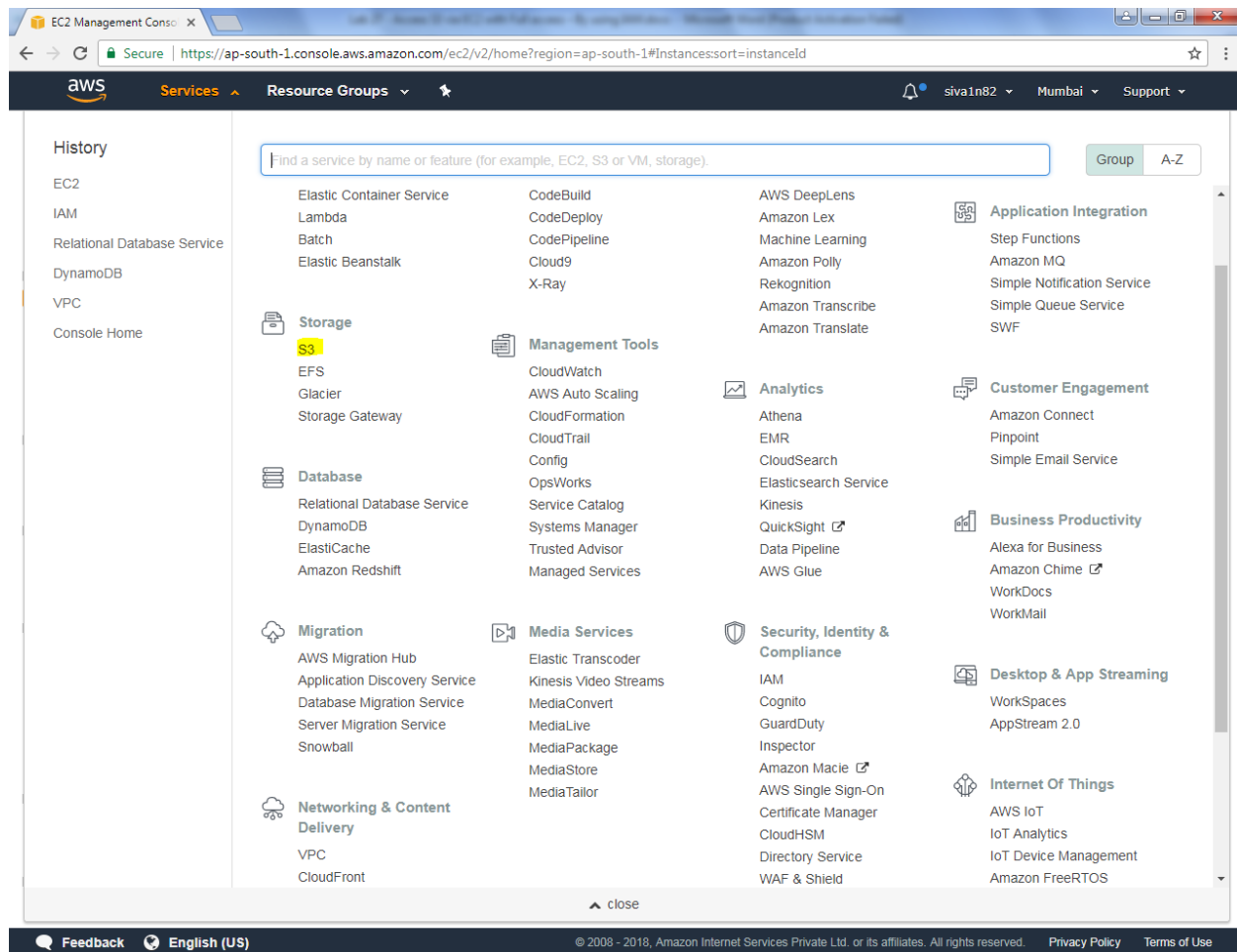


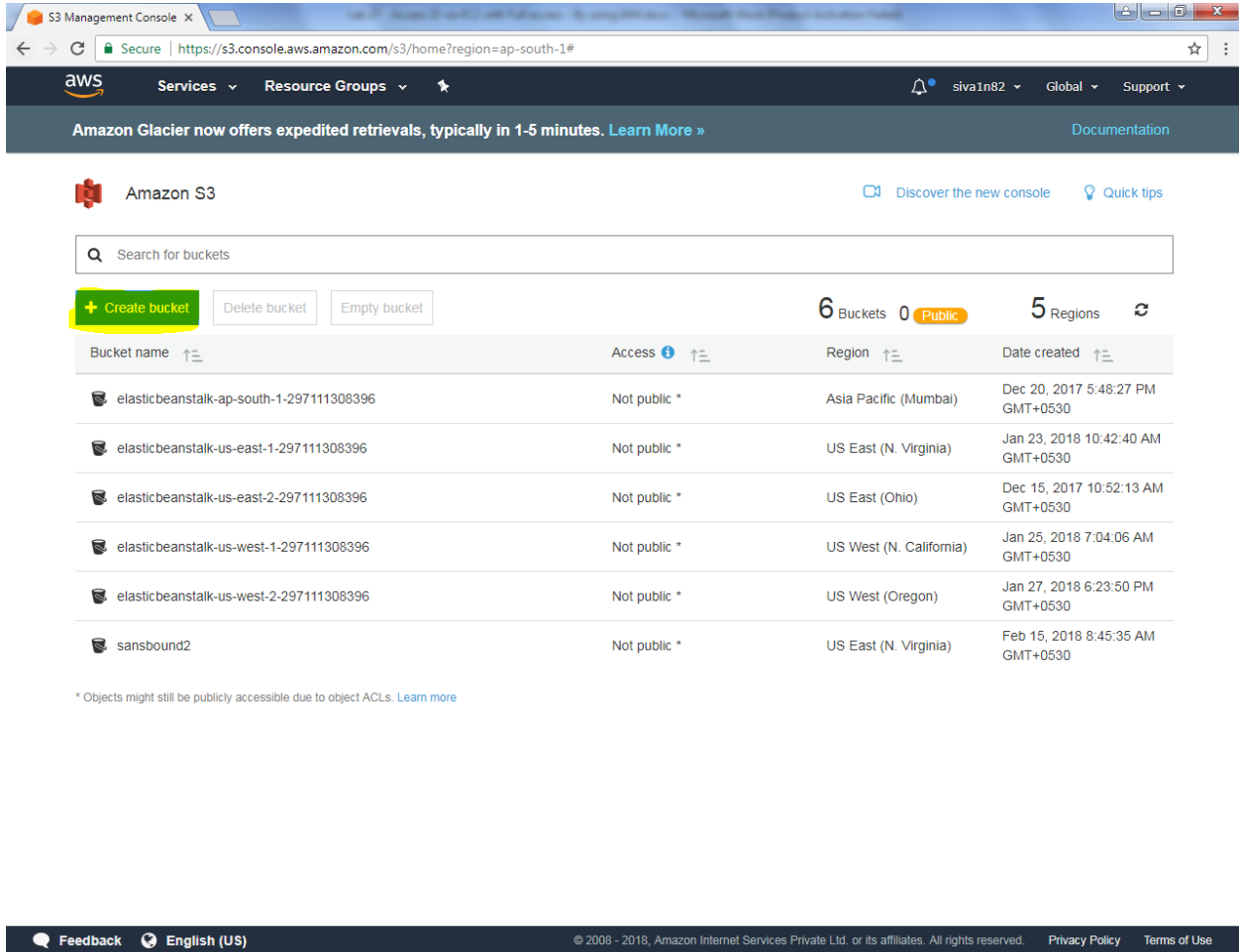
Lab 27

Access S3 via EC2 with Full access – By using IAM

Click “S3” service



Click “Create bucket”.



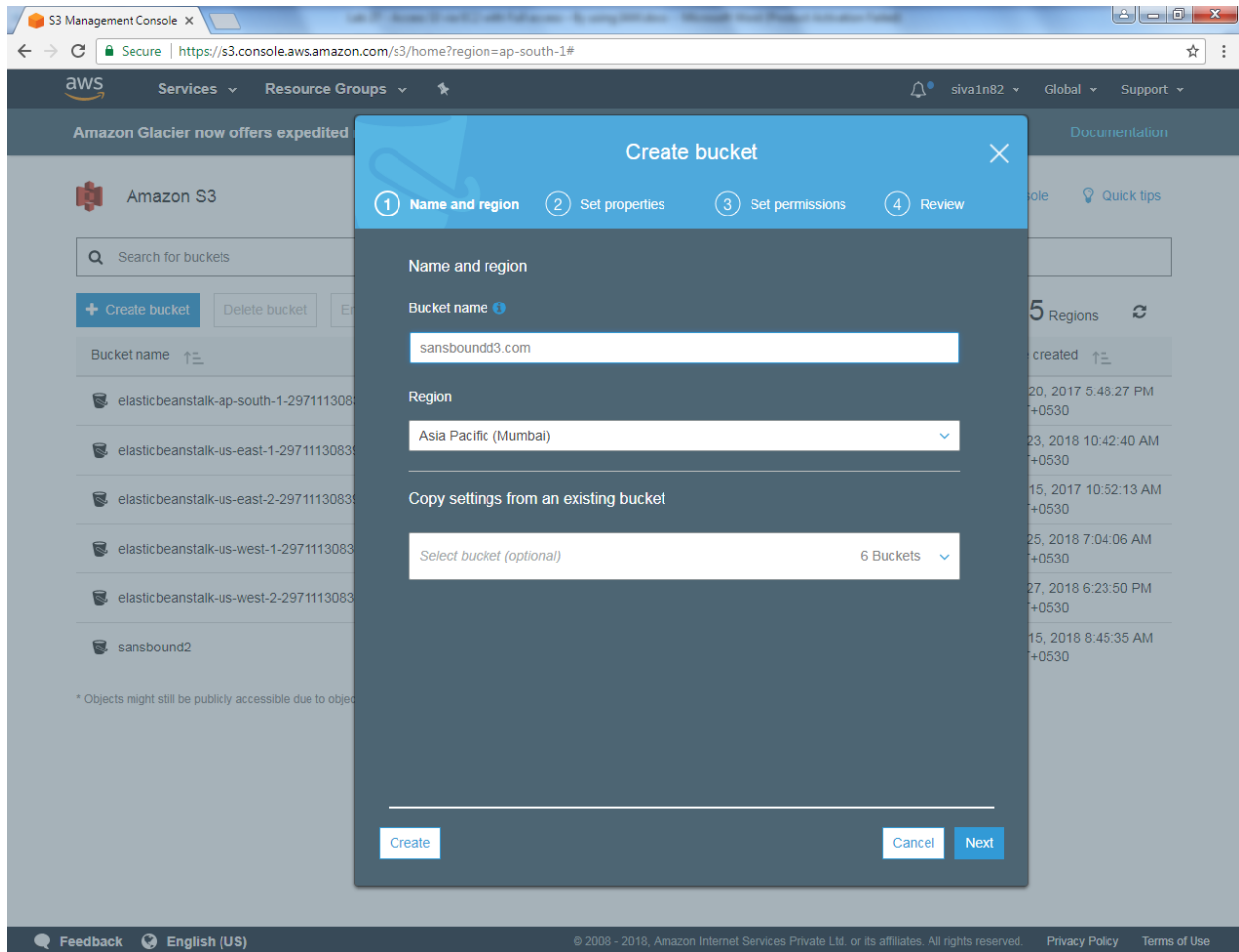
The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and user information. Below this is a banner for Amazon Glacier. The main header says 'Amazon S3' with links to 'Discover the new console' and 'Quick tips'. A search bar is present. Below the search bar, there are buttons: '+ Create bucket' (highlighted in green), 'Delete bucket', and 'Empty bucket'. To the right, it shows '6 Buckets', '0 Public', and '5 Regions'. A table lists the buckets with columns for Bucket name, Access, Region, and Date created.

Bucket name	Access	Region	Date created
elasticbeanstalk-ap-south-1-297111308396	Not public *	Asia Pacific (Mumbai)	Dec 20, 2017 5:48:27 PM GMT+0530
elasticbeanstalk-us-east-1-297111308396	Not public *	US East (N. Virginia)	Jan 23, 2018 10:42:40 AM GMT+0530
elasticbeanstalk-us-east-2-297111308396	Not public *	US East (Ohio)	Dec 15, 2017 10:52:13 AM GMT+0530
elasticbeanstalk-us-west-1-297111308396	Not public *	US West (N. California)	Jan 25, 2018 7:04:06 AM GMT+0530
elasticbeanstalk-us-west-2-297111308396	Not public *	US West (Oregon)	Jan 27, 2018 6:23:50 PM GMT+0530
sansbound2	Not public *	US East (N. Virginia)	Feb 15, 2018 8:45:35 AM GMT+0530

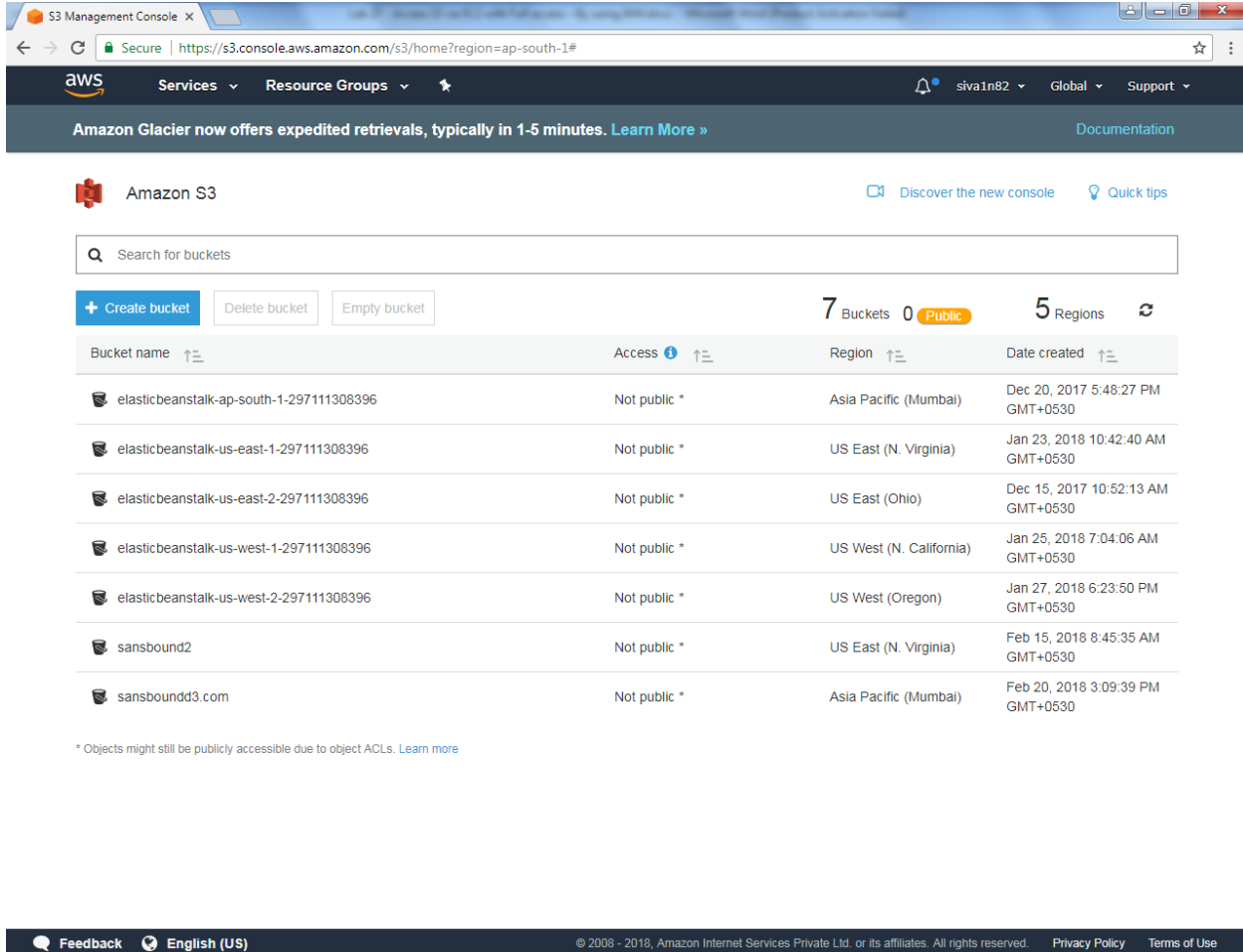
* Objects might still be publicly accessible due to object ACLs. [Learn more](#)

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type sansboundd3.com



Bucket has been successfully created.



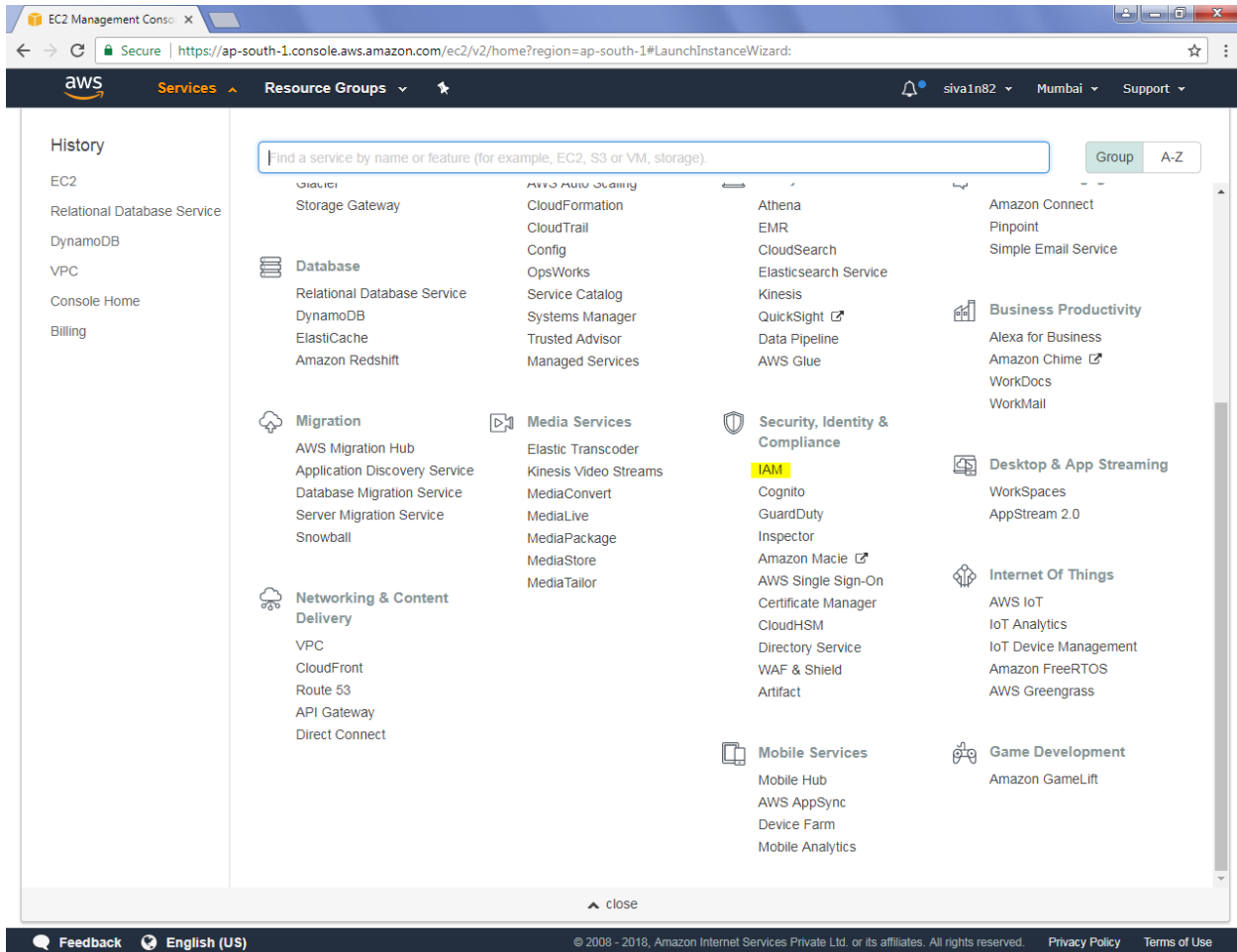
The screenshot shows the AWS S3 Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and a user profile 'siva1n82'. A banner for Amazon Glacier is visible. Below the navigation bar, the 'Amazon S3' section is active, showing a search bar and buttons for 'Create bucket', 'Delete bucket', and 'Empty bucket'. A summary shows 7 Buckets, 0 Public, and 5 Regions. A table lists the buckets with columns for Bucket name, Access, Region, and Date created.

Bucket name	Access	Region	Date created
elasticbeanstalk-ap-south-1-297111308396	Not public *	Asia Pacific (Mumbai)	Dec 20, 2017 5:48:27 PM GMT+0530
elasticbeanstalk-us-east-1-297111308396	Not public *	US East (N. Virginia)	Jan 23, 2018 10:42:40 AM GMT+0530
elasticbeanstalk-us-east-2-297111308396	Not public *	US East (Ohio)	Dec 15, 2017 10:52:13 AM GMT+0530
elasticbeanstalk-us-west-1-297111308396	Not public *	US West (N. California)	Jan 25, 2018 7:04:06 AM GMT+0530
elasticbeanstalk-us-west-2-297111308396	Not public *	US West (Oregon)	Jan 27, 2018 6:23:50 PM GMT+0530
sansbound2	Not public *	US East (N. Virginia)	Feb 15, 2018 8:45:35 AM GMT+0530
sansboundd3.com	Not public *	Asia Pacific (Mumbai)	Feb 20, 2018 3:09:39 PM GMT+0530

* Objects might still be publicly accessible due to object ACLs. [Learn more](#)

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click “IAM” service



The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a 'Services' dropdown menu, and a 'Resource Groups' dropdown. The main content area displays a grid of AWS services. The 'IAM' service is highlighted in yellow under the 'Security, Identity & Compliance' category. The left sidebar shows a 'History' section with links to EC2, Relational Database Service, DynamoDB, VPC, Console Home, and Billing. The bottom of the console features a footer with 'Feedback', 'English (US)', and copyright information.

EC2 Management Console

Find a service by name or feature (for example, EC2, S3 or VM, storage).

Group A-Z

Database

- Relational Database Service
- DynamoDB
- ElastiCache
- Amazon Redshift

Migration

- AWS Migration Hub
- Application Discovery Service
- Database Migration Service
- Server Migration Service
- Snowball

Networking & Content Delivery

- VPC
- CloudFront
- Route 53
- API Gateway
- Direct Connect

Media Services

- Elastic Transcoder
- Kinesis Video Streams
- MediaConvert
- MediaLive
- MediaPackage
- MediaStore
- MediaTailor

Security, Identity & Compliance

- IAM**
- Cognito
- GuardDuty
- Inspector
- Amazon Macie
- AWS Single Sign-On
- Certificate Manager
- CloudHSM
- Directory Service
- WAF & Shield
- Artifact

Mobile Services

- Mobile Hub
- AWS AppSync
- Device Farm
- Mobile Analytics

Business Productivity

- Alexa for Business
- Amazon Chime
- WorkDocs
- WorkMail

Desktop & App Streaming

- WorkSpaces
- AppStream 2.0

Internet Of Things

- AWS IoT
- IoT Analytics
- IoT Device Management
- Amazon FreeRTOS
- AWS Greengrass

Game Development

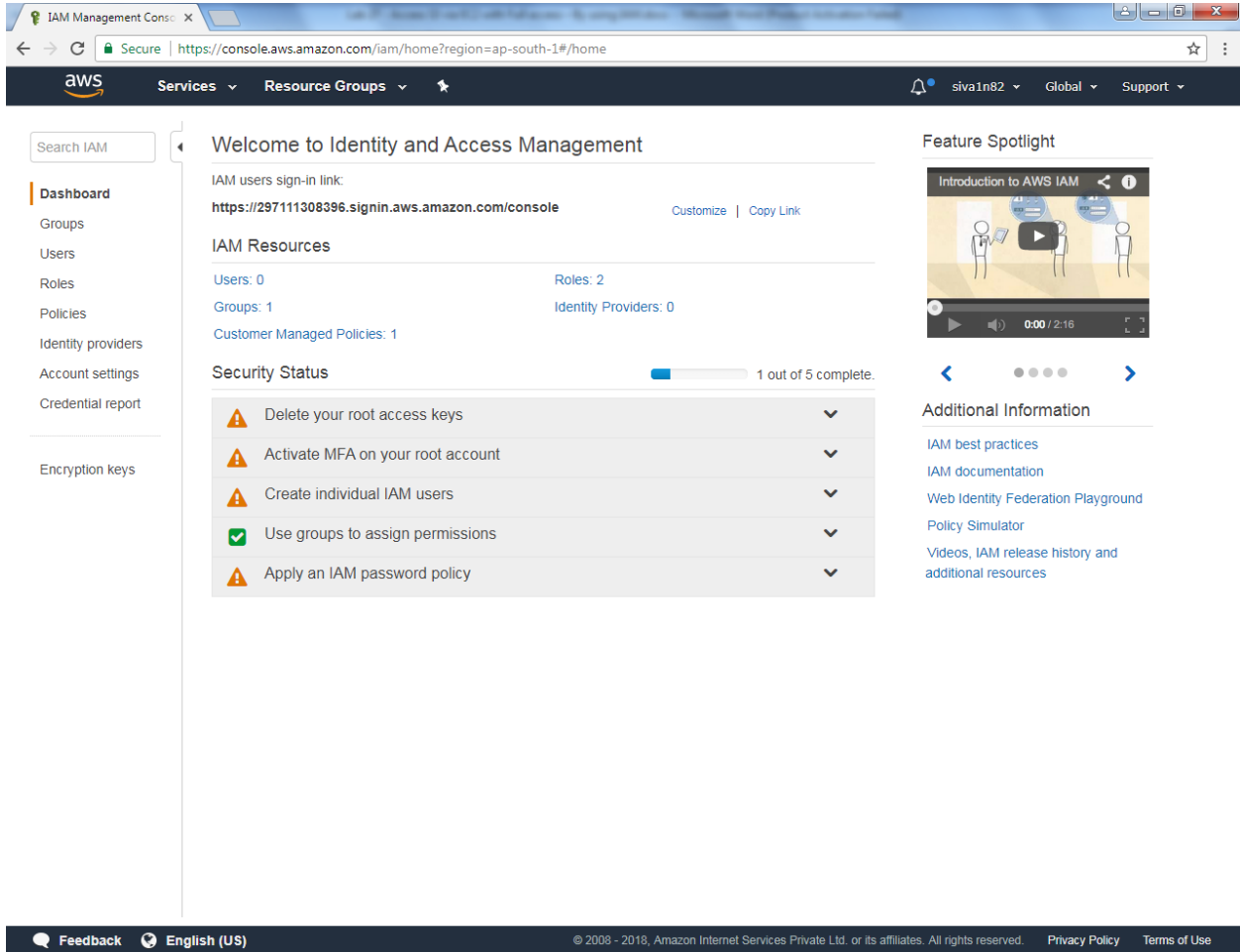
- Amazon GameLift

close

Feedback English (US)

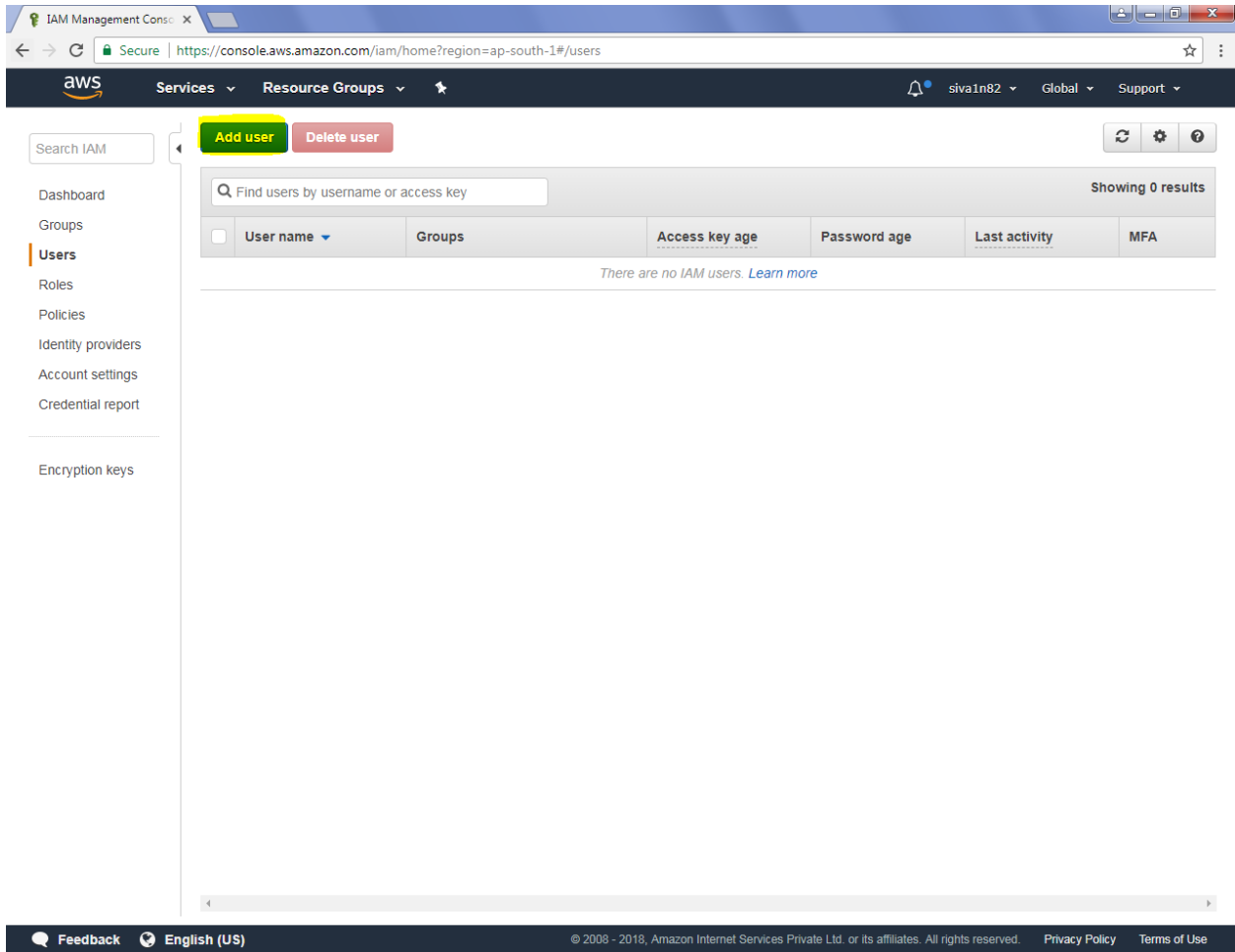
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click “Users”.



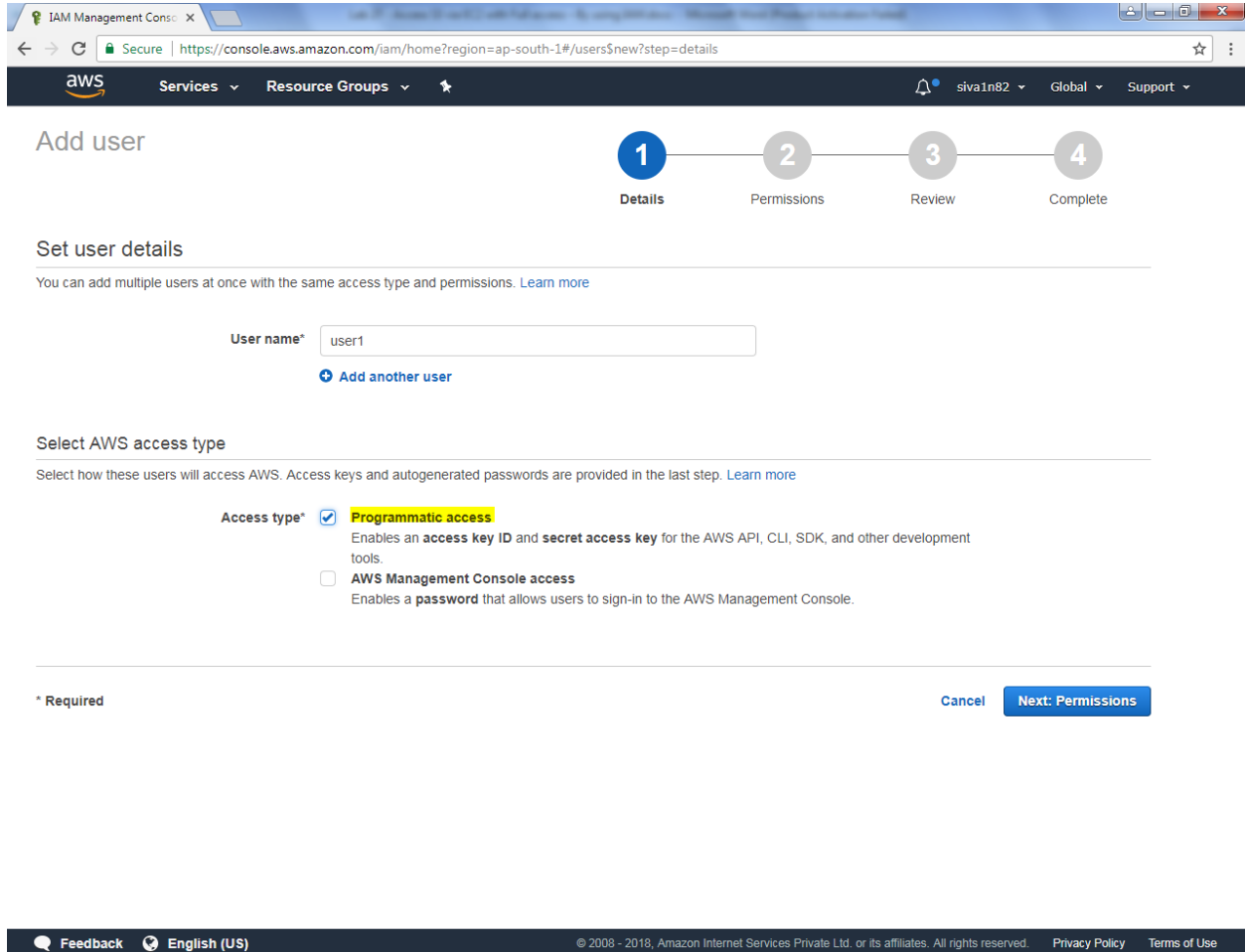
The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The left sidebar contains a 'Search IAM' box and a list of navigation items: Dashboard, Groups, Users, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area is titled 'Welcome to Identity and Access Management' and includes an IAM users sign-in link, IAM resource counts (Users: 0, Groups: 1, Roles: 2, Identity Providers: 0), and a 'Security Status' section with a progress bar indicating '1 out of 5 complete'. The security status items are: Delete your root access keys, Activate MFA on your root account, Create individual IAM users, Use groups to assign permissions, and Apply an IAM password policy. The right sidebar features a 'Feature Spotlight' video titled 'Introduction to AWS IAM' and an 'Additional Information' section with links to IAM best practices, IAM documentation, Web Identity Federation Playground, Policy Simulator, and Videos, IAM release history and additional resources.

Click “Add user”.



The screenshot shows the AWS IAM Management Console interface. The browser address bar displays the URL `https://console.aws.amazon.com/iam/home?region=ap-south-1#/users`. The AWS logo and navigation menu are visible at the top. On the left sidebar, the 'Users' link is highlighted. The main content area features a search bar labeled 'Find users by username or access key' and a table with columns: 'User name', 'Groups', 'Access key age', 'Password age', 'Last activity', and 'MFA'. The table is currently empty, with a message stating 'There are no IAM users. [Learn more](#)'. The 'Add user' button is highlighted in yellow, and the 'Delete user' button is in red. The footer contains links for 'Feedback', 'English (US)', and copyright information.

Type user name and select the access type as programmatic access.



IAM Management Console

Secure | [https://console.aws.amazon.com/iam/home?region=ap-south-1#/users\\$new?step=details](https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=details)

aws Services Resource Groups

siva1n82 Global Support

Add user

- 1 Details
- 2 Permissions
- 3 Review
- 4 Complete

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[Add another user](#)

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

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

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

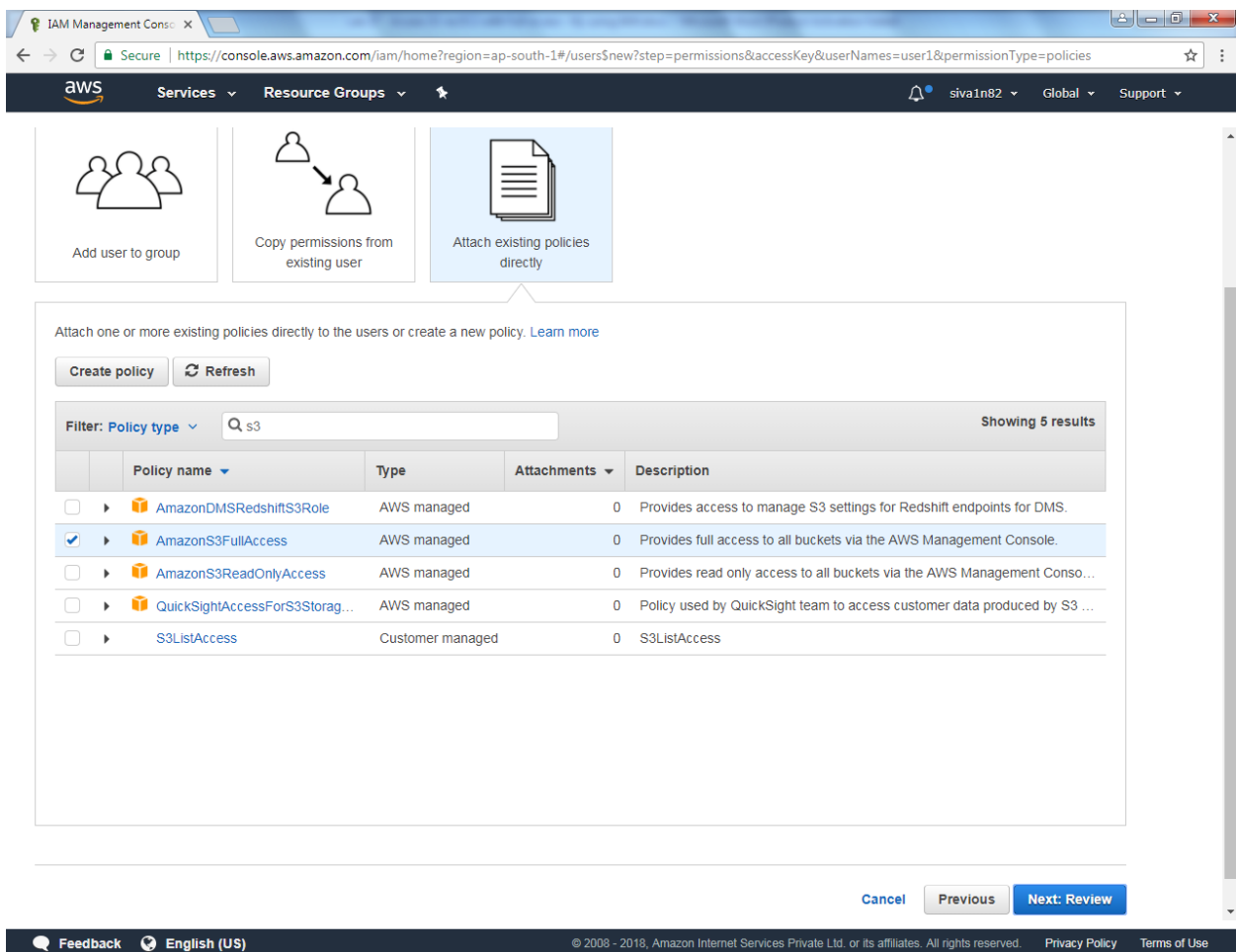
* Required

[Cancel](#) [Next: Permissions](#)

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click "Next".

Select attach existing policies directly and provide **AmazonS3 Full access**.



The screenshot shows the AWS IAM Management Console interface. At the top, there are three main actions: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly'. The 'Attach existing policies directly' option is selected and highlighted with a blue border. Below this, a section titled 'Attach one or more existing policies directly to the users or create a new policy. [Learn more](#)' contains a 'Create policy' button and a 'Refresh' button. A search filter is set to 'Policy type' with a search box containing 's3'. Below the search bar, a table displays the search results. The table has columns for 'Policy name', 'Type', 'Attachments', and 'Description'. The 'AmazonS3FullAccess' policy is selected, indicated by a blue checkmark in the first column. The table shows 5 results.

	Policy name	Type	Attachments	Description
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	AWS managed	0	Provides access to manage S3 settings for Redshift endpoints for DMS.
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	0	Provides full access to all buckets via the AWS Management Console.
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	AWS managed	0	Provides read only access to all buckets via the AWS Management Conso...
<input type="checkbox"/>	QuickSightAccessForS3Storag...	AWS managed	0	Policy used by QuickSight team to access customer data produced by S3 ...
<input type="checkbox"/>	S3ListAccess	Customer managed	0	S3ListAccess

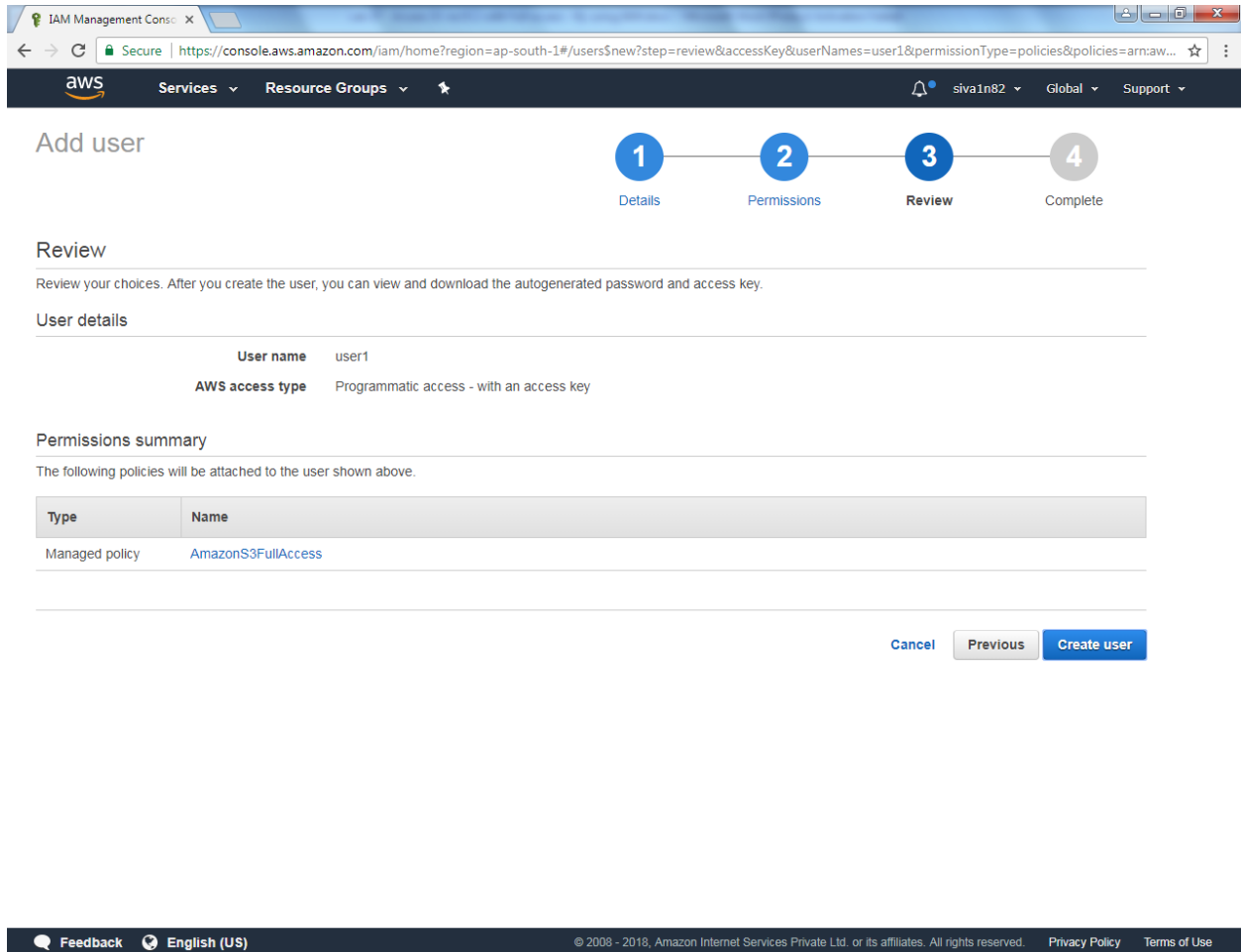
Showing 5 results

Cancel Previous **Next: Review**

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Click "Next".

Click “Create user”.



Add user

1 Details 2 Permissions 3 **Review** 4 Complete

Review

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

User details

User name	user1
AWS access type	Programmatic access - with an access key

Permissions summary

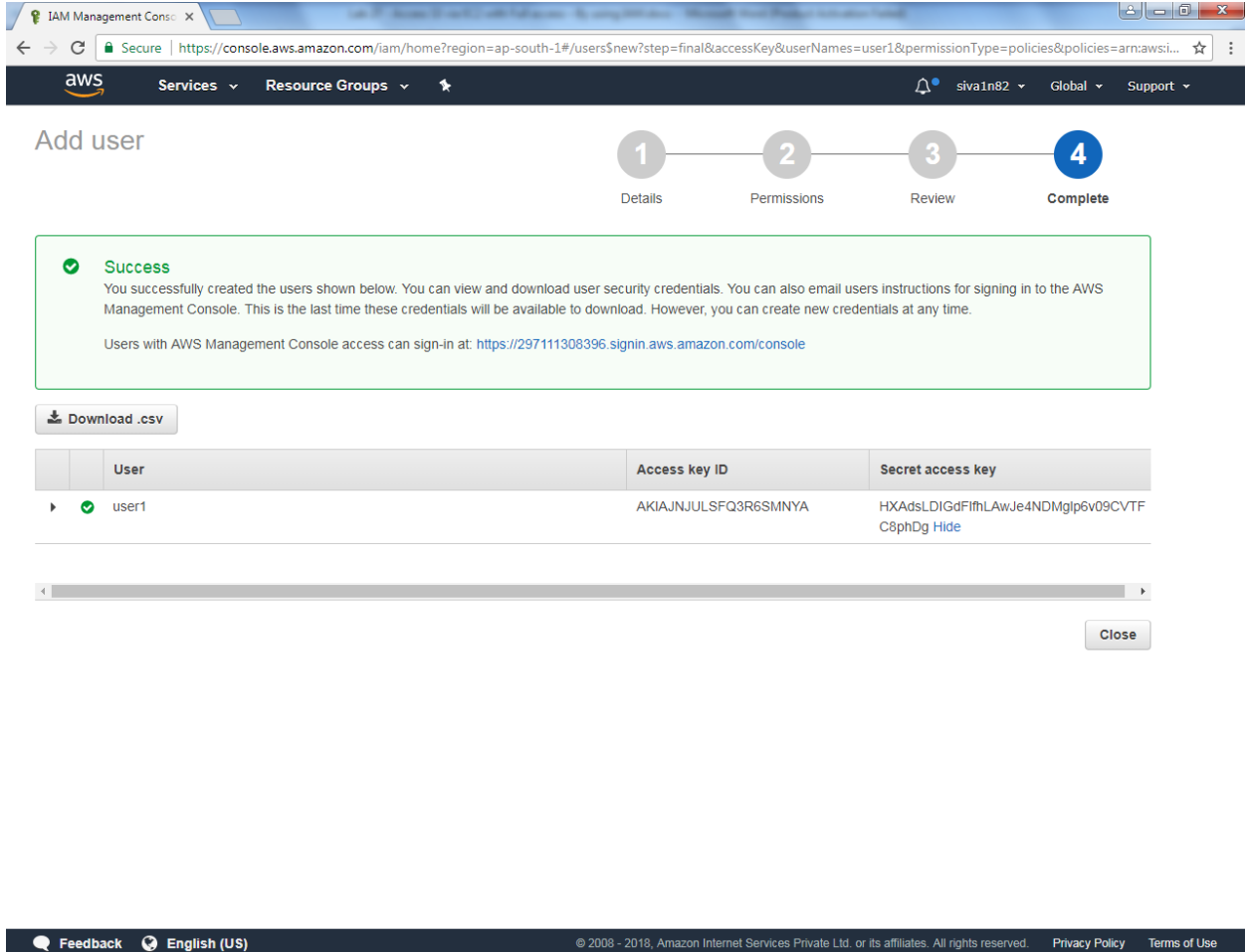
The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonS3FullAccess

[Cancel](#) [Previous](#) [Create user](#)

[Feedback](#) [English \(US\)](#) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

You can able to view the access key.



IAM Management Console

Secure | [https://console.aws.amazon.com/iam/home?region=ap-south-1#/users\\$new?step=final&accessKey&userNames=user1&permissionType=policies&policies=arn:aws:iam::ap-south-1:policy/AWSIAMReadOnlyAccess](https://console.aws.amazon.com/iam/home?region=ap-south-1#/users$new?step=final&accessKey&userNames=user1&permissionType=policies&policies=arn:aws:iam::ap-south-1:policy/AWSIAMReadOnlyAccess)

aws Services Resource Groups

siva1n82 Global Support

Add user

- 1 Details
- 2 Permissions
- 3 Review
- 4 Complete

✓ **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://297111308396.signin.aws.amazon.com/console>

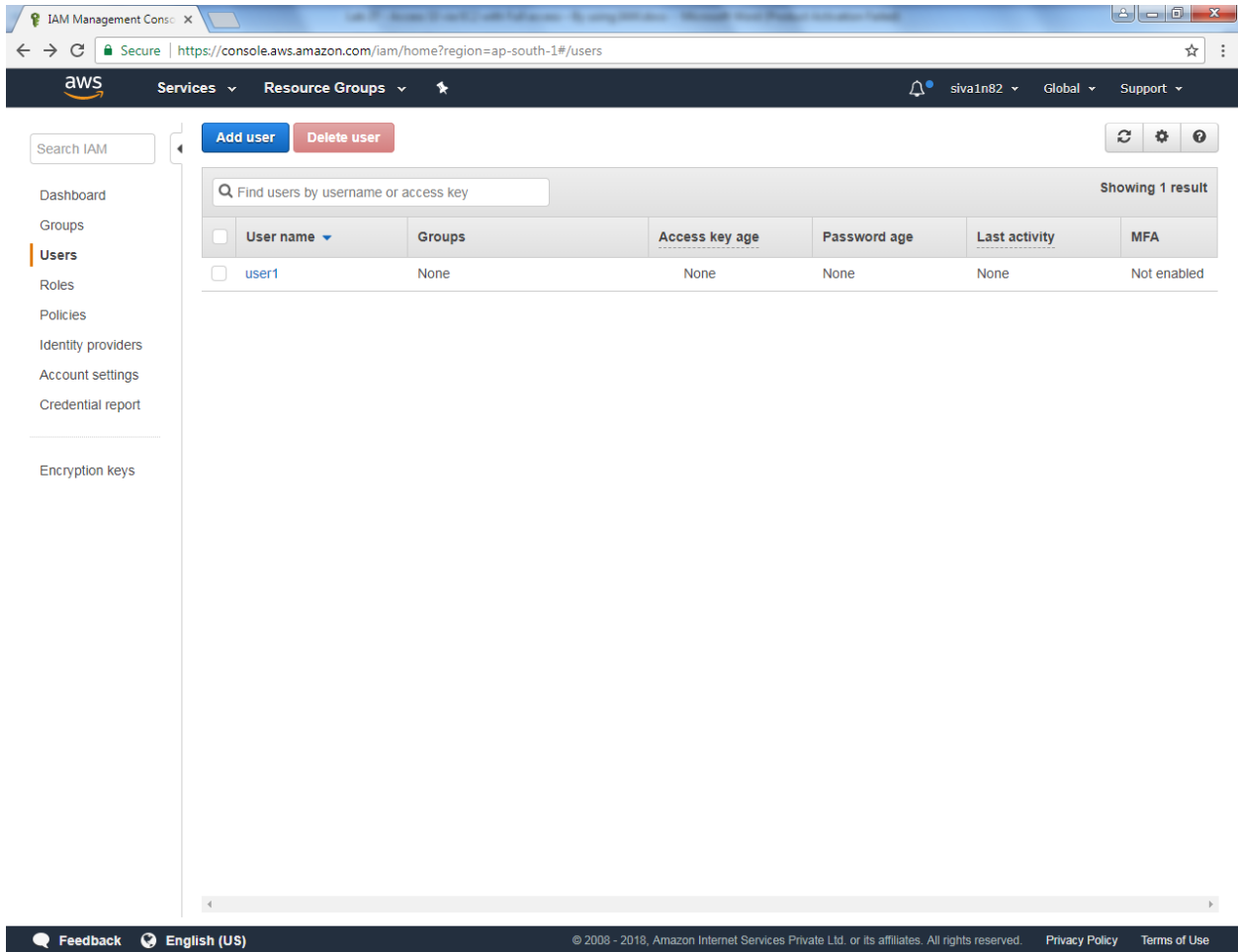
Download .csv

	User	Access key ID	Secret access key
▶ ✓	user1	AKIAJNJULSFQ3R6SMNYA	HXAdsLDIGdFifhLawJe4NDMglp6v09CVTF C8phDg Hide

Close

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

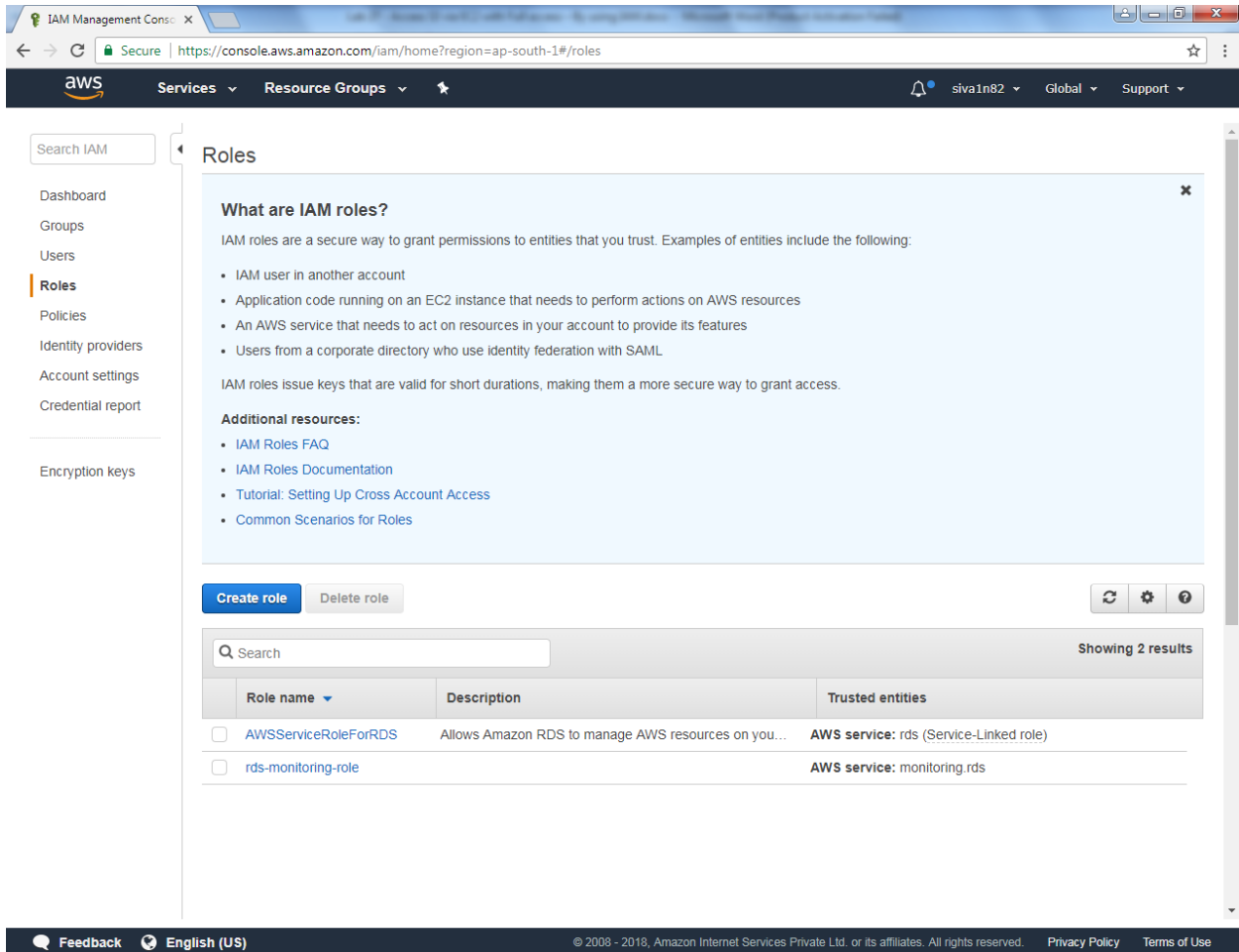
You can able to view the user.



The screenshot shows the AWS IAM console interface. The left sidebar contains navigation links: Dashboard, Groups, Users (selected), Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has a search bar and a table of users. The table has columns: User name, Groups, Access key age, Password age, Last activity, and MFA. One user, 'user1', is listed with 'None' for Groups, Access key age, Password age, and Last activity, and 'Not enabled' for MFA. The bottom of the page includes a footer with 'Feedback', 'English (US)', and copyright information.

<input type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity	MFA
<input type="checkbox"/>	user1	None	None	None	None	Not enabled

Click Roles and click create role.



The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information. The left sidebar contains a search bar and a list of navigation links: Dashboard, Groups, Users, Roles (highlighted), Policies, Identity providers, Account settings, Credential report, and Encryption keys.

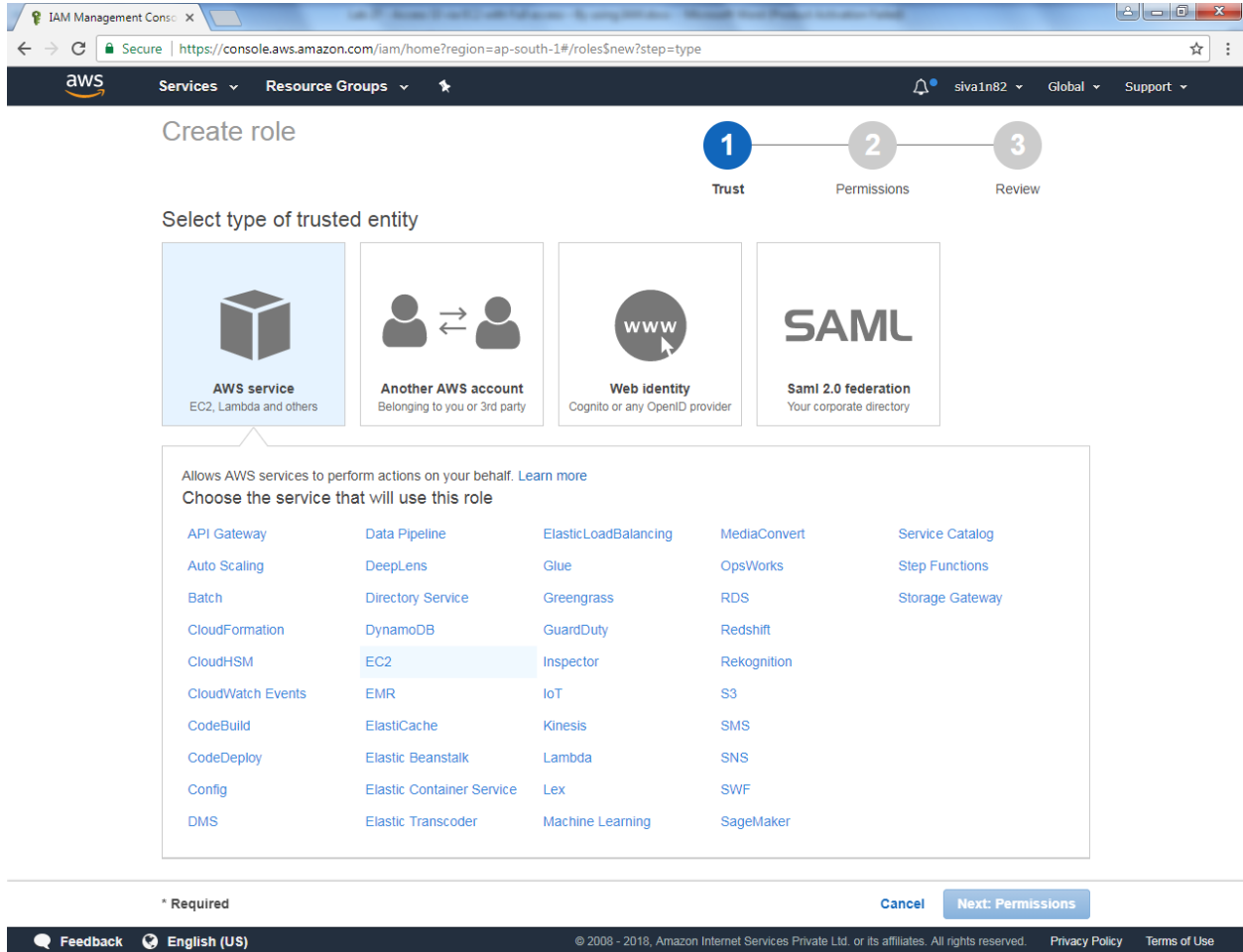
The main content area is titled 'Roles'. It features a light blue informational box titled 'What are IAM roles?' which explains that IAM roles are a secure way to grant permissions to entities. It lists examples: IAM user in another account, application code on an EC2 instance, an AWS service needing access, and users from a corporate directory. It also mentions that IAM roles issue keys for short durations. Below this, 'Additional resources' are listed: IAM Roles FAQ, IAM Roles Documentation, Tutorial: Setting Up Cross Account Access, and Common Scenarios for Roles.

Below the informational box are 'Create role' and 'Delete role' buttons. A search bar is present with the text 'Showing 2 results'. Below the search bar is a table of roles:

Role name	Description	Trusted entities
<input type="checkbox"/> AWSServiceRoleForRDS	Allows Amazon RDS to manage AWS resources on you...	AWS service: rds (Service-Linked role)
<input type="checkbox"/> rds-monitoring-role		AWS service: monitoring.rds

The footer of the console includes a 'Feedback' link, 'English (US)' language selection, and copyright information: © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. It also links to 'Privacy Policy' and 'Terms of Use'.

Click “EC2” Service



The screenshot shows the AWS IAM console 'Create role' page. The browser address bar indicates the URL: [https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles\\$new?step=type](https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles$new?step=type). The page title is 'Create role'. A progress bar at the top shows three steps: 1. Trust (selected), 2. Permissions, and 3. Review. Below the progress bar, the section 'Select type of trusted entity' is displayed. It contains four cards: 'AWS service' (EC2, Lambda and others), 'Another AWS account' (Belonging to you or 3rd party), 'Web identity' (Cognito or any OpenID provider), and 'SAML' (Saml 2.0 federation, Your corporate directory). The 'AWS service' card is selected, and a list of AWS services is shown below it. The services are arranged in a grid, and 'EC2' is highlighted. At the bottom of the page, there are buttons for 'Cancel' and 'Next: Permissions'. The footer includes a feedback link, language selection (English (US)), and copyright information (© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use).

Create role

1 Trust 2 Permissions 3 Review

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML
Saml 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)
Choose the service that will use this role

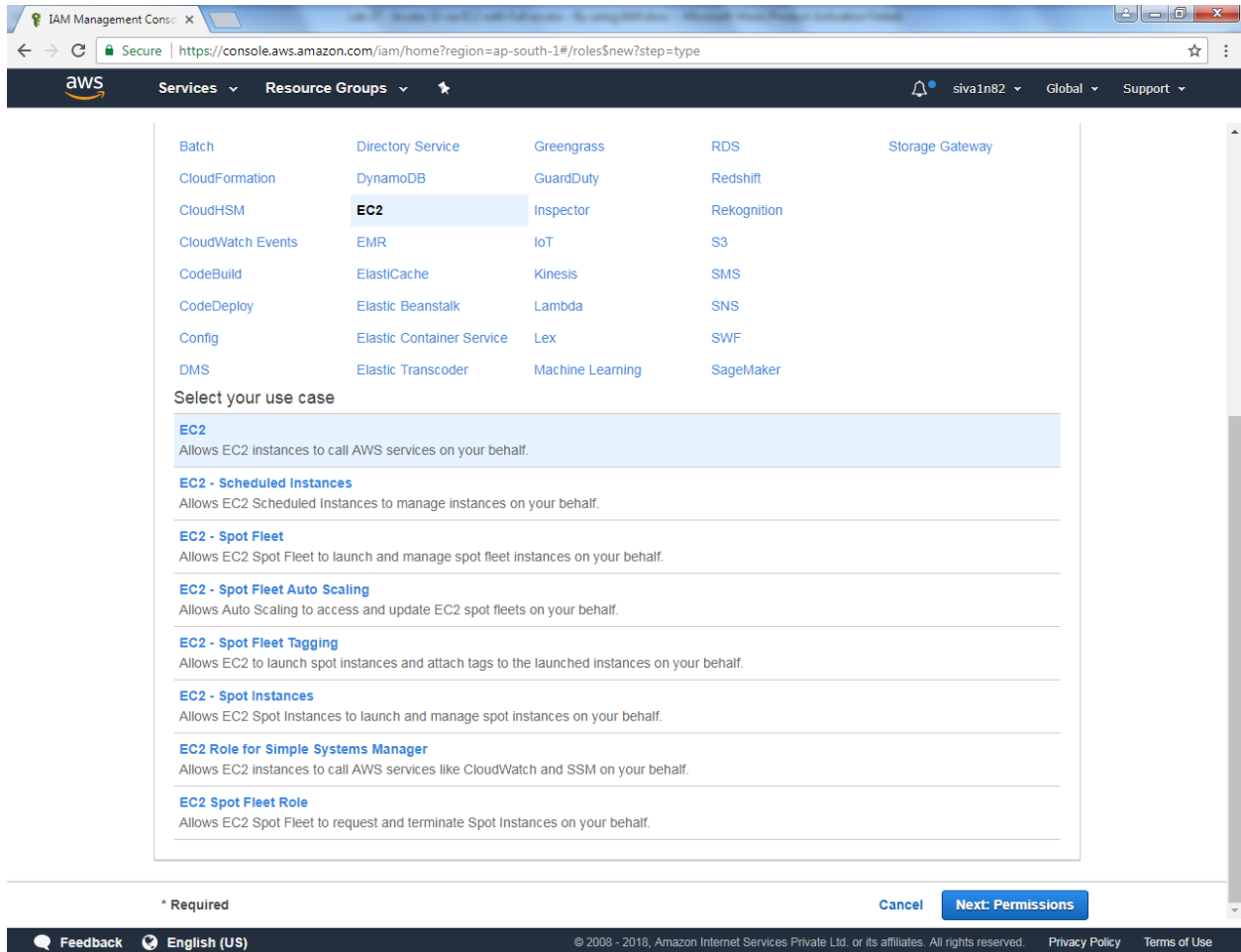
API Gateway	Data Pipeline	ElasticLoadBalancing	MediaConvert	Service Catalog
Auto Scaling	DeepLens	Glue	OpsWorks	Step Functions
Batch	Directory Service	Greengrass	RDS	Storage Gateway
CloudFormation	DynamoDB	GuardDuty	Redshift	
CloudHSM	EC2	Inspector	Rekognition	
CloudWatch Events	EMR	IoT	S3	
CodeBuild	ElastiCache	Kinesis	SMS	
CodeDeploy	Elastic Beanstalk	Lambda	SNS	
Config	Elastic Container Service	Lex	SWF	
DMS	Elastic Transcoder	Machine Learning	SageMaker	

* Required

[Cancel](#) [Next: Permissions](#)

[Feedback](#) [English \(US\)](#) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Click “EC2” service.



The screenshot shows the AWS IAM console interface. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and a user profile 'siva1n82'. Below this is a grid of service categories. 'EC2' is highlighted in the second column. Below the grid, the 'Select your use case' section is expanded, showing a list of roles with their descriptions. At the bottom, there are 'Cancel' and 'Next: Permissions' buttons.

Service Category	Service Name
Batch	Directory Service
CloudFormation	DynamoDB
CloudHSM	EC2
CloudWatch Events	EMR
CodeBuild	ElastiCache
CodeDeploy	Elastic Beanstalk
Config	Elastic Container Service
DMS	Elastic Transcoder
Greengrass	GuardDuty
Inspector	IoT
Kinesis	Lambda
Lex	Machine Learning
RDS	Redshift
Rekognition	S3
SMS	SNS
SWF	SageMaker
Storage Gateway	

Select your use case

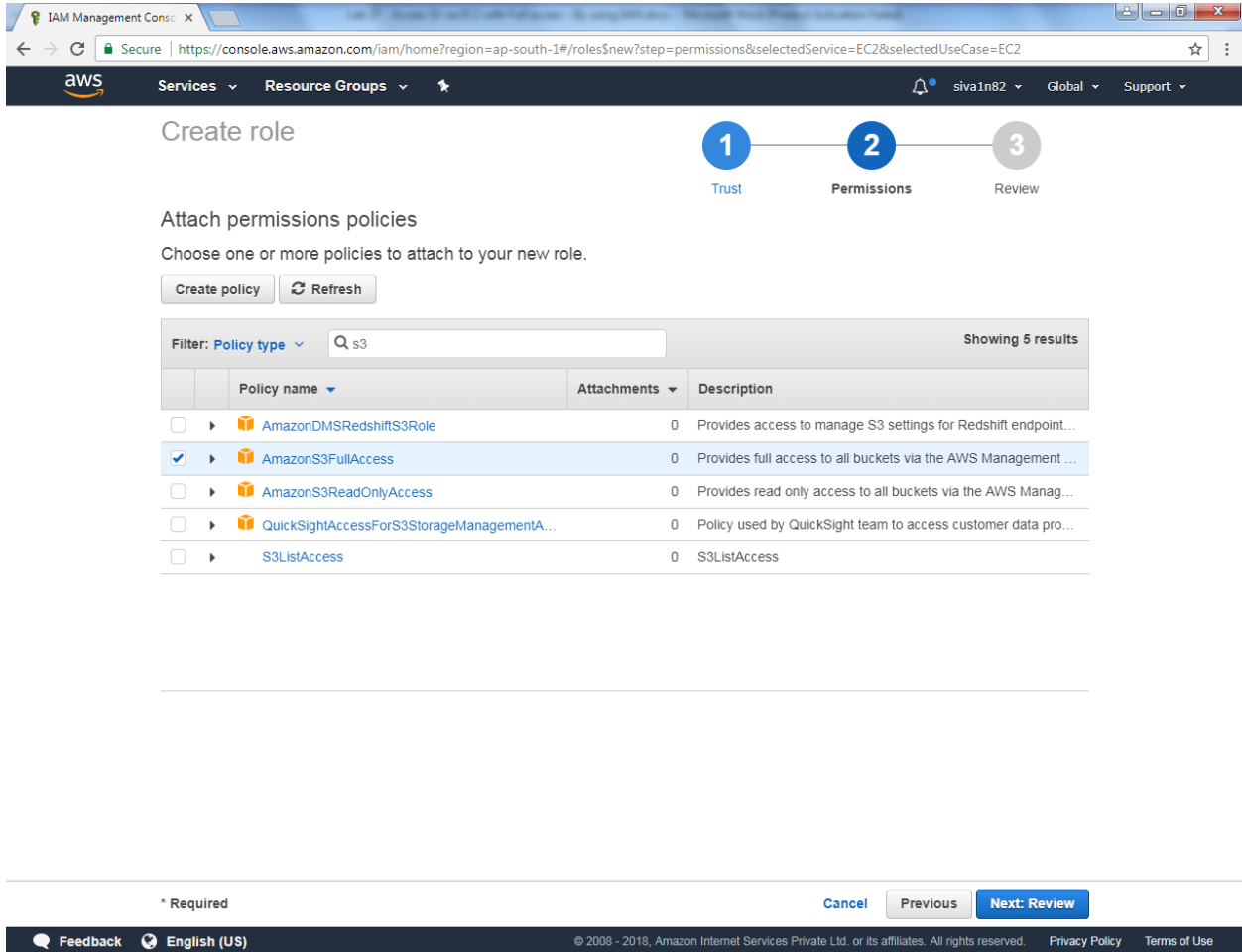
- EC2**
Allows EC2 instances to call AWS services on your behalf.
- EC2 - Scheduled Instances**
Allows EC2 Scheduled Instances to manage instances on your behalf.
- EC2 - Spot Fleet**
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging**
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- EC2 - Spot Instances**
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- EC2 Role for Simple Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and SSM on your behalf.
- EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

* Required

Cancel Next: Permissions

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Select “AmazonS3 Full access”



Create role

1 Trust 2 **Permissions** 3 Review

Attach permissions policies

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

Create policy Refresh

Filter: Policy type Q s3 Showing 5 results

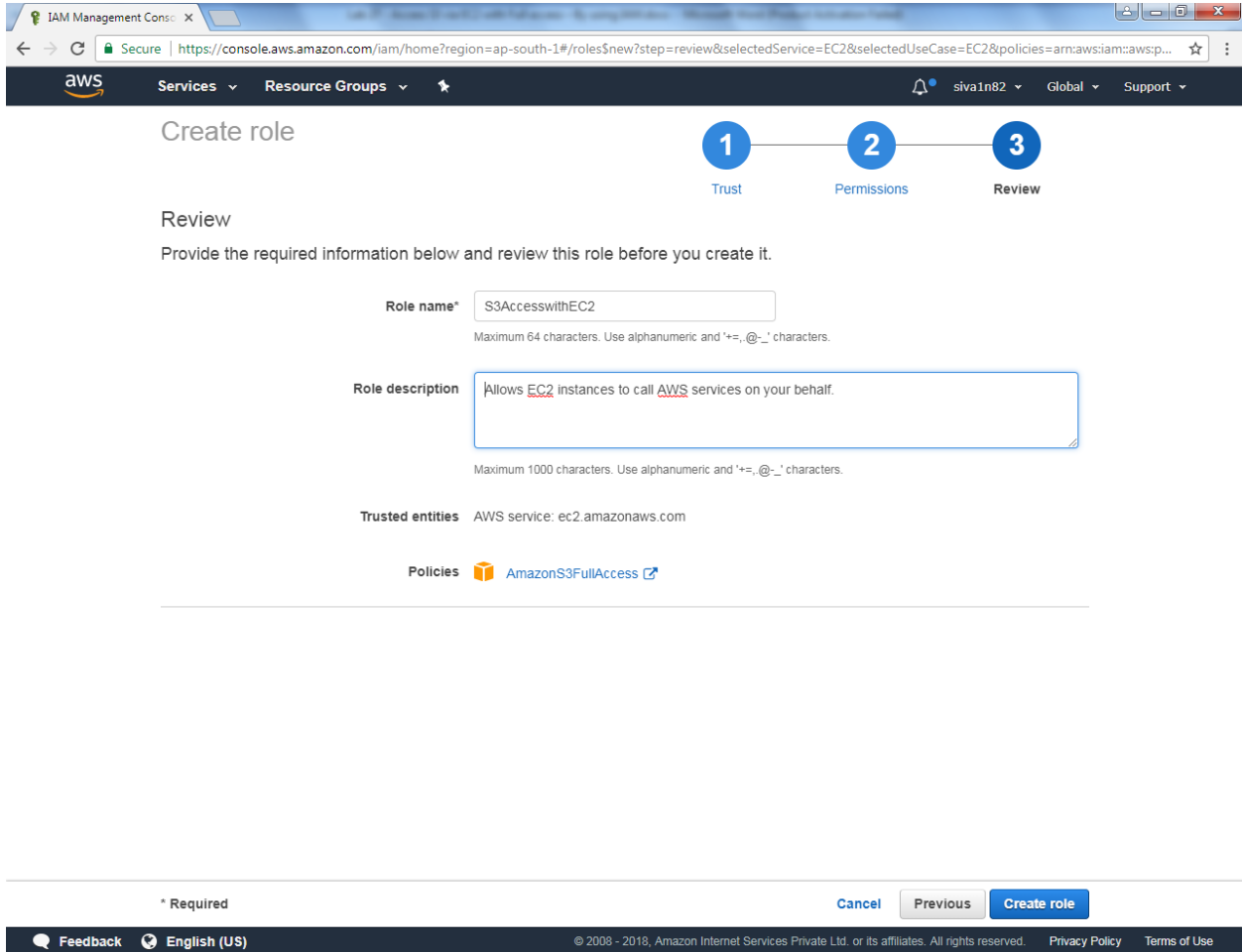
	Policy name	Attachments	Description
<input type="checkbox"/>	AmazonDMSRedshiftS3Role	0	Provides access to manage S3 settings for Redshift endpoint...
<input checked="" type="checkbox"/>	AmazonS3FullAccess	0	Provides full access to all buckets via the AWS Management ...
<input type="checkbox"/>	AmazonS3ReadOnlyAccess	0	Provides read only access to all buckets via the AWS Manag...
<input type="checkbox"/>	QuickSightAccessForS3StorageManagementA...	0	Policy used by QuickSight team to access customer data pro...
<input type="checkbox"/>	S3ListAccess	0	S3ListAccess

* Required

Cancel Previous **Next: Review**

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type role name as “S3AccesswithEC2” and click “Create role”.



IAM Management Console

Secure | [https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles\\$new?step=review&selectedService=EC2&selectedUseCase=EC2&policies=arn:aws:iam::aws:policy...](https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles$new?step=review&selectedService=EC2&selectedUseCase=EC2&policies=arn:aws:iam::aws:policy...)

aws Services Resource Groups

siva1n82 Global Support

Create role

- 1 Trust
- 2 Permissions
- 3 Review


Review

Provide the required information below and review this role before you create it.

Role name*
Maximum 64 characters. Use alphanumeric and "+=, @, _" characters.

Role description
Maximum 1000 characters. Use alphanumeric and "+=, @, _" characters.

Trusted entities AWS service: ec2.amazonaws.com

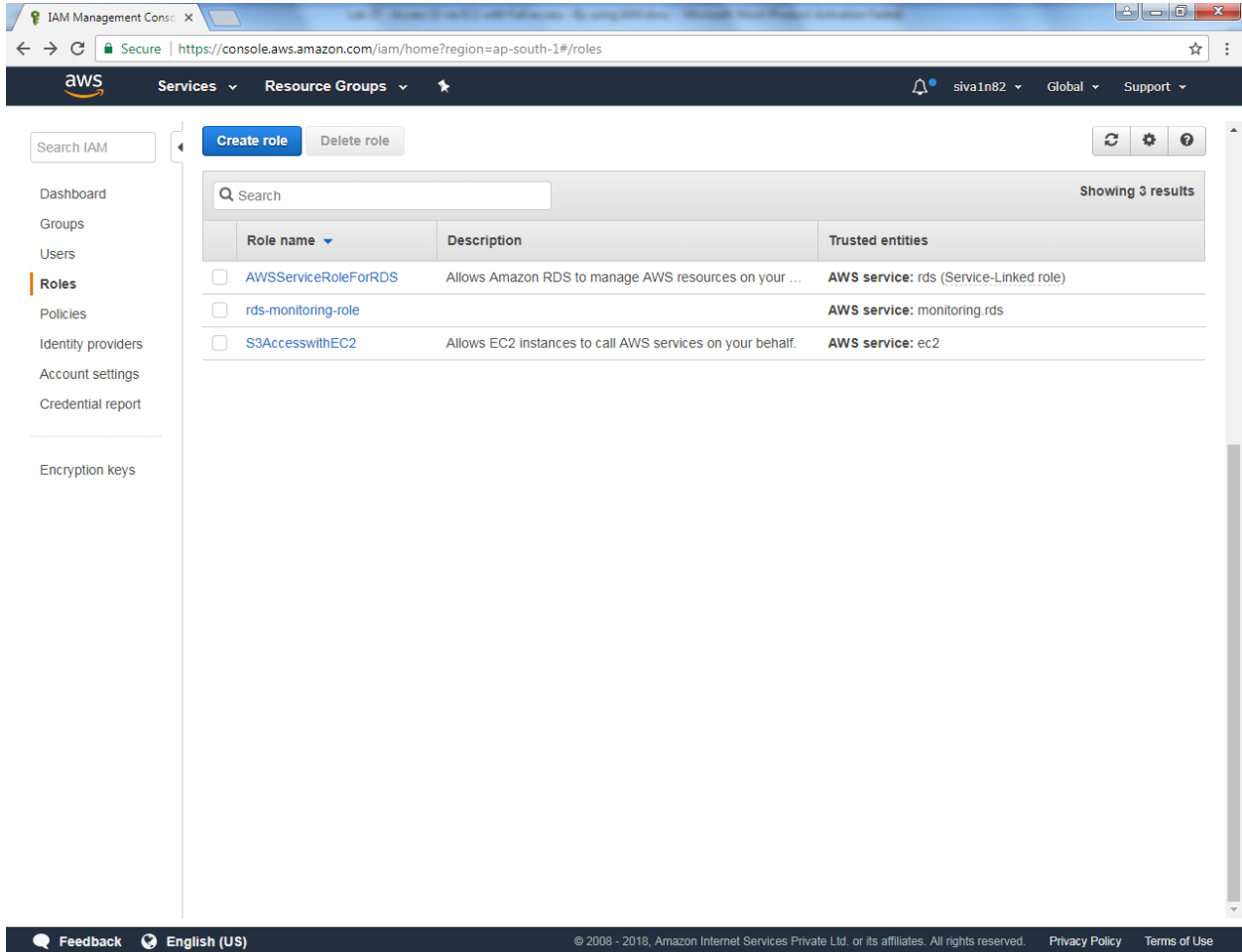
Policies  [AmazonS3FullAccess](#)

* Required

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

[Feedback](#) [English \(US\)](#) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

You can able to view the roles as below.

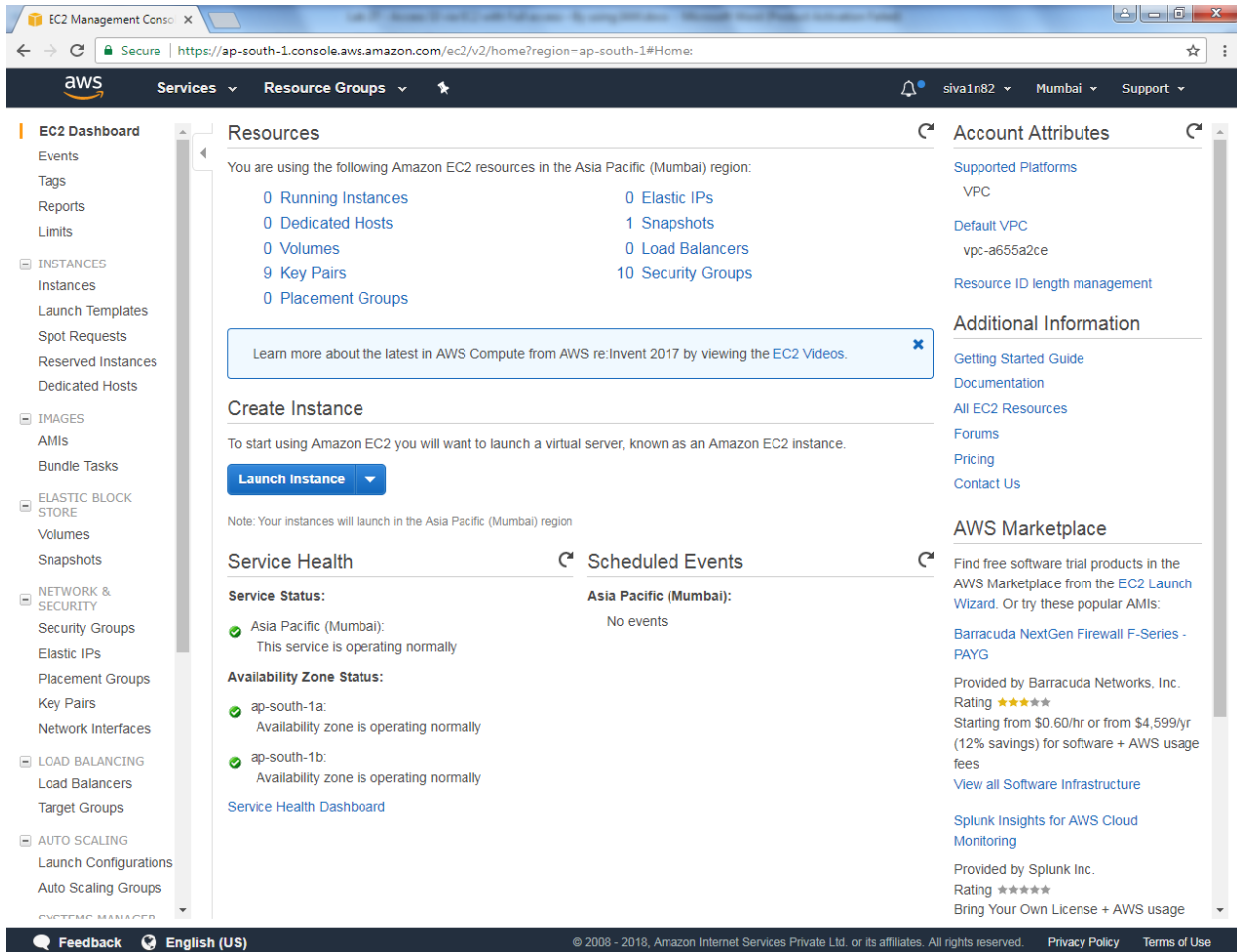


The screenshot shows the AWS IAM console interface. The browser address bar displays the URL `https://console.aws.amazon.com/iam/home?region=ap-south-1#/roles`. The console header includes the AWS logo, navigation tabs for Services and Resource Groups, and user information for 'siva1n82'. On the left sidebar, the 'Roles' menu item is selected. The main content area shows a list of roles with the following data:

Role name	Description	Trusted entities
<input type="checkbox"/> AWSServiceRoleForRDS	Allows Amazon RDS to manage AWS resources on your ...	AWS service: rds (Service-Linked role)
<input type="checkbox"/> rds-monitoring-role		AWS service: monitoring.rds
<input type="checkbox"/> S3AccesswithEC2	Allows EC2 instances to call AWS services on your behalf.	AWS service: ec2

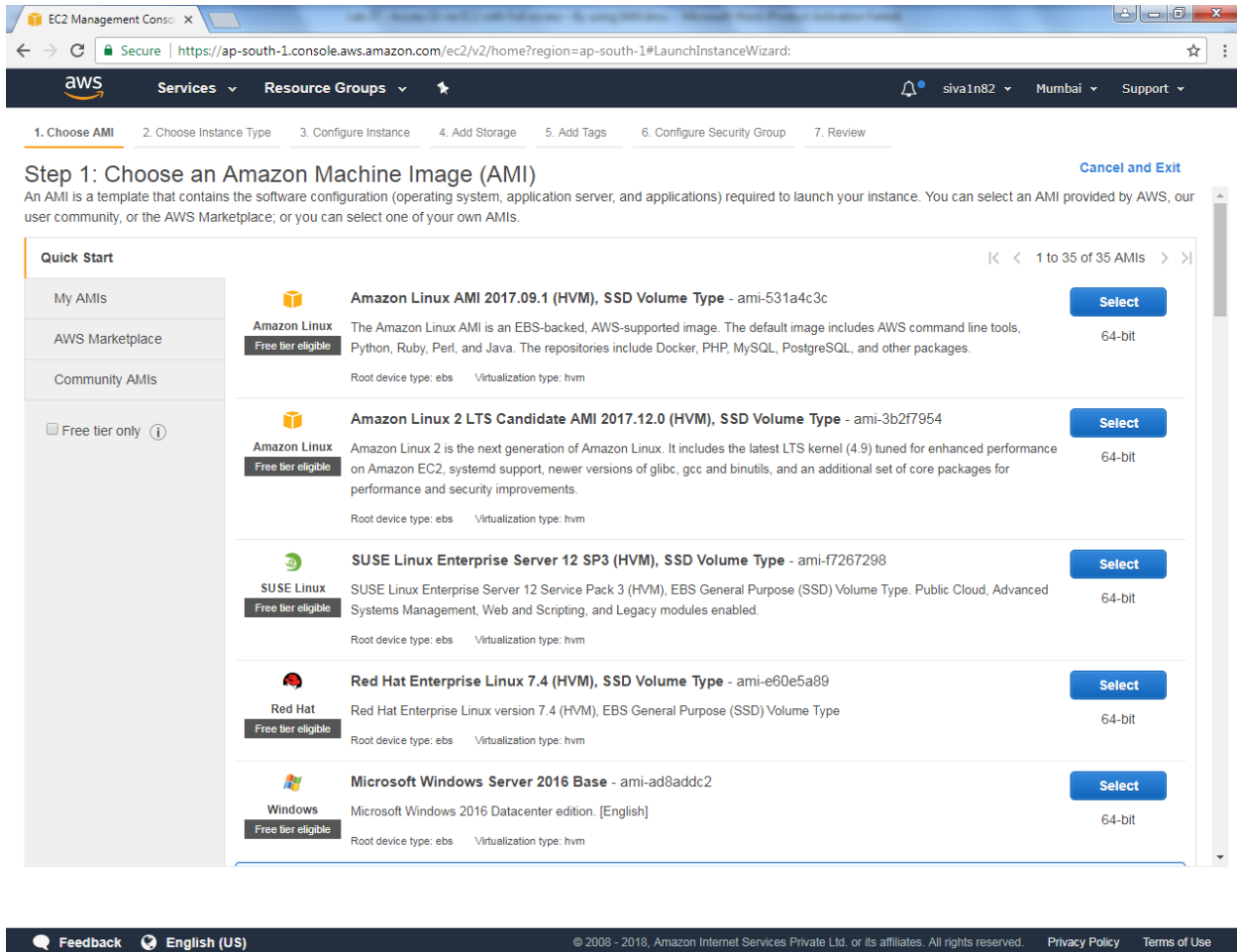
The footer of the console includes a Feedback link, the language setting 'English (US)', and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' along with links to Privacy Policy and Terms of Use.

Click “Launch instance”.



The screenshot shows the AWS Management Console for the Asia Pacific (Mumbai) region. The left sidebar contains the navigation menu with categories like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, and AUTO SCALING. The main content area is titled 'Resources' and lists various EC2 resources: 0 Running Instances, 0 Elastic IPs, 0 Dedicated Hosts, 1 Snapshots, 0 Volumes, 0 Load Balancers, 9 Key Pairs, 10 Security Groups, and 0 Placement Groups. A 'Create Instance' section is visible, featuring a 'Launch Instance' button. Below this, there are sections for 'Service Health' and 'Scheduled Events'. The 'Service Health' section shows the status of the Asia Pacific (Mumbai) region and its availability zones (ap-south-1a and ap-south-1b), all of which are operating normally. The 'Scheduled Events' section shows no events. On the right side, there are sections for 'Account Attributes' and 'Additional Information', including links to supported platforms, default VPC, resource ID length management, getting started guide, documentation, all EC2 resources, forums, pricing, contact us, and AWS Marketplace.

Select “Amazon Linux”.



The screenshot shows the AWS Management Console interface for the EC2 Launch Wizard. The browser address bar indicates the URL: <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>. The console header shows the AWS logo, navigation tabs (Services, Resource Groups), and user information (siva1n82, Mumbai, Support).

The wizard progress bar shows seven steps: 1. Choose AMI (active), 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review.






Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start

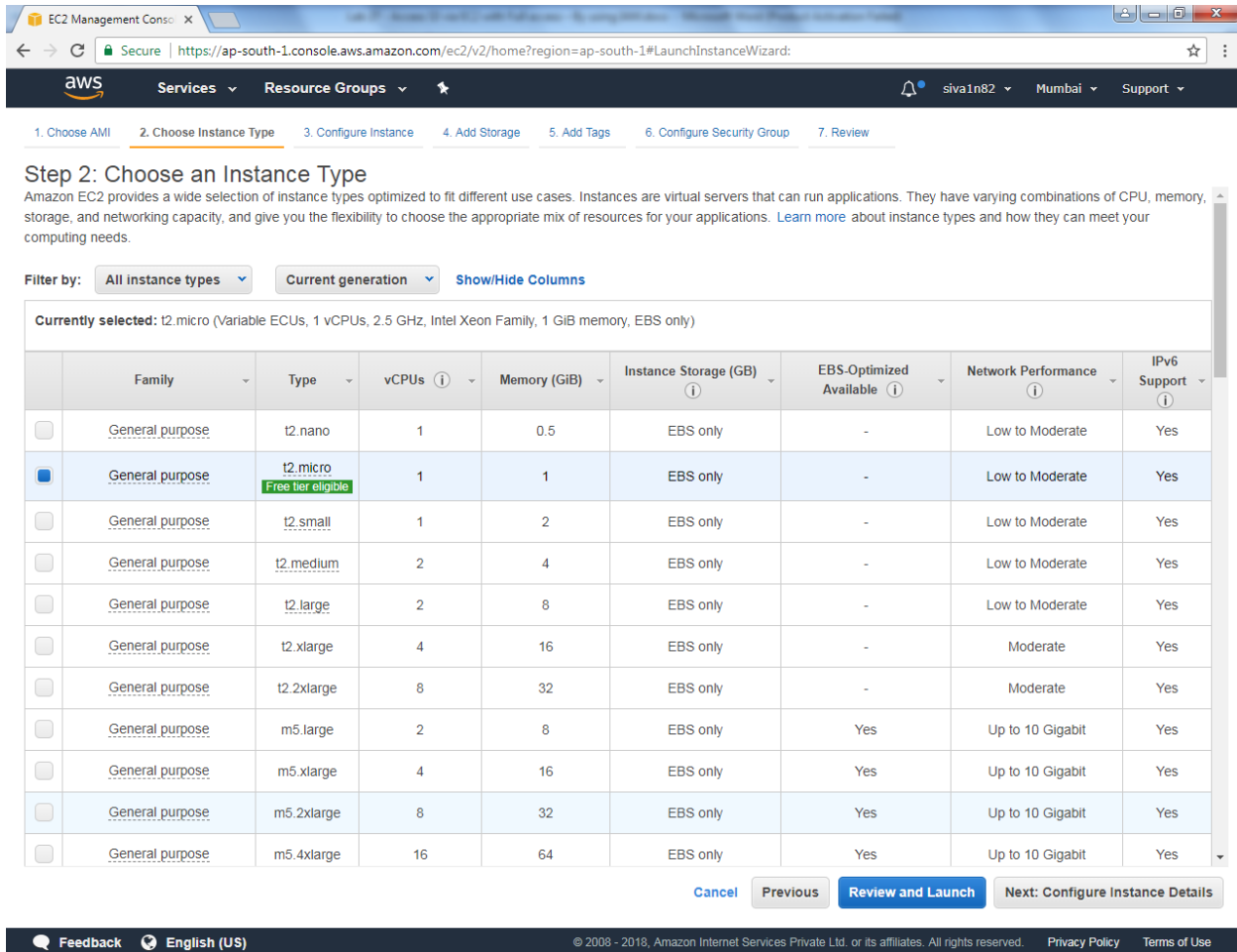
- My AMIs
- AWS Marketplace
- Community AMIs
- ☐ Free tier only ⓘ

1 to 35 of 35 AMIs

Logo	OS Name	AMI ID	Architecture	Action
	Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-531a4c3c	ami-531a4c3c	64-bit	Select
The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages. Root device type: ebs Virtualization type: hvm				
	Amazon Linux 2 LTS Candidate AMI 2017.12.0 (HVM), SSD Volume Type - ami-3b2f7954	ami-3b2f7954	64-bit	Select
Amazon Linux 2 is the next generation of Amazon Linux. It includes the latest LTS kernel (4.9) tuned for enhanced performance on Amazon EC2, systemd support, newer versions of glibc, gcc and binutils, and an additional set of core packages for performance and security improvements. Root device type: ebs Virtualization type: hvm				
	SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-f7267298	ami-f7267298	64-bit	Select
SUSE Linux Enterprise Server 12 Service Pack 3 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled. Root device type: ebs Virtualization type: hvm				
	Red Hat Enterprise Linux 7.4 (HVM), SSD Volume Type - ami-e60e5a89	ami-e60e5a89	64-bit	Select
Red Hat Enterprise Linux version 7.4 (HVM), EBS General Purpose (SSD) Volume Type Root device type: ebs Virtualization type: hvm				
	Microsoft Windows Server 2016 Base - ami-ad8addc2	ami-ad8addc2	64-bit	Select
Microsoft Windows 2016 Datacenter edition. [English] Root device type: ebs Virtualization type: hvm				

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Select “t2.micro”.



Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation [Show/Hide Columns](#)

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

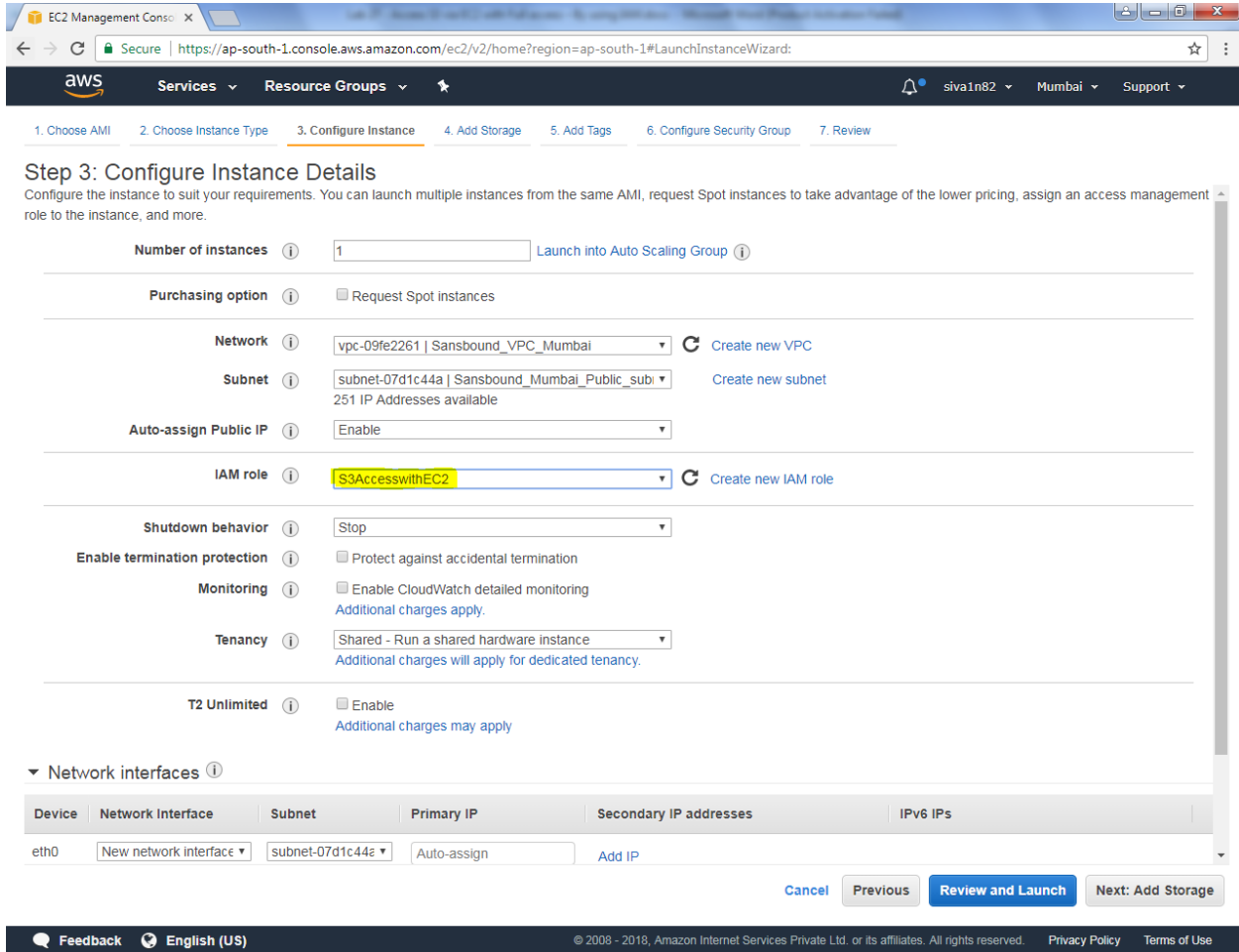
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Instance Details](#)

[Feedback](#)
[English \(US\)](#)
© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.
[Privacy Policy](#)
[Terms of Use](#)

Click “Next”.

Select VPC and Subnet, then select IAM role as “S3AccesswithEC2”.



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-09fe2261 | Sansbound_VPC_Mumbai [Create new VPC](#)

Subnet subnet-07d1c44a | Sansbound_Mumbai_Public_subi [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP Enable

IAM role S3AccesswithEC2 [Create new IAM role](#)

Shutdown behavior Stop

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

Tenancy Shared - Run a shared hardware instance
[Additional charges will apply for dedicated tenancy.](#)

T2 Unlimited ☐ Enable
[Additional charges may apply](#)

Network interfaces

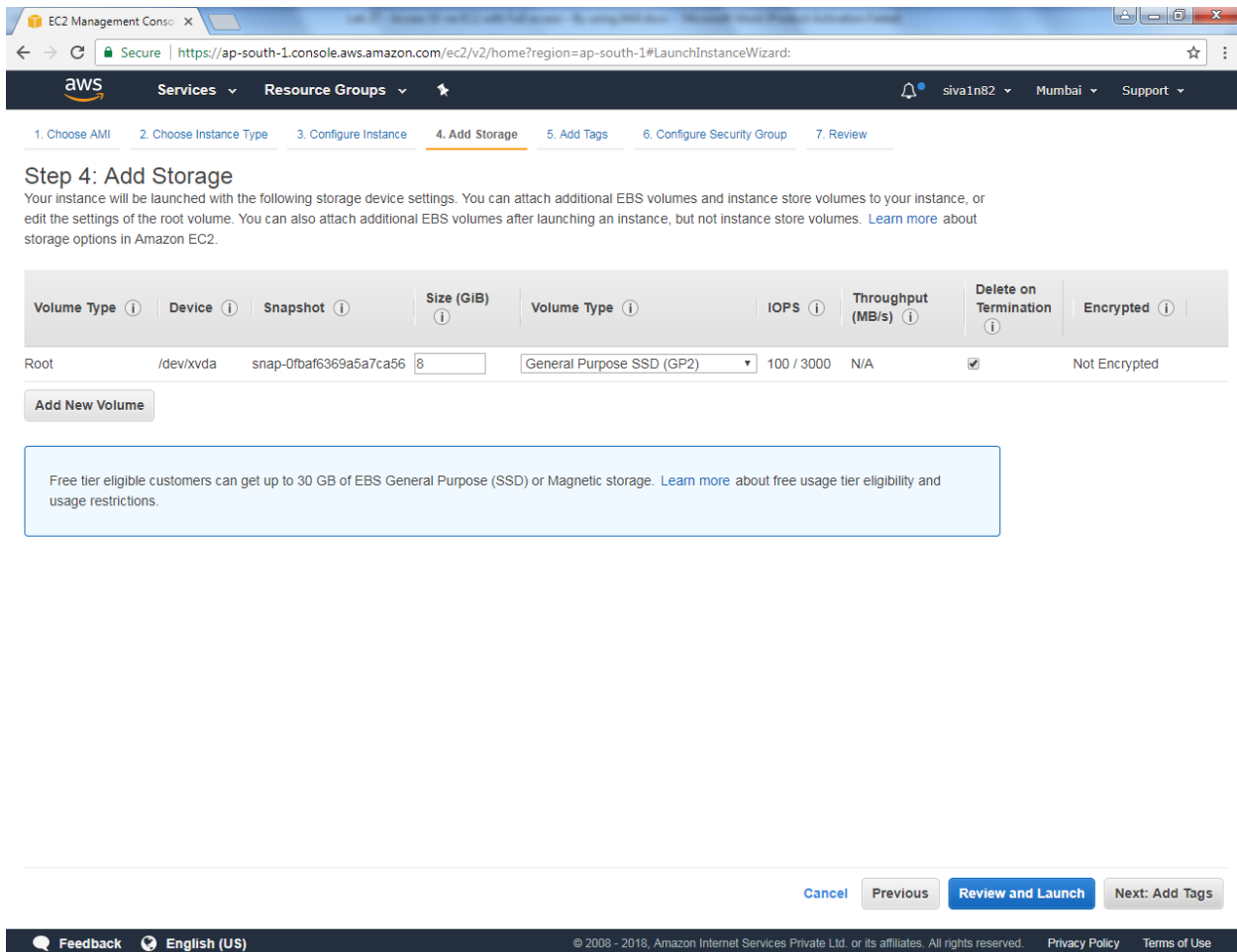
Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-07d1c44a	Auto-assign	Add IP	

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

[Feedback](#) [English \(US\)](#) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Click “Next”.

Click “Next”.



EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>

Services Resource Groups

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

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0fbaf6369a5a7ca56	8	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

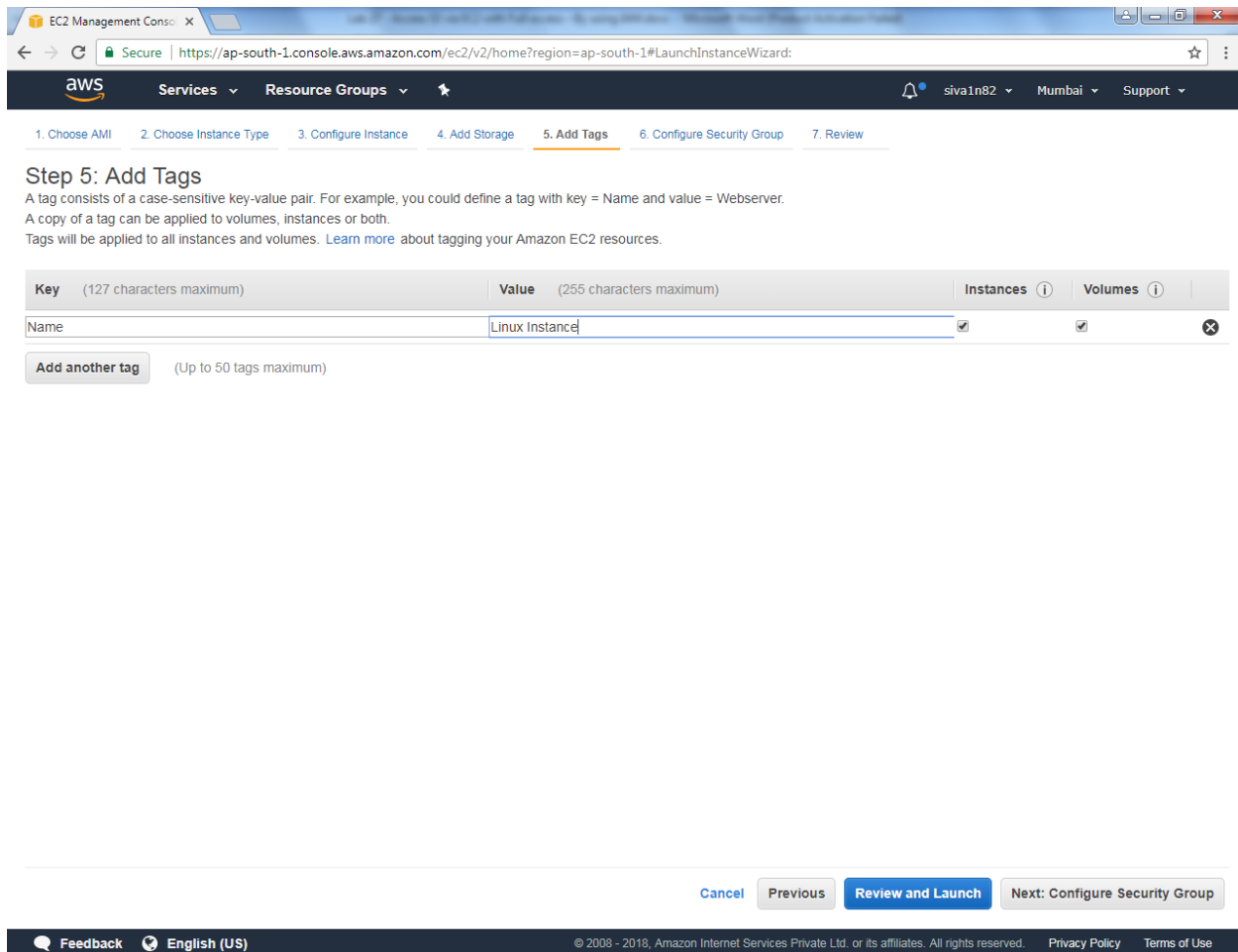
[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

Cancel Previous **Review and Launch** Next: Add Tags

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Type Name as Linux Instance.



The screenshot shows the AWS Management Console interface for the 'Launch Instance Wizard'. The browser address bar shows the URL: `https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:`. The console header includes the AWS logo, 'Services', 'Resource Groups', and user information 'siva1n82' in 'Mumbai'. A progress bar at the top indicates the current step is '5. Add Tags', with other steps being '1. Choose AMI', '2. Choose Instance Type', '3. Configure Instance', '4. Add Storage', '6. Configure Security Group', and '7. Review'.

Step 5: Add Tags
A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (127 characters maximum)	Value (255 characters maximum)	Instances <small>(i)</small>	Volumes <small>(i)</small>
Name	Linux Instance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

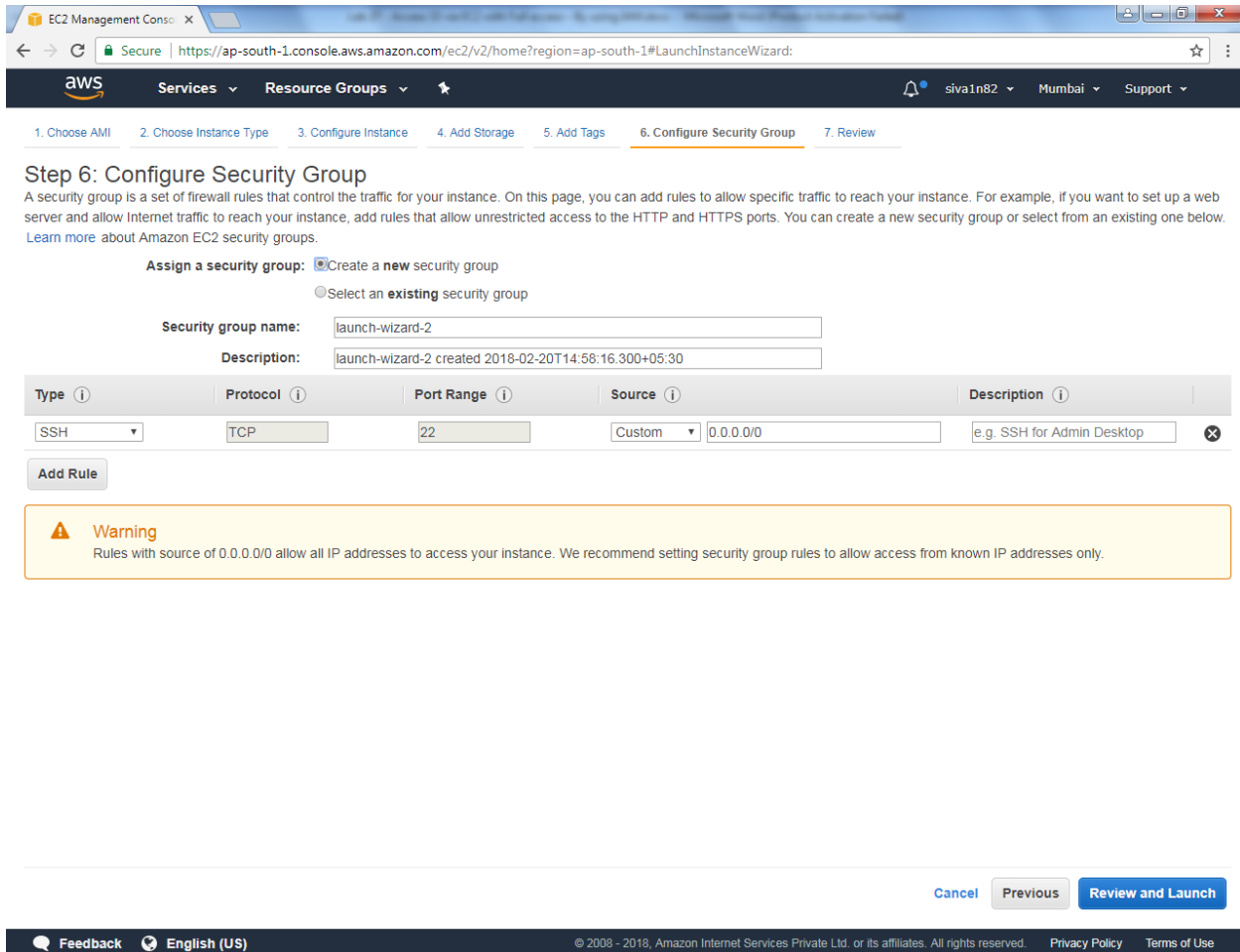
[Add another tag](#) (Up to 50 tags maximum)

At the bottom of the wizard, there are four buttons: 'Cancel', 'Previous', 'Review and Launch' (highlighted in blue), and 'Next: Configure Security Group'.

The footer contains a 'Feedback' link, 'English (US)' language selection, and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' along with 'Privacy Policy' and 'Terms of Use' links.

Click "Next".

Create a new security group for access ssh port.



The screenshot shows the AWS Management Console interface for the 'Configure Security Group' step of the EC2 Instance Wizard. The browser address bar shows the URL: <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:>. The console header includes the AWS logo, navigation tabs (Services, Resource Groups), and user information (siva1n82, Mumbai, Support).

The wizard progress bar shows seven steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group (active), and 7. Review.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group ☐ Select an existing security group

Security group name:

Description:

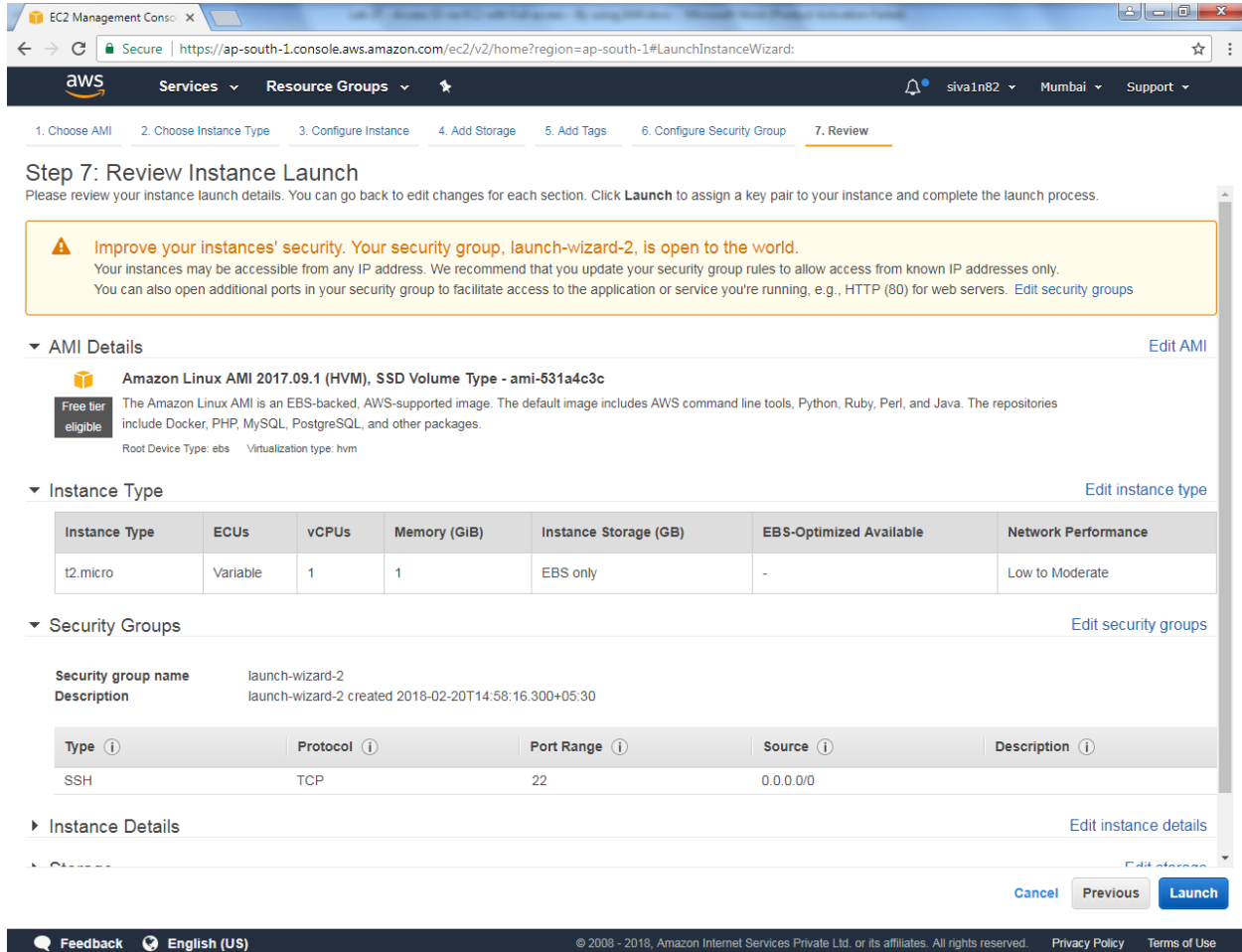
Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Feedback](#) [English \(US\)](#) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Click “Launch”.



EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:>

Services Resource Groups

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

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, launch-wizard-2, is open to the world.

Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only. You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ AMI Details [Edit AMI](#)

Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-531a4c3c

Free tier eligible The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root Device Type: ebs Virtualization type: hvm

▼ Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

▼ Security Groups [Edit security groups](#)

Security group name launch-wizard-2

Description launch-wizard-2 created 2018-02-20T14:58:16.300+05:30

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	0.0.0.0/0	

► Instance Details [Edit instance details](#)

► Storage [Edit storage](#)

[Cancel](#) [Previous](#) [Launch](#)

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Choose the key and Click Launch instances.

Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair ▼

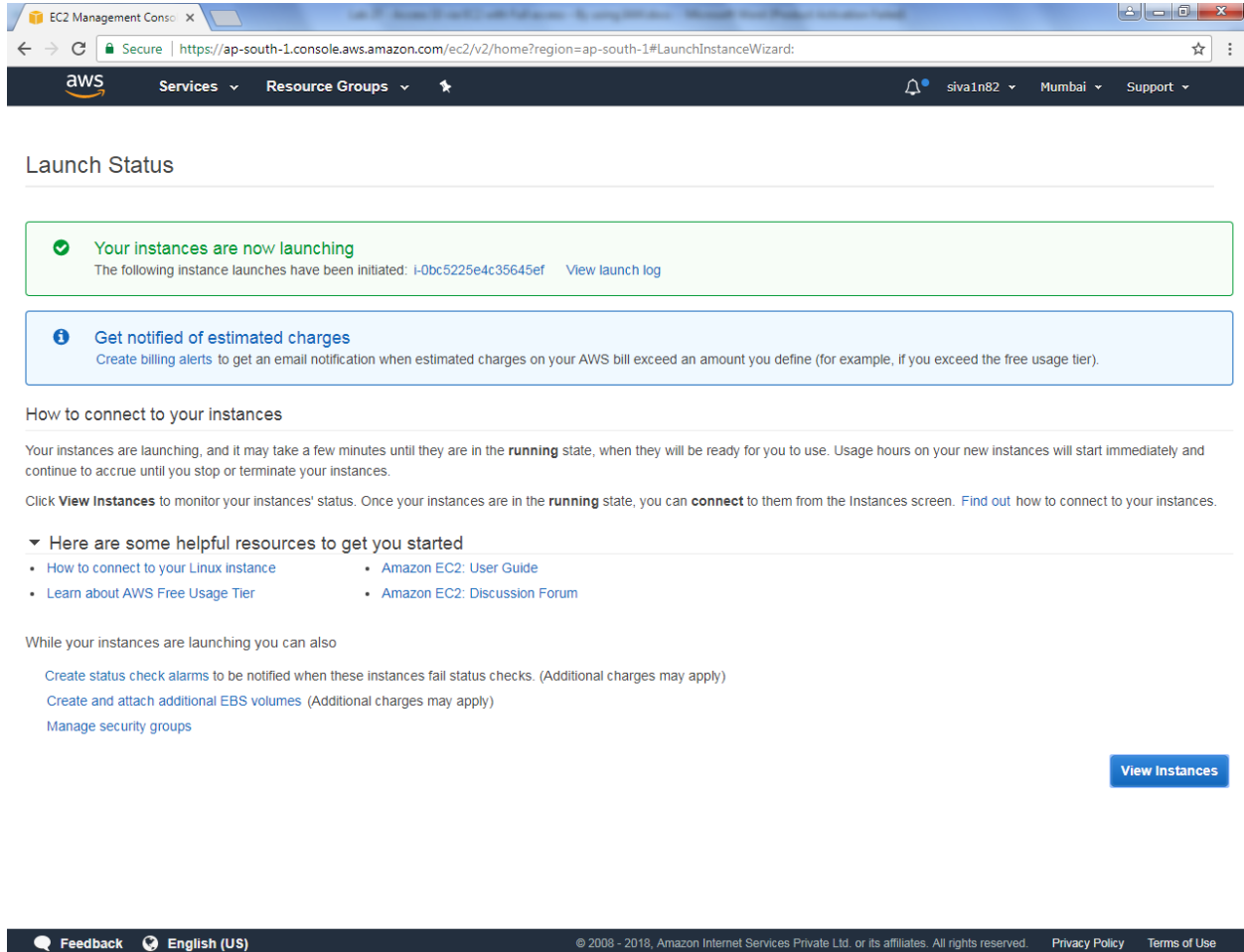
Select a key pair

Eveningaws ▼

☒ I acknowledge that I have access to the selected private key file (Eveningaws.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

Click “View instances”.



The screenshot shows the AWS Management Console interface. At the top, the browser address bar displays the URL: <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:>. The console header includes the AWS logo, navigation tabs for Services and Resource Groups, and user information for 'siva1n82' in the 'Mumbai' region. The main content area is titled 'Launch Status'. It features a green success message: 'Your instances are now launching' with a checkmark icon, stating that instance launches have been initiated with ID 'i-0bc5225e4c35645ef' and a link to 'View launch log'. Below this is a blue informational message: 'Get notified of estimated charges' with an information icon, explaining that billing alerts can be created to receive email notifications when estimated charges exceed a defined threshold. The section 'How to connect to your instances' provides instructions on the 'running' state and includes a link to 'Find out how to connect to your instances'. A dropdown menu 'Here are some helpful resources to get you started' lists links for Linux instances, AWS Free Usage Tier, Amazon EC2 User Guide, and Amazon EC2 Discussion Forum. Further down, under 'While your instances are launching you can also', there are links to create status check alarms, attach additional EBS volumes, and manage security groups. A prominent blue button labeled 'View Instances' is located at the bottom right of the main content area. The footer contains a feedback link, language selection (English (US)), and copyright information for Amazon Internet Services Private Ltd.

EC2 Management Console

Secure | <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:>

aws Services Resource Groups siva1n82 Mumbai Support

Launch Status

✓ **Your instances are now launching**
The following instance launches have been initiated: [i-0bc5225e4c35645ef](#) [View launch log](#)

i **Get notified of estimated charges**
Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

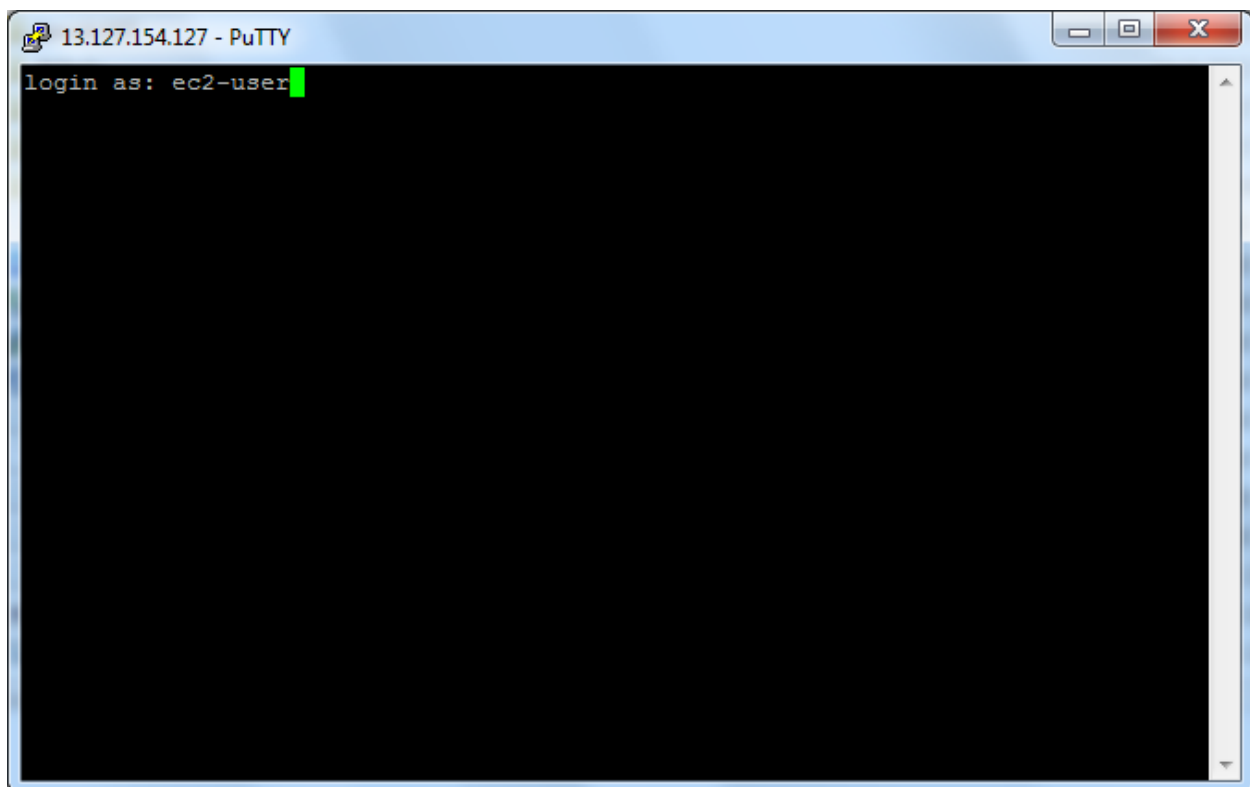
While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

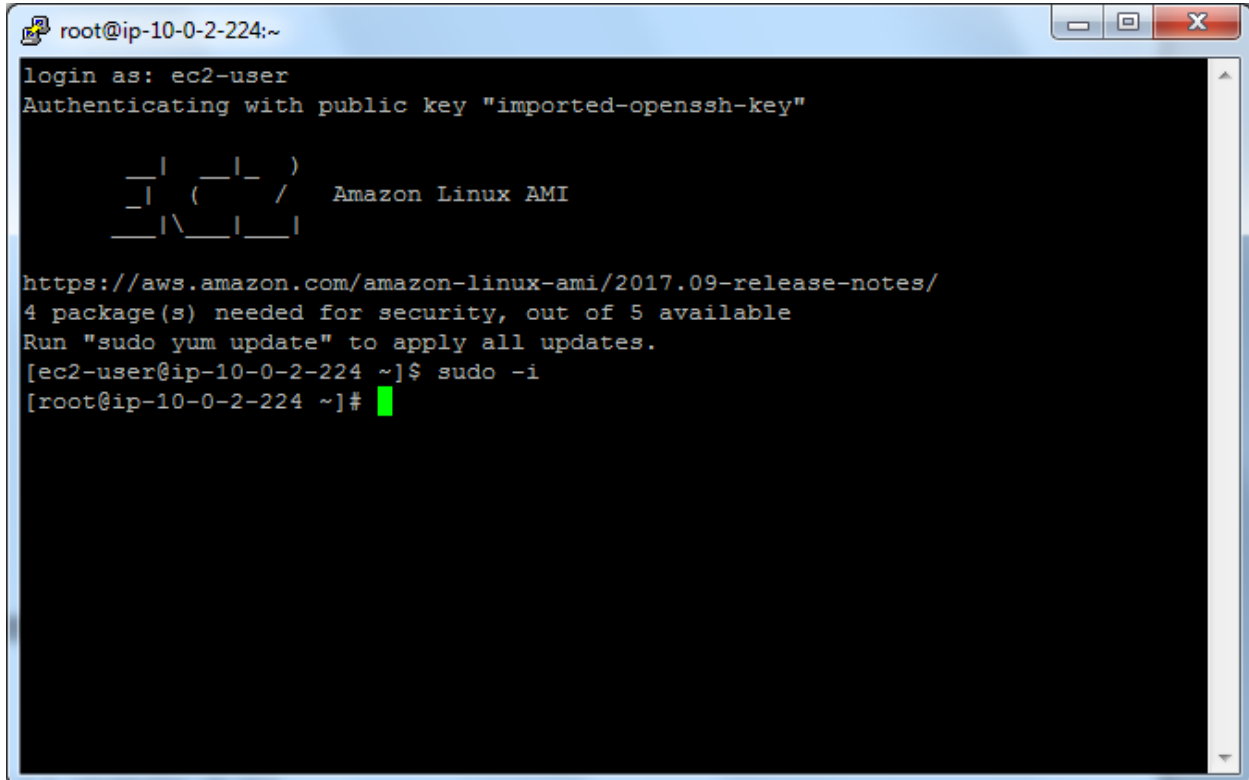
[View Instances](#)

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Login to Linux instance by using SSH.

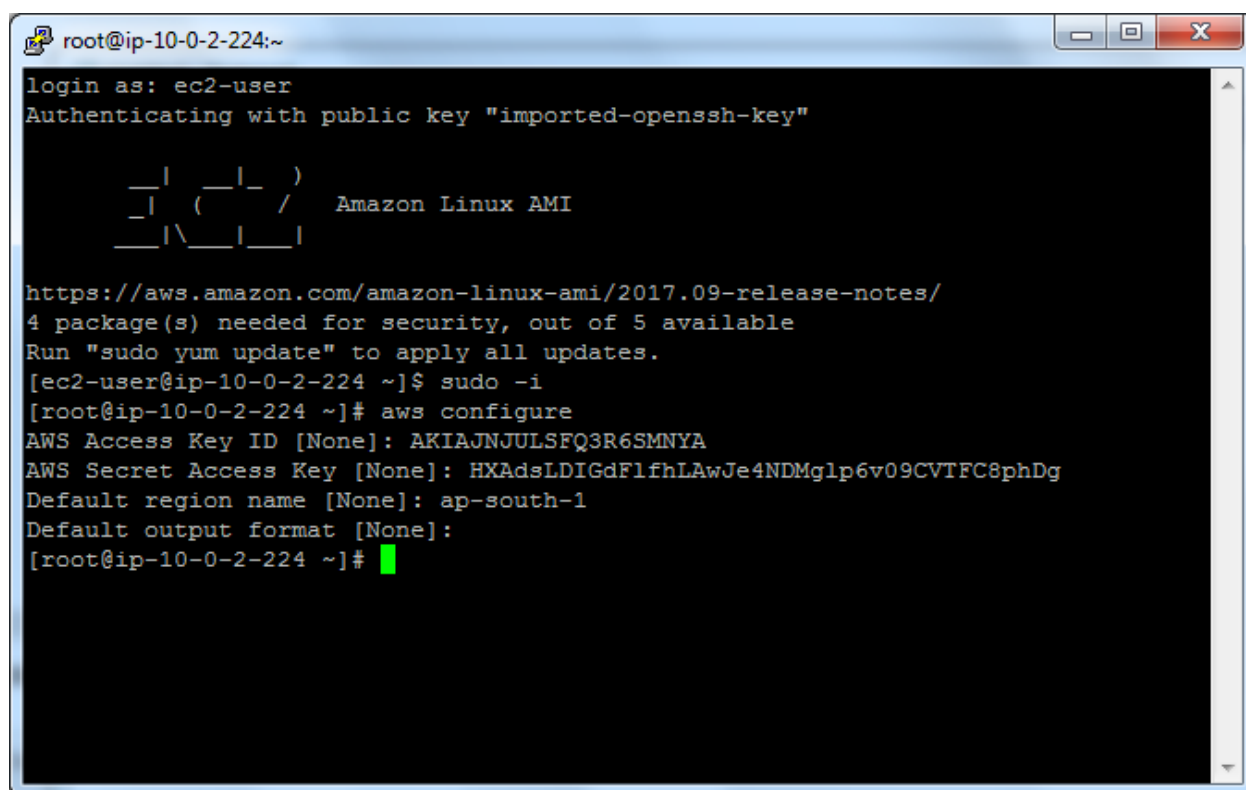


Type `sudo -i`



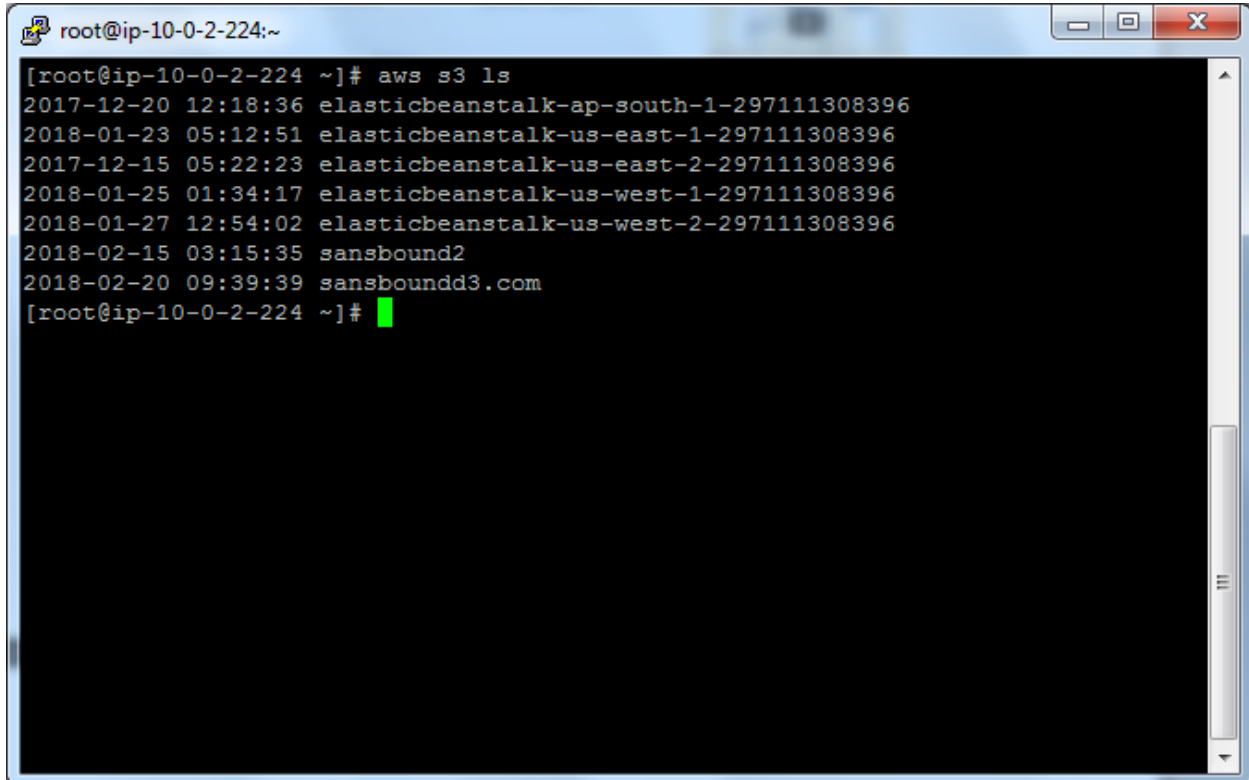
```
root@ip-10-0-2-224:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
  _ | _ | _ )  
  _ | ( _ | /  Amazon Linux AMI  
  _ | \ _ | _ |  
  
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/  
4 package(s) needed for security, out of 5 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-0-2-224 ~]$ sudo -i  
[root@ip-10-0-2-224 ~]#
```

Login to aws configure mode by using access key ID and secret access key. You must type the region to configure.



```
root@ip-10-0-2-224:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
  _| _|_ )  
  _| ( _| /  Amazon Linux AMI  
  __| \__|__|  
  
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/  
4 package(s) needed for security, out of 5 available  
Run "sudo yum update" to apply all updates.  
[ec2-user@ip-10-0-2-224 ~]$ sudo -i  
[root@ip-10-0-2-224 ~]# aws configure  
AWS Access Key ID [None]: AKIAJNJULSFQ3R6SMNYA  
AWS Secret Access Key [None]: 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  
Default region name [None]: ap-south-1  
Default output format [None]:  
[root@ip-10-0-2-224 ~]#
```

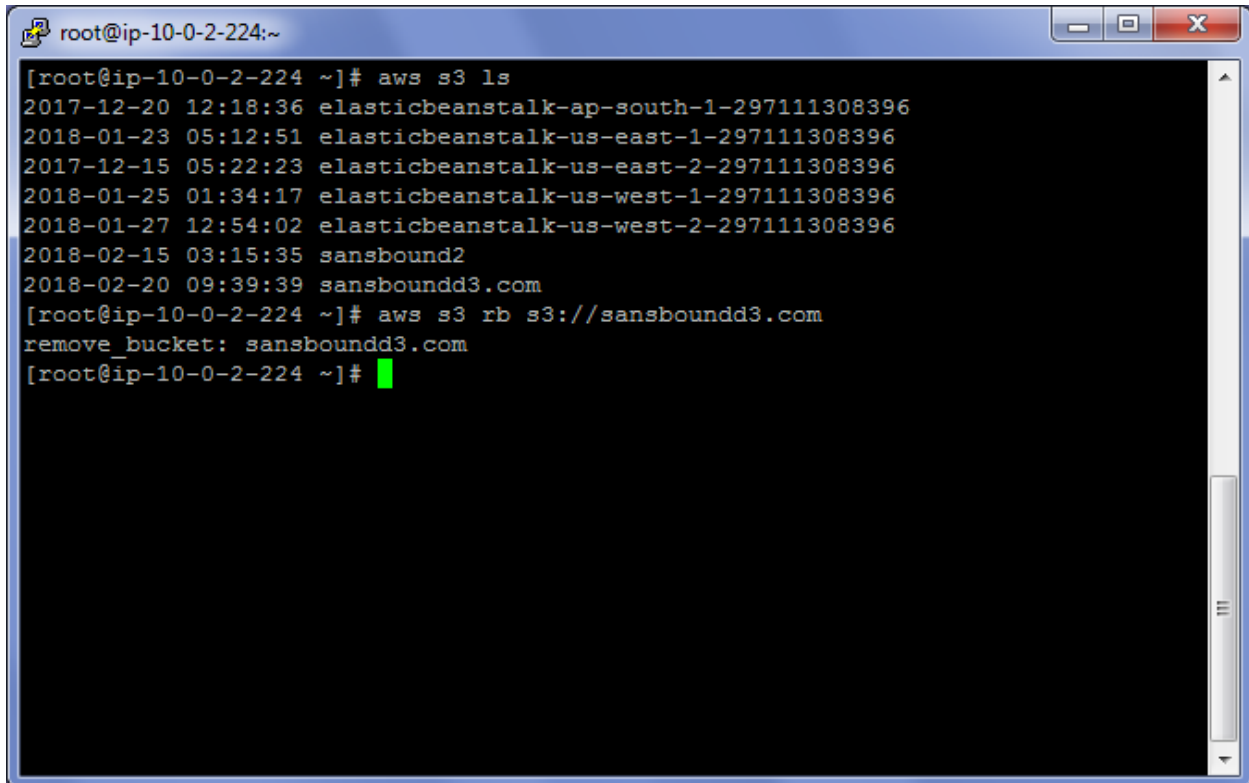
Type `aws s3 ls` command to list the bucket.



```
root@ip-10-0-2-224:~  
[root@ip-10-0-2-224 ~]# aws s3 ls  
2017-12-20 12:18:36 elasticbeanstalk-ap-south-1-297111308396  
2018-01-23 05:12:51 elasticbeanstalk-us-east-1-297111308396  
2017-12-15 05:22:23 elasticbeanstalk-us-east-2-297111308396  
2018-01-25 01:34:17 elasticbeanstalk-us-west-1-297111308396  
2018-01-27 12:54:02 elasticbeanstalk-us-west-2-297111308396  
2018-02-15 03:15:35 sansbound2  
2018-02-20 09:39:39 sansboundd3.com  
[root@ip-10-0-2-224 ~]#
```


Type `aws s3 rb s3://sansboundd3.com`

Successfully removed the bucket.

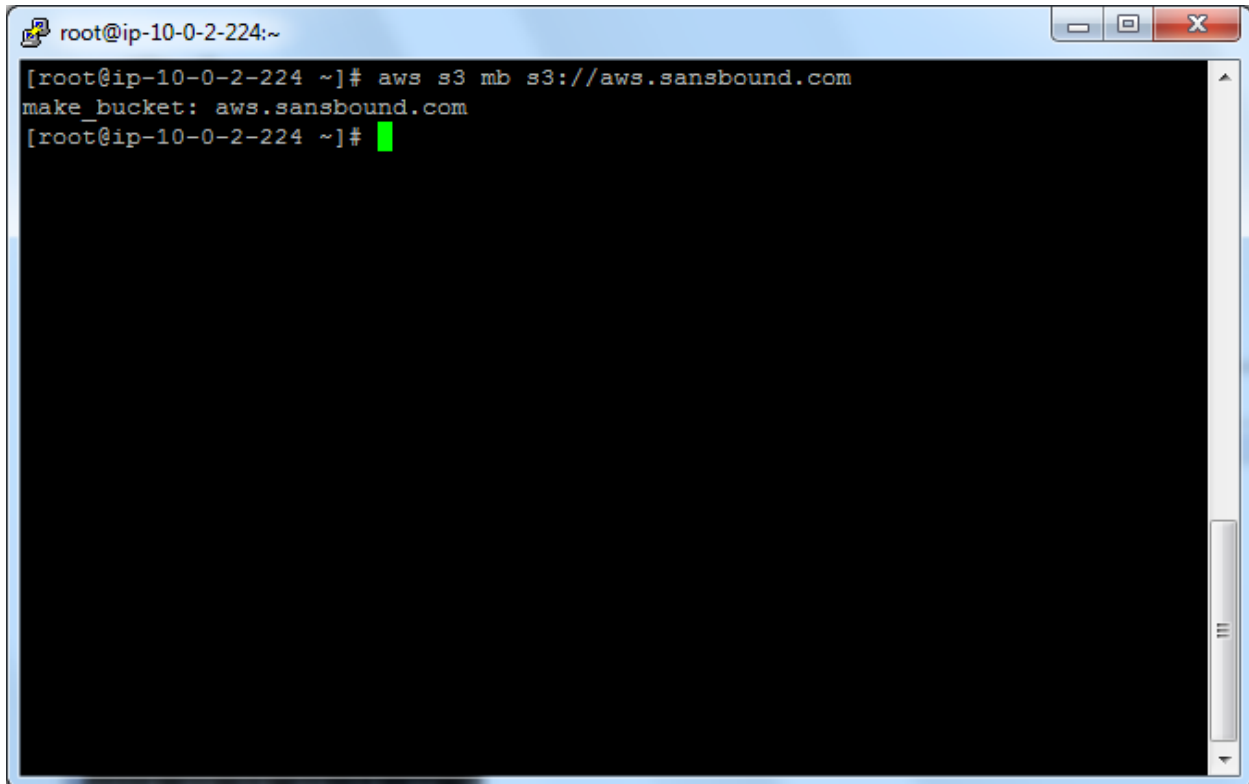
A terminal window titled 'root@ip-10-0-2-224:~' with standard window controls. The terminal shows the following commands and output:

```
[root@ip-10-0-2-224 ~]# aws s3 ls
2017-12-20 12:18:36 elasticbeanstalk-ap-south-1-297111308396
2018-01-23 05:12:51 elasticbeanstalk-us-east-1-297111308396
2017-12-15 05:22:23 elasticbeanstalk-us-east-2-297111308396
2018-01-25 01:34:17 elasticbeanstalk-us-west-1-297111308396
2018-01-27 12:54:02 elasticbeanstalk-us-west-2-297111308396
2018-02-15 03:15:35 sansbound2
2018-02-20 09:39:39 sansboundd3.com
[root@ip-10-0-2-224 ~]# aws s3 rb s3://sansboundd3.com
remove_bucket: sansboundd3.com
[root@ip-10-0-2-224 ~]#
```

Type

Aws s3 mb s3://aws.sansbound.com

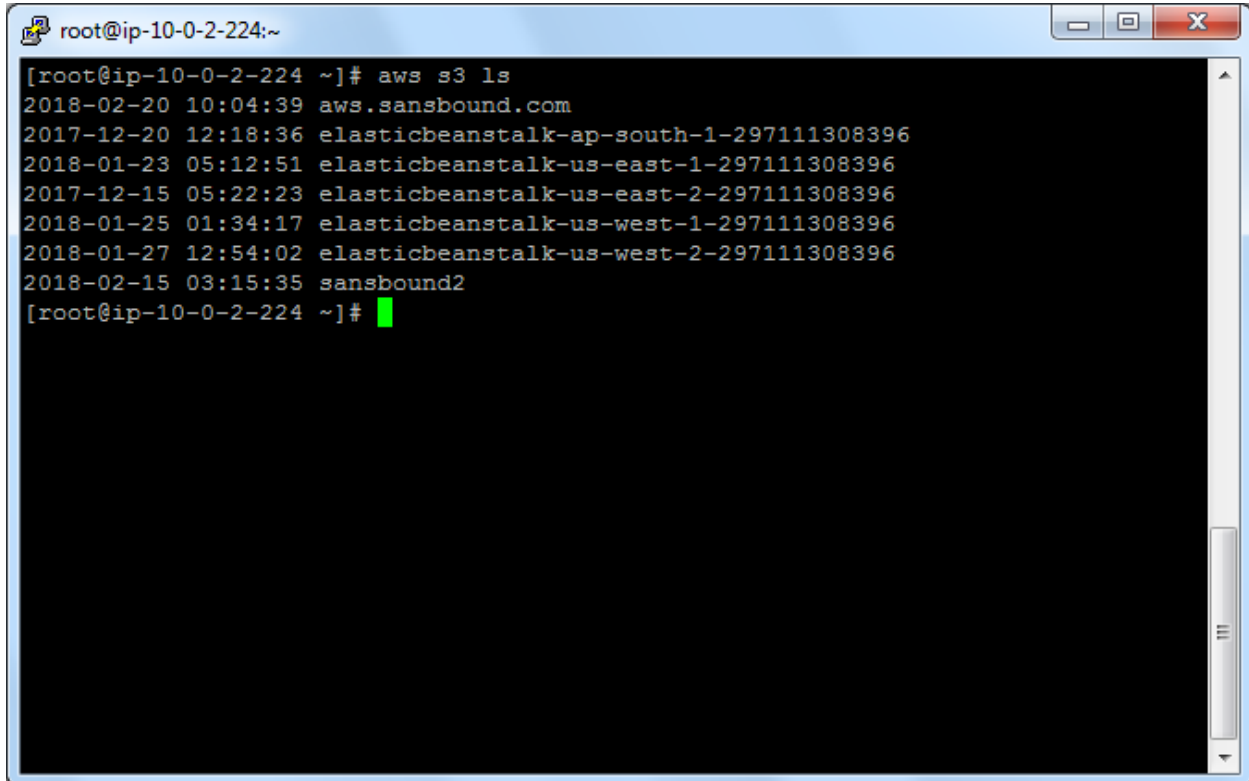
Successfully created the bucket.



```
root@ip-10-0-2-224:~  
[root@ip-10-0-2-224 ~]# aws s3 mb s3://aws.sansbound.com  
make_bucket: aws.sansbound.com  
[root@ip-10-0-2-224 ~]#
```

Type

Aws s3 ls



```
root@ip-10-0-2-224:~  
[root@ip-10-0-2-224 ~]# aws s3 ls  
2018-02-20 10:04:39 aws.sansbound.com  
2017-12-20 12:18:36 elasticbeanstalk-ap-south-1-297111308396  
2018-01-23 05:12:51 elasticbeanstalk-us-east-1-297111308396  
2017-12-15 05:22:23 elasticbeanstalk-us-east-2-297111308396  
2018-01-25 01:34:17 elasticbeanstalk-us-west-1-297111308396  
2018-01-27 12:54:02 elasticbeanstalk-us-west-2-297111308396  
2018-02-15 03:15:35 sansbound2  
[root@ip-10-0-2-224 ~]#
```

Bucket details listed successfully.