



でのバックアップと復旧のアプローチ AWS

AWS 規範ガイドンス



AWS 規範ガイド: でのバックアップと復旧のアプローチ AWS

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon の商標およびトレードドレスは、Amazon 以外の製品およびサービスに使用することはできません。また、お客様に誤解を与える可能性がある形式で、または Amazon の信用を損なう形式で使用することもできません。Amazon が所有していないその他のすべての商標は、Amazon との提携、関連、支援関係の有無にかかわらず、それら該当する所有者の資産です。

Table of Contents

序章	1
をデータ保護プラットフォーム AWS として使用する理由	2
ターゲットを絞ったビジネス成果	4
AWS サービスの選択	5
バックアップとリカバリソリューションの設計	7
AWS Backup	8
Amazon S3	10
Amazon S3 ストレージクラスを使用する	10
標準 S3 バケットの作成	12
Amazon S3 バージョニングの使用	12
のカスタマイズされた設定ファイルのバックアップと復元 AMIs	12
カスタムバックアップと復元	13
バックアップデータの保護	13
EBS ボリュームEC2のある Amazon	14
Amazon のEC2バックアップとリカバリ	16
AMIs または スナップショット	16
サーバーボリューム	17
個別のサーバーボリューム	18
インスタンスストアボリューム	19
標準のタグ付けと施行	20
EBS ボリュームバックアップの作成	21
EBS ボリュームの準備	21
コンソールからのスナップショットの作成	23
AMIs の作成	23
Amazon Data Lifecycle Manager	24
AWS Backup	25
マルチボリュームバックアップ	25
バックアップの保護	27
スナップショットのアーカイブ	28
スナップショットとAMI作成の自動化	28
ボリュームまたはインスタンスを復元する。	29
EBS スナップショットからのファイルとディレクトリの復元	30
Amazon EBSスナップショットからの EBSボリュームの復元	30
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	32

から実行中のインスタンスを復元する AMI	32
オンプレミスからのバックアップとリカバリー	34
ファイルゲートウェイ	35
ボリュームゲートウェイ	35
テープゲートウェイ	36
アプリケーションのバックアップと復旧	38
クラウドネイティブ AWS サービス	39
Amazon RDS	39
DNS CNAME の使用	40
DynamoDB	42
ハイブリッドアーキテクチャ	44
集中型バックアップ管理ソリューションの移行	45
ディザスタリカバリ	47
オンプレミス DR から AWS	47
クラウドネイティブワークロードの DR	49
単一のアベイラビリティ・ゾーン内の DR	50
地域障害の DR	50
バックアップをクリーンアップする	52
FAQ	53
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?	53
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?	53
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てEBSボリュームを引き 続き使用できますか?	53
次のステップ	54
リソース	55
ドキュメント履歴	56
用語集	59
#	59
A	60
B	62
C	64
D	68
E	71
F	74
G	75
H	76

I	78
L	80
M	81
O	85
P	88
Q	91
R	91
S	94
T	98
U	99
V	100
W	100
Z	101
.....	cii

でのバックアップとリカバリのアプローチ AWS

コラム・ニザミ、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、復旧時間目標 (RTO)、復旧時点目標 (RPO)、およびコンプライアンス要件を満たすために、低コスト、高い拡張性、より高い耐久性を提供します。

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

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

もう 1 つのアプローチは、ワークロードをモダナイズしてイミュータブルアーキテクチャを使用し、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 Machine Images (AMI)

企業データの増加が加速するにつれて、それを保護する作業はますます困難になっています。バックアップ手法の耐久性とスケ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 を使用したバックアップとリカバリ](#)
- [EBS ボリュームEC2を使用した Amazon のバックアップとリカバリ](#)
- [オンプレミスのインフラから AWSへのバックアップとリカバリ](#)
- [AWS からデータセンターへのアプリケーションのバックアップとリカバリ](#)
- [クラウドネイティブ AWS サービスのバックアップとリカバリ](#)
- [ハイブリッドアーキテクチャのバックアップと復旧](#)
- [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% (11 9s) の耐久性を実現するように設計されています。両プラットフォームとも、少なくとも3つの地理的に分散したアベイラビリティ・ゾーンにまたがるオブジェクト・レプリケーションにより、データの信頼性の高いバックアップを提供します。多くの AWS サービスは、ストレージ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に多数のオプション AWS を提供します。
- **グローバルインフラストラクチャ:** AWS サービスは世界中で利用できるため、コンプライアンスとワークロードの要件を満たすリージョンでデータをバックアップして保存できます。
- **コンプライアンス:** AWS インフラストラクチャは、以下の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簡単に既存のコンプライアンスの成果に合わせるすることができます。
 - 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がサービスコストを削減し、AWS サービスの TCO を削減するのに役立ちます。は、これらのコスト削減を価格の低下を通じての顧客に AWS 引き渡します。
- Pay-as-you-go 料金: AWS サービスを必要に応じて購入し、使用予定の期間のみ購入します。AWS 料金設定には前払い料金、終了違約金、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、次のようなバックアップとリカバリのアプローチをサポートするために使用できる AWS サービスの概要を説明することです。

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

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

データ保護のための AWS サービスの選択

AWS 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多数のストレージと補完サービスを提供します。これらのサービスは、クラウドネイティブアーキテクチャとハイブリッドアーキテクチャの両方をサポートできます。異なるサービスは、異なるユースケースに対してより効果的です。

- [Amazon S3](#) 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。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、耐久性の高い汎用オブジェクトストレージソリューションを提供します。
- [AWS Storage Gateway](#) はハイブリッドユースケースに最適です。Storage Gateway は Amazon S3 の機能を活用して、一般的なオンプレミスのバックアップとストレージの要件に対応します。アプリケーションは、以下の標準ストレージプロトコルを使用して、仮想マシン (VM) またはハードウェアゲートウェイアプライアンスを介してサービスに接続します。
 - ネットワークファイルシステム (NFS)
 - サーバーメッセージブロック (SMB)
 - インターネットスモールコンピュータシステムインターフェイス (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、[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

AWS Backup のコストは、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 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 および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の設計では、手頃な価格のストレージと最小限のコンピューティングリソースを使用して継続的なレプリケーションを維持することで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 とクロスリージョン 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、リソース関係の履歴が時間の経過とともに維持されます。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。例えば、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。を使用して 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、スケジュールに基づいて Lambda 関数を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、データ保護機能を確認してください。AWS Command Line Interface (AWS CLI)、および API オペレーションを使用して AWS SDKs、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 を使用したバックアップとリカバリ

Amazon Simple Storage Service (Amazon S3) を使用すると、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。例えば、AWS CLI または 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 SDKs。

AWS のサービス 次の例のように、Amazon S3 を耐久性と信頼性の高いストレージに使用します。

- 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保存します。
- 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備えたオンプレミス環境を提供します。
- Amazon RDS はデータベーススナップショットに Amazon S3 を使用します。Amazon S3

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 統合機能を使用して、バックアップとリカバリ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容量を提供し、バックアップデータセットの増加に応じてボリュームやメディアの管理は必要ありません。pay-for-what-you-use 使用モデルと GB/月あたりの低コストにより、Amazon S3 ストレージクラスは幅広いデータ保護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。

- [頻繁にアクセスされるデータ \(設定ファイル、計画外のバックアップ、日次バックアップなど\) の汎用ストレージ用の高頻度アクセスストレージクラス](#)。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。Amazon S3
- 存続期間が長い [アクセス頻度の低いデータ \(毎月のバックアップなど\) のアクセス頻度の低いストレージクラス](#)。これには S3 Standard-IA ストレージクラスが含まれます。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非常に長い存続期間のデータ (例: 年次バックアップ) 用です。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、アプリケーションに変更を加えることなく、データは自動的に適切なストレージクラスに移行されます。詳細については、「[Amazon S3 オブジェクトのライフサイクル管理](#)」を参照してください。

バックアップのコストを削減するには、次の例のように、目標復旧時間 (RTO) と目標復旧時点 (RPO) に基づいて階層型ストレージクラスアプローチを使用します。

- 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およびアーカイブ S3 バケットを使用して、アプリケーションおよびワークロードデータのスナップショットを保存 point-in-time できます。データスナップショットの整理 point-in-time に役立つ標準 S3 プレフィックスを作成できます。たとえば、1 時間ごとにバックアップを作成する場合は、YYYY/MM/DD/HH/<WorkloadName>/<files...> などのバックアッププレフィックスを使用することを検討します。これにより、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 point-in-time。

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、バックアップスケジュールよりも point-in-time 頻繁に変更される設定ファイルやその他のオブジェクトに役立ちます。また、ファイルを個別に元に戻す必要がある場合にも役立ちます。

Amazon S3 を使用したのカスタマイズされた設定ファイルのバックアップと復元 AMIs

オブジェクトバージョニング機能を備えた Amazon S3 は、ワークロード設定とオプションファイルの記録システムになります。例えば、[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 ISV。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。このアプローチを適用する場合、更新されたバージョンを使用するAMIのように 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、および API オペレーションを使用して AWS SDKs、Amazon S3 を使用するバックアップスクリプトと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ために、同様のアプローチを取ることができます RPO。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。セキュリティはすべてのの基盤です AWS のサービス。Amazon S3 は、保管中と転送中のアクセスコントロールと暗号化の機能を提供します。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。次の操作を行うことで、保管中のオブジェクトの暗号化を設定できます。

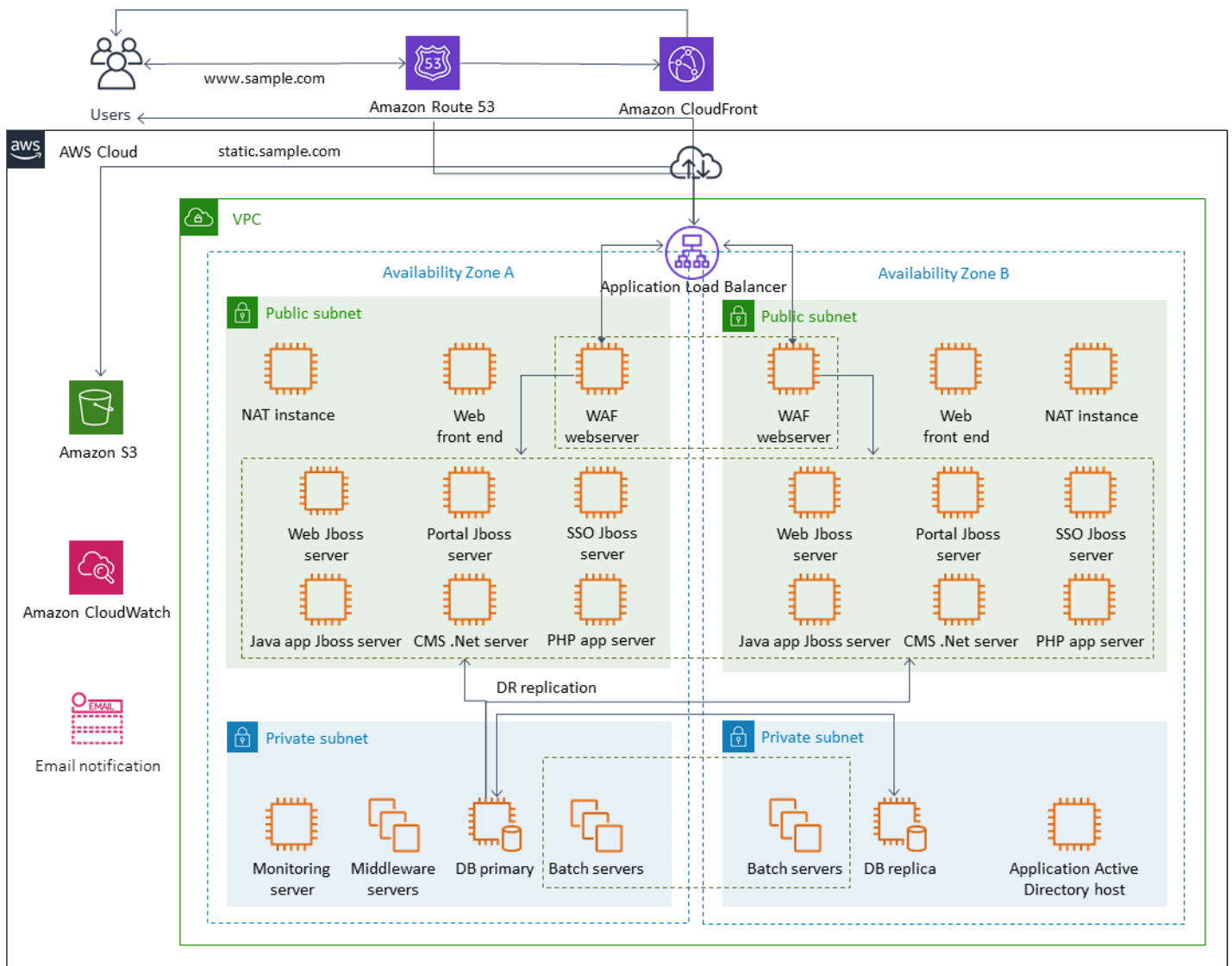
- [Amazon S3 マネージド暗号化キーによるサーバー側の暗号化](#) の使用 (デフォルト)
- [に保存されている AWS Key Management Service \(AWS KMS\) キーによるサーバー側の暗号化 AWS KMS の使用](#)
- [クライアント側の暗号化](#) の使用

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 は、個々のオブジェクトのアクセス許可と S3 バケット内の特定のプレフィックスパスを制御できます。でオブジェクトレベルのログ記録を使用することで、S3 オブジェクトへのアクセスを監査できます。 [AWS CloudTrail](#)

EBS ボリューム EC2 を使用した Amazon 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、ストレージ用の Amazon Elastic Block Store (Amazon EBS) ボリュームまたはインスタンスストアボリュームをバックアップする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 に基づくアーキテクチャの大部分 AWS を持つ上に完全に存在するワークロード環境を示しています EC2。次の図に示すように、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、最適化という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で意味をなす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 を検討して、Amazon のワークロードを補完してくださいEC2。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、主に永続的ストレージに 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しく説明する、バックアップとリカバリのため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を使用した Amazon の EC2 バックアップとリカバリ AMIs](#)
- [AMIs および EBS スナップショットを使用した EBS ボリュームバックアップの作成](#)
- [Amazon EBS ボリュームまたは EC2 インスタンスの復元](#)

スナップショットとを使用した Amazon の EC2 バックアップとリカバリ AMIs

Amazon マシンイメージ (AMI) を使用して EC2 インスタンスの完全バックアップを作成する必要があるか、個々のボリュームのスナップショットを作成する必要があるかを検討してください。

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

AMI には次のものが含まれます。

- 1 つ以上のスナップショット。Instance-store-backed には、インスタンスのルートボリューム (オペレーティングシステム、アプリケーションサーバー、アプリケーションなど) のテンプレート AMIs が含まれます。
- 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 AMI 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

を使用して AMIs、事前設定されたソフトウェアとデータで新しいインスタンスを起動できます。ベースラインを確立する AMIs ときに を作成できます。ベースラインは、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 AMI の 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作成されます。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、または から AMIs 管理および公開されている AWS プラットフォームとアプリケーションを使用している場合は AWS Marketplace、データ用に別々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AMI新しく更新された の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、新しく公開された で、設定情報を含むすべてのカスタムデータをバックアップおよび復元するための慎重なテストと計画が必要ですAMI。

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するかによって影響を受けます。インスタンスのバックアップとして機能するAMIのように を作成する場合は、復元プロセスAMIの一環として 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。潜在的な衝突の例としては、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 (SIDs) 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 としてAMI、ボリュームレベルのバックアップを別々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AMIの作成](#)。ロールバックする場合は、インスタンス起動ウィザードを使用してインスタンスを作成します。インスタンス起動ウィザードで、AMI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](#)。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](#)を参照してください。AWS Management Console または AWS Command Line Interface () を使用できますAWS CLI。

インスタンスのコストAMI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コストの詳細については、[Amazon のEBS料金表](#)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 のプライマリ永続ストレージオプションですEC2。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ゾーンに配置されます。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、0.1~0.2% の年間障害率 (AFR) 向け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一般的なコモディティディスクドライブの 20 倍になり、約 4% AFR ので障害が発生します。例えば、1,000 個の EBS ボリュームが 1 年間実行されている場合、1 つまたは 2 つのボリュームに障害が発生することが予想されます。

Amazon は、データのバックアップを取る point-in-time ためのスナップショット機能 EBS 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 では、任意の EBS ボリュームのスナップショット (バックアップ) を作成できます。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得し、Amazon S3 に配置します。このスナップショットは複数のアベイラビリティ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 の [EBS ドキュメント](#) を参照してください。

スナップショットを作成したのと同じリージョンの [Amazon EC2 コンソール](#) から、復元オペレーションの実行、スナップショットの削除、スナップショットに関連付けられたタグなどのスナップショットメタデータの更新を行うことができます。

スナップショットを復元すると、フル EBS ボリュームデータを含む新しい Amazon 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

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。永続化のために、EBSボリュームを作成し、インスタンスにアタッチして、定期的にインスタンスストアボリュームからEBSボリュームにデータをコピーします。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 のタグ付けと標準の適用 AMIs

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 ボリュームの管理と復元に必要な関連情報が存在するように、ボリュームのタグ付けは重要です。タグは、EC2インスタンスからソースボリュームへ、AMIs またはソースボリュームからスナップショットへ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](#)」の技術ホワイトペーパーを参照してください。

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

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

AWS Config ルールとIAMアクセス許可を使用してタグ付けポリシーを適用できます。IAMは強制タグの使用をサポートしているため、Amazon EBSスナップショットを操作するとき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。アクセスIAM許可ポリシーで定義されたタグが 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拒否で失敗します。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 。使用開始に役立つように、 はマネージドルールと呼ばれるカスタマイズ可能な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 を継続的に追跡しますが、これらの変更がルールの条件に違反していないかどうかを確認します。リソースがルールに違反すると、 はリソースとルールを非準拠として AWS Config フラグ付けします。[必須タグ管理ルール](#)は現在、スナップショット および をサポートしていないことに注意してくださいAMIs。

AMIs および EBSスナップショットを使用したEBSボリュームバックアップの作成

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、まだ必要かどうか不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 を作成する前に EBSボリュームを準備する AMI

スナップショットを作成したり、 を作成する前にAMI、EBSボリュームに必要な準備を行います。 を作成するAMI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 にも適用されますAMI。

パワーオンインスタンスで使用されているアタッチ済みEBSボリュームのスナップショットを作成できますEC2。ただし、スナップショットは、スナップショットコマンドの発行時にEBSボリュームに書き込まれたデータのみをキャプチャします。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が。

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。たとえば、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リングして、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ときは、スナップショットを作成する前にインスタンスを停止します。Windows には、アプリケーション整合性のあるスナップショットの作成に役立つボリュームシャドウコピーサービス (VSS) が用意されています。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AMIできるように Windows 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AMIからを作成します。Sysprep は、SIDs コンピュータ名、ドライバなどの一意の情報を Amazon EC2 Windows インスタンスから削除します。複製すると、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ー製品で問題が発生するSIDs可能性があります。AMI がバックアップ目的で、すべての一意の情報をその

そのまま使用して同じインスタンスを復元する場合は、インスタンスで Sysprep を使用しないでください。

コンソールからのEBSボリュームスナップショットの手動作成

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 ボリューム 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。

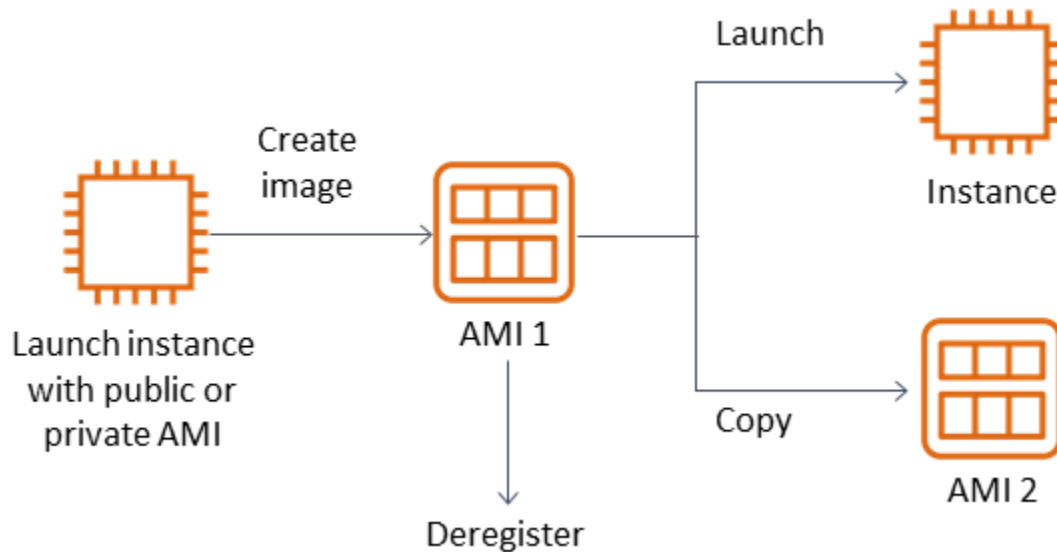
説明を入力し、適切なタグを追加します。Name タグを追加して、後でボリュームを見つけやすくします。タグ付け戦略に基づいて、その他の適切なタグを追加します。

AMIs の作成

は、インスタンスを起動するために必要な情報AMI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ボリュームのルートEBSボリュームとスナップショットが含まれます。EBS スナップショットからのみ新しいインスタンスを起動することはできません。から新しいインスタンスを起動する必要がありますAMI。

を作成するとAMI、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 作成プロセスでは、インスタンスにアタッチされたボリュームごとに Amazon EBSスナップショットが作成され、これらの Amazon EBSスナップショットAMI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AMIの を作成したら、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。アプリケーション移行または DR のために、あるリージョン AMIsから別のリージョンにコピーすることもできます。



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 を作成AMIする必要がありますVMWARE AWS。Amazon EC2コンソールAMIから を作成するには、インスタンスを選択し、アクションを選択し、イメージを選択してから、イメージの作成を選択します。

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](#) を使用できます。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 (およびそのアタッチされた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ため、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および Amazon に含まれる機能ですEBS。Amazon Data Lifecycle Manager は課金されません。

AWS Backup

AWS Backup は Amazon Data Lifecycle Manager と一意です。これは、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ポール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 配列内の EBS ボリューム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している必要があります。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 配列内の EBS ボリュームを復元すると、配列の整合性が低下します。


RAID 配列のスナップショットの一貫したセットを作成するには、[CreateSnapshotsAPI](#) 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。

Snapshots > Create Snapshot

Create Snapshot

Select resource type Volume Instance

Instance ID*  

Description 

Exclude root volume

Volume ID	Volume Type	Encryption
vol-11111111	Root	Encrypted
vol-22222222	EBS	Not Encrypted
vol-33333333	EBS	Not Encrypted
vol-44444444	EBS	Not Encrypted

Copy tags from volume

Key	Value
(127 characters maximum)	(255 characters maximum)

This resource currently has no tags
Choose the Add tag button or [click to add a Name tag](#)

50 remaining (Up to 50 tags maximum)

* Required

RAID 設定に複数のボリュームがアタッチされているインスタンスのスナップショットは、まとめてマルチボリュームスナップショットとして取得されます。マルチボリュームスナップショットは point-in-time、EC2 インスタンスにアタッチされた複数の EBS ボリュームにわたって、データ調整されたクラッシュコンシステントなスナップショットを提供します。スナップショットは複数のボリューム間で自動的に作成されるため、ボリューム間で調整するためにインスタンスを停止する必要はありません。EBS 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、アーカイブアカウントとして別のアカウントを指定し、他のすべてのアカウントがバックアップをコピーできるようにします。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、リージョンで障害が発生した場合に、別のAWSリージョンでEC2インスタンスを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、偶発的な削除保護レイヤーが追加され、ディザスタリカバリ (DR) 目標もサポートされる可能性があります。AWS Backup は、[クロスリージョンバックアップ](#)をサポートします。

[ec2:DeleteSnapshot](#) および [ec2:DeregisterImage](#) アクションへのアクセスIAM許可をブロックすることを検討してください。代わりに、保持ポリシーとメソッドでEBSスナップショットと Amazon EC2 のライフサイクルを管理できますAMI。削除アクションをブロックすることは、EBSスナップショットに1回限りの書き込み、読み取り、多数 (WORM) 戦略を実装する方法の1つです。EBSスナップショットやその他のAWSリソースをサポートする[AWS Backup ポールトロック](#)を使用することもできます。

さらに、[ec2:ModifyImageAttribute](#) AMIsおよび [ec2:ModifySnapshotAttribute](#) IAMアクションをブロックすることで、ユーザーが および EBSスナップショットを共有できないようにすることを検討してください。これにより、AMIおよび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、バックアップポータルで同様のオペレーションをユーザーが実行できないようにします。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、誤って削除された EBS スナップショットを復元するのに役立つ [ごみ箱機能](#) が含まれています。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 コンソールでは複数のスナップショットを選択して 1 回のオペレーションで削除できるため、ユーザーは複数のスナップショットを削除することについて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、ボリュームのコピーを 90 日以上復元する予定のない参照目的で保存するための費用対効果の高い方法です。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完全に削除する前の、適切な中間ステップです。例えば、スナップショットのアーカイブは end-of-lifecycle、使用されなくなった EBS ボリュームのステップとして検討できます。削除するよりもアーカイブする方が、ごみ箱を使用するよりもコスト効率の高い削除保持方法でもあります。

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

バックアップアプローチでは、スナップショットの作成前と AMI 作成後にオペレーション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 作成時にインスタンスを停止して起動する必要がある場合があります。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 および 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 SDK。

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 ランブックを実行するためのアクセス許可をユーザーに付与できます。Amazon EC2 の破壊的コマンドに対するアクセス許可を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も役立ちます。[AWS-CreateSnapshot](#) および [AWS-CreatelImage](#) ランブックを使用してスナップショットとAMIを作成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](#) および [AWS-UpdateWindowsAmi](#) ランブックも含まれています。

AWS CLI および [AWS Tools for Windows PowerShell](#) を使用して、スナップショットとAMI作成プロセスを自動化することもできます。[aws ec2 create-snapshot](#) AWS CLI コマンドを使用して、オートメーションの1ステップとしてEBSボリュームのスナップショットを作成できます。[aws ec2 create-snapshots](#) コマンドを使用して、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のクラッシュコンシステントで同期されたスナップショットを作成できます。

を使用してAWS CLI新しいAMI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インスタンスの復元

EC2 インスタンスにアタッチされた1つのボリュームのみを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、復元されたボリュームをEC2インスタンスにアタッチできます。関連付けられたすべてのボリュームを含むEC2インスタンス全体を復元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。最良の結果を得るには、復元プロセスを低い環境 (非本番環境など) で定期的にテストし、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、および復元プロセスが期待どおりに機能していることを確認します。リストアッププロセスが、リストアップ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ップを調整します。リストアッププロセスをできるだけ自動化し、テストすることで、リストアップ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ッププロセスは、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
- から実行中のインスタンスを復元する AMI

EBS スナップショットからのファイルとディレクトリの復元

[EBS スナップショット](#)は、point-in-time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

既存のEC2インスタンスにアタッチされたボリュームを復元するには、スナップショットからボリュームを作成し、インスタンスにアタッチします。コンソール、AWS CLI、または APIオペレーションを使用して、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スナップショットのデータは、EBSボリュームに非同期的にロードされることに注意してください。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 ボリュームを初期化](#)できます。

- 追加料金で、Amazon EBSは[高速スナップショット復元](#)をサポートしているため、ボリュームを初期化する必要はありません。

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

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

1. Amazon EC2コンソールの Elastic Block Store メニューで、スナップショットを選択します。
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] エントリまたは [Block Devices] エントリ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 ボリューム 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 ボリュームメニューで、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、置き換える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ボリュームを選択し、アクション、ボリュームのアタッチを選択して、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ー (LVM) を使用できます。

- e. EC2 Elastic Block Store ボリューム メニューでそれを選択し、アクション、デタッチボリュームを選択して、置き換える可能性のある以前のボリュームをデタッチします。

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

EBS スナップショットからのEC2インスタンスの作成または復元

EC2 インスタンス全体の復元に使用されるバックアップを作成するには、Amazon マシンイメージ (AMI) を作成することをお勧めします。は、仮想化タイプなどのマシン情報を AMIs キャプチャします。また、デバイスマッピングなど、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、同じ設定で復元できるようにします。

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

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されるスナップショットを検索し、選択します。
3. [アクション] を選択し、[スナップショットから画像を作成] を選択します。
4. 画像の名前 (たとえば `YYYYMMDD-restore-for-i-012345678998765de`) を入力し、新しい画像に適したオプションを選択します。

イメージが作成されて使用可能になったら、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。

から実行中のインスタンスを復元する AMI

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。1 つの方法は、既存のインスタンスを停止し、から新しいインスタンスを起動している間はオフラインのままにして AMI、必要な更新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、ドメインネームサービス (DNS) レコードを更新して、新しいインスタンスを参照できます。

ただし、復元中にインサービス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てください。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。例えば、同じ SIDs とコンピュータ名で実行されているドメイン結合された Windows インスタンスで問題が発生する可能性があります。一意の識別子を必要とするネットワークアプリケーションやサービスでも同様の問題が発生する可能性があります。

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

オンプレミスのインフラから AWS へのバックアップとリカバリ

AWS を使用して、オンプレミスインフラストラクチャのバックアップの耐久性の高いオフサイトストレージを作成できます。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およびリカバリアプローチに統合 SDKs するための広範な API オペレーションとを提供します。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 を通じ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 で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ストレージプロトコルをサポートします。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。

- SMB ベースまたは NFS ベースのアクセスを使用して、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 Amazon S3 クラウドストレージ上の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示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。

- 信頼された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向けるテープゲートウェイ。このゲートウェイは Amazon S3 に接続します。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。

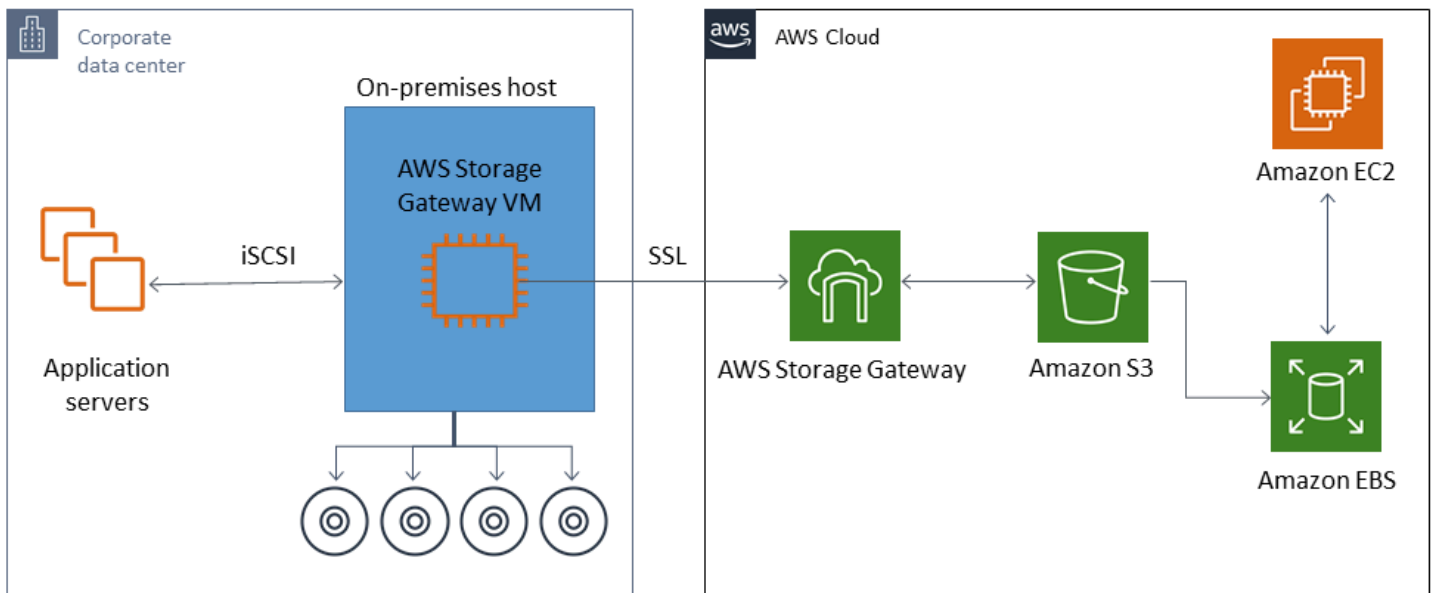
ファイルゲートウェイ

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 と 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、またはファイルゲートウェイに書き込むか、ファイルゲートウェイに書き込む SMB/NFS ことができるスクリプト。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。長期保持のニーズは、バックアップを低コストの S3 Standard-Infrequent Access および S3 Glacier ストレージクラスに階層化することで解決されます。

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 および NFS プロトコルをサポートしているため、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ンングを使用すると、ファイルの以前のオブジェクトバージョンを復元し、SMB または NFS を使用し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用すると、オンプレミスサーバー用にクラウドベースの iSCSI ブロックストレージボリュームを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、ボリュームの完全な point-in-time 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簡単に保存できます。スナップショットとして保存されると、ボリューム全体を EBS ボリュームとして復元し、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 ソリューションを加速できます。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。



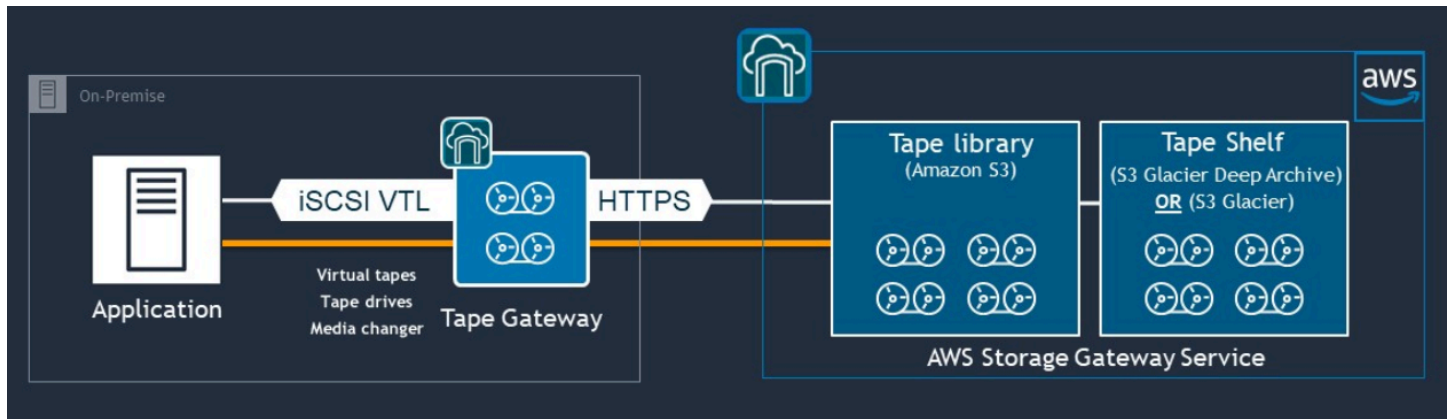
ボリュームゲートウェイは Amazon の Amazon EBS ボリューム機能と統合されているため EC2、AWS Backup を使用してスナップショットプロセスを自動化およびスケジュールできます。ボリュームゲートウェイには、耐久性の高い Amazon S3 ベースの Amazon EBS スナップショットとタグ付け機能という利点があります。詳細については、[Amazon EBS スナップショットのドキュメント](#)を参照してください。

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、および広範な機能を提供します。Amazon S3 に保存されているすべての仮想テープは、少なくとも 3 つの地理的に分散したアベイラビリティゾーンにレプリケートされ、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、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ることと、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、Amazon S3、S3 Glacier Flexible Retrieval、S3 Glacier Deep Archive などの高度にスケーラブル、冗長、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) として機能します。

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の iSCSI ベースの VTL、既存のバックアップアプリケーションに Storage Gateway を提示します。既存のバックアップ・アプリケーションやワークフローを使い続けながら、大規模にスケーラブルな Amazon S3 に保存された仮想テープのコレクションに書き込むことができます。仮想テープ上のデータに即時または頻繁にアクセスする必要がなくなった場合、バックアップアプリケーションはそれを S3 Glacier Flexible Retrieval または S3 Glacier Deep Archive にアーカイブし、ストレージコストをさらに削減することができます。

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

AWS からデータセンターへのアプリケーションのバックアップとリカバリ

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

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

クラウドネイティブ AWS サービスのバックアップとリカバリ

バックアップと復旧のアプローチは、ワークロードで使用される AWS のサービスを対象とする必要があります。は、データを管理および操作するためのサービス固有の機能とオプション AWS を提供します。コンソール、AWS CLI、および API オペレーションを使用して SDKs、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。は DynamoDB と Amazon の両方 AWS Backup をサポートしており、要件を満たす場合は使用 RDS する必要があります。

Amazon のバックアップとリカバリ RDS

Amazon RDS には、データベースのバックアップを自動化する機能が含まれています。Amazon は、データベースインスタンスのストレージボリュームスナップショット RDS を作成し、個々のデータベースだけでなく、DB インスタンス全体をバックアップします。Amazon を使用すると RDS、自動バックアップのバックアップウィンドウを設定し、データベースインスタンススナップショットを作成し、リージョンとアカウント間でスナップショットを共有およびコピーできます。

Amazon RDS には、DB インスタンスをバックアップおよび復元するための 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、point-in-time DB インスタンスのリカバリ (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 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 RDS 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。RDS また、Amazon は 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、データベーストランザクションログとともに毎日のバックアップを使用して 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 コンソールでデータベースの説明タブを確認します。

を開始すると PITR、トランザクションログは、DB インスタンスをリクエストされた時刻に復元するための最も適切な日次バックアップと組み合わせられます。

- 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。Amazon RDSコンソールまたは `CreateDBSnapshot` API 呼び出しを使用して DB スナップショットを作成できます。これらのスナップショットは、コンソールを使用するか、`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 RDS の Amazon 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 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 RDS を禁止します。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。例えば、[mysqldump コマンドを Amazon RDS MySQL データベースとともに](#) 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。場合によっては、Amazon 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 RDS も提供します。例えば、Amazon RDS には、[SQL サーバー RDS データベースのデータベースバックアップをエクスポートおよびインポート](#) するストアードプロシージャが用意されています。

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 レコードを使用したデータベース復旧中のクライアントへの影響の軽減

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。DB インスタンスを復元してライブ 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 RDS。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 インスタンスエンドポイントを指す別のDNSCNAMEレコードを作成し、クライアントにこのDNS名前を使用させることができます。その後、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CNAMEように更新できます。

CNAME レコードの有効期限 (TTL) を適切な値に設定します。TTL 指定するは、別のリクエストが行われる前にレコードがDNSリゾルバーでキャッシュされる期間を決定します。一部のDNSリゾルバーまたはアプリケーションはを優先せずTTL、レコードをよりも長くキャッシュする場合がありますことに注意してくださいTTL。Amazon Route 53 では、より長い値 (172,800 秒、2 日など) を指定すると、再DNS帰的リゾルバーがこのレコードの最新情報を取得するために Route 53 に対して行う必要がある呼び出しの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。

アプリケーションとクライアントのオペレーティングシステムは、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ためにフラッシュまたは再起動する必要があるDNS情報をキャッシュする場合があります。

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では、データベースの復元、復元されたインスタンスDNSへのトラフィックの移行のための更新、および以前のインスタンスに書き込まれる可能性のあるデータの修復がサポートされる場合があります。そうでない場合は、DNSCNAME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 は を提供します。これによりPITR、DynamoDB テーブルデータのほぼ継続的なバックアップが作成されます。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 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API。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 メトリクスとアラーム
- [タグ]
- ストリーム設定
- TTL の設定

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

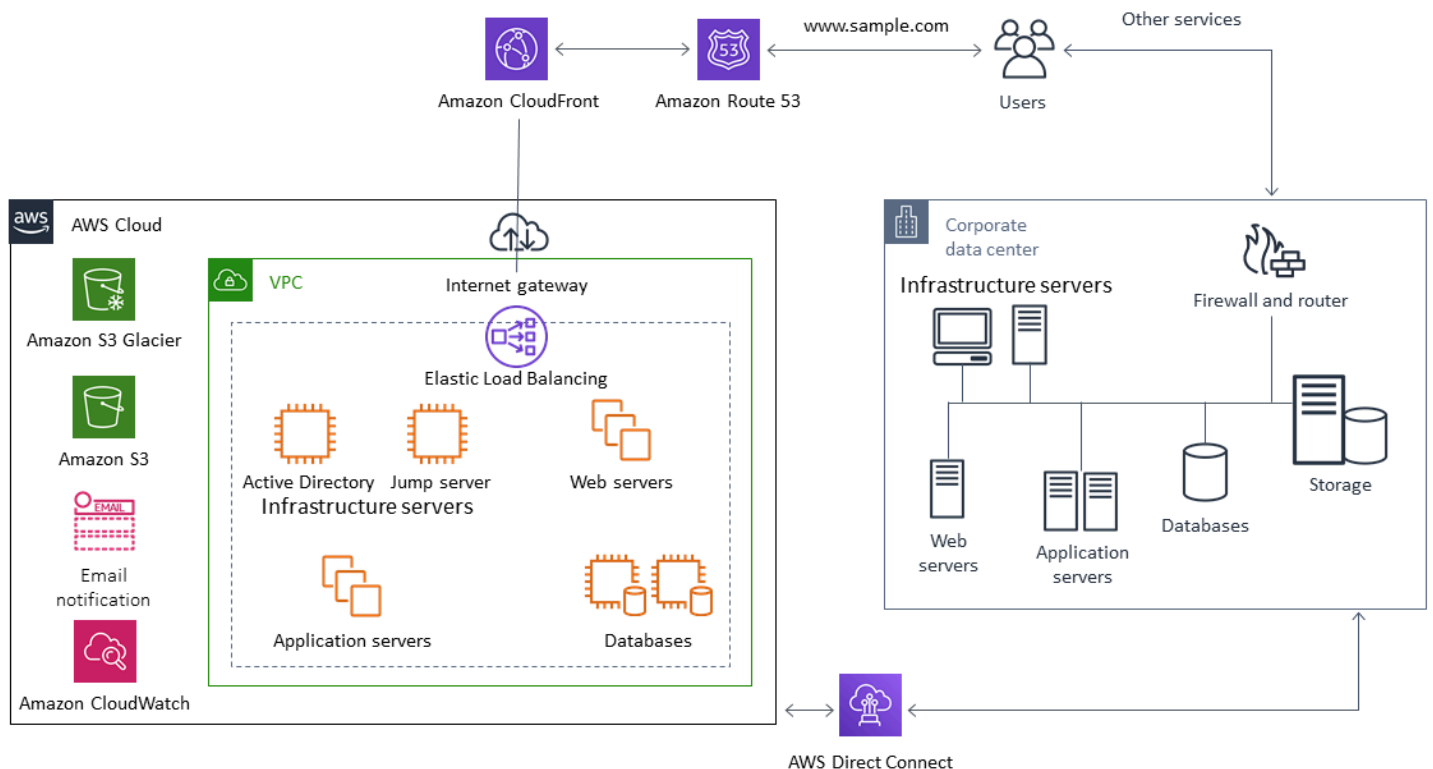
復元プロセスでは、新しく復元されたテーブル名を使用するようにクライアントにどのように指示するかを考慮する必要があります。設定ファイル、AWS Systems Manager パラメータストア値、またはクライアントが使用するテーブル名を反映するように動的に更新できる別のリファレンスから DynamoDB テーブル名を取得するようにアプリケーションとクライアントを設定できます。

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。アクセスIAM許可を使用して既存の 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。これらのお客様のデータセンターは、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。例えば、[AWS Direct Connect](#) を使用すると、オンプレミス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で使用します。多

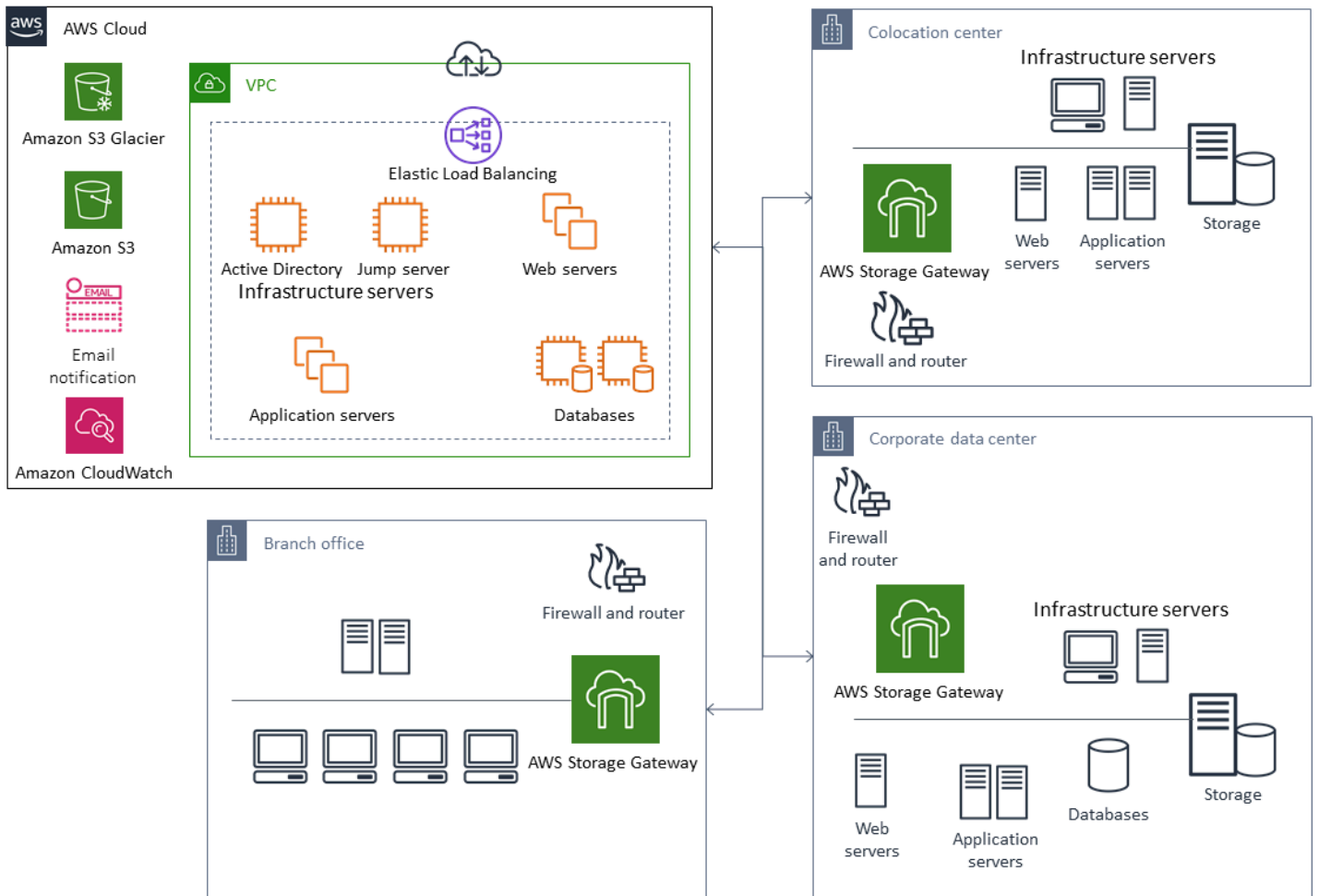
くのは、オンプレミスインフラストラクチャ向けに市場をリードするバックアップおよび復元ソリューションISVsを提供し、ハイブリッドアプローチをサポートするためにソリューションを拡張しています。

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 インスタンスに移動して、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てください。

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 インスタンス近くのメディアサーバーは、インターネット転送のコストを節約します。Amazon S3 にバックアップすると、メディアサーバーは全体的なバックアップとリカバリの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 のために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。



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 を提供しています。

トピック

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

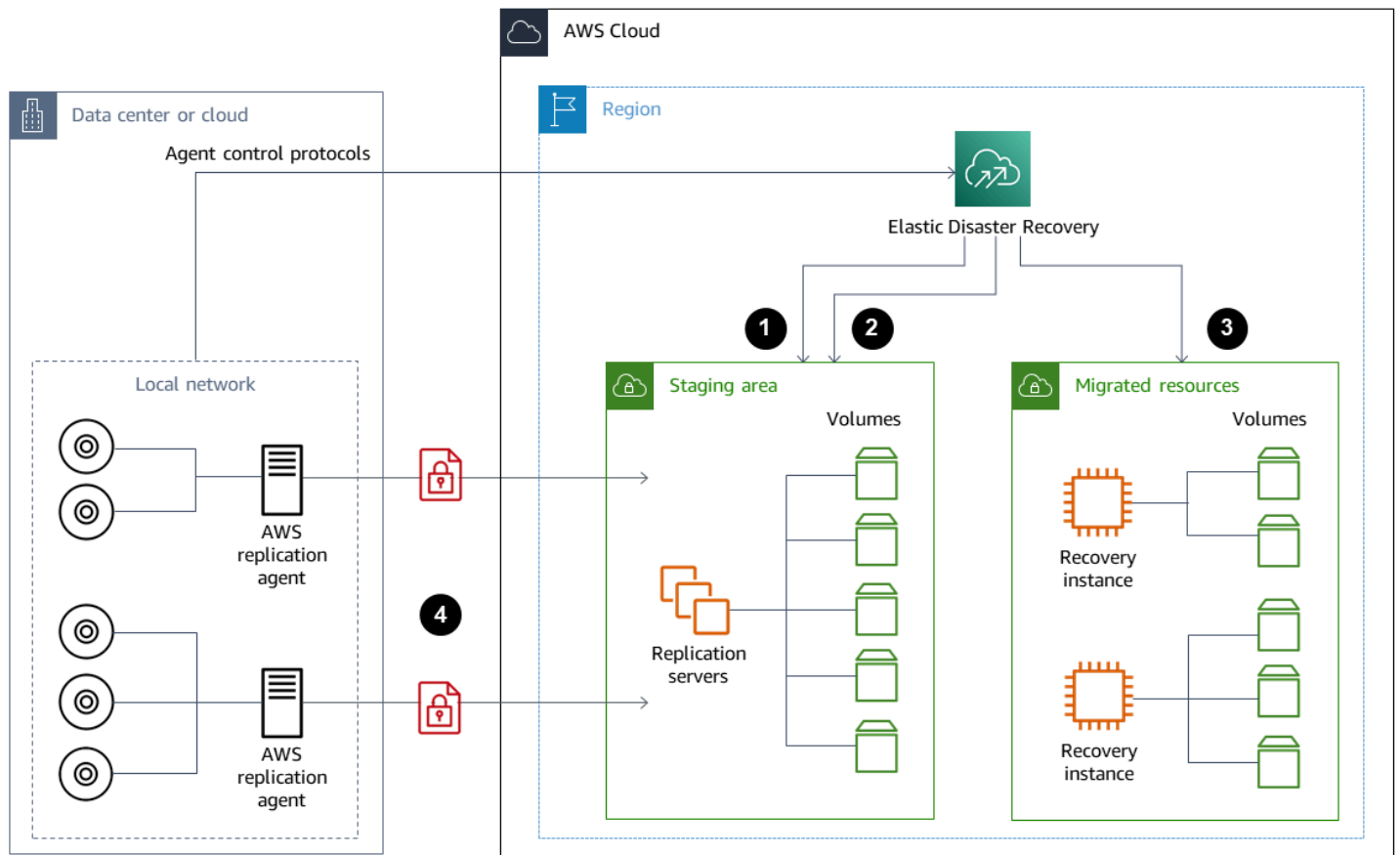
オンプレミス DR から AWS

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 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を作成[AWS Elastic Disaster Recovery](#)するためにを提供します AWS。Elastic Disaster Recovery は、マシンをターゲットAWSアカウントの低コストのステージングエリアに継続的にレプリケートし、優先します AWS リージョン。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、で実行されている低電力の Amazon EC2 同等物と同期します AWS。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 () を低く、より一貫性のあるものにすることができます RTO。



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 分単位と秒単位で起動RPO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が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 ポリ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ポリリュームを提供できます。これらのポリリュームは、Amazon EBSスナップショットEC2を使用して Amazon で使用するためにすばやくプロビジョニングすることもできます。特に、ストアドポリ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。ポリリュームゲートウェイは、オンプレミスでの使用や Amazon での使用のために復元できる、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EC2。ワークロードの目標復旧時点 (RPO) に基づいてスナップショットをスケジュール point-in-timeできます。

Important

ポリリュームゲートウェイポリリュームは、ブートポリリュームとしてではなくデータポリリュームとして使用することを目的としています。

Amazon EC2 マシンイメージ (AMI) は、オンプレミスサーバーに一致し、データポリリュームを個別に指定する設定で使用できます。を設定してテストしたらAMI、ポリリュームゲートウェイスナップショットに基づいて、データポリリュームAMIとともに 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、環境を徹底的にテストして、EC2特に Windows ワークロードでインスタンスが正常に動作していることを確認する必要があります。

クラウドネイティブワークロードの DR

クラウドネイティブのワークロードが DR 目標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 の考慮事項とオプションについて説明しますEC2。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 EC2 での Amazon の DR

複数のアベイラビリティ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 およびその他のサービス用のマルチ AZ サーバーアーキテクチャを実現できます。

アーキテクチャにロードバランシングできない EC2 インスタンスがあり、一度に 1 つのインスタンスしか実行できない場合は、次のいずれかのオプションを使用できます。

- 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。失敗した場合にインスタンスを置き換えるために AMI 使用できるを作成します。から新しくプロビジョニングされたインスタンスを自動的に設定してサービスを提供できるように AMI、適切なオートメーションと設定を定義してください。Auto Scaling グループを指し、複数のアベイラビリティ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 AMI の新しいを作成し、を使用して、別のアベイラビリティゾーンで停止状態の新しい EC2 インスタンスを AMI 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。

リージョン EC2 の障害における Amazon 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、のメリットと照らし合わせて慎重に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 のバックアップとリカバリに固有の利用可能な機能をいくつか紹介します EC2。

AWS AMIs および 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 AMIsを別のリージョンにコピーし、そのリージョン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 また、Amazon Data Lifecycle Manager は、バックアップ設定の一部としてクロスリージョンコピーをサポートします。

[AWS Elastic Disaster Recovery](#) を使用して、Amazon EC2サーバーを自動化し、1つのリージョンの代替 DR リージョンに継続的にレプリケートできます。Elastic Disaster Recovery を使用すると、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できます。Elastic Disaster Recovery は、バックアップとリカバリが RTO および RPOの目標を達成できない場合に役立ちます。Elastic Disaster Recovery を使用すると、を分RTOに、を秒未満の範囲RPOに減らすことができます。

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

バックアップをクリーンアップする

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

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

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

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

バックアップとリカバリ FAQ

どのバックアップスケジュールを選択すればよいですか？

復旧ポイントの目的 () 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RPO。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たびにスナップショットを作成します point-in-time。

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。開発およびテストアクティビティから、開発アカウントと非本番アカウントにはさらに多くの point-in-timeリカバリ (PITR) バックアップがある場合があります。

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てEBSボリュームを引き続き使用できますか？

スナップショットは非同期で発生します。 point-in-timeスナップショットはすぐに作成されますが、変更されたすべてのブロックが Amazon S3 に転送されるまで、スナップショットのステータスは保留中です。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。

追加リソース

AWS リソース

- [AWS 規範ガイド](#)
- [「AWS ドキュメント」](#)
- [AWS 参考文献](#)
- [「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: クラウドでのリカバリ \(ホワイトペーパー\)](#)
- [ディザスタリカバリシリーズ \(AWS アーキテクチャブログ記事\)](#)
- [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。今後の更新について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 セクションのガイドを更新しました。	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」 ためのガイド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」 セクションと 「データ保護のための AWS サービスの選択」 セクションに、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を使用した Amazon の EC2 バックアップとリカバリ AMIs、スナップショットまたはを作成する前の EBS ボリュームの準備 AMI、Amazon EBS スナップショットまたはセクションからの復元で AMI、明確化が追加されました。 Backup とリカバリ FAQ に を追加しました。	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 Data Lifecycle 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、 のサービスを追加しました。Backup を使用した Backup とリカバリのセクションを追加しましたAWS。 「Amazon S3 と Amazon S3 Glacier を使用したバックアップとリカバリ」セクションに、新しい Amazon S3 Glacier ストレージクラスに関する情報を追加しました。「 EBS ボリューム EC2 を使用した Amazon のバックアップとリカバリ 」セクションに、ドキュメントへのリンクと追加情報を追加しました。「 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。スナップショットとセクション を使用して Amazon EC2バックアップとリカバリにスナップショットAMIs を取得する方法についての情報を追加しました。	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 規範的ガイドの用語集

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

数字

7 Rs

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

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

A

ABAC

[「属性ベースのアクセスコントロール」](#)を参照してください。

抽象化されたサービス

[「マネージドサービス」](#)を参照してください。

ACID

[不可分性、一貫性、分離性、耐久性](#)を参照してください。

アクティブ - アクティブ移行

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

アクティブ - パッシブ移行

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

集計関数

行のグループを操作し、グループの単一の戻り値を計算する SQL 関数。集計関数の例には、SUM や [MAX](#) があります。

AI

[「人工知能」](#)を参照してください。

AIOps

[「人工知能オペレーション」](#)を参照してください。

匿名化

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

アンチパターン

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

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

人工知能オペレーション (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。移行戦略での AWS AIOps の使用方法の詳細については、「[オペレーション統合ガイド](#)」を参照してください。

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。

不可分性、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コントロール (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「[for 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。

アベイラビリティゾーン

他のアベイラビリティゾーンの障害から 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)

組織がクラウドに正常に移行するための効率的で効果的な計画を立て AWS ののに役立つ、からのガイドラインとベストプラクティスのフレームワークです。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編成しています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、AWS CAF は、クラウド導入を成功させるための組織の準備に役立つ人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、[AWS CAFウェブサイト](#)と[AWS CAF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、作業の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

個人や組織に混乱を与えたり、損害を与えたりすることを意図した[ボット](#)。

BCP

[事業継続計画](#)を参照してください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。 [エンディアン性](#) も参照してください。

二項分類

バイナリ結果 (2 つの可能なクラスのうちの一つ) を予測するプロセス。例えば、お客様の機械学習モデルで「この E メールはスパムですか、それともスパムではありませんか」などの問題を予測する必要があるかもしれません。または「この製品は書籍ですか、車ですか」などの問題を予測する必要があるかもしれません。

ブルームフィルター

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

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンは 1 つの環境 (青) で実行し、新しいアプリケーションバージョンは別の環境 (緑) で実行します。この戦略は、最小限の影響ですばやく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ウラーなど、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、個人や組織に混乱を与えたり、損害を与えたりすることを意図しているものがあります。

ボットネット

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

ブランチ

コードリポジトリに含まれる領域。リポジトリに最初に作成するブランチは、メインブランチといます。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なら、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、「[About branches](#) (GitHub documentation)」を参照してください。

ブレイクグラスアクセス

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、Well-Architected ガイドの「[ブレイクグラスプロセスの実装](#)」インジケータ AWS を参照してください。

ブラウンフィールド戦略

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

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

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

事業継続計画 (BCP)

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

C

CAF

[AWS 「クラウド導入フレームワーク」](#) を参照してください。

Canary デプロイ

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

CCoE

[「Cloud Center of Excellence」](#) を参照してください。

CDC

[「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、同期を維持するために、ターゲットシステムの変更の監査やレプリケーションなど、さまざまな目的で使用できます。

カオスエンジニアリング

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

CI/CD

[「継続的インテグレーションと継続的デリバリー」](#) を参照してください。

分類

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

クライアント側の暗号化

ターゲットがデータ AWS のサービスを受信する前に、ローカルでデータを暗号化します。

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 [CCoE の投稿](#) を参照してください。

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

組織は通常、に移行する際に次の 4 つのフェーズを実行します AWS クラウド。

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

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

CMDB

[「設定管理データベース」](#)を参照してください。

コードリポジトリ

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

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する [AI](#) の分野。例えば、はオンプレミスのカメラネットワークに CV を追加するデバイス AWS Panorama を提供し、Amazon SageMaker AI は CV のイメージ処理アルゴリズムを提供します。

設定ドリフト

ワークロードの場合、設定は想定した状態から変化します。これにより、ワークロードが非標準になる可能性があり、通常は段階的で意図的ではありません。

設定管理データベース (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、移行のポートフォリオ検出および分析段階で CMDB のデータを使用します。

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 とリージョン、または組織全体の単一のエンティティとしてデプロイできます。詳細については、AWS Config ドキュメントの「[コンフォーマンスパック](#)」を参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

ソフトウェアリリースプロセスのソース、ビルド、テスト、ステージング、本番稼働の各段階を自動化するプロセス。CI/CD is commonly described as a pipeline. CI/CDは、プロセスの自動化、生産性の向上、コード品質の向上、迅速な提供に役立ちます。詳細については、「[継続的デリバリーの利点](#)」を参照してください。CD は継続的デプロイ (Continuous Deployment) の略語でもあります。詳細については「[継続的デリバリーと継続的なデプロイ](#)」を参照してください。

CV

「[コンピュータビジョン](#)」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

一元化された管理とガバナンスにより、分散され分散されたデータ所有権を提供するアーキテクチャフレームワーク。

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。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していることを確認できます。詳細については、「[でのデータ境界の構築 AWS](#)」を参照してください。

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

[「データベース定義言語」](#)を参照してください。

ディープアンサンブル

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

ディープラーニング

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

defense-in-depth

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を採用するときは AWS、AWS Organizations 構造の異なるレイヤーに複数のコントロールを追加して、リソースの安全性を確保します。例えば、アプローチでは defense-in-depth、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で利用できるサービス](#)を参照してください。

デプロイ

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

開発環境

[???](#)「環境」を参照してください。

検出管理

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

開発値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速度と品質に悪影響を及ぼす制約を特定して優先順位を付けるために使用されるプロセス。は、もともと効率的な製造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DVSMを拡張します。ソフトウェア開発プロセスを通じて価値を創造し、動かすために必要なステップとチームに焦点を当てています。

デジタルツイン

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

ディメンションテーブル

[スタースキーマ](#)では、ファクトテーブル内の量的データに関するデータ属性を含む小さなテーブル。ディメンションテーブル属性は通常、テキストフィールドまたはテキストのように動作する離散数値です。これらの属性は、クエリの制約、フィルタリング、結果セットのラベル付けによく使用されます。

ディザスタ

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

ディザスタリカバリ (DR)

[災害](#)によるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。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については、[「従来の Microsoft ASP.NET \(ASMX\) ウェブサービスをコンテナと Amazon API Gateway を使用して段階的にモダナイズする」](#)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の追跡。例えば、AWS CloudFormation を使用して[システムリソースのドリフトを検出](#)したり、を使用して AWS Control Tower、ガバナンス要件への準拠に影響を与える可能性のある[ランディングゾーンの変更を検出](#)したりできます。

DVSM

[「開発値ストリームマッピング」](#)を参照してください。

E

EDA

[「探索的なデータ分析」](#)を参照してください。

EDI

[「電子データ交換」](#)を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

[「サービスエンドポイント」](#)を参照してください。

エンドポイントサービス

仮想プライベートクラウド (VPC) 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、インターフェイスエンドポイントを作成することでVPC、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の作成」](#)を参照してください。

エンタープライズリソース計画 (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、アイデンティティとアクセスの管理、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。

探索的なデータ分析 (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。データを収集または集計し、初期調査を実行してパターンを見つけ、異常を検出し、仮定を確認します。EDAは、サマリー統計を計算し、データの視覚化を作成することによって実行されます。

F

ファクトテーブル

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

フェイルファスト

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

障害分離境界

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

機能ブランチ

[「ブランチ」](#)を参照してください。

特徴量

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

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Descriptions (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として表されます。詳細については、[「を使用した機械学習モデルの解釈可能性 AWS」](#)を参照してください。

機能変換

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

数ショットプロンプト

同様のタスクを実行するように依頼する前に、タスクと必要な出力を示す [LLM](#) 少数の例を に提供します。この手法はコンテキスト内学習のアプリケーションであり、モデルはプロンプトに埋め

込まれた例 (ショット) から学習します。少数のショットプロンプトは、特定のフォーマット、推論、またはドメインの知識を必要とするタスクに効果的です。[「ゼロショットプロンプト」](#) も参照してください。

FGAC

[「きめ細かなアクセスコントロール」](#) を参照してください。

きめ細かなアクセスコントロール (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

[「基盤モデル」](#) を参照してください。

基盤モデル (FM)

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

G

生成 AI

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

ジオブロッキング

[地理的制限](#) を参照してください。

地理的制限 (ジオブロッキング)

Amazon では CloudFront、特定の国のユーザーがコンテンツディストリビューションにアクセスできないようにするオプションです。アクセスを許可する国と禁止する国は、許可リストまたは

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

Gitflow ワークフロー

下位環境と上位環境が、ソースコードリポジトリでそれぞれ異なるブランチを使用する方法。Gitflow ワークフローはレガシーと見なされ、[トランクベースのワークフロー](#)は最新の推奨アプローチです。

ゴールデンイメージ

システムまたはソフトウェアの新しいインスタンスをデプロイするためのテンプレートとして使用されるシステムまたはソフトウェアのスナップショット。例えば、製造では、ゴールデンイメージを使用して複数のデバイスにソフトウェアをプロビジョニングし、デバイスの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 () 全体のリソース、ポリシー、コンプライアンスを管理するのに役立つ高レベルのルール OUs。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは AWS Config、Amazon AWS Security Hub、GuardDuty、AWS Trusted Advisor Amazon Inspector、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

[「高可用性」](#)を参照してください。

異種混在データベースの移行

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

ハイアベイラビリティ (HA)

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

ヒストリアンのモダナイゼーション

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

ホールドアウトデータ

[機械学習](#) モデルのトレーニングに使用されるデータセットから保留される、ラベル付きの履歴データの一部。ホールドアウトデータを使用してモデル予測をホールドアウトデータと比較することで、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

ソースデータベースを、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) に移行します。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。緊急性のため、通常、修正は一般的な DevOps リリースワークフローの外部で行われます。

ハイパーケア期間

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

|

laC

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

IIoT

[「産業モノのインターネット」](#) を参照してください。

イミュータブルインフラストラクチャ

既存のインフラストラクチャを更新、パッチ適用、または変更するのではなく、本番ワークロードに新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的に [ミュータブルなインフラストラクチャ](#) よりも一貫性、信頼性、予測性が高くなります。詳細については、AWS Well-Architected フレームワークの [「イミュータブルインフラストラクチャを使用したデプロイ」](#) 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 (インGRESS) VPC

AWS マルチアカウントアーキテクチャでは、アプリケーション外からのネットワーク接続を受け入れ、検査し、ルーティング VPC するです。 [AWS セキュリティリファレンスアーキテクチャ](#) 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インターフェイス VPCs を保護するために、インバウンド、アウトバウンド、検査を使用してネットワークアカウントを設定することをお勧めします。

|

増分移行

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

インダストリー 4.0

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

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

産業モノのインターネット (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、[「産業モノのインターネット \(IIoT\) 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。

検査 VPC

AWS マルチアカウントアーキテクチャでは、VPCs (同じまたは異なる内 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VPCを管理する一元化されたです。[AWS セキュリティリファレンスアーキテクチャ](#)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インターフェイスVPCsを保護するために、インバウンド、アウトバウンド、検査を使用してネットワークアカウントを設定することをお勧めします。

IoT

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

解釈可能性

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

IoT

[「モノのインターネット」](#)を参照してください。

IT 情報ライブラリ (ITIL)

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

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

ラベルベースのアクセスコントロール (LBAC)

ユーザーとデータ自体にそれぞれ明示的にセキュリティラベル値が割り当てられている、必須のアクセスコントロール (MAC) の実装。ユーザーセキュリティラベルとデータセキュリティラベルが交差する部分によって、ユーザーに表示される行と列が決まります。

ランディングゾーン

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

大規模言語モデル (LLM)

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

大規模な移行

300 台以上のサーバの移行。

LBAC

[「ラベルベースのアクセスコントロール」](#)を参照してください。

最小特権

タスクの実行には必要最低限の権限を付与するという、セキュリティのベストプラクティス。詳細については、IAMドキュメントの[「最小特権の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

[「7R」](#)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。[エンディアンネス](#)も参照してください。

LLM

[「大規模言語モデル」](#)を参照してください。

下位環境

[「???」](#)「環境」を参照してください。

M

機械学習 (ML)

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

メインブランチ

[「ブランチ」](#)を参照してください。

マルウェア

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

マネージドサービス

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

製造実行システム (MES)

生産プロセスを追跡、モニタリング、文書化、制御するためのソフトウェアシステム。このソフトウェアシステムは、加工品を現場の完成製品に変換します。

MAP

[「移行促進プログラム」](#) を参照してください。

メカニズム

ツールを作成し、ツールの導入を推進し、調整のために結果を検査する完全なプロセス。メカニズムは、動作中にそれ自体を強化して改善するサイクルです。詳細については、AWS Well-Architected フレームワークの [「メカニズムの構築」](#) を参照してください。

メンバーアカウント

組織の一部である管理アカウント AWS アカウント 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。

メッセージキューイングテレメトリトランスポート (MQTT)

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

マイクロサービス

明確に定義された上で通信APIsし、通常は小規模で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。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、軽量な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APIs。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)

コンサルティングサポート、トレーニング、およびサービスを提供する AWS プログラムは、組織がクラウドへの移行のための強固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ちます。MAPには、レガシー移行を体系的に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ための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と所有者、移行エンジニア、デベロッパー、スプリントに取り組む 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には、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 EC2を使用して Amazon への移行をリホストします。

移行ポートフォリオ評価 (MPA)

に移行するためのビジネスケースを検証するための情報を提供するオンラインツール AWS クラウド。MPAは、詳細なポートフォリオ評価 (サーバーの適切なサイズ設定、料金設定、TCO比較、移行コスト分析) と移行計画 (アプリケーションデータ分析とデータ収集、アプリケーショングループ化、移行の優先順位付け、ウェブプランニング) 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)

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 AWS CAF。詳細については、「[移行準備ガイド](#)」を参照してください。MRAは[AWS 移行戦略](#)の最初のフェーズです。

移行戦略

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

ML

「[機械学習](#)」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

組織のアプリケーションのモダナイゼーションの準備状況を判断し、利点、リスク、依存関係を特定し、組織がこれらのアプリケーションの将来の状態をどの程度適切にサポートできるかを決定するのに役立つ評価。評価の結果として、ターゲットアーキテクチャのブループリント、モダナイゼーションプロセスの開発段階とマイルストーンを詳述したロードマップ、特定され

たギャップに対処するためのアクションプランが得られます。詳細については、[「」の「アプリケーションのモダナイゼーション準備状況の評価 AWS クラウド」](#)を参照してください。

モノリシックアプリケーション (モノリス)

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

MPA

[「移行ポートフォリオ評価」](#)を参照してください。

MQTT

[「Message Queuing Telemetry Transport」](#)を参照してください。

多クラス分類

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

ミュータブルインフラストラクチャ

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

O

OAC

[「オリジンアクセスコントロール」](#)を参照してください。

OAI

[「オリジンアクセスアイデンティティ」](#)を参照してください。

OCM

[「組織の変更管理」](#)を参照してください。

オフライン移行

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

OI

[「オペレーションの統合」](#)を参照してください。

OLA

[「運用レベルの契約」](#)を参照してください。

オンライン移行

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

OPC-UA

[「オープンプロセス通信 - 統合アーキテクチャ」](#)を参照してください。

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

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

運用レベルの契約 (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、各当事者が相互に提供することを約束する機能的な IT グループを明確にする契約 SLA。

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の理解、評価、防止、または範囲の縮小に役立つ質問のチェックリストおよび関連するベストプラクティス。詳細については、AWS Well-Architected フレームワークの [「運用準備状況レビュー \(ORR\)」](#) を参照してください。

運用テクノロジー (OT)

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

オペレーション統合 (OI)

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

組織の証跡

組織 AWS アカウント 内のすべてのイベント 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、ドキュメントの「[組織の証跡の作成](#)」を参照してください。CloudTrail

組織の変更管理 (OCM)

人材、文化、リーダーシップの観点から、破壊的で重要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、文化的および組織的な変化を促進することで、組織が新しいシステムや戦略の準備と移行を支援します。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から、このフレームワークを人材アクセラレーションと呼びます。詳細については、[OCMガイド](#)を参照してください。

オリジンアクセスコントロール (OAC)

では CloudFront、Amazon Simple Storage Service (Amazon S3) コンテンツを保護するためのアクセスを制限するための拡張オプションです。OACは、すべての S3 バケット、AWS KMS (SSEKMS) によるサーバー側の暗号化 AWS リージョン、および 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)

では CloudFront、Amazon S3 コンテンツを保護するためのアクセスを制限するオプションです。を使用するとOAI、は Amazon S3 が認証できるプリンシパル CloudFront を作成します。認証されたプリンシパルは、特定の CloudFront ディストリビューションを介してのみ S3 バケット内のコンテンツにアクセスできます。「」も参照してください。より詳細で拡張[OAC](#)されたアクセスコントロールを提供します。

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 (出力) 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VPCを処理する ます。[AWS セキュリティリファレンスアーキテクチャ](#)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インターフェイスVPCsを保護するために、インバウンド、アウトバウンド、検査を使用してネットワークアカウントを設定することをお勧めします。

P

アクセス許可の境界

ユーザーまたはロールが持つことができるアクセス許可の上限を設定するために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。例としては、名前、住所、連絡先情報PIIなどがあります。

PII

[個人を特定できる情報](#)を参照してください。

プレイブック

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

PLC

[「プログラム可能なロジックコントローラー」](#)を参照してください。

PLM

[「製品ライフサイクル管理」](#)を参照してください。

ポリシー

アクセス許可の定義 ([アイデンティティベースのポリシー](#)を参照)、アクセス条件の指定 ([リソースベースのポリシー](#)を参照)、または の組織内のすべてのアカウントに対する最大アクセス許可の定義 AWS Organizations ([サービスコントロールポリシー](#)を参照) が可能なオブジェクト。

多言語の永続性

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

ポートフォリオ評価

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

述語

true または を返すクエリ条件。通常は false WHERE 句にあります。

述語のプッシュダウン

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

予防的コントロール

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

プリンシパル

アクションを実行し 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、AWS アカウント IAM 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「[ロールの用語と概念](#)」の「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

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

プライベートホストゾーン

Amazon Route 53 が 1 つ以上の 内のドメインとそのサブドメインのDNSクエリに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VPCs。詳細については、Route 53 ドキュメントの「[プライベートホストゾーンの使用](#)」を参照してください。

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

設計、開発、発売から成長と成熟、辞退と削除まで、ライフサイクル全体にわたる製品のデータとプロセスの管理。

本番環境

[「環境」](#)を参照してください。

プログラム可能なロジックコントローラー (PLC)

製造では、マシンをモニタリングし、承認プロセスを自動化する、信頼性が高く、適応性の高いコンピュータです。

プロンプトの連鎖

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

仮名化

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

publish/subscribe (pub/sub)

マイクロサービス間の非同期通信を可能にするパターン。スケーラビリティと応答性を向上させます。たとえば、マイクロサービスベースの [MES](#)、マイクロサービスは他のマイクロサービスがサブスクライブできるチャンネルにイベントメッセージを発行できます。システムは、公開サービスを変更せずに新しいマイクロサービスを追加できます。

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

[責任、説明責任、相談、通知 \(RACI\) を参照してください。](#)

RAG

[「取得拡張生成」](#)を参照してください。

ランサムウェア

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

RASCI マトリックス

[責任、説明責任、相談、通知 \(RACI\) を参照してください。](#)

RCAC

[「行と列のアクセスコントロール」](#)を参照してください。

リードレプリカ

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

再構築

[「7R」](#)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)

サービスが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

[「7R」](#) を参照してください。

リージョン

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

回帰

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

リホスト

[「7R」](#) 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

[「7R」](#) を参照してください。

プラットフォーム変更

[「7R」](#) を参照してください。

再購入

[「7R」](#) を参照してください。

回復性

中断に耐えたり、中断から回復したりするアプリケーションの機能。[高可用性](#)と[ディザスタリカバリ](#)は、回復性を計画する際の一般的な考慮事項です AWS クラウド。詳細については、[AWS クラウド「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。

責任、説明責任、相談、情報 (RACI) マトリックス

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

レスポンスコントロール

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

保持

[「7R」](#)を参照してください。

廃止

[「7R」](#)を参照してください。

取得拡張生成 (RAG)

レスポンスを生成する前に、ガ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LLMを参照する[生成 AI](#) テクノロジー。たとえば、RAGモデルは組織のナレッジベースやカスタムデータのセマンティック検索を実行する場合があります。詳細については、「[RAG とは](#)」を参照してください。

ローテーション

攻撃者が認証情報にアクセスするのをより困難にするために、[シークレット](#)を定期的に更新するプロセス。

行と列のアクセスコントロール (RCAC)

アクセスルールが定義されている基本的で柔軟なSQL式を使用します。RCACは、行のアクセス許可と列マスクで構成されます。

RPO

「[目標復旧時点](#)」を参照してください。

RTO

[目標復旧時間](#)を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdPs) が使用するオープンスタンダード。この機能を使用すると、フェデレーテ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 [AWS Management Console](#) したり、AWS API オペレーションを呼び出したりできます。組織内のすべてのユーザーIAMに対して [ユーザーを作成する必要はありません](#)。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SAMLの「[About SAML 2.0-based federation](#)」を参照してください。

SCADA

「[監視コントロールとデータ取得](#)」を参照してください。

SCP

「[サービスコントロールポリシー](#)」を参照してください。

シークレット

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

設計によるセキュリティ

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

セキュリティコントロール

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

セキュリティ強化

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

セキュリティ情報とイベント管理 (SIEM) システム

セキュリティ情報管理 (SIM) システムとセキュリティイベント管理 (SEM) 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、その他の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、アラートを生成します。

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修正するように設計された、事前定義されたプログラムされたアクション。これらの自動化は、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、認証情報のローテーションなどがあります。

サーバー側の暗号化

送信先で、それを受け取る AWS のサービス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)

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制御するポリシー AWS Organizations。は、ガードレール SCPs を定義するか、管理者がユーザーまたはロールに委任できるアクションの制限を設定します。を許可リストまたは拒否リスト SCPs として使用して、許可または禁止するサービスまたはアクションを指定できます。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

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベルの目標 (SLO)

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

責任共有モデル

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

SIEM

[セキュリティ情報とイベント管理システム](#)を参照してください。

単一障害点 (SPOF)

システムを中断する可能性のある、アプリケーションの単一の重要なコンポーネントの障害。

SLA

[「サービスレベルアグリーメント」](#)を参照してください。

SLI

[「サービスレベルインジケータ」](#)を参照してください。

SLO

[「サービスレベルの目標」](#)を参照してください。

split-and-seed モデル

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

SPOF

[単一障害点](#)を参照してください。

star スキーマ

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

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、宿主にと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](#)。このパターンを適用する方法の例については、「[従来の Microsoft ASP.NET \(ASMX\) ウェブサービスをコンテナと Amazon API Gateway を使用して段階的にモダナイズする](#)」を参照してください。

サブネット

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

監視コントロールとデータ収集 (SCADA)

製造では、ハードウェアとソフトウェアを使用して物理アセットと生産オペレーションをモニタリングするシステム。

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

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

システムプロンプト

動作を指示 [LLM](#) するために、コンテキスト、指示、またはガイドラインを に提供するための手法。システムプロンプトは、コンテキストを設定し、ユーザーとのやり取りのルールを確立するのに役立ちます。

T

tags

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

ターゲット変数

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

タスクリスト

ランブックの進行状況を追跡するために使用されるツール。タスクリストには、ランブックの概要と完了する必要が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

VPCs とオンプレミスの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トランジットハブ。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の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「[AWS Organizations を他の AWS サービスで使用する 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

ピザを2つ用意できる小さな 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VPCsできる 2 つの間の接続。詳細については、Amazon VPCドキュメントの「[What is VPC peering](#)」を参照してください。

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

[「書き込み 1 回」、「読み取り 多数」を参照してください。](#)

WQF

[AWS 「ワークロード認定フレームワーク」を参照してください。](#)

1 回書き、多く読み込む (WORM)

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

Z

ゼロデイ 익스プロイト

[ゼロデイ脆弱性](#) を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

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

ゼロショットプロンプト

タスクを実行するための指示を [LLM](#) に提供しますが、そのガイドに役立つ例 (ショット) はありません。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 LLM 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

平均使用量 CPU とメモリ使用量が 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。