のBackup とリカバリのアプローチ AWS

AWS 規範ガイダンス

AWS 規範ガイダンス: のBackup とリカバリのアプローチ AWS

Table of Contents

AWS におけるバックアップとリカバリーのアプローチ

クーラム・ニザミ、Amazon Web Services（AWS）

2023 年 4 月（ドキュメント履歴）

このガイドでは、オンプレミス、クラウドネイティブ、ハイブリッドの各アーキテクチャにおいて、Amazon Web Services（AWS）のサービスを利用したバックアップとリカバリの実装方法について説明します。これらのアプローチは、復旧時間目標（RTO）、復旧時点目標（RPO）、およびコンプライアンス要件を満たすために、低コスト、高い拡張性、より高い耐久性を提供します。

このガイドは、企業の IT 環境やクラウド環境におけるデータの保護を担当するテクニカルリーダーを対象としています。

このガイドでは、さまざまなバックアップ・アーキテクチャ（クラウドネイティブ・アプリケーション、ハイブリッド環境、オンプレミス環境）を取り上げています。また、アーキテクチャの不変コンポーネント向けのスケーラブルで信頼性の高いデータ保護ソリューションを構築するために使用できる関連Amazon Web Services（AWS）サービスについても説明します。

もう 1 つのアプローチは、ワークロードを近代化してイミュータブル・アーキテクチャーを使用し、コンポーネントのバックアップとリカバリーの必要性を減らすことである。イミュータブル・アーキテクチャーを実装し、バックアップとリカバリーの必要性を減らすために、以下のような多くのサービスを提供している：

- AWS Lambda によるサーバーレス
- Amazon Elastic Container Service（Amazon ECS）、Amazon Elastic Kubernetes Service（Amazon EKS）、および AWS Fargate によるコンテナ。
- Amazon Elastic Compute Cloud（Amazon EC2）とAmazon Machine Images（AMI）

企業データの増加が加速するにつれて、それを保護する作業はますます困難になっています。バックアップ手法の耐久性とスケーラビリティに関する疑問はよく出てきます。たとえば、クラウドはバックアップと復元のニーズを満たすのにどのように役立つのかという質問です。

このガイドには以下のトピックが含まれている：

- AWS データ保護のためのサービスの選択
- バックアップとリカバリソリューションの設計
- AWS Backup を使ったバックアップとリカバリー

- Amazon S3 と Amazon S3 Glacier を使用したバックアップとリカバリ
- EBS ボリュームを使用した Amazon EC2 のバックアップとリカバリ
- オンプレミスのインフラから AWS へのバックアップとリカバリ
- AWS からデータセンターへのアプリケーションのバックアップとリカバリ
- クラウドネイティブ AWS サービスのバックアップとリカバリ
- ハイブリッドアーキテクチャのバックアップと復旧
- AWSによる ディザスタリカバリ
- バックアップをクリーンアップする

なぜ AWS をデータ保護プラットフォームとして使いますか？

AWS は、安全で、高性能で、柔軟性があり、費用を節約でき、使いやすいクラウドコンピューティングプラットフォームです。AWS は、スケーラブルなバックアップとリカバリ・ソリューションを作成、実装、管理するために必要な未分化の重労働を引き受けます。

データ保護戦略の一環として AWS を利用することには多くの利点がある：

- 耐久性： Amazon Simple Storage Service（Amazon S3）、Amazon S3 Glacier、S3 Glacier Deep Archive は、99.9999999 パーセント（11 ナイン）の耐久性を目指して設計されています。両プラットフォームとも、少なくとも3つの地理的に分散したアベイラビリティ・ゾーンにまたがるオブジェクト・レプリケーションにより、データの信頼性の高いバックアップを提供します。多くの AWS サービスは、ストレージとエクスポート/インポート操作に Amazon S3 を使用しています。例えば、Amazon Elastic Block Store（Amazon EBS）はスナップショット・ストレージに Amazon S3 を使用しています。
- セキュリティ：AWS は、転送中および静止中のアクセス制御とデータ暗号化のために多くのオプションを提供します。
- グローバルインフラストラクチャ：AWS サービスは世界中で利用できるため、コンプライアンスやワークロードの要件を満たすデータをリージョンにバックアップして保存できます。
- コンプライアンス：AWS インフラストラクチャは以下の基準に準拠していることが認定されているため、バックアップソリューションを既存のコンプライアンス体制に簡単に組み込むことができます。
  - Service Organization Controls (SOC)
  - 監査業務基準書（SSAE）16
  - 国際標準化機構（ISO）27001

  - Payment Card Industry Data Security Standard (PCI DSS)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - セクション 1
  - Federal Risk and Authorization Management Program (FedRAMP)
- スケーラビリティ：AWS を使えば、容量を心配する必要はありません。ニーズの変化に応じて、管理上のオーバーヘッドなしに、使用量を増減することができます。
- 総所有コスト（TCO）の削減：AWS の事業規模は、サービス・コストの削減を促進し、AWS サービスの TCO 削減に貢献します。AWS は、これらのコスト削減を価格低下を通じて顧客に還元されます。
- 従量課金制：AWS サービスを必要なときに必要な期間だけ購入します。AWS の価格設定には、初期費用、解約違約金、長期契約がありません。

ターゲットを絞ったビジネス成果

このガイドの目的は、次のようなバックアップとリカバリのアプローチをサポートするために使用できる AWS サービスの概要を説明することです。

- オンプレミスのアーキテクチャ
- クラウドネイティブアーキテクチャ
- ハイブリッドアーキテクチャ
- ネイティブサービス
- ディザスタリカバリ

ベストプラクティスと考慮事項がサービスの概要とともに説明されています。また、このガイドでは、バックアップとリカバリについて、あるアプローチと別のアプローチとのトレードオフについても説明します。

AWS データ保護のためのサービスの選択

AWS バックアップとリカバリのアプローチの一部として使用できる多数のストレージサービスと補完サービスを提供します。これらのサービスは、クラウドネイティブアーキテクチャとハイブリッドアーキテクチャの両方をサポートできます。異なるサービスは、異なるユースケースに対してより効果的です。

- Amazon S3 および Amazon S3 Glacier と S3 Glacier Deep Archive は、ハイブリッドユースケースとクラウドネイティブユースケースの両方に適しています。これらのサービスは、個々のファイル、サーバー、またはデータセンター全体のバックアップに適した、優れた耐久性を持つ汎用オブジェクトストレージソリューションを提供します。
- AWS Storage Gateway はハイブリッドユースケースに最適です。Storage Gateway は Amazon S3 の機能を活用して、一般的なオンプレミスのバックアップとストレージの要件に対応します。アプリケーションは、以下の標準ストレージプロトコルを使用して、仮想マシン (VM) またはハードウェアゲートウェイアプライアンスを介してサービスに接続します。
  - ネットワークファイルシステム (NFS)
  - サーバーメッセージブロック (SMB)
  - Internet Small Computer System Interface (iSCSI)

  ゲートウェイは、こうした一般的なオンプレミスプロトコルを、 AWS 次のようなストレージサービスに橋渡しします。
  - Amazon S3
  - Amazon S3 Glacier
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway を使用すると、ファイル、ボリューム、スナップショット、仮想テープ用の柔軟で高性能なストレージを簡単に提供できます。 AWS
- AWS Backupは、複数のサービスにわたるデータのバックアップを一元化および自動化するためのフルマネージド型バックアップサービスです。 AWS AWS Backupを使用すると、バックアップポリシーを一元的に設定し、次のような AWS リソースのバックアップアクティビティを監視できます：
  - EBS ボリューム
  - EC2 インスタンス (Windows アプリケーションを含む)

- Amazon RDS および Amazon Aurora データベース
- DynamoDB テーブル
- Amazon Neptune データベース
- Amazon DocumentDB (MongoDB 互換) データベース
- Amazon EFS ファイルシステム
- Amazon FSx for Lustre ファイルシステムおよび Amazon FSx for Windows File Server ファイルシステム
- オンプレミスおよび VMware Cloud on 内の VMware ワークロード AWS
- Storage Gateway ボリューム

  AWS Backup の費用は、1 か月間に使用、復元、転送するストレージに基づきます。詳細については、「AWS Backup 料金」を参照してください。

- AWS Elastic Disaster Recoveryターゲットアカウントと優先リージョンの低コストのステージングエリアにマシンを継続的に複製します。 AWS Elastic ディザスタリカバリは DR とクロスリージョン premises-to-cloud DR の両方に使用できます。
- AWS Config AWS AWS アカウント内のリソース設定の詳細が表示されます。これには、リソースの相互関係や、過去にどのように構成されていたかが含まれます。このビューでは、リソースの設定と関係が時間の経過とともにどのように変化したかを確認できます。

  AWS Config リソースの設定記録を有効にすると、 AWS リソースの関係の履歴が長期にわたって保持されます。これにより、最大 7 AWS 年間のリソース関係 (削除されたリソースを含む) を特定して追跡できます。たとえば、Amazon EBS スナップショットボリュームと、そのボリュームがアタッチされた EC2 AWS Config インスタンスとの関係を追跡できます。
- AWS Lambda は、ワークロードのバックアップとリカバリの手順をプログラムで定義して自動化するために使用できます。 AWS SDK AWS を使用してサービスやそのデータを操作できます。Amazon CloudWatch イベントを使用して Lambda 関数を定期的に実行することもできます。

AWS サービスはバックアップと復元のための特定の機能を提供します。 AWS 使用している各サービスについて、 AWS マニュアルを参照して、そのサービスが提供するバックアップ、復元、およびデータ保護機能を確認してください。 AWS Command Line Interface (AWS CLI)、 AWS SDK、API オペレーションを使用して、 AWS データのバックアップとリカバリのサービス固有の機能を自動化できます。

バックアップとリカバリソリューションの設計

データのバックアップと復元に関する包括的な戦略を立てるときは、まず、起こり得る障害や災害の状況と、それらがビジネスに及ぼす潜在的な影響を特定する必要があります。業界によっては、データセキュリティ、プライバシー、記録保持に関する規制要件を考慮する必要があります。

Backup とリカバリのプロセスには、ワークロードとそれをサポートするビジネスプロセスの目標復旧時間 (RTO) と目標復旧時点 (RPO) を満たすために、以下のような適切なレベルの詳細度を含める必要があります：

- ファイルレベルのリカバリ (アプリケーションの構成ファイルなど)
- アプリケーションデータレベルのリカバリ (MySQL 内の特定のデータベースなど)
- アプリケーションレベルのリカバリ (特定の Web サーバーアプリケーションバージョンなど)
- Amazon EC2 ボリュームレベルのリカバリ (EBS ボリュームなど)
- EC2 インスタンスレベルのリカバリ (EC2 インスタンスなど)
- マネージドサービスのリカバリ (DynamoDB テーブルなど)

ソリューションのすべてのリカバリ要件と、アーキテクチャ内のさまざまなコンポーネント間のデータ依存性を必ず考慮してください。復元プロセスを円滑に進めるには、アーキテクチャ内のさまざまなコンポーネント間でバックアップとリカバリを調整してください。

次のトピックでは、インフラストラクチャの構成に基づいたバックアップとリカバリのアプローチについて説明します。IT インフラストラクチャは、大きく分けてオンプレミス、ハイブリッド、またはクラウドネイティブに分類できます。

AWS Backup を使ったバックアップとリカバリー

AWS Backup は、AWS サービス全体のデータのバックアップを一元化し、自動化するフルマネージドバックアップサービスです。AWS Backup は、Amazon CloudWatch、AWS CloudTrail、AWS Identity and Access Management （ IAM ）、AWS Organizations、その他のサービスを統合するオーケストレーションレイヤーを提供します。この一元化された AWS クラウド・ネイティブ・ソリューションは、グローバルなバックアップ機能を提供し、ディザスタリカバリやコンプライアンス要件の達成を支援します。AWS Backup を使用すれば、バックアップポリシーを一元的に設定し、AWSリソースのバックアップアクティビティを監視できます。

AWS Backup は、AWS アカウントおよびリージョン全体で、AWS リソースの標準的なバックアッププランを実施するための理想的なソリューションです。AWS Backup は複数の AWS リソースタイプをサポートするため、まとめてバックアップする必要がある複数の AWS リソースを使用するワークロードのバックアップ戦略の維持と実施が容易になります。AWS Backup はまた、複数の AWS リソースを含むバックアップとリストア操作をまとめて監視することもできます。

コンプライアンスや監査要件がある場合は、「AWS Backup Audit Manager」 機能を使用して監査フレームワークやレポートを作成し、コンプライアンス要件をサポートすることができます。また、「AWS Backup Vault Lock」 機能は、AWS Backup のバックアップ保管庫に保存されたすべてのバックアップに対して、Write-Once, Read-Many （ WORM ）設定を強制することで、コンプライアンス要件をサポートします。

AWS Backup にとって重要な差別化要因は、組織へのサポートです。このサポートを使用すると、組織または組織単位レベルでバックアップポリシーを定義および管理し、関連する各 AWS アカウントおよびリージョンにそれらのポリシーを自動的に実装することができます。新しい AWS アカウントやリージョンをオンボーディングするときに、バックアッププランを個別に定義して管理する必要はありません。

AWS Backup は、タグを使用することで、組織全体のバックアップ・ポリシーの導入を容易にします。それぞれに固有の頻度と保存期間を設定した個別のバックアッププランを作成し、バックアップに含めるリソースを選択する固有のキーと値のペアタグを作成できます。

たとえば、毎日 05:00 UTC にバックアップを開始し、35 日間の保存ポリシーを定めた日次バックアッププランを作成できます。このバックアップ計画には、タグキーバックアップとタグ値デイリーを持つ、サポートされているすべての AWS リソースが、この計画に従ってバックアップされることを指定する「バックアップリソースの割り当て」 を含めることができます。さらに、毎月 1 日の 05:00 UTC から開始し、366 日間の保存ポリシーが適用される月次バックアッププランを作成することもできます。このバックアップ計画には、タグキーbackupとタグ値を持つ、サポートされてい

るすべての AWS リソースが、この計画に従って月別にバックアップされることを指定する、バックアップリソースの割り当てを含めることができます。

次に、タグポリシーと「required-tags」 AWS Config ルールを使って、AWS がサポートするすべてのリソースがこのタグキーとタグ値のいずれかを持つようにすることができます。このアプローチは、サポートされている AWS Backup リソースに対して、AWS で標準的なバックアップアプローチを一貫して実装し、維持するのに役立ちます。このアプローチを拡張して、Recovery Point Objective（RPO）の要件が異なるアプリケーションやアーキテクチャレイヤーのバックアップを標準化できます。

バックアップ保管庫を保護するための対策を講じることをおすすめします。たとえば、バックアップ保管庫が削除されたり、意図しない AWS アカウントと共有されたりしないように、Organizations サービス・コントロール・ポリシー（SCP）を実装することができます。詳細とその他の重要なセキュリティ上の考慮事項については、「AWS におけるバックアップの安全性を確保するためのセキュリティのベストプラクティスTop 10」のブログ記事を参照してください。

AWS Backup は、複数の AWS リソースをサポートし、一括して対処することができるため、AWS のディザスタリカバリ（DR）計画の実施を簡素化することができます。例えば、AWS Backup がサポートするほとんどの AWS リソースタイプに対して、「クロスリージョン」「クロスアカウント」バックアップを実装することができます。クロスアカウント・バックアップは、コピーが別のアカウントで利用できるため、バックアップの安全性が向上します。クロスリージョンバックアップでは、バックアップが複数のリージョンで利用できるため、可用性が向上します。サポートされる AWS リソースタイプの詳細については、「リソース別の機能利用可能性」の表を参照してください。

AWS Backup オープンソース・ソリューションによるバックアップとリカバリー」の例を参考に、あなたの AWS Organizations 組織のバックアップ管理に IaC（Infrastructure as Code）と CI/CD（Continuous Integration and Continuous Delivery）アプローチを導入することができます。このソリューションには、リストアされた AWS リソースに AWS タグを自動的に再適用したり、セカンダリ・バックアップ保管庫をDR目的で別のアカウントとリージョンに確立したりするカスタム機能が含まれています。

Amazon S3 と Amazon S3 Glacier を使用したバックアップとリカバリ

Amazon S3 と Amazon S3 Glacier は、オンプレミス、ハイブリッド、クラウドネイティブアーキテクチャでの使用に最適なストレージサービスです。これらのサービスは、スケーラブルな容量を備え、バックアップデータセットが増大してもボリュームやメディアの管理を必要としない、耐久性に優れた低コストのストレージプラットフォームを提供します。 pay-for-what-you-use モデルと GB/月あたりの低コストにより、これらのサービスは幅広いデータ保護ユースケースに適しています。

> **Note**
>
> 一部のストレージクラスには、最低期間料金がかかります。詳細については、「Amazon S3 の料金」を参照し、ウェブページ検索を使用して を検索しますduration。

トピック

- Amazon S3
- Amazon S3 Glacier
- Amazon S3 と Amazon S3 Glacier にあるバックアップデータの保護

Amazon S3

Amazon S3 を使えば、いつでも、どんな量のデータでも保存し、取り出すことができます。アプリケーションデータやファイルレベルのバックアップ復元処理のための耐久性のあるストアとして、Amazon S3 を使用することができます。例えば、 AWS CLI または SDKs を使用して、バックアップスクリプトを使用してデータベースインスタンスから Amazon S3 にデータベースバックアップをコピーできます。

AWS のサービスは、次の例のように、耐久性と信頼性に優れたストレージとして Amazon S3 を使用します。

- Amazon EC2 は、Amazon S3 を使用して EBS ボリュームと EC2 インスタンスストアの Amazon EBS スナップショットを格納します。
- Storage Gateway は Amazon S3 と統合され、Amazon S3 ベースのファイル共有、ボリューム、テープライブラリをオンプレミス環境に提供します。

- Amazon RDS はデータベースのスナップショットに Amazon S3 を使用します。

多くのサードパーティのバックアップソリューションも Amazon S3 を使用します。例えば、Arcserve Unified Data Protection は Amazon S3 をサポートし、オンプレミスおよびクラウドネイティブサーバーの耐久性のあるバックアップを実現しています。

これらのサービスの Amazon S3 統合機能を使えば、バックアップとリカバリーのアプローチを簡素化できます。同時に、Amazon S3 が提供する高い耐久性と可用性の恩恵を受けることができます。

Amazon S3 は、バケットと呼ばれるリソース内にオブジェクトとしてデータを保存します。必要な数のオブジェクトを保存できます。きめ細かなアクセスコントロールを使用して、バケット内のオブジェクトの書き込み、読み取り、削除を行えます。1 つのオブジェクトのサイズは最大 5 TB です。

Amazon S3 は、以下のクラスを含むさまざまなユースケース向けに設計されたストレージクラスを提供しています:

- S3 Standard は、頻繁にアクセスされるデータ (例えば、設定ファイル、計画外のバックアップ、毎日のバックアップ) の汎用ストレージ用です。
- S3 Standard-IA は、保存期間は長いもののアクセス頻度の低いデータ(例えば、月次バックアップなど) に使用します。IA は infrequent access (低頻度アクセス) の略です。

Amazon S3 は、ライフサイクルを通してデータを管理するために設定できるライフサイクルポリシーを提供しています。ポリシーが設定されると、アプリケーションを変更することなく、データは適切なストレージクラスに移行されます。詳細については、「Amazon S3 オブジェクトのライフサイクル管理」を参照してください。

バックアップにかかるコストを削減するには、以下の例のように、目標復旧時間 (RTO) と目標復旧時点 (RPO) に基づいて、階層化されたストレージクラスのアプローチを使用できます:

- S3 Standard を使用した過去 2 週間の毎日バックアップ
- S3 Standard-IA を使用した過去 3 か月間の週次バックアップ
- S3 Glacier Flexible Retrieval での過去 1 年間の四半期ごとのバックアップ
- S3 Glacier Deep Archive での過去 5 年間の年次バックアップ
- S3 Glacier Deep Archive から 5 年経過後にバックアップが削除されます

オブジェクトライフサイクル管理を使えば、バックアップの移行を自動化できます。

> **Note**
>
> 一部のストレージクラスには、最低期間料金がかかります。詳細については、「Amazon S3 の料金」を参照し、ウェブページ検索を使用して を検索しますduration。

バックアップとアーカイブ用の標準 S3 バケットの作成

S3 のライフサイクルポリシーを通じて、企業のバックアップと保持ポリシーを実装したバックアップとアーカイブ用の標準的な S3 バケットを作成することができます。コスト配分のタグ付けと AWS 請求レポートは、バケットレベルで割り当てられたタグに基づいています。コスト配分が重要な場合は、それに応じてコストを配分できるように、プロジェクトまたはビジネスユニットごとに個別のバックアップおよびアーカイブ S3 バケットを作成します。

バックアップスクリプトとアプリケーションは、作成したバックアップおよびアーカイブ S3 バケットを使用して、アプリケーションおよびワークロードデータの point-in-time スナップショットを保存できます。データ point-in-time スナップショットの整理に役立つ標準 S3 プレフィックスを作成できます。たとえば、1 時間ごとにバックアップを作成する場合は、`YYYY/MM/DD/HH/<WorkloadName>/<files...>` などのバックアッププレフィックスを使用することを検討します。これにより、 point-in-time バックアップを手動またはプログラムですばやく取得できます。

Amazon S3 バージョニングを使用してロールバック履歴を自動的に維持する

S3 オブジェクトのバージョニングを有効にすると、以前のバージョンに戻す機能など、オブジェクトの変更履歴を維持できます。これは、 point-in-time バックアップスケジュールよりも頻繁に変更される可能性のある設定ファイルやその他のオブジェクトに役立ちます。また、ファイルを個別に元に戻す必要がある場合にも役立ちます。

Amazon S3 を使用して、AMI 用にカスタマイズされた設定ファイルをバックアップおよびリカバリする

オブジェクトバージョニング機能を備えた Amazon S3 は、ワークロード設定とオプションファイルの記録システムになります。例えば、ISV によって維持される標準の AWS Marketplace Amazon EC2 イメージを使用できます。このイメージには、複数の構成ファイルで構成が管理されているソフトウェアが含まれている可能性があります。カスタマイズした設定ファイルは Amazon S3 で管理できます。インスタンスの起動時に、これらの設定ファイルをインスタンスユーザーデータの一部と

してインスタンスにコピーすることができます。この方法を適用すると、更新されたバージョンを使用するために AMI をカスタマイズして再作成する必要はありません。

カスタムバックアップおよび復元プロセスでの Amazon S3 の使用

Amazon S3 は、既存のカスタムバックアッププロセスに素早く統合できる汎用バックアップストアを提供します。 AWS CLI、 AWS SDKs 、および API オペレーションを使用して、Amazon S3 を使用するバックアップおよび復元スクリプトとプロセスを統合できます。例えば、毎晩データベースのエクスポートを行うデータベースバックアップスクリプトがあるとします。このスクリプトをカスタマイズして、夜間バックアップを Amazon S3 にコピーしてオフサイトに保存できます。この方法の概要については、「クラウドへのファイル一括アップロード」チュートリアルを参照してください。

個々の RPO に基づいて、さまざまなアプリケーションのデータをエクスポートおよびバックアップする場合にも同様のアプローチをとることができます。さらに、 AWS Systems Manager を使用して、マネージドインスタンスでバックアップスクリプトを実行できます。Systems Manager は、個々のバックアッププロセスに対して、自動化、アクセスコントロール、スケジューリング、ロギング、通知を提供します。

Amazon S3 Glacier

Amazon S3 Glacier は、データアーカイブとオンラインバックアップのための安全で耐久性のあるストレージを提供する、低コストのクラウドアーカイブストレージサービスです。コストを低く抑えるために、S3 Glacier は数ミリ秒から数時間までの 3 つのストレージクラスを提供しています。S3 Glacier Flexible Retrieval と S3 Glacier Deep Archive には、データの復元に必要な時間に応じて追加のオプションが用意されています。S3 Glacier を使用すると、オンプレミスのソリューションと比べて大幅に節約しながら、その量にかかわらず、確実に格納できます。S3 Glacier は、長期または無期限の保持要件があるバックアップデータの保存や、長期間のデータアーカイブに最適です。S3 Glacier は以下のストレージクラスを提供します:

- S3 Glacier Instant Retrieval は、四半期に 1 度必要になる可能性があり、素早く (ミリ秒単位で) 復元する必要があるデータをアーカイブします。
- S3 Glacier Flexible Retrieval は、年に 1～2 回、数時間以内に復元する必要があるデータをアーカイブします。
- S3 Glacier Deep Archive は、12 時間以内に復元する必要のある長期バックアップサイクルのデータをアーカイブします。

次の表は、アーカイブの取り出しオプションをまとめたものです。

ストレージクラス	迅速	Standard	大容量
S3 Glacier Instant Retrieval	該当しない	該当しない	該当しない
S3 Glacier Flexible Retrieval	1～5 分	3～5 時間	5～12 時間
S3 Glacier Deep Archive	利用不可	12 時間以内	48 時間以内

Amazon S3 を使えば、S3 バケットを作成する際に各オブジェクトにストレージクラスを設定することができます。オブジェクトを作成したら、そのオブジェクトを別のストレージクラスの新しいオブジェクトにコピーして、ストレージクラスを変更できます。または、指定したルールに基づいてオブジェクトのストレージクラスを自動的に変更するライフサイクル設定を有効にすることもできます。

バックアップおよび復元プロセスを自動化するには、、 AWS Management Console AWS CLI、AWS SDKs を使用して Amazon S3 Glacier および S3 Glacier Deep Archive にアクセスします。詳細については、Amazon S3 Glacier　を参照してください。

> **Note**
>
> S3 Glacier ストレージクラスには最低期間料金がかかります。詳細については、「Amazon S3 の料金」を参照し、ウェブページ検索を使用して を検索しますduration。

Amazon S3 Glacier への Amazon S3 ライフサイクルオブジェクト移行の使用と Amazon S3 Glacier アーカイブの管理との比較

Amazon S3 では、S3 オブジェクトを Amazon S3 Glacier ストレージクラスに簡単に移行できるため、バックアップのライフサイクルとコストを管理できます。ただし、オブジェクトのサイズや、アーキテクチャ内のさまざまなコンポーネントのオブジェクトのコレクションを復元する必要があるかどうかによっては、このプロセスを自分で管理したほうがよい場合もあります。

まとめて復元する必要のある小さなオブジェクトが多数ある場合は、以下のオプションがコストに及ぼす影響を検討します。

- ライフサイクルポリシーを使用して、オブジェクトを Amazon S3 Glacier に個別に自動移行する
- オブジェクトを 1 つのファイルに圧縮して Amazon S3 Glacier に保存する

Amazon S3 Glacier では、使用するストレージクラスに応じて、各オブジェクトに最低容量料金が設定されています。たとえば、S3 Glacier インスタント検索では、オブジェクトごとに 128 KB の最小容量料金が課金されます。 up-to-date 詳細については、パフォーマンスチャートを参照してください。

S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive にアーカイブする各オブジェクトに対して、Amazon S3 はオブジェクト名とその他のメタデータに 8 KB のストレージを使用します。Amazon S3 でこのメタデータを保存する目的は、ユーザーが Amazon S3 API を使用して、アーカイブされたオブジェクトのリアルタイムのリストを取得できるようにすることです。この追加のストレージに対しては、S3 Standard 料金が発生します。

Amazon S3 はまた、S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive ストレージクラスにアーカイブされる各オブジェクトのインデックスと関連メタデータ用に 32 KB のストレージを追加します。この追加データは、オブジェクトを特定して復元するのに必要です。この追加ストレージには、Amazon S3 Glacier または S3 Glacier Deep Archive の料金が課金されます。

オブジェクトを 1 つのファイルに圧縮することで、Amazon S3 Glacier が使用する追加ストレージを削減できるだけでなく、多数の小さなオブジェクトに対して最低容量料金が発生するのを回避できます。

もう 1 つの重要な考慮事項は、ライフサイクルポリシーがオブジェクトに個別に適用されることです。これは、オブジェクトのコレクションを特定の時点からまとめて復元しなければならない場合、バックアップの整合性に影響を与える可能性があります。オブジェクト間で同じ有効期限とライフサイクルの移行時間を設定していても、すべてのオブジェクトが同時に移行される保証はありません。ライフサイクルルールが満たされてから、ルールのアクションが完了するまでに遅延が生じる場合があります。詳細については、「AWS Knowledge Center」を参照してください。

最後に、ライフサイクルポリシーのアーカイブを使用する場合と、作成したアーカイブを別途管理する場合の復元作業について検討します。Amazon S3 Glacier から各オブジェクトの復元を個別に開始する必要があります。このため、多数のオブジェクトのまとめての復元を開始するには、スクリプトを記述するか、ツールを使用する必要があります。S3 Batch オペレーションを使用して個々のリクエストの数を減らすことができますし、Amazon S3 コンソールを使用することもできます。

Amazon S3 と Amazon S3 Glacier にあるバックアップデータの保護

データセキュリティは共通の懸念であり、セキュリティを非常に重視 AWS しています。セキュリティはすべての AWS サービスの基盤です。Amazon S3 などのストレージサービスは、保存中と転送中の両方でアクセス制御と暗号化を行う強力な機能を備えています。すべての Amazon S3 および Amazon S3 Glacier API エンドポイントは、転送中のデータを暗号化するための SSL/TLS (Secure Sockets Layer/Transport Layer Security) をサポートしています。Amazon S3 Glacier は、保管中のすべてのデータをデフォルトで暗号化します。Amazon S3 では、次のようにして保存中のオブジェクトのサーバー側の暗号化を選択できます。

- Amazon S3 が管理する暗号化キーによるサーバー側の暗号化の使用
- に保存されている AWS Key Management Service （ AWS KMS) キーによるサーバー側の暗号化 AWS KMSの使用

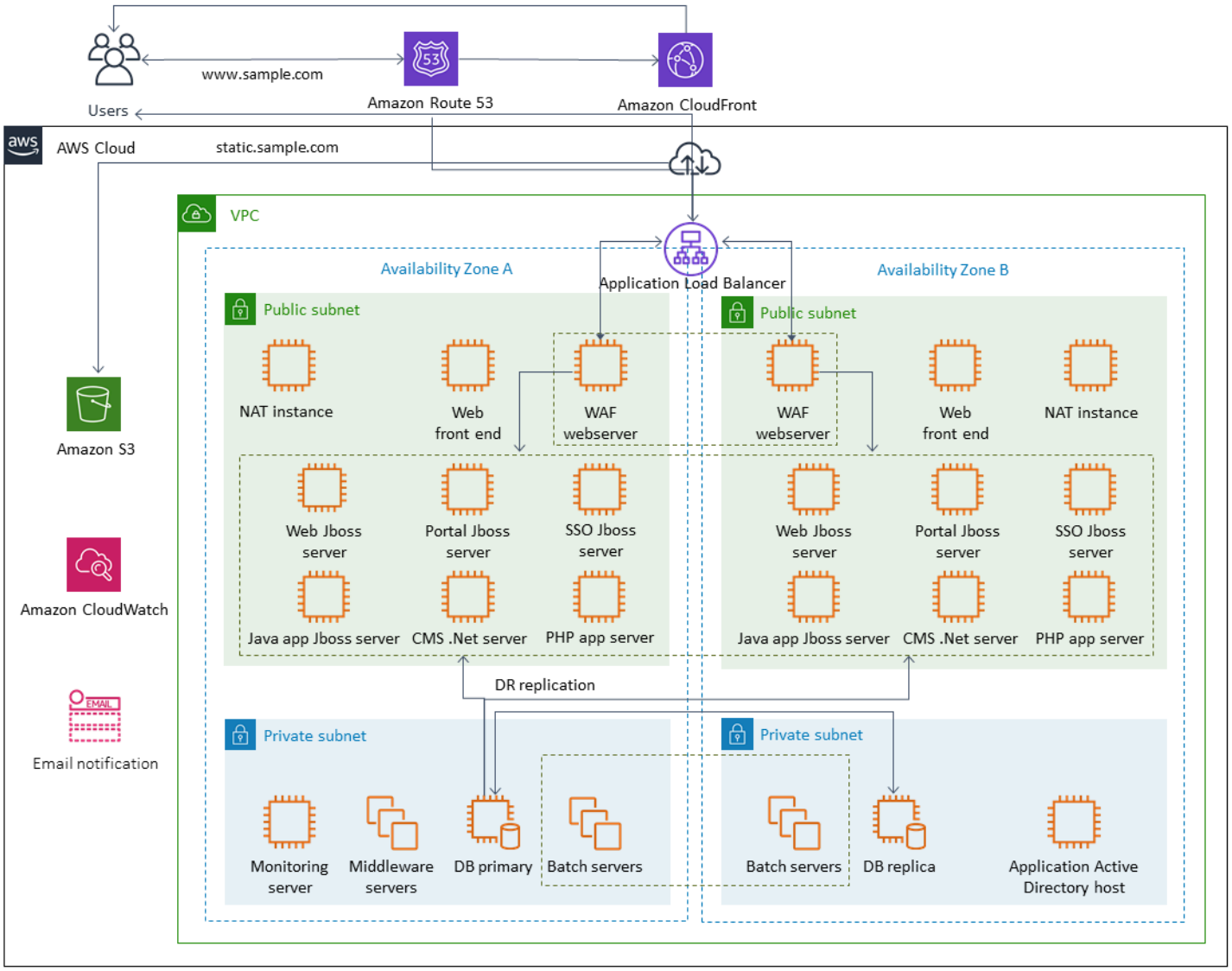
または、 にアップロードする前にデータを暗号化することもできます AWS。詳細については、「クライアント側暗号化」のドキュメントを参照してください。

AWS Identity and Access Management (IAM) を使用して、S3 オブジェクトへのアクセスを制御できます。IAM では、S3 バケット内の個々のオブジェクトと特定のプレフィックスパスに対する権限を制御できます。AWS CloudTrailによるオブジェクトレベルロギングを使えば、S3 オブジェクトへのアクセスを監査できます。

EBS ボリュームを使用した Amazon EC2 のバックアップとリカバリ

AWS には、Amazon EC2 インスタンスをバックアップする複数の方法が用意されています。このセクションでは、Amazon Elastic Block Store (Amazon EBS) ボリュームやインスタンスストアボリュームをストレージとしてバックアップする際のさまざまな側面について説明します。のバックアップが要件を満た AWS している場合は、 でバックアップを管理する最初の選択肢 AWS Backup として を検討してください。バックアップは、それが意図された機能に復元できる場合にのみ有効であることを忘れてはなりません。リストアとリカバリの機能を定期的にテストして、これを確認する必要があります。

次の図のソリューションアーキテクチャは、Amazon EC2 に基づくアーキテクチャの大部分 AWS を持つ に完全に存在するワークロード環境を示しています。次の図が示すように、シナリオにはウェブサーバー、アプリケーションサーバー、モニタリングサーバー、データベース、Active Directory が含まれます。



AWS は、このアーキテクチャで表される多くの Amazon EC2 サーバーに多くの完全に機能するサービスを提供し、インスタンスとストレージの作成、プロビジョニング、バックアップ、復元、最適化という差別化されていない作業を実行します。複雑さと管理を減らすために、これらのサービスがアーキテクチャに適しているかどうかを検討してください。 は、Amazon EC2 ベースのアーキテクチャの可用性を向上させるためのサービス AWS も提供します。特に、Amazon EC2 Auto Scaling と Elastic Load Balancing は、Amazon EC2 でのワークロードを補完するものとして検討してください。これらのサービスを使用すると、アーキテクチャの可用性と耐障害性が向上し、障害が発生したインスタンスをユーザーへの影響を最小限に抑えながら復元できるようになります。

EC2 インスタンスは主に、永続ストレージとして Amazon EBS ボリュームを使用します。Amazon EBS には、このセクションで詳細に説明されているバックアップとリカバリの機能が多数用意されています。

トピック

スナップショットと AMI による Amazon EC2 のバックアップとリカバリ

Amazon Machine Image (AMI) を使って EC2 インスタンスのフルバックアップを作成する必要があるのか、それとも個々のボリュームのスナップショットを取る必要があるのかを検討します。

バックアップには AMI または Amazon EBS スナップショットを使用する

AMI には以下のものが含まれています。

- 1 つ以上のスナップショット。I nstance-store-backed AMIs には、インスタンスのルートボリューム (オペレーティングシステム、アプリケーションサーバー、アプリケーションなど) のテンプレートが含まれています。
- AMI を使用してインスタンスを起動できる AWS アカウントを制御する起動許可。
- インスタンスの起動時にインスタンスにアタッチするボリュームを指定するブロックデバイスマッピング

AMI を使用して、事前設定されたソフトウェアとデータを使用して新しいインスタンスを起動できます。AMI は、ベースラインを設定したいときに作成できます。ベースラインとは、より多くのインスタンスを起動するための再利用可能な設定です。既存の EC2 インスタンスの AMI を作成すると、インスタンスにアタッチされているすべてのボリュームのスナップショットが取得されます。スナップショットにはデバイスマッピングが含まれます。

スナップショットを使用して新しいインスタンスを起動することはできませんが、既存のインスタンス上のボリュームを置き換えるために使用できます。データの破損やボリューム障害が発生した場合は、撮影したスナップショットからボリュームを作成し、古いボリュームを置き換えることができます。スナップショットを使用して新しいボリュームをプロビジョニングし、新しいインスタンスの起動時にアタッチすることもできます。

で AWS 維持および公開されているプラットフォームとアプリケーションの AMIs を使用している場合は AWS Marketplace、データ用に個別のボリュームを維持することを検討してください。データ

ボリュームは、オペレーティングシステムやアプリケーションボリュームとは別のスナップショットとしてバックアップできます。次に、 によって、 AWS または から公開された新しく更新された AMIs で、データボリュームのスナップショットを使用します AWS Marketplace。このアプローチでは、設定情報を含むすべてのカスタムデータを、新しく公開した AMI にバックアップして復元するための綿密なテストと計画が必要です。

復元プロセスは、AMI バックアップとスナップショットバックアップのどちらを選択したかに影響されます。インスタンスのバックアップとして機能する AMI を作成する場合、復元プロセスの一環として AMI から EC2 インスタンスを起動する必要があります。衝突の可能性を避けるため、既存のインスタンスをシャットダウンする必要がある場合もあります。衝突の可能性がある例としては、ドメインに参加している Windows インスタンスのセキュリティ識別子 (SID) があります。スナップショットの復元プロセスでは、既存のボリュームをデタッチし、新しく復元したボリュームをアタッチする必要がある場合があります。または、アプリケーションが新しくアタッチされたボリュームを参照するように設定を変更する必要がある場合もあります。

AWS Backup は、インスタンスレベルのバックアップを AMIsし、ボリュームレベルのバックアップを個別のスナップショットとしてサポートします。

- インスタンス上のすべての EBS ボリュームの完全なバックアップを行うには、Linux または Windows で実行されている EC2 インスタンスの AMI を作成します。 https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/Creating_EBSbacked_WinAMI.htmlロールバックする場合は、インスタンス起動ウィザードを使用してインスタンスを作成します。インスタンス起動ウィザードで、AMI AMIsを選択します。
- 個々のボリュームをバックアップするには、スナップショット を作成します。スナップショットを復元するには、「スナップショットからボリュームを作成する」を参照してください。 AWS Management Console または AWS Command Line Interface () を使用できますAWS CLI。

インスタンス AMI のコストは、インスタンス上のすべてのボリュームのストレージであり、メタデータではありません。EBS スナップショットのコストは、個々のボリュームのストレージです。ボリュームストレージのコストの詳細については、「Amazon EBS 料金表」ページを参照してください。

サーバーボリューム

EBS ボリュームは、Amazon EC2 の主要な永続ストレージオプションです。このブロックストレージは、データベースなどの構造化データや、ボリューム上のファイルシステム内のファイルなどの非構造化データに使用できます。

EBS ボリュームは特定のアベイラビリティーゾーンに置かれます。ボリュームは複数のサーバーにレプリケートされ、単一のコンポーネントの障害によるデータの損失を防ぎます。故障とは、ボリュームのサイズと性能に応じて、ボリュームの完全または部分的な喪失を指します。

EBS ボリュームは、年間故障率 (AFR) が 0.1 ~ 0.2% になるように設計されています。これにより、EBS ボリュームの信頼性が、約 4% の AFR で故障する一般的なコモディティディスクドライブに比べて EBS ボリュームの信頼性が 20 倍に高まります。例えば、1,000 個の EBS ボリュームを 1 年間稼動させる場合、1 個か 2 個のボリュームに障害が発生することを想定しておく必要があります。

Amazon EBS は、データの point-in-time バックアップを作成するためのスナップショット機能もサポートしています。すべての EBS ボリュームタイプは、耐久性のあるスナップショット機能を提供し、99.999% の可用性を実現するように設計されています。詳細については、「Amazon Compute サービスレベルアグリーメント」を参照してください。

Amazon EBS は、あらゆる EBS ボリュームのスナップショット (バックアップ) を作成する機能を提供しています。スナップショットは、EBS ボリュームのバックアップを作成するための基本機能です。スナップショットは EBS ボリュームのコピーを取り、Amazon S3 に置き、複数のアベイラビリティーゾーンに冗長的に保存されます。最初のスナップショットはボリュームの完全コピーであり、進行中のスナップショットはブロックレベルの増分変更のみを保存します。Amazon EBS スナップショットの作成方法の詳細については、「Amazon EC2 のドキュメント」を参照してください。

スナップショットを取得したのと同じリージョンで、Amazon EC2コンソールからスナップショットに関連付けられたリストア操作、スナップショットの削除、タグなどのスナップショットメタデータの更新を実行できます。

スナップショットをリストアすると、フルボリュームのデータを持つ新しい Amazon EBS ボリュームが作成されます。部分的な復元のみが必要な場合は、実行中のインスタンスに別のデバイス名でボリュームをアタッチできます。次にそれをマウントし、オペレーティングシステムのコピーコマンドを使って、バックアップボリュームから本番ボリュームにデータをコピーします。

Amazon EC2 ドキュメント で説明 AWS されているように、Amazon EBS スナップショットコピー機能を使用して、リージョン間で Amazon EBS スナップショットをコピーすることもできます。Amazon EC2 この機能を使用すると、基盤となるレプリケーションテクノロジーを管理しなくても、バックアップを別のリージョンに保存できます。

個別のサーバーボリュームを確立する

オペレーティングシステム、ログ、アプリケーション、およびデータには、すでに標準の個別のボリュームセットを使用している場合があります。個別のサーバーボリュームを確立することで、ディ

スクスペースの枯渇が原因でアプリケーションやプラットフォームに障害が発生した場合の影響範囲を軽減できます。通常、物理ハードドライブで物理的なハードディスクドライブの場合、ボリュームを迅速に拡張する柔軟性がないため、このリスクは通常より大きくなります。物理ドライブの場合は、新しいドライブを購入してデータをバックアップし、新しいドライブにデータを復元する必要があります。を使用すると AWS、Amazon EBS を使用してプロビジョニングされたボリュームを拡張できるため、このリスクが大幅に軽減されます。詳細については、「AWS ドキュメント」を参照してください。

アプリケーションデータ、ユーザーデータ、ログ、スワップファイル用に別々のボリュームを用意して、これらのリソースに別々のバックアップポリシーと復元ポリシーを使用できるようにします。データ用にボリュームを分けることで、データのパフォーマンスとストレージの要件に基づいて異なるボリュームタイプを使用することもできます。そして、異なるワークロードに対してコストを最適化し、微調整できます。

インスタンスストアボリュームに関する考慮事項

インスタンスストアは、インスタンス用のブロックレベルの一時ストレージを提供します。このストレージは、ホストコンピュータに物理的にアタッチされたディスク上にあります。インスタンスストアは、バッファ、キャッシュ、スクラッチデータ、その他の一時的なコンテンツなど、頻繁に変更される情報の一時的な保存に最適です。また、ウェブサーバーのロードバランストプールなど、複数のインスタンスにまたがってレプリケートされるデータにも適しています。

インスタンスストア上のデータは、関連付けられたインスタンスの運用中のみ維持されます。インスタンスが再ブートされた場合、その再ブートが意図的なものでも、意図せずに行われたとしても、インスタンスストアのデータは維持されます。ただし、次のいずれの状況でも、インスタンスストアのデータは失われます。

- 基盤となるドライブが故障しました。
- インスタンスが停止しました。
- インスタンスが終了します。

したがって、価値のある長期的なデータをインスタンスストアに依存してはなりません。代わりに、Amazon S3、Amazon EBS、または Amazon EFS などのより堅牢なデータストレージを使用してください。

インスタンスストアボリュームの一般的な戦略は、目標復旧時点 (RPO) と目標復旧時間 (RTO) に基づいて、必要に応じて必要なデータを定期的に Amazon S3 に永続化することです。その後、新しい

インスタンスが起動されたときに、Amazon S3 からインスタンスストアにデータをダウンロードできます。インスタンスが停止する前に、Amazon S3 にデータをアップロードすることもできます。永続化のため、EBS ボリュームを作成してインスタンスにアタッチし、そのデータをインスタンスストアボリュームから EBS ボリュームに定期的にコピーします。詳細については、AWS ナレッジセンターを参照してください。

EBS スナップショットと AMI のタグ付けと標準の適用

すべての AWS リソースにタグを付けることは、コスト配分、監査、トラブルシューティング、通知にとって重要な方法です。EBS ボリュームでは、ボリュームの管理と復元に必要な関連情報が表示されるようにするためのタグ付けが重要です。タグは EC2 インスタンスから AMI に、またはソースボリュームからスナップショットに自動的にコピーされません。バックアッププロセスには、これらのソースからの関連タグが含まれていることを確認してください。これは、将来これらのバックアップを使用するために、アクセスポリシー、添付ファイル情報、コスト配分などのスナップショットメタデータを設定するのに役立ちます。 AWS リソースのタグ付けの詳細については、「 タグ付けのベストプラクティス」テクニカルホワイトペーパーを参照してください。

すべての AWS リソースに使用するタグに加えて、次のバックアップ固有のタグを使用します。

- ソースインスタンス ID
- ソースボリューム ID (スナップショット用)
- 回復ポイントの説明

AWS Config ルールと IAM アクセス許可を使用して、タグ付けポリシーを適用できます。IAM は強制的なタグ使用をサポートしているため、Amazon EBS スナップショットを使用する際に特定のタグの使用を義務付ける IAM ポリシーを作成できます。IAM アクセス権限ポリシーで定義されたタグで権限を付与せずに `CreateSnapshot` 操作を試みると、スナップショットの作成はアクセスが拒否されて失敗します。詳細については、「Amazon EBS スナップショットの作成時のタグ付けとより強力なセキュリティポリシーの実装に関するブログ記事」を参照してください。

AWS Config ルールを使用して、 リソースの設定を自動的に評価できます AWS 。開始に役立つように、 は、マネージドルールと呼ばれるカスタマイズ可能な定義済みルール AWS Config を提供します。独自のカスタムルールを作成することもできます。はリソース間の設定変更 AWS Config を継続的に追跡しますが、これらの変更がルールの条件に違反していないかどうかを確認します。リソースがルールに違反すると、 はリソースとルールを非準拠の として AWS Config フラグ付けします。「required-tags」 マネージドルールは現在、スナップショットと AMI をサポートしていないことに注意してください。

AMI と EBS スナップショットで EBS ボリュームバックアップを作成します

AWS には、AMIs とスナップショットを作成および管理するための豊富なオプションが用意されています。ニーズに合ったアプローチを使用できます。多くのカスタマーが直面する一般的な問題は、スナップショットのライフサイクルを管理し、目的や保存ポリシーなどによってスナップショットを明確に調整することです。適切なタグ付けを行わないと、スナップショットが誤って削除されたり、自動クリーンアッププロセスの一環として削除されたりするリスクがあります。また、まだ必要かどうかが明確にわからないため、古いスナップショットが保存されているために料金を支払うことになる可能性もあります。

スナップショットまたは AMI を作成する前に EBS ボリュームを準備する

スナップショットを作成したり AMI を作成したりする前に、EBS ボリュームに必要な準備を行います。AMI を作成すると、インスタンスにアタッチされている EBS ボリュームごとに新しいスナップショットが作成されるため、これらの準備は AMI にも適用されます。

電源が入っている EC2 インスタンスが使用している、アタッチされた EBS ボリュームのスナップショットを取ることができます。ただし、スナップショットでは、スナップショットコマンドを実行した時点で EBS ボリュームに書き込まれているデータのみがキャプチャされます。そのため、アプリケーションやオペレーティングシステムによってキャッシュされたデータは除外される可能性があります。ベストプラクティスは、システムを I/O を一切実行していない状態にすることです。理想的には、マシンはトラフィックを受け付けず、停止状態ですが、24 時間 365 日の IT 運用が標準となっているため、このような状況はまれです。システムメモリからアプリケーションが使用しているディスクにデータをフラッシュし、スナップショットを取るのに十分な時間、ボリュームへのファイル書き込みを一時停止できれば、スナップショットは完了するはずです。

クリーンバックアップを作成するには、データベースまたはファイルシステムを停止する必要があります。これを行う方法は、データベースまたはファイルシステムによって異なります。

データベースのプロセスは以下のとおりです:

1. 可能であれば、データベースをホットバックアップモードにします。
2. Amazon EBS スナップショットコマンドを実行します。
3. データベースをホットバックアップモードから解除するか、リードレプリカを使用している場合はリードレプリカインスタンスを終了します。

ファイルシステムのプロセスも同様ですが、オペレーティングシステムやファイルシステムの能力に依存します。例えば、XFS は一貫したバックアップのためにデータをフラッシュできるファイルシステムです。詳細については、「xfs_freeze」を参照してください。あるいは、I/O のフリーズをサポートする論理ボリュームマネージャーを使用すれば、このプロセスを簡単に行うことができます。

しかし、ボリュームへのすべてのファイル書き込みをフラッシュまたは一時停止できない場合は、次のようにします:

1. オペレーティングシステムからボリュームをアンマウントします。
2. スナップショットコマンドを発行します。
3. ボリュームを再マウントして、一貫性のある完全なスナップショットを作成します。スナップショットのステータスがペンディングの間は、ボリュームを再マウントして使用できます。

スナップショットの処理はバックグラウンドで継続され、スナップショットの作成は迅速に行われ、特定の時点がキャプチャされます。バックアップしているボリュームは、ほんの数秒でアンマウントされます。停止が予想される短いバックアップウィンドウをスケジュールして、クライアントが適切に処理するように設定できます。

ルートデバイスとして機能する EBS ボリュームのスナップショットを作成する場合は、スナップショットを取る前にインスタンスを停止します。Windows には、アプリケーション整合性のあるスナップショットの作成に役立つ Volume Shadow Copy Service (VSS) が用意されています。 AWS には、VSS 対応アプリケーションのイメージレベルのバックアップを作成するために実行できる Systems Manager ドキュメントが用意されています。スナップショットには、これらのアプリケーションとディスクとの間で保留されているトランザクションのデータが含まれます。すべてのアタッチされたボリュームのバックアップを実行する際に、インスタンスのシャットダウンあるいは切断を必要としません。詳細については、AWS ドキュメントを参照してください。

> **Note**
>
> 別の同様のインスタンスをデプロイするために Windows AMI を作成する場合は、EC2Config または EC2Launch を使用してインスタンスを Sysprep します。次に、停止したインスタンスから AMI を作成します。Sysprep は Amazon EC2 Windows インスタンスから SID、コンピュータ名、ドライバなどの固有の情報を削除します。重複した SID は、Active Directory、Windows Server Update Services (WSUS)、ログインの問題、Windows ボリュームキーのアクティベーション、Microsoft Office、およびサードパーティ製品で問題を引き起こす可能性があります。AMI がバックアップ目的で、同じインスタンスをすべての固有情報をそのまま復元したい場合は、インスタンスで Sysprep を使用しないでください。

EBS ボリュームのスナップショットをコンソールから手動で作成します。

インスタンスで完全にテストされていない大きな変更を加える前に、適切なボリュームまたはインスタンス全体のスナップショットを作成します。例えば、インスタンス上のアプリケーションやシステムソフトウェアをアップグレードしたり、パッチを当てたりする前にスナップショットを作成したい場合があります。

スナップショットはコンソールから手動で作成できます。Amazon EC2 コンソールの[Elastic Block Store Volumes] ページで、バックアップするボリュームを選択します。次に [Actions] メニューから [Create Snapshot] を選択します。フィルタボックスにインスタンス ID を入力すると、特定のインスタンスにアタッチされているボリュームを検索できます。

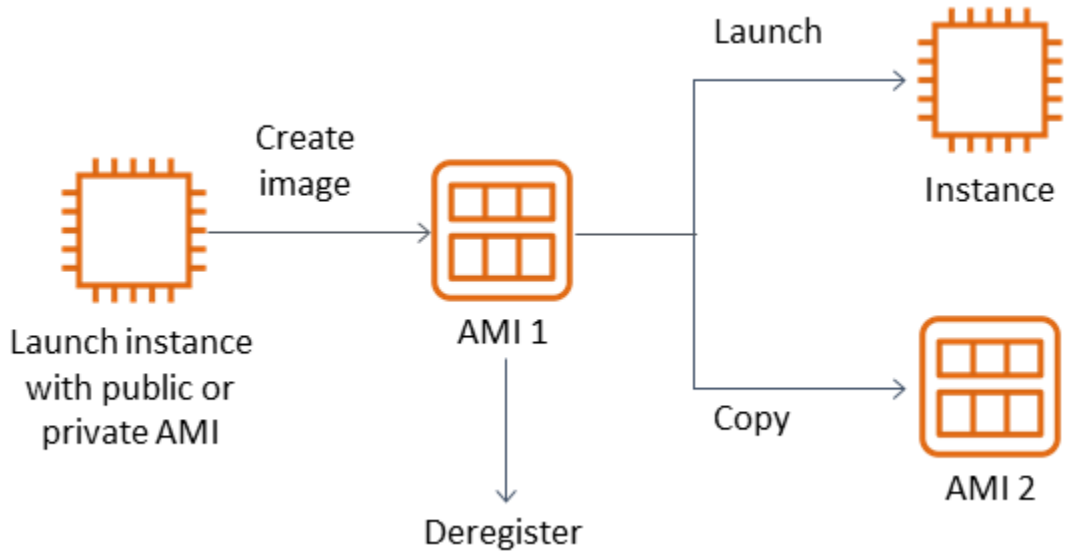
説明を入力し、適切なタグを追加します。Name タグを追加して、後でボリュームを見つけやすくします。タグ付け戦略に基づいて、その他の適切なタグを追加します。

AMI の作成

AMI はインスタンスの起動に必要な情報を提供します。AMI には、イメージの作成時にインスタンスにアタッチされた EBS ボリュームのルートボリュームとスナップショットが含まれます。EBS スナップショットだけから新しいインスタンスを起動することはできません。新しいインスタンスは AMI から起動する必要があります。

AMI を作成すると、使用しているアカウントとリージョンに作成されます。AMIの作成プロセスは、インスタンスにアタッチされた各ボリュームの Amazon EBS スナップショットを作成し、AMI はこれらの Amazon EBS スナップショットを参照します。これらのスナップショットは Amazon S3 に保存され、高い耐久性を持ちます。

EC2 インスタンスの AMI を作成した後、AMI を使用してインスタンスを再作成するか、インスタンスのコピーをさらに起動できます。アプリケーションの移行や DR のために AMI をあるリージョンから別のリージョンにコピーすることもできます。



VMWARE 仮想マシンなどの仮想マシンを に移行しない限り、EC2 インスタンスから AMI を作成する必要があります AWS。Amazon EC2 コンソールから AMI を作成するには、インスタンスを選択し、[アクション]、[イメージ]、[イメージの作成] の順に選択します。

Amazon Data Lifecycle Manager

Amazon EBS スナップショットの作成、保持、削除を自動化するには、「Amazon Data Lifecycle Manager」 を使うことができます。スナップショット管理を自動化することで、以下のことが可能になります:

- 定期的なバックアップスケジュールを実施して貴重なデータを保護する。
- 監査担当者または社内のコンプライアンスが必要とするバックアップを保持する。
- 古いバックアップを削除してストレージコストを削減する。

Amazon Data Lifecycle Manager を使用すると、EC2 インスタンス (およびそれに接続された EBS ボリューム) または個別の EBS ボリュームのスナップショット管理プロセスを自動化できます。クロスリージョンコピーなどのオプションをサポートしているので、スナップショットを他の AWS リージョンに自動的にコピーすることができます。代替リージョンへのスナップショットのコピーは、DR の取り組みを支援し、代替リージョンでオプションを復元する方法の 1 つです。Amazon Data Lifecycle Manager を使って、高速スナップショット・リストアをサポートするスナップショットライフサイクルポリシーを作成することもできます。

Amazon Data Lifecycle Manager は、Amazon EC2 と Amazon EBS に含まれる機能です。Amazon Data Lifecycle Manager は課金されません。

AWS Backup

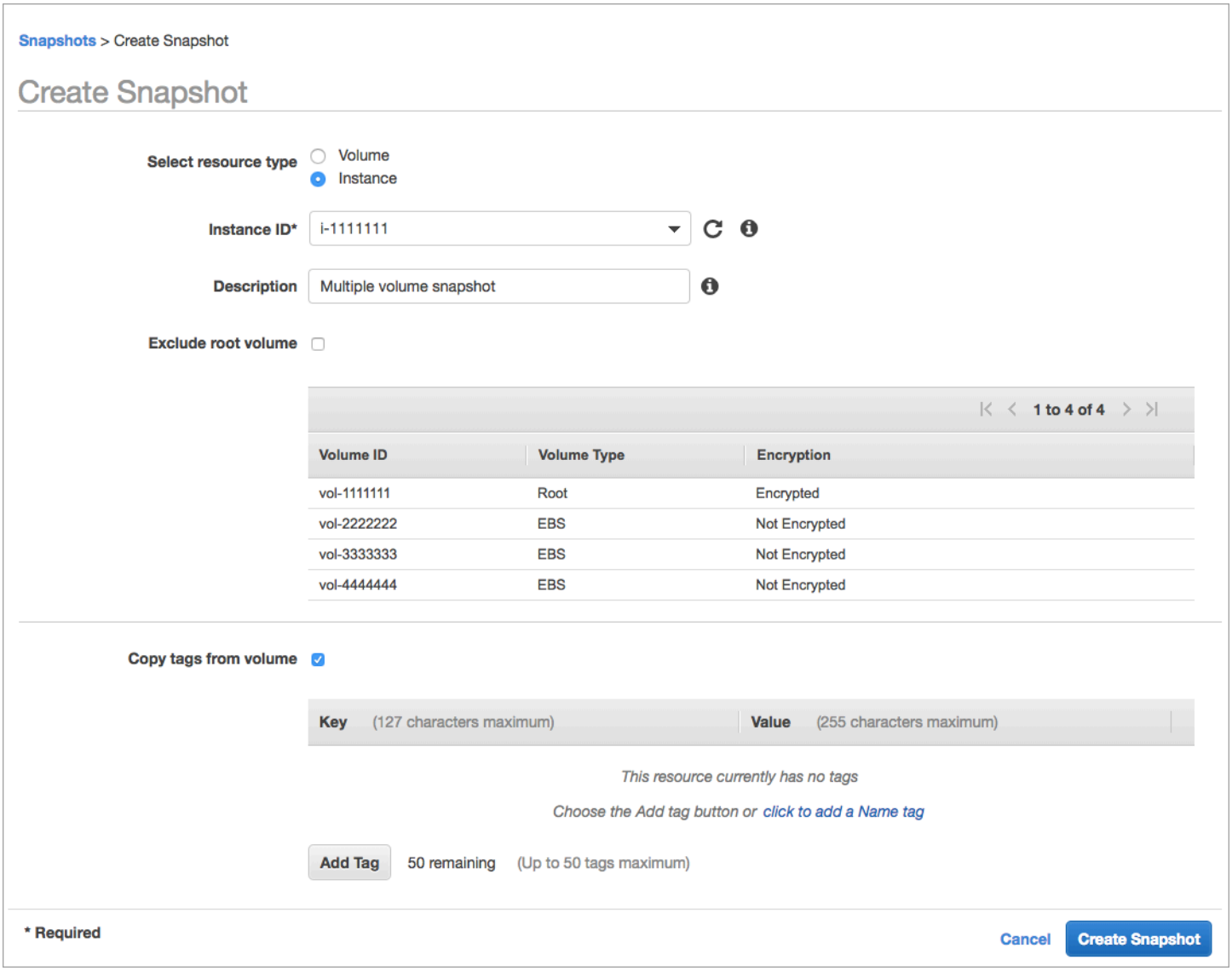
AWS Backup は、複数の AWS サービスにまたがるリソースを含むバックアッププランを作成できるため、Amazon Data Lifecycle Manager と一意です。リソースのバックアップを個別に調整するのではなく、一緒に使用しているリソースをカバーするようにバックアップを調整できます。

AWS Backup には、完了したバックアップのリカバリポイントへのアクセスを制限できるバックアップボールトの概念も含まれています。復元オペレーションは、個々のリソースに進み、作成されたバックアップを復元する AWS Backup のではなく、 から開始できます。 には、監査管理やレポートなどの追加機能のホスト AWS Backup も含まれています。詳細については、このガイドの「AWS Backup を使ったバックアップとリカバリー」セクションを参照してください。

マルチボリュームバックアップの実行

スナップショットを使用して RAID アレイの EBS ボリューム上のデータをバックアップする場合、スナップショットは一貫性がなければなりません。これは、ボリュームのスナップショットが個別に作成されるためです。同期していないスナップショットから RAID アレイの EBS ボリュームを復元すると、アレイの整合性が低下します。

RAID アレイのスナップショットの一貫したセットを作成するには、 CreateSnapshots API オペレーションを使用するか、Amazon EC2 コンソールにログインし、Elastic Block Store 、スナップショット 、スナップショットの作成 を選択します。



RAID 構成で複数のボリュームが接続されているインスタンスのスナップショットは、まとめてマルチボリュームスナップショットとして取得されます。マルチボリュームスナップショットは point-in-time、EC2 インスタンスにアタッチされた複数の EBS ボリュームにまたがる、データ調整されたクラッシュコンシステントなスナップショットを提供します。スナップショットは複数の EBS ボリュームにまたがって自動的に作成されるため、一貫性を保つためにインスタンスを停止してボリューム間で調整する必要はありません。ボリュームのスナップショットが開始された後 (通常は 1、2 秒)、ファイルシステムは操作を続けることができます。

スナップショットが作成されると、各スナップショットは個別のスナップショットとして扱われます。シングルボリュームのスナップショットと同様に、リストア、削除、リージョンやアカウントをまたいだコピーなど、すべてのスナップショット操作を実行できます。単一ボリュームのスナップショットと同じように、マルチボリュームスナップショットにタグを付けることもできます。復元、

コピー、または保存中にマルチボリュームスナップショットをまとめて管理するためにタグを付けることをお勧めします。詳細については、AWS ドキュメントを参照してください。

これらのバックアップは、論理ボリュームマネージャーまたはファイルシステムレベルのバックアップからも実行できます。このような場合、従来のバックアップエージェントを使用すると、データをネットワーク経由でバックアップできます。インターネットや AWS Marketplace では、エージェントベースのバックアップソリューションが数多く提供されています。

別の方法として、1 つの大きなボリュームに存在するプライマリシステムボリュームのレプリカを作成する方法があります。これにより、バックアップする必要があるのは大きなボリュームが 1 つだけで、バックアップはプライマリシステムでは行われないため、バックアッププロセスが簡略化されます。ただし、まず、バックアップ中に 1 つのボリュームで十分なパフォーマンスを発揮できるかどうか、および最大ボリュームサイズがアプリケーションに適しているかどうかを判断します。

Amazon EC2 バックアップの保護

バックアップのセキュリティを考慮し、バックアップの偶発的または悪意ある削除を防ぐことが重要です。そのためには、複数の方法を組み合わせて使用することができます。セキュリティ侵害による重要なバックアップの損失を防ぐため、バックアップを別の AWS アカウントにコピーすることをお勧めします。複数の AWS アカウントをお持ちの場合は、他のすべてのアカウントがバックアップをコピーできるアーカイブアカウントとして別のアカウントを指定できます。例えば、AWS Backup でのクロスアカウントバックアップでこれを達成することができます。

また、災害対策計画では、ある地域で障害が発生した場合に、別の AWS リージョンで EC2 インスタンスを複製できるようにする必要がある場合もあります。同じアカウント内の別のリージョンにバックアップをコピーすることで、この目標を達成できます。これにより、偶発的な削除を防止するレイヤーを追加できるだけでなく、ディザスタリカバリ (DR) 目標もサポートできます。AWS Backup はクロスリージョンバックアップをサポートしています。

ec2:DeleteSnapshot および ec2:DeregisterImage アクションへの IAM アクセス許可をブロックすることを検討してください。代わりに、保持ポリシーと方法に EBS スナップショットと Amazon EC2 AMI のライフサイクルを管理させることができます。削除アクションをブロックすることは、EBS スナップショットの WORM (Write-Once、Read-Many) 戦略を実装する方法の 1 つです。EBS スナップショットやその他の AWS リソースをサポートするボールAWS Backup トロック を使用することもできます。

さらに、ec2:ModifyImageAttribute および ec2: IAM アクションをブロックして、ユーザーが AMIs と EBS ModifySnapshotAttribute スナップショットを共有できないようにすることを検討してください。これにより、AMIs とスナップショットが組織の外部 AWS にあるアカウントと共有されなくな

ります。を使用している場合は AWS Backup、バックアップボールトで同様の操作を実行できないようにユーザーを制限します。詳細については、このガイドの「AWS Backup」セクションを参照してください。

Amazon EC2 には、誤って削除してしまった EBS スナップショットを復元するのに役立つごみ箱機能があります。ユーザーにスナップショットの削除を許可している場合は、必要なスナップショットが永久に削除されないように、この機能をオンにします。Amazon EC2 のコンソールでは、複数のスナップショットを選択して 1 回の操作で削除することができるため、ユーザーは複数のスナップショットを削除することに特に注意する必要があります。また、クリーンアップスクリプトや自動化を使用するときは、必要なスナップショットを誤って削除しないように注意してください。ごみ箱機能は、このような状況からの保護に役立ちます。

EBS スナップショットのアーカイブ

EBSスナップショットのアーカイブは、90 日以上リストアするつもりのないボリュームのコピーを参照目的で保持するためのコスト効率のよい方法です。これは、EBS ボリュームに関連するすべてのスナップショットを永久に削除する前の、良い中間ステップになります。例えば、使用されなくなった EBS ボリュームの end-of-lifecycle ステップとしてスナップショットをアーカイブすることを検討できます。削除するよりもアーカイブする方が、ごみ箱を使用するよりもコスト効率の高い削除保持方法でもあります。

Systems Manager、、 AWS SDKs を使用したスナップショット AWS CLI と AMI の作成の自動化

バックアップ方法によっては、スナップショットまたは AMI の作成前後に操作が必要になる場合があります。例えば、ファイルシステムを静止させるために、サービスを停止して開始する必要がある場合があります。または、AMI の作成中にインスタンスを停止して起動する必要がある場合もあります。また、アーキテクチャ内の複数のコンポーネントのバックアップをまとめて作成する必要がある場合もあります。各コンポーネントのバックアップには、作成前と作成後の手順が異なります。

プロセスを自動化し、バックアッププロセスが一貫して適用されていることを確認することで、バックアップのメンテナンスウィンドウ時間を短縮できます。カスタムの作成前および作成後のオペレーションを自動化するには、 AWS CLI と SDK を使用してバックアッププロセスをスクリプト化します。

自動化は Systems Manager ランブックで定義できます。このランブックは、オンデマンドで実行することも、Systems Manager のメンテナンス期間中に実行することもできます。Systems Manager Runbook を実行するアクセス権限をユーザーに付与すれば、Amazon EC2 の混乱を招くコマンドへのアクセス権限をユーザーに付与する必要はありません。また、バックアッププロセスとタグがユー

ザーによって一貫して適用されていることを確認するのにも役立ちます。AWSCreateSnapshot および AWS CreateImageランブックを使用してスナップショットと AMIsを作成することも、他のユーザーにそのスナップショットと AMI を使用するアクセス許可を付与することもできます。Systems Manager には、AMI のパッチ適用と AMI の作成を自動化するための AWSUpdateLinuxAmi ランブックと AWSUpdateWindowsAmi ランブックも含まれています。

AWS CLI および を使用してAWS Tools for Windows PowerShell、スナップショットと AMI の作成プロセスを自動化することもできます。aws ec2 create-snapshot AWS CLI コマンドを使用して、オートメーションの 1 ステップとして EBS ボリュームのスナップショットを作成できます。aws ec2 create-snapshots コマンドを使用すると、EC2 インスタンスにアタッチされているすべてのボリュームについて、クラッシュコンシステントで同期されたスナップショットを作成できます。

AWS CLI を使用して、新しい AMIs を作成できます。aws ec2 register-image コマンドを使用して EC2 インスタンス用の新しいイメージを作成できます。インスタンスのシャットダウン、イメージ作成、再起動を自動化するには、このコマンドと aws ec2 stop-instances と aws ec2 start-instances コマンドを組み合わせます。

Amazon EBS ボリュームまたは EC2 インスタンスのリストア

EC2 インスタンスにアタッチされたボリュームを 1 つだけ復元する必要がある場合は、そのボリュームを個別に復元し、既存のボリュームをデタッチして、復元したボリュームを EC2 インスタンスにアタッチできます。すべての関連ボリュームを含む EC2 インスタンス全体をリストアする必要がある場合は、インスタンスの Amazon Machine Image (AMI) バックアップを使用する必要があります。

復旧時間を短縮し、依存するアプリケーションやプロセスへの影響を減らすには、復元プロセスで置き換えるリソースを考慮する必要があります。最良の結果を得るためには、リストアプロセスが目標復旧時点 (RPO) と目標復旧時間 (RTO) を満たしていること、およびリストアプロセスが期待通りに動作することを検証するために、より低い環境 (たとえば非本番環境) でリストアプロセスを定期的にテストしてください。リストアプロセスが、リストアするインスタンスに依存するアプリケーションやサービスにどのような影響を与えるかを検討し、必要に応じてリストアを調整します。リストアプロセスをできるだけ自動化し、テストすることで、リストアプロセスが失敗したり、実施に一貫性がなくなったりするリスクを減らします。

複数のインスタンスでトラフィックを処理する Elastic Load Balancing を使用している場合、障害が発生したインスタンスや障害のあるインスタンスをサービスから外すことができます。その後、新しいインスタンスを復元して置き換えることができます。その間、他のインスタンスはユーザーに影響を与えずにトラフィックを処理し続けます。

以下に説明するリストアプロセスは、Elastic Load Balancing を使用していないインスタンスの場合です:

- EBS スナップショットからの個々のファイルとディレクトリの復元
- Amazon EBS スナップショットからの EBS ボリュームの復元
- EBS スナップショットからの EC2 インスタンスの作成または復元
- AMI からの実行中のインスタンスの復元

EBS スナップショットからファイルとディレクトリの復元

EBS スナップショットは、スナップショットの作成に使用された元のボリュームの point-in-time 正確なレプリカを提供します。個々のファイルまたはディレクトリを復元するには、以下の手順を実行する必要があります。

1. まず、ファイルまたはディレクトリを含む EBS スナップショットからボリュームを復元します。
2. ファイルを復元する EC2 インスタンスにボリュームをアタッチします。
3. 復元されたボリュームから EC2 インスタンスボリュームにファイルをコピーします。
4. 復元したボリュームをデタッチして削除します。

Amazon EBS スナップショットからの EBS ボリュームの復元

スナップショットからボリュームを作成し、インスタンスにアタッチすることで、既存の EC2 インスタンスにアタッチされたボリュームをリストアできます。コンソール、、または API オペレーションを使用して AWS CLI、既存のスナップショットからボリュームを作成できます。その後、オペレーティングシステムを使用してボリュームをインスタンスにマウントできます。

Amazon EBS スナップショットからのデータは、非同期で EBS ボリュームにロードされることに注意します。データがロードされていないボリュームにアプリケーションがアクセスすると、Amazon S3 からデータがロードされている間、通常よりもレイテンシーが高くなります。レイテンシーの影響を受けやすいアプリケーションにおいてこの影響を回避するには、次の 2 つのオプションがあります。

- EBS ボリュームの初期化が可能です。
- 追加料金で、Amazon EBS は高速スナップショットリストアをサポートし、ボリュームの初期化を不要にします。

同じマウントポイントを使用する必要のあるボリュームを交換する場合は、そのボリュームをアンマウントして、新しいボリュームをその場所にマウントできるようにします。ボリュームをアンマウントするには、まずそのボリュームを使用しているプロセスをすべて停止します。ルートボリュームを置き換える場合は、ルートボリュームをデタッチする前にインスタンスを停止する必要があります。

例えば、コンソールを使用してボリュームを以前の point-in-time バックアップに復元するには、次の手順に従います。

1. Amazon EC2 コンソールの [Elastic Block Store] メニューで、[Snapshots] を選択します。
2. 復元したいスナップショットを検索し、選択します。
3. [アクション]、そして[ボリュームの作成] の順に選択します。
4. EC2 インスタンスと同じアベイラビリティゾーンに新しいボリュームを作成します。
5. Amazon EC2 のコンソールで、インスタンスを選択します。
6. インスタンスの詳細で、[Root device] エントリーまたは [Block Devices] エントリーで置き換えたいデバイス名をメモします。
7. ボリュームをデタッチします。ルートボリュームと非ルートボリュームでは手順が異なります。

   ルートボリュームの場合:

   a. EC2 インスタンスを停止します。
   b. [EC2 Elastic Block Store Volumes] メニューで、置き換えるルートボリュームを選択します。
   c. [アクション] を選択して、[ボリュームのデタッチ] を選択します。
   d. [EC2 Elastic Block Store Volumes] メニューで、新しいボリュームを選択します。
   e. [アクション] を選択し、[ボリュームのアタッチ] を選択します。
   f. ボリュームをアタッチするインスタンスを選択し、先にメモしたのと同じデバイス名を使用します。

   非ルートボリュームの場合:

   a. [EC2 Elastic Block Store Volumes] メニューで、置き換えたい非ルートボリュームを選択します。
   b. [アクション] を選択して、[ボリュームのデタッチ] を選択します。
   c. [EC2 Elastic Block Store ボリューム] メニューで新しいボリュームを択し、[アクション]、[ボリュームのアタッチ] の順に選択して新しいボリュームをアタッチします。アタッチするインスタンスを選択し、使用可能なデバイス名を選択します。
   d. インスタンスのオペレーティングシステムを使用して既存のボリュームをアンマウントし、新しいボリュームをその場所にマウントします。

Linux では、umount コマンドを使うことができます。Windows では、ディスク管理システムユーティリティなどの論理ボリュームマネージャ (LVM) を使うことができます。

e. [EC2 Elastic Block Store ボリューム] メニューでそのボリュームを選択し、[アクション]、[ボリュームのデタッチ] の順に選択して、置き換える前のボリュームをデタッチします。

をオペレーティングシステム AWS CLI のコマンドと組み合わせて使用して、これらのステップを自動化することもできます。

EBS スナップショットからの EC2 インスタンスの作成または復元

EC2 インスタンス全体をリストアするために使用するバックアップを作成するには、Amazon マシンイメージ (AMI) を作成することを推奨します。AMI は、仮想化タイプなどのマシン情報を取得します。また、EC2 インスタンスにアタッチされている各ボリュームのスナップショットを作成し、デバイスマッピングも含めて、同じ構成でリストアできるようにします。

ただし、EBS スナップショットを使用してインスタンスを復元する必要がある場合は、まず、新しい EC2 インスタンスのルートボリュームとなる EBS スナップショットから AMI を作成します。

1. Amazon EC2 コンソールの [Elastic Block Store] メニューで、[Snapshots] を選択します。
2. 新しい EC2 インスタンスのルートボリュームの作成に使用するスナップショットを検索して選択します。
3. [アクション] を選択し、[スナップショットから画像を作成] を選択します。
4. 画像の名前 (たとえば YYYYMMDD-restore-for-i-012345678998765de) を入力し、新しい画像に適したオプションを選択します。

イメージが作成されて使用できるようになったら、ルートボリュームの EBS スナップショットを使用する新しい EC2 インスタンスを起動できます。

AMI からの実行中のインスタンスの復元

AMI バックアップから新しいインスタンスを起動して、実行中の既存のインスタンスを置き換えることができます。ひとつの方法は、既存のインスタンスを停止し、オフラインのまま AMI から新しいインスタンスを起動し、必要なアップデートを実行することです。このアプローチにより、両方のインスタンスが同時に実行されて競合が発生するリスクが軽減されます。インスタンスが提供するサービスがダウンしている場合や、メンテナンスの時間帯に復元を実行している場合には、この方法でも問題ありません。新しいインスタンスをテストしたら、古いインスタンスに割り当てられた

Elastic IP アドレスを再割り当てできます。その後、新しいインスタンスを指すようにドメインネームサービス (DNS) レコードを更新できます。

ただし、復元中に稼働中のインスタンスのダウンタイムを最小限に抑える必要がある場合は、AMI バックアップから新しいインスタンスを起動してテストすることを検討します。その上で、既存のインスタンスを新しいインスタンスで置き換えます。

両方のインスタンスが実行されている間は、新しいインスタンスがプラットフォームレベルまたはアプリケーションレベルの衝突を引き起こさないようにする必要があります。たとえば、同じ SID とコンピューター名で実行されているドメインに参加している Windows インスタンスで問題が発生する可能性があります。一意の識別子を必要とするネットワークアプリケーションやサービスでも同様の問題が発生する可能性があります。

準備が整う前に他のサーバーやサービスが新しいインスタンスに接続するのを防ぐには、セキュリティグループを使用して、アクセスやテスト用に自分の IP アドレスを除く新しいインスタンスのすべてのインバウンド接続を一時的にブロックします。また、新しいインスタンスのアウトバウンド接続を一時的にブロックして、サービスやアプリケーションが他のリソースへの接続や更新を開始しないようにすることもできます。新しいインスタンスの準備ができたら、既存のインスタンスを停止し、新しいインスタンスでサービスとプロセスを開始し、実装したインバウンドまたはアウトバウンドのネットワーク接続のブロックを解除します。

オンプレミスのインフラから AWS へのバックアップとリカバリ

AWS を使えば、オンプレミスのインフラストラクチャーのバックアップを、耐久性のあるオフサイト・ストレージに保存できます。このシナリオで AWS ストレージサービスを使うことで、バックアップとアーカイブ作業に集中できます。ストレージ・インフラのプロビジョニング、スケーリング、バックアップ・タスクのためのインフラ容量を心配する必要はありません。

Amazon S3 と Amazon S3 Glacier は、これらのサービスを新規および既存のバックアップとリカバリーのアプローチに統合するための広範な API 操作と SDK を提供しています。これにより、バックアップソフトウェアベンダーは、自社のアプリケーションを AWS ストレージソリューションと直接統合することができます。

このシナリオでは、オンプレミスのインフラで使用しているバックアップ・アーカイブ・ソフトウェアが、API 操作を通じて AWS と直接インターフェースします。バックアップ・ソフトウェアは AWS 認識なので、オンプレミス・サーバーから Amazon S3 または Amazon S3 Glacier に直接データをバックアップします。

既存のバックアップ・ソフトウェアが AWS クラウドをネイティブにサポートしていない場合、Storage Gateway を使用することができます。クラウドストレージサービスである Storage Gateway は、オンプレミスのシステムからスケーラブルなクラウドストレージへのアクセスを可能にします。Amazon S3 または Amazon S3 Glacier に暗号化されたデータを安全に保存しながら、既存のアプリケーションと連携するオープンスタンダードのストレージプロトコルをサポートしています。Storage Gateway は、オンプレミスのブロックベースのストレージワークロードのバックアップとリカバリのアプローチの一部として使用できます。

Storage Gateway は、バックアップ用にクラウドベースのストレージに移行したいというハイブリッドシナリオに役立ちます。Storage Gateway はまた、オンプレミス・ストレージへの設備投資を削減するのにも役立ちます。Storage Gateway は、VM または専用のハードウェアアプライアンスとして導入します。このガイドでは、Storage Gateway をバックアップとリカバリにどのように適用するかに焦点を当てます。

Storage Gateway には、さまざまな要件を満たす 3 つのオプションがあります。

- アプリケーション・データ・ファイルとバックアップ・イメージを、SMB ベースまたは NFS ベースのアクセスを使って、Amazon S3 クラウドストレージ上に耐久性のあるオブジェクトとして保存するためのファイルゲートウェイ。

- クラウドベースのiSCSIブロックストレージボリュームをオンプレミスアプリケーションに提供するためのボリュームゲートウェイ。ボリュームゲートウェイは、ローカルキャッシュまたはオンプレミスのフルボリュームを提供すると同時に、ボリュームのフルコピーを AWS クラウドに保存します。
- 信頼できるバックアップソフトウェアをオンプレミスのストレージゲートウェイに送り、次に Amazon S3 と Amazon S3 Glacier に接続するためのテープゲートウェイ。このオプションでは、既存の投資やプロセスを中断することなく、クラウドの拡張性と耐久性を実現し、安全かつ長期的に保存できます。

ファイルゲートウェイ

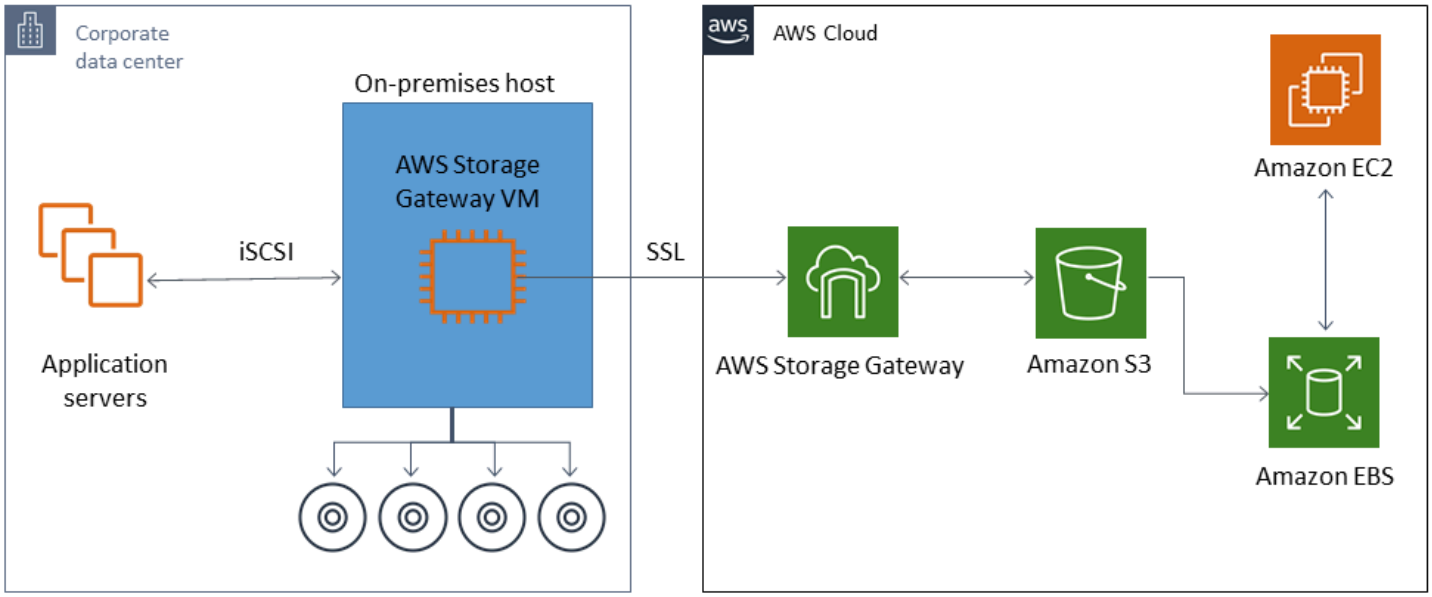
多くの組織は、バックアップなどの二次データや三次データをクラウドに移行することからクラウドへの移行を開始します。ファイルゲートウェイの SMB および NFS インターフェイスのサポートにより、IT グループはバックアップジョブを既存のオンプレミスバックアップシステムからクラウドに移行できます。バックアップ・アプリケーション、ネイティブ・データベース・ツール、または SMB や NFS に書き込めるスクリプトは、ファイル・ゲートウェイに書き込めます。ファイルゲートウェイは、バックアップを最大 5 TiB のサイズの Amazon S3 オブジェクトとして保存します。適切な大きさのローカルキャッシュがあれば、最近のバックアップをオンサイトでの高速リカバリに使用できます。長期保存のニーズには、低コストの S3 Standard-Infrequent Access と Amazon S3 Glacier ストレージ階層にバックアップを階層化することで対応します。

ファイルゲートウェイは、ブロックベースのストレージを Amazon S3 に移行させ、耐久性の高いオフサイトバックアップを実現します。特に、最近バックアップしたファイルを素早くリストアする必要がある場合に便利です。ファイルゲートウェイは SMB と NFS プロトコルをサポートしているので、ユーザーはネットワークファイル共有にアクセスするのと同じ方法でファイルにアクセスできます。Amazon S3 オブジェクトのバージョン管理機能も活用できます。オブジェクトのバージョニングを使えば、ファイルの以前のオブジェクトバージョンを復元し、SMB や NFS を使って簡単にアクセスできます。

ボリュームゲートウェイ

ボリュームゲートウェイを使えば、クラウドベースの iSCSI ブロックストレージボリュームをオンプレミスのサーバーにプロビジョニングできます。ボリュームゲートウェイは、耐久性と拡張性に優れたクラウドベースのオフサイトストレージとして、ボリュームデータを Amazon S3 に保存します。ボリュームゲートウェイを使用すると、ボリュームのポイントインタイムの完全なスナップショットを作成し、Amazon EBS スナップショットとしてクラウドに保存できます。スナップショットとして保存した後は、ボリューム全体を EBS ボリュームとして復元して EC2 インスタ

ンスにアタッチできるため、クラウドベースの DR ソリューションが加速します。ボリュームは Storage Gateway にリストアすることもでき、オンプレミスのアプリケーションを以前の状態に戻すことができます。



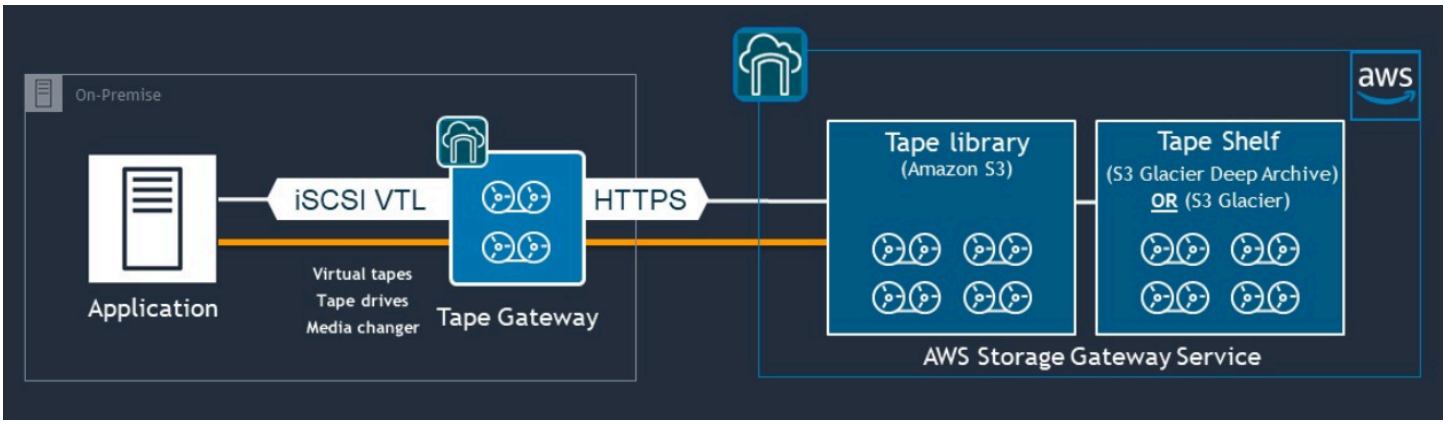
ボリューム・ゲートウェイは Amazon EC2 の Amazon EBS ボリューム機能と統合されているため、AWS Backup を使用してスナップショット・プロセスを自動化し、スケジュールすることができます。ボリュームゲートウェイには、耐久性のある Amazon S3 ベースの Amazon EBS スナップショットとタグ付け機能という利点もあります。詳細については、Amazon EBS スナップショットに関する文書を参照してください。

テープゲートウェイ

テープゲートウェイは、オフサイトの仮想テープバックアップストア用に、Amazon S3 と Amazon S3 Glacier の高い耐久性、低コストの階層型ストレージ、豊富な機能を備えています。Amazon S3 と Amazon S3 Glacier に保存されているすべての仮想テープは、地理的に分散した少なくとも 3 つのアベイラビリティーゾーンに複製および保存されます。仮想テープは 11 ナインの耐久性によって保護されます。

AWS はまた、定期的にフィキシティ・チェックを行い、データが読み取れるか、エラーが混入していないかを確認します。Amazon S3 に保存されたテープはすべて、デフォルトのキーまたはあなたの AWS KMS キーを使用したサーバー側の暗号化によって保護されます。さらに、テープの移植性に関連する物理的なセキュリティリスクを回避できます。テープゲートウェイを使用すると、正しいデータを取得できます。オフサイトでのテープの倉庫保管では、復元中に間違ったテープや壊れたテープが届く可能性があります。

Amazon S3 にデータを保存すれば、月々のストレージコストを節約できます。S3 Glacier Deep Archive アーカイブを使用すると、長期間のアーカイブ要件に合わせてさらに節約できます。



テープゲートウェイは、オンプレミス環境から、拡張性、冗長性、耐久性の高いストレージサービスにまたがる仮想テープライブラリ（VTL）として機能する：Amazon S3、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive などです。

テープゲートウェイは、仮想メディアチェンジャーと仮想テープドライブを備えたオープンスタンダード iSCSI ベースの VTL として、既存のバックアップアプリケーションにストレージゲートウェイを提示します。既存のバックアップ・アプリケーションやワークフローを使い続けながら、大規模にスケーラブルな Amazon S3 に保存された仮想テープのコレクションに書き込むことができます。仮想テープ上のデータに即時または頻繁にアクセスする必要がなくなった場合、バックアップアプリケーションはそれを S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive にアーカイブし、ストレージコストをさらに削減することができます。

S3 Glacier または S3 Glacier Deep Archive にアーカイブされているテープは、通常、それぞれ 3 ~ 5 時間または 12 時間で取得できます。テープゲートウェイは、仮想テープにアクセスするための iSCSI ベースのテープライブラリインターフェイスと互換性のあるバックアップアプリケーションで使用できます。また、テープ 1 本あたりの最小 100 GB のストレージサイズも考慮します。詳細については、テープ・ゲートウェイをサポートするサードパーティ製バックアップアプリケーションのリストを確認してください。

AWS からデータセンターへのアプリケーションのバックアップとリカバリ

クラウドベースのワークロードとオンプレミスインフラストラクチャに DR や事業継続性などのシナリオを実装するよう求めるポリシーがあるかもしれません。オンプレミスサーバー用のデータバックアップフレームワークが既にある場合は、VPN 接続または AWS Direct Connect 経由で、そのフレームワークを AWS リソースに拡張できます。EC2 インスタンスにバックアップエージェントをインストールし、データ保護ポリシーに従ってデータとアプリケーションをバックアップできます。アプリケーションレベルのバックアップを保存する中間サービスとして Amazon S3 を使用することもできます。その後、API 操作、SDK、または AWS CLI を使用して、データをオンプレミス環境にリストアすることができます。

Amazon EC2 以外の AWS サービスにあるデータをバックアップするには、AWS CLI、SDK、API 操作を使って、希望のフォーマットにデータを抽出します。次に、データを Amazon S3 にコピーし、データを Amazon S3 からオンプレミス環境にコピーします。サービスによっては Amazon S3 への直接エクスポートが可能です。例えば、Amazon RDS は Microsoft SQL Server データベースの Amazon S3 へのネイティブバックアップをサポートします。

クラウドネイティブ AWS サービスのバックアップとリカバリ

バックアップとリカバリのアプローチは、ワークロードで使用される AWS サービスを対象とする必要があります。AWS は、データを管理および操作するためのサービス固有の機能とオプションを提供します。コンソール、AWS CLI、SDK、API オペレーションを使用して、使用している AWS サービスのバックアップとリカバリを実装することができます。このガイドでは、例として Amazon RDS と Amazon DynamoDB について説明します。AWS Backup は、DynamoDB と Amazon RDS の両方をサポートしているため、要件を満たす場合は使用する必要があります。

Amazon RDS のバックアップと復旧

Amazon RDS には、データベースバックアップを自動化する機能が含まれています。Amazon RDS は、データベースインスタンスのストレージボリュームのスナップショットを作成し、個々のデータベースのみではなく、DB インスタンス全体をバックアップします。Amazon RDS を使用すると、自動バックアップ用のバックアップウィンドウを設定したり、データベースインスタンスのスナップショットを作成したり、リージョンやアカウント間でスナップショットを共有したりコピーしたりできます。

Amazon RDS には、DB インスタンスのバックアップと復元に 2 つの異なるオプションがあります。

- 自動バックアップは、DB インスタンスのポイントインタイムリカバリ (PITR) を提供します。自動バックアップは、新しい DB インスタンスを作成するとデフォルトでオンになっています。

  Amazon RDS は、DB インスタンスの作成時に定義したバックアップウィンドウ中に、データの完全バックアップを毎日実行します。自動バックアップの保存期間は最大 35 日まで設定できます。Amazon RDS はまた、DB インスタンスのトランザクションログを 5 分ごとに Amazon S3 にアップロードします。Amazon RDS は、毎日のバックアップとデータベーストランザクションログを使用して DB インスタンスを復元します。`LatestRestorableTime` (通常、最後の 5 分) までの保持期間中であれば、インスタンスを任意の秒にリストアできます。

  DB インスタンスの復元可能な最新の時刻を確認するには、`DescribeDBInstances` API 呼び出しを使用します。または、Amazon RDS コンソールの [説明] タブでデータベースを確認してください。

PITR を開始すると、トランザクションログと最も適切な日次バックアップが組み合わされ、DB インスタンスが要求された時刻に復元されます。

- DB スナップショットはユーザーが開始するバックアップであり、DB インスタンスを必要な頻度で既知の状態に復元するために使用できます。その後、いつでもその状態に復元できます。DB スナップショットを作成するには、Amazon RDS コンソールか `CreateDBSnapshot` API コールを使用します。これらのスナップショットは、コンソールまたは `DeleteDBSnapshot` API 呼び出しを使用して明示的に削除するまで保持されます。

これらのバックアップオプションはどちらも、AWS Backup に含まれる Amazon RDS でサポートされています。AWS Backup を使用して Amazon RDS データベースの標準バックアッププランを設定することを検討し、特定のデータベースのバックアッププランが独自の場合はユーザー主導のインスタンスバックアップオプションを使用することを検討します。

Amazon RDS は DB インスタンスが使用する基盤となるストレージへの直接アクセスを防ぎます。これにより、RDS DB インスタンス上のデータベースをローカルディスクに直接エクスポートすることもできなくなります。場合によっては、クライアントユーティリティを使用してネイティブのバックアップおよび復元機能を使用できます。たとえば、Amazon RDS MySQL データベースで mysqldump のコマンド実行 を使用して、データベースをローカルクライアントマシンにエクスポートできます。Amazon RDS には、データベースのネイティブバックアップと復元を実行するための拡張オプションも用意されている場合があります。例えば、Amazon RDS はSQL Server データベースの RDS データベースバックアップをエクスポートインポートするストアドプロシージャを提供しています。

バックアップと復元の全体的なアプローチの一環として、データベースの復元プロセスとそれがデータベースクライアントに与える影響を徹底的にテストします。

DNS CNAME レコードを使用して、データベース復旧中のクライアントへの影響を軽減します。

PITR または RDS DB インスタンススナップショットを使用してデータベースを復元すると、新しいエンドポイントを持つ新しい DB インスタンスが作成されます。この方法では、特定の DB スナップショットまたは特定の時点から複数の DB インスタンスを作成できます。RDS DB インスタンスを復元してライブの RDS DB インスタンスを置き換える場合は、特別な考慮事項があります。たとえば、中断や変更を最小限に抑えながら、既存のデータベースクライアントを新しいインスタンスにリダイレクトする方法を決定する必要があります。また、リストアされたデータの時間と、新しいイン

スタンスが書き込みを受け始める際のリカバリ時間を考慮することで、データベース内のデータの継続性と一貫性を確保する必要があります。

DB インスタンスのエンドポイントを指す別の DNS CNAME レコードを作成し、クライアントにこの DNS 名を使用させることができます。そうすれば、データベースクライアントを更新しなくても、復元された新しいエンドポイントを指すように CNAME を更新できます。

CNAME レコードの TTL (Time to Live) を適切な値に設定します。指定する TTL によって、別のリクエストが行われるまでレコードが DNS リゾルバーにキャッシュされる時間が決まります。DNS リゾルバやアプリケーションの中には、TTL を守らず、TTL よりも長い間レコードをキャッシュするものがあるかもしれないことに注意することが重要です。Amazon Route 53 の場合、より長い値 (たとえば、172800 秒、または 2 日間) を指定すると、DNS 再帰リゾルバがこのレコードの最新情報を取得するために Route 53 に行わなければならない呼び出しの回数を減らすことができます。これによりレイテンシーが軽減され、Route 53 サービスの請求額が削減されます。詳細については、「Amazon Route 53 によりドメインのトラフィックをルーティングする方法」を参照してください。

アプリケーションやクライアントオペレーティングシステムは DNS 情報をキャッシュする場合もあるため、新しい DNS 解決リクエストを開始して更新された CNAME レコードを取得するには、フラッシュまたは再起動する必要があります。

データベースの復元を開始し、復元したインスタンスにトラフィックを移すときは、すべてのクライアントが以前のインスタンスではなく、復元されたインスタンスに書き込んでいることを確認します。データアーキテクチャによっては、データベースの復元、DNS の更新、復元したインスタンスへのトラフィックの移行、前のインスタンスにまだ書き込まれているデータの修正がサポートされている場合があります。そうでない場合は、DNS CNAME レコードを更新する前に既存のインスタンスを停止できます。そうすれば、新しく復元したインスタンスからすべてのアクセスが可能になります。これにより、個別に処理できる一部のデータベースクライアントで接続の問題が一時的に発生することがあります。クライアントへの影響を軽減するために、メンテナンスの時間帯にデータベースを復元できます。

指数バックオフを使用して再試行してデータベース接続障害をスムーズに処理するアプリケーションを作成します。これにより、復元中にデータベース接続が使用できなくなった場合でも、アプリケーションが予期せずクラッシュすることなく、アプリケーションを回復できます。

復元プロセスが完了したら、以前のインスタンスを停止状態に保つことができます。または、セキュリティグループのルールを使用して、不要になったことを確認するまで前のインスタンスへのトラフィックを制限できます。段階的に廃止するアプローチでは、まず実行中のデータベースへのアクセ

スをセキュリティグループによって制限します。インスタンスが不要になった場合は、最終的に停止できます。最後に、データベースインスタンスのスナップショットを作成して削除します。

DynamoDB のバックアップと復旧

DynamoDB には、DynamoDB のテーブルデータをほぼ継続的にバックアップする PITR が用意されています。有効にすると、明示的にオフにするまで、DynamoDB は過去 35 日間のテーブルの増分バックアップを維持します。

また、DynamoDB コンソール、AWS CLI、または DynamoDB API を使用して、DynamoDB テーブルのオンデマンドバックアップを作成することもできます。詳細については、「DynamoDB テーブルをバックアップする」を参照してください。AWS Backup を使用して、定期的な、または今後のバックアップをスケジュールできます。または Lambda 関数を使用して、バックアップ方法をカスタマイズおよび自動化できます。DynamoDB のバックアップに Lambda 関数を使う方法については、ブログ記事「Amazon DynamoDB のオンデマンドバックアップをスケジュールするサーバーレスソリューション」を参照してください。スケジューリングスクリプトとクリーンアップジョブを作成したくない場合は、AWS Backup を使用してバックアップ計画を作成できます。バックアッププランには、DynamoDB テーブルのスケジュールと保持ポリシーが含まれます。AWS Backup は、保持スケジュールに基づいてバックアップを作成し、以前のバックアップを削除します。また AWS Backup には、低コストの階層型ストレージ、クロスアカウント、クロスリージョンコピーなど、DynamoDB サービスでは利用できない高度な DynamoDB バックアップオプションも含まれています。詳細については、「高度な DynamoDB バックアップ」を参照してください。

リストアした DynamoDB テーブルに対して、手動で以下の設定を行う必要があります:

- 自動スケーリングポリシー
- IAM ポリシー
- Amazon CloudWatch メトリクスおよびアラーム
- タグ
- ストリーム設定
- TTL 設定

バックアップから新しいテーブルにリストアできるのは、テーブルデータ全体のみです。復元されたテーブルに書き込むことができるのは、アクティブになってからです。

復元プロセスでは、新しく復元されたテーブル名を使用するようにクライアントにどのように指示するかを考慮する必要があります。設定ファイル、AWS Systems Manager パラメータストア値、また

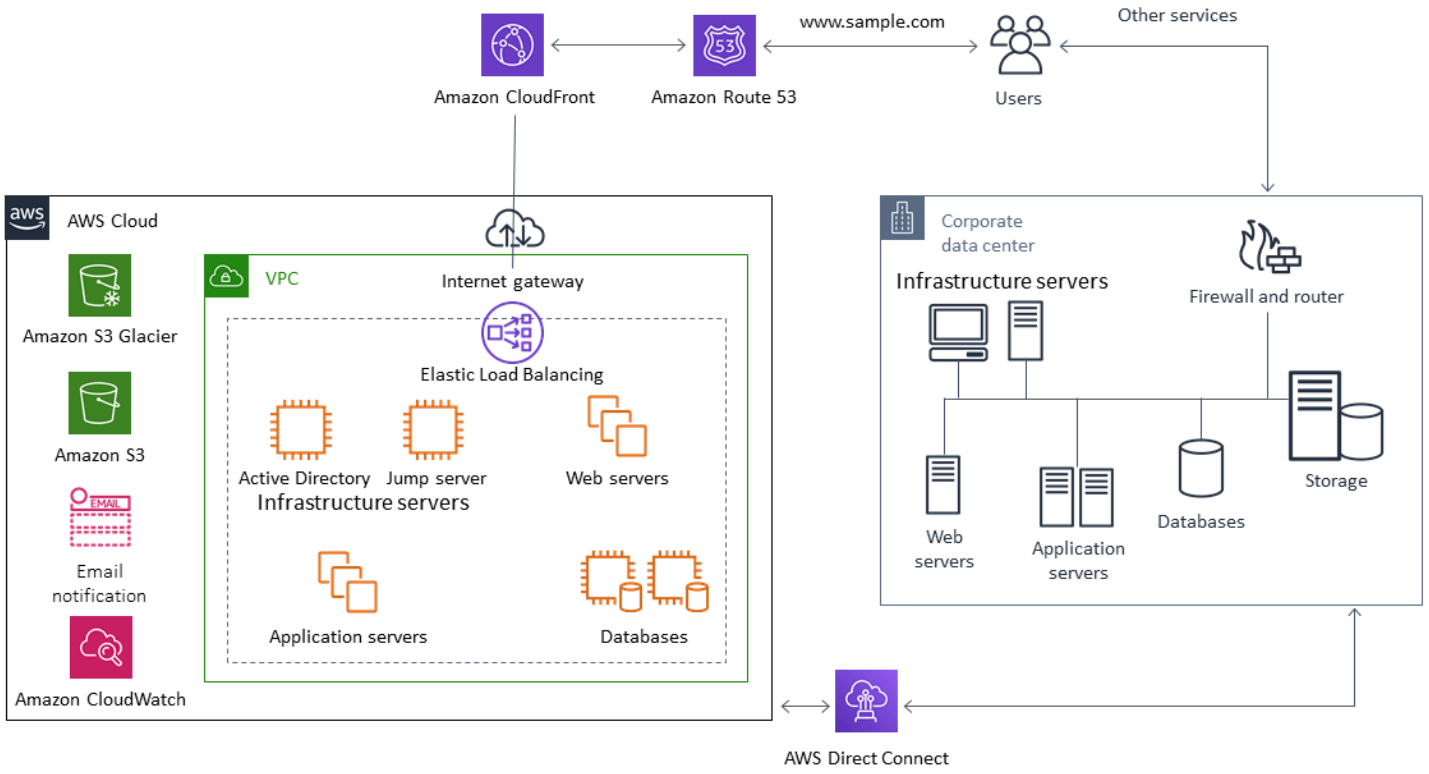
はクライアントが使用するテーブル名を反映するように動的に更新できる別の参照から DynamoDB テーブル名を取得するようにアプリケーションとクライアントを設定できます。

復元プロセスの一環として、切り替えプロセスを慎重に検討する必要があります。IAM 権限を使用して既存の DynamoDB テーブルへのアクセスを拒否し、新しいテーブルへのアクセスを許可することもできます。その後、新しいテーブルを使用するようにアプリケーションとクライアントの設定を更新できます。また、既存の DynamoDB テーブルと新しく復元した DynamoDB テーブルとの違いを調整する必要がある場合もあります。

ハイブリッドアーキテクチャのバックアップと復旧

このガイドで説明するクラウドネイティブとオンプレミスのデプロイは、ワークロード環境にオンプレミスと AWS インフラストラクチャのコンポーネントが含まれるハイブリッドシナリオに組み合わせることができます。Webサーバー、アプリケーション・サーバー、モニタリング・サーバー、データベース、Microsoft Active Directoryなどのリソースは、顧客のデータセンターか AWS でホストされます。AWS クラウドで実行されているアプリケーションは、オンプレミスで実行されているアプリケーションに接続されます。

これは企業のワークロードでは一般的なシナリオになりつつあります。多くの企業が独自の AWS データセンターを保有し、容量の増強に使用しています。これらの顧客のデータセンターは、多くの場合、大容量のネットワークリンクによって AWS ネットワークに接続されています。例えば、「AWS Direct Connect」 を使えば、オンプレミスのデータセンターから AWS へのプライベートな専用接続を確立できます。これにより、データ保護の目的でデータをクラウドにアップロードするための帯域幅と一定の待ち時間が確保されます。また、ハイブリッドワークロードでも一貫したパフォーマンスとレイテンシーを実現できます。次の図は、ハイブリッド環境アプローチの一例を示しています。



適切に設計されたデータ保護ソリューションでは、通常、このガイドのクラウドネイティブソリューションとオンプレミスソリューションで説明されているオプションを組み合わせて使用します。多く

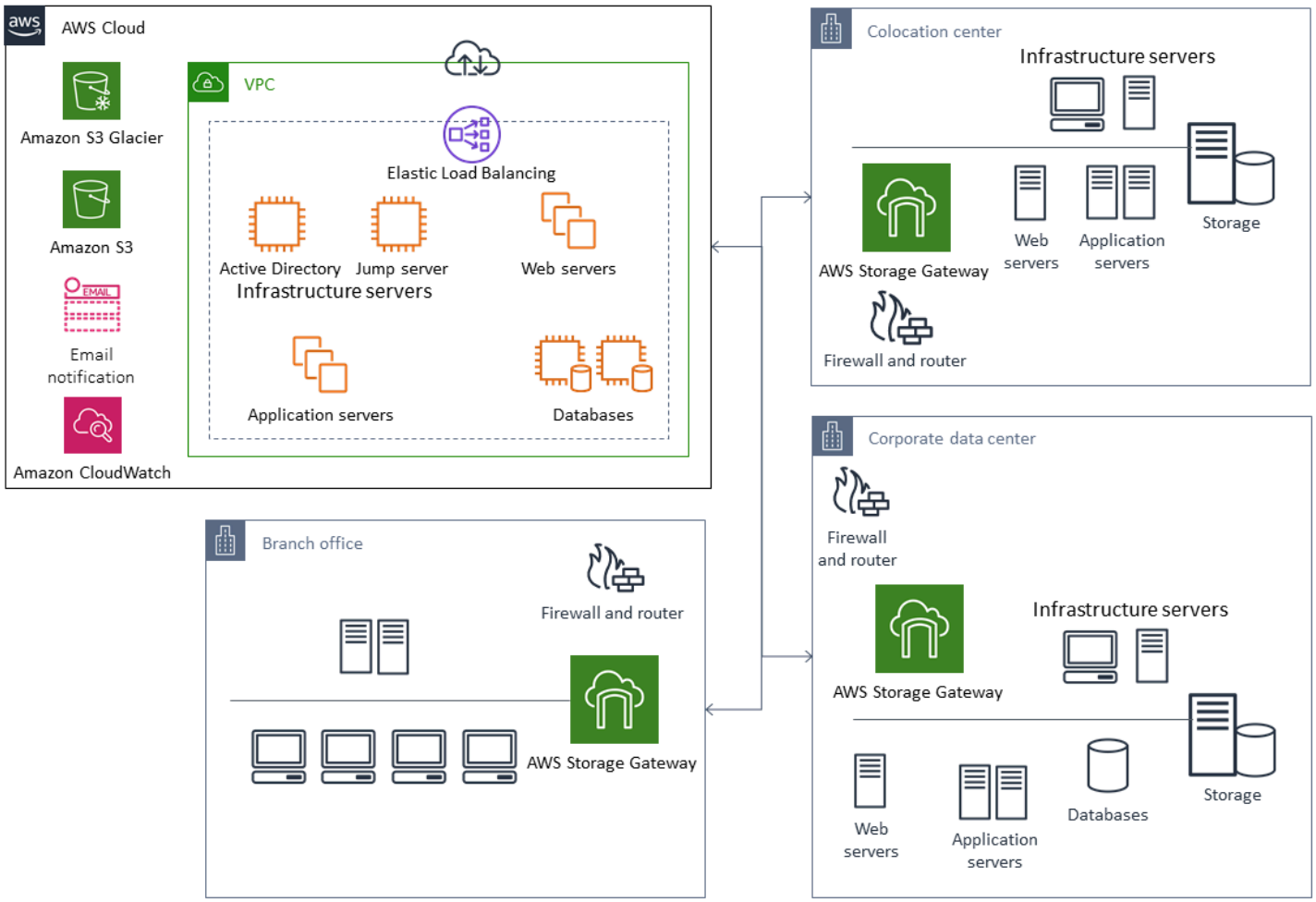
の ISV は、オンプレミスインフラストラクチャ向けに市場をリードするバックアップおよび復元ソリューションを提供しており、ハイブリッドアプローチをサポートするようにソリューションを拡張しています。

可用性を高めるため、クラウドへの一元化されたバックアップ管理ソリューションをクラウドの移行

既存のバックアップ管理ソリューションへの投資を AWS と共に使用することで、アプローチの耐障害性とアーキテクチャを向上させることができます。プライマリバックアップサーバーと 1 台以上のメディアサーバーまたはストレージサーバーを、保護対象のサーバーやサービスに近い複数の場所にオンプレミスに配置している場合があります。このような場合は、プライマこの場合、プライマリバックアップサーバーを EC2 インスタンスに移行し、オンプレミスの災害から保護し、高可用性を確保することを検討します。

バックアップデータフローを管理するには、保護するサーバーと同じリージョンの EC2 インスタンスに 1 つ以上のメディアサーバーを作成できます。EC2 インスタンスの近くにあるメディアサーバーは、インターネット転送にかかる費用を節約できます。Amazon S3 または Amazon S3 Glacier にバックアップすると、メディアサーバーはバックアップとリカバリの全体的なパフォーマンスを向上させます。

また、Storage Gateway を使用して、地理的に分散したデータセンターやオフィスからのデータへの一元的なクラウドアクセスを提供することもできます。例えば、ファイル・ゲートウェイは、世界中に広がるアプリケーション・ワークフローのために、AWS に保存されたデータへのオンデマンドで低遅延なアクセスを可能にします。キャッシュの更新などの機能を使用して地理的に分散した場所のデータを更新できるため、オフィス間でコンテンツを簡単に共有できます。


AWS Cloud
Amazon S3 Glacier
Amazon S3
Email notification
Amazon CloudWatch
VPC
Elastic Load Balancing
Active Directory
Jump server
Infrastructure servers
Web servers
Application servers
Databases
Colocation center
Infrastructure servers
AWS Storage Gateway
Web servers
Application servers
Storage
Firewall and router
Corporate data center
Firewall and router
AWS Storage Gateway
Infrastructure servers
Web servers
Application servers
Databases
Storage
Branch office
Firewall and router
AWS Storage Gateway

AWSによる ディザスタリカバリ

バックアップと復元のアプローチとそれをサポートするサービスとテクノロジーを使用して、ディザスタリカバリ (DR) ソリューションを実装できます。多くの企業が AWS クラウドをバックアップとリストア、そして DR サイトとして利用している。AWS は、DR と事業継続をサポートする多くのサービスと機能を提供しています。

トピック

- AWS へのオンプレミス DR
- クラウドネイティブワークロードの DR

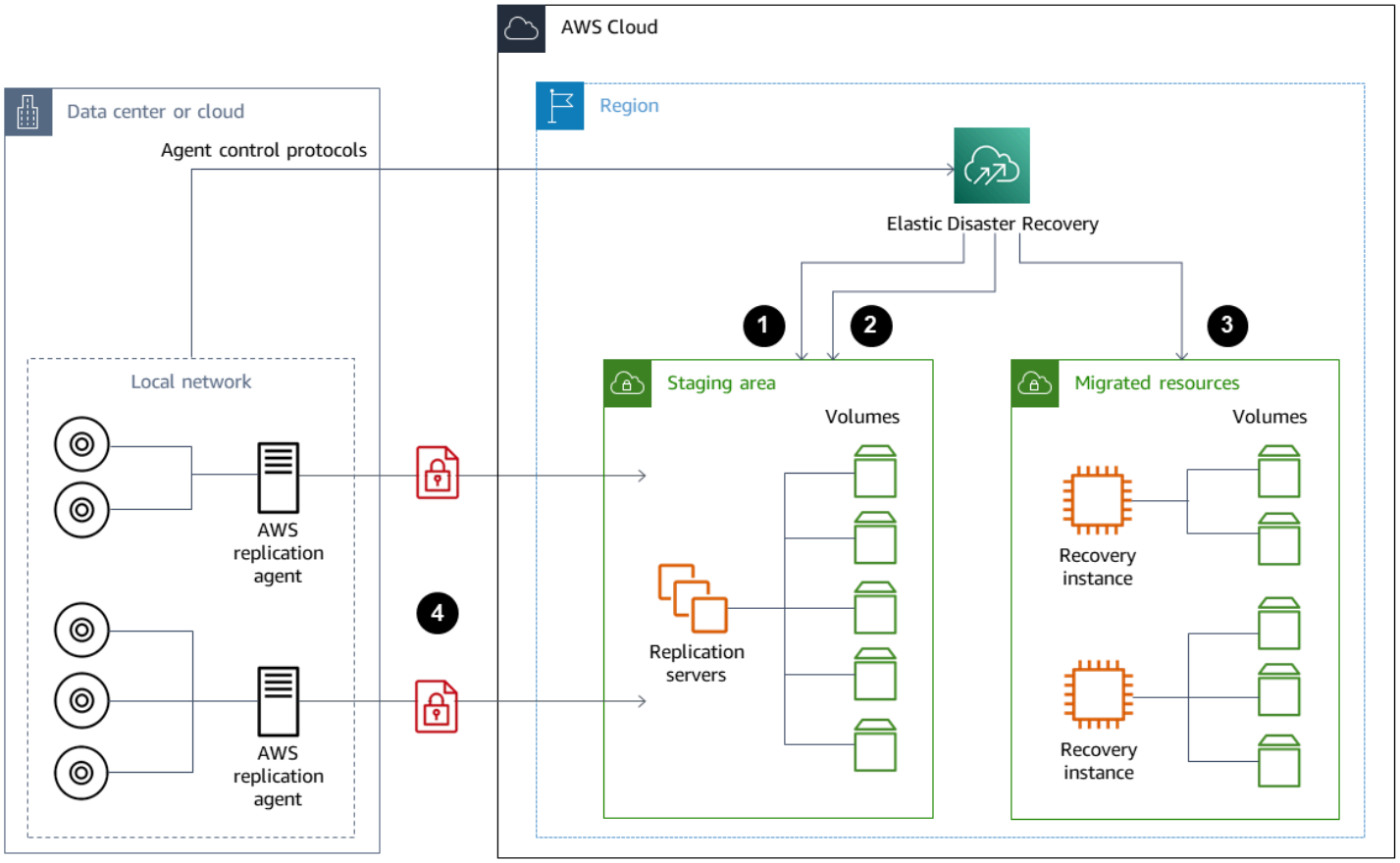
AWS へのオンプレミス DR

AWS をオンプレミス· ワークロードのオフサイト· ディザスタリカバリ (DR) 環境として使用することは、一般的なハイブリッド· シナリオです。使用するテクノロジーを選択する前に、必要な復旧時間や復旧時点の目標などの DR 目標を明確にします。この定義に役立つのは、「DR 計画チェックリスト」を使用することです。

AWS には、DR 環境を迅速にセットアップしてプロビジョニングするのに役立つオプションが多数用意されています。ワークロードの依存関係をすべて考慮し、DR 計画とソリューションを徹底的かつ定期的にテストして整合性を検証すること。

AWS は、ルートボリュームとオペレーティングシステムを含むオンプレミスサーバーの完全なレプリカを AWS 上に作成するための「AWS Elastic Disaster Recovery」 を提供します。Elastic Disaster Recoveryは、対象となるAWSアカウントと優先 AWS リージョン にある低コストのステージング· エリアに、マシンを継続的にレプリケートします。ブロックレベルのレプリケーションは、オペレーティングシステム、システム状態設定、データベース、アプリケーション、ファイルを含む、サーバーのストレージの正確なレプリカです。災害が発生した場合、Elastic Disaster Recoveryに指示して、数千台のマシンを数分で完全にプロビジョニングされた状態で迅速に起動させることができます。

Elastic Disaster Recoveryは、オンプレミスの各サーバーにインストールされたエージェントを使用します。エージェントは、オンプレミスサーバーの状態を、AWS 上で稼働している低性能の Amazon EC2 サーバーと同期させます。また、伸縮性ディザスタリカバリでは、DR のフェイルオーバーとフェイルバックのプロセスを自動化することもできます。フェイルオーバーとフェイルバックのプロセスを自動化することで、目標復旧時間 (RTO) をより短く、より一貫性のあるものにすることができます。



1. レプリケーションサーバーのステータスレポート
2. ステージングエリア、リソースは自動的に作成され、終了されます。
3. RTO が分、RPO が秒で起動されたリカバリインスタンス
4. 継続的なブロックレベルのレプリケーション（圧縮および暗号化）

DR プロセスをテストし、ライブステージング環境がオンプレミス環境とコンフリクトを起こさないことを確認することが重要です。たとえば、オンプレミス、ステージング、開始した DR 環境で、適切なライセンスが利用可能で機能していることを確認します。また、作業をポーリングして中央データベースから取得する可能性のあるワーカータイプのプロセスが、重複や競合を避けるために適切に設定されていることも確認します。DR プロセスには、復旧用サーバーインスタンスをオンラインにする前に実行する必要のある必要な手順をすべて含めます。また、復旧用サーバーインスタンスがオンラインで利用可能になった後に実行する手順も含めます。「AWS Elastic Disaster Recovery 計画自動化ソリューション」のようなソリューションや、DR計画の自動化を支援する別のアプローチを使うことができます。

「Storage Gateway ボリュームゲートウェイ」を使用して、オンプレミスサーバーにクラウドベースのボリュームを提供できます。これらのボリュームは、Amazon EBS スナップショットを使用して Amazon EC2 で使用できるようにすばやくプロビジョニングすることもできます。特に、ストアドボリュームゲートウェイは、オンプレミスアプリケーションにデータセット全体への低レイテンシーアクセスを提供します。ボリュームゲートウェイは、オンプレミスまたは Amazon EC2 で使用するために復元できる、耐久性のあるスナップショットベースのバックアップも提供します。ワークロードのリカバリポイント目標（RPO）に基づいて、ポイントインタイムスナップショットをスケジュールできます。

> **Important**
>
> ボリュームゲートウェイボリュームは、ブートボリュームとしてではなくデータボリュームとして使用することを目的としています。

オンプレミスのサーバーと同じ構成のAmazon EC2 Amazon Machine Image（AMI）を使用し、データボリュームを個別に指定することができます。AMI を設定してテストしたら、ボリュームゲートウェイのスナップショットに基づくデータボリュームとともに AMI から EC2 インスタンスをプロビジョニングします。このアプローチでは、特に Windows ワークロードの場合、EC2 インスタンスが適切に動作していることを確認するために、環境を徹底的にテストする必要があります。

クラウドネイティブワークロードの DR

クラウドネイティブのワークロードが DR 目標とどのように関連しているかを検討してください。AWS は、世界中のリージョンに複数のアベイラビリティーゾーンを提供します。AWSクラウドを使用している多くの企業は、アベイラビリティ ゾーンの喪失に耐えられるようにワークロード アーキテクチャと DR の目標を調整しています。AWS Well-Architected Frameworkの「信頼性の柱」は、このベストプラクティスをサポートしています。複数のアベイラビリティーゾーンを使用するように、ワークロードとそのサービスとアプリケーションの依存関係を構築できます。そうすれば、DR を自動化して DR の目標を最小限またはまったく行わずに達成できます。

しかし実際には、すべてのコンポーネントについて、冗長でアクティブで自動化されたアーキテクチャを確立できない場合があります。アーキテクチャのすべてのレイヤーを調べて、目標を達成するために必要な DR プロセスを判断します。これはワークロードによって異なり、アーキテクチャやサービスの要件も異なる可能性があります。このガイドでは、Amazon EC2 の考慮事項とオプションについて説明します。その他の AWS サービスについては、「AWS のドキュメント」を参照して、高可用性とDRのオプションを決定することができます。

単一のアベイラビリティ・ゾーンにおける Amazon EC2 の DR

複数のアベイラビリティーゾーンのクライアントを積極的にサポートし、サービスを提供するようにワークロードを設計するようにします。Amazon EC2 Auto Scaling と Elastic Load Balancing を使用して、Amazon EC2 やその他のサービスのマルチ AZ サーバーアーキテクチャを実現できます。

使用しているアーキテクチャに、負荷分散できない EC2 インスタンスがあり、常に 1 つのインスタンスしか実行できない場合は、以下のオプションのいずれかを使用できます。

- 最小、最大、および希望するサイズが1であり、複数の可用性ゾーン用に構成されたAuto Scaling グループを作成します。障害が発生した場合にインスタンスの交換に使用できる AMI を作成します。AMI から新しくプロビジョニングされたインスタンスが自動的に構成され、サービスを提供できるように、適切な自動化と構成を定義していることを確認します。Auto Scaling グループを指し、複数のアベイラビリティーゾーン用に設定されたロードバランサーを作成します。オプションで、ロードバランサーエンドポイントを指す Amazon Route 53 エイリアスを作成します。
- アクティブなインスタンスの Route 53 レコードを作成し、クライアントにこのレコードを使用して接続させます。アクティブなインスタンスの新しい AMI を作成し、その AMI を使用して、別のアベイラビリティゾーンに停止状態の新しい EC2 インスタンスをプロビジョニングするスクリプトを作成します。スクリプトを定期的に実行し、以前に停止したインスタンスを終了するように設定します。アベイラビリティーゾーンに障害が発生した場合は、代替のアベイラビリティーゾーンでバックアップインスタンスを起動します。次に、この新しいインスタンスを指すように Route 53 レコードを更新します。

ソリューションが防ぐように設計された障害をシミュレートして、ソリューションを徹底的にテストします。また、ワークロードアーキテクチャが変更されたときに DR ソリューションが必要とする更新についても検討します。

Amazon EC2 の地域障害時の DR

AWS リージョンの破綻はまれだが、AWS リージョンが将来破綻する可能性はあります。お客様は、マルチリージョン DR プランを確立して維持するために必要な複雑さ、コスト、労力と、メリットを慎重に比較検討する必要があります。AWS は、グローバルな可用性、フェイルオーバー、DR のために、マルチリージョンアーキテクチャをサポートする機能を提供しています。このガイドでは、Amazon EC2 のバックアップとリカバリに特有の機能のいくつかについて説明します。

AWS AMI と Amazon EBS スナップショットは、1 つのリージョン内で新しいインスタンスをプロビジョニングするために使用できるリージョンリソースです。ただし、スナップショットと AMI を別のリージョンにコピーし、それらを使用してそのリージョンに新しいインスタンスをプロビジョ

ニングすることはできます。リージョンの障害 DR プランをサポートするために、AMI とスナップショットを他のリージョンにコピーするプロセスを自動化できます。AWS Backup と Amazon Data Lifecycle Manager は、バックアップ設定の一部としてクロスリージョンコピーをサポートします。

「AWS Elastic Disaster Recovery」は、あるリージョンの Amazon EC2 サーバーを自動化し、別の DR リージョンに継続的に複製するために使用できます。Elastic Disaster Recoveryは、マルチリージョンDRアプローチを簡素化し、ドリルを使用してクロスリージョンAmazon EC2 DRプランを定期的にテストするのに役立ちます。Elastic Disaster Recoveryは、バックアップとリカバリが RTO と RPO の目標を達成できない場合に役立ちます。Elastic Disaster Recovery は、RTO を数分に、RPO を 1 秒未満に抑えるのに役立ちます。

どのソリューションを使用する場合でも、障害発生時に使用するプロビジョニング、フェイルオーバー、フェイルバックのプロセスを決定する必要があります。Route 53 をヘルスチェックとドメインネームシステムのフェイルオーバーと組み合わせて使用すると、ソリューションをサポートしやすくなります。

バックアップをクリーンアップする

コストを削減するには、復元や保存の目的で不要になったバックアップをクリーンアップしてください。AWS Backup と Amazon Data Lifecycle Manager を使用して、バックアップの一部の保存ポリシーを自動化できます。しかし、このようなツールがあっても、個別に取得したバックアップのクリーンアップアプローチは必要です。

タグ付け戦略はクリーンアップ戦略の前提条件です。タグ付けを使用してクリーンアップすべきリソースを特定し、所有者に適切に通知し、クリーンアッププロセスを自動化します。AWS によって作成されたバックアップには作成日が設定されていますが、バックアップをワークロード、保存要件、および復元ポイントの識別に関連付けるにはタグ付けが重要です。

自動化を使用してスナップショットのクリーンアッププロセスを実装できます。たとえば、スナップショットのアカウントをスキャンして、対応するボリュームがアタッチ状態か利用可能状態かを判断できます。指定した時間のしきい値で結果をさらに絞り込むことができます。ボリュームにアタッチされたタグを使用して、スナップショットの所有者に E メールを自動送信して、そのスナップショットの削除が予定されていることを警告できます。この自動修正は、AWS Config ルール、AWS CLI を使用するスクリプト、または AWS SDK を使用する Lambda 関数を使用して実装できます。

Systems Manager は、AWS-DeleteEBSVolumeSnapshots および AWS-DeleteSnapshot ドキュメントを提供し、Amazon EBS スナップショットのクリーンアップの開始と自動化を支援します。AWS CLI および AWS SDK を使用して Amazon RDS スナップショットなどの他の AWS リソースのクリーンアップを自動化することもできます。

バックアップとリカバリ FAQ

どのバックアップスケジュールを選択すればよいですか?

目標復旧時点RPO) に沿ったバックアップスケジュールの頻度を定義します。ワークロードの負荷が最も小さく、ユーザーへの影響を軽減できるバックアップ時間を定義します。ワークロードに大きな変更を加える予定があるときはいつでも、ポイントインタイムスナップショットを作成します。

開発用アカウントにバックアップを作成する必要がありますか?

開発アカウントで、ワークロードを破壊する可能性のある変更をテストし、破壊する変更を実行する前にバックアップを作成します。開発およびテスト活動から、開発アカウントと非本番アカウントには、さらに多くのポイントインタイムリカバリ (PITR) バックアップがあるかもしれません。

スナップショットの作成中にアプリケーションをアップグレードし、EBS ボリュームの使用を継続しても影響はありませんか。

スナップショットは非同期に行われる。ポイントインタイムのスナップショットはすぐに作成されるが、スナップショットのステータスは、すべての変更されたブロックが Amazon S3 に転送されるまで保留されます。最初の大きなスナップショットや、多数のブロックが変更された後続のスナップショットの場合、転送には数時間かかることがあります。転送中、進行中のスナップショットは、ボリュームへの進行中の読み書きの影響を受けません。詳細については、AWS ドキュメントを参照してください。

次のステップ

まず、バックアップとリカバリのアプローチを非運用環境で評価、実装、テストすることから始めます。リカバリプロセスを徹底的にテストし、復元したワークロードが想定どおりに動作していることを確認することが重要です。

アーキテクチャ内のすべてのコンポーネントに加えて、アーキテクチャ内の 1 つのコンポーネントについてもリカバリプロセスをテストします。それぞれのリカバリ時間を検証してください。また、バックアップと復元のプロセスが上流と下流の依存関係に与える影響も検証してください。サービス停止がアップストリームの依存関係に与える影響を確認し、ダウンストリームのバックアップへの影響を確認します。

その他のリソース

AWS リソース

- AWS 規範ガイダンス
- AWS ドキュメント
- AWS 全般のリファレンス
- AWS 用語集

AWS サービス

- AWS Backup
- Amazon CloudWatch
- Amazon CloudWatch Events
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- IAM
- Amazon RDS
- Amazon S3
- Amazon S3 Glacier
- Storage Gateway
- AWS Systems Manager

その他のリソース

- AWS Backup によるバックアップとリカバリー（ソリューション）
- AWS 上のワークロードのディザスターリカバリー： クラウドにおけるリカバリ（ホワイトペーパー）
- ディザスタリカバリシリーズ（AWS アーキテクチャのブログ記事）
- DR 計画チェックリスト

- AWS を使用したバックアップとリカバリーのアプローチ（テクニカルペーパー — アーカイブ済み）
- AWS Backup の開始方法
- AWS Marketplace — バックアップとリストア

ドキュメント履歴

このガイドは、このドキュメントの大きな変更点をまとめたものです。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
更新した情報	「オンプレミスDRから AWS へ」のセクションの情報を更新しました。	2023 年 4 月 13 日
セクションを追加しました	スナップショットから「インスタンスを作成または復元する」ためのガイダンスと手順を追加しました。	2023 年 3 月 7 日
Elastic Disaster Recovery に関する情報を追加し、説明を追加しました	「AWS によるディザスタリカバリ」と「データ保護のための AWS サービスの選択」のセクションに、AWS Elastic Disaster Recovery に関する情報を追加しました。「スナップショットと AMI を使用した Amazon EC2 のバックアップとリカバリ」、「スナップショットまたは AMI を作成する前に EBS ボリュームを準備する」、「Amazon EBS スナップショットまたは AMI からリストアする」のセクションで、説明を追加しました。バックアップとリカバリ FAQ に追加されました。	2023 年 1 月 19 日
リンクを追加しました	Amazon Data Lifecycle Manager セクションに Amazon DataLifecycle	2022 年 10 月 31 日

	Manager のドキュメントへのリンクを追加しました。	
更新した情報	「ボリュームの復元」に関する情報を更新しました。	2022 年 8 月 30 日
情報を更新し、新しいセクションを追加しました	「データ保護 AWS サービスの選択」セクションに、サービスを追加しました。「AWS Backup を使用したバックアップとリカバリ」セクションを追加しました。「Amazon S3 と Amazon S3 Glacier を使用したバックアップとリカバリー」セクションに、新しい Amazon S3 Glacier ストレージクラスに関する情報を追加しました。「EBS ボリュームを使用した Amazon EC2 のバックアップとリカバリ」セクションに、ドキュメントと追加情報へのリンクを追加しました。「AWS クラウドネイティブサービスのバックアップとリカバリ」セクションに、AWS Backup の使用に関する推奨事項を追加しました。「その他のリソース」セクションに、リソースを追加しました。	2022 年 1 月 28 日

更新した情報	ストレージクラスの設定に関する情報を「S3 Glacier フレキシブル検索」セクションに追加しました。スナップショットの取得に関する情報を「スナップショットと AMI によるAmazon EC2 バックアップとリカバリ」セクションに追加しました。	2021 年 9 月 9 日
更新した情報	AWS Backup セクションに、AWS Backup がサポートする AWS サービスに関する情報を追加しました。	2021 年 6 月 1 日
初版発行	—	2020 年 7 月 29 日

AWS 規範的ガイダンスの用語集

以下は、AWS 規範的ガイダンスによって提供される戦略、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する。
- 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: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 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: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- 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: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 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の購入、アプリケーションの書き換え、お客様の既存のオペレーションの変更を行うことなく、インフラストラクチャをクラウドに移行できます。この移行シナリオは AWS の VMware Cloud に固有のもので、お客様のオンプレミス環境と、および AWS の間の仮想マシン (VM) 互換性とワークロードの移植性をサポートします。インフラストラクチャを AWS の VMware Cloud に移行するときに、お客様のオンプレミスのデータセンターから VMware Cloud Foundation テクノロジーを使用できます。例: AWS の Oracle データベースをホストしているハイパーバイザーを VMware Cloud 上に再配置する。
- 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

「不可分性、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。アクティブ/パッシブ移行よりも柔軟性がありますが、より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

行のグループを操作し、グループの単一の戻り値を計算するための SQL 関数。集計関数の例には、 SUMや などがあります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

繰り返し発生する問題に対して、そのソリューションが逆効果であったり、効果がなかったり、代替ソリューションよりも効果が低かったりする場合によく使用されるソリューション。

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AWS の ABAC とは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

AWS リージョン 内の仕切られた場所は、他のアベイラビリティーゾーンに障害が発生してもその影響を受けず、低コスト、低レイテンシーで同一リージョン内の他のアベイラビリティーゾーンに接続できます。

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドに正常に移行するための効率的で効果的な計画を立てるのを支援する AWS から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。AWSCAF 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、運用の観点と呼ばれる 6 つの重点を置く分野にガイダンスを編成しています。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、クラウドの導入を成功させるための組織の準備を支援するために、人材開発、トレーニング、コミュニケーションに関する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 ワークロード資格フレームワーク (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、作業の見積もりを提供するツール。AWSWQF は AWS Schema Conversion Tool (AWS SCT) と共に含まれます。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

BCP

「ビジネス継続性計画」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、「ブランチについて (GitHub ドキュメント) 」を参照してください。

ブレーククロスアクセス

例外的な状況や承認されたプロセスでは、ユーザーが通常アクセス許可AWS アカウントを持たない 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、 AWS Well-Architected ガイダンスの「Break Glass 手順の実装」インジケータ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。

CCoE

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

CDC

「変更データキャプチャ」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os エンジニアリング

システムの耐障害性をテストするために、意図的に障害や破壊的なイベントを導入する。AWS Fault Injection Service (AWS FIS) を使用して、AWSワークロードに負荷を掛け、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

ターゲットの AWS のサービス が受け取る前に、データをローカルで暗号化すること。

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 の投稿 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、エッジコンピューティングテクノロジーに一般的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、AWS クラウドへの移行時に通常実行する 4 つの段階。

- 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 Stephen Orban が AWS クラウドエンタープライズ戦略ブログの クラウドファーストジャーニーと導入ステージ というブログ記事で定義したものです。これらが、AWS 移行戦略とどのような関係があるかについては、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AWS CodeCommit。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

画像内の人物、場所、物を人間と同等以上の精度で識別するために機械が使用するAIの分野です。多くの場合、深層学習モデルを使用して構築され、1 つの画像または一連の画像からの有用な情報の抽出、分析、分類、理解を自動化します。

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

組み合わせることで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できる、AWS Config ルールと修復アクションのコレクション。コンフォーマンスパックは、1 つのエンティティとして AWS アカウント とリージョンに、または YAML テンプレートを使用して組織全体にデプロイできます。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。

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一要素です。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。AWS クラウド でデータ最小化を実践することで、プライバシーリスク、コスト、分析の二酸化炭素排出量を削減することができます。

データ境界

信頼できる ID だけが想定されるネットワークから信頼できるリソースにアクセスできるようにするAWS一連の予防ガードレール。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。通常、データウェアハウスには大量の履歴データが含まれており、クエリや分析には通常使用されます。

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。

defense-in-depth

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 AWS に採用すると、AWS Organizations 構造内の各層に複数のコントロールが追加され、リソースの安全を維持できます。例えば、 defense-in-depth アプローチは多要素認証、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

AWS Organizations では、互換性のあるサービスは AWS メンバーアカウントを登録することで、組織のアカウントやそのサービスのアクセス許可を管理できるようになります。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。

デプロイメント

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子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よく使用されます。

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。

での災害対策

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、 Well-Architected Framework ドキュメントの「Disaster recovery options in the cloud」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逸脱の追跡。例えば、 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、 AWS Control Towerを使用してガバナンス要件への準拠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

「調査データ分析」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。

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。エンドポイントサービスは AWS PrivateLink を使って作成でき、アクセス許可を他の AWS アカウントまたは AWS Identity and Access Management (IAM) プリンシパルに付与することができます。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。例えば、AWS CAF セキュリティエピックには、アイデンティティとアクセスの管理、検出型制御、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。

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 内の中央テーブル。事業運営に関する量子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 種類の列が含まれます。

フェイルファスト

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

障害分離境界

ではAWS クラウド、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。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、「 による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。

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。

G

Geo ブロック

「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)

Amazon では CloudFront、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最新の推奨アプローチです。

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 AWS Security Hub、 GuardDuty、Amazon Inspector AWS Trusted Advisor、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 。

高可用性

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) システムを近代化し、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。

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。その緊急性により、通常は一般的な DevOps リリースワークフローの外部で修正が行われます。

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している、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

「産業分野における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、本番稼働用ワークロードに新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラ

クチャは、本質的にミュータブルな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「イミュータブルなインフラストラクチャのベストプラクティスを使用したデプロイ」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内で、アプリケーション外部からの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内で、(同一または異なる AWS リージョン の) VPC、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 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。

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、「AWS を使用した機械学習モデルの解釈」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、Well-Architected の、スケーラブルで安全なマルチアカウント 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。

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。

マネージドサービス

AWS のサービス が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、プラットフォームをAWS運用し、ユーザーが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する対象になります。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。

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、結果を検査して調整を行う完全なプロセス。メカニズムとは、動作中に自身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「Building mechanisms」を参照してください。

メンバーアカウント

AWS Organizations の組織に含まれる管理アカウント以外の、すべての AWS アカウント。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。

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てマイクロサービスを統合する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、AWS でのマイクロサービスの実装を参照してください。

Migration Acceleration Program (MAP)

組織がクラウドへの移行の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、オペレーション、ビジネスアナリストと所有者、移行エンジニア、デベロッパー、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、ターゲットサブネット、セキュリティグループ、AWS アカウントが挙げられます。

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 への移行を再ホストする。

Migration Portfolio Assessment (MPA)

AWS クラウド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。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、すべての人に無料で利用できる AWS コンサルタントと APN パートナーコンサルタントです。

移行準備状況評価 (MRA)

組織のクラウド対応状況に関するインサイトを獲得し、長所と短所を特定し、AWS CAF を使用して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 AWS クラウドに移行するために使用するアプローチ。詳細については、この用語集の「7 Rs エントリ」と「組織の準備を行っ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。

MPA

「移行ポートフォリオ評価」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、AWS クラウドのアプリケーションのモダナイズ戦略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、AWS クラウドで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評価する 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。

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。

変更可能な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。一貫性、信頼性、予測可能性を向上させるために、 AWS Well-Architected フレームワークでは、イミュータブルインフラストラクチャをベストプラクティスとして使用することをお勧めします。

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

「組織の変更管理」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。

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 (TAK)

インシデントや障害の可能性の範囲を理解、評価、防止、または縮小するのに役立つ質問と関連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「運用準備状況レビュー (TAK)」を参照してください。

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

AWS Organizations 内の一組織の、すべての AWS アカウント のイベントをすべてログ記録している AWS CloudTrail が作成した証跡。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、 ドキュメントの「組織の証跡の作成」を参照してください。 CloudTrail

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更のスピードから、このフレームワークは 人材の高速化 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)

では CloudFront、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためにアクセスを制限するための拡張オプションです。OAC は、すべての AWS リージョン のすべての S3 バケット、AWS KMS (SSE-KMS) を使用したサーバー側の暗号化、S3 バケットへのダイナミックな PUT および DELETE リクエストをサポートしています。

オリジンアクセスアイデンティティ (OAI)

では CloudFront、Amazon S3 コンテンツを保護するためにアクセスを制限するオプションです。OAI を使用する場合、 は Amazon S3 が認証できるプリンシパル CloudFront を作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。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。

TAK

「運用準備状況レビュー」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、アプリケーションの内部から開始し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。

ポリシー

アクセス許可の定義 (アイデンティティベースのポリシー を参照)、アクセス条件の指定 (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の定義 AWS Organizations (サービスコントロールポリシー を参照) が可能なオブジェクト。

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。通常`false`、 `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および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てリソースにアクセスできる AWS 内のエンティティです。このエンティティは、通常は AWS アカウント のルートユーザー、IAM ロール、ユーザーのいずれかになります。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

エンジニアリングプロセス全体を通してプライバシーを考慮に入れたシステムエンジニアリングのアプローチ。

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

非準拠の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「 での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

本番環境

「環境」を参照してください。

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。

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、相談、報告 (RACI)」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、相談、報告 (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)

RPO とは、データが最後に復旧した時点を起点とする経過時間の、許容される値のことです。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)

RTO とは、サービスが中断してから復旧するまでに経過した時間 (遅延) の、許容される値のことです。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的な領域内の 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、レジリエンスを実現するために他のリージョンと分離され、独立しています。詳細については、AWS 全般のリファレンス の「Managing AWS リージョン」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。

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。

ローテーション

定期的にシークレットを更新して、攻撃者が認証情報にアクセスするのをより困難にするプロセス。

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 (IdPs) が使用するオープンスタンダード。この機能では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、組織内の全員に IAM のユーザーを作成しなくても、ユーザーが AWS Management Console にログインしたり AWS API オペレーションを呼び出したりできます。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。

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

ではAWS Secrets Manager、暗号化された形式で保存する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された情報。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、単一の文字列、または複数の文字列です。詳細については、Secrets Manager ドキュメントの「シークレット」を参照してください。

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、主に予防的 、検出的 、応答性 、プロアクティブ の 4 つのタイプがあります。

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正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。これらのオートメーションは、セキュリティのベストプラクティスの実装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には、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、認証情報のローテーションなどがあります。

サーバー側の暗号化

データを受信した AWS のサービス によって、送信先でデータが暗号化されること。

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 (SCP)を参照してください。

サービスエンドポイント

AWS のサービス のエントリポイントの URL。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、サービスのヘルスを表すターゲットメトリクス。

責任共有モデル

ユーザーが、クラウドセキュリティとコンプライアンスに関する責任を AWS と共有するモデルのこと。AWS はクラウド自体のセキュリティに対して責任を負い、ユーザーはクラウド内のセキュリティに対して責任を負います。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単一の重要なコンポーネントの障害。

SLA

「サービスレベルアグリーメント」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。

split-and-seed 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なアプローチ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。

star スキーマ

トランザクションデータまたは測定データを保存するために 1 つの大きなファクトテーブルを使用し、データ属性を保存するために 1 つ以上の小さなディメンションテーブルを使用するデータベースの組織構造。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。

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

潜在的な問題を検出したり、パフォーマンスを監視したりするために、ユーザーインタラクションをシミュレート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。

T

タグ

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「Transit Gateway 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

AWS Organizations の組織およびそのアカウントで、ユーザーに代わって指定したサービスにタスクを実行させるためにアクセス許可を付与すること。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、AWS Organizations ドキュメントのAWS Organizations を他の AWS サービスと併用する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 つのピザを供給できる小規模な 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、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禁止するストレージモデル。認可されたユーザーは、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、イミュータブルな 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、通常はマルウェアです。

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。

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。