エンタープライズ環境への Amazon FSx for NetApp ONTAP のデプロイ

AWS 規範ガイダンス

AWS 規範ガイダンス: エンタープライズ環境への Amazon FSx for NetApp ONTAP のデプロイ

Table of Contents

エンタープライズ環境への Amazon FSx for NetApp ONTAP のデプロイ

Luigi Seregni、Antonio Aga Rossi、Giulio Dipace、Amazon Web Services (AWS)

2023 年 8 月 (ドキュメント履歴)

ワークロードをクラウドに移行すると、組織の成長を促進し、変化する市場環境に適応できるようになります。スケーラビリティ、俊敏性、耐障害性を実現するクラウドの機能によって、アプリケーションのサービスレベルを高めることができるためです。

毎年、新しい国際会計基準 (IFRS) などの新しいルールと規制が導入されるなか、基準の進化についてゆくには、多くの場合、計算能力の向上が必要になりますが、それをオンプレミスのシステムで実現するのは難しい場合があります。ハイパフォーマンスコンピューティング (HPC) アプリケーションは非常に高いストレージスループット要件を持つため、クラウドまたはハイブリッドクラウド環境への移行の最有力候補です。

Amazon FSx for NetApp ONTAP は、そうした HPC アプリケーションの高いスループット要件に対応したクラウドサービスであり、オンプレミスの ONTAP ワークロードと下位互換性があります。このガイドを使用すると、完全な機能セットを備えた FSx for ONTAP ソリューションをエンタープライズ環境にデプロイできます。特にエンタープライズ環境と題している理由は、このガイドが FSx for ONTAP サービスにのみ焦点を当てるのではなく、包括的な視点で、この種のファイルシステムを複雑な環境にデプロイするための考慮事項を紹介しているためです。

さらにこのガイドでは、Active Directory の統合、サービスアカウントのデプロイ、ONTAP コマンドラインのトラブルシューティング、ストレージ仮想マシン (SVM) の設定など、一般的なデプロイの課題についても説明します。

ガイドには次の 4 つのセクションがあります。

- アーキテクチャ – この章では、FSx for ONTAP を使用する可能性のあるエンタープライズアーキテクチャの概要を示し、さまざまなコンポーネント間の相互作用と適切な使用パターンについて説明します。
- ファイルシステムの作成 – このセクションでは、完全に機能する FSx for ONTAP 環境を構築するためのすべてのアクションを紹介します。ソリューションを手動でデプロイするためのステップバイステップのガイドラインを掲載しています。
- ベストプラクティス – この章では、エンタープライズ環境で FSx for ONTAP をデプロイするアクティビティから得られた推奨事項とベストプラクティスを紹介します。

- よくある質問 – このセクションには、テクノロジーに関する一般的な懸念事項に対する一連の質問が掲載されています。

対象者

このガイドは、HPC ワークロードと Active Directory 統合をサポートする FSx for ONTAP ソリューションをデプロイするクラウド管理者とアーキテクトを支援することを目的としています。

目的

このガイドは、お客様や組織が以下のことを行うのに役立ちます。

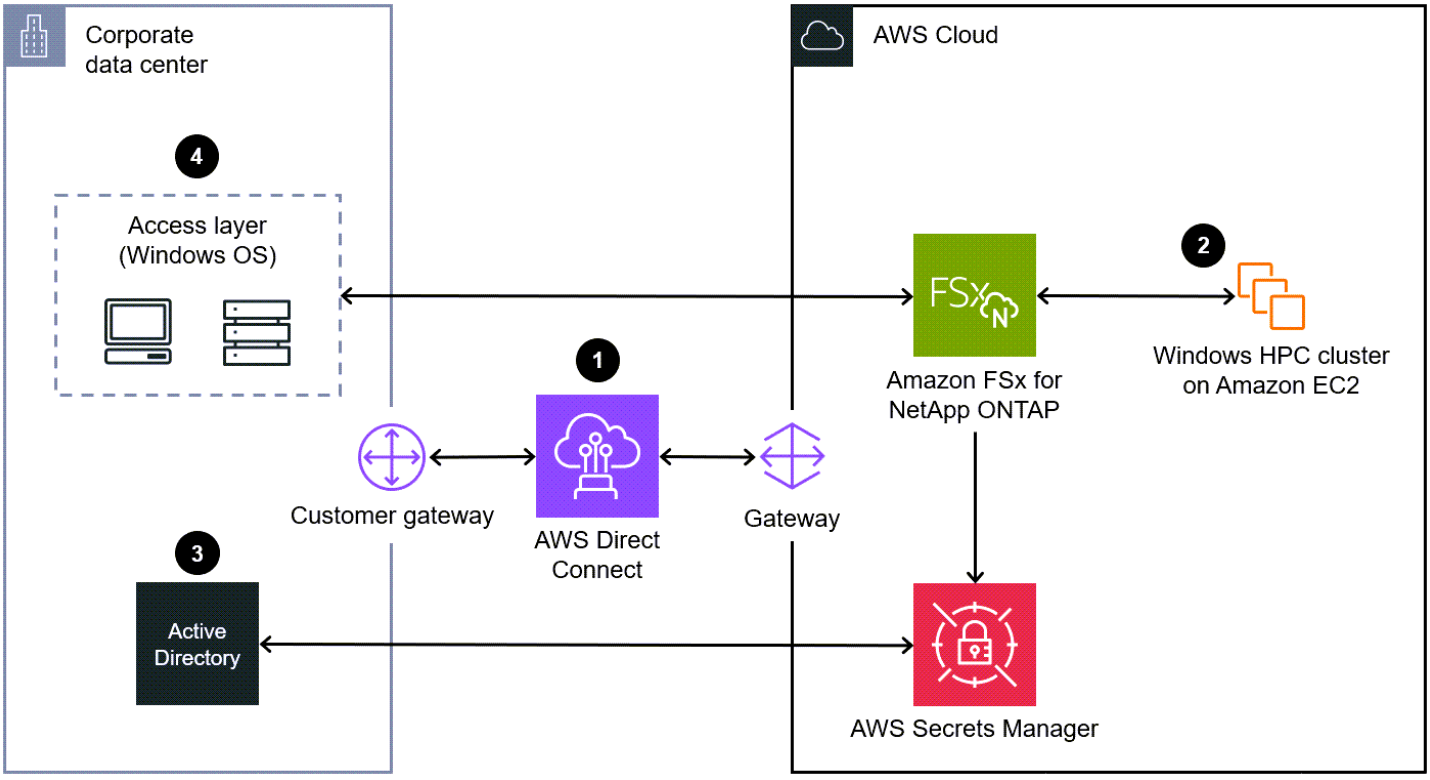
- アーキテクチャを理解し、完全な機能セットを備えた FSx for ONTAP ソリューションをエンタープライズ環境にデプロイする
- FSx for ONTAP を Active Directory と統合する
- サービスアカウントを作成して、本番環境で FSx for ONTAP を Active Directory に接続する
- Amazon FSx のストレージ階層を管理する
- ONTAP コマンドラインを使用してトラブルシューティングする
- ストレージ仮想マシン (SVM) の設定の問題をトラブルシューティングする (NetApp ドキュメント)
- Service Message Block (SMB) プロトコルを使用して、FSx for ONTAP ファイルシステムのデータにアクセスする

エンタープライズ環境に FSx for ONTAP をデプロイするためのアーキテクチャ

Amazon FSx for NetApp ONTAP は、AWS クラウドでフルマネージド型の ONTAP ファイルシステムを起動して実行できるストレージサービスです。FSx for ONTAP は Windows または Linux オペレーティングシステム (OS) をサポートしており、ネットワークファイルシステム (NFS)、サーバーメッセージブロック (SMB)、Internet Small Computer System Interface (iSCSI) などの業界標準プロトコルを通じてアクセスできます。さらに、このファイルシステムは圧縮と重複排除をサポートしているためストレージコストを削減できます。

このガイドでは Windows ワークロードのデプロイを重点的に取り上げます。例えば、FSx for ONTAP は数百の Windows ノードで構成される HPC のサードパーティー製ソリューションの共有ストレージとして使用できます。こうしたノードは書き込みおよび読み取りのスループット要件が非常に高く、グリッドスケジューラに接続されています。

次の図は、ハイブリッドクラウド環境でのエンタープライズ HPC ワークロードと FSx for ONTAP デプロイの一般的な例です。このアーキテクチャはこのガイド全体で参照します。



このアーキテクチャの特徴は次のとおりです。

1. オンプレミスのデータセンター環境とクラウド環境を、AWS Direct Connect を使用して接続します。
2. Windows を実行している HPC ワークロードは AWS クラウドにデプロイされます。
3. Active Directory はオンプレミスの環境にデプロイされます。
4. Windows で実行されているアクセスレイヤーシステムは、オンプレミスの環境にデプロイされます。

カスタマーアクセスレイヤー

エンドユーザーはカスタマーアクセスレイヤーを通じて AWS クラウドのワークロードにアクセスします。アプリケーションにアクセスしたり、SMB マウントを使用して Amazon FSx のデータにアクセスするには Amazon WorkSpaces または Citrix が一般的に使用されます。

アクティブディレクトリ

Microsoft Active Directory は通常、オンプレミスでインストールおよび管理されます。多くの組織では、ユーザー認証とアクセスコントロールをファイルレベルおよびフォルダレベルで提供するために、FSx for ONTAP SVM を Active Directory ドメインに結合しようと考えます。SMB クライアントは Active Directory 内の既存のユーザー ID を使用して自分自身を認証し、SVM のボリュームにアクセスできます。詳細については、「Working with Microsoft Active Directory in FSx for ONTAP」を参照してください。SVM が Active Directory ドメインに確実に到達できるようにするには、適切なネットワークルールを確立する必要があります。

Amazon FSx ファイルシステムがマネージドボリューム上でファイルを作成、編集、削除できるようにするためには、Active Directory ドメインのサービスアカウントを作成する必要があります。詳細については、「Delegating permissions to your Amazon FSx service account」を参照してください。Active Directory は多くのエンタープライズ組織の主要なコンポーネントであり、新しいアカウントのデプロイには、たとえ権限が制限されていても、かなり時間がかかる場合があります。

Amazon FSx リソース

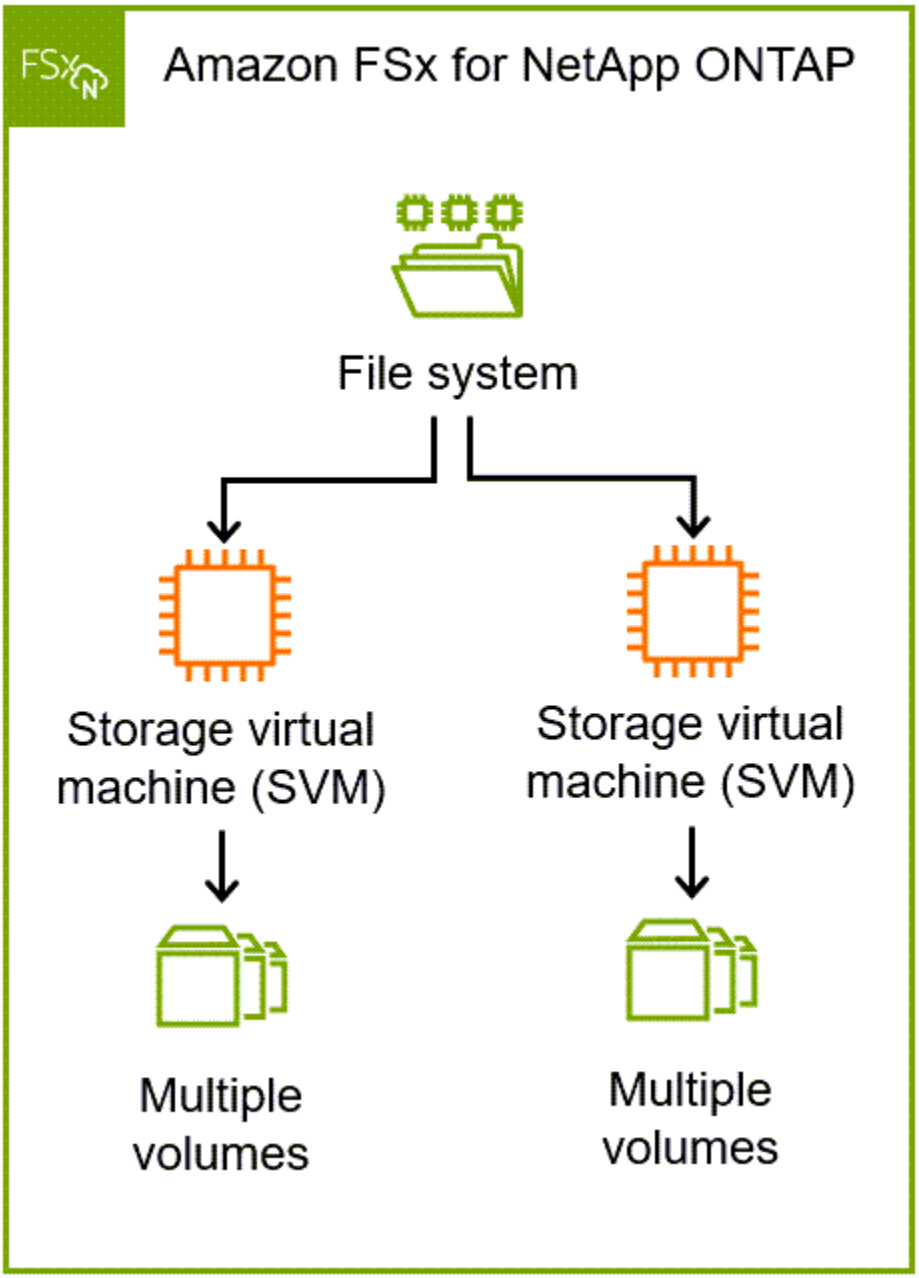
以下は FSx for ONTAP の主なリソースタイプです。

- ファイルシステムは FSx for ONTAP の主要なリソースで、オンプレミスの NetApp ONTAP クラスターに相当します。トラブルシューティングの際には NetApp CLI コマンドを使用して、ファ

イル共有エンドポイントと SSH 接続を確立できます。コマンドのトラブルシューティングの詳細は、このガイドの後半で説明します。

- ストレージ仮想マシン (SVM) は独自の管理およびデータアクセスエンドポイントを備えた分離された仮想ファイルサーバーです。FSx for ONTAP と Active Directory ドメインの統合の管理は、SVM レベルで行われます。したがって、Active Directory に関するエラーが発生した場合、SVM からトラブルシューティングを開始するとよいでしょう。
- ボリュームはデータの整理とグループ化に使用する仮想リソースです。ボリュームは論理コンテナであり、そこに格納されたデータはファイルシステムの物理容量を消費します。ボリュームは SVM でホストされます。ボリュームはそれぞれ異なる階層化ポリシーで設定できます。階層化ポリシーは、パフォーマンスを最適化した SSD レイヤーにデータを保存するか、コストを最適化したキャパシティレイヤーに保存するかを定義することで、パフォーマンスとコストを管理するのに役立つ強力なツールです。

次の図は、FSx for ONTAP ファイルシステムのリソース構造の説明です。すべてのコンポーネントを完全に管理する Amazon FSx。



ジャンクションパスを使用すると、複数のボリュームを単一の論理名前空間に結合できます (NetApp ドキュメント)。クライアントからは、ジャンクションは通常のディレクトリとして認識されます。ジャンクションパスは、複数のボリュームを使用する利点 (スナップショットや移行オプションのきめ細かな制御など) と、単一のアクセスポイントを介して複数のボリュームのデータにアクセスする利便性を提供します。

Amazon EC2 の Windows HPC クラスター

本ガイドでは、Amazon FSx を Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで構成された、重要な高スループット Windows HPC クラスターのストレージレイヤーとして扱います。Amazon EC2 で HPC クラスターをセットアップする場合のアプローチは複数あります。アプローチの例については、「Amazon EC2 ドキュメント」で Amazon EC2 での Windows HPC クラスターの設定に関するチュートリアルを参照してください。HPC クラスターコンピューティングノードはワーカーノードとも呼ばれ、SMB 共有を介して Amazon FSx ファイルシステムとやり取りします。SMB 共有はコンピューティングノードで自動または手動で作成できます。

AWS Secrets Manager

エンタープライズのアーキテクチャは通常、HashiCorp Terraform などの Infrastructure as Code (IaC) ツールを使用してデプロイされます。IaC スクリプトに機密情報を含めないようにすることがセキュリティのベストプラクティスです。Active Directory のサービスアカウントのパスワードなどの機密情報を保存するには通常、AWS Secrets Manager が使用されます。

Active Directory に結合された FSx for ONTAP ファイルシステムの作成

このセクションでは、エンタープライズ環境で Amazon FSx for NetApp ONTAP ファイルシステムを作成し、ストレージ仮想マシン (SVM) をオンプレミスデータセンターの Active Directory ドメインに結合するためのデプロイ手順について説明します。この章では、以下のプロセスの概要を説明します。

- Active Directory サービスアカウントをプロビジョニングする – ファイルシステムがマネージドボリュームのファイルを作成、編集、削除できるようにするために、Active Directory ドメインのサービスアカウントを作成します。
- FSx for ONTAP ファイルシステムをセットアップする – FSx for ONTAP のファイルシステム、SVM、ボリュームを設定します。
- FSx for ONTAP のモニタリング – FSx for ONTAP の使用状況とアクティビティのログ記録とモニタリングを構成します。

Active Directory サービスアカウントをプロビジョニングする

Amazon FSx for NetApp ONTAP SVM をオンプレミスの Active Directory ドメインに結合する場合は、Amazon FSx ファイルシステムが存続する間、有効な Active Directory サービスアカウントを維持する必要があります。Amazon FSx は、ファイルシステムをフルマネージし、障害が発生したファイル SVM の置き換えや NetApp ONTAP ソフトウェアへのパッチ適用など、Active Directory ドメインの結合解除と再結合を必要とするタスクを実行できる必要があります。サービスアカウントの認証情報を含む Active Directory の設定を Amazon FSx で定期的に更新してください。

このサービスアカウントには、Active Directory の次のアクセス許可が必要です。

- コンピュータをドメインに結合するアクセス許可
- ファイルシステムを結合している組織単位 (OU) では、次のアクセス許可が必要です。
  - パスワードのリセット
  - アカウントのデータの読み取りと書き込みを制限する
  - DNS ホスト名への書き込み
  - サービスプリンシパル名への書き込み
  - コンピュータオブジェクトを作成および削除する

- アカウントの読み取りおよび書き込み制限

Active Directory ドメイン管理者は Active Directory ユーザーとコンピュータの MMC スナップインを使用して、サービスアカウントを手動で作成できます。手順については、「FSx for ONTAP ドキュメント」で「Delegating permissions to your Amazon FSx service account」を参照してください。このアカウントはプログラムで設定することもできます。例えば、次の例に示すとおり、PowerShell を使用できます。

```
param(
    [string] $DomainName,
    [string] $Username, #Service Account username
    [string] $Firstname, #Service Account Firstname
    [string] $Lastname, #Service Account Lastname
    [string] $saOU, #OU where Service Account is created
    [string] $delegateOrganizationalUnit #OU where Service Account has delegation
)

#Retrieve Active Directory domain credentials of a Domain Admin
$DomainCredential = ...

#Import Active Directory PowerShell module
...

#Create Service Account in specified OU
New-Active DirectoryUser -Credential $DomainCredential -SamAccountName $Username -
UserPrincipalName "$Username@$DomainName" -Name "$Firstname $Lastname" -GivenName
 $Firstname -Surname $Lastname -Enabled $True -ChangePasswordAtLogon $False -
DisplayName "$Lastname, $Firstname" -Path $saOU -CannotChangePassword $True -
PasswordNotRequired $True
$user = Get-Active Directoryuser -Identity $Username
$userSID = [System.Security.Principal.SecurityIdentifier] $user.SID

#Connect to Active Directory drive
Set-Location Active Directory:

$ACL = Get-Acl -Path $delegateOrganizationalUnit
$Identity = [System.Security.Principal.IdentityReference] $userSID

#GUID of Active Directory Class
$Computers = [GUID]"bf967a86-0de6-11d0-a285-00aa003049e2"
$ResetPassword = [GUID]"00299570-246d-11d0-a768-00aa006e0529"
$ValidatedDNSHostName = [GUID]"72e39547-7b18-11d1-adef-00c04fd8d5cd"
```

```
$ValidatedSPN = [GUID]"f3a64788-5306-11d1-a9c5-0000f80367c1"
$AccountRestrictions = [GUID]"4c164200-20c0-11d0-a768-00aa006e0529"

#Delegation list
$rules = @()
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($Identity,
 "CreateChild, DeleteChild", "Allow", $Computers, "All"))
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($Identity,
 "ExtendedRight", "Allow", $ResetPassword, "Descendents", $Computers))
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($Identity,
 "ReadProperty, WriteProperty", "Allow", $AccountRestrictions, "Descendents",
 $Computers))
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($userSID,
 "Self", "Allow", $ValidatedDNSHostName, "Descendents", $Computers))
$rules += $(New-Object System.DirectoryServices.ActiveDirectoryAccessRule($userSID,
 "Self", "Allow", $ValidatedSPN, "Descendents", $Computers))

#Set delegation
foreach($rule in $rules) {
    $ACL.AddAccessRule($rule)
}
Set-Acl -Path $delegateOrganizationalUnit -AclObject $ACL
```

FSx for ONTAP ファイルシステムをセットアップする

Amazon FSx for NetApp ONTAP ドキュメントには、AWS マネジメントコンソールのクイック作成オプションまたは標準作成オプションを使用してファイル共有を設定する手順が記載されています。このガイドでは、HPC ワークロードと Active Directory 統合をサポートする必要がある企業向けに、追加の推奨事項とガイダンスを紹介します。

AWS マネジメントコンソールで FSx for ONTAP ファイルシステムを作成する手順については、「Creating FSx for ONTAP file systems」を参照してください。各セクションに記載された、エンタープライズ環境でのセットアップに関する以下の推奨事項と考慮事項に注意してください。

ファイルシステムの詳細セクション

1. [デプロイタイプ] で以下のいずれかを選択します。
   - 本番ワークロードには [マルチ AZ] を選択します。このオプションは、アベイラビリティーゾーンにアクセスできなくなった場合にデータの可用性を維持するのに役立ちます。

- ディザスタリカバリの目的の場合、非本番環境のワークロードの場合、またはアプリケーションレイヤーにレプリケーションが組み込み済みのためストレージレベルで追加の冗長性が必要ないワークロードの場合、シングル AZ を使用します。これは、こうしたタイプのワークロードに対して費用対効果の高いオプションです。

デプロイタイプの設定に関する詳細と推奨事項については、このガイドの「ベストプラクティス」セクションで「アベイラビリティーゾーンのデプロイオプションを選択する上でのベストプラクティス」を参照してください。

2. [プロビジョンド SSD IOPS] で、以下のいずれかを選択します。
   - Amazon FSx で SSD ストレージ GiB あたり 3 IOPS を自動的にプロビジョニングする場合は、[自動] を選択します。ファイルシステムあたり最大 160,000 SSD IOPS です。
   - IOPS の数を指定する場合は、[ユーザープロビジョンド] モードを選択します。より高いレベルの IOPS でプロビジョニングする場合は、その月のインクルードレートを上回ってプロビジョニングされた平均 IOPS に対して支払います。これは、IOPS 月単位で測定されます。

   詳細については、「FSx for ONTAP ドキュメント」の「Storage capacity and IOPS」、「Considerations when updating storage and IOPS」、「Impact of storage capacity on performance」を参照してください。

デフォルトのストレージ仮想マシン設定セクション

1. [ルートボリュームのセキュリティスタイル] で、以下のいずれかを選択します。
   - 主に Linux ベースのクライアント (NFS プロトコル) からファイルシステムにアクセスする場合は [Unix] を選択します。
   - 主に Windows ベースのクライアント (SMB プロトコル) からファイルシステムにアクセスする場合は、[NTFS] を選択します。
   - Linux ベースと Windows ベースのクライアントからファイルシステムに均等にアクセスする場合は、[混在] を選択します。これは高度な設定です。

   詳細については、「NetApp ドキュメンテーション」の「What the security styles and their effects are」を参照してください。

2. [Active Directory] で、[Active Directory への参加] を選択します。
3. [NetBIOS 名] には、SVM 用に作成される Active Directory コンピュータオブジェクトの NetBIOS 名を入力します。通常は SVM 名と同じですが、異なる場合があります。NetBIOS 名は 15 文字を超えてはいけません。

4. [Active Directory ドメイン名] には Active Directory の完全修飾ドメイン名 (FQDN) を入力します。ドメイン名は 255 文字を超えてはいけません。
5. [DNS サーバーの IP アドレス] にはドメインの DNS サーバーの IPv4 アドレスを入力します。IP アドレスを 3 つまで入力できます。
6. [サービスアカウントのユーザー名] と [サービスアカウントのパスワード] には、既存の Active Directory のサービスアカウントのユーザー名とパスワードを入力します。これは、このガイドの「Active Directory サービスアカウントをプロビジョニングする」で設定したサービスアカウントです。
7. [組織単位 (OU)] には、ファイルシステムに結合させる組織単位の識別パス名を入力します。
8. [委任されたファイルシステム管理者グループ] には、ファイルシステムを管理できる Active Directory 内のグループ名を入力します デフォルトのグループは `Domain Admins` です。

デフォルトのボリューム設定セクション

1. [ボリューム名] には、データボリュームの名前を入力します。名前は 203 文字以下とし、英数字とアンダースコア (_) を使用できます。
2. [ジャンクションパス] には、ボリュームをマウントするファイルシステム内の場所を入力します。名前の先頭には `/vol1` のようにスラッシュが入らなければなりません。詳細については、このガイドの「Amazon FSx リソース」セクションを参照してください。
3. [ボリュームサイズ] には、ボリュームのストレージ容量をメビバイト (MiB) で入力します。20 ~ 104857600 (100 TiB) の範囲の任意の整数を入力します。
4. [ストレージ効率] では、ストレージ効率機能 (重複排除、圧縮、コンパクト化) を有効にするかどうかを選択します。詳細については、「FSx for ONTAP ドキュメンテーション」で「Storage efficiency」を参照してください。これらの効率機能がご使用の HPC ワークロードと互換性がある場合は、エンタープライズ環境で使用することをお勧めします。
5. [容量プールの階層化ポリシー] では、ボリュームの新しい階層化ポリシーを選択します。階層化ポリシーの詳細と推奨事項については、このガイドの「ベストプラクティス」セクションで「ストレージ階層と階層化ポリシーにおけるベストプラクティス」を参照してください。

FSx for ONTAP のモニタリング

Amazon FSx for NetApp ONTAP の使用状況とアクティビティのログ記録とモニタリングは、ファイルシステムの状態を理解するのに役立つことから、ベストプラクティスとなっています。ログデータを使用して、システムの信頼性、運用、効率に影響する問題をトラブルシューティングできます。こ

れはエンタープライズ環境では特に重要です。ファイルシステムに問題が起きると、処理タスクの結果が損なわれたり、不正確な結果が出たり、サービスレベルアグリーメントに違反したりする可能性があるためです。これにより HPC ワークロードの所有者が罰金を科されたり、誤ったデータに基づいて意思決定が行われたりする可能性があります。エンタープライズ環境のモニタリングのベストプラクティスについては、このガイドの「FSx for ONTAP ファイルシステムのモニタリングのベストプラクティス」を参照してください。

FSx for ONTAP の使用状況とアクティビティのログ記録とモニタリングには、AWS およびサードパーティー製のさまざまなツールとサービスを使用できます。例えば、Amazon CloudWatch、ONTAP のイベント管理システム (EMS)、NetApp の Cloud Insights サービス、NetApp Harvest、NetApp Grafana、AWS CloudTrail を使用できます。詳細については、「Amazon FSx for NetApp ONTAP のモニタリング」を参照してください。

FSx for ONTAP をエンタープライズ環境にデプロイする場合のベストプラクティス

このセクションでは、Amazon FSx for NetApp ONTAP をエンタープライズ環境にデプロイして運用する場合のベストプラクティスと考慮事項を説明します。これらの推奨事項は AWS プロフェッショナルサービスのエクスペリエンスに基づいています。

このガイドの推奨事項に加え、以下のベストプラクティスに従ってください。

- Active Directory を使用する際のベストプラクティス (FSx for ONTAP ドキュメント)
- データ保護 (FSx for ONTAP ドキュメント)
- IAM でのセキュリティのベストプラクティス (AWS Identity and Access Management (IAM) ドキュメント)
- NetApp ONTAP FlexGroup ボリュームのベストプラクティスおよび実装ガイド (NetApp ドキュメント)

ストレージ階層と階層化ポリシーにおけるベストプラクティス

ストレージ階層は、Amazon FSx for NetApp ONTAP ファイルシステムの物理的なストレージメディアです。次のストレージ階層があります。

- SSD 階層はアクティブなデータ用に設計された高性能ソリッドステートドライブ (SSD) ストレージで、この階層のストレージサイズはユーザーが選択します。
- 容量プール階層は、非常に柔軟な伸縮性のあるストレージ階層で、アクセス頻度の低いデータのコストを最適化できます。SSD 階層は容量プール階層よりも大幅に高速です。FSx for ONTAP の SSD ストレージではファイル運用のレイテンシーがミリ秒未満、容量プール階層では数十ミリ秒です。

これらの階層の詳細については、「FSx for ONTAP のストレージ階層」を参照してください。

ボリュームレベルで構成する階層化ポリシーは、SSD 階層に保存されているデータを容量プール階層に移行するかどうか、いつ移行するかを決定します。FSx for ONTAP には 4 つの異なる階層化ポリシー (スナップショットのみ、自動、すべて、なし) が用意されています。各ポリシーの詳細については、「FSx for ONTAP ドキュメント」で階層化ポリシーを参照してください。

ファイル共有のボリュームに階層化ポリシーを設定する場合は、次の推奨事項を考慮してください。

- HPC ワークロードは SSD 階層のデータにアクセスするようにし、パフォーマンスのボトルネックとなるのを防止します。HPC ワークロードがアクセスするボリュームは、階層化ポリシーをなしまたはスナップショットのみに設定することをお勧めします。
- ファイル共有にデータを移行する場合は、ターゲットのボリューム階層化ポリシーをすべてに設定することをお勧めします。これにより、すべてのデータが SSD 階層に移行され、その後すぐに容量プール階層に移動されるため、コストを削減できます。さらに、SSD 階層の容量の使用率が 98% 以上になると、その階層への書き込みは停止します。階層化ポリシーをすべてに設定すると、移行中にこの階層化のしきい値に到達するのを防ぐことができます。移行が完了した後で、階層化ポリシーを変更してパフォーマンスとコストのバランスを取ることができます。詳細については、「Migrating file shares to Amazon FSx for NetApp ONTAP using AWS DataSync」(AWS ブログポスト) を参照してください。

NetApp ONTAP の最大ディレクトリサイズを使用する際のベストプラクティス

maxdirsize (NetApp ドキュメント) は、各ディレクトリに保存できるファイルの最大数を決定する NetApp ONTAP 設定です。この設定はボリュームに適用されるため、ボリューム内のすべてのディレクトリの `maxdirsize` 設定は同じになります。デフォルト値は 320 MB で、ディレクトリごとに最大 430 万個のファイルを保存できます。

`maxdirsize` の値を増やすことで、より大きなディレクトリをサポートできます。値を増やすと、減らすことはできません。減らすにはディレクトリを再作成する必要があります。ディレクトリはメモリにロードされるため、ディレクトリのサイズとファイルシステムのパフォーマンスはトレードオフの関係にあります。カスタム設定を検証するにはテストが必要です。NetApp ではこの値をデフォルトのままにしておくことが推奨されています。詳細については、「NetApp ONTAP FlexGroup ボリュームのベストプラクティスおよび実装ガイド」(NetApp ドキュメント) を参照してください。

`maxdirsize` 設定をカスタマイズする場合、次の式を使用して、1 つのフォルダに収まるファイルの数を判定できます。

```
max number of files in each directory = maxdirsize in MB × 53 × 0,25
```

FSx for ONTAP ファイルシステムのモニタリングのベストプラクティス

他の AWS のサービスと同様に、FSx for ONTAP は Amazon CloudWatch と統合されています。CloudWatch を使用すると AWS リソースのメトリクスをほぼリアルタイムでモニタリングできます。メトリクスはファイルシステムレベルとボリュームレベルで利用でき、詳細なモニタリングメトリクスによってリソースのよりきめ細かいレポート情報を取得して分析できます。詳細については、「FSx for ONTAP ドキュメント」の「Monitoring with Amazon CloudWatch」を参照してください。CloudWatch で FSx for ONTAP をモニタリングする場合は、次の推奨事項を考慮してください。

- `StorageUsed` ファイルシステムメトリクスを使用して、ストレージ階層でモニタリング結果をフィルタリングすることをお勧めします。
- `StorageCapacity` ファイルシステムメトリクスを使用して、SSD 階層容量の使用率が 80% 以上となった場合に通知する CloudWatch アラームを設定します。これにより、ボリュームの階層化が適切に機能し、新しいデータの容量を確実に維持できます。詳細については、「Tiering thresholds」を参照してください。

アベイラビリティーゾーンのデプロイオプションを選択する上でのベストプラクティス

Amazon FSx for NetApp ONTAP は、単一 AZ またはマルチ AZ の設定でデプロイできます。各オプションは可用性と耐久性のレベルが異なります。これらのデプロイオプションの詳細については、「FSx for ONTAP ドキュメント」の「Availability and durability」を参照してください。

マルチ AZ では、FSx for ONTAP ファイルシステムがアクティブ/パッシブ設定でデプロイされます。したがって、ファイル共有に接続するサーバーはすべて、プライマリアベイラビリティーゾーンのエンドポイントのみを使用します。セカンダリアベイラビリティーゾーンのエンドポイントはフェイルオーバー専用であり、プライマリアベイラビリティーゾーンで障害が発生しない限り、読み取りまたは書き込みには使用されません。

FSx for ONTAP ファイルシステムを作成した後で、アベイラビリティーゾーンのデプロイオプションを変更することはできません。アベイラビリティーゾーンの設定を変更するには、新しいファイルシステムを作成し、データを新しいファイルシステムに移行する必要があります。

ただし、単一 AZ オプションを使用してファイル共有をデプロイした場合でも、他のアベイラビリティーゾーンからアクセスできます。セキュリティグループやネットワークアクセスコントロール

リスト (ネットワーク ACL) といったネットワーク設定は、クライアントがファイルシステムのエンドポイントに接続できるようにしておく必要があります。このアプローチを使用すると、クロス AZ トラフィックの各方向 (読み取りと書き込み) で料金が発生します。詳細については、「Amazon FSx for NetApp ONTAP」を参照してください。

デプロイオプションを選択する際は、マルチ AZ 設定の耐障害性と単一 AZ 設定のパフォーマンスのどちらかを選択する必要があります。ユースケースでの実用に適している場合は、マルチ AZ オプションの高可用性を選択することをお勧めします。ただし、単一 AZ オプションのほうがコスト効率が高く、レイテンシーを短縮できる可能性があります。HPC ワークロードと、レイテンシーの増加を許容できるかどうかで検討してください。

よくある質問

FSx for ONTAP ボリュームのシンプロビジョニングとはどのような意味ですか?

シンプロビジョニングとは一般に、仮想化テクノロジーを使用することで、システムが実際にプロビジョニングされているより多くのリソースを利用できるように見せることを意味します。銀行のキャッシュリザーブのようなもので、銀行に物理的に保管されている金額は銀行口座の合計金額よりも少なくなります。Amazon FSx for NetApp ONTAP でボリュームを作成すると、ストレージは事前に予約されません。しかし、データを追加するにつれてサイズが徐々に増加します。詳細については、「FSx for ONTAP storage tiers」を参照してください。

FSx for ONTAP でサポートされているプロトコルは何ですか?

FSx for ONTAP ファイルシステムにアクセスできるプロトコルは、Network File System (NFS)、Server Message Block (SMB)、Internet Small Computer System Interface (iSCSI) です。詳細については、「FSx for ONTAP ドキュメント」の「Accessing data」を参照してください。

FSx for ONTAP を Windows 環境で使用しています。Active Directory との統合を有効にする前提条件はありますか?

はい。Active Directory ドメインでサービスアカウントを作成する必要があります。詳細については、このガイドの「Active Directory サービスアカウントをプロビジョニングする」を参照してください。適切なネットワーク接続を確保する必要もあります。ファイルシステムを設定するときは、参加する組織単位 (OU) を必ず指定してください。詳細については、「FSx for ONTAP ドキュメント」の「Prerequisites for joining an SVM to a self-managed Microsoft AD」を参照してください。

ボリューム階層化ポリシーは変更できますか?

はい。階層化ポリシーはいつでも変更できます。詳細については、「Amazon FSx ドキュメント」の「Setting a volume's tiering policy」を参照してください。

ファイルシステムの階層化ポリシーと書き込みオペレーションが機能せず、メトリクスに SSD ストレージ階層の使用率が 98% 超と表示されます。どうすればよいですか?

SSD ストレージ階層の使用率が 98% 以上になると、すべての階層化機能と書き込みオペレーションが停止します。詳細については、「Amazon FSx ドキュメント」で「Tiering thresholds」を参照してください。オペレーションを再開するには、SSD ストレージ容量を増やしてください。SSD 階層に保持するデータが少なくなるように、階層化ポリシーを変更することを検討してください。詳細については、「Amazon FSx ドキュメント」の「Managing volume storage capacity」および「Setting a volume's tiering policy」を参照してください。

マルチ AZ 配置で、アクティブ/アクティブ設定はサポートされていますか?

いいえ。マルチ AZ 配置でサポートされているのはアクティブ/パッシブ設定です。詳細については、このガイドの「アベイラビリティーゾーンのデプロイオプションを選択する上でのベストプラクティス」を参照してください。

FSx for ONTAP のシングル AZ 配置とマルチ AZ 配置の料金は同額ですか?

いいえ。マルチ AZ 設定の料金はシングル AZ 設定の約 2 倍です。シングル AZ 配置では、クロス AZ トラフィックに関する変更があります。詳細については、「Amazon FSx for NetApp ONTAP」を参照してください。

リソース

Amazon FSx for NetApp ONTAP ドキュメント

- ストレージ階層
- サポートされているクライアント
- ボリュームの管理
- SMB 共有の管理
- FSx for ONTAP SVM をアクティブディレクトリドメインに結合させるためのベストプラクティス
- Volume data tiering and thresholds
- File system metrics for Amazon CloudWatch monitoring
- TieringPolicy (API リファレンス)

その他の AWS リソース

- AWS ストレージサービスの選択
- Amazon FSx for NetApp ONTAP の料金
- Migrating file shares to Amazon FSx for NetApp ONTAP using AWS DataSync (AWS ブログ記事)

NetApp のリソース

- NetApp ONTAP FlexGroup volumes: Best practices and implementation guide (NetApp PDF)
- ジャンクションパスとは何ですか (NetApp ナレッジベース)
- maxdirsize とは何ですか (NetApp ナレッジベース)

ドキュメント履歴

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

変更	説明	日付
初版発行	—	2023 年 8 月 29 日

AWS 規範的ガイダンスの用語集

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

数字

7 Rs

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

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

A

ABAC

「属性ベースのアクセス制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

アクティブ - アクティブ移行

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

アクティブ - パッシブ移行

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

集計関数

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

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

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

アンチパターン

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

アプリケーション制御

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン

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

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドに正常に移行するための効率的で効果的な計画を立てるのを支援する AWS からのガイドラインとベストプラクティスのフレームワーク。AWSCAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用の観点と呼ばれる 6 つの重点を置く分野にガイダンスを編成しています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、AWS CAF は、クラウドの導入を成功させるための組織の準備を支援するために、人材開発、トレーニング、コミュニケーションに関するガイダンスを提供します。詳細については、AWS CAF ウェブサイト と AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード資格フレームワーク (AWS WQF)

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

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

動作グラフ

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

二項分類

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

ブルームフィルター

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

ブルー/グリーンデプロイ

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

ボット

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

ボットネット

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

ブランチ

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

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

ブレークグラスアクセス

例外的な状況で、承認済みプロセスを経て、通常は AWS アカウント へのアクセス許可がないユーザーを迅速にそのアカウントにアクセスさせるための手段。詳細については、 AWS Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータを参照してください。

ブラウンフィールド戦略

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

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

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

ビジネス継続性計画 (BCP)

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

C

CAF

「AWS クラウド導入フレームワーク」を参照してください

カナリアデプロイ

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

CCoE

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

CDC

「変更データキャプチャ」を参照してください。

変更データキャプチャ (CDC)

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

カオスエンジニアリング

障害や破壊的なイベントを意図的に導入して、システムの耐障害性をテストすること。AWS Fault Injection Service (AWS FIS) を使用すると、AWS ワークロードに負荷をかける実験を行い、それへの反応を評価できます。

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

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

クライアント側の暗号化

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

Cloud Center of Excellence (CCoE)

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

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

組織が、AWS クラウド への移行時に通常実行する 4 つの段階。

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

これらのステージは、Stephen Orban が AWS クラウド エンタープライズ戦略ブログの「The Journey Toward Cloud-First & the Stages of Adoption」という記事で定義したものです。これらが、AWS 移行戦略とどのような関係があるかについては、移行準備ガイドを参照してください。

CMDB

「構成管理データベース (CMDB)」を参照してください。

コードリポジトリ

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

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

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

設定ドリフト

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

構成管理データベース (CMDB)

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

コンフォーマンスパック

組み合わせることでコンプライアンスチェックとセキュリティチェックをカスタマイズできる、AWS Config ルールと修復アクションのコレクション。コンフォーマンスパックは、1 つのエンティティとして AWS アカウント とリージョンに、または YAML テンプレートを使用して組織全体にデプロイできます。詳細については、AWS Config ドキュメントのコンフォーマンスパックを参照してください。

継続的インテグレーションと継続的デリバリー (CI/CD)

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

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一要素です。詳細については、データ分類を参照してください。

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

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

データ最小化

厳密に必要なデータのみを収集し、処理するという原則。AWS クラウド でデータ最小化を実践することで、プライバシーリスク、コスト、分析の二酸化炭素排出量を削減することができます。

データ境界

AWS 環境における一連の予防的ガードレール。これによって、想定されたネットワークをアクセス元とする信頼できる ID のみ、信頼できるリソースにアクセスできるようにします。詳細については、「Building a data perimeter on AWS」を参照してください。

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

ディープラーニング

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

多層防御

一連のセキュリティメカニズムとコントロールをコンピュータネットワーク全体に層状に重ねて、ネットワークとその内部にあるデータの機密性、整合性、可用性を保護する情報セキュリティの手法。この戦略を AWS に採用すると、AWS Organizations 構造内の各層に複数のコントロールが追加され、リソースの安全を維持できます。たとえば、多層防御アプローチでは、多要素認証、ネットワークセグメンテーション、暗号化を組み合わせることができます。

委任管理者

AWS Organizations では、互換性のあるサービスは AWS メンバーアカウントを登録することで、組織のアカウントやそのサービスのアクセス許可を管理できるようになります。このアカウントを、そのサービスの委任管理者と呼びます。詳細、および互換性のあるサービスの一覧は、AWS Organizations ドキュメントのAWS Organizations で使用できるサービスを参照してください。

デプロイ

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

開発環境

「環境」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

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

ディザスタ

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

ディザスタリカバリ (DR)

ディザスタによるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。詳細については、AWS 上のワークロードのディザスタリカバリを参照のこと：AWS Well-Architected Frameworkのクラウドにおける復旧を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

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

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

ベースライン設定からの偏差を追跡します。例えば、AWS CloudFormation を使用してシステムリソースの偏差を検出したり、AWS Control Tower を使用して、ガバナンス要件への準拠に影響しかねないランディングゾーンの変更を検出したりできます。

DVSM

「開発バリューストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

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

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

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

障害分離境界

AWS クラウド クラウドにおける、可用性ゾーン、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は、障害の影響を狭め、ワークロードの耐障害性を向上させるのに有用です。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 Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「AWS を使用した機械学習モデルの解釈」を参照してください。

機能変換

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

数ショットプロンプト

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

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

FGAC

「きめ細かなアクセス制御」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

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

G

生成 AI

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

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

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

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

Gitflow ワークフロー

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

ゴールデンイメージ

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

グリーンフィールド戦略

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

ガードレール

組織単位 (OU) 全般のリソース、ポリシー、コンプライアンスを管理するのに役立つ概略的なルール。予防ガードレールは、コンプライアンス基準に一致するようにポリシーを実施します。これらは、サービスコントロールポリシーと IAM アクセス許可の境界を使用して実装されます。検出ガードレールは、ポリシー違反やコンプライアンス上の問題を検出し、修復のためのアラートを発信します。これらは、AWS Config、AWS Security Hub CSPM、Amazon GuardDuty、AWS Trusted Advisor、Amazon Inspector、カスタムの 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、オペレーショントテクノロジー (OT) システムをモダナイズし、アップグレードするためのアプローチ。ヒストリアンは、工場内のさまざまなソースからデータを収集して保存するために使用されるデータベースの一種です。

ホールドアウトデータ

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

同種データベースの移行

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

ホットデータ

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

ホットフィックス

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

ハイパーケア期間

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

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「インダストリアル IoT」を参照してください。

イミュータブルインフラストラクチャ

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

インバウンド (受信) VPC

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

増分移行

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

インダストリー 4.0

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

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

産業分野における IoT (IIoT)

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

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「IoT」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

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

大規模言語モデル (LLM)

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

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースアクセス制御」を参照してください。

最小特権

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

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「ブランチ」を参照してください。

マルウェア

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

マネージドサービス

AWS のサービス は AWS 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運用し、ユーザーは、そのエンドポイントにアクセスして、データの保存や取得を行います。マネージドサービスの例として、Amazon Simple Storage Service (Amazon S3) と Amazon DynamoDB が挙げられます。このサービスは、抽象化されたサービスとも呼ばれます。

製造実行システム (MES)

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

MAP

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

メカニズム

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

メンバーアカウント

AWS Organizations の組織に含まれる管理アカウント以外の、すべての AWS アカウント。アカウントが組織のメンバーになることができるのは、一度に 1 つのみです。

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

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

マイクロサービス

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

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

「機械学習」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

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

モノリシックアプリケーション (モノリス)

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

MPA

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

MQTT

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

多クラス分類

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

ミュータブルなインフラストラクチャ

本番ワークロードに使用する既存のインフラストラクチャを更新および変更するためのモデル。これよりも一貫性、信頼性、予測可能性に優れているため、Well-Architected AWS フレームワークでは、イミュータブルインフラストラクチャの使用をベストプラクティスとして推奨しています。

O

OAC

「オリジンアクセス制御」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

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

OI

「オペレーション統合」を参照してください。

Ola

「オペレーショナルレベルアグリーメント」を参照してください。

オンライン移行

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

OPC-UA

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

Open Process Communications - Unified Architecture (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

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

運用テクノロジー (OT)

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

オペレーション統合 (OI)

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

組織の証跡

AWS Organizations 内の一組織の、すべての AWS アカウント のイベントをすべてログ記録している AWS CloudTrail が作成した証跡。証跡は、組織に含まれている各 AWS アカウント に作成され、各アカウントのアクティビティを追跡します。詳細については、CloudTrail ドキュメントの組織の証跡の作成を参照してください。

組織変更管理 (OCM)

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

オリジンアクセスコントロール (OAC)

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

オリジンアクセスアイデンティティ (OAI)

CloudFront の、Amazon S3 コンテンツを保護するためのアクセス制限オプション。OAI を使用すると、CloudFront が、Amazon S3 に認証可能なプリンシパルを作成します。認証されたプリンシパルは、S3 バケット内のコンテンツに、特定の CloudFront ディストリビューションを介し

てのみアクセスできます。OACも併せて参照してください。OAC では、より詳細な、強化されたアクセスコントロールが可能です。

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

「個人を特定できる情報」を参照してください。

プレイブック

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

PLC

「プログラマブルロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

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

多言語の永続性

データアクセスパターンやその他の要件に基づいて、マイクロサービスのデータストレージテクノロジーを個別に選択します。マイクロサービスが同じデータストレージテクノロジーを使用している場合、実装上の問題が発生したり、パフォーマンスが低下する可能性があります。マイクロサービスは、要件に最も適合したデータストアを使用すると、より簡単に実装でき、パフォーマンスとスケーラビリティが向上します。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 `false` を返すためのクエリ条件。一般的に、`WHERE` 句に記述されます。

述語プッシュダウン

データベースクエリを最適化する手法。これによって、転送前にクエリ内のデータをフィルタリングします。この手法を取ると、リレーショナルデータベースから取得し処理する必要のあるデータの量が減少するため、クエリのパフォーマンスが向上します。

予防的コントロール

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

プリンシパル

アクションを実行してリソースにアクセスできる AWS 内のエンティティです。このエンティティは、通常は AWS アカウント のルートユーザー、IAM ロール、ユーザーのいずれかになりま

す。詳細については、IAM ドキュメントの「ロールに関する用語と概念」にあるプリンシパルを参照してください。

プライバシーバイデザイン

開発プロセス全体を通してプライバシーが考慮されているシステムエンジニアリングのアプローチ。

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

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

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

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

プロンプトチェイニング

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

仮名化

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

発行/サブスクライブ (pub/sub)

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

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

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

RAG

「検索拡張生成」を参照してください。

ランサムウェア

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

RASCI マトリックス

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

RCAC

「行と列のアクセス制御」を参照してください。

リードレプリカ

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

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

地理的な領域内の AWS リソースのコレクション。各 AWS リージョン は、耐障害性、安定性、レジリエンスを実現するために他のリージョンと分離され、独立しています。詳細については、「アカウントが使用できる AWS リージョン を指定する」を参照してください。

回帰

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

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

プラットフォーム変更

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

中断に抵抗または中断から回復するアプリケーションの機能。AWS クラウド での回復力を計画する際には、一般的に、高可用性とディザスタリカバリが考慮されます。詳細については、「AWS クラウド の耐障害性」を参照してください。

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンシブコントロール

有害事象やセキュリティベースラインからの逸脱について、修復を促すように設計されたセキュリティコントロール。詳細については、「AWS でのセキュリティコントロールの実装」の「レスポンシブコントロール」を参照してください。

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

取得拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナ

レッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」を参照してください。

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能ではフェデレーティッドシングルサインオン (SSO) が有効になるため、組織内の全員に IAM のユーザーを作成しなくても、ユーザーが AWS マネジメントコンソール にログインしたり AWS API オペレーションを呼び出したりできます。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントのSAML 2.0 ベースのフェデレーションについてを参照してください。

SCADA

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

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

セキュリティバイデザイン

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

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントへの自動レスポンスまたは自動修復を目的として、事前定義およびプログラムされたアクション。こうした自動化は、検出またはレスポンシブのセキュリティコントロールとして機能し、AWS セキュリティのベストプラクティス実装に役立ちます。自動レスポンスアクションの例には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

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

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

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

責任共有モデル

ユーザーが、クラウドセキュリティとコンプライアンスに関する責任を AWS と共有するモデル。AWS はクラウド自体のセキュリティに対して責任を負い、ユーザーはクラウド内のセキュリティに対して責任を負います。詳細については、責任共有モデルを参照してください。

SIEM

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

単一障害点 (SPOF)

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

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

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

SPOF

「単一障害点」を参照してください。

スタースキーマ

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

strangler fig パターン

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

サブネット

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

監視制御とデータ取得 (SCADA)

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

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

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

システムプロンプト

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

T

tags

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

ターゲット変数

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

タスクリスト

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

テスト環境

「環境」を参照してください。

トレーニング

お客様の機械学習モデルに学習するデータを提供すること。トレーニングデータには正しい答えが含まれている必要があります。学習アルゴリズムは入力データ属性をターゲット (お客様が予測したい答え) にマッピングするトレーニングデータのパターンを検出します。これらのパター

ンをキャプチャする機械学習モデルを出力します。そして、お客様が機械学習モデルを使用して、ターゲットがわからない新しいデータでターゲットを予測できます。

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

AWS Organizations の組織およびそのアカウントで、ユーザーに代わって指定したサービスにタスクを実行させるためにアクセス許可を付与すること。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、AWS Organizations ドキュメントのAWS Organizations を他の AWS サービスと併用するを参照してください。

チューニング

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

ツーピザチーム

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

U

不確実性

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

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

現在のレコードに何らかの形で関連している行のグループに計算を実行する SQL 関数。ウィンドウ関数は、移動平均を計算したり、現在の行の相対位置に基づいて他の行の値にアクセスするといったタスクの処理に役立ちます。

ワークロード

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

ワークストリーム

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

WORM

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

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

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

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

ゼロショットプロンプト

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

ゾンビアプリケーション

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