームに送信する必要があります。
2. カットオーバー中またはハイパーケア期間中に特定された問題に対処します。
3. クラウド運用チームがワークロードを受け入れる準備ができていることを確認します。
4. すべてのプロジェクト管理ツールとリポジトリを更新して、ウェーブのステータスを反映します。

ゲートの終了条件

次のプロジェクトガバナンスアクティビティが完了したら、次のゲートに進みます。

- すべてのステークホルダーが、移行されたアプリケーションとサーバーを確認しました。
- 移行チームは、カットオーバー中またはハイパーケア期間中に特定されたアプリケーションまたはサーバーの問題に対処しました。
- クラウド運用チームは、移行されたアプリケーションとサーバーを受け入れる準備ができていることを確認しました。

- ウェーブステータスを反映するために、すべてのプロジェクト管理ツールとリポジトリを更新しました。

ゲート 9: ハイパーケア期間の終了

ハイパーケア期間は通常 1～4 日間で、移行チームが移行したアプリケーションまたはサーバーに関する問題を解決すると終了します。ハイパーケア期間の終了時に、移行チームはクラウド運用 (Cloud Ops) チームとミーティングを行い、移行されたアプリケーションとサーバーを確認します。このゲートでは、移行チームは移行されたワークロードの継続的なサポートを Cloud Ops チームに転送します。Cloud Ops チームは、ハイパーケア期間が完了したこと、およびそれらが問題に関する連絡窓口になったことをアプリケーション所有者に通知します。必要に応じて、このコミュニケーションにアンケートを含め、アプリケーション所有者を招待して、移行とカットオーバーのプロセスに関するフィードバックを提供できます。

1. 移行したアプリケーションとサーバーをクラウド運用チームの設定管理データベース (CMDB) に組み込みます。
2. ServiceNow などの Cloud Ops 技術管理サポートツールにアプリケーション情報を組み込みます。
3. ステップ 3: ゲートごとに標準の E メールテンプレートを作成する 「」で作成したハイパーケア完了の通信 E メールをゲートごとに送信します。ウェーブ情報の E メールをカスタマイズし、クラウド運用チームに連絡する方法の手順を含めます。
4. ソースサーバーとサポートインフラストラクチャの廃止プロセスを開始するために、インフラストラクチャサポートチームに移行を通知します。このステップは通常、Cloud Ops チームまたはプロジェクトマネージャーによって実行されます。

ゲートの終了条件

このゲートは、次のプロジェクトガバナンスアクティビティを実行すると完了します。

- Cloud Ops は、すべてのワークロード関連情報を CMDB に組み込みました。
- Cloud Ops は、すべてのアプリケーション情報を技術管理サポートツールに組み込みました。
- ハイパーケアに関する完全なコミュニケーション E メールをすべての利害関係者に送信しました。
- インフラストラクチャチームは、不要になったサポートインフラストラクチャの廃止を開始しました。

リソース

AWS 大規模な移行

大規模な移行に関する AWS 完全な 規範ガイダンスシリーズにアクセスするには、「 への大規模な移行 AWS クラウド」を参照してください。

その他のリファレンス

- 準備フェーズ (AWS 規範ガイダンス)

寄稿者

このドキュメントの寄稿者は次のとおりです。

- Pratik Chunawala、プリンシパルクラウドアーキテクト
- Bill David、Principal Customer Solutions Manager
- Wally Lu、プリンシパルコンサルタント
- Amit Rudraraju、シニアクラウドアーキテクト

ドキュメント履歴

以下の表は、本ガイドの重要な変更点について説明したものです。今後の更新に関する通知を受け取る場合は、RSS フィード をサブスクライブできます。

変更	説明	日付
初版発行	—	2022 年 2 月 28 日

AWS 規範ガイダンス用語集

以下は、 AWS 規範ガイダンスが提供する戦略、ガイド、パターンで一般的に使用される用語です。エントリを提案するには、用語集の最後のフィードバックの提供リンクを使用します。

数字

7 Rs

アプリケーションをクラウドに移行するための 7 つの一般的な移行戦略。これらの戦略は、ガートナーが 2011 年に特定した 5 Rs に基づいて構築され、以下で構成されています。

- リファクタリング/アーキテクチャの再設計 — クラウドネイティブ特徴を最大限に活用して、俊敏性、パフォーマンス、スケーラビリティを向上させ、アプリケーションを移動させ、アーキテクチャを変更します。これには、通常、オペレーティングシステムとデータベースの移植が含まれます。例: オンプレミスの Oracle データベースを Amazon Aurora PostgreSQL 互換エディションに移行します。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: オンプレミスの Oracle データベースを の Oracle 用 Amazon Relational Database Service (Amazon RDS) に移行します AWS クラウド。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: カスタマーリレーションシップ管理 (CRM) システムを Salesforce.com に移行します。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: オンプレミスの Oracle データベースを の EC2 インスタンス上の Oracle に移行します AWS クラウド。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。サーバーをオンプレミスプラットフォームから同じプラットフォームのクラウドサービスに移行します。例: Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。

- 使用停止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

属性ベースのアクセスコントロールを参照してください。

抽象化されたサービス

「マネージドサービス」を参照してください。

ACID

アトミック性、一貫性、分離性、耐久性を参照してください。

アクティブ - アクティブ移行

(双方向レプリケーションツールまたは二重書き込み操作を使用して) ソースデータベースとターゲットデータベースを同期させ、移行中に両方のデータベースが接続アプリケーションからのトランザクションを処理するデータベース移行方法。この方法では、1 回限りのカットオーバーの必要がなく、管理された小規模なバッチで移行できます。より柔軟ですが、アクティブ/パッシブ移行よりも多くの作業が必要です。

アクティブ - パッシブ移行

ソースデータベースとターゲットデータベースを同期させながら、データがターゲットデータベースにレプリケートされている間、接続しているアプリケーションからのトランザクションをソースデータベースのみで処理するデータベース移行の方法。移行中、ターゲットデータベースはトランザクションを受け付けません。

集計関数

行のグループで動作し、グループの単一の戻り値を計算する SQL 関数。集計関数の例には、SUMおよび が含まれますMAX。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

データセット内の個人情報を完全に削除するプロセス。匿名化は個人のプライバシー保護に役立ちます。匿名化されたデータは、もはや個人データとは見なされません。

アンチパターン

繰り返し起こる問題に対して頻繁に用いられる解決策で、その解決策が逆効果であったり、効果がなかったり、代替案よりも効果が低かったりするもの。

アプリケーションコントロール

マルウェアからシステムを保護するために、承認されたアプリケーションのみを使用できるようにするセキュリティアプローチ。

アプリケーションポートフォリオ

アプリケーションの構築と維持にかかるコスト、およびそのビジネス価値を含む、組織が使用する各アプリケーションに関する詳細情報の集まり。この情報は、ポートフォリオの検出と分析プロセス の需要要素であり、移行、モダナイズ、最適化するアプリケーションを特定し、優先順位を付けるのに役立ちます。

人工知能 (AI)

コンピューティングテクノロジーを使用し、学習、問題の解決、パターンの認識など、通常は人間に関連づけられる認知機能の実行に特化したコンピュータサイエンスの分野。詳細については、「人工知能 (AI) とは何ですか?」を参照してください。

AI オペレーション (AIOps)

機械学習技術を使用して運用上の問題を解決し、運用上のインシデントと人の介入を減らし、サービス品質を向上させるプロセス。 AWS 移行戦略での AIOps の使用方法については、オペレーション統合ガイド を参照してください。

非対称暗号化

暗号化用のパブリックキーと復号用のプライベートキーから成る 1 組のキーを使用した、暗号化のアルゴリズム。パブリックキーは復号には使用されないため共有しても問題ありませんが、プライベートキーの利用は厳しく制限する必要があります。

原子性、一貫性、分離性、耐久性 (ACID)

エラー、停電、その他の問題が発生した場合でも、データベースのデータ有効性と運用上の信頼性を保証する一連のソフトウェアプロパティ。

属性ベースのアクセス制御 (ABAC)

部署、役職、チーム名など、ユーザーの属性に基づいてアクセス許可をきめ細かく設定する方法。詳細については、 AWS Identity and Access Management (IAM) ドキュメントの「 の ABAC AWS」を参照してください。

信頼できるデータソース

最も信頼性のある情報源とされるデータのプライマリーバージョンを保存する場所。匿名化、編集、仮名化など、データを処理または変更する目的で、信頼できるデータソースから他の場所にデータをコピーすることができます。

アベイラビリティーゾーン

他のアベイラビリティーゾーンの障害から AWS リージョン 隔離され、同じリージョン内の他のアベイラビリティーゾーンへの低コストで低レイテンシーのネットワーク接続を提供する 内の別の場所。

AWS クラウド導入フレームワーク (AWS CAF)

のガイドラインとベストプラクティスのフレームワークは、組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るのに役立ちます。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを整理します。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、クラウド導入を成功させるための組織の準備に役立つ人材開発、トレーニング、コミュニケーションのガイダンスを提供します。詳細については、AWS CAF ウェブサイト と AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業見積もりを提供するツール。AWS WQF は AWS Schema Conversion Tool （ AWS SCT) に含まれています。データベーススキーマとコードオブジェクト、アプリケーションコード、依存関係、およびパフォーマンス特性を分析し、評価レポートを提供します。

B

不正なボット

個人や組織を混乱させたり、損害を与えたりすることを意図したボット。

BCP

「事業継続計画」を参照してください。

動作グラフ

リソースの動作とインタラクションを経時的に示した、一元的なインタラクティブビュー。Amazon Detective の動作グラフを使用すると、失敗したログオンの試行、不審な API 呼び出し、その他同様のアクションを調べることができます。詳細については、Detective ドキュメントのData in a behavior graphを参照してください。

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアン性も参照してください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの 1 つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

要素がセットのメンバーであるかどうかをテストするために使用される、確率的でメモリ効率の高いデータ構造。

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (青) で実行し、新しいアプリケーションバージョンを別の環境 (緑) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

ボット

インターネット経由で自動タスクを実行し、人間のアクティビティややり取りをシミュレートするソフトウェアアプリケーション。インターネット上の情報のインデックスを作成するウェブクローラーなど、一部のボットは有用または有益です。悪質なボットと呼ばれる他のボットの中には、個人や組織を混乱させたり、損害を与えたりすることを意図したものもあります。

ボットネット

マルウェアに感染し、ボットハーダーまたはボットオペレーターとして知られる、単一の当事者によって制御されているボットのネットワーク。ボットは、ボットとその影響をスケールするための最もよく知られているメカニズムです。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発したり、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチの概要」(GitHub ドキュメント) を参照してください。

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようになります。詳細については、 Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータ AWS を参照してください。

ブラウンフィールド戦略

環境の既存インフラストラクチャ。システムアーキテクチャにブラウンフィールド戦略を導入する場合、現在のシステムとインフラストラクチャの制約に基づいてアーキテクチャを設計します。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

価値を生み出すためにビジネスが行うこと (営業、カスタマーサービス、マーケティングなど)。マイクロサービスのアーキテクチャと開発の決定は、ビジネス能力によって推進できます。詳細については、ホワイトペーパー AWSでのコンテナ化されたマイクロサービスの実行 の ビジネス機能を中心に組織化 セクションを参照してください。

ビジネス継続性計画 (BCP)

大規模移行など、中断を伴うイベントが運用に与える潜在的な影響に対処し、ビジネスを迅速に再開できるようにする計画。

C

CAF

AWS 「クラウド導入フレームワーク」を参照してください。

Canary デプロイ

エンドユーザーへのバージョンのスローリリースと増分リリース。確信が持てば、新しいバージョンをデプロイし、現在のバージョン全体を置き換えます。

CCoE

「Cloud Center of Excellence」を参照してください。

CDC

「データキャプチャの変更」を参照してください。

変更データキャプチャ (CDC)

データソース (データベーステーブルなど) の変更を追跡し、その変更に関するメタデータを記録するプロセス。CDC は、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストします。AWS Fault Injection Service （ AWS FIS ） を使用して、 AWS ワークロードにストレスを与え、その応答を評価する実験を実行できます。

CI/CD

継続的インテグレーションと継続的デリバリーを参照してください。

分類

予測を生成するのに役立つ分類プロセス。分類問題の機械学習モデルは、離散値を予測します。離散値は、常に互いに区別されます。例えば、モデルがイメージ内に車があるかどうかを評価する必要がある場合があります。

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前のローカルでのデータの暗号化。

Cloud Center of Excellence (CCoE)

クラウドのベストプラクティスの作成、リソースの移動、移行のタイムラインの確立、大規模変革を通じて組織をリードするなど、組織全体のクラウド導入の取り組みを推進する学際的なチーム。詳細については、 AWS クラウド エンタープライズ戦略ブログの CCoE 投稿を参照してください。

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的にエッジコンピューティングテクノロジーに接続されています。

クラウド運用モデル

IT 組織において、1 つ以上のクラウド環境を構築、成熟、最適化するために使用される運用モデル。詳細については、「クラウド運用モデルの構築」 を参照してください。

導入のクラウドステージ

組織が に移行するときに通常実行する 4 つのフェーズ AWS クラウド :

- プロジェクト — 概念実証と学習を目的として、クラウド関連のプロジェクトをいくつか実行する
- 基礎固め — お客様のクラウドの導入を拡大するための基礎的な投資 (ランディングゾーンの作成、CCoE の定義、運用モデルの確立など)
- 移行 — 個々のアプリケーションの移行
- 再発明 — 製品とサービスの最適化、クラウドでのイノベーション

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。移行戦略との関連性については、 AWS「移行準備ガイド」を参照してください。

CMDB

「設定管理データベース」を参照してください。

コードリポジトリ

ソースコードやその他の資産 (ドキュメント、サンプル、スクリプトなど) が保存され、バージョン管理プロセスを通じて更新される場所。一般的なクラウドリポジトリには、 GitHubまたは が含まれますBitbucket Cloud。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

めったにアクセスされず、通常は過去のデータです。この種類のデータをクエリする場合、通常は低速なクエリでも問題ありません。このデータを低パフォーマンスで安価なストレージ階層またはクラスに移動すると、コストを削減することができます。

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI は CV 用の画像処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定は想定状態から変化します。ワークロードが非準拠になる可能性があり、通常は段階的かつ意図的ではありません。

構成管理データベース (CMDB)

データベースとその IT 環境 (ハードウェアとソフトウェアの両方のコンポーネントとその設定を含む) に関する情報を保存、管理するリポジトリ。通常、CMDB のデータは、移行のポートフォリオの検出と分析の段階で使用します。

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイすることも、組織全体にデプロイすることもできます。詳細については、 AWS Config ドキュメントの「コンフォーマンスパック」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバ

リーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

ネットワーク内のデータを重要度と機密性に基づいて識別、分類するプロセス。データに適した保護および保持のコントロールを判断する際に役立つため、あらゆるサイバーセキュリティのリスク管理戦略において重要な要素です。データ分類は、 AWS Well-Architected フレームワークのセキュリティの柱のコンポーネントです。詳細については、データ分類を参照してください。

データドリフト

実稼働データと ML モデルのトレーニングに使用されたデータとの間に有意な差異が生じたり、入力データが時間の経過と共に有意に変化したりすることです。データドリフトは、ML モデル予測の全体的な品質、精度、公平性を低下させる可能性があります。

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元管理とガバナンスを備えた分散型の分散型データ所有権を提供するアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。でデータ最小化を実践 AWS クラウドすることで、プライバシーリスク、コスト、分析のカーボンフットプリントを削減できます。

データ境界

AWS 環境内の一連の予防ガードレール。信頼された ID のみが、期待されるネットワークから信頼されたリソースにアクセスできるようにします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

raw データをお客様の機械学習モデルで簡単に解析できる形式に変換すること。データの前処理とは、特定の列または行を削除して、欠落している、矛盾している、または重複する値に対処することを意味します。

データ出所

データの生成、送信、保存の方法など、データのライフサイクル全体を通じてデータの出所と履歴を追跡するプロセス。

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには通常、大量の履歴データが含まれており、通常はクエリや分析に使用されます。

データベース定義言語 (DDL)

データベース内のテーブルやオブジェクトの構造を作成または変更するためのステートメントまたはコマンド。

データベース操作言語 (DML)

データベース内の情報を変更 (挿入、更新、削除) するためのステートメントまたはコマンド。

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせる。ディープアンサンブルを使用して、より正確な予測を取得したり、予測の不確実性を推定したりできます。

ディープラーニング

人工ニューラルネットワークの複数層を使用して、入力データと対象のターゲット変数の間のマッピングを識別する機械学習サブフィールド。

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリ

ティの手法。この戦略を採用するときは AWS、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加して、リソースの安全性を確保します。たとえば、多層防御アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

では AWS Organizations、互換性のあるサービスが AWS メンバーアカウントを登録して組織のアカウントを管理し、そのサービスのアクセス許可を管理できます。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、 AWS Organizations ドキュメントのAWS Organizationsで使用できるサービスを参照してください。

デプロイ

アプリケーション、新機能、コードの修正をターゲットの環境で利用できるようにするプロセス。デプロイでは、コードベースに変更を施した後、アプリケーションの環境でそのコードベースを構築して実行します。

開発環境

「環境」を参照してください。

検出管理

イベントが発生したときに、検出、ログ記録、警告を行うように設計されたセキュリティコントロール。これらのコントロールは副次的な防衛手段であり、実行中の予防的コントロールをすり抜けたセキュリティイベントをユーザーに警告します。詳細については、Implementing security controls on AWSのDetective controlsを参照してください。

開発バリューストリームマッピング (DVSM)

ソフトウェア開発ライフサイクルのスピードと品質に悪影響を及ぼす制約を特定し、優先順位を付けるために使用されるプロセス。DVSM は、もともとリーンマニュファクチャリング・プラクティスのために設計されたバリューストリームマッピング・プロセスを拡張したものです。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

建物、工場、産業機器、生産ラインなど、現実世界のシステムを仮想的に表現したものです。デジタルツインは、予知保全、リモートモニタリング、生産最適化をサポートします。

ディメンションテーブル

スタースキーマでは、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する

離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けに一般的に使用されます。

ディザスタ

ワークロードまたはシステムが、導入されている主要な場所でのビジネス目標の達成を妨げるイベント。これらのイベントは、自然災害、技術的障害、または意図しない設定ミスやマルウェア攻撃などの人間の行動の結果である場合があります。

ディザスタリカバリ (DR)

災害によるダウンタイムとデータ損失を最小限に抑えるために使用する戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

各コンポーネントが提供している変化を続けるドメイン、またはコアビジネス目標にコンポーネントを接続して、複雑なソフトウェアシステムを開発するアプローチ。この概念は、エリック・エヴァンスの著書、Domain-Driven Design: Tackling Complexity in the Heart of Software (ドメイン駆動設計:ソフトウェアの中心における複雑さへの取り組み) で紹介されています (ボストン: Addison-Wesley Professional、2003)。strangler fig パターンでドメイン駆動型設計を使用する方法の詳細については、コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズ を参照してください。

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差を追跡します。たとえば、 AWS CloudFormation を使用してシステムリソースのドリフトを検出したり、 を使用して AWS Control Tower 、ガバナンス要件のコンプライアンスに影響を与える可能性のあるランディングゾーンの変更を検出したりできます。

DVSM

「開発値ストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

IoT ネットワークのエッジにあるスマートデバイスの計算能力を高めるテクノロジー。クラウドコンピューティングと比較すると、エッジコンピューティングは通信レイテンシーを短縮し、応答時間を短縮できます。

電子データ交換 (EDI)

組織間のビジネスドキュメントの自動交換。詳細については、「電子データ交換とは」を参照してください。

暗号化

人間が読み取り可能なプレーンテキストデータを暗号文に変換するコンピューティングプロセス。

暗号化キー

暗号化アルゴリズムが生成した、ランダム化されたビットからなる暗号文字列。キーの長さは決まっておらず、各キーは予測できないように、一意になるように設計されています。

エンディアン

コンピュータメモリにバイトが格納される順序。ビッグエンディアンシステムでは、最上位バイトが最初に格納されます。リトルエンディアンシステムでは、最下位バイトが最初に格納されます。

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これら

のアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

エンタープライズの主要なビジネスプロセス (会計、MES、プロジェクト管理など) を自動化および管理するシステム。

エンベロープ暗号化

暗号化キーを、別の暗号化キーを使用して暗号化するプロセス。詳細については、 AWS Key Management Service （ AWS KMS) ドキュメントの「エンベロープ暗号化」を参照してください。

環境

実行中のアプリケーションのインスタンス。クラウドコンピューティングにおける一般的な環境の種類は以下のとおりです。

- 開発環境 — アプリケーションのメンテナンスを担当するコアチームのみが使用できる、実行中のアプリケーションのインスタンス。開発環境は、上位の環境に昇格させる変更をテストするときに使用します。このタイプの環境は、テスト環境と呼ばれることもあります。
- 下位環境 — 初期ビルドやテストに使用される環境など、アプリケーションのすべての開発環境。
- 本番環境 — エンドユーザーがアクセスできる、実行中のアプリケーションのインスタンス。CI/CD パイプラインでは、本番環境が最後のデプロイ環境になります。
- 上位環境 — コア開発チーム以外のユーザーがアクセスできるすべての環境。これには、本番環境、本番前環境、ユーザー承認テスト環境などが含まれます。

エピック

アジャイル方法論で、お客様の作業の整理と優先順位付けに役立つ機能カテゴリ。エピックでは、要件と実装タスクの概要についてハイレベルな説明を提供します。たとえば、 AWS CAF セキュリティエピックには、ID とアクセスの管理、検出コントロール、インフラストラクチャセキュリティ、データ保護、インシデント対応が含まれます。 AWS 移行戦略のエピックの詳細については、プログラム実装ガイド を参照してください。

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

データセットを分析してその主な特性を理解するプロセス。お客様は、データを収集または集計してから、パターンの検出、異常の検出、および前提条件のチェックのための初期調査を実行します。EDA は、統計の概要を計算し、データの可視化を作成することによって実行されます。

F

ファクトテーブル

星スキーマの中央テーブル。事業運営に関する量的データを保存します。通常、ファクトテーブルには、メジャーを含む列とディメンションテーブルへの外部キーを含む列の 2 つのタイプの列が含まれます。

フェイルファスト

開発ライフサイクルを短縮するために頻繁で段階的なテストを使用する哲学。これはアジャイルアプローチの重要な部分です。

障害分離の境界

では AWS クラウド、アベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界で、障害の影響を制限し、ワークロードの耐障害性を向上させるのに役立ちます。詳細については、AWS 「障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

お客様が予測に使用する入力データ。例えば、製造コンテキストでは、特徴量は製造ラインから定期的にキャプチャされるイメージの可能性もあります。

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械

学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

数ショットプロンプト

同様のタスクの実行を求める前に、タスクと必要な出力を示す少数の例を LLM に提供します。この手法は、プロンプトに埋め込まれた例 (ショット) からモデルが学習するコンテキスト内学習のアプリケーションです。少数ショットプロンプトは、特定のフォーマット、推論、またはドメインの知識を必要とするタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセスコントロール」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

段階的なアプローチを使用する代わりに、変更データキャプチャによる継続的なデータレプリケーションを使用して、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

一般化データとラベル付けされていないデータの大規模なデータセットでトレーニングされている大規模な深層学習ニューラルネットワーク。FMs は、言語の理解、テキストと画像の生成、自然言語の会話など、さまざまな一般的なタスクを実行できます。詳細については、「基盤モデルとは」を参照してください。

G

生成 AI

大量のデータでトレーニングされ、シンプルなテキストプロンプトを使用して画像、動画、テキスト、オーディオなどの新しいコンテンツやアーティファクトを作成できる AI モデルのサブセット。詳細については、「生成 AI とは」を参照してください。

ジオブロッキング

地理的制限を参照してください。

地理的制限 (ジオブロッキング)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リストを使って指定します。詳細については、CloudFront ドキュメントのコンテンツの地理的ディストリビューションの制限を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローはレガシーと見なされ、トランクベースのワークフローはモダンで推奨されるアプローチです。

ゴールデンイメージ

そのシステムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

新しい環境に既存のインフラストラクチャが存在しないこと。システムアーキテクチャにグリーンフィールド戦略を導入する場合、既存のインフラストラクチャ (別名ブラウンフィールド) との互換性の制約を受けることなく、あらゆる新しいテクノロジーを選択できます。既存のインフラストラクチャを拡張している場合は、ブラウンフィールド戦略とグリーンフィールド戦略を融合させることもできます。

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは AWS Config、、Amazon GuardDuty AWS Security Hub、、 AWS Trusted Advisor Amazon Inspector、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

別のデータベースエンジンを使用するターゲットデータベースへお客様の出典データベースの移行 (例えば、Oracle から Amazon Aurora)。異種間移行は通常、アーキテクチャの再設計作業の一部であり、スキーマの変換は複雑なタスクになる可能性があります。AWS は、スキーマの変換に役立つ AWS SCTを提供します。

ハイアベイラビリティ (HA)

課題や災害が発生した場合に、介入なしにワークロードを継続的に運用できること。HA システムは、自動的にフェイルオーバーし、一貫して高品質のパフォーマンスを提供し、パフォーマンスへの影響を最小限に抑えながらさまざまな負荷や障害を処理するように設計されています。

ヒストリアンのモダナイゼーション

製造業のニーズによりよく応えるために、オペレーションテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

ホールドアウトデータ

機械学習モデルのトレーニングに使用されるデータセットから保留される、ラベル付きの履歴データの一部。モデル予測をホールドアウトデータと比較することで、ホールドアウトデータを使用してモデルのパフォーマンスを評価できます。

同種データベースの移行

お客様の出典データベースを、同じデータベースエンジンを共有するターゲットデータベース (Microsoft SQL Server から Amazon RDS for SQL Server など) に移行する。同種間移行は、通常、リホストまたはリプラットフォーム化の作業の一部です。ネイティブデータベースユーティリティを使用して、スキーマを移行できます。

ホットデータ

リアルタイムデータや最近の翻訳データなど、頻繁にアクセスされるデータ。通常、このデータには高速なクエリ応答を提供する高性能なストレージ階層またはクラスが必要です。

ホットフィックス

本番環境の重大な問題を修正するために緊急で配布されるプログラム。緊急性が高いため、通常の DevOps のリリースワークフローからは外れた形で実施されます。

ハイパーケア期間

カットオーバー直後、移行したアプリケーションを移行チームがクラウドで管理、監視して問題に対処する期間。通常、この期間は 1～4 日です。ハイパーケア期間が終了すると、アプリケーションに対する責任は一般的に移行チームからクラウドオペレーションチームに移ります。

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

AWS クラウド 環境内のアクセス許可を定義する 1 つ以上の IAM プリンシパルにアタッチされたポリシー。

アイドル状態のアプリケーション

90 日間の平均的な CPU およびメモリ使用率が 5～20% のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するか、オンプレミスに保持するのが一般的です。

IIoT

「産業用モノのインターネット」を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更する代わりに、本番環境のワークロード用に新しいインフラストラクチャをデプロイするモデル。イミュータブルインフラストラクチャは、本質的にミュータブルインフラストラクチャよりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS 「 Well-Architected Framework」の「Deploy using immutable infrastructure best practice」を参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリ

ケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

アプリケーションを 1 回ですべてカットオーバーするのではなく、小さい要素に分けて移行するカットオーバー戦略。例えば、最初は少数のマイクロサービスまたはユーザーのみを新しいシステムに移行する場合があります。すべてが正常に機能することを確認できたら、残りのマイクロサービスやユーザーを段階的に移行し、レガシーシステムを廃止できるようにします。この戦略により、大規模な移行に伴うリスクが軽減されます。

インダストリー 4.0

2016 年に Klaus Schwab によって導入された用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩によるビジネスプロセスのモダナイゼーションを指します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

アプリケーションのインフラストラクチャを一連の設定ファイルを使用してプロビジョニングし、管理するプロセス。IaC は、新しい環境を再現可能で信頼性が高く、一貫性のあるものにするため、インフラストラクチャを一元的に管理し、リソースを標準化し、スケールを迅速に行えるように設計されています。

産業分野における IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「Building an industrial Internet of Things (IIoT) digital transformation strategy」を参照してください。

インスペクション VPC

AWS マルチアカウントアーキテクチャでは、VPC (同一または異なる 内 AWS リージョン)、インターネット、オンプレミスネットワーク間のネットワークトラフィックの検査を管理する一元化された VPCs。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

IoT

インターネットまたはローカル通信ネットワークを介して他のデバイスやシステムと通信する、センサーまたはプロセッサが組み込まれた接続済み物理オブジェクトのネットワーク。詳細については、「IoT とは」を参照してください。

解釈可能性

機械学習モデルの特性で、モデルの予測がその入力にどのように依存するかを人間が理解できる度合いを表します。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

IoT

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

IT サービスを提供し、これらのサービスをビジネス要件に合わせるための一連のベストプラクティス。ITIL は ITSM の基盤を提供します。

IT サービス管理 (ITSM)

組織の IT サービスの設計、実装、管理、およびサポートに関連する活動。クラウドオペレーションと ITSM ツールの統合については、オペレーション統合ガイド を参照してください。

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

強制アクセス制御 (MAC) の実装で、ユーザーとデータ自体にそれぞれセキュリティラベル値が明示的に割り当てられます。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロー

ドとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、安全でスケーラブルなマルチアカウント AWS 環境のセットアップ を参照してください。

大規模言語モデル (LLM)

大量のデータに対して事前トレーニングされた深層学習 AI モデル。LLM は、質問への回答、ドキュメントの要約、テキストの他の言語への翻訳、文の完了など、複数のタスクを実行できます。詳細については、LLMs」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、IAM ドキュメントの最小特権アクセス許可を適用するを参照してください。

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。エンディアン性も参照してください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

パターン認識と学習にアルゴリズムと手法を使用する人工知能の一種。ML は、モノのインターネット (IoT) データなどの記録されたデータを分析して学習し、パターンに基づく統計モデルを生成します。詳細については、「機械学習」を参照してください。

メインブランチ

「ブランチ」を参照してください。

マルウェア

コンピュータのセキュリティまたはプライバシーを侵害するように設計されたソフトウェア。マルウェアは、コンピュータシステムの中断、機密情報の漏洩、不正アクセスにつながる可能性があります。マルウェアの例としては、ウイルス、ワーム、ランサムウェア、トロイの木馬、スパイウェア、キーロガーなどがあります。

マネージドサービス

AWS のサービス はインフラストラクチャレイヤー、オペレーティングシステム、プラットフォーム AWS を運用し、エンドポイントにアクセスしてデータを保存および取得します。Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB は、マネージドサービスの例です。これらは抽象化されたサービスとも呼ばれます。

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステムで、原材料を工場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整を行うために結果を検査する完全なプロセス。メカニズムは、動作時にそれ自体を強化および改善するサイクルです。詳細については、 AWS 「 Well-Architected フレームワーク」の「メカニズムの構築」を参照してください。

メンバーアカウント

組織の一部である管理アカウント AWS アカウント を除くすべて AWS Organizations。アカウントが組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

メッセージキューイングテレメトリトランスポート (MQTT)

リソースに制約のある IoT デバイス用の、パブリッシュ/サブスクライブパターンに基づく軽量 machine-to-machine (M2M) 通信プロトコル。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、AWS「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

各アプリケーションプロセスをマイクロサービスとして実行する独立したコンポーネントを使用してアプリケーションを構築するアプローチ。これらのマイクロサービスは、軽量 API を使用して、明確に定義されたインターフェイスを介して通信します。このアーキテクチャの各マイクロサービスは、アプリケーションの特定の機能に対する需要を満たすように更新、デプロイ、およびスケーリングできます。詳細については、「 でのマイクロサービスの実装 AWS」を参照してください。

Migration Acceleration Program (MAP)

組織がクラウドに移行するための強力な運用基盤を構築し、移行の初期コストを相殺するのに役立つコンサルティングサポート、トレーニング、サービスを提供する AWS プログラム。MAP には、組織的な方法でレガシー移行を実行するための移行方法論と、一般的な移行シナリオを自動化および高速化する一連のツールが含まれています。

大規模な移行

アプリケーションポートフォリオの大部分を次々にクラウドに移行し、各ウェーブでより多くのアプリケーションを高速に移動させるプロセス。この段階では、以前の段階から学んだベストプラクティスと教訓を使用して、移行ファクトリー チーム、ツール、プロセスのうち、オートメーションとアジャイルデリバリーによってワークロードの移行を合理化します。これは、AWS 移行戦略 の第 3 段階です。

移行ファクトリー

自動化された俊敏性のあるアプローチにより、ワークロードの移行を合理化する部門横断的なチーム。移行ファクトリーチームには、通常、運用、ビジネスアナリストおよび所有者、移行エンジニア、デベロッパー、およびスプリントで作業する DevOps プロフェッショナルが含まれます。エンタープライズアプリケーションポートフォリオの 20～50% は、ファクトリーのアプローチによって最適化できる反復パターンで構成されています。詳細については、このコンテンツセットの移行ファクトリーに関する解説とCloud Migration Factory ガイドを参照してください。

移行メタデータ

移行を完了するために必要なアプリケーションおよびサーバーに関する情報。移行パターンごとに、異なる一連の移行メタデータが必要です。移行メタデータの例としては、ターゲットサブネット、セキュリティグループ、 AWS アカウントなどがあります。

移行パターン

移行戦略、移行先、および使用する移行アプリケーションまたはサービスを詳述する、反復可能な移行タスク。例: AWS Application Migration Service を使用して Amazon EC2 への移行をリホストします。

Migration Portfolio Assessment (MPA)

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。MPA は、詳細なポートフォリオ評価 (サーバーの適切なサイジング、価格設定、TCO 比較、移行コスト分析) および移行プラン (アプリケーションデータの分析とデータ収集、アプリケーションのグループ化、移行の優先順位付け、およびウェーブプランニング) を提供します。MPA ツール (ログインが必要) は、すべての AWS コンサルタントと APN パートナーコンサルタントが無料で利用できます。

移行準備状況評価 (MRA)

AWS CAF を使用して、組織のクラウド準備状況に関するインサイトを取得し、長所と短所を特定し、特定されたギャップを埋めるためのアクションプランを構築するプロセス。詳細については、移行準備状況ガイド を参照してください。MRA は、AWS 移行戦略の第一段階です。

移行戦略

ワークロードを に移行するために使用するアプローチ AWS クラウド。詳細については、この用語集の「7 Rs エントリ」と「組織を動員して大規模な移行を加速する」を参照してください。

ML

???「機械学習」を参照してください。

モダナイゼーション

古い (レガシーまたはモノリシック) アプリケーションとそのインフラストラクチャをクラウド内の俊敏で弾力性のある高可用性システムに変換して、コストを削減し、効率を高め、イノベーションを活用します。詳細については、「」の「アプリケーションをモダナイズするための戦略 AWS クラウド」を参照してください。

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定されたギャップに対処するためのアクションプランが得られます。詳細については、『』の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」を参照してください。

モノリシックアプリケーション (モノリス)

緊密に結合されたプロセスを持つ単一のサービスとして実行されるアプリケーション。モノリシックアプリケーションにはいくつかの欠点があります。1 つのアプリケーション機能エクスペリエンスの需要が急増する場合は、アーキテクチャ全体をスケーリングする必要があります。モノリシックアプリケーションの特徴を追加または改善することは、コードベースが大きくなると複雑になります。これらの問題に対処するには、マイクロサービスアーキテクチャを使用できます。詳細については、モノリスをマイクロサービスに分解する を参照してください。

MPA

「移行ポートフォリオ評価」を参照してください。

MQTT

「Message Queuing Telemetry Transport」を参照してください。

多クラス分類

複数のクラスの予測を生成するプロセス (2 つ以上の結果の 1 つを予測します)。例えば、機械学習モデルが、「この製品は書籍、自動車、電話のいずれですか?」 または、「このお客様にとって最も関心のある商品のカテゴリはどれですか?」と聞くかもしれません。

ミュータブルインフラストラクチャ

本番ワークロードの既存のインフラストラクチャを更新および変更するモデル。Well-Architected AWS フレームワークでは、一貫性、信頼性、予測可能性を向上させるために、イミュータブルインフラストラクチャの使用をベストプラクティスとして推奨しています。

O

OAC

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

移行プロセス中にソースワークロードを停止させる移行方法。この方法はダウンタイムが長くなるため、通常は重要ではない小規模なワークロードに使用されます。

OI

「 オペレーションの統合」を参照してください。

OLA

「運用レベルの契約」を参照してください。

オンライン移行

ソースワークロードをオフラインにせずにターゲットシステムにコピーする移行方法。ワークロードに接続されているアプリケーションは、移行中も動作し続けることができます。この方法はダウンタイムがゼロから最小限で済むため、通常は重要な本番稼働環境のワークロードに使用されます。

OPC-UA

「Open Process Communications - Unified Architecture」を参照してください。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

産業用オートメーション用のmachine-to-machine (M2M) 通信プロトコル。OPC-UA は、データの暗号化、認証、認可スキームを備えた相互運用性標準を提供します。

オペレーショナルレベルアグリーメント (OLA)

サービスレベルアグリーメント (SLA) をサポートするために、どの機能的 IT グループが互いに提供することを約束するかを明確にする契約。

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問とそれに関連するベストプラクティスのチェックリスト。詳細については、 AWS Well-Architected フレームワークの「Operational Readiness Reviews (ORR)」を参照してください。

運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携するハードウェアおよびソフトウェアシステム。製造では、OT と情報技術 (IT) システムの統合が、Industry 4.0 変換の主な焦点です。

オペレーション統合 (OI)

クラウドでオペレーションをモダナイズするプロセスには、準備計画、オートメーション、統合が含まれます。詳細については、オペレーション統合ガイド を参照してください。

組織の証跡

組織 AWS アカウント 内のすべての のすべてのイベント AWS CloudTrail をログに記録する、 によって作成された証跡 AWS Organizations。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、CloudTrail ドキュメントの組織の証跡の作成を参照してください。

組織変更管理 (OCM)

人材、文化、リーダーシップの観点から、主要な破壊的なビジネス変革を管理するためのフレームワーク。OCM は、変化の導入を加速し、移行問題に対処し、文化や組織の変化を推進することで、組織が新しいシステムと戦略の準備と移行するのを支援します。 AWS 移行戦略では、クラウド導入プロジェクトに必要な変化のスピードにより、このフレームワークは人材アクセラレーションと呼ばれます。詳細については、OCM ガイド を参照してください。

オリジンアクセスコントロール (OAC)

Amazon Simple Storage Service (Amazon S3) コンテンツを保護するための、CloudFront のアクセス制限の強化オプション。OAC は AWS リージョン、すべての S3 バケット、 AWS KMS (SSE-KMS) によるサーバー側の暗号化、S3 バケットへの動的 PUT および DELETEリクエストをサポートします。

オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介してのみアクセスできます。OACも併せて参照してください。OAC では、より詳細な、強化されたアクセスコントロールが可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション内から開始されたネットワーク接続を処理する VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

P

アクセス許可の境界

ユーザーまたはロールが使用できるアクセス許可の上限を設定する、IAM プリンシパルにアタッチされる IAM 管理ポリシー。詳細については、IAM ドキュメントのアクセス許可の境界を参照してください。

個人を特定できる情報 (PII)

直接閲覧した場合、または他の関連データと組み合わせた場合に、個人の身元を合理的に推測するために使用できる情報。PII の例には、氏名、住所、連絡先情報などがあります。

PII

個人を特定できる情報を参照してください。

プレイブック

クラウドでのコアオペレーション機能の提供など、移行に関連する作業を取り込む、事前定義された一連のステップ。プレイブックは、スクリプト、自動ランブック、またはお客様のモダナイズされた環境を運用するために必要なプロセスや手順の要約などの形式をとることができます。

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

アクセス許可を定義 (アイデンティティベースのポリシーを参照)、アクセス条件を指定 (リソースベースのポリシーを参照)、または の組織内のすべてのアカウントに対する最大アクセス許可を定義 AWS Organizations （ サービスコントロールポリシーを参照) できるオブジェクト。

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。詳細については、マイクロサービスでのデータ永続性の有効化 を参照してください。

ポートフォリオ評価

移行を計画するために、アプリケーションポートフォリオの検出、分析、優先順位付けを行うプロセス。詳細については、「移行準備状況ガイド」を参照してください。

述語

`true` または を返すクエリ条件。一般的に`false`は `WHERE`句にあります。

述語プッシュダウン

転送前にクエリ内のデータをフィルタリングするデータベースクエリ最適化手法。これにより、リレーショナルデータベースから取得して処理する必要があるデータの量が減少し、クエリのパフォーマンスが向上します。

予防的コントロール

イベントの発生を防ぐように設計されたセキュリティコントロール。このコントロールは、ネットワークへの不正アクセスや好ましくない変更を防ぐ最前線の防御です。詳細については、Implementing security controls on AWSのPreventative controlsを参照してください。

プリンシパル

アクションを実行し AWS 、リソースにアクセスできる のエンティティ。このエンティティは通常、、IAM AWS アカウントロール、または ユーザーのルートユーザーです。詳細については、IAM ドキュメントのロールに関する用語と概念内にあるプリンシパルを参照してください。

プライバシーバイデザイン

開発プロセス全体を通じてプライバシーを考慮するシステムエンジニアリングアプローチ。

プライベートホストゾーン

1 つ以上の VPC 内のドメインとそのサブドメインへの DNS クエリに対し、Amazon Route 53 がどのように応答するかに関する情報を保持するコンテナ。詳細については、Route 53 ドキュメントの「プライベートホストゾーンの使用」を参照してください。

プロアクティブコントロール

非準拠リソースのデプロイを防ぐように設計されたセキュリティコントロール。これらのコントロールは、プロビジョニング前にリソースをスキャンします。リソースがコントロールに準拠していない場合、プロビジョニングされません。詳細については、 AWS Control Tower ドキュメントの「 コントロールリファレンスガイド」および「 セキュリティコントロールの実装」の「プロアクティブコントロール」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

設計、開発、発売から成長と成熟まで、製品のデータとプロセスのライフサイクル全体にわたる管理。

本番環境

「環境」を参照してください。

プログラム可能なロジックコントローラー (PLC)

製造では、マシンをモニタリングし、製造プロセスを自動化する、信頼性の高い適応可能なコンピュータです。

プロンプトの連鎖

1 つの LLM プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改善または拡張したりするために使用されます。これにより、モデルのレスポンスの精度と関連性が向上し、より詳細でパーソナライズされた結果が得られます。

仮名化

データセット内の個人識別子をプレースホルダー値に置き換えるプロセス。仮名化は個人のプライバシー保護に役立ちます。仮名化されたデータは、依然として個人データとみなされます。

パブリッシュ/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。スケーラビリティと応答性を向上させます。たとえば、マイクロサービスベースの MES では、マイクロサービスは他のマイクロサー

ビスがサブスクライブできるチャネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

SQL リレーショナルデータベースシステムのデータにアクセスするために使用される手順などの一連のステップ。

クエリプランのリグレッション

データベースサービスのオプティマイザーが、データベース環境に特定の変更が加えられる前に選択されたプランよりも最適性の低いプランを選択すること。これは、統計、制限事項、環境設定、クエリパラメータのバインディングの変更、およびデータベースエンジンの更新などが原因である可能性があります。

R

RACI マトリックス

責任、説明責任、相談、通知 (RACI) を参照してください。

RAG

「取得拡張生成」を参照してください。

ランサムウェア

決済が完了するまでコンピュータシステムまたはデータへのアクセスをブロックするように設計された、悪意のあるソフトウェア。

RASCI マトリックス

責任、説明責任、相談、情報 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

読み取り専用に使用されるデータベースのコピー。クエリをリードレプリカにルーティングして、プライマリデータベースへの負荷を軽減できます。

再設計

「7 Rs」を参照してください。

目標復旧時点 (RPO)

最後のデータリカバリポイントからの最大許容時間です。これにより、最後の回復時点からサービスが中断されるまでの間に許容できるデータ損失の程度が決まります。

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的エリア内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、耐障害性を提供するために、他の とは独立しています。詳細については、AWS リージョン「アカウントで使用できる を指定する」を参照してください。

回帰

数値を予測する機械学習手法。例えば、「この家はどれくらいの値段で売れるでしょうか?」という問題を解決するために、機械学習モデルは、線形回帰モデルを使用して、この家に関する既知の事実 (平方フィートなど) に基づいて家の販売価格を予測できます。

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

プラットフォーム変更

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または回復するアプリケーションの機能。高可用性とディザスタリカバリは、 で回復性を計画する際の一般的な考慮事項です AWS クラウド。詳細については、AWS クラウド「レジリエンス」を参照してください。

リソースベースのポリシー

Amazon S3 バケット、エンドポイント、暗号化キーなどのリソースにアタッチされたポリシー。このタイプのポリシーは、アクセスが許可されているプリンシパル、サポートされているアクション、その他の満たすべき条件を指定します。

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

移行活動とクラウド運用に関わるすべての関係者の役割と責任を定義したマトリックス。マトリックスの名前は、マトリックスで定義されている責任の種類、すなわち責任 (R) 、説明責任 (A) 、協議 (C) 、情報提供 (I) に由来します。サポート (S) タイプはオプションです。サポートを含めると、そのマトリックスは RASCI マトリックスと呼ばれ、サポートを除外すると RACI マトリックスと呼ばれます。

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、Implementing security controls on AWSのResponsive controlsを参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

取得拡張生成 (RAG)

LLM がレスポンスを生成する前にトレーニングデータソースの外部にある信頼できるデータソースを参照する生成 AI テクノロジー。たとえば、RAG モデルは、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行する場合があります。詳細については、「RAG とは」を参照してください。

ローテーション

攻撃者が認証情報にアクセスすることをより困難にするために、シークレットを定期的に更新するプロセス。

行と列のアクセス制御 (RCAC)

アクセスルールが定義された、基本的で柔軟な SQL 表現の使用。RCAC は行権限と列マスクで構成されています。

RPO

「目標復旧時点」を参照してください。

RTO

目標復旧時間を参照してください。

ランブック

特定のタスクを実行するために必要な手動または自動化された一連の手順。これらは通常、エラー率の高い反復操作や手順を合理化するために構築されています。

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能を使用すると、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、 AWS Management Console にログインしたり AWS API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントのSAML 2.0 ベースのフェデレーションについてを参照してください。

SCADA

「監視コントロールとデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存する AWS Secrets Managerパスワードやユーザー認証情報などの機密情報または制限付き情報。シークレット値とそのメタデータで構成されます。シークレット値は、バイナリ、1 つの文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

設計によるセキュリティ

開発プロセス全体でセキュリティを考慮するシステムエンジニアリングアプローチ。

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、予防的、検出的、応答的、プロアクティブの 4 つの主なタイプがあります。

セキュリティ強化

アタックサーフェスを狭めて攻撃への耐性を高めるプロセス。このプロセスには、不要になったリソースの削除、最小特権を付与するセキュリティのベストプラクティスの実装、設定ファイル内の不要な機能の無効化、といったアクションが含まれています。

Security Information and Event Management (SIEM) システム

セキュリティ情報管理 (SIM) とセキュリティイベント管理 (SEM) のシステムを組み合わせたツールとサービス。SIEM システムは、サーバー、ネットワーク、デバイス、その他ソースからデータを収集、モニタリング、分析して、脅威やセキュリティ違反を検出し、アラートを発信します。

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修復するように設計された、事前定義されたプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動応答アクションの例としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先で、それ AWS のサービス を受け取る によるデータの暗号化。

サービスコントロールポリシー (SCP)

AWS Organizationsの組織内の、すべてのアカウントのアクセス許可を一元的に管理するポリシー。SCP は、管理者がユーザーまたはロールに委任するアクションに、ガードレールを定義したり、アクションの制限を設定したりします。SCP は、許可リストまたは拒否リストとして、許可または禁止するサービスやアクションを指定する際に使用できます。詳細については、 AWS Organizations ドキュメントの「サービスコントロールポリシー」を参照してください。

サービスエンドポイント

のエントリポイントの URL AWS のサービス。ターゲットサービスにプログラムで接続するには、エンドポイントを使用します。詳細については、AWS 全般のリファレンスの「AWS のサービス エンドポイント」を参照してください。

サービスレベルアグリーメント (SLA)

サービスのアップタイムやパフォーマンスなど、IT チームがお客様に提供すると約束したものを明示した合意書。

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

サービスレベルのインジケータによって測定される、サービスの状態を表すターゲットメトリクス。

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、お客様はクラウドのセキュリティを担当します。詳細については、責任共有モデルを参照してください。

SIEM

セキュリティ情報とイベント管理システムを参照してください。

単一障害点 (SPOF)

システムを中断する可能性のあるアプリケーションの 1 つの重要なコンポーネントの障害。

SLA

「サービスレベルの契約」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、『』の「アプリケーションをモダナイズするための段階的アプローチ AWS クラウド」を参照してください。

SPOF

単一障害点を参照してください。

スタースキーマ

1 つの大きなファクトテーブルを使用してトランザクションデータまたは測定データを保存し、1 つ以上の小さなディメンションテーブルを使用してデータ属性を保存するデータベース組織構造。この構造は、データウェアハウスまたはビジネスインテリジェンスの目的で使用するように設計されています。

strangler fig パターン

レガシーシステムが廃止されるまで、システム機能を段階的に書き換えて置き換えることにより、モノリシックシステムをモダナイズするアプローチ。このパターンは、宿主の樹木から根を成長させ、最終的にその宿主を包み込み、宿主に取って代わるイチジクのつるを例えています。そのパターンは、モノリシックシステムを書き換えるときのリスクを管理する方法として Martin Fowler により提唱されました。このパターンの適用方法の例については、コンテナと Amazon API Gateway を使用して、従来の Microsoft ASP.NET (ASMX) ウェブサービスを段階的にモダナイズを参照してください。

サブネット

VPC 内の IP アドレスの範囲。サブネットは、1 つのアベイラビリティーゾーンに存在する必要があります。

監視コントロールとデータ収集 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと本番稼働をモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーとのやり取りをシミュレートして潜在的な問題を検出したり、パフォーマンスをモニタリングしたりする方法でシステムをテストします。Amazon CloudWatch Synthetics を使用してこれらのテストを作成できます。

システムプロンプト

LLM にコンテキスト、指示、またはガイドラインを提供して動作を指示する手法。システムプロンプトは、コンテキストを設定し、ユーザーとのやり取りのルールを確立するのに役立ちます。

T

tags

AWS リソースを整理するためのメタデータとして機能するキーと値のペア。タグは、リソースの管理、識別、整理、検索、フィルタリングに役立ちます。詳細については、「AWS リソースのタグ付け」を参照してください。

ターゲット変数

監督された機械学習でお客様が予測しようとしている値。これは、結果変数 のことも指します。例えば、製造設定では、ターゲット変数が製品の欠陥である可能性があります。

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要のある一般的なタスクのリストが含まれています。各一般的なタスクには、推定所要時間、所有者、進捗状況が含まれています。

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパターンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

VPC とオンプレミスネットワークを相互接続するために使用できる、ネットワークの中継ハブ。詳細については、 AWS Transit Gateway ドキュメントの「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

デベロッパーが機能ブランチで機能をローカルにビルドしてテストし、その変更をメインブランチにマージするアプローチ。メインブランチはその後、開発環境、本番前環境、本番環境に合わせて順次構築されます。

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「Using AWS Organizations with other AWS services AWS Organizations 」を参照してください。

チューニング

機械学習モデルの精度を向上させるために、お客様のトレーニングプロセスの側面を変更する。例えば、お客様が機械学習モデルをトレーニングするには、ラベル付けセットを生成し、ラベルを追加します。これらのステップを、異なる設定で複数回繰り返して、モデルを最適化します。

ツーピザチーム

2 枚のピザで養うことができるくらい小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。詳細については、深層学習システムにおける不確実性の定量化 ガイドを参照してください。

未分化なタスク

ヘビーリフティングとも呼ばれ、アプリケーションの作成と運用には必要だが、エンドユーザーに直接的な価値をもたらさなかったり、競争上の優位性をもたらしたりしない作業です。未分化なタスクの例としては、調達、メンテナンス、キャパシティプランニングなどがあります。

上位環境

???「環境」を参照してください。

V

バキューミング

ストレージを再利用してパフォーマンスを向上させるために、増分更新後にクリーンアップを行うデータベースのメンテナンス操作。

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

プライベート IP アドレスを使用してトラフィックをルーティングできる、2 つの VPC 間の接続。詳細については、Amazon VPC ドキュメントの「VPC ピア機能とは」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

頻繁にアクセスされる最新の関連データを含むバッファキャッシュ。データベースインスタンスはバッファキャッシュから、メインメモリまたはディスクからよりも短い時間で読み取りを行うことができます。

ウォームデータ

アクセス頻度の低いデータ。この種類のデータをクエリする場合、通常は適度に遅いクエリでも問題ありません。

ウィンドウ関数

現在のレコードに関連する行のグループに対して計算を実行する SQL 関数。ウィンドウ関数は、移動平均の計算や、現在の行の相対位置に基づく行の値へのアクセスなどのタスクの処理に役立ちます。

ワークロード

ビジネス価値をもたらすリソースとコード (顧客向けアプリケーションやバックエンドプロセスなど) の総称。

ワークストリーム

特定のタスクセットを担当する移行プロジェクト内の機能グループ。各ワークストリームは独立していますが、プロジェクト内の他のワークストリームをサポートしています。たとえば、ポートフォリオワークストリームは、アプリケーションの優先順位付け、ウェーブ計画、および移行メタデータの収集を担当します。ポートフォリオワークストリームは、これらの設備を移行ワークストリームで実現し、サーバーとアプリケーションを移行します。

WORM

「Write Once」、「Read Many」を参照してください。

WQF

AWS 「ワークロード認定フレームワーク」を参照してください。

write once, read many (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。承認されたユーザーは、必要な回数だけデータを読み取ることができますが、変更することはできません。このデータストレージインフラストラクチャはイミュータブルと見なされます。

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

実稼働システムにおける未解決の欠陥または脆弱性。脅威アクターは、このような脆弱性を利用してシステムを攻撃する可能性があります。開発者は、よく攻撃の結果で脆弱性に気付きます。

ゼロショットプロンプト

LLM にタスクを実行する手順を提供しますが、タスクのガイドに役立つ例 (ショット) はありません。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「数ショットプロンプト」も参照してください。

ゾンビアプリケーション

平均 CPU およびメモリ使用率が 5% 未満のアプリケーション。移行プロジェクトでは、これらのアプリケーションを廃止するのが一般的です。

翻訳は機械翻訳により提供されています。提供された翻訳内容と英語版の間で齟齬、不一致または矛盾がある場合、英語版が優先します。