

Lab: IAM Access Key & Access Secret Key (Terminal, Powershell)

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

Giới thiệu

Bài lab làm quen với dịch vụ IAM thông qua phương thức sử dụng AWS CLI (trên hệ điều hành Linux)

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:

Bước 1: Cài đặt AWS CLI

Lab: IAM Access Key & Access Secret Key (Terminal, Powershell)

Bước 2: (Optional) Tạo IAM User và setup AWS Credential cho AWS CLI

- Học viên thực hiện tạo IAM User với option **programing access**. Sau đó, trên terminal của máy tính cá nhân, gõ command dưới đây để thực hiện cài đặt credential

```
aws configure
```

Học viên chuẩn bị sẵn các command để thực thi thay cho việc sử dụng AWS Console:

<https://awscli.amazonaws.com/v2/documentation/api/latest/reference/iam/index.html#cli-aws-iam>

Bước 3: 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 Access Key & Access Secret Key (Terminal, Powershell)


The screenshot shows the AWS IAM console interface. On the left sidebar, under 'Access management', the 'Users' link is highlighted with a red box and a red arrow points to it. The main content area displays details for the user 'arn:aws:iam::138239152910:user/techmaster-demo-user'. Below the user details, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Access Advisor'. The 'Permissions' tab is selected, showing a section titled 'Permissions policies'. Inside this section, there is a blue box with the heading 'Get started with permissions' and a message stating '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](#)'. The 'Add permissions' button in this box is highlighted with a red box and a red arrow points to it. To the right of this box is a link '+ Add inline policy'. Below the blue box, there is a section for '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 Access Key & Access Secret Key (Terminal, Powershell)

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

Cancel

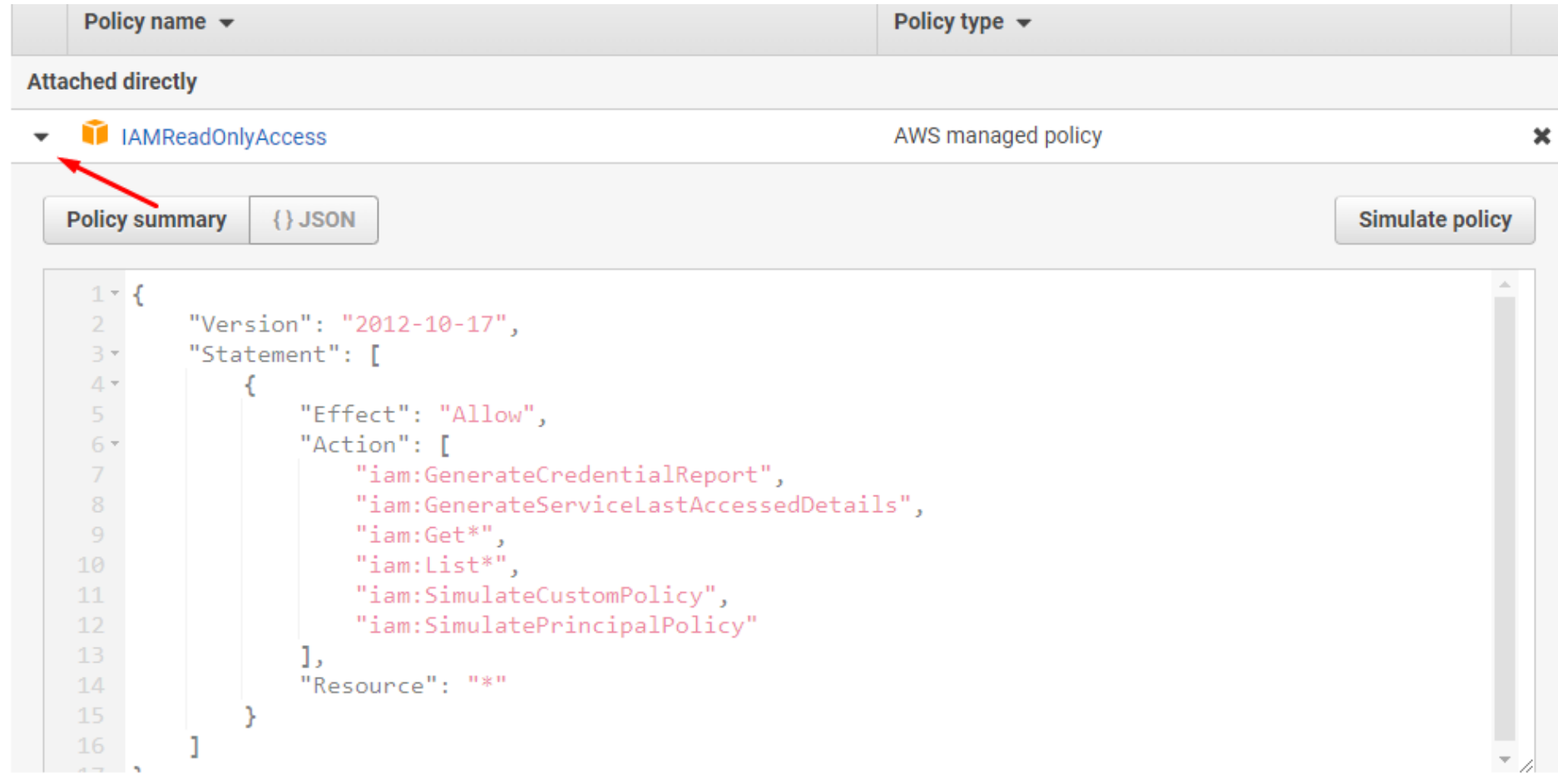
Next: Review

- 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 4: 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 Access Key & Access Secret Key (Terminal, Powershell)




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, showing a JSON policy document. The document is as follows:

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "iam:GenerateCredentialReport",
8         "iam:GenerateServiceLastAccessedDetails",
9         "iam:Get*",
10        "iam:List*",
11        "iam:SimulateCustomPolicy",
12        "iam:SimulatePrincipalPolicy"
13      ],
14      "Resource": "*"
15    }
16  ],
17 }
```

- 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 Access Key & Access Secret Key (Terminal, Powershell)

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/techmaster-demo-user"
    }
  ]
}
```

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

Lab: IAM Access Key & Access Secret Key (Terminal, Powershell)

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 5: 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 6: IAM Switch Role với AWS CLI