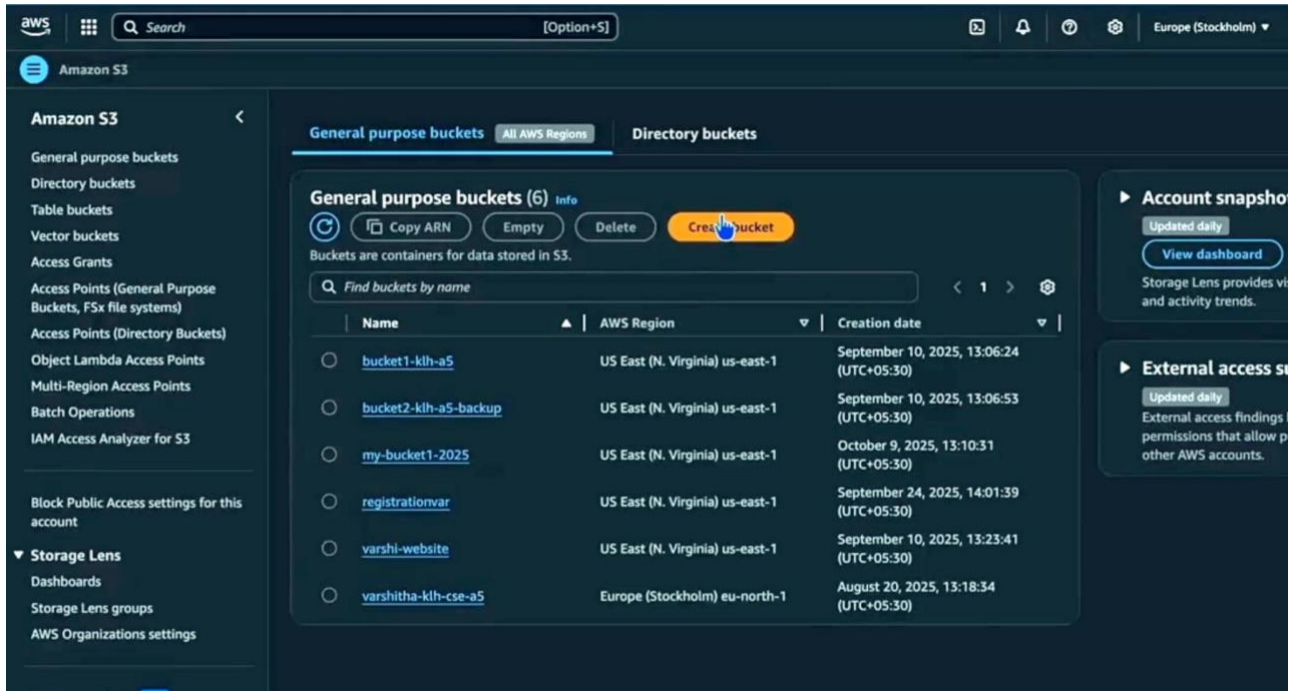


# Create a Secure EC2 Instance with S3 Access using IAM

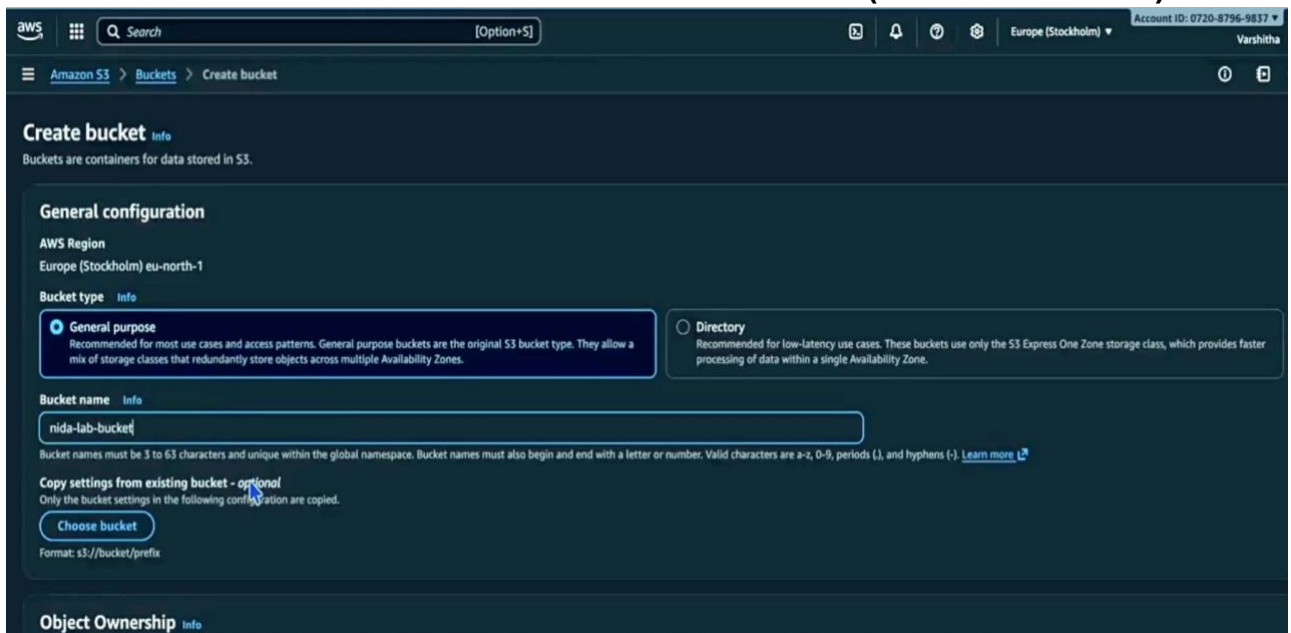
## 1. S3 Console — List of Buckets



The screenshot shows the Amazon S3 console interface. On the left is a navigation menu with options like 'General purpose buckets', 'Directory buckets', 'Table buckets', 'Vector buckets', 'Access Grants', 'Access Points (General Purpose Buckets, FSx file systems)', 'Access Points (Directory Buckets)', 'Object Lambda Access Points', 'Multi-Region Access Points', 'Batch Operations', 'IAM Access Analyzer for S3', 'Block Public Access settings for this account', 'Storage Lens', 'Dashboards', 'Storage Lens groups', and 'AWS Organizations settings'. The main area is titled 'General purpose buckets (6)' and includes buttons for 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. Below this is a search bar and a table listing six buckets. The table has columns for 'Name', 'AWS Region', and 'Creation date'. The buckets listed are: 'bucket1-klh-a5', 'bucket2-klh-a5-backup', 'my-bucket1-2025', 'registrationvar', 'varshi-website', and 'varshitha-klh-cse-a5'. To the right of the table are sections for 'Account snapshot' and 'External access settings'.

Name	AWS Region	Creation date
<a href="#">bucket1-klh-a5</a>	US East (N. Virginia) us-east-1	September 10, 2025, 13:06:24 (UTC+05:30)
<a href="#">bucket2-klh-a5-backup</a>	US East (N. Virginia) us-east-1	September 10, 2025, 13:06:53 (UTC+05:30)
<a href="#">my-bucket1-2025</a>	US East (N. Virginia) us-east-1	October 9, 2025, 13:10:31 (UTC+05:30)
<a href="#">registrationvar</a>	US East (N. Virginia) us-east-1	September 24, 2025, 14:01:39 (UTC+05:30)
<a href="#">varshi-website</a>	US East (N. Virginia) us-east-1	September 10, 2025, 13:23:41 (UTC+05:30)
<a href="#">varshitha-klh-cse-a5</a>	Europe (Stockholm) eu-north-1	August 20, 2025, 13:18:34 (UTC+05:30)

## 2. Create S3 Bucket — Enter bucket name (nida-lab-bucket)



The screenshot shows the 'Create bucket' page in the Amazon S3 console. The page title is 'Create bucket' and it includes a sub-header 'Buckets are containers for data stored in S3.' The 'General configuration' section shows the 'AWS Region' set to 'Europe (Stockholm) eu-north-1'. Under 'Bucket type', the 'General purpose' option is selected, with a description: 'Recommended for most use cases and access patterns. General purpose buckets are the original S3 bucket type. They allow a mix of storage classes that redundantly store objects across multiple Availability Zones.' The 'Directory' option is also visible, with a description: 'Recommended for low-latency use cases. These buckets use only the S3 Express One Zone storage class, which provides faster processing of data within a single Availability Zone.' The 'Bucket name' field is filled with 'nida-lab-bucket'. Below this, there is a note: 'Bucket names must be 3 to 63 characters and unique within the global namespace. Bucket names must also begin and end with a letter or number. Valid characters are a-z, 0-9, periods (.), and hyphens (-). Learn more.' There is a section for 'Copy settings from existing bucket - optional' with a 'Choose bucket' button. At the bottom, there is a section for 'Object Ownership'.

### 3. Bucket Created Successfully

Successfully created bucket "nida-lab-bucket"  
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

General purpose buckets (7) [Info](#) [Copy ARN](#) [Empty](#) [Delete](#) [Create bucket](#)

Buckets are containers for data stored in S3.

Find buckets by name

Name	AWS Region	Creation date
<a href="#">bucket1-klh-a5</a>	US East (N. Virginia) us-east-1	September 10, 2025, 13:06:24 (UTC+05:30)
<a href="#">bucket2-klh-a5-backup</a>	US East (N. Virginia) us-east-1	September 10, 2025, 13:06:53 (UTC+05:30)
<a href="#">my-bucket1-2025</a>	US East (N. Virginia) us-east-1	October 9, 2025, 13:10:31 (UTC+05:30)
<a href="#">nida-lab-bucket</a>	Europe (Stockholm) eu-north-1	November 2, 2025, 11:54:02 (UTC+05:30)
<a href="#">registrationvar</a>	US East (N. Virginia) us-east-1	September 24, 2025, 14:01:39 (UTC+05:30)
<a href="#">varshi-website</a>	US East (N. Virginia) us-east-1	September 10, 2025, 13:23:41 (UTC+05:30)
<a href="#">varshitha-klh-cse-a5</a>	US East (N. Virginia) us-east-1	August 20, 2025, 13:18:34 (UTC+05:30)

**Account snapshot** [Info](#) [View dashboard](#)  
Updated daily  
Storage Lens provides visibility into storage usage and activity trends.

**External access summary - new** [Info](#)  
Updated daily  
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

### 4. Upload File to S3 — Add sample.rtf

eu-north-1.console.aws.amazon.com/s3/upload/nida-lab-bucket?region=eu-north-1

Upload [Info](#)

Add the files and folders you want to upload to S3. To upload a file larger than 160GB, use the AWS CLI, AWS SDKs or Amazon S3 REST API. [Learn more](#)

Drag and drop files and folders you want to upload here, or choose [Add files](#) or [Add folder](#).

**Files and folders (1 total, 389.0 B)** [Remove](#) [Add files](#) [Add folder](#)

All files and folders in this table will be uploaded.

Find by name

Name	Folder	Type	Size
<input type="checkbox"/> sample.rtf	-	text/rtf	389.0 B

**Destination** [Info](#)

**Destination**  
[s3://nida-lab-bucket](#)

**Destination details**  
Bucket settings that impact new objects stored in the specified destination.

**Permissions**

## 5. Upload Status — Upload succeeded

**Upload: status**

After you navigate away from this page, the following information is no longer available.

**Summary**

Destination	Succeeded	Failed
s3://nida-lab-bucket	1 file, 389.0 B (100.00%)	0 files, 0 B (0%)

**Files and folders** (1 total, 389.0 B)

Find by name

Name	Folder	Type	Size	Status	Error
sample.rtf	-	text/rtf	389.0 B	Succeeded	-

## 6. IAM Console

**Roles (11)**

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
<a href="#">AWSServiceRoleForAPIGateway</a>	AWS Service: ops.apigateway (Service)	-
<a href="#">AWSServiceRoleForResourceExplorer</a>	AWS Service: resource-explorer-2 (Service)	17 minutes ago
<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linker)	-
<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service)	-
<a href="#">Ec2s3Access</a>	AWS Service: ec2	-
<a href="#">registrationFunction-role-75zvckz3</a>	AWS Service: lambda	-
<a href="#">registrationFunction-role-801u962l</a>	AWS Service: lambda	38 days ago
<a href="#">registrationFunction-role-ljzkygxs</a>	AWS Service: lambda	-
<a href="#">s3crr_role_for_bucket1-klh-a5</a>	AWS Service: s3	-
<a href="#">s3crr_role_for_bucket1-klh-a5_1</a>	AWS Service: s3	52 days ago

## 7. Create Role — Select trusted entity (AWS service → EC2)

The screenshot shows the 'Select trusted entity' step in the AWS IAM console. The left sidebar indicates the current step is 'Step 1: Select trusted entity', with 'Step 2: Add permissions' and 'Step 3: Name, review, and create' following. The main content area is titled 'Select trusted entity' and includes an 'Info' link. Under the 'Trusted entity type' section, five options are listed: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. The 'AWS service' option is highlighted with a blue border and a radio button. Below this, the 'Use case' section is visible, with a dropdown menu set to 'EC2'.

Step 1  
● Select trusted entity  
○ Step 2: Add permissions  
○ Step 3: Name, review, and create

### Select trusted entity [Info](#)

**Trusted entity type**

- ☒ **AWS service**  
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**  
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**  
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**  
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**  
Create a custom trust policy to enable others to perform actions in this account.

**Use case**  
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

**Service or use case**  
EC2

## 8. Add Permissions — Attach AmazonS3FullAccess policy

The screenshot shows the 'Add permissions' step in the AWS IAM console. The left sidebar indicates the current step is 'Step 2: Add permissions', with 'Step 1: Select trusted entity' and 'Step 3: Name, review, and create' following. The main content area is titled 'Add permissions' and includes an 'Info' link. Under the 'Permissions policies (1/1083)' section, a search bar contains 'AmazonS3F' and a filter dropdown is set to 'All types'. Below the search results, a table lists the policies. The 'AmazonS3FullAccess' policy is selected and highlighted with a blue border. The table columns are 'Policy name', 'Type', and 'Description'. Below the table, there is a section for 'Set permissions boundary - optional'. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

Step 1  
○ Select trusted entity  
● Add permissions  
○ Step 3: Name, review, and create

### Add permissions [Info](#)

**Permissions policies (1/1083) [Info](#)**

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

Filter by Type  
AmazonS3F All types 1 match

<input checked="" type="checkbox"/>	Policy name <a href="#">↗</a>	Type	Description
<input checked="" type="checkbox"/>	AmazonS3FullAccess	AWS managed	Provides full access to all buckets via t...

► Set permissions boundary - optional

Cancel Previous Next

## 9. Role Details — Enter role name and review trust policy

**Role name**  
Enter a meaningful name to identify this role.  
  
Maximum 64 characters. Use alphanumeric and '+', '@', '-' characters.

**Description**  
Add a short explanation for this role.  
  
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: '\_', '=', '@', '/', '[', ']', '#', '%', '^', '~', '``'.

**Step 1: Select trusted entities** Edit

**Trust policy**

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

## 10. Role Created — Confirmation in Roles list

**Role Awsec2s3 created.** View role X

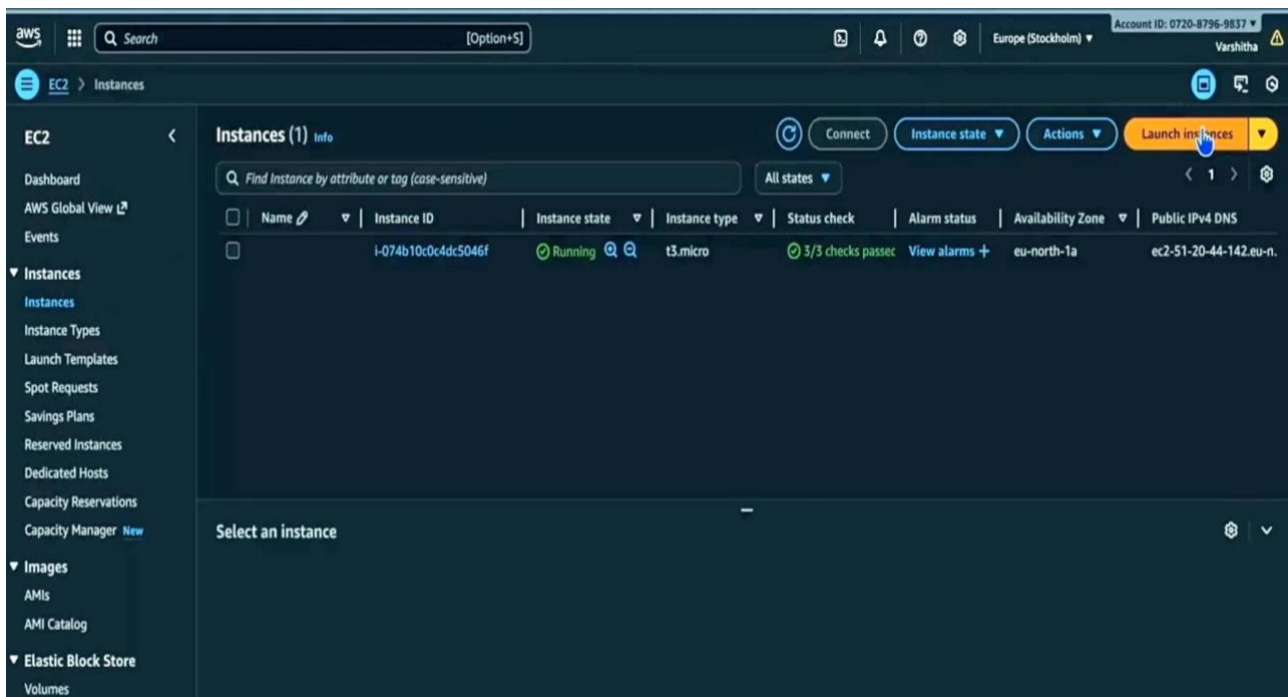
**Roles (12)** Info Refresh Delete Create role

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

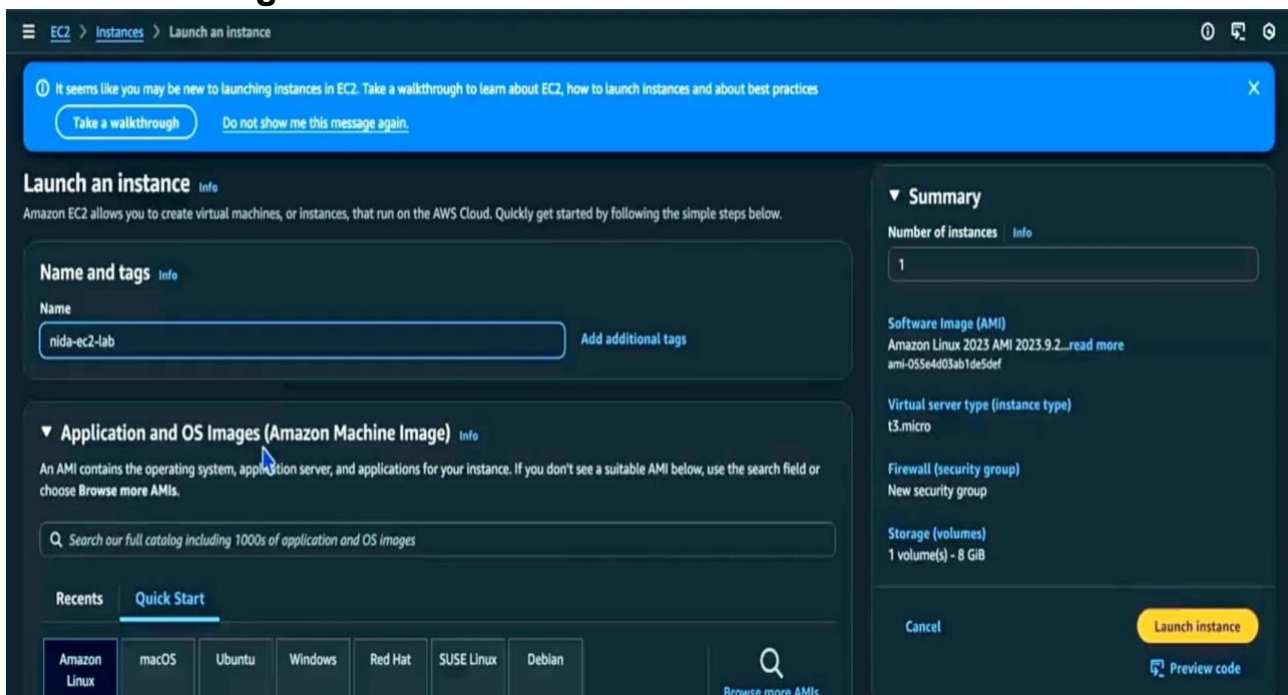
<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	<a href="#">Awsec2s3</a>	AWS Service: ec2	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForAPIGateway</a>	AWS Service: ops.apigateway (Service)	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForResourceExplorer</a>	AWS Service: resource-explorer-2 (Service)	18 minutes ago
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linker)	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service)	-
<input type="checkbox"/>	<a href="#">Ec2s3Access</a>	AWS Service: ec2	-
<input type="checkbox"/>	<a href="#">registrationFunction-role-75zvckz3</a>	AWS Service: lambda	-
<input type="checkbox"/>	<a href="#">registrationFunction-role-801u962l</a>	AWS Service: lambda	38 days ago



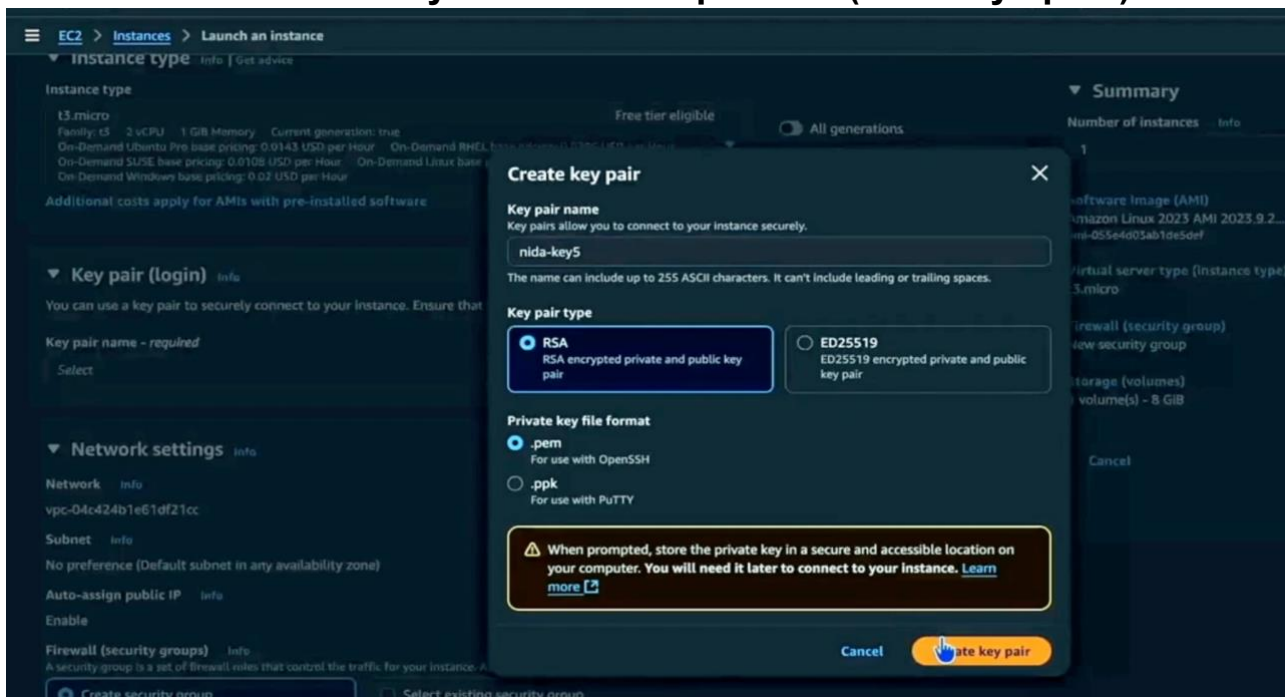
## 11. EC2 Console



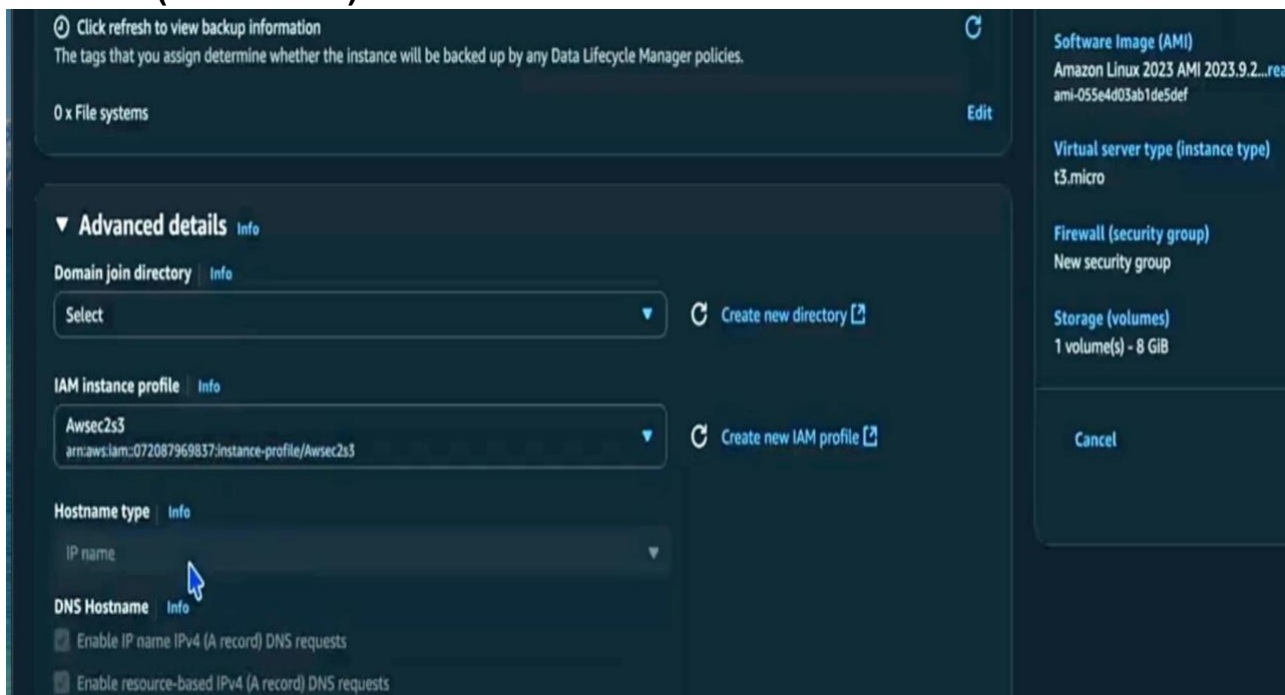
## 12. Launch Instance — Name, AMI selection and basic settings



### 13. Create Key Pair — Save .pem file (nida-key5.pem)




### 14. Advanced Details — IAM instance profile (Awsec2s3) attached




## 15. SSH Terminal — Successful SSH connection to EC2 (ec2-user)

```
. . . Downloads — ec2-user@ip-172-31-26-127:~ — ssh -i nida-key5.pem ec...  
Last login: Sun Nov 2 11:13:05 on console  
[(base) syednida@192 ~ % cd Downloads  
[(base) syednida@192 Downloads % chmod 400 nida-key5.pem  
[(base) syednida@192 Downloads % ssh -i "nida-key5.pem" ec2-user@51.20.132.242  
The authenticity of host '51.20.132.242 (51.20.132.242)' can't be established.  
ED25519 public key fingerprint is SHA256:EKpmkjckO3XaRZbbF9Nt/lzK8C1sGgfvYV2a/bLdyM8.  
This key is not known by any other names.  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '51.20.132.242' (ED25519) to the list of known hosts.
```



```
Amazon Linux 2023  
  
https://aws.amazon.com/linux/amazon-linux-2023
```



```
[ec2-user@ip-172-31-26-127 ~]$ █
```

## 16. AWS CLI — Verify S3 access (aws s3 ls and list object)

```
[ec2-user@ip-172-31-26-127 ~]$ aws s3 ls
2025-09-10 07:42:13 bucket1-klh-a5
2025-09-10 07:42:02 bucket2-klh-a5-backup
2025-10-09 07:40:32 my-bucket1-2025
2025-11-02 06:24:03 nida-lab-bucket
2025-09-24 08:31:41 registrationvar
2025-09-10 08:09:58 varshi-website
2025-08-20 07:48:37 varshitha-klh-cse-a5
[ec2-user@ip-172-31-26-127 ~]$ aws s3 ls s3://nida-lab-bucket
2025-11-02 06:24:32      389 sample.rtf
[ec2-user@ip-172-31-26-127 ~]$
```



## Conclusion

All steps were completed: an S3 bucket was created and a sample file uploaded. An IAM role with S3 access was created and attached to an EC2 instance. The EC2 instance successfully accessed the S3 bucket using the AWS CLI, confirming the configuration