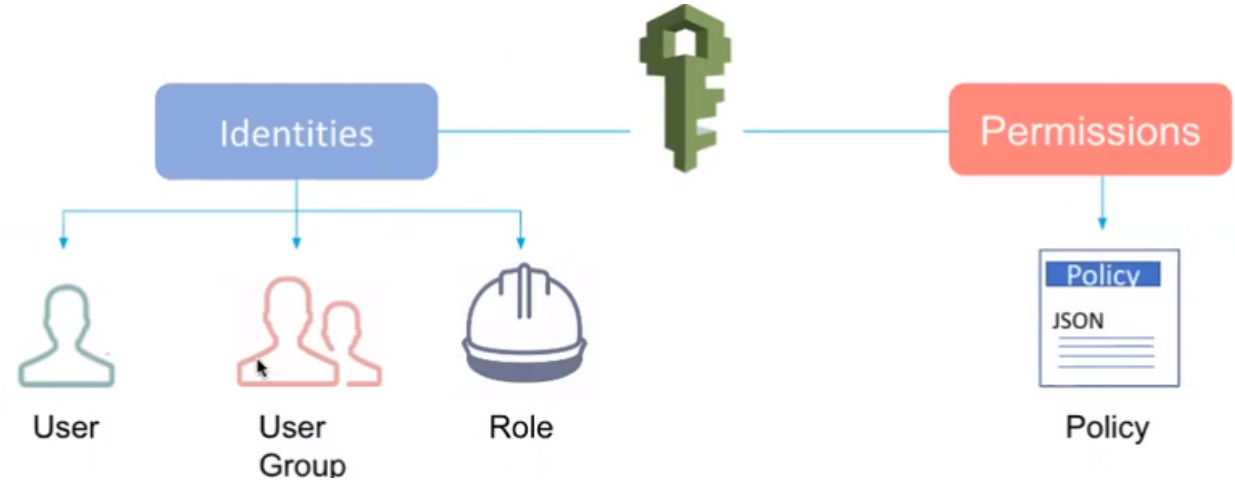
IAM

IAM = Identity Access Management

Kimliklendirme ve yetkilendirme. İçeriye girme ya da bir programı kullanmak için izin

Principal: AWS'de belirli bir userın, servisin, accountun belirli haklara sahip olup olmadığını belirtir. NotPrincipal ile verilmeyen yetkiler belirtilir.



3 temel Idendity var.

- User

Bir hesapta max. 5000 IAM oluşturma yetkimiz var. IAM User yukarıda olduğu gibi gerçek insanlar olabilir, web uygulama, servis ya da yazılım olabilir.

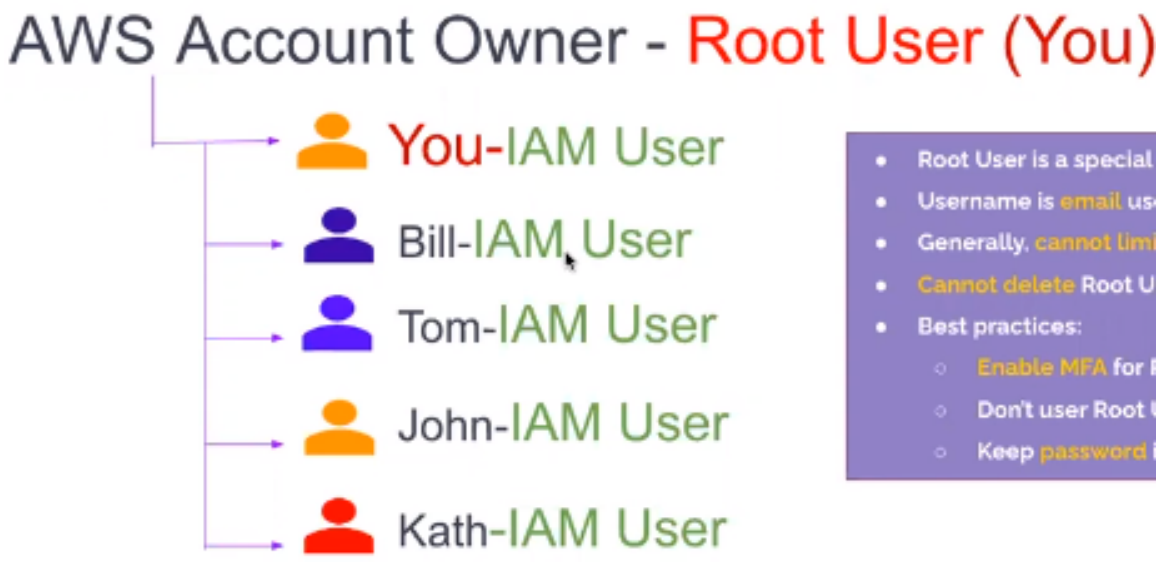
- Group
- Role

Access Management kısmı ise önceden belirlenmiş policyler ile hallediliyor.

- Policies

Tek hesap üzerinden birden fazla IAM User oluşturuyoruz. Bunun 2 temel nedeni var. İlki root user çok yetkili. Yanlışlıkla geri dönülmez bir hata yapılabilir. Bir diğeri birden

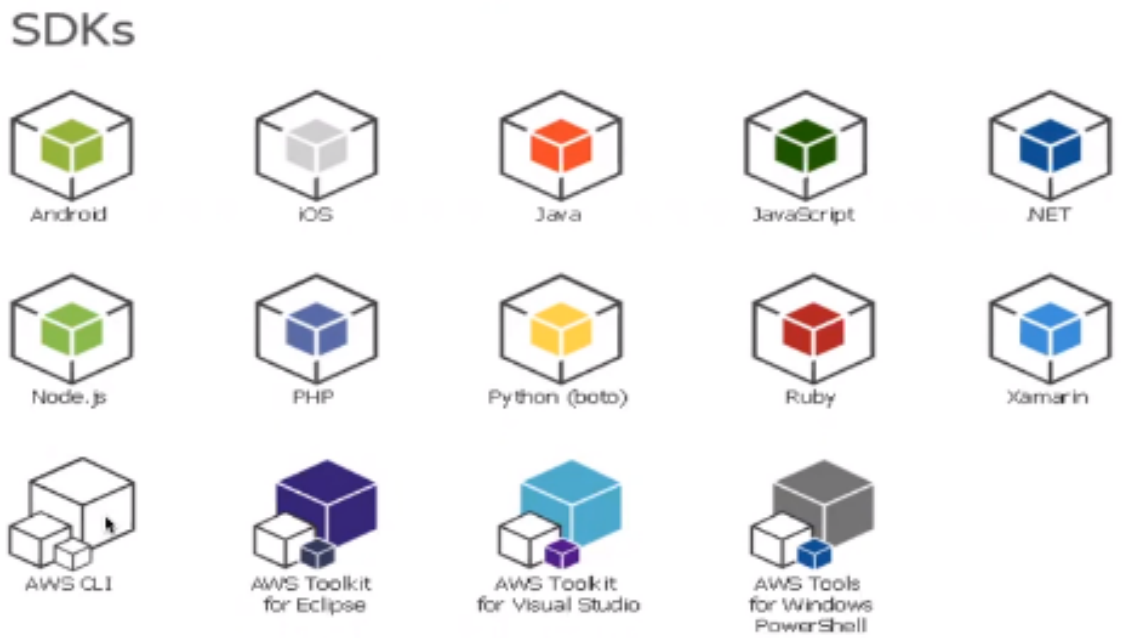
fazla kişi aynı hesabı kullanıyorsa IAM tanımlamazsak herkes root ile girmek dyurumunda kalır. Bu da tracklamaya imkan bırakmaz. Yani biri yanlış bir şey yaptı bunu tespit edemeyiz.



Yeni bir user oluşturulduğunda Credentials dosyası indiriilir. Bunu sadece 1 kez indirebiliyoruz. Bu dosya .csv uzantılı. Kaydetmek lazım. İçinde CLI ile giriş yaparken kullanacağımız **Access key**
ID ve **Secret access key** var.

AWS'ye 2 şekilde girilir. 1 normal konsoldan diğeri SDK(Software Development Key) sayesinde. CLI'da bunlardan biri.

Yeri gelecek yazdığımız kod/program AWS'den EC2 kaldırmasını ya da farklı işlemler isteyecek. Ancak AWS python, Java vs.den anlamaz. Bu diller ile anlaşabilmesi için SDK kullanıyoruz.



IAM POLICIES

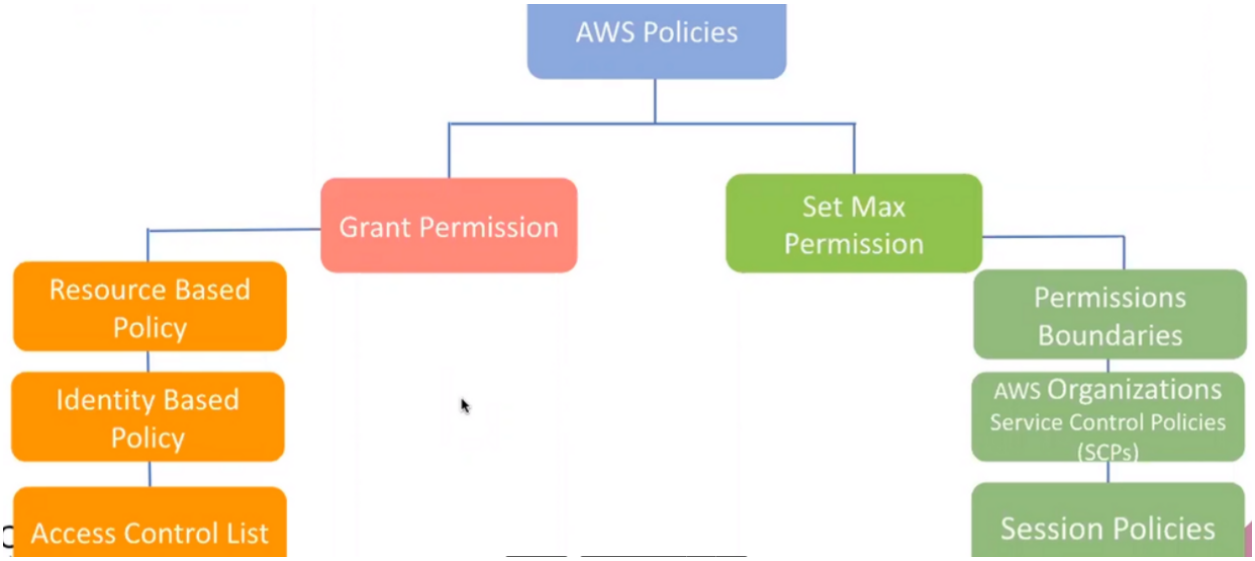
Genellikle JSON formatında yazılır. Belirli yetkiler kısıtlanır ya da belirli yetkiler verilebilir bu policylerle. AdministratorAccess policy'nin JSON dosyası aşağıdadır.

```
1  {
2     "Version": "2012-10-17",
3     "Statement": [
4        {
5           "Effect": "Allow",
6           "Action": "*",
7           "Resource": "*"
8        }
9     ]
10 }
```

Version kısmı sabit. Effect yapılması istenen eylem. Yukarıda izin vermesi isteniliyor. Action bölümü neye izin verilsin sorusuna cevap verir. *() her şey anlamında. Resource ise yetki alanını belirtir. (*) varsa tüm servisler için verilir bu yetki. Bu bir izin verme policysidir (Allow Policy).

Yukarıdaki Identity Based Policy'dir. Eğer Resource Base olsaydı Resource'un altında Principals diye bir bölüm olacaktır. Orada da hangi servise izin verileceğini belirtirdik.

Policy Types

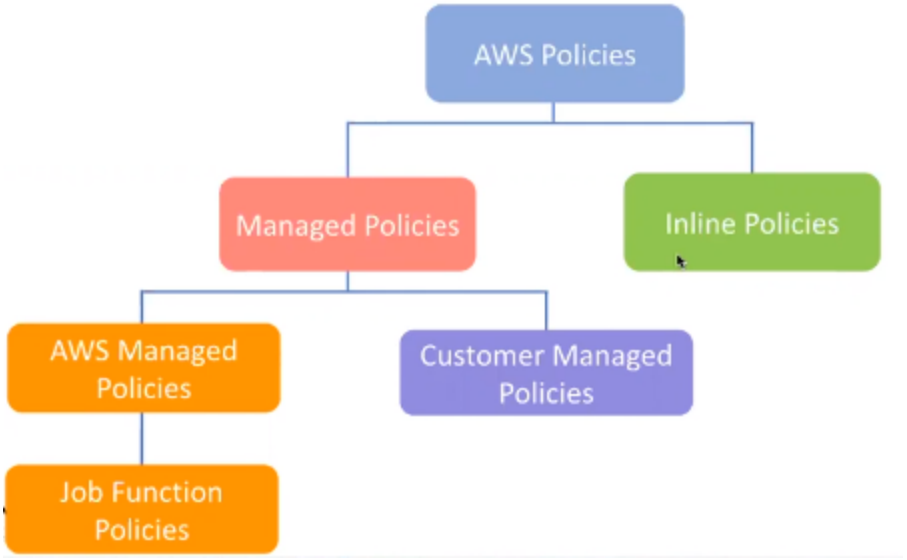


Resourse Based Policy: Belirli servislere belirli yetkiler verilliyor. Örneğin Load Balancer'a EC2 kaldırma yetkisi verilmesi gibi.

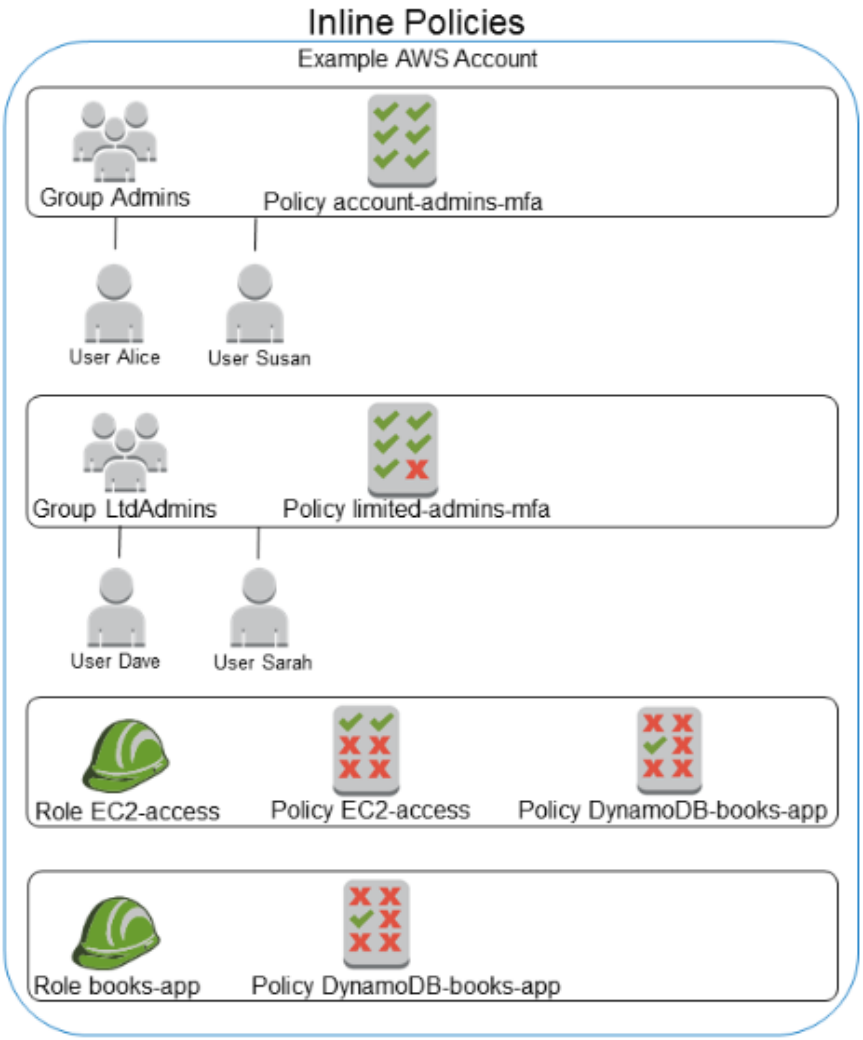
Identity Based Policy: Kullanıcılara belirli işlemleri yapabilmesi için yetki verilme olayı

Access Control List: Başka hesaplarda bulunan resim/dosyalara erişim yetkisi.

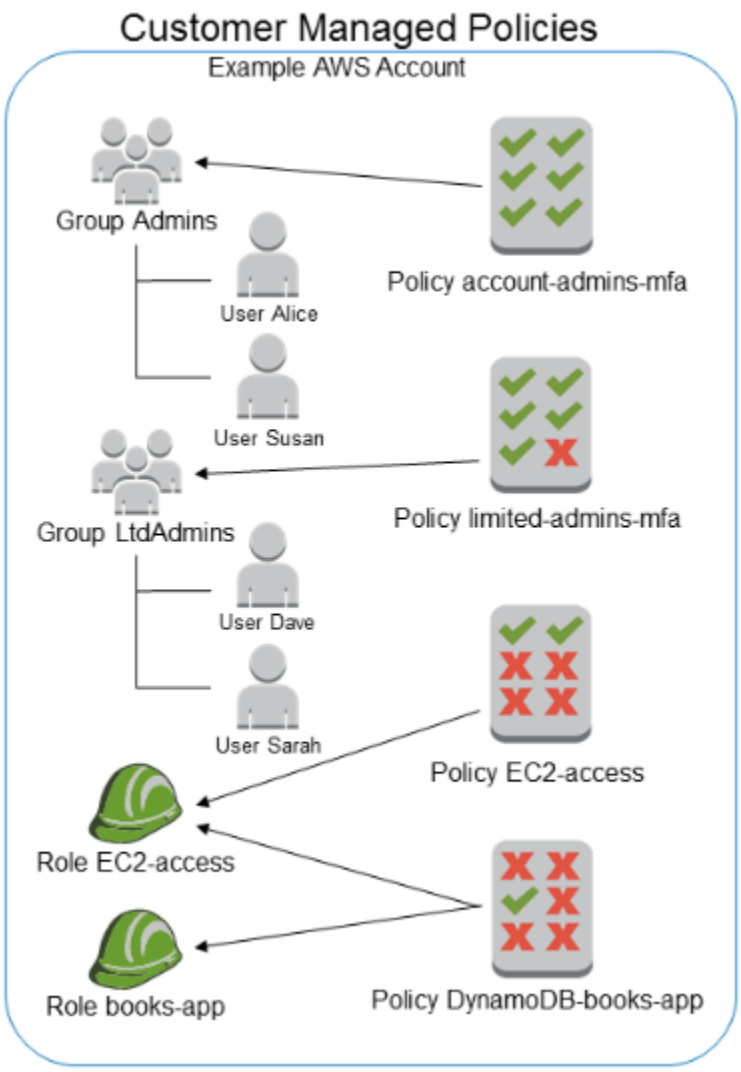
Set Max Permission: Daha çok yetkileri sınırlama üzerine kurulu



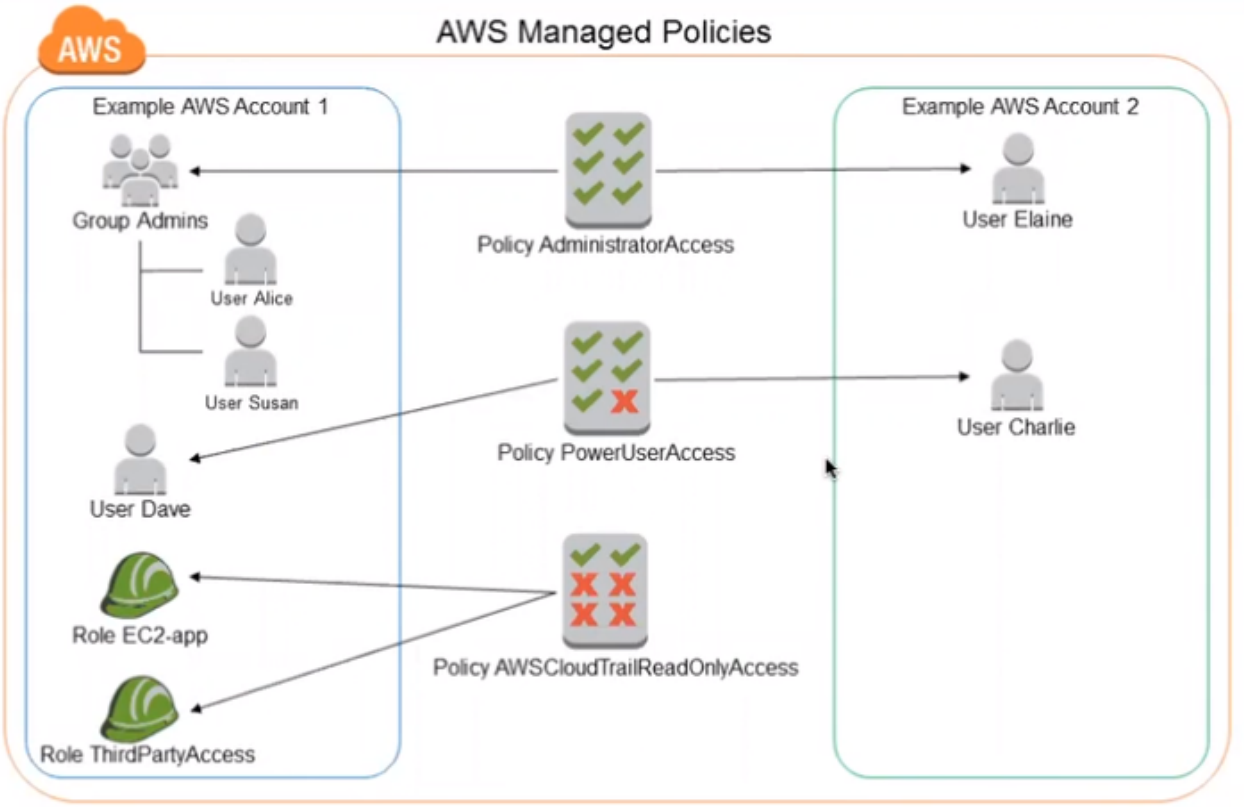
Inline Policy: Kullanıcıya özeldir. Sadece o kişi görebilir. O kullanıcı sistemden silinirse policy de silinir. Örneğin denetleme görevi için



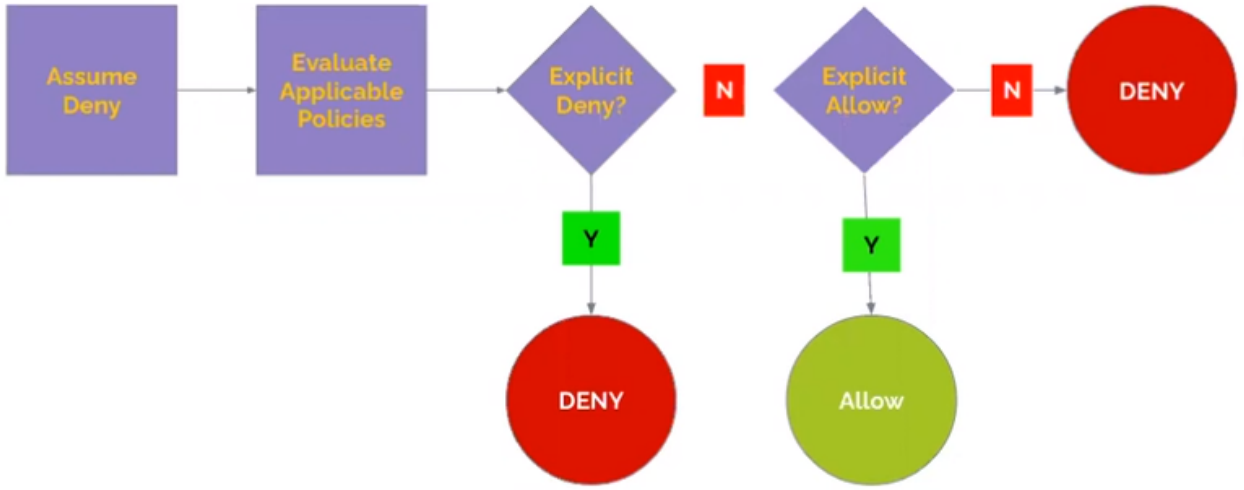
Customer Managed Policies: Benim hesabımdan hazırlanan policylerdir. Hesabı kullanan herkes görebilir.



AWS Managed Policies: AWS'nin oluşturduğu hazır policylerdir. Herkes görebilir. Job Function da iş odaklı olan policyler. Örn, • Data Scientist • Security Auditor • System Administrator• Billing • Network Administrator



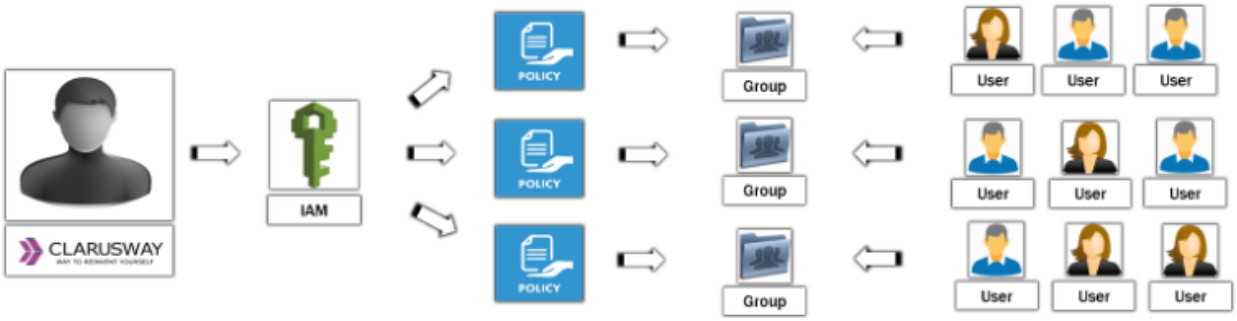
Policy Çalışma Mantığı



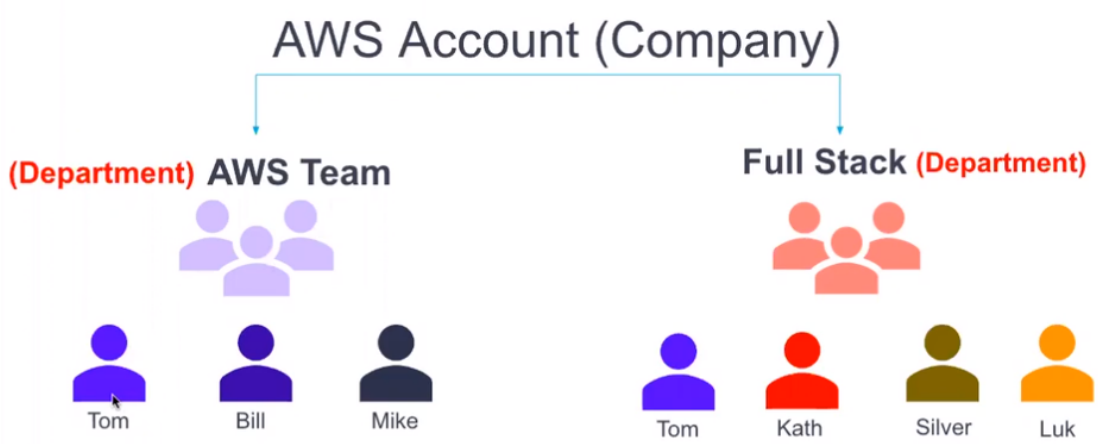
AWS'de en başta her şey Deny'dır. Hiç bir servisi kullanamayız. Policy de açıkça bir Deny varsa sonuç DENY. Açıkça Allow varsa sonuç ALLOW. Ancak Açık bir şekilde Allow ya da Deny olduğu belirtilmemişse sonuç DENY'dır.

IAM User Group

Şirketteki tüm personele tek tek yetki vermek yerine belirli gruplar oluşturulup gruplara yetki verilir. Şirket çalışanları bu gruplara dahil edilir. Otomatik olarak gruba verilen yetkilere haiz olurlar.



Bir kullanıcı max. 10 ayrı gruba dahil olabilir. Max. 300 adet group kurulabilir. Bir grouptaki max kullanıcı sayısı 5000dir.

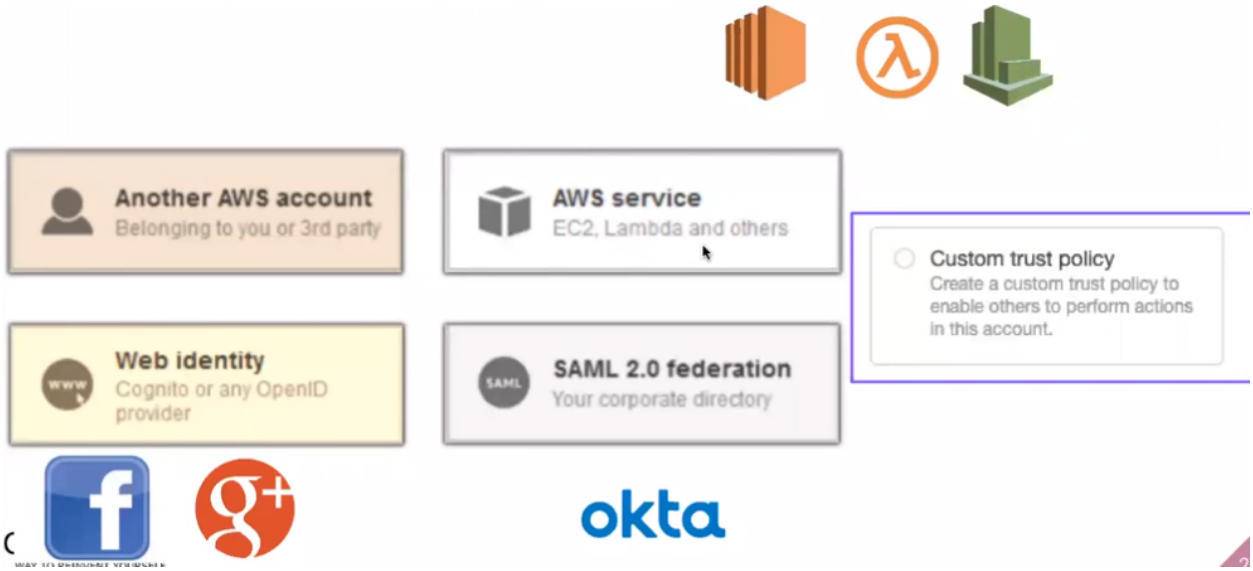


Yukarıdaki resimde Tom iki grupta da var. Diyelim ki AWS Team'in tüm servislere erişim yetkisi var. Full Stack grubu ise sadece Database'e erişebiliyor. Yukarıda anlatılan Policy Çalışma Mantığına göre Tom'un sadece Database'e erişim yetkisi olur. Çünkü burada bir çakışma var. Bu durumda Amazon Deny'ı tercih eder.

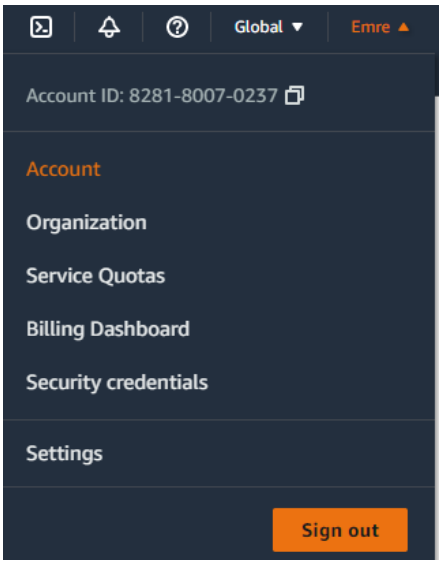
IAM Roles

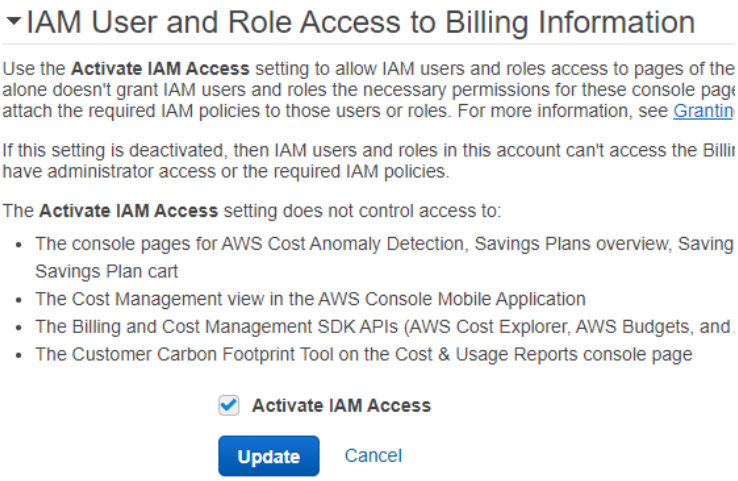
Bir kullanıcının AWS kaynaklarını nasıl kullanabileceğini belirleyebileceğimiz bir yetkilendirme sistemidir. Doğal olarak bu yetkilendirmeyi belirli policyler ile yaparız. Ör. sıradan bir öğretmene müdür yardımcısı görevi (role'ü) verirsek müdür yardımcısına ait yetkilere sahip olur. AWS IAM Role'un şöyle bir dezavantajı var. Yukarıdaki öğretmen artık müdür yardımcısı görevlerine sahip ve o role'de olduğu sürece öğretmenlik yapamaz.

Aşağıdakilere IAM Role tanımlayabiliriz. Ancak biz daha çok bir servisin başka bir servise erişebilmesi için kullanıyoruz

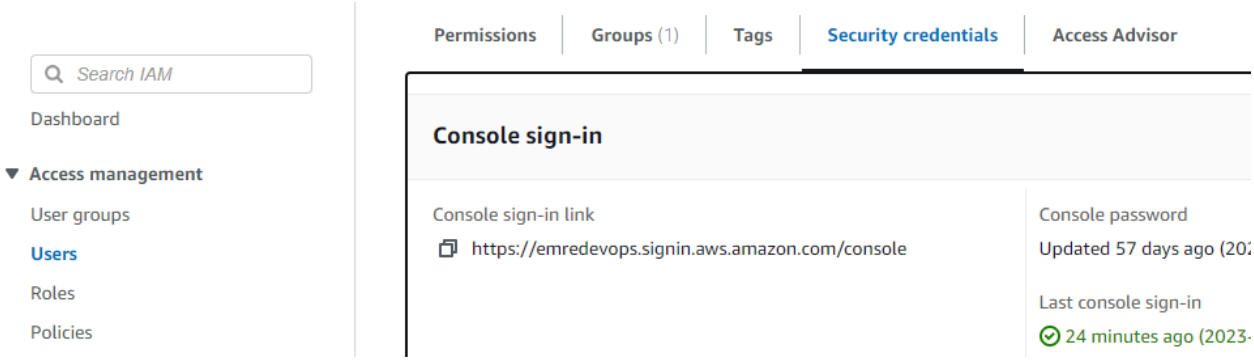


- Konsola IAM ile giriş yapabilmek için accounta giriyoruz. Activate IAM Access kutusunu seçiyoruz





- Access Key ya da Secret Access key'i unuttuk ne yapacağız



Users da Security credendials den yeni bir access key oluşturabiliriz. Aynı anda max ik tane oluşturulur. Öncekini silmek gerek. Silmeden önce deactivate etmek gerek.