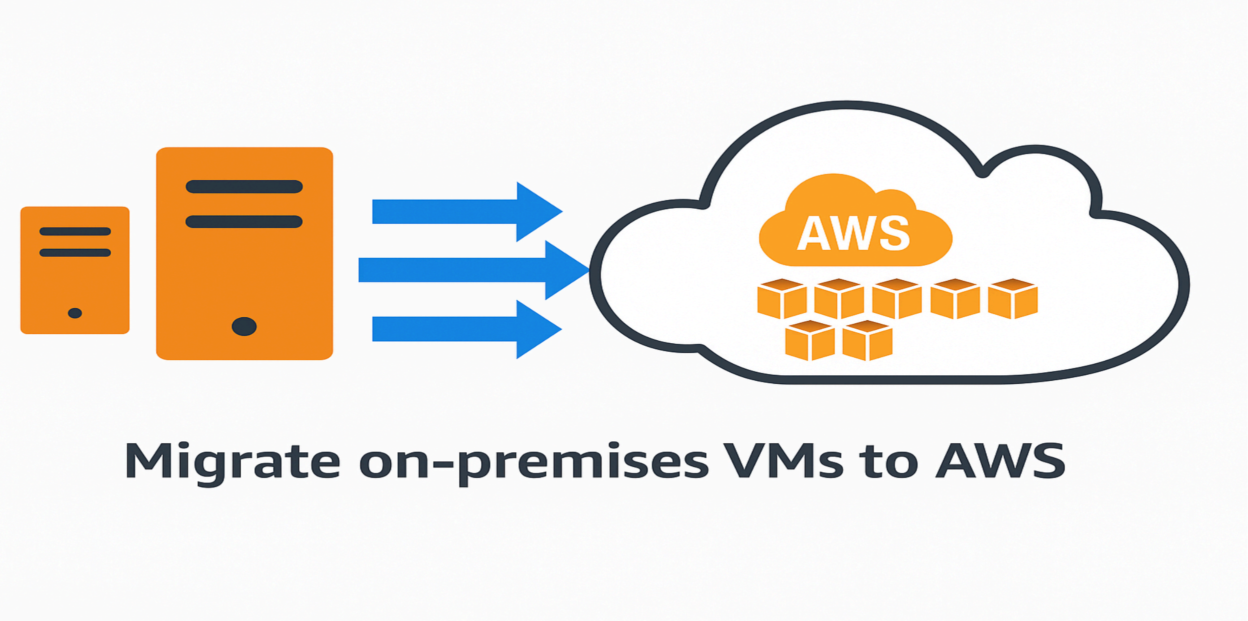
AWS Server Migration

Project Objective

Migrate existing on-premises VM-based applications to AWS using AWS VM Import to preserve current software, configurations, and settings, following AWS-native tools and best practice



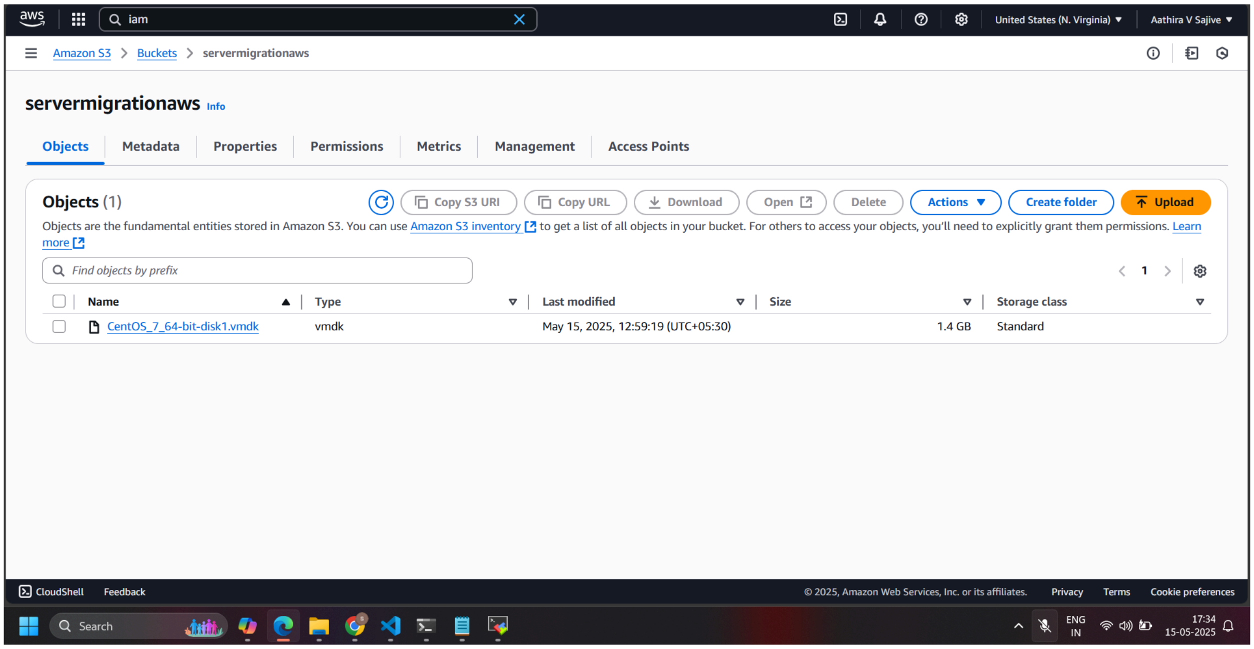
Prerequisites

1. **AWS Account**
    - AWS account with necessary **IAM permissions** to use VM Import/Export, EC2, S3, and IAM. sign up for a free account here.
2. **Source VM Requirements**
    - Supported virtualization formats:
        - VMware (.vmdk)
        - Hyper-V (.vhd/.vhdx)
        - RAW (.raw)

3. **AWS CLI Setup**
    - AWS CLI installed and configured with access credentials.
4. **S3 Bucket**
    - Create an S3 bucket to store VM image files temporarily.
5. **VM Import Role**
    - Create a service role named `vmimport` with a trust policy allowing VM Import/Export.
    - Attach an IAM policy that allows access to the S3 bucket and EC2 actions.

Exporting VM & Uploading to Amazon S3

Based on the virtualization platform you're using (e.g., VMware, Hyper-V), export your virtual machine as a `.vmdk`, `.vhd`, or `.ova` file. Once the image is generated, upload it to a designated Amazon S3 bucket. Make sure to retain the details of the S3 bucket name and the image file name, as they will be required during the import process into AWS.



servermigrationaws Info

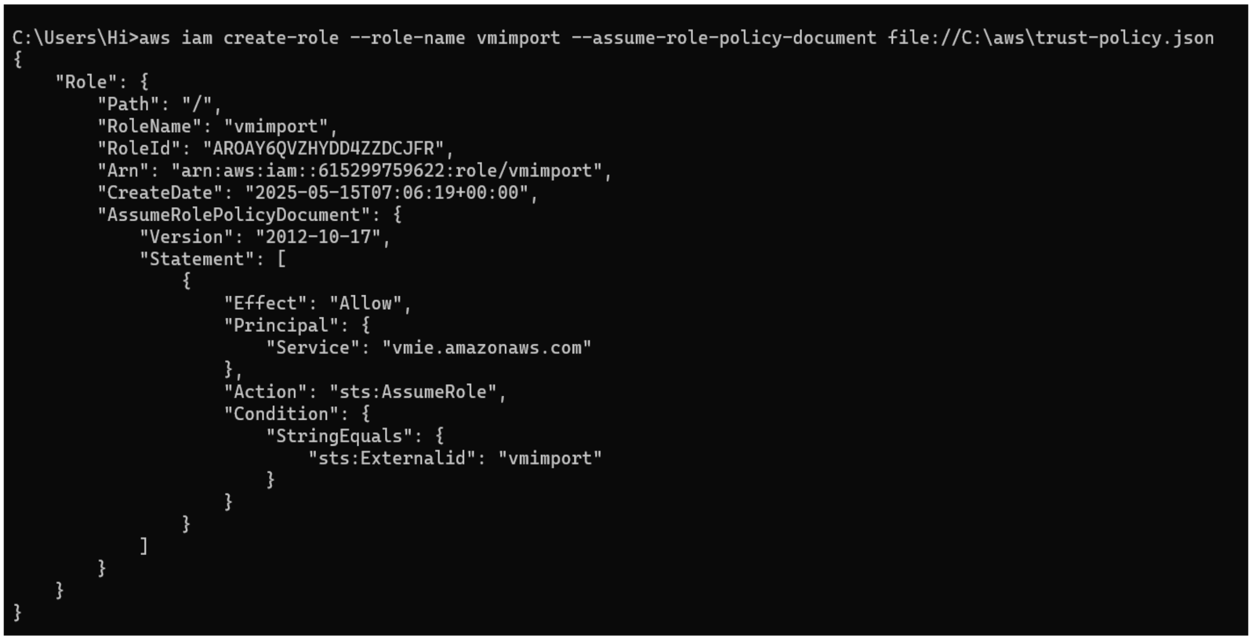
Objects (1)

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

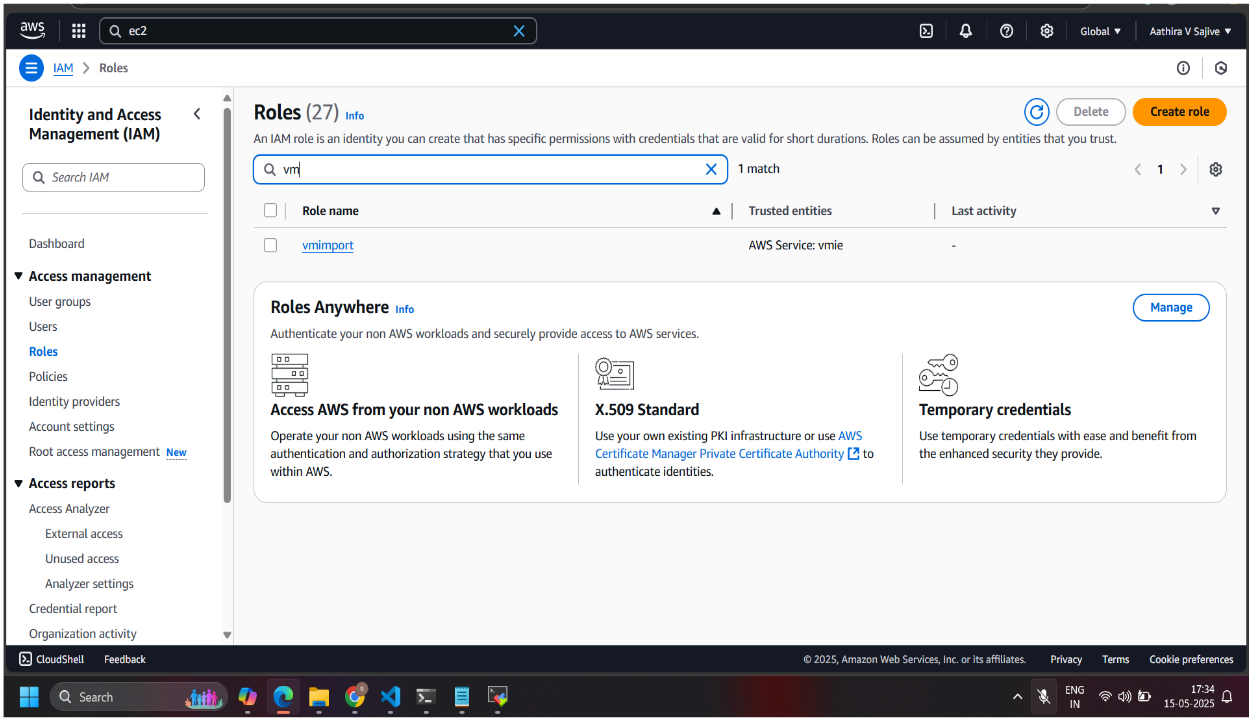
Name	Type	Last modified	Size	Storage class
CentOS_7_64-bit-disk1.vmdk	vmdk	May 15, 2025, 12:59:19 (UTC+05:30)	1.4 GB	Standard

Create IAM Role and Trust Policy for VM Import

As part of the setup, create an IAM role named `vmimport` that AWS can assume during the VM import process. This role must include a trust policy that authorizes the VM Import/Export service to use the role. Also, attach a permissions policy that grants access to the required S3 bucket and EC2 actions.



```
C:\Users\Hi>aws iam create-role --role-name vmimport --assume-role-policy-document file://C:\aws\trust-policy.json
{
    "Role": {
        "Path": "/",
        "RoleName": "vmimport",
        "RoleId": "AROAY6QVZHYDD4ZZDCJFR",
        "Arn": "arn:aws:iam::615299759622:role/vmimport",
        "CreateDate": "2025-05-15T07:06:19+00:00",
        "AssumeRolePolicyDocument": {
            "Version": "2012-10-17",
            "Statement": [
                {
                    "Effect": "Allow",
                    "Principal": {
                        "Service": "vmie.amazonaws.com"
                    },
                    "Action": "sts:AssumeRole",
                    "Condition": {
                        "StringEquals": {
                            "sts:Externalid": "vmimport"
                        }
                    }
                }
            ]
        }
    }
}
```



Roles (27) Info

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

vm — 1 match

□	Role name ▲	Trusted entities	Last activity
□	vmimport	AWS Service: vmie	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

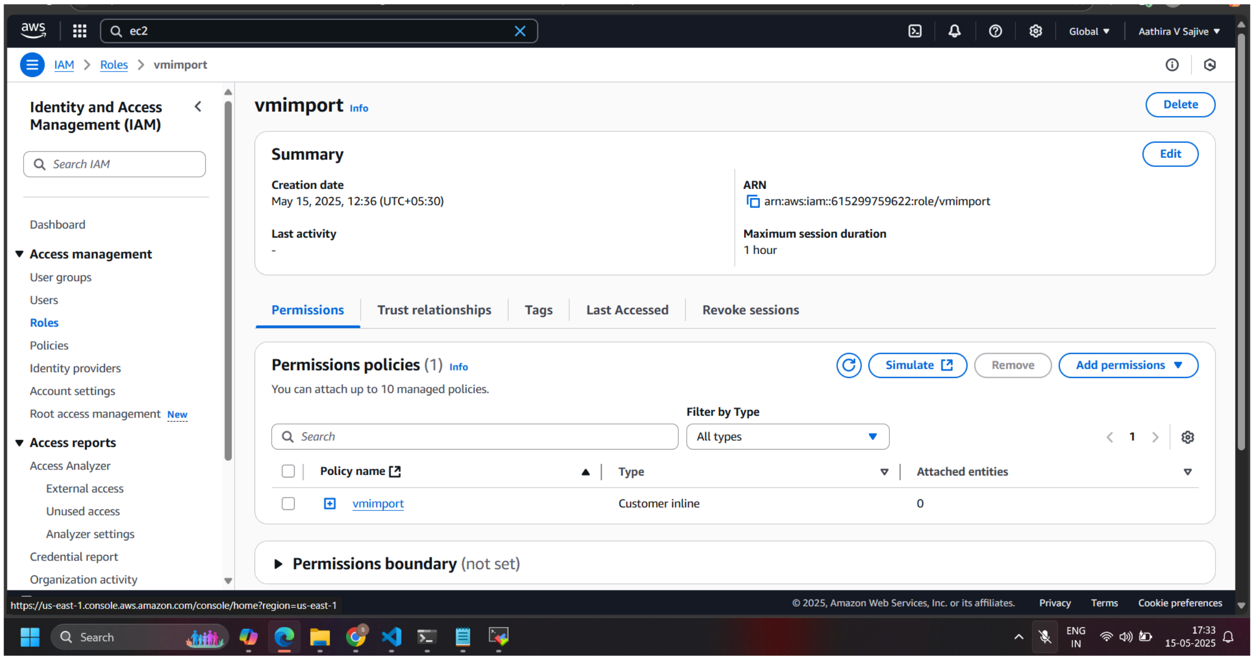
X.509 Standard

Use your own existing PKI infrastructure or use AWS Certificate Manager Private Certificate Authority to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

© 2025, Amazon Web Services, Inc. or its affiliates.



vmimport Info

Summary

Creation date
May 15, 2025, 12:36 (UTC+05:30)

ARN
arn:aws:iam::615299759622:role/vmimport

Last activity
-

Maximum session duration
1 hour

Permissions policies (1) Info

You can attach up to 10 managed policies.

	Policy name	Type	Attached entities
□	vmimport	Customer inline	0

Permissions boundary (not set)

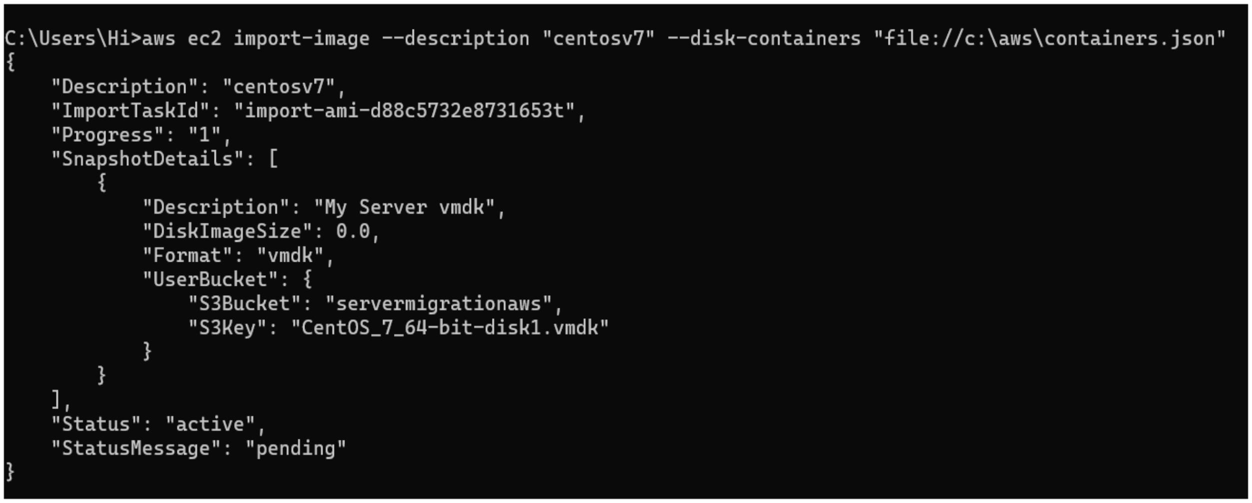
https://us-east-1.console.aws.amazon.com/console/home?region=us-east-1

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

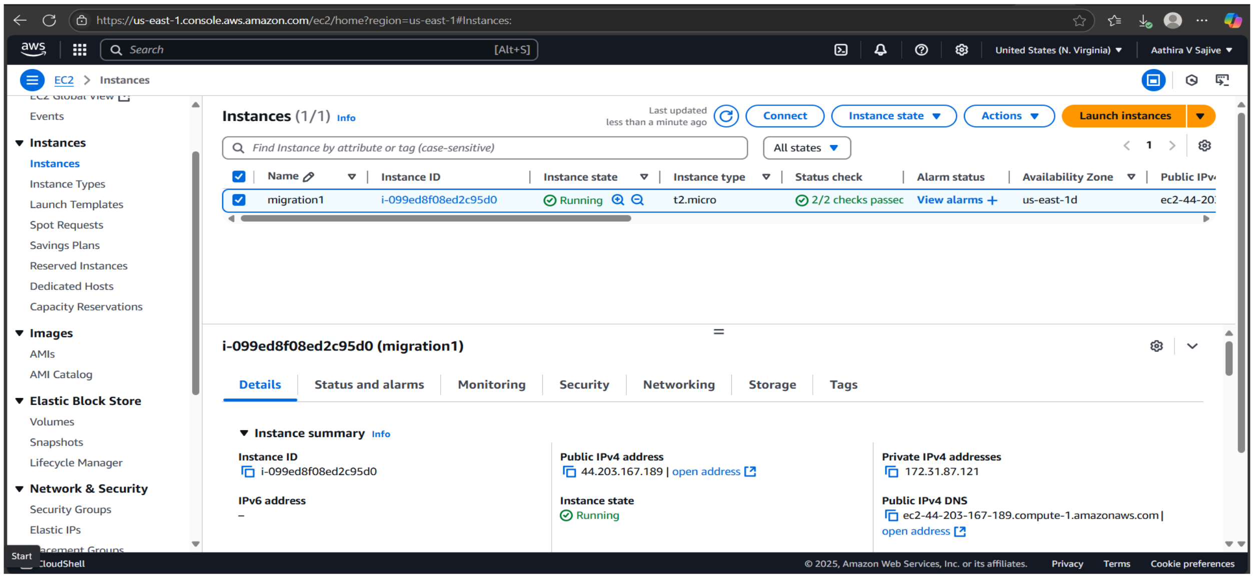
ENG IN 17:33 15-05-2025

VM Image Import and Task Execution

Once the virtual machine image is successfully uploaded to Amazon S3, initiate the import process using the AWS CLI or SDK. This involves running the `import-image` command and specifying the S3 bucket name and image file. AWS creates an import task that converts the uploaded VM image into an Amazon Machine Image (AMI). Monitor the progress of this import task using the `describe-import-image-tasks` command. After the task completes, the resulting AMI can be used to launch EC2 instances that mirror the original on-premises VM configuration.



```
C:\Users\Hi>aws ec2 import-image --description "centosv7" --disk-containers "file://c:\aws\containers.json"
{
    "Description": "centosv7",
    "ImportTaskId": "import-ami-d88c5732e8731653t",
    "Progress": "1",
    "SnapshotDetails": [
        {
            "Description": "My Server vmdk",
            "DiskImageSize": 0.0,
            "Format": "vmdk",
            "UserBucket": {
                "S3Bucket": "servermigrationaws",
                "S3Key": "CentOS_7_64-bit-disk1.vmdk"
            }
        }
    ],
    "Status": "active",
    "StatusMessage": "pending"
}
```



Instances (1/1) Info

Last updated less than a minute ago

☑	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
☑	migration1	i-099ed8f08ed2c95d0	Running	t2.micro	2/2 checks passec	View alarms +	us-east-1d	ec2-44-20:

i-099ed8f08ed2c95d0 (migration1)

Instance summary Info

Instance ID
i-099ed8f08ed2c95d0

Public IPv4 address
44.203.167.189 | open address

Private IPv4 addresses
172.31.87.121

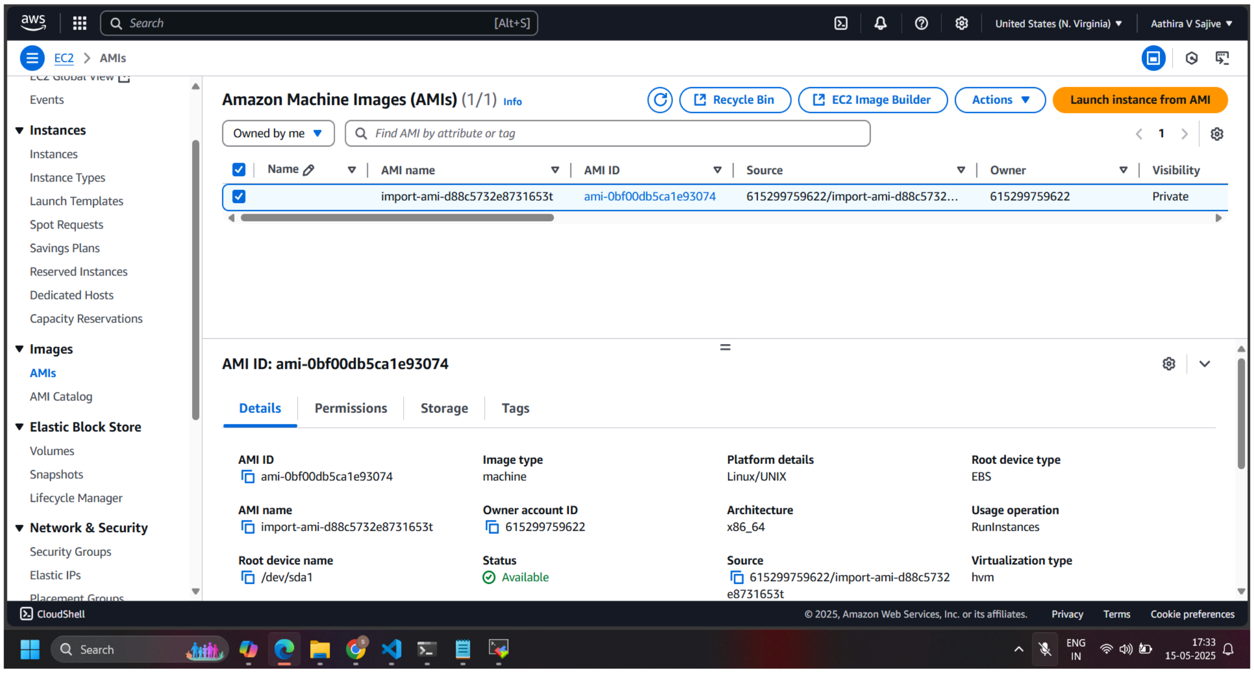
IPv6 address
–

Instance state
Running

Public IPv4 DNS
ec2-44-203-167-189.compute-1.amazonaws.com |
open address

Launch EC2 Instance from Custom AMI

After the VM import task completes and the custom Amazon Machine Image (AMI) is available, proceed to launch a new EC2 instance using this AMI. Select the appropriate instance type based on performance requirements, configure networking settings (VPC, subnet, security groups), and assign storage volumes as needed. Ensure the instance is launched in the desired region and availability zone. This newly launched EC2 instance will replicate the original on-premises server, retaining its applications, configurations, and settings.



Amazon Machine Images (AMIs) (1/1) Info

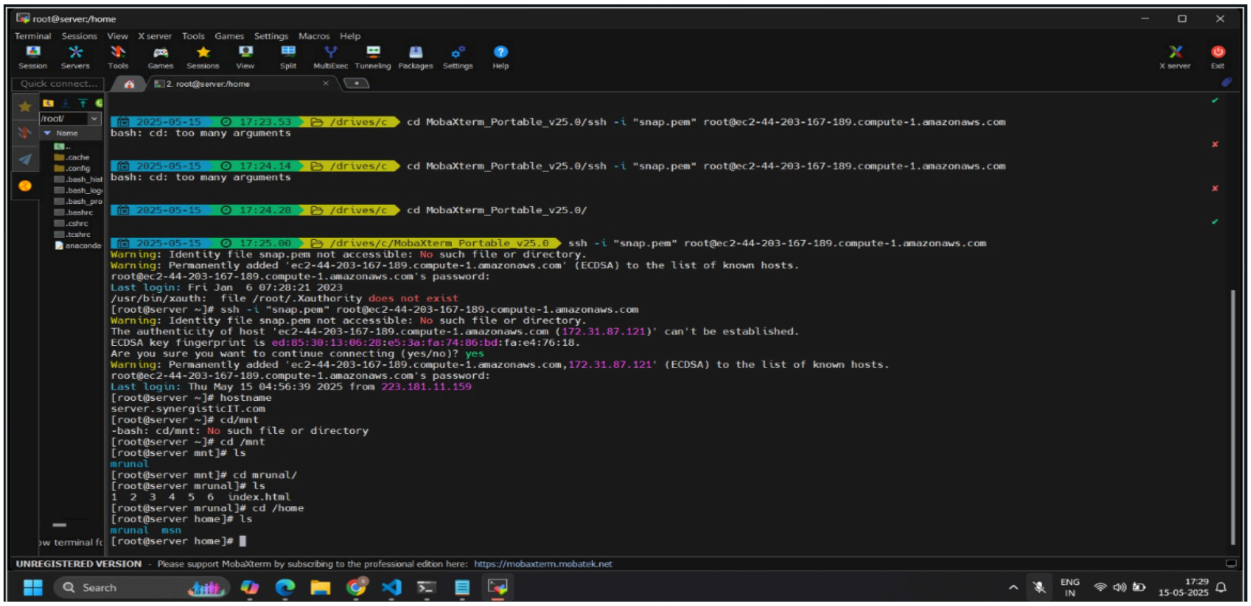
☑	Name	AMI name	AMI ID	Source	Owner	Visibility
☑		import-ami-d88c5732e8731653t	ami-0bf00db5ca1e93074	615299759622/import-ami-d88c5732...	615299759622	Private

AMI ID: ami-0bf00db5ca1e93074

AMI ID ami-0bf00db5ca1e93074	Image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name import-ami-d88c5732e8731653t	Owner account ID 615299759622	Architecture x86_64	Usage operation RunInstances
Root device name /dev/sda1	Status Available	Source 615299759622/import-ami-d88c5732 e8731653t	Virtualization type hvm

Post-Launch Validation and Configuration

Once the EC2 instance is running, perform a thorough validation to ensure the system operates as expected. Verify network connectivity (SSH/RDP), application functionality, and operating system configurations. Check that all required services have started correctly and that data and settings have been preserved.


root@server:/home
Terminal Sessions View X server Tools Games Settings Macros Help
Session Servers Tools Games Sessions View Split MultiExec Tunneling Packages Settings Help
X server Exit
Quick connect...
2. root@server:/home
/root/
Name
.cache
.config
.bash_hist
.bash_log
.bash_pro
.bashrc
.cshrc
.tcshrc
anaconda
UNREGISTERED VERSION - Please support MobaXterm by subscribing to the professional edition here: https://mobaxterm.mobatek.net
Search
ENG IN
17:29
15-05-2025

```
 2025-05-15  17:23.53  /drives/c  cd MobaXterm_Portable_v25.0/ssh -i "snap.pem" root@ec2-44-203-167-189.compute-1.amazonaws.com
bash: cd: too many arguments

 2025-05-15  17:24.14  /drives/c  cd MobaXterm_Portable_v25.0/ssh -i "snap.pem" root@ec2-44-203-167-189.compute-1.amazonaws.com
bash: cd: too many arguments

 2025-05-15  17:24.28  /drives/c  cd MobaXterm_Portable_v25.0/

 2025-05-15  17:25.00  /drives/c/MobaXterm_Portable_v25.0  ssh -i "snap.pem" root@ec2-44-203-167-189.compute-1.amazonaws.com
Warning: Identity file snap.pem not accessible: No such file or directory.
Warning: Permanently added 'ec2-44-203-167-189.compute-1.amazonaws.com' (ECDSA) to the list of known hosts.
root@ec2-44-203-167-189.compute-1.amazonaws.com's password:
Last login: Fri Jan  6 07:28:21 2023
/usr/bin/xauth:  file /root/.Xauthority does not exist
[root@server ~]# ssh -i "snap.pem" root@ec2-44-203-167-189.compute-1.amazonaws.com
Warning: Identity file snap.pem not accessible: No such file or directory.
The authenticity of host 'ec2-44-203-167-189.compute-1.amazonaws.com (172.31.87.121)' can't be established.
ECDSA key fingerprint is ed:85:30:13:06:28:e5:3a:fa:74:86:bd:fa:e4:76:18.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-44-203-167-189.compute-1.amazonaws.com,172.31.87.121' (ECDSA) to the list of known hosts.
root@ec2-44-203-167-189.compute-1.amazonaws.com's password:
Last login: Thu May 15 04:56:39 2025 from 223.181.11.159
[root@server ~]# hostname
server.synergisticIT.com
[root@server ~]# cd/mnt
-bash: cd/mnt: No such file or directory
[root@server ~]# cd /mnt
[root@server mnt]# ls
mrunal
[root@server mnt]# cd mrunal/
[root@server mrunal]# ls
1  2  3  4  5  6  index.html
[root@server mrunal]# cd /home
[root@server home]# ls
mrunal  msn
[root@server home]# 
```

Importance of Server Migration

Server migration is a critical process that allows organizations to modernize their IT infrastructure by transitioning from on-premises systems to more scalable, secure, and cost-efficient cloud environments like AWS. It helps eliminate hardware dependencies, reduce maintenance overhead, and enhance disaster recovery capabilities. Migrating to AWS also enables access to advanced services such as automation, monitoring, machine learning, and global availability. Ultimately, server migration supports business agility, operational resilience, and long-term digital transformation goals.

Conclusion

The successful migration of on-premises virtual machines to AWS using VM Import ensures minimal disruption while preserving existing configurations, software, and system settings. By leveraging AWS-native tools and best practices, the project enables improved scalability, high availability, and operational efficiency in the cloud environment. With the EC2 instances now running on AWS, the infrastructure is better positioned for future growth, cost optimization, and enhanced security.