

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 sınırlandırılması.

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 Oluřturma

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

User group name
Enter a meaningful name to identify this group.

Maximum 128 characters. Use alphanumeric and '+=, @, _' characters.

Add users to the group - *Optional* (0) [Info](#)
An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

User name [↗](#)

Groups

Last activity [↗](#)

Creation time [↗](#)

No resources to display

Attach permissions policies - *Optional* (Selected 1/850) [Info](#)
You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

1 match

“EC2FullAccess” [✕](#)

Clear filters


☒

Policy name [↗](#)

Type

Description

☒

 AmazonEC2FullAccess

AWS managed

Provides full access to Amaz

[Cancel](#) [Create group](#)

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

User details


User name

EC2-Admin

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and +, -, @, _ (hyphen)

☒ Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a [best practice](#) to manage their access in IAM Identity Center.



Are you providing console access to a person?

☐ Specify a user in Identity Center - Recommended

We recommend that you use Identity Center to provide console access to a person. With Identity Center, you can centrally manage user access to their AWS accounts and cloud applications.

☒ I want to create an IAM user

We recommend that you create IAM users only if you need to enable programmatic access through access keys, service-specific credentials for AWS CodeCommit or Amazon Keyspaces, or a backup credential for emergency account access.

Console password

☐ Autogenerated password

You can view the password after you create the user.

☒ Custom password

Enter a custom password for the user:


EC2-Admin-Password

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # % ^ & * () _ + - (hyphen) = [] ' , .

☒ Show password

☒ Users must create a new password at next sign-in (recommended).

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.



If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

The screenshot displays the AWS Management Console interface for the Stockholm Region. The left-hand navigation pane includes sections for 'New EC2 Experience' (with a sub-link 'Start what you know'), 'EC2 Dashboard', 'EC2 Global View', 'Events', 'Limits', 'Instances' (expanded), 'Instance Types', 'Launch Templates', 'Spot Requests', 'Savings Plans', 'Reserved Instances', 'Dedicated Hosts', 'Capacity Reservations', 'Images', 'AMIs', and 'AMI Catalog'. The main content area is titled 'Resources' and contains a message: 'You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:'. Below this message is a table listing various EC2 resources:

Resource Type	Count	Resource Name	Count	Resource Name	Count
Instances (running)	0	Auto Scaling Groups		Dedicated Hosts	0
Elastic IPs	0	Instances		Key pairs	0
Load balancers	0	Placement groups		Security groups	1
Snapshots	0	Volumes			

Below the table, there is a link: 'Learn more about the latest in AWS Compute from AWS re:invent by viewing the [EC2 Videos](#)'. To the right of the main content area, there is a section titled 'Account attributes' which lists supported platforms (VPC, Default VPC, Settings, EBS encryption, Zones, EC2 Serial Console, Default credit specification, Console experiments). At the bottom of the console, there is a 'Launch instance' button and a 'Migrate a server' button. The 'Service health' section shows the status of the Region (Europe (Stockholm)) as 'This service is operating normally'.

IAM Politikaları Kullanarak Kaynaklara Erişimin Sınırlanması

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "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.

Edit S3-Read-Policy

1 2

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. [Learn more](#)

Visual editor

JSON

[Import managed policy](#)

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "VisualEditor0",
6       "Effect": "Allow",
7       "Action": "s3:ListBucket",
8       "Resource": "arn:aws:s3:::aws-sysops-project"
9     },
10    {
11      "Sid": "VisualEditor1",
12      "Effect": "Allow",
13      "Action": "s3:ListAllMyBuckets",
14      "Resource": "*"
15    }
16  ]
17 }

```

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

Character count: 236 of 2,048.
The current character count includes character for all inline policies in the user: s3-User.

Cancel

Review policy

Amazon S3

Buckets

Access Points

Object Lambda Access Points

Multi-Region Access Points

Batch Operations

IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens

Dashboards

AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

Amazon S3 > Buckets

Account snapshot

View Storage Lens dashboard

Buckets (6)

Info

Copy ARN

Empty

Delete

Create bucket

Q sys

X

1 match

< 1 >

Name	AWS Region	Access	Creation date
aws-synops-project	EU (Frankfurt) eu-central-1	<div>Insufficient permissions</div>	May 23, 2023, 13:50:14 (UTC+03:00)

S3-User Kullanıcı Profili