SAP on AWS グリーンフィールド実装のベストプラクティス

AWS 規範ガイダンス

AWS 規範ガイダンス: SAP on AWS グリーンフィールド実装のベストプラクティス

Table of Contents

SAP on AWS グリーンフィールド実装のベストプラクティス

Almaz Thornton、Johnny Frye、Raveendra Voore、Amazon Web Services (AWS)

2024 年 7 月 (ドキュメント履歴)

SAP のグリーンフィールド導入は、SAP エンタープライズリソースプランニング (ERP) アプリケーションの新規導入を含め、大規模なビジネストランスフォーメーションの一環として行われるのが一般的です。アマゾン ウェブ サービス (AWS) の Greenfield SAP 実装は、 AWS 移行するオンプレミスまたはクラウドに既存のサーバーフットプリントがないため、移行時の SAP とは異なります。代わりに、新しいサーバーのサイズ設定とプロビジョニングが行われます。さらに、グリーンフィールドのプロジェクトの方が、技術面でも機能面でも対象範囲が広い傾向があります。グリーンフィールド導入は移行ほど多くは行われていないため、プロジェクトに適したガイドをすぐには見つけられないのが一般的です。

本ガイドでは、SAP のグリーンフィールド導入に携わっている IT リーダーやプロジェクトマネージャー向けの、推奨事項とベストプラクティスをご紹介します。こちらのガイドラインは SAP の移行プロジェクトにも関連しているため、移行やグリーンフィールド導入の管理に付随する障害を取り除くのに役立ちます。本ガイドラインは、移行または導入プロジェクトの主な 3 つの段階に基づき、3 つの章に分かれています。

- 計画段階 — 初回の計画立案、チームの編成、要件の収集を行います。
- 設計段階 — 要件をアーキテクチャダイアグラム、ビルド仕様書、設計文書に書き換えます。
- ビルド段階 — SAP グリーンフィールド導入の開発、設定、テストを行います。

このガイドでは、 AWS および SAP サービスに関する 100 レベルの知識、IT プロジェクト管理の深い知識、移行方法に関する SAP と AWS移行に関する AWS SAP HANA パターンの認識があることを前提としています。

概要

本ドキュメントでは、SAP on AWSグリーンフィールド導入で得た学びに焦点を当てます。これらの推奨事項のほとんどは、 AWS 移行プロジェクトの標準 SAP にも適用できます。この記事では、プロジェクトの計画、設計、構築の段階に関するアドバイスをご紹介します。メンテナンスとオペレーションの段階に関する解説も含まれていますが、これらの段階は、本ガイドの対象ではありません。ベストプラクティスを実際に活用するときは、ウォーターフォール型、反復型、アジャイル型、あるいはハイブリッドのアプローチを用います。

本ガイドで述べるインフラストラクチャーチームの主な利害関係者とは、以下を指します。

- AWS 実装パートナー – AWS プロフェッショナルサービスまたは AWS パートナーです。その役割は、SAP アプリケーションが実行される AWS インフラストラクチャを構築することです。
- SAP Basis チーム — このチームは、システムインテグレーター (SI) かベンダー企業から派遣されるか、社内の従業員で編成されるか、あるいはその両方の混合で編成されます。役割は、SAP ソフトウェアのインストール、技術レベルの設定、アップグレード、一般的なメンテナンスです。
- SI インフラストラクチャリーダー — 製品の所有者としての役割を果たす個人です。大規模なプロジェクトチームから要請された技術要件を提供したり、インフラストラクチャチームを主導したりします。
- 顧客インフラストラクチャリーダー — こちらも製品の所有者としての役割を果たす個人です。大規模なプロジェクトチームから要請された技術要件を提供したり、インフラストラクチャチームを主導したりします。SI インフラストラクチャリーダーと顧客インフラストラクチャリーダーは、共同リーダーシップモデルとして対等に機能させることができますが、指名するインフラストラクチャーリーダーを 1 人のみにすることもできます。

この規範ガイダンスは、特にグリーンフィールド SAP プロジェクトの AWS 側面に焦点を当てています。

SAP 環境を にデプロイする場合 AWS、通常、インフラストラクチャチームは、ビジネスニーズに合わせて SAP を設定およびカスタマイズする機能チームと開発チームより数か月先です。両チームはデリバリータイムラインが異なるため、インフラストラクチャチームの構築段階が、機能チームの計画段階の時期にあたるようなことがあります。加えて、SAP 環境の構築作業は繰り返しの多い反復作業です。例えば、N+2 のシナリオでは 3 つの開発環境を構築することになります。環境の完成期日がすべて同じ日付でない限り、構築段階は、プロジェクトの構成方法や環境が必要になる時期に応じて 3 つ作成することができます。本ガイダンスをご自身のプロジェクトの特定の段階に使用す

るときは、以上の差を念頭におくようにします。そうすれば、機能開発チームとより効果的にコミュニケーションを取り、協力することができるはずです。

対象者

このドキュメントは、プロジェクト実装のガイドとして、また SAP on 実装中に期待を設定し、強力な IT リーダーシップを提供するためのツールとして、プロジェクトマネージャーを念頭に置いて書かれています AWS 。大規模な SAP 導入では、インフラストラクチャチームのメンバー全員が、プロジェクトマネージャーと共に自らの仕事の管理に携わることになる可能性があります。クラウドジャー二ー全般を管理し、ベストプラクティスが順守されていることに対して説明責任を負う、インフラストラクチャの総合的なプロジェクトマネージャーを 1 名任命することが推奨されます。

計画段階のベストプラクティス

SAP グリーンフィールド導入の計画段階では、通常、プロジェクトの最中にさまざまな課題や機会が生じます。このセクションでは、 AWS プロフェッショナルサービスチームが関与した AWS グリーンフィールド実装に関する SAP に基づく 5 つの主要な学習について説明します。以下の推奨事項の中には、プロジェクトを開始する前やコンサルティングチームが参加する前でも、実践に生かせるものがあります。役割と責任を記したマトリックスや、チームの連絡先リストなどの文書の下書きは、計画立案のプロセスを迅速化するのに役立ちます。

RACI マトリックスを作成する

インフラストラクチャチームの役割分担を示すマトリックスの作成は、あらゆる導入プロジェクトに欠かせません。このマトリックスは、責任 (Responsible)、説明責任 (Accountable)、相談先 (Consulted)、報告先 (Informed) (RACI) を示した包括的な表です。RACI は、複雑なチーム構造の役割、割り当て、タスクを明確にするために使用されます。これは、 AWS SAP クラウドチーム、SAP Basis チーム、SAP システムインテグレーター (SI)、および顧客と協力して開発する必要があります。作成を主導するのはどのグループでも構いませんし、プロジェクトマネージャーが主導しても構いません。利害関係者から意見を求めることなく RACI を作成すると、矛盾やギャップ、ときには対立なども生じます。プロジェクトのすべての段階を考慮に入れることが重要です。事前に RACI を作成しておけば、関係者全員の連携を強化し、透明性を確保することができます。RACI は、プロジェクトの開始前に作成しておくのが理想的です。

以下は、SAP グリーンフィールド導入プロジェクトの、RACI マトリックスのサンプルから一部を抜粋したものです。

RACI マトリックスの完全版をダウンロード

Topic: Program Governance	SAP Basis	AWS Professional Services or AWS Partner	SAP Systems Integrator	Customer
AWS project management and governance	I	R	I	A
SAP AWS team staffing	C	R	C	A
Onboarding	I	I	I	RA
Access	I	I	I	RA
Engagement security	-	RA	-	I
Collaboration tools - access	I	I	I	RA
Financials	-	R	-	A
Status reportiing	I	RA	I	I
Program reporting	C	R	C	A
Advisory of AWS services for SAP throughout project phase	I	R	C	A
Topic: AWS Platform and Architecture				
Architecture of target AWS SAP environment, including HA/DR capabilities	I	R	C	A
Design of backup/restore strategies on AWS infrastructure	I	R	C	A
Provide host names and ports for SAP	R	C	I	A
Open firewall	C	I	I	R
AWS infrastructure design per SAP sizing requirements provided by Basis	C	R	C	A
Automating and provisioning of AWS infrastructure	I	R	C	A
Post-infrastructure build steps (e.g., request domain join)	I	R	I	A
Review of AWS infrastructure security	I	R	I	A
AWS infrastructure issues resolution before system handover to Basis	I	R	I	A
Project team infrastructure support, Level 1 (project team always goes through Basis; no direct contact to AWS)	R	C	I	A
AWS support ticket (involves TAM)	C	R	I	A
Identify HA relevant SAP application	C	I	R	A
AWS go-live check, including SAP AWS requirements - infrastructure	I	C	R	A
SAP cutover to production	I	C	R	A

SoW を確認する

AWS コンサルティングおよびアドバイザリーサービスの作業明細書 (SoW) のすべての要素を理解し、主要な利害関係者と SoW を共同でレビューして、成果物が全員に明確に理解されるようにします。インフラストラクチャチームが SoW で定義されている以上のことを行う場合は、リスク、前提、アクション、問題、依存関係、決定 (RAAIDD) ログにそのことを記録してください。グリーンフィールド SAP 実装プロジェクトでは、俊敏性と俊敏性を維持することが最も重要であるため、SoW からの逸脱は一般的なシナリオです。ただし、 AWS 実装パートナーが文書化されている範囲を超えて提供を開始した場合、期待が不明瞭になる可能性があります。変更が生じた場合は、新しい作業範囲とそれによって生じる可能性のあるトレードオフとを記した最新のリストを作成しておく必要があります。ウォーターフォール型のプロジェクトでは、作業範囲の変更管理プロセスを規定し実行に移すことが不可欠です。アジャイル型のプロジェクトでは、作業範囲の管理にはバックログの優先順位付けプロセスの方が適しています。

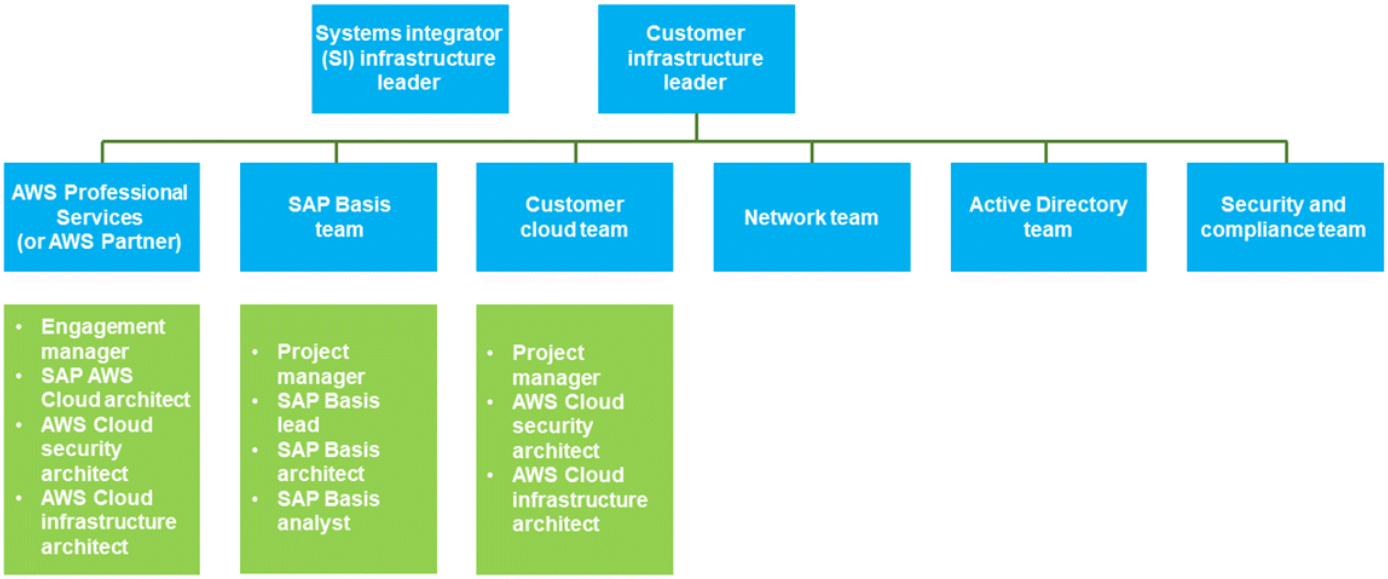
考慮事項:

- プロジェクトの進行中は最新の作業範囲を把握し、新しい成果物があれば明記します。そうすることで、予測事項を管理でき、バックログの優先付けを行う際は支援を求めることができます。
- ドキュメントの変更やタスクを既存のデリバリーのバックログと共に特定して優先付けすれば、ドキュメントをプロジェクトの終了時まで遅らせることなく、期間中随時作成することができます。
- プロジェクト全体で定期的な SoW ウォークスルーを実施して、成果物と優先順位の整合性を維持します。
- 本番稼働カットオーバーでは、ハイパーケアのサポートに役立つように、少なくとも 12 か月前に読み取り専用アクセスが承認された SoW があることを確認してください。

チームの組織図と連絡先リストを作成する

チームとリーダーシップ構造とを示す、組織の概略図を作成します。さらに掘り下げるときは、インフラストラクチャチームのメンバーと、各種機能 (セキュリティ、ネットワークとファイアウォールのオペレーション、Microsoft Active Directory、インハウスのクラウドオペレーション、サーバーオペレーションなど) の主要連絡先を含めた全員の氏名、肩書、役割が載ったチーム横断的な連絡先リストを作成します。誰がどのような役割でそのプロジェクトに関わっているのかを、全員が把握している必要があります。チーム内でこうした情報が共有されていないと、遅延や誤解が起きることは避けられないためです。また、利害関係者の肩書きを把握しておくことも同様に重要です。例えば、設計の分科会や日々の簡単な打ち合わせに、話し合いの主要メンバーでもない限りディレクターレベルの利害関係者を招こうと考える人はいないはずです。肩書や役割を把握していれば、適切な人物を関連する会合に呼ぶことができます。組織図を使ってチームが視覚化されていると、チーム内の構造を理解したうえで、プロジェクトに共に取り組むことができます。

次の図は、一般的な SAP on AWS インフラストラクチャの組織図の例を示しています。



インハウスのクラウドチームのエンゲージメントモデルを作成する

IT 組織に社内 AWS クラウドチームがある場合は、そのチームとエンゲージメントモデルを確立し、AWS 実装パートナー (AWS Professional Services や AWS Partner など) が実行する作業と比較して、そのチームが実行する作業を明確にする必要があります。考慮すべき主な役割の 1 つに、チームが構築して引き渡した環境に対するサポートがあります。例えば、数十の AWS SAP アプリケーション用にマルチランドスケープインフラストラクチャとマルチ環境インフラストラクチャを構築している SAP クラウドアーキテクトが 2 人しかいない場合、新しい環境の構築と構築を同時に完了する環境をサポートする帯域幅はありません。その場合は、完成後の環境のサポートをインハウスのクラウドチームに引き継いでもらうことが 1 つの方法となります。そうすれば、インハウスのチームはその環境を理解し、環境の責任を負う機会が得られます。プロジェクトが進行し、新しい作業範囲が決まれば、チームは最終的にその環境のメンテナンスと拡張に対する責任を負うことになります。

社内のクラウドインフラストラクチャとクラウド DevOps チームは、使用するオートメーションソフトウェアの種類についても合意する必要があります。例えば、 AWS CloudFormation または Terraform をコードとしてのインフラストラクチャ (IaC) ツールとして使用するかどうかなどです。同様に、ブートストラップボリュームや SAP インストールなどの設定タスクに AWS Systems Manager または Ansible を使用することに決める場合もあります。このような決定事項は文書に記録しておきます。さらに、サードパーティーのモニタリングとオブザーバビリティダッシュボードの要件があるが、これは SoW の成果物ではない場合は、その間に Amazon CloudWatch と Amazon Simple Notification Service (Amazon SNS) を使用してモニタリングと口グ記録フックを配置するこ

とを検討してください。インハウスのクラウドチームは、サードパーティーのモニタリングソリューションの統合を後から実行することができます。

エンゲージメントモデルまたはサポート契約も RACI マトリックスの一部であり、SoW で説明されている必要があります。 AWS サービスを使用することで達成できる自動化にはかなりのレベルがあります。SoW と RACI マトリックスは、グリーンフィールド SAP 実装プロジェクトの一環として達成する必要があるものと、運用チームに委任できるものを特定する必要があります。

エンゲージメントモデルを確立するときは、ウォーターフォール、アジャイル、または混合アプローチが前進するための主要な方法かどうかを判断する必要があります。 AWS プロフェッショナルサービスでは、ウォーターフォールアプローチと比較して、アジャイルまたは混合アプローチを実装したエンゲージメントのタスク完了が 300% 増加し、計画時間が 94% 短縮されました。計画段階では、顧客の助けを借りてコミュニケーション計画とツールアプローチを選択する必要があります。次の表は、コミュニケーションプランの例を示しています。

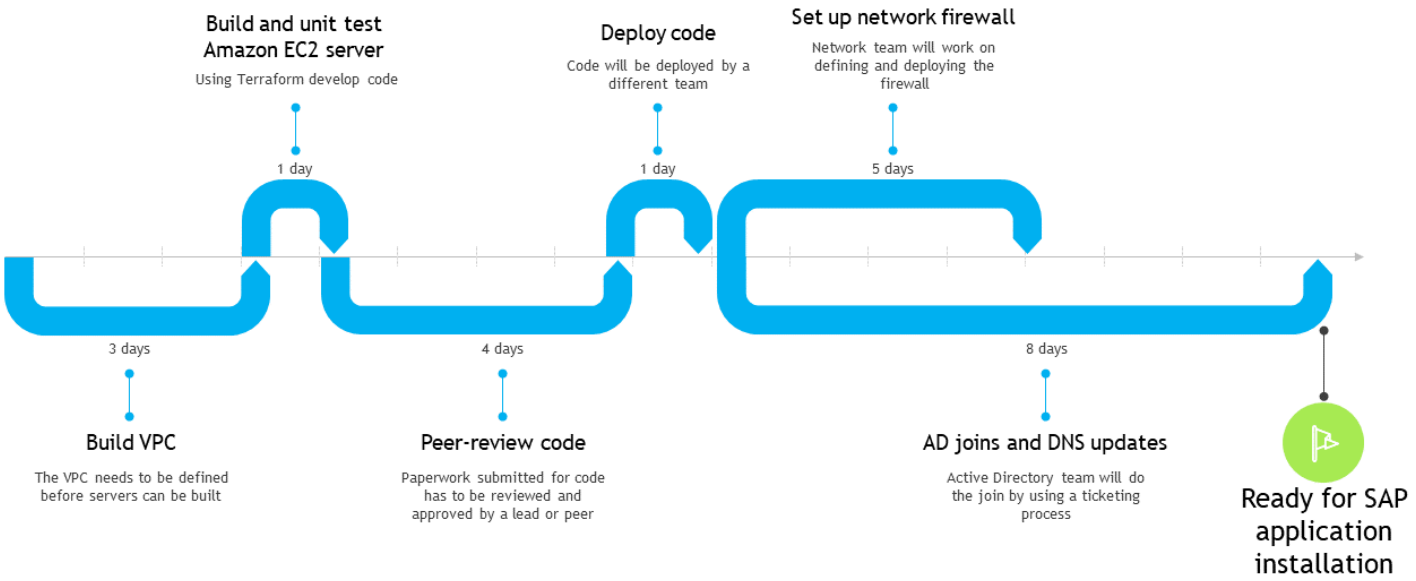
Communication plan

Meeting	Duration	Frequency	Notes	Deliverables	Stakeholders
Scrum meetings (for each workstream)	15–30 minutes	Daily or twice weekly	Daily: Monday – Friday Twice weekly: Monday, Thursday	• What did I do yesterday to advance the sprint goal? • What will I do today to advance the sprint goal? • Are there any impediments that will prevent us from meeting the sprint goal?	All project team members are invited
Internal scrum meeting	15–30 minutes	Weekly	Tuesday	• Like scrum but internal only	Internal scrum team
Sprint review and retrospective	1.5 hours	Every 3 weeks on Fridays	Fridays at 9:00 AM PST	• Review sprint goals. • Demo and solicit feedback for each story. • Discuss stories not completed and identify the blockers. • Identify risks and impediments. Revise team backlog.	All project team members are invited
Sprint planning and backlog grooming	1.0 hours	Every 3 weeks on Mondays after review	Mondays at 1:00PM PST		All project team members are invited
Leadership status meeting	30 minutes	Weekly	Thursdays at 1:00PM PST	• Meet with customer champion	EM/customer champion
Internal account team and AWS Professional Services calls	30 minutes	Bi-weekly	Fridays at 1:00PM PST	• CSM to make agenda or team members to bring agenda items/concerns	Account team and AWS Professional Services team
External account team, AWS Professional Services, and customer	1 hour	Bi-weekly	Dependent on customer	• Discuss budget, issues, accomplishment, goals.	Account team, AWS Professional Services team, customer leadership
Quarterly business review	1–2 hours	Quarterly	Dependent on customer	• Discuss high-level accomplishments and milestones	Account team, AWS Professional Services team, customer executive leadership

最後に、プロジェクトを早期にサポートする顧客と SAP Basis チームを特定してください。新しいソリューションを実装および移行する際のトレーニングは、ナレッジ転送セッションを早期に開始するために重要です。

クラウドの構築およびデプロイのプロセスを記録する

自社の IT 組織にインハウスのクラウドチームがあるときは、そのチームがフロー図 (ダイアグラム) を使ってクラウドの構築とデプロイのプロセスを記録し、チーム全体にこの図を配布します。主要な利害関係者が、プロセス内の障害や非効率な要素をすぐに特定し、既存の内部プロセスが、非効率性や遅延の発生に関してどのような役割を果たしているのかを把握できるようにします。以下の例では、Active Directory の参加 (join) とドメインネームシステム (DNS) の更新 (update) のプロセスに、完了まで最も長い時間がかかっていることがわかります。このようなビジュアルがあれば、プロセス内の特定のステップにかかる時間をどうすれば短縮できるかといった問題を、チームが協力して解決する際のモチベーションになります。

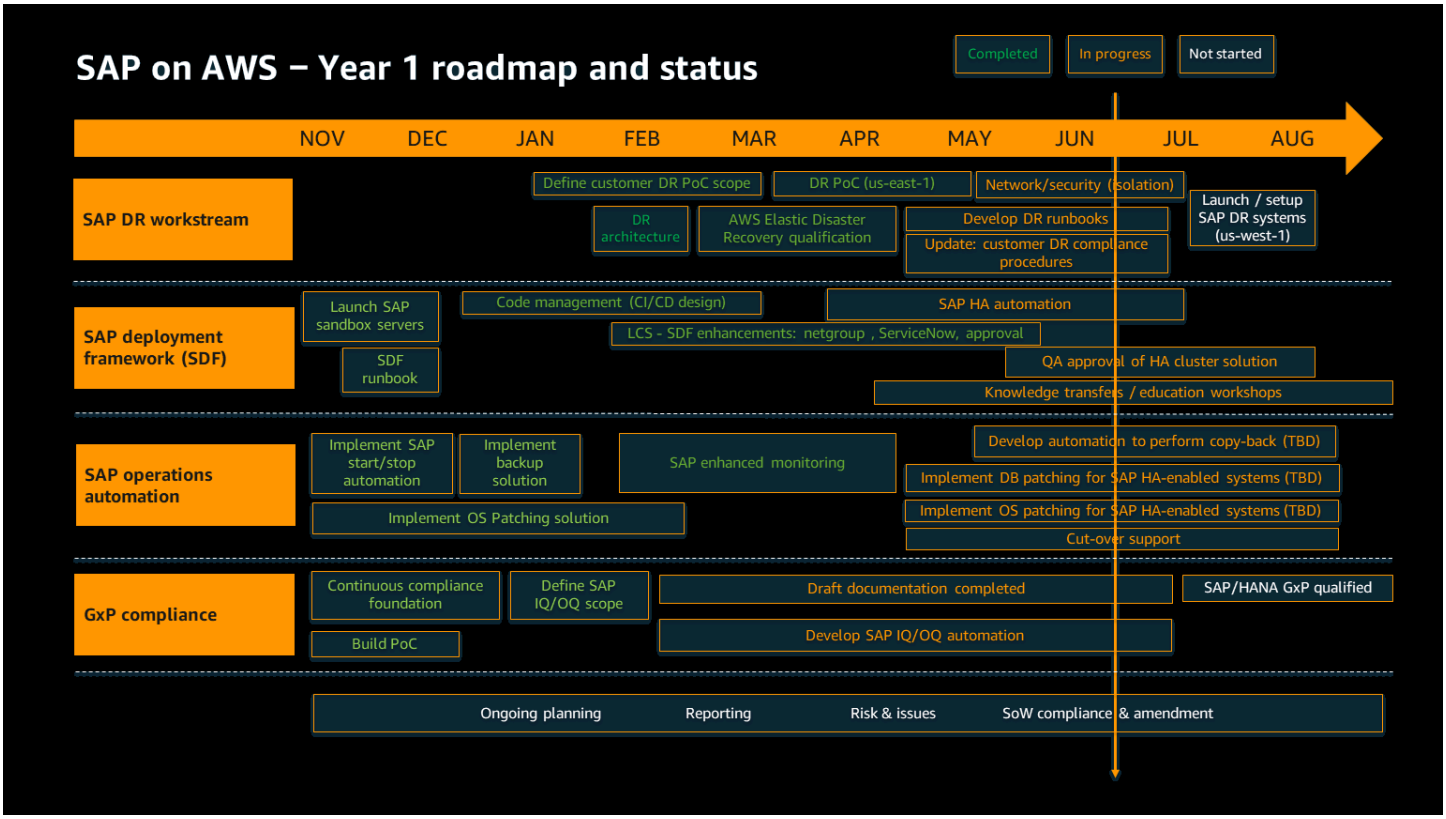


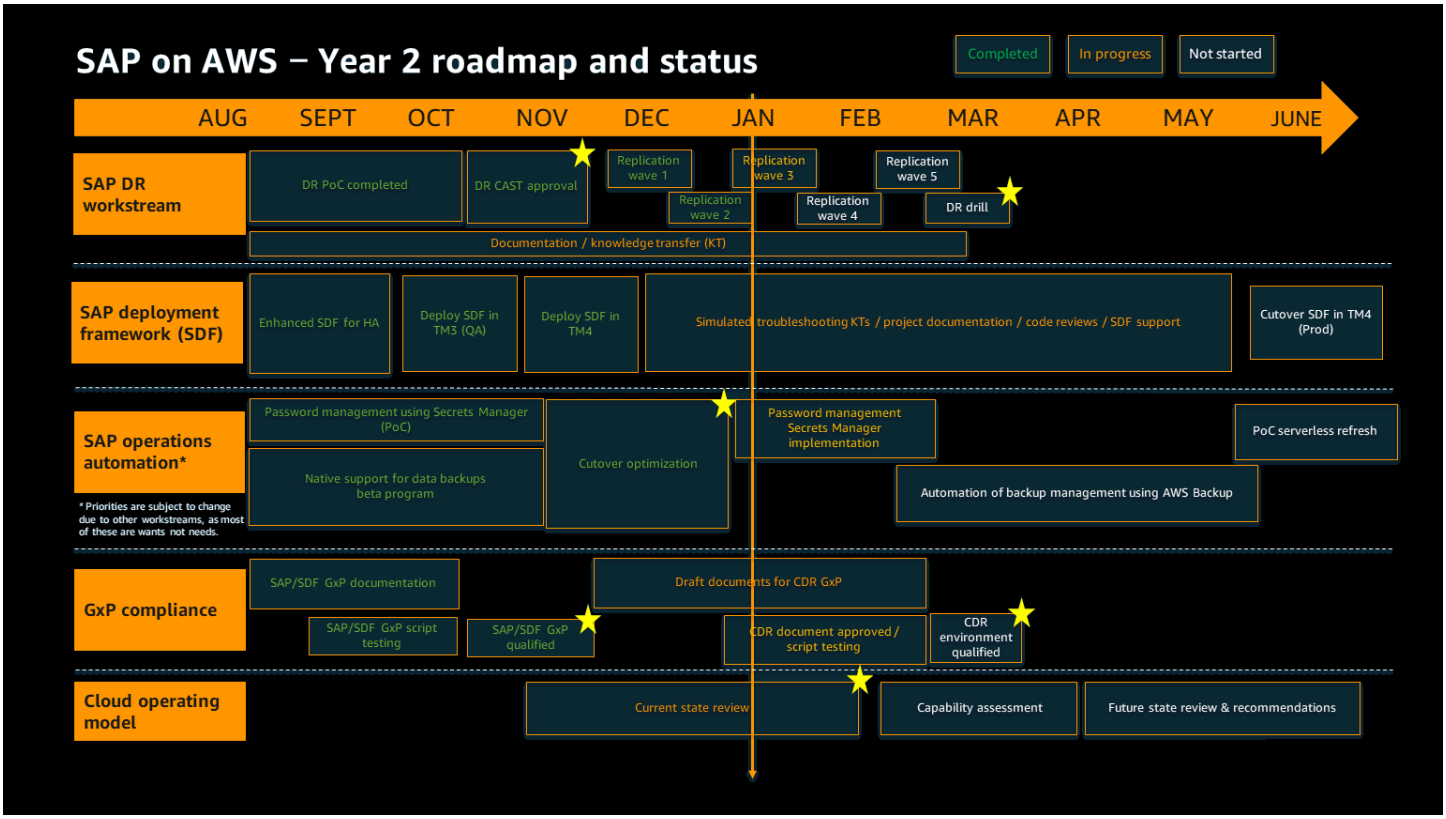
考慮事項:

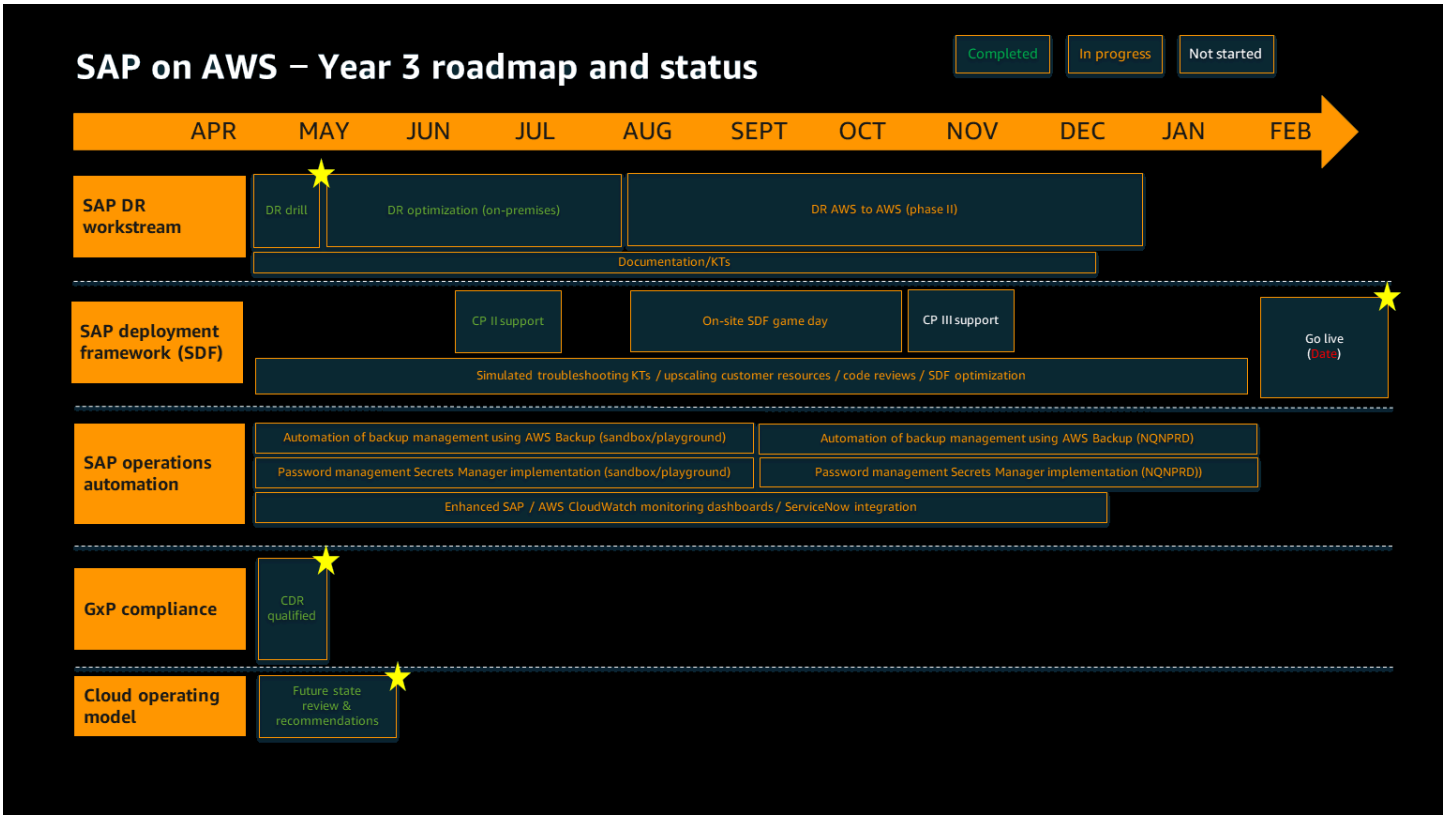
- ヘルプデスクのプロセスとワークフローとを分けて記録し、この情報をインフラストラクチャチームに配布して、1 人の担当者に頼らなくても済むよう、全員がヘルプデスクツールにアクセスできるようにします。Active Directory の参加、DNS の更新、ファイアウォールの開放、暗号化キーのリクエストを行う場合、複雑で時間のかかるチケットプロセスが発生することがよくあります。プロジェクトの計画段階で、これらのプロセスを記録し、各チームのサービスレベルアグリーメント (SLA) を検討することが重要です。これは、削除する際に特に注意が必要な、遅延や障害の理由を説明するときにも役立ちます。
- Active Directory とファイアウォール、またはネットワークタスクに、指定された連絡先を割り当てます。これらの専用リソースは、プロジェクトに含める必要があります。サービスチケットに頼らねばならない場合は、サービス SLA を管理することはできません。

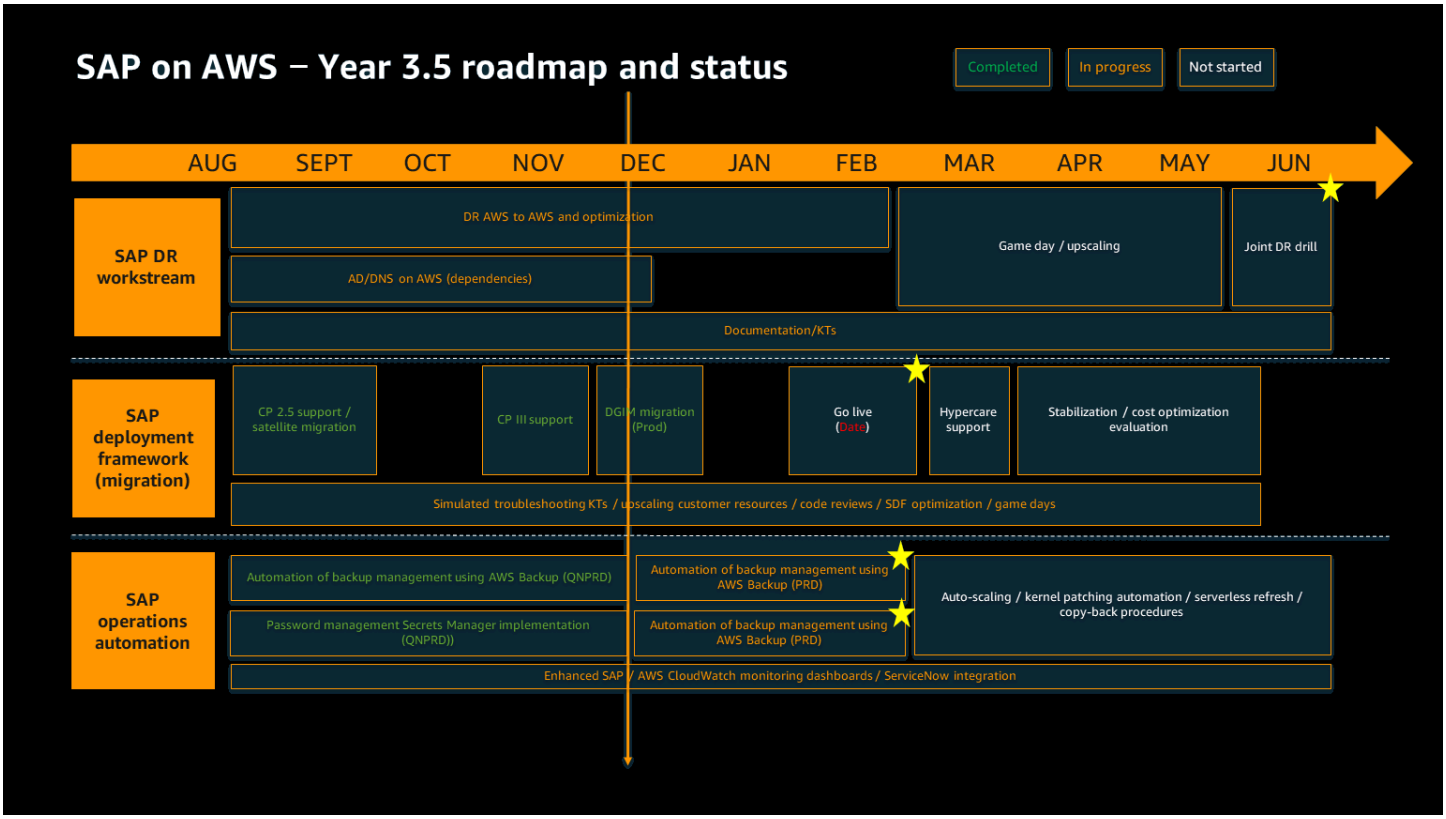
プロジェクトロードマップとマイルストーントラッカー

次のグラフは、複数年にわたる SAP on AWS グリーンフィールドプロジェクトのロードマップの例を示しています。

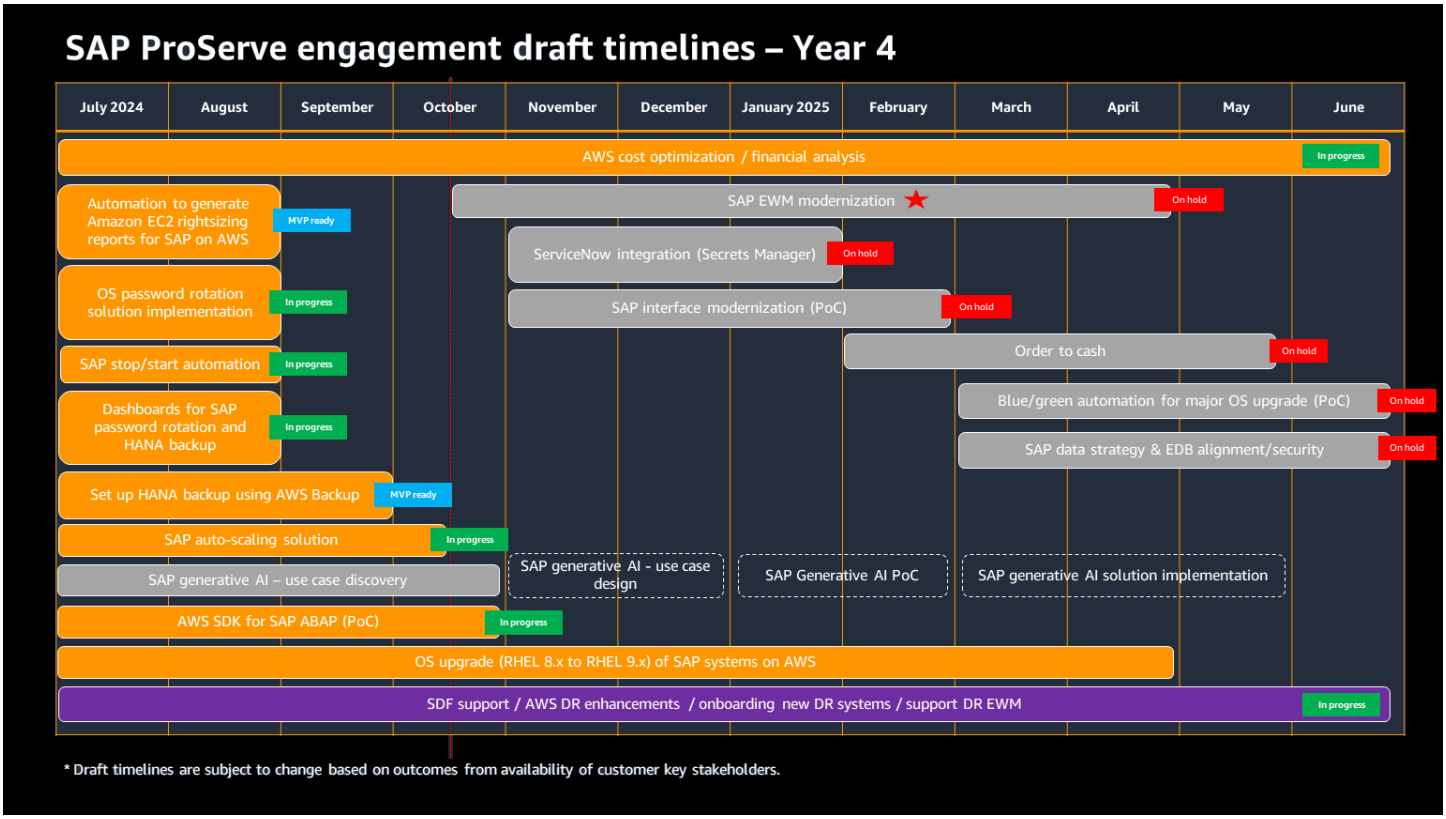



SAP on AWS – Year 2 roadmap and status
Completed
In progress
Not started
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
MAR
APR
MAY
JUNE
SAP DR workstream
DR PoC completed
DR CAST approval
Replication wave 1
Replication wave 2
Replication wave 3
Replication wave 4
Replication wave 5
DR drill
Documentation / knowledge transfer (KT)
SAP deployment framework (SDF)
Enhanced SDF for HA
Deploy SDF in TM3 (QA)
Deploy SDF in TM4
Simulated troubleshooting KTs / project documentation / code reviews / SDF support
Cutover SDF in TM4 (Prod)
SAP operations automation*
Password management using Secrets Manager (PoC)
Native support for data backups beta program
Cutover optimization
Password management Secrets Manager implementation
PoC serverless refresh
Automation of backup management using AWS Backup
* Priorities are subject to change due to other workstreams, as most of these are wants not needs.
GxP compliance
SAP/SDF GxP documentation
SAP/SDF GxP script testing
SAP/SDF GxP qualified
Draft documents for CDR GxP
CDR document approved / script testing
CDR environment qualified
Cloud operating model
Current state review
Capability assessment
Future state review & recommendations


SAP on AWS – Year 3 roadmap and status
Completed
In progress
Not started
APR
MAY
JUN
JUL
AUG
SEPT
OCT
NOV
DEC
JAN
FEB
SAP DR workstream
DR drill
DR optimization (on-premises)
DR AWS to AWS (phase II)
Documentation/KTs
SAP deployment framework (SDF)
CP II support
On-site SDF game day
CP III support
Go live (Date)
Simulated troubleshooting KTs / upscaling customer resources / code reviews / SDF optimization
SAP operations automation
Automation of backup management using AWS Backup (sandbox/playground)
Automation of backup management using AWS Backup (NQNPRD)
Password management Secrets Manager implementation (sandbox/playground)
Password management Secrets Manager implementation (NQNPRD))
Enhanced SAP / AWS CloudWatch monitoring dashboards / ServiceNow integration
GxP compliance
CDR qualified
Cloud operating model
Future state review & recommendations



次の図は、同じプロジェクトの AWS プロフェッショナルサービスとのエンゲージメントタイムラインの例を示しています。



次の図は、このプロジェクトの本番稼働用マイルストーントラッカーを示しています。

Go-live milestone tracker

Milestone	Projected start	Projected end	Start	End	Notes
Shutdown	Day 1 – 6 PM	Day 1 – 8:30 PM			
Snapshot	Day 1 – 8:30 PM	Day 1 – 10:30 PM			
Pre-data migration	Day 1 – 10:30 PM	Day 1 – 12 AM			
Data migration (go/no-go #1)	Day 2 – 12 AM	Day 2 – 10 PM			
Data verification (go/no-go #2)	Day 3 – 12 AM	Day 3 – 10 AM			
Basis OV	Day 3 – 5 PM	Day 3 – 11 PM			
Function OV	Day 3 – 5 PM	Day 3 – 11 PM			
Production (go/no-go #3)	Day 3 – 11 PM	Day 3 – 11:30 PM			

設計段階のベストプラクティス

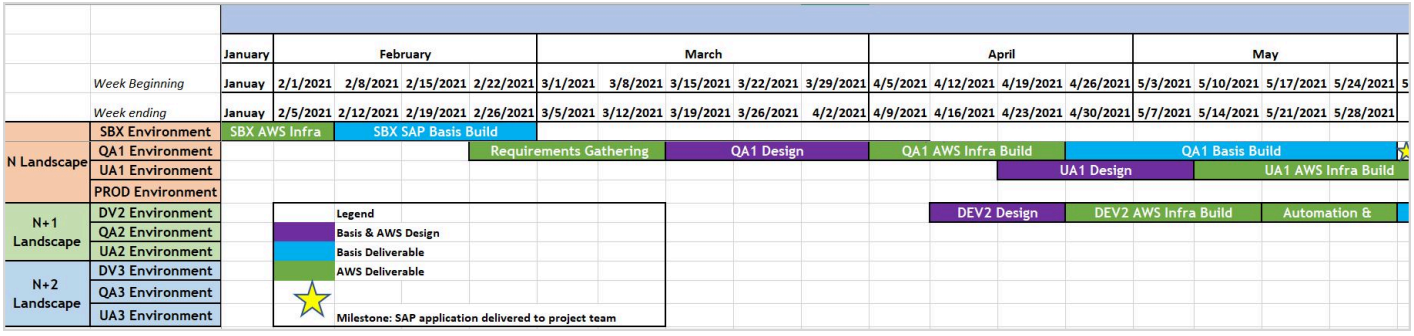
SAP グリーンフィールド導入の設計段階は、構築段階を成功に導くための基礎となる部分です。この段階では、インフラストラクチャの利害関係者と協力してさまざまな要件を収集し、アーキテクチャを文書に記録します。検討しなければならない調整事項は他にもあります。プロジェクトの各利害関係者が、タイムライン、ランドスケープ戦略、そして、高可用性 (HA) 環境およびディザスタリカバリ (DR) 環境を含めた SAP on AWS のアーキテクチャに合意していることを確認する必要があります。こちらのセクションでは、プロジェクトの設計段階で生じやすい課題への、推奨される対処方法について説明します。

デリバリーのタイムラインとランドスケープのダイアグラムを作成する

ビジネストランスフォーメーションプロジェクトのタイムラインを受け取ったら、すぐにインフラストラクチャのデリバリータイムラインを作成します。すぐに作成すれば、前もって計画を立て、インフラストラクチャチームの内部で意見を調整することができます。タイムラインを作成するための主な情報は、SAP プロジェクトチームのシステムインテグレーター (SI) から入手します。SAP Basis チームが作業を完了すべき日付と、同チームが SAP アプリケーションをインストールするため、インフラストラクチャの準備を完了しておくべき日付を逆算して算出します。

考慮事項:

- デリバリータイムラインを視覚的に表示すれば、チームは、現在は何を構築しているか、その期日はいつか、どのようなリソースの競合があり得るかを一目で把握できます。また、主要な利害関係者は、構築中の環境、プロジェクトの期間、 と AWS SAP Basis チーム間の引き渡しを、理解しやすい方法で視覚化できます。

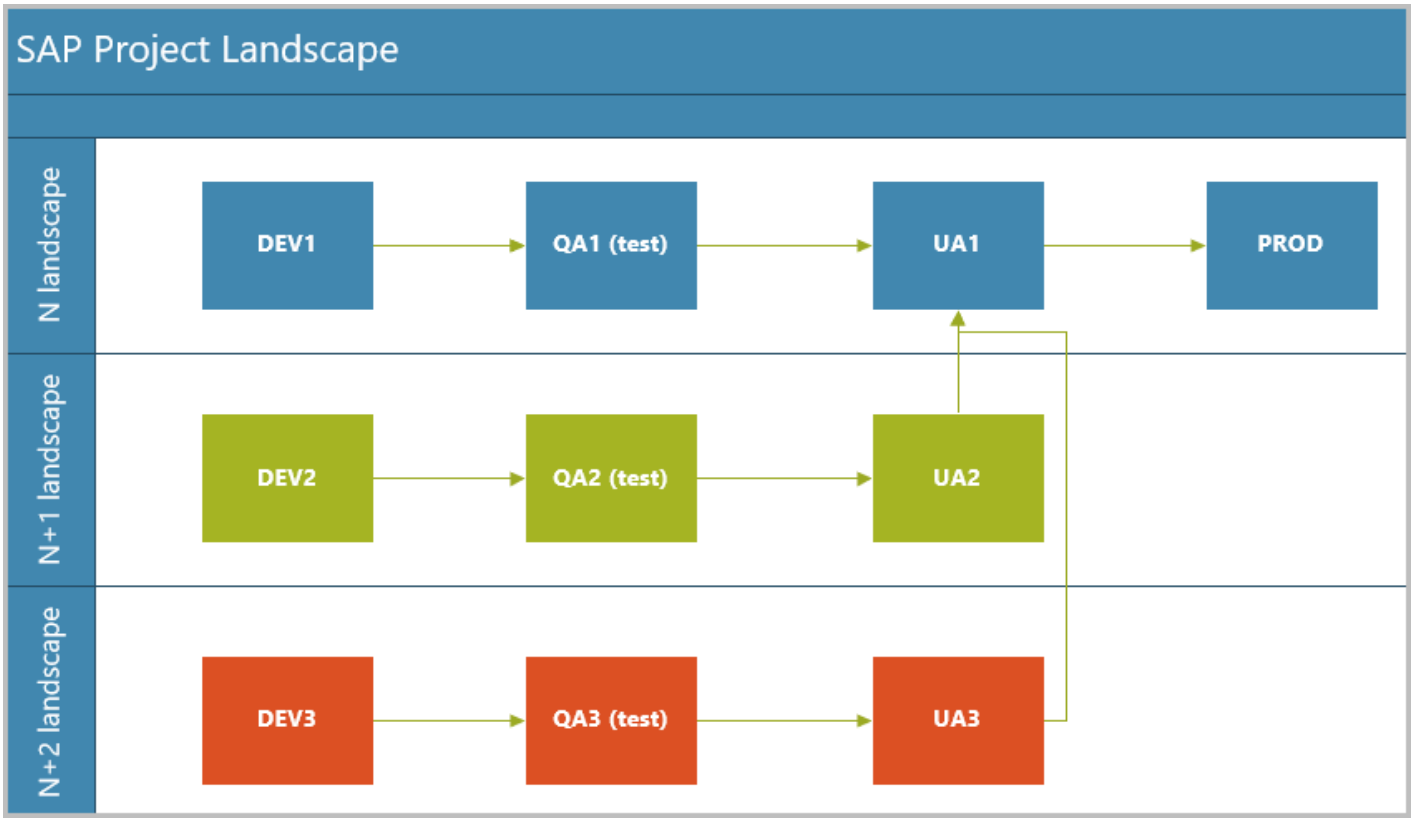


- SAP グリーンフィールド導入の一般的な所要期間は 1 年間かそれ以上にわたります。この期間には、インフラストラクチャチームがインフラストラクチャコンポーネントを活発に作成しない時期

も含まれます。したがって、その時期のアクティビティと成果物を考慮に入れておく必要があります。マップすべきアクティビティには、HA の設定とテスト、DR の設定とテスト、パフォーマンスのテスト、自動化スクリプトの作成などがあります。

- グリーンフィールド導入では、ランドスケープと環境を把握する際に混乱することがあります。環境とランドスケープ (N、N+1、N+2) とを区別して色分けしたタイムラインを使えば、利害関係者も情報のマトリックスをすぐに理解することができます。

  こちらは、SAP のランドスケープを概略的に示したダイアグラムのサンプルです。各ボックスは環境を表します。環境はアプリケーション (SAP S/4HANA など) の集合です。ランドスケープは特定のリリースに使用される環境の集合です。



- ロードマップを作成するときは、高レベルのロードマップを再検討し、チームが確立されるまで四半期ごとに長期計画を行うことをお勧めします。移行に加えて、クラウドセンターオブエクセレンス (CCoE) のワークストリーム、運用の自動化、セキュリティとコンプライアンス、クラウドディザスタリカバリなどの他のロードマップ項目を含めます。

リージョンのサービスを把握し決定事項を記録する

設計フェーズの開始時に、プライマリリージョンを正しく選択 AWS リージョン できるように、特定の で利用できるサービスを理解し、話し合う時間を取ることをお勧めします。特に SAP では高性

能なインスタンスが必要になることが多いため、そのためのリソースがプライマリリージョンまたはセカンダリージョンで利用できることを確認しておかねばなりません。インスタンスタイプは、SAP アプリケーションで認定されているものを選びます。選択した AWS リージョン でそのインスタンスタイプを使用できることを確認します。instance-type-offerings のAWS Command Line Interface (AWS CLI) コマンドを使用すれば、すばやく簡単に確認できます。導入に使用するリージョンで現時点でサービスを利用できない場合は、そのリージョンでインフラストラクチャをオーダーするのに要する時間を考慮に入れいます。

リージョン関連の決定事項は、確認および再確認して記録します。この決定事項は、より規模の大きいプロジェクトチームに回覧して主要な利害関係者に情報が行き渡るようにします。プロジェクトにアーキテクチャ検証委員会がある場合は、決定が確定する前に事項を提起し、委員全員が意見を述べられるようにします。

考慮事項:

- 重要な考慮事項の 1 つが、SAP と統合する境界システムです。境界または衛星アプリケーションをホストしている場合は AWS、レイテンシーに関する不要な議論を防ぐために、同じプライマリリージョンで SAP をホストすることをお勧めします。レイテンシーに問題がないことを確認できたとしても、境界アプリケーションを SAP アプリケーションとは異なるリージョンに構築する理由を利害関係者に説明するのは簡単なことではありません。
- ディザスタリカバリ (DR) のサイトも、DR のテストを実際に即して調整できるよう、SAP や SAP と統合するシステムと同じ場所にする必要があります。システムごとに異なるソリューションが必要になる場合があります。例えば、BusinessObjects や Winshuttle などの大規模な SAP システムは で動作せず AWS Elastic Disaster Recovery 、Amazon Relational Database Service (Amazon RDS) データベースを使用する別のソリューションが必要になる場合があります。

命名規則を作成する

ホスト、SAP 環境、Virtual Private Cloud (VPC)、 AWS およびアカウントの命名規則を徹底的に検証し、文書化します。既存の基準または規則には必ず従います。グリーンフィールド導入では、命名規則はおそらく一から定義しなければならないはずです。必ず整合性を保ちましょう。例えば、VPC Pre-Prod、SAP 環境 UAT、および AWS アカウント TST を呼び出す場合、サポートの観点からこれら 3 つの名前を関連付けるのは困難です。必ず合意を得た上で、それぞれの文字が意味を持つように、ただし柔軟性の余地は残して、名前を付けます。例えば、将来別のリージョンに切り替えなければならなくなった場合に備えて、リージョン名をサーバー名に書き込むことは避けます。オンプレミスサーバーに使用している命名規則は使用しません。代わりに、自分の組織でまだ使用したことがなければ、クラウドの柔軟な命名規則を使用することが推奨されます。

考慮事項:

- 変更の可能性がある情報には AWS タグを使用します。
- 非本番環境を本番用 VPC の中に置くことはできません。置くことが要件になっている場合は、妥当な理由があることを確認してから承諾します。

決定事項はすべて記録する

決定事項は、すべての変更履歴、決定を下した人、決定した日付、決定に立ち会った人を詳細に記録しておくことが推奨されます。決定事項は、Atlassian Confluence やスプレッドシートなど公開されている場所に保管し、適切に承認されるようにします。利害関係者やチームメンバーが、すでに合意済みであることを忘れて、設計や構築の段階に入ってから決定事項に異議を唱えるような場合があります。そうした場合に備え、異議に対処できるようデータをすぐに取り出せるようにしておくことが推奨されます。記録しておくべき決定事項には、以下のようなものがあります。

- リージョンの決定
- HA 関連のアプリケーション
- ディザスタリカバリの決定事項
- プロジェクト段階の環境支援モデル
- バックアップと復元の方法およびツール
- VPC の構造
- AWS アカウントの決定
- セキュリティに関する決定事項

さらに、すべての製品機能のリクエストを追跡し、チームが変更を実装するのにかかった時間を文書化します。

構築フェーズのベストプラクティス

このセクションでの推奨事項は、プロジェクトの構築フェーズを円滑に進めるのに役立ちます。構築フェーズには、コード、開発、デプロイ、実装のアクティビティが含まれ、多くの場合、設計レビューと承認セッション、そして構築内容、タイムライン、終了の基準について認識を合わせるためのキックオフミーティングで構成されています。これは、コードが記述され、ピアレビューされ、すべての AWS サービスにデプロイされるフェーズです。

以下の推奨事項では、テストや検証アクティビティも含まれます。

スタンドアップミーティングを毎日開催する

どのプロジェクト方法論を使っていたとしても、必ず毎日スタンドアップミーティングを開催してください。毎日のスタンドアップミーティングはアジャイル手法と関連していますが、ウォーターフォールモデルなど他の方法論でもチームをつなぐメカニズムとして非常に役立ちます。さまざまな方法論のベストプラクティスを取り入れたハイブリッドなプロジェクトフレームワークを使用することもできます。

考慮事項:

- Jira ボードのような軽量なものを使って、あらゆるタスクのストーリーを作成します。これらのボードは、毎日のスタンドアップミーティングのガイドになります。チームに余力と専門知識があれば、Scaled Agile Framework (SAFe) の手法を使用してエピックを作成することもできます。しかし、ほとんどのインフラストラクチャチームは、複雑なスクラムボードを管理することによる管理上のオーバーヘッドは望んでいないため、軽量なツールをお勧めします。また、ボードがあれば、チームが行う作業に関するレポートを作成でき、スコープを制御するメカニズムも得ることができます。
- グリーンフィールドの SAP プロジェクトでは、スコープがロックされた後に多くの SAP アプリケーション、または境界アプリケーションが追加されることは珍しくありません。プロジェクト範囲の制御、優先順位付け、可視化するための適切なメカニズムがなければ、プロジェクトを順調に進めるためのリソースの追加要求や作業の優先順位の変更が困難になります。

統一されたビルド仕様書を使用する

すべての環境とランドスケープに対して 1 つのビルド仕様スプレッドシートを使います。こうすることで、簡単に配置、検索できる単一のドキュメントを作成することができます。問題が発生したら

簡単に復旧できるよう、バージョン管理を有効にすることをお勧めします。SAP Basis チームと協力してフォーマットを作成します。Basis チームは SAP システムに関する詳細情報を常に把握し、仕様を 1 つにまとめることで、社内のクラウドチームがプロジェクト完了後すぐにオーナーシップを取って、すべてのメタデータを 1 か所で確認できるようになります。

サーバー要件の 1 つのサンプルとして、サーバー構築の主要なメタデータを取得するのに使用するテンプレートの例を次に示します。

Landscape	Environment	SAP SID	Application Name	Application ID	Instance Role / Component	Hostname (AWS)	Domain Name	User-Friendly Hostname (CNAME)	IP Address	HA Cluster (Yes/No)	OS Type	OS	Build Status
N	DV1	DS4	SAP S/4 HANA	S4H	ASCS/ERS Server	AWSS4HDV101	xx.xxxx.com	SAPS4.xx.xxxx.com	12.345.678.901	Yes	RHEL	Red Hat Enterprise Linux for SAP	AD Join in progress

AWS サービスクォータに注意する

Amazon Elastic Compute Cloud (Amazon EC2) インスタンスにプロビジョニングできる仮想 CPU (vCPUs) の数にはクォータがあります。EC2 インスタンスをデプロイする場合、EC2 インスタンスのタイプによって一定数の vCPU が必要です。すべての AWS アカウントには、プロビジョニングできる vCPUsの数にソフト制限があります。EC2 インスタンスをデプロイすると、ソフト制限は約 100 ~ 150 vCPUs ずつ自動的に増加します。ただし、複数の EC2 インスタンス (例えば 20 個) を同時にデプロイしようとすると、ソフト制限を超える可能性があります。この制限にかかる可能性がある場合は、EC2 インスタンスをデプロイする前に、クォータを引き上げるリクエストを送信してください。デプロイの途中で Service Quotas の制限に達するのを防ぐことができます。

セキュリティのためのキーローテーション戦略を策定する

AWS Key Management Service (AWS KMS) を使用すると、お客様は暗号化キーを簡単に作成および管理し、さまざまな AWS のサービスやさまざまなアプリケーションでの使用を制御できます。SAP 実装の場合、 AWS KMS キーは Amazon Elastic Block Store (Amazon EBS) ボリュームに保存され、SAP バイナリおよび SAP HANA ファイルシステムに使用される保管中のデータを暗号化するために使用されます。KMS キーは、ソフトウェアメディアとバックアップを保持するために Amazon Simple Storage Service (Amazon S3) バケットに保存されているデータ、および `/usr/sap/trans`および の Amazon Elastic File System (Amazon EFS) ファイルシステムに保存されているデータにも使用されます`/sapmnt`。 AWS KMS を使用すると、 AWS マネージドキーまたはカスタマーマネージドキーのいずれかを柔軟に使用できます。構築フェーズの開始時に、セキュリティキーの管理戦略と決定事項を文書化して共有することをお勧めします。カスタマーマネージドキーから AWS マネージドキーへの切り替えなど、プロジェクトの途中でセキュリティポリシーを変更する場合は、SAP 環境を完全に再構築する必要があり、プロジェクトのタイムラインに影響を与える可能性があります。

キーの使用とローテーションについて、すべてのセキュリティ関係者から同意を得てください。クラウドまたはオンプレミス環境向けの既存のキーローテーションポリシーを検討し、 AWSで使用できるようにこれらのポリシーを変更します。キー管理の戦略についてコンセンサスを得ることが難しい場合は、意思決定者にセキュリティのベースラインとレベル設定に関する考慮事項を理解してもらうためのトレーニングを実施してください。環境を構築する前に、キーローテーションに関する決定を下すことが重要です。例えば、カスタマーマネージドキーから AWS マネージドキーに変更する場合、Amazon EBS で問題が発生し、暗号化キーをオンラインで変更することはできません。EBS ボリュームは、新しいキーを使って再構築しなければなりません。そのため、SAP インスタンスを再構築する必要がありますが、これは理想的なシナリオではありません。

同様に、プロジェクトで Vormetric などの外部キー管理ソリューションを使用し、キーマテリアルを にインポートする場合は AWS KMS、セキュリティの意思決定者が外部 KMS キーと AWS KMS キーのキーローテーションの違い (自動ローテーション) を認識していることを確認してください。セキュリティポリシーに従って外部 KMS キーを使用し、ローテーションすると、キーマテリアルだけでなく、キーの Amazon リソースネーム (ARN) も変更されます。つまり、EBS ボリュームを再作成する必要があり、SAP システム全体を小規模に移行させる必要があります。一方、 でカスタマーマネージドキーまたは AWS マネージドキーの自動ローテーションを有効にすると AWS KMS、キーマテリアルは変更されますが、キー ARN は変わりません。つまり、EBS ボリュームは影響を受けません。キーローテーションの詳細については、 AWS KMS ドキュメントの「キーのローテーション AWS KMS」を参照してください。

もう 1 つのセキュリティアプローチは、データベースとオペレーティングシステムのパスワードローテーション AWS Secrets Manager に を使用することです。これは、標準ダッシュボードから入手できます。さらに、悪意のあるアクティビティから環境を保護するために、ディザスタリカバリ環境の AWS Identity and Access Management (IAM) ロールが本番環境から分離されていることを確認してください。

未使用サーバーの廃止

有用性がなくなった直後に概念実証 (PoC) サーバーを廃止することをお勧めします。使用していないサーバーを稼働させると、コストがかかる可能性があります。グリーンフィールドの SAP 実装のために構築したすべてのサーバーを把握し、構築フェーズであまり使用されていないサーバーは停止して廃止することが重要です。サーバーを廃止する前に、EC2 インスタンスの Amazon マシンイメージ (AMI) バックアップを作成することができます。そうすることで、今後まったく同じサーバーを起動する必要が生じた場合に、バックアップを復元することができます。

サーバーの廃止は、実装プロジェクトの終了まで先延ばしにするべきではありません。プロジェクトの全期間と、実装完了後のメンテナンスフェーズまたは運用フェーズにおいても、使用されていない

サーバーの使用状況を監視し、停止し、最終的には破棄する必要があります。料金はすぐに蓄積されるため、SAP Basis チームメンバーにこれらのサーバーの廃止を教えるプロセスを最初に設定してください。

リソース

リファレンス

- AWS KMS keys ローテーション
- での SAP HANA AWS
- AWS Well-Architected フレームワーク用の SAP レンズの紹介 (ブログ記事)

ツール

- で Infrastructure as Code を使用する自動化 CloudFormation
- ベストプラクティス 2.7 – 変更のテスト、統合、デプロイを自動化する (AWS Well-Architected Framework、SAP レンズ)
- ベストプラクティス 2.5 – 変更をテストおよび検証する (AWS Well-Architected Framework、SAP レンズ)

ガイドとパターン

- SAP on AWS migration methodology
- SAP HANA から AWS: AWS 移行のパターン

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
新しいサンプルを追加	コミュニケーション計画、プロジェクトロードマップ、マイルストーントラッカーの例を追加するためにガイドを更新しました。	2024 年 7 月 18 日
初版発行	—	2022 年 4 月 12 日

AWS 規範ガイダンスの用語集

以下は、 AWS 規範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する。
- リプラットフォーム (リフトアンドリシェイプ) — アプリケーションをクラウドに移行し、クラウド機能を活用するための最適化レベルを導入します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの Oracle 用の Amazon Relational Database Service (Amazon RDS) に移行する。
- 再購入 (ドロップアンドショップ) — 通常、従来のライセンスから SaaS モデルに移行して、別の製品に切り替えます。例: 顧客関係管理 (CRM) システムを Salesforce.com に移行する。
- リホスト (リフトアンドシフト) — クラウド機能を活用するための変更を加えずに、アプリケーションをクラウドに移行します。例: お客様のオンプレミスの Oracle データベースを AWS クラウドの EC2 インスタンス上の Oracle に移行する。
- 再配置 (ハイパーバイザーレベルのリフトアンドシフト) – 新しいハードウェアを購入したり、アプリケーションを書き換えたり、既存の運用を変更したりすることなく、インフラストラクチャをクラウドに移行できます。オンプレミスプラットフォームから同じプラットフォームのクラウドサービスにサーバーを移行します。例： Microsoft Hyper-Vアプリケーションを に移行します AWS。
- 保持 (再アクセス) — アプリケーションをお客様のソース環境で保持します。これには、主要なリファクタリングを必要とするアプリケーションや、お客様がその作業を後日まで延期したいアプリケーション、およびそれらを移行するためのビジネス上の正当性がないため、お客様が保持するレガシーアプリケーションなどがあります。
- 廃止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

ABAC

「属性ベースのアクセス制御」をご覧ください。

抽象化されたサービス

「マネージドユーザー」をご覧ください。

ACID

「原子性、一貫性、分離性、耐久性 (ACID)」をご覧ください。

アクティブ/アクティブ移行

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

アクティブ/パッシブ移行

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

集計関数

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

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

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

アンチパターン

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

アプリケーション制御

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン (AZ)

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

AWS クラウド導入フレームワーク (AWS CAF)

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

AWS ワークロード認定フレームワーク (AWS WQF)

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

B

不正なボット

個人や組織に混乱や損害を与えることを目的としたボット。

BCP

「ビジネス継続性計画 (BCP)」をご覧ください。

動作グラフ

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

ビッグエンディアンシステム

最上位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

二項分類

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

ブルームフィルター

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

ブルー/グリーンデプロイ

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

ボット

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

ボットネット

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

ブランチ

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

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

ブレークグラスアクセス

例外的な状況では、承認されたプロセスを通じて、ユーザーが AWS アカウント 通常アクセス許可を持たない にすばやくアクセスできるようにします。詳細については、 AWS Well-Architected ガイダンスの「ブレークグラス手順の実装」インジケータを参照してください。

ブラウンフィールド戦略

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

バッファキャッシュ

アクセス頻度が最も高いデータが保存されるメモリ領域。

ビジネス能力

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

ビジネス継続性計画 (BCP)

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

C

CAF

「AWS クラウド導入フレームワーク」を参照してください

カナリアデプロイ

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

CCoE

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

CDC

「変更データキャプチャ」を参照してください。

変更データキャプチャ (CDC)

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

カオスエンジニアリング

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

CI/CD

「継続的インテグレーションと継続的デリバリー」を参照してください。

分類

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

クライアント側の暗号化

ターゲットがデータ AWS のサービス を受信する前に、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に接続されています。

クラウド運用モデル

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

導入のクラウドステージ

組織が、 AWS クラウドへの移行時に通常実行する 4 つの段階。

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

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

CMDB

「構成管理データベース (CMDB)」を参照してください。

コードリポジトリ

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

コールドキャッシュ

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

コールドデータ

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

コンピュータビジョン (CV)

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

設定ドリフト

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

構成管理データベース (CMDB)

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

コンフォーマンスパック

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

継続的インテグレーションと継続的デリバリー (CI/CD)

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

CV

「コンピュータビジョン」を参照してください。

D

保管中のデータ

ストレージ内にあるデータなど、常に自社のネットワーク内にあるデータ。

データ分類

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

データドリフト

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

転送中のデータ

ネットワーク内 (ネットワークリソース間など) を活発に移動するデータ。

データメッシュ

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

データ最小化

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

データ境界

AWS 環境内の一連の予防ガードレール。信頼された ID のみが、期待されるネットワークから信頼されたリソースにアクセスできるようにします。詳細については、「 でのデータ境界の構築 AWS」を参照してください。

データの前処理

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

データ出所

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

データ件名

データを収集、処理している個人。

データウェアハウス

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

データベース定義言語 (DDL)

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

データベース操作言語 (DML)

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

DDL

「データベース定義言語」を参照してください。

ディープアンサンブル

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

深層学習

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

多層防御

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

委任管理者

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

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

トラブルシューティング

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

開発環境

「環境」を参照してください。

検出管理

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

開発バリューストリームマッピング (DVSM)

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

デジタルツイン

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

ディメンションテーブル

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

ディザスタ

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

ディザスタリカバリ (DR)

ディザスタによるダウンタイムとデータ損失を最小限に抑えるための戦略とプロセス。詳細については、 AWS Well-Architected フレームワークの「 でのワークロードのディザスタリカバリ AWS: クラウドでのリカバリ」を参照してください。

DML

「データベース操作言語」を参照してください。

ドメイン駆動型設計

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

DR

「ディザスタリカバリ」を参照してください。

ドリフト検出

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

DVSM

「開発バリューストリームマッピング」を参照してください。

E

EDA

「探索的データ分析」を参照してください。

EDI

「電子データ交換」を参照してください。

エッジコンピューティング

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

電子データ交換 (EDI)

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

暗号化

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

暗号化キー

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

エンディアン

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

エンドポイント

「サービスエンドポイント」を参照してください。

エンドポイントサービス

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

エンタープライズリソースプランニング (ERP)

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

エンベロープ暗号化

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

環境

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

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

エピック

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

ERP

「エンタープライズリソース計画」を参照してください。

探索的データ分析 (EDA)

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

F

ファクトテーブル

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

フェイルファスト

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

障害分離境界

では AWS クラウド、障害の影響を制限し、ワークロードの耐障害性を高めるのに役立つアベイラビリティーゾーン AWS リージョン、コントロールプレーン、データプレーンなどの境界。詳細については、「AWS 障害分離境界」を参照してください。

機能ブランチ

「ブランチ」を参照してください。

特徴量

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

特徴量重要度

モデルの予測に対する特徴量の重要性。これは通常、Shapley Additive Deskonations (SHAP) や積分勾配など、さまざまな手法で計算できる数値スコアで表されます。詳細については、「 を使用した機械学習モデルの解釈可能性 AWS」を参照してください。

機能変換

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

数ショットプロンプト

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

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

FGAC

「きめ細かなアクセス制御」を参照してください。

きめ細かなアクセス制御 (FGAC)

複数の条件を使用してアクセス要求を許可または拒否すること。

フラッシュカット移行

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

FM

「基盤モデル」を参照してください。

基盤モデル (FM)

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

G

生成 AI

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

ジオブロッキング

「地理的制限」を参照してください。

地理的制限 (ジオブロッキング)

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

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

Gitflow ワークフロー

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

ゴールデンイメージ

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

グリーンフィールド戦略

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

ガードレール

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

H

HA

「高可用性」を参照してください。

異種混在データベースの移行

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

高可用性 (HA)

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

ヒストリアンのモダナイゼーション

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

ホールドアウトデータ

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

同種データベースの移行

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

ホットデータ

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

ホットフィックス

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

ハイパーケア期間

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

I

IaC

「Infrastructure as Code」を参照してください。

ID ベースのポリシー

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

アイドル状態のアプリケーション

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

IIoT

「インダストリアル IoT」を参照してください。

イミュータブルインフラストラクチャ

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

インバウンド (受信) VPC

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

増分移行

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

インダストリー 4.0

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

インフラストラクチャ

アプリケーションの環境に含まれるすべてのリソースとアセット。

Infrastructure as Code (IaC)

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

インダストリアル IoT (IIoT)

製造、エネルギー、自動車、ヘルスケア、ライフサイエンス、農業などの産業部門におけるインターネットに接続されたセンサーやデバイスの使用。詳細については、「インダストリアル IoT (IIoT) デジタルトランスフォーメーション戦略の構築」を参照してください。

インスペクション VPC

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

IoT

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

解釈可能性

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

IoT

「IoT」を参照してください。

IT 情報ライブラリ (ITIL)

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

IT サービス管理 (ITSM)

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

ITIL

「IT 情報ライブラリ」を参照してください。

ITSM

「IT サービス管理」を参照してください。

L

ラベルベースアクセス制御 (LBAC)

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

ランディングゾーン

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

大規模言語モデル (LLM)

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

大規模な移行

300 台以上のサーバの移行。

LBAC

「ラベルベースアクセス制御」を参照してください。

最小特権

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

リフトアンドシフト

「7 Rs」を参照してください。

リトルエンディアンシステム

最下位バイトを最初に格納するシステム。「エンディアン性」もご覧ください。

LLM

「大規模言語モデル」を参照してください。

下位環境

「環境」を参照してください。

M

機械学習 (ML)

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

メインブランチ

「ブランチ」を参照してください。

マルウェア

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

マネージドサービス

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

製造実行システム (MES)

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

MAP

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

メカニズム

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

メンバーアカウント

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

MES

「製造実行システム」を参照してください。

Message Queuing Telemetry Transport (MQTT)

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

マイクロサービス

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

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

マイクロサービスアーキテクチャ

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

Migration Acceleration Program (MAP)

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

大規模な移行

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

移行ファクトリー

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

移行メタデータ

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

移行パターン

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

Migration Portfolio Assessment (MPA)

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

移行準備状況評価 (MRA)

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

移行戦略

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

ML

「機械学習」を参照してください。

モダナイゼーション

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

モダナイゼーション準備状況評価

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

モノリシックアプリケーション (モノリス)

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

MPA

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

MQTT

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

多クラス分類

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

ミュータブルなインフラストラクチャ

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

O

OAC

「オリジンアクセス制御」を参照してください。

OAI

「オリジンアクセスアイデンティティ」を参照してください。

OCM

「組織変更管理」を参照してください。

オフライン移行

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

OI

「オペレーション統合」を参照してください。

Ola

「オペレーショナルレベルアグリーメント」を参照してください。

オンライン移行

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

OPC-UA

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

Open Process Communications - Unified Architecture (OPC-UA)

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

オペレーショナルレベルアグリーメント (OLA)

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

運用準備状況レビュー (ORR)

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

運用テクノロジー (OT)

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

オペレーション統合 (OI)

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

組織の証跡

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

組織変更管理 (OCM)

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

オリジンアクセス制御 (OAC)

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

オリジンアクセスアイデンティティ (OAI)

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

ORR

「運用準備状況レビュー」を参照してください。

OT

「運用テクノロジー」を参照してください。

アウトバウンド (送信) VPC

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

P

アクセス許可の境界

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

個人を特定できる情報 (PII)

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

PII

「個人を特定できる情報」を参照してください。

プレイブック

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

PLC

「プログラマブルロジックコントローラー」を参照してください。

PLM

「製品ライフサイクル管理」を参照してください。

ポリシー

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

多言語の永続性

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

ポートフォリオ評価

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

述語

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

述語プッシュダウン

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

予防的コントロール

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

プリンシパル

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

プライバシーバイデザイン

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

プライベートホストゾーン

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

プロアクティブコントロール

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

製品ライフサイクル管理 (PLM)

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

本番環境

「環境」を参照してください。

プログラマブルロジックコントローラー (PLC)

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

プロンプトチェイニング

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

仮名化

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

発行/サブスクライブ (pub/sub)

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

Q

クエリプラン

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

クエリプランのリグレッション

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

R

RACI マトリックス

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

RAG

「検索拡張生成」を参照してください。

ランサムウェア

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

RASCI マトリックス

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

RCAC

「行と列のアクセス制御」を参照してください。

リードレプリカ

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

リアーキテクト

「7 Rs」を参照してください。

目標復旧時点 (RPO)

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

目標復旧時間 (RTO)

サービスの中断から復旧までの最大許容遅延時間。

リファクタリング

「7 Rs」を参照してください。

リージョン

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

リグレッション

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

リホスト

「7 Rs」を参照してください。

リリース

デプロイプロセスで、変更を本番環境に昇格させること。

再配置

「7 Rs」を参照してください。

リプラットフォーム

「7 Rs」を参照してください。

再購入

「7 Rs」を参照してください。

回復性

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

リソースベースのポリシー

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

実行責任者、説明責任者、協業先、報告先 (RACI) に基づくマトリックス

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

レスポンシブコントロール

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

保持

「7 Rs」を参照してください。

廃止

「7 Rs」を参照してください。

検索拡張生成 (RAG)

生成 AI の技術。これにより、LLM では、レスポンスの生成前に、トレーニングデータソースの外部にある信頼できるデータソースが参照されます。例えば、RAG モデルによって、組織のナレッジベースまたはカスタムデータのセマンティック検索を実行できる場合があります。細については、「RAG (検索拡張生成) とは何ですか?」を参照してください。

ローテーション

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

行と列のアクセス制御 (RCAC)

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

RPO

「目標復旧時点」を参照してください。

RTO

「目標復旧時間」を参照してください。

ランブック

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

S

SAML 2.0

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

SCADA

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

暗号化された形式で保存する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。シークレット値には、バイナリ、1 つの文字列、複数の文字列を指定できます。詳細については、Secrets Manager ドキュメントの「Secrets Manager シークレットの概要」を参照してください。

セキュリティバイデザイン

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

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

セキュリティイベントへの自動レスポンスまたは自動修復を目的として、事前定義およびプログラムされたアクション。これらの自動化は、セキュリティのベストプラクティスを実装するのに役立つ検出的または応答的な AWS セキュリティコントロールとして機能します。自動レスポンスアクションの例には、VPC セキュリティグループの変更、Amazon EC2 インスタンスへのパッチ適用、認証情報の更新などがあります。

サーバー側の暗号化

送信先にあるデータの、それ AWS のサービス を受け取る による暗号化。

サービスコントロールポリシー (SCP)

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

サービスエンドポイント

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

サービスレベルアグリーメント (SLA)

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

サービスレベルインジケータ (SLI)

エラー率、可用性、スループットといった、サービスパフォーマンス面の指標。

サービスレベル目標 (SLO)

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

責任共有モデル

クラウドのセキュリティとコンプライアンス AWS について と共有する責任を説明するモデル。AWS はクラウドのセキュリティを担当しますが、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

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

単一障害点 (SPOF)

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

SLA

「サービスレベルアグリーメント」を参照してください。

SLI

「サービスレベルインジケータ」を参照してください。

SLO

「サービスレベルの目標」を参照してください。

スプリットアンドシードモデル

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

SPOF

「単一障害点」を参照してください。

スタースキーマ

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

strangler fig パターン

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

サブネット

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

監視制御とデータ取得 (SCADA)

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

対称暗号化

データの暗号化と復号に同じキーを使用する暗号化のアルゴリズム。

合成テスト

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

システムプロンプト

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

T

タグ

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

ターゲット変数

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

タスクリスト

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

テスト環境

「環境」を参照してください。

トレーニング

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

トランジットゲートウェイ

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

トランクベースのワークフロー

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

信頼されたアクセス

ユーザーに代わって AWS Organizations およびそのアカウントで組織内でタスクを実行するために指定したサービスにアクセス許可を付与します。信頼されたサービスは、サービスにリンクされたロールを必要なときに各アカウントに作成し、ユーザーに代わって管理タスクを実行します。詳細については、 ドキュメントの「 を他の AWS のサービス AWS Organizations 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 枚のピザを分け合えることができるくらい小さな DevOps チーム。ツーピザチームの規模では、ソフトウェア開発におけるコラボレーションに最適な機会が確保されます。

U

不確実性

予測機械学習モデルの信頼性を損なう可能性がある、不正確、不完全、または未知の情報を指す概念。不確実性には、次の 2 つのタイプがあります。認識論的不確実性は、限られた、不完全なデータによって引き起こされ、弁論的不確実性 は、データに固有のノイズとランダム性によって引き起こされます。

未分化なタスク

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

上位環境

「環境」を参照してください。

V

バキューミング

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

バージョンコントロール

リポジトリ内のソースコードへの変更など、変更を追跡するプロセスとツール。

VPC ピアリング

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

脆弱性

システムのセキュリティを脅かすソフトウェアまたはハードウェアの欠陥。

W

ウォームキャッシュ

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

ウォームデータ

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

ウィンドウ関数

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

ワークロード

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

ワークストリーム

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

WORM

「Write-Once-Read-Many」を参照してください。

WQF

「AWS ワークロード資格フレームワーク」を参照してください

Write-Once-Read-Many (WORM)

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

Z

ゼロデイエクスプロイト

ゼロデイ脆弱性を悪用した攻撃 (一般的にマルウェアによる)。

ゼロデイ脆弱性

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

ゼロショットプロンプト

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

ゾンビアプリケーション

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

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