

TASK 6.2P

CLOUD COMPUTING

Controlling Account Access Using IAM

**Task 1: Explore the users and groups, and inspect policies**

**Steps:**

- **Identify your current AWS Region.**
- **View the IAM users (user-1, user-2, user-3).**
- **Check the permissions, group memberships, and security credentials of each user.**
- **Inspect the pre-created groups: EC2-Admin, EC2-Support, S3-Support.**
- **Review attached policies:**
  - **AmazonEC2ReadOnlyAccess (read-only EC2 access).**
  - **AmazonS3ReadOnlyAccess (read-only S3 access).**
  - **EC2-Admin-Policy (Describe, Start, Stop EC2 instances).**

**IAM Dashboard**

**IAM resources**

User groups	Users	Roles	Policies	Identity providers
3	3	12	0	0

**What's new**

- AWS IAM announces support for encrypted SAML assertions. 3 months ago
- AWS CodeBuild announces support for project ARN and build ARN IAM condition keys. 3 months ago
- IAM Roles Anywhere credential helper now supports TPM 2.0. 4 months ago
- Announcing AWS STS support for ECDSA-based signatures of OIDC tokens. 5 months ago

**AWS Account**

Account ID: 992382662313  
Account Alias: Create  
Sign-in URL for IAM users in this account: https://992382662313.signin.aws.amazon.com/console

**Tools**

Policy simulator: The simulator evaluates the policies that you choose and determines the effective permissions for each of the actions that you specify.

**Additional information**

Security best practices in IAM  
IAM documentation

**Users (3)**

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
user-1	/spl66/	-	-	-	2 minutes	-
user-2	/spl66/	-	-	-	2 minutes	-
user-3	/spl66/	-	-	-	2 minutes	-

The screenshot shows the AWS IAM User Groups page. On the left, there's a navigation sidebar with sections like Identity and Access Management (IAM), Access management (User groups), and Access reports. The main area is titled "User groups (3) Info" and contains a table with three rows:

Group name	Users	Permissions	Creation time
EC2-Admin	0	Defined	4 minutes ago
EC2-Support	0	Defined	4 minutes ago
S3-Support	0	Defined	4 minutes ago

At the bottom of the page, there's a footer with links for Privacy, Terms, and Cookie preferences, along with system status and connectivity icons.

## Task 2: Add users to groups

### Task 2.1: Add user-1 to the S3-Support group

- Add user-1 to S3-Support group.
- Grants read-only access to S3 buckets.

### Task 2.2: Add user-2 to the EC2-Support group

- Add user-2 to EC2-Support group.
- Grants read-only access to EC2 resources.

### Task 2.3: Add user-3 to the EC2-Admin group

- Add user-3 to EC2-Admin group.
- Grants permission to view, start, and stop EC2 instances.

Screenshot of the AWS IAM console showing the process of adding users to a user group.

**Add users to S3-Support**

**Other users in this account (3)**

User name	Groups	Last activity	Creation time
user-1	0	None	4 minutes ago
user-2	0	None	4 minutes ago
user-3	0	None	4 minutes ago

**S3-Support**

**Summary**

User group name: S3-Support  
Creation time: April 22, 2025, 02:33 (UTC+10:00)  
ARN: arn:aws:iam::992382662313:group/spl66/S3-Support

**Users** (1)

**Users in this group (1)**

User name	Groups	Last activity	Creation time
user-1	1	None	6 minutes ago

# JASVEENA-224001588

The screenshot shows the AWS IAM User Groups page for the 'EC2-Support' group. The left sidebar includes sections for Identity and Access Management (IAM), Access management (User groups, Users, Roles, Policies, Identity providers, Account settings, Root access management), and Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity). The main content area displays the 'EC2-Support' group details, including its ARN (arn:aws:iam::992382662313:group/spl66/EC2-Support) and creation time (April 22, 2025, 02:35 (UTC+10:00)). The 'Users' tab is selected, showing a table with no resources to display. The 'Permissions' and 'Access Advisor' tabs are also present.

**EC2-Support Info**

**Summary**

User group name: EC2-Support  
Creation time: April 22, 2025, 02:35 (UTC+10:00)  
ARN: arn:aws:iam::992382662313:group/spl66/EC2-Support

**Users** | Permissions | Access Advisor

**Users in this group (0)**

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name	Groups	Last activity	Creation time
No resources to display			

**Add users to EC2-Support**

**Other users in this account (1/3)**

User name	Groups	Last activity	Creation time
user-1	1	None	7 minutes ago
<input checked="" type="checkbox"/> user-2	0	None	7 minutes ago
<input type="checkbox"/> user-3	0	None	7 minutes ago

**Add users**

CloudShell Feedback 18°C Mostly cloudy Search © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 02:41 22-04-2025

OnTrack TRAFICLIGHTCONTROLLER Remote Traffic Light Controller jass esd - Traffic Light System Guided Lab: Exploring AWS EC2 Support | IAM | Global voclabs/user3904332=s224001588@deakin.edu.au @ 9923-8266-2313 New Chrome available

JASVEENA-224001588

The screenshot shows two consecutive screenshots of the AWS IAM interface.

**Screenshot 1: Add users to EC2-Admin**

This screen shows a list of other users in the account: user-1, user-2, and user-3. The user-3 row is selected. A modal dialog is open, showing the user-3 row with columns: Groups (1), Last activity (None), and Creation time (8 minutes ago). Buttons for 'Cancel' and 'Add users' are at the bottom right.

User Name	Groups	Last Activity	Creation Time
user-1	1	None	8 minutes ago
user-2	1	None	8 minutes ago
user-3	0	None	8 minutes ago

**Screenshot 2: EC2-Admin group summary**

The main page shows the EC2-Admin group summary. It includes the user group name (EC2-Admin), creation time (April 22, 2025, 02:33 (UTC+10:00)), and ARN (arn:aws:iam::992382662313:group/spl66/EC2-Admin). The 'Users' tab is selected, showing one user added to the group: user-3. A green notification bar at the top says "1 user added to this group."

**Left Sidebar:**

- Identity and Access Management (IAM)
- Access management
  - Users
  - Roles
  - Policies
  - Identity providers
  - Account settings
  - Root access management [New](#)
- Access reports
  - Access Analyzer
    - External access
    - Unused access
    - Analyzer settings
  - Credential report
  - Organization activity

### Task 3: Sign in and test user permissions

#### Task 3.1: Get the console sign-in URL

- Locate and copy the IAM sign-in link for users.

#### Task 3.2: Test user-1 permissions

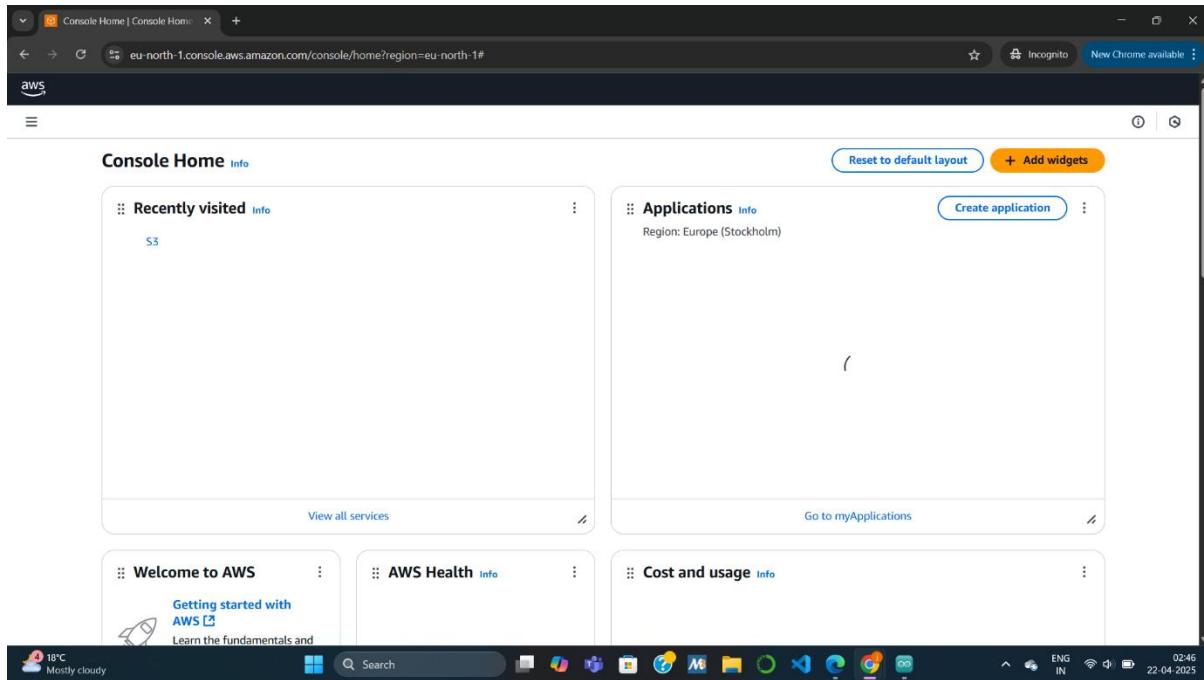
- Sign in as user-1.
- Confirm they can view S3 buckets but cannot access EC2.

#### Task 3.3: Test user-2 permissions

- Sign in as user-2.
- Confirm they can view EC2 instances but cannot stop/start them.
- Confirm they cannot access S3.

#### Task 3.4: Test user-3 permissions

- Sign in as user-3.
- Confirm they can view, stop, and start EC2 instances.
- Verifies that user-3 has proper admin access to EC2.



The screenshot shows the AWS CloudWatch Metrics console. At the top, there is a search bar and a navigation bar with options like 'Reset to default layout' and '+ Add widgets'. Below the search bar, there are two main sections: 'Recently visited' (with a link to S3) and 'Applications' (with a message about access denied). The 'Applications' section also includes a 'Create application' button and a 'Select Region' dropdown set to 'eu-north-1 (Current Region)'. Below these are sections for 'Welcome to AWS', 'AWS Health', and 'Cost and usage'. The 'Cost and usage' section shows current month costs and a cost breakdown. On the left side, there is a sidebar for 'Amazon S3' containing links for general purpose buckets, directory buckets, table buckets, access grants, access points, object lambda access points, multi-region access points, batch operations, IAM access analyzer, and block public access settings. There is also a 'Storage Lens' section with links for dashboards, storage lens groups, and AWS organizations settings. At the bottom, there is a 'Feature spotlight' section with a count of 11. The footer includes standard browser controls, a weather widget (18°C, mostly cloudy), and system status information.

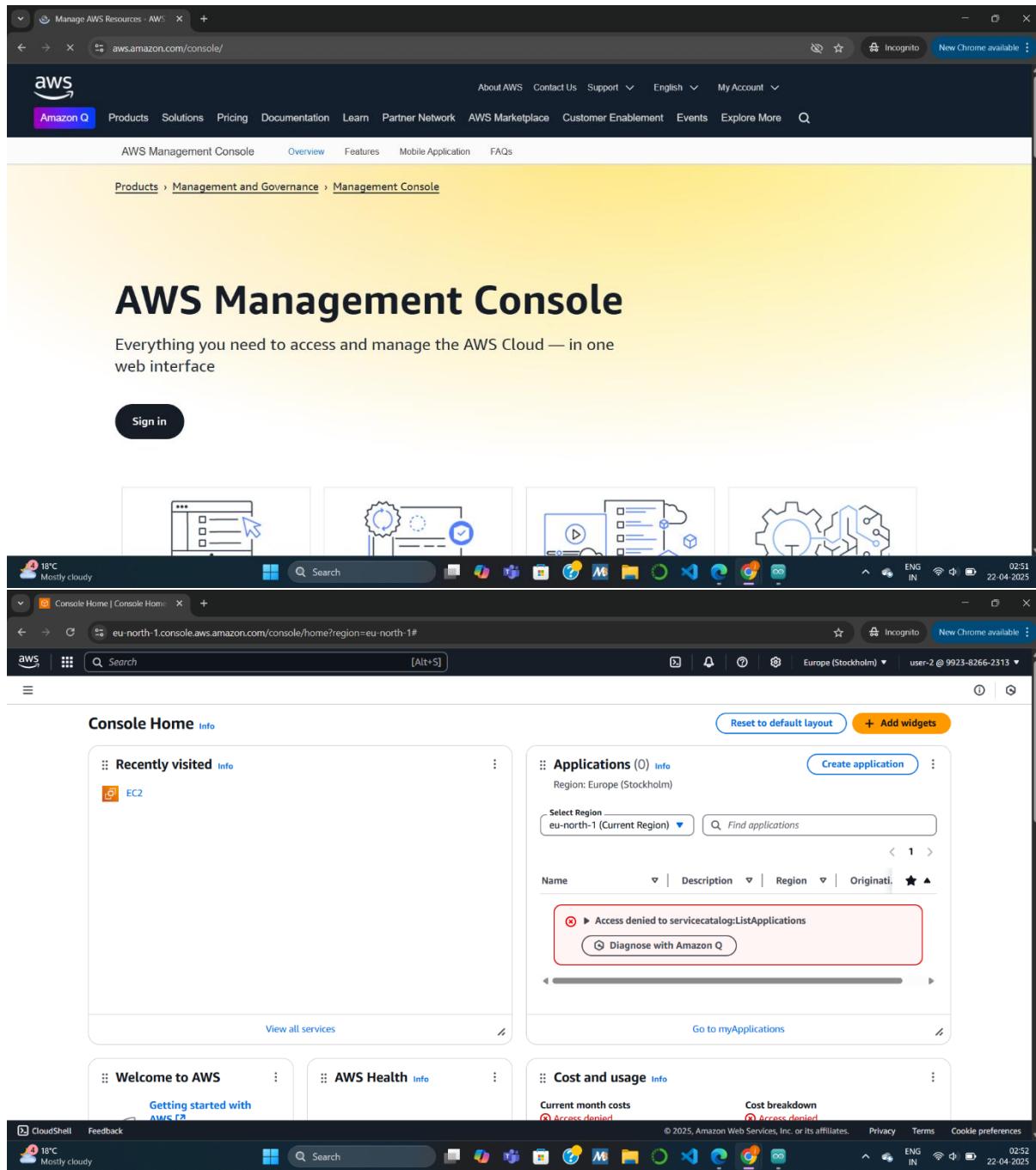
# JASVEENA-224001588

The screenshot shows a web browser window for the Amazon S3 service. The URL in the address bar is <https://us-east-1.console.aws.amazon.com/s3/buckets/c144539a3736917l10048141t1w992382662313-s3bucket-1cv8jciqirua?region=us-east-1&bucketType=general&tab=objs>. The page title is "c144539a3736917l10048141t1w992382662313-s3bucket-1cv8jciqirua". The left sidebar contains navigation links for "Amazon S3", "General purpose buckets", "Storage Lens", and "Feature spotlight". The main content area is titled "Objects (0)" and includes buttons for "Copy S3 URI", "Copy URL", "Download", "Open", "Delete", "Actions", "Create folder", and "Upload". A message states, "Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)". Below this is a search bar and a table header with columns: Name, Type, Last modified, Size, and Storage class. The message "No objects" is displayed, followed by "You don't have any objects in this bucket." and a "Upload" button.

# JASVEENA-224001588

The screenshot shows a dual-browser setup within a single CloudShell window. The top browser tab displays the Amazon S3 console at <https://us-east-1.console.aws.amazon.com/s3/buckets/c144539a3736917l10048141t1w992382662313-s3bucket-1cv8jciqirua?region=us-east-1&bucketType=general&tab=objects>. The S3 bucket named 'c144539a3736917l10048141t1w992382662313-s3bucket-1cv8jciqirua' is empty, showing a message: "No objects. You don't have any objects in this bucket." Below the table are "Upload" and "Actions" buttons. The left sidebar of the S3 console includes sections for General purpose buckets, Storage Lens, and Feature spotlight.

The bottom browser tab displays the Amazon EC2 console at <https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances>. The EC2 dashboard shows a message: "You are not authorized to perform this operation. User: arn:aws:iam::992382662313:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action". The left sidebar of the EC2 console includes sections for EC2, Instances, Images, and Elastic Block Store.



The screenshot shows the AWS EC2 Dashboard for the eu-north-1 region. The left sidebar includes links for Dashboard, Instances (with sub-links for Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images, and Elastic Block Store. The main content area has a blue header bar with a message: "You can change your default landing page for EC2." with "Permanently dismiss" and "Change landing page" buttons. Below this is the "Resources" section, which displays the following count for the Europe (Stockholm) Region:

	Instances (running)	Auto Scaling Groups	Capacity Reservations
Instances	0	0	0
Dedicated Hosts	0	Elastic IPs	0
Key pairs	0	Load balancers	0
Security groups	1	Snapshots	0
			Volumes
			0

Below the resources are sections for "Launch instance" (with "Launch instance" and "Migrate a server" buttons) and "Service health" (which shows an error: "An error occurred: An error occurred retrieving service health information" with a "Diagnose with Amazon Q" button). The right side features the "Account attributes" section with links for Default VPC, Settings (Data protection and security, Allowed AMIs, Zones, EC2 Serial Console, Default credit specification, EC2 console preferences), and Explore AWS (with a link to Optimize EC2 Cost with Spot Instances and EC2 Auto Scaling). The bottom of the screen shows the Windows taskbar with various pinned icons and the system tray.

# JASVEENA-224001588

The screenshot shows two stacked browser windows for the AWS EC2 service.

**Top Window: Instances (1) Info**

- Left Sidebar:** EC2 navigation menu with options like Dashboard, EC2 Global View, Events, Instances (selected), Images, and Elastic Block Store.
- Table Headers:** Instances (1) Info, Last updated less than a minute ago, Connect, Instance state, Actions, Launch instances.
- Table Rows:** One instance listed: i-0b715f2c6a522eea1, Running, t2.micro, 2/2 checks passed, us-east-1a, ec2-52-1-.

**Bottom Window: Instance summary for i-0b715f2c6a522eea1**

- Left Sidebar:** EC2 navigation menu with options like Dashboard, EC2 Global View, Events, Instances (selected), Images, and Elastic Block Store.
- Instance Summary:** Updated less than a minute ago.
  - Instance ID:** i-0b715f2c6a522eea1
  - IPv6 address:** -
  - Hostname type:** IP name: ip-10-1-11-100.ec2.internal
  - Answer private resource DNS name:** -
  - Auto-assigned IP address:** 52.1.215.204 [Public IP]
  - IAM Role:** -
  - IMDSv2:** -
- Right Side:** Action buttons for Connect, Instance state (dropdown showing Stop instance, Start instance, Reboot instance, Hibernate instance, Terminate (delete) instance), Public IPv4 address (10.1.11.100), Private IPv4 address (52.1.215.204), Public IPv4 DNS (ec2-52-1-21), Private IP DNS name (ip-10-1-11-100.ec2.internal), Instance type (t2.micro), VPC ID (vpc-08583b4e79020fce (Lab VPC)), Subnet ID (subnet-0d6f3c3a5ef052aa6 (Public Subnet 1)), and Instance ARN.
- Bottom Status:** © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences ENG IN 02:55 22-04-2025

**Instance details | EC2 | us-east-1**

us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#instanceDetailsInstanceId=i-0b715f2c6a522eea1

**EC2**

- Dashboard
- EC2 Global View
- Events
- Instances**
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity Reservations
- Images
- AMIs
- AMI Catalog
- Elastic Block Store
- Volumes
- Snapshots
- Lifecycle Manager

**Diagnose with Amazon Q**

**Failed to stop the Instance i-0b715f2c6a522eea1**

You are not authorized to perform this operation. User: arn:aws:iam::992382662313:user/spl66/user-2 is not authorized to perform: ec2:StopInstances on resource: arn:aws:ec2:us-east-1:992382662313:instance/i-0b715f2c6a522eea1 because no identity-based policy allows the ec2:StopInstances action. Encoded authorization failure message: VzUw1Ws0YqfE53P-C0Q1A483dJcrh1WdNkWbw71ExBa\_srV3fLGA2wpoU1UNMgQCarnUVPyfIvgJ9fc1Pu85PmfhLqASy2MSuU\_GflLitFI9Km2jfp0r2QGxXuAMH8cmrVubazTzELUwOgOnQJN9JFkJKm1qCy\_HqG2b58mPky2zWv1AeU92QuNGZV3lbMYGPWP1ljy9O4glU43DZxosM4vR7cMC3amzc-PR-Zz6B1BCbw2BIRrq7WHy5hk2W1LZUP16nolR3Ccmu8sJXw4oTyl2tHt694qfvgFWetZkkvXy6ku2Prnjz\_HG1icwY\_pfua1Y8R1b9Wyurh0h67heg-7bqYqYAC7\_OPkuldKv88fkksQFSOkn8ovEXAO1Drp89TJA1DJ09Ao1tx1wfECt06h9unP3QJhdJsw240sgf\_B-CqGQpLWt6S63U\_Dk2MlVeWsjMjsOLflluxQRoz5azXISjewWEoawW8euckiA57PSuJowz\_r0hfOSYJHrdeY0s5hn96UVWpxXPKBmB- yoDWSYu3m0H21QsBnxRpFCQ07hGy2\_dpl11BknBKIPUBD1P9kknT5cdy2s6LBUDpuEV99Cr98l2PoMtK3WVnxzL0K28CdYxxz3BUE\_EX1rnC6Bpkuy7Zoog6az7f58ASrtVz66TC5bCjt4o4w6VpaJo-ehAkmmMeso\_TVbu3FRVYzK7l0/VvGKEAW-b0KeNmfb2Lc1HC- 865Sbwg83ISB9A84rBrxTM5ksavm9RtdPDglhw\_X5QgC3Kk\_L0PM2907XUcmkZ-CLVFBfytd\_b6t5Wyo1NkB-EFez2MOz75najlICP9-83NzuxXcpqmspq9fqfQ)1nTXydtgt30egba53219PsRGCBwqfnvA- 2uQAVDqmtXqaleSr95Ylk5CE2Loc8SBYQgjAywJfhN2Gld8Coy3yt5xbFelQGpJkfJT5t3aDORescg0L\_ov5SgwTzwojAM9spsWctNbD3ak

**Instance summary for i-0b715f2c6a522eea1**

Updated less than a minute ago

<b>Instance ID</b>	52.1.215.204   <a href="#">open address</a>	<b>Public IPv4 address</b>	10.1.11.100   <a href="#">open address</a>
<b>IPv6 address</b>	-	<b>Instance state</b>	Running
<a href="#">View details</a>		<a href="#">Private IP/DNS names (IPv4 and IPv6)</a>	

**Cloud Home | Console Home**

**Console Home**

**Recently visited**

- EC2
- S3

**Applications (0)**

Region: US East (N. Virginia)

Select Region: us-east-1 (Current Region)

**Welcome to AWS**

Getting started with AWS

**AWS Health**

**Cost and usage**

Current month costs: Access denied

Cost breakdown: Access denied

**Diagnose with Amazon Q**

The screenshot shows the AWS S3 console interface. On the left, a sidebar titled "Amazon S3" lists various bucket types: General purpose buckets, Directory buckets, Table buckets, Access Grants, Access Points, Object Lambda Access Points, Multi-Region Access Points, Batch Operations, and IAM Access Analyzer for S3. Below this, there's a link to "Block Public Access settings for this account". Under "Storage Lens", there are links for Dashboards, Storage Lens groups, and AWS Organizations settings. A "Feature spotlight" section is also present.

The main content area displays an "Account snapshot - updated every 24 hours" with a link to "View Storage Lens dashboard". It includes a note that "Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets." Below this, there are tabs for "General purpose buckets" (selected) and "Directory buckets".

The "General purpose buckets" table lists one item:

Name	AWS Region	IAM Access Analyzer	Creation date
c144559a373691710048141t1w992382662313-s3bucket-1cv8jciqinua	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	April 22, 2025, 02:33:31 (UTC+10:00)

At the bottom of the browser window, the Windows taskbar is visible, showing icons for File Explorer, Edge, and other applications. The system tray shows the date and time as "22-04-2025".

**Instances | EC2 | us-east-1**

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

**EC2 > Instances**

**Instances Info**

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

All states

Name | Instance ID | Instance state | Instance type | Status check | Alarm status | Availability Zone | Public IPv4

You are not authorized to perform this operation. User: arn:aws:iam::992382662313:user/spl66/user-1 is not authorized to perform: ec2:DescribeInstances because no identity-based policy allows the ec2:DescribeInstances action

Select an instance

**Console Home | Console Home**

18°C Mostly cloudy

Search

Reset to default layout + Add widgets

**Recently visited**

EC2

**Applications (0)**

Create application

Region: US East (N. Virginia)

Select Region: us-east-1 (Current Region)

Find applications

Access denied to servicecatalog>ListApplications

Diagnose with Amazon Q

**Welcome to AWS**

Getting started with AWS

**AWS Health**

**Cost and usage**

Cost breakdown

Current month costs

Access denied

CloudShell Feedback

18°C Mostly cloudy

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 02:59 22-04-2025

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

ENG IN 03:01 22-04-2025

# JASVEENA-224001588

The screenshot shows the AWS EC2 Instances page. On the left, a sidebar menu is open under the 'EC2' section, showing options like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, and AMI Catalog. Below these, the 'Elastic Block Store' section is visible with Volumes, Snapshots, and Lifecycle Manager. The main content area displays a table titled 'Instances (1) Info'. The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, Availability Zone, and Public IPv4. One row is shown, corresponding to the instance i-0b715f2c6a522eea1, which is 'Running' on an 't2.micro' instance type with an 'ec2-52-1-21' public IP. A search bar at the top of the table allows filtering by attribute or tag. Action buttons include 'Connect', 'Instance state', 'Actions', and 'Launch instances'. Below the table, a modal window titled 'Select an instance' is partially visible.

**Instances (1) Info**

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
	i-0b715f2c6a522eea1	Running	t2.micro	2/2 checks passed	User: arn:aws:	us-east-1a	ec2-52-1-21

**Select an instance**

**Instance summary for i-0b715f2c6a522eea1**

**Stop instance**

Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.

Instance ID: i-0b715f2c6a522eea1 | Stop protection: Off (Can stop instance)

**You will be billed for associated resources**

After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.

**Associated resources**

You will continue to incur charges for these resources while the instance is stopped.

Cancel | Stop

© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback 18°C Mostly cloudy 03:01 22-04-2025

Instances (1) i-0b715f2c6a522eea1

EC2 Instances i-0b715f2c6a522eea1

CloudShell Feedback 18°C Mostly cloudy 03:02 22-04-2025

The screenshot shows the AWS EC2 Instances details page for an instance with ID i-0b715f2c6a522eea1. A green success message at the top indicates "Successfully initiated stopping of i-0b715f2c6a522eea1". The main content area displays various instance details:

- Instance summary for i-0b715f2c6a522eea1**
- Public IPv4 address:** 52.1.215.204 | [open address](#)
- Private IPv4 addresses:** 10.1.11.100
- Public IPv4 DNS:** ec2-52-1-215-204.compute-1.amazonaws.com | [open address](#)
- Private IP DNS name (IPv4 only):** ip-10-1-11-100.ec2.internal
- Instance state:** Stopping
- Instance type:** t2.micro
- VPC ID:** vpc-08583b4e79020fce (Lab VPC)
- Elastic IP addresses:** -
- AWS Compute Optimizer finding:** User: arnaws:iam::992382662313:user/spl66/user-3 is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: \* because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action
- Auto Scaling Group name:** -

The left sidebar shows navigation links for EC2 (Dashboard, EC2 Global View, Events, Instances, Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations), Images, and Elastic Block Store.