OBSS SUMMER INTERN(HRMS Uygulaması) - Üst Seviye Tasarım Dokümanı

1. Doküman Tanımı ve Amaç:

Bu belge, HRMS (Human Resource Management System) kullanıcıların iş ilanlarına başvurmasını sağlayan bir profesyonel ağ uygulamasıdır. Uygulama, kullanıcıların OBSS şirketinin açtığı iş ilanlarına başvurabilmesini, insan kaynaklarının da ilan oluşturup ilanları, başvuruları ve kara listeyi yönetebilmesini sağlar.

2. Fiziksel Deployment ve Mantıksal Tasarım Diyagramı:

metin, ekran görüntüsü, yazılım, sayı, numara içeren bir resim

Açıklama otomatik olarak oluşturuldu

3. Çözüm Mimarisi:

Veritabanı: MongoDB kullanılarak, kullanıcı profilleri, iş ilanları ve diğer ilgili veriler depolanır.

Arama Motoru: ElasticSearch, serbest metin aramasını desteklemek için kullanılır.

Kimlik Doğrulama ve Yetkilendirme: LDAP (Lightweight Directory Access Protocol), kullanıcı kimlik doğrulama ve rol tabanlı yetkilendirmeyi sağlar.

Kimlik ve Yetki Yönetimi: JWT (JSON Web Token), kimlik doğrulama ve yetkilendirmeyi diğer sistemlerle entegre etmek için kullanılır.

LinkedIn Entegrasyonu: OAuth2 protokolü kullanılarak, kullanıcıların LinkedIn hesaplarıyla giriş yapmaları ve yetkilendirme yapmaları sağlanır.

Güvenlik ve Rol Kontrolleri: Spring Security, kimlik doğrulama ve yetkilendirme işlemlerini yönetir.

Servislere Bağlanma: çoklu servis uygulamalarını yönetir.

4. Bileşen Açıklamaları:

Veritabanı Bileşeni: MongoDB, kullanıcı profillerini, iş ilanlarını ve uygulama verilerini saklar.

Arama Motoru Bileşeni: ElasticSearch, serbest metin aramasını hızlı ve etkili bir şekilde gerçekleştirir.

Kimlik Doğrulama ve Yetkilendirme Bileşeni: LDAP, kullanıcı kimliklerini doğrular ve rolleri yönetir.

Kimlik ve Yetki Yönetimi Bileşeni: JWT, kullanıcı kimlikleri ve yetkileri için token tabanlı bir çözüm sunar.

LinkedIn Entegrasyon Bileşeni: OAuth2 ile LinkedIn hesaplarına erişim sağlar ve kimlik doğrulama işlemini yürütür.

Güvenlik ve Rol Kontrolleri Bileşeni: Spring Security, uygulama güvenliğini sağlar ve rol tabanlı yetkilendirmeyi yönetir.

Mail Gönderme Bileşeni: Java Mail Sender, istenen koşullarda kullanıcıya e-posta göndererek kullanıcının bilgilendirilmesini sağlar

Servislere Bağlanma Bileşeni: Docker; projeye ElasticSearch, MongoDB gibi yapıları bağlayarak birlikte çalışılabilirliği arttırmak ve hızlı bir şekilde projeyi ayağa kaldırmak için kullanılmıştır.

5. Mimari Kararlar ve Gerekçeleri:

MongoDB Seçimi: Esnek veri modeli imkanı sağlaması sayesinde proje büyüdükçe yeni alanlar veya belirli alanlar içeren belgeler eklemek kolay olduğundan ve verileri BSON formatında sakladığı için veri okuma ve yazma işlemlerinde yüksek performans sunduğundan dolayı MongoDB seçildi

ElasticSearch Kullanımı: Serbest metin aramasını hızlandırmak ve optimize etmek ve daha önce kullanmadığımdan denemek istediğim için ElasticSearch seçildi.

LDAP Kullanımı: Kurumsal kimlik doğrulama ve yetkilendirme için LDAP tercih edildi.

JWT Kullanımı: Çeşitli sistemler arası kimlik doğrulama ve yetkilendirme işlemlerini kolaylaştırmak için JWT kullanıldı.

LinkedIn OAuth2: Kullanıcıların LinkedIn hesaplarıyla giriş yapmalarını ve uygulamaya erişim sağlamalarını kolaylaştırmak için LinkedIn OAuth2 entegrasyonu tercih edildi.

Spring Security: Güvenlik ve rol tabanlı yetkilendirmeyi sağlamak için Spring Security kullanıldı.

Java Mail Sender: Java tabanlı uygulamalarda e-posta gönderimi için güçlü ve esnek bir çözüm oldugundan ve Spring tarafından sağlanan yapılar ve Spring Boot tarafından otomatik yapılandırma sayesinde kolayca kullanılabilir.- olduğundan tercih edildi.

Testlerde Mock Yapısı: Testlerin daha izole olmasını, gerçek bağımlılıklar olmadığından testlerin daha hızlı çalışmasını daha hafif olmasını sağladığından tercih edilmiştir.

Angular: Daha önce geliştiriğim Angular projelerinin olmasından dolayı Angular seçildi.

Bootstrap: Kullanıcı arayüzü tasarımının daha kolay ve efektif olması için seçildi.

6. Ölçeklenebilirlik ve Performans:

Uygulama, ölçeklenebilir tasarım ilkelerine göre geliştirilir.

Veritabanı ve arama motoru ölçeklenebilirlik için yatay olarak genişletilebilir.

7. Güvenlik Tasarımı:

Kullanıcı kimlik doğrulaması ve yetkilendirmesi Oauth2 ile güvenli bir şekilde yönetilir.

Insan kaynaklarının kimlik doğrulaması ve yetkilendirmesi LDAP server ile güvenli bir şekilde yönetilir.

Kimlik bilgileri ve yetkiler, JWT kullanılarak güvenli bir şekilde taşınır.