記事
Toshihiko Minamoto · 2020年8月27日 37m read

Amazon EC2 における InterSystems のテクノロジー: リファレンスアーキテクチャ

企業はグローバルコンピューティングインフラストラクチャを迅速かつ効率的に成長させて管理すると同時に、資本コストと費用を最適化して管理する必要があります。 Amazon Web Services（AWS）および Elastic Compute Cloud（EC2）コンピューティングおよびストレージサービスは、非常に堅牢なグローバルコンピューティングインフラストラクチャを提供することにより、最も要求の厳しいCachéベースのアプリケーションのニーズを満たします。

企業は Amazon EC2 インフラストラクチャを利用し、コンピューティング能力を迅速にプロビジョニングしたり、既存のオンプレミスインフラストラクチャをクラウドに迅速かつ柔軟に拡張したりできます。 AWSは、セキュリティ、ネットワーキング、コンピューティング、ストレージのための豊富なサービスセットと堅牢でエンタープライズレベルの仕組みを提供します。

AWS の中核となっているのは、Amazon EC2 です。 さまざまな OS とマシン構成（CPU、RAM、ネットワークなど）をサポートするクラウドコンピューティングインフラストラクチャです。 AWS は、Amazon マシンイメージ（AMI）と呼ばれる構成済みの仮想マシン（VM）イメージを、さまざまな Linux® および Windows ディストリビューションとバージョンを含むゲスト OS と共に提供しています。AWS で実行される仮想化インスタンスの基盤として、追加のソフトウェアが使用される場合もあります。 このような AMI を最初に使用し、追加のソフトウェアやデータなどをインスタンス化してインストールまたは構成し、アプリケーション固有またはワークロード固有の AMI を作成できます。

あらゆるプラットフォームやデプロイメントモデルと同様に、パフォーマンス、可用性、運用、管理手順などのアプリケーション環境に関わるすべての側面が正しく機能するように注意を払う必要があります。

このドキュメントでは、次のような各分野の詳細について説明しています。

- **ネットワークのセットアップと構成。** このセクションでは、リファレンスアーキテクチャ内のさまざまなレイヤーとロールの論理サーバーグループをサポートするサブネットなど、AWS 内で Caché ベースのアプリケーションのネットワークをセットアップする方法について説明します。
- **サーバーのセットアップと構成。** このセクションでは、各レイヤーのさまざまなサーバーの設計に関連するサービスとリソースについて説明します。
  また、アベイラビリティーゾーン全体で高可用性を実現するためのアーキテクチャも取り上げます。
- **セキュリティ。** このセクションではインスタンスとネットワークのセキュリティを構成し、ソリューション全体やレイヤーとインスタンス間で認可済みアクセスを実現する方法など、AWS のセキュリティメカニズムについて説明します。
- **デプロイと管理。**
  このセクションでは、パッケージ化、デプロイ、監視、および管理の詳細について説明します。

アーキテクチャとデプロイシナリオ

このドキュメントでは、Caché、Ensemble、HealthShare、TrakCare、および DeepSee、iKnow、CSP、Zen、Zen Mojo といった関連する組み込みテクノロジーなどの InterSystems のテクノロジーに基づく堅牢かつパフォーマンスと可用性の高いアプリケーションを提供する AWS 内のいくつかのリファレンスアーキテクチャをサンプルとして提供します。

Caché と関連コンポーネントを AWS でホストする方法を理解するため、まずは典型的な Caché デプロイのアーキテクチャとコンポーネントを確認し、いくつかの一般的なシナリオとトポロジを探っていきましょう。

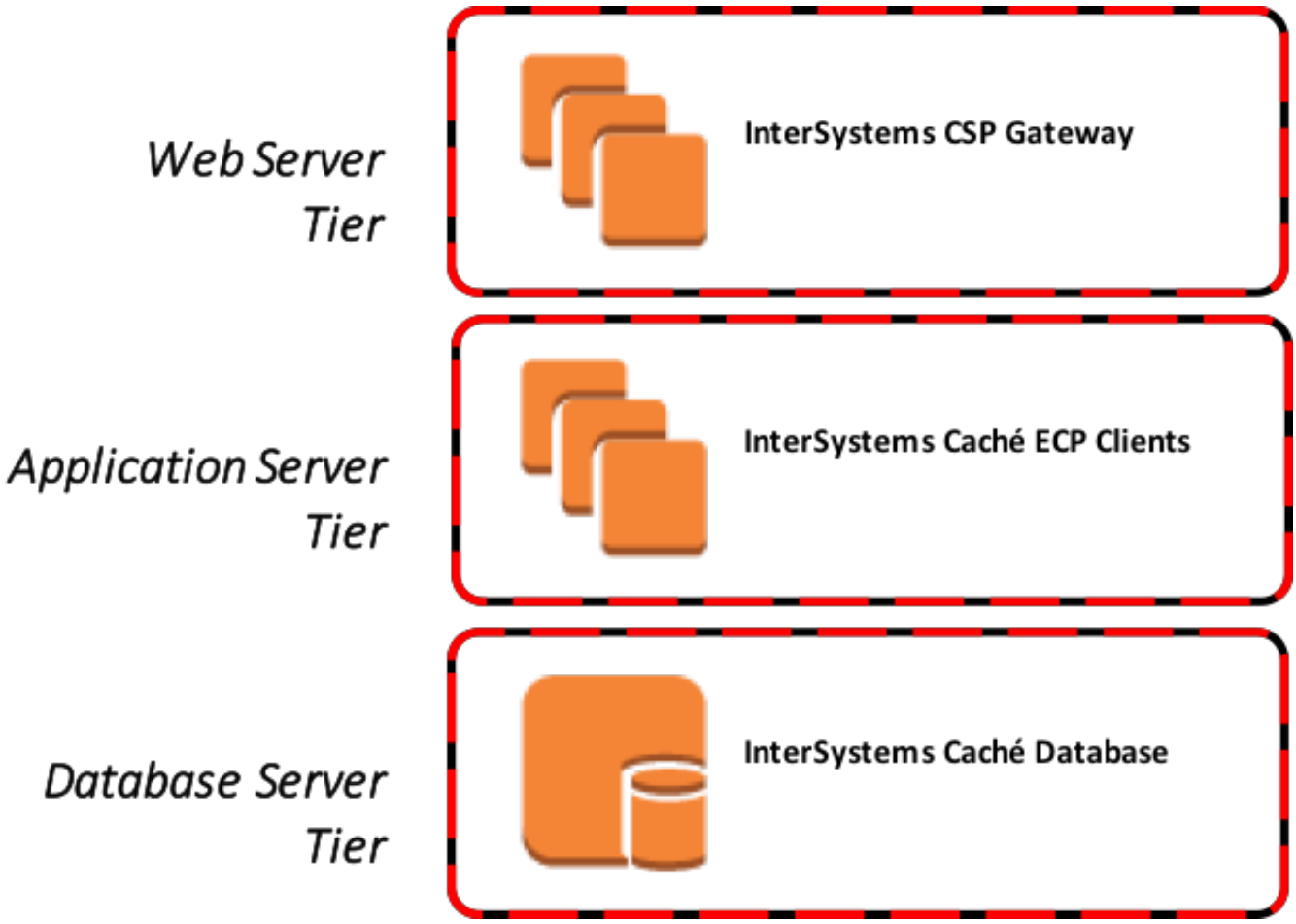
Caché アーキテクチャのレビュー

InterSystems のデータプラットフォームは絶え間なく進化しており、高度なデータベース管理システムと迅速なアプリケーション開発環境を提供することで、複雑なデータモデルの処理と分析、および Web アプリケーションとモバイルアプリケーションの開発に飛躍的進歩をもたらしています。

これは、複数モードのデータアクセスを提供する新世代のデータベーステクノロジーです。
データは単一の統合データディクショナリに1回だけ記述され、オブジェクトアクセス、高性能 SQL、および強力な多次元アクセスによりすぐに利用できます（これらはすべて同じデータに同時にアクセスできます）。

アクセス可能な Caché の高レベルアーキテクチャコンポーネントの階層とサービスを図1に示します。これらの一般的な階層は、InterSystems TrakCare および HealthShare 製品の両方にも適用されます。

図 1: 高レベルのコンポーネント階層



一般的なデプロイシナリオ

デプロイにはさまざまな組み合わせが可能ですが、このドキュメントではハイブリッドモデルと完全なクラウドホストモデルの 2 つのシナリオについて説明します。

ハイブリッドモデル

このシナリオでは、企業はオンプレミスのエンタープライズリソースと AWS EC2 リソースの両方を、必要に応じて災害復旧、社内メンテナンスでの不測の事態、プラットフォームの変更計画、または短期的あるいは長期的な能力の増強に活用したいと考えています。 このモデルは、オンプレミスのフェイルオーバーミラーメンバーセットに対して高レベルの可用性を提供し、事業継続性と災害復旧を実現できます。

このシナリオでのこのモデルは、オンプレミスデプロイと AWS アベイラビリティーゾーン間の接続に VPN

トンネルを利用し、AWS リソースを企業のデータセンターの拡張先として提供しています。 *AWS Direct Connect* などの他の接続方法もあります。 ただし、このドキュメントの中では説明していません。 AWS Direct Connect に関する詳細については、こちらを参照してください。

この例の Amazon Virtual Private Cloud（VPC）を設定してオンプレミスのデータセンターの災害復旧に対応する方法については、こちらを参照してください。

図 2: オンプレミスの障害復旧に AWS VPC を使用するハイブリッドモデル

上記の例は、AWS VPC に VPN で接続されたオンプレミスデータセンター内で動作するフェイルオーバーミラーペアを示しています。 図の中の VPC は、特定 AWS リージョンにある 2 つのアベイラビリティーゾーンで複数のサブネットを提供しています。 レジリエンシーを高めるため、2 つの災害復旧（DR）非同期ミラーメンバー（各アベイラビリティーゾーンに 1 つ）があります。

クラウドホストモデル

このシナリオでは、データレイヤーとプレゼンテーションレイヤーの両方を含む Caché ベースのアプリケーションは、単一 AWS リージョン内の複数のアベイラビリティーゾーンを使用して AWS クラウド内に完全に維持されています。 同じVPNトンネル、AWS Direct Connect、さらには純粋なインターネット接続モデルも利用できます。

図 3: 完全な本番ワークロードに対応したクラウドホストモデル

上記の図 3 の例は、VPC 内にアプリケーションの本番環境全体をデプロイするデプロイモデルを示しています。 このモデルは、アベイラビリティーゾーン間の同期的なフェイルオーバーミラーリングに対応した 2 つのアベイラビリティーゾーンと共に、ロードバランシングされた Web サーバーと関連するアプリケーションサーバーを ECP クライアントとして活用しています。 それぞれの層は、ネットワークセキュリティ制御のために個別のセキュリティグループに分離されています。 IPアドレスと一定範囲のポートは、アプリケーションのニーズに応じて必要な場合にのみ開かれます。

ストレージとコンピューティングリソース

ストレージ

複数のストレージタイプを選択できます。 このリファレンスアーキテクチャでは、*Amazon Elastic Block Store*（Amazon EBS）と *Amazon EC2 Instance Store* インスタンスストア（エフェメラルドライブとも呼ばれます）のボリュームについて想定されるいくつかの使用事例を説明します。 さまざまなストレージオプションの詳細は、こちらとこちらをご覧ください。

Elastic Block Storage（EBS）

EBS は、Linux または Windows で従来型のファイルシステムとしてフォーマットおよびマウント可能で、Amazon EC2 インスタンス（仮想マシン）で使用する耐久性のあるブロックレベルのストレージを提供します。また、最も重要な事ですが、ボリュームはデータベースにとって重要な単一の Amazon EC2 インスタントの稼働期間とは独立して存続するインスタンス外のストレージになっています。

さらに、Amazon EBS はボリュームのポイントインタイムスナップショットを作成し、Amazon S3 に保存する機能を提供します。 これらのスナップショットは新しい Amazon EBS ボリュームの開始ポイントとして、および長期的な耐久性の確保を目的としてデータを保護するために使用できます。 同じスナップショットを使用して必要な数のボリュームをインスタンス化することができます。 これらのスナップショットは AWS リージョン間でコピーできるため、複数の AWS リージョンを地理的な拡張、データセンターの移行、災害復旧により簡単に活用できるようになっています。 Amazon EBS ボリュームのサイズの範囲は 1 GB から 16 TB の範囲で、1 GB 単位で割り当てられます。

Amazon EBS 内には、マグネティックボリューム、汎用（SSD）、プロビジョンド IOPS（SSD）という 3 種類のタイプがあります。 次のサブセクションでは、それぞれについて簡単に説明します。

マグネティックボリューム

マグネティックボリュームは、中程度または突発的な I/O 要件を持つアプリケーションにコスト効率の高いストレージを提供します。 マグネティックボリュームは平均で毎秒約 100 件の入出力操作（IOPS）を実現するように設計されており、ベストエフォートで数百 IOPS にバーストする機能を備えています。 バースト機能がインスタンスの起動時間を高速にするため、マグネティックボリュームは起動ボリュームとしての使用にも適しています。

汎用（SSD）

汎用（SSD）ボリュームは、幅広いワークロードに適した費用対効果の高いストレージを提供します。 これらのボリュームは、数ミリ秒のレイテンシ、長時間にわたって 3,000 IOPS までバーストする機能、3 IOPS/GB から最大 10,000 IOPS（3,334 GBの場合）までのベースラインパフォーマンスを提供します。 汎用（SSD）ボリュームのサイズは 1 GB から 16 TB の範囲です。

プロビジョンド IOPS（SSD）

プロビジョンド IOPS（SSD）ボリュームは、ランダムアクセス I/O スループットにおけるストレージのパフォーマンスと整合性に影響されやすいデータベースワークロードなど、I/O 集中型のワークロードに予測可能な高パフォーマンスを提供するように設計されています。 ボリュームの作成時に IOPS レートを指定すると、Amazon EBS は 1 年間のうち 99.9% の時間についてプロビジョニングされた IOPS の 10% の範囲内でパフォーマンスを提供します。 プロビジョンド IOPS（SSD）ボリュームのサイズは 4 GB から 16 TB の範囲で、ボリュームごとに最大20,000 IOPS をプロビジョニングできます。 プロビジョニングされた IOPS とリクエストされたボリュームサイズの最大比率は 30 です。例えば、3,000 IOPS のボリュームのサイズは少なくとも 100 GB である必要があります。 プロビジョンド IOPS（SSD）ボリュームのスループットは、プロビジョニングされた IOPS ごとに 256 KB であり、最大で 320 MB/秒となります（1,280 IOPS の場合）。

このドキュメントで説明するアーキテクチャでは EBS ボリュームを使用しています。予測可能な低レイテンシの入出力操作毎秒（IOPS）とスループットが必要な本番ワークロードに適しているためです。 すべての VM タイプが EBS ストレージにアクセスできるわけではないため、特定の EC2 インスタンスのタイプを選択する際には注意が必要です。
注意: Amazon EBS ボリュームはネットワークに接続されたデバイスであるため、Amazon EC2 インスタンスによって実行される他のネットワーク I/O と共有ネットワークの全体的な負荷も、個々の Amazon EBS ボリュームのパフォーマンスに影響を与える可能性があります。 Amazon EC2 インスタンスが Amazon EBS ボリュームでプロビジョンド IOPS を十分に活用できるようにするには、選択した Amazon EC2 インスタンスのタイプを Amazon EBS 最適化インスタンスとして起動してください。

EBS ボリュームの詳細については、こちらを参照してください。

EC2 インスタンスストレージ（エフェメラルドライブ）

EC2 インスタンスストレージは、稼働中の Amazon EC2 インスタンスをホストしているのと同じ物理サーバー上に構成され、接続されたディスクストレージのブロックで構成されています。 提供されるディスクストレージの容量は、Amazon EC2 インスタンスのタイプによって異なります。 インスタンスストレージを提供する Amazon EC2 インスタンスファミリーでは、インスタンスが大きいほど、インスタンスストアのボリュームが大きくなる傾向があります。

Amazon EC2 インスタンスファミリーにはストレージ最適化（I2）と高密度ストレージ（D2）があり、それぞれが特定の使用事例を対象とした特殊な用途のインスタンスストレージを提供しています。 例えば、I2

インスタンスは 365,000 超のランダム読み取り IOPS と 315,000 書き込み IOPS に対応できる非常に高速な SSD ベースのインスタンスストレージを提供し、コスト的に魅力的な価格モデルを提供しています。

このストレージは EBS ボリュームのように永続的ではなく、インスタンスの存続期間中のみ使用できるものであるため、接続を解除したり別のインスタンスに接続したりすることはできません。
インスタンスストレージは、絶えず変化する情報を一時的に保存するためのものです。 InterSystems のテクノロジーと製品の領域では、エンタープライズサービスバス（ESB）としての Ensemble や Health Connect
の使用、エンタープライズキャッシュプロトコル（ECP）を使用するアプリケーションサーバー、または CSP Gateway と Web サーバーの使用などが、このタイプのストレージとストレージ最適化インスタンスタイプに適した使用事例になるでしょう。また、プロビジョニングツールと自動化ツールを使用することで、これらの効率を合理化して柔軟性を高めることができます。

インスタンスストアの詳細については、こちらを参照してください。

コンピューティング

EC2 インスタンス

さまざまな使用事例に最適化された多数のインスタンスタイプを利用できます。 インスタンスタイプは、CPU、メモリ、ストレージ、ネットワーク容量のさまざまな組み合わせで構成されており、それらを無数に組み合わせてアプリケーションのリソース要件を適切なサイズに調整できます。

このドキュメントでは、*Amazon EC2 の M4*
汎用インスタンスタイプを適切な環境のサイジングを行うために参照しています。また、これらのインスタンスは EBS ボリュームの機能と最適化を提供しています。
アプリケーションの容量要件と価格モデルに基づいて、他のインスタンスを使用することもできます。

M4 インスタンスは最新世代の*汎用*インスタンスです。 このファミリーは、コンピューティング、メモリ、ネットワークリソースをバランスよく提供しているため、多くのアプリケーションに適しています。 仮想 CPU の数は 2 個から 64 個、メモリ容量は 8 GB から 256 GB を提供し、対応する専用 EBS 帯域幅が決まっています。

個々のインスタンスタイプに加えて、専用ホスト、スポットインスタンス、リザーブドインスタンス、専用インスタンスなどの階層化された分類もあり、それぞれ価格、パフォーマンス、分離の程度が異なります。

現在利用可能なインスタンスの可用性と詳細については、こちらを参照してください。

可用性と運用

Web/アプリサーバーの負荷分散

Cachéベースのアプリケーションには、外部および内部の負荷分散されたWebサーバーが必要となる場合があります。 外部のロードバランサーはインターネットまたは WAN（VPN または Direct Connect）経由でのアクセスに使用され、内部のロードバランサーは内部トラフィックに使用される可能性があります。 AWS Elastic Load Balancing は、アプリケーションロードバランサーとクラシックロードバランサーの 2
種類のロードバランサーを提供します。

クラシックロードバランサー

クラシックロードバランサーは、アプリケーションやネットワークレベルの情報に基づいてトラフィックをルーティングし、高可用性、自動スケーリング、堅牢なセキュリティが必要な複数の EC2 インスタンス間でのトラフィックを単純にロードバラ
ンシングするのに適しています。仕様の詳細と機能については、こちらを参照してください。

アプリケーションロードバランサー

アプリケーションロードバランサーは Elastic Load Balancing
サービスの負荷分散オプションであり、アプリケーションレイヤーで動作し、1 つ以上の Amazon EC2
インスタンスで実行されている複数のサービスや
コンテナ全体の内容に応じてルーティングのルールを定義する機能を提供します。 さらに、WebSockets および HTTP/2 に対応しています。仕様の詳細と機能については、こちらを参照してください。

例

次の例では最高レベルの可用性を提供するため、独立したアベイラビリティーゾーンに 3 つの Web
サーバーのセットが定義されています。 Web サーバーのロードバランサーは、ユーザーセッションを Cookie
を使用する特定の EC2
インスタンスに固定する機能を提供する*スティッキーセッション*を使用して構成する必要があります。
ユーザーがアプリケーションにアクセスし続けると、トラフィックは同じインスタンスにルーティングされます。

次の図4では、AWS 内のクラシックロードバランサーの簡単な例を示しています。

図 4: クラシックロードバランサーの例

データベースミラーリング

Caché ベースのアプリケーションを AWS にデプロイする場合、Caché データベースサーバーの高可用性を確保するには、同期的なデータベースミラーリングを使用して特定のプライマリ AWS リージョンで高可用性を確保し、稼働時間サービスレベル契約の要件によっては非同期なデータベースミラーリングを使用して災害復旧用のセカンダリ AWS リージョン内のホットスタンバイにデータを複製する必要があります。

データベースミラーは、フェイルオーバーメンバーと呼ばれる2つのデータベースシステムの論理グループです。これらのメンバーはネットワークでのみ接続された物理的に独立したシステムです。 ミラーは、2 つのシステムを解決した後、自動的に片方をプライマリシステムとするため、もう片方は自動的にバックアップシステムになります。 外部クライアントワークステーションまたはほかのコンピュータは、ミラーリング構成中に指定されたミラーの仮想IP（VIP）を介してミラーに接続します。
ミラーVIPは、ミラーのプライマリシステムのインターフェイスに自動的にバインドされます。
注意: AWS ではミラー VIP を構成することはできないため、代替ソリューションが考案されています。ただし、サブネット間のミラーリングはサポートされています。

AWS にデータベースミラーをデプロイするための現在推奨されているのは、3
つの異なるアベイラビリティーゾーンの同じ VPC に 3
つのインスタンス（プライマリ、バックアップ、アービター）を構成することです。 こうすることで、AWS
は常に 99.95% の SLA でこれらの VM のうち少なくとも 2 つが外部に接続されていることを保証します。
その結果、データベースのデータ自体の適切な分離と冗長性を提供しています。 AWS EC2
のサービスレベル契約に関する詳細については、こちらを参照してください。

フェイルオーバーメンバー間のネットワーク遅延には厳密な上限はありません。
遅延の増加による影響は、アプリケーションによって異なります。 フェイルオーバーメンバー間のラウンドトリップ時間がディスク書き込みサービス時間と同じである場合、影響はありません。 ただし、アプリケーションがデータの永続化（ジャーナル同期と呼ばれることもあります）を待つ必要がある場合はラウンドトリップ時間が問題になることがあります。
データベースミラーリングとネットワーク遅延に関する詳細については、こちらを参照してください。

仮想 IP アドレスと自動フェイルオーバー

ほとんどの IaaS クラウドプロバイダーには、データベースのフェイルオーバー設計で一般的に使用される仮想 IP（VIP）アドレスを提供する機能がありません。 この問題を解決するために ECP クライアントや CSP Gateway などの最も一般的に使用される接続方法が Caché、Ensemble、HealthShare 内で拡張されたため、VIP
の機能を使用してこれらをミラー対応にする必要はなくなりました。

xDBC、TCP/IP ソケットによる直接接続などの接続方法や、その他の直接接続プロトコルについては引き続き VIP を使用する必要があります。 この問題を解決するため、InterSystems

のデータベースミラーリングテクノロジーは、AWS の Elastic Load Balancer（ELB）とやり取りして VIP のような機能を実現する API を使用することで、AWS 内でこれらの接続方法に対して自動フェイルオーバーを提供できるようにしています。その結果、AWS 内で完全かつ堅牢な高可用性を実現しています。

さらに、AWS は最近になってアプリケーションロードバランサーと呼ばれる新しいタイプの ELB を導入しました。 このタイプのロードバランサーはレイヤー 7 で実行され、コンテンツベースのルーティングをサポートし、コンテナで実行されるアプリケーションをサポートしています。 コンテンツベースのルーティングは、パーティション分割されたデータやデータシャーディングを使用するビッグデータタイプのプロジェクトのデプロイで特に役に立ちます。

仮想 IP の場合と同様に、これは唐突なネットワーク構成の変更であり、フェイルオーバーが発生していることを障害が発生したプライマリミラーメンバーに接続されている既存のクライアントに通知するアプリケーションロジックを必要としないものです。 障害の性質によっては、障害そのもの、アプリケーションのタイムアウトやエラー、新しいプライマリによる古いプライマリインスタンスの強制停止、あるいはクライアントが使用した TCP キープアライブタイマーの失効が原因でこれらの接続が終了する可能性があります。

その結果、ユーザーは再接続してログインする必要になるかもしれません。
この動作はアプリケーションの動作によって決まります。 利用可能なさまざまなタイプの ELB に関する詳細については、こちらをご覧ください。

AWS EC2 インスタンスから AWS Elastic Load Balancer メソッドの呼び出し

このモデルでは、ELB はフェイルオーバーミラーメンバーと潜在的な DR 非同期ミラーメンバーの両方が定義され、現在のプライマリミラーメンバーであるアクティブなエントリが 1 つだけのサーバープールか、アクティブなミラーメンバーのエントリを 1 つ持つサーバープールのみを持つことができます。

図 5: Elastic Load Balancer と対話する API メソッド（内部）

ミラーメンバーがプライマリミラーメンバーになると、新しいプライマリミラーメンバーの ELB を調整/指示するために API 呼び出しが EC2 インスタンスから AWS ELB に発行されます。

図 6: ロードバランサーの API を使用したミラーメンバー B へのフェイルオーバー

同様のモデルは、プライマリミラーメンバーとバックアップミラーメンバーの両方が利用できなくなった場合の DR 非同期ミラーメンバーの昇格にも適用されます。

図 7: ロードバランサーの API を使用した DR 非同期ミラーのプライマリへの昇格

標準の推奨される DR 手順のとおり、上記図 6 の DR メンバーの昇格では非同期複製によるデータ損失の可能性があるため、人間による判断が必要になります。
ただし、その操作を実行した後は ELB 上での管理操作は必要ありません。 昇格中に API が呼び出されると、トラフィックが自動的にルーティングされます。

API の詳細

AWS ロードバランサのリソースを呼び出すためのこの API は、具体的には次のようにプロシージャコールの一部として ^ZMIRROR ルーチンで定義されています。

$$CheckBecomePrimaryOK^ZMIRROR()

このプロシージャの中に、AWS ELB REST API、コマンドラインインターフェイスなどから使用するために選択した API ロジックまたはメソッドを挿入します。 ELB と効果的かつ安全に対話するには、AWS Identity and Access Management（IAM）ロールを使用してください。これにより、長期間有効な認証情報を EC2 インスタンスに配布する必要がなくなります。 IAM ロールは、Caché が AWS ELB と対話するために使用できる一時的な権限を提供します。EC2 インスタンスに割り当てられた IAM ロールの使用に関する詳細は、こちらを参照してください。

AWS Elastic Load Balancer のポーリングメソッド

2017.1で利用可能な CSP Gateway の *mirrorstatus.cxw* ページを使用するポーリングメソッドは、ELB サーバープールに追加された各ミラーメンバーに対する ELB ヘルスモニターのポーリングメソッドとして使用できます。 プライマリミラーのみが「SUCCESS」に応答するため、ネットワークトラフィックはアクティブなプライマリミラーメンバーのみに送信されます。

このメソッドでは、^ZMIRROR にロジックを追加する必要はありません。 ほとんどの負荷分散ネットワークアプライアンスには、ステータスチェックの実行頻度に制限があることに注意してください。
通常、最高頻度は一般的にほとんどの稼働時間サービスレベル契約で許容される 5 秒以上に設定されています。

次のリソースの HTTP リクエストは、ローカルキャッシュ構成のミラーメンバーのステータスをテストします。

/csp/bin/mirrorstatus.cxw

それ以外の場合、ミラーステータスリクエストのパスを実際の CSP ページのリクエストに使用されるのと同じ階層構造を使用し、適切なキャッシュサーバーとネームスペースに解決する必要があります。

例: /csp/user/
パスにある構成サービスアプリケーションのミラーステータスをテストする場合は次のようになります。

/csp/user/mirrorstatus.cxw
注意: ミラーライセンスチェックを実行しても、CSP ライセンスは消費されません。

ターゲットインスタンスがアクティブなプライマリメンバーであるかどうかに応じて、ゲートウェイは以下の CSP 応答のいずれかを返します。

**** 成功（プライマリメンバーである）**

```
==============================

 HTTP/1.1 200 OK

 Content-Type: text/plain

 Connection: close

 Content-Length: 7

 SUCCESS
```

**** 失敗（プライマリメンバーではない）**

```
==============================

 HTTP/1.1 503 Service Unavailable

 Content-Type: text/plain

 Connection: close

 Content-Length: 6

 FAILED
```

**** 失敗（キャッシュサーバーが *MirrorStatus.cxw* のリクエストをサポートしていない）**

```
==============================
```

HTTP/1.1 500 Internal Server Error

Content-Type: text/plain

Connection: close

Content-Length: 6

FAILED

次の図は、ポーリングメソッドを使用するさまざまなシナリオを表しています。

図 8: すべてのミラーメンバーへのポーリング

上の図 8 のように、すべてのミラーメンバーは動作しており、プライマリミラーメンバーのみがロードバランサーに「SUCCESS」を返しているため、ネットワークトラフィックはこのミラーメンバーにのみ送信されます。

図 9: ポーリングを使用したミラーメンバー B へのフェイルオーバー

次の図は、DR 非同期ミラーメンバーの負荷分散プールへの昇格を表しています。これは通常、同じ負荷分散ネットワークアプライアンスがすべてのミラーメンバーにサービスを提供していることを前提としています（地理的に分割されたシナリオについては、この記事の後半で説明します）。

標準の推奨される DR 手順のとおり、DR
メンバーの昇格では非同期複製によるデータ損失の可能性があるため、人間による判断が必要になります。
ただし、その操作を実行した後は ELB 上での管理操作は必要ありません。
新しいプライマリは自動的に検出されます。

図 10: ポーリングを使用した DR 非同期ミラーメンバーのフェイルオーバーと昇格

バックアップと復元

バックアップ操作には、いくつかのオプションがあります。 InterSystems 製品を使用した AWS
のデプロイでは、次の 3 つのオプションを実行できます。 最初の 2 つのオプションは、スナップショットを作成する前にデータベースによるディスクへの書き込みを一時停止し、スナップショットに成功したら更新を再開するというスナップショットタイプの手順を使用しています。 いずれかのスナップショット方式を使用してクリーンなバックアップを作成するには、次のおおまかな手順を実行します。

- データベースのFreeze API呼び出しにより、データベースへの書き込みを一時停止する。
- OS とデータディスクのスナップショットを作成する。
- データベースのThaw API呼び出しにより、Cachéの書き込みを再開する。
- バックアップファシリティはバックアップ場所にアーカイブする。

クリーンで一貫したバックアップを確保するために、整合性チェックなどの追加手順を定期的に追加することができます。

どのオプションを使用するかという決定ポイントは、組織の運用要件とポリシーによって異なります。
さまざまなオプションをさらに詳しく検討するには、InterSystemsにご相談ください。

EBS スナップショット

EBS スナップショットは、高可用性で低コストの Amazon S3
ストレージにポイントインタイムスナップショットを作成するための非常に高速で効率的な方法です。 EBS
スナップショットと共に InterSystems External Freeze および Thaw API の機能を使って、実質的に 24 時間 365 日の運用レジリエンシーとクリーンな定期バックアップを実現できます。 Amazon CloudWatch Events などの

AWS が提供するサービスか、Cloud Ranger や N2W Software Cloud Protection Manager
などの市場で入手可能なサードパーティ
製ソリューションを使用してプロセスを自動化する方法は多数存在します。

また、AWS ダイレクト API
を呼び出し、独自にカスタマイズしたバックアップソリューションをプログラムで作成することができます。API の活用方法の詳細については、こちらとこちらをご覧ください。
注意: InterSystems はこれらのサードパーティ製品を推奨または明示的に検証していません。テストと検証はお客様の責任で実施してください。

論理ボリュームマネージャのスナップショット

別の方法として、市場に出回っている多くのサードパーティ製バックアップツールを使用する場合は、VM
そのものにバックアップエージェントを展開し、Linux
の論理ボリュームマネージャ（LVM）のスナップショットか Windows のボリュームシャドウコピーサービス（VSS）と組み合わせてファイルレベルのバックアップを活用することができます。

このモデルには、Linux および Windows
ベースのインスタンスをファイルレベルで復元できるというメリットがあります。
このソリューションで注意すべき点は、AWS やほとんどの IaaS クラウドプロバイダはテープメディアを提供しないため、すべてのバックアップリポジトリは短期アーカイブ用のディスクベースになっており、長期保管（LTR）を行うには Amazon S3 の低コストストレージ、そして最終的には Amazon Glacier
を活用できるということです。 このモデルを使用する場合は、ディスクベースのバックアップリポジトリを最も効率的に使用できるように、重複除去テクノロジーをサポートするバックアップ製品を使用することを強くお勧めします。

こういったクラウド対応のバックアップ製品には、Commvault、EMC Networker、HPE Data Protector、Veritas Netbackup などさまざまな製品があります。
注意: InterSystems はこれらのサードパーティ製品を推奨または明示的に検証していません。テストと検証はお客様の責任で実施してください。

Caché Online Backup

小規模なデプロイでは、組み込みの Caché Online Backup ファシリティもオプションとして考えられます。
InterSystems のデータベースオンラインバックアップユーティリティは、データベース内のすべてのブロックをキャプチャしてデータベースファイルにデータをバックアップし、出力をシーケンシャルファイルに書き込みます。 この、InterSystems独自のバックアップメカニズムは、本番システムのユーザーにダウンタイムを引き起こさないように設計されています。

AWS ではオンラインバックアップが完了した後、バックアップ出力ファイルとシステムが使用中のその他すべてのファイルをファイル共有（CIFS/NFS）として機能する EC2 にコピーする必要があります。
このプロセスは、仮想マシン内でスクリプト化して実行しなければなりません。

オンラインバックアップは、バックアップに低コストのソリューションを実装したい小規模サイト向けのエントリーレベルのアプローチですが、 データベースのサイズが大きくなるにつれ、スナップショットテクノロジーを使った外部バックアップがベストプラクティスとして推奨されます。外部ファイルのバックアップ、より高速な復元時間、エンタープライズ全体のデータビューと管理ツールなどのメリットがあります。

災害復旧

AWS に Caché ベースのアプリケーションをデプロイする場合は、ネットワーク、サーバー、ストレージなどの DR リソースを異なる AWS
リージョンか、最小限の独立したアベイラビリティーゾーンに配置することをお勧めします。 指定された DR AWS リージョンに必要な容量は、組織のニーズによって異なります。 ほとんどの場合、DRモードでの運用時には本番容量の100%が必要となりますが、弾性モデルとして必要になるまでは、より少ない容量をプロビジョニングできます。 容量が少ないと Web
サーバーとアプリケーションサーバーの数が減り、データベースサーバーに使用できる EC2

インスタンスタイプがさらに小さくなる可能性があります。また、昇格時には EBS ボリュームが大きな EC2インスタンスタイプに接続されます。

非同期データベースミラーリングは、DR AWS リージョンの EC2 インスタンスに対する継続的な複製処理を実行するために使用されます。 ミラーリングは、データベースのトランザクションジャーナルを使用して、プライマリシステムのパフォーマンスへの影響を最小限に抑えながら、TCP/IPネットワーク経由で更新を複製します。 これらの DR 非同期ミラーメンバーには、ジャーナルファイルの圧縮と暗号化を構成することを強くお勧めします。

アプリケーションにアクセスする公開インターネット上のすべての外部クライアントは、追加の DNS サービスである Amazon Route53 経由でルーティングされます。 Amazon Route53 は、トラフィックを現在アクティブなデータセンターに転送するスイッチとして使用されます。Amazon Route53 は、主に次の 3 つの機能を実行します。

- **ドメイン登録** – Amazon Route53では、example.com などのドメイン名を登録できます。
- **ドメインネームシステム（DNS）サービス** – Amazon Route53 は、www.example.com などのわかりやすいドメイン名を 192.0.2.1 などの IP アドレスに変換します。 Amazon Route53 は世界中のネットワークに展開された権威 DNS サーバーを使用して DNS クエリに応答し、レイテンシを削減します。
- **ヘルスチェック** – Amazon Route53 はインターネット経由でアプリケーションに自動的にリクエストを送信し、到達可能であり、利用可能であり、機能していることを確認しています。

これらの機能に関する詳細は、こちらを参照してください。

このドキュメントでは、DNS フェイルオーバーと Route53 ヘルスチェックについて説明します。ヘルスチェックの監視と DNS フェイルオーバーの詳細は、こちらとこちらを参照してください。

Route53 は、各エンドポイントに通常のリクエストを送信してその応答を検証することで機能します。エンドポイントが有効なレスポンスを提供できない場合、DNSレスポンスには含まれなくなり、代わりに利用可能な代替エンドポイントを返します。 このようにして、ユーザートラフィックは障害のあるエンドポイントから離れ、利用可能なエンドポイントに向けられます。

上記の方法を使用すると、特定のリージョンと特定のミラーメンバーへのトラフィックのみが許可されます。これは、この記事で前述した InterSystems CSP Gateway から提示される mirrorstatus.cxw ページであるエンドポイント定義によって制御されます。プライマリミラーメンバーのみが、ヘルスチェックからの「SUCCESS」を HTTP 200 として報告します。

次の図は、フェイルオーバールーティングポリシーの概要を表しています。この方法やその他の詳細については、こちらを参照してください。

図 11: Amazon Route53 のフェイルオーバールーティングポリシー

常に、エンドポイント監視に基づいて、1つのリージョンのみがオンライン状態を報告します。これにより、トラフィックは常に1つのリージョンにのみ流れるようになります。エンドポイント監視は、指定されたプライマリ AWS リージョンのアプリケーションがダウン状態であり、セカンダリ AWS リージョンのアプリケーションがライブになっていることを検出するため、リージョン間のフェイルオーバーにさらに手順を追加する必要はありません。これは、DR 非同期ミラーメンバーが手動でプライマリに昇格されると、CSP Gateway が Elastic Load Balancer のエンドポイント監視に HTTP 200 を報告できるようになるためです。

上記のソリューションの代替案は多くあり、組織の運用要件やサービスレベル契約に基づいてカスタマイズすることができます。

モニタリング

Amazon CloudWatch は、すべての AWS クラウドリソースとアプリケーションに監視サービスを提供できます。

Amazon CloudWatch を使用し、メトリックの収集と追跡、ログファイルの収集と監視、アラームの設定、AWS リソースの変更への自動対応を行うことができます。 Amazon CloudWatch は、Amazon EC2 インスタンス、アプリケーションとサービスによって生成されたカスタム指標、およびアプリケーションが生成したログファイルなどの AWS リソースを監視できます。 Amazon CloudWatch
を使用し、システム全体のリソース使用率、アプリケーションパフォーマンス、運用状態を可視化できます。
詳細については、こちらを参照してください。

自動プロビジョニング

現在、Terraform、Cloud Forms、Open Stack、Amazon 独自の CloudFormation
など、数多くのツールが市場に出回っています。 これらのツールを使用し、Chef / Puppet / Ansible
などのその他のツールと組み合わせることで、DevOps に対応した完全な Infrastructure-as-Code
を提供したり、アプリケーションの立ち上げを完全に自動化したりできます。 Amazon CloudFormation
の詳細については、こちらを参照してください。

ネットワーク接続

アプリケーションの接続要件に応じて、インターネット、VPN、または Amazon Direct Connect
を使用した専用リンクのいずれかを使用して複数の接続モデルを利用することができます。
選択方法は、アプリケーションとユーザーのニーズによって異なります。 これら 3
つの方法の帯域幅使用率はそれぞれ異なるため、AWS 担当者に相談するか Amazon
マネジメントコンソールで特定のリージョンで使用可能な接続オプションを確認することをお勧めします。

セキュリティ

パブリック IaaS
クラウドプロバイダーにアプリケーションをデプロイするかどうかを決定するには注意が必要です。 組織のセキュリティコンプライアンスを維持するには、組織の標準セキュリティポリシーまたはクラウド専用に作成された新しいポリシーに従う必要があります。 また、組織のデータが国外に保存され、データが存在する国の法律に準拠している場合には関連するデータの主権を把握しておく必要があります。 クラウドデプロイメントには、クライアントデータセンターと物理的なセキュリティ管理の外にデータが置かれるため、付加リスクが伴います。 使用中でないデータ（データベースとジャーナル）と使用中のデータ（ネットワーク通信）には、InterSystemsのデータベースとジャーナル暗号化と合わせて、前者にはAESを、後者にはSSL/TLS暗号化を使用することを強くお勧めします。

すべての暗号化キー管理と同様に、データの安全を確保し、不要なデータアクセスやセキュリティ違反を防止するには、組織のポリシーに基づいて、適切な手順を文書化し、それに従う必要があります。

Amazonは、Caché ベースのアプリケーションに非常に安全な運用環境を提供するための広範なドキュメントと事例を提供しています。こちらで参照できる Identity Access
Management（IAM）に関するさまざまなディスカッションのトピックを確認してください。

アーキテクチャ図の例

下の図は、データベースミラーリング（同期フェイルオーバーと DR 非同期）、ECP
を使用したアプリケーションサーバー、負荷分散された複数の Web
サーバーの構成で高可用性を提供する典型的な Caché のインストール環境を表しています。

TrakCareの例

次の図は、負荷分散された複数の Web サーバー、ECP クライアントとしての 2
台のプリントサーバー、データベースミラーで構成される典型的な TrakCare のデプロイを表しています。
仮想IPアドレスは、ECPまたはCSP Gatewayに関連付けられていない接続にのみ使用されます。

ECPクライアントとCSP Gatewayはミラー対応であり、VIPを必要としません。

Direct Connect を使用している場合、災害復旧シナリオで有効にできる複数の回線やリージョンアクセスなどのオプションがあります。
電気通信事業者に相談し、事業者がサポートする高可用性と災害復旧シナリオを理解することが重要です。

下のサンプルリファレンスアーキテクチャ図には、アクティブまたはプライマリリージョンにおける高可用性と、プライマリ AWS リージョンが利用不可である場合の別の AWS リージョンへの災害復旧が含まれます。
また、この例では、データベースミラーには、1つのミラーセット内にTrakCare DB、TrakCare Analytics、およびIntegrationネームスペースが含まれています。

図 12: TrakCare AWS リファレンスアーキテクチャ図 – 物理アーキテクチャ

さらに、次の図は、関連するインストールされたエンドユーザ向けソフトウェア製品と機能的な目的で、より論理的なアーキテクチャを示しています。

図 13: TrakCare AWS リファレンスアーキテクチャ図 – 論理アーキテクチャ

HealthShare の例

次の図は、負荷分散される複数のWebサーバーと、Information Exchange、Patient Index、Personal Community、Health Insight、Health Connectといった複数のHealthShare製品による典型的なHealthSharaeデプロイメントを示しています。
それぞれの製品は、複数のアベイラビリティーゾーン内に 1 組のデータベースミラーを含めて高可用性を実現しています。 仮想IPアドレスは、ECPまたはCSP Gatewayに関連付けられていない接続にのみ使用されます。
HealthShare製品間のWebサービス通信に使用されるCSP Gatewayはミラー対応であり、VIPを必要としません。

下のサンプルリファレンスアーキテクチャ図には、アクティブまたはプライマリリージョンにおける高可用性と、プライマリリージョンが利用不可である場合の別の AWS リージョンへの災害復旧が含まれます。

図 14: HealthShare AWS リファレンスアーキテクチャ図 – 物理アーキテクチャ

さらに、次の図は、関連するインストール済みのエンドユーザ向けのソフトウェア製品、接続要件と手法、およびそれぞれの機能的な目的で、より論理的なアーキテクチャを示しています。

図 15: HealthShare AWS リファレンスアーキテクチャ図 – 論理アーキテクチャ

#AWS #iFind #インターシステムズビジネスソリューションとアーキテクチャ #クラウド #システム管理 #Caché

ソースURL:https://jp.community.intersystems.com/post/amazon-ec2-%E3%81%AB%E3%81%8A%E3%81%91%E3%82%8B-intersystems-%E3%81%AE%E3%83%86%E3%82%AF%E3%83%8E%E3%83%AD%E3%82%B8%E3%83%BC-%E3%83%AA%E3%83%95%E3%82%A1%E3%83%AC%E3%83%B3%E3%82%B9%E3%82%A2%E3%83%BC%E3%82%AD%E3%83%86%E3%82%AF%E3%83%81%E3%83%A3