AWS Architecture Design

本架构建议使用亚马逊 AWS 云计算产品和服务，能够满足初创公司当前和未来快速发展的需求。AWS 创新的业务模式让初创公司获得解放，能够快速扩展，让产品更快上市，同时控制成本并保持公司规模精简不臃肿。

概述

客户当前的 LAMP 架构搭建在桌面 PC 上，必须在可管理性、安全性、可扩展性、高性能、弹性伸缩、高可用性、灾难恢复等方面综合考虑，才能应对未来业务快速发展的需求。

初期的架构要做到简单、灵活、高效，满足业务和需求的经常性变化，通常成本是很重要的一个因素。使用 AWS 的 EC2 弹性云计算服务器，根据业务需要购买计算能力，让投资发挥最大效益。

在业务高速发展阶段，服务器需求也随之增长，AWS 的可扩展架构通过自动添加计算资源满足业务高峰的需求。在业务高峰度过后，又可以释放多余的计算资源。

AWS 让客户专注于业务设计、开发，无需费时费力的考虑服务器选型、采购、部署，网络，防火墙，安全等方面的问题，甚至无需为 IT 设备的维修、维护、监控等问题分神费力。

假定

为简化复杂度，本方案基于以下假定和条件：

典型的服务器结构分为三层，分别是：Web Server， App Server， Database Server。如果是初期仅运行 PHP 程序，则可以修改为两层，Web Server 和 App Server 合为一层。

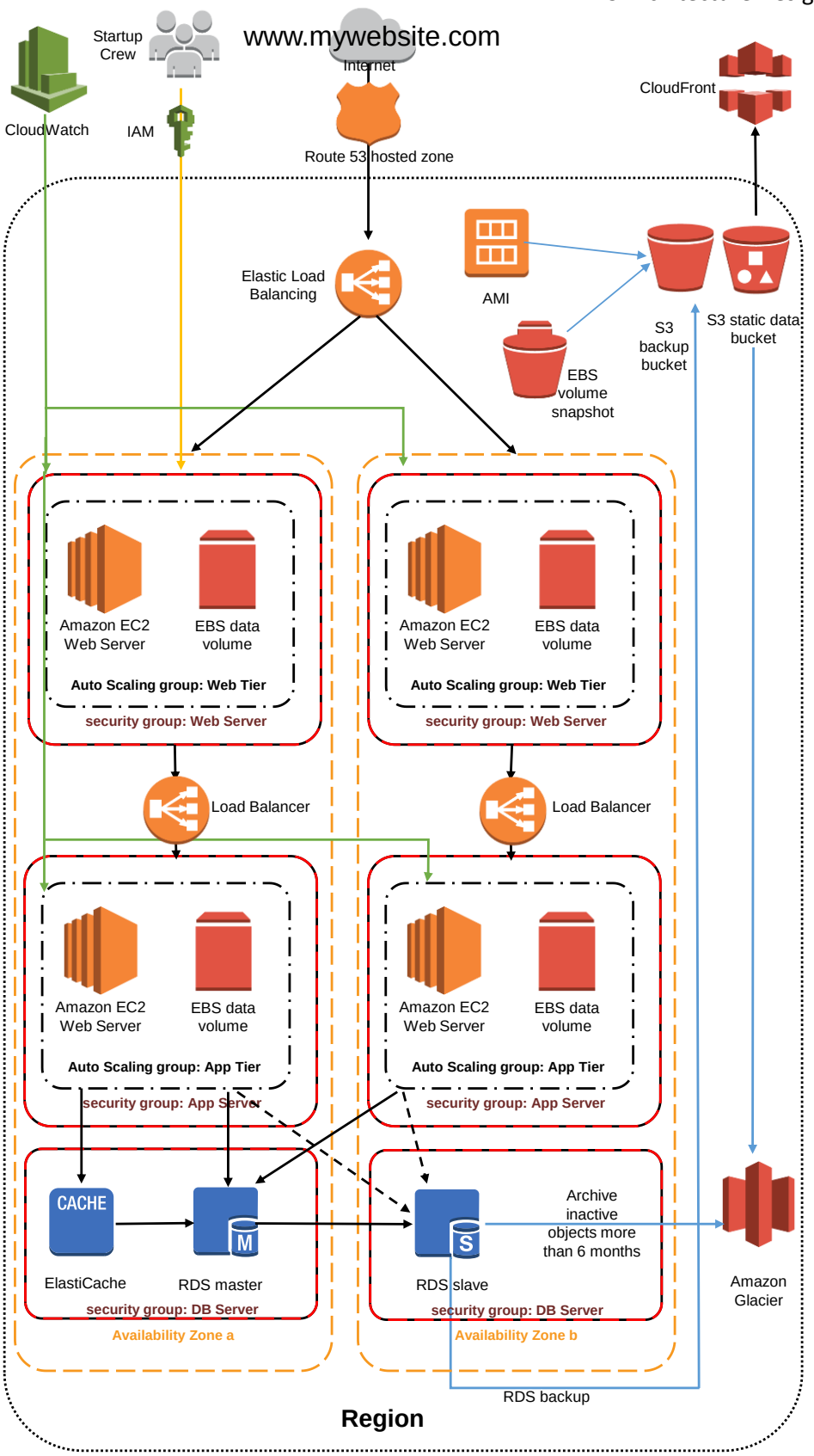
没有海量数据的查询和并发访问，如果需要可以使用 NOSQL，如 DynamoDB。

没有考虑数据仓库计算需求，如果有，可以选择 RedShift、EMR 等产品。

没有需要长时间运行的任务，如果需要可以使用 SQS 消息队列、SNS 通知服务等产品。

架构

根据客户需求和未来发展的需要，为其设计的架构如下图所示：



在这个架构中使用到的 AWS 服务有：

首先，Amazon VPC 将内部资源与外部网络隔离。为可访问 Internet 的 Web Server 创建公有子网，而将 Database Server、AppServer 等后端系统放在不能访问 Internet 的私有子网中。

利用 Security Groups 和网络访问控制列表等多种安全层，帮助对各个子网中 Amazon EC2 实例的访问进行控制。

对于 web 访问的客户，由 AWS Route 53 提供外部 DNS 服务。对于公司员工，通过 Direct Connect、VPN、IAM 认证访问 AWS，CloudTrail 可用于安全审计。

CloudFront 进行内容分发 CDN，缓存常用的静态、动态文件，实现低延迟、高速数据传输。

Elastic Load Balancer （简称 ELB）在云中的多个 Amazon EC2 实例间自动分配应用程序的访问流量。它可以让您实现更高水平的应用程序容错性能，把业务请求分发到多个 Availability Zone（简称 AZ）的 Web Server 上。

EC2 为 Web Server、App Server、DB Server 提供计算资源。EC2 提供大小可调的计算容量。

对于不同应用服务器可以定制各自的 AMI 镜像，实现服务器的快速安装、部署。

Auto Scaling 实现 EC2 的自动伸缩。Auto Scaling 组可以包含来自相同地区的一个或多个 EC2 可用区域的 EC2 实例。

借助 Amazon CloudWatch，您可以全面了解整个系统的资源使用率、应用程序性能和运行状况。使用这些分析结果，您可以及时做出反应，保证应用程序顺畅运行。

Elastic Block Store（简称 EBS）为 EC2 提供数据持久化存储。

Security Groups 设计的安全策略可以确保允许的网络访问。

使用 ElastiCache 作为缓存，可以提供更快的 Web 应用程序响应。

MySQL 数据库使用 RDS 服务（MySQL 或 Aurora），数据文件存储到 EBS 上。数据库部署到不同的 AZ，进行主、从复制，实现高可用和读写分离。

EBS volume Snapshot、AMI 的备份，都可以存储在 S3 上。S3 同时也存储了静态的数据和对象。

数据库、历史数据、归档数据的备份使用 Glacier 完成。

使用 CloudFormation 创建模版，方便部署 AWS 资源和应用。

AWS OpsWorks 应用程序管理服务，便于部署和操作不同形态和规模的应用程序，如 PHP 应用。

解决的问题

针对客户关心的问题，AWS 有如下的支持：

Scaling to meet the demand

在 Web 层和 App 层上的 Auto Scaling group 可以分别按需扩展和收缩。Auto Scaling 既适合需求稳定的应用程序，同时也适合每小时、每天、每周使用量不停波动的应用程序。在 Auto Scaling 中使用 AMI 可以简单的添加新的 EC2 实例。数据库的扩展可以手工进行数据分区、分片，或者迁移到 DynamoDB 上实现自动扩展。

Their lack of provision for Disaster Recovery

在上图的 AWS 架构中，有 2 个可用 AZ，数据库有跨 AZ 的主从复制，确保一个 AZ 出问题的时候， ELB 会对访问请求进行分发，这都是自动化的，对最终用户没有感知，在故障 AZ 恢复后，ELB 可以重新把用户路由到恢复的 AZ。

使用 EBS 存储的 data volume，在 EC2 故障时，也可以确保 EBS 上的数据安全。

当 RDS 切换到 slave 时，ElastiCache 可以连接到 slave 继续服务。

Their ability to configure their database and data access layer for high performance and throughput

EC2 可以随时调整配置满足数据库性能需求。RDS 配置了主、从复制，可以实现读写分离，分担数据库的访问压力。前端还有 ElastiCache 作为缓存，也可减少对数据库的读请求。这些都可以提升数据库的性能和吞吐量。

Making the user experience in the browser very low latency even though a large portion of their user base will be from far away

AWS 有遍布全球的 region，可以满足就近访问的需求。AWS Route 53 可以把用户请求路由到最近的服务器。配备 CloudFront 和 S3 可以对静态数据提供低延迟的访问。Web Server 配备高 IOPS 性能的 EBS 也可以提升响应速度。

Effective distribution of load

在 Web Server 前端的 ELB 可以做到将用户请求均衡到不同的 Web Server 上。在 App Server 前端也有负载均衡可以把应用请求分配到不同的 App Server 上。

大部分静态内容的访问由 CloudFront 承担，减轻了 Web 层、App 层和 DB 层的压力。

A self-healing infrastructure that recovers from failed service instances

ELB 会检查 EC2 实例的健康情况，将他们移除或移入。当 CloudWatch 发现有问题的 instance，Auto Scaling 会根据规则增加新的 instance 消除资源不足的影响。跨 AZ 部署的 RDS，数据库可以自动 failover 到 slave instance 。

Security of data at rest and in transit

每个 EC2 的 Security Groups 可以设置不同的访问策略，比如只允许访问服务器的 80/443 端口，对于数据库只允许访问数据库主机的 3306 端口。VPC 把内部资源与外部网络隔离。设置 IAM 进行网络访问控制和授权。传输数据可以使用 SSL 加密传输。

securing access to the environment as the delivery team expands

所有内部员工的访问均需要有 IAM 授权，CloudTrail 用于安全审计。在 VPC 里，可以把 App Server 和 DB Server 设置为内网访问，进行安全隔离和访问控制，提升安全性。

An archival strategy for inactive objects greater than 6 months

Glacier 可以按照 S3 里设定的规则把静态数据和数据库里的历史数据归档，把 6 个月以上的非活动数据备份。

Ability to easily manage and replicate multiple environments based on their blueprint architecture

AWS OpsWorks 可以定义应用程序的架构和每个组件的规范（包括软件包安装，软件配置和存储等资源）。使用 CloudFormation 可以将现有的 AWS 资源定义为模版，通过定制或修改模版，可以轻松复制出多个环境，用于不同用途。

综上，使用 AWS 可伸缩的产品和服务，可以帮助初创公司构建可管理的、安全的、高可用、可扩展的、经济实惠的 IT 架构，让客户无后顾之忧，满足公司当前和未来发展的需要。