でのバックアップ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: でのバックアップとリカバリのアプローチ AWS

Table of Contents

でのバックアップとリカバリのアプローチ AWS

Khurram Nizami、Amazon Web Services (AWS)

2024 年 6 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、目標復旧時間 (RTO)、目標復旧時点 (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、アーキテクチャのイミュータブルでないコンポーネント用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、関連する 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、イミュータブルアーキテクチャを使用するようにワークロードをモダナイズし、コンポーネントのバックアップとリカバリの必要性を減らすことです。 は、イミュータブルアーキテクチャを実装し、バックアップとリカバリの必要性を減らすために、次のような多くのサービス AWS を提供します。

- を使用したサーバーレス AWS Lambda
- Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS)、および を使用するコンテナ AWS Fargate
- Amazon Elastic Compute Cloud (Amazon EC2) とAmazon マシンイメージ (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：

- データ保護のための AWS 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 を使ったバックアップとリカバリー
- 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
- オンプレミスインフラストラクチャから へのバックアップとリカバリ AWS
- 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復旧
- ハイブリッドアーキテクチャのバックアップと復旧
- によるディザスタリカバリ AWS
- バックアップをクリーンアップする

をデータ保護プラットフォーム AWS として使用する理由

AWS は、安全で高性能、柔軟性、コスト削減、easy-to-use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およびリカバリソリューションの作成、実装、管理に必要な差別化されていない重労働に対処します。

データ保護戦略 AWS の一部として を使用することには、多くの利点があります。

- 耐久性: Amazon Simple Storage Service (Amazon S3) と S3 Glacier Deep Archive は、99.999999999 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ー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、ストレージおよびエクスポート/インポートオペレーションに Amazon S3 を使用します。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: 転送中および保管中のアクセスコントロールとデータ暗号化のための多くのオプション AWS を提供します。
- グローバル infrastructure: AWS services は世界中で利用できるため、コンプライアンスとワークロードの要件を満たす リージョンにデータをバックアップして保存できます。
- Compliance: AWS infrastructure は、以下の標準への準拠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計画に簡単に適合させることができます。
  - 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: では AWS、容量について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 オペレーションの規模により、サービスコストが削減され、AWS サービスの TCO が削減されます。 は、これらのコスト削減を価格の低下を通じて顧客に AWS 引き渡します。
- Pay-as-you-go料金: 必要に応じて、使用予定の期間のみ AWS サービスを購入します。 AWS 料金には前払い料金、終了ペナルティ、長期契約はありません。

ターゲットを絞ったビジネス成果

このガイドの目的は、以下のバックアップおよび復旧アプローチをサポートするために使用できる AWS サービスの概要を提供することです。

- 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
- AWS ネイティブサービス
- ディザスタリカバリ (DR)

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。

データ保護のための AWS サービスの選択

AWS には、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ストレージと補完サービスが多数用意されています。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 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。これにより、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がもたらされます。
- 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、これらの一般的なオンプレミスプロトコルを次のような AWS ストレージサービスにブリッジします。
  - Amazon S3
  - S3 Glacier Deep Archive
  - Amazon EBS

  Storage Gateway を使用すると、 内のファイル、ボリューム、スナップショット、仮想テープに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、 サービス間で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バックアップ AWS サービスです。 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
- Storage Gateway ボリューム

のコスト AWS Backup は、1 か月に消費、復元、および転送したストレージに基づきます。詳細については、「AWS Backup の料金」を参照してください。

- AWS Elastic Disaster Recovery は、ターゲット AWS アカウント と優先リージョンのステージングエリアサブネットにマシンをレプリケートします。ステージングエリア設計は、手頃な料金のストレージと、レプリケーションを継続するために最小限のコンピューティングリソースを使用してコストを削減します。Elastic Disaster Recovery は、オンプレミスからクラウドへの DR、およびクロスリージョン DR に使用できます。
- AWS Config は、 AWS アカウント内の AWS リソースの設定の詳細ビューを提供します。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 リソースAWS Config の設定記録を有効にすると、時間の経過とともにリソース関係の履歴が保持されます。これにより、最大 7 年間の AWS 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、 は、Amazon EBS スナップショットボリュームとボリュームがアタッチされた EC2 インスタンスの関係を追跡 AWS Config 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 SDKs、 AWS のサービスとそのデータを操作できます。Amazon EventBridge 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 のサービスは、バックアップと復元に固有の機能を提供します。使用している AWS サービスごとに、 AWS ドキュメントを参照して、サービスが提供するバックアップ、復元、データ保護の機能を確認してください。 AWS Command Line Interface (AWS CLI)、 AWS SDKs、および API オペレーションを使用して、データのバックアップとリカバリのサービス AWS 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 を使ったバックアップとリカバリー

Amazon Simple Storage Service (Amazon S3) を使用して、いつでも任意の量のデータを保存および取得できます。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。たとえば、 AWS CLI または AWS 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、耐久性と信頼性の高いストレージに 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 ストレージクラスを使用してバックアップデータストレージコストを削減する

Amazon S3 は、オンプレミス、ハイブリッド、クラウドネイティブのアーキテクチャで使用できる複数のストレージクラスを提供します。すべてのストレージクラスはスケーラブルなキャパシティを提供するため、バックアップデータセットが大きくなるにつれてボリュームやメディアの管理は必要ありません。使用量に応じた従量制料金モデルで、GB/月あたりのコストが低いため、Amazon S3

ストレージクラスは幅広いデータ保護のユースケースに適しています。Amazon S3 ストレージクラスは、以下のカテゴリーを含むさまざまなユースケース向けに設計されています。

- 高頻度アクセスストレージクラスは、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) の汎用ストレージ向けです。これには、すべての Amazon S3 オブジェクトのデフォルトである S3 Standard ストレージクラスが含まれます。
- 低頻度アクセスストレージクラスは、保存期間は長いが、アクセス頻度は低いデータ (毎月のバックアップなど) 向けです。これには、S3 Standard-IA ストレージクラスなどがあります。IA は infrequent access (低頻度アクセス) の略です。
- S3 Glacier ストレージクラスは、アクセスがほとんど必要のない保存期間が非常に長いデータ (例: 毎年のバックアップ) 向けです。これには、最低コストのストレージを提供する S3 Glacier Deep Archive が含まれます AWS。

アクセスパターンが不明または変更されたバックアップの場合は、S3 Intelligent-Tiering ストレージクラスを使用できます。S3 Intelligent-Tiering は、オブジェクトが最後にアクセスされた日数に基づいて、オブジェクトを最も費用対効果の高い階層に自動的に移行します。

> **Note**
>
> 一部のストレージクラスには、最小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 `duration` を検索します。

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自動的に移行されます。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

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。 AWS 請求のコスト配分のタグ付けとレポートは、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とアーカイブ S3 バケットを使用して、アプリケーションとワークロードデータのポイントインタイムスナップショットを保存できます。標準の S3 プレフィックスを作成すると、ポイントインタイムデータのスナップショットを整理しやすくなります。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。こうしておけば、ポイントインタイム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、ポイントインタイムの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便利です。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。たとえば、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 での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事項であり、 AWS セキュリティを非常に重視しています。セキュリティはあらゆる AWS のサービスの基盤です。Amazon S3 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 エンドポイントは、転送中のデータを暗号化するために SSL/TLS をサポートしています。保管中のオブジェクトの暗号化をセットアップするには、以下を実行します。

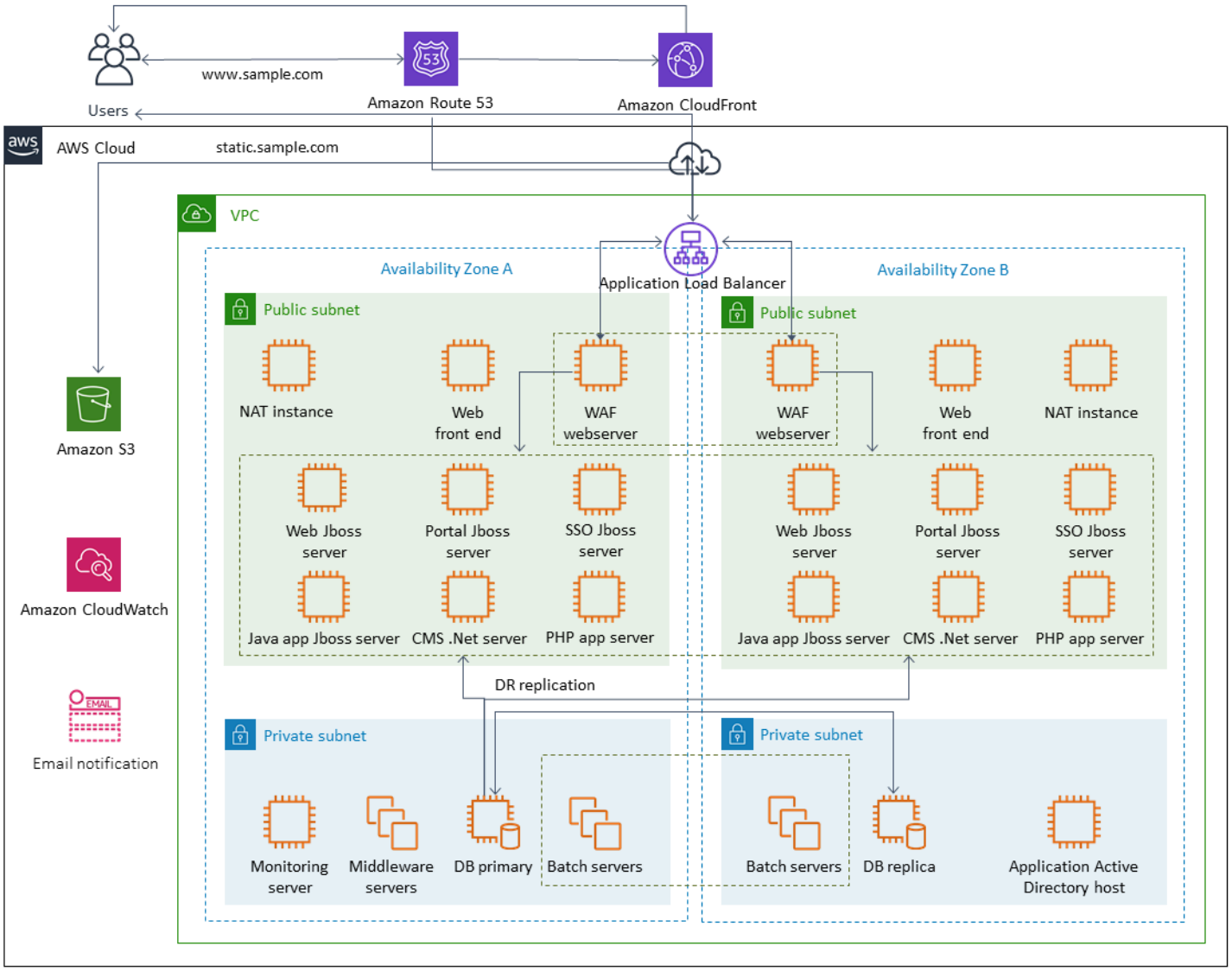
- Amazon S3 が管理する暗号化キーによるサーバー側の暗号化 (デフォルト) の使用
- に保存されている AWS Key Management Service (AWS KMS) キーによるサーバー側の暗号化 AWS KMSの使用
- クライアント側の暗号化の使用

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。でのオブジェクトレベルのログ AWS CloudTrail記録を使用して、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ための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。要件を満たす AWS 場合は、 でバックアップを管理するための最初の選択肢 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、ディザスタリカバリ (DR) レプリケーションが含まれます。



AWS は、このアーキテクチャで表される多くの Amazon EC2 サーバーに多くのフル機能のサービスを提供し、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、最適化の差別化されていない作業を実行します。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、複雑さと管理を軽減します。 は、Amazon EC2 ベースのアーキテクチャの可用性を向上させるサービス 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
- 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
- Amazon EBS ボリュームまたは EC2 インスタンスのリストア

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 マシンイメージ (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。インスタンスストアバックアップされた AMI には、インスタンスのルートボリュームのテンプレート (例えば、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) が含まれます。
- 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

> **Note**
>
> ほとんどの場合、Windows、RedHat、SUSE、SQL Server の AMI には、正しいライセンス情報が存在する必要があります。詳細については、「AMI 請求情報の理解」を参照してください。スナップショットから AMI を作成する場合、`RegisterImage` オペレーションはスナップショットのメタデータから正しい請求情報を取得しますが、これには適切なメタデータが必要です。正しい請求情報が適用されたかどうかを確認するには、新しい AMI の [プラットフォームの詳細] フィールドを確認します。フィールドが空であるか、所定のオペレーティングシステムコード (Windows、RedHat、SUSE、SQL など) と一致しない場合、AMI の作成は失敗しているため、この AMI を破棄して「インスタンスから AMI を作成する」の手順に従う必要があります。

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。

によって AWS 、または から管理および公開されているプラットフォームおよびアプリケーション 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 から発行された新しく更新された AMIs で、データボリューム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 としてサポートし、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、EC2 インスタンスの AMI を作成します。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、[マイ AMI] 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。または AWS Command Line Interface () を使用できます AWS マネジメントコンソール 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すが、メタデータのストレージではありません。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 の料金の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、データのポイントインタイムバックアップを取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 EBS 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 EBS スナップショットは、Amazon EBS ドキュメントで説明されているように、Amazon EBS スナップショットコピー機能を使用して AWS リージョン間でコピーすることもできます。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、ファインチューニングできます。

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、通知のための重要なプラクティスです。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のテクニカルペーパー」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 。開始しやすくするために、 はマネージドルールと呼ばれるカスタマイズ可能な事前定義されたルール 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 を継続的に追跡しながら、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した場合、 はリソースとルールを非準拠として 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 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ボリュームシャドウコピーサービス (VSS) を提供します。 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取得するために実行できる Systems Manager ドキュメント AWS を提供します。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 の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。

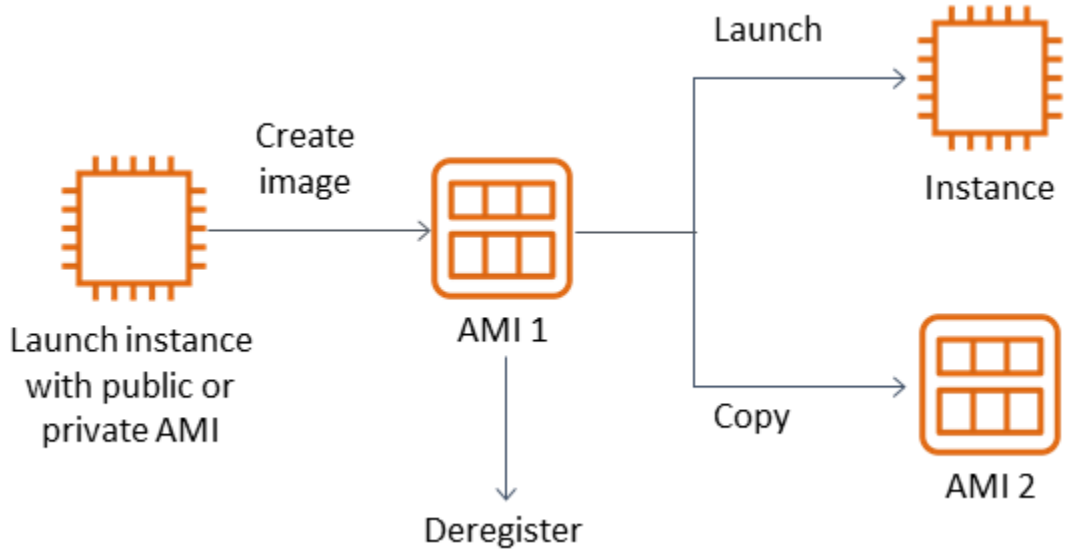
説明を入力し、適切なタグを追加します。Name タグを追加して、後でボリュームを見つけやすくします。タグ付け戦略に基づいて、その他の適切なタグを追加します。

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 に移行する場合を除き、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

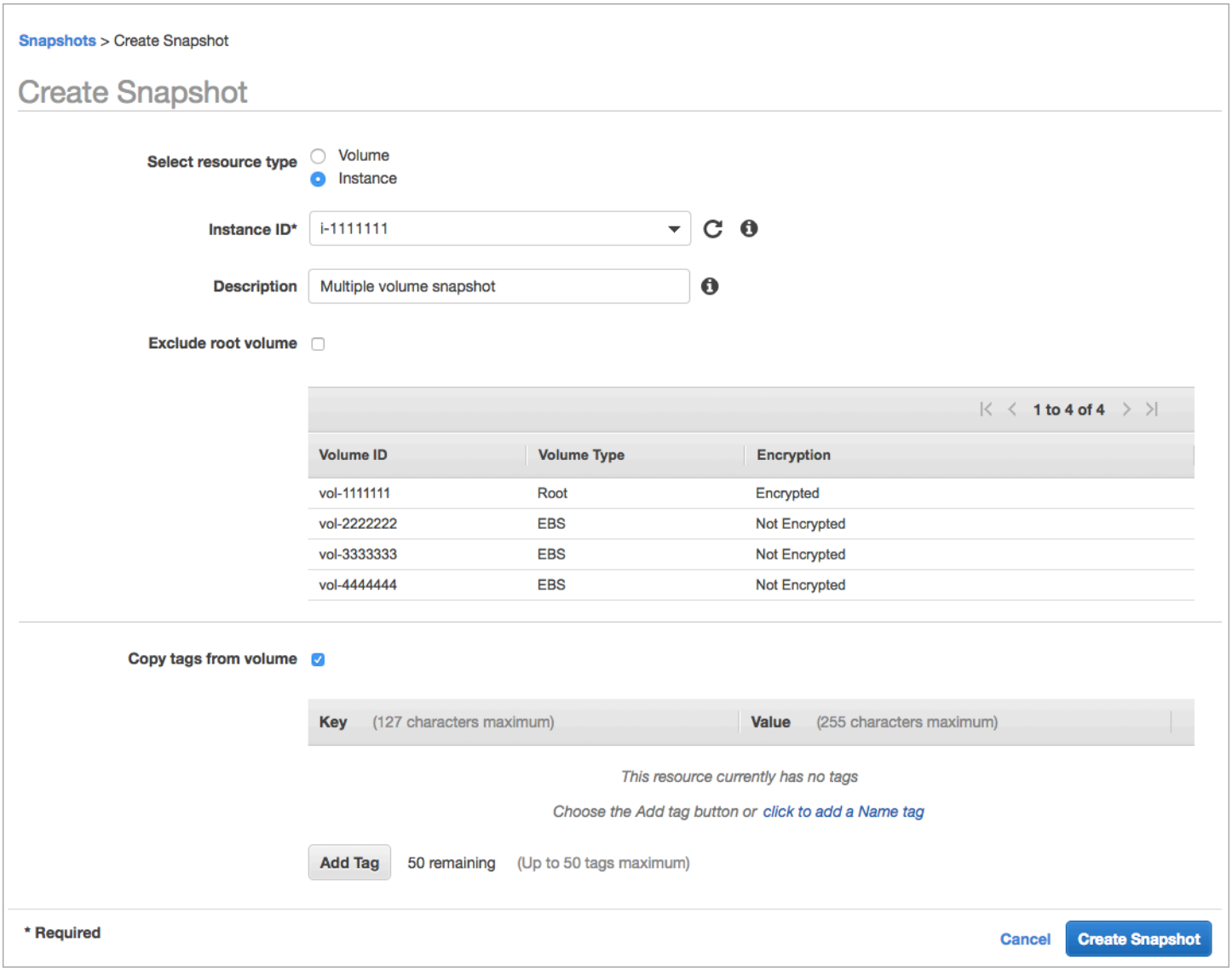
AWS Backup は、複数の AWS サービスにまたがるリソースを含むバックアッププランを作成できるため、Amazon Data Lifecycle Manager と一意です。リソースのバックアップを個別に調整するのではなく、一緒に使用しているリソースをカバーするようにバックアップを調整できます。

AWS Backup には、完了したバックアップの復旧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 アレイの一貫したスナップショット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て [Elastic Block Store] → [Snapshots] → [Create Snapshot] 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を使用すると、EC2 インスタンスにアタッチされている複数の EBS ボリュームにわたって、ポイントインタイムで、データ調整済みの Crash-consistent スナップショットを取得できます。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 の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。セキュリティ違反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 アカウントがある場合は、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。

ディザスタリカバリプランでは、リージョンで障害 AWS リージョン が発生した場合に別の で EC2 インスタンスを再現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、偶発的な削除保護を追加し、ディザスタリカバリ (DR) 目標をサポートできます。 は、クロスリージョンバックアップのサポート AWS Backup を提供します。

ec2:DeleteSnapshot と ec2:DeregisterImage アクションに対する IAM パーミッションをブロックすることを検討します。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 Write-Once-Read-Many (WORM) 戦略を実装する方法の 1 つです。また、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AWS Backup ボールトロックを使用することもできます。

さらに、ec2: ModifyImageAttribute と ec2: ModifySnapshotAttribute の IAM アクションをブロックして、ユーザーが AMI と EBS スナップショットを共有できないようにすることも検討します。これにより、AMIs とスナップショットが組織の外部にある AWS 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 EBS 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。たとえば、使用しなくなった EBS ボリュームのライフサイクルの終了段階として、スナップショットのアーカイブを検討することができます。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。AWS-CreateSnapshot 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、他のユーザーにそれら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 パッチ適用と AMI 作成を自動化するための AWS-UpdateLinuxAmi ランブックと AWS-UpdateWindowsAmi ランブックも含まれています。

AWS CLI および を使用して、スナップショットと AMI の作成プロセスAWS Tools for Windows PowerShell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、自動化の 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、Crash-consistent で同期されたスナップショットを作成できます。

CLI AWS 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 マシンイメージ (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、 AWS CLI、または API 操作を使用して、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。

たとえば、コンソールを使用してボリュームを以前の時点の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コマンド AWS CLI 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。

> **Note**
>
> ほとんどの場合、Windows、RedHat、SUSE、SQL Server の AMI には、正しいライセンス情報が存在する必要があります。詳細については、「AMI 請求情報の理解」を参照してください。スナップショットから AMI を作成する場合、RegisterImage オペレーションはスナップショットのメタデータから正しい請求情報を取得しますが、これには適切なメタデータが必要です。正しい請求情報が適用されたかどうかを確認するには、新しい AMI の [プラットフォームの詳細] フィールドを確認します。フィールドが空であるか、所定のオペレーティングシステムコード (Windows、RedHat、SUSE、SQL など) と一致しない場合、AMI の作成は失敗しているため、この AMI を破棄して「インスタンスから AMI を作成する」の手順に従う必要があります。

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、[スナップショット] 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 (例えば 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。
5. (Windows、RedHat、SUSE、SQL Server のみ) 正しい請求情報が適用されたかどうかを確認するには、新しい AMI の [プラットフォームの詳細] フィールドを確認します。フィールドが空であるか、所定のオペレーティングシステムコード (Windows や RedHat など) と一致しない場合、AMI の作成は失敗しているため、この AMI を破棄してインスタンスから AMI を作成するの手順に従う必要があります。

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。

オンプレミスインフラストラクチャから へのバックアップとリカバリ AWS

オンプレミスインフラストラクチャバックアップの耐久性の高いオフサイトストレージ AWS に を使用できます。このシナリオで AWS ストレージサービスを使用することで、バックアップとアーカイブのタスクに集中できます。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 は、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もできます。

このシナリオでは、オンプレミスインフラストラクチャで使用しているバックアップおよびアーカイブソフトウェアは、 API オペレーション AWS を介して と直接インターフェイスします。バックアップソフトウェアは AWS認識されているため、オンプレミスサーバーから Amazon S3 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は、Storage Gateway を使用できます。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 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 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。

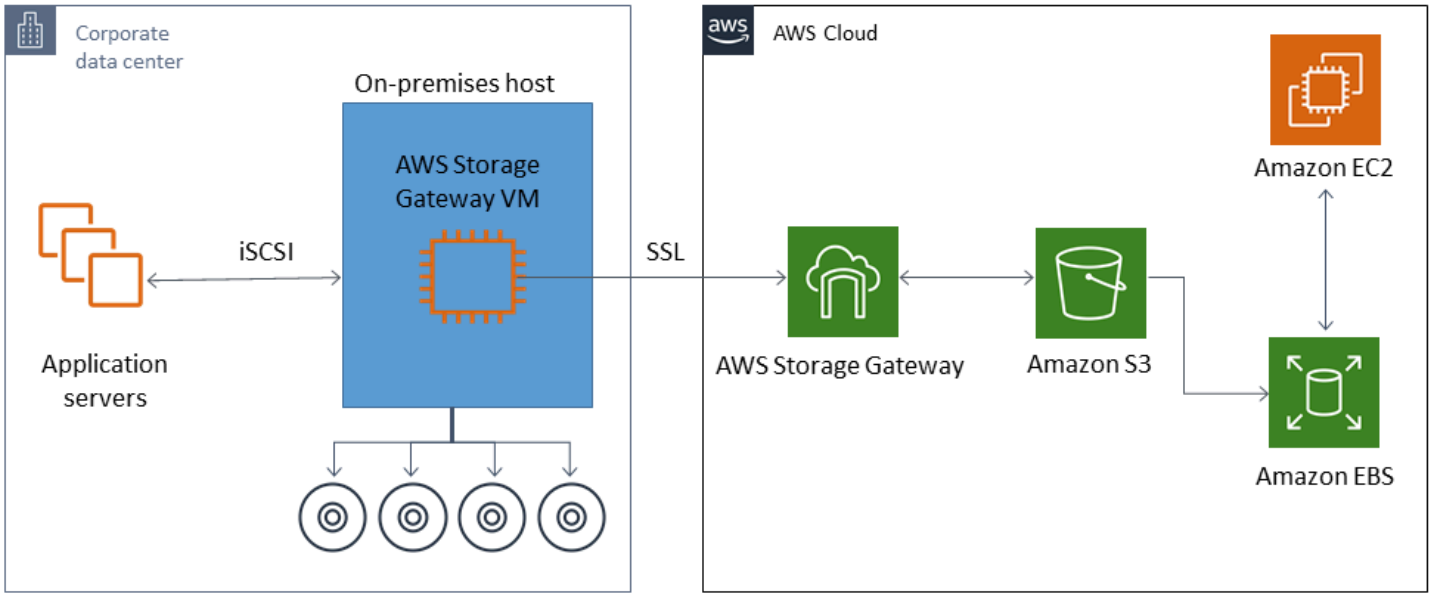
ファイルゲートウェイ

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 Glacier ストレージクラス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。



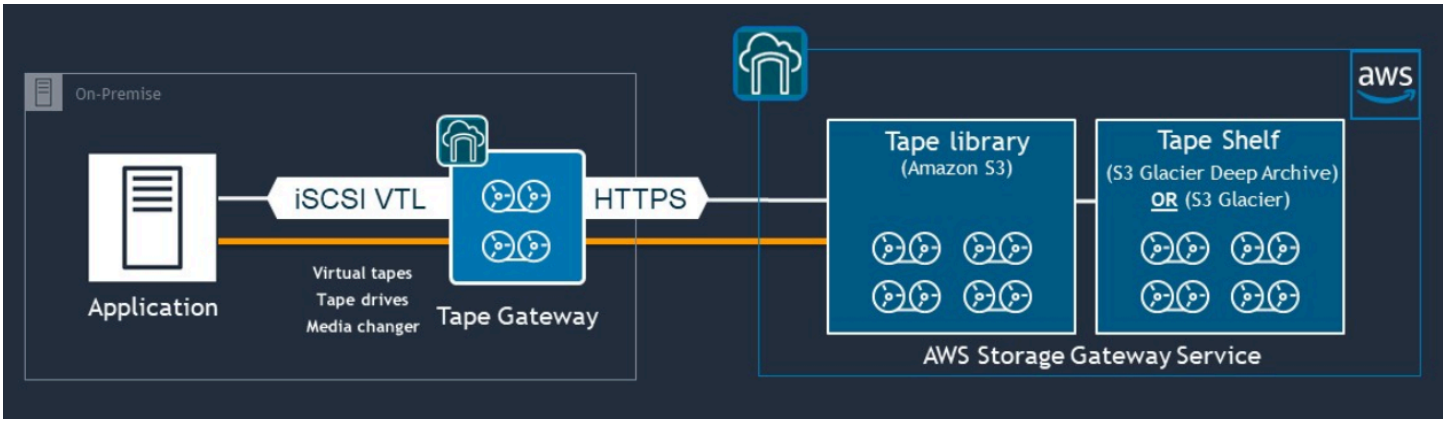
ボリュームゲートウェイは Amazon EC2 の Amazon EBS ボリューム機能と統合されるため、 AWS Backup を使用してスナップショットプロセスを自動化およびスケジュールできます。ボリュームゲートウェイには、耐久性のある Amazon S3 ベースの Amazon EBS スナップショットとタグ付け機能という利点もあります。詳細については、Amazon EBS スナップショットに関する文書を参照してください。

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 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 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 また、 は定期的に修正チェックを実行して、データを読み取ることができ、エラーが発生していないことを確認します。Amazon S3 に保存されているすべてのテープは、デフォルトキーまたは 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復旧

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。 は、データを管理し、操作するためのサービス固有の機能とオプション AWS を提供します。コンソール、、 SDKs AWS CLI、および 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、他の機能も提供する の 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し、特定のデータベースのバックアッププランが一意である場合は、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てください。

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。

DynamoDB コンソール、、または DynamoDB API を使用して AWS CLI、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。を使用して定期的または将来のバックアップをスケジュールすることも AWS Backup、Lambda 関数を使用してバックアップアプローチをカスタマイズおよび自動化することもできます。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ない場合は、 AWS Backup を使用してバックアッププランを作成できます。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。 は、保持スケジュールに基づいてバックアップ AWS Backup を作成し、以前のバックアップを削除します。 には、低コストの階層型ストレージ、クロスアカウントおよび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 AWS Backup 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、テーブルがアクティブになった後のみです。

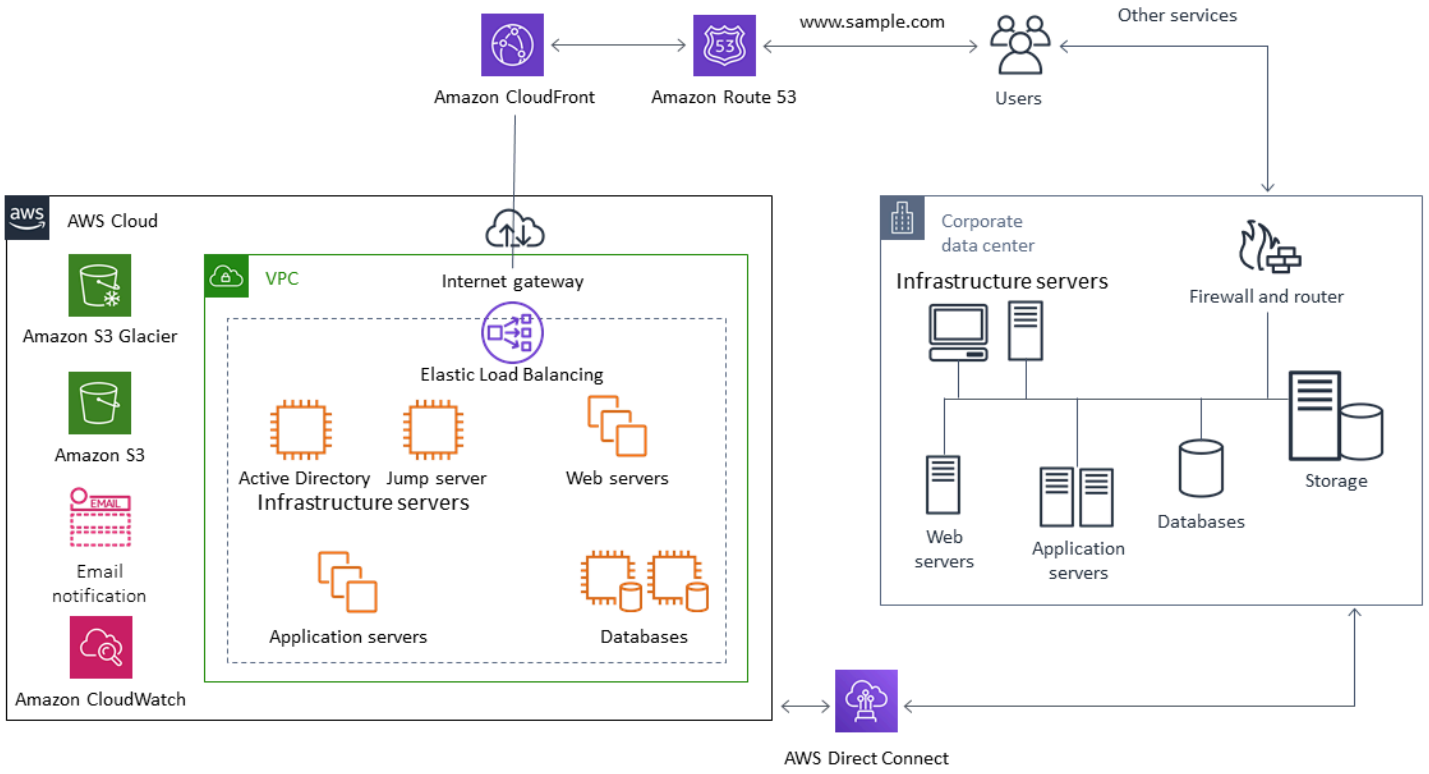
復元プロセスでは、新しく復元されたテーブル名を使用するようにクライアントにどのように指示するかを考慮する必要があります。設定ファイル、 AWS Systems Manager パラメータストア値、またはクライアントが使用するテーブル名を反映するように動的に更新できる別のリファレンスから DynamoDB テーブル名を取得するようにアプリケーションとクライアントを設定できます。

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デプロイとオンプレミスデプロイは、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コンポーネントがあるハイブリッドシナリオと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。多くの企業には独自のデータセンターがあり、 を使用して容量を補強 AWS しています。これらのカスタマーデータセンターは、多くの場合、大容量の AWS ネットワークリンクによってネットワークに接続されます。たとえば、 Direct Connectを使用すると、オンプレミスのデータセンターから へのプライベートな専用接続を確立できます AWS。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

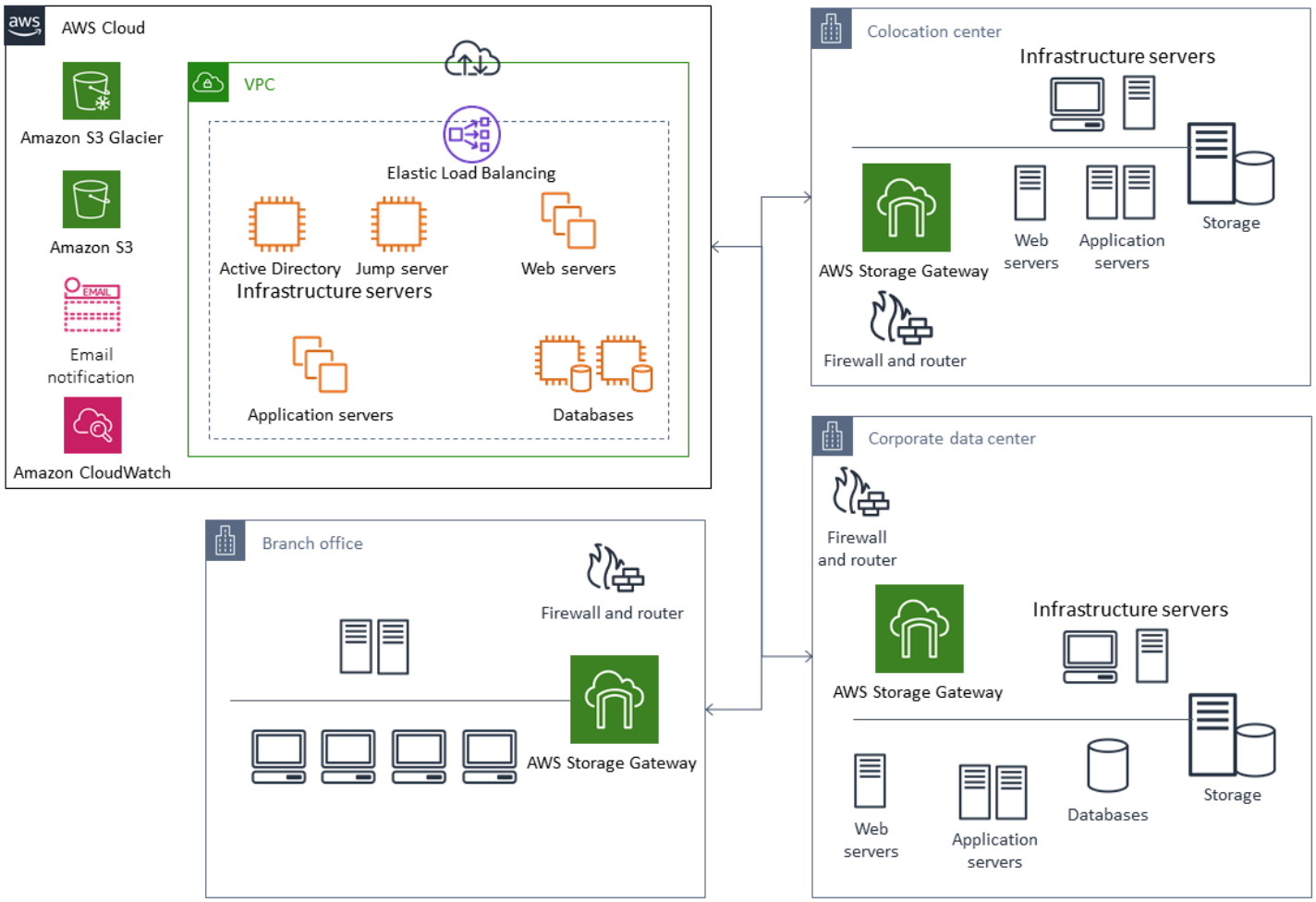
の ISV は、オンプレミスインフラストラクチャ向けに市場をリードするバックアップおよび復元ソリューションを提供しており、ハイブリッドアプローチをサポートするようにソリューションを拡張しています。

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

で既存のバックアップ管理ソリューションへの投資を使用することで AWS、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 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。たとえば、ファイルゲートウェイを使用すると、世界中のアプリケーションワークフロー AWS の に保存されているデータに、低レイテンシーでオンデマンドでアクセスできます。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
Web servers
Infrastructure 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

によるディザスタリカバリ AWS

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。多くの企業は、バックアップと復元、および DR サイトとして AWS クラウドを使用しています。 は、DR とビジネス継続性をサポートする多くのサービスと機能 AWS を提供します。

トピック

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

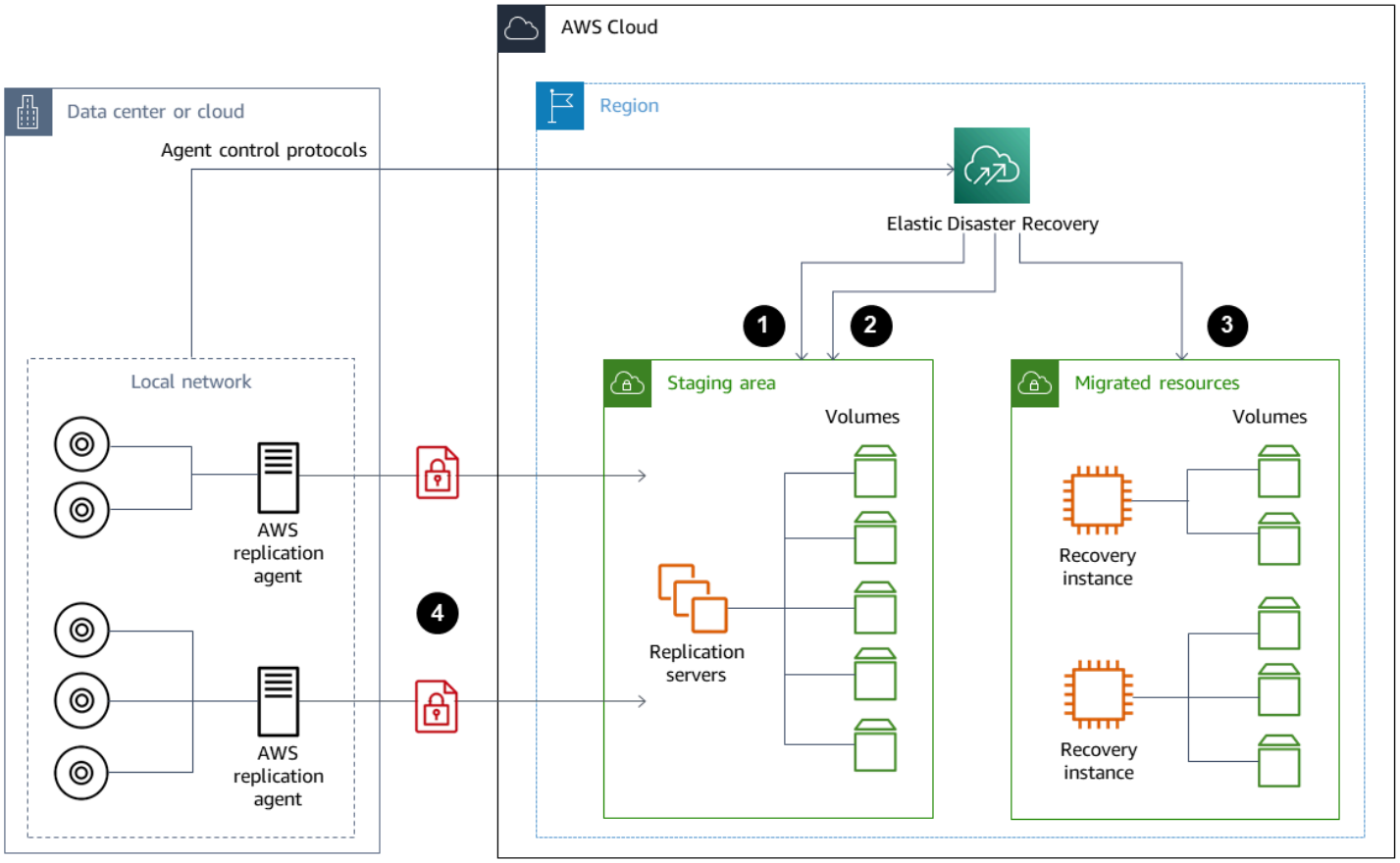
オンプレミス DR から へ AWS

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 AWS として を使用することは、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 では、ルートボリュームや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AWS Elastic Disaster Recoveryを作成できます AWS。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 マシンイメージ (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ワークロードが DR 目標にどのように適合するかを検討してください。 は、世界中の リージョンで複数のアベイラビリティーゾーン AWS 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 フレームワークの信頼性の柱は、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 のリージョン別の障害時の DR

可用性要件が非常に高いお客様 (ダウンタイムを許容できないミッションクリティカルなアプリケーションなど) は、複数のリージョン AWS で を使用して、リージョンレベルでの問題に対する耐障害性を高めることができます。お客様は、マルチリージョン DR プランの確立と維持に必要な複雑さ、コスト、労力を利点と慎重に比較検討する必要があります。 は、グローバルな可用性、フェイルオーバー、DR のためのマルチリージョンアーキテクチャをサポートする機能 AWS を提供します。 このガイドでは、Amazon EC2 のバックアップとリカバリに固有の利用可能な機能のいくつかについて説明します。

AWS AMIs 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。リージョン障害 DR プランをサポートするために、AMIs 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 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ています。

「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持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。によって作成されたバックアップ AWS には作成日が調整されていますが、バックアップをワークロード、保持要件、復元ポイント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。この自動修復は、 AWS Config ルール、を使用したスクリプト AWS CLI、または AWS SDK を使用した Lambda 関数を使用して実装できます。

Systems Manager は、Amazon EBS スナップショットのクリーンアップを開始および自動化するのに役立つ AWS-DeleteEBSVolumeSnapshots および AWS-DeleteSnapshot ドキュメントを提供します。 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
- AWS Config
- Amazon DynamoDB
- Amazon EBS
- Amazon EC2
- Amazon EventBridge
- IAM
- Amazon RDS
- Amazon S3
- 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)
- でのワークロードのディザスタリカバリ AWS: クラウドでの復旧 (ホワイトペーパー)
- ディザスタリカバリシリーズ (AWS アーキテクチャブログ記事)
- IT ディザスタリカバリ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)
- の開始方法 AWS Backup

ドキュメント履歴

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

変更	説明	日付
更新した情報	Amazon S3 セクションのガイダンスを更新しました。	2024 年 6 月 28 日
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	「 によるディザスタリカバリ AWS」および「データ保護のための AWS サービスの選択」セクションで、 に関する情報を追加しました AWS Elastic Disaster Recovery。「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 Manager のドキュメントへのリンクを追加しました。	2022 年 10 月 31 日
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	「データ保護のための AWS サービスの選択」セクションに、 のサービスが追加されました。を使用したバックアップとリカバリ AWS Backupのセクションを追加しました。「Amazon S3 と Amazon 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 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。「クラウドネイティブ AWS サービスのバックアップと復旧」セクションに、 の使用に関する推奨事項を追加しました AWS Backup。「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、が AWS Backup 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 規範ガイダンスの用語集

以下は、 AWS 規範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を購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例： Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。
- 廃止 — 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制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

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な方法ですが、さらに多くの作業が必要となります。

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

複数行に処理を行い、グループ全体を対象に単一の戻り値を計算する SQL 関数。集計関数の例としては、SUM や MAX などがあります。

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

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

アンチパターン

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

アプリケーション制御

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 の重要な要素であり、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?」をご覧ください。

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン (AZ)

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

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るための、 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です。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを整理しています。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、組織がクラウド導入を成功させるための準備を支援します。詳細については、AWS CAF ウェブサイトと AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

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

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

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「動作グラフのデータ」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」もご覧ください。

二項分類

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

ブルームフィルター

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

ブルー/グリーンデプロイ

それぞれが独立しているが、同一の環境を 2 つ作成するデプロイ戦略。現在のアプリケーションバージョンを 1 つの環境 (ブルー) で実行し、新しいアプリケーションバージョンを別の環境 (グリーン) で実行します。この戦略は、最小限の影響で迅速にロールバックするのに役立ちます。

ボット

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

ボットネット

マルウェアに感染しており、ボットハーダーまたはボットオペレーターと呼ばれる単一の当事者によって制御されているボットのネットワーク。ボットネットは、ボットとその影響力を拡大する仕組みとして、非常によく知られています。

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといいます。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発した

り、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチの概要」(GitHub ドキュメント) を参照してください。

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようにします。詳細については、 AWS Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータ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、AWSでのコンテナ化されたマイクロサービスの実行ホワイトペーパーの「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

カナリアデプロイ

エンドユーザーへのバージョンリリースを、時間をかけて段階的に行うこと。確信が持てたら新規バージョンをデプロイして、現在のバージョン全体を置き換えます。

CCoE

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

CDC

「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。

カオスエンジニアリング

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

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

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

クライアント側の暗号化

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

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

リモートデータストレージと IoT デバイス管理に通常使用されるクラウドテクノロジー。クラウドコンピューティングは、一般的に、エッジコンピューティング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、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されました。AWS 移行戦略との関連性については、「移行準備ガイド」を参照してください。

CMDB

「構成管理データベース (CMDB)」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 や Bitbucket Cloud があります。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオといった、ビジュアル形式の情報を分析および抽出する AI の分野。例えば、Amazon SageMaker AI では、CV 用の画像処理アルゴリズムを利用できます。

設定ドリフト

ワークロードにおいて、設定が想定した状態から変化すること。これによって、ワークロードが非準拠になる可能性がありますが、この状態は、徐々に生じ、意図的なものではありません。

構成管理データベース (CMDB)

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

コンフォーマンスパック

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

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番の各ステージを自動化するプロセス。CI/CD は一般的にパイプラインと呼ばれます。プロセスの自動化、生産性の向上、コード品質の向上、配信の加速化を可能にします。詳細については、「継続的デリバリーの利点」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「継続的デリバリーと継続的なデプロイ」を参照してください。

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

非一元的で分散型のデータ所有権を持つとともに、一元的な管理およびガバナンスを行えるアーキテクチャフレームワーク。

データ最小化

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

データ境界

AWS 環境内の一連の予防ガードレール。信頼できる ID のみが、期待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します。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

分析などのビジネスインテリジェンスをサポートするデータ管理システム。データウェアハウスには、一般的に、大量の履歴データが含まれており、多くの場合、それらはクエリや分析に使用されます。

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

予測のために複数の深層学習モデルを組み合わせます。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。

深層学習

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

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を採用するときは AWS、リソースの保護に役立つように、 AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加します。たとえば、多層防御アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

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

Organizations ドキュメントの「AWS Organizationsで使用できるサービス」を参照してください。

トラブルシューティング

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、「 AWSでのセキュリティコントロールの実装」の「検出的コントロール」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

スタースキーマにおいて、ファクトテーブルの定量データに関するデータ属性が含まれる小さいテーブル。ディメンションテーブルの属性は、通常、テキストフィールド、またはテキストのように扱える個別の数値で示されます。これらの属性は、一般的に、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使用されます。

ディザスタ

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

ディザスタリカバリ (DR)

ディザスタ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の戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

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

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

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

DVSM

「開発バリューストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 内でホストして、他のユーザーと共有できるサービス。を使用してエンドポイントサービスを作成し AWS PrivateLink 、他の AWS アカウント または AWS Identity and Access Management (IAM) プリンシパルにアクセス許可を付与できます。これらのアカウントまたはプリンシパルは、インターフェイス VPC エンドポイントを作成することで、エンドポイントサービスにプライベートに接続できます。詳細については、Amazon Virtual Private Cloud (Amazon VPC) ドキュメントの「エンドポイントサービスを作成する」を参照してください。

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

スタースキーマの中央にあるテーブル。ビジネスオペレーションに関する定量的データが保存されます。一般的に、ファクトテーブルは、2 種類の列で構成されます。1 つは測定値が含まれる列、もう 1 つはディメンションテーブルへの外部キーが含まれる列です。

フェイルファスト

開発ライフサイクルを短縮するために、頻繁かつ段階的にテストを行う哲学であり、アジャイルアプローチでは、この考え方がきわめて重要です。

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高めるのに役立つ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、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

追加のソースによるデータのエンリッチ化、値のスケーリング、単一のデータフィールドからの複数の情報セットの抽出など、機械学習プロセスのデータを最適化すること。これにより、機械学習モデルはデータの恩恵を受けることができます。例えば、「2021-05-27 00:15:37」の日付を「2021 年」、「5 月」、「木」、「15」に分解すると、学習アルゴリズムがさまざまなデータコンポーネントに関連する微妙に異なるパターンを学習するのに役立ちます。

数ショットプロンプト

LLM に、タスクと望ましい出力を示す例を少数提示した後に、類似のタスクを実行させること。この手法は、プロンプトに記述された例 (ショット) からモデルが学習する「インコンテキスト学

習」の一種です。数ショットプロンプトは、特定のフォーマット、推論、専門知識が必要なタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセス制御」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

変更データのキャプチャによる継続的なデータ複製を利用して、段階的なアプローチではなく、可能な限り短時間でデータを移行するデータベース移行方法。目的はダウンタイムを最小限に抑えることです。

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

大規模な深層学習ニューラルネットワークであり、一般化およびラベル付けされていないデータからなる大規模データセットでトレーニングされています。FM により、言語理解、テキストおよび画像生成、自然言語での会話といった、一般的な各種タスクを実行できます。詳細については、「基盤モデルとは何ですか?」を参照してください。

G

生成 AI

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

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

特定の国のユーザーがコンテンツ配信にアクセスできないようにするための、Amazon CloudFront のオプション。アクセスを許可する国と禁止する国は、許可リストまたは禁止リスト

を使って指定します。詳細については、CloudFront ドキュメントの「コンテンツの地理的ディストリビューションの制限」を参照してください。

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローは古いと見なされている方法であり、トランクベースのワークフローは推奨されている新しい方法です。

ゴールデンイメージ

システムまたはソフトウェアのスナップショットであり、システムまたはソフトウェアの新規インスタンスをデプロイするテンプレートとして使用されます。製造の例で言えば、ゴールデンイメージを使用すると、複数のデバイスにソフトウェアをプロビジョニングして、デバイス製造オペレーションの速度、スケーラビリティ、生産性を向上させることができます。

グリーンフィールド戦略

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

ガードレール

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

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

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

高可用性 (HA)

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

ヒストリアンのモダナイゼーション

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

ホールドアウトデータ

機械学習モデルのトレーニング用データセットから保留される、ラベル付き履歴データの一部。ホールドアウトデータを使用すると、モデル予測をホールドアウトデータと比較して、モデルのパフォーマンスを評価できます。

同種データベースの移行

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

ホットデータ

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

ホットフィックス

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

ハイパーケア期間

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

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「インダストリアル IoT」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

既存インフラストラクチャの更新、パッチ適用、変更などを行わずに、本番環境ワークロードに使用する新規インフラストラクチャをデプロイするモデル。本質的に、イミュータブルインフラストラクチャは、ミュータブルインフラストラクチャよりも一貫性、信頼性、予測性に優れています。詳細については、 AWS Well-Architected フレームワークにある「イミュータブルインフラストラクチャを使用してデプロイする」のベストプラクティスを参照してください。

インバウンド (受信) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーションの外部からネットワーク接続を受け入れ、検査し、ルーティングする VPC。AWS Security Reference Architecture では、アプリケーションとより広範なインターネット間の双方向のインターフェイスを保護するために、インバウンド、アウトバウンド、インスペクションの各 VPC を使用してネットワークアカウントを設定することを推奨しています。

増分移行

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

インダストリー 4.0

2016 年に Klaus Schwab 氏が提唱した用語で、接続、リアルタイムデータ、オートメーション、分析、AI/ML の進歩による、ビジネスプロセスのモダナイズを意味します。

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

インダストリアル 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、「インダストリアル IoT (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「IoT」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

ランディングゾーンは、スケーラブルで安全な、適切に設計されたマルチアカウント AWS 環境です。これは、組織がセキュリティおよびインフラストラクチャ環境に自信を持ってワークロードとアプリケーションを迅速に起動してデプロイできる出発点です。ランディングゾーンの詳細については、「安全でスケーラブルなマルチアカウント AWS 環境のセットアップ」を参照してください。

大規模言語モデル (LLM)

大量のデータで事前トレーニングされた深層学習 AI モデル。LLM では、質問への回答、ドキュメントの要約、他言語へのテキスト翻訳、文を完成させるなど、さまざまなタスクを実行できます。詳細については、「大規模言語モデル (LLM) とは何ですか?」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

「ラベルベースアクセス制御」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」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「ブランチ」を参照してください。

マルウェア

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

マネージドサービス

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

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するソフトウェアシステムであり、工場では、これによって、原材料から製品を完成させます。

MAP

「Migration Acceleration Program」を参照してください。

メカニズム

ツールを作成してその導入を推進し、導入結果を調べて調整を行うための包括的なプロセス。メカニズムとは、運用中にそれ自体を強化し改善するサイクルを意味します。詳細については、AWS 「 Well-Architected フレームワーク」の「メカニズムの構築」を参照してください。

メンバーアカウント

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

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

発行/サブスクライブのパターンに基づく、軽量のマシンツーマシン (M2M) 通信プロトコルであり、リソースに限りのある IoT デバイスに使用されます。

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たマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

ワークロードを 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、「組織を動員して大規模な移行を加速する」を参照してください。

ML

「機械学習」を参照してください。

モダナイゼーション

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

MPA

「Migration Portfolio Assessment」を参照してください。

MQTT

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

多クラス分類

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

ミュータブルなインフラストラクチャ

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

O

OAC

「オリジンアクセス制御」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

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

OI

「オペレーション統合」を参照してください。

Ola

「オペレーショナルレベルアグリーメント」を参照してください。

オンライン移行

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

OPC-UA

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

Open Process Communications - Unified Architecture (OPC-UA)

産業オートメーション用のマシンツーマシン (M2M) 通信プロトコル。OPC-UA により、相互運用の際に、データ暗号化、認証、認可の各スキームを標準化できます。

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

質問と関連するベストプラクティスのチェックリスト。インシデントや起こり得る障害を理解、評価、防止したり、その範囲を縮小したりする際に役立ちます。詳細については、 AWS Well-Architected フレームワークの「Operational Readiness Reviews (ORR)」を参照してください。

運用テクノロジー (OT)

産業オペレーション、機器、インフラストラクチャを制御するために物理環境と連携させるハードウェアおよびソフトウェアシステム。製造分野では、Industry 4.0 への変革を進める上で、OT と情報技術 (IT) システムの統合に焦点が当てられています。

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

オリジンアクセス制御 (OAC)

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

オリジンアクセスアイデンティティ (OAI)

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

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

「個人を特定できる情報」を参照してください。

プレイブック

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

PLC

「プログラマブルロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

次の操作を可能にするオブジェクト: アクセス許可を定義する (ID ベースのポリシーを参照)。アクセス条件を指定する (リソースベースのポリシーを参照)。 AWS Organizations の組織における全アカウントにアクセス許可の上限を定義する (サービスコントロールポリシーを参照)。

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。

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、「移行の準備状況の評価」を参照してください。

述語

`true` または `false` を返すためのクエリ条件。一般的に、`WHERE` 句に記述されます。

述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、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、「AWSでのセキュリティコントロールの実装」の「予防的コントロール」を参照してください。

プリンシパル

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

プライバシーバイデザイン

開発プロセス全体を通してプライバシーが考慮されている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

非準拠リソースのデプロイ防止を目的としたセキュリティコントロール。このコントロールにより、プロビジョニング前にリソースをスキャンします。コントロールに準拠していないリソースは、プロビジョニングされません。詳細については、 AWS Control Tower ドキュメントの「コントロールリファレンスガイド」および「 セキュリティコントロールの実装」の「プロアクティブコントロール」を参照してください。 AWS

製品ライフサイクル管理 (PLM)

製品の設計、開発、発売から、成長、成熟、衰退、廃棄に至る、製品のライフサイクル全体を通してデータとプロセスを管理すること。

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

製造分野で使用される、信頼性と適応性に優れたコンピュータであり、これによって、マシンをモニタリングするとともに、製造プロセスを自動化します。

プロンプトチェイニング

1 つの LLM プロンプトによる出力を次のプロンプトの入力に使用して、より良いレスポンスを生成します。この手法を使用すると、複雑なタスクをサブタスクに分割したり、事前レスポンスを繰り返し改良または拡張したりできます。これによって、モデルのレスポンスの精度と関連性が向上し、粒度の高いパーソナライズされた結果を得られます。

仮名化

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

発行/サブスクライブ (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。これにより、スケーラビリティと応答性を向上させます。例えば、マイクロサービスベースの MES の場合、マイクロサービスは、他のマイクロサービスがサブスクライブ可能なチャネルにイベントメッセージを発行できます。このシステムでは、発行サービスの変更なしに、新規マイクロサービスを追加できます。

Q

クエリプラン

手順などの一連のステップであり、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ます。

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

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RAG

「検索拡張生成」を参照してください。

ランサムウェア

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

RASCI マトリックス

「実行責任者、説明責任者、協業先、報告先 (RACI)」を参照してください。

RCAC

「行と列のアクセス制御」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。

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

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

リグレッション

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。

リプラットフォーム

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または中断から回復するアプリケーションの機能。 AWS クラウドでの回復力を計画する際には、一般的に、高可用性とディザスタリカバリが考慮されます。詳細については、「AWS クラウド の耐障害性」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。サポートが含まれる場合は RASCI マトリックスと呼ばれ、含まれない場合は 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、「 AWSでのセキュリティコントロールの実装」の「レスポンシブコントロール」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。

検索拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」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情報を更新して、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 (IdP) が使用しているオープンスタンダード。この機能を使用すると、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは組織内のすべてのユーザーを IAM で作成しなくても、 AWS マネジメントコンソール にログインしたり AWS 、API オペレーションを呼び出すことができます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントの「SAML 2.0 ベースのフェデレーションについて」を参照してください。

SCADA

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

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

セキュリティバイデザイン

開発プロセス全体を通してセキュリティが考慮されているシステムエンジニアリングのアプローチ。

セキュリティコントロール

脅威アクターによるセキュリティ脆弱性の悪用を防止、検出、軽減するための、技術上または管理上のガードレール。セキュリティコントロールには、主に 4 つの種類があります。4 つとは、予防、検出、レスポンシブ、プロアクティブです。

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への自動レスポンスまたは自動修復を目的として、事前定義およびプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンス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、認証情報の更新などがあります。

サーバー側の暗号化

送信先で、それ AWS のサービス を受け取る によるデータの暗号化。

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

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

責任共有モデル

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

SIEM

「Security Information and Event Management システム」を参照してください。

単一障害点 (SPOF)

特定のアプリケーションを構成する単一の重要なコンポーネントで発生し、システム稼働に支障をきたす可能性のある障害。

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。

スプリットアンドシードモデル

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

SPOF

「単一障害点」を参照してください。

スタースキーマ

データベースの編成構造を意味し、1 つの大きいファクトテーブルにトランザクションデータまたは測定データが保存され、1 つ以上の小さいディメンションテーブルにデータ属性が保存されます。この構造は、データウェアハウスやビジネスインテリジェンスを用途とするように設計されています。

strangler fig パターン

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

サブネット

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

監視制御とデータ取得 (SCADA)

製造分野において、ハードウェアとソフトウェアを使用して物理アセットと本番運用をモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

ユーザーとのやり取りをシミュレートして、起こり得る問題を検出したり、パフォーマンスをモニタリングしたりすることで、システムをテストします。Amazon CloudWatch Synthetics を使用すると、こうしたテストを作成できます。

システムプロンプト

コンテキスト、指示、ガイドラインなどを提示して、LLM に動作を指示する手法。システムプロンプトは、コンテキストを設定して、ユーザーとやり取りするルールを確立するのに有用です。

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「トランジットゲートウェイとは」を参照してください。

トランクベースのワークフロー

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

信頼されたアクセス

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

チューニング

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

ツーピザチーム

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

U

不確実性

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

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

現在のレコードに何らかの形で関連している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといった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 ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

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

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

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

ゼロショットプロンプト

LLM にタスク実行の手順は提示するが、実行のガイドとして役立つ例 (ショット) は提示しない方法。LLM は、事前トレーニング済みの知識を使用してタスクを処理する必要があります。ゼロショットプロンプトの有効性は、タスクの複雑さとプロンプトの品質によって異なります。「数ショットプロンプト」も参照してください。

ゾンビアプリケーション

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

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