Güvenlik ve Erişim Kontrolü

Proje: AWS hizmetlerini kullanarak güvenlik ve erişim kontrolü önlemlerini uygulamak ve AWS kaynaklarına sınırlı ve güvenli erişim sağlamaktır.

Proje Açıklaması: AWS Identity and Access Management (IAM) hizmetini kullanarak IAM kullanıcıları, grupları ve rolleri oluşturmayı içerir.

Projenin Temel Adımları:

- IAM kullanıcıları, grupları ve rolleri oluşturarak erişim kontrollerinin yapılandırılması.
- AWS Identity and Access Management (IAM) politikalarını kullanarak kaynaklara erişimin sınırlanması.

Projede Kullanılacak AWS Hizmetleri:

• IAM (Identity and Access Management)

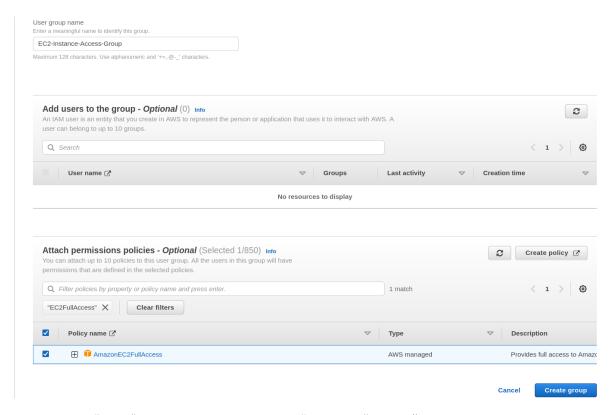
AWS Identity and Access Management (IAM)

Amazon Web Services (AWS) üzerinde kullanıcıları, grupları ve rolleri yönetmek için hizmet sağlayan bir IAM hizmetidir. IAM, AWS kaynaklarına erişimi kontrol etmek, kimlik doğrulama ve yetkilendirme politikalarını tanımlamak ve güvenliği sağlamak için kullanılır.

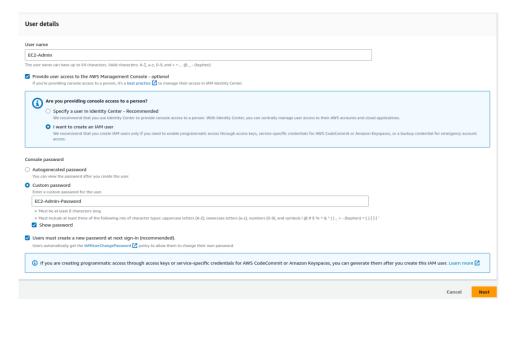
- User Groups: Benzer yetkilere sahip kullanıcıların aynı kaynaklara erişimini sağlamak için kullanılır.
- Users: AWS hizmetlerine erişim sağlayabilmek için kullanıcılara izinler atanır.
- Roles: Roller, kimlik bilgileri yerine geçen geçici yetkilendirmelerdir ve AWS kaynaklarına erişmek için kullanılır. Bir rol, bir hizmet veya bir kullanıcı tarafından geçici olarak devralınabilir.
- Policies: Politikalar, kimlik doğrulama ve yetkilendirme kontrollerini tanımlar ve hangi kaynaklara erişilebileceğini belirler.
- Identity Providers: Kimlik sağlayıcıları, dış sistemlerde depolanan kimlik bilgilerini kullanarak AWS hizmetlerine erişimi sağlar. AWS IAM, OpenID Connect (OIDC) ve SAML protokollerini destekler ve bu protokolleri kullanarak kimlik sağlayıcılarıyla entegrasyon sağlar.

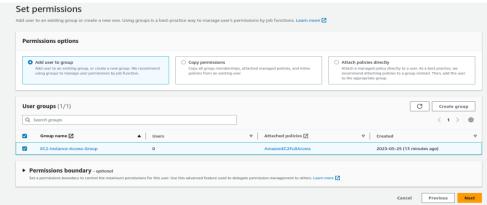
User Group, Users ve Policies Oluşturma

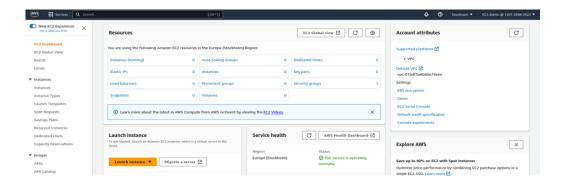
Amazon IAM hizmetine gidildikten sonra solda bulunan "User Group" seçeneği seçilir. Grup ismi girildikten sonra istenilen hizmete erişim vermek için uygun hizmet seçilir ve "Create Group" seçeneği seçilerek grup oluşturulur. Proje kapsamında EC2 hizmetine full erişimi olan bir kullanıcı grubu seçilecektir.



IAM hizmetinde "Users" sekmesine gidildikten sonra "Add Users" seçeneğine tıklanır. Kullanıcı için isim oluşturulur. Aynı sayfada bulunan "Provide user access to the AWS Management Console – optional" seçeneği oluşturulan kullanıcının Amazon Management Console'a erişim sağlayıp sağlayamamasını belirtir. Eğer ki konsola erişim seçeneği disable olarak ayarlanırsa oluşturulan kullanıcı için sadece API çağrıları yapılabilir. Bunun için bu seçenek enable olarak ayarlanır. "I want to create an IAM user" seçeneği seçilir ve kullanıcı için parola oluşturulur. Next seçeneği seçildikten sonra kullanıcıya atanacak izinler belirtilir. Kullanıcı için projede oluşturulan grup kullanılacaktır. İstenildiği takdirde bir policy üzerinden izinler tanımlanabilir. Review and Create seçeneği seçilerek kullanıcı oluşturulur. Verilen linke tıklandığı zaman oluşturulan kullanıcı için giriş yapılabilir.







IAM Politikaları Kullanarak Kaynaklara Erişimin Sınırlanması

IAM yönetim konsolunda yeni bir kullanıcı açılır. Oluşturulan kullanıcıda "Permission" tabında "Add Permission > Create Inline Policy" seçeneği seçilerek yeni bir policy oluşturulur. JSON formatına aşağıdaki kod yapıştırılır.

```
"Sid": "VisualEditor0",

"Effect": "Allow",

"Action": "s3:ListBucket",

"Resource": "arn:aws:s3:::aws-sysops-project"

},

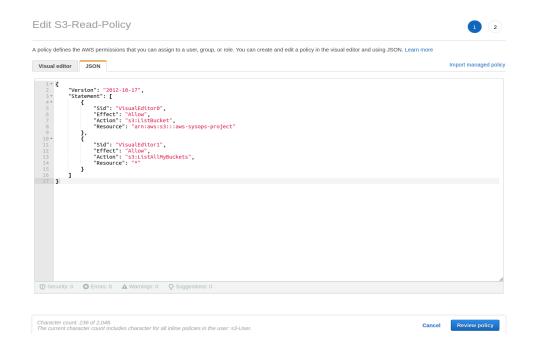
{
    "Sid": "VisualEditor1",

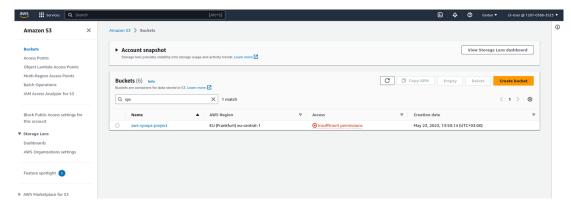
"Effect": "Allow",

"Action": "s3:ListAllMyBuckets",

"Resource": "*"
}
]
```

Yukarıdaki örnekte "bucket-name" kısmını ilgili S3 bucket'ının adıyla değiştirilmesi gerekmektedir. Bu politika yalnızca belirtilen bucket'ı listeleme yetkisi verecektir. Diğer S3 işlemleri (nesne oluşturma, alma, vb.) bu politika ile kısıtlanmış olacaktır. Ardından create policy seçeneği seçilerek policy oluşturulur.





S3-User Kullanıcı Profili