AWS for SaaS サービスでのネットワーク接続オプション

AWS 規範ガイダンス

AWS 規範ガイダンス: AWS for SaaS サービスでのネットワーク接続オプション

Table of Contents

AWS for SaaS サービスでのネットワーク接続オプション

Tomas Sykora と Luca Schumann、Amazon Web Services

2025 年 9 月 (ドキュメント履歴)

このガイドでは、コンシューマーアプリケーションを Software as a Service (SaaS) プロバイダーに接続するための一般的なシナリオについて説明します。ここでは、オンプレミス、 内、 AWS クラウド他のクラウドサービスプロバイダー (CSP) クラウド内、またはハイブリッドアーキテクチャ内のリソースに接続する方法について説明します。これらのシナリオには以下が含まれます。

- HTTPS 経由のウェブサービスの公開
- TCP ベースのサービスの公開
- AWS AppSync を使用して publish-subscribe (Pub/Sub) および GraphQL APIs
- AWS リソースを使用してリアルタイムアプリケーション用の WebSockets公開する
- インタラクティブなサービス通信のための双方向アクセスの有効化

このガイドで説明されているベストプラクティスに従うことで、SaaS プロバイダーは顧客の信頼を高め、SaaS サービスへのスケーラブルで安全で回復力のあるアクセスをサポートできます。

このガイドには、SaaS サービスのコンシューマーネットワーク要件をどの程度満たしているかを評価するのに役立つ自己評価基準も含まれています。接続パターン以外にも、 AWS ネットワーキングサービスの包括的な比較、さまざまなデプロイシナリオの大まかなアーキテクチャ図、特定のビジネスコンテキストに基づいて適切なアプローチを選択する方法に関する実践的なガイダンスがあります。このガイドでは、ネットワークオプションごとのセキュリティ上の考慮事項について説明し、回避すべき一般的な落とし穴について説明し、技術的要件と運用効率のバランスを取る実装の推奨事項を提供します。さらに、ネットワークに関する意思決定をビジネスモデル、成長目標、規制コンプライアンスのニーズに合わせるための戦略的フレームワークも用意されています。

対象者

このガイドは SaaS プロバイダーを対象としています。で SaaS サービスのネットワーク接続を設計、実装、最適化するクラウドアーキテクト、製品マネージャー、ネットワークエンジニアを支援します AWS クラウド。このガイドの概念と推奨事項を理解するには、 AWS 基礎、SaaS のコア概念、および高レベルのネットワーク原則に精通している必要があります。

目的

このガイドでは、コンシューマーが SaaS サービスへのアクセスを最適化するのに役立つネットワークアーキテクチャのオプションとフィールドテスト済みのベストプラクティスについて説明します。このガイドの推奨事項を実装すると、以下がサポートされます。

- 統合の容易さ – オンボーディングから本番稼働までの複雑なカスタマージャーニーを提供し、顧客の価値創出までの時間を短縮し、収益認識サイクルを短縮できるようにします。
- 適応性 – 進化するニーズに適応することで、既存のネットワークインフラストラクチャとシームレスに統合できます。これにより、製品の価値提案が強化されます。
- 総所有コスト – ネットワークアクセスを標準化して、テナントあたりの変更コストとコストを削減します。デプロイの一貫性を向上させることで、根本原因の分析や修復にかかる時間を短縮することもできます。
- 依存関係管理 – さまざまなネットワークアクセスオプションの依存関係、長期的な影響、トレードオフを理解します。これにより、製品リーダーは十分な情報に基づいた製品に関する意思決定を行うことができます。
- 互換性と拡張性 — コア機能の開発を運用インフラストラクチャから切り離します。これにより、開発チームはより迅速に動き、顧客にとっての価値の創造に集中できます。
- 信頼の促進 – SaaS サービスへの回復力、耐障害性、安全性、スケーラブルなアクセスを提供することで、規制リスクを軽減し、顧客の成長をサポートする能力への信頼を得ることができます。

SaaS サービスのネットワークアクセスの決定を評価する

市場について

ここでネットワークに関する決定を行うことで、SaaS 製品の価値提案を顧客に配信できるかどうかが決まります。これらの決定は戦略的に重要ですが、SaaS サービスへのアクセスを提供することは、純粋に技術的なトピックとして認識されることがよくあります。この認識に伴うリスクには、収益認識サイクルの長期化、運用上の非効率性、ビジネス戦略との不整合が含まれます。例えば、迅速な拡張が戦略的ビジネス目標である場合、意思決定プロセスの指針となるのは、検討しているソリューションが拡張をサポートするのに十分なスケーラビリティと柔軟性があるかどうかです。ビジネスの成長に成功した場合でも、運用上のオーバーヘッドが将来の成長の障害になることはありません。コスト構造がずれると、すべての利益が浪費される可能性があります。

たとえば、次の市場上の考慮事項が、ネットワーキングなどの製品の技術的側面にどのように影響するかを考えてみましょう。

- ビジネスモデルがサブスクリプションベースである場合、顧客は多額の先行投資ではなく、予測可能な経常コストのソリューションを好む可能性があります。
- ビジネス戦略が高価値のエンタープライズレベルの顧客を対象としている場合、セキュリティ、ガバナンス、規制のコンプライアンス基準によって、SaaS サービスが考慮されるかどうかが決まります。
- ターゲット市場が主にスタートアップである場合、統合の容易さ、価値創出までの時間、適応性が重要な要素である可能性があります。スタートアップは通常、スピードと俊敏性を優先します。ブランドを構築し、収益を迅速に生み出す必要があるため、迅速かつ簡単に統合でき、費用対効果の高いスケーリング、エキスパートへの依存の軽減、貴重なサイクルを結び付けないソリューションが好まれる可能性があります。
- 一部の企業では、安定した高スループット、低レイテンシーのアクセスが必要です。これには、エンターテインメントおよびメディア業界、製造、金融取引処理が含まれます。これらがターゲット顧客である場合、信頼性が主な懸念事項です。

いずれの場合も、ネットワークアクセスがシームレスでない場合、顧客は正常な SaaS サービスを認識する可能性があります。ネットワークが障害になった場合、これはビジネスケースをサポートしていません。顧客が提供するサービスに確実にアクセスできない場合、SaaS サービスの価値提案は nil です。

ロールについて

ビジネス目標をサポートする役割は、自分が何者であるか、特定の個人とチームの目標は何か、顧客は何者であるか、顧客にとって何が重要かによって異なります。通常顧客とやり取りするチームの一員でなくても、顧客が誰で、何を必要としているのかを懸念する必要があります。エンジニアリングチームと開発チームは、社内の顧客、特に定期的にやり取りする顧客にも関心を持つ必要があります。通常、これらは運用チームとカスタマーサクセスチームです。

販売組織の一員である場合は、純粋に見えるテクノロジーのトピックであっても、ネットワーキングについて製品チームやエンジニアリングチームとコミュニケーションを取ることが重要です。ターゲット市場の構造に関するインサイトを共有します。問題点と、既存および潜在的な顧客やパートナーのニーズを伝えます。見逃した機会、セグメントあたりの予測成長率、イベントに関するデータとエピソードを共有します。ビジネスの成長をサポートする組織の能力にチャレンジする質問をします。これにより、機会の数が増え、ビジネスの長期的な収益性が向上します。最終的に、これは組織が将来の拡張と開発に資金を提供するのに役立ちます。

エンジニアリング組織に属している場合は、ソリューションのドラフトを作成する前に、組織のビジネス戦略を理解してください。ビジネス戦略と連携することで、さまざまなネットワークアクセスオプションを評価するための適切なメトリクスを選択できます。また、組織が成長するにつれて、高価で大規模なネットワーク再設計を防ぐこともできます。ビジネスの連携は、チームが将来の課題に必要なリソースを保護し、保持するのに役立ちます。チームの人員数、専門的な開発のための予算、または最先端のテクノロジーへのアクセスは、ビジネスの連携を示す能力によって異なります。理想的には、意思決定が組織のビジネスの成功にどのように貢献したかを示すことができます。したがって、メトリクスの選択基準など、意思決定プロセスをキャプチャすることをお勧めします。メトリクスを定期的に見直して、ビジネス目標に沿っていることを確認します。これは、チームが自業自得のクレジットを取得するのに役立ちます。定期的なレビューは、チームが仮定や古くなった過去の理由に基づいて意思決定を行っていないことを確認するのにも役立ちます。

以下のセクションのメトリクスのリストは、ネットワークアクセスに関連しています。

- 製品および商用メトリクス
- ネットワークの決定に影響を与えるエンジニアリングメトリクス

このガイドでは、SaaS サービスに最適なネットワークアクセスアプローチを特定するため、全体でこれらのメトリクスのサブセットを使用します。ビジネスに最も重要で関連性の高いメトリクスを選択し、それらのメトリクスに基づいてアプローチを評価します。

ネットワークの決定に影響を与える製品および商用メトリクス

製品チームとコマーシャルチームは、成功基準を使用して、ビジネス目標を達成しているかどうかを評価します。このセクションでは、組織が行うネットワークアクセスの決定によってプラスまたはマイナスの影響を受ける可能性のある製品または商用メトリクスについて説明します。

これらのメトリクスと自己評価の質問を使用して、ネットワークアクセスアプローチがビジネスポジションと市場戦略とどのように整合しているかを評価します。この評価は、現在のネットワーク決定が企業の市場差別化、競争上の利点、ターゲットオーディエンスのニーズをサポートしているかどうかを判断するのに役立ちます。

このセクションには、以下のトピックに関するメトリクスと自己評価の質問が含まれています。

- ビジネスモデルと市場ポジション
- 対応可能な市場、新規クライアント獲得率、成長、スケーラビリティの合計
- カスタマーエクスペリエンスとリテンション
- 効率と財務パフォーマンス
- 規制コンプライアンスとリスク管理
- パートナー戦略

ビジネスモデルと市場ポジション

これらのメトリクスは、競争上の差別化、市場リーチ、ブランド認識など、市場での貴社の立場に関連しています。ネットワークアクセスアプローチとビジネスモデルの整合性を評価することが重要です。サブスクリプションベース、使用量ベース、freemium、階層型、マーケットプレイス、APIファースト、ホワイトラベルのいずれであっても、評価を実行します。モデルが組織の目標と顧客の目標をサポートしていることを確認します。

ハイスコア基準

ネットワークアクセスアプローチは、ビジネスモデルとシームレスに連携します。これにより、サービスの採用と提供が容易になります。ビジネスモデルの長期的な財務可能性をサポートし、コスト構造は予想される成長と互換性があります。サービスを採用する際の顧客やパートナーの摩擦を最小限に抑えます。これにより、ユーザーエクスペリエンスが向上し、サービスのより広範な取り込みが促進されます。

低スコアインジケータ

選択したネットワークアクセスアプローチが、サポートすべきビジネスモデルと一致しない。コスト構造とデプロイまでのリードタイムは、ターゲット市場への導入を妨げます。継続的なインフラストラクチャと運用コストは、潜在的な利益を妨げます。これにより、ビジネスの成長が妨げられ、意図した規模での運用が困難になります。または、ネットワークアクセスアプローチのプロパティにより、規制上の理由からお客様がサービスを検討できない場合があります。

自己評価の質問

- 選択したネットワークアクセスアプローチが初期デプロイと継続的な配信に与えるコストへの影響は何ですか? このアプローチの固定コストと変動コストはいくらですか?
- ネットワークアクセスアプローチは、ビジネスモデルの成長需要を満たすために効果的かつ効率的にスケールできますか? 個々のテナントサイズとオンボーディングされたテナントの数を考慮してください。
- ネットワークアクセスアプローチには、ビジネスモデルの柔軟性や適応性を制限する可能性のある技術的または運用上の制限がありますか?
- ネットワークアクセスアプローチの場合、デプロイのリードタイムは、ビジネスモデルが必要とする市場投入までの時間とどのように整合していますか?

対応可能な市場、新規クライアント獲得率、成長、スケーラビリティの合計

ネットワークの意思決定が組織の能力に与える影響を評価して、新しい市場に進出し、顧客を効果的に獲得し、運用のスケーラビリティを維持することが重要です。これらの要因は変換率に影響します。また、ネットワークアクセスアプローチが重要な市場セグメントへの拡大をサポートしているか、特定の顧客タイプのみを提供するように制限しているかにも影響します。

ハイスコア基準

ネットワークアクセスアプローチは、組織がターゲット市場の大部分に到達するのに役立ちます。または、他のネットワークアプローチと効果的に組み合わせて市場リーチを拡大することもできます。このアプローチでは、追加の統合作業を最小限に抑える必要があります。このアプローチは、デプロイ、迅速な市場参入、拡大の短いリードタイムをサポートします。これにより、多数の並列デプロイが可能になります。お客様にとって統合は簡単です。これにより、導入の障壁が軽減され、カスタマーエクスペリエンスが向上します。このアプローチは、運用上のオーバーヘッドを最小限に抑え、運用能力を維持し、成長予測をサポートします。

低スコアインジケータ

ネットワークアクセスアプローチは、ターゲット市場の一部のみをサポートするか、主にビジネス戦略で優先順位が付けられていないニッチなセグメントに適しています。既にサポートされている他のネットワークアクセスアプローチを効果的に補完するものではありません。デプロイラグ市場需要のリードタイム。これにより、市場の拡大と新しいクライアント獲得が制限されます。デプロイモデルはシーケンシャルであるため、需要の増加に応じてサービスのボトルネックのリスクが高まります。複雑な統合プロセスは潜在的なクライアントを抑止し、取得率と変換率に悪影響を及ぼします。運用上のオーバーヘッドが大きいと、組織の運用能力が低下します。これは、予測される成長のブロック要因になります。

これらの指標については、新しいネットワークアクセスアプローチの導入が組織の戦略的ビジネス目標の達成に役立つかどうかを評価します。新しいネットワークアクセスアプローチが、望ましい結果をもたらすことなく、新しい製品の依存関係を作成するか、運用リソースを消費するかを検討してください。

自己評価の質問

- 現在のアプローチに、ターゲット市場のより大きなセグメントに到達できないギャップはありますか?
- ターゲット市場の 70～90% をカバーするためにサポートする必要がある、重複しない標準化されたネットワークアクセスアプローチの最小セットは何ですか?
- 各ネットワークアクセスアプローチは、どのような到達を可能にしますか。また、インフラストラクチャコスト、運用サイクル、エキスパートへの依存関係など、重要なメトリクスの関連する増加はどのようなものですか。
- ネットワークインフラストラクチャのデプロイ機能とサービス制限は、ターゲット市場の拡大期待にどのように合致していますか?
- ネットワーク統合は、新規顧客の参入障壁となりますか? 変換率を向上させるために、これらにどのように対処できますか?
- ネットワーク管理の運用オーバーヘッドは、成長とスケーラビリティのために容量にどのように影響しますか?
- ネットワークデプロイのリードタイムを短縮し、市場拡大と顧客獲得を改善するために、どのような戦略を実装できますか?
- お客様のエコシステムへのデプロイや統合を遅らせるエキスパートリソースへの依存関係はありますか?

カスタマーエクスペリエンスとリテンション

このセクションのメトリクスは、組織の顧客を獲得し、最も重要な点として顧客を維持する能力を理解するのに役立ちます。ネットワークアクセスアプローチと顧客満足度の関係を理解することは、製品チームとエンジニアリングチームがデータから情報を得た意思決定を行うのに役立ちます。

ハイスコア基準

ネットワークアクセスアプローチは信頼性が高く、管理が容易です。これは、高い顧客満足度 (CSAT) とネットプロデューサースコア (NPS) の結果に寄与します。これらのスコアは、ブランドの評判と顧客ロイヤルティが高いことを示しています。顧客の既存のエコシステムとのシームレスな統合により、導入の摩擦が低く、エキスパートへの依存度が低くなります。組織は一貫してサービスレベルアグリーメント (SLAs) を満たしているため、顧客の信頼と契約上の義務が強化されます。顧客は安定していて信頼できるサービスを享受しているため、顧客保持率は高くなります。

低スコアインジケータ

統合が難しく、サービスへのアクセスに一貫性がないと、顧客の不満や否定的なフィードバックが生じることがよくあります。これにより、ブランドの評判が損なわれます。新規顧客は、エキスパートへの依存やオンボーディングや統合時間が長引くため、無料プランやトライアルプランから有料サービスへの変換に失敗します。SLAs を頻繁に満たさないと、罰金が科せられ、信頼性が失われ、顧客保持率が低下する可能性があります。

自己評価の質問

- ネットワークパフォーマンス (速度、稼働時間、レイテンシーなど) は CSAT と NPS の結果にどのように直接影響しますか? これらのスコアを高めることができる具体的なネットワークの改善は何ですか?
- 現在のネットワークレイテンシーと稼働時間のメトリクスは、最初のユーザーエクスペリエンスと導入率にどのように影響しますか? これらのメトリクスを最適化するには、どのような特定のネットワークパフォーマンスの改善が必要ですか?
- 新規顧客の統合を複雑にするネットワーク設定やセキュリティ設定に、繰り返し発生する問題はありますか? これらのプロセスを合理化するにはどうすればよいですか?
- ネットワークアクセスの設定のしやすさは、新規ユーザーのオンボーディングエクスペリエンスにどのように影響しますか? 最初のユーザーのインプレッションを強化するために最適化できる特定のネットワークアクセスポイントまたはリードタイムはありますか?

- 新しいクライアントのネットワークサービスのプロビジョニングを自動化する際の課題は何ですか。スケーラビリティと信頼性を向上させるために、このプロセスを調整するにはどうすればよいですか?
- 最近の SLA 違反の根本原因を分析します。ネットワーク設定、キャパシティプランニング、または外部ベンダーの問題に関連していましたか?
- ネットワークの問題が原因で SLA のコミットメントを逃す頻度はどのくらいですか? 最も頻繁に発生するネットワーク関連の障害は何ですか?
- 過去に顧客満足度に最も大きなプラスの影響を与えたネットワークパフォーマンスの改善はどれですか?

効率と財務パフォーマンス

このカテゴリでは、コスト効率、長期的な実行可能性、収益性、投資収益率 (ROI)、総所有コスト (TCO) など、ビジネスの財務状態と収益性の側面を評価します。標準化によりネットワーク運用を合理化することで、運用上のオーバーヘッドとメンテナンスコストを削減できます。これにより、組織の成長目標がサポートされます。

ハイスコア基準

ネットワークアクセスアプローチのコスト構造は、ビジネスモデルとよく一致しています。持続可能な成長と、収益性の向上を実現する大幅なコスト削減をサポートします。効率的なネットワークアクセスにより、迅速な顧客オンボーディングが可能になり、価値を提供する時間を短縮し、市場浸透を加速できます。これにより、収益認識サイクルが直接短縮されます。

低スコアインジケータ

お客様は、アプリケーションとサービスの配信を高速化するために、お客様の競争に目を向けています。組織では、複雑で多様なネットワーク設定に関連する運用コストが増加し、リードタイムが長くなりました。コスト構造とビジネスモデルが一致していないため、サブスクリプションベースのサービスの前払いコストが高くなる可能性があります。面倒なオンボーディングプロセスにより、市場浸透が減少し、収益認識が遅れます。

自己評価の質問

- 新しいサービスデプロイの現在のリードタイムと、それらが市場投入までの時間と収益認識にどのように影響するか。
- 標準化されたネットワークオペレーションは、オーバーヘッドとメンテナンスコストをどの程度効果的に削減しますか?

- エキスパートリソースは、最初の統合を正常に完了したり、毎日運用したり、問題をトラブルシューティングしたり、変更を実装したりするために必要ですか?
- 技術的進歩の観点から、現在のネットワーク投資はどの程度持続可能ですか? 予測された市場開発に沿った将来性のあるテクノロジーに投資していますか?
- 個々のテナントのネットワークトラフィックと使用状況に関連するコストをどの程度効果的に割り当てて追跡していますか?

規制コンプライアンスとリスク管理

ネットワーク関連の規制への準拠を検証することは基本的に重要です。これにより、法的に運用されており、顧客の信頼を維持できることを確認できます。ネットワーク運用全体の標準化により、コンプライアンスプロセスが簡素化され、さまざまな管轄区域や地域にわたる一貫性が促進されます。これらの対策は、サービスを拡張するのに役立ちます。

ハイスコア基準

ネットワーク運用は、市場の拡大、導入の摩擦の軽減、顧客の信頼の向上につながる、複雑性のない法的な基準に一貫して準拠しています。デジタル運用レジリエンス法 (DORA) や米国国立標準技術研究所 (NIST) などの重要な規制フレームワークへの準拠が実証されているため、規制コンプライアンスに敏感な顧客を獲得できます。コンプライアンスステータスを継続的に可視化することで、監査の完了に必要な時間が短縮されます。

低スコアインジケータ

ネットワークコンプライアンスのギャップにより、導入の摩擦、サービス起動の遅延、法的課題、および潜在的な罰金が発生します。これらの課題により、新しい市場への拡大計画が遅延またはキャンセルされます。さまざまな管轄区域で標準のコンプライアンスプラクティスを維持することは困難であり、運用効率と市場の評価に影響します。

自己評価の質問

- ネットワーク運用は、該当する規制または業界のガイドラインにどの程度合致していますか? 最近のコンプライアンス監査で明らかになったことは何ですか?
- デジタルおよびネットワークセキュリティ領域における新しい規制への準拠をどのように維持していますか?
- ドキュメントとレポートプロセスは、さまざまな規制機関の要件を満たす上でどの程度効果的ですか?

- 潜在的なコンプライアンスリスクが法的課題につながる前に特定して対処するために、どのようなリスク管理戦略を実施していますか?
- ネットワーク管理チームは、ネットワークアクセスアプローチをサポートするために、どの程度のレベルのコンプライアンストレーニングと認識が必要ですか?

パートナー戦略

ネットワークアクセスアプローチが、認識されているパートナー、プラットフォーム、マーケットプレイスのエコシステムとどの程度一致しているかを評価します。これは、特に成長戦略がパートナーによるスケーリングに依存している場合に不可欠です。

ハイスコア基準

ネットワークアクセスアプローチは、パートナーエコシステム全体で統合されています。そのコスト構造は、主要なパートナーのビジネスモデルとよく一致しています。パートナーは、SaaS サービスをシームレスに統合するために必要なネットワークスキルを持ち、持続的なアクセスと機能を提供できます。

低スコアインジケータ

選択したネットワークアクセスアプローチには、希少または調達が難しい特殊なスキル、リソース、または機器が必要です。これは、プラットフォームやマーケットプレイスで一般的に使用される標準のネットワークアクセスプロトコルとは異なります。これにより、予測不可能なコスト構造になり、調整が困難になります。ネットワークアクセスアプローチが主要パートナーのビジネスモデルと一致しない。

自己評価の質問

- パートナーにとってのネットワークアクセスアプローチのコストへの影響は何ですか。これらのコストはビジネスモデルとどのように一致しますか? コストの大部分を負担しているのは統合のどの側ですか? 運用サイクルをいくつ投資する必要がありますか?
- ネットワークアクセスアプローチでは、パートナー関係やエコシステムのスケーラビリティに影響を与える可能性のある統合やメンテナンスの障壁はありますか?
- ネットワークアクセスアプローチを最適化して、エコシステム全体の互換性と統合の容易さを高めるにはどうすればよいですか?

ネットワークの決定に影響を与えるエンジニアリングメトリクス

製品チームや商用チームと同様に、エンジニアリングチームは成功基準を使用してビジネス目標を達成しているかどうかを評価します。ただし、これらのメトリクスは異なり、セキュリティとコンプライアンスの要件を開発、運用、満たすチームの能力に焦点を当てています。このセクションでは、組織が行うネットワークアクセスの決定によってプラスまたはマイナスの影響を受ける可能性のあるエンジニアリングメトリクスについて説明します。

これらのメトリクスと自己評価の質問を使用して、現在のネットワークアクセスアプローチをビジネス要件と技術的能力に照らして評価します。この評価は、アーキテクチャのギャップを特定し、戦略的目標に沿った改善に優先順位を付けるのに役立ちます。これらの基準を定期的に確認することで、ネットワークアクセス戦略が顧客のニーズと組織の成長計画の両方を引き続きサポートしていることを確認できます。

このセクションでは、以下のカテゴリとトピックに関するメトリクスと自己評価の質問について説明します。

- 開発メトリクス
  - デプロイ頻度、デプロイ時間、スプリント速度
  - 柔軟性と機能配信
  - 変更失敗率
  - コード品質とエンジニアリングチームのパフォーマンス
  - 技術的負債の削減
  - スケーラビリティ、容量、パフォーマンス
- オペレーショナルエクセレンスメトリクス
  - 運用レジリエンスとディザスタリカバリ
  - サービスおよびアプリケーションのパフォーマンスモニタリング
- セキュリティとガバナンスのメトリクス
  - セキュリティ、コンプライアンス、脆弱性の管理

SaaS サービスのネットワークアクセスに関連する開発メトリクス

このセクションでは、以下のメトリクスについて説明します。

- デプロイ頻度、デプロイ時間、スプリント速度
- 柔軟性と機能配信

- 変更失敗率
- コード品質とエンジニアリングチームのパフォーマンス
- 技術的負債の削減
- スケーラビリティ、容量、パフォーマンス

デプロイ頻度、デプロイ時間、スプリント速度

開発サイクルの効率を最適化するには、ネットワークスタックのプロビジョニングがスプリント速度に与える影響を理解することが不可欠です。

ハイスコア基準

ネットワークスタックのプロビジョニングは合理化および自動化されており、手動による介入は最小限に抑えられます。スプリント速度には大きな影響はありません。ネットワークスタックのプロビジョニングと再デプロイは、どのチームメンバーでも実行できます。これにより、ボトルネックと特殊なリソースへの依存関係が軽減されます。

低スコアインジケータ

ネットワークスタックをプロビジョニングするには、多数のストーリーポイントが必要です。これは、新機能の開発を妨げる複雑で時間のかかるプロセスを提案します。ネットワークスタックを頻繁に再デプロイすると、かなりの時間とコストのオーバーヘッドが発生します。ネットワークプロビジョニングタスクには専門的なエンジニアリングの専門知識が必要です。これによりボトルネックが発生し、開発サイクルが遅くなります。

自己評価の質問

- デプロイプロセスには、どのような手動ステップが含まれますか。デプロイの頻度と時間にどのように影響しますか?
- デプロイに障害が発生した場合のロールバックの処理方法。デプロイの頻度と復旧時間にはどのような影響がありますか?
- 新しい環境を設定するときに、ネットワークスタックのプロビジョニングに必要なストーリーポイントはいくつありますか?
- 開発プロセス中のネットワークスタックの頻繁な再デプロイに関連する追加コストと時間オーバーヘッドはどれくらいですか?
- ネットワークスタックのプロビジョニングは、専門的なエンジニアリングの専門知識に依存していますか、それともチームメンバーが管理できるタスクですか?

柔軟性と機能配信

ネットワークアクセスアプローチは、エンジニアリングチームが新機能を効率的に革新およびデプロイする能力に影響を与える可能性があります。

ハイスコア基準

ネットワークアクセスアプローチは、迅速でシームレスな機能デプロイに必要な柔軟性を提供します。幅広い通信プロトコル、一方向および双方向通信、メッセージサイズをサポートしています。開発プロセスやイノベーションには大きな制約はありません。

低スコアインジケータ

ネットワークアクセスアプローチは、サポートされている通信プロトコルの欠如、メッセージサイズの柔軟性の欠如、または特定のテクノロジーや関連するエキスパートリソースへの依存により、チームが新機能をロールアウトする能力を制限します。これにより、開発サイクルが遅くなり、サービスの進化が妨げられる可能性があります。

自己評価の質問

- ネットワークアクセスアプローチは、新機能の開発とデプロイにおけるチームの俊敏性にどのように影響しますか?
- ネットワークアクセスアプローチには、特定の通信プロトコルまたはテクノロジーのサポートを制限する制限がありますか?
- このアプローチは、サービスへの新しいテクノロジーとイノベーションの統合をどのように促進または制限しますか?
- ネットワークアクセスアプローチは、開発タイムラインと製品ロードマップにどのように影響しますか?

変更失敗率

選択したネットワークアクセスアプローチは、新しいサービスや機能をデプロイする際の変更失敗率に影響を与える可能性があります。コントロールを大きくすると、多くの場合、柔軟性が向上しますが、複雑なルーティング設定を管理する場合など、設定ミスの可能性も高くなります。

ハイスコア基準

障害のリスクを最小限に抑えながら、ネットワークスタックに変更を実装できます。十分なテストメカニズムが存在し、効率的なロールバックメカニズムが存在し、効果的なモニタリングは問題を迅速に特定して解決するのに役立ちます。

低スコアインジケータ

ネットワークアクセスアプローチは、変更中に失敗する傾向があります。テストオプションが限られている、デプロイ戦略が複雑である、モニタリングおよびトラブルシューティング機能が不十分である。トラブルシューティングセッションに参加するには、複数の関係者が必要です。これにより、ダウンタイムが増加し、SaaS サービスの可用性が低下する可能性があります。

自己評価の質問

- ネットワークスタックの更新時に変更の失敗のリスクを軽減するために、どのような対策が講じられていますか?
- 徹底的なテストと検証プロセスはありますか?
- システムは、失敗した変更からどのくらい早く回復できますか? 効率的なロールバックプロセスはありますか?
- ネットワークスタックの変更中および変更後に問題を迅速に検出して対処するプロアクティブモニタリングおよびアラートシステムはありますか?
- ネットワークスタックデプロイの過去の変更失敗率。過去のインシデントからどのような教訓を得ましたか?
- ネットワークアクセスアプローチは、変更の実装をどのように促進または制限するか。このアプローチはサービスの中断を最小限に抑えますか?
- ネットワークアクセスアプローチを含む変更をデプロイすると、本番環境での SaaS サービスの可用性に影響を与えるリスクは何ですか?

コード品質とエンジニアリングチームのパフォーマンス

ネットワークアクセスアプローチは、SaaS サービスのコード品質に間接的に影響を与える可能性があります。ネットワークアクセスが標準化されていないと、エンジニアリングチームが複数の統合アプローチをサポートせざるを得なくなり、コードベースが肥大化する可能性があります。これにより、高いパフォーマンスのエンジニアリングチームを維持するために必要なコード品質の深さと制御をチームが開発する能力が妨げられる可能性があります。

ハイスコア基準

サポートされているネットワークアクセスアプローチ全体でコードのモジュール性と再利用性により、エンジニアリングチームは集中し続けます。ネットワークアクセスアプローチは、既存のデプロイパイプラインや自動テスト戦略と互換性があります。

低スコアインジケータ

ネットワークアクセスアプローチの統合とメンテナンスが多すぎるため、エンジニアリングチームのパフォーマンスが低下します。一部のアプローチでは、機能の欠落や不足に対応するために、複雑さを大幅に増やしたり、技術的負債を発生させたり、回避策の開発を必要としたりします。

自己評価の質問

- ネットワークアクセスアプローチはネットワークの変動性をどのように管理しますか?
- 接続の中断を処理するための追加のコードを開発する必要がありますか?
- 新しいネットワークアクセスアプローチは既存のアプローチとシームレスに統合されていますか、それとも大規模なカスタム開発が必要ですか?
- 新しいネットワークアクセスアプローチを採用するために必要な変更の範囲を教えてください。既存のコードベースと自動テストを効果的に使用できますか?
- 選択したネットワークアクセスアプローチでサービスをデプロイまたは再デプロイするのはどの程度簡単または困難ですか? これは頻繁に実行できますか? エキスパートリソースへの依存関係はありますか?
- ネットワークアクセスアプローチは、コーディング標準とベストプラクティスへの準拠を促進または複雑にしますか?
- このアプローチは、新機能や修正のtime-to-marketにどのように影響しますか?

技術的負債の削減

ネットワークアクセスアプローチが技術的負債に与える影響を評価するには、そのスケーラビリティ、オブザーバビリティ、セキュリティ機能を考慮する必要があります。

ハイスコア基準

このアプローチは、顧客ベースが拡大するにつれてインフラストラクチャ管理を効果的に合理化します。堅牢なオブザーバビリティ機能をout-of-the-box提供します。これにより、効率的なモニタリングとメンテナンスが促進されます。

低スコアインジケータ

ネットワークアクセスアプローチでは、通信チャネルの保護が不十分であり、定性的メトリクスの観測に十分なツールがありません。また、顧客ベースの増加に伴ってインフラストラクチャ管理のための追加の開発が必要になる場合や、信頼性の問題の回避策が必要になる場合もあります。

自己評価の質問

- ネットワークアクセスアプローチは、インフラストラクチャの長期的なスケーラビリティにどのように影響しますか? 追加投資を最小限に抑えてシームレスな成長を促進しますか?
- 含まれているオブザーバビリティツールはどの程度包括的ですか? プロアクティブモニタリングと問題解決は可能ですか?
- 時間の経過に伴うコードベースのメンテナンスと進化に対するネットワークアクセスアプローチの予想される影響は何ですか?
- このアプローチは、既存のインフラストラクチャや計画されたインフラストラクチャとうまく統合されていますか? 大幅な変更や追加が必要ですか?

スケーラビリティ、容量、パフォーマンス

SaaS サービスに対するネットワークアクセスアプローチの適合性を判断するには、需要の増加に応じて最適なパフォーマンスを維持する方法を分析することが重要です。

ハイスコア基準

ネットワークアクセスアプローチにより、シームレスに拡張が容易になります。リクエスト処理中に低レイテンシーを維持し、トラフィックの急増を効率的に処理します。トラフィックレベルの増加に関係なく一貫したパフォーマンスを提供し、増加に運用上の制限を課すことはありません。

低スコアインジケータ

ネットワークアクセスアプローチは、固有の帯域幅制限やインフラストラクチャ容量の不足などが原因で、効果的にスケールされません。リソースのプロビジョニングと管理は複雑さを高め、依存関係を作成します。レイテンシー、ジッター、スループットの変動性の増加、特に混雑したネットワーク状況により、サービスのパフォーマンスが低下します。

自己評価の質問

- ネットワークアクセスアプローチは、増加するテナントとそのデータボリュームにどのように対応しますか?
- 将来の需要を満たすために本質的にスケーラブルですか?
- ピークトラフィック期間や急激なスケーリングイベントでも、パフォーマンスが一貫していることを確認するには、どのような対策を実施していますか?
- このアプローチは、ネットワークレイテンシーとジッターをどのように処理しますか? データスループットを最適化し、遅延を最小限に抑えるメカニズムはありますか?

- ネットワークアクセスアプローチは、さまざまなネットワーク条件に適応できますか? すべてのお客様にシングルテナントエクスペリエンスを提供できますか?
- ネットワークアクセスアプローチが基盤となるインフラストラクチャに与える影響は何ですか? 既存のシステムに大幅なアップグレードや変更が必要ですか?

SaaS サービスのネットワークアクセスに関連するオペレーショナルエクセレンスメトリクス

このセクションでは、以下のメトリクスについて説明します。

- 運用レジリエンスとディザスタリカバリ
- サービスおよびアプリケーションのパフォーマンスモニタリング

運用レジリエンスとディザスタリカバリ

ネットワークアクセスアプローチは、SaaS サービスがさまざまな種類の中断に耐え、災害から迅速に回復するのに役立ちます。

ハイスコア基準

確立されたテスト済みのディザスタリカバリ計画は、ネットワークアクセスアプローチがディザスタリカバリ要件を満たしていることを一貫して示しています。ネットワークアクセスアプローチは高可用性設定をサポートし、自動、迅速、信頼性の高いフェイルオーバーメカニズムをサポートします。

低スコアインジケータ

ネットワークアクセスアプローチにより、一貫したディザスタリカバリ戦略を構築するのが困難になります。中断後、復旧時間が長くなります。ネットワークインフラストラクチャの頻繁な運用上の障害は、サービス提供に影響を与えています。

自己評価の質問

- 前回のディザスタリカバリドリルはいつ行われ、どのような結果になりましたか?
- 中断後の重要なサービスの復旧にはどのくらいの時間がかかりますか? ネットワークインフラストラクチャのどの部分を再デプロイする必要がありますか?
- ディザスタリカバリ計画を合理化するために、ネットワークインフラストラクチャにどのような改善を加えることができますか?

- 最も重要なネットワークコンポーネントに冗長性がありますか?
- 重大な停止後にネットワークインフラストラクチャの再デプロイの可能性を自動化しましたか?
- ネットワークアクセスアプローチは耐障害性と信頼性をどのようにサポートしていますか? ネットワークの中断を処理し、データの整合性を維持するための組み込みメカニズムはありますか?

サービスおよびアプリケーションのパフォーマンスモニタリング

ネットワークアクセスアプローチは、最適なオペレーションとサービスの稼働時間を検証するために使用されるパフォーマンスモニタリングツールに影響を与える可能性があります。サービスによっては、低レベルのメトリクス (パケットドロップレートなど) または高レベルのメトリクス (セッション期間など) にアクセスできる場合があります。低レベルのメトリクスは、ネットワークの動作に関する詳細な技術的洞察を提供しますが、解釈が複雑になる場合があります。対照的に、高レベルのメトリクスは、ユーザーエクスペリエンス全体を測定するより直接的で簡単な方法を提供することがよくあります。これは、基盤となるネットワーク状態の影響をサービス品質の明確な指標に集約するためです。

ハイスコア基準

ほぼリアルタイムのインサイトを提供する包括的なモニタリングツールがすぐに利用できます。パフォーマンスの問題に対処する自動アラートおよび応答システムがあります。ユーザーに影響を与える前に、潜在的なサービスのボトルネックや障害を予測できます。

低スコアインジケータ

頻繁なサービスの中断やパフォーマンスの問題は、観察されたり対処されたりすることなく発生します。サービスパフォーマンスを可視化できないと、パフォーマンスのボトルネックへの対応が遅くなります。ネットワークインフラストラクチャの問題をトラブルシューティングするには、マルチパーティーチームが必要です。

自己評価の質問

- 現在利用可能なモニタリングツールとネットワークインフラストラクチャメトリクス サービス異常の検出にどの程度効果的ですか?
- パフォーマンスの問題はどのくらい迅速に特定して解決できますか?
- 潜在的なパフォーマンスの問題を予測するメカニズムはありますか?
- オブザーバビリティ機能を強化するためにどのような改善を加えることができますか?

SaaS サービスのネットワークアクセスに関連するセキュリティとガバナンスのメトリクス

このセクションでは、以下のメトリクスについて説明します。

- セキュリティ、コンプライアンス、脆弱性の管理

セキュリティ、コンプライアンス、脆弱性の管理

セキュリティ標準への準拠や脆弱性の管理など、ネットワークアクセスアプローチのセキュリティ側面を評価することが重要です。

ハイスコア基準

ネットワークアクセスアプローチは、チームが国際標準化機構 (ISO) 27001、System and Organization Controls 2 (SOC 2) 、NIST などのセキュリティフレームワークに準拠するのに役立ちます。これにより、定期的なセキュリティ監査を簡単に実行できます。強力な暗号化と認証メカニズムが導入されています。ネットワークは分離され、必要なリソースのみが顧客のインフラストラクチャに公開されます。過剰なオーバーヘッドなしで、ネットワーク異常をほぼリアルタイムで検出できます。

低スコアインジケータ

ネットワークアクセスアプローチは、セキュリティ違反や脆弱性が繰り返し発生する傾向があり、主要なセキュリティ標準に準拠していません。セキュリティインシデントの検出と対応が遅れることがよくあります。

自己評価の質問

- 選択したネットワークアクセスアプローチにリンクされた最近のセキュリティ違反はありますか。また、それらから何を学びましたか。
- ネットワークアクセスアプローチは、グローバルセキュリティ標準にどのように準拠していますか?
- セキュリティの脅威を検出して対応するのにどれくらいの時間がかかりますか? ネットワークアクセスは、この機能をどのように支援または制限しますか?
- ネットワークアクセスアプローチでセキュリティ評価はどのくらいの頻度で実施されますか? 一般的なツールを使用してネットワークアクセスアプローチのセキュリティを評価することはできますか、それとも特殊なソフトウェアが必要ですか?

- ネットワークアクセスアプローチにはどのようなレベルのセキュリティが固有のものであり、業界のベストプラクティスや規制要件とどのように整合していますか?

SaaS サービスの AWS ネットワークサービスの概要

このセクションでは、このガイドで参照される AWS ネットワークサービスについて説明します。また、それらの機能を比較し、各サービスのセキュリティ上の考慮事項についても説明します。

このセクションは、以下のトピックで構成されます。

- AWS ネットワークサービス
- サービス機能の比較
- セキュリティ機能と考慮事項

AWS ネットワークサービス

このガイドで一貫して説明 AWS のサービス されている を次に示します。

AWS PrivateLink

AWS PrivateLink は、顧客が既に で運用されている場合に SaaS サービスへのアクセスを提供するクラウドネイティブサービスです AWS クラウド。顧客はインターフェイス VPC エンドポイントを介して SaaS サービスに接続します。これは、お客様の の 1 つ以上のサブネットにプロビジョニングされるエンドポイントネットワークインターフェイスです AWS アカウント。このガイドのシナリオでは、トラフィックはインターフェイス VPC エンドポイントを通過し、アカウントの Network Load Balancer に到着します。Network Load Balancer は、エンドポイントサービスとして登録した SaaS アプリケーションにトラフィックを転送します。リソース VPC エンドポイントを通じて、AWS PrivateLink はデータベースなどの他のリソースへのアクセスにも役立ちます。

Amazon VPC Lattice

Amazon VPC Lattice は、SaaS プロバイダーが複数の VPCs および で運用している顧客にサービスを安全かつ効率的に提供できるようにするアプリケーションネットワークサービスです AWS アカウント。顧客は VPC Lattice を介して SaaS サービスにアクセスします。これにより、一貫したネットワーク接続、堅牢なアクセスコントロール、高度なトラフィック管理が提供されます。これらのシナリオでは、トラフィックは VPC Lattice を介して登録されたアプリケーションサービスに流れます。使用するコンピューティングサービスに関係なく、スケーラブルで安全な通信を提供します。

VPC ピアリング

VPC ピアリングは、プライベート IPv4 アドレスまたは IPv6 アドレスを使用してトラフィックをルーティングする 2 つの仮想プライベートクラウド (VPCs) 間のネットワーク接続です。VPC ピア接続は通常、同じ組織内のエンティティなど、信頼されたエンティティ間で使用されます。顧客が VPCs の 1 つへのピアリングリクエストを作成します。これを受け入れると、トラフィックは両方の VPCs間でどちらの方向にも流れる可能性があります。この接続アプローチは、中間サービスやインフラストラクチャを管理せずに 2 つの VPCs 間で直接通信する必要があるため、その一意性が際立っています。

AWS Transit Gateway

AWS Transit Gateway は、VPCs、仮想プライベートネットワーク (VPN) 接続、AWS Direct Connect ゲートウェイ、VPC 内のサードパーティーの仮想アプライアンス、およびその他のトランジットゲートウェイを接続できる一元化されたネットワークトランジットハブです。トランジットゲートウェイは、アタッチメントごとに異なるルートテーブルを持つことができます。これにより、ルーティングの柔軟性が最大限に高まり、ネットワークを分離するのに役立ちます。多くの場合、多くの VPCsまとめて接続したり、一元的な検査を行ったりするために使用されます。

AWS Site-to-Site VPN

AWS Site-to-Site VPN は、インターネットプロトコルセキュリティ (IPsec) テクノロジーを使用して、オンプレミスネットワーク、リモートオフィス、ファクトリー、その他のクラウドプロバイダー、 AWS グローバルネットワーク間の接続を確立できます。接続は、 の VPC 内の仮想プライベートゲートウェイまたはトランジットゲートウェイから、 、オンプレミス AWS クラウド、または別の CSP のクラウドにある物理またはソフトウェアベースのカスタマーゲートウェイ AWS クラウド に確立されます。接続は、インターネットまたは物理 AWS Direct Connect 接続を介して行うことができます。を使用して Site-to-Site VPN 接続を高速化することもできます AWS Global Accelerator。高速接続はトラフィックを AWS エッジロケーションにルーティングし、レイテンシーを短縮してパフォーマンスを向上させます。

AWS Direct Connect

AWS Direct Connect は、オンプレミスのデータセンターと の間に高速なプライベート接続を確立します AWS クラウド。パブリックインターネットをバイパスすることで、 は へのより信頼性が高く、安全で、一貫した低レイテンシーの接続 Direct Connect を提供します AWS クラウド。お客様はいずれかのDirect Connect ロケーションに接続し、ホスト接続または専用接続を選択します AWS。

これは SaaS サービスのまれなアーキテクチャ選択ですが、大企業コンシューマーが少ないが大規模な SaaS プロバイダーに適しています。

サービス機能の比較

次の表は、このガイドで説明 AWS のサービス されている でサポートされている機能の概要を示しています。以下は、この表に含まれる機能の説明です。

- 重複する CIDR 範囲 – 同じ CIDR 範囲または重複する CIDR 範囲を持つ 2 つ以上のネットワークを接続できます
- 双方向通信 – 双方向通信チャネルをサポートして、SaaS コンシューマーがデータベースなどの内部リソースを SaaS プロバイダーに公開できるようにします。
- IPv6 – シングルスタックまたはデュアルスタックの IPv6 をサポート 可能
- ジャンボフレーム – 最大 8,500 バイトのフレームサイズのジャンボフレームをサポート
- Hybrid-cloud – オンプレミスネットワークへの接続をサポート可能
- マルチクラウド – さまざまなクラウドサービスプロバイダー上のネットワーク間の接続をサポート可能

サービスまたはアプローチ	CIDR 範囲の重複	双方向通信	IPv6	ジャンボフレーム	ハイブリッドクラウド	マルチクラウド
VPC ピアリング接続	いいえ	はい	はい	はい[5]	いいえ	いいえ
AWS PrivateLink	はい	はい [1]	はい	はい	No[6]	No[6]
Amazon VPC Lattice	はい	はい [1]	はい	はい	No[6]	No[6]
AWS Transit Gateway	いいえ	はい	はい	はい	はい[3]	はい[3]

AWS Site-to-Site VPN	いいえ	はい	はい	いいえ	はい	はい
AWS Direct Connect	いいえ	はい	はい	はい [2]	はい	はい
パブリックインターネットアクセス[4]	該当しない	いいえ	はい	はい	はい	はい

1. Amazon VPC Lattice での VPC リソースの使用
2. プライベート仮想インターフェイスとトランジット仮想インターフェイスのみ
3. Site-to-Site VPN または AWS Direct Connect アタッチメントを使用
4. Application Load Balancer など、アプリケーションをパブリックにアクセス可能にする AWS リソースの一般的な用語
5. 1 つの 内のピアリング接続のみ AWS リージョン
6. 環境間の既存の Layer 3 接続を介して可能

セキュリティ機能と考慮事項

次の表は、このガイドで説明 AWS のサービス されている のセキュリティ機能の概要を示しています。

- 認証の方法 – 顧客だけがサービスに接続できるようにする方法。受信リクエストの別のレベルの認証は通常、特に共有テナント環境では依然として必要です。
- 転送中の暗号化 – 転送中の暗号化がデフォルトで提供されているかどうかを示します。ネイティブ暗号化とは、VPCs 間、 VPCs またはデータセンター間のすべてのトラフィックに対して AWS が提供する暗号化を指します。補足暗号化とは、ユーザーが制御し、それぞれのサービスで停止できる暗号化のことです。

サービスまたはアプローチ	認証の方法	転送時の暗号化

VPC ピアリング接続	顧客の AWS アカウント および VPC へのピアリングリクエストを開始するか、開始したリクエストを受け入れます。「VPC ピアリング接続の承諾または拒否」を参照してください。	ネイティブ暗号化のみ
AWS PrivateLink	サービスへのエンドポイントの作成 AWS アカウント を許可する を選択します。これらのアカウントは、許可されたプリンシパルと呼ばれます。「接続リクエストを承諾または拒否する」を参照してください。	ネイティブ暗号化のみ
Amazon VPC Lattice	VPC Lattice サービスまたはサービスネットワークを顧客の と共有します AWS アカウント。「VPC Lattice エンティティを共有する」を参照してください。	ネイティブ暗号化と補足 TLS 暗号化
AWS Transit Gateway	顧客が からピアリングアタッチメントリクエストを作成するか AWS アカウント、リクエストを開始します。Amazon VPC Transit Gateway の「Transit Gateway ピアリングアタッチメント」を参照してください。	VPN アタッチメントを使用したネイティブ暗号化と補足的な IPsec 暗号化

AWS Site-to-Site VPN	顧客のデバイスで IPsec 事前共有キーまたはプライベート証明書を使用します。AWS Site-to-Site VPN 「トンネル認証オプション」を参照してください。	補足 IPsec 暗号化
AWS Direct Connect	お客様は、 から仮想インターフェイスリクエストを作成します AWS アカウント。Direct Connect 仮想インターフェイスとホスト仮想インターフェイスを参照してください。	選択したサイトで可能な補足レイヤー 2 暗号化。Direct Connect 「ロケーション」を参照してください。
パブリックインターネットアクセス[1]	カスタム認証が必要です。	追加の TLS 暗号化が可能

1. Application Load Balancer など、アプリケーションをパブリックにアクセス可能にする AWS リソースの一般的な用語

SaaS サービスのネットワークアクセスオプションの評価

組織にとって重要なメトリクスは、顧客層、ビジネス戦略、組織目標によって異なります。このガイドでは、ネットワークアクセスアプローチを選択するために使用できるメトリクスを示しますが、ユースケースの固有の要件を満たすメトリクスを優先する必要があります。

このセクションは、以下のトピックで構成されます。

- 評価メトリクス
- 合計所有コスト
- ネットワーク値マップ

評価メトリクス

一部のメトリクスは組織やユースケース間で一貫性があり、これらは評価に役立つメトリクスです。以下は、これらのメトリクスです。

- 統合の容易さ – 新規顧客をどのくらい迅速かつ簡単にオンボーディングできますか？
- 総所有コスト (TCO) — コスト構造は何ですか？ 固定インフラストラクチャコストと変動インフラストラクチャコスト以外にも、運用上のオーバーヘッド、エキスパートへの依存、変更の実装コスト、コンプライアンスに関連するコストに関する重要な追加考慮事項があります。詳細については「合計所有コスト」セクションを参照してください。
- スケーラビリティ – ネットワークアクセスアプローチは、会社の成長をサポートするためにスケールできますか？ 顧客ベースのスケーリングには、アーキテクチャと組織の重要な考慮事項があります。現在サポートしている顧客の 5 ~ 100 倍に対応するようにスケールする方法を検討してください。
- 適応性 – 変更を簡単に実装できますか？ 変更には、新しいアプリケーション、新機能、別のプラットフォーム、または別のネットワークが含まれる場合があります。
- ネットワーク分離 — 顧客に公開しているネットワークインフラストラクチャの量 適切なアクセスレベルを提供しているか、ネットワーク全体を公開しているか。ネットワークリソースを早期に分離すると、セキュリティ、プライバシー、コンプライアンスの保証を後で提供しやすくなります。
- オブザーバビリティ — サービスの障害や機能低下を検出するにはどうすればよいですか？ 問題を特定するのはどれくらい簡単で高速ですか？ 顧客が障害点を理解し、解決するのに役立つのは、どのくらいの速さ (およびオーバーヘッド) ですか？

- 修復までの時間 — サービス障害または機能低下を検出してからオペレーションを再開するまでのリードタイムはどれくらいですか？ この能力に影響を与える要因は何ですか？

その他のメトリクスは、ビジネスオペレーション、戦略、または目標に関連するため、組織やサービスに固有のものです。これらのメトリクスを評価できるのはお客様だけです。以下は、これらのメトリクスです。

- ビジネスモデルの調整 — ビジネスモデルとは何ですか。また、個々のアクセスアプローチはどの程度それに合っていますか。
- 総アドレス可能市場 (TAM) – 現在および将来の市場はどの程度ですか。また、ネットワークアクセスアプローチによってどの程度カバーされていますか。
- 投資利益率 (ROI) — 利益率とマージンにはどのような改善が期待されますか？ 予想される財務上の利点は、適応可能で柔軟なサービスアクセスのニーズを満たすのに十分ですか？
- 規制コンプライアンス – どのような規制要件が適用され、どの市場に当てはまりますか？
- サービスレベルアグリーメント (SLAs) – 顧客は SaaS サービスを高可用性にする必要がありますか？ 契約上、どのようなコミットメントを維持する義務がありますか？

合計所有コスト

このセクションでは、総所有コスト (TCO) について説明します。TCO は、ネットワークアクセスアプローチの比較に使用される評価メトリクスの 1 つです。TCO は、固定および可変インフラストラクチャコスト、運用オーバーヘッド、スペシャリストの依存関係、変更コスト、コンプライアンスコストで構成される複合メトリクスです。

各ネットワークアクセスアプローチの TCO 評価は、ユースケースによって異なる場合があります。例えば、シンプルなウェブサービスと 5 つのテナントを持つ SaaS プロバイダーの変更コストは、複雑で相互接続された製品ポートフォリオと数百または数千のテナントを持つ SaaS プロバイダーとは異なります。さらに、すべてのコンポーネントが同じ重みを持つわけではありません。たとえば、ネットワーキングスペシャリストの雇用は、サービスの個々のデプロイをサポートするインフラストラクチャコストよりもコストがかかることがよくあります。次の表の値は、最初の方向と詳細な説明の参照点として使用します。

アクセスアプローチ	固定インフラストラクチャコスト	インフラストラクチャ	運用オーバーヘッド	スペシャリストの依存関係	変更コスト	コンプライアンスコスト

		コストの変動				
VPC ピアリング接続	なし	なし	高	低	高	中程度
AWS PrivateLink	低	低	低	なし	低	低
Amazon VPC Lattice	Medium	中	低	低	低	低
AWS Transit Gateway	Medium	中	低	低	低	Medium
AWS Site-to-Site VPN	Medium	高い	高	中	中	低
AWS Direct Connect	高	中	Medium	高い	高	低
パブリックインターネットアクセス	低	高	中程度	低	低	高

VPC ピアリングのコスト

VPC ピアリング接続に関連する直接インフラストラクチャコストはありません。トラフィックが同じアベイラビリティーゾーン内にとどまる場合、データ転送料金はかかりません。ただし、追加のピアリング接続ごとに管理と複雑さが指数関数的に増大するため、運用上のオーバーヘッドが大きくなる可能性があります。ネットワーキングの基本的な理解はピアリング接続を設定するのに十分ですが、ネットワーク上の変更は、少数のピアリング接続では実装が困難です。両当事者が個々のサー

ビスではなく VPC 全体を相互に公開しているため、コンプライアンスコストはわずかに高くなります。

AWS PrivateLink コスト

AWS PrivateLink は、運用上のオーバーヘッドが小さい費用対効果の高いソリューションです。これは、SaaS プロバイダーが Network Load Balancer のみを管理し、コンシューマーが VPC エンドポイントのみを管理する必要があるためです。両側を透過的に変更できるため、コストとリソースを大量に消費する組織間のコラボレーションを削減できます。SaaS プロバイダーがネットワーク全体ではなく、希望するサービスのみを公開しているため、コンプライアンスコストは低い傾向があります。

Amazon VPC Lattice のコスト

Amazon VPC Lattice は、中程度の固定および可変インフラストラクチャコストでバランスの取れたコスト構造を提供します。フルマネージド型のサービスネットワークとして、複数の VPCs。これにより、手動ネットワーク設定と比較して、初期デプロイと継続的な管理の両方が簡素化されます。複雑なルーティング更新なしでポリシーベースのコントロールを通じて変更を実装できるため、ネットワークスペシャリストへの依存を軽減できます。VPC Lattice は、組み込みのモニタリングおよびログ記録機能を通じてきめ細かなアクセスコントロールと包括的な可視性を提供するため、コンプライアンスコストは従来のネットワークアプローチよりも低くなる傾向があります。これにより、規制コンプライアンスの実証が容易になります。

AWS Transit Gateway コスト

AWS Transit Gateway では、時間単位およびデータ処理料金が よりも高くなりますが AWS PrivateLink、運用上のオーバーヘッドも同様です。すべてのルートテーブルを正しくセットアップ AWS するには、 AWS Transit Gateway でのサービスとルーティングに関する深い知識が必要です。インフラストラクチャの変更には、ルーティングまたは DNS 更新が必要になる場合があります。コンプライアンスコストは VPC ピアリングに似ています。これは、両者がサブネットまたは VPCs している可能性があるためです。 AWS Transit Gateway ルートテーブルは複数のコンシューマーによって共有されるため、注意して処理する必要があり、それらの間のトラフィックを許可してはいけません。

AWS Site-to-Site VPN コスト

Site-to-Site VPN は基本的にインターネットにトラフィックを送信するため、可変コストはデータ転送料金と比較して最も高くなります。マネージド仮想プライベートネットワーク (VPN) サービスで

すが、特にカスタマーゲートウェイでは運用上の大きなオーバーヘッドが発生します。プロビジョニングとオペレーションにはネットワークに関する高度な知識が必要であり、変更には多くの場合、両方の当事者からのアクションが必要です。セキュリティチームは追加のレビューなしで IPsec トンネルを事前承認することがよくあるため、通常、コンプライアンスコストは低くなります。

AWS Direct Connect コスト

AWS Direct Connect は、 へのプライベート物理接続であるため、固定インフラストラクチャコストが最大になります AWS クラウド。ボーダーゲートウェイプロトコル (BGP) セッション (必要な場合) をセットアップして運用し、VPN 接続を運用し、トラフィックエンジニアリングを実行するには、専門知識が必要です。このサービスは、プライベート接続と Media Access Control Security (MACsec) と IPsec 暗号化を追加するオプションをブレンドするため、セキュリティチームの労力を軽減します。

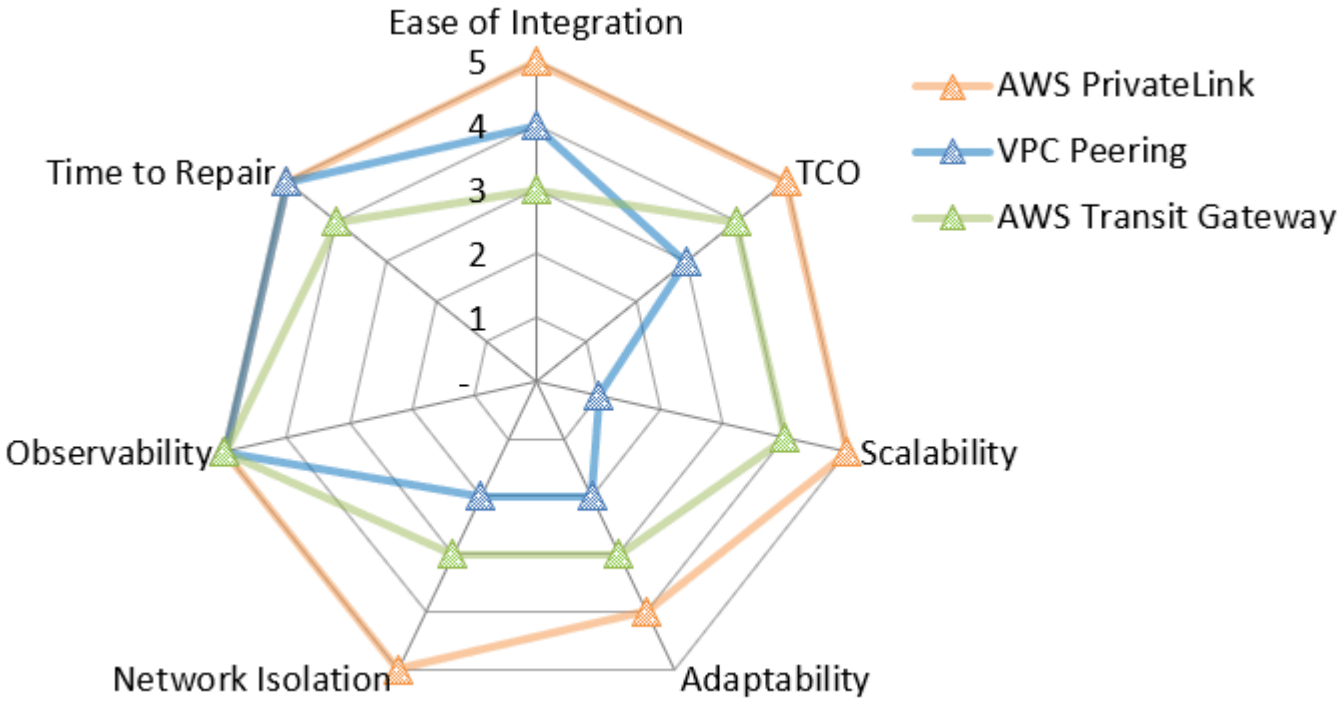
パブリックインターネットアクセスのコスト

パブリックインターネットアクセスとは、Application Load Balancer など、アプリケーションをパブリックにアクセス可能にするために使用できる AWS リソースを指します。このアプローチでは、インターネットへのデータ転送料金など、 サービスへのアクセスの提供に関連する変動コストが発生します。サービスをインターネットに公開し、追加のセキュリティおよび認証メカニズムが必要になるため、運用上のオーバーヘッドとコンプライアンスコストがかかる可能性があります。ただし、複雑なルーティングはなく、どちらの当事者も互いのインフラストラクチャの詳細を知る必要はありません。

ネットワーク値マップ

全体像を把握し、情報に基づいた意思決定を行うために、このガイドには各シナリオのネットワークバリューマップが含まれています。評価はシナリオごとに異なるため、同じサービスのスコアは 2 つのシナリオで異なる場合があります。値マップはレーダーチャートで、架空の完全スコアはすべてのカテゴリで 5 になります。

たとえば、次の図はサンプルのレーダーチャートを示しています。これには、評価に役立つメトリクスのみが含まれます。評価できる追加のメトリクスを含む独自の値マップを作成することをお勧めします。


Ease of Integration
5
4
3
2
1
-
TCO
Scalability
Adaptability
Network Isolation
Observability
Time to Repair
AWS PrivateLink
VPC Peering
AWS Transit Gateway

の SaaS サービスのネットワークアクセスシナリオ AWS クラウド

このセクションでは、 の SaaS サービスのさまざまなネットワークアクセスオプションについて説明します AWS クラウド。ここでは、コンシューマー、 内の接続ニーズを持つ可能性のあるユーザー、オンプレミスのデータセンター AWS クラウド、または他のクラウドサービスプロバイダー (CSPs) の観点からアプローチについて説明します。さらに、複数のタイプのコンシューマー環境からのアクセスをサポートする必要が生じる場合があります。

これらの多様な環境におけるネットワーク接続要件を理解することは、包括的なアクセス戦略を作成する上で不可欠です。アーキテクチャ上の意思決定では、運用効率を維持しながら、さまざまなセキュリティモデル、期待されるパフォーマンス、技術的な制約を考慮する必要があります。適切なアプローチは、ビジネスの成長に合わせてスケールし、実装の複雑さと継続的な管理オーバーヘッドの両方を最小限に抑える、安全で信頼性の高い接続を提供します。

ネットワークアクセスオプションを評価するときは、インフラストラクチャコストだけでなく、運用オーバーヘッドやコンプライアンス要件など、各アプローチが総所有コストにどのように影響するかを検討してください。一部のアプローチはスケーラビリティに優れていますが、複雑になる場合があります。一方、ネットワーク分離を犠牲にして統合の容易さを優先するアプローチもあります。コンシューマーの技術的能力とリソースも、最適なソリューションを決定する上で重要な役割を果たします。

のコンシューマーにとって AWS クラウド、 などのサービスはセキュリティとスケーラビリティに大きな利点 AWS PrivateLink をもたらします。オンプレミスのコンシューマーは、一貫したパフォーマンス AWS Direct Connect のために の恩恵を受けるか、費用対効果の高い接続のために Site-to-Site VPN の恩恵を受ける可能性があります。マルチクラウドシナリオでは、相互運用性の課題を慎重に検討する必要があり、トランジット VPC アーキテクチャを使用してアクセスパターンを標準化する場合があります。いずれの場合も、SaaS サービスの進化に合わせてネットワークアーキテクチャが回復力と適応性を維持できるように、設計は将来のコンシューマーとトラフィックの増加を予測する必要があります。

このセクションでは、以下のシナリオについて説明します。

- で運用されている SaaS コンシューマー AWS
- オンプレミスで運用されているサービスコンシューマー
- 他のクラウドサービスプロバイダーで運用されている SaaS コンシューマー
- ハイブリッド環境のサポート

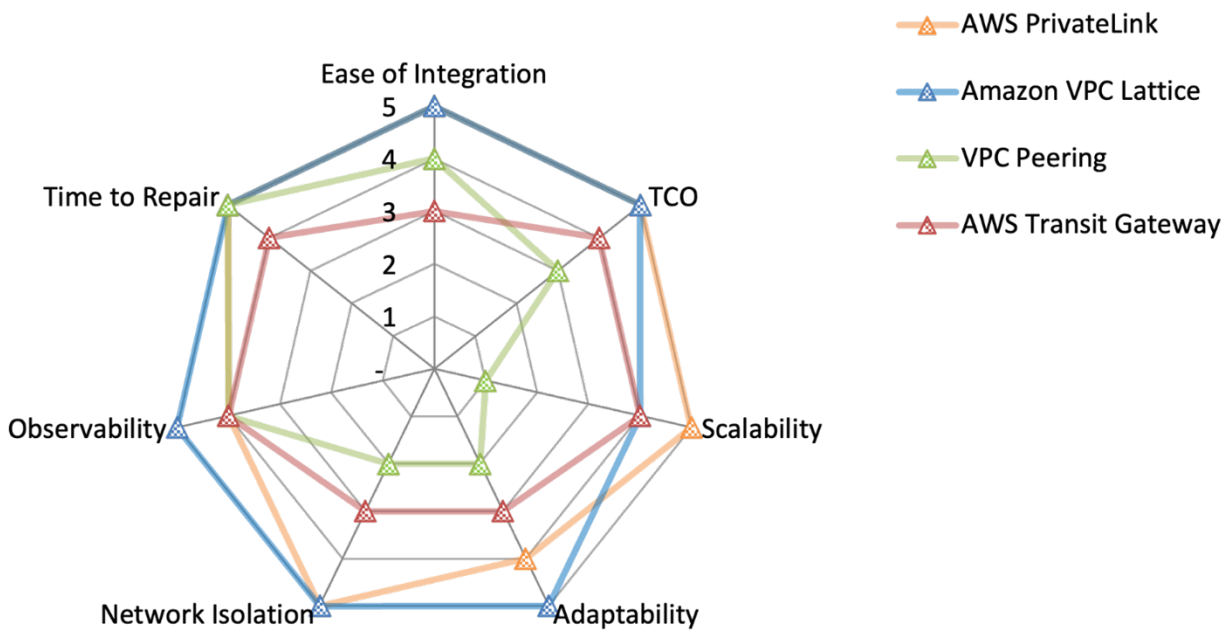
で運用されている SaaS コンシューマー AWS

このセクションでは、お客様とコンシューマーの両方が で運用されている場合の接続オプションについて説明します AWS クラウド。このシナリオは、多くの が AWS のサービス ネイティブに統合され、両方の当事者が AWS のサービス ポートフォリオ全体にアクセスできるため、最大の柔軟性を提供します。

このセクションでは、以下のネットワークアクセスアプローチについて説明します。

- との統合 AWS PrivateLink
- Amazon VPC Lattice サービスの共有
- VPC ピアリング接続の作成
- を使用した VPCs の接続 AWS Transit Gateway

次のネットワーク値マップは、各評価メトリクスの各オプションスコアをまとめたものです。評価メトリクスの詳細については、このガイドの「評価メトリクス」を参照してください。マップでは、5 は最低 TCO、最適なネットワーク分離、修復時間など、最適なスコアを表します。このレーダーチャートの読み方の詳細については、このガイドネットワーク値マップの「」を参照してください。



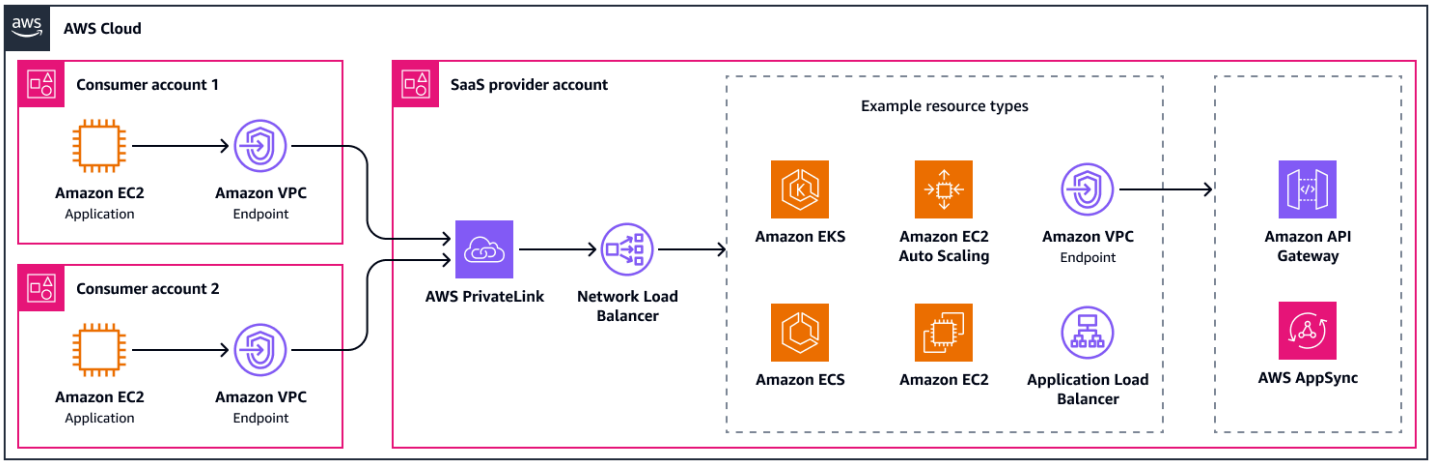
レーダーチャートには、次の値が表示されます。

評価メトリクス	AWS PrivateLink	Amazon VPC Lattice	VPC ピアリング	AWS Transit Gateway
統合のしやすさ	5	5	4	3
TCO	5	5	3	4
スケーラビリティ	5	4	1	4
適応性	4	5	2	3
ネットワーク分離	5	5	2	3
可観測性	4	5	4	4
修復にかかる時間	5	5	5	4

との統合 AWS PrivateLink

AWS PrivateLink は、SaaS サービスを統合する最もクラウドネイティブな方法です。SaaS プロバイダーは、Network Load Balancer の背後でアプリケーションをホストできます。Network Load Balancer は、Application Load Balancer、Amazon Elastic Container Service (Amazon ECS)、Amazon Elastic Kubernetes Service (Amazon EKS)、Auto Scaling グループと直接統合されます。Network Load Balancer からのトラフィックを SaaS プロバイダーアカウントのインターフェイス VPC エンドポイントにルーティングすることもできます。これにより、API を使用して、Amazon API Gateway や などのアプリケーションにアクセスできますAWS AppSync。アプリケーションが、データベースなど、ロードバランシングされていない顧客環境内のリソースにアクセスする必要がある場合は、リソース VPC エンドポイントを使用できます。

AWS PrivateLink は、アベイラビリティーゾーンあたり最大 100 Gbps の帯域幅をサポートします。次の図は、いくつかの統合が可能な基本設定を示しています。2 つのコンシューマーアカウントを SaaS プロバイダーアカウントに接続します AWS PrivateLink。コンシューマーアカウントにサービスエンドポイントがあり、SaaS プロバイダーアカウントに Network Load Balancer があります。



この方法による利点は以下の通りです。

- 統合の容易さ: ルートテーブルの変更は必要ありません
- 統合の容易さ: を通じてエンドポイントサービスを提供 AWS Marketplaceできます。
- 統合の容易さ: VPC エンドポイントがフレンドリ DNS 名をサポート
- スケーラビリティ: 数千の SaaS コンシューマーにスケールできます
- 適応性: CIDR 範囲の重複のサポート
- 適応性: IPv6 のサポート
- 適応性: クロスリージョンサポート
- TCO: AWS PrivateLink はフルマネージド型サービスであるため、運用作業が少なくて済みます
- ネットワーク分離: SaaS プロバイダーからトラフィックを開始できないため、SaaS コンシューマーのセキュリティ上の利点
- ネットワーク分離: サブネットまたは VPC 全体が公開されていないため、SaaS プロバイダーのセキュリティ上の利点

このアプローチの欠点は次のとおりです。

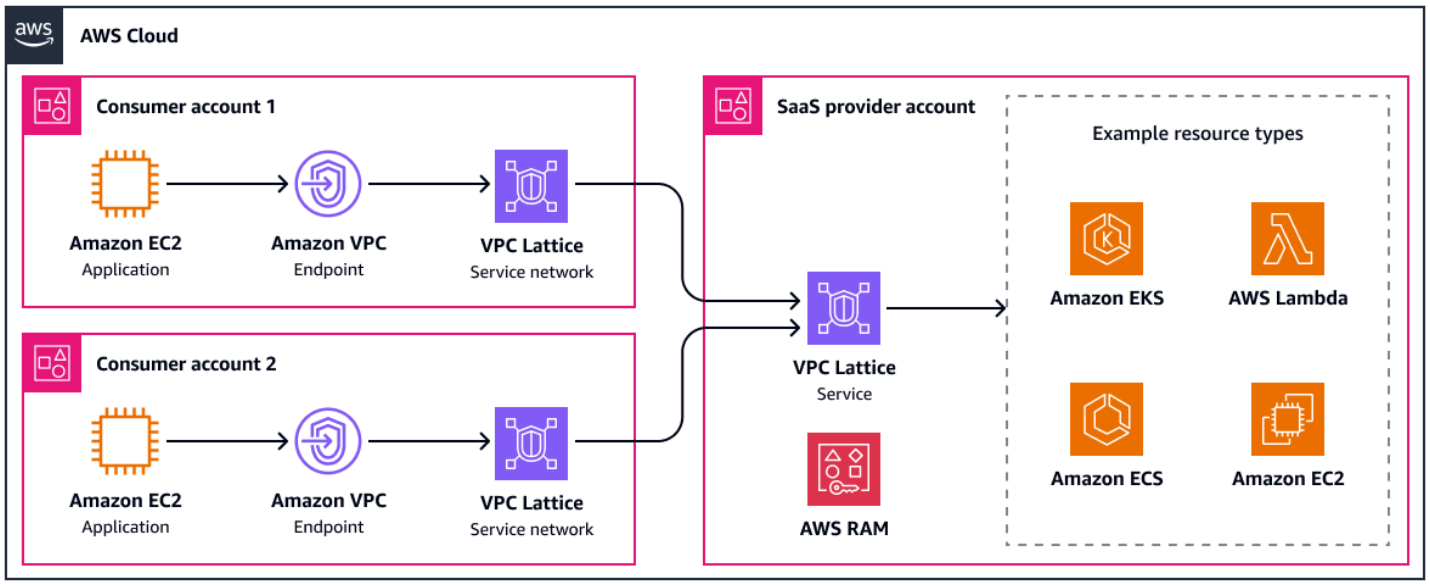
- 適応性: SaaS プロバイダーはコンシューマーと同じアベイラビリティーゾーンを使用する必要があります
- 適応性: クライアントが開始する接続のみをサポートし、サービスが開始する通信にはリソース VPC エンドポイントが必要です
- 適応性: Network Load Balancer は、 AWS PrivateLink

Amazon VPC Lattice サービスの共有

SaaS アプリケーションの接続オプションとして Amazon VPC Lattice を使用するには、まず SaaS アプリケーションコンポーネントを表す 1 つ以上の VPC Lattice サービスを作成します。Amazon EC2 インスタンス、コンテナ、 AWS Lambda 関数などのバックエンドターゲットにトラフィックを送信するようにリスナーとルーティングルールを設定します。詳細については、「VPC Lattice サービスネットワーク内の Saas サービスの接続」(AWS ブログ記事) を参照してください。概念的には、これは Application Load Balancer の設定とほぼ同じです。次に、 AWS Resource Access Manager (AWS RAM) を使用して顧客 AWS アカウント または組織と SaaS サービスを安全に共有し、アクセス許可を指定します。お客様がリソース共有を受け入れると、SaaS サービスを既存または新しく作成された VPC Lattice サービスネットワークに関連付けることで、service-to-service通信が可能になります。

各 VPC Lattice サービスは、アベイラビリティーゾーンごとに 1 秒あたり最大 10 Gbps および 10,000 リクエストをサポートできます。認証ポリシーを実装することで、顧客は SaaS アプリケーションにアクセスできるサービスとリソースをきめ細かく制御できます。リソースゲートウェイを使用して、TCP 接続を必要とするリソースにアクセスできます。たとえば、管理している Amazon EKS クラスターや、アプリケーションがアクセスする必要があるカスタマー管理のリソースなどです。SaaS サービスにリソースゲートウェイを使用する方法の詳細については、「VPC リソース AWS PrivateLink のサポート AWS アカウント を使用して 全体で SaaS 機能を拡張する」(AWS ブログ記事) を参照してください。

次の図は、いくつかの統合例を含む高レベルの VPC Lattice 設定を示しています。カスタマーマネージドサービスネットワークを使用して SaaS アプリケーションにアクセスします。



この方法による利点は以下の通りです。

- 統合の容易さ: ルートテーブルの変更は必要ありません
- 統合の容易さ: すぐに使えるサービス検出
- スケーラビリティ: 数千の SaaS コンシューマーにスケールできます
- 適応性: CIDR 範囲の重複のサポート
- 適応性: IPv6 のサポート
- 適応性: VPC Lattice サービスとして任意の AWS コンピューティングサービスと統合
- TCO: VPC Lattice はフルマネージドサービスであるため、運用作業が少なくて済みます
- TCO: 高度なトラフィックルーティングによる組み込みロードバランシング
- ネットワーク分離: 認証ポリシーによるきめ細かな認可
- ネットワーク分離: SaaS プロバイダーからトラフィックを開始できないため、SaaS コンシューマーのセキュリティ上の利点
- ネットワーク分離: サブネットまたは VPC 全体を公開していないため、SaaS プロバイダーのセキュリティ上の利点

このアプローチの欠点は次のとおりです。

- 適応性: クライアントが開始した接続のみをサポートし、サービスが開始した通信にはリソースゲートウェイが必要です
- 適応性: クロスリージョンサポートなし

VPC ピアリング接続の作成

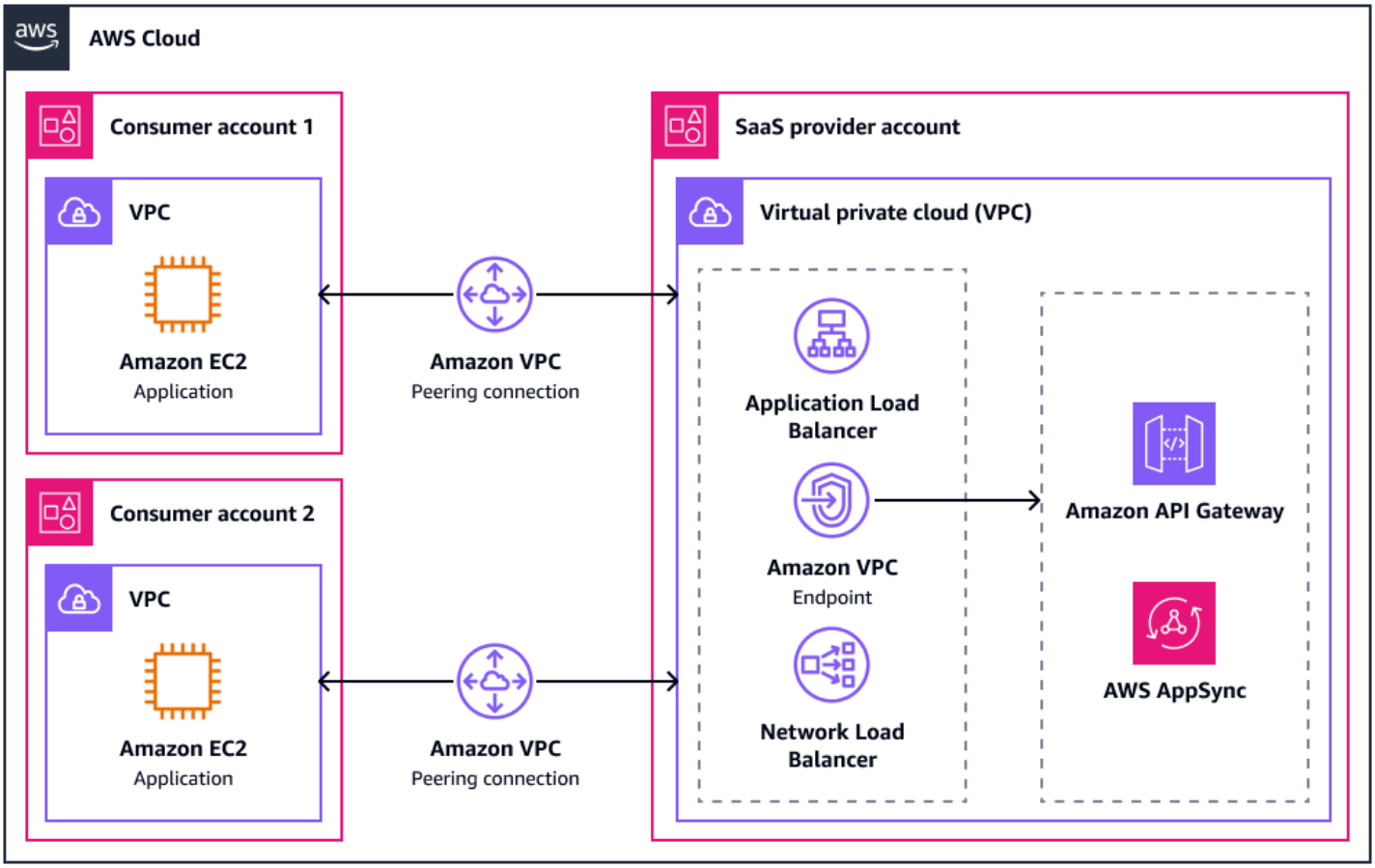
VPC ピアリングを使用して SaaS プロバイダーの VPC をコンシューマーの VPC に接続すると、両者は接続を開始できます。これには、両方のアカウントでセキュリティグループ、ファイアウォール、ネットワークアクセスコントロールリスト (NACLs) を適切に設定する必要があります。そうしないと、不要なトラフィックがピアリング接続を介してネットワークに入る可能性があります。セキュリティグループを使用して、ピア接続された VPCs からセキュリティグループを参照できます。これは、許可リストのセキュリティグループが許可リストの IP アドレスと比較してより明示的で詳細なアクセスコントロールを提供するため、アプリケーションへのアクセスを制御するのに役立ちます。

VPC ピアリングを使用すると、VPC にデプロイされたサービスまたはリソースを通じて SaaS サービスにアクセスできます。ほとんどの SaaS アプリケーションは Application Load Balancer または

Network Load Balancer の背後にあります。 AWS AppSync プライベート APIsまたは Amazon API Gateway プライベート APIs は、インターフェイス VPC エンドポイントを介したピアリング接続のターゲットになる可能性があるため、SaaS アプリケーションへの他の一般的なエントリポイントです。

ピアリング接続を確立したら、両方のアカウントの VPCs のルートテーブルを更新して、ピアリング接続をそれぞれの CIDR 範囲のネクストホップとして定義する必要があります。このソリューションは、複数のピアリング接続の管理がすぐに複雑になるため、コンシューマーが少ない SaaS プロバイダーにのみ推奨されます。

次の図は、いくつかの統合が可能な基本設定を示しています。2 つのコンシューマーアカウントの VPCs には、SaaS プロバイダーアカウントの VPC とのピアリング接続があります。



この方法による利点は以下の通りです。

- 修復までの時間: 通信の単一障害点がない
- スケーラビリティ: VPC ピアリングに対する帯域幅の制限なし

- TCO: ピアリング接続または同じアベイラビリティーゾーン内のピアリング接続経由のトラフィックにはコストがかかりません
- TCO: 管理するインフラストラクチャがない
- 適応性: IPv6 のサポート
- 適応性: リージョン間ピアリングをサポート

このアプローチの欠点は次のとおりです。

- 適応性: 推移的ルーティングはサポートされていません
- 適応性: CIDR 範囲の重複はサポートされていません
- スケーラビリティ: スケーラビリティの制限 (VPC あたり最大 125 個のピアリング接続)
- TCO: ピアリング接続を追加するたびに複雑さが指数関数的に増加
- TCO: ルートテーブルの管理、ピアリング接続自体、セキュリティグループルール、トラフィック検査のオーバーヘッド
- ネットワーク分離: 両当事者の VPCs全体が公開されるため、厳格なセキュリティコントロールが必要

を使用した VPCs の接続 AWS Transit Gateway

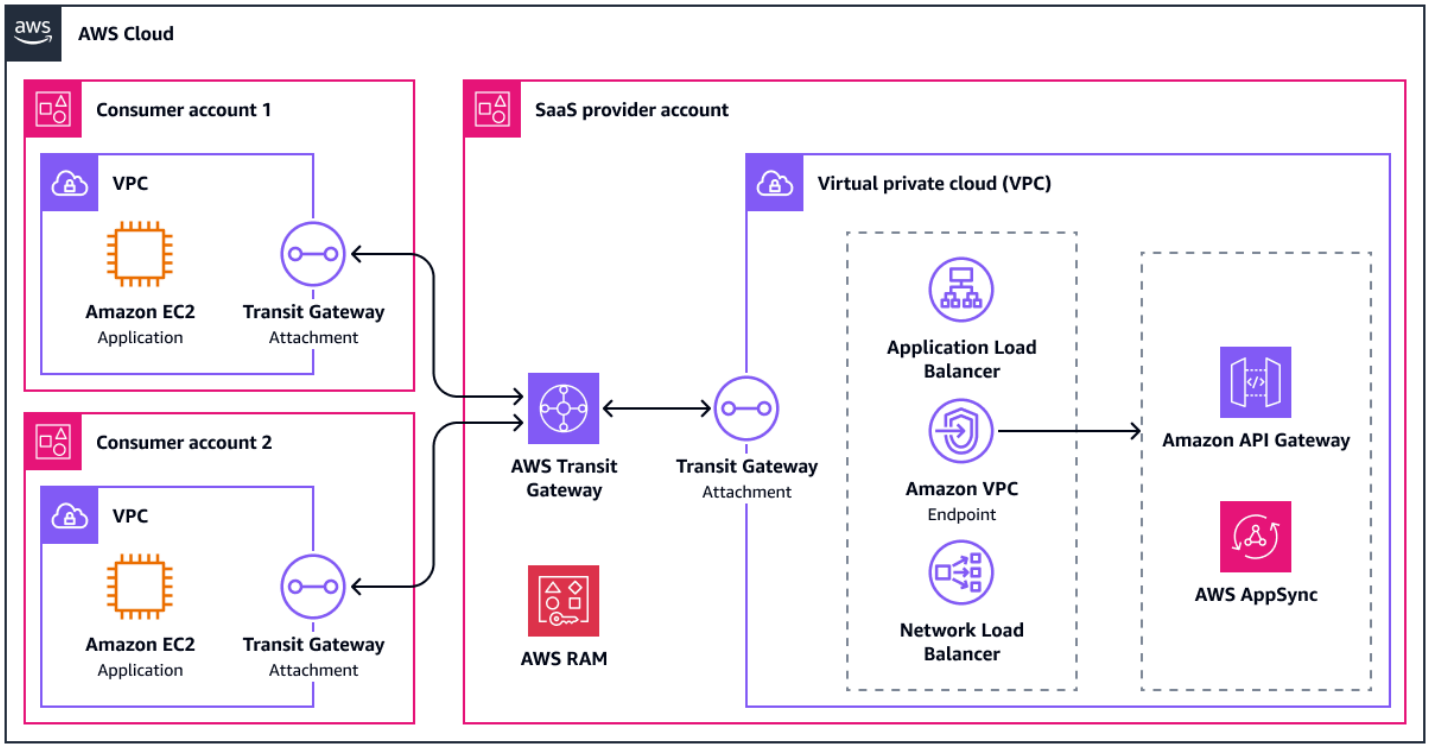
を介して VPCs を接続するとAWS Transit Gateway、VPC アタッチメントが作成され、VPC との間でトラフィックをルーティングする各アベイラビリティーゾーンのサブネットにネットワークインターフェイスがデプロイされます。VPC アタッチメントのすべてのアベイラビリティーゾーンに専用/28サブネットを配置することをお勧めします。詳細については、「Amazon VPC Transit Gateways 設計のベストプラクティス」を参照してください。VPCs は、デプロイされたネットワークインターフェイスを介してトラフィックを送信するために更新されたルートテーブルを必要とし、それに応じて Transit Gateway ルートテーブルを更新する必要があります。マルチテナント設定では、SaaS プロバイダーの VPC にすべてのコンシューマーの VPCs。コンシューマーの VPCs には、SaaS プロバイダーの VPC へのルートのみが必要です。

Transit Gateway は、設計上高可用性です。VPC フローログによるモニタリングをサポートし、Transit Gateway アタッチメントの最大帯域幅はアベイラビリティーゾーンあたり 100 Gbps です。VPC ピアリングと同様に、このアプローチによりクロス VPC セキュリティグループ参照が可能になり、環境間のアクセスコントロールが簡素化されます。

Transit Gateway を使用して SaaS サービスにコンシューマーを接続するには、主に 2 つのオプションがあります。

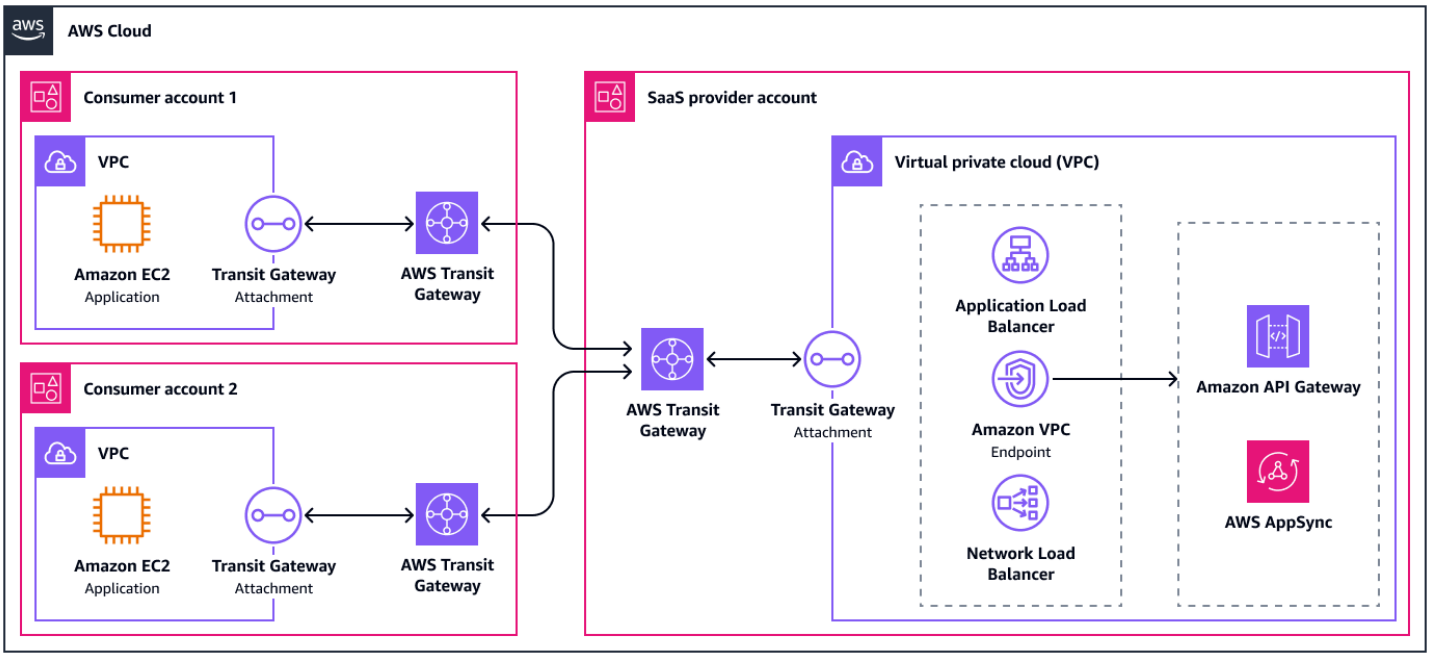
オプション 1: RAM の使用

最初のオプションでは、サービスプロバイダーは () を使用して Transit Gateway をコンシューマーと共有します。 AWS Resource Access ManagerAWS RAMこれにより、コンシューマーは自分のアカウントに VPC アタッチメントをデプロイできます。次の図は、このオプションを大まかに示しています。



オプション 2: ピア接続トランジットゲートウェイ

2 番目のオプションは、トランジットゲートウェイをコンシューマーのアカウントのトランジットゲートウェイとピアリングすることです。これにより、トランジットゲートウェイ内のルートテーブルを完全に制御できるため、コンシューマーはより柔軟になります。例えば、サービスとワークロードの間に一元的な検査を設定できます。このオプションの欠点は、トランジットゲートウェイ間の静的ルーティングのみがサポートされていることです。次の図は、このオプションを大まかに示しています。



この方法による利点は以下の通りです。

- スケーラビリティ: 最大 5,000 個のアタッチメントをサポート
- スケーラビリティ: 接続されたすべての VPCsを 1 か所で管理およびモニタリング
- 適応性: Transit Gateway は VPNs、 Direct Connect ゲートウェイ、およびサードパーティー SD-WAN アプライアンスにアタッチすることもできます
- 適応性: 検査 VPC の追加などの柔軟なアーキテクチャ
- 適応性: 推移的ルーティングのサポート
- 適応性: リージョン内およびリージョン間のトランジットゲートウェイをピアリングできます
- 適応性: IPv6 のサポート
- TCO: AWS Transit Gateway はフルマネージド型サービスであるため、運用作業が少なくて済みます
- TCO: 追加の Transit Gateway アタッチメントごとに TCO が直線的に増加

このアプローチの欠点は次のとおりです。

- 統合のしやすさ: ルーティング設定には高度なネットワーク知識が必要です
- 適応性: CIDR 範囲の重複はサポートされていません
- TCO: ルートテーブルエントリ、セキュリティグループルール、トラフィック検査の管理によるオーバーヘッド

- セキュリティ: 両当事者の VPCs全体が公開されるため、厳しいセキュリティコントロールが必要

オンプレミスで運用されているサービスコンシューマー

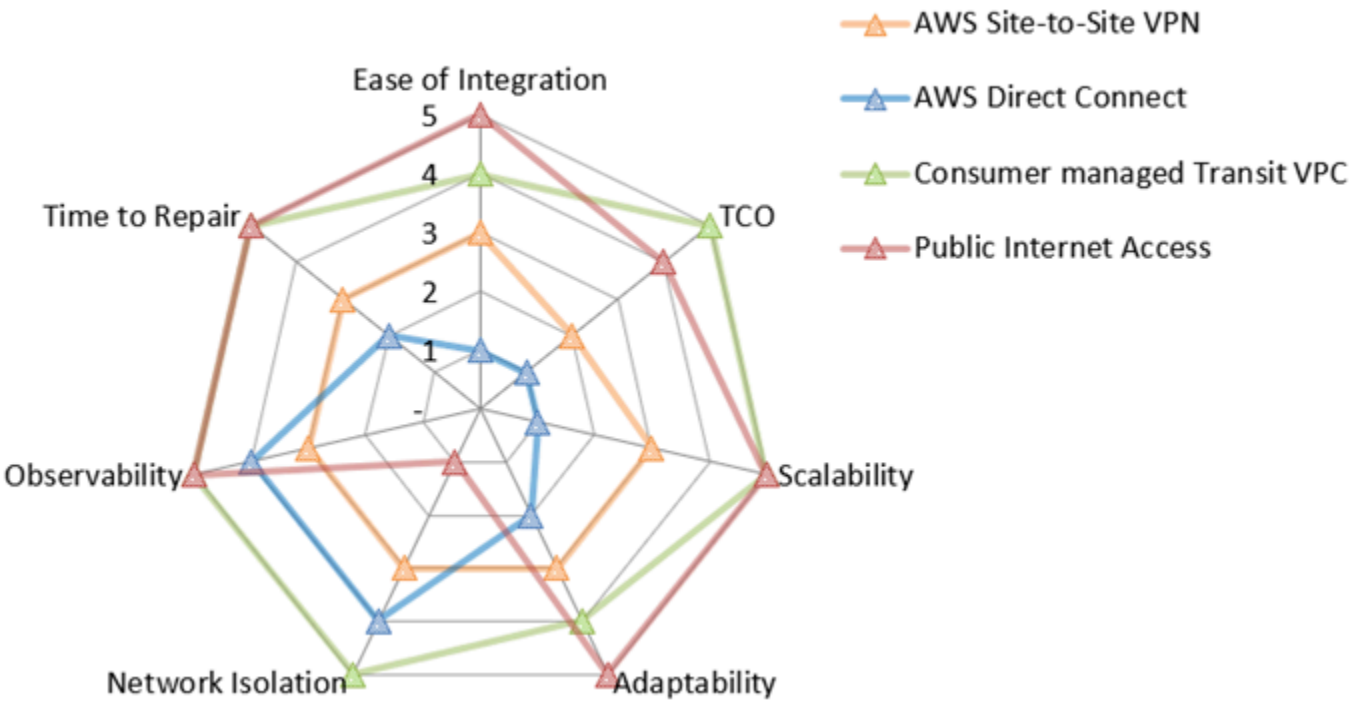
このセクションでは、 の AWS クラウド SaaS ワークロードとオンプレミスデータセンター間の接続オプションについて説明します。オンプレミスの要件を持つ多くのコンシューマーは、特にエンタープライズレベルで、クラウドを物理ネットワークの拡張と見なし、それをアーキテクチャに反映したいと考えています。つまり、論理トンネルまたはプライベート物理接続を介して、クラウド内の SaaS サービスへのプライベート接続が可能になります。他のコンシューマーは、このセクションでも説明されているパブリックインターネット経由の接続を受け入れます。

このセクションでは、以下のネットワークアクセスアプローチについて説明します。

- との接続 AWS Site-to-Site VPN
- との接続 AWS Direct Connect
- トランジット VPC アーキテクチャとの接続
- パブリックインターネットを介した接続

次のネットワーク値マップは、各評価メトリクスの各オプションスコアをまとめたものです。評価メトリクスの詳細については、このガイドの「評価メトリクス」を参照してください。マップでは、5 は最低 TCO、最適なネットワーク分離、修復時間など、最適なスコアを表します。このレーダーチャートの読み方の詳細については、このガイドネットワーク値マップの「」を参照してください。

> **Note**
>
> プロバイダー管理のトランジット VPC オプションは、スコアがどのサービスが運用されているかに大きく依存するため、除外されます。



レーダーチャートには、次の値が表示されます。

評価メトリクス	AWS Site-to-Site VPN	AWS Direct Connect	コンシューマー管理のトランジット VPC	パブリックインターネットアクセス
統合のしやすさ	3	1	4	5
TCO	2	1	5	4
スケーラビリティ	3	1	5	5
適応性	3	2	4	5
ネットワーク分離	3	4	5	1
可観測性	3	4	5	5
修復にかかる時間	3	2	5	5

との接続 AWS Site-to-Site VPN

AWS Site-to-Site VPN 接続は、仮想プライベートゲートウェイまたはトランジットゲートウェイのいずれかで終了できます。仮想プライベートゲートウェイは、単一の VPC にアタッチできる Site-to-Site VPN 接続 AWS の側面にある VPN エンドポイントです。トランジットゲートウェイは、複数の VPCs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トランジットハブです。Site-to-Site VPN 接続の AWS 側の VPN エンドポイントとしても使用できます。 Site-to-Site このセクションでは、両方のオプションについて説明します。

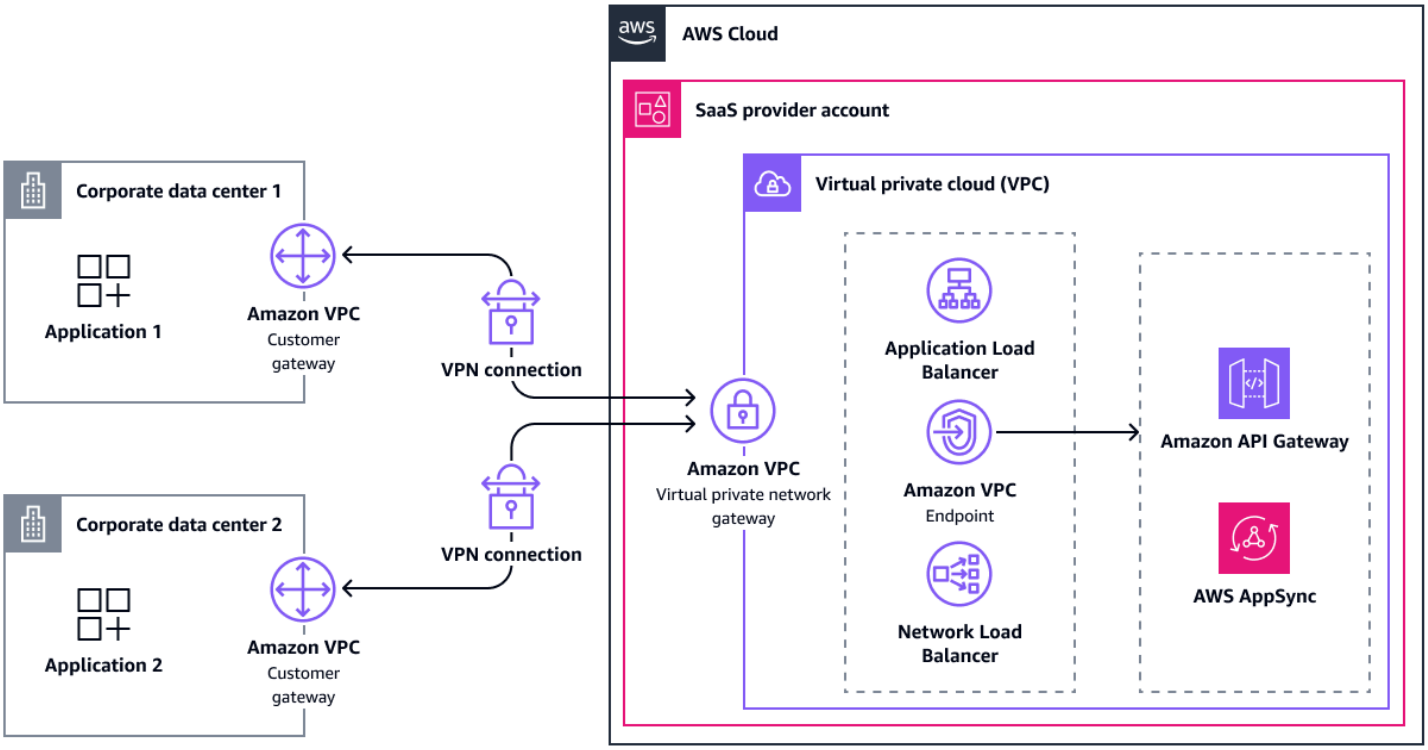
仮想プライベートゲートウェイを介した接続

仮想プライベートゲートウェイを作成したら、SaaS サービスを含む VPC にアタッチします。次に、ルート伝達を有効にして VPN ルートを VPC ルートテーブルに伝達します。これらのルートは、静的ルートまたは BGP アドバタイズされた動的ルートのいずれかです。

高可用性のために、Site-to-Site VPN 接続には 2 つの VPN トンネルがあり、 AWS 側の 2 つのアベイラビリティーゾーンで終了します。使用できなくなった場合、2 番目のトンネルが引き継ぐことができます。1 つのトンネルで最大帯域幅は 1.25 Gbps です。仮想プライベートゲートウェイは等コストマルチパスルーティング (ECMP) をサポートしていないため、一度に使用できるトンネルは 1 つだけです。

耐障害性を高めるために、2 番目の物理カスタマーゲートウェイへの 2 番目の VPN 接続を設定できます。接続が確立されると、コンシューマーは SaaS プロバイダーの VPC 内のリソースにアクセスできます。

次の図は、このアーキテクチャを示しています。



この方法による利点は以下の通りです。

- 修復までの時間: セカンダリ VPN トンネルへのマネージドフェイルオーバー
- オブザーバビリティ: Network Synthetic Monitor を使用したマネージドアクティブモニタリングの統合
- 統合の容易さ: BGP による動的ルーティングのサポート
- 適応性: ほとんどのオンプレミスネットワーク機器との互換性
- 適応性: IPv6 サポート
- TCO: AWS Site-to-Site VPN はフルマネージド型サービスであるため、運用作業が少なくて済みます
- TCO: 仮想ゲートウェイのコストはかかりませんが、それぞれ 2 つのパブリック IPv4 アドレスに課金されます。
- ネットワーク分離: インターネットを介した安全なプライベート通信を有効にする

このアプローチの欠点は次のとおりです。

- 統合の容易さ: コンシューマーはカスタマーゲートウェイを設定する必要があります

- スケーラビリティ: ECMP サポートがないため、仮想ゲートウェイあたりの帯域幅は 1.25 Gbps に制限されます。
- スケーラビリティ: ネットワークの複雑さと運用オーバーヘッドの増加によるスケーリングの制限
- 適応性: VPN トンネルの内部 IP アドレスのみの IPv6 サポート
- 適応性: 推移的ルーティングなし
- TCO: SaaS プロバイダーの多数の VPN 接続を維持、管理、設定するための運用オーバーヘッド

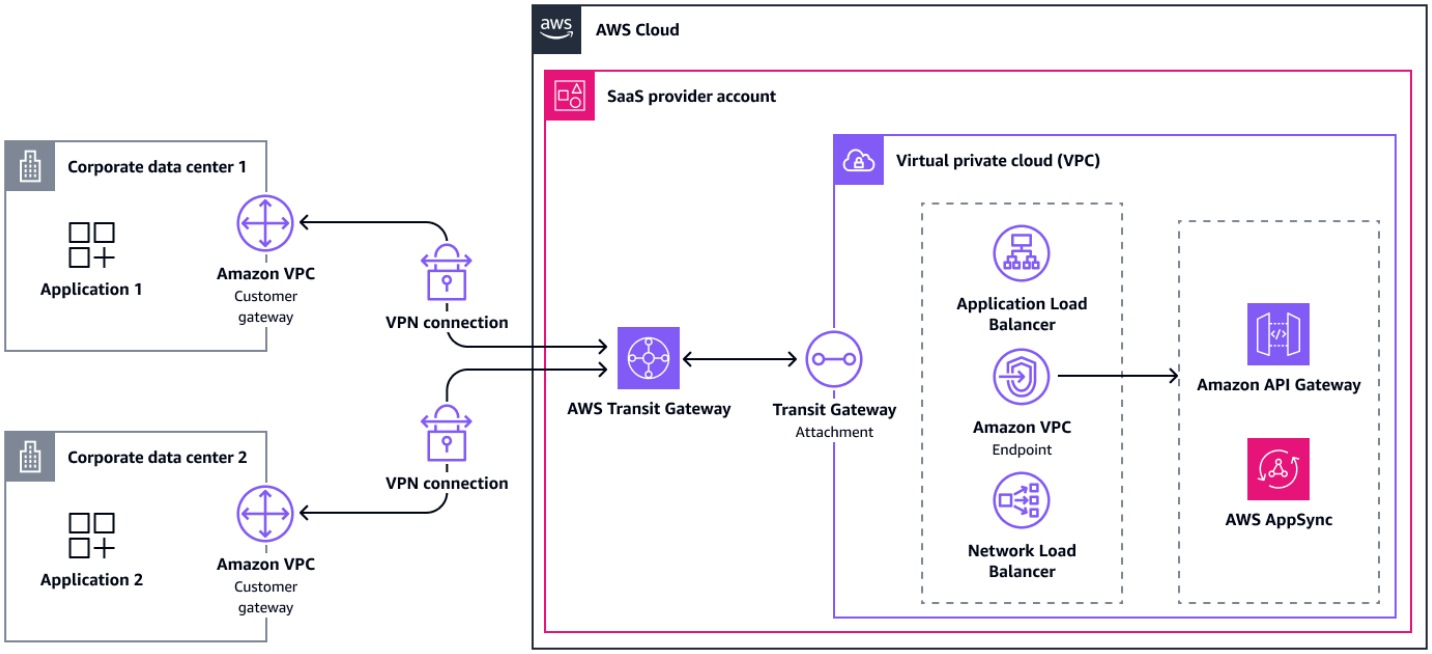
トランジットゲートウェイを介した接続

トランジットゲートウェイを介した接続は、仮想ゲートウェイと似ています。ただし、注意すべきいくつかの違いがあります。

まず、VPN アタッチメントのルートはトランジットゲートウェイルートテーブル内で自動的に伝播できますが、アタッチされた VPCs にルートを手動で追加する必要があります。

仮想ゲートウェイと比較して、Transit Gateway は ECMP をサポートしています。カスタマーゲートウェイが ECMP をサポートしている場合、両方のトンネルを使用して合計最大スループット 2.5 Gbps を実現できます。同じオンプレミスネットワークとトランジットゲートウェイの間に複数の接続を確立できます。このアプローチを使用すると、接続ごとに最大帯域幅を最大 2.5 Gbps 増やすことができます。

次の図は、このアーキテクチャを示しています。



この方法による利点は以下の通りです。

- 修復までの時間: セカンダリ VPN トンネルへのマネージドフェイルオーバー
- オブザーバビリティ: Network Synthetic Monitor を使用したマネージドアクティブモニタリングの統合
- 統合の容易さ: BGP による動的ルーティングのサポート
- スケーラビリティ: ECMP サポートにより、VPN スループットをスケーリングして大きな帯域幅要件を満たすことができます
- スケーラビリティ: 単一のトランジットゲートウェイでサポートされている多数の VPN 接続 (最大約 5,000)
- スケーラビリティ: すべての VPN 接続を管理およびモニタリングするための 1 つの場所
- 適応性: ほとんどのオンプレミスネットワーク機器との互換性
- 適応性: IPv6 サポート
- 適応性: の柔軟性を継承する AWS Transit Gateway
- TCO: AWS Transit Gateway はフルマネージドサービスであるため、運用作業が少なくて済みます
- TCO: 仮想ゲートウェイのコストはかかりませんが、それぞれ 2 つのパブリック IPv4 アドレスに課金されます。
- ネットワーク分離: インターネットを介した安全なプライベート通信を有効にする

このアプローチの欠点は次のとおりです。

- 統合の容易さ: コンシューマーはカスタマーゲートウェイを設定する必要があります
- スケーラビリティ: ネットワークの複雑さと運用オーバーヘッドの増加によるスケーリングの制限
- 適応性: VPN トンネルの内部 IP アドレスのみの IPv6 サポート
- TCO: SaaS プロバイダーの多数の VPN 接続を維持、管理、設定するための運用オーバーヘッド
- TCO: の使用に対する追加料金 AWS Transit Gateway
- TCO: トランジットゲートウェイルートテーブルの管理がさらに複雑になる

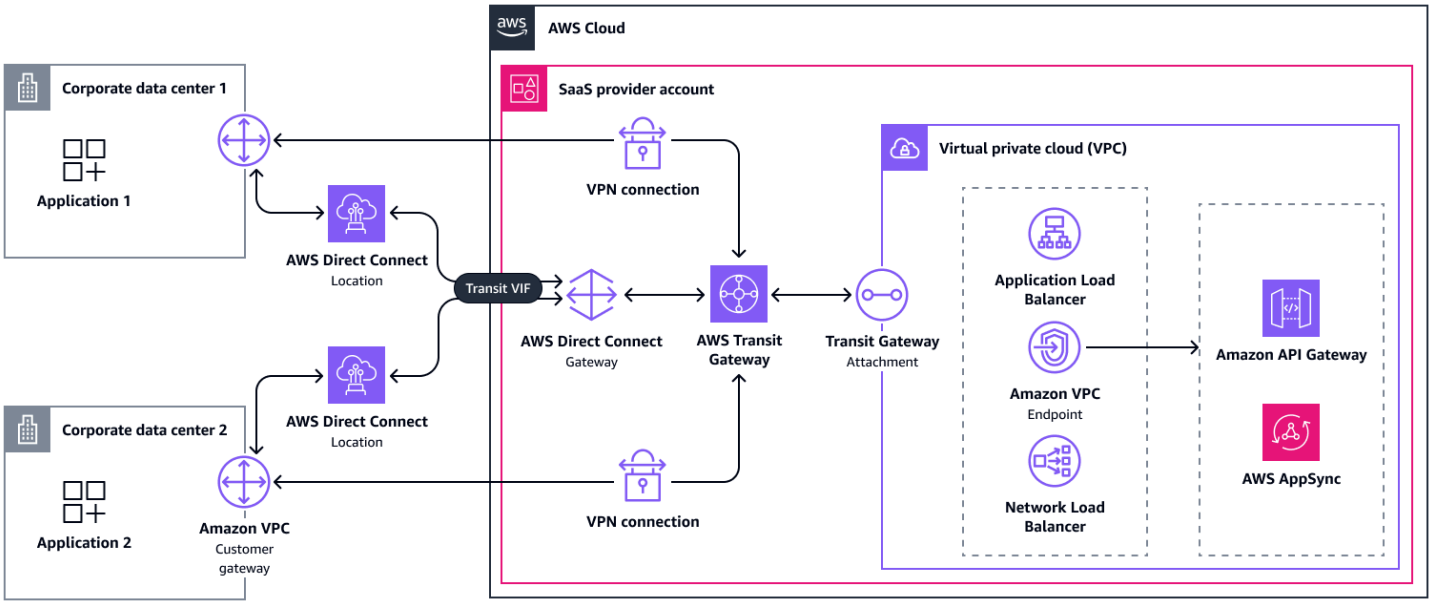
との接続 AWS Direct Connect

AWS Direct Connect は、標準イーサネット光ファイバケーブルを介して内部ネットワークを Direct Connect ロケーションにリンクします。他のアーキテクチャオプションとは異なり、専用接続は数分で確立できません。代わりに、すべての要件が満たされた場合、このプロセスには最大数日かかるこ

とがあります。そうでない場合は、時間がかかる場合があります。したがって、このアプローチについては、 AWS アカウントチームに問い合わせるか、サポート AWS サポート を受けることをお勧めします。オプションで、 AWS パートナーによって提供され、他の顧客と共有されるホスト接続を選択できます。アーキテクチャは同じです。レイテンシーの短縮、帯域幅の向上、規制要件への準拠などから選択できます Direct Connect 。

Direct Connect 接続を使用するには、コンシューマーがパブリック、プライベート、またはトランジット仮想インターフェイスを作成する必要があります。さまざまなアーキテクチャオプションを使用できます。複数のオンプレミスロケーションを に接続するための最も柔軟な AWS クラウド は、 Direct Connect ゲートウェイに接続されたトランジット仮想インターフェイスです。 Direct Connect ゲートウェイは、サービスプロバイダーが最大 6 つのトランジットゲートウェイに接続できるようにするグローバルな論理コンポーネントです。さらに、最大 30 個の仮想インターフェイスをゲートウェイに接続できます。スケーリングでは、追加の Direct Connect ゲートウェイを作成できます。SaaS プロバイダーアカウントでは、前述のようにトランジットゲートウェイが VPCs にアタッチされます。

コンシューマーは、希望する耐障害性のレベルに応じて、合計 1 つまたは 2 つのDirect Connect 場所から 1 つまたは 4 つの Direct Connect 接続を使用して接続できます。詳細については、「最大の耐障害性 Direct Connect のための設定」を参照してください。インターネット経由 AWS Site-to-Site VPN の接続は、 Direct Connect 接続の低コストのバックアップパスとしても機能します。サポートされている Direct Connect 専用接続では、MACsec を使用して、 Direct Connect ロケーションとデータセンター間のリンクをレイヤー 2 で暗号化できます。データの機密性を高めるために Site-to-Site VPN 接続を持つことが一般的です。Site-to-Site VPN 接続は、通常の VPN アタッチメントを使用してトランジットゲートウェイで終了できます。次の図は、このアーキテクチャを示しています。



この方法による利点は以下の通りです。

- オブザーバビリティ: Network Synthetic Monitor を使用したマネージドアクティブモニタリングの統合
- スケーラビリティ: 帯域幅スループットの向上のサポート
- 適応性: IPv6 サポート
- TCO: データ転送を減らす可能性
- TCO: 一貫したネットワークエクスペリエンス
- ネットワークの分離: 規制要件を満たすことができるプライベート接続

このアプローチの欠点は次のとおりです。

- 統合の容易さ: セットアップにかかる時間と手動作業
- スケーラビリティ: 追跡するクォータが複数あるため、数十 Direct Connect の接続を超えるスケーラビリティが制限されています
- 適応性: 設定オプションは使用可能な Direct Connect 場所によって異なります
- TCO: スケジュールされた Direct Connect メンテナンスは、アクションを必要とするダウンタイムを引き起こす可能性があります

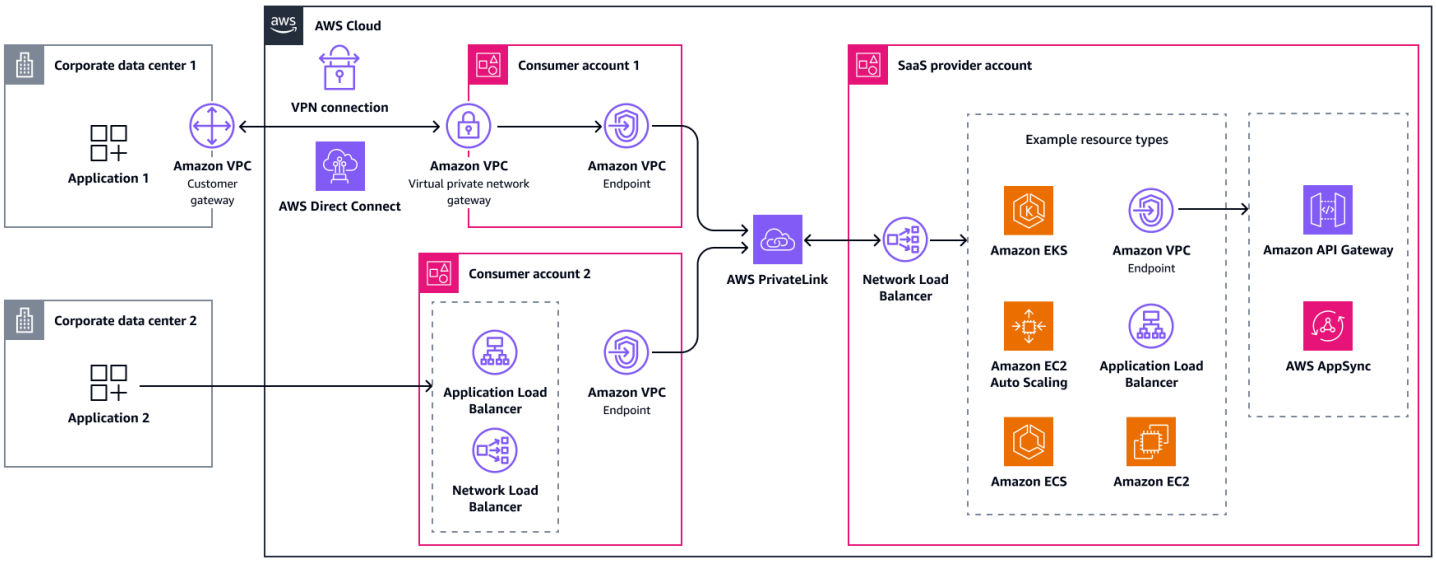
トランジット VPC アーキテクチャとの接続

トランジット VPC は、接続方法をコンシューマーに柔軟に提供するアーキテクチャオプションであり AWS、SaaS プロバイダーは を通じてサービスへの統一されたアクセスからメリットを得ることができます AWS PrivateLink。コンシューマーは、オンプレミスから、エントリポイント (仮想プライベートゲートウェイなど) と AWS PrivateLink リソースであるインターフェイス VPC エンドポイントのみを含むトランジット VPC に接続します。トランジット VPCs は、SaaS プロバイダーまたはコンシューマーが所有する必要があります。このセクションでは、両方のオプションについて説明します。

オンプレミスデータセンターと互換性のある CIDR 範囲を使用して、トランジット VPC とサブネットを作成できます。プライベート接続が必要な場合は、コンシューマーは AWS Direct Connect または を介してその VPC に接続できます AWS Site-to-Site VPN。VPC エンドポイントを指す Application Load Balancer または Network Load Balancer を使用して、パブリックインターネットからトランジットアカウントへのアクセスを設定することもできます。

コンシューマー管理のトランジット VPC

このアプローチでは、SaaS プロバイダーはトランジット VPCs の管理をコンシューマーに任せることになります。技術的な観点からは、SaaS プロバイダーのアーキテクチャは、 を介してコンシューマーに接続する場合と同じです AWS クラウド AWS PrivateLink。販売と製品の観点から見ると、一部のコンシューマー AWS アカウント がまだいないため、追加の労力です。アカウントを開いて運用することをためらっている可能性があります。SaaS プロバイダーは、オンプレミスデータセンターを作成して AWS アカウント 接続する方法に関するガイダンスをコンシューマーに提供する必要があります。次の図は、コンシューマーがトランジット VPCs を所有するパブリックアクセスとプライベートアクセスの組み合わせを示しています。



この方法による利点は以下の通りです。

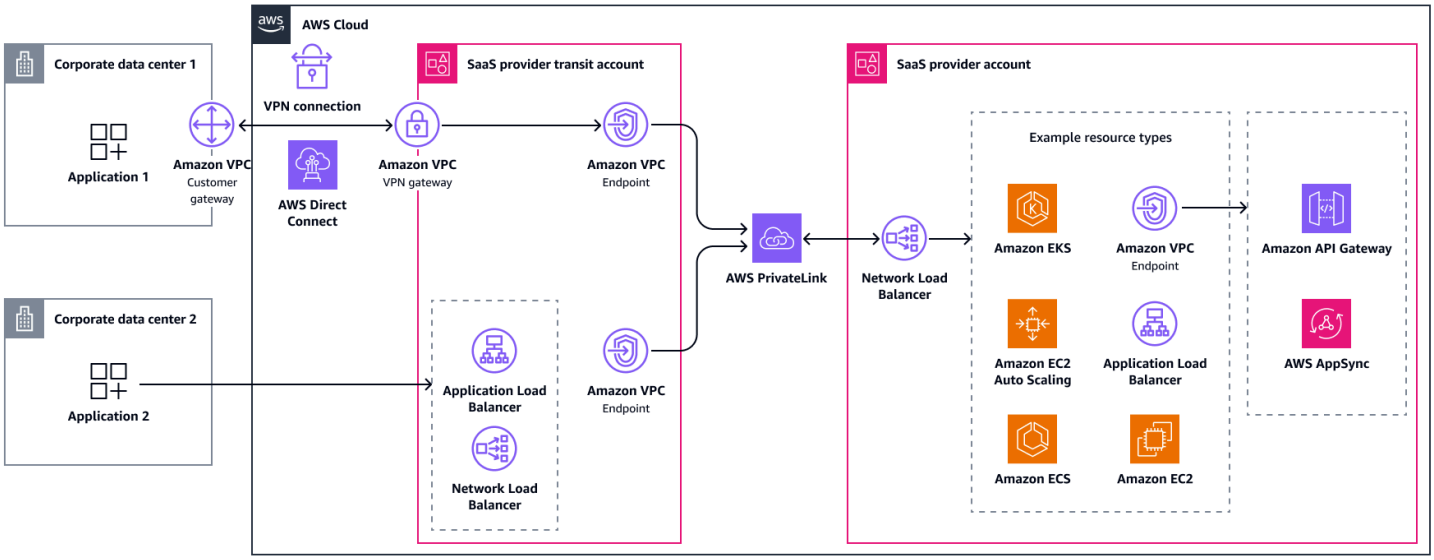
- 修復までの時間: 運用オーバーヘッドは SaaS コンシューマーに大きくオフロードされます
- 適応性: SaaS コンシューマーはさまざまなアクセスオプションから選択可能
- 適応性: Site-to-Site VPN または Direct Connect
- すべてのメトリクス: サービスプロバイダーが AWS PrivateLink 利点を継承する

このアプローチの欠点は次のとおりです。

- 統合の容易さ: SaaS コンシューマーには少なくとも 1 つの が必要です AWS アカウント
- TCO: トランジット VPC はフルマネージドサービスではなくアーキテクチャであるため、より多くの運用作業が必要です

プロバイダー管理のトランジット VPC

このアプローチでは同じテクノロジーを使用しますが、アカウントの境界と責任は変わります。ここで、SaaS プロバイダーはトランジット VPCsを所有します。できれば SaaS サービスとは別のアカウントで所有します。このデカップリングにより、コストを削減し、リスクを軽減し、トランジットアカウントを個別にスケーリングできます。高度な分離を必要とする環境では、サブネットを使用するか、コンシューマーごとに個別のトランジット VPC を作成することで、テナント間で追加の分離を作成できます。その後、コンシューマーはトランジット VPC に接続する方法を選択できます。このアプローチは、アドレス可能な市場全体を拡大するためのより多くのオプションを提供しますが、追加のアーキテクチャコンポーネントを運用およびモニタリングする必要があるため、SaaS プロバイダーの TCO は高くなります。



この方法による利点は以下の通りです。

- 適応性: SaaS コンシューマーはさまざまなアクセスオプションから選択可能
- 適応性: SaaS コンシューマーには は必要ありません AWS アカウント
- 適応性: Site-to-Site VPN または Direct Connect

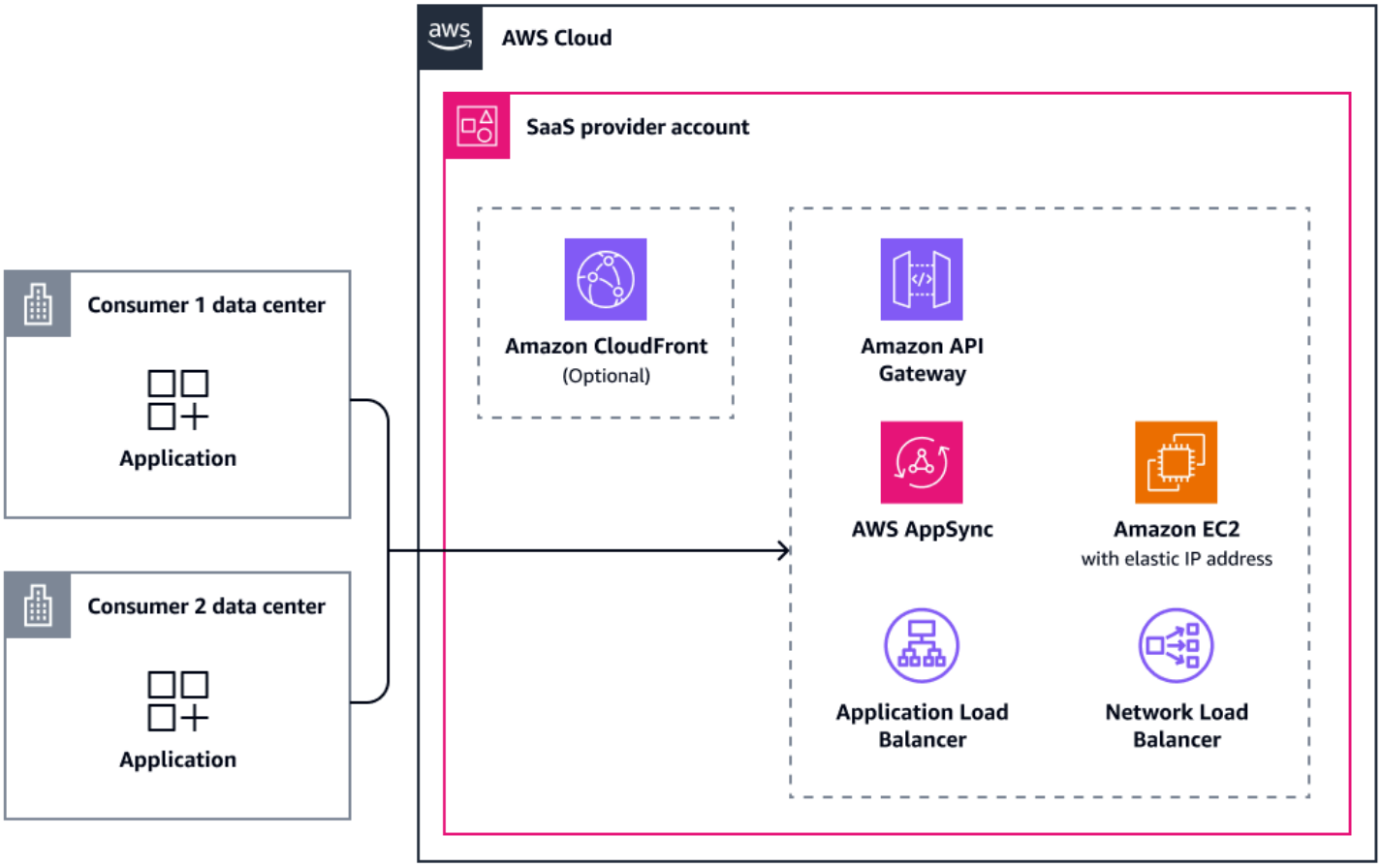
このアプローチの欠点は次のとおりです。

- TCO: トランジット VPC はフルマネージドサービスではなくアーキテクチャであるため、より多くの運用作業が必要です
- TCO: SaaS プロバイダーは追加のアーキテクチャコンポーネントを運用およびモニタリングする必要があります

パブリックインターネットを介した接続

パブリックインターネットアクセスは、SaaS サービスへのアクセスを提供する有効なオプションでもありますが、従来の意味ではプライベート接続を提供しません。一部のコンシューマーは、コンシューマーと SaaS プロバイダーの間に追加のネットワークインフラストラクチャを必要としないため、パブリックアクセスアプローチを引き続き希望する場合があります。これにより、攻撃対象領域の増加と引き換えに、複雑さ、コスト、統合時間を短縮できます。強力な認証および認可メカニズムは、脅威レベルの増加を軽減するのに役立ちます。トラフィックは常に暗号化する必要があります。このシナリオでは、 を使用するなど、セキュリティレイヤーを追加することをお勧めしますAWS WAF。

このシナリオのアーキテクチャは簡単です。コンシューマーはインターネット経由でパブリックホスト (SaaS プロバイダー) に接続します。アプリケーションは、Elastic IP アドレスを持つパブリック Amazon Elastic Compute Cloud (Amazon EC2) インスタンスで直接ホストできます。推奨されるオプションは、Application Load Balancer または同様のサービスの背後でホストすることです。パフォーマンスを向上させ、静的アセットをキャッシュするには、Amazon CloudFront などのコンテンツ配信ネットワークを使用できます。2 つのグローバル静的エニーキャスト IP アドレスで最小限のレイテンシーでアプリケーションを処理するには、Amazon EC2 インスタンス、Network Load Balancer、または Application Load Balancer AWS Global Acceleratorの前に配置できます。さらに、CloudFront、Application Load Balancer AWS AppSync、Amazon API Gateway はすべて と統合されます AWS WAF。次の図は、パブリックインターネットアクセス接続オプションの概要を示しています。



次の表に、このシナリオでサポートされているプロトコルと統合を示します。

サービスまたはリソース	IPv6	AWS WAF 統合	Global Accelerator エンドポイントにすることができます
Amazon CloudFront	サポート対象	サポート	サポートされていません
Amazon API Gateway	サポート対象	サポート	サポートされていません
AWS AppSync	一部サポートされています	サポート	サポートされていません
Elastic IP アドレスを持つ Amazon EC2	サポート	サポート外	サポート

Application Load Balancer	サポート対象	サポート対象	サポート
Network Load Balancer	サポート	サポート外	サポート

この方法による利点は以下の通りです。

- 統合の容易さ: シンプルさとアクセシビリティ
- スケーラビリティ: 無制限のスケール
- 適応性: CIDR 範囲の競合の可能性なし
- 適応性: CloudFront のサポート

このアプローチの欠点は次のとおりです。

- ネットワーク分離: プライベート接続なし
- ネットワーク分離: 強力なセキュリティ対策が必要

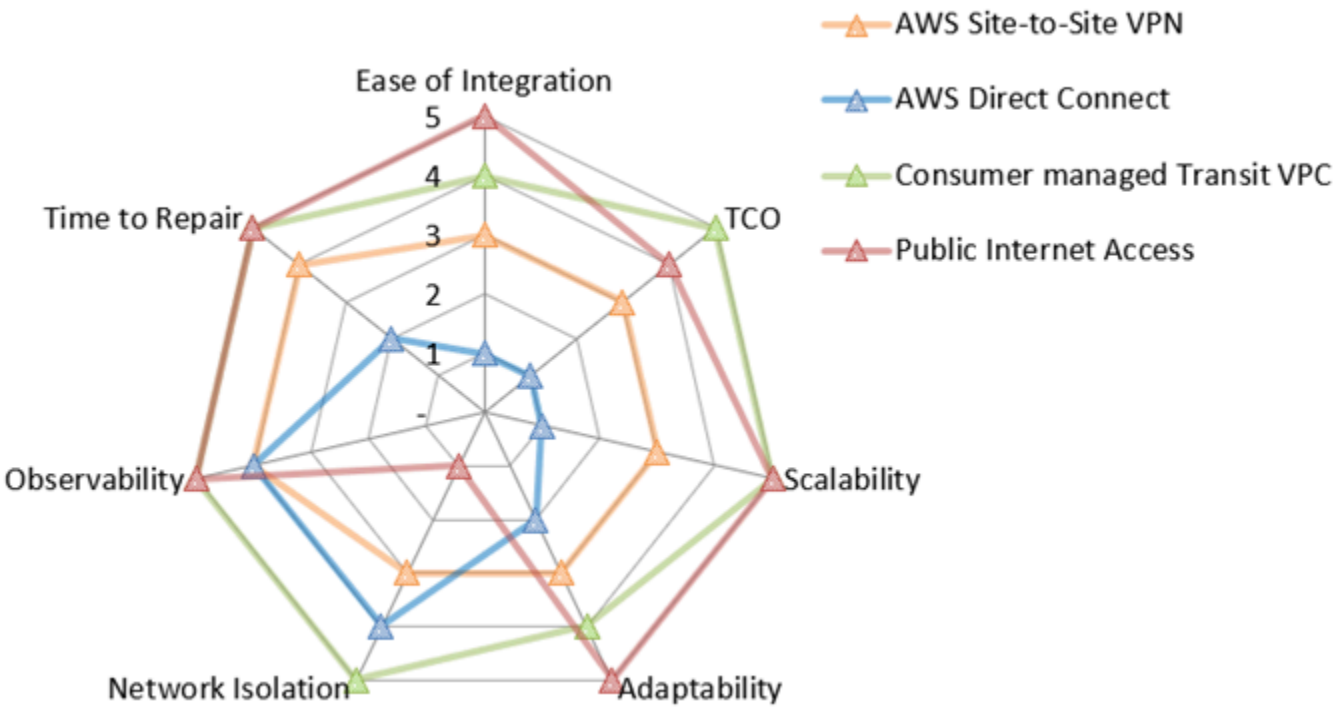
選択したサービスに応じて、その他の利点と欠点が適用されます。

他のクラウドサービスプロバイダーで運用されている SaaS コンシューマー

このシナリオでは、他のクラウドサービスプロバイダー (CSPs) のコンシューマー向けのソリューションについて説明します。このシナリオでは、オンプレミスデータセンターへの接続といくつかの共通点を共有します。実際、オンプレミス環境のすべての接続オプションは、他の CSPs のコンシューマーにも同様に有効です。一部の CSPs では、 とのプライベート接続も AWS Direct Connect 可能です。ほとんどの CSPs AWS Site-to-Site VPN または AWS クラウド を介して に接続する方法に関するドキュメントとサポートを提供しています AWS Direct Connect。

Site-to-Site VPN を選択すると、コンシューマーはそれぞれの CSP のマネージドゲートウェイまたは同様のリソースからメリットを得ることができます。オンプレミスのシナリオのように、コンシューマーが必ずしも自分で設定する必要はありません。これは、修復時間とオブザーバビリティの改善など、Site-to-Site VPN のメトリクスの一部に影響します。これは、接続の両端が管理されるようになったためです。

次のネットワーク値マップは、各評価メトリクスの各オプションスコアをまとめたものです。Site-to-Site VPN の値は異なりますが、オンプレミス接続のネットワーク値マップと非常に似ています。評価メトリクスの詳細については、このガイドの評価メトリクス「」を参照してください。マップでは、5 は最低 TCO、最適なネットワーク分離、修復時間など、最適なスコアを表します。このレーダーチャートの読み方の詳細については、このガイドネットワーク値マップの「」を参照してください。



レーダーチャートには、次の値が表示されます。

評価メトリクス	AWS Site-to-Site VPN	AWS Direct Connect	コンシューマー管理のトランジット VPC	パブリックインターネットアクセス
統合のしやすさ	3	1	4	5
TCO	3	1	5	4
スケーラビリティ	3	1	5	5
適応性	3	2	4	5

ネットワーク分離	3	4	5	1
可観測性	4	4	5	5
修復にかかる時間	4	2	5	5

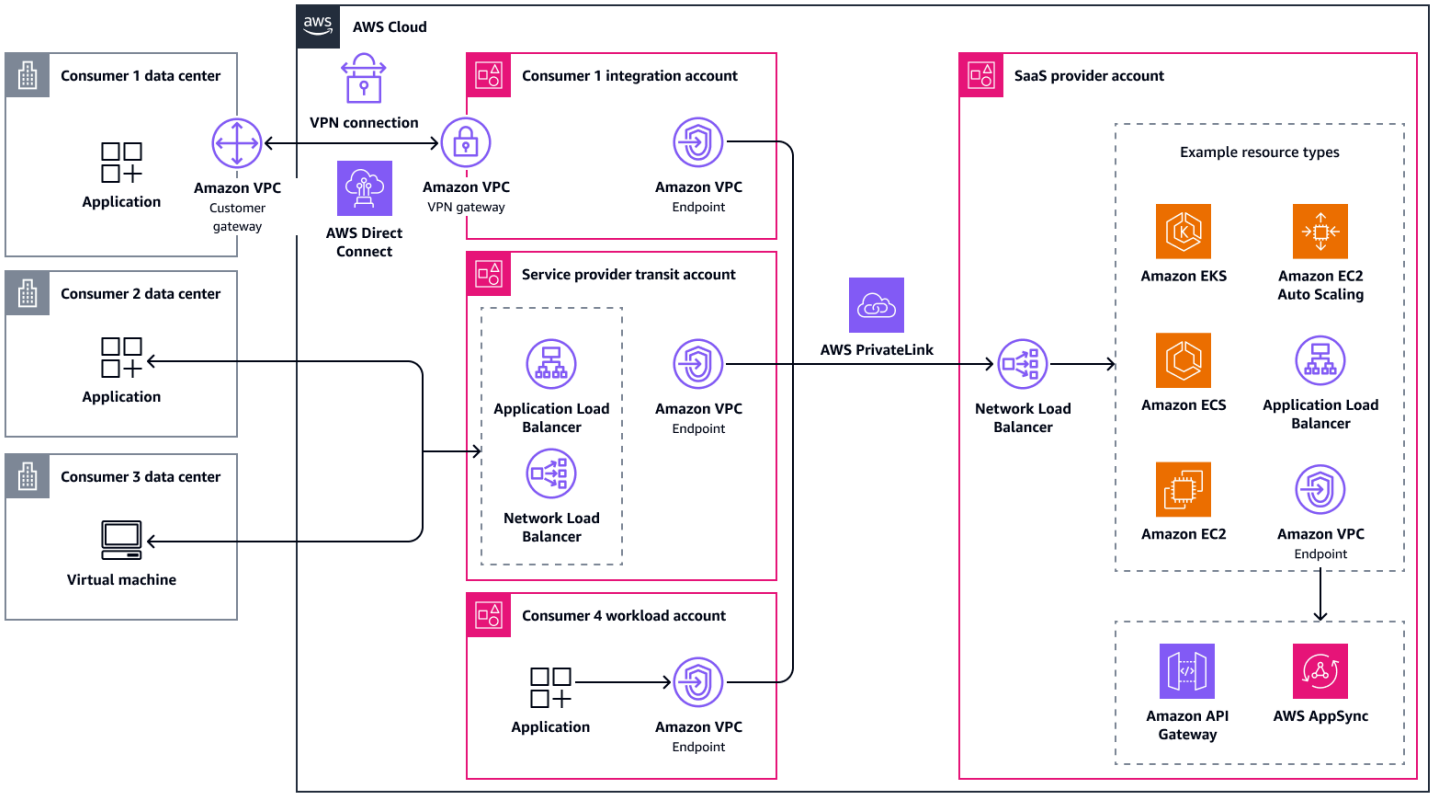
ハイブリッド環境のサポート

コンシューマーは、それぞれに独自の技術的およびセキュリティ上の制約があるさまざまな環境から来るのが一般的です。一部のお客様は、インターネット経由または専用ネットワークリンクを介した安全な接続を必要とするオンプレミスデータセンターから完全に運用されている場合があります。他の はすでに 内でワークロードを実行しており、低レイテンシーのプライベートネットワークパス AWS を想定している場合があります。3 番目のグループは、接続が異なるクラウドネットワークをブリッジする必要がある他の CSPs に依存する場合があります。

いずれにしても、アーキテクチャを簡素化し、運用の複雑さを軽減するために、SaaS アプリケーションへの標準化されたネットワークアクセスを目指す必要があります。前述の 2 つのアプローチであるパブリックインターネットアクセスとトランジット VPCs、これらのシナリオでうまく機能します。パブリックインターネットアクセスは、お客様に最小限のセットアップで最速のオンボーディングパスを提供します。トランジット VPCs、多くの場合 を使用して、より制御されたプライベートアクセスを提供します AWS PrivateLink。

SaaS サービスを設計するときは、単一のネットワークアクセスモデルを採用するか、複数のアプローチを階層型サービスに結合できます。たとえば、接続のしやすさと迅速なオンボーディングを優先する顧客にパブリックアクセスデプロイ層を提供し、厳格なコンプライアンスまたはセキュリティコントロール要件を持つ顧客にプライベートアクセスデプロイ層を提供することができます。これらの階層には、さまざまなコスト、パフォーマンス、リスクプロファイルがあります。また、両方のアプローチを 1 つのアーキテクチャに統合することもできます。この場合、パブリックパスとプライベートパスが分離されたままになるように、強力なセキュリティ対策があることを確認してください。

次の図は、コンシューマーがデータセンターまたは CSP からプライベートに接続するか、パブリックに接続するか、 経由で直接接続する AWS PrivateLink (にワークロードがある場合) ハイブリッドアクセスアプローチを示しています AWS クラウド。


AWS Cloud
Consumer 1 data center
Application
Amazon VPC
Customer gateway
VPN connection
AWS Direct Connect
Amazon VPC
VPN gateway
Consumer 1 integration account
Amazon VPC
Endpoint
Consumer 2 data center
Application
Consumer 3 data center
Virtual machine
Service provider transit account
Application Load Balancer
Network Load Balancer
Amazon VPC
Endpoint
Consumer 4 workload account
Application
Amazon VPC
Endpoint
AWS PrivateLink
SaaS provider account
Network Load Balancer
Example resource types
Amazon EKS
Amazon EC2 Auto Scaling
Amazon ECS
Application Load Balancer
Amazon EC2
Amazon VPC
Endpoint
Amazon API Gateway
AWS AppSync

の SaaS サービスの高度なネットワークアクセスシナリオ AWS クラウド

の SaaS サービスのネットワークアクセスシナリオ AWS クラウド セクションで説明するアーキテクチャは、ほとんどのユースケースのソリューションを見つけるのに役立ちます。ただし、特定の技術要件があるシナリオがいくつかあります。その多くは、このガイドの範囲外です。

このセクションでは、以下の高度な技術要件と考慮事項について説明します。

- 双方向通信
- TCP、UDP、および独自のプロトコル

双方向通信

場合によっては、アプリケーションが期待どおりに動作するために双方向トラフィックが必要になることがあります。一般的なユースケースは、ウェブフックまたは通知サービスです。一般的に、サーバーとクライアントの間に WebSocket 接続を確立することでこれを実現できます。この接続は TCP セッションを開いたままにし、両方の参加者が接続経由でトラフィックを送信できるようにします。このガイドで説明するほとんどのサービスは、Network Load Balancer、Application Load Balancer、Amazon API Gateway、および AWS AppSync (プライベートリアルタイムエンドポイント経由) など AWS PrivateLink、WebSocket をネイティブにサポートしています。

それ以外の場合、SaaS プロバイダー側のアプリケーションは、データベースなどのコンシューマー側のリソースにアクセスする必要がある場合があります。接続などの双方向チャネルを介して AWS Site-to-Site VPN 接続する場合、これは問題ではありません。

一方、 AWS PrivateLink Elastic Load Balancing は一方向トラフィックのみをサポートします。これらのサービスを使用する場合は、SaaS サービスから開始するトラフィックに別のネットワークパスを設定する必要があります。たとえば、これは逆方向の追加の AWS PrivateLink 接続である可能性があります。

TCP、UDP、および独自のプロトコル

多くのアプリケーションは HTTP または HTTPS を介して提供されますが、すべてではありません。一部の では、Message Queuing Telemetry Support (MQTT) など、TCP 上に他の Layer 7 プロトコルを使用する場合があります。また、UDP を使用してコンシューマーにサービスを提供している場

合もあります。まれに、サービスはパケット内で送信する必要がある独自のプロトコルを使用します (レイヤー 3)。これらのシナリオでは、SaaS サービスをサポートするサービスを理解することが重要です。

Layer 3 サービスでは、 AWS PrivateLink と Network Load Balancer を使用できます。どちらもすべての TCP トラフィックと UDP トラフィックをサポートします。

Layer 7 サービスの場合、Application Load Balancer と Amazon CloudFront は HTTP、HTTPS、WebSocket、Google リモートプロシージャコール (gRPC) をサポートしています。同様に、Amazon API Gateway と AWS AppSync はそれぞれ HTTP、HTTPS、WebSocket をサポートしています。Amazon CloudFront は、現在 HTTP/3 をサポートしている唯一のサービスです。

Amazon VPC Lattice を使用して、レイヤー 7 アプリケーションとレイヤー 3 リソースを接続できます。HTTP、HTTPS、gRPC、TCP、TLS パススルーをサポートしています。

アプリケーションがレイヤー 3 経由でのみトラフィックを処理できる場合は、、、 AWS Transit Gateway AWS Direct Connect AWS Site-to-Site VPN、VPC ピアリングなどのコア AWS ネットワークサービスを使用することが重要です。その後、トラフィックは SaaS コンシューマーから SaaS サービスのコンピューティングレイヤーに直接ルーティングされます。

でのネットワークアクセスのアンチパターン AWS クラウド

アンチパターンとは、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です。このセクションで説明する設計オプションは通常機能しますが、大きな欠点があります。可能な場合は、より良い代替手段が利用できるため、避ける必要があります。

このセクションでは、以下のアンチパターンと課題について説明します。

- アベイラビリティーゾーンの との不一致 AWS PrivateLink
- AWS Site-to-Site VPN 間の接続 AWS アカウント

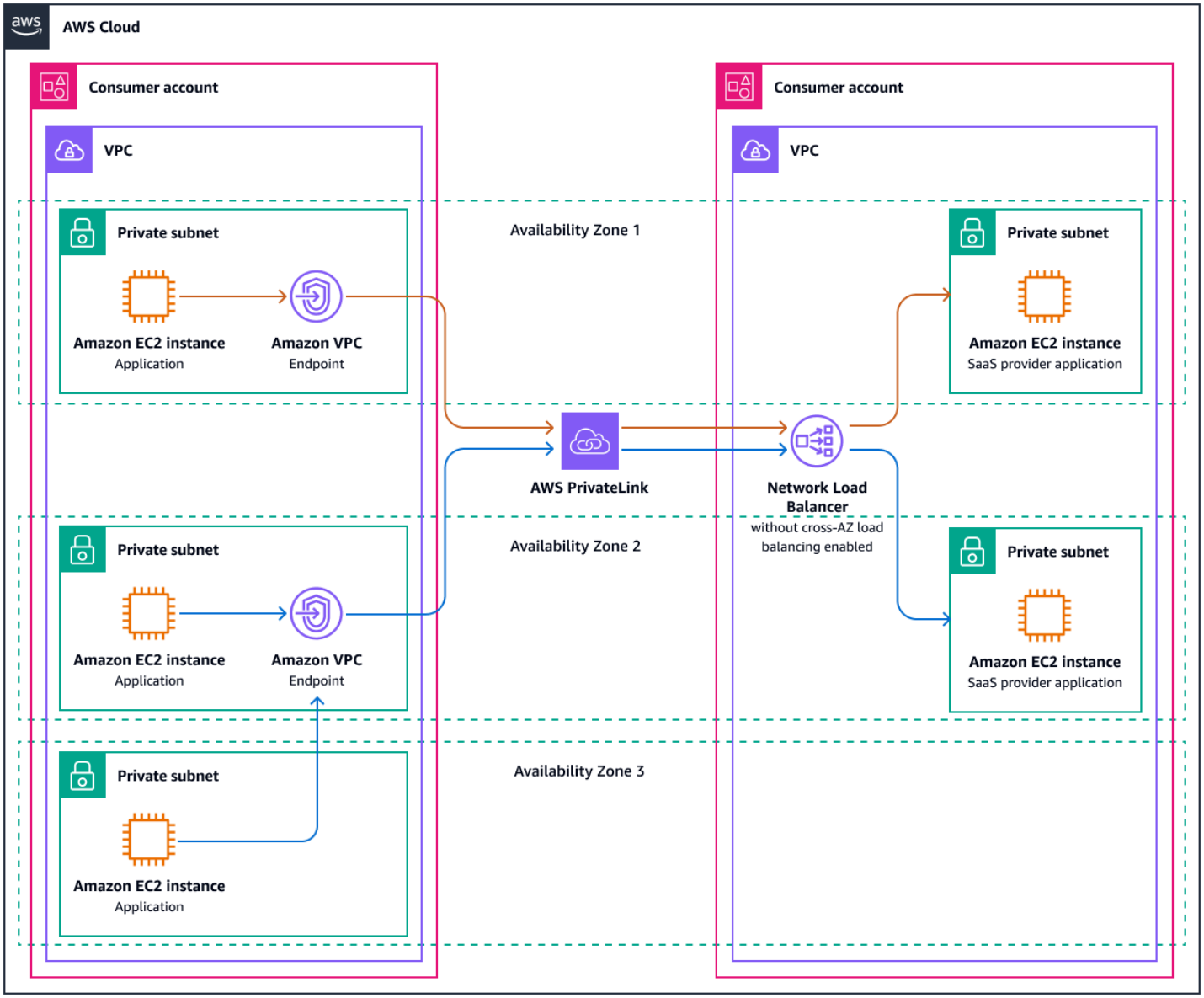
アベイラビリティーゾーンの との不一致 AWS PrivateLink

を介してアプリケーションへのアクセスを提供する場合 AWS PrivateLink、SaaS コンシューマーは、アプリケーションがデプロイされているアベイラビリティーゾーンでのみインターフェイス VPC エンドポイントを作成できます。たとえば、アプリケーションが use1-az1と にデプロイされている場合use1-az2、コンシューマーは に VPC エンドポイントをデプロイできませんuse1-az3。SaaS サービスをすべてのアベイラビリティーゾーンにデプロイすることをお勧めします。の大部分 AWS リージョン には 3 つのアベイラビリティーゾーンがありますが、それ以上のアベイラビリティーゾーンもあります。包括的なリストについては、「リージョンとアベイラビリティーゾーン」を参照してください。を選択するときは、アベイラビリティーゾーンの数を考慮してください AWS リージョン。

> **Note**
>
> アベイラビリティーゾーン名はアベイラビリティーゾーン IDs。詳細については、「 AWS リソースのアベイラビリティーゾーン IDs」を参照してください。

SaaS プロバイダーがすべてのアベイラビリティーゾーンにデプロイしないことを選択した場合、いくつかの結果があります。SaaS サービスが use1-az1と にデプロイされているがuse1-az2、コンシューマーが を含む 3 つのアベイラビリティーゾーンすべてを使用しているとしますuse1-az3。インターフェイス VPC エンドポイントは use1-az1と のコンシューマー側にデプロイされuse1-az2、 のアプリケーションはこれらのエンドポイントのいずれかにアクセスuse1-az3する必要があります。まず、一致しないアベイラビリティーゾーンのサブネットからそれぞれの VPC エンドポイ

ントへのトラフィックを許可する必要があります。コンシューマーは、リージョン AWS PrivateLink DNS 名を使用することを決定できます。これにより、VPC エンドポイントのいずれかに解決され、2 つのエンドポイント間でトラフィックが均等に分散されます。または、コンシューマーは、などのエンドポイントにトラフィックを直接送信することを選択できますuse1-az2。これにより、トラフィックの 67% が でプロバイダー側に到着use1-az2し、33% が に到着しますuse1-az1。次の図は、このシナリオを示しています。



大量のコンシューマーとトラフィックの不均等な分散により、ワークロードが 1 つのアベイラビリティーゾーンで容量の問題が発生し、別のアベイラビリティーゾーンで容量不足になる可能性があります。この問題に対処するために、SaaS プロバイダーは Network Load Balancer でクロスゾーン負荷分散を有効にすることで、トラフィックを均等に負荷分散することを決定できます。これには追加料金が発生します。

サービスプロバイダーが一致するアベイラビリティーゾーンが 1 つしかない場合、すべてのトラフィックは 1 つのエンドポイント経由で入ります。これにより、不均衡がさらに大きくなります。その結果、SaaS サービスはコンシューマーにとって高可用性ではなくなりました。コンシューマーが使用していない追加のアベイラビリティーゾーンでアプリケーションを提供するかどうかは関係ありません。最悪の場合、SaaS プロバイダーは、同じアベイラビリティーゾーンを使用しないコンシューマーにサービスを提供できない可能性があります。

まれに、SaaS プロバイダーがすべてのアベイラビリティーゾーンにアプリケーションをプロビジョニングする実行可能なオプションがない場合、欠落しているアベイラビリティーゾーンにのみサブネットを作成し、それらの空のアベイラビリティーゾーンにサービスを拡張することもできます。その後、クロスゾーン負荷分散は、着信トラフィックを他のアベイラビリティーゾーンの実際のアプリケーションエンドポイントに分散できます。

AWS Site-to-Site VPN 間の接続 AWS アカウント

オンプレミス環境からクラウドに移行する企業は、ネットワーク全体をリフトアンドシフトしようとすることがあります。これは、オンプレミスとクラウドのネットワーキングプラクティスに大きな違いがあるため、問題を引き起こす可能性があります。この考え方の移行が行われない場合、ある VPC AWS Site-to-Site VPN から別の VPC への接続などが発生する可能性があります。このアプローチでは、 の専用ネットワーキングサービスを活用できないため AWS クラウド、管理が簡素化され、パフォーマンスが向上します。クラウドネイティブ設計に適応することで、運用上のオーバーヘッドが軽減され、VPCs 間の信頼性とスケーラビリティが向上します。

この接続オプションを SaaS プロバイダーとして提供することを検討している場合は、自分またはコンシューマーにその理由を尋ね AWS Site-to-Site VPN てください。次に、これらの要件から逆算して、より良い接続オプションを見つけます。このガイドのサービス機能の比較セクションには、オプションの特定に役立つマトリックスが含まれています。次に、このガイドの関連セクションを参照して、ユースケースに対応するアーキテクチャアプローチを見つけることができます。

次の手順

このガイドでは、さまざまなシナリオにおけるさまざまなネットワークアクセスアプローチについて説明し、各アーキテクチャの利点と欠点について説明します。ネットワークアクセスアプローチの選択が単なるテクノロジーの議論ではない理由を理解する必要があります。ビジネスとテクノロジーの連携が不可欠です。次のステップと推奨事項は、現在の機能の評価、市場ニーズの分析、ガバナンスコントロールの実装を通じて、ネットワークアーキテクチャ戦略の評価と標準化に役立ちます。

このセクションは、以下のトピックで構成されます。

- 現在のアーキテクチャと機能の評価
- 市場分析と顧客分析
- 戦略的連携
- 標準化
- ガバナンス
- 繰り返し

現在のアーキテクチャと機能の評価

このガイドの自己評価フレームワーク、現在の規制要件、市場の現在の状態 (顧客と競合分析の両方の観点から) など、関連するデータソースに対して現在のネットワークアーキテクチャを確認します。例えば、 AWS Well-Architected フレームワークの使用を検討してください。これは、 で本番環境システムを大規模に実行してきた数十年の経験に基づいています AWS クラウド。

潜在的な例外、1 回限り、過去の製品決定を確認します。興味を持ってチャレンジし、その有効性を自動的に引き受けないでください。数年前の顧客要件は無効になる可能性があります。困難な前提は、アーキテクチャの複雑さを簡素化し、軽減する機会をもたらします。

簡単に説明すると、組織内のさまざまなロールが観察結果にアクセスして理解できるように文書化します。現在の状態がターゲット状態と異なる場所、ターゲット状態、影響、観測が行われたタイミングをキャプチャします。この情報を記録すると、組織は新しいデータに基づいて意思決定を行うことができます。

市場分析と顧客分析

市場トレンドに関するインサイトを収集します。コンシューマーが自分のような SaaS サービスにアクセスするために現在推奨される方法は何ですか? 顧客がいる場所にまだ出会っていますか? 顧客の

コホートや行動は変化しましたか? エグゼクティブは、新しい市場、特定の規制要件を持つ地域、または新しい顧客層に向けて船を操縦しましたか? ビジネスモデルまたは運用モデルが変更されましたか? たとえば、サービスのホワイトラベル付けを検討していますか? 成長計画には、パートナーがそれらのパートナーとつながったときに顧客がサービスを利用できるように、パートナーと連携することが含まれていますか?

戦略的連携

現在の能力、現在のアーキテクチャ、市場、顧客を理解したら、戦略的調整会議を呼び出します。関連する製品、ビジネス、テクノロジーの利害関係者とともに、どの要件がまだ有効で、どの新しい要件を検討する必要があるかを問いかけます。不要になった要件を削除することで、複雑さを軽減する機会を見つけます。これは委員会による設計ではありません。エンジニアリングチームは実際のアーキテクチャと実装の詳細を準備し、所有する必要があります。ただし、この会議では、これが顧客や組織にとってのメリットを最大化する一連の要件である理由を明確にする必要があります。

標準化

顧客を惹きつけるには、サービスへの接続方法を自由に選択させようとするかもしれません。結局のところ、どのソリューションも技術的に機能し、それらをすべて管理および運用するための専門知識とリソースを持っている可能性があります。これは特定の時点までうまく機能しますが、ビジネス規模が拡大するにつれて、管理が困難になります。オブザーバビリティスタックは、複数のソリューションからのメトリクスをサポートする必要があり、サイト信頼性エンジニアもそれらを理解できる必要があります。接続アプローチごとにup-to-dateドキュメントが必要です。アプリケーションの主な変更は、提供するアクセスアプローチごとに評価する必要があります。アクセスアプローチごとに自動化とInfrastructure as Code (IaC) を記述して維持する必要があります。サービスへのアクセスを標準化しない場合の追加オーバーヘッドは、顧客に提供する柔軟性と照らし合わせて検討する必要があります。

意思決定の指針として北極星が必要な場合は、標準化をお勧めします。顧客が提供するサービスとやり取りする方法の標準化は、通常、組織全体の多くの成功メトリクスを改善するために実行できる 1 つの最も影響力のあるアクションです。標準化により、製品チームはサービスのコスト構造を理解し、データ駆動型の製品決定を簡単に行うことができます。運用チームは、事前定義された標準に従って開発、ロールアウト、運用される環境で、問題をトラブルシューティングし、トラブルシューティングプロセスの一部を自動化することが容易になります。これは、悪意のあるアクターによる異常、予期しない動作、またはアクションを検出するのに役立ちます。標準化により、技術的負債も削減されます。エンジニアリングチームが本番環境への変更をテストしてロールアウトするサイクルが

少なくなります。また、市場投入までの時間を短縮し、セルフサービスオンボーディングの成功を向上させ、規制リスクを軽減することもできます。

したがって、現在実施されている可能性のある 1 回限りの確認もお勧めします。既存の顧客をサポートするのに費やす運用サイクルの数を定量化します。結果を履歴データと比較し、現在のアプローチが今後何年もスケールするかどうかを評価します。標準から逸脱する必要がある場合は、それらのリクエストの背後にある要件にチャレンジしてください。影響を評価し、直接的なメリットと長期的なコミットメントのバランスを取ります。

カスタマイズは避けられないが、標準と矛盾する場合は、責任共有モデルを検討してください。このモデルでは、製品は要求された変更から大きく保護され、カスタマイズは最小限の専用環境で行われます。例については、トランジット VPC アーキテクチャとの接続「」セクションを参照してください。

ガバナンス

規制要件と独自の内部標準に準拠するには、ガバナンスが不可欠です。適切なガバナンスを導入することで、標準を適用する場所と方法を制御できます。また、標準からの逸脱を検出し、必要な是正措置をリソース所有者に通知するためのコントロールを確立します。AWS Organizations、AWS CloudTrail、、および AWS ConfigAWS Control Towerは、 のワークロードの管理と管理 AWS のサービス に役立つ多くの のいくつかです AWS クラウド。

繰り返し

初期の作業から学んだことを使用して、将来整合性を保つために、軽量で反復可能なプロセスを設定します。入力が必要なロール、必要な頻度、データの精度、データの共有方法、およびデータに対して誰が対応するかを定義します。

リソース

AWS ドキュメント

- でのサードパーティーサービスの統合 AWS クラウド (AWS 規範ガイダンス)
- マルチテナント SaaS 認可と API アクセスコントロール (AWS 規範ガイダンス)
- 1 つのコントロールプレーンで複数の SaaS 製品のテナントを管理する (AWS 規範ガイダンス)
- とは AWS Direct Connect (Direct Connect ドキュメント)
- AWS PrivateLinkとは (Amazon VPC ドキュメント)
- とは AWS Site-to-Site VPN (AWS Site-to-Site VPN ドキュメント)
- とは AWS Transit Gateway (Amazon VPC ドキュメント)
- VPC ピアリングとは (Amazon VPC ドキュメント)

その他の AWS リソース

- Amazon Virtual Private Cloud 接続オプション (AWS ホワイトペーパー)
- AWS re:Invent 2021 - AWS ワークロードに適したロードバランサーを選択する方法 (YouTube)
- SaaS とは (ウェブサイト) AWS
- AWS SaaS Factory プログラム (AWS Partner プログラム)
- でのマルチテナントアーキテクチャのガイダンス AWS (AWS ソリューションライブラリ)

ドキュメント履歴

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

変更	説明	日付
初版発行	—	2025 年 9 月 12 日

AWS 規範ガイダンスの用語集

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

数字

7 Rs

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

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

- 廃止 — お客様のソース環境で不要になったアプリケーションを停止または削除します。

A

A2A (Agent-to-Agent)

タスクの委任と状態転送をサポートするagent-to-agentコラボレーション用のステートフルプロトコル。

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。

[エージェント]

目標を達成するためのツールを使用して、自律的に推論、計画、アクションを実行できる AI システム。

エージェントオペレーション

AI エージェントを本番環境で大規模に構築、テスト、デプロイ、実行するための運用プラクティス。

集計関数

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

AI

「人工知能」をご覧ください。

AIOps

「AI オペレーション」をご覧ください。

匿名化

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

アンチパターン

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

アプリケーション制御

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

アプリケーションポートフォリオ

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

人工知能 (AI)

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

AI オペレーション (AIOps)

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

非対称暗号化

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

原子性、一貫性、分離性、耐久性 (ACID)

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

属性ベースのアクセス制御 (ABAC)

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

信頼できるデータソース

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

アベイラビリティーゾーン (AZ)

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

AWS クラウド導入フレームワーク (AWS CAF)

組織がクラウドへの移行を成功させるための効率的で効果的な計画を立て AWS るための、 のガイドラインとベストプラクティスのフレームワークです。 AWS CAF は、ビジネス、人材、ガバナンス、プラットフォーム、セキュリティ、運用という 6 つの重点分野にガイダンスを整理しています。ビジネス、人材、ガバナンスの観点では、ビジネススキルとプロセスに重点を置き、プラットフォーム、セキュリティ、オペレーションの視点は技術的なスキルとプロセスに焦点を当てています。例えば、人材の観点では、人事 (HR)、人材派遣機能、および人材管理を扱うステークホルダーを対象としています。この観点から、 AWS CAF は、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。

シチズンデベロッパー

専門的な技術スキルを持たないノーコード/ローコードプラットフォームを使用して AI アプリケーションを作成するビジネスユーザー。

クライアント側の暗号化

ターゲットが AWS のサービス 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。

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。たとえば、 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。

FM ゲートウェイ

基盤モデルへのアクセスを制御および正規化する一元化された仲介者。LLM ゲートウェイとも呼ばれます。

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。

ガードレール (AI)

エージェントの入力と出力をフィルタリング、検証、制約して、責任ある安全な AI 動作を確保するのに役立つ安全メカニズム。

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。

ヒューman-in-the-loop (HitL)

エージェント???の実行が重要な決定時点で人間によるレビューと承認のために一時停止するワークフローパターン。

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。

MCP

「モデルコンテキストプロトコル」を参照してください。

モデルコンテキストプロトコル (MCP)

エージェントツーツール通信のステートレスプロトコル。

MCP サーバー

Model Context Protocol を通じて 1 つ以上のツールを公開するサービス。

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 とは独立しています。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 にログイン AWS マネジメントコンソール したり AWS API オペレーションを呼び出したりでき、組織内のすべてのユーザーを IAM で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

「監視制御とデータ取得」を参照してください。

SCP

「サービスコントロールポリシー」を参照してください。

シークレット

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

セキュリティバイデザイン

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

セキュリティコントロール

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

セキュリティ強化

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

Security Information and Event Management (SIEM) システム

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

セキュリティレスポンスの自動化

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

サーバー側の暗号化

送信先にあるデータを、 AWS のサービス が受信する によって暗号化します。

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。

シャドウ AI

組織内の管理対象チャネルの外部で構築または使用される認可されていない AI アプリケーション。

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。

tool

エージェントが外部システムでオペレーションを実行するために呼び出すことができる関数または API。

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。