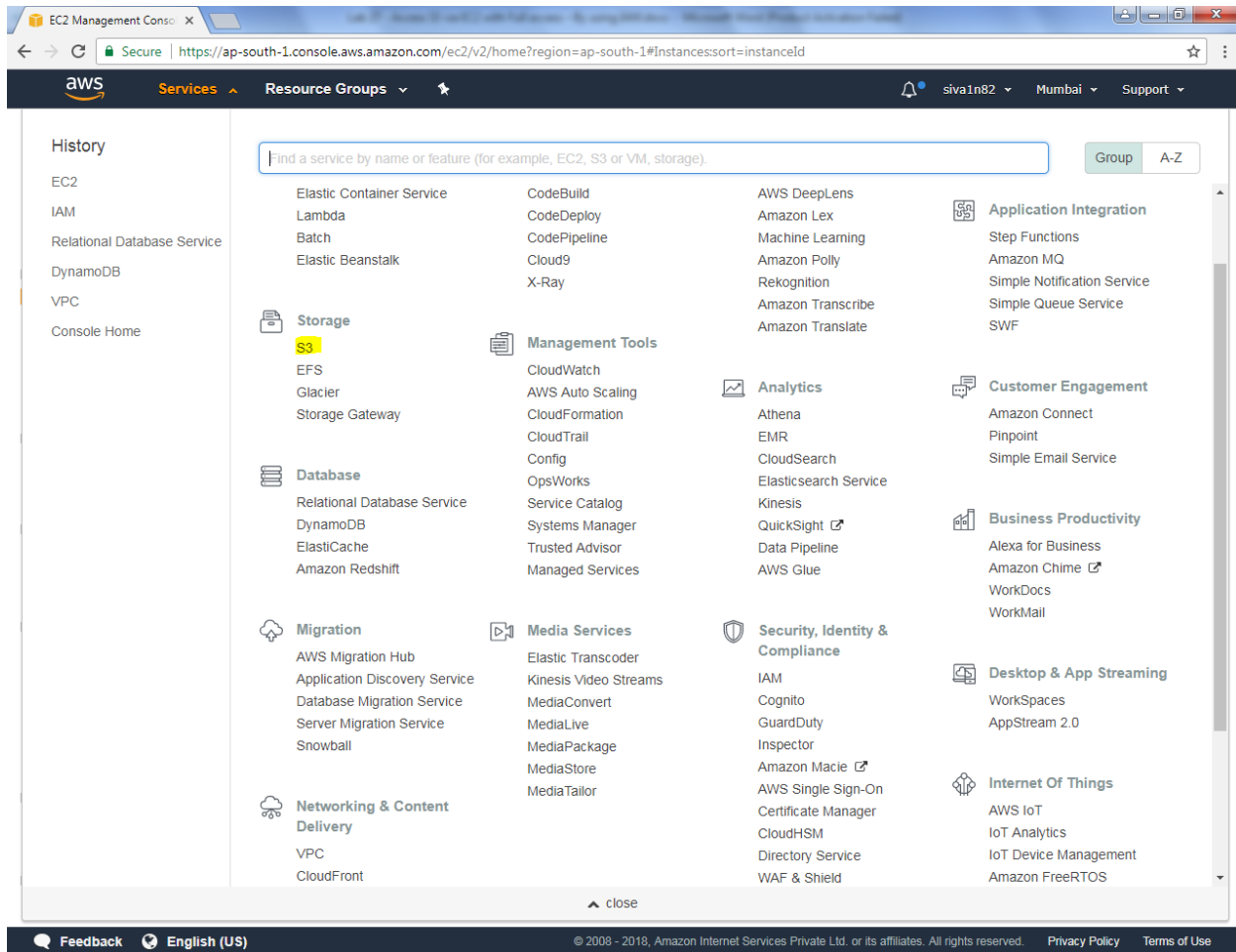


Lab 27

Access S3 via EC2 with Full access – By using IAM

Click “S3” service



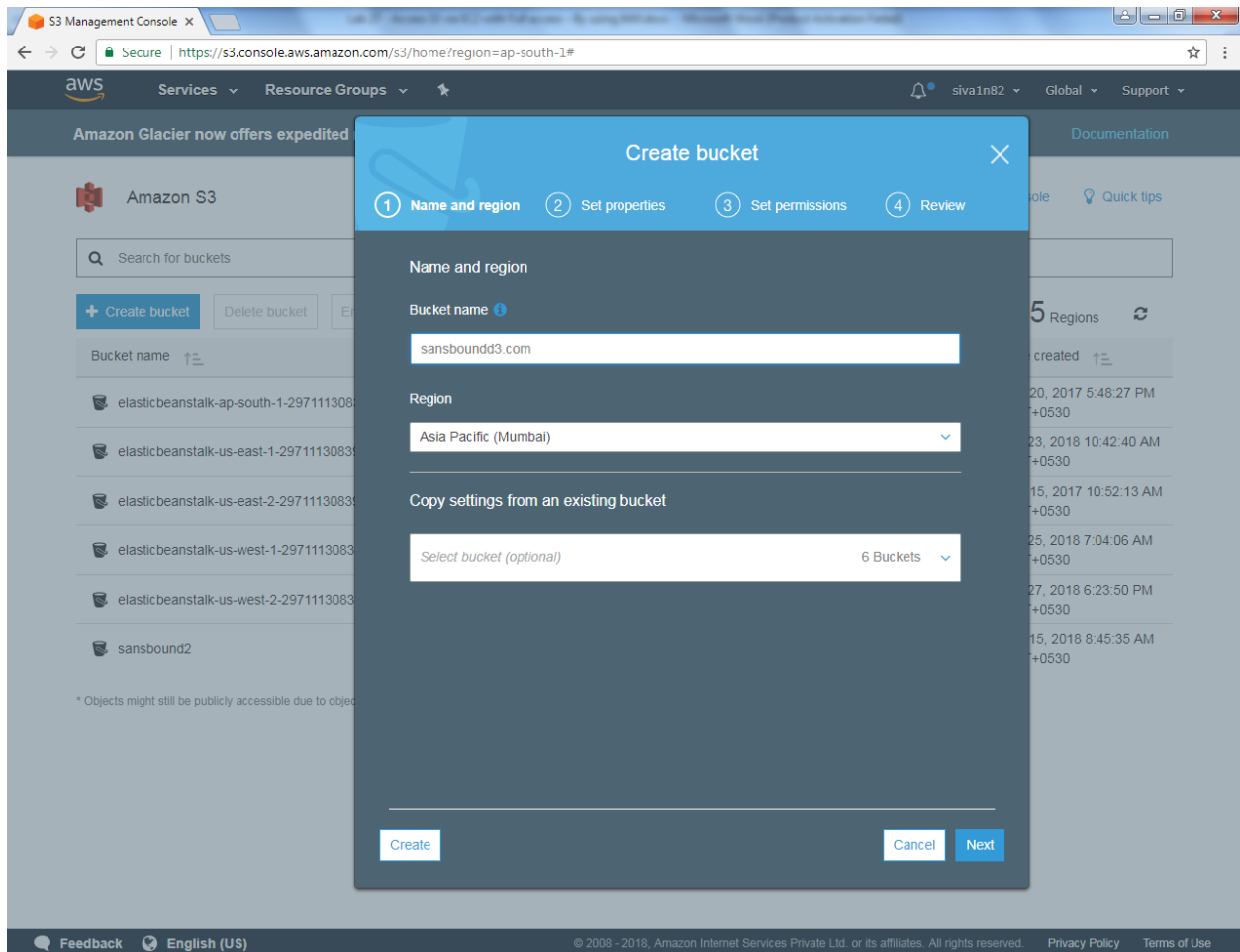
Click “Create bucket”.

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 a user profile 'siva1n82'. Below this, a banner for Amazon Glacier is visible. The main header reads 'Amazon S3' with links to 'Discover the new console' and 'Quick tips'. A search bar labeled 'Search for buckets' is present. Below the search bar, there are three buttons: '+ Create bucket' (highlighted with a green box), 'Delete bucket', and 'Empty bucket'. To the right of these buttons, it shows '6 Buckets', '0 Public' (in an orange box), and '5 Regions'. A table lists the existing buckets with columns for 'Bucket name', 'Access', 'Region', and 'Date created'. The buckets listed are: 'elasticbeanstalk-ap-south-1-297111308396' (Asia Pacific (Mumbai)), 'elasticbeanstalk-us-east-1-297111308396' (US East (N. Virginia)), 'elasticbeanstalk-us-east-2-297111308396' (US East (Ohio)), 'elasticbeanstalk-us-west-1-297111308396' (US West (N. California)), 'elasticbeanstalk-us-west-2-297111308396' (US West (Oregon)), and 'sansbound2' (US East (N. Virginia)). All buckets are marked as 'Not public *'. At the bottom, a footer contains 'Feedback', 'English (US)', and copyright information.

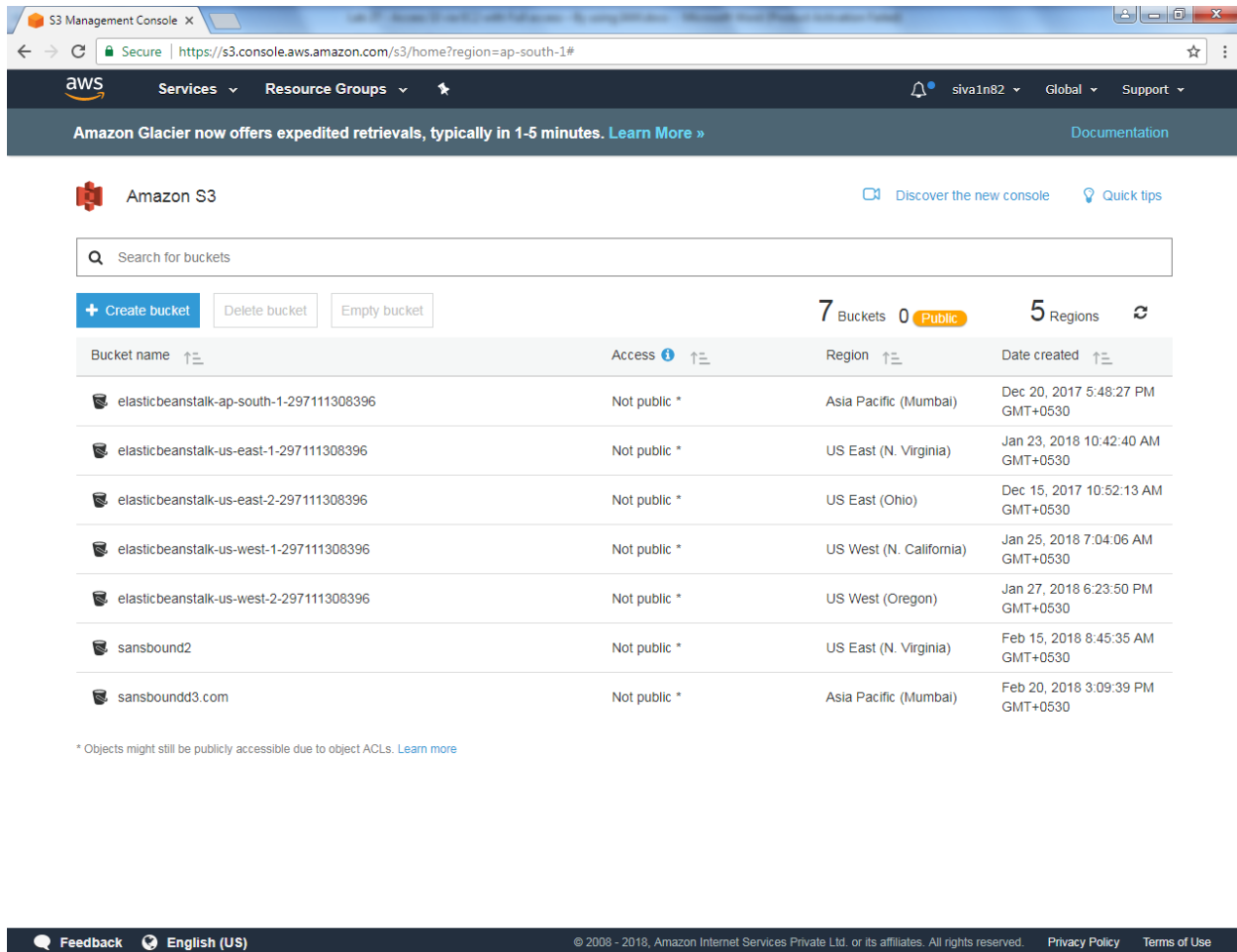
Bucket name	Access	Region	Date created
elasticbeanstalk-ap-south-1-297111308396	Not public *	Asia Pacific (Mumbai)	Dec 20, 2017 5:48:27 PM GMT+0530
elasticbeanstalk-us-east-1-297111308396	Not public *	US East (N. Virginia)	Jan 23, 2018 10:42:40 AM GMT+0530
elasticbeanstalk-us-east-2-297111308396	Not 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](#)

Type sansboundd3.com



Bucket has been successfully created.

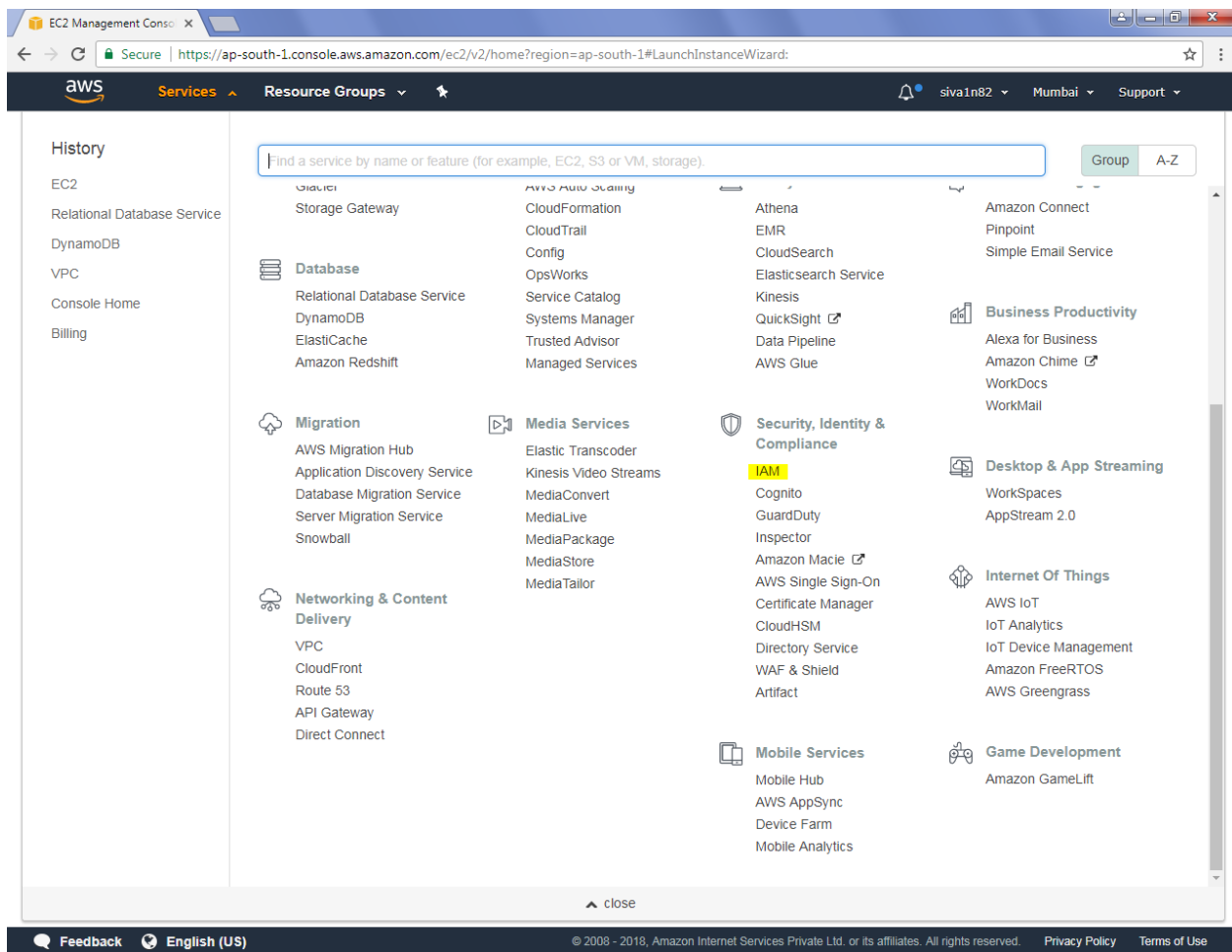


The screenshot displays the AWS S3 Management Console interface. At the top, there's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and a user profile 'siva1n82'. Below this, a banner for Amazon Glacier is visible. The main header shows 'Amazon S3' with links to 'Discover the new console' and 'Quick tips'. A search bar is present with the placeholder text 'Search for buckets'. Below the search bar, there are buttons for '+ Create bucket', 'Delete bucket', and 'Empty bucket'. To the right, summary statistics show '7 Buckets', '0 Public' (with a yellow tag), and '5 Regions'. The main content area is a table listing buckets with columns for 'Bucket name', 'Access', 'Region', and 'Date created'. The table contains seven entries, all with 'Not public *' access. At the bottom, a footer bar includes 'Feedback', 'English (US)', and copyright information.

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](#)

Click "IAM" service



Click “Users”.

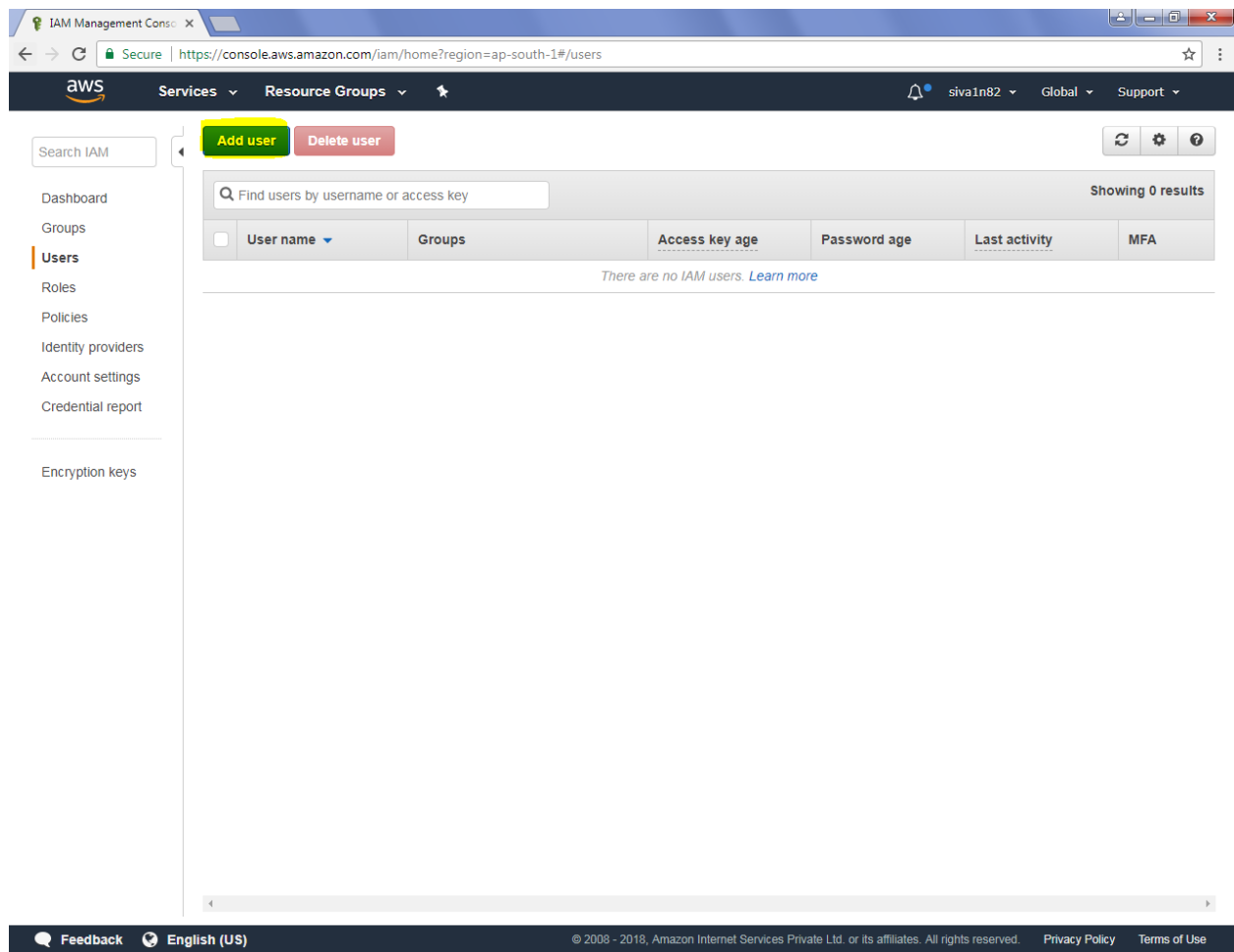
The screenshot displays the AWS IAM Management Console interface. At the top, the browser address bar shows the URL `https://console.aws.amazon.com/iam/home?region=ap-south-1#/home`. The console header includes the AWS logo, navigation tabs for Services and Resource Groups, and user information for 'siva1n82' in the 'Global' region. The left sidebar lists navigation options: Search IAM, 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 provides the following information:

- IAM users sign-in link:** `https://297111308396.signin.aws.amazon.com/console` (with 'Customize' and 'Copy Link' options).
- IAM Resources:**
 - Users: 0
 - Groups: 1
 - Roles: 2
 - Identity Providers: 0
 - Customer Managed Policies: 1
- Security Status:** A progress bar indicates '1 out of 5 complete'. Below it is a list of tasks:
 - Delete your root access keys (Warning icon)
 - Activate MFA on your root account (Warning icon)
 - Create individual IAM users (Warning icon)
 - Use groups to assign permissions (Success icon)
 - Apply an IAM password policy (Warning icon)

The right sidebar contains a 'Feature Spotlight' section with a video player for '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.

At the bottom of the console, there is a footer with 'Feedback', '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 “Add user”.



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

The screenshot shows the AWS IAM console 'Add user' wizard. The browser address bar shows the URL: [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). The navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information 'siva1n82'. The wizard progress bar shows four steps: 1. Details (active), 2. Permissions, 3. Review, and 4. Complete.

Add user

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's a navigation bar with the AWS logo, 'Services', 'Resource Groups', and a user profile 'siva1n82'. Below this, three main actions are presented: 'Add user to group', 'Copy permissions from existing user', and 'Attach existing policies directly' (which is highlighted with a blue box and a callout arrow). The 'Attach existing policies directly' section contains a sub-header 'Attach one or more existing policies directly to the users or create a new policy. [Learn more](#)'. Below this are 'Create policy' and 'Refresh' buttons. A filter section shows 'Filter: Policy type' and a search box containing 's3', with a note 'Showing 5 results'. A table lists the following policies:

	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

At the bottom right of the console, there are three buttons: 'Cancel', 'Previous', and 'Next: Review' (which is highlighted in blue). The footer contains 'Feedback', 'English (US)', and copyright information.

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

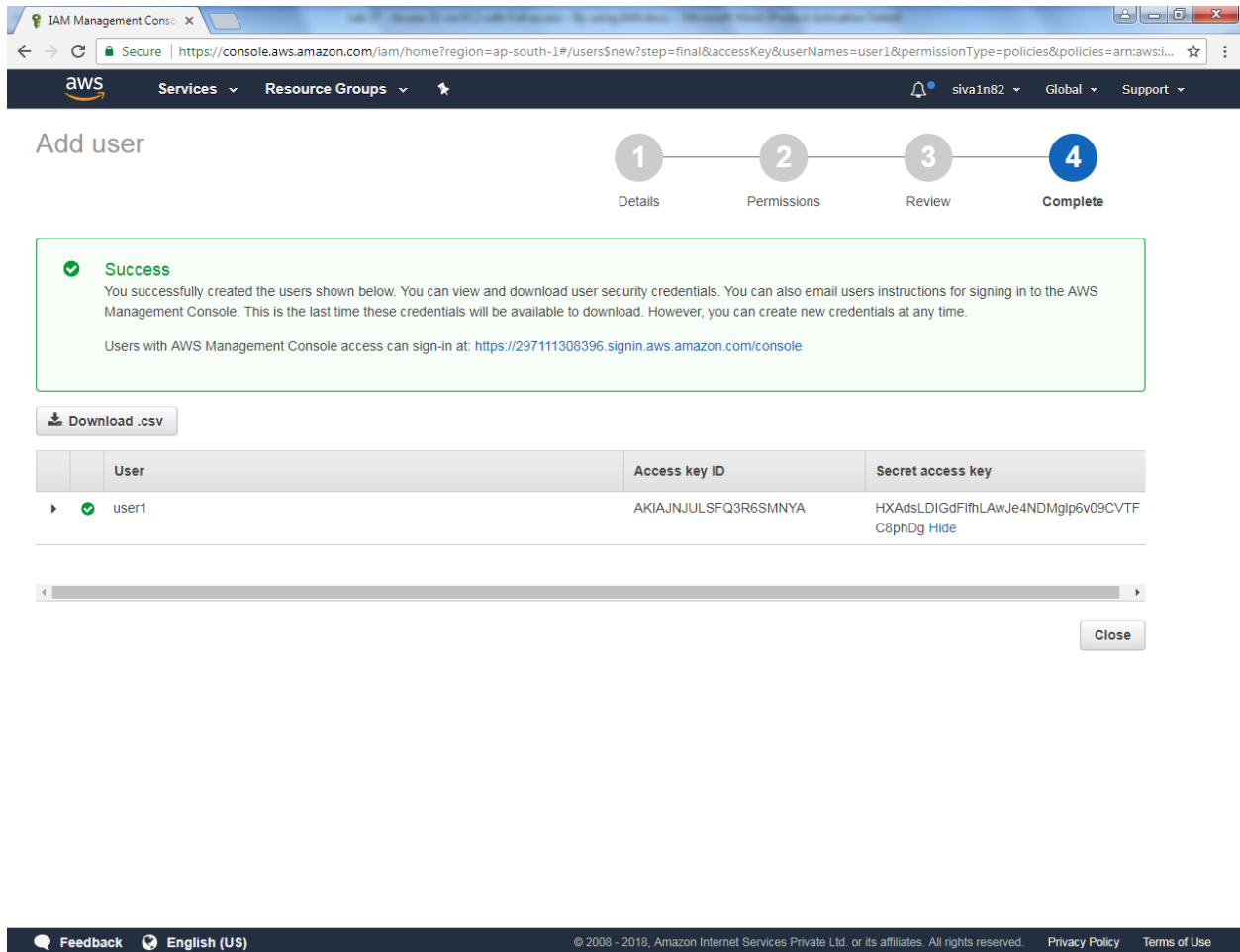
The following policies will be attached to the user shown above.

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.



The screenshot shows the AWS IAM Management Console interface. At the top, the breadcrumb navigation indicates the path: **Add user**. A progress bar shows four steps: 1. Details, 2. Permissions, 3. Review, and 4. Complete (highlighted in blue). Below the progress bar, a green success message states: "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." Below the message is a link: "Users with AWS Management Console access can sign-in at: <https://297111308396.signin.aws.amazon.com/console>". A button labeled "Download .csv" is present. Below this is a table with three columns: "User", "Access key ID", and "Secret access key". The table contains one row for "user1". The "Access key ID" is "AKIAJNJULSFQ3R6SMNYA" and the "Secret access key" is "HXAdsLDIGdFfthLAWJe4NDMglp6v09CVTF C8phDg" with a "Hide" link. A "Close" button is at the bottom right of the table area. The footer of the console shows "Feedback", "English (US)", and copyright information.

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	HXAdsLDIGdFfthLAWJe4NDMglp6v09CVTF 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 Management Console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information 'siva1n82'. The left sidebar contains a search bar and navigation links: Dashboard, Groups, **Users**, Roles, Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has 'Add user' and 'Delete user' buttons, a search bar 'Find users by username or access key', and a table of users. The table shows one user, 'user1', with 'None' for Groups, Access key age, Password age, Last activity, and 'Not enabled' for MFA. The footer includes '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.

Search IAM

Dashboard
Groups
Users
Roles
Policies
Identity providers
Account settings
Credential report
Encryption keys

Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- [IAM Roles FAQ](#)
- [IAM Roles Documentation](#)
- [Tutorial: Setting Up Cross Account Access](#)
- [Common Scenarios for Roles](#)

Create role Delete role

Search Showing 2 results

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

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 'Create role' wizard. 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 navigation bar shows the user is logged in as 'siva1n82' with a 'Global' region and 'Support' link.

The 'Create role' wizard has three steps: 1. Trust, 2. Permissions, and 3. Review. Step 1 is currently active.

The 'Select type of trusted entity' section shows four options:

- AWS service**: EC2, Lambda and others (Selected)
- Another AWS account**: Belonging to you or 3rd party
- Web identity**: Cognito or any OpenID provider
- SAML**: SAML 2.0 federation, Your corporate directory

A tooltip for the 'AWS service' option states: 'Allows AWS services to perform actions on your behalf. [Learn more](#)'. Below this, a list of services is shown, with 'EC2' highlighted:

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	

At the bottom of the wizard, there is a 'Cancel' button and a 'Next: Permissions' button. The footer of the console shows 'Feedback', 'English (US)', and copyright information: '© 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 user information 'siva1n82'. Below this, a grid of AWS services is displayed, including Batch, Directory Service, Greengrass, RDS, and Storage Gateway. The 'EC2' service is highlighted in the grid. Below the grid, the 'Select your use case' section is active, showing several options for EC2 roles. The 'EC2' option is selected, which allows EC2 instances to call AWS services on your behalf. Other options include 'EC2 - Scheduled Instances', 'EC2 - Spot Fleet', 'EC2 - Spot Fleet Auto Scaling', 'EC2 - Spot Fleet Tagging', 'EC2 - Spot Instances', 'EC2 Role for Simple Systems Manager', and 'EC2 Spot Fleet Role'. At the bottom of the console, there are buttons for 'Cancel' and 'Next: Permissions', along with a footer containing 'Feedback', 'English (US)', and copyright information.

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”.

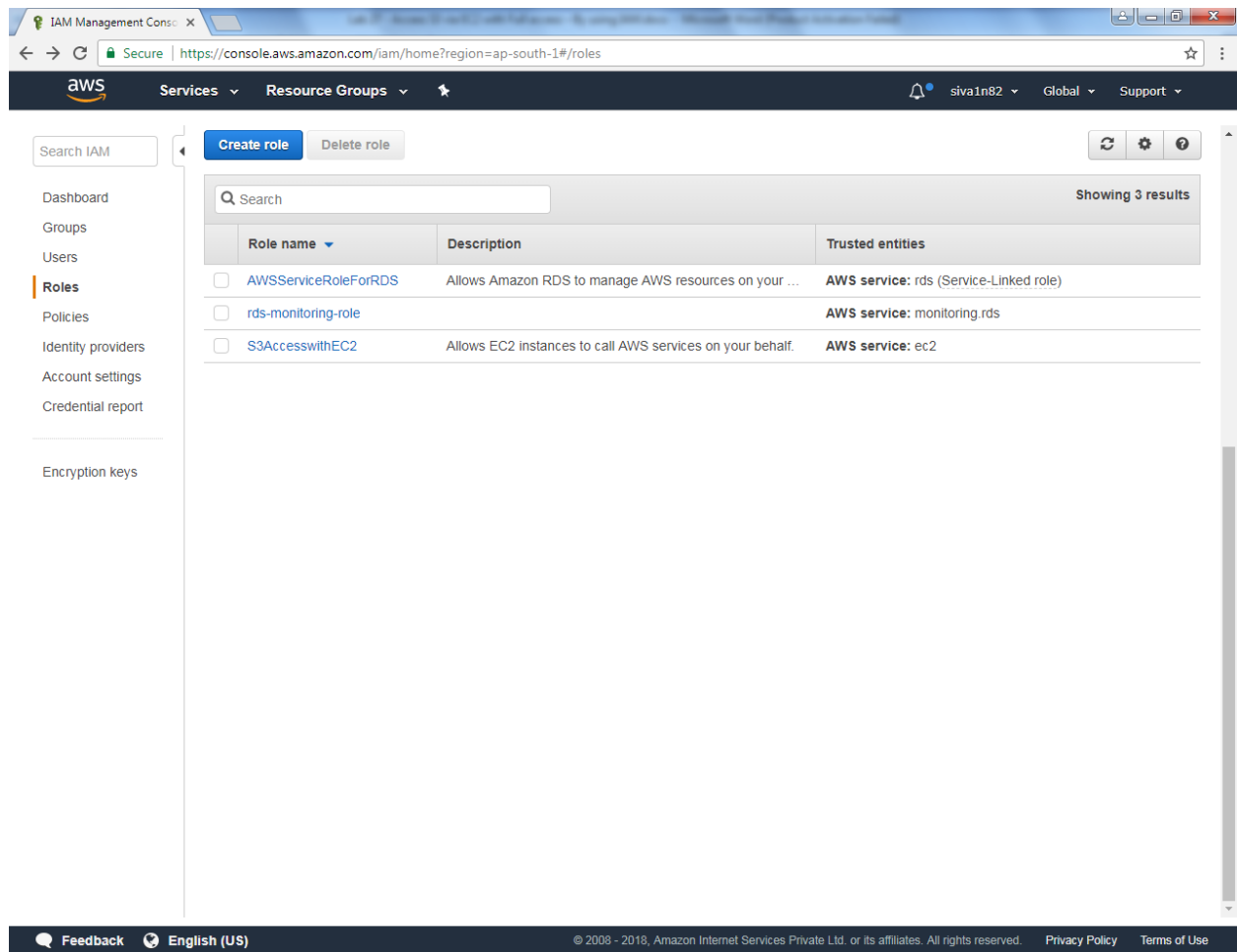
The screenshot shows the AWS IAM console 'Create role' page, specifically the 'Review' step (Step 3 of 3). The page header includes the AWS logo, navigation tabs for 'Services' and 'Resource Groups', and user information 'siva1n82'. The main heading is 'Create role', followed by a progress indicator with three steps: 1. Trust, 2. Permissions, and 3. Review (the current step). Below the heading, the text 'Review' is followed by the instruction 'Provide the required information below and review this role before you create it.'

The form contains the following fields and information:

- Role name***: A text input field containing 'S3AccesswithEC2'. Below the field, a note states: 'Maximum 64 characters. Use alphanumeric and "+=, @ _" characters.'
- Role description**: A text area containing 'Allows EC2 instances to call AWS services on your behalf.' Below the text area, a note states: 'Maximum 1000 characters. Use alphanumeric and "+=, @ _" characters.'
- Trusted entities**: A label 'AWS service:' followed by the text 'ec2.amazonaws.com'.
- Policies**: A section showing a selected policy 'AmazonS3FullAccess' with a blue checkmark icon.

At the bottom of the form, there is a '* Required' label, a 'Cancel' button, a 'Previous' button, and a 'Create role' button. 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.' along with links to 'Privacy Policy' and 'Terms of Use'.

You can able to view the roles as below.



The screenshot shows the AWS IAM console interface. The top navigation bar includes the AWS logo, 'Services', 'Resource Groups', and user information 'siva1n82'. The left sidebar contains a 'Search IAM' box and a list of navigation items: Dashboard, Groups, Users, Roles (highlighted), Policies, Identity providers, Account settings, Credential report, and Encryption keys. The main content area has 'Create role' and 'Delete role' buttons. Below these is a search bar and a table of roles. The table has three columns: Role name, Description, and Trusted entities. It displays three roles: 'AWSServiceRoleForRDS', 'rds-monitoring-role', and 'S3AccesswithEC2'. Each role has a checkbox in the 'Role name' column. The 'Trusted entities' column lists the AWS service each role is associated with.

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

Click “Launch instance”.

EC2 Management Console

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

Services Resource Groups

siva1n82 Mumbai Support

EC2 Dashboard

- Events
- Tags
- Reports
- Limits
- INSTANCES
 - Instances
 - Launch Templates
 - Spot Requests
 - Reserved Instances
 - Dedicated Hosts
- IMAGES
 - AMIs
 - Bundle Tasks
- ELASTIC BLOCK STORE
 - Volumes
 - Snapshots
- NETWORK & SECURITY
 - Security Groups
 - Elastic IPs
 - Placement Groups
 - Key Pairs
 - Network Interfaces
- LOAD BALANCING
 - Load Balancers
 - Target Groups
- AUTO SCALING
 - Launch Configurations
 - Auto Scaling Groups

Resources

You are using the following Amazon EC2 resources in the Asia Pacific (Mumbai) region:

0 Running Instances	0 Elastic IPs
0 Dedicated Hosts	1 Snapshots
0 Volumes	0 Load Balancers
9 Key Pairs	10 Security Groups
0 Placement Groups	

Learn more about the latest in AWS Compute from AWS re:Invent 2017 by viewing the [EC2 Videos](#).

Create Instance

To start using Amazon EC2 you will want to launch a virtual server, known as an Amazon EC2 instance.

[Launch Instance](#)

Note: Your instances will launch in the Asia Pacific (Mumbai) region

Service Health

Service Status:

✓ Asia Pacific (Mumbai):
This service is operating normally

Availability Zone Status:

✓ ap-south-1a:
Availability zone is operating normally

✓ ap-south-1b:
Availability zone is operating normally

[Service Health Dashboard](#)

Scheduled Events

Asia Pacific (Mumbai):
No events

Account Attributes

Supported Platforms

VPC

Default VPC
vpc-a655a2ce

Resource ID length management

Additional Information

- [Getting Started Guide](#)
- [Documentation](#)
- [All EC2 Resources](#)
- [Forums](#)
- [Pricing](#)
- [Contact Us](#)

AWS Marketplace

Find free software trial products in the AWS Marketplace from the [EC2 Launch Wizard](#). Or try these popular AMIs:

[Barracuda NextGen Firewall F-Series - PAYG](#)

Provided by Barracuda Networks, Inc.
Rating ★★★★★
Starting from \$0.60/hr or from \$4,599/yr (12% savings) for software + AWS usage fees
[View all Software Infrastructure](#)

[Splunk Insights for AWS Cloud Monitoring](#)

Provided by Splunk Inc.
Rating ★★★★★
Bring Your Own License + AWS usage

Feedback English (US)

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

Select "Amazon Linux".

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

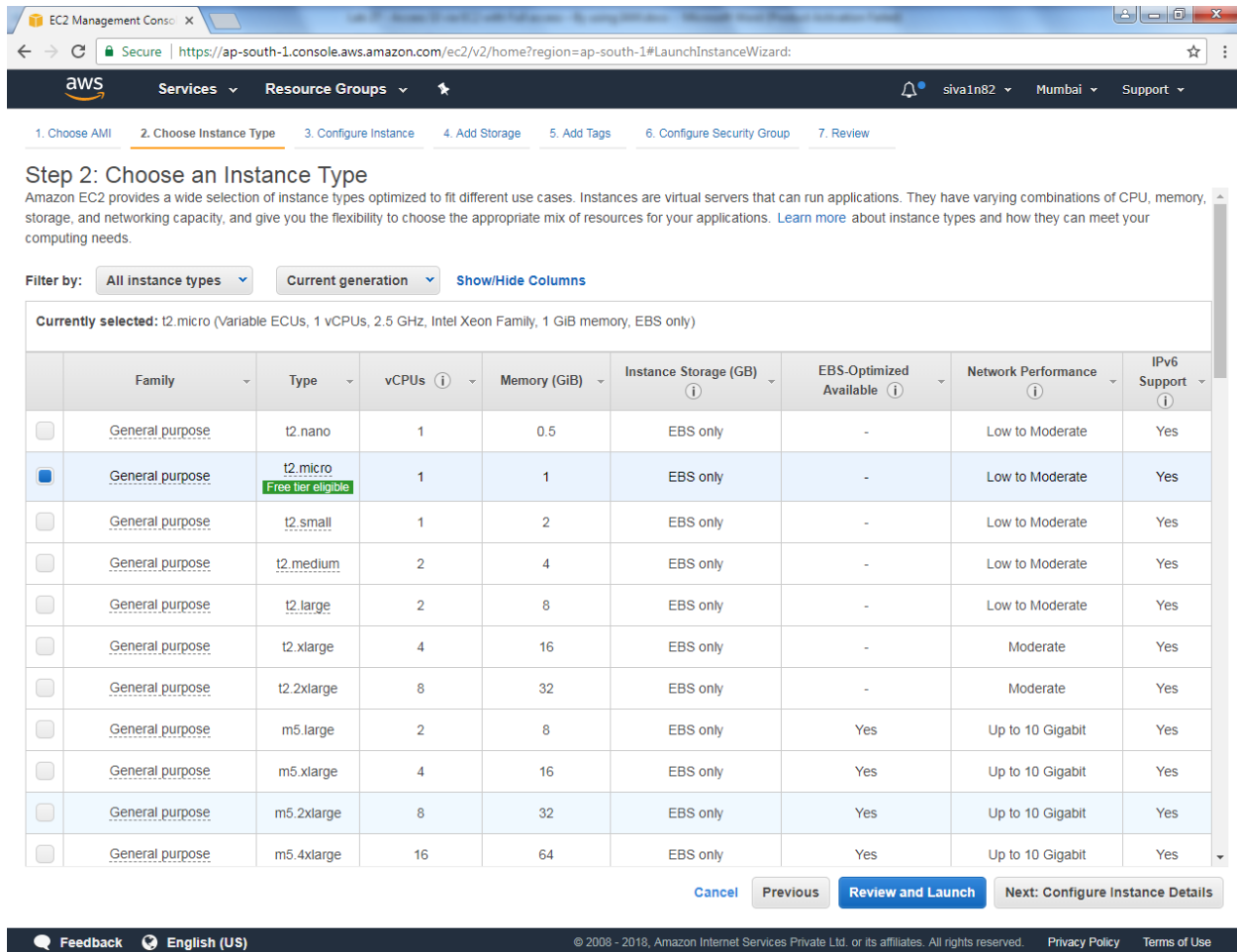
☐ Free tier only ⓘ

1 to 35 of 35 AMIs

Logo	AMI Name	AMI ID	Architecture	Buttons
Amazon Linux	Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type	ami-531a4c3c	64-bit	Select
Amazon Linux	Amazon Linux 2 LTS Candidate AMI 2017.12.0 (HVM), SSD Volume Type	ami-3b2f7954	64-bit	Select
SUSE Linux	SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type	ami-f7267298	64-bit	Select
Red Hat	Red Hat Enterprise Linux 7.4 (HVM), SSD Volume Type	ami-e60e5a89	64-bit	Select
Windows	Microsoft Windows Server 2016 Base	ami-ad8addc2	64-bit	Select

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 Free tier eligible	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”.

The screenshot shows the 'Step 3: Configure Instance Details' page in the AWS Management Console. The page is part of the 'Launch Instance Wizard' and includes a progress bar at the top with steps: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance (active), 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 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-09fe2261 | Sansbound_VPC_Mumbai [Create new VPC](#)

Subnet subnet-07d1c44a | Sansbound_Mumbai_Public_sub [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”.

The screenshot shows the AWS Management Console interface for the 'Launch Instance Wizard' in the 'ap-south-1' region. The wizard is at step 4, 'Add Storage'. The breadcrumb trail at the top shows: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (active), 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.

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 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 ⓘ	Volumes ⓘ
Name	Linux Instance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

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

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

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

Click “Next”.

Create a new security group for access ssh port.

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 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

Add Rule

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.

Cancel Previous **Review and Launch**

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](#)

[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

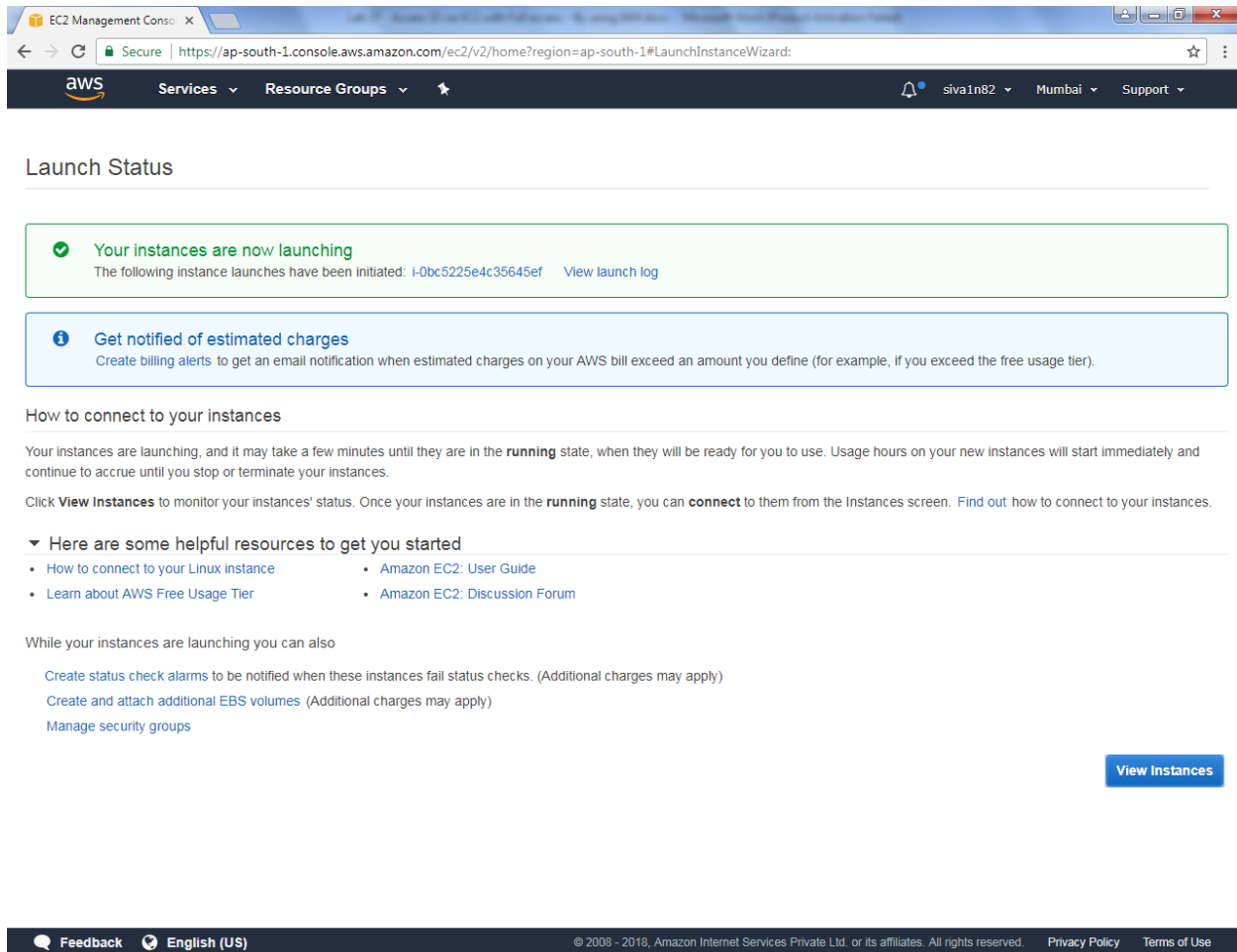
Eveningaws ▼

☒ 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 two informational boxes: a green one stating 'Your instances are now launching' with a link to 'View launch log', and a blue one titled 'Get notified of estimated charges' with a link to 'Create billing alerts'. Below these, a section 'How to connect to your instances' provides instructions on the 'running' state and includes a link to 'View Instances'. A list of helpful resources is provided, including links to Linux instance connection guides, the AWS Free Usage Tier, the Amazon EC2 User Guide, and the Amazon EC2 Discussion Forum. Further instructions on creating status check alarms, attaching EBS volumes, and managing security groups are listed. A blue 'View Instances' button 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](#)

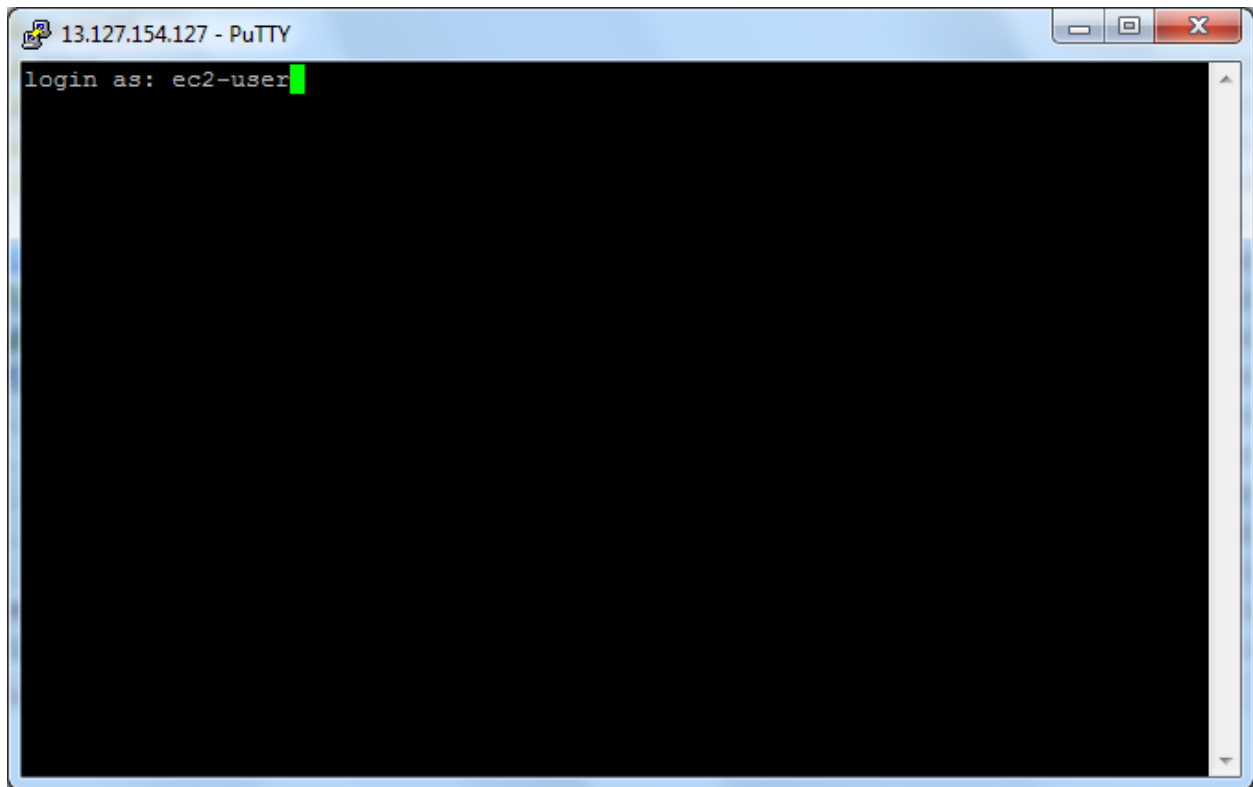
While your instances are launching you can also

- [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](#)

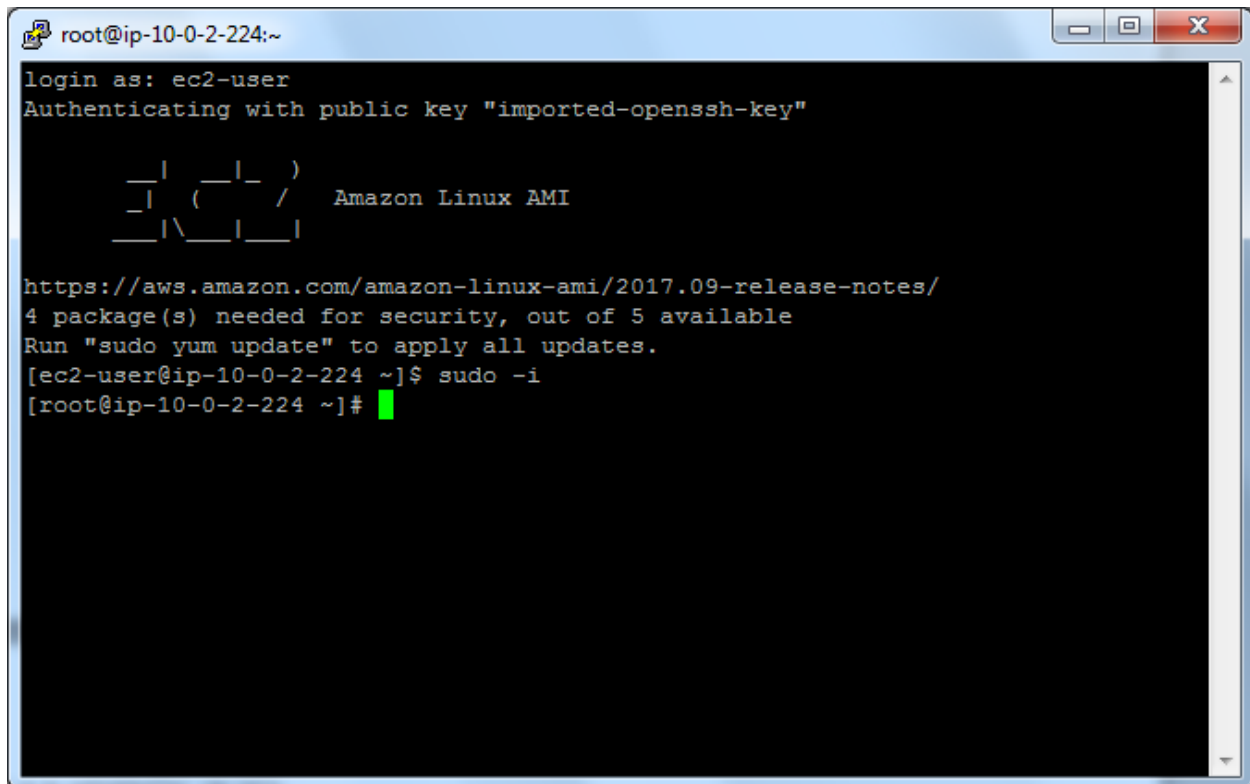
[View Instances](#)

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.

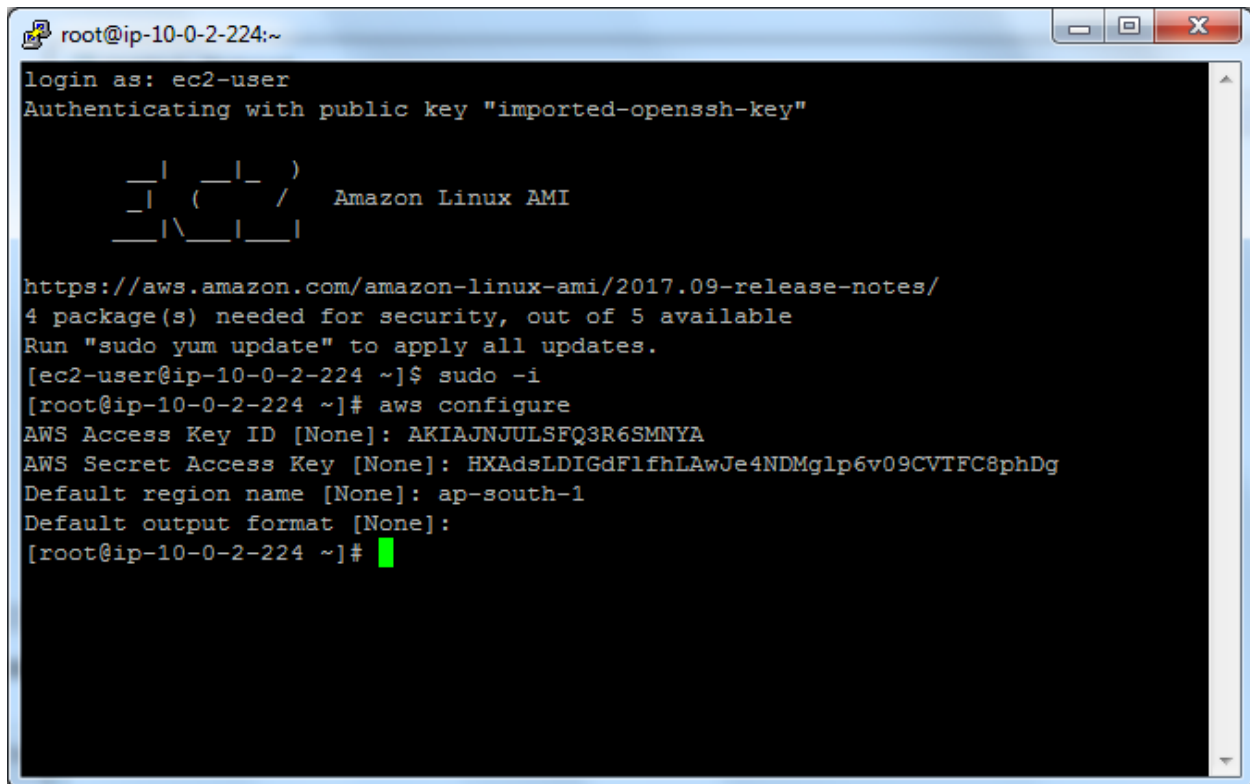


Type `sudo -i`

A terminal window titled 'root@ip-10-0-2-224:~' with standard window controls. The terminal output shows a login for 'ec2-user' using a public key. It displays the Amazon Linux AMI logo, a URL for release notes, and a message about security updates. The user runs 'sudo -i' to switch to root, indicated by a green cursor.

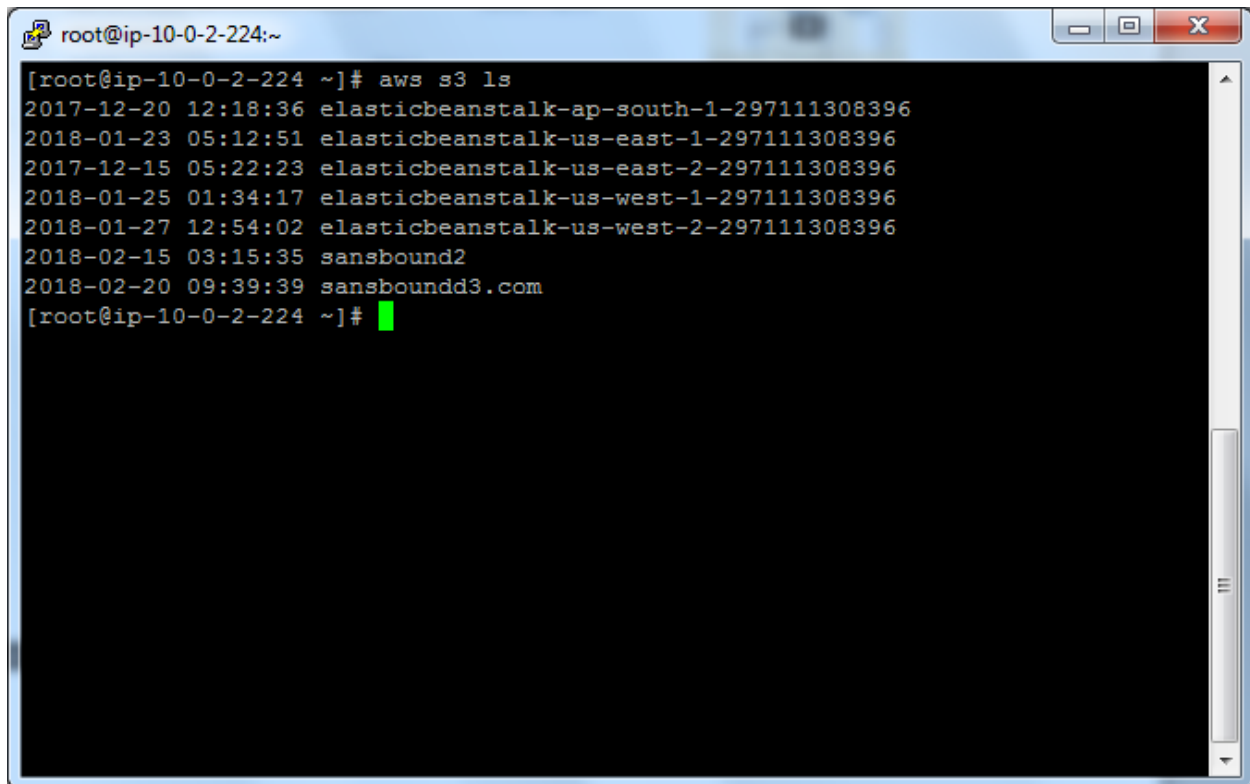
```
root@ip-10-0-2-224:~  
login as: ec2-user  
Authenticating with public key "imported-openssh-key"  
  
  _| _| _| )  
  _| ( _| /  Amazon Linux AMI  
  __| \__|__|  
  
https://aws.amazon.com/amazon-linux-ami/2017.09-release-notes/  
4 package(s) needed for security, out of 5 available  
Run "sudo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

A terminal window titled 'root@ip-10-0-2-224:~' with standard window controls. The terminal output shows the login process for 'ec2-user' using a public key. It displays the Amazon Linux AMI logo, a URL for release notes, and system update information. The user then runs 'sudo -i' to become root and 'aws configure' to set up AWS credentials. The configuration steps include entering the Access Key ID, Secret Access Key, default region (ap-south-1), and default output format. The prompt returns to root with a green cursor.

```
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 ~]#
```

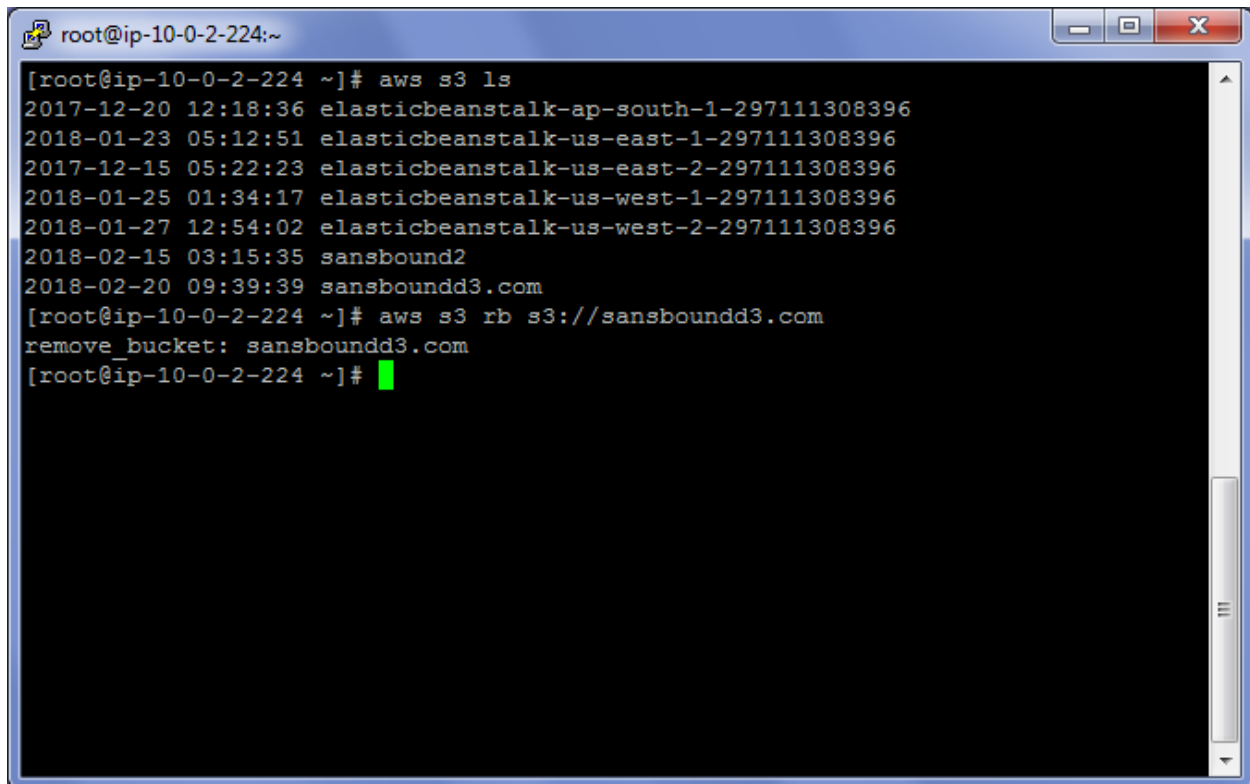
Type `aws s3 ls` command to list the bucket.

A terminal window titled 'root@ip-10-0-2-224:~' with standard window controls. The terminal displays the output of the command 'aws s3 ls'. The output lists seven S3 buckets with their creation dates, times, and ARNs. The last line shows the prompt '[root@ip-10-0-2-224 ~]#' followed by a green cursor.

```
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.

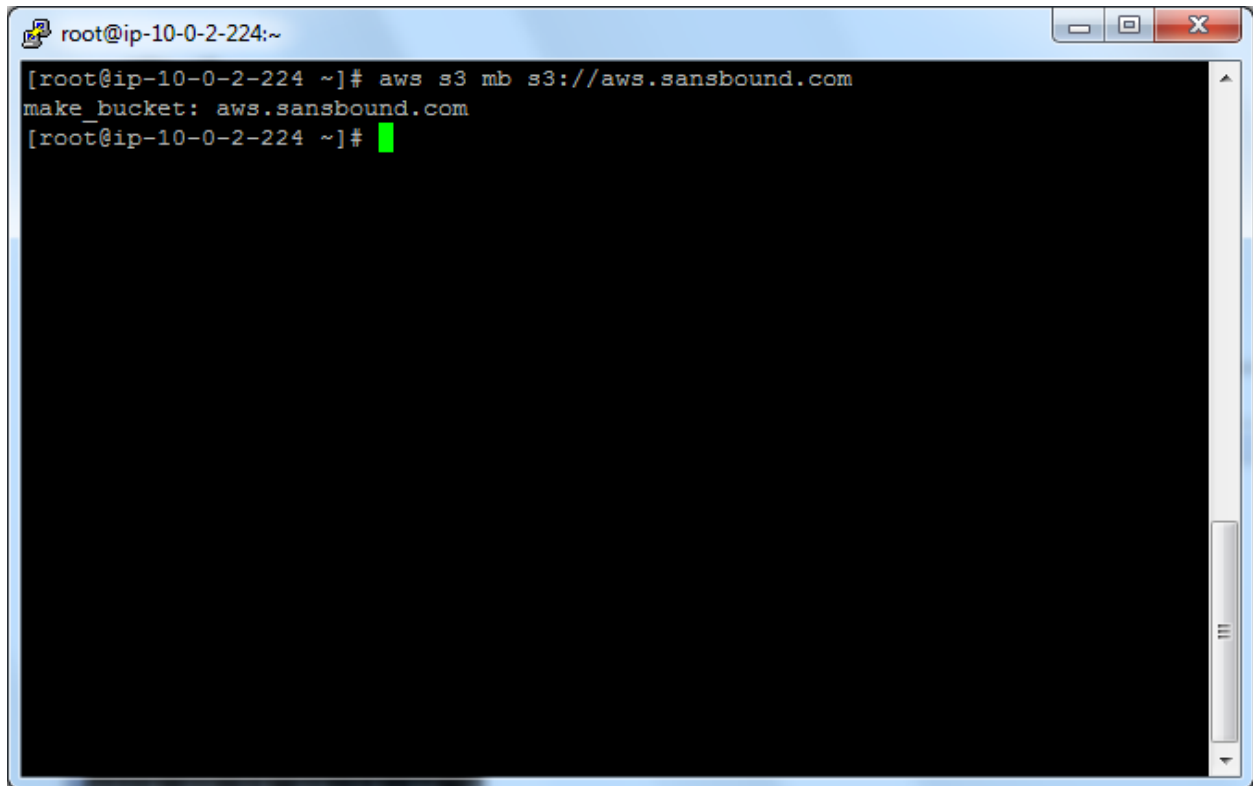
A terminal window with a blue title bar and standard window controls. The prompt is root@ip-10-0-2-224:~. The first command is aws s3 ls, which lists several S3 buckets with their creation dates and times. The second command is aws s3 rb s3://sansboundd3.com, which successfully removes the bucket sansboundd3.com. A green cursor is visible on the line following the second command.

```
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 ~]# aws s3 rb s3://sansboundd3.com  
remove_bucket: sansboundd3.com  
[root@ip-10-0-2-224 ~]#
```

Type

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

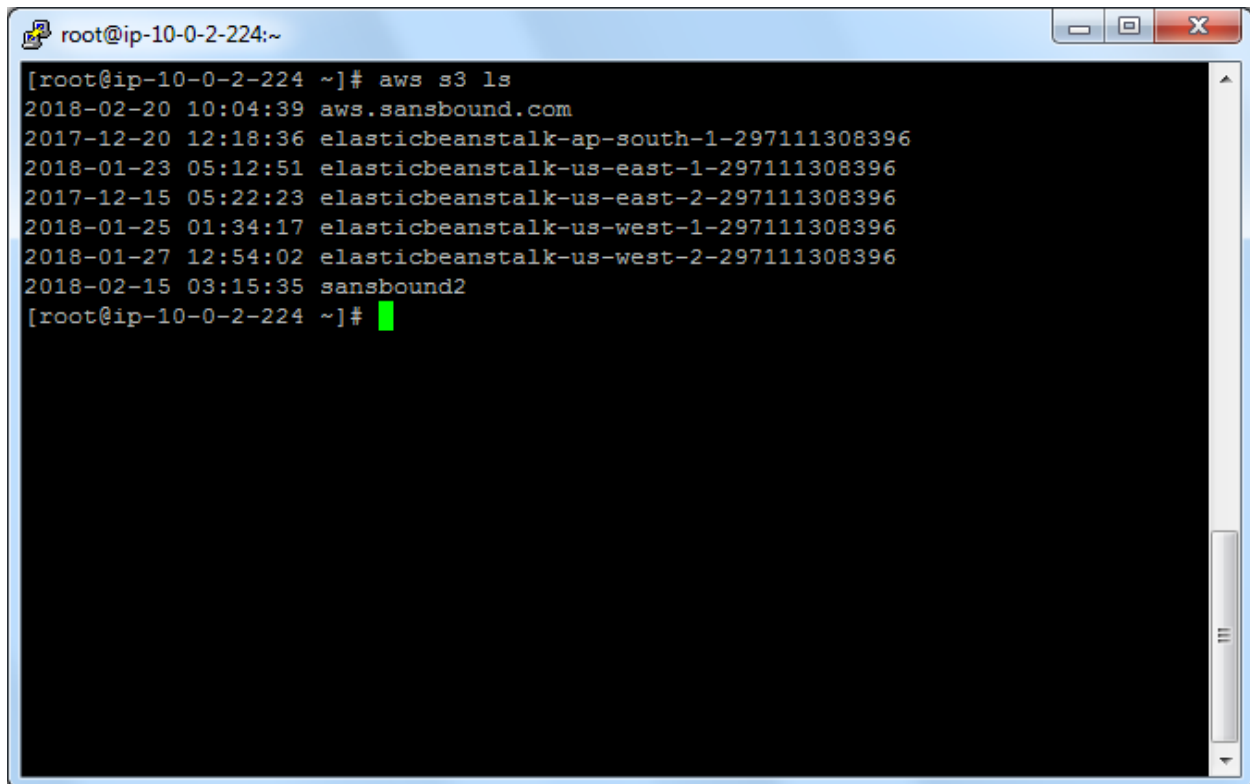
Successfully created the bucket.

A terminal window with a blue title bar and standard window controls. The prompt is 'root@ip-10-0-2-224:~'. The command 'aws s3 mb s3://aws.sansbound.com' is entered and executed. The output is 'make_bucket: aws.sansbound.com'. A green cursor is visible on the line following the prompt.

```
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 ~]#
```

Typ

Aws s3 ls

A terminal window titled 'root@ip-10-0-2-224:~' with standard window controls. The terminal displays the output of the 'aws s3 ls' command, listing seven S3 buckets with their creation dates, times, and names. The output is as follows:

```
[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.