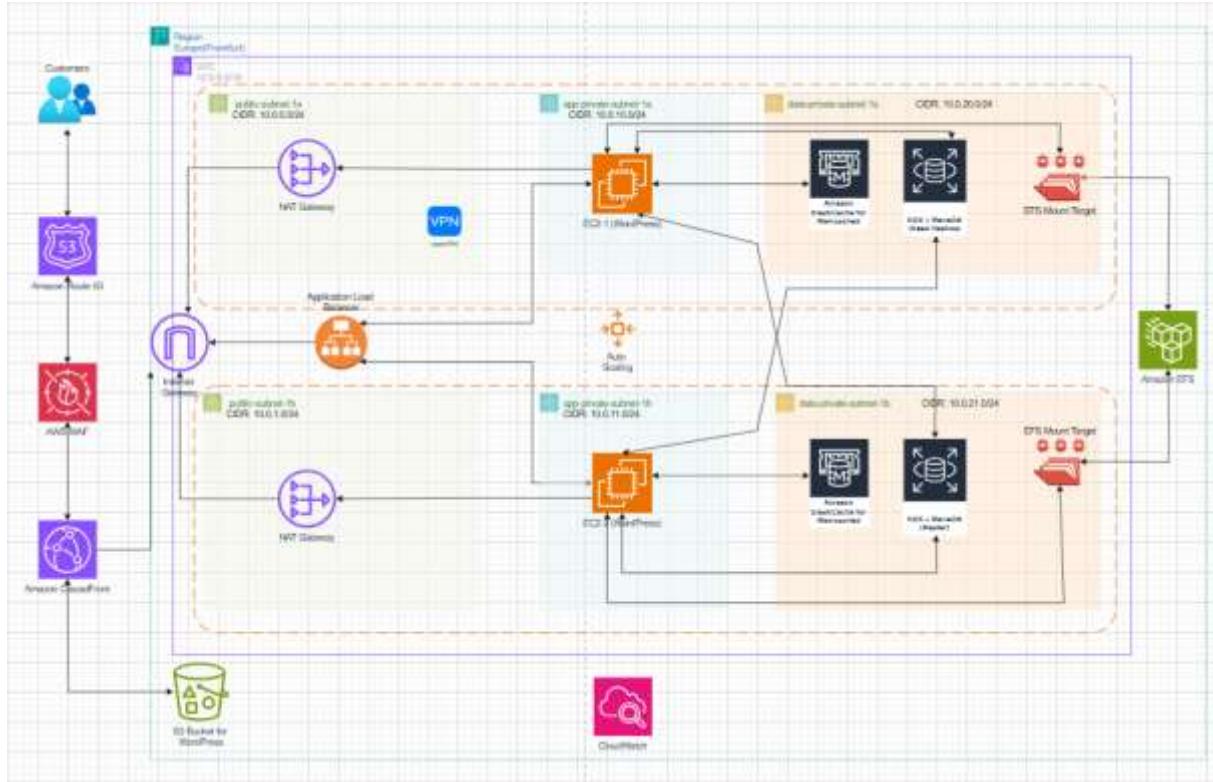


ADİLE AKKILIÇ

21360859052

1. AWS MİMARİSİ



Drawio linki

<https://drive.google.com/file/d/1YAcR3n8cCIO58FxbpfQcbAdGAcsdgtKg/view?usp=sharing>

2. AWS MALİYET



AWS Calculator maliyet hesabı detayları :

<https://calculator.aws/#/estimate?id=1ea76e2a861ba45d5cf847cb9c276552cc5c9de>

<https://calculator.aws/#/estimate?id=1ea76e2a861ba45d5cf847cb9c276552cc5c9de>

3. TEKNİK DETAYLAR

Bu bölümde, hosting-101.com sitesi için AWS üzerinde kurulan bulut altyapısının teknik tasarımını detaylandırmaktadır. Mimari, yüksek erişilebilirlik, güvenlik ve dinamik ölçeklenebilirlik odağında kurgulanmıştır. Sistem; sanal özel ağ yapısı (VPC), alt ağların segmentasyonu, güvenlik bileşenleri ve otomatik ölçeklenme mekanizmalarıyla, trafiği değişken ve saldırı riski yüksek web projeleri için referans bir örnek oluşturmaktadır.

3.1.ONAYLANAN MİMARİ NETWORKÜN DETAYLANDIRILMASI

Sistem, izole bir sanal ağıda (VPC) barındırılmıştır. CIDR bloğu olarak 10.0.0.0/16 atanmış, bu geniş adres aralığı çeşitli alt ağlara bölünerek farklı işlevlerin ayırtılması sağlanmıştır:

Alt Ağ Türü	CIDR Bloğu	Açıklama
Public Subnet 1A	10.0.0.0/24	NAT Gateway, Application Load Balancer, VPN
Public Subnet 1B	10.0.1.0/24	NAT Gateway yedeği
Private Subnet 1A	10.0.10.0/24	EC2 (WordPress), ElastiCache
Private Subnet 1B	10.0.11.0/24	EC2 (WordPress), ElastiCache
Data Subnet 1A	10.0.20.0/24	RDS (MariaDB), EFS Mount
Data Subnet 1B	10.0.21.0/24	RDS (MariaDB), EFS Mount

- Public subnetlerde, NAT Gateway'ler ve ALB (yük dengeleyici) gibi interne açık servisler yer alır.
- Private subnetlerde, sadece iç erişime açık olan WordPress sunucuları ve cache sistemi (ElastiCache) barındırılır.
- Data subnetlerde ise, veritabanı (RDS/MariaDB) ve dosya sistemi (EFS) izole edilmiştir.
- RDS ve EFS, doğrudan internete kapalı olup sadece private subnetten ulaşılabilir yapıdadır.
- EC2 instance'larına doğrudan erişim engellenmiş; kullanıcı istekleri sadece Application Load Balancer (ALB) üzerinden yönlendirilir.

Bu segmentasyon sayesinde, hem güvenlik seviyesi artırılmış hem de kaynakların daha verimli yönetilmesi sağlanmıştır.

3.2.VPC ve CIDR Yapılandırması

AWS altyapısının en kritik unsurlarından biri güvenlidir. Bu projede, farklı katmanlarda şu güvenlik önlemleri uygulanmıştır:

- AWS WAF (Web Application Firewall): Tüm web trafiği önce CloudFront'a, ardından 1 adet Web ACL (Access Control List) ve toplam 10 adet kural grubu (Rule Group) üzerinden filtrelenir. Bu sayede DDoS, XSS ve benzeri saldırılar proaktif olarak engellenir.
- Route 53: DNS seviyesinde akıllı yönlendirme ve güvenlik kuralları uygulanarak istenmeyen isteklerin önüne geçilir.

- ALB (Application Load Balancer): Layer 7 (uygulama katmanı) trafiği şifreli olarak (SSL/TLS) yönlendirilir; bu, veri bütünlüğünü ve gizliliğini sağlar.
- IAM (Identity and Access Management): Her AWS servisine yalnızca gerekli erişim hakları atanmıştır. Gereksiz ayrıcalıklar verilmemiştir (“least privilege” prensibi).
- Security Group & NACL (Network ACL): EC2, RDS ve EFS gibi kaynaklar için ayrı güvenlik grupları oluşturulmuş; sadece gerekli portlara (örneğin 80/443, 3306 vb.) izin verilmiştir. Geri kalan tüm erişimler reddedilmiştir.

3.3. VPC ve CIDR Yapılandırması

VPC için belirlenen 10.0.0.0/16 CIDR bloğu, farklı işlevler için /24'lük subnetlere ayrılmıştır. Her bir /24 subnet 256 IP adresi içerir.

Aşağıda subnetlerin dağılımı ve aralıkları verilmiştir:

Subnet	CIDR Bloğu	IP Arahığı
public-subnet-1a	10.0.0.0/24	10.0.0.0 – 10.0.0.255
public-subnet-1b	10.0.1.0/24	10.0.1.0 – 10.0.1.255
app-private-subnet-1a	10.0.10.0/24	10.0.10.0 – 10.0.10.255
app-private-subnet-1b	10.0.11.0/24	10.0.11.0 – 10.0.11.255
data-private-subnet-1a	10.0.20.0/24	10.0.20.0 – 10.0.20.255
data-private-subnet-1b	10.0.21.0/24	10.0.21.0 – 10.0.21.255

Bu şekilde, ağ kaynakları farklı amaçlar için ayrılmış ve subnetler arası izolasyon sağlanmıştır.