

Lab: IAM User & Policy Getting Started (Console)

[Lý thuyết](#)[Ghi chú](#)[Bình luận](#)

Giới thiệu

Bài lab làm quen với dịch vụ IAM, bắt đầu bằng việc khởi tạo một IAM User với quyền hạn nhỏ nhất, cho tới khi hoàn thành cấp phát các quyền hạn cho User và học cách quản lý các quyền hạn này.

Mục tiêu bài học

Kết thúc bài lab, học viên cần hiểu được khái niệm về IAM User và IAM Policy, cơ chế hoạt động của IAM Policy và cấu trúc định nghĩa ra một Policy

Chuẩn bị

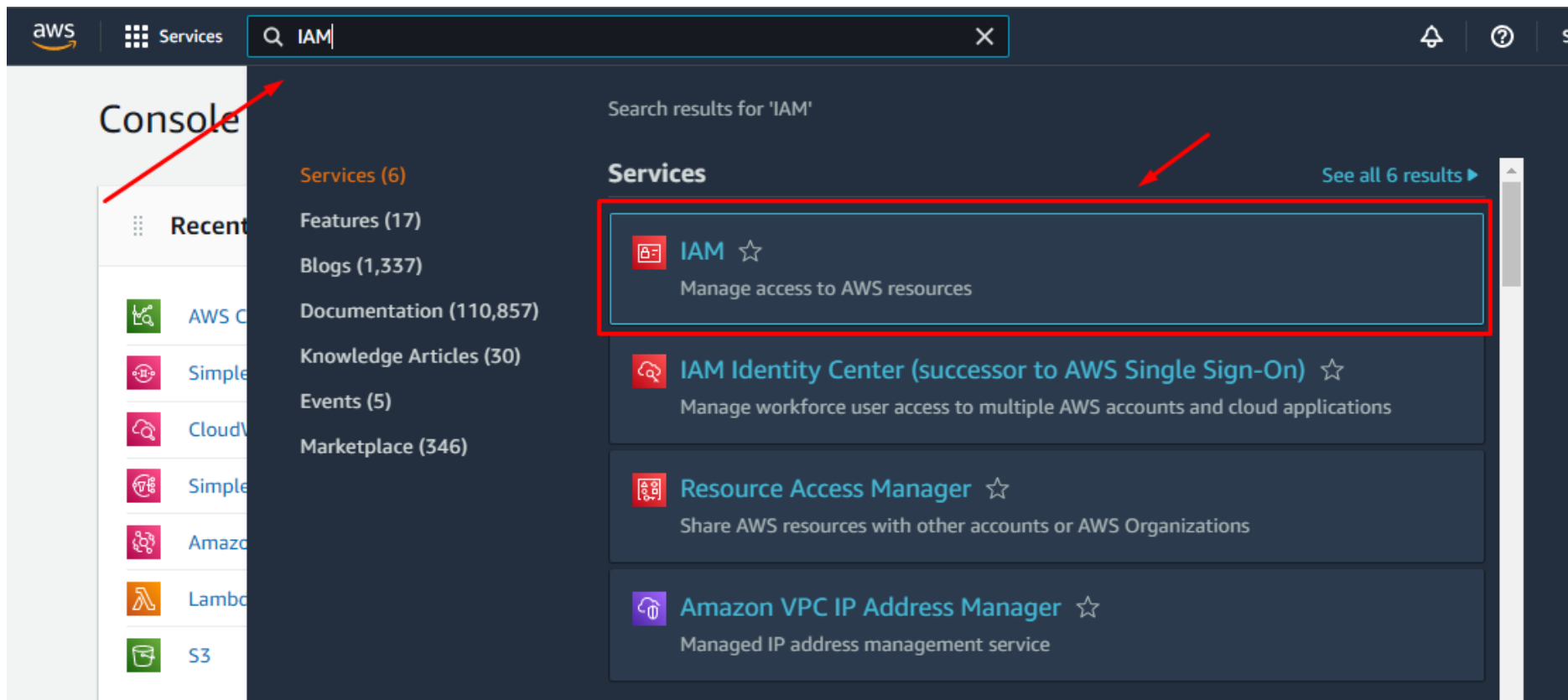
Trước khi thực hiện bài Lab, học viên cần lưu ý:

- Chuẩn bị account AWS đã được active
- Cấp phép sử dụng các dịch vụ liên quan đến IAM (không nên sử dụng root user)

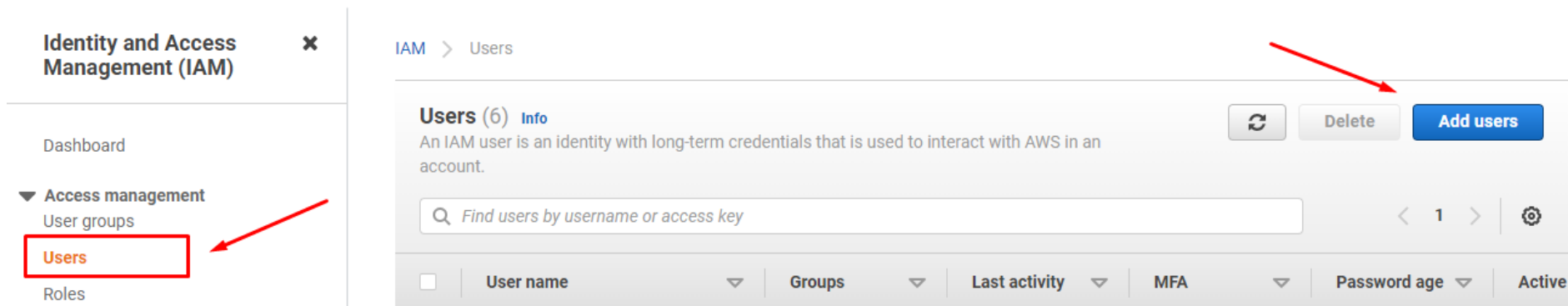
Các bước thực hành

Học viên thực hành theo các bước sau:

Lab: IAM User & Policy Getting Started (Console)



- Tiếp đó, truy cập giao diện IAM User và chọn **Add User** button



Lab: IAM User & Policy Getting Started (Console)

Add user



Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

techmaster-demo-user

[+ Add another user](#)

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

Select AWS credential type*

**Access key - Programmatic access**

Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

**Password - AWS Management Console access**

Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password*



Autogenerated password



Custom password

* Required

[Cancel](#)[Next: Permissions](#)

- Sau đó, click next tới bước cuối cùng, sau đó tạo User, tải file credential về (file này sẽ chỉ xuất hiện 1 lần sau khi tạo user)

Lab: IAM User & Policy Getting Started (Console)

**Success**

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: <https://lamdn8.signin.aws.amazon.com/console>

 **Download .csv**

	User	Password	Email login instructions
▶	✓ techmaster-demo-user	***** Show	Send email 

[Close](#)

- Mở file credential và thực hiện login với tab ẩn danh dựa trên các thông tin được mô tả trong file. Sau khi đăng nhập, thực hiện truy cập các tài nguyên bất kì, học viên sẽ nhận thấy rằng User này không có bất kì quyền hạn gì cả

Bước 2: Tạo IAM Policy cho phép User có quyền chỉ xem (readOnly)

- Quay trở lại với giao diện quản lý IAM user với tài khoản Admin, tiến hành thêm quyền hạn cho IAM User demo

Lab: IAM User & Policy Getting Started (Console)

Dashboard

- Access management
 - User groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- Access reports
 - Access analyzer
 - Archive rules
 - Analyzers
 - Settings
- Credential report
- Organization activity

User ARN arn:aws:iam::138239152910:user/techmaster-demo-user

Path /

Creation time 2022-07-30 14:36 UTC+0700

Permissions Groups Tags Security credentials Access Advisor

Permissions policies

Get started with permissions
This user doesn't have any permissions yet. Get started by adding the user to a group, copying permissions from another user, or attaching a policy directly. [Learn more](#)


Add permissions [Add inline policy](#)


Permissions boundary (not set)


- Trên phần tìm kiếm Policy, lựa chọn Policy có tên **iamReadOnlyAccess**. Sau đó, học viên click “next” tới bước cuối cùng và hoàn thành thao tác gắn Policy cho User.

Lab: IAM User & Policy Getting Started (Console)

Use IAM policies to grant permissions. You can assign an existing policy or create a new one.


 Add user to group

 Copy permissions from existing user

 Attach existing policies directly

Create policy

Showing 1 result

	Policy name ▾	Type	Used as
<input checked="" type="checkbox"/>	 IAMReadOnlyAccess	AWS managed	None

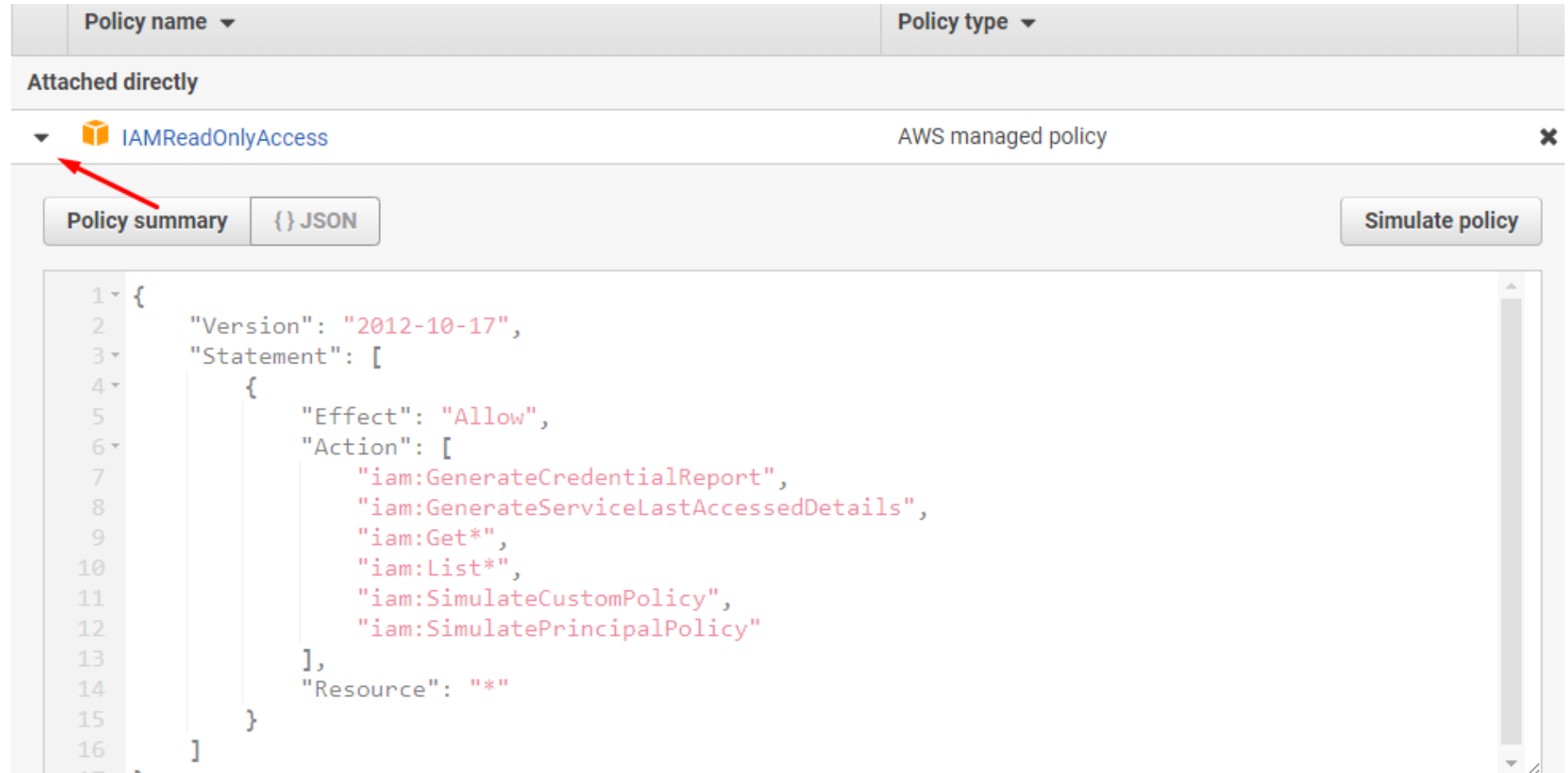
CancelNext: Review

- Học viên thực hiện kiểm tra quyền hạn của IAM User sau khi được gắn policy. Khi đó IAM User sẽ có quyền xem tất cả các tài nguyên thuộc dịch vụ IAM

Bước 3: Thay đổi IAM Policy nhằm chỉ định tài nguyên truy cập cụ thể

- Quay trở lại giao diện quản lý IAM User trên account admin, tiến hành review IAM Policy iamReadOnlyAccess (Học viên cũng có thể truy cập giao diện quản lý IAM Policy để tìm kiếm). Tại phần Resource, trong bản ghi IAM Policy, giá trị đang được cài đặt là "*", tương ứng với việc các thao tác được định nghĩa tại phần Action có hiệu lực với mọi tài nguyên

Lab: IAM User & Policy Getting Started (Console)




The screenshot shows the AWS IAM console interface. At the top, there are tabs for 'Policy name' and 'Policy type'. Below this, the 'Attached directly' section is visible. A red arrow points to the policy name 'IAMReadOnlyAccess', which is an 'AWS managed policy'. Below the policy name, there are two tabs: 'Policy summary' and '{} JSON'. The 'Policy summary' tab is selected, and the policy document is displayed in a code editor. The policy document is a JSON object with the following structure:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

- Tại phần Resource, trong bản ghi IAM Policy, giá trị đang được cài đặt là "*", tương ứng với việc các thao tác được định nghĩa tại phần Action có hiệu lực với mọi tài nguyên. Học viên thực hiện thao tác copy Policy Document, lưu tại text editor, sau đó xóa IAM Policy này khỏi User
- Sau đó, học viên thực hiện copy arn của IAM user ở mục Summary. Chúng ta sẽ sử dụng ARN này để chỉ định tài nguyên cụ thể ở phần Resource. Cụ thể hơn, trong các bước tiếp theo, học viên sẽ tiến hành thực hiện việc cấp quyền iamReadOnly cho chỉ IAM User này

Lab: IAM User & Policy Getting Started (Console)

User ARN	arn:aws:iam::138239152910:user/techmaster-demo-user 
Path	/
Creation time	2022-07-30 14:36 UTC+0700

- Thay thế đoạn ARN vào phần Resource trong Policy, chúng ta có đoạn Policy Document có dạng như sau:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:GenerateCredentialReport",
        "iam:GenerateServiceLastAccessedDetails",
        "iam:Get*",
        "iam:List*",
        "iam:SimulateCustomPolicy",
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "arn:aws:iam::<account-id>:user/*"
    }
  ]
}
```

- Copy đoạn Policy Document trên và tiến hành **add inline policy**

Lab: IAM User & Policy Getting Started (Console)

Summary

Delete user

User ARN arn:aws:iam::138239152910:user/techmaster-demo-user

Path /

Creation time 2022-07-30 14:36 UTC+0700

Permissions

Groups

Tags

Security credentials

Access Advisor

▼ Permissions policies (1 policy applied)

Add permissions

➕ Add inline policy

Policy name ▼

Policy type ▼

- Paste vào phần Json Editor và lưu lại (giảng viên mô tả một số thao tác trên phần visual editor - là công cụ giúp generate IAM Policy Document)
- Học viên chuyển sang cửa sổ trình duyệt với IAM user đang được sử dụng nhằm demo, thực hiện một số thao tác với dịch vụ IAM và đưa ra đánh giá

Bước 4: Thay đổi IAM Policy với Explicit Denied

- Tiến hành thực hiện lại bước thứ 2, nhằm thêm IAM Policy với quyền **iamReadOnlyAccess**. Sau đó, học viên nhận thấy rằng quyền hạn của IAM User demo đã được tăng trở lại với các thao tác lên dịch vụ IAM
- Sau đó, thực hiện Edit IAM Inline Policy được tạo tại bước thứ 3, với phần Effect được chuyển từ “Allow” sang “Deny”. Học viên thực hiện thao tác với IAM user demo và đưa ra đánh giá

Bước 5: Gom nhóm IAM User bằng cách sử dụng IAM Group