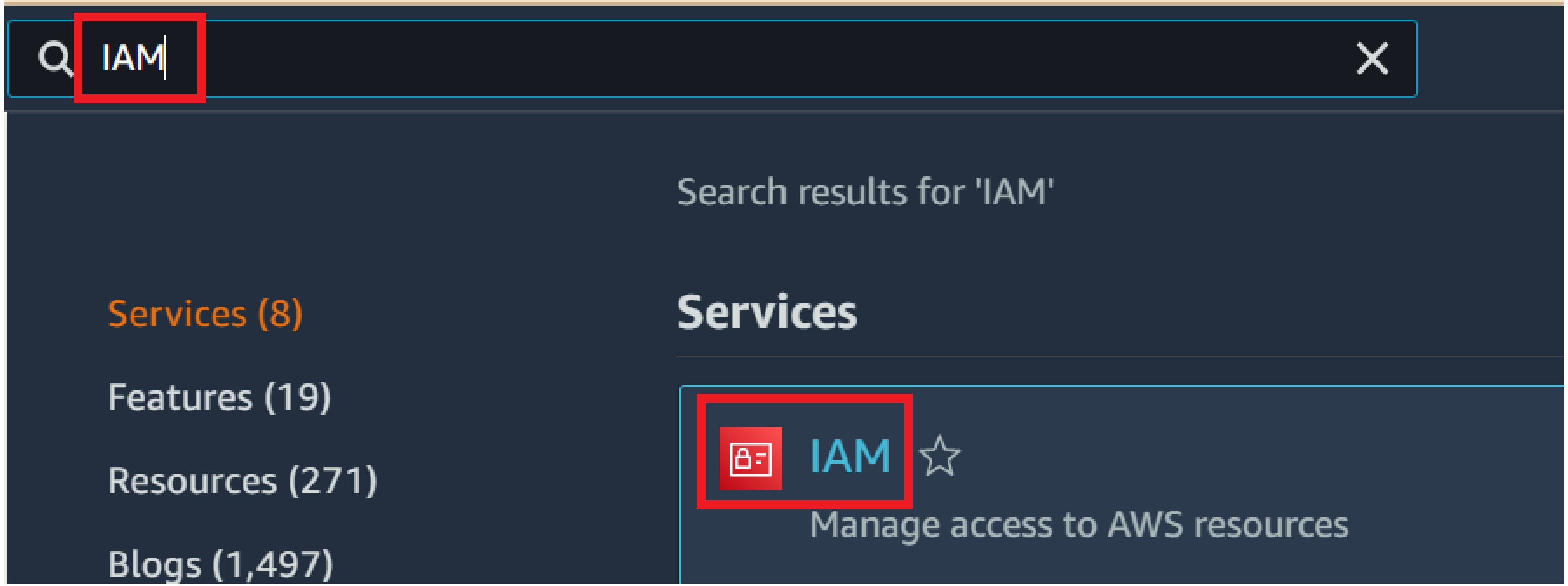
上奇集團

CHASE EXCELLENCE

S3權限設置

IAM

先規劃及設定好S3的Policy，再套用在User上



IAM

Search results for 'IAM'

Services (8)

Features (19)

Resources (271)

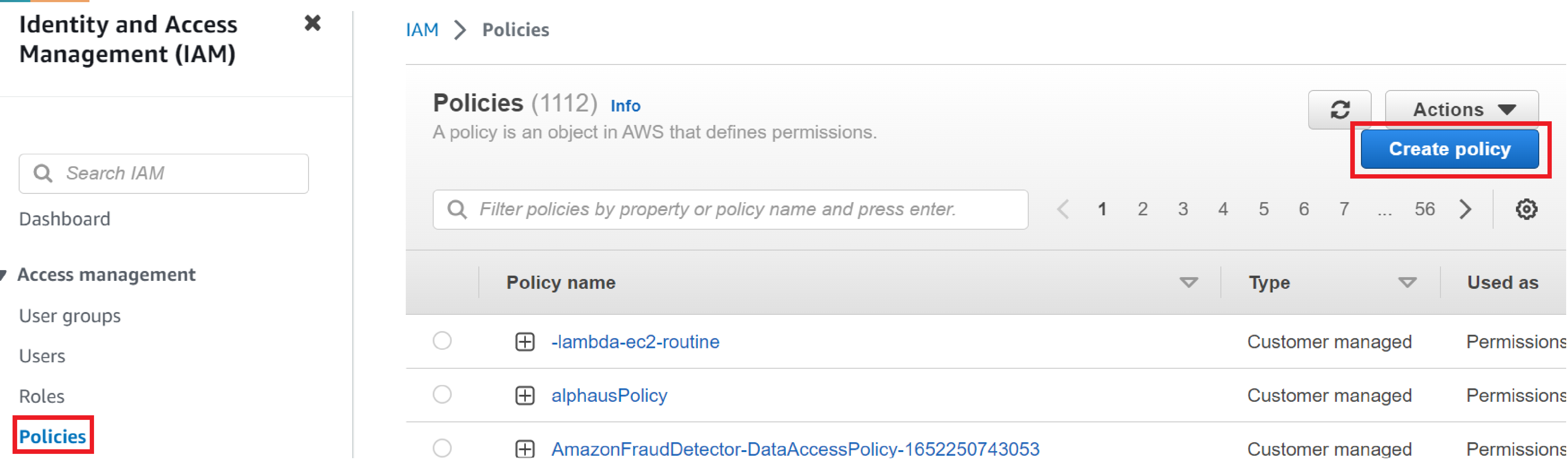
Blogs (1,497)

Services

IAM ☆

Manage access to AWS resources

在 Policies 的地方，點選 Create policy



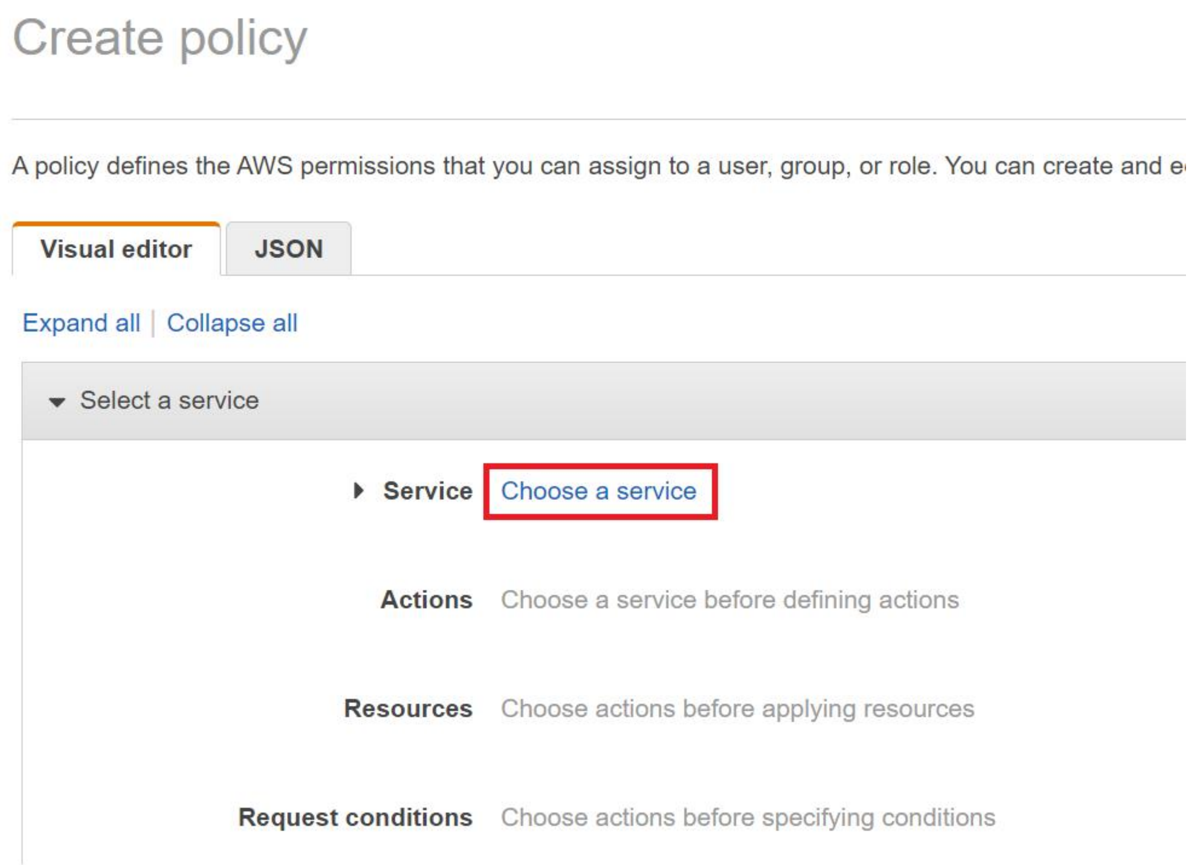
Policies (1112) Info

A policy is an object in AWS that defines permissions.

Filter policies by property or policy name and press enter.

	Policy name	Type	Used as
○	⊞ -lambda-ec2-routine	Customer managed	Permissions
○	⊞ alphausPolicy	Customer managed	Permissions
○	⊞ AmazonFraudDetector-DataAccessPolicy-1652250743053	Customer managed	Permissions

點選 Choose a service，選擇S3服務



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and e

Visual editor | JSON

Expand all | Collapse all

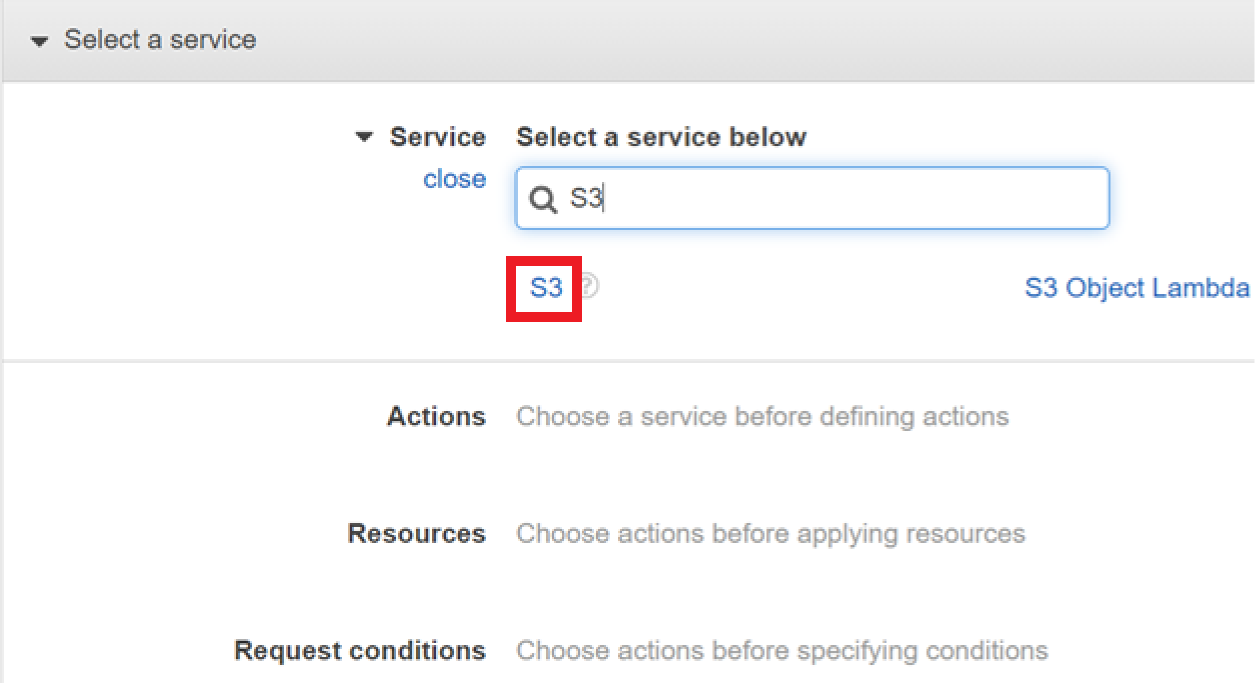
Select a service

Service: Choose a service

Actions: Choose a service before defining actions

Resources: Choose actions before applying resources

Request conditions: Choose actions before specifying conditions



Select a service

Service close: Select a service below

S3

S3 | S3 Object Lambda

Actions: Choose a service before defining actions

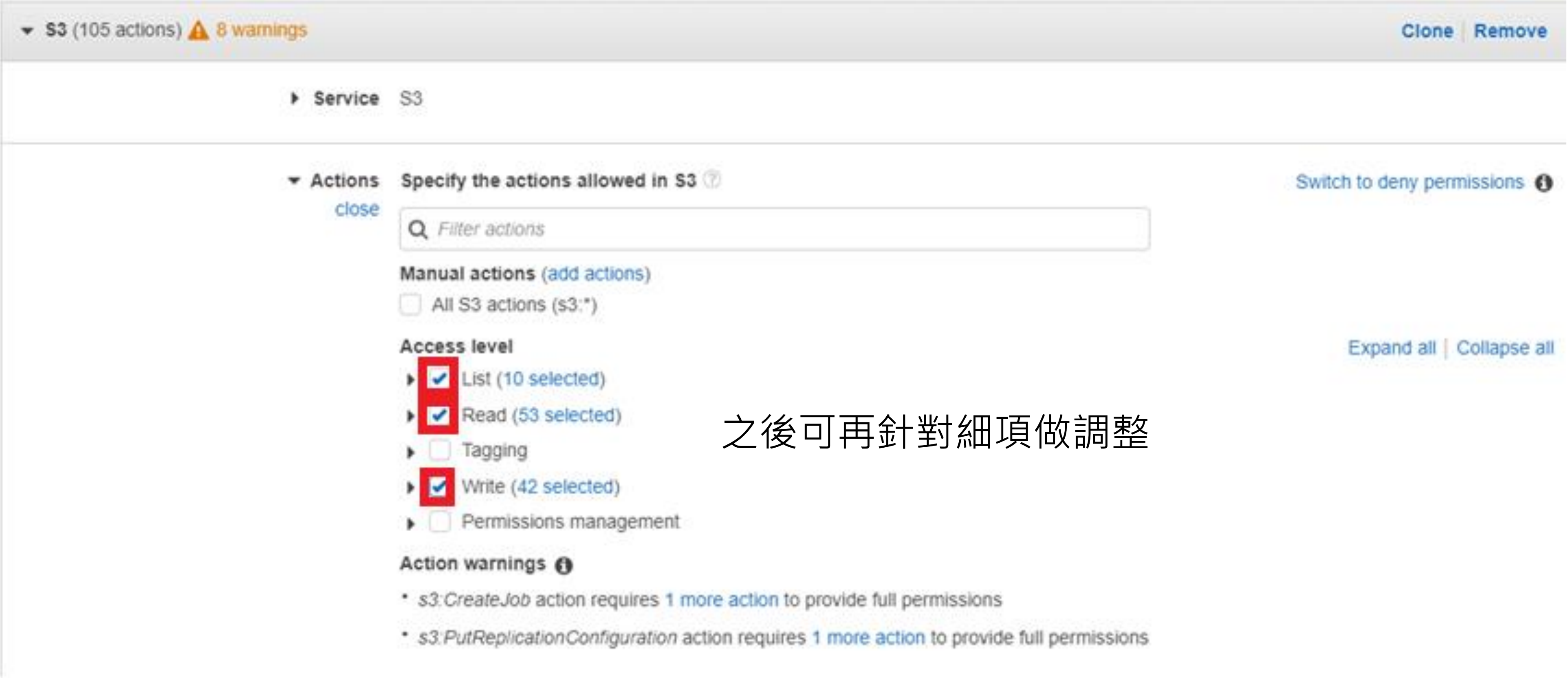
Resources: Choose actions before applying resources

Request conditions: Choose actions before specifying conditions

Full List => 完整開放能夠列出所有檔案跟Buckets功能的權限

Full Read => 完整開放讀的權限

Full Write => 完整開放寫的權限



▾ S3 (105 actions) ⚠ 8 warnings

Clone | Remove

▸ Service S3

▾ Actions Specify the actions allowed in S3

close

Switch to deny permissions

Filter actions

Manual actions (add actions)

□ All S3 actions (s3:*)

Access level

Expand all | Collapse all

▸ ☑ List (10 selected)

▸ ☑ Read (53 selected)

▸ □ Tagging

▸ ☑ Write (42 selected)

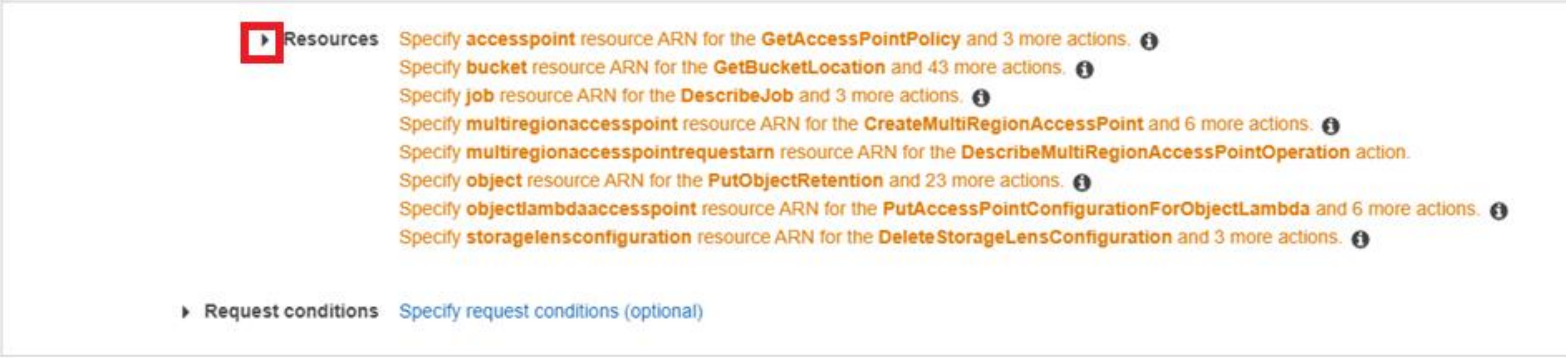
▸ □ Permissions management

Action warnings

- s3:CreateJob action requires 1 more action to provide full permissions
- s3:PutReplicationConfiguration action requires 1 more action to provide full permissions

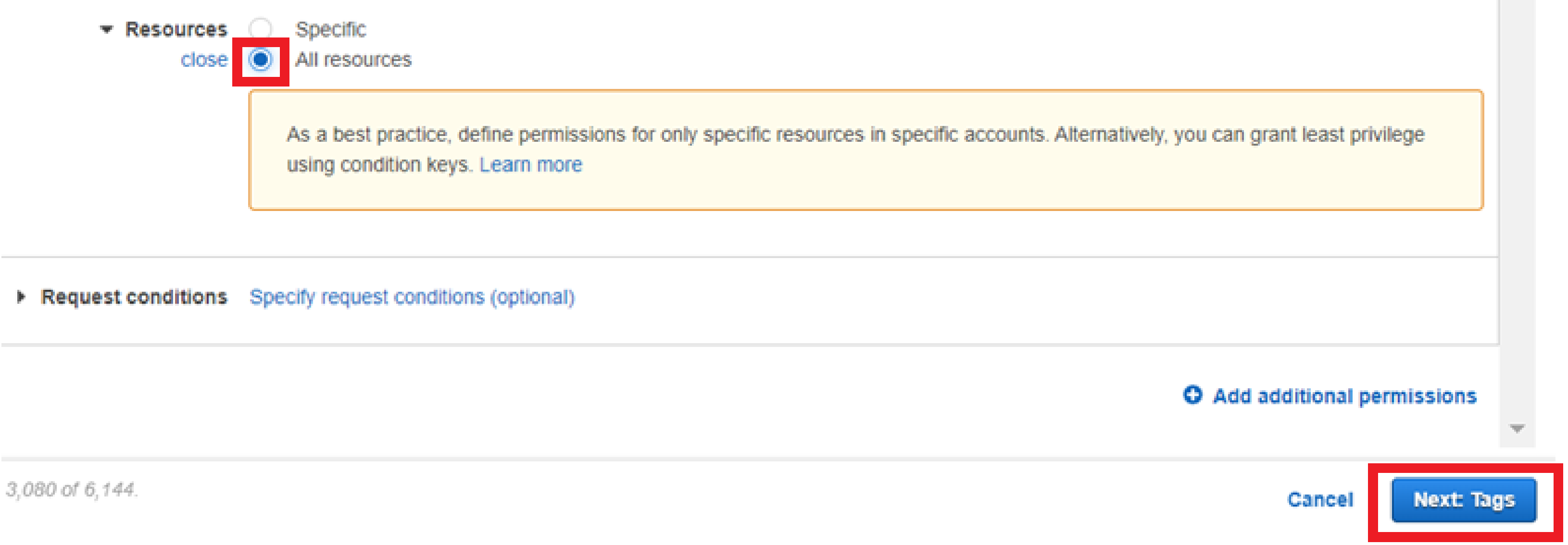
之後可再針對細項做調整

展開 Resources，選擇 All resources (開放對所有資源的權限)



▸ Resources
Specify **accesspoint** resource ARN for the **GetAccessPointPolicy** and 3 more actions. ℹ
Specify **bucket** resource ARN for the **GetBucketLocation** and 43 more actions. ℹ
Specify **job** resource ARN for the **DescribeJob** and 3 more actions. ℹ
Specify **multiregionaccesspoint** resource ARN for the **CreateMultiRegionAccessPoint** and 6 more actions. ℹ
Specify **multiregionaccesspointrequestarn** resource ARN for the **DescribeMultiRegionAccessPointOperation** action.
Specify **object** resource ARN for the **PutObjectRetention** and 23 more actions. ℹ
Specify **objectlambdaaccesspoint** resource ARN for the **PutAccessPointConfigurationForObjectLambda** and 6 more actions. ℹ
Specify **storagelensconfiguration** resource ARN for the **DeleteStorageLensConfiguration** and 3 more actions. ℹ

▸ **Request conditions** Specify request conditions (optional)



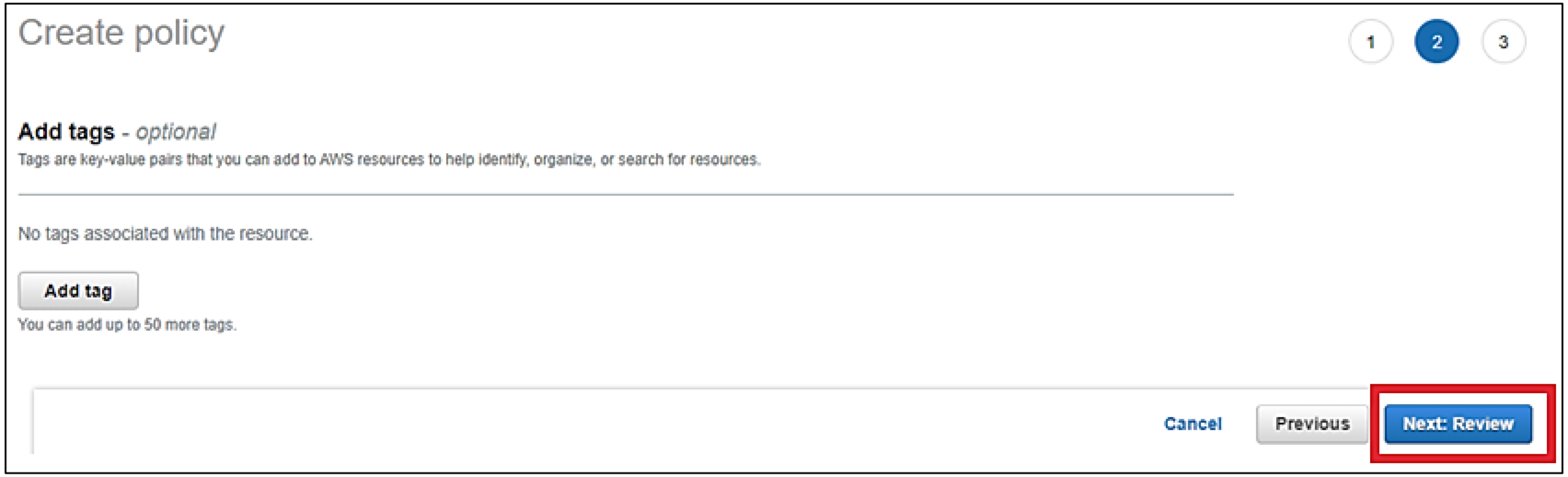
▾ **Resources** ○ Specific
close ● All resources

As a best practice, define permissions for only specific resources in specific accounts. Alternatively, you can grant least privilege using condition keys. Learn more

▸ **Request conditions** Specify request conditions (optional)

設置Tag是方便日後做辨識用

如不需要特別設置，直接點選 Next:Review 即可



Create policy

Add tags - *optional*

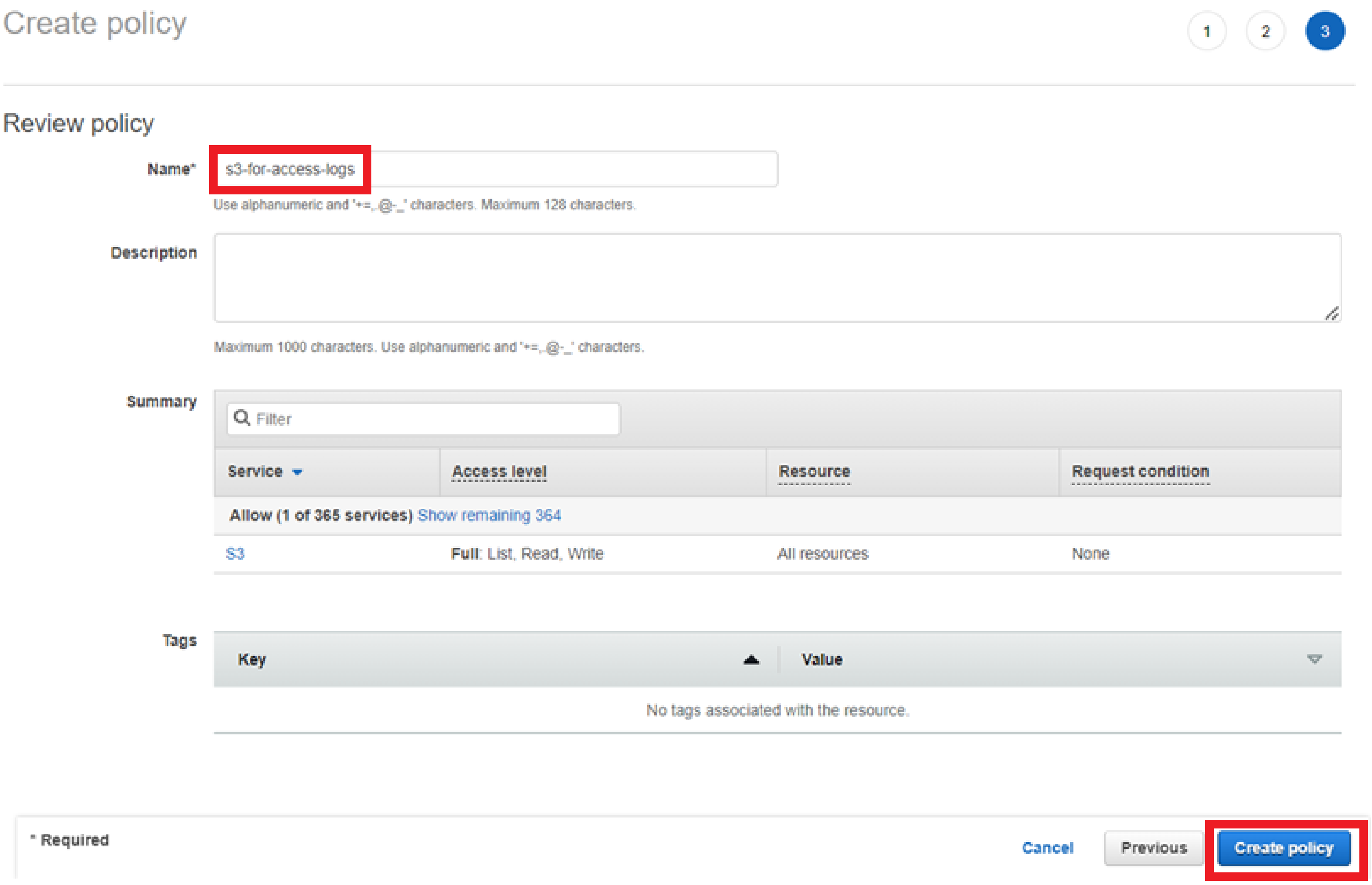
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

You can add up to 50 more tags.

為這個權限取名，通常會取它的用途當名字

可直接點選 Create policy，此Policy就建置完成



Create policy

Review policy

Name* s3-for-access-logs

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

Description

Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Service	Access level	Resource	Request condition
Allow (1 of 365 services) Show remaining 364			
S3	Full: List, Read, Write	All resources	None

Tags

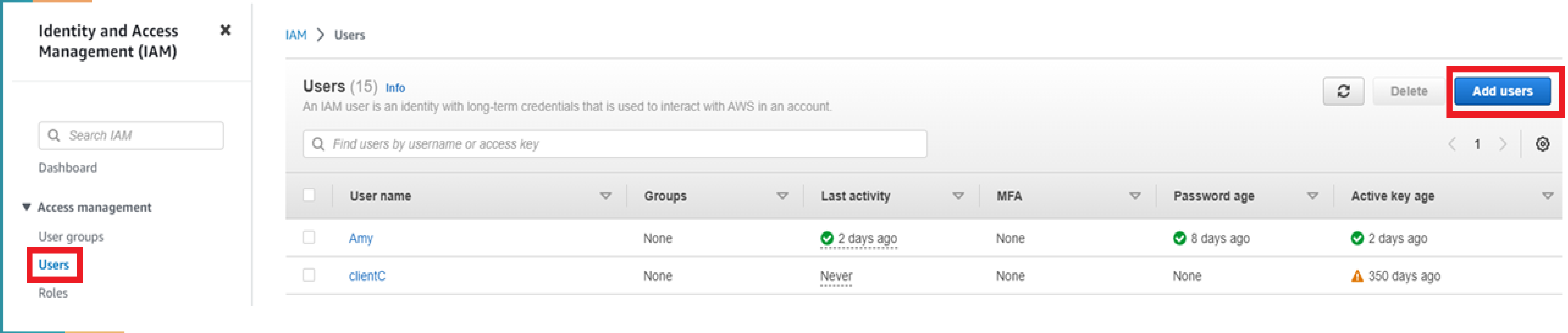
Key	Value
No tags associated with the resource.	

* Required

創建使用者

- 如果還未創建使用者，需先創建後再賦予權限

若還未創建User，需在IAM \ Users的地方，點選 Add users。



Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

User groups

Users

Roles

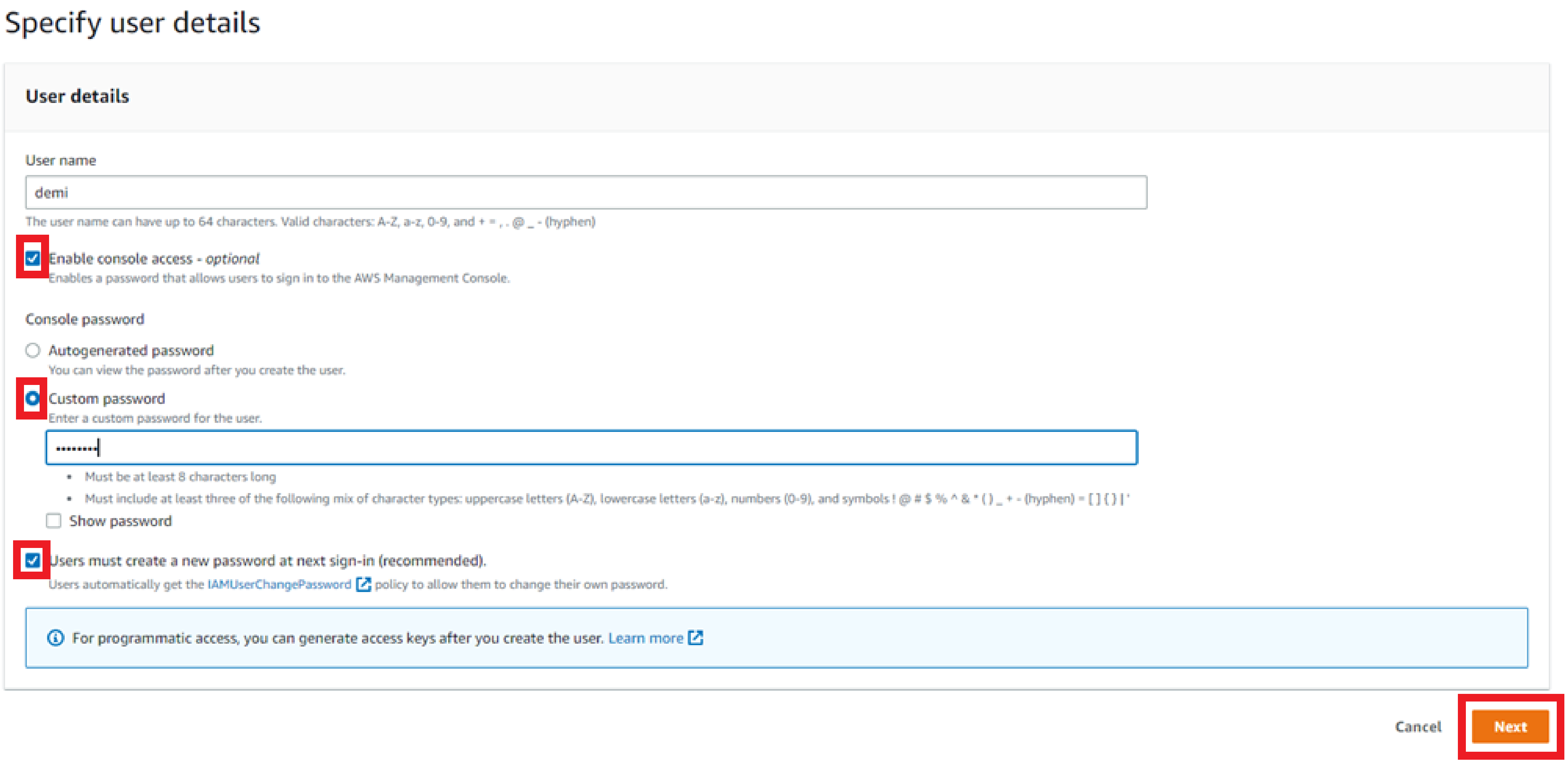
IAM > Users

Users (15) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

□	User name	Groups	Last activity	MFA	Password age	Active key age
□	Amy	None	✓ 2 days ago	None	✓ 8 days ago	✓ 2 days ago
□	clientC	None	Never	None	None	⚠ 350 days ago

為使用者命名，並且希望他在登入後重建密碼



Specify user details

User details

User name

demi

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

☑ Enable console access - *optional*

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

Console password

○ Autogenerated password

You can view the password after you create the user.

● Custom password

Enter a custom password for the user.

••••••••

- 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

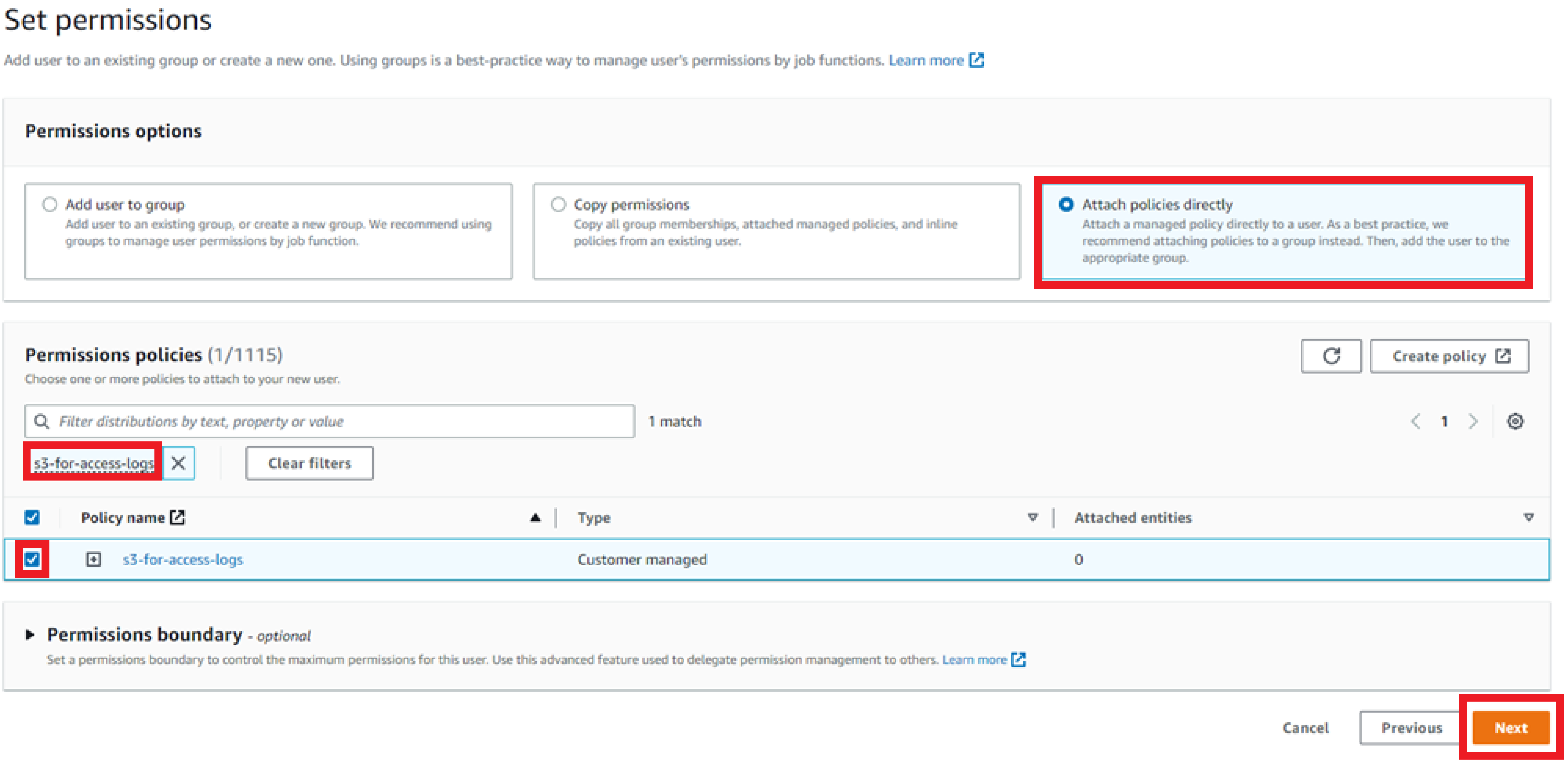
☑ Users must create a new password at next sign-in (recommended).

Users automatically get the IAMUserChangePassword policy to allow them to change their own password.

ⓘ For programmatic access, you can generate access keys after you create the user. Learn more

可以預先附加權限給使用者！

在Permissions policies的欄位，搜尋Policy(如s3-for-access-logs)



Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.

● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1115)
Choose one or more policies to attach to your new user.

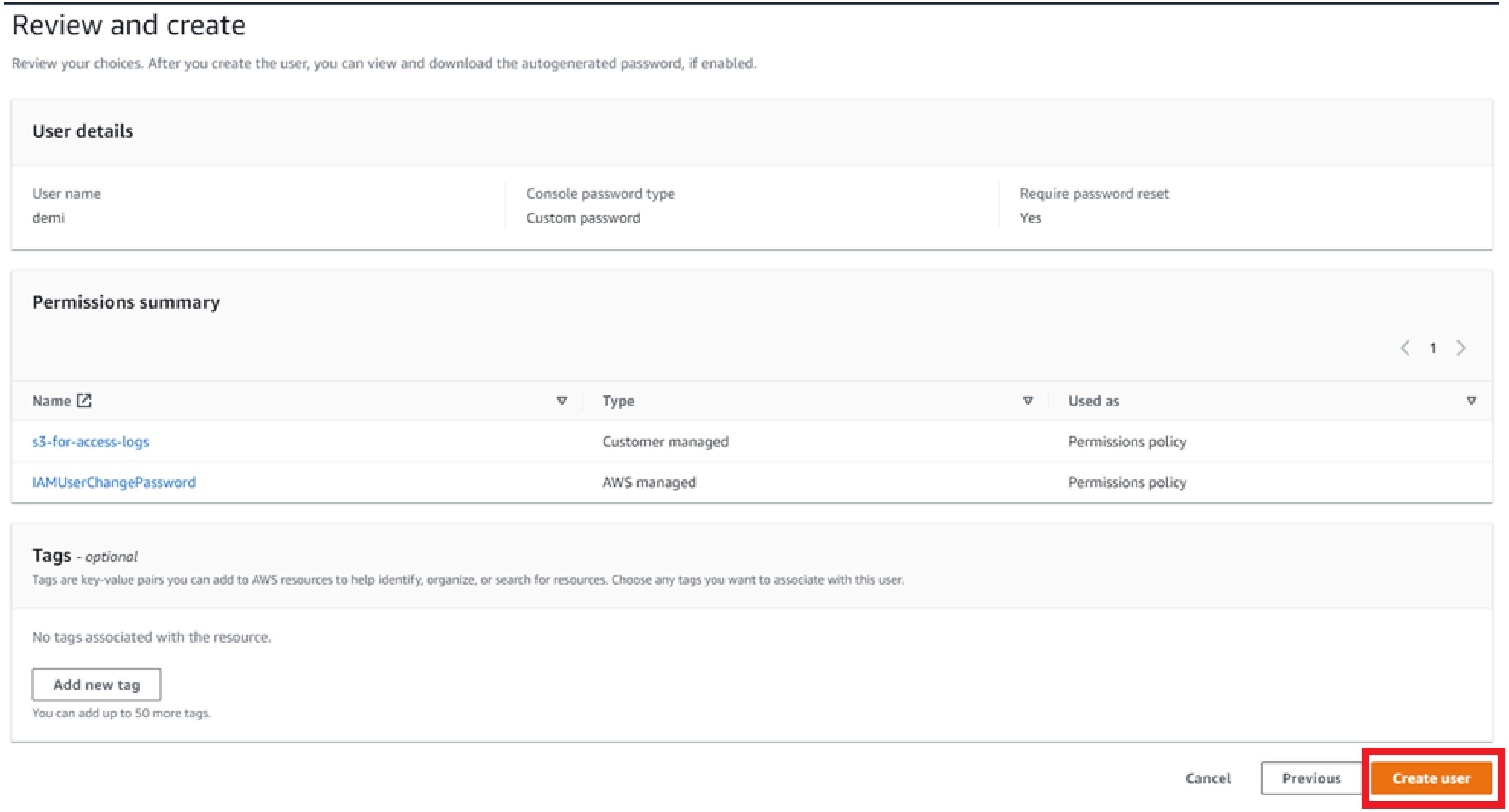
Filter distributions by text, property or value — 1 match

s3-for-access-logs ✕ Clear filters

☑	Policy name	Type	Attached entities
☑	s3-for-access-logs	Customer managed	0

▸ **Permissions boundary** - *optional*
Set a permissions boundary to control the maximum permissions for this user. Use this advanced feature used to delegate permission management to others. Learn more

點選 Create user



Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details

User name	Console password type	Require password reset
demi	Custom password	Yes

Permissions summary

< 1 >

Name	Type	Used as
s3-for-access-logs	Customer managed	Permissions policy
IAMUserChangePassword	AWS managed	Permissions policy

Tags - *optional*

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

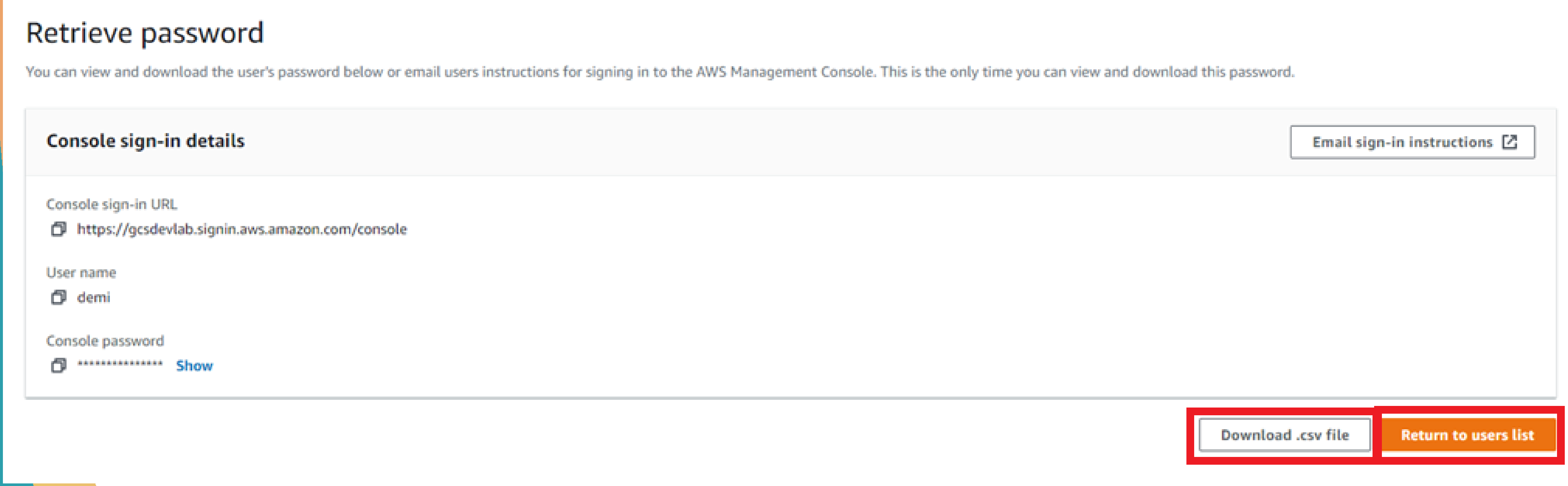
Add new tag

You can add up to 50 more tags.

vices

務必先點選 Download .csv file，將登入資訊的CSV檔下載下來。並妥善保管

再按 Return to users list 回到User清單。



Retrieve password

You can view and download the user's password below or email users instructions for signing in to the AWS Management Console. This is the only time you can view and download this password.

Console sign-in details

Console sign-in URL

https://gcsdevlab.signin.aws.amazon.com/console

User name

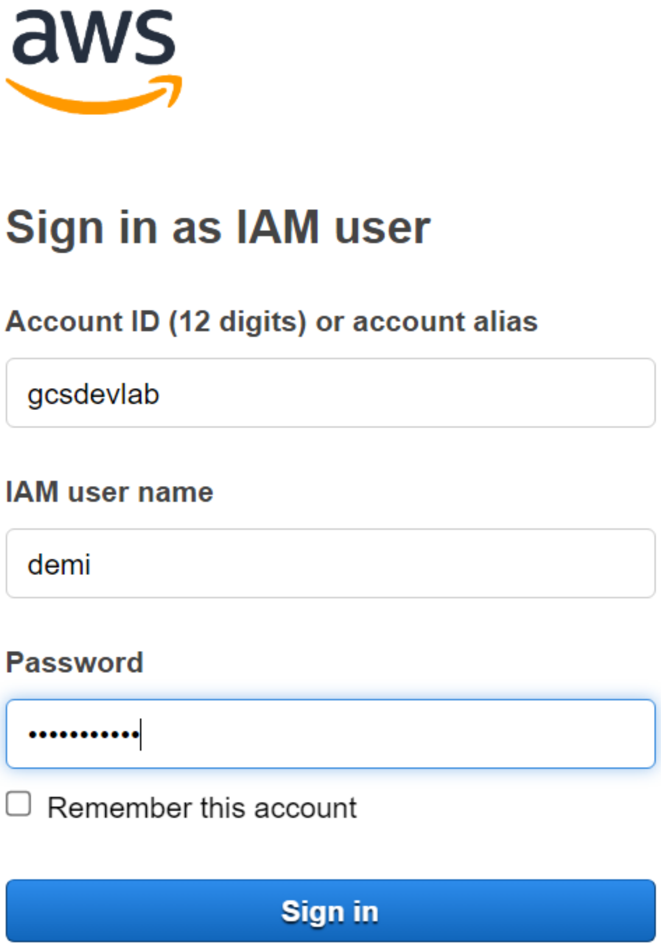
demi

Console password

**************** Show

使用Console Sign-in URL進行登入，並請管理者更新密碼

請務必使用複雜性的高強度密碼



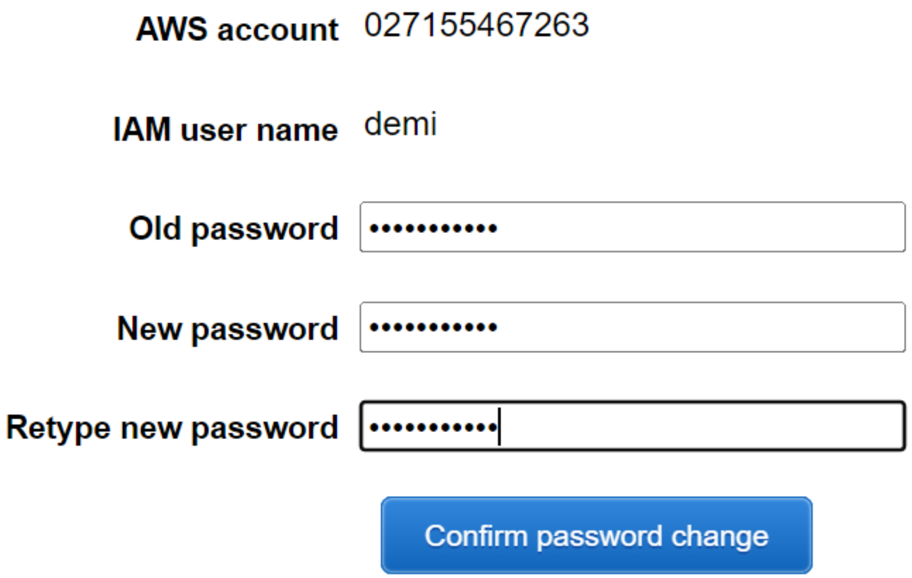
Sign in as IAM user

Account ID (12 digits) or account alias: gcsdevlab

IAM user name: demi

Password: •••••••••••

☐ Remember this account



AWS account 027155467263

IAM user name demi

Old password •••••••••••

New password •••••••••••

Retype new password •••••••••••

設置使用者權限

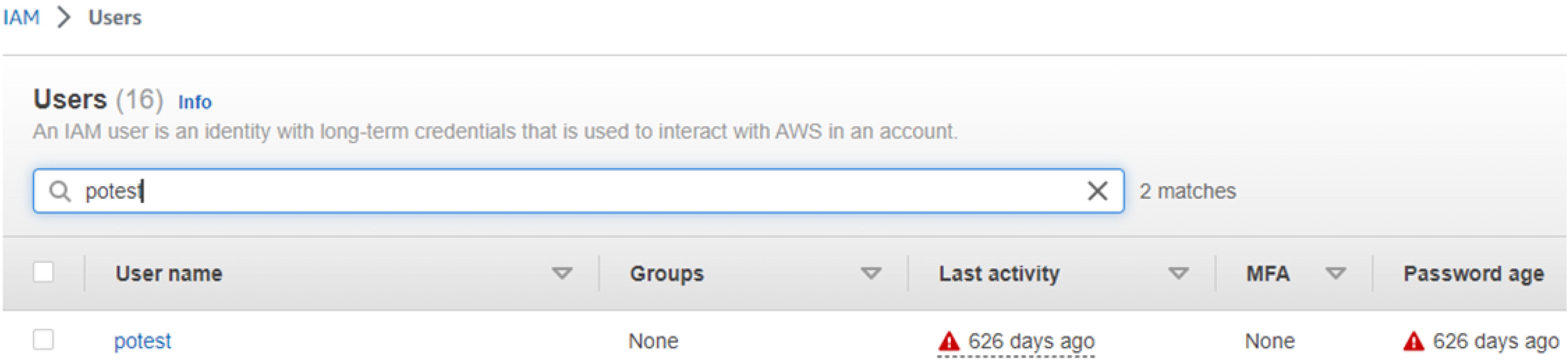
- 創建好權限和使用者後，可以賦予權限
- 如果在創建使用者時尚未指定權限

GrandTechCloudServices

將此Policy套用在User上。

若User已創建好，可跳過Add Users的步驟，直接選擇你要新增policy的user

若在創建User的時候已指定權限，可以直接跳去測試階段



IAM > Users

Users (16) Info

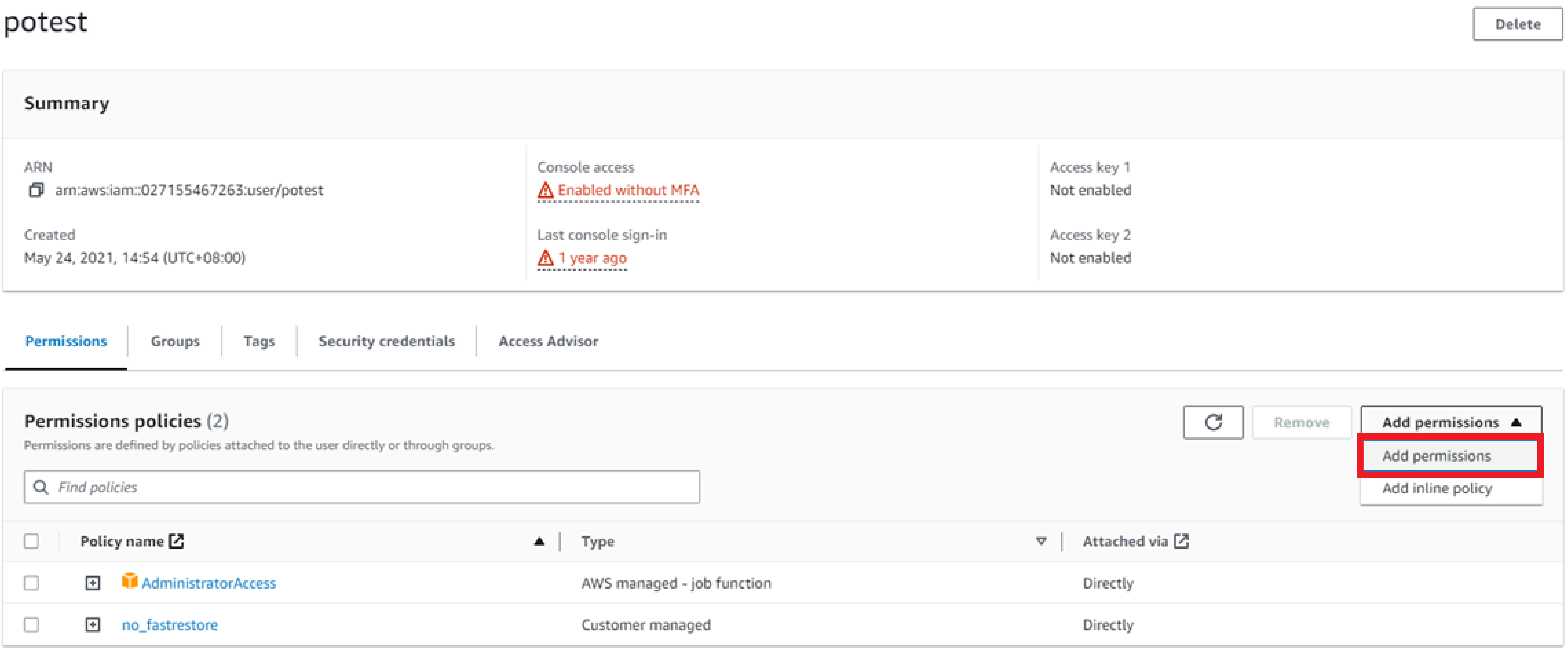
An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

potest

2 matches

□	User name	Groups	Last activity	MFA	Password age
□	potest	None	▲ 626 days ago	None	▲ 626 days ago

點選 Add permissions



potest

Delete

Summary

ARN
arn:aws:iam::027155467263:user/potest

Created
May 24, 2021, 14:54 (UTC+08:00)

Console access
⚠ Enabled without MFA

Last console sign-in
⚠ 1 year ago

Access key 1
Not enabled

Access key 2
Not enabled

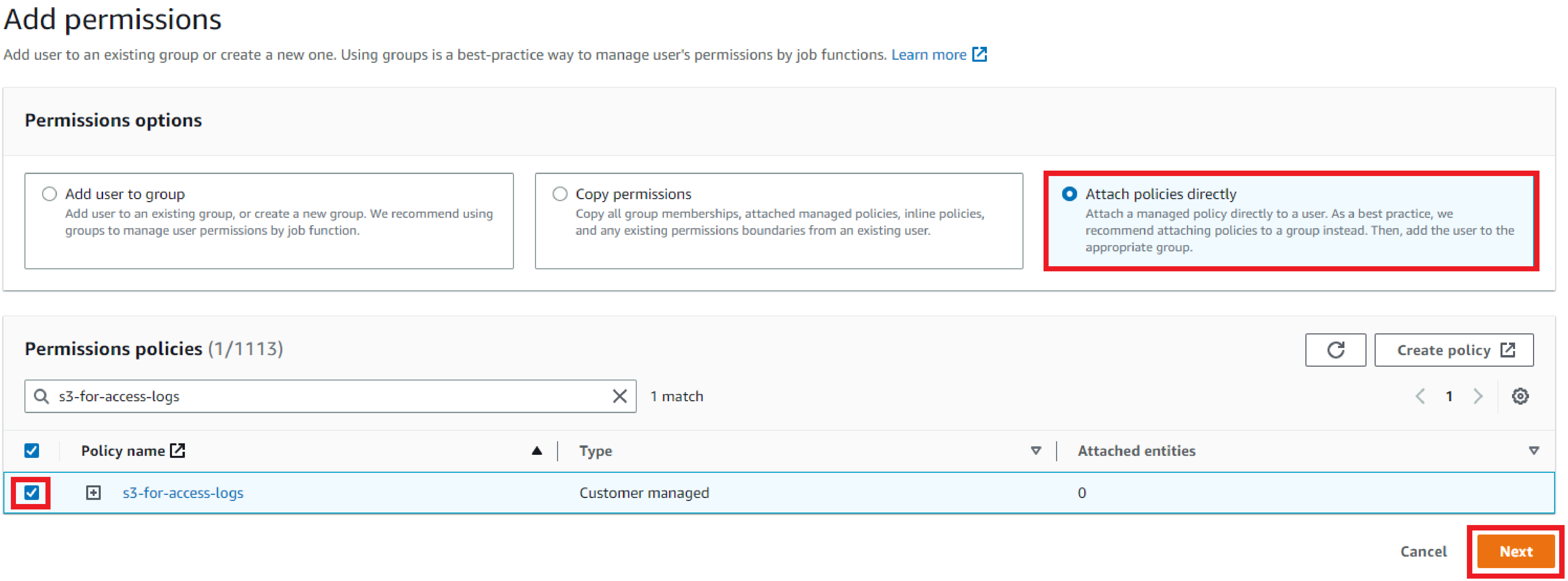
Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

□	Policy name ▲	Type	Attached via
□	AdministratorAccess	AWS managed - job function	Directly
□	no_fastrestore	Customer managed	Directly

附加權限給使用者

在Permissions policies 的欄位，搜尋Policy (如s3-for-access-logs)



Add permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more

Permissions options

○ Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.

○ Copy permissions
Copy all group memberships, attached managed policies, inline policies, and any existing permissions boundaries from an existing user.

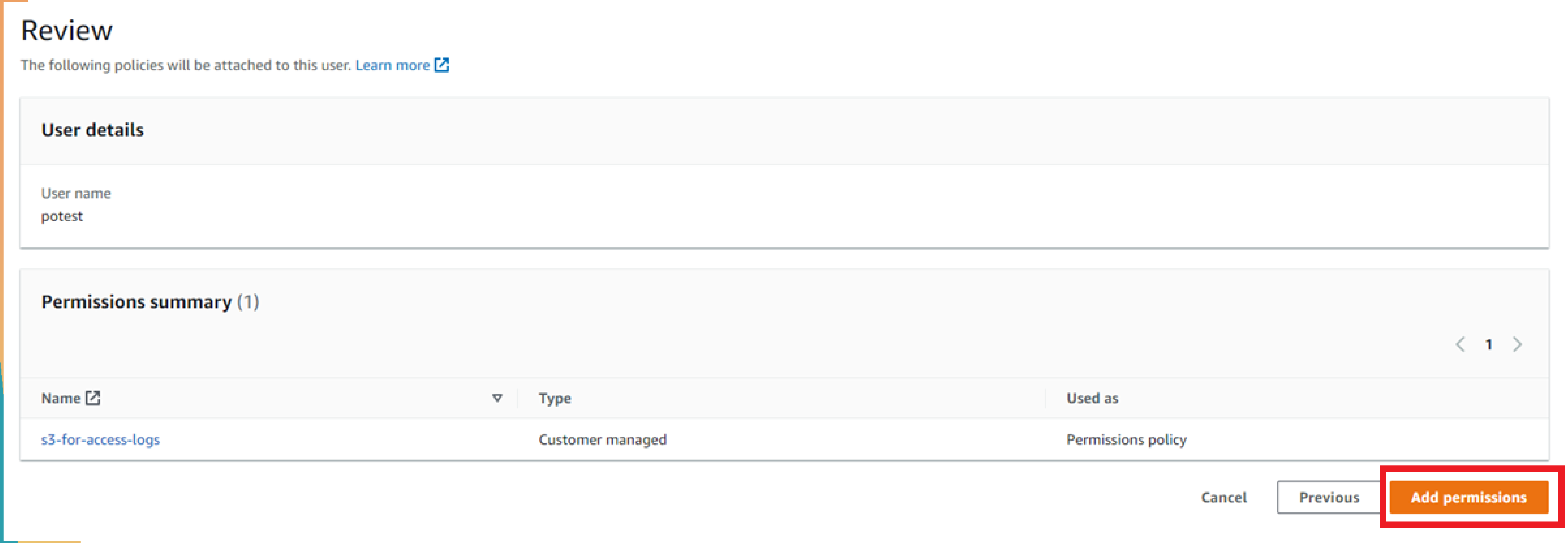
● Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1113)

s3-for-access-logs — 1 match

☑	Policy name	Type	Attached entities
☑	s3-for-access-logs	Customer managed	0

確認完畢，點選 Add permissions，將權限套用在User上



Review

The following policies will be attached to this user. Learn more

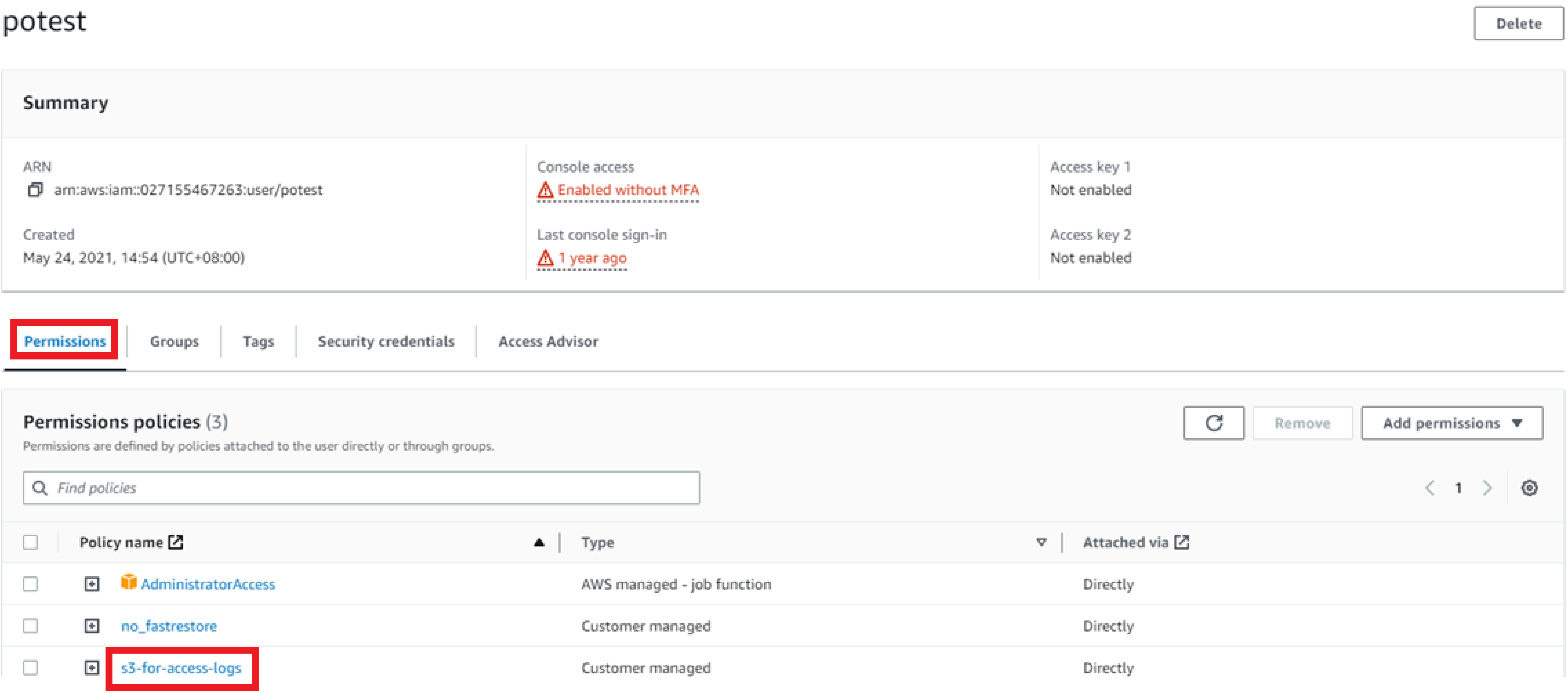
User details

User name
potest

Permissions summary (1)

Name	Type	Used as
s3-for-access-logs	Customer managed	Permissions policy

確認此 Policy (S3-for-access-logs)成功套用在User上



potest

Delete

Summary

ARN
arn:aws:iam::027155467263:user/potest

Created
May 24, 2021, 14:54 (UTC+08:00)

Console access
⚠ Enabled without MFA

Last console sign-in
⚠ 1 year ago

Access key 1
Not enabled

Access key 2
Not enabled

Permissions | Groups | Tags | Security credentials | Access Advisor

Permissions policies (3)

Permissions are defined by policies attached to the user directly or through groups.

Remove | Add permissions ▼

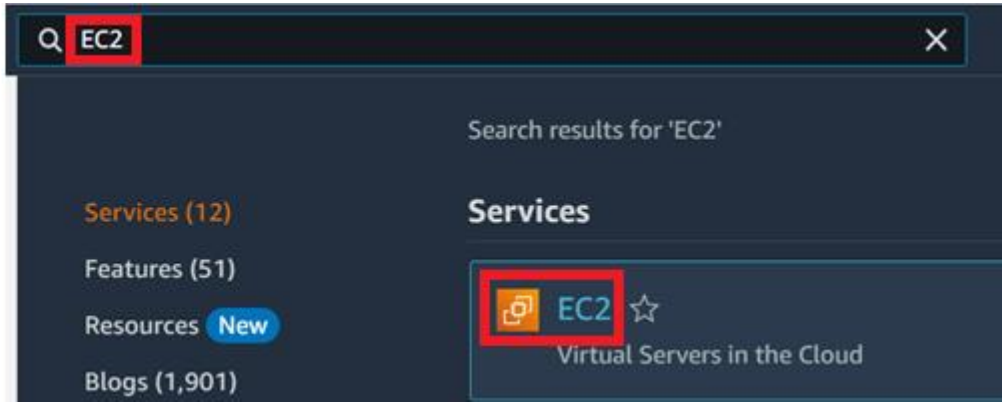
Find policies

□	Policy name	Type	Attached via
□	AdministratorAccess	AWS managed - job function	Directly
□	no_fastrestore	Customer managed	Directly
□	s3-for-access-logs	Customer managed	Directly

測試

因為沒有權限，不能看到s3以外的服務

(可點進EC2試試看)



EC2

Search results for 'EC2'

Services (12)

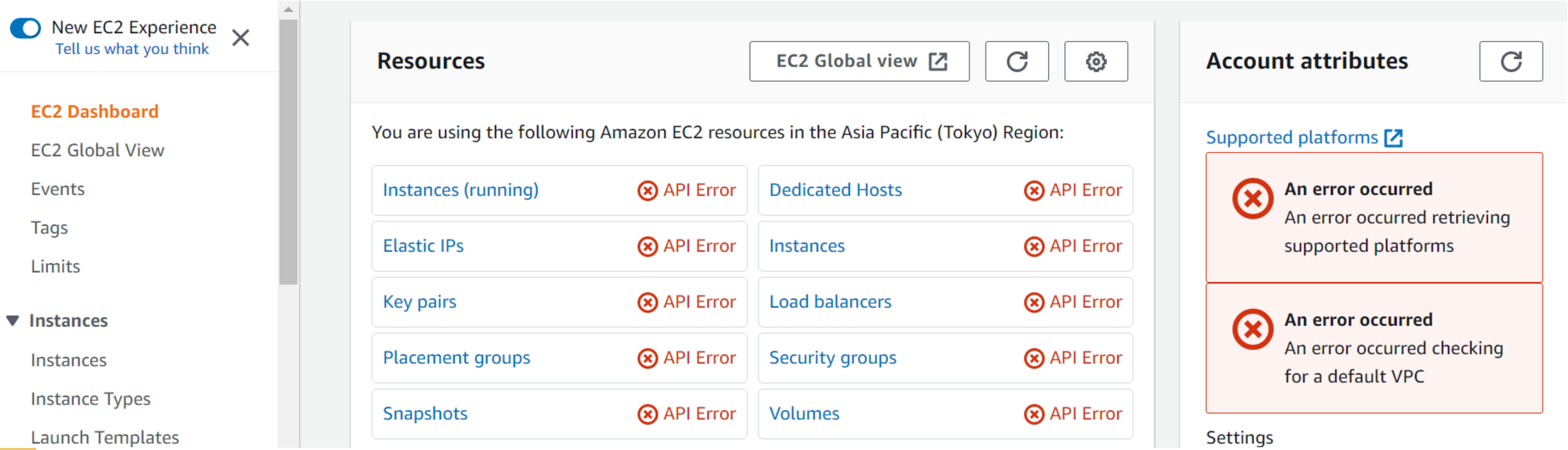
Features (51)

Resources New

Blogs (1,901)

Services

EC2 ☆
Virtual Servers in the Cloud



New EC2 Experience
Tell us what you think

EC2 Dashboard

EC2 Global View

Events

Tags

Limits

▼ Instances

Instances

Instance Types

Launch Templates

Resources

EC2 Global view

You are using the following Amazon EC2 resources in the Asia Pacific (Tokyo) Region:

Instances (running)	⊗ API Error	Dedicated Hosts	⊗ API Error
Elastic IPs	⊗ API Error	Instances	⊗ API Error
Key pairs	⊗ API Error	Load balancers	⊗ API Error
Placement groups	⊗ API Error	Security groups	⊗ API Error
Snapshots	⊗ API Error	Volumes	⊗ API Error

Account attributes

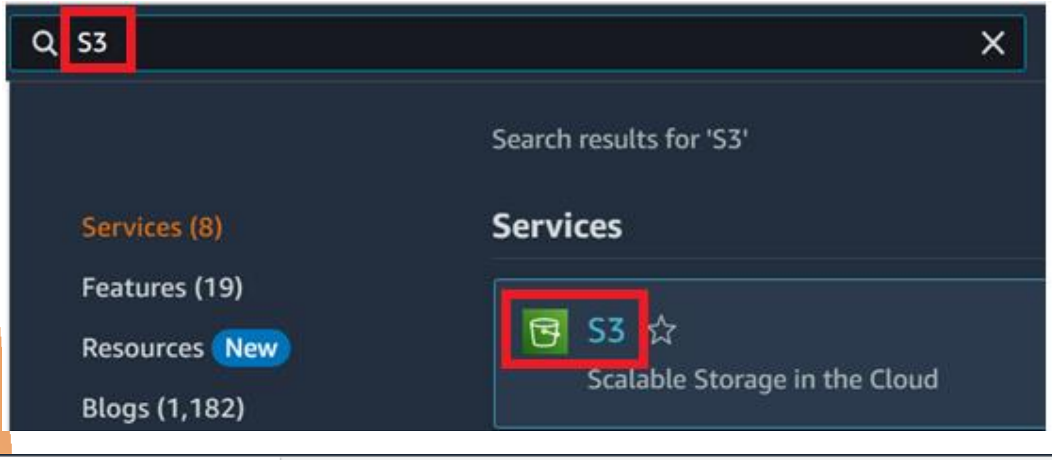
Supported platforms

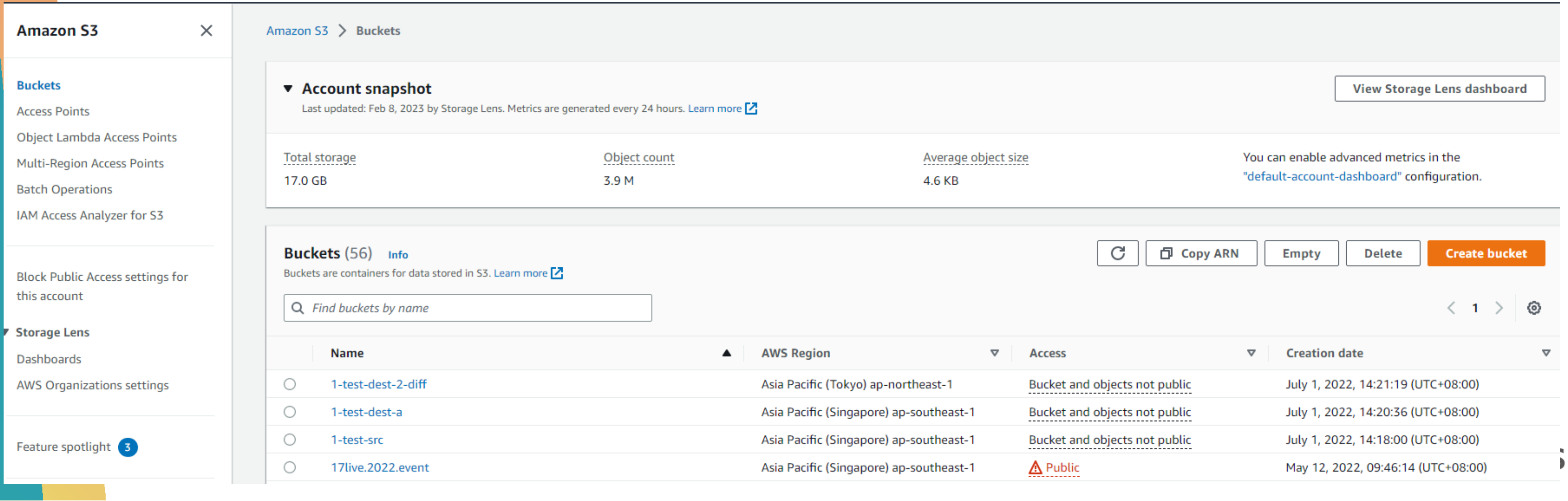
An error occurred
An error occurred retrieving supported platforms

An error occurred
An error occurred checking for a default VPC

Settings

進到s3驗證，如果可以看到bucket，就是有List的權限





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 3
Amazon S3 > Buckets
View Storage Lens dashboard
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1

▼ Account snapshot

Last updated: Feb 8, 2023 by Storage Lens. Metrics are generated every 24 hours. Learn more

Total storage: 17.0 GB

Object count: 3.9 M

Average object size: 4.6 KB

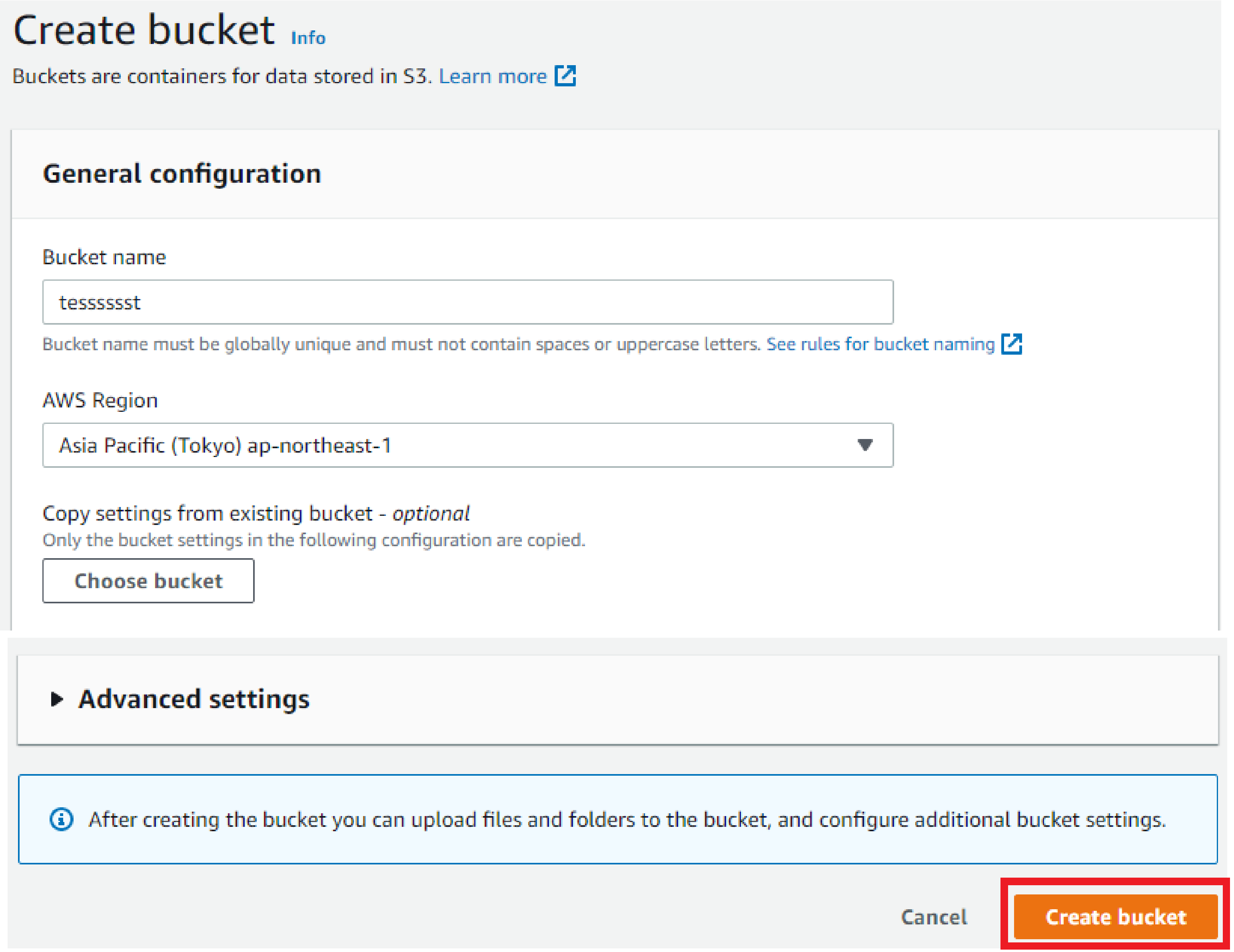
You can enable advanced metrics in the "default-account-dashboard" configuration.

Buckets (56) Info

Buckets are containers for data stored in S3. Learn more

	Name	AWS Region	Access	Creation date
○	1-test-dest-2-diff	Asia Pacific (Tokyo) ap-northeast-1	Bucket and objects not public	July 1, 2022, 14:21:19 (UTC+08:00)
○	1-test-dest-a	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	July 1, 2022, 14:20:36 (UTC+08:00)
○	1-test-src	Asia Pacific (Singapore) ap-southeast-1	Bucket and objects not public	July 1, 2022, 14:18:00 (UTC+08:00)
○	17live.2022.event	Asia Pacific (Singapore) ap-southeast-1	⚠ Public	May 12, 2022, 09:46:14 (UTC+08:00)

如果可以創建Bucket，就是有Write的權限



Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name

tesssssst

Bucket name must be globally unique and must not contain spaces or uppercase letters. See rules for bucket naming

AWS Region

Asia Pacific (Tokyo) ap-northeast-1

Copy settings from existing bucket - *optional*

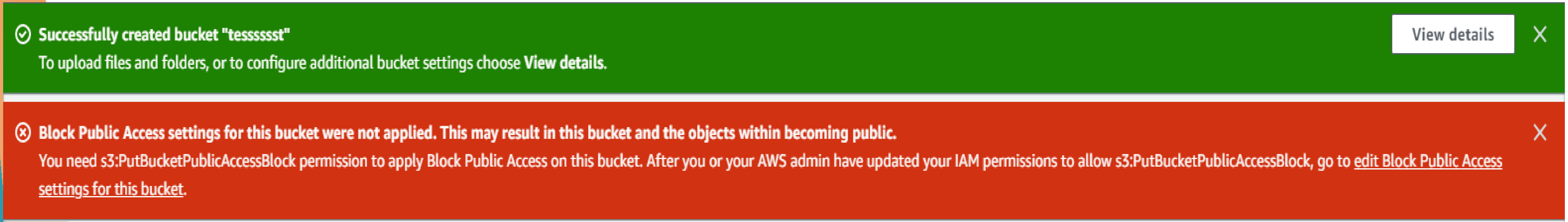
Only the bucket settings in the following configuration are copied.

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

上奇集團 CHASE EXCELLENCE

TechCloudServices

有其他錯誤是另外兩大項權限沒開啟的部分，不用擔心
以下圖為例已有寫入、讀取和列表的權限

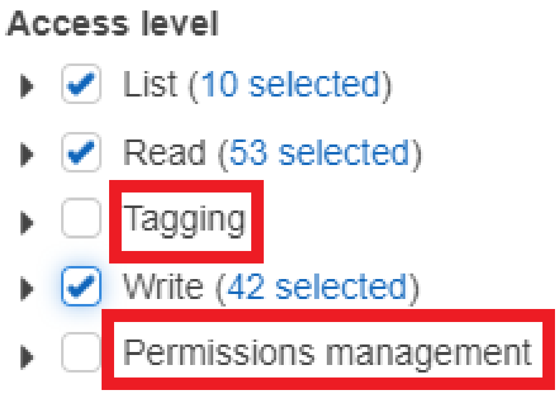


Successfully created bucket "tesssssst"

To upload files and folders, or to configure additional bucket settings choose **View details**.

Block Public Access settings for this bucket were not applied. This may result in this bucket and the objects within becoming public.

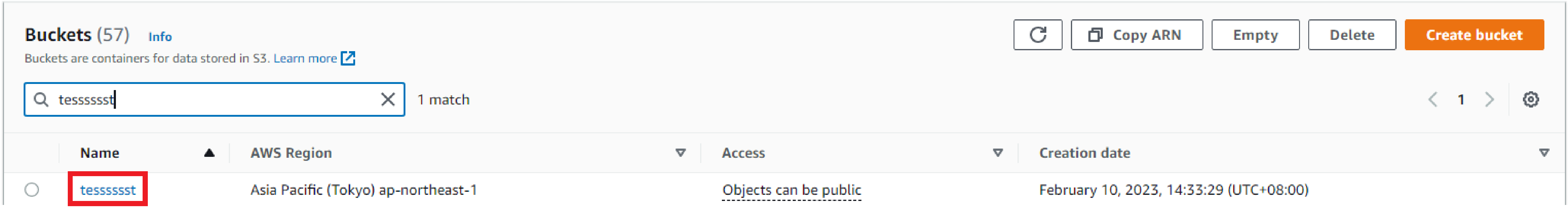
You need s3:PutBucketPublicAccessBlock permission to apply Block Public Access on this bucket. After you or your AWS admin have updated your IAM permissions to allow s3:PutBucketPublicAccessBlock, go to edit Block Public Access settings for this bucket.



Access level

- ☑ List (10 selected)
- ☑ Read (53 selected)
- □ Tagging
- ☑ Write (42 selected)
- □ Permissions management

進到Bucket驗證，上傳的檔案可以下載，就是有Read的權限



Buckets (57) Info

Buckets are containers for data stored in S3. Learn more

tesssssst

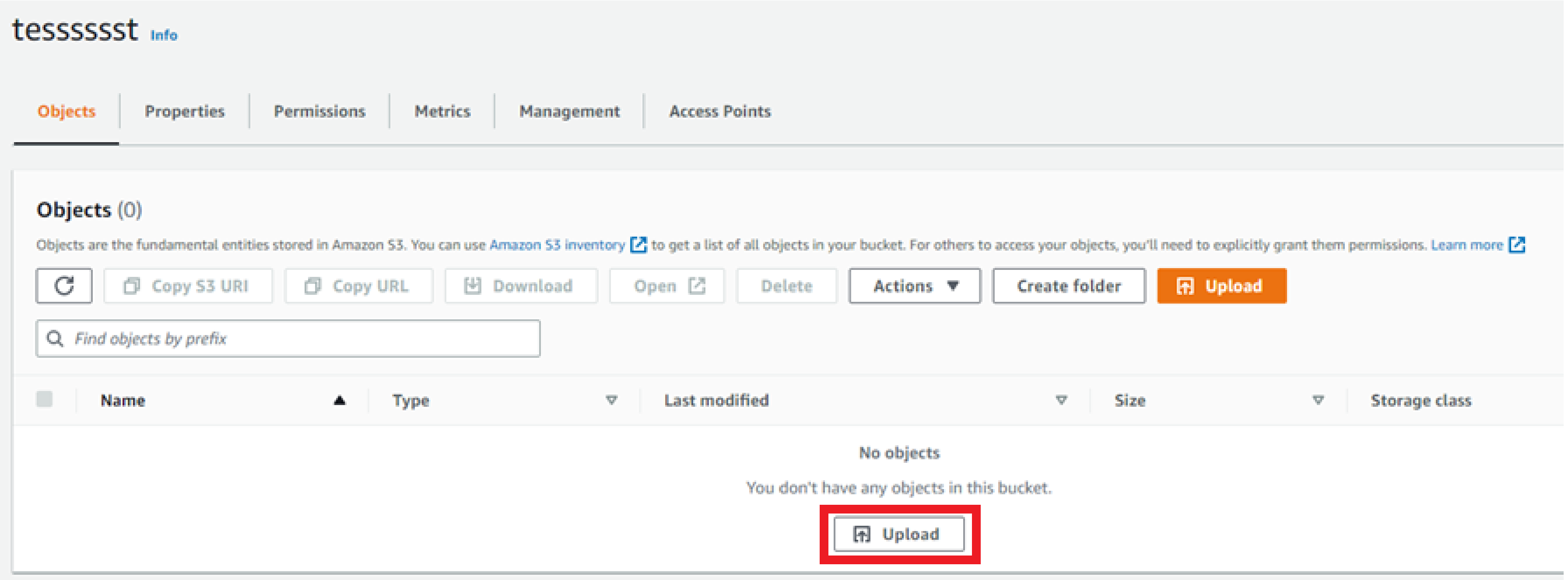
1 match

Name	AWS Region	Access	Creation date
○ tesssssst	Asia Pacific (Tokyo) ap-northeast-1	Objects can be public	February 10, 2023, 14:33:29 (UTC+08:00)

點選 tesssssst，

進入Bucket上傳

Object



tesssssst Info

Objects (0)

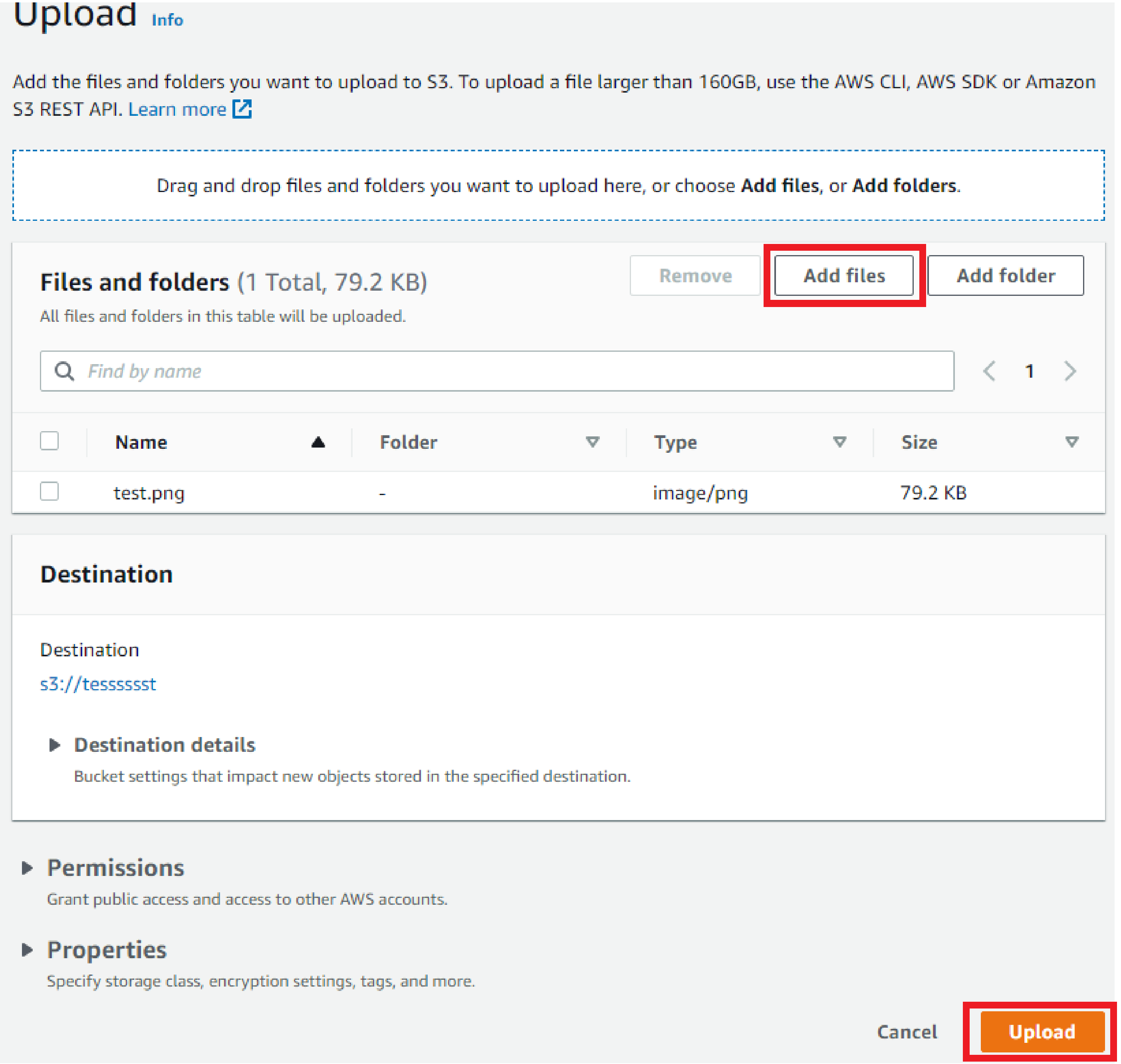
Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. Learn more

No objects

You don't have any objects in this bucket.

點選 Add files，

上傳檔案



Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDK or Amazon S3 REST API. Learn more

Drag and drop files and folders you want to upload here, or choose **Add files**, or **Add folders**.

Files and folders (1 Total, 79.2 KB)

All files and folders in this table will be uploaded.

	Name	Folder	Type	Size
□	test.png	-	image/png	79.2 KB

Destination

Destination

s3://tesssssst

▶ **Destination details**

Bucket settings that impact new objects stored in the specified destination.

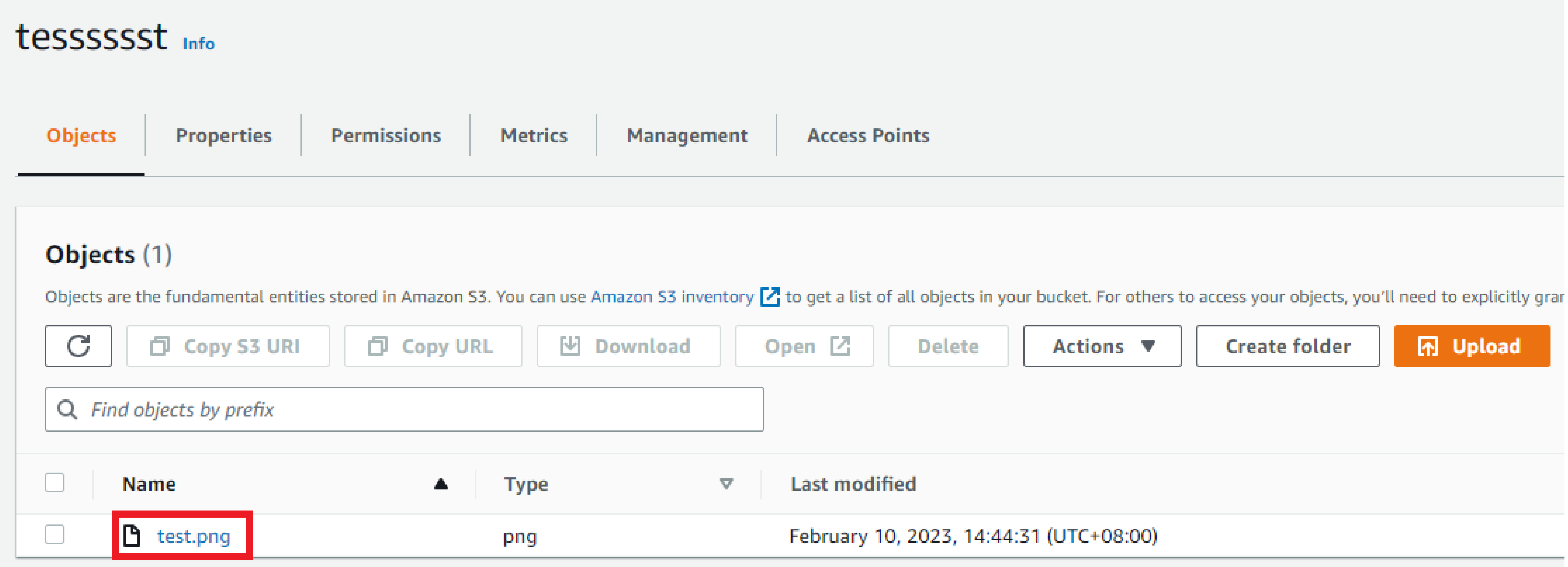
▶ **Permissions**

Grant public access and access to other AWS accounts.

▶ **Properties**

Specify storage class, encryption settings, tags, and more.

點選test.png檔案，嘗試下載



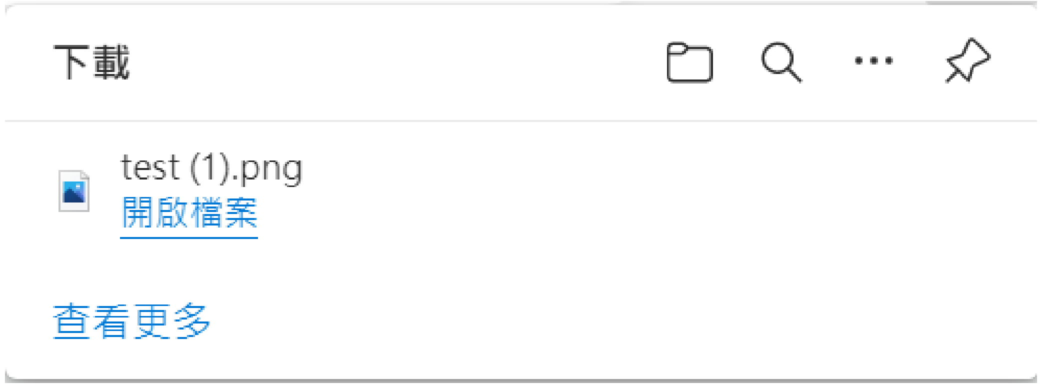
tesssssst Info

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grar

□	Name ▲	Type ▽	Last modified
□	test.png	png	February 10, 2023, 14:44:31 (UTC+08:00)

成功下載，表示有讀的權限

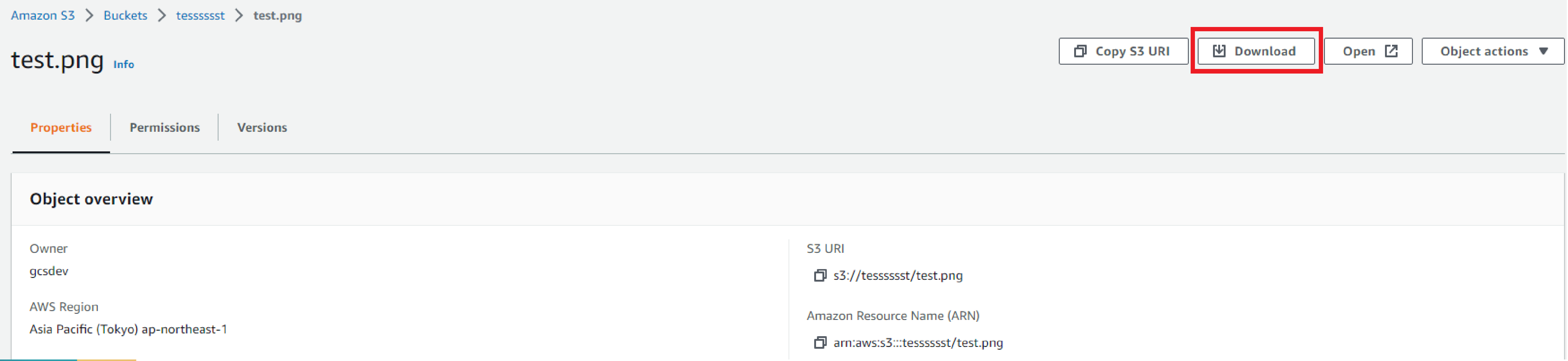


下載

test (1).png

開啟檔案

查看更多



test.png Info

Object overview

Owner
gcsdev

AWS Region
Asia Pacific (Tokyo) ap-northeast-1

S3 URI
s3://tessssst/test.png

Amazon Resource Name (ARN)
arn:aws:s3:::tessssst/test.png

上奇集團 CHASE EXCELLENCE

Thank you