AWS Well-Architected Framework

SAP Lens

SAP Lens: AWS Well-Architected Framework

Table of Contents

概要

公開日: 2021 年 10 月 28 日 (ドキュメント履歴)

このペーパーでは、AWS Well-Architected フレームワーク用の SAP Lens について説明します。お客様に実証された設計原則と AWS での SAP ワークロードを優れた設計にするためのベストプラクティスを集めたものです。SAP Lens を AWS Well-Architected Frameworkの捕捉として使用します。このフレームワークは、AWS で、安全、高性能、回復力があり、効率的なアプリケーションとワークロードを構築するための基礎を提供します。

SAP Lens は、AWS がお客様、AWS パートナー、SAP スペシャリストコミュニティから収集したインサイトに基づいています。レンズは、実行している SAP にクラウドネイティブのアプローチを採用するのに役立つように設計されています。これは、AWS Well-Architected Framework の 5 本の柱である運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、およびコスト最適化に沿って、改善のための最も一般的な領域をハイライトします。

このコンテンツでは、エンタープライズリソースプランニング (ERP) アプリケーションで最もよく知られた企業、SAP が提供する AWS で動作するソフトウェアとして SAP に言及します。このガイダンスは、SAP Business Suite、SAP S/4HANA、サポート製品を含む、AWS で実行できるすべての SAP ソフトウェアをカバーすることを目的としています。レコメンデーションが 1 つの SAP アプリケーションまたはデータベースに固有の場合、強調されています (例えば、SAP HANA データベース)。

このドキュメントの対象読者は、SAP テクノロジーアーキテクト、クラウドアーキテクト、および AWS で SAP システムを構築、運用、保守するチームメンバーです。

レンズの使用方法

このレンズを使用して、SAP on AWS ワークロードを、実装前、実装中、実装後に評価します。このレンズは、AWS Well-Architected Framework のコンテンツを追加し、それらの基盤となるベストプラクティスを解釈して SAP ワークロード設計に採用する方法を明確にします。

このレンズと Framework を連携して使用し、エンタープライズチームと密接に協力して、SAP とエンタープライズの要件に対応することをお勧めします。重複を避けるため、ガイダンスがより包括的な内容か、特定の SAP のコンテキストがない場合は、AWS Well-Architected Framework へのリンクを表示しています。

このレンズを使用するには、以下のステップを実行してください。

1. このドキュメント、幅広い内容の AWS Well-Architected Framework と柱となるホワイトペーパーをよく読んで理解してください。
2. SAP 固有の設計ドキュメント、オペレーション手順、モニタリング履歴 (利用可能な場合) を集めます。
3. SAP ワークロード実装とオペレーションをこのドキュメントで説明されているベストプラクティスと比較します。
4. それぞれのベストプラクティスについて、実行されているかどうかを記録し、必須のものの評価を優先します。
5. ワークロードがうまく設計されていない領域に対応する解決策として、提供されている提案を使用します。

さらに専門的なガイダンスが必要な場合は、AWS アカウントチームに連絡して、SAP スペシャリストソリューションアーキテクトを依頼します。

ワークロードをレビューした後、ワークロードがうまく設計された箇所と、改善が必要な箇所を示すベストプラクティスのリストが得られます。

- 優れたアーキテクチャコンポーネントの場合: 知識をチームと共有し、組織全体で増強します。
- ワークロードがまだ準拠できていないベストプラクティスの場合: ビジネスに対する技術的負債およびリスクとして扱います。内部のリスク管理プロセスに従い、これらのリスクを継続的に、モニタリングして改善します。
- さらに詳しい分析が必要な領域、または改善に支援が必要な場合: AWS プロフェッショナルサービスに問い合わせるか、AWS パートナーに相談します (AWS SAP 認定パートナーリストを参照).

詳細については、以下のリンクと情報を参照してください。

- AWS ドキュメント: レビュープロセス - AWS Well-Architected Framework

定義

期間	説明	例 (該当する場合)
SAP ワークロード	ワークロードとは、ビジネス価値をもたらす SAP のリソースの集合体です。SAP コンテキストでは、これには、SAP アプリケーションおよび SAP バックエンドプロセスの顧客向けコンポーネントが含まれます。ワークロードは、単一の AWS アカウント内にあるリソースのサブセットからなる、または複数の AWS アカウントにまたがるリソースの集合である場合があります。	
SAP 製品	あらゆる業種でビジネスプロセスのためのソリューションを提供するエンタープライズソフトウェア会社、SAP の製品。場合により、 SAP ソリューションとも呼ばれます .	SAP S/4HANA オンプレミスエディション、Concur、Qualtrics
SAP システム	通常、SAP システム識別子 (SID) によって特徴付けられるアーキテクチャの論理グルーピング (より大きいメカニズムの一部として連携して働く一連のもの)。	本番稼働 ERP システム
SAP システム識別子 (SAP SID/DB SID)	SAP システムを一意に識別するために使用する文字と数字の組み合わせ。	PRD、HDB、PR1
SAP 環境	1 つまたは複数の SAP 製品またはテクノロジーコンポーネントの統合されたグループ化。リンクされており 本稼働環境への道筋を形成します。	サンドボックス、開発、QA、トレーニング、テスト、本番稼働前、お

期間	説明	例 (該当する場合)
		よび本番稼働。
SAP インスタンスまたはホスト	インスタンスは、AWS クラウドで仮想サーバーとして動作する Amazon マシンイメージ (AMI) のコピーです。SAP コンテキストでは、通常、Amazon EC2 サービスでのコンピューティングインスタンスです。	
SAP テクニカルコンポーネント	インスタンスまたはホストで動作する SAP システムのコンポーネントをまとめる管理単位。これらは、SAP アプリケーションの技術的アーキテクチャ構築ブロックです。	アプリケーションサーバー (PAS または AAS)、SAP HANA データベース、Web Dispatcher
サービス (AWS サービス)	ビジネスおよび組織の要件に合わせて調整され、組み合わせて使用される 200 を超えるクラウドサービス。多数の AWS のサービスの詳細については、アマゾン ウェブ サービスの概要ホワイトペーパーを参照してください。	Amazon EC2、Simple Storage Service (Amazon S3)、Amazon EFS
SAP デプロイ/デプロイパターン	SAP プロビジョニングツール (SUM、SWPM) でのオプションに関連して SAP がどのようにデプロイされているかを説明するために使用されます。	高可用性 (HA)、分散、スタンドアロン

期間	説明	例 (該当する場合)
SAPS 評価 (多くの場所で SAPS と呼ばれます)	SAP アプリケーションパフォーマンススタンダード (SAPS) – は、SAP 環境におけるシステム構成の性能を記述するハードウェアに依存しない測定単位です。販売およびディストリビューション (SD) ベンチマークから派生しており、100 の SAPS が 1 時間あたり 2,000 の完全に業務処理された注文明細項目と定義されます。 詳細はこちら: SAP スタンダードアプリケーションベンチマーク .	Amazon EC2 インスタンスタイプ *c5.large* は、3,650 の SAPS を提供します。

AWS ドキュメント: AWS 用語集

ワークロードコンテキストチェックリスト

ビジネスのコンテキストに関する理解を深めるには、以下の情報を収集する必要があります。

ID	優先度	ワークロードコンテキスト
□ C1	必須	ワークロードの名前
□ C2	必須	ビジネスの目的、重要業績評価指標 (KPI)、ワークロードの対象ユーザーを含む説明。
□ C3	必須	レンズのレビューをリードするレビュー所有者
□ C4	必須	ワークロードのメンテナンスに責任があるワークロード所有者
□ C5	必須	ワークロードを後援するビジネスステークホルダー
□ C6	必須	情報セキュリティ、ファイナンス、リーガルなど、ワークロードに関与しているビジネスパートナー
□ C7	推奨される	ワークロードを説明するアーキテクチャ設計ドキュメント
□ C8	推奨される	ワークロードと関連付けられている AWS アカウント ID
□ C9	推奨される	ワークロードに関連した規制コンプライアンス要件 (ある場合)

Well-Architected 設計原則

このセクションでは、SAP ワークロードを設計および運用するときに関連する、設計原則、ベストプラクティス、改善の提案について説明します。

それぞれの Well-Architected の柱で見つかるガイダンスも読んで適用することをお勧めします。これには、すべてのワークロードに関連する、運用上の優秀性、セキュリティ、信頼性、パフォーマンス効率、コスト最適化の基盤となるベストプラクティスが含まれます。

柱

- 運用上の優秀性
- セキュリティ
- 信頼性
- パフォーマンス効率
- コスト最適化

設計原則の完全なリストは、次を参照してください。 柱別にまとめた設計原則.

運用上の優秀性

運用上の優秀性の柱では、ワークロードを効率的に開発して実行し、オペレーションに関するインサイトを得て、ビジネス価値をもたらすためのサポートプロセスを継続的に改善する能力に重点を置きます。

このセクションには、一連の設計原則と SAP ワークロードのガイダンスを提供するために具体的にカスタマイズされたレコメンデーションが記載されています。それらの 運用上の優秀性の柱 には、幅広い設計原則とレコメンデーションが含まれます。この後の SAP ガイダンスと併せて読むことを強く推奨します。

1 - 状態の理解と反応ができるように SAP ワークロードを設計する

SAP ワークロードの状態を理解できるようにするには、ワークロードをどう設計すればよいでしょうか? SAP ワークロードを設計する際には、すべてのコンポーネントにわたって内部および外部状態を理解するために必要な情報を提供するようにします。インフラストラクチャ、SAP テクノロジー/ベース、フロントエンド、ネットワークコンポーネントを検討します。リアルタイムのモニタリングができるメトリクスをキャプチャする、モニタリングとログ記録のアプローチ、および修復とイベント後の分析ができる履歴ログ記録を設計します。

ID	優先度	ベストプラクティス
□ BP 1.1	必須	SAP on AWS のモニタリングの前提条件を実装する
□ BP 1.2	必須	SAP にインフラストラクチャモニタリングを実装する
□ BP 1.3	必須	SAP の個別アプリケーションモニタリングの実装
□ BP 1.4	強く推奨	ワークロード設定モニタリングを実装する
□ BP 1.5	強く推奨	ユーザーアクティビティモニタリングを実装する
□ BP 1.6	強く推奨	依存関係のモニタリングを実装する
□ BP 1.7	推奨される	SAP ワークロード全体でヘルスモニタリングの一括管理を実装する
□ BP 1.8	推奨される	自動化された応答と回復技術を使用してモニタリングアラートに対応する

詳細については、以下のリンクと情報を参照してください。

- AWS ドキュメント: AWS Data Provider for SAP (SAP 向け AWS データプロバイダー)
- AWS サービス: Amazon CloudWatch
- SAP on AWS ブログ: Serverless Monitoring for SAP (SAP 向けサーバーレスモニタリング)
- SAP on AWS ブログ: AWS DevOps for SAP - driving innovation and lowering costs (SAP 向け AWS DevOps – イノベーションの促進とコストの削減)
- AWS Marketplace: SAP モニタリング向け製品とツール
- SAP Note: 1656250 - SAP on AWS: Support Prerequisites (サポートの前提条件) [SAP ポータルへのアクセス権が必要]
- SAP ドキュメント: SAP Solution Manager 7.2 - Application Operations

ベストプラクティス 1.1 - SAP on AWS をモニタリングするための前提条件を実装する

SAP on AWS の SAP 認定要件は、SAP Note 1656250 に記載されています。この Note には、SAP 向け AWS データプロバイダーの設定、Amazon CloudWatch 詳細モニタリングの有効化、SAP

NetWeaver ソリューションでの SAP 拡張モニタリングの使用の手順が含まれています。これらの前提条件を有効にすると、AWS と SAP により SAP ワークロードの状態が完全に理解および調査されるようにできます。これらの前提条件は、全体的な SAP モニタリング戦略に入れる必要があります。

提案 1.1.1 - SAP サポート前提条件をチェックする

SAP サポートポータルで SAP on AWS ワークロードの最新のサポート前提条件について SAP Note 1656250 をチェックします。この Note の詳細な手順に従ってください。

- SAP Note: 1656250 - SAP on AWS: Support Prerequisites (サポートの前提条件) [SAP ポータルへのアクセス権が必要]

提案 1.1.2 - SAP NetWeaver ワークロード向け AWS データプロバイダーをインストールする

SAP 向け AWS データプロバイダーは、SAP NetWeaver ワークロードをサポートする EC2 インスタンスそれぞれでインストールする必要があります。SAP 向け AWS データプロバイダーは、AWS サービスからパフォーマンス関連のメトリクスを収集し、SAP 内部アプリケーションモニタリングシステムに提供します。トランザクションコード ST06n や通常、SAPOSCOL サービスから収集される外部メトリクスを使用する Systems Manager のモニタリングなどの SAP ツールは、AWS メトリクスにアクセスするために SAP 向け AWS データプロバイダーが必要です。

詳細なモニタリングと、特定の間隔で SAP がモニタリングデータを受信するために必要な API コールの増加のため、SAP 向け AWS データプロバイダーの実行に関連して間接的なコストが発生します。参照先 SAP 向け AWS データプロバイダーのインストール で詳細を確認してください。この理由で、SAP サポートと分析が必要な場合、非本番稼働環境では、SAP 向け AWS データプロバイダーのみを有効にすることを検討した方がよいかもしれません。

- AWS ドキュメント: AWS Data Provider for SAP (SAP 向け AWS データプロバイダー)

提案 1.1.3 - SAP ワークロードのモニタリング戦略を作成する

SAP アプリケーションの現在のヘルスと履歴のヘルスを内側から外側と外側から内側の両方の視点で観察する方法を決定します。連携してエンドユーザーエクスペリエンスを提供するすべてのコンポーネントを検討します。内部 SAP アプリケーションメトリクスと外部ユーザーパフォーマンスおよび信頼性モニタリングに加えて、基盤となる AWS コンピューティング、ストレージ、ネットワークサービスからメトリクスをキャプチャするかを検討します。各コンポーネントの異なるツールを評価し、必要なときに根本原因分析を実行するための 1 つの場所 (例えば、ログの集約) でこれらをま

とめる方法を決定します。この情報を使用してアラートしきい値を設計する方法としきい値に達したときに実行する修復アクションを決定します。

SAP Solution Manager のモニタリング、サードパーティーのモニタリングツール、カスタム SAP モニタリングメトリクスを設計の開始ポイントとして取り込める CloudWatch ダッシュボードの機能を理解します。

- AWS ドキュメント: SAP NetWeaver on AWS: Monitoring Guide (SAP NetWeaver on AWS: モニタリングガイド)
- SAP on AWS ブログ: Serverless Monitoring for SAP NetWeaver (SAP NetWeaver 向けサーバーレスモニタリング)
- SAP on AWS ブログ: Serverless Monitoring for SAP HANA (SAP HANA 向けサーバーレスモニタリング)
- AWS サービス動画: Gaining Better Observability of Your VMs with Amazon CloudWatch (Amazon CloudWatch で VM の可観測性を改善する)
- AWS Marketplace: SAP モニタリング向け製品とツール
- SAP ドキュメント: SAP Solution Manager 7.2 - Application Operations
- SAP ドキュメント: SAP NetWeaver Alert Monitor

ベストプラクティス 1.2 – SAP のインフラストラクチャモニタリングを実施する

SAP アプリケーションの動作を維持し、ユーザーをサポートするため使用されるサポートサービスについても情報を提供する、インフラストラクチャモニタリングを設定します。例としては、CPU とメモリ使用率、ストレージとファイルシステム使用率、パフォーマンス (IOPS およびスループット)、ネットワークのスループットがあります。SAP が使用するあらゆる依存基礎サービスが含まれます。これにはオンプレミスアクティブディレクトリサービス、DNS、高可用性 (HA) やバックアップソフトウェアのようなサードパーティーツールなどがあります。DataDog、Splunk、DynaTrace、Avantra など、この情報を相互に関連付け可視化するのに役立つ AWS Marketplace の AWS ツールと SAP 固有のツールを評価します。この情報を使用して、傾向を識別し、是正措置が必要とされるタイミングを特定します。

提案 1.2.1 - SAP をサポートするサービスに CloudWatch メトリクスとアラームを実装する

Amazon CloudWatch の詳細なモニタリングメトリクスとすべての SAP システムに対するアラームのしきい値を実装します。これらのメトリクスとアラームには、SAP システムの可用性とパフォーマンスに影響する可能性がある一般的な問題のモニタリングを含める必要があります。一般的なインフラストラクチャモニタリング領域は、Amazon Elastic Compute Cloud (EC2) インスタン

ス、Amazon Elastic Block Storage (Amazon EBS) ボリューム、Elastic Load Balancing (ELB) に重点を置きます。

共通のモニタリング項目には以下が含まれます。

- Amazon EC2 の高い CPU 使用率
- Amazon EC2 の高いメモリ使用率
- Amazon EBS ストレージページング
- Amazon EBS ストレージのスループット
- Amazon EBS ストレージ IOPS
- Amazon EBS ストレージの空き容量といっぱいになっているボリュームの割合
- Amazon EC2 ネットワークの飽和
- ELB/ALB のヘルスとターゲットグループのヘルス

しきい値はシステムの履歴本番稼働使用状況の正常なパターンを基にします。問題を避けるためにアラームのしきい値を継続的に確認し、調整します。

使用を開始するには、以下のリソースを確認します。

- SAP on AWS ブログ: Serverless Monitoring for SAP NetWeaver (SAP NetWeaver 向けサーバーレスモニタリング)
- SAP on AWS ブログ: Serverless Monitoring for SAP HANA (SAP HANA 向けサーバーレスモニタリング)
- AWS ドキュメント: Create a CloudWatch Custom Metric (CloudWatch カスタムメトリクスを作成する)
- AWS ドキュメント: CloudWatch ダッシュボードの作成
- AWS ドキュメント: Amazon CloudWatch でのアラームの使用

提案 1.2.2 - SAP サービスに AWS のサービスクォータモニタリングを実装する

モニタリングツールまたはプロセスを実装して、 AWS Service Quotas を環境内で必要な SAP リソースについて追跡します。SAP 環境では、複数の Amazon EC2 インスタンスタイプを組み合わせて使用することも多く、一部のタイプでは異なる オンデマンドサービスクォータを使用することがあることも考慮してください .例えば、 `x1*` と `u*` EC2 インスタンスタイプには異なるサービスクォータがあり、以下の組み合わせたクォータとは別個です。 `c5` 、 `m5` 、および `r5` インスタンス

タイプ新しいワークロードを計画している場合、または既存のワークロードをスケーリングする場合は、Service Quotas にサポートされることを確認し、クォータライセンスが必要な場合は、AWS Support に依頼します。

- AWS ドキュメント: Service Quotas - AWS 全般のリファレンス
- AWS ドキュメント: オンデマンドインスタンス - Amazon Elastic Compute Cloud Service Quotas
- AWS ドキュメント: Requesting a quota increase - Service Quotas (クォータの引き上げをリクエストする - Service Quotas)

ベストプラクティス 1.3 - SAP の個別アプリケーションモニタリングの実装

内部状態、ステータス、ビジネス成果の達成に関する情報が得られるように、アプリケーションとデータベースのモニタリングを設定します。例としては、取引の応答時間、利用できる作業プロセス、キューの深度、エラーとダンプメッセージ、停止したバッチジョブ、取引のスループットがあります。この情報を使用して、是正措置が必要とされるタイミングを特定します。

提案 1.3.1 - SAP アプリケーションをサポートするデータベースのモニタリングを実装する

SAP データベースを継続的にモニタリングして、SAP システムの可用性とパフォーマンスに影響する可能性がある一般的な問題に対するアラートを確立します。共通のモニタリング項目には以下が含まれます。

- データエリアの空き容量
- ロギングエリアの空き容量
- 過剰なロックアクティビティ
- キャッシュ利用率
- 平均クエリ応答時間
- 必要なセキュリティパッチとホットフィックス
- 上部テーブルのサイズと拡大

アラートのしきい値はシステムの履歴生産使用状況の正常なパターンを基にします。アラームしきい値を継続的に確認して調整し、問題を回避してワークロードの変化や成長に対応します。

特定のデータベースのモニタリングを有効にする方法の詳細については、データベースソフトウェアプロバイダーのインストールおよび運用ガイドを参照してください。

提案 1.3.2 - SAP トランザクションとツールを使用して SAP アプリケーションを理解する

内部状態、ステータス、およびビジネス成果の達成に関する情報を提供するために SAP アプリケーションコードを設定します。この情報を使用して、応答が必要とされるタイミングを特定します。共通のモニタリング項目には以下が含まれます。

- アプリケーション (ASCS、PAS、AAS) とデータベースサービスの可用性
- アクティブな同時利用ユーザーの数
- ユーザーのための作業プロセスの可用性
- ユーザートランザクションの応答時間
- バッチおよび非インタラクティブトランザクションの応答時間
- エラーメッセージとダンプ
- 失敗したジョブ
- フルキューとスローキュー

SAP Solution Manager に SAP EarlyWatch Alert レポートシステム を設定し、SAP システムのステータスに関する定期的なレポートを作成します。これらのレポートに記載されている問題を定期的に確認し、修復して問題を回避し、ワークロードサービスの中断を避けます。

- SAP Note: 2729186 - General Process of EWA Generation (EWA 生成の一般的なプロセス) [SAP ポータルへのアクセス権が必要]
- SAP ドキュメント: SAP Solution Manager 7.2 - Application Operations
- SAP Lens [パフォーマンス効率]: ベストプラクティス 16.1 – パフォーマンスを評価するデータを持つ

提案 1.3.3 - データ回復と保護メカニズムのモニタリングを実装する

障害や災害の場合に SAP データを保護するメカニズムのモニタリングを実装します。共通のモニタリング項目には以下が含まれます。

- 例えば、Amazon S3 に AWS Backint Agent で実行するような通常のデータベースバックアップのアラート
- データベースレプリケーションのアラート、例えば、アベイラビリティーゾーンでの HANA システムレプリケーションの障害または遅延
- ファイルストレージバックアップのアラート、例えば、EBS スナップショット、Amazon EFS バックアップ、または Amazon FSx バックアップ

- リージョンにまたがるデータの回復性を提供する回復メカニズム (例えば、クロスリージョンレプリケーションのある Amazon S3 バケット、Amazon S3 同期または CloudEndure Disaster Recovery) のアラート
- アカウントにまたがるデータの回復性を提供するメカニズム (例えば、WORM S3 バケットまたはロギングアカウントへの同じリージョンレプリケーションがある Amazon S3 バケット) のアラート

詳細については、以下のリンクを参照してください。

- AWS ブログ: AWS Backup Audit Manager を使用したバックアップコンプライアンスのモニタリング、評価、デモンストレーション
- SAP ドキュメント: SAP HANA System Replication Verification and Monitoring (SAP HANA システムレプリケーションの検証とモニタリング)

提案 1.3.4 - 独立した可観測性が得られるように SAP ツール外の SAP モニタリングデータを公開する

SAP モニタリングツールは、アプリケーションとオペレーティングシステムレベルのモニタリングに限定され、SAP サービスの可用性とヘルスのエンドツーエンドビューが得られる幅広いサポートサービスをカバーしません。SAP アプリケーションを設定して、選択した包括的な、外部モニタリングと可視性ツールにメトリクスを提供します。

以前のベストプラクティスで収集したメトリクスを使用し、これらの結果を外部化して、トレンドをモニタリング、アラート、レポートできる独立したツールを持てるようにします。独立したツールでは、SAP システムの可用性とリンクすることなく (SAP が災害または障害モードの場合)、可観測性、根本原因分析、履歴およびトレンドレポート作成が可能です。

- SAP on AWS ブログ: Serverless Monitoring for SAP NetWeaver (SAP NetWeaver 向けサーバーレスモニタリング)
- SAP on AWS ブログ: Serverless Monitoring for SAP HANA (SAP HANA 向けサーバーレスモニタリング)
- AWS ドキュメント: Create a CloudWatch Custom Metric (CloudWatch カスタムメトリクスを作成する)
- AWS Marketplace: SAP モニタリング向け製品とツール

ベストプラクティス 1.4 – ワークロード設定モニタリングを実装する

現在の設定とこの設定に対する変更に関する情報が得られるようにワークロードを設計および設定します。例としては、新しいまたは削除された EC2 インスタンス、スケーリングイベント、コード変更、パッチレベル、セキュリティグループ設定、リソース削除があります。この情報を使用して、いつ対応が必要かを決め、変更が予想されていたか、許可されているかを判断します。設定変更のコストへの影響をモニタリングし、必要な場合は、予算を調整または分析します。

提案 1.4.1 - ワークロード設定モニタリングを実装する

AWS CloudTrail をセットアップして設定し、特に SAP 本番稼働用アカウントで、高優先度で重要なイベントをモニタリングします。イベントの例としては、新しい Amazon EC2 インスタンス、Amazon EC2 の廃止または変更、セキュリティグループの変更、AWS KMS および IAM セキュリティ変更イベントがあります。これらのイベントを使用して、CloudWatch ログアラーム (必要な場合) を設定し、予期しない変更の場合は対処します。

- AWS ドキュメント: AWS CloudTrail とは
- AWS サービス: AWS CloudTrail
- AWS ドキュメント: Amazon CloudWatch Logs による CloudTrail ログファイルをモニタリングする
- AWS ドキュメント: AWS CloudTrail セキュリティのベストプラクティス

提案 1.4.2 - ワークロード設定の実施と修復を実装する

AWS Config をセットアップして設定し、SAP 本番稼働アプリケーションをサポートする AWS リソースの設定ポリシーを追跡、評価、適用します。一般的な例としては、SAP バックアップを含む S3 バケット読み取り専用保護の適用、必須の Amazon EC2 EBS 暗号化、一般的なネットワークポートのブロック、すべてのリソースに必要なタグがあることの確認があります。AWS Config マネージドルール を使用して、セキュリティを向上させ、SAP をサポートする AWS 環境のコントロール体制を変更します。AWS タグを使用して、設定ルールを適用し、可能なところでは自動化された修復を適用します。

- AWS サービス: AWS Config
- AWS ドキュメント: AWS Config の開始方法
- AWS ドキュメント: AWS Config ルールの設定
- SAP on AWS ブログ: Audit your SAP systems with AWS Config – Part I (AWS Config で SAP システムを監査する – パート I)

- SAP on AWS ブログ: Audit your SAP systems with AWS Config – Part II (AWS Config で SAP システムを監査する – パート II)
- SAP on AWS ブログ: Tagging Recommendations for SAP on AWS (SAP on AWS のタグ付けレコメンデーション)

提案 1.4.3 - ワークロードコストモニタリングを実装する

カスタム予算で AWS Budgets をセットアップして設定します。カスタム予算は、請求しきい値を超える (または超えると予測される) ときにアラートを発します。予算を予想される SAP 環境の支出に合わせ、異常をモニタリングしてコスト超過を回避します。予算レポートを使用して、リザーブドインスタンスと Savings Plans の使用と範囲をモニタリングします。AWS タグを使用して、SAP ワークロードでのコスト割り当てと使用量の理解を支援します。

- AWS ブログ: Getting Started with AWS Budgets (AWS Budgets の開始方法)
- AWS ブログ: AWS Budgets Reports
- AWS ドキュメント: AWS Cost Explorer
- AWS ドキュメント: AWS Cost Anomaly Detection
- SAP on AWS ブログ: Tagging Recommendations for SAP on AWS (SAP on AWS のタグ付けレコメンデーション)

ベストプラクティス 1.5 – ユーザーアクティビティモニタリングを実装する

SAP アプリケーションを設定して、例えば、応答時間、アクティブユーザーの数、トランザクション放棄率、注文処理時間などのユーザーアクティビティに関する情報を提供します。内側から外側へのアプローチ (SAP 内部ダイアログ応答時間のモニタリング) と外側から内側へのアプローチ (エージェントまたはロボットをエンドユーザーの場所に地理的にデプロイ) の両方を検討して、エクスペリエンスで接続性がどのようなロールを果たすか理解します。この情報を使用して、アプリケーションの使用方法や使用パターンを理解したり、パフォーマンスが低いために対応が必要とされるタイミングを特定したりできます。

提案 1.5.1 - エンドユーザーの場所からユーザーエクスペリエンスモニタリングを実装する

エンドユーザーの場所にユーザーエージェントまたはロボットをデプロイして、外側から内側へのモニタリングアプローチにより、SAP ユーザーエクスペリエンスでネットワークと接続性がどのようなロールを果たすかを理解することを検討します。このタイプのエンドユーザーの場所ベースのモニタリングでは、中心的なインフラストラクチャやアプリケーションでは検出できない問題のインサイトや早期の警告が得られる場合があります。

エンドユーザーの場所からの SAP アプリケーションの応答性を測定するためのエンドユーザーエクスペリエンスを提供する、SAP またはサードパーティーツールを実装します。例えば、SAP は、Solution Manager でエンドユーザーエクスペリエンスモニタリングを提供し、複数のサードパーティー製品はリモートの場所にロボット (またはモニタリングスクリプト) をデプロイしてユーザーエクスペリエンスを測定できます。

- SAP ドキュメント: SAP User Experience Monitoring (SAP ユーザーエクスペリエンスモニタリング)
- AWS Marketplace: SAP モニタリング向け製品とツール

ベストプラクティス 1.6 – 依存関係のモニタリングを実装する

依存するリソースの状態 (到達可能性や応答時間など) に関する情報が得られるように、ワークロードを設定します。外部依存関係の例としては、インターフェイス (例えば、SAP PI/PO 経由)、外部データストア、DNS、オンプレミスコンポーネント、アクティブディレクトリコントローラーとネットワークデバイスなどがあります。この情報を使用して、応答が必要とされるタイミングを特定します。エンドツーエンドの依存関係のヘルスをモニタリングするためのクロステクノロジーメトリクスを提供できるサードパーティーモニタリングツールを検討してください。

提案 1.6.1 - 主要な SAP インターフェイスとクロスシステムビジネスプロセスの正常性追跡を実装する

SAP ワークロードが依存するキーインターフェイスを特定しモニタリングします。これらのインターフェイスエンドポイントのヘルス、エラー、キューの長さと成功率をモニタリングします。SAP の組み込みメカニズムまたはサードパーティー統合ツールを使用してインターフェイス障害または遅延にアラートを設定し、モニタリングツールにフィードします。すべてのインターフェイスパスウェイ:

- 異なる AWS ホスト SAP システム間 (RFC またはウェブサービス/HTTPS 経由で直接)
- AWS ホスト SAP システムとオンプレミスシステムの間 (HTTPS/SFTP - SAP PI またはサードパーティー統合プラットフォーム経由)
- AWS ホスト SAP システムと SAP Business Technology Platform (SAP Cloud Connector 経由) の間
- AWS ホスト SAP システムと外部パーティーシステムの間 (通常、インターネット/VPN 経由の HTTPS)

SAP と SAP 以外の環境でのシステム間依存関係モニタリングに Solution Manager ビジネスプロセスモニタリングを使用することを検討します。

- SAP ドキュメント: SAP Business Process and Interface Monitoring (SAP Business プロセスとインターフェイスのモニタリング)
- AWS Marketplace: SAP モニタリング向け製品とツール

提案 1.6.2 - SAP が依存するエンタープライズサービスの正常性追跡を実装する

SAP ワークロードが、ビジネスユーザーにとって正常な状態であるためには、通常、複数の基本的なエンタープライズサービスに依存します。モニタリングアプローチとツールでこれらの基盤サービスを検討します。基本的なサービスの例としては、オンプレミスシステム接続性のための Direct Connect、認証/SSO のためのアクティブディレクトリ、時間の同期のためのネットワークタイムプロトコル (NTP)、アンチウイルスサービス、オペレーティングシステムのパッチリポジトリ (例えば、Microsoft Windows Update または SUSE パッチ適用) への接続性が含まれます。

- AWS ブログ: Amazon CloudWatch Agent with AWS Systems Manager integration - unified metrics and log collection for Linux and Windows (AWS Systems Manager 統合を備えた Amazon CloudWatch エージェント - Linux と Windows 用の統合されたメトリクスとログ収集)
- AWS ドキュメント: CloudWatch エージェントを使用した Amazon EC2 Instances インスタンスとオンプレミスサーバーからのメトリクスとログの収集
- AWS ドキュメント: AWS Direct Connect の強化されたモニタリング機能

ベストプラクティス 1.7 – SAP ワークロード全体でヘルスモニタリングの一括管理を実装する

ワークロード全体のトランザクションフローに関する情報が得られるように、SAP アプリケーション、AWS のサービス、依存するコンポーネントを設定します。複数のソースからのメトリクスを組み合わせて、SAP ワークロードのヘルスの一括管理する可視性を作成し、このダッシュボードに主要なユーザーがアクセスできるようにします。この情報を使用して、応答が必要とされるタイミングをすばやく特定し、ビジネスに影響する問題につながる要素の特定に役立てます。

提案 1.7.1 - アプリケーションメトリクス、ワークロード設定、ユーザーメトリクス、依存関係ヘルスを 1 つの場所で結合する

アプリケーションモニタリングメトリクス、ワークロード設定データ、ユーザーメトリクスと依存関係のヘルスを 1 つの場所またはツールに組み合わせ、SAP ワークロードとそのヘルスをエンド

ユーザービジネスプロセスがエンドツーエンドでモニタリングできるようにします。これは、SAP Solution Manager、カスタム CloudWatch ダッシュボードとメトリクス、またはサードパーティーのモニタリングツールの使用により実現できます。

ベストプラクティスは、ワークロードの可用性のドリルダウンビューが可能な、ヘルスとトレンドの交通信号を備えたビジネス向けヘルスダッシュボードを作成することです。ドリルダウン機能により、ユーザーとオペレーターは、問題の原因になっている、またはパフォーマンスが低い可能性がある、テクノロジースタックの特定のコンポーネントを評価できます。

- AWS ドキュメント: CloudWatch ダッシュボードの作成
- SAP on AWS ブログ: Serverless Monitoring for SAP NetWeaver (SAP NetWeaver 向けサーバーレスモニタリング)
- SAP on AWS ブログ: Serverless Monitoring for SAP HANA (SAP HANA 向けサーバーレスモニタリング)
- AWS Marketplace: SAP モニタリング向け製品とツール
- SAP ドキュメント: SAP Solution Manager 7.2 - Application Operations

ベストプラクティス 1.8 – 自動化された応答と回復技術を使用してモニタリングアラートに対応する

イベントへの対応を自動化し、手動プロセスによって発生するエラーを減らして、迅速かつ一貫した対応を実現します。

提案 1.8.1 - オートメーションサービスを使用して、イベントに対する応答を自動化する

モニタリングツールからトリガーされる修復アクティビティの実行を自動化するには、複数の方法があります。一般的に、すべての SAP アプリケーションとデータベースイベントを、それに応じてイベントベースのオートメーションを提供する単一のチャネルに送り込む必要があります。

AWS リソースの状態変更や SAP の独自のカスタムイベントからのイベントに応答するには、EventBridge ルール を作成して、イベント ターゲット (例えば、Lambda 関数、Amazon Simple Notification Service (Amazon SNS) トピック、Amazon ECS タスク、AWS Systems Manager オートメーションなど) でアクションを呼び出すことができます。AWS Systems Manager オートメーションは、sapcontrol コマンドを呼び出し、自動的に SAP システムタスクを実行するために使用できます。

リソースのしきい値を超えるメトリクス (待機時間など) に応答するには、 CloudWatch アラーム 1 つ以上のアクションを実行する Amazon EC2 アクション 、 Auto Scaling アクション 通知を Amazon SNS トピック .

アラームに応答してカスタムアクションを実行する必要がある場合は、Amazon SNS 通知または AWS Systems Manager オートメーションを通じて Lambda を呼び出します (例えば、アクション `aws:runCommand` を使用します)、次を参照してください。 AWS ブログ: SAP システムの起動停止自動化をAWS Systems Manager で実現 .

Amazon SNS を使用して、イベント通知とエスカレーションメッセージを発行し、人々に情報を提供します。

また、AWS は、AWS のサービス API と SDK を通じてサードパーティーシステムもサポートしています。AWS パートナーやサードパーティーでは、モニタリング、通知、応答を可能にするモニタリングツールを多数提供しています。これらのツールには、Avantra、New Relic、Splunk、Loggly、SumoLogic、Datadog などがあります。

組織に該当する場合は、イベントとインタラクションをサードパーティー ITIL ツールにプッシュすることを検討します。例としては、 AWS から ServiceNow への 統合などがあります。

自動化された手順が失敗した場合に、手動でも重要な手順を実施できるようにしておく必要があります。

2 – SAP 変更の欠点を減らし、修正を簡単にし、フローを改善する

どのように欠陥を減らし、修正を容易にして、本番環境へのフローを改善するのですか? リファクタリング、品質についてのすばやいフィードバック、バグ修正を可能にし、本番環境への変更のフローを改善するアプローチを採用します。これらにより、本番環境に採用される有益な変更を加速させ、デプロイされた問題を制限できます。またデプロイアクティビティを通じて挿入された問題をすばやく特定し、修復できます。

ID	優先度	ベストプラクティス
□ BP 2.1	必須	バージョン管理と設定管理を使用する
□ BP 2.2	必須	コード品質の向上のためにプラクティスを実装する
□ BP 2.3	必須	構築およびデプロイ管理システムを使用する
□ BP 2.4	必須	複数の環境を使用する

ID	優先度	ベストプラクティス
□ BP 2.5	必須	変更をテストし、検証する
□ BP 2.6	強く推奨	小規模かつ可逆的な変更を頻繁に行う
□ BP 2.7	推奨される	変更のテスト、統合、デプロイを自動化する

詳細については、以下のリンクと情報を参照してください。

- AWS 動画: Ops を考慮に入れて設計する
- AWS ドキュメント: AWS デベロッパーツール
- AWS ドキュメント: AWS Launch Wizard for SAP
- SAP on AWS ブログ: DevOps for SAP – Driving Innovation and Lowering Costs (SAP 向け DevOps – イノベーションの促進とコストの削減)

ベストプラクティス 2.1 - バージョン管理と設定管理を使用する

Configuration Management システムは、手動プロセスによって発生するエラーと、変更を導入する労力を減らします。そうすることで、変更の追跡、新しいバージョンのデプロイ、既存バージョンへの変更の検出、以前のバージョンの回復 (障害が発生する場合に、その前の良好な状態に戻すなど) をサポートします。設定管理システムのバージョン管理機能を SAP 全体のすべての手順 (インフラストラクチャ、データベース、アプリケーション、SAP カスタムコードと開発) に統合します (例えば、ABAP、Java、UI5/JavaScript)。

各タイプの設定に異なるバージョン管理システムを検討しますが、メトリクスをセントラルリリース計画ツールに統合します。非トランスポータブル設定とバイナリバージョニングを環境全体で管理する方法を検討します。(例: SAP カーネルバージョンが環境全体で整合していることをどのように確認しますか?)。

提案 2.1.1 - SAP 開発コードとバージョン管理に SAP 変更管理またはその他のサードパーティー製ツールを実装する

すべての開発アプローチと SAP アプリケーション (ABAP、Java、UI5/JavaScript) およびその他の拡張機能やスクリプティングエリアをサポートするカスタムコードを実装していることを確認します。複数の SAP デプロイパターンですべての SAP アプリケーションとコードデプロイをオーケス

トレートする方法を検討します (例えば、AWS と SAP ビジネステクノロジープラットフォームでホストされている関連した開発を同時にリリースする方法)。

- AWS サービス: AWS CodeCommit
- AWS 動画: AWS CodeCommit の紹介
- SAP on AWS ブログ: SAP 用の AWS DevOps ツール、パート 1: Cloud Foundry アプリケーション
- SAP on AWS ブログ: AWS DevOps tools for SAP, Part 2: SAP Fiori Apps (SAP 向け AWS DevOps ツール、パート 2: SAP Fiori アプリ)
- SAP ドキュメント: SAP 変更制御管理
- SAP ドキュメント: SAP BTP のベストプラクティス - ライフサイクル管理

提案 2.1.2 - SAP アプリケーションの設定管理システムを実装する

ABAP、Java、およびその他の SAP テクノロジーに設定管理ツールを実装し、非トランスポータブル設定とバイナリバージョニングを環境全体で管理する方法を検討します。(例: SAP カーネルバージョンが環境全体で整合していることをどのように確認しますか?)。SAP Solution Manager を使用して、設定とバージョン変更を計画し、SAP アプリケーションに実装します。

- SAP ドキュメント: Enhanced Change & Transport System (CTS+) (拡張された変更および転送システム (CTS+))
- SAP ドキュメント: SAP Solution Manager: Planning Landscape Changes (SAP Solution Manager: 環境変更の計画)

提案 2.1.3 - オペレーティングシステムの設定管理システムを実装する

AMI ベーキングまたは Ansible、Chef または Puppet などのインプレース設定管理ソフトウェアを使用して、SAP ワークロード オペレーティングシステム全体の設定管理を整合します。脆弱性のアラートを発し、オペレーティングシステムにパッチを適用して強化するように促す、セキュリティに重点を置いた設定管理ツールを検討します。

- AWS ドキュメント: AWS Systems Manager State Manager
- AWS ドキュメント: Configuration management in Amazon EC2 (Amazon EC2 での構成管理)
- AWS ドキュメント: AWS OpsWorks とは?
- AWS ドキュメント: Amazon Inspector とは

提案 2.1.4 - データベースの設定管理システムを実装する

データベースソフトウェアベンダーと連携して、使用しているデータベースの設定管理アプローチを理解します。

- SAP ドキュメント: SAP HANA Platform Lifecycle Management (SAP HANA プラットフォームライフサイクル管理)

提案 2.1.5 - インフラストラクチャの設定管理システムを実装する

Infrastructure as Code (IaC) アプローチを使用して SAP ワークロードをサポートする AWS リソースをプロビジョンおよび管理します。AWS CloudFormation と AWS Cloud Development Kit は、AWS リソースでプログラムにより設定をプロビジョニングして管理できるツールです。ルールとポリシーを作成して定期的にインフラストラクチャを評価し、コンプライアンスを評価して問題があれば解決できる、設定監査と管理ツールを検討します。

- AWS ドキュメント: AWS Launch Wizard for SAP
- AWS ドキュメント: AWS Systems Manager インベントリ
- AWS ドキュメント: AWS Systems Manager Change Manager
- SAP on AWS ブログ: Infrastructure as Code Example: Terraform and SAP on AWS (Infrastructure as Code の例: Terraform と SAP on AWS)
- SAP Lens [信頼性]: ベストプラクティス 11.3 - サービスの可用性を復元するためのアプローチを定義する

ベストプラクティス 2.2 – コード品質の向上のためにプラクティスを実装する

コード品質の向上のためにプラクティスを実装し、欠陥を最小限に抑えます。例えば、テスト駆動型デプロイ、コードレビュー、標準の導入などがあります。少なくとも SAP Code Inspector ツールを使用します。

提案 2.2.1 - コード品質の向上のためにプラクティスを実装する

例えば、テスト駆動型デプロイ、ペアプログラミング、コードレビュー、規約の導入などがあります。

提案 2.2.2 - SAP 開発用 Code Amazon Inspector ツールを使用して、このプロセスを CI/CD パイプラインに統合する

SAP ワークロードでの自動コード検査とリンティングに以下のツールを検討してください。

- AWS ドキュメント: Amazon CodeGuru - AWS Java および Python 開発用

- SAP ドキュメント: SAP Code Inspector for ABAP and SAP-specific development (ABAP と SAP 固有の開発向け SAP Code Inspector)

ベストプラクティス 2.3 – 構築およびデプロイ管理システムを使用する

構築およびデプロイ管理システムを使用します。ABAP 変更および転送システム (CTS)、ウェブ IDE または SAP ツールなど SAP 認定ビルドとデプロイシステムを使用していることを確認します。これらのシステムは、手動プロセスによって発生するエラーと、変更を導入する労力を減らします。

提案 2.3.1 - SAP 構築およびデプロイシステムを実装する

ABAP 変更および転送システム (CTS)、ウェブ IDE、SAP BTP 継続的デリバリーサービスまたはその他の SAP ツールなど SAP 認定ビルドとデプロイシステムを実装します。

- AWS 動画: ソフトウェア開発のための継続的インテグレーションのベストプラクティス
- SAP on AWS ブログ: AWS DevOps tools for SAP, Part 2: SAP Fiori Apps (SAP 向け AWS DevOps ツール、パート 2: SAP Fiori アプリ)
- SAP ドキュメント: Enhanced Change & Transport System (CTS+) (拡張された変更および転送システム (CTS+))
- SAP ドキュメント: Deploying Applications to BTP (BTP へのアプリケーションのデプロイ)

ベストプラクティス 2.4 – 複数の環境を使用する

複数の SAP 環境を使用して、ワークロードの実験、開発、テストを行います。環境が本稼働環境に近づくにつれて増加するコントロールレベルを使用して、デプロイ時にワークロードが意図したとおりに運用するように確信を強化します。通常、SAP 環境には、開発、テスト、製造の 3 層環境が最小要件です。

提案 2.4.1 - 実験に一時的な環境を使用する

テクノロジーテストおよびデベロッパーチームに、実験とリスクの軽減を有効にするための最小のコントロールを備えた、サンドボックスまたは一時的な環境を提供します。

- AWS ドキュメント: AWS Launch Wizard for SAP
- SAP on AWS ブログ: Infrastructure as Code Example: Terraform and SAP on AWS (Infrastructure as Code の例: Terraform と SAP on AWS)

提案 2.4.2 - 並行して作業し、俊敏性を向上させられるように開発環境を整備する

並行作業ができるように非本番稼働環境を提供し、開発とテストの俊敏性を高めます。開発者が必要なイノベーションの手段を利用できるように、本番に近い環境でより厳格なコントロールを実装します。通常、SAP 環境には、開発、テスト、本番稼働の 3 層環境が最小要件です。

- AWS ドキュメント: AWS Launch Wizard for SAP

提案 2.4.3 - リリース品質を向上させるため、できる限り本番稼働を再現する統合テスト環境を整備する

テストとステージング環境では、本番稼働環境のインターフェイス、セキュリティ、回復性、パフォーマンスの特性をできる限り忠実にミラーリングして、リリースする前にアーキテクチャとコードインタラクションの問題を特定する必要があります。この環境のコスト効率を向上させるために使用されていない場合、クラスターのセカンダリリソースをシャットダウンすることまたは環境のアプリケーションサーバーのパフォーマンスを (水平的および垂直的に) スケールダウンすることを検討します。

- SAP on AWS ブログ: SAP システムの起動停止自動化を AWS Systems Manager で実現

提案 2.4.4 - Infrastructure as Code (IaC) と設定管理システムを使用して一貫性のある環境をデプロイする

Infrastructure as Code (IaC) を使用したり、構成管理システムを使用したりして本番環境に存在するコントロールに準拠して設定された環境をデプロイし、システムがデプロイ時に予想どおりに動作することを確認します。タグ付けとリソースグループを使用して環境メタデータにラベル付けを行い強化し、オートメーションとコンプライアンスの目的に使用できるようにします。

- SAP on AWS ブログ: Infrastructure as Code Example: Terraform and SAP on AWS (Infrastructure as Code の例: Terraform と SAP on AWS)
- SAP on AWS ブログ: Tagging Recommendations for SAP on AWS (SAP on AWS のタグ付けレコメンデーション)
- AWS ドキュメント: AWS Launch Wizard for SAP
- AWS ドキュメント: AWS リソースグループとは何ですか。

提案 2.4.5 - 使用していないときは非本番稼働環境をオフにする

環境を使用しない場合は、オフにして、アイドル状態のリソース (夜間や週末の開発システムなど) に関連するコストを避けることができます。

- SAP on AWS ブログ: SAP システムの起動停止自動化を AWS Systems Manager で実現

ベストプラクティス 2.5 – 変更をテストし、検証する

すべてのライフサイクルステージ (開発、テスト、本番環境など) で変更をテストし、その結果を検証してください。テスト結果を使用して、新機能を確認し、失敗したデプロイのリスクと影響を緩和します。テストと検証を自動化し、レビューの一貫性を確保し、手動プロセスによって発生するエラーとそれにかかる労力を減らすことができます。

提案 2.5.1 - すべてのライフサイクルステージ (開発、テスト、本番環境など) で変更をテストし、その結果を検証する

提案 2.5.2 - 変更および主要なプロジェクトをリリースするときに比較するための、機能テスト、パフォーマンス、回復性にまたがるテスト結果のベースラインを維持する

提案 2.5.3 - 異なるレベルの変更にどのレベルのテストが必要かを理解する。例えば、フルスイートのテストとマイナーな更新のための対象を絞った回帰テスト。テストの定義と、本番稼働にリリースするためにテストが必要な変更の範囲について合意する。

提案 2.5.4. - サードパーティー製ツールとテストハーネスにより可能な箇所でテストを自動化する。まずは定期的な変更タイプと頻繁なリリースに重点を置く。

ベストプラクティス 2.6 – 小規模かつ可逆的な変更を頻繁に行う

頻繁に、小さく、可逆的な変更を行うことで、変更の範囲と影響を減らします。多数の SAP NetWeaver ソリューションは、「パッチフォワード」アプローチのみをサポートしますが、ロールバックを可能にするカスタム開発での機能トグルの使用を検討します。これにより、トラブルシューティングが容易になり、修復がすばやくできるようになります。また変更を元に戻すこともできます。

提案 2.6.1 - 可能な場合、開発とリリースを頻繁かつ小規模な変更に分割する

提案 2.6.2 - 多数の SAP ソリューションは、「パッチフォワード」アプローチのみをサポートする (そして可逆的転送を許可しない) ため、カスタム開発で機能トグルを使用して、ロールバック/撤回ではなく機能の無効化を許可する

提案 2.6.3 - 不可逆的な SAP の変更については、システム全体のスナップショット、データベースのバックアップ、復元オプションなど、ロールバックオプションの追加を検討する

- AWS ドキュメント: Amazon EBS クラッシュコンシステントスナップショット
- AWS ドキュメント: AWS Backint for SAP HANA

ベストプラクティス 2.7 – 変更のテスト、統合、デプロイを自動化する

ワークロードのビルド、デプロイ、テストを自動化します。これにより、手動プロセスによって発生するエラーと、変更をデプロイする労力を減らすことができます。

提案 2.7.1 - 構築、テスト、デプロイ、検証を通じたコードのチェックインから統合とデプロイのパイプラインを完全自動化する

提案 2.7.2 - アプリケーション変更のデプロイパイプラインにエンドツーエンドの構築をオーケストレートするために SAP Solution Manager ChaRM、Focused Build またはサードパーティー製の変更・リリース管理ツールを実装する

- SAP ドキュメント: SAP Solution Manager Change Request Management (SAP Solution Manager 変更リクエストの管理)
- SAP ドキュメント: SAP Focused Build
- AWS Marketplace: DevOps 向け製品とツール
- AWS Marketplace - テスト用の製品とツール
- SAP on AWS ブログ: SAP 用の AWS DevOps ツール、パート 1: Cloud Foundry アプリケーション

3 – ワークロードを運用する方法を理解する

ワークロードをサポートして運用する準備が整っていることはどうすれば確認できるでしょうか? 運用準備状況を ークロード 、プロセスと手順、人事に関して評価し、次に関する運用上のリスクを理解します: ークロード .一般的なオペレーションのためのランブック、問題のためのプレイブックを作成し、できる限り多数のオペレーションを自動化して、回復力を高め エラーを減少します。

ID	優先度	ベストプラクティス
□ BP 3.1	必須	従業員の対応力を確保する
□ BP 3.2	必須	クラウド運用モデルが運用目的と一致することを確認する
□ BP 3.3	必須	設計標準を共有し、新しいサポートスタッフに手順を指導する
□ BP 3.4	必須	ランブックを使用して SAP 環境オペレーションを実行する
□ BP 3.5	必須	プレイブックを使用して問題を調査する

ID	優先度	ベストプラクティス
□ BP 3.6	強く推奨	オートメーションを使用して SAP 環境オペレーションを実行する

詳細については、以下のリンクと情報を参照してください。

- AWS ホワイトペーパー: AWS クラウド運用モデル
- AWS サービス: AWS Config
- AWS ドキュメント: AWS Systems Manager の特徴
- SAP on AWS ブログ: DevOps for SAP – Driving Innovation and Lowering Costs (SAP 向け DevOps – イノベーションの促進とコストの削減)

ベストプラクティス 3.1 – 従業員の対応力を確保する

運用上のニーズに対応できるようにトレーニングを受けた、適切な人数の従業員が配置されていること、およびまた、適切な SAP、AWS、またはサードパーティーの認定を備えていることを検証するメカニズムを導入します。効果的なサポートを継続できるように必要に応じて従業員のトレーニングを実施し、従業員の対応力を調整します。

提案 3.1.1 - SAP オペレーションチームが必要な学習と認定を評価する

環境と依存関係により、異なる認定が適用される場合があります。テクノロジースタックをサポートできるようになるためにチームに必要な認定を評価します。

- AWS ドキュメント: AWS トレーニング
- AWS ドキュメント: AWS 認定
- オペレーティングシステム認定
  - SUSE ドキュメント: SUSE Enterprise Linux 認定
  - Red Hat ドキュメント: Red Hat Enterprise Linux 認定
  - Microsoft ドキュメント: Microsoft Windows 認定

ベストプラクティス 3.2 – クラウド運用モデルが運用目的と一致することを確認する

SAP ワークロードに適切なクラウド運用モデルを特定して、クラウドプラットフォームサポートのデプロイの速度、セキュリティ、オペレーションと責任に対して特定されたビジネス要件と一致する

ようにします。クラウドの導入に成功し、ビジネスの俊敏性を向上させるには、適切なクラウド運用モデルが重要です。

提案 3.2.1 - ビジネスの目的に適切なクラウド運用モデルを採用する

IT とビジネスの要件に従って、適切なクラウド運用モデルが採用されていることを確認します。どのチームがワークロードを構築して運用するかを決定します。SAP Basis/テクノロジーチームと開発チームの両方が DevOps モデルで SAP ワークロードを構築して実行する、共有の所有者のモデルに向かって進む計画を立てます。

- AWS ガイダンス: AWS クラウド でのオペレーションのモダナイゼーション
- AWS ホワイトペーパー: クラウド運用モデルの構築
- AWS 動画: Cloud Operating Models for Accelerated Transformation (トランスフォーメーションを加速するためのクラウド運用モデル)

ベストプラクティス 3.3 – 設計標準を共有し、新しいサポートスタッフに手順を指導する

既存のベストプラクティス、設計標準、チェックリスト、業務手順、ガバナンス要件をチーム間で共有します。すべてのチームが SAP ワークロードのすべてのコンポーネントにまたがるサポート手順を認識するようにします。

提案 3.3.1 - 既存のベストプラクティス、設計標準、チェックリスト、運用手順、ガイダンス、ガバナンスの要件をチーム間で共有し、複雑になるのを防ぎながら開発努力の成果を最大化する

提案 3.3.2 - 継続的な改善とイノベーションを支援するために、設計標準の変更、追加、例外を申請する手順を設ける

提案 3.3.3 - チームが公開済みのコンテンツを把握していることを確認し、コンテンツを活用して、やり直しや無駄な労力を制限する

提案 3.3.4 - チームが SAP ワークロードの異なるコンポーネントのサポートコールをログに記録する方法を知っていることを確認する

誰がオペレーティングシステム、データベース、SAP アプリケーションをサポートしていますか? 例えば、AWS またはオペレーティングシステムベンダーが、クラスタリングまたはパッチ適用の問題を直接サポートするかどうかを理解します。EC2 を含むオペレーティングシステムライセンスの場合、AWS はこのサポートを直接提供します。

- AWS ドキュメント: How to log a case with AWS Support (AWS Support でケースを口グに記録する方法)
- AWS ドキュメント: AWS サポート
- SAP Note: 1656250 - SAP on AWS: Support prerequisites (サポートの前提条件) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 3.4 – ランブックを使用して SAP 環境オペレーションを実行する

ランブックは、具体的な成果を達成するための文書化された手順です。ランブックに手順を文書化することにより、一貫性を保ち、汎用イベントにすみやかに対応できるようになります。実行される一般的な SAP オペレーションを理解し、レビューサイクルで具体的なバージョン管理されたドキュメントを作成します。

- AWS Well-Architected Framework [運用上の優秀性]: 運用即応性
- AWS ドキュメント: AWS Incident Manager を使用するランブックとオートメーション

提案 3.4.1 - SAP セキュリティオペレーションのための具体的なランブックを作成する

一般的な SAP セキュリティオペレーションのランブックを作成することを検討します。

- ユーザープロビジョニングとアイデンティティ管理
- Firefighter アクセス
- 認可の変更
- セキュリティと認可の監査
- 暗号化キーのローテーション
- TLS 証明書管理

提案 3.4.2 - SAP スケーリングとパフォーマンスオペレーションに特定のランブックを作成する

一般的なスケーリングとパフォーマンスオペレーションのランブックを作成することを検討します。

- ディスクボリュームのリサイズ
- SAP アプリケーションサーバーの水平的と垂直的スケーリング
- データベースサーバーのリサイズ
- ロードバランシングへのサーバーの追加または削除

提案 3.4.3 - 障害中の SAP オペレーションに特定のランブックを作成する

障害中のオペレーションのランブックを作成することを検討します。

- システムの再起動とシステムを再起動する順序
- SAP バックアップとリストア
- クラスターフェイルオーバー
- ストレージ障害
- 重要なインターフェイスの再開と再生
- DNS とネットワークルーティングの変更
- ランサムウェアからの復旧

提案 3.4.4 - SAP メンテナンスオペレーションに特定のランブックを作成する

次のメンテナンスオペレーションのランブックを作成することを検討します。

- SAP の起動と停止
- SAP の更新/システムコピー
- 毎日のヘルスチェック
- エラー管理/ABAP ダンプ
- SAP アプリケーション、オペレーティングシステム、データベースへのパッチ適用
- ログローテーション、クリーンアップ、アーカイブ

SAP 環境のデータベースアプリケーションログとトレースファイルのクリーンアップを検討します。例: SAP Note: 2399996 - Automating SAP HANA Cleanup (SAP HANA クリーンアップの自動化) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 3.5 – プレイブックを使用して問題を調査する

調査プロセスをプレイブックに文書化することで、よく理解されていない問題に対する一貫性のある迅速な対応が可能になります。これらのプレイブックをオペレーションだけでなく、非本番稼働環境やゲームデーなどの指定された練習セッションでも定期的に使用して、検証し進化させます。

提案 3.5.1 - インシデント対応で使用する問題プレイブックを作成する

頻繁に発生する問題と特定された問題のそれぞれに使用されるトラブルシューティングステップを理解し、具体的な、バージョン管理された、レビューサイクルのあるドキュメントを作成します。プレイブックには以下を含めることを推奨します。

- パフォーマンスの問題調査
- 容量の問題調査
- 認証とサインオンの問題の調査
- セキュリティインシデント調査
- 接続性とネットワークの調査
- ランサムウェアとウイルスの調査
- インターフェイスエラー調査
- バッチジョブエラー調査
- デプロイまたはトランスポートエラーの調査

プレイブックに関連するサポート機能やチームとの統合およびコミュニケーションステップが含まれていることを確認します。一般的なコミュニケーションステップには、重大インシデントデスク、セキュリティインシデントチームまたは変更管理チームへの通知と進捗の最新情報の提供が含まれます。

提案 3.5.2 - 通常の SAP ゲームデーを実行し、オペレーション手順をテストし、プレイブックを検証する

運用チームに SAP ゲームデーを定期的に実行することを検討します。ゲームデーでは、障害やイベントをシミュレーションしてシステム、プロセス、チームの対応をテストします。その目的は、例外的な出来事が発生した場合にチームが実行することになっているアクションを実際に実行することです。こうしたゲームデーを定期的に実施することで、チームは対応方法に関する「基礎体力」をつけることができます。ゲームデーでは、運用、セキュリティ、信頼性、パフォーマンス、コストの各分野をカバーする必要があります。専用の実験環境を使用して、運用手順と回復プロセスを検証して練習するために実世界のシナリオをシミュレートします。

ベストプラクティス 3.6 – オートメーションを使用して SAP 環境オペレーションを実行する

SAP 環境構築とランドスケープオペレーションのためのオートメーションパイプラインを作成します。Infrastructure as Code テクニック (例えば、CloudFormation、Launch Wizard for SAP) を使用するオートメーションを使用すると、繰り返し可能で俊敏な環境の作成または拡張が可能になります。

自動化されたパイプラインとランドスケープオペレーションは、マニュアルプロセスが原因のエラーを減らし、デプロイ変更の労力を減らして、ビジネスニーズに反応する速度を高めます。

自動化された方法で一般的な環境タスク (例えば、System Copy、Start SAP、Stop SAP、Scale SAP) を実行できる、自動化された SAP 環境運用パイプラインを作成します。時間ベースのシステムシャットダウンまたはユーザーロードによるオートスケーリングなど運用上のイベントに対応してこれらのパイプラインを呼び出します。

提案 3.6.1- Infrastructure as Code テクニックを実装して SAP 環境に再現可能でコード主導の構築パイプラインを作成する

AWS CloudFormation、AWS Cloud Development Kit または AWS Launch Wizard for SAP などのツールを使用して、繰り返し可能な、制御されたすばやい環境デプロイを作成します。

- SAP on AWS ブログ: Infrastructure as Code Example: Terraform and SAP on AWS (Infrastructure as Code の例: Terraform と SAP on AWS)
- AWS ドキュメント: AWS Launch Wizard for SAP

提案 3.6.2 - オートメーションで共通の SAP 環境オペレーションを実装する

オーケストレーションと Infrastructure as Code (IaC) のツールを組み合わせて使用して、一般的な SAP 環境オペレーションを自動化された方法で実行します。AWS CloudFormation、AWS Systems Manager – Run Automations、SAP Landscape Management (LaMa) および AWS Lambda などのツールは、デプロイパイプラインでの一般的な SAP 環境オペレーションを実行するようにオーケストレートできます。

ツール間の複雑なまたは深い統合が必要な サードパーティーオートメーションツールを検討します (例: Terraform、Ansible、Chef)。

自己修復とセルフメンテナンス環境が可能になるように、SAP ワークロードイベントへの応答に自動化されたオペレーションを使用することを検討します。

- SAP Note: 2574820 - SAP Landscape Management Cloud Manager for Amazon Web Services (AWS) (アマゾン ウェブ サービス (AWS) 向け SAP Landscape Management Cloud Manager) [SAP ポータルへのアクセス権が必要]
- AWS ドキュメント: AWS Launch Wizard for SAP
- AWS ドキュメント: AWS Systems Manager オートメーション
- AWS Marketplace: DevOps 向け製品とツール

4 – SAP ワークロードを定期的に検証し改善する

SAP ワークロードが継続して効率的に稼働することをどのように検証しますか? SAP ワークロードを定期的に改善し、AWS からの新しいサービスリリースを活用することを目標とします。SAP ワークロードを維持するためだけに時間とリソースを使います。SAP ワークロードの効率性を進歩させるために継続的な増分の改善を目指します。パフォーマンス、回復性またはコスト効率を向上させる是正措置により、パッチ適用、小規模な変更、以前に決定した設計の再評価を計画します。

ID	優先度	ベストプラクティス
□ BP 4.1	必須	SAP ワークロードのライフサイクルイベントを理解して計画する
□ BP 4.2	必須	パッチ管理を定期的に実行してソフトウェアを最新の状態に維持する
□ BP 4.3	強く推奨	事業継続性計画と障害復旧を定期的にテストする
□ BP 4.4	強く推奨	定期的なワークロードレビューを実行して、回復力、パフォーマンス、俊敏性、コストを最適化する

ベストプラクティス 4.1 – SAP ワークロードのライフサイクルイベントを理解して計画する

SAP ワークロードは、非常に大きく SAP に依存して、新しいソフトウェアと脆弱性のパッチ適用、オペレーティングシステムとデータベースのカーネル、サポートのためのエスカレーションを提供します。SAP は定期的に、リリースタイプ、メンテナンス期間、計画された可用性、 製品可用性マトリックス (PAM) と SAP Notes など、SAP ソフトウェアリリースに関する情報を公開しています。SAP アプリケーションのそれぞれの詳細を取得し、ローカルに追跡して、SAP ソフトウェアが最新か、サポートされているか、メンテナンスの観点からいつ耐用年数が終了するかを理解します

PAM は、サポートされているデータベースプラットフォームとオペレーティングシステムを含む、プラットフォームの可用性と互換性に関する情報も提供します。これにより、SAP ワークロードの基盤となるコンポーネントのパッチ適用とアップグレードをガイドします。オペレーティングシステムベンダーにも独自のパッチ適用とサポートライフサイクルがあり、アップグレードなどの SAP メンテナンスとライフサイクルイベントを計画するとき、考慮する必要があります。

提案 4.1.1 - 主なサポートとライフサイクルの日付を考慮して、SAP アプリケーションのオペレーションロードマップを作成する

すべての SAP ソフトウェア アプリケーション、カーネルバージョン、オペレーティングシステム、データベースバージョンを一元的に登録してリストし、サポートされているバージョンとメンテナンスウィンドウに関する PAM 情報と統合します。SAP を最新の状態に保ちサポートを受けられる状態を継続する必要があるすべてのコンポーネントで、このリストを統合ビューとして使用して、パッチ適用、アップグレードとプラットフォームの変更を計画します。

- SAP ドキュメント: SAP Release & Maintenance Strategy: Product Availability Matrix (SAP リリースとメンテナンス戦略: 製品可用性マトリックス) [SAP ポータルへのアクセス権が必要]

提案 4.1.2 - 認証情報、証明書およびライセンスの有効期限のカレンダーを管理する

前述のメジャーな SAP ライフサイクルイベントとパッチ適用とともに、マイナーシステムイベントを計画する運用カレンダーを用意します。これらのメンテナンスイベントの例としては、システム認証情報の期限切れ、証明書 (例えば、システム間での STRUST 統合用) の期限切れやライセンス更新作業または必要な更新 (例えば、移行、開発または POC 目的のための一時的な SAP またはデータベースライセンス) があります。

- AWS ドキュメント: AWS Certificate Manager

提案 4.1.3 - SAP ソフトウェアが寿命になる前にアップグレードまたは代替案を計画する

主要な SAP ライフサイクルイベントと運用維持 (パッチ適用、ソフトウェアアップグレード、移行と必要な場合のリプラットフォーム) を可視化する SAP 環境ロードマップを作成します。このライフサイクルカレンダーをビジネスおよび技術的なステークホルダーに連絡します。これらの SAP ライフサイクルアクティビティ/プロジェクトに資金を提供する投資を計画します。ビジネスステークホルダーとどこでメンテナンスウィンドウを実行するか、ダウンタイムや再起動が必要になるかを前もって計画します。

- SAP ドキュメント: SAP Roadmap Explorer

提案 4.1.4 - 最新の状態を保ち、主な SAP Notes に申し込んでサポートアドバイスを受ける

SAP ワークロードの主要な SAP Notes とナレッジベース記事 (KBA) にサブスクライブして、サポートの可能性やアドバイスの変更や更新が通知されるようにします。「お気に入り」の SAP Notes 機

能を使用して、SAP ワークロードの頻繁にアクセスする重要なメモのリストを維持し、簡単にアクセスして比較できるようにします。

- SAP サポートポータル - お気に入りの SAP Notes [SAP ポータルへのアクセス権が必要]

ベストプラクティス 4.2 – パッチ管理を定期的に実行してソフトウェアを最新の状態に維持する

定期的にパッチ管理を実行し、問題を解決して、ガバナンスに準拠するようにします。オペレーティングシステム、データベースおよび SAP アプリケーションレイヤーでのパッチを検討します。パッチ適用プロセスが、既存のサーバーにパッチを適用するのか、新しいサーバーをプロビジョンしてパッチを適用するのかを理解します。パッチ管理を自動化して、マニュアルプロセスによるエラーを減らし、パッチ適用の負担レベルを下げ、メジャー SAP、データベース、カーネルパッチ適用に必要なアプリケーションのダウンタイムを短縮します。

提案 4.2.1 - SAP パッチ管理手順を実装して、定期的に SAP Security Notes と新しくリリースされたパッチを確認する

オペレーティングシステム、データベースおよび SAP アプリケーションレイヤーでのパッチを検討します。

AWS ドキュメント: AWS セキュリティ速報

SAP ドキュメント: SAP EarlyWatch Alert

SAP ドキュメント: SAP セキュリティ関連のノートとニュース

オペレーティングシステム	Guidance
SUSE Linux Enterprise Server (SLES)	SUSE 更新アドバイザリ
Red Hat Enterprise Linux	Red Hat セキュリティアドバイザリ
Microsoft Windows	Microsoft セキュリティアラート
Oracle Enterprise Linux	Oracle セキュリティアラート

この項目の詳細については、次を参照してください。[セキュリティ]: ベストプラクティス 6.2 - オペレーティングシステムを構築し、保護する .

提案 4.2.2 - SAP 環境全体でパッチを調整し自動化するために、AWS Systems Manager や AWS OpsWorks などの自動化されたツールを検討する

- AWS ドキュメント: AWS Systems Manager Patch Manager
- AWS ドキュメント: AWS OpsWorks
- AWS ドキュメント: AWS OpsWorks とは?
- SAP Lens [セキュリティ]: ベストプラクティス 6.2 - オペレーティングシステムを構築し、保護する。

ベストプラクティス 4.3 – 事業継続性計画と障害復旧を定期的にテストする

SAP システムは、通常、ビジネスクリティカルで、主要なお客様向けトランザクションに依存します。IT オペレーションの迅速な再開を可能にし、障害または災害の状況でのデータ損失を最小限にすることは、運用上の優秀性に重要です。オペレーションチームとシステムが、何をいつなすべきかを知り、障害発生時には、ただちにワークロードサービスを再開できるようにするには、業務継続計画 (BCP) と障害復旧手順が必要です。

サービスを正常に再開するのに重要なことは、BCP 手順と障害復旧計画を定期的にテストし、システムとサポートチームの進化に合わせて改善し、洗練することです。本当の危機的状況ではないときに BCP と回復計画をテストすると、現実のシステム障害や災害が発生したとき、サービスを正常に再開し、目標復旧時間 (RTO) と 目標復旧時点 (RPO) に間に合わせる能力に自信を持つことができます。

提案 4.3.1. - BCP および障害回復テストカレンダーを作成する

SAP ワークロードの定期的な (少なくとも手動) BCP と障害復旧テストのスケジュールを設定するカレンダーを作成します。テクノロジー運用チーム、サポートスタッフとビジネスステークホルダーをテストに参加させて、手順が理解され、期待が一致するようにします。できる限りリアルな状況でテストすることを目標にします。

以下のシナリオをテストしてそれぞれの回復メトリクスを検証することを検討してください。

- SAP アプリケーションサービス障害

  (例えば、設定変更のために SAP アプリケーションサービスがスタートできない)
- シングルインスタンスホスト障害

  (例えば、SAP アプリケーションサーバー EC2 インスタンスに到達できなくなる)

- 単一ストレージボリューム障害

  (例えば、1 つの EBS ボリュームに到達できなくなる)
- ネットワーク障害と冗長接続への切り替え

  (例えば、オンプレミス Direct Connect 接続に到達できない)
- プライマリとセカンダリのクラスター化されたコンポーネント間での自動フェイルオーバー

  (例えば、SUSE HAE クラスターが、プライマリ HANA データベースを代替アベイラビリティーゾーンにあるセカンダリデータベースに移行させる)
- プライマリコンポーネントとセカンダリコンポーネント間でのマニュアルフェイルオーバー

  (例えば、Oracle DataGuard をマニュアルで呼び出すと、代替アベイラビリティーゾーンにあるセカンダリデータベースに切り換わる)
- 複数の冗長化されたコンポーネント間でのロードバランシング

  (例えば、プライマリウェブディスパッチャーがアベイラビリティーゾーンの高可用性ペアで失敗する)
- 代替 AWS リージョンでの SAP アプリケーションの回復 (必要な場合)
- ランサムウェアの被害を受けた場合にバックアップから回復する

  (例えば、Simple Storage Service (Amazon S3) WORM バックアップから SAP ERP システム全体を回復する)

提案 4.3.2 - ワークロード変更の一環として定期的に BCP と障害回復手順を見直す

時間の経過に伴い、ワークロードが進化し変化するとき、BCP と回復手順がこれらの変更で考慮されていることを確認します。コードまたはインフラストラクチャの変更が RTO または RPO に影響する可能性がある場合、ドキュメントと設定が更新されていること、および新しい BCP と回復プロセスが、リリースプロセスまたは定期的なテストカレンダーの一環としてテストされることを確認します。

- AWS ドキュメント: Business Continuity Plan (BCP) Definition (ビジネス継続性の計画 (BCP) の定義)
- AWS ドキュメント: Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス)
- SAP Lens [信頼性]: ベストプラクティス 11.4 – 定期的な回復力テストの実施

ベストプラクティス 4.4 – 定期的なワークロードレビューを実行して、回復力、パフォーマンス、俊敏性、コストを最適化する

SAP on AWS を実行するときは、継続的で段階的に改善するために専用の時間とリソースを計画して、ワークロードの効果と効率性を進歩させます。AWS は、SAP ワークロードを最適化できるように、定期的に新しいサービス、アプローチ、改善された SLA をリリースし、お客様が利用できる値下げを行っています。新しいサービスリリースが自分の SAP ワークロードに適切かどうかを理解して検証し、該当する場合は、本番稼働環境に実装してワークロードを進化させます。

提案 4.4.1 - SAP ワークロードの定期的なレビューを計画する

AWS チーム、AWS パートナー、または内部エキスパートと連携し、Well-Architected Framework SAP Lens (このドキュメント) を使用して、定期的に SAP ワークロードをレビューします。少なくとも毎年 1 回ワークロードのレビューを計画します。改善アクティビティを特定、検証、優先順位付けし、修正を発行してバックログに取り込みます。

提案 4.4.2 - Amazon EC2 インスタンスのサイジングとパフォーマンスを確認する

履歴 CloudWatch メトリクスを検証して、SAP ワークロードの CPU 使用量とメモリ使用率を確認します。低 CPU またはメモリ使用率について各 SAP コンポーネントを確認し、ワークロード要件への適合が向上するように EC2 インスタンスを適切にサイジングすることを検討します。パフォーマンスの適合とコストの最適化に、新しくリリースされた SAP 認定 EC2 インスタンスタイプを検討します。オペレーションバックログで新しい改善の利用を計画します。

参照先 コスト最適化 (SAP ワークロードで Amazon EC2 を使用する場合)。

- AWS ドキュメント: SAP 向け Amazon EC2 インスタンスタイプ

提案 4.4.3 - Amazon EBS サイジングとパフォーマンスを確認する

CloudWatch 履歴メトリクスからボリューム消費、スループットと IOPS 使用量を確認して、SAP ワークロード全体でのストレージ使用量を確認します。各 SAP コンポーネントにサイズ超過のストレージまたは 低スループット/IOPS 利用率がないか確認し、ワークロード要件への適合が改善されるように、Amazon EBS ストレージサイズとタイプを適切にサイジングすることを検討します。パフォーマンスの適合とコストの最適化に、新しくリリースされた SAP 認定 Amazon EBS タイプを検討します。オペレーションバックログで新しい改善の利用を計画します

- AWS ドキュメント: 適切なサイジング
- SAP Lens [コスト最適化]: ベストプラクティス 18.4 - 各ストレージオプションがコストに与える影響を必要な属性に基づいて評価する .

提案 4.4.4 - SAP ワークロードオペレーションの効率性を改善する新しいサービスを確認する

SAP ワークロードでのオペレーションを向上させられる新しいサポートサービスリリースを確認します。AWS Support 契約の一部としてテクニカルアカウントマネージャー (TAM) を割り当てられている場合は、TAM が新サービスと最適化の検討をお手伝いします。

共有ファイルストレージ、インターフェイスサービス (例えば、AWS Transfer、API Gateway)、セキュリティサービス (例えば、Amazon GuardDuty、AWS Firewall)、バックアップツール (例えば、AWS Backint)、オートメーションツール (例えば、Launch Wizard for SAP) などの新しいリリースを検討します。

オペレーションバックログで新しい改善の利用を計画します。

- AWS ドキュメント: 「最新情報」フィード
- AWS ドキュメント: Proactive Services from Support (サポートからのプロアクティブなサービス)

提案 4.4.5 - AWS ブログとお知らせで SAP をモニタリングする

SAP on AWS ブログフィードと AWS 「最新情報」フィードにサブスクライブして、新しくリリースされたサービスの発表、イノベーションアプローチや値下げの最新情報を得ることを検討します。

- SAP on AWS ブログフィード

提案 4.4.6 - 新しい、または改善された AWS のサービスを活用するために定期的な強化作業を計画する

運用予算が十分であり、予定されたサポートチームが、新しい AWS サービスとワークロードの進化の実装とテストに定期的に取り組めることを確認します。

セキュリティ

このセキュリティの柱では、データ、システム、資産を保護して、クラウドテクノロジーを活用してセキュリティを強化する能力について説明します。このレンズは、SAP のいくつかの中核的な原則とリソースをハイライトします。これらのプラクティスの多くは SAP に固有ではないため、エンタープライズの中核的な原則を考慮し、環境全体でのコントロールを確立することに重点を置くことをお勧めします。それらの セキュリティの柱 には、幅広い設計原則とレコメンデーションが含まれます。この後の SAP ガイダンスと併せて読むことを強く推奨します。

デプロイ戦略が、AWS ベース、オンプレミス、またはハイブリッドのいずれでも 、SAP セキュリティノートおよびニュースで推奨されるガイドラインに従い、SAP ワークロード特有の最新のセキュリティレコメンデーションを把握するようにします。

5 – セキュリティスタンダードとそれがどのように SAP ワークロードに適用されるかを理解する

SAP ワークロードの重要性と整合するセキュリティスタンダードとコントロールをどのように定義しますか? スタンダードは、製品、組織、業界、または法域のベストプラクティスに従って、システムをセキュリティで保護するために必要なポリシーと手順を定義する公開されたドキュメントです。SAP ワークロードを評価するためのフレームワークを提供します。一部のスタンダードは、規制要件のコンプライアンスを満たすために必須であり、その他は任意ですが、ロールと責任を確立する役に立ちます。

ID	優先度	ベストプラクティス
□ BP 5.1	必須	セキュリティロールと責任の定義
□ BP 5.2	強く推奨	SAP ワークロード内のデータを分類する
□ BP 5.3	強く推奨	アプリケーションとデータ分類に基づいて必要なセキュリティコントロールを決定します。
□ BP 5.4	強く推奨	セキュリティコントロールの実装戦略を作成する

ベストプラクティス 5.1 – セキュリティロールと責任を定義する

SAP ワークロードをセキュリティで保護するための要件を定義することで、対応が必要なリスクを特定でき、セキュリティ関連のロールと責任が適切に割り当てられていることを確認できます。この提案では、AWS、SAP、およびセキュリティ戦略を構築できるベースラインを形成するためのサービスプロバイダーについて説明します。

提案 5.1.1 - AWS 責任共有モデルを理解する

AWS はクラウドのセキュリティに責任があり、お客様は、クラウドでのセキュリティに責任があります。以下のリソースを確認して理解します。

- AWS ドキュメント: AWS 責任共有モデル

- AWS ドキュメント: AWS Response to Abuse and Compromise (不正使用と侵害に対する AWS の対応)
- AWS ドキュメント: AWS Acceptable Use Policy (AWS 適正利用規約)

AWS 責任共有モデルのコンテキストでお客様とお客様のパートナーとの間での責任の分担を理解します。

提案 5.1.2 - コンプライアンス証明書、レポート、証明を含む、SAP と AWS にまたがるセキュリティ基盤を理解する

SAP と AWS がサポートするセキュリティスタンダードとコンプライアンス認定を理解します。自分の業界や国にどれが関連するかを判断します (例えば、PCI-DSS、GDPR、HIPAA)。これらのコントロールは、コンプライアンスと認定プログラムを強化し、セキュリティスタンダードに適合するために必要な取り組みを削減します。

詳細については、以下の SAP および AWS ドキュメントを参照してください。

- AWS ドキュメント: AWS コンプライアンス
- AWS ドキュメント: AWS コンプライアンスセンター
- AWS ドキュメント: コンプライアンスプログラム
- AWS ドキュメント: コンプライアンスプログラムによる AWS 対象範囲内のサービス
- SAP ドキュメント: Trust Center

提案 5.1.3 - SAP ワークロードをサポートするサービスプロバイダーのセキュリティ基盤を評価する

サードパーティー組織に依存してすべてまたは一部の SAP ワークロードを管理している場合、必要なセキュリティコントロールに適合するサードパーティーの能力を評価します。これには、エンタープライズにより義務づけられるリーガルおよび規制要件が含まれます。

ベストプラクティス 5.2 – SAP ワークロード内のデータを分類する

データの機密性はリスクを軽減するために必要なコントロールに影響する可能性があります。AWS では、業界または組織内のスタンダードフレームワークを参照して採用し、SAP ワークロードとその中に含まれるデータを分類することをお勧めします。

提案 5.2.1 - データ分類と処理要件を決定する

組織に既に整備されているデータ分類フレームワークを特定します。これらのフレームワークは、機密性、整合性、可用性を保護する必要があるデータなど、情報の重要度に基づいてデータを分類する

のに役立ちます。スタンダード分類モデル、例えば US 情報分類スキーム が存在し、業種、ビジネスまたは IT 要件に基づいてカスタマイズできます。

分類に適切なガイドラインに従って、データを処理する方法を理解します。これには、スタンダードまたは規制要件 (例えば、PCI-DSS または GDPR) および一般的なプライバシーの考慮事項 (例えば、個人識別情報 (PII) の処理) に関連した具体的なセキュリティコントロールが含まれます。以下のドキュメントは次の追加情報を提供します。

- AWS ドキュメント: データ分類: 安全なクラウド導入ホワイトペーパー
- AWS ドキュメント: 一般データ保護規則 (GDPR) センター
- 情報システムと組織のための NIST セキュリティとプライバシーコントロール
- ISO 27001 – 付録 A.8: アセット管理
- Well-Architected Framework [セキュリティ]: データ保護

提案 5.2.2 - 特定の処理ルールで SAP のデータタイプを識別する

SAP システムにサポートされているビジネスプロセスに基づいて、データの処理とストレージに要件がある可能性があります。場所と業界向けのガイダンスを使用してよく理解します。SAP の例には以下が含まれる可能性があります。

- 保存されたカード所有者データを保護し、PCI コンプライアンスを確保するためにデジタル決済アドオンが必要かどうかを評価します。
- 例えば、一部の国や法域では、特定の地理的場所に保存することが要求されるなど、HR データのデータレジデンシー要件を評価します。
- 機密データが見えないようにしつつ、データの整合性を維持するために、非本番稼働環境システムでどのデータを暗号化する必要があるかを検討します。

提案 5.2.3 - 定義されたフレームワークに従ってすべてのワークロードを分類する

ビジネスの使用と重要なデータタイプの存在に従って、SAP システムを分類します。SAP ERP などのトランザクションシステムは、SAP BW などの分析的システムまたは Solution Manager などの管理システムより機密データを含む可能性が高いと考えられますが、機能およびセキュリティのエキスパートによる確認が必要です。

さらに、同じコントロールが非本番稼働環境ワークロードに適用されるかどうかを評価します。例えば、非本番稼働環境ワークロードには本番稼働データが含まれていて、同じセキュリティコントロールに従う必要はありますか?

ベストプラクティス 5.3 – SAP ワークロードの特定のセキュリティコントロールの必要性を評価する

データ分類に基づいて、以前のベストプラクティスで確立されたスタンダードと要件に適合するために役立つコントロールを評価します。これには、ロケーション、AWS アカウント戦略と非本番稼働用 SAP ワークロードのスクランブル要件が含まれます。

提案 5.3.1 - 地理的な場所要件を評価する

SAP ワークロードは、1 つまたは多数の AWS リージョンとアベイラビリティーゾーン (AZ) でデプロイされる可能性があります。各 AWS リージョンは、1 つの地理的領域内にある、複数の、隔離され、物理的にも分かれている AZ で成り立っています。レイテンシーと回復性についてリージョンを評価することに加え、セキュリティとコンプライアンス要件に適合できるかどうかを検討する必要があります。特定の運用管轄地域がある隔離されたリージョンの例には以下が含まれます。

- AWS GovCloud (US) - 機密データ、規制されたワークロードをホストし、最も厳格な米国政府のセキュリティとコンプライアンス要件に対応するように設計されています。
- 中国でのアマゾン ウェブ サービス - AWS は地元のパートナーと連携して、中国のリーガル要件と規制要件に適合するようにしています

一部の業界と国には、IT システムで処理および格納されるすべての顧客コンテンツは特定の国の国境内にとどまらなければならないというデータレジデンシー要件があります。

- AWSドキュメント: Addressing Data Residency with AWS (AWS によるデータレジデンシーへの対応)

場所に関する決定を下す前に、その AWS リージョンのサービスの可用性をレビューして、必要なサービスが使用できることを確認してください。

- AWSドキュメント: リージョン別のサービス

提案 5.3.2 - SAP ワークロードに対して必要な AWS アカウント戦略を決定する

AWS で SAP ワークロードを運用するときの重要な考慮事項は、組織のセキュリティ管理に応じて採用する AWS アカウント戦略です。SAP を SAP 以外のワークロードから切り離し、生産を生産以外のものとは別のアカウントで行うことを考慮する必要があります。

AWS 組織と AWS Control Tower の使用も含め、組織の既存の AWS アカウント管理戦略を理解します。セキュリティ機能とログ機能を別々のアカウントに分離することを検討します。詳細については、以下を参照してください。

- Well-Architected Framework [セキュリティ]: AWS アカウントの管理と分離
- AWSドキュメント: ベストプラクティスの AWS 環境を確立する
- AWSドキュメント: Organizing Your AWS Environment Using Multiple Accounts (複数のアカウントを使用した AWS 環境の組織化)

採用するアカウント戦略は、AWS 内のネットワーク構成にも影響を与えます。SAP ワークロードに応じた適切な AWS アカウント戦略を決定する一環として、以下のことを考慮する必要があります。

- 非生産システムと生産システム間の通信を可能にするための、VPC ピアリング または Transit Gateway のセットアップの必要性などのクロスアカウントアクセスの要件。例えば、環境内の SAP トランスポートの移動。
- SAP ワークロードから異なる AWS アカウントでデプロイされる共有サービス (ディレクトリ管理リソースなど) とネットワーク管理コンポーネントに対する依存性。

提案 5.3.3 - データスクランブリングのコントロールをレビューする (該当する場合)

SAP のお客様の多くは、回帰テストや性能テストも含め、テスト目的で製品データのコピーに依存しています。生産データのコピーを作成する場合は、生産データを意図しないアクセスや改変から保護するために追加しなければならないコントロールを決定してください。

以下のオプションを考慮してください。

- SAP またはサードパーティープロバイダーから提供される従来のデータスクランブリングメカニズム
- 生産データのコピー時にアクセスを制限するための追加のアカウントまたはネットワークコントロールの使用
- 生産用と同じコントロールでの非生産アカウントの使用

ベストプラクティス 5.4 – セキュリティコントロールの実装戦略を作成する

データ分類に基づくビジネス要件を評価した後、より幅広い組織のセキュリティコントロールと、入手可能なアプリケーションガイドおよびオープン標準のバランスを取る戦略を作成します。実装の労力を考慮に入れ、リスクを確認します。

提案 5.4.1 - リスクを評価するためのマトリックスを特定する

特定の業界や地域向けのさまざまなリスク管理フレームワークがあります。組織によって採用されたリスクフレームワークと、これを SAP ワークロードに関連するリスクの管理に適用する方法を理解します。

- AWSドキュメント: リスクマトリックスの例
- AWSドキュメント: Scaling a governance, risk, and compliance program for the cloud (ガバナンス、リスク、およびコンプライアンスプログラムのクラウド向けのスケーリング)
- NIST リスクマネジメントフレームワーク

提案 5.4.2 - 組織によって義務づけられているセキュリティおよびコンプライアンス要件を評価する

クラウドセンターオブエクセレンス、リーガルチーム、コンプライアンスチーム、およびマネージドサービスプロバイダーに相談して、セキュリティベースラインとコントロールの実施方法を理解します。これらのコントロールのすべてを SAP ワークロードに容易に適用できるかどうか、また、例えば、AWS サービスの許可リストと拒否リスト、インバウンドおよびアウトバウンドトラフィックフローとアクセス制限など、例外を必要とする分野を特定できるかどうかを評価します。

提案 5.4.3 - 例外プロセスを特定し、合意する

状況によっては、SAP 用のソフトウェア、ビジネス、またはサポート要件により、標準的なセキュリティパターンからの逸脱が必要になることがあります。例外について変更諮問委員会またはセキュリティ設計機関との合意と文書化が必要なプロセスを特定し、プロセスを定期的に再評価します。

AWSドキュメント: Change Management in the Cloud (クラウドにおける変更管理)

6 – インフラストラクチャおよびソフトウェアコントロールを使用して、セキュリティの構成ミスを軽減する

SAP アプリケーションと基盤となるデータベース、オペレーティングシステム、ストレージ、およびネットワークをどのように保護しますか? SAP ソフトウェアと、オペレーティングシステムおよびデータベースのパッチ、パラメータ、クラウドサービス、およびインフラストラクチャなど、関連する基盤構成を強化することをお勧めします。強化は、組織によって決定された適切なレベルでの、生産と非生産の両方を含むあらゆる SAP 環境の安全性の確保に役立ちます。

コミットメント割引を適用する機会を見つけるために、 AWS 責任共有モデル SAP 環境のセキュリティに関するアクティビティをガイドします。例えば、EC2 インスタンスのファームウェアアップデートは、AWS が責任を持つ「クラウドのセキュリティ」アクティビティですが、同じ EC2 イン

スタンスでも、オペレーティングシステムとアプリケーションの管理は、お客様が責任を持つ「クラウドでのセキュリティ」アクティビティです。

ID	優先度	ベストプラクティス
□ BP 6.1	必須	セキュリティと監査が SAP ネットワーク設計に組み込まれていることを確認する
□ BP 6.2	必須	オペレーティングシステムを構築し、保護する
□ BP 6.3	必須	データベースとアプリケーションを保護する
□ BP 6.4	必須	該当するすべてのソフトウェアのアップグレードとパッチ適用のプランを確立する

詳細については、次の情報を参照してください。

- AWSドキュメント: AWS のセキュリティホワイトペーパー
- SAP Note: 2191528 - Third-party report showing security vulnerabilities (セキュリティの脆弱性を示すサードパーティーレポート) [SAP ポータルへのアクセス権が必要]
- SAP ドキュメント: ABAP Platform Security Guide

ベストプラクティス 6.1 – セキュリティと監査が SAP ネットワーク設計に組み込まれていることを確認する

SAP ワークロードをホストするネットワークへのアクセスを保護することは、悪意あるアクティビティに対する防御の最前線です。ビジネス要件と特定の SAP ソリューションを評価して、有効にする必要があるポート、プロトコル、およびトラフィックパターンを決定します。組織のセキュリティスタンダードと、ネットワーク設計を単純化するために使用できるツールおよびパターンを検討します。定期的に、または変更が発生するたびに監査します。

提案 6.1.1 – SAP のネットワークトラフィックフローを理解する

まず、トラフィックフローを理解します。SAP ワークロードのネットワークトラフィックパターンは、インバウンドトラフィック、アウトバウンドトラフィック、および内部トラフィックに分類できます。ソースとデスティネーションが信頼できるネットワーク境界内にあるかどうかを特定して、ルールセットの定義を支援する必要があります。

ユーザーアクセスやインターフェイス接続など、既知のインバウンドトラフィックフローとアウトバウンドトラフィックフローに加えて、SAP サポートへの接続 (SAProuter 経由) や、ソース IP アドレスに基づいてアクセスを制限する SAP SaaS サービスなど、SAP 固有の要件を考慮します。

内部トラフィックについては、コンポーネントおよびシステム間のトラフィックの他、AWS と共有サービス間のトラフィックを考慮します。次のようなツール VPC フローログ と VPC Reachability Analyzer は、Amazon VPC へのトラフィックフローと Amazon VPC からのトラフィックフローの理解に役立ちます。

詳細については、次の情報を参照してください。

- SAP ドキュメント: TCP/IP Ports for All SAP Products

提案 6.1.2 – トラフィックフローの許可と拒否のオプションを評価する

まず、SAP システムが運用されている AWS アカウントにオンプレミスネットワーク内のユーザーとシステムをどのように接続するかを理解します。これについては、 「ネットワークから Amazon VPC への接続オプション」で説明されています .

VPC へのネットワークトラフィックと VPC からのネットワークトラフィックのフローを制御するための 2 つの主な方法として、 セキュリティグループ と ネットワークアクセスコントロールリスト (ネットワーク ACL) の使用があります。セキュリティグループは、EC2 インスタンスレベルで仮想ファイアウォールの役目を果たし、インバウンドおよびアウトバウンドトラフィックを制御し、ステートフルです。ネットワーク ACL は、VPC のセキュリティのためのオプションのレイヤーであり、1 つ以上のサブネットとの間のトラフィックを制御するファイアウォールの役目を果たし、セキュリティグループとは違ってネットワーク ACL はステートレスです。

VPC の外側のネットワークコンポーネントの依存性も考慮してください。これには、Amazon CloudWatch エンドポイントなど、AWS によって提供される外部ネットワークコンポーネントが含まれることがあります。また、オペレーティングシステムのパッチ用のソフトウェアリポジトリなど、インターネットでホストされるサービスも含まれることがあります。

AWS の標準オプションに加えて、SAP 自体も追加のネットワークセキュリティオプションを提供しており、 SAProuter AWS ニュースブログ、 SAP Web Dispatcher 、および SAP ゲートウェイ ネットワークベースのアクセスコントロールリストの使用などがあります .これらは AWS のサービスおよび構成と連携して、SAP システムへのネットワークアクセスを許可または制限します。

詳細については、次の情報を参照してください。

- SAP on AWS ブログ: VPC Subnet Zoning Patterns for SAP on AWS (SAP on AWSAWS の VPC サブネットゾーニングパターン)
- Well-Architected Framework [セキュリティ]: インフラストラクチャ保護 – ネットワークの保護
- Well-Architected Framework [マネジメントとガバナンスレンズ]: ネットワーク接続
- SAP ドキュメント: Network and Communication Security (ネットワークと通信セキュリティ)

提案 6.1.3 – 設計ガイドラインと AWS ツーリングを使用して、ネットワークセキュリティを簡素化する

SAP システムは、多くの場合、複雑な統合要件を持ち、クラウドはネットワークセキュリティ管理を簡素化するための追加の手段となります。以下のアプローチを検討してください。

- 管理の簡素化が可能な場合、個々の IP アドレスまたは IP の範囲の参照は避けます。
- すべての SAP ワークロードについて SAP システム番号の標準セットを使用して、必要なネットワークポートの範囲を減らします。
- VPC エンドポイント は、Amazon S3 や Amazon CloudWatch などの AWS サービスにアクセスするための VPC からのアウトバウンドインターネットアクセスの要件をなくします。可能な場合や、ビジネス要件によって必要とされない場合は、これらのサービスとの間の SAP トラフィックがパブリックインターネットを経由せず、すべてのトラフィックが AWS によって管理されているネットワークコンポーネントを経由するようにできます。
- 以下を使用することによって、セキュリティグループを簡素化します。 VPC プレフィックスリスト や セキュリティグループのルール 。これらは、IP アドレスの範囲ではなく、他のセキュリティグループを参照します。
- セキュリティグループの作成、更新、および管理にオートメーションを使用して、構成のズレを避けます。
- 以下の使用を検討します。 AWS Firewall Manager これは VPC と AWS アカウント全体でのセキュリティグループの集中管理のためです。
- 以下の使用を検討します。 SAProuter 、 SAP Web Dispatcher 、および Elastic Load Balancing。これらを組み合わせることで、バックエンドシステムへのエントリポイントを難読化できます。
- 複数の SAP Internet Communication Manager (ICM) エントリポイントを使用して、よりきめ細かなアクセスコントロールを提供することを検討します。

詳細については、次の情報を参照してください。

- SAP ドキュメント: ネットワークベースのアクセスコントロールリスト

- SAP ドキュメント: TCP/IP Ports for All SAP Products

ベストプラクティス 6.2 – オペレーティングシステムを構築し、保護する

SAP ソフトウェアの基盤となるオペレーティングシステムを保護することで、悪意ある人物が SAP アプリケーション内のデータへの不正なアクセス権を得て、ソフトウェアの可用性に影響を与えたり、ミッションクリティカルな実装を不安定化させたりする可能性を軽減できます。SAP、オペレーティングシステムベンダー、データベースベンダー、または AWS からのレコメンデーションに従って、オペレーティングシステムの安全を確保してください。選択した SAP ソリューションとオペレーティングシステムによっては、サービスの有効化/無効化、特定のカーネルパラメータの設定、およびさまざまな組み合わせのセキュリティパッチの適用が必要になる場合があります。SAP の要件が組織の要件にどのように対応するかを考慮し、矛盾点があれば特定します。

提案 6.2.1 – セキュアなオペレーティングシステムをプロビジョニングするためのアプローチを決定する

Amazon マシンイメージ (AMI) は、EC2 インスタンスを起動するために必要な情報を提供します。AMI がオペレーティングシステムレベルでセキュアであることを確認する必要があります。そうでない場合、AMI が時間の経過とともに再利用され、更新されるたびに、セキュリティホールが任意の数のインスタンスに伝播する恐れがあります。

AMI は、オペレーティングシステムベンダーからの標準イメージか、お客様自身が構築したカスタムイメージのいずれかです。どちらの場合も、一貫したアプローチにより、オペレーティングシステムが起動時にセキュアであり、継続的に維持されることを確実にする必要があります。Infrastructure as Code (IaC) ツール、例えば、 AWS CloudFormation などの使用は、イメージセキュリティの一貫性の達成に役立ちます。HANA ベースの SAP ソリューションの場合、 AWS Launch Wizard for SAP は、セキュリティコンポーネントのインストールを自動化するためにカスタマイズできるプレおよびポストインストールスクリプトなど、インストールプロセスを簡素化します。

詳細については、コンピューティングリソースの保護、特に脆弱性管理の実行と攻撃面の削減に関する「AWS Well-Architected Framework [セキュリティの柱]」ガイダンスを参照してください。

- Well-Architected Framework [セキュリティ]: コンピューティングの保護

提案 6.2.2 – セキュアなオペレーティングシステムを維持するためのアプローチを決定する

コンピューティングの保護に関する Well-Architected Framework [セキュリティの柱] の説明で述べたように、選択したオペレーティングシステムが EC2 Image Builder によってサポートされている場合は、SAP 固有の AMI の構築、テスト、デプロイと継続的なパッチ管理を簡素化できます。セ

キュリティパッチ適用の自動化によるオペレーティングシステムのセキュリティ体制の維持については、AWS Systems Manager Patch Manager も調べてください。

- Well-Architected Framework [セキュリティ]: コンピューティングの保護
- AWSドキュメント: EC2 Image Builder
- AWSドキュメント: AWS Systems Manager Patch Manager

提案 6.2.3 – オペレーティングシステムに適用できる追加のセキュリティレコメンデーションをレビューする

SAP ソフトウェアの基盤となるオペレーティングシステムの強化に必要な項目の完全なリストを作成します。例えば、Linux ベースのシステムでのファイルシステム許可は SAP ガイドラインに従って設定する必要がありますが、Windows ベースのシステムでは、Administrator グループのアクセスを制限するのがベストプラクティスです。

以下の SAP 固有のレコメンデーションは、お客様の環境に該当する可能性があります。

- SAP ドキュメント: SAP NetWeaver セキュリティガイド - オペレーティングシステムのセキュリティ

オペレーティングシステム	Guidance
サポートされるすべての UNIX/Linux オペレーティングシステム	• SAP ドキュメント: UNIX/LINUX での SAP システムのセキュリティ
SUSE Linux Enterprise Server (SLES)	• SAP Note: 2684254 - SAP HANA DB: Recommended OS settings for SLES 15 / SLES for SAP Applications 15 (SAP HANA DB: SLES 15 / SLES for SAP Applications 15 で推奨される OS 設定) [SAP ポータルへのアクセス権が必要] • SAP Note: 2578899 - SUSE Linux Enterprise Server 15: Installation Note (SUSE Linux Enterprise Server 15: インストールに関する注意) [SAP ポータルへのアクセス権が必要] • オペレーティングシステム固有のドキュメント: SUSE 強化ガイド

オペレーティングシステム	Guidance
Red Hat Enterprise Linux	• SAP Note: 2777782 - SAP HANA DB: Recommended OS Settings for RHEL 8 (SAP HANA DB: RHEL 8 で推奨される OS 設定) [SAP ポータルへのアクセス権が必要] • SAP Note: 2772999 - Red Hat Enterprise Linux 8.x: Installation and Configuration (Red Hat Enterprise Linux 8.x: インストールと構成) (SELinux サポートについての特定の説明あり) [SAP ポータルへのアクセス権が必要]
Microsoft Windows	• SAP ドキュメント: SAP System Security on Windows (Windows での SAP システムのセキュリティ) • SAP Note: 1837765 - Security policies for <SID>adm and SAPService<SID> on Windows (Windows での adm および SAPService のセキュリティポリシー) [SAP ポータルへのアクセス権が必要]
Oracle Enterprise Linux	• (ガイダンスについては SAP またはベンダーのドキュメントを参照)

提案 6.2.4 – オペレーティングシステムのセキュリティ体制を検証する

オペレーティングシステムがセキュアにデプロイされ、パッチが適用されたら、オペレーティングシステムのセキュリティ体制を検証して、オペレーティングシステムが高いレベルのセキュリティを継続的に維持して、違反行為がないことを確認します。サードパーティーのホスト侵入保護、侵入検知、アンチウイルス、およびオペレーティングシステムファイアウォールソフトウェアを使用して、この検証を自動化することを検討します。

詳細については、次の情報を参照してください。

- Well-Architected Framework [セキュリティ]: セキュアなオペレーション
- Well-Architected Framework [セキュリティ]: 検出
- Well-Architected Framework [セキュリティ]: コンピューティングの保護

ベストプラクティス 6.3 – データベースとアプリケーションを保護する

悪意ある人物が読み取り専用レベルでもアクセス権を取得すると、重要なビジネスデータのセキュリティが侵害されるため、データベースおよびアプリケーションレイヤーでのセキュリティ警戒が不可欠です。どのような場合でも、データベースのアクセス保護とアプリケーションのセキュリティに関する標準的な SAP ベストプラクティスに従ってください。これらは、オンプレミスとクラウドベースの両方のインストールに適用され、SAP システムの基盤となるサポートされる各データベースについてのガイドラインです。

提案 6.3.1 選択したデータベースについて、データベースセキュリティに関する SAP ガイダンスに従う

該当するガイドラインについては、以下を参照してください。

データベース	ドキュメント
SAP HANA	• AWSドキュメント: AWS SAP HANA セキュリティ • SAP ドキュメント: SAP HANA セキュリティガイド • SAP ドキュメント: SAP HANA 管理ガイド • SAP Note: 2159014 - FAQ: SAP HANA Security (FAQ: SAP HANA セキュリティ) [SAP ポータルへのアクセス権が必要]
SAP ASE	SAP ドキュメント: SAP ASE でのセキュリティ管理
IBM Db2	(ガイダンスについては SAP またはベンダーのドキュメントを参照)
Oracle	SAP ドキュメント: SAP データベースガイド - Oracle
Microsoft SQL Server	SAP Note: 3019299 - Security Audit Questions or Security Customization in NetWeaver and SQL Server systems (NetWeaver および SQL Server システムにおけるセキュリティ監査に関する質問またはセキュリティカスタマイズ) [SAP ポータルへのアクセス権が必要]
SAP MaxDB	SAP ドキュメント: SAP MaxDB Security Guide

提案 6.3.2 – アプリケーションのセキュリティに関する SAP ガイダンスに従う

SAP NetWeaver ベースのソリューションについては、『SAP NetWeaver セキュリティガイド』に詳しいガイダンスがあります。

- SAP ドキュメント: ABAP Platform Security Guide

ベストプラクティス 6.4 – 適用可能なすべてのソフトウェアのアップグレードとパッチ適用のプランを確立する

SAP と基盤となるオペレーティングシステムおよびデータベースのベンダーは、一定のスケジュールで標準的なセキュリティアップデートをリリースし、脆弱性を修正するための緊急アップデートも提供します。各ベンダーからの最新のセキュリティ情報を確認してください。セキュリティホールの導入を回避するには、定期的に最新のセキュリティフィックスで SAP アプリケーションと基盤となるすべてのコンポーネントを最新の状態に保つことをお勧めします。また、重要なセキュリティパッチがリリースされたときに緊急フィックスを適用するためのプランを立てておくことをお勧めします。

提案 6.4.1 - オペレーティングシステム、データベース、およびソフトウェアソリューションのベンダーからのアラートを購読する

さまざまなベンダーポータルのセキュリティアップデートを購読することで、新しいセキュリティ問題や修正をリリースされたタイミングで知ることができます。これは、必要な変更を計画するのに役立ちます。

- AWS ドキュメント: AWS セキュリティ速報
- SAP ドキュメント: SAP EarlyWatch Alert
- SAP ドキュメント: SAP セキュリティ関連のノートとニュース

オペレーティングシステム	Guidance
SUSE Linux Enterprise Server (SLES)	SUSE 更新アドバイザリ
Red Hat Enterprise Linux	Red Hat セキュリティアドバイザリ
Microsoft Windows	Microsoft セキュリティアラート
Oracle Enterprise Linux	Oracle セキュリティアラート

提案 6.4.2 – 推奨された変更と、ビジネスおよび実装の取り組みに対するリスクをレビューする

SAP チームは、システムアップタイムに対するニーズと、SAP セキュリティの向上のために推奨されたシステム変更の重要性とのバランスを取ることを学ぶ必要があります。これを怠ると、サービスの中断、財政上の影響、生産性の喪失など、不必要なリスクが生じる恐れがあります。脆弱性を修正するためにベンダーから推奨された変更と実装ステップをレビューし、それらをすみやかに実装するプランを立てます。これは、このレンズで述べられている運用上の優秀性のベストプラクティス、特にセキュリティに関するランブックの作成に直接関係します。

- SAP Lens [運用上の優秀性]: 提案 3.4.1 - SAP セキュリティオペレーションのための具体的なランブックを作成する

提案 6.4.3 – 脆弱性に迅速に対応するプランを確立する

新しい SAP セキュリティレコメンデーションとセキュリティ関連のパッチを可能な限り迅速に適用することが、AWS ベースの SAP ソリューションにとっても、別の場所にインストールされているソリューションにとっても非常に重要です。新しいサービスと機能の SAP セキュリティノートおよびニュース を定期的にレビューして、記載されているパッチ、ノート、およびレコメンデーションにより、セキュリティ問題を迅速に修正します。場合によっては、SAP 管理者は根本的な脆弱性が解決されるまで、一時的な緩和措置または管理措置を講じなければならないこともあります。インシデント対応に関するセキュリティの柱のレコメンデーションにも従ってください。

- Well-Architected Framework [セキュリティ]: インシデント対応
- SAP ドキュメント: SAP セキュリティノートおよびニュース

7 – ID および許可による SAP ワークロードへのアクセスの制御

SAP ワークロードへのアクセスをどのように制御しますか? AWS、SAP、およびその他のサードパーティーによって提供されるメカニズムを使用して、エンドユーザーとインターフェイスシステムが正しく識別され、認証されるようにします。最小特権を確保するために、許可はどのように管理されますか? アクセスはどのように監査され、報告されますか? まず、ユーザーのカテゴリを識別してから、コントロールおよび ID 管理アプローチを通じて組織的に作業して、SAP ワークロードへのアクセスを制限します。

ID	優先度	ベストプラクティス
□ BP 7.1	必須	SAP ユーザーカテゴリとアクセスメカニズムを理解する
□ BP 7.2	必須	SAP ワークロードの特権アクセスを管理する

ID	優先度	ベストプラクティス
□ BP 7.3	必須	組織の ID 管理アプローチと SAP への適用を理解する
□ BP 7.4	強く推奨	ユーザーアクセスと認可の変更およびイベントについてロギングとレポートを実装する

ベストプラクティス 7.1 – SAP のユーザーカテゴリとアクセスメカニズムを理解する

SAP システムにアクセスするユーザーのタイプによって、適用する必要があるセキュリティコントロールが決まります。各ユースケースを調べることで、戦略を開発できます。これには、ID、認証、ツーリング、およびそれらの要件をサポートするメカニズムの管理方法を含める必要があります。

提案 7.1.1 データアクセス許可と許可されるアクションを理解する

SAP システムには、多くの場合、機密性の高いビジネスデータが含まれます。ユーザータイプを定義して、データアクセス許可を理解します(例えば、管理データベースユーザーにはアプリケーションユーザーのきめ細かなコントロールがないため、より重要かもしれません)。 [セキュリティ] も参照してください。 ベストプラクティス 5.2 – SAP ワークロード内のデータを分類する.

SAP システムのアクセスに関して、以下の質問を考慮します。

- 管理ユーザーまたはサービスユーザーが取るアクションは、一意に識別可能な個人まで追跡可能な必要がありますか?
- アクセス権が付与されるのは、アプリケーションのどのレイヤーですか?
- 許可によって機能のサブセットへのアクセスを制限できますか?
- その他のコントロール、例えば、特定のサービスのみを公開することによって、機能のサブセットへのアクセスを制限できますか?
- 取られたアクションを監査するための要件はありますか?

提案 7.1.2 – ユーザーが SAP システムにアクセスするネットワークや場所を理解する

ネットワークや場所は、セキュリティリスクプロファイルの一因となることが多く、信頼できるユーザーとみなされるかどうかを決めることがあります。一般に、これは無許可アクセスを防止するためのコントロールと組み合わされます (以下を参照 ベストプラクティス 6.1 – セキュリティと監査が SAP ネットワーク設計に組み込まれていることを確認する) を指定する必要があります。

超えは設計に影響を与えることがあります。例えば、信頼できないインターネットユーザーまたはデバイスが SAP ワークロードにアクセスするには、社内ネットワークからの信頼できるユーザーに比べて、追加の認証要素を必要とすることがあります。

ベストプラクティス 7.2 – SAP ワークロードへの特権アクセスを管理する

可能な場合は、最小特権のアプローチを採用します。ユーザビリティと効率性を管理しつつ、最小限のユーザーセットに、特定のロールを遂行するために必要な最小アクセスのみを付与します。管理アカウント (例えば、 <sid>adm) は、SAP ワークロードの信頼性やデータのセキュリティに大きな影響を与えるアクセス権をデフォルトで持ちます。このリスクをどのように制限できるか検討してください。

提案 7.2.1 – AWS 認証情報と認証を管理する

AWS Identity and Access Management (IAM) により、AWS のサービスとリソースへのアクセスを安全に管理できます。IAM を使用すると、さまざまな SAP およびクラウド管理タスクについて AWS ユーザーとグループを作成し、管理できます。IAM 許可を使用して、AWS リソースへのユーザーアクセスを許可および拒否します。特に特権 (ルート) アクセスの制限と保護については、標準ガイダンスに従う必要があります。

- AWS ドキュメント: IAM でのセキュリティのベストプラクティス

ユーザーに割り当てられていないが、SAP アプリケーションのオペレーションに必要なアクセスについては、最小特権の確保に特に注意を払います。

- AWS ドキュメント: IAM ロールを使用して Amazon EC2 インスタンスでのアプリケーション実行権限を付与する

提案 7.2.2 – SAP 管理認証情報と認証を管理する

必要なときだけ、期間限定の昇格された許可を承認および付与するプロセスを実装します。誰にどのような理由でアクセスが付与されたかに対処する監査機能を使用します。

特権アカウントのユーザーネーム/パスワードの使用を制限します。可能な場合は、直接アクセスを無効にします。特権アクセス管理ソリューションやパスワードボールトなど、認証情報を安全に保存します。

ランブック、RunCommand、および Secrets Manager を使用する特定のタスクについて、オペレーティングシステムへの直接アクセスを制限するために、システムマネージャーをどのように使用できるか評価します。

- AWS ドキュメント: SSM Agent を介してルートレベルコマンドへのアクセスを制限する
- AWS ドキュメント: AWS Secrets Manager パラメータからの Parameter Store シークレットの参照

ベストプラクティス 7.3 – 組織の ID 管理アプローチと SAP への適用を理解する

一般的な SAP ワークロードは複数のシステムで、したがって複数の ID で構成されます。これらのユーザーを管理するための集中アプローチにより、セキュリティリスクとオペレーションの複雑性を軽減できます。焦点は、集中的なユーザー管理、シングルサインオン、および多要素認証を考慮して、AWS サービスとサードパーティーツールをアプローチでどのように使用できるかです。

提案 7.3.1 – 指名ユーザーの ID プロバイダーを決める

ユーザーはアクティブディレクトリなどの ID ストアに関連付けられます。これは、ロール、許可、ID などのアイデンティティ情報を管理するための中央リポジトリとして機能します。ID の各セットについて、これを ID プロバイダーに関連付けることができるかどうか判断します。ID プロバイダーによって、ユーザー認証の負担を軽減できます。シングルサインオン (SSO) を容易にし、ユーザー ID のライフサイクル (新規加入者、移動者、退去者など) も管理します。

人間に関連付けられない名前付きユーザーの例外を考慮します。これには、バッチ、ジョブスケジューリング、統合、およびモニタリングユーザーなどが含まれます。

- AWS ドキュメント: AWS ディレクトリサービス | Amazon Web Services (AWS)

提案 7.3.2 – 認証メカニズムを決める

SAP ワークロードの各レイヤーでサポートされる認証メカニズム (SAML、Kerberos、X.509、SAP シングルサインオンチケットなど) を理解します。アプリケーションと統合するための要件を評価します。可能な場合は、シングルサインオンを使用して、複数のユーザー認証情報を管理する管理上およびセキュリティ上の影響を回避します。

- SAP ドキュメント: User Authentication and single sign-on (ユーザー認証とシングルサインオン)
- AWS ドキュメント: クラウドアプリケーション - AWS シングルサインオン
- SAP on AWS ブログ: AWS SSO による SAP シングルサインオンの有効化 パート 1: SAP Netweaver ABAP と AWS SSO の統合
- SAP on AWS ブログ: AWS SSO による SAP シングルサインオンの有効化 パート 2: SAP Netweaver Java と AWS SSO の統合

- SAP on AWS ブログ: Enable Single Sign On for SAP Cloud Platform Foundry and SAP Cloud Platform Neo with AWS SSO (AWS SSO で SAP Cloud Platform Foundry と SAP Cloud Platform Neo のシングルサインオンを有効にする)

提案 7.3.3 – 多要素認証を検討する

多要素認証 (MFA) は、ログオン認証情報に加えて保護を強化するベストプラクティスです。これら複数の要素により、SAP アプリケーションのセキュリティが強化されます。ユースケースとしては、信頼できないデバイスから SAP へのアクセス、AWS 管理コンソールへのアクセス、バックアップの削除や EC2 インスタンスの終了などの特権アクティビティがあります。

- SAP on AWS ブログ: Securing SAP Fiori with MFA (MFA による SAP Fiori の保護)
- AWS ドキュメント: IAM のサインインページでの MFA デバイスの使用 - AWS ID とアクセス
- AWS ドキュメント: MFA 削除の設定 - Amazon Simple Storage Service
- AWS ドキュメント: Amazon EC2: 特定の EC2 オペレーション (GetSessionToken) に対して MFA を要求する

提案 7.3.4 – 証明書管理のアプローチを決める

クライアントベースの証明書は認証に使用でき、認証情報が不要です。システム間通信のセッション管理と証明書ローテーションのための時間ベースの有効期限切れを含むアプローチを決めます。AWS は SAP によって信頼される認証局を提供します。証明書は、次を使用して発行、管理できます。 AWS Certificate Manager (ACM) .

- SAP Note: 2801396 - SAP Global Trust List (SAP グローバル信頼リスト) [SAP ポータルへのアクセス権が必要]
- SAP Note: 3040959 - How to get a CA signed server certificate in ABAP (ABAP で CA 署名付きサーバー証明書を取得する方法) [SAP ポータルへのアクセス権が必要]
- SAP Lens [運用上の優秀性]: 提案 3.4.1 - SAP セキュリティオペレーションのための具体的なランブックを作成する
- SAP Lens [運用上の優秀性]: 提案 4.1.2 - 認証情報、証明書およびライセンスの有効期限のカレンダーを管理する

ベストプラクティス 7.4 – ユーザーアクセスと認可の変更およびイベントについてロギングとレポートを実装する

SAP システムのユーザーアクセスと認可イベントをログに記録し、分析し、定期的に監査する必要があります。SAP アプリケーションおよびデータベースのセキュリティイベントをアーキテクチャの他のコンポーネントと統合し、照合します。これにより、重大なセキュリティ問題や違反が発生した場合に、エンドツーエンドな追跡が可能です。中央のセキュリティ情報およびイベント管理 (SIEM) システムでイベントの分析を自動化します。これにより、オペレーションチームは、予定外または疑わしいアクティビティが通常のシステムコントロールの外部で発生したかどうか理解できます。その後、必要に応じて修正することができます。

提案 7.4.1 – AWS Identity and Access Management (IAM) イベントを口グに記録する

AWS IAM イベントの履歴口グの保持を検討します。これは AWS アカウント内のユーザーや認可の変更を検出または監査するのに使用できます。口グの保持期間と口グに記録するイベントのタイプを、組織によって必要とされるセキュリティポリシーに基づいて決定します。

オペレーションチームが SAP システムのインフラストラクチャレベルで監査の質問に答えられるようにします。

- 新しい AWS コンソール/CLI ユーザーは、いつ、誰によって作成されましたか?
- AWS IAM ロールは、いつ、誰によって変更されましたか?
- AWS ユーザーが最後に正常にサインインしたのはいつですか?
- AWS アカウントへのサインインの試みに失敗した疑わしい回数はありますか?

詳細については、以下を参照してください。

- AWS ドキュメント: IAM ベストプラクティス: AWS アカウントのアクティビティを監視する
- AWS ドキュメント: AWS CloudTrail による IAM および AWS STS の API コールの口グ記録
- AWS Well-Architected Framework [セキュリティ]: 検出
- AWS セキュリティブログ: Visualizing Amazon GuardDuty findings (Amazon GuardDuty の調査結果を視覚化する)

提案 7.4.2 – オペレーティングシステムでのユーザーおよび認可の変更を口グに記録する

検出または監査に使用できるように、オペレーティングシステム (OS) のユーザーおよび認可イベントの履歴ログを保持することを検討します。ログの保持期間とログに記録するイベントのタイプを、組織によって必要とされるセキュリティポリシーに基づいて決定します。

オペレーションチームが SAP システムのオペレーティングシステムレベルで次のような監査の質問に答えられるようにします。

- 新しいスーパーユーザー OS アカウントは、いつ、誰によって作成されましたか?
- OS アカウントの許可は、いつ、誰によって変更されましたか?
- OS ユーザーが最後に正常にサインインしたのはいつですか?
- OS アカウントへのサインインの試みに失敗した疑わしい回数はありますか?
- OS ユーザーが昇格された許可を最後に使用したのはいつですか?

オペレーティングシステムの監査の詳細については、以下を考慮してください。

オペレーティングシステム	Guidance
SUSE Linux Enterprise Server (SLES)	Linux 監査フレームワークのセットアップ | セキュリティガイド
Red Hat Enterprise Linux	第 13 章システム Red Hat Enterprise Linux 8 の監査 | セキュリティガイド
Microsoft Windows	Windows 監査ポリシーレコメンデーション
Oracle Enterprise Linux	Oracle Linux 8 システムセキュリティの強化 - 監査とモニタリング

提案 7.4.3 – SAP アプリケーションとデータベースのユーザーおよび認可イベントをログに記録する

検出または監査に使用できるように、SAP のユーザーおよび認可イベントの履歴ログを保持することを検討します。アプリケーションスタック (ABAP 認可など) とデータベース (SAP HANA など) の両方を考慮します。ログの保持期間とログに記録するイベントのタイプを、組織によって必要とされるセキュリティポリシーに基づいて決定します。

オペレーションチームがイベントの SAP アプリケーションおよびデータベースレベルで次のような監査の質問に答えられるようにします。

- 新しい SAP またはデータベースアカウントは、いつ、誰によって作成されましたか?
- SAP またはデータベースアカウントの許可は、いつ、誰によって変更されましたか?
- SAP またはデータベースユーザーが最後に正常にサインインしたのはいつですか?
- アカウントへのサインインの試みに失敗した疑わしい回数はありますか?
- アカウントが最後に使用した機密トランザクションコードまたはツールは何ですか?

詳細については、以下を参照してください。

- SAP ドキュメント: SAP Access Control and Governance | User Access (SAP アクセスコントロールとガバナンス | ユーザーアクセス)
- SAP ドキュメント: SAP NetWeaver ABAP: The Security Audit Log (SAP NetWeaver ABAP: セキュリティ監査ログ)
- SAP ドキュメント: SAP NetWeaver JAVA: The Security Audit Log (SAP NetWeaver JAVA: セキュリティ監査ログ)
- SAP ドキュメント: SAP HANA: Auditing Activity in SAP HANA (SAP HANA: SAP HANA でのアクティビティの監査)

提案 7.4.4 – 分析のために、ユーザーおよび認可イベントをセキュリティ情報およびイベント管理 (SIEM) システムで統合する

ユーザーおよび認可イベントのすべてを SAP ワークロードコンポーネントから中央の SIEM ツールに送信して、照合と分析を可能にすることを検討します。SAP Enterprise Threat Detection、サードパーティーのアドオンなどのツールを使用するか、SAP 監査ログをアプリケーションおよびデータベースサーバーから取り込みおよび分析ツールに直接送信します。

ワークロードのベースライン動作を確立し、異常がないかモニタリングして、セキュリティインシデントの検出を高めます。

検討 AWS Marketplace SIEM ソリューション ワークロードをリアルタイムでモニタリングし、セキュリティ問題を特定し、根本原因の分析と修正を加速することを検討します。

詳細については、以下のリソースを考慮してください。

- AWS Marketplace: SIEM ソリューション

- AWS ドキュメント: AWS Security Hub
- SAP ドキュメント: SAP Enterprise Threat Detection
- Well-Architected Framework [セキュリティ]: セキュリティインシデント対応
- AWS ドキュメント: AWS セキュリティインシデント対応 - テクニカルホワイトペーパー

8 – SAP の保管中のデータと送信中のデータを保護する

SAP データをどのように保護しますか? SAP システムは、多くの場合、ビジネス内のコア機能を実行し、機密性の高いエンタープライズデータを保存します。ベストプラクティスは、保管中と送信中のデータを少なくとも 1 つの暗号化メカニズムを使用して暗号化し、社内または社外のセキュリティ要件と規制に準拠することです。次にリストされているコントロールに加えて、 AWS 責任共有モデル AWS は複数の暗号化ソリューションを備えています。多くの AWS サービスは、最小限の労力とパフォーマンスへの影響で暗号化を実行できる機能を備えています。データベースおよび SAP アプリケーションレイヤーで使用可能な暗号化オプションがあるので、検討してください。

ID	優先度	ベストプラクティス
□ BP 8.1	強く推奨	保管中のデータを暗号化する
□ BP 8.2	強く推奨	送信中のデータを暗号化する
□ BP 8.3	強く推奨	脅威から保護するためにデータ復旧メカニズムの安全を確保する

ベストプラクティス 8.1 – 保管中のデータを暗号化する

保管中のデータとは、デジタル的に保存されたデータを指します。このデータが承認されたユーザーにのみ表示され、ストレージまたはデータベースへのアクセスがアプリケーションとは無関係に侵害されるときには保護状態を保つように、暗号化を使用します。

提案 8.1.1 – 暗号化が適用されるレベルを定義する

一般に、暗号化をデプロイするスタックが多いほど、データの安全性は高まります。このセキュリティ強化には、デプロイと管理の複雑さの増加が伴います。AWS は、サービス内で使用可能な保管中の暗号化オプションを使用することをお勧めします。必要なときには、[セキュリティ] で定義されているオペレーティングシステムまたはデータベースの追加の暗号化を検討してください。 ベストプラクティス 5.3 - SAP ワークロードの特定のセキュリティコントロールの必要性を評価する.

提案 8.1.2 – SAP サービスおよびソリューション向けの AWS 暗号化オプションを理解する

保管中のデータについて SAP が依存するコアの AWS サービスは、Amazon EC2 (AMI プラス EBS ボリューム)、Amazon FSx for Windows File Server、または共有ファイルシステム向けの Amazon EFS とバックアップまたはその他のオブジェクトストアユースケース向けの Amazon S3 です。

- AWS ドキュメント: EBS -backed AMI での暗号化の利用
- AWS ドキュメント: Amazon EBS Encryption
- AWS ドキュメント: Amazon EFS 暗号化 / Amazon FSx 暗号化
- AWS ドキュメント: Amazon S3 の暗号化

これらのサービスの保存されたデータは、AWS または AWS KMS からの顧客管理キーを使用して、保管中に暗号化できます。

オペレーティングシステムの暗号化オプションには、BitLocker、DM-crypt、および SuSE Remote Disk があります。

以下のリンクを参考に、データベースの暗号化オプションに関する情報を見つけてください。

データベース	Guidance
SAP HANA	SAP ドキュメント: Server-Side Data Encryption Services (サーバー側のデータ暗号化サービス)
SAP ASE	SAP ドキュメント: SAP ASE 暗号化の概要
IBM Db2	IBM ドキュメント: Db2 暗号化の概要
Oracle	SAP Note: 2591575 - Oracle Transparent Data Encryption (TDE) と SAP NetWeaver の使用 [SAP ポータルへのアクセス権が必要]
Microsoft SQL Server	SAP Note: 1380493 - SQL Server Transparent Data Encryption (TDE) [SAP ポータルへのアクセス権が必要]
SAP MaxDB	SAP ドキュメント: SAP MaxDB データベース管理 - 暗号化

提案 8.1.3 – 暗号化の方法とキー管理ストアを定義する

一般に、キー管理はエンタープライズレベルで定義され、これにより、SAP ワークロードでの使用が許されるキー管理オプションが決まります。AWS KMS は、AWS サービスの暗号化キーの管理を簡素化するセキュアで回復性の高いサービスです。独自のハードウェアセキュリティモジュール (HSM) を管理する必要がある場合は、AWS CloudHSM を使用できます。

- AWS ドキュメント: AWS 暗号化ツールおよびサービスのオプション
- AWS ドキュメント: AWS Key Management Service (AWS KMS)
- AWS ドキュメント: AWS CloudHSM

マスターキーを保護するメカニズムも検討してください。キーのアクセスの制限、ローテーションの管理、および復元力の確保をどのように行いますか?

HANA の保管中のデータの暗号化のルートキーは、ファイルシステム内のインスタンスセキュアストア (インスタンス SSFS) または SAP Data Custodian SaaS Solution でのみ安全に保存できることに注意してください。インスタンスストアを使用する場合、マスターキーは AWS Secrets Manager にローテーションポリシーとともに保存できます。

- SAP Note: 2154997 - Migration of hdbuserstore entries to ABAP SSFS (hdbuserstore エントリの ABAP SSFS への移行) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2755815 - How to Ensure Recoverability of Hana's Data-At-Rest Encryption (HANA の保管中データの暗号化の回復性を確保する方法) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 8.2 – 送信中のデータを暗号化する

送信中のデータの暗号化を使用すると、データがあるポイントから別のポイントへ移動しているときの傍受、アクセス、または改ざんがより困難になります。セキュアなプロトコルとネットワークレベルの暗号化が設定されていて、潜在的な脅威を最小化し、要件に応じた保護レベルを提供していることを確認します。

Well-Architected Framework [セキュリティ]: 伝送中のデータの保護

提案 8.2.1 – SAP およびデータベースプロトコルに基づくアプリケーショントラフィックを暗号化する

SAP プロトコルを使用するアプリケーショントラフィックの場合 (SAPGUI Dialog、RFC、および CPIC) は、SAP SNC を使用してトランスポートレイヤーセキュリティを適用します。

- SAP ドキュメント: SAP システムにおける SNC で保護された通信パス

データベーストラフィックについては、可能な場合、クライアントとデータベース間のセキュアな接続を使用します。

データベース	Guidance
SAP HANA	SAP ドキュメント: SAP HANA: データ通信の保護
SAP ASE	SAP ドキュメント: SAP ASE における SSL
IBM Db2	SAP Note: 2385640 - DB6: database connection using SSL encryption (DB6: SSL 暗号化を使用したデータベース接続) [SAP ポータルへのアクセス権が必要]
Oracle	SAP Note: 973450 - Oracle Database network encryption and data integrity (Oracle データベースネットワークの暗号化とデータの整合性) [SAP ポータルへのアクセス権が必要]
Microsoft SQL Server	SAP Note: 1570930 - SQL Server network encryption with SAP (SAP による SQL Server ネットワークの暗号化) [SAP ポータルへのアクセス権が必要]
SAP MaxDB	SAP ドキュメント: MaxDB ネットワークと通信

提案 8.2.2 – インターネットプロトコルに基づく SAP アプリケーショントラフィックを暗号化する

インターネットプロトコル (HTTP、P4 (RMI)、LDAP) に基づくアプリケーショントラフィックについては、SSL/TLS を使用して、トランスポートレイヤーセキュリティを適用します。

- SAP ドキュメント: トランスポートレイヤーセキュリティ

提案 8.2.3 – ファイル転送またはメッセージ転送プロトコルに基づくデータ交換を暗号化する

ファイルベースの転送の場合、AWS は、SFTP または FTPS 経由でのセキュアなファイル交換のために、AWS Transfer Family を提供します。AWS Transfer Family は Amazon S3 と Amazon EFS 管のデータの転送をサポートします。

- AWS ドキュメント: AWS Transfer Family

メッセージレベルのデータ整合性チェックを使用すると、データが送信中に改ざんされていないことを確認できます。SAP によってサポートされている 1 つ以上のメッセージレベルセキュリティスタンダードを使用して、メッセージ内のデータに署名し、その整合性を確認することを検討してください。

- SAP ドキュメント: SAP ABAP ウェブサービスメッセージレベルセキュリティ
- SAP ドキュメント: SAP NetWeaver プロセス統合セキュリティガイド
- SAP ドキュメント: SAP クラウド統合メッセージレベルセキュリティ

IDOC ベースのメッセージについては、SNC を使用して、ALE によって使用される RFC 接続を保護します。

- SAP ドキュメント: IDocs での機密データの取り扱い

提案 8.2.4 – 管理アクセスを暗号化する

SAP の管理には、Windows と SSH ベースの両方のツールを使用するのが一般的です。Bastian Hosts などのセキュリティコントロールに加えて、このトラフィックの暗号化が可能かどうか検討します。

または、AWS Systems Manager セッションマネージャー は、暗号化に TLS を使用して AWS 管理コンソール経由でオペレーティングシステムにアクセスするセキュアなメカニズムを提供します。

- AWS ドキュメント: Amazon EC2 Windows ガイド - 送信中の暗号化
- AWS ドキュメント: Amazon EC2 Linux ガイド - 送信中の暗号化
- AWS ドキュメント: AWS Systems Manager でのデータ保護 – データ暗号化

提案 8.2.5 – 送信中の暗号化を可能にする AWS サービスの機能を評価する

アプリケーションベースの暗号化に加えて、多くの AWS サービスは送信中の暗号化機能を備えています。各サービスについて、会社のスタンダード、実装の取り組み、および関連する利点を評価します。以下は、SAP ワークロードに関連する例です。

- AWS ドキュメント: Amazon S3 - 送信中の暗号化 - デフォルトで有効であり、Amazon S3 へのバックアップに推奨。
- AWS ドキュメント: Amazon EFS - 送信中の暗号化 / Amazon FSx - 共有ファイルシステムの場合に必要なことがあります。

- AWS ドキュメント: Elastic Load Balancing - この機能はすべてのタイプのロードバランサーで使用できるわけではないため、暗号化要件と、エンドツーエンドな TLS パススルーが必要かどうかをレビューします。
- AWS ドキュメント: Amazon EC2 - 送信中の暗号化 - より新しい世代のインスタンスタイプのみが、この機能を備えています。

提案 8.2.6 – ネットワークレベルの暗号化を実装する

SAP のお客様は、一般に、Direct Connect または Direct Connect と VPN の組み合わせのいずれかを使用して、AWS 上のリソースへの信頼できる接続性を提供しています。

AWS Direct Connect は、送信中のトラフィックを暗号化しません。暗号化が必要な場合は、例えば、VPN over Direct Connect を使用して、トランスポートレベルの暗号化を実装してください。

AWS は、ネットワークチャネルの暗号化に使用できるサイト間 VPN を提供します。AWS Marketplace から、または Bring-Your-Own-License で Open VPN などのサードパーティー VPN ソリューションをデプロイすることもできます。

- AWS ドキュメント: AWS マネージド VPN
- AWS ドキュメント: AWS Direct Connect + VPN
- AWS ドキュメント: ソフトウェアサイト間 VPN

ベストプラクティス 8.3 - データ復旧メカニズムを確保して、脅威から保護する

悪意あるアクティビティから保護するために、組織のセキュリティフレームワーク内で定められているガイドラインに従ってください。それらの 日本語ガイド: AWS クラウド環境をランサムウェアから保護する には、インシデント前およびインシデント対応の一環としての重要な項目の概要が説明されていて、ネットワークコントロール、パッチ適用、最小特権許可などが含まれています。SAP システムの場合、脅威は他のアプリケーションと同様ですが、影響はより大きくなる可能性があります。SAP がレコードのシステムの場合や、ミッションクリティカルなトランザクションのために必要とされる場合は、以下の提案を検討して、悪意ある攻撃からバックアップを保護してください。

- SAP Note: 2663467 - Tips to avoid a Ransomware situation (ランサムウェア状況を回避するためのヒント) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2496239 - Ransomware / malware on Windows (Windows でのランサムウェア / マルウェア) [SAP ポータルへのアクセス権が必要]

提案 8.3.1 – 追加のコントロールで個別アカウントのバックアップを保護する

データのプライマリコピーから隔離されたアカウントでバックアップを直接、またはレプリケーションを使用して保護することにより、システム侵害がデータ復旧メカニズムにも影響を与えるリスクを最小化できます。

セカンダリアカウントは、ユースケースに応じたアクセス要件を持つ “データバンカー” として見ることができます。

Amazon S3 を使用するバックアップの場合、追加のコントロールとして、write-once-read-many (WORM) モデルを使用してオブジェクトを保存する S3 Object Lock、または 多要素認証削除を含めることができます。 .

レプリケーションを使用する場合は、使用可能なさまざまなオプション、例えば、 削除マーカーレプリケーション (デフォルトでは、削除マーカーはレプリケートされません) や S3 レプリケーション時間制御などを理解してください .コストを最適化するには、プライマリとセカンダリの両方のバケットでハウスキーピングが実行されることを確認します。

提案 8.3.2 – 復旧能力を検証する

バックアップは、悪意あるアクティビティからデータを保護する最後の防衛線ですが、バックアップが不完全であったり、バックアップが有効でなかったりするために復旧できない場合は役に立ちません。バックアップにアクセスできない場合や復号化できない場合も、復旧は不可能です。暗号化キーと認証情報をどのように保護するか考慮してください。

代替アカウントでの再構築も含めて、悪意あるシナリオに応じた復旧テストを実行してください。

- SAP Lens [運用上の優秀性]: ベストプラクティス 4.3 - 事業継続性計画と障害復旧を定期的にテストする

9 – セキュリティイベントのロギング、テスト、および対応のためのセキュリティ戦略を実装する

適切なロギング、テスト、および文書化された対応方法でサポートされている戦略的セキュリティプランはありますか? 戦略的セキュリティプランを持つことは、あらゆるセキュリティ課題に対処するために行わなければならない事前タスクと事後タスクの形成に役立ちます。AWS 上の SAP ワークロードのセキュリティインシデントの識別と修復に役立つロギング、検出、および追加保護の手順は、Well-Architected Framework のセキュリティの柱で詳しく述べられているものと同じです。この

セクションのガイダンスに加えて、「セキュリティの柱」にある検出とインシデント対応に関するベストプラクティスをレビューしてください。

ID	優先度	ベストプラクティス
□ BP 9.1	必須	SAP アプリケーションとデータベースのログ分析に関するセキュリティ戦略を理解する
□ BP 9.2	強く推奨	セキュリティバグに関する定期的なテストを実行する
□ BP 9.3	強く推奨	セキュリティイベントに対応する文書化されたプランを持つ

- Well-Architected Framework [セキュリティ]: 検出
- Well-Architected Framework [セキュリティ]: インシデント対応

ベストプラクティス 9.1 – SAP アプリケーションおよびデータベースのセキュリティログ分析に関する戦略を理解する

適切な詳細度のセキュリティログを保持しなければ、インシデント対応、フォレンジックなセキュリティ分析、および脅威のモデリングのために必要な貴重なデータが失われることがあります。SAP セキュリティスタッフは、お客様のビジネス上のセキュリティ要件に応じて、SAP システムに影響する潜在的なセキュリティインシデントを評価できなければなりません。AWS 上で実行する SAP ワークロードの場合、「Well-Architected Framework セキュリティの柱」で説明されている AWS サービスは、以下の提案と組み合わせて、有効な出発点となります。

- Well-Architected Framework [セキュリティ]: 検出 – 構成

提案 9.1.1 – セキュリティイベントの検出に必要なログを決める

個々の SAP ソフトウェアおよびサポートされるデータベースについて、SAP NetWeaver Guide Finder や SAP NetWeaver セキュリティガイドを参照して、該当するログ (例えば、 読み取りアクセスログ) を指定する必要があります。さらに、SAP アドバイザリをレビューして、 セキュリティロギング と、開発アクティビティのベストプラクティスに関する関連トピックを確認してください。

- SAP ドキュメント: SAP NetWeaver Guide Finder

- SAP ドキュメント: ABAP Platform Security Guide
- SAP ドキュメント: セキュリティロギング

提案 9.1.2 – ログの保存と分析のメカニズムを開発する

セキュアな SAP インストールのためには、潜在的なセキュリティイベントに関する関連データが必要ですが、同じように重要なのは、そのデータを安全に保存することと、データを効率的かつ迅速に検索し、分析するために必要なツールを用意することです。AWS でのオプションとしては、CloudWatch エージェント を使用して、セキュリティ関連のインスタンスログと SAP アプリケーションログを Amazon CloudWatch ロググループに保存する方法があります。 .そのようなログは、Amazon S3 にエクスポートして、 包括的なログ分析を行ったり、 サードパーティーのログ分析ソリューションと統合したりできます .

AWS セキュリティログでの SAP の組み立て、結合、および分析については、以下を参照してください。

- SAP Lens [セキュリティ]: 提案 7.4.4 – 分析のために、ユーザーおよび認可イベントをセキュリティ情報およびイベント管理 (SIEM) システムで統合する
- SAP on AWS ブログ: SAP HANA monitoring: A serverless approach using Amazon CloudWatch (SAP HANA モニタリング: Amazon CloudWatch を使用したサーバーレスアプローチ)
- SAP on AWS ブログ: SAP Monitoring: A serverless approach using Amazon CloudWatch (SAP モニタリング: Amazon CloudWatch を使用したサーバーレスアプローチ)

ベストプラクティス 9.2 – セキュリティバグがないか、定期的にテストする

「Well-Architected Framework セキュリティの柱」のインシデント対応のセクションで述べられているように、シミュレーション、ランブックの作成、およびゲームデーの実施は、AWS 上の SAP も含め、あらゆるワークロードについて推奨されます。このタイプの定期的なテストによって、新しい攻撃ベクトルや脆弱性を特定できるだけでなく、セキュリティインシデントが発生した際の迅速で効果的な対応のための SAP セキュリティリソースを準備できます。

Well-Architected Framework [セキュリティ]: インシデント対応 - シミュレーション

提案 9.2.1 – 標準のセキュリティおよび侵入テストに加えて、SAP アプリケーションをターゲットとして含める

試験的なセキュリティテストは、セキュアな環境を維持するための重要な部分です。AWS で標準的な侵入テストを実施することに加えて、悪意あるアクティビティの追加の潜在的ターゲットとして

SAP ソリューションを加えてください。SAProuter、Web Dispatcher、Cloud Connector、SAP Fiori など、アーキテクチャで公開されることが多い SAP 固有のソフトウェアソリューションを念頭に置いてください。

- AWS ドキュメント: 侵入テスト

ベストプラクティス 9.3 – セキュリティイベントに対応するための文書化されたプランを持つ

SAP アプリケーションにかかわるセキュリティイベントに対応するための文書化されたプランがなければ、セキュリティチームの対応が遅く、包括的でないものになり、イベントの緩和においても、原因の理解においても、効果の薄いものになる可能性があります。SAP アプリケーションについて、セキュリティ対応パターンを徹底的に文書化します。

提案 9.3.1 - 文書化されたインシデント管理プランを作成することで、セキュリティイベントに備える

これは、「AWS Well-Architected Framework セキュリティの柱」のインシデント対応の準備に関するガイダンスに直接対応しています。このドキュメントを参照し、それに従って SAP アプリケーションを含めます。

- Well-Architected Framework [セキュリティ]: インシデント対応 - 準備

信頼性

信頼性の柱には、意図した機能を期待どおりに正しく一貫して実行するワークロードの能力が含まれます。これには、ワークロードのライフサイクル全体を通じてワークロードを運用およびテストする能力が含まれます。多くのビジネスでは、信頼性について Well-Architected であることが SAP ワークロードの重要な要件です。これは、多くの SAP ワークロードのミッションクリティカルな性質と、SAP アーキテクチャとこれが課す制限を理解する必要性によります。

他の柱と同様に、AWS Well-Architected Framework、特に基礎、変更管理、および障害管理のベストプラクティスについてレビューすることをお勧めします。SAP Lens で信頼性を考慮するときには、個々のシステムにわたる機能以外の要件と、これらの要件をもたらすビジネスの優先度について、明確でバランスの取れた理解を持つことを第一に考えてください。次に、可用性と災害対策 (DR) を区別します。可用性は、コンポーネントの障害にもかかわらず、エンドユーザーが SAP システムに引き続きアクセスできるシナリオに関連します。これとは対照的に、ワークロード全体が使用不能になるシナリオでは、DR イベントが宣言されます。

10 – 障害に耐える設計

SAP ワークロードを障害に耐えるようにどのように設計しますか? ビジネス要件からさかのぼって、SAP インフラストラクチャとデータの可用性目標に合わせたアプローチを定義します。それぞれの障害シナリオについて、回復性要件、受け入れ可能なデータ損失、および平均復旧時間 (MTTR) は、サポートするコンポーネントとビジネスアプリケーションの重要性に比例する必要があります。SAP の可用性のために提供されるアーキテクチャのパターンは、ほとんどのお客様の要件に対応していますが、定義した条件に基づいて適応させることができます。これらの条件には、各障害について認識されたリスクと影響を含める必要があり、コストとパフォーマンスも考慮する必要があります。どのような場合も、初期テストと定期的なテストによって、決定を検証してください。

ID	優先度	ベストプラクティス
□ BP 10.1	必須	ビジネス要件に合った SAP ワークロード可用性目標について合意する
□ BP 10.2	強く推奨	可用性および容量要件に適した SAP デプロイパターンを選択する
□ BP 10.3	強く推奨	重要な SAP データの可用性に役立つアプローチを定義する
□ BP 10.4	推奨される	ビジネス要件に基づく一連の条件に対して設計を検証する

詳細については、以下の情報を参照してください。

- AWS ドキュメント: Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス) 以下が含まれます。 障害シナリオ とアーキテクチャパターン
- AWS ドキュメント: The Amazon Builders' Library: アベイラビリティーゾーンを使用した静的安定性
- AWS ドキュメント: Multiple data center HA network connectivity
- SAP ドキュメント: SAP HANA システムアーキテクチャの概要

ベストプラクティス 10.1 – ビジネス要件に合った SAP ワークロードの可用性目標について合意する

可用性目標を理解することは、組織にとって重要な要素に注意を向けるための最初のステップです。これは、アーキテクチャパターンの評価に使用できる条件を定義する上で役立ちます。

提案 10.1.1 – 範囲内の SAP アプリケーションとそれらの相互依存関係を特定する

AWS にデプロイした、またはデプロイする予定の SAP アプリケーションを特定します。場所に関係なく、これらのアプリケーションの依存関係を理解します。

提案 10.1.2 – 障害の影響に基づいてシステムを分類する

計画された可用性と障害のリスクに応じたシステム分類について、公開されているスタンダードはありません。「ミッションクリティカル」や「非常に重要」などの用語を使用したシステムの定義は、パターンの定義、アプリケーショングループの識別、およびコストの正当化に役立ちます。生産アプリケーションは、停止によって異なる影響を受ける可能性があります。考慮すべき要素は、次のとおりです。

- 収益創出または収益報告
- 外向きまたは内向き
- コアビジネス対技術サポート
- 他のシステムとの密結合対疎結合

非生産環境もビジネスの間接的なサポートにおいて重要な役割を果たすことがあります。これらはプロジェクトのフェーズとスケールに従って分類する必要があり、トランスポートパス (通常営業とプロジェクトなど) やサポートの役割 (開発、ユニットテスト、生産コピー、トレーニングなど) を考慮に入れる必要があります。

提案 10.1.3 – 停止によるビジネスへの影響を評価する

影響は測定可能でなければならず、停止の期間を考慮する必要があります。影響分野の例としては、健康と安全性、財務、法務、規制、ブランドなどがあります。

提案 10.1.4 – コンプライアンスおよび規制要件を理解する

データレジデンシーと場所間の距離に関するコンプライアンスまたは規制要件を理解することは、事業継続性の確保に役立ちます。

提案 10.1.5 – 最小許容稼働率を定義する

各システムまたは各システムグループについて、ビジネス要件に応じた許容可能稼働率を合意し、文書化します。このコンテキストでは、以下の用語が使用されます。

- MTTR – 平均復旧時間
- RTO – 目標復旧時間
- RPO – 目標復旧時点

用語の詳しい説明については、「Well-Architected Framework [信頼性]」を参照してください。 可用性 .SAP における信頼性の詳細については、次のホワイトペーパーを参照してください。

- AWS ドキュメント: Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス)

ベストプラクティス 10.2 – 可用性および容量要件に適したアーキテクチャを選択する

SAP on AWS をデプロイするほとんどのお客様の要件に適した SAP 可用性の標準的なアーキテクチャパターンがあります。以下の提案を参考にして、お客様の可用性および容量要件に最適なパターンを判断してください。ビジネス要件に対して、各障害シナリオのリスクと影響を評価します。

SAP の可用性に関する追加情報については、次のホワイトペーパーを参照してください。 Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス) .

提案 10.2.1 – SAP システムに必要なすべてのコンポーネントと AWS サービスを特定する

SAP システムに必要な技術コンポーネントをすべて特定します。コア (データベース、アプリケーションサーバー、中央のサービス、グローバルファイルシステム) から始めて、オプションコンポーネント (例えば、ウェブディスパッチャー、SAProuter、クラウドコネクター) へと広げていきます。これらのコンポーネントをサポートするために必要な AWS サービスを決めます。

提案 10.2.2 – SLA、耐久性、可用性、および履歴データを障害の可能性のガイドとして使用する

障害の可能性は主観的です。公開されているサービスレベルアグリーメント (SLA) と過去のパフォーマンスは、将来の潜在的な障害リスクの目安にしかなりません。ただし、さまざまなシナリオの想定頻度は、やはり有益なデータポイントです。統計上、年に一度は発生する可能性のあるものは、まだ発生していない障害より設計の決定に与える影響が大きいかもしれません。

以下の情報はサービスの理解を深めるのに役立ちます。

- AWS Personal Health Dashboard は、AWS がユーザーに影響を及ぼす可能性のあるイベントを検出したときにアラートと修正ガイダンスを提供します。
- AWS Post-Event Summaries は、AWS サービスの可用性に影響を及ぼすあらゆる主要なサービスイベントについて提供されます。
- Amazon Compute Service Level Agreement は、コンピューティングサービスの SLA をリストします。
- AWS ドキュメント: Amazon EBS 耐久性と可用性
- AWS ドキュメント: Amazon EFS データ保護と可用性
- AWS ドキュメント: AWS Direct Connect の回復性に関する推奨事項

その他のサポートサービスの障害の可能性も評価する必要があり、これにはドメインネームサービス、ロードバランサー、サーバーレス機能などが含まれますが、これらに限りません。

詳細については、「SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス」ホワイトペーパーを参照してください。.

提案 10.2.3 – クラスタリング、回復性、およびロードバランシングのためのオプションを評価する

SAP システムは、可用性を確保するために、メカニズムの異なる複数のホストに分散することができます。例えば、クラスタリングソリューションを使用して、単一障害点 (SAP データベースや SAP セントラルサービスなど) を保護することができます。SAP アプリケーション層を水平に拡張でき、ロードバランシングを使用してウェブディスパッチャーの可用性を高めることができます。

- AWS ドキュメント: SAP NetWeaver Deployment and Operations Guide for Windows - High Availability System Deployment (高可用性システムのデプロイ)
- AWS ドキュメント: SAP on AWS – IBM Db2 HADR with Pacemaker
- AWS ドキュメント: SQL Server Deployment for High Availability (SQL Server 高可用性のためのデプロイ)
- SAP ドキュメント: High Availability Partners (高可用性パートナー)

提案 10.2.4 - アベイラビリティーゾーン内の EC2 インスタンスファミリーの可用性を決める

一部の Amazon EC2 インスタンスファミリー (例えば、X および U) は、すべての AZ で使用可能なわけではありません。AWS アカウントチームまたは AWS サポートとともに、使用したい EC2 インスタンスファミリーが目的のアベイラビリティーゾーンで使用できることを確認します。論理 AZ 識

別子は、アカウントによって異なる場合があることに注意してください。詳細については、AWS のドキュメントを参照してください。

- AWS ドキュメント: AWS リソースの AZ ID

提案 10.2.5 – 容量を確保するための戦略を調査する

容量確保に役立つ最善の方法は、障害の際に使用できる同様のサイズのインスタンスを用意しておくことです。その他の戦略としては、クラウドネイティブなオプション (オンデマンドインスタンス、EC2 インスタンス復旧など) や共有容量の再割り当てがあります。

必要なときに容量が使用できるように、SAP 単一障害点をサポートする Amazon EC2 インスタンスについて少なくとも 2 つの AZ で容量コミットメントを行うことをお勧めします。

EC2 容量は、以下を使用して予約できます。 ゾーンリザーブドインスタンス または オンデマンドキャパシティ予約 .ゾーンリザーブドインスタンスとオンデマンドキャパシティ予約は、両方とも、同じ AWS 組織内の AWS アカウント間で共有できるため、重大な障害 (完全な AZ 障害など) の際には、別の環境の犠牲容量を使用するというアプローチが可能です。

キャパシティ予約の詳細については、以下を参照してください。

- AWS ドキュメント: Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス)

提案 10.2.6 – 複数のアベイラビリティーゾーンにまたがって VPC を設計する

初期の設計が 1 つか 2 つのアベイラビリティーゾーンに依存する場合でも、複数の AZ でインスタンスをプロビジョニングできるように VPC とサブネットを設計します。これにより設計に回復性が組み込まれ、接続性とサービスへのアクセスを事前に確認できます。

ベストプラクティス 10.3 – 重要な SAP データの可用性を確保するアプローチを定義する

SAP アプリケーション用のビジネスデータは、主にデータベースに保存されますが、バイナリ (実行可能ファイル、ライブラリ、スクリプトなど)、構成、インターフェイスの場合はファイルベースのデータを含むこともあります。選択したアプローチの耐久性、整合性、および復旧オプションを調べて、データの重要性や許容可能データ損失率 (RPO) に合うことを確認する必要があります。

提案 10.3.1 – MTTR 要件を評価して、要件を満たす方法を特定する

[信頼性] 提案 10.1.5 – 最小許容稼働率を定義する で、各アプリケーションの MTTR 要件を定義します。障害のリスクとシステムの可用性を保護するメカニズムを評価した後は、要件を満たせることを確認し、各障害シナリオで予想される MTTR を文書化します。コスト、複雑さ、または整合性の点で妥協が必要な場合は、ビジネス所有者と協議して、合意を得ます。

提案 10.3.2 – バックアップからの復旧が必要になる障害シナリオを判断する

バックアップは、多くの場合、可用性を確保または復旧するための 2 次的なメカニズムですが、ほとんどのアーキテクチャは何らかの形でバックアップに依存します。以下は、分析の参考になる障害シナリオの例です。シナリオ、分類、および影響の詳細度は、要件とアーキテクチャによって異なります。

	発生リスクの比較	必要なバックアップ	潜在的なデータ損失	推計復旧時間
計画/管理保守	計画			
リソースの枯渇または侵害 (高い CPU 使用率/ファイルシステムがいっぱい/メモリ不足/ストレージの問題)	ミディアム			
分散ステートレスコンポーネントの障害 (ウェブディスパッチャーなど)	ミディアム			
分散ステートフルコンポーネントの障害 (アプリケーションサーバーなど)	ミディアム			
単一障害点 (データベース/SAP セントラルサービス)	ミディアム			
AZ/ネットワーク障害	低			
コアサービスの障害 (DNS/Amazon EFS/API コール)	低/中			
破損/過失による削除/悪意のあるアクティビティ/コードデプロイの誤り	低			
リージョン障害	非常に低い			

提案 10.3.3 – データのレプリケーションが必要な場所を決める

データのレプリケーションは、同じデータのコピーを複数の場所に置くことによって信頼性を高めるために使用され、多くの場合、RPO が低いシステムの要件です。可用性または復旧のためにレプリケーションが必要かどうかを判断するときには、サービスがゾーン別 (Amazon EC2 および Amazon EBS とそれらがサポートするデータベースなど) かリージョン別 (共有ストレージと Amazon S3 など) かを考慮してください。

データベース	レプリケーションテクノロジー	Guidance
SAP HANA	HANA システムレプリケーション	SAP ドキュメント: HANA システムレプリケーション
SAP ASE	SAP Replication Server	SAP ドキュメント: SAP Replication Server
Oracle	Oracle Data Guard	SAP Note: 105047 - Support for Oracle functions in the SAP environment (SAP 環境での Oracle Functions のサポート) [SAP ポータルへのアクセス権が必要]
Microsoft SQL Server	SQL Server Always ON	• SAP ドキュメント: Database High-Availability with SQL Server AlwaysOn (SQL Server AlwaysOn によるデータベースの高可用性) • AWS ドキュメント: SQL Server Deployment for High Availability (SQL Server 高可用性のためのデプロイ)
SAP MaxDB	MaxDb スタンバイデータベース	SAP Note: 952783 - FAQ: SAP MaxDB high availability (FAQ: SAP MaxDB 高可用性) [SAP ポータルへのアクセス権が必要]
IBM Db2	HADR	SAP Note: 1612105 - DB6: FAQ on Db2 High Availability Disaster Recovery (HADR) (DB6: Db2 High Availability Disaster Recovery (HADR) についてのよくある質問) [SAP ポータルへのアクセス権が必要]

AWS DataSync を使用して、必要な場合、 Amazon EFS と Amazon FSx の両方をリージョンにまたがって保護できます。

CloudEndure Disaster Recovery は、AWS アカウント間も含め、アベイラビリティーゾーンまたはリージョン間でインスタンスを継続的に複製します。

Amazon S3 レプリケーション

バックアップやその他のオブジェクトストレージは、Amazon S3 に保存されることがあり、以下を使用して複製できます。 Amazon S3 レプリケーション .

提案 10.3.4 – 一貫した構成データとバイナリを確保する戦略を立てる

予測可能な動作と障害後のテスト済みセットアップを確保するためには、一貫性のある構成データとバイナリが重要です。これには、オペレーティングシステムのパッケージ、アプリケーションのパラメータ、およびクラスター構成が含まれます。回復力のためのもの (追加のアプリケーションサーバー、セカンダリデータベースノードなど) も含め、アプリケーションのすべてのインスタンスについて整合性を確保する方法を決めます。

Amazon EFS、Amazon FSx、および Amazon S3 は、共有バイナリまたは構成を集中管理できる耐久性の高い場所を提供します。

[運用上の優秀性] ベストプラクティス 2.1 - バージョン管理と設定管理を使用する の柱のバージョン管理と構成管理のメカニズムを参照してください。

提案 10.3.5 – データ整合性のための包括的アプローチを持つ

重要な SAP データの整合性を確保するためのアプローチは、単一のデータセットに注目するだけでなく、データセット内とシステム内およびデータセット間とシステム間の依存性も考慮する必要があります。例えば、プルの元になるソースシステムではなく SAP BW システムを復旧する必要がある場合、変更ポインターにはどのような影響が予想され、整合性のある復旧を確保するためにどのようなメカニズムが存在しているでしょうか?

提案 10.3.6 – データを再生または再送信できるインターフェイスの戦略を立てる

システム間のデータ交換について、統合が疎結合かどうかと、ソースまたはターゲットでデータを再生または再送信できるかどうかを判断します。シナリオを中断したり、停止中にキャッシュしたりできるキューイング機能があるかどうかをレビューします。

提案 10.3.7 – データバンカーの使用を評価する

偶発的な削除や悪意ある行動などの状況により、オンラインデータが使用不能または入手不能になるような障害シナリオでは、データの保護または復旧可能性を確保するために異なるアプローチが必要になることがあります。

ネットワーク分離とアクセスコントロールをカバーするセキュリティフレームワークでの予防が最良の防御ですが、復旧と回復のコンテキストで影響を考慮する必要があります。

保持期間が限られた 書き込み専用 バックアップアカウントを使用するのが、このようにまれですが潜在的に高い影響力を持つシナリオでの一般的なアプローチです。

- SAP Lens [セキュリティ]: ベストプラクティス 8.3 - データ復旧メカニズムを確保して、脅威から保護する

ベストプラクティス 10.4 – ビジネス要件に基づく一連の条件に対して設計を検証する

ビジネスの要件に基づき、障害のリスク、ビジネスへの影響、および許容可能なトレードオフのバランスを取って、一連の条件を設定します。これらの条件を使用して、設計を検証し、必要な場合は調整を加えます。

提案 10.4.1 – 停止によるビジネスのコストを評価する

AWS サービスまたは SAP コンポーネントの障害は、回復性および復旧戦略に応じて異なる影響を SAP システムに及ぼします。障害のタイプによって、停止の期間 (RTO) と潜在的なデータ損失 (RPO) が決まります。

障害ごとに、停止のリスクとビジネスのコストを評価します。例えば、システムが使用できないことによって影響を受ける収益創出プロセスがありますか、また、時間あたりのコストはどのくらいですか?

提案 10.4.2 – アーキテクチャのコストを評価する

SAP 環境では、AWS の月額で最大の要素は、一般に Amazon EC2 とストレージ関連のサービスです。コストへの影響を理解して、信頼性要件に応じた最良のアーキテクチャを選択してください。主な要因には以下のものがあります。

- ハードウェアの利用率を最大化しないデプロイパターン
- 冗長なデータコピー
- オペレーティングシステムのライセンスコスト
- クラスタリングソフトウェアライセンスのコスト
- メンテナンス、テスト、およびスキルを備えた人材に関連するコスト

詳細については、[コスト最適化]: コスト最適化のためのベストプラクティス を参照してください。

提案 10.4.3 – フレームワークの他の柱に対して設計を評価する

信頼性は単独で設計することはできず、AWS Well-Architected Framework の他の柱に対して評価する必要があります。これを評価するための質問の例を以下に示します。

- 運用上の優秀性 — ソリューション管理の経験とスキルはありますか?
- セキュリティ — データはレプリケーションや復旧などの際に保護されていますか?
- パフォーマンス — レプリケーションまたはバックアップアクティビティはユーザーのパフォーマンスに影響を与えますか?
- コスト最適化 — ソリューションのコストは想定されるリスクに合っていますか?

11 – 障害を検出し、対応する

SAP ワークロードに影響を与える障害をどのように検出し、対応しますか? ソフトウェアまたは操作手順によって SAP ワークロードのヘルスと回復性を確立する方法を設計します。可能な場合は予防を重視して、潜在的な障害と実際の障害を監視します。コンポーネント分散されているか、それとも単一障害点かを考慮して、ワークロードへの影響を最小化する回復性ソリューションを設計します。リスクのプロファイルを理解するための定期的なテストに加えて、オートメーションによって回復性を向上させられるか調べます。

ID	優先度	ベストプラクティス
□ BP 11.1	必須	SAP アプリケーション、AWS リソース、および接続性の障害をモニタリングする
□ BP 11.2	強く推奨	可用性を維持するためのアプローチを定義する
□ BP 11.3	強く推奨	サービスの可用性を復元するためのアプローチを定義する
□ BP 11.4	強く推奨	定期的な回復力テストを実施する
□ BP 11.5	推奨される	障害への対応を自動化する

詳細については、以下を参照してください。

- AWS ドキュメント: Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス) 以下が含まれます。 障害シナリオ と アーキテクチャパターン

ベストプラクティス 11.1 – SAP アプリケーション、AWS リソース、および接続性の障害をモニタリングする

SAP アプリケーション、AWS リソース、および接続性の障害のモニタリングは、障害または潜在的な障害に迅速に対応するのに役立ちます。

提案 11.1.1 – AWS Personal Health Dashboard および通知を使用する

それらの AWS Personal Health Dashboard は、アプリケーションを支援する AWS サービスのステータスをパーソナライズして表示するため、SAP ワークロードに影響する問題をすぐに把握できます。例えば、 Amazon Elastic Block Store (Amazon EBS) ボリュームのうち、 Amazon EC2 インスタンスの 1 つに関連するものが失われた場合です。

ダッシュボードは予想通知も提供し、E メールも含む複数のチャネルでアラートをセットアップできるため、計画的変更のプランニングに役立つ関連情報を適時に受け取ることができます。例えば、AWS ハードウェアメンテナンスアクティビティが発生し、 Amazon EC2 インスタンスの 1 つに影響がある場合は、今後の変更を計画し、関連する問題に予防的に対処するのに役立つ情報を含んだ通知を受け取ります。

提案 11.1.2 – AWS サービスを評価して、SAP システムのヘルスを理解する

AWS が提供する多数の 管理およびガバナンス サービスを評価する必要があります。EC2 インスタンス障害、高い CPU 使用率、ファイルシステム使用率など、障害または潜在的な障害を示すメトリクスに注目します。

詳細については、「運用上の優秀性の柱」を参照してください。

- SAP Lens [運用上の優秀性]: ベストプラクティス 1.1 - SAP on AWS をモニタリングするための前提条件を実装する
- SAP Lens [運用上の優秀性]: ベストプラクティス 1.4 – ワークロード設定モニタリングを実装する

提案 11.1.3 – 障害をモニタリングする SAP ツールの機能を評価する

Solution Manager や Landscape Manager など、SAP のツールでは、アプリケーションのコンテキストでモニタリングデータを表示できます。SAP には、以下のモニタリングソリューションがあります。これらのツールの評価の一環として、追加のライセンシングコストをレビューしてください。

- SAP ドキュメント: SAP Focused run
- SAP ドキュメント: SAP Solution Manager
- SAP ドキュメント: SAP Landscape Manager (LaMa)
- SAP Note: 2574820 - SAP Landscape Management Cloud Manager for Amazon Web Services (AWS) (アマゾン ウェブ サービス (AWS) 向け SAP Landscape Management Cloud Manager) [SAP ポータルへのアクセス権が必要]

提案 11.1.4 – AWS と SAP のモニタリングのためのサードパーティーツールを評価する

AWS Marketplace から以下のモニタリングソリューションを入手できます。これらやその他のサードパーティーツールを評価してください。

- AWS ドキュメント: Monitoring Solutions in AWS Marketplace (AWS Marketplace のモニタリングソリューション)

ベストプラクティス 11.2 – 可用性を維持するためのアプローチを定義する

単一の技術的要素の障害や AWS サービスの障害に耐えられる回復力のあるアーキテクチャを持つことで、可用性を維持します。メカニズムには、冗長な容量、ロードバランシング、およびソフトウェアクラスターなどが含まれます。

提案 11.2.1 – リソースの枯渇やサービスの低下による障害を回避する

リソースのオーバープロビジョニング、増加のプロアクティブなモニタリング、および制限の設定による使用量のスロットリングを調査します。

運用上の優秀性の柱では、SAP アプリケーションの状態を理解し、適切なアクションを取るためのさまざまな方法が説明されています。以下を参照してください。[運用上の優秀性]: 1 - 状態の理解と反応ができるように SAP ワークロードを設計する .

パフォーマンスの柱は、容量の適切なサイジングとスケーリングに関するガイダンスによって支援します。[パフォーマンス]: 16 – 継続的なパフォーマンスと最適化のオプションを理解する .

提案 11.2.2 – 計画保守の戦略を持つ

ビジネスに保守停止を最小限にする要件がある場合は、すべてのレベル、つまり、SAP アプリケーション、データベース、オペレーティングシステム、および AWS でメンテナンス戦略を開発する必要があります。以下の点を考慮してください。

- プライマリノードとセカンダリノードを切り替えるためのレプリケーションおよびクラスターソリューションの使用。
- ローリング停止を容易にするための超過容量と拡張縮小メカニズム。
- 可能な場合は、オペレーティングシステムのライブパッチ適用アプローチの使用。
  - SUSE Linux Enterprise Live Patching
  - Red Hat Reducing downtime for SAP HANA ホワイトペーパー
- AWS ドキュメント: AWS Systems Manager Patch Manager パッチグループの使用
- SAP Note: 1913302 - HANA: 短時間のメンテナンスタスクのための DB 接続の中断 [SAP ポータルへのアクセス権が必要]
- SAP Note: 2077934 - Rolling kernel switch in HA environments (HA 環境でのローリングカーネルスイッチ) [SAP ポータルへのアクセス権が必要]
- SAP Note: 953653 - Rolling Kernel Switch (ローリングカーネルスイッチ) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2254173 - Linux: Rolling Kernel Switch in Pacemaker-based NetWeaver HA environments (Linux: ペースメーカーベースの NetWeaver HA 環境でのローリングカーネルスイッチ) [SAP ポータルへのアクセス権が必要]

一時的にパフォーマンスを高めることによって計画保守の全体的ダウンタイムを短縮する AWS サービスのエラスティック機能も評価してください。例えば、データベースを実行している Amazon EC2 インスタンスのサイズを拡張して、アップグレードアクティビティのために CPU とストレージのスループットを高めたり、EBS ボリュームのタイプを gp2 から io2 に切り替えて、データベースの再編成中のストレージスループットを高めたりします。

提案 11.2.3 – SAP の単一障害点をソフトウェアクラスターまたはその他のメカニズムで保護する

高可用性 (HA) クラスタリングソリューションを使用して、アベイラビリティーゾーン間の SAP の単一障害点 (SAP セントラルサービスとデータベース) の自律的フェイルオーバーを実現できます。

複数の SAP 認定クラスタリングソリューションがあり、 SAP ウェブサイトに記載されています .SAP クラスタリングソリューションは、SAP ではなく、クラスターソフトウェアベンダー自身によってサポートされています。SAP はソリューションを認定しているだけです。カスタムビルドのソリューションは認定されず、ソリューションビルダーのサポートが必要です。

単一障害点にクラスタリングソリューションを使用しないことにした場合は、サービスの復元に関連するエラーを最小化するために、スクリプティングまたはランブックを検討してください。

提案 11.2.4 – サポートするコンポーネントについては、冗長容量またはオートスケーリング

使用状況に合った静的、動的、またはスケジュールされた容量変更を評価します。最小容量要件と、障害およびメンテナンスによる影響を調べます。適切な場合は、障害から復旧する時間が得られるように、オーバープロビジョニングします。

AZ 障害の発生時に 100% の容量を維持する必要がある場合は、アプリケーション層を 3 つの AZ に、必要な総容量の 50% ずつデプロイすることを検討してください。

SAP アプリケーションサーバーレイヤーを複数の AZ にデプロイすることに加えて、SAP on AWS ブログ投稿で説明されているようなスケーリングソリューションを検討することもできます。 Amazon EC2 Auto Scaling .

- SAP on AWS ブログ: Using AWS to enable SAP Application Auto Scaling (AWS を使用した SAP アプリケーションのオートスケーリングの有効化)
- AWS ドキュメント: SAP 向け Amazon EC2 インスタンスタイプ
- SAP Note: 1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products (AWS 上の SAP アプリケーション: サポートされる DB/OS および Amazon EC2 製品) [SAP ポータルへのアクセス権が必要]

提案 11.2.5 – 特定されたすべての障害シナリオに対応する容量を確保する

以下は、分析の参考になる障害シナリオの例です。シナリオ、分類、および影響の詳細度や範囲は、要件とアーキテクチャによって異なります。

障害シナリオの例	発生リスクの比較
計画/管理保守	計画
リソースの枯渇または侵害 (高い CPU 使用率/ファイルシステムがいっぱい/メモリ不足/ストレージの問題)	ミディアム
分散ステートレスコンポーネントの障害 (ウェブディスパッチャーなど)	ミディアム
分散ステートフルコンポーネントの障害 (アプリケーションサーバーなど)	ミディアム

障害シナリオの例	発生リスクの比較
単一障害点 (データベース/SAP セントラルサービス)	ミディアム
AZ/ネットワーク障害	低
コアサービスの障害 (DNS/Amazon EFS/API コール)	低/中
破損/過失による削除/悪意のあるアクティビティ/コードデプロイの誤り	低
リージョン障害	非常に低い

キャパシティ予約に関する詳しいガイダンスは、次をよく確認してください。[信頼性]: 提案 10.2.5 - 容量を確保するための戦略を調査する および AWS のホワイトペーパー: Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス) .

AWS を使用して、アカウント内で利用可能なリザーブドインスタンスを確認できます。 AWS Cost Explorer RI レポート .

提案 11.2.6 – 該当する場合は、固有の可用性を持つ AWS のサービスを使用します

いくつかの AWS のサービスは、設計の一部として固有の可用性を備えており、高可用性を実現するために複数のアベイラビリティーゾーンで実行されます。SAP のコンテキストで使用される関連サービスには、以下のようなものがあります。

- AWS サービス: Amazon EFS
- AWS サービス: Elastic Load Balancing
- AWS サービス: Route 53
- AWS サービス: AWS Transit Gateway
- AWS サービス: Amazon S3

また、踏み台ホストや SAPRouter などのステートレスサービスを使用するコンポーネントは、Auto Scaling グループを使用して高可用性を実現できます。

提案 11.2.7 – AWS のベストプラクティスに従って、ネットワーク接続を確保する

使用中の AWS リージョンへのネットワーク接続の回復力を確保するために、以下の AWS ベストプラクティスを 1 つ以上評価すること。

- AWS ドキュメント: AWS Direct Connect Resiliency Toolkit
- AWS ドキュメント: AWS VPN CloudHub

クラスターソリューションがオーバーレイ IP に依存している場合、VPC 外からのアクセスを可能にするために以下を検討してください。

- AWS ドキュメント: SAP on AWS High Availability with Overlay IP Address Routing (オーバーレイ IP アドレスルーティングによる SAP on AWS の高可用性)

ベストプラクティス 11.3 – サービスの可用性を復元するためのアプローチを定義する

可用性の復元は、特定の障害シナリオで、サービスの損失が発生することを前提としています。リストアのアプローチでは、サービスの復元に必要な時間、および可用性目標を達成するために必要なアクションを検討する必要があります。

提案 11.3.1 – EC2 インスタンスのインスタンスの復旧を有効にする

Amazon EC2 インスタンスをモニタリングし、基盤となるハードウェアの障害が原因でインスタンスに障害が発生した場合に自動的にインスタンスを復旧する Amazon CloudWatch アラームを作成できます。このアクションにより、マニュアルによる介入の必要性を取り除くことができますが、スタートアップ、アプリケーションの再起動、ロード時間を、目標復旧時間 (RTO) の計算に含める必要があります。クラスタリングソリューションを使用してハードウェア障害から保護する場合は、インスタンスリカバリがクラスターソリューションと互換性があるかどうかを評価する必要があります。

- AWS ドキュメント: Amazon EC2 インスタンスの復旧

提案 11.3.2 – AMI と Infrastructure as Code を使用して EC2 インスタンスを再構築する戦略を立てる

Infrastructure as Code (IaC) の利点は、プログラムで環境全体を構築および破棄できることです。回復力を考慮した設計であれば、 AWS CloudFormation のテンプレートや AWS Systems Manager のオートメーションにより、数分で環境を実装することができます。 .オートメーションは、高可用性と迅速な復旧を維持するために不可欠です。

戦略の一環として、次の AWS のサービスを評価する必要があります。

- AWS サービス: EC2 Image Builder

- AWS サービス: AWS Launch Wizard for SAP
- AWS サービス: AWS Cloud Development Kit
- SAP on AWS ブログ: DevOps for SAP (SAP 向け DevOps)

提案 11.3.3 – Amazon EBS の障害を理解する

1 つまたは複数の EBS ボリュームに障害が発生した場合、SAP ワークロードの可用性と耐久性に影響を与える可能性があります。そのため、Amazon EBS の障害発生率、通知メカニズム、復旧オプションについて理解しておく必要があります。

- AWS ドキュメント: Amazon EBS の耐久性
- AWS ドキュメント: ボリュームのステータスのモニタリング
- AWS サービス: AWS Personal Health Dashboard
- AWS ドキュメント: Amazon EBS スナップショットを使用したボリュームリカバリ

提案 11.3.4 – AWS Personal Health Dashboard の通知に対応するための戦略を立てる

AWS Personal Health Dashboard からの通知を受け取り、対処するための戦略を立てる必要があります。これには、CloudWatch を使用して Amazon SNS を開始したり、 AWS Health API を介して ITSM ツールと統合したりすることが含まれます 。

提案 11.3.5 – 可用性に影響を与える偶発的または悪意のあるイベントから保護されていることを確認する

SAP ワークロードの可用性に影響を与える可能性のある偶発的または悪意のあるイベントから確実に保護するために、次のアプローチを検討する必要があります。

- 最小特権の原則を 実装し、 AWS Identity and Access Management 内で職務の分離を実施します。
- AWS ナレッジセンターの記事のガイダンスに従ってください。 EC2 インスタンスの偶発的な終了からデータを保護するにはどうすればよいですか?
- Amazon EC2 の ベストプラクティスに従ってください。
- [セキュリティ] のセキュリティガイダンスにも従う必要があります。 ベストプラクティス 8.3 - データ復旧メカニズムを確保して、脅威から保護する。

提案 11.3.6 – AWS の SAP ワークロード以外の依存関係を特定します。

共有サービスやサポートコンポーネントまたはシステムなど、SAP ビジネスプロセスの基本的な依存関係を理解します。例えば、アクティブディレクトリ、DNS、ID プロバイダー、SaaS サービス、オンプレミスシステムなどです。障害発生時の影響と必要な緩和策を評価します。

ベストプラクティス 11.4 – 定期的な回復力テストの実施

ソフトウェアと手順が予測可能な結果をもたらすことを証明するために、重要な障害シナリオに対する回復性を定期的にテストします。アーキテクチャ、ソフトウェア、サポート担当者の変更について評価し、追加テストが必要かどうかを判断します。

提案 11.4.1 – ビジネス要件に基づき、対象範囲内の重要な障害シナリオを定義します。

ビジネス要件に合わせて、テストできる重大な障害シナリオを定義する必要があります。以下は、分析の指針として使用できる障害シナリオの例です。シナリオ、分類、および影響の詳細度や範囲は、要件とアーキテクチャによって異なります。

障害シナリオの例	発生リスクの比較
計画/管理保守	計画
リソースの枯渇または侵害 (高い CPU 使用率/ファイルシステムがいっぱい/メモリ不足/ストレージの問題)	ミディアム
分散ステートレスコンポーネントの障害 (ウェブディスパッチャーなど)	ミディアム
分散ステートフルコンポーネントの障害 (アプリケーションサーバーなど)	ミディアム
単一障害点 (データベース/SAP セントラルサービス)	ミディアム
AZ/ネットワーク障害	低
コアサービスの障害 (DNS/Amazon EFS/API コール)	低/中
破損/過失による削除/悪意のあるアクティビティ/コードデプロイの誤り	低
リージョン障害	非常に低い

提案 11.4.2 – 重大な障害をシミュレートするためのテストケースを定義する。

SAP のワークロードに影響を与える重要な障害シナリオをシミュレートするために、完全なテストセットを定義しておく必要があります。

障害のシナリオによっては、シミュレーションが実際に発生する障害を完全に表現できない場合があることを認識しておく必要があります。例えば、ハードウェアの問題をシミュレートするために、EC2 インスタンスの障害を引き起こすことはできませんが、Nitro ベースのインスタンスでは、インスタンスを再起動させるためにカーネルパニックを発生させることができます。

加えて、 AWS Fault Injection Simulation は、 お客様の AWS リソース内の障害をシミュレートするのに役立つように設計されています。

- AWS ドキュメント: SAP on HANA の高可用性設定ガイド
- AWS ドキュメント: 診断割り込みの送信

提案 11.4.3 – 各テストケースに期待される動作を定義する

テストのベースラインを作成するには、期待される結果のセットを文書化する必要があります。

提案 11.4.4 – 変更の影響を評価するためのアプローチと、その後に必要なテストを定義する

変更が環境に与える影響を評価するためのアプローチと、その変更の一部として必要なテストを定義して、可用性と信頼性に対するアプローチを無効にしないように支援する必要があります。例えば、ソフトウェアのアップグレード、パッチ、パラメータの変更などです。

提案 11.4.5 – テストスケジュールを定義する

初期実装、変更点のテスト、環境の定期的な検証をカバーするテストスケジュールを確実に立ててください。

提案 11.4.6 – テスト結果を確認する

テスト結果に基づいて、テストケース、設定、またはアーキテクチャの改善点を特定します。

提案 11.4.7 – テスト前の状態に戻すために必要なアクティビティを定義する

各テストの一環として、テスト前の状態に戻すために必要なアクティビティを定義する必要があります。これは、各テストケースを他のテストから分離し、テストが本番稼働システムの可用性と信頼性に影響を与えないようにするためです。

ベストプラクティス 11.5 – 障害時の対応を自動化する

障害時の対応を自動化することで、サービスへの影響を最小限に抑えることができます。障害、容量の低下、接続性の喪失に対応するオートメーションを設計します。誤検出を回避するために、明確な調停基準が定義されていることを確認してください。

提案 11.5.1 – 破損のリスクについてオートメーションを評価する

データの破損がリスクとなるコンポーネントの場合、高可用性 (HA) ソリューションで、データレプリケーションの方法、スプリットブレインの回避、接続の安定性、およびアプリケーションの認識が考慮されていることを確認してください。

提案 11.5.2 – オートメーションを開始するヘルスチェックメカニズムを評価する

ヘルスチェックは、誤検出の結果としてオートメーションが開始されないようにするためのコントロール機能を使用して設計する必要があります。

12 – データ回復の計画

SAP ワークロードの論理的なデータ関連の復旧をどのように計画しますか? ビジネス要件から逆算して、ビジネスデータを復旧または再構築するためのアプローチを定義します。回復力をどのように設計したかに応じて、さまざまなシナリオがこのカテゴリに当てはまる可能性があります。少なくとも、バックアップまたは災害対策 (DR) によって、偶発的な削除、論理データの破損、およびマルウェアからユーザーを保護する必要があります。サービスに戻るまでの時間とシステム間の依存関係を考慮して、復旧の決定について慎重に検討します。

ID	優先度	ベストプラクティス
□ BP 12.1	必須	ビジネスデータの一貫した復旧方法を確立する
□ BP 12.2	強く推奨	設定データの復旧方法を確立する
□ BP 12.3	強く推奨	SAP システム全体に対する復旧アプローチを定義する
□ BP 12.4	推奨される	定期的なテストを実施して、復旧手順を検証する

ベストプラクティス 12.1 – ビジネスデータの一貫した復旧方法を確立する

データの損失や破損が発生した場合に、個々のシステムのビジネスデータの一貫性を確保するのに役立つデータ復旧計画を定義します。

提案 12.1.1 - データベースの状態を認識するバックアップメカニズムを使用して、一貫性のあるバックアップを実現

SAP は、データベースベンダーのバックアップ機能 (例えば brtools) と統合し、SAP のトランザクションまたは管理コンソール内で可視性を提供するためのメカニズムを提供します。また、サードパーティーのバックアッププロバイダーまたは AWS Backint Agent for SAP HANA を含むストレージソリューションと統合するオプションがあります 。これらのサポートされているオプションは、データベースの状態を認識し、変更を継続的にキャプチャするか、データベースを静止 (アクティビティの一時停止または削減) しながら、例えば、ストレージスナップショットを使用して一貫したコピーを作成します。

各データベースベンダーの SAP ガイド、および AWS のドキュメントを確認します。

- AWS ドキュメント: AWS Backint Agent for SAP HANA
- SAP ドキュメント: SAP NetWeaver と ABAP プラットフォームのためのガイドファインダー
- SAP on AWS ブログ: How to back up Microsoft SQL Server databases for SAP with VSS Snapshots (VSS スナップショットで SAP 用 Microsoft SQL Server データベースをバックアップする方法)
- AWS ブログ: Amazon EC2 インスタンス上の複数の Amazon EBS ボリューム間でクラッシュ整合性のあるスナップショットを作成する

提案 12.1.2 – ビジネスに不可欠なファイルベースのデータの耐久性と復旧可能性を評価する

データベース内に保存されていないビジネスデータは、別のバックアップ戦略が必要な場合があります。

標準的な SAP NetWeaver システムでは、ファイルベースのインターフェイスファイル、SAP トランスポートディレクトリのコンテンツ、およびバッチログ、ジョブログ、ワークプロセスディレクトリログを含むログが含まれることがよくあります。SAP NetWeaver 以外およびドキュメント管理ソリューションなどのサポートシステムには、評価する必要のある他のファイルベースのビジネスデータが含まれている場合があります。該当する Amazon EFS または Amazon FSx を 評価して、そのようなファイルシステムの可用性と耐久性を向上させます。

ファイルシステムのバックアップは、スナップショット、AWS バックアップ、またはサードパーティーのバックアップソリューションを使用して実行することができます。

ビジネスデータは、バイナリおよび設定データとは別に評価する必要があります。これらのデータは、SAP のダウンロード、再インストール、または Infrastructure as Code を介して再プロビジョニングできる場合があります。以下を参照してください。

- SAP Lens [運用上の優秀性]: 提案 12.2.1 - 設定の作成と変更に対する Infrastructure as Code アプローチを定義する
- SAP Lens [運用上の優秀性]: 提案 12.2.2 - ルートボリュームを含むファイルシステムのコンテンツのバックアップのためのアプローチを定義する

提案 12.1.3 – データベースのバックアップとログの耐久性と場所を評価する

バックアップやログは、ライブデータのレコードですが、それ自体に障害が発生する可能性があります。アクティブなデータコピーに関連するバックアップの場所を評価することによって、障害の影響を最小限に抑える方法を検討してください。以下の点を検討することが重要です。

- バックアップの保護にかかる時間 - 復旧ポイントに影響する
- バックアップの取得/復旧にかかる時間 - 復旧時間に影響する

追加情報については、次のドキュメントをご覧ください。

- AWS ドキュメント: AWS Backint Agent for HANA
- AWS ドキュメント: FSR (スナップショットの高速復元)
- AWS ドキュメント: Amazon S3 レプリケーションオプション

提案 12.1.4 – ポイントインタイムリカバリの要件を評価する

特定の時点に復旧する必要がある場合、それが可能なバックアップ設計になっていますか? バックアップ方法はデータベースを認識し、一貫性のある復旧ポイントにデータベースをロールフォワードできますか? 一貫性を保つために必要なファイルベースの復旧を検討しましたか?

以下の点を考慮してください。

- ログの間隔とログの保護速度
- 増分バックアップまたは差分バックアップによる復旧時間の短縮

- バックアップカタログまたはその他のメカニズムが必要な場合
- データベースやストレージのオプションを使用して、過去にさかのぼることは可能か

提案 12.1.5 – データ消失による復旧のメカニズムを見直す

データの破損、削除、元に戻すことができない誤ったコードのデプロイなど、重大なデータ損失の状況からの復旧が何を意味するかを判断します。データベースまたはストレージベースのレプリケーションを使用する場合のデータ損失の伝播と、バックアップなどのセカンダリ復旧メカニズムを使用した場合の RTO および RPO の影響を評価します。

提案 12.1.6 – データバンカーを作成する

以下のガイダンスに従います。 提案 10.3.7 - バックアップからの復旧が必要になる障害シナリオを判断する 誤って削除したり、悪意あるアクティビティからバックアップを保護したりするためのデータバンカーを作成します。

ベストプラクティス 12.2 – 設定データの復旧方法を確立する

SAP ワークロードを実行するために必要な多くのさまざまなタイプのデータは、SAP データベースには存在しません。これには、オペレーティングシステムの設定、必要な AWS リソースを再作成するためのメタデータ、ファイルシステム内に保存されている SAP アプリケーションで必要なデータなどが含まれます。データ損失の際に、このデータを復旧または再作成するプロセスを定義します。

提案 12.2.1 – 設定の作成と変更に対する Infrastructure as Code アプローチを定義する

個々のインスタンスに直接マニュアルで変更を加えると、システム間の設定に不整合が生じ、状態を復旧するためにバックアップに依存する可能性があります。Infrastructure as Code を使用することにより、SAP システムをデプロイし、アプリケーションコードを管理するのと同じ方法で変更を実装できます。コードパイプラインのような DevOps のメカニズムは、追加のコントロールとテストを提供し、ランドスケープ内での一貫性と再現性を確保するのに役立ちます。

アプローチの一環として、以下の AWS のサービスを評価する必要があります。

- AWS サービス: AWS Launch Wizard for SAP
- AWS サービス: EC2 Image Builder
- AWS サービス: AWS Cloud Development Kit
- SAP on AWS ブログ: DevOps for SAP (SAP 向け DevOps)
- AWS ドキュメント: Introduction to DevOps on AWS (AWS での DevOps 入門)

提案 12.2.2 – ルートボリュームを含むファイルシステムのコンテンツのバックアップのためのアプローチを定義する

オペレーティングシステムのパッケージと設定、アプリケーションのバイナリ、ファイルシステムのコンテンツは、実行中の SAP システムに不可欠ですが、コア SAP データベースのバックアップの一部ではありません。Amazon Machine Images (AMI)、EBS ボリュームスナップショット、その他のバックアップオプションなど、このデータを保護および復旧するメカニズムを評価します。

AMI、スナップショット、ファイルシステムのコピーの頻度と整合性、復旧の詳細度、所要時間時間などを検討する必要があります。

特定のシナリオでは、Infrastructure as Code を使用することで、再作成と復旧との比較に注力し、ビジネス以外のデータのバックアップ要件を減らすことができます。

- SAP ドキュメント: Required File Systems and Directories (必要なファイルシステムとディレクトリ)
- AWS ドキュメント: バックアップとリカバリのソリューションの設計

提案 12.2.3 – マニュアル設定を文書化する

データベースに含まれていない、コードでデプロイ可能な、またはボリュームバックアップを使用して復元できるマニュアルアクティビティは、最悪のシナリオでも SAP システムを再作成できるように記録する必要があります。

ベストプラクティス 12.3 - SAP システム全体の復旧アプローチを定義する

SAP システム全体が複数の SAP システムで構成されている場合、ビジネスの優先順位に基づいて、各システムの復旧順序を定義する詳細なアプローチを作成する必要があります。データの損失がシステムおよびビジネスオペレーション全体の一貫性にどのように影響するかを評価します。

提案 12.3.1 – 復旧の優先順位と計画を含むビジネス継続性計画を作成し、整合性を確保する

[信頼性] で決定されたシステムの分類に基づいて、各 SAP システムを復元する優先順位を決定する事業継続性計画 (BCP) を用意します。 提案 10.1.2 – 障害の影響に基づいてシステムを分類する .計画では、システム間の整合性要件と、復元の優先度に対するマルチテナントデータベースの使用の影響も考慮する必要があります。

提案 12.3.2 – 共有サービスへの依存関係を評価する

復旧方法を定義する際には、SAP ワークロードを実行するための基盤の一部 (DNS、アクティブディレクトリなど)、または復元自体を実行するために必要な共有サービス (バックアップツールなど) を検討します。リスクを評価し、これらの依存関係に関連する前提条件を復元します。

提案 12.3.3 – 災害時のランブックを作成する

事前に定義されたランブックは、災害時に実証済みの一連のステップに従うことを保証し、リスクや重要な活動が見落とされるのを低減します。

ベストプラクティス 12.4 – 復旧手順を検証するための定期的なテストを実施する

ソフトウェアと手順が予測可能な結果をもたらすことを証明し、バックアップファイルの状態と健全性を検証するために、重要な障害シナリオからの復旧を定期的にテストします。追加のテストが必要かどうかを判断するには、アーキテクチャ、ソフトウェア、またはサポート担当者への変更を評価する必要があります。

提案 12.4.1 – 復旧テストの障害シナリオを特定する

[信頼性] に基づいて、復旧が必要となる障害シナリオを定義する必要があります。 提案 10.3.2 – バックアップからの復旧が必要になる障害シナリオを判断する プロセスとツールを検証するために必要なテストの適切なレベルを決定する。

提案 12.4.2 – システム変更が復旧アプローチに与える影響を判断する

変更の影響を評価するアプローチと、そのアプローチが無効にならないことを確認するために必要なその後の復旧テストを定義します。ワークロードの復旧に影響を与える可能性のある変更のタイプの例には、ソフトウェアのアップグレード、パッチ、およびパラメータの変更などがあります。

マネージドサービスパートナーや主要な担当者の変更など、SAP 環境をサポートするために使用される運用モデルに大幅な変更があった場合にも、復旧テストを計画する必要があります。

提案 12.4.3 – 復旧テストプランを定義する

復旧の必要性が生じるような重要な障害シナリオをシミュレートするために、完全なテストセットを定義しておく必要があります。復旧テストは、最初の実装時に計画し、その後は定期的に、あるいは必要に応じて実施する必要があります。

- SAP Lens [運用上の優秀性]: ベストプラクティス 4.3 - 事業継続性計画と障害復旧を定期的にテストする .

パフォーマンス効率

パフォーマンス効率の柱では、コンピューティングリソースを効率的に使ってシステム要件を満たし、需要の変化と技術の進化に合わせて効率性を維持することに重点を置きます。パフォーマンスの最適化は、パフォーマンスをモニタリングおよび測定し、進化する要件に合わせてコンピューティングインフラストラクチャを調整する、データ駆動型のプロセスである必要があります。

13 – 最適なコンピューティングソリューションを選択する

SAP ワークロードに最適なコンピューティングソリューションをどのように選択しますか? SAP ツールや既存のワークロードからのメトリクスを使用して、パフォーマンス要件を評価および推定します。コンピューティング要件を、ワークロードに最適な SAP がサポートするインスタンスにマッピングします。インスタンスタイプの特定のストレージまたはネットワーク要件、および選択した AWS リージョンとアベイラビリティーゾーンでの必要なインスタンスタイプの可用性を検討します。

ID	優先度	ベストプラクティス
□ BP 13.1	必須	パフォーマンス要件を評価または推定する
□ BP 13.2	必須	SAP ワークロードに適した EC2 インスタンスを選択する
□ BP 13.3	強く推奨	システムまたはコンポーネントの自律的なスケーリングを可能にするアーキテクチャを選択する
□ BP 13.4	強く推奨	ネットワークのパフォーマンスとレイテンシーを考慮して、パフォーマンスのインスタンスの場所を選択します

詳細については、以下の情報を参照してください。

- AWS ドキュメント: SAP 向け Amazon EC2 インスタンスタイプ
- SAP ドキュメント: Certified and Supported SAP HANA Hardware (認定およびサポートされている SAP HANA ハードウェア)

- SAP Note: 1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products (AWS 上の SAP アプリケーション: サポートされる DB/OS および Amazon EC2 製品) [SAP ポータルへのアクセス権が必要]
- SAP Note: 1656250 - SAP on AWS: Support prerequisites (サポートの前提条件) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 13.1 – パフォーマンス要件を評価または推定する

将来のハードウェア要件は、既存の SAP システムの容量と使用パターンを調べることで推定できます。SAP は、新規および既存のシステムのハードウェアのサイジングのためのいくつかのツールを提供しています。サイジングの見積もりをさらに検証するために、概念実証 (POC) のデプロイとパフォーマンステストを使用できます。

提案 13.1.1 – ソースハードウェアの SAPS パフォーマンスメトリクスを参照する

SAP によるハードウェアのベンチマークでは、 SAP Application Performance Standard (SAPS) を使用します。これは、SAP 環境におけるシステム構成のパフォーマンスを記述するハードウェアに依存しない測定単位です。オンプレミスサーバーハードウェアの SAPS 値を取得するには、既存のハードウェアベンダーと SAP ベンチマークディレクトリを参照してください。

SAPS に基づくサイジングは、基本的な容量要件に最小限の変更を加える移行に適しています。これは、リフトアンドシフト移行と呼ばれることがよくあります。

提案 13.1.2 – 過去の使用状況の詳細について、SAP EarlyWatch Alert レポートとモニタリングツールを参照する

SAP EarlyWatch Alert レポートは、ピークメモリや CPU 使用率など、SAP アプリケーションの使用率情報を提供します。月末の決算や大量のバッチロードなど、いくつかのピークイベントにまたがるこれらのレポートを総合的に分析することで、システムの使用状況について貴重なインサイトを得ることができます。

EarlyWatch に加え、インフラストラクチャレベルのモニタリングツールは、より詳細に、より深いインサイトを提供することができます。

提案 13.1.3 – SAP HANA サイジングレポートを使用して、コンピューティング要件を見積もる

SAP HANA に移行する場合、ターゲットコンピューティングのサイズを見積もるために、SAP が提供するツールを使用します。これらのツールによって生成される出力には、SAP HANA データベースのハードウェアサイジング要件の詳細が記載されています。

- SAP ドキュメント: HANA プラットフォーム向け SAP HANA 管理ガイド
- AWS ドキュメント: SAP HANA Sizing (SAP HANA のサイジング)
- SAP Note: 1793345 – Sizing for SAP Suite on HANA (SAP Suite on HANA のサイジング) [SAP ポータルへのアクセス権が必要]
- SAP Note: 1872170 – ABAP on HANA sizing report (S/4HANA, Suite on HANA...) (ABAP on HANA のサイジングレポート (S/4HANA、Suite on HANA...)) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2296290 – New Sizing Report for SAP BW/4HANA (SAP BW/4HANA の新しいサイジングレポート) [SAP ポータルへのアクセス権が必要]
- SAP Note: 1958910 - EarlyWatch Alert For HANA Database (HANA データベースの EarlyWatch Alert) [SAP ポータルへのアクセス権が必要]

提案 13.1.4 – グリーンフィールドの実装と機能の変更には SAP Quick Sizer を使用する

SAP Quick Sizer は、SAP の新規実装や変更 (ユーザー数の増加、新機能や新モジュールなど) の際のサイジングに使用できます。このツールは、アプリケーションの要件をハードウェアの仕様に変換するのに役立ちます。最良の結果を得るためには、技術チームと機能チームが協力して、Quick Sizer ツールに値を入力する必要があります。

複雑な実装のサイジングを検証するために、SAP エキスパートサイジングの利用をお勧めします。

SAP のツールやサービスの詳細については、以下を参照してください。

- SAP ドキュメント: SAP: Sizing Benchmarks (サイジングベンチマーク)

提案 13.1.5 – サイジングの精度を高めるために、概念実証のデプロイを使用する

AWS のサービスの柔軟性を活用し、SAP ワークロードの適切なサイジングと、ビジネス需要の変化に応じた拡張を行うことができます。概念実証 (POC) を使用してクラウドへの移行をテストし、パフォーマンス要件を分析します。これにより、コストとパフォーマンスの両面でワークロードを適切に調整できます。

ベストプラクティス 13.2 - SAP のワークロードに適した EC2 インスタンスを選択する。

AWS は SAP と協力し、AWS のサービスが幅広いインスタンスタイプで SAP ソフトウェアの実装と運用に適していることを確認しています。適切なインスタンスを特定するために、関連する SAP ノートやドキュメントからのガイダンスを使用します。EC2 インスタンスファミリーは、SAP ワークロードの実行に適した CPU とメモリの比率、ストレージやネットワークスループットの特性を備

えています。パフォーマンスメトリクス、SAPS の数値、およびコンピューティングの見積もりを使用して、要件を適切なインスタンスタイプにマッピングします。選択したリージョンとアベイラビリティーゾーンで、これらのインスタンスが利用可能であることを確認します。

提案 13.2.1 – サポートされるデータベース、オペレーティングシステム、AWS のサービスに関する SAP のガイダンスに従う

AWS は、SAP 製品のデプロイに利用できるサービスを提供しています。SAP Note: 1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products (AWS 上の SAP アプリケーション: サポートされる DB/OS および Amazon EC2 製品) 現在どの SAP 製品、データベース、オペレーティングシステムの組み合わせと Amazon EC2 インスタンスタイプがサポートされているかを説明しています。

AWS CLI を使用して、特定の AZ 内の個々のインスタンスタイプの可用性を判断し、 インスタンスタイプの拡張性を説明することができます 。

- AWS ドキュメント: SAP 向け Amazon EC2 インスタンスタイプ
- SAP ドキュメント: SAP NetWeaver ベンチマーク

提案 13.2.2 – ハードウェアメトリクスと SAPS を選択の指針にする

SAP がサポートする Amazon EC2 インスタンスファミリーは、それぞれ特定の vCPU とメモリの比率を提供します。パフォーマンスプロファイルを理解するために、お客様の要件に基づいて各インスタンスファミリーを評価する必要があります。現行世代の Amazon EC2 インスタンス (AWS Nitro ベース) は最高のパフォーマンスを提供し、利用可能で、デプロイシナリオの認証を受けている場合は、使用する必要があります。

SAP アプリケーションサーバーは、汎用 (m*) またはメモリ最適化 (r*) インスタンスのいずれかを使用できます。より高い vCPU/メモリ比率が必要な場合は、コンピューティング最適化 (c*) インスタンスの使用を検討してください。AnyDB データベースサーバーの場合、メモリ最適化 (r*) インスタンスは必要なコアとメモリの比率に適していますが、特に CPU 単位のライセンスが適用されるデプロイでは、サイジングを検証するために追加の分析を行う必要があります。メモリ上で動作する SAP HANA データベースの場合、メモリ最適化 (r*、x*、u*) が唯一のオプションとなります。

提案 13.2.3 – SAP HANA のハードウェアディレクトリとメモリ要件を使用して、SAP HANA 用の EC2 インスタンスを選択する

AWS は、SAP HANA ワークロードを実行するための Amazon EC2 インスタンスのサブセットに対する SAP HANA 認定を取得しています。これらのインスタンスの詳細と、サポートされる IaaS ア

プリケーションタイプ (OLAP、OLTP、SAP Business One、Scale-Out) は次に記載されています。Certified and Supported SAP HANA Hardware (認定およびサポートされている SAP HANA ハードウェア) と SAP 向け Amazon EC2 インスタンスタイプ 。

データベースのサイズと実際のワーキングメモリの使用量によって、必要なメモリとインスタンスの選択が決まります。

非本番稼働ワークロードの場合、追加のオプションがあります。以下のブログを参照してください。

- SAP on AWS ブログ: SAP HANA ワークロードの非本稼働環境における小さいサイズの X1e インスタンス

提案 13.2.4 – EC2 インスタンスの機能とスループット特性を意識する

Amazon EC2 インスタンスにはさまざまな機能とスループット特性があり、特に高い I/O とスループットを必要とするワークロードの場合は、ユースケースに基づいて評価する必要があります。これらには、 Elastic Network Adapter (ENA) による ネットワーク機能の強化、I/O パフォーマンス、Amazon EBS の最適化、プレイスメントグループへの適合性などが含まれます。機能の一覧は、こちらをご覧ください。

- AWS ドキュメント: 汎用インスタンス
- AWS ドキュメント: メモリ最適化インスタンス
- AWS ドキュメント: コンピュート最適化インスタンス

ベストプラクティス 13.3 – システムまたはコンポーネントの独立したスケーリングを可能にするアーキテクチャを選択する

SAP システムとコンポーネントは、制約を受けることなく拡張できる柔軟性を備えている必要があります。これは、割り当てられたハードウェア内で、または一部のコンポーネントの水平スケーリングを使用して実現できます。どのアーキテクチャがこのスケーリングを可能にするかを検討し、関連するトレードオフを評価します。

提案 13.3.1 – システム間またはコンポーネント間のパフォーマンスへの影響を検討する

個々のシステムまたはコンポーネントを分離し、コンポーネント間のパフォーマンスへの悪影響を回避します。複数の小さなインスタンスサイズをデプロイすることで、インスタンスの再利用、ワークロードに応じたスケーリング、容量のオンデマンド化などのオプションが提供されます。コスト上の理由からリソースの使用を最適化しようとする場合は、例外があります。詳細については、コストの柱を参照してください。

提案 13.3.2 – 最高のパフォーマンスを得るために容量の柔軟性を考慮する

アプリケーションサーバーなどのコンポーネントのスケーリングが可能なアーキテクチャを選択することで、パフォーマンス要件に合わせて容量を調整し、月末の処理や季節的なピークなどの例外的な需要に合わせてスケールアップすることができます。

ベストプラクティス 13.4 – リージョンとアベイラビリティーゾーンを選択してレイテンシーを最小化する

エンドユーザー、重要なインターフェイス、システム内トラフィックに影響を与える主要なビジネスプロセスのレイテンシーを最小化するリージョンとアベイラビリティーゾーンに SAP インスタンスをデプロイします。

提案 13.4.1 – リージョンとクラウドの接続を選択し、パフォーマンスを最適化する

SAP エンドユーザーと企業のデータセンターへの近さに基づいてリージョンを選択します。データ転送の要件に対応するために、あらゆるクラウド接続オプション (ダイレクト接続や VPN など) のサイズを決定します。

SAP パフォーマンスツールを使用して、ユーザーの応答時間の内訳 (ネットワーク、GUI、アプリケーション、データベースなど) を把握し、レイテンシーの増加によるネットワークのラウンドトリップ時間への変更の影響を評価できます。さまざまな場所にあるシステム間の高周波、低レイテンシーのインターフェイスに焦点を当てることをお勧めします。

レイテンシーの増加が特定のエンドユーザーグループに影響を与える場合は、エンドユーザーコンピューティングサービスとアクセラレータの使用を検討してください。

- AWS ドキュメント: AWS Direct Connect
- AWS ドキュメント: AWS Global Accelerator とは? - AWS Global Accelerator
- SAP on AWS ブログ: Amazon AppStream 2.0 を使った SAP GUI の展開

提案 13.4.2 – システム内レイテンシーに関する SAP のガイドラインに注意する

SAP は、アプリケーションからデータベースへのトラフィックと SAP HANA システムのレプリケーションのための許容可能なネットワークレイテンシーに関するガイダンスを提供しています。

- SAP Note: 1100926 - FAQ: Network performance (よくある質問: ネットワークパフォーマンス) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2543171 - Latency issue between application server and database (アプリケーションサーバーとデータベース間のレイテンシーの問題) [SAP ポータルへのアクセス権が必要]

これらのノートにおけるデータベースとアプリケーションサーバーの接続に関するガイダンスは、単一のデータセンターで稼働するシステムに基づいており、マルチ AZ 配置による回復力の利点は反映されていません。アベイラビリティーゾーンとは、1 つの AWS リージョン内の電源の冗長性、ネットワーク、接続性を備えた 1 つ以上の専用データセンターで、一定の距離 (最低 10km) を隔てて配置されています。

AWS における高可用性 (HA) SAP アーキテクチャは、通常、SAP アプリケーションサーバーインスタンスを含む複数の AZ にインフラストラクチャをデプロイすることになります。データベースを大量に呼び出す SAP トランザクションやバッチジョブがある場合、これらのジョブをデータベースと同じ AZ にある SAP アプリケーションサーバーで実行することをお勧めします。また、エンドユーザーには SAP Logon Groups (トランザクション SMLG)、バックグラウンド処理ジョブには、バッチサーバーグループ (トランザクション SM61) を使用します。これにより、SAP ワークロードのうちレイテンシーの影響を受けやすい部分が、適切なアプリケーションサーバーで実行されるようになります。NIPING などのツールを使ってレイテンシーを測定します。

SAP では、SYNC モードでの SAP HANA 同期レプリケーションをサポートするために、レイテンシーを 1.0ms 以下にすることを推奨しており、これはアベイラビリティーゾーンをまたいで達成することが可能です。

- SAP ドキュメント: SAP HANA Network Requirements (AP HANA ネットワーク要件)

提案 13.4.3 – SAP HANA のスケールアウトにプレイスメントグループを使用する

SAP HANA のスケールアウトデプロイにおいて、ノード間通信の SAP 認定を満たすには、クラスタープレイスメントグループを使用する必要があります。

- AWS ドキュメント: プレイスメントグループ - Amazon Elastic Compute Cloud

14 – 最適なストレージソリューションを選択する

SAP のワークロードに最適なストレージソリューションをどのように選択すればよいのでしょうか? このストレージをどのように設定するかは、システムのパフォーマンスに影響します。AWS はブロック、ファイル、オブジェクトストレージなど幅広いサービスを提供し、お客様の SAP データベース、アプリケーション、バックアップのストレージニーズに応えます。SAP によってベンチマークおよび認定されたガイドラインに従うことをお勧めします。SAP HANA の場合、非常に具体的なガイドラインがあります。その他のデータベースでは、ワークロードに合わせたより多くの分析が必要になります。

ID	優先度	ベストプラクティス
□ BP 14.1	必須	機能に合わせてマウントポイントとボリュームの関連付けを作成する
□ BP 14.2	必須	パフォーマンス要件に合わせた Amazon EBS のタイプを選択し、設定する
□ BP 14.3	推奨される	Amazon EFS と Amazon FSx のパフォーマンスが SAP のユースケースに適しているかどうかを評価する
□ BP 14.4	推奨される	ストレージの代わりとしてメモリを検討する
□ BP 14.5	推奨される	稼働中のシステムへの影響を制限するために、バックアップソリューションとバックアップのパフォーマンスのスケジュールを選択する

ベストプラクティス 14.1 – 機能に合わせてマウントポイントとボリュームの関連付けを作成する

SAP ファイルシステムには、独自のパフォーマンスと共有の要件があります。例えば、データベースのパフォーマンスプロファイルでは、データファイルシステムは多くの読み取り I/O オペレーションをサポートする必要がありますが、ログファイルシステムはスループットに制約される可能性が高くなります。すべてのアプリケーションサーバーがログやトランスポートファイルにアクセスできるように、 `sapmnt` と `trans` などのファイルシステムを共有する必要があります。これらの違いを認識した上で、ファイルシステムとボリュームのマッピングを検討し、パフォーマンスのボトルネックがないこと、アクセス要件が満たされていることを確認する必要があります。

提案 14.1.1 – 各システムの SAP ファイルシステムおよびディレクトリの要件を確認する

SAP のファイルシステムには、システムディレクトリ (ルート、ブート)、実行ファイル、ページまたはスワップ、およびアプリケーション固有の要件が含まれています。それぞれを分析して検討する必要があります。

- 特にルートディレクトリの場合に、ファイルシステムの容量がいっぱい (100% 使用) の場合の影響

- 構築の一貫性 (AMI に含まれているかどうか、またはデプロイパターンに含まれているかどうかを含む)
- 回復力の要件
- 共有の要件
- パフォーマンスプロファイル

コア SAP ファイルシステム要件は SAP ドキュメントに記載されています: SAP Required Filesystems and Directories.これらをベースラインとして使用し、組織固有のその他の要件を含めてください。

提案 14.1.2 – ファイルシステムの機能に合わせて、適切な AWS ストレージサービスをマッピングする

ファイルシステムは、ローカルまたは共有 (NFS/SMB) のいずれかになります。共有ファイルシステムの場合は、Amazon EFS や Amazon FSx などの AWS のサービスの使用を検討してください。これらのサービスは、ホストされている NFS サーバーと比較して信頼性と可用性の利点を提供します。

Amazon EC2 インスタンスストアは、インスタンスのための一時的なブロックレベルのストレージを提供する別のファイルシステムのオプションです。永続性、インスタンスタイプ間での可用性がなく、インスタンスの復旧を使用できないため、これを使用することは推奨しません。

提案 14.1.3 – サポートされているファイルシステムの種類を使用する

SAP がサポートする Linux ディストリビューションは、さまざまなタイプのファイルシステムを推奨しています。それ以降のバージョンでは XFS 上で標準化していますが、OS やデータベースのバージョンによってパフォーマンスや機能に影響がないことを確認し、サポートを検討する必要があります。

- SAP Note: 405827 - Linux: Recommended file systems (Linux: 推奨されるファイルシステム) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2972496 - SAP HANA Filesystem Types (SAP HANA ファイルシステムのタイプ) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 14.2 – パフォーマンス要件に沿った EBS タイプを選択し、設定する

ファイルシステム機能とストレージサービスごとに、ストレージレイアウトのガイドラインとチューニングオプションを評価し、IOPS とスループットパフォーマンスが最適化されていることを確認します。

提案 14.2.1 – EBS ボリュームタイプのストレージ特性およびオプションを評価する

AWS には、SAP ワークロードのさまざまなパフォーマンス要件に対応するため、独自の特性を持つさまざまなボリュームタイプがあります。過去のデータ、またはサイジングを使用して、IOPS とスループットの要件を評価します。パフォーマンス、耐久性、柔軟性、コストなどを考慮し、ボリュームタイプを選択します。

次の gp3# io1 # io2 ######### IOPS とスループットは、ボリュームサイズに依存しません。

次の IOPS ######### ボリュームサイズに合わせます。必要な IOPS とスループットを確保するために、ボリュームのオーバーサイズが必要な場合があります。

- AWS ドキュメント: Amazon EBS ボリュームのタイプ

提案 14.2.2 – LVM ストライピングメカニズムを使用して線形に拡大する

単一の EBS ボリュームでパフォーマンス要件を満たせない場合は、Logical Volume Management (LVM) を使用したストライピングを検討します。例えば、1 つのボリュームが 250 MiB/s のスループット容量を持つ場合、4 つのボリュームにまたがってストライプセットを持つことで 1000 MiB/s のスループットを実現できます。

ボリュームは同じサイズとパフォーマンス特性である必要があります。

SAP HANA のベンチマークテストでは、データボリュームに 256 KB のストライプサイズ、ログボリュームに 64 KB のストライプサイズを使用した場合に、最高のパフォーマンスを得ることができました。

スループット、I/O、添付されたボリューム数などのインスタンス制限に注意してください。

- AWS ドキュメント: EBS ボリュームに LVM 論理ボリュームを作成する
- SAP Note: 2931808 - Usage of Logical Volume Manager (LVM) with SAP HANA (SAP HANA での Logical Volume Manager (LVM) の使用) [SAP ポータルへのアクセス権が必要]

- AWS ドキュメント: オペレーティングシステムとストレージ設定 - SAP HANA on AWS

提案 14.2.3 – SAP HANA のパフォーマンスを確保するために、AWS が提供するストレージのガイドラインに従う

AWS は SAP と連携し、定義されたパフォーマンスベンチマークに従って SAP HANA ワークロード用のストレージを認証しています。AWS が提供する設定は、SAP TDI 5 Storage KPI のフレームワークの中で、パフォーマンス、コスト、耐久性のバランスを取っています。準拠しているストレージのレイアウトは、ドキュメントで詳しく説明されており、起動ウィザードやクイックスタートのデプロイで使用されています。

- AWS ドキュメント: SAP HANA のストレージ設定 - SAP HANA on AWS

AWS の設定から逸脱する場合は、ハードウェアチェックツールを実行することをお勧めします。

- SAP Note: 1943937 - Hardware Configuration Check Tool - Central Note (ハードウェア設定チェックツール - Central Note) [SAP ポータルへのアクセス権が必要]

汎用 SSD とプロビジョンド IOPS SSD のどちらを選ぶかを決める際には、汎用 SSD が SAP KPI を満たしていることを理解することが重要です。SAP HANA などのインメモリデータベースは、データベースのスタートアップ時にディスクからメモリにデータをロードする必要があります。パフォーマンスの高いストレージソリューションと設計は、スタートアップ時間を大幅に改善し、バックアップや復元など、ストレージのパフォーマンスに依存するタスクも高速化することができます。

大規模なシステムや非常に高いアップタイムが要求されるシステムでは、プロビジョンド IOPS が有効な場合があります。最適なデプロイパターンについての詳しいガイダンスは、AWS チームにお問い合わせください。

提案 14.2.4 – 低コストで高性能なローカルバックアップを実現するには、以下を使用します。 **st1** ストレージ

SAP ソリューションでバックアップを保存するためにローカルストレージが必要な場合、低コストで高いスループットを実現する `st1` インスタンスタイプの利用を検討してください。 `st1` は、アクセス頻度が高く、スループット重視のワークロード向けに設計された低コストのブロックストレージタイプです。

SAP HANA の場合は、AWS Backint Agent for SAP HANA の使用を検討し、2 段階バックアップによるパフォーマンスとコストへの影響を回避してください。

ベストプラクティス 14.3 - Amazon EFS と Amazon FSx のパフォーマンスが SAP のユースケースに適しているかどうかを評価する

Amazon EFS (Linux) と Amazon FSx (Windows) は、複数のアベイラビリティーゾーンにまたがることができる、耐久性と可用性の高いファイルシステムを提供します。どちらのソリューションも高いパフォーマンスを発揮するように設計されていますが、ネットワークファイルシステムを選択する際には、アクセスパターンを検討してください。例えば、多くの小さなファイル、高度な並列書き込み、または高い書き込み/読み取り比率は適切でない場合があります。SAP ワークロードの場合、SAP HANA XSA、Java 実行ファイル、大量のジョブログやスプールログが該当する可能性があります。

提案 14.3.1 – スケールとパフォーマンスのオプションを評価する

Amazon EFS には、パフォーマンスに関する 2 つのモード (汎用と最大 I/O) と、2 つの異なるパフォーマンスモード (バーストモードとプロビジョニング) があります。SAP アプリケーションの場合、通常、汎用パフォーマンスモードで十分な I/O が得られます。ファイルシステムのデータ量がスループット要求に対して少ない場合など、プロビジョニングスループットを検討する必要のあるシナリオがあるかもしれません。

- AWS ドキュメント: Amazon Elastic File System (EFS) | よくある質問 - スケールとパフォーマンス
- AWS ドキュメント: Amazon FSx for Windows ファイルサーバーの特徴 | スケールとパフォーマンス

提案 14.3.2 - 短期的な必要性に応じて、一時的なプロビジョニングを検討する

移行や 1 回限りのアクティビティに関連するユースケースでは、イベントの期間中、パフォーマンス特性を調整できる一時ファイルシステムが有効の場合があります。

ベストプラクティス 14.4 – ストレージの代わりにメモリを検討する

データベースやアプリケーションレイヤーでサポートされるシナリオにメモリを使用することによるパフォーマンス上の利点を検討します。SAP HANA はデフォルトでメモリを使用しますが、ロードを最適化したり、静的データをオフロードしたりするオプションが有効な場合があります。リレーショナルデータベースはキャッシングを利用する必要があり、アプリケーションサーバーはスワップが要件であるかどうかを検討する必要があります。

提案 14.4.1 – SAP HANA のメモリ使用量を最適化する

SAP HANA のメモリ要件とオペレーティングシステムのメモリ指標との相関関係を把握し、メモリのボトルネックがパフォーマンスに影響を与えないようにします。

- SAP ドキュメント: SAP HANA Memory Usage and the Operating System (SAP HANA のメモリ使用量とオペレーティングシステム)
- SAP Note: 1999997 - FAQ: SAP HANA Memory (よくある質問: SAP HANA メモリ) [SAP ポータルへのアクセス権が必要]

ホストの再起動を伴わないシナリオでデータベースのスタートアップパフォーマンスを向上させるには、SAP HANA Fast Restart オプションの使用を検討します。SAP HANA Fast Restart オプションは、RAM の一部を一時ファイルシステム (`tempfs`) として専用化し、オペレーティングシステムによって持続的メモリ (オペレーティングシステムの再起動まで) として扱われ、列ストアメイン部分をその `tempfs` に配置することができ、インデックスサーバーの再起動またはクラッシュまでその状態を維持します。そのため、ストレージからの再読み込み (I/O を使用) は必要ありません。

- SAP ドキュメント: HANA Fast Restart ドキュメント

提案 14.4.2 – リレーショナルデータベースでデータベースキャッシュを利用する

高い読み取り IOP を必要とするリレーショナルデータベースでは、データベースキャッシングにより、スループットを大幅に向上させ、データ検索のレイテンシーを低減することができます。キャッシュは、データベースの隣接データアクセスレイヤーとして機能し、読み取りパフォーマンスを向上させます。

以下のドキュメントでは、キャッシュの使用例に関する情報を提供していますが、この詳細のほとんどは AWS データベースに関連しているため、リレーショナルデータベース構成に固有の情報については、SAP Notes を参照してください。

- AWS ドキュメント: キャッシュ (以下が含まれます データベースのキャッシング)

提案 14.4.3 – SAP アプリケーションのスワップ領域の必要性を評価する

物理メモリリソースが枯渇すると、SAP はスワップを使用して非アクティブなページをディスクベースの専用ストレージエリアに移動させます。スワップはメモリ不足によるアプリケーションのクラッシュを防ぐことができますが、スワップが頻繁に使用されないように設定パラメータとメモリサイジングを適用することをお勧めします。

スワップの使用が予想される場合、割り当てられたボリュームの特性を評価し、さらなるパフォーマンスの問題を回避してください。スワップは、SAP アプリケーションでホストの物理メモリが不足した場合に、メモリ不足の状況を回避することができます。

- SAP Note: 153641 - Swap space requirement for R/3 64-bit kernel (R/3 64 ビットカーネルに必要なスワップ領域) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2999334 - SWAP Utilization (SWAP 使用率) (HANA 関連) [SAP ポータルアクセスが必要]
- SAP Note: 2488097 - FAQ: Memory usage for the ABAP Server on Windows (よくある質問: Windows 版 ABAP サーバーのメモリ使用量) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 14.5 – 適切なバックアップソリューションとスケジュールを選択する

バックアップの方法によっては、ストレージの読み取りと書き込みオペレーションの両方が大幅に増加する可能性があり、アプリケーションのパフォーマンスに悪影響を与える可能性があります。これは、ボリュームが大きく、期間が長いデータベースレベルのバックアップに特に当てはまります。

提案 14.5.1 – 適切なバックアップウィンドウを決定する

ビジネス要件に沿ったバックアップオペレーションを実行するために、最も適切なウィンドウを定義します。夜間バッチスケジュールや許容ランタイムなど、重要な依存関係を検討します。

提案 14.5.2 – バックアップのパフォーマンスへの影響を最小限に抑えるためのオプションを検討する

ストレージやネットワークの制約を分析し、バックアップの影響を最小化するためのオプションを評価します。これには、データベースまたはストレージレベルでのデルタチェンジバックアップを使用することで、期間を短縮することが含まれる場合があります。信頼性の柱を参照して、バックアップの一貫性や全体の復元時間に悪影響を与えないようにしてください。

- SAP Lens [信頼性]: ベストプラクティス 12.1 - ビジネスデータの一貫した復旧方法を確立する

15 – オペレーティングシステム、データベース、SAP アプリケーションのチューニングオプションを評価する

SAP システムのパフォーマンスに対するさまざまなチューニングオプションの効果をどのように理解し、評価するのでしょうか? SAP ソフトウェア製品、サポートされるオペレーティングシステム

とデータベース、およびバージョンの組み合わせによって、推奨されるパフォーマンスが大きく異なるため、1 つのドキュメントで優れたパフォーマンスのためのレコメンデーションを網羅することはできません。このことを念頭に置き、以下のガイダンスは SAP のユースケースの大部分に適用できるはずであり、該当する場合は特定の重点分野を呼び出します。

ID	優先度	ベストプラクティス
□ BP 15.1	必須	SAP のパフォーマンスに関するオペレーティングシステムのガイドラインに従う
□ BP 15.2	強く推奨	ハードウェアの選択に合わせてデータベースのパラメータを変更する
□ BP 15.3	強く推奨	ハードウェアの選択に合わせて SAP のパラメータを変更する
□ BP 15.4	推奨される	回復と可用性のためにチューニングする

ベストプラクティス 15.1 – SAP のパフォーマンスに関するオペレーティングシステムのガイドラインに従う

SAP は、デプロイする SAP ソフトウェアがサポートする各オペレーティングシステムに最適なパフォーマンスを実現するためのチューニング方法について、具体的なガイダンスを提供しています。関連するチューニングパラメータを理解し、オペレーティングシステム固有のオプションを利用して、パフォーマンスチューニングをより簡単かつダイナミックに行うために、デプロイするオペレーティングシステムに関するすべての SAP ドキュメントを必ずお読みください。

提案 15.1.1 – インストール、バージョンアップ、インフラストラクチャの変更に先立ち、オペレーティングシステム関連の SAP Notes を確認する

オペレーティングシステムを構築または更新する場合 (オートメーションまたはマニュアル)、SAP ソフトウェアとオペレーティングシステムのバージョンの組み合わせに固有の適切なパフォーマンス設定が適用されていることを確認します。

提案 15.1.2 – オペレーティングシステムベンダー提供の SAP チューニングを評価する

Red Hat と SUSE は、SAP の実行に最適化されたツールや設定を含むイメージとリポジトリを提供しています。これらは、AWS Marketplace や bring-your-own-subscription (BYOS) モデルで提供されています。

ベンダーは、自社のオペレーティングシステムが SAP アプリケーションに最適化されていることを確認するために投資しています。ベンダー提供の `saptune` などのチューニングツールや、Red Hat Enterprise Linux 用の (Ansible) システムロールを使用すると、パフォーマンスチューニングのための既知のベースラインを定義するのに役立ちます。特定の SAP ワークロードに最適なオペレーティングシステムのチューニングを妨げることなく、これらのツールにより、最も一般的な要件の調査、計算、適用に関連する労力を軽減することができます。また、 `tuned` デーモンに関連付けられた設定は、CPU カウントや使用可能なメモリなど、システムから収集した情報を使用して動的に調整することもできます。

オペレーティングシステム	Guidance
SUSE Linux Enterprise Server (SLES)	SAP Note: 1275776 - Linux: Preparing SLES for SAP environments (Linux: SAP 環境用 SLES の準備) [SAP ポータルへのアクセス権が必要]
Red Hat Enterprise Linux	SAP Note: 2777782 - SAP HANA DB: Recommended OS Settings for RHEL 8 (SAP HANA DB: RHEL 8 で推奨される OS 設定) [SAP ポータルへのアクセス権が必要]
Microsoft Windows	(ガイダンスについては SAP またはベンダーのドキュメントを参照)
Oracle Enterprise Linux	SAP Note: 2478541 - Operating System Requirements for Oracle Database (Oracle Database のオペレーティングシステム要件) [SAP ポータルへのアクセス権が必要]

提案 15.1.3 – オペレーティングシステムに関連するネットワークパラメータを適用する

SAP システムのパフォーマンスは、特に SAP HANA のスケールアウトデータベースの設計や、システム環境における異なるアプリケーションサーバーインスタンスとデータベースインスタンス間の通信において、ネットワークの誤設定によって深刻な影響を受ける可能性があります。AWS では、インスタンスの最大ネットワークスループットはインスタンスファミリーやサイズによって決まるケースが多いのですが、OS レベルや SAP ソフトウェア自体のネットワーク設定のチューニングが影響を与えることがあります。

以下の AWS と SAP のレコメンデーションを参照してください。

- AWS ドキュメント: 同じ Amazon VPC 内で Amazon EC2 Linux インスタンス間のネットワークスループットをベンチマーク
- AWS ドキュメント: Elastic Network Adapter – Amazon EC2 向けの高性能パフォーマンスネットワークインターフェイス
- AWS ドキュメント: クラスタープレイスメントグループ
- SAP Note: 2198693 - Key Monitoring Metrics for SAP on Amazon Web Services (AWS) (アマゾンウェブ サービス (AWS) 上の SAP の主なモニタリングメトリクス) [SAP ポータルへのアクセス権が必要]
- SAP Note: 1612283 - Hardware Configuration Standards and Guidance (ハードウェアの設定に関する標準とガイダンス) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2081065 - Troubleshooting SAP HANA Network (SAP HANA ネットワークのトラブルシューティング) [SAP ポータルへのアクセス権が必要]
- SAP Note: 1100926 - FAQ: Network performance (よくある質問: ネットワークパフォーマンス) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 15.2 – ハードウェアの選択に合わせてデータベースパラメータを変更する

SAP は、基礎となるデータベースの特定のパラメータを変更することによって SAP システムのパフォーマンスを最適化するための具体的なガイダンスを提供しています。これらのパラメータは、データベースのタイプによって異なり、分析型アプリケーションをサポートしているか、トランザクション型アプリケーションをサポートしているかによって異なる場合があります。

提案 15.2.1 – SAP HANA 固有のチューニングパラメータを確認する (該当する場合)。

オペレーティングシステムと SAP HANA データベースのパラメータは、パフォーマンスに大きな影響を与える可能性があります。オペレーティングシステムとストレージの設定については、SAP on AWS のレコメンデーションに従ってください。

- AWS ドキュメント: SAP HANA on AWS – オペレーティングシステムとストレージ設定

メモリ割り当てを含む SAP HANA パラメータに関するガイダンスについては、SAP のノートやドキュメントを参照してください。

- SAP Note: 2000000 - FAQ: SAP HANA Performance Optimization (よくある質問: SAP HANA パフォーマンスの最適化) [SAP ポータルへのアクセス権が必要]
- SAP ドキュメント: HANA パラメータ: global_allocation_limit
- SAP Note: 1999997 - FAQ: SAP HANA Memory (よくある質問: SAP HANA メモリ) [SAP ポータルへのアクセス権が必要]
- SAP Note: 2926166 - How to limit the overall SAP HANA memory allocation (SAP HANA 全体のメモリ割り当てを制限する方法) [SAP ポータルへのアクセス権が必要]

提案 15.2.2 – SAP HANA 以外のデータベースのチューニングガイドを見直す

SAP システムの基礎となるデータベースにかかわらず、システムのパフォーマンスは、データベースのチューニングの方法に依存する部分があります。各データベースには、利用可能なコンピューティング、メモリ、ディスクストレージに基づくチューニングのための具体的なレコメンデーションがあります。一部のデータベースパラメータは、使用する EC2 インスタンスサイズに依存します。例えば、Oracle データベースの場合、利用可能な物理メモリによって `db_cache_size` が制限されます。

お使いのデータベースに関連する情報については、以下を参照してください。

データベース	Guidance
SAP ASE	SAP Note: 2473646 - Performance and Tuning information for ASE -SAP ASE (ASE のパフォーマンスとチューニング情報 - SAP ASE) [SAP ポータルへのアクセス権が必要]
IBM Db2	SAP Note: 2751102 – DB6: DB2 11.5 Standard Parameter Settings (DB6: DB2 11.5 標準パラメータ設定) [SAP ポータルへのアクセス権が必要]
Oracle	SAP Note: 2470718 – Oracle Database Parameter 12.2 / 18c / 19c (Oracle データベースパラメータ 12.2/18c/19c) [SAP ポータルへのアクセス権が必要]
Microsoft SQL Server	SAP Note: 2779607 – Configuration Parameters for SQL Server 2019 (SQL Server 2019 の設定パラメータ) [SAP ポータルアクセスが必要]、SAP Note: 2729848 – SAP Installation Media and SQL4SAP for

データベース	Guidance
	SQL Server 2019 (SAP インストールメディアと SQL4SAP for SQL Server 2019) [SAP ポータルへのアクセス権が必要]
SAP MaxDB	SAP Note: 819641 – FAQ: SAP MaxDB performance (よくある質問: SAP MaxDB パフォーマンス) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 15.3 – ハードウェアの選択に合わせて SAP パラメータを変更する

SAP アプリケーションのパラメータをチューニングすることで、アプリケーションのパフォーマンスを向上させることができます。これらのパラメータは、多くの場合、基盤となるハードウェア設定とオペレーティングシステムのタイプに依存します。

提案 15.3.1 – SAP が **PHYS_MEMSIZE ######################**

最近の SAP ソフトウェアのバージョンでは、カーネルリリース 7.40 以降を使用して、特定のパラメータのセルフチューニングが可能であり、推奨されています。例えば、多くのパラメータは、インスタンスで利用可能なメインメモリ (PHYS_MEMSIZE) に関連する数式で得られます。これにより、SAP ソフトウェアの基盤となる EC2 インスタンスのサイズを変更する際に、変化するパフォーマンス要件に合わせてメモリパラメータを自動的にチューニングできます。

- SAP ドキュメント: SAP Memory Management: Parameter Reference (SAP メモリ管理: パラメータリファレンス)
- SAP Note: 2085980 – New features in memory management as of Kernel Release 7.40 (Kernel Release 7.40 のメモリ管理に関する新機能) [SAP ポータルへのアクセス権が必要]

提案 15.3.2 – SAP のスワップ領域と最大使用メモリを確認する

SAP on AWS を実行する場合、ディスク上のスワップ領域を過剰に使用すると、Amazon EBS の I/O クレジット枯渇を引き起こし、パフォーマンス低下につながる可能性があります。AWS で利用可能なさまざまな EBS ストレージオプション を評価し、パフォーマンスニーズに合わせてスワップ領域を設定します。AWS

- SAP Note: 1597355 - Swap-space recommendation for Linux (Linux におけるスワップ領域を推奨する) [SAP ポータルへのアクセス権が必要]
- SAP ドキュメント: Swap Space Requirements (スワップ領域の要件)

ベストプラクティス 15.4 – 復旧と可用性のオプションのためのパフォーマンスチューニングを検討する

Well-Architected Reliability と運用上の優秀性の両方の柱に沿って、選択した復旧と回復力の要件に応じた SAP システムのチューニングを評価し、パフォーマンスへの影響を最小限に抑える必要があります。バックアップ時のシステムパフォーマンス、選択したデータベースのクラスタリングオプション (例えば、同期と非同期の SAP HANA システムレプリケーション)、複数の SAP アプリケーションサーバーインスタンスへの負荷分散などの項目を検討します。

提案 15.4.1 – バックアップと復旧ソリューションのパフォーマンスに関するレコメンデーションを検討する

サポートされている各データベースには、バックアップと復旧オペレーションのパフォーマンスを最適化するためのさまざまなレコメンデーションがあり、これらは多くの場合、サードパーティー製品を含むバックアップと復元を管理するために選択したソフトウェアソリューションと連携して機能します。AWS の例としては、EBS ボリュームの最大 IOPS やスループットの設定、AWS Backint Agent for SAP HANA を使用する際の同時実行パラメータの設定などがあります。

一般に、EC2 インスタンスとバックアップ対象のストレージ (EBS ボリューム、S3 バケット、EFS ファイルシステムなど) 間のスループットを向上させるためのガイドラインに従うことで、バックアップと復旧のパフォーマンスを向上させることができます。例えば、バックアップのリポジトリとして Amazon S3 を使用する場合、Amazon S3 の AWS Command Line Interface (CLI) を使用すると、最大同時リクエスト数やマルチパートのチャンクサイズなどの 設定パラメータを 介してパフォーマンスを向上させることができます。

詳細については、以下を参照してください。

- AWS ドキュメント: AWS Backint Agent for SAP HANA
- AWS ドキュメント: SAP NetWeaver on AWS – Backup and Recovery (バックアップと復旧)
- SAP on AWS ブログ: Build for availability and reliability (可用性と信頼性を高めるために構築する)

データベース	Guidance
SAP HANA	• AWS ドキュメント: SAP HANA on AWS – Storage Configuration for SAP HANA (SAP HANA のストレージ設定) [SAP ポータルへのアクセス権が必要]

データベース	Guidance
	• SAP Note: 1842096 - HANA Backup & Restore Performance (HANA バックアップと復元パフォーマンス) [SAP ポータルへのアクセス権が必要] • SAP Note: 2945518 - Performance issues encountered on HANA when a data backup is running (データバックアップ実行時に HANA で発生するパフォーマンスの問題) [SAP ポータルへのアクセス権が必要]
SAP ASE	(ガイダンスについては SAP またはベンダーのドキュメントを参照)
IBM Db2	(ガイダンスについては SAP またはベンダーのドキュメントを参照)
Oracle	SAP Note: 2084077 - How to plan backup cycle for Oracle database (Oracle データベースのバックアップサイクルを計画する方法) [SAP ポータルへのアクセス権が必要]
Microsoft SQL Server	SAP Note: 1420452 - FAQ: Restore and recovery with MS SQL Server (よくある質問: MS SQL Server による復元と復旧) [SAP ポータルへのアクセス権が必要]
SAP MaxDB	SAP Note: 1377148 - FAQ: SAP MaxDB backup / recovery (よくある質問: SAP MaxDB バックアップ/復旧) [SAP ポータルへのアクセス権が必要]

提案 15.4.2 – クラスタリングパラメータの設定を確認する

SAP HANA やその他のデータベースのクラスタリングオプションは、多くの場合、プライマリインスタンスとフェイルオーバーインスタンス間のクラスター内の確認済み接続 (つまり、ハートビート) に依存しています。SAP 管理者は、システム内で発生するアクションの速度と、通信の中断の検出漏れがある場合に発生する可能性のあるフェイルオーバーの副作用のバランスを取る必要があります。タイムアウトパラメータと関連する設定については、レコメンデーションに従ってください。

- AWS ドキュメント: SAP HANA on AWS: High Availability Configuration Guide for SLES and RHEL (SAP HANA on AWS: SLES および RHEL の高可用性設定ガイド)
- AWS ドキュメント: SAP HANA on AWS Operations Guide: Networking (SAP HANA on AWS オペレーションガイド: ネットワーク)

- AWS ドキュメント: SAP on AWS – IBM Db2 HADR with Pacemaker
- SAP Note: 1612105 - DB6: FAQ on Db2 High Availability Disaster Recovery (HADR) (DB6: Db2 High Availability Disaster Recovery (HADR) についてのよくある質問) [SAP ポータルへのアクセス権が必要]
- オペレーティングシステム固有のドキュメント: SUSE Linux SAP HSR スケールアップパフォーマンス最適化シナリオ
- オペレーティングシステム固有のドキュメント: Automated SAP HANA ペースメーカークラスターのスケールアップにおけるシステムレプリケーション

16 – 継続的なパフォーマンスと最適化のオプションを理解する

パフォーマンスの変化や最適化の機会を測定するために、どのようなプロセスや手順を導入していますか? 過去のモニタリングデータからアプリケーションのパフォーマンス要件をベースライン化し、逸脱が発生した場合にシステム管理者に通知するアラートを設定します。システム管理者がマニュアルまたは自動化されたアクションでそのような問題を修正するための手順を用意します。

ID	優先度	ベストプラクティス
□ BP 16.1	必須	パフォーマンスを評価するためのデータがある
□ BP 16.2	必須	ベースラインパフォーマンスの要件の設定
□ BP 16.3	強く推奨	データを活用してパフォーマンストレンドを把握する
□ BP 16.4	強く推奨	パフォーマンスに関する問題を特定し、分類する
□ BP 16.5	強く推奨	パフォーマンス要求に応じて動的に拡張する
□ BP 16.6	推奨される	分析のための生産負荷シミュレーションのメカニズムを開発する

ID	優先度	ベストプラクティス
□ BP 16.7	推奨される	パフォーマンスデータに基づいてサイジングと設定を継続的に最適化する

ベストプラクティス 16.1 – パフォーマンスを評価するデータを持つ

SAP システムのパフォーマンスを評価し、パフォーマンスが最適でない場合に対処するためには、リソースのモニタリングに関する Well-Architected Framework Performance Excellence ガイドラインに記載されているように、コンピューティング、メモリ、ストレージ、ネットワークに関するモニタリングデータを収集する必要があります。Well-Architected Framework 運用上の優秀性の柱に説明されているように、システムの現状を理解し、重要なパフォーマンス指標を導入し、診断のためにタイムリーにメトリクスを収集することは、パフォーマンスの問題を調査するために非常に重要です。

- Well-Architected Framework [パフォーマンス効率]: リソースをモニタリングして、それらが期待通りに機能していることを確認する
- Well-Architected Framework [運用上の優秀性]: ワークロードの状態の把握

提案 16.1.1 – パフォーマンスメトリクスに関連するデータを収集し、保存する

関連する SAP モニタリングデータを収集して表示するには、AWS Data Provider for SAP をインストールして設定し、SAP ワークロードをサポートする選択したモニタリングツールでメトリクスを設定する必要があります。モニタリングの詳細とその他のレコメンデーションは、運用上の優秀性の柱に記載されています。

- AWS ドキュメント: AWS Data Provider for SAP (SAP 向け AWS データプロバイダー)
- SAP Lens [運用上の優秀性]: ベストプラクティス 1.1 - SAP on AWS をモニタリングするための前提条件を実装する
- SAP Lens [運用上の優秀性]: ベストプラクティス 1.2 - SAP のインフラストラクチャモニタリングを実施する
- SAP Lens [運用上の優秀性]: ベストプラクティス 1.3 - SAP の個別アプリケーションモニタリングの実装

ベストプラクティス 16.2 – ベースラインパフォーマンスの要件を設定する

すべての SAP アプリケーションには、固有のパフォーマンス要件があります。過去のモニタリングデータを使用することで、SAP 管理チームはこれらのアプリケーションのベースラインパフォーマンスを理解し、パフォーマンスの変化の程度を特定し、理解できます。意図しない CPU の急上昇、ストレージのスループット低下、メモリ消費量の増加、より複雑なパフォーマンスの低下などの異常を検出するために、関連するアラートを設定できます。このモニタリングデータを使用して、パフォーマンスをさらに微調整できます。

提案 16.2.1 – SAP 固有の KPI を反映したデータを収集し、評価する

この提案は、Well-Architected Framework パフォーマンス効率の柱の リソースモニタリングに関する議論における追加提案と密接に連携しています。

この一般的なガイダンスに加え、SAP 特有の KPI として、ダイアログの応答時間、バッファスワップ、使用メモリなどがあります。これらの KPI は、実行中の SAP ソフトウェアのタイプとバージョンによって異なる場合があります。KPI とモニタリングに関するレコメンデーションの詳細については、このドキュメントの運用上の優秀性の柱に記載されています。

- SAP Lens [運用上の優秀性]: ベストプラクティス 1.2 - SAP のインフラストラクチャモニタリングを実施する
- SAP Lens [運用上の優秀性]: ベストプラクティス 1.3 - SAP の個別アプリケーションモニタリングの実装

ベストプラクティス 16.3 – データを使用してパフォーマンスの傾向を特定する

パフォーマンスのベースラインを設定した後、システム管理者は、KPI が望ましい基準値内で安定しているかどうかを確認するために、時間の経過とともに傾向をモニタリングする必要があります。パフォーマンスデータから KPI の許容できない値への傾向が示された場合、システム管理者はパフォーマンスへの影響を回避または軽減するための措置を講じることができます。

提案 16.3.1 – SAP システムのパフォーマンスに関する定期的なレビューを実施する

システム管理者は、KPI を定期的にレビューすることで、パフォーマンス関連データの傾向を把握し、どのアラートが最も有効かを判断することができます。これらのアラートを使用して、傾向が続く場合は通知を自動化し、潜在的なパフォーマンスの問題に対処するための自動修復手段を講じることができます (例えば、パフォーマンス指標に対応して SAP パラメータを動的に変更するなど)。KPI と関連する傾向の例は、SAP EarlyWatch Alert レポートに記載されており、場合によって

は、有用なメトリクスを追加してカスタマイズすることもできます。SAP サービスレベルレポートは、SAP ワークロードのサービスレベルアグリーメント (SLA) を締結している場合にも有用です。

- SAP ドキュメント: サービスレベルレポート
- SAP Note: 1040343 - SAP EarlyWatch Alert [SAP ポータルへのアクセス権が必要]
- SAP Note: 1829914 - Customize EWA Reports (Customize EWA レポートをカスタマイズする) [SAP ポータルへのアクセス権が必要]

提案 16.3.2 – 傾向を把握するために過去のデータを保持する

システム動作の傾向を把握するために、パフォーマンスデータおよび関連するログを所定の期間保持する必要があります。SAP システムのパフォーマンスチューニングは、パフォーマンスの傾向または周期的なパフォーマンスイベントを構成するものを理解するために、数日、数週間、および数か月の履歴期間を振り返る機能に依存します。パフォーマンスへの影響を観察するためにデータの保持が必要な一般的なイベントには、以下のようなものがあります。

- 月末および年末の財務処理
- ビジネスのマイルストーンにおけるレポート要件の増加 (例えば、半期に一度の大規模なセールスキックオフの後など)
- ビジネス内の大規模な新しい SAP ユーザー人口のオンボーディング
- インフラストラクチャのサイジング、データベースパッチ、オペレーティングシステムのバージョンアップ、SAP ソフトウェアのアップグレードなど、テクノロジーの変更。

ベストプラクティス 16.4 – パフォーマンスに関する問題を特定し、分類する

主要なメトリクスがパフォーマンスの低下を示している場合、根本的な原因を改善するためのプロセスを整備します。オートメーション (ダイナミックスケーリングに関する以下のベストプラクティスを参照) を使用すれば、マニュアルによる介入の必要性を減らすことができますが、それができない場合、管理者向けの自動アラートプロセスを用意することが不可欠となります。

提案 16.4.1 – パフォーマンスアラートを適切に設定する

モニタリングとアラートについては、Well-Architected Framework パフォーマンス効率の柱で説明したガイドラインに従い、SAP アラート機能が追加機能を提供する場合はそれを利用します。その他の詳細は [運用上の優秀性] でもご覧いただけます 1 - 状態の理解と反応ができるように SAP ワークロードを設計する .

- Well-Architected Framework [パフォーマンス効率]: モニタリング

- SAP ドキュメント: SAP NetWeaver Alert Monitor

提案 16.4.2 – パフォーマンスインシデントの自動修復

パフォーマンスインシデントの管理には、Well-Architected Framework 運用上の優秀性の柱で詳述されているオペレーションに関するベストプラクティスが含まれますが、潜在的なパフォーマンス障害を事前に検出し、自動修復することによって、パフォーマンス問題の深刻化を防ぎ、エンドユーザーエクスペリエンスを改善することができます。パフォーマンス問題を軽減するための自動化されたプロセスが使用できない場合、運用チームがパフォーマンス問題にどのように対応すべきかの詳細なランブックを用意しておけば、パフォーマンスインシデントに早く対応できます。

- SAP Lens [運用上の優秀性]: ベストプラクティス 1.8 自動化された応答と回復技術を使用してモニタリングアラートに対応する
- Well-Architected Framework [運用上の優秀性]: ベストプラクティス: 運用する

ベストプラクティス 16.5 – パフォーマンス要求に対して拡張する

AWS でワークロードを運用する最大のメリットは、ユースケースに必要なパフォーマンスに合わせて、コンピューティング性能の増減やストレージのパフォーマンス特性の変更が可能なことです。SAP ワークロードの場合、パフォーマンスのボトルネックを回避するために、必要に応じて動的スケーリングを使用します。SAP HANA データベースクラスターのスケールアウトなど、動的スケーリングが不可能なシナリオでは、マニュアルによるデプロイプロセスを使用します。

提案 16.5.1 – SAP ワークロードを受動的に拡張する

ワークロードのパフォーマンス要件の動的な変化に対応し、SAP リソースを必要に応じて拡張できます。可能な限り、スケールインまたはスケールアウトにはオートメーションを使用しますが、それができない場合 (データベースインスタンスのスケールアップなど) には、マニュアルで行うプロセスを用意してください。考慮すべき点:

- 需要に応じてアプリケーションサーバーの容量を追加または削除したり、インスタンスサイズを変更したりする
- プログラムによる仮想リソースの再配布のために SAP パラメータを変更する
- ストレージタイプの変更 (例えば、Amazon EBS の `gp3` を `io2` へ、またはその逆など、AWS 内で) 行うことで、ストレージのパフォーマンスを最適化します。

提案 16.5.2 – 予測可能な SAP ワークロードのスケーリングをスケジュールする

オートメーションまたはマニュアルのいずれであっても、予測可能なパフォーマンスパターンに基づいて SAP ワークロードをスケーリングすることが推奨されます。例えば、SAP ECC システムで月末の財務処理により、アプリケーションサーバーのインスタンスの処理要件が 20% 増加することが予測される場合、システム管理者は、アプリケーションサーバーの数やサイズを事前に増やし、使用量が予測どおりに減少したらインスタンス数をスケールインさせることができます。

ベストプラクティス 16.6 – 分析のための生産負荷シミュレーションのメカニズムを開発する

テストシステム内に本番稼働データのクローンを持つことで、システム管理者は本番稼働の SAP ワークロードをシミュレーションし、ストレスやボリュームテストなどの重要なパフォーマンステストを実施することができます。このタイプのテストは、潜在的なパフォーマンスのボトルネックを特定し、本番稼働環境でのパフォーマンス問題の発生を防止するのに役立ちます。

提案 16.6.1 – SAP システムにおける自動ストレステストとボリュームテストを実施する

AWS で実行する場合、本番稼働データをテスト環境にコピーするのは比較的簡単です (例えば、本番稼働環境から EBS スナップショットを使用して 新しいテストインスタンスを作成する)、ただし、マニュアルまたは自動のコピー後のステップを正しく実行するように注意する必要があります。コピー後のステップには、トランザクション BDLS による論理システム名の変更、機密本番稼働データのスクランブルや削除、関連するテストシステムとの統合設定などがあります。また、必要に応じてインスタンスのプロビジョニング、設定、シャットダウンが可能なため、分離されたパフォーマンステストシステムを永続的に維持する必要がないことも利点の一つです。

テストシステムへの負荷のかけ方はさまざまです。

- AWS では、 Distributed Load Testing ソリューションが自動負荷テストに役立つかもしれません
- eCATT (Extended Computer Aided Test Tool) による SAP ソフトウェアでの スクリプトの作成と自動化
- サードパーティーの自動テストソリューションの使用
- SAP システム内で適切なプログラムを大規模に開始するための、オペレーティングシステムレベルでのスクリプトの作成

ベストプラクティス 16.7 – パフォーマンスデータに基づいてサイジングと設定を継続的に最適化する

インシデント対応プロセス以外でも、定期的にパフォーマンスメトリクスを確認します。そうすることで、サイズが小さい、大きすぎる、あるいはまったく使われなくなったシステムコンポーネント

を発見できます。SAP ワークロードのパフォーマンス最適化を定期的に行い、実際のユーザー負荷に応じたシステムコンポーネントの適切なサイジングに重点を置く必要があります。このアクティビティは、ユーザーエクスペリエンスを向上させ、アーキテクチャの不要な部分を排除し、ワークロードのコスト効率と耐障害性の両方を向上させるのに役立ちます。

提案 16.7.1 – 過去のパフォーマンスメトリクスを参考に、アーキテクチャの適切なサイジングを定期的に実行する

SAP のワークロードを定期的に確認し、コンポーネントのサイズを適正化する機会を設けます。ストレージ、コンピューティング、ネットワーク、およびサポートサービスを増減して、ビジネスパフォーマンス要件により適合させる必要があるかどうかを検討します。

詳細については、以下のリソースを参照してください。

- SAP Lens [コスト最適化]: ベストプラクティス 20.5 - 使用状況を確認し、最適化を図る
- SAP Lens [運用上の優秀性]: ベストプラクティス 4.4 - 定期的なワークロードレビューを実行して、回復力、パフォーマンス、俊敏性、コストを最適化する
- AWS ドキュメント: 規模の適正化

コスト最適化

コスト最適化の柱には、システムのライフサイクル全体を通じた微調整と改善の継続的なプロセスが含まれます。この最適化は、最初の概念実証の設計から、本番稼働ワークロードの継続的なオペレーションに至るまで行われる必要があります。適切なソリューションと料金モデルを選択し、ビジネス成果の達成とコストの最小化を可能にする、コストを意識したシステムを構築できます。長期的なコスト最適化を実現するには、削除または縮小可能なデータ、インフラストラクチャリソース、分析ジョブを特定する必要があります。

17 – SAP のアーキテクチャパターンを評価し、コスト効率を高める

SAP のアーキテクチャパターンの評価にコスト面の配慮をどのように取り入れますか? アーキテクチャについて決定する場合、設計の検討の一環としてコストへの影響を十分に理解する必要があります。

ID	優先度	ベストプラクティス
□ BP 17.1	必須	SAP マネージドサービスの利用を評価する

ID	優先度	ベストプラクティス
□ BP 17.2	必須	SAP アプリケーションアーキテクチャパターンのコスト特性を評価する
□ BP 17.3	必須	各環境の設計においてコストが最適化されるような決定を行うためのビジネス要件を理解する
□ BP 17.4	強く推奨	SAP コンポーネントのサイズ、詳細度、および最新の利用可能な EC2 インスタンスの選択肢を確認する
□ BP 17.5	強く推奨	コスト効率を高める目的でオンデマンドキャパシティの使用を検討する
□ BP 17.6	推奨される	共有サービスおよびソリューションのコストメリットと影響を評価する
□ BP 17.7	推奨される	オートメーションのコストメリットを評価する

ベストプラクティス 17.1 - SAP マネージドサービスの利用を評価する

AWS の責任共有モデルにより、お客様は AWS 上の SAP ワークロードを管理する責任を負います。あるいは、サービスプロバイダーを利用して AWS の SAP ワークロードを管理することができます。サービスプロバイダーを評価する際、初期費用と継続的費用の両方のコスト管理を適切に委託し、継続的プロセスとして扱う必要があります。

複数の AWS パートナーが SAP 環境のデプロイとオペレーションのサービスを提供しています。サービスの範囲や成熟度はパートナーによって異なります。このようなサービスには、例えば効率、一元化されたサポート、デプロイサービスの自動化といった利点があります。それにより、全体的なコストの削減が可能であるため、お客様の具体的なビジネス要件に基づいて評価する必要があります。パートナーの AWS コンピテンシーを評価する際、SAP コンサルティングコンピテンシー や AWS パートナーネットワーク (APN) を参考にしてください。

提案 17.1.1 – コスト管理に関連したロールと責任を理解する

各種マネージドサービス製品は、それぞれ異なるコストモデルに基づいてインフラストラクチャ、ライセンス、サービスをカバーしています。コスト管理の責任がどこにあるかを見極めましょう。そのプロセスでは次のような質問が役に立ちます。

- プロバイダーのコストは
  - インフラストラクチャ支出の割合に基づくのか
  - 合意した総保有コスト (TCO) に基づくのか
- 大まかにクラス分けされているか (S、M、L)。 適切な変更管理プロセスが確立されていて、コストが制御可能で内容がわかるようになっているか
- インフラストラクチャコストの可視性と透明性は十分か
- コストガバナンスがイノベーションや柔軟性を制限していないか

提案 17.1.2 – コスト管理と最適化のアプローチについて全当事者と合意する

各種マネージドサービスを評価するときは、マネージドサービスパートナーのコスト管理に対するアプローチを理解してください。どのように協力すればお客様の組織のコストを継続的に最適化できるかを考える必要があります。

この評価には、定期的なレビュープロセスが必要です。また、共有報酬モデルなどのインセンティブを提供すると、パートナーの責任感が強まり、コストの削減を達成したときに両当事者が財政的なメリットを受けることになるため、有効でしょう。

ベストプラクティス 17.2 – SAP アプリケーションアーキテクチャパターンのコスト特性を評価する

SAP 環境のアーキテクチャを形作る際、インフラストラクチャの規模や場所に加えてコンポーネント数のコストを考慮してください。ソリューションのビジネス要件を確立し、リスクや最適化の機会を認識することで、大幅なコスト削減が実現できます。

提案 17.2.1 – 選択した SAP インストールパターンを見直す

各 SAP アプリケーションについて、スタンドアロン、分散型、高可用性 (HA) といったデプロイパターンを定義します。コスト特性と信頼性特性のバランスを取りながらビジネス要件を満たすようなアーキテクチャパターンを選択します。効果的なアプローチとしては、ビジネスのダウンタイムのコストを数量化し、そこから逆算していく方法が考えられます。可用性に影響する個々の障害のリスクと、そのリスクを削減するのにかかるコストを計算し、バランスを取ります。

さらに、アーキテクチャに最適なサイジングができるだけの柔軟性が備わっているかどうかを検討します。オペレーティングシステムのライセンスやストレージを見直す、複数のアプリケーションサーバーを単一ホストで管理する、といった方法でコストを削減できる場合があります。アプリケーション層に対しては、サポートされているインスタンスファミリーにおいて CPU やメモリを細かく調整

し、それに合わせて価格を設定したインスタンスサイズが提供されています。小規模なインスタンスを複数デプロイした場合、インスタンス再利用やワークロードに基づいたスケーリングの選択肢が広がります。

論理的なグループ分けを評価し、コンポーネント、システム (SID)、環境を組み合わせたときの効果を検討してください。これらのアクティビティによってオペレーションの複雑さが増し、信頼性が低下するかどうかを考えます。

- AWS ドキュメント: Architecture Guidance for Availability and Reliability of SAP on AWS (SAP on AWS の可用性と信頼性のためのアーキテクチャガイダンス)
- SAP Lens [信頼性]: 信頼性の設計原則
- AWS Well-Architected Framework [信頼性]: 信頼性の柱

提案 17.2.2 – 例外的なマルチテナントの使用または単一ホストでの複数データベースのホスティングを評価する

ほとんどのデータベースでは、システムの要件に合わせた柔軟なインスタンスサイジングを活用して各システムを個別にサイジングします。ただし、その原則に従わない方がコスト面のメリットが大きいケースもあります。例:

- HANA ベースのコンポーネントが必要とするメモリが、用意されている最小の EC2 インスタンスサイズより少ない場合は、 SAP HANA マルチテナントデータベースコンテナの使用を検討します。他のコンポーネントと一緒にホストすれば、コンピューティングリソースを効率的に使用できます。
- Oracle および SQL Server などのリレーショナルデータベースに適したコアベースのデータベースライセンスモデル
- アップタイム要件とバージョン依存関係のために密接に結びついているアプリケーション。これには、管理ツール (例えばソリューションマネージャーや SAP HANA Cockpit)、一部の SAP NetWeaver Gateway デプロイオプション (Fiori および ECC) が含まれます。

提案 17.2.3 – 回復力やスケーラビリティを必要としないシステムについて単一ホストインストールパターンの使用を評価する

個々のアプリケーションや環境について、単一ホストモデルのメリットを考える必要があります。単一ホストモデルを利用することで、システムの運用コストやストレージの重複、ソフトウェアライセンスのコスト、マネージドサービスのコストを節約できる場合があります。特に非本番稼働環境で一般的なアーキテクチャオプションには、次のようなものがあります。

- 共同ホストデータベース、アプリケーション、SAP Central Services
- 個別のデータベース (データベースライセンスを最小限に抑える)詳細については次を参照 [コスト最適化]: ベストプラクティス 18.3 - ライセンス形態の影響と最適化オプションを評価する .
- アプリケーションと SAP Central Services の組み合わせ

提案 17.2.4 – コスト効率が最も良く、要件に合ったリージョンを選ぶ

SAP リージョンを選択する際の主要な基準は、近接性、データレジデンシー、サービスの可用性です。複数の選択肢があるデプロイでは、各 AWS リージョンで提供されている料金が地元市場の条件に基づくことに注意してください。そのため、AWS サービスの料金はリージョンごとに異なります。料金の差とその影響を確認してください。

提案 17.2.5 – 障害発生時にスケールできるアーキテクチャを使用する

復旧メカニズムとクラウドの伸縮性により、冗長ストレージが 100% 稼働する必要のない設計が可能です。ビジネス要件が、より柔軟な RTO または RPO を許すようであれば、以下の点を考慮してください。

データベース:

- 目標復旧時点が許すなら、プライマリデータベースノードからの変更を適用するのに同等のコンピューティング性能を必要としないセカンダリまたはスタンバイデータベースノードを検討します。復旧時間への影響を考慮した上で、セカンダリにより小さなインスタンスまたは共有インスタンスをデプロイし、必要なときだけスケールアップする場合のコスト面でのメリットを検討します。より小さなインスタンスを使用すると、プライマリシステムインスタンスとセカンダリシステムインスタンスの関係は 1 対 1 に保たれます。共有インスタンスアーキテクチャが、セカンダリデータベースを非複製システムデータベースとともに単一インスタンスにプールします。障害が発生した場合、テイクオーバーが起こる前に非複製システムを停止しなければなりません。これは、RTO の増加につながります。
- セカンダリ SAP HANA データベースにより小さいインスタンスを使用している場合は、メモリの事前ロード機能をオフにしてスタンバイ時のメモリフットプリントを小さくし、コストを削減します。SAP によるメモリ要件の見積もりは、 Secondary System Usage (セカンダリシステムの使用) のヘルプドキュメントに記載されています。
  - SUSE ドキュメント: SAP HANA System Replication Scale-Up - Cost Optimized Scenario (SAP HANA システム複製スケールアップ - コスト最適化シナリオ) | SUSE
- 目標復旧時間と回復力の要件が許せば、データとログのバックアップに関してマルチ AZ ストレージを使用するアプローチを検討してください (Amazon FSx、Amazon EFS、Amazon S3 など)。こ

れらのアプローチでは、冗長セカンダリリソースを必要とせずにデータの地理的保護が可能です。障害が発生した場合、オンデマンドでセカンダリリソースを作成し、ロケーション間バックアップとログストレージから迅速に復元することができます。

- SAP on AWS ブログ: How to use snapshots to create an automated recovery procedure for SAP ASE databases (スナップショットを使用した SAP ASE データベースの自動化された回復手順を作成する方法)

アプリケーション:

- AWS インスタンスリカバリ は、CloudWatch アラームを使用して Amazon EC2 インスタンスをモニタリングし、ハードウェア障害が原因でインスタンスに問題が発生した場合に自動的にインスタンスを復旧します。カバーされている障害シナリオを確認し、十分な保護が提供されているかを評価してください。
- アプリケーションサーバーをすばやく再作成しなければならないシナリオでは、プロビジョン済みで実行されていない EC2 インスタンス、テンプレート化した AMI、一般的なステージングサーバーを使用したストレージレプリケーション、Infrastructure as Code (IaC) などのオプションがあります。

提案 17.2.6 – 障害発生時の最小コンピューティング性能のコストを検討する

SAP コンポーネントをアベイラビリティーゾーン間で分散させることで、障害発生時のキャパシティ予約にかかるコストが削減できます。アベイラビリティーゾーン間でコンポーネントを分散させれば、ワークロードの一部が地理的に散らばっているため、余分な容量が必要になりません。これにより、AZ 障害が発生しても影響範囲を最小限に抑えることができます。

例えば、障害が発生して 1 つのアベイラビリティーゾーンが失われた状況で 100% の容量が必要なシナリオでは、2 つのアベイラビリティーゾーンの間で 200% の容量をプロビジョンするのではなく、3 つのアベイラビリティーゾーンで 150% をプロビジョンします。

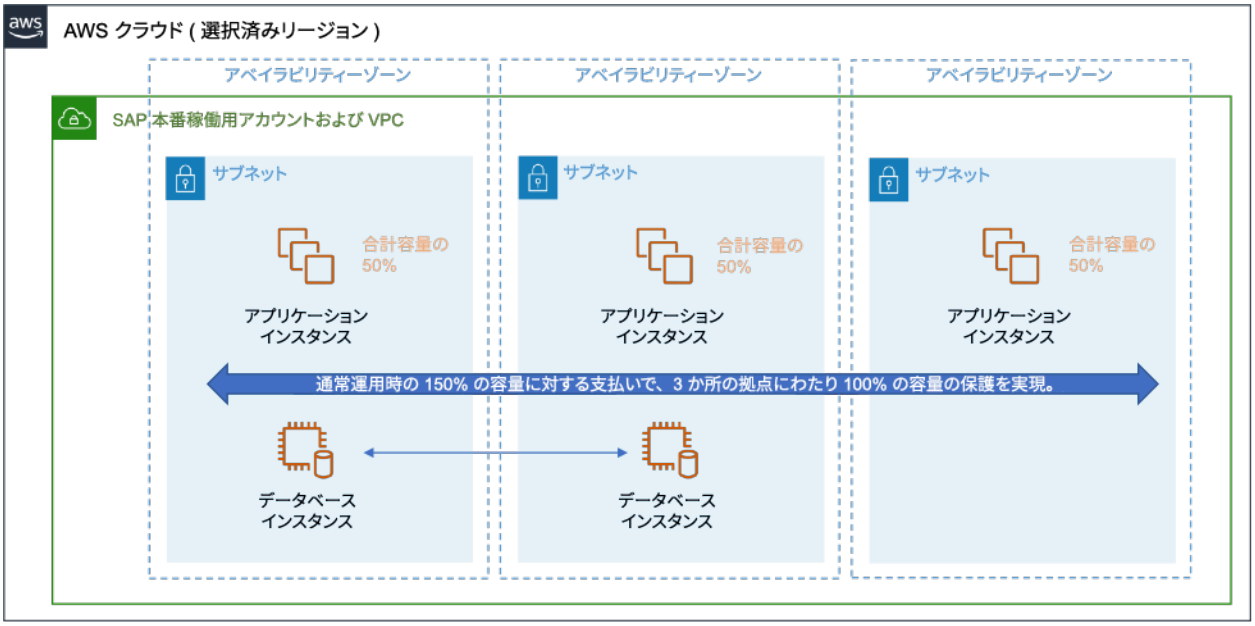

図: 通常のオペレーションで 150% の容量を 3 つのアベイラビリティーゾーンに分散させたアーキテクチャの例

提案 17.2.7 – ストレージのみに基づいた復旧オプションの使用を評価する

AWS では全般に、広範な障害シナリオからの保護を保証するため、ストレージレプリケーションよりデータベースレプリケーションを推奨しています。アプリケーションレイヤーまたはそれほど重要でないインスタンスについては、コンピューティングが不要なストレージレプリケーションを使用した DR ソリューションでコストを削減することができます。それにより、変更管理に関連した複雑さも軽減されます。

- AWS ドキュメント: CloudEndure Disaster Recovery - アマゾン ウェブ サービス (AWS)
- SAP ドキュメント: CloudEndure Disaster Recovery for SAP Applications
- AWS ドキュメント: Replicating automated backups to another AWS Region - Amazon Relational Database Service (Amazon RDS) (別の AWS リージョンへの自動バックアップのレプリケーション - Amazon Relational Database Service (Amazon RDS))

提案 17.2.8 – ネットワーク関連のコストを理解する

SAP のお客様の多くは、オンプレミスネットワークと Amazon VPC を安全に接続する必要があります。適切なサイズの Direct Connect か VPN 接続、またはその両方を使用すると、パフォーマンスおよび信頼性の要件を満たしながらコストを最小限に抑えることができます。

データ転送のコストは、リージョン、VPC、アベイラビリティーゾーンの設計に左右されます。SAP コンポーネントの分散とレプリケーションを、どうすれば信頼性に影響することなく最適化できるか評価してください。

例えば、大量のデータを転送する 2 つのシステムが別々の場所にある場合は、データ転送コストへの影響を考えます。

- AWS ドキュメント: Amazon EC2 オンデマンド料金
- AWS ドキュメント: Architecture Patterns - General SAP Guides (アーキテクチャパターン - 一般 SAP ガイド)

詳細なガイダンスは、Well-Architected Framework のコスト最適化の柱のレビュー、 Plan for Data Transfer - Cost Optimization Pillar (データ転送を計画する - コスト最適化の柱) をご覧ください。

ベストプラクティス 17.3 – 各環境の設計においてコストが最適化されるような決定を行うためのビジネス要件を理解する

システムまたは環境それぞれのコストをその特性に基づいて最適化しましょう。ビジネス要件に合わせて容量、パフォーマンス、信頼性、運用時間を検討します。エンドユーザーエクスペリエンスやビジネスプロセスにとってあまり重要でない環境やアプリケーションの場合は、ストレージやコンピューティング、運用時間を最小限に抑えてコストを削減します。構成を簡素にすることで削減できるコストと、テストまたはサポートのオペレーション要件の間でバランスを取ります。

提案 17.3.1 – 非本番稼働環境で本番稼働のデータの完全コピーが必要かを評価する

非本番稼働環境に本番稼働データの完全コピーを用意することは、ストレージコストとコンピューティングコストに大きく影響します。テスト要件を満たしながら本番稼働データのコピーの数を最小限に抑えることを検討しましょう。非本番稼働環境のデータストレージコストは、次のような方法で抑えることができます。

- 開発およびテストシステムに使用するストレージ容量を少なくします。
- データスライシングツールを使用して非本番稼働システムのテストデータから小さなサブセットを切り取ります。
- 一時本番稼働コピーの使用を検討します。一時本番稼働コピーは、オンデマンドで作成して、ビジネスニーズやテストが終わった時点ですばやく廃棄またはアーカイブすることができます。
- SAP HANA データベースに対して推奨されている 50% の作業メモリが、非本番稼働システムで必要かどうかを評価します。

提案 17.3.2 – 非本番稼働環境で常に本番稼働と同じパフォーマンスが必要かを評価する

非本番稼働システムと一部のサポートシステムでは、ユーザーの数が比較的少ないか、処理するトランザクションボリュームが大幅に少ない、または応答時間の要件が柔軟であるのが普通です。以下の点を考慮してください。

- 小さめの EC2 インスタンスタイプを使用することで、ワークロードの SAP Application Performance Standard (SAPS) を小さくします。
- 使用するアプリケーションサーバーの数を少なくします。
- 低コストの Amazon EBS ストレージタイプを使用します (例えば、 `io2` ではなく `gp3`)。
- 非本番稼働システムのボリュームとして、パフォーマンス特性が低めのものを選びます (例えば、10,000 IOPS ではなく 3,000 IOPS)。
- クラウドの伸縮性が意味するのは、ロードテストやスケーリングテストなど、本番稼働と同等のパフォーマンスを必要とする非本番稼働テストリソースをスケールアップできることです。

提案 17.3.3 – 非本番稼働環境で本番稼働と同等の運用時間が必要かを評価する

テスト、トレーニング、およびサンドボックスシステムのような非本番稼働環境では、本番稼働環境より運用時間が短いことがあります。サポートチームのタイムゾーンと営業時間を考慮して、すべてのシステムが年中無休 24 時間体制であるべきかどうかを判断します。この情報を使って最低の料金モデルを選択します。

例えば、オンデマンド料金モデルで SAP トレーニングシステムを週 40 時間実行した場合 (最大 23% のアップタイム)、3 年間のリザーブドインスタンスまたは Savings Plan で常時 100% 実行した場合より安価です。

提案 17.3.4 – 非本番稼働環境で常に本番稼働と同等の信頼性が必要かを評価する

個々のシステムの信頼性要件に合わせてコスト効率の最も高いアーキテクチャを選びましょう。[信頼性]: ベストプラクティス 10.1 – ビジネス要件に合った SAP ワークロードの可用性目標について合意する を参照してください。詳細なガイダンスは、 信頼性の柱 - AWS Well-Architected フレームワークをご覧ください。

テスト目的だけに本番稼働環境同様のアーキテクチャを用意する場合は、本番稼働をミラーリングしなければならない頻度について考えます。信頼性またはパフォーマンステストのために非本番稼働環境でデータベースの高可用性を実現する必要があるなら、テスト期間外にセカンダリインスタンスをシャットダウンまたはスケールダウンすればコストが削減できます。

オートメーションの使用や、本番稼働同様のパフォーマンスを常に必要とするわけではない環境にオンデマンド料金を適用することで、コスト効率を高めることができます。

提案 17.3.5 – サポートおよびレガシーシステムなどコア以外のシステムのビジネス要件を評価する

参照目的だけにある環境、またはビジネス上それほど重要な役割を持たない環境については、アップタイム、パフォーマンス、信頼性の要件をコアの本番稼働システムと比較して評価します。

例えばレガシーの ERP システムなら、以前のアプリケーションからの変換やビジネス再編を理由とした参照目的で維持する場合があるでしょう。このようなシステムでは、必要なときだけ EC2 インスタンスを実行し、Amazon EBS ストレージの料金だけ支払うようにしてコストを最適化できます。コスト効率がさらに高いのは、バックアップを介してシステムを Amazon S3 と Amazon S3 Glacier にアーカイブするというソリューションです。

ベストプラクティス 17.4 – SAP コンポーネント用に EC2 インスタンスの規模、詳細度、最新製品を確認する

小規模な EC2 インスタンスを選ぶと、SAP ワークロードのコストの柔軟性が高くなります。水平スケーリングが可能になり、使用しないときにコンピューティングをオフにしたり、ピーク負荷時にスケールアップしたりできます。アプリケーション層に一貫した EC2 インスタンスサイズを採用すれば、リザーブドインスタンスおよび Savings Plans 契約の利点をあらゆるワークロードで最大限に活用できます。最新の AWS SAP 認定インスタンスを考慮に入れてください。運用上の影響、ライセンスコスト、サポート、共有および再利用性もコンポーネントごとに評価する必要があります。

提案 17.4.1 – 小規模なアプリケーションサーバーを複数使用して柔軟性を持たせた場合のコストメリットを評価する

SAP ワークロードの多くで、イミュータブルなアプリケーションサーバーを設計することができます。基本ユニットをレプリケーションして水平スケーリングする標準のアプリケーションサーバー構成では、一貫した繰り返し可能なユニットのオプションが使用できます。利点は、再利用性、コンピューティング使用率、予約、オートメーションです。オペレーティングシステムのライセンスやストレージの重複、管理コストなど、ユニットごとの要件を評価に含める必要があります。

以下の点を考慮してください。

- SAP on AWS ブログ: DevOps for SAP – Driving Innovation and Lowering Costs (SAP 向け DevOps – イノベーションの促進とコストの削減) .
- SAP on AWS ブログ: Using AWS to allow SAP Application Auto Scaling (AWS を使用して SAP Application Auto Scaling を有効にする)

提案 17.4.2 – SAP HANA スケールアウト構成 (がサポートされている場合) のコストメリットを評価する

SAP OLAP ワークロードは、 スケールアップとスケールアウトの 構成の両方でデプロイできます。SAP は、運用を簡略化するためにスケールアウトより先にスケールアップすることを推奨しています。しかし、大量の分析ワークロードやネイティブの SAP HANA ワークロードで大規模なコンピューティングが必要となる場合は、スケールアウト実装が適切なことがあります。

S/4HANA も一部のケースでスケールアウト構成をサポートしていますが、制限があります。次を参照してください。SAP Note: 2408419 - SAP S/4HANA - Multi-Node Support (SAP S/4HANA - マルチノードのサポート) [SAP ポータルへのアクセス権が必要]。

スケールアップとスケールアウトのどちらを選ぶかを検討するときは、次の点を考慮します。

- Certified EC2 instance sizes (認定 EC2 インスタンスのサイズ) のうち、スケールアップとスケールアウトに利用できるもの
- 各インスタンスファミリー用の EC2 メモリの 1 GiB あたりのコスト。大規模な EC2 インスタンスは、小規模なインスタンスに比べて 1 GiB あたりのコストが高いのが普通です。
- スケールアウトデプロイによって生じる、データ分散管理の複雑さと運用諸経費。次を参照してください。SAP Note: 2081591 - FAQ: SAP HANA Table Distribution (FAQ: SAP HANA テーブルディストリビューション) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 17.5 – コスト効率を高める目的でオンデマンドキャパシティの使用を検討する

オンデマンド料金モデルは、短めの運用時間、短期プロジェクト、試験的運用が必要となる、または (例えばパフォーマンステストのために) 短期間だけ容量を拡張する必要がある SAP ワークロードに適しています。使用している SAP アーキテクチャのどこでオンデマンド料金が利用できるかを特定します。

提案 17.5.1 – 年中無休 24 時間体制を必要としない SAP システムでのオンデマンドの利用を評価する

オンデマンド料金モデルとその他の料金モデルを利用した場合の損益分岐点に基づいて ([信頼性]: ベストプラクティス 18.1 - Amazon EC2 の利用可能な支払いおよび契約オプションを理解する)、オンデマンドの方が低コストかどうかを評価します。この評価では、Savings Plan 契約全体も考慮に入れます。

一般的なユースケースとしては、営業時間または短期のビジネス実験 (トライアルアップグレード、概念実証など) 以外には必要でない非本番稼働システムが挙げられます。

- SAP on AWS ブログ: SAP システムの起動停止自動化を AWS Systems Manager で実現

提案 17.5.2 - ピーク負荷に備えてスケジュールされたスケーリングオプションと動的スケーリングオプションを評価する

オンデマンドキャパシティは、通常、容量要件が短期間だけ急上昇したピークの SAP ワークロードで使用されます。以下の点を考慮してください。

- 期間、月末、年末、季節性ピークなど、使用パターンが既知である場合のピークには、スケジュールベースの SAP アプリケーションサーバースケーリングを使用します。
- ピークがより不確実でユーザー負荷に合わせてリアルタイムでスケーリングする必要があるアプリケーション層には、動的スケーリングを適用します。SAP 対応で、必要なガバナンスとコントロールを備えたメカニズムを検討します。

注記: アプリケーション層の動的スケーリングを評価する際は、ステートフルな SAP コンポーネントが原因で SAP アプリケーションサーバーがシャットダウンされた場合にユーザー接続とバッチジョブ影響が受ける影響を考慮します。この要件への対処には、AWS、SAP、APN パートナーの開発によるツールが役立ちます。

- AWS ドキュメント: Systems Manager オートメーションアクションのリファレンス
- SAP ドキュメント: SAP Landscape Management (SAP 環境管理)
- SAP on AWS ブログ: Using AWS to enable SAP Application Auto Scaling (AWS を使用した SAP アプリケーションのオートスケーリングの有効化)

ベストプラクティス 17.6 – 共有サービスおよびソリューションのコストメリットと影響を評価する

複数の SAP システムが同じ機能を必要とするケースでは、既存のソリューションや共有コンポーネントを使用して管理とコストを一元化すると、コスト効率が高まります。AWS アカウント境界の内側、または専用のアカウントで管理できる一般的な機能には、モニタリング、バックアップ、接続性があります。標準化、重複の削減、複雑さの軽減がコストの削減につながります。

適度な隔離を維持しながら、また運用に影響する可能性のある依存関係を作り出すことなく、コスト削減のためにリソースを共有する方法を見つけましょう。

提案 17.6.1 – 共有サービスごとに 1 対多のセットアップと比べた 1 対 1 のコストメリットを評価する

SAP 環境では、マルチアカウント戦略の一環として、非本番稼働ワークロードと本番稼働ワークロードを別々のアカウントに隔離するのが標準的なパターンです。これは、一部のサービスにとって論理的境界となります。管理境界を含むことでセグメント化を余儀なくする各シナリオの複雑さと運用コスト、さらにリージョン、AZ、VPC、アカウント間でのデータ転送コストの影響を検討します。

マルチアカウント設計では、一部の AWS サービスを一元的にホストし、ハブアンドスポーク設計で複数のアプリケーションおよびアカウントからアクセスしてコストを節約することができます。次のサービスが含まれます。

- スポーク VPC からのアウトバウンドトラフィック用専用 VPC と NAT ゲートウェイ
- ロードバランサーとウェブディスパッチャーの一元化モデル
- 転送その他のファイル共有ニーズのための共有 Amazon EFS または Amazon FSx

提案 17.6.2 – 既存のサービスを再利用してコストを削減できる場所を評価する

この提案は、さまざまなレベルに当てはまります。

- AWS のサービスがあるところでそれを利用すると、諸経費が最小限に抑えられるので消費ベースの料金モデルに最適です。例として、Amazon EFS、SAP HANA 向け AWS Backint、AWS Backup が挙げられます。
- 一部の機能 (例えばエンタープライズバックアップ) に対して全社的な標準が設定されている場合は、それを使用して運用の一貫性とスケールメリットを保つ必要があります。
- AWS Marketplace または BYOL (Bring-Your-Own-License) では、具体的なビジネス要件に合った APN パートナーソリューションが入手できます。
- ライセンス込みの AWS Marketplace マシンイメージにより、初期コストを削減できる可能性があります。このシナリオでは、ライセンス制限を考慮する必要があります。なぜなら、異なるインスタンスタイプへの移植性が制限されるとソリューションの柔軟性に影響が及ぶからです。

提案 17.6.3 – ビルド・購入・オープンソースの各アプローチを使った場合の影響を理解する

AWS のソリューションも APN パートナーのソリューションも、自分でビルドを作成する部分、オープンソースの部分、既製品の部分が異なる比率で組み合わさっています。バックアップソリューション、高可用性 (HA) ソリューション、共有ストレージソリューションがその例です。

自分でビルドを作成するアプローチ、またはオープンソースソリューションの使用を検討する場合は、次の点を考慮する必要があります。

- サービスレベルアグリーメント (SLA)
- ビルドとメンテナンスに必要なスキル
- サービスの停止がビジネスに及ぼす影響

また、具体的なビジネス要件に合わせて購入しようとしているソリューションについて、入手可能な商用モデルとその機能性を評価する必要があります。商用モデルの条件、例えば使用権を購入するのか利用に応じて料金を支払うのか、料金はどのように計算されるのかを検討します。

ベストプラクティス 17.7 – オートメーションのコストメリットを評価する

AWS にオートメーションを導入することのメリットは、効率と生産性が上昇し、組織のコストの削減につながることです。

提案 17.7.1 – ビルドオートメーションの効率を評価する

Infrastructure as Code を使ったビルドプロセスのオートメーションは、コスト効率に優れ、市場投入までの時間と生産性の改善につながります。品質、整合性、反復性、回復性といった面で DevOps のベストプラクティスがどの程度のメリットをもたらすかを、オートメーションの開発にかかる初期投資の高さと比較する必要があります。

AWS Professional Services または AWS パートナーと協力し、その経験を活用すれば、全体的な労力を減らすことができます。

AWS Launch Wizard for SAP は、オートメーションを通じて SAP デプロイを加速させます。このサービスは、AWS での SAP HANA アプリケーションのサイジング、設定、デプロイの手順を SAP のベストプラクティスに沿って案内します。これは追加料金なしで利用できるサービスで、AWS によるサポートも提供されます。

- AWS ドキュメント: Infrastructure as Code
- AWS ドキュメント: AWS CloudFormation
- SAP on AWS ブログ: AWS for SAP DevOps (SAP DevOps 向け AWS)

提案 17.7.2 – 運用のオートメーションの効率を評価する

運用の実施とモニタリングを自動化する上で AWS およびサードパーティーのツールをどのように利用できるかを調べ、反復タスクのコストと手間を減らしましょう。以下の点を考慮してください。

- AWS サービス: AWS Systems Manager

詳細なガイダンスは、[運用上の優秀性] ベストプラクティス 3.6 - オートメーションを使用して SAP 環境オペレーションを実行する をご覧ください。

18 – SAP コンピューティングリソースのコスト効率を評価する

SAP ワークロード用のコンピューティングおよびストレージオプションはどのように評価すればよいでしょうか。 SAP を AWS に実装または移行する場合は、コスト目標を達成できるように、SAP ワークロードに対してコスト効率の良い EC2 インスタンスとストレージソリューションを選ぶ必要があります。

ID	優先度	ベストプラクティス
□ BP 18.1	必須	Understand the payment and commitment options available for Amazon EC2 (Amazon EC2 の利用可能な支払いおよび契約オプションを理解する)
□ BP 18.2	必須	EC2 インスタンスの選択における主要な検討事項としてコストを使用する
□ BP 18.3	強く推奨	ライセンス形態の影響と最適化オプションを評価する
□ BP 18.4	強く推奨	各ストレージオプションがコストに与える影響を必要な属性に基づいて評価する

ベストプラクティス 18.1 - Amazon EC2 の利用可能な支払いおよび契約オプションを理解する

オンデマンド料金に比べて大幅な割引となるリザーブドインスタンスと Savings Plans の使用を検討します。1 年契約と 3 年契約を、全額前払い、一部前払い、前払いなしの 3 つの支払いオプションで利用できます。

提案 18.1.1 – 料金モデル間の損益分岐点を理解する

リザーブドインスタンス には、スタンダードリザーブドインスタンス (オンデマンド料金の最大 72% 引き) とコンバーティブルリザーブドインスタンス (オンデマンド料金の最大 54% 引き) があ

ります。 Savings Plans には、Compute Savings Plans (オンデマンド料金の最大 66% 引き) と EC2 Instance Savings Plans (オンデマンド料金の最大 72% 引き) があります。

Amazon EC2 オンデマンドの時間料金と比べてどれだけの割引になるかは、次の要因によって決まります。

- 契約期間
- 支払いオプション
- リザーブドインスタンスまたは Savings Plan の種類
- インスタンスファミリー

メモリ最適化インスタンスファミリー (例えば、 `X1` と `X1e`) では契約での割引率が高いため、SAP、特に SAP HANA ワークロードのために料金オプションを理解することが重要です。

AWS 料金計算ツール内のアドバンストオプションを使って損益分岐点を特定します。この計算ツールで前提となっている条件を認識する必要があります。わかりやすく説明するため、各インスタンスファミリーについて、リザーブドインスタンスまたは Savings Plan を使用した場合の TCO がオンデマンドを使用した場合の TCO を下回るポイントを次のような式で特定する例を考えてみましょう。

(契約の実質的時間料金 / オンデマンドの時間料金) * 730 時間

各 RI 契約期間と種類 および各 Savings Plan 契約期間と種類 の実質的時間料金を参照します。異なる損益分岐点をわかりやすく示した以下の例を比較してください。

例 1: バージニア北部 (us-east-1) の M5 ファミリーの場合、3 年契約で前払いなしのスタンダードリザーブドインスタンスまたは EC2 Savings Plan の方が TCO が低くなるポイントは、月間 315 時間 (月曜から金曜まで、1 日最大 16 時間) です。

例 2: バージニア北部 (us-east-1) の X1 インスタンスファミリーの場合、3 年契約で前払いなしのスタンダードリザーブドインスタンスまたは EC2 Savings Plan の方が TCO が低くなるポイントは、月間 235 時間 (月曜から金曜まで、1 日最大 12 時間) です。

その際、 コスト管理 に関する総合的なガイダンスと Well-Architected フレームワークの コスト最適化の柱 を参考にしてください。次の SAP on AWS Pricing Guide (SAP on AWS 料金ガイド) にも AWS で実行する SAP ワークロードについてのガイダンスがあります。コストを分析する際、AWS のすべての料金 (AWS 中国リージョンを除く) が米ドル (USD) で表示されていることに注意してください。ただし、支払い時に別の通貨を選択することができます。 AWS では現在、どの通貨がサポートされていますか? .

- AWS ドキュメント: Savings Plans - Compute Savings Plans and Reserved Instances (Savings Plans - Compute Savings Plans とリザーブドインスタンス)
- AWS ドキュメント: Savings Plans - Plan Types (Savings Plans - プランの種類)
- AWS ドキュメント: リザーブドインスタンスのタイプ

提案 18.1.2 – SAP に関連する各料金モデルの検討事項を理解する

リザーブドインスタンスと Savings Plans には、時間料金の割引の他にも検討すべきメリットがあります。AWS ドキュメントの Comparing Savings Plans to RIs table (Savings Plans と RI の比較表) では、リザーブドインスタンスと Savings Plans を比較しています。

ゾーンリザーブドインスタンス を使用すると、特定のアベイラビリティーゾーン内でキャパシティ予約が可能になります。Savings Plans はキャパシティ予約を提供していませんが、 オンデマンドキャパシティ予約 と組み合わせることでゾーンリザーブドインスタンスと同じ機能が提供できます。[信頼性]: ベストプラクティス 10.2 - 可用性および容量要件に適したアーキテクチャを選択する で容量戦略の詳細を確認してください。

Amazon EC2 スポットインスタンス を使用すると、AWS クラウド上の未使用の EC2 容量を利用できます。スポットインスタンスは、オンデマンドインスタンスの料金に比べて最大 90% の割引価格で利用できます。AWS が容量を必要とする場合、スポットインスタンスは 2 分前までの通知をもって AWS により解放される場合があります。そのため、スポットインスタンスは一般に SAP ワークロードの実行には適していません。

そして オンデマンドインスタンス を使用する場合は、SAP システムの開始がアプリケーションのパフォーマンスに及ぼす影響に加えて、SAP システムとその基礎にある EC2 インスタンスの停止と開始が運用に及ぼすその他の影響を、必要な運用時間に基づいて検討する必要があります。

提案 18.1.3 – リザーブドインスタンスと Savings Plans 契約の一括請求と共有に関するエンタープライズ戦略を評価する

リザーブドインスタンスと Savings Plans は、 一括請求 を利用すると AWS 組織の全アカウントでの使用に適用されます。組織の管理アカウントは、管理アカウントを含めた組織内の任意のアカウントに対し、リザーブドインスタンス割引と Savings Plans 割引を無効にすることができます。つまり、リザーブドインスタンスと Savings Plans の割引は、割引が無効になっているアカウントとは共有されません。リザーブドインスタンスと Savings Plans の割引をあるアカウントと共有するためには、両方のアカウントで割引共有が有効になっている必要があります。この設定は永続的ではなく、いつでも変更できます。

- AWS ドキュメント: AWS Organizations の一括請求 (コンソリデーティッドビリング)

- AWS ドキュメント: リザーブドインスタンスと Savings Plans の割引共有の無効化

契約の共有戦略を決定する際、組織で採用している全体的な AWS アカウント戦略 が重要な要因となります。SAP ワークロードが専用の AWS アカウントで実行されているのか、AWS にホストされている他のワークロードと一緒に実行されているのかも考慮に入れる必要があります。リザーブドインスタンスと Savings Plans の割引が組織の一括請求にどのように適用されているかを理解するには、次のドキュメントを参照してください。

- AWS ドキュメント: 一括請求について

SAP Note: 1656250 - SAP on AWS: Support prerequisites (サポートの前提条件) [SAP ポータルへのアクセス権が必要] に詳しく記載されているとおり、SAP on AWS に関するサポートは、料金ベースの AWS サポート契約 (ビジネスサポート、エンタープライズサポートなど) を結んだ場合のみ提供されます。コストと要件に基づいて適切なサポートプランを特定してください。

- AWS ドキュメント: AWS サポートのプラン比較

AWS が組織内の各メンバーアカウントに対して個別にサポート料金を計算することに注意してください。

ベストプラクティス 18.2 – EC2 インスタンスの選択における主要な検討事項として コストを使用する

ワークロードに適した SAP 認定 EC2 インスタンスを選択することで、コストを最適化できます。各システムを詳細に分析し、できる限りデータ駆動型の決定を下します。一般的なガイダンスについては、Well-Architected Framework の コスト最適化の柱 - 費用対効果の高いリソースをご覧ください。

提案 18.2.1 – リージョンで利用可能な最新世代のインスタンスを選択する

最新世代の Amazon EC2 インスタンスは、より低いコストでより優れたパフォーマンスを提供することが多いため、利用可能でデプロイシナリオに対して認定されている場合は最新世代を使用するようにしてください。

- AWS ドキュメント: SAP 向け Amazon EC2 インスタンスタイプ
- AWS ドキュメント: 利用可能なリージョン

> **Note**
>
> 一部の Amazon EC2 インスタンスファミリー (例えば X1 およびハイメモリ) は、リージョン内の一部のアベイラビリティーゾーンで利用できない場合があります。計画の際は、SAP ワークロードに必要なインスタンスタイプがターゲットのアベイラビリティーゾーンで利用可能であることを確認してください。

提案 18.2.2 – コストとパフォーマンス要件のバランスを取る

SAP に対応した Amazon EC2 インスタンスファミリーで提供されるパフォーマンスは、 SAPSを測定単位とします。各インスタンスファミリーを、自身のパフォーマンス要件に従って評価する必要があります。SAPS あたりのコストと GiB あたりのコストの比率を理解することが推奨されます。

コンピューティング最適化 (**C**)	汎用 (**M***)	メモリ最適化 (**R***)
1 vCPU: 2 GiB	1 vCPU: 4 GiB	1 vCPU: 8 GiB

ワークロードが SAPS (CPU) よりメモリの方を多く必要とする場合は、GiB メモリあたりのコストが最も低いインスタンスファミリーを選択するのが得策です。コンポーネントがメモリより SAPS (CPU) の方を多く必要とする場合は、SAPS あたりのコストが最も低いインスタンスファミリーを選択します。

AMD プロセッサを搭載した SAP 認定インスタンスファミリーは、同等の Intel プロセッサ搭載 EC2 に比べてコストが 10% 低いのが普通です。例えば、同じパフォーマンス KPI でも C5a のコストは C5 に比べて 10% 低くなります。

非本番稼働 SAP HANA ワークロードの場合は、次に記載されている要件を満たしたインスタンスファミリーの使用を検討してください。SAP Note: 2271345 - Cost-Optimized SAP HANA Hardware for Non-Production Usage (非本番稼働環境に適したコスト最適化 SAP HANA ハードウェア) [SAP ポータルへのアクセス権が必要]。

提案 18.2.3 – 成長プロファイルとピーク容量要件の予測可能性を確認する

AWS にある既存の SAP 環境や同種の移行であれば、グリーンフィールド実装や異種の移行に比べて成長や使用状況のパターンが予測しやすい傾向にあります。

成長に関する履歴データがないシステムの場合は、コスト面で利点があり、中短期的な成長に対応できる EC2 インスタンスサイズを検討する必要があります。要件の変化に合わせてインスタンスサイ

ズをスケールできるよう、計画を立てます。アーキテクチャの設計に、リソース消費量の変化に応じて異なる EC2 インスタンスファミリー間を移動できるような柔軟性を持たせる必要があります。

同様に、ピーク容量の変化が考慮されていることを確認します。

SAP HANA 環境をサイジングするときは、データベースのサイズだけでなく作業メモリの要件も考慮に入れてください。SAP HANA サイジングのレポートおよびツールを参照してサイズと使用状況を推定します。

提案 18.2.4 – インスタンス契約の柔軟性を検討する

契約期間中にコンポーネント (例えば、SAP HANA データベース) のスケールアップが必要になった場合、それが別のインスタンスファミリーへの移行につながるかどうかを評価します。これは、料金モデルの選択に関係します。

- AWS ドキュメント: Amazon EC2 インスタンスタイプ

ベストプラクティス 18.3 – ライセンス形態の影響と最適化オプションを評価する

SAP ワークロードを AWS に移行させる際、SAP ワークロードで必要なソフトウェアのライセンスに関連して商業的影響が生じることがあります。このような影響と利用可能なオプションを理解する必要があります。

提案 18.3.1 – ソフトウェアライセンスに対する CPU とメモリの影響を理解する

SAP 向けの Amazon EC2 インスタンスタイプ で使用できる vCPU とメモリの各組み合わせを評価します。

- SAP ドキュメント: SAP Components licensed by vCPU or Memory (vCPU またはメモリ別の SAP コンポーネントライセンス)
- SAP ドキュメント: SAP HANA Allocated Memory Pools and Allocation Limits (SAP HANA 割り当てられたメモリプールと割り当て制限)

Oracle ベースの環境については、以下を確認してください。

- Oracle License Considerations, Licensing Oracle Software in the Cloud Computing Environment (Oracle ライセンスの検討事項、クラウドコンピューティング環境における Oracle ソフトウェアのライセンス)

- 次に記載されている Oracle プレミアムサポート要件。SAP Note: 2069760 - Oracle Linux 7.x SAP Installation and Upgrade (Oracle Linux 7.x SAP のインストールとアップグレード) [SAP ポータルへのアクセス権が必要]

Microsoft Windows および SQL Server 環境については、以下を確認してください。

- AWS ドキュメント: AWS での Microsoft ライセンス
- SAP Note: 2139358 - Effect of changes in licensing terms of SQL Server (SQL Server のライセンス条件の変化が及ぼす影響) [SAP ポータルへのアクセス権が必要]

IBM Db2 環境については、以下を確認してください。

- 対象パブリック・クラウドにおける IBM BYOSL ポリシー
- AWS ドキュメント: Track IBM license usage with AWS License Manager (AWS License Manager で IBM ライセンスの使用状況を追跡する)

CPU またはメモリ別にライセンスされている ISV およびサードパーティー製品への影響を理解します。

- ライセンスコストの最適化に CPU オプションの最適化 機能を使用することを考える
- ソフトウェアライセンスと関連コストの管理に AWS License Manager を使用することを考える
- AWS ドキュメント: Amazon EC2 インスタンスタイプ別の物理コア数

提案 18.3.2 – オペレーティングシステムの購入オプションを理解する

SAP をサポートしている各オペレーティングシステムについて、複数の購入オプションが用意されています。

1. Amazon EC2 で提供されるライセンス
2. AWS Marketplace で提供されるライセンス
3. Bring-Your-Own-License (BYOL)

オプションの中には、一部のオペレーティングシステムで利用できないものもあります。要件とライセンス契約を評価し、どのオプションのコスト効率が最も良いかを特定する必要があります。以下のオペレーティングシステムのコストを Amazon EC2 コストの一部として含めることができます。

- Windows Server
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server (SLES)

以下のオペレーティングシステムは、AWS Marketplace を介して購入できます。

- Red Hat Enterprise Linux for SAP (Red Hat Enterprise Linux ベースの EC2 コストに基づく)
- SUSE Linux Enterprise Server for SAP (Amazon Linux ベースの EC2 コストに基づく)

以下のオペレーティングシステムには Bring-Your-Own-License (BYOL) を使用します。

- Windows Server
- Red Hat Enterprise Linux[1]
- SUSE Linux Enterprise Server (SLES)
- Red Hat Enterprise Linux (RHEL)[2]
- SUSE Linux Enterprise Server (SLES)[2]
- Oracle Enterprise Linux (Oracle Premium Support の要件については、SAP Note: 2069760 - Oracle Linux 7.x SAP Installation and Upgrade (Oracle Linux 7.x SAP のインストールとアップグレード) を参照) [SAP ポータルへのアクセス権が必要]

[1] SAP は Red Hat Enterprise Linux 8 以降、SAP ワークロードで 標準の RHEL をサポートしていないため、SAP Note: 2871484 - SAP supported variants of Red Hat Enterprise Linux (SAP 対応の Red Hat Enterprise Linux バリアント) [SAP ポータルへのアクセス権が必要] を検討します。

[2] これらの製品は、サポート期間が長いため、アップグレードにかかる運用コストを削減できる可能性があります。詳細については、SUSE ドキュメント: SUSE Enterprise Support Policy (SUSE エンタープライズサポートポリシー) と Red Hat ドキュメント: Red Hat Enterprise サポートポリシー をご覧ください。

提案 18.3.3 – ライセンスの制限を緩和するために Amazon EC2 Dedicated Hosts の使用を検討する

Amazon EC2 の Dedicated Hosts では、完全に専用であるハードウェアにアクセスできます。専用のインフラストラクチャで 独自のライセンスソフトウェアを 使用することができます。Amazon EC2 Dedicated Hosts は、Windows Server および SQL Server ライセンスなどのソフトウェアライセンスの管理に便利な AWS License Manager と統合することができます。

提案 18.3.4 – ギガバイトあたり、またはコアあたりのライセンスモデルから離れることのコストメリットを評価する

クラウドへの移行の一環として、SAP Runtime データベースのライセンスモデルを使用することを検討してください。

SAP は、SAP HANA、SAP ASE、サードパーティーデータベースを Runtime データベースのライセンスモデルに基づいてライセンシングする機能を提供しています。SAP からライセンスが付与された Runtime データベースは、SAP からライセンスが付与されたソフトウェアと SAP 指定ユーザーのみをサポートします。SAP の Runtime データベースは、SAP アプリケーションバリュー (SAV) としてライセンスが付与され、その額は SAP ソフトウェア料金の一定の割合として設定されます。

Runtime ライセンスはメモリのギガバイト数や CPU のコア数に基づいて計算されず、SAP ライセンス契約の対象となるすべての環境に適用されるため、特に複数の非本番稼働システムを持つ場合にはギガバイト単位またはコア単位のライセンスモデルよりコスト上のメリットがあります。

SAP ライセンス契約の枠内で既に SAP HANA Database Runtime ライセンスの使用権が付与されている場合は、SAP HANA を基礎のデータベースとして使用できない SAP コンポーネントに対して SAP ASE Database Runtime ライセンスを使用する追加的な権利があるかどうか、またはそのコンポーネントに対して SAP HANA を使用した場合のインフラストラクチャコストを削減できないかどうかを特定する必要があります。

- SAP ドキュメント: SAP Licensing Guide (SAP ライセンスガイド) を参照するか、SAP アカウントチームにご相談ください。

ベストプラクティス 18.4 – 各ストレージオプションがコストに与える影響を必要な属性に基づいて評価する

SAP システムのホスト、アーカイブ、安全確保に、オブジェクトストレージ、ファイルストレージ、ブロックストレージサービスのどれを使うかを決定します。コストが低く俊敏性が高いストレージを設計します。

提案 18.4.1 – ワークロードの I/O およびスループットの要件に合わせて最もコスト効率良く設計できる方法を評価する

ほとんどの SAP 要件では、EBS ボリュームとしてソリッドステートディスク (SSD) が推奨されています。コスト効率の良い選択を行うために、多くの SAP ワークロードに適している汎用 Amazon EBS タイプから始めることをお勧めします。その後、CloudWatch のメトリクスとアプリケーション/データベースモニタリングを使って使用状況を確認します。より高い I/O またはスループットが

必要な場合は、プロビジョンド IOPS Amazon EBS タイプを使用すればニーズを満たすことができます。

- AWS ドキュメント: Amazon EBS ボリュームのタイプ

コスト面とパフォーマンス面の検討事項を考慮するため、SAP HANA データおよびログボリュームに使用するストレージ設定は、SAP ストレージ KPI を満たす必要があります。以下のドキュメントで概説されているストレージレイアウトは、SAP TDI ガイドラインに沿ってテストされたものです: SAP HANA Tailored Data Center Integration (SAP HANA に合わせたデータセンター統合)

- AWS ドキュメント: Storage Configuration for SAP HANA (SAP HANA のストレージ設定)

提案 18.4.2 – ストレージのサイズと設定の動的な変化を計画する

データ使用量または IOPS 要件に従ってストレージを適切にサイジングすることでストレージコストを最適化します。

必要に応じてボリュームサイズを動的に拡張します。アプリケーションのアップグレードなど、高いパフォーマンスが必要なアクティビティの実行中にボリュームタイプを変更するオプションを評価してください。

- AWS ドキュメント: EBS ボリュームへの変更のリクエスト

コストを確実に制御できるように、孤立したボリュームや使用されていないボリュームを定期的に確認します。

- AWS ドキュメント: Amazon EBS ボリュームまたはスナップショット情報を一覧表示する

提案 18.4.3 – オブジェクトストレージのコストメリットを評価する

SAP システムのコアデータは、Amazon EBS 上のデータベースの中にあります。Amazon S3 は、バックアップやアーカイブなどの補助データと画像やドキュメントなどのラージオブジェクト向けに低コストのオブジェクトストレージを提供します。保持または耐久性のニーズに合った ストレージタイプ を選べば、コストがさらに最適化されます。

提案 18.4.4 – 共有ファイルシステムのコストメリットを評価する

Amazon Elastic File System (Amazon EFS) は、サーバーレスで一度設定したらそのまま使える、伸縮自在なファイルシステムであり、ストレージのプロビジョニングや管理を行うことなくファイル

データを共有できます。パフォーマンスや容量の要件に合ったストレージクラスを選ぶことで、コストをさらに最適化できます。

Amazon FSx は、Windows Server 上に構築された高可用性、高耐久性のフルマネージドファイルストレージソリューションです。データの重複排除により冗長データを削除することで、コストをさらに最適化できます。

Amazon EFS または Amazon FSx の一般的な SAP ユースケースには、 `sapmnt`、トランスポート、インターフェイスファイル、バックアップの保存、ソフトウェアなどがあります。Amazon EFS または Amazon FSx を使用すると、独自の高可用性 NFS ソリューションをデプロイする場合に比べてコスト面でメリットがあります。

- AWS ドキュメント: Amazon EFS
- AWS ドキュメント: Amazon FSx

19 – ストレージのコスト効率を高めるために SAP データの使用を最適化する

SAP データの使用をどのように最適化すれば、ストレージおよびメモリ関連のコストを最小限に抑えられるでしょうか。 コストを考慮してデータベースストレージ、バックアップ、および補助ファイルシステムを設計し、ロケーション、保持、ハウスキーピング戦略を評価します。

ID	優先度	ベストプラクティス
□ BP 19.1	必須	アクセスおよび保持の要件を理解する
□ BP 19.2	強く推奨	定期的なハウスキーピングを通じて不要なデータを削除する
□ BP 19.3	推奨される	圧縮、再編成、再利用戦略を使用する
□ BP 19.4	強く推奨	バックアップ戦略に改善の余地がないか確認する
□ BP 19.5	推奨される	ライブデータの階層化オプションを検討する

ID	優先度	ベストプラクティス
□ BP 19.6	推奨される	アーカイブおよびオフロードオプションを評価する

ベストプラクティス 19.1 – アクセスおよび保持の要件を理解する

データにどのようにアクセスしているか、データをどのように保持しているかを理解します。アクティブなデータ、ドキュメント管理システム、バックアップを考慮に入れます。

提案 19.1.1 – SAP システムにある異なるタイプのビジネスデータを分類する

異なるタイプのデータとデータへのアクセス頻度 (データの温度) をビジネスの視点から分類すれば、SAP システムのデータをアーカイブまたはオフロードする機会を特定し、コストを最適化することができます。

以下は、SAP システムで一般的なデータタイプです。

- リファレンス — 値が頻繁には変化しないデータ (都市、国、換算レートなど)
- SAP マスターデータ — 値がほとんど変化しないデータ (SAP カスタマーマスター、製品など)
- 監査 — 監査目的で保管されるデータ (変更ログなど)
- 取引 — 日常業務の中で作成されるデータ (販売伝票など)
- 分析 — 分析や意思決定のために作成されるデータ (月次売上レポートなど)

データの温度を次のように分類します。

- ホット — 頻繁にアクセスするデータ
- ウォーム — あまり頻繁にアクセスしないデータ
- コールド — たまにしかアクセスしないデータ

保持の要件を次のように分類します。

- 災害対策 (DR) 目的で保持する
- 参照目的で保持する
- コンプライアンスまたは監査目的で保持する

ベストプラクティス 19.2 – 定期的なハウスキーピングを通じて不要なデータを削除する

定期的にハウスキーピングと再編成を行ってデータベースのサイズや他のファイルシステムの使用を最小限に抑えれば、データのフットプリントが小さくなり、コストが削減できます。

提案 19.2.1 – SAP 技術テーブルのサイジングを確認し、定期的にハウスキーピングを実施する

SAP は、技術テーブルのデータ管理について包括的なガイダンスを提供しています。これらのテーブルの成長を特定し、それに対処すれば、ストレージとコンピューティングのコストを削減できます。これは、特にデータベースのサイズとメモリの要件が直接的に関連している SAP HANA インスタンスに当てはまります。

- SAP Note: 2388483 - How-To: Data Management for Technical Tables (ハウツー: 技術テーブルのデータ管理) [SAP ポータルへのアクセス権が必要]

参照されている「最大のテーブル」の SQL ステートメントを使用して同等のテーブルサイズ、特に Basis テーブルとしてマークされているテーブルのサイズを調べます。確立された SAP カスタマーによくある例は、完了した SAP ワークフロー項目の多くが削除可能またはアーカイブ可能であるケースです。移行の前にハウスキーピングを実施することは、タイムラインやパフォーマンスの改善にもつながります。SAP HANA を使用している場合は、'/SDF/HDB_SIZING' でクリーンアップの詳細と予想ディスク要件が取得できます。

提案 19.2.2 – ログ、トレース、インターフェイスファイル、バックアップの自動または定期クリーンアップを通じてファイルシステムの成長を制御する

ストレージコストは使用状況によって増減するため、障害分析に不要でありながらコストの増加を助長しているファイルのコピーやバックアップをなくし、基礎の使用料を最適化する必要があります。

- SAP Note: 2399996 - How-To: Configuring automatic SAP HANA Cleanup with SAP HANACleaner (ハウツー: SAP HANACleaner を使って SAP HANA 自動クリーンアップを設定する) [SAP ポータルへのアクセス権が必要]

ベストプラクティス 19.3 – 圧縮、再編成、再利用戦略を使用する

SAP がサポートしているデータベースには、スペースを再利用するためのメカニズムが備わっています。メモリまたは EBS ボリュームの拡張に関連するコストの増加を最小限に抑えるため、これらのメカニズムを定期メンテナンス作業に含める必要があります。

提案 19.3.1 – データ圧縮を使用する

圧縮は、SAP HANA のデフォルト特性の 1 つです。他のデータベースで圧縮を使用するには追加のライセンスが必要な場合がありますが、コスト面とパフォーマンス面でメリットがあるため、検討すべき手段です。以下のドキュメントは、各種データベースのための出発点ですが、追加情報を記載した SAP およびデータベースドキュメントに言及しています。

データベース	SAP ドキュメントまたは SAP Notes
SAP HANA	SAP Note: 2112604 - FAQ: SAP HANA Compression (FAQ: SAP HANA 圧縮) [SAP ポータルへのアクセス権が必要]
SAP ASE	(ガイダンスについては SAP またはベンダーのドキュメントを参照)
IBM Db2	SAP Note: 1555903 - DB6: Supported IBM Db2 Database Features (DB6: サポートされている IBM Db2 データベース機能) [SAP ポータルへのアクセス権が必要]
Oracle	SAP Note: 1289494 - FAQ: Oracle compression (FAQ: Oracle の圧縮) [SAP ポータルへのアクセス権が必要]
Microsoft SQL Server	SAP Note: 1488135 - Database compression for SQL Server (SQL Server のデータベース圧縮) [SAP ポータルへのアクセス権が必要]
SAP MaxDB	(ガイダンスについては SAP またはベンダーのドキュメントを参照)

提案 19.3.2 – データベースの再編成操作と再利用操作を使用する

自然な使用やアーカイブおよびクリーンアップ処理によってデータベース内に生じた未使用のスペースは、再編成または再利用操作を行わないと実際の節約につながらない場合があります。定期的にスペースを再利用すれば、全体的な成長を抑え、ストレージまたはメモリを追加する必要性を減らすこ

とができます。以下のドキュメントは、各種データベースのための出発点ですが、SAP およびデータベースドキュメントに言及しています。

データベース	SAP ドキュメントまたは SAP Notes
SAP HANA	SAP Note: 2499913 - How to shrink SAP HANA Data Volume size (SAP HANA データボリュームのサイズを縮小する方法) [SAP ポータルへのアクセス権が必要]
SAP ASE	SAP Note: 2543407 - reorg rebuild with online - SAP ASE for Business Suite (オンラインでの再編成/再構築 - Business Suite 向け SAP ASE) [SAP ポータルへのアクセス権が必要]
IBM Db2	SAP Note: 1942183 - DB6: When to consider a table or index reorganization (DB6: テーブルまたはインデックスの再編成を考えるタイミング) [SAP ポータルへのアクセス権が必要]
Oracle	SAP Note: 541538 - FAQ: Reorganization (FAQ: 再編成) [SAP ポータルへのアクセス権が必要]
Microsoft SQL Server	SAP Note: 1721843 - MSSQL: Post-steps after archiving, deleting or compression (MSSQL: アーカイブ、削除または圧縮後の手順) [SAP ポータルへのアクセス権が必要]
SAP MaxDB	(ガイダンスについては SAP またはベンダーのドキュメントを参照)

ベストプラクティス 19.4 – バックアップ戦略に改善の余地がないか確認する

AWS で SAP を実行する場合は、バックアップおよび保持のアプローチを評価して、ロケーション、保持、復旧に関連するコストを最適化する必要があります。

提案 19.4.1 – バックアップのロケーションを評価する

Amazon S3 は、低コストで耐久性が高く、ストレージクラスのオプションが用意されているため、SAP システムのバックアップに適した長期ストレージソリューションです。Amazon EBS ボリューム上のデータを Amazon S3 にコピーするには、特定時点のスナップショット、統合データベースツール、または direct API コールを使用します。

スナップショットは、 増分 バックアップです。つまり、最後にスナップショットを作成した後で変更されたデバイス上のブロックのみが保存されます。データが重複しないため、作成にかかる時間が短く、ストレージコストが節約できます。

データベースのバックアップソリューションは、データベースの状態を把握して一貫性を維持する必要があります。AWS では、Amazon S3 と直接統合できる SAP HANA バックアップソリューション (AWS Backint for SAP HANA) を追加コストなしで提供しています。SAP 対応の他のデータベースについては、データベースベンダーまたはサードパーティーが Amazon S3 へのバックアップをサポートするバックアップツールを提供しています。

- SAP ドキュメント: Featured backup solutions (注目のバックアップソリューション)

特別な要件またはステージングエリアについては、まず Amazon EBS にバックアップしなければならない場合があります。そのようなユースケースでは、低コストの HDD ボリュームである ST1 ボリュームタイプを使用すると、バックアップに適したスループットおよびパフォーマンス特性が得られます。また、 ST1 の使用により、SAP データベースをディスクにバックアップする必要がある場合のストレージコストを抑えることができます。

- AWS ドキュメント: Amazon EBS ボリュームのタイプ

バックアップに Amazon EFS を使用する場合は、EFS-Infrequent Access を検討してください。このストレージクラスでは、日常的にアクセスする必要のないファイルのストレージコストが削減できます。Amazon EFS One Zone-Infrequent Access は、データが 1 つのアベイラビリティーゾーンにのみ存在するため、バックアップには推奨されません。

提案 19.4.2 – 標準バックアップの保持ポリシーを確認し、実施する

コストを制御するためには、ビジネス要件に沿った保持ポリシーを実施する必要があります。Amazon S3 は、1 GB あたりのコスト、最短ストレージ期間の変更、(該当する場合は) 取得料金といった特性を備えた、異なるユースケース用の広範なストレージクラスを提供しています。バックアップの保持およびアクセス要件を理解することで、要件を満たすストレージクラスはどれかが特定しやすくなります。

S3 Lifecycle ポリシーを使用すれば、アプリケーションに変更を加えることなく自動的に別のストレージクラスに移転できます。例えば保持期間の短いバックアップであれば、最小ストレージ期間料金および取得料金が設定されている S3-IA や S3 Glacier よりも、S3 Standard の方が適しているでしょう。監査目的の月次バックアップのように保持期間の長いバックアップには、期間の長さに応じて S3-IA または S3 Glacier が適しています。

- AWS ドキュメント: Amazon S3 のストレージクラス
- AWS サービス: Amazon Data Lifecycle Manager
- AWS ドキュメント: Amazon EFS ライフサイクルの管理
- AWS サービス: AWS Backup

提案 19.4.3 – アドホックバックアップの戦略を作成する

システムまたは関連ファイルシステムのアドホックバックアップが必要な場合があります。アドホックバックアップは、変更の前、または特定の時点におけるシステムの状態を示すものとして作成します。アドホックバックアップは、標準の保持期間とは合わない可能性があるため、削除を含めたストレージの使用およびライフサイクルポリシーがバックアップの個々の要件にとって最もコスト効率の良いものとなるように、個別のスケジュールまたはプロセスを使う必要があります。

提案 19.4.4 – バックアップのセットアップを復旧アプローチに照らし合わせてみる

バックアップは、システムを過去のある時点の状態に戻し、障害シナリオから守るために使用します。バックアップストレージを堅牢に、しかし過剰にならない程度に使用して高いコスト効率を維持するには、復旧アプローチを見直す必要があります。古い、より詳細なバックアップについて、当然のように課されていた要件を検証してみましょう。これらの古いバックアップが、復旧の際に必要となるかどうかを特定します。

例えば、データベースとファイルシステム両方のバックアップを使用するのは、有効な戦略です。しかし、復旧の主要なメカニズムがデータベース復元ツールの使用である場合は、一部のボリュームのスナップショットバックアップについて保持期間を短縮したり削除したりすることで、コストを最適化できます。

- AWS ドキュメント: Amazon EBS スナップショット
- AWS ドキュメント: AWS Trusted Advisor ベストプラクティスチェックリスト

ベストプラクティス 19.5 – ライブデータの階層化オプションを検討する

SAP HANA を使った場合のコンピューティングコストは、主に必要なメモリの量によって決まります。そのため、データのオフロードおよび階層化オプションを使用すれば、コンピューティングコストを削減できます。他のデータベースにも階層化オプションはありますが、ここでは特に取り上げません。利用可能なオプションを理解するには、データベースプロバイダーにご相談ください。

提案 19.5.1 – SAP HANA OLAP ベースのワークロードについて動的階層化、拡張ノード、ニアラインストレージ (NLS) を評価する

SAP HANA 動的階層化は、SAP HANA データベースでの履歴データの管理を可能にするオプションのアドオンです。動的階層化の目的は、頻繁にはアクセスされないデータの管理用に SAP HANA メモリに (SAP HANA のインメモリストアとは対照的な) ディスク中心の列指向ストアを加えることです。動的階層化は、ネイティブの SAP HANA ユースケースのみに使用でき、Business Warehouse (BW) on HANA や BW/4 HANA ユースケースには使用できません。

SAP HANA 拡張ノードは、ウォームデータの保存専用にセットアップされ、予約された特殊目的の SAP HANA ワーカーノードです。SAP HANA 拡張ノードを使うと、SAP ビジネスウェアハウス (BW) またはネイティブの SAP HANA 分析ユースケースのためのウォームデータが保存できます。SAP HANA 拡張ノードに保存できるデータの総量は、拡張ノードの合計メモリの 1 倍から 2 倍です。

SAP BW ニアラインストレージ (NLS) と SAP IQ を使うと、BW on HANA または BW/4 HANA データベースの外にコールドデータを保存できます。NLS が HANA データベースのコールドデータを SAP IQ Server 上のストレージに移動させます。

- AWS ドキュメント: SAP Data Tiering (SAP データ階層化)

提案 19.5.2 – OLTP ベースのワークロードについて Data Aging と SAP HANA Native Storage Extension (NSE) を評価する

Data Aging は、アクセス頻度の低いデータをディスク領域に保存することで SAP HANA メモリに空き容量を作ります。

- AWS ドキュメント: SAP Data Tiering (SAP データ階層化)

提案 19.5.3 – 大量の分析データへのデータレイクの使用を検討する

SAP および SAP 以外のデータを分析する場合、S3 ベースのデータレイクをコスト効率の良いデータストレージオプションとして使用できます。

- SAP on AWS ブログ: Building data lakes with SAP on AWS (SAP on AWS を使ったデータレイクの構築)

ベストプラクティス 19.6 – アーカイブおよびオフロードオプションを評価する

アクセス頻度の低いデータをアーカイブするオプション、またはラージオブジェクトを二アラインストレージにオフロードするオプションを検討して、インフラストラクチャおよびバックアップのコストを削減しましょう。

提案 19.6.1 – アクセス頻度の低いデータで構成されたラージテーブルのアーカイブを実施する

特に SAP HANA データベースでは、アーカイブ戦略を通じてデータベースの成長を管理するとコスト上のメリットがあります。

- SAP ドキュメント: Data Archiving (データアーカイブ)

提案 19.6.2 – Amazon S3 を宛先として使えるアーカイブツールを評価する

Amazon S3 は、可用性と耐久性の高い設計で、コスト効率の良い広範なストレージクラスを提供します。そのため、総保有コスト (TCO) を最小限に抑えた SAP アーカイブデータの保存に最適です。

- AWS ドキュメント: Amazon S3 のストレージクラス
- SAP ドキュメント: SAP Certified Archiving Solutions (SAP 認定アーカイブソリューション)

提案 19.6.3 – ラージオブジェクトにデータ管理システムを使用する

請求書や画像などのラージオブジェクトについて、オフロードしてデータを SAP データベースの外で管理する場合のオプションとコストメリットを理解しましょう。データへのアクセスに関するビジネス要件、実装の手間、継続的な管理の複雑さを検討します。

ラージオブジェクトはデータベースのサイズを大きくし、リソースおよびバックアップのコストを増やします。データ管理システムのオプションが、低コストのストレージソリューションを提供する可能性があります。

- SAP ドキュメント: SAP Document Management (SAP ドキュメント管理)
- SAP ドキュメント: Search for Certified ILM Solutions (認定 ILM ソリューションを見つける)

20 – 可視性、計画、ガバナンスをもってコストを管理する

クラウド財務管理 (CFM) をどのように実施すれば、コストを最適化し、コスト意識を維持できるでしょうか。 開始から運用まで、SAP クラウドインフラストラクチャ予算のコントロールを確立し、ビジネス要件に沿って継続的に使用状況を最適化するには、どうすればよいでしょうか。

ID	優先度	ベストプラクティス
□ BP 20.1	必須	プロジェクトフェーズにおける消費モデルおよび環境の使用状況を計画する
□ BP 20.2	必須	異なる料金アプローチを活用した数年計画のコストモデルを確立する
□ BP 20.3	強く推奨	コスト配分、および不正検出などの追跡のために予算とメカニズムを確立する
□ BP 20.4	推奨される	コスト関連の承認手続きとコントロールを確立する
□ BP 20.5	推奨される	使用状況を確認し、最適化を図る

ベストプラクティス 20.1 – プロジェクトフェーズにおける消費モデルおよび環境の使用状況を計画する

移行や実装などの多くのプロジェクトでは、段階的アプローチでシステムのデプロイを進めます。サイジングおよび使用状況のプロファイルを確立する安定化期間もあります。柔軟性とオンデマンドインスタンス機能を活用してこの期間のコストを最小限に抑えましょう。

提案 20.1.1 – 必要な場合のみシステムをデプロイするよう計画する

リードタイムが短いなら、システムを必要なときだけデプロイするオプションが選べます。短期プロジェクトのシステムの場合は、オンデマンドインスタンスを使用してその期間だけのためにプロジェクトシステムを構築します。

提案 20.1.2 – 予想される期間と使用状況プロファイルに従って料金オプションを評価する

プロジェクトの長さと作業時間が料金モデルを左右します。プロジェクトの開始時は、デフォルトでオンデマンド料金モデルを選ぶのが普通です。予算が定義されていること、状況に合わせて安価なオプションに適応できるよう評価されていることを確認します。

提案 20.1.3 – 使用されていないシステムの保留または廃止を計画する

プロジェクトがアクティブでなくなっている場合、またはオブジェクトが既にアーカイブされている場合は、インスタンスのシャットダウンを通じて削減できるコストと、廃止を通じて節約できるストレージを検討します。プロジェクトは通常、移行の際にシステムのコピーを複数作成します。システムのシャットダウンは、必ず使用されていないときに行ってください。

ベストプラクティス 20.2 – 異なる料金アプローチを活用した数年計画のコストモデルを確立する

容量要件の数年計画を確立し、料金モデルをフルに活用して AWS の割引を最大限に利用しましょう。コストのベースラインを設定し、コストを追跡します。柔軟なクラウド料金モデルを利用すれば、インフラストラクチャをビジネス要件の変化に柔軟に合わせることができます。Savings Plans やリザーブドインスタンスの長期契約を結ぶ前に、少なくとも 3 年にわたる SAP システムの使用状況を予想し、計画します。テスト、SAP Quick Sizer の出力、成長予測を参考にして契約プランを検討し、ワークロードに対して最大限の割引を利用できるようにします。

提案 20.2.1 – 主要なビジネスイベントを理解して容量見積もりを立てる

SAP ワークロードは、使用パターンや運用時間が既知で、全般に安定しています。SAP システムについて、十分に理解された定常状態の容量ベースラインを確立しましょう。そのために、デプロイ初期の数週間にパフォーマンステストや本番稼働環境のモニタリングを実施します。

定常状態の容量見積もりは、以下を考慮に入れ、少なくとも 3 年の期間を対象として立てます。

- 合併、買収、資産売却といった大規模なビジネスイベント
- データストレージの要件やビジネスプロセスの頻度に影響する可能性がある規制の変更
- 通常のビジネスオペレーションによるデータの成長 (SAP HANA などのインメモリデータベースでは、データがストレージだけでなくコンピューティングのサイジングにも関係するため、特に重要)
- システムの大規模なアップグレード、交換、廃止

提案 20.2.2 – 1 年契約と 3 年契約のどちらが適切かを評価する

SAP ワークロードの中に 3 年契約からメリットを得るものがどれだけあるかを評価し、容量見積もりに基づいて割引を最大限活用します。以下の点を考慮してください。

- SAP ワークロードのすべてのコンピューティングニーズに対して 3 年契約を使用できるか。
- ニーズのうち、変化しないと確信が持てるものに対して 3 年契約を使用できるか。 例えば、SAP プライマリアプリケーションサーバー、プライマリデータベースなどです。
- SAP ワークロードは、AWS 組織の一部で、今後 SAP 容量要件が変化してコンピューティングニーズが減少した場合に組織が超過分の容量を利用することができるか。
- SAP ワークロードは、AWS 組織の一部で、年中無休 24 時間体制ではない非本番稼働環境のコンピューティング性能を共有することができるか。
- 中期的な容量の変化が生じた場合、3 年契約を通じて得られるメリットは、容量を使い切れないことによる無駄を上回るか (例えば、短期契約と比較したときの損益分岐点が 20 か月目か)。
- 短期的に発生するビジネスの大きな変化や置き換えに影響されやすいアプリケーションについて、短期契約 (1 年) を検討できるか。
- 為替変動を考慮に入れる必要があるか。AWS の料金は (AWS China を除いて) 米ドル (USD) で設定されています。固定された為替レートが望ましい場合は、全額前払いの料金モデルを検討してください。

ワークロードの容量要件に合った契約期間を選び、割引を最大限に活用できるような計画を立てます。

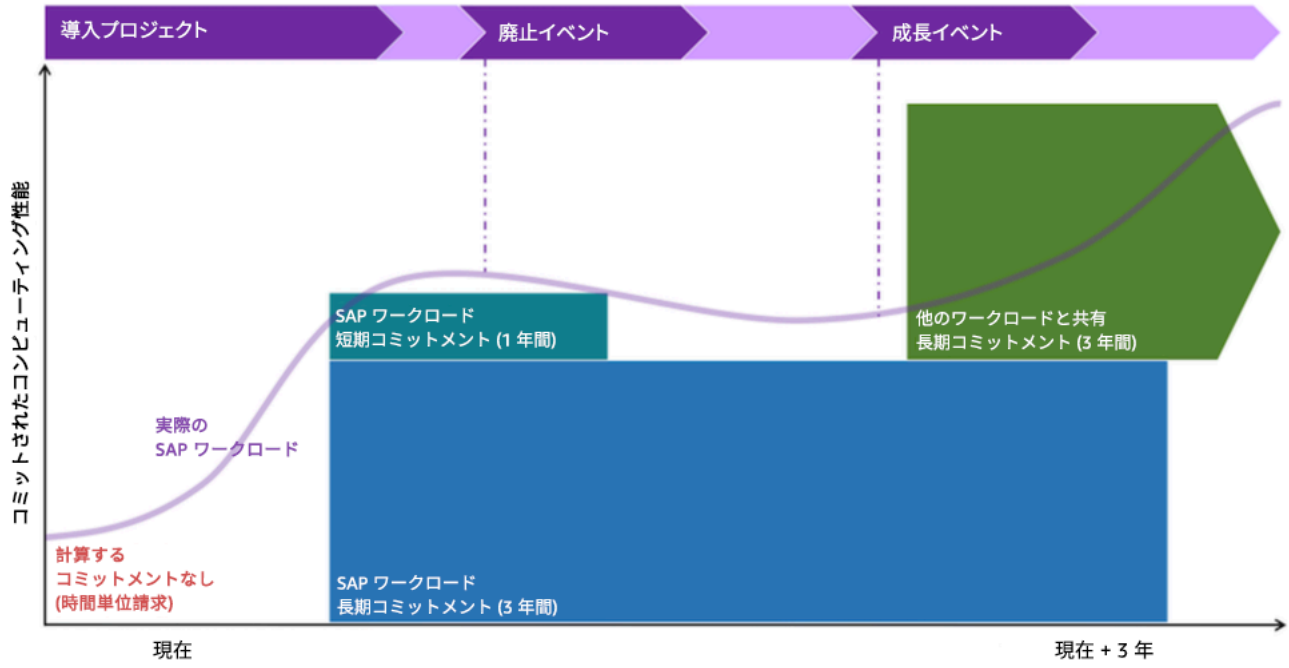

図: SAP on AWS のコンピューティング契約を計画するタイムライン例

提案 20.2.3 – コンピューティングタイプを固定して割引を最大限活用するのが適切かを評価する

SAP ワークロードは、一般に AWS コンピューティングタイプの一部しか使用しません。そのため、特定のコンピューティングファミリーまたは特定のインスタンスタイプを契約することが割引の最大化に適しているかどうかを検討する必要があります。コンピューティングの料金アプローチとして割引率が最も高いのは、EC2 Instance Savings Plans と標準リザーブドインスタンスです。

以下の点を考慮してください。

- お使いの環境で最も使用頻度が高いコンピューティングタイプを調べ、特定の EC2 Instance Savings Plans または標準リザーブドインスタンスの購入を検討します。例えば、複数の SAP アプリケーションで `m5.xlarge` をアプリケーションサーバーとして使用している場合です。その場合、契約プランを常時使用する可能性が高いので、EC2 の特定の Savings Plan または標準リザーブドインスタンスが適しています。
- ワークロードの成長やビジネスイベントの発生時に EC2 ファミリーを変更する可能性が高いコンピューティングコンポーネントを特定します。これらのコンポーネントについては、より汎用性の高い Compute Savings Plans またはコンバーティブルリザーブドインスタンスの購入を検討してください。例えば、たった 6 か月後にサイズの増加が原因で EC2 `r5` と `X1e` の間で移行しなければならない SAP HANA データベースがある場合です。それには、短期のコンバーティブルリザーブドインスタンスまたは Compute Savings Plan が適しています。
- 汎用コンピューティングと特定コンピューティングの料金を比較して損得分岐点を割り出し、それを考慮した上で契約タイプを選択します。例えば、サイジングが 3 年目に変化する場合は、標準リザーブドインスタンスを 3 年分購入する方が、3 年契約のコンバーティブルリザーブドインスタンスを購入するより安い場合があります。また、リザーブドインスタンスの残存期間を AWS リザーブドインスタンスマーケットプレイスで販売してもよいでしょう。
- インスタンスタイプを変更する前に、AWS マーケットプレイスでプライベートの販売者が出品しているソフトウェアや 1 年サブスクリプションのソフトウェアの使用を確認します。そうすることで、余計なソフトウェアコストの発生を防げます。どちらのプランも、ソフトウェア製品を指定の期間にわたって Amazon EC2 インスタンス上で実行することを約束する代わりに、割引が受けられます。例えば、 `r4.xlarge` インスタンスでソフトウェアを実行する 1 年間のサブスクリプションを購入します。その後、インスタンスタイプを `r5.xlarge` に変更することにしました。サブスクリプションはまだアクティブですが、インスタンスには適用されなくなります。その結果、`r5.xlarge` 上のソフトウェアに対して追加のオンデマンド料金を払う必要が生じます。年間サブスクリプションの有効期限が切れるのを待ってからインスタンスサイズを変更することを考えてください。

提案 20.2.4 – Savings Plans とリザーブドインスタンスのどちらが適切か、あるいは両方使用すべきかを評価する

対象となる SAP ワークロードに適しているなら、Savings Plans とリザーブドインスタンスを併用して異なるモデルからメリットが得られるようにしましょう。契約期間とコンピューティング要件を総合的に判断し、料金モデルを選びます。

Savings Plans とリザーブドインスタンスの違いについては、[コスト最適化]: ベストプラクティス 18.1 - Amazon EC2 の利用可能な支払いおよび契約オプションを理解する および Compute Savings Plans and Reserved Instances (Compute Savings Plans とリザーブドインスタンス) を参照してください。

[信頼性]: ベストプラクティス 10.2 - 可用性および容量要件に適したアーキテクチャを選択する .Savings Plans とリザーブドインスタンスのキャパシティ予約の違いおよびトレードオフについて解説しています。

提案 20.2.5 – 予算および追跡の目的で容量計画をコストモデルに変換する

Savings Plans、リザーブドインスタンスの選択肢、オンデマンド予算をコスト計画に変換し、少なくとも 3 年にわたる SAP 環境の AWS 支出を見積もります。予算および追跡の目的で、コンピューティング見積もりと他の AWS コストを組み合わせて SAP ワークロードのコストモデルを完成させます。

SAP コストを見積もる際、必ず次のコストを含めます。

- コンピューティングに不随するストレージのコスト (Amazon EBS ボリュームなど)
- 共有ファイルストレージのコスト (Amazon EFS、Amazon FSx など)
- バックアップストレージのコスト (Amazon S3、Amazon S3 Glacier など)
- ネットワークおよび VPC のコスト (Elastic Load Balancer、NAT ゲートウェイ、Transit Gateway、ネットワークアウトバウンドコスト、Direct Connect、VPN など)
- 管理およびガバナンスサービスのコスト (CloudWatch の詳細なメトリクス、AWS CloudTrail、AWS Config など)
- セキュリティサービスのコスト (AWS WAF、Amazon GuardDuty、AWS Shield など)
- AWS Support のコスト (Business または Enterprise)
- エンタープライズ割引プログラムまたは従量制割引が利用できないか検討する (担当の AWS アカウントマネージャーに詳細を問い合わせてください)
- 通貨: AWS の料金は米ドル (USD) で設定されています。請求通貨は選択できます。請求通貨を選択すると、米ドルで計算された請求額が市場で適切な為替レートで選択した通貨に換算されます。

ベストプラクティス 20.3 – コスト配分、および不正検出などの追跡のために予算とメカニズムを確立する

Well-Architected Framework には、財務管理を実施するための ガイドライン があります。クラウドコストに関する予測と、ビジネスニーズに応じた年間、四半期、月間、あるいは 1 日あたりの予算を設定します。使用状況に合わせて定期的に予測に調整を加え、パターンや異常を検出します。アカウント戦略やタグ付け戦略を使ってコスト配分のメカニズムを確立します。

提案 20.3.1 – コストおよび請求ツールを使用して支出の可視性を高める

確立された SAP システムでは、使用状況パターンにあまり動きがないのが普通です。永続的に利用するかプロジェクトフェーズ中のみ利用するかにかかわらず、オンデマンド料金モデルを利用する場合は、Amazon EC2 のコストに変動が見られます。データボリューム管理戦略を用意していない場合、Amazon EBS および Amazon S3 のコストは予想より高くなる可能性があります。

支出の可視性を高める目的で使える、セットアップの簡単なツールが、 AWS Cost Anomaly Detection です。このツールを使うと、高度な機械学習 (ML) テクノロジーを通じて異常な支出や根本原因を特定し、対策をとることができます。予想されるコストと使用状況に合わせたカスタムの予算を設定するには、 AWS Budgets を使用します。予算アラートを設定して、しきい値を超えた場合に通知が届くようにしましょう。

AWS Cost Explorer と AWS Billing and Cost Management は、可視性と分析のためのツールです。

詳細なガイダンスは、Well-Architected Framework [コスト最適化]: 経費支出と使用量の認識 に記載されています。

提案 20.3.2 – タグを使って支出を分析し、配分する

支出を分析するには、 コスト配分タグ を作成して、個々のアカウント、リソース、ビジネスユニット、SAP 環境ごとに AWS リソースの料金を特定します。作成したコスト配分タグは、AWS 請求レポートに表示され、Cost Explorer で分析できます。コスト配分タグを使用すると、個々の SAP 環境に関連するコストが特定できます。これにより、一時的な環境やプロジェクト環境が不要になった場合など、特定の環境に関連したコストを削減または除外する措置が必要なことを把握できます。コスト配分タグが付いていないリソースを特定するプロセスを用意する必要があります。これらのリソースにコスト配分タグを付けるための措置を実施します。

- SAP on AWS ブログ: Tagging recommendations for SAP on AWS (SAP on AWS のタグ付けレコメンデーション)

ベストプラクティス 20.4 – コスト関連の承認手続きとコントロールを確立する

場合によっては、従来型のコスト評価プロセスをクラウドの使用に向けて適応させる必要があります。適切な財務慣行と財務ポリシーを実施する方法を、 AWS クラウド財務管理のガイドで確認してください。

提案 20.4.1 – 管理者にコストへの影響について学んでもらう

コスト最適化に向けて、責任を割り振り、インセンティブを与えるメカニズムを導入します。

提案 20.4.2 – IAM コントロールを使用してインスタンスのプロビジョニングを特定のユーザーのみに許可する

アカウントの境界内でリソースタイプと職務に沿った IAM ポリシーを使用し、コストを制御します。例えば、プロジェクトチームに対し、サンドボックスアカウント内での小規模な追加システムの制御を許可する場合があるでしょう。ただしその場合は、さらなる承認プロセスを用意し、本番稼働アカウントでの大きなインスタンスへのアクセスを制限します。

ベストプラクティス 20.5 – 使用状況を確認し、最適化を図る

SAP ワークロードを定期的に確認し、コスト最適化の機会を特定します。定期的な確認作業では、AWS の請求書と SAP ワークロード予算の間に見られる差異と異常をできるだけなくすこと、SAP クラウドリソースがすべて適切にサイジングされているか、過剰にプロビジョニングされていないかを確認すること、SAP ワークロードのコスト効率の改善につながるような新たな AWS サービスまたは値下げが発表されていないか確認することに焦点を置きます。

提案 20.5.1 – 使用量が当初の計画より多い場合は追加コストを最小限に抑える

予期しないビジネスイベントが発生した場合や、さらなるパフォーマンスが必要になった場合、クラウドの使用量が増えて推定コストを超えることがあります。このような変化を分析するときは、新たなコストの最適化を念頭に置きます。変化が持続的なものであれば、Savings Plan の契約またはリザーブドインスタンスを増やすことを検討します。

短期間だけキャパシティを増やす必要がある場合は、オートスケーリングまたはスケジュールされたオンデマンドインスタンス容量を使った水平スケーリング (例えば、SAP アプリケーションサーバーの追加) を行ってコストを最小化することを検討します。

提案 20.5.2 – SAP ワークロードの使用状況メトリクスを確認し、可能な限り適切なサイジングを行う

SAP システムを支えるコンポーネントについて、サイジングが適切かを定期的に確認します。CloudWatch メトリクスに基づいて以下の点を検討します。

- SAP EC2 コンピューティングは適切なサイズか。 CPU またはメモリの使用率が低いか。 小さい EC2 インスタンスサイズに移行できるか。
- SAP ストレージは適切なサイズか。 プロビジョニングしていながら使用していない超過スペースがないか。 ボリュームサイズを削減できるか。
- SAP ストレージのパフォーマンスは適切か。 過剰にプロビジョニングされ、削減可能な IOPS または MBps はないか。
- バックアップとスナップショットは適切に管理されているか。 S3 Standard にあるバックアップコピーが多すぎないか。それを Amazon S3 Infrequently Accessed または Amazon S3 Glacier にアーカイブできないか。
- 例えば AWS Compute Optimizer や AWS Trusted Advisor のようなツールを使用して最適化の余地がある領域を特定します。SAP 特有のコンピューティングおよびストレージの制限について次で確認します。SAP Note: 1656099 - SAP Applications on AWS: Supported DB/OS and Amazon EC2 products (AWS 上の SAP アプリケーション: サポートされる DB/OS および Amazon EC2 製品) [SAP ポータルへのアクセス権が必要]。

わかったことに基づいて、引き続き SAP ワークロードコンポーネントを定期的にサイジングし、Savings Plans およびリザーブドインスタンスを最大限に使用します。

提案 20.5.3 – AWS の新しいサービスおよびプランのうち、どれを採用すればさらなるコスト最適化が可能かを理解する

AWS は、定期的に新しいサービスや値下げを発表しています。少なくとも 1 年に 1 回、新しい SAP on AWS サービスの発表を確認し、自身のアーキテクチャで活用する方法を検討してください。AWS と結んだ Enterprise Support 契約の中でテクニカルアカウントマネージャー (TAM) を割り当てられている場合は、TAM が定期的な新サービスと最適化の検討をお手伝いします。

最新のお知らせとニュースを受け取るため、 SAP on AWS ブログ および 最新情報 フィードに登録しましょう。

SAP ワークロードを継続的に最適化する方法については、[運用上の優秀性]: ベストプラクティス 4.4 - 定期的なワークロードレビューを実行して、回復力、パフォーマンス、俊敏性、コストを最適化する をご覧ください。

まとめ

この Lens では、AWS 上で信頼性が高く、安全かつ効率的で、コスト効率に優れた SAP ワークロードを設計、構築、運用するためのアーキテクチャガイダンスを提供しました。一般的なパターン、学んだ教訓、包括的な SAP 設計推奨事項を取り上げました。

フレームワークをワークロードに適用すると、堅牢で安定した効率的なシステムが構築できるため、お客様は SAP ワークロードでの価値の高い運用タスクと、集中的に取り組む分野を広げることに専念できます。

SAP エコシステムは、アプリケーション、ツール、プロセスの成長と成熟に伴い、進化を続けます。こうした進化が起こるにつれ、私たちは、お客様が SAP アプリケーションを適切に設計できるよう支援するためにこの文章を更新し続けます。

寄稿者

本ドキュメントは、次の人物および組織が寄稿しました。

- John Studdert: EMEA SAP スペシャリスト SA マネージャー、Amazon Web Services
- Peter Perbellini: APJ SAP スペシャリスト SA シニアマネージャー、Amazon Web Services
- Adam Hill: プリンシパル SAP スペシャリスト SA、Amazon Web Services
- Nerys Olver: シニア SAP コンサルタント、Amazon Web Services
- Wilson Puvvula: シニアグローバルアカウント SA、Amazon Web Services
- Christopher Spruell: シニアグローバルアカウント SA、Amazon Web Services
- Eneko Bilbao: プリンシパル SAP スペシャリスト SA、Amazon Web Services
- Sabari Radhakrishnan: プリンシパル SAP スペシャリスト SA、Amazon Web Services
- Somckit Khemmanivanh: EC2 Enterprise シニアシステム開発エンジニア、Amazon Web Services
- Sander Bleijenbergh: ISV シニア SA、Amazon Web Services
- Harpreet Singh: パートナー SA シニアマネージャー、Amazon Web Services
- Manoj Muthukrishnan: シニア SAP スペシャリスト SA、Amazon Web Services
- Jongnam Lee: Well-Architected Data Analytics Lens リード SA、Amazon Web Services
- Ben Potter: Well-Architected セキュリティの柱リード SA、Amazon Web Services

ドキュメント履歴

このホワイトペーパーの更新に関する通知を受け取るには、RSS フィードをサブスクライブしてください。

変更	説明	日付
マイナーな更新	壊れたリンクを修正。	January 20, 2022
初版発行	SAP Lens 初回発行。	October 28, 2021

> **Note**
>
> RSS の更新をサブスクライブするには、使用しているブラウザに対して RSS プラグインを有効にする必要があります。

柱別にまとめた設計原則

以下に、このペーパーで紹介した設計原則を AWS Well-Architected Framework の柱ごとにまとめます。

運用上の優秀性

- 1 - 状態の理解と反応ができるように SAP ワークロードを設計する
- 2 – SAP 変更の欠点を減らし、修正を簡単にし、フローを改善する
- 3 – ワークロードを運用する方法を理解する
- 4 – SAP ワークロードを定期的に検証し改善する

セキュリティ

- 5 – セキュリティスタンダードとそれがどのように SAP ワークロードに適用されるかを理解する
- 6 – インフラストラクチャおよびソフトウェアコントロールを使用して、セキュリティの構成ミスを軽減する
- 7 – ID および許可による SAP ワークロードへのアクセスの制御
- 8 – SAP の保管中のデータと送信中のデータを保護する
- 9 – セキュリティイベントのロギング、テスト、および対応のためのセキュリティ戦略を実装する

信頼性

- 10 – 障害に耐える設計
- 11 – 障害を検出し、対応する
- 12 – データ回復の計画

パフォーマンス効率

- 13 – 最適なコンピューティングソリューションを選択する
- 14 – 最適なストレージソリューションを選択する

- 15 – オペレーティングシステム、データベース、SAP アプリケーションのチューニングオプションを評価する
- 16 – 継続的なパフォーマンスと最適化のオプションを理解する

コスト最適化

- 17 – SAP のアーキテクチャパターンを評価し、コスト効率を高める
- 18 – SAP コンピューティングリソースのコスト効率を評価する
- 19 – ストレージのコスト効率を高めるために SAP データの使用を最適化する
- 20 – 可視性、計画、ガバナンスをもってコストを管理する

注記

お客様は、この文書に記載されている情報を独自に評価する責任を負うものとします。本書は、(a) 情報提供のみを目的とし、(b) AWS の現行製品と慣行について説明しており、これらは予告なしに変更されることがあり、(c) AWS およびその関連会社、サプライヤーまたはライセンサーからの契約上の義務や保証をもたらすものではありません。AWS の製品やサービスは、明示または暗示を問わず、一切の保証、表明、条件なしに「現状のまま」提供されます。お客様に対する AWS の責任は、AWS 契約により規定されます。本書は、AWS とお客様の間で締結されるいかなる契約の一部でもなく、その内容を修正するものでもありません。

AWS Glossary

For the latest AWS terminology, see the AWS glossary in the AWS の用語集 Reference.