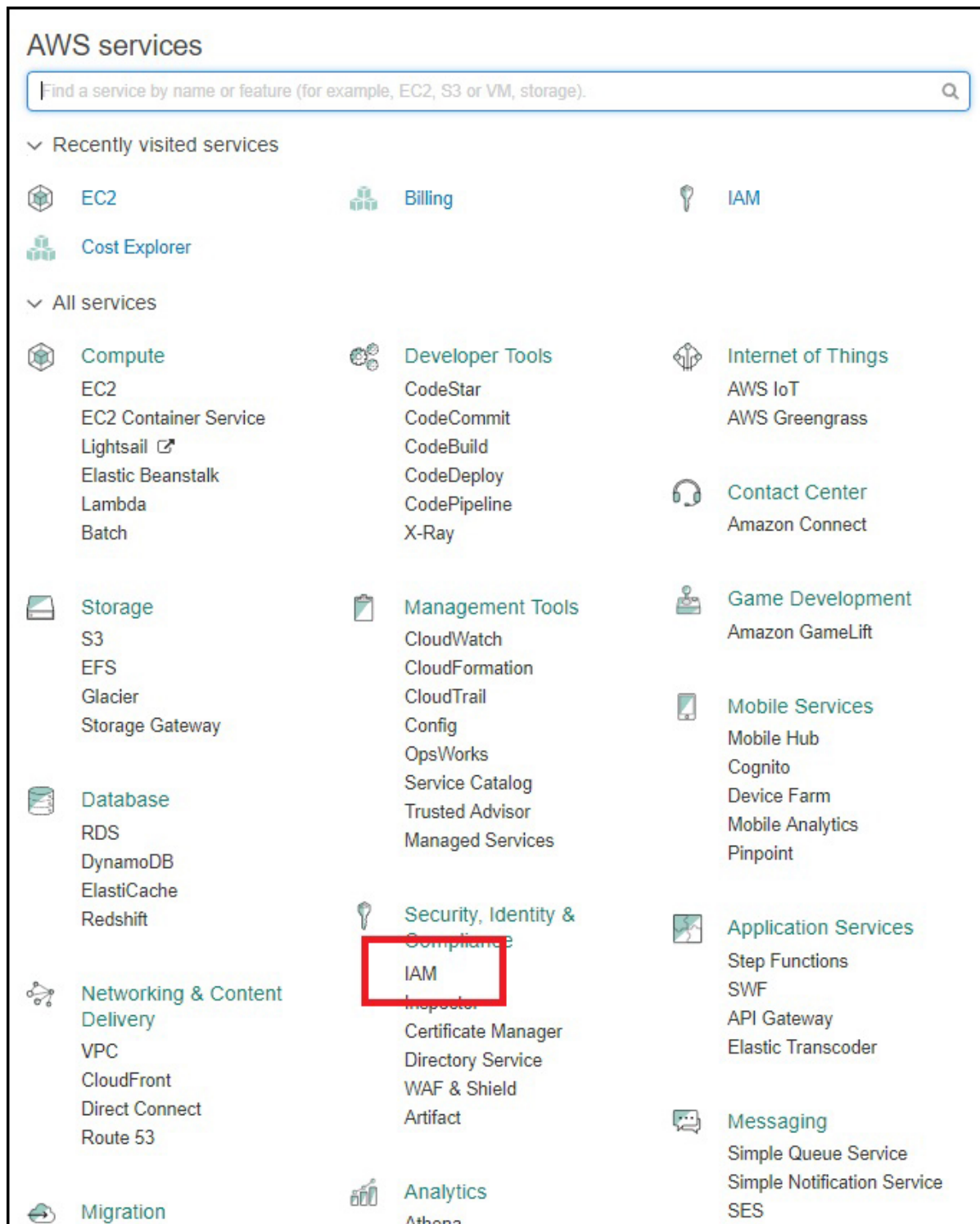


Create the Access Key

Aug 2017

Before we can start our own Terraform Script, we need to create an access key in AWS. This key is used by Terraform to create the EC2 Instance on your own account, otherwise you would need to put login details in to each script, which is a really bad idea from a security perspective.

Login to your AWS Console.



Select the option IAM.

Services

Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:
https://303216744559.signin.aws.amazon.com/console

IAM Resources

Users: 0

Groups: 0

Customer Managed Policies: 0

Roles: 0

Identity Providers: 0

Security Status

1 out of 5 complete.

✓

Delete your root access keys

▼

⚠

Activate MFA on your root account

▼

⚠

Create individual IAM users

▼

⚠

Use groups to assign permissions

▼

⚠

Apply an IAM password policy

▼

Services

Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Welcome to Identity and Access Management

IAM users sign-in link:
https://303216744559.signin.aws.amazon.com/console

IAM Resources

Users: 0

Groups: 0

Customer Managed Policies: 0

Roles: 0

Identity Providers: 0

Security Status

1 out of 5 complete.

✓

Delete your root access keys

▲

▼

Delete your AWS root account access keys, because they provide unrestricted access to your AWS resources. Instead, use IAM user access keys or temporary security credentials. [Learn More](#)

Manage Security Credentials

⚠

Activate MFA on your root account

▼

⚠

Create individual IAM users

▼

⚠

Use groups to assign permissions

▼

⚠

Apply an IAM password policy

▼

You are accessing the security credentials page for your AWS account. The account credentials provide unlimited access to your AWS resources.

To help secure your account, follow an [AWS best practice](#) by creating and using AWS Identity and Access Management (IAM) users with limited permissions.

Continue to Security Credentials

Get Started with IAM Users

☐ Don't show me this message again

Services

Resource Groups

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the [IAM Console](#). To learn more about the types of AWS credentials and how they're used, see [AWS Security Credentials](#) in AWS General Reference.

+

Password

+

Multi-Factor Authentication (MFA)

+

Access Keys (Access Key ID and Secret Access Key)

+

CloudFront Key Pairs

+

X.509 Certificates

+

Account Identifiers

Services

Resource Groups

MR AL WALKER

Global

Support

Search IAM

Dashboard

Groups

Users

Roles

Policies

Identity providers

Account settings

Credential report

Encryption keys

Your Security Credentials

Use this page to manage the credentials for your AWS account. To manage credentials for AWS Identity and Access Management (IAM) users, use the IAM Console. To learn more about the types of AWS credentials and how they're used, see AWS Security Credentials in AWS General Reference.

+

 Password

+

 Multi-Factor Authentication (MFA)

-

 Access Keys (Access Key ID and Secret Access Key)

You use access keys to sign programmatic requests to AWS services. To learn how to sign requests using your access keys, see the signing documentation. For your protection, store your access keys securely and do not share them. In addition, AWS recommends that you rotate your access keys every 90 days.
Note: You can have a maximum of two access keys (active or inactive) at a time.

Created	Deleted	Access Key ID	Last Used	Last Used Region	Last Used Service	Status	Actions
<div>Create New Access Key</div>							

Important Change - Managing Your AWS Secret Access Keys

As described in a previous announcement, you cannot retrieve the existing secret access keys for your AWS root account, though you can still create a new root access key at any time. As a best practice, we recommend creating an IAM user that has access keys rather than relying on root access keys.

+

 CloudFront Key Pairs

+

 X.509 Certificates

+

 Account Identifiers

Create Access Key

✓ Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

Show Access Key

Download Key File

Close

Create Access Key

✓ Your access key (access key ID and secret access key) has been created successfully.

Download your key file now, which contains your new access key ID and secret access key. If you do not download the key file now, you will not be able to retrieve your secret access key again.

To help protect your security, store your secret access key securely and do not share it.

Hide Access Key

Access Key ID:

Secret Access Key:

Download Key File

Close