

AWS雲端技術入門保證班

第三天

大綱

1. IAM 功能介紹
2. IAM Console介紹
3. IAM Policy Simulator
4. IAM 功能介紹(2)

什麼是IAM

取用AWS資源，需要經過驗證。而這些驗證及監控的機制管理，稱其為Identity Access Management。

IAM的功能

限制特定用戶登入

限制特定用戶請求AWS資源

限制AWS資源間的請求

限制跨帳號間的AWS資源請求與管理

IAM的調用方式

AWS Management Console

AWS Command Line Tools

AWS SDKs

IAM HTTPs API

Users

root

IAM User

Federating Existing Users

Federating Existing Users

使用場景

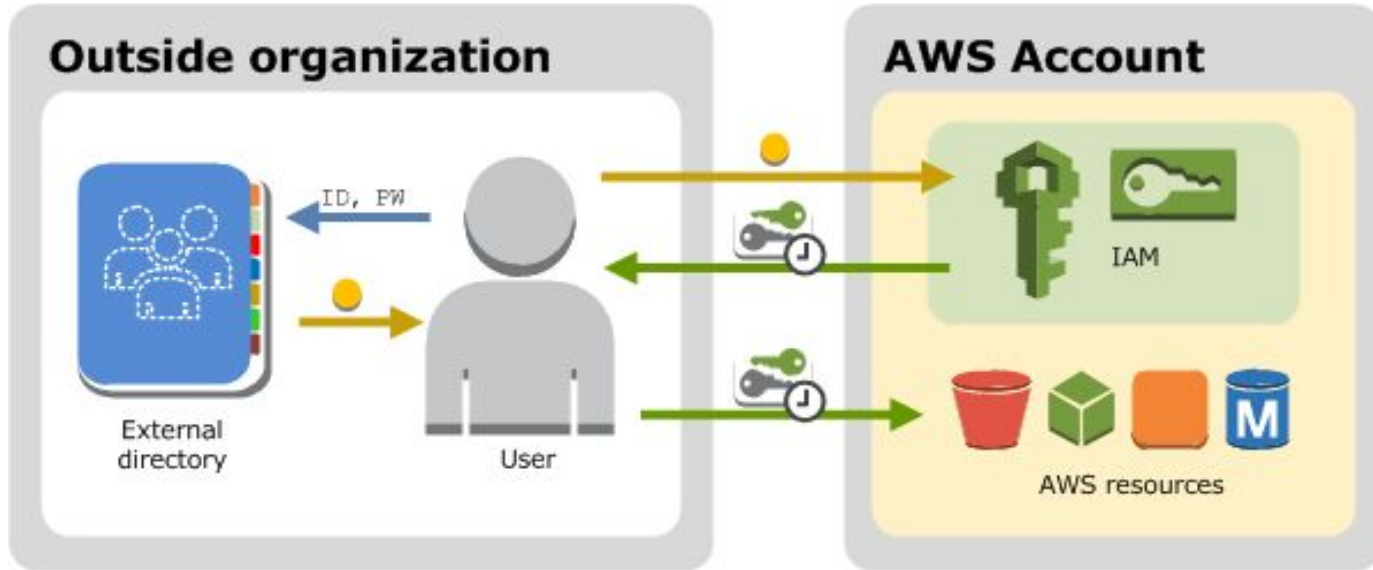
Your users already have identities in a corporate directory.

corporate directory is compatible with Security Assertion Markup Language 2.0 (SAML 2.0), you can configure your corporate directory to provide single-sign on (SSO) access to the AWS Management Console for your users.

Your users already have Internet identities.

creating a mobile app or web-based app that can let users identify themselves through an Internet identity provider like Login with Amazon, Facebook, Google, or any OpenID Connect (OIDC) compatible identity provider, the app can use federation to access AWS.

Federating Existing Users



Federated Users and Roles

聯合身分用戶需要透過 role來取得aws服務，對role設定policy，而後用戶連入時，會套用此role的設定。

Federated users don't have permanent identities in your AWS account the way that IAM users do. To assign permissions to federated users, you can create an entity referred to as a role and define permissions for the role. When a federated user signs in to AWS, the user is associated with the role and is granted the permissions that are defined in the role.

Permissions and Policies

功能介紹

helps you to define what a user or other entity is allowed to do in an account, often referred to as authorization. Permissions are granted through policies that are created and then attached to users, groups, or roles.

Identity-based and Resource-based Policies

Resource-base與 User-base的差異

我們可為資源設policy, 限制其能存取的對象

A resource-based policy contains slightly different information than a user-based policy. In a resource-based policy you specify what actions are permitted and what resource is affected (just like a user-based policy). However, you also explicitly list who is allowed access to the resource. (In a user-based policy, the "who" is established by whomever the policy is attached to.)

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": {"AWS": "arn:aws:iam::777788889999:user/bob"},
    "Action": [
      "s3:PutObject",
      "s3:PutObjectAcl"
    ],
    "Resource": "arn:aws:s3:::example-bucket/*"
  }
}
```

Security Features Outside of IAM

ec2, 使用金鑰登入

Amazon EC2

在 Amazon Elastic Compute Cloud 中，需要使用密鑰對（對於 Linux 实例）或使用用戶名稱和密碼（對於 Windows 实例）來登錄实例。

RDS, 使用帳密登入

Amazon RDS

在 Amazon Relational Database Service 中，需要使用與數據庫關聯的用戶名稱和密碼來登錄數據庫引擎。

EC2與 RDS 透過Security group 來控制封包流出流入

Amazon EC2 和 Amazon RDS

在 Amazon EC2 和 Amazon RDS 中，需要使用安全組來控制發送到实例或數據庫的流量。

WorkSpaces

Amazon WorkSpaces

在 Amazon WorkSpaces 中，用戶使用用戶名稱和密碼登錄桌面。

Quick Links to Common Tasks

展示常見任務

Sign in as an IAM user

Manage passwords for IAM users

Manage permissions for IAM users

List the users in your AWS account and get information about their credentials

Add multi-factor authentication (MFA)

Get an access key

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

Common Tasks Demo

IAM的最佳实践

- Lock Away Your AWS Account (Root) Access Keys
- Create Individual IAM Users
- Use AWS-Defined Policies to Assign Permissions Whenever Possible
- Use Groups to Assign Permissions to IAM Users
- Grant Least Privilege
- Use Access Levels to Review IAM Permissions
- Configure a Strong Password Policy for Your Users
- Enable MFA for Privileged Users
- Use Roles for Applications That Run on Amazon EC2 Instances
- Delegate by Using Roles Instead of by Sharing Credentials
- Rotate Credentials Regularly
- Remove Unnecessary Credentials
- Use Policy Conditions for Extra Security
- Monitor Activity in Your AWS Account
- Video Presentation About IAM Best Practices

Lock Away Your AWS Account (Root) Access Keys

access key的功能

an access key (an access key ID and secret access key) to make programmatic requests to AWS.

不要使用 root身分的 access key

do not use your AWS account (root) access key. The access key for your AWS account gives full access to all your resources for all AWS services, including your billing information. You cannot restrict the permissions associated with your AWS account access key.

Lock Away Your AWS Account (Root) Access Keys

因此，在保护 AWS 账户访问密钥时应像对待您的信用卡号或任何其他敏感机密信息一样。以下是执行该操作的一些方式：

- 如果您尚未拥有 AWS 账户的访问密钥，请勿创建它，除非绝对需要。应使用您的账户的电子邮件地址和密码登录 [AWS 管理控制台](#)，为自己创建具有管理权限的 IAM 用户，正如下一部分所说明的那样。
- 如果您已经拥有 AWS 账户的访问密钥，请删除它。如果您一定要保留它，请定期轮换（更改）访问密钥。若要删除或轮换 AWS 账户访问密钥，请转至 AWS 管理控制台中的[安全证书页](#)并使用您账户的电子邮件地址和密码登录。可以在 **Access Keys (访问密钥)** 部分管理您的访问密钥。
- 切勿与任何人分享您的 AWS 账户密码或访问密钥。本文档的其余部分讨论了避免与其他用户分享您的账户证书以及避免将证书嵌入应用程序中的几种方法。
- 使用强密码有助于保护对 AWS 管理控制台 进行账户级别的访问。有关管理 AWS 账户密码的信息，请参阅[更改 AWS 账户（“根”）密码](#)。
- 对您的 AWS 账户启用 AWS Multi-Factor Authentication (MFA)。有关更多信息，请参阅 [在 AWS 中使用多重验证 \(MFA\)](#)。

Create Individual IAM Users

創建個別的IAM用戶並進行操作行為的差異化，且可針對用戶做出功能變化。

By creating individual IAM users for people accessing your account, you can give each IAM user a unique set of security credentials. You can also grant different permissions to each IAM user. If necessary, you can change or revoke an IAM user's permissions any time.

若 root access key 給出去了，則安全性堪慮。

(If you give out your AWS root credentials, it can be difficult to revoke them, and it is impossible to restrict their permissions.)

Use AWS-Defined Policies to Assign Permissions

推薦使用aws 寫好的policy, 因為他們會由aws維護及更新。

We recommend that you use the managed policies that are created and maintained by AWS to grant permissions whenever possible. A key advantage of using these policies is that they are maintained and updated by AWS as new services or new APIs are introduced.

適用場景在一些通用任務上

AWS-managed policies are designed to support common tasks. They typically provide access to a single service or a limited set of actions.

Use Groups to Assign Permissions to IAM Users

使用群組來管理用戶

Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (administrators, developers, accounting, etc.).

用群組的話，好處在於可針對群體更改權限

you can make changes for everyone in a group in just one place. As people move around in your company, you can simply change what IAM group their IAM user belongs to.

Grant Least Privilege

在您创建 IAM 策略时，请遵循授予最小权限这一标准的安全建议，即仅授予执行任务所需的权限。首先，确定用户需要执行的任务，然后，拟定仅允许用户执行这些任务的策略。

应先尽量授予一组具有最小许可的许可，然后根据需要授予额外许可，而不应先授予过于宽松的许可，而后再试图收紧。

在界定一组正确的许可时，需开展某些研究，以确定特定任务所需的许可、特定产品所支持的操作及为执行这些操作所需的许可。

可額外使用Access Advisor 這個選項卡來確認用戶的權限能力及存取權限的最近一次時間

http://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies_access-advisor.html

Use Access Levels to Review IAM Permissions

用 List 讀 寫 full access 四種能力 來設計資源取用

When you review a policy, you can view the policy summary that includes a summary of the access level for each service within that policy. AWS categorizes each service action into one of four access levels based on what each action does: `List`, `Read`, `Write`, or `Permissions management`. You can use these access levels to determine which actions to include in your policies.

Configure a Strong Password Policy for Your Users

增加密碼複雜度，使破解難度變高。

Enable MFA for Privileged Users

users have a device that generates a unique authentication code (a one-time password, or OTP). Users must provide both their normal credentials (like their user name and password) and the OTP. The MFA device can either be a special piece of hardware, or it can be a virtual device (for example, it can run in an app on a smartphone).

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html

Use Roles for Applications That Run on Amazon EC2 Instances

使用情境

Applications that run on an Amazon EC2 instance need credentials in order to access other AWS services.

IAM Role 提供 temporary credentials

To provide credentials to the application in a secure way, use IAM roles. A role is an entity that has its own set of permissions, but that isn't a user or group. Roles also don't have their own permanent set of credentials the way IAM users do. In the case of Amazon EC2, IAM dynamically provides temporary credentials to the EC2 instance, and these credentials are automatically rotated for you.

Delegate by Using Roles Instead of by Sharing Credentials

盡可能透過使用Role的方式進行功能，而非Credentials。

Rotate Credentials Regularly

定期輪換 用戶的Credential

Change your own passwords and access keys regularly, and make sure that all IAM users in your account do as well.

Remove Unnecessary Credentials

Remove IAM user credentials (that is, passwords and access keys) that are not needed.

範例

For example, an IAM user that is used for an application does not need a password (passwords are necessary only to sign in to AWS websites). Similarly, if a user does not and will never use access keys, there's no reason for the user to have them.

可觀看 最近使用時間

For passwords and access keys, the credential report shows how recently the credentials have been used. Passwords and access keys that have not been used recently might be good candidates for removal.

Use Policy Conditions for Extra Security

進階針對某些用戶設定權限

To the extent that it's practical, define the conditions under which your IAM policies allow access to a resource.

比如 ip, 或 mfa 驗證

For example, you can write conditions to specify a range of allowable IP addresses that a request must come from. You can also specify that a request is allowed only within a specified date range or time range. You can also set conditions that require the use of SSL or MFA (multi-factor authentication). For example, you can require that a user has authenticated with an MFA device in order to be allowed to terminate an Amazon EC2 instance.

Monitor Activity in Your AWS Account

監看帳戶活動

use logging features in AWS to determine the actions users have taken in your account and the resources that were used.

Logging features are available in the following AWS services:

- [Amazon CloudFront](#) – Logs user requests that CloudFront receives. For more information, see [Access Logs](#) in the *Amazon CloudFront Developer Guide*.
- [AWS CloudTrail](#) – Logs AWS API calls and related events made by or on behalf of an AWS account. For more information, see the [AWS CloudTrail User Guide](#).
- [Amazon CloudWatch](#) – Monitors your AWS cloud resources and the applications you run on AWS. You can set alarms in CloudWatch based on metrics that you define. For more information, see the [Amazon CloudWatch User Guide](#).
- [AWS Config](#) – Provides detailed historical information about the configuration of your AWS resources, including your IAM users, groups, roles, and policies. For example, you can use AWS Config to determine the permissions that belonged to a user or group at a specific time. For more information, see the [AWS Config Developer Guide](#).
- [Amazon Simple Storage Service \(Amazon S3\)](#) – Logs access requests to your Amazon S3 buckets. For more information, see [Server Access Logging](#) in the *Amazon Simple Storage Service Developer Guide*.

商業案例探討

http://docs.aws.amazon.com/zh_cn/IAM/latest/UserGuide/IAM_UseCases.html

商業案例探討

Joe 是 Example Corp 创始人。在公司成立之初，他创建了自己的 **AWS 账户**，他本人使用 AWS 产品。之后，他雇佣了员工，担任**开发人员、管理员、测试人员、管理人员及系统管理员**。

第一步—創建Admin 群組及管理者用戶

Joe 將 AWS 管理控制台 與 AWS 帳戶的安全證書結合使用，

Joe自己創建了名為 Joe 的用戶和名為 Admins 的組。他向 Admins 組授予了在所有 AWS 帳戶的資源上執行所有操作的權限 (即，根特權)，然後將 Joe 用戶添加到 Admins 組。

Joe 停止使用 AWS 帳戶的證書與 AWS 互動，而他開始只使用他的用戶證書。

第二步—考慮所有用戶的基本權限

Joe 还创建了一个名为 AllUsers 的组，这样他就可以将任何账户范围内的权限轻松应用于 AWS 账户内的所有用户。

第三步—因應不同單位，建立不同群組

他将本人添加至该群组。随后，他又创建了名为 Developers、Testers、Managers 及 SysAdmins 的群组。他为每位员工创建了用户，并将这些用户归入各自的群组。他还将所有用户添加至 AllUsers 群组。

第四步－設計使用EC2之相關策略

对 AllUsers 组附加一个策略。如果来源 IP 地址位于 Example Corp 企业网络外部, 则此策略拒绝用户的任何 AWS 请求。

System Administrators – 需要创建和管理 AMI、实例、快照、卷、安全组等的权限。Joe 向 SysAdmins 组附加了一个策略, 该策略授予组成员使用所有 Amazon EC2 操作的权限。

Developers – 只需能够使用实例即可。因此, Joe 向 Developers 组附加了允许开发人员调用 DescribeInstances、RunInstances、StopInstances、StartInstances 及 TerminateInstances 的策略。

Managers – 应无法执行任何 Amazon EC2 操作, 但可列出当前可用的 Amazon EC2 资源。因此, Joe 向 Managers 组附加了一个仅允许用户调用 Amazon EC2“Describe”API 的策略。

第五步—有人員出現職務變動

其中一位开发人员 Don 的角色发生转变，成为一名管理人员。Joe 将 Don 从 Developers 群组转移至 Managers 群组。现在，Don 处于 Managers 群组中，因此他使用 Amazon EC2 实例的能力受到限制。他无法启动或启用实例。即使他是启动或启用实例的用户，也无法停止或终止现有实例。他只能列出 Example Corp 用户已启动的实例。

第六步－設計使用S3之相關策略

Example Corp 的公司还使用了 Amazon S3。Joe 已为公司创建了 Amazon S3 存储段, 并命名为 `example_bucket`, 並创建其他用户和群组。

作为员工, Don 和 Mary 都需要能够在公司的存储桶中创建他们自己的数据。他们还需要读取和写入所有开发人员都要处理的共享数据。为做到这一点, Joe 采用 Amazon S3 密钥前缀方案, 在 `example_bucket` 中按照逻辑方式排列数据

第七步 — 設計S3之Bucket結構以因應人員取用

```
/example_bucket
  /home
    /don
    /mary
  /share
    /developers
    /managers
```

Joe 针对每位员工将主 /example_bucket 分隔成一系列主目录，并为开发人员和管理人员群组留出一个共享区域。

现在，Joe 创建一组策略，以便向用户和群组分配许可：

- **Don** 的主目录访问 – Joe 向 Don 附加的策略允许后者读取、写入和列出带 Amazon S3 键前缀 /example_bucket/home/don/ 的任何对象
- **Mary** 的主目录访问 – Joe 向 Mary 附加的策略允许后者读取、写入和列出带 Amazon S3 键前缀 /example_bucket/home/mary/ 的任何对象
- **Developers** 组的共享目录访问 – Joe 向该组附加的策略允许开发人员读取、写入和列出 /example_bucket/share/developers/ 中的任何对象
- **Managers** 组的共享目录访问 – Joe 向该组附加的策略允许管理人员读取、写入和列出 /example_bucket/share/managers/ 中的任何对象

第八步—有人員出現職務變動

用戶的角色轉換

此時，其中一位開發人員 Don 的角色發生轉變，成為一名管理人員。我們假設他不再需要訪問 share/developers 目錄中的文檔。作為管理員，Joe 將 Don 從 Managers 群組移動至 Developers 群組。通過簡單的重新分配，Don 將自動獲得所有授予 Managers 群組的權限，但將無法訪問 share/developers 目錄中的數據。

第九步—與其他公司進行資料交換

组织经常与合作公司、顾问及承包商合作。Example Corp 为 Widget Company 的合作伙伴，而 Widget Company 的员工 Natalie 需要将数据放入存储桶中，以供 Example Corp 使用。Joe 创建了一个名为 WidgetCo 的组和名为 Natalie 的用户，并将 Natalie 添加至 WidgetCo 组。Joe 还创建了一个名为 example_partner_bucket 的专用存储桶，以供 Natalie 使用。

休息一下，冷卻同學思緒。

五種取得 aws resource 的身分

IAM Users IAM Groups

IAM Roles

Temporary Credentials

Federate user

The Account "Root" User

User的使用場景

You created an AWS account and you're the only person who works in your account.

Other people in your group need to work in your AWS account, and your group is using no other identity mechanism.

You want to use the command-line interface (CLI) to work with AWS.

Users in your company are authenticated in your corporate network and want to be able to use AWS without having to sign in again—that is, you want to allow users to federate into AWS.

兩種方式

使用 公司已存在的identity system

使用 custom proxy server

http://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_enable-console-custom-url.html

Don't create IAM users. Configure a federation relationship between your enterprise identity system and AWS. You can do this in two ways:

- If your company's identity system is compatible with SAML 2.0, you can establish trust between your company's identity system and AWS. For more information, see [About SAML 2.0-based Federation](#).
- Create and use a custom proxy server that translates user identities from the enterprise into IAM roles that provide temporary AWS security credentials. For more information, see [Creating a URL that Enables Federated Users to Access the AWS Management Console \(Custom Federation Broker\)](#).

Role的使用場景

You're creating an application that runs on an Amazon Elastic Compute Cloud (Amazon EC2) instance and that application makes requests to AWS.

Role的使用場景

You're creating an app that runs on a mobile phone and that makes requests to AWS.

Don't create an IAM user and distribute the user's access key with the app. Instead, use an identity provider like Login with Amazon, Amazon Cognito, Facebook, or Google to authenticate users and map the users to an IAM role. The app can use the role to get temporary security credentials that have the permissions specified by the policies attached to the role. For more information, see the following:

- Amazon Cognito Overview in the AWS Mobile SDK for Android Developer Guide
- Amazon Cognito Overview in the AWS Mobile SDK for iOS Developer Guide
- About Web Identity Federation

User 在aws上要注意的事情

- Users
 - Adding a User
 - How IAM Users Sign In to Your AWS Account
 - Managing Users
 - Changing Permissions for a User
- Passwords
 - Access Keys
 - Retrieving Lost Passwords or Access Keys
- Multi-Factor Authentication (MFA)
 - Finding Unused Credentials
 - Getting Credential Reports
 - Using IAM with AWS CodeCommit: Git Credentials, SSH Keys, and AWS Access Keys
 - Working with Server Certificates

Finding Unused Credentials

找出已經沒有使用的Credentials，確保雲端安全。

When users leave your organization or services are no longer used, it is important to find the credentials that they were using and ensure that they are no longer operational. Ideally, you delete credentials if they are no longer needed. You can always recreate them at a later date if the need arises. At the very least you should change the credentials so that the former users no longer have access.

Of course, the definition of "unused" can vary and usually means a credential that has not been used within a specified period of time.

Retrieving Your Lost or Forgotten Passwords or Access Keys

失去Cred或密碼，不能回復，但可以刪除或重設。

For security reasons, you cannot retrieve console passwords or the secret access key part of an access key pair after you create it. If you lose one of these, it cannot be recovered and you must have your administrator reset your password or create a new access key for you, as appropriate.

Getting Credential Reports for Your AWS Account

調閱Credential地使用報告，來得知各個用戶的使用狀況。

You can generate and download a credential report that lists all users in your account and the status of their various credentials, including passwords, access keys, and MFA devices. You can get a credential report from AWS

use credential reports to assist in your auditing and compliance efforts. You can use the report to audit the effects of credential lifecycle requirements, such as password and access key rotation. You can provide the report to an external auditor, or grant permissions to an auditor so that he or she can download the report directly.

IAM Roles

- Roles Terms and Concepts
- Common Scenarios for Roles: Users, Applications, and Services
- Identity Providers and Federation
- Creating IAM Roles
- Using IAM Roles
- Managing IAM Roles
- How IAM Roles Differ from Resource-based Policies

Roles Terms and Concepts

定義

essentially a set of permissions that grant access to actions and resources in AWS.

- An IAM user in the same AWS account as the role
- An IAM user in a different AWS account as the role
- A web service offered by AWS such as Amazon Elastic Compute Cloud (Amazon EC2)
- An external user authenticated by an external identity provider (IdP) service that is compatible with SAML 2.0 or OpenID Connect, or a custom-built identity broker.

Delegation

定義

granting permission to someone that allows access to resources that you control.

能對下面三種帳號 進行 資源分配

- The same account.
- Two accounts that are both under your (organization's) control.
- Two accounts owned by different organizations.

Federation

定義

Federation is creating a trust relationship between an external identity provider and AWS. Users can sign in to a web identity provider, such as Login with Amazon, Facebook, Google, or any IdP that is compatible with OpenID Connect (OIDC).

Policy

An IAM policy is a document in JSON format in which you define the permissions for a role. The document is written according to the rules of the IAM Policy Language.

創建role的時候，會有兩個policy，一個為trust policy，一個為permissions policy
When you create a role, you create two separate policies for it: a trust policy, which specifies who is allowed to assume the role (the trusted entity, or principal; see the next term), and the permissions policy, which defines what actions and resources the principal is allowed to use.

Trust policy

Permissions

Trust relationships

Access Advisor

Revoke sessions

You can view the trusted entities that can assume the role and the access conditions for the role. [Show policy document](#)

Edit trust relationship

Trusted entities

The following trusted entities can assume this role.

Trusted entities

The identity provider(s) `ec2.amazonaws.com`

Conditions

The following conditions define how and when trusted entities can assume the role.

There are no conditions associated with this role.

Edit Trust Relationship

You can customize trust relationships by editing the following access control policy document.

Policy Document

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Principal": {  
7         "Service": "ec2.amazonaws.com"  
8       },  
9       "Action": "sts:AssumeRole"  
10    }  
11  ]  
12 }
```

Cancel

Update Trust Policy

Permission policy

Permissions

Trust relationships

Access Advisor

Revoke sessions

Managed Policies



The following managed policies are attached to this role. You can attach up to 10 managed policies.

Attach Policy

Policy Name	Actions
s3_iii_common	Show Policy Detach Policy Simulate Policy
iii_ec2_group2	Show Policy Detach Policy Simulate Policy
iii_s3_group2	Show Policy Detach Policy Simulate Policy

Inline Policies



Cross-account access

定義

Granting access to resources in one account to a trusted principal in a different account is often referred to as cross-account access.

Roles: Users, Applications, and Services

讓用戶可以切換身分

讓ec2可以使用temp credentials調用資源

- IAM users in your account using the IAM console can *switch to* a role to temporarily use the permissions of the role in the console. The users give up their original permissions and take on the permissions assigned to the role. When the users exit the role, their original permissions are restored.
- An application or a service offered by AWS (like Amazon EC2) can *assume* a role by requesting temporary security credentials for a role with which to make programmatic requests to AWS. You use a role this way so that you don't have to share or maintain long-term security credentials (for example, by creating an IAM user) for each entity that requires access to a resource.

Roles: Users, Applications, and Services

簡單版用途

自己的帳號間切換身分

The simplest way to use roles is to grant your IAM users permissions to switch to roles that you create within your own or another AWS account.

複雜用途

讓程式碼或外部用戶 調用 AssumeRole 取得 temp cred,

granting access to applications and services, or federated external users, you can call the `AssumeRole` API. This API call returns a set of temporary credentials that the application can use in subsequent API calls. Actions attempted with the temporary credentials have only the permissions granted by the associated role. An application doesn't have to "exit" the role the way a user in the console does; rather the application simply stops using the temporary credentials and resumes making calls with the original credentials.

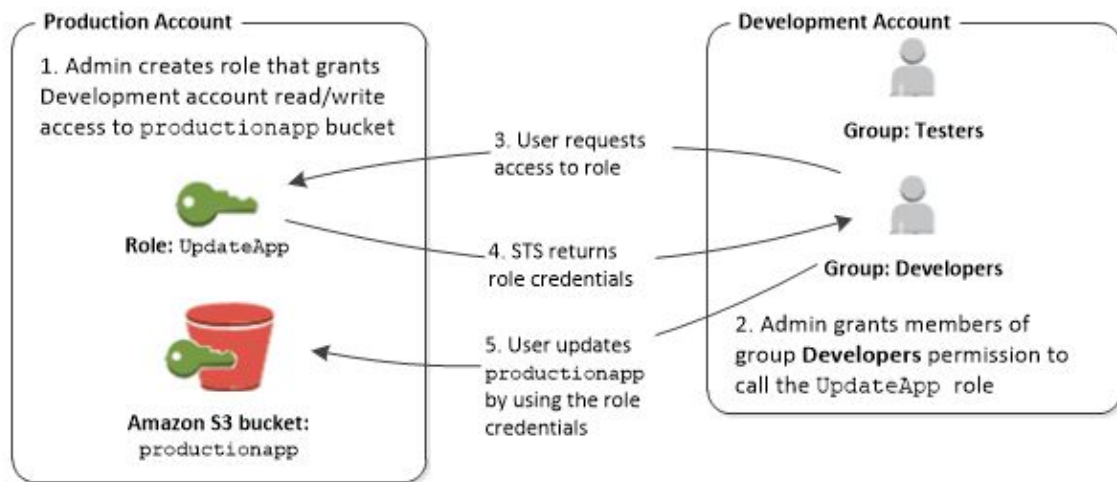
Providing Access to an IAM User in Another AWS Account That You Own

一个账户中的用户可以切换为相同或不同账户中的角色。使用角色过程中，用户只能执行角色允许的操作并且只能访问角色允许的资源；其原始用户权限处于暂停状态。用户退出角色时，恢复原始用户权限。

A user in one account can switch to a role in the same or a different account. While using the role, the user can perform only the actions and access only the resources permitted by the role; their original user permissions are suspended. When the user exits the role, the original user permissions are restored.

實際案例

your organization has multiple AWS accounts to isolate a development environment from a production environment. Users in the development account might occasionally need to access resources in the production account, such as when you are promoting an update from the development environment to the production environment.



Providing Access to AWS Accounts Owned by Third Parties

When third parties require access to your organization's AWS resources, you can use roles to delegate access to them.

案例

For example, a third party might provide a service for managing your AWS resources. With IAM roles, you can grant these third parties access to your AWS resources without sharing your AWS security credentials. Instead, the third party can access your AWS resources by assuming a role that you create in your AWS account.

開放第三方來取用AWS服務時要注意的事情

Important

When you grant third parties access to your AWS resources, they can access any resource that you give them permissions to and their use of your resources is billed to you. Ensure that you limit their use of your resources appropriately.

Providing Access to Externally Authenticated Users

使用 Role及 第三方的 identity provider, 讓用戶可有短暫取得aws資源的能力

Your users might already have identities outside of AWS, such as in your corporate directory. If those users need to work with AWS resources (or work with applications that access those resources), then those users also need AWS security credentials. You can use an IAM role to specify permissions for users whose identity is federated from your organization or a third-party identity provider (IdP).

Policy Simulator

Policy Simulator

應用場景

透過不污染真實環境的沙盒環境中，撰寫Policy，測試可行性，
you can test and troubleshoot IAM and resource-based policies

可針對用戶或群組做 policy測試，可針對整體或單條policy做效果測試
Test policies that are attached to IAM users, groups, or roles in your AWS account.
If more than one policy is attached to the user, group, or role, you can test all the policies, or select individual policies to test. You can test which actions are allowed or denied by the selected policies for specific resources.

可使用對象

默认情况下，可访问 AWS 控制台的任何用户均可使用该模拟器来测试尚未附加到用户、组或角色的策略。只需从顶部的模式菜单中选择 New Policy，在 Policy Sandbox 下选择 Create New Policy，然后将策略键入或复制到该模拟器中。此处添加的策略仅用于模拟，因此不会披露敏感信息。

若是想要測已存在用戶或資源的policy

要測用戶的policy, 必須可以看到用戶policy

要測資源的policy, 必須能夠看到資源的policy

To allow a console user to test policies that are attached to IAM users, groups, or roles, you must provide your users with permissions to retrieve those policies. To allow console users to test resource-based policies, you must provide your users with permission to retrieve the resource's policy.

使用流程

登入aws console, 並切換至IAM Console

進入Policy Simulator頁面

撰寫Policy

選擇欲測試的Service、相關action及Condition

執行測試

觀察結果

實際展示流程一登入至IAM Console



Security, Identity & Compliance

IAM

Inspector

Certificate Manager

Directory Service

WAF & Shield

Compliance Reports

進入Policy 模擬器

Welcome to Identity and Access Management

We encountered the following errors while processing your request:

- ✖ User: arn:aws:iam::129729052534:user/student1 is not authorized to perform: iam:GetAccountSummary
- ✖ User: arn:aws:iam::129729052534:user/student1 is not authorized to perform: iam:ListAccountAliases

IAM Resources

We encountered the following errors while processing your request:

- ✖ User: arn:aws:iam::129729052534:user/student1 is not authorized to perform: iam:GetAccountSummary
- ✖ User: arn:aws:iam::129729052534:user/student1 is not authorized to perform: iam:ListAccountAliases

Security Status

 1 out of 5 complete. 4 checks failed.

- | | | |
|---|-----------------------------------|---|
| ? | Activate MFA on your root account | ▼ |
| ? | Create individual IAM users | ▼ |
| ? | Use groups to assign permissions | ▼ |

Feature Spotlight



Additional Information

[IAM documentation](#)

[Web Identity Federation Playground](#)

[Policy Simulator](#)

[Videos, IAM release history and additional resources](#)

更改為New Policy



Users, Groups, and Roles

Users

Policy Simulator

Select service Select actions

▸ Global Settings ⓘ

Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
---------	--------	---------------	---------------------	------------

Users, Groups, and Roles

Users

Policy Simulator


Select service Select actions

▸ Global Settings ⓘ

Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]


Service	Action	Resource Type	Simulation Resource	Permission
---------	--------	---------------	---------------------	------------

創建新的模擬Policy

 IAM Policy Simulator

Mode : New Policy ▾

student1 ▾



Policy Sandbox

Create New Policy

Custom IAM Policies

Resource Policies

Policy Simulator

Select service ▾ Select actions ▾ Select All Deselect All

Reset Contexts Clear Results Run Simulation

▸ Global Settings ⓘ

Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
---------	--------	---------------	---------------------	------------

demo用之S3 Policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": ["s3:ListBucket"],  
      "Resource": ["arn:aws:s3:::*"]  
    },  
    {  
      "Effect": "Allow",  
      "Action": [  
        "s3:PutObject",  
        "s3:GetObject",  
        "s3:DeleteObject"  
      ],  
      "Resource": ["arn:aws:s3:::*"]  
    }  
  ]  
}
```

填入Policy後 Apply

Policy Sandbox

Policy name: [Back](#)

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:*:*:*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:*:*:*"]
    }
  ]
}
```

[Apply](#) [Reset](#)

選擇想要測試的服務

Policy Sandbox

Policy name: Back

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": ["arn:aws:s3:::*"]
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": ["arn:aws:s3:::*"]
    }
  ]
}
```

Apply Reset

Policy Simulator

Select service ▼

Select actions ▼

Select All

Deselect All

Reset Contexts

Clear Results

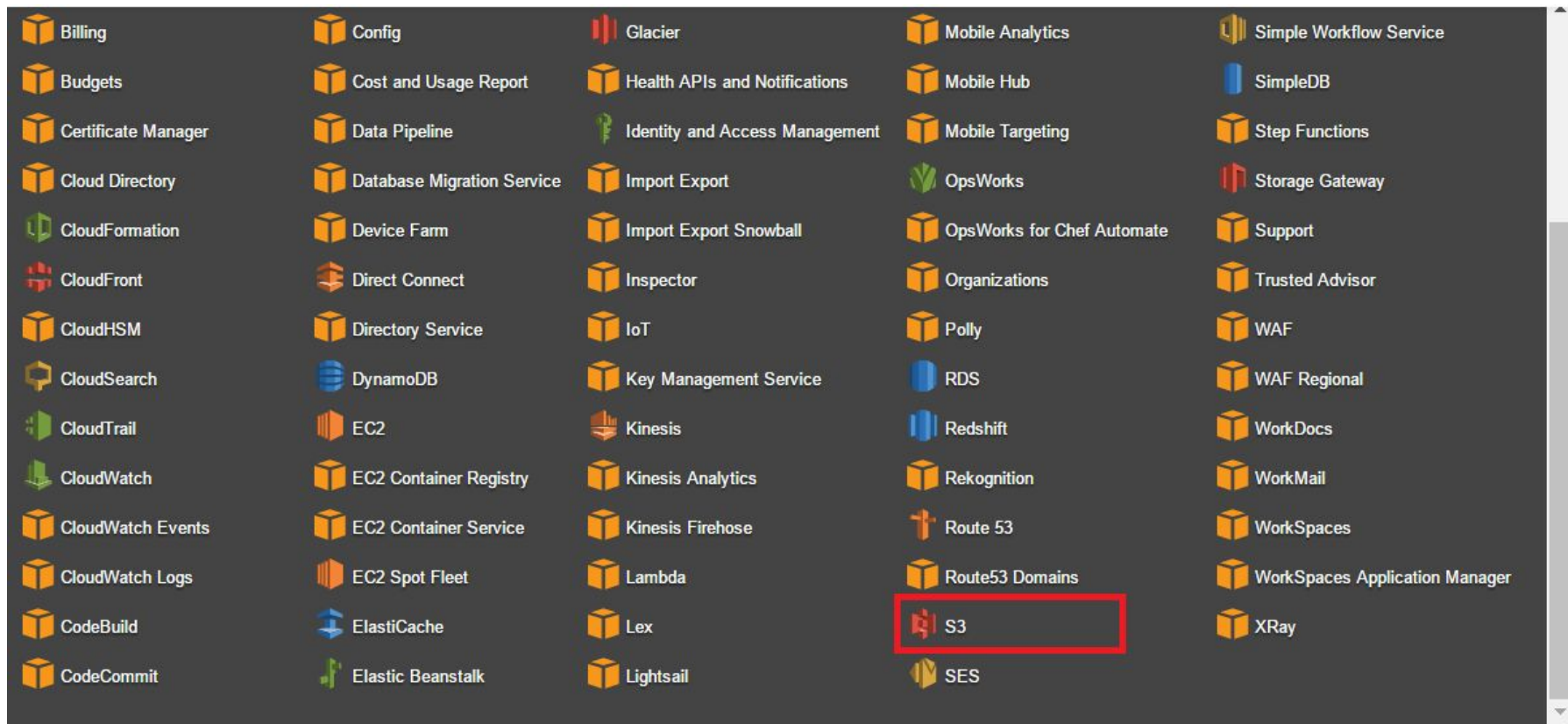
Run Simulation

► Global Settings ⓘ

Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
---------	--------	---------------	---------------------	------------

選擇S3



選擇actions, Demo選擇Select All

Policy Simulator

Amazon S3 ▼ **Select actions** ▼ **Select All** Deselect All Reset Contexts Clear Results **Run Simulation**

Policy Simulator

Amazon S3 ▼ **Select All** Deselect All Reset Contexts Clear Results **Run Simulation**

產生模擬結果

Policy Sandbox

Policy name: tempov27d

Back

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    }
  ]
}
```

Apply

Reset

Policy Simulator

Amazon S3

53 Action(s) sel...

Select All

Deselect All

Reset Contexts

Clear Results

Run Simulation

Global Settings ⓘ

Action Settings and Results [53 actions selected. 0 actions not simulated. 4 actions allowed. 49 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon S3	AbortMultipartUpload	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	CreateBucket	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	DeleteBucket	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	DeleteBucketPolicy	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	DeleteBucketWebsite	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	DeleteObject	not required	*	allowed 1 matching statements.
Amazon S3	DeleteObjectVersion	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetAccelerateConfiguration	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketAcl	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketCORS	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketLocation	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketLogging	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketNotification	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketPolicy	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketRequestPayment	not required	*	denied Implicitly denied (no matching sta...
Amazon S3	GetBucketTagging	not required	*	denied Implicitly denied (no matching sta...

可針對資源的細部狀況進行測試

Policy Sandbox

Policy name:

tempov27d

Back

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": ["s3:ListBucket"],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetObject",
        "s3:DeleteObject"
      ],
      "Resource": "*"
    }
  ]
}
```

Policy Simulator

Amazon S3

53 Action(s) sel...

Select All

Deselect All

Reset Contexts

Clear Results

Run Simulation

Global Settings ⓘ

There are no global AWS condition keys in the selected policies.

Action Settings and Results [53 actions selected. 53 actions not simulated. 0 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon S3	AbortMultipartUpload	not required	*	Not simulated
Resource You can specify the resource and context keys used to simulate this action. By default the simulation resource is "".				
ARN	<input type="text" value="*"/>		<input checked="" type="checkbox"/> Include Resource Policy	
Amazon S3	CreateBucket	not required	*	Not simulated