### AWS nedir?

### AWS, dağıtılmış BT altyapısını kullanarak isteğe bağlı olarak çeşitli BT hizmetleri sunan ve esnek, güvenilir, ölçeklenebilir ve uygun maliyetli bulut bilişim çözümleri sunan Amazon Web Services'ın kısaltmasıdır.

## AWS Altyapısı

* AWS Bölgesi, dünyada birden fazla Erişilebilirlik Alanına sahip olduğu fiziksel bir konumdur.
* Erişilebilirlik Alanları, her biri ayrı tesislerde bulunan yedek güç, ağ iletişimi ve bağlantıya sahip bir veya daha fazla ayrı veri merkezinden oluşur.
* AWS Cloud, dünya çapında 25'ten fazla coğrafi Bölgede 80'den fazla Erişilebilirlik Alanında çalışır.



### Uç Konumlar

### Uç konumu, son kullanıcıların AWS'de bulunan ve içeriği önbelleğe almak için kullanılan hizmetlere eriştiği yerdir. Uç konumları, CloudFront ve Route 53 isteklerine hizmet eder.

### AWS Yerel Alanları

### AWS Yerel Alanları, işlem, depolama, veritabanı ve diğer belirli AWS hizmetlerini son kullanıcılara daha yakın bir konuma yerleştirir.

### AWS Ücretsiz Kullanım mı?

### AWS Ücretsiz Kullanımı, müşterilere AWS hizmetlerini her hizmet için belirtilen sınırlara kadar ücretsiz olarak keşfetme ve deneme olanağı sağlar. Ücretsiz kullanımı kullanarak 85'ten fazla ürünü keşfedebilir ve AWS'de oluşturmaya başlayabilirsiniz.

### 

### 

## IAM'ye Giriş

* AWS IAM, Kimlik ve Erişim Yönetimi anlamına gelir ve AWS ortamlarında kimlik doğrulama ve yetkilendirme süreçlerini yöneten birincil hizmettir.
* IAM bileşenleri temel olarak iki terim altında kategorize edilebilir; kimlikler ve izinler.

AWS IAM'de üç kimlik vardır:

1. Kullanıcılar 2- Gruplar 3- Roller

İzinler, kullanıcılara yetkilendirme kullanan farklı ilke türleri olarak tanımlanabilir.

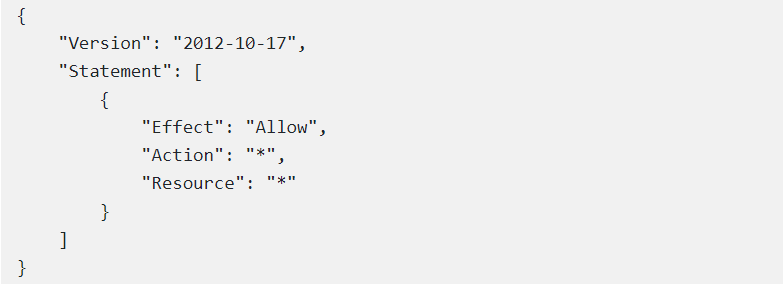
* Koşullarıdır
* AWS'deki bir kullanıcı bir ad, AWS Management Console'da oturum açmak için bir parola ve API veya CLI ile kullanılabilecek en fazla iki erişim anahtarından oluşur.

### Hesap Kök Kullanıcısı

* AWS hesabı sahibi aynı zamanda tüm AWS hizmetlerine tam erişime sahip bir AWS hesabı kök kullanıcısıdır.

### Yeni IAM kullanıcıları oluşturma sınırı, hesap başına 5000 kullanıcıyla sınırlıdır.

## IAM – Politikalar



### IAM Politikası Türleri

### 

1- Yönetilen politikalar:

IAM tarafından yönetilen politika, bir AWS hesabındaki birden çok varlığa (kullanıcı, kullanıcı grubu veya rol) eklenebilen bağımsız bir politikadır. Bunlar yalnızca varlıklara uygulanabilir, kaynaklara uygulanamaz.

* AWS tarafından yönetilen politikalar:

AWS tarafından yönetilen politikalar, AWS tarafından oluşturulan ve yönetilen yönetilen politikalardır. Politikaları kullanma konusunda yeniyseniz AWS, AWS tarafından yönetilen politikaları kullanarak başlamanızı önerir.

* Müşteri tarafından yönetilen politikalar:

Müşteri tarafından yönetilen politikalar, AWS hesaplarındaki kullanıcılar (AWS müşterileri) tarafından oluşturulan ve yönetilen yönetilen politikalardır.

2-Satır içi politikalar:

Satır içi ilkeler, doğrudan tek bir kullanıcıya, gruba veya role katıştırdığınız ve oluşturup yönettiğiniz ilkelerdir.

### İş Fonksiyonu Politikaları

* AWS tarafından yönetilen iş işlevi politikaları, yaygın BT iş işlevleriyle yakından eşleşecek şekilde tasarlanmıştır.
* İş fonksiyonu durumundaki yönetilen ilkeler aşağıda listelenmiştir:
* [Yönetici](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_administrator)
* [Fatura](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_accounts-payable)
* [Veritabanı Yöneticisi](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_database-administrator)
* [Veri Bilimcisi](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_data-scientist)
* [Geliştirici Güçlü Kullanıcı](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_developer-power-user)
* [Ağ Yöneticisi](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_network-administrator)
* [Güvenlik Denetçisi](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_security-auditor)
* [Destek Kullanıcısı](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_support-user)
* [Sistem Yöneticisi](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_system-administrator)
* [Yalnızca Görüntüleme Kullanıcısı](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_job-functions.html#jf_view-only-user)

## IAM – Gruplar

IAM grubu olarak; Birden çok kullanıcının izinlerini yönetmeyi kolaylaştırabilecek izinleri belirtmenize olanak tanıyan IAM kullanıcıları koleksiyonu.

* Grupların kimlik bilgileri yoktur.
* Yönetilen IAM politikaları gruplara eklenebilir.
* Satır içi IAM politikaları gruplara eklenebilir.
* Gruplar yalnızca kullanıcıları içerebilir, ancak diğer grupları içeremez.
* Bir gruptaki IAM kullanıcılarının sınırı, hesabın kullanıcı kotasına, yani en fazla 5000'e eşittir.
* Bir IAM kullanıcısı, en fazla 10 farklı IAM grubunun üyesi olabilir.

## IAM – Roller

* Bir kimliğin AWS kaynaklarına nasıl ve hangi yetkilerle erişebileceğini belirlediğimiz yetkilendirme sistemidir.
* Her rolün iki ilkesi vardır: Güven ilkesi ve izin ilkesi.
* IAM rolleri, güvendiğiniz varlıklara izin vermenin güvenli bir yoludur.
* EC2 bulut sunucusu ile S3 hizmetine erişip oradaki dosyaları okuyup bu hizmete kaydedebilmemiz için bir sanal makine-EC2'ye atayabileceğimiz bir rol oluşturabiliriz.