VMware Cloud on の ID とアクセスの管理 AWS

AWS 規範ガイダンス

AWS 規範ガイダンス: VMware Cloud on の ID とアクセスの管理 AWS

Table of Contents

VMware Cloud on の ID とアクセスの管理 AWS

Richard Milner-Watts、Abdenour Kansab、および Chris Porter、Amazon Web Services

Vern Bolinius (VMware)

2024 年 9 月 (ドキュメント履歴)

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

ID およびアクセス管理は、システムへのアクセスを、許可されたユーザーとアプリケーションのみに制限するという原則です。これには、必要なネットワークリソースのみにアクセスを制限することも含まれます。クラウド環境では、ID 管理とアクセス管理は通常、ユーザー、ユーザーグループ、アプリケーションの識別、認証、認可に使用するポリシーとサービスで構成されています。

VMware Cloud on は、 で VMware vSphere ベースのワークロード AWS をサポートします AWS クラウド。このクラウドインフラストラクチャを設定、管理、バックアップ、監視、分析するために、多くの VMware サービスおよびツールを使用できます。ID とアクセスの管理に使用する機能と制御は、サービス間で異なります。このドキュメントでは、次の VMware サービスの ID とアクセスを管理するためのベストプラクティスとレコメンデーションについて説明します。

- VMware Aria Operations
- VMware Aria Operations for Logs
- VMware Aria Operations for Networks
- VMware Cloud on AWS
- VMware Cloud Services Console
- VMware HCX
- VMware NSX
- VMware Live Cyber Recovery
- VMware Live Site Recovery
- VMware vCenter Server

このガイドでは、VMware Cloud on および関連する VMware VMware サービスのアイデンティティとアクセス管理の概要 AWS とベストプラクティスについて説明します。各サービスの簡単な説明と、そのサービスの ID アクセスと管理に関する考慮事項についても説明します。また、VMware Cloud on の一部としてサービスを設定するための推奨事項も提供します AWS。

> **Important**
>
> このガイドで説明する VMware サービスの多くは、他のクラウドやオンプレミスの VMware ソリューションでも使用されています。このガイドに記載する推奨事項とベストプラクティスは、VMware Cloud on AWS専用です。これらの推奨事項は、他の環境では適用されない場合があります。

対象者

このガイドは、VMware Cloud on をクラウド環境またはハイブリッド環境に実装する責任を負うアーキテクトとセキュリティエンジニアを対象とし AWS ています。

ターゲットを絞ったビジネス成果

このガイドは以下を行う際に役立ちます。

1. VMware Cloud on および関連する VMware サービスのさまざまな ID AWS およびアクセス管理コントロールを理解する
2. VMware Cloud on を安全に運用するための推奨ベストプラクティスに精通する AWS
3. 外部 ID プロバイダーによるフェデレーション認証で利用できるオプションを理解する

ID 管理の概要

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware では、ID、認証、認可の管理に、次の業界標準のコンセプトと ID の階層を使用しています。

- ユーザーとは、何らかの役割で特定の環境にアクセスする個人のことです。ローカルユーザーを作成したり、フェデレーションを使用して外部 ID プロバイダーのユーザーを認証したりできます。詳細については、「ID フェデレーションと SSO」を参照してください。
- グループは、ユーザーの集合を論理的にグループ化するメカニズムを提供します。これにより、それらのユーザーに一貫性のあるアクセス許可を提供でき、管理オーバーヘッドを軽減できます。ロールは、ユーザーまたはグループにアクセス許可を付与するために使用されます。詳細については、「Roles and Permissions in the SDDC」(VMware ドキュメント) を参照してください。
- VMware クラウドの組織は、1 つまたは複数の VMware サービスへのアクセスを制御します。ユーザーとグループは、組織内のサービスにアクセスするにはいずれかの組織に属している必要があります。Identity Governance and Administration の機能を有効にすると、フェデレーテッド ID はセルフサービスで VMware 組織への加入をリクエストできます。詳細については、「VMware Cloud Services Console」を参照してください。

アクセス許可により特定のオブジェクトにアクセスできるようになります。またアクセス許可は、親オブジェクトから継承することも可能です。1 人のユーザーまたは 1 つのグループに重複する複数のアクセス許可が割り当てられている場合、最も制限の緩いものが適用されます。詳細については、「Hierarchical Inheritance of Permissions」を参照してください (VMware ドキュメント)。

これらの構造的要素を使用することで、最小特権のポリシーを採用し、ユーザーの要件に基づいてインフラストラクチャ内に論理的なアクセス境界を設定することができます。最小特権とは、ユーザーとアプリケーションに、タスクを実行するための必要最小限のアクセスのみを許可する原則のことです。不正アクセスが発生した場合は、この業界のベストプラクティスに従うことで、損害を与えたり機密データを盗んだりする攻撃者の能力を抑制できます。また、この原則に従うことで、承認済みのユーザーであってもアクセスすべきでないデータにはアクセスさせないようにすることができます。

必要なリソース以外はアクセスできないようにすれば、生産性も向上し、トラブルシューティングのサポートの必要性を減らすことができます。

VMware Cloud on を使用する場合 AWS、ID とアクセスを管理するための 2 つの主要なサービスとツールである VMware Cloud Services Consoleと がありますVMware vCenter Server。これらサービスの詳細については、本ガイドの後半では説明します。

ID フェデレーションと SSO

多くの企業が、外部の ID プロバイダー (IdP) とのフェデレーションを設定したいと考えています。設定すると、ユーザーにシングルサインオン (SSO) のエクスペリエンスを提供できます。VMware Cloud と vCenter Server は、共にエンタープライズフェデレーションをサポートしています。

- VMware Cloud は、Security Assertion Markup Language (SAML) 2.0 ベースの IdPs をサポートし、Lightweight Directory Access Protocol (LDAP) をサポートしています。詳細については、「What is enterprise federation and how does it work with VMware Cloud Services」(VMware ドキュメント) を参照してください。
- VMware Cloud on で vCenter Server を操作する場合 AWS、外部 IdP を使用した vCenter Server へのフェデレーションは現在サポートされていません。使用できるのは組み込みの IdP のみです。こちらは LDAP を介した Microsoft Active Directory の使用をサポートしています。詳細については、「Identity Sources for vCenter Server with vCenter Single Sign-On」(VMware ドキュメント) を参照してください。

本ガイドで取り上げている、その他の関連する VMware サービスの中には、IdP からのダイレクトフェデレーションもサポートしているものがあります。ただし、すべてのサービスでフェデレーションを設定すると、ユーザーの管理ポイントが増え、管理が難しくなります。代わりに、VMware Cloud Services Console のグループとロールを使用すれば、共通の ID ソースを使用したり、他の VMware Cloud サービスのアクセス許可を設定したりできます。また、Hybrid Linked Mode を設定し、オンプレミスの vCenter Server インスタンスと同じ ID を使用することもできます。これにより、フェデレーションと ID の管理ポイントが 2 つのサービスまで減ります。Hybrid Linked Mode の詳細については、「Configuring Hybrid Linked Mode」(VMware ドキュメント) を参照してください。

一般的なベストプラクティス

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

> **Important**
>
> このガイドで説明する VMware サービスの多くは、他のクラウドやオンプレミスの VMware ソリューションでも使用されています。このガイドに記載する推奨事項とベストプラクティスは、VMware Cloud on AWS専用です。これらの推奨事項は、他の環境では適用されない場合があります。

VMware クラウドインフラストラクチャへの ID とアクセスを管理するには、次の AWS 推奨事項を考慮してください。

- 最小特権のポリシーを適用します。ロールベースのアクセスコントロール (RBAC) を使って、ユーザーが自らの役割を果たすために必要となる、最小限のアクセス許可およびアクセス権限を付与します。
- アクセス許可は、できるだけ個々のユーザーではなくグループに付与します。
- ローカルユーザーを設定することは避けます。外部のフェデレーション ID プロバイダーに対してユーザーを認証します。
- すべてのユーザーに多要素認証を設定します。
- パスワードポリシーには、パスワードの強度とローテーションに関する要件を含めます。
- VMware の組織と関連サービスを管理者として完全に制御するための Break Glass の手順を文書化します。「Break Glass」は、、ガラスを破って火災警報器を引くという意味から来る名称で、例外的な状況でも、承認済みおよび監査済みの手順を使って、管理者のアクセス権限をすばやく利用できるようにする方法を意味します。
- オンプレミスのデータセンターまたは複数の vCenter Server インスタンスを使用している場合は、Hybrid Linked Mode を使用してクラウドの vCenter Server インスタンスをオンプレミスの

vCenter Single Sign-On ドメインに接続します。これで、vSphere Client の単一のインターフェイスからクラウドとオンプレミス両方のリソースを管理できます。

- vCenter Server、HCX Cloud Manager、NSX Manager などの管理エンドポイントは、できるだけ、パブリックインターネットからではなく内部のネットワークからのみアクセスできるように設定します。
- 管理には、cloudadmin アカウントのようなローカルの認証情報は使用しません。このようなアカウントは、Break Glass 手順の際に使用できるよう確保しておきます。管理用のローカルユーザーアカウントを使って実行されたアクションは特定の個人に帰属することができないため、これらのアカウントは、説明責任を伴わずに変更を施す際などに使用します。
- ルートユーザーや管理ユーザーなどローカルアカウントのパスワードは堅牢な値に変更し、その認証情報は監査を受けるパスワードストアに安全に保管します。こうしたパスワードへのアクセスを許可する承認プロセスを設定します。
- ローカルの認証情報を長期間 (数か月以上など) 保存する場合は、認証情報をローテーションするプロセスを設定します (VMware HCX を使用してネットワークを拡張する場合など)。

これらの推奨事項は、VMware Cloud on のすべての VMware サービス設定に適用されます AWS。各サービスにおけるその他推奨事項については、本ガイドで後ほど解説します。

VMware アイデンティティ管理サービス

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware Cloud on を使用する場合 AWS、ID とアクセスを管理するための 2 つの主要なサービスとツールである VMware Cloud Services Consoleと がありますVMware vCenter Server。

VMware Cloud Services Console

VMware Cloud Services Console (VMware ドキュメント) は、VMware Cloud on を含む VMware Cloud Services ポートフォリオの管理に役立ちます AWS。このサービスでは次のことが行えます。

- ユーザーやグループなどのエンティティの管理
- VMware Live Cyber Recovery や VMware Aria Suite などの他のクラウドサービスへのアクセスを制御する組織を管理する
- リソースやサービスへのロールの割り当て
- 組織にアクセスできる OAuth アプリケーションの表示
- 組織のエンタープライズフェデレーションの設定
- VMware Aria や VMware Cloud on などの VMware Cloud サービスを有効にしてデプロイする AWS
- 請求とサブスクリプションの管理
- VMware サポートの利用

ID とアクセスの管理

VMware Cloud Services Console でユーザー、グループ、ロール、組織を適切に設定することにより、最小特権のアクセスポリシーを実装できます。

VMware Cloud Services Console へのアクセスを保護することは非常に重要です。このサービスの管理ユーザーは、VMware クラウドの環境全体でアクセス許可を変更したり、請求情報などの機密情報

にアクセスしたりする可能性があるためです。すべてのコンソール機能 (請求やサポートなど) にアクセスするには、ユーザーを VMware Customer Connect プロファイル (正式名称は MyVMware) にリンクする必要があります。

VMware Cloud Services Console では、ユーザーとグループにアクセス許可を付与する際に次の種類のロールを使用します。

- 組織ロール — VMware Cloud の組織に直接関係するロールで、VMware Cloud Services Console 内でアクセス許可を付与します。基本のロールは次の 2 つです。組織オーナーロールは、組織を管理するためのアクセス許可をすべて持っています。組織メンバーロールは、VMware Cloud Services Console に読み取りアクセスが行えます。詳細については、「What organization roles are available in VMware Cloud Services」(VMware ドキュメント) を参照してください。
- サービスロール — 特定のサービスを使用するための、アクセス許可の割り当てを許可するロールです。例えば、DR 管理サービスロールを持つエンティティは、専用サービスコンソールで VMware Live Cyber Recovery を管理できます。組織内で利用可能なサービスはすべて、1 つ以上のサービスロールが関連付けられています。利用可能なサービスロールの詳細については、そのサービスの VMware ドキュメントを参照してください。

VMware Cloud Services Console は認証ポリシーをサポートしています。このポリシーでは、ユーザーはログイン時に 2 つ目の認証トークンを入力しなければならない、つまり多要素認証(MFA) が必須であると規定することが可能です。

このサービスにおける ID とアクセスの管理に関する詳細は、「Identity and Access Management」(VMware ドキュメント) を参照してください。

AWS レコメンデーション

AWS では、VMware Cloud on AWS向けに VMware Cloud Services Console を設定する際に 一般的なベストプラクティス に加えて以下のことを推奨しています。

- 組織を作成するときは、VMware Customer Connect プロファイル と、vmwarecloudroot@example.com など、個人用ではない、会社用の電子メールアドレスを使用します。このアカウントはサービスあるいはルートアカウントとして取り扱います。また、使用状況を監査し、このメールアカウントへのアクセスは制限する必要があります。会社の ID プロバイダー (IdP) とのアカウントフェデレーションをすぐに設定し、ユーザーがこのアカウントを使用しなくても組織にアクセスできるようにします。このアカウントは、フェデレーション IdP で発生した問題に対処する、Break Glass の手順で使用するために確保しておきます。

- 組織のフェデレーティッド ID を使用して、VMware Live Cyber Recovery などの他のクラウドサービスへのアクセスを許可します。複数のサービスで使用しているユーザーやフェデレーションは、個別には管理しません。これにより、ユーザーの入社時あるいは退職時などに、複数のサービスへのアクセス管理が容易になります。
- 組織オーナーのロールは、むやみに割り当てないようにします。このロールを持つエンティティは、組織のあらゆる側面や関連するクラウドサービスへのフルアクセスを自らに付与できます。

VMware vCenter Server

VMware vCenter Server (VMware のウェブサイト) は、VMware vSphere 環境を管理するための管理プレーンです。vCenter Server では、仮想マシンなどの vSphere リソースにアクセスし、VMware HCX や VMware Live Site Recovery などのアドオンにアクセスできるエンティティを管理します。vCenter Server の管理は vSphere Client アプリケーションを使って行います。vCenter Server では次のことが行えます。

- 仮想マシン、VMware ESXi ホスト、VMware vSAN ストレージの管理。
- vCenter Single Sign-On の設定および管理。

オンプレミスのデータセンターを使用している場合、Hybrid Linked Mode を使用して、クラウドの vCenter Server インスタンスをオンプレミスの vCenter Single Sign-On ドメインに接続できます。vCenter Single Sign-On ドメインに、Enhanced Linked Mode を使用して接続された vCenter Server インスタンスが複数含まれている場合は、それらのインスタンスはすべてクラウドの SDDC にリンクされます。このモードを使用すると、オンプレミスとクラウドのデータセンターを単一の vSphere Client インターフェイスで表示、管理でき、オンプレミスのデータセンターとクラウドの SDDC の間でワークロードを移行することができます。詳細については、「Configuring Hybrid Linked Mode」(VMware ドキュメント) を参照してください。

ID とアクセスの管理

VMware Cloud on のソフトウェア定義データセンター (SDDCs) (VMware ウェブサイト) では AWS、vCenter Server の運用方法はオンプレミス SDDC と似ています。主な違いは、VMware Cloud on AWS がマネージドサービスであることです。そのため、ホスト、クラスター、仮想マシンの管理など、特定の管理タスクはVMware が担います。詳細については、「What's Different in the Cloud?」および「Global permissions」(VMware ドキュメント) を参照してください。

VMware が SDDC の一部の管理タスクを実行するため、クラウドの管理者に必要な権限は、オンプレミスデータセンターの管理者の権限よりも少なくて済みます。VMware Cloud on AWS SDDC

を作成すると、cloudadmin ユーザーが自動的に作成され、CloudAdmin ロールが割り当てられます (VMware ドキュメント) 。特権付与されたこのローカルユーザーアカウントを使用することで、vCenter Server と vCenter Single Sign-On にアクセスできます。VMware Cloud VMware Services Console で VMware Cloud on AWS Administrator または Administrator (Delete Restricted) サービスロールを持つユーザーは、cloudadmin ユーザーの認証情報を取得できます。CloudAdmin ロールには、VMware Cloud on AWS SDDC の vCenter Server で可能な最大のアクセス許可があります。このサービスロールの詳細については、「CloudAdmin Privileges 」(VMware のドキュメント) を参照してください。cloudadmin ユーザーは、VMware Cloud on AWSの vCenter Server で使用できる唯一のローカルユーザーです。他のユーザーにアクセス権限を付与するときは外部の ID ソースを使用します。

vCenter Single Sign-On は、セキュリティトークンの交換インフラストラクチャを提供する認証ブローカーです。ユーザーが vCenter Single Sign-On の認証を受けると、そのユーザーは、API 呼び出しを使用して vCenter Server やその他のアドオンサービスの認証に使用できるトークンを受け取ります。cloudadmin ユーザーは、vCenter Server の外部 ID ソースを設定することができます。詳細については、「Identity Sources for vCenter Server with vCenter Single Sign-On」(VMware ドキュメント) を参照してください。

vCenter Server では、ユーザーとグループにアクセス許可を付与する際に次の 3 つのタイプのロールを使用します。

- システムロール — このロールは編集や削除は行えません。
- サンプルロール — このロールは、頻繁に実行されるタスクの組み合わせとして機能します。こちらのロールはコピー、編集、削除が可能です。
- カスタムロール — システムロールとサンプルロールで必要なアクセス制御を使用できない場合、vSphere Client でカスタムロールを作成できます。既存のロールを複製して変更することもできれば、新たにロールを作成することもできます。詳細については、「Create a vCenter Server Custom Role」(VMware ドキュメント) を参照してください。

SDDC インベントリ内の各オブジェクトでユーザーまたはグループに割り当てることのできるロールは 1 つのみです。1 つのオブジェクトで、ユーザーまたはグループが、組み込みのロールの組み合わせを必要とする場合、2 つの選択肢があります。1 つ目の方法は、必要なアクセス許可を持つカスタムロールを作成することです。もう 1 つの方法は、2 つのグループを作成し、それぞれに組み込みのロールを割り当て、両方のグループにユーザーを追加することです。

AWS レコメンデーション

AWS では、VMware Cloud on AWS向けに vCenter Server を設定する際に 一般的なベストプラクティス に加えて以下のことを推奨しています。

- vCenter Single Sign-On で外部 ID ソースを設定するときは、cloudadmin のユーザーアカウントを使用する。外部 ID ソースから、管理目的で使用するための適切なユーザーを割り当てて、cloudadmin ユーザーの使用は中止します。vCenter Single Sign-On の設定に関するベストプラクティスについては、「Information Security and Access for vCenter Server」(VMware ドキュメント) を参照してください。
- vSphere Client で、各 vCenter Server インスタンスの cloudadmin の認証情報を新しい値に更新し、それらを安全に保存します。この変更は、VMware Cloud Services Console には反映されません。例えば、Cloud Services Console で認証情報を表示すると更新前の値が表示されます。

> **Note**
>
> このアカウントの認証情報が失われると、VMware のサポートでそれらがリセットされます。

- cloudadmin アカウントは、日常的なアクセスには使用しません。このアカウントは、Break Glass 手順の一環として使用できるように確保しておきます。
- vCenter Server へのネットワークアクセスは、プライベートネットワークのみに制限します。

関連する VMware サービス

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

この章では、VMware VMware Cloud on に関連する以下の VMware サービスのアイデンティティとアクセスを管理するためのベストプラクティスと推奨事項について説明します AWS。

- VMware Cloud Services Console で管理されるサービス
  - VMware Cloud on AWS
  - VMware NSX
  - VMware Aria Operations for Logs
  - VMware Aria Operations for Networks
  - VMware Aria Operations
  - VMware Live Cyber Recovery
- VMware vCenter Server で管理されるサービス
  - VMware HCX
  - VMware Live Site Recovery

このガイドでは、各サービスの簡単な説明と、そのサービスの ID アクセスと管理コントロールについて説明し、VMware Cloud on の一部としてそのサービスを設定するための AWS 推奨事項を示します AWS。

VMware Cloud on AWS

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware Cloud on AWS (VMware ドキュメント) は、オンプレミスの VMware vSphere ベースの環境を に移行および拡張するのに役立つように、 AWS と VMware が共同で設計したサービスです AWS クラウド。

このサービスへのアクセスを許可する組織に属している場合は、VMware Cloud Services Console AWS から VMware Cloud on にアクセスできます。VMware Cloud on では AWS、次のことができます。

- SDDC の作成と削除。
- SDDC グループの管理。
- SDDC の管理。ネットワークやクラスターのパラメータを含みます。
- VMware vCenter Server の cloudadmin ユーザー認証情報へのアクセス。このユーザーの詳細については、本ガイドの「VMware vCenter Server」を参照してください。
- VMware NSX の cloud_admin ユーザー認証情報へのアクセス。このユーザーの詳細については、本ガイドの「VMware NSX」を参照してください。
- VMware Live Site Recovery や VMware HCX などのアドオンサービスを有効にして SDDCs 内にデプロイします。
- HCX や VMware Live Site Recovery などのアドオンサービスのコンソールにアクセスします。

ID とアクセスの管理

VMware Cloud Services Console を使用して、アイデンティティと VMware Cloud on へのアクセスを管理します AWS。VMware Cloud on では AWS、次のサービスロールを使用できます。

- 管理者 – このロールは VMware Cloud on へのフルアクセスがあります AWS。
- 管理者 (制限付き削除) – このロールは AWS、SDDC 削除オペレーションを除く VMware Cloud on へのフルアクセスがあります。
- NSX Cloud Admin
- NSX Cloud Auditor

> **Note**
>
> NSX Cloud Admin と NSX Cloud Auditor は、VMware NSX の使用に関連します。詳細については、「VMware NSX」を参照してください。

Cloud Services Portal 内の SDDC にアクセスするには、2 つの Administrator ロールのうちの 1 つが必要です。NSX Cloud の 2 つのロールのうちいずれか 1 つを持っていないユーザーは、Cloud Services Portal 内の SDDC の [Networking and Security] タブにはアクセスできず、NSX の管理者認証情報にもアクセスできません。

AWS レコメンデーション

AWS では、VMware Cloud on AWSを設定する際に 一般的なベストプラクティス に加えて以下のことを推奨しています。

- 管理者にアクセス権限を付与するときは Administrator (Delete Restricted) ロールのみを使用する。Administrator は、SDDC を削除する必要がある場合の Break Glass アクセス用に取っておきます。
- NSX ロールは、ネットワークやファイアウォールの設定にアクセスする必要のないユーザーには付与しない。詳細については、このガイドの「VMware NSX」を参照してください。
- cloudadmin のローカルユーザーアカウントのパスワードは、堅牢な値に変更し、その認証情報は、監査を受けるパスワードストアに安全に保管する。このパスワードは、vSphere Web クライアントを使用して VMware vCenter Server で変更することができます。

VMware NSX

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware NSX (VMware ドキュメント) はレイヤー 2 からレイヤー 7 までの開放型システム間相互接続 (OSI) モデルを再現したネットワーク仮想化レイヤーで、スイッチング、ルーティング、ファイアウォールなどの機能があります。NSX には 2 つのバージョンがあります。オリジナルバージョン (NSX-V) では、vCenter Server もデプロイする必要があります。新バージョン (NSX-T) は vCenter Server から切り離されているため、ハイブリッドアーキテクチャをサポートできます。VMware Cloud on は NSX-T AWS を使用します。

NSX は、vSphere および vSAN とともに、VMware Cloud on のコアコンポーネントです AWS。NSX は SDDC 内のすべてのネットワーク機能を提供し、オーバーレイネットワークとネッ

トワークアンダーレイを形成する AWS ネイティブコンポーネント間のインタラクションを管理します。NSX は、NSX API を呼び出してリソースを管理する vCenter Server や VMware HCX など、他のサービスと緊密に連携しています。

NSX では、以下のことが行えます。

- スイッチングとルーティングの管理。
- ファイアウォールの管理。VM 間、またはネットワークとパブリックインターネット間のインライン検査のための、分散型ファイアウォールを使用した管理を含みます。
- 仮想プライベートネットワーク (VPN) の管理。
- Dynamic Host Configuration Protocol (DHCP) とドメインネームシステム (DNS) の設定。

NSX には、VMware Cloud Services Console か、専用の NSX Manager ウェブユーザーインターフェイス (UI) からアクセスすることができます。NSX Manager ウェブ UI では、VMware Cloud Services Console では利用できない追加機能をいくつか利用できます。詳細については、「SDDC Network Administration with NSX Manager」(VMware ドキュメント) を参照してください。

VMware Cloud on AWSで NSX にアクセスするときは、次の点に注意します。

- VMware Cloud Services Console から NSX にアクセスするには、VMware Cloud on AWS Administrator ロールを割り当てる必要があります。NSX には、SDDC の Networking and Security タブからアクセスできます。このロールの詳細については、本ガイドの「VMware Cloud on AWS」を参照してください。
- NSX Manager のウェブ UI を開くには、SDDC の [Settings] タブでリンクを選択するか、SDDC の[Summary] ページで [Open NSX Manager] を選択します。詳細については、「Open NSX Manager」(VMware ドキュメント) を参照してください。
- SDDC が Payment Card Industry Data Security Standard (PCI DSS) モードの場合、VMware Cloud Services Console の [Networking and Security] タブから NSX にアクセスすることはできません。NSX Manager ウェブ UI を使用する必要があります。

ID とアクセスの管理

VMware NSX の ID とアクセスの管理には VMware Cloud Services Console を使用します。VMware Cloud on の NSX では AWS、次のサービスロールを使用できます。

- NSX Cloud Admin — このロールを使うと、VMware Cloud on AWSで VMware NSX の機能を管理することができます。

- NSX Cloud Auditor — このロールを使うと、NSX サービスの設定とイベントを閲覧できますが、変更を加えることはできません。

> **Note**
>
> 名前には NSX Cloud とありますが、これらのロールは VMware NSX Cloud のサービスとは関係ありません。

次のユーザーは NSX にアクセスできます。

- cloud_admin ローカルユーザー。多くの特権が付与された組み込みのローカル NSX ユーザーです。NSX Cloud Admin のロールを持つユーザーは、このユーザーアカウントの認証情報にアクセスすることができます。名前は似ていますが、cloud_admin ユーザーは cloudadmin@vmc.local vCenter Single Sign-On ローカルユーザーとは異なります。
- VMware Cloud Services Console で NSX Cloud Admin サービスロールまたは NSX Cloud Auditor サービスロールのいずれかを割り当てられているユーザー。このユーザーは、VMware Cloud Services Console のユーザーでも、外部のフェデレーションユーザーでもかまいません。
- ID ソースから NSX へのアクセス権限を LDAP を介して直接付与されたユーザー。

AWS レコメンデーション

AWS では、VMware Cloud on AWS向けに NSX を設定する際に 一般的なベストプラクティス に加えて以下のことを推奨しています。

- 社内に、ネットワークとファイアウォールの管理は担当するが SDDC の管理は担当しないユーザーがいる場合、これらのユーザーには NSX ロールのいずれか 1 つを付与しますが、Administrator ロールは付与しません。これらのユーザーは、NSX には NSX Manager のウェブ UI からアクセスする必要があります。
- cloud_admin のローカルユーザーアカウントのパスワードは堅牢な値に変更し、その認証情報は、監査を受けるパスワードストアに安全に保管します。このパスワードを変更するときは、VMware サポートに連絡する必要があります。
- NSX 内で、外部ユーザーにアクセス権限を直接付与することはしません。代わりに、VMware Cloud Services Console でエンタープライズフェデレーションを設定し、ロールとグループを使用してこのサービスへのアクセス権限を付与します。

VMware Aria Operations for Logs

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware Aria Operations for Logs (VMware ドキュメント) (旧 VMware vRealize Log Insight Cloud) は、VMware SDDC で生成されたログデータの視覚化とクエリに役立つ、ログストレージと分析ツールです。VMware Aria Operations for Logs では、次のことが行えます。

- vRealize Operations のオンプレミスインスタンスとの統合。
- マシンで生成されたあらゆる種類のログデータの収集と分析。
- アラートを設定する
- 他の VMware サービスの、ログのモニタリングと分析。

この一元化されたログ管理サービスには 2 つのバージョンがあります。VMware vRealize Log Insight はオンプレミスのバージョンで、SDDC 内でアプライアンスとして実行することができます。VMware Aria Operations for Logs は、Software as a Service (SaaS) のバージョンです。VMware Cloud on AWS では、クラウドバージョンをデフォルトのログ記録サービスとして使用します。これは変更できません。オンプレミスのバージョンを使用するときは、ログをクラウドインスタンスからオンプレミスインスタンスに転送する必要があります。

VMware Aria Operations for Logs は VMware Cloud on に含まれています AWS。組み込まれたバージョンでは、取り込みの容量と保存期間に制限があります。これらの制限は、必要に応じてプレミアムサブスクリプションにアップグレードすることで増やすことができます。詳細については、「Subscriptions and Billing」(VMware ドキュメント) を参照してください。

ID とアクセスの管理

VMware Aria Operations for Logs の ID とアクセスの管理には VMware Cloud Services Console を使用します。VMware Aria Operations for Logs では、フェデレーション ID やグループを含め、VMware Cloud Services Console で設定したものと同じユーザーを使用します。このサービスのアクセス許可を付与するときは、VMware Aria Operations for Logs 内でサービスロールを割り当て

るか、カスタムロールを設定します 詳細については、「Service Roles」(VMware ドキュメント) を参照してください。

VMware vRealize Log Insight にはデフォルトのロールが 2 つあります。Administrator ロールにはフルアクセスとコントロールの権限があります。User ロールには読み取り権限があり、ダッシュボードを作成できます。カスタムロールを使用すると、特定のデータセットのみにアクセスを許可できます。これらのデータセットには、ユーザーが使用できるログデータを制限するフィルタが含まれています。詳細については、「Create a Data Set」(VMware ドキュメント) を参照してください。

AWS レコメンデーション

本ガイドに記載している「一般的なベストプラクティス」に従ってください。このサービスの ID とアクセスの管理に関して追加の推奨事項はありません。

VMware Aria Operations for Networks

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware Aria Operations for Networks (旧 VMware vRealize Network Insight Cloud) は、vRealize Network Insight の SaaS バージョンです。「VMware vRealize Network Insight 」(VMware ドキュメント) は、ワークロードのトラフィックフローを把握するのに役立ちます。このサービスを使用すれば、ネットワークの問題を診断したり、ワークロードのセグメント化に役立つファイアウォールルールをモデル化したりできます。VMware Aria Operations for Networks では、次のことが行えます。

- ハイブリッド環境とマルチクラウド環境の確認。
- トラフィックフローのトラブルシューティングと分析。
- アプリケーションの検出と分析。
- ワークロード間の依存関係のマッピング。

このサービスには 3 つのバージョンがあります。VMware vRealize Network Insight はオンプレミス専用のバージョンです。VMware Aria Operations for Networks は SaaS バージョンです。vRealize

Network Insight Universal は、オンプレミスのソリューションとして、またはフェデレーションクラウド SaaS ソリューションとしてデプロイできます。すべてのバージョンは VMware Cloud on と互換性があります AWS。

ID とアクセスの管理

VMware Aria Operations for Networks の ID とアクセスの管理には VMware Cloud Services Console を使用します。VMware Aria Operations for Networks では、フェデレーション ID やグループを含め、VMware Cloud Services Console で設定したものと同じユーザーを使用します。VMware Aria Operations for Networks で使用できるサービスロールは、以下のとおりです。

- Administrator — このロールにはフルアクセスとコントロールの権限があります。
- Member — このロールのアクセス権限は制限付きです。
- Auditor — このロールのアクセス権限は読み取り専用です。

AWS レコメンデーション

本ガイドに記載している「一般的なベストプラクティス」に従ってください。このサービスの ID とアクセスの管理に関して追加の推奨事項はありません。

VMware Aria Operations

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware Aria Operations (VMware ドキュメント) (旧 VMware vRealize Operations Cloud) は、VMware Cloud on AWSのオペレーション管理プラットフォームです。このサービスは、人工知能と機械学習 (AI/ML) を活用して、ハイブリッドクラウドのデプロイにおけるアプリケーションとインフラストラクチャの最適化、プランニング、スケールをサポートします。VMware Aria Operations では、次のことが行えます。

- パフォーマンスと容量の、AI/ML を活用した最適化に関する推奨事項の確認。

- コンプライアンスとリソース設定の管理。
- ユーザーの問題の解決やアラートへの対応など、トラブルシューティングに役立つツールへのアクセス。
- Management Pack (VMware ドキュメント) を使った、本サービスのモニタリング、トラブルシューティング、修復機能の拡張。

このオペレーション管理サービスには 2 つのバージョンがあります。VMware vRealize Operations はオンプレミスのバージョンで、SDDC 内でアプライアンスとして実行することができます。VMware Aria Operations は、vRealize Operations の Software as a Service (SaaS) バージョンです。どちらのバージョンも VMware Cloud on と互換性があります AWS。VMware Cloud on AWS はマネージドサービスであり、一部のリソースへのアクセスは制限されているため、すべての vRealize オペレーション機能がサポートされているわけではありません。詳細については、「Known Limitations」(VMware ドキュメント) を参照してください。

ID とアクセスの管理

VMware Aria Operations の ID とアクセスの管理には VMware Cloud Services Console を使用します。VMware Aria Operations では、フェデレーション ID を含め、VMware Cloud Services Console で設定するものと同じユーザーを使用します。このサービスのアクセス許可を付与するときは、VMware Aria Operations 内でサービスロールを割り当てるか、カスタムロールを設定します 利用できるサービスロールの詳細については、「Roles and Privileges 」(VMware のドキュメント) を参照してください。

組み込みのロールには Administrator、GeneralUser、ReadOnly の 3 種類があり、必要に応じて、特定のアクセス許可要件に一致するカスタムロールを作成することが可能です。グループを作成すると、複数ユーザーのアクセス許可を管理することに伴う管理オーバーヘッドを最小限に抑えられます。

ローカルユーザーは VMware vRealize Operations のオンプレミスバージョンがサポートしており、フェデレーションユーザーはクラウドとオンプレミスの両方のバージョンがサポートしています。ただし、外部 ID プロバイダへのユーザーのフェデレーションは、vRealize Operations の、オンプレミスとクラウドのバージョン間で異なります。オンプレミスバージョンでは、LDAP を介して外部の IdP からユーザーを直接フェデレーションするか、vCenter Server でフェデレーションした ID を使用することが可能です。クラウドバージョンでは、フェデレーションユーザーを含め、VMware Cloud Services Console で設定したものと同じユーザーを使用します。

AWS レコメンデーション

AWS では、VMware Cloud on AWS向けに VMware Aria Operations を設定する際に 一般的なベストプラクティス に加えて以下のことを推奨しています。

- ユーザーを直接フェデレーションすることは避けます。クラウドバージョンでは、VMware Cloud Services Console でユーザーをフェデレーションし、ロールとグループを使用してこのサービスへのアクセス権限を付与します。オンプレミスバージョンでは、認証済みのソースの ID を使用するか、シングルサインオン (SSO) を有効にします。詳細については、「Authentication sources」と「Configure a Single Sign-On Source」(VMware ドキュメント) を参照してください。

VMware Live Cyber Recovery

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware Live Cyber Recovery (VMware ドキュメント) は、ディザスタリカバリへの階層型アプローチを提供するサービスとしてのディザスタリカバリ (DRaaS) ソリューションです。目標復旧時点 (RPO) と目標復旧時間 (RTO) のコストとタイムスケールを、特定のワークロードの要件を満たすように調整することができます。そうすることで、信頼性の高い保護と、ディザスタリカバリリソースの効率的な活用との間でバランスを取ることができます。VMware Live Cyber Recovery では、次のことができます。

- 仮想マシンのバックアップの作成。
- 耐久性の高いクラウドストレージへのバックアップの保管。
- オンデマンドからホットスタンバイまで、復旧する対象に合わせたデプロイ方法の柔軟な選択。
- カスタム RPO と RTO の設定。

ID とアクセスの管理

VMware Cloud Services Console を使用して、アイデンティティと VMware Live Cyber Recovery へのアクセスを管理します。VMware Live Cyber Recovery は、フェデレーティッド ID や VMware

Cloud Services Console で設定したグループなど、同じユーザーを使用します。このサービスのアクセス許可を付与するには、VMware Live Cyber Recovery サービスロールを割り当てるか、VMware Live Cyber Recovery 内でカスタムロールを作成します。使用可能なサービスロールの詳細については、VMware Live Cyber Recovery エンドユーザーロール」(VMware ドキュメント) を参照してください。

VMware Live Cyber Recovery には、サービスの運用に使用できるいくつかの組み込みロールが含まれています。

- Administrator — API トークンへのアクセスを除く、完全なコントロール権限があります。
- Auditor — ユーザーインターフェースに読み取り専用でアクセスできます (ユーザー管理は除く)。コンプライアンスレポートへのアクセス権限があります。
- DR Admin — ディザスタリカバリ計画を作成、テスト、実行します。
- Backup Admin — 保護対象のサイトと保護グループを管理します。VM をリストアするためのアクセス権限があります。
- Plan Tester — ディザスタリカバリ計画を作成し、テスト復旧を実行します。
- SDDC Admin — SDDC を管理します。

AWS レコメンデーション

本ガイドに記載している「一般的なベストプラクティス」に従ってください。このサービスの ID とアクセスの管理に関して追加の推奨事項はありません。

VMware HCX

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware HCX (VMware ドキュメント) は、SDDC 間でワークロード移行を実行できる、アプリケーションモビリティプラットフォームです。VMware HCX は VMware Cloud on に含まれ AWS ており、ワークロードの移行に使用できます。VMware HCX では、次のことが行えます。

- SDDC 間でのマルチサイトメッシュの設定。

- HCX サイト間でのネットワークの拡張。
- 仮想マシンの移行。

ID とアクセスの管理

VMware HCX の ID とアクセスの管理には VMware vCenter Server を使用します。VMware HCX では、リソースや以降の作成および管理のため、vCenter Server や NSX へのアクセスを含め、他の VMware サービスにアクセスできる必要があります。VMware HCX には次の 2 つのコンポーネントサービスがあります。

- HCX Cloud Manager — VMware Cloud Services Console で、SDDC の VMware HCX を有効にします。これにより、選択した SDDC 内に HCX Cloud Manager アプライアンスがインストールされます。詳細については、「Deploying the HCX Installer OVA in the vSphere Client」(VMware のドキュメント) を参照してください。デプロイ後は、vCenter Server の cloudadmin 認証情報を使って HCX Cloud Manager サービスにアクセスできます。
- HCX Connector — HCX Connector Open Virtualization Archive (OVA) ファイルは、HCX Cloud Manager サービスから取得できます。このファイルを使用して、HCX Cloud Manager アプライアンスを任意の vCenter Server インスタンスにインストールします。このインスタンスは VMware HCX の移行ソースとしてセットアップされます。HCX Connector の各インスタンスは、それぞれ独自の管理者認証情報とルート認証情報があります。

両方のコンポーネントサービスをデプロイすると、vCenter Server 経由で VMware HCX にアクセスできます。Administrators vCenter Single Sign-On グループには、HCX Administrator ロールが自動的に付与されます。HCX をインストールすると、vCenter Single Sign-On にロールと特権が多数追加されます。これらを使用すると、VMware HCX のアクセス制御を、さまざまなユーザーのタイプに基づいてきめ細かく作成できます。

AWS レコメンデーション

AWS では、VMware Cloud on AWS向けに VMware HCX を設定する際に 一般的なベストプラクティス に加えて以下のことを推奨しています。

- ゲートウェイファイアウォールルールを使用して HCX Cloud Manager サービスへのネットワークアクセスを制限する。
- オンプレミスの HCX Connector の管理者とルートユーザーの認証情報を安全に保管する。自社のポリシーに従ってこれらの認証情報をローテーションすることを検討します。これらの認証情報は、VMware が HCX Cloud Manager のためにお客様に代わって管理します。

- オンプレミスの HCX Connector インスタンスでは、さまざまなタイプの HCX ユーザーの、ニーズに合ったカスタム HCX ロールを作成することを検討します。例えば、HCX を設定し管理するユーザーには制限の緩いロールを作成し、移行のみを管理するユーザーには制限の厳しいロールを作成するなどです。
- VMware HCX と VMware Cloud on をペアリングする場合は AWS、cloudadmin ユーザーを使用する必要があります。
- HCX Cloud を VMware Cloud on とペアリングする場合 AWS、VMware Cloud on AWS SDDC と Active Directory 間の認証はサポートされていません。詳細については、「[VMC on AWS] AD unsupported for HCX Cloud to Cloud setup」を参照してください (VMware ナレッジベースの記事 90433)。

VMware Live Site Recovery

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

VMware Live Site Recovery (VMware ドキュメント) は、オンプレミス環境向けの VMware Site Recovery Manager サービスに基づくオンデマンドのディザスタリカバリサービス (DRaaS) ソリューションです。VMware Live Site Recovery では、次のことができます。

- レプリケーション、オーケストレーション、自動化の実装を通じて、サイトに障害が発生した場合にワークロードを保護する。
- エンドツーエンドのディザスタリカバリソリューションを構築し、SDDC の保護に役立てる。

ID とアクセスの管理

VMware vCenter Server を使用して、アイデンティティと VMware Live Site Recovery へのアクセスを管理します。VMware Live Site Recovery は、仮想マシンのレプリケーションや電源オフなど、ユーザーに代わってオペレーションを実行します。VMware Live Site Recovery は、ロールと権限を使用して、適切なアクセス許可を持つユーザーのみが、リカバリプランのすべてのステップを実行するなど、リカバリオペレーションを実行できるようにします。

詳細については、VMware Live Site Recovery の権限、ロール、アクセス許可」(VMware ドキュメント) を参照してください。

フェデレーティッド ID を使用して vCenter Server にアクセスする場合は、Hybrid Linked Mode を使用してこれらのグループにエンティティを追加する必要があります。詳細については、「Configuring Hybrid Linked Mode」(VMware ドキュメント) を参照してください。

AWS レコメンデーション

では、 に加えて一般的なベストプラクティス、VMware Cloud on の VMware Live Site Recovery を設定するときに、次のことを AWS 推奨しています AWS。

- ソースサイトとターゲットサイトの両方で、ユーザーに同じロールが割り当てられていることを確認します。これにより、保護されたオブジェクトと復旧したオブジェクトに同じアクセス許可が付与されます。
- Hybrid Linked Mode を使用して、vCenter Server 内のフェデレーティッド ID のロール割り当てを管理します。
- VMware Live Site Recovery は、SDDC 内でのみプライベート IP アドレスを使用します。一般的なベストプラクティス に合わせて、VMware Cloud on AWS vCenter がプライベート IP アドレスを解決していることを確認します。

サンプルグループとロール

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

次の表は、VMware Cloud on AWSを使用する際の ID およびアクセス管理戦略の例です。ユーザーペルソナ、ペルソナがアクセスする必要のある VMware サービス、組織とグループのメンバーシップ、割り当てられたロール、使用される ID のタイプ (ローカルユーザーやフェデレーション ID など) について概説しています。この表を出発点として、このガイドで推奨されているベストプラクティスに従った企業戦略を設計してください。

ユーザーペルソナ	アクセスしたサービス	VMware Cloud のサンプルグループ名	VMware Cloud サービスロール	vCenter Single Sign-On のサンプルグループ名	vCenter Single Sign-On ロール	アイデンティティソース
組織のブレークグラス	VMware Cloud Services Console	なし	組織の所有者	なし	なし	ローカルユーザー (サービスアカウントの E メールアドレス)
VMware 管理者	VMware Cloud Services Console vCenter Server	`vmware_admins`	組織の所有者	`vmware_admins`	管理者	フェデレーション ID プロバイダー

ユーザーペルソナ	アクセスしたサービス	VMware Cloud のサンプルグループ名	VMware Cloud サービスロール	vCenter Single Sign-On のサンプルグループ名	vCenter Single Sign-On ロール	アイデンティティソース
	HCX VMware Live Site Recovery VMware Live Cyber Recovery vRealize Operations					
バックアップ管理者	vCenter Server	なし	なし	`vmware_backups`	パワーユーザー	フェデレーション ID プロバイダー
ディザスタリカバリ管理者	vCenter Server VMware Cloud Services Console VMware Live Site Recovery VMware Live Cyber Recovery	`vmware_dr`	組織のメンバー DR 管理者 DR SDDC 管理者	`vmware_dr`	SrmAdministrator HmsCloudAdmin	フェデレーション ID プロバイダー

ユーザーペルソナ	アクセスしたサービス	VMware Cloud のサンプルグループ名	VMware Cloud サービスロール	vCenter Single Sign-On のサンプルグループ名	vCenter Single Sign-On ロール	アイデンティティソース
VMware オペレーター	VMware Cloud Services Console vCenter Server HCX vRealize Operations	`vmware_ops`	組織のメンバー vROps 管理者	`vmware_ops`	パワーユーザー	フェデレーション ID プロバイダー
ネットワークチーム	VMware Cloud Services Console vCenter Server	`vmware_networks`	組織のメンバー NSX Cloud Admin	`vmware_networks`	Readonly	フェデレーション ID プロバイダー

ユーザーペルソナ	アクセスしたサービス	VMware Cloud のサンプルグループ名	VMware Cloud サービスロール	vCenter Single Sign-On のサンプルグループ名	vCenter Single Sign-On ロール	アイデンティティソース
セキュリティチーム	VMware Cloud Services Console vCenter Server HCX (一時アクセス) VMware Live Site Recovery VMware Live Cyber Recovery vRealize Operations	`vmware_security`	組織のメンバー vROps ReadOnly	`vmware_security`	Readonly	フェデレーション ID プロバイダー
監査人	VMware Cloud Services Console vCenter Server	`vmware_audit`	組織のメンバー	`vmware_audit`	Readonly	フェデレーション ID プロバイダー

次のステップ

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

このガイドでは、VMware Cloud on および関連する VMware VMware サービスのアイデンティティ AWS とアクセスを管理するために推奨されるベストプラクティスについて説明しました。これらの推奨事項は、クラウドおよびハイブリッドクラウドのインフラストラクチャを保護し、不正アクセスを阻止するように設計されているだけでなく、それらのスケール性と効率性を高めるようにも設計されています。ユーザーをグループに割り当てた後にロールをグループに割り当てると、アクセス許可をより迅速に付与または制限することができ、ユーザーを個別に設定することに伴うオーバーヘッドを最小限に抑えることができます。また、外部の ID プロバイダーとのフェデレーション、および vCenter Single Sign-On を使用することで、シームレスなシングルサインオンエクスペリエンスをユーザーに提供できます。

ご自身の会社に適した ID とアクセスの管理戦略を設計するには、サンプルグループとロール の表を参照してください。本ガイドで推奨事項を確認した後は、リソース セクションに記載されているリンクをご確認いただくことをお勧めします。これらのリソースは、VMware Cloud サービスの詳細と、本ガイドで解説しているベストプラクティスの設計方法について学ぶのに役立ちます。

リソース

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

関連 AWS リソース

- VMware Cloud on AWS の概要と運用モデル
- VMware Cloud on のワークロードのディザスタリカバリオプション AWS
- VMware Cloud on のストレージオフロードオプションの設定 AWS
- VMware Cloud on AWS を使用して に VMware SDDC をデプロイする AWS
- VMware HCX AWS を使用して VMware SDDC を VMware Cloud on に移行する

VMware ドキュメント

VMware Cloud on AWS

- VMware Cloud Services を使用したエンタープライズ フェデレーションの設定
- VMware Cloud Services Identity とアクセス管理

VMware vCenter Server と vCenter Single Sign-On

- vSphere での認可について
- VMware Cloud on での vSphere 管理 AWS
- vSphere での vCenter Single Sign-On の使用
- Configuring vCenter Single Sign-On Identity Sources
- Hierarchical Inheritance of Permissions
- Information Security and Access for vCenter Server
- vSphere Required Privileges for Common Tasks

VMware NSX

- NSX Administration Guide
- Information Security and Access for NSX-T Data Center

VMware HCX

- VMware HCX Documentation
- VMware HCX User Account and Role Requirements

VMware Aria と vRealize スイート

- VMware vRealize Operations のドキュメント
- Roles and Privileges in vRealize Operations Cloud
- VMware vRealize Log Insight Datasheet
- Getting Started with VMware Aria Operations for Logs
- VMware Cloud Services ドキュメント
- vRealize Network Insight のユーザー管理

VMware Live Site Recovery

- VMware Live Site Recovery ドキュメント
- VMware Live Site Recovery の権限、ロール、アクセス許可

VMware Live Cyber Recovery

- VMware Live Cyber Recovery ドキュメント
- VMware Live Cyber Recovery エンドユーザーロール

ドキュメント履歴

> **注意**
>
> 2024 年 4 月 30 日現在、VMware Cloud on AWS は AWS またはそのチャネルパートナーによって再販されなくなりました。このサービスは、Broadcom を通じて引き続き利用できます。詳細については、 AWS 担当者にお問い合わせください。

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
VMware サービス	VMware Cloud Disaster Recovery を VMware Live Cyber Recovery に置き換え、VMware Site Recovery を VMware Live Site Recovery に置き換えました。詳細については、VMware Live Recovery リリースノートを参照してください。	2024 年 9 月 4 日
VMware HCX へのアクセス	VMware HCX for VMware Cloud on の設定に関するAWS 推奨事項を更新しましたAWS。	2023 年 6 月 5 日
初版発行	—	2022 年 11 月 3 日

AWS 規範的ガイダンスの用語集

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

数字

7 Rs

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

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

A

ABAC

「属性ベースのアクセスコントロール」を参照してください。

抽象化されたサービス

「 マネージドサービス」を参照してください。

ACID

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

行のグループに対して動作し、グループの単一の戻り値を計算する SQL 関数。集計関数の例としては、 SUMや などがありますMAX。

AI

「人工知能」を参照してください。

AIOps

「人工知能オペレーション」を参照してください。

匿名化

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

アンチパターン

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

アプリケーションコントロール

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン

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

AWS クラウド導入フレームワーク (AWS CAF)

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 るのに役立つ、 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、組織がクラウド導入を成功させるための準備に役立つ、人材開発、トレーニング、コミュニケーションのためのガイダンスを提供します。詳細については、AWS CAF ウェブサイト と AWS CAF のホワイトペーパー を参照してください。

AWS ワークロード認定フレームワーク (AWS WQF)

データベース移行ワークロードを評価し、移行戦略を推奨し、作業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

個人または組織に混乱や損害を与えることを目的としたボット。

BCP

「事業継続計画」を参照してください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。エンディアンネスも参照してください。

二項分類

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

ブルームフィルター

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

ブルー/グリーンデプロイ

2 つの異なる同一の環境を作成するデプロイ戦略。現在のアプリケーションバージョンは 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、影響を最小限に抑えながら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インタラクション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います。既存のブランチから新しいブランチを作成し、その新しいブランチで機能を開発したり、バグを修正したりできます。機能を構築するために作成するブランチは、通常、機能ブランチと呼ばれます。機能をリリースする準備ができたら、機能ブランチをメインブランチに統合します。詳細については、「ブランチの概要」(GitHub ドキュメント) を参照してください。

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、通常はアクセス許可 AWS アカウント を持たない にユーザーが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 ガイダンスの AWS ブレークグラスプロシージャ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。

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、ターゲットシステムでの変更を監査またはレプリケートして同期を維持するなど、さまざまな目的に使用できます。

カオスエンジニアリング

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

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

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

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、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の CCoE 投稿を参照してください。

クラウドコンピューティング

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

クラウド運用モデル

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

導入のクラウドステージ

組織が に移行するときに通常実行する 4 つのフェーズ AWS クラウド：

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

これらのステージは、 AWS クラウド エンタープライズ戦略ブログのブログ記事「クラウドファーストへのジャーニー」と「導入のステージ」で Stephen Orban によって定義されています。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、 GitHubまたは が含まれますBitbucket Cloud。コードの各バージョンはブランチと呼ばれます。マイクロサービスの構造では、各リポジトリは 1 つの機能専用です。1 つの CI/CD パイプラインで複数のリポジトリを使用できます。

コールドキャッシュ

空である、または、かなり空きがある、もしくは、古いデータや無関係なデータが含まれているバッファキャッシュ。データベースインスタンスはメインメモリまたはディスクから読み取る必

要があり、バッファキャッシュから読み取るよりも時間がかかるため、パフォーマンスに影響します。

コールドデータ

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

コンピュータビジョン (CV)

機械学習を使用してデジタルイメージやビデオなどのビジュアル形式から情報を分析および抽出する AI の分野。例えば、 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、設定は想定状態から変化します。これにより、ワークロードが非準拠になる可能性があり、通常は段階的で意図的ではありません。

構成管理データベース (CMDB)

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

コンフォーマンスパック

コンプライアンスチェックとセキュリティチェックをカスタマイズするためにアセンブルできる AWS Config ルールと修復アクションのコレクション。YAML テンプレートを使用して、コンフォーマンスパックを AWS アカウント および リージョンの単一のエンティティとしてデプロイするか、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

一元的な管理とガバナンスにより、分散型の分散データ所有権を提供するアーキテクチャフレームワーク。

データ最小化

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

データ境界

AWS 環境内の一連の予防ガードレール。信頼できる 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。

多層防御

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

委任管理者

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

デプロイ

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

開発環境

???「環境」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

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

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ドリフトを検出したり、 を使用して AWS Control Tower 、ガバナンス要件のコンプライアンスに影響を与える可能性のあるランディングゾーンの変更を検出したりできます。

DVSM

「開発値ストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

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

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

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かつ段階的なテストを使用する哲学。これはアジャイルアプローチの重要な部分です。

障害分離の境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を向上させるアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界です。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、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

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

数ショットプロンプト

LLM に同様のタスクの実行を求める前に、タスクと必要な出力を示す少数の例を提供します。この手法は、プロンプトに埋め込まれた例 (ショット) からモデルが学習するコンテキスト内学習の

アプリケーションです。少数ショットプロンプトは、特定のフォーマット、推論、またはドメイン知識を必要とするタスクに効果的です。「ゼロショットプロンプト」も参照してください。

FGAC

「きめ細かなアクセスコントロール」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

段階的なアプローチを使用するのではなく、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)

一般化およびラベル付けされていないデータの大規模なデータセットでトレーニングされている大規模な深層学習ニューラルネットワーク。FMsは、言語の理解、テキストと画像の生成、自然言語での会話など、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、「基盤モデルとは」を参照してください。

G

生成 AI

大量のデータでトレーニングされ、シンプルなテキストプロンプトを使用してイメージ、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)

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

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

Gitflow ワークフロー

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

ゴールデンイメージ

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 (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、Amazon GuardDuty、、 AWS Trusted Advisor Amazon Inspector、およびカスタム AWS Lambda チェックを使用して実装されます。

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

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

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

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

ホットデータ

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

ホットフィックス

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

ハイパーケア期間

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

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「産業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、本番ワークロード用の新しいインフラストラクチャをデプロイするモデル。イミュータブルなインフラストラクチャは、本質的にミュータブルなインフラストラクチャよりも一貫性、信頼性、予測性が高くなります。詳細については、 AWS 「 Well-Architected Framework」の「Deploy using immutable infrastructure best practice」を参照してください。

インバウンド (受信) VPC

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

増分移行

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

インダストリー 4.0

2016 年に Klaus Schwab によって導入された用語で、接続性、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。

産業分野における IoT (IIoT)

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

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「モノのインターネット」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

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

大規模言語モデル (LLM)

大量のデータに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、LLMs」を参照してください。

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースのアクセスコントロール」を参照してください。

最小特権

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

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。エンディアン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、およびプラットフォームを AWS 運用し、ユーザーがエンドポイントにアクセスしてデータを保存および取得する 。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。これにより、加工品目を工場の完成製品に変換します。

MAP

「移行促進プログラム」を参照してください。

メカニズム

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

メンバーアカウント

組織の一部である管理アカウント AWS アカウント 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、パブリッシュ/サブスクライブパターンに基づく軽量 machine-to-machine (M2M) 通信プロトコル。

マイクロサービス

明確に定義された API を介して通信し、通常は小規模な自己完結型のチームが所有する、小規模で独立したサービスです。例えば、保険システムには、販売やマーケティングなどのビジネス

機能、または購買、請求、分析などのサブドメインにマッピングするマイクロサービスが含まれる場合があります。マイクロサービスの利点には、俊敏性、柔軟なスケーリング、容易なデプロイ、再利用可能なコード、回復力などがあります。詳細については、AWS「サーバーレスサービスを使用したマイクロサービスの統合」を参照してください。

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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、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 を使用して Amazon EC2 への移行をリホストします。

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

???「機械学習」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

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

モノリシックアプリケーション (モノリス)

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

MPA

「移行ポートフォリオ評価」を参照してください。

MQTT

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

多クラス分類

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

ミュータブルインフラストラクチャ

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

O

OAC

「オリジンアクセスコントロール」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織の変更管理」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

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

オープンプロセス通信 - 統合アーキテクチャ (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

インシデントや潜在的な障害の範囲を理解、評価、防止、または縮小するのに役立つ質問のチェックリストと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)

物理環境と連携して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重要な焦点です。

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

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

オリジンアクセスアイデンティティ (OAI)

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

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

個人を特定できる情報を参照してください。

プレイブック

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

PLC

「プログラム可能なロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

アクセス許可の定義 (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。一般的に `false`WHERE句にあります。

述語プッシュダウン

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

予防的コントロール

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

プリンシパル

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

プライバシーバイデザイン

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

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

設計、開発、発売から成長と成熟まで、ライフサイクル全体を通じて製品のデータとプロセスを管理し、辞退と削除を行います。

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 ("")

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、信頼性が高く適応可能なコンピュータです。

プロンプトの連鎖

1 つの LLM プロンプトの出力を次のプロンプトの入力として使用して、より良いレスポンスを生成します。この手法は、複雑なタスクをサブタスクに分割したり、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。

パブリッシュ/サブスクライブ (pub/sub)

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

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

Q

クエリプラン

SQL リレーショナルデータベースシステム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、情報提供 (RACI) を参照してください。

RAG

「拡張生成の取得」を参照してください。

ランサムウェア

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

RASCI マトリックス

責任、説明責任、相談、情報提供 (RACI) を参照してください。

RCAC

「行と列のアクセスコントロール」を参照してください。

リードレプリカ

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

再設計

「7 Rs」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 R」を参照してください。

リージョン

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

回帰

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

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

プラットフォーム変更

「7 R」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。で回復性を計画するときは、高可用性とディザスタリカバリが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 「回復力」を参照してください。

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンシブコントロール

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

保持

「7 R」を参照してください。

廃止

「7 R」を参照してください。

取得拡張生成 (RAG)

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

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

目標復旧時間を参照してください。

ランブック

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

S

SAML 2.0

多くの ID プロバイダー (IdP) が使用しているオープンスタンダード。この機能により、フェデレーティッドシングルサインオン (SSO) が有効になるため、ユーザーは にログイン 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に対して IAM でユーザーを作成する必要はありません。SAML 2.0 ベースのフェデレーションの詳細については、IAM ドキュメントのSAML 2.0 ベースのフェデレーションについてを参照してください。

SCADA

「監視コントロールとデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存する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、単一の文字列、または複数の文字列にすることができます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの内容」を参照してください。

設計によるセキュリティ

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

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントに自動的に応答または修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としては、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先で、それ AWS のサービス を受け取る によるデータの暗号化。

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットなど、サービスのパフォーマンス側面の測定。

サービスレベル目標 (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。

スプリットアンドシードモデル

モダナイゼーションプロジェクトのスケーリングと加速のためのパターン。新機能と製品リリースが定義されると、コアチームは解放されて新しい製品チームを作成します。これにより、お

客様の組織の能力とサービスの拡張、デベロッパーの生産性の向上、迅速なイノベーションのサポートに役立ちます。詳細については、『』の「アプリケーションをモダナイズするための段階的アプローチ AWS クラウド」を参照してください。

SPOF

単一障害点を参照してください。

star スキーマ

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

strangler fig パターン

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

サブネット

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

監視コントロールとデータ収集 (SCADA)

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

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

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

システムプロンプト

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

T

tags

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

ターゲット変数

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

タスクリスト

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

テスト環境

???「環境」を参照してください。

トレーニング

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

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内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 の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

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

U

不確実性

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

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

「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。

Write Once, Read Many (WORM)

データを 1 回書き込み、データの削除や変更を防ぐストレージモデル。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

ゼロデイエクスプロイト

ゼロデイ脆弱性を利用する攻撃、通常はマルウェア。

ゼロデイ脆弱性

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

ゼロショットプロンプト

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

ゾンビアプリケーション

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

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