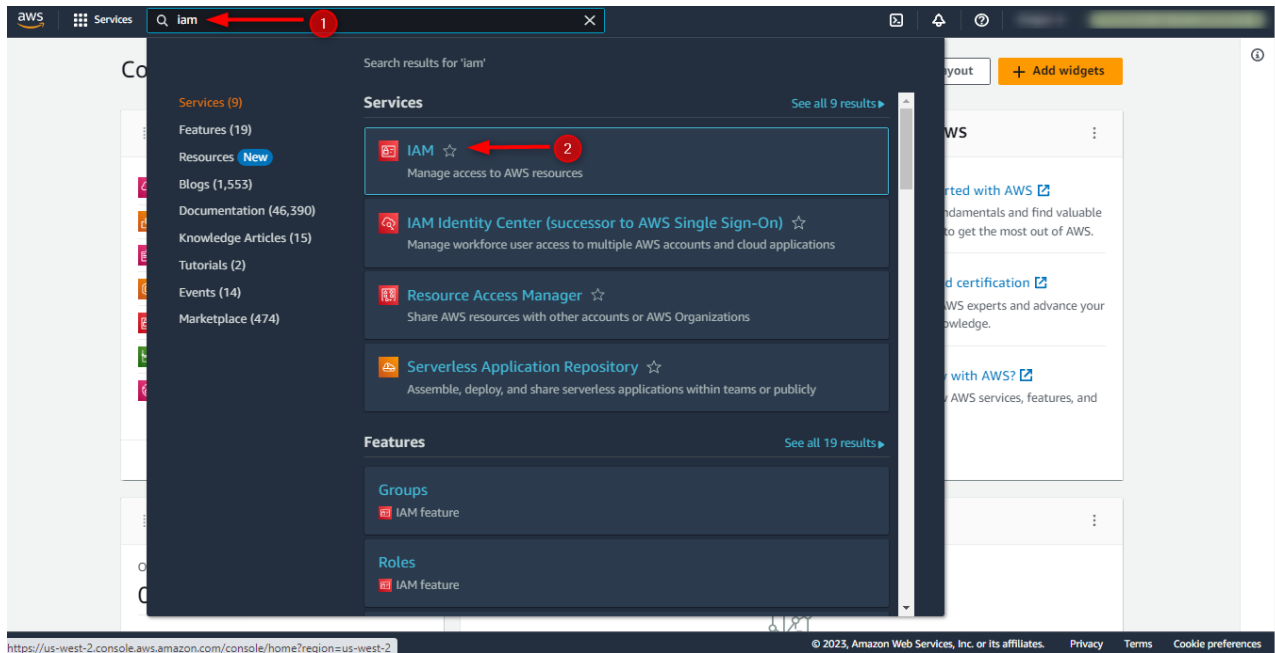
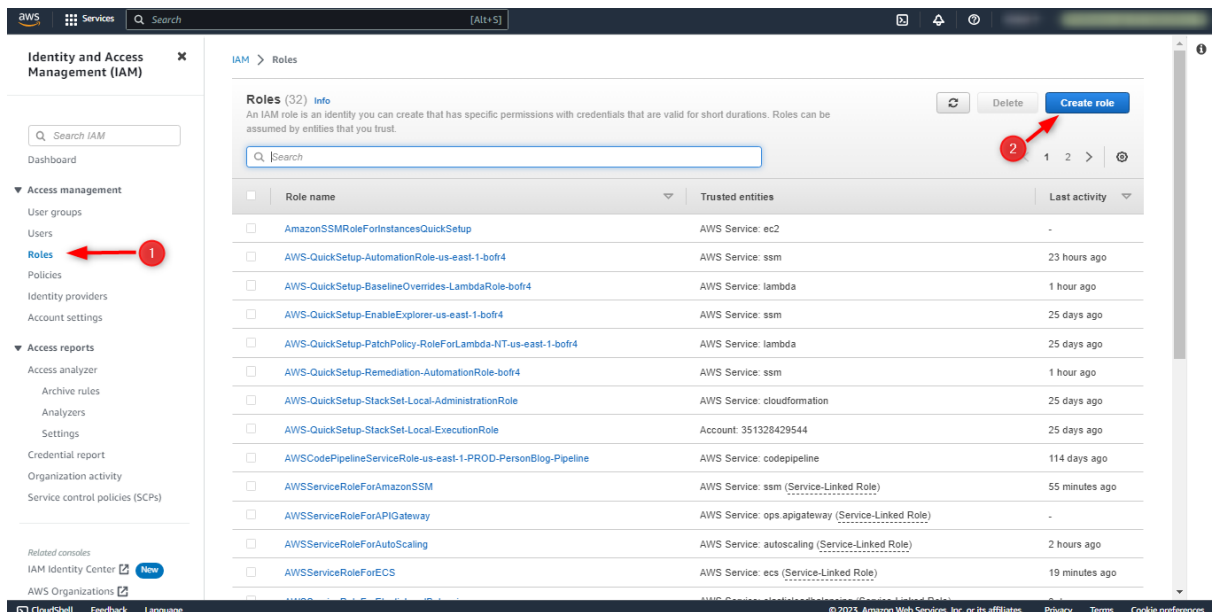


IAM Role para gerenciar SSM

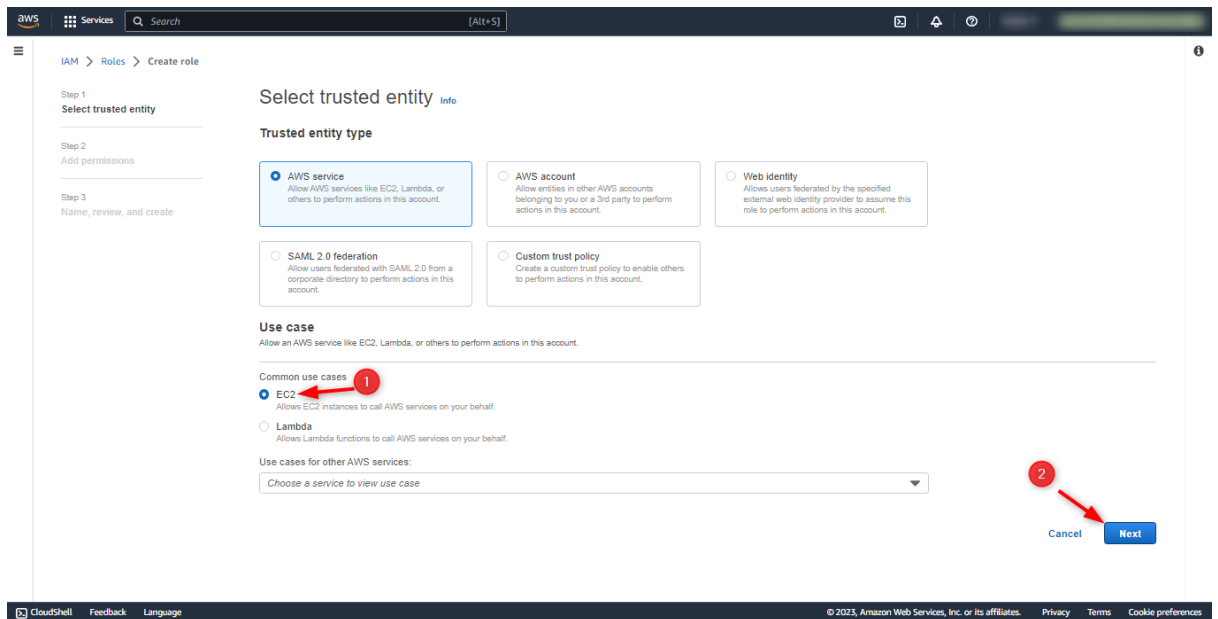
1. Digite IAM no campo de pesquisa e selecione IAM



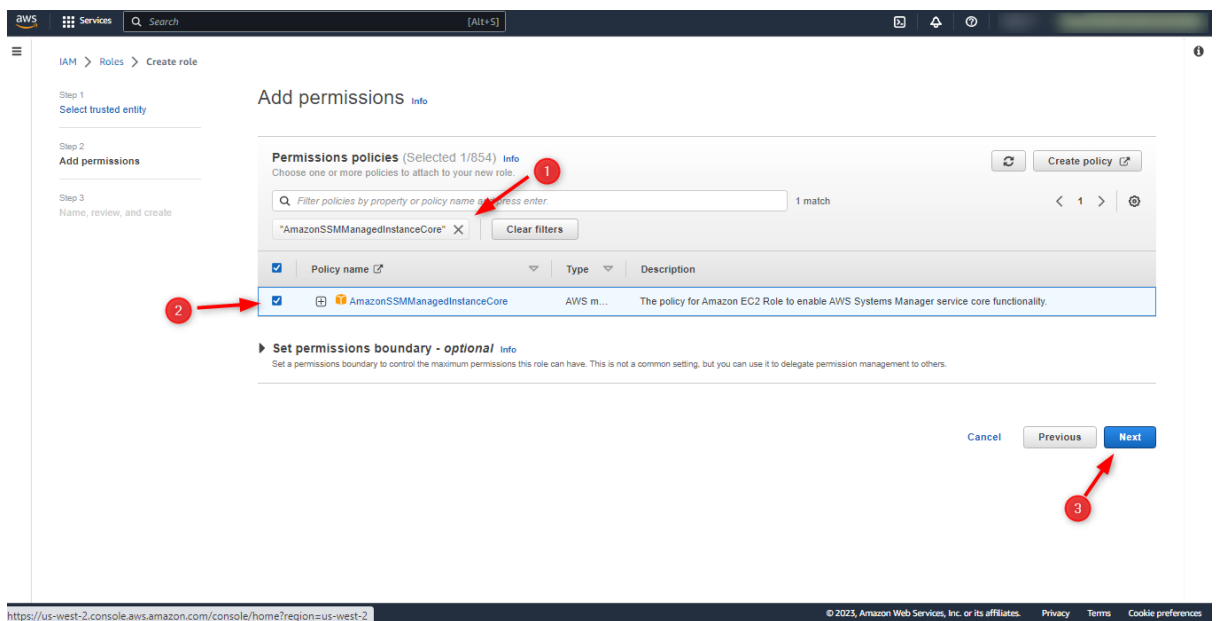
2. Clique em Roles e em seguida Create Roles.



3. Selecione EC2 em Common use cases em seguida clique em Next.



4. Digite AmazonSSMManagedInstanceCore no campo de pesquisa e pressione Enter, em seguida selecione a política e clique em Next



5. Digite o nome da sua role e desça a página até o final.

Step 3
Name, review, and create

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
EC2-ssm-Teste
Maximum 64 characters. Use alphanumeric and "+", "@", "-", "." characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use alphanumeric and "+", "@", "-", "." characters.

Step 1: Select trusted entities Edit

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13      }  
14    ]  
15  }  
16 }
```

6. Clique em Create role para finalizar.

Step 2: Add permissions Edit

Permissions policy summary

Policy name	Type	Attached as
AmazonSSMManagedInstanceCore	AWS managed	Permissions policy

Tags

Add tags - optional [Info](#)
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.

[Add tag](#)
You can add up to 50 more tags.

[Cancel](#) [Previous](#) **Create role**