Application Migration Service

User Guide

Application Migration Service: User Guide

Copyright © 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
Document History ... 2
Getting Started ... 3
- Application Migration Service initialization and permissions ... 3
  - Initializing Application Migration Service ... 3
  - Additional Policies ... 3
  - Manually initializing Application Migration Service ... 4
- Accessing the Application Migration Service Console ... 5
- Supported AWS Regions ... 5
- MGN service quota limits ... 6
- Using the AWS Migration Hub with MGN ... 7
- MGN Technical Training Materials ... 8
- Using the Application Migration Service Console ... 9
  - Source Servers page ... 13
- Migration workflow ... 22
- Best Practices ... 22
  - Planning ... 22
  - Testing ... 22
  - Successful Implementation ... 22
  - Best Practices for Ensuring Project Success ... 23
- Quick start guide ... 23
  - First time setup ... 23
  - Adding source servers ... 29
  - Configuring launch settings ... 31
  - Launching a Test instance ... 34
  - Launching a Cutover instance ... 46

Settings ... 59
- Replication Settings ... 59
  - Replication Settings template vs individual server settings ... 59
  - Replication Server settings ... 66

Network Requirements ... 83
- Service architecture and network architecture overview ... 83
- Network setting preparations ... 85
  - Staging Area Subnet ... 85
  - Network requirements ... 85
  - Operational subnets ... 85
- Network requirements ... 85
  - Communication over TCP port 443 ... 86
  - Communication between the source servers and Application Migration Service over TCP port 443 ... 86
  - Communication between the Staging Area Subnet and Application Migration Service over TCP port 443 ... 88
  - Communication between the source servers and the Staging Area Subnet over TCP port 1500 ... 88

Source Servers ... 90
- Adding source servers ... 90
  - Installation requirements ... 91
  - AWS Replication Agent installation instructions ... 95
  - Supported operating systems ... 125
- Agentless snapshot based replication for vCenter source environments ... 127
  - Agentless replication overview ... 127
  - Prerequisites ... 130
  - VMware limitations ... 130
  - Generating vCenter Client IAM credentials ... 130
  - Installing the AWS MGN vCenter Client ... 137

Replicating servers from vCenter to AWS ... 142
Differentiating agentless and agent-based servers ... 143
Source Servers page ... 146
Interacting with the Source Servers page ... 148
Command menus ... 165
Filtering ... 200
Server details ... 203
Migration dashboard ... 208
Server info ... 271
Tags ... 273
Disk Settings ... 278
Replication Settings ... 282
Launch settings ... 284
Launching Test and Cutover instances ... 287
Preparing for Test and Cutover instance launch ... 287
Launch settings ... 287
General launch settings ... 290
EC2 Launch Template ... 295
Launching Test instances ... 312
Ready for testing indicators ... 313
Starting a Test ... 313
Reverting or Finalizing a Test ... 317
Launching Cutover instances ... 324
Ready for cutover indicators ... 325
Starting a Cutover ... 326
Reverting or Finalizing a Cutover ... 330
Launch History ... 337
Overview ... 339
Job Details ... 344
Monitoring Application Migration Service ... 351
Monitoring with CloudWatch ... 351
MGN and EventBridge ... 352
Event samples ... 352
Registering Event Rules ... 354
Logging Application Migration Service with AWS CloudTrail ... 355
AWS Application Migration Service information in CloudTrail ... 355
Understanding AWS Application Migration Service log file entries ... 356
Security ... 357
Overview ... 357
Identity and access management ... 358
Authenticating with identities ... 358
Grant permission to tag resources during creation ... 360
AWS managed policies ... 361
Managing access using policies ... 378
Using service-linked roles ... 381
Policy structure ... 388
Resilience ... 388
Infrastructure security ... 389
Compliance validation ... 390
Cross-service confused deputy prevention ... 390
Troubleshooting ... 392
Troubleshooting Launch Errors ... 392
Do I need to recreate the entire launch template for every version? ... 392
Error - AccessDeniedException - Must be admin user ... 393
VPCIdNotSpecified error ... 394
Troubleshooting Communication Errors ... 394

Solving Communication Problems over TCP Port 443 between the Staging Area and the Application Migration Service Service Manager ... 395
Calculating the Required Bandwidth for TCP Port 1500 ... 396
Verifying Communication over Port 1500 ... 396
Solving Communication Problems over Port 1500 ... 397
Troubleshooting Agent Issues ... 398
Error: Installation Failed ... 398
Troubleshooting agentless replication issues ... 403
Other Troubleshooting Topics ... 403
Windows License Activation - AWS ... 403
Migration Leaving Behind Replication Volumes after Cutover ... 404
Replication Lag Issues ... 404
Windows Driver Changes ... 404
Windows Dynamic Disk Troubleshooting ... 404
Deleting MGN Resources ... 404
FAQ ... 406
Application Migration Service Concepts ... 406
What is the Recovery Time Objective (RTO) of Application Migration Service? ... 406
What is the Recovery Point Objective (RPO) of Application Migration Service? ... 406
General Questions ... 406
Can Application Migration Service protect or migrate physical servers? ... 407
What data is stored on and transmitted through Application Migration Service servers? ... 407
What is the Recovery Time Objective (RTO) of Application Migration Service? ... 407
What is the Recovery Point Objective (RPO) of Application Migration Service? ... 407
What to consider when replicating Active Directory ... 407
Does Application Migration Service work with LVM and RAID configurations? ... 407
What is there to note regarding SAN/NAS Support? ... 407
Does Application Migration Service support Windows License Migration? ... 408
Can you perform an OS (Operating System) upgrade with Application Migration Service? ... 408
What are the MGN service quota limits? ... 408
What are the Private APIs used by MGN to define actions in the IAM Policy? ... 409
Which Post Launch scripts does MGN support? ... 410
Agent Related ... 411
What does the AWS Replication Agent do? ... 411
What kind of data is transferred between the Agent and the Application Migration Service Service Manager? ... 411
Can a proxy server be used between the source server and the Application Migration Service Console? ... 412
What are the pre-requisites needed to install the AWS Replication Agent? ... 412
What ports does the AWS Replication Agent utilize? ... 412
What kind of resources does the AWS Replication Agent utilize? ... 412
Can Application Migration Service migrate containers? ... 413
Does the AWS Replication Agent cache any data to disk? ... 413
How is communication between the AWS Replication Agent and the Application Migration Service Service Manager secured? ... 413
Is it possible to change the port the AWS Replication Agent utilizes from TCP Port 1500 to a different port? ... 413
How do I manually uninstall the Application Migration Service Agent from a server? ... 413
When do I need to reinstall the Agent? ... 413
How much bandwidth does the AWS Replication Agent consume? ... 414
How many disks can the AWS Replication Agent replicate? ... 414
Is it possible to add a disk to replication without a complete resync of any disks that have already been replicated? ... 414
Is the AWS Replication Agent installed on launched Test and Cutover instances? ... 414
Agentless replication related ... 414
In which situations would you recommend using agentless replication (snapshot shipping)? ... 415
In which situations would you recommend using agent-based replication? ... 415

How does agentless replication work? ... 415
Does agentless replication require installing any component in the customer's source data center? ... 415
Is the agentless feature available in all Regions that Application Migration Service (MGN) service supports? ... 415
Does agentless replication support the same source operating systems that are supported by agent-based replication? ... 416
Is the agentless feature supported in CloudEndure Migration? ... 416
Which virtualization environments are supported by the agentless feature? ... 416
On which operating systems can the MGN vCenter Client be installed? ... 416
Do I need to generate special credentials to install the MGN vCenter Client? ... 416
What are the agentless replication prerequisites? ... 416
How do I install the MGN vCenter Client? ... 416
Replication Related ... 417
What is the lifecylce of the snapshots and volumes automatically created during migration? ... 417
What do Lag and Backlog mean during replication? ... 417
Is the replicated data encrypted? ... 418
How is the Replication Server provisioned and managed in the Staging Area? ... 418
What type of Replication Server is utilized in the Application Migration Service Staging Area? ... 418
Does Application Migration Service compress data during replication? ... 418
Are events that are generated by the Application Migration Service servers logged in Cloudtrail in AWS? ... 418
How many snapshots does Application Migration Service create? ... 418
Does Application Migration Service Delete Snapshots? ... 418
How much capacity is allocated to the Staging Area? ... 418
Why is 0.0.0.0:1500 added to inbound rules in the Staging Area? ... 419
Can Application Migration Service replicate Oracle ASM? ... 419
How long does a rescan take? ... 419
Is Application Migration Service replication crash consistent? ... 419
AWS Related ... 419
What does the Application Migration Service Machine Conversion Server do? ... 420
How do I change the server AMI on AWS after Migration? ... 420
Which AWS services are automatically installed when launching a Test or Cutover instance? ... 420
How long does it take to copy a disk from the Application Migration Service Staging Area to production? ... 420
What are the differences between Conversion Servers and Replication Servers? ... 420
Can I prevent Application Migration Service from cleaning up Test instance resources in AWS? ... 421
Why are my Windows Server disks read-only after launching the Test or Cutover instance? ... 421
What impacts the conversion and boot time of Test and Cutover instances? ... 421
How is the AWS Licensing Model Tenancy chosen for Application Migration Service? ... 421
How does Application Migration Service interact with Interface VPC Endpoints? ... 422
How do I use MGN with CloudWatch and EventBridge dashboards? ... 422
Does MGN work with...? ... 426
Does MGN work with Microsoft Windows Failover Clustering? ... 426
Does MGN work with Bitlocker encryption ... 426
Release Notes ... 427
May 2022 ... 427
February 2022 ... 427
January 2022 ... 427
December 2021 ... 427
November 2021 ... 427
October 2021 ... 427
July 2021 ... 427
April 2021 ... 428
AWS glossary ... 429

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 enables 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.

Document History for User Guide

The following is the latest major documentation update for Application Migration Service. We also update the documentation frequently to address the feedback that you send us.

- **Latest major documentation update:** March, 2022

Getting Started with AWS Application Migration Service

Topics

- Application Migration Service initialization and permissions (p. 3)
- Accessing the Application Migration Service Console (p. 5)
- Supported AWS Regions (p. 5)
- MGN service quota limits (p. 6)
- Using the AWS Migration Hub with MGN (p. 7)
- MGN Technical Training Materials (p. 8)
- Using the Application Migration Service Console (p. 9)
- Migration workflow (p. 22)
- Best Practices (p. 22)
- Quick start guide (p. 23)

Application Migration Service initialization and permissions

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

Initializing Application Migration Service

Application Migration Service must be initialized upon first use from within the Application Migration Service Console. The initialization process occurs automatically once a user accesses the Application Migration Service Console. The user is directed to create the Replication Settings template, and upon saving the template, the service is initialized by creating the IAM Roles which are required for the service to work.

> **Important**
> Application Migration Service is **NOT** compatible with CloudEndure Migration

Application Migration Service can only be initialized by the Admin user of your AWS Account.

During initialization the following IAM roles will be created:

1. **AWSServiceRoleForApplicationMigrationService**
2. **AWSApplicationMigrationReplicationServerRole**
3. **AWSApplicationMigrationConversionServerRole**
4. **AWSApplicationMigrationMGHRole**

Learn more about Application Migration Service roles and managed policies (p. 361).

Additional Policies

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

- **AWSApplicationMigrationFullAccess** - This policy provides permissions to all public APIs of AWS Application Migration Service (MGN), as well as permissions to read KMS key information.
- **AWSApplicationMigrationEC2Access** - This policy allows Amazon EC2 operations required to use Application Migration Service (MGN) to launch the migrated servers as EC2 instances.
- **AWSApplicationMigrationReadOnlyAccess** - The Read-Only policy allows the user to view all data available in the Application Migration Service 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 (p. 95).

  You can find all of these policies in the IAM Console.

  > **Important**
  > You must attach the AWSApplicationMigrationFullAccess and the AWSApplicationMigrationEC2Access policies to your IAM users and roles in order to be able to launch Test and Cutover instances and to complete a full migration cycle with Application Migration Service.

Manually initializing Application Migration Service

You can manually initialize Application Migration Service through the API. This can help you automate service initialization through script when initializing multiple accounts.

> **Note**
> You will need to create the Replication Settings Template after initializing the service.

To initialize Application Migration Service manually:

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	Path	Trusted Entity
AWSApplicationMigrationReplicationServerRole	/service-role/	ec2.amazonaws.com
AWSApplicationMigrationConversionServerRole	/service-role/	ec2.amazonaws.com
AWSApplicationMigrationMGHRole	/service-role/	mgn.amazonaws.com

Example using the AWS CLI:

```
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.

1. Attach Managed Policy **AWSApplicationMigrationReplicationServerPolicy** to Role **AWSApplicationMigrationReplicationServerRole**
2. Attach Managed Policy **AWSApplicationMigrationConversionServerPolicy** to Role **AWSApplicationMigrationConversionServerRole**
3. Attach Managed Policy **AWSApplicationMigrationMGHAccess** to Role **AWSApplicationMigrationMGHRole**

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 Application Migration Service roles and managed policies (p. 361).

Accessing the Application Migration Service Console

You can access 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 Application Migration Service:

Region name	Region identity	Support in 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 (Mumbai)	ap-south-1	Yes
Asia Pacific (Osaka)	ap-northeast-3	Yes
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
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 (Ireland)	eu-west-1	Yes
Europe (London)	eu-west-2	Yes
Europe (Milan)	eu-south-1	Yes
Europe (Paris)	eu-west-3	Yes
Europe (Stockholm)	eu-north-1	Yes

Region name	Region identity	Support in Application Migration Service
Middle East (Bahrain)	me-south-1	Yes
South America (São Paulo)	sa-east-1	Yes

Learn more about AWS Regional services.

MGN service quota limits

The following are the 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: 20	The maximum number of servers that can be actively replicating at any time. You can increase this value to 60. Learn more about requesting a quota increase. For larger migrations, contact Support.
Max Non-Archived Source Servers	Each supported AWS Region: 4000	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".
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.

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 MGN service limits in the AWS General Reference

Using the AWS Migration Hub with MGN

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 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 MGN navigation menu.

Application Migration Service supports auto tagging in MGH. Migrated resources (Amazon EC2 instances or Amazon Machine Images (AMIs)) reported to Migration Hub by 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 MGN:

- AWS Application Migration Service - A Technical Introduction

Using the Application Migration Service Console

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

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

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

Each 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.

Application Migration Service
Source Servers
Launch history
Settings
Migration Hub
Documentation
Application Migration Servi
Replication Settin
Replication Servers
Subnet
Replication Server instar
t3.small
EBS volume type (for rep
Faster, General Purpose
Data routing and t
Use private IP for data r
Yes
Create public IP
Yes
Replication resourc
Key

Source Servers page

The Source Servers page lists all of the source servers you added to Application Migration Service and allows you to interact with your servers and perform a variety of actions. Learn more about the Source Servers page. (p. 146) (p. 90)

You can control your source servers within the Application Migration Service Console through the **Actions, Replication**, and **Test and Cutover** menus.

You can review the progress of all commands through the **Launch history** tab. Learn more about Launch history. (p. 337)

Application Migration Service
Source Servers
Launch history
Settings
Migration Hub
Documentation
Application Migration Servi
Launch history (28
Filter launch histor
Job ID
mgn-job0000000032-terminate-cutover
mgn-job0000000033-terminate-cutover
mgn-job0000000030-cutover
mgn-job0000000031-cutover
mgn-job0000000032-cutover

The commands within the **Actions, Replication**, and **Test and Cutover** 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.

You can use the **Filter source servers...** box to filter servers based on a variety of parameters.

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, 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 means that a command was completed successfully.

Example:

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

Example:

Each message shows details and links to supplemental information.

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 view 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 (p. 203).

Application Migration Service
Source servers
31: testing
31: testing (s-0000000031)
Next actions
Info
Complete testing and mark as 'Ready for cutover'
Migration dashboard
Server info
Tags
Disks setti
Lifecycle
Info
Not ready
Ready for testing
Test in progress
Launch status
Waiting
Last test
Job ID:
mgn-job00000
Started:
December 19,
(UTC+2:00)

Certain 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, Application Migration Service will indicate which servers are being edited.

Application Migration Service
Source Servers
Edit replication
Edit Replication Settings
Selected servers (5)
server1
server2
server3
server4
server5
Replication settings
Info
Replication servers
Replication Servers are EC2 instances that are launched in your AWS
automatically launched in the "staging area" subnet and discarded w
Server can serve multiple source servers.

In order for setting changes you have made in the Application Migration Service Console to take effect, you have to choose the **Save** option at the bottom of each settings page.

Migration workflow

The general process is:

1. Install the AWS Replication Agent on the source server.

   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. (p. 127)
2. Wait until Initial Sync is finished.
3. Launch Test instances.
4. Perform acceptance tests on the servers. After the Test instance is tested successfully, finalize the Test and delete the Test instance.
5. Wait for the Cutover window.
6. Confirm that there is no Lag.
7. Stop all operational services on the source server.
8. Launch a Cutover instance.
9. Confirm that the Cutover instance was launched successfully and then finalize the Cutover.
10. 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 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 a Application Migration Service SME.
2. Share project timelines with 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 Application Migration Service.
5. Coordinate Cutover windows with Application Migration Service in advance.

Quick start guide

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

Topics

- First time setup (p. 23)
- Adding source servers (p. 29)
- Configuring launch settings (p. 31)
- Launching a Test instance (p. 34)
- Launching a Cutover instance (p. 46)

First time setup

The first setup step for Application Migration Service is creating the Replication Settings template.

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

You will automatically be prompted to create the Replication Settings template the first time you log into Application Migration Service. This template will determine how data replication will work for each newly added source server.

> **Important**
> Prior to configuring your Replication Settings template, ensure that you meet the Network Requirements for running Application Migration Service (p. 83).

The replication settings configured in this template will be applied to 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. (p. 59)

Learn more about changing individual server and multiple server replication settings. (p. 59)

The Replication Settings template is made up of the following sections:

- **Replication Servers** - 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 start using Application Migration Service with the default Replication Server settings or you can configure your own settings.

Configurable Replication Server settings include:

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

- Data routing and throttling - Application Migration Service gives you multiple options to control how data is routed from your source servers to the Replication Servers on AWS. You can start using Application Migration Service with the default **Data routing and throttling** options or you can configure your own settings.

Configurable data routing and throttling settings include:

- Use Private IP
- Network data bandwidth throttling.

- Replication resource tags - Replication resource tags allow you to add custom Tags to your Application Migration Service resources.

Saving and editing Replication Settings

After you have configured your template, click the orange **Create template** button.

Your Replication Settings template will be saved and you'll be redirected into the Application Migration Service Console **Source Servers** page.

You can edit your Replication Settings template at any time by clicking on **Settings** in the left-hand navigation menu. You will be able to edit individual server replication settings after adding your source servers to Application Migration Service.

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

Adding source servers

Add source servers to 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. (p. 90)

> **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. (p. 127)

Prior to adding your source servers, ensure that you meet all of the Network requirements (p. 83).

The following is the MGN agent network architecture diagram:

Corporate data center / Any Cloud
Agent control protocols
AWS Replication Agent
Continuous, block-level data replication (compressed & encrypted)
AWS Replication Agent
Disks

Migration Lifecycle

After the source server has been added to 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 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 Application Migration Service.

Learn more about the Migration Lifecycle states. (p. 209)

Once the Initial Sync process has completed successfully, data replication will start automatically.

Configuring launch settings

After you have added your source servers to the 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.

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 edit your EC2 Launch Template.

Migration dashboard | Server info | Tags | Disks sett

General launch settings Info

Instance type right sizing

Off

Start instance upon launch

Yes

Copy private IP

No

EC2 Launch Template Info

Template ID

lt-2

Instance type

a1.2xlarge

EBS volumes

Volume 1 (80 GiB, EBS, General Purpose SSD (gp2))

Launch settings are composed of the following:

- **Instance type right-sizing** - The Instance type right-sizing feature allows Application Migration Service to launch a Test or Cutover instance type that best matches the hardware configuration of the source server. When enabled, 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 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.

Application Migration Service automatically creates an **EC2 Launch Template** for each new source server. 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. (p. 287)

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 enables 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**
> Windows source servers need to have at least 2 GB of free space to successfully launch a Test instance.

> **Note**
> 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**

Starting a Test

To launch a Test 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 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.

The **Launch test instances for X servers** dialog will appear. Choose **Launch** to begin the test.

The 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.

Launch job started
Launch job started for 1 server/s
Application Migration Service
Launch History
Job
Job: mgnjob-
Details
Type
Launch
Status
Started
Start time
11/5/2020, 1:45:00 PM
Completed time
-
Job log
Info
Filter job log by property or value
Time
Event
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. 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 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**.

The Application Migration Service Console will confirm that the servers were marked as ready for cutover.

The 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 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**.

Choose **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 enables 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, 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.

5. 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 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:

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.

   The **Revert cutover for X servers** dialog will appear. Choose **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 Application Migration Service Console will indicate **Cutover finalized** when the cutover has completed successfully.

The 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. The **Archive X server** dialog will appear. Choose **Archive**.

d. To see your archived servers, open the **Preferences** menu by choosing the gear button.

Toggle the **Show only archived servers** option and choose **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.

Settings

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 Settings template and how to set individual server Replication Settings.

You must configure the Replication Settings template upon first use of Application Migration Service. The Replication Settings 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 Settings template are automatically passed down to every server you add to Application Migration Service.

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

Topics

- Replication Settings (p. 59)

Replication Settings

Replication Settings determine how data will be replicated from your source servers to AWS. Your Replication Settings are governed by the Replication Settings template, which you must configure before adding your source servers to Application Migration Service. You can later edit the Replication Settings template 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 Application Migration Service.

In addition, you can control a variety of other source server settings through the **Settings** tab, including **Tags**.

Topics

- Replication Settings template vs individual server settings (p. 59)
- Replication Server settings (p. 66)

Replication Settings template vs individual server settings

The Replication Settings template determines how data replication will work for each new server you add to 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 Settings template upon your first use of Application Migration Service.

The configured replication settings can later 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 Settings template (p. 23)

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

This will open the **Replication settings template** view.

Choose **Edit template** 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 Application Migration Service.

To edit the settings for an individual server or group of servers, select the box to the left of each server name on the **Source Servers** page.

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

You will be redirected to the **Edit Replication Settings** tab.

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.

If you want to choose different settings for selected servers than those set in the Replication Settings template, edit these settings individually. Any setting that has not been changed is labeled with the **Do not change** option.

For any setting that you want to change, choose the setting option from the dropdown menu under each setting category.

Choose **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 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

Staging area subnet

Choose the **Staging area subnet** that you want to allocate as the Staging Area subnet for all of your Replication Servers.

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.

The Staging Area Subnet is the subnet within which Replication Servers subnet 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 best practice is to not change the default Replication Server instance type unless there is a business need for doing so.

By default, 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 to any type you wish. The dropdown 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.xl 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.

Note
By default, Replication Servers are automatically assigned a public IP address from Amazon's public IP space.

Dedicated instance for Replication Server

Choose whether you would like to use a **Dedicated instance for Replication Server**.

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 EC2 cost you incur during replication.

Amazon EBS volume type

Choose the default 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.

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. (p. 278)

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.

Choose whether to use the default Amazon EBS encryption Volume Encryption Key, or enter a custom customer-managed key (CMK) in the regular key ID format. If you choose the **Default** option, the default key is used (which can be an EBS-managed key or a CMK).

If the **Custom** option is chosen, 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, choose **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.

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 a customer managed KMS key

If you decide to use a customer-managed key, or if you default Amazon EBS encryption key is a CMK, you will need to add permissions in order to give the key Amazon EC2 access under the **Statement** field of your KMS key policy.

Navigate to the Key Management Service (KMS) Console and select the KMS key you plan to use with Application Migration Service.

Scroll to **Key policy** and click **Switch to policy view**.

Click **Edit** and add the following JSON under the **Statement** field.

Important
For the `kms:CallerAccount: "[account id]"` field, replace "account id" with your Account ID.

Important
For the `kms:ViaService: "ec2.[region_code].amazonaws.com"` field, replace "region_code" with the code of the region you are using.

```
{
            "Sid": "Allow access through EBS for all principals in the account that are
 authorized to use EBS",
            "Effect": "Allow",
            "Principal": {
                "AWS": "*"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:CreateGrant",
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:CallerAccount": "[account id]",
                    "kms:ViaService": "ec2.[region_code].amazonaws.com"
                }
            }
        }
```

Click **Save changes**.

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 best practice is to have Application Migration Service 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 enabled, Application Migration Service will constantly monitor whether the rules within this security group are enforced, in order to maintain uninterrupted data replication. If these rules are altered, Application Migration Service will automatically fix the issue.

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

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 drop-down list in the 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 Application Migration Service.

Data routing and throttling

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

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 Settings template view and the individual source serve 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.

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

Note
If you selected the Default subnet, it is highly unlikely that the Private IP is enabled for that Subnet. Ensure that Private IP (VPN, AWS Direct Connect, or VPC peering) is enabled for your chosen subnet if you wish to use this option.

Note
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.

Note
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).

Create public IP

When the **Use Private IP** option is chosen, you will have the option to create a public IP. Public IPs are enabled 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.

Throttle bandwidth

You can control the amount of network bandwidth used for data replication per server. By default, 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.**

If you chose to throttle bandwidth, then 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 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 Application Migration Service.

Choose **Add new tag** to add a new tag.

Enter a **custom tag key** and an optional tag value.

Note
You can add up to 40 tags.

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
- EBS volumes
- Snapshots
- Security groups (optional)

Learn more about AWS Tags in this EC2 article.

Saving and editing Replication Settings

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

Network requirements

Topics

- Service architecture and network architecture overview (p. 83)
- Network setting preparations (p. 85)
- Network requirements (p. 85)

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 MGN architecture.

The following is the MGN network diagram:

Corporate data center / Any Cloud
TCP 443
Control Protocols
Web Proxy
(Optional)
Local Network
AWS
Replication
Agent
AWS
Replication
Agent
TCP 1500
Data
Transfer

Network setting preparations

Topics

- Staging Area Subnet (p. 85)
- Network requirements (p. 85)
- Operational subnets (p. 85)

Staging Area Subnet

Before setting up Application Migration Service you should create a subnet which will be used by Application Migration Service as a staging area for data replicated from your source servers to AWS. You must specify this subnet in the Replication Settings template. You can override this subnet for specific source servers in the Replication Settings. 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. (p. 59)

Network requirements

The Replication Servers launched by Application Migration Service in your Staging Area Subnet need to be able to send data over TCP port 443 to the Application Migration Service 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 Application Migration Service'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” .

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 Application Migration Service.

Learn more about launching Test and Cutover instances (p. 34).

Learn more about how Amazon EC2 Launch Templates are used (p. 295).

Network requirements

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

> **Note**
> All communication is encrypted with TLS.

Topics

- Communication over TCP port 443 (p. 86)
- Communication between the source servers and Application Migration Service over TCP port 443 (p. 86)

- Communication between the Staging Area Subnet and Application Migration Service over TCP port 443 (p. 88)
- Communication between the source servers and the Staging Area Subnet over TCP port 1500 (p. 88)

Communication over TCP port 443

Add the following IP addresses and URLs to your firewall:

The Application Migration Service AWS Region-specific Console address:

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

Amazon S3 service URLs (required for downloading 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 Application Migration Service.
- The Staging Area Subnet should have access to S3.
- The following S3 buckets should be whitelisted:

```
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/
```

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 Application Migration Service.

2. Between the Staging Area Subnet and Application Migration Service.

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

Each source server that is added to Application Migration Service must continuously communicate with Application Migration Service (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 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 Application Migration Service Console (including hardware information, running services, installed applications and packages, etc.)
- 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 Application Migration Service

If there is no connection between your source servers and Application Migration Service, make sure that your corporate firewall enables connectivity from the source servers to Application Migration Service 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 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. Application Migration Service is not responsible for the update, validation or support of security and firewall information.

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

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 Application Migration Service over TCP port 443

The Replication Servers in the Staging Area Subnet must continuously communicate with Application Migration Service 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 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 Application Migration Service

You can establish communication between the Staging Area Subnet and 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 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 AreaSubnet and before it is written to the volumes.

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

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 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 Application Migration Service by reviewing the Supported Operating Systems documentation (p. 125).

In addition, Application Migration Service allows you to perform agentless snapshot replication (p. 127) 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. 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 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 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 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 (p. 90)
- Agentless snapshot based replication for vCenter source environments (p. 127)
- Source Servers page (p. 146)
- Server details (p. 203)

Adding source servers

Add source servers to 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 (p. 104)
- Windows installation instructions (p. 112)
- Agentless replication instructions (p. 127)

> **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 (p. 91)
- AWS Replication Agent installation instructions (p. 95)
- Supported operating systems (p. 125)

Installation requirements

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

Topics

- General requirements (p. 91)
- Source server requirements (p. 91)
- Linux installation requirements (p. 92)
- Windows installation requirements (p. 94)

General requirements

- Ensure that the source server operating system is supported by AWS. Learn more about supported operating systems. (p. 125)
- Ensure that your setup meets all networking requirements. Learn more about network requirements. (p. 83)
- 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. Application Migration Service calculates the unique ID of the source server from the MAC address. When a MAC address changes, Application Migration Service is no longer able to correctly identify the source server. Consequently, replication will stop. If this happens, you will need to re-install 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**
> Application Migration Service does not support paravirtualized source servers.
>
> **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: /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 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. (run yum install dhclient in CMD)
- 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.

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

   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-devel.

   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 linux-headers are not a symbolic link.

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/SUSE:
   sudo yum install kernel-devel-`uname -r`
   On Debian/Ubuntu:
   sudo apt-get install linux-headers-`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, Oracle, and SUSE package directory

   Debian package directory

   Ubuntu package directory

Windows installation requirements

Note
Ensure that your source server operating system is supported. Learn more about supported operating systems. (p. 125)

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

- At least 2 GB of free disk space on the root directory (/)

- At least 300 MB of free RAM

Learn more about AWS Replication Agent installation hardware requirements. (p. 91)

AWS Replication Agent installation instructions

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

Topics

- Generating the required AWS credentials (p. 95)
- Installation instructions (p. 103)
- Installing the Agent on a secured network (p. 122)
- Uninstalling the Agent (p. 122)
- Reinstalling the Agent (p. 124)

Generating the required AWS credentials

In order to install the AWS Replication Agent, you must first generate the required AWS credentials. You will need to create at least one AWS Identity and Access Management (IAM) user, and assign the proper permission policy 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.

> **Note**
> You can use the same credentials to install multiple Agents.

1. Open the **AWS Management Console** and look for **IAM** under **Find Services**.

aws
Services
AWS Management
AWS services
Find Services
You can enter names, keywords or acronyms.
IAM
IAM
Manage access to AWS resources
Recently visited services
IAM
EC2
Key Management Service
All services
Compute
EC2
Lightsail
Lambda
Batch
Feedback
English (US)

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. These steps show the path for adding a new user for Application Migration Service. Choose **Add user**.

4. Give the user a **User name** and select the **Programmatic access** access type. Choose **Next: Permissions**.

5. Choose the **Attach existing policies directly** option. Search for **AWSApplicationMigrationAgentPolicy**. Select the policy and choose **Next: Tags.** Learn more about the AWSApplicationMigrationAgentPolicy.

6. Add tags if you wish to use them. Tags are optional. These instructions do not include adding tags. Choose **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. The AWS Management Console will confirm that the user has been successfully created and will provide you with the **Access key ID** and **Secret access key** that you will need in order to install the AWS Replication Agent.

You need the Access key ID and secret access key in order to install the AWS Replication Agent on your source servers. You can save this information as .csv file by choosing the **Download .csv** option.

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, etc).

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 (p. 104)
- Windows (p. 112)

Linux

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

   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.

   > **Important**
   > 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.py.sha512` (replace <region> with the AWS Region into which you are replicating. Ex. us-east-1: https://aws-application-migration-service-hashes-us-east-1.s3.us-east-1.amazonaws.com/latest/linux/aws-replication-installer-init.py.sha512

   > **Note**
   > The Linux installer creates the "Application Migration Service" group and "Application Migration Service" 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 "Application Migration Service" user to "sudoers" .

   > **Note**
   > 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.py` . Replace `<region>` with the AWS Region into which you are replicating.

   > **Note**
   > You can generate a custom installation command through the **Add servers** prompt. Learn more about the Add servers prompt (p. 166).

2. 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 python3 aws-replication-installer-init.py
   ```

   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:

   - --region

This parameter specifies the AWS Region into which you are replicating. Enter the complete AWS Region name (for example: eu-central-1). You will be automatically prompted for this parameter after running the installer command in a standard installation.

- --aws-access-key-id

  This parameter specifies the AWS Access Key ID. Enter the full AWS Access Key ID that was previously generated (p. 95). You will be automatically prompted for this parameter after running the installer command in a standard installation.

- --aws-secret-access-key

  This parameter specifies the AWS Secret Access Key. Enter the full AWS Secret Access Key that was previously generated (p. 95). You will be automatically prompted for this parameter after running the installer command in a standard installation.

- --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 MGN. You cannot use the --tags flag to modify tags of source servers that have already been added to 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. (p. 122)

- --endpoint

  Use this parameter to specify the Private Link endpoint you created for Application Migration Service if you do not wish to open your firewall ports to access the default MGN endpoint. Learn more about installing the Agent on a blocked network. (p. 122)

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

```
[ec2-user@mgn-agent-sample ~]$ sudo python3 aws-replic
The installation of the AWS Replication Agent has star
```

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

```
[ec2-user@mgn-agent-sample ~]$ sudo python3 aws-replic
The installation of the AWS Replication Agent has star
AWS Region Name: us-east-1
AWS Access Key ID: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYE
```

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 python3 aws-replication-installer-init.py --region regionname --aws-access-key-id AKIAIOSFODNN7EXAMPLE --aws-secret-access-key wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)

Note

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

4. 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.

```
[ec2-user@mgn-agent-sample ~]$ sudo python3 aws-replic
The installation of the AWS Replication Agent has star
AWS Region Name: us-east-1
AWS Access Key ID: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYE
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are
To replicate some of the disks, type the path of the d
```

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, etc). To replicate all of the disks, press Enter. The installer will identify the selected disks and print their size.

```
[ec2-user@mgn-agent-sample ~]$ sudo python3 aws-replic
The installation of the AWS Replication Agent has star
AWS Region Name: us-east-1
AWS Access Key ID: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYE
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are
To replicate some of the disks, type the path of the d
Identified volume for replication: /dev/xvda of size 8
```

The installer will confirm that all disks were successfully identified.

```
[ec2-user@mgn-agent-sample ~]$ sudo python3 aws-repli
The installation of the AWS Replication Agent has sta
AWS Region Name: us-east-1
AWS Access Key ID: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCY
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks ar
To replicate some of the disks, type the path of the
Identified volume for replication: /dev/xvda of size
All volumes for replication were successfully identif
```

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 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.
- 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, Application Migration Service can no longer replicate them, so they are removed from the list of replicated disks. When they are re-connected, 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 this will also cause a resync. Perform a test after installing the Agent to ensure that the correct disks have been added.

5. 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.

```
[ec2-user@mgn-agent-sample ~]$ sudo python3 aws-repli
The installation of the AWS Replication Agent has sta
AWS Region Name: us-east-1
AWS Access Key ID: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCY
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks ar
To replicate some of the disks, type the path of the
Identified volume for replication: /dev/xvda of size
All volumes for replication were successfully identif
Downloading the AWS Replication Agent onto the source
Installing the AWS Replication Agent onto the source
```

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

```
[ec2-user@mgn-agent-sample ~]$ sudo python3 aws-replic
The installation of the AWS Replication Agent has star
AWS Region Name: us-east-1
AWS Access Key ID: AKIAIOSFODNN7EXAMPLE
AWS Secret Access Key: wJalrXUtnFEMI/K7MDENG/bPxRfiCYE
Identifying volumes for replication.
Choose the disks you want to replicate. Your disks are
To replicate some of the disks, type the path of the d
Identified volume for replication: /dev/xvda of size 8
All volumes for replication were successfully identif
Downloading the AWS Replication Agent onto the source
Installing the AWS Replication Agent onto the source s
Syncing the source server with the Application Migrati
The following is the source server ID: s-3146f90b19exa
The AWS Replication Agent was successfully installed.
[ec2-user@mgn-agent-sample ~]$
```

You can review this process in real time on the **Source Servers** page. Learn more about the initial sync process (p. 214).

Windows

1. Download the Agent installer (AWSReplicationWindowsInstaller.exe)**.** Copy or distribute the downloaded Agent installer to each Windows source server that you want to add to 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.

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

Important
We recommend using Windows PowerShell, which support ctrl+v pasting, and not Windows Command Prompt (cmd), which does not.

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.

Note
You can generate a custom installation command through the **Add servers** prompt. Learn more about the Add servers prompt (p. 166).

Note
Microsoft Windows Server versions 2003 and 2008 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 (p. 166) 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 (N. Virginia)	us-east-1	https://aws-application-migration-service-us-east-1.s3.us-east-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
US East (Ohio)	us-east-2	https://aws-application-migration-service-us-east-2.s3.us-east-2.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
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
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 (Tokyo)	ap-northeast-1	https://aws-application-migration-service-ap-northeast-1.s3.ap-northeast-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
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 (Osaka)	ap-northeast-3	https://aws-application-migration-service-ap-northeast-3.s3.ap-northeast-3.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

Region name	Region identity	Download Link
Asia Pacific (Mumbai)	ap-south-1	https://aws-application-migration-service-ap-south-1.s3.ap-south-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 (Stockholm)	eu-north-1	https://aws-application-migration-service-eu-north-1.s3.eu-north-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
EU (Milan)	eu-south-1	https://aws-application-migration-service-eu-south-1.s3.eu-south-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
Europe (Paris)	eu-west-3	https://aws-application-migration-service-eu-west-3.s3.eu-west-3.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
Canada (Central)	ca-central-1	https://aws-application-migration-service-ca-central-1.s3.ca-central-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

Region name	Region identity	Download Link
Middle East (Bahrain)	me-south-1	https://aws-application-migration-service-me-south-1.s3.me-south-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe
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
Africa (Cape Town)	af-south-1	https://aws-application-migration-service-af-south-1.s3.af-south-1.amazonaws.com/latest/windows/AwsReplicationWindowsInstaller.exe

2. 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** 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.

   Available parameters include:

   - --region

     This parameter specifies the AWS Region into which you are replicating. Enter the complete AWS Region name (for example: eu-central-1). You will be automatically prompted for this parameter after running the installer command in a standard installation.
   - --aws-access-key-id

     This parameter specifies the AWS Access Key ID. Enter the full AWS Access Key ID that was previously generated (p. 95). You will be automatically prompted for this parameter after running the installer command in a standard installation.
   - --aws-secret-access-key

     This parameter specifies the AWS Secret Access Key. Enter the full AWS Secret Access Key that was previously generated (p. 95). You will be automatically prompted for this parameter after running the installer command in a standard installation.
   - --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 MGN. You cannot use the --tags flag to modify tags of source servers that have already been added to 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. (p. 122)

- --endpoint

  Use this parameter to specify the Private Link endpoint you created for Application Migration Service if you do not wish to open your firewall ports to access the default MGN endpoint. Learn more about installing the Agent on a blocked network. (p. 122)

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

3. The installer will prompt you to enter your **AWS Region Name**, the **AWS Access Key ID** and the **AWS Secret Access Key** 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.

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 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`)

4. 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:, D:, etc). 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 al
l 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.

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 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.
- 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, Application Migration Service can no longer replicate them, so they are removed from the list of replicated disks. When they are re-connected, 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.

5. 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 al
l 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.
```

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

```
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 al
l 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 (p. 214).

Installing the Agent on a secured network

The Application Migration Service AWS Replication Agent installer needs network access to 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 enable private IP in the Replication Settings (p. 78).

Create a VPC Endpoint for Application Migration Service

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

Use the created VPC Endpoint for Application Migration Service

Once you have created the VPC Endpoint, the AWS Replication Agent can connect to 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 MGN via the endpoint over your VPN/DirectConnect connection.

Create a S3 Endpoint for Application Migration Service

To allow the AWS Replication Agent installer to communicate with S3, create an interface S3 endpoint for 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 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 MGN via the endpoint over your VPN/DirectConnect connection.

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 Application Migration Service Console.

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

Uninstalling the Agent through the Application Migration Service Console

To uninstall the AWS Replication Agent though the 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 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.

On the **Disconnect X server/s from service** dialog, choose **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. (p. 166)

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/stopAgent.sh
```

```
/var/lib/aws-replication-agent/install_agent --remove
```

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 (p. 104)
- Windows (p. 112)

Supported operating systems

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.

Windows notes

Note
It is recommended to install all available Windows updates on the server.

Note
Windows source servers need to have at least 2 GB of free disk space in order to launch a Test or Cutover instance successfully.

Note
The WMI service must be enabled to install the AWS Replication Agent.

Linux notes

Note
Application Migration Service does not support 32 bit versions of Linux.

Note
Ensure that you have Python installed on the source server (version 2.4+, version 3.0+) for Agent installation.

Note
Only servers using the GRUB bootloader are supported.

Note
Kernel versions earlier than 2.6.18-164 are not supported by AWS and Application Migration Service. Therefore, servers that run these kernel versions cannot be replicated by Application Migration Service.

Note
Secure Boot is not supported in Linux.

Note
Kernel version 4.9.256 is not supported. Agent installation will fail on servers that run this kernel version.

Note
MGN does not support the migration of servers using the Oracle ASM Filter Driver.

General notes

Note
Application Migration Service does not support paravirtualized source servers.

Note
Application Migration Service only supports x86 based operating systems.

Windows

The following Windows operating systems are supported:

- Microsoft Windows Server 2003 32 bit *See notes 9, 10 and 11 (p. 126).
- Microsoft Windows Server 2003 64 bit *See notes 9, 10 and 11 (p. 126).
- Microsoft Windows Server 2003 R2 32 bit *See notes 9, 10 and 11 (p. 126).
- Microsoft Windows Server 2003 R2 64 bit *See notes 9, 10 and 11 (p. 126).
- Microsoft Windows Server 2008 32 bit *See notes 9 and 10 (p. 126).
- Microsoft Windows Server 2008 64 bit *See notes 9, 10, and 12 (p. 126).
- Microsoft Windows Server 2008 R2 64 bit (patched) *See notes 3 and 6. (p. 126)
- Microsoft Windows Server 2012 64 bit *See note 6. (p. 126)
- Microsoft Windows Server 2012 R2 64 bit *See notes 3 and 6 (p. 126).
- Microsoft Windows Server 2016 64 bit *See notes 3 and 6 (p. 126).
- Microsoft Windows Server 2019 64 bit *See notes 3 and 6 (p. 126).
- Microsoft Windows Server 2022 64 bit *See notes 3 and 6 (p. 126).
- Microsoft Windows 10 64 bit*See notes 7 and 8 (p. 126).

Linux

The following Linux operating systems are supported:

- SUSE Linux (SLES) 12 and higher. *SP1 and higher.
- Debian Linux 9 and higher *See note 2 (p. 126).
- Ubuntu 12.04 and higher *See note 2 (p. 126).
- Red Hat Enterprise Linux (RHEL) 6.0 and higher *See notes 1, 3, 4 and 13. (p. 126)
- Oracle Linux 6.0 and higher *Oracle Linux 6.0+ running Unbreakable Enterprise Kernel Release 3 or higher or Red Hat Compatible Kernel only.
- CentOS 6.0 and higher *See notes 3, 4, and 13 (p. 126).
- CentOS 5.0 - Only supported for agentless replication from vCenter

Notes

Note 1: AWS requires that servers running Red Hat Enterprise Linux (RHEL) must have Cloud Access (BYOL) licenses in order to be copied to AWS.

Note 2: Only Kernel 3.x or above are supported for Debian/Ubuntu on AWS.

Note 3: Nitro instance types will work with RHEL 7.0+ or CentOS 7.0+ in a Linux environment and with Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and Windows 2022 in a Windows environment. This specific limitation does not apply to other instance type families.

Note 4: Kernel versions 2.6.32-71 are not supported in RHEL 6.0 and CentOS 6.0 on AWS.

Note 5: Kernel versions earlier than 2.6.18-164 are not supported by Application Migration Service. Therefore, servers that run these kernel versions cannot be replicated by Application Migration Service.

Note 6: Microsoft Windows Server versions 2008 R2 and above require .Net Framework version 4.5 or above to be installed by the end user.

Note 7: Windows 10 with BYOL licensing requires UEFI support and GPT boot. You must choose the **UEFI** option under **Boot Mode** in the Launch settings (p. 294).

Note 8: Ensure that the auto sleep function is disabled in Windows 10. Data replication may be interrupted if the feature is enabled.

Note 9: Microsoft Windows Server 2003 and 2008 have reached their end of life. We recommend that customers upgrade to more modern operating system versions.

Note 10: The AWS Replication Agent and agent installer uses a separate installer file (AwsReplicationWindowsLegacyInstaller.exe) for Microsoft Windows Server versions 2003 and 2008 because these OSs are using older versions of software components that cannot be upgraded due to the end-of-life status of Microsoft Windows Server 2003 and 2008.

Note 11: 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.

Note 12: Windows 2008 x64 requires SP2 and other Microsoft updates to support the SHA-2 signature of the AWS Replication Agent driver.

Note 13: A pre-requirement for installing the AWS Replication Agent on RHEL8 and CentOS 8 is first running the following:

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

Agentless snapshot based replication for vCenter source environments

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. 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 prevent you from installing the AWS Replication Agent on each individual server.

Agentless replication overview

Agentless snapshot based replication enables you to replicate Source Servers on your vCenter environment into AWS without installing the AWS Replication Agent.

In order to enable 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 MGN and is available for installation as a binary installer. The installation process will install services on the client VM which will allow MGN to remotely discover your VMs that are suitable for agentless replication, and to perform data replication between your vCenter environment and AWS though 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 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 MGN driver (that is used by the AWS Replication Agent)
- MGN Service
- MGN Console

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

AWS MGN Architecture - Agentless Replication
aws
Agent control protocols
Corporate data center
ESXi
VDDK
MGN
vCenter
Appliance
Guest 1
vCenter
Client
vCenter
Appliance
API
AWS
Replication
Agents
Snapshot
shipping
(compressed
& encrypted)
Guest 2

Prerequisites

1. Ensure that you have initialized Application Migration Service (p. 3).

VMware limitations

1. MGN supports VMC on AWS for agentless replication.
2. 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 MGN.
3. AWS does not provide support for migrating VMware Virtual Volumes.
4. 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.

1. Open the **AWS Management Console** and look for **IAM** under **Find Services**.

aws
Services
AWS Management
AWS services
Find Services
You can enter names, keywords or acronyms.
IAM
IAM
Manage access to AWS resources
Recently visited services
IAM
EC2
Key Management Service
All services
Compute
EC2
Lightsail
Lambda
Batch
Feedback
English (US)

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. These steps show the path for adding a new user for Application Migration Service. Choose **Add user**.

4. Give the user a **User name** and select the **Programmatic access** access type. Choose **Next: Permissions**.

5. Choose the **Attach existing policies directly** option. Search for **AWSApplicationMigrationVCenterClientPolicy** and **AWSApplicationMigrationAgentPolicy**. Select the policies and choose **Next: Tags.**

6. Add tags if you wish to use them. Tags are optional. These instructions do not include adding tags. Choose **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. The AWS Management Console will confirm that the user has been successfully created and will provide you with the **Access key ID** and **Secret access key** that you will need in order to install the AWS Replication Agent.

You need the Access key ID and secret access key in order to install the AWS Replication Agent on your source servers. You can save this information as .csv file by choosing the **Download .csv** option.

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, etc).

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 MGN.

MGN vCenter Client notes

Ensure that you review the notes below prior to installing the MGN vCenter Client. Once you have read the notes, proceed to install the client (p. 140).

vCenter Client requirement notes

Note
You must install the AWS MGN vCenter Client on a VM that has outbound and inbound network connectivity to the 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.

Note
The AWS MGN vCenter Client currently only supports VirtualDiskFlatVer2BackingInfo VMDK on CBT. Learn more about this in the VMware knowledgebase.

Note
You must download this VDDK version to the VM on which the AWS MGN vCenter Client is installed. VDDK 6.7 must be used, regardless of the vCenter version used.

Note
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

Note
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

Note
VMs that are being replicated into AWS should have at least 2 GiB of free disk space.

Note
The VM on which the AWS MGN vCenter Client is installed should not allow any incoming (ingress) traffic.

Note
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.

Note
Patching of guest OS running AWS vCenter client should be handled by the customer as part of shared responsibility.

Note
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 re-installing the AWS Replication Agent.

Note
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.

Note
Only a trusted administrator should have access to the VM on which the AWS MGN vCenter Client is installed.

Note
The AWS MGN vCenter Client should be located in an isolated and dedicated network and considered a sensitive segment.

Note
You can disable the vCenter Client auto-update mechanism by running the following command: `touch /var/lib/aws-vcenter-client/.disable_auto_updates` Once auto-updates are disabled, you will need to reinstall the client to perform a manual update. If you disable 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 (p. 140).

vCenter Client installer notes

Note
The AWS MGN vCenter Client installer only supports vCenter 6.7 and 7.x

Note
The AWS MGN vCenter Client installer can only be installed on 64 bit Ubuntu 18, RH8 or AL2 VMs.

Note
If you are using a RH8 environment, ensure that you run the `sudo yum install python3` command to install python prior to launching the client installer.

Note
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-secret-access-key AWS_SECRET_ACCESS_KEY]
[--region REGION]
[--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]

Note
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]

Note
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 requirement notes

Note
Application Migration Service supports VM hardware version 7 and higher with CBT enabled. Ensure that you upgrade any VMs you have to hardware version 7 or higher. Ensure that CBT support is enabled in your vSphere deployment. MGN enables CBT on replicating VMs. You can disable CBT after Cutover.

Note
The VM being replicated into MGN must not contain any existing VMware snapshots.

Note
Once added to MGN, snapshot-based replication will create snapshots on the replicated VM, which may result in slower disk performance.

Note
VMs with independent disks, Raw Device Mappings (RDM), or direct-attach disks (iSCSI, NBD) are not supported for replication into MGN.

Note
The VM being replicated into 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.

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` 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`

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 (ex. eu-west-1)
   - The Private Link endpoint for 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/lin/f7f2bd6e.0`)). Otherwise, press **Enter** to disable 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).

     Note
     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.

     Note
     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/vddk.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 Application Migration Service.

6. Once the AWS vCenter client has been installed, all of the VMs in your vCenter will be added to 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 MGN Console.

   Note
   The MGN vCenter Appliance is excluded from the discovered servers list.

Replicating servers from vCenter to AWS

Once you have successfully installed the AWS vCenter client, all of your vCenter VMs will be added to 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 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 (p. 312) and perform all other regular MGN operations on the server.

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 MGN Console identifies the replication type, whether it is through **Snapshot shipping** (agentless) or **Agent based**.

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.**

3. Similarly, in the Server details view, under the **Migration dashboard**, the **Data replication status** box will show the **Replication type** as **Snapshot shipping**.

Source Servers page

The **Source Servers** page lists all of the source servers that have been added to Application Migration Service. 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 Application Migration Service and you will most likely interact with Application Migration Service predominantly through this page.

Topics

- Interacting with the Source Servers page (p. 148)
- Command menus (p. 165)
- Filtering (p. 200)

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 (38)
Active source servers
Filter source ser
Source server name
11: not_ready (initiating)
12: not_ready (initiating) - had error
13/not_ready/initiating
14: not_ready (initial_sync)
15: not_ready (creating_snapshot)

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.

Application Migration Service
Source servers
Source servers (38)
Active source servers
Filter source se
Source server name
11: not_ready (initiating)
12: not_ready (initiating) - had error
13/not_ready/initiating
14: not_ready (initial_sync)
15: not_ready (creating_snapshot)

- **Source server name** - This column shows the unique server name for each source server.

Application Migration Service
Source servers
Source servers (38)
Active source servers
Filter source se
Source server name
11: not_ready (initiating)
12: not_ready (initiating) - had error
13/not_ready/initiating
14: not_ready (initial_sync)
15: not_ready (creating_snapshot)

- **Alerts** - This column shows whether any alerts exist for the server.

Application Migration Service
Source servers
Source servers (38)
Active source servers
Filter source se
Source server name
18: not_ready (stalled)
19/not_ready/stalled
25: ready_for_test (stalled)
26/ready_for_test/stalled

A healthy server for which a Test or Cutover instance has not been launched will not show any indicators.

A healthy server for which a Test of Cutover instance has been launched will show a blue **Launched** indicator.

A server that is experiencing a temporary issue such as lag or backlog will show a clock icon and a gray warning message.

A server that is experiencing significant issues, such as a stall, will show a red x and a red message.

- **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. (p. 127)

Application Migration Service
Source servers
Source servers (38)
Active source servers
Filter source se
Source server name
11: not_ready (initiating)
12: not_ready (initiating) - had error
13/not_ready/initiating
14: not_ready (initial_sync)
15: not_ready (creating_snapshot)

- **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 (p. 209) (p. 214).

Application Migration Service
Source servers
Source servers (38)
Active source servers
Filter source se
Source server name
48: disconnected
47: cutover
43: cutting_over
44: cutting_over
45/cutting_over/pending_snapshot_shipping
46/cutting_over/pending_snapshot_shipping
35: ready_for_cutover

  - **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.

Application Migration Service
Source servers
Source servers (38)
Active source servers
Filter source se
Source server name
48: disconnected
47: cutover
43: cutting_over
44: cutting_over
45/cutting_over/pending_snapshot_shipping
46/cutting_over/pending_snapshot_shipping
35: ready_for_cutover

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.

Application Migration Service
Source servers
Source servers (38)
Active source servers
Filter source se
Source server name
46/cutting_over/pending_snapshot_shipping
45/cutting_over/pending_snapshot_shipping
44: cutting_over
43: cutting_over
42/ready_for_cutover/shipping_snapshot
41/ready_for_cutover/shipping_snapshot

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 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, control data replication, and manage your testing and cutover for one or more source servers through the command menu buttons. Select one or more servers on the **Source Servers** page and choose the **Actions**, **Replication**, or **Test and Cutover** menu to control your source servers.

Topics

- Actions menu (p. 166)

- Replication menu (p. 184)
- Test and Cutover menu (p. 185)

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
construct the installation command, then copy the command and down

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

IAM secret access key

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

4. Download the installer onto your source server (or copy it the

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

To construct a custom installation command, first select your operating system. The installation command is different for Windows and Linux.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

Note

If you want to install the AWS Replication Agent on a legacy Windows OS (Windows Server 2003 or Windows Sever 2008), 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.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command
4. Download the installer onto your source server (or copy it there
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_legacy/AwsReplicationWindowsLegac
5. Copy and input the command below into the powershell command
AwsReplicationWindowsLegacyInstaller.exe --region eu-we

Next, 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.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there a
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_legacy/AwsReplicationWindowsLegacyI
5. Copy and input the command below into the powershell command li
AwsReplicationWindowsLegacyInstaller.exe --region eu-west

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.

Choose 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.

Next, enter the IAM access key ID and IAM secret access key you previously generated for AWS Replication Agent installation (p. 95). The form will not send the secret, but will add it to the installation command.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

If you have not yet created an IAM User for MGN, choose **Create User**. This option will redirect you to IAM where you can seamlessly create a new User.

Through this form, you can quickly create a new IAM User for AWS Replication Agent installation. Enter a unique name in the **IAM user name** field and choose **Go**.

This will open the IAM Console with all the requires options pre-selected, including the correct agent installation IAM policy. Follow the prompts in the IAM console to create the IAM User and then input the generated credentials into the agent installation prompt in the MGN console.

Add user

Review

Review your choices. After you create the user, you can view and downloa

User details

User name	mgn-agent-installer
AWS access type	Programmatic access - with an a
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AWSApplicationMigrationAgentPolicy

Tags

No tags were added.

Next, if you are adding a Windows source server to 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.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

Finally, 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 (p. 95).

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

- **View server details** - Choosing the **View server details** option will open the server details view for the selected server. This option is only available when a single server is selected.
- **Disconnect from service** - Choose the **Disconnect from service** 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 the **Mark as archived** 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 choose **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. (p. 59)
- **Start data replication** - To start data replication for a source server on which data replication has previously been stopped, reinstall the AWS Replication Agent on the server.
- **Stop data replication** - To stop data replication for a source server, open the Actions menu and choose **Disconnect from service**. This will uninstall the AWS Replication Agent from the source server and therefore stop data replication.
- **Pause data replication** - To pause data replication, stop the flow of data between the source server and Application Migration service by closing TCP port 1500 outbound on your firewall or by closing TCP port 1500 inbound in the Replication Server security group.
- **Resume data replication** - To resume data replication, undo the change you made to pause data replication (either re-open TCP port 1500 outbound on your firewall or open TCP port 1500 inbound in the Replication Server security group.

Test and Cutover menu

The Test and Cutover menu allows you to manage your Test and Cutover instances. You can see a more in-depth step-by-step guide to launching Test and Cutover instances in the Launching Test and Cutover instances documentation (p. 312).

- **Launch test instances**- Choose the **Launch test instances** option to launch a Test instance for this server.

The **Launch test instances for X** servers dialog will appear. Choose **Launch** to begin the test.

The Application Migration Service Console will indicate **1 launch job complete** after the test has been completed successfully.

- **Mark as Ready for cutover** - 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.

The **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**.

The 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 the **Revert to "ready for testing"** 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 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 the **Launch cutover instances** 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 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 the **Finalize cutover** 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 Application Migration Service Console will indicate **X servers cutover. Data replication has been stopped for servers** once the cutover has been completed successfully. The 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 the **Revert to "Ready for cutover"** 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. Choose **Revert**.

- **Edit launch settings** - Choose the **Edit launch settings** option to edit the launch settings for this server. This will redirect you to the **Launch settings** tab. Learn more about Launch settings. (p. 287)

- **Terminate launched instance** - Choose the **Terminate launched instance** 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.

The **Terminate launched instance** dialog will appear. Click **Terminate**.

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:

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.

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**.

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:

Topics

- Migration dashboard (p. 208)
- Server info (p. 271)

- Tags (p. 273)
- Disk Settings (p. 278)
- Replication Settings (p. 282)
- Launch settings (p. 284)

Migration dashboard

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 (p. 209)
- Data replication status (p. 229)
- Events and metrics (p. 232)
- Server actions and replication control (p. 233)

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 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 (p. 213)
- Ready for testing (p. 218)
- Test in progress (p. 219)
- Ready for cutover (p. 226)
- Cutover in progress (p. 227)
- Cutover complete (p. 228)

Not ready

The **Not ready** Lifecycle state represents several possible scenarios:

Topics

- Server undergoing Initial Sync (p. 214)
- Unable to complete initiation (p. 216)

Server undergoing Initial Sync

A source server that has been added to 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.

Here you can see 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 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".

Data replication status
Info
Initiating
Replication progress
0%
Total replicated storage
0 of 16 GiB
Lag
-
Backlog
1.54 GiB
Replication initiation steps
Create security groups
Launch Replication Server
Boot Replication Server
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
Last start time
3/25/2021, 11:34:32 AM
Next attempt time
-

You will have to 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 has been fixed.

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. You can review the test launch details by clicking on the **Job ID**.

This will open the job within the **Launch History** page in a new tab.

Application Migration Service > Launch history > Job: mgn-job00

Job: mgn-job0000000025-test

Details

Type	Status
Launch	Started
Start time	**Completed time**
3/24/2021, 11:36:32 AM	-

Job log Info

Filter job log by property or value

Time	Event
3/25/2021, 11:42:17 AM	Job started
3/25/2021, 11:43:17 AM	Cleanup started

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 tell that the Test instance was successfully launched through several indicators:

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 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**.

Data replication status

The **Data replication status** section provides an overview of the overall source server status, including:

- **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 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 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.

If there are initialization, replication, or connectivity errors, the **Data replication status** section will show the cause of the issue (for example, a stall).

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.**

Events and metrics

You can review Application Migration Service events and metrics in AWS CloudTrail. Click on **View CloudTrail Event** History to openAWS CloudTrail in a new tab.

Learn more about monitoring MGN. (p. 351)

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 (p. 233)
- Replication menu (p. 251)
- Test and Cutover menu (p. 251)
- Alerts and errors (p. 265)

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
construct the installation command, then copy the command and down

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

IAM secret access key

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

4. Download the installer onto your source server (or copy it ther

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

To construct a custom installation command, first select your operating system. The installation command is different for Windows and Linux.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

Note

If you want to install the AWS Replication Agent on a legacy Windows OS (Windows Server 2003 or Windows Sever 2008), 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.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command
4. Download the installer onto your source server (or copy it there
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_legacy/AwsReplicationWindowsLegac
5. Copy and input the command below into the powershell command
AwsReplicationWindowsLegacyInstaller.exe --region eu-we

Next, 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.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there a
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_legacy/AwsReplicationWindowsLegacyI
5. Copy and input the command below into the powershell command li
AwsReplicationWindowsLegacyInstaller.exe --region eu-west

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.

Choose 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.

Next, enter the IAM access key ID and IAM secret access key you previously generated for AWS Replication Agent installation (p. 95). The form will not send the secret, but will add it to the installation command.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

If you have not yet created an IAM User for MGN, choose **Create User**. This option will redirect you to IAM where you can seamlessly create a new User.

Through this form, you can quickly create a new IAM User for AWS Replication Agent installation. Enter a unique name in the **IAM user name** field and choose **Go**.

This will open the IAM Console with all the requires options pre-selected, including the correct agent installation IAM policy. Follow the prompts in the IAM console to create the IAM User and then input the generated credentials into the agent installation prompt in the MGN console.

Add user

Review

Review your choices. After you create the user, you can view and downloa

User details

User name	mgn-agent-installer
AWS access type	Programmatic access - with an a
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AWSApplicationMigrationAgentPolicy

Tags

No tags were added.

Next, if you are adding a Windows source server to 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.

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

Finally, 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 (p. 95).

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
IAM secret access key
This form does not send the secret – it only adds it to the installation command you
4. Download the installer onto your source server (or copy it there af
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.sha
5. Copy and input the command below into the powershell command lir
AwsReplicationWindowsInstaller.exe --region eu-west-1

- **View server details** - Choosing the **View server details** option will open the server details view for the selected server. This option is only available when a single server is selected.
- **Disconnect from service** - Choose the **Disconnect from service** 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 the **Mark as archived** 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 choose **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** - Choosing the **Edit replication settings** option will redirect you to the **Replication settings** tab, where you can edit specific replication settings for the selected source server. Learn more about editing replication settings. (p. 59)

Test and Cutover menu

The Test and Cutover menu allows you to manage your Test and Cutover instances.

- **Launch test instances**- Choose the **Launch test instances** option to launch a Test instance for this server.

The **Launch test instances for X** servers dialog will appear. Choose **Launch** to begin the test.

The 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.

The **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**.

The 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 the **Revert to "ready for testing"** 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 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 the **Launch cutover instances** 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 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 the **Finalize cutover** 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 Application Migration Service Console will indicate **X servers cutover. Data replication has been stopped for servers** once the cutover has been completed successfully. The 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 the **Revert to "Ready for cutover"** 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. Choose **Revert**.

- **Edit launch settings** - Choose the **Edit launch settings** option to edit the launch settings for this server. This will redirect you to the **Launch settings** tab. Learn more about Launch settings. (p. 287)

- **Terminate launched instance** - Choose the **Terminate launched instance** 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.

The **Terminate launched instance** dialog will appear. Click **Terminate**.

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 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:

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:

Rescanning server:

The **Next actions** box will detail the exact issue.

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.

The **Lifecycle** section will show a red indicator.

The **Data replication status** box will include details of the issue.

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".

Server info

The **Server info** tab shows a variety of general server information, hardware, and network information.

Migration dashboard
Server info
Tags
Disks sett
Server info Info
General information
Last updated
4/6/2020, 3:00:00 AM
Date added
3/23/2021, 11:36:32 AM
AWS ID
ARN
Hardware
CPUs
Model: model-1, Cores: 1
Model: model-8, Cores: 8

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 hint**s: 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 is 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. 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.

Choose **Manage tags** to add or remove tags.

The **Manage tags** page will open. Choose **Add new tag** to add a new tag.

Add a tag **Key** and an optional tag **Value**. Choose **Save** to save your added tags.

To remove a tag, choose **Remove** to the right of the tag you want to remove, and then choose **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 settings include:

- **Disk name**
- **Replicate disk** - Whether the disk is being replicated.
- **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**.

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 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).

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**
> 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 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).

Choose **Change** to confirm the change.

Replication Settings

The **Replication Settings** tab allows you to edit the Replication Settings for an individual source server.

Migration dashboard
Server info
Tags
Disks settings
Replication Settings
Info
Replication Servers
Subnet
Replication Server instance type
m5.xlarge
Use dedicated Replication Server
No
EBS
Defa
Defa
Use
Alwa
Yes
Addi
Data routing and throttling
Use private IP for data replication (VPN, DirectConnect or VPC peering)
No
Thro
No t

After the source server is added to 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 or multiple source servers through the **Replication Settings** tab.

Edit each setting as required and then choose **Save replication settings.**

Learn more about Replication Settings. (p. 59)

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.

Migration dashboard
Server info
Tags
Disks sett
General launch settings Info
Instance type right sizing
On
Start instance upon launch
Yes
Copy private IP
Yes (127.0.0.1)
EC2 Launch Template Info
Template ID
lt-1
Instance type
a1.2xlarge

Launch settings, including the EC2 launch template, are automatically created every time you add a server to 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. (p. 287)

Launching Test and Cutover instances

Application Migration Service 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. Application Migration Service 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. EC2 Launch Templates 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 Test and Cutover instance Launch settings, you can launch them directly through the Application Migration Service console. 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.

Topics

- Preparing for Test and Cutover instance launch (p. 287)
- Launch settings (p. 287)
- Launching Test instances (p. 312)
- Launching Cutover instances (p. 324)
- Launch History (p. 337)

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 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. Application Migration Service will automatically use the default Subnet and Security groups. Ensure 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 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 though the Application Migration Service Console.

> **Note**
> You can modify launch settings for multiple servers at a time by using the 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.

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

Migration dashboard
Server info
Tags
Disks sett
General launch settings
Info
Instance type right sizing
On
Start instance upon launch
Yes
Copy private IP
Yes (127.0.0.1)
EC2 Launch Template
Info
Template ID
lt-1
Instance type
a1.2xlarge

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 (p. 290)
- EC2 Launch Template (p. 295)

General launch settings

The **General launch settings** section allows you to control a variety of server-specific settings. Choose **Edit** to edit the general settings.

Make your changes and then choose **Save settings** to save your changes.

Launch Settings Info

EC2 Launch Template
lt-1

Instance type right sizing Info

Basic

Start instance upon launch Info

Yes

Copy private IP Info

Yes (127.0.0.1)

Changing this to "No" will not remove the copied IP from the EC2 Launch Template

Operating system licensing Info

BYOL

Windows BYOL is only allowed for EC2 Dedicated Hosts, or under special circumstances

Transfer server tags Info

Yes

Boot mode Info

Legacy BIOS

Topics

- Instance type right-sizing (p. 292)
- Start instance upon launching (p. 292)
- Copy Private IP (p. 293)
- Operating system licensing (p. 293)
- Transfer server tags (p. 294)
- Boot mode (p. 294)

Instance type right-sizing

The Instance type right-sizing feature allows Application Migration Service to launch a Test or Cutover instance type that best matches the hardware configuration of the source server.

If you select the **Basic** option, Application Migration Service will launch a Test or Cutover AWS instance type that best matches the OS, CPU, and RAM of your source server.

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 Application Migration Service when this feature is enabled will overwrite the instance type defined in your EC2 launch template.
>
> **Note**
> Hardware changes and the resulting AWS instance type change may take up to 90 minutes to be processed by Application Migration Service.

If you select the **None** option, 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 right-sizing instance type selected by Application Migration Service will show on the **Server details** tab.

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.

If you choose the **Yes** option, then the Test or Cutover AWS instance will be launched and started automatically upon Test or Cutover launch.

If you choose the **No**, then the instances will be launched in a stopped state and you will have to start the Test or Cutover AWS instance manually from the EC2 Console.

Copy Private IP

Choose whether you want 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.

Application Migration Service will monitor the source server on an hourly basis to identify the Private IP. Application Migration Service will use the private IP of the primary network interface.

The **No** option is chosen by default. Choose the **No** option if you do not want the private IP of the Test or Cutover instance to match that of the source machine.

Choose the **Yes** option if you want to use a Private IP. The IP will be shown in brackets next to the option.

> **Note**
> If you chose the **Yes** option, 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 share 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.

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 enable BYOL licensing for Windows, you have to change the **Placement.tenancy** type in the EC2 launch template to **Host**. Otherwise, instance launch will fail.

Transfer server tags

Choose whether you want Application Migration Service to transfer any user-configured custom tags from your source servers onto your Test or Cutover instance.

If you choose the **Yes** 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 Application Migration Service. These resources include:

- EC2 instances
- Conversion groups
- Security groups
- EBS volumes
- Snapshots

> **Note**
> Application Migration Service automatically adds system tags to all resources.

If you choose the **No** option, server tags will not be transferred. You can always add tags from the AWS 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

> **Important**
> This setting is only valid for Windows source servers

Choose the Windows boot mode for the Test or Cutover instance.

You can either choose the **Legacy BIOS** or the **UEFI** boot mode.

Note: When the BIOS option is chosen, 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 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

Application Migration Service 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 Application Migration Service upon the installation of the AWS Replication Agent.

Note
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.

Note
You cannot use the same template for multiple servers.

Note
The Launch template can only be edited from EC2.

Note
Many EC2 launch template settings can be changed, but some may not be used by the Application Migration Service launch process and some may interfere with the Application Migration Service launch process. Learn more about individual launch template settings. (p. 305)

Important
You must set the EC2 launch template you want to use with MGN as the **default** launch template.

Important
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 MGN instance launch will fail.

The Application Migration Service EC2 launch template panel shows a summary of the key template values; to view all the values or to change any of them, choose **Modify**.

On the **About modifying EC2 Launch Templates** dialog, choose **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.

EC2 > Launch templates > Modify template (Create new version)

Modify template (Create new versio

Modifying a template allows you to create a new template version from
manage templates in a structured and controlled way. It also allows you
rolling out updates to templates without having to change a reference t

Launch template name and version description

Launch template name

mgn-

Template version description

A prod webserver for MyApp

Max 255 chars

Auto Scaling guidance **Info**

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

☐ Provide guidance to help me set up a template that I can use wit

▶ **Source template**

Launch template contents

Specify the details of your launch template version below. Leaving a fiel
the launch template version.

Learn more about EC2 launch template settings and configuration options in this EC2 article.

Working with EC2 launch templates

Topics

- Selecting the default template (p. 301)
- Launch template cleanup and fixing (p. 303)
- Launch template key considerations (p. 303)
- Full launch template setting review (p. 305)
- Saving your EC2 launch template (p. 312)

Selecting the default template

Application Migration Service 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 dropdown 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 a good practice to delete versions of the Launch template that you no longer need.

To set the new version fo your launch template as the default, navigate back to the main **EC2 > Launch Templates** page. Choose your launch template by selecting the toggle to the left of the **Launch template ID**. Open the Actions menu and choose **Set default version**.

Select the **Template version** from the drop-down menu and then choose **Set as default version.**

The EC2 Console will confirm the version change.

Launch template cleanup and fixing

Application Migration Service 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 (p. 305) before creating your launch template.

1. **Instance Type** - Ensure that you select an instance type that matches the hardware requirements of your source server. Application Migration Service always utilizes the instance type that is set on the EC2 launch template unless the **Instance right-sizing** feature is enabled.

> **Note**
> If you change your instance type and do not disable to the Instance right-sizing feature, then 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 disable 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 enable 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 enable 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** - Ensure that you disable 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 postboot script.

   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** - 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. 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 Application Migration Service.
10. **Launch template name** - Do not alter this field. 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 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** - Do not remove a volume from the EC2 launch template. If you remove a volume, MGN will launch the instance with the default values for the volume.

    > **Note**
    > If you wish to set a KMS key, you should do so through the EBS Encryption (p. 72)section of the Replication Settings within the 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 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 Application Migration Service. If the AMI is not configured properly (licensing, flags, etc), 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 Application Migration Service.

- **Key pair (login)** - Do **NOT** alter this field. Do not include a key pair with the launch template.

- **Networking platform** - Ensure that you select **Virtual Private Cloud (VPC)**. **EC2-Classic** 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. Each disk is composed of the following fields:
  - **Volume 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. Application Migration Service automatically sets **Provisioned IOPS SSD (io1)** as the default. We recommend not changing the volume type for test instances, as the io1 volume ensures that tests are performed as quickly as possible. You may want to change the volume type for cutover 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 guidelines. For Provisioned IOPS SSD volumes, you can provision up to 50 IOPS per GiB for io1, and 500 IOPS per Gib for io2. For General Purpose SSD volumes, baseline performance is 3 IOPS per GiB, with a minimum of 100 IOPS and a maximum of 16000 IOPS. General purpose SSD volumes under 1000 GiB can burst up to 3000 IOPS.
  - **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, 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 MGN Console or tags manually assigned to the server.

- **Network interfaces** - The network interface is created by default based on your Replication Settings Template. The network interface section is composed of the following fields:
  - **Device index** - Do **NOT** change or edit this field. The value should alwasys 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.
  - **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. 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 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, which will accrue additional costs if not connected to a running instance.
- **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 postboot script.

Network interfaces Info
Network interface 1
Device index Info
0
Network interface Info
Don't include in launch tem..
Subnet Info
subnet-
IP addresses available: 4087
Auto-assign public IP Info
Enable
Secondary IP Info
123.123.123.1
Add IP
IPv6 IPs Info
2001:0db8:85a3:0000:0000:
Add IP
Delete on termination Info
Yes
Elastic Fabric Adapter Info
Enable
EFA is only compatible with certain
types.
Add network interface

- **Advanced details** - In this section, we will focus on the fields you should **NOT** change or edit in order to 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 enables 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**
> Windows source servers need to have at least 2 GB of free space to successfully launch a Test instance.

> **Note**
> 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 (p. 313)
- Starting a Test (p. 313)
- Reverting or Finalizing a Test (p. 317)

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, 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.

The **Launch test instances for X servers** dialog will appear. Choose **Launch** to begin the test.

The 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.

Launch job started
Launch job started for 1 server/s
Application Migration Service
Launch History
Job
Job: mgnjob-
Details
Type
Launch
Status
Started
Start time
11/5/2020, 1:45:00 PM
Completed time
-
Job log
Info
Filter job log by property or value
Time
Event
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.

Topics

- Reverting a Test (p. 317)
- Marking as Ready for cutover (p. 319)

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 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**.

The Application Migration Service Console will confirm that the servers were marked as ready for cutover.

The 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 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**.

Choose **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 enables 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, 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 (p. 325)
- Starting a Cutover (p. 326)
- Reverting or Finalizing a Cutover (p. 330)

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.

5. 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 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:

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.

   The **Revert cutover for X servers** dialog will appear. Choose **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 Application Migration Service Console will indicate **Cutover finalized** when the cutover has completed successfully.

The 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. The **Archive X server** dialog will appear. Choose **Archive**.

d. To see your archived servers, open the **Preferences** menu by choosing the gear button.

Toggle the **Show only archived servers** option and choose **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 Application Migration Service.

You can access the Launch History by choose **Launch History** on the left-hand navigation menu.

aws
Services
Search for services, features, marketplace
Application Migration Service
Source Servers
Launch history
Settings
Migration Hub
Documentation
Application Migration Servi
Launch history (28
Filter launch histor
Job ID
mgn-job0000000032-terminate-cutover
mgn-job0000000033-terminate-cutover
mgn-job0000000030-cutover
mgn-job0000000031-cutover
mgn-job0000000032-cutover
Feedback
English (US)

Topics

- Overview (p. 339)
- Job Details (p. 344)

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 (ex. 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 (ex. 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)

Application Migration Service > Launch history

Launch history (28)

Filter launch history by property or value

Job ID	Job type	Initiated by	Statu
mgn-job0000000032-terminate-cutover	Terminate	Terminate launched instances	Com
mgn-job0000000033-terminate-cutover	Terminate	Terminate launched instances	Com
mgn-job0000000030-cutover	Launch	Launch cutover instances	Start
mgn-job0000000031-cutover	Launch	Launch cutover instances	Start
mgn-job0000000032-cutover	Launch	Launch cutover instances	Com

You can sort the Launch History by any column by clicking the column header. (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

"cutover" ✕ | Clear filters

Job ID	Job type	Initiated by	Statu
mgn-job0000000033-terminate-cutover	Terminate	Terminate launched instances	Comp
mgn-job0000000033-cutover	Launch	Launch cutover instances	Comp
mgn-job0000000032-terminate-cutover	Terminate	Terminate launched instances	Comp
mgn-job0000000032-cutover	Launch	Launch cutover instances	Comp
mgn-job0000000031	Launch	Launch cutover	Starte

Job Details

You can view a detailed breakdown of each individual job by choosing the Job ID. Choose the **Job ID** of any Job to open the Job details view.

The Job details view is composed of three sections:

Topics

- Details (p. 344)
- Job log (p. 345)
- Jobs - Source servers (p. 349)

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**.

Job log

The Job log section shows a detailed log of all of the operations performed during the Job.

You can use this section to troubleshoot any potential issues and determine in which step of the launch process they occurred.

You can 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. (ex. Job log filtered by **Event: Failed to take snapshot** and a specific **Source Server Id: 7**)

Jobs - Source servers

The Source servers section shows a list of all source servers involved in the Job and their status.

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 (p. 203)

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 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 enables 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* enables 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.

Metric name	Description
`TotalSourceServerCount`	Number of source servers, including those that are archived.

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?

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 (p. 352)
- MGN Source server lifecycle state change (p. 353)
- MGN Source server data replication stalled change (p. 353)

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 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 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 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 enable 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 enabled 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* enables 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 enables 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": "AAAAAAAAAAAAAAAAAAA",
        "arn": "arn:aws:sts::1234567890:assumed-role/Admin/user-Isengard",
        "accountId": "1234567890",
        "accessKeyId": "BBBBBBBBBBBBBBBBBBBB",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AAAAAAAAAAAAAAAAAAA",
                "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 Application Migration Service

Topics

- Overview (p. 357)
- Identity and access management for Application Migration Service (p. 358)
- Resilience in Application Migration Service (p. 388)
- Infrastructure security in Application Migration Service (p. 389)
- Compliance validation for Application Migration Service (p. 390)
- Cross-service confused deputy prevention (p. 390)

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 Application Migration Service (Application Migration Service), 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 Application Migration Service. It shows you how to configure 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 Application Migration Service resources.

The customer is responsible for making sure that no mis-configurations are present during and after the migration process, including:

1. The replication server should be accessed only from the CIDR range of the source servers. Proper security groups rules should be assigned to the replication server after it is created.
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 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, IAM users don't have permissions for Application Migration Service (Application Migration Service) resources and operations. To allow IAM users to manage Application Migration Service resources, you must create an IAM policy that explicitly grants them permissions, and attach the policy to the IAM 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.

Authenticating with identities in Application Migration Service

Authentication is how you sign in to AWS using your identity credentials. For more information about signing in using the AWS Management Console, see Signing in to the AWS Management Console as an IAM user or root user in the *IAM User Guide*.

You must be *authenticated* (signed in to AWS) as the AWS account root user, an IAM user, or by assuming an IAM role. You can also use your company's single sign-on authentication or even sign in using Google or Facebook. In these cases, your administrator previously set up identity federation using IAM roles. When you access AWS using credentials from another company, you are assuming a role indirectly.

To sign in directly to the AWS Management Console, use your password with your root user email address or your IAM user name. You can access AWS programmatically using your root user or IAM users access keys. AWS provides SDK and command line tools to cryptographically sign your request using your credentials. If you don't use AWS tools, you must sign the request yourself. Do this using *Signature Version 4*, a protocol for authenticating inbound API requests. For more information about authenticating requests, see Signature Version 4 signing process in the *AWS General Reference*.

Regardless of the authentication method that you use, you might also 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 Using multi-factor authentication (MFA) in AWS in the *IAM User Guide*.

AWS account root user

When you first create an AWS account, you begin with a single 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 do not use the root user for your everyday tasks, even the administrative ones. Instead, adhere to the best practice of using the root user only to create your first IAM user. Then securely lock away the root user credentials and use them to perform only a few account and service management tasks.

IAM users and groups

An *IAM user* is an identity within your AWS account that has specific permissions for a single person or application. An IAM user can have long-term credentials such as a user name and password or a set of access keys. To learn how to generate access keys, see Managing access keys for IAM users in the *IAM User Guide*. When you generate access keys for an IAM user, make sure you view and securely save the key pair. You cannot recover the secret access key in the future. Instead, you must generate a new access key pair.

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:

- **Temporary IAM user permissions** – An IAM user can assume an IAM role to temporarily take on different permissions for a specific task.
- **Federated user access** – Instead of creating an IAM user, you can use existing identities from AWS Directory Service, your enterprise user directory, or a web identity provider. These are known as *federated users*. AWS assigns a role to a federated user when access is requested through an identity provider. For more information about federated users, see Federated users and roles in the *IAM User Guide*.
- **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 How IAM roles differ from resource-based policies 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.
  - **Principal permissions** – When you use an IAM user or role to perform actions in AWS, you are considered a principal. Policies grant permissions to a principal. When you use some services, you might perform an action that then triggers another action in a different service. In this case, you must have permissions to perform both actions. To see whether an action requires additional dependent actions in a policy, see in the *Service Authorization Reference*.
  - **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 IAM 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: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 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*. MGN read-only permissions are included in the general IAM ReadOnlyAccess policy.

Topics

- AWS managed policy: AWSApplicationMigrationServiceRolePolicy (p. 362)
- AWS managed policy: AWSApplicationMigrationConversionServerPolicy (p. 366)
- AWS managed policy: AWSApplicationMigrationReplicationServerPolicy (p. 367)
- AWS managed policy: AWSApplicationMigrationAgentPolicy (p. 368)
- AWS managed policy: AWSApplicationMigrationMGHAccess (p. 369)
- AWS managed policy: AWSApplicationMigrationFullAccess (p. 370)
- AWS managed policy: AWSApplicationMigrationEC2Access (p. 371)
- AWS managed policy: AWSApplicationMigrationReadOnlyAccess (p. 376)

- AWS managed policy: AWSApplicationMigrationVCenterClientPolicy (p. 376)
- MGN updates for AWS managed policies (p. 377)

AWS managed policy: AWSApplicationMigrationServiceRolePolicy

This policy is attached to the Application Migration Service Service Linked role (SLR). Learn more. (p. 381)

This policy allows 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": [
     "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 Application Migration Service Conversion server's instance role.

This policy allows the Application Migration Service (MGN) Conversion Server, which are EC2 instances launched by Application Migration Service, to communicate with the MGN service. An IAM role with this policy is attached (as an EC2 Instance Profile) by MGN to the MGN Conversion Servers, which are automatically launched and terminated by MGN, when needed. We do not recommend that you attach this policy to your IAM users or roles. MGN Conversion Servers are used by Application Migratino Service when users choose to launch Test or Cutover instances using the 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 Application Migration Service Replication server's instance role.

This policy allows the Application Migration Service (MGN) Replication Servers, which are EC2 instances launched by Application Migration Service - to communicate with the 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 Application Migration Service to the MGN Replication Servers which are automatically launched and terminated by MGN, as needed. MGN Replication Servers are used to facilitate data replication from your external servers to AWS, as part of the migration process managed using MGN. We do not recommend that you attach this policy to your IAM 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 (MGN) to migrate external servers to AWS. Attach this policy to your IAM users or roles 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: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 (MGN) to send meta-data about the progress of servers being migrated using MGN to AWS Migration Hub (MGH). 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 IAM users or roles. Migration-progress data is only sent after the AWS "home region" is set in MGH; if the Home AWS Region is different then the AWS Region into which a server is being migrated, this data will be sent cross-region; to stop MGN from sending this meta-data to MGH, detach it from your IAM 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 (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 IAM users or roles.

Permissions details

This policy includes the following permissions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "mgn:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "kms:ListAliases",
                "kms:DescribeKey"
            ],
            "Resource": "*"
        },
        {
            "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": "*"
        },
        {
            "Effect": "Allow",
            "Action": "license-manager:ListLicenseConfigurations",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "elasticloadbalancing:DescribeLoadBalancers",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:ListInstanceProfiles",
            "Resource": "*"
        }
    ]
}
```

AWS managed policy: AWSApplicationMigrationEC2Access

You can attach the `AWSApplicationMigrationEC2Access` policy to your IAM identities.

This policy allows Amazon EC2 operations required to use Application Migration Service (MGN) to launch the migrated servers as EC2 instances. Attach this policy to your IAM 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:CreateLaunchTemplateVersion",
                "ec2:ModifyLaunchTemplate",
                "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"
                },
                "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/*"
        ],
        "Condition": {
            "StringEquals": {
                "ec2:CreateAction": [
                    "CreateSecurityGroup",
                    "CreateVolume",
                    "CreateSnapshot",
                    "RunInstances"
                ]
            },
            "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"
            }
        }
```

```
        }
    ]
}
```

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 Application Migration Service (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 MGN console. Attach this policy to your IAM 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"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplateVersions",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets"
      ],
      "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 (MGN) to migrate external servers to AWS. Attach this policy to your IAM 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/*"
  }
 ]
}
```

MGN updates for AWS managed policies

View details about updates to AWS managed policies for MGN since March 1, 2021.

Change	Description	Date
AWSApplicationMigrationEC2Access (p. 331) - Updated policy	Updated the AWSApplicationMigrationEC2Access policy to add additional permissions and restrict certain existing permissions. This policy is only intended to be used for the MGN console. The restriction prevents certain requests from being called directly by the calling identity, whilst enabling an AWS service (MGN) to make the request to EC2 on behalf of the calling identity.	March 2, 2021
AWSApplicationMigrationFullAccess (p.) Updated policy	Updated the AWSApplicationMigrationFullAccess policy to include EC2 permissions.	February 13, 2022
AWSApplicationMigrationServiceRolePolicy (p.) Updated policy	MGN added a new policy to allow Application Migration	December 15, 2021

Change	Description	Date
	Service to manage AWS resources on your behalf.	
AWSApplicationMigrationVCenterCMGNPolicy (p) New policy	MGN added a new policy that allows the installation and usage of the AWS vCenter Appliance.	Novermber 7, 2021
AWSApplicationMigrationReadOnlyAccess (p) Updated policy	MGN added a new policy. This policy provides permissions to all read-only public APIs of Application Migration Service (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 MGN console. Attach this policy to your IAM users or roles.	November 7, 2021
AWSApplicationMigrationFullAccess (p) Updated policy	Updated the AWSApplicationMigrationFullAccess policy to include missing IAM permissions.	July 19, 2021
AWSApplicationMigrationAgentPolicy (p) New policy	MGN added a new policy to allow the installation of the AWS Replication Agent on source servers.	April 18, 2021
AWSApplicationMigrationConversionServerPolicy (p) New policy	MGN added a new policy that allows Application Migration Service to communicate with the service.	April 18, 2021
AWSApplicationMigrationMGHAccessPolicy (p) New policy	MGN added a new policy to allow Application Migration Service access to your account's AWS Migration Hub	April 18, 2021
AWSApplicationMigrationReplicationServerPolicy (p) New policy	MGN added a new policy to allow the Application Migration Service Replication Servers to communicate with the service, create and manage resources on your behalf.	April 7, 2021
MGN started tracking changes	MGN 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 IAM identities or AWS resources. A policy is an object in AWS that, when associated with an identity or resource, defines their permissions. You can sign in as the root user or an IAM user, or you can assume an IAM role. When you then make a request, AWS evaluates the related identity-based or resource-based policies. 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**.

Every IAM entity (user or role) starts with no permissions. In other words, by default, users can do nothing, not even change their own password. To give a user permission to do something, an administrator must attach a permissions policy to a user. Or the administrator can add the user to a group that has the intended permissions. When an administrator gives permissions to a group, all users in that group are granted those permissions.

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 an IAM 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, IAM users and roles don't have permission to create or modify 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 IAM users or groups that require those permissions. To learn how to attach policies to an IAM user or group, see Adding and removing IAM identity permissions in the IAM User Guide. 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 MGN (p. 379)
- Full Access (p. 380)
- Read-Only Policy (p. 380)

Customer Managed Policies in MGN

You can create your own custom IAM policies to allow permissions for Application Migration Service actions and resources. You can attach these custom policies to the IAM users, roles, or groups that require those permissions. You can also create your own custom IAM policies for integration between Application Migration Service and other AWS services. The following example IAM policies grant permissions for various Application Migration Service actions. Use them to limit Application Migration Service access for your IAM users and roles.

Full Access

The following policy grants full access to all MGN and EC2 resources needed to initialize the service, replicate servers, launch servers in AWS, and perform all required MGN actions. 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

Read-Only Policy

The Read-Only policy allows a user to read from Application Migration Service and 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

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 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 Application Migration Service

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 Application Migration Service. Service-linked roles are predefined by 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 Application Migration Service easier because you don’t have to manually add the necessary permissions. Application Migration Service defines the permissions of its service-linked roles, and unless defined otherwise, only 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 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 Application Migration Service

Application Migration Service uses the service-linked role named **AWSServiceRoleForApplicationMigrationService**. This is a managed IAM policy with scoped permissions that MGN 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 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": [
  "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 Application Migration Service

You don't need to manually create a service-linked role. When you configure the Replication Configuration Template for 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 Application Migration Service 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 Application Migration Service

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 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 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 Application Migration Service resources used by AWSServiceRoleforApplicationMigrationService

Resources can be cleaned up without stopping any Application Migration Service services. Cleaning up Application Migration Service resources will cause 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 Application Migration Service service-linked roles

Application Migration Service supports using service-linked roles in all of the AWS Regions where the service is available.

Application Migration Service does not support using service-linked roles in every Region where the service is available. You can use the AWSServiceRoleForApplicationMigrationService role in the following Regions.

Region name	Region identity	Support in 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 (Mumbai)	ap-south-1	Yes
Asia Pacific (Osaka)	ap-northeast-3	Yes
Asia Pacific (Seoul)	ap-northeast-2	Yes
Asia Pacific (Singapore)	ap-southeast-1	Yes
Asia Pacific (Sydney)	ap-southeast-2	Yes
Asia Pacific (Tokyo)	ap-northeast-1	Yes

Region name	Region identity	Support in Application Migration Service
Canada (Central)	ca-central-1	Yes
Europe (Frankfurt)	eu-central-1	Yes
Europe (Ireland)	eu-west-1	Yes
Europe (London)	eu-west-2	Yes
Europe (Milan)	eu-south-1	Yes
Europe (Paris)	eu-west-3	Yes
Europe (Stockholm)	eu-north-1	Yes
Middle East (Bahrain)	me-south-1	Yes
South America (São Paulo)	sa-east-1	Yes

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 Application Migration Service API action for which you are granting or denying permission.
- **Resource**: The resource that's affected by the action. For 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 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 Application Migration Service

As a managed service, 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 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 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.)

Additionally, requests must be signed using an access key ID and a secret access key that is associated with an IAM principal. Or you can use the AWS Security Token Service (AWS STS) to generate temporary security credentials to sign requests.

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. 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 though the IAM permissions boundary and the aws:CurrentTime global context key.

Application Migration Service customers should use Amazon EBS encryption.

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 addressses 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-tosite VPN. Learn more about the AWS Site-to-site VPN.

Application Migration Service creates and uses the "aws-replication" user within the Source server. The 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**
> Application Migration Service only uses these permissions to read from block devices.

Compliance validation for Application Migration Service

Third-party auditors assess the security and compliance of 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 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 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 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 (p. 392)
- Troubleshooting Communication Errors (p. 394)
- Troubleshooting Agent Issues (p. 398)
- Troubleshooting agentless replication issues (p. 403)
- Other Troubleshooting Topics (p. 403)

Troubleshooting Launch Errors

Topics

- Do I need to recreate the entire launch template for every version? (p. 392)
- Error - AccessDeniedException - Must be admin user (p. 393)
- VPCIdNotSpecified error (p. 394)

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, Application Migration Service (MGN) uses the version marked as the default for its purposes. So in order to actually have 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 on 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 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 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 MGN. You must be the Admin user of your AWS Account to initialize MGN. Learn more about initiatlizng 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 MGN 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"

Troubleshooting Communication Errors

Topics

- Solving Communication Problems over TCP Port 443 between the Staging Area and the Application Migration Service Service Manager (p. 395)
- Calculating the Required Bandwidth for TCP Port 1500 (p. 396)
- Verifying Communication over Port 1500 (p. 396)
- Solving Communication Problems over Port 1500 (p. 397)

Solving Communication Problems over TCP Port 443 between the Staging Area and the Application Migration Service Service Manager

- **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 you are allowing outbound DNS resolution and 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 on **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 S3, EC2, and MGN in the AWS Region.

  6. If the address is not **0.0.0.0/0**, you will need 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.

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 machines. The recommended bandwidth should be at least the sum of the average write speed of all replicated Source machines.

Minimal bandwidth = the sum of the write speed of all Source machines

For example, suppose you are replicating two Source machines. One has a write speed of 5 MBps (meaning it 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 Machines

To calculate the required bandwidth for transferring replicated data over TCP Port 1500, you need to know the write speed of your Source machines. Use the following tools to find the write speed of your Source machines:

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 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 machine, 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 presents 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 machine, 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 machine/infrastructure may block communication.
- The **Use VPN...** checkbox in Application Migration ServiceConsole 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 enable the network ACL on the Staging Area subnet:

1. Sign in to the AWS console, click on **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 t**ab, 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 on the **Edit** button.

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 on **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 machines.

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 machines.

   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 (p. 398)

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 Application Migration Service Console. After you fix the issue that caused the installation failure, you need to re-run 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 machine, 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).

At the moment, only 64 bit operating systems are supported for Application Migration Service.

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, (broken registry key etc),

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 (p. 90).

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 Machine

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 machine. 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:

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

      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

Note: This command looks for kernel-devel.

On Debian/Ubuntu: apt-cache search linux-headers

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

   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 sameversion 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 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

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 MGN Service Manager.

6. **Powerpath support**

   powermt check

   If so, contact AWS Support for instructions on how to install the 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 python installer_linux.py

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 power shell 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.

Troubleshooting agentless replication issues

1. If a machine is stalled for over an hour due to a bad VM configuration, we recommend manually deleting the VM snapshot.

2. Replicating two or more servers that share the same UUID on VMWare may cause a stall due to a VM configuration error. If you experience a stall and have two or more servers that share a UUID, change the UUID of one of the servers to solve the issue.

Other Troubleshooting Topics

Topics

- Windows License Activation - AWS (p. 403)
- Migration Leaving Behind Replication Volumes after Cutover (p. 404)
- Replication Lag Issues (p. 404)
- Windows Driver Changes (p. 404)
- Windows Dynamic Disk Troubleshooting (p. 404)
- Deleting MGN Resources (p. 404)

Windows License Activation - 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 Application Migration Service.

Most likely, you have a script running in your AWS account that renames EBS volumes to match the name of the EC2 instance they are attached to.

However, by renaming an EBS volume used by Application Migration Service for replication you are severing its association with Application Migration Service and Application Migration Service will not automatically clean up such volumes.

Replication Lag Issues

Potential solutions:

- Make sure that the Source server is up and running.
- Make sure that Application Migration Services 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 machine was rebooted recently or the Application Migration Service services were restarted, the disks are re-read after this and until it's finished, the Lag will grow.
- If the Source machine had a spike of write operations, the Lag will grow until Application Migration Service manages to flush all the written data to the test or cutover instance Replication Server.

Windows Driver Changes

Users may see changes in Windows drive letter assignments (ex. Drive D changed to E) on Target machines launched by 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 re-mapping 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 MGN Resources

You can delete various MGN resources, including source severs, 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 Settings template.

This command:

- Deletes a single Replication Settings 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.

FAQ

Topics

- Application Migration Service Concepts (p. 406)
- General Questions (p. 406)
- Agent Related (p. 411)
- Agentless replication related (p. 414)
- Replication Related (p. 417)
- AWS Related (p. 419)
- Does MGN work with...? (p. 426)

Application Migration Service Concepts

Topics

- What is the Recovery Time Objective (RTO) of Application Migration Service? (p. 406)
- What is the Recovery Point Objective (RPO) of Application Migration Service? (p. 406)

What is the Recovery Time Objective (RTO) of Application Migration Service?

The Recovery Time Objective (RTO) of Application Migration Service is typically measured in minutes. The RTO is highly dependent on the OS boot time.

What is the Recovery Point Objective (RPO) of Application Migration Service?

The Recovery Point Objective (RPO) of Application Migration Service is typically in the sub-second range.

General Questions

Topics

- Can Application Migration Service protect or migrate physical servers? (p. 407)
- What data is stored on and transmitted through Application Migration Service servers? (p. 407)
- What is the Recovery Time Objective (RTO) of Application Migration Service? (p. 407)
- What is the Recovery Point Objective (RPO) of Application Migration Service? (p. 407)
- What to consider when replicating Active Directory (p. 407)
- Does Application Migration Service work with LVM and RAID configurations? (p. 407)
- What is there to note regarding SAN/NAS Support? (p. 407)
- Does Application Migration Service support Windows License Migration? (p. 408)
- Can you perform an OS (Operating System) upgrade with Application Migration Service? (p. 408)
- What are the MGN service quota limits? (p. 408)
- What are the Private APIs used by MGN to define actions in the IAM Policy? (p. 409)
- Which Post Launch scripts does MGN support? (p. 410)

Can Application Migration Service protect or migrate physical servers?

Because 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?

Application Migration Service store only configuration and log data on the Application Migration Service 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 is the Recovery Time Objective (RTO) of Application Migration Service?

The Recovery Time Objective (RTO) of Application Migration Service is typically measured in minutes. The RTO is highly dependent on the OS boot time.

What is the Recovery Point Objective (RPO) of Application Migration Service?

The Recovery Point Objective (RPO) of Application Migration Service is typically in the sub-second range.

What to 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 Application Migration Service work with LVM and RAID configurations?

Yes, 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, 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 Application Migration Service support Windows License Migration?

Application Migration Service conforms to the Microsoft Licensing on AWS guidelines.

Can you perform an OS (Operating System) upgrade with Application Migration Service?

No. Application Migration Service copies the entire machine as-is. However, you can copy the data disks exclusively and attach them to a new machine with an upgraded OS.

What are the MGN service quota limits?

The following are the 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: 20	The maximum number of servers that can be actively replicating at any time. You can increase this value to 60. For larger migrations, contact Support.
Max Non-Archived Source Servers	Each supported AWS Region: 4000	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".
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

Name	Default	Description
		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.
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 MGN service limits in the AWS General Reference

What are the Private APIs used by 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 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\

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 Service 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 ran 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

}
```

Agent Related

Topics

- What does the AWS Replication Agent do? (p. 411)
- What kind of data is transferred between the Agent and the Application Migration Service Service Manager? (p. 411)
- Can a proxy server be used between the source server and the Application Migration Service Console? (p. 412)
- What are the pre-requisites needed to install the AWS Replication Agent? (p. 412)
- What ports does the AWS Replication Agent utilize? (p. 412)
- What kind of resources does the AWS Replication Agent utilize? (p. 412)
- Can Application Migration Service migrate containers? (p. 413)
- Does the AWS Replication Agent cache any data to disk? (p. 413)
- How is communication between the AWS Replication Agent and the Application Migration Service Service Manager secured? (p. 413)
- Is it possible to change the port the AWS Replication Agent utilizes from TCP Port 1500 to a different port? (p. 413)
- How do I manually uninstall the Application Migration Service Agent from a server? (p. 413)
- When do I need to reinstall the Agent? (p. 413)
- How much bandwidth does the AWS Replication Agent consume? (p. 414)
- How many disks can the AWS Replication Agent replicate? (p. 414)
- Is it possible to add a disk to replication without a complete resync of any disks that have already been replicated? (p. 414)
- Is the AWS Replication Agent installed on launched Test and Cutover instances? (p. 414)

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 Application Migration Service Replication Server, ensuring near-zero RPO.

What kind of data is transferred between the Agent and the Application Migration Service Service Manager?

The AWS Replication Agent sends the following types of information to the Application Migration Service Service Manager:

- 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.
- Installed applications (Windows)
- Installed Packages (Linux)
- Running services.
- Machine's Private IP address.

Can a proxy server be used between the source server and the 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 whitelisted the MGN IPs and URLs (p. 86)for both SSL Interception and Authentication.

What are the pre-requisites 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.

Pre-requistes can be found here (p. 91).

What ports does the AWS Replication Agent utilize?

The Agent utilizes TCP Port 443 to communicate to the Application Migration Service Service Manager and TCP Port 1500 for replication to AWS.

What kind of resources does the AWS Replication Agent utilize?

The AWS Replication Agent is lightweight and non-disruptive. The agent utilizes approximately 5% CPU and 250MB of RAM.

Can Application Migration Service migrate containers?

Application Migration Service only supports the replication of full servers. Nevertheless, Application Migration Service 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?

Application Migration Service does not write any cache or do any sort of journaling to disk. The Agent holds a buffer which is large enough to map all volume's blocks ~250MB 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 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 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 Application Migration Service Service Manager 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 Application Migration Service Agent can only utilize TCP Port 1500 for replication.

How do I manually uninstall the Application Migration Service Agent from a server?

You can the section called “Uninstalling the Agent” (p. 122).

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 (ex. Windows Server 2012 to Windows Server 2016)

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 enabled by selecting the specific server and selecting the **Settings** page in the Application Migration Service Console.

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, the agent will automatically detect the additional disk, and it will actually show up on the MGN console, under 'Disks Settings'. However, you will notice that it is not marked for replication.

The only way to get this disk to replicate is to re-install the agent. Before re-installing, you can note the current 'Total Replicated storage'. When you re-install 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 re-scanning 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 re-install 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.

Agentless replication related

Topics

- In which situations would you recommend using agentless replication (snapshot shipping)? (p. 415)
- In which situations would you recommend using agent-based replication? (p. 415)

- How does agentless replication work? (p. 415)
- Does agentless replication require installing any component in the customer's source data center? (p. 415)
- Is the agentless feature available in all Regions that Application Migration Service (MGN) service supports? (p. 415)
- Does agentless replication support the same source operating systems that are supported by agent-based replication? (p. 416)
- Is the agentless feature supported in CloudEndure Migration? (p. 416)
- Which virtualization environments are supported by the agentless feature? (p. 416)
- On which operating systems can the MGN vCenter Client be installed? (p. 416)
- Do I need to generate special credentials to install the MGN vCenter Client? (p. 416)
- What are the agentless replication prerequisites? (p. 416)
- How do I install the MGN vCenter Client? (p. 416)

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 and 7.0.

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. (p. 127)

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 Application Migration Service (MGN) service supports?

Yes. Both agent-based and agentless replication is supported in 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 (p. 125) of agent-based. Additionally, the following OS are supported by agentless replication, but are not supported for agent-based replication:

- Windows Server 2003 - 64 bit only
- Windows Server 2008 - 64 bit only
- CentOS 5

Is the agentless feature supported in CloudEndure Migration?

No. This feature is only available on Application Migration Service.

Which virtualization environments are supported by the agentless feature?

The agentless replication feature is available for vCenter versions 6.7 and 7.0. 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 64 bit Ubuntu 18, RH8 or AL2 VMs.

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. 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. Learn more in the agentless replication documentation. (p. 130)

What are the agentless replication prerequisites?

The only prerequisite for agentless replication is to ensure that you have initialized Application Migration Service. (p. 3)

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 (p. 137).

Replication Related

Topics

- What is the lifecylce of the snapshots and volumes automatically created during migration? (p. 417)
- What do Lag and Backlog mean during replication? (p. 417)
- Is the replicated data encrypted? (p. 418)
- How is the Replication Server provisioned and managed in the Staging Area? (p. 418)
- What type of Replication Server is utilized in the Application Migration Service Staging Area? (p. 418)
- Does Application Migration Service compress data during replication? (p. 418)
- Are events that are generated by the Application Migration Service servers logged in Cloudtrail in AWS? (p. 418)
- How many snapshots does Application Migration Service create? (p. 418)
- Does Application Migration Service Delete Snapshots? (p. 418)
- How much capacity is allocated to the Staging Area? (p. 418)
- Why is 0.0.0.0:1500 added to inbound rules in the Staging Area? (p. 419)
- Can Application Migration Service replicate Oracle ASM? (p. 419)
- How long does a rescan take? (p. 419)
- Is Application Migration Service replication crash consistent? (p. 419)

What is the lifecylce 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.

Is the replicated data encrypted?

Application Migration Service encrypts all the data in transit.

How is the Replication Server provisioned and managed in the Staging Area?

Application Migration Service provisions the Replication Server(s) and automatically manages the addition and removal of the servers as necessary.

What type of Replication Server is utilized in the Application Migration Service Staging Area?

Application Migration Service provisions a t3.Small server. The typical ratio of volumes to replication servers is 15:1.

Does Application Migration Service compress data during replication?

Yes, 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 Application Migration Service servers logged in Cloudtrail in AWS?

Yes, Application Migration Service generates standard AWS API calls that are visible in CloudTrail.

How many snapshots does 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 Application Migration Service Delete Snapshots?

Application Migration Service automatically deletes snapshots that are no longer used (such as those left over after source servers have been removed from the 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?

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 Application Migration Service replicate Oracle ASM?

Replication of Oracle with ASM is supported.

Application Migration Service replication works directly on block devices and not on mounts. ASM volumes are presented as block devices and therefore replicated transparently by Application Migration Service. MGN does not support use of the Oracle ASM Filter Driver. Servers with this feature enabled cannot be migrated using MGN. The servers will appear to be in CDP, but the data will not actually replicate.

How long does a rescan take?

A rescan may occur after a reboot of the source server. 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 re-scan.) The re-scan is functioning normally as long as its moving forward and is not "stuck".

Is Application Migration Service replication crash consistent?

Yes, Application Migration Service is crash-consistent.

AWS Related

Topics

- What does the Application Migration Service Machine Conversion Server do? (p. 420)
- How do I change the server AMI on AWS after Migration? (p. 420)
- Which AWS services are automatically installed when launching a Test or Cutover instance? (p. 420)
- How long does it take to copy a disk from the Application Migration Service Staging Area to production? (p. 420)
- What are the differences between Conversion Servers and Replication Servers? (p. 420)
- Can I prevent Application Migration Service from cleaning up Test instance resources in AWS? (p. 421)
- Why are my Windows Server disks read-only after launching the Test or Cutover instance? (p. 421)
- What impacts the conversion and boot time of Test and Cutover instances? (p. 421)
- How is the AWS Licensing Model Tenancy chosen for Application Migration Service? (p. 421)
- How does Application Migration Service interact with Interface VPC Endpoints? (p. 422)
- How do I use MGN with CloudWatch and EventBridge dashboards? (p. 422)

What does the 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.

How do I change the server AMI on AWS after Migration?

After the machine has been launched by 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 Application Migration Service.

Which AWS services are automatically installed when launching a Test or Cutover instance?

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 combining the Application Migration Service APIs and the AWS APIs - you can use the 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.

Application Migration Service installs EC2Launch (Windows 2016 only.) Customers need to configure EC2Launch based on the specific requirements explained here. 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 Application Migration Service Staging Area to production?

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 Application Migration Service 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 Application Migration Service Service Manager.

The Conversion Server machines, just like the Replication servers are managed automatically by Application Migration Service. Any attempt to disrupt their automated functionality will result in failed conversions.

Can I prevent Application Migration Service from cleaning up Test instance resources in 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 enable 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 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, 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 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.

How is the AWS Licensing Model Tenancy chosen for Application Migration Service?

Application Migration Service conforms to the Microsoft Licensing on AWS guidelines.

How does 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 Application Migration Service. You can use this connection to enable 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 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 Application Migration Service, you define an *interface VPC endpoint* for 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 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 enables 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 Application Migration Service using CloudWatch, which collects raw data and processes it into readable, near real-time metrics. 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:

aws
Services
Search for services, features, marketplace
[Alt+S]
ReadOnly/taitza-Isenga
CloudWatch
Cross service dashboard
Cross service dashboard
Info
1h
3h
12h
1d
1w
Cross service dashboard
Filter by resource group
Info
Application Migration Service
View Application Migration Service dashboard
LagDuration: Average
1.00
0.50
0
05:00
06:00
07:00
s-0901409c255f918da
s-06e1ac730122ba55a
s-0e54e450f951ed1b3
s-07193d06cc71130ae
s-02b8e47bb9fb3f9f0
s-06bf399851008be67
s-0428b26ece9e4e64b
ActiveSourceServerCount:
Count
1,664.0
1,663.0
1,662.0
04:30
05:00
ActiveSourceServerCount
EC2
View EC2 dashboard
CPU Utilization: Average
No data available.
Try adjusting the dashboard time range.
StatusCheckFailed: Sum
Elastic Block Store (EBS)
View Elastic Block Store (EBS) dashboard
VolumeReadBytes: Sum
VolumeWriteBytes: Sum

MGN events can be selected when defining a rule from the EventBridge console:

Learn more about monitoring MGN (p. 351).

Does MGN work with...?

Does MGN work with Microsoft Windows Failover Clustering?

Yes.

Does MGN work with Bitlocker encryption

MGN does not support OS-based disk encryption features such as BitLocker. These should be disabled before using MGN.

Release Notes

May 2022

- 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. (p. 127)

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, Ohio), US West (Oregon), Europe (Ireland, Frankfurt, Stockholm), Asia Pacific (Sydney, Singapore).

AWS glossary

For the latest AWS terminology, see the AWS glossary in the *AWS General Reference*.