Job Search Tool

Infrastructure Solution Design Document 1

**Revision history**

Describe the changes made and the reason for the change between the revisions.

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision** | **Date** | **Description of changes** | **Author** |
| P1.0-1 | 2016-09-12 | Created draft version | Sivarajan Chitraikani |

|  |  |
| --- | --- |
| **Reviewed/Approved** | **Name** |
| Yes/No |  |

Table of Contents

[Job Search Tool 1](#_Toc461613306)

[Infrastructure Solution Design Document P1.0-1 1](#_Toc461613307)

[1 Introduction 4](#_Toc461613308)

[1.1 Purpose of the document 4](#_Toc461613309)

[1.2 Intended audience 4](#_Toc461613310)

[1.3 Definitions, Acronyms, and Abbreviations 4](#_Toc461613311)

[1.3.1 Definitions 4](#_Toc461613312)

[1.3.2 Acronyms and Abbreviations 4](#_Toc461613313)

[1.4 References 5](#_Toc461613314)

[1.5 Functions 5](#_Toc461613315)

[1.6 Detailed design process 5](#_Toc461613316)

[1.7 Caveats and Limitations 5](#_Toc461613317)

[2 CONCEPTUAL DESIGN 6](#_Toc461613318)

[2.1 Conceptual Application Design 6](#_Toc461613319)

[2.1.1 Application Context 6](#_Toc461613320)

[2.2 Conceptual Infrastructure Design 6](#_Toc461613321)

[2.2.1 Components 7](#_Toc461613322)

[2.3 Current Operational Model 8](#_Toc461613323)

[2.3.1 Constraints 8](#_Toc461613324)

[2.4 Target Operational Model 9](#_Toc461613325)

[2.4.1 Automation 9](#_Toc461613326)

[2.4.2 Authentication and Authorization 9](#_Toc461613327)

[3 DETAILED DESIGN 10](#_Toc461613328)

[3.1 AWS Account 10](#_Toc461613329)

[3.2 Network 10](#_Toc461613330)

[3.3 DNS 10](#_Toc461613331)

[3.4 Access 10](#_Toc461613332)

[3.5 Security 10](#_Toc461613333)

[3.5.1 AWS Virtual Private Network (VPC) 10](#_Toc461613334)

[3.5.2 AWS Identity and Access Management (IAM) 10](#_Toc461613335)

[3.5.3 AWS Amazon Linux 10](#_Toc461613336)

[3.6 Scalability 11](#_Toc461613337)

[3.7 Manageability 11](#_Toc461613338)

[3.7.1 AWS CloudTrail 11](#_Toc461613339)

[3.7.2 AWS CloudWatch 11](#_Toc461613340)

[3.7.3 AWS Config 12](#_Toc461613341)

[3.8 Integration 12](#_Toc461613342)

# Introduction

## Purpose of the document

The purpose of this document is to specify the high-level design for the

Job Search Tool Redesign solution. This document acts as a map for the implementation of the solution. It also provides descriptions for the major components

## Intended audience

This section shall specify the intended audience (Steering Committee, System Administrators, Project Managers, Programmers, etc.) and suggest how they should use it. It shall also specify skills required to fully benefit from the document. Intended audience is technicians responsible for doing installation and configuration of the Intermediate Basic ecommerce Solution on the Amazon Web Services platform.

## Definitions, Acronyms, and Abbreviations

### Definitions

|  |  |
| --- | --- |
| **Term** | **Description** |
| Cloud Delivery Team | Initial team of resources in IKEA who will act as the receiving group for the Pilot |
| Function | A capability of the solution, available for activation either by the user or  as a response to an event. All functions respond to an input and produce an output. |

### Acronyms and Abbreviations

|  |  |  |
| --- | --- | --- |
| **Term** | **Short form for** | **Description** |
| COM | Current Operating Model | The current or As-Is view |
| TOM | Target Operating Model | The To-Be view |
| AWS | Amazon Web Services | Amazon Web Services is a collection of  remote computing services that make up  a cloud-computing platform offered by  Amazon.com. |
| EC2 | Elastic Compute Cloud |  |
| EB | Elastic Beanstalk |  |
| ELB | Elastic Load Balancing |  |
| VPC | Virtual Private Cloud |  |
| S3 | Simple Storage Service | Amazon S3 is used to store and retrieve any amount of data at any time, from anywhere on the web using the simple and intuitive web interface of the AWS Management Console |
| Route 53 |  | Amazon Route 53 is a scalable Domain  Name System (DNS) web service |
| IAM | Amazon Identity and Access  Management |  |
| WAF | Web Application Firewall |  |

## References

|  |  |  |
| --- | --- | --- |
| **Ref.** | **Name / Title / Description** | **Link** |
| 1 | AWS documentation | http://aws.amazon.com/documentation/ |
| 2 | AWS Elastic Beanstalk | http://docs.aws.amazon.com/elasticbeanstalk/latest/dg/W  elcome.html |

## Functions

The solution includes the following components and functions.

|  |
| --- |
| Supported functions |
| Amazon Linux |
| CloudTrail |
| CloudWatch |
| Elastic Beanstalk |
| EC2 |
| IAM |
| Intermediate Basic eCommerce Solution |
| RDS |
| Route53 |
| VPC |
| S3 |
| VPN connectivity to IKEA Corporate Network |

## Detailed design process

After the high level design of the solution has been completed, CDT focuses on the detailed level of the design. The following steps are conducted:

First a conceptual design is made, then the team discusses which patterns could be used to enhance the design, the patterns we are talking about regarding this solution is about security and connectivity.

## Caveats and Limitations

The current design is not definitive and by no means an enforcing design. It is manufactured based on initial requirements. We, from **IKEA IT Cloud Services**, would like to see the design evolves over time and that the Target model is reached.

# CONCEPTUAL DESIGN

This section of this document provides details about the following topics:

* Conceptual Application Design
* Conceptual Infrastructure Design

## Conceptual Application Design

Conceptual application design offers an overview of core functional components in the Job Search Tool Redesign Solution. Its focus is on logical design and its included components and subcomponents

### Application Context

The following figure represents a high-level context in which the solution will exist

## Conceptual Infrastructure Design

The Conceptual Infrastructure Design for Job Search Tool Solution will be supported by AWS services to securely host production and test environments. Job Search Tool Solution will be hosted on AWS and the application itself will be portable in that it is containerized and will not be dependent on the underlying AWS specific infrastructure (except AWS S3). AWS S3 can be easily replaced with FTP.

To support Job Search Tool Solution; AWS infrastructure will incorporate the following design components: Elastic Beanstalk, RDS, EC2instances, VPC, S3, Security Groups and Roles.

The following diagram shows an architectural overview over the solution

### Components

The previous view is on a high level; this section describes the individual components in more detail

#### Public Network

The public network is actually divided in three subnets, one in each availability zone. This subnet has an internet gateway configured and all resources residing here is reachable over the internet.

***Amazon S3 (Simple Storage Service)***

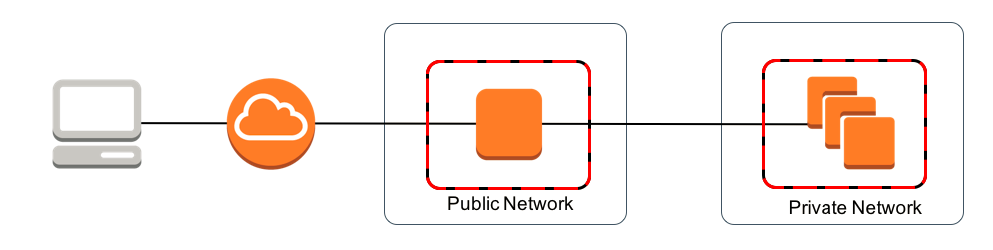
S3 buckets are accessible over internet for uploading files. The files uploaded will be used by programs running in Amazon Beanstalk worker environment

***WEB SERVER – LOAD BALANCER***

The load balancer is placed in the public subnet across multiple availability zones. It has public visibility, i.e. external IP address.

***JUMP HOST***

This is the logical design of the Jumphost running Amazon Linux. It is included in an auto scaling group with minimum one instance and maximum of one, by doing this we have a “cold standby” which starts immediately after a failure.



#### Private Network

The private network is also divided in three subnets, one in each Availability Zone. This network is not accessible from the Internet, but there is a routing table in place allowing traffic towards the VPN.

***WEB SERVER***

AWS Beanstalk Web Server is used for hosting JST Web Application. AWS Beanstalk Web Server runs in 64bit Amazon Linux 2016.03 v2.1.3 running Tomcat 8 Java 8

***Worker Environment***

AWS Beanstalk Worker Environment is used for hosting JST Batch Application. AWS Beanstalk Worker Environment runs in 64bit Amazon Linux 2016.03 v2.1.3 running Java 8

***DATABASE SERVER (RDS)***

AWS RDS with MySql V5.6.27 is used as database for JST

## Current Operational Model

### Constraints

The creation of the infrastructure is manual work; it should be migrated to an automated setup using CloudFormation or with scripts that utilizes the AWS SDK.

## Target Operational Model

TOM is the recommended to-be view of the solution

### Automation

Create scripts for common tasks on AWS, Beanstalk Application setup and for deploying new versions of the application. Maven build scripts are capable are producing deployable packages.

### Authentication and Authorization

The internal url of the microsite should use the AuthApp from

AkamaiCDN-TS to authenticate IKEA co-workers in order to have authenticated access to internal jobs

# DETAILED DESIGN

This chapter will go through the components and patterns involved, how they are designed and how to implement them (for the solution).

## AWS Account

An account has been created and added to the IKEA Consolidated billing account.

## Network

Amazon Virtual Private Cloud (Amazon VPC) enables us to launch AWS resources into a virtual network that we’ve defined.

## DNS

The URL will be

External Users (Available for all users in the Internet)

[https://ww8.ikea.com/ext/job/search/external/[country\_code]/[language\_code]/home](https://ww8.ikea.com/ext/job/search/external/%5bcountry_code%5d/%5blanguage_code%5d/home)

For Internal Users (Available for IKEA Co-workers only)

[https://ww8.ikea.com/ext/job/search/internal/[country\_code]/[language\_code]/home](https://ww8.ikea.com/ext/job/search/internal/%5bcountry_code%5d/%5blanguage_code%5d/home)

country\_code and language\_code are changeable according to the supported regions

## Access

Access to the AWS console is handled by IAM roles. Access is also enabled for users on the AWOT AWS Account via a federated mechanism. The user management is done using IKEA IT central Identity and Access Management, this is realized integrating the AWS console with IKEA IT ADFS.

## Security

|  |
| --- |
| The AWS cloud security infrastructure has been architected to be one of the most flexible and secure cloud computing environments available today. It provides an extremely scalable, highly reliable platform that enables customers to deploy applications and data quickly and securely. See http://aws.amazon.com/security/ for more information. |

### AWS Virtual Private Network (VPC)

|  |
| --- |
| Amazon VPC provides advanced security features such as security groups and network access control lists to enable inbound and outbound filtering at the instance level and subnet level.See http://aws.amazon.com/vpc/ for more information |

### AWS Identity and Access Management (IAM)

|  |
| --- |
| AWS Identity and Access Management (IAM) enable you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources. See http://aws.amazon.com/iam/ for more information. |

### AWS Amazon Linux

|  |
| --- |
| The Amazon Linux AMI is a supported and maintained Linux image provided by Amazon Web Services for use on Amazon Elastic Compute Cloud (Amazon EC2). It is designed to provide a stable, secure, and high performance execution environment for applications running on Amazon EC2. It also includes packages that enable easy integration with AWS, including launch configuration tools and many popular AWS libraries and tools. Amazon Web Services provides ongoing security and maintenance updates to all instances running the Amazon Linux AMI. The Amazon Linux AMI is provided at no additional charge to Amazon EC2 users.See http://aws.amazon.com/amazon-linux-ami/ for more information. |

#### Access

No direct access to the underlying server(s) is needed. Although, when creating

the Beanstalk Application, it offers the user to enter an EC2 key pair for remote access. The Jump Host can be used for accessing the servers. Note that this contradicts the purpose of a PaaS and should be avoided.

#### Updates

The environment will be fully cycled to the latest release of Amazon Linux in a rolling fashion, either when new releases of Amazon Linux comes out or when the environment is rebuilt. Both scenarios are initiated from the user.

## Scalability

Job Search Tool utilizes AWS Auto Scaling functionality, Auto Scaling is a web service designed to launch or terminate Amazon EC2 instances automatically based on user-defined policies, schedules, and health checks. Auto Scaling is enabled by default when deploying on Elastic Beanstalk. It scales on Network Out traffic. When the CloudWatch metric on your environment for Network-Out exceeds 6000000 (≈5.7MB) bytes in a 5-minute period, AutoScaling will launch a new EC2 instance. When Network-Out is below 2000000 (≈1.9MB) AutoScaling will remove an EC2 instance (unless you are already at your min-size of instances).

## Manageability

AWS and Elastic Beanstalk offer straightforward manageability with an easy to

use web interface and good documentation. For example, updating the

Job Search Tool Solution Beanstalk Application is a one pushbutton operation.

### AWS CloudTrail

|  |
| --- |
| AWS CloudTrail is a web service that records AWS API calls for your account and delivers log files to you. The recorded information includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters, and the response elements returned by the AWS service. With CloudTrail, you can get a history of AWS API calls for your account, including  API calls made via the AWS Management Console, AWS SDKs, command line tools, and higher-level AWS services (such as AWS CloudFormation). The AWS API call history produced by CloudTrail enables security analysis, resource change tracking, and compliance auditing. See https://aws.amazon.com/cloudtrail/ for more information. |

### AWS CloudWatch

|  |
| --- |
| Amazon CloudWatch is a monitoring service for AWS cloud resources and the applications you run on AWS. You can use Amazon CloudWatch to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in your AWS resources.  See https://aws.amazon.com/cloudwatch/ for more information. |
| The Beanstalk Source Bundle has been configured to extract several application and OS logfiles to a Log Group named after the Beanstalk environment name. |

### AWS Config

|  |
| --- |
| AWS Config is a fully managed service that provides you with an AWS resource inventory, configuration history, and configuration change notifications to enable security and governance. This service has been enabled for Intermediate Basic eCommerce Solution. See https://aws.amazon.com/config/ for more information. |

## Integration