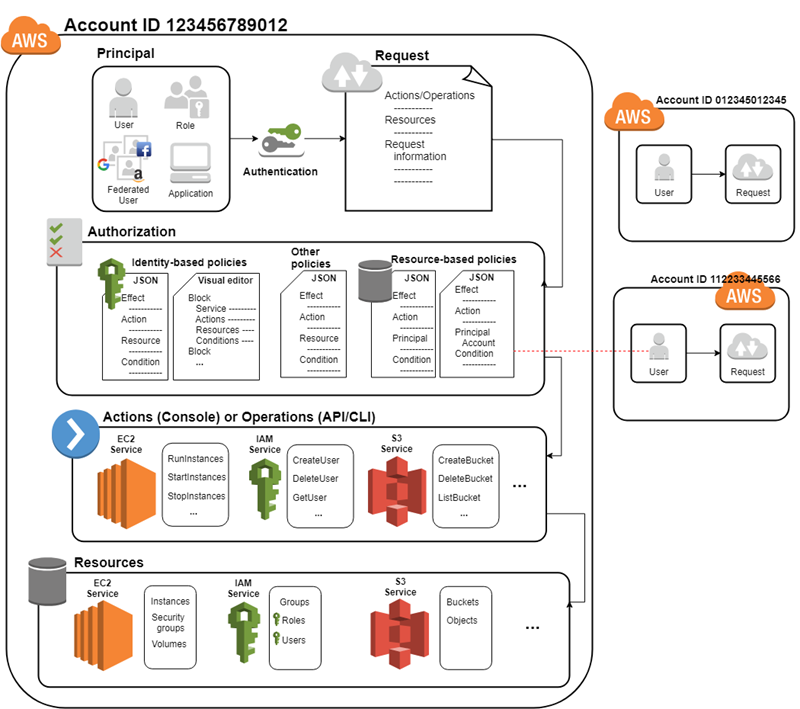
* **IAM** (Identity and Access Management)
  + Là 1 service giúp kiếm soát truy cập vào AWS resource
  + Đặc điểm
    - Tất cả billing sẽ tính vào root user
    - Global Service
  + Price
    - Free



* **Feature**

****

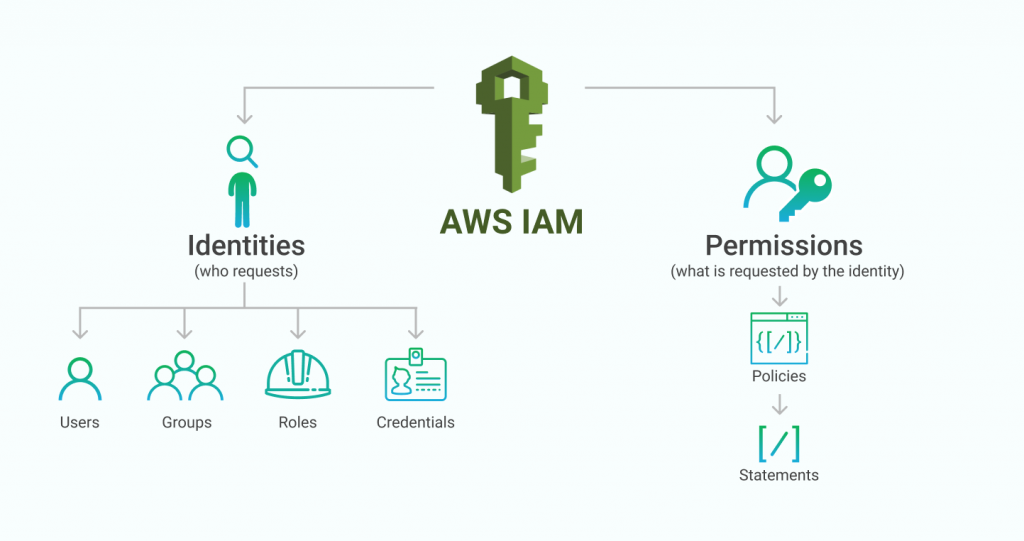
* **Flow**



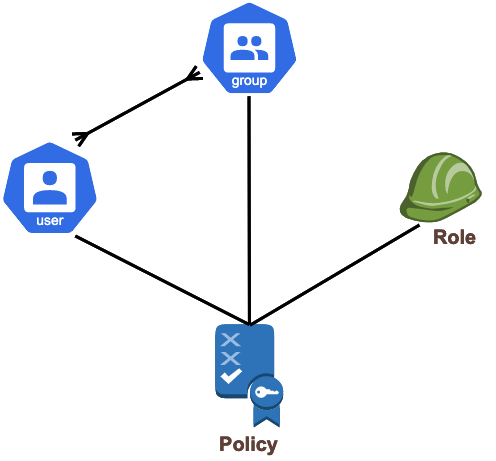
* + Principals
    - Là 1 person hoặc 1 application thực hiện request tới AWS resource
  + Request
  + Authenticated (signed in) & Authorized (has permissions) thông qua policy
    - Check xem principal có quyền truy cập vào resource không thông qua policy
  + Action & operation
    - Sau khi authen xong thì AWS sẽ thực thi các action & operation trong request
    - Tuỳ từng service thì có những action & operation khác nhau
  + Resource
    - Là các resource của từng service

<https://docs.aws.amazon.com/IAM/latest/UserGuide/intro-structure.html>

* **Các thành phần**



* + **Identity**
    - Bao gồm:
      * Users (Root User, IAM User, Federating existing user)
      * Groups
      * Roles/ Temporary security credentials
      * AWS resources (S3, EC2, application, …)



* + **Root user**
    - Đăng nhập bằng email & password trên UI Console
    - Đăng nhập thông qua access key trên CLI, SDK
    - Có full quyền admin
    - Best practice
      * Không nên đăng nhập nhiều, chỉ đăng nhập khi cần cấp quyền cho User, hoặc xem và thanh toán billing
      * Nên tạo MFA và remove access key (để tránh hacker scan được nếu upload code lên git, ...)
      * Nên tạo 1 IAM Group & IAM User và gán quyền admin để thay thế cho truy cập thường xuyên Root user
      * Set password policy cho IAM User để bảo mật cả IAM User
    - Bao gồm các thuộc tính
      * Access key (access key ID + a secret access key)
      * Password policy cho IAM User
      * MFA (Multi-factor authentication)
        + Phải điền thêm token ở device khác nữa mới đăng nhập được
      * Security Token Service (STS)

|  |  |
| --- | --- |
| *Login* | *Basic information*    *Security*    *Password policy*    *MFA* |

* + **IAM User**
    - Đăng nhập bằng email & password trên UI Console
    - Đăng nhập thông qua access key trên CLI, SDK
    - Bị giới hạn quyền do Root User cấp
    - Có thể có nhiều IAM user trong 1 Root user
    - Mỗi IAM user sẽ độc lập với nhau trong 1 Root user
    - Best practices
      * Mỗi IAM user có thể đại diện cho 1 person, application, service …
      * Long-term
    - Bao gồm các thuộc tính:
      * Account ID (Alias Account), username, password, console link
        + Thông tin để user đăng nhập thông tin console
      * Access key (access key ID + a secret access key)
        + Để đăng nhập thông qua CLI, SDK, API
        + Hoặc sử dụng cho các service kết nối với nhau (có thể sử dụng Role để thay thế)
        + Có tối đa 2 access key
      * Password rotation policy
      * MFA
      * Access type

Có 2 options

* + - * + Programmatic access

Cấp cho user access key và secret key cho sử dụng các tools như: API, CLI, SDK, ...

* + - * + AWS Management Console access

Cấp pasword cho đăng nhập console (generate ra password hoặc tự custom)

* + - * Permissions
        + Sử dụng policy để định nghĩa permission
        + Có các options

Group cho user (recommended)

Copy permission từ user khác

Gán permission trực tiếp cho user

* + - * + Permissions boundary

Để giới hạn quyền

Không thể thêm ngoài các permission đã define

* + - * X.509 Certificates
        + Dành cho SSL/TLS server certificate cho HTTPS connection cho website & Application
      * SSH keys for AWS CodeCommit
        + Giống private git
      * Access Advisor
        + Hiển thị thông tin của lần truy cập cuối cùng vào các servie mà user đã sử dụng
    - Có thể tạo nhiều user 1 lần, download user information (định dạng file csv) và send notification cho user

|  |  |
| --- | --- |
|  | *Login* |

* + **Federating existing user**
    - Đăng nhập thông qua Single Sign-On (SSO) 🡺 không cần tạo IAM User
    - Usecases
      * Login with Amazon, Facebook, Google, any OpenID Connect (OIDC), ...
      * Cho phép user đã đăng nhập thông qua tài khoản công ty
    - Sử dụng Session Role để định nghĩa permission


        Users who are already authenticated elsewhere can be federated into AWS without
          requiring an IAM user.
      

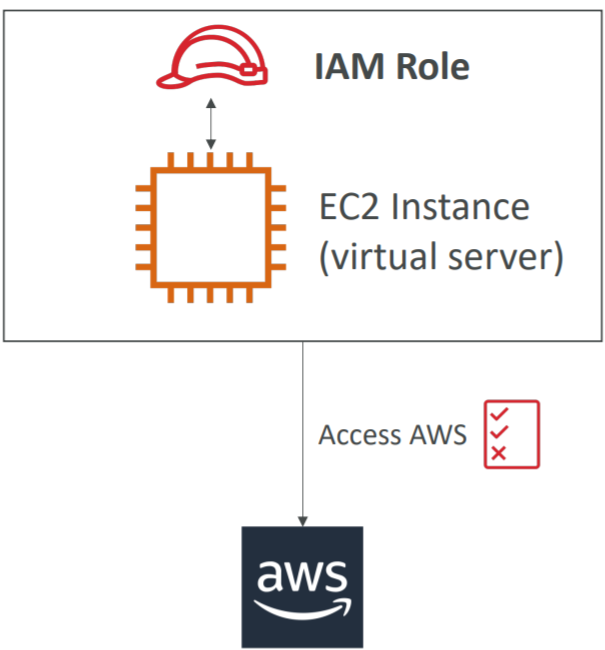
* + **IAM Group**
    - Có thể có nhiều Group trong 1 Root user
    - 1 group bao gồm 1 list các user có các policy giống nhau
    - 1 user có thể thuộc nhiều group
    - Best practices
      * Mỗi User trong group thường có role giống nhau

VD: project, department, position, ...

* + - Bao gồm các thuộc tính:
      * Name
      * Permission (tối đa 10 policies)
      * IAM users
      * Access Advisor
        + Hiển thị thông tin của lần truy cập cuối cùng vào các servie mà user đã sử dụng

|  |  |
| --- | --- |
| *Example of relationship between AWS accounts, users, and user groups* | *A user can belong to many groups* |

* + **IAM Role**



*Some AWS service will need to perform actions on your behalf*

* + - Giống user nhưng không có username & password, access key
    - Bao gồm 1 tập các policy
    - Có thể tái sử dụng
    - Usecases
      * Có thể gán cho AWS Service, Other AWS Account (Not for IAM User, IAM Group), Federating Existing User, Web Identity
        + AWS Service

Cho phép các AWS service (EC2, Lambda, …) thay mặt root user thực thi các action


        Application on an EC2 instance accessing an AWS resource
      

*Sau khi tạo Role thì sẽ vào EC2 để*

*Thay cho lưu access key trên application trên EC2 🡺 bảo mật hơn*

* + - * Other AWS Account

Cho phép account khác hoặc 3rd party truy cập resource


        Use a role to delegate permissions to a user in a different account
      

*Tạo 2 account khác nhau cho dev, product*

*Cho phép developer update resource trên product account*

* + - * Web Identity

Sử dụng cho Cognito hoặc OpenID

* + - * SAML 2.0 federation

Sử dụng cho Single Sign-On (SSO), corporate directory (mạng công ty)

Gán cho Federating existing user để sử dụng như 1 external user (thay cho IAM user)

* + - Bao gồm các thuộc tính
      * ARN
      * Maximum session duration
      * Type of trusted entity

Có các option

* + - * + AWS Service

EC2, Lambda, …các AWS service khác

* + - * + Other AWS Account

sử dụng cho account khác hoặc 3rd party

* + - * + Web Identity

Sử dụng cho Cognito hoặc OpenID

* + - * + SAML 2.0 federation

Sử dụng cho corporate directory (mạng công ty)

* + - * Permission
      * Access Advisor
  + **Temporary secutiry credentials**
    - Là thông tin đăng nhập tạm thời, tự động hết hạn sau 1 khoảng thời gian
    - Giống Role nhưng không tái sử dụng được
    - Session được generate từ AWS Security Token Service (AWS STS)

<https://sts.amazonaws.com>

* + - Usecase
      * Short-term
      * Sử dụng kết hợp với Federating existing user để đăng nhập single sign-on
  + **Policy**
    - Định nghĩa identity sẽ được thực hiện action nào với condition như nào
    - Đặc điểm
      * Định nghĩa bằng file JSON
      * Có thể attach policy nhiều các Identity, AWS resource

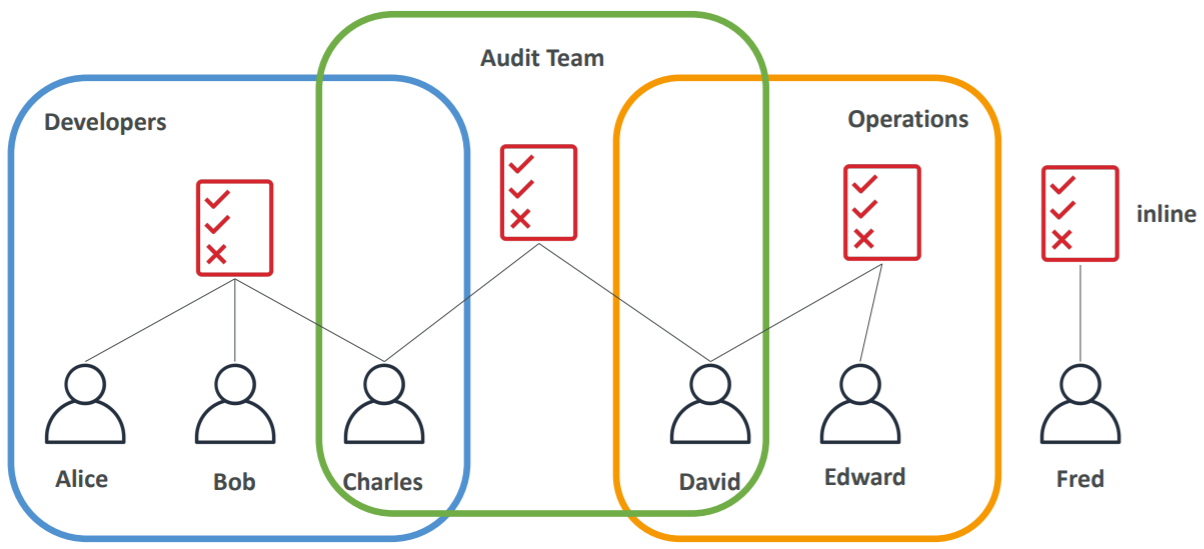
Khi attach policy vào identity thì sẽ gọi là permission

* + - * AWS sẽ tính toán kết hợp các policy lại để xác định xem request allow hay deny

Deny sẽ được ưu tiên hơn Allow

* + - * Có thể tạo nhiều policy và gộp lại với nhau được
      * Chỉ nên cấp vừa đủ permission cho User thực hiện
    - Các thành phần
      * Version & các statement
      * 1 statement là 1 single permission
      * Các thành phần trong 1 statement
        + Sid (Optional): statement ID
        + Effect: allow hoặc deny request
        + Principal: chỉ định identity
        + Action/NotAction: action thao tác với AWS Service
        + Resource: chỉ định resource được apply thông qua ARN (ID của resource)
        + Condition (Optional): điều kiện cho resource được apply

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| *Policies and permissions in IAM - AWS Identity and Access Management* | *Resource*    *ARN*   |  |  |  | | --- | --- | --- | | *Restrict based on tags* | *Force MFA* | *Restrict the client IP* |   *Condition* |



*Attach policy to Identities (IAM User, IAM Group, IAM Role)*

|  |  |
| --- | --- |
|  |  |

*Blacklist & WhiteList*

* + - VD:

|  |  |
| --- | --- |
|  |  |


        Policy summary dialog image
      

*Sau khi tạo xong policy sẽ xem được summary*

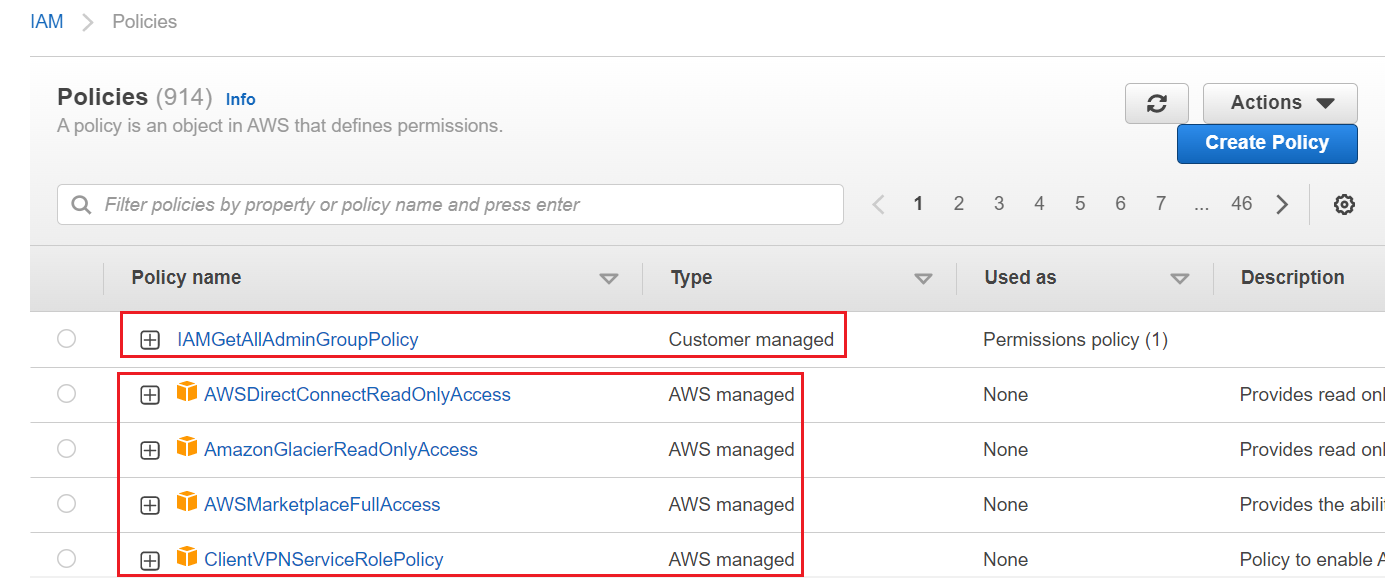
More example: <https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_examples.html>

* + - Có 2 loại
      * Customer managed

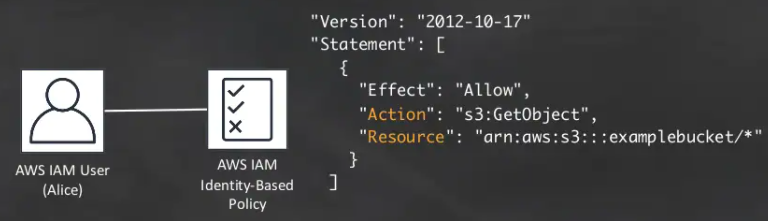
Policy do mình tự tạo

* + - * AWS managed

Policy do AWS tạo sẵn



* + - Có 6 loại
      * Identity-based policy
        + Policy cho identity (User, Group, Role)



* + - * Resource-based policy
        + Inline policy cho resource (S3 bucket, EC2, ..., IAM User, IAM Group, IAM Role)
        + Có thể trên cùng account hoặc granting cross-account access (Giống Other AWS Account trong IAM Role)

|  |  |
| --- | --- |
|  | Identity-based vs resource-based policies  <https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_identity-vs-resource.html> |

* + - * + Policy Evaluation Logic

|  |  |
| --- | --- |
|  |  |

* + - * Session policy
        + Temporary Session cho Role hoặc Federated User trong API, CLI


                Evaluation of a session policy, permissions boundary, and identity-based
                    policy
            

* + - * Permissions boundary
        + Giới hạn permission được thực hiện cho User, Role (Không support Group)

VD: Action chỉ được thực hiện khi có cả identity-based policy & Permission boundary

* + - * + Usecases

Tạo Role cho Lambda function

Tạo Role cho EC2 instances

Admin giới hạn permission được thực hiện cho Groups & Users

|  |  |
| --- | --- |
| Evaluation of a resource-based policy, permissions boundary, and                                 identity-based policy |  |

* + - * Organizations SCP
        + Sử dụng cho AWS Organizations service control policy (SCP)
        + SPC là 1 service để nhóm và quản lý tập trung các AWS account

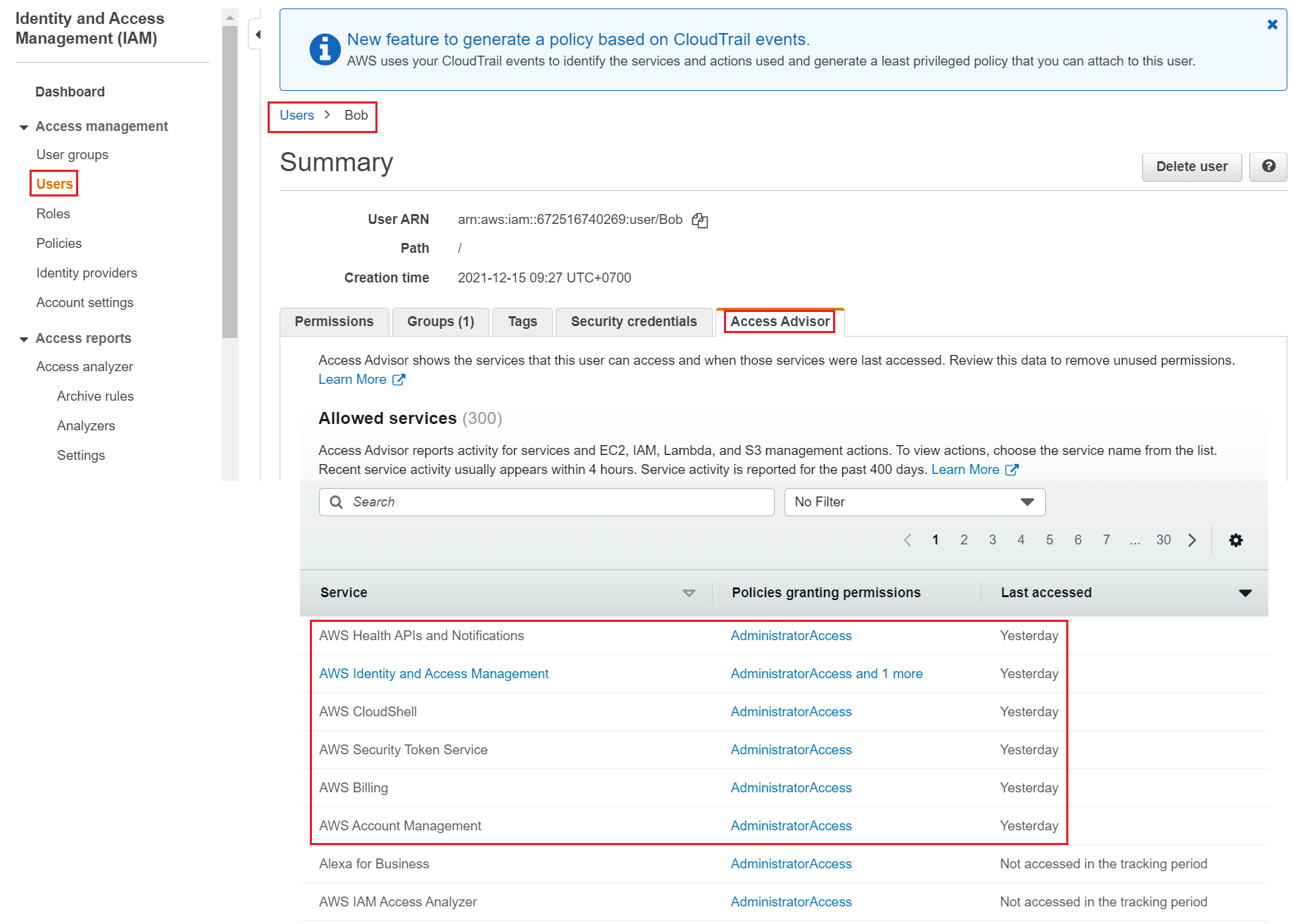

                Evaluation of an SCP, permissions boundary, and identity-based
                    policy
            

* + - * ACL (Access Control List)
        + Không sử dụng JSON
        + Cho phép account khác có thể truy cập được (Giống Resource-based policy và
      * Policies Evaluation

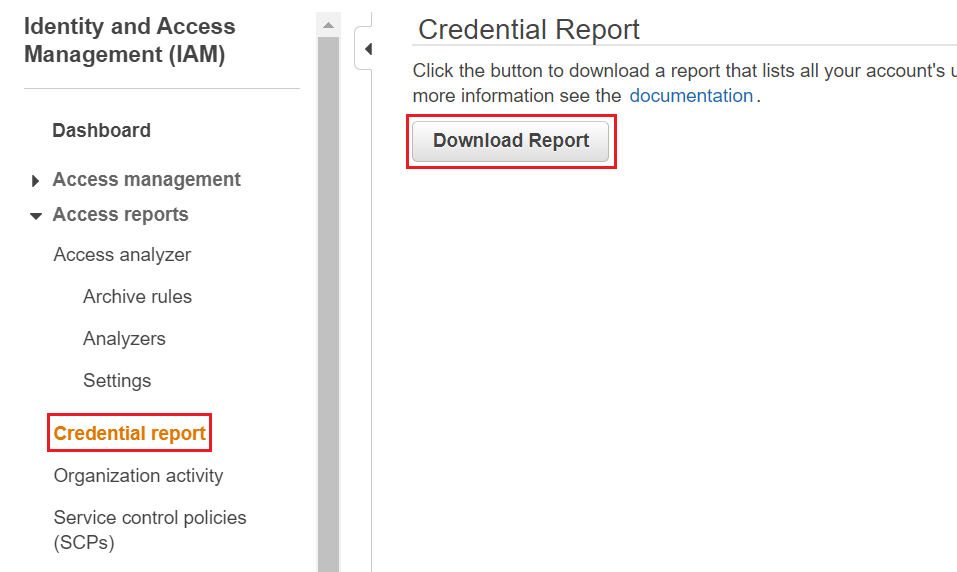

        Evaluation flow chart
      

[*https://docs.aws.amazon.com/IAM/latest/UserGuide/reference\_policies\_evaluation-logic.html*](https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_evaluation-logic.html)

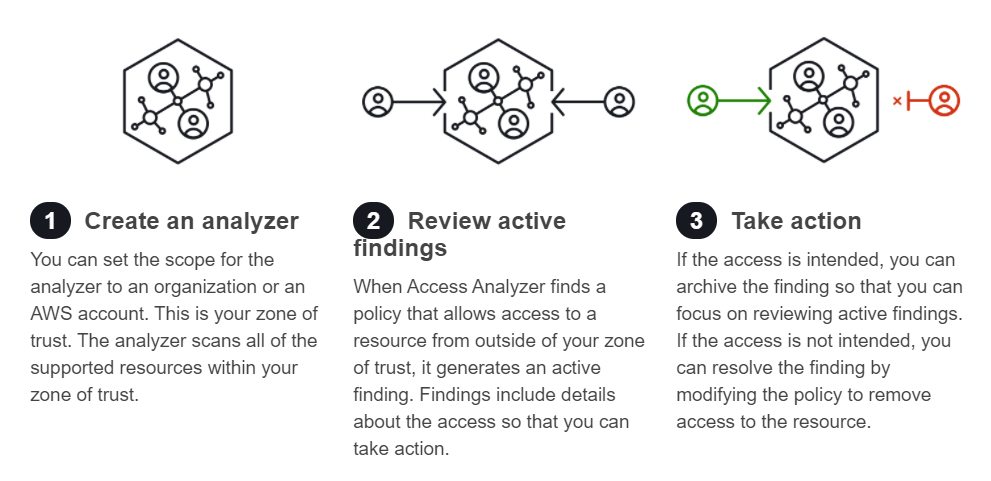
* + **Permission**
    - Khi attach policy vào identity thì sẽ gọi là permission
* **Tools**
  + Security
    - Access Advisor (user-level)
      * Để xem IAM User sử dụng service nào gần nhất 🡺 từ đó sẽ review lại policy đã cấp cho User



* + - Credentials Report (account-level)
      * Giống Access Advisor nhưng sẽ list ra tất cả IAM User trong Account



* + **IAM Access Analyzer**
    - Tool support phân tích các policy, permission



* + **Visual editor**
    - Tool để visualize policy
* **Login vào user thông qua Console, CLI, SDK**
  + Console
    - Đăng nhập thông qua Email/Username, password, MFA
    - Cho phép thao tác với AWS thông qua UI
  + CLI (Command Line Interface)
    - Đăng nhập thông qua access keys
    - Tools cho phép thao tác với AWS thông qua Command-line shell
    - Có thể sử dụng CloudShell trực tiếp trên AWS Console
  + SDK (Software Developer Kit)
    - Đăng nhập thông qua access keys
    - Sử dụng cho lập trình, thao tác với AWS service thông qua API
    - Support
      * Web: JavaScript, Python, PHP, .NET, Java, Go, Node.js, C++
      * Mobile: Android, iOS
      * IoT Devices: Embedded C, Arduino, …

|  |  |
| --- | --- |
| *Console*  *AWS SDK for Java on Twitter: &quot;We&#39;re happy to announce the general  availability of the AWS SDK for Java v2, featuring first class nonblocking  IO support, and a pluggable HTTP layer! https://t.co/R3jwTOYQVe*  *SDK* | *CLI*    *CloudShell* |

* **Config**
  + Setup


      Example layout of AWS account, groups, and users
    

<https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started.html>

* + IAM User, Group, Role, Root user

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id.html>

* + Common task

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction_quick-links-common-tasks.html>

* **Reference**

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>