



AWS MIGRATION

AWS (Amazon Web Services) migration refers to the process of moving an organization's applications, data, and other business elements to the cloud platform provided by AWS. This migration can involve moving from on-premises data centres, other cloud providers, or a hybrid environment to AWS. A successful migration to AWS can bring various benefits, including scalability, cost-efficiency, agility, and improved security.

Here is a general guide to help you understand the key steps involved in an AWS migration:

1. Assessment and Planning:

- a) **Assess Your Current Environment:** Understand your existing infrastructure, applications, and data dependencies. Identify any dependencies and potential challenges.
- b) **Define Objectives:** Clearly define the goals of your migration, such as cost reduction, improved performance, scalability, or modernization.
- c) **Create a Migration Plan:** Develop a detailed plan that outlines tasks, timelines, and resources needed for each phase of the migration.

2. Designing the AWS Architecture:

- a) **Select AWS Services:** Choose the AWS services that align with your requirements. AWS provides a wide range of services for computing, storage, databases, networking, and more.
- b) **Architect for Scalability and Resilience:** Design your architecture to take advantage of AWS scalability and ensure high availability and fault tolerance.
- c) **Consider Security:** Implement security best practices, such as encryption, identity and access management (IAM), and network security.

3. Data Migration:

- a) **Transfer Data to AWS:** Move your data to AWS using various migration methods, such as AWS Snowball, AWS DataSync, or traditional data transfer methods.
- b) **Database Migration:** If you're migrating databases, use services like AWS Database Migration Service (DMS) for a seamless transition.

4. Application Migration:

- a) **Rehost, Refactor, or Rebuild:** Decide whether to lift and shift (rehost), refactor, or rebuild your applications based on your objectives and requirements.
- b) **Use Containers and Serverless:** Consider containerization (using services like Amazon ECS or EKS) or serverless computing (AWS Lambda) for modernization.

5. Testing:

- a) **Perform Testing:** Conduct thorough testing of applications and infrastructure in the AWS environment to identify and resolve any issues.

- b) **Implement a Rollback Plan:** Have a rollback plan in case any issues arise during or after migration.

6. Optimization:

- a) **Cost Optimization:** Optimize your AWS resources to ensure cost efficiency. Use services like AWS Cost Explorer to monitor and manage costs.
- b) **Performance Optimization:** Fine-tune configurations for better performance based on actual usage patterns.

7. Training and Documentation:

- a) **Training:** Ensure that your team is trained on AWS services and best practices.
- b) **Documentation:** Document the new AWS environment, including configurations, security policies, and procedures.

8. Monitoring and Management:

1. **Implement Monitoring:** Set up monitoring tools (e.g., AWS CloudWatch) to track the performance, health, and security of your AWS resources.
2. **Incident Response Plan:** Develop an incident response plan to address and resolve issues promptly.

9. Go-Live and Post-Migration Support:

- a) **Go-Live:** Execute the migration plan and monitor the performance immediately after the migration.
- b) **Provide Post-Migration Support:** Address any issues that may arise and provide support to end-users as needed.

AWS Application Migration Service

AWS Application Migration Service (MGN) is a highly automated lift-and-shift (rehost) solution that simplifies, expedites, and reduces the cost of migrating applications to AWS. It allows companies to lift-and-shift a large number of physical, virtual, or cloud servers without compatibility issues, performance disruption, or long cutover windows. MGN replicates source servers into your AWS account. When you're ready, it automatically converts and launches your servers on AWS so you can quickly benefit from the cost savings, productivity, resilience, and agility of the Cloud. Once your applications are running on AWS, you can leverage AWS services and capabilities to quickly and easily replatform or refactor those applications – which makes lift-and-shift a fast route to modernization.

Here are some AWS services commonly used for application migration:

1. **AWS Server Migration Service (SMS):** AWS SMS is used for migrating on-premises virtualized servers to AWS. It supports the migration of VMware and Microsoft Hyper-V virtual machines. Server replication, automated incremental updates, server grouping, and multi-server application migration.

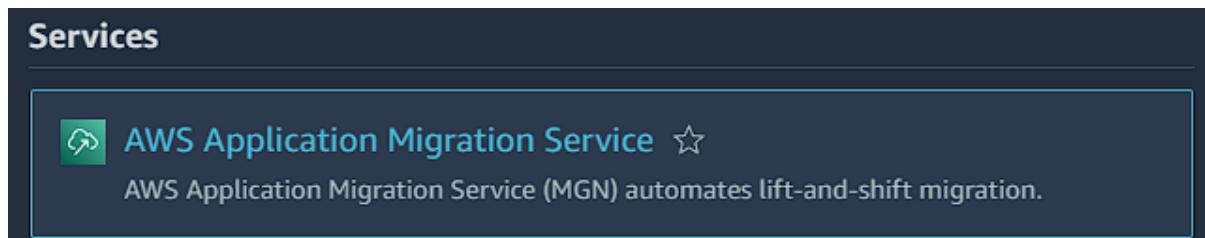
2. **AWS Database Migration Service (DMS):** DMS is specifically designed for database migrations. It supports the migration of various database engines to and from AWS. Schema conversion, ongoing replication, and minimal downtime during migration.
3. **AWS DataSync:** AWS DataSync is a service for fast and secure data transfer between on-premises and AWS. Supports one-time or recurring transfers, provides network optimization, and is suitable for large-scale data migrations.
4. **AWS Data Migration Hub:** This is a centralized location to monitor the progress of application migrations across multiple AWS services. Visibility into the status of migrations, tracking of resource changes, and troubleshooting capabilities.
5. **AWS Migration Hub:** Migration Hub provides a single location to track the progress of application migrations across multiple AWS and partner solutions. Centralized migration tracking, progress reporting, and integration with various migration tools.
6. **AWS Serverless Application Model (SAM):** SAM is an open-source framework for building serverless applications. It simplifies the process of defining serverless applications on AWS. Simplified syntax for defining serverless resources, local testing and debugging, and easy deployment.
7. **AWS CloudEndure Migration:** CloudEndure Migration is an agent-based service that facilitates the migration of physical, virtual, and cloud-based servers to AWS. Continuous data replication, automated machine conversion, and minimal cutover time.

TO BEGIN WITH THE LAB:

Basically, we need to decide source and destination for data migration.

STEP 1: Create MGN in the Target Region

1. Log in to AWS Console. Then search MGN in the search box and choose this service shown below i.e. AWS Application Migration Service (MGN)



2. To you the console would look like this.

3. Here now you have to click on Get Started to move forward. From here you will start your service.
4. So, once you have clicked on Set up Service it will say that; default templates are created.
5. Now you have to add servers here.

[Application Migration Service](#) > [Set up Application Migration Service](#)

Set up Application Migration Service

Service initialization

In order to use Application Migration Service in this region, the service must first be initialized by an Admin user of the AWS account. Once the service is initialized, you can modify the default service templates on the Settings page.

By continuing, you are allowing application Migration Service to create all the IAM roles required to facilitate data replication and the launching of migrated servers. [Learn more](#)

[View roles](#)

[Cancel](#) [Set up service](#)

Default templates created
Every time you add a source server to Application Migration Service, its Replication settings, Launch settings and Post-launch action settings are initialized based on default templates. You can edit the default templates in the Settings page.
The next step to setting up Application Migration Service is adding your source servers by installing the AWS Replication agent on them.

[Application Migration Service](#) > Active source servers

Windows Migration Accelerator (WMA) Program
If you are migrating 40 or more servers per month (including at least 15 Windows servers), you may qualify for up to \$250 credit per server by joining the WMA program. [Learn more](#)

Migration tip #1
It's important to test launch your servers in AWS at least two weeks before the cutover. Testing is non-disruptive. [Learn more](#)

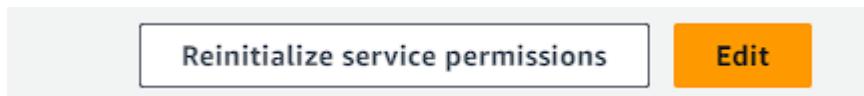
Hide future tips

6. After your default templates are created now, click on the hamburger icon and from the left under settings you will find an option as replication template.

▼ Settings

Replication template

7. Click on it and there you will see that a default template has been created for you by the service itself.
8. But for now, you have to click on edit to change some settings.



9. Now you need select a subnet of your choice, then select replication server instance type to t2.micro (because it is eligible for free tier)

Replication server configuration Info

Replication servers are lightweight EC2 instances launched by Application Migration Service to facilitate the transfer of blocks of data from the disks on your source servers to AWS.

Staging area subnet
The staging area subnet is the subnet within which replication servers and conversion servers are launched. By default, Application Migration Service will use the default subnet on your AWS Account.

subnet-0e332b1830a91b4cd
vpc-062d767592c9ad3e0

Replication Server instance type
The replication server instance type is the default EC2 instance type to use for replication servers. The recommended best practice is to not change the replication server instance type unless there is a business need to do so.

t2.micro

10. Then select EBS volume type to gp2 and keep EBS encryption to default.

Volumes Info

For each disk on an added source server there is an identically-sized EBS volume attached to a replication server, and each replication server can handle replication of disks from multiple source servers.

EBS volume type (for replicating disks over 500GiB)
The default EBS Volume type to be used by the replication servers.

Faster, General Purpose SSD (gp2)

EBS encryption
This option will encrypt your replicated data at rest on the staging area subnet disks and the replicated disks.

Default

11. For the security group you have to create a new security group with port 1500 open for everywhere in inbound rule.

The screenshot shows the 'Inbound rules' section of a AWS Application Migration Service configuration. It displays a single rule: 'sgr-0a2628c9d2f47d3de'. The rule details are: Type: Custom TCP, Protocol: TCP, Port range: 1500, Source: Custom, and Destination: 0.0.0.0/0. There is a search bar and a delete button.

12. After creating your security group refresh your page again and select your security group.

The screenshot shows the 'Security groups' section. It includes a note about security groups acting as virtual firewalls. Below is a checkbox for 'Always use Application Migration Service security group' and a dropdown menu for 'Additional security groups'. A selected item 'aws-mgn-sg' is listed with a delete icon.

13. For the demo purpose, select create public IP.

14. Now click on save template and your replication template will be edited as per your choice.

The screenshot shows the 'Data routing and throttling' section. It contains a note about data flow from external servers to replication servers. Below are several configuration options: 'Create public IP' (selected), 'Use private IP for data replication (VPN, DirectConnect, VPC peering, etc.)', 'Create public IP, and use Private IP for data replication (VPN, DirectConnect, VPC peering, etc.)', and 'Throttle network bandwidth (per server - in Mbps)'.

The screenshot shows the 'Replication resources tags' section. It features a button 'Add new tag' and a note stating 'You can add up to 50 more tags.' At the bottom right are 'Cancel' and 'Save template' buttons.

STEP 2: Create Peering connection

1. Now you have to create VPC Peering connection between the two regions that you have selected for the data migration. (like mine are Sydney and Oregon)
2. Go to peering connection and create a connection from your source between both the region.

Create peering connection

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them privately. [Info](#)

Peering connection settings

Name - *optional*

Create a tag with a key of 'Name' and a value that you specify.

Select a local VPC to peer with

VPC ID (Requester)



VPC CIDRs for vpc-08586d288974cbdca

CIDR	Status	Status reason
172.31.0.0/16	Associated	-

Select another VPC to peer with

Account

- My account
 Another account

Region

- This Region (ap-southeast-2)
 Another Region



VPC ID (Acceptor)

3. Once your connection is created, it will look like this.

A VPC peering connection pcx-0112e4ca9b6a7b287 / my-vpc-01 has been requested.
Remember to change your region to us-west-2 to accept the peering connection.

VPC > Peering connections > pcx-0112e4ca9b6a7b287

pcx-0112e4ca9b6a7b287 / my-vpc-01

Details [Info](#)

Requester owner ID 463646775279	Acceptor owner ID 463646775279	VPC Peering connection ARN arnaws:ec2:ap-southeast-2:463646775279:vpc-peering-connection/pcx-0112e4ca9b6a7b287
Peering connection ID pcx-0112e4ca9b6a7b287	Requester VPC vpc-08586d288974cbdca	Acceptor VPC vpc-062d767592c9ad3e0
Status Initiating Request to 463646775279	Requester CIDRs 172.31.0.0/16	Acceptor CIDRs -
Expiration time Friday, January 12, 2024 at 23:34:16 GMT+5:30	Requester Region Sydney (ap-southeast-2)	Acceptor Region Oregon (us-west-2)

DNS [Route tables](#) [Tags](#)

DNS settings

Requester VPC (vpc-08586d288974cbdca) Info	Acceptor VPC (vpc-062d767592c9ad3e0) Info
Allow accepter VPC to resolve DNS of hosts in requester VPC to private IP addresses <input checked="" type="radio"/> Enabled	Allow requester VPC to resolve DNS of hosts in accepter VPC to private IP addresses <input checked="" type="radio"/> Enabled

- But there is a catch here, now you created peering connection using default VPC, because of it there is a failure on the other side because of the overlapping of the CIDR. That is why you need to create a new VPC and then again create your peering connection.

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
-	pcx-0112e4ca9b6a7b287	Failed	vpc-08586d288974cbdca	vpc-062d767592c9ad3e0	-	-

pcx-0112e4ca9b6a7b287

Details [DNS](#) [Route tables](#) [Tags](#)

Details

Requester owner ID 463646775279	Acceptor owner ID 463646775279	VPC Peering connection ARN arnaws:ec2:us-west-2:463646775279:vpc-peering-connection/pcx-0112e4ca9b6a7b287
Peering connection ID pcx-0112e4ca9b6a7b287	Requester VPC vpc-08586d288974cbdca	Acceptor VPC vpc-062d767592c9ad3e0
Status Failed due to incorrect VPC-ID, Account ID, or overlapping CIDR range	Requester CIDRs -	Acceptor CIDRs -
Expiration time -	Requester Region Sydney (ap-southeast-2)	Acceptor Region Oregon (us-west-2)

- Now create new VPC for source region then again create your peering connection from there only.
- While creating your VPC you need to select VPC and more because is kind of an automation type of mode for creating VPC.

VPC settings

Resources to create [Info](#)

Create only the VPC resource or the VPC and other networking resources.

VPC only

VPC and more

7. Give it a name and the auto generate option should be ON.

8. Then give your CIDR block.

Name tag auto-generation [Info](#)

Enter a value for the Name tag. This value will be used to auto-generate Name tags for all resources in the VPC.

Auto-generate

on-prem

IPv4 CIDR block [Info](#)

Determine the starting IP and the size of your VPC using CIDR notation.

10.31.0.0/16

65,536 IPs

CIDR block size must be between /16 and /28.

IPv6 CIDR block [Info](#)

No IPv6 CIDR block

Amazon-provided IPv6 CIDR block

9. Now for the number of availability zones, select it to 2 because you need two zones.

10. Number of public subnets should be 2.

11. Number of private subnets should also be 2.

12. Keep NAT gateways to none.

13. Select S3 for VPC endpoints.

Number of Availability Zones (AZs) [Info](#)

Choose the number of AZs in which to provision subnets. We recommend at least two AZs for high availability.

1	2	3
---	---	---

► Customize AZs

Number of public subnets [Info](#)

The number of public subnets to add to your VPC. Use public subnets for web applications that need to be publicly accessible over the internet.

0	2
---	---

Number of private subnets [Info](#)

The number of private subnets to add to your VPC. Use private subnets to secure backend resources that don't need public access.

0	2	4
---	---	---

► Customize subnets CIDR blocks

NAT gateways (\$) [Info](#)

Choose the number of Availability Zones (AZs) in which to create NAT gateways. Note that there is a charge for each NAT gateway

None	In 1 AZ	1 per AZ
------	---------	----------

VPC endpoints [Info](#)

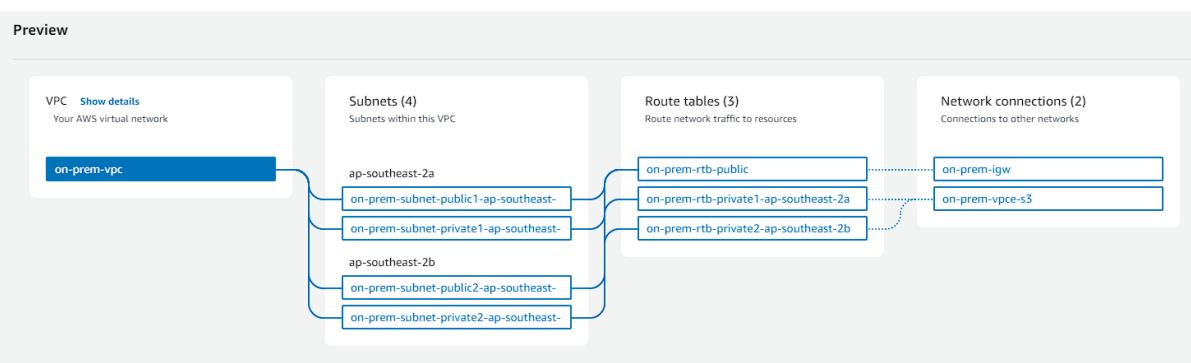
Endpoints can help reduce NAT gateway charges and improve security by accessing S3 directly from the VPC. By default, full access policy is used. You can customize this policy at any time.

None	S3 Gateway
------	------------

14. As you can see it is giving you the preview for the VPC.

15. Whatever the requirements are, it is creating them itself.

16. Now click on create VPC and you will see your workflow is also been created.



Create VPC workflow

Success

▼ Details

- ✓ Create VPC: vpc-01b1a53cbacfe0803 [🔗](#)
- ✓ Enable DNS hostnames
- ✓ Enable DNS resolution
- ✓ Verifying VPC creation: vpc-01b1a53cbacfe0803 [🔗](#)
- ✓ Create S3 endpoint: vpce-001c0165c351400d2 [🔗](#)
- ✓ Create subnet: subnet-0df2749c2d79c99dc [🔗](#)
- ✓ Create subnet: subnet-049499c498fa16e61 [🔗](#)
- ✓ Create subnet: subnet-0835e2186b1d91fd4 [🔗](#)
- ✓ Create subnet: subnet-05b8ca29c2b92ea3f [🔗](#)
- ✓ Create internet gateway: igw-0a50ade97105662e5 [🔗](#)
- ✓ Attach internet gateway to the VPC
- ✓ Create route table: rtb-07272965c34986557 [🔗](#)
- ✓ Create route
- ✓ Associate route table
- ✓ Associate route table
- ✓ Create route table: rtb-08b9dea6ca3f16c22 [🔗](#)
- ✓ Associate route table
- ✓ Create route table: rtb-0c39fb3dd86f62432 [🔗](#)
- ✓ Associate route table
- ✓ Verifying route table creation
- ✓ Associate S3 endpoint with private subnet route tables: vpce-001c0165c351400d2 [🔗](#)

[View VPC](#)

17. Now go back to peering connection and create your connection.
18. Once you have created a new Peering connection, you will see that at your destination it asking you to accept the connection.

Peering connections (2) Info						
Actions Create peering connection						
Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
○ -	pxc-02413da8c9eb2da5e	Pending acceptance	vpc-01b1a53cbacfe0803	vpc-062d767592c9ad3e0	10.31.0.0/16	-
○ -	pxc-0112e4ca9b6a7b287	Failed	vpc-08586d288974cbdca	vpc-062d767592c9ad3e0	-	46364

19. So, to accept it, select your connection, then click on actions, now click on accept invite.

Peering connections (1/2) Info						
Actions Create peering connection						
View details Accept request Reject request Edit DNS settings Edit ClassicLink settings Manage tags Delete peering connection						
Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs
○ -	pxc-02413da8c9eb2da5e	Pending acceptance	vpc-01b1a53cbacfe0803	vpc-062d767592c9ad3e0	-	46364
○ -	pxc-0112e4ca9b6a7b287	Failed	vpc-08586d288974cbdca	vpc-062d767592c9ad3e0	-	46364

20. Soon after, you will see this window from here accept the request.

Accept VPC peering connection request



Are you sure you want to accept this VPC peering connection request? (pcx-02413da8c9eb2da5e)

Requester VPC vpc-01b1a53cbacfe0803	Acceptor VPC vpc-062d767592c9ad3e0	Requester CIDRs 10.31.0.0/16
Acceptor CIDRs -	Requester Region Sydney (ap-southeast-2)	Acceptor Region Oregon (us-west-2)
Requester owner ID 463646775279 (This account)	Acceptor owner ID 463646775279 (This account)	
		Cancel Accept request

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs	Requester owner ID
-	pcx-02413da8c9eb2da5e	Active	vpc-01b1a53cbacfe0803	vpc-062d767592c9ad3e0	10.31.0.0/16	172.31.0.0/16	463646775279

21. Once you have accepted the request, you will get this message to fix your route table.

Your VPC peering connection (pcx-02413da8c9eb2da5e) has been established. To send and receive traffic across this VPC peering connection, you must add a route to the peered VPC in one or more of your VPC route tables. Info	Modify my route tables now	
---	--	--

22. To avoid the confusion between the route table, first go to your VPC, then select your VPC and in the details of VPC, you can find this option for Main Route Table. Now select this option to directly go the desired route table.

DNS hostnames

Enabled

Main route table

[rtb-09d1bc0ec680f0fd1](#)

23. For this, now you have to make some changes in your route table. Go to your route table, select your route table then click on routes. Then click on edit routes.

rtb-09d1bc0ec680f0fd1					
Details	Routes	Subnet associations	Edge associations	Route propagation	Tags
Routes (3)					
Filter routes	Both				
Destination	Target	Status		Propagated	
gl-68a54001	vpc-0b002d0693ce59b19	Active		No	
0.0.0.0/0	igw-00ca4cab2b0693512	Active		No	
172.31.0.0/16	local	Active		No	

24. Now in the edit route section, click on add route, there you need to write the CIDR of your source region because you are at your destination region right now.

25. Then select Peering connection in target and click on save changes.

Edit routes				
Destination	Target	Status	Propagated	
pl-68a54001	vpce-0b002d0693ce59b19	Active	No	
172.31.0.0/16	local Q local	Active	No	
Q 0.0.0.0/0	Internet Gateway Q igw-00ca4cab2b0693512	Active	No	<button>Remove</button>
Q 10.31.0.0/16	Peering Connection Q ppx-02413da8c9eb2da5e	-	No	<button>Remove</button>
<button>Add route</button>				
				<button>Cancel</button> <button>Preview</button> <button>Save changes</button>

26. Once it has been done then go to your source region and so the same thing.

Destination	Target	Status	Propagated	
10.31.0.0/16	local Q local	Active	No	
Q 172.31.0.0/16	Peering Connection Q ppx-02413da8c9eb2da5e	-	No	<button>Remove</button>
<button>Add route</button>				
				<button>Cancel</button> <button>Preview</button> <button>Save changes</button>

STEP 3: Create EC2 Instances

1. Now navigate to EC2 and create 2 instances in your source region.
2. First create a windows instance. Then create a Linux instance.
3. While creating the windows instance, in the network settings, select the VPC which you created and for the subnet select any public subnet. Disable auto assign public IP.
4. Then create your windows instance.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below



Search our full catalog including 1000s of application and OS images

Quick Start

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Microsoft Windows Server 2022 Base

ami-015e01fec392ea845 (64-bit (x86))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

▼ Instance type [Info](#) | [Get advice](#)

Instance type

t2.micro

Free tier eligible

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand SUSE base pricing: 0.0146 USD per Hour
On-Demand Linux base pricing: 0.0146 USD per Hour
On-Demand Windows base pricing: 0.0192 USD per Hour
On-Demand RHEL base pricing: 0.0746 USD per Hour

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-01b1a53cbacfe0803 (on-prem-vpc)
10.31.0.0/16



Subnet [Info](#)

subnet-049499c498fa16e61 on-prem-subnet-public2-ap-southeast-2b
VPC: vpc-01b1a53cbacfe0803 Owner: 463646775279
Availability Zone: ap-southeast-2b IP addresses available: 4091 CIDR: 10.31.16.0/20

[Create new subnet](#)

Auto-assign public IP [Info](#)

Disable



Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group

Select existing security group

Common security groups [Info](#)

Select security groups



[Compare security group rules](#)

default sg-02295957ac962458e

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

5. The steps for creating Linux instance are also same. Just remember to select Linux 2 AMI.
6. Then just launch your instance.

Name and tags [Info](#)

Name

[Add additional tags](#)

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below



Search our full catalog including 1000s of application and OS images

Quick Start



[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

ami-0d13b3038380b0796 (64-bit (x86)) / ami-0fd0bb835243a6706 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible



▼ Network settings [Info](#)

VPC - required [Info](#)

vpc-01b1a53cbacfe0803 (on-prem-vpc)
10.31.0.0/16

Subnet [Info](#)

subnet-049499c498fa16e61 on-prem-subnet-public2-ap-southeast-2b
VPC: vpc-01b1a53cbacfe0803 Owner: 463646775279
Availability Zone: ap-southeast-2b IP addresses available: 4090 CIDR: 10.31.16.0/20

Create new subnet [\[+\]](#)

Auto-assign public IP [Info](#)

Disable

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Common security groups [Info](#)

Select security groups

default sg-02295957ac962458e X
VPC: vpc-01b1a53cbacfe0803

Compare security group rules

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

7. Once both of your instances are created then allocate elastic IP to both of them.

Instances (2) Info										
C Connect Instance state Actions Launch instances [+]										
<input type="checkbox"/>	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
<input type="checkbox"/>	on-prem-win-...	i-011c564eafe1240e4	Running Q Q	t2.micro	2/2 checks passed No alarms +	ap-southeast-2b	-	-	-	-
<input type="checkbox"/>	on-prem-lin-s...	i-0656d401bbd253d19	Running Q Q	t2.micro	2/2 checks passed No alarms +	ap-southeast-2b	-	-	-	-

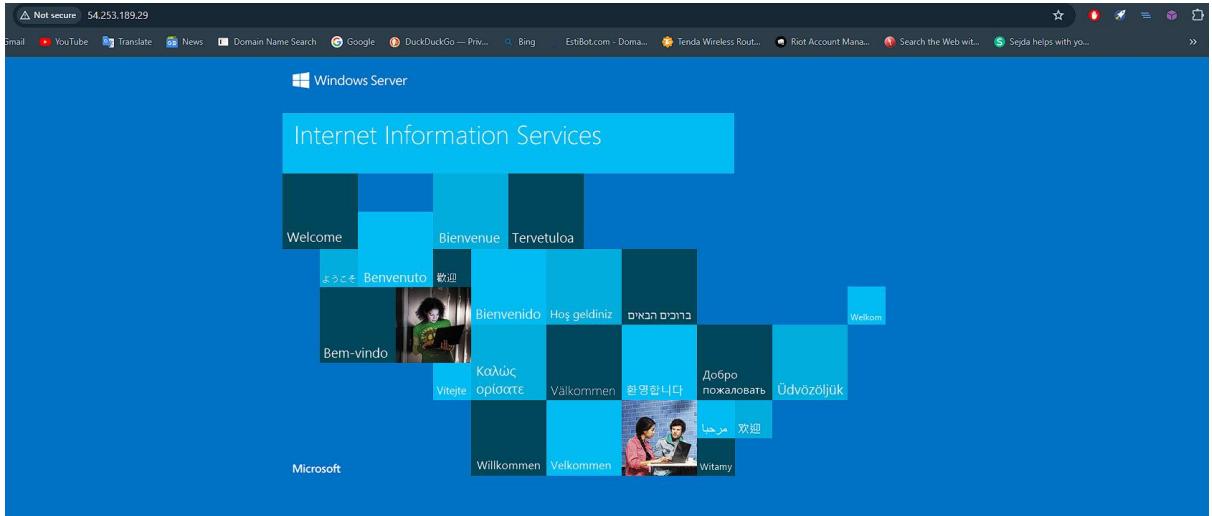
8. Now create two elastic IPs, one for Windows instance and one for Linux instance.

Elastic IP addresses (2)								
C Actions Allocate Elastic IP address [+]								
<input type="checkbox"/>	Name	Allocated IPv4 add...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address	
<input type="checkbox"/>	eip-lin	13.210.111.14	Public IP	eipalloc-01dc11ff8cebb271d	-	-	-	
<input type="checkbox"/>	eip-win	54.253.189.29	Public IP	eipalloc-0ef3dae200b76827	-	-	-	

9. Now associate these elastic IPs to the instances.

10. After this, go back to the instances and try to establish a remote desktop connection with windows instance.
11. Before that you need to add port 3389 and port 80 to the inbound rules of the windows instance.
12. There you need to open server manager dashboard in the windows instance and install IIS (Internet Information Service) over there.

13. Once you have installed IIS on windows instance then you need to copy its public IP address and paste it in a new tab. You can see that IIS is successfully installed on it.



14. Now SSH in to the Linux instance and install HTTPD on it.

15. But before that add port 22 and 80 on Linux instance.

16. Now connect it to the session manager.

17. In there you need to run some commands. Run these commands step by step and it will install the HTTPD or the apache test server on your linux instance.

```
sudo -i  
yum update -y  
yum install httpd -y  
systemctl status httpd  
systemctl start httpd  
systemctl enable httpd
```



STEP 4: Now go to Target MGN and create Server

1. Here you have to add the servers but before adding the servers you need to have access keys and secret access keys.
2. For that go to IAM and create a user then download its access and secret keys.
3. Attach this policy to the user and then create your user.

Permissions policies (1/1360)

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

Filter by Type

Policy name	Type
<input type="checkbox"/> AWSApplicationMigrationAgentInstallationPolicy	AWS managed
<input checked="" type="checkbox"/> AWSApplicationMigrationAgentPolicy	AWS managed

- Once your user is created now go and create its access and secret keys.

IAM > Users > mgn-demo-user > Create access key

Step 1 Access key best practices & alternatives

Step 2 - optional Set description tag

Step 3 Retrieve access keys

Access key best practices

Access key key ID Secret access key

AKIAWX44AK7X613G52Y ***** Show

If you lose or forget your secret access key, you cannot retrieve it. Instead, create a new access key and make the old key inactive.

Download .csv file Done

- After everything is set up, now go back to MGN. There you need to select and go to source server.
- Now you have add your server.

Active source servers

Source server name Alerts Migration lifecycle Data replication status Last snapshot Next step

No servers

Add your source servers to this console by installing the AWS Replication Agent. Alternatively, you can add source servers without installing an agent on each guest server by installing the AWS vCenter client on your vCenter.

Add server

This account is currently replicating 0 servers out of a quota of 150 concurrent replicating servers. [Learn more](#)

- In there choose it for Linux.
- Then select replicate all disks.

AWS Replication Agent installation

- Select your operating system

Linux

Windows

Legacy OS: Windows Server 2003 or Windows Server 2008

- Select your replication preferences [Info](#)

Replicate all disks

- Now give your access and secret keys.

3. Provide the required credentials [Info](#)

Create an IAM role or user with the AWSApplicationMigrationAgentInstallationPolicy policy.

IAM access key ID

AKIAWX44AK7X6I3GIS2Y

IAM secret access key

This form does not send the secret – it only adds it to the installation command you can copy.

.....

Show

Session token

Session token is only required when using temporary credentials.

4. User provided resource id - optional [Info](#)

10. Once you have given the keys it will give you a command which you have to use on your Linux instance SSH session client and install it there.

5. Download the installer using this command:

```
sudo wget -O ./aws-replication-installer-init https://aws-application
```

 Copy

If you need to validate the installer hash, the correct hash can be found here:

<https://aws-application-migration-service-hashes-us-west-2.s3.us-west-2.amazonaws.com/latest/linux/aws-replication-installer-init.sha512>

6. Copy and input the command below into the command line on your source server

```
sudo chmod +x aws-replication-installer-init; sudo ./aws-replication- ▶
```

 Copy

11. Copy these commands there.

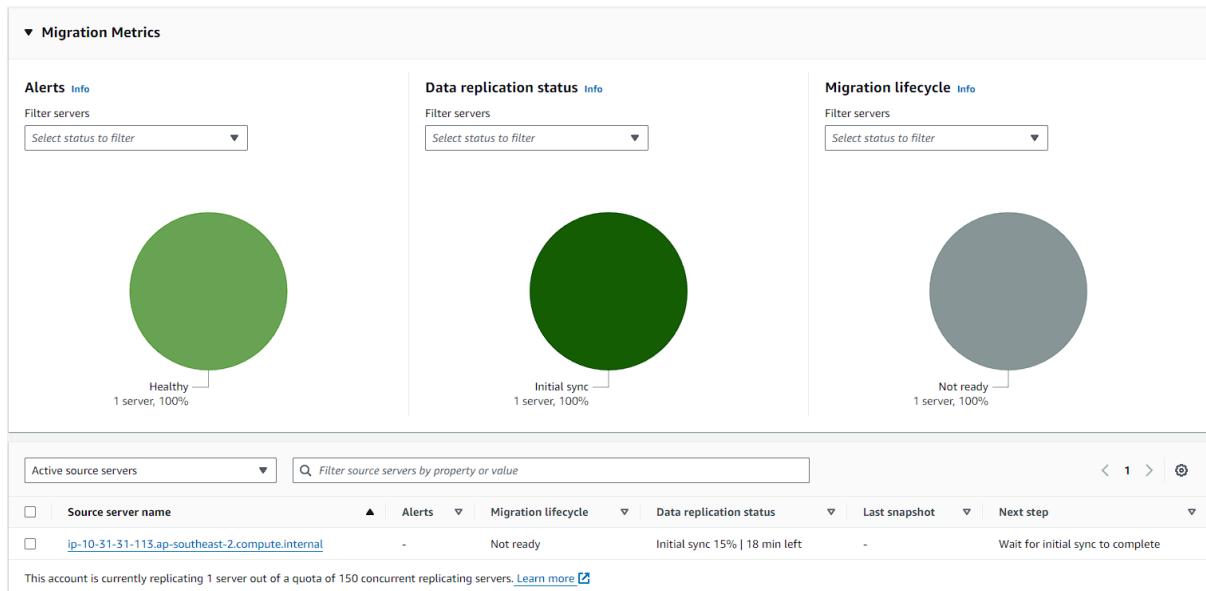
```
[root@ip-10-31-31-113 ~]# sudo wget -O /aws-replication-installer-init https://aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com/latest/linux/aws-replication-installer-init
2024-01-05 21:00:44 +0000 https://aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com/latest/linux/aws-replication-installer-init
Resolving aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com (aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com... 3.5.80.208, 3.5.83.159, 52.92.130.210, ...
[aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com (aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com) 3.5.80.208] connected.
HTTP request sent, awaiting response... 200 OK
Length: 10921096 [BOM] (application/octet-stream)
Saving to: '/aws-replication-installer-init'

100%[=====] 10,921,096 4.66MB/s in 2.2s

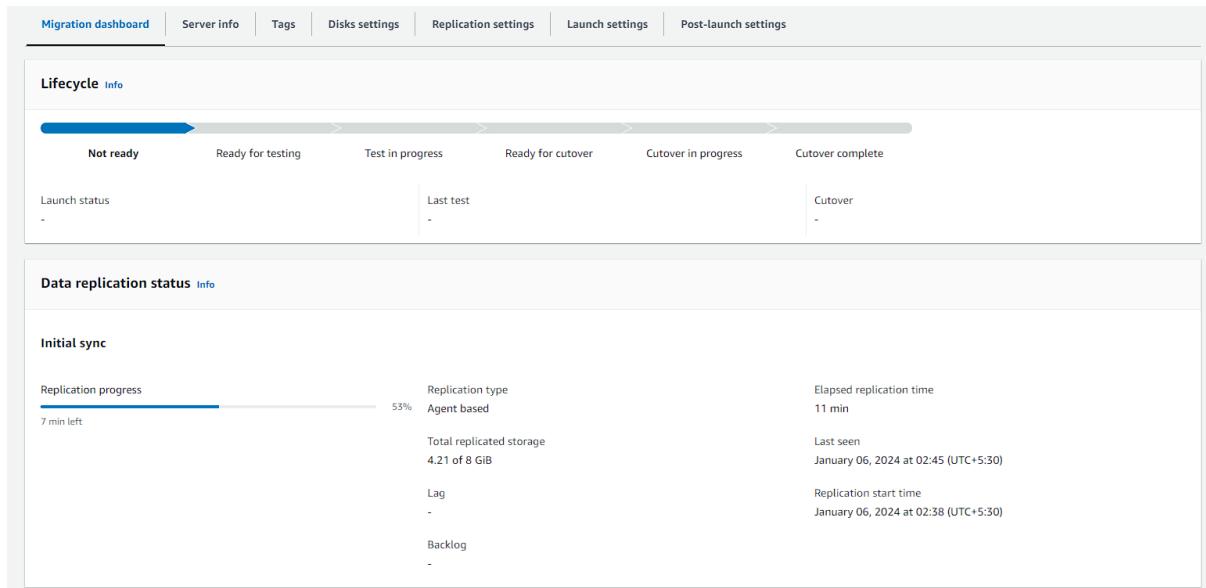
2024-01-05 21:00:47 (4.66 MB/s) - '/aws-replication-installer-init' saved [10921096/10921096]
```

```
[root@ip-10-31-31-113 ~]# sudo chmod +x aws-replication-installer-init; sudo ./aws-replication-installer-init --region us-west-2 --aws-access-key-id AKIAW44AK7X6I3G1S2Y --aws-secret-access-key jwNlVw+U3QifQH0CLf5BhJNwz2Kq17Spf3zA3
[sudo] password for root:
The installation of the AWS Replication Agent has started.
Identifying volumes for replication.
Identified volume for replication: /dev/xvda of size 8 GiB
8 GiB volume successfully identified.
Downloading the AWS Replication Agent onto the source server...
Finished.
Installing the AWS Replication Agent onto the source server...
Finished.
Syncing the source server with the Application Migration Service Console...
Finished
The following is the source server ID: -525Aaa969b0aa2c0c.
You now have 1 active source server out of a total quota of 150.
For more information about replication limits, see https://docs.aws.amazon.com/mgn/latest/ug/MGN-service-limits.html
The AWS Replication Agent was successfully installed.
[root@ip-10-31-31-113 ~]#
```

12. Once your commands have run successfully then if you go back to your MGN, then you will see, that a server has been added here.



13. And if you will open your server, you can see the data replication status.



14. Now you have to wait for some time, till the process gets complete.

The screenshot shows the Migration dashboard interface. At the top, there are tabs: Migration dashboard (selected), Server info, Tags, Disks settings, Replication settings, Launch settings, and Post-launch settings. Below the tabs, the Lifecycle section displays a progress bar with six stages: Not ready, Ready for testing (highlighted in blue), Test in progress, Ready for cutover, Cutover in progress, and Cutover complete. Under each stage, there are 'Launch status' and 'Last test' fields, all currently showing '-'. The Data replication status section indicates the process is 'Healthy'. It shows the following details:

Replication progress	Replication type	Elapsed replication time
Initial replication finished	Agent based	24 min
	Total replicated storage 8 of 8 GiB	Last seen January 06, 2024 at 02:57 (UTC+5:30)
	Lag -	Replication start time January 06, 2024 at 02:38 (UTC+5:30)
	Backlog -	

15. Now as Linux data has started migrating, move towards windows data.
16. Go in the Remote session of the windows instance and do the same thing there too.
17. First go to MGN and add a server for windows.
18. The process is almost same, select windows for the OS.
19. Then select replicate all disks.
20. Provide access and secret access keys.
21. Then you need to download an installer then copy it and paste it in the windows server.

AWS Replication Agent installation

1. Select your operating system

- Linux
 Windows
 Legacy OS: Windows Server 2003 or Windows Server 2008

2. Select your replication preferences [Info](#)

Replicate all disks



3. Provide the required credentials [Info](#)

Create an IAM role or user with the AWSApplicationMigrationAgentInstallationPolicy policy.

IAM access key ID

AKIAWX44AK7X6I3GIS2Y

IAM secret access key

This form does not send the secret – it only adds it to the installation command you can copy

.....

Show

Session token

Session token is only required when using temporary credentials

4. User provided resource id - *optional* [Info](#)

5. Download the [installer](#) onto your source server (or copy it there after downloading)

If you need to validate the installer hash, the correct hash can be found here:

<https://aws-application-migration-service-hashes-us-west-2.s3.us-west-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe.sha512>

22. After downloading the installer paste it in the windows server

23. Now open command prompt in the windows server



24. Open CMD and go to this path. Say to the desktop or to the path where you will install this AWS replication windows installer.
25. After that copy the code from MGN and paste it in the CMD, it will execute it and create a new server for data replication.

```
Administrator: Command Prompt - .\AwsReplicationWindowsInstaller.exe --region us-west-2 --aws-access-key-id AKIAWX44AK7X6l3Gis2Y --aws-secr...
Microsoft Windows [Version 10.0.20348.2159]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd c:\Users\Administrator\Desktop

C:\Users\Administrator\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is FCCD-25A0

Directory of c:\Users\Administrator\Desktop

01/05/2024  09:53 PM    <DIR>      .
01/05/2024  07:59 PM    <DIR>      ..
01/05/2024  09:51 PM        7,085,240 AwsReplicationWindowsInstaller.exe
06/21/2016  03:36 PM           527 EC2 Feedback.website
06/21/2016  03:36 PM           554 EC2 Microsoft Windows Guide.website
                           3 File(s)   7,086,321 bytes
                           2 Dir(s)  16,051,916,800 bytes free

C:\Users\Administrator\Desktop>.\AwsReplicationWindowsInstaller.exe --region us-west-2 --aws-access-key-id AKIAWX44AK7X6l3Gis2Y --aws-secret-access-key jwNlVs+U3QifJhQcLE+3RjlWowS2Xq375pfr34A3 --no-prompt
The installation of the AWS Replication Agent has started.
```

26. As you can see the command has been executed successfully.

```

c:\Users\Administrator\Desktop>.\AwsReplicationWindowsInstaller.exe --region us-west-2 --aws-access-key-id AKIAWX44AK7X6I3GIS2Y --aws-secret-access-key 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 --no-prompt
The installation of the AWS Replication Agent has started.
Verifying that the source server has enough free disk space to install the AWS Replication Agent (a minimum of 2 GB of free disk space is required).
Identifying volumes for replication.
Disk to replicate identified: c:0 of size 30 GiB
All volumes for replication were successfully identified.
Downloading the AWS Replication Agent onto the source server...
Finished.
Installing the AWS Replication Agent onto the source server...
Finished.
Syncing the source server with the Application Migration Service Console...
Finished.
The following is the source server ID: s-5785398d62575044c.
You now have 2 active source servers out of a total quota of 150.
Learn more about increasing source servers limit at https://docs.aws.amazon.com/mgn/latest/ug/MGN-service-limits.html
The AWS Replication Agent was successfully installed.

```

27. Now if you will come back to MGN you can see that a windows server has been created and it up and running to migrate data.

Application Migration Service > Active source servers > EC2AMAZ-MNFV449

EC2AMAZ-MNFV449 (s-5785398d62575044c)

Actions ▾ Replication ▾ Test and cutover ▾

Next actions [Info](#)

Wait for initial sync to complete

Migration dashboard [Server info](#) [Tags](#) [Disks settings](#) [Replication settings](#) [Launch settings](#) [Post-launch settings](#)

Lifecycle [Info](#)

Not ready > Ready for testing > Test in progress > Ready for cutover > Cutover in progress > Cutover complete

Launch status	Last test	Cutover
-	-	-

28. Below are the steps and progress.

Data replication status [Info](#)

Initiating

Replication progress	0%	Replication type	Agent based	Elapsed replication time	39 sec
		Total replicated storage	0 of 30 GiB	Last seen	January 06, 2024 at 03:31 (UTC+5:30)
		Lag	-	Replication start time	-
		Backlog	-		

Replication initiation steps

- ① Create security groups
- ② Launch Replication Server
- ③ Boot Replication Server
- ④ Authenticate with service
- ⑤ Download replication software
- ⑥ Create staging disks
- ⑦ Attach staging disks
- ⑧ Pair Replication Server with AWS Replication Agent
- ⑨ Connect AWS Replication Agent to Replication Server
- ⑩ Start data transfer

29. These are the two servers. They might take their time to replicate data.

Active source servers		Filter source servers by property or value				
	Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	EC2AMAZ-MNFV449	-	Not ready	Initial sync 1% 5 hr left	-	Wait for initial sync to complete
<input type="checkbox"/>	ip-10-31-31-113.ap-southeast-2.compute.internal	-	Ready for testing	Healthy	an hour ago	Launch test instance

This account is currently replicating 2 servers out of a quota of 150 concurrent replicating servers. [Learn more](#)

30. Now if you will go to EC2 of the destination region. You will see that a instance is up and running.

Instances (1) Info									
C Connect Instance state Actions Launch instances									
<input type="text"/> Find Instance by attribute or tag (case-sensitive) Clear filters									
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
AWS Application Migr...	i-0d6b1f6c548834470	Running Q Q	t2.micro	2/2 checks passed	View alarms +	us-west-2b	ec2-18-237-114-207.us...	18.237.114.207	-

31. And if you visit to the snapshots part of the EC2 under elastic block store (EBS).

32. You will see that snapshots are being created for your replicated data.

Snapshots (4) Info									
C Recycle Bin Actions Create snapshot									
Owned by me Search									
Name	Snapshot ID	Volume size	Description	Storage tier	Snapshot status	Started	Progress		
AWS Application Migration Service Snapshot	snap-05627bc7c80750b24	8 GiB	AWS Application Migration ...	Standard	Completed	2024/01/06 02:49 GMT+5:...	Available (1)		
AWS Application Migration Service Base Snapshot	snap-0c2261a59afea0817	1 GiB	AWS Application Migration ...	Standard	Completed	2024/01/06 02:35 GMT+5:...	Available (1)		
AWS Application Migration Service Snapshot	snap-0faeabff0c028c3a9	30 GiB	AWS Application Migration ...	Standard	Completed	2024/01/06 03:37 GMT+5:...	Available (1)		
AWS Application Migration Service Snapshot	snap-0f134d2bca91a9b5d	30 GiB	AWS Application Migration ...	Standard	Completed	2024/01/06 03:35 GMT+5:...	Available (1)		

STEP 5: Checking Server

1. Now go back to check if any one of your servers is healthy or not.

Active source servers		Filter source servers by property or value				
	Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	EC2AMAZ-MNFV449	-	Not ready	Initial sync 15% 3 hr left	-	Wait for initial sync to complete
<input type="checkbox"/>	ip-10-31-31-113.ap-southeast-2.compute.internal	-	Ready for testing	Healthy	3 minutes ago	Launch test instance

This account is currently replicating 2 servers out of a quota of 150 concurrent replicating servers. [Learn more](#)

2. As you can see the Linux is the one that is ready to get launched.

3. Now open it. Go to launch settings. Then click on modify EC2 launch template.

EC2 Launch Template Info		Modify
Template ID lt-0ff6bbccbb2e13121	Primary network interface	
Instance type (ignored when right-sizing is active) c5.large	Description	-
EBS volumes Volume 1 (8 GiB, EBS, General Purpose SSD (gp3))	Subnet	-
Security groups -	Public IP	No
Tenancy	Private IP addresses	-
Placement group -		

4. In there, first you need to give it a name.

Launch template name and version description

Launch template name

created-and-used-by-application-migration-service-s-5254aa969bdae2cac-240501-210506 (lt-0ff6bbccbb2e13121)

Template version description

lin-tm

Max 255 chars

Auto Scaling guidance | [Info](#)

Select this if you intend to use this template with EC2 Auto Scaling

Provide guidance to help me set up a template that I can use with EC2 Auto Scaling

► **Source template**

5. Then select instance type to t2.micro

▼ Instance type [Info](#) | [Get advice](#)

[Advanced](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Linux base pricing: 0.0116 USD per Hour
On-Demand SUSE base pricing: 0.0116 USD per Hour
On-Demand Windows base pricing: 0.0162 USD per Hour
On-Demand RHEL base pricing: 0.0716 USD per Hour

Free tier eligible

All generations

[Compare instance types](#)

[Additional costs apply for AMIs with pre-installed software](#)

6. In the network settings, select your subnet.

7. Then select your existing security group.

▼ Network settings [Info](#)

Subnet [Info](#)

subnet-0e332b1830a91b4cd

VPC: vpc-062d767592c9ad3e0 Owner: 463646775279

Availability Zone: us-west-2b IP addresses available: 4090 CIDR: 172.31.16.0/20

 [Create new subnet](#) 

When you specify a subnet, a network interface is automatically added to your template.

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

[Select existing security group](#)

[Create security group](#)

Common security groups [Info](#)

Select security groups

 [Compare security group rules](#)

aws-mgn-sg sg-038e634a017e9e1f4 

VPC: vpc-062d767592c9ad3e0

Security groups that you add or remove here will be added to or removed from all your network interfaces.

► Advanced network configuration

8. In the EBS volumes select volume type to gp2 and you can increase the size from 8gb to whatever you like. Disk Size totally depends on you.

▼ Storage (volumes) [Info](#)

EBS Volumes

[Hide details](#)

▼ Volume 1 (Template)

[Remove](#)

Storage type [Info](#)

EBS

Device name - *required* [Info](#)

/dev/xvda

Snapshot [Info](#)

Don't include in launch tem...

Size (GiB) [Info](#)

8

Volume type [Info](#)

gp2

IOPS [Info](#)

100 / 3000

Delete on termination [Info](#)

Don't include in launch tem...

Encrypted [Info](#)

Don't include in launch tem...

KMS key [Info](#)

Don't include in launch tem...

KMS keys are only applicable when encryption is set on this volume.

9. Once you have done all the above settings now modify it and you will see that these are the specification that you changed. Before the instance type was c5.large but now it is t2.micro

EC2 Launch Template Info		Modify
Template ID	lt-0ff6bbccbb2e13121	
Instance type (ignored when right-sizing is active)	t2.micro	
EBS volumes	Volume 1 (8 GiB, EBS, General Purpose SSD (gp2))	
Security groups	sg-038e634a017e9e1f4	
Tenancy	-	
Placement group	-	
Primary network interface		
Description	-	
Subnet	subnet-0e332b1830a91b4cd	
Public IP	No	
Private IP addresses	-	

10. Now go back and click on test and cutover, then click on Launch test instance.

Application Migration Service > Active source servers > ip-10-31-31-113.ap-southeast-2.compute.internal

ip-10-31-31-113.ap-southeast-2.compute.internal (s-5254aa969bdae2cac)

Actions ▾ Replication ▾ Test and cutover ▲

Testing

Next actions [Info](#) Launch test instances

11. Once you have done that you can see that a Conversion Server is also been started as an EC2 instance.

Instances (2) [Info](#)

View job details [X](#)

Launch job mgnjob-574b264d96e7b1642 created
Starting to launch test instance for 1 server.

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
<input type="checkbox"/>	AWS Application Migration Service Replication Server	i-0d6b1f6c548834470	Running	t2.micro	2/2 checks passed	View alarms +	us-west-2b	ec2-1
<input type="checkbox"/>	AWS Application Migration Service Conversion Server	i-088cb05538603d2c1	Running	m4.large	Initializing	View alarms +	us-west-2b	ec2-5

12. And if you come back to MGN you can see that the logs are generating and it is showing you what is going on the back end of the server.

Job log (4) [Info](#)

Filter job log by property or value [X](#)

Time	Event	Additional data
January 06, 2024 at 04:04 (UTC+5:30)	Job started	
January 06, 2024 at 04:04 (UTC+5:30)	Started taking snapshot	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal
January 06, 2024 at 04:05 (UTC+5:30)	Finished taking snapshot	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal
January 06, 2024 at 04:05 (UTC+5:30)	Conversion started	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal

13. Once the conversion is completed you can see that the Conversion server has stopped.

Instances (2) [Info](#)

Find Instance by attribute or tag (case-sensitive)

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public
<input type="checkbox"/>	AWS Application Migration Service Replication Server	i-0d6b1f6c548834470	Running	t2.micro	2/2 checks passed	View alarms +	us-west-2b	ec2-1
<input type="checkbox"/>	AWS Application Migration Service Conversion Server	i-088cb05538603d2c1	Stopping	m4.large	-	View alarms +	us-west-2b	ec2-5

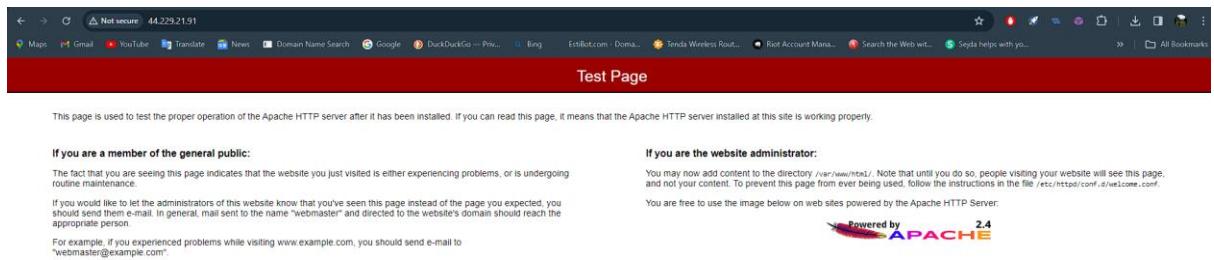
14. In the logs too, it has been stopped.

Job log (6) Info		
Time	Event	Additional data
January 06, 2024 at 04:04 (UTC+5:30)	Job started	
January 06, 2024 at 04:04 (UTC+5:30)	Started taking snapshot	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal
January 06, 2024 at 04:05 (UTC+5:30)	Finished taking snapshot	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal
January 06, 2024 at 04:05 (UTC+5:30)	Conversion started	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal
January 06, 2024 at 04:07 (UTC+5:30)	Conversion ended	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal Conversion Server instance ID: i-088cb05538603d2c1
January 06, 2024 at 04:07 (UTC+5:30)	Started launching test/ cutover EC2 instance	Source server : ip-10-31-31-113.ap-southeast-2.compute.internal

15. And if you go back to your instance which was created on the destination region, and if you copy its public IP after allocating it an elastic IP.

16. So, you can see your test which you created on the source region EC2 instance.

17. This means that our migration is successfully completed.

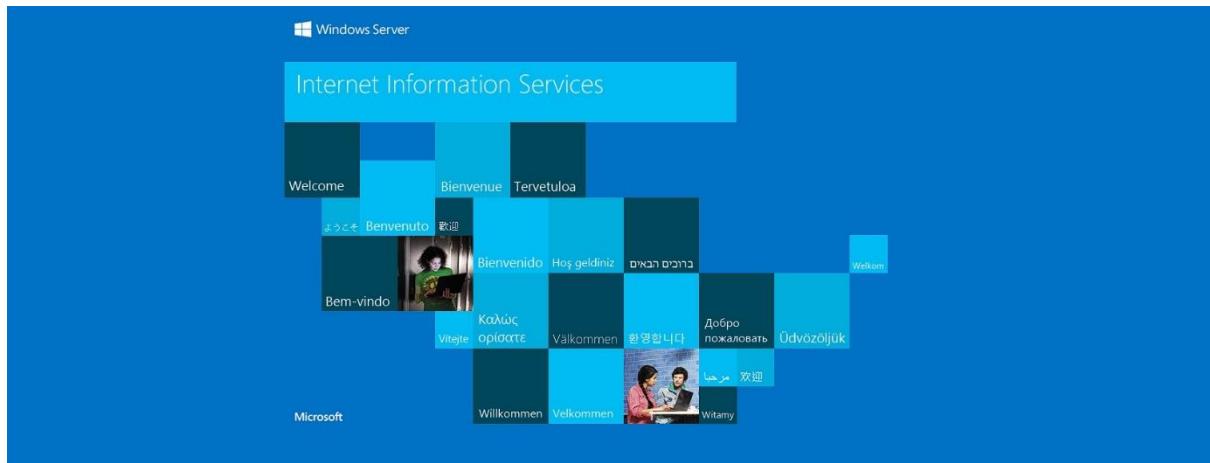


18. The same thing is going to happen with windows server too.

19. Check it in the MGN that is healthy or not and when it is healthy then you can go and modify its EC2 instance settings then you will see a conversion instance.

20. Once the conversion is complete then if you go its instance and allocate it with an elastic IP.

21. Then copy its public IP and paste it in a new browser, then you will see your IIS installed on it too. Which means that it has been migrated successfully.



AFTER COMPLETING YOUR MIGRATION DELETE ALL YOUR INSTACNES AND MGN ACCORDINGLY.

DO NOT FORGET TO DISSOCIATE YOUR ELASTIC IP.