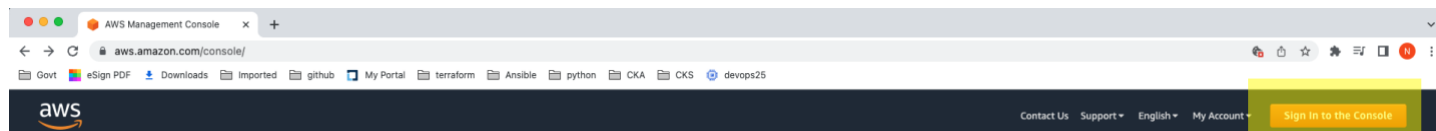


How to Login to AWS EC2

Using **AWS SSM** (Session Manager) **OR** Using the **Connect** Option on **AWS Console**

Login to AWS Account

<https://aws.amazon.com/console/>



Sign in

☒ Root user

Account owner that performs tasks requiring unrestricted access. [Learn more](#)

☐ IAM user

User within an account that performs daily tasks. [Learn more](#)

Root user email address

Next

By continuing, you agree to the [AWS Customer Agreement](#) or other agreement for AWS services, and the [Privacy Notice](#). This site uses essential cookies. See our [Cookie Notice](#) for more information.

— New to AWS? —

Create a new AWS account



Root user sign in ⓘ

Email:

Password

[Forgot password?](#)

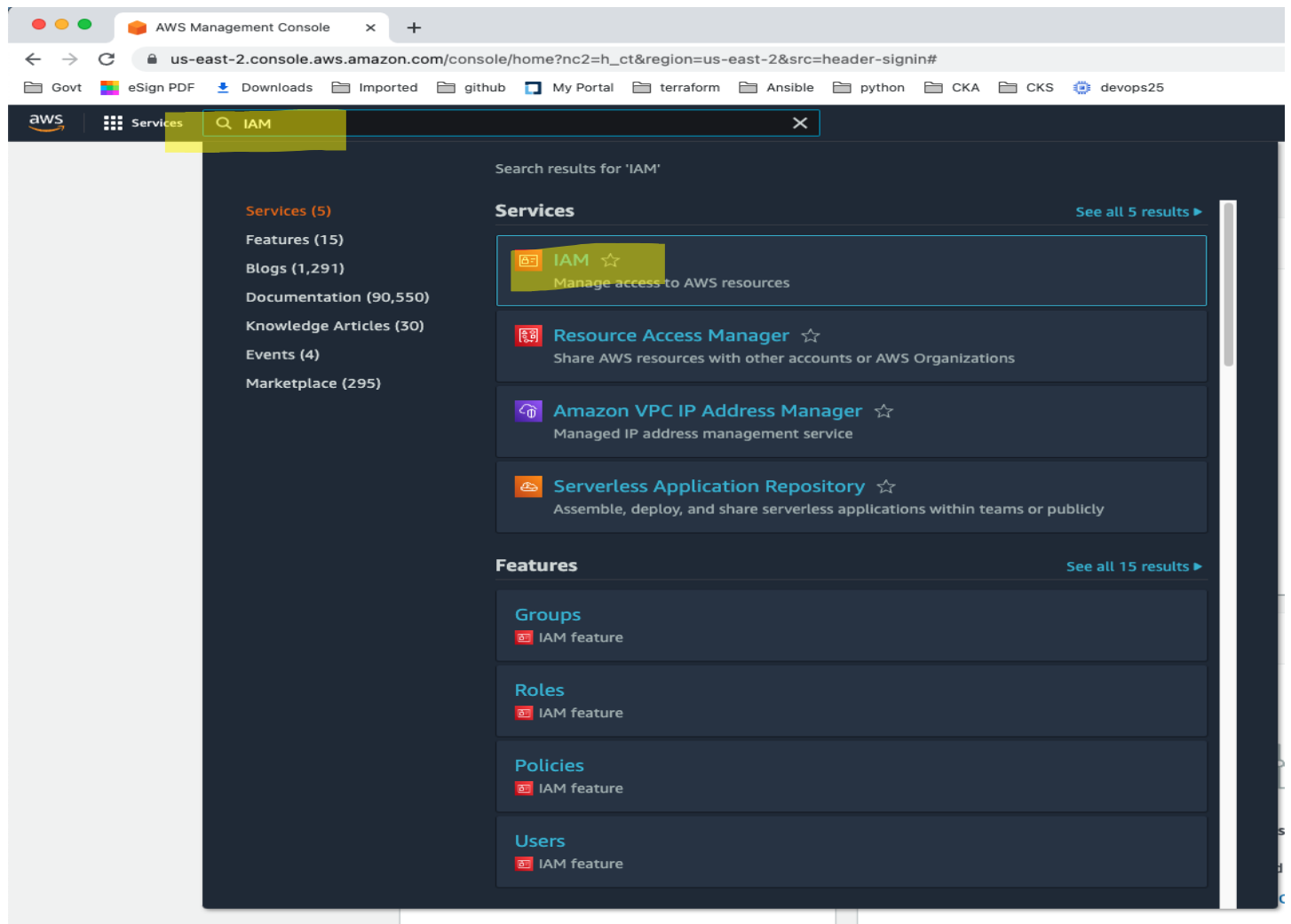
Sign in

[Sign in to a different account](#)

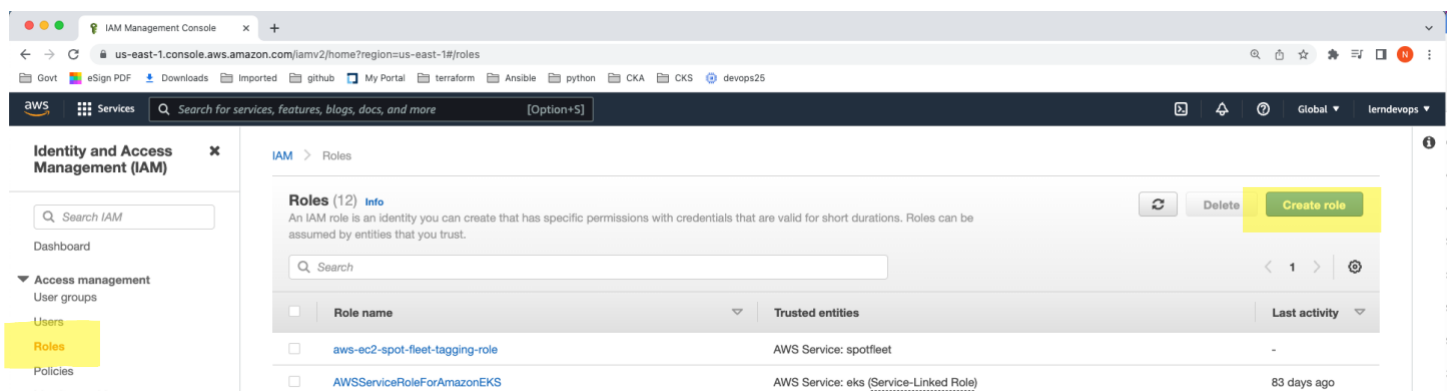
[Create a new AWS account](#)

Create an IAM Role

go to IAM



Click on Roles & then Create Role



Select the Options as Below & Click on Next

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The left sidebar indicates the current step is 'Step 1: Select trusted entity'. The main content area is titled 'Select trusted entity' and contains two sections: 'Trusted entity type' and 'Use case'.

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Common use cases

- ☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.
- ☐ **Lambda**
Allows Lambda functions to call AWS services on your behalf.

Use cases for other AWS services:
Choose a service to view use case

At the bottom right, there are 'Cancel' and 'Next' buttons.

Add permissions as below & click on Next

The screenshot shows the 'Add permissions' step in the AWS IAM console. The left sidebar indicates the current step is 'Step 2: Add permissions'. The main content area is titled 'Add permissions' and contains a search bar and a table of permissions policies.

Permissions policies (Selected 1/740)
Choose one or more policies to attach to your new role.

Search: SSM (14 matches)

Clear filters

	Policy name	Type	Description
<input type="checkbox"/>	AmazonEC2RoleforSSM	AWS m...	This policy will soon be deprecated. Please use AmazonSSMManagedInstanceCore policy to...
<input type="checkbox"/>	AmazonSSMAutomationApproverAccess	AWS m...	Provides access to view automation executions and send approval decisions to automation ...
<input checked="" type="checkbox"/>	AmazonSSMManagedInstanceCore	AWS m...	The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality.
<input type="checkbox"/>	AmazonSSMDirectoryServiceAccess	AWS m...	This policy allows SSM Agent to access Directory Service on behalf of the customer for dom...

Enter the role name & click on Create role

IAM Management Console

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=EC2&step=review&trustedEntityType=AWS_SERVICE

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Services Search for services, features, blogs, docs, and more [Option+S]

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

ec2_ssm_role

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

Description
Add a short explanation for this policy.

Allows EC2 instances to call AWS services on your behalf.

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

IAM Management Console

us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles

Govt eSign PDF Downloads Imported github My Portal terraform Ansible python CKA CKS devops25

Services Search for services, features, blogs, docs, and more [Option+S]

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

- User groups
- Users
- Roles**
- Policies
- Identity providers
- Account settings

Access reports

Role ec2_ssm_role created

View role

IAM > Roles

Roles (13) Info

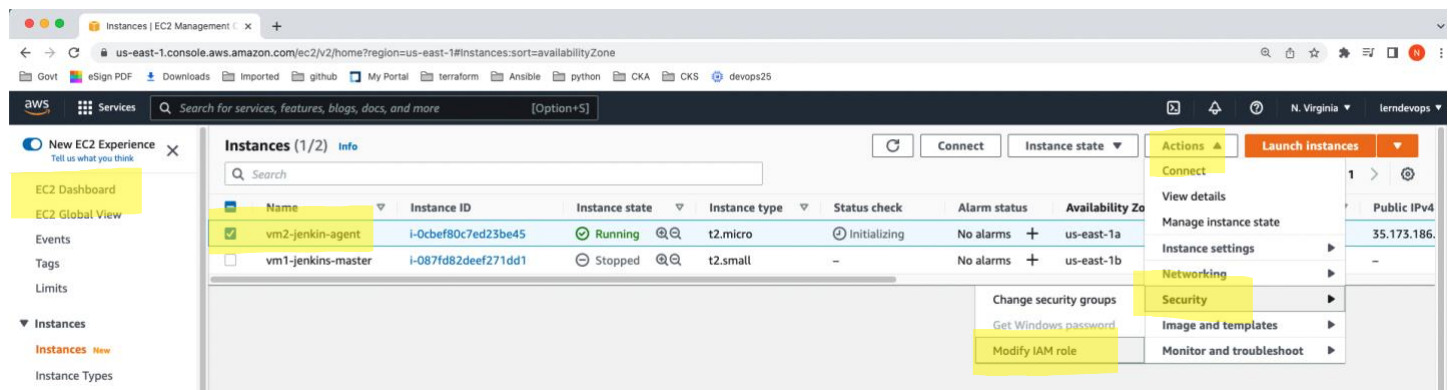
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

ec2 2 matches

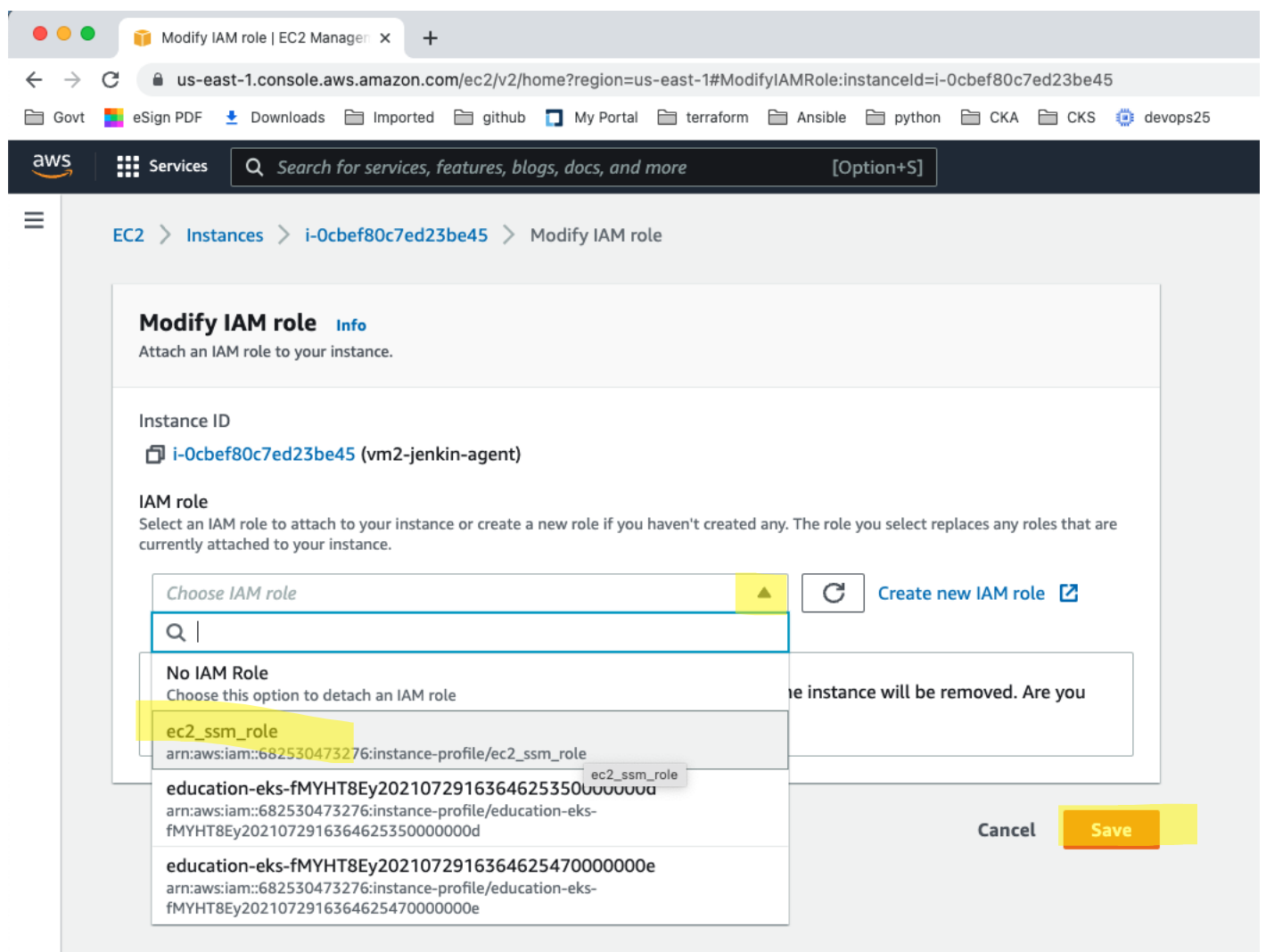
<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	aws-ec2-spot-fleet-tagging-role	AWS Service: spotfleet	-
<input type="checkbox"/>	ec2_ssm_role	AWS Service: ec2	-

Attach IAM Role to Existing EC2 Instance

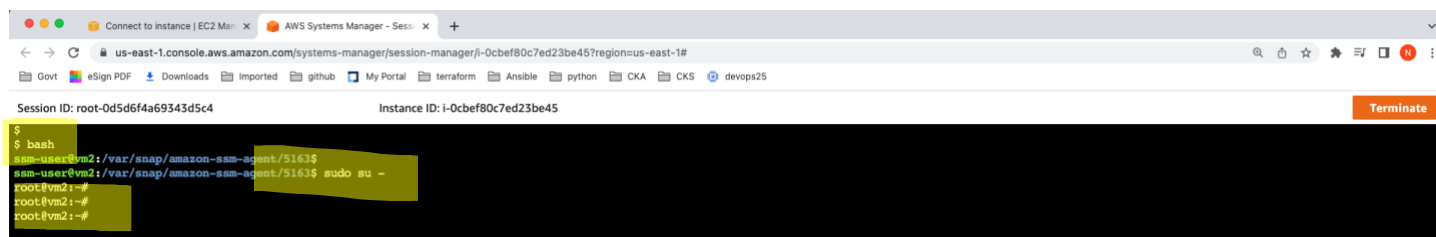
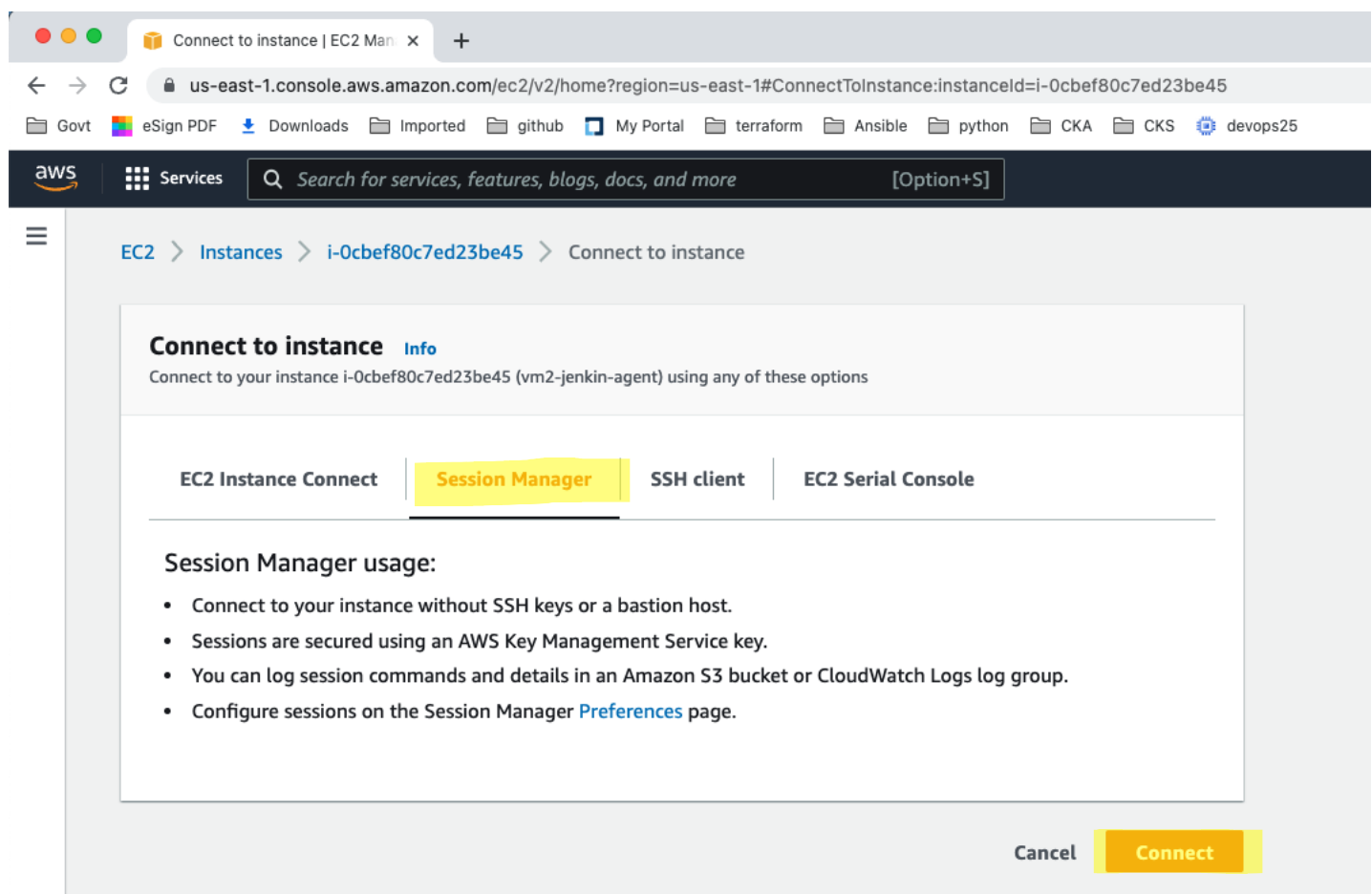
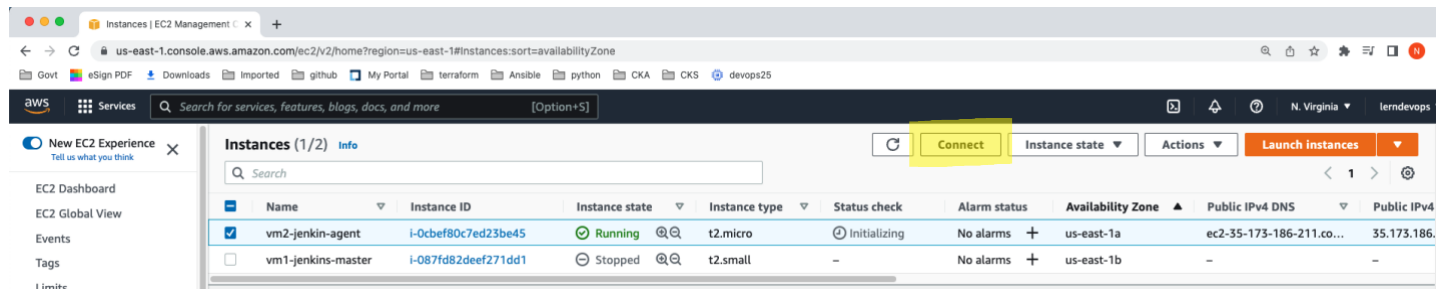
Go to EC2 Dashboard, Select any Instance & Actions as Below



Choose IAM role & Save



Connect to EC2



Attach IAM Role While Creating EC2 Instance

Launch instance wizard | EC2 | x

us-east-1.console.aws.amazon.com/ec2/v2/home?region=us-east-1#LaunchInstanceWizard:

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances ⓘ 1 [Launch into Auto Scaling Group](#) ⓘ

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-87dab7fa (default) [Create new VPC](#)

Subnet ⓘ No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP ⓘ Use subnet setting (Enable) ⓘ

Hostname type ⓘ Use subnet setting (IP name) ⓘ

DNS Hostname ⓘ ☒ Enable IP name IPv4 (A record) DNS requests ☒ Enable resource-based IPv4 (A record) DNS requests ☐ Enable resource-based IPv6 (AAAA record) DNS requests

Placement group ⓘ ☐ Add instance to placement group

Capacity Reservation ⓘ Open ⓘ

Domain join directory ⓘ No directory ⓘ [Create new directory](#)

IAM role ⓘ ec2_ssm_role ⓘ [Create new IAM role](#)

Shutdown behavior ⓘ Stop ⓘ

Stop - Hibernate behavior ⓘ ☐ Enable hibernation as an additional stop behavior

Enable termination protection ⓘ ☐ Protect against accidental termination

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: /](#)

more info:

<https://docs.aws.amazon.com/systems-manager/latest/userguide/session-manager.html>