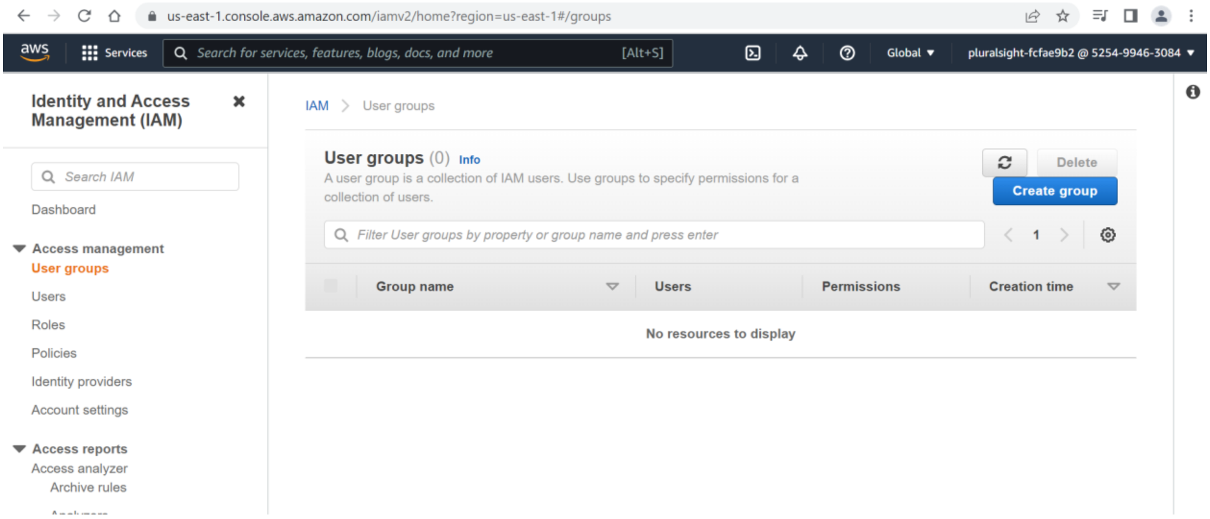
1. Create Groups Based on Required Access


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

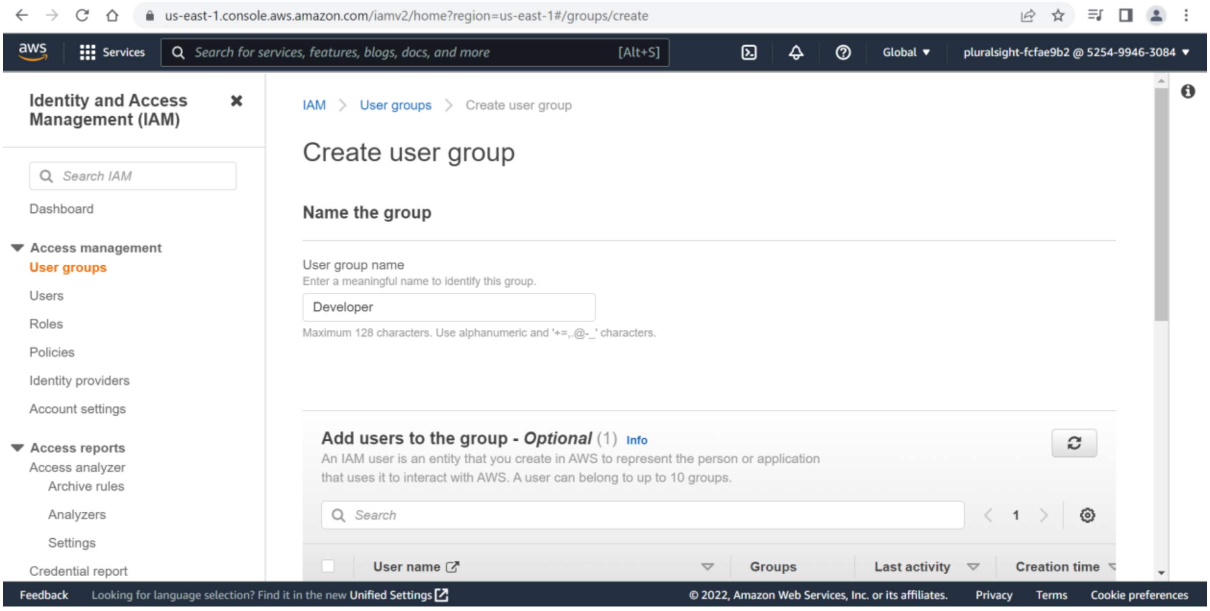
User groups (0) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

□	Group name	Users	Permissions	Creation time

No resources to display


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

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global ▾
pluralsight-fcfae9b2 @ 5254-9946-3084 ▾
Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access analyzer
Archive rules
Analyzers
Settings
Credential report
IAM > User groups > Create user group
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create user group

Name the group

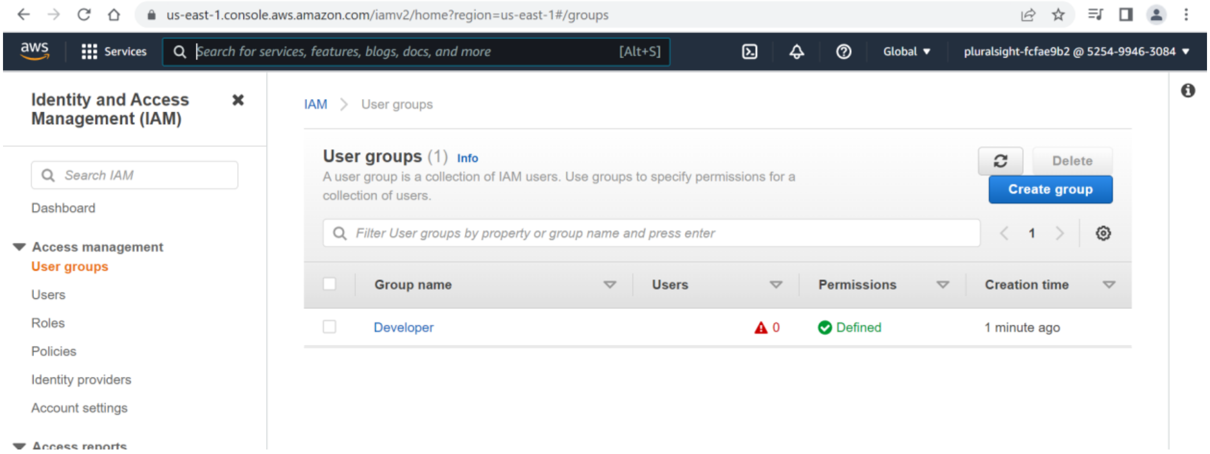
User group name
Enter a meaningful name to identify this group.
Developer
Maximum 128 characters. Use alphanumeric and '+=,.@-_' characters.

Add users to the group - *Optional* (1) Info

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS. A user can belong to up to 10 groups.

Search

□	User name	Groups	Last activity	Creation time


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

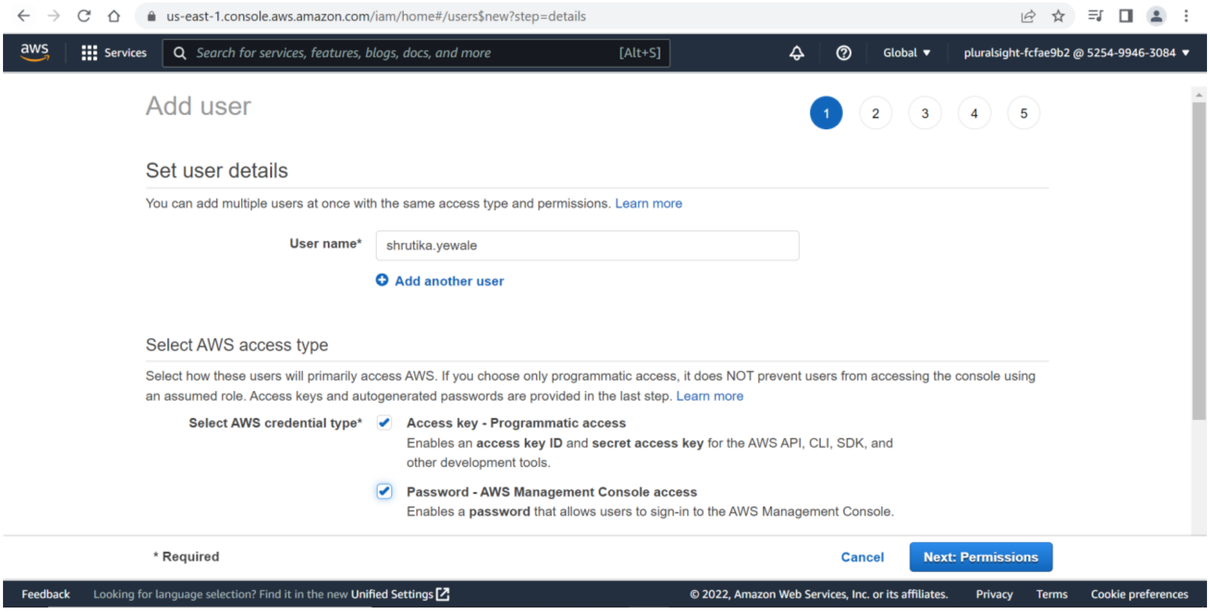
User groups (1) Info

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Filter User groups by property or group name and press enter

□	Group name	Users	Permissions	Creation time
□	Developer	⚠ 0	✓ Defined	1 minute ago

2. Create Users and Apply Groups



us-east-1.console.aws.amazon.com/iam/home#/users$new?step=details

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
1
2
3
4
5

Add user

Set user details

You can add multiple users at once with the same access type and permissions. Learn more

User name* shrutika.yewale

Add another user

Select AWS access type

Select how these users will primarily access AWS. If you choose only programmatic access, it does NOT prevent users from accessing the console using an assumed role. Access keys and autogenerated passwords are provided in the last step. Learn more

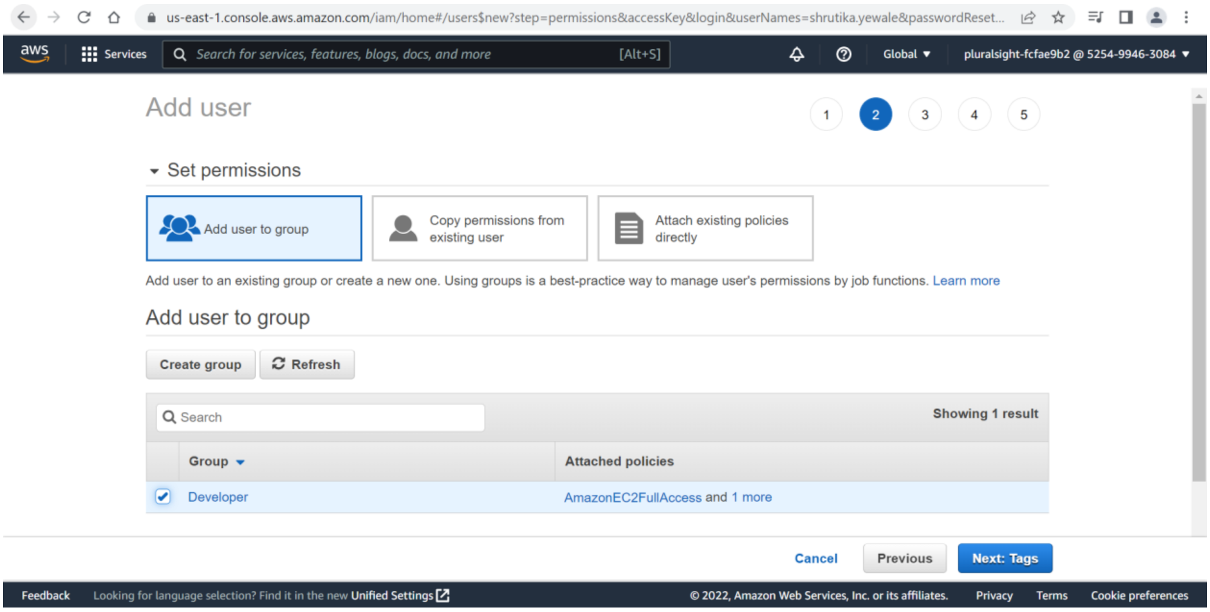
Select AWS credential type*

☑ **Access key - Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.

☑ **Password - AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

* Required

Cancel
Next: Permissions
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



us-east-1.console.aws.amazon.com/iam/home#/users$new?step=permissions&accessKey&login&userNames=shrutika.yewale&passwordReset...

aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
1
2
3
4
5

Add user

Set permissions

Add user to group
Copy permissions from existing user
Attach existing policies directly

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

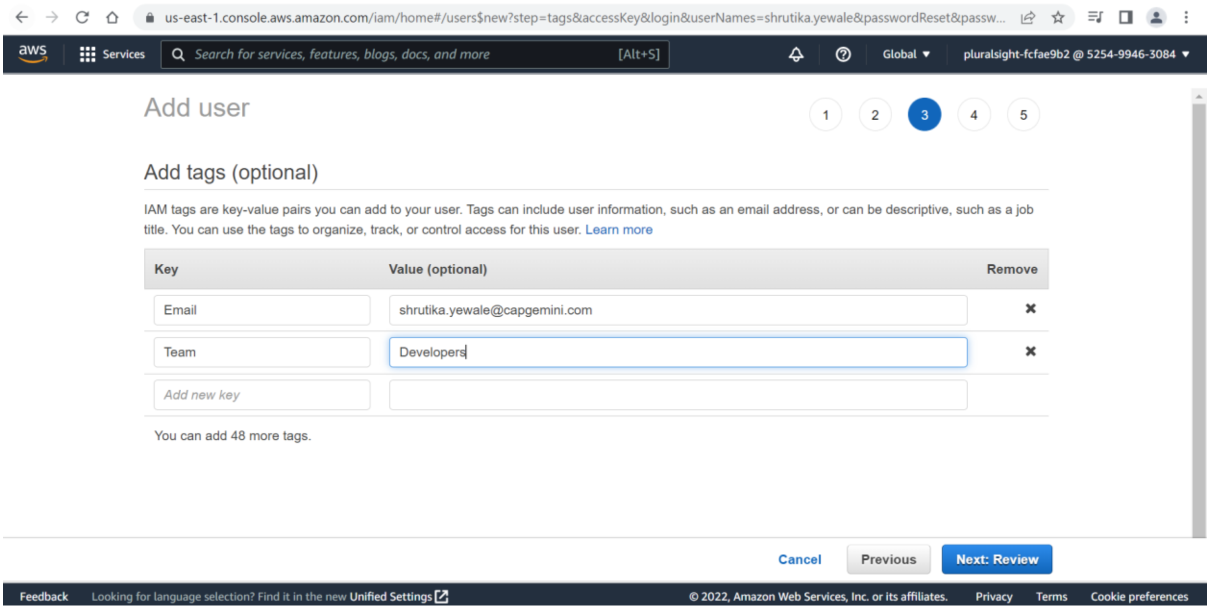
Add user to group

Create group
Refresh
Search

Showing 1 result

	Group	Attached policies
☑	Developer	AmazonEC2FullAccess and 1 more

Cancel
Previous
Next: Tags
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


us-east-1.console.aws.amazon.com/iam/home#/users$new?step=tags&accessKey&login&userNames=shrutika.yewale&passwordReset&passw...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
1
2
3
4
5
Cancel
Previous
Next: Review
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

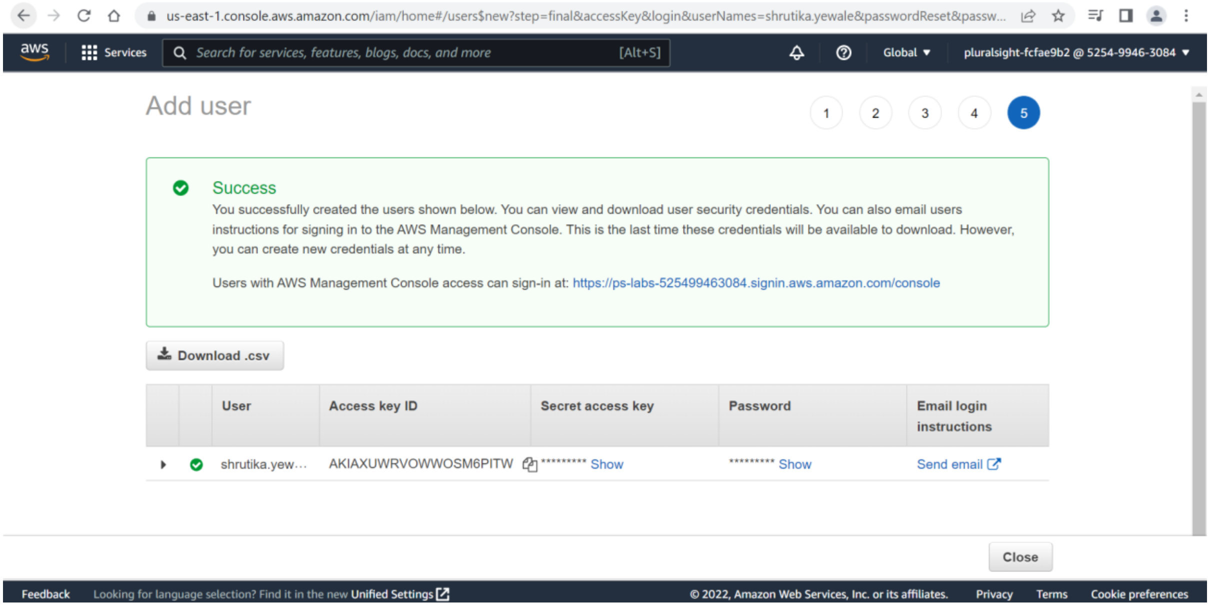
Add user

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. Learn more

Key	Value (optional)	Remove
Email	shrutika.yewale@capgemini.com	✖
Team	Developers	✖
Add new key		

You can add 48 more tags.


us-east-1.console.aws.amazon.com/iam/home#/users$new?step=final&accessKey&login&userNames=shrutika.yewale&passwordReset&passw...
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
1
2
3
4
5
Download .csv
Close
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Add user

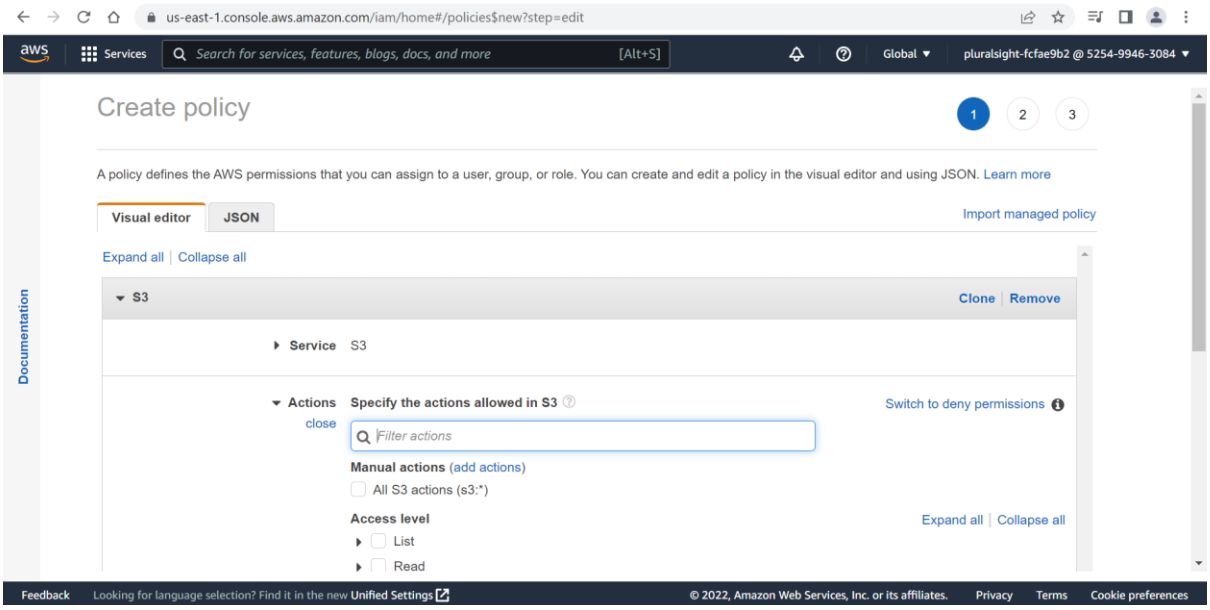
Success

You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

Users with AWS Management Console access can sign-in at: https://ps-labs-525499463084.signin.aws.amazon.com/console

		User	Access key ID	Secret access key	Password	Email login instructions
▸	✓	shrutika.yew...	AKIAXUWRVOWWOSM6PITW	******** Show	******** Show	Send email

3. Create A Custom Policy Access To S3 Bucket Functionality



us-east-1.console.aws.amazon.com/iam/home#/policies$new?step=edit
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
Documentation
1
2
3
Visual editor
JSON
Import managed policy
Expand all | Collapse all
Clone | Remove
Switch to deny permissions
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the visual editor and using JSON. Learn more

S3

Service S3

Actions close — Specify the actions allowed in S3

Filter actions

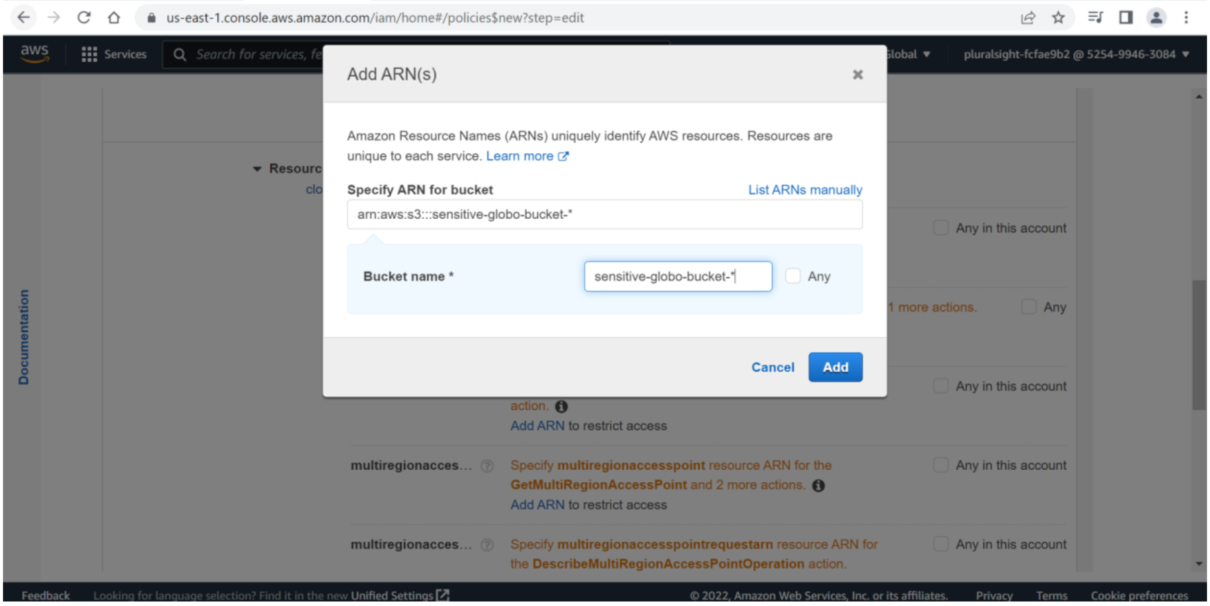
Manual actions (add actions)

□ All S3 actions (s3:*)

Access level — Expand all | Collapse all

□ List

□ Read



us-east-1.console.aws.amazon.com/iam/home#/policies$new?step=edit
aws
Services
Search for services, fe
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
Documentation
Resourc
clo
×
List ARNs manually
Cancel
Add
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Add ARN(s)

Amazon Resource Names (ARNs) uniquely identify AWS resources. Resources are unique to each service. Learn more

Specify ARN for bucket

arn:aws:s3:::sensitive-globo-bucket-*

Bucket name * sensitive-globo-bucket-* □ Any

□ Any in this account

1 more actions. □ Any

□ Any in this account

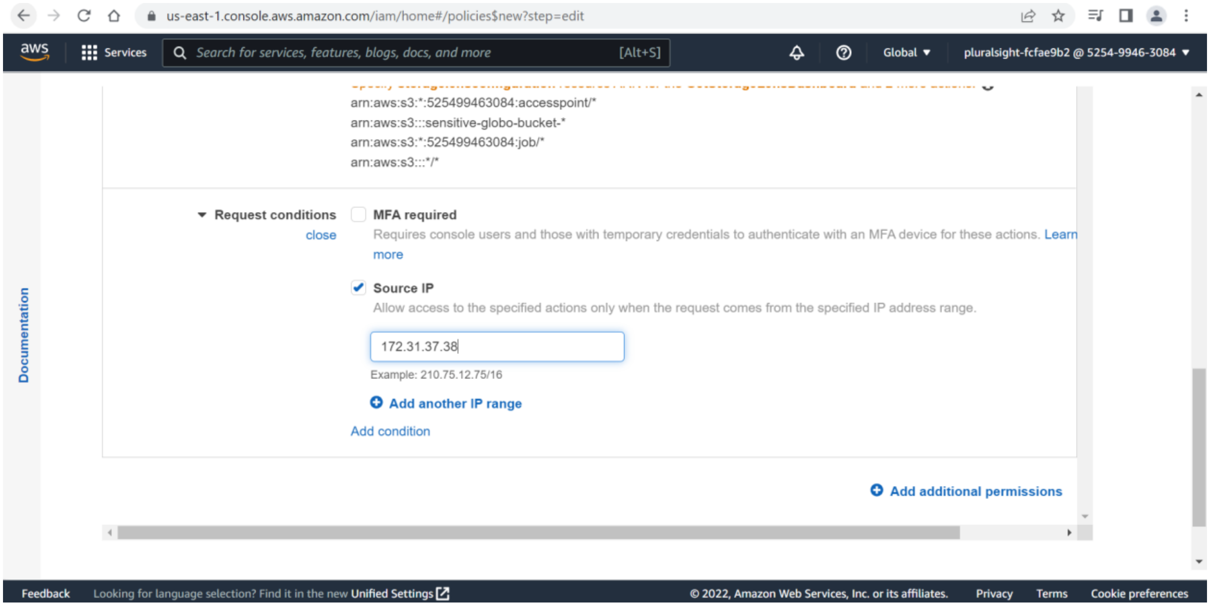
action.

Add ARN to restrict access

multiregionacces... — Specify **multiregionaccesspoint** resource ARN for the **GetMultiRegionAccessPoint** and 2 more actions. □ Any in this account

Add ARN to restrict access

multiregionacces... — Specify **multiregionaccesspointrequestarn** resource ARN for the **DescribeMultiRegionAccessPointOperation** action. □ Any in this account



us-east-1.console.aws.amazon.com/iam/home#/policies$new?step=edit
aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
Documentation
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

arn:aws:s3:*:525499463084:accesspoint/*
arn:aws:s3:::sensitive-globo-bucket-*
arn:aws:s3:*:525499463084:job/*
arn:aws:s3:::*/*

Request conditions close

□ MFA required

Requires console users and those with temporary credentials to authenticate with an MFA device for these actions. Learn more

☑ Source IP

Allow access to the specified actions only when the request comes from the specified IP address range.

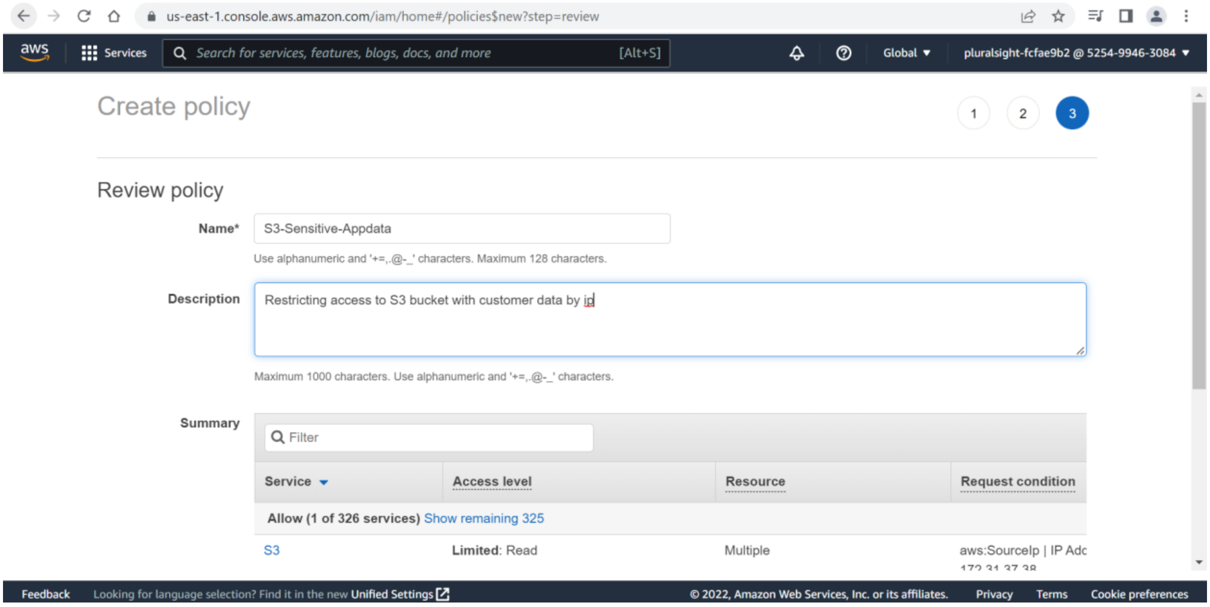
172.31.37.38

Example: 210.75.12.75/16

Add another IP range

Add condition

Add additional permissions


us-east-1.console.aws.amazon.com/iam/home#/policies$new?step=review
aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
1
2
3
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Create policy

Review policy

Name* S3-Sensitive-Appdata

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

Description Restricting access to S3 bucket with customer data by ip

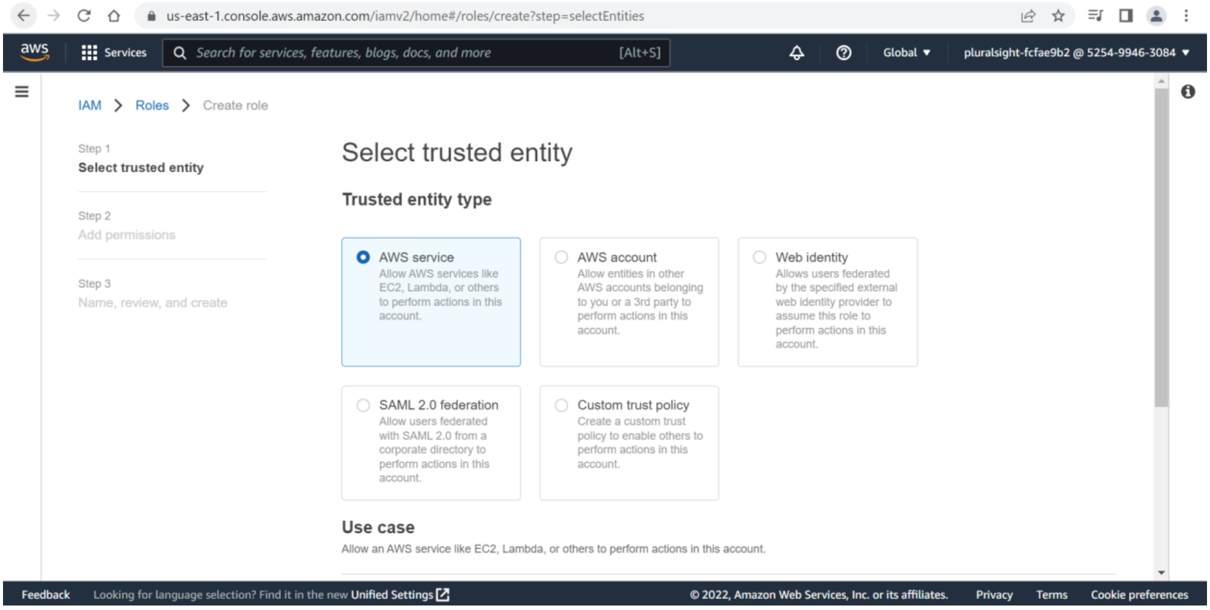
Maximum 1000 characters. Use alphanumeric and '+=,.@-_' characters.

Summary

Filter

Service	Access level	Resource	Request condition
Allow (1 of 326 services) Show remaining 325			
S3	Limited: Read	Multiple	aws:SourceIp | IP Adc 172.31.37.38

4. Create a Custom Role for EC2 Instance Access to S3 Bucket


us-east-1.console.aws.amazon.com/iamv2/home#/roles/create?step=selectEntities
aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
pluralsight-fcfae9b2 @ 5254-9946-3084
IAM
Roles
Create role
Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity

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.

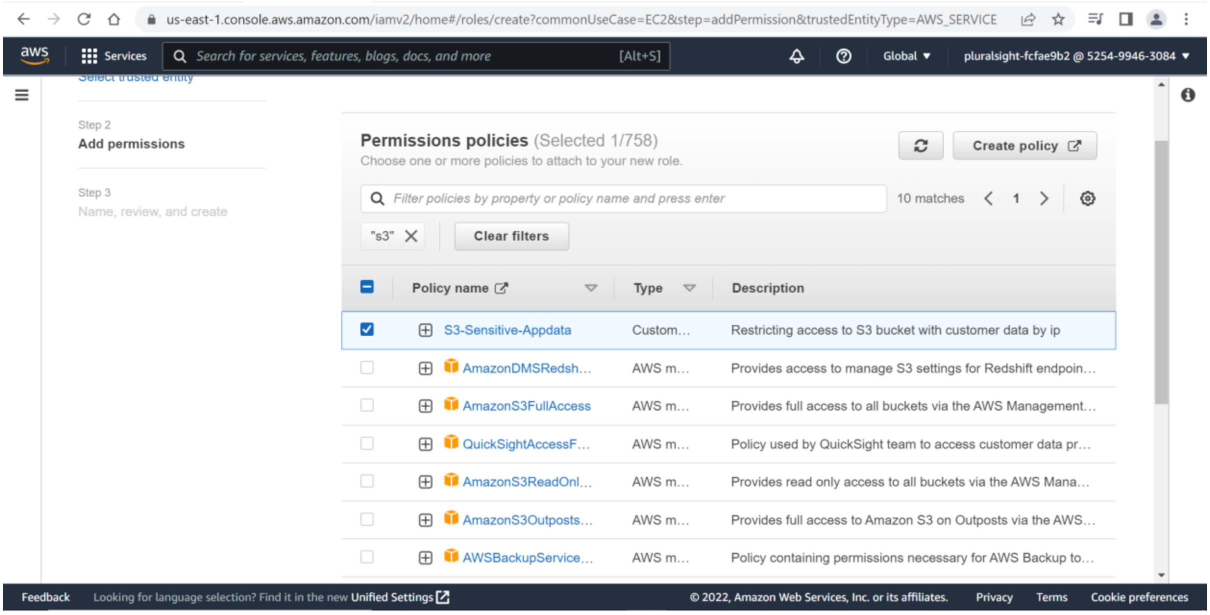
○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ 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.



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

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global ▼
pluralsight-fcfae9b2 @ 5254-9946-3084 ▼
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

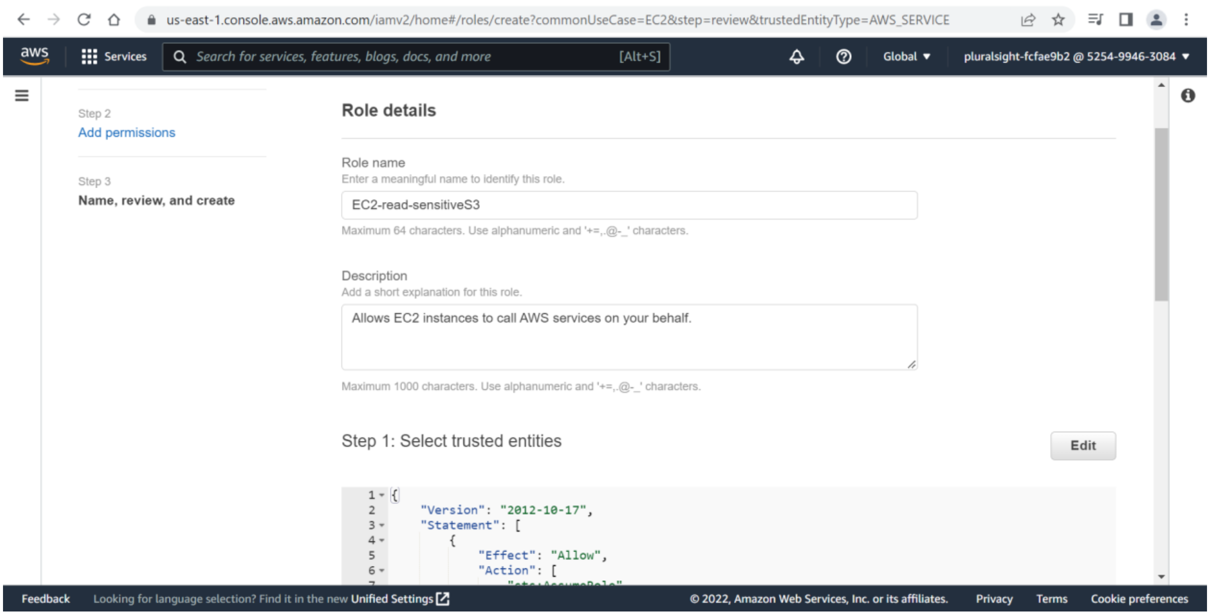
Permissions policies (Selected 1/758)

Choose one or more policies to attach to your new role.

Create policy
Filter policies by property or policy name and press enter
10 matches
1
"s3"
Clear filters

▣	Policy name	Type	Description
☑	S3-Sensitive-Appdata	Custom…	Restricting access to S3 bucket with customer data by ip
□	AmazonDMSRedsh…	AWS m…	Provides access to manage S3 settings for Redshift endpoin…
□	AmazonS3FullAccess	AWS m…	Provides full access to all buckets via the AWS Management…
□	QuickSightAccessF…	AWS m…	Policy used by QuickSight team to access customer data pr…
□	AmazonS3ReadOnl…	AWS m…	Provides read only access to all buckets via the AWS Mana…
□	AmazonS3Outposts…	AWS m…	Provides full access to Amazon S3 on Outposts via the AWS…
□	AWSBackupService…	AWS m…	Policy containing permissions necessary for AWS Backup to…

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



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

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global ▼
pluralsight-fcfae9b2 @ 5254-9946-3084 ▼

Step 2
Add permissions

Step 3
Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.

EC2-read-sensitiveS3

Maximum 64 characters. Use alphanumeric and '+=,.@-_' characters.

Description
Add a short explanation for this role.

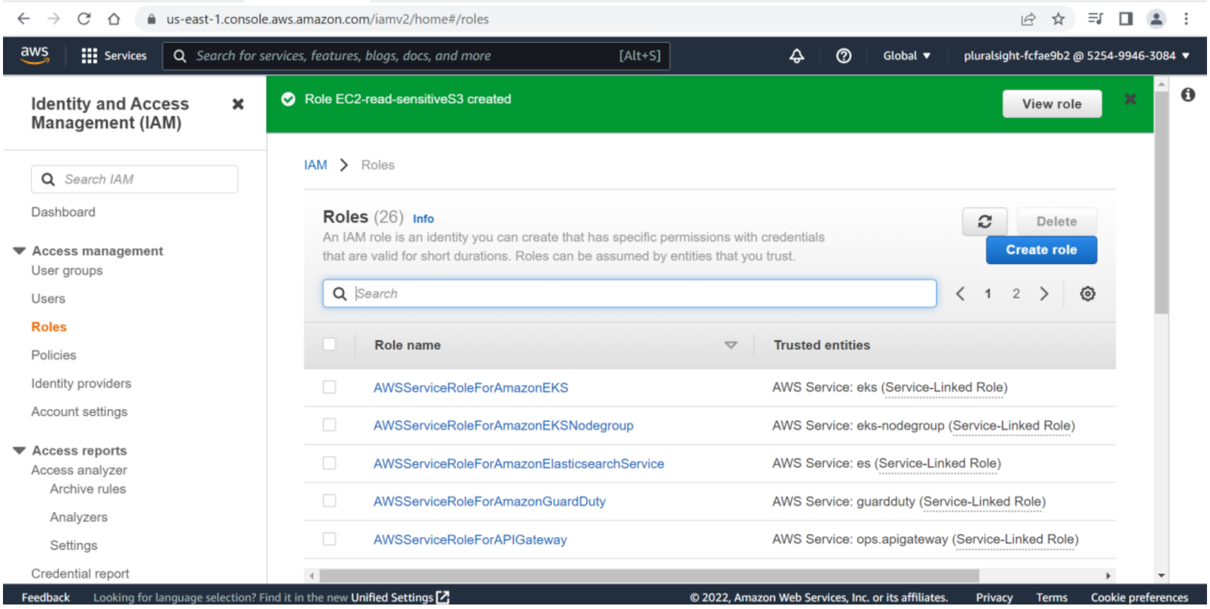
Allows EC2 instances to call AWS services on your behalf.

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

Step 1: Select trusted entities

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "sts:AssumeRole"
```

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



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

Role EC2-read-sensitiveS3 created

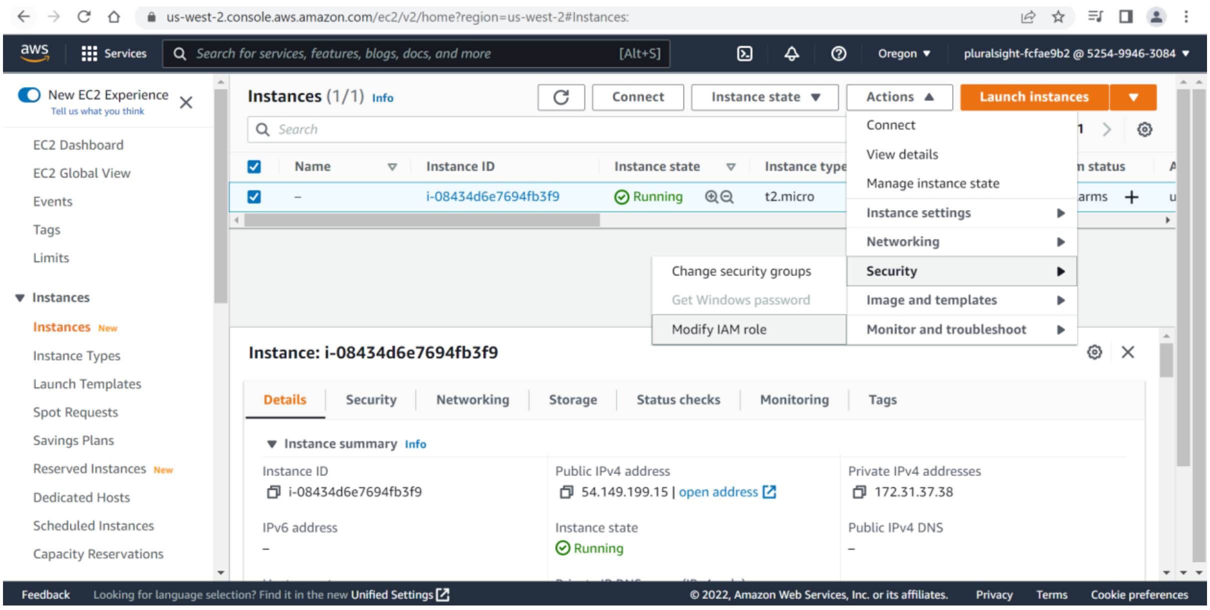
Identity and Access Management (IAM)

IAM > Roles

Roles (26) 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.

Role name	Trusted entities
AWSServiceRoleForAmazonEKS	AWS Service: eks (Service-Linked Role)
AWSServiceRoleForAmazonEKSNodegroup	AWS Service: eks-nodegroup (Service-Linked Role)
AWSServiceRoleForAmazonElasticsearchService	AWS Service: es (Service-Linked Role)
AWSServiceRoleForAmazonGuardDuty	AWS Service: guardduty (Service-Linked Role)
AWSServiceRoleForAPIGateway	AWS Service: ops.apigateway (Service-Linked Role)



us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:

Instances (1/1) Info

Name	Instance ID	Instance state	Instance type
–	i-08434d6e7694fb3f9	Running	t2.micro

Actions > Security > Modify IAM role

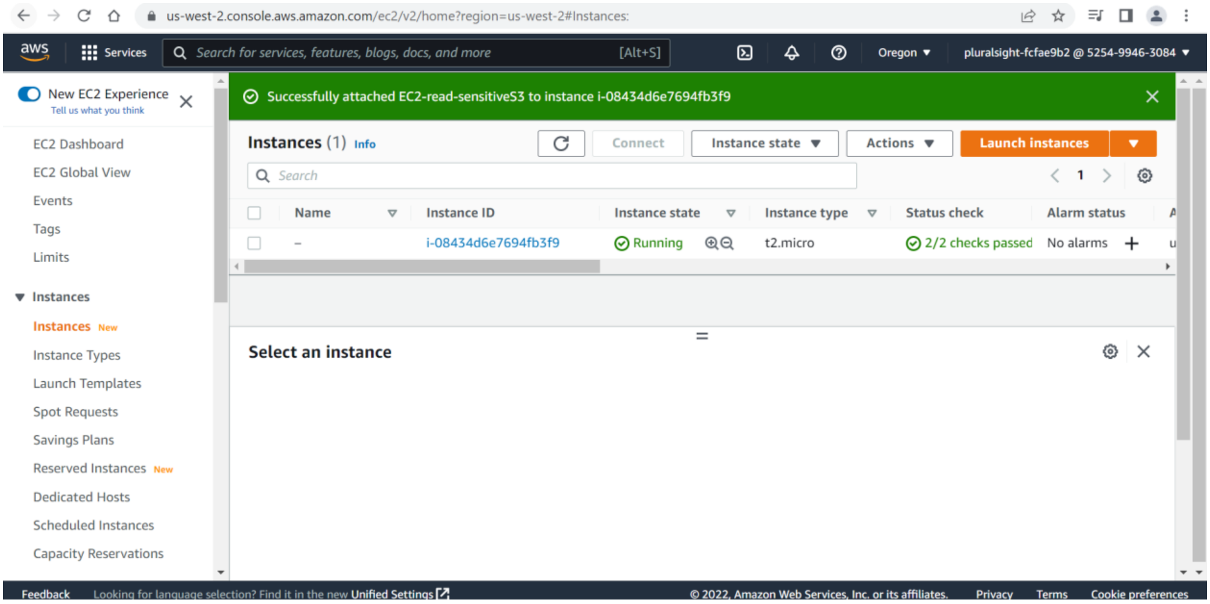
Instance: i-08434d6e7694fb3f9

Details | Security | Networking | Storage | Status checks | Monitoring | Tags

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-08434d6e7694fb3f9	54.149.199.15 | open address	172.31.37.38

IPv6 address	Instance state	Public IPv4 DNS
–	Running	–



us-west-2.console.aws.amazon.com/ec2/v2/home?region=us-west-2#Instances:

Successfully attached EC2-read-sensitiveS3 to instance i-08434d6e7694fb3f9

Instances (1) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status
–	i-08434d6e7694fb3f9	Running	t2.micro	2/2 checks passed	No alarms

Select an instance