目次

1. クラウドコンピューティング
2. ON DemandサービスとSLA
3. 仮想化（Virtualization）
4. クラウド·コンピューティング·モデル
5. AWSの紹介
6. EC2(Elastic Compute Cloud)
7. RDS : Relation Database Service
8. S3
9. VPC
10. IAM
11. ELB, Auto Scaling

**1. クラウドコンピューティング**

* インターネットを使用して共有リソース（サーバー、ネットワーク、ストレージ）を使用できるサービスである。
* 企業、あるいは個人がコンピュータが必要なときはサーバーあるいはPCを購入して電源を繋ぐ。そして オペレーティングシステム(operating system)という
* クラウドコンピューティングはこのようなすべての作業をサービス形で提供する。
* Amazon AWS, Microsoft Azure, Google Colud Platform

**2. ON DemandサービスとSLA**

**On Demand**

* クラウドコンピューティングユーザーが要請した分だけサービスを提供し、費用を請求するモデルを意味する。
* 例えば、IBMのサーバーを購入せずにCPU4個に主記憶装置8Gigabyteが必要な場合、IBMに要請してサーバーを提供してもらうことになる。

**SLA**

* SLAとは、オンデマンドサービスを使用する際のクラウドコンピューティングサービスユーザとサービス提供者（AWS）との間のサービスレベルに関する協約書である。
* つまりSLA を通じて使った分の費用を支払うことになる。

**3. 仮想化（Virtualization）**

仮想化とは、複数の物理的資源を一つに統合して管理したり、一つの物理的資源を複数に分割して使用する技術で、サーバ仮想化、デスクトップ仮想化、ストレージ仮想化などの技術がある。

* **一つの物理的資源を一緒に使用**   
  仮想化は一つの高性能コンピュータを分割して複数のサービスユーザーに提供できるようにする。
* **複数の物理的資源を統合**  
  仮想化は複数の物理的サーバーを統合し、まるで一台の高性能コンピュータを使用するかのようにする。

**仮想化の種類**

**1) ホスト仮想化(Host Virtualization)**

* Host OSの上にGuest OSが実行される方式である。
* コンピュータにインストールされたオペレーティングシステムに仮想マシンをインストールし、仮想マシンにGuest OSをインストールする。
* 教育環境でよく使われる。
* VM Workstation, VMServer, Virtual Boxなどがある
* 長所:Host OS 制約がない
* 短所:Host OSの上に再びGuest OSをインストールして使用するため、オーバーヘッドが大きい。

**2) ハイパーバイザー (Hypervisor)**

* HostOSがなく、ハードウェアがハイパーバイザーを設置して使用する方式
* ハードウェアの上に別途のHost OS を設置せずにハイパーバイザーという仮想化ソフトウェアを設置する。 そしてハイパーバイザーの上にGuest OSを設置する仕組みである。
* 長所 : Host OSを持っていないため、オーバーヘッドが少ない
* 短所: マシンに対する管理機能がないため、管理のためのコンピュータ、コンソールが必要だ。

**ハイパー仮想化の種類**

Type 1 (Native, Bare metal)

オペレーティングシステムがプログラムを制御するようにハイパーバイザーがそのハードウェアで直接実行され、仮想システム(Guest)はハードウェアの上で2番目のレベルで実行される環境

Type 2 (Hosted)  
ハイパーバイザーが一般プログラムのようにホストOS環境で実行され、仮想システム(GuestOS)はハードウェアの上で3番目のレベルで実行される環境をいう。

**3) コンテナ仮想化(Container)**

* Host OS 上にコンテナ管理ソフトウェアを設置し、論理的なコンテナを分けて使用する。
* コンテナ方式は、Host OS の上にコンテナ（Docker など）を設置し、それぞれのコンテナごとにアプリケーションを使用する方式である。
* 長所:オーバーヘッドが少なくスピードが速い
* 短所:もしDockerを使用する場合、Linuxベースのオペレーティングシステムを使用しなければならない

**４ クラウド·コンピューティング·モデル**

**On-Premise**

サーバー、データベース、ネットワーク装備などを全て購入して構築し運営するサービスを意味する。 一般的にIDC(*Internet Data Center*)にサーバを設置し、専用ネットワークを通じて運営するシステム形態である。

**IDC施設**

* サーバーラック(Server Rack) : ラックはサーバーをインストールする装置を意味する
* ケーブルタワー : 各種サーバにケーブルを接続して通信し、ケーブルはケーブルタワーに設置する
* 恒温恒湿器:IDCの温度、湿度などを調節する。

On-Premiseにシステムを構築するためには、施設やサーバーの購入などの費用が発生し、IDCを運営するための各種付帯費用や人材費用などが発生する。 AWSは全世界にリージョンを置き、AWSでこのようなIDCを構築し、サービスする。

**クラウドコンピューティングの種類**

* Private Cloud: 企業内部で企業内部の組織員のためのサービス
* Public Cloud: インターネットを使用して提供するクラウドコンピューティングの形態としてAWS、Azureなどがある
* Hybrid Cloud: private、publicをすべて提供

**クラウド·コンピューティング·モデル**

**Iaas (Infrastructure as a Service)**

* インフラをサービス形態で提供することにより、サーバ、ストレージ、ネットワーク関連の物理的装備をサービス形態で提供
* -AWSでは、EC2、S3、VPCなどのサービスが該当

**PaaS(Platform as a Service)**

* インフラに設置されるオペレーティングシステム、ミドルウェア、データベース管理システムなどのソフトウェアを提供する
* AWSでは、LinuxおよびWindowsオペレーティングシステム、Oracle、MySQLなどのDBMSを提供

**Saas (Softward as a Service)**

* アプリケーションをサービス形態で提供
* グーグルオフィス、ドロップボックス、Gmail

**5 AWSの紹介**

**コンピューティングサービス**

**Amazon EC2**

* さまざまなタイプの仮想化サーバーをサポートする
* Windows、Linux、Auroraなどをサポートする

**Amazon Auto Scaling**

* 特定の条件に従って自動的にサーバーを追加、削除するサービス
* つまり、使用量に応じた増設と縮小を自動的に行う

**Amazon Lightsail**

* VPS(Virtual Private Server)はウェブサイトおよびウェブアプリケーションを配布または管理する

**Amazon Workspace**

* デスクトップ仮想化サービスで社内PCを仮想化し、個人PCに文書を保存せずにサーバーに保管する。

**ネットワーキング·サービス**

**Amazon Route 53**

* クラウドベースのDNS(Domain Name System)

**Amazon VPN**

* ネットワークアクセス制御、DHCP、VPNを使用して仮想プライベートネットワークを構成する

**AWS Direct Connect**

* AWSを接続するために専用線を構成することで、AWS-On-Premiseを接続する

**Amazon ELB(Elastic Load Balancer)**

* ネットワーク負荷を分散させるためにL4スイッチの役割を果たす

**ストレージ·サービス**

**Amazon S3**

* 汎用的なストレージを提供するサービスで、データ保管、ウェブサイトホスティングなどのデータを保管·管理

**Amazon DynamoDB**

* NoSQLサービスで大容量データを保存·分析するためのサービス

**Amazon Elastic Cache**

* In-memoryベースのCacheサービス

**ストレージ**

長期的にデータを保存およびアクセスできるようにするコンピュータ コンポーネント。

**メモリーとストレージとの重要な違いは**、メモリーのデータはコンピューターの電源が切れるとすべて消えるという点。 一方、ストレージのデータは、コンピュータがオフになる回数に関係なく、破損していない状態を維持

**分析プラットフォーム**

**Amazon Kinesis**

* 大規模ストリーミングサービスを行うために大量のサービスを保存、分類するサービス
* 機械学習分析、ビデオ、オーディオ、アプリケーションログ、IoTデータをリアルタイムで収集できる

**Amazon RedShift**

* Data warehouseとデータレイクをサポートする分析用サーバー

**Amazon EMR**

* 保存されたデータを分類して分析するサービス提供

**Amazon CloudSearch**

* 大量のデータを検索できるサービスで、情報をモバイルに配信できる

**Amazon SES (Simple Email Services)**

外部に大量のメール送信サービス

**Amazon Elastic Transcoder**

* 動画エンコードをサポートするサービス

**AWS Well-Architected及び6大原則**

1. 運用の優秀性の原則 : システムの実行と監視に関するプロセスと手順を改善する
2. セキュリティ原則 : データの機密性と整合性、ユーザー権限の管理、セキュリティ イベントの検知のための設定を提供する
3. 安定性原則: 実行するワークロードと要求事項を満たすために迅速に復旧する方法を提供
4. 性能効率性原則: 最適化されたリソース選択および性能モータリング方法を提供
5. 費用最適化原則 : 不必要な費用が発生しないようにする
6. 持続可能性の原則: クラウドワークロードの実行が環境に与える環境を最小限に抑える。

**AWSのメリット**

1. 初期投資費用が発生しない : 固定費用を可変費用に代替
2. 運用コストが減少する: 使用した分のコストの支払い、運用コストの削減、規模の経済面へのコスト削減
3. 弾力的運営及び拡張 : 容量を予測せずに必要なだけ拡張可能
4. 速度と敏捷性:必要な時点でインフラを構築、拡張可能
5. 事業を拡大するためには世界中にいくらでも拡大することができる
6. ビジネスに集中してより高い競争力を持つことができる

**AWSの使い方**

1. サイトで使用する
2. AWS CLI(Command Line Interface)使用、個別コマンドの入力を受けて使用
3. SDK(Softward Development Kit)使用、プログラムで連動する時に使用、Node.js、Re-act.jsなどで連携使用可能

**リージョン、アベイラビリティゾーン**

**リージョン**

* AWSで世界中にあるデータセンターの物理的位置

**アベイラビリティゾーン (AZ:Availablity Zone)**

* 論理的データセンターのグループ
* 高い可用性、拡張性の提供、 可用領域間のデータ レプリケーションのサポート

**AWSの料金政策**

1. 使用量に応じてお支払い(pay-as-you-go) :自分が使った分だけお支払い
2. コミットによるコスト削減(Save when you commit) : AWSを削減できる方法で、1~3年期間の約定条件でコストを削減する
3. より多く使用し、より少ない費用を支払う(Payless by using more) : 大量購入割引を通じてコストを削減できるようにする。 使えば使うほど1GBあたりの料金が安くなる

**AWS Cost Management**

使用時の予想を策定し、コストを予測できる機能を提供する

1. AWSコストエクスプローラ(Cost Explorer):コストデータをチャートで提供、クラウドユーザーの購入タイプ、購入オプションなどを含め、将来のコスト予測が可能
2. AWS予算:費用及び使用量の追跡、 AWS予算を使用して予約インスタンスも貯蓄計画(Saving Plan)に対する集計使用量などをモニタリング
3. 適正サイズの推奨事項:コストエクスプローラの機能で、適正サイズの推奨事項の機能はEC2でインスタンスを縮小または終了し、コスト削減要素を識別
4. 適正サイズの推奨事項:EC2でインスタンスを縮小または終了してコスト削減要素を識別する
5. 貯蓄計画(Saving Plan):柔軟な料金モデルを提供、最大72%のコスト削減が可能

**6 EC2(Elastic Compute Cloud)**

* AWSが提供するサーバー、すなわちWindowsサーバー、Linuxサーバーなどを仮想化環境で提供する
* EC2内部ストレージは揮発性ストレージ、ファイルストレージサービスの使用が必要

**EC2インスタンスタイプ**

* **T.Mシリーズ** : 汎用インスタンスを意味、Webサイト、Webアプリケーション、マイクロサービスに利用可能
* **Cシリーズ**:複数のCPUを搭載したサーバ、Webサーバ、バッチ処理、科学的分析に使用可能
* **Rシリーズ**: メモリ最適化を実行するコンピューティング
* **I.Dシリーズ**:ストレージ最適化を実行するサーバー
* **Gシリーズ**:GPU最適化を実行するサーバー

**インバウンド/アウトバウンド**

* AWSのセキュリティグループ（security Groups）は、ファイアウォールのような役割
* インバウンドは外部からAWSに入るデータの意味
* アウトバウンドAWSから外部に出るデータ統制

**7 RDS : Relation Database Service**

* AWSで提供するリレーショナルデータベースサービスである。 企業で使用される顧客データ管理、取引データ管理などに活用されるデータベースである。
* MariaDB、MySQL、Microsoft SQL Server、Oracle PostgreSQの関係型データベースを提供し、Auroraデータベースも提供する。

**Amazon Aurora 特徴**

* Enterprise級リレーショナルデータベース
* MySQL, PostgrSQL 互換
* 標準MYSQLデータベースより最大5倍速い
* Amazon S3で継続的バックアップ
* 遅延時間が短い読み取り専用レプリカを最大15まで構成可能

**AWSデータベースサービス**

* **RDS** :テーブル形式でSQLをサポートするリレーショナルデータベース
* **DynamoDB** : 非関係型データベースサービス、NoSQLサービス
* **RedShift** : データウェアハウスサービス
* **DocumentDB** : Mongo DBと互換可能なデータベースサービス
* **Nepture** : グラフデータベース

**アクセス**

* Public Access:インターネットを通じて直接RDSに接続
* Private Access:AWS内部でのみ接続可能

**8 S3**

**ストレージ·サービス**

EBS(Elastic Block Store) S3, EFS(Elastic File System) などがある。 EC2生成時にあるストレージはインスタンスストアで揮発性である

**EBS(Elastic Block Store)**

* インスタンス用の永久ブロックストレージを提供
* 複製によりデータを保護
* 異なるドライブタイプを提供
* 数分で拡張縮小可能
* スナップショット機能提供
* SSD、ハードディスクドライブ提供

**2S3 (Simple Storage Service)**

* いつでもどこでも希望するデータを保存·検索できるサービス、データストレージインフラを提供
* バケット内のオブジェクトとして保存、単一オブジェクト1つは最大5TB制限
* 99.99...%の可用性を提供
* バケットおよびオブジェクトの細分化アクセスが可能
* S3はインターネットクラウドストレージで、S3を使用するためには一つのリージョンにバケットを作り、バケットにオブジェクトをアップロードしなければならない

**S3ストレージクラス**

* S3 Standard : 3つ以上の利用可能領域
* S3 Standard Infrequent Access(IA) : オブジェクトに関連する検索コストの発生、頻繁にアクセスしないデータに適している
* S3 Intelligent – Tiering :アクセスパターンを使用して階層間オブジェクトを自動的に移動、 3つ以上の利用可能領域
* S3 One Zone IA :1つの利用可能領域でS3 Standard Infrequent Access(IA)より約20%安い
* S3 Glacier :リアルタイムアクセスがサポートされていないため、リアルタイムにするにはまず復元、オブジェクト復元に1分~12時間かかります
* S3 Glacier Deep Archive : 長期保管のための最低費用ストレージ、3つ以上の利用可能領域、12時間以内の検索に対応
* Glacier : 長期間データを保管するための安価なストレージサービス
* 3~5時間または12時間以内に復旧可能、医療情報アーカイブ、コンプライアンスアーカイブ、科学的データストレージ、マグネチックテーブルの代替

**9 VPC**

**Virtual Private Cloud**

* AWS で使用できる仮想ネットワークである。 つまり、AWSで他の仮想ネットワークと論理的に分離·管理される
* AWS を使えば一つのVPC、インターネットゲートウェイ、ルーティングテーブル、サブネットは存在する。 これをデフォルトVPC という。

**VPCの核心概念**

* Subnet : VPCのIPアドレス範囲でVPC内でネットワークを分離する単位
* ルーティング テーブル: サブネットに接続され、ネットワーク トラフィックを配信する
* インターネットゲートウェイ: VPCと接続され、VPC内のネットワークとインターネットを接続する際に使用
* NACL(Network Access Control) : VPCからサブネット単位でネットワークのインバウンドトラフィックとアウトバウンドトラフィックを制御するファイアウォール機能
* CIDR:サブネットマスクの値を簡単に表示する表記法

**VPC構成**

VPC生成 -> サブネットを作って -> サブネットをVPCに接続 -> サブネットをルーティングテーブルに登録 -> インターネットゲートウェイ生成 -> VPCに登録

**10. IAM**

**Identity and Access Management**

* AWSが提供する資源(Resource)を安全に管理するためのアクセス制御サービス、すなわちユーザーグループ生成、ユーザー生成、権限マッピングなどを通じてアクセス制御を遂行
* グループ(Group):多数のユーザーを束ねて役割を付与
* ユーザー(User):特定のグループに所属して役割を付与
* ポリシー（Policy）:グループに付与される役割
* 役割(Role):権限

**11. ELB, Auto Scaling**

**ELB(Elastic Load Balancing)**

* ネットワーク装置の中でL4スイッチの役割をするAmazon AWSサービスでEC2インスタンスの負荷を調節する。 L4 スイッチというのはラウンドロビン方式でサービスを分散して呼び出すことである。
* ラウンドロビン : AサーバーとBサーバーがある時にAを一度呼び出して、その次にB、そしてまたAを呼び出す方式で使用
* Application Load Balancer : OSI 7階層、流れを妨げない状態で動的にサービスを追加可能
* Network Load Balancer : OSIの4階層であるネットワーク階層で動作するサービスで、複数の利用可能領域間でトラフィックを分散する
* Classic Load Balancer : 複数の利用可能領域で複数のEC2 インスタンスのトラフィックを分散することで、異常なインスタンスを感知し、正常なインスタンスにのみトラフィックをルーティングする。 HTTP、HTTPS、TCP、SSLをすべてサポート
* Galeway Load Balancer : 他社の仮想アプライアンスと統合して使用でき、次世代ファイアウォール、ウェブファイアウォール、侵入探知および侵入防止システムなどを一緒に使用できる、Auto Scalingと共に作動して最適化されたリソースを使用できるようにする。

**Auto Scaling**

* EC2 インスタンスに負荷が発生するのは、自動的にEC2 インスタンスを拡張して負荷を処理できるサービスである
* Auto Scalingグループは複数のEC2インスタンスを生成し、最小インスタンス数を指定することができる。
* システムに負荷が発生すると、自動的にインスタンスを増加させ、負荷を減少させる
* Auto Scalingを使うためにはELBが必要

**Auto Scaling構成要素**

* グループ:EC2 インスタンスを管理する論理的単位、グループは最小インスタンス数と最大インスタンス数を指定
* 構成テンプレート:EC2インスタンスのAMI(Amazon Machine Image)ID、インスタンスタイプ、キーペア、セキュリティグループ、ブロックデバイスマッピングなどの情報を指定
* 調整オプション:EC2インスタンスを拡張するためのオプションを設定、どのような条件のときにインスタンスを拡張するかを決定