



User Guide

Application Migration Service



Application Migration Service: User Guide

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon's trademarks and trade dress may not be used in connection with any product or service that is not Amazon's, in any manner that is likely to cause confusion among customers, or in any manner that disparages or discredits Amazon. All other trademarks not owned by Amazon are the property of their respective owners, who may or may not be affiliated with, connected to, or sponsored by Amazon.

Table of Contents

What Is AWS Application Migration Service?	1
Getting started	2
AWS Application Migration Service initialization and permissions	2
Initializing AWS MGN via the console	2
Creating the templates	4
Initializing AWS MGN via the API	5
Accessing the AWS Application Migration Service console	9
Supported AWS Regions	9
AWS MGN service quota limits	11
Using the AWS Migration Hub with AWS MGN	14
MGN technical training materials	15
Using the AWS Application Migration Service console	15
Source servers page	16
Migration workflow	17
Best practices	18
Planning	18
Testing	18
Successful implementation	18
Best practices for ensuring project success	19
Quick start guide	19
First time setup	19
Adding source servers	20
Configuring launch settings	22
Launching a test instance	23
Launching a cutover instance	28
Settings	32
Replication settings	32
Replication template vs individual server settings	33
Replication server settings	36
Launch template	52
General launch settings	53
Default EC2 launch template	54
MAP program tagging	55
Post-launch settings	55

Activating post-launch settings	56
Editing the post-launch settings template	58
Network requirements	74
Service architecture and network architecture overview	74
Network setting preparations	75
Staging area subnet	75
Network requirements	75
Operational subnets	76
Network requirements	76
Communication over TCP port 443	76
Communication between the source servers and AWS Application Migration Service over TCP port 443	78
Communication between the staging area subnet and AWS Application Migration Service over TCP port 443	82
Communication between the source servers and the staging area subnet over TCP port 1500	83
Source servers	84
Adding source servers	85
Installation requirements	85
AWS Replication Agent installation instructions	93
Supported operating systems	128
Agentless snapshot based replication for vCenter source environments	133
Agentless replication overview	133
Prerequisites	135
VMware limitations	135
Generating vCenter Client IAM credentials	136
Installing the AWS MGN vCenter Client	137
Replicating servers from vCenter to AWS	143
Updating the vCenter credentials	144
Differentiating agentless and agent-based servers	145
Source servers page	147
Interacting with the source servers page	148
Command menus	150
Migration metrics	156
Filtering	161
Server details	162

Migration dashboard	165
Server info	186
Tags	187
Disk settings	188
Replication settings	192
Launch settings	193
Post-launch settings	193
Applications	203
Applications page	203
Interacting with the Applications page	204
Commands menu	205
Filtering	211
Application details	212
Overview dashboard	214
Source server migration metrics	215
Source servers table	219
Tags	219
Waves	220
Waves page	220
Interacting with the Waves page	221
Commands menu	223
Filtering	228
Wave details	229
Overview dashboard	231
Applications	232
Source servers	235
Tags	239
MGN Connectors	240
Prerequisites for installing the MGN connector	240
Architecture overview when using MGN connector	241
Permissions	242
MGNConnectorInstallerRole	243
AWSApplicationMigrationConnectorManagementRole	243
Setup instructions	245
Installing the MGN connector on a secured network	246
Global view	246

Create VPC endpoints	247
Create a Route 53 inbound endpoint	248
Modify replication settings	248
Verify VPC endpoints are being used	249
MGN Connectors page	249
Interacting with the MGN connector page	250
Actions menu	251
MGN connector details	256
Import and export	258
Importing your data inventory	258
Importing your data inventory from a local disk	258
Importing your data inventory from an S3 bucket	259
Import history	260
Required permissions	261
Import parameters	262
Exporting your data inventory	264
Exporting your data inventory to a local disk	265
Exporting your data inventory to an S3 bucket	265
Export history	267
Required permissions	267
Amazon S3 bucket permission requirements	268
Export parameters	268
Bulk configuration editing	270
Global view	271
Setting up your AWS Organizations	271
Activate trusted access for application migration service	272
Setting up CloudFormation StackSets	273
Using an AWS KMS Customer Managed Key (CMK) for encryption in member account	274
Inviting an AWS account to join your organization	275
Using global view	275
Source servers in member accounts	275
Applications	277
Waves	278
Import/Export	278
Launching test and cutover instances	279
Preparing for test and cutover instance launch	279

Launch settings	280
General launch settings	282
EC2 launch template	288
Launching test instances	296
Ready for testing indicators	297
Starting a test	298
Reverting or finalizing a test	298
Launching cutover instances	300
Ready for cutover indicators	301
Starting a cutover	301
Reverting or finalizing a cutover	302
Launch history	304
Overview	305
Job details	306
Monitoring Application Migration Service	309
Monitoring with CloudWatch	309
MGN and EventBridge	310
Event samples	311
Registering event rules	313
Logging AWS Application Migration Service with AWS CloudTrail	314
AWS Application Migration Service information in CloudTrail	315
Understanding AWS Application Migration Service log file entries	316
Security	318
Overview	318
Identity and access management	319
Federated identity	319
Authenticating with identities	320
Grant permission to tag resources during creation	323
AWS managed policies	324
Managing access using policies	367
Using service-linked roles	371
Policy structure	382
Resilience	383
Infrastructure security	383
Compliance validation	385
Cross-service confused deputy prevention	385

Troubleshooting	388
Troubleshooting launch errors	388
Do I need to recreate the entire launch template for every version?	388
Error - AccessDeniedException - Must be admin user	390
VPCIdNotSpecified error	390
Error: Failed to connect using HTTP channel	390
Could not take up-to-date snapshot. Launching from snapshot taken on...	391
Troubleshooting communication errors	391
Solving communication problems over TCP Port 443 between the staging area and the AWS Application Migration Service	392
Authenticate with service errors	393
Calculating the required bandwidth for TCP Port 1500	393
Verifying communication over Port 1500	394
Solving communication problems over Port 1500	395
Troubleshooting agent issues	397
Error: Installation failed	397
Where can I find the AWS MGN Agent logs?	405
Troubleshooting agentless replication issues	405
Common replication errors	406
Agent not seen	407
Not converging	407
Snapshot failure	408
Unstable network	408
Failed to connect AWS replication Agent to replication software	408
Failed to establish communication with replication software	408
Failed to create firewall rules	408
Failed to authenticate with service	409
Failed to create staging disks	409
Failed to pair the replication agent with replication server	409
Unknown data replication error	410
Other troubleshooting topics	410
Re-initialize the AWS Application Migration Service	410
Windows license activation – AWS	411
Migration leaving behind replication volumes after cutover	411
Replication lag issues	411
Windows Driver changes	412

Windows Dynamic Disk troubleshooting	412
Deleting AWS MGN resources	412
Set UEFI boot mode	413
FAQ	414
General questions	414
Can AWS Application Migration Service protect or migrate physical servers?	415
What data is stored on and transmitted through Application Migration Service servers? ...	415
What should I consider when replicating Active Directory?	415
Does AWS Application Migration Service work with LVM and RAID configurations?	415
What is there to note regarding SAN/NAS support?	416
Does AWS Application Migration Service support Windows License migration?	416
Can you perform an OS (Operating System) upgrade with AWS Application Migration Service?	416
What are the AWS Application Migration Service quota limits?	416
What are the Private APIs used by AWS MGN to define actions in the IAM Policy?	418
Which post-launch scripts does AWS MGN support?	420
What happens if I use a custom DNS?	421
Can I use AWS Application Migration Service to migrate servers from VMware Cloud on AWS (VMC) to Amazon EC2?	421
When should I use AWS Elastic Disaster Recovery (AWS DRS) for migration?	421
Agent related	422
What does the AWS Replication Agent do?	423
What kind of data is transferred between the agent and the AWS Application Migration Service?	423
Can a proxy server be used between the source server and the AWS Application Migration Service console?	424
What are the prerequisites needed to install the AWS Replication Agent?	424
What ports does the AWS Replication Agent utilize?	424
What privileges does the AWS Replication Agent require?	424
Is it possible to install the agent on servers running operating systems that are not listed as supported?	425
What kind of resources does the AWS Replication Agent utilize?	425
Can AWS Application Migration Service migrate containers?	425
Does the AWS Replication Agent cache any data to disk?	425
How is communication between the AWS Replication Agent and the AWS Application Migration Service secured?	425

Is it possible to change the port the AWS Replication Agent utilizes from TCP Port 1500 to a different port?	426
How do I manually uninstall the AWS Application Migration Service agent from a server?	426
When do I need to reinstall the agent?	426
How much bandwidth does the AWS Replication Agent consume?	426
How many disks can the AWS Replication Agent replicate?	427
Is it possible to add a disk to replication without a complete resync of any disks that have already been replicated?	427
Is the AWS Replication Agent installed on launched test and cutover instances?	427
How do temporary credentials work?	427
Which Windows and Linux OSs support no-rescan upon reboot?	427
Agentless replication related	428
In which situations would you recommend using agentless replication (snapshot shipping)?	429
In which situations would you recommend using agent-based replication?	429
How does agentless replication work?	430
Does agentless replication require installing any component in the customer's source data center?	430
Is the agentless feature available in all Regions that AWS MGN service supports?	430
Does agentless replication support the same source operating systems that are supported by agent-based replication?	430
Is the agentless feature supported in CloudEndure migration?	430
Which virtualization environments are supported by the agentless feature?	430
On which operating systems can the MGN vCenter Client be installed?	430
Do I need to generate special credentials to install the MGN vCenter Client?	431
What are the agentless replication prerequisites?	431
How do I install the MGN vCenter Client?	431
Can a proxy server be used between the source server and the AWS Application Migration Service console?	431
Replication related	431
What is the lifecycle of the snapshots and volumes automatically created during migration?	432
What do Lag and Backlog mean during replication?	433
What is Continuous, Block level data replication?	433
What are the Replication initiation Steps?	433

Is the replicated data encrypted?	434
How is the Replication Server provisioned and managed in the Staging Area?	434
What type of replication server is utilized in the AWS Application Migration Service staging area?	435
Can we set specific IP addresses for the replication server or conversion server in the AWS Application Migration Service staging area?	435
Does AWS Application Migration Service compress data during replication?	435
Are events that are generated by the AWS Application Migration Service servers logged in Cloudtrail in AWS?	435
How many snapshots does AWS Application Migration Service create?	435
Does AWS Application Migration Service delete snapshots?	436
How much capacity is allocated to the staging area?	436
Why is 0.0.0.0:1500 added to inbound rules in the staging area?	436
Can AWS Application Migration Service replicate Oracle ASM?	436
How long does a rescan take?	436
How can I control the bandwidth used for replication?	436
Are migrations performed by Application Migration Service crash consistent?	436
How can I perform an SSL connectivity and bandwidth test?	437
AWS related	438
What does the AWS Application Migration Service Machine Conversion Server do?	439
What boot modes are supported by the AWS Application Migration Service?	439
How can we encrypt an unencrypted AWS Application Migration Service base snapshot? .	439
How do I change the server AMI on AWS after Migration?	440
Which AWS services are automatically installed when launching a test or cutover instance?	440
How long does it take to copy a disk from the AWS Application Migration Service staging area to production?	441
What are the differences between conversion servers and replication servers?	441
Can I prevent AWS Application Migration Service from cleaning up test instance resources in AWS?	441
Why are my Windows server disks read-only after launching the test or cutover instance?	442
What impacts the conversion and boot time of test and cutover instances?	442
How is the AWS Licensing Model Tenancy chosen for AWS Application Migration Service?	443
How does AWS Application Migration Service interact with Interface VPC Endpoints?	443

How do I use MGN with CloudWatch and EventBridge dashboards?	444
Does AWS MGN work with...?	446
Does AWS MGN work with Microsoft Windows Failover Clustering?	446
Does AWS MGN work with Bitlocker encryption?	446
Post-launch actions related	446
What operating systems does the post-launch actions framework support?	446
What version of AWS Systems Manager Agent will be installed on my instance?	446
Why is the AWS Systems Manager Agent not executing my post launch actions?	446
Release notes	448
June 2024	448
May 2024	448
March 2024	448
January 2024	448
December 2023	449
November 2023	449
September 2023	449
August 2023	449
June 2023	450
May 2023	450
April 2023	450
March 2023	451
January 2023	451
November 2022	452
August 2022	452
July 2022	452
June 2022	452
May 2022	453
February 2022	453
January 2022	453
December 2021	453
November 2021	453
October 2021	454
July 2021	454
April 2021	454
Document history	455
AWS Glossary	457

What Is 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.

Getting started with AWS Application Migration Service

Topics

- [AWS Application Migration Service initialization and permissions](#)
- [Accessing the AWS Application Migration Service console](#)
- [Supported AWS Regions](#)
- [AWS MGN service quota limits](#)
- [Using the AWS Migration Hub with AWS MGN](#)
- [MGN technical training materials](#)
- [Using the AWS Application Migration Service console](#)
- [Migration workflow](#)
- [Best practices](#)
- [Quick start guide](#)

AWS Application Migration Service initialization and permissions

In order to use AWS Application Migration Service (AWS MGN), the service must first be initialized for any AWS Region in which you plan to use AWS MGN.

You can initialize the service via the console or via the API.

During the initialization process:

- The required IAM roles and policies will be created.
- The required templates are configured.

Initializing AWS MGN via the console

AWS Application Migration Service (AWS MGN) must be initialized upon first use from within the AWS MGN console by creating a replication template.

Once you create the replication template, the initialization process takes place automatically.

⚠ Important

The AWS Application Migration Service can only be initialized by the IAM user with the "AdministratorAccess" managed policy attached in your AWS Account.

IAM role creation

During initialization the following IAM roles will be created.

1. **AWSServiceRoleForApplicationMigrationService**
2. **AWSApplicationMigrationReplicationServerRole**
3. **AWSApplicationMigrationConversionServerRole**
4. **AWSApplicationMigrationMGHRole**
5. **AWSApplicationMigrationLaunchInstanceWithDrsRole**
6. **AWSApplicationMigrationLaunchInstanceWithSsmRole**
7. **AWSApplicationMigrationAgentRole**

Learn more about [AWS Application Migration Service roles and managed policies](#).

Additional policies

You can create roles with granular permission for AWS Application Migration Service. The service comes with the following predefined managed IAM policies:

- **AWSApplicationMigrationFullAccess** – This policy provides permissions to all public APIs of AWS Application Migration Service (AWS MGN), as well as permissions to read KMS key information.
- **AWSApplicationMigrationEC2Access** – This policy allows Amazon EC2 operations required to use AWS Application Migration Service (AWS MGN) to launch the migrated servers as EC2 instances.
- **AWSApplicationMigrationSSMAccess** – This policy allows Amazon SSM operations required to use AWS Application Migration Service (AWS MGN) to run SSM documents post migration of source servers.

- **AWSApplicationMigrationReadOnlyAccess** – The read-only policy allows the user to view all data available in the AWS MGN console but does not allow them to modify any data or perform any actions. This policy also includes several EC2 read-only permissions.
- **AWSApplicationMigrationAgentPolicy** – This policy allows a user to install the AWS Replication Agent. [Learn more about installing the AWS Replication Agent.](#)
- **AWSApplicationMigrationAgentInstallationPolicy** – This policy allows a user to install the AWS Replication Agent. [Learn more about installing the AWS Replication Agent.](#)
- **AWSApplicationMigrationServiceEc2InstancePolicy** – This policy allows installing and using the AWS Replication Agent, which is used by AWS Application Migration Service (AWS MGN) to migrate source servers that run on EC2 (cross-Region or cross-AZ). An IAM role with this policy should be attached (as an EC2 Instance Profile) to the EC2 Instances.

You can find all of these policies in the [IAM Console](#).

Important

You must attach the `AWSApplicationMigrationFullAccess` and the `AWSApplicationMigrationEC2Access` policies to your users and roles in order to be able to launch test and cutover instances and to complete a full migration cycle with AWS MGN.

Creating the templates

As part of the initialization of AWS Application Migration Service, you have the opportunity to configure three templates.

- Replication template (mandatory)
- Launch template (optional)
- Post-launch template (optional)

Creating your replication template

To initialize AWS Application Migration Service, you must first create a replication template.

The replication template determines how data replication will work for each new server you add. The settings configured in this template will be applied to each newly added source server. [Learn more about the replication template.](#)

Configuring your launch template

As part of the AWS MGN initialization process, you can configure your launch template. Every source server added to AWS MGN has launch settings that control actions performed after the server is launched in AWS. These settings are created automatically based on this default launch template, which can be modified at any time. You can also choose to modify the launch template for an individual source server.

[Learn more about the launch template.](#)

Configuring a post-launch template

As part of the AWS MGN initialization process, you can configure your post-launch template. The post-launch template controls which post-launch actions will be executed when launching new instances. These settings are created automatically for each server based on the post-launch template and can be modified at any time. You can also modify the post-launch settings for any individual source server.

To configure the post-launch actions, complete the following steps:

1. [Activate post-launch actions.](#)
2. [Configure predefined post-launch actions](#) according to your preferences.
3. [Configure custom post-launch actions](#) according to your preferences.

Initializing AWS MGN via the API

You can initialize AWS Application Migration Service through the API. This option allows you to automate service initialization through a script when initializing multiple accounts.

To initialize the service via the API, take the following steps:

1. Create the required IAM roles.
2. Create the replication template and launch template.

Note

You must complete both steps to finalize the service initialization process.

Creating the required IAM roles

To initialize AWS MGN via the API, create the following IAM roles through the [IAM CreateRoleAPI](#). Learn more about [creating IAM roles in the AWS IAM documentation](#). Creation of each role must include the following parameters:

Role name	Trusted entities		
	Principal	Action	Condition
AWSApplicationMigrationReplicationServerRole	"ec2.amazonaws.com"	"sts:AssumeRole"	-
AWSApplicationMigrationConversionServerRole	"ec2.amazonaws.com"	"sts:AssumeRole"	-
AWSApplicationMigrationMGNRole	"mgn.amazonaws.com"	"sts:AssumeRole"	-
AWSApplicationMigrationLaunchInstanceWithDrsRole	"ec2.amazonaws.com"	"sts:AssumeRole"	-
AWSApplicationMigrationLaunchInstanceWithSsmRole	"ec2.amazonaws.com"	"sts:AssumeRole"	-
AWSApplicationMigrationAgentRole	"mgn.amazonaws.com"	["sts:AssumeRole", "sts:SetSourceIdentity"]	{"StringLike": {"sts:SourceIdentity": "s-*", "aws:SourceAccount": "<SOURCE-ACCOUNT-ID>"}}

Example using the AWS CLI without a source identity:

```
aws iam create-role --path "/service-role/" --role-name
AWSApplicationMigrationReplicationServerRole --assume-role-policy-document
{
  "Version": "2012-10-17",
```

```
"Statement": [  
  {  
    "Effect": "Allow",  
    "Principal": {  
      "Service": "ec2.amazonaws.com"  
    },  
    "Action": "sts:AssumeRole"  
  }  
]  
}
```

After the roles have been created, attach the following AWS managed policies to the roles through the [IAM AttachRolePolicy API](#). Learn more about [adding and removing IAM identity permissions in the AWS IAM documentation](#).

```
aws iam attach-role-policy --  
policy-arn arn:aws:iam::aws:policy/service-role/  
AWSApplicationMigrationReplicationServerPolicy --role-name  
AWSApplicationMigrationReplicationServerRole
```

Example using the AWS CLI with a source identity:

```
aws iam create-role --path "/service-role/" --role-name  
AWSApplicationMigrationAgentRole --assume-role-policy-document  
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Principal": {  
        "Service": "mgn.amazonaws.com"  
      },  
      "Action": [  
        "sts:AssumeRole",  
        "sts:SetSourceIdentity"  
      ],  
      "Condition": {  
        "StringLike": {  
          "sts:SourceIdentity": "s-*",  
          "aws:SourceAccount": "<SOURCE-ACCOUNT-ID>"  
        }  
      }  
    }  
  ]  
}
```

```
    }  
  ]  
}
```

1. Attach Managed Policy **AWSApplicationMigrationReplicationServerPolicy** to Role **AWSApplicationMigrationReplicationServerRole**
2. Attach Managed Policy **AWSApplicationMigrationConversionServerPolicy** to Role **AWSApplicationMigrationConversionServerRole**
3. Attach Managed Policy **AWSApplicationMigrationMGHAccess** to Role **AWSApplicationMigrationMGHRole**
4. Attach Managed Policies **AmazonSSMManagedInstanceCore** and **AWSElasticDisasterRecoveryEc2InstancePolicy** to Role **AWSApplicationMigrationLaunchInstanceWithDrsRole**
5. Attach Managed Policy **AmazonSSMManagedInstanceCore** to Role **AWSApplicationMigrationLaunchInstanceWithSsmRole**
6. Attach Managed Policy **AWSApplicationMigrationAgentPolicy_v2** to Role **AWSApplicationMigrationAgentRole**

Once the policies are attached to the roles, run the `aws mgn initialize-service` command. This will automatically create the service-linked role, create instance profiles, add Roles to Instance Profiles, and will finish service initialization.

[Learn more about AWS Application Migration Service roles and managed policies.](#)

Creating the templates

To finalize the initialization process, you will need to [create the replication template](#) and launch template by running the following commands:

- `aws mgn create-replication-configuration-template`
- `aws mgn create-launch-configuration-template`

Accessing the AWS Application Migration Service console

You can access AWS Application Migration Service through the AWS Console or through the following link:

<https://console.aws.amazon.com/mgn/home>

Supported AWS Regions

The following AWS Regions are supported by AWS Application Migration Service:

Region name	Region identity	Support in AWS Application Migration Service
US East (Ohio)	us-east-2	Yes
US East (N. Virginia)	us-east-1	Yes
US West (N. California)	us-west-1	Yes
US West (Oregon)	us-west-2	Yes
Africa (Cape Town)	af-south-1	Yes
Asia Pacific (Hong Kong)	ap-east-1	Yes
Asia Pacific (Jakarta)	ap-southeast-3	Yes
Asia Pacific (Melbourne)	ap-southeast-4	Yes
Asia Pacific (Mumbai)	ap-south-1	Yes
Asia Pacific (Hyderabad)	ap-south-2	Yes
Asia Pacific (Osaka)	ap-northeast-3	Yes
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes

Region name	Region identity	Support in AWS Application Migration Service
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes
Canada (Central)	ca-central-1	Yes
Europe (Frankfurt)	eu-central-1	Yes
Europe (Zurich)	eu-central-2	Yes
Europe (Ireland)	eu-west-1	Yes
Europe (London)	eu-west-2	Yes
Europe (Paris)	eu-west-3	Yes
Europe (Milan)	eu-south-1	Yes
Europe (Spain)	eu-south-2	Yes
Europe (Stockholm)	eu-north-1	Yes
Israel (Tel Aviv)	il-central-1	Yes
Middle East (Bahrain)	me-south-1	Yes
Middle East (UAE)	me-central-1	Yes
South America (São Paulo)	sa-east-1	Yes
AWS GovCloud (US-East)	us-gov-east-1	Yes
AWS GovCloud (US-West)	us-gov-west-1	Yes

Learn more about [AWS Regional services](#).

AWS Application Migration Service regional support includes [AWS Local Zones](#) associated with the above supported regions.

AWS MGN service quota limits

The following are the AWS MGN service quota limits:

Name	Default	Description
Concurrent jobs in progress	Each supported AWS Region: 20	Launching a test or cutover instance, or a cleanup action is considered a "job". This parameter is the maximum number of Jobs that can be run concurrently. Jobs that are "completed" are not counted against this quota.
Max active source servers	Each supported AWS Region: 150	The maximum number of servers that can be actively replicating at any time. For larger migrations, contact Support. Learn more about requesting a quota increase.
Max non-archived source servers	Each supported AWS Region: 4,000	This parameter is used for agentless migrations. This is the max number of servers that can be managed by MGN, in non-archived state. This includes the servers that are actively replicating, as well as any servers whose replication has not yet started. The number of actively replicating servers is controlled by the

Name	Default	Description
		<p>parameter "Max active source servers".</p> <p>For larger migrations, contact Support. Learn more about requesting a quota increase</p>
Max source servers in a single job	Each supported AWS Region: 200	Launching a test or cutover instance, or a cleanup action is considered a "Job". If you select multiple servers, and perform one of these actions, they are grouped into a single Job. This is the maximum number of servers that can be grouped into a single Job.
Max source servers in all jobs	Each supported AWS Region: 200	Launching a test or cutover instance, or a cleanup action is considered a "job". This is the maximum total number of servers that can be configured in all active jobs. Jobs that are "completed" are not counted against this quota.
Max total source servers per AWS account	Each supported AWS Region: 50,000	This parameter is the maximum total servers, both active and archived, that can be migrated in a single account in each AWS Region. Servers that are deleted, are not counted against this quota.

Name	Default	Description
Max concurrent jobs per source server	Each supported AWS Region: 1	Launching a test or cutover instance, or a cleanup action is considered a "job". This is the maximum number of active jobs, that can be configured per server. Jobs that are "completed" are not counted against this quota.
Max actions per source server	Each supported AWS Region: 100	This parameter is the maximum amount of custom post-migration actions that can be associated with a specific source server.
Max actions per account template	Each supported AWS Region: 100	This parameter is the maximum amount of custom post-migration actions that can be associated with an account template.
Max source servers per application	Each supported AWS Region: 200	This parameter is the maximum total servers, both active and archived, that can be added to an application.
Max active applications	Each supported AWS Region: 200	This parameter is the maximum number of applications that are in an active status.
Max archived applications	Each supported AWS Region: 10,000	This parameter is the maximum number of applications that are in an archived status.

Name	Default	Description
Max applications per wave	Each supported AWS Region: 1000	This parameter is the maximum total applications, both active and archived, that can be added to a wave.
Max active waves	Each supported AWS Region: 200	This parameter is the maximum number of waves that are in an active status.
Max archived waves	Each supported AWS Region: 10,000	This parameter is the maximum number of waves that are in an archived status.
Global View - Max Managed Accounts	5,000	This is the maximum number of member accounts that can be managed by a single management account.

You can learn about the AWS MGN service limits in the [AWS General Reference](#)

Using the AWS Migration Hub with AWS MGN

AWS Application Migration Service works with the AWS Migration Hub (MGH), allowing you to organize your servers into applications and then to track the progress of all your MGN at the server and app level, even as you move servers into multiple AWS Regions.

You must choose a Migration Hub Home Region for AWS MGN to work with the Migration Hub. [Learn more about choosing a Migration Hub Home Region.](#)

You can access the AWS Migration Hub from the AWS MGN navigation menu.

AWS Application Migration Service supports auto tagging in MGH. Migrated resources (Amazon EC2 instances or Amazon Machine Images (AMIs)) reported to Migration Hub by AWS MGN are automatically tagged with Application Discovery Service server IDs. If you turn on cost allocation tagging, you can view the cost of the AWS resources that are tagged by Migration Hub in the AWS Cost Explorer Service. Resource tagging by Migration Hub can't be turned off. This tagging

is implemented automatically and doesn't count against your limit of 50 tags per resource. Learn more about tagging migration resources in the [Migration Hub documentation](#).

MGN technical training materials

The following technical trainings are available for AWS MGN:

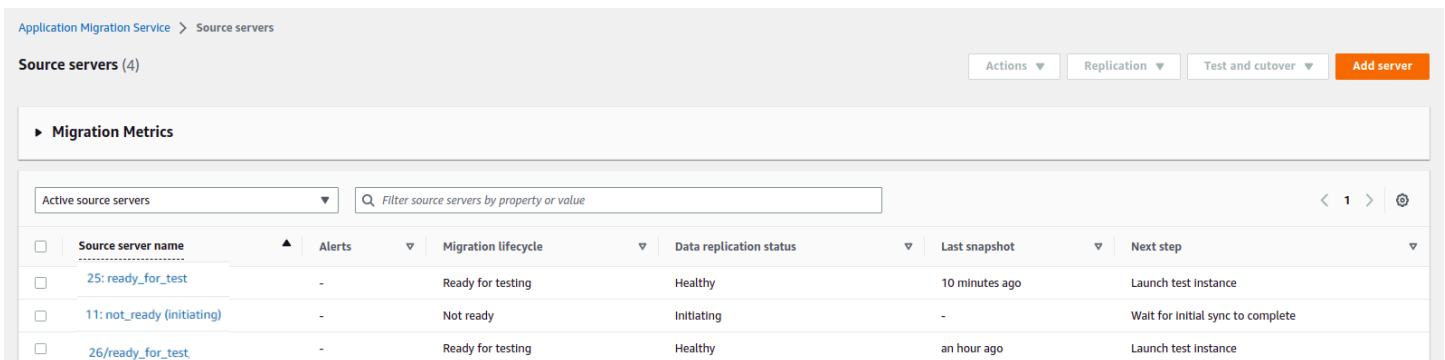
- [AWS Application Migration Service - A Technical Introduction](#)
- [Blog posts related to AWS MGN](#)
- [AWS MGN video playlist](#)

Using the AWS Application Migration Service console

AWS Application Migration Service is AWS Region-specific. Ensure that you select the correct Region from the **Select a Region** menu when using AWS Application Migration Service, just like you would with other AWS Region-specific services such as Amazon EC2.



AWS Application Migration Service is divided into several primary pages. Each page contains additional tabs and actions. The default view for the AWS Application Migration Service console is the **Source servers** page. This page automatically opens every time you open AWS Application Migration Service.

A screenshot of the AWS Application Migration Service console showing the 'Source servers' page. The page has a breadcrumb 'Application Migration Service > Source servers' and a title 'Source servers (4)'. There are buttons for 'Actions', 'Replication', 'Test and cutover', and 'Add server'. Below the title is a 'Migration Metrics' section with a dropdown for 'Active source servers' and a search bar 'Filter source servers by property or value'. A table lists the source servers with columns for 'Source server name', 'Alerts', 'Migration lifecycle', 'Data replication status', 'Last snapshot', and 'Next step'.

<input type="checkbox"/>	Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	25: ready_for_test	-	Ready for testing	Healthy	10 minutes ago	Launch test Instance
<input type="checkbox"/>	11: not_ready (initiating)	-	Not ready	Initiating	-	Wait for Initial sync to complete
<input type="checkbox"/>	26/ready_for_test	-	Ready for testing	Healthy	an hour ago	Launch test Instance

You can navigate to other AWS Application Migration Service pages through the left-hand **AWS Application Migration Service** navigation menu. You can also access the AWS Migration Hub and the AWS Application Migration Service documentation through this menu.

Each AWS Application Migration Service page will open in the right-hand main view. Here, you can interact with the various tabs, actions, and settings on the page.

Source servers page

The **Source servers** page lists all of the source servers you added to AWS Application Migration Service and allows you to interact with your servers and perform a variety of actions. [Learn more about the source servers page.](#)

- To control your source servers within the AWS Application Migration Service console, use the **Actions**, **Replication**, and **Test and cutover** menus. The commands within those menus influence the specific source servers you have selected. You can select a single source server or multiple source servers for any command by checking the box to the left of the server name.
- To review the progress of all commands, use the **Launch history** tab. [Learn more about Launch history.](#)
- Use the **Filter source servers...** box to filter servers based on a variety of parameters.

AWS Application Migration Service color codes the state of each source server. Use the **Alerts** column to easily determine the state of your server.

A clock icon with gray text indicates that the server is experiencing temporary issues. The nature of the issue will be identified (for example, "Lagging").

A red x and text indicates that the server is experiencing significant issues that need to be addressed before replication can resume. The nature of the issue will be indicated (for example, "Stalled")

When various commands are initiated, AWS Application Migration Service will display information messages at the top of the **Source Servers** page. Application Migration Service color codes these messages for clarity.

- A green message indicates that a command was completed successfully.
- A red message means that a command was not completed successfully.

Each message shows details and links to supplemental information.

AWS Application Migration Service allows you to interact with and manage each server. Choose the source server name to be redirected to the Server details view.

The **Server details** tab shows specific details for an individual server. From here, you can review the server's migration lifecycle and health, view various technical details, manage tags, manage disks, edit the server's replication settings, and edit the server's launch settings through the various tabs. [Learn more about the Server details view.](#)

Certain AWS Application Migration Service commands, such as **Edit replication settings**, allow you to interact with multiple source servers at once. When multiple source servers are selected by checking the box to the left of the server name and the **Replication > Edit replication settings** option is chosen, AWS Application Migration Service will indicate which servers are being edited.

For your changes to take effect, click **Save** at the bottom of each settings page.

Migration workflow

The general process is:

1. Initialize AWS Application Migration Service in the target region. Refer to the [list](#) of supported AWS regions.
2. Install the AWS Replication Agent on the source server. Learn more about [agent installation](#).

Note

If you are using the agentless replication for vCenter feature, then you will need to add your source servers by installing the AWS MGN vCenter Client. [Learn more about agentless replication.](#)

3. Wait until the initial sync is finished. After installing the agent, you need to wait for the initial synchronization process to complete. This process performs block level replication from the source server to the replication server in staging area.
4. Launch test instances. Once the initial sync is finished, you can launch a target machine in Test Mode. This allows you to perform acceptance testing and verify that the migrated environment is functioning correctly.
5. Perform acceptance tests on the servers. After the test instance is tested successfully, finalize the test and delete the test instance.
6. Configure Post-launch actions (if needed). Learn more about [Post-launch settings](#).
7. Wait for the cutover window.
8. Confirm that there is no lag.

9. Stop all operational services on the source server.
10. Launch a cutover instance. Launch the target machine in Cutover Mode, which initiates the final migration process.
11. Confirm that the cutover instance was launched successfully and then finalize the cutover.
12. Archive the source server.

Best practices

Planning

1. Plan your Migration project prior to installing the AWS Replication Agent on your source servers.
2. Do not perform any reboots on the source servers prior to a cutover.
3. Do not archive or disconnect the source server from AWS until your launched cutover instance in AWS is working as expected.

Testing

1. Perform test at least two weeks before you plan to migrate your source servers. This time frame is intended for identifying potential problems and solving them, before the actual cutover takes place. After performing the test launch, validate connectivity to your test instances (using SSH for Linux or RDP for Windows), and perform acceptance tests for your application.
2. Ensure that you perform a Test prior to performing a cutover.

Successful implementation

The following are the required steps to complete a successful migration implementation with AWS Application Migration Service:

1. Deploy the AWS Replication Agent on your source servers.
2. Confirm that the data replication status is **Healthy**.
3. Test the launch of Test instances a week before the actual cutover.
4. Address any issues that come up, such as Launch setting misconfiguration and potential AWS limits. .
5. Launch cutover instances for the servers on the planned date.

Best practices for ensuring project success

1. Train a field technical team & assign an AWS Application Migration Service SME.
2. Share project timelines with AWS Application Migration Service.
3. Monitor data replication progress and report any issues in advance.
4. Perform a test for every server in advance, and report issues to AWS Application Migration Service.
5. Coordinate cutover windows with AWS Application Migration Service in advance.

Quick start guide

This section will guide you through first time AWS Application Migration Service setup, including:

Topics

- [First time setup](#)
- [Adding source servers](#)
- [Configuring launch settings](#)
- [Launching a test instance](#)
- [Launching a cutover instance](#)

First time setup

The first setup step for AWS Application Migration Service is creating the replication template.

Choose **Get started** on the AWS Application Migration Service landing page.

You will automatically be prompted to initialize the service the first time you log into AWS Application Migration Service.

Initializing the service will create a replication template. This template will determine how data replication will work for each newly added source server.

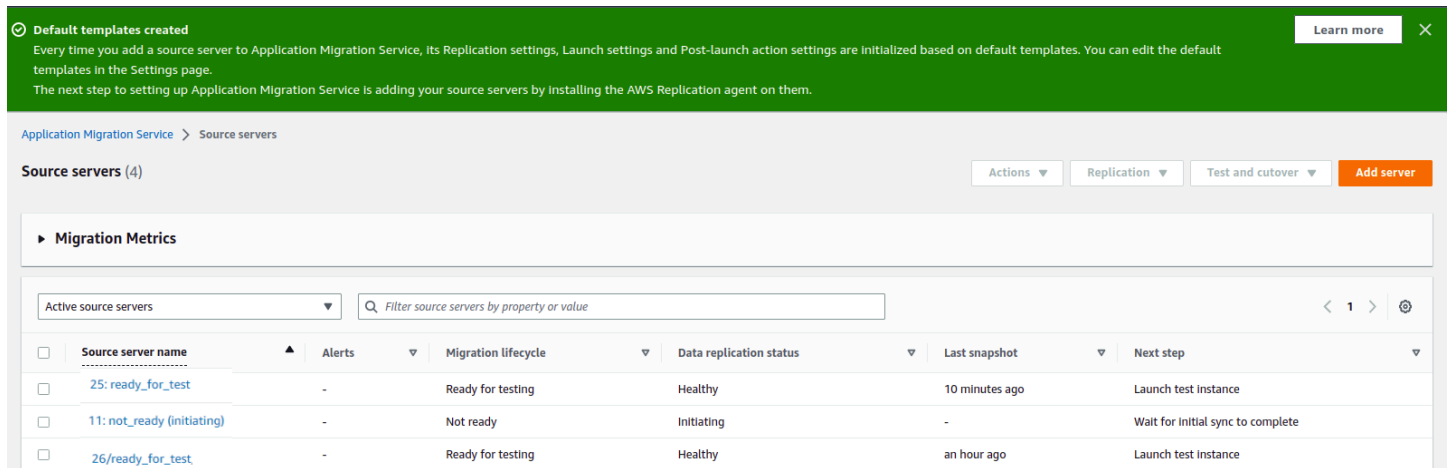
The configured replication settings can be changed at any time for any individual source server or group of source servers. [Learn more about replication settings.](#)

[Learn more about changing individual server and multiple server replication settings.](#)

Important

Prior to configuring your replication template, ensure that you meet the [Network requirements for running AWS Application Migration Service](#).

Once AWS Application Migration Service is initialized you'll be redirected into the AWS Application Migration Service console **Source servers** page.



Application Migration Service > Source servers

Source servers (4) Actions Replication Test and cutover Add server

Migration Metrics

Active source servers < 1 > ⚙

<input type="checkbox"/>	Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	25: ready_for_test	-	Ready for testing	Healthy	10 minutes ago	Launch test instance
<input type="checkbox"/>	11: not_ready (initiating)	-	Not ready	Initiating	-	Wait for initial sync to complete
<input type="checkbox"/>	26/ready_for_test	-	Ready for testing	Healthy	an hour ago	Launch test instance

To edit your replication template, click **Replication template** on the left-hand navigation menu. You will be able to edit individual server replication settings after adding your source servers to AWS Application Migration Service.

The next step of the setup process is adding your source servers to AWS Application Migration Service.

Adding source servers

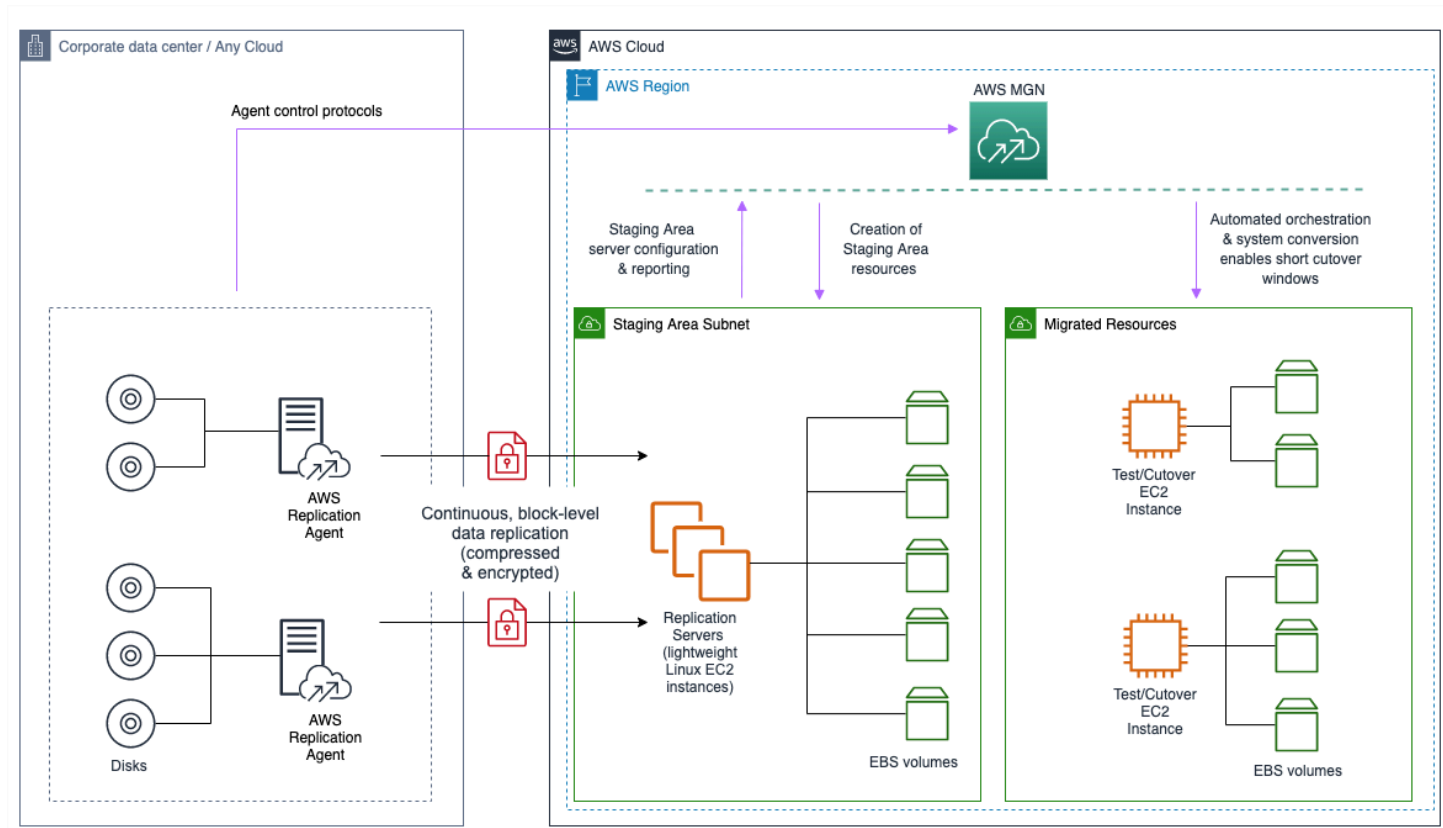
Add source servers to AWS Application Migration Service by installing the AWS Replication Agent (also referred to as "the Agent") on them. The Agent can be installed on both Linux and Windows servers. [Learn more about adding source servers](#).

Note

If you are using the agentless replication for vCenter feature, then you will need to add your source servers by installing the AWS MGN vCenter Client. [Learn more about agentless replication](#).

Prior to adding your source servers, ensure that you meet all of the [network requirements](#).

The following is the AWS MGN agent network architecture diagram:



Migration lifecycle

After the source server has been added to AWS Application Migration Service, it will undergo the migration lifecycle steps.

The migration lifecycle shows the current state of each source server within the migration process. Lifecycle states include:

- **Not ready** – The server is undergoing the initial sync process and is not yet ready for testing. Data replication can only commence once all of the initial sync steps have been completed.
- **Ready for testing** – The server has been successfully added to AWS Application Migration Service and data replication has started. test or cutover instances can now be launched for this server.
- **Test in progress** – A Test instance is currently being launched for this server.
- **Ready for cutover** – This server has been tested and is now ready for a cutover instance to be launched.

- **Cutover in progress** – A cutover instance is currently being launched for this server.
- **Cutover complete** – This server has been cutover. All of the data on this server has been migrated to the AWS cutover instance.
- **Disconnected** – This server has been disconnected from AWS Application Migration Service.

[Learn more about the migration lifecycle states.](#)

Once the initial async process has completed successfully, data replication will start automatically.


Configuring launch settings

After you have added your source servers to the AWS Application Migration Service console, you will need to configure the launch settings for each server. The launch settings are a set of instructions that determine how a test or cutover instance will be launched for each source server on AWS. You must configure the launch settings prior to launching test or cutover instances. You can use the default settings or configure the settings to fit your requirements.

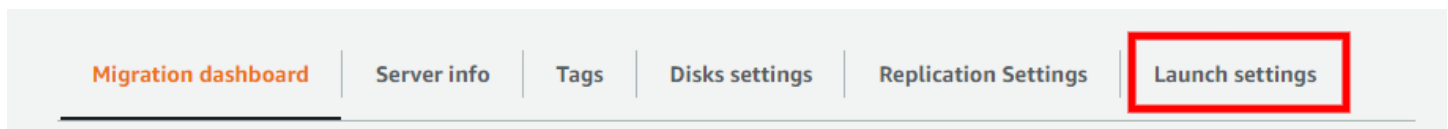
Note

You can change the launch settings after a test or cutover instance has been launched. You will need to launch a new test or cutover instance for the new settings to take effect.

You can access the launch settings by clicking on the source server name of a source server on the **Source servers** page.

	Source server name	Alerts	Replication type	Migration lifecycle	Data replication status	Last snapshot
<input type="checkbox"/>	25: ready_for_test (stalled)	 Stalled	Agent based	Ready for testing	Stalled	a day ago

Within the individual server view, navigate to the **Launch settings** tab.



Here you can see your **General launch settings** and **EC2 launch template**. Click the **Edit** button to edit your Launch settings or **Modify** to change your EC2 launch template.

Launch settings are composed of the following:

- **Instance type right-sizing** – The Instance type right-sizing feature allows AWS Application Migration Service to launch a test or cutover instance type that best matches the hardware configuration of the source server. When activated, this feature overrides the instance type selected in the EC2 launch template.
- **Start instance upon launch** – Choose whether you want to start your test and cutover instances automatically upon launch or whether you want to start them manually through the Amazon EC2 Console.
- **Copy private IP** – Choose whether you want Application Migration Service to verify that the private IP used by the test or cutover instance matches the private IP used by the source server.
- **Transfer server tags** – Choose whether you want AWS Application Migration Service to transfer any user-configured custom tags from your source servers to your test or cutover instance.
- **OS Licensing** – Choose whether you want to Bring Your Own Licenses (BYOL) from the source server to the test or cutover instance.

AWS Application Migration Service automatically creates an **EC2 launch template** for each new source server. AWS Application Migration Service bases the majority of the instance launch settings on this template. You can edit this template to fit your needs.

[Learn more about Launch settings.](#)

Launching a test instance

After you have added all of your source servers and configured their launch settings, you are ready to launch a test instance. It is crucial to test the migration of your source servers to AWS prior to initiating a cutover in order to verify that your source servers function properly within the AWS environment.

Important

It is a best practice to perform a test at least two weeks before you plan to migrate your source servers. This time frame allows you to identify potential problems and solve them, before the actual cutover takes place. After launching test instances, use either SSH (Linux) or RDP (Windows) to connect to your instance and ensure that everything is working correctly.

You can test one source server at a time, or simultaneously test multiple source servers. For each source server, you will be informed of the success or failure of the test. You can test your source server as many times as you want. Each new test first deletes any previously launched test instance and dependent resources. Then, a new test instance is launched, which reflects the most up-to-date state of the source server. After the test, data replication continues as before. The new and modified data on the source server is transferred to the staging area subnet and not to the test instances that were launched during the test.

Note

- When launching a test or custover instance, you can launch up to 100 source servers in a single operation. Additional source servers can be launched in subsequent operations.
- Windows source servers need to have at least 2 GB of free space to successfully launch a test instance.
- Take into consideration that once a test instance is launched, actual resources will be used in your AWS account and you will be billed for these resources. You can terminate the operation of launched Test instances once you verify that they are working properly without impact in order to data replication.

Ready for testing indicators

Prior to launching a Test instance, ensure that your source servers are ready for testing by looking for the following indicators on the **Source servers** page:

1. Under the **Migration lifecycle** column, the server should show **Ready for testing**.
2. Under the **Data replication status** column, the server should show the **Healthy** status.
3. Under the **Next step** column, the server should show **Launch test instance**.

<input type="checkbox"/>	Source server name ▲	Alerts ▼	Replication type ▼	Migration lifecycle ▼	Data replication status	Last snapshot ▼	Next step ▼
<input type="checkbox"/>	21: ready_for_test	-	Agent based	Ready for testing	Healthy	21 hours ago	Launch test instance

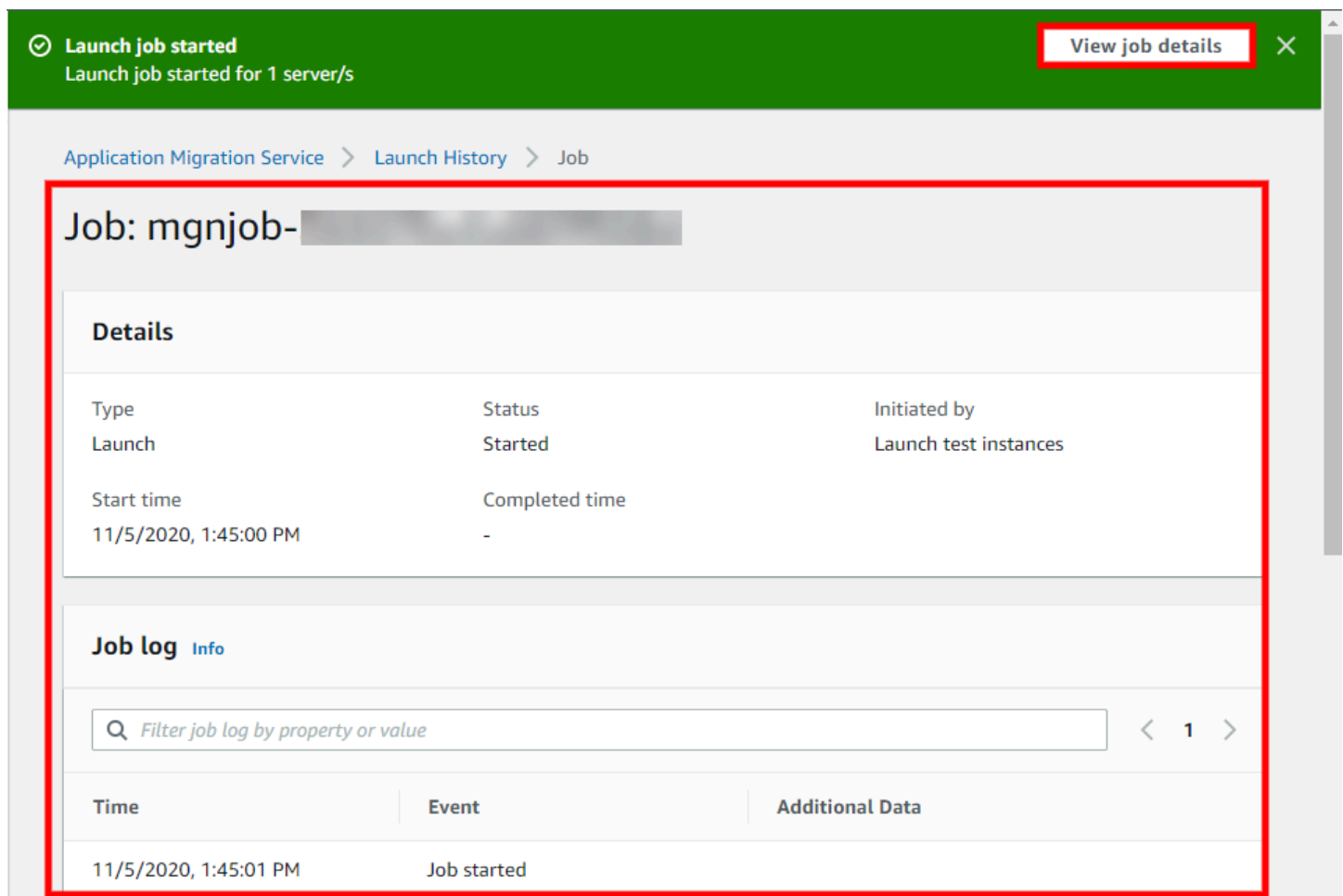
Starting a test

To launch a test instance for a single source server or multiple source servers, take the following steps:

- Go to the **Source servers** page and check the box to the left of each server for which you want to launch a test instance.
- Open the **Test and cutover** menu.
- Under **Testing**, choose the **Launch test instances** option to launch a test instance for this server.
- When the **Launch test instances for X servers** dialog appears, choose **Launch** to begin the test.

The AWS Application Migration Service console will indicate **Launch job started** when the test has started.

Choose **View job details** on the dialog to view the specific Job for the test launch in the **Launch History** tab.



The screenshot shows the AWS Application Migration Service console. At the top, a green notification banner displays a checkmark icon, the text "Launch job started", and "Launch job started for 1 server/s". A red box highlights a "View job details" button with a close icon (X) in the top right corner of the notification.

Below the notification, the breadcrumb navigation reads "Application Migration Service > Launch History > Job". The main content area is titled "Job: mgnjob-[redacted]".

The "Details" section contains the following information:

Type	Status	Initiated by
Launch	Started	Launch test instances

Start time	Completed time
11/5/2020, 1:45:00 PM	-

The "Job log" section includes an "Info" link, a search box with the placeholder text "Filter job log by property or value", and a page indicator showing "< 1 >".

The job log table has the following data:

Time	Event	Additional Data
11/5/2020, 1:45:01 PM	Job started	

Successful test launch indicators

You can tell that the Test instance launch started successfully through several indicators on the **Source Servers** page.

1. The Alerts column will show the **Launched** status, indicating that a test instance has been launched for this server.
2. The **Migration lifecycle** column will show **Test in progress**.
3. The **Next step** column will show **Complete testing and mark as 'Ready for cutover'**.

Reverting or finalizing a test

After you have launched your test instances, open the Amazon EC2 Console and SSH or RDP into your test instances in order to ensure that they function correctly. Validate connectivity and perform acceptance tests for your application.

Reverting a test

If you encounter any issues and want to launch new test instances, or if you are performing a scheduled test and plan to perform additional tests prior to cutover, you can revert the test. This will revert your source servers' **Migration lifecycle** status to **Ready for testing**, indicating that these servers still require additional testing before they are ready for cutover. During a revert, you will also have the option to delete your Test instances for cost-saving purposes.

To revert a test:

1. Check the box to the left of every source server that has a launched test instance for which you want to revert the test.
2. Open the **Test and cutover** menu.
3. Under **Testing**, choose **Revert to "ready for testing"**
4. When the **Revert testing for X servers** dialog appears, select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Revert**.

The AWS Application Migration Service console will indicate that testing has been reverted. The selected source servers' **Migration lifecycle** column will show the **Ready for testing** status,

the **Next step** column will show **Launch test instance** and the launched Test instances will be deleted if that option was selected.

Marking as Ready for cutover

If you are completely done with your testing and are ready for cutover, you can finalize the test. This will change your source servers' **Migration lifecycle** status to **Ready for cutover**, indicating that all testing is complete and that these servers are now ready for cutover. You will also have the option to delete your Test instances for cost saving purposes.

To finalize a test:

1. Check the box to the left of every source server that has a launched Test instance for which you want to finalize the test.
2. Open the **Test and Cutover** menu.
3. Under **Testing**, choose **Mark as "Ready for cutover"**
4. Mark X servers as "Ready for cutover" dialog will appear. Select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Continue**.
5. The AWS Application Migration Service console will confirm that the servers were marked as ready for cutover.

The console will indicate that testing has been finalized. The selected source servers' **Migration lifecycle** column will show the **Ready for cutover** status and the launched test instances will be deleted if that option was selected. The **Next step** column will show **Terminate launched instance; Launch cutover instance**.

6. You can now terminate the launched test instance directly from the Amazon EC2 Console as that instance is no longer needed (if you have not done so already through the AWS MGN Console). You can quickly access the Test instance by navigating to the specific servers > **Server Details** > **Migration dashboard** > **Lifecycle** > **Launch status** and choosing **View in EC2 Console**.
7. The Amazon EC2 Console will automatically search for and display the test instance. Select the instance, open the **Instance state** menu, and choose **Terminate instance**. When the confirmation dialogue appears, click **Terminate**.

Launching a cutover instance

Once you have finalized the testing of all of your source servers, you are ready for cutover. You should perform the cutover at a set date and time. The cutover will migrate your source servers to the cutover instances on AWS.

Important

It is a best practice to perform a test at least two weeks before you plan to migrate your source servers. This time frame allows you to identify potential problems and solve them, before the actual migration takes place. After launching test instances, use either SSH (Linux) or RDP (Windows) to connect to your instance and ensure that everything is working correctly.

You can cutover one source server at a time, or simultaneously cutover multiple source servers. For each source server, you will be informed of the success or failure of the cutover. For each new cutover, AWS Application Migration Service first deletes any previously launched Test instance and dependent resources. Then, it launches a new cutover instance which reflects the most up-to-date state of the source server. After the cutover, data replication continues as before. The new and modified data on the source server is transferred to the Staging Area Subnet, and not to the cutover instances that were launched during the cutover.

Ready for cutover indicators

Prior to launching a cutover instance, ensure that your source servers are ready for cutover by looking for the following indicators on the **Source Servers** page:

1. Under the **Migration lifecycle** column, the server should show **Ready for cutover** .
2. Under the **Data replication status** column, the server should show the **Healthy** status.
3. Under the **Next step** column, the server should show **Terminate launched instance; Launch cutover instance** if you have not terminated your latest launched test instance.
4. Alternatively, the Next step column will show **Launch cutover instance** if you have terminated your latest launched test instance.

Starting a cutover

To launch a cutover instance for a single source server or multiple source servers, take the following steps:

1. Go to the **Source servers** page and check the box to the left of each server you want to cutover.
2. Open the **Test and cutover** menu.
3. Under **Cutover**, choose the **Launch cutover instances** option.
4. When the **Launch cutover instances for X servers** dialog appears, choose **Launch** to begin the cutover.

On the **Source servers** page, the **Migration lifecycle** column will show **Cutover in progress** and the **Next step** column will show **Finalize cutover**. When the cutover starts, the Application Migration Service Console will indicate **Launch job started**.

5. Choose **View job details** on the dialog to view the specific Job for the cutover launch in the **Launch History** tab.

Successful cutover launch indicators

You can tell that the cutover instance launch was started successfully through several indicators on the **Source servers** page.

1. The **Alerts** column will state **Launched**.
2. The **Migration lifecycle** column will state **Cutover in progress**.
3. The **Data replication status** will state **Healthy**.
4. The **Next step column** will state **Finalize cutover**.

Reverting or finalizing a cutover

Once you have launched your cutover instances, open the Amazon EC2 Console and SSH or RDP into your cutover instances in order to ensure that they function correctly. Validate connectivity and perform acceptance tests for your application.

Note

You should turn on Termination Protection after you have completed your testing and before you are ready to finalize the cutover. Learn more about enabling termination protection in [this Amazon EC2 article](#).

Reverting a cutover

If you encounter any issues and want to launch new cutover instances, you can revert the cutover. This will revert your source servers' **Migration lifecycle** status to **Ready for cutover**, indicating that these servers have not undergone cutover. During a revert, you will also have the option to delete your Cutover instances for cost-saving purposes.

To revert a cutover:

1. Check the box to the left of every source server that has a launched cutover instance you want to revert.
2. Open the **Test and cutover** menu.
3. Under **Cutover**, choose **Revert to "ready for cutover"**
4. This will revert your source servers' **Migration lifecycle** status to **Ready for cutover**, indicating that these servers have not undergone cutover.

When the **Revert cutover for X servers** dialog appears, click **Revert**.

initializing a cutover

If you are completely done with your migration and performed a successful cutover, you can finalize the cutover. This will change your source servers' **Migration lifecycle** status to **Cutover complete**, indicating that the cutover is complete and that the migration has been performed successfully. In addition, this will stop data replication and cause all replicated data to be discarded. All AWS resources used for data replication will be terminated.

To finalize a cutover:

1. Check the box to the left of every source server that has a launched cutover instance you want to finalize.
2. Open the **Test and cutover** menu.

3. Under **Cutover**, choose **Finalize cutover**.
4. The **Finalize cutover for X servers** dialog will appear. Choose **Finalize**. This will change your source servers' **Migration lifecycle** status to **Cutover complete**, indicating that the cutover is complete and that the migration has been performed successfully. In addition, this will stop data replication and cause all replicated data to be discarded. All AWS resources used for data replication will be terminated.

The AWS Application Migration Service console will indicate **Cutover finalized** when the cutover has completed successfully.

The AWS Application Migration Service console will automatically stop data replication for the source servers that were cutover in order to save resource costs. The selected source servers' **Migration lifecycle** column will show the **Cutover complete** status, the **Data replication** status column will show **Disconnected**, and the **Next step** column will show **Mark as archived**. The source servers have now been successfully migrated into AWS.

5. You can now archive your source servers that have launched cutover instances. Archiving will remove these source servers from the main **Source servers** page, allowing you to focus on source servers that have not yet been cutover. You will still be able to access the archived servers through filtering options.

To archive your cutover source servers:

- a. Check the box to the left of the of each source server for which the **Migration lifecycle** column states **Cutover complete**.
- b. Open the **Actions** menu and choose **Mark as archived**.
- c. When the **Archive X server** dialog appears, click **Archive**.
- d. To see your archived servers, choose **Archived source servers** from the drop-down menu in the source servers view.

You will now be able to see all of your archived servers. Use the same drop-down menu to see only **Active source servers** or **Discovered source servers**, according to your preferences.

Settings

AWS Application Migration Service uses replication settings to determine how data will be replicated from your source servers to AWS. The following documentation explains how to configure your initial replication template and how to set individual server replication settings.

You must configure the replication template upon first use of AWS Application Migration Service. The replication template determines how your servers will be replicated to AWS through a variety of settings, including Replication Server instance type, Amazon EBS volume type, Amazon EBS encryption, security groups, data routing, and tags. The settings configured in the replication template are automatically passed down to every server you add to AWS Application Migration Service.

Once you have configured your Replication template, you can make changes to individual servers or a group of servers by editing their replication settings within the Server Details View.

You can also configure optional post-launch settings that will automate target instance deployment and prepare your migrated servers for disaster recovery with Elastic Disaster Recovery (AWS DRS).

Topics

- [Replication settings](#)
- [Launch template](#)
- [Post-launch settings](#)

Replication settings

Replication settings determine how data will be replicated from your source servers to AWS. Your replication settings are governed by the replication template, which you must configure before adding your source servers to AWS Application Migration Service. You can later edit the replication settings at any point. The settings configured in the replication settings template are then transferred to each newly added server.

You can edit the replication settings for each server or group of servers after the servers have been added to AWS Application Migration Service.

In addition, you can control a variety of other source server settings through the **Settings** section on the left-hand menu.

Topics

- [Replication template vs individual server settings](#)
- [Replication server settings](#)

Replication template vs individual server settings

The Replication template determines how data replication will work for each new server you add to AWS Application Migration Service. The settings configured in this template will be applied to each newly added source server. You will be prompted to configure your replication template upon your first use of AWS Application Migration Service.

The screenshot shows the AWS Application Migration Service console for the 'Replication template' page. At the top, there is a breadcrumb 'Application Migration Service > Replication template'. The main heading is 'Replication template'. Below this, a paragraph explains that source servers inherit replication settings from this template, which can be modified at any time. A light blue information box states: 'Changes made to the templates will only be applied to newly added servers.' On the right side, there are two buttons: 'Reinitialize service permissions' and 'Edit'. The configuration is organized into three sections: 'Replication server configuration', 'Volumes', and 'Security groups'. Each section contains two columns of settings.

Replication server configuration Info	
Subnet subnet-██████████	Replication Server instance type t3.small

Volumes Info	
EBS volume type (for replicating disks over 500 GiB) Faster, General Purpose SSD (gp2)	EBS encryption ARN

Security groups Info	
Always use Application Migration Service security group Yes	Additional security groups sg-██████████ sg-██████████

The configured replication settings can be changed at any time, for individual source servers or for a group of source servers. The changes made will only affect the server or group of servers selected and will not affect the replication settings template. [Learn more about configuring your initial replication template.](#)

To edit the replication settings for your entire account, you will need to edit your Replication template using the following steps.

- Choose **Replication template**, under **Settings** on the left-hand navigation menu.
- This will open the **Replication template** view. Click **Edit** to edit your account-wide replication settings. These settings changes will be applied to each newly added server but will not affect servers that have already been added to AWS Application Migration Service.

To edit the settings for an individual server or group of servers, take the following steps.

- select the box to the left of each server name on the **Source servers** page.

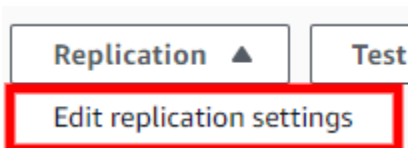
Application Migration Service > Source servers

Source servers (38) Actions ▾ Replication ▾ Test and cutover ▾

Active source servers ▾ < 1 > ⚙️

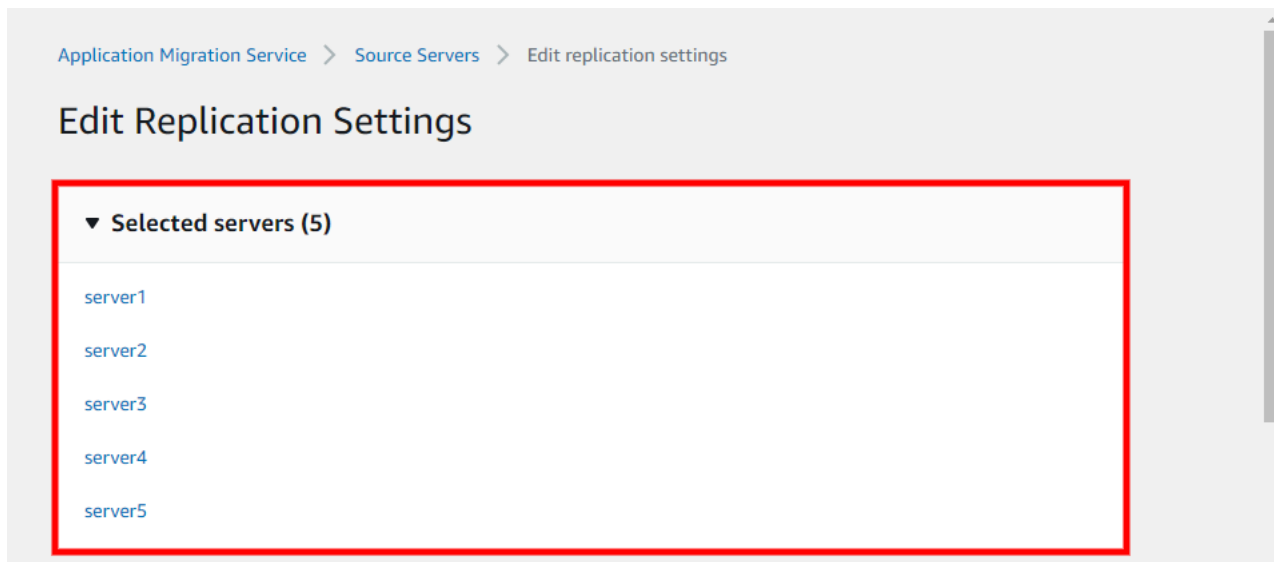
<input type="checkbox"/>	Source server name ▲	Alerts ▾	Replication type ▾	Migration lifecycle ▾	Data replication status	Last snapshot ▾	Next step ▾
<input checked="" type="checkbox"/>	11: not_ready (initiating)	-	Agent based	Not ready	Initiating	-	Wait for initial sync to complete
<input checked="" type="checkbox"/>	12: not_ready (initiating) - had error	-	Agent based	Not ready	Initiating	-	Wait for initial sync to complete
<input checked="" type="checkbox"/>	13/not_ready/initiating	-	Snapshot shipping	Not ready	Initiating	-	Wait for snapshot transfer to complete
<input type="checkbox"/>	14: not_ready (initial_sync)	-	Agent based	Not ready	Initial sync 38% 68 sec left	-	Wait for initial sync to complete

- Open the **Replication** menu and choose **Edit replication settings**.



- You will be redirected to **Edit replication settings**.

The names of the servers for which you are editing the replication settings will appear under the **Selected servers** dropdown.



- You can edit individual replication settings under the **Replication settings** category.

Replication Servers [Info](#)

Staging area subnet [Info](#)

subnet-
vpc-

Replication Server instance type [Info](#)

t3.small

EBS volume type (for replicating disks over 500GiB) [Info](#)

Faster, General Purpose SSD (gp2)

EBS encryption [Info](#)

Default

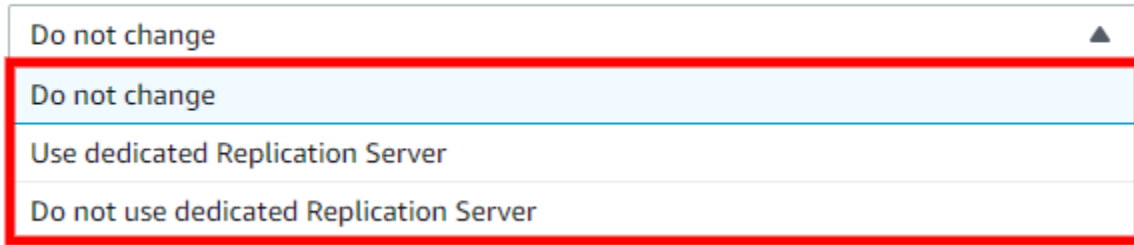
Security groups [Info](#)

Always use Application Migration Service security group

Additional security groups

Choose additional security groups

- If you want to choose different settings for selected servers than those set in the replication template, edit these settings individually. Any setting that has not been changed is labeled with the **Do not change** option.
- To change the settings, choose the preferred option from the drop-down menu under each setting category.

Dedicated instance for Replication Server [Info](#)

The screenshot shows a dropdown menu with the following options:

- Do not change
- Do not change
- Use dedicated Replication Server
- Do not use dedicated Replication Server

- Click **Save replication settings** to save your changes.

The individual replication settings categories are explained in the following sections.

Replication server settings

Replication servers are lightweight Amazon EC2 instances that are used to replicate data between your source servers and AWS. Replication servers are automatically launched and terminated as needed. You can modify the behavior of the replication servers by modifying the settings for a single source server or multiple source servers. Alternatively, you can run AWS Application Migration Service with the default replication server settings.

You can configure a variety of replication server options, including:

- The subnet within which the replication server will be launched
- Replication Server instance type
- Amazon EBS volume types
- Amazon EBS encryption
- Security groups

Once you have finalized your changes, click the orange **Save replication settings** button on the bottom right of the page.

Replication settings Info
Edit

Replication Servers

Subnet
[Redacted]

Replication Server Instance type
m5.xlarge

Use dedicated Replication Server
No

Data routing and throttling

Use private IP for data replication (VPN, DirectConnect or VPC peering)
No

Create public IP
Yes

Replicated disks

[View details under Disks settings](#)

Replication resources tags

Key	Value
abc	abc example

EBS encryption
Default

Default EBS volume type for disks over 500GiB
Use lower cost magnetic disks (st1)

Always use Application Migration Service security group
Yes

Additional security groups
[Redacted]

Throttle network bandwidth
No throttling

Staging area subnet

Choose the **Staging area subnet** that you want to allocate as the staging area subnet for all of your replication servers.

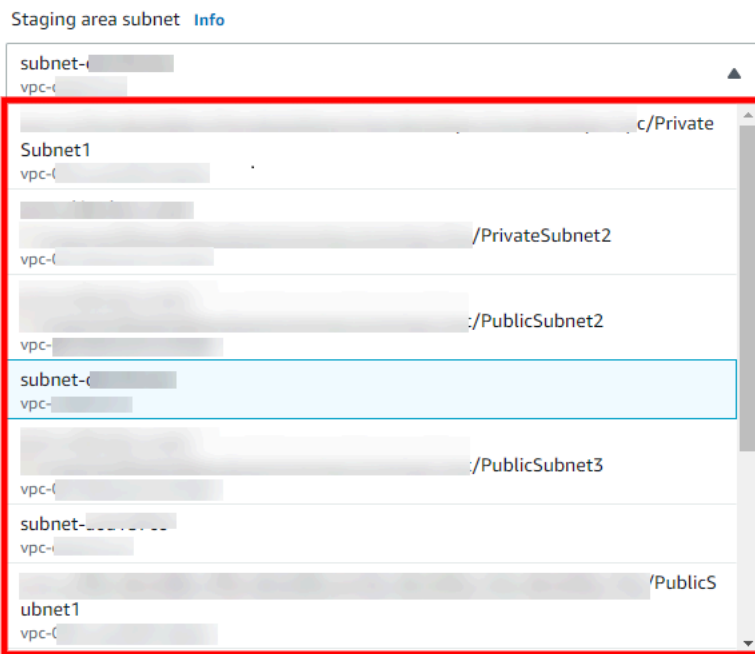
Replication Servers Info

Staging area subnet Info

▼

The best practice is to create a single dedicated, separate subnet for all of your migration waves using your AWS Account. Learn more about creating subnets in [this AWS VPC article](#).

If a default subnet does not exist, select a specific subnet. The drop-down menu contains a list of all subnets that are available in the current AWS Region.

**Note**

Changing the subnet does not significantly interfere with ongoing data replication, although there may be a minor delay of several minutes while the servers are moved from one subnet to another.

Using multiple subnets

The best practice is to use a single staging area subnet for all of your migration waves within a single AWS Account. You may want to use multiple subnets in certain cases, such as the migration of thousands of servers.

Note

Using more than one staging area subnet might result in higher compute consumption as more replication servers will be needed.

Launching replication servers in Availability Zones

If you want your replication servers to be launched in a specific Availability Zone, then select or create a subnet in that specific Availability Zone. Learn more about using Availability Zones in [this Amazon EC2 article](#).

Replication server instance type

Choose the **Replication server instance type**. This will determine the instance type and size that will be used for the launch of each replication server.



The image shows a screenshot of a web interface for selecting a replication server instance type. The label 'Replication Server Instance type' is followed by a blue 'Info' link. Below the label is a dropdown menu with 'm5.xlarge' selected and a downward-pointing arrow on the right. The entire selection area is enclosed in a red rectangular border.

The best practice is to not change the default replication server instance type unless there is a business need for doing so.

By default, AWS Application Migration Service utilizes the t3.small instance type. This is the most cost effective instance type and should work well for most common workloads. You can change the replication server instance type to speed up the initial sync of data from your source servers to AWS. Changing the instance type will likely lead to increased compute costs.

You can change the **Replication server instance** type according to your preferences. The drop-down menu contains all available instance types. Recommended and commonly used instance types are displayed first.

You can search for a specific instance type within the search box.

The replication server instance type can be changed for servers that are replicating too slowly or servers that are constantly busy or experience frequent spikes. These are the most common instance type changes that are made:

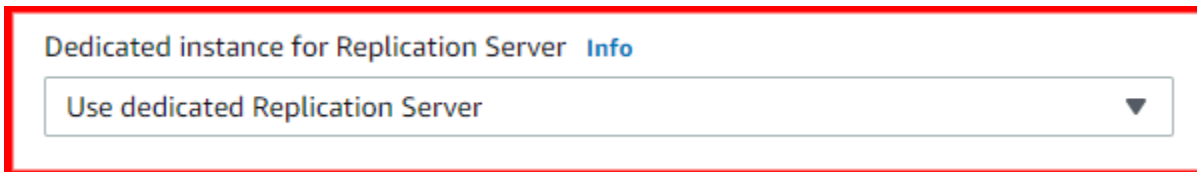
- Servers with less than 26 disks – Change the instance type to m5.large. Increase the instance type to m5.xlarge or higher as needed.
- Servers with more than 26 disks (or servers in AWS Regions that do not support m5 instance types) – Change the instance type to m4.large. Increase to m4.xlarge or higher, as needed.

Note

- Changing the replication server instance type will not affect data replication. Data replication will automatically continue from where it left off, using the new instance type you selected.
- By default, replication servers are automatically assigned a public IP address from Amazon's public IP space.
- Replication Servers are only supported on x86_64 CPU architecture instance types.

Dedicated instance for replication server

Choose whether you would like to use a **Dedicated instance for replication server**.



The screenshot shows a dropdown menu titled "Dedicated instance for Replication Server" with an "Info" link. The selected option is "Use dedicated Replication Server". The entire dropdown is highlighted with a red border.

When an external server is very write-intensive, the replication of data from its disks to a shared Replication Server can interfere with the data replication of other servers. In these cases you should choose the **Use dedicated replication server** option (and also consider changing Replication server instance type).

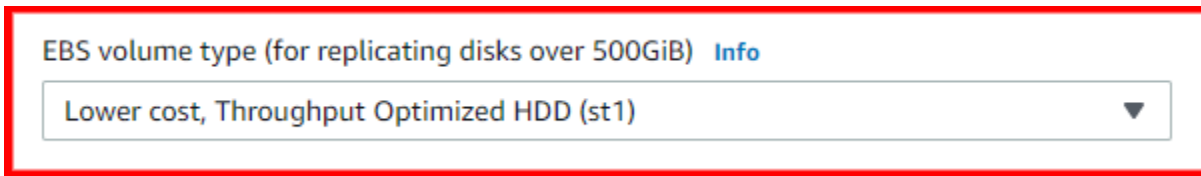
Otherwise, choose the **Do not use dedicated replication server** option.

Note

Using a dedicated replication server may increase the Amazon EC2 cost you incur during replication.

Amazon EBS volume type

Choose the default Amazon **Amazon EBS volume type** to be used by the replication servers for large disks.



Each disk has minimum and maximum sizes and varying performance metrics and pricing. Learn more about Amazon EBS volume types in [this Amazon EBS article](#).

The best practice is to not change the default Amazon EBS volume type, unless there is a business need for doing so.

Note

This option only affects disks over 500 GiB (by default, smaller disks always use Magnetic HDD volumes).

The default **Lower cost, Throughput Optimized HDD (st1)** option utilizes slower, less expensive disks.

You may want to use this option if:

- You want to keep costs low
- Your large disks do not change frequently
- You are not concerned with how long the initial sync process will take

The **Faster, General Purpose SSD (gp3)** option utilizes faster, but more expensive disks.

EBS volume type (for replicating disks over 500GiB) [Info](#)

Faster, General Purpose SSD (gp3) ▼

You may want to use this option if:

- Your source server has disks with a high write rate or if you want faster performance in general
- You want to speed up the initial sync process
- You are willing to pay more for speed

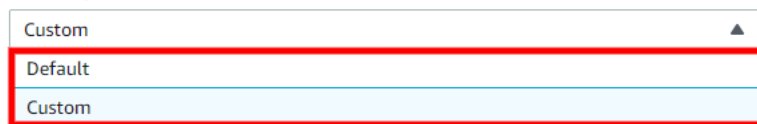
Note

You can customize the Amazon EBS volume type used by each disk within each source server in that source server's settings. [Learn more about changing individual source server volume types.](#)

Amazon EBS encryption

Choose whether to use the default or custom Amazon **EBS encryption**. This option will encrypt your replicated data at rest on the Staging Area Subnet disks and the replicated disks.

- Default – The default Amazon EBS encryption Volume Encryption Key will be used (which can be an EBS-managed key or a CMK).
- Custom – You will need to enter a custom customer-managed key (CMK) in the regular key ID format.

EBS encryption [Info](#)

Custom

Default

Custom

If you select the **Custom** option, the **EBS encryption key** box will appear. Enter the ARN or key ID of a customer-managed CMK from your account or another AWS account. Enter the encryption key (such as a cross-account KMS key) in the regular key ID format (KMS key example: 123abcd-12ab-34cd-56ef-1234567890ab).

To create a new AWS KMS key, click **Create an AWS KMS key**. You will be redirected to the Key Management Service (KMS) Console where you can create a new key to use.

EBS encryption [Info](#)

Custom

EBS encryption key



Choose an AWS KMS key or enter an ARN

[Create an AWS KMS key](#)

Learn more about EBS Volume Encryption in [this Amazon EBS article](#).

⚠ Important

Reversing the encryption option after data replication has started will cause data replication to start from the beginning.

Using an AWS KMS Customer Managed Key (CMK) for encryption

If you decide to use a Customer Managed Key (CMK), or if your default Amazon EBS encryption key is a CMK, you will need to add additional permissions to the key to allow AWS Application Migration Service (AWS MGN) to use it.

To modify the existing key policy using the AWS Management Console *policy view*.

1. Navigate to the AWS Key Management Service (AWS KMS) Console and select the AWS KMS key you plan to use with AWS MGN.
2. Scroll to **Key policy** and click **Switch to policy view**.
3. Click **Edit** and add the following JSON statements to the **Statement** field.

```
{
  "Sid": "Allow AWS Services permission to describe a customer managed key for
encryption purposes",
  "Effect": "Allow",
  "Principal": {
    "AWS": "arn:aws:iam::${ACCOUNT_ID}:root"
  },
  "Action": [
    "kms:DescribeKey"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": [
        "${ACCOUNT_ID}"
      ]
    }
  },
  "Bool": {
    "aws:ViaAWSService": "true"
  }
}
```

```

    },
    {
      "Sid": "Allow AWS MGN permissions to use a customer managed key for EBS
encryption",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::${ACCOUNT_ID}:root"
      },
      "Action": [
        "kms:CreateGrant"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "kms:CallerAccount": [
            "${ACCOUNT_ID}"
          ],
          "kms:GranteePrincipal": [
            "arn:aws:iam::${ACCOUNT_ID}:role/aws-service-role/mgn.amazonaws.com/
AWSServiceRoleForApplicationMigrationService"
          ]
        }
      },
      "ForAllValues:StringEquals": {
        "kms:GrantOperations": [
          "CreateGrant",
          "DescribeKey",
          "Encrypt",
          "Decrypt",
          "GenerateDataKey",
          "GenerateDataKeyWithoutPlaintext"
        ]
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  ],
  {
    "Sid": "Allow EC2 to use this key on behalf of the current AWS Application
Migration Service user, during target launches",
    "Effect": "Allow",
    "Principal": {
      "AWS": [
        "arn:aws:iam::${ACCOUNT_ID}:root",

```



```

    "arn:aws:iam::${ACCOUNT_ID}:role/aws-service-role/mgn.amazonaws.com/
    AWSServiceRoleForApplicationMigrationService"
  ],
  "Action": [
    "kms:ReEncrypt*",
    "kms:GenerateDataKey*"
  ],
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "kms:CallerAccount": [
        "${ACCOUNT_ID}"
      ],
      "kms:ViaService": "ec2.${REGION}.amazonaws.com"
    }
  }
}

```

Important

- Replace `ACCOUNT_ID` with the AWS Account ID you are migrating into.
- Replace `REGION` with the region you are migrating into.
- The last statement can be made stricter by ensuring the principal refers to users who are going to perform [StartTest](#) or [StartCutover](#) API calls

4. Click **Save changes**.

Note

If you are using a Customer Managed Key (CMK) from another account, you need to take an additional step from within that account to allow the service to leverage the CMK. From the account in which you want to stage MGN replication servers, create a grant that delegates the relevant permissions to the appropriate service-linked role. The Grantee Principal element of the grant is the ARN of the appropriate service-linked role. The key-id is the ARN of the key.

The following is an example [create-grant](#) CLI command that gives the service-linked role named **AWSServiceRoleForApplicationMigrationService** in account 111122223333 permissions to use the customer-managed key in account 444455556666.

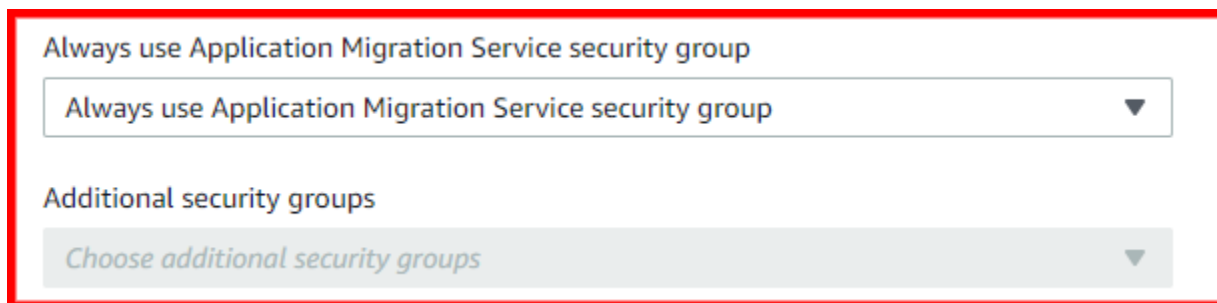
```
aws kms create-grant \  
--region us-west-2 \  
--key-id arn:aws:kms:us-  
west-2:444455556666:key/1a2b3c4d-5e6f-1a2b-3c4d-5e6f1a2b3c4d \  
--grantee-principal arn:aws:iam::111122223333:role/aws-service-role/  
mgn.amazonaws.com/AWSServiceRoleForApplicationMigrationService \  
--operations "Encrypt" "Decrypt" "ReEncryptFrom" "ReEncryptTo" "GenerateDataKey"  
"GenerateDataKeyWithoutPlaintext" "DescribeKey" "CreateGrant"
```

For this command to succeed, the user making the request must have permissions for the `CreateGrant` action.

Always use Application Migration Service security group

Choose whether you would like to **Always use the Application Migration Service security group**.

A security group acts as a virtual firewall, which controls the inbound and outbound traffic of the staging area subnet.



The screenshot shows two dropdown menus. The first dropdown is labeled "Always use Application Migration Service security group" and is currently set to "Always use Application Migration Service security group". The second dropdown is labeled "Additional security groups" and is currently set to "Choose additional security groups". Both dropdowns have a downward arrow on the right side.

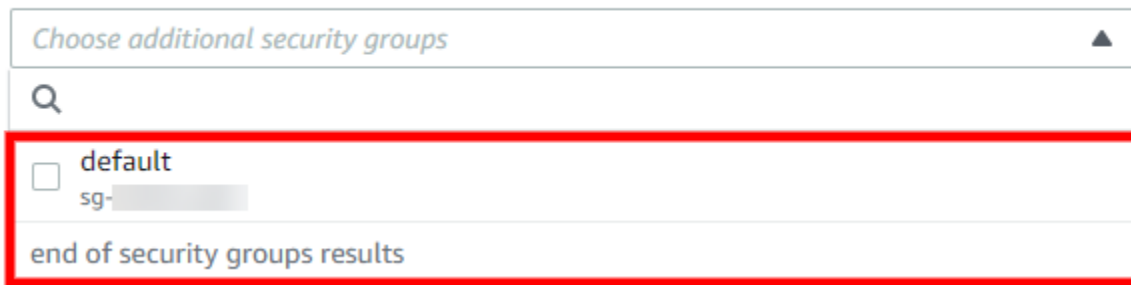
The best practice is to have AWS Application Migration Service (AWS MGN) automatically attach and monitor the default Application Migration Service Security Group. This group opens inbound TCP Port 1500 for receiving the transferred replicated data. When the default Application Migration Service Security Group is activated, AWS MGN will constantly monitor whether the rules within this security group are enforced, in order to maintain uninterrupted data replication. If these rules are altered, AWS MGN will automatically fix the issue.

Select the **Always use Application Migration Service security group** option to allow data to flow from your source servers to the replication servers, and that the replication servers can communicate their state to the AWS Application Migration Service servers.

Otherwise, select the **Do not use Application Migration Service security group option**. Selecting this option is not recommended.

Additional security groups can be chosen from the Additional security groups dropdown. The list of available security groups changes according to the **Staging area subnet** you selected.

Additional security groups



The screenshot shows a dropdown menu titled "Additional security groups". The dropdown is open, displaying a search bar with a magnifying glass icon. Below the search bar, there is a list of security groups. The first item is "default" with a checkbox next to it. Below the list, there is a message "end of security groups results". A red rectangular box highlights the search bar and the "default" option.

You can search for a specific security group within the search box.

You can add security groups via the AWS Console, and they will appear on the security group dropdown list in the AWS Application Migration Service Console. Learn more about AWS security groups in [this VPC article](#).

You can use the default Application Migration Service security group, or you can select another security group. However, take into consideration that any selected security group that is not the Application Migration Service default, will be added to the default group, since the default security group is essential for the operation of AWS MGN.

Data routing and throttling

AWS Application Migration Service allows you to control how data is routed from your source servers to the replication servers on AWS through the **Data routing and throttling** settings.

Data routing and throttling [Info](#)

Use private IP for data replication (VPN, DirectConnect, VPC peering)

Use private IP ▼

Create public IP

Create public IP ▼

Network bandwidth throttling

Do not throttle bandwidth ▼

By default, data is sent from the source servers to the replication servers over the public internet, using the public IP that was automatically assigned to the replication servers. Transferred data is always encrypted in transit.

Note

The **Data routing and throttling** view differs slightly between the replication template view and the individual source server replication settings view, but the instructions apply to both views.

Use private IP for data replication

Choose the **Use private IP** option if you want to route the replicated data from your source servers to the staging area subnet through a private network with a VPN, AWS Direct Connect, VPC peering, or another type of existing private connection.

Choose **Do not use private IP** if you do not want to route the replicated data through a private network.

Use private IP for data replication (VPN, DirectConnect, VPC peering)

Use private IP ▲

Do not use private IP

Use private IP

⚠ Important

Data replication will not work unless you have already set up the VPN, AWS Direct Connect, or VPC peering in the AWS Console.

ℹ Note

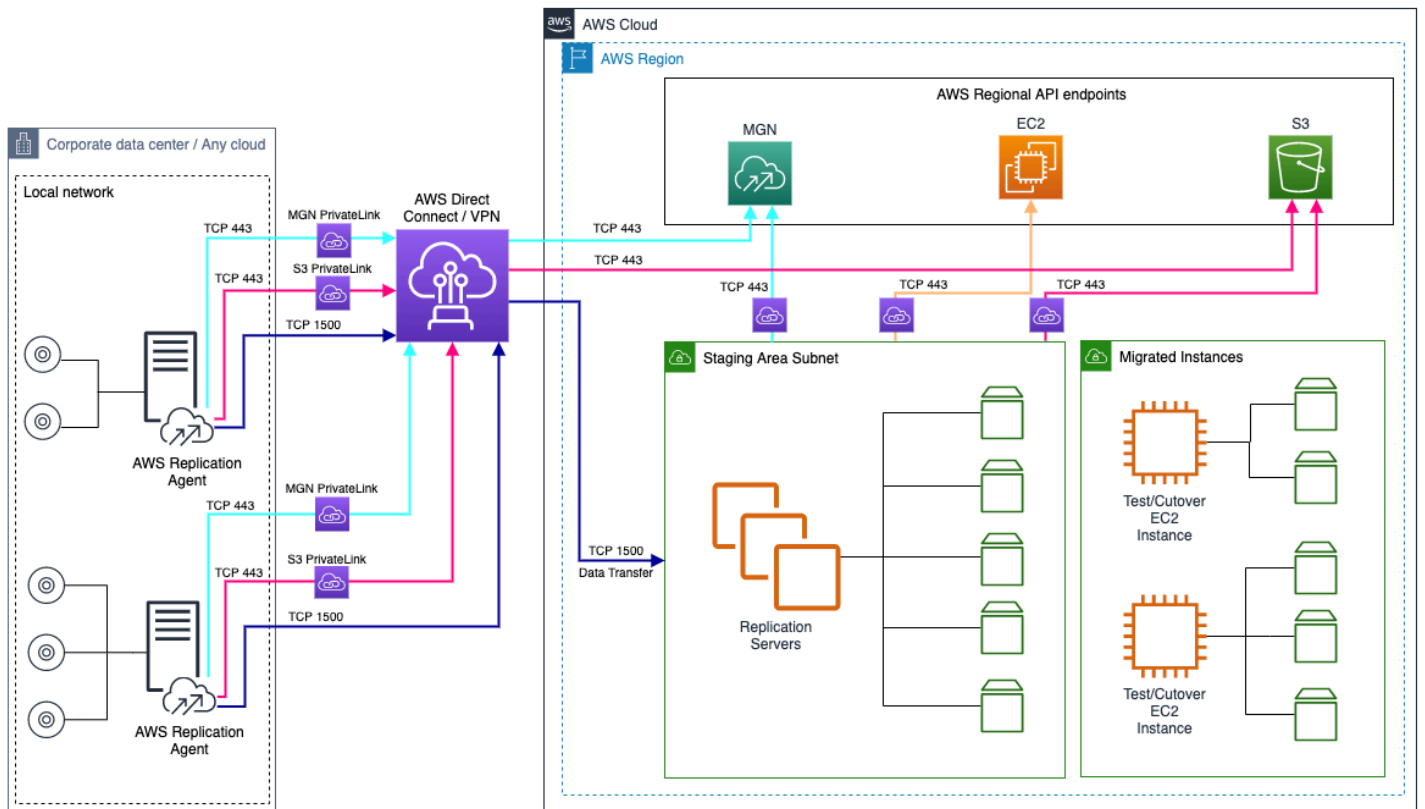
- If you selected the Default subnet, it is highly unlikely that the private IP is used for that subnet. Ensure that Private IP (VPN, AWS Direct Connect, or VPC peering) is used for your chosen subnet if you wish to use this option.
- You can safely switch between a private connection and a public connection for individual server settings choosing the **Use private IP** or **Do not use private IP** option, even after data replication has begun. This switch will only cause a short pause in replication, and will not have any long-term effect on the replication.
- Choosing the **Use private IP** option will not create a new private connection.

You should use this option if you want to:

- Allocate a dedicated bandwidth for replication
- Use another level of encryption
- Add another layer of security by transferring the replicated data from one private IP address (source) to another private IP address (on AWS)

Network architecture diagram – private IP

The following diagram illustrates the high-level interaction between the different replication system components when using private IP or VPC endpoint.



Create public IP

When the **Use private IP** option is chosen, you will have the option to create a public IP. Public IPs are used by default. Choose **Create public IP** if you want to create a public IP. Choose **Do not create a public IP** if you do not want to create a public IP.

Use private IP for data replication (VPN, DirectConnect, VPC peering)

Use private IP ▼

Create public IP ▲

Create public IP

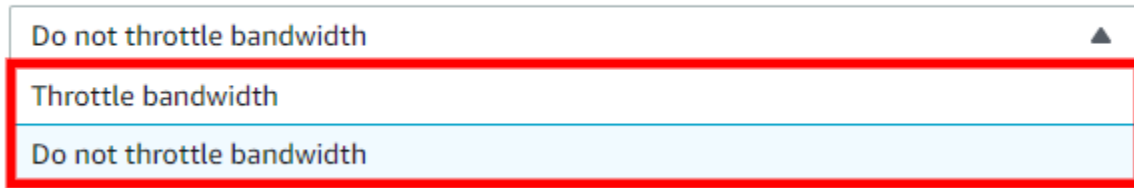
Do not create public IP

Throttle bandwidth

You can control the amount of network bandwidth used for data replication per server. By default, AWS Application Migration Service will use all available network bandwidth utilizing five concurrent connections.

Choose **Throttle bandwidth** if you want to control the transfer rate of data sent from your source servers to the Replication Servers over TCP Port 1500. Otherwise, choose **Do not throttle bandwidth**.

Network bandwidth throttling



If you chose to throttle bandwidth, the **Throttle network bandwidth** (per server, in Mbps) box will appear. Enter your desired bandwidth in Mbps.

Replication resources tags

Add custom **Replication resources tags** to resources created by AWS Application Migration Service in your AWS account.

These are resources required to facilitate data replication, testing and cutover. Each tag consists of a key and an optional value. You can add a custom tag to all of the AWS resources that are created on your AWS account during the normal operation of AWS Application Migration Service.

To add a new tag, take the following steps:

1. Click **Add new tag**.
2. Enter a **Custom tag key** and an optional tag value.

Note

Application Migration Service already adds tags to every resource it creates, including service tags and user tags.

These resources include:

- Amazon EC2 instances
- Amazon EC2 launch templates

- Amazon EBS volumes
- Snapshots
- Security groups (optional)

Learn more about AWS Tags in [this Amazon EC2 article](#).

Launch template

The **Launch template** allows you to control the way AWS Application Migration Service launches instances in AWS. The default configuration defined in the template will be automatically applied to every newly added server.

You can change the settings for existing and newly added servers individually within the source server details view, **Launch settings** tab. Changes made to server launch settings will only affect the selected server and will not affect the launch template.

To edit the launch template for your entire account, you will need to edit your Launch template. Choose **Launch template** from the left-hand navigation menu.

This will open the account template view. Click **Edit** to update your account-level launch template.

Launch template

Every source server added to this service has launch settings that control actions performed after the server is launched in AWS. These settings are created automatically based on this default launch template, and can be modified for any source server. The default can be modified at any time.

🔗 Changes made to the templates will only be applied to newly added servers.

Edit

General launch settings Info

Configure the default settings that will be used when launching target servers.

<p>Instance type right sizing On</p> <p>Copy private IP No</p> <p>Transfer server tags No</p>	<p>Start instance upon launch Yes</p> <p>Operating system licensing License-Included</p>
---	--

Default EC2 Launch Template Info

Configure the default settings that will be applied to the EC2 launch template of every target server.

<p>Template ID lt-051dd205c4ca15f61</p> <p>Instance type -</p> <p>Security groups</p>	<p>Default target subnet -</p> <p>EBS volume type General Purpose SSD (gp3)</p>
---	---

Note

Ensure the Account Level EC2 Launch Template is not deleted. If it is, edit and save the launch template page to create a new Account Level Template.

General launch settings

In the **General launch settings** section, you can define the following:

- **Instance type right sizing**
- **Start instance upon launch**
- **Copy private IP**
- **Transfer server tags**
- **Operating system licensing**
- **Boot mode**

Instance right sizing – The Instance type right-sizing feature allows AWS Application Migration Service to launch a test or cutover instance type that best matches the hardware configuration of the source server. If you select this option, AWS Application Migration Service will launch a test or cutover AWS instance type that best matches the OS, CPU, and RAM of your source server. Please note that the AWS instance type selected by Application Migration Service when this option is selected will overwrite the instance type defined in your EC2 launch template.

Start instance upon launch – Select this option whether you want to start your test and cutover instances automatically upon launch or whether you want to launch them in a stopped state.

Copy private IP – Select this option if you want AWS Application Migration Service to ensure that the private IP used by the test or cutover instance matches the private IP used by the source server. AWS Application Migration Service monitors the source server on an hourly basis to identify the Private IP and uses the private IP of the primary network interface if this option is selected. Make sure that the IP range of the subnet you set in the EC2 Launch Template includes the Private IP address for this feature to work.

Transfer server tags – Select this option if you want AWS Application Migration Service to transfer any user-configured custom tags from your source servers onto your test or cutover instance. If you

select this option, server tags will be transferred. These tags are attached to all source servers, all launched test and cutover instances, and all of the ephemeral resources that are created on your AWS Account during the normal operation of AWS Application Migration Service such as snapshots, EBS volumes, replication and conversion servers, and security groups.

Operating system licensing – Select this option if you want to Bring Your Own Licenses (BYOL) from the source server into the test or cutover instance. Select “Bring your own license (**BYOL**)” option if you are migrating a Linux server as all Linux licenses are BYOL by default. Any RHEL, SUSE or Debian licenses will be transferred in their current form to the migrated instance.

For Windows servers, choose the “Bring your own license (**BYOL**)” option if you want to BYOL your Windows licenses. This will set up a Dedicated Host. All the licenses from the source Windows source server will be automatically transferred to the test or cutover instance. Please note that if you use BYOL licensing for Windows, you have to change the **Placement.tenancy** type in the EC2 launch template to **Host**. Otherwise, instance launch will fail.

Boot mode – When a computer boots, the first software that it runs is responsible for initializing the platform and providing an interface for the operating system to perform platform-specific operations. In Amazon EC2, two variants of the boot mode software are supported: Unified Extensible Firmware Interface (UEFI) and Legacy BIOS. The boot mode allows AWS Application Migration Service to launch a test or cutover instance type that best matches the configuration of the source server. You can select between keep the source boot mode or change it to BIOS/UEFI modes.

Default EC2 launch template

In the **Default EC2 launch template** section, you can define the following options:

- **Default target subnet** – Choose the target subnet for the test and cutover machines. All the test and cutover machines will be launched in this target subnet.
- **Target security groups** – Choose a number of security groups for the test and cutover machines. Upon the target launch, the selected security groups will be attached to the EC2 instances.
- **Default instance type** – Choose a default instance type for the test and cutover machines. The instance type chosen in this template will be propagated to source server’s launch template and will be used to launch the target instance.
- **EBS volume type** – Choose an EBS volume type for the test and cutover machines. The EBS volume type can be chosen from io1, io2, gp3, st1, and sc1 volume types.

If this setting is not chosen, the default instance type selected in the launch template will be GP3 with maximum IOPS (16000). If a volume type is selected in this option, and if the disk size does not match the limits of the volume type, the default volume type GP3 will be used with maximum IOPS.

Note

Note: if you manually delete the default launch template, AWS Application Migration Service will generate a new default launch template. Any changes previously made to the default template will be discarded, including subnet and security groups. You can reconfigure the same changes on the new default launch template, and they will be applied to servers added to the console, after you make the changes.

MAP program tagging

Use this setting to determine whether to apply MAP program tags to your launched instances.

Check the box to the left of **Add MAP tag to Launched Instances** option, if you want AWS MGN to automatically tag your launched instances with the tag key and value combination required for MAP program.

If you checked the box, you must specify the MAP tag value that will be used in your MAP tagging. AWS MGN will automatically tag your migrated resources with the key: "map-migrated", and the value of the tag, that you provided. For more details about the tag value that should be used here, please refer to the MAP tagging guide provided in your MAP term.

[Learn more about the AWS Migration Acceleration Program \(MAP\).](#)

Post-launch settings

Post-launch settings allow you to control and automate actions performed after the server has been launched in AWS. These settings are created automatically based on the **Post-launch template**.

To access the template, click **Post-launch template** on the left-hand navigation menu.

Application Migration Service > Post-launch template

Post-launch template

This feature allows you to configure and automate actions performed after the server is launched in AWS. The template controls the default post-launch settings of every newly added source server. You can modify the template or individual server settings at any time.

Changes made to the templates will only be applied to newly added servers.

Post-launch actions settings [Info](#) [Edit](#)

Activate post-launch actions	Deployment
No	Test and cutover instances

The settings defined in the template will be applied to every newly added server. You can change the settings for existing and newly added servers individually within the server details view.

To use the post-launch settings feature, you must first activate it.

The **Post-launch template** allows you to control various post-launch actions, including:

- Deployment of test and cutover instances
- Disaster recovery configuration (installing the AWS Replication Agent for AWS DRS and configuring the target disaster recovery AWS Region)
- Operating system conversion on the target machine
- License and subscription changes on the target machine

Activating post-launch settings

In order to be able to use the post-launch template, you must first activate the post-launch actions. This will allow AWS MGN to:

- Install the Systems Manager Agent (SSM Agent) on your servers
- Run the post-launch actions

Important

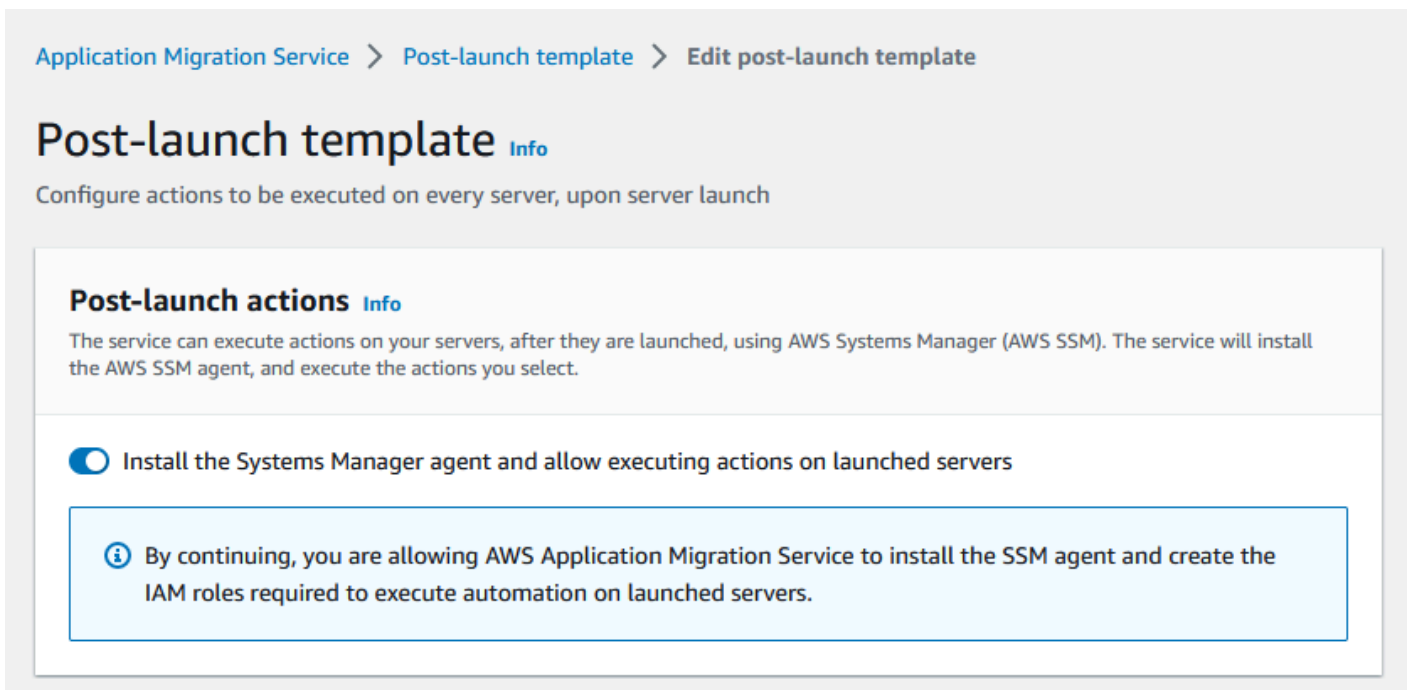
This feature is activated and deactivated at the account level. You must activate the feature to see and activate the individual actions.

To activate the post-launch actions:

1. Navigate to **Settings > Post-launch settings template**.
2. Click **Edit**.



3. When the **Post-launch actions** dialog appears, toggle the **Install System Manager agent and allow executing actions on launched servers** option.



4. Click **Save template** at the bottom of the page.
5. You will be returned to the **Settings > Post-launch template** view, and the post-launch actions will now be shown. Click **Edit** to change the settings.

Post-launch template

This feature allows you to configure and automate actions performed after the server is launched in AWS. The template controls the default post-launch settings of every newly added source server. You can modify the template or individual server settings at any time.

Changes made to the templates will only be applied to newly added servers.

▼ **Post-launch actions settings** [info](#) Edit

Activate post-launch actions
Yes

Deployment
Cutover instances only

Filter by

▼ **Activation status**

Active

Not active

▼ **Platform**

Linux

Windows

▼ **Creator**

Me

AWS

3rd party

▼ **Categories**

Actions (12) Card view ▼ Edit Delete Create action

Q Find actions < 1 > ⌂

Action Name	Powered by	Status	Platform	Order	Description
SSM agent	AWS SSM	Active	Windows and Linux	1	Install SSM agent
Replace SUSE subscription	AWS MGN	Not active	Linux	20	This action will convert a SUSE Linux subscription to an AWS provided... More
CentOS to Rocky	AWS MGN	Not active	Linux	30	This action will convert the operating system of instances running... More
Windows MS-SQL license conversion	AWS MGN	Not active	Windows	40	Convert windows MS-SQL BYOL to AWS License.

Editing the post-launch settings template

AWS MGN supports post-launch modernization actions, giving you the opportunity to move and improve. The service provides a variety of out-of-the-box actions that you can execute on your EC2 launch instances, as well as allows you to create your own actions.

The actions described in the following sections can be edited within the post-launch template. Once you have edited your settings, choose **Save template**.

Activating and deactivating post-launch actions

This setting controls whether post-launch actions are activated or deactivated. You must leave the **Install System Manager agent and allow executing actions on launched servers** option toggled in order for post-launch actions to work. Untoggling the option will disallow AWS MGN to install the SSM Agent on your servers and post-launch actions will no longer be executed on them.

Application Migration Service > Post-launch template > Edit post-launch template

Post-launch template Info

Configure actions to be executed on every server, upon server launch

Post-launch actions Info

The service can execute actions on your servers, after they are launched, using AWS Systems Manager (AWS SSM). The service will install the AWS SSM agent, and execute the actions you select.

Install the Systems Manager agent and allow executing actions on launched servers

i By continuing, you are allowing AWS Application Migration Service to install the SSM agent and create the IAM roles required to execute automation on launched servers.

Deploying post-launch actions

Use this setting to choose whether to execute the post-launch actions on your cutover instances, on your test instances, or on both cutover and test instances.

Deployment Info

Choose whether to execute the post-launch actions on your cutover instances only, or on both your cutover and test instances.

Test and cutover instances
(recommended)

All post-launch actions will be executed on test and cutover instances.

Cutover instances only

All post-launch actions will only be executed on the cutover instances.

Test instances only

All post-launch actions will only be executed on the test instances.

i Note

Only trusted, authorized users should have access to parameter store. For enhanced security, ensure that users who do not have permissions to execute SSM documents/commands, do not have access to parameter store. [Learn more about restricting access to Systems Manager parameters.](#)

Encrypt post-launch action parameters

The post-launch action parameters are stored in AWS Systems Manager (SSM) [Parameter Store](#) . For enhanced security, ensure that users who do not have permissions to execute SSM documents, do not have access to the Parameter Store. For an additional layer of security you can select to encrypt the action parameters using AWS Key Management Service (KMS) encryption.

AWS SSM encrypts the parameter value of SecureString parameters type using AWS KMS with an AWS managed key or with the default KMS key provided by AWS. You can specify different keys for each parameter, or use the same key for multiple parameters.

Post-launch actions table

The post-launch actions table includes both predefined actions and custom actions that will be executed on your new EC2 instances.

- Predefined post-launch actions are provided out of the box. They are prepopulated with the necessary values and only need to be activated or deactivated. These actions are based on public SSM documents that cannot be changed and have certain unchangeable parameters such as the platform name and order.
- Custom post-launch actions are based on SSM documents that you create and upload to your account.

Use the **Filter by** options on the left-hand side to filter the available actions according to your preferences.

Click the settings icon in the right-hand corner of the screen to alternate between card and list view, according to your preferences.

▼ **Post-launch actions settings** Info Edit

Activate post-launch actions: Yes Deployment: Cutover instances only

Filter by

- ▼ Activation status
 - Active
 - Not active
- ▼ Platform
 - Linux
 - Windows
- ▼ Creator
 - Me
 - AWS
 - 3rd party
- ▼ Categories
 - Backup
 - Configuration
 - Disaster recovery
 - License & subscription
 - Observability
 - Operating system
 - Validation
 - Other

Actions (12) Card view Edit Delete Create action

<p>SSM agent Powered by AWS SSM</p> <p><input checked="" type="radio"/> Active</p> <p>Platform: Windows and Linux Order: 1</p> <p>Description: Install SSM agent</p>	<p>Replace SUSE subscription Powered by AWS MGN</p> <p><input type="radio"/> Not active</p> <p>Platform: Linux Order: 20</p> <p>Description: This action will convert a SUSE Linux subscription to an AWS provided... More</p>	<p>CentOS to Rocky Powered by AWS MGN</p> <p><input type="radio"/> Not active</p> <p>Platform: Linux Order: 30</p> <p>Description: This action will convert the operating system of instances running... More</p>	<p>Windows MS-SQL license conversion Powered by AWS MGN</p> <p><input type="radio"/> Not active</p> <p>Platform: Windows Order: 40</p> <p>Description: Convert windows MS-SQL BYOL to AWS License.</p>	<p>CloudWatch agent installation Powered by AWS CloudWatch</p> <p><input type="radio"/> Not active</p> <p>Platform: Windows and Linux Order: 101</p> <p>Description: Install and configure CloudWatch agent.</p>
<p>Join domain Powered by AWS Directory Service</p> <p><input type="radio"/> Not active</p> <p>Platform: Windows and Linux Order: 330</p> <p>Description: Join your instances to an AWS Directory Service domain.</p>	<p>Volume integrity validation Powered by AWS MGN</p> <p><input type="radio"/> Not active</p> <p>Platform: Windows and Linux Order: 401</p> <p>Description: Ensure that volumes on launched instances are identical to the source... More</p>	<p>EC2 connectivity check Powered by AWS MGN</p> <p><input type="radio"/> Not active</p> <p>Platform: Windows and Linux Order: 405</p> <p>Description: Check network connectivity to a predefined list of ports and hosts.</p>	<p>Process status validation Powered by AWS MGN</p> <p><input type="radio"/> Not active</p> <p>Platform: Windows and Linux Order: 410</p> <p>Description: Verify that major processes are in a running state following instance... More</p>	<p>DR after migration Powered by AWS MGN</p> <p><input type="radio"/> Not active</p> <p>Platform: Windows and Linux Order: 805</p> <p>Description: This action will install the AWS Elastic Disaster Recovery (DRS)... More</p>

Predefined post-launch actions

AWS Application Migration Service allows you to execute various predefined post-launch actions on your EC2 launch instance. Use these out-of-the-box actions to modernize your servers while you're migrating: Change existing license, upgrade your operating system, configure disaster recovery, and more.

Choose from a variety of predefined post-launch actions

- [Install the SSM agent](#)
- [Configure AWS Elastic Disaster Recovery \(AWS DRS\)](#)
- [Convert operating systems](#)
- [Replace SUSE subscription](#)
- [Conduct EC2 connectivity checks](#)
- [Validate volume integrity](#)
- [Verify process status](#)
- [Convert MS-SQL license](#)
- [Install a CloudWatch Agent](#)
- [Upgrade Windows](#)
- [Create AMI from instance](#)

- [Join Directory Service domain](#)
- [Configure Time Sync](#)
- [Validate disk space](#)
- [Verify HTTP/HTTPS response](#)
- [Enable Amazon Inspector](#)
- [Verify Tags](#)
- [Auto Scaling group setting](#)
- [Enable Refactor Spaces](#)
- [App2Container for Replatforming](#)
- [Dynatrace](#)

Install the SSM agent

The AWS Systems Manager (AWS SSM) allows AWS Application Migration Service to execute modernization actions on your servers after they are launched.

When you activate the post-launch actions, AWS Application Migration Service will install the **AWS SSM agent** and create the required IAM roles.

The AWS SSM agent must be installed for any other post-launch action to run. Therefore, this is the only post-launch action that is activated by default and cannot be deactivated.

[Learn more about SSM.](#)

Configure AWS Elastic Disaster Recovery (AWS DRS)

Note

This feature is supported on operating systems that are supported by AWS Elastic Disaster Recovery (AWS DRS). [See the AWS DRS documentation.](#)

This action is not supported in MGN GovCloud regions (US-East, US-West).

Use the **DR after migration** feature to configure disaster recovery using AWS Elastic Disaster Recovery.

This action will install the AWS Elastic Disaster Recovery (AWS DRS) Replication Agent on your Amazon EC2 instance.

You must select the target disaster recovery region, which is the AWS Region in which the Recovery instances will be deployed. AWS Elastic Disaster Recovery must be available in the selected Region and initiated in your account. You must initialize AWS DRS for this action to work.

Important

Ensure that you review the costs associated with AWS Elastic Disaster Recovery in the [service pricing documentation](#).

[Learn more about DRS AWS Regions.](#)

[Learn more about initializing AWS DRS.](#)

Convert operating systems

Note

This feature is supported on CentOS version 8.x.

Use the **CentOS to Rocky** feature to perform changes to the target machine operating system. It allows you to convert any of your source servers that are running CentOS to [Rocky Linux](#).

Replace SUSE subscription

Note

- This feature is supported on SUSE Linux versions 12 SP 1 and later.
- This action is not supported on SLES4SAP servers.

Use the **Replace SUSE subscription** feature to choose whether you want to change the SUSE Linux subscription of any source server that runs SUSE to an AWS-provided SUSE subscription.

An AWS-provided SUSE subscription allows AWS to manage your licenses, including renewal handling, saving you time and simplifying your billing and license management processes

Conduct EC2 connectivity checks

Use the **EC2 connectivity check** feature to conduct network connectivity checks to a predefined list of ports and hosts.

Note

Up to 5 Port:IP couples can be checked in a single action.

Validate volume integrity

Use the **Volume integrity validation** feature to ensure that EBS volumes on the launched instance are:

- The same size as the source (rounded up)
- Properly mounted on the Amazon EC2 instance
- Accessible

This feature allows you to conduct the required validations automatically and saves the time of manual validations.

Note

Up to 50 volumes can be checked in a single action.

Verify process status

Use the **Process status validation** feature to ensure that processes are in running state following instance launch. You will need to provide a list of processes that you want to verify, and define how long the service should wait before testing begins.

To check a specific process that should run multiple times, include it several times in the list.

Convert MS-SQL license

Use the **Windows MS-SQL license conversion** feature to easily convert Windows MS-SQL BYOL to an AWS license.

AWS MGN will do the following:

- Check the SQL edition (Enterprise, Standard, or Web) as part of the launch process
- Use the right AMI with the right billing code to launch from

The SSM document will run and verify that the right billing code is used post launch.

The action uses the following APIs:

- [DescribeImages](#)
- [DescribeInstances](#)

To allow the SSM document to run these APIs, you will need to have the required permissions or have access to a role with those permissions and then provide the role's ARN as an input parameter to the SSM automation document.

Install a CloudWatch Agent

Use the **CloudWatch agent installation** feature to install and configure the CloudWatch Agent and Application Insights.

You will need the following policy to run this post-launch action (in addition to the [full access policy](#)):

- AWSApplicationMigrationSSMAccess (or any other user-defined policy that allows that specific document to run)

The launched instance will require the following policies:

- CloudWatchAgentServerPolicy – The permissions required to use AmazonCloudWatchAgent on servers
- AmazonSSMManagedInstanceCore – The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality

To ensure that the launch instance has the right policies, create a role that has the required permissions as per the policies above or has access to a role with those permissions.

- Go to **Launch settings > EC2 launch template > Modify > Advance > IAM instance profile**.

- Use an existing profile or create a new one using the **Create new IAM profile** link.

Note

- You must attach both policies to the template for the CloudWatch agent to operate. Without the CloudWatchAgentServerPolicy, the action will still be marked as successful but the CloudWatch Agent will not be active.
- Configuring the Application Insights is optional. You can choose to skip the Application Insights agent configuration and only install the CloudWatch agent. To do so, simply provide the required parameterStoreName parameter and leave the other parameters empty.

[Learn more about the CloudWatch Agent.](#)

Upgrade Windows

Use the **Windows upgrade** feature to easily upgrade your migrated server to Windows Server 2012 R2, 2016, 2019, or 2022 ([see the full list of available OS versions](#)).

You will need the following policy to run this post-launch action (in addition to the [full access policy](#)).

- AWSApplicationMigrationSSMAccess (or any other user-defined policy that allows that specific document to run)

To allow the SSM document to run these APIs, you will need to have the required permissions (including [CreateImages](#), [RunInstances](#), [DescribeInstances](#), and more) or have access to a role with those permissions and then provide the role's ARN as an input parameter to the SSM automation document.

[Learn more about the different permissions required to perform the upgrade.](#)

The SSM document will:

- Create an Amazon Machine Image (AMI) from the instance using the [CreateImage](#) API.
- Use the AMI to create a new instance and then upgrade that instance.

- Create an AMI from the upgraded instance and terminate the upgraded instance.

Note

- This operation may run for several hours.
- All other post-launch actions will run on the instance launched by MGN and not on the upgraded instance.

[Learn more about upgrading Windows.](#)

Create AMI from instance

Use the **Create AMI from Instance** feature to create a new Amazon Machine Image (AMI) from your AWS MGN launched instance.

You will need the following policy to run this post-launch action (in addition to the [full access policy](#)):

- `AWSApplicationMigrationSSMAccess` (or any other user-defined policy that allows that specific document to run)

Attach the following permissions to your instance:

The action uses the following APIs:

- [CreateImages](#)
- [DescribeImages](#)

To allow the SSM document to run these APIs, you will need to have the required permissions or have access to a role with those permissions and then provide the role's ARN as an input parameter to the SSM automation document.

[Learn more about creating AMI from instance.](#)

Join Directory Service domain

Use this **Join domain** feature to simplify the AWS Join Domain process. If you activate this action, your instance will be managed by the AWS Cloud Directory (instead of on-premises).

You will need the following policy to run this post-launch action (in addition to the [full access policy](#)):

- [AWSApplicationMigrationSSMAccess](#) (or any other user-defined policy that allows that specific document to run)

The launched instance will require the following policies:

- AmazonSSMManagedInstanceCore – The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality.
- AmazonSSMDirectoryServiceAccess – This policy allows the SSM Agent to access Directory Service on behalf of the customer for domain-join the managed instance.

To ensure that the launched instance has the right policies, create a role that has the required permissions as per the policies above or has access to a role with those permissions.

- Go to **Launch settings > EC2 launch template > Modify > Advance > IAM instance profile**.
- Use an existing profile or create a new one using the **Create new IAM profile** link.

Configure Time Sync

Use the **Time Sync** feature to set the time for your Linux instance using ATSS.

[Learn more about Amazon Time Sync.](#)

Validate disk space

Use the **Disk space validation** feature to obtain visibility into the disc space that you have at your disposal, as well as logs with actionable insights.

Verify HTTP/HTTPS response

Use the **Verify HTTP/HTTPS response** feature to conduct HTTP/HTTPS connectivity checks to a predefined list of URLs. The feature will verify that HTTP/HTTPS requests (for example, https://localhost) receive the correct response.

Enable Amazon Inspector

The **Enable Inspector** feature allows you to run security scans on your EC2 resources. The Amazon Inspector service will be enabled at the account level.

Note

Amazon Inspector is a paid AWS service. For additional information, [refer to the full Inspector pricing documentation](#).

This action uses the following APIs:

- [Enable](#)
- [BatchGetAccountStatus](#)
- [CreateServiceLinkedRole](#)

To allow the SSM document to run these APIs, you will need to have the required permissions or have access to a role with those permissions and then provide the role's ARN as an input parameter to the SSM automation document.

Verify Tags

Use the **Verify tags** feature to validate that tags which have been defined in the launch template and on the source server are copied to the migrated server.

Auto Scaling group setting

Use the **Auto Scaling group setting** when you would like to create an Auto Scaling group for a migrated stateless web application.

Enable Refactor Spaces

Use this action to create an AWS Migration Hub Refactor Spaces environment. Refactor Spaces helps accelerate application refactoring by automating the creation of refactor environments in AWS. A Refactor Spaces environment includes the AWS infrastructure, multi-account networking, and routing needed to support the iterative transformation of applications to microservices.

[Learn more about Refactor Spaces.](#)

This action is available in all [Regions](#) where Refactor Spaces is available.

App2Container for Replatforming

Use this action to activate application Replatforming using the [AWS App2Container service](#). This action provides automation for discovering, analyzing, and containerizing all [supported](#)

[applications](#) discovered on the launched EC2 instance. The action also takes care of App2container prerequisites settings, installation, and initialization, so you can focus on the application containerization and deployment.

This action is not available in GovCloud regions.

[Learn more about the App2Container for Replatforming action.](#)

Dynatrace

Note

This action is provided by a third party vendor, and is not available in the GovCloud Regions.

This action installs Dynatrace OneAgent on your launched instance.

To configure this action, you will need to have an existing Dynatrace account and configure the required additionalArguments for your particular usage.

[Learn more about Dynatrace](#)

Custom post-launch actions

AWS Application Migration Service (AWS MGN) allows you to execute any SSM document that you like – public SSM document or ones you created and uploaded to your account.

You can configure a custom action to execute any SSM document that is available in your account.

Create action

To add a new customer action, go to the **Post-launch actions settings** and click **Create action**.

The page includes the following parameters:

- **Action name** – The name of the action in AWS MGN, which should be intuitive and meaningful to your migration users.
- **Activate this action** – Use this checkbox to activate or deactivate the custom action.
- **This action must be completed successfully before finalizing cutover** – This checkbox will dictate whether or not the script will prevent the cutover.

- **System Manager document name** – Select any Systems Manager document that is available for the specific account.
- **View in Systems Manager** – Click to open **System Managers** and view additional information about the document.
- **Description** – Add a description or keep the default.
- **Document version** – Select which SSM document version to run. AWS MGN can run a default version, the latest version, or a specific version, according to your preferences.
- **Category** – Select from various available categories including disaster recovery, security, validation, and more.
- **Order** – Specify the order in which the actions will be executed. The lower the number, the earlier the action will be executed. 1–1,000 are reserved for predefined actions and 1,001–10,000 for custom actions. The numbers must be unique but don't need to be consecutive.
- **Operating system** – Select the source server's operating systems for which the custom action can be configured for. Note that if you associate a script with the wrong operating system, it will be skipped.
- **Creator** – Who created the action. For custom actions, the default is always **Me**.

The **Action parameters** change according to the specific SSM document that is selected.

Note that for the instance ID parameter, you can choose to use the launch instance ID, in which case, AWS MGN will dynamically populate the value.

Note

Only trusted, authorized users should have access to the parameter store. For enhanced security, ensure that users who do not have permissions to execute SSM documents / commands, do not have access to parameter store. [Learn more about restricting access to Systems Manager parameters.](#) Action parameters are stored in the SSM parameter store as regular strings. Changing parameters in the SSM Parameter store may impact the post launch action execution on target instances. We recommend you consider security implications, when choosing to use parameters that contain scripts or sensitive information, such as API keys and database passwords.

Add action [Info](#)

You can associate any Systems Manager document with a post-launch action

Action settings [Info](#)

Action name

The name must be unique. Min: 1 character, Max: 256 characters.

Activate this action

Actions that are active will be executed on the launched instance, after it is launched.

This action must be completed successfully before finalizing cutover.

Systems Manager document name

Select any Systems Manager document that is available for this account.

Description

Specify the action description. Up to 70 characters will be displayed on the card.

Document version

Select the document version to use.

Category

Select the action category which is available for this account.

Order

Specify the order in which the actions will be executed (range 1,001-10,000).

Operating systems

Select the source server's operating systems for which the action can be configured for.

Creator

Action creator.

Cancel

Add action

Edit each setting as required and then click **Add action**.

Edit action

Use this page to edit the parameters detailed in the **Create action** section.

Edit each setting as required and then click **Save action**.

Application Migration Service > Post-launch template > Edit action

Edit action [Info](#)

You can associate any Systems Manager document with a post-launch action


Action settings [Info](#)

Action name
The name must be unique. Min: 1 character, Max: 256 characters.

Activate this action
Actions that are active will be executed on the launched instance, after it is launched.

This action must be completed successfully before finalizing cutover.

Systems Manager document name
Select any Systems Manager document that is available for this account.

 [View in Systems Manager](#) 

Description
Specify the action description. Up to 70 characters will be displayed on the card.

189 characters left

Document version
Select the document version to use.

Category
Select the action category which is available for this account.

Order
Specify the order in which the actions will be executed (range 1,001-10,000).

Operating systems
Select the source server's operating systems for which the action can be configured for.

Creator
Action creator.

Network requirements

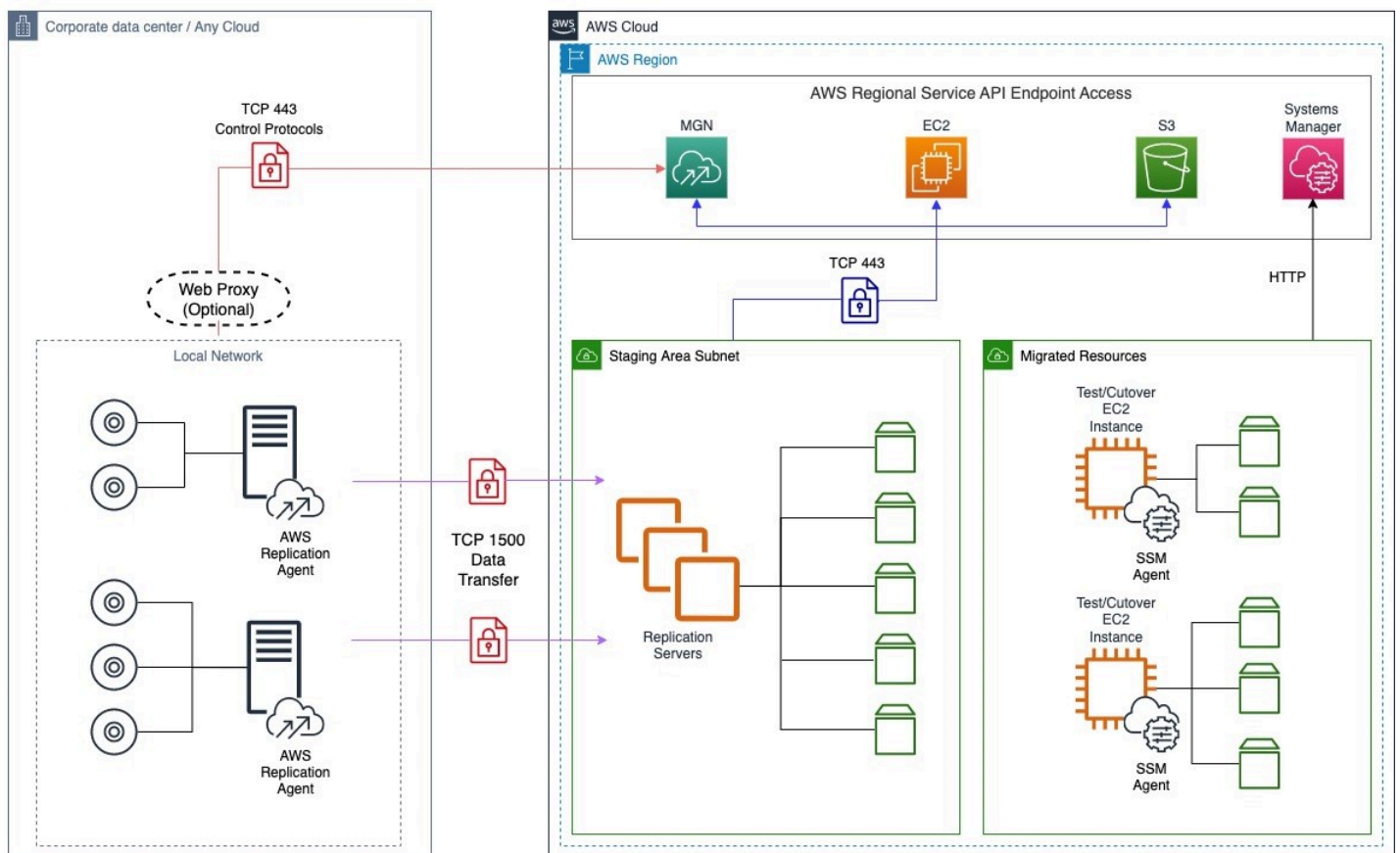
Topics

- [Service architecture and network architecture overview](#)
- [Network setting preparations](#)
- [Network requirements](#)

Service architecture and network architecture overview

Watch the [AWS Application Migration Service - Service architecture and network architecture video](#) for an in-depth overview of the AWS MGN architecture.

The following is the AWS MGN network diagram:



Network setting preparations

Topics

- [Staging area subnet](#)
- [Network requirements](#)
- [Operational subnets](#)

Staging area subnet

Before setting up AWS Application Migration Service (AWS MGN), you should create a subnet which will be used by the service as a staging area for data replicated from your source servers to AWS.

- You must specify this subnet in the replication settings template. While you can use an existing subnet in your AWS account, the best practice is to create a new dedicated subnet for this purpose. [Learn more about replication settings.](#)
- You can override this subnet for specific source servers in the [replication settings](#).

Network requirements

- The replication servers launched by AWS Application Migration Service (AWS MGN) in your staging area subnet need to be able to send data over TCP port 443 to the AWS MGN API endpoint at `https://mgn.{region}.amazonaws.com/`. Replace “{region}” with the AWS Region code you are replicating to, for example “us-east-1” .
- The source servers on which the AWS Replication Agent is installed need be able to send data over TCP port 1500 to the Replication Servers in the Staging Area Subnet. They also need to be able to send data to AWS MGN's API endpoint at `https://mgn.{region}.amazonaws.com/`. Replace “{region}” with the AWS Region code you are replicating to, for example “us-east-1” .

Note

SSL interception should not be applied for communication between replication servers and the AWS MGN's API endpoint, as well as between source servers and the AWS MGN's API endpoint.

Operational subnets

Test and cutover instances are launched in a subnet you specify in the Amazon EC2 launch template associated with each source server. The Amazon EC2 launch template is created automatically when you add a source server to AWS Application Migration Service.

[Learn more about launching test and cutover instances.](#)

[Learn more about how Amazon EC2 launch templates are used.](#)

Network requirements

To prepare your network for running AWS Application Migration Service, you need to set the following connectivity settings:

Note

All communication is encrypted with TLS.

Topics

- [Communication over TCP port 443](#)
- [Communication between the source servers and AWS Application Migration Service over TCP port 443](#)
- [Communication between the staging area subnet and AWS Application Migration Service over TCP port 443](#)
- [Communication between the source servers and the staging area subnet over TCP port 1500](#)

Communication over TCP port 443

Add the following IP addresses and URLs to your firewall:

The AWS Application Migration Service Region-specific console address:

- (mgn.<region>.amazonaws.com *example: mgn.eu-west-1.amazonaws.com*)

Amazon S3 service URLs (required for downloading AWS Application Migration Service software)

- The AWS Replication Agent installer should have access to the S3 bucket URL of the AWS Region you are using with AWS Application Migration Service.
- The staging area subnet should have access to S3.
- The following S3 buckets should be allowlisted:

```
https://aws-mgn-clients-<REGION>.s3.<REGION>.amazonaws.com/
https://aws-mgn-clients-hashes-<REGION>.s3.<REGION>.amazonaws.com/
https://aws-mgn-internal-<REGION>.s3.<REGION>.amazonaws.com/
https://aws-mgn-internal-hashes-<REGION>.s3.<REGION>.amazonaws.com/
https://aws-application-migration-service-<REGION>.s3.<REGION>.amazonaws.com/
https://aws-application-migration-service-hashes-<REGION>.s3.<REGION>.amazonaws.com/
https://amazon-ssm-<REGION>.s3.<REGION>.amazonaws.com/
```

Note

Agent installation and replication server components require S3 bucket for service functionality.

If you use an Amazon S3 VPC Endpoint, you must provide sufficient permissions for service functionality. See the following example policy for replicating to us-east-1:

```
{
  "Version": "2008-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "*"
      },
    },
    {
      "Action": "s3:GetObject",
      "Resource": [
        "arn:aws:s3:::aws-mgn-clients-us-east-1/*",
        "arn:aws:s3:::aws-mgn-clients-hashes-us-east-1/*",
        "arn:aws:s3:::aws-mgn-clients-us-east-1/*",
        "arn:aws:s3:::aws-mgn-clients-us-east-1/*",
        "arn:aws:s3:::aws-mgn-clients-hashes-us-east-1/*",
        "arn:aws:s3:::aws-mgn-internal-us-east-1/*",
      ]
    }
  ]
}
```

```
"arn:aws:s3:::aws-mgn-internal-hashes-us-east-1/*",  
"arn:aws:s3:::aws-application-migration-service-us-east-1/*",  
"arn:aws:s3:::aws-application-migration-service-hashes-us-east-1/*",  
"arn:aws:s3:::amazon-ssm-us-east-1/*"  
]  
}  
]  
}
```

AWS specific

The staging area subnet requires outbound access to the [EC2 endpoint of its AWS Region](#).

TCP port 443 is used for two communication routes:

1. Between the source servers and AWS Application Migration Service.
2. Between the staging area subnet and AWS Application Migration Service.

Communication between the source servers and AWS Application Migration Service over TCP port 443

Each source server that is added to AWS Application Migration Service (AWS MGN) must continuously communicate with AWS MGN (`mgn.<region>.amazonaws.com`) over TCP port 443.

The following are the main operations performed through TCP port 443:

- Downloading the AWS Replication Agent on the source servers.
- Upgrading installed agents.
- Connecting the source servers to the AWS Application Migration Service console and displaying their replication status.
- Monitoring the source servers for internal troubleshooting and the use of resource consumption metrics (such as CPU, RAM).
- Reporting source server-related events (for example, a removal of disk, or resizing of a disk).
- Transmit source server-related information to the AWS Application Migration Service console (including hardware information, running services, and installed applications and packages).
- Preparing the source servers for test or cutover.

⚠ Important

Make sure that your corporate firewall allows connections over TCP port 443.

Solving communication problems over TCP port 443 between the source servers and AWS Application Migration Service

If there is no connection between your source servers and AWS Application Migration Service (AWS MGN), make sure that your corporate firewall enables connectivity from the source servers to AWS MGN over TCP Port 443. If the connectivity is blocked, enable it.

Enabling Windows Firewall for TCP port 443 connectivity

⚠ Important

The information provided in this section is for general security and firewall guidance only. The information is provided on "AS IS" basis, with no guarantee of completeness, accuracy or timeliness, and without warranty or representations of any kind, expressed or implied. In no event will AWS Application Migration Service and/or its subsidiaries and/or their employees or service providers be liable to you or anyone else for any decision made or action taken in reliance on the information provided here or for any direct, indirect, consequential, special or similar damages (including any kind of loss), even if advised of the possibility of such damages. AWS Application Migration Service is not responsible for the update, validation, or support of security and firewall information.

ℹ Note

Enabling Windows Firewall for TCP port 443 connectivity will allow your servers to achieve outbound connectivity. You may still need to adjust other external components, such as firewall blocking or incorrect routes, in order to achieve full connectivity.

Note

These instructions are intended for the default OS firewall. You will need to consult the documentation of any third-party local firewall you use to learn how to enable TCP port 443 connectivity.

1. On the source server, open the **Windows Firewall** console.
2. On the console, select the **Outbound Rules** option from the tree.

Outbound Rules											
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
BranchCache Content Retrieval (HTTP-Out)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80
BranchCache Hosted Cache Client (HTTP-Out)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80, 443
BranchCache Hosted Cache Server(HTTP-Out)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local subnet	UDP	Any	3702
✓ Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any
✓ Cast to Device functionality (qWave-TCP-Out)	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	Any	2177
✓ Cast to Device functionality (qWave-UDP-Out)	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	2177
✓ Cast to Device streaming server (RTP-Stre-Out)	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any	Any
✓ Cast to Device streaming server (RTP-Stre-Out)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any
✓ Cast to Device streaming server (RTP-Stre-Out)	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
✓ Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	Any	53
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547
✓ Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any	Any	TCP	Any	445
✓ Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any
✓ Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	TCP	Any	IPHTTPS
✓ Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any

3. On the **Outbound Rules** table, select the rule that relates to the connectivity to Remote Port - 443. Check if the **Enabled** status is **Yes**.

Outbound Rules											
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
BranchCache Content Retrieval (HTTP-Out)	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80
BranchCache Hosted Cache Client (HTTP-Out)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80, 443
BranchCache Hosted Cache Server(HTTP-Out)	BranchCache - Hosted Cach...	All	No	Allow	No	SYSTEM	Any	Any	TCP	80, 443	Any
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow	No	%system...	Any	Local subnet	UDP	Any	3702
✓ Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No	Any	Any	Any	Any	Any	Any
✓ Cast to Device functionality (qWave-TCP-Out)	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	TCP	Any	2177
✓ Cast to Device functionality (qWave-UDP-Out)	Cast to Device functionality	Private...	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	2177
✓ Cast to Device streaming server (RTP-Stre-Out)	Cast to Device functionality	Private	Yes	Allow	No	%System...	Any	Local subnet	UDP	Any	Any
✓ Cast to Device streaming server (RTP-Stre-Out)	Cast to Device functionality	Public	Yes	Allow	No	%System...	Any	PlayTo Renderers	UDP	Any	Any
✓ Cast to Device streaming server (RTP-Stre-Out)	Cast to Device functionality	Domain	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
✓ Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	Any	53
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547
✓ Core Networking - Group Policy (LSASS-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any	Any	TCP	Any	445
✓ Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any
✓ Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	TCP	Any	IPHTTPS
✓ Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any

4. If the **Enabled** status of the rule is **No**, right-click it and select **Enable Rule** from the pop-up menu.

Outbound Rules											
Name	Group	Profile	Enabled	Action	Override	Program	Local Address	Remote Address	Protocol	Local Port	Remote Port
✓ AllJoyn Router (TCP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ AllJoyn Router (UDP-Out)	AllJoyn Router	Domai...	Yes	Allow	No	%System...	Any	Any	UDP	Any	Any
BranchCache Content Retrieval (HTTP-O...	BranchCache - Content Retr...	All	No	Allow	No	SYSTEM	Any	Any	TCP	Any	80
BranchCache Hosted Cache Client (HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No			Any	TCP	Any	80, 443
BranchCache Hosted Cache Server(HTTP...	BranchCache - Hosted Cach...	All	No	Allow	No			Any	TCP	80, 443	Any
BranchCache Peer Discovery (WSD-Out)	BranchCache - Peer Discove...	All	No	Allow	No			Local subnet	UDP	Any	3702
✓ Captive Portal Flow	Captive Portal Flow	All	Yes	Allow	No			Any	Any	Any	Any
✓ Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes	Allow	No			PlayTo Renderers	TCP	Any	2177
✓ Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes	Allow	No			PlayTo Renderers	UDP	Any	2177
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Private	Yes	Allow	No			Local subnet	UDP	Any	Any
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Public	Yes	Allow	No			PlayTo Renderers	UDP	Any	Any
✓ Cast to Device streaming server (RTP-Stre...	Cast to Device functionality	Domain	Yes	Allow	No			Any	UDP	Any	Any
✓ Core Networking - DNS (UDP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	Any	53
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	68	67
✓ Core Networking - Dynamic Host Config...	Core Networking	All	Yes	Allow	No	%System...	Any	Any	UDP	546	547
✓ Core Networking - Group Policy (LSASS-...	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ Core Networking - Group Policy (NP-Out)	Core Networking	Domain	Yes	Allow	No	System	Any	Any	TCP	Any	445
✓ Core Networking - Group Policy (TCP-Out)	Core Networking	Domain	Yes	Allow	No	%System...	Any	Any	TCP	Any	Any
✓ Core Networking - Internet Group Mana...	Core Networking	All	Yes	Allow	No	System	Any	Any	IGMP	Any	Any
✓ Core Networking - IPHTTPS (TCP-Out)	Core Networking	All	Yes	Allow	No	%System...	Any	Any	TCP	Any	IPHTTPS
✓ Core Networking - IPv6 (IPv6-Out)	Core Networking	All	Yes	Allow	No	System	Any	Any	IPv6	Any	Any

Enabling Linux Firewall for TCP port 443 connectivity

1. Enter the following command to add the required Firewall rule:

```
sudo iptables -A OUTPUT -p tcp --dport 443 -j ACCEPT
```

2. To verify the creation of the Firewall rule, enter the following commands:

```
sudo iptables -L
```

```
Chain INPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain FORWARD (policy ACCEPT)
```

```
target prot opt source destination
```

```
Chain OUTPUT (policy ACCEPT)
```

```
target prot opt source destination
```

```
ACCEPT tcp -- anywhere anywhere tcp dpt:443
```

Communication between the staging area subnet and AWS Application Migration Service over TCP port 443

The replication servers in the staging area subnet must continuously communicate with AWS Application Migration Service (AWS MGN) over TCP port 443. The main operations that are performed through this route are:

- Downloading the replication software by the replication servers.
- Connecting the replication servers to AWS Application Migration Service, and displaying their replication status.
- Monitoring the replication servers for internal troubleshooting use and resource consumption metrics (such as CPU, RAM).
- Reporting replication-related events.

Note

The staging area subnet requires S3 access.

Configuring communication over TCP port 443 between the staging area subnet and AWS Application Migration Service

You can establish communication between the staging area subnet and AWS Application Migration Service over TCP port 443 directly.

There are two ways to establish direct connectivity to the Internet for the VPC of the staging area, as described in the [VPC FAQ](#).

1. [Public IP address + Internet gateway](#)
2. [Private IP address + NAT instance](#)

Communication between the source servers and the staging area subnet over TCP port 1500

Each source server with an installed AWS Replication Agent continuously communicates with the AWS Application Migration Service replication servers in the staging area subnet over TCP port 1500. TCP port 1500 is needed for the transfer of replicated data from the source servers to the staging area subnet.

The replicated data is encrypted and compressed when transferred over TCP port 1500. Prior to being moved into the staging area subnet, the data is encrypted on the source infrastructure. The data is decrypted after it arrives at the staging area subnet and before it is written to the volumes.

TCP port 1500 is primarily used for the replication server data replication stream.

AWS Application Migration Service uses TLS 1.2 end to end from the agent installed on the source server to the Replication Server. Each replication server gets assigned a specific TLS server certificate, which is distributed to the corresponding Agent and validated against on the agent side.

Establishing communication over TCP port 1500

 **Important**

To allow traffic over TCP port 1500, make sure that your corporate firewall enables this connectivity.

Source servers

You must add your source servers to the AWS Application Migration Service console in order to migrate them into AWS. Source servers are added by installing the AWS Replication Agent on each individual server. The following documentation provides installation paths for both Linux and Windows servers. Ensure that your servers are supported by AWS Application Migration Service by reviewing the [Supported Operating Systems documentation](#).

In addition, AWS Application Migration Service allows you to perform [agentless snapshot replication](#) from your vCenter source environment into AWS. This is achieved by installing the AWS MGN vCenter Client in your vCenter environment. Agentless snapshot replication has its own unique credentials, installation, and replication mechanisms. AWS Application Migration Service recommends using agent-based replication when possible, as it supports CDP (Continuous Data Protection) and provides the shortest cutover window. Agentless replication should be used when your company's policies or technical issues prevent you from installing the AWS Replication Agent on each individual server.

Once your source servers have been added to AWS Application Migration Service, you can monitor and interact with them from the Source servers page. The Source servers page is the default view in the AWS Application Migration Service Console, and will be the page that you interact with the most. On the Source servers page, you can view all of your source servers, monitor their migration lifecycle and data replication state, see the next step in the migration process for each server, and sort your servers by a variety of categories. You can also perform a variety of commands from the Source servers page through the command menus. These menus allow you to full control your servers by managing data replication, launching test and cutover instances, and disconnecting servers from AWS Application Migration Service.

You can click on any individual source server on the Source servers page in order to access the server details view. This view will allow you to see the details for individual servers. Here you will be able to see an in-depth view of the server's migration lifecycle, browse an overview of the server's technical details, manage tags, manage disks, and most importantly, configure the individual replication settings and launch settings for the server.

Topics

- [Adding source servers](#)
- [Agentless snapshot based replication for vCenter source environments](#)
- [Source servers page](#)

- [Server details](#)

Adding source servers

Add source servers to AWS Application Migration Service by installing the AWS Replication Agent (also referred to as "the Agent") on them. The Agent can be installed on both Linux and Windows servers. You can add source servers from vCenter without installing an agent through the agentless replication feature.

Quick links:

- [Linux installation instructions](#)
- [Windows installation instructions](#)
- [Agentless replication instructions](#)

Note

While the use of AWS Application Migration Service is free for 90 days, you will incur charges for any AWS infrastructure that is provisioned during migration and after cutover, such as compute (Amazon EC2) and storage (Amazon EBS) resources. These are billed to your account separately, at your regular rates.

Topics

- [Installation requirements](#)
- [AWS Replication Agent installation instructions](#)
- [Supported operating systems](#)

Installation requirements

Before installing the AWS Replication Agent on your source servers, ensure that they meet the following requirements:

Topics

- [General requirements](#)
- [Source server requirements](#)
- [Linux installation requirements](#)
- [Windows installation requirements](#)

General requirements

- Ensure that the source server operating system is supported by AWS. [Learn more about supported operating systems.](#)
- Ensure that your setup meets all networking requirements. [Learn more about network requirements.](#)
- Ensure MAC address stability – ensure that the MAC addresses of the source servers do not change upon a reboot or any other common changes in your network environment. AWS Application Migration Service calculates the unique ID of the source server from the MAC address. When a MAC address changes, AWS Application Migration Service is no longer able to correctly identify the source server. Consequently, replication will stop. If this happens, you will need to reinstall the AWS Replication Agent and start replication from the beginning.

Source server requirements

The following are universal requirements for both Linux and Windows source servers:

- Root directory – Verify that your source server has at least 2 GB of free disk space on the root directory (/) .
- RAM – Verify that your source server has at least 300 MB of free RAM to run the AWS Replication Agent.

Note

AWS Application Migration Service does not support fully paravirtualized source servers. Source servers with partial paravirtualization, such as VMWare's paravirtualization of I/O devices, is supported.

Note

The AWS Replication Agent installer supports multipath.

Linux installation requirements

Ensure that your Linux source server meets the following installation requirements prior to installing the AWS Replication Agent:

- Python is installed on the server – Python 2 (2.4 or above) or Python 3 (3.0 or above).
- The following tools are required for agent installation only. The installer will attempt to install them if they are not present already:

```
make gcc perl tar gawk rpm
```

- Verify that you have at least 2 GB of free disk space on the root directory (/) of your source server for the installation. To check the available disk space on the root directory, run the following command:

```
df -h /
```

- Free disk space on the /tmp directory – for the duration of the installation process only, verify that you have at least 500 MB of free disk space on the /tmp directory. To check the available disk space on the /tmp directory run the following command:

```
df -h /tmp
```

After you have entered the above commands for checking the available disk space, the results will be displayed as follows:

```
ubuntu@Linux-1:~$ df -h /
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1      7.8G  1.4G  6.0G  19% /
ubuntu@Linux-1:~$ df -h /tmp
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1      7.8G  1.4G  6.0G  19% /tmp
```

- The active bootloader software is GRUB 1 or 2.
- Ensure that /tmp is mounted as read+write.

- Ensure that `/tmp` is mounted with the `exec` option. Verify that the `/tmp` directory is mounted in a way that allows you to run scripts and applications from it.

To verify that the `/tmp` directory is mounted without the `noexec` option, run the following command:

```
sudo mount | grep '/tmp'
```

If the result is similar to the following example, it means that the issue exists in your OS:

```
$ sudo mount | grep '/tmp'
/dev/xvda1 on /tmp type ext4 (rw,noexec)
```

To fix and remove the `noexec` option from the mounted `/tmp` directory, run the following command:

```
sudo mount -o remount,exec /tmp
```

The following example illustrates the troubleshooting procedure:

```
ubuntu@Linux-1:~$ sudo mount | grep '/tmp'
/dev/xvda1 on /tmp type ext4 (rw,noexec)
ubuntu@Linux-1:~$ sudo mount -o remount,exec /tmp
ubuntu@Linux-1:~$ sudo mount | grep '/tmp'
/dev/xvda1 on /tmp type ext4 (rw)
```

- The AWS Application Migration Service user needs to be either a root user or a user in the `sudoers` list.
- Ensure that the `dhclient` package is installed. If not, please install the package using following -

For Redhat/CentOS/Fedora/AmazonLinux:

```
sudo yum install dhclient
```

OR

```
sudo yum install dhcp-client
```

For Ubuntu/Debian:

```
sudo apt install isc-dhcp-client
```

For SUSE, check the [link](#) for the instructions to install "dhcp-client" package

- Verify that you have *kernel-devel/linux-headers* installed that are exactly the same version as the kernel you are running.

The version number of the kernel headers should be completely identical to the version number of the kernel. To handle this issue, follow these steps:

1. Identify the version of your running kernel.

```
uname -r
```

```
[root@ip-192-168-20-156 ~]# uname -r
4.14.177-107.254.amzn1.x86_64
[root@ip-192-168-20-156 ~]#
```

The *uname -r* output version should match the version of one of the installed kernel headers packages (*kernel-devel-<version number> / linux-headers-<version number>*).

2. Identify the version of your *kernel-devel/linux-headers*.

To identify the version of your running kernel, run the following command:

On RHEL/CENTOS/Oracle/SUSE:

```
rpm -qa | grep kernel
```

```
[root@ip-192-168-20-156 ~]# rpm -qa |grep kernel
kernel-4.14.177-107.254.amzn1.x86_64
kernel-headers-4.14.181-108.257.amzn1.x86_64
kernel-devel-4.14.177-107.254.amzn1.x86_64
kernel-tools-4.14.181-108.257.amzn1.x86_64
[root@ip-192-168-20-156 ~]#
```

Note

This command looks for kernel related packages. The *kernel-devel* package is the specific package to look for.

On Debian/Ubuntu:

```
apt-cache search linux-headers
```

```
ubuntu@Linux-1:~$ apt-cache search linux-headers
linux-headers-3.13.0-24 - Header files related to Linux kernel version
 3.13.0
linux-headers-3.13.0-24-generic - Linux kernel headers for version 3.1
3.0 on 64 bit x86 SMP
linux-headers-3.13.0-24-lowlatency - Linux kernel headers for version
3.13.0 on 64 bit x86 SMP
```

3. Verify that the folder that contains the *kernel-devel/linux-headers* is not a symbolic link.

Sometimes, the content of the *kernel-devel/linux-headers*, which match the version of the kernel, is actually a symbolic link. In this case, you will need to remove the link before installing the required package.

To verify that the folder that contains the *kernel-devel/linux-headers* is not a symbolic link, run the following command:

On RHEL/CENTOS/Oracle:

```
ls -l /usr/src/kernels
```

On Debian/Ubuntu/SUSE:

```
ls -l /usr/src
```

```
ubuntu@Linux-1:~$ ls -l /usr/src
total 8
lrwxrwxrwx 1 root root 41 May 29 15:40 3.13.0-116-generic -> /usr/src/linux-
headers-3.13.0-116-generic
drwxr-xr-x 24 root root 4096 Apr 5 20:43 linux-headers-3.13.0-116
drwxr-xr-x 7 root root 4096 Apr 5 20:43 linux-headers-3.13.0-116-generic
ubuntu@Linux-1:~$
```

In the above example, the results show that the actual **linux-headers-*** folders are not symbolic links.

4. [If a symbolic link exists] Delete the symbolic link.

If you found that the content of the *kernel-devel/linux-headers*, which match the version of the kernel, is a symbolic link, you need to delete the link. Run the following command:

```
rm /usr/src/<LINK NAME>
```

For example:

```
rm /usr/src/linux-headers-4.4.1
```

5. Install the correct *kernel-devel/linux-headers* from the repositories.

If none of the already installed *kernel-devel/linux-headers* packages match your running kernel version, you need to install the matching package.

Note

You can have several kernel headers versions simultaneously on your OS, and you can therefore safely install new kernel headers packages in addition to your existing ones (without uninstalling the other versions of the package.) A new kernel headers package does not impact the kernel, and does not overwrite older versions of the kernel headers.

Note

For everything to work, you need to install a kernel headers package with the exact same version number of the running kernel.

To install the correct *kernel-devel/linux-headers*, run the following command:

On RHEL/CENTOS/Oracle:

```
sudo yum install kernel-devel-`uname -r`
```

On Oracle with Unbreakable Enterprise Kernel:

```
sudo yum install kernel-uek-devel-`uname -r`
```

On Debian/Ubuntu:

```
sudo apt-get install linux-headers-`uname -r`
```

On SUSE:

```
sudo zypper install kernel-default-devel-`uname -r`
```

6. [If no matching package was found] Download the matching *kernel-devel/linux-headers* package.

If no matching package was found on the repositories configured on your server, you can download it manually from the Internet and then install it.

To download the matching *kernel-devel/linux-headers* package, navigate to the following sites:

RHEL, CENTOS, and Oracle [package directory](#)

SUSE [package directory](#)

Debian [package directory](#)

Ubuntu [package directory](#)

If the *kernel-devel/linux-headers* packages are not available for the current running kernel version, consider upgrading the kernel to a version that has corresponding *kernel-devel* packages available. System administrators should validate that the appropriate *kernel-devel* packages are available before upgrading the kernel.

Windows installation requirements

Note

Ensure that your source server operating system is supported. [Learn more about supported operating systems.](#)

Note

Ensure that your source server meets the agent installation hardware requirements, including:

- At least 2 GB of free disk space on the disk containing the "Program Files(x86)" directory
- At least 300 MB of free RAM

[Learn more about AWS Replication Agent installation hardware requirements.](#)

AWS Replication Agent installation instructions

You must install the AWS Replication Agent on each source server that you want to add to AWS Application Migration Service. Agent installation is composed of the following steps:

Topics

- [Generating the required AWS credentials](#)
- [Installing the AWS Replication Agent in AWS](#)
- [Installation instructions](#)
- [Installing the Agent on a secured network](#)
- [Uninstalling the Agent](#)
- [Reinstalling the Agent](#)

Generating the required AWS credentials

In order to install the AWS Replication Agent, you must first generate the required AWS credentials.

Important

Temporary credentials have many advantages. You don't need to rotate them or revoke them when they're no longer needed, and they cannot be reused after they expire. You can specify for how long the credentials are valid, up to a maximum limit. Because they provide enhanced security, using temporary credentials is considered best practice and the recommended option.

Topics

- [Temporary credentials](#)
- [Permanent credentials](#)

Temporary credentials

The temporary credentials provided by AWS Application Migration Service utilize a similar mechanism to the one used by [IAM Roles Anywhere](#).

To create temporary credentials, you will need to do the following:

1. [Create a new IAM Role](#) with the **AWSApplicationMigrationAgentInstallationPolicy** policy.
2. Request temporary security credentials [through AWS STS](#) through the [AssumeRole API](#).

An example of generating temporary credentials via AWS CLI can be found [here](#).

[Learn more about how temporary credentials work.](#)

Permanent credentials

Where possible, we recommend using temporary credentials instead of creating users who have long-term credentials such as passwords and access keys. However, there are specific use cases that require long-term credentials (for example, agentless snapshot based replications). [Learn more about long-term credentials.](#)

Installing the AWS Replication Agent in AWS

When installing an AWS Replication Agent on an AWS EC2 instance (when the source server is in AWS Regions), you don't need to generate credentials. Instead, you can use an instance profile with the required IAM policy:

- Go to the EC2 console and select your EC2 instance.
- From the top right-hand menu, select **Actions > Security > Modify IAM role**.
- Use a role that contains the [AWSApplicationMigrationServiceEc2InstancePolicy](#) policy.

If none exists, click **Create new IAM role**, attach the policy and return to the EC2 console window.

- Select your new role from the drop-down list and click **Update**.

Installation instructions

Once you have generated the required AWS credentials, you can install the AWS Replication Agent on your source servers. There are separate installation instructions for Linux and for Windows. Each operating system has its own installer and various installation options and parameters.

Topics

- [Linux](#)
- [Windows](#)

Linux

1. Ensure that the necessary service roles have been created by clicking on the Reinitialize service permissions button on the AWS Application Migration Service console's replication settings page. You must have the permissions necessary to create IAM roles in order for this operation to succeed.
2. Download the agent installer with the `wget` command your Linux source server. This `wget` command will download the Agent installer file - `aws-replication-installer-init` onto your server.

The Agent installer follows the following format: `https://aws-application-migration-service-<region>.s3.<region>.amazonaws.com/latest/linux/aws-replication-installer-init`. Replace `<region>` with the AWS Region into which you are replicating.

The following is an example of the full `wget` command for `us-east-1`:

```
wget -O ./aws-replication-installer-init https://aws-application-migration-service-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/aws-replication-installer-init
```

The command line will indicate when the installer has been successfully downloaded.

Important

- You need root privileges to run the Agent installer file on a Linux server. Alternatively, you can run the Agent Installer file with `sudo` permissions.
- If you need to validate the installer hash, the correct hash can be found here: `https://aws-application-migration-service-hashes-`

`<region>.s3.<region>.amazonaws.com/latest/linux/aws-replication-installer-init.sha512` (replace `<region>` with the AWS Region into which you are replicating. For example, `us-east-1`):

`https://aws-application-migration-service-hashes-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/aws-replication-installer-init.sha512`

- Replicating EC2 instances that were launched with marketplace product codes, is not supported.

Note

- The Linux installer creates the "aws-replication" group and "aws-replication" user within that group. The Agent will run within the context of the newly created user. Agent installation will attempt to add the user to "sudoers". Installation will fail if the Agent is unable to add the newly created "aws-replication" user to "sudoers".
- AWS Regions that are not opt-in also support the shorter installer path: `https://aws-application-migration-service-<region>.s3.amazonaws.com/latest/linux/aws-replication-installer-init`. Replace `<region>` with the AWS Region into which you are replicating.
- You can generate a custom installation command through the **Add servers** prompt. [Learn more about the Add servers prompt.](#)

The following table contains the installer download link by supported AWS Region:

Region name	Region identity	Download Link
US East (Ohio)	us-east-2	<code>https://aws-application-migration-service-us-east-2.s3.us-east-2.amazonaws.com/latest/linux/aws-replication-installer-init</code>

Region name	Region identity	Download Link
US East (N. Virginia)	us-east-1	https://aws-application-migration-service-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/aws-replication-installer-init
US West (N. California)	us-west-1	https://aws-application-migration-service-us-west-1.s3.us-west-1.amazonaws.com/latest/linux/aws-replication-installer-init
US West (Oregon)	us-west-2	https://aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com/latest/linux/aws-replication-installer-init
Africa (Cape Town)	af-south-1	https://aws-application-migration-service-af-south-1.s3.af-south-1.amazonaws.com/latest/linux/aws-replication-installer-init

Region name	Region identity	Download Link
Asia Pacific (Hong Kong)	ap-east-1	https://aws-application-migration-service-ap-east-1.s3.ap-east-1.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Jakarta)	ap-southeast-3	https://aws-application-migration-service-ap-southeast-3.s3.ap-southeast-3.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Mumbai)	ap-south-1	https://aws-application-migration-service-ap-south-1.s3.ap-south-1.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Osaka)	ap-northeast-3	https://aws-application-migration-service-ap-northeast-3.s3.ap-northeast-3.amazonaws.com/latest/linux/aws-replication-installer-init

Region name	Region identity	Download Link
Asia Pacific (Seoul)	ap-northeast-2	https://aws-application-migration-service-ap-northeast-2.s3.ap-northeast-2.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Singapore)	ap-southeast-1	https://aws-application-migration-service-ap-southeast-1.s3.ap-southeast-1.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Sydney)	ap-southeast-2	https://aws-application-migration-service-ap-southeast-2.s3.ap-southeast-2.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Tokyo)	ap-northeast-1	https://aws-application-migration-service-ap-northeast-1.s3.ap-northeast-1.amazonaws.com/latest/linux/aws-replication-installer-init

Region name	Region identity	Download Link
Canada (Central)	ca-central-1	https://aws-application-migration-service-ca-central-1.s3.ca-central-1.amazonaws.com/latest/linux/aws-replication-installer-init
Europe (Frankfurt)	eu-central-1	https://aws-application-migration-service-eu-central-1.s3.eu-central-1.amazonaws.com/latest/linux/aws-replication-installer-init
Europe (Ireland)	eu-west-1	https://aws-application-migration-service-eu-west-1.s3.eu-west-1.amazonaws.com/latest/linux/aws-replication-installer-init
Europe (London)	eu-west-2	https://aws-application-migration-service-eu-west-2.s3.eu-west-2.amazonaws.com/latest/linux/aws-replication-installer-init

Region name	Region identity	Download Link
Europe (Milan)	eu-south-1	https://aws-application-migration-service-eu-south-1.s3.eu-south-1.amazonaws.com/latest/linux/aws-replication-installer-init
Europe (Paris)	eu-west-3	https://aws-application-migration-service-eu-west-3.s3.eu-west-3.amazonaws.com/latest/linux/aws-replication-installer-init
Europe (Stockholm)	eu-north-1	https://aws-application-migration-service-eu-north-1.s3.eu-north-1.amazonaws.com/latest/linux/aws-replication-installer-init
Middle East (Bahrain)	me-south-1	https://aws-application-migration-service-me-south-1.s3.me-south-1.amazonaws.com/latest/linux/aws-replication-installer-init

Region name	Region identity	Download Link
South America (São Paulo)	sa-east-1	https://aws-application-migration-service-sa-east-1.s3.sa-east-1.amazonaws.com/latest/linux/aws-replication-installer-init
Middle East (UAE)	me-central-1	https://aws-application-migration-service-me-central-1.s3.me-central-1.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Melbourne)	ap-southeast-4	https://aws-application-migration-service-ap-southeast-4.s3.ap-southeast-4.amazonaws.com/latest/linux/aws-replication-installer-init
Asia Pacific (Hyderabad)	ap-south-2	https://aws-application-migration-service-ap-south-2.s3.ap-south-2.amazonaws.com/latest/linux/aws-replication-installer-init

Region name	Region identity	Download Link
Europe (Zurich)	eu-central-2	https://aws-application-migration-service-eu-central-2.s3.eu-central-2.amazonaws.com/latest/linux/aws-replication-installer-init
Europe (Spain)	eu-south-2	https://aws-application-migration-service-eu-south-2.s3.eu-south-2.amazonaws.com/latest/linux/aws-replication-installer-init
Tel Aviv	il-central-1	https://aws-application-migration-service-il-central-1.s3.il-central-1.amazonaws.com/latest/linux/aws-replication-installer-init
AWS GovCloud (US-East)	us-gov-east-1	https://aws-application-migration-service-us-gov-east-1.s3.us-gov-east-1.amazonaws.com/latest/linux/aws-replication-installer-init

Region name	Region identity	Download Link
AWS GovCloud (US-West)	us-gov-west-1	https://aws-application-migration-service-us-gov-west-1.s3.us-gov-west-1.amazonaws.com/latest/linux/aws-replication-installer-init

3. [Generate the temporary credentials](#) that are required to install the AWS Replication Agent.

Important

When using [temporary credentials](#) (created using an IAM role instead of a user), you will need to enter the following parameters into the command prompt:

- AWS access key
- AWS secret access key
- AWS session token

The request to enter an AWS session token will only appear if the system identifies that you are using temporary credentials. AWS access key for temporary credentials begins with the letters ASIA.

4. Once the agent installer has successfully downloaded, copy and input the installer command into the command line on your source server in order to run the installation script.

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

You can choose to add the Region and required credential as parameters in the installation scripts:

- **--region** – The AWS Region in which the installer will register the source server.
- **--aws-access-key-id** – The AWS IAM Access Key used for authenticating the installing user. If this parameter is not provided, the installer will prompt for it.
- **--aws-secret-access-key** – The AWS IAM Secret Access Key tied to the AWS IAM Access Key used for authenticating the installing user. If this parameter is not provided, the installer will prompt for it.

- **--aws-session-token** – The session token is generated when using [temporary credentials](#) that are generated using AWS STS. If you use temporary credentials and do not provide this parameter, the installer will prompt for it.

If you require additional customization, you can add a variety of parameters to the installation script in order to manipulate the way the agent is installed on your server. Add the parameters to the end of the installation script.

Available parameters include:

- **--no-prompt**

This parameter will run a silent installation.

- **--devices**

This parameter specifies which specific disks to replicate. The devices should be mentioned with comma separated, example `--devices="/dev/sda,/dev/sdb,/dev/sdc,/dev/sdd"`

- **--force-volumes**

This parameter must be used with the `--no-prompt` parameter. This parameter will cancel the automatic detection of physical disks to replicate. You will need to specify the exact disks to replicate using the `--devices` parameter (including the root disk, failure to specify the root disk will cause replication to fail). This parameter should only be used as a troubleshooting tool if the `--devices` parameter fails to identify the disks correctly.

- **--tags**

Use this parameter to add resource tags to the source server. Use a space to separate each tag (for example: `--tags KEY=VALUE [KEY=VALUE ...]`)

 **Note**

This flag may only be used when adding new source servers to AWS MGN. You cannot use the `--tags` flag to modify tags of source servers that have already been added to AWS MGN.

- **--s3-endpoint**

Use this parameter to specify a VPC endpoint you created for S3 if you do not wish to open your firewall ports to access the default S3 endpoint. [Learn more about installing the Agent on a blocked network.](#)

- `--user-provided-id`

This parameter allows you to provide a name to the source server that you are about to add, or identify a source server that needs to be updated.

- `--endpoint`

Use this parameter to specify the private link endpoint you created for AWS Application Migration Service if you do not wish to open your firewall ports to access the default AWS MGN endpoint. [Learn more about installing the Agent on a blocked network.](#)

- `--no-replication`

By default after agent installation, the replication begins automatically. This attribute allows you to install the agent without immediately starting the replication. The 90-day free replication period excludes hours where the replication was stopped.

To start the replication post installation of replication agent using `--no-replication` attribute you can start replication by using the "Start Replication" option from Replication menu for the source server in the AWS MGN Dashboard or by using AWS CLI [start-replication](#)

The installer will confirm that the installation of the AWS Replication Agent has started.

```
root@ip-172-31-7-211:~# sudo chmod +x aws-replication-installer-init; ./aws-replication-installer-init
The installation of the AWS Replication Agent has started.
```

5. The installer will prompt you to enter your **AWS Region Name**, the **AWS Access Key ID**, the **AWS Secret Access Key**, and the **AWS Session Token** that you previously generated. Enter the complete AWS Region name (for example, eu-central-1) and the full credentials.

```
root@ip-172-31-7-211:~# sudo chmod +x aws-replication-installer-init; ./aws-replication-installer-init
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key: *****
AWS Session Token: IqS7b73pZ21uXV7E3R//////////wBACVt1UWnc3QCM7JNEQC1By21C7MwvNpPtL3dyF+ztDXAnaTpJpC55o8DghBga1BdzFTAd1n480qo07J+hKtC5xb56d9F91o921wQpE1qAq2k//////////BBBAeADK3MTEKwJQ3NTHM5IM61gukV5NurC4h2u0KvBwN5M47aKCAgntMyD79s10Dz+rowh13Dca+QwX12z8Kk69
```

Note

- You can also enter these values as part of the installation script command parameters. If you do not enter these parameters as part of the installation script, you will be prompted to enter them one by one as described above. (for example: `sudo chmod +x aws-replication-installer-init; sudo ./aws-replication-installer-init --region regionname --aws-access-key-`

```
id AKIAIOSFODNN7EXAMPLE --aws-secret-access-key wJalrXUtnFEMI/
K7MDENG/bPxRfiCYEXAMPLEKEY).
```

- The AWS Access Key ID and AWS Secret Access Key values will be hidden when entered into the installer.

6. Once you have entered your credentials, the installer will identify volumes for replication. The installer will display the identified disks and prompt you to choose the disks you want to replicate.

```
root@ip-172-31-7-211:~# sudo chmod +x aws-replication-installer-init; ./aws-replication-installer-init
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key: *****
AWS Session Token: Iqo3b3p21uXZVjE7R////////wAcwZ1WVnc3QEMJG8Q2C7B216NwvPNAFTJudyE+z1DXanaTp3Ca5oaN0phB91BdzFYAdlnw4Boqo0D7j+kNtE5xb56uD9F91e921wQpE1qgA3j////////8BEAEaDk3MTEXMjQ5NTMSMyIMb1guX5Nuft4h2oBkV9vBw5M6s7ANRtAqN8yD39sJj05b++0wh190ra+Qew3lP12n8K8E9
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: /dev/xvdb,/dev/xvdc,/dev/xvda
To replicate some of the disks, type the path of the disks, separated with a comma (for example, /dev/sda,/dev/sdb). To replicate all disks, press Enter:
```

To replicate some of the disks, type the path of the disks, separated by a comma, as illustrated in the installer (such as: /dev/sda, /dev/sdb, and more). To replicate all of the disks, click **Enter**. The installer will identify the selected disks and print their size.

```
root@ip-172-31-7-211:~# sudo chmod +x aws-replication-installer-init; ./aws-replication-installer-init
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key: *****
AWS Session Token: Iqo3b3p21uXZVjE7R////////wAcwZ1WVnc3QEMJG8Q2C7B216NwvPNAFTJudyE+z1DXanaTp3Ca5oaN0phB91BdzFYAdlnw4Boqo0D7j+kNtE5xb56uD9F91e921wQpE1qgA3j////////8BEAEaDk3MTEXMjQ5NTMSMyIMb1guX5Nuft4h2oBkV9vBw5M6s7ANRtAqN8yD39sJj05b++0wh190ra+Qew3lP12n8K8E9
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: /dev/xvdb,/dev/xvdc,/dev/xvda
To replicate some of the disks, type the path of the disks, separated with a comma (for example, /dev/sda,/dev/sdb). To replicate all disks, press Enter:
Identified volume for replication: /dev/xvdb of size 19 GiB
Identified volume for replication: /dev/xvdc of size 1 GiB
Identified volume for replication: /dev/xvda of size 8 GiB
```

The installer will confirm that all disks were successfully identified.

```
root@ip-172-31-7-211:~# sudo chmod +x aws-replication-installer-init; ./aws-replication-installer-init
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key: *****
AWS Session Token: Iqo3b3p21uXZVjE7R////////wAcwZ1WVnc3QEMJG8Q2C7B216NwvPNAFTJudyE+z1DXanaTp3Ca5oaN0phB91BdzFYAdlnw4Boqo0D7j+kNtE5xb56uD9F91e921wQpE1qgA3j////////8BEAEaDk3MTEXMjQ5NTMSMyIMb1guX5Nuft4h2oBkV9vBw5M6s7ANRtAqN8yD39sJj05b++0wh190ra+Qew3lP12n8K8E9
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: /dev/xvdb,/dev/xvdc,/dev/xvda
To replicate some of the disks, type the path of the disks, separated with a comma (for example, /dev/sda,/dev/sdb). To replicate all disks, press Enter:
Identified volume for replication: /dev/xvdb of size 19 GiB
Identified volume for replication: /dev/xvdc of size 1 GiB
Identified volume for replication: /dev/xvda of size 8 GiB
```

Note

When identifying specific disks for replication, do not use apostrophes, brackets, or disk paths that do not exist. Type only existing disk paths. Each disk you selected for replication is displayed with the caption **Disk to replicate identified**. However, the displayed list of identified disks for replication may differ from the data you entered. This difference can be due to several reasons:

- The root disk of the source server is always replicated, whether you select it or not. Therefore, it always appears on the list of identified disks for replication.
- AWS Application Migration Service replicates whole disks. Therefore, if you choose to replicate a partition, its entire disk will appear on the list and will later be replicated.

If several partitions on the same disk are selected, then the disk encompassing all of them will appear only once on the list.

- Incorrect disks may be chosen by accident. Ensure that the correct disks have been chosen.

⚠ Important

If disks are disconnected from a server, AWS Application Migration Service can no longer replicate them, so they are removed from the list of replicated disks. When they are reconnected, the AWS Replication Agent cannot know that these were the same disks that were disconnected and therefore does not add them automatically. To add the disks after they are reconnected, rerun the AWS Replication Agent installer on the server. Note that the returned disks will need to be replicated from the beginning. Any disk size changes will be automatically identified, but this will also cause a resync. Perform a test after installing the Agent to ensure that the correct disks have been added.

7. After all of the disks that will be replicated have been successfully identified, the installer will download and install the AWS Replication Agent on the source server.

```
root@ip-172-31-7-211:~# sudo chmod +x aws-replication-installer-init; ./aws-replication-installer-init
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID: *****
AWS Secret Access Key: *****
AWS Session Token: Iqo7b1j221x2Vj5Dh//////////waaCXVhWnc1q2MSJGM4QC1Bp216JWwPn8FtJdyE*ztDXana7pJc5e5Nq8d8g18dzFYAdinw48oqo07j*4Ntt5xb56d9F91e921wQpE1qAgJa//////////BBEAkADok3MTEkMjQ5NTM3Ny1Mb1guxV2Nurf14h2o8KvsBwN5M4*7aNRKAgpNkyQ73sYU5B++Dwh19Dra+Qaw31P12m8K86

Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: /dev/xvdb,/dev/xvdc,/dev/xvda
To replicate some of the disks, type the path of the disks, separated with a comma (for example, /dev/sda,/dev/sdb). To replicate all disks, press Enter:
Identified volume for replication: /dev/xvdb of size 10 GiB
Identified volume for replication: /dev/xvdc of size 1 GiB
Identified volume for replication: /dev/xvda of size 8 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.
```

8. Once the AWS Replication Agent is installed, the server will be added to the AWS Application Migration Service Console and will undergo the initial sync process. The installer will provide you with the source server's ID.

```
root@ip-172-31-7-211:~# sudo chmod +x aws-replication-installer-init; ./aws-replication-installer-init
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID: *****
AWS Secret Access Key: *****
AWS Session Token: Iqo7b1j221x2Vj5Dh//////////waaCXVhWnc1q2MSJGM4QC1Bp216JWwPn8FtJdyE*ztDXana7pJc5e5Nq8d8g18dzFYAdinw48oqo07j*4Ntt5xb56d9F91e921wQpE1qAgJa//////////BBEAkADok3MTEkMjQ5NTM3Ny1Mb1guxV2Nurf14h2o8KvsBwN5M4*7aNRKAgpNkyQ73sYU5B++Dwh19Dra+Qaw31P12m8K86

Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: /dev/xvdb,/dev/xvdc,/dev/xvda
To replicate some of the disks, type the path of the disks, separated with a comma (for example, /dev/sda,/dev/sdb). To replicate all disks, press Enter:
Identified volume for replication: /dev/xvdc of size 1 GiB
Identified volume for replication: /dev/xvdb of size 10 GiB
Identified volume for replication: /dev/xvda of size 8 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-381f1c5f90a1e0d1
You now have 1 active source server out of a total quota of 200.
Check 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.
```

You can review this process in real time on the **Source servers** page. [Learn more about the initial sync process.](#)

Windows

1. Ensure that the necessary service roles have been created by clicking on the **Reinitialize service permissions** button on the AWS Application Migration Service console replication settings page. You must have the permissions necessary to create IAM roles in order for this operation to succeed.
2. Download the agent installer (AWSReplicationWindowsInstaller.exe). Copy or distribute the downloaded agent installer to each Windows source server that you want to add to AWS Application Migration Service.

The agent installer follows the following format: `https://aws-application-migration-service-<region>.s3.<region>.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe`. Replace `<region>` with the AWS Region into which you are replicating.

The following is an example of the installer link for us-east-1:

```
https://aws-application-migration-service-us-east-1.s3.us-east-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
```

Important

- You need to run the agent installer file as an Administrator on each Windows server.
- If you need to validate the installer hash, the correct hash can be found here: `https://aws-application-migration-service-hashes-<region>.s3.<region>.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe.sha512` (replace `<region>` with the AWS Region into which you are replicating, for example, us-east-1:

```
https://aws-application-migration-service-hashes-us-east-1.s3.us-east-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe.sha512
```

- We recommend using Windows PowerShell, which support ctrl+v pasting, and not Windows Command Prompt (cmd), which does not.
- Replicating EC2 instances that were launched with marketplace product codes, is not supported.

Note

- AWS Regions that are not opt-in also support the shorter installer path: `https://aws-application-migration-service-<region>.s3.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe`. Replace `<region>` with the AWS Region into which you are replicating.
- You can generate a custom installation command through the **Add servers** prompt. [Learn more about the Add servers prompt.](#)
- Microsoft Windows Server versions 2003, 2003 R2, 2008 and 2008 R2 use a unique version of the AWS Replication Agent that is only valid for legacy Windows OSs (`AwsReplicationWindowsLegacyInstaller.exe`). DO NOT use this installer file to install the agent on any other OS types. You can generate an installer by following the steps outlines in the [Add servers actions prompt documentation](#) or directly download it from `https://aws-application-migration-service-<region>.s3.amazonaws.com/latest/windows_legacy/AwsReplicationWindowsLegacyInstaller.exe`. Replace `<region>` with the AWS Region into which you are replicating. If you need to validate the installer hash, the correct hash can be found here: `https://aws-application-migration-service-hashes-<region>.s3.amazonaws.com/latest/windows_legacy/AwsReplicationWindowsLegacyInstaller.exe.sha512` (replace `<region>` with the AWS Region into which you are replicating).

The following table contains the installer download link by supported AWS Region:

Region name	Region identity	Download Link
US East (Ohio)	us-east-2	<code>https://aws-application-migration-service-us-east-2.s3.us-east-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe</code>

Region name	Region identity	Download Link
US East (N. Virginia)	us-east-1	https://aws-application-migration-service-us-east-1.s3.us-east-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
US West (N. California)	us-west-1	https://aws-application-migration-service-us-west-1.s3.us-west-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
US West (Oregon)	us-west-2	https://aws-application-migration-service-us-west-2.s3.us-west-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Africa (Cape Town)	af-south-1	https://aws-application-migration-service-af-south-1.s3.af-south-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
Asia Pacific (Hong Kong)	ap-east-1	https://aws-application-migration-service-ap-east-1.s3.ap-east-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Jakarta)	ap-southeast-3	https://aws-application-migration-service-ap-southeast-3.s3.ap-southeast-3.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Mumbai)	ap-south-1	https://aws-application-migration-service-ap-south-1.s3.ap-south-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Osaka)	ap-northeast-3	https://aws-application-migration-service-ap-northeast-3.s3.ap-northeast-3.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
Asia Pacific (Seoul)	ap-northeast-2	https://aws-application-migration-service-ap-northeast-2.s3.ap-northeast-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Singapore)	ap-southeast-1	https://aws-application-migration-service-ap-southeast-1.s3.ap-southeast-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Sydney)	ap-southeast-2	https://aws-application-migration-service-ap-southeast-2.s3.ap-southeast-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Tokyo)	ap-northeast-1	https://aws-application-migration-service-ap-northeast-1.s3.ap-northeast-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
Canada (Central)	ca-central-1	https://aws-application-migration-service-ca-central-1.s3.ca-central-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Europe (Frankfurt)	eu-central-1	https://aws-application-migration-service-eu-central-1.s3.eu-central-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Europe (Ireland)	eu-west-1	https://aws-application-migration-service-eu-west-1.s3.eu-west-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Europe (London)	eu-west-2	https://aws-application-migration-service-eu-west-2.s3.eu-west-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
Europe (Milan)	eu-south-1	https://aws-application-migration-service-eu-south-1.s3.eu-south-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Europe (Paris)	eu-west-3	https://aws-application-migration-service-eu-west-3.s3.eu-west-3.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Europe (Stockholm)	eu-north-1	https://aws-application-migration-service-eu-north-1.s3.eu-north-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Middle East (Bahrain)	me-south-1	https://aws-application-migration-service-me-south-1.s3.me-south-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
South America (São Paulo)	sa-east-1	https://aws-application-migration-service-sa-east-1.s3.sa-east-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Middle East (UAE)	me-central-1	https://aws-application-migration-service-me-central-1.s3.me-central-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Melbourne)	ap-southeast-4	https://aws-application-migration-service-ap-southeast-4.s3.ap-southeast-4.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Asia Pacific (Hyderabad)	ap-south-2	https://aws-application-migration-service-ap-south-2.s3.ap-south-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
Europe (Zurich)	eu-central-2	https://aws-application-migration-service-eu-central-2.s3.eu-central-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Europe (Spain)	eu-south-2	https://aws-application-migration-service-eu-south-2.s3.eu-south-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Tel Aviv	il-central-1	https://aws-application-migration-service-il-central-1.s3.il-central-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
AWS GovCloud (US-East)	us-gov-east-1	https://aws-application-migration-service-us-gov-east-1.s3.us-gov-east-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
AWS GovCloud (US-West)	us-gov-west-1	https://aws-application-migration-service-us-gov-west-1.s3.us-gov-west-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

3. [Generate the temporary credentials](#) that are required to install the AWS Replication Agent.

Important

When using [temporary credentials](#) (created using an IAM role instead of a user), you will need to enter the following parameters into the command prompt:

- AWS access key
- AWS secret access key
- AWS session token

The request to enter an AWS session token will only appear if the system identifies that you are using temporary credentials. AWS access key for temporary credentials begins with the letters ASIA.

4. Run the agent installer file – `AWSReplicationWindowsInstaller.exe` – as an Administrator. The CMD will open.

To run the installer with the default settings, enter your **AWS Region Name**, the **AWS Access Key ID** and the **AWS Secret Access Key**, and the **AWS Session Token** as described in the next step.

If you require additional customization, you can add a variety of parameters to the installation script in order to manipulate the way the Agent is installed on your server. Add the parameters to the end of the installation script.

- `--no-prompt`

This parameter will run a silent installation.

- `--devices`


This parameter specifies which specific disks to replicate.

- `--force-volumes`

This parameter must be used with the `--no-prompt` parameter. This parameter will cancel the automatic detection of physical disks to replicate. You will need to specify the exact disks to replicate using the `--devices` parameter (including the root disk, failure to specify the root disk will cause replication to fail). This parameter should only be used as a troubleshooting tool if the `--devices` parameter fails to identify the disks correctly.

- `--tags`

Use this parameter to add resource tags to the source server. Use a space to separate each tag (for example: `--tags KEY=VALUE [KEY=VALUE ...]`)

 **Note**

This flag may only be used when adding new source servers to AWS MGN. You cannot use the `--tags` flag to modify tags of source servers that have already been added to AWS MGN.

- `--s3-endpoint`

Use this parameter to specify a VPC endpoint you created for S3 if you do not wish to open your firewall ports to access the default S3 endpoint. [Learn more about installing the Agent on a blocked network.](#)

- `--user-provided-id`

This parameter allows you to provide a name to the source server that you are about to add, or identify a source server that needs to be updated.

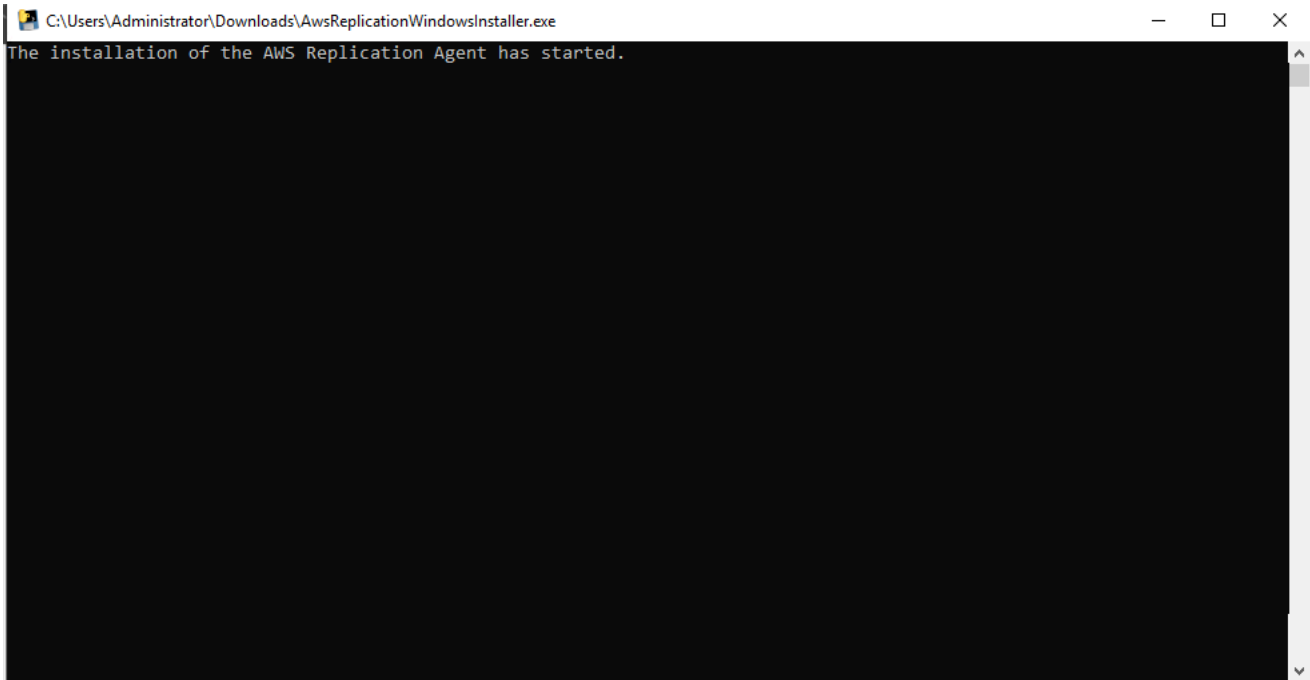
- `--endpoint`

Use this parameter to specify the Private Link endpoint you created for AWS Application Migration Service if you do not wish to open your firewall ports to access the default AWS MGN endpoint. [Learn more about installing the agent on a blocked network.](#)

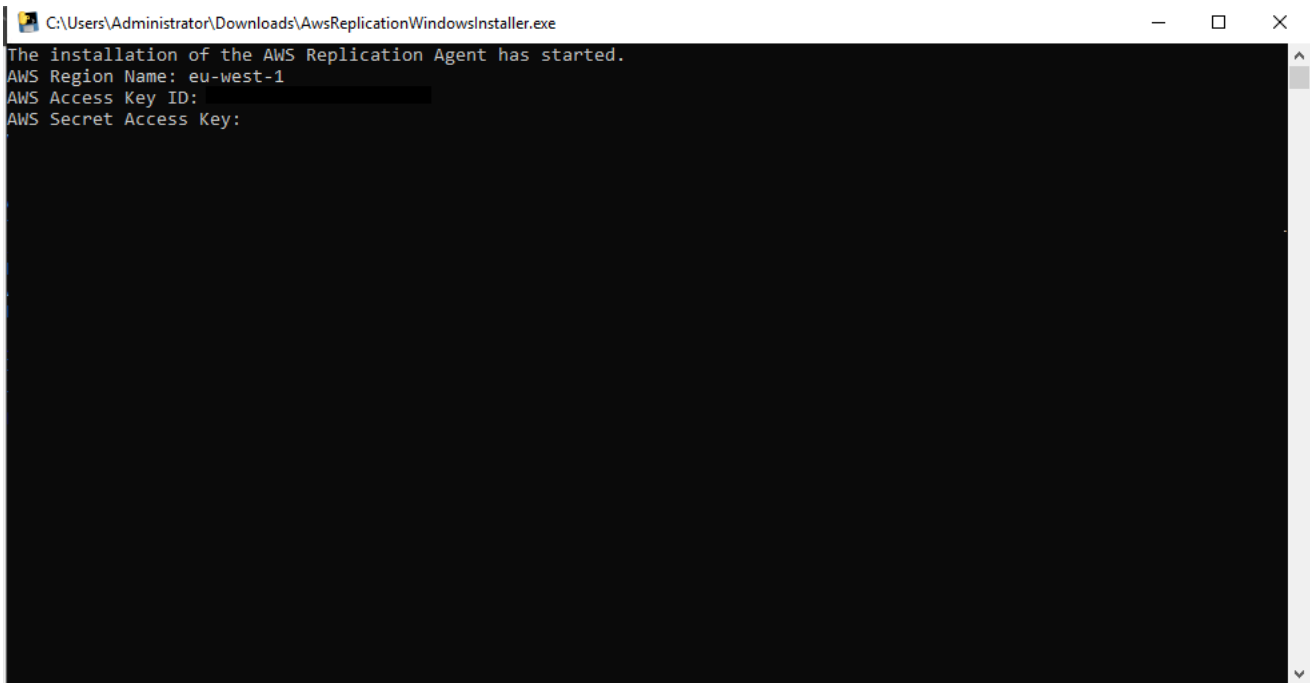
- `--no-replication`

By default after agent installation, the replication begins automatically. This attribute allows you to install the agent without immediately starting the replication. The 90-day free replication period excludes hours where the replication was stopped.

The installer will confirm that the installation of the AWS Replication Agent has started.



5. The installer will prompt you to enter your **AWS Region Name**, the **AWS Access Key ID**, the **AWS Secret Access Key** (and the **AWS Session Token** if appropriate) that you previously generated. Enter the complete AWS Region name (for example: eu-central-1), and the full AWS Access Key ID and AWS Secret Access Key.

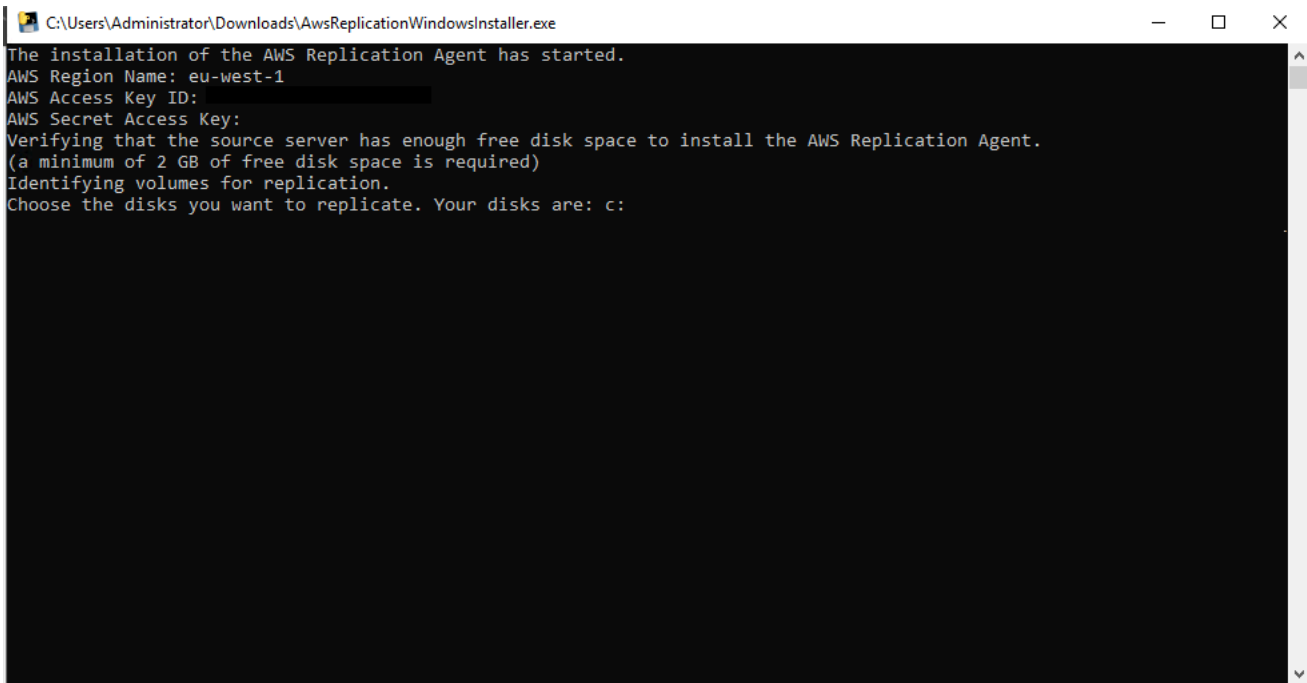
A screenshot of a Windows command prompt window titled "C:\Users\Administrator\Downloads\AwsReplicationWindowsInstaller.exe". The window shows the following text: "The installation of the AWS Replication Agent has started.", "AWS Region Name: eu-west-1", "AWS Access Key ID:", and "AWS Secret Access Key:". The rest of the window is black, indicating that the user has entered their credentials and the installer is proceeding.

```
C:\Users\Administrator\Downloads\AwsReplicationWindowsInstaller.exe
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key:
```

Note

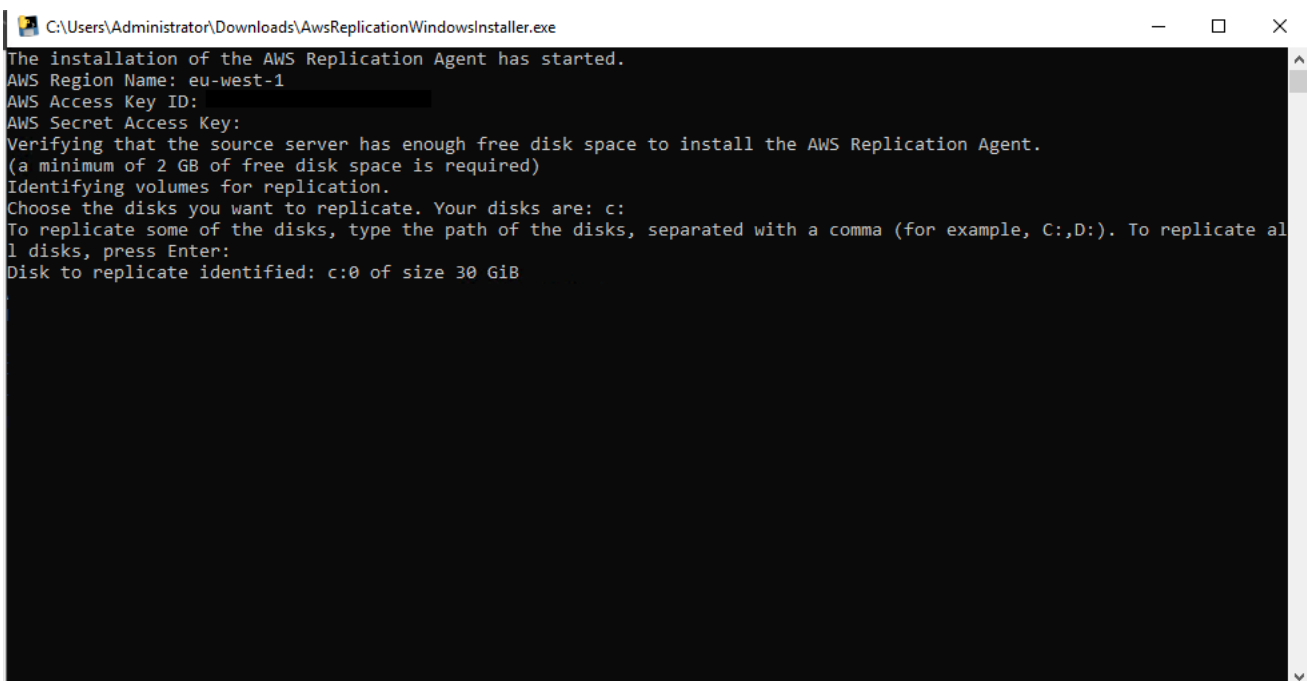
You can also enter these values as part of the installation script command parameters. If you do not enter these parameters as part of the installation script, you will be prompted to enter them one by one as described above. (for example: `AwsReplicationWindowsInstaller.exe --region regionname --aws-access-key-id AKIAIOSFODNN7EXAMPLE --aws-secret-access-key wJa1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)

6. Once you have entered your credentials, the installer will verify that the source server has enough free disk space for Agent installation and identify volumes for replication. The installer will display the identified disks and prompt you to choose the disks you want to replicate.



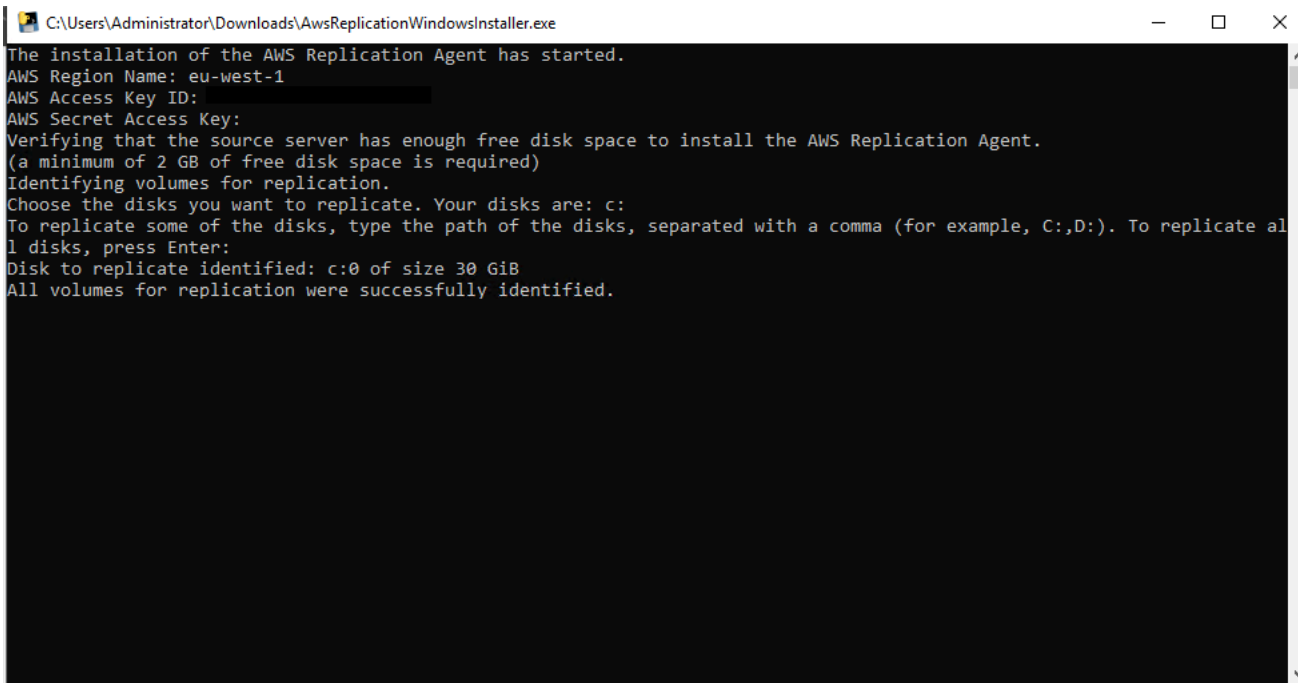
```
C:\Users\Administrator\Downloads\AwsReplicationWindowsInstaller.exe
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key:
Verifying that the source server has enough free disk space to install the AWS Replication Agent.
(a minimum of 2 GB of free disk space is required)
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are: c:
```

To replicate some of the disks, type the path of the disks, separated by a comma, as illustrated in the installer (for example: C: or D:). To replicate all of the disks, press **Enter**. The installer will identify the selected disks and print their size.



```
C:\Users\Administrator\Downloads\AwsReplicationWindowsInstaller.exe
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key:
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.
Choose the disks you want to replicate. Your disks are: c:
To replicate some of the disks, type the path of the disks, separated with a comma (for example, C:,D:). To replicate all disks, press Enter:
Disk to replicate identified: c:0 of size 30 GiB
```

The installer will confirm that all of the disks were successfully identified.

A screenshot of a Windows command prompt window titled "C:\Users\Administrator\Downloads\AwsReplicationWindowsInstaller.exe". The window shows the following text:

```
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key:
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.
Choose the disks you want to replicate. Your disks are: c:
To replicate some of the disks, type the path of the disks, separated with a comma (for example, C:,D:). To replicate all
l disks, press Enter:
Disk to replicate identified: c:\0 of size 30 GiB
All volumes for replication were successfully identified.
```

Note

When identifying specific disks for replication, do not use apostrophes, brackets, or disk paths that do not exist. Type only existing disk paths. Each disk that you selected for replication is displayed with the caption **Disk to replicate identified**. However, the displayed list of identified disks for replication may differ from the data you entered. This difference can be due to several reasons:

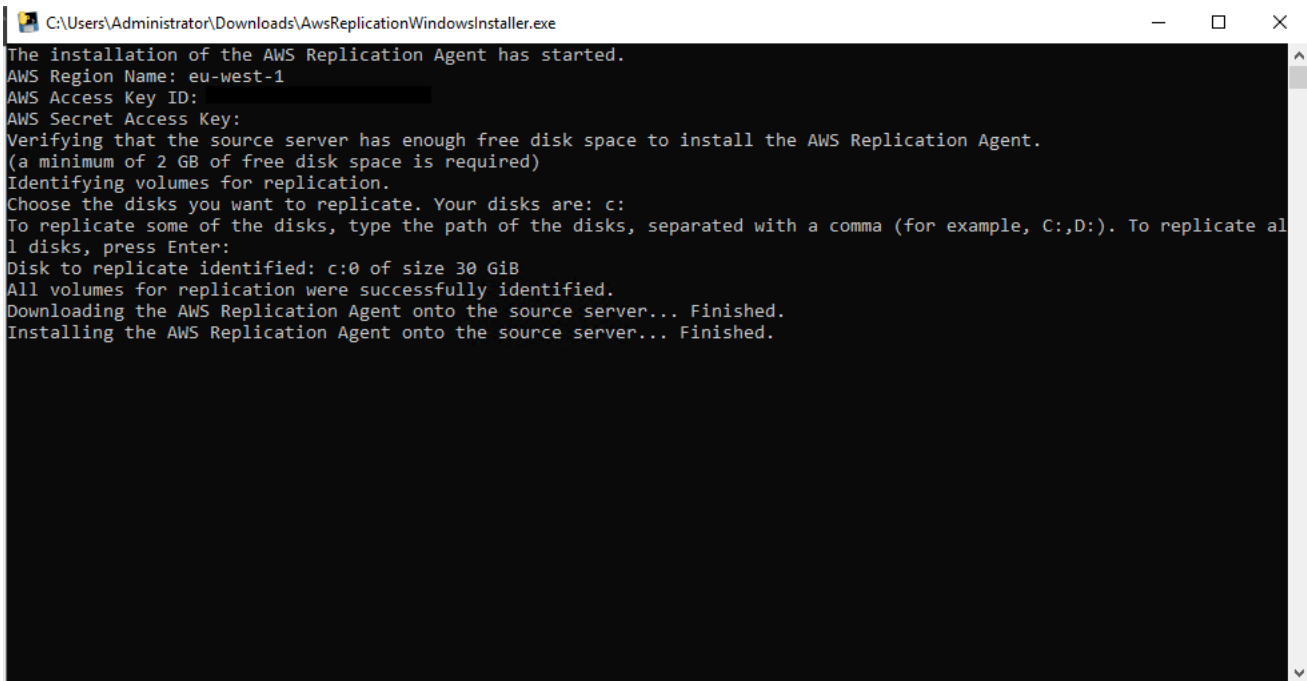
- The root disk of the source server is always replicated, whether you select it or not. Therefore, it always appears on the list of identified disks for replication.
- AWS Application Migration Service replicates whole disks. Therefore, if you choose to replicate a partition, its entire disk will appear on the list and will later be replicated. If several partitions on the same disk are selected, then the disk encompassing all of them will only appear once on the list.
- Incorrect disks may be chosen by accident. Ensure that the correct disks have been chosen.

Important

If disks are disconnected from a server, AWS Application Migration Service can no longer replicate them, so they are removed from the list of replicated disks. When they are

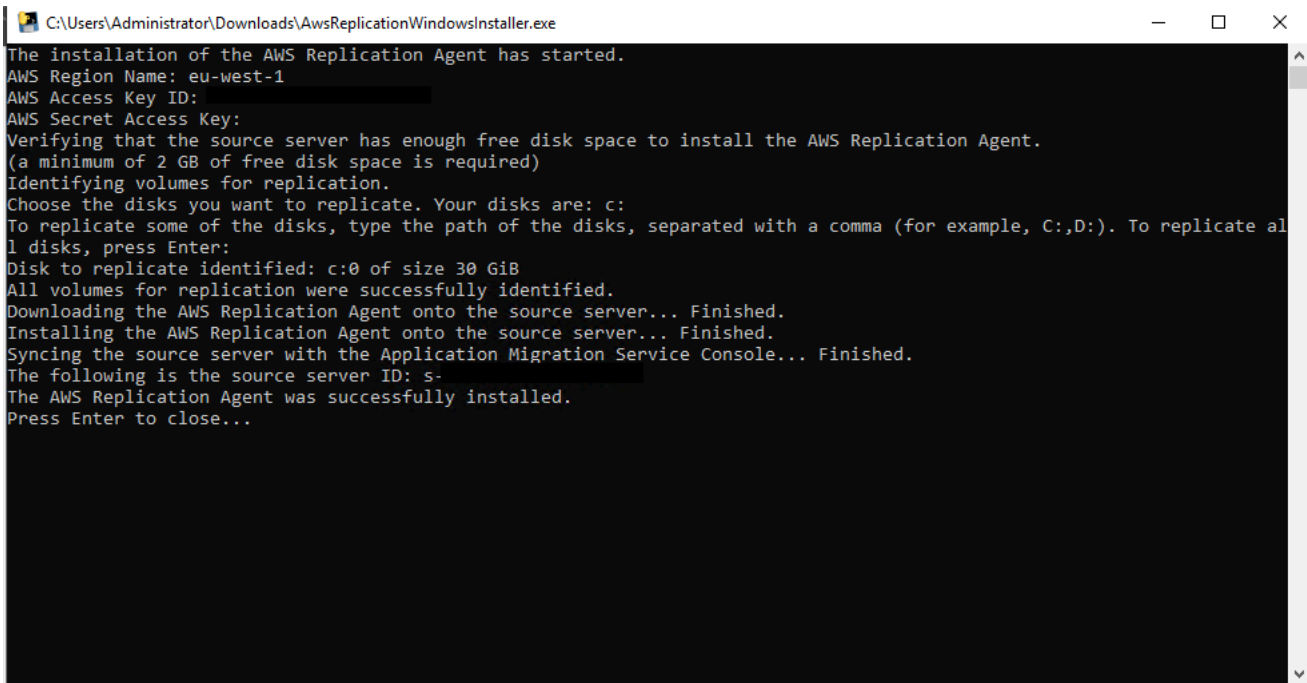
reconnected, the AWS Replication Agent cannot know that these were the same disks that were disconnected and therefore does not add them automatically. To add the disks after they are reconnected, rerun the AWS Replication Agent installer on the server. Note that the returned disks will need be replicated from the beginning. Any disk size changes will be automatically identified, but will also cause a resync. Perform a test after installing the Agent to ensure that the correct disks have been added.

7. After all of the disks that will be replicated have been successfully identified, the installer will download and install the AWS Replication Agent on the source server.



```
C:\Users\Administrator\Downloads\AwsReplicationWindowsInstaller.exe
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key:
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.
Choose the disks you want to replicate. Your disks are: c:
To replicate some of the disks, type the path of the disks, separated with a comma (for example, C:,D:). To replicate all
1 disks, press Enter:
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.
```

8. Once the AWS Replication Agent is installed, the server will be added to the AWS Application Migration Service Console and will undergo the initial sync process. The installer will provide you with the source server's ID.

A screenshot of a Windows command prompt window titled "C:\Users\Administrator\Downloads\AwsReplicationWindowsInstaller.exe". The window displays the following text:

```
The installation of the AWS Replication Agent has started.
AWS Region Name: eu-west-1
AWS Access Key ID:
AWS Secret Access Key:
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.
Choose the disks you want to replicate. Your disks are: c:
To replicate some of the disks, type the path of the disks, separated with a comma (for example, C:,D:). To replicate all
 disks, press Enter:
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-
The AWS Replication Agent was successfully installed.
Press Enter to close...
```

You can review this process in real time on the **Source servers** page. [Learn more about the initial sync process.](#)

Installing the Agent on a secured network

The Application Migration Service AWS Replication Agent installer needs network access to AWS MGN and S3 endpoints. If your on premises network is not open to MGN and S3 endpoints, then you can install the Agent with the aid of PrivateLink.

You can connect your on premises network to the subnet in your staging area VPC using AWS VPN or DirectConnect. To use the AWS VPN or DirectConnect, you must [use private IP in the replication settings.](#)

Create a VPC endpoint for AWS Application Migration Service

To allow the AWS Replication Agent installer to communicate with AWS MGN, create an interface VPC endpoint for AWS MGN in your staging area subnet. For more information, see [Creating an interface endpoint](#) in the *Amazon VPC User Guide*.

If the AWS replication agents are installed with a principal using [AWSApplicationMigrationAgentInstallationPolicy](#) and a VPCE policy is used (to scope down access), add the following statement to your policy:

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "execute-api:Invoke",
  "Resource": "arn:aws:execute-api:<region>:*:*/POST/CreateSessionForMgn"
}
```

Use the created VPC Endpoint for AWS Application Migration Service

Once you have created the VPC Endpoint, the AWS Replication Agent can connect to AWS Application Migration Service (AWS MGN) via VPN/DirectConnect by using the `--endpoint` installation parameter. Learn more about [Private DNS for interface endpoints](#) in the *Amazon VPC User Guide*.

Run the AWS Replication Agent installer with the `--endpoint` parameter. Enter your endpoint-specific DNS hostname within the parameter. The installer will then be able to connect to AWS MGN via the endpoint over your VPN/DirectConnect connection.

Create a S3 endpoint for AWS Application Migration Service

To allow the AWS Replication Agent installer to communicate with S3, create an interface S3 endpoint for AWS MGN in your staging area subnet. For more information, see [Endpoints for Amazon S3](#) in the *Amazon VPC User Guide*.

Use the created S3 Endpoint for AWS Application Migration Service

Once you have created the VPC Endpoint, the AWS Replication Agent can connect to S3 via VPN/DirectConnect by using the `--s3-endpoint` installation parameter. Learn more about [Private DNS for interface endpoints](#) in the *Amazon VPC User Guide*.

Run the AWS Replication Agent installer with the `--s3-endpoint` parameter. Enter your endpoint-specific DNS hostname. The installer will then be able to connect to AWS MGN via the endpoint over your VPN/DirectConnect connection.

Prescriptive guidance

A detailed guide for rehosting servers using MGN over private networks is available here:

[Migrating on-premises servers to AWS over private networks by using AWS Application Migration Service.](#)

Uninstalling the Agent

Uninstalling the AWS Replication Agent from a source server stops the replication of that server. Uninstalling the AWS Replication Agent will remove the source server from the AWS Application Migration Service Console.

Note

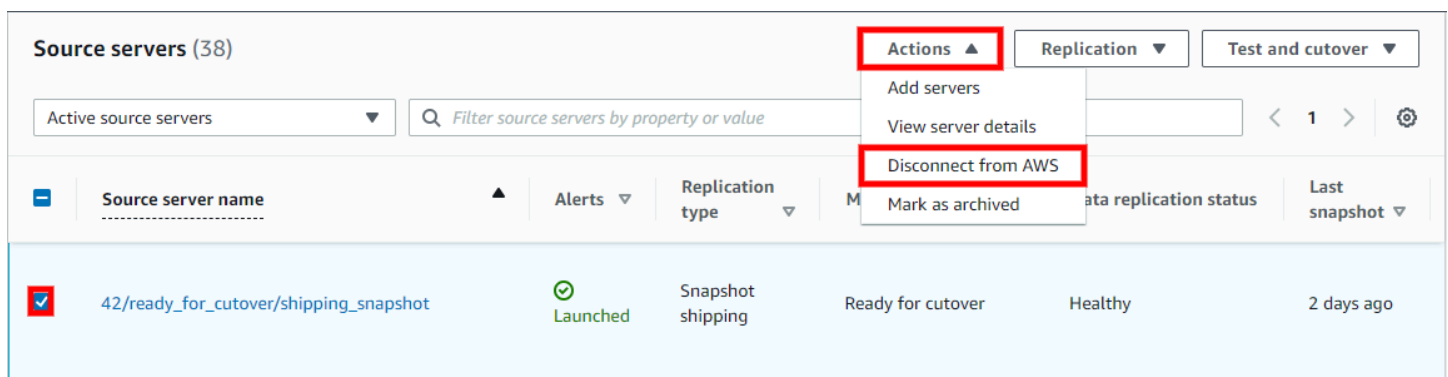
- The source server must be able to communicate with the AWS MGN service in order for the Agent to be uninstalled successfully.
- If the Agent is uninstalled directly from a source server without disconnecting the server from AWS MGN or finalizing the cutover within the AWS MGN Console, the replication metering period will continue and once 2160 hours have elapsed, billing for replication will begin.

Uninstalling the Agent through the AWS Application Migration Service Console

To uninstall the AWS Replication Agent through the AWS Application Migration Service Console.

Navigate to the **Source servers** page.

Check the box to the left of each server that you want to disconnect from AWS Application Migration Service (by uninstalling the AWS Replication Agent). Open the **Actions** menu, and choose the **Disconnect from service** option to disconnect the selected server from Application Migration Service and AWS.



The screenshot shows the AWS Application Migration Service console interface. At the top, there's a header for 'Source servers (38)'. Below this, there's a search bar with the text 'Filter source servers by property or value'. To the right of the search bar, there are three buttons: 'Actions' (highlighted with a red box), 'Replication', and 'Test and cutover'. Below the search bar, there's a table with columns: 'Source server name', 'Alerts', 'Replication type', 'M', 'Data replication status', and 'Last snapshot'. The first row in the table has a checked checkbox, the name '42/ready_for_cutover/shipping_snapshot', a green checkmark icon with the text 'Launched', 'Snapshot shipping', 'Ready for cutover', 'Healthy', and '2 days ago'. The 'Actions' menu is open, showing options: 'Add servers', 'View server details', 'Disconnect from AWS' (highlighted with a red box), and 'Mark as archived'.

On the **Disconnect X server/s from service** dialog, click **Disconnect**.

The AWS Replication Agent will be uninstalled from all of the selected source servers. You will then be able to archive these servers. [Learn more about archiving.](#)

Uninstalling the Agent manually through the source server

To uninstall the AWS Replication Agent manually through the source server:

Windows

Copy the following folder to a new location: `C:\Program Files (x86)\AWS Replication Agent\dist`

From the new location, run in CMD as an administrator:

```
install_agent_windows.exe --remove
```

Linux

Run as root or with sudo the following commands:

```
/var/lib/aws-replication-agent/uninstall-agent.sh
```

Reinstalling the Agent

To reinstall the AWS Replication Agent, download the latest version of the agent and follow the installation instructions. The AWS Replication Agent can be installed over an existing agent installation. You do not need to remove any previous versions prior to install.

- [Linux](#)
- [Windows](#)

Supported operating systems

AWS Application Migration Service allows replication of any physical, virtual or cloud-based source server to the AWS Cloud for a large variety of operating systems.

There may be a number of additional considerations to take into account when determining if your source operating system will be supported by AWS Application Migration Service. Ensure that you check the [Additional Considerations](#) section in conjunction with the below lists of supported operating systems.

Note

- AWS Application Migration Service does not support fully paravirtualized source servers. Source servers with partial paravirtualization, such as VMWare's paravirtualization of I/O devices, is supported.
- AWS Application Migration Service only supports operating systems built for the x86 system architecture.

Windows

The following Windows operating systems are supported:

- Microsoft Windows Server 2022 64-bit
- Microsoft Windows Server 2019 64-bit
- Microsoft Windows Server 2016 64-bit
- Microsoft Windows 10 64-bit

The following End of Life Windows operating systems are supported:

- Microsoft Windows Server 2012 R2 64-bit
- Microsoft Windows Server 2012 64-bit
- Microsoft Windows Server 2008 R2 64-bit (patched)
- Microsoft Windows Server 2008 64-bit
- Microsoft Windows Server 2008 32-bit
- Microsoft Windows Server 2003 R2 64-bit
- Microsoft Windows Server 2003 R2 32-bit
- Microsoft Windows Server 2003 64-bit
- Microsoft Windows Server 2003 32-bit

Linux

The following Linux operating systems are supported:

- Amazon Linux (AL) 1, 2, and 2023

- CentOS 5.5 to 7.9
- Debian Linux 8 to 11
- Oracle Linux (OL) 6.0 to 7.0 (running Unbreakable Enterprise Kernel Release 3 or higher or Red Hat compatible Kernel only)
- Oracle Linux (OL) 8.5 to 8.9 (running Unbreakable Enterprise Kernel Release 6 or Red Hat Compatible Kernel only) – see the tested UEK kernels below:
 - 5.15.0-200.131.27.el8uek.x86_64
 - 5.15.0-101.103.2.1.el8uek.x86_64
 - 5.15.0-3.60.5.1.el8uek.x86_64
 - 5.4.17-2136.314.6.3.el8uek.x86_64
 - 5.4.17-2136.307.3.1.el8uek.x86_64
 - 5.4.17-2136.300.7.el8uek.x86_64
- Red Hat Enterprise Linux (RHEL) 5.5 to 9.0
- Rocky Linux 8 and 9
- SUSE Linux Enterprise Server 11 SP4 to 15 SP5
- Ubuntu LTS 12.04 to 24.04

Additional considerations

There may be a number of additional considerations to take into account when determining if your source operating system will be supported by AWS Application Migration Service. Ensure that you check the below considerations in conjunction with the above lists of supported operating systems.

Windows

- It is recommended to install all available Windows updates on the server.
- Windows source servers need to have at least 2 GB of free disk space in order to launch a test or cutover instance successfully.
- The WMI service must be activated to install the AWS Replication Agent.
- Microsoft Windows Server versions 2008 R2 and above require .Net Framework version 4.5 or above to be installed by the end user.
- Ensure that the [auto sleep function in Windows 10](#) is deactivated. Data replication may be interrupted if the feature is activated.

Additional notes for older versions of Windows

- The Nitro instance family can only be used with Windows Server 2008 R2 and upwards. Earlier versions are not supported.
- Windows 2003 does not support TLS 1.2, as such, you cannot download the AWS Replication Agent installer directly by using the default browser. The file needs to be copied to the server using another transfer method.
- The AWS Replication Agent and agent installer uses a separate installer file (AwsReplicationWindowsLegacyInstaller.exe) for Microsoft Windows Server 2003 (32-bit and 64-bit), Microsoft Windows Server 2008 (32-bit and 64-bit) and Microsoft Windows Server 2008 R2 (64-bit) because these OSs are using older versions of software components that cannot be upgraded due to their end-of-life status.
- Windows 2008 x64 requires SP2 and other Microsoft updates to support the SHA-2 signature of the AWS Replication Agent driver.
- Microsoft Windows Server 2003 (32-bit and 64-bit) and Microsoft Windows Server 2008 (32-bit and 64-bit) require .Net Framework version 3.5 to be installed by the end user.

Linux

- Ensure that you have Python installed on the source server (version 2.4+, version 3.0+) for Agent installation.
- Only servers using the GRUB bootloader are supported.
- Secure Boot is not supported in Linux.
- AWS Application Migration Service does not support 32 bit versions of Linux.
- Migration of servers using the Oracle ASM Filter Driver is fully supported for Oracle, CentOS, and Red Hat Enterprise Linux (RHEL) 6.0 to 8.7.
- Boot disks that span multiple physical disks are not supported.
- AWS requires that servers running Red Hat Enterprise Linux (RHEL) must have Cloud Access (BYOL) licenses in order to be recovered to AWS. Note that servers running RHEL Cloud Access Gold Images allow you to access AWS Red Hat Update Infrastructure (RHUI), Red Hat Satellite, or Red Hat Subscription Manager (RHSM). If you are using RHEL Cloud Access Gold Images, you will not be able to access RHUI upon migrating to AWS unless you link your AWS account to your Red Hat account via the Red Hat portal, and select the Gold image AMI in the launch template.

- You must select an AWS provided RHEL AMI in the Launch Template for servers running Red Hat Enterprise Linux (RHEL) Pay as You Go (PAYG) images. This will allow access to RHUI after migration. Note that usage of these images will incur EC2 charges for software and infrastructure per AWS Marketplace rates.
- Only Kernel 3.x or above are supported for Debian/Ubuntu on AWS.
- Azure kernels are not supported as they are not compatible with the Amazon EC2 hardware. Ubuntu servers from Azure will be required to switch the kernel to a standard kernel or the AWS tuned Ubuntu kernel 'linux-aws'.
- Kernel versions 2.6.32-71 are not supported in RHEL 6.0/CentOS 6.0/Oracle Linux 6.0 on AWS.
- Oracle Linux source servers must be running Unbreakable Enterprise Kernel Release 3 or higher or a Red Hat Compatible Kernel only.
- Kernel version 4.9.256 is not supported. Agent installation will fail on servers that run this kernel version.
- Kernel versions earlier than 2.6.18-164 are not supported by AWS Application Migration Service. Therefore, servers that run these kernel versions cannot be replicated by AWS Application Migration Service.
- Nitro instance types will work with RHEL 7.4+/CentOS 7.4+/Oracle Linux 7.4+. This specific limitation does not apply to other instance type families.
- A pre-requirement for installing the AWS Replication Agent on RHEL 8/CentOS 8/OL 8 is first running the following:

```
sudo yum install elfutils-libelf-devel
```

- The AWS Replication Agent is supported on SUSE Linux Enterprise Server (SLES) 11 SP4 and higher.
- The post-launch actions feature is not supported on CentOS 5.x, CentOS 6.x, RHEL 6.x and Oracle 6.x.
- For SUSE Linux (SLES) 11 SP4 to work, you must install the Xen drivers before installing the AWS Replication Agent. You must reboot the server after installing the Xen drivers (before installing the AWS Replication Agent). Use the following command to install the drivers:

```
zypper install -y xen-kmp-default
```

- Machines that boot off a disk configured with GPT partitioning need to have the package 'grub2-pc-modules' installed.

- Linux kernel version upto 6.8 is supported.

Agentless snapshot based replication for vCenter source environments

AWS Application Migration Service (AWS MGN) allows you to perform agentless snapshot replication from your vCenter source environment into AWS. This is achieved by installing the AWS MGN vCenter Client in your vCenter environment. AWS MGN recommends using agent-based replication when possible, as it supports CDP (Continuous Data Protection) and provides the shortest cutover window. Agentless replication should be used when your company's policies prevent you from installing the AWS Replication Agent on each individual server.

Agentless replication overview

Agentless snapshot-based replication allows you to replicate source servers on your vCenter environment into AWS without installing the AWS Replication Agent.

In order to use agentless replication, you must dedicate at least one VM in your vCenter environment to host the AWS MGN vCenter Client. The AWS MGN vCenter Client is a software bundle distributed by AWS MGN and is available for installation as a binary installer. The installation process will install services on the client VM which will allow AWS MGN to remotely discover your VMs that are suitable for agentless replication, and to perform data replication between your vCenter environment and AWS through the use of periodic snapshot shipping.

Agentless snapshot based replication is divided into two main operations: discovery and replication:

The discovery process involves periodically scanning your vCenter environment to detect source server VMs that are suitable for agentless replication, and adding these VMs to the AWS MGN Console. Once a source server has been added, you may choose to initiate agentless replication on the source VM using the MGN API or Console. The discovery process also collects all of the necessary information from vCenter in order to perform an agentless conversion process once a migration job is launched.

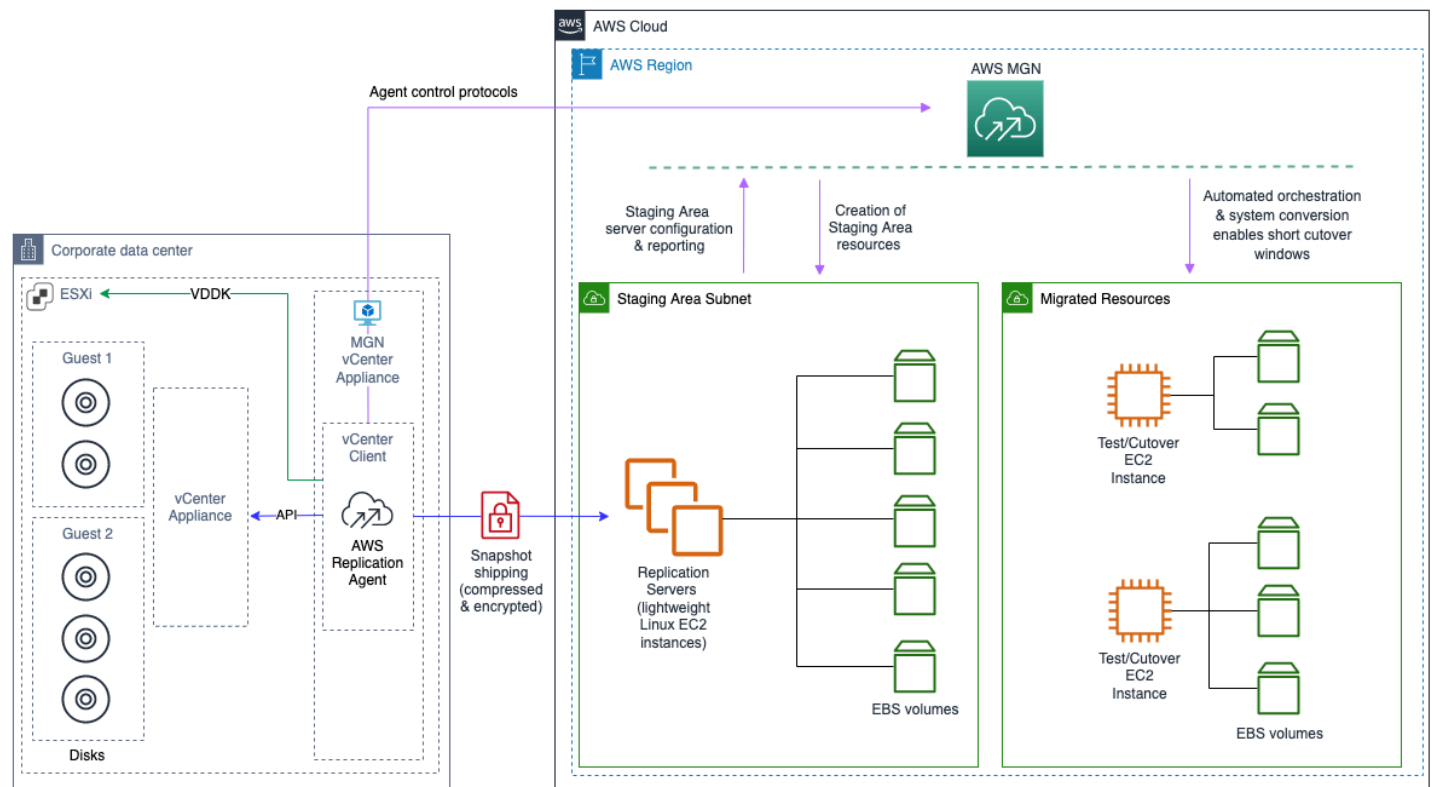
The replication process involves continuously starting and monitoring the "snapshot shipping processes" on the source server VM being replicated. A "snapshot shipping process" is a long running logical operation which consists of taking a VMware snapshot on the replicated VM, and

launching an ephemeral replication agent process which uses VMware's Changed Block Tracking (CBT) feature to identify changed volume data location, using Virtual Disk Development Kit (VDDK) to read the modified data, and sending the data from the source environment to the customer's target AWS account. The first snapshot shipping process performs an "initial sync" which sends the entire disk contents of the replicating VM into AWS. Following snapshot shipping processes will leverage CBT in order to only sync disk changes to the customer's target AWS account. Each successful snapshot shipping process completes the replication operation by creating a group of consistent EBS snapshots in the customer's AWS account, which can then be used by the customer to launch test and cutover instances through the regular MGN mechanisms.

The following are the main system components of agentless replication:

- AWS MGN vCenter Client – A software bundle that is installed on a dedicated VM in your vCenter environment in order to facilitate agentless replication.
- vCenter Replication Agent – A java agent that is based on the AWS Replication Agent, which replicates a single VM using VDDK and CBT as the data source instead of the AWS MGN driver (that is used by the AWS Replication Agent)
- AWS MGN Service
- AWS MGN Console

The following diagram illustrates the high level interaction between the different agentless replication system components:



Prerequisites

1. Ensure that you have [initialized AWS Application Migration Service](#).

VMware limitations

1. AWS MGN supports VMC on AWS for agentless replication.
2. AWS MGN partially supports vMotion, Storage vMotion, and other features based on virtual machine migration (such as DRS and Storage DRS) subject to the following limitations:
 - Migrating a virtual machine to a new ESXi host or datastore after one replication run ends, and before the next replication run begins, is supported as long as the vCenter account has sufficient permissions on the destination ESXi host, datastores, and datacenter, and on the virtual machine itself at the new location.
 - Migrating a virtual machine to a new ESXi host, datastore, and/or datacenter while a replication run is active – that is, while a virtual machine upload is in progress – is not supported. Cross vCenter vMotion is not supported for use with AWS MGN.
3. AWS does not provide support for migrating VMware Virtual Volumes.

4. AWS MGN does not support replicating VMware VMs that have snapshots.

Generating vCenter Client IAM credentials

In order to use the AWS MGN vCenter Client, you must first generate the correct IAM credentials.

You will need to create at least one AWS Identity and Access Management (IAM) user, and assign the proper permission policies to this user. You will obtain an Access key ID and Secret access key, which you will need to enter into the Agent installation prompt in order to begin the installation. We recommend that you use **IAM access last used information** to rotate and remove access keys safely. For more information, see [Rotating access keys](#).

1. Open the **AWS Management Console** and look for **IAM** under **Find Services**.
2. From the **IAM** main page, choose **Users** from the left-hand navigation menu.
3. You can either select an existing user or add a new user. To add a new user, click **Add user**.
4. Give the user a **User name** and select the **Programmatic access** access type. Click **Next: Permissions**.
5. Choose the **Attach existing policies directly** option. Search for **AWSApplicationMigrationVCenterClientPolicy** and **AWSApplicationMigrationAgentPolicy**. Select the policies and click **Next: Tags**.
6. Add tags if you wish to use them and then click **Next: Review**.
7. Review the information. Ensure that the **Programmatic access** type is selected and that the correct policy is attached to the user. Choose **Create user**.
8. A confirmation message will appear and you can see the **Access key ID** and **Secret access key** that you will need in order to install the AWS Replication Agent on your source servers.

To save this information as .csv file, click **Download .csv**.

You can also access this information and re-generate your security credentials by navigating to **IM > Users > Your user**.

Open the **Security credentials** tab and scroll down to **Access keys**. Here you can manage your access keys (create, delete, and more).

Installing the AWS MGN vCenter Client

The first step to deploying the agentless solution is installing the AWS MGN vCenter Client on your vCenter environment.

Note

If you have multiple vCenter environments, you will need to install multiple clients. You may not have more than one AWS MGN vCenter Client installed per AWS Account. If you have multiple vCenter environments, you can either use a different AWS Account for each environment or you can migrate your VMs serially, environment by environment, into the same AWS Account.

After the AWS MGN vCenter Client has been installed, it will discover all of the VMs in your vCenter environment and add them to AWS MGN.

AWS MGN vCenter Client requirements

Ensure that you review the notes below prior to installing the AWS MGN vCenter Client. Once you have read the notes, proceed to [install the client](#).

vCenter Client requirements

- You must install the AWS MGN vCenter Client on a VM that has outbound and inbound network connectivity to the AWS Application Migration Service API endpoints and outbound and inbound network connectivity to the vCenter endpoint. Customers who want to use PrivateLink can use VPN or DirectConnect to connect to AWS.
- The AWS MGN vCenter Client currently only supports VirtualDiskFlatVer2BackingInfo VMDK on CBT. [Learn more about this in the VMware knowledgebase](#).
- You must download [this VDDK version](#) to the VM on which the AWS MGN vCenter Client is installed. VDDK 7.0.3.3 must be used, regardless of the vCenter version used.
- The AWS MGN vCenter Client requires the following vCenter user permissions for agentless deployment. It is a best practice to create a dedicated role with these permissions and a dedicated user group with which the role will be associated. Every new user created for the AWS MGN vCenter Client will need to be a member of that group in order to obtain the required permissions. The vCenter predefined role: " Consolidated Backup user (sample) " provides most

of these permissions. If that role is used, the following additional permission must be provided:

Toggle disk change tracking.

- Change configuration
 - Acquire disk lease
 - Toggle disk change tracking
- Provisioning
 - Allow read-only disk access
 - Allow virtual machine download
- Snapshot management
 - Create snapshot
 - Remove snapshot
- The VM on which the AWS MGN vCenter Client is installed should meet the following RAM, CPU, and memory requirements:
 - Minimal requirements (these requirements will allow the replication of up to 5 servers in parallel) – 2 GiB RAM, 1 core, 10 GiB of free disk space
 - Optional performance requirements (these requirements will allow the replication of the maximum number of 50 servers in parallel) – 16 GiB RAM, 8 cores, 10 GiB of free disk space
- VMs that are being replicated into AWS should have at least 2 GiB of free disk space.
- The VM on which the AWS MGN vCenter Client is installed should not allow any incoming (ingress) traffic.
- The VM on which the AWS MGN vCenter Client is installed should only allow outgoing traffic as following:
 - Egress TCP on the port on which the vCenter API is ran.
 - Egress TCP on port 443 for communication with the MGN API.
 - Egress TCP on port 1500 – for the replication server.
- Patching of guest OS running AWS vCenter client should be handled by the customer as part of shared responsibility.
- IAM credentials used by the vCenter Client should be rotated on a regular schedule. Learn more about how to rotate access keys for IAM users in [this IAM blog post](#). IAM credentials can be regenerated by reinstalling the AWS Replication Agent.
- The VM that hosts the AWS MGN vCenter Client should only be used for client hosting and ~~should not be used for any other purposes.~~

- Only a trusted administrator should have access to the VM on which the AWS MGN vCenter Client is installed.
- The AWS MGN vCenter Client should be located in an isolated and dedicated network and considered a sensitive segment.
- You can deactivate the vCenter Client auto-update mechanism by running the following command: `touch /var/lib/aws-vcenter-client/.disable_auto_updates` Once auto-updates are deactivated, you will need to reinstall the client to perform a manual update. If you deactivate the auto-update mechanism, you will be responsible for ensuring that all security updates are performed on the client. After a manual update, you should validate the new hash against the [installer hash](#).

vCenter Client installer notes

- The AWS MGN vCenter Client installer only supports vCenter 6.7, 7.0 and 8.0.
- The MGN vCenter Client can be installed on the following 64 bit Linux versions:
 - Ubuntu 18.x+ (64 bit) - 22.04
 - Amazon Linux 2
 - RHEL 8.x
- If you are using a RHEL 8.x environment, ensure that you run the `sudo yum install python3` command to install python prior to launching the client installer.
- The following flags are used by the installer:
 - usage: `aws-vcenter-client-installer-init.py [-h]`
 - `[--aws-access-key-id AWS_ACCESS_KEY_ID]`
 - `[--aws-access-key-id AWS_ACCESS_KEY_ID]`
 - `[--aws-secret-access-key AWS_SECRET_ACCESS_KEY]`
 - `[--region REGION]`
 - `[--endpoint ENDPOINT]`
 - `[--s3-endpoint S3_ENDPOINT]`
 - `[--vcenter-host VCENTER_HOST]`
 - `[--vcenter-port VCENTER_PORT]`
 - `[--vcenter-user VCENTER_USER]`
 - `[--vcenter-password VCENTER_PASSWORD]`

- [--vcenter-ca-path VCENTER_CA_PATH]
- [--vddk-path VDDK_PATH]
- [--vcenter-client-tags KEY=VALUE [KEY=VALUE ...]]
- [--source-server-tags KEY=VALUE [KEY=VALUE ...]]
- [--disable-ssl-cert-validation]
- [--no-prompt]
- Use this flag for an unattended installation. If you are using this flag, you must also use the --force-delete-existing client flag.

[--force-delete-existing-client]

- Use this flag to delete an existing version of the vCenter Client from your VM. You must use this flag if you've previously installed the vCenter Client on the VM. If you use the --no-prompt flag, you must also use this flag.

[--version]

Optional arguments:

-h, --help show this help message and exit

vCenter environment requirements

- AWS Application Migration Service (AWS MGN) supports VM hardware version 7 and higher with CBT activated. Ensure that you upgrade any VMs you have to hardware version 7 or higher. Ensure that CBT support is activated in your vSphere deployment. MGN activates CBT on replicating VMs. You can deactivate CBT after cutover.
- The VM being replicated into AWS MGN must not contain any existing VMware snapshots.
- Once added to AWS MGN, snapshot-based replication will create snapshots on the replicated VM, which may result in slower disk performance.
- VMs with independent disks, Raw Device Mappings (RDM), or direct-attach disks (iSCSI, NBD) are not supported for replication into AWS MGN.
- The VM being replicated into AWS MGN can be either stopped or running. Changing the VM state during data replication will not affect data replication and will cause no data corruption.

AWS MGN vCenter Client installation instructions

To install the AWS MGN vCenter Client, follow these steps:

1. Download the AWS MGN vCenter Client installer onto a VM within your vCenter environment. You can download the client from this URL: [https://aws-application-migration-service-\(region\).s3.\(region\).amazonaws.com/latest/vcenter-client/linux/aws-vcenter-client-installer-init.py](https://aws-application-migration-service-(region).s3.(region).amazonaws.com/latest/vcenter-client/linux/aws-vcenter-client-installer-init.py) Replace (region) with the AWS Region into which you are replicating.

The following is an example of the installer link for us-east-1: <https://aws-application-migration-service-us-east-1.s3.us-east-1.amazonaws.com/latest/vcenter-client/linux/aws-vcenter-client-installer-init.py>

If you need to validate the installer hash, the correct hash can be found here: [https://aws-application-migration-service-hashes-\(region\).s3.\(region\).amazonaws.com/latest/vcenter-client/linux/aws-vcenter-client-installer-init.py.sha512](https://aws-application-migration-service-hashes-(region).s3.(region).amazonaws.com/latest/vcenter-client/linux/aws-vcenter-client-installer-init.py.sha512)

The following is an example of the installer hash link for us-east-1: <https://aws-application-migration-service-hashes-us-east-1.s3.us-east-1.amazonaws.com/latest/vcenter-client/linux/aws-vcenter-client-installer-init.py.sha512>

2. In command prompt, navigate to the directory where you downloaded the AWS MGN vCenter Client installer and run the installer with the following command: `sudo python3 aws-vcenter-client-installer-init.py`
3. The installer will prompt you for your credentials, enter the required info in each field and then press **Enter**:
 - AWS Access Key ID – Enter the AWS Access Key ID you generated in the previous section.
 - AWS Secret Access Key – Enter the AWS Secret Access Key you generated in the previous section.
 - AWS Region name – The AWS Region of your account (for example, eu-west-1).
 - The Private Link endpoint for AWS Application Migration Service (optional, leave blank if not using Private Link).
 - The VPC endpoint for S3 (optional, leave blank if not using a VPC endpoint).

4. The installer will then prompt you to enter your vCenter information, enter the required info in each field and then press **Enter**:

- vCenter IP or hostname
- vCenter port (press Enter to use the default TCP Port 443)
- vCenter username
- vCenter password
- Path to vCenter root CA certificate (optional) - To use SSL certificate validation, download the certificates from `https://<vcenter-ip>/certs/download.zip` (example: `wget https://<vcenter-ip>/certs/download.zip --no-check-certificate`) then enter the path of the certificate (example: `/usr/local/src/linux/f7f2bd6e.0`). Otherwise, press **Enter** to deactivate SSL certificate validation.

 **Note**

- The certificate must be located in a file that's readable to the vCenter client user, such as a shared directory. If the certificate is not located in a shared directory, you will see a permission error in the logs (Error 13).
- To use a certificate in your vCenter environment, you must setup a connection using a hostname. Using an IP will not work with a certificate.
- It's a security best practice to use certificates. Customers that do not use certificated authentication are responsible for any security issues that may arise.

- Path to VDDK tarball - Provide the path to the [VDDK tarball](#) you previously downloaded onto the VM. (example: `path/to/VMware-vix-disklib-7.0.3-21933544.x86_64.tar.gz`)
- Resource tags for the AWS vCenter client (optional) - Use the following format for tagging:

`KEY=VALUE [KEY=VALUE ...]` add resource tags to the AWS vCenter client; use a space to separate each tag (e.g., `--vcenter-client-tags tag1=val1 tag2=val2 tag3=val3`)

- Resource tags for source servers to be discovered by the AWS vCenter client (optional) - Use the following format for tagging:

`KEY=VALUE [KEY=VALUE ...]` add resource tags to the source servers added by discovery; use a space to separate each tag (e.g., `--vcenter-client-tags tag1=val1 tag2=val2 tag3=val3`)

5. The installer will proceed to download and install the AWS vCenter client and will register it with AWS Application Migration Service.
6. Once the AWS vCenter client has been installed, all of the VMs in your vCenter will be added to AWS Application Migration Service. The VMs will be added in the DISCOVERED state.

Note

- If you have a significant amount of VMs in your vCenter environment, it may take some time for all of the VMs to become visible in the AWS MGN Console.
- The MGN vCenter Appliance is excluded from the discovered servers list.

You can configure transparent proxy either by using an environment variable prior to the installation (Linux and Windows), or by using the `--proxy-address` flag in the Linux installer:

- Using the installer: `./aws-vcenter-client-installer-init.py --proxy-address http://PROXY:PORT/`
- Using environment variable: `export https_proxy=http://PROXY:PORT/; ./aws-vcenter-client-installer-init.py`

Make sure the proxy has a trailing forward slash.

Replicating servers from vCenter to AWS

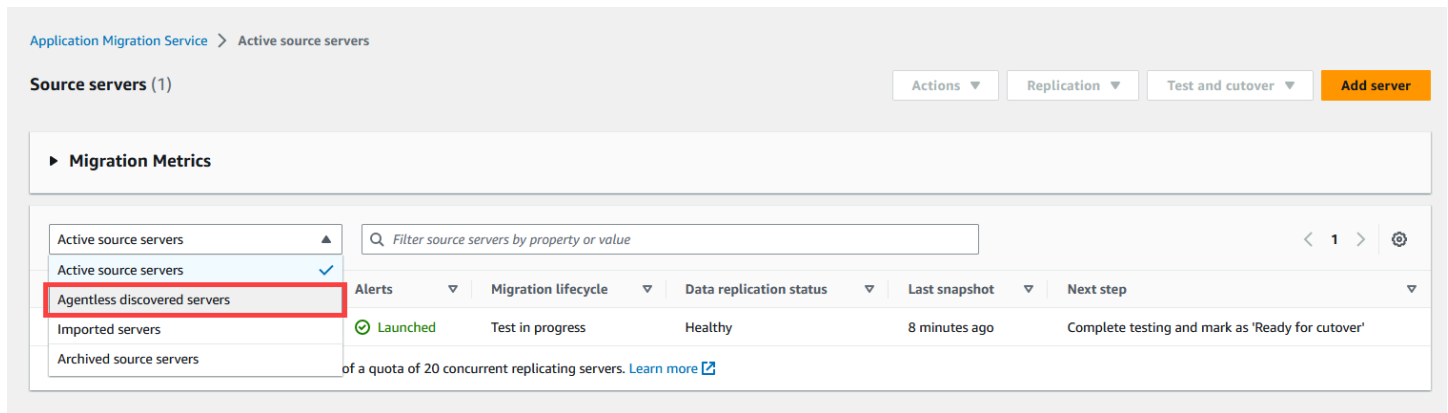
Once you have successfully installed the AWS vCenter client, all of your vCenter VMs will be added to AWS MGN in the DISCOVERED state. The DISCOVERED state means that the VM has not been replicated to AWS.

Note

VMware only sends data for up to 50 servers in parallel. Replicating more than 50 servers at once will cause the rest to be queued and will result in a longer wait.

By default, the MGN Console only shows active servers. You can tell which servers are being shown by looking at the filtering box under the main **Source servers** title.

To see your discovered non-replicating servers that have been added from vCenter, open the filtering menu and choose **Discovered source servers**.



You will now see all of your non-replicating DISCOVERED VMs.

To replicate one or more VMs into AWS, select the box to the left of each VM name, choose the **Replication** menu, and then choose **Start data replication**.

Choose **Start** on the **Start data replication for x servers** dialog.

The AWS MGN Console will indicate that data replication has started.

To view the data replication progress, open the filtering menu and return to the default **Active source servers** view.

You will now only see your replicating source servers. You can follow the launch process on the main **Source servers** view.

Once the VM has reached the **Ready for testing** state under **Migration lifecycle**, you can continue to [launch test and cutover instances](#) and perform all other regular AWS MGN operations on the server.

Updating the vCenter credentials

Users who want to change the vCenter credentials used by the AWS MGN appliance should follow these steps. This change requires root privileges on the appliance:

1. In the command prompt, navigate to the `aws-vcenter-client` directory:

```
cd /var/lib/aws-vcenter-client/1.1.7/
```

2. Run the vCenter configuration update tool with the following command:

```
sudo ./vcenter_configuration_update
```

3. The tool will receive flags or prompt you for your vCenter credentials. Provide the required info in each field and then press Enter:

- New vCenter username (--new-vcenter-user)
- New vCenter password (--new-vcenter-password)

4. The tool will verify the new vCenter credentials by attempting to connect to vCenter using them.

5. Upon successful connection to vCenter, the tool will save the new vCenter configuration and restart the necessary services.

6. In case of failure to connect to vCenter, the new credentials will not be stored, and the previous configuration will be retained. The following error message will be displayed:

```
Failed to connect to the vCenter endpoint using the new connection details. The configuration changes will not be applied.
```

Differentiating agentless and agent-based servers

You can differentiate an agentless vCenter VM that's replicating through snapshot shipping and an agent-based server (from any source infrastructure) through several ways:

1. On the **Source servers** page, under the **Replication type** column, the AWS MGN Console identifies the replication type, whether it is through **Snapshot shipping** (agentless) or **Agent based**.

Application Migration Service > Source Servers

Source Servers (3) Actions Replication Test and Cutover

Filter source servers by property or value

<input type="checkbox"/>	Hostname	Alerts	Replication type	Migration lifecycle	Data replication status	Last consistent snapshot	Next step
<input type="checkbox"/>	vm/	-	Snapshot shipping	Ready for testing	Transferring snapshot 100% No ETA yet	9/16/2021, 11:51:14 PM	Launch test instance.
<input type="checkbox"/>	vm,	-	Snapshot shipping	Not ready	Initiating	-	Wait for snapshot transfer to complete.
<input type="checkbox"/>	ip-	-	Agent based	Ready for testing	Healthy	9/22/2021, 12:25:09 PM	Launch test instance.

2. In the server details view, under the **Migration dashboard**, agentless servers that are replicated through snapshot shipping will have an additional **Lifecycle** step – **Not started**.

Migration dashboard | Server info | Tags | Disks settings | Replication Settings | Launch settings

Lifecycle Info

Not started | Not ready | Ready for testing | Test in progress | Ready for cutover | Cutover in progress | Cutover complete

Launch status: -

Last test: Job ID: -
Started: 9/14/2021, 4:51:48 PM

Cutover: -

3. Similarly, in the server details view, under the **Migration dashboard**, the **Data replication status** box will show the **Replication type** as **Snapshot shipping**.

Data replication status [Info](#)

Transferring snapshot

Replication progress 100%

Replication type
Snapshot shipping

Elapsed replication time
8 d

Total replicated storage
16 of 16 GiB

Last seen
9/16/2021, 11:51:13 PM

Backlog
-

Replication start time
9/14/2021, 12:50:56 PM

Last consistent snapshot
9/16/2021, 11:51:14 PM

Source servers page

The **Source servers** page lists all of the source servers that have been added to AWS Application Migration Service (AWS MGN). The **Source servers** page allows you to manage your source servers and perform a variety of commands for one or more servers (such as controlling replication and launching test and cutover instances). The **Source servers** page is the main page of AWS MGN console and you will most likely interact with AWS Application Migration Service predominantly through this page.

Application Migration Service > Source servers

Source servers (4) Actions ▾ Replication ▾ Test and cutover ▾ [Add server](#)

► Migration Metrics

Active source servers ▾ < 1 > ⚙

<input type="checkbox"/>	Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	25: ready_for_test	-	Ready for testing	Healthy	10 minutes ago	Launch test instance
<input type="checkbox"/>	11: not_ready (initiating)	-	Not ready	Initiating	-	Wait for initial sync to complete
<input type="checkbox"/>	26/ready_for_test	-	Ready for testing	Healthy	an hour ago	Launch test instance

Topics

- [Interacting with the source servers page](#)
- [Command menus](#)
- [Migration metrics](#)
- [Filtering](#)

Interacting with the source servers page

The **Source servers** page shows a list of source servers. Each row on the list represents a single server.

Application Migration Service > Source servers

Source servers (4) Actions Replication Test and cutover Add server

► Migration Metrics

Active source servers < 1 > ⌂

<input type="checkbox"/>	Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	25: ready_for_test	-	Ready for testing	Healthy	10 minutes ago	Launch test instance
<input type="checkbox"/>	11: not_ready (initiating)	-	Not ready	Initiating	-	Wait for initial sync to complete
<input type="checkbox"/>	26/ready_for_test	-	Ready for testing	Healthy	an hour ago	Launch test instance

The **Source servers** page provides key information for each source server under each of the columns on the page.

The columns include:

- **Selector column** – This blank checkbox selector column allows you to select one or more source servers. When a server is selected, you can interact with the server through the **Actions**, **Replication**, and **Test and cutover** menus. Selected servers are highlighted.
- **Source server name** – This column shows the unique server name for each source server.
- **Alerts** – This column shows whether any alerts exist for the server.
 - **No indication** – a healthy server for which a test or cutover instance has not been launched.
 - **Launched** – a healthy server for which a test of cutover instance has been launched.
 - **A clock icon with a warning message** – a server that is experiencing a temporary issue such as lag or backlog
 - **A red x and message** – a server that is experiencing significant issues, such as a stall.
- **Replication type** – This column identifies whether the server is being replicated through the default **Agent based** replication or through **Snapshot shipping**. [Learn more about agentless based snapshot shipping replication for vCenter.](#)
- **Migration lifecycle** – This column shows the migration lifecycle state for each source server. This way you can easily know which lifecycle step the server is undergoing. Migration lifecycle steps include the following: [Learn more about Migration lifecycle steps.](#)
 - **Not ready**
 - **Ready for testing**

- **Test in progress**
- **Ready for cutover**
- **Cutover in progress**
- **Cutover complete**
- **Disconnected**
- **Data replication status** – This column shows the current status of data replication for the server. The information presented in this column changes based on the server's Migration lifecycle state and whether the server is experiencing any issues.

This column will show a variety of information, including:

- **Not Started** – Data replication has not started.
- **Paused** – Data replication has been paused.
- **Healthy** – The server is healthy and ready for Test or Cutover instance launch.
- **Done** – The server has been successfully cutover and data replication has been stopped as a result.
- **Percentage complete** – The percentage of the server's storage that was successfully replicated if the server is undergoing initial sync or a rescan.
- **Lag** – Whether server is experiencing any lag. If it is; the lag time is indicated.
- **Backlog** – Whether there is any backlog on the server (in MiB).
- **Last snapshot** – This column shows the time the last consistent snapshot was taken of the source server. Servers that are still in the initial sync process and those that have been disconnected will not show any info in this field. Healthy servers will show a recent snapshot. Unhealthy servers' last snapshot indicates the last time they were healthy.
- **Next step** – This column shows the next step that needs to be undertaken in order to successfully complete a cutover for the server. The information presented in this column changes based on the server's Migration lifecycle state and whether the server is experiencing any issues.

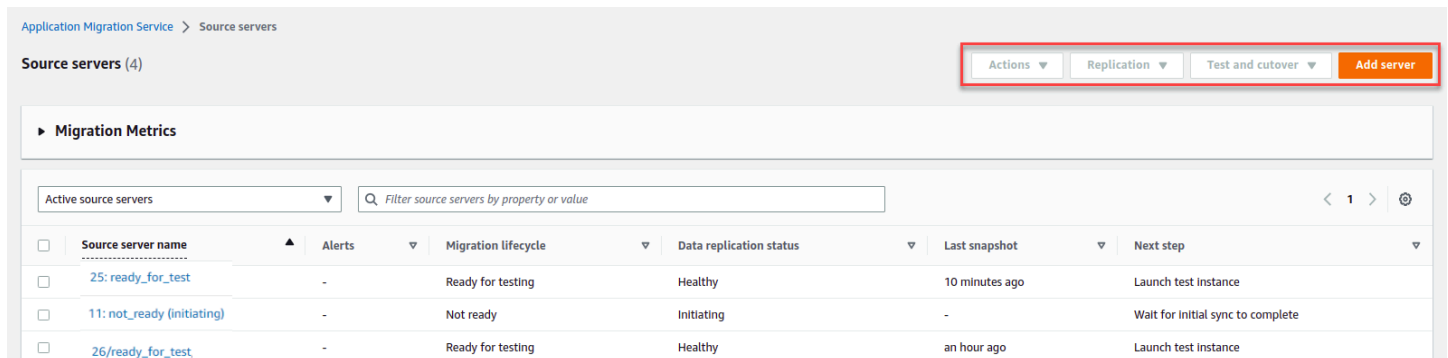
This column will show a variety of next steps, including:

- **Wait for initial sync to complete** – Data replication is initiating for the server. Wait for the initial sync process to complete.
- **Start data replication** – Data replication has not been started or is paused.
- **Launch test instance** – The server is ready to launch a test instance.

- **Complete testing and mark as 'ready for cutover'** – The server has launched a Test instance that needs to be reverted or finalized.
- **Launch cutover instance** – The server had a Test instance launched and finalized and now is ready to launch a cutover instance.
- **Finalize cutover** – The server has launched a cutover instance that needs to be finalized.
- **Terminate launched instance, Launch cutover instance** – The server is ready for cutover. Terminate the launched Test instance and launch a cutover instance.
- **Resolve cause of stalled data replication** – The server is experiencing significant issues such as a stall that need to be addressed.
- **Wait for lag to disappear, then X.** – The server is experiencing a temporary lag. Wait for the lag to disappear and then perform the indicated action.
- **Mark as archived** – The server has been successfully cut over and can now be archived.

Command menus

You can perform a variety of actions, add servers, control data replication, and manage your testing and cutover for one or more source servers through the command menu buttons on the **Source servers** page.



Application Migration Service > Source servers

Source servers (4)

Migration Metrics

Active source servers < 1 > ⌂

<input type="checkbox"/>	Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	25: ready_for_test	-	Ready for testing	Healthy	10 minutes ago	Launch test instance
<input type="checkbox"/>	11: not_ready (initiating)	-	Not ready	Initiating	-	Wait for initial sync to complete
<input type="checkbox"/>	26/ready_for_test	-	Ready for testing	Healthy	an hour ago	Launch test instance


Add a source server

To add a server, simply click **Add server**.

To run a variety of commands on your source servers, select one or more servers and choose the **Actions**, **Replication**, or **Test and cutover** menu.

The **Add servers** prompt will open, allowing you to create a custom installation command by taking the following steps:

- 1. Select your operating system. The installation command is different for Windows and Linux

 **Note**

If you want to install the AWS Replication Agent on a legacy Windows OS (Windows Server 2003, Windows Server 2008 or Windows Server 2008 R2), you must choose the **Legacy OS: Windows Server 2003 or Windows Server 2008** box. This will download a unique version of the AWS Replication Agent installer that is only valid for legacy Windows OSs (`AwsReplicationWindowsLegacyInstaller.exe`). **Do not** use this installer file to install the agent on any other OS types.

- 2. Select your replication preferences for the source server. The selected preferences will be added as installation prompts to the custom installation command that will be generated by this form.

Choose the **Replicate all disks** option to replicate all of the disks of the source server. This is the default option. This option adds the `--no-prompt` prompt to the installation command.

Select the **Choose which disks to replicate** option to choose which specific disks you want to replicate. You will be prompted to select which disks to replicate during agent installation.

- 3. Enter the credentials [you previously generated for AWS Replication Agent installation](#). The form will not send the secret, but will add it to the installation command.
- 4. If you are adding a Windows source server to AWS MGN, download the installer onto the source server. The installer will be downloaded from the AWS Region of your account. If you're adding a Linux source server, skip this step.
- 5. Copy the generated custom installation command and either input it into the command line on your source server. Proceed with [AWS Replication Agent installation as instructed in the documentation](#).

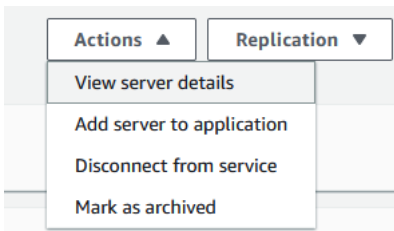
To run a variety of commands on your source servers, select one or more servers and choose the **Actions**, **Replication**, or **Test and cutover** menu.

Topics

- [Actions menu](#)
- [Replication menu](#)
- [Test and cutover menu](#)

Actions menu

The **Actions** menu allows you to perform the following actions:



- **View server details** – Choose this option to see the server details view for the selected server. This option is only available when a single server is selected.
- **Add server to application** – Choose this option to easily add servers to an application.
- **Disconnect from service** – Choose this option to disconnect the selected server from Application Migration Service and AWS. This option should be used when data replication is complete.

On the **Disconnect X server/s from service** dialog, choose **Disconnect**.

⚠ Important

This will uninstall the AWS Replication Agent from the source server and data replication will stop for the source server. If you need to restart data replication for this server, you will need to reinstall the agent. This action will not affect any test or cutover instances that have been launched for this source server, but you will no longer be able to identify which source servers your Amazon EC2 instances correspond to.

- **Mark as archived** – Choose this option in order to archive the server. You should only archive servers for which you have already performed a cutover. Archived servers will be removed from the main **Source servers** page, but can still be accessed through filtering options.

On the **Archive X servers** dialog, select **Archive**.

To see your archived servers, open the **Preferences** menu by choosing the gear button.

Select the **Show only archived servers** option and click **Confirm**.

You will now be able to see all of your archived servers. Unselect this option to see your non-archived servers.

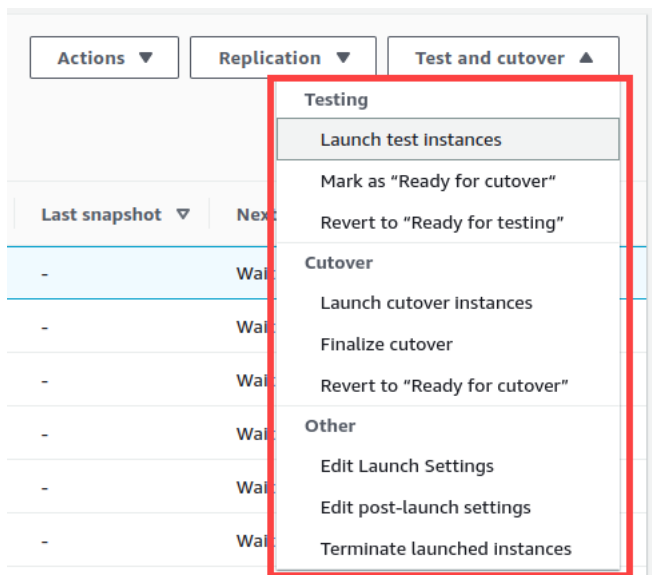
Replication menu

The Replication menu allows you to manage data replication for the source server through the following actions:

- **Edit replication settings** – Choosing the **Edit replication settings** option will redirect you to the **Replication settings** tab, where you can edit the specific replication settings for the selected source server. [Learn more about editing replication settings.](#)
- **Start data replication** – To start data replication for a source server on which data replication has previously been stopped, you can now restart replication using the "start option". you don't necessarily have to reinstall the agent.
- **Stop data replication** – To stop data replication for a source server, select the "stop data replication" option from the replication button. Stopping the replication will stop billing, delete existing snapshots, EBS volumes and will terminate replication servers. Configuration will be retained, and the agent will not be uninstalled.
- **Pause data replication** – To pause data replication for a source server, select the "pause data replication" option from the replication button. Pausing the replication, will not stop billing, or delete existing snapshots or EBS volumes. Replication servers will not be terminated and the agent will not be uninstalled from the source server.
- **Resume data replication** – To resume data replication for a source server, select the "resume data replication" option from the replication button. Selecting the resume action on a source server in paused state will sync any changes since the last synchronization and complete the data replication flow.

Test and cutover menu

The **Test and cutover** menu allows you to manage your test and cutover instances. For a more in-depth step-by-step guide to launching test and cutover instances, see the [Launching test and cutover instances documentation.](#)



- **Launch test instances** – Choose this option to launch a test instance for this server.

When the **Launch test instances for X servers** dialog will appears, cick **Launch** to begin the test.

The AWS Application Migration Service Console will indicate **1 launch job complete** after the test has been completed successfully.

- **Mark as "Ready for cutover"** – Use this option to finalize testing for this server after you have completed all of the necessary tests in preparation for cutover.

When the **Mark X servers as "Ready for cutover"** dialog appears, select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Continue**.

The AWS Application Migration Service Console will indicate that testing has been finalized. The selected source servers' **Migration lifecycle** column will show the **Ready for cutover** status and the launched Test instances will be deleted if that option was selected.

- **Revert to "ready for testing"** – Choose this option to revert a finalized test for this server if you want to run further tests prior to initiating a cutover.

The **Revert testing for X servers** dialog will appear. Select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Revert**.

The AWS Application Migration Service Console will indicate that testing has been reverted. The selected source servers' **Migration lifecycle** column will show the **Ready for testing** status and the launched Test instances will be deleted if that option was selected.

- **Launch cutover instances** – Choose this option to launch a cutover instance for this server after you have finalized all of your testing and are ready to initiate a cutover.

The **Launch cutover instances for X servers** dialog will appear. Choose **Launch** to begin the cutover.

The AWS Application Migration Service Console will indicate **1 launch job complete** after the cutover has been completed successfully.

This will change your source servers' **Migration lifecycle** status to **Cutover in progress**, indicating that the cutover is in progress but has not yet been finalized.

- **Finalize cutover** – Choose this option to finalize the cutover for this server after you have successfully performed a cutover.

This will change your source servers' **Migration lifecycle** status to **Cutover complete**, indicating that the cutover is complete and that the migration has been performed successfully. In addition, this will stop data replication and cause all replicated data to be discarded. All AWS resources used for data replication will be terminated.

The **Finalize cutover for X servers** dialog will appear. Choose **Finalize**.

The AWS Application Migration Service Console will indicate **X servers cutover. Data replication has been stopped for servers** once the cutover has been completed successfully. The AWS Application Migration Service Console will automatically stop data replication for the cutover source servers in order to save resource costs. The selected source servers' **Migration lifecycle** column will show the **Cutover** status, the **Data replication** column will show **Disconnected** and the **Next step** column will state **Mark as archived**. The source servers have now been successfully migrated into AWS and can be archived.

Note

This action does not uninstall the AWS Replication Agent from the source server. Use the **Disconnect from service** option under the **Actions** menu when you have completed the migration and want to uninstall the agent from your source server.

- **Revert to "ready for cutover"** – Choose this option to revert a finalized cutover for this server if you encounter any issues or want to reverse the cutover for any reason.

This will revert your source servers' **Migration lifecycle** to the **Ready for cutover** status, indicating that these servers have not undergone cutover.

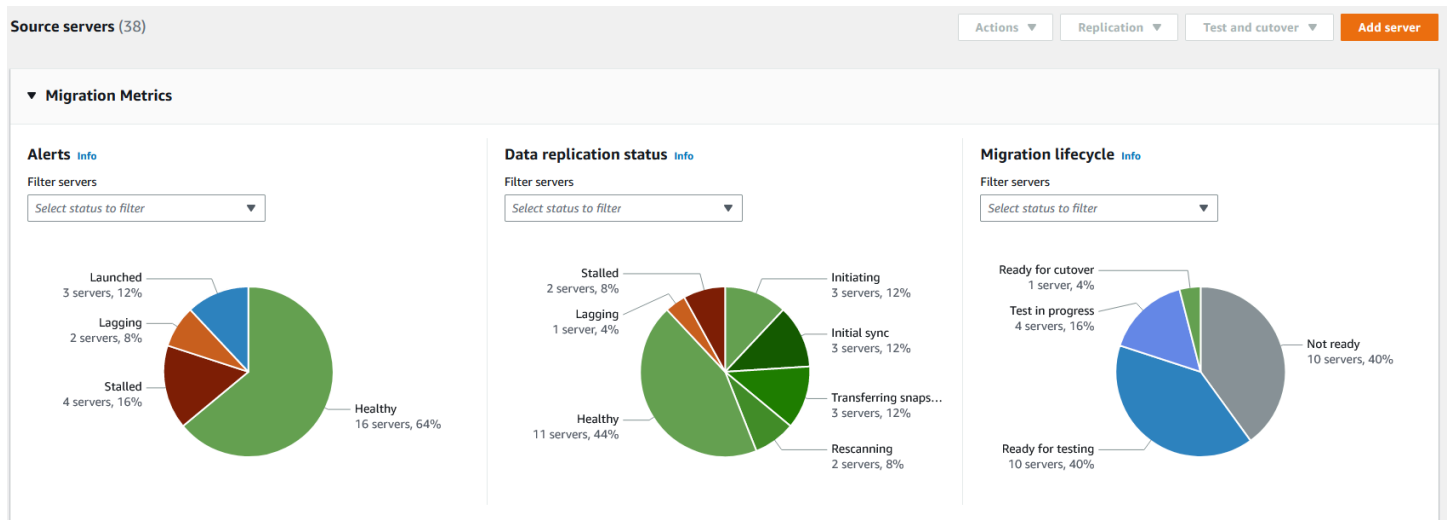
The **Revert cutover for X servers** dialog will appear. Click **Revert**.

- **Edit launch settings** – Use this option to edit the launch settings for this server. You will be redirected to the **Edit launch settings** page. [Learn more about launch settings.](#)
- **Edit post-launch settings** – Use this option to edit the post-launch settings for the selected source server or group of source servers. [Learn more about post-launch settings.](#)
- **Terminate launched instance** – Choose this option if you want to delete your test or cutover instance for any reason at any time. It can only be selected for a server that has a launched test or cutover instance.

When the **Terminate launched instance** dialog appears, click **Terminate**.

Migration metrics

The source server migration metrics present an aggregated overview of your source servers, focused on three topics: **Alerts**, **Data replication status**, and **Migration status**.



Topics

- [Alerts](#)
- [Data replication status](#)
- [Migration lifecycle](#)

Alerts

The source server **Alerts** migration metric presents an aggregated overview of the application associated servers alerts. You can look up an individual source server's **Alerts** in the **Source servers** table at the bottom of the page.



- A healthy server for which a test or cutover instance has not been launched will display a **Healthy** status.
- A healthy server for which a test of cutover instance has been launched will display a **Healthy** status.
- A server that is experiencing a temporary issue such as lag or backlog will display a **Lagging** status.
- A server that is experiencing significant issues, such as a stall, will display a **Stalled** status.

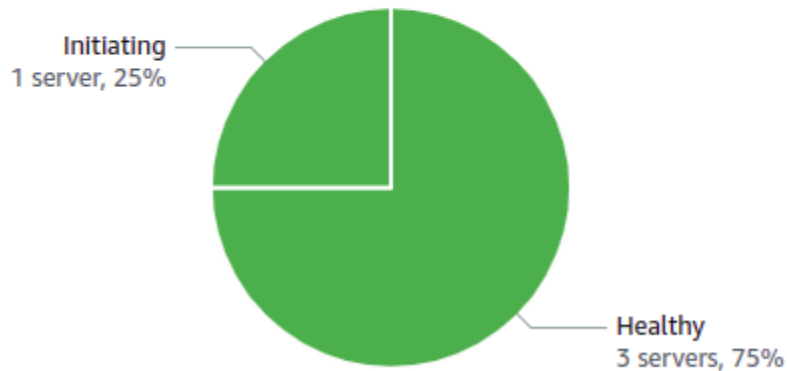
Data replication status

The source server **Data replication status** migration metric presents an aggregated overview of the your source servers' data replication status. You can look up an individual source server's **Data replication status** status in the **Source servers** table at the bottom of the page.

Data replication status [Info](#)

Filter servers

Select status to filter ▼



Source server **Data replication status** can have one of the following values:

- **Transferring snapshot**
- **Initial sync**
- **Finalizing sync**
- **Lagging**
- **Healthy**
- **Stalled**
- **Rescanning**
- **Not started**
- **Initiating**
- **Creating snapshot**
- **Paused**
- **Disconnected**

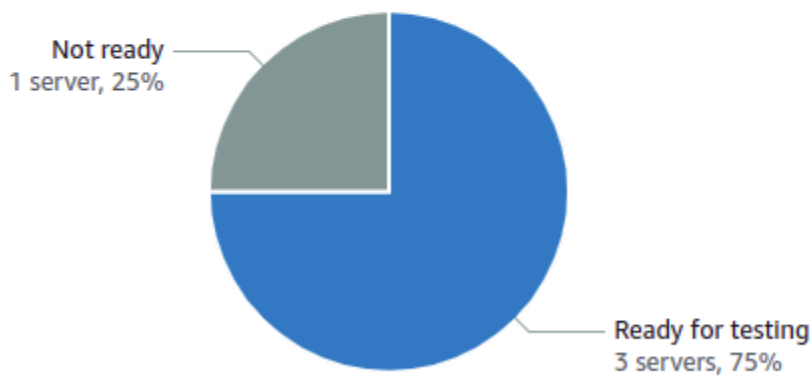
Migration lifecycle

The source server **Migration lifecycle** metric shows an aggregated overview of your source servers' migration lifecycle. You can look up an individual source server's **Migration lifecycle** status in the **Source servers** table at the bottom of the page.

Migration lifecycle [Info](#)

Filter servers

Select status to filter ▼



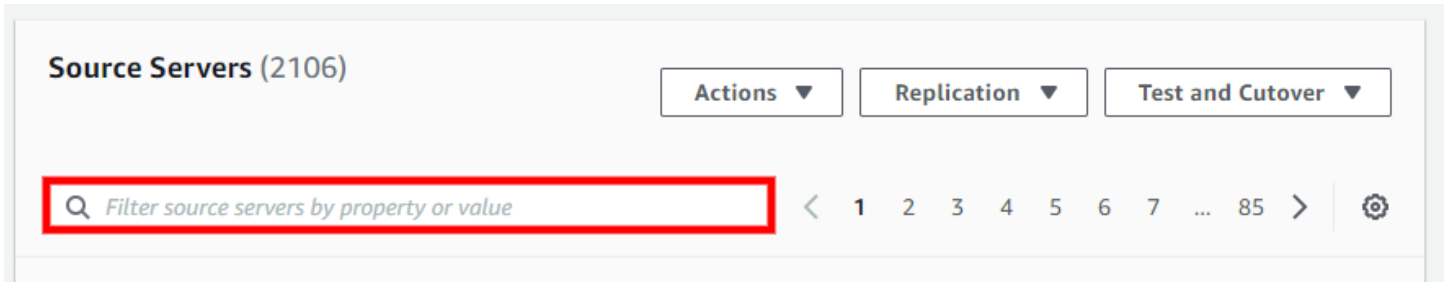
Source server **Migration lifecycle** can have one of the following values:

- **Stopped**
- **Not ready**
- **Ready for testing**
- **Test in progress**
- **Ready for cutover**
- **Cutover in progress**
- **Cutover complete**
- **Disconnected**
- **Discovered**

Filtering

You can customize the **Source servers** page through filtering. Filtering allows you to easily filter your servers by one or multiple properties.

Click within the **Filter servers** field and choose the filtering property from the **Properties** menu.



You can filter by a variety of properties, including:

- Alerts – Filter by specific alert (lagging, stalled, launched).
- Hostname – Filter by a specific hostname or a specific string of characters.
- Migration lifecycle – Filter by the migration lifecycle state.
- Data replication status – Filter by the data replication status.
- Next step – Filter by next step.
- SourceServerID – Filter by specific source server ID or string.
- Tags – Filter by tags. Relevant specific tag values will appear under the **Tags** category. Choose the value to filter by.

You can filter by multiple properties at once in order to narrow down your results.

Here you see an example of filtering the source servers list by several properties:

Application Migration Service > Source servers

Source servers (38) Actions Replication Test and cutover

Active source servers 2 matches < 1 >

Alerts: Lagging and Migration lifecycle: Ready for testing Clear filters

<input type="checkbox"/>	Source server name	Alerts	Replication type	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	24: ready_for_test (lagging)	Lagging	Agent based	Ready for testing	Lag 2 hr 74 min left	a day ago	Wait for lag to disappear, then launch test instance
<input type="checkbox"/>	23: ready_for_test (rescan)	Lagging	Agent based	Ready for testing	Rescanning 18% left	a day ago	Wait for lag to disappear, then launch test instance

Choose **Clear filters** to clear the current filtering properties selected.

Server details

You can access the server details view by clicking on the **Source server name** of any server on the **Source servers** page.

Source servers (38) Actions Replication Test and cutover

Active source servers < 1 >

<input type="checkbox"/>	Source server name	Alerts	Replication type	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	31: testing	-	Agent based	Test in progress	Healthy	a day ago	Complete testing and mark as 'Ready for cutover'

You can also access the server details view by checking the box to the left of any single source server on the **Source servers** page and choosing **Actions > View server details**.

Source servers (38) Actions Replication Test and cutover

Active source servers < 1 >

Actions View server details Disconnect from AWS Mark as archived

<input type="checkbox"/>	Source server name	Alerts	Re ty	lifecycle	Data replication status
<input checked="" type="checkbox"/>	31: testing	-	Agent based	Test in progress	Healthy

The server details view shows information and options for an individual server. Here, you can fully control and monitor the individual server.

You can also perform a variety of actions, control replication, and launch test and cutover instances for the individual server from the server details view.

The **Next actions** box serves as a helpful guide to the state of the server and the next steps you need to take in order to complete the migration process for the server.

The server details view is divided into several tabs, including:

- Migration dashboard
- Server info

- [Tags](#)
- [Disk settings](#)
- [Replication settings](#)
- [Launch settings](#)

Topics

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

Migration dashboard

Application Migration Service > Active source servers > ip-

ip- Actions ▾ Replication ▾ Test and cutover ▾ Add server

Next actions [Info](#)

Launch test instance

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	Post-launch actions status	Last test	Cutover
-	Actions completed ✔ All actions succeeded	Job ID: mgnjob-0b68928f4cfe3ffdb Started: 26 February 2023 at 16:23 (UTC+2:00)	-

Data replication status [Info](#)

Healthy

Replication progress	Replication type	Elapsed replication time
✔ Initial replication finished	Agent based	8 d
	Total replicated storage	Last seen
	8 of 8 GiB	27 February 2023 at 14:40 (UTC+2:00)
	Lag	Replication start time
	-	19 February 2023 at 16:45 (UTC+2:00)
	Backlog	
	-	

Post-launch actions (2) [Info](#)

Name	Execution status	Start time	End time	Details	Link
SSM Agent installed	✔ Succeeded	26 February 2023 at 16:36 (UTC+2:00)	26 February 2023 at 16:36 (UTC+2:00)	-	Troubleshooting FAQ
DR after migration	✔ Succeeded	26 February 2023 at 16:38 (UTC+2:00)	26 February 2023 at 16:38 (UTC+2:00)	-	View in DR5

Events and metrics [🔗](#)

[View AWS CloudTrail event history](#)

The **Migration dashboard** tab allows you to monitor the server in relation to the migration lifecycle.

Here, you can see the lifecycle state the source server is currently on, a detailed view of the data replication status, and any events that the source server has undergone (in AWS CloudTrail). You

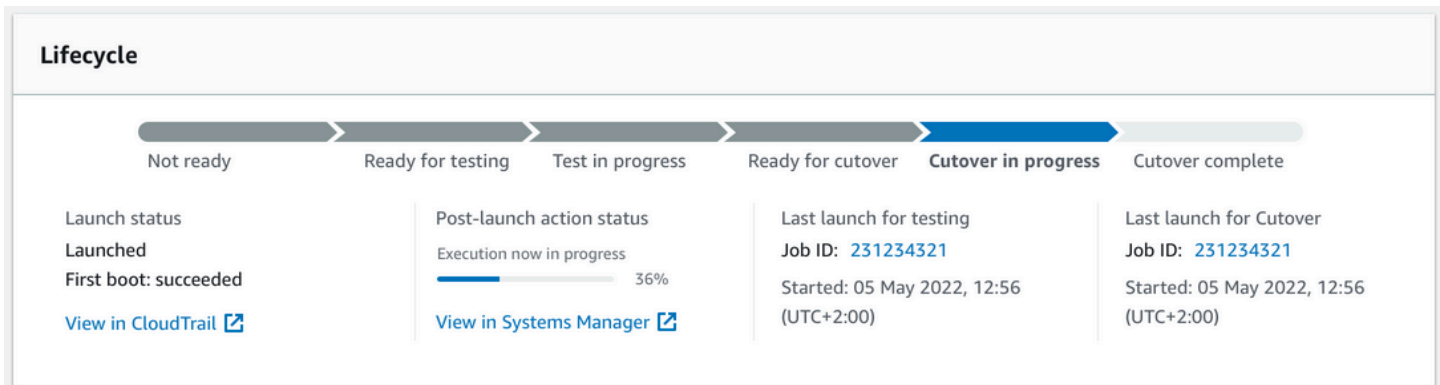
can use the Migration dashboard to monitor the status of your source server and to troubleshoot migration and data replication issues.

Topics

- [Lifecycle](#)
- [Data replication status](#)
- [Post-launch actions](#)
- [Events and metrics](#)
- [Server actions and replication control](#)

Lifecycle

The **Lifecycle** view shows the current state of each server within the migration lifecycle.



Lifecycle states include:

- **Not ready** – The server is undergoing the Initial Sync process and is not yet ready for testing. Data replication can only commence once all of the Initial Sync steps have been completed.
- **Ready for testing** – The server has been successfully added to AWS Application Migration Service and data replication has started. Test or cutover instances can now be launched for this server.
- **Test in progress** – A test instance is currently being launched for this server.
- **Ready for cutover** – This server has been tested and is now ready for a cutover instance to be launched.
- **Cutover in progress** – A cutover instance is currently being launched for this server.
- **Cutover complete** – This server has been cutover. All of the data on this server has been migrated to the cutover instance.

The lifecycle always displays the **Launch status**, **Last test**, and **Cutover status** for each server that has undergone these stages.

Topics

- [Not ready](#)
- [Ready for testing](#)
- [Test in progress](#)
- [Ready for cutover](#)
- [Cutover in progress](#)
- [Cutover complete](#)

Not ready

The **Not ready** lifecycle state represents several possible scenarios:

Topics

- [Server undergoing initial sync](#)
- [Unable to complete initiation](#)

Server undergoing initial sync

A source server that has been added to AWS Application Migration Service will automatically begin the initial sync process after AWS Replication Agent installation.

Data replication can only commence after all of the initial sync steps have been completed. The server will be in the **Not ready** lifecycle state until initial sync has been successfully completed.

Initial sync steps include:

- Initiation
 - Creating firewall rules
 - Creating replication server
 - Booting replication server
 - Resolving Service Manager address
 - Authenticating with the Service Manager
 - Downloading replication software

- Creating staging disks
- Pairing replication server with agent
- Establishing communication between AWS Replication Agent and replication server
- Sync (0% to 100%)
- Flush backlog (if any)
- Create first launchable snapshot

You can review the overall progress of the Initial Sync process under the **Data replication status** view.

It provides the percentage of completion, the time left until initial sync is finished, and whether there are any issues (such as a stall).

You can tell that a server has successfully completed the initial sync process through several indicators on the main **Source servers** page as well as on the **Migration dashboard** tab for an individual server.

On the main **Source servers** page, a newly added server that has completed initial sync for the first time will show **Ready for testing** under the **Migration lifecycle** column and **Healthy** under the **Data replication status** column.

On the individual server view, under the **Migration dashboard** tab, the **Lifecycle** section will show the **Ready for testing** status. The **Data replication status** section will show the **Healthy** status.

Note

Servers will automatically undergo initial sync every time there is a network disconnect.

Unable to complete initiation

The server will be in the **Not ready** Lifecycle state until Initial Sync has been successfully completed.

If the Initial Sync process is stalled for any reason, the **Data replication status** section will indicate that replication has stalled.

Scroll down to the Replication initiation steps to see the step on which the error occurred. The step on which initial sync failed will be marked with a red "x".

You must fix the indicated issue before the initial sync process can continue. You will not be able to migrate your server and the server will remain in the **Not ready** state until the issue is resolved.

Each step has unique troubleshooting methods.

Ready for testing

Once the server has successfully completed the Initial Sync process, it will enter the **Ready for testing** lifecycle state.

The **Data replication status** box will show a **Healthy** state, indicating that the server is healthy.

You can now launch a test instance for this server. The server will stay in the **Ready for testing** lifecycle state until you launch a Test instance for the server.

Test in progress

Once you have launched a Test instance for your server, the migration dashboard will show the **Test in progress** lifecycle state.

Within the **Lifecycle** box, you can review the **Launch status** and **Last test** information fields for the test instance.

- The **Launch status** field will show the time of the test instance launch. While the Testing instance is being launched, the **Launch status** field will show **Waiting**.
- Once the test instance has been launched, the Launch status will show **Launched**. Wait for the instance to boot and then choose **View in EC2 console** link to open the EC2 Console in a new tab, in order to view and monitor your launched test instance.
- The AWS EC2 Console will open in a new tab and will automatically search for and display your test instance.
- The **Last test** field will show the date of the last test. To review the test launch details, click **Job ID**, which will open the job within the **Launch History** page in a new tab.
- On the main **Source servers** page, the **Migration lifecycle** column will show **Ready for testing** and the **Next step** column will show **Launch test instance**.
- The server will stay in the **Test in progress** Lifecycle state until you finalize your testing and mark the server as **Ready for cutover**.

You can use the following indicators to verify that your test instance was successfully launched::

- On the **Server Details > Lifecycle** pane, the Launch status will state **Launched**.
- On the main **Source servers** page, the **Alerts** column will show the **Launched** status.

Ready for cutover

After you have finalized your testing, the Migration dashboard will show the **Ready for cutover** lifecycle state.

- The **Launch status** field will show the time of the last test instance launch. Click on the **View in EC2 console** link to open the EC2 Console in a new tab in order to view and monitor your launched Test instance.
- The **Last test** field will show the date the last test was started. You can review the test launch details by clicking on the **Job ID**. This will open the relevant Job.
- The **Cutover** field will show the date of the last cutover instance launch, if applicable. You can review the cutover launch details by clicking on the **Job ID**. This will open the relevant Job.
- On the **Source servers** page, the **Migration lifecycle** column will show **Ready for cutover** and the **Next step** column will show **Terminate test instance; Launch cutover instance**.

The server will stay in the **Ready for cutover** Lifecycle state until you launch a cutover instance.

Cutover in progress

Once you have launched a cutover instance for your server, the Migration dashboard will show the **Cutover in progress** Lifecycle state.

- The **Launch status** field will show the last time of cutover launch. Click on the **View in EC2 console** link to open the EC2 Console in a new tab in order to view and monitor your launched cutover instance.
- The **Last test** field will show the date the last test was started. You can review the test launch details by clicking on the **Job ID**. This will open the Job.
- The **Cutover** field will show the date of the last cutover instance launch. You can review the cutover launch details by clicking on the **Job ID**. This will open the Job.
- On the **Source servers** page, the **Migration lifecycle** column will show **Cutover in progress** and the **Next step** column will show **Complete the cutover**.

The server will stay in the **Cutover in progress** Lifecycle state until you complete the cutover.

Cutover complete

Once you have completed your cutover instance launch for your server, the Migration dashboard will show the **Cutover complete** lifecycle state. This is the final state in the migration lifecycle. This state indicates that you have successfully migrated your source server to AWS.

- The **Launch status** field will show **Launched**. Click on the **View in EC2 console** link to open the EC2 Console in a new tab in order to view and monitor your launched cutover instance.
- The **Last test** field will show the date the last test was started. You can review the test launch details by clicking on the **Job ID**. This will open the Job.
- The **Cutover** field will show the date you finalized your Cutover instance launch. You can review the cutover launch details by clicking on the **Job ID**. This will open the Job.
- The AWS Application Migration Service Console will automatically stop data replication for the source servers that were cutover in order to save resource costs.
- On the **Source servers** page, the selected source servers' **Migration lifecycle** column will show the **Cutover complete** status, the **Data replication status** column will show **Disconnected** and the **Next step** column will show **Mark as archived**.

The lifecycle also shows the status of any post-launch actions for the server. [Learn more about post-launch actions.](#)

Data replication status

The **Data replication status** section provides an overview of the overall source server status, including:

Data replication status [Info](#)

Healthy

Replication progress



Total replicated storage

16 of 16 GiB

Elapsed replication time

3 min

Lag

-

Last seen

3/25/2021, 11:32:32 AM

Backlog

1.54 GiB

Replication start time

1/4/2020, 7:38:00 PM

- **Replication progress** – The percentage of the server's storage that was successfully replicated.
- **Rescan progress** – The percentage of the server's storage that was rescanned (in the event of a rescan)
- **Total replicated storage** – The total amount of storage replicated (in GiB).
- **Lag** – Whether the server is experiencing any lag. If it is - the lag time is indicated.
- **Backlog** – Whether there is any backlog on the server (in MiB)
- **Elapsed replication time** – Time elapsed since replication first began on the server.
- **Last seen** – The last time the server successfully connected to AWS Application Migration Service.
- **Replication start time** – The date and time replication first began on the server.

Data replication can be in one of several states, as indicated in the panel title:

- **Initial sync:** initial copying of data from external servers is not done. Progress bar and **Total replicated storage** fields will indicate how far along the process is.
- **Healthy:** all data has been copied and any changes at source are continuously being replicated (data is flowing).
- **Rescan:** an event happened that forced the agent on the external server to rescan all blocks on all replicated disks (same as initial sync but faster because only changed blocks need to be copied; a rescan progress bar will also appear).
- **Stalled:** data is not flowing and user intervention is required (either initial sync will never complete, or state at source will become further and further the state at AWS). When the state is stalled, then the replication initiation checklist is also shown, indicating where the error occurred that caused the stalled state.

This panel also shows:

- **Total replicated storage:** size of all disks being replicated for this source server, and how much has been copied to AWS (once initial sync is complete)
- **Lag:** if you launch a recovery instance now, how far behind will it be from state at source. Normally this should be none.
- **Backlog:** how much data has been written at source but has not yet been copied to AWS. Normally this should be none.

- **Last seen:** when is the last time the AWS Replication Agent communicated with the AWS DRS service or the replication server.

If everything is working as it should and replication has finished initializing, the Data replication progress section will show a **Healthy** status.

Data replication status [Info](#)

Healthy


<p>Replication progress</p> <div style="display: flex; align-items: center;"> <div style="width: 100%; height: 10px; background-color: #0070c0; margin-bottom: 5px;"></div> 100% </div>	<p>Total replicated storage</p> <p>16 of 16 GiB</p> <p>Lag</p> <p>-</p> <p>Backlog</p> <p>1.54 GiB</p>	<p>Elapsed replication time</p> <p>3 min</p> <p>Last seen</p> <p>3/25/2021, 11:32:32 AM</p> <p>Replication start time</p> <p>1/4/2020, 7:38:00 PM</p>
---	--	---

If there are initialization, replication, or connectivity errors, the **Data replication status** section will show the cause of the issue (for example, a stall).

Data replication status [Info](#)


Stalled

<p>Replication progress</p> <div style="display: flex; align-items: center;"> <div style="width: 100%; height: 10px; background-color: #c00000; margin-bottom: 5px;"></div> 92% </div>	<p>Total replicated storage</p> <p>14.7 of 16 GiB</p> <p>Lag</p> <p>-</p> <p>Backlog</p> <p>1.54 GiB</p>	<p>Elapsed replication time</p> <p>3 min</p> <p>Last seen</p> <p>3/25/2021, 11:32:32 AM</p> <p>Replication start time</p> <p>-</p>
--	--	--



Data replication stalled

Failed to connect AWS Replication Agent to Replication Server.

[How can I solve this?](#) 

If the error occurred during the initialization process, then the exact step during which the error occurred will be marked with a red "x" under **Replication initiation steps**.



Data replication stalled

Failed to connect AWS Replication Agent to Replication Server.

[How can I solve this?](#)

Replication initiation steps

	Last start time
✔ Create security groups	
✔ Launch Replication Server	3/25/2021, 11:34:32 AM
✔ Boot Replication Server	
	Next attempt time
✔ Authenticate with service	
✔ Download replication software	-
✔ Create staging disks	
✔ Attach staging disks	
⋮ Pair Replication Server with AWS Replication Agent	
✘ Connect AWS Replication Agent to Replication Server	
⌵ Start data transfer	

Post-launch actions

The **Post-launch actions** view shows the current execution status of post-launch actions.

The status includes:

- Name – the name of the action is a link to the detailed execution status in the [AWS Systems Manager](#) console.
- Execution status – provides the current action status.
- Start time – the start time of the execution of the action script. This column will be empty for actions that have not yet started execution.
- End time – the end time of the execution of the action script. This column will be empty for actions that have not yet completed execution.
- Details – error messages will be shown in this column.
- Link – used by the “DR after migration” action. Provides a link to the replicated server in the [AWS Elastic Disaster Recovery](#) console.

Post-launch actions (2) Info						
Name	Execution status	Start time	End time	Details	Link	
SSM Agent installed	✔ Succeeded	June 01, 2022, 10:37 (UTC+3:00)	June 01, 2022, 10:37 (UTC+3:00)	-	-	
DR after migration	✔ Succeeded	June 01, 2022, 10:42 (UTC+3:00)	June 01, 2022, 10:42 (UTC+3:00)	-	View in DRS	

Events and metrics

You can review AWS Application Migration Service events and metrics in AWS CloudTrail. Click on **View CloudTrail Event History** to open AWS CloudTrail in a new tab.

Events and metrics ↗
View CloudTrail event history

Learn more about [monitoring AWS MGN](#).

Learn more about AWS CloudTrail events in the [AWS CloudTrail user guide](#).

Server actions and replication control

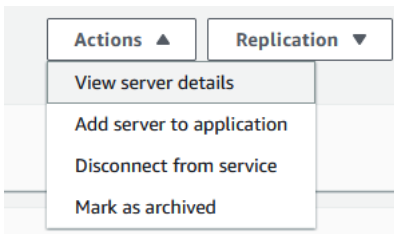
You can perform a variety of actions, control data replication, and manage your testing and cutover for an individual server from the server details view.

Topics

- [Actions menu](#)
- [Replication menu](#)
- [Test and cutover menu](#)
- [Alerts and errors](#)

Actions menu

The **Actions** menu allows you to perform the following actions:



- **Add servers** – Choosing the **Add servers** option will open the Add servers prompt, through which you can construct a custom installation command to use when adding Linux or Windows source servers.

Add servers

To add your source servers to this console, you need to install the AWS Replication Agent on them. Use the options below to construct the installation command, then copy the command and download the installer. [Learn more](#)

Agentless replication is available. [Learn more](#)

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. IAM access key ID [Info](#)


[Create IAM user](#)

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

[Show](#)
4. 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-eu-west-1.s3.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe.sha512>

To construct a custom installation command, take the following steps:

1. Select your operating system. The installation command is different for Windows and Linux.

 **Note**

If you want to install the AWS Replication Agent on a legacy Windows OS (Windows Server 2003, Windows Server 2008 or Windows Server 2008 R2), you must choose the **Legacy OS: Windows Server 2003 or Windows Server 2008** box. This will download a unique version of the AWS Replication Agent installer that is only valid for legacy Windows OSs (`AwsReplicationWindowsLegacyInstaller.exe`). **Do not** use this installer file to install the agent on any other OS types.

2. Select your replication preferences for the source server. The selected preferences will be added as installation prompts to the custom installation command that will be generated by this form.

Choose the **Replicate all disks** option to replicate all of the disks of the source server. This is the default option. This option adds the `--no-prompt` prompt to the installation command.

Select the **Choose which disks to replicate** option to choose which specific disks you want to replicate. You will be prompted to select which disks to replicate during agent installation.

3. Enter the credentials that [you previously generated for AWS Replication Agent installation](#). The form will not send the secret, but will add it to the installation command.
 4. If you have not yet obtained the necessary credentials, [follow these instructions](#).
 5. If you are adding a Windows source server to AWS MGN, download the installer onto the source server. The installer will be downloaded from the AWS Region of your account. If you're adding a Linux source server, skip this step.
 6. Copy the generated custom installation command and either input it into the command line on your source server. Proceed with [AWS Replication Agent installation as instructed in the documentation](#).
- **View server details** – Choosing this option to open the server details view for the selected server. This option is only available when a single server is selected.
 - **Disconnect from service** – Choose this option to disconnect the selected server from Application Migration Service and AWS. This option disconnects the source server and should be used when data replication is complete.

On the **Disconnect X server/s from service** dialog, choose **Disconnect**.

⚠ Important

This will uninstall the AWS Replication Agent from the source server and data replication will stop for the source server. If you need to restart data replication for this server, you will need to reinstall the agent. This action will not affect any test or cutover instances that have been launched for this source server, but you will no longer be able to identify which source servers your Amazon EC2 instances correspond to.

- **Mark as archived** – Choose this option to archive the server. You should only archive servers for which you have already performed a cutover. Archived servers will be removed from the main **Source servers** page, but can still be accessed through filtering options.

On the **Archive X servers** dialog, select **Archive**.

To see your archived servers, open the **Preferences** menu by clicking the gear button. Select the **Show only archived servers** option and click **Confirm**. You will now be able to see all of your archived servers. Unselect this option to see your non-archived servers.

Replication menu

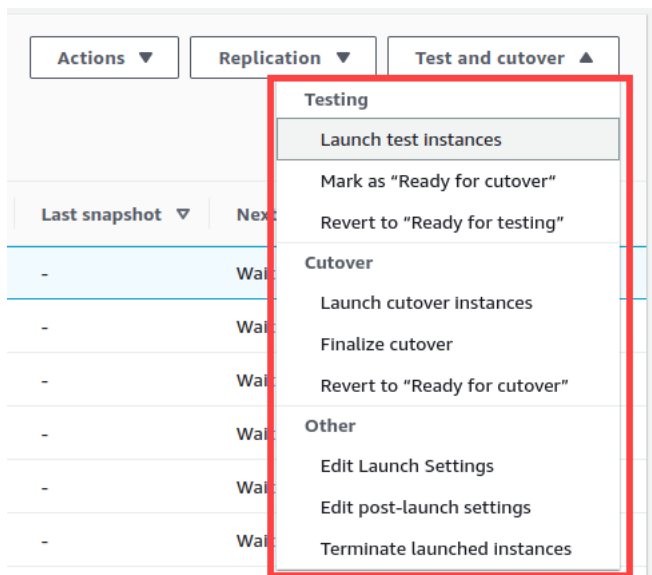
The Replication menu allows you to manage data replication for your source servers through the following actions:



- **Edit replication settings** – Choose this option to be redirected to the **Edit replication settings** page, where you can edit specific replication settings for the selected source server. [Learn more about editing replication settings.](#)

Test and cutover menu

The **Test and cutover menu** allows you to manage your test and cutover instances.



- **Launch test instances** – Choose this option to launch a test instance for this server.

When the **Launch test instances for X servers** dialog appears, click **Launch** to begin the test.

The AWS Application Migration Service Console will indicate **1 launch job complete** after the test has been completed successfully.

- **Finalize testing** – Choose the **Mark as "Ready for cutover"** option to finalize testing for this server after you have completed all of the necessary tests in preparation for cutover.

When the **Mark X servers as "Ready for cutover"** dialog appears, select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and click **Continue**.

The AWS Application Migration Service Console will indicate that testing has been finalized. The selected source servers' **Migration lifecycle** column will show the **Ready for cutover** status and the launched Test instances will be deleted if that option was selected.

- **Revert to "ready for testing"** – Choose this option to revert a finalized test for this server if you want to run further tests prior to initiating a cutover.

When the **Revert testing for X servers** dialog appears, select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Revert**.

The AWS Application Migration Service Console will indicate that testing has been reverted. The selected source servers' **Migration lifecycle** column will show the **Ready for testing** status and the launched Test instances will be deleted if that option was selected.

- **Launch cutover instances** – Choose this option to launch a cutover instance for this server after you have finalized all of your testing and are ready to initiate a cutover.

When the **Launch cutover instances for X servers** dialog appears, click **Launch** to begin the cutover.

The AWS Application Migration Service Console will indicate **1 launch job complete** after the cutover has been completed successfully.

This will change your source servers' **Migration lifecycle** status to **Cutover in progress**, indicating that the cutover is in progress but has not yet been finalized.

- **Finalize cutover** – Choose this option to finalize the cutover for this server after you have successfully performed a cutover.

This will change your source servers' **Migration lifecycle** status to **Cutover complete**, indicating that the cutover is complete and that the migration has been performed successfully. In addition, this will stop data replication and cause all replicated data to be discarded. All AWS resources used for data replication will be terminated.

When the **Finalize cutover for X servers** dialog appears, click **Finalize**.

The AWS Application Migration Service Console will indicate **X servers cutover. Data replication has been stopped for servers** once the cutover has been completed successfully. The AWS Application Migration Service Console will automatically stop data replication for the cutover source servers in order to save resource costs. The selected source servers' **Migration lifecycle** column will show the **Cutover** status, the **Data replication** column will show **Disconnected** and the **Next step** column will state **Mark as archived**. The source servers have now been successfully migrated into AWS and can be archived.

Note

This action does not uninstall the AWS Replication Agent from the source server. Use the **Disconnect from service** option under the **Actions** menu when you have completed the migration and want to uninstall the agent from your source server.

- **Revert to "ready for cutover"** – Choose this option to revert a finalized cutover for this server if you encounter any issues or want to reverse the cutover for any reason.

This will revert your source servers' **Migration lifecycle** to the **Ready for cutover** status, indicating that these servers have not undergone cutover.

When the **Revert cutover for X servers** dialog appears, click **Revert**.

- **Edit launch settings** – Use this option to edit the launch settings for this server. This will redirect you to the **Launch settings** tab. [Learn more about Launch settings.](#)
- **Terminate launched instance** – Choose this option if you want to delete your test or cutover instance for any reason at any time. This option can only be selected for a server that has a launched test or cutover instance.

When the **Terminate launched instance** dialog appears, click **Terminate**.

- **Edit post-launch settings** – Choose this option to edit the post-launch settings for the selected source server or group of source servers. [Learn more about post-launch settings.](#)

Alerts and errors

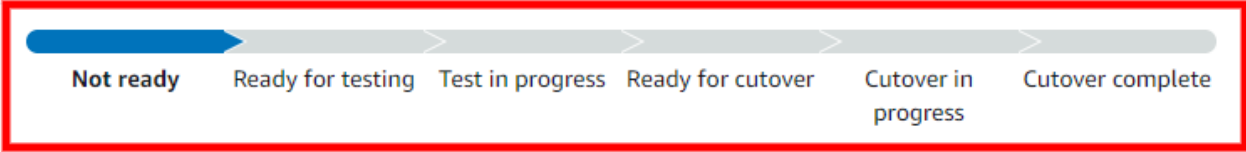
You can easily distinguish between healthy servers and servers that are experiencing issues on the **Migration dashboard** in several ways.

The entire AWS Application Migration Service Console is color-coded for ease of use.

Healthy servers with no errors are characterized by the color blue. Both the **Lifecycle** and **Data replication status** boxes will display all steps and information in blue if the server is healthy.

The following are examples of healthy servers:

Lifecycle [Info](#)



Launch status	Last test	Cutover
-	-	-

Data replication status [Info](#)

Healthy

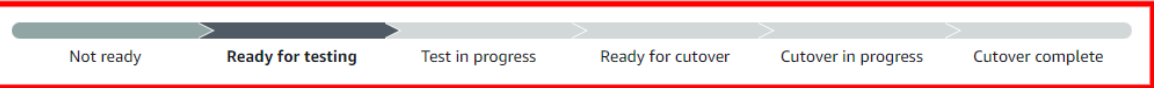
Replication progress	100%	Total replicated storage	16 of 16 GiB	Elapsed replication time	3 min
		Lag	-	Last seen	3/25/2021, 11:32:32 AM
		Backlog	1.54 GiB	Replication start time	1/4/2020, 7:38:00 PM

Servers that are experiencing temporary issues will be characterized by the color yellow. This can include issues such as lag or a rescan. These issues will not break replication, but may delay replication or indicate a bigger problem.

The following are examples of servers experiencing temporary issues:

Lagging server:

Lifecycle [Info](#)



Launch status	Last test	Cutover
-	-	-

Data replication status [Info](#)**Healthy (with lag)**

Replication progress



Total replicated storage

16 of 16 GiB

Elapsed replication time

3 min

Lag

2 hr

Last seen

3/25/2021, 11:32:32 AM

Backlog

1.54 GiB

Replication start time

1/4/2020, 7:38:00 PM

Rescanning server:

Data replication status [Info](#)**Rescanning**

Replication progress



Total replicated storage

16 of 16 GiB

Elapsed replication time

3 min

Rescan progress



Rescanned storage: 1.1 of 16 GiB left

Lag

2 hr

Last seen

3/25/2021, 11:32:32 AM

Backlog

1.54 GiB

Replication start time

1/4/2020, 7:38:00 PM

The **Next actions** box will detail the exact issue.**Next actions** [Info](#)


🕒 Lagging

Wait for lag to disappear, then launch test instance

Servers that are experiencing serious issues will be characterized by the color red. These issues can include a loss of connection, a stall, or other issues. You will have to fix these issues in order for data replication to resume.

The **Next actions** box will detail the exact issue.


Next actions [Info](#)

 **Stalled**

Resolve cause of stalled data replication [View details](#)

The **Lifecycle** section will show a red indicator.

Lifecycle [Info](#)




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

Launch status	Last test	Cutover
-	-	-

The **Data replication status** box will include details of the issue.

Data replication status [Info](#)


Stalled

Replication progress	Total replicated storage	Elapsed replication time
 92%	14.7 of 16 GiB	3 min
	Lag	Last seen
	-	3/25/2021, 11:32:32 AM
	Backlog	Replication start time
	1.54 GiB	-



Data replication stalled

Failed to connect AWS Replication Agent to Replication Server.


[How can I solve this?](#) 

If the stall occurred during initiation, scroll down to **Replication initiation steps**. The exact step where the issue arose will be marked with a red "x".













Data replication stalled

Failed to connect AWS Replication Agent to Replication Server.

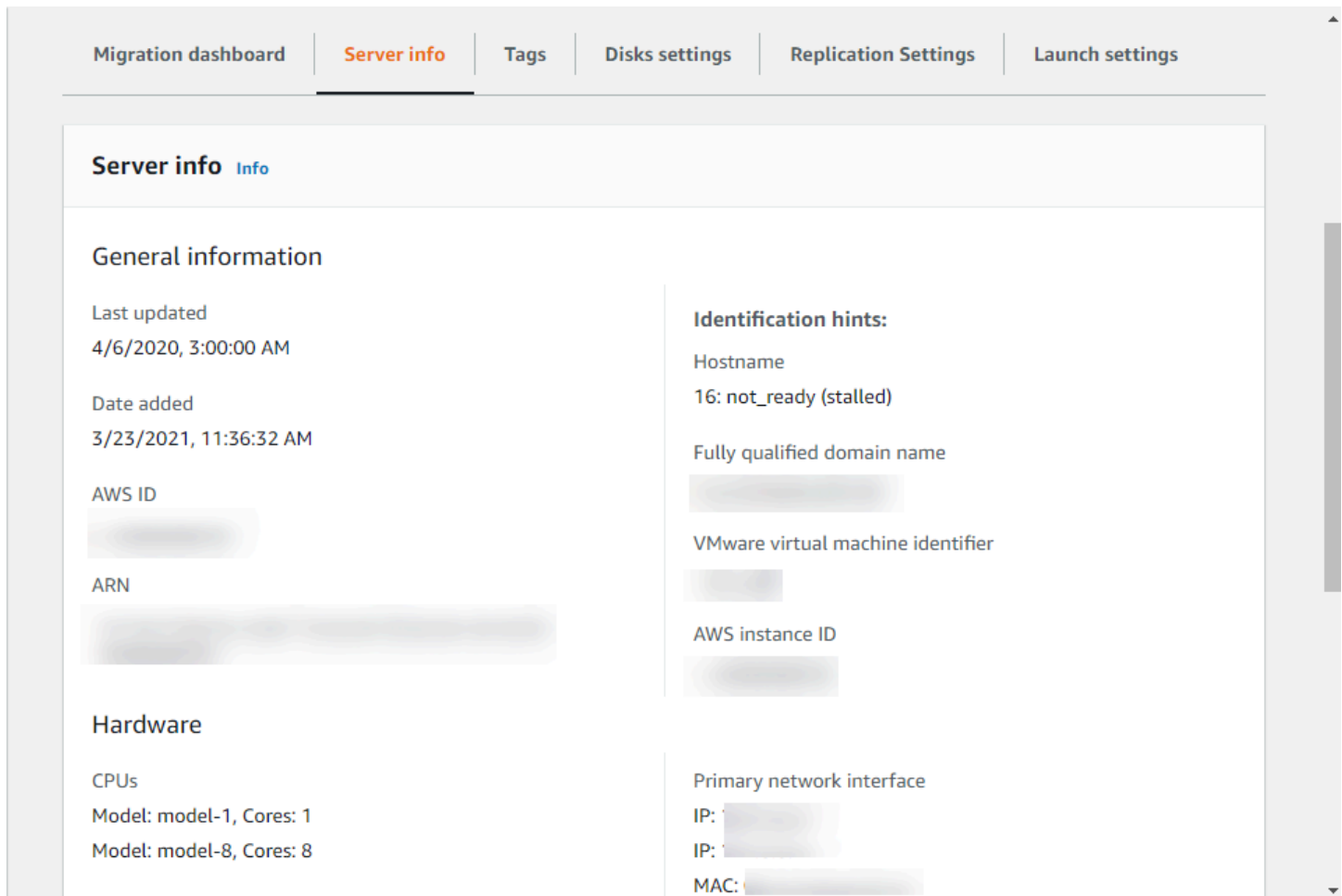
[How can I solve this?](#) 

Replication initiation steps

 Create security groups	Last start time
 Launch Replication Server	3/25/2021, 11:34:32 AM
 Boot Replication Server	
 Authenticate with service	Next attempt time
 Download replication software	-
 Create staging disks	
 Attach staging disks	
 Pair Replication Server with AWS Replication Agent	
 Connect AWS Replication Agent to Replication Server	
 Start data transfer	

Server info

The **Server info** tab shows a variety of general server information, hardware, and network information.



The screenshot shows the 'Server info' tab selected in a navigation menu. The main content area is titled 'Server info' and contains three sections: 'General information', 'Hardware', and 'Identification hints'. The 'General information' section includes 'Last updated' (4/6/2020, 3:00:00 AM), 'Date added' (3/23/2021, 11:36:32 AM), 'AWS ID', and 'ARN'. The 'Hardware' section lists 'CPUs' with 'Model: model-1, Cores: 1' and 'Model: model-8, Cores: 8'. The 'Identification hints' section lists 'Hostname' (16: not_ready (stalled)), 'Fully qualified domain name', 'VMware virtual machine identifier', 'AWS instance ID', and 'Primary network interface' (with IP and MAC addresses). The interface has a light gray background and a white content area.

This tab shows you general information about the source server:

- **General information**

- **Last updated:** when was the data in this tab updated.
- **Date added:** when was this server added to the service.
- **AWS ID:** the ID of this source server resource
- **arn:** the AWS Resource Name for this source server.
- **Identification hints:** under most circumstances, the source server name is the best identifier, as it is what is used throughout the console as the name of the source server. If you need to validate which external server this is referring to in your data center, you can use one of the additional

fields: Fully qualified domain name, VMware virtual machine identifier (only if source is VMWare), AWS instance ID (only if source is running on AWS).

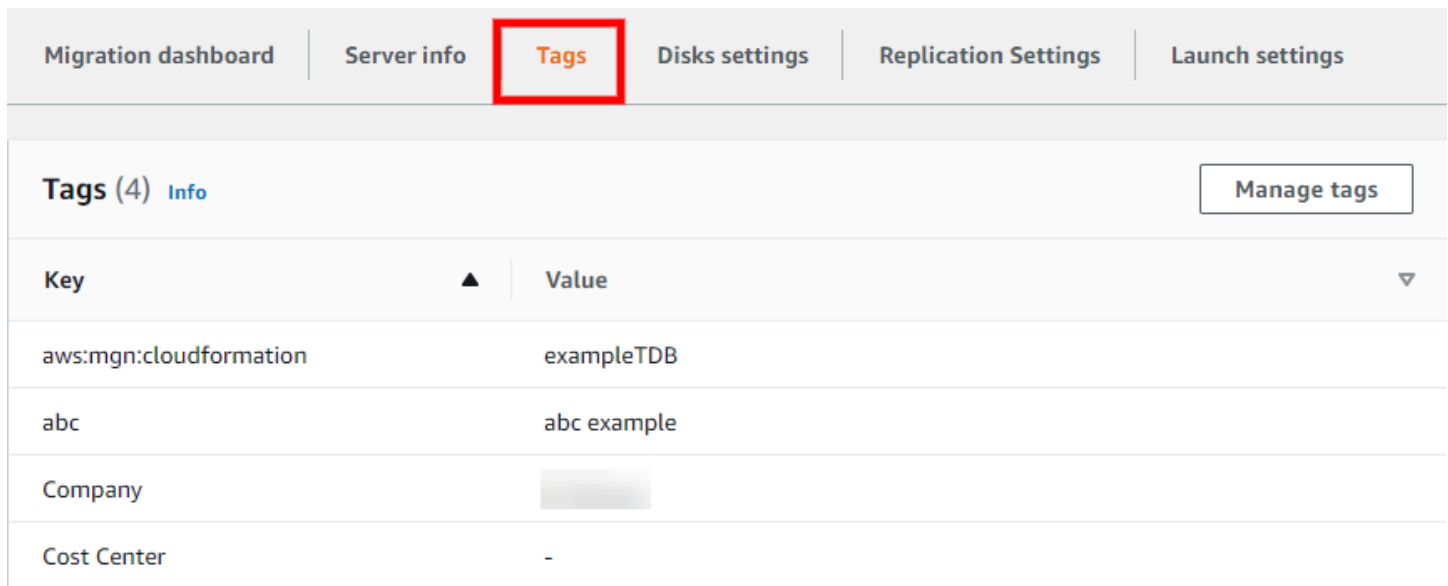
- **Hardware and operating system:** the CPUs, RAM, disks, and network interfaces on the external server, as well as the type and full name of the operating system running on that server. The disks shown are all the disk on the source server, and may include disks not being replicated.
- **Recommended instance type:** this is the EC2 instance type the service is auto-recommending to use for the launched recovery instance. This is based only on the CPUs and RAM at the source (and not on utilization information). This is the instance type that will be launched for this server by default.

Information shown includes:

- **Last updated**
- **Date added**
- **Hostname**
- **Fully qualified domain name**
- **VMware virtual machine identifier (if relevant)**
- **AWS instance ID**
- **AWS ID**
- **ARN**
- **Operating system** information
- **CPUs**
- **RAM**
- **Network interfaces**
- **Recommended instance type**

Tags

The Tags section shows any tags that have been assigned to the server. A tag is a label that you assign to an AWS resource and can be used to search and filter your resources or track your AWS costs. Each tag consists of a key and an optional value. Learn more about AWS tags in [this Amazon EC2 article](#).



Key	Value
aws:mgn:cloudformation	exampleTDB
abc	abc example
Company	
Cost Center	-

To add tags, take the following steps:

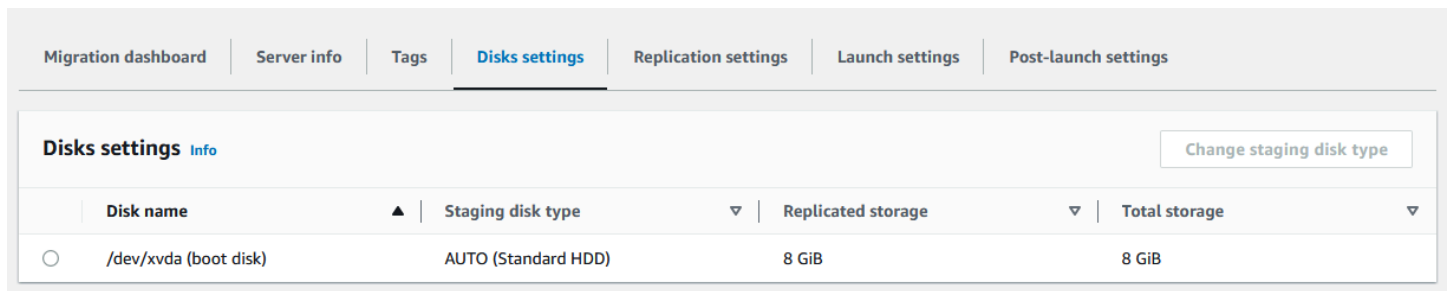
- Click **Manage tags**.
- The **Manage tags** page will open. Click **Add new tag**.
- Add a tag **Key** and an optional tag **Value**.
- Click **Save**.

To remove a tag, take the following steps:

- Click **Remove**, located to the right of the tag you want to remove.
- Click **Save**.

Disk settings

The **Disk settings** tab shows a list of all of the disks on the source server and information for each disk.



Disk name	Staging disk type	Replicated storage	Total storage
<input type="radio"/> /dev/xvda (boot disk)	AUTO (Standard HDD)	8 GiB	8 GiB

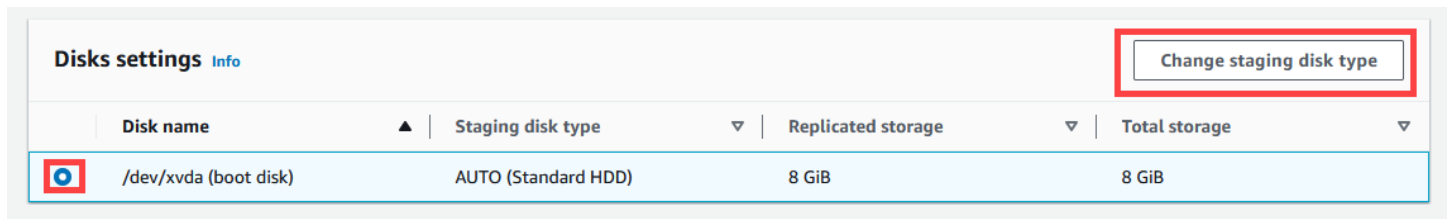
Disk settings include:

- **Disk name**
- **Staging disk type** – The corresponding Amazon EBS volume disk type that is being used for the disk.
- **Replicated storage** – The amount of storage that has been replicated from the disk to the Replication Server.
- **Total storage** – The total storage capacity of the disk.

Change staging disk type

You can change the EBS volume disk type for each disk or for a group of disks.

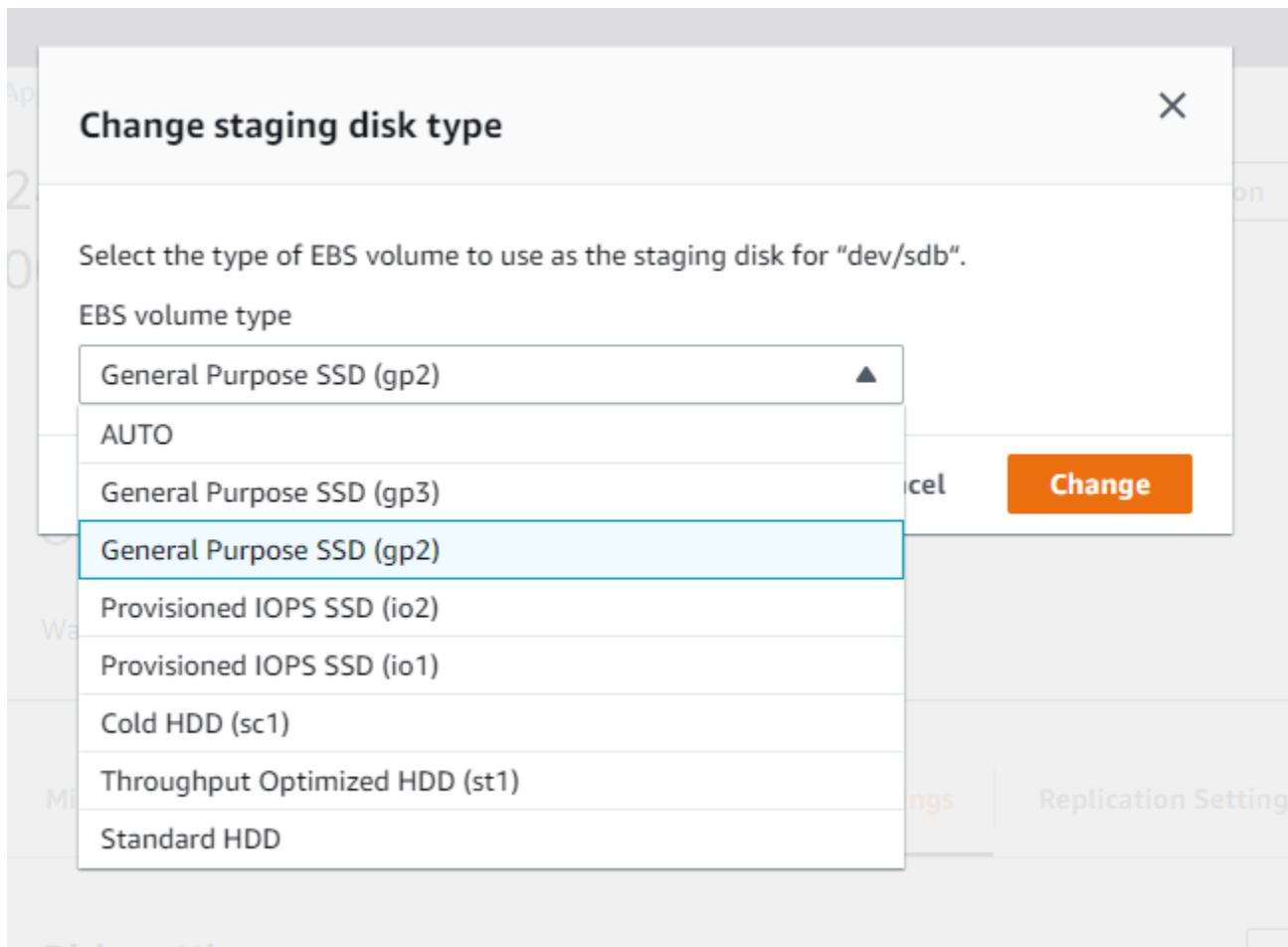
To change the EBS volume disk type, select the circle to the left of each disk name and choose **Change staging disk type**.



The screenshot shows the 'Disks settings' interface. At the top right, there is a button labeled 'Change staging disk type' which is highlighted with a red box. Below this is a table with the following columns: 'Disk name', 'Staging disk type', 'Replicated storage', and 'Total storage'. The first row of the table is highlighted in light blue and contains the following data: a selected radio button (also highlighted with a red box), the disk name '/dev/xvda (boot disk)', the staging disk type 'AUTO (Standard HDD)', the replicated storage '8 GiB', and the total storage '8 GiB'.

Disk name	Staging disk type	Replicated storage	Total storage
<input checked="" type="radio"/> /dev/xvda (boot disk)	AUTO (Standard HDD)	8 GiB	8 GiB

On the **Change staging disk type** dialog, select the type of EBS volume to use for the disk or group of disks.



Select the **AUTO** option if you want AWS Application Migration Service to automatically select the most cost-effective EBS volume disk type for each disk based on the disk size and type based on the option you defined in the **Replication settings** (either the default **Lower cost, Throughput Optimized HDD (st1)** option or the **Faster, General Purpose SSD (gp3)** option).

AWS Application Migration Service uses a single replication server per 15 source disks. Selecting the **AUTO** option will ensure that the least amount of replication servers are used, resulting in increased cost savings.

Note

AWS Application Migration Service will always use EBS magnetic volumes for disks that are under 500 GiB in size when the **AUTO** option is selected.

If you do not want AWS Application Migration Service to automatically select a disk, you can select a disk manually. Select the disk type from the **EBS volume type** menu.

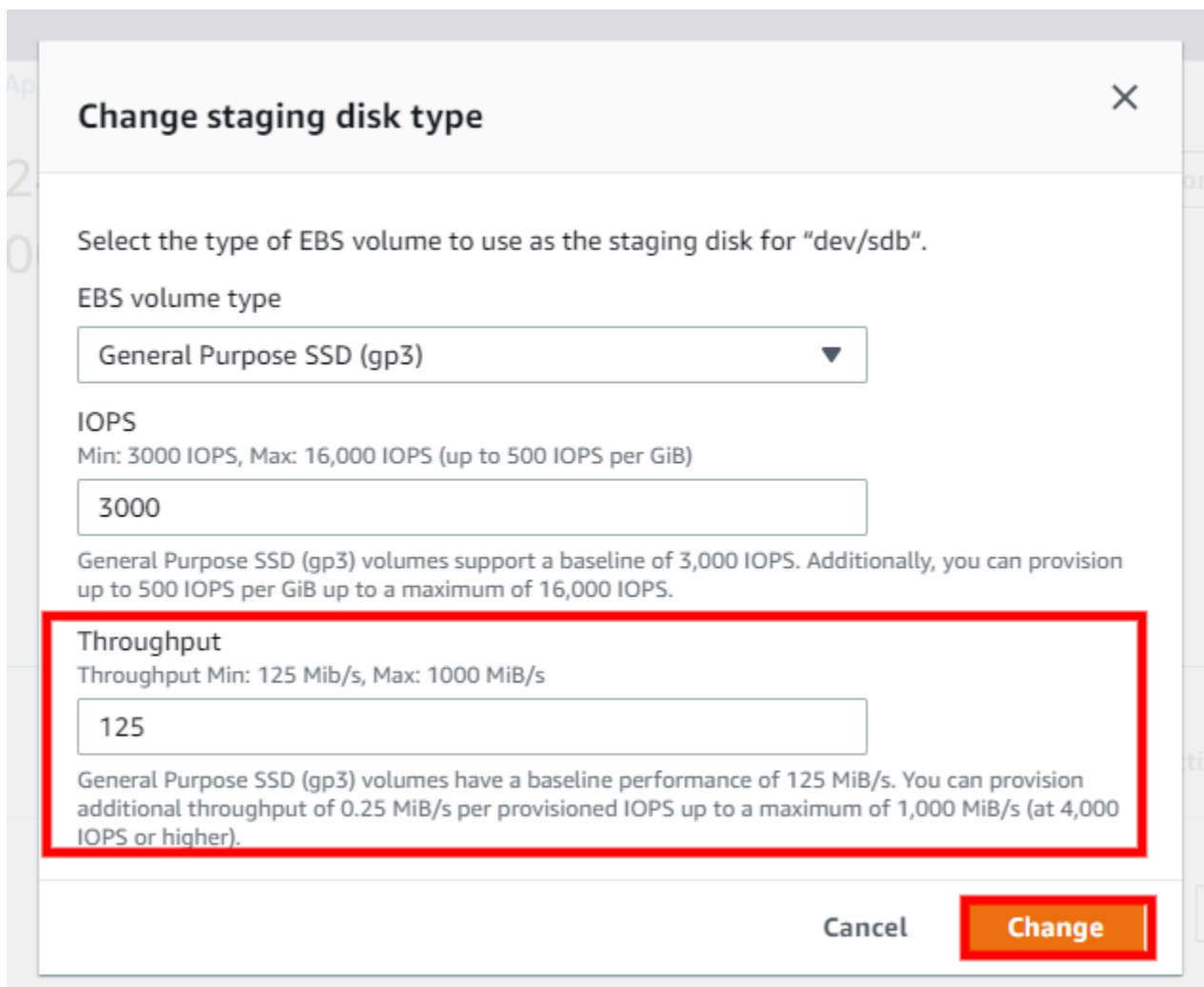
Note

When replicating into an AZ, ensure that the AZ supports the staging disk type chosen.

For certain disks, you can configure the amount of IOPS to be allocated per GB of disk space under **IOPS**. You can allocate up to 50 IOPS per GB. 64,000 IOPS are available for Nitro-based instances. Other instances are guaranteed up to 32,000 IOPS. The maximum IOPS per instance is 80,000.

Choose **Change** to confirm the change.

For **General Purpose SSD (gp3)** disks, you'll also be able to set the **Throughput**. General Purpose SSD (gp3) volumes have a baseline performance of 125 MiB/s. You can provision additional throughput of 0.25 MiB/s per provisioned IOPS up to a maximum of 1,000 MiB/s (at 4,000 IOPS or higher).



Change staging disk type ✕

Select the type of EBS volume to use as the staging disk for "dev/sdb".

EBS volume type

General Purpose SSD (gp3) ▼

IOPS

Min: 3000 IOPS, Max: 16,000 IOPS (up to 500 IOPS per GiB)

3000

General Purpose SSD (gp3) volumes support a baseline of 3,000 IOPS. Additionally, you can provision up to 500 IOPS per GiB up to a maximum of 16,000 IOPS.

Throughput

Throughput Min: 125 MiB/s, Max: 1000 MiB/s

125

General Purpose SSD (gp3) volumes have a baseline performance of 125 MiB/s. You can provision additional throughput of 0.25 MiB/s per provisioned IOPS up to a maximum of 1,000 MiB/s (at 4,000 IOPS or higher).

Cancel **Change**

Choose **Change** to confirm the change.

Replication settings

The **Replication settings** tab allows you to edit the replication settings for an individual source server.

The screenshot displays the 'Replication settings' tab in the AWS Application Migration Service console. The navigation bar includes 'Migration dashboard', 'Server info', 'Tags', 'Disks settings', 'Replication settings' (active), 'Launch settings', and 'Post-launch settings'. An 'Edit' button is located in the top right corner.

Replication Servers

- Subnet: [Redacted]
- Replication Server instance type: m5.xlarge
- Use dedicated Replication Server: No
- EBS encryption: Default
- Default EBS volume type for disks over 500GiB: Use lower cost magnetic disks (st1)
- Always use Application Migration Service security group: Yes
- Additional security groups: [Redacted]

Data routing and throttling

- Use private IP for data replication (VPN, DirectConnect or VPC peering): No
- Throttle network bandwidth: No throttling
- Create public IP: Yes

Replicated disks

[View details under Disks settings](#)

Replication resources tags

Key	Value
abc	abc example
aws:mgn:cloudformation	exampleTDB
Company	Corp
Cost Center	-

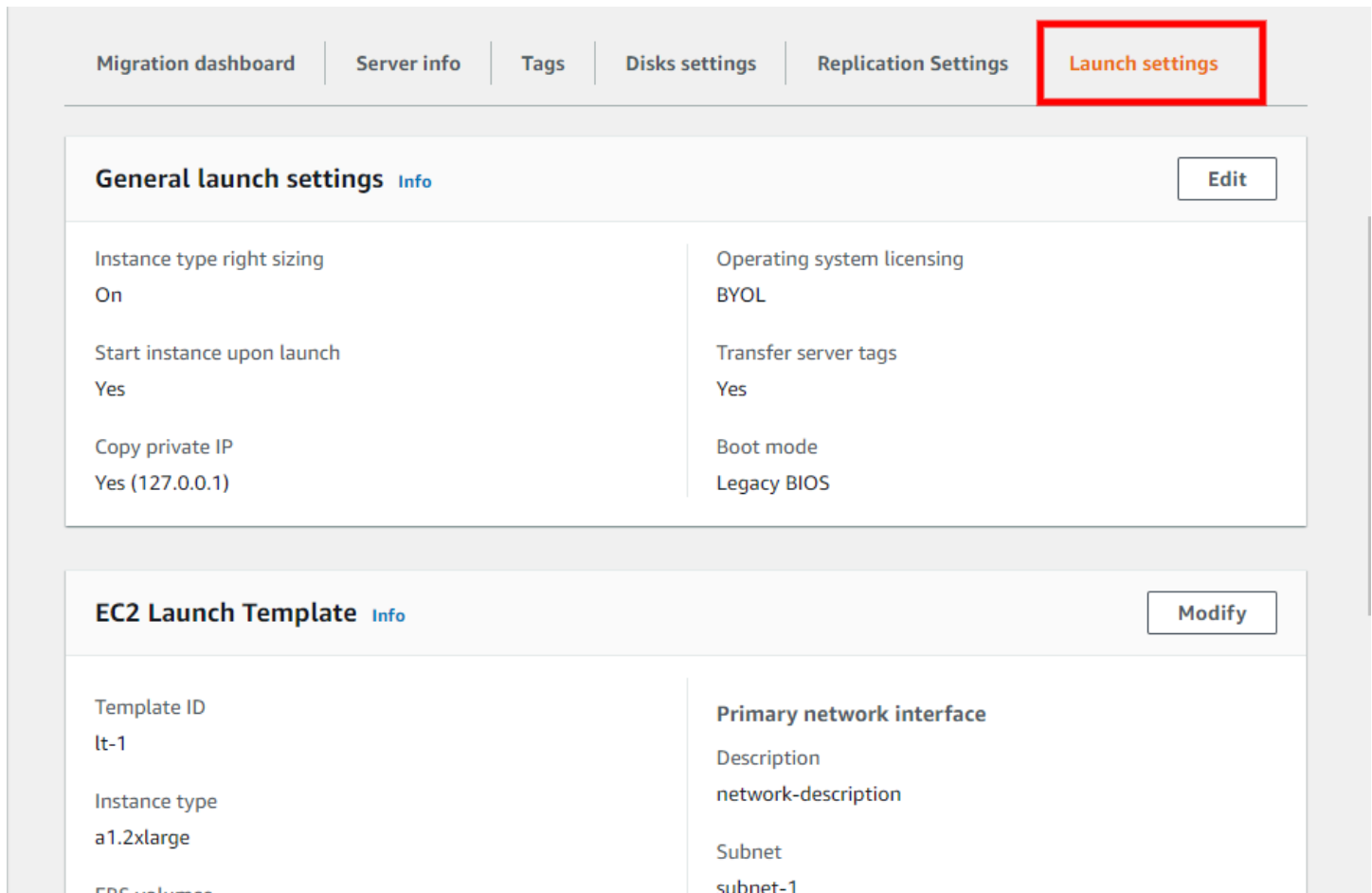
After the source server is added to AWS Application Migration Service, the replication settings that are defined in the replication settings template are automatically applied to the server. You can later edit them for a single source server through the **Replication settings** tab.

Edit each setting as required and then choose **Save replication settings**.

[Learn more about replication settings.](#)

Launch settings

The launch settings are a set of instructions that comprise an EC2 launch template and other settings, which determine how a test or cutover instance will be launched for each source server on AWS.



The screenshot displays the AWS Migration dashboard with the 'Launch settings' tab selected and highlighted by a red box. The dashboard is divided into two main sections: 'General launch settings' and 'EC2 Launch Template'. Each section has an 'Info' link and an action button ('Edit' or 'Modify').

General launch settings Info Edit	
Instance type right sizing On	Operating system licensing BYOL
Start instance upon launch Yes	Transfer server tags Yes
Copy private IP Yes (127.0.0.1)	Boot mode Legacy BIOS

EC2 Launch Template Info Modify	
Template ID lt-1	Primary network interface
Instance type a1.2xlarge	Description network-description
FRS volumes	Subnet subnet-1

Launch settings, including the EC2 launch template, are automatically created every time you add a server to AWS Application Migration Service.

The launch settings can be modified at any time, including before the source servers have even completed initial sync.

[Learn more about individual launch settings.](#)

Post-launch settings

Post-launch settings allow you to control and automate actions performed after the server has been launched in AWS. These settings are created automatically based on the **Post-launch settings template**.

You must activate the post-launch actions using one of the following options:

- **Activating the post-launch actions for a specific server:**
 - Navigate to the **Source servers** page and select a source server.
 - Click **Post-launch settings > Edit**.
 - You will be redirected to the **Edit post-launch settings** screen. Activate the toggle and click **Save settings**.

Alternatively, you can select a specific source server, open the **Test and cutover** drop-down menu located in the top right corner of the screen and select **Edit post-launch settings**.

- **Activating the post-launch actions for all servers:**
 - Navigate to the **Settings** page and choose **Post-launch settings template**. You will only need to do this once and the change will apply to all newly added servers.

After the post-launched actions have been activated from the template, you can deactivate and activate them for individual servers. [Learn more about activating post-launch settings](#).

Application Migration Service > Active source servers > s-0000000011 > Post-launch settings > Edit post-launch settings

Edit post-launch settings [Info](#)

Post-launch actions

Post-launch actions [Info](#)

The service can execute actions on your servers, after they are launched, using AWS Systems Manager (AWS SSM). The service will install the AWS SSM agent, and execute the actions you select.

Install the Systems Manager agent and allow executing actions on launched servers

⚠ If you do not activate this feature, this service will not install the SSM agent. Post-launch actions will not be executed on any of your servers.

Cancel **Save settings**

The settings configured in the template will be applied to every newly added server. You can change the settings for existing and newly added servers individually within the server details view.

The **Post-launch settings** template allows you to control various post-launch actions, including:

- Deployment of test and cutover instances
- Disaster recovery configuration (installing the AWS Replication Agent for AWS DRS and configuring the target disaster recovery AWS Region)
- Operating system conversion on the target machine
- License and subscription changes on the target machine

Editing the post-launch settings

To edit the post-launch settings for a single source servers, check the box to the left of the Hostname of each source server for which you want testing to edit the post-launch settings, open the **Replication** menu, and choose **Edit post-launch settings**.

The screenshot shows the 'Source servers (38)' page in the AWS Migration Service console. A table lists source servers with columns for Source server name, Alerts, Migration lifecycle, and Data replication status. The first server, '21: ready_for_test', is selected. The 'Replication' menu is open, and 'Edit post-launch settings' is highlighted.

Source server name	Alerts	Migration lifecycle	Data replication status
<input checked="" type="checkbox"/> 21: ready_for_test	-	Ready for testing	Healthy
<input type="checkbox"/> 22: ready_for_test - windows	-	Ready for testing	Healthy
<input type="checkbox"/> 23: ready_for_test (rescan)	⊙ Lagging	Ready for testing	Rescanning 18% 10 min left
<input type="checkbox"/> 24: ready_for_test (lagging)	⊙ Lagging	Ready for testing	Lag 2 hr 119 min left
<input type="checkbox"/> 25: ready_for_test (stalled)	⊙ Stalled	Ready for testing	Stalled
<input type="checkbox"/> 26/ready_for_test/stalled	⊙ Stalled	Ready for testing	Stalled
<input type="checkbox"/> 27/ready_for_test/pending_snapshot_shipping	-	Ready for testing	Healthy
<input type="checkbox"/> 28/ready_for_test/shipping_snapshot	-	Ready for testing	Healthy
<input type="checkbox"/> 29: reverted_ready_for_test	-	Ready for testing	Healthy
<input type="checkbox"/> 30: reverted_ready_for_test	⊙ Launched	Ready for testing	Healthy

Alternatively, when editing the settings for a single server, you can choose **Edit** from the **Post-launch settings** tab.

The screenshot shows the Application Migration Service interface. At the top, there is a breadcrumb trail: "Application Migration Service > Active source servers > 11: not_ready (initiating)". Below this, the server name "11: not_ready (initiating) (s-0000000011)" is displayed. To the right of the server name are three buttons: "Actions", "Replication", and "Test and cutover".

Below the server name is a section titled "Next actions" with an "Info" link. The text below it says "Wait for initial sync to complete".

Below this is a navigation bar with several tabs: "Migration dashboard", "Server info", "Tags", "Disks settings", "Replication settings", "Launch settings", and "Post-launch settings". The "Post-launch settings" tab is currently selected and highlighted.

Below the navigation bar is a section titled "Post-launch actions settings" with an "Info" link. To the right of this section is a red-bordered "Edit" button. Below the section title, there are two settings:

Activate post-launch actions	Deployment
No	Test and cutover instances

The following settings can be edited within the post-launch settings template. Once you have edited all your settings, click **Save template**.

Activating and deactivating post-launch actions

This setting controls whether post-launch actions are active or inactive. You must leave the **Install System Manager agent and allow executing actions on launched servers** option toggled in order for post-launch actions to work. Untoggling the option will disallow AWS MGN to install the SSM Agent on your servers and post-launch actions will no longer be executed on them.

The feature is activated and deactivated at the account level from the **Settings > Post-launch template** screen. [Learn more about activating post-launch settings.](#)

After it was activated once, the feature can also be deactivated and reactivated for a single server. Simply selecting a server, go to the **Post-launch settings** tab and click **Edit**.

When the feature is inactive:

- All actions are hidden.
- You will not be able to activate actions at the account level or the feature level.

When the feature is active:

- The actions are visible.

- You can activate them.

Application Migration Service > Post-launch template > Edit post-launch template

Post-launch template [Info](#)

Configure actions to be executed on every server, upon server launch

Post-launch actions [Info](#)

The service can execute actions on your servers, after they are launched, using AWS Systems Manager (AWS SSM). The service will install the AWS SSM agent, and execute the actions you select.

Install the Systems Manager agent and allow executing actions on launched servers

i By continuing, you are allowing AWS Application Migration Service to install the SSM agent and create the IAM roles required to execute automation on launched servers.

Deploying post-launch actions

Use this setting to choose whether to deploy the post-launch actions only on your cutover instances or on both cutover and test instances.

Deployment [Info](#)

Choose whether to execute the post-launch actions on your cutover instances only, or on both your cutover and test instances.

Test and cutover instances (recommended)
All post-launch actions will be executed on test and cutover instances.

Cutover instances only
All post-launch actions will only be executed on the cutover instances.

Test instances only
All post-launch actions will only be executed on the test instances.

Types of post-launch actions

AWS MGN supports post-launch modernization actions, giving you the opportunity to move and improve. All post-launch actions are based on SSM documents (either public or ones you created) that can be executed on your EC2 launch instances.

There are 2 types of post-launch actions:

- **Predefined post-launch actions** – These out-of-the box actions are based on public SSM documents that cannot be changed and have certain unchangeable parameters such as the platform name and order. Fields are prepopulated with the necessary values and only need to be activated or deactivated.
- **Custom post-launch actions** – These actions are based on SSM documents that you create and upload to your account.

Use the **Filter by** options on the left-hand side to filter the available actions according to your preferences.

Click the settings icon in the right-hand corner of the screen to alternate between card and list view, according to your preferences.

Migration dashboard | Server info | Tags | Disks settings | Replication settings | Launch settings | **Post-launch settings**

▼ **Post-launch actions settings** [Info](#) Edit

Activate post-launch actions
Yes

Deployment
Test and cutover instances

Filter by

▼ **Activation status**

Active
 Not active

▼ **Platform**

Linux
 Windows

▼ **Creator**

Me
 AWS
 3rd party

▼ **Categories**

Backup
 Configuration
 Disaster recovery
 License & subscription
 Observability
 Operating system
 Validation
 Other

Actions (10) Card view ▼ Edit Delete Create action

< 1 > ⚙️

Action Name	Powered by	Status	Platform	Order	Description
SSM agent	AWS SSM	Active	Windows and Linux	1	Install SSM agent
Replace SUSE subscription	AWS MGN	Not active	Linux	20	This action will convert a SUSE Linux subscription to an AWS provided... More
CentOS to Rocky	AWS MGN	Not active	Linux	30	This action will convert the operating system of instances running... More
CloudWatch agent installation	AWS CloudWatch	Not active	Windows and Linux	101	
Join domain	AWS Directory Service	Not active	Windows and Linux	330	
Volume integrity validation	AWS MGN	Not active	Windows and Linux	401	

Predefined post-launch actions

AWS MGN supports post-migration modernization actions, allowing you to move and improve. Use these out-of-the-box actions to modernize your servers by executing various post-launch actions on your EC2 launch instance.

Choose from a variety of predefined post-launch actions.

- [Configure AWS Elastic Disaster Recovery \(AWS DRS\)](#)
- [Convert operating systems](#)
- [Change license and subscription](#)
- [Conduct EC2 connectivity checks](#)
- [Validate volume integrity](#)
- [Verify process status](#)
- [Convert MS-SQL license conversion](#)
- [Install a CloudWatch Agent](#)
- [Upgrade Windows](#)
- [Create AMI from instance](#)
- [Join Directory Service domain](#)
- [Configure Time Sync](#)
- [Validate disk space](#)
- [Verify HTTP/HTTPS response](#)
- [Enable Amazon Inspector](#)
- [Verify Tags](#)
- [Auto Scaling group setting](#)
- [Enable Refactor Spaces](#)
- [App2Container for Replatforming](#)
- [Dynatrace](#)

Custom post-launch actions

AWS Application Migration Service (AWS MGN) allows you to execute any SSM document that you like – public SSM document or ones you created and uploaded to your account.

You can configure a custom action to execute any SSM document that is available in your account.

Create action

This page allows you to define actions that will be executed on your EC2 launch instance. It includes the following parameters:

- **Action name** – The name of the action in AWS MGN, which should be intuitive and meaningful to your migration users.
- **System Manager document name** – Select any Systems Manager document that is available for the specific account.
- **View in Systems Manager** – Click to open **System Managers** and view additional information about the document.
- **Description** – Add a description or keep the default.
- **Document version** – Select which SSM document version to run. AWS MGN can run a default version, the latest version, or a specific version, according to your preferences.
- **Category** – Select from various available categories including disaster recovery, security, validation, and more.
- **Order** – Specify the order in which the actions will be executed. The lower the number, the earlier the action will be executed. 1–1,000 are reserved for predefined actions and 1,001–10,000 for custom actions. The numbers must be unique but don't need to be consecutive.
- **Operating system** – Select the source server's operating systems for which the custom action can be configured for. Note that if you associate a script with the wrong operating system, it will be skipped.
- **This action must be completed successfully before finalizing cutover** – This checkbox will dictate whether or not the script will prevent the cutover.

The **Action parameters** are dependent on the specific SSM document that is selected.

Note that for the instance ID parameter, you can choose to use the launch instance ID, in which case, AWS MGN will dynamically populate the value.

Add action [Info](#)

You can associate any Systems Manager document with a post-launch action

Action settings [Info](#)

Action name

The name must be unique. Min: 1 character, Max: 256 characters.

Activate this action

Actions that are active will be executed on the launched instance, after it is launched.

This action must be completed successfully before finalizing cutover.

Systems Manager document name

Select any Systems Manager document that is available for this account.

Description

Specify the action description. Up to 70 characters will be displayed on the card.

Document version

Select the document version to use.

Category

Select the action category which is available for this account.

Order

Specify the order in which the actions will be executed (range 1,001-10,000).

Operating systems

Select the source server's operating systems for which the action can be configured for.

Creator

Action creator.

Cancel

Add action

Edit each setting as required and then click **Add action**.

Edit action

Use this page to edit the parameters detailed in the **Create action** section.

Edit each setting as required and then click **Save action**.

Applications

Many customers have clusters of servers with dependencies between them. AWS Application Migration Service provides the user with a way to represent a group of servers by associating them with an **Application**.

You can monitor the migration status and progress of an application and its associated servers. You can also perform operation on the application, such as edit, tagging, archive, as well as bulk operations on the servers associated with the application.

Topics

- [Applications page](#)
- [Application details](#)

Applications page

The **Applications** page lists all the applications that have been added to AWS Application Migration Service. The **Applications** page allows you to manage your applications and perform a variety of commands for one or more applications (such as controlling replication and launching test and cutover instances).

The screenshot displays the AWS Application Migration Service console. The left sidebar shows the 'Applications' menu item highlighted with a red box. The main content area shows a table of 11 applications. The table has columns for Application name, Wave name, Migration status, Alerts, and Number of servers. The 'Applications' menu item in the left sidebar is highlighted with a red box.

Application name	Wave name	Migration status	Alerts	Number of servers
Application-A	-	In progress	Stalled	3
Application-B	Wave 1	In progress	Healthy	3
Application-C	-	In progress	Healthy	2
Application-D	Wave-4	In progress	Healthy	1
Application-E	-	Completed	Healthy	1
Application-F	-	In progress	Healthy	1
MGN-6583: Application-A: no server has alert	MGN-6583	In progress	Healthy	2
MGN-6583: Application-B: no servers	MGN-6583	Not started	Healthy	0
Zehorit: Application-F : 1 server "Cutover in progress"	Wave 3	Completed	Healthy	1
Zehorit: Application-H	Wave 2	Not started	Healthy	0
Zehorit: Application-I	Wave 3	Not started	Healthy	0

Last update: September 21, 2022 at 09:42 (UTC+3:00)

Topics

- [Interacting with the Applications page](#)

- [Commands menu](#)
- [Filtering](#)

Interacting with the Applications page

The **Applications** page shows a list of applications. Each row on the list represents a single application.

Application Migration Service > Applications

Applications (11) [Info](#) Actions ▾ Edit Delete Add application

Active applications ▾ < 1 > ⚙️

<input type="checkbox"/>	Application name ▲	Wave name ▼	Migration status ▼	Alerts ▼	Number of servers ▼
<input type="checkbox"/>	Application-A	-	⊖ In progress	⊗ Stalled	3
<input type="checkbox"/>	Application-B	Wave 1	⊖ In progress	⊙ Healthy	3
<input type="checkbox"/>	Application-C	-	⊖ In progress	⊙ Healthy	2
<input type="checkbox"/>	Application-D	Wave-4	⊖ In progress	⊙ Healthy	1
<input type="checkbox"/>	Application-E	-	⊙ Completed	⊙ Healthy	1
<input type="checkbox"/>	Application-F	-	⊖ In progress	⊙ Healthy	1
<input type="checkbox"/>	MGN-6583: Application-A: no server has alert	MGN-6583	⊖ In progress	⊙ Healthy	2
<input type="checkbox"/>	MGN-6583: Application-B: no servers	MGN-6583	⊖ Not started	⊙ Healthy	0
<input type="checkbox"/>	Zehorit: Application-F: 1 server "Cutover in progress"	Wave 3	⊙ Completed	⊙ Healthy	1

The **Applications** page provides key information for each application under each of the columns on the page.

The columns include:

- **Selector column** – This blank checkbox selector column allows you to select one or more applications. When an application is selected, you can interact with the application through the **Actions** menu, **Edit**, and **Delete** buttons. Selected applications are highlighted.
- **Application name** – This column shows the unique application name for each application.
- **Wave name** – This column shows the name of the wave the application is associated with. An application cannot be associated with more than one wave at a time.

This column is hidden by default.

- **Migration status** – This column shows the migration status for each application.
 - **Not started** – None of the application associated servers has started replication yet.
 - **In progress** – At least one of the application associated servers has started replication and not all of its servers completed migration.

- **Completed** – All the application associated servers completed migration (have been cut over).
- **Alerts** – This column shows whether any alerts exist for the application.
 - **Stalled** – An application that has at least one server that is experiencing significant issues, such as a stall.
 - **Lagging** – An application that has at least one server that is experiencing a temporary issue such as lag or backlog.
 - **Healthy** – A healthy active application.

Archived applications do not display any alerts.

- **Number of servers** – This column shows the total number of servers associated with each application.

Commands menu

Use the command menu to add applications, perform a variety of actions, and manage your testing and cutover for one or more applications.

You can either **Add application** or select one or more applications from the **Applications** page and then manage them using the **Actions** menu, **Edit**, or **Delete** buttons.

Topics

- [Add application](#)
- [Edit application](#)
- [Delete application](#)
- [Actions menu](#)

Add application

To add an application, click **Add application**. When the **Add application** prompt opens, configure the application name, add a description (optional), associate source servers (optional), and add tags (optional).

[Application Migration Service](#) > [Applications](#) > Add application

Add application [Info](#)

Application settings

Application name

Example: App no. 1

Description - optional

Example: This is a description of App no. 1. (600 character limit)

Servers

Select servers to associate with this application.

Select servers

A server may be associated with a single application.

Application tags - optional

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Add application

- **Application name** – Application name is mandatory, with a limit of 256 characters. The name must be unique per account per region. Uniqueness verification for application name in Migration Application Service is case-insensitive.
- **Description** – Application description is optional, with a limit of 600 characters.
- **Servers** – You can add up to 200 servers to an application. Checking a server in the drop-down list will associate it with the application.
- **Tags** – You can add up to 50 tags to an application.

When you are done configuring your application settings, click **Add application** to create the application.

Edit application

To edit an application, click **Edit**. When the **Edit application** prompt opens, edit the application name, description, and tags, as well as associate or disassociate source servers.

Application Migration Service > Applications > Edit application

Edit application [Info](#)

Application settings

Application name

Description - *optional*

Servers

Select servers to associate with this application.

test-394672209 ×
s-3d3eae12a5dcfa943

test-807742204 ×
s-31b5704048829430f

test-671556424 ×
s-3d3e0b8e54c469ecd

test-398052867 ×
s-34f3caeffece2c6c2

test-635325094 ×
s-39e060ea1cdac8625

A server may be associated with a single application.

Application tags - *optional*

No tags associated with the resource.

You can add up to 50 more tags.

Cancel

- **Application name** – Application name is mandatory, with a limit of up to 256 characters. The name must be unique per account per region. Uniqueness verification for application name in Migration Application Service is case-insensitive.
- **Description** – Application description is optional, with a limit of 600 characters.
- **Servers** – You can add up to 200 servers to an application. Checking a server in the dropdown list will associate it with the application. Unchecking an associated server will disassociate it from the application.
- **Tags** – You can add up to 50 tags to an application.

To finalize your changes, click **Save changes**.

Delete application

To delete an application, click **Delete**. When the **Delete application** prompt opens, verify that you want to delete the selected application.

Deleting the application will disassociate the servers from the application, but will not delete them.

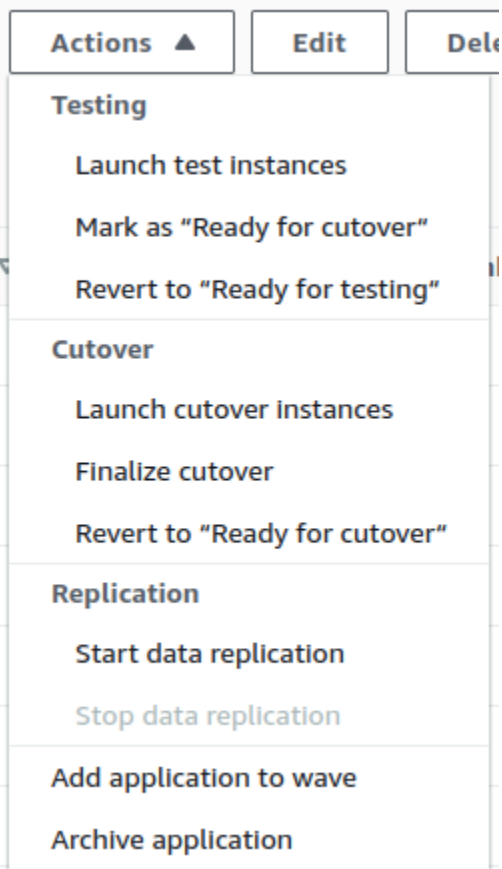
Click **Delete** to confirm the deletion.

Actions menu

The **Actions** menu allows you to perform actions on selected applications.

Note

An application must have **all** of its associated servers in the correct lifecycle for the desired action, otherwise it will be excluded.



The **Actions** menu allows you to perform the following actions:


- **Launch test instances** – Choose this option to launch test instances for this application servers.
- **Mark as "Ready for cutover"** – Choose this option to finalize testing for this application after you have completed all the necessary tests in preparation for cutover.

The **Mark servers as "Ready for cutover"** dialog will appear. Select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Continue**.

- **Revert to "ready for testing"** – Choose this option to revert a finalized test for this application if you want to run further tests prior to initiating a cutover.


The **Revert testing** dialog will appear. Select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Revert**.

- **Launch cutover instances** – Choose this option to launch cutover instances for this application servers after you have finalized all of your testing and are ready to initiate a cutover.
- **Finalize cutover** – Choose this option to finalize the cutover for this application servers after you have successfully performed a cutover.

 **Note**

This action does not uninstall the AWS Replication Agent from the source servers. When you have completed the migration and want to uninstall the agent from your source servers, go to **Source servers** page and select the relevant servers. Use the **Disconnect from service** option under the **Actions** menu.

- **Revert to "ready for cutover"** – Choose this option to revert a finalized cutover for this application if you encounter any issues or want to reverse the cutover for any reason.
- **Start data replication** – Choose this option to start replicating the application source servers.

 **Note**

This action is applicable if all the application associated servers are **Agentless snapshot based** and are in **Discovered** lifecycle state.

- **Add applications to wave** – Choose this option to associate the selected applications to a wave.
- **Archive applications** – Choose this option to archive the selected applications. You should only archive applications for which you have already performed a cutover.

 **Important**

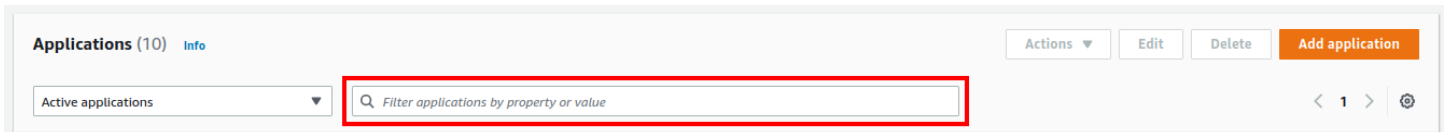
An application can be archived only if all servers that compose it are in one of these states: archived, cutover, or disconnected. If that is the case, the application will be archived and the servers that are not yet archived (but can be) will also be archived.

Archived applications will be removed from the main applications page, but can still be accessed through the selector options.

Filtering

You can customize the **Applications** page through filtering. Filtering allows you to easily filter your applications by one or multiple properties.

Click within the **Filter applications** field and choose the filtering property from the **Properties** menu.



You can filter by a variety of properties, including:

Properties
Application name
Application ID
Wave name
Migration status
Alerts
Number of servers

Tags
test
aws:tag:domain

- Application name – Filter by application name.
- Application ID – Filter by application ID.
- Wave name – Filter by wave name.
- Migration status – Filter by the migration status (Not started, In progress, Completed).
- Alerts – Filter by health status alert (Stalled, Lagging, Healthy).
- Number of servers – Filter by a number of servers.
- Tags - Filter by tags. Relevant specific tag values will appear under the **Tags** category. Choose the value by which to filter.

You can filter by multiple properties at once in order to narrow down your results.

Here you see an example of filtering the applications list by several properties:

Application Migration Service > Applications

Applications (3) Info Actions ▾ Edit Delete **Add application**

Active applications 2 matches < 1 > ⚙

Alerts = Healthy × and **Number of servers = 1** × Clear filters

<input type="checkbox"/>	Application name	Wave name	Migration status	Alerts	Number of servers
<input type="checkbox"/>	arch-app	-	In progress	Healthy	1
<input type="checkbox"/>	MGN-6555	-	In progress	Healthy	1

Last update: September 29, 2022 at 10:29 (UTC+3:00)

To clear the selected filtering properties, click **Clear filters**.

Application details

There are several ways you can access the **Application details** view.

Click on the **Application name** of any application on the **Applications** page.

Applications (3) Info Actions ▾ Edit Delete **Add application**

Active applications < 1 > ⚙

<input type="checkbox"/>	Application name	Wave name	Migration status	Alerts	Number of servers
<input type="checkbox"/>	App 3	wave 3	In progress	Healthy	2

Click on the **Application** of any server on the **Source servers** page.

Source servers (17) Actions ▾ Replication ▾ Test and cutover ▾

Active source servers < 1 > ⚙

<input type="checkbox"/>	Source server name	Application	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step
<input type="checkbox"/>	ip-172-31-35-46.eu-central-1.compute.internal	arch-app	-	Ready for cutover	Healthy	an hour ago	Launch cutover instance

Click on the **Application name** in the **Server info** tab.

Migration dashboard | **Server info** | Tags | Disks settings | Replication settings | Launch settings | Post-launch settings

Server info [Info](#)

General information

Last updated
September 29, 2022 at 10:05 (UTC+3:00)

Date added
September 01, 2022 at 15:40 (UTC+3:00)

AWS ID
s-0d1b696ed7bee64ac

ARN
arn:aws:mgn:eu-west-1:027888403785:source-server/s-0d1b696ed7bee64ac

Application name
App 3

Hardware

CPU
Model: Intel(R) Xeon(R) CPU E5-2676 v3 @ 2.40GHz, Cores: 1

Identification hints

Hostname
ip-172-31-36-230.eu-central-1.compute.internal

Fully qualified domain name
ip-172-31-36-230.eu-central-1.compute.internal

VMware virtual machine identifier
-

AWS instance ID
i-03df59d8c6e5a59e9

Primary network interface
IP: 172.31.36.230
MAC: 06-A9-1B-34-14-A4

Operating system


Type
Linux

Click on the **Application name** of any application in the **Applications** table inside **Wave details** -> **Applications** tab.

Applications | Source servers | Tags

Alerts [Info](#)


Filter applications
Select status to filter



Healthy
1 application, 100%

Migration status [Info](#)

Filter applications
Select status to filter



In progress
1 application, 100%

Applications (1) [Info](#)

Filter source servers by property or value

Application name	Migration status	Alerts	Number of servers	Archived
App 3	In progress	Healthy	2	Active

Last update: September 29, 2022 at 11:08 (UTC+3:00)

The **Application details** view shows information and options for an individual application. Here, you can control and monitor the individual application.

Application Migration Service > Applications > Application-0

Application-0 (app-0) Actions ▾ Edit Delete

Overview [Info](#)

Description 0.he9o2pnqw8n	Last status update October 02, 2022 at 11:00 (UTC+3:00)	Migration status 🔄 In progress
State Active	Wave name Wave-0	Alerts 🟢 Healthy

Alerts [Info](#)

Filter servers
Select status to filter ▾

Launched 1 server, 33.3%	Healthy 2 servers, 66.7%
-----------------------------	-----------------------------

Data replication status [Info](#)

Filter servers
Select status to filter ▾

Initial sync 1 server, 33.3%	Healthy 2 servers, 66.7%
---------------------------------	-----------------------------

Migration lifecycle [Info](#)

Filter servers
Select status to filter ▾

Ready for cut... 1 server, 33.3%	Not ready 1 server, 33.3%	Ready for tes... 1 server, 33.3%
-------------------------------------	------------------------------	-------------------------------------

You can also perform a variety of actions on the application, and perform batch operations such as launch Test and Cutover instances for the servers associated with the application.



The **Application details** view is divided into several dashboards:

Topics

- [Overview dashboard](#)
- [Source server migration metrics](#)
- [Source servers table](#)
- [Tags](#)

Overview dashboard

The **Overview** dashboard provides an overview of the overall application status, including:

Overview Info		
Description Application description (can be up to 600 characters)	Last status update October 02, 2022 at 15:33 (UTC+3:00)	Migration status  In progress
State Active	Wave name Wave 1	Alerts  Healthy

- **Description** – The description of the application.
- **State** – The state of the application. **State** can be in one of two states: **Active** or **Archived**.
- **Last status update** – Time stamp of when application status was updated (update occurs every five minutes).
- **Wave name** – Name of the wave that the application is associated with.
- **Migration status** – The application migration status.

Application **Migration status** can have one of the following values:

Not started – If none of its servers has started replication yet.

Completed – If all of its servers completed migration (have been cutover).

In progress – At least one of its servers has started replication and not all of its servers completed migration.

- **Alerts** – The application alert.

An application that has at least one server that is experiencing significant issues, such as a stall, will display a **Stalled** status.

An application that has at least one server that is experiencing a temporary issue such as lag or backlog will display a **Lagging** status.

A healthy active application will display a **Healthy** status.

An archived application will not display a status.

Source server migration metrics

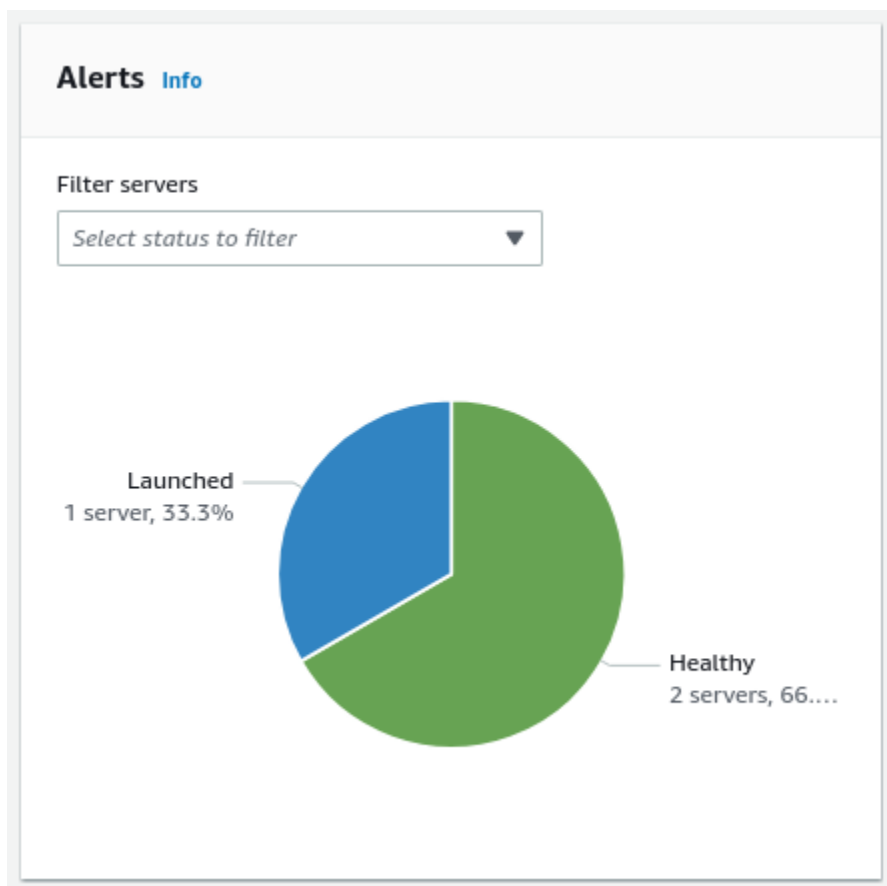
The source server migration metrics show an aggregated overview of the application associated servers on three topics: **Alerts**, **Data replication status** and **Migration status**.

Topics

- [Alerts](#)
- [Data replication status](#)
- [Migration lifecycle](#)

Alerts

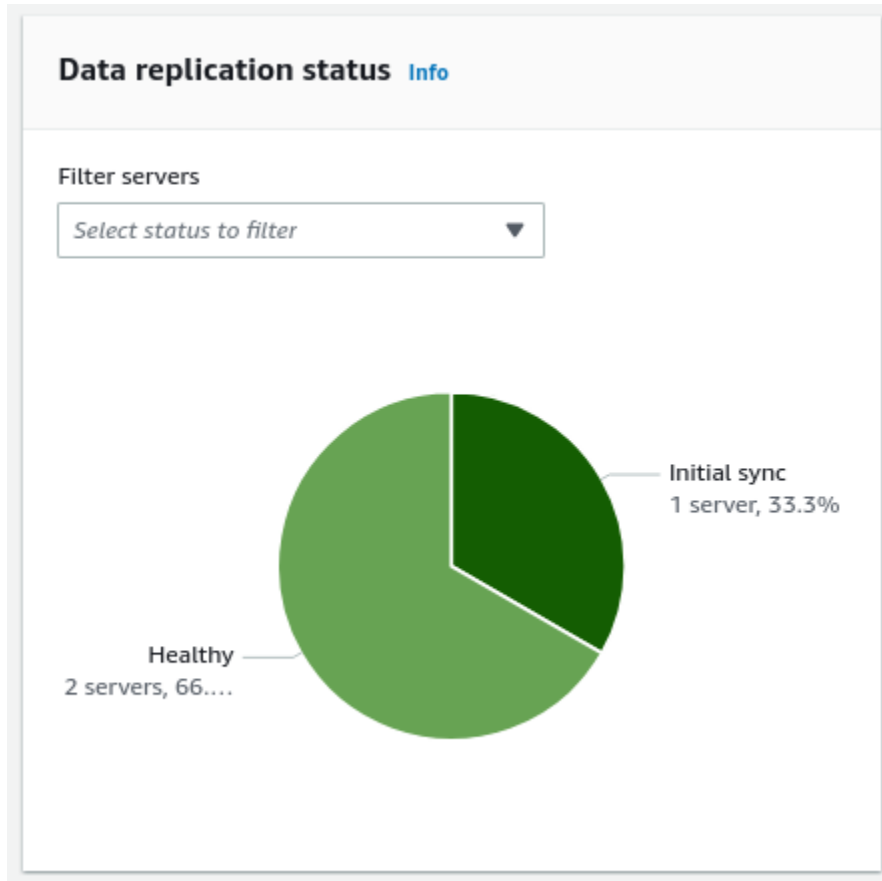
The source server **Alerts** migration metric presents an aggregated overview of the application associated servers alerts. You can look up an individual source server **Alerts** status at the **Source servers** table at the bottom of the page.



- A healthy server for which a test or cutover instance has not been launched will display a **Healthy** status.
- A healthy server for which a test or cutover instance has been launched will display a **Healthy** status.
- A server that is experiencing a temporary issue such as lag or backlog will display a **Lagging** status.
- A server that is experiencing significant issues, such as a stall, will display a **Stalled** status.

Data replication status

The source server **Data replication status** migration metric presents an aggregated overview of the application associated servers data replication status. You can look up an individual source server **Data replication status** status at the **Source servers** table at the bottom of the page.



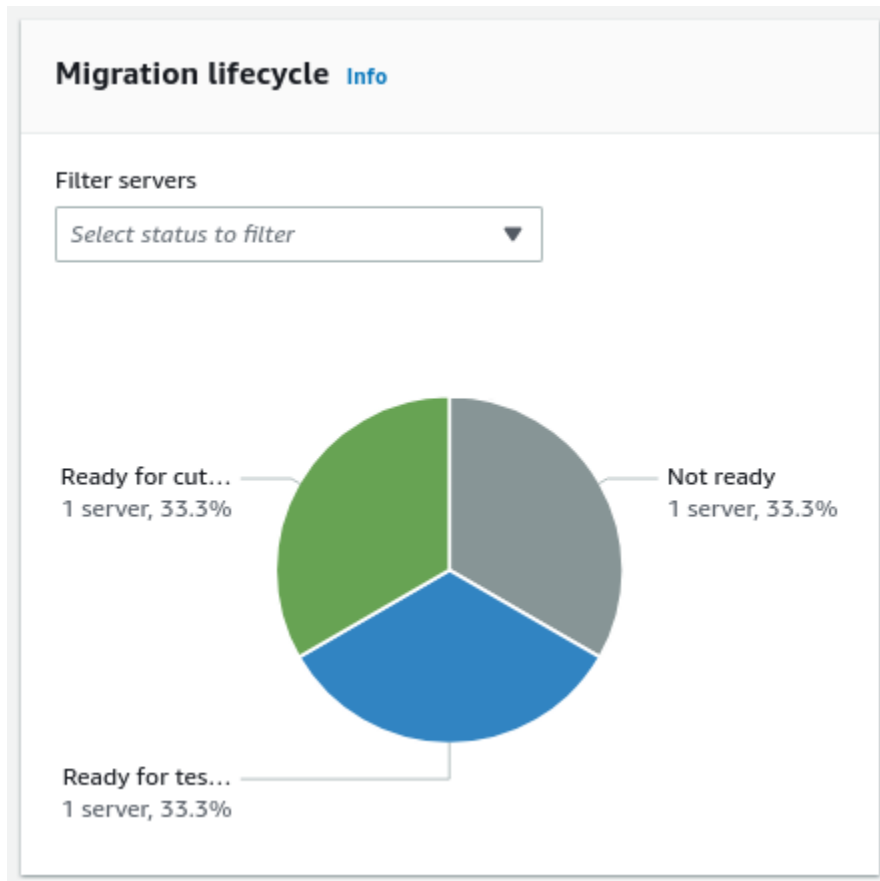
Source server **Data replication status** can have one of the following values:

- **Transferring snapshot**
- **Initial sync**
- **Finalizing sync**
- **Lagging**
- **Healthy**
- **Stalled**
- **Rescanning**
- **Not started**
- **Initiating**

- **Creating snapshot**
- **Paused**
- **Disconnected**

Migration lifecycle

The source server **Migration lifecycle** metric shows an aggregated overview of the application associated servers migration lifecycle. You can look up an individual source server **Migration lifecycle** status at the **Source servers** table at the bottom of the page.



Source server **Migration lifecycle** can have one of the following values:

- **Stopped**
- **Not ready**
- **Ready for testing**
- **Test in progress**
- **Ready for cutover**

- **Cutover in progress**
- **Cutover complete**
- **Disconnected**
- **Discovered**

Source servers table

The **Source servers** table lists all the servers that are associated with the application.

To perform batch operations on all the servers, use the application **Actions** menu at the top of the page. To perform an operation on a single server, go to the specific server's **Server details** page by clicking the server **Source server name**.

Source servers (3) Info							
<input type="text" value="Filter source servers by property or value"/>							
Source server name	Alerts	Migration lifecycle	Data replication status	Last snapshot	Next step	Archived	
14/not_ready (initial_sync)	-	Not ready	Initial sync 38% left	-	Wait for initial sync to complete	Active	
28/ready_for_test/shipping_snapshot	-	Ready for testing	Healthy	a day ago	Launch test instance	Active	
42/ready_for_cutover/shipping_snapshot	✔ Launched	Ready for cutover	Healthy	2 days ago	Terminate launched instance; Launch cutover instance	Active	

Tags

The **Tags** section shows any tags that have been assigned to the application. A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Learn more about AWS tags in [this Amazon EC2 article](#).

Tags (3)	
Key	Value
Tag1	value 1
Test key	test value
aws:tag:domain	beta

Waves

AWS Application Migration Service helps users manage their migration by grouping **Source servers** and **Applications** in **Waves**. These are logical groups, describing the migration plan over time.

You can:

- Monitor the wave's migration status, progress, and associated applications
- Perform operations on the wave, such as editing, tagging, and archiving
- Perform bulk operations on the applications associated with the wave

Topics

- [Waves page](#)
- [Wave details](#)

Waves page

The **Waves** page lists all the waves that have been added to AWS Application Migration Service (AWS MGN). The **Waves** page allows you to manage your waves and perform a variety of commands for one or more waves (such as controlling replication and launching test and cutover instances).

The screenshot shows the AWS Application Migration Service interface. The left-hand navigation menu has the 'Waves' option highlighted with a red box. The main content area displays a table of waves. The table has the following data:

Wave name	Migration status	Alerts	Number of applications
MGN-6583	Not started	Healthy	0
w12	Completed	Healthy	1
Wave 1	In progress	Healthy	193

Additional details from the screenshot include: 'Waves (3) Info' header, 'Active waves' dropdown, search filter 'Filter waves by property or value', and 'Last update: October 11, 2022 at 11:08 (UTC+5:00)'.

Topics

- [Interacting with the Waves page](#)
- [Commands menu](#)

- [Filtering](#)

Interacting with the Waves page

The **Waves** page shows a list of waves. Each row on the list represents a single wave.

Application Migration Service > Waves

Waves (3) Info

Active waves

<input type="checkbox"/>	Wave name	Migration status	Alerts	Number of applications
<input type="checkbox"/>	MGN-6583	Not started	Healthy	0
<input type="checkbox"/>	w12	Completed	Healthy	1
<input type="checkbox"/>	Wave 1	In progress	Healthy	193

The **Waves** page provides key information for each wave under each of the columns on the page.

The columns include:

- **Selector column** – This blank checkbox selector column allows you to select one or more waves. When a wave is selected, you can interact with the wave through the **Actions** menu, **Edit**, and **Delete** buttons. Selected waves are highlighted.

Application Migration Service > Waves

Waves (3) Info

Active waves

<input type="checkbox"/>	Wave name	Migration status	Alerts	Number of applications
<input checked="" type="checkbox"/>	MGN-6583	Not started	Healthy	0
<input checked="" type="checkbox"/>	w12	Completed	Healthy	1
<input type="checkbox"/>	Wave 1	In progress	Healthy	193

- **Wave name** – This column shows the unique wave name for each wave.

Application Migration Service > Waves

Waves (3) Info

Active waves

<input type="checkbox"/>	Wave name	Migration status	Alerts	Number of applications
<input type="checkbox"/>	MGN-6583	Not started	Healthy	0
<input type="checkbox"/>	w12	Completed	Healthy	1
<input type="checkbox"/>	Wave 1	In progress	Healthy	193

- **Migration status** – This column shows the migration status for each wave.

Application Migration Service > Waves

Waves (3) Info

Active waves Filter waves by property or value

Wave name	Migration status	Alerts	Number of applications
MGN-6583	Not started	Healthy	0
w12	Completed	Healthy	1
Wave 1	In progress	Healthy	193

- **Not started** – If none of the wave's associated servers has started replication yet.
- **In progress** – At least one of the wave's associated applications has started replication and not all of its applications completed migration.
- **Completed** – If all the wave associated applications completed migration (have been cutover).
- **Alerts** – This column shows whether any alerts exist for the wave.

Application Migration Service > Waves

Waves (3) Info

Active waves Filter waves by property or value

Wave name	Migration status	Alerts	Number of applications
MGN-6583	Not started	Healthy	0
w12	Completed	Healthy	1
Wave 1	In progress	Healthy	193

A wave that has at least one application that is experiencing significant issues, such as a stall, will display a **Stalled** status.

An wave that has at least one application that is experiencing a temporary issue such as lag or backlog will display a **Lagging** status.

A healthy active wave will display a **Healthy** status.

Archived waves do not display any alerts.

- **Number of applications** – This column shows the total number of applications associated with each wave.

Application Migration Service > Waves

Waves (3) Info

Active waves Filter waves by property or value

Actions Edit Delete Add wave

Wave name	Migration status	Alerts	Number of applications
MGN-6583	Not started	Healthy	0
w12	Completed	Healthy	1
Wave 1	In progress	Healthy	193

Commands menu

Use the commands menu to add waves, perform a variety of actions, and manage your testing and cutover for one or more waves.

Topics

- [Add wave](#)
- [Edit wave](#)
- [Delete wave](#)
- [Actions menu](#)

Add wave

To add a wave, click the **Add wave** button. You will then see the **Add wave** prompt that includes the following parameters:

- **Wave name** – Select a wave name. The name must be unique per account per region. Note that uniqueness verification for wave name in Migration Application Service is case-insensitive.
- **Description (optional)** – Add a description of the wave according to your preferences.
- **Associate applications (optional)** – You can add up to 200 applications to a single wave. Checking an application in the dropdown list will associate it with the wave.
- **Add tags (optional)** – You can up to 50 tags according to your preferences.

Application Migration Service > Waves > Add wave

Add wave [Info](#)

Wave settings

Wave name

Description - optional

Applications
Select applications to associate with this wave.

An application may be associated with a single wave.

Wave tags - optional
No tags associated with the resource.

You can add up to 50 more tags.

[Cancel](#)

Click **Add wave** to create the wave.

Edit wave

To edit a wave, click **Edit wave**. You will see the **Edit wave** prompt, which allows you to edit the following parameters:

- **Wave name** – Select a wave name. The name must be unique per account per region. Note that uniqueness verification for wave name in Migration Application Service is case-insensitive.
- **Description (optional)** – Add a description of the wave according to your preferences.

- **Associate applications (optional)** – You can add up to 200 applications to a single wave. Checking an application in the dropdown list will associate it with the wave.
- **Add tags (optional)** – You can up to 50 tags according to your preferences.

Application Migration Service > Waves > Edit wave

Edit wave [Info](#)

Wave settings

Wave name

Description - *optional*

Applications

Select applications to associate with this wave.

App-193 ×

An application may be associated with a single wave.

Wave tags - *optional*

No tags associated with the resource.

You can add up to 50 more tags.

[Cancel](#) [Save changes](#)

After you edit the parameters as required, click the **Save changes** button to save your changes.

Delete wave

To delete a wave, click the **Delete wave** button and the **Delete wave** prompt will open. You will need to verify that you want to delete the selected wave.

When you delete the wave, all associated applications will disassociate from the wave but will not be deleted.

Click **Delete** to confirm the deletion.

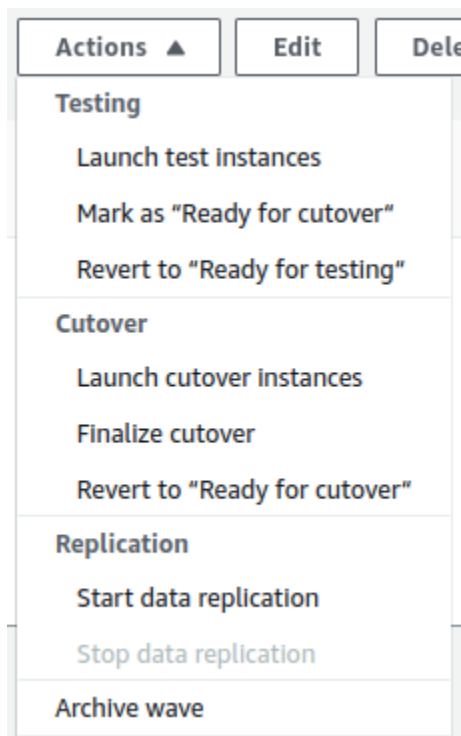
Actions menu

The **Actions** menu allows you to perform actions on selected waves.

Note

A wave must have **all** of its associated servers in the correct lifecycle for the desired action, otherwise it will be excluded.

Use this menu to perform the following actions:



- **Launch test instances** – Choose this option to launch test instances for this wave servers.

- **Mark as "Ready for cutover"** – Choose this option to finalize testing for this wave after you have completed all the necessary tests in preparation for cutover.

Once the **Mark servers as "Ready for cutover"** dialog will appear, select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Continue**.

- **Revert to "ready for testing"** – Choose this option to revert a finalized test for this wave if you want to run additional tests prior to initiating a cutover.

The **Revert testing** dialog will appear. Select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Revert**.

- **Launch cutover instances** – Choose this option to launch cutover instances for this wave servers after you have finalized all of your testing and are ready to initiate a cutover.
- **Finalize cutover** – Choose this option to finalize the cutover for this wave servers after you have successfully performed a cutover.

Note

This action does not uninstall the AWS Replication Agent from the source servers. When you have completed the migration and want to uninstall the agent from your source servers, go to **Source servers** page and select the relevant servers. Use the **Disconnect from service** option under the **Actions** menu.

- **Revert to "ready for cutover"** – Choose this option to revert a finalized cutover for this wave if you encounter any issues or want to reverse the cutover for any reason.
- **Start data replication** – Choose this option to start replication of the wave source servers.

Note

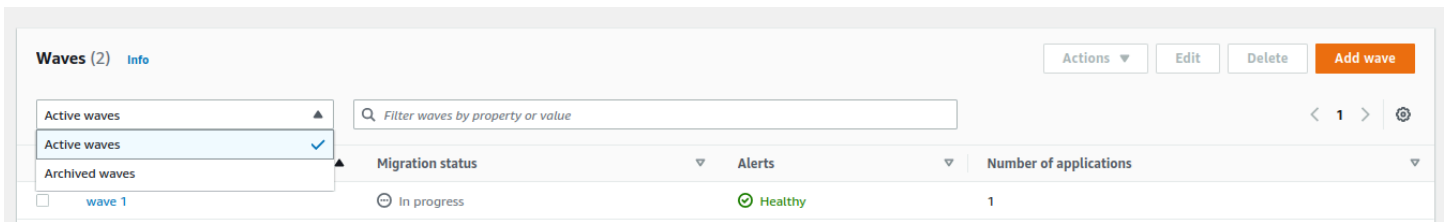
This action is applicable if all the wave's associated servers are **Agentless snapshot based** and are in **Discovered** lifecycle state.

- **Archive waves** – Choose this option to archive the selected waves. You should only archive waves for which you have already performed a cutover.

⚠ Important

A wave can be archived only if all servers that are part of in one of these states: archived, cutover or disconnected. If that is the case, the wave and its associated applications will be archived. The servers that are not yet archived (but can be) will also be archived.

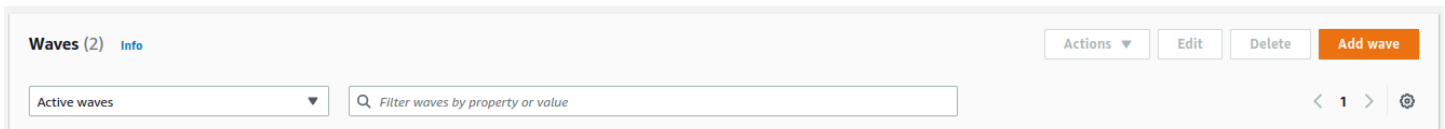
- Archived waves will be removed from the main Waves page, but can still be accessed through the selector options.



Filtering

Use filtering to easily filter your waves by one or multiple properties.

Click within the **Filter waves** field and choose the filtering property from the **Properties** menu.



You can filter by a variety of properties, including:

Properties
Wave name
Wave ID
Migration status
Alerts
Number of applications
Tags
Test key
aws:tag:domain

- Wave name – Filter by wave name.
- Wave ID – Filter by wave ID.
- Migration status – Filter by the migration status (Not started, In progress, Completed).
- Alerts – Filter by health status alert (Stalled, Lagging, Healthy).
- Number of applications – Filter by a number of applications.
- Tags – Filter by tags. Relevant specific tag values will appear under the **Tags** category. Choose the value to filter by.

You can filter by multiple properties at once in order to narrow down your results.

Here you see an example of filtering the waves list by several properties:

Waves (2) Info

Active waves

Filter waves by property or value

Alerts = Healthy and Number of applications = 1

Clear filters

Wave name	Migration status	Alerts	Number of applications
wave 1	In progress	Healthy	1

Last update: October 11, 2022 at 12:36 (UTC+3:00)

To clear the selected filtering properties, click **Clear filters**.

Wave details

There are several ways you can access the **Wave details** view.

Click the **Wave name** of any wave on the **Waves** page.

Waves (2) Info

Active waves

Filter waves by property or value

Wave name	Migration status	Alerts	Number of applications
wave 1	In progress	Healthy	1

Click the **Wave** of any application on the **Applications** page.

Applications (3) Info

Active applications

Filter applications by property or value

Application name	Wave name	Migration status	Alerts	Number of servers
App 1	Wave 2	In progress	Healthy	3

Click the **Wave name** in the **Overview** dashboard inside **Application details** of an application.

App 2 (app-083181d1ef5a1ea8d) Actions ▾ Edit Delete

Overview [Info](#)

Description App 2 description	Last status update October 11, 2022 at 13:06 (UTC+3:00)	Migration status ⊖ In progress
State Active	Wave name wave 1	Alerts ⊕ Healthy

The **Wave details** view shows information and options for an individual wave. Here, you can control and monitor the individual wave.

Application Migration Service > Waves > MGN-6583

MGN-6583 (wave-322545120585b477f) Actions ▾ Edit Delete

Overview [Info](#)

Description This is the wave description.	Wave start time September 29, 2022 at 12:02 (UTC+3:00)	Migration status ⊖ In progress
State Active	Current duration 13 days	Alerts ⊕ Healthy
Last status update October 12, 2022 at 09:53 (UTC+3:00)		

Applications | Source servers | Tags

Alerts [Info](#)

Filter applications

Health Status	Count	Percentage
Healthy	1 application	33.3%
Archived	2 applications	66.7%

Migration status [Info](#)

Filter applications

Migration Status	Count	Percentage
In progress	1 application	33.3%
Completed	2 applications	66.7%

You can also perform a variety of actions on the wave, and perform batch operations such as launch test and cutover instances for the servers associated with the wave.

The **Wave details** view is divided into several dashboards:

Topics

- [Overview dashboard](#)
- [Applications](#)

- [Source servers](#)
- [Tags](#)

Overview dashboard

The **Overview** dashboard provides an overview of the overall wave status, including:

Overview Info		
Description This is the wave description.	Wave start time September 29, 2022 at 12:02 (UTC+3:00)	Migration status 🔄 In progress
State Active	Current duration 12 days	Alerts 🟢 Healthy
Last status update October 11, 2022 at 15:03 (UTC+3:00)		

- **Description** – The description of the wave.
- **State** – The state of the wave. **State** can be in one of two states: **Active** or **Archived**
- **Last status update** – Time stamp of when wave status was updated (update occurs every five minutes).
- **Wave start time** – Time stamp of when the earliest replication started for a server associated with this wave.
- **Current duration** – Duration of replication time since **Wave start time**. If wave is archived, duration is until the moment the wave was archived.
- **Migration status** – The wave migration status.

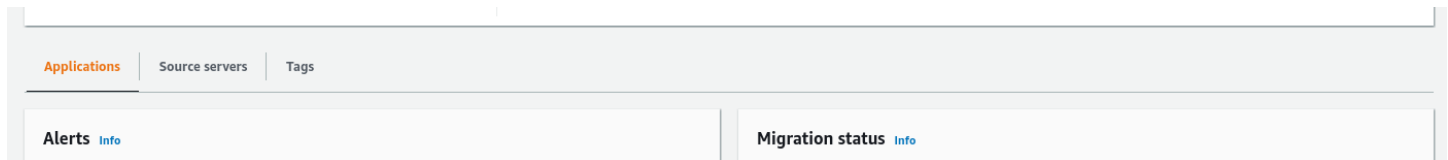
Wave **Migration status** can have one of the following values:

- **Not started** – If none of its applications has started replication yet.
- **Completed** – If all of its applications completed migration (have been cutover).
- **In progress** – At least one of its applications has started replication and not all of its applications completed migration.
- **Alerts** – The wave alert.
 - A wave that has at least one application that is experiencing significant issues, such as a stall, will display a **Stalled** status.
 - A wave that has at least one application that is experiencing a temporary issue such as lag or backlog will display a **Lagging** status.
 - A healthy active wave will display a **Healthy** status.

- An archived wave will not display a status.

Applications

The **Applications** tab shows migration metrics aggregating statuses as well as a list of all the wave associated applications.



Topics

- [Application migration metrics](#)
- [Applications table](#)

Application migration metrics

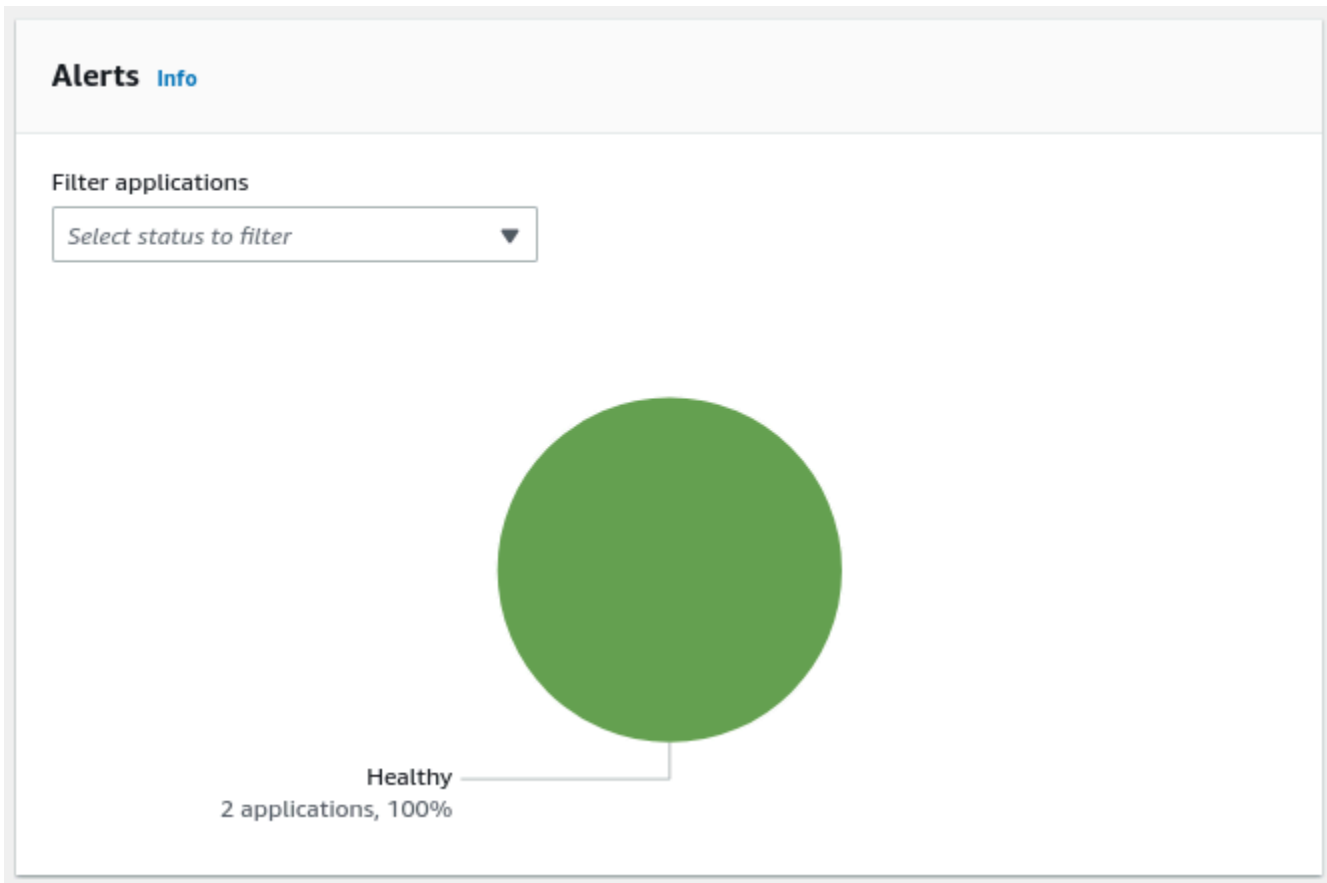
The application migration metrics show an aggregated overview of the wave's associated servers on two topics: **Alerts** and **Migration status**.

Topics

- [Alerts](#)
- [Migration status](#)

Alerts

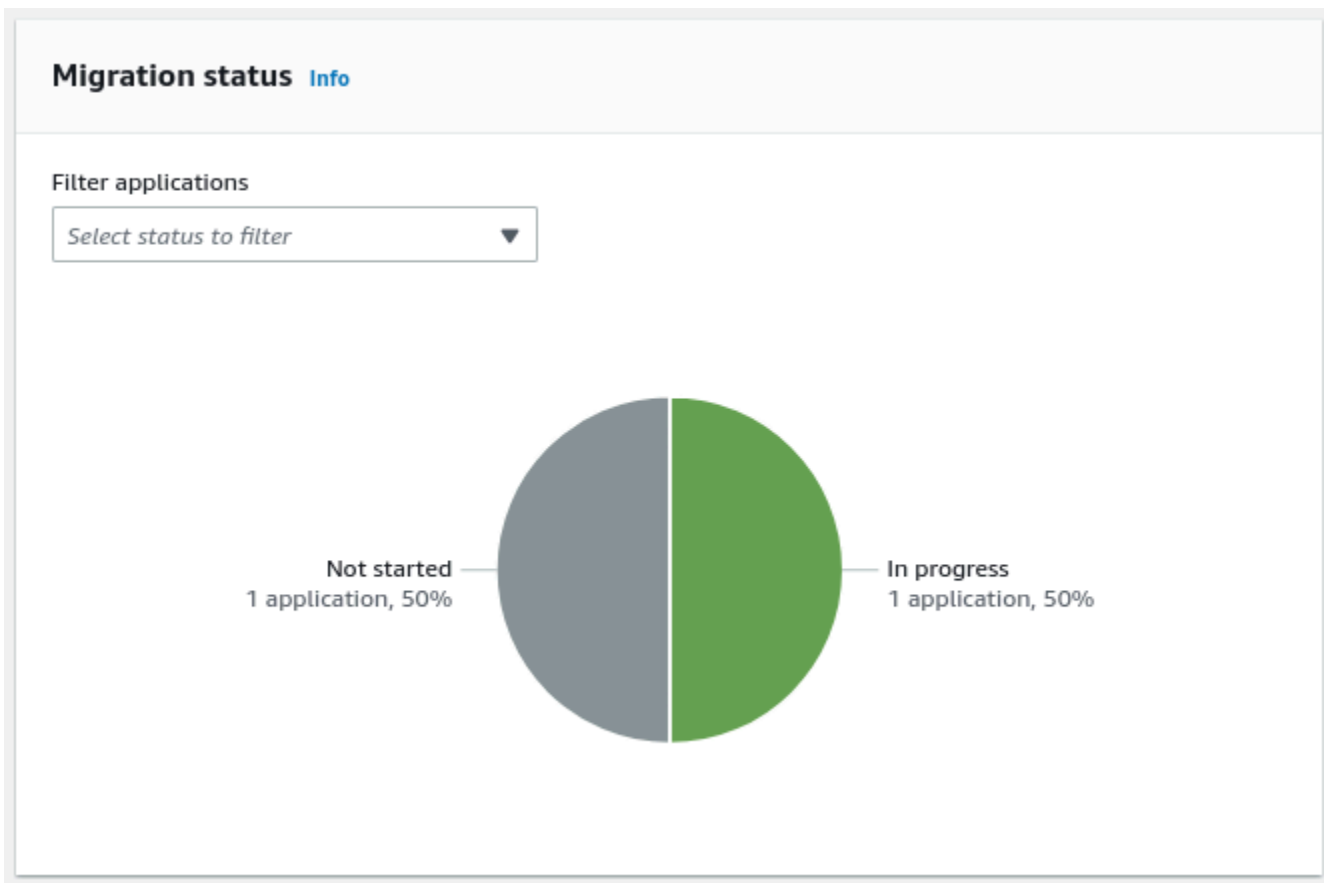
The application **Alerts** metric provides an aggregated overview of the alerts related to the wave's associated applications. You can look up an individual application **Alerts** status at the **Applications** table at the bottom of the page.



- A healthy application will display a **Healthy** status.
- An application that is experiencing a temporary issue such as lag or backlog will display a **Lagging** status.
- An application that is experiencing significant issues, such as a stall, will display a **Stalled** status.

Migration status

The application **Migration status** metric provides an aggregated overview of the migration status of the wave's associated applications. You can look up an individual application **Migration status** status at the **Applications** table at the bottom of the page.



Application **Migration status** can have one of the following values:

- **Not started**
- **In progress**
- **Completed**

Applications table

The **Applications** table lists all the applications that are associated with the wave.

You can perform batch operations on all the applications via the wave **Actions** menu at the top of the page. You can perform an operation on a single application from its own **Application details** page, by clicking the application's **Application name**.

Applications (2) Info					
<input type="text" value="Filter source servers by property or value"/>					< 1 > ⚙️
Application name	Migration status	Alerts	Number of servers	Archived	
App 1	⊖ In progress	✔️ Healthy	3	Active	
App 3	⊖ Not started	✔️ Healthy	0	Active	
Last update: October 11, 2022 at 15:32 (UTC+3:00)					

Source servers

The **Source servers** tab shows migration metrics aggregating statuses as well as a list of all the wave's associated applications.

Applications	Source servers	Tags
Alerts Info	Data replication status Info	Migration lifecycle Info

Topics

- [Source server migration metrics](#)
- [Source servers table](#)

Source server migration metrics

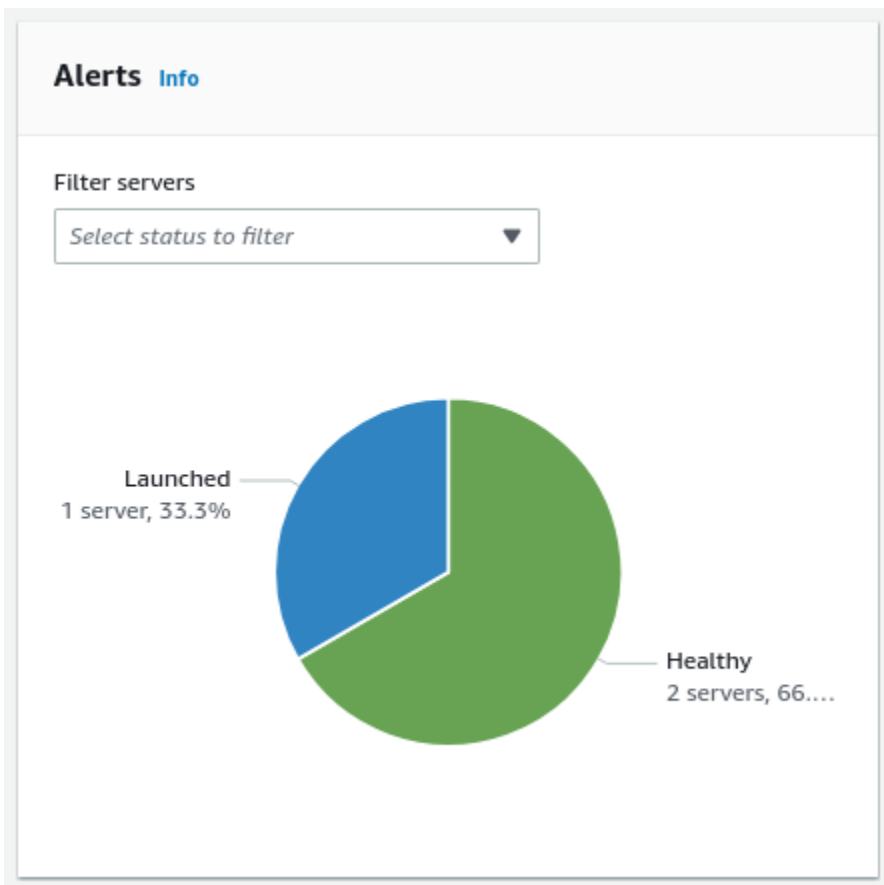
The source server migration metrics provide an aggregated overview of the wave's associated servers on three topics: **Alerts**, **Data replication status**, and **Migration status**.

Topics

- [Alerts](#)
- [Data replication status](#)
- [Migration lifecycle](#)

Alerts

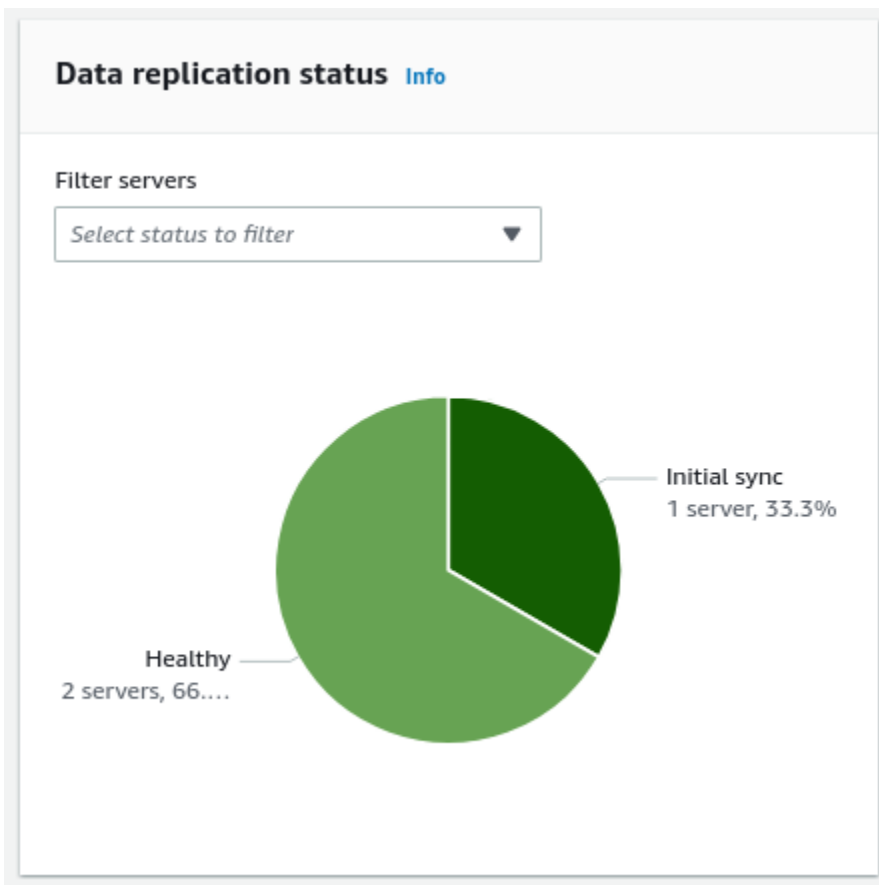
The source server **Alerts** metric provides an aggregated overview of the alerts related to the wave's associated servers. You can look up an individual source server **Alerts** status at the **Source servers** table at the bottom of the page.



- A healthy server for which a test or cutover instance has not been launched will display a **Healthy** status.
- A healthy server for which a test or cutover instance has been launched will display a **Healthy** status.
- A server that is experiencing a temporary issue such as a lag or backlog will display a **Lagging** status.
- A server that is experiencing significant issues, such as a stall, will display a **Stalled** status.

Data replication status

The source server **Data replication status** metric provides an aggregated overview of the data replication status of the wave's associated servers. You can look up an individual source server **Data replication status** status at the **Source servers** table at the bottom of the page.

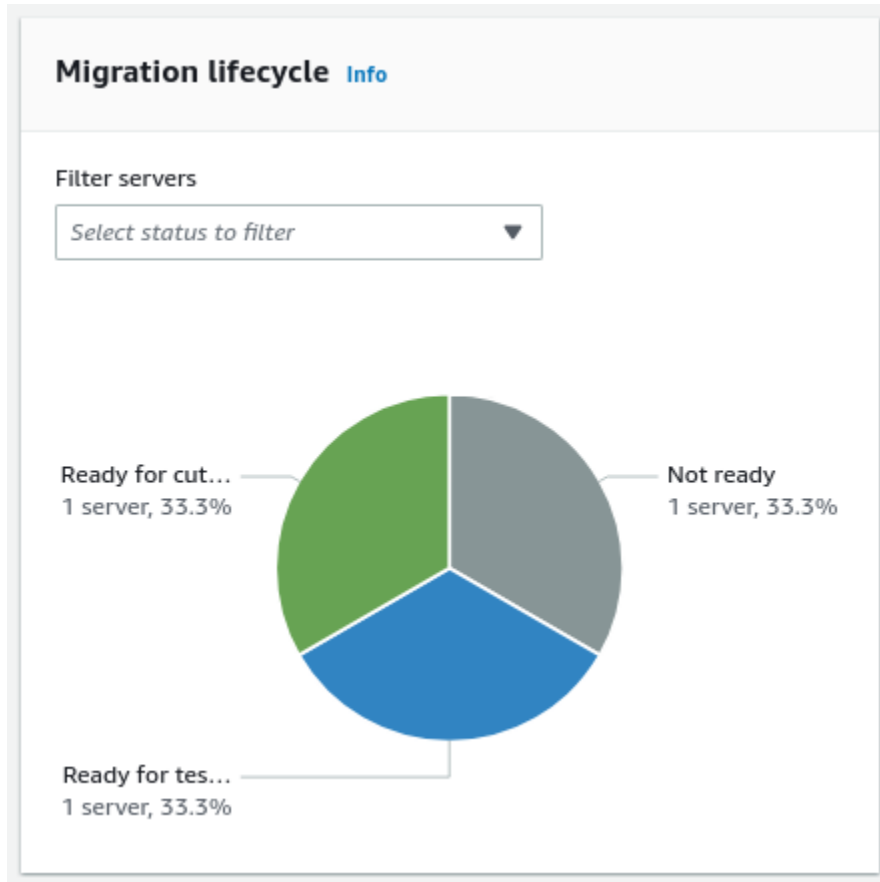


Source server's **Data replication status** can have one of the following values:

- **Transferring snapshot**
- **Initial sync**
- **Finalizing sync**
- **Lagging**
- **Healthy**
- **Stalled**
- **Rescanning**
- **Not started**
- **Initiating**
- **Creating snapshot**
- **Paused**
- **Disconnected**

Migration lifecycle

The source server's **Migration lifecycle** metric provides an aggregated overview of the migration lifecycle of the wave's associated servers. You can look up an individual source server's **Migration lifecycle** status at the **Source servers** table at the bottom of the page.



The source server's **Migration lifecycle** can have one of the following values:

- **Stopped**
- **Not ready**
- **Ready for testing**
- **Test in progress**
- **Ready for cutover**
- **Cutover in progress**
- **Cutover complete**
- **Disconnected**
- **Discovered**

Source servers table

The **Source servers** table lists all the servers that are associated with the wave.

You can perform batch operations on all the servers via the wave **Actions** menu at the top of the page. You can perform an operation on a single server from its own **Server details** page, by clicking on the server **Source server name**.

Source servers (3) Info							
<input type="text" value="Filter source servers by property or value"/> < 1 > 							
Source server name ▲	Alerts ▼	Migration lifecycle ▼	Data replication status ▼	Last snapshot ▼	Next step ▼	Archived ▼	
14: not_ready (initial_sync)	-	Not ready	Initial sync 38% left	-	Wait for initial sync to complete	Active	
28/ready_for_test/shipping_snapshot	-	Ready for testing	Healthy	a day ago	Launch test instance	Active	
42/ready_for_cutover/shipping_snapshot	✔ Launched	Ready for cutover	Healthy	2 days ago	Terminate launched instance; Launch cutover instance	Active	

Tags

The **Tags** section shows any tags that have been assigned to the wave. A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs. Learn more about AWS tags in [this Amazon EC2 article](#).

Applications Source servers Tags	
Tags (2)	
Key	Value
Test key	test value
aws:tag:domain	dev

MGN Connectors

Large-scale migrations, involving many source servers, often require preparation and planning. The source servers may have a wide variety of operating system version, and may be distributed across multiple data centers.

Before the migration execution can begin, various actions may need to be performed, for example:

- Verifying the prerequisites to install the MGN replication agent on the source servers.
- Installing the AWS MGN replication agents on the source servers.

To address these needs, AWS Application Migration Service offers the MGN connector – a feature that allows you to automate running commands on your source environment.

You can install the AWS MGN connector in your source environment and use it to perform actions on source servers in your data center.

This feature, combined with the post-launch action framework, offers automation across the entire deployment process.

Topics

- [Prerequisites for installing the MGN connector](#)
- [Architecture overview when using MGN connector](#)
- [Permissions](#)
- [Setup instructions](#)
- [Installing the MGN connector on a secured network](#)
- [MGN Connectors page](#)
- [MGN connector details](#)

Prerequisites for installing the MGN connector

Installing the MGN connector requires a dedicated Linux server. The MGN connector can be deployed on the same server that hosts the MGN vCenter Client installer (agentless appliance). This server should be used only for the MGN connector and MGN agentless appliance, and should not be used for any other purposes.

The MGN connector can be installed on servers running the following Linux versions:

- Ubuntu 18.x+ (64 bit) - 22.04 (x86_64)
- Amazon Linux 2 (x86_64)
- RHEL8.x (x86_64)

In order to utilize AWS Application Migration Service connector, you must meet the following prerequisites:

- openssl

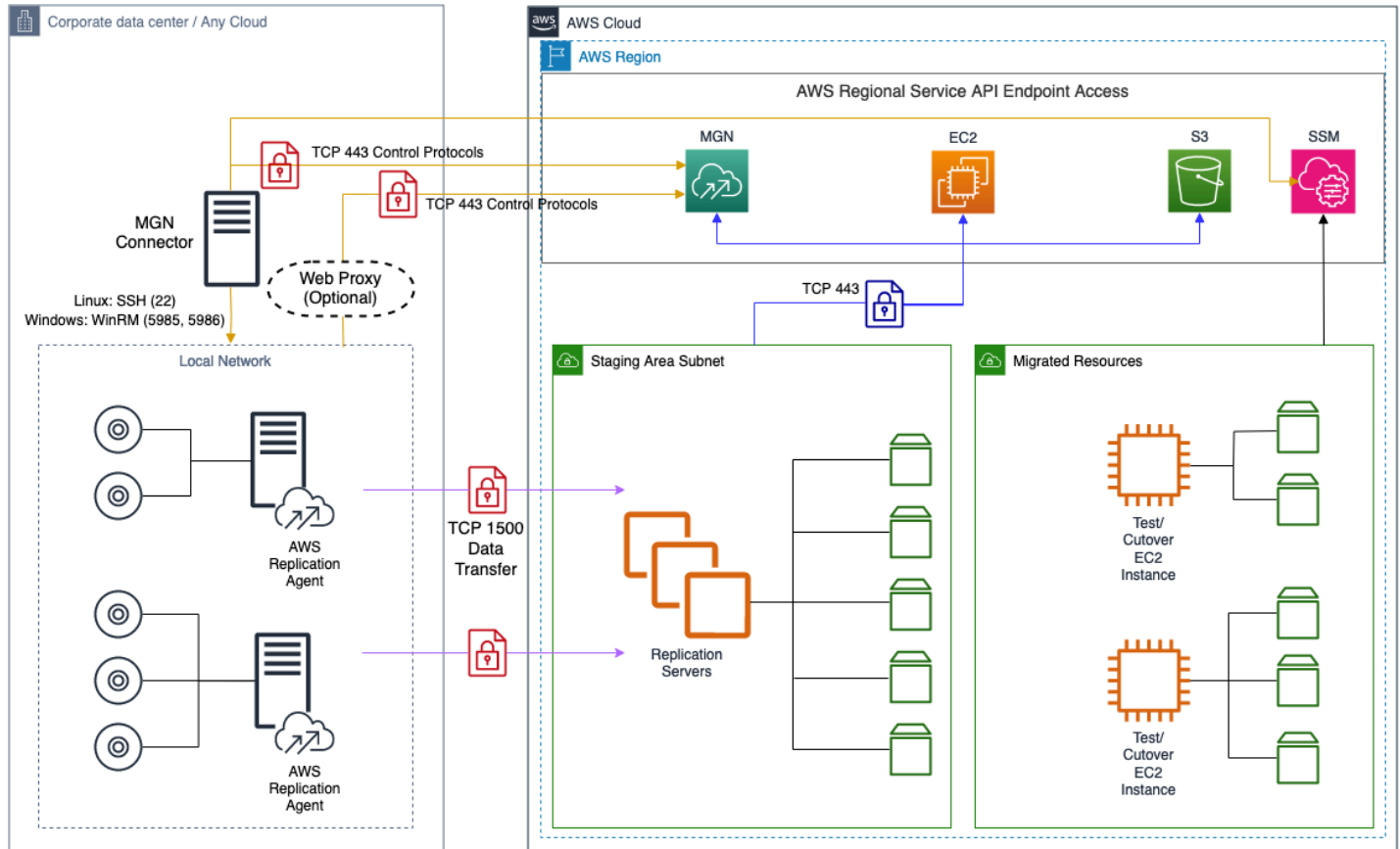
The AWS MGN vCenter Client installer can only be installed on Ubuntu 18 64 bit, RHEL8 or AL2 VMs.

If the SSM agent is installed, it must be removed before installing the MGN connector. See [Uninstalling SSM Agent from Linux instances](#) in the *AWS Systems Manager User Guide*.

In addition, you must also have the required [permissions](#).

Architecture overview when using MGN connector

The following is the architecture overview when using AWS MGN with MGN connector.



Permissions

In order to use the MGN connector, you must have the required permissions.

For security best practices, it is recommended that the MGN connector will be accessed only by allowed personnel and will have the required OS patches. It is also recommended that the servers to which the MGN connector connects, will have all the required OS patches.

If you configure outputting logs to S3, it is recommended to apply S3 bucket security practices - following AWS official reference to [S3 security practices](#)

You need to create the following IAM roles:

MGNConnectorInstallerRole

The MGNConnectorInstallerRole role is used to install the Connector. The user or identity that installs the Connector will require permission to assume this role. To create the role:

1. Create a policy from the following JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mgn:CreateConnector",
        "mgn:TagResource"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

2. Name the policy **MGNConnectorInstallerPolicy**
3. Create a role with your account as the trusted entity. Alternatively use a custom trust policy that will grant the user or identity that will install the Connector, permission to assume this role.
4. Attach the **MGNConnectorInstallerPolicy** policy to the Permission policies.
5. Name the role **MGNConnectorInstallerRole**

AWSApplicationMigrationConnectorManagementRole

The AWSApplicationMigrationConnectorManagementRole role is the role that is initially assumed by the Connector. To create the role:

1. After replacing **ACCOUNT-ID** with your account number, create a policy from the following JSON:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": "sts:AssumeRole",
```

```

        "Resource": "arn:aws:iam::*:role/
AWSApplicationMigrationConnectorSharingRole_ACCOUNT-ID",
        "Effect": "Allow"
    },
    {
        "Condition": {
            "Null": {
                "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
            }
        },
        "Action": "secretsmanager:GetSecretValue",
        "Resource": "arn:aws:secretsmanager::*:secret:*",
        "Effect": "Allow"
    }
]
}

```

2. In order for the MGN connector to send logs to S3, append the following statement to the above policy:

```

{
    "Action": [
        "s3:GetObject",
        "s3:PutObject"
    ],
    "Resource": "*",
    "Effect": "Allow"
}

```

3. In order for the MGN connector to send logs to CloudWatch, append the following statement to the above policy:

```

{
    "Effect": "Allow",
    "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:PutLogEvents",
        "logs:GetLogEvents",
        "logs:FilterLogEvents"
    ],
}

```



```
"Resource": "*"
}
```

4. Name the policy **MgnConnectorPolicy**
5. Create a role with the following trust relationship:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. Attach the following policies:
 - a. **AmazonSSMManagedInstanceCore**
 - b. **MgnConnectorPolicy**
7. Name the role **AWSApplicationMigrationConnectorManagementRole**

Setup instructions

In order to set up your MGN connector, take the following steps:

1. Make sure your account have the required permissions as defined [here](#).
2. If the MGN connector manages source servers from multiple accounts, set up the global view feature and set up your AWS Organization, following the instructions [here](#).

After you set up your AWS Organization, configure the CloudFormation StackSet in order to create the required role per management account. Use the template "Enable Application Migration Service Connector access". Full instructions are available [here](#).

3. If the MGN connector manages source servers from a single account, and both the MGN connector and the source servers belong to the same account:

- a. After replacing **ACCOUNT-ID** with your account number, create a role using the following trust policy:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::ACCOUNT-ID:role/
AWSApplicationMigrationConnectorManagementRole"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

- b. Attach the **AWSApplicationMigrationAgentInstallationPolicy** policy to the Permission policies.
 - c. Name the role **AWSApplicationMigrationConnectorSharingRole_ACCOUNT-ID** (replace **ACCOUNT-ID** with your account number).
4. [Create a new MGN connector](#) on the MGN connectors page.

Installing the MGN connector on a secured network

The MGN connector and the AWS Replication Agents that the MGN connector installs, require network access to various AWS endpoints. If your on-premises network is not open to AWS endpoints, then you can install the MGN connector and the AWS Replication Agents with the aid of PrivateLink.

You can connect your on-premises network to your VPCs using AWS VPN or DirectConnect.

Global view

If you are using the [Global view](#) feature, which provides cross-account view and operations, you will have at least one staging VPC per member account.

You will also need to designate a VPC in the management account in order to allow the MGN connector to communicate with AWS services via PrivateLink. If you are migrating some of your source servers into the management account, you can use the same VPC as a staging VPC.

The following sections apply to the MGN connector VPC as well as to each staging VPC.

Create VPC endpoints

To allow the MGN connector and AWS Replication Agents to communicate with AWS services, create the VPC endpoints listed below. For each endpoint:

1. Select your staging area VPC or MGN connector VPC (see [Global view](#) above).
2. **Enable private DNS names.**
3. Choose a subnet, and ensure that a route exists from the MGN connector or AWS Replication Agent to the selected subnet.
4. Ensure that the security groups associated with the endpoint allow inbound traffic from the MGN connector and source servers.

Create the following interface endpoints:

1. **com.amazonaws.*region*.ssm** – The endpoint for the Systems Manager service. This endpoint is required by the SSM Agent, which is installed by the MGN connector installer.
2. **com.amazonaws.*region*.ec2messages** – Systems Manager uses this endpoint to make calls from the SSM Agent to the Systems Manager service.
3. **com.amazonaws.*region*.ssmmessages** – This endpoint is required only if you wish to connect to the MGN connector using Session Manager.
4. **com.amazonaws.*region*.kms** – This endpoint is required only if you wish to connect to the MGN connector using Session Manager and using AWS KMS encryption to add an additional layer of encryption to the session. For more information, see [Turn on KMS key encryption of session data](#) in the *Amazon Systems Manager User Guide*.
5. **com.amazonaws.*region*.s3** – Systems Manager uses this endpoint to update the SSM Agent and to perform patching operations. The MGN connector installer and the AWS Replication Agent installer download installation assets from this endpoint.
 - a. Note that private DNS names are disabled by default for the S3 endpoint.
 - b. If you wish to also **Enable private DNS only for inbound endpoint**, you must first create an S3 gateway VPC endpoint. For more information, see [S3 Private DNS](#) in the *Amazon Simple Storage Service User Guide*.
6. **com.amazonaws.*region*.secretsmanager** – The MGN connector calls this endpoint to retrieve source server credentials.

7. **com.amazonaws.region.sts** – The MGN connector calls this endpoint to retrieve credentials of the AWS Replication Agent installer role.
8. **com.amazonaws.region.mgn** – The endpoint for MGN. This endpoint is required by the MGN connector, the AWS Replication Agent, and their respective installers. If a VPCE Policy is used (to scope down access), add the following statement to your policy:

```
{
  "Effect": "Allow",
  "Principal": "*",
  "Action": "execute-api:Invoke",
  "Resource": "arn:aws:execute-api:<region>:*:*/POST/CreateSessionForMgn"
}
```

For more information, see [Creating an interface endpoint](#) in the *Amazon VPC User Guide*.

Create a Route 53 inbound endpoint

To route your traffic to the VPC endpoints created above, create a Route 53 inbound endpoint in your staging area VPC or the MGN connector VPC (see [Global view](#) above).

Ensure that the security group associated with the inbound endpoint allows traffic from your on-premises DNS resolvers.

Configure DNS resolvers on your on-premises network to forward DNS queries for the endpoints of the above AWS services, to the IP addresses of your Route 53 inbound endpoint. To find the regional endpoints of these services, see [Service endpoints](#) in the *AWS General Reference Guide*. For example, the endpoint of the MGN service in the US East (Ohio) Region (us-east-2) is **mgn.us-east-2.amazonaws.com**

For more information, see [Forwarding inbound DNS queries to your VPCs](#) in the *Amazon Route 53 User Guide*.

Modify replication settings

In order to allow the AWS Replication Agent to communicate with the replication server without using the public internet, you must use Private IP for data replication. The replication server requires access to the EC2 service. Therefore:

- If your staging area VPC has a VPC endpoint for `com.amazonaws.region.ec2` with private DNS names enabled, or if your staging area subnet has a route to the public internet via a NAT gateway, then the replication server can communicate with EC2 over its private IP. Choose the option:

Use private IP for data replication

- Otherwise, if your staging area subnet has a route to the public internet via an internet gateway, a public IP is required for the replication server to reach EC2. Choose the option:

Create public IP, and use Private IP for data replication

Ensure that the security groups associated with the MGN VPC endpoint allow inbound traffic from the replication server.

Verify VPC endpoints are being used

Use CloudTrail to verify that calls to AWS services from the MGN connector and its associated source servers, are made via the `vpcEndpointIds` of the VPC endpoints you have created.

MGN Connectors page

The MGN connectors page lists all the installed MGN connectors, providing a quick overview of your MGN connectors and their status and allowing you to quickly perform actions.

The screenshot shows the AWS Application Migration Service console. The left sidebar contains navigation options for Source servers, Applications, Waves, Global view, Launch history, MGN connectors (selected), Import and Export, Settings, Containers, and AWS Migration Hub, Documentation, and Release Notes. The main content area is titled 'Application Migration Service > MGN connectors'. It features a 'How it works' section, a search bar, and a table of MGN connectors. The table has columns for Name, Registered source servers, and Last seen. Two connectors are listed: MGN Connector 1 (17 servers) and MGN Connector 2 (0 servers). Above the table are buttons for Actions, Edit, Delete, and Add MGN connector.

Name	Registered source servers	Last seen
MGN Connector 1	17	September 07, 2019 at 15:50 (UTC-4:00)
MGN Connector 2	0	September 07, 2019 at 15:50 (UTC-4:00)

Topics

- [Interacting with the MGN connector page](#)
- [Actions menu](#)

Interacting with the MGN connector page

The **MGN Connectors** page displays the list of MGN connectors, and supports adding, deleting and editing MGN connectors as well as performing actions using the MGN connectors.

The **MGN Connectors** page provides information for each MGN connector, including:

- **MGN Connector name** - The unique name for each MGN connector. Additional details of the MGN connector are available in the MGN details page. Click the MGN connector name, to view its details.
- **Registered servers** - The number of registered source servers managed by this MGN connector.
- **Last seen** - The last time AWS Application Migration Service communicated with the MGN connector.

The screenshot shows the AWS Application Migration Service console. The left sidebar contains navigation options like Source servers, Applications, Waves, Global view, Launch history, MGN connectors, Import and Export, Settings, Containers, AWS Migration Hub, Documentation, and Release Notes. The main content area is titled 'Application Migration Service > MGN connectors'. It features a 'How it works' section, a search bar for filtering connectors, and a table of existing connectors. The table has three columns: Name, Registered source servers, and Last seen. Two connectors are listed: 'MGN Connector 1' with 17 registered source servers and 'MGN Connector 2' with 0 registered source servers. Both were last seen on September 07, 2019 at 15:50 (UTC-4:00). Above the table are buttons for 'Actions', 'Edit', 'Delete', and 'Add MGN connector'.

Name	Registered source servers	Last seen
MGN Connector 1	17	September 07, 2019 at 15:50 (UTC-4:00)
MGN Connector 2	0	September 07, 2019 at 15:50 (UTC-4:00)

Actions menu

Use the actions menu to manage your MGN connector.

Topics

- [Add MGN connector](#)
- [Edit connector](#)
- [Delete MGN connector](#)
- [Actions menu](#)

Add MGN connector

To add an MGN connector, click **Add MGN connector**, to open the Add MGN connector page. Set up your MGN connector by providing the following:

- **Connector name:** The MGN connector name is used to identify the connector. This field is mandatory, and limited to 256 characters. The name must be unique (case-insensitive) per account per Region.

- Obtain the SSM hybrid activation parameters (installation key and ID), which is required in order install the SSM agent on the MGN connector. For more information on SSM activation parameters see [here](#).
- In the SSM hybrid activation set the `AWSApplicationMigrationConnectorManagementRole` in the management account.
- Activation setting → select an existing IAM role → `AWSApplicationMigrationConnectorManagementRole`
- See the [permissions](#) page for the required permissions of `AWSApplicationMigrationConnectorManagementRole`.
- Temporary IAM credentials of the `MGNConnectorInstallerRole` role that you created [here](#).
- Request temporary security credentials [through AWS STS](#) through the [AssumeRole API](#).
- [Learn more about how temporary credentials work](#).

To download the MGN connector software, use the following commands:

- **Download the installer command** - Copy and paste the command into the command prompt of the server you've designated for the MGN connector. This will download the AWS MGN installer.
- **Copy and paste this command into the command line on your MGN connector** - Copy and paste the command into the command prompt of the same server. This will install the AWS MGN connector software.

After the MGN connector is installed it automatically begins communicating with the console and appears in the MGN connectors list.

Next, you must register source servers to the MGN connector.

You may install multiple MGN connectors to handle large amount of source servers or multiple data centers. Each MGN connector is able to handle up to 500 source servers. AWS MGN supports up to 50 MGN connectors per account per region.

Edit connector

To edit an MGN connector, click **Edit**. When the **Edit MGN connector** page opens, you can modify the MGN connector name and tags.

To finalize your changes, click **Save changes**.

Delete MGN connector

To delete an MGN connector, click **Delete**. When the **Delete MGN connector** dialog opens, verify that you want to delete the selected MGN connector. Once an MGN connector is uninstalled, it can no longer be used to manage your source servers.

Note

Deleting the MGN connector will disassociate the servers from the MGN connector, but will not delete them from servers inventory.

Actions menu

The **Actions** menu allows you to perform various actions on the selected MGN connector.

• Register server credentials

- Once you have the MGN connector set up and ready to use, you can register source servers to the MGN connector. To do so click on the MGN connector name, then click "Register servers".
- The servers list contain the source servers that were imported via the import feature or discovered by the agentless replication process.
- Select the source servers you want to register to the MGN connector. Click the "Register servers with the MGN connector" button.

The screenshot shows the AWS Application Migration Service console. The breadcrumb navigation is: Application Migration Service > MGN connectors > connector-12345678901234568 > Register servers. The main content area displays a table of servers (23 total) with a search filter and pagination controls. The table has columns for Source server name, Account, Wave, and Application. Three servers are selected with checkboxes: 11: not_ready (initiating), 12: not_ready (initiating) - had error, and 13: not_ready (initiating). At the bottom right, there are 'Cancel' and 'Register servers with the MGN connector' buttons.

Source server name	Account	Wave	Application
<input checked="" type="checkbox"/> 11: not_ready (initiating)	123456789012	-	-
<input checked="" type="checkbox"/> 12: not_ready (initiating) - had error	123456789012	-	-
<input checked="" type="checkbox"/> 13: not_ready (initiating)	123456789012	-	-
<input type="checkbox"/> 15: not_ready (creating_snapshot)	123456789012	-	-
<input type="checkbox"/> 16: not_ready (creating_snapshot)	123456789012	-	-
<input type="checkbox"/> 17: not_ready (rescan)	123456789012	-	-
<input type="checkbox"/> 21: ready_for_test	123456789012	-	-
<input type="checkbox"/> 22: ready_for_test - windows	123456789012	-	-
<input type="checkbox"/> 23: ready_for_test (rescan)	123456789012	-	-
<input type="checkbox"/> 25: ready_for_test (stalled)	123456789012	-	-

- In order to perform actions on your source server, you must provide source server credentials. Server credentials are stored in AWS Secrets Manager. You can use an existing secret from the AWS Secrets Manager or create a new one.
 - Use existing secret
 - Using AWS Secrets Manager AWS MGN can use the stored source server credentials and API keys in order to connect to the source machine and perform actions on it. You must specify the secret that stores the source server credentials, using an existing secret.
 - You may designate the same secret for multiple source servers, if they share the same credentials.
 - Be sure to add the `AWSApplicationMigrationServiceManaged` tag to the secret. The value is ignored, and may be left empty.
 - Create new secret
 - **Secret name** - Enter a name for your new secret. The name you specify will be saved in AWS Secret Manager.
 - **Encryption key** - To encrypt, either use the KMS key provided by Secret Manager or create your own customer managed KMS key.
 - **For Windows servers:**

- **Communication protocol** – the protocol used for communication between the MGN connector and source servers. Using HTTPS is recommended to ensure secure and encrypted communication between the MGN connector and the source servers.
- **UserName** – A user that is authorized to install the agent and perform actions on the source server.
- **Password** – The specific source server's password.
- **CertificateAuthority** (Optional) - The certificate authority to validate during the WinRM connection.
- **For Linux servers:**
 - **UserName** – A user that is authorized to install the agent and perform actions on the source server.
 - **Provide one of the following:**
 - **Password** – The specific source server's password.
 - **PrivateKey** – The source server's private key.
 - **HostKey** (Optional) – include the host key to validate it during SSH connection.
- **Tags** - Secret key-value pairs will be assigned to the new secret. Note that `AWSApplicationMigrationServiceManaged` tag will also be added.
- Here is the structure of the secrets manager entry:

```
{
  "WinUserName": "windows_username",
  "WinPassword": "windows_password",
  "WinCertificateAuthority": "",
  "WinCaValidation": false,
  "LinuxUserName": "linux_username",
  "LinuxPrivateKey": "linux_private_key",
  "LinuxHostKey": "linux_host_key",
  "LinuxHostKeyValidation": false
}
```

• **Note**

The CA/HostKey validation is turned on by default, indicated by the validation flag being set to true. Provide the CA or HostKey in the json for validation. If you don't

provide it, you must explicitly disable validation by setting the validation flag to false. The key algorithm in HostKey, must be provided in the following format:

```
"HostKey": "algorithm_name thumbprint"
```

List of supported algorithms: "ssh-ed25519", "ecdsa-sha2-nistp256", "ecdsa-sha2-nistp384", "ecdsa-sha2-nistp521", "rsa-sha2-512", "rsa-sha2-256", "ssh-rsa", "ssh-dss"

- Once you have defined the credentials for your source servers, you can use the MGN connector to perform actions on them.
- The **Verify prerequisites** action ensures the AWS replication agent can be installed on each of the source servers. The verification process ensures there's enough disk space, RAM and CPU for installing the AWS replication agent.
- Following the prerequisite check, you can proceed to **install the replication agent**, to start your migration execution.
- After performing an action, you can **view the command history** for information on the command status.

MGN connector details

There are several ways you can access the **MGN connector details** view.

Click the **MGN connector name** of any MGN connector to open its details page.

The screenshot displays the 'MGN Connector 1' details page. At the top, the breadcrumb navigation shows 'Application Migration Service > MGN connectors > appliance-12345678901234567'. The connector name 'MGN Connector 1' is followed by an 'info' link and a 'Command history' button. The 'Overview' section shows the state as 'Active' and the last seen time as 'September 07, 2019 at 22:50 (UTC+3:00)'. Below this is a 'Servers (17)' section with a search filter and buttons for 'Unregister servers', 'Register servers', and 'Actions'. A dropdown menu for 'Actions' is open, showing options: 'Register server credentials', 'Verify prerequisites', 'Install replication agent', and 'View command history'. The main table lists 17 servers with columns for Source server name, Account, Prerequisites, Agent installed, Credentials secret, and Next step.

Source server name	Account	Prerequisites	Agent installed	Credentials secret	Next step
14: not_ready (initial_sync)	123456789012	Verified	Yes	some/secret/name	Wait for initial sync to complete
18: not_ready (stalled)	123456789012	Invalid	Yes	some/secret/name	Resolve cause of stalled data replication
19: not_ready (stalled)	123456789012	Invalid	Yes	some/secret/name	Resolve cause of stalled data replication
20: not_ready (shipping_snapshot)	123456789012	In progress	Yes	some/secret/name	Wait for snapshot transfer to complete
24: ready_for_test (lagging)	123456789012	Invalid	Yes	some/secret/name	Wait for lag to disappear, then launch test instance
28: ready_for_test (shipping_snapshot)	123456789012	Not verified	Yes	some/secret/name	Launch test instance
30: reverted_ready_for_test	123456789012	Not verified	Yes	some/secret/name	Launch test instance
32: testing	123456789012	Not verified	Yes	some/secret/name	Complete testing and mark as 'Ready for cutover'
34: testing/pending_snapshot_shipping	123456789012	Not verified	Yes	some/secret/name	Complete testing and mark as 'Ready for cutover'
36: ready_for_cutover	123456789012	Not verified	Yes	some/secret/name	Terminate launched instance; Launch cutover instance

The page includes the following details:

- **Overview** – View all the information related to the specific MGN connector including state and when it last communicated with AWS Application Migration Service.
- **Source servers** – This section features all the source servers managed by the MGN connector.

Each row in the "servers" table provides details about a single source server, including:

- **Hostname** – The source server's hostname.
- **Account** - The source server account id.
- **Prerequisites** – The status of prerequisites verification, with the following options: **Verified**, **Not verified**, **In progress**, or **Invalid**.
- **Agent installed** – Indicates whether the AWS MGN Agent is installed on the server.
- **Credential secret** – The secret of the specific source server.
- **Next step** – What is the new action in the connector installation workflow. Options include:
 - **Initiate test** – Test your source server before migration.
 - **Mark as tested** – Mark that the source server is ready for migration.
 - **Check prerequisites** – Ensure that the source server meets the required prerequisites.
 - **Wait for check to complete** – This indicates that the prerequisites are being verified. If this step is completed successfully, the next step will be **Install agent**. If not, the next step will be **Resolve cause of invalidity**.
 - **Resolve cause of invalidity** – This indicates that the prerequisite verification process failed and that a specific issue needs to be resolved.
- **Tags** - This section features the tags associated with your connector.

Import and export

The import and export feature allows you to easily plan and coordinate your migrations.

Use this feature to import and export your source servers, applications, and waves from and to a CSV file. The file can also include launch template attributes to simplify bulk configurations.

- Import from a CSV file – Import your data from a local disk or an S3 bucket and create entities in your account.
- Export to a CSV file – Export data from your account to a local disk or an S3 bucket and merge it into a single file that you can easily review and process offline.

Topics

- [Importing your data inventory](#)
- [Exporting your data inventory](#)
- [Bulk configuration editing](#)

Importing your data inventory

The **Import** feature allows you to easily import your inventory of servers, applications, and waves from a CSV file that is saved in your local disk or an S3 bucket.

Topics

- [Importing your data inventory from a local disk](#)
- [Importing your data inventory from an S3 bucket](#)
- [Import history](#)
- [Required permissions](#)
- [Import parameters](#)

Importing your data inventory from a local disk

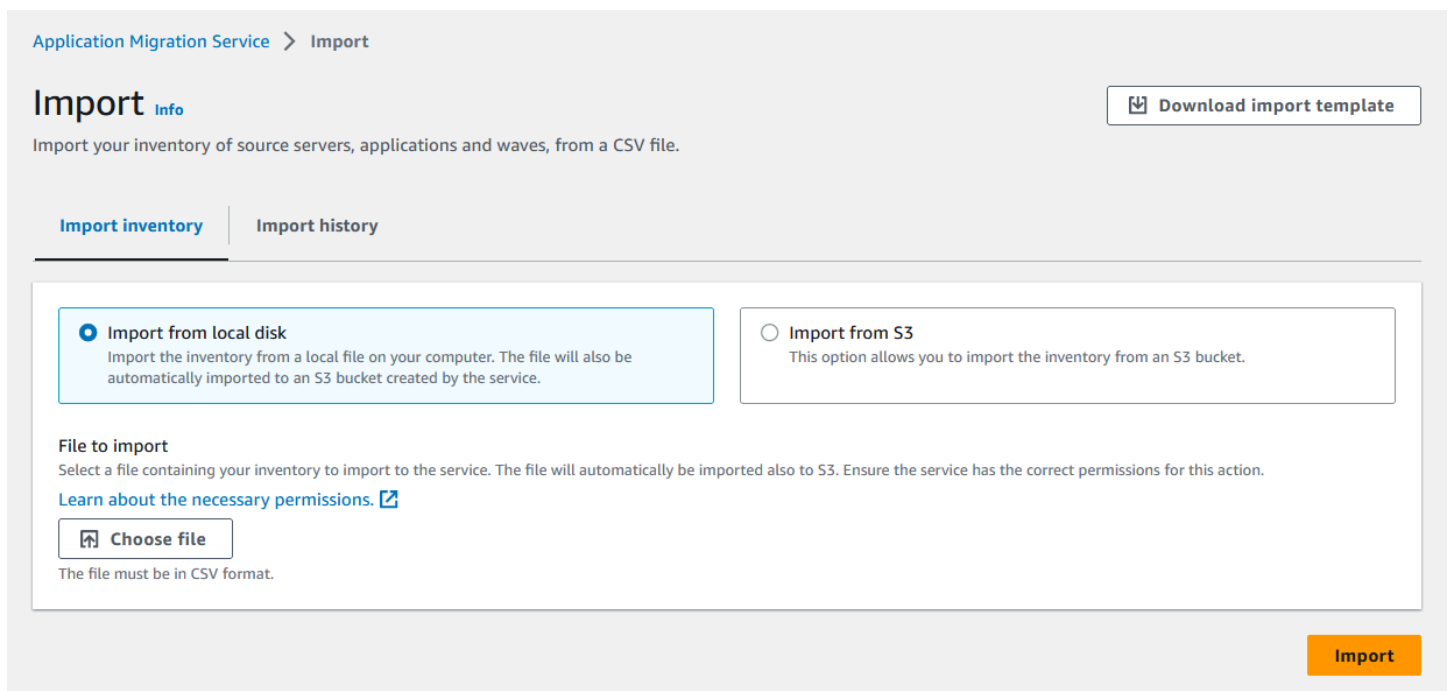
To import your inventory from a local disk, take the following steps:

1. Select **Import** from the left-hand navigation menu (under **Import and export**) and you'll be navigated to the **Import inventory** tab.

2. Select **Import from local disk**.
3. Click **Choose file** to choose the CSV file from your which you want to import the data.
4. Click **Import**.

Note

The file will also be automatically imported to an S3 bucket created by AWS MGN. It is highly recommended that you [apply Amazon S3 bucket security practices](#) where your CSV files are stored.



Application Migration Service > Import

Import Info

Import your inventory of source servers, applications and waves, from a CSV file.

[Download import template](#)

Import inventory | Import history

- Import from local disk**
Import the inventory from a local file on your computer. The file will also be automatically imported to an S3 bucket created by the service.
- Import from S3**
This option allows you to import the inventory from an S3 bucket.

File to import
Select a file containing your inventory to import to the service. The file will automatically be imported also to S3. Ensure the service has the correct permissions for this action.
[Learn about the necessary permissions.](#)

[Choose file](#)
The file must be in CSV format.

Import

Importing your data inventory from an S3 bucket

To import your inventory from an S3 bucket, take the following steps:

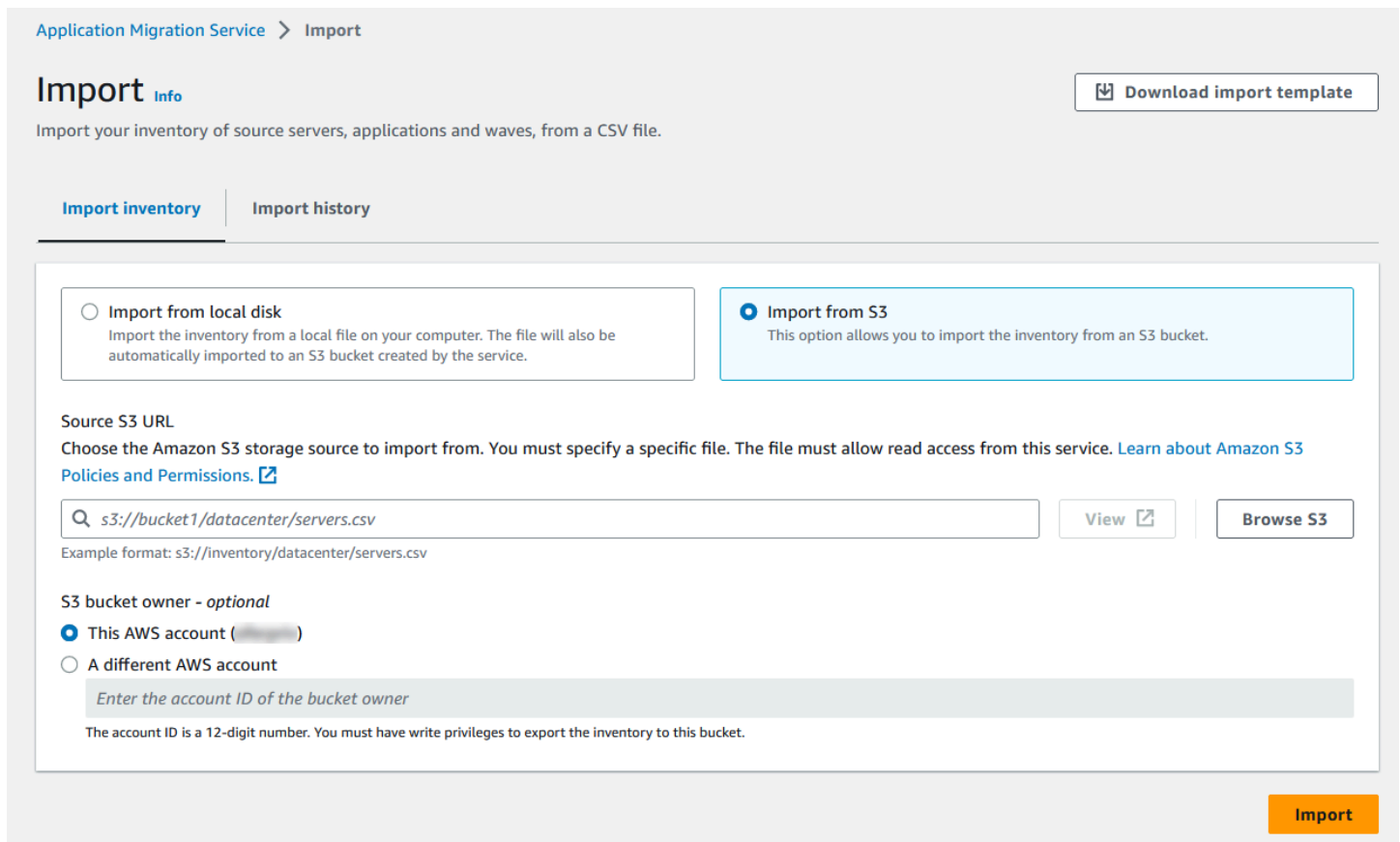
1. Select **Import** from the left-hand navigation menu (under **Import and export**) and you'll be navigated to the **Import inventory** tab.
2. Select **Import from S3**.
3. Click **Browse** to choose the Amazon S3 storage source from which you want to import the data.

4. Click **Import**.

Note

It is highly recommended that you [apply Amazon S3 bucket security practices](#) where your CSV files are stored.

[Learn more about S3 permissions and policies.](#)



Application Migration Service > Import

Import Info

Import your inventory of source servers, applications and waves, from a CSV file.

[Download import template](#)

Import inventory | Import history

Import from local disk
Import the inventory from a local file on your computer. The file will also be automatically imported to an S3 bucket created by the service.

Import from S3
This option allows you to import the inventory from an S3 bucket.

Source S3 URL
Choose the Amazon S3 storage source to import from. You must specify a specific file. The file must allow read access from this service. [Learn about Amazon S3 Policies and Permissions.](#)

[View](#) [Browse S3](#)

Example format: s3://inventory/datacenter/servers.csv

S3 bucket owner - optional

This AWS account ()

A different AWS account

The account ID is a 12-digit number. You must have write privileges to export the inventory to this bucket.

Import

Import history

Select the **Import history** tab to view the files imported in the last 7 days, including their status and the task's start and end time.

You can change the settings according to your preferences by clicking on the settings icon located in the right-hand corner of the screen.

To see all the related task messages, click the task ID. To copy the messages, click **Copy**.

Required permissions

In order to use the import feature, you will need to create a role with the following policies (or any extension of them):

Managed policies:

- [AWSApplicationMigrationFullAccess](#)
- [AWSApplicationMigrationEC2Access](#)

Additional policies:

```
{
  "Sid": "AllowS3Access",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject"
  ],
  "Resource": "arn:aws:s3:::your-bucket/*"
}
```

When starting an import on an Amazon S3 bucket source that is owned by another account, ensure that the role or user has access to the Amazon S3 objects. When using the API, the Amazon S3 bucket owner parameter defaults to the current user's account ID.

The following is an example of an S3 bucket policy in the target account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ExampleStatement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Dave"
      },
      "Action": [
        "s3:GetObject"
      ],
      "Resource": "arn:aws:s3:::awsexamplebucket1/*"
    }
  ]
}
```

```
]
}
```

Note

If the Amazon S3 objects are encrypted with SSE-KMS, ensure that the role or user initiating the import has access to decrypt using the AWS KMS key. This feature does not support SSE-C encrypted Amazon S3 objects.

Import parameters

The imported file can include multiple parameters, including:

- **mgn:account-id** – The ID of the account into which to import. This account must be managed by the calling account. Defaults to the calling account.
- **mgn:app:description** – The description of the application being imported.
- **mgn:app:name** – The name of the application being imported.
- **mgn:app:tag:appkey1** – The value of the application tag key (in this example, the tag key is appkey1).
- **mgn:launch:iam-instance-profile:name** – The name of the instance profile associated with the launch instance.
- **mgn:launch:instance-type** – The EC2 instance type of the launch instance (for example, m4.large).
- **mgn:launch:nic:0:network-interface-id** – The ID of the network interface that appears first in the launch template ("0" refers to the first network interface, "1" would refer to the second network interface, and so on).
- **mgn:launch:nic:0:private-ip:0** – The private IP that appears first in the network interface that appears first in the launch template.
- **mgn:launch:nic:0:security-group-id:0** – The security group that appears first in the network interface that appears first in the launch template.
- **mgn:launch:nic:0:subnet-id** – The subnet ID that appears first in the network interface that appears first in the launch template.
- **mgn:launch:placement:host-id** – The host ID of the placement of the launch instance.

- **mgn:launch:placement:tenancy** – This tenancy of the launch instance.
- **mgn:launch:tag:instance:key1** – The value of launch instance tag "key1" (in this example, the tag key is key1).
- **mgn:launch:volume:/dev/sda:type** – The type of the launch instance's volume whose name is /dev/sda (in this Linux machine example, the volume's name is /dev/sda; for a Windows machine, a typical volume name would be c:0).

whose name is /dev/sda (in this example, the volume's name is /dev/sda).

- **mgn:region** – The AWS Region from which you are importing. Rows from other Regions will be ignored.
- **mgn:server:fqdn-for-action-framework** – The FQDN that the MGN connector uses to connect to the server.
- **mgn:server:platform** – The server's platform (Linux or Windows).
- **mgn:server:tag:serverkey1** – The value of the server tag key (in this example, the tag key is serverkey1).
- **mgn:server:user-provided-id** – The server's user-provided ID. The MGN connector uses this parameter when installing the AWS replication agent on the server.
- **mgn:wave:description** – The description of the imported wave.
- **mgn:wave:name** – The name of the imported wave.
- **mgn:wave:tag:appkey1** – The value of the wave tag key (in this example, the tag key is appkey1).

Note

Currently, it is only possible to import into the Region being called.

Additional considerations

Please note the following considerations regarding the import parameters:

1. Server entries must include either the server IP address, or the FQDN.
2. If a row provides a property of a resource (e.g. mgn:wave:description is a property of a wave), then that row should also provide a parameter that identifies that resource (as explained in the following considerations).

3. If a resource's ID (mgn:server:id, mgn:app:id, or mgn:wave:id) is provided, the service will look for this resource in order to update it. If this resource is not found, the import will fail.
4. If a resource's ID is not provided, the service will look for a resource's alternative identification:
 - For an application: mgn:app:name
 - For a wave: mgn:wave:name
 - For a server: mgn:server:user-provided-id
5. If a resource's alternative identification exists in AWS MGN, the service will update this resource with new values (if applicable).
6. If a resource's alternative identification does not exist in AWS MGN, the service will create the resource.
7. 2 rows that refer to the same resource need not provide the same parameters for that resource, but they must not conflict. For example, if 2 rows provide the same mgn:wave:name, it is acceptable for one row to provide mgn:wave:description and for the other row to leave the value blank. However, the 2 rows must not provide conflicting values of mgn:wave:description.

Creating a CSV file in Microsoft Excel

When saving the CSV file in Microsoft Excel, ensure to save it in the **MS-DOS** CSV data format.

Exporting your data inventory

The **Export** feature allows you to easily export your inventory of servers, applications, and waves to a CSV file that is saved in your local disk or an S3 bucket.

Topics

- [Exporting your data inventory to a local disk](#)
- [Exporting your data inventory to an S3 bucket](#)
- [Export history](#)
- [Required permissions](#)
- [Amazon S3 bucket permission requirements](#)
- [Export parameters](#)

Exporting your data inventory to a local disk

To export your inventory to a local disk, take the following steps:

1. Select **Export** from the left-hand navigation menu (under **Import and export**) and you'll be navigated to the **Export inventory** tab.
2. Select **Export to a local disk**.
3. Specify the name of the CSV file into which you want to download the data.

Note

- The file will also be automatically downloaded to an S3 bucket created by AWS Application Migration Service.
- You must have the required permissions to perform this action.
- It is highly recommended that you [apply S3 bucket security practices](#) where your CSV files are stored.

4. Click **Export**.

Export Info

Export your inventory of source servers, applications and waves, to a CSV file.

Export inventory | Export history

Export to local disk
Export the inventory to a local file on your computer. The file will also be automatically exported to an S3 bucket created by the service.

Export to S3
Export the inventory to an S3 bucket.

Destination filename
Specify the name of the file to download. The file will also be automatically exported to an S3 bucket created by the service. Ensure the user has the correct permissions for this action.
[Learn about the necessary permissions.](#)

Example servers.csv

Export

Exporting your data inventory to an S3 bucket

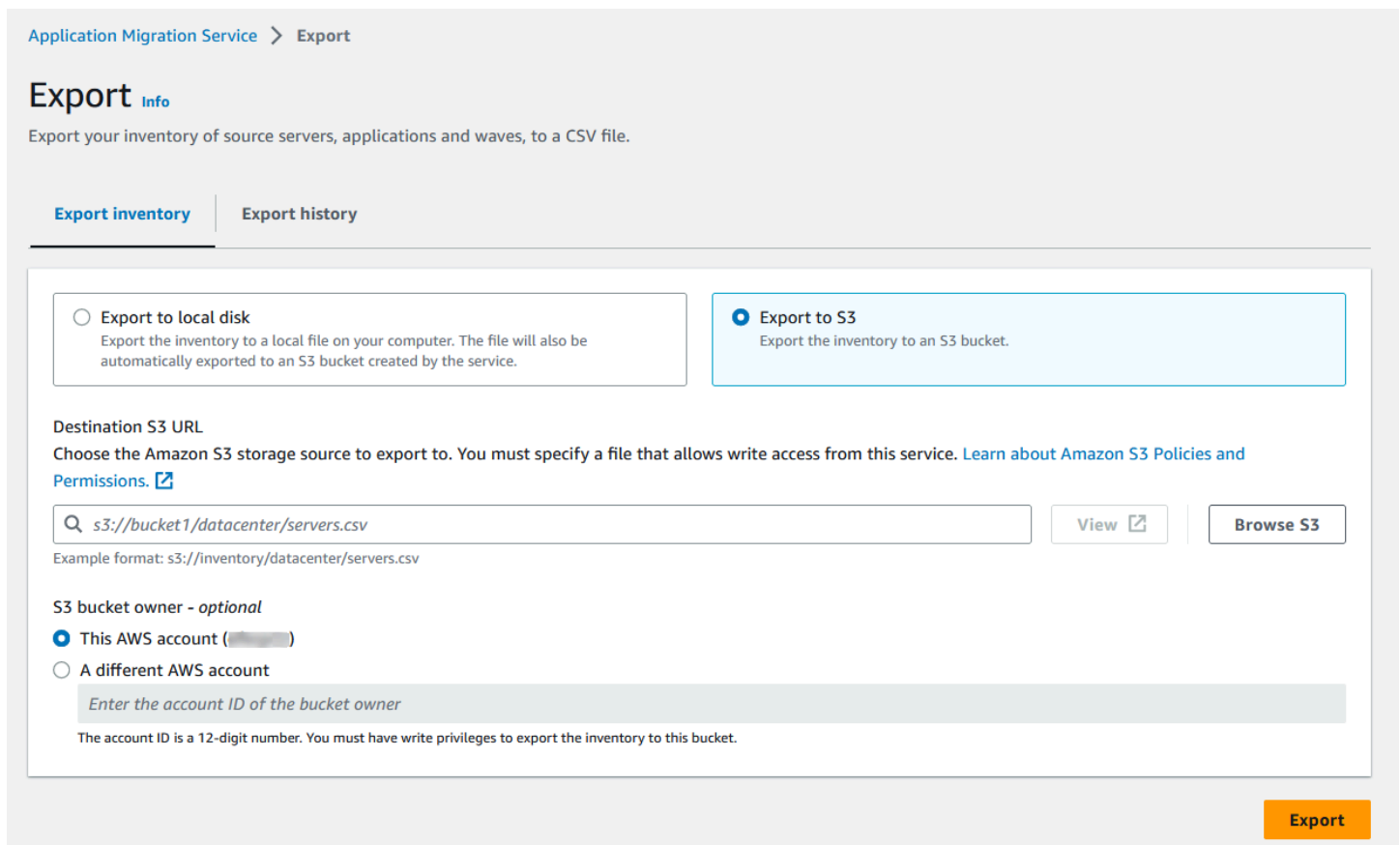
To export your inventory to an S3 bucket, take the following steps:

1. Select **Export** from the left-hand navigation menu (under **Import and export**) and you'll be navigated to the **Export inventory** tab.
2. Select **Export to S3 bucket**.
3. Click **Browse S3** to choose the Amazon S3 storage target to which you want to export the data.
4. Specify the Amazon S3 bucket owner (the current AWS account or a different one) according to your preferences. If you select a different AWS account, you must enter the bucket owner's account ID.

Note

- You must have write privileges to export an inventory to a specific bucket.
- It is highly recommended that you [apply S3 bucket security practices](#) where your CSV files are stored. [Learn more about S3 permissions and policies.](#)

5. Click **Export**.



Application Migration Service > Export

Export Info

Export your inventory of source servers, applications and waves, to a CSV file.

Export inventory | Export history

Export to local disk
Export the inventory to a local file on your computer. The file will also be automatically exported to an S3 bucket created by the service.

Export to S3
Export the inventory to an S3 bucket.

Destination S3 URL
Choose the Amazon S3 storage source to export to. You must specify a file that allows write access from this service. [Learn about Amazon S3 Policies and Permissions.](#)

Example format: s3://Inventory/datacenter/servers.csv

S3 bucket owner - optional

This AWS account ()

A different AWS account

The account ID is a 12-digit number. You must have write privileges to export the inventory to this bucket.

Export history

Select the **Export history** tab to view the files exported in the last 7 days, including their status, progress, and the task's start and end time.

You can change the settings according to your preferences by clicking on the settings icon located in the right-hand corner of the screen.

To see all the related task messages, click the task ID. To copy the messages, click **Copy**.

Required permissions

In order to use the export feature, you will need to create a role with the following policies (or any extension of them):

Managed policies:

- `AWSApplicationMigrationReadOnlyAccess`

Additional policies:

```
{
  "Sid": "AllowS3Access",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject"
  ],
  "Resource": "arn:aws:s3:::your-bucket/*"
},
{
  "Sid": "AllowMgnStartExport",
  "Effect": "Allow",
  "Action": [
    "mgn:StartExport"
  ],
  "Resource": "*"
}
```

When starting an export on an Amazon S3 bucket source that is owned by another account, ensure that the role or user has access to the Amazon S3 objects. When using the API, the Amazon S3 bucket owner parameter defaults to the current user's account ID.

The following is an example of an Amazon S3 bucket policy in the target account:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ExampleStatement",
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::123456789012:user/Dave"
      },
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::awsexamplebucket1/*"
    }
  ]
}
```

Note

If the Amazon S3 objects are encrypted with SSE-KMS, ensure that the role or user initiating the export has access to decrypt using the AWS KMS key. This feature does not support SSE-C encrypted Amazon S3 objects.

Amazon S3 bucket permission requirements

Before you create an export job, you must create the destination S3 bucket to export to. AWS Application Migration Service doesn't create the S3 bucket for you. The S3 bucket that you specify can't be publicly accessible, and can't be configured as a [Requester Pays](#) bucket. After you create the S3 bucket, confirm that the bucket has the required permissions policy to allow AWS Application Migration Service to write the export files to it.

Export parameters

The exported file can include multiple parameters, including:

- **mgn:account-id** – The ID of the account being exported.
- **mgn:app:description** – The description of the application being exported.

- **mgn:app:id** – The ID of the application being exported.
- **mgn:app:name** – The name of the application being exported.
- **mgn:app:tag:appkey1** – The value of the application tag key (in this example, the tag key is appkey1).
- **mgn:launch:iam-instance-profile:name** – The name of the instance profile associated with the launch instance.
- **mgn:launch:instance-type** – The EC2 instance type of the launch instance (for example, m4.large).
- **mgn:launch:nic:0:network-interface-id** – The ID of the network interface that appears first in the launch template ("0" refers to the first network interface, "1" would refer to the second network interface, and so on).
- **mgn:launch:nic:0:private-ip:0** – The private IP that appears first in the network interface that appears first in the launch template.
- **mgn:launch:nic:0:security-group-id:0** – The security group that appears first in the network interface that appears first in the launch template.
- **mgn:launch:nic:0:subnet-id** – The subnet ID that appears first in the network interface that appears first in the launch template.
- **mgn:launch:placement:host-id** – The host ID of the placement of the launch instance.
- **mgn:launch:placement:tenancy** – This tenancy of the launch instance. Expected values: default, dedicated, or host.
- **mgn:launch:tag:instance:key1** – The value of launch instance tag "key1" (in this example, the tag key is key1).
- **mgn:launch:volume:/dev/sda:type** – The type of the launch instance's volume whose name is /dev/sda (in this example, the volume's name is /dev/sda).
- **mgn:region** – The AWS Region from which you are exporting.
- **mgn:server:fqdn-for-action-framework** – The FQDN that the MGN connector uses to connect to the server.
- **mgn:server:id** – The server ID.
- **mgn:server:lifecycle-state** – The server's lifecycle state.
- **mgn:server:platform** – The server's platform (Linux or Windows).
- **mgn:server:replication-type** – The type of the replication (agent-based or agentless).
- **mgn:server:replication-state** – The state of the replication.

- **mgn:server:tag:serverkey1** – The value of the server tag key (in this example, the tag key is serverkey1).
- **mgn:server:user-provided-id** – The server's user-provided ID. The MGN connector uses this parameter when installing the AWS replication agent on the server.
- **mgn:wave:description** – The description of the exported wave.
- **mgn:wave:id** – The ID of the exported wave.
- **mgn:wave:name** – The name of the exported wave.
- **mgn:wave:tag:appkey1** – The value of the wave tag key (in this example, the tag key is appkey1).

Note

If the bucket you're exporting to is encrypted with customer managed keys (KMS), that KMS key's policies must give AWS MGN permission to use it. This permission is given through the user or role that initiates the export job.

If you choose to encrypt your export using a key protected by AWS Key Management Service (AWS KMS), the key must be in the same Region as the destination S3 bucket.

Bulk configuration editing

You can use the **Import and export** feature to implement bulk configurations by taking the following steps:

1. Export all of the data to a CSV file.
2. Edit your file (add tags, make changes, and more).
3. Import the edited data back into the service.

Global view

AWS Application Migration Service (AWS MGN) offers the global view feature that allows you to manage large-scale migrations across multiple accounts. This feature provides both visibility and the ability to perform specific actions on source servers, apps, and waves in different AWS accounts.

Global view utilizes AWS Organizations to structure a management account (that has access to source servers in multiple member accounts) and member accounts (that only have access to their own source servers).

In order to use this feature:

- You need to have an AWS account in which AWS Application Migration Service is initialized.
- This account must be management account in AWS Organizations or a delegated admin for AWS Application Migration Service.

Note

MGN delegated admin has the same feature permissions as management account in AWS Organizations.

Setting up your AWS Organizations

The AWS Organizations service allows you to consolidate multiple AWS accounts into a single organization that you create and manage. You can create member accounts or invite existing accounts to join your organization. [Learn more about AWS Organizations.](#)

To use global view, you must first create your organization via the AWS Organizations console.

To set up your organization, take the following steps:

1. Create an AWS organization.
 - a. Go to the AWS Organizations console.
 - b. [Create a new AWS organization.](#)
 - c. [Invite member accounts](#) you want to manage within AWS MGN.

Activate trusted access for application migration service

To use global view, you must activate trusted access to AWS Application Migration Service (AWS MGN) for your organization.

If you wish to configure global view, attach the following managed policy to the user: `AWSOrganizationsFullAccess`

To enable service access for your organization, take the following steps:

1. Activate trusted access for AWS MGN
 - a. log in as management account.
 - b. Select **Global view** from the left-hand navigation menu.
 - c. Activate service access by clicking the 'Enable AWS Organizations service access' button

[Learn more about activating trusted access.](#)

2. Select members and turn them into delegated admins for AWS MGN

To do so, call the following API:

[RegisterDelegatedAdministrator](#)

Note

Under **Requested Syntax**, include the service name as follows:

```
{
  "AccountId": "string",
  "ServicePrincipal": "mgn.amazonaws.com"
}
```

Important

You can register up to 5 delegated administrators.

Setting up CloudFormation StackSets

After you set up your organization, you need to configure CloudFormation StackSet in order to create the required role per management account: `AWSApplicationMigrationSharingRole_<MANAGEMENT_ACCOUNT_ID>`.

AWS CloudFormation StackSets extends the capability of stacks by enabling you to create, update, or delete stacks across multiple accounts and AWS Regions with a single operation.

[Learn more about CloudFormation StackSets.](#)

Important

You can choose to create the roles manually in each member account of the organization. However, this will need to be done for each account, one by one, while StackSet automatically creates the roles in all accounts.

To set up your StackSet, take the following steps:

1. Set up your StackSet
 - a. Go to the CloudFormation console.
 - b. Select **StackSets**.
 - c. Click on 'Activate trusted access' button.
 - d. Create StackSet.
 - e. On the **Choose a template** page, under **Prerequisites – prepare template**, choose **Use a sample template**.
 - f. Under **Select a sample template**, select **Create roles to access multiple accounts via AWS Application Migration Service**, and then click **Next**.
 - g. Fill in the name and description according to your preferences or use the existing values.
 - h. Under **Parameters**, add the account ID of each admin or delegated admin and click **Next**.
 - i. Select or fill in the required parameters according to your preferences.

Important

- Under **Deployment targets**, select **Deploy to organization**.
- Select only one specific AWS Region – it is advisable to select your StackSet Region.

- To provide enhanced stability, it is advisable to set the **Failure tolerance optional** to a high value (at least as high as the number of accounts within the organization).

- j. Check the box next to **I acknowledge that AWS CloudFormation might create IAM resources with custom names** and click **Submit**.

Once all the steps are completed, you should be able to see your new StackSet in **StackSet details > Stack instances**.

Using an AWS KMS Customer Managed Key (CMK) for encryption in member account

If you decide to use a Customer Managed Key (CMK), or if your default Amazon EBS encryption key is a CMK in member account, you will need to add additional permissions to the `AWSApplicationMigrationSharingRole_<MANAGEMENT_ACCOUNT_ID>` to allow management account to use it.

By using Administrator access, add the following permissions to the `AWSApplicationMigrationSharingRole_<MANAGEMENT_ACCOUNT_ID>`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Allow management account use CMK of member account",
      "Effect": "Allow",
      "Action": [
        "kms:CreateGrant",
        "kms:DescribeKey",
        "kms:ReEncrypt*",
        "kms:GenerateDataKey*"
      ],
      "Resource": "$KEY_ARN"
    }
  ]
}
```

Inviting an AWS account to join your organization

After you create an organization and verify the email address associated with the management account, you can invite existing AWS accounts to join your organization. Only management accounts can send an invitation to other accounts.

When you invite an account, AWS Organizations sends an invitation to the account owner, who decides whether to accept or decline the invitation. You can use the AWS Organizations console to initiate and manage invitations that you send to other accounts.

[Learn how to send invitations to other AWS accounts.](#)

Using global view

Use the global view feature to see source servers across various member accounts and to perform various actions such as installing the SSM Agent.

If you wish to use global view, attach the following managed policy to the user:

```
AWSOrganizationsReadOnlyAccess
```

The main **Global view** page provides an overview of your account. The information will change according to whether you have a management account or a member account.

- Management Account – for management accounts, this page will display **Account information** that includes the AWS organizations permissions, number of linked accounts, and the total number of source servers, applications, and waves. The **Linked account** section will display the relevant information for the linked accounts only.
- Member – for member accounts, this page will only display the **Account information** that includes the AWS organizations permissions,, and the number of source servers, applications, and waves in the specific account.

As a management account, you will be able to choose between **All accounts** and **My account** from the drop-down menu, allowing you to change your view of presented source servers, applications, or waves.

Source servers in member accounts

As a management account, you can view source servers in your account and all member accounts. You can also perform specific actions on managed servers.

Single managed source server

As a management account, you can perform the following actions on a single managed source server.

- Change staging disk type
- Edit replication settings
- Launch settings – edit general launch settings only
- Post launch
 - Deactivate the post-launch feature for this server
 - Change deployment settings (test and cutover, test only, or cutover only)
- Start/stop replication
- Test and cutover drop-down menu:
 - Launch test
 - Mark as ready for cutover
 - Revert to ready for testing
 - Launch cutover
 - Finalize cutover
 - Revert to ready for cutover
 - Terminate launch instances

Multiple managed source server

As a management account, you can perform the following actions on multiple managed source servers.

- Edit replication settings – the edited servers must be from the same account
- Add server to application – the added servers must be from the same account
- Disconnect servers from service
- Mark as archived
- Start/stop replication
- Change staging disk type
- Edit replication settings

- Launch settings – edit general launch settings only
- Post launch
 - Deactivate the post-launch feature for this server
 - Change deployment settings (test and cutover, test only, or cutover only)
- Start/stop replication
- Test and cutover drop-down menu:
 - Launch test
 - Mark as ready for cutover
 - Revert to ready for testing
 - Launch cutover
 - Finalize cutover
 - Revert to ready for cutover
 - Terminate launch instances

Applications

As a management account, you can perform the following actions on a single or multiple managed applications:

- Add application
- Edit application
- Delete application
- Test and cutover drop-down menu (these actions can also be performed on multiple applications):
 - Launch test
 - Mark as ready for cutover
 - Revert to ready for testing
 - Launch cutover
 - Finalize cutover
 - Revert to ready for cutover
 - Add application to wave
 - Start/stop replication

- Archive application

Waves

As a management account, you can perform the following actions on a single managed applications:

- Add wave
- Edit wave
- Delete wave
- Test and cutover drop-down menu (these actions can also be performed on multiple waves):
 - Launch test
 - Mark as ready for cutover
 - Revert to ready for testing
 - Launch cutover
 - Finalize cutover
 - Revert to ready for cutover
 - Add application to wave
 - Start/stop replication
 - Archive application

Import/Export

Use this feature to import and export your source servers, applications, and waves from a single or multiple accounts using the CSV template file.

Launching test and cutover instances

AWS Application Migration Service (AWS MGN) allows you to launch test and cutover instances in AWS. Prior to launching instances, you must configure your Launch settings. The following documentation explains how to configure Launch settings and how to launch Test and cutover instances using the configured settings.

Launch settings determine how your Test and cutover instances will be launched in AWS. Through Launch settings, you can fully customize your test and cutover instances by configuring key metrics, such as the Subnet within which the instance will be launched, the instance type to be used, licence transfers, replication status, and a variety of other settings. AWS MGN ensures that your test and cutover instances constantly abide by the latest AWS security, instance, and other updates by utilizing EC2 launch templates. EC2 launch templates always use the latest EC2 instance and technology. They integrate with Application Migration Service in order to give you full control over every single setting within your test and cutover instance. Once you have configured your instance's launch settings, you can launch them directly through the AWS MGN console. During the launch process, either during test or cutover instance launch, the AWS Replication agent is removed from the test or cutover instance, and will not run on it.

Topics

- [Preparing for test and cutover instance launch](#)
- [Launch settings](#)
- [Launching test instances](#)
- [Launching cutover instances](#)
- [Launch history](#)

Preparing for test and cutover instance launch

Prior to launching your instances, you must ensure that your environment is set up properly to ensure successful launches. Check the following prior to continuing:

- Prepare your subnets for launch - Plan which subnets you will use to launch your test and cutover instances. You will use these subnets in your EC2 launch template when you configure your Launch settings.

- Create security groups within the subnets - Create the Security groups you want to use within your prepared subnets. You will set these Security groups in your EC2 Launch template when you configure launch settings.

Note

Customers that want to run a proof of concept can skip this step. AWS Application Migration Service will automatically use the default subnet and Security groups. Make sure that you have not deleted your default subnet.

Launch settings

The launch settings are a set of instructions that are comprised of two sections: general launch settings and the EC2 launch template that determine how a test or cutover instance will be launched for each source server in AWS.

Launch settings, including the EC2 launch template, are automatically created every time you add a source server to AWS Application Migration Service.

The Launch settings can be modified at any time, including before the source server has completed its initial sync.

Note

Any changes made to the launch settings will only affect newly launched test and cutover instances.

Note

For many customers, there is no need to modify the launch settings or the EC2 launch template in order to launch test or cutover instances.

Launch settings can only be changed for one server at a time through the AWS Application Migration Service console.

Note

You can modify launch settings for multiple servers at a time by using the AWS Application Migration Service API.

You can access the launch settings of a specific source server through the server details view by choosing its Hostname from the **Source servers** page.

Source servers (38)								Actions ▾	Replication ▾	Test and cutover ▾
Active source servers ▾		Filter source servers by property or value						< 1 >	⚙️	
<input type="checkbox"/>	Source server name ▾	Alerts ▾	Replication type ▾	Migration lifecycle ▾	Data replication status	Last snapshot ▾	Next step ▾			
<input type="checkbox"/>	31: testing	-	Agent based	Test in progress	Healthy	a day ago	Complete testing and mark as 'Ready for cutover'			

Within the individual server view, navigate to the **Launch settings** tab.

The screenshot shows the AWS Management Console interface for the 'Launch settings' tab. The navigation bar at the top includes 'Migration dashboard', 'Server info', 'Tags', 'Disks settings', 'Replication Settings', and 'Launch settings' (highlighted with a red box). Below the navigation bar, there are two main sections:

- General launch settings** (with an 'Info' link and an 'Edit' button):
 - Instance type right sizing: On
 - Start instance upon launch: Yes
 - Copy private IP: Yes (127.0.0.1)
 - Operating system licensing: BYOL
 - Transfer server tags: Yes
 - Boot mode: Legacy BIOS
- EC2 Launch Template** (with an 'Info' link and a 'Modify' button):
 - Template ID: lt-1
 - Instance type: a1.2xlarge
 - FRS volumes
 - Primary network interface: network-description, subnet-subnet-1

The **Launch settings** tab is divided into two sections:

- General launch settings
- EC2 launch template

We will discuss each launch setting category in detail in the following sections:

Topics

- [General launch settings](#)
- [EC2 launch template](#)

General launch settings

The **General launch settings** section allows you to control a variety of server-specific settings. Click **Edit** to change the general settings.

General launch settings [Info](#)

Edit

Instance type right sizing	Operating system licensing
On	BYOL
Start instance upon launch	Transfer server tags
Yes	Yes
Copy private IP	Boot mode
Yes (127.0.0.1)	Legacy BIOS

Make your changes and then choose **Save settings** to finalize your changes.

Topics

- [Instance type right-sizing](#)
- [Start instance upon launching](#)
- [Copy Private IP](#)
- [Operating system licensing](#)
- [Transfer server tags](#)
- [Boot mode](#)

Instance type right-sizing

The instance type right-sizing feature allows AWS Application Migration Service to launch a test or cutover instance type that best matches the hardware configuration of the source server.

Instance type right sizing [Info](#)

Basic ▼

If you select the **Basic** option, AWS Application Migration Service will launch a test or cutover AWS instance type that best matches the OS, CPU, and RAM of your source server.

AWS Application Migration Service will launch a new instance type after every change of configuration on the source server (ex. added/removed disks, added/removed RAM)

⚠ Important

The AWS instance type selected by AWS Application Migration Service when this feature is activated will overwrite the instance type defined in your EC2 launch template.

ℹ Note

Hardware changes and the resulting AWS instance type change may take up to 90 minutes to be processed by AWS Application Migration Service.

If you select the **None** option, AWS Application Migration Service will launch the AWS instance type as configured in your EC2 launch template. You should select this option if you want to determine the instance type that will be launched in AWS for all your test or cutover servers.

The service will provide recommendations from these instance families (if they are available in your target region):

- c5
- m5
- c4
- m4
- r5
- r4
- i3
- d2

The right-sizing instance type selected by AWS Application Migration Service will show on the **Server details** tab.

ℹ Note

The T family instance type is not supported for right-sizing. If you want to use the T family, avoid using right-sizing.

Start instance upon launching

Choose whether you want to start your test and cutover instances automatically upon launch or whether you want to launch them in a stopped state.

Start instance upon launch [Info](#)


If you click **Yes**, the test or cutover AWS instance will be launched and started automatically upon test or cutover launch.

If you click **No**, the instances will be launched in a stopped state and you will have to start the test or cutover AWS instance manually from the Amazon EC2 console.

Copy Private IP

Choose whether you want AWS Application Migration Service to ensure that the private IP used by the test or cutover instance matches the private IP used by the source server.

Copy private IP [Info](#)

 Changing this to "No" will not remove the copied IP from the EC2 Launch Template

AWS Application Migration Service (AWS MGN) will monitor the source server on an hourly basis to identify the private IP. AWS MGN will use the private IP of the primary network interface.

The **No** option is chosen by default. Click **No** if you do not want the private IP of the test or cutover instance to match that of the source machine.

Click **Yes** if you want to use a private IP. The IP will be shown in brackets next to the option.

Note

If you clicked **Yes**, ensure that the IP range of the subnet you set in the EC2 launch template includes the private IP address.

Note

If the both the source server and the test or cutover instance shares the same subnet though a VPN, then the source private IP is already in use, and the **Copy private IP** option should not be used.

Operating system licensing

Choose whether you want to Bring Your Own Licenses (BYOL) from the source server into the test or cutover instance.

Operating system licensing [Info](#)

BYOL

Windows BYOL is only allowed for EC2 Dedicated Hosts, or under special circumstances, Dedicated Instances. [Learn more](#) 

The **Use default** option will use the default licensing mechanism for your operating system.

Choose the **BYOL** option if you are migrating a Linux server. All Linux licenses are BYOL by default. Any RHEL, SUSE or Debian licenses will be transferred in their current form to the migrated instance. Make sure to ensure that the terms of your licenses allow this license transfer.

Choose the **BYOL** option if you want to BYOL your Windows licenses. This will set up a Dedicated Host. All the licenses from the source Windows source server will be automatically transferred to the Test or Cutover instance. [Learn more about dedicated hosts.](#)

Important

If you activate BYOL licensing for Windows, you have to change the **Placement.tenancy** type in the EC2 launch template to **Host**. Otherwise, instance launch will fail.

Note

- Windows Desktop Editions require BYOL – [note the specific restrictions for AWS Provided Licenses.](#)

- If you are using Windows Servers datacenter: Azure addition, [note the specified restrictions for BYOL](#).

Transfer server tags

Choose whether you want AWS Application Migration Service to transfer any user-configured custom tags from your source servers onto your test or cutover instance.

Transfer server tags [Info](#)

If you click **Yes**, server tags will be transferred. These tags are attached to all source servers, all launched test and cutover instances, and all of the ephemeral resources that are created on your AWS Account during the normal operation of AWS Application Migration Service. These resources include:

- EC2 instances
- Conversion groups
- Security groups
- EBS volumes
- Snapshots

Note

AWS Application Migration Service automatically adds system tags to all resources.

Note

Transfer server tags only copies tags associated with the source servers in the AWS Application Migration Service console, and does not copy the EC2 source server tags (in case of AWS to AWS migration)

If you choose the **No** option, server tags will not be transferred. You can always add tags from the Amazon EC2 console as described in [this EC2 article](#).

Note

Tags that are added on the EC2 launch template will take precedence over tags that are transferred directly from the source server.

Boot mode

Choose the boot mode for the test or cutover instance.

You can either choose the **Legacy BIOS**, **UEFI** or **Use source boot mode**. By default, the boot mode is set to **Use source boot mode**. When this option is selected, MGN will launch the test or cutover instance using the same boot mode as the source server.

Note: When the BIOS option is chosen, AWS MGN converts any non-BIOS instance type to BIOS. As such, the server will be limited to four partitions that cannot equal more than 2TiB due to BIOS limitations.

Note

You must choose the **UEFI** boot mode for any BYOL source server that is UEFI, as AWS MGN is unable to convert BYOL source servers that boot in UEFI to BIOS.

Note

UEFI boot is only available for Nitro instances.
All Nitro based instance types can also run on UEFI instead of Legacy BIOS.
Refer to [this page for a list of supported instance types](#).

EC2 launch template

AWS Application Migration Service (AWS MGN) utilizes EC2 launch templates to launch test and cutover EC2 instances for each source server.

The EC2 launch template is created automatically for each source server that is added to AWS MGN upon the installation of the AWS Replication Agent.

Note

- AWS MGN selects defaults to provide the best performance while migrating your servers to AWS. We recommend you review the EC2 launch template to ensure the selected templates are suitable for your use case.
- You cannot use the same template for multiple servers.
- The Launch template can only be edited from the Amazon EC2 console.
- Many EC2 launch template settings can be changed, but some may not be used by the AWS MGN launch process and some may interfere with IT. [Learn more about individual launch template settings.](#)

Important

- You must set the EC2 launch template you want to use with AWS MGN as the **default** launch template.
- The EC2 launch template does not automatically set a specific subnet. As such, EC2 will attempt to launch in a subnet within the default VPC. If you have removed your default VPC, EC2 will fail to launch any instance for which there is no valid subnet specified. Ensure that you specify a subnet if that is the case, or AWS MGN instance launch will fail.

The AWS MGN EC2 launch template panel shows a summary of the key template values. To view all the values or to change any of them:

1. Click **Modify**.
2. When the **About modifying EC2 launch templates** dialog appears, click **Modify**.

This will redirect you to **EC2 > Launch templates > Modify template** in a new tab, where you'll be able to make any necessary changes.

Learn more about EC2 launch template settings and configuration options in [this EC2 article](#).

Working with EC2 launch templates

Topics

- [Selecting the default template](#)
- [Launch template cleanup and fixing](#)
- [Launch template key considerations](#)
- [Full launch template setting review](#)
- [Saving your EC2 launch template](#)

Selecting the default template

AWS MGN uses the version of the Launch template that is marked as default.

In order to select the default launch template, on the **Modify template (Create new version)** page, under the **Launch template name and version description** category, open the **Source template** menu and choose the EC2 launch template you want to use as the default template from the drop-down menu.

Every time you modify the Launch template, a new version of the launch template is created. You will be notified that the Launch template has been modified and that a new version (version number) has been created. Make sure to take note of the version number and the **Launch template ID** so that you could easily identify your launch template and version.

Note

It's good practice to delete versions of the launch template that you no longer need.

To set the new version of your launch template as the default:

1. Navigate back to the main **EC2 > Launch templates** page.
2. Choose your launch template by selecting the toggle to the left of the **Launch template ID**.
3. Open the Actions menu and choose **Set default version**.
4. Select the **Template version** from the drop-down menu and then choose **Set as default version**.

The Amazon EC2 console will confirm the version change.

Launch template cleanup and fixing

AWS Application Migration Service (AWS MGN) runs a mechanism every hour to ensure that the settings selected are correct. This mechanism can fix issues such as an incorrect instance type, but it cannot fix other settings and augmentations. Ensure that you follow the instructions in the following sections and do not change or edit any fields that should not be changed.

If you encounter any issues with the launch template, you can negate all of your changes and fix all issues rapidly by choosing the original default launch template that was first automatically created by Application Migration Service upon Agent installation.

Launch template key considerations

There are several key considerations when configuring your EC2 launch template. Review these key considerations as well as the [full launch settings](#) before creating your launch template.

1. **Instance Type** – Ensure that you select an instance type that matches the hardware requirements of your source server. AWS Application Migration Service always utilizes the instance type that is set on the Amazon EC2 launch template unless the **Instance right-sizing** feature is activated.

Note

If you change your instance type and do not deactivate the instance right-sizing feature, then AWS Application Migration Service will use the instance type determined by the **Instance right-sizing** feature and not the instance type you chose in the EC2 launch template. Application Migration Service verifies the instance type once per hour, as a result, if you did not deactivate the instance right-sizing feature, the first time instance launch may still utilize the instance type you set in the EC2 launch template, but any subsequent launches will utilize the right-sizing instance.

2. **Subnet** – You can select an existing subnet or create a new subnet.

Note

Customers that do not have a default VPC must modify the EC2 launch template and explicitly define the subnet in which to launch. Failure to do so will result in errors when launching test or cutover instances.


3. **Private IP** – If you use the **Copy private IP** feature, then do not add your own IP to the EC2 launch template.
4. **Private IP and Subnet** – Each subnet contains a CIDR block of IP ranges. If you use the **Copy private IP** feature, then ensure that this IP is included in the CIDR block range. Otherwise, instance launch will fail.
5. **Private IP and ENI** – Make sure that you deactivate the **Copy private IP** feature if you wish to define an ENI to use on the EC2 launch template.
6. **Network interfaces** – The EC2 launch template only supports two network interfaces. If you require more than two network interfaces, you will need to define them after the test or cutover instance has been launched. This can be done through a post launch action.

If you wish to use an Elastic IP, you must create an ENI to specify the IP and then edit the Network interfaces to use the ENI. Learn more about working with Amazon Elastic Inference in [this Developer Guide article](#).

7. **Networking platform** – AWS Application Migration Service only supports **Virtual Private Cloud (VPC)**. EC2-Classic is **not** supported. Do **not** add any security groups under the network platform.
8. **Custom device name** – Do not alter this field. AWS Application Migration Service uses the device name as defined on the source server in order to map disks on the test or cutover instance. You can use this field to identify your disks.
9. **Disks** – You cannot add disks to the EC2 launch template. Any disks that are added that do not exist on the source machine will be ignored by AWS Application Migration Service.
10. **Launch template name** – Do not alter this field. AWS Application Migration Service automatically names this field.
11. **System tag** – Do not alter this field. Application Migration Service automatically adds system tags that match the EC2 launch template to the specific source server. You can recognize which source server the launch template is matched with by the **ID** field.
12. **Automatic cleanup** – Application Migration Service deletes the EC2 launch template and launch configuration for machines that have been disconnected from AWS Application Migration Service or machines for which the cutover has been finalized 90 minutes after disconnect or cutover finalization. This aids in ensuring that your account does not surpass the AWS 5000 EC2 launch template limit.
13. **Volumes** – For each EBS volume, the service uses the user-selected values. If no matching volume exists in the launch template, the service will use the default value. If the launch template

includes a volume that does not exist in the source server, the system will disregard the specific volume.

If you delete the EC2 launch template, the service will create a new one with default values.

 **Note**

If you wish to set a KMS key, you should do so through the [EBS Encryption](#) section of the replication settings within the AWS Application Migration Service console.

Full launch template setting review

This section reviews the entire EC2 launch template and identifies which fields should and should not be changed in order for the EC2 launch template to work with Application Migration Service. Editing or changing any fields that are marked as "do not edit" or "do not change" can cause AWS Application Migration Service to not function.

- **Launch template name** – This name is automatically generated when the template is first created upon Agent installation. The name cannot be changed.
- **Template version description** – You can give the template any description you wish.
- **AMI** – Customers do not typically choose a specific AMI to include in the launch template. If you edit the launch template to use an existing AMI, the contents of the AMI will not be used by AWS Application Migration Service. If the AMI is not configured properly (licensing, flags, and more), then this may prevent the test or cutover instance launched from booting correctly or from being properly licensed.
- **Instance type** – You can select any instance type you want. The launch template will show the instance type suggested by AWS Application Migration Service.
- **Key pair (login)** – **Do not** alter this field. Do not include a key pair with the launch template.
- **Networking platform** – Be sure to select **Virtual Private Cloud (VPC)**. **EC2-Classical** is not supported.

- **Security groups** – **Do not** add Security group here. This field should remain blank. You can add security groups later under **Network interface**.
- **Storage (volumes)** – This section will show all of the disks that you chose to replicate from your source server upon AWS Replication Agent installation.

⚠ Important

Initial settings for EBS volumes are not derived from activity on the Source Server. Default values are chosen to give maximum performance on first launch.

Each disk is composed of the following fields:

- **Storage type** – Shows the default volume type (EBS). This cannot be changed.
- **Device name** – **Do not** change or edit this field. The device name shown here corresponds to the disk name on the source server. This field allows you to identify which disk is which.
- **Snapshot** – **Do not** change or edit this field. Snapshots should not be included in the launch template.
- **Size** – **Do not** change or edit this field.
- **Volume type** – You can select any volume type you want to use. AWS Application Migration Service automatically sets **General Purpose SSD (gp3)** as the default. You may want to change the volume type in order to reduce costs. Ensure that you read the caveats in the [EBS documentation](#).
- **IOPS** – Set the number of I/O operations per second that the volume can support. You can select any number as long as it matches the [EBS guidelines](#).
 - Provisioned IOPS SSD (io1) : 50 IOPS per GiB of storage
 - Provisioned IOPS SSD (io2) : 500 IOPS per GiB of storage
 - General Purpose SSD (gp3) : 500 IOPS per GiB of storage

AWS Application Migration Service automatically provisions the maximum IOPS possible for the volume, based on the above ratio. This is to minimize the impact of the [performance penalty](#) when working with EBS volumes created from snapshots.

- **Delete on termination** – **Do not** change or edit this field. This should not be included in the launch template.

- **Encrypted** – **Do not** change or edit this field. This should not be included in the launch template.
- **Key** – **Do not** change or edit this field. This should not be included in the launch template.
- **Add volume** – **Do not** use this functionality. You cannot add volumes to the source server through the launch template.
- **Remove (volume)** – **Do not** use this functionality. You cannot remove volumes from the source server through the launch template. If you do, AWS MGN will automatically create a volume using the default volume settings.
- **Resource tags** – You can add up to 50 tags. These will be transferred to your test and cutover instances. Note that these tags may interfere with other tags that have already been added to the source server. Launch template tags always take precedence over tags set in the AWS MGN console or tags manually assigned to the server.
- **Network interfaces** – The network interface is created by default based on your replication template. The network interface section is composed of the following fields:
 - **Device index** – **Do not** change or edit this field. The value should always be "0".
 - **Network interface** – Use this option only if you want use a pre-existing ENI (Elastic Network Interface). The Launch Template will overwrite certain ENI settings. Use this if you want to add an Elastic IP. You will have to attach the Elastic IP to the ENI.

 **Note**

When selecting an pre-existing ENI, you must change the **Auto-assign public IP** value to **Don't include in launch template** for a successful target launch.

- **Description** – Add an optional description for the network interface (if chosen).
- **Subnet** – Choose the subnet. This is the subnet within which the network interface is located and the test or cutover instance will be launched. AWS Application Migration Service selects the default VPC subnet by default (if one exists).
- **Auto-assign public IP** - Choose whether you want the public IP to be auto-assigned.
- **Primary IP** – Use this field if you wish to utilize a private IP. The private IP you set in the **Copy private IP** field in the AWS MGN launch settings will be copied to this field.
- **Secondary IP** - Define a secondary IP, if needed.

- **IPv6 IPs** – Define IPv6 IPs, if needed.
- **Security groups** – Choose a security group. If no security group is chosen, then the default VPC security group will be used by default.
- **Delete on termination** – We suggest choosing "Yes". Choosing "No" will make this network interface a permanent ENI.
- **Elastic Fabric Adapter** – **Do not** change or edit this field.
- **Network card index** – **Do not** change or edit this field.
- **Add network interface** – Note that the EC2 launch template only supports two network interfaces. If you require more than two network interfaces, you will need to define them after the test or cutover instance has been launched. This can be done through a post-launch action.
- **Advanced details** – In this section, we will focus on the fields you should **not** change or edit in order to allow AWS Application Migration Service to function properly. **Do not** change or edit any of the following fields:
 - RAM disk ID
 - Kernel
 - Nitro Enclave
 - Metadata accessible

Saving your EC2 launch template

Once you have finished editing your template, save it by choosing **Create template version** at the bottom of the template.

Launching test instances

After you have added all of your source servers and configured their launch settings, you are ready to launch a test instance. It is crucial to test the migration of your source servers to AWS prior to initiating a cutover in order to verify that your source servers function properly within the AWS environment.

Important

- It is a best practice to perform a test at least two weeks before you plan to migrate your source servers. This time frame allows you to identify potential problems and solve

them, before the actual cutover takes place. After launching test instances, use either SSH (Linux) or RDP (Windows) to connect to your instance and ensure that everything is working correctly.

- When launching a test or cutover instance, you can launch up to 100 source servers in a single operation. Additional source servers can be launched in subsequent operations.

You can test one source server at a time, or simultaneously test multiple source servers. For each source server, you will be informed of the success or failure of the test. You can test your source server as many times as you want. Each new test first deletes any previously launched Test instance and dependent resources. Then, a new test instance is launched, which reflects the most up-to-date state of the source server. After the test, data replication continues as before. The new and modified data on the source server is transferred to the Staging Area Subnet and not to the test instances that were launched during the test.

Note

- Windows source servers need to have at least 2 GB of free space to successfully launch a test instance.
- Take into consideration that once a test instance is launched, actual resources will be used in your AWS account and you will be billed for these resources. You can terminate the operation of launched Test instances once you verify that they are working properly without impact in order to data replication.

Topics

- [Ready for testing indicators](#)
- [Starting a test](#)
- [Reverting or finalizing a test](#)

Ready for testing indicators

Prior to launching a Test instance, ensure that your source servers are ready for testing by looking for the following indicators on the **Source servers** page:

1. Under the **Migration lifecycle** column, the server should show **Ready for testing**.

2. Under the **Data replication status** column, the server should show the **Healthy** status.
3. Under the **Next step** column, the server should show **Launch test instance**

Starting a test

To launch a test instance for a single source server or multiple source servers:

1. Go to the **Source servers** page.
2. Check the box to the left of each server for which you want to launch a test instance.
3. Open the **Test and cutover** menu.
4. Under **Testing**, choose the **Launch test instances** option to launch a test instance for this server.
5. When the **Launch test instances for X servers** dialog appears, click **Launch** to begin the test.

The AWS Application Migration Service console will indicate **Launch job started** when the test has started.

Choose **View job details** on the dialog to view the specific job for the test launch in the **Launch history** tab.

Successful test launch indicators

You can tell that the test instance launch started successfully through several indicators on the **Source servers** page.

1. The Alerts column will show the **Launched** status, indicating that a Test instance has been launched for this server.
2. The **Migration lifecycle** column will show **Test in progress**.
3. The **Next step** column will show **Complete testing and mark as 'Ready for cutover'**.

Reverting or finalizing a test

After you have launched your test instances, open the Amazon EC2 console and SSH or RDP into your test instances in order to ensure that they function correctly. Validate connectivity and perform acceptance tests for your application.

Topics

- [Reverting a test](#)
- [Marking as Ready for cutover](#)

Reverting a test

If you encounter any issues and want to launch new Test instances, or if you are performing a scheduled test and plan to perform additional tests prior to cutover, you can revert the test. This will revert your source servers' **Migration lifecycle** status to **Ready for testing**, indicating that these servers still require additional testing before they are ready for cutover. During a revert, you will also have the option to delete your Test instances for cost-saving purposes.

To revert a test:

1. Check the box to the left of every source server that has a launched Test instance for which you want to revert the test.
2. Open the **Test and cutover** menu.
3. Under **Testing**, choose **Revert to "ready for testing"**.
4. The **Revert testing for X servers** dialog will appear. Select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and choose **Revert**.

The AWS Application Migration Service console will indicate that testing has been reverted. The selected source servers' **Migration lifecycle** column will show the **Ready for testing** status, the **Next step** column will show **Launch test instance** and the launched Test instances will be deleted if that option was selected.

Marking as Ready for cutover

If you are completely done with your testing and are ready for cutover, you can finalize the test. This will change your source servers' **Migration lifecycle** status to **Ready for cutover**, indicating that all testing is complete and that these servers are now ready for cutover. You will also have the option to delete your Test instances for cost saving purposes.

To finalize a test:

1. Check the box to the left of every source server that has a launched Test instance for which you want to finalize the test.
2. Open the **Test and cutover** menu.
3. Under **Testing**, choose **Mark as "Ready for cutover"**.
4. When the **Mark X servers as "Ready for cutover"** dialog appears, select whether you want to terminate the launched instances used for testing. It is recommended to terminate these instances, as you will be charged for them even though you will no longer need them. Check the **Yes, terminate launched instances (recommended)** box and click **Continue**.

The AWS Application Migration Service console will confirm that the servers were marked as ready for cutover.

The AWS Application Migration Service console will indicate that testing has been finalized. The selected source servers' **Migration lifecycle** column will show the **Ready for cutover** status and the launched Test instances will be deleted if that option was selected. The **Next step** column will show **Terminate launched instance; Launch cutover instance**.

You can now terminate the launched Test instance directly from the Amazon EC2 console as that instance is no longer needed (if you have not done so already through the AWS MGN console). You can quickly access the Test instance by navigating to the specific servers > **Server details** > **Migration dashboard** > **Lifecycle** > **Launch status** and choosing **view in EC2 console**.

The Amazon EC2 console will automatically search for and display the Test instance. Select the instance, open the **Instance state** menu, and choose **Terminate instance**.

Click **Terminate**.

Launching cutover instances

Once you have finalized the testing of all of your source servers, you are ready for cutover. You should perform the cutover at a set date and time. The cutover will migrate your source servers to the cutover instances on AWS.

Important

It is a best practice to perform a test at least two weeks before you plan to migrate your source servers. This time frame allows you to identify potential problems and solve them,

before the actual migration takes place. After launching Test instances, use either SSH (Linux) or RDP (Windows) to connect to your instance and ensure that everything is working correctly.

You can cutover one source server at a time, or simultaneously cutover multiple source servers. For each source server, you will be informed of the success or failure of the cutover. For each new cutover, AWS Application Migration Service first deletes any previously launched Test instance and dependent resources. Then, it launches a new cutover instance which reflects the most up-to-date state of the source server. After the cutover, data replication continues as before. The new and modified data on the source server is transferred to the staging area subnet, and not to the cutover instances that were launched during the cutover.

Topics

- [Ready for cutover indicators](#)
- [Starting a cutover](#)
- [Reverting or finalizing a cutover](#)

Ready for cutover indicators

Prior to launching a cutover instance, ensure that your source servers are ready for cutover by looking for the following indicators on the **Source servers** page:

1. Under the **Migration lifecycle** column, the server should show **Ready for cutover** .
2. Under the **Data replication status** column, the server should show the **Healthy** status.
3. Under the **Next step** column, the server should show **Terminate launched instance; Launch cutover instance** if you have not terminated your latest launched test instance.
4. Alternatively, the Next step column will show **Launch cutover instance** if you have terminated your latest launched test instance.

Starting a cutover

To launch a cutover instance for a single source server or multiple source servers, go to the **Source servers** page and check the box to the left of each server you want to cutover.

Open the **Test and cutover** menu.

Under **Cutover**, choose the **Launch cutover instances** option.

The **Launch cutover instances for X servers** dialog will appear. Choose **Launch** to begin the cutover.

On the **Source servers** page, the **Migration lifecycle** column will show **Cutover in progress** and the **Next step** column will show **Finalize cutover**.

The AWS Application Migration Service console will indicate **Launch job started** when the cutover has started.

Choose **View job details** on the dialog to view the specific job for the cutover launch in the **Launch history** tab.

Successful cutover launch indicators

You can tell that the cutover instance launch was started successfully through several indicators on the **Source servers** page.

1. The **Alerts** column will state **Launched**.
2. The **Migration lifecycle** column will state **Cutover in progress**.
3. The **Data replication status** will state **Healthy**.
4. The **Next step column** will state **Finalize cutover**.

Reverting or finalizing a cutover

Once you have launched your cutover instances, open the Amazon EC2 console and SSH or RDP into your cutover instances in order to ensure that they function correctly. Validate connectivity and perform acceptance tests for your application.

Note

You should turn on Termination Protection after you have completed your testing and before you are ready to finalize the cutover. Learn more about enabling termination protection in [this Amazon EC2 article](#).

Reverting a cutover

If you encounter any issues and want to launch new cutover instances, you can revert the cutover. This will revert your source servers' **Migration lifecycle** status to **Ready for cutover**, indicating that these servers have not undergone cutover. During a revert, you will also have the option to delete your Cutover instances for cost-saving purposes.

To revert a cutover take the following steps:

1. Check the box to the left of every source server that has a launched cutover instance you want to revert.
2. Open the **Test and cutover** menu.
3. Under **Cutover**, choose **Revert to "ready for cutover"**.
4. This will revert your source servers' **Migration lifecycle** status to **Ready for cutover**, indicating that these servers have not undergone cutover.

When the **Revert cutover for X servers** dialog appears, click **Revert**.

Finalizing a cutover

If you are completely done with your migration and performed a successful cutover, you can finalize the cutover. This will change your source servers' **Migration lifecycle** status to **Cutover complete**, indicating that the cutover is complete and that the migration has been performed successfully. In addition, this will stop data replication and cause all replicated data to be discarded. All AWS resources used for data replication will be terminated.

To finalize a cutover:

1. Check the box to the left of every source server that has a launched cutover instance you want to finalize.
2. Open the **Test and cutover** menu.
3. Under **Cutover**, choose **Finalize cutover**.
4. The **Finalize cutover for X servers** dialog will appear. Choose **Finalize**. This will change your source servers' **Migration lifecycle** status to **Cutover complete**, indicating that the cutover is complete and that the migration has been performed successfully. In addition, this will stop data replication and cause all replicated data to be discarded. All AWS resources used for data replication will be terminated.

The AWS Application Migration Service console will indicate **Cutover finalized** when the cutover has completed successfully.

The AWS Application Migration Service console will automatically stop data replication for the source servers that were cutover in order to save resource costs. The selected source servers' **Migration lifecycle** column will show the **Cutover complete** status, the **Data replication** status column will show **Disconnected**, and the **Next step** column will show **Mark as archived**. The source servers have now been successfully migrated into AWS.

5. You can now archive your source servers that have launched cutover instances. Archiving will remove these source servers from the main **Source servers** page, allowing you to focus on source servers that have not yet been cutover. You will still be able to access the archived servers through filtering options.

To archive your cutover source servers:

- a. Check the box to the left of the of each source server for which the **Migration lifecycle** column states **Cutover complete**.
- b. Open the **Actions** menu and choose **Mark as archived**.
- c. When the **Archive X server** dialog will appears, click **Archive**.
- d. To see your archived servers, open the **Preferences** menu by choosing the gear button.

Toggle the **Show only archived servers** option and click **Confirm**.

You will now be able to see all of your archived servers. Untoggle the **Show only archived servers** option to show non-archived servers.

Launch history

The **Launch history** tab allows you to track and manage all of the operation performed in AWS Application Migration Service.

You can access the Launch History by choose **Launch history** on the left-hand navigation menu.

Topics

- [Overview](#)
- [Job details](#)

Overview

The Launch History tab shows all of the operations (referred to as "Jobs") performed on your account. Each Job corresponds to a single operation (for example, Launch cutover instance, Launch test instance, etc.) Each Job is composed of one or more servers. The main Launch History view allows you to easily identify all key Job parameters, including:

- **Job ID** – The unique ID of the Job.
- **Job type** – The type of Job (Launch or Terminate)
- **Initiated by** – The command or action that initiated the job (for example, Launch cutover instances or Terminate launched instances)
- **Status** – The status of the Job (Pending, Completed, or Started)
- **Servers** – The number of servers that are included in the Job.
- **Start time** – The time the job was started.
- **Completed time** – The time the Job was completed (blank if the job was not completed).

You can sort the launch history by any column by clicking the column header. (for example, sorting by **Job ID**).

You can search for specific Jobs by any of the available fields within the **Find launch history by property or value** search bar.

Example: Filtered search for the value "cutover", only showing Jobs that mention cutover.

Application Migration Service > Launch history

Launch history (28)

Filter launch history by property or value 6 matches < 1 >

"cutover" × Clear filters

Job ID	Job type	Initiated by	Status	Servers	Start time	Completed time
mgn-job0000000033-terminate-cutover	Terminate	Terminate launched instances	Completed	1	a day ago	a day ago
mgn-job0000000033-cutover	Launch	Launch cutover instances	Completed	1	a day ago	a day ago
mgn-job0000000032-terminate-cutover	Terminate	Terminate launched instances	Completed	1	a day ago	a day ago
mgn-job0000000032-cutover	Launch	Launch cutover instances	Completed	1	a day ago	a day ago
mgn-job0000000031-cutover	Launch	Launch cutover instances	Started	1	a day ago	

Job details

To view a detailed breakdown of each individual job, choose the **Job ID** of the specific job.

The **Job details** view is composed of 3 sections:

Topics

- [Details](#)
- [Job log](#)
- [Jobs – Source servers](#)

Details

The **Details** section shows the same information as the main Job log page, including the **Type**, **Status**, **Initiated by**, **Start time**, and **Completed time**.

Application Migration Service > Launch History > Job

Job: 150

Details

Type	Status	Initiated by
Launch	Started	Launch cutover instances
Start time	Completed time	
10/26/2020, 10:56:12 AM	-	

Job log

The Job log section shows a detailed log of all of the operations performed during the job.

Job log Info		
<input type="text" value="Filter job log by property or value"/>		< 1 2 3 >
Time	Event	Additional Data
10/26/2020, 10:38:13 AM	Job started	Source Server ID: 1 Conversion Server instance ID: conversionServer 0
10/26/2020, 10:39:13 AM	Cleanup started	Source Server ID: 2 Conversion Server instance ID: conversionServer 1
10/26/2020, 10:40:13 AM	Cleanup ended	Source Server ID: 3 Conversion Server instance ID: conversionServer 2
10/26/2020, 10:41:13 AM	Cleanup failed	Source Server ID: 4 Conversion Server instance ID: conversionServer 3
10/26/2020, 10:42:13 AM	Started taking snapshot	Source Server ID: 5 Conversion Server instance ID: conversionServer 4
10/26/2020, 10:43:13 AM	Finished taking snapshot	Source Server ID: 6 Conversion Server instance ID: conversionServer 5
10/26/2020, 10:44:13 AM	Failed to take snapshot	Source Server ID: 7 Conversion Server instance ID: conversionServer 6

Use this section to troubleshoot any potential issues and determine in which step of the launch process they occurred.

Use the **Filter job log by property or value** search bar to filter the job log.

You can filter by a variety of properties, including **Time**, **Event**, **Source server Id**, **Source server hostname**, **Conversion server instance IS**, **Test/cutover instance ID**, and **Error**.

You can filter by multiple values at once. (for example, Job log filtered by **Event: Failed to take snapshot** and a specific **Source server Id: 7**).

Job log [Info](#)

Q Filter job log by property or value 1 match < 1 >

Event: Failed to take snapshot X and Source Server Id: 7 X Clear filters

Time	Event	Additional Data
10/26/2020, 10:44:13 AM	Failed to take snapshot	Source Server ID: 7 Conversion Server instance ID: conversionServer 6

Jobs – Source servers

The **Source servers** section shows a list of all source servers involved in the job and their status.

Source servers (1)

Q Filter source servers by property or value < 1 >

Source server name	Status
43: cutting_over	In progress

You can use the **Filter source servers by property or value** search bar to filter by **Source server name** or **Status**.

Choose the **Source server name** of any of source server from the list to open the Server Details view for that server. [Learn more about server details.](#)

Monitoring Application Migration Service

Monitoring is an important part of maintaining the reliability, availability, and performance of Application Migration Service and your other AWS solutions. AWS provides the following monitoring tools to watch Application Migration Service, report when something is wrong, and take automatic actions when appropriate:

- *Amazon CloudWatch* monitors your AWS resources and the applications you run on AWS in real time. You can collect and track metrics, create customized dashboards, and set alarms that notify you or take actions when a specified metric reaches a threshold that you specify. For example, you can have CloudWatch track CPU usage or other metrics of your Amazon EC2 instances and automatically launch new instances when needed. For more information, see the [Amazon CloudWatch User Guide](#).
- *Amazon CloudWatch Events* delivers a near real-time stream of system events that describe changes in AWS resources. CloudWatch Events allows automated event-driven computing, as you can write rules that watch for certain events and trigger automated actions in other AWS services when these events happen. For more information, see the [Amazon CloudWatch Events User Guide](#).
- *Amazon CloudWatch Logs* allows you to monitor, store, and access your log files from Amazon EC2 instances, CloudTrail, and other sources. CloudWatch Logs can monitor information in the log files and notify you when certain thresholds are met. You can also archive your log data in highly durable storage. For more information, see the [Amazon CloudWatch Logs User Guide](#).
- *AWS CloudTrail* captures API calls and related events made by or on behalf of your AWS account and delivers the log files to an Amazon S3 bucket that you specify. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred. For more information, see the [AWS CloudTrail User Guide](#).

Monitoring Application Migration Service with Amazon CloudWatch

You can monitor Application Migration Service using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. These statistics are kept for 15 months, so that you can access historical information and gain a better perspective on how your web application or service is performing. You can also set alarms that watch for certain thresholds, and send

notifications or take actions when those thresholds are met. For more information, see the [Amazon CloudWatch User Guide](#).

Application Migration Service supports six CloudWatch metrics in the AWS/MGN namespace.

Application Migration Service includes the following metrics across all Source servers. The following metrics are dimensionless.

Metric name	Description
ActiveSourceServerCount	Number of Source servers that are not archived.
TotalSourceServerCount	Number of source servers, including those that are archived.

AWS Application Migration Service includes the following metrics by individual source server. The following metrics have a single dimension: **SourceServerID**.

Metric name	Description
LagDuration	The amount of time that has passed since the last consistent snapshot.
Backlog	The amount of data yet to be synced.
DurationSinceLastTest	The amount of time that has passed since the last Test instance launch.
ElapsedReplicationDuration	The cumulative amount of time this server has been replicating for (from which billing information is derived).

Application Migration Service EventBridge sample events

Application Migration Service sends events to Amazon EventBridge whenever a Source server launch has completed, a Source server reaches the READY_FOR_TEST lifecycle state for the first time, and when the data replication state becomes Stalled or when the data replication state

is no longer Stalled . You can use EventBridge and these events to write rules that take actions, such as notifying you, when a relevant event occurs. For more information, see [What is Amazon EventBridge?](#)

AWS Application Migration Service sends events on a best-effort basis to EventBridge. Event delivery is not guaranteed.

Event samples

The following are sample MGN events in EventBridge:

Topics

- [MGN source server launch result](#)
- [MGN source server lifecycle state change](#)
- [MGN source server data replication stalled change](#)

MGN source server launch result

Emitted when a test or cutover instance launch was completed (successfully or with failure).

Possible states (referring to the **state** field within the **details** field):

1. TEST_LAUNCH_SUCCEEDED
2. TEST_LAUNCH_FAILED
3. CUTOVER_LAUNCH_SUCCEEDED
4. CUTOVER_LAUNCH_FAILED

Sample event:

```
{
  "version": "0",
  "id": "9da9af57-9253-4406-87cb-7cc400e43465",
  "detail-type": "MGN Source Server Launch Result",
  "source": "aws.mgn",
  "account": "111122223333",
  "time": "2016-08-22T20:12:19Z",
```

```
"region": "us-west-2",
"resources": [
  "arn:aws:mgn:us-west-2:111122223333:source-server/s-12345678901234567"
],
"detail": {
  "state": "*TEST_LAUNCH_SUCCEEDED*",      "job-id": "*mgnjob-04ca7d0d3fb6afa3e*"
}
}
```

MGN source server lifecycle state change

Emitted when a source server reaches the `READY_FOR_TEST` lifecycle state for the first time.

Sample event:

```
{
  "version": "0",
  "id": "9da9af57-9253-4406-87cb-7cc400e43465",
  "detail-type": "MGN Source Server Lifecycle State Change",
  "source": "aws.mgn",
  "account": "111122223333",
  "time": "2016-08-22T20:12:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:mgn:us-west-2:111122223333:source-server/s-12345678901234567"
  ],
  "detail": {
    "state": "*READY_FOR_TEST*"
  }
}
```

MGN source server data replication stalled change

Emitted when the data replication state becomes stalled, and when data replication state is no longer stalled (not stalled).

Possible states (referring to the **state** field within the **details** field):

1. STALLED

2. NOT_STALLED

Sample event:

```
{
  "version": "0",
  "id": "9da9af57-9253-4406-87cb-7cc400e43465",
  "detail-type": "MGN Source Server Data Replication Stalled Change",
  "source": "aws.mgn",
  "account": "111122223333",
  "time": "2016-08-22T20:12:19Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:mgn:us-west-2:111122223333:source-server/s-12345678901234567"
  ],
  "detail": {
    "state": "*STALLED*"
  }
}
```

Registering event rules

You create CloudWatch Events event rules that capture events coming from your Application Migration Service resources.

Note

When you use the AWS Management Console to create an event rule, the console automatically adds the IAM permissions necessary to grant Amazon CloudWatch Events permissions to call your desired target type. If you are creating an event rule using the AWS CLI, you must grant permissions explicitly. For more information, see [Events and Event Patterns](#) in the Amazon CloudWatch User Guide.

To create your CloudWatch Events rules:

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

2. On the navigation pane, choose **Events, Create rule**.
3. For **Event source**, select **Event Pattern** as the event source, and then select **Build custom event pattern**.
4. Paste one following event pattern into the text area, depending on the event rule you wish to create:

- a. To catch all MGN events:

```
{
  "source": ["aws.mgn"]
}
```

- b. To catch all Lifecycle state changes:

```
{
  "detail-type": ["MGN Source Server Lifecycle State Change"],
  "source": ["aws.mgn"]
}
```

- c. To catch all events relating to a given source server:

```
{
  "source": ["aws.mgn"],
  "resources": [
    "arn:aws:mgn:us-west-2:111122223333:source-server/s-12345678901234567"
  ]
}
```

5. For **Targets**, choose **Add target**. For **Target type**, choose your desired target.
6. Choose **Configure details**.
7. For **Rule definition**, type a name and description for your rule and choose **Create rule**.

Logging AWS Application Migration Service with AWS CloudTrail

AWS Application Migration Service is integrated with AWS CloudTrail, a service that provides a record of actions taken by a user, role, or an AWS service in AWS Application Migration Service. CloudTrail captures all API calls for AWS Application Migration Service as events. The calls captured include calls from the AWS Application Migration Service console and code calls to the AWS

Application Migration Service API operations. If you create a trail, you can allow a continuous delivery of CloudTrail events to an Amazon S3 bucket, including events for AWS Application Migration Service. If you don't configure a trail, you can still view the most recent events in the CloudTrail console in **Event history**. Using the information collected by CloudTrail, you can determine the request that was made to AWS Application Migration Service, the IP address from which the request was made, who made the request, when it was made, and additional details.

To learn more about CloudTrail, see the [AWS CloudTrail User Guide](#).

AWS Application Migration Service information in CloudTrail

CloudTrail is activated on your AWS account when you create the account. When activity occurs in AWS Application Migration Service, that activity is recorded in a CloudTrail event along with other AWS service events in **Event history**. You can view, search, and download recent events in your AWS account. For more information, see [Viewing events with CloudTrail Event history](#).

For an ongoing record of events in your AWS account, including events for AWS Application Migration Service, create a trail. A *trail* allows CloudTrail to deliver log files to an Amazon S3 bucket. By default, when you create a trail in the console, the trail applies to all AWS Regions. The trail logs events from all Regions in the AWS partition and delivers the log files to the Amazon S3 bucket that you specify. Additionally, you can configure other AWS services to further analyze and act upon the event data collected in CloudTrail logs. For more information, see the following:

- [Overview for creating a trail](#)
- [CloudTrail supported services and integrations](#)
- [Configuring Amazon SNS notifications for CloudTrail](#)
- [Receiving CloudTrail log files from multiple regions](#) and [Receiving CloudTrail log files from multiple accounts](#)

All AWS Application Migration Service actions are logged by CloudTrail and are documented in the AWS Application Migration Service API. For example, calls to the `DescribeSourceServers` action to generate entries in the CloudTrail log files.

Every event or log entry contains information about who generated the request. The identity information helps you determine the following:

- Whether the request was made with root or AWS Identity and Access Management (IAM) user credentials.

- Whether the request was made with temporary security credentials for a role or federated user.
- Whether the request was made by another AWS service.

For more information, see the [CloudTrail `userIdentity` element](#).

Understanding AWS Application Migration Service log file entries

A trail is a configuration that allows for the delivery of events as log files to an Amazon S3 bucket that you specify. CloudTrail log files contain one or more log entries. An event represents a single request from any source and includes information about the requested action, the date and time of the action, request parameters, and so on. CloudTrail log files aren't an ordered stack trace of the public API calls, so they don't appear in any specific order.

The following example shows a CloudTrail log entry that demonstrates the `DescribeSourceServers`.

```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AAAAAAAAAAAAAAAAAAAA",
    "arn": "arn:aws:sts::1234567890:assumed-role/Admin/user",
    "accountId": "1234567890",
    "accessKeyId": "BBBBBBBBBBBBBBBBBBBB",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AAAAAAAAAAAAAAAAAAAA",
        "arn": "arn:aws:iam::1234567890:role/Admin",
        "accountId": "1234567890",
        "userName": "Admin"
      },
      "webIdFederationData": {},
      "attributes": {
        "creationDate": "2021-10-20T14:19:17Z",
        "mfaAuthenticated": "false"
      }
    }
  },
  "eventTime": "2021-10-20T14:19:59Z",
  "eventSource": "mgn.amazonaws.com",
```



```
"eventName": "DescribeSourceServers",
"awsRegion": "eu-west-1",
"sourceIPAddress": "54.240.197.234",
"userAgent": "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/94.0.4606.81 Safari/537.36",
"requestParameters": {
  "maxResults": 1000,
  "filters": {}
},
"responseElements": null,
"requestID": "d7618669-db08-4b53-bf6e-8a2cd57a677d",
"eventID": "436c17a7-3a54-4f4e-815d-4d980339744e",
"readOnly": true,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "1234567890",
"eventCategory": "Management"
}
```

Security in AWS Application Migration Service

Topics

- [Overview](#)
- [Identity and access management for AWS Application Migration Service](#)
- [Resilience in AWS Application Migration Service](#)
- [Infrastructure security in AWS Application Migration Service](#)
- [Compliance validation for AWS Application Migration Service](#)
- [Cross-service confused deputy prevention](#)

Overview

Cloud security at AWS is the highest priority. As an AWS customer, you benefit from a data center and network architecture that is built to meet the requirements of the most security-sensitive organizations.

Security is a shared responsibility between AWS and you. The [shared responsibility model](#) describes this as security of the cloud and security in the cloud:

- **Security of the cloud** – AWS is responsible for protecting the infrastructure that runs AWS services in the AWS Cloud. AWS also provides you with services that you can use securely. Third-party auditors regularly test and verify the effectiveness of our security as part of the [AWS Compliance Programs](#). To learn about the compliance programs that apply to AWS Application Migration Service (AWS MGN), see [AWS Services in Scope by Compliance Program](#).
- **Security in the cloud** – Your responsibility is determined by the AWS service that you use. You are also responsible for other factors including the sensitivity of your data, your company's requirements, and applicable laws and regulations

This documentation helps you understand how to apply the shared responsibility model when using AWS Application Migration Service. It shows you how to configure AWS Application Migration Service to meet your security and compliance objectives. You also learn how to use other AWS services that help you to monitor and secure your AWS Application Migration Service resources.

The customer is responsible for making sure that no misconfigurations are present during and after the migration process, including:

1. Access to replication servers should be allowed only from source servers CIDR range by applying proper security groups rules on replication servers.
2. After the migration, the customer should make sure that only allowed ports are exposed to the public internet.
3. Hardening of OS packages and other software deployed in the servers is completely under the customer's responsibility and we recommend the following:
 - a. Packages should be up to date and free of known vulnerabilities.
 - b. Only necessary OS/application services should be up and running.
4. Enabling the Anti-DDOS protection (AWS Shield) in the customer's AWS Account to eliminate the risk of denial of service attacks on the replication servers as well as the migrated servers.

Identity and access management for AWS Application Migration Service

AWS Identity and Access Management (IAM) is an AWS service that helps an administrator securely control access to AWS resources. IAM administrators control who can be authenticated (signed in) and authorized (have permissions) to use AWS resources. IAM enables you to create users and groups under your AWS account. You control the permissions that users have to perform tasks using AWS resources. You can use IAM for no additional charge.

By default, users created via the IAM service don't have permissions for AWS Application Migration Service (AWS MGN) resources and operations. To allow these users to manage AWS Application Migration Service resources, you must create an IAM policy that explicitly grants them permissions, and attach the policy to the users or groups that require those permissions.

When you attach a policy to a user or group of users, it allows or denies the users permission to perform the specified tasks on the specified resources. For more information, see [Policies and Permissions](#) in the *IAM User Guide* guide.

Federated identity

As a best practice, require human users, including users that require administrator access, to use federation with an identity provider to access AWS services by using temporary credentials.

A *federated identity* is a user from your enterprise user directory, a web identity provider, the AWS Directory Service, the Identity Center directory, or any user that accesses AWS services by using

credentials provided through an identity source. When federated identities access AWS accounts, they assume roles, and the roles provide temporary credentials.

For centralized access management, we recommend that you use AWS IAM Identity Center. You can create users and groups in IAM Identity Center, or you can connect and synchronize to a set of users and groups in your own identity source for use across all your AWS accounts and applications. For information about IAM Identity Center, see [What is IAM Identity Center?](#) in the *AWS IAM Identity Center User Guide*.

Authenticating with identities in AWS Application Migration Service

Authentication is how you sign in to AWS using your identity credentials. You must be *authenticated* (signed in to AWS) as the AWS account root user, as an IAM user, or by assuming an IAM role.

You can sign in to AWS as a federated identity by using credentials provided through an identity source. AWS IAM Identity Center (IAM Identity Center) users, your company's single sign-on authentication, and your Google or Facebook credentials are examples of federated identities. When you sign in as a federated identity, your administrator previously set up identity federation using IAM roles. When you access AWS by using federation, you are indirectly assuming a role.

Depending on the type of user you are, you can sign in to the AWS Management Console or the AWS access portal. For more information about signing in to AWS, see [How to sign in to your AWS account](#) in the *AWS Sign-In User Guide*.

If you access AWS programmatically, AWS provides a software development kit (SDK) and a command line interface (CLI) to cryptographically sign your requests by using your credentials. If you don't use AWS tools, you must sign requests yourself. For more information about using the recommended method to sign requests yourself, see [Signing AWS API requests](#) in the *IAM User Guide*.

Regardless of the authentication method that you use, you might be required to provide additional security information. For example, AWS recommends that you use multi-factor authentication (MFA) to increase the security of your account. To learn more, see [Multi-factor authentication](#) in the *AWS IAM Identity Center User Guide* and [Using multi-factor authentication \(MFA\) in AWS](#) in the *IAM User Guide*.

AWS account root user

When you create an AWS account, you begin with one sign-in identity that has complete access to all AWS services and resources in the account. This identity is called the AWS account *root user* and is accessed by signing in with the email address and password that you used to create the account. We strongly recommend that you don't use the root user for your everyday tasks. Safeguard your root user credentials and use them to perform the tasks that only the root user can perform. For the complete list of tasks that require you to sign in as the root user, see [Tasks that require root user credentials](#) in the *IAM User Guide*.

IAM users and groups

An [IAM user](#) is an identity within your AWS account that has specific permissions for a single person or application. Where possible, we recommend relying on temporary credentials instead of creating IAM users who have long-term credentials such as passwords and access keys. However, if you have specific use cases that require long-term credentials with IAM users, we recommend that you rotate access keys. For more information, see [Rotate access keys regularly for use cases that require long-term credentials](#) in the *IAM User Guide*.

An [IAM group](#) is an identity that specifies a collection of IAM users. You can't sign in as a group. You can use groups to specify permissions for multiple users at a time. Groups make permissions easier to manage for large sets of users. For example, you could have a group named *IAMAdmins* and give that group permissions to administer IAM resources.

Users are different from roles. A user is uniquely associated with one person or application, but a role is intended to be assumable by anyone who needs it. Users have permanent long-term credentials, but roles provide temporary credentials. To learn more, see [When to create an IAM user \(instead of a role\)](#) in the *IAM User Guide*.

IAM roles

An [IAM role](#) is an identity within your AWS account that has specific permissions. It is similar to an IAM user, but is not associated with a specific person. You can temporarily assume an IAM role in the AWS Management Console by [switching roles](#). You can assume a role by calling an AWS CLI or AWS API operation or by using a custom URL. For more information about methods for using roles, see [Using IAM roles](#) in the *IAM User Guide*.

IAM roles with temporary credentials are useful in the following situations:

- **Federated user access** – To assign permissions to a federated identity, you create a role and define permissions for the role. When a federated identity authenticates, the identity is associated with the role and is granted the permissions that are defined by the role. For information about roles for federation, see [Creating a role for a third-party Identity Provider](#) in the *IAM User Guide*. If you use IAM Identity Center, you configure a permission set. To control what your identities can access after they authenticate, IAM Identity Center correlates the permission set to a role in IAM. For information about permission sets, see [Permission sets](#) in the *AWS IAM Identity Center User Guide*.
- **Temporary IAM user permissions** – An IAM user or role can assume an IAM role to temporarily take on different permissions for a specific task.
- **Cross-account access** – You can use an IAM role to allow someone (a trusted principal) in a different account to access resources in your account. Roles are the primary way to grant cross-account access. However, with some AWS services, you can attach a policy directly to a resource (instead of using a role as a proxy). To learn the difference between roles and resource-based policies for cross-account access, see [Cross account resource access in IAM](#) in the *IAM User Guide*.
- **Cross-service access** – Some AWS services use features in other AWS services. For example, when you make a call in a service, it's common for that service to run applications in Amazon EC2 or store objects in Amazon S3. A service might do this using the calling principal's permissions, using a service role, or using a service-linked role.
 - **Forward access sessions (FAS)** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. When you use some services, you might perform an action that then initiates another action in a different service. FAS uses the permissions of the principal calling an AWS service, combined with the requesting AWS service to make requests to downstream services. FAS requests are only made when a service receives a request that requires interactions with other AWS services or resources to complete. In this case, you must have permissions to perform both actions. For policy details when making FAS requests, see [Forward access sessions](#).
- **Service role** – A service role is an [IAM role](#) that a service assumes to perform actions on your behalf. An IAM administrator can create, modify, and delete a service role from within IAM. For more information, see [Creating a role to delegate permissions to an AWS service](#) in the *IAM User Guide*.
- **Service-linked role** – A service-linked role is a type of service role that is linked to an AWS service. The service can assume the role to perform an action on your behalf. Service-linked roles appear in your AWS account and are owned by the service. An IAM administrator can view, but not edit the permissions for service-linked roles.

- **Applications running on Amazon EC2** – You can use an IAM role to manage temporary credentials for applications that are running on an EC2 instance and making AWS CLI or AWS API requests. This is preferable to storing access keys within the EC2 instance. To assign an AWS role to an EC2 instance and make it available to all of its applications, you create an instance profile that is attached to the instance. An instance profile contains the role and enables programs that are running on the EC2 instance to get temporary credentials. For more information, see [Using an IAM role to grant permissions to applications running on Amazon EC2 instances](#) in the *IAM User Guide*.

To learn whether to use IAM roles or IAM users, see [When to create an IAM role \(instead of a user\)](#) in the *IAM User Guide*.

Grant permission to tag resources during creation

Some resource-creating Amazon MGN API actions enable you to specify tags when you create the resource. You can use resource tags to implement attribute-based control (ABAC).

To enable users to tag resources on creation, they must have permissions to use the action that creates the resource, such as `mgn:RegisterAgentForMgn`. If tags are specified in the resource-creating action, Amazon performs additional authorization on the `mgn:TagResource` action to verify if users have permissions to create tags. Therefore, users must also have explicit permissions to use the `mgn:TagResource` action.

In the IAM policy definition for the `mgn:TagResource` action, use the `Condition` element with the `mgn:CreateAction` condition key to give tagging permissions to the action that creates the resource. The following example demonstrates a policy that allows an agent installer to create a source server and apply any tags to the source server on creation. The installer is not permitted to tag any existing resources (it cannot call the `mgn:TagResource` action directly).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
      ]
    }
  ]
}
```

```

    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "mgn:RegisterAgentForMgn",
      "mgn:UpdateAgentSourcePropertiesForMgn",
      "mgn:UpdateAgentReplicationInfoForMgn",
      "mgn:UpdateAgentConversionInfoForMgn",
      "mgn:GetAgentInstallationAssetsForMgn",
      "mgn:GetAgentCommandForMgn",
      "mgn:GetAgentConfirmedResumeInfoForMgn",
      "mgn:GetAgentRuntimeConfigurationForMgn",
      "mgn:UpdateAgentBacklogForMgn",
      "mgn:GetAgentReplicationInfoForMgn"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": "mgn:TagResource",
    "Resource": "arn:aws:mgn:*:*:source-server/*",
    "Condition": {
      "StringEquals": {
        "mgn:CreateAction": "RegisterAgentForMgn"
      }
    }
  }
]
}

```

The `mgn:TagResource` action is only evaluated if tags are applied during the resource-creating action. Therefore, an installer that has permissions to create a resource (assuming there are no tagging conditions) does not require permissions to use the `mgn:TagResource` action if no tags are specified in the request. However, if the installer attempts to create a resource with tags, the request fails if the installer does not have permissions to use the `mgn:TagResource` action.

AWS managed policies for AWS Application Migration Service

To add permissions to users, groups, and roles, it is easier to use AWS managed policies than to write policies yourself. It takes time and expertise to [create IAM customer managed policies](#) that provide your team with only the permissions they need. To get started quickly, you can use our AWS managed policies. These policies cover common use cases and are available in your AWS account. For more information about AWS managed policies, see [AWS managed policies](#) in the *IAM User Guide*.

AWS services maintain and update AWS managed policies. You can't change the permissions in AWS managed policies. Services occasionally add additional permissions to an AWS managed policy to support new features. This type of update affects all identities (users, groups, and roles) where the policy is attached. Services are most likely to update an AWS managed policy when a new feature is launched or when new operations become available. Services do not remove permissions from an AWS managed policy, so policy updates won't break your existing permissions.

Additionally, AWS supports managed policies for job functions that span multiple services. For example, the **ReadOnlyAccess** AWS managed policy provides read-only access to all AWS services and resources. When a service launches a new feature, AWS adds read-only permissions for new operations and resources. For a list and descriptions of job function policies, see [AWS managed policies for job functions](#) in the *IAM User Guide*. AWS MGN read-only permissions are included in the general IAM ReadOnlyAccess policy.

Topics

- [AWS managed policy: AWSApplicationMigrationServiceRolePolicy](#)
- [AWS managed policy: AWSApplicationMigrationConversionServerPolicy](#)
- [AWS managed policy: AWSApplicationMigrationReplicationServerPolicy](#)
- [AWS managed policy: AWSApplicationMigrationAgentPolicy](#)
- [AWS managed policy: AWSApplicationMigrationMGHAccess](#)
- [AWS managed policy: AWSApplicationMigrationFullAccess](#)
- [AWS managed policy: AWSApplicationMigrationEC2Access](#)
- [AWS managed policy: AWSApplicationMigrationSSMAccess](#)
- [AWS managed policy: AWSApplicationMigrationReadOnlyAccess](#)
- [AWS managed policy: AWSApplicationMigrationVCenterClientPolicy](#)
- [AWS managed policy: AWSApplicationMigrationAgentInstallationPolicy](#)
- [AWS managed policy: AWSApplicationMigrationAgentPolicy_v2](#)

- [AWS managed policy: AWSApplicationMigrationServiceEc2InstancePolicy](#)
- [AWS MGN updates for AWS managed policies](#)

AWS managed policy: AWSApplicationMigrationServiceRolePolicy

This policy is attached to the AWS MGN Service-Linked Role (SLR). [Learn more.](#)

This policy allows AWS Application Migration Service to manage AWS resources on your behalf.

Permissions details

This policy includes the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "mgn:ListTagsForResource",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "kms:ListRetirableGrants",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource": "*"
    },
    {
```

```

"Effect": "Allow",
"Action": [
  "ec2:DescribeAccountAttributes",
  "ec2:DescribeAvailabilityZones",
  "ec2:DescribeImages",
  "ec2:DescribeInstances",
  "ec2:DescribeInstanceTypes",
  "ec2:DescribeInstanceAttribute",
  "ec2:DescribeInstanceStatus",
  "ec2:DescribeLaunchTemplateVersions",
  "ec2:DescribeLaunchTemplates",
  "ec2:DescribeSecurityGroups",
  "ec2:DescribeSnapshots",
  "ec2:DescribeSubnets",
  "ec2:DescribeVolumes",
  "ec2:GetEbsDefaultKmsKeyId",
  "ec2:GetEbsEncryptionByDefault"
],
"Resource": "*"
},
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount"
      ],
      "Resource": "arn:aws:organizations::*:account/*"
    },
  {
    "Effect": "Allow",
    "Action": [
      "organizations:DescribeOrganization",
      "organizations:ListAWSServiceAccessForOrganization",
      "organizations:ListDelegatedAdministrators",
      "organizations:ListAccounts"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:RegisterImage",
      "ec2:DeregisterImage"
    ],
    "Resource": "*"
  }

```

```
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:DeleteSnapshot"
  ],
  "Resource": "arn:aws:ec2:*:*:snapshot/*",
  "Condition": {
    "Null": {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateLaunchTemplateVersion",
    "ec2:ModifyLaunchTemplate",
    "ec2>DeleteLaunchTemplate",
    "ec2>DeleteLaunchTemplateVersions"
  ],
  "Resource": "arn:aws:ec2:*:*:launch-template/*",
  "Condition": {
    "Null": {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2>DeleteVolume"
  ],
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Condition": {
    "Null": {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:StartInstances",
```

```

    "ec2:StopInstances",
    "ec2:TerminateInstances",
    "ec2:ModifyInstanceAttribute",
    "ec2:GetConsoleOutput",
    "ec2:GetConsoleScreenshot"
  ],
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "Null": {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:RevokeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:AuthorizeSecurityGroupEgress"
  ],
  "Resource": "arn:aws:ec2:*:*:security-group/*",
  "Condition": {
    "Null": {
      "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateVolume"
  ],
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Condition": {
    "Null": {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateSecurityGroup"
  ],

```

```

"Resource": "arn:aws:ec2:*:*:security-group/*",
"Condition": {
  "Null": {
    "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateSecurityGroup"
  ],
  "Resource": "arn:aws:ec2:*:*:vpc/*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateLaunchTemplate"
  ],
  "Resource": "arn:aws:ec2:*:*:launch-template/*",
  "Condition": {
    "Null": {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateSnapshot"
  ],
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Condition": {
    "Null": {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateSnapshot"
  ],
  "Resource": "arn:aws:ec2:*:*:snapshot/*",

```

```
"Condition": {
  "Null": {
    "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:DetachVolume",
    "ec2:AttachVolume"
  ],
  "Resource": "arn:aws:ec2:*:*:instance/*",
  "Condition": {
    "Null": {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:AttachVolume"
  ],
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Condition": {
    "Null": {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:DetachVolume"
  ],
  "Resource": "arn:aws:ec2:*:*:volume/*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:RunInstances"
  ],
  "Resource": "arn:aws:ec2:*:*:instance/*",
```

```

"Condition": {
  "Null": {
    "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
  }
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:RunInstances"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:subnet/*",
    "arn:aws:ec2:*:*:image/*",
    "arn:aws:ec2:*:*:network-interface/*",
    "arn:aws:ec2:*:*:launch-template/*"
  ]
},
{
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": [
    "arn:aws:iam:*:*:role/service-role/AWSApplicationMigrationReplicationServerRole",
    "arn:aws:iam:*:*:role/service-role/AWSApplicationMigrationConversionServerRole"
  ],
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": "ec2.amazonaws.com"
    }
  }
},
{
  "Effect": "Allow",
  "Action": "ec2:CreateTags",
  "Resource": [
    "arn:aws:ec2:*:*:launch-template/*",
    "arn:aws:ec2:*:*:security-group/*",
    "arn:aws:ec2:*:*:volume/*",
    "arn:aws:ec2:*:*:snapshot/*",
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {

```



```

    "StringEquals": {
      "ec2:CreateAction": [
        "CreateLaunchTemplate",
        "CreateSecurityGroup",
        "CreateVolume",
        "CreateSnapshot",
        "RunInstances"
      ]
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags",
      "ec2:ModifyVolume"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition": {
      "Null": {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      }
    }
  }
]
}

```

AWS managed policy: AWSApplicationMigrationConversionServerPolicy

This policy is attached to the AWS Application Migration Service conversion server's instance role.

This policy allows the AWS Application Migration Service (AWS MGN) conversion server, which are EC2 instances launched by AWS Application Migration Service, to communicate with the AWS MGN service. An IAM role with this policy is attached (as an EC2 Instance Profile) by AWS MGN to the AWS MGN Conversion Servers, which are automatically launched and terminated by AWS MGN, when needed. We do not recommend that you attach this policy to your users or roles. AWS MGN conversion servers are used by AWS Application Migration Service when users choose to launch test or cutover instances using the AWS MGN console, CLI, or API.

Permissions details

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS managed policy: AWSApplicationMigrationReplicationServerPolicy

This policy is attached to the AWS Application Migration Service replication server's instance role.

This policy allows the AWS Application Migration Service (AWS MGN) Replication Servers, which are EC2 instances launched by AWS Application Migration Service - to communicate with the AWS MGN service, and to create EBS snapshots in your AWS account. An IAM role with this policy is attached (as an EC2 Instance Profile) by AWS Application Migration Service to the AWS MGN replication servers which are automatically launched and terminated by AWS MGN, as needed. AWS MGN Replication Servers are used to facilitate data replication from your external servers to AWS, as part of the migration process managed using AWS MGN. We do not recommend that you attach this policy to your users or roles.

Permissions details

This policy includes the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

    "Effect": "Allow",
    "Action": [
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:GetChannelCommandsForMgn",
        "mgn:SendChannelCommandResultForMgn",
        "mgn:GetAgentSnapshotCreditsForMgn",
        "mgn:DescribeReplicationServerAssociationsForMgn",
        "mgn:DescribeSnapshotRequestsForMgn",
        "mgn:BatchDeleteSnapshotRequestForMgn",
        "mgn:NotifyAgentAuthenticationForMgn",
        "mgn:BatchCreateVolumeSnapshotGroupForMgn",
        "mgn:UpdateAgentReplicationProcessStateForMgn",
        "mgn:NotifyAgentReplicationProgressForMgn",
        "mgn:NotifyAgentConnectedForMgn",
        "mgn:NotifyAgentDisconnectedForMgn"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeSnapshots"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSnapshot"
    ],
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
        "Null": {
            "aws:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSnapshot"

```

```

        ],
        "Resource": "arn:aws:ec2:*:*:snapshot/*",
        "Condition": {
            "Null": {
                "aws:RequestTag/
AWSApplicationMigrationServiceManaged": "false"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": "CreateSnapshot"
            }
        }
    }
]
}

```

AWS managed policy: AWSApplicationMigrationAgentPolicy

You can attach the `AWSApplicationMigrationAgentPolicy` policy to your IAM identities.

This policy allows installing and using the AWS Replication Agent, which is used with AWS Application Migration Service (AWS MGN) to migrate external servers to AWS. Attach this policy to your users whose credentials you provide when installing the AWS replication agent.

Permissions details

This policy includes the following permissions.

```

{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [

```

```

        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "mgn:RegisterAgentForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": "mgn:TagResource",
    "Resource": "arn:aws:mgn:*:*:source-server/*"
}
]
}

```

AWS managed policy: AWSApplicationMigrationMGHAccess

This policy allows AWS Application Migration Service (AWS MGN) to send metadata about the progress of servers being migrated using AWS MGN to AWS Migration Hub (MGH). AWS MGN automatically creates an IAM role with this policy attached and assumes this role. We do not recommend that you attach this policy to your users or roles. Migration-progress data is only sent after the AWS "home region" is set in AWS MGH. If the Home AWS Region is different than the AWS Region into which a server is being migrated, this data will be sent cross-region. To stop AWS MGN from sending this metadata to AWS MGH, detach it from your users or roles.

Permissions details

This policy includes the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS managed policy: AWSApplicationMigrationFullAccess

You can attach the `AWSApplicationMigrationFullAccess` policy to your IAM identities.

This policy provides permissions to all public APIs of AWS Application Migration Service (AWS MGN), as well as permissions to read KMS key, License Manager, Resource Groups, Elastic Load Balancing, IAM, and EC2 information. Attach this policy to your users or roles.

Permissions details

This policy includes the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
```

```
"Effect": "Allow",
"Action": [
  "mgn:*"
],
"Resource": "*"
},
{
  "Sid": "VisualEditor1",
  "Effect": "Allow",
  "Action": [
    "kms:ListAliases",
    "kms:DescribeKey"
  ],
  "Resource": "*"
},
{
  "Sid": "VisualEditor2",
  "Effect": "Allow",
  "Action": [
    "ec2:DescribeKeyPairs",
    "ec2:DescribeTags",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePlacementGroups",
    "ec2:DescribeAccountAttributes",
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeImages",
    "ec2:DescribeInstances",
    "ec2:DescribeInstanceTypes",
    "ec2:DescribeInstanceAttribute",
    "ec2:DescribeInstanceStatus",
    "ec2:DescribeInstanceTypeOfferings",
    "ec2:DescribeLaunchTemplateVersions",
    "ec2:DescribeLaunchTemplates",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeSubnets",
    "ec2:DescribeVolumes",
    "ec2:GetEbsEncryptionByDefault",
    "ec2:GetEbsDefaultKmsKeyId"
  ],
  "Resource": "*"
},
{
  "Sid": "VisualEditor3",
```

```

    "Effect": "Allow",
    "Action": "license-manager:ListLicenseConfigurations",
    "Resource": "*"
  },
  {
    "Sid": "VisualEditor4",
    "Effect": "Allow",
    "Action": "elasticloadbalancing:DescribeLoadBalancers",
    "Resource": "*"
  },
  {
    "Sid": "VisualEditor5",
    "Effect": "Allow",
    "Action": "iam:ListInstanceProfiles",
    "Resource": "*"
  },
  {
    "Sid": "VisualEditor6",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
      "arn:aws:iam::*:role/service-role/
AWSApplicationMigrationLaunchInstanceWithSsmRole",
      "arn:aws:iam::*:role/service-role/AWSApplicationMigrationLaunchInstanceWithDrsRole"
    ],
    "Condition": {
      "StringEquals": {
        "iam:PassedToService": "ec2.amazonaws.com"
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Sid": "VisualEditor7",
    "Effect": "Allow",
    "Action": [
      "drs:DescribeSourceServers"
    ],
    "Resource": "*"
  },
  {
    "Sid": "VisualEditor8",

```



```
"Effect": "Allow",
"Action": [
  "ssm:SendCommand"
],
"Resource": [
  "arn:aws:ec2:*:*:instance/*"
],
"Condition": {
  "Bool": {
    "aws:ViaAWSService": "true"
  },
  "Null": {
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
  }
}
},
{
  "Sid": "VisualEditor9",
  "Effect": "Allow",
  "Action": [
    "ssm:ListCommandInvocations"
  ],
  "Resource": "*"
},
{
  "Sid": "VisualEditor10",
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeInstanceInformation",
    "ssm:GetCommandInvocation"
  ],
  "Resource": "*",
  "Condition": {
    "Bool": {
      "aws:ViaAWSService": "true"
    }
  }
},
{
  "Sid": "VisualEditor11",
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeDocument",
    "ssm:SendCommand"
```

```

],
"Resource": [
  "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
  "arn:aws:ssm:*:*:document/AWSMigration-*"
],
"Condition": {
  "Bool": {
    "aws:ViaAWSService": "true"
  }
}
},
{
  "Sid": "VisualEditor12",
  "Effect": "Allow",
  "Action": [
    "drs:DisconnectSourceServer"
  ],
  "Resource": "arn:aws:drs:*:*:source-server/*",
  "Condition": {
    "Bool": {
      "aws:ViaAWSService": "true"
    },
    "Null": {
      "aws:ResourceTag/AWSApplicationMigrationServiceConfiguredDR": "false"
    }
  }
},
{
  "Sid": "VisualEditor13",
  "Effect": "Allow",
  "Action": [
    "ssm:GetParameter",
    "ssm:PutParameter"
  ],
  "Resource": "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-*"
},
{
  "Sid": "VisualEditor14",
  "Effect": "Allow",
  "Action": [
    "servicequotas:GetServiceQuota"
  ],
  "Resource": "*"
},

```

```
{
  "Sid": "VisualEditor15",
  "Effect": "Allow",
  "Action": [
    "ssm:GetAutomationExecution"
  ],
  "Resource": "arn:aws:ssm:*:*:automation-execution/*"
},
{
  "Sid": "VisualEditor16",
  "Effect": "Allow",
  "Action": [
    "ssm:GetDocument"
  ],
  "Resource": [
    "arn:aws:ssm:*:*:document/AWSDisasterRecovery-InstallDRAgentOnInstance",
    "arn:aws:ssm:*:*:document/AWSMigration-*"
  ]
},
{
  "Sid": "VisualEditor17",
  "Effect": "Allow",
  "Action": [
    "ssm:GetParameters"
  ],
  "Resource": "arn:aws:ssm:*:*:parameter/ManagedByAWSApplicationMigrationService-*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "ssm.amazonaws.com"
    }
  }
},
{
  "Sid": "VisualEditor18",
  "Effect": "Allow",
  "Action": [
    "ssm:StartAutomationExecution"
  ],
  "Resource": "arn:aws:ssm:*:*:automation-definition/AWSMigration-*:$DEFAULT",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "mgn.amazonaws.com"
    }
  }
}
```

```
},
{
  "Sid": "VisualEditor19",
  "Effect": "Allow",
  "Action": "ssm:ListCommands",
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": "ssm.amazonaws.com"
    }
  }
},
{
  "Sid": "VisualEditor20",
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeParameters"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
        "mgn.amazonaws.com"
      ]
    }
  }
}
]
```

AWS managed policy: AWSApplicationMigrationEC2Access

You can attach the AWSApplicationMigrationEC2Access policy to your IAM identities.

This policy allows Amazon EC2 operations required to use AWS Application Migration Service (AWS MGN) to launch the migrated servers as EC2 instances. Attach this policy to your users or roles. This policy is only intended to be used for the MGN console.

Permissions details

This policy includes the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": [
        "arn:aws:iam::*:role/service-role/AWSApplicationMigrationConversionServerRole"
      ],
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DeleteSnapshot"
      ],
      "Resource": "arn:aws:ec2:*:*:snapshot/*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
        },
        "Bool": {
          "aws:ViaAWSService": "true"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes"
      ],
      "Resource": "*",
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```

    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateLaunchTemplateVersion",
      "ec2:ModifyLaunchTemplate",
      "ec2>DeleteLaunchTemplateVersions"
    ],
    "Resource": "arn:aws:ec2:*:*:launch-template/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateLaunchTemplate"
    ],
    "Resource": "arn:aws:ec2:*:*:launch-template/*",
    "Condition": {
      "Null": {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
      },
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": [
          "mgn.amazonaws.com"
        ]
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2>DeleteLaunchTemplate"
    ],
    "Resource": "arn:aws:ec2:*:*:launch-template/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      }
    }
  },

```

```

    "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
        "mgn.amazonaws.com"
      ]
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DeleteVolume"
    ],
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:GetConsoleOutput",
      "ec2:GetConsoleScreenshot"
    ],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "Null": {
        "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",

```

```

"Action": [
  "ec2:RevokeSecurityGroupEgress",
  "ec2:AuthorizeSecurityGroupIngress",
  "ec2:AuthorizeSecurityGroupEgress"
],
"Resource": "arn:aws:ec2:*:*:security-group/*",
"Condition": {
  "Null": {
    "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
  },
  "Bool": {
    "aws:ViaAWSService": "true"
  }
}
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateVolume"
  ],
  "Resource": "arn:aws:ec2:*:*:volume/*",
  "Condition": {
    "Null": {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
    },
    "Bool": {
      "aws:ViaAWSService": "true"
    }
  }
}
},
{
  "Effect": "Allow",
  "Action": "ec2:CreateSecurityGroup",
  "Resource": "arn:aws:ec2:*:*:vpc/*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateSecurityGroup"
  ],
  "Resource": "arn:aws:ec2:*:*:security-group/*",
  "Condition": {
    "Null": {
      "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
    }
  }
}

```



```

    },
    "Bool": {
      "aws:ViaAWSService": "true"
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateSnapshot"
    ],
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
      "Null": {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateSnapshot"
    ],
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
      "Null": {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DetachVolume",
      "ec2:AttachVolume"
    ],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {

```

```

    "Null": {
      "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
    },
    "Bool": {
      "aws:ViaAWSService": "true"
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:AttachVolume"
    ],
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
      "Null": {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DetachVolume"
    ],
    "Resource": "arn:aws:ec2:*:*:volume/*",
    "Condition": {
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:RunInstances"
    ],
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "Null": {
        "aws:RequestTag/AWSApplicationMigrationServiceManaged": "false"
      }
    }
  }
}

```

```

    },
    "Bool": {
      "aws:ViaAWSService": "true"
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:RunInstances"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:subnet/*",
      "arn:aws:ec2:*:*:image/*",
      "arn:aws:ec2:*:*:network-interface/*",
      "arn:aws:ec2:*:*:launch-template*"
    ],
    "Condition": {
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": [
      "arn:aws:ec2:*:*:security-group/*",
      "arn:aws:ec2:*:*:volume/*",
      "arn:aws:ec2:*:*:snapshot/*",
      "arn:aws:ec2:*:*:instance/*",
      "arn:aws:ec2:*:*:launch-template*"
    ],
    "Condition": {
      "StringEquals": {
        "ec2:CreateAction": [
          "CreateSecurityGroup",
          "CreateVolume",
          "CreateSnapshot",
          "RunInstances",
          "CreateLaunchTemplate"
        ]
      }
    }
  }
]

```

```

    },
    "Bool": {
      "aws:ViaAWSService": "true"
    }
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:CreateTags",
      "ec2:ModifyVolume"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition": {
      "Null": {
        "ec2:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
      },
      "Bool": {
        "aws:ViaAWSService": "true"
      }
    }
  },
  {
    "Effect": "Allow",
    "Action": "ssm:ListCommands",
    "Resource": "*",
    "Condition": {
      "ForAnyValue:StringEquals": {
        "aws:CalledVia": "ssm.amazonaws.com"
      }
    }
  }
]
}

```

AWS managed policy: AWSApplicationMigrationSSMAccess

You can attach the AWSApplicationMigrationSSMAccess policy to your IAM identities.

This policy allows Amazon SSM operations required to use AWS Application Migration Service (AWS MGN) to run SSM documents post migration of source servers. Attach this policy to your users or roles. This policy is only intended to be used for the AWS MGN console.

Permissions details

This policy includes the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation"
      ],
      "Resource": [
        "*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "mgn.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:DescribeDocument",
        "ssm:StartAutomationExecution"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/*",
        "arn:aws:ssm:*:*:automation-definition/*:*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "mgn.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

```

        ]
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "ForAnyValue:StringEquals": {
          "aws:CalledVia": [
            "mgn.amazonaws.com"
          ]
        },
        "Null": {
          "aws:ResourceTag/AWSApplicationMigrationServiceManaged": "false"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:ListDocuments"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:ListDocumentVersions",
        "ssm:GetDocument"
      ],
      "Resource": "arn:aws:ssm:*:*:document/*"
    }
  ]
}

```

AWS managed policy: AWSApplicationMigrationReadOnlyAccess

You can attach the `AWSApplicationMigrationReadOnlyAccess` policy to your IAM identities.

This policy provides permissions to all read-only public APIs of AWS Application Migration Service (AWS MGN), as well as some read-only APIs of other AWS services that are required in order to make full read-only use of the AWS MGN console. Attach this policy to your users or roles.

Permissions details

This policy includes the following permissions.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgn:DescribeJobLogItems",
        "mgn:DescribeJobs",
        "mgn:DescribeSourceServers",
        "mgn:DescribeReplicationConfigurationTemplates",
        "mgn:GetLaunchConfiguration",
        "mgn:DescribeVcenterClients",
        "mgn:GetReplicationConfiguration",
        "mgn:DescribeLaunchConfigurationTemplates",
        "mgn:ListSourceServerActions",
        "mgn:ListTemplateActions",
        "mgn:ListApplications",
        "mgn:ListWaves",
        "mgn:ListExports",
        "mgn:ListImports",
        "mgn:ListImportErrors",
        "mgn:ListExportErrors"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
    }
  ]
}
```

```

        "Resource": "*"
      },
      {
        "Effect": "Allow",
        "Action": [
          "servicequotas:GetServiceQuota"
        ],
        "Resource": "*"
      }
    ]
  }
}

```

AWS managed policy: AWSApplicationMigrationVCenterClientPolicy

You can attach the `AWSApplicationMigrationVCenterClientPolicy` policy to your IAM identities.

This policy allows installing and using the AWS VCenter Client, which is used with AWS Application Migration Service (AWS MGN) to migrate external servers to AWS. Attach this policy to your users or roles whose credentials you provide when installing the AWS VCenter Client.

Permissions details

This policy includes the following permissions.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "mgn:CreateVcenterClientForMgn",
        "mgn:DescribeVcenterClients"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mgn:GetVcenterClientCommandsForMgn",
        "mgn:SendVcenterClientCommandResultForMgn",
        "mgn:SendVcenterClientLogsForMgn",

```



```

        "mgn:SendVcenterClientMetricsForMgn",
        "mgn>DeleteVcenterClient",
        "mgn:TagResource",
        "mgn:NotifyVcenterClientStartedForMgn"
    ],
    "Resource": "arn:aws:mgn:*:*:vcenter-client/*"
}
]
}

```

AWS managed policy: AWSApplicationMigrationAgentInstallationPolicy

This policy allows installing the AWS Replication Agent, which is used with AWS Application Migration Service to migrate source servers to AWS. Attach this policy to your users or roles whose credentials you provide during the installation step of the AWS Replication Agent. The installed AWS Replication Agent will communicate with AWS Application Migration Service using the recommended strong authentication method.

Permissions details

This policy includes the following permissions.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mgn:GetAgentInstallationAssetsForMgn",
        "mgn:SendClientMetricsForMgn",
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:VerifyClientRoleForMgn"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "mgn:IssueClientCertificateForMgn",
      "Resource": "arn:aws:mgn:*:*:source-server/*",
      "Effect": "Allow"
    }
  ],
}

```

```

    {
      "Condition": {
        "StringEquals": {
          "mgn:CreateAction": "RegisterAgentForMgn"
        }
      },
      "Action": "mgn:TagResource",
      "Resource": "arn:aws:mgn:*:*:source-server/*",
      "Effect": "Allow"
    }
  ]
}

```

AWS managed policy: AWSApplicationMigrationAgentPolicy_v2

This policy allows using the AWS Replication Agent, which is used with AWS Application Migration Service to migrate source servers to AWS. We do not recommend that you attach this policy to your users or roles.

Permissions details

This policy includes the following permissions.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",
        "mgn:GetAgentCommandForMgn",
        "mgn:GetAgentConfirmedResumeInfoForMgn",
        "mgn:GetAgentRuntimeConfigurationForMgn",
        "mgn:UpdateAgentBacklogForMgn",
        "mgn:GetAgentReplicationInfoForMgn",
        "mgn:IssueClientCertificateForMgn"
      ],
      "Resource": "arn:aws:mgn:*:*:source-server/${aws:SourceIdentity}",
    }
  ]
}

```

```

        "Effect": "Allow"
      }
    ]
  }

```

AWS managed policy: AWSApplicationMigrationServiceEc2InstancePolicy

This policy allows installing and using the AWS Replication Agent, which is used by AWS Application Migration Service (AWS MGN) to migrate source servers that run on EC2 (cross-Region or cross-AZ). An IAM role with this policy should be attached (as an EC2 Instance Profile) to the EC2 Instances.

Permissions details

This policy includes the following permissions.

- `mgn` – Allows to install and use the AWS Replication Agent

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "MgnAgentInstallation",
      "Effect": "Allow",
      "Action": [
        "mgn:SendClientLogsForMgn",
        "mgn:RegisterAgentForMgn",
        "mgn:GetAgentInstallationAssetsForMgn"
      ],
      "Resource": "*"
    },
    {
      "Sid": "MgnAgentReplication",
      "Effect": "Allow",
      "Action": [
        "mgn:SendAgentMetricsForMgn",
        "mgn:SendAgentLogsForMgn",
        "mgn:UpdateAgentSourcePropertiesForMgn",
        "mgn:UpdateAgentReplicationInfoForMgn",
        "mgn:UpdateAgentConversionInfoForMgn",

```

```

    "mgn:GetAgentCommandForMgn",
    "mgn:GetAgentConfirmedResumeInfoForMgn",
    "mgn:GetAgentRuntimeConfigurationForMgn",
    "mgn:UpdateAgentBacklogForMgn",
    "mgn:GetAgentReplicationInfoForMgn"
  ],
  "Resource": "arn:aws:mgn:*:*:source-server/*"
},
{
  "Sid": "MgnSourceServerTagResource",
  "Effect": "Allow",
  "Action": "mgn:TagResource",
  "Resource": "arn:aws:mgn:*:*:source-server/*",
  "Condition": {
    "StringEquals": {
      "mgn:CreateAction": "RegisterAgentForMgn"
    }
  }
}
]
}

```

AWS MGN updates for AWS managed policies

View details about updates to AWS managed policies for AWS Application Migration Service since March 1, 2021.

Change	Description	Date
AWSApplicationMigrationFullAccess – Updated policy	Updated the AWSApplicationMigrationFullAccess policy to support SecureString parameter type in SSM Parameters Store for post-migration framework actions.	March 10, 2024
AWSApplicationMigrationServiceEc2InstancePolicy – Updated policy	Created a new revision of the managed policy to support MGN in GovCloud and added	December 28, 2023

Change	Description	Date
	SID to statements in the managed policy	
AWSApplicationMigrationServiceEc2InstancePolicy – New policy	<p>This policy allows installing and using the AWS Replication Agent, which is used by AWS Application Migration Service (AWS MGN) to migrate source servers that run on EC2 (cross-Region or cross-AZ). An IAM role with this policy should be attached (as an EC2 Instance Profile) to the EC2 Instances.</p>	August 21, 2023
AWSApplicationMigrationServiceRolePolicy – Updated policy	<p>Updated the AWSApplicationMigrationServiceRolePolicy with Organizations permissions to support the global view feature.</p>	June 18, 2023
AWSApplicationMigrationFullAccess – Updated policy	<p>Updated the AWSApplicationMigrationFullAccess policy to support specific automation SSM documents.</p>	April 1, 2023

Change	Description	Date
<p>AWSApplicationMigrationFullAccess – Updated policy</p> <p>AWSApplicationMigrationSSMAccess – Updated policy</p> <p>AWSApplicationMigrationReadOnlyAccess – Created policy</p>	<p>Updated the AWSApplicationMigrationFullAccess policy to support both command and automation SSM documents for post-migration framework actions.</p> <p>Updated the AWSApplicationMigrationSSMAccess policy to support both command and automation SSM documents for the custom actions feature.</p> <p>Updated the AWSApplicationMigrationReadOnlyAccess policy to support the new import and export feature.</p>	<p>March 21, 2023</p>
<p>AWSApplicationMigrationEC2Access – Updated policy</p>	<p>Updated the AWSApplicationMigrationEC2Access policy to support: DescribeSnapshots, DescribeImages, DescribeVolumes.</p>	<p>January 29, 2023</p>

Change	Description	Date
<p>AWSApplicationMigrationEC2Access – Updated policy</p> <p>AWSApplicationMigrationReadOnlyAccess – Updated policy</p> <p>AWSApplicationMigrationSSMAccess – Created policy</p>	<p>Updated the AWSApplicationMigrationEC2Access policy to support: CreateLaunchTemplate, DeleteLaunchTemplate.</p> <p>Updated the AWSApplicationMigrationReadOnlyAccess policy to support: DescribeLaunchConfigurationTemplates, ListSourceServerActions, ListTemplateActions, ListApplications, ListWaves.</p> <p>Created new AWSApplicationMigrationSSMAccess policy to support new custom actions feature.</p>	November 28, 2022
<p>AWSApplicationMigrationAgentPolicy – Updated policy</p> <p>AWSApplicationMigrationAgentInstallationPolicy – Updated policy</p>	<p>Updated the AWSApplicationMigrationAgentPolicy policy and the AWSApplicationMigrationAgentInstallationPolicy policy to support sending additional metrics during the agent installation process.</p>	September 20, 2022

Change	Description	Date
AWSApplicationMigrationAgentInstallationPolicy – New policy	<p>AWS MGN added a new policy. This policy allows installing the AWS Replication Agent, which is used with Application Migration Service to migrate source servers to AWS. Attach this policy to your users or roles whose credentials you provide during the installation step of the AWS Replication Agent. The installed AWS Replication Agent will communicate with Application Migration Service using the recommended strong authentication method.</p>	<p>June 15, 2022</p>
AWSApplicationMigrationFullAccess – Updated policy	<p>Updated the AWSApplicationMigrationFullAccess policy to support the Post Migration Framework.</p>	<p>May 16, 2022</p>
AWSApplicationMigrationAgentPolicy_v2 – New policy	<p>AWS Application Migration Service added a new policy. This policy allows using the AWS Replication Agent, which is used with AWS Application Migration Service to migrate source servers to AWS. We do not recommend that you attach this policy to your users or roles.</p>	<p>May 10, 2022</p>

Change	Description	Date
AWSApplicationMigrationReadOnlyAccess – Updated policy	Updated the AWSApplicationMigrationReadOnlyAccess policy to include service quotas.	April 3, 2022
AWSApplicationMigrationEC2Access – Updated policy	<p>Updated the AWSApplicationMigrationEC2Access policy to add additional permissions and restrict certain existing permissions. This policy is only intended to be used for the AWS MGN console.</p> <p>The restriction prevents certain requests from being called directly by the calling identity, whilst enabling an AWS Application Migration Service (AWS MGN) to make the request to EC2 on behalf of the calling identity.</p>	March 2, 2022
AWSApplicationMigrationServiceRolePolicy – Updated policy	AWS Application Migration Service added a new policy to allow AWS Application Migration Service to manage AWS resources on your behalf.	December 15, 2021
AWSApplicationMigrationVCenterClientPolicy – New policy	AWS Application Migration Service added a new policy that allows the installation and usage of the AWS vCenter Appliance.	November 7, 2021

Change	Description	Date
AWSApplicationMigrationAgentPolicy – New policy	AWS Application Migration Service added a new policy to allow the installation of the AWS Replication Agent on source servers.	April 18, 2021
AWSApplicationMigrationConversionServerPolicy – New policy	AWS Application Migration Service added a new policy that allows AWS Application Migration Service to communicate with the service.	April 18, 2021
AWSApplicationMigrationMGHAccess – New policy	AWS Application Migration Service added a new policy to allow AWS Application Migration Service access to your account's AWS Migration Hub	April 18, 2021
AWSApplicationMigrationReplicationServerPolicy – New policy	AWS Application Migration Service added a new policy to allow the AWS Application Migration Service replication servers to communicate with the service, create and manage resources on your behalf.	April 7, 2021
AWS MGN started tracking changes	AWS Application Migration Service started tracking changes for AWS managed policies.	April 7, 2021

Managing access using policies

You control access in AWS by creating policies and attaching them to AWS identities or resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. AWS evaluates these policies when a principal (user, root user, or role session) makes a request. Permissions in the policies determine whether the request is allowed or denied. Most policies are stored in AWS as JSON documents. For more information about the structure and contents of JSON policy documents, see [Overview of JSON policies](#) in the *IAM User Guide*.

Administrators can use AWS JSON policies to specify who has access to what. That is, which **principal** can perform **actions** on what **resources**, and under what **conditions**.

By default, users and roles have no permissions. To grant users permission to perform actions on the resources that they need, an IAM administrator can create IAM policies. The administrator can then add the IAM policies to roles, and users can assume the roles.

IAM policies define permissions for an action regardless of the method that you use to perform the operation. For example, suppose that you have a policy that allows the `iam:GetRole` action. A user with that policy can get role information from the AWS Management Console, the AWS CLI, or the AWS API.

Identity-based policies

Identity-based policies are JSON permissions policy documents that you can attach to an identity, such as a user, role, or group. These policies control what actions that identity can perform, on which resources, and under what conditions. To learn how to create an identity-based policy, see [Creating IAM Policies](#) in the IAM User Guide.

Identity-based policies can be further categorized as inline policies or managed policies. Inline policies are embedded directly into a single user, group, or role. Managed policies are standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies include AWS managed policies and customer managed policies. To learn how to choose between a managed policy or an inline policy, see [Choosing Between Managed Policies and Inline Policies](#) in the IAM User Guide.

Using identity-based policies

By default, users and roles don't have permission to create or modify AWS Application Migration Service resources. They also can't perform tasks using the AWS Management Console, AWS CLI, or AWS API. An IAM administrator must create IAM policies that grant users and roles permission to

perform specific API operations on the specified resources they need. The administrator must then attach those policies to the users or groups that require those permissions. To understand how to attach policies to a user or group, learn about [adding and removing IAM identity permissions](#). To learn how to create an IAM identity-based policy using example JSON policy documents, see [Creating policies on the JSON tab in the IAM User Guide](#).

Topics

- [Customer-managed policies in AWS MGN](#)
- [Full Access](#)
- [Read-Only Policy](#)
- [Restrict permission to act on a source server associated with given AWS vCenter client](#)

Customer-managed policies in AWS MGN

You can create your own custom IAM policies to allow permissions for AWS Application Migration Service actions and resources. You can attach these custom policies to the users, roles, or groups that require those permissions. You can also create your own custom IAM policies for integration between AWS Application Migration Service and other AWS services. The next few topics provide example of the IAM policies which grants permission for various AWS Application Migration Service actions. Use them to limit AWS Application Migration Service access for your users and roles.

Full Access

The following policy This policy provides permissions to all public APIs of AWS Application Migration Service (AWS MGN), as well as permissions to read KMS key, License Manager, Resource Groups, Elastic Load Balancing, IAM, and EC2 information. This policy should be granted to an administrator or a power-user.

If you wish to grant a user the Full Access policy, attach the following policy managed policy to the user:

`AWSApplicationMigrationFullAccess`

Important

You must attach the [AWSApplicationMigrationFullAccess](#) and the [AWSApplicationMigrationEC2Access](#) policies to your users and roles in order to be able to launch test and cutover instances and to complete a full migration cycle with AWS MGN.

Read-Only Policy

The Read-Only policy allows a user to read from AWS Application Migration Service and Amazon EC2 resources, but does not allow them to perform any actions, such as initialize the service, replicate servers, or launch servers in AWS. This policy can be granted to a user in a support role.

If you wish to grant a user the Read-Only policy, attach the following policy managed policy to the user:

AWSApplicationMigrationReadOnlyAccess

Restrict permission to act on a source server associated with given AWS vCenter client

To restrict access to source servers associated with a given AWS vCenter client, use the condition element `mgn:VcenterClientId` condition key. The following example demonstrates a policy that allows an AWS vCenter client to call the `mgn:UpdateAgentSourcePropertiesForMgn` action only on a source server associated with the calling AWS vCenter client.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "mgn:UpdateAgentSourcePropertiesForMgn",
      "Resource": "arn:aws:mgn:*:*:source-server/*",
      "Condition": {
        "StringEquals": {
          "mgn:VcenterClientId": "${aws:SourceIdentity}"
        }
      }
    }
  ]
}
```

Resource-based policies

Resource-based policies are JSON policy documents that you attach to a resource. Examples of resource-based policies are IAM *role trust policies* and Amazon S3 *bucket policies*. In services that support resource-based policies, service administrators can use them to control access to a specific resource. For the resource where the policy is attached, the policy defines what actions a specified

principal can perform on that resource and under what conditions. You must [specify a principal](#) in a resource-based policy. Principals can include accounts, users, roles, federated users, or AWS services.

Resource-based policies are inline policies that are located in that service. You can't use AWS managed policies from IAM in a resource-based policy.

Access control lists (ACLs)

Access control lists (ACLs) control which principals (account members, users, or roles) have permissions to access a resource. ACLs are similar to resource-based policies, although they do not use the JSON policy document format.

Amazon S3, AWS WAF, and Amazon VPC are examples of services that support ACLs. To learn more about ACLs, see [Access control list \(ACL\) overview](#) in the *Amazon Simple Storage Service Developer Guide*.

Other policy types

AWS supports additional, less-common policy types. These policy types can set the maximum permissions granted to you by the more common policy types.

- **Permissions boundaries** – A permissions boundary is an advanced feature in which you set the maximum permissions that an identity-based policy can grant to an IAM entity (IAM user or role). You can set a permissions boundary for an entity. The resulting permissions are the intersection of an entity's identity-based policies and its permissions boundaries. Resource-based policies that specify the user or role in the `Principal` field are not limited by the permissions boundary. An explicit deny in any of these policies overrides the allow. For more information about permissions boundaries, see [Permissions boundaries for IAM entities](#) in the *IAM User Guide*.
- **Service control policies (SCPs)** – SCPs are JSON policies that specify the maximum permissions for an organization or organizational unit (OU) in AWS Organizations. AWS Organizations is a service for grouping and centrally managing multiple AWS accounts that your business owns. If you enable all features in an organization, then you can apply service control policies (SCPs) to any or all of your accounts. The SCP limits permissions for entities in member accounts, including each AWS account root user. For more information about Organizations and SCPs, see [How SCPs work](#) in the *AWS Organizations User Guide*.
- **Session policies** – Session policies are advanced policies that you pass as a parameter when you programmatically create a temporary session for a role or federated user. The resulting session's permissions are the intersection of the user or role's identity-based policies and the session

policies. Permissions can also come from a resource-based policy. An explicit deny in any of these policies overrides the allow. For more information, see [Session policies](#) in the *IAM User Guide*.

Multiple policy types

When multiple types of policies apply to a request, the resulting permissions are more complicated to understand. To learn how AWS determines whether to allow a request when multiple policy types are involved, see [Policy evaluation logic](#) in the *IAM User Guide*.

Using service-linked roles for AWS Application Migration Service

AWS Application Migration Service uses AWS Identity and Access Management (IAM) [service-linked roles](#). A service-linked role is a unique type of IAM role that is linked directly to AWS Application Migration Service. Service-linked roles are predefined by AWS Application Migration Service and include all the permissions that the service requires to call other AWS services on your behalf.

A service-linked role makes setting up AWS Application Migration Service easier because you don't have to manually add the necessary permissions. AWS Application Migration Service defines the permissions of its service-linked roles, and unless defined otherwise, only AWS Application Migration Service can assume its roles. The defined permissions include the trust policy and the permissions policy, and that permissions policy cannot be attached to any other IAM entity.

You can delete a service-linked role only after first deleting their related resources. This protects your AWS Application Migration Service resources because you can't inadvertently remove permission to access the resources.

For information about other services that support service-linked roles, see [AWS Services That Work with IAM](#) and look for the services that have **Yes** in the **Service-Linked Role** column. Choose a **Yes** with a link to view the service-linked role documentation for that service.

Service-linked role permissions for AWS Application Migration Service

AWS Application Migration Service uses the service-linked role named **AWSServiceRoleForApplicationMigrationService**. This is a managed IAM policy with scoped permissions that AWS Application Migration Service needs to run in your account.

The **AWSServiceRoleForApplicationMigrationService** service-linked role trusts the following services to assume the role:

- `mgn.amazonaws.com`

The role permissions policy allows AWS Application Migration Service to complete the following actions on the specified resources.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "mgn:ListTagsForResource",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "kms:ListRetirableGrants",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "mgh:AssociateCreatedArtifact",
        "mgh:CreateProgressUpdateStream",
        "mgh:DisassociateCreatedArtifact",
        "mgh:GetHomeRegion",
        "mgh:ImportMigrationTask",
        "mgh:NotifyMigrationTaskState",
        "mgh:PutResourceAttributes"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeAccountAttributes",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSnapshots",

```



```

        "ec2:DescribeSubnets",
        "ec2:DescribeVolumes",
        "ec2:GetEbsDefaultKmsKeyId",
        "ec2:GetEbsEncryptionByDefault"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeAccount"
    ],
    "Resource": "arn:aws:organizations::*:account/*"
},
{
    "Effect": "Allow",
    "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAccounts"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:RegisterImage",
        "ec2:DeregisterImage"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2>DeleteSnapshot"
    ],
    "Resource": "arn:aws:ec2::*:snapshot/*",
    "Condition": {
        "Null": {
            "aws:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
        }
    }
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateLaunchTemplateVersion",
        "ec2:ModifyLaunchTemplate",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteLaunchTemplateVersions"
      ],
      "Resource": "arn:aws:ec2:*:*:launch-template/*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2>DeleteVolume"
      ],
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "Null": {
          "aws:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:GetConsoleOutput",
        "ec2:GetConsoleScreenshot"
      ],
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Condition": {
        "Null": {

```

```

                "aws:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/
AWSApplicationMigrationServiceManaged": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateSecurityGroup"
            ],
            "Resource": "arn:aws:ec2:*:*:security-group/*",
            "Condition": {
                "Null": {
                    "aws:RequestTag/
AWSApplicationMigrationServiceManaged": "false"
                }
            }
        }
    ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSecurityGroup"
      ],
      "Resource": "arn:aws:ec2:*:*:vpc/*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateLaunchTemplate"
      ],
      "Resource": "arn:aws:ec2:*:*:launch-template/*",
      "Condition": {
        "Null": {
          "aws:RequestTag/
AWSApplicationMigrationServiceManaged": "false"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot"
      ],
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Condition": {
        "Null": {
          "ec2:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateSnapshot"
      ],
      "Resource": "arn:aws:ec2:*:*:snapshot/*",
      "Condition": {
        "Null": {

```

```

                "aws:RequestTag/
AWSApplicationMigrationServiceManaged": "false"
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DetachVolume",
                "ec2:AttachVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:instance/*",
            "Condition": {
                "Null": {
                    "ec2:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*",
            "Condition": {
                "Null": {
                    "ec2:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DetachVolume"
            ],
            "Resource": "arn:aws:ec2:*:*:volume/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RunInstances"
            ],

```

```

        "Resource": "arn:aws:ec2:*:*:instance/*",
        "Condition": {
            "Null": {
                "aws:RequestTag/
AWSApplicationMigrationServiceManaged": "false"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:RunInstances"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:security-group/*",
            "arn:aws:ec2:*:*:volume/*",
            "arn:aws:ec2:*:*:subnet/*",
            "arn:aws:ec2:*:*:image/*",
            "arn:aws:ec2:*:*:network-interface/*",
            "arn:aws:ec2:*:*:launch-template/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": [
            "arn:aws:iam:*:*:role/service-role/
AWSApplicationMigrationReplicationServerRole",
            "arn:aws:iam:*:*:role/service-role/
AWSApplicationMigrationConversionServerRole"
        ],
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "ec2.amazonaws.com"
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": "ec2:CreateTags",
        "Resource": [
            "arn:aws:ec2:*:*:launch-template/*",
            "arn:aws:ec2:*:*:security-group/*",
            "arn:aws:ec2:*:*:volume/*",

```

```

        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
        "StringEquals": {
            "ec2:CreateAction": [
                "CreateLaunchTemplate",
                "CreateSecurityGroup",
                "CreateVolume",
                "CreateSnapshot",
                "RunInstances"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:CreateTags",
        "ec2:ModifyVolume"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:volume/*"
    ],
    "Condition": {
        "Null": {
            "ec2:ResourceTag/
AWSApplicationMigrationServiceManaged": "false"
        }
    }
}
]
}

```

You must configure permissions to allow an IAM entity (such as a user, group, or role) to create, edit, or delete a service-linked role. For more information, see [Service-Linked Role Permissions](#) in the *IAM User Guide*.

Creating a service-linked role for AWS Application Migration Service

You don't need to manually create a service-linked role. When you configure the Replication Configuration Template for AWS Application Migration Service, a service-linked role is

automatically created. MGN automatically creates the IAM service-linked role, which you can see in the IAM console. You don't need to manually create or configure this role.

If you delete this service-linked role, and then need to create it again, you can use the same process to recreate the role in your account. When you create the first new replication configuration template in MGN, it creates the service-linked role for you again.

In the AWS CLI or the AWS API, create a service-linked role with the AWS Application Migration Service name. For more information, see [Creating a Service-Linked Role](#) in the *IAM User Guide*. If you delete this service-linked role, you can use this same process to create the role again.

Editing a service-linked role for AWS Application Migration Service

AWS Application Migration Service does not allow you to edit the `AWSServiceRoleForApplicationMigrationService` service-linked role. After you create a service-linked role, you cannot change the name of the role because various entities might reference the role. However, you can edit the description of the role using IAM. For more information, see [Editing a Service-Linked Role](#) in the *IAM User Guide*.

Deleting a service-linked role for AWS Application Migration Service

If you no longer need to use a feature or service that requires a service-linked role, we recommend that you delete that role. That way you don't have an unused entity that is not actively monitored or maintained. However, you must clean up the resources for your service-linked role before you can manually delete it.

Note

If AWS Application Migration Service is using the role when you try to delete the resources, the deletion might fail. If that happens, wait for a few minutes and try the operation again.

To clean up AWS Application Migration Service resources used by `AWSServiceRoleForApplicationMigrationService`

1. Identify and delete any waves and applications in all AWS Regions
 - a. identify any waves:

```
aws mgn list-waves
```


b. Delete any waves:

```
aws mgn delete-wave --wave-id {WaveID}
```

c. Identify any application:

```
aws mgn list-applications
```

d. Delete any application:

```
aws mgn delete-application --application-id {ApplicationID}
```

2. Identify and delete any source servers in all AWS Regions**a. Identify any active source servers:**

```
aws mgn describe-source-servers --filters isArchived=False --query  
"items[*].sourceServerID"
```

b. Disconnect any archived source server:

```
aws mgn disconnect-from-service --source-server-id {SourceServerID}
```

c. Archive any disconnected source servers:

```
aws mgn mark-as-archived --source-server-id {SourceServerID}
```

d. Delete any archived source server:

```
aws mgn delete-source-server --source-server-id {SourceServerID}
```

3. Identify and delete any AWS MGN jobs in all AWS Regions**a. Identify any AWS MGN jobs**

```
aws mgn describe-jobs
```

b. Delete any AWS MGN jobs:

```
aws mgn delete-job --job-id {MGNJobId}
```

4. Identify and delete any AWS MGN replication templates

a. Identify any AWS MGN replication template:

```
aws mgn describe-replication-configuration-templates
```

b. Remove any AWS MGN replication templates:

```
aws mgn delete-replication-configuration-template --replication-configuration-  
template-id {rct-TemplateID}
```

Resources can be cleaned up without stopping any service provided by AWS Application Migration Service. Cleaning up AWS Application Migration Service resources will cause AWS Application Migration Service to stop working. For more information, see [Cleaning up a Service-Linked Role](#) in the *IAM User Guide*.

To manually delete the service-linked role using IAM

Use the IAM console, the AWS CLI, or the AWS API to delete the `AWSServiceRoleForApplicationMigrationService` service-linked role. For more information, see [Deleting a Service-Linked Role](#) in the *IAM User Guide*.

Supported Regions for AWS MGN service-linked roles

AWS Application Migration Service supports using service-linked roles in all of the [AWS Regions where the service is available](#).

Policy structure

An IAM policy is a JSON document that consists of one or more statements. Each statement is structured as follows.

```
{  
  "Statement": [  
    {  
      "Effect": "effect",  
      "Action": "action",  
      "Resource": "arn",  
      "Condition": {  
        "condition": {  
          "key": "value"
```

```
}
    ]
  }
}
```

There are various elements that make up a statement:

- **Effect:** The effect can be `Allow` or `Deny`. By default, IAM users don't have permission to use resources and API actions, so all requests are denied. An explicit allow overrides the default. An explicit deny overrides any allows.
- **Action:** The action is the specific AWS Application Migration Service API action for which you are granting or denying permission.
- **Resource:** The resource that's affected by the action. For AWS Application Migration Service, you must specify "*" as the resource.
- **Condition:** Conditions are optional. They can be used to control when your policy is in effect.

Resilience in AWS Application Migration Service

The AWS global infrastructure is built around AWS Regions and Availability Zones. Regions provide multiple physically separated and isolated Availability Zones, which are connected through low-latency, high-throughput, and highly redundant networking. With Availability Zones, you can design and operate applications and databases that automatically fail over between zones without interruption. Availability Zones are more highly available, fault tolerant, and scalable than traditional single or multiple data center infrastructures.

For more information about AWS Regions and Availability Zones, see [AWS Global Infrastructure](#).

Infrastructure security in AWS Application Migration Service

As a managed service, AWS Application Migration Service is protected by the AWS global network security procedures that are described in the [Amazon Web Services: Overview of Security Processes](#) whitepaper.

You use AWS published API calls to access AWS Application Migration Service through the network. Clients must support Transport Layer Security (TLS) 1.2 or later. Clients must also support cipher

suites with perfect forward secrecy (PFS) such as Ephemeral Diffie-Hellman (DHE) or Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). Most modern systems such as Java 7 and later support these modes.

All parties involved in the communication authenticate each other using TLS, IAM policies and tokens. The communication between the Agents and the replication server are based on TLS 1.2 only with the highest standard of cipher suite (PFS, ECDHE. Requests between the agent and AWS Application Migration Service as well as between the replication server and Application Migration Service are signed using an access key ID and a secret access key that is associated with an IAM principal).

All requests must be signed using the [AWS Security Token Service](#) (AWS STS), which allows you to generate temporary security credentials to sign requests. Alternatively, use credentials that associated with an IAM principal.

AWS Application Migration Service customers must ensure that they manually delete their access keys after installing the AWS Replication Agent and successful migration. AWS does not delete these keys automatically. AWS Application Migration Service does delete the keys from source servers after they are disconnected from the service. If you want your keys to automatically stop working at a certain date after you have finished using them so that you do not have to worry about manually deleting them, you can do so through the [IAM permissions boundary](#) and the [aws:CurrentTime global context key](#).

AWS Application Migration Service customers should use [Amazon EBS encryption](#).

AWS Application Migration Service customers should secure their replication servers by reducing their exposure to the public internet. This can be done through:

1. Using security groups to only allow permitted IP addresses to connect to the replication servers. [Learn more about Security Groups](#).
2. Using a VPN to connect to the replication servers, such as the AWS site-to-site VPN. [Learn more about the AWS Site-to-site VPN](#).

AWS Application Migration Service creates and uses the "aws-replication" user within the Linux Source server. The AWS Application Migration Service replication server and AWS Replication Agent run under this user. Although this is not a root user, this user needs to be part of the disk group that grants this user full read and write permissions to block devices.

Note

AWS Application Migration Service only uses these permissions to read from block devices.

Compliance validation for AWS Application Migration Service

Third-party auditors assess the security and compliance of AWS Application Migration Service as part of multiple AWS compliance programs.

For a list of AWS services in scope of specific compliance programs, see [AWS Services in Scope by Compliance Program](#) . For general information, see [AWS Compliance Programs](#) .

You can download third-party audit reports using AWS Artifact. For more information, see [Downloading Reports in AWS Artifact](#) .

Your compliance responsibility when using AWS Application Migration Service is determined by the sensitivity of your data, your company's compliance objectives, and applicable laws and regulations. AWS provides the following resources to help with compliance:

- [Security and Compliance Quick Start Guides](#) – These deployment guides discuss architectural considerations and provide steps for deploying security- and compliance-focused baseline environments on AWS.
- [Architecting for HIPAA Security and Compliance Whitepaper](#) – This whitepaper describes how companies can use AWS to create HIPAA-compliant applications.
- [AWS Compliance Resources](#) – This collection of workbooks and guides might apply to your industry and location.
- [Evaluating Resources with Rules](#) in the *AWS Config Developer Guide* – AWS Config; assesses how well your resource configurations comply with internal practices, industry guidelines, and regulations.
- [AWS Security Hub](#) – This AWS service provides a comprehensive view of your security state within AWS that helps you check your compliance with security industry standards and best practices.

Cross-service confused deputy prevention

The confused deputy problem is a security issue where an entity that doesn't have permission to perform an action can coerce a more-privileged entity to perform the action. In AWS, cross-service

impersonation can result in the confused deputy problem. Cross-service impersonation can occur when one service (the *calling service*) calls another service (the *called service*). The calling service can be manipulated to use its permissions to act on another customer's resources in a way it should not otherwise have permission to access. To prevent this, AWS provides tools that help you protect your data for all services with service principals that have been given access to resources in your account.

We recommend using the [aws:SourceArn](#) and [aws:SourceAccount](#) global condition context keys in resource policies to limit the permissions that AWS Application Migration Service gives another service to the resource. If you use both global condition context keys, the `aws:SourceAccount` value and the account in the `aws:SourceArn` value must use the same account ID when used in the same policy statement.

The value of `aws:SourceArn` must be `"arn:aws:mgn:*:123456789012:source-server/*"`

The most effective way to protect against the confused deputy problem is to use the `aws:SourceArn` global condition context key with the full ARN of the resource. If you don't know the full ARN of the resource or if you are specifying multiple resources, use the `aws:SourceArn` global context condition key with wildcards (*) for the unknown portions of the ARN. For example, `arn:aws:servicename:123456789012:*` .

The following example shows how you can use the `aws:SourceArn` and `aws:SourceAccount` global condition context keys in AWS Application Migration Service to prevent the confused deputy problem.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Sid": "ConfusedDeputyPreventionExamplePolicy",
    "Effect": "Allow",
    "Principal": {
      "Service": "mgn.amazonaws.com"
    },
    "Action": "sts:AssumeRole",
    "Condition": {
      "StringLike": {
        "aws:SourceArn": "arn:aws:mgn:*:123456789012:source-
server/*",
        "aws:SourceAccount": "123456789012"
      }
    }
  }
}
```

```
}  
}
```

Troubleshooting

Topics

- [Troubleshooting launch errors](#)
- [Troubleshooting communication errors](#)
- [Troubleshooting agent issues](#)
- [Troubleshooting agentless replication issues](#)
- [Common replication errors](#)
- [Other troubleshooting topics](#)

Troubleshooting launch errors

Topics

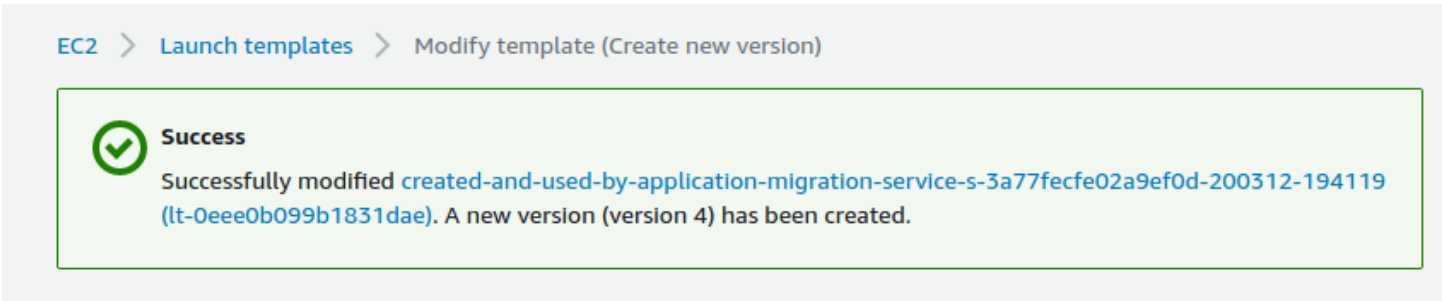
- [Do I need to recreate the entire launch template for every version?](#)
- [Error - AccessDeniedException - Must be admin user](#)
- [VPCIdNotSpecified error](#)
- [Error: Failed to connect using HTTP channel](#)
- [Could not take up-to-date snapshot. Launching from snapshot taken on...](#)

Do I need to recreate the entire launch template for every version?

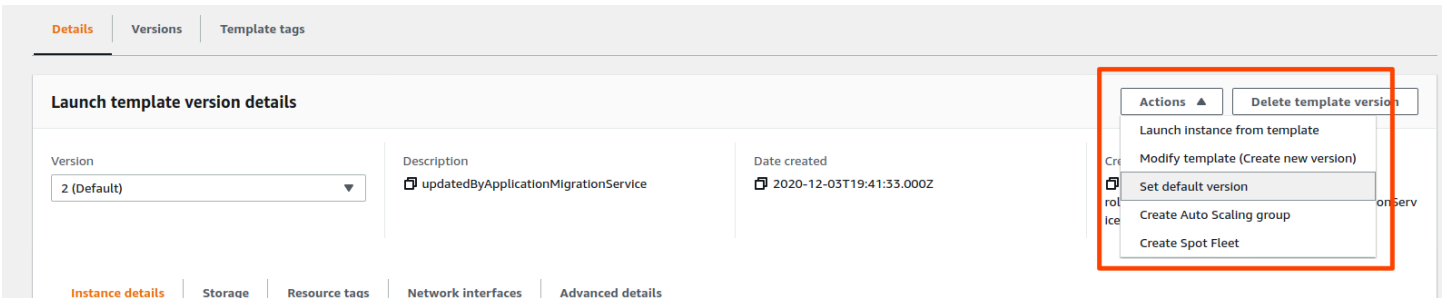
When you save a new template version, it is tagged as the latest version. However, for a multitude of reasons, AWS Application Migration Service (AWS MGN) uses the version marked as the default for its purposes. So in order to actually have AWS MGN recognize the changes you make, you need to go into the template itself, and change the default version to the version you have just updated.

Create the new template version. The window after creating the new template pops up a success box.

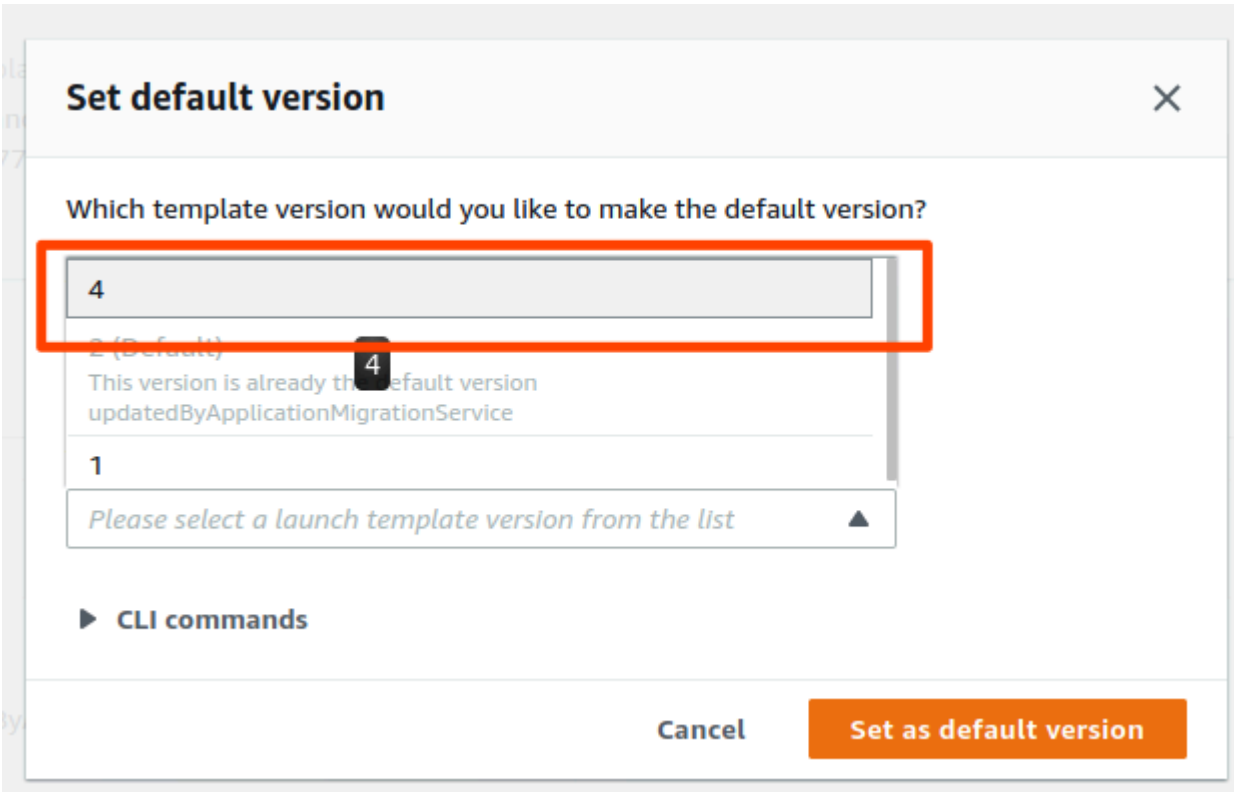
Click the launch template in the box, and then click **Actions** and choose **Set default version**.



Finally, from the drop down menu, select the latest version, and then click **Set as default version**.

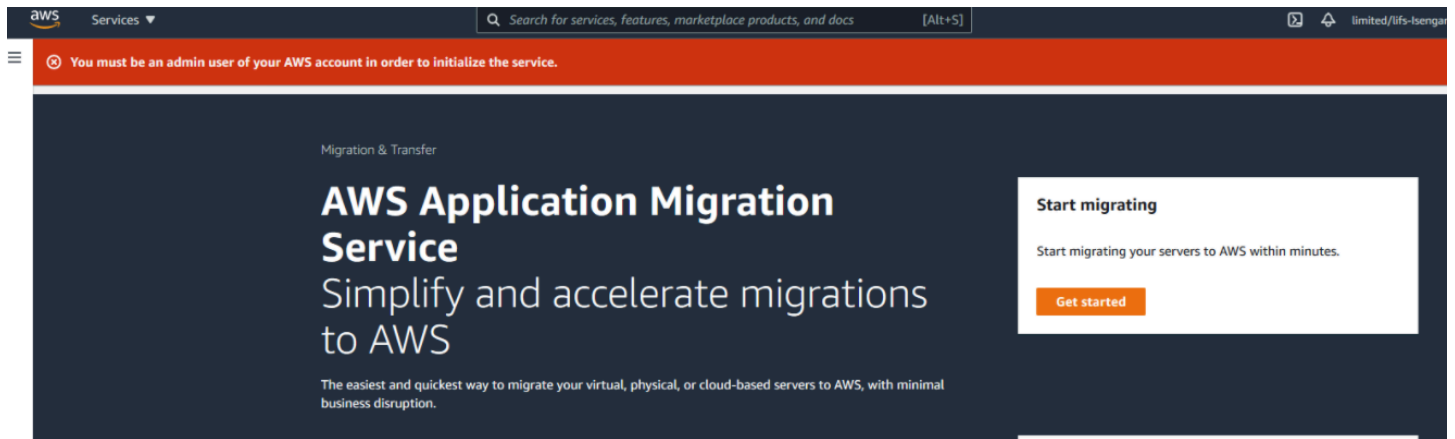


The AWS MGN console should refresh and reflect the changes after this.



Error - AccessDeniedException - Must be admin user

If you receive an AccessDeniedException error when attempting to log into AWS Application Migration Service (AWS MGN) for the first time and set up your replication settings template, it means that you are not the administrator of your AWS Account and therefore cannot initialize AWS MGN. You must be the Admin user of your AWS Account to initialize AWS MGN. [Learn more about initializing MGN.](#)



VPCIdNotSpecified error

The EC2 launch template does not automatically set a specific Subnet. As such, EC2 will attempt to launch in a Subnet within the default VPC. If you have removed your default VPC, EC2 will fail to launch any instance for which there is no valid Subnet specified. Ensure that you specify a subnet if that is the case, or AWS Application Migration Service instance launch will fail. You may see the VPCIdNotSpecified error if:

- A default subnet/VPC is not selected in the EC2 launch template.
- An incorrect target subnet is specified in the EC2 launch template.
- the EC2 launch template with the correct subnet settings is not set as the default.

Error: Failed to connect using HTTP channel

This error mostly occurs when the conversion server is unable to communicate with the necessary AWS Endpoints for [staging area communication](#).

- Check if any network changes were made in the staging area that could affect the conversion server reaching the AWS Endpoints (firewall settings, DNS settings, security group settings, route table settings, and access control list settings).

- Test TCP Port 443 connectivity with a test instance from the staging area subnet, to the [required endpoints](#).
- If the issue persists after confirming network connectivity please [create a case](#) with AWS Premium Support for further investigation.

Could not take up-to-date snapshot. Launching from snapshot taken on...

When a test or cutover instance is launched, AWS Application Migration Service (AWS MGN) will attempt to create the latest consistent snapshot of the source server. AWS MGN will wait for all the snapshots to become available and once they are ready, will proceed with the launch workflow.

If you see a timeout message when launching a test or cutover instance, it means the snapshot creation timed out. In this case, AWS MGN will use the latest successful snapshot for that source server to launch the instance. This ensures you can still launch an instance, but the instance will only contain data current up to the timestamp specified in the message.

To launch a test or cutover instance with the most up-to-date data, determine why the latest snapshot could not be created. Common causes include the source server not having a "Healthy" status, or backlog/lag.

Also check the CloudTrail Event History for errors on the CreateSnapshot and DescribeSnapshot API calls, which can prevent timely EBS snapshot creation. Resolving these underlying issues will allow successful creation of up-to-date snapshots for test and cutover instances.

Troubleshooting communication errors

Topics

- [Solving communication problems over TCP Port 443 between the staging area and the AWS Application Migration Service](#)
- [Authenticate with service errors](#)
- [Calculating the required bandwidth for TCP Port 1500](#)
- [Verifying communication over Port 1500](#)
- [Solving communication problems over Port 1500](#)

Solving communication problems over TCP Port 443 between the staging area and the AWS Application Migration Service

- **DHCP** – [Check the DHCP options set of the VPC of the staging area.](#)

Ensure that the IPv4 CIDR, the DHCP options set, the route table, and the network ACL are correct.

- **DNS** – Ensure that your security groups allow outbound DNS resolution over TCP Port 53, and outbound HTTPS connectivity over TCP Port 443.
- **Route Rules** – the route rules on the staging area subnet may be inaccurately set. The route rules should allow outbound traffic to the Internet.

To check and set the route rules on the staging area subnet:

1. Sign in to [AWS console](#), click **Services** and select **VPC** under **Networking & Content Delivery**.
2. On the **VPC Dashboard** toolbar, select the **Route Tables** option.
3. On **Route Tables** page, check the box of the route table of your staging area.
4. This will open the details for your Route Table. Navigate to the **Routes** tab.
5. Within the **Target** column of the **Routes** tab, find the route you are using for the outbound communication to the Internet (either **igw**- Internet Gateway, **vgw** - **VPN** or **i** - EC2 instance). Verify that the address space in the Destination column is allowing access to Amazon S3, Amazon EC2, and AWS MGN in the AWS Region.
6. If the address is not **0.0.0.0/0**, change it to **0.0.0.0/0**.

Click the **Edit** button.

7. Input **0.0.0.0/0** into the Destination field for the correct **Target**. Click **Save**.

Note: If you are using VPN, enter a specific IP address range in the **Destination** column.

- **Network ACL** – The network ACL on the staging area subnet may block the traffic. Verify that the ephemeral ports are open.

Authenticate with service errors

The replication server needs to be able to reach the AWS MGN endpoint and have the proper IAM permissions. This can fail for a number of reasons, including:

- The replication server is in a subnet without access to VPC endpoints for AWS MGN or the [public endpoints](#).
- In some use cases, when using a custom DNS server, DNS traffic shifts to TCP instead of UDP. The solution for this is to [update](#) the [Migration Service Security Group](#) to allow outbound TCP traffic on port 53.
- The Replication Server does not have the proper [IAM policy](#).

Calculating the required bandwidth for TCP Port 1500

The required bandwidth for transferring the replicated data over TCP Port 1500 should be based on the write speed of the participating source servers. The recommended bandwidth should be at least the sum of the average write speed of all replicated source servers.

Minimal bandwidth = the sum of the average write speeds of all Source servers

For example, suppose you are replicating two source servers. One has a write speed of 5 MBps (meaning 5 megabytes of data every second), while the other has 7 MBps. In this case, the recommended bandwidth should be at least 12 MBps.

Finding the write speed of your source servers

To calculate the required bandwidth for transferring replicated data over TCP Port 1500, you need to know the write speed of your source servers. Use the following tools to find the write speed of your source servers:

Linux

Use the `iostat` command-line utility, located in the `systat` package. The `iostat` utility monitors system input/output device loading and generates statistical reports.

The links below lead to third-party websites not affiliated with or endorsed by AWS. The content on these external sites has not been reviewed or verified by AWS.

The `iostat` utility is installed [with yum](#) (RHEL/CentOS), via [apt-get](#) (Ubuntu) and via [zypper](#) (SUSE.)

To use `iostat` for checking the write speed of a Source Server, enter the following:`iostat -x <interval>`

- `-x` - displays extended statistics.
- `<interval>` - the number of seconds `iostat` waits between each report. Each subsequent report covers the time since the previous report.

For example, to check the write speed of a machine every 3 seconds, enter the following command:

```
iostat -x 3
```

We recommend that you run the `iostat` utility for at least 24 hours, since the write speed to the disk changes during the day, and it will take 24 hours of runtime to identify the average running speed.

Windows

Install and use the DiskMon application. DiskMon logs and displays all hard disk activity on a Windows system.

[Installing DiskMon](#)

DiskMon read and write offsets are presented in terms of sectors (512 bytes). Events can be either timed for their duration (in microseconds), or stamped with the absolute time that they were initiated.

Verifying communication over Port 1500

If there is a connection problem from the Source server to the Replication Servers or the Staging Area, use the following methods to check the connection.

To verify the integrity of the connection from a Source server to the Staging Area over TCP Port 1500:

1. Launch a new Linux machine in the Staging Area subnet.
2. On the new Linux machine, run the following command to open a listener in the Staging Area subnet:

```
nc -l 1500
```

3. On the Source Server, run the following command to check connectivity:

```
telnet <new machine ip> 1500
```

Solving communication problems over Port 1500

To solve connectivity problems between Source server and the staging area, check the following:

- The Network ACL on the staging area subnet may deny the traffic.
- Route Rules on the staging area subnet may be inaccurately set.
- The firewall, both internal and external, in the Source Server/infrastructure may block communication.
- The **Use VPN...** checkbox in AWS Application Migration Service console may not be set correctly.

Enabling the network ACL

The Network ACL on the staging area subnet may block connectivity. By default, the network ACL allows connectivity. However, if the ACL setting was changed to deny traffic, you need to change it back.

To check and activate the network ACL on the staging area subnet:

1. Sign in to the AWS console, click **Services** and select **VPC** under **Networking & Content Delivery**.
2. On the **Resources** list, select the **Network ACL** option:
3. On **Network ACL** page, select the check box next to the Network ACL of your staging area.
4. On the details table of the selected **Network ACL**, select the **Inbound Rules** tab.
5. On the **Inbound Rules** tab, verify that the rule that determines the traffic to replication server subnet set to **Allow**.

Note: The target should allow traffic on TCP Port 1500 from the address space of the source environment. The Network ACL does not necessarily need to be open to all port ranges, as in the screenshot below.

6. If the rule is set to **Deny**, click **Edit**.
7. Click the dropdown under **Allow/Deny** and select **Allow**. Click **Save**.
8. You will also need to check the **Ephemeral Ports** on the **Outbound Rules** tab. Within the same **Network ACL**, navigate to the **Outbound Rules** tab.

9. You will need to ensure that you are allowing the correct **Ephemeral Port range** for your particular client. [Ephemeral Port range varies based on each client's operating system](#). Click the Edit button to edit your **Ephemeral Port's Port Range** category.
10. Edit the **Port Range** and click **Save**. You may have to create a new Rule by clicking the **Add another rule** button.

Setting route rules on the staging area subnet

To check and set the route rules on the staging area subnet in AWS:

1. Sign in to AWS console, click **Services** and select **VPC** under **Networking & Content Delivery**.
2. On the **VPC Dashboard** toolbar, select the **Route Tables** option.
3. On the **Route Tables** page, check the box of the Route Table of your staging network.
4. This will open the details for your Route Table. Navigate to the **Routes** tab.
5. Within the **Target** column of the **Routes** tab, find the route you are using for the inbound traffic from the **Source** on TCP Port 1500 (either **igw** - Internet Gateway, **vgw** - VPN or **i** – EC2 instance). Verify that the **Destination address** is **0.0.0.0/0**.

Note: The Rule may be specific to the address space of the source servers.

6. If the address is not 0.0.0.0/0, you will need change it to 0.0.0.0/0.

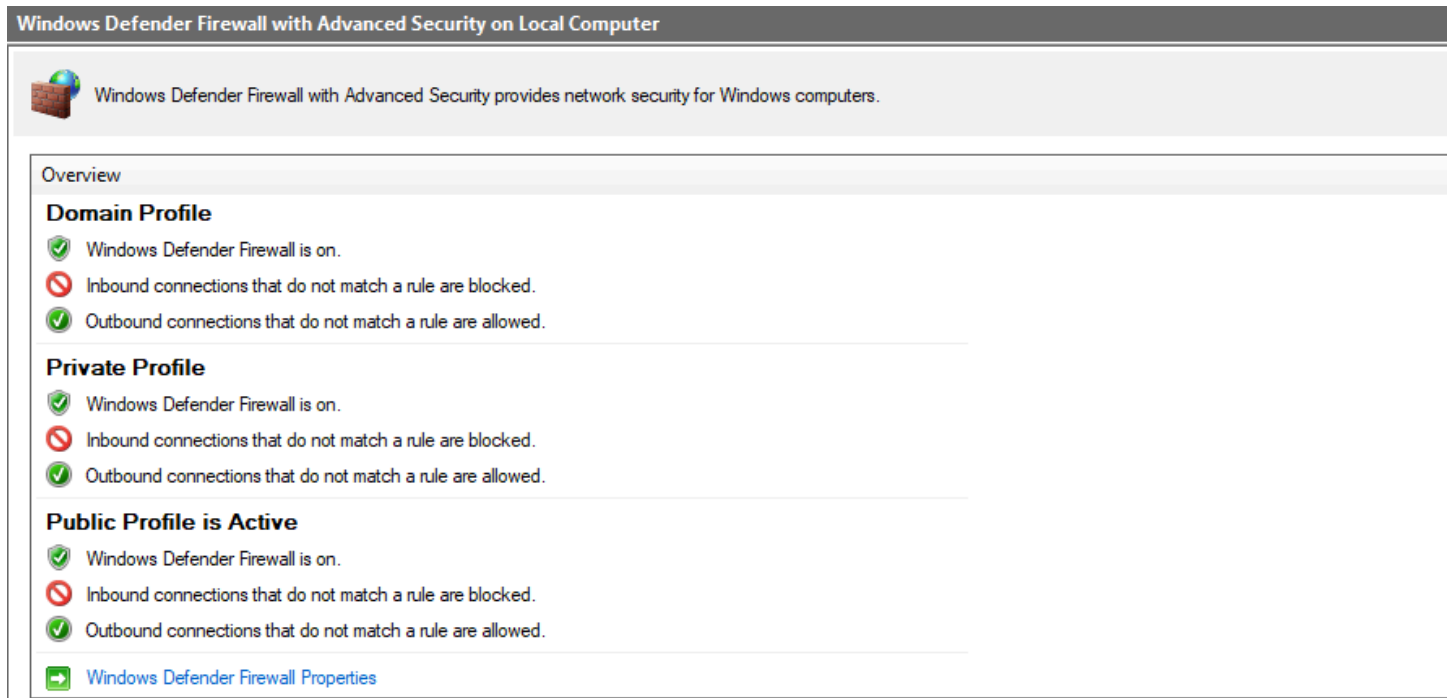
Note: The Rule may be specific to the address space of the Source Servers.

1. Click the Edit button.
2. Input **0.0.0.0/0** into the **Destination** field for the correct target. Click **Save**.

Note: If you are using VPN, enter a specific IP address range in the **Destination** column.

Firewall (both internal and external) in the source server/infrastructure.

Firewall issues may have several causes. Check the following if you experience any firewall issues, such as Windows Firewall connection issues:



- Ensure that the subnet you assigned for the replication servers still exists.

Troubleshooting agent issues

Topics

- [Error: Installation failed](#)
- [Where can I find the AWS MGN Agent logs?](#)

Error: Installation failed

When the installation of the AWS Replication Agent on a source server fails during the running of the Installer file, you will receive an error message.

This type of error means that the agent was not installed on the source server, and therefore the server will not appear on the AWS Application Migration Service console. After you fix the issue that caused the installation to fail, you need to rerun the Agent Installer file to install the agent.

This app cant run on your PC error - Windows

If you encounter the following error "This app can't run on your PC", when trying to install the AWS Replication Agent on your Windows 10 source Server, try the following.

This error is indicative that your particular version of Windows 10 is likely the 32-bit version. To verify this, you can

1. Use the Windows key + I keyboard shortcut to open the Settings app.
2. Click System.
3. Click About.
4. Under System type, you will see two pieces of information: if it says 32-bit operating system, x64-based processor, then it means that your PC is running a 32-bit version of Windows 10 on a 64-bit processor.

If it says 32-bit operating system, x86-based processor, then your computer doesn't support Windows 10 (64-bit).

If your OS is indeed 64-bit, then there may be other elements blocking the installation of your agent. The block is actually coming from the Windows Operating System itself. You would need to identify what the cause is. One of the way is running [sfc scan](#).

Is having a mounted '/tmp' directory a requirement for the agent?

The simple requirement is just to have enough free space. There is no need for this to be a separate mount. The need for the '/tmp' requirement is actually only if '/tmp' is a separate mount. If '/tmp' is not a separate mount, then it would fall under '/', for which we have the 2 GiB free requirement. This allows for the '/tmp' to fall into this requirement.

Installation failed - old agent

Installation may fail due to an old AWS Replication Agent. Ensure that you are attempting to install the latest version of the AWS Replication Agent. You can learn how to download the Agent [here](#).

Installation cannot be completed - CloudEndure Agent

Agent installation will fail if the source server already has the CloudEndure User Agent installed on it. You will need to [uninstall the CloudEndure Agent](#) and then install the AWS Replication Agent in order to proceed.

At times, uninstalling the CloudEndure Agent alone is not enough, as the Agent driver may remain. If that is the case, you will need to delete the agent driver manually.

Linux

Run the following command to identify the CloudEndure driver:

```
lsmod | grep CE_AgentDriver
```

Then, run the following command to delete the driver if it exists:

```
rmmod CE_AgentDriver
```

Windows

Run the following command in cmd to identify the CloudEndure driver:

```
sc query ce_driver
```

```
sc query ce_filter_driver
```

Then, run the following command to delete the driver if it exists:

```
sc delete ce_driver
```

```
sc delete ce_filter_driver
```

Installation failed on Linux Server

If the installation failed on a Linux Source server, check the following:

1. Free Disk Space

Free disk space on the root directory – verify that you have at least 3 GB of free disk on the root directory (/) of your Source Server. To check the available disk space on the root directory, run the following command: `df -h /`

Free disk space on the /tmp directory – for the duration of the installation process only, verify that you have at least 500 MB of free disk on the /tmp directory. To check the available disk space on the /tmp directory run the following command: `df -h /tmp`

After you have entered the above commands for checking the available disk space, the results will be displayed as follows:

```
ubuntu@Linux-1:~$ df -h /
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1      7.8G  1.4G  6.0G  19% /
ubuntu@Linux-1:~$ df -h /tmp
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1      7.8G  1.4G  6.0G  19% /tmp
```

2. The format of the list of disks to replicate

During the installation, when you are asked to enter the disks you want to replicate, do NOT use apostrophes, brackets, or disk paths that do not exist. Type only existing disk paths, and separate them with a comma, as follows:

```
/dev/xvda,/dev/xvdb.
```

3. Version of the Kernel headers package

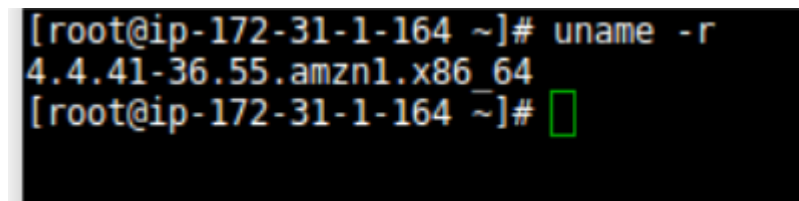
Verify that you have kernel-devel/linux-headers installed that are exactly of the same version as the kernel you are running.

The version number of the kernel headers should be completely identical to the version number of the kernel. To handle this issue, follow these steps:

a. Identify the version of your running kernel.

To identify the version of your running kernel, run the following command:

```
uname -r
```



```
[root@ip-172-31-1-164 ~]# uname -r
4.4.41-36.55.amzn1.x86_64
[root@ip-172-31-1-164 ~]#
```

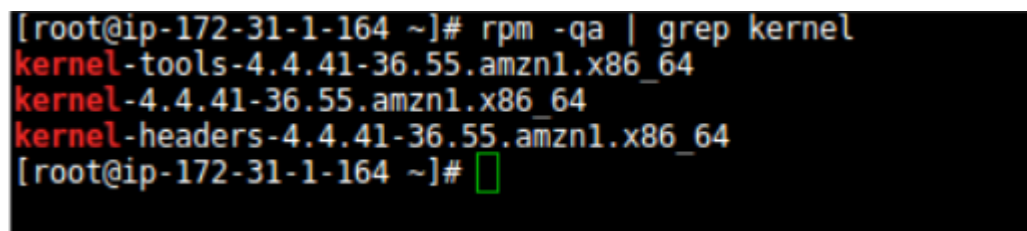
The 'uname -r' output version should match the version of one of the installed kernel headers packages (kernel-devel-<version number> / linux-headers-<version number>).

b. Identify the version of your kernel-devel/linux-headers.

To identify the version of your running kernel, run the following command:

On RHEL/CENTOS/Oracle/SUSE:

```
rpm -qa | grep kernel
```



```
[root@ip-172-31-1-164 ~]# rpm -qa | grep kernel
kernel-tools-4.4.41-36.55.amzn1.x86_64
kernel-4.4.41-36.55.amzn1.x86_64
kernel-headers-4.4.41-36.55.amzn1.x86_64
[root@ip-172-31-1-164 ~]#
```

Note: This command looks for kernel-level.

On Debian/Ubuntu: apt-cache search linux-headers

```
ubuntu@Linux-1:~$ apt-cache search linux-headers
linux-headers-3.13.0-24 - Header files related to Linux kernel version
3.13.0
linux-headers-3.13.0-24-generic - Linux kernel headers for version 3.1
3.0 on 64 bit x86 SMP
linux-headers-3.13.0-24-lowlatency - Linux kernel headers for version
3.13.0 on 64 bit x86 SMP
```

c. **Verifying that the folder that contains the kernel-devel/linux-headers is not a symbolic link.**

Sometimes, the content of the kernel-devel/linux-headers, which match the version of the kernel, is actually a symbolic link. In this case, you will need to remove the link before installing the required package.

To verify that the folder that contains the kernel-devel/linux-headers is not a symbolic link, run the following command:

On RHEL/CENTOS/Oracle/SUSE:

```
ls -l /usr/src/kernels
```

On Debian/Ubuntu:

```
ls -l /usr/src
```

```
ubuntu@Linux-1:~$ ls -l /usr/src
total 8
lrwxrwxrwx 1 root root 41 May 29 15:40 3.13.0-116-generic -> /usr/src/linux-
headers-3.13.0-116-generic
drwxr-xr-x 24 root root 4096 Apr 5 20:43 linux-headers-3.13.0-116
drwxr-xr-x 7 root root 4096 Apr 5 20:43 linux-headers-3.13.0-116-generic
ubuntu@Linux-1:~$
```

In the above example, the results show that the linux-headers are not a symbolic link.

d. **[If a symbolic link exists] Delete the symbolic link.**

If you found that the content of the kernel-devel/linux-headers, which match the version of the kernel, is actually a symbolic link, you need to delete the link. Run the following command:

```
rm /usr/src/<LINK NAME>
```

For example: `rm /usr/src/linux-headers-4.4.1`

e. **Install the correct kernel-devel/linux-headers from the repositories.**

If none of the already installed kernel-devel/linux-headers packages match your running kernel version, you need to install the matching package.

Note: You can have several kernel headers versions simultaneously on your OS, and you can therefore safely install new kernel headers packages in addition to your existing ones (without uninstalling the other versions of the package.) A new kernel headers package does not impact the kernel, and does not overwrite older versions of the kernel headers.

Note: For everything to work, you need to install a kernel headers package with the exact same version number of the running kernel.

To install the correct kernel-devel/linux-headers, run the following command:

On RHEL/CENTOS/Oracle/SUSE:

```
sudo yum install kernel-devel-`uname -r`
```

On Oracle with Unbreakable Enterprise Kernel:

```
sudo yum install kernel-uek-devel-`uname -r`
```

On Debian/Ubuntu:

```
sudo apt-get install linux-headers-`uname -r`
```

f. **[If no matching package was found] Download the matching kernel-devel/linux-headers package.**

If no matching package was found on the repositories configured on your machine, you can download it manually from the Internet and then install it.

To download the matching kernel-devel/linux-headers package, navigate to the following sites:

- [RHEL, CENTOS, Oracle, and SUSE package directory](#)
- [Debian package directory](#)
- [Ubuntu package directory](#)

4. The make, openssl, wget, curl, gcc and build-essential packages.

Note: Usually, the existence of these packages is not required for Agent installation. However, in some cases where the installation fails, installing these packages will solve the problem.

If the installation failed, the `make`, `openssl`, `wget`, `curl`, `gcc`, and `build-essential` packages should be installed and stored in your current path.

To verify the existence and location of the required packages, run the following command:

```
which <package>
```

For Example, to locate the `make` package:

```
which make
```

```
[root@ip-172-31-1-164 ~]# which make
/usr/bin/make
[root@ip-172-31-1-164 ~]#
```

5. Error: `urlopen error [Errno 10060] Connection times out.`

This error occurs when outbound traffic is not allowed over TCP Port 443. Port 443 needs to be open outbound to the AWS MGN Service endpoint.

6. Powerpath support

Contact AWS Support for instructions on how to install the AWS Application Migration Service Agent on such machines.

7. Error: You need to have root privileges to run this script.

Make sure you run the installer either as root or by adding `sudo` at the beginning:

```
sudo ./aws-replication-installer-init
```

Installation failed on Windows machine

If the installation failed on a Windows Source server, check the following:

1. .NET Framework

Verify that .NET Framework version 3.5 or above is installed on your Windows Source servers.

2. Free disk space

Verify that there is at least 1 GB of free disk space on the root directory (C:\) of your Source servers for the installation.

3. net.exe and sc.exe location

Verify that the net.exe and/or sc.exe files, located by default in the C:\Windows\System32 folder, are included in the **PATH Environment Variable**.

- a. Navigate to **Control Panel >System and Security >System >Advanced system settings**.
- b. On the **System Properties** dialog box **Advanced** tab, click the **Environment Variables** button.
- c. On the **System Variables** section of the **Environment Variables** pane, select the **Path** variable. Then, click the **Edit** button to view its contents.
- d. On the **Edit System Variable** pane, review the defined paths in the **Variable value** field. If the path of the net.exe and/or sc.exe files does not appear there, manually add it to the **Variable value** field, and click **OK**.

Windows - Installation Failed - Request Signature

If the AWS Replication Agent installation fails on Windows with the following error:

```
botocore.exceptions.ClientError: An error occurred (InvalidSignatureException) when calling the GetAgentInstallationAssetsForMgn operation: {"message":"The request signature we calculated does not match the signature you provided. Check your AWS Secret Access Key and signing method. Consult the service documentation for details."}
```

Attempt to rerun the installer with PowerShell instead of CMD. At times, when the installer is ran in CMD, the AWS Secret Key does not get pasted properly into the installer and causes installation to fail.

Error – certificate verify failed

This error (CERTIFICATE_VERIFY_FAILED) may indicate that the OS does not trust the certification authority used by our endpoints. To resolve this issue, try the following steps:

1. Open Microsoft Edge or Internet Explorer to update the operating system trusted root certificates. This will work if the operating system does not have restrictions to download the certificates.
2. If the first step does not resolve the issue, [download and install the Amazon Root Certificates manually](#).

Where can I find the AWS MGN Agent logs?

The AWS MGN Agent logs are stored in agent.log.0:

- **Linux:** /var/lib/aws-replication-agent/agent.log.0
- **Windows 64 bit:** C:\Program Files (x86)\AWS Replication Agent\agent.log.0
- **Windows 32 bit:** C:\Program Files\AWS Replication Agent\agent.log.0

In addition, you can review the installation log located in: <install_path>\aws_replication_agent_installer.log

Troubleshooting agentless replication issues

Discovery related troubleshooting

- No machines are discovered -

Verify vCenter client is still connected to the service and able to communicate with the required endpoints.

Verify vCenter user permissions, which you have configured the MGN Agentless client with, are correct by reviewing the [agentless snapshot based replication section](#).

- The same Machine is discovered twice -

Source Servers are identified by their vCenter UUID. If a server changes its UUID (which may happen in edge cases), the same guest can appear as two source servers, where only one of them is responsive (the new UUID). In this case, you may archive the previous source server, or use the API to delete it.

- Two machines with the same UUID -

Both replications are stalled, duplicate UUID reported to the service log. The workaround is to change the UUID of one of the machines. [Learn more about changing UUID](#)

Agentless Replication related troubleshooting

- Replication state is STALLED -

Verify vCenter client is still connected to the service and able to communicate with the required endpoints.

- dataReplicationError is UNSUPPORTED_VM_CONFIGURATION -

Try to delete all VMWare snapshots on the guest, and wait for the next iteration. This usually works around snapshotting and CBT issues

- dataReplicationError is LAST_SNAPSHOT_JOB_FAILED

Check to see if the snapshots are successfully being created in vCenter. You can check this by clicking on the VM which is in the error state > Choosing Monitor tab > Tasks

Check the replication log which can be found at `/var/lib/aws-vcenter-client/active/tmp/Unique-ID/snapshot-num.log.0`

Logs

`/var/lib/aws-vcenter-client/active/aws-vcenter-client-upgrader.log` - This is the log for the upgrade process of the Agentless client software

`/var/lib/aws-vcenter-client/active/vcenter_commands_client.log` - This is the main agentless client log that will show the log of the agentless discovery process, etc.

`/installation-directory/aws-vcenter-client-installer.log` - This log will show any issues with the installation process of the MGN agentless client. This will be located in the directory that you have executed the installer from.

`/var/lib/aws-vcenter-client/active/tmp/Unique-ID/snapshot-num.log.0` - When you start replication for a discovered server, it will create a snapshot in vCenter and generate this log which is similar to the agent log. For each snapshot, there is a different log. This will show a log of replication process for the snapshot.

Common replication errors

This section describes common replication errors, possible explanations, and potential mitigations.

Replication errors

- [Agent not seen](#)
- [Not converging](#)

- [Snapshot failure](#)
- [Unstable network](#)
- [Failed to connect AWS replication Agent to replication software](#)
- [Failed to establish communication with replication software](#)
- [Failed to create firewall rules](#)
- [Failed to authenticate with service](#)
- [Failed to create staging disks](#)
- [Failed to pair the replication agent with replication server](#)
- [Unknown data replication error](#)

Agent not seen

- If you see this message, ensure that:
 - The source Server has access to the AWS Application Migration Service service.
 - The replication agent is in running state. For Windows, use Windows services management console (services.msc) or command line (for example, get-services PowerShell). For Linux, use the command `systemctl status aws-replication`.

If the agent is indeed in running state, verify that the connectivity to the Regional AWS MGN endpoint on TCP Port 443. [Learn more about verifying connectivity to AWS MGN regional endpoints.](#)

Not converging

This error message (NOT_CONVERGING) could indicate an inadequate replication speed.

Not converging error implies that there is a backlog, but the transfer of data in comparison to the growth of the data on the source server is slower. If the source server is writing more to the disk as compared to the speed at which its sending the data then we get the not converging error.

- Follow the instructions on [calculating the required bandwidth](#).
- [Verify network bandwidth](#).
- Verify replicator Amazon EBS volumes (associated with the source server) performance. If required, modify EBS volume type from the AWS MGN console: Go to the specific source server page and select the **Disk settings** tab.

- Verify the source server performance. For example CPU and Memory utilization.

Snapshot failure

This error message (SNAPSHOTS_FAILURE) indicates that the service is unable to take a consistent snapshot.

This can be caused by:

- Inadequate IAM permissions – Check your CloudTrail logs for any errors in the CreateSnapshot API call. Ensure that you have the required IAM permissions (attached to the required IAM roles).
Restrictive Service Control Policies – Check if your AWS Organization has a Service Control Policy (SCP) that is preventing the snapshot creation.
- API throttling – Check your CloudTrail logs for API throttling errors.

Unstable network

This error message (UNSTABLE_NETWORK) may indicate that there are network issues. Check your connectivity, then [run the network bandwidth test](#).

Failed to connect AWS replication Agent to replication software

This error message (FAILED_TO_PAIR_AGENT_WITH_REPLICATION_SOFTWARE) may indicate a pairing issue. AWS MGN needs to provide the replication server and agent with information to allow them to communicate. Make sure there is network connectivity between the agent, migration server, and the AWS MGN endpoint.

If the issue persists, contact support.

Failed to establish communication with replication software

This error message (FAILED_TO_ESTABLISH_AGENT_REPLICATOR_SOFTWARE_COMMUNICATION) may suggest that there are network connectivity issues. Make sure you have network connectivity between the agent, replication server and the AWS MGN endpoint.

Failed to create firewall rules

This error message (Firewall rules creation failed) can be caused by several reasons.

1. Ensure that the IAM permission prerequisites are met.
2. Review the replication settings of the associated source server.

Failed to authenticate with service

This error message (Failed to authenticate the replication server with the service) may indicate a communication issue between the replication server and the AWS MGN endpoint on TCP Port 443. Check the subnet you selected and ensure that TCP Port 443 is open from your replication server.

To verify the connection:

- Launch a test Amazon Linux 2 EC2 instance in the same subnet that was selected in the replication settings.
- On the server, run the following command:

```
wget <enter_MGN_regional_endpoint>
```

- If the command fails, there is a connectivity problem.

Failed to create staging disks

This error message (Failed to create staging disks) may indicate that your AWS account is configured to use encrypted EBS disks, but the IAM user does not have the required permissions to encrypt using the selected KMS key.

Check your CloudTrail logs for any errors in the CreateVolume API call. Then ensure that you have the required IAM permissions attached to the specified IAM role. If the issue persists, also check your KMS Key Policy for any statements that may prevent AWS MGN from using the selected KMS key.

Failed to pair the replication agent with replication server

This error message (Failed to pair replication agent with replication server) may be caused by multiple reasons. Make sure that you have connectivity between the replication agent, the replication server, and the AWS MGN endpoint. If the issue persists, contact Support.

Unknown data replication error

Unknown errors (unknown_error) can occur for any number of reasons. There are several steps you can take to attempt to mitigate the issue:

- Check connectivity.
- Check throttling.
- Check performance issue on the replication server.
- Check the [network bandwidth](#) between the agent and the replication server.
- [Check the replication agent logs.](#)

Other troubleshooting topics

Topics

- [Re-initialize the AWS Application Migration Service](#)
- [Windows license activation – AWS](#)
- [Migration leaving behind replication volumes after cutover](#)
- [Replication lag issues](#)
- [Windows Driver changes](#)
- [Windows Dynamic Disk troubleshooting](#)
- [Deleting AWS MGN resources](#)
- [Set UEFI boot mode](#)

Re-initialize the AWS Application Migration Service

AWS Application Migration Service can be re-initialized in case of any issues with IAM service roles

To re-initialize the AWS MGN service, please follow these steps:

- Open the AWS Application Migration Service Console and navigate to the correct region you are migrating to.
- In the left navigation pane, select "Settings". Under "Replication template," click "Reinitialize service permissions" and then click "Confirm."

Windows license activation – AWS

AWS Application Migration Service converts the Windows OS licenses to AWS Windows licenses and activates them against the AWS KMS.

If license activation failed, follow [this AWS guide](#) to resolve.

Migration leaving behind replication volumes after cutover

If you are seeing left behind replication volumes in AWS after running the cutover process, then ensure that the names of the replication volumes match those given to them by AWS Application Migration Service (AWS MGN).

Most likely, you have a script running in your AWS account that renames Amazon EBS volumes to match the name of the EC2 instance they are attached to.

However, by renaming an EBS volume used by AWS MGN for replication you are severing its association with AWS MGN, and AWS MGN will not automatically clean up such volumes.

This can also occur if MGN service tags associated with EBS volumes are modified.

Key: `AWSApplicationMigrationManaged`; Value: `mgn.amazonaws.com`

Key: Name;Value: `AWS Application Migration Service Replication Volume`

Replication lag issues

Potential solutions:

- Make sure that the Source server is up and running.
- Make sure that AWS MGN services are up and running.
- Make sure that TCP Port 1500 is not blocked outbound from the source server to the replication server.
- If the MAC address of the Source had changed, that would require a reinstallation of the AWS Replication Agent.
- If the source server was rebooted recently or the AWS Application Migration Service were restarted, the disks are re-read after this and until its finished, the Lag will grow.
- If the source server had a spike of write operations, the lag will grow until AWS Application Migration Service manages to flush all the written data to the test or cutover instance replication server.

To learn more about replication lag troubleshooting, please refer [AWS Support knowledge center article](#).

Windows Driver changes

Users may see changes in Windows drive letter assignments (for example, Drive D changed to E) on target machines launched by AWS Application Migration Service.

This happens because Windows sometimes re-configures the drive letters when a machine comes up on a new infrastructure, for example, if the Source server had a drive letter mapped to a disk that was not replicated (such as a network drive). You can solve this issue by remapping the drive letters on the test or cutover instance correctly after it has been launched.

Windows Dynamic Disk troubleshooting

Moving a Windows Dynamic Disk from a local computer to another computer may change the disk status to "Foreign", resulting in a disruption in replication. The solution is to import the foreign disk, as discussed in [this Microsoft troubleshooting article](#).

Deleting AWS MGN resources

You can delete various AWS MGN resources, including source servers, jobs, and the replication settings template, through the MGN API. Use the following API commands to delete resources:

DeleteSourceServer

Use the *DeleteSourceServer* API command to delete source servers.

This command:

- Deletes a single source server by ID.
- Successful deletion should result in a 204 HTTP response code.
- To delete source server the server should be in a *DISCONNECTED* or *CUTOVER* state. If the source server has not been cut over, you must first call the *DisconnectFromService* API and then call the *DeleteSourceServer* API.

DeleteJob

Use the *DeleteJob* API command to delete a Job.

This command:

- Deletes a single Job by ID.
- Successful deletion should result in a 204 HTTP response code.
- Job must be in a *COMPLETED* state to be deleted.

DeleteReplicationConfigurationTemplate

Use the *DeleteReplicationConfigurationTemplate* API command to delete the replication template.

This command:

- Deletes a single replication template by ID.
- Successful deletion should result in a 204 HTTP response code.
- All source servers and jobs must first be deleted before calling the *DeleteReplicationConfigurationTemplate* API.

Set UEFI boot mode

UEFI boot mode can only be used with Nitro based EC2 Instance types. Nitro requires ENA driver, which is only supported from kernel 3.10. If you are getting the following error: "Source server boot mode is UEFI which is inconsistent with target instance." It might be due to OS using old UEFI format, which was used up to kernel 3.8.

If this is the case you should set the source server boot mode to 'Legacy BIOS'.

FAQ

Topics

- [General questions](#)
- [Agent related](#)
- [Agentless replication related](#)
- [Replication related](#)
- [AWS related](#)
- [Does AWS MGN work with...?](#)
- [Post-launch actions related](#)

General questions

Topics

- [Can AWS Application Migration Service protect or migrate physical servers?](#)
- [What data is stored on and transmitted through Application Migration Service servers?](#)
- [What should I consider when replicating Active Directory?](#)
- [Does AWS Application Migration Service work with LVM and RAID configurations?](#)
- [What is there to note regarding SAN/NAS support?](#)
- [Does AWS Application Migration Service support Windows License migration?](#)
- [Can you perform an OS \(Operating System\) upgrade with AWS Application Migration Service?](#)
- [What are the AWS Application Migration Service quota limits?](#)
- [What are the Private APIs used by AWS MGN to define actions in the IAM Policy?](#)
- [Which post-launch scripts does AWS MGN support?](#)
- [What happens if I use a custom DNS?](#)
- [Can I use AWS Application Migration Service to migrate servers from VMware Cloud on AWS \(VMC\) to Amazon EC2?](#)
- [When should I use AWS Elastic Disaster Recovery \(AWS DRS\) for migration?](#)

Can AWS Application Migration Service protect or migrate physical servers?

Because AWS Application Migration Service works at the OS layer it can protect and migrate not only virtual servers but physical ones as well.

What data is stored on and transmitted through Application Migration Service servers?

AWS Application Migration Service store only configuration and log data on the AWS Application Migration Service console's encrypted database. Replicated data is always stored on the customer's own cloud VPC. The replicated data is encrypted in transit.

What should I consider when replicating Active Directory?

There are two main approaches when it comes to migrating Active Directory or domain controllers from a disaster:

1. Replicating the entire environment, including the AD server(s) – in this approach it is recommended to launch the test or cutover AD servers first, wait until it's up and running, and then launch the other test or cutover instances, to make sure the AD servers are ready to authenticate them.
2. Leaving the AD server(s) in the source environment – in this approach, the test or cutover instances will communicate back to the AD server in the source environment and will take the source server's place in the AD automatically.

In this case, it is important to conduct any tests using an isolated subnet in the AWS cloud, so to avoid having the test or cutover instances communicate into the source AD server outside of a cutover.

Does AWS Application Migration Service work with LVM and RAID configurations?

Yes, AWS Application Migration Service works with any such configuration.

What is there to note regarding SAN/NAS support?

If the disks are represented as block devices on the machine, as most SAN are, AWS Application Migration Service will replicate them transparently, just like actual local disks.

If the disks are mounted over the network, such as an NFS share, as most NAS implementations are, the AWS Replication Agent would need to be installed on the actual NFS server in order to replicate the disk.

Does AWS Application Migration Service support Windows License migration?

AWS Application Migration Service conforms to the [Microsoft Licensing on AWS](#) guidelines.

Can you perform an OS (Operating System) upgrade with AWS Application Migration Service?

Yes. AWS Application Migration Service allows you to [perform an OS upgrade](#) using a predefined action. The action will clone your machine and upgrade the clone. After the upgrade, verify that the cloned machine is working well, and then you can begin using it.

What are the AWS Application Migration Service quota limits?

The following are the AWS Application Migration Service service quota limits:

Name	Default	Description
Concurrent jobs in progress	Each supported AWS Region: 20	Launching a test or cutover instance, or a cleanup action is considered a "job". This parameter is the maximum number of Jobs that can be run concurrently. Jobs that are Completed are not counted against this quota.
Max active source servers	Each supported AWS Region: 20	The maximum number of servers that can be actively

Name	Default	Description
		<p>replicating at any time. You can increase this value to 60. For larger migrations, contact Support.</p>
<p>Max non-archived source servers</p>	<p>Each supported AWS Region: 4,000</p>	<p>This parameter is used for agentless migrations. This is the max number of servers that can be managed by MGN, in non-archived state. This includes the servers that are actively replicating, as well as any servers whose replication has not yet started. The number of actively replicating servers is controlled by the parameter Max active source servers.</p>
<p>Max source servers in a single job</p>	<p>Each supported AWS Region: 200</p>	<p>Launching a test or cutover instance, or a cleanup action is considered a "Job". If you select multiple servers, and perform one of these actions, they are grouped into a single job. This is the maximum number of servers that can be grouped into a single Job.</p>

Name	Default	Description
Max source servers in all jobs	Each supported AWS Region: 200	Launching a test or cutover instance, or a cleanup action is considered a "Job". This is the maximum total number of servers that can be configured in all active Jobs. Jobs that are Completed are not counted against this quota.
Max total source servers per AWS account	Each supported AWS Region: 50,000	This parameter is the maximum total servers, both active and archived, that can be migrated in a single account in each AWS Region. Servers that are deleted, are not counted against this quota.
Max concurrent jobs per source server	Each supported AWS Region: 1	Launching a test or cutover instance, or a cleanup action is considered a "Job". This is the maximum number of active Jobs, that can be configured per server. Jobs that are Completed are not counted against this quota.

You can learn about the AWS Application Migration Service limits in the [AWS General Reference](#).

What are the Private APIs used by AWS MGN to define actions in the IAM Policy?

MGN utilizes the following Private API resources as actions in the IAM Policy. [Learn more about Actions, resources, and condition keys for MGN.](#)

- `BatchCreateVolumeSnapshotGroupForMgn` – Grants permission to create volume snapshot group.
- `BatchDeleteSnapshotRequestForMgn` – Grants permission to batch delete snapshot request.
- `DescribeReplicationServerAssociationsForMgn` – Grants permission to describe replication server associations.
- `DescribeSnapshotRequestsForMgn` – Grants permission to describe snapshots requests.
- `GetAgentCommandForMgn` – Grants permission to get agent command.
- `GetAgentConfirmedResumeInfoForMgn` – Grants permission to get agent confirmed resume info.
- `GetAgentInstallationAssetsForMgn` – Grants permission to get agent installation assets.
- `GetAgentReplicationInfoForMgn` – Grants permission to get agent replication info.
- `GetAgentRuntimeConfigurationForMgn` – Grants permission to get agent runtime configuration.
- `GetAgentSnapshotCreditsForMgn` – Grants permission to get agent snapshots credits.
- `GetChannelCommandsForMgn` – Grants permission to get channel commands.
- `NotifyAgentAuthenticationForMgn` – Grants permission to notify agent authentication.
- `NotifyAgentConnectedForMgn` – Grants permission to notify agent is connected.
- `NotifyAgentDisconnectedForMgn` – Grants permission to notify agent is disconnected.
- `NotifyAgentReplicationProgressForMgn` – Grants permission to notify agent replication progress.
- `RegisterAgentForMgn` – Grants permission to register agent.
- `SendAgentLogsForMgn` – Grants permission to send agent logs.
- `SendAgentMetricsForMgn` – Grants permission to send agent metrics.
- `SendChannelCommandResultForMgn` – Grants permission to send channel command result.
- `SendClientLogsForMgn` – Grants permission to send client logs.
- `SendClientMetricsForMgn` – Grants permission to send client metrics.
- `UpdateAgentBacklogForMgn` – Grants permission to update agent backlog.
- `UpdateAgentConversionInfoForMgn` – Grants permission to update agent conversion info.
- `UpdateAgentReplicationInfoForMgn` – Grants permission to update agent replication info.
- `UpdateAgentReplicationProcessStateForMgn` – Grants permission to update agent replication process state.
- `UpdateAgentSourcePropertiesForMgn` – Grants permission to update agent source properties.
- `CreateVcenterClientForMgn` – Grants permission to create a vCenter client.

- `GetVcenterClientCommandsForMgn` – Grants permission get a vCenter client.
- `SendVcenterClientCommandResultForMgn` – Grants permission to send vCenter client command result.
- `SendVcenterClientLogsForMgn` – Grants permission to send vCenter client logs.
- `SendVcenterClientMetricsForMgn` – Grants permission to send vCenter client metrics.
- `NotifyVcenterClientStartedForMgn` – Grants permission to notify vCenter client started.
- `IssueAgentCertificateForMgn` – Grants permission to send certificate signing request.

Which post-launch scripts does AWS MGN support?

MGN can run scripts on a launched test or cutover instance. This is done by creating the following folder on the source server and placing the scripts within that folder.

Linux: `/boot/post_launch` (any files that are marked as executable)

Windows: `C:\Program Files (x86)\AWS Replication Agent\post_launch\` (any `.exe`, `.cmd`, or `.bat` files)

Once you put these scripts in the above folders on the source server, the folder will be replicated to the test or cutover instance and be executed once after the instance boots for the first time.

Note

Post-launch scripts on Windows run under the Local System context. Post-launch scripts on Linux run under the 'root' user.

Uninstalling VMTools from Windows

The following script can be utilized to uninstall VMTools post migration from Windows. This is a powershell script. It needs to be wrapped by a `.CMD` file, as powershell scripts are not run automatically by the `post_launch`.

```
$regpath = "HKLM:\Software\Microsoft\Windows\CurrentVersion\uninstall"  
  
Get-childItem $regpath | % {
```



```
$keypath = $_.pschildname

$key = Get-Itemproperty $regpath\$keypath

if ($key.DisplayName -match "VMware Tools") {

$VMwareToolsGUID = $keypath

}

MsiExec.exe /x $VMwareToolsGUID /qn /norestart

}
```

What happens if I use a custom DNS?

Custom DNS settings can cause issues in the replication servers.

Therefore, if you are using a custom DNS, you will need to add a TCP port 53 to the security group outbound rules, for replication and conversion servers.

Can I use AWS Application Migration Service to migrate servers from VMware Cloud on AWS (VMC) to Amazon EC2?

Yes, you can. For migrations of source servers from [VMC](#) to EC2 you have two options. You can install the agentless appliance in your VMC environment, and migrate your servers using [agentless replication](#), or install the [AWS replication agent](#) on each of your source servers, and use agent-based replication for your migration.

When should I use AWS Elastic Disaster Recovery (AWS DRS) for migration?

In cases that DRS supports a feature that does not exist in MGN, DRS can be used for migration. You can install the DRS replication agent on your source servers. Following replication, you can launch recovery instances in your target environment, to complete the migration.

DRS can be used for migration, as the DRS and MGN services use shared technology for performing block level replication. Both MGN and DRS have a replication agent, for replicating servers into a

staging area in AWS. MGN supports launching test and cutover instances from the staging area. DRS supports launching recovery instances from the staging area. The technology used by both of these services for launching instances in AWS is very similar. DRS also has the capability to failback to the source environment, after the source environment has recovered. This capability does not exist in MGN.

Note that you cannot install the DRS and MGN agents on the same server at the same time. If you already installed the MGN agent on a server, and want to use DRS for migration, you must uninstall the MGN agent before installing the DRS agent.

Note that there are costs associated with using the DRS service. For DRS pricing information see [AWS Elastic Disaster Recovery pricing](#).

Agent related

Topics

- [What does the AWS Replication Agent do?](#)
- [What kind of data is transferred between the agent and the AWS Application Migration Service?](#)
- [Can a proxy server be used between the source server and the AWS Application Migration Service console?](#)
- [What are the prerequisites needed to install the AWS Replication Agent?](#)
- [What ports does the AWS Replication Agent utilize?](#)
- [What privileges does the AWS Replication Agent require?](#)
- [Is it possible to install the agent on servers running operating systems that are not listed as supported?](#)
- [What kind of resources does the AWS Replication Agent utilize?](#)
- [Can AWS Application Migration Service migrate containers?](#)
- [Does the AWS Replication Agent cache any data to disk?](#)
- [How is communication between the AWS Replication Agent and the AWS Application Migration Service secured?](#)
- [Is it possible to change the port the AWS Replication Agent utilizes from TCP Port 1500 to a different port?](#)
- [How do I manually uninstall the AWS Application Migration Service agent from a server?](#)

- [When do I need to reinstall the agent?](#)
- [How much bandwidth does the AWS Replication Agent consume?](#)
- [How many disks can the AWS Replication Agent replicate?](#)
- [Is it possible to add a disk to replication without a complete resync of any disks that have already been replicated?](#)
- [Is the AWS Replication Agent installed on launched test and cutover instances?](#)
- [How do temporary credentials work?](#)
- [Which Windows and Linux OSs support no-rescan upon reboot?](#)

What does the AWS Replication Agent do?

The AWS Replication Agent performs an initial block-level read of the content of any volume attached to the server and replicates it to the replication server. The agent then acts as an OS-level read filter to capture writes and synchronizes any block level modifications to the AWS Application Migration Service replication server, ensuring near-zero RPO.

What kind of data is transferred between the agent and the AWS Application Migration Service?

The AWS Replication Agent sends the following types of information to the Service Manager of AWS Application Migration Service:

- Monitoring metrics of the agent itself
- Replication status (started, stalled, resumed)
- Backlog information
- OS and hardware information

When an Agent is installed on a source server, it collects the following information on the machine:

- Host name and ID
- List of CPUs including models and number of cores
- Amount of RAM
- Hardware and OS information

- Number of disks and their size – in Windows, disk letters; in Linux, block device names
- Machine's Private IP address

Can a proxy server be used between the source server and the AWS Application Migration Service console?

Yes. The proxy is configured using an environment variable prior to the install.

```
https_proxy=https://PROXY:PORT/
```

For example: `https_proxy=https://10.0.0.1:8088/`

Make sure the proxy has a trailing forward slash.

Ensure that you have allowlisted the [MGN IPs and URLs](#) for both SSL Interception and Authentication.

What are the prerequisites needed to install the AWS Replication Agent?

The installation requirements for source server depend on the type of OS that the server runs – either Linux or Windows.

Prerequisites [can be found here](#).

What ports does the AWS Replication Agent utilize?

The Agent utilizes TCP Port 443 to communicate with the Service Manager of Application Migration Service and TCP Port 1500 for replication to AWS.

What privileges does the AWS Replication Agent require?

The AWS Replication Agent installer requires root privileges or the use of the `sudo` command during installation. It creates an "aws-replication" group and user, and attempts to add the "aws-replication" user to the "sudoers" file to grant necessary permissions. Ensure that the user running the installation has sufficient privileges to modify the "sudoers" file. If the installation fails due to insufficient permissions, you may need to manually add the "aws-replication" user to the "sudoers" file before attempting the installation again.

Is it possible to install the agent on servers running operating systems that are not listed as supported?

The agent is designed and tested to work on the officially supported operating systems listed in the documentation. Installing the agent on other unsupported operating systems may be possible but is not recommended. Any installation or replication issues encountered when using unsupported operating systems will need to be handled through your own troubleshooting or support channels, as the AWS engineering team will be limited in their ability to assist. We advise using the agent only on supported OS versions to ensure the best experience. Please refer to the [documentation](#) for the list of supported operating systems before installation.

What kind of resources does the AWS Replication Agent utilize?

The AWS Replication Agent is lightweight and nondisruptive. The agent utilizes approximately 5% CPU and 250 MB of RAM.

Can AWS Application Migration Service migrate containers?

AWS Application Migration Service (AWS MGN) only supports the replication of full servers. Nevertheless, AWS MGN replicates on a server level and therefore any containers within the selected servers will be replicated.

Does the AWS Replication Agent cache any data to disk?

AWS Application Migration Service does not write any cache or do any sort of journalling to disk. The Agent holds a buffer which is large enough to map all volume's blocks ~250 MB in memory.

The agent then acts as a sort of write filter and will replicate changed blocks directly from memory to the Replication Server. In cases where the data is no longer in memory, the agent will read the block from the volume directly. This is the case where you may see backlog in the AWS Application Migration Service console. The cause of this is the volume of change is greater than the bandwidth available.

How is communication between the AWS Replication Agent and the AWS Application Migration Service secured?

All communication is encrypted using SSL. In addition, each Agent is assigned a key during installation which is used to encrypt all traffic. All keys are unique and are not shared across multiple agents.

Is it possible to change the port the AWS Replication Agent utilizes from TCP Port 1500 to a different port?

No. The AWS Application Migration Service Agent can only utilize TCP Port 1500 for replication.

How do I manually uninstall the AWS Application Migration Service agent from a server?

Follow the steps in the [the section called “Uninstalling the Agent”](#) section.

When do I need to reinstall the agent?

Typically, you need to reinstall the Agent after any major upgrade to the source server.

Linux

- Any kernel upgrade
- After adding new volumes

Windows

- Any OS upgrade (for example, Windows Server 2012 to Windows Server 2016)

Note

If you [upgrade using a post-launch action](#), an agent upgrade is not required.

- After adding new volumes

How much bandwidth does the AWS Replication Agent consume?

The AWS Replication Agent opens up to five connections and will attempt to maximize available bandwidth.

Throttling can be activated via the AWS Application Migration Service console by either selecting a specific server and clicking the **Replication settings** tab or by changing the **Replication template** (in this case the change will only affect newly added servers).

How many disks can the AWS Replication Agent replicate?

The agent can replicate up to 50 disks from a single server.

Is it possible to add a disk to replication without a complete resync of any disks that have already been replicated?

When you are adding a disk to a source server, AWS Application Migration Service will not automatically identify this disk and add it to the **Disk settings** section in the console.

The only way to get this disk to replicate is to reinstall the agent. Before reinstalling, you can note the current **Total replicated storage**. When you reinstall the agent, you will notice the value of replicated storage changes.

You will also notice an additional progress bar appear, which indicates that we are rescanning the original volumes. This is not a resync, but a scan, to verify that all the blocks on the source still match the blocks on the replication side. This process is significantly quicker than a resync, as there is no actual block data transferred, unless there is a difference. This is needed, as a reinstall results in the driver which performs the IO tracking being unloaded and reset, so we have no way of being certain of the sync status. Whilst the rescan on the original volumes is happening, the agent is also ensuring that the initial sync of the new volume is being completed in parallel.

Is the AWS Replication Agent installed on launched test and cutover instances?

During the launch process, either upon test or cutover instance launch, the AWS Replication agent is removed from the test or cutover instance, and will not run on it.

How do temporary credentials work?

The temporary credential mechanism was developed specifically to provide an easy and secure way to install AWS MGN Agents. The main flow of the temporary credentials' creation process relies on generating an x509 certificate per agent and then using this x509 certificate to receive temporary IAM credentials. This process utilizes a similar mechanism to the one used by [IAM Roles Anywhere](#).

Which Windows and Linux OSs support no-rescan upon reboot?

A shutdown (from the OS menu or CLI) of any supported Linux or Windows source server no longer causes a rescan in AWS MGN once the source server is restarted.

A rescan means that the agent on the source server rereads all blocks on all replicated disks and transmits blocks that are different from the previously replicated data. A rescan is similar to the initial sync but is faster because only blocks that are different need to be transmitted.

Rescans can still happen following a hard reboot, crashes, or when you add or remove disks to or from the source server.

Supported OSs include:

Windows Server

- 2012r1
- 2012r2
- 2016
- 2019
- 2022

Linux

- CentOS 6–8
- Oracle 6–8
- RHEL 6–9
- Rocky 8 and 9
- SLES 12 and 15
- Debian 9–11
- Ubuntu 16, 18, 20, and 22
- Amazon Linux 2

Note

For Linux, no-rescan on reboot is supported only on environments that use initramfs.

Agentless replication related

Topics

- [In which situations would you recommend using agentless replication \(snapshot shipping\)?](#)
- [In which situations would you recommend using agent-based replication?](#)
- [How does agentless replication work?](#)
- [Does agentless replication require installing any component in the customer's source data center?](#)
- [Is the agentless feature available in all Regions that AWS MGN service supports?](#)
- [Does agentless replication support the same source operating systems that are supported by agent-based replication?](#)
- [Is the agentless feature supported in CloudEndure migration?](#)
- [Which virtualization environments are supported by the agentless feature?](#)
- [On which operating systems can the MGN vCenter Client be installed?](#)
- [Do I need to generate special credentials to install the MGN vCenter Client?](#)
- [What are the agentless replication prerequisites?](#)
- [How do I install the MGN vCenter Client?](#)
- [Can a proxy server be used between the source server and the AWS Application Migration Service console?](#)

In which situations would you recommend using agentless replication (snapshot shipping)?

Agentless replication best serves customers whose company's security policies do not allow installing an agent on each of their source servers, or for operating systems that are only supported by agentless replication. This solution is only available for data centers using vCenter version 6.7, 7.0 and 8.0.

In which situations would you recommend using agent-based replication?

Agent-based replication is our default recommendation for all use cases, except when your company's security policies prevent you from using this method or if the OS is not supported. Using agent-based replication provides Continuous Data Replication, and ensures a cutover window of minutes. When using agentless replication, the data is transferred using snapshot shipping. Upon cutover, you may need to wait to have a fully updated snapshot, and your cutover window may be longer.

How does agentless replication work?

You can learn more about how agentless replication works and see a high-level diagram of the agentless replication framework in the [agentless replication documentation](#).

Does agentless replication require installing any component in the customer's source data center?

Yes. In order to use agentless replication, customers must install the MGN vCenter Client in their source data center. The client discovers the source servers and replicates their data to AWS.

Is the agentless feature available in all Regions that AWS MGN service supports?

Yes. Both agent-based and agentless replication is supported in AWS Application Migration Service (AWS MGN) in all Regions.

Does agentless replication support the same source operating systems that are supported by agent-based replication?

Agentless replication supports all of the [supported OSs](#) of agent-based replication.

Is the agentless feature supported in CloudEndure migration?

No. This feature is only available on AWS Application Migration Service.

Which virtualization environments are supported by the agentless feature?

The agentless replication feature is available for vCenter versions 6.7, 7.0 and 8.0. Other virtualization environments are not supported.

On which operating systems can the MGN vCenter Client be installed?

The MGN vCenter Client can be installed on the following 64 bit Linux versions:

- Ubuntu 18.x+ (64 bit) - 22.04

- Amazon Linux 2
- RHEL 8.x

Do I need to generate special credentials to install the MGN vCenter Client?

Yes. In order to use the AWS MGN vCenter Client, you must first generate the correct IAM credentials. Learn more in the [agentless replication documentation](#).

What are the agentless replication prerequisites?

The only prerequisite for agentless replication is to ensure that you have [initialized AWS Application Migration Service](#).

How do I install the MGN vCenter Client?

You can learn more about installing the MGN vCenter Client as well as installation requirements in the [agentless replication documentation](#).

Can a proxy server be used between the source server and the AWS Application Migration Service console?

Yes. You can configure transparent proxy either by using an environment variable prior to the installation (Linux and Windows), or by using the `--proxy-address` flag in the Linux installer:

- Using the installer: `./aws-vcenter-client-installer-init.py --proxy-address http://PROXY:PORT/`
- Using environment variable: `export https_proxy=http://PROXY:PORT/; ./aws-vcenter-client-installer-init.py`

Make sure the proxy has a trailing forward slash (/).

Replication related

Topics

- [What is the lifecycle of the snapshots and volumes automatically created during migration?](#)
- [What do Lag and Backlog mean during replication?](#)

- [What is Continuous, Block level data replication?](#)
- [What are the Replication initiation Steps?](#)
- [Is the replicated data encrypted?](#)
- [How is the Replication Server provisioned and managed in the Staging Area?](#)
- [What type of replication server is utilized in the AWS Application Migration Service staging area?](#)
- [Can we set specific IP addresses for the replication server or conversion server in the AWS Application Migration Service staging area?](#)
- [Does AWS Application Migration Service compress data during replication?](#)
- [Are events that are generated by the AWS Application Migration Service servers logged in Cloudtrail in AWS?](#)
- [How many snapshots does AWS Application Migration Service create?](#)
- [Does AWS Application Migration Service delete snapshots?](#)
- [How much capacity is allocated to the staging area?](#)
- [Why is 0.0.0.0:1500 added to inbound rules in the staging area?](#)
- [Can AWS Application Migration Service replicate Oracle ASM?](#)
- [How long does a rescan take?](#)
- [How can I control the bandwidth used for replication?](#)
- [Are migrations performed by Application Migration Service crash consistent?](#)
- [How can I perform an SSL connectivity and bandwidth test?](#)

What is the lifecycle of the snapshots and volumes automatically created during migration?

For each source block device, we create a corresponding EBS volume. On occasion if there is an issue with the agent on the source machine being able to send data to a volume, we may create a new volume to replace the old one. Our workflow does not necessarily delete the old volume straight away, and it may remain present for around 10 minutes after the replacement volume comes online. But this is going to be rare, if your network connection is stable.

With regards to the snapshots, we take regular snapshots, so that we can take advantage of the incremental nature of snapshots. If we were for example to take a snapshot once every 6 hours, the snapshot would contain 6 hours worth of snapshots, and could potentially take a long time

to complete. By taking them more frequently, we shorten the time taken to create the actual snapshot. This in turn means that when you trigger a test or cutover instance, the time taken to get the process started is not delayed unnecessarily by waiting for EBS snapshots to complete. We would generally keep 5–6 snapshots of a volume, to be sure that there is at least one that is completed when we need it for launch. EBS snapshot creation time has no SLA, and sometimes can be delayed significantly. EBS snapshot creation is also not guaranteed. A snapshot creation can fail (Not the API call, but the actual creation process). Hence we keep the additional snapshots, just in case something more recent actually failed.

What do Lag and Backlog mean during replication?

During replication you may see a server falls out of Continuous Data Protection (CDP) mode. This may occur for various reasons, typically related to the network throughput or interruption.

- **Lag** – The amount of time since the server was last in CDP mode.
- **Backlog** – The amount of data that was written to the disk and still needs to be replicated in order to reach CDP mode.
- **ETA** – The estimated time remaining to return to CDP.

What is Continuous, Block level data replication?

During continuous block-level replication, the replication agent continuously monitors disk input/output (IO) activity on the protected disks. It then replicates all WRITE operations, which involve modifying or adding data, to the Replication Server, ensuring that the data is duplicated and kept up-to-date on the replication server.

What are the Replication initiation Steps?

The following replication steps are involved in the automatic creation of the replication server in the staging area and initiation of data transfer over TCP port 1500:

- **Create security groups** - Creating EC2 security groups with inbound TCP port 1500 allowed. This security group will be attached to replication server.
- **Launch Replication Server** - AWS EC2 instance is launched based on the replication configuration set.
- **Boot Replication Server** - The EC2 instance completes boot process which will now function as a replication server.

- **Authenticate with service** - Using the user data scripts and the EC2 instance configuration, the instance (replication server) will authenticate with AWS Application Migration Service using service/vpc endpoint.
- **Download replication software** - The Replication Server downloads replication software from S3. This replication software will write the incoming replicated data to the Replication Server disks.
- **Create staging disks** - The Replication Server creates replication disks to store the incoming replicated data. The number of replication disks that are created depends on the size of the replicated data.
- **Attach the staging disks** – In the previous step, the replication disks were created independently, without being attached to a specific Replication Server. Now, they are attached to a Replication Server.
- **Pair the Replication Server with AWS Replication Agent** – Until this stage, the AWS Application Migration Service managed the communication between the Agent on the Source infrastructure and the Replication Server on the Target infrastructure. Now, the AWS Application Migration Service knows that all the initiation steps have been completed successfully. Therefore, it provides the Agent and the Replication Server information about each other, so that they could start communicating with each other directly.
- **Connect AWS Replication Agent to the Replication Server** – The Agent and the Replication Server begin communicating with each other directly.
- **Start data transfer** - Replication begins from source server to Replication Server over TCP 1500.

Is the replicated data encrypted?

AWS Application Migration Service encrypts all the data in transit.

How is the Replication Server provisioned and managed in the Staging Area?

AWS Application Migration Service provisions the Replication Server(s) and automatically manages the addition and removal of the servers as necessary. The AWS Application Migration Service automatically replaces the replication server on a periodic basis. This ensures the replication server is using the latest public Amazon Machine Image (AMI) available for MGN. The latest AMI contains the most up-to-date patches, security updates, and bug fixes. Regularly updating the replication server AMIs allows MGN to maintain the replication servers with the newest components and protections. Customers do not need to take any action to receive new replication server AMIs. MGN

will automatically replace the existing replication server as needed when new AMIs are released. This helps keep the replication process secure and up-to-date without any additional effort from users.

What type of replication server is utilized in the AWS Application Migration Service staging area?

AWS Application Migration Service provisions a t3.Small server. The typical ratio of volumes to replication servers is 15:1.

Can we set specific IP addresses for the replication server or conversion server in the AWS Application Migration Service staging area?

No, you cannot specify or assign static IP addresses for the replication server or conversion server in AWS MGN. These servers are managed and maintained by the MGN service itself. The IP addresses for these servers are dynamically assigned from the available pool of IP addresses in the Virtual Private Cloud (VPC) that you specify during the MGN setup process. It's important to note that while you cannot control the specific IP addresses assigned to these servers, you can control the VPC and subnet in which they are deployed. This allows you to configure network access controls and security policies according to your organizational requirements.

Does AWS Application Migration Service compress data during replication?

Yes, AWS Application Migration Service utilizes LZ4 compression during transit resulting in 60–70% compression depending on the type of data.

Are events that are generated by the AWS Application Migration Service servers logged in Cloudtrail in AWS?

Yes, AWS Application Migration Service generates standard AWS API calls that are visible in CloudTrail.

How many snapshots does AWS Application Migration Service create?

5–7 for each disk. Frequency and exact number depend on various factors, such as change rate on the source server and network stability.

There is currently no mechanism for users to adjust the frequency and number of snapshots.

Does AWS Application Migration Service delete snapshots?

AWS Application Migration Service automatically deletes snapshots that are no longer used (such as those left over after source servers have been removed from the AWS Application Migration Service console).

How much capacity is allocated to the staging area?

A volume is created for each volume in the source infrastructure of the same size.

Why is 0.0.0.0:1500 added to inbound rules in the staging area?

AWS Application Migration Service uses TCP Port 1500 for replication between the Source Agents and the replication server. The connection is open for all IPs and can be managed by ACLs or networks controls to limit inbound IPs.

Can AWS Application Migration Service replicate Oracle ASM?

Replication of Oracle with ASM is supported. AWS Application Migration Service also fully supports the use of the Oracle ASM Filter Driver.

How long does a rescan take?

The rescan time will vary depending on the size of the source disks. The time depends on the performance of the disks (linear read), staging area disk performance, and the rate of write operations on the source server (which are sent in parallel with the rescan). The rescan is functioning normally as long as it is moving forward and is not "stuck".

How can I control the bandwidth used for replication?

We recommend you do not limit the bandwidth used for replication. If you have business reasons to require replication to use less bandwidth, you can temporarily use the throttling feature to limit the bandwidth. This will cause lag, that will automatically recover once you remove the throttling.

Are migrations performed by Application Migration Service crash consistent?

Yes, MGN's services are crash-consistent.

How can I perform an SSL connectivity and bandwidth test?

Note

This tool is designed for AWS only.

You can use our SSL bandwidth tool to check for replication bandwidth availability.

1. In your target region, launch a c5.large test server using the public AMI named CE-ssl-speedtest.
2. Select the same subnet as the subnet used in the replication settings of your source machine.
3. Make sure that the security group allows TCP Port 1500 inbound access.
4. On the source machine, browse to `https://{test_server_ip}:1500/speedtest`
5. Click **Start**.

Note

- Browse to the web page using the test server **public** or **private** IP according to what you defined in your replication settings.
- The following are the AMI details per region:
 - ami-00b38c08ab3506ea7 – US East (N. Virginia)
 - ami-0bd8423a4d80563fc – US East (Ohio)
 - ami-00b7159e9c985a8da – US West (N. California)
 - ami-033a4924b13126a7b – US West (Oregon)
 - ami-0bf60b09675c8d9b6 – Africa (Cape Town)
 - ami-0f01375b50763621b – Asia Pacific (Hong Kong)
 - ami-0b1aeb50834102c18 – Asia Pacific (Mumbai)
 - ami-0b1aeb50834102c18 – Asia Pacific (Hyderabad)
 - ami-044fa8034a31d7578 – Asia Pacific (Tokyo)
 - ami-08b042df0d4c458ea – Asia Pacific (Seoul)
 - ami-0971e46306691cd68 – Asia Pacific (Osaka)
 - ami-0afd42552b236f9dd – Asia Pacific (Singapore)
 - ami-04e7cc6b5d9e8ffa1 – Asia Pacific (Sydney)

- ami-02f31943dfd88549d – Asia Pacific (Jakarta)
- ami-033db317ada5abd55 – Asia Pacific (Melbourne)
- ami-01c24408802db503d – Canada (Central)
- ami-0b8643189a66159c9 – Europe (Stockholm)
- ami-0dd5a09d2ae8f46b3 – Europe (Ireland)
- ami-097fb47f3a1c2bf7e – Europe (London)
- ami-0a3f9008725d0b4d1 – Europe (Paris)
- ami-0c65965703bb0e541 – Europe (Milan)
- ami-01b6fcc2337f6420d – Europe (Spain)
- ami-07b7defb87a46bb48 – Europe (Frankfurt)
- ami-01b3e93b3ac0e1340 – Europe (Zurich)
- ami-016edc078b48f370b – Israel (Tel Aviv)
- ami-0c90e298af7a2e563 – Middle East (Bahrain)
- ami-0f7c14e62ef760768 – Middle East (UAE)
- ami-0edd5ecfc56804583 – South America (São Paulo)
- ami-00eb76deb85085b3e – AWS GovCloud (US-West)
- ami-0ba277e7ced412965 – AWS GovCloud (US-East)
- Ensure that the security groups are configured to permit connectivity on inbound port 1500.

AWS related

Topics

- [What does the AWS Application Migration Service Machine Conversion Server do?](#)
- [What boot modes are supported by the AWS Application Migration Service?](#)
- [How can we encrypt an unencrypted AWS Application Migration Service base snapshot?](#)
- [How do I change the server AMI on AWS after Migration?](#)
- [Which AWS services are automatically installed when launching a test or cutover instance?](#)
- [How long does it take to copy a disk from the AWS Application Migration Service staging area to production?](#)

- [What are the differences between conversion servers and replication servers?](#)
- [Can I prevent AWS Application Migration Service from cleaning up test instance resources in AWS?](#)
- [Why are my Windows server disks read-only after launching the test or cutover instance?](#)
- [What impacts the conversion and boot time of test and cutover instances?](#)
- [How is the AWS Licensing Model Tenancy chosen for AWS Application Migration Service?](#)
- [How does AWS Application Migration Service interact with Interface VPC Endpoints?](#)
- [How do I use MGN with CloudWatch and EventBridge dashboards?](#)

What does the AWS Application Migration Service Machine Conversion Server do?

The machine conversion server converts the disks to boot and run on AWS.

Specifically, the machine conversion server makes bootloader changes, injects hypervisor drivers and installs cloud tools.

What boot modes are supported by the AWS Application Migration Service?

The agent supports systems using either BIOS (Basic Input/Output System) or UEFI (Unified Extensible Firmware Interface) boot modes. BIOS is the traditional boot mode that initializes hardware and bootstraps the operating system. UEFI is a more modern boot firmware that provides additional boot configurations and security features over BIOS. Both boot modes are fully supported by the agent, giving users flexibility to choose the mode that best fits their systems and requirements. Users can install the agent on servers using either UEFI or legacy BIOS firmware.

How can we encrypt an unencrypted AWS Application Migration Service base snapshot?

The encryption status of AWS Application Migration Service base snapshots is determined by the default EBS (Elastic Block Store) encryption setting for the respective AWS region. Encryption Scenarios:

- Default EBS Encryption Enabled:

If the default EBS encryption is enabled for the region, the base snapshots created by MGN will be encrypted.

- **Default EBS Encryption Disabled:**

If the default EBS encryption is not enabled, the base snapshots will be unencrypted.

- **Encrypting Existing Unencrypted Base Snapshots -**

To encrypt an existing unencrypted base snapshot, follow these steps:

1. Delete the unencrypted base snapshot from the snapshots console.
2. Enable default EBS encryption for the AWS region where the MGN source environment is located.
3. Initiate a new test or cutover migration in MGN. During this process, MGN will create a new encrypted base snapshot based on the default EBS encryption setting for the region.

 **Note**

Enabling default EBS encryption at the region level will encrypt all newly created EBS volumes and snapshots in that region.

How do I change the server AMI on AWS after Migration?

After the machine has been launched by AWS Application Migration Service switching the AMI can be done by launching a vanilla machine from the required AMI, stopping that machine, detaching all the disks (including the root) and then attaching the disks from the test or cutover instance created by AWS Application Migration Service.

Which AWS services are automatically installed when launching a test or cutover instance?

AWS Application Migration Service automatically installs EC2Config. After installation, EC2Config automatically installs the SSM EC2 Configuration Service.

CloudWatch, AWS Powershell or CLI are not automatically installed. This can be done by the combining the AWS Application Migration Service APIs and the AWS APIs – you can use the AWS

Application Migration Service APIs to determine the EC2 instance IDs of the machines and then use AWS API/CLI to turn on the detailed monitoring. An alternative approach would be to do it via AWS API only based on the tags you associate with the machine. A third approach would be to do so from the post-launch script.

AWS Application Migration Service installs EC2Launch (Windows 2016 only). You will need to configure EC2Launch based on [these specific requirements](#). This configuration step needs to be performed post Migration using the wizard in C:\Program Data\Amazon\EC2-Windows\Launch\Settings\Ec2LaunchSettings.exe on the test or cutover instance.

How long does it take to copy a disk from the AWS Application Migration Service staging area to production?

AWS Application Migration Service uses internal cloud provider snapshots. This process typically takes less than a minute and the size of the volume does not impact the time.

What are the differences between conversion servers and replication servers?

Replication servers run on Linux and conversion servers (for Windows machines) run on Windows.

The conversion is done by AWS Application Migration Service (AWS MGN) automatically bringing up a vanilla Windows conversion server machines in the same subnet with the replication servers as part of the launch job.

Both conversion and replication servers have public IPs.

The conversion servers will use the same security groups as the Replication Server.

The conversion server must be able to access the AWS MGN's service manager.

The conversion server machines, just like the Replication servers are managed automatically by AWS Application Migration Service. Any attempt to disrupt their automated functionality will result in failed conversions.

Can I prevent AWS Application Migration Service from cleaning up test instance resources in AWS?

AWS Application Migration Service will, by default, removes any resources created during the test process either when requested by the user or when a new Test instance is launched.

To prevent this in AWS, you can [activate Termination Protection](#) for the test or cutover instance, and the resources will not be removed upon a new instance launch.

Why are my Windows server disks read-only after launching the test or cutover instance?

When launching test or cutover instances Windows Server may boot with all the disks as read-only.

This is a common issue that occurs when detaching and attaching data disks. This issue can be resolved using steps in [this Microsoft TechNet article](#).

What impacts the conversion and boot time of test and cutover instances?

Prior to launching the test or cutover instance, AWS Application Migration Service goes through a machine conversion server process on the boot volume. The conversion process is fairly quick.

While the actual conversion process itself is quick, the time to boot the test or cutover instance varies depending on many factors unrelated to any AWS Application Migration Service processes. Some of these are controllable and should be taken into account when recovery or cutover times are of importance.

- Operating system – The amount of time required to boot the operating system is dependent on the OS itself. While Linux servers typically boot quickly, Windows servers may take additional time, due to the nature of the Windows OS. If opportunity permits, test the boot time of the source server. If Linux OS takes a long time to boot ensure to check that dhclient (Dynamic Host Configuration Protocol Client) is installed and the system so it can pull an IP.
- Scheduled Windows Updates – If the Windows server has pending patches, ensure those are installed prior to launching the test or cutover instance. If pending patches remain, the boot time in the cloud may be severely impacted as the patch process may commence upon the initial boot.
- Boot volume type – Depending on services/applications, boot time may be impacted by disk performance. It is recommended that boot volumes be tested with a higher performance SSD and even by provisioning IOPs to ensure throughput. This may be more critical during the first initial boot of the server in the cloud, as all initial settings are applied. In many cases, the boot volume type may be scaled back after the initial boot and should be tested.

Note

The first boot of Windows machines on AWS may take up to 45 minutes due to Windows adjusting to the AWS virtual hardware.

How is the AWS Licensing Model Tenancy chosen for AWS Application Migration Service?

AWS Application Migration Service conforms to the [Microsoft Licensing on AWS](#) guidelines.

How does AWS Application Migration Service interact with Interface VPC Endpoints?

If you use Amazon Virtual Private Cloud (Amazon VPC) to host your AWS resources, you can establish a private connection between your VPC and AWS Application Migration Service. You can use this connection to allow AWS Application Migration Service to communicate with your resources on your VPC without going through the public internet.

Amazon VPC is an AWS service that you can use to launch AWS resources in a virtual network that you define. With a VPC, you have control over your network settings, such as the IP address range, subnets, route tables, and network gateways. With VPC endpoints, the routing between the VPC and AWS services is handled by the AWS network, and you can use IAM policies to control access to service resources.

To connect your VPC to AWS Application Migration Service, you define an *interface VPC endpoint* for AWS Application Migration Service. An interface endpoint is an elastic network interface with a private IP address that serves as an entry point for traffic destined to a supported AWS service. The endpoint provides reliable, scalable connectivity to AWS Application Migration Service without requiring an internet gateway, network address translation (NAT) instance, or VPN connection. For more information, see [What is Amazon VPC](#) in the *Amazon VPC User Guide*.

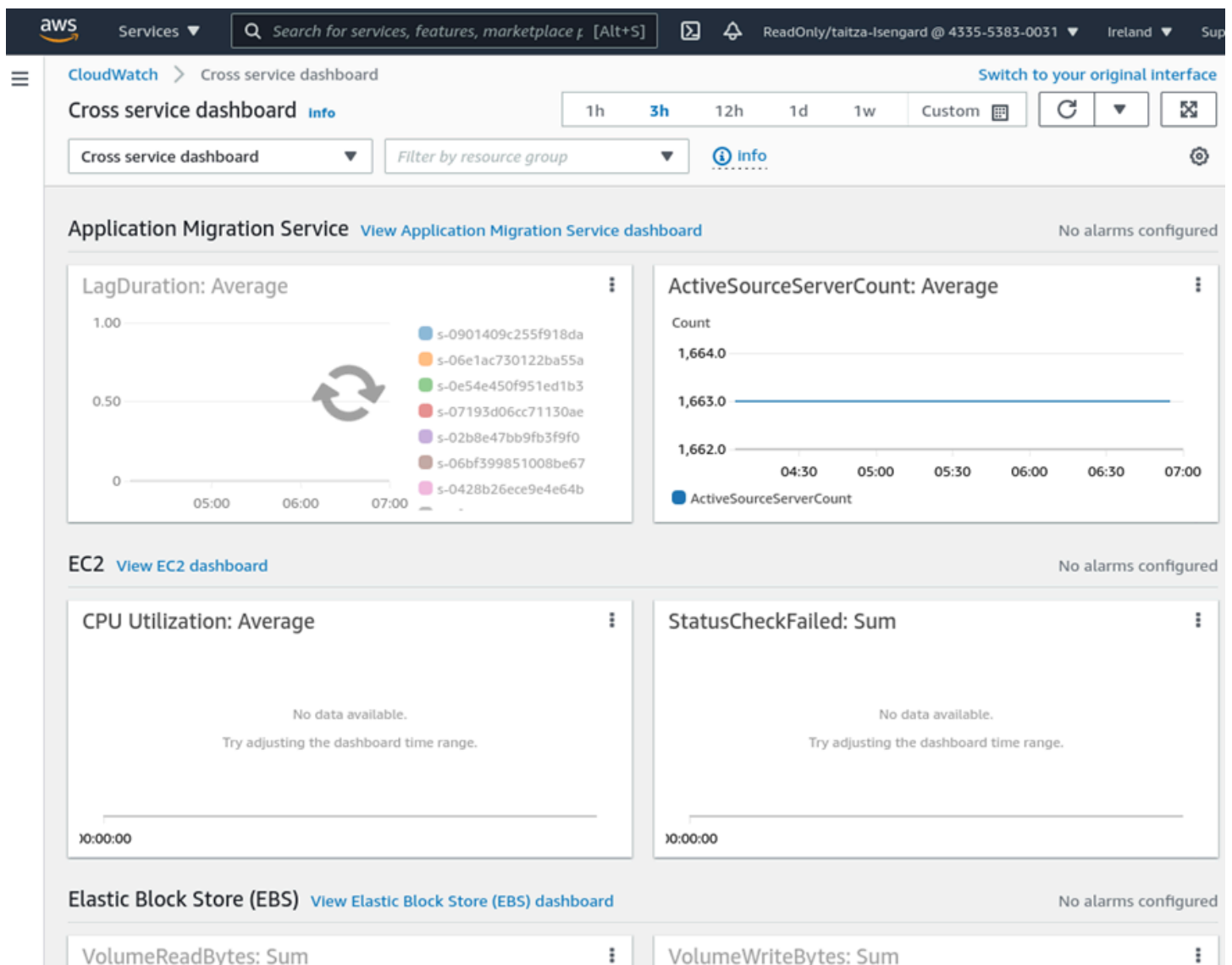
Interface VPC endpoints are powered by AWS PrivateLink, an AWS technology that allows private communication between AWS services using an elastic network interface with private IP addresses. For more information, see [AWS PrivateLink](#).

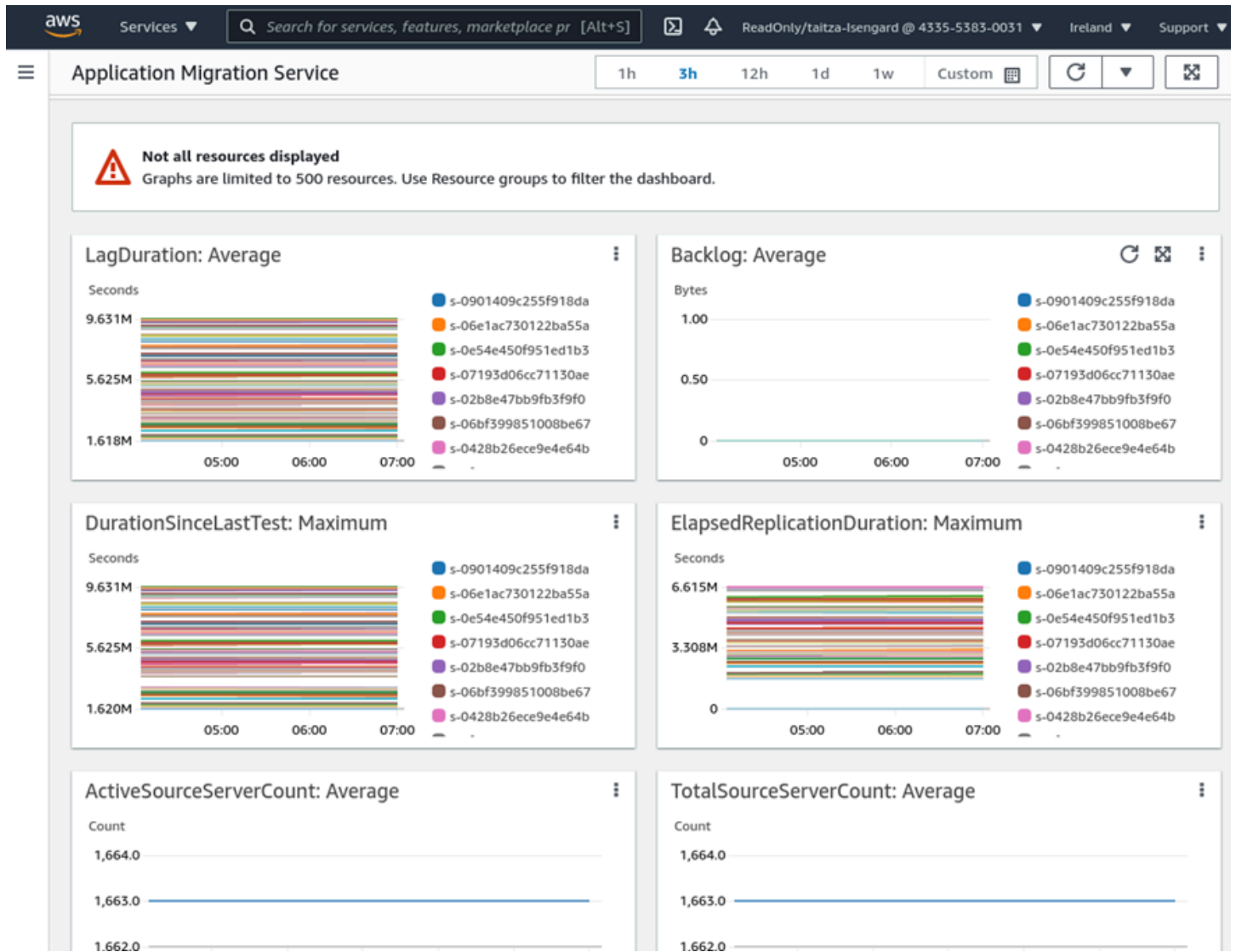
For more information, see [Getting Started](#) in the *Amazon VPC User Guide*.

How do I use MGN with CloudWatch and EventBridge dashboards?

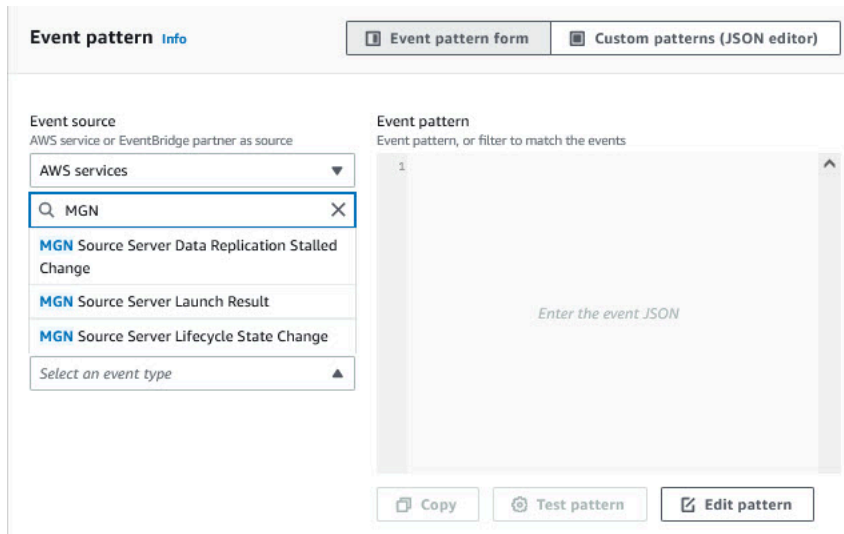
You can monitor AWS Application Migration Service using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. AWS Application Migration Service sends events to Amazon EventBridge whenever a source server launch has completed, a source server reaches the `READY_FOR_TEST` lifecycle state for the first time, and when the data replication state becomes stalled or when the data replication state is no longer Stalled. You can use EventBridge and these events to write rules that take actions, such as notifying you, when a relevant event occurs.

You can see MGN in CloudWatch automatic dashboards:





MGN events can be selected when defining a rule from the EventBridge console:



[Learn more about monitoring MGN.](#)

Does AWS MGN work with...?

Does AWS MGN work with Microsoft Windows Failover Clustering?

Yes.

Does AWS MGN work with Bitlocker encryption?

AWS Application Migration Service does not support OS-based disk encryption features such as BitLocker. These should be deactivated before using AWS MGN.

Post-launch actions related

Topics

- [What operating systems does the post-launch actions framework support?](#)
- [What version of AWS Systems Manager Agent will be installed on my instance?](#)
- [Why is the AWS Systems Manager Agent not executing my post launch actions?](#)

What operating systems does the post-launch actions framework support?

Verify that your operating systems [are supported by AWS Systems Manager](#).

What version of AWS Systems Manager Agent will be installed on my instance?

AWS Application Migration Service uses the latest [AWS Systems Manager Agent](#) version available in your instance's region.

Why is the AWS Systems Manager Agent not executing my post launch actions?

- By default, [AWS Systems Manager](#) doesn't have permission to perform actions on your instances. Grant access by using an AWS Identity and Access Management (IAM) instance profile. You can

create an instance profile for AWS Systems Manager by attaching one or more IAM policies that define the necessary permissions to a new role or to a role you already created. You can use the managed policy AmazonSSMManagedInstanceCore which allows an instance to use AWS Systems Manager service core functionality or create a custom policy. For more information, see [Create an IAM instance profile for AWS Systems Manager](#).

- The instances you connect to must also allow HTTPS (port 443) outbound traffic to the following endpoints:

```
ec2messages.<REGION>.amazonaws.com  
ssm.<REGION>.amazonaws.com  
ssmmessages.<REGION>.amazonaws.com
```

You can connect to the required endpoints by using interface endpoints. For more information, see [Creating VPC endpoints for AWS Systems Manager](#).

Alternatively, you can use public IP addresses for communication between your instances and the internet.

- Another reason might be that the managed instance has limited available CPU or memory resources. Although your instance might otherwise be functional, if the instance doesn't have enough available resources, you can't establish a session. For more information, see [Troubleshooting an unreachable instance](#).

Release notes

June 2024

- Added support for deploying AWS Replication Agent on a secured network in the Europe (Spain), Europe (Zurich), Middle East (UAE), Asia Pacific (Hyderabad), Asia Pacific (Osaka) and Asia Pacific (Sydney) regions. [Learn about installing the agent on a secured network.](#)
- Added support for encrypting post-launch action parameters. Learn about [post launch action.](#)
- [AWS managed policy updates](#) - Updated the AWSApplicationMigrationFullAccess policy to support SecureString parameter type in SSM Parameters Store for post-migration framework actions.
- Added support for migrating servers with Kernel versions up to 6.8.
- Added support for Ubuntu LTS 24.04
- Introduced a new predefined post-launch action: Dynatrace. [Learn more about Dynatrace action](#)

May 2024

- Added support for deploying AWS Replication Agent on a secured network in the Israel (Tel Aviv) region. [Learn about installing the agent on a secured network.](#)

March 2024

- Added support for migration of Linux servers retaining boot mode UEFI.
- Added support for migrating servers running Rocky Linux 9.0 and SUSE Linux Enterprise Server 15 service packs 4 and 5.
- Added support for migrating servers with Kernel versions up to 6.5.

January 2024

- Added support for agentless replication on VMware vCenter version 8. [Learn about agentless replication](#)

December 2023

- Added support for the MGN connector to communicate with Windows servers over HTTP and to authenticate with Linux servers using a password. [Learn more about MGN connector actions.](#)
- [AWS managed policy updates](#) – Created a new revision to support MGN in AWS GovCloud and added Statement ID (SID) to a managed policy statement: AWSApplicationMigrationServiceEc2InstancePolicy.
- Added support for deploying AWS Replication Agent on a secured network in the Asia Pacific (Jakarta) Region. [Learn about installing the agent on a secured network.](#)

November 2023

- Introduced a new predefined post-launch action: [App2Container for Replatforming.](#)

September 2023

- Introduced **MGN connector**, a feature that helps automate the agent installation on source servers. [Learn more here.](#)
- Display tags as columns in the source servers, applications and waves table in the console.
- Added support for Amazon Linux 2023.
- Added support for kernel versions up to 6.1.
- Added support for using agentless replication with a proxy server. For more information see [agentless replication installation instructions.](#)

August 2023

- Introduced 3 new predefined post-launch actions:
 - [Verify tags](#)
 - [Auto Scaling group setting](#)
 - [Enable Refactor Spaces](#)

[Learn more about predefined post-launch actions.](#)

- Service launch in the Israel (Tel Aviv) region.

June 2023

- Service launch in the following regions: Europe (Zurich), Europe (Spain), Asia Pacific (Hyderabad), Asia Pacific (Melbourne).
- Introduced Import and export from local disk. You can now import and export your source servers, applications, and waves from and to a CSV file on your local disk. [Learn more about the import and export feature.](#)
- Introduced 4 new predefined post-launch actions:
 - [Configure Time Sync](#)
 - [Validate disk space](#)
 - [Verify HTTP/HTTPS response](#)
 - [Enable Amazon Inspector](#)

[Learn more about predefined post-launch actions.](#)

- Introduced global view, that allows you to manage migrations across multiple accounts using an integration with AWS Organizations. This feature provides visibility and the ability to perform actions on source servers, apps, and waves in different AWS accounts from a single console. [Learn more about global view.](#)
- Add new actions to the source server data replication process. You can now stop and start, pause and resume data replication, from the console. You can also install the AWS Replication Agent without immediately starting the data replication. [Learn more about data replication actions.](#)
- [AWS managed policy updates](#) – Updated the AWSApplicationMigrationServiceRolePolicy policy to support the global view feature.

May 2023

- Service launch in the following regions: AWS GovCloud (US-East) and AWS GovCloud (US-West).

April 2023

- [AWS managed policy updates](#) – Updated the AWSApplicationMigrationFullAccess policy to further support automation SSM documents.

March 2023

- Introduced **Import and export**, a new feature that allows you to import and export your source servers, applications, and waves from and to a CSV file. [Learn more about the import and export feature.](#)
- Added support for CentOS 5.5–5.11 and RHEL 5.5–5.11.
- Added support for migration of servers using the Oracle ASM Filter Driver.
- Introduced 8 new predefined post-launch actions:
 - [Conduct EC2 connectivity checks](#)
 - [Validate volume integrity](#)
 - [Verify process status](#)
 - [Convert MS-SQL license conversion](#)
 - [Install a CloudWatch Agent](#)
 - [Upgrade Windows](#)
 - [Create AMI from instance](#)
 - [Join Directory Service domain](#)

[Learn more about predefined post-launch actions.](#)

- Introduced major UI enhancements to the post-launch action feature. [Learn more about the new post-launch actions layout.](#)
- Enhanced the source server page dashboard, adding migration metrics view of the displayed servers.
- Service launch in the following regions: Middle East (UAE).
- [AWS managed policy updates](#) – Updated the AWSApplicationMigrationFullAccess policy, the AWSApplicationMigrationSSMAccess policy, and the AWSApplicationMigrationReadOnlyAccess policy.

January 2023

- [AWS managed policy updates](#) – Updated the AWSApplicationMigrationEC2Access policy.

November 2022

- Introduced support for Application management. [Learn more about Applications.](#)
- Introduced support for Wave management. [Learn more about Waves.](#)
- Added support for additional launch template options. [Learn more.](#)
- Added support for post-launch custom actions. [Learn more.](#)
- Added support for no rescan upon reboot for specific operating systems. [Learn more about the no-rescan feature.](#)
- The service onboarding process has been simplified. All initial templates: replication template, launch template, and post-launch template are initialized with defaults. The templates can be modified from the Settings page. [Learn more.](#)
- Added support for SUSE 11 operating system.
- [AWS managed policy updates](#) – added one new policy and updated two existing policies.
Application Migration Service AWS Application Migration Service AWS Application Migration Service

August 2022

- Added support for migration using [AWS Local Zones.](#)
- Service launch in the following region: Asia Pacific (Jakarta).
- Added additional instance families to the right-sizing mechanism. [Learn more.](#)

July 2022

- Added support for automatically tagging migrated resources with the required MAP program tags. [Learn more about automatic tagging.](#)

June 2022

- Added support for updating vCenter credentials for agentless replication. [Learn more about updating vCenter credentials for agentless replication.](#)
- Support for agent installation using temporary credentials. [Learn more about agent installation using temporary credentials.](#)

May 2022

- Added support for post-launch settings. Post-launch settings allow you to control and automate actions performed after the server has been launched in AWS. [Learn more about post-launch settings.](#)
- Added support for Linux SUSE SLES 12 service packs 1 and 2.

February 2022

- Added support for Microsoft Windows Server 2003, Microsoft Windows Server 2008, Microsoft Windows Server 2022, and Microsoft Windows 10.
- Added support for gp3 and io2 EBS volume types for replication servers.
- Added support for UEFI boot for Windows.

January 2022

- Added support for Kernel 5.15.

December 2021

- Added support for Kernels 5.8-5.14.

November 2021

- Service launch in the following regions: Europe (Paris), Europe (Milan), Middle East (Bahrain), and Africa (Cape Town).
- Application Migration Service now supports an additional replication method that does not require agent installation on each source server. This option is available for source servers running on VMware vCenter versions 6.7 and 7.0. [Learn more about agentless replication.](#)

October 2021

- Service launch in the following regions: Asia Pacific (Mumbai), Asia Pacific (Seoul), Asia Pacific (Hong Kong), Europe (London).

July 2021

- Service launch in the following regions: US West (N. California), South America (São Paulo), Canada (Central), Asia Pacific (Osaka).

April 2021

- Service initial launch in: US East (N. Virginia), US East (Ohio), US West (Oregon), Europe (Ireland), Europe (Frankfurt), Europe (Stockholm), Asia Pacific (Sydney), Asia Pacific (Singapore).

Document history for user guide

The following is the latest major policy updates for AWS Application Migration Service. We also update the documentation frequently to address the feedback that you send us.

For additional details regarding new features and major updates, [see the AWS MGN release notes](#).

Change	Description	Date
Updated AWS managed policy	Updated the AWSApplicationMigrationFullAccess policy to support SecureString parameter type in SSM Parameters Store for post-migration framework actions.	March 10, 2024
Updated AWS managed policy	Updated the AWSApplicationMigrationServiceEc2InstancePolicy to support MGN to GovCloud and added SID to statements in the managed policy.	December 28, 2023
Created AWS managed policy	Created the AWSApplicationMigrationServiceEc2InstancePolicy .	August 21, 2023
Updated AWS managed policy	Updated the AWSApplicationMigrationServiceRolePolicy policy to support the global view feature.	June 4, 2023
Updated AWS managed policy	Updated the AWSApplicationMigrationServiceRolePolicy policy	April 1, 2023

Change	Description	Date
	to support specific automation SSM documents.	
Updated AWS managed policy	Updated the AWSApplicationMigrationFullAccess policy to support both command and automation SSM documents for post-migration framework actions.	March 21, 2023
Updated AWS managed policy	Updated the AWSApplicationMigrationSSMAccess policy to support both command and automation SSM documents for the custom actions feature.	March 21, 2023
Updated AWS managed policy	Updated the AWSApplicationMigrationReadOnlyAccess policy to support the new import and export feature.	March 21, 2023
Updated AWS managed policy	Updated the AWSApplicationMigrationEC2Access policy to support: DescribeSnapshots, DescribeImages, DescribeVolumes.	January 29, 2023

AWS Glossary

For the latest AWS terminology, see the [AWS glossary](#) in the *AWS Glossary Reference*.